PingOne

July 3, 2025

PINGONE

Copyright

All product technical documentation is
Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

Refer to https://docs.pingidentity.com for the most current product documentation.

Trademark

Ping Identity, the Ping Identity logo, PingAccess, PingFederate, PingID, PingDirectory, PingDataGovernance, PingIntelligence, and PingOne are registered trademarks of Ping Identity Corporation ("Ping Identity"). All other trademarks or registered trademarks are the property of their respective owners.

Disclaimer

The information provided in Ping Identity product documentation is provided "as is" without warranty of any kind. Ping Identity disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Ping Identity or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Ping Identity or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Table of Contents

PingOne . . . 23

Release Notes . . . 27

Early Access . . . 59

Introduction . . . 61

Getting Started . . . 80

- Accessing the admin console . . . 84
- Starting a trial . . . 86
  - Creating an environment . . . 89
  - Building a customer solution . . . 92
  - Building a workforce solution . . . 97
- Building solutions . . . 99
- Managing administrators . . . 104
  - Invite administrators to register . . . 109
    - Accepting the administrator account registration invitation . . . 109
  - Adding administrators . . . 109
    - Completing the administrator account registration . . . 109
  - Managing administrator roles . . . 109
- PingOne SSO . . . 117
  - Getting started with PingOne SSO . . . 119
  - Setting up single sign-on . . . 120
    - PingAccess . . . 121
    - PingCentral . . . 128
    - PingDirectory . . . 134
    - PingFederate . . . 138
    - PingOne Advanced Identity Cloud . . . 143
    - PingOne for Enterprise or PingID . . . 146
- Strong Authentication (MFA) . . . 149
- Licenses and Platform Limits . . . 151
  - Viewing your licenses . . . 152
  - License assignment . . . 153
  - Standard license types . . . 154
  - License FAQ . . . 155
  - Licenses and identity limits . . . 155
  - Standard platform limits . . . 158
- Platform logging and reporting . . . 163

Services logging and reporting . . . 165

Tutorials . . . 166
Customize the look and feel of PingOne authentication pages . . . 168
Add a SAML application . . . 175
Build a custom sign-on policy . . . 178
Create a group . . . 180
Control user access . . . 182
Add custom attributes to a user . . . 184
Sync users between two environments . . . 186
Integrate PingOne with a Node.js Express app. . . . 191
Configure a multi-factor authentication experience using PingOne and PingID. . . . 196
Starting a trial . . . 197
Adding a new environment . . . 200
Adding an existing PingID tenant to a new PingOne environment. . . . 205
Creating demo users . . . 209
Creating a group with dynamic membership . . . 211
Creating a web application . . . 215
Performing the user simulation . . . 219
Accessing the application portal . . . 222
Reviewing the synchronization of users in PingID . . . 223
Configure a basic passwordless login experience using PingOne and PingOne MFA . . . 224
Starting a trial . . . 225
Adding an environment . . . 228
Creating a registration application . . . 231
Creating a login application . . . 233
Creating a registration policy . . . 235
Creating a passwordless login policy. . . . 237
Creating a group with dynamic membership . . . 239
Copying the sign-on URLs . . . 242
Simulating a registration and successful login . . . 244
Simulating a registration and access control-based login failure . . . 249
Accessing the application portal . . . 254

Use Cases . . . 255
Configuring PingOne as an external IdP in ZIdentity . . . 257
Securing your APIs using PingOne and Amazon Verified Permissions . . . 257
Setting up PingOne SSO and PingID as the external MFA provider for Microsoft Entra ID . . . 265
Setting up PingOne SSO, DaVinci, and PingID as the external MFA provider for Microsoft Entra ID . . . 290
Using PingGateway no-code application and API protection . . . 319

PingOne Expression Language . . . 319
Using the expression builder . . . 321
Samples . . . 322

Expressions and concatenation . . . 326
Arrays and lists . . . 327
Maps and objects . . . 328
Operators . . . 330
Collection operations . . . 333
Disabled and restricted SpEL features . . . 335
Variables . . . 336
Custom library functions . . . 338
Null safe usage . . . 372
References . . . 374

Overview page . . . 374

Monitoring . . . 377
Dashboards . . . 379
Authentication dashboard . . . 379
User Demographics Dashboard . . . 380
MFA dashboard . . . 383
Enrollments chart . . . 386
Enrollments by type chart . . . 386
SMS/Voice chart . . . 388
User devices and app version charts . . . 389
Authentications by type chart . . . 392
Audit . . . 393
Running an audit report . . . 393
Audit parameters . . . 394
Alerts . . . 396
Viewing alerts . . . 396
Adding an alert . . . 397
Editing an alert . . . 397
Deleting an alert . . . 398

Directory . . . 398
Users . . . 400
Viewing users . . . 400
Searching for users . . . 402
Viewing developer information for a user . . . 404
Adding a user . . . 405
Managing user roles . . . 407
Editing a user . . . 412
Managing a user’s devices and services . . . 416
Managing a user’s credentials . . . 417
User Devices report . . . 418
Enabling consent updates . . . 418

Enabling end users to view consents . . . 419
Viewing consents for a user . . . 419
Enabling or unlocking a user account or device . . . 419
Deleting a user . . . 420
Managing user sessions . . . 421
Changing a user's population . . . 422
Verifying an email address for a user . . . 423
Resetting a user password . . . 424
SCIM filter language . . . 424
Groups . . . 427
About groups and populations . . . 427
Viewing groups . . . 436
Viewing group membership . . . 439
Searching for groups . . . 440
Managing groups . . . 441
Just-in-time provisioning of external groups . . . 453
Populations . . . 455
Managing populations . . . 455
User Attributes . . . 461
Attribute access control . . . 461
Viewing user attributes . . . 461
Adding user attributes . . . 462
Editing user attributes . . . 463
Mapping attributes . . . 464
Disabling or enabling a user attribute . . . 465
Viewing the user attribute schema . . . 465
Characters supported in user attributes . . . 466
Administrator Roles . . . 471
Viewing role details . . . 476
Adding a custom administrator role . . . 478
Custom role scenarios . . . 484
Viewing administrator role events . . . 489
Group roles . . . 490

Applications . . . 491
Applications . . . 493
Viewing application details . . . 494
Viewing sign-on statistics by application . . . 496
Adding an application . . . 497
Editing an application . . . 498
SAML . . . 499
OIDC . . . 506
Native . . . 513
Single page . . . 523

Worker . . . 532
Device authorization . . . 540
Configuring web applications . . . 548
Creating a web application. . . . 548
Associating an authentication policy with a web app . . . 550
Deleting an application . . . 552
System applications . . . 552
Device custom verification URIs . . . 553
Configuring a redirect for a device custom verification URI . . . 554
Redirect URIs . . . 556
Application access control. . . . 558
Authentication policies for applications . . . 560
Applying authentication policies . . . 561
Viewing OIDC attributes . . . 563
Customizing OIDC attributes . . . 563
Device authorization . . . 564
Request Parameter Signature Requirement . . . 569
Pushed authorization requests . . . 569
RequestedAuthnContext . . . 571
CORS . . . 572
Refresh token rotation. . . . 572
Rotating the client secret . . . 573
Viewing the client secret . . . 573
Generating a client secret . . . 574
Revoking a client secret . . . 575
Including external groups . . . 575
Using the advanced configuration editor . . . 576
Configuring roles for a worker application . . . 577
Viewing scopes . . . 579
Editing scopes. . . . 580
Customizing access token lifetime . . . 580
SAML 2.0 single logout . . . 582
PKCE enforcement . . . 584
Editing custom ID token mappings. . . . 584
Getting an access token . . . 586
Downloading IdP metadata . . . 586
Response types . . . 587
Response mode values . . . 587
Grant types . . . 588
Token endpoint authentication methods . . . 589
Editing an application for the Microsoft Entra ID external authentication method . . . 589
Application catalog . . . 589
Adding an application from the application catalog . . . 590

Adding Microsoft 365 to the application portal . . . 592
Enabling Kerberos authentication . . . 595
Configuring an authentication claim for the Microsoft 365 application . . . 596
Adding AWS to the application portal . . . 597
Resources . . . 599
Resource scopes . . . 599
Viewing resources . . . 600
Adding a custom resource . . . 601
Editing a resource . . . 602
Editing an OIDC resource . . . 603
Deleting a resource . . . 604
Rotating the client secret . . . 605
Viewing the client secret . . . 605
Generating a client secret . . . 606
Revoking a client secret . . . 607
Access tokens and ID tokens . . . 607
Customizing access tokens . . . 608
Token introspection . . . 608
Attribute access control . . . 609
Configuring attribute access control . . . 609
Application permissions . . . 610
Adding application permissions . . . 611
Application portal . . . 614
Configuring the application portal . . . 615
Applying authentication policies to the application portal . . . 615
Adding resource links to the application portal . . . 617
Editing a resource link . . . 617
Deleting a resource link . . . 618

DaVinci . . . 618

Authentication . . . 620
Authentication policies . . . 622
Viewing authentication policies . . . 622
Adding an authentication policy . . . 622
Adding a login authentication step . . . 624
Adding a multi-factor authentication or PingID step . . . 625
Adding an identifier first authentication step . . . 626
Adding a progressive profiling step . . . 628
Adding a terms of service prompt . . . 629
Adding an external identity provider sign-on step . . . 629
Editing an authentication policy . . . 631
FIDO2 . . . 635
Progressive profiling . . . 636

Identifier first authentication . . . 636
Setting up passwordless authentication. . . . 637
Setting the default authentication policy . . . 637
Resolving a lockout . . . 637
Password policies . . . 638
Managing password policies . . . 640
MFA policies . . . 642
Adding an MFA policy . . . 643
FIDO policies . . . 643
Adding a FIDO policy . . . 644
Managing FIDO policies . . . 649
Managing the Global Authenticators Table . . . 649
MFA Settings . . . 651
Configuring MFA settings . . . 651
Step-up authentication for APIs . . . 652
Setting up step-up authentication for APIs . . . 654

Strong Authentication (MFA) . . . 655
Introduction to strong authentication (MFA) . . . 659
Overview of authentication methods . . . 659
What is the difference between PingID and PingOne MFA? . . . 667
What is a typical strong authentication (MFA) workflow? . . . 668
Setting up an environment for strong authentication (MFA) . . . 669
Creating a new PingOne environment with MFA . . . 669
Integrating a PingID account with a PingOne environment . . . 670
What you need to know before integrating or migrating a PingID account into a PingOne environment . . . 671
Integrating a PingID account with a new PingOne environment . . . 675
Integrating an existing PingID account with an existing PingOne environment . . . 678
Migrating PingID management from the legacy PingID admin portal to a PingOne environment . . . 683
Considerations after integrating or migrating a PingID account into a PingOne environment . . . 685
Configuring strong authentication methods (MFA) . . . 685
Configuring mobile applications . . . 686
(Workforce Only) Configuring the PingID mobile application settings . . . 687
PingID mobile app PIN requirements . . . 690
PingID Mobile Device Management (MDM) . . . 691
Managing MDM tokens . . . 692
Generate an MDM token . . . 693
Rotate an MDM token . . . 693
Revoke an MDM token . . . 694

Third-party MDM system configuration for PingID integration . . 695
Configuring Workspace ONE UEM for PingID mobile app 695
Installing an APNs certificate for iOS in Workspace ONE UEM. 696
Configuring Android for Work for Workspace ONE UEM. 699
Configuring Workspace ONE UEM for PingID MDM integration 701
Updating a PingID token in Workspace ONE UEM 707
Configuring MobileIron for PingID 710
Installing an APNs certificate for iOS in MobileIron 710
Configuring Android for Work for MobileIron . 713
Configuring MobileIron for PingID MDM integration 715
Updating a PingID token in MobileIron 721
Configuring Microsoft Intune for PingID 723
Installing an APNs certificate for iOS in Microsoft Intune 724
Configuring Android for Work for Microsoft Intune 728
Adding the PingID mobile app for iOS in Microsoft Intune 734
Adding the PingID mobile app for Android in Microsoft Intune 737
Setting the PingID mobile app configuration policies for Microsoft Intune 740
Updating a PingID token in Microsoft Intune . 745
Configuring authenticator app authentication 747
Configuring email authentication 747
Configuring FIDO2 authentication (Passkeys). 748
(Customer Only) Configuring WhatsApp authentication 749
Configuring SMS and voice authentication 749
(Workforce Only) Configuring the PingID desktop application 751
Configuring the PingID desktop app PIN 752
Configure PingID Proxy for the PingID desktop app 753
Configuring Proxy Auto Configuration for the PingID desktop app 756
Configuring Kerberos Proxy authentication for the PingID desktop app 756
(Workforce Only) Configuring YubiKey OTP authentication for PingID 757
Configuring OATH token authentication 758
Configuring an MFA policy for strong authentication 759
Updating an existing MFA policy to use FIDO2 769

Strong authentication (MFA) integrations . . . 771
Integrating with PingFederate . . . 772
Configuring PingID policy . . . 774
Managing PingID in PingOne . . . 774
Accessing the legacy PingID admin portal from PingOne . . . 774
Using MyAccount to manage PingID devices . . . 775
PingID Offline MFA . . . 775
User directory for PingID Offline MFA . . . 778
Bypass MFA for a specific user . . . 780
Pre-populating or restricting user registration data . . . 780
PingID user life cycle management. . . . 781
PingID branding and themes . . . 781
PingID language support . . . 781
Using the PingID Device Trust agent. . . . 782
Strong authentication monitoring and dashboards . . . 792

Threat Protection using PingOne Protect. . . . 793
Introduction to PingOne Protect . . . 796
Getting started with PingOne Protect . . . 797
Risk policies . . . 817
Creating and managing staging policies . . . 819
Evaluating staging policy risk data . . . 820
Predictors . . . 823
Configuring predictors . . . 830
Adding predictors. . . . 833
Adding custom predictors . . . 835
Adding composite predictors . . . 836
Deleting a predictor . . . 839
Testing predictors . . . 840
Risk evaluations . . . 841
Reviewing risk evaluations . . . 842
Updating completion status for risk evaluations . . . 845
Providing feedback for risk evaluations . . . 846
Threat Protection Dashboard . . . 846
Threat Protection Dashboard filters . . . 849
Risk heat map . . . 851
Risk events . . . 852
High risk models . . . 853
Browser distribution . . . 854
OS distribution . . . 855
Top 20 high risk users . . . 856
Risky IP . . . 857
PingOne Signals (Protect) SDK . . . 858
Best practices for PingOne Protect . . . 858

Troubleshooting PingOne Protect . . . 861

Identity Verification using PingOne Verify . . . 863
Introduction to PingOne Verify . . . 866
Getting started with PingOne Verify . . . 869
PingOne Verify key concepts . . . 880
Document authentication . . . 880
Face verification . . . 882
Configuring language localization . . . 884
Types of verification . . . 885
ID verification . . . 888
Enabling user ID verification . . . 888
Viewing user ID verification status . . . 890
Resetting a user's ID verification status . . . 892
Manually approving a user's ID . . . 894
Verify policies . . . 896
Creating a verify policy . . . 896
Managing a verify policy . . . 900
Deleting a verify policy . . . 906
Identity Verification Dashboard . . . 906
Viewing license information . . . 908

Digital Credentials using PingOne Credentials . . . 908
Introduction to PingOne Credentials . . . 910
Credentials scenarios . . . 916
Creating and receiving a credential . . . 917
Presenting and verifying a user credential . . . 918
Revoking a credential and notifying the user . . . 920
Getting started with PingOne Credentials . . . 922
Customizing notification templates . . . 927
Credential management method comparison . . . 929
Creating a credential . . . 930
Editing a credential . . . 935
Revoking a credential . . . 938

Authorization using PingOne Authorize . . . 938
Introduction to Authorization . . . 942
Getting started with PingOne Authorize . . . 948
Adding PingOne Authorize to your environment . . . 948
Adding a worker application . . . 949
Tutorials . . . 952
Build dynamic authorization policies . . . 952
Building your first dynamic authorization policy . . . 952
Adding an attribute . . . 953

Adding and testing a policy . . . 956
Updating and retesting a policy . . . 960
Publishing a policy and configuring an endpoint . . . 963
Making decision requests and examining recent decisions . . . 966
Manage API access . . . 975
Tutorial 1: Controlling access to APIs managed by an API service . . . 975
Setting up your environment . . . 976
Adding a banking application in PingOne . . . 979
Getting an access token . . . 984
Configuring the authorization plugin for Kong Gateway . . . 987
Adding a managed API service for the Meme Game in PingOne . . . 992
Adding a Meme Game application in PingOne . . . 994
Tutorial 2: Controlling access to specific API operations . . . 999
Adding player and admin users for the Meme Game . . . 1000
Defining an operation for a privileged action . . . 1003
Getting memes of another user . . . 1007
Tutorial 3: Fine-grained API authorization . . . 1011
Adding users for the Meme Game . . . 1012
Defining an API operation that uses fine-grained policies . . . 1014
Adding a game invitee list attribute . . . 1016
Adding a policy for the API operation . . . 1018
Testing the end-to-end use case with Postman . . . 1025
Trust Framework . . . 1028
Attributes . . . 1029
Adding an attribute . . . 1031
Adding resolvers to an attribute . . . 1032
Adding processors to an attribute . . . 1034
Adding value settings to an attribute . . . 1036
Resolvers . . . 1037
Built-in attributes . . . 1047
Generated attributes . . . 1055
Generating an attribute . . . 1057
Interpolating attributes . . . 1061
Adding repetition settings to an attribute . . . 1063
Deleting an attribute . . . 1065
Services . . . 1066
Connecting a service . . . 1067
Connecting an HTTP service . . . 1068
Connecting to PingOne Protect . . . 1073
Connecting an LDAP Gateway service . . . 1076
Service caching . . . 1080
Service configuration constraints . . . 1081
Deleting a service . . . 1082

Conditions . . . 1082
Adding a named condition . . . 1088
Processors . . . 1090
Value settings . . . 1097
Testing Trust Framework elements . . . 1101
Viewing dependents . . . 1109
Code editor . . . 1110
Policies . . . 1112
Adding a policy or policy set. . . . 1115
Targets . . . 1116
Statements . . . 1116
Statement templates . . . 1117
Adding statements to policies and rules . . . 1131
Combining algorithms . . . 1134
Policy testing . . . 1136
Testing policies . . . 1136
Testing statement processing . . . 1141
Version history . . . 1144
Naming versions . . . 1145
Publishing versions. . . . 1146
Decision endpoints . . . 1147
Adding a decision endpoint . . . 1148
Editing a decision endpoint . . . 1149
Deleting a decision endpoint . . . 1150
PingOne Authorize event monitoring . . . 1151
Recent decisions . . . 1154
API services . . . 1156
Defining your API in PingOne Authorize . . . 1158
Defining operations for protected actions . . . 1161
Adding custom policies for API services and operations . . . 1168
Deploying an API service. . . . 1174
Editing an API service . . . 1175
Deleting an API service or operation . . . 1177
Troubleshooting API Access Management . . . 1178
API gateways . . . 1182
API gateway integrations . . . 1182
Amazon Web Services integration . . . 1183
Setting up PingOne Authorize . . . 1184
Configuring Amazon API Gateway . . . 1185
Configuring Amazon CloudFront. . . . 1193
Apigee integration . . . 1203
Setting up PingOne Authorize . . . 1203
Configuring Apigee . . . 1204
Configuring the PingAuth shared flow . . . 1207

Kong Gateway integration . . . 1210
Setting up PingOne Authorize . . . 1211
Configuring Kong Gateway . . . 1213
Troubleshooting Kong Gateway integration . . . 1219
Kong Konnect integration . . . 1221
Setting up PingOne Authorize . . . 1222
Configuring Kong Konnect . . . 1222
Editing an API gateway . . . 1232
Deleting an API gateway . . . 1232
Rotating an API gateway credential . . . 1232
Application roles . . . 1234
Adding an application role . . . 1235
Authorization Dashboard . . . 1237
Authorization API reference . . . 1240

Integrations . . . 1240
External IdPs . . . 1242
Viewing IdPs . . . 1243
Adding a vendor-specific IdP . . . 1244
Amazon . . . 1244
Apple . . . 1247
Facebook . . . 1252
GitHub . . . 1255
Google . . . 1259
LinkedIn . . . 1262
LinkedIn (legacy) . . . 1264
Microsoft . . . 1267
OIDC authentication . . . 1268
Entra ID external authentication method . . . 1273
PayPal . . . 1273
X . . . 1276
Yahoo . . . 1279
Adding an IdP - OIDC . . . 1282
Discovery document URI . . . 1284
Adding an IdP - SAML . . . 1285
Editing an IdP . . . 1287
Deleting an IdP . . . 1288
SAML 2.0 single logout . . . 1289
Downloading metadata for SAML IdPs . . . 1291
IdP attributes . . . 1292
Mapping the group attribute from an external IdP . . . 1292
Initiating SSO from PingOne . . . 1293
Setting up IdP-initiated SSO . . . 1293

Authoritative IdPs . . . 1295
Configuring an authoritative IdP . . . 1297
Viewing or changing the authoritative IdP for a user . . . 1297
Provisioning . . . 1298
Inbound and outbound provisioning . . . 1298
Outbound group provisioning . . . 1300
Viewing provisioning rules and connections . . . 1300
Group provisioning FAQ . . . 1301
Configuring provisioning . . . 1303
Creating a connection . . . 1304
Creating an outbound rule . . . 1305
Creating an inbound rule . . . 1306
Creating an outbound rule for a connection through an LDAP gateway . . . 1307
Creating an inbound rule for a connection through an LDAP gateway . . . 1308
Adding a user filter . . . 1309
Adding an LDAP filter . . . 1310
Example user filters . . . 1310
Adding attribute mapping for outbound provisioning . . . 1313
Adding attribute mapping for inbound provisioning . . . 1314
Configuring outbound group provisioning . . . 1318
Enabling or disabling a connection . . . 1320
Enabling or disabling a rule . . . 1320
Sync status . . . 1321
Viewing sync status . . . 1322
Outbound provisioning sync summary examples . . . 1324
Using reporting to identify sync issues . . . 1325
Using user identity details to identify sync issues . . . 1326
Using group identity details to identify sync issues . . . 1326
Using audit logs to identify sync issues . . . 1327
Provisioning configuration change resync behavior . . . 1327
Creating a SCIM connection . . . 1329
SCIM provisioning features . . . 1333
SCIM filter expressions . . . 1333
SCIM provisioning known limitations . . . 1334
Creating a Salesforce connection . . . 1335
Salesforce attribute mapping . . . 1338
Creating a Salesforce Communities connection . . . 1339
Salesforce Communities provisioning features . . . 1342
Salesforce Communities attribute mapping . . . 1342
Salesforce Communities known limitations . . . 1343
Creating a Salesforce Leads and Contacts connection . . . 1344
Salesforce Contacts provisioning features . . . 1346
Manage Leads and Contacts . . . 1346
Salesforce Contacts attribute mapping . . . 1347

Salesforce Contacts known limitations . . . 1347
Creating an Aquera connection . . . 1348
Aquera provisioning known limitations . . . 1350
Creating a Workday connection . . . 1350
Configuring write-back provisioning . . . 1352
Identifying your Workday hostname . . . 1353
Creating a Workday Integration System User . . . 1354
Adding the Integration System User to a Security Group . . . 1355
Configuring the Domain Security Policy Permissions for the Security Group . . . 1356
Configuring Business Process Security Policy permissions for write-back . . . 1359
Activating the Security Policy Changes . . . 1360
Workday attribute mapping . . . 1360
Creating a Workday Integration System with a Field Override Service . . . 1361
Adding Workday Integration System IDs to PingOne . . . 1363
Syncing custom attributes from Workday into PingOne . . . 1364
Workday provisioner known limitations . . . 1366
Creating a Microsoft Azure Office 365 connection . . . 1367
Microsoft Azure Office 365 attribute mapping . . . 1370
Creating a Zoom connection . . . 1371
Zoom provisioning features . . . 1373
Creating an application in Zoom . . . 1373
Zoom attribute mapping . . . 1374
Creating a Slack connection . . . 1375
Slack provisioning features . . . 1377
Slack attribute mapping . . . 1377
Slack provisioning known limitations . . . 1377
Creating a ServiceNow connection . . . 1377
ServiceNow default attributes . . . 1379
ServiceNow supported attributes . . . 1379
ServiceNow provisioning features . . . 1381
ServiceNow provisioning known limitations . . . 1382
Creating a Google Workspace connection . . . 1382
Finding Google application details . . . 1384
Google Workspace attribute mapping . . . 1384
Google Workspace provisioning known limitations . . . 1385
Creating a GitHub EMU connection . . . 1385
Getting a GitHub EMU access token . . . 1387
GitHub EMU attribute mapping . . . 1388
GitHub EMU provisioning features . . . 1389
GitHub EMU provisioning known limitations . . . 1389
Creating an LDAP gateway provisioning connection . . . 1389
Active Directory attributes . . . 1391
PingDirectory attributes . . . 1392

Default attribute mapping for inbound provisioning through an LDAP gateway . . . 1393
Known issues for provisioning through an LDAP gateway . . . 1394
Editing a provisioning connection . . . 1394
Editing a provisioning rule . . . 1395
Troubleshooting test connection failure . . . 1395
Deleting a connection . . . 1397
Deleting a rule . . . 1397
Using the SCIM API to import users . . . 1398
Gateways . . . 1399
LDAP gateways . . . 1399
Before configuring an LDAP gateway . . . 1401
Best practices for configuring Active Directory for LDAP gateways . . . 1404
Importing an LDAP certificate to PingOne . . . 1409
Setting up an LDAP gateway . . . 1409
Adding an LDAP gateway . . . 1410
Adding a user type . . . 1412
Mapping the group attribute from an LDAP gateway . . . 1413
Starting a gateway instance . . . 1414
Running a standalone gateway as a Windows service . . . 1415
Starting a gateway instance as a standalone Java application . . . 1418
Starting the gateway instance in a Docker container . . . 1420
Verifying a gateway instance . . . 1421
Configuring multiple gateway instances . . . 1421
Creating or deleting a gateway credential . . . 1422
Creating an authentication policy that uses the gateway . . . 1422
Adding the authentication policy to an application . . . 1424
Kerberos authentication . . . 1424
Creating SPNs . . . 1425
SPN reference . . . 1426
Configuring end user browsers . . . 1429
Configuring Mozilla Firefox . . . 1430
Configuring Microsoft Edge . . . 1431
Configuring Google Chrome . . . 1432
Retaining credentials . . . 1432
Clearing credentials . . . 1433
Manually migrating users to PingOne . . . 1433
Troubleshooting an LDAP gateway instance . . . 1433
Troubleshooting LDAP authentication . . . 1438
Troubleshooting Kerberos . . . 1439
RADIUS gateways . . . 1441
Before you begin configuring a RADIUS gateway . . . 1444
Enable users to enter an OTP with their username in MS-CHAP v2, or EAP-MSCHAPv2 mode . . . 1445

Setting up a RADIUS gateway . . . 1448
Adding a RADIUS gateway . . . 1448
Starting a gateway instance . . . 1450
Starting the gateway instance in a Docker container . . . 1450
Starting a gateway instance as a standalone Java application . . . 1452
Verifying a gateway instance . . . 1453
Configuring multiple gateways . . . 1453
Creating or deleting a gateway credential . . . 1453
Running a standalone RADIUS gateway as a Windows service . . . 1454
Adding the RADIUS Gateway service . . . 1455
Removing the RADIUS Gateway service . . . 1456
Upgrading the PingOne RADIUS Gateway . . . 1457
Troubleshooting a RADIUS gateway instance . . . 1457
Authorize gateways . . . 1459
Requirements for Authorize gateways . . . 1461
Setting up an Authorize gateway . . . 1463
Adding a gateway . . . 1463
Starting a gateway instance . . . 1468
Verifying a gateway instance . . . 1470
Configuring a gateway instance . . . 1471
Configuring multiple gateway instances . . . 1473
Authentication for Authorize gateway endpoints . . . 1474
Service caching . . . 1475
Creating or deleting an Authorize gateway credential . . . 1477
Upgrading a gateway instance . . . 1478
Deleting a gateway . . . 1480
Authorization policies . . . 1480
Publishing policy versions . . . 1481
Making decision requests . . . 1487
Visualizing authorization decisions . . . 1488
Logging for Authorize gateways . . . 1490
Webhooks . . . 1497
Creating or editing a webhook . . . 1498
Deleting a webhook . . . 1500
Enabling or disabling a webhook . . . 1500
PingFederate . . . 1500
Creating a connection . . . 1501
Adding the connection in PingFederate . . . 1502
Viewing connection details . . . 1502
Editing a connection . . . 1503

Deleting a connection . . . 1504

User Experience . . . 1504
Notification templates . . . 1506
Viewing notification templates . . . 1507
Adding a notification template . . . 1508
Editing a notification template . . . 1509
Delivery methods and variables . . . 1510
Reporting for notifications . . . 1514
Notification Policies . . . 1515
Branding and themes . . . 1518
Viewing a list of available themes . . . 1518
Previewing a theme . . . 1519
Editing environment branding . . . 1520
Adding a theme . . . 1520
Editing a theme . . . 1525
Selecting an active theme . . . 1530
Deleting a theme . . . 1530
Self Service . . . 1531
Configuring the self-service portal . . . 1531
Agreements . . . 1533
Viewing agreements . . . 1533
Adding an agreement . . . 1534
Adding a language to an agreement . . . 1535
Creating localized content . . . 1535
Previewing an agreement . . . 1536
Enabling a language for an agreement . . . 1537
Enabling or disabling an agreement . . . 1537
Adding the agreement to the authentication policy . . . 1538
Viewing previous revisions . . . 1538
Deleting an agreement . . . 1538
Auditing for agreement consents . . . 1539
Viewing the consent history for a specific user . . . 1539
Languages . . . 1540
Viewing languages . . . 1540
Changing the default language . . . 1540
Adding a language . . . 1541
Deleting a language . . . 1541
Enabling or disabling a language . . . 1542
Configuring localized content . . . 1542
Modifying translatable keys . . . 1543
Deleting translatable keys . . . 1543
Adding a custom key for DaVinci . . . 1544
Setting up DaVinci Forms for multi-language support . . . 1546

Downloading a language bundle . . . 1550
Uploading a language bundle . . . 1551
Forms . . . 1552
Creating a form . . . 1552
Configuring a sign-on form . . . 1553
Configuring a registration form . . . 1556
Configuring an MFA form . . . 1557
Using translatable keys . . . 1560
Using dynamic text . . . 1561
Form properties . . . 1562
Form fields . . . 1563
Form toolbox . . . 1567

Settings . . . 1568
Environment properties . . . 1570
Viewing and switching environments . . . 1571
Adding an environment . . . 1572
Editing an environment . . . 1575
Managing opt-ins for early access features in PingOne . . . 1578
Adding an icon to an environment . . . 1580
Deleting an environment . . . 1582
Recovering a deleted Production environment . . . 1589
Promoting a Sandbox environment . . . 1591
Adding a service to an environment . . . 1593
Administrator security . . . 1594
Configuring administrator security . . . 1594
Configuring administrator security - PingID . . . 1597
Certificates and key pairs . . . 1599
Viewing certificates and key pairs . . . 1600
Adding a certificate and key pair . . . 1600
Importing a certificate and key pair . . . 1602
Downloading a certificate . . . 1602
Designating default keys . . . 1603
Assigning a key pair to an application . . . 1603
Key rotation policy . . . 1604
Viewing the signing key for an application . . . 1604
Updating the key rotation for an application . . . 1605
Converting PEM certificates to a different format . . . 1605
Generating a CSR . . . 1607
Generating a CSR for a custom domain . . . 1607
Importing the CA response . . . 1608
Domains . . . 1609
Setting up a custom domain . . . 1609
Setting up a trusted email domain . . . 1612

Removing a custom domain or trusted email domain . . . 1614
Sender . . . 1615
Configuring a custom SMTP email notification server . . . 1615
Using a custom email provider for notifications . . . 1619
Example: Using SendGrid as custom email provider for notifications . . . 1620
Configuring trusted email addresses . . . 1621
(Customer Only) Configuring WhatsApp as a sender . . . 1623
Configuring an SMS/Voice sender account with PingOne . . . 1625
Using a Twilio account with PingOne . . . 1625
Configuring a Twilio account for PingOne . . . 1626
Managing a Twilio account in PingOne . . . 1629
Using Twilio Verify with PingOne . . . 1630
Using a Syniverse account with PingOne . . . 1631
Configuring a Syniverse account for PingOne . . . 1631
Managing a Syniverse account in PingOne . . . 1634
Using a custom provider account with PingOne . . . 1635
Configuring a custom notification provider for PingOne . . . 1635
Use Case: Configuring Telesign as a provider with PingOne . . . 1640
Use Case: Configuring Burst SMS as a provider with PingOne . . . 1642
Using a Twilio account with PingOne to support Twilio Studio flows . . . 1643
Managing a custom provider account in PingOne . . . 1646
Sender IDs per country . . . 1646

Managing your PingOne user profile . . . 1649
Administrators: Managing your PingOne environment . . . 1651
End users: Accessing your PingOne profile . . . 1653
Editing your profile . . . 1654
Managing authentication methods . . . 1655
Completing the administrator account registration . . . 1658
Administrators: Verifying your own email address . . . 1659
End users: Verifying an email address . . . 1661
Changing your password . . . 1661
Managing accounts and sessions . . . 1662
Managing consents . . . 1664

Developer Tools . . . 1664
PingOne API Reference . . . 1666
Tools for developers . . . 1666
Monitoring activity with Splunk . . . 1666
Integrating with other Ping Identity software . . . 1674
IP address and domain reference . . . 1675
PingOne browser support . . . 1677

Operational Status . . . 1678

Copyright © 2025 Ping Identity Corporation

PingOne

PingOne is a cloud-based identity as a service (IDaaS) framework for secure identity access management that uses an organization-based model to define tenant accounts and their related entities within the PingOne platform.

What's new?

As part of our ongoing commitment to enterprise security and supporting best practices, multi-factor authentication (MFA) will be mandatory for all PingOne administrators starting June 1, 2025. Learn more in PingOne administrators MFA requirement - FAQ.

Release Notes

- Release Notes

Get Started with PingOne

- Introduction to PingOne
- Start a PingOne trial
- Getting Started with PingOne
- PingOne Tutorials
- PingOne Solutions
- PingOne SSO
- Strong Authentication (MFA)
- Authentication
- Threat Protection using PingOne Protect
- Identity Verification using PingOne Verify
- Digital Credentials using PingOne Credentials
- Authorization using PingOne Authorize

Copyright © 2025 Ping Identity Corporation

Use PingOne

- Administrators: Managing your PingOne environment
- Managing your PingOne user profile
- Monitoring PingOne
- Managing users in PingOne
- Managing applications in PingOne
- Managing integrations in PingOne
- Managing the user experience in PingOne
- Managing environment settings in PingOne
- PingOne Use Cases

Troubleshoot PingOne

- Ping Identity System Status
- Audit logs
- Verifying a gateway instance
- Viewing sync status

Copyright © 2025 Ping Identity Corporation

Learn More

- Training: PingOne Overview for Developers (existing customers only)
- Training: Getting Started with PingOne for Developers (existing customers only)
- PingOne Advanced Services
- PingOne Platform API Reference
- PingOne Community
- PingOne Support
- Ping Identity Partner Portal (partners)

Copyright © 2025 Ping Identity Corporation

PingOne Release Notes

PingIdentity.

Review release notes for the PingOne Cloud Platform and PingOne Services.

Subscribe to get automatic updates: PingOne Release Notes RSS feed

July 2025

July 3

New PingOne Verify settings available in themes

Improved PingOne

You can now update the appearance of the image on your identity verification pages to better match your company styles and branding. Learn more in Branding and themes.

July 2

Updated UI for Branding and Themes

Improved PingOne

We've updated the **Branding and Themes** UI with a new look and feel for a more streamlined experience. This new UI includes search and sort capabilities that make it easier to find the theme you need. It also lets you preview the appearance of your PingOne forms when you switch themes or update theme properties. Learn more in Branding and themes.

July 1

New Help Desk Admin role added

New PingOne

We've created the **Help Desk Admin** role to delegate access for helping end users authenticate with PingOne. Administrators with this role can manage MFA methods and devices for users and reset passwords. This role can be assigned at the environment or population level. Learn more in Built-in PingOne administrator roles.

June 2025

June 30

New Singapore domain

New PingOne

We've expanded to add a new data residency region for Singapore. Customers can now register new PingOne organizations with data residency and processing contained within Singapore. These organizations will use the new .sg domain name. Learn more about regional domains in Organizations.

Copyright © 2025 Ping Identity Corporation

June 25

OIDC session management

New PingOne

PingOne now supports OpenID Connect (OIDC) session management, allowing OIDC-based applications in the same browser mode to monitor the user session status. When enabled, PingOne includes the `session_state` parameter in its authorization response with the session status, such as `unchanged`, `changed`, or `error`. Learn more about OIDC session management in Editing an application - OIDC.

June 22

PingOne MFA mobile SDK 2.1

New PingOne MFA

We've released version 2.1 of the PingOne MFA mobile SDK. This version includes the following features and enhancements:

- Security enhancements
- Bug fixes
- Support for the new Singapore PingOne region
- When developing apps with the MFA SDK, you now need to use version 1.8.1 or later of the SDK.
- In the iOS version of the SDK, the `setDevicePairedAfterReinstall` method has been deprecated.

Learn more in the documentation for the Android version and the documentation for the iOS version.

June 17

PingOne Notifications - Twilio Verify

New PingOne MFA

You can now use Twilio Verify for sending PingOne notifications. Learn more in Using Twilio Verify with PingOne and in Phone Delivery Settings in the PingOne developer documentation.

June 12

Ability to delete translatable keys for language management

PingOne New

In addition to creating and updating key-value pairs, PingOne **Languages** now includes the ability to delete unwanted or unused keys for a language. Learn more in Deleting translatable keys.

Copyright © 2025 Ping Identity Corporation

June 4

Signals (PingOne Protect) SDK - new version for web

New PingOne Protect SDK

We've released a new version of the Signals (PingOne Protect) SDK for web, 5.6.0. You can find details in the SDK Changelog in the PingOne developer documentation.

Multi-factor authentication enforced for all access to the admin console

Improved PingOne

Per announcements earlier this year, and as part of our continued efforts to support best practice security measures in PingOne, multi-factor authentication (MFA) is now required for all administrators accessing the PingOne admin console. Learn more about configuration options for administrator security in Administrator security.

June 3

Virtual server IDs for SAML applications

New PingOne

You can now add custom virtual server IDs to SAML applications. This new capability allows you to identify your server differently when connecting to the same SAML application in different scenarios, such as from different environments or for different populations. Virtual server IDs also provide configuration flexibility and added protection against unauthorized access. Learn more in Editing an application - SAML.

Configure the one-time passcode (OTP) length for Workforce use cases

New Strong Authentication PingID

You can now configure the length of the one-time passcode for Email, SMS, and Voice authentication methods in workforce use cases (PingID).

This feature was previously only available for customer use cases.

Learn more: Configuring an MFA policy for strong authentication

May 2025

May 28

SMS notifications for users in China

Info PingOne

To adjust to regulatory changes, SMS notifications sent with the default Ping server to users in China now use the Twilio SMS template.

Copyright © 2025 Ping Identity Corporation

If you use the Ping server for sending PingOne SMS notifications, your users in China will now see notifications branded with Twilio's name rather than Ping Identity.

Major update to PingOne Forms

Improved PingOne DaVinci

New form templates

When you create a form in PingOne, there are now 18 templates to get you started. The following 11 templates have been added:

- Two new MFA Device Selection templates. These templates prompt the user to select an MFA method to set up or authenticate with. Powered by your MFA policy.
- Six new OTP Prompt templates. These templates present a UI for a user to register or authenticate with a one-time passcode (OTP) using email, text message, or voice call. The templates allow you to include the user's phone number or email address as dynamic text and link to a passcode resend branch in your flow.
- Two new Authenticator App Prompt templates. These templates prompt the user to scan a QR code to set up or authenticate with a TOTP authenticator app.
- One new Magic Link Prompt template. This template prompts the user to click a magic link received by email.

New components

The following seven components have been added to the form builder:

- Fields
  - **Checkbox**: Show a single checkbox with a rich text label. This component allows you to link to an externally hosted Terms and Conditions document.

    Learn more in Form fields.
- Toolbox
  - **Agreements**: Show the title and full body text of a PingOne agreement.
  - **Phone number input**: Prompt a user to select a country code and enter their phone number.
  - **Polling**: Show a spinner or animated dots and enable Polling and Challenge controls in the Show Form node. Loop the flow or pause on this form while another branch of the flow finishes.
  - **QR code**: Show a scannable QR code that contains a value from your DaVinci flow, with optional human-friendly fallback text.
  - **MFA Device Selection - Registration and Authentication**: Prompt the user to select an MFA method to set up or authenticate with. Powered by your MFA policy.
  - **FIDO2**: Prompt a user to set up or authenticate with a FIDO2 authentication method, such as biometrics or a security key.

    Learn more in Form toolbox.

Copyright © 2025 Ping Identity Corporation

Improved components

- **Translatable Rich Text**: You can now select an icon to show with your rich text.
- **Submit Button**: You can now remove the **Submit Button** to make room for a different submit method, such as MFA Device Selection, Polling, or FIDO2. Only one submit method is allowed per form.
- **Submit Button**, **Flow Button**, and **Flow Link**: Enabling **Override Default Styles** doesn't affect the look of your form until you change a value. You can also override some colors while keeping others linked to the theme.

Learn more in Form toolbox.

New features

PingOne Forms now supports dynamic text in the **Translatable Rich Text** component and field labels. This update allows you to take a value from your DaVinci flow, such as the user's first name, and show it in the form as read-only text or target for a hyperlink. Learn more in Using dynamic text.

Other improvements

We've improved the order and grouping of PingOne attributes on the **Fields** tab.

Changes to the PingOne Forms connector's Show Form **node**

- We've added direct links to the **Forms** and **Branding and Themes** sections of the PingOne admin console.
- We've renamed the **Pre-Populate Field Values** table to **Initial Field Values** and removed the unnecessary heading with the add and edit buttons.
- We've added a **Dynamic Text** table. This lets you populate dynamic text with a value from your flow.
- We've added properties to support the new components.

May 27

Sign-off method for application portal and self-service (MyAccount app)

New PingOne PingOne SSO

You can now choose the sign-off method PingOne uses when end users sign off from the application portal and the PingOne Self-Service - MyAccount app. You can select either **OIDC Logout** or **SAML 2.0 Single Logout** on the following pages in PingOne:

- **Applications > Application Portal**: Learn more in Configuring the application portal.
- **User Experience > Self Service**: Learn more in Configuring the self-service portal.

SAML 2.0 SLO support with the PingOne Authentication connector

New PingOne PingOne SSO DaVinci

Copyright © 2025 Ping Identity Corporation

PingOne now supports SAML 2.0 single logout (SLO) from identity providers (IdPs) configured as part of a DaVinci flow using the PingOne Authentication connector. End users can now sign off from IdPs through SAML 2.0 SLO for flows configured using the Sign On with External Identity Provider capability from the PingOne Authentication connector. Learn more about SAML 2.0 SLO in Applications and External IdPs.

May 20

MFA with multiple authentication policies

Info PingOne MFA

To enhance security, in cases where multiple authentication policies are defined for accessing an application, PingOne no longer proceeds to the next authentication policy if a user has an MFA device that is unreachable, locked, or blocked.

May 16

Verify users in India with Aadhaar verification using PingOne Verify policies

Improved PingOne Verify

You can now verify users in India using PingOne Verify policies. Indian residents are issued an Aadhaar ID, which is a 12-digit identification number. When you configure Aadhaar verification in PingOne Verify policies, PingOne Verify gains the ability to directly integrate with India's Aadhaar National Registry. Learn more in Creating a verify policy.

May 13

FIDO Attestation improvements

Improved Strong Authentication PingID PingOne MFA

The following improvements are now available in FIDO2 policy:

- Add enterprise attestation

  You can now verify that a device is an Enterprise FIDO device. You can also check that the device matches the serial number configured for the user.

- Additional User Display Name attributes

  You can now include the **Environment Name** and **Organization name** with the **User Display Name**. This information displays when a user registers their FIDO device.

Learn more in Adding a FIDO policy

May 12

Use of short codes for PingOne SMS notifications - United States and Canada

Info PingOne MFA

Copyright © 2025 Ping Identity Corporation

To improve delivery reliability for PingOne SMS notifications sent with the default Ping server, the use of short codes has been expanded.

If you use the Ping server for sending PingOne SMS notifications, and you haven't customized notification content, your users in the United States and Canada might see notifications coming from a different number than previously.

May 11

OATH token authentication for customer use cases

New Strong Authentication PingOne MFA

OATH token authentication is now available for customer (PingOne MFA) use cases. Learn more in Configuring OATH token authentication

May 7

Administrator Security enhancements

Improved PingOne

We've added a new **Limit MFA to specific populations** setting for environments using the **PingOne & External IdP** option for Administrator Security. If you select this option, you can select specific populations that will require secondary authentication through PingOne after the initial authentication with the IdP. Users in populations that are not selected will authenticate only once, through the IdP. Learn more in Configuring administrator security.

May 1

Invite administrators to register with PingOne

New PingOne

You can now invite other administrators to register for PingOne. To use this feature, you must use PingOne as your identity provider, have administrator security enabled with PingOne or a hybrid authentication source, and have the appropriate permissions.

In the invitation, provide their first and last name, their email address, and specify the administrator roles that you want the administrator to have. You can also set an expiration time on the invitation. The maximum time allowed is 24 hours.

The new administrators receive an email indicating that they were added as an administrator in PingOne. The email contains a registration link and instructs them to click the link, copy the invite code, paste it into the appropriate field, and create a password to complete the registration process.

Learn more about this process in Inviting administrators to register and Accepting the administrator account registration.

The PingOne administrator **Getting Started** experience has also been updated and now includes this functionality.

Copyright © 2025 Ping Identity Corporation

April 2025

April 30

Production environment deletion protection

Improved PingOne

Production environments can now be deleted, but the environment will be in a recoverable state for 30 days before it is permanently deleted. Sandbox environments are still deleted immediately and are not recoverable. Additionally, you can promote Sandbox environments to Production, but you can no longer demote Production environments to Sandbox.

> **Best practice**
>
> Any Sandbox environment containing production resources or used for production purposes should be promoted to Production to prevent accidental deletion.

Learn more in Sandbox and Production environments, Deleting an environment, and Recovering a deleted Production environment.

April 29

Support for Microsoft Entra ID external authentication methods with PingOne, PingID, and DaVinci

New PingOne SSO DaVinci PingID

External authentication methods allow Microsoft Entra ID users to leverage external authentication providers for multi-factor authentication (MFA). You can now use DaVinci with PingOne SSO and PingID to configure an EAM for Entra ID. Learn more in Setting up PingOne SSO, DaVinci, and PingID as the external MFA provider for Microsoft Entra ID.

April 28

WhatsApp as an authentication method

New Strong Authentication PingOne MFA

You can now enable and configure WhatsApp as an authentication so that your users can receive a one-time passcode (OTP) by WhatsApp message.

This authentication method is available for customer (PingOne MFA) use cases only, and requires you to have your own WhatsApp Business Account.

Learn more in Configuring WhatsApp authentication.

Define cooldown period for sending notifications

New Strong Authentication PingOne MFA PingID

Copyright © 2025 Ping Identity Corporation

To prevent the malicious use of notifications, you can now define a notification cooldown period during which the user must wait before sending another notification. You can define notification cooldown periods for WhatsApp, Email, and SMS/Voice notifications.

Learn more in Notification Policies

April 24

Administrator Roles UI enhancements

Improved PingOne

The roles on the **Built-In Roles** tab of the **Administrator Roles** page are now organized into categories that clearly separate the roles used for single sign-on to other Ping products from the main PingOne roles. These categories are also used throughout the UI to simplify role assignment. Learn more in Administrator Roles.

Skip account lock verification during authentication

New Strong Authentication PingOne MFA PingID

We've added the ability to skip account lock validation when applying an MFA policy. Learn more in Configuring an MFA policy for strong authentication.

April 22

Support for `x5t` header parameter in OIDC applications

New PingOne

PingOne can now include the `x5t` header parameter in access tokens, ID tokens, and JSON Web Token (JWT)-based refresh tokens for OIDC-based applications. This new capabiliity improves interoperability with applications, custom resources, or both that require the `x5t` parameter in the digital signature verification process. Learn more in Editing an application - OIDC.

April 11

Amazon Web Services integration kit 1.4.0

New PingOne Authorize

We've released version 1.4.0 of the Amazon Web Services integration kit. Now you can extend Amazon CloudFront's authorization capabilities by deploying the integration kit as a Lambda@Edge function. Integrating PingOne Authorize with CloudFront enables optimized content delivery and globally distributed access control of web applications and APIs. Learn more in Configuring Amazon CloudFront.

Copyright © 2025 Ping Identity Corporation

April 10

Improvements to PingID OOTB Registration and Authentication DaVinci flows

Improved | Strong Authentication | PingID

PingID out-of-the-box (OOTB) registration and authentication flows in DaVinci have been expanded to include:

- **FIDO2 (Passkey) support**: FIDO2 device authentication is now supported.
- **Rename device during pairing**: The ability for users to specify a nickname for a device during pairing is now supported for PingID.
- **PingOne branding support**: PingOne branding and themes are now supported.
- **Customizable Settings button**: The MyAccount **Settings** button is now supported. The Settings URL now points to the MyAccount URL and can be customized in the Flow settings if required.
- **Define self-enrollment behavior**: Admins can now choose whether users with no paired devices are directed to the registration screen or blocked from registering until they access their MyAccount or MyDevices page. This is defined in the DaVinci Flow settings for the relevant flow.
- **OATH resync flow support**: The OATH resync flow isn't supported for OOTB PingID registration and authentication flows.
- **Error screen improvements**: Improvements to the error screens are now included in the OOTB PingID registration and authentication DaVinci flows.

April 9

Updated UI for External IdPs

Improved | PingOne

We modernized **External IdPs** in PingOne with a new look and feel. Learn more in External IdPs.

April 2

Early access opt in for new features

New | PingOne

You can now try out new PingOne features before they're released and provide feedback directly to Ping from the admin console. You decide which features to enable during the early access period and the environments in which to enable them. You can also opt out of a previously enabled feature during the early access period. Learn more in Managing opt-ins for early access features in PingOne and PingOne Early Access Features.

> **Note**
>
> Not all features will be available for early access. Early access feature availability is determined by Ping, and the features you can enable are dependent on a number of factors including licensing, environment configuration, and administrator permissions. All released features are enabled at GA. You can't opt in or out of released features.

Copyright © 2025 Ping Identity Corporation

PingOne MFA mobile SDK 2.0

New PingOne MFA

We've released version 2.0 of the PingOne MFA mobile SDK. This version includes the following features and enhancements:

- You can now require users to carry out number matching when authenticating.
- Apps can now be configured so the same device can be paired in multiple geographic regions.
- Using the PingOne API, you can now cancel an authentication that has already begun. This option can be used for situations where the user wants to change to a different authentication device.

Learn more in the documentation for the Android version and the documentation for the iOS version.

Authentication using number matching

New PingOne MFA

You can now specify that a mobile push requires the user to match a number that they were shown when requesting access. When you enable this option, you can have users select the correct number from a group of three numbers, or you can require users to actually enter the number that was shown.

This feature requires version 2.0 or higher of the PingOne MFA SDK.

Pairing mobile device in multiple regions

New PingOne MFA

When developing mobile apps with the PingOne MFA SDK, you can now configure the apps such that it is possible for the same device to be paired in multiple geographic regions. Learn more about this feature in the documentation for the SDK for iOS and the documentation for the SDK for Android.

This feature requires version 2.0 or higher of the PingOne MFA SDK.

March 2025

March 31

Manually enter number for number matching

Improved Strong Authentication PingID

You can now configure PingID mobile app's number matching feature to require users to enter the correct number manually, rather than selecting from a list of three numbers.

- Learn more in (Workforce Only) Configuring the PingID mobile application settings.
- Learn about the user experience in Authenticating using number matching.

Copyright © 2025 Ping Identity Corporation

Expanded management capabilities for migrated PingID accounts in PingOne

New Strong Authentication PingID

The ability to migrate existing PingID accounts to a PingOne environment and fully manage them from PingOne is now available for all admins. You can now migrate:

- An existing PingID account to a new PingOne environment.
- An existing PingID account to an existing PingOne environment.
- If you integrated a PingID account with a PingOne environment before March 31, 2025, you can migrate the PingID management from the legacy PingID admin portal to PingOne.

Learn more in Integrating a PingID account with a PingOne environment.

March 26

Updated LDAP gateway client application

New PingOne

We've released LDAP gateway client application version 3.4.0. This version includes:

- Added `correlationId` to LDAP gateway client application log to help troubleshoot issues.
- Upgraded dependencies to improve security.
- Updated base image to reduce Docker image size.

March 25

Specify preferred language for populations

New PingOne

We've added the ability to select a **Language** for **Populations**, making it easier to specify the preferred language for a user when building authentication experiences in PingOne DaVinci. Learn more in Managing populations.

Manage Microsoft Active Directory user passwords

New PingOne

For workforce contexts, you can now manage Microsoft Active Directory user passwords using a PingOne LDAP gateway with **User Types**, where the **Password Authority** section is set to **LDAP** and **Password changes from PingOne enabled**. You can enable the following requirements:

- **Force password reset on next sign on**: To force users to reset their password, they must first authenticate using the current password. If the user provides the correct current password, they must provide the current password one more time and define a new password. The new password is sent to Active Directory.

Copyright © 2025 Ping Identity Corporation

- **Create or generate password**: When you set a temporary password, it's sent to Active Directory and the user must authenticate using the temporary password. If the user provides the correct current password, the user must re-enter the temporary password and define a new password, which is sent to Active Directory.

AAGUID in API responses for FIDO2 devices

New PingOne MFA

When using the `devices` endpoint to request details of a single MFA device or all MFA devices, responses for activated FIDO2 devices can now include the authenticator attestation identifier (AAGUID) for the type of authenticator. For details, see the new `fidoDeviceMetadata` object under MFA devices in the PingOne API documentation.

March 23

PingOne Protect (Signals) SDK - new versions

PingOne Protect SDK

We've released new versions of the PingOne Protect (Signals) SDK:

- iOS - 5.3.0
- Android - 5.2.0

You can find details in the SDK Changelog.

March 20

Kong Gateway integration kit enhancement

New PingOne Authorize

We've released version 1.2.0 of the `ping-auth` plugin for Kong Gateway. This version improves security by supporting referenceable shared secrets in Kong.

Learn more in Configuring Kong Gateway for PingOne Authorize integration.

March 19

Configure authentication failure limit for FIDO2 devices

Improved Strong Authentication PingID PingOne MFA

When configuring an MFA policy, you can now specify the maximum number of times authentication can fail when using a FIDO2 device, before the user is blocked. You can also specify the amount of time the user is blocked from authenticating with that device.

Learn more in Configuring an MFA policy for strong authentication.

Copyright © 2025 Ping Identity Corporation

March 17

Custom domain infrastructure changes

Info PingOne

As part of our continued efforts to support best practice security measures in PingOne, we'll be using Cloudflare instead of Amazon CloudFront as our custom domain ingress infrastructure. This change is being deployed in a phased approach and affects you only if you use custom domains. Learn more about custom domains in Setting up a custom domain.

- **Phase 1**: All custom domains added in PingOne after March 17, 2025 will use Cloudflare instead of CloudFront. There will be no change to existing custom domains in Phase 1.
- **Phase 2**: Some time in the next quarter, Ping will release a migration option that will enable you to migrate your existing custom domains to Cloudflare on your own schedule. When Phase 2 is released, detailed migration instructions will be provided.
- **Phase 3**: Approximately 1 year after the completion of Phase 2, any custom domains that you haven't yet migrated will be migrated to Cloudflare automatically.

Action required

In most cases, no action is required at this time, and this change should be largely unnoticeable. However, you should contact your organization's network infrastructure team and direct them to review the Custom domain migration to Cloudflare support post for more information (sign on required). This post contains details about how to assess whether your network and firewall settings require updates to support the new infrastructure.

March 10

ID of authenticating device in ID token

New PingOne

ID tokens now include a new claim called `p1.mfa_device_id`, the ID of the device that was used to authenticate. You can find more information about the content of ID tokens in ID Token claims.

March 4

PingID device trust predictor in risk policies

New PingOne PingID PingOne Protect

For workforce contexts, risk evaluations can now include the new PingID device trust predictor if your users install the PingID device trust agent on their computers. This predictor requires a PingID and PingOne Protect license.

Learn more in Using the PingID device trust agent, PingID device trust predictor, and the Risk Predictors section in the API documentation.

Copyright © 2025 Ping Identity Corporation

February 2025

February 25

Language used for notifications

Improved PingOne MFA

When determining what language should be used for a notification sent to a user, PingOne now takes into account the language preference information included in the Accept-Language header sent by the browser. You can find a full description of the logic used for choosing a language in Runtime logic for content selection in the API documentation.

Push notifications - removal of legacy Google cloud messaging option

Info PingOne

With Google dropping support for its legacy cloud messaging APIs, native applications in PingOne no longer let you choose between **Cloud Messaging** and **Firebase Cloud Messaging**. The HTTP v1 API is now used for push notifications, and you must provide your Firebase Admin SDK private key.

Apply a specific notification policy to an MFA policy

Improved Strong Authentication PingOne MFA PingID

You can now select which notification policy you want to apply to an MFA policy.

Learn more in Configuring an MFA policy for strong authentication.

February 24

Remember Me option in MFA policies

New PingOne MFA

You can now use the PingOne API to implement "remember me" functionality in your web applications so that users do not have to authenticate when accessing applications from a remembered browser during the period specified, which can be from one hour to 90 days.

If you include this option, use the new **Remember Me Configurations** section when defining MFA policies to specify which policies should allow the option. For instructions on implementing this feature, see Remembered Devices.

February 20

Ability to limit custom role access to Overview page added

New PingOne

Copyright © 2025 Ping Identity Corporation

We've added a new **Display Environment Overview** permission that controls access to the **Overview** page for the environment. This permission is included in all built-in administrator roles in PingOne, but you can remove it from custom roles to restrict access to this page. This permission affects visibility in the admin console only and doesn't affect API access. Learn more about built-in and custom roles in Administrator Roles.

February 12

Population theme updates

Improved PingOne

If a population doesn't have a selected theme, the population now uses the active theme for the environment. This update ensures that preferred branding is displayed to users when building authentication experiences in PingOne DaVinci. Learn more in Managing populations.

Using expressions to access authentication JWT for token fulfillment

New PingOne

You can now use expressions to retrieve information from the authentication JSON Web Token (JWT) for access token and ID token fulfillment. Expressions are supported when using private key JWT and client secret JWT as the token endpoint authentication method. This capability improves interoperability between OpenID Connect (OIDC) applications and resources. Learn more in Token endpoint authentication methods and PingOne expression language variables.

February 5

PingOne Notifications - multiple custom SMS/voice providers

New PingOne MFA

You can now define up to three custom providers to use for SMS/voice notifications. After you've defined the providers, you can specify in your notification policies the order of provider preference to use in different geographical locations.

February 4

Multi-factor authentication required for access to admin console - updates

Improved PingOne

As part of our continued efforts to support best practice security measures in PingOne, we've made the following updates to enhance the multi-factor authentication (MFA) requirements introduced earlier this year:

- **Update Admin MFA Settings modal**: Prompts administrators to update **Administrator Security** settings when signing on to environments in which enhanced security is not yet enabled. Use the modal to:
  - **Update Now**: Enforces new default security settings based on current environment policies. Displays information about the authentication policy and settings that will be enabled when you update.

    The confirmation message redirects you to the **Administrator Security** page so that you can verify the updates and make changes if necessary.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> This update cannot be reversed from the admin console. Contact Ping Identity Support for changes during the opt-in period (until June 1, 2025).

  - **Remind me later**: Delays the update. Administrators will be prompted again in the next browser session.

- **Policy mapping changes**: The current default authentication policy for the environment is mapped to the new system security policy to ensure consistency.

Action Required

Review and update the **Administrator Security** settings to enhance the security of your environments. For assistance, contact Ping Identity Support during the opt-in period.

Ping Identity will require MFA for all PingOne administrators as of June 1, 2025. Learn more in the PingOne administrators MFA requirement - FAQ.

January 2025

January 31

Access token enhancements

Improved PingOne

To reduce administrative and development tasks, PingOne now always includes the organization ID and environment ID in its access tokens. The claims are included in access tokens as `org` and `env`, respectively. If your organization's processes require the organization ID, environment ID, or both, you can now retrieve this information by reading the JSON Web Token (JWT)-based access tokens or sending introspection requests and reviewing the results.

Role assignment event enhancements

Improved PingOne

The role events in the PingOne audit report now use human-readable text instead of UUIDs for the role that was created or deleted and the scope or level at which the role change was made. Additionally, you can now easily monitor role assignment events by running a preconfigured audit report directly from the **Administrator Roles** page. Learn more in Viewing administrator role events.

January 30

Detection of replay attacks

Improved PingOne Protect

PingOne Protect now detects replay attacks that use an intercepted valid payload from the Signals SDK.

Copyright © 2025 Ping Identity Corporation

January 29

Updated defaults for new native applications

Improved PingOne

When adding a new native application, PingOne creates the application with the following new defaults to align with current security best practices:

- **Response Type**: **Code**
- **Grant Type**: **Authorization Code**
- **PKCE Enforcement**: **S256_REQUIRED**

Existing native applications won't be updated to use the new defaults. You can update the settings for new and existing native applications as needed. Learn more in Editing an application - Native.

Format of phone numbers in Mexico

Info PingOne MFA

The format of Mexican phone numbers that was used prior to August 2019 (adding "1" before the area code) is no longer supported.

January 28

PingID as a digital wallet

New PingOne Credentials

You can now add PingID as a digital wallet to issue verifiable credentials. Learn more in Creating a credential. You can find end user documentation in Manage and share Credentials in the PingID End User Guide.

Terminate user sessions with only ID token

New PingOne

You can now enable OIDC-based applications to send a sign-off request for PingOne to terminate a user session using only the ID token. This is most useful for applications that don't have access to the session token cookie. This capability is controlled by a new per-application setting, **Terminate User Session by ID Token**. Learn more in Editing an application.

January 21

OIDC-based LinkedIn external identity provider

New PingOne

Copyright © 2025 Ping Identity Corporation

The LinkedIn external identity provider (IdP) now uses an OpenID Connect (OIDC)-based connection to allow your users to sign on to an application with LinkedIn. The legacy OAuth 2.0-based IdP connection for LinkedIn has been deprecated. Existing applications using the legacy IdP will continue to work, but new applications default to the new OIDC-based connection. Learn more in Adding an identity provider - LinkedIn.

January 20

Introducing Authorize gateways

New PingOne PingOne Authorize

We've released Authorize gateway version 1.0.0. To reduce authorization latency when you have demanding performance requirements, you can now deploy authorization policies managed in PingOne to Authorize gateway instances located on-premise or in your private cloud. In highly regulated environments, this also ensures data privacy by keeping sensitive data for authorization decisions within your secure trust boundary. Learn more in Authorize gateways.

January 14

Custom OAuth parameters for HTTP service requests

Improved PingOne Authorize

You can now send additional parameters in HTTP service requests. For HTTP services authenticated with the Client Credentials grant type, use the **Custom OAuth Parameters** setting to add custom key-value pairs to the token endpoint request. This level of customization is useful when integrating with authorization servers that enforce specific configuration constraints. Learn more in Connecting an HTTP service.

Troubleshooting LDAP authentication

Improved PingOne

We've added the following information to the gateway client application logs to help solve authentication issues reported by end users. Find out whether a user:

- Entered an incorrect username.
- Entered a correct username but an incorrect password.

> **Note**
>
> For security reasons, this information is only visible to admins and isn't displayed to end users. The end-user experience remains unchanged. The standard message is `Incorrect username or password. Please try again.`

Improved application management experience

Improved PingOne

To improve the administrator experience, we've moved application endpoints and URLs from the **Configuration** tab to the **Overview** tab. This makes it easier and faster to navigate to the configuration details you need for day-to-day application management. Learn more in Viewing application details.

Copyright © 2025 Ping Identity Corporation

January 10

Authorization Dashboard enhancements

Improved PingOne Authorize

We've refreshed the **Authorization Dashboard** to improve your user experience. You can track authorizations and decision counts by date, and view the average execution time for services, in addition to the maximum execution time. Learn more in Authorization Dashboard.

January 9

Step-up authentication for APIs

New PingOne PingOne Authorize

You can now force step-up authentication when users access sensitive resources through APIs. When authenticated users try to access more sensitive resources, such as salary data, health records, or premium content, you can require a higher level of authentication and also set limits on the amount of time allowed since the last authentication event.

Use the new **Respond with authentication step-up challenge** statement template to implement step-up authentication challenges in policies that protect API services and operations.

Learn more in Step-up authentication for APIs and Statement templates.

Define Public Key Credential Hints in the FIDO policy

Improved PingOne

You can now define Public Key Credential Hints. This field allows you to select the authenticating device that your users are most likely to choose during pairing. The selection is considered as a 'hint' to the authenticator.

Learn more in Adding a FIDO policy.

RADIUS gateway enhancements

New PingOne

We've updated the RADIUS gateway client application to version 1.3.0.

This version includes the following enhancements:

- Support for the use of a forward web proxy server to handle traffic between the RADIUS gateway client and PingOne.
- Support for the EAP-MSCHAPv2 protocol when integrating the RADIUS gateway with a Network Policy Server (NPS).

Learn more in RADIUS gateways.

RADIUS gateway security enhancement

Improved PingOne

Copyright © 2025 Ping Identity Corporation

We've made some enhancements to the RADIUS Client security configuration to mitigate the risk of a BlastRADIUS attack.

Learn more in Adding a RADIUS gateway.

RADIUS gateway fails to forward requests to the NPS Server

Fixed | STAGING-24934 | PingOne

We've fixed an issue that was preventing RADIUS gateway from forwarding requests to the NPS (Network Policy Server) in instances where the RADIUS client and the NPS shared the same IP address.

January 6

PingID account in PingOne

New | Strong Authentication | PingOne MFA | PingID

We've added the ability to create a new PingID account and manage it from a PingOne environment. Many features that were previously managed by the legacy PingID admin portal (on the **Configuration** tab and the **Device and Pairing** tab) can now be managed in PingOne.

Administrators can also take advantage of additional functionality available in PingOne including:

- PingID accounts in PingOne can now configure the full range of authentication methods from PingOne's MFA policy.
- All application-specific configurations can be done from the relevant application on the PingOne **Applications** tab. A PingID mobile application and a PingID desktop application appear in the **Applications** list by default.

  Learn more in Configuring the PingID mobile application settings, and Configuring the PingID desktop application.
- PingID's email, sms, and voice providers can now be configured from PingOne.

  Learn more in Sender.
- You can now edit and customize PingID notification templates from PingOne.
- You can view MFA dashboards and reporting in PingOne. PingID reports are still available in the legacy PingID admin portal.

A small number of features are still managed by the legacy PingID admin console, such as PingID policy.

Early access to manage PingID out of PingOne

New | Strong Authentication | PingID

We've provided a limited number of existing customers with the ability to migrate the management of their PingID account to PingOne.

To help administrators who are familiar with specific fields for specific features in the legacy PingID admin portal to find the equivalent fields in PingOne, in the legacy PingID admin portal for all relevant fields we've added a link to the equivalent field in PingOne.

Copyright © 2025 Ping Identity Corporation

Note

- For customers with early access, it is important to read What you need to know before integrating or migrating a PingID account into a PingOne environment before migrating your account.
- Customers who want to join the early access track should contact their Ping Identity representative.

Bypass MFA for a specific user

New | Strong Authentication | PingOne MFA | PingID

It's now possible to bypass MFA for a specific user for a specific time period or for an unlimited time. When bypass is enabled, the user is able to access their account or application without authenticating using MFA.

Learn more in Bypass MFA for a specific user.

Documentation improvements

Improved | Strong Authentication | PingOne MFA

PingOne MFA documentation has been improved and is now included as part of a single section, *Strong authentication*. The new section includes a dedicated page for each authentication method, outlining the features of that authentication method, and various configuration options. It also indicates which authentication methods are supported by the use case (workforce, customer, or both), and includes details of requirements and limitations for each authentication method.

Learn more in Strong Authentication (MFA).

December 2024

December 16

Device Authorization app restored to PingID policy

Fixed | STAGING-25145 | PingOne

For PingID accounts that are integrated with PingOne environments, we've fixed an issue in the legacy PingID admin portal that was preventing the Device Authorization app from showing in the PingID policy applications list.

December 10

Population alternative identifiers and theme

New | PingOne

We've added the ability to configure **Alternative Identifiers** for **Populations**, making it easier to determine a user's population based on an identifier value in a DaVinci flow. Additionally, populations can now specify a **Theme**, making it easier to determine the preferred branding for a user when building authentication experiences in PingOne DaVinci. Learn more in Managing populations.

Copyright © 2025 Ping Identity Corporation

Add custom attributes from Workday into PingOne

New PingOne

You can add custom attributes from Workday into PingOne. Learn more in Creating a Workday Integration System with a Field Override Service, Adding Workday Integration System IDs to PingOne, and Syncing custom attributes from Workday into PingOne.

December 9

Define the user presence timeout for FIDO devices

Improved PingOne MFA

You can now define a user presence timeout value for FIDO2 devices. The **User Presence Timeout** field defines the amount of time the user has to perform a user presence gesture with their FIDO device before the request expires. Learn more in Adding a FIDO policy.

November 2024

November 20

Added Active Directory compatibility to the Reset Password capability

Improved PingOne

The **Reset Password** capability in the DaVinci LDAP connector is now compatible with Active Directory. Learn more in LDAP Connector.

November 19

User demographic dashboard

New PingOne

The User demographic dashboard shows a summary of user demographic profiles and activity for the selected environment. Learn more in User Demographics Dashboard.

November 18

Simplified OIDC application configuration and integration

New PingOne

Copyright © 2025 Ping Identity Corporation

We've enhanced the application configuration process for OpenID Connect (OIDC) applications. The new **Integrate** tab provides access to prefilled code examples, instructions, and sample apps for testing connections. Initial support is available for Node.js Express and the Ping SDK for JavaScript. Learn more in Integrate PingOne with a Node.js Express app or Integrate Ping SDK for JavaScript with PingOne.

November 14

Manually approve a user's ID

Improved PingOne Verify

You can now manually approve a user's ID from the transaction log. Learn more in Manually approving a user's ID.

November 13

Specifying authentication policy for SAML applications using `flowPolicyId`

New PingOne

PingOne now supports using the `flowPolicyId` HTTP request parameter to indicate the authentication policy for PingOne to use when authenticating users to a SAML application. You can include the `flowPolicyId` HTTP request parameter in the **Initiate Single Sign-On URL** to specify a PingOne authentication policy or a DaVinci flow policy. Learn more in Editing an application - SAML.

Amazon API Gateway integration kit retries for client network errors

New PingOne Authorize

We've released Amazon API Gateway integration kit version 1.3.0. This version includes a retry mechanism to improve the handling of client network errors caused by connection resets. Use the `maxRetries` setting in `config.js` to set the maximum number of retries you want before returning a failed response to the client. The default is `1`. Learn more in Configuring Amazon API Gateway for PingOne Authorize integration.

November 12

Language localization

New PingOne Verify

Use language localization to configure one or more languages and modify text fields of PingOne Verify text that is presented to end users in notification and agreements. Learn more in Configuring PingOne Verify language localization.

November 11

Deletion of staging policies when promoting to production

New PingOne Protect

Copyright © 2025 Ping Identity Corporation

When you promote a staging policy to production, the staging policy will now be automatically deleted from your list of risk policies. You can no longer unlink PingOne Protect staging policies from a production policy. Learn more in Creating and managing staging policies.

November 6

PingOne Protect (Signals) SDK - new versions

New PingOne Protect SDK

We've released new versions of the PingOne Protect (Signals) SDK:

- iOS - 5.2.8
- Android - 5.1.5
- Web - 5.4.0

You can find details in the SDK Changelog.

November 5

Support for `offline_access` scope in OIDC applications

New PingOne

PingOne now supports the `offline_access` scope for OIDC-based applications. Add `offline_access` as an allowed scope to enable an application to use the Refresh Token grant type to access previously approved resources when the user is not present and on a per-request basis. This allows the application to drive the decision to request a refresh token based on whether or not it needs a refresh token. Learn more in Editing an application.

October 2024

October 31

Optional sequential character password restrictions added

Improved PingOne

To provide more opportunities to enhance password security, we've added options for restricting the use of sequential characters in user passwords. Enforce one or more of these restrictions for your users by adding them to your password policies. Learn more in Password policies.

October 29

SSO into PingOne Advanced Identity Cloud

New PingOne

Copyright © 2025 Ping Identity Corporation

You can now set up single-sign on (SSO) from the PingOne admin console into PingOne Advanced Identity Cloud. With this capability, you can also now assign Advanced Identity Cloud tenant roles in PingOne for use in SSO. Learn more in Setting up SSO to PingOne Advanced Identity Cloud and Administrator Roles.

AuthnStatement session validity duration for SAML applications

New PingOne

You can now optionally specify a value for the `SessionNotOnOrAfter` attribute using the new **AuthnStatement session validity duration** setting in SAML applications. This new capability improves interoperability, especially if the SAML application requires a longer `SessionNotOnOrAfter` value than the lifetime of the SAML assertion defined in the Assertion Validity Duration setting. Learn more in Editing an application - SAML.

October 24

Enhanced Getting Started experience for customer use cases

Improved PingOne

We've updated the **Getting Started** experience for creating a password-based customer solution. Enhancements include a more flexible configuration that makes it easier to test different authentication, registration, account recovery, and profile management use cases. Additionally, the underlying DaVinci flows used by the **Getting Started** experience have been updated to follow our best practices for flow creation and user interface standards.

Learn more on the **Passwords** tab of Building a customer solution.

October 21

Native, Worker, and Device Authorization apps removed from PingID policy

Fixed PID-14123 PingOne

For PingID accounts that are integrated with PingOne environments, the legacy PingID admin portal no longer lists Native, Worker, and Device Authorization apps in the **PingID Policy Applications** list.

Learn more in Administrator Roles and Custom role scenarios.

October 16

Enhanced user interface for external groups

Improved PingOne

We've enhanced the UI for external groups to make it easier to determine the source of the group at a glance. The details page for external groups has also been updated to provide more information and includes a link to the configuration details so that you can easily make changes if needed. Warning and informational messages have been added to alert you to potential issues.

Learn more in About groups and populations and Viewing groups.

Copyright © 2025 Ping Identity Corporation

Updated LDAP Gateway client application

New PingOne

We’ve released LDAP Gateway client application version 3.3.0. This version includes:

- Support for using a forward web proxy server that requires authentication to handle traffic between the gateway client and PingOne.
- Upgraded dependencies for better security and stability.

Learn more about using a web proxy server in Starting a gateway instance.

October 15

Custom administrator roles

New PingOne

For increased security and flexibility of role assignment, we’ve introduced the ability to create custom administrator roles in PingOne. PingOne administrators with the proper role assignment can now create, edit, and assign custom roles using any of the permissions available in PingOne. Custom roles can then be assigned to implement delegated administration and to provide least-privileged access to PingOne resources. The new **Administrator Roles** UI includes enhanced permission descriptions, privileged permissions tags, and labels that ensure you include permissions essential to using the PingOne admin console. Like built-in roles, custom roles can be assigned to users, groups, worker apps, or PingFederate gateways.

October 9

PingOne notifications - sending through an external email service

New PingOneMFA

You can now use an external email service to send notifications to your users. Learn more in Using a custom email provider for notifications.

October 6

Configure the one-time passcode (OTP) length

New PingOne MFA

You can now configure the length of the one-time passcode presented to the user. This feature is available for Email, SMS, and Voice authentication methods. Learn more: Adding an MFA policy

October 4

Multi-factor authentication required for access to admin console - updates

Improved PingOne

Copyright © 2025 Ping Identity Corporation

As part of our continued efforts to support best practice security measures in PingOne, we have enhanced the multi-factor authentication requirements introduced earlier this year.

The following updates have been made:

- You can now enable enhanced administrator security on a per environment basis for organizations that were created before July 18, 2024. Go to **Settings > Administrator Security** and click **Enable Enhanced Security**. You will be prompted to confirm your choice. If you later want to disable enhanced administrator security before it is required for all environments, click **Disable Enhanced Security** on the same page, and respond to the prompt.
- You can now select the MFA authentication methods you want to support for administrators. Learn more in Configuring administrator security.
- You can now enable enhanced security for environments using PingID and PingOne SSO. Learn more in Configuring administrator security - PingID.
- The **Multi-factor Authentication** setting for all existing administrator users has been updated to **Enabled** so that these users can enroll a second authentication factor if enhanced security is enabled for their environment.

Learn more in Administrator security and the PingOne administrators MFA requirement - FAQ.

Amazon API Gateway integration kit retries for 5xx errors

New PingOne Authorize

We've released Amazon API Gateway integration kit version 1.2.0. This version includes a retry mechanism to improve handling of 5xx errors caused by transient network or service issues. Use the `maxRetries` setting in `config.js` to set the maximum number of retries you want before returning a failed response to the client. The default is `1`. Learn more in Configuring Amazon API Gateway for PingOne Authorize integration.

October 3

Support for Microsoft Entra ID external authentication methods by authentication policies

New PingOne

External authentication methods allow Microsoft Entra ID users to leverage external authentication providers for multi-factor authentication (MFA). You can now enable this integration with PingOne authentication policies. Learn more in Setting up PingOne SSO and PingID as the external MFA provider for Microsoft Entra ID.

October 2

Merge or overwrite memberships in outbound group provisioning

New PingOne

You can now merge or overwrite memberships when a group with the same name exists on the target. Learn more in Configuring outbound group provisioning.

Copyright © 2025 Ping Identity Corporation

September 2024

September 30

MFA policies - application name in authenticator app

New PingOneMFA

To help users recognize which application the OTP displayed in their authenticator app is for, the MFA policy configuration page now includes an option called **Show application name**. Use this option to specify the text that should be displayed alongside the OTP in the authenticator app.

September 29

FIDO policies - localhost as relying party

Improved PingOneMFA

To facilitate testing, when you define a FIDO policy in a **Sandbox** environment in PingOne, you can now set **Relying Party ID** to `localhost`.

September 9

Enhanced administrator onboarding experience

New PingOne

We've released a significant update in the PingOne **Administrators** environment to streamline the onboarding process for new PingOne administrators. This release introduces a **Getting Started** experience tailored to address common points of confusion and help new administrators quickly understand and manage their responsibilities within the platform. Learn more in the Introduction to PingOne.

August 2024

August 22

Updated API gateway integration kits

New PingOne Authorize

We've released new versions of the following API gateway integration kits:

- Amazon API Gateway integration kit 1.1.0
- Apigee integration kit 1.1.0
- Kong integration kit 1.1.0

Copyright © 2025 Ping Identity Corporation

These versions improve how the integration kits handle rate limiting to achieve more reliable and stable authorization services. Learn more about connecting your API gateway to PingOne Authorize in PingOne Authorize API gateway integrations.

August 21

Default MFA status for new users setting enabled by default

Improved PingOne

The **Default MFA status for new users** setting on the **MFA Settings** page is now enabled by default in all new environments. This setting allows just-in-time registration of new multi-factor authentication (MFA) methods for PingOne administrators the first time they sign-on to the admin console. Learn more in Configuring MFA settings.

August 19

New risk predictor - Traffic Anomaly

New PingOne Protect

A new risk predictor called Traffic Anomaly has been added in order to detect traffic anomalies in terms of variables such as users, devices, and sessions.

The Traffic Anomaly predictor will eventually include a variety of rules, some of which you can select to enable or disable. In this initial release of the predictor, PingOne Protect detects situations where there are a large number of risk evaluations requested for a single user within a short period of time, and optionally can also detect situations where the number of users per device during a given period is suspicious.

When a risk level of High is calculated for the Traffic Anomaly predictor, it is recommended that you deny access because the suspicious activity is likely due to malicious behavior.

For details, see Predictors, Configuring predictors, and the Risk Predictors section of the PingOne API documentation.

User IP from Signals (Protect) SDK payload

Improved PingOne Protect

Due to the use of corporate proxies and other network tools, the user's true IP was often masked by an internal IP, reducing the benefit provided by risk predictors that factor in the IP or user location. To handle such situations, if PingOne Protect encounters an internal IP, it now uses the user IP that is included in the Signals (Protect) SDK payload. This feature requires version 5.2.7 or later of the Signals SDK for Web.

Deprecation of User Risk Behavior (organization-wide) predictor

Info PingOne Protect

The User Risk Behavior (organization-wide) predictor has been deprecated. The predictor can still be used in existing PingOne environments, but is not available in new environments.

Copyright © 2025 Ping Identity Corporation

August 9

Updated LDAP Gateway client application

New PingOne

We've released LDAP Gateway client application version 3.2.2, which includes improved support for unauthenticated proxy for LDAP gateway provisioning sync.

August 7

Updated LDAP Gateway client application

New PingOne

We've released LDAP Gateway client application version 3.2.0. This version includes:

- Support for using a forward web proxy server to handle WebSocket traffic between the gateway client and PingOne
- Debug logging improvements
- Bug fixes

Learn more about using a web proxy server in LDAP gateways and Starting a gateway instance.

August 5

User group conditions in composite predictors

New PingOne Protect

When creating composite risk predictors, you can now include conditions that check what PingOne user groups the user belongs to. For details, see Adding composite predictors and the example in the PingOne API documentation.

New admin alert - suspicious traffic

New PingOne Protect

You can now add an alert to receive an email notification if PingOne Protect detects a pattern of suspicious traffic that requires your attention. For details on adding alerts, see Adding an alert.

Bot detection enhancement

New PingOne Protect

The Bot Detection predictor now has an option that you can select to expand the types of bot activity that PingOne Protect can detect. For details, see Configuring predictors and the Risk Predictors section of the PingOne API documentation.

Copyright © 2025 Ping Identity Corporation

PingOne Early Access Features

This section provides early access documentation for the PingOne features available to customers who opt in to preview new functionality.

Early access features can be enabled only at the environment level. You can't enable an early access feature for an entire organization.

Not all features are enabled for early access. Additionally, early access features related to services that aren't in the environment or that aren't allowable by the license assigned to the environment aren't available for opt-in.

Learn more in Managing opt-ins for early access features in PingOne.

Important

Early access features are provided for preview purposes only and are not covered under standard Support SLAs. You can open support cases for feedback, bug reports, configuration questions, or other inquiries related to early access features, but resolution times for these cases will vary. These cases often require collaboration with our Engineering and Product teams, so timelines might exceed the usual SLAs for your Support package.
Topics for these features are draft documentation for early access purposes only and are not complete or final.

Copyright © 2025 Ping Identity Corporation

Introduction to PingOne

PingOne is a multi-tenant cloud-based identity as a service (IDaaS) platform for secure identity access management. PingOne uses an organization-based model to define tenant accounts and their related entities within the platform.

To fully leverage the administrator capabilities of PingOne, familiarize yourself with the following key concepts.

Organizations

In PingOne, the organization is the top-level identifier and defines your enterprise within the platform. Each organization contains one or more tenants, known as environments, which define separate working domains within an organization.

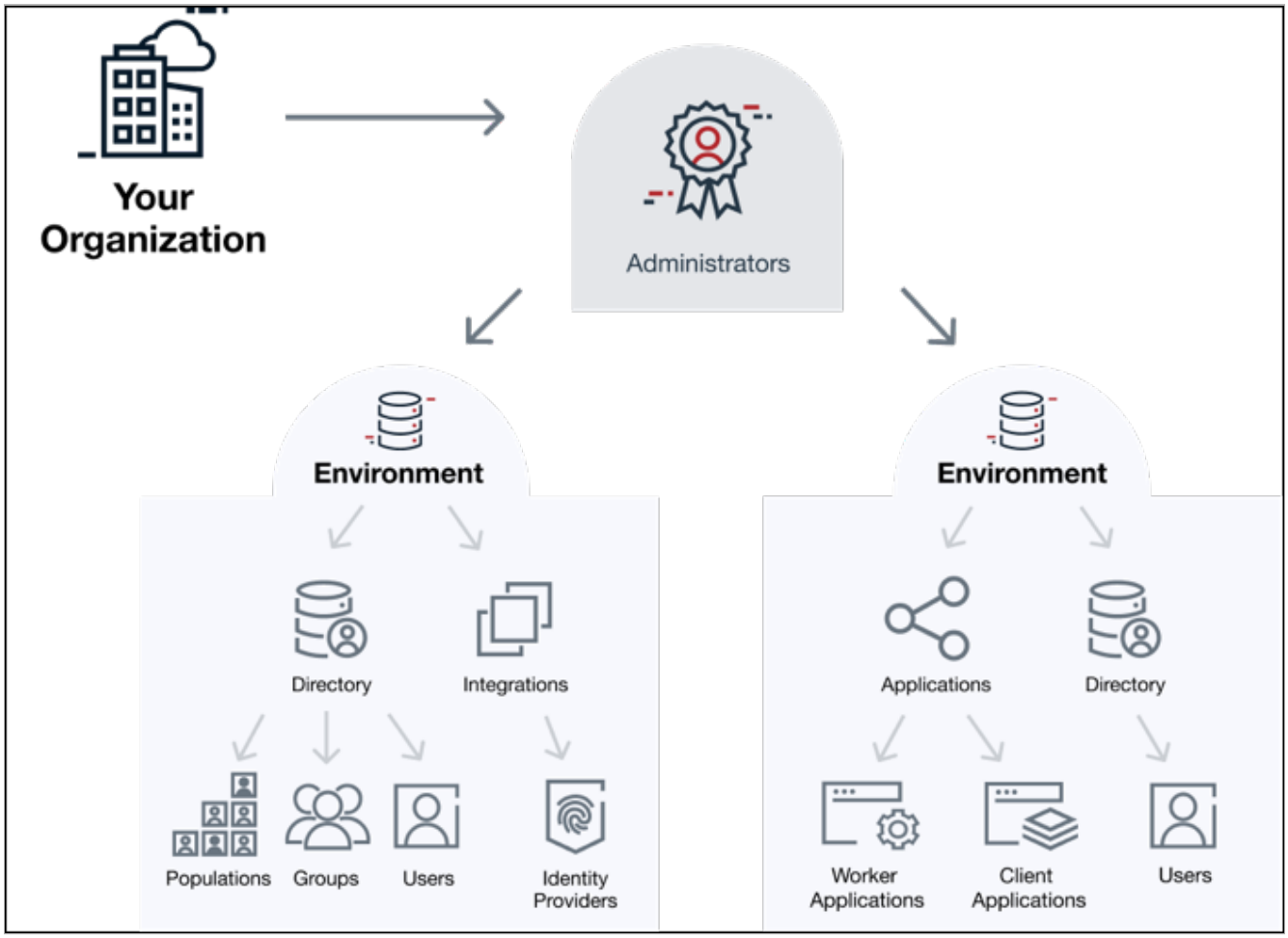
Each organization is based in a specific geographical region, such as North America (US), or Asia Pacific. All of the environment resources for the organization are hosted in this region. You should have organizations in each of the regions in which you operate. Learn more in the IP address and domain reference.

> **Important**
>
> PingOne data centers are available worldwide. For optimum performance, use the data center closest to your geographic region.
> Examples throughout this documentation use URLs for the North America (US) data center. To view URLs for data centers outside of North America (US), expand the **PingOne URLs by geographic region** table.

Region	Admin console	User self-service	Management API endpoints	Authentication and authorization API endpoints
Australia	console.pingone.com.au	apps.pingone.com.au	api.pingone.com.au	auth.pingone.com.au
Canada	console.pingone.ca	apps.pingone.ca	api.pingone.ca	auth.pingone.ca
Europe	console.pingone.eu	apps.pingone.eu	api.pingone.eu	auth.pingone.eu
Singapore	console.pingone.sg	apps.pingone.sg	api.pingone.sg	auth.pingone.sg
Asia Pacific	console.pingone.asia	apps.pingone.asia	api.pingone.asia	auth.pingone.asia
In the Asia Pacific region, new organizations are registered under the pingone.com.au domain. Ping Identity also supports existing organizations registered under the pingone.asia domain. Both domains provide Australia-only data residency.				

When an organization is created, an **Administrators** environment is created automatically. Learn more in Environments.

Copyright © 2025 Ping Identity Corporation



After you create your organization, you can create the environments that meet the requirements of your business.

Environments

In PingOne, tenants are called environments. Environments define separate working domains within an organization and contain assets such as your PingOne services and Ping Identity products, application connections, and user identities.

Environment usage

There are many ways to use environments within an organization. If your company is made up of several different business units, you can use environments to define those units and ensure each one has access only to the assets that pertain to their business. For example, if you use PingOne for both customer and employee (workforce) use cases, you could have a Customer environment and an Employee environment. Those environments would include services, applications, and policies applicable only to those use cases.

You can also create Sandbox environments to deploy and test new features or configuration changes before releasing them to your Production environments.

After reviewing this section, learn more about creating environments in Adding an environment.

To access the **Environments** page, click the Ping Identity logo on the sidebar or the **Home** icon at the top of the admin console.

Copyright © 2025 Ping Identity Corporation

Identities and source environments

In PingOne, every identity resides in a single source environment, which is the environment where the identity exists. For example, if you create an identity in the **Administrators** environment, then the **Administrators** environment is that identity's source environment.

In most cases, you should create all administrator identities in the **Administrators** environment to make it easier to manage them and to help prevent privilege escalation.

> **Important**
>
> Identities don't have to reside in the same environments to which they have access.
> End users and customers should reside in a separate environment from your administrator identities.

In some scenarios, you might not have administrator access to the source environment for your identity (where your identity resides). In this case, your source environment is different from the environment you can work in, but you authenticate to your source environment.

Users with the Identity Data Admin role, for example, are the only users who can have access to their identity's source environment to manage other administrators and their roles. Administrators with other built-in roles assigned do not have access to their source environment.

> **Note**
>
> Different administrators can be assigned different roles that determine what they have access to and in where they have that access. You can find more details in Administrator roles and permissions.

Sandbox and Production environments

When you create an environment, you can select **Sandbox** or **Production** for the environment type. Sandbox environments allow you to test configuration changes before you deploy them to production. Production environments are intended for live configurations that are deployed for real-world use. Both environment types count toward your license entitlements.

You can promote a Sandbox environment to Production, but Production environments can't be demoted to Sandbox. Learn more in Promoting a Sandbox environment to Production.

> **Note**
>
> When you delete a Sandbox environment, the environment is removed immediately and can't be recovered. When you delete a Production environment, the environment is unusable and moved into a pending deletion status for 30 days. The environment is still listed on the **Environments** page and is recoverable within that 30-day period. Learn more in Deleting an environment.
> If you have a trial license, you can't create Production environments or promote Sandbox environments to production.

> **Best practice**
>
> Don't use Sandbox environments for production activities. Production environments include deletion protection to safeguard important data. Learn more in Deleting an environment.

Copyright © 2025 Ping Identity Corporation

Administrators environment

An **Administrators** environment is created automatically when an organization is created in PingOne. You should create all administrators for the organization in the **Administrators** environment to keep them separate from your end users and to improve security.

By default, the **Administrators** environment includes the PingOne SSO and PingOne MFA services.

> **Note**
>
> Do not add other services or products to the **Administrators** environment.

In PingOne, administrators don't need to belong to an environment to administer that environment. When you assign roles to your administrators, you can decide for which environments they have those roles. You can also limit certain roles to particular populations or applications within an environment. Learn more in Managing administrator roles.

> **Note**
>
> Organizations created before July 1, 2020 might not include an administrator license or a dedicated administrators environment. However, you should still create and manage your PingOne administrator accounts in a single environment.
> If your **Administrators** environment was renamed, but is still assigned the ADMIN license, use that environment for storing administrator identities.
> If you do not have an administrator license, contact your Ping representative. Certain PingOne functionality is available only with an administrator license.
> Throughout this documentation, the **Administrators** environment refers to the environment in your organization that is assigned the ADMIN license.

If your **Administrators** environment was created automatically when your organization was created, it has several restrictions to ensure that:

- You can't change the license assigned to the **Administrators** environment.
- You can't delete the **Administrators** environment.

Environment contents

Environments encompass:

PingOne services and other Ping product integrations

PingOne services provide distinct, advanced capabilities in PingOne. Services are deployed at the environment level, and the services available to you depend on your PingOne license. PingOne services provide the following capabilities:

- Single sign-on with PingOne SSO: Allows users to use single sign-on (SSO) to access all their applications and services with one set of credentials. Learn more in PingOne SSO.
- Strong authentication (MFA): Provides multi-factor authentication (MFA) with PingOne MFA for Customer environments, and PingID for Workforce environments. Learn more in Strong Authentication (MFA).

Copyright © 2025 Ping Identity Corporation

- Threat protection with PingOne Protect: Prevents identity fraud by incorporating advanced features and real-time detection and enables customers to combat bad actors and address both password and MFA fatigue. Learn more in Threat Protection using PingOne Protect.
- Identity verification with PingOne Verify: Enables secure user verification based on a government-issued document and live face capture (a selfie). Learn more in Identity Verification using PingOne Verify.
- Digital credentials with PingOne Credentials: Allows an issuer to create verifiable credentials that they can send to a compatible wallet app. Learn more in Digital Credentials using PingOne Credentials.
- Authorization with PingOne Authorize: Controls what end users can see and do inside of applications and APIs. Learn more in Authorization using PingOne Authorize.

Your environments can also be used to configure SSO to other Ping products you use, such as PingFederate and PingOne Advanced Identity Cloud.

Populations

A population defines a set of users, similar to an organizational unit (OU). In a given environment, you can use populations to simplify the management of users. For example, you can create a population for similar types of users and apply a password policy to that population. You must create at least one population before you can create users. Learn more in Populations.

> **Note**
>
> An individual user can't belong to more than one population at the same time, but you can move a user to a different population.

Groups

Groups are used to organize a collection of user identities and make it easier to manage access to applications. Groups offer more fine-grained access control than populations. A user can belong to multiple groups, but only one population. For example, you could use a population to contain all your employees and use a group to define subsets, such as Marketing, HR, Contractors, or US Employees. Learn more in Groups.

Users

A user is a unique identity that interacts with the applications and services in the environment to which the user is assigned. An identity is the full representation of a user profile, including relationships, roles, and attributes. Users are associated with populations instead of being defined within a population. Learn more in Users.

Applications

Application resources define the connection between PingOne and the actual application, also known as a client connection. Connections to external resources use open standards protocols. Client connections define the configuration for OpenID Connect (OIDC) and OAuth clients.

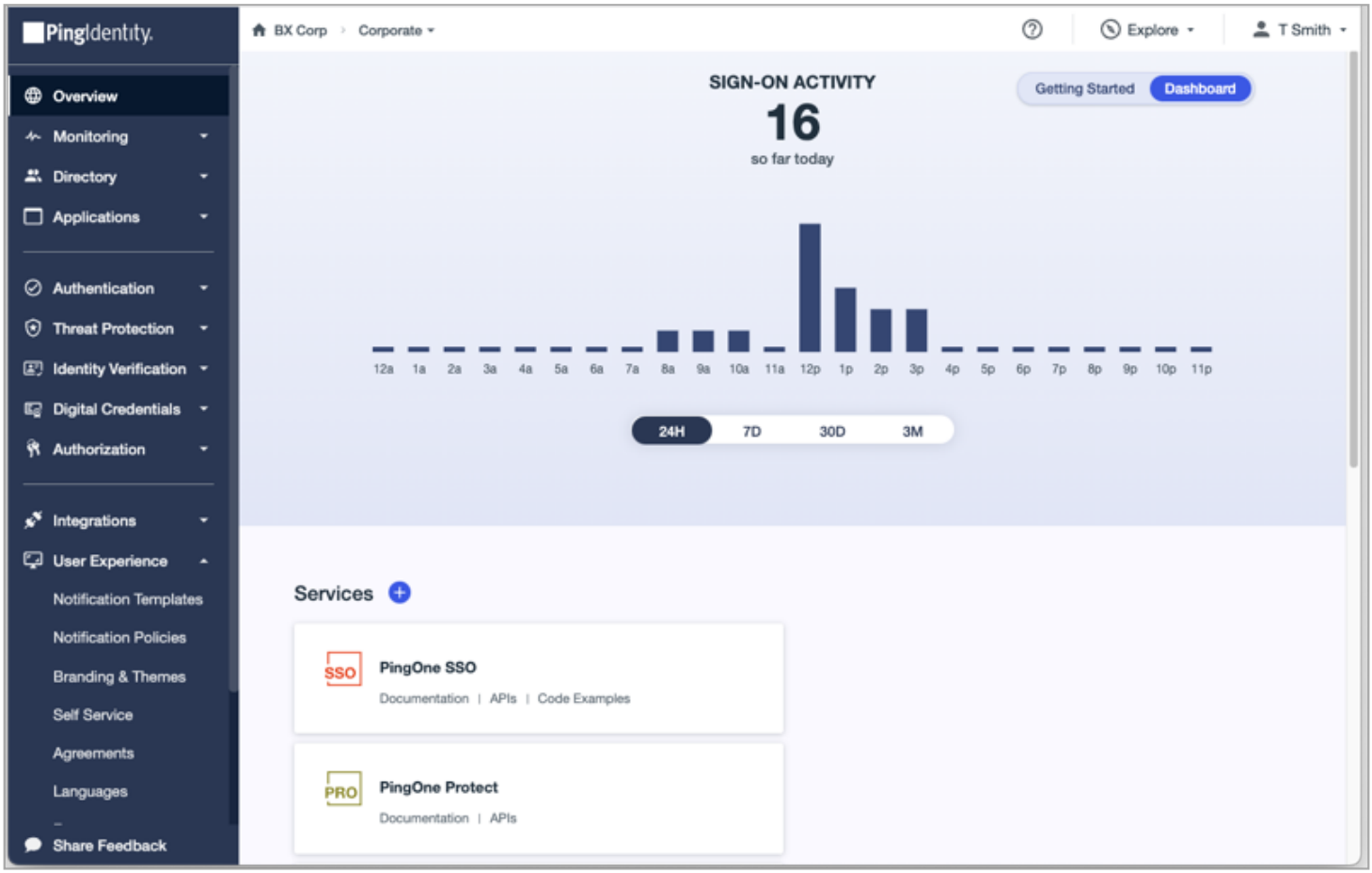
Application grants describe which scopes the application can request. Scopes define the permissions for the application. Learn more in Applications and Editing an application.

Copyright © 2025 Ping Identity Corporation

Environment dashboard

The environment dashboard is accessed by clicking **Overview** in the sidebar. This dashboard provides:

- A list of the products and services included in the environment
- A graph showing the activity that has occurred within the environment (if the environment contains PingOne services)
- Links to documentation, APIs, and code examples for each product and service in the environment



Activities

Activities, or events, are collections of user-activity information, such as sign-on attempts, password reset attempts, and total active user counts. This audit data can be exported, reported on, or streamed out to customer SIEM (Security Information and Event Management) solutions. Learn more about auditing events and running audit reports in Audit.

Branding and images

User interface branding elements are defined in the branding resource. This resource contains configuration properties for customizable elements of the PingOne user interface. All end user interfaces are branded according to the theme defined in the branding resource. Learn more in Branding and themes.

Copyright © 2025 Ping Identity Corporation

Password policies

Password policies define the strength and complexity requirements for a password for users within an environment. Learn more in Password policies.

Authentication policies

Authentication policies dictate how the user's identity will be verified. For example, a single-factor authentication policy requires a single piece of evidence to verify a user's identity, such as a password. A multi-factor policy could require evidence to verify a user's identity, such as a TOTP authenticator app, FIDO2 biometrics, a push notification sent to the user's mobile device, or a one-time passcode (OTP) sent over SMS, voice, or email. Learn more in Authentication policies.

Notification templates

Notification templates are used to create messages that inform end users about certain events, such as device pairing and password resets. You can create templates for SMS, email, or voice messages. Learn more in Notification templates.

External identity providers

External identity providers (IdPs) allow linked users to authenticate using the credentials provided by the external identity provider (IdP). An external IdP includes mapping PingOne user attributes to attributes from the IdP.

You can also use an external IdP to secure the PingOne admin console.

Learn more in External IdPs.

Certificates and key pairs

When you create a new environment, PingOne creates two default key pairs: one for signing and one for encryption. You can create additional certificate and key pairs as necessary for your environment. Learn more in Certificates and key pairs.

Administrator roles and permissions

An administrator role is a collection of permissions that can be assigned to a user, application, or connection, and then applied to a level, or scope, within PingOne. The combination of the role permissions and the level at which the role is applied determines what an administrator can do (permissions) and where they can do it (level or scope).

In PingOne, roles can be applied to the organization, environment, population, or application level, although not all roles can be applied at all levels.

PingOne includes a number of built-in administrator roles. These roles are not hierarchical, and there is no super admin role that has permissions to perform every action at every level in PingOne. The roles available to your organization depend on your configuration and licensing.

> **Note**
>
> Add all of your PingOne administrators to the **Administrators** environment to keep them separate from end users and to improve security. Administrators do not have to belong to an environment to have administrator permissions over that environment. Learn more in Environments.

Copyright © 2025 Ping Identity Corporation

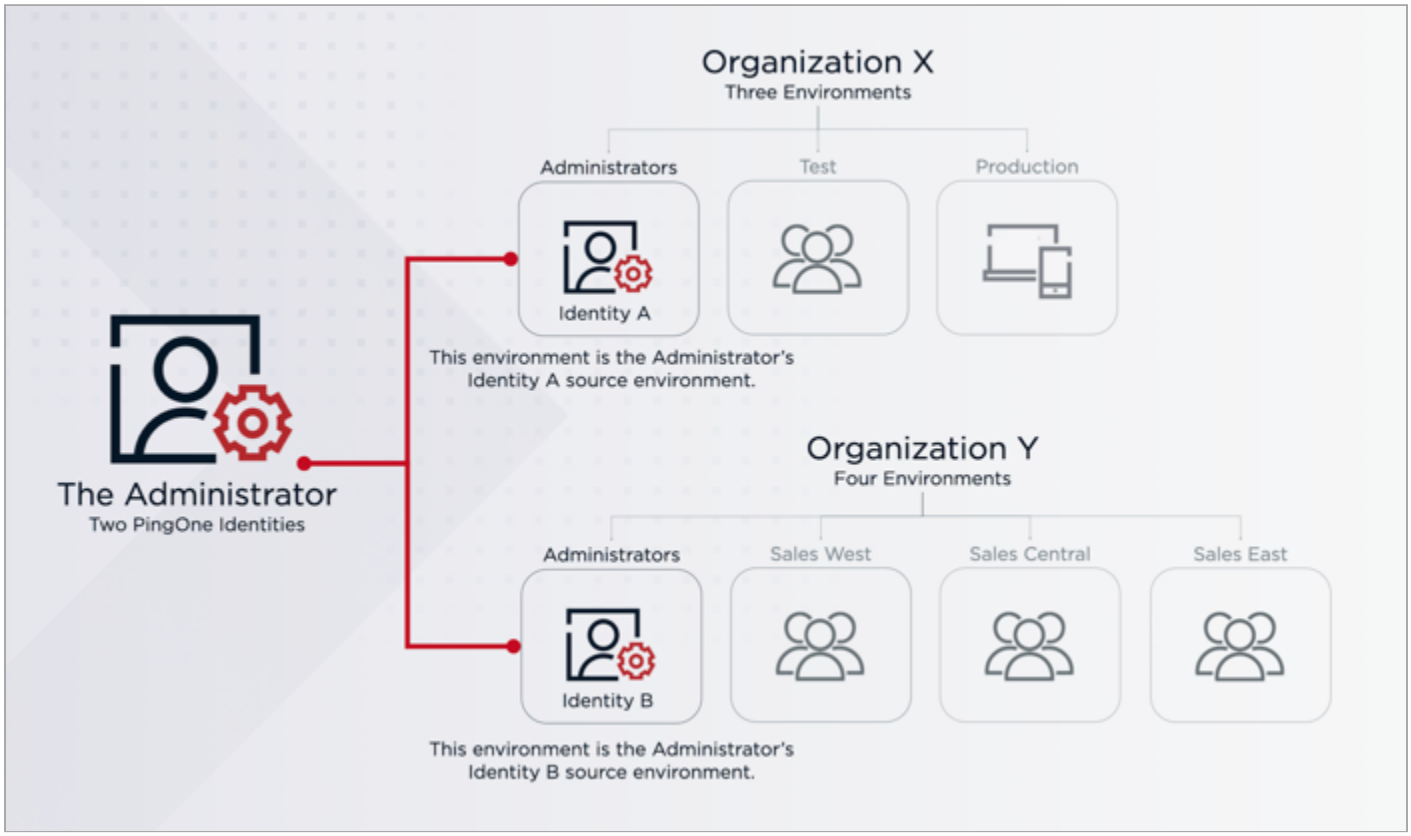
PingOne administrators can have multiple administrator identities across multiple environments in a single organization, a single administrator identity over multiple environments, or a combination of both. They can also have different roles that apply in those different contexts.

For some complex use cases, you might need multiple administrator identities to configure multiple organizations. An example use case is a contractor working with more than one company to configure environments. In this scenario, the contractor would need an administrator identity in each company's organization. Similarly, if a company has organizations in multiple geographic regions, an administrator who needs to manage all of those organizations needs an identity in each organization.

> **Note**
>
> You can't have more than one instance of the same identity in a single environment. For these complex use cases, you must create those identities in multiple environments.

If you have multiple administrator identities associated with the same email address, you can select which organization you want to authenticate to after signing on. You'll need to choose the identity with the right permissions based on the actions you intend to take.

Copyright © 2025 Ping Identity Corporation



Learn more about administrators and their roles in:

- Managing administrators
- Managing administrator roles
- Environments
- Configuring roles for a worker application

Groups and populations

Groups and populations are both used to organize users, but they differ in several ways.

A user can belong to multiple groups, but only one population. A population is a fundamental organizational unit to which you can assign a particular sign-on policy and IdP, while groups offer more fine-grained control over user access to applications.

For example, you could create two populations in your environment. One population would contain all of your finance employees, and the other would contain your engineering and support staff. You can assign each of these populations a different sign-on policy, and can also set different IdPs for each.

Within each population, you can create groups to define subsets of the population. Although a user can belong to only one population at a time, they can belong to multiple groups. These groups can then be given access to different applications. For example, in your employee population, you might have groups for different departmental organizations such as Marketing, Engineering, and Payroll.

Copyright © 2025 Ping Identity Corporation

You can create groups at the population level or the environment level. A population-level group can contain users from that population only, but an environment-level group can contain users from different populations in the same environment. Administrators who are assigned roles scoped only to the population level can create groups for those populations only and cannot create groups at the environment level.

Key differences between groups and populations are summarized in the following table:

Populations and Groups comparison

Populations	Groups	Both
• Users can belong to only one population • You can assign a sign-on policy to a population • You can assign an identity provider to a population • You can create groups within a population to define subsets of that population	• Users can belong to more than one group • Groups can contain users from more than one population • Sign-on policies and identity providers can't be assigned to groups • You can create groups within a population • Groups allow fine-grained control over access to applications	• Populations and groups are defined at the environment level • Administrator roles can be assigned to groups and populations

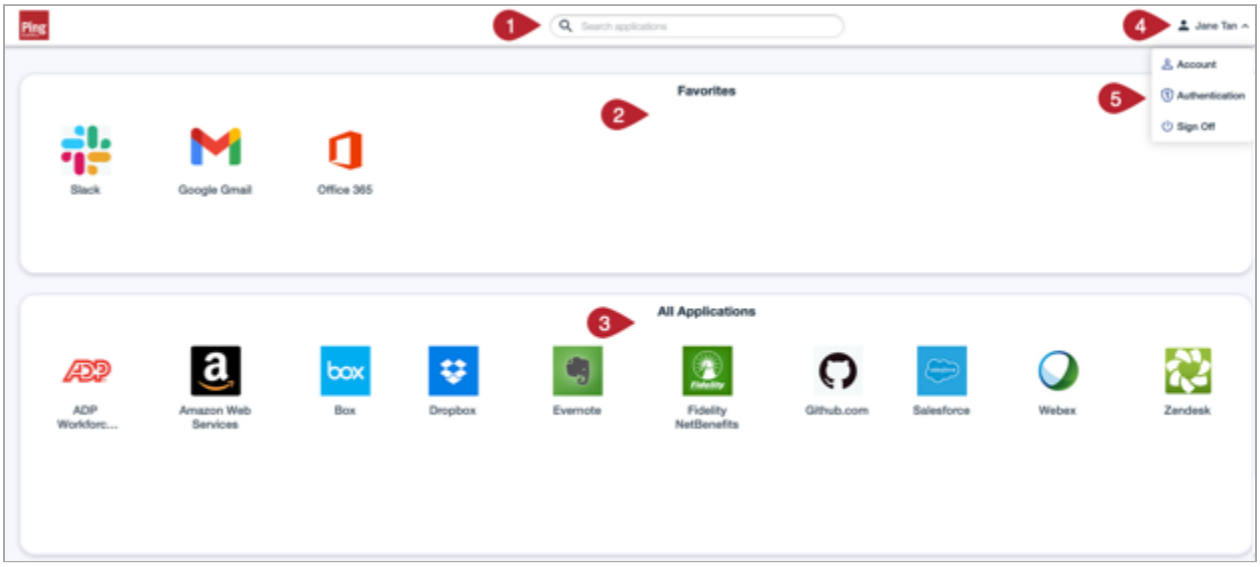
On the **Groups** page, population-level groups include the name of the population under the group name.

Learn more in Groups and Populations.

PingOne application portal

The PingOne application portal is a unified interface that enables your users to use SSO to access the applications you've added for your organization.

Copyright © 2025 Ping Identity Corporation



PingOne application portal key sections:

1. Search bar
2. **Favorites** section
3. **All Applications** section
4. User avatar
5. User control panel

Search bar

When you enter a search string, the search bar generates a list of the closest matches. Click the application row to launch the application directly from the results list.

Favorites and All Applications

- Click an application icon to launch the application in a new browser tab.
- To add an application to favorites on the desktop version, drag it into the **Favorites** section.
- Hover over the application's icon to see its description. You can also click the star in the description to add or remove an application from favorites.
- To remove an application from favorites in the desktop version, drag it back to the **All Applications** section.
- In the desktop version, you can reorder application icons in the **Favorites** area by dragging and dropping them.

> **Note**
>
> You can't reorder favorites in the mobile version.

- To add an application to favorites in the mobile version, tap the **Star** on the application line, either on the **All Apps** tab or from the search bar.

Copyright © 2025 Ping Identity Corporation

- To remove an application from favorites in the mobile version, tap the **Pencil** icon, and then tap the **Star** on the line of the application that you want to remove. When you're finished, tap **Done**.

User control panel

- Click the **User avatar** to access the **User control panel**.
- Click **Account** to access your PingOne profile. Learn more in End users: Accessing your PingOne profile.
- Click **Authentication** to manage your MFA (multi-factor authentication) devices.
- Click **Sign Off** to sign off of all applications and end your PingOne session.

How the PingOne application portal works

The PingOne application portal grants users access to SAML and OpenID Connect applications. The applications that a user sees depend on the access controls for each application. Learn more about adding an application in Adding an application.

> **Tip**
>
> To make an OIDC application available on the PingOne application portal, the application must have an **Initiate Single Sign-on URL**. You can add this URL after creating the application by going to the **Configuration** tab and entering the URL into the **Initiate Login URI** field.
> Learn more in Editing an application - OIDC.

Showing or hiding applications

Even if a user has access to an application, you can specify whether to include it in the Application Portal. For example, you could show or hide an application if the SSO flow is being triggered through means other than on the Application Portal. Learn more in Application access control and Editing an application.

Preview the PingOne Application Portal

1. In PingOne, go to **Applications** > **Applications**.
2. Click the **PingOne Application Portal** application.
3. Copy the **Home Page URL** and paste it into a new browser tab.
4. Enter a user's credentials in the **Username** and **Password** fields.
5. Click **Sign On**.

PingOne Dashboards

Administrators can use PingOne Dashboards to view and monitor activities for a service.

Learn more about the information each dashboard provides in the following sections:

- Overview page

Copyright © 2025 Ping Identity Corporation

- Authentication dashboard
- Authorization Dashboard
- MFA dashboard
- Threat Protection Dashboard
- User Demographics Dashboard
- Identity Verification Dashboard

PingOne Solutions

PingOne uses PingOne Services to help solve a wide variety of identity problems.

PingOne Solutions packages are packages of PingOne Services designed to help you easily manage your organization's identity challenges by allowing you to choose the package that's right for you, whether your organization is small with basic requirements or large with a complex deployment.

PingOne for Customers, PingOne for B2B, and PingOne for Workforce packages are each available in two package tiers: Essential and Plus. You can add other PingOne Services to a package if your solution requires additional capabilities.

Every PingOne for Customers, PingOne for B2B, and PingOne for Workforce solution package lets you orchestrate Ping products seamlessly using PingOne DaVinci. With DaVinci, you can rapidly build, test, and optimize identity experiences using a drag-and-drop interface and no-code orchestration to weave together Ping identity services and capabilities.

We also offer solutions that combine DaVinci flows with PingOne and other tools to address complex business challenges. The PingOne for Customers Passwordless solution uses a set of tailored DaVinci flows to create a registration and sign on process that incorporates passwordless, password, and MFA options.

Learn about PingOne Solutions packages and their included capabilities:

- PingOne for Customers is a cloud solution designed to improve customer experiences and meet business needs by combining no code orchestration with SSO and MFA authentication services.
- PingOne for B2B is a cloud solution designed to improve the business-to-business experience and meet the needs of partners and customers by combining no code orchestration with SSO and MFA authentication services.
- PingOne for Workforce is a cloud-based solution that helps you orchestrate the experiences your work-anywhere employees need.
- PingOne Neo is a decentralized identity solution that gives control of identity data back to users. PingOne Neo empowers businesses to give their users full control over how they securely store and share verified credentials without unnecessary friction.
- PingOne for Customers Passwordless lets you offer your end users a variety of flexible passwordless options for account creation, sign-on, profile management, and account recovery using a simple Getting Started experience and pre-built DaVinci flows.

PingOne for Customers

PingOne for Customers is a cloud solution combining no-code orchestration with authentication, user management, and multi-factor authentication (MFA) services to meet business needs and improve customer experiences.

Copyright © 2025 Ping Identity Corporation

PingOne for Customers is available in two solution packages:

- Essential: Rapidly build identity experiences using no-code orchestration with authentication and user management.
- Plus: Enhance security with MFA alternatives to passwords to streamline the sign-on process.

Additional capabilities are available as add-ons based on your solution requirements. Try PingOne today with a no-cost 30-day trial to see how your organization can leverage cloud-based identity solutions to meet your unique business needs.

The following table details the available solution packages, optional add-ons, and trial offerings:

PingOne for Customers Solution Package Capabilities

Capability	Essential	Plus	Add-on	Trial
Authentication and SSO	Yes	Yes		Yes
Directory	Yes	Yes		Yes
Outbound Provisioning	Yes	Yes		Yes
Orchestration Starter Pack	Yes	Yes		
Connect to external LDAP	Yes	Yes		Yes
Multi-factor Authentication		Yes		Yes
API Access Management		Yes		
Advanced Access Security			Yes	
Risk Management			Yes	Yes
Identity Verification			Yes	Yes
Dynamic Authorization			Yes	Yes
Fraud Detection			Yes	
Advanced Authorization			Yes	
Additional Regions/Environments			Yes	

PingOne for B2B

PingOne for B2B is a cloud solution combining no-code orchestration with authentication, user management, and multi-factor authentication (MFA) services to meet business-to-business needs and improve the security of your third-party access experiences.

Copyright © 2025 Ping Identity Corporation

PingOne for B2B is available in two solution packages:

- Essential: Rapidly build identity experiences using no-code orchestration with authentication and user management.
- Plus: Enhance security with MFA alternatives to passwords to streamline the sign-on process.

Additional capabilities are available as add-ons based on your solution requirements. Try PingOne today with a no-cost 30-day trial to see how your organization can leverage cloud-based identity solutions to meet your unique business needs.

The following table details the available solution packages, optional add-ons, and trial offerings:

PingOne for B2B Solution Package Capabilities

Capability	Essential	Plus	Add-on	Trial
Authentication and SSO	Yes	Yes		Yes
Directory	Yes	Yes		Yes
Outbound Provisioning	Yes	Yes		Yes
Orchestration Starter Pack	Yes	Yes		
Connect to external LDAP	Yes	Yes		Yes
Multi-factor Authentication		Yes		Yes
API Access Management		Yes		
Advanced Access Security			Yes	
Risk Management			Yes	Yes
Identity Verification			Yes	Yes
Dynamic Authorization			Yes	Yes
Fraud Detection			Yes	
Advanced Authorization			Yes	
Additional Regions/Environments			Yes	

PingOne for Workforce

PingOne for Workforce is a cloud-based solution that helps you orchestrate the experiences your work-anywhere employees need.

Copyright © 2025 Ping Identity Corporation

Featuring identity intelligence, drag-and-drop workflows, passwordless sign-on, centralized authentication and a unified admin portal, PingOne for Workforce is available in two solution packages:

- Essential: Centralize single sign-on (SSO), Directory, and basic MFA for software as a service (SaaS) apps, and integrate with your Microsoft environment
- Plus: Create an LDAP connection to on-prem identity data, and enhance security and experience with intelligent, adaptive authentication

Additional capabilities are available as add-ons based on your solution requirements. Try PingOne today with a no-cost 30-day trial and start delivering the seamless, secure experiences that your employees are looking for.

PingOne for Workforce Solution Package Capabilities

Capability	Essential	Plus	Add-on	Trial
Standards-based AuthN/SSO (OIDC/SAML)	Yes	Yes		Yes
Directory	Yes	Yes		Yes
Application Portal	Yes	Yes		Yes
Outbound provisioning	Yes	Yes		Yes
Application Catalog	Yes	Yes		Yes
O365 with WS-Fed/WS-Trust	Yes	Yes		Yes
Basic MFA	Yes	Yes		Yes
Inbound provisioning (SCIM, Workday, User onboarding through AD/LDAP Gateway)		Yes		Yes
Adaptive Multi-Factor Authentication		Yes		Yes
Gateway - Integrate with AD/LDAP		Yes		Yes
Orchestration Starter Pack	Yes	Yes		
Advanced, including non-standards based, SSO				Yes
Risk Management				Yes
Advanced Authorization			Yes	
Additional Regions/Environments/Perf Reqs.				Yes

Copyright © 2025 Ping Identity Corporation

PingOne Neo

PingOne Neo is a decentralized identity solution that gives control of identity data back to users. PingOne Neo empowers businesses to give their users full control over how they securely store and share verified credentials without unnecessary friction.

PingOne Neo also provides organizations with identity verification capabilities and the capability to issue credentials for users to store in their wallet app and verify user data with access to:

PingOne Credentials

PingOne Credentials is a service that allows issuers to customize and issue verifiable digital credentials that users can store in their wallet app with no code required.

PingOne Verify

PingOne Verify is a service that enables secure user identity verification based on a government-issued document and live face capture (a selfie) using the PingOne Verify Integration Kit. Learn more in PingOne Verify Integration Kit.

PingOne Neo SDK

PingOne Neo SDK provides embedded identity verification and a digital wallet into your mobile applications. PingOne Neo SDK works with PingOne Verify and PingOne Credentials. Android and iOS are both supported.

What is decentralized identity and why is it important?

Traditionally, users have to authenticate with more than one IdP requesting various types of information. This leads to an unsustainable situation in which personally identifiable information (PII) is spread across multiple IdPs, leaving remnants of data in multiple places. User data can quickly become out-of-date, and users are left with little or no control over their identity data.

Decentralized identity focuses on giving control of personal data back to the individual. The foundation of decentralized identity is that individuals can store identity-related data in a digital wallet on a mobile device so that they can keep that information updated and share exactly what data they want — down to the attribute — with businesses and other individuals. Personal information is stored with the user only, and the user controls how their information is collected and shared.

Businesses also benefit under this model because decentralized identity enables companies to better protect customer privacy, improve the user experience, and alleviate the challenges associated with collecting personal data. Businesses only need to receive and maintain the minimum amount of user data necessary, and only after obtaining the user's permission.

The decentralized identity model is different from the traditional model. With decentralized identity, the organizations that issue information that users can store and share have no connection to the organizations that the user can choose to share that independently verifiable data with, thereby enabling increased privacy and boosting identity verification.

Using PingOne Neo

How data issuers use PingOne Neo

Issuers only hold information relevant to the service they provide. They can use PingOne Credentials to create and issue verifiable credentials and develop their own app that runs the PingOne Neo SDK for ultimate customization.

Verifiable credentials can be created for a number of use cases, such as:

- A state or province-issued driving license

Copyright © 2025 Ping Identity Corporation

- A national ID card or passport
- An educational institution holding your transcripts to issue proof of qualifications
- A store wanting to issue a loyalty card
- A medical provider to issue a vaccination certificate

How data verifiers use PingOne Neo

A verifier can be any organization that wants to verify your identity, qualifications, or certifications, such as your date of birth, driver license, or proof of medical records.

Verifiers request verification information from a user to continue an interaction. Information verification requests could include:

- A bar or liquor store requesting proof of age
- An event organizer checking someone has a valid ticket

A typical verification flow is initiated from the verification site:

1. The verifier defines the information request and presents the request to the user through a QR code.
2. The user opens the information request in their digital wallet by scanning the QR code and approving the fields they want to share.
3. When the verifier receives the information, they verify the credibility of the user data. If satisfied, the verifier can continue interacting with the user and provide the service requested.

Where do your users fit in?

Users can collect, store, and share their personal information using a digital wallet that's stored on their mobile app. The digital wallet holds a unique private key tied to the individual's identity.

Users might:

- Receive digital cards from issuers with verifiable information, such as proof of qualification, loyalty cards, and medical records.
- Share verified information with verifiers or other individuals who require proof of ID or other identification information.

  Your users control what information they share with a verifier, down to the attribute level. For example, if asked for proof of age, rather than sharing their entire driver license, which might contain other sensitive information like their address, they can choose to share only the age attribute.

Learn more on the PingOne Neo website.

Copyright © 2025 Ping Identity Corporation

Getting Started with PingOne

The PingOne admin console simplifies environment organization and provides access to admin consoles for all Ping products and services.

From the main administrator console, you have one-click access to:

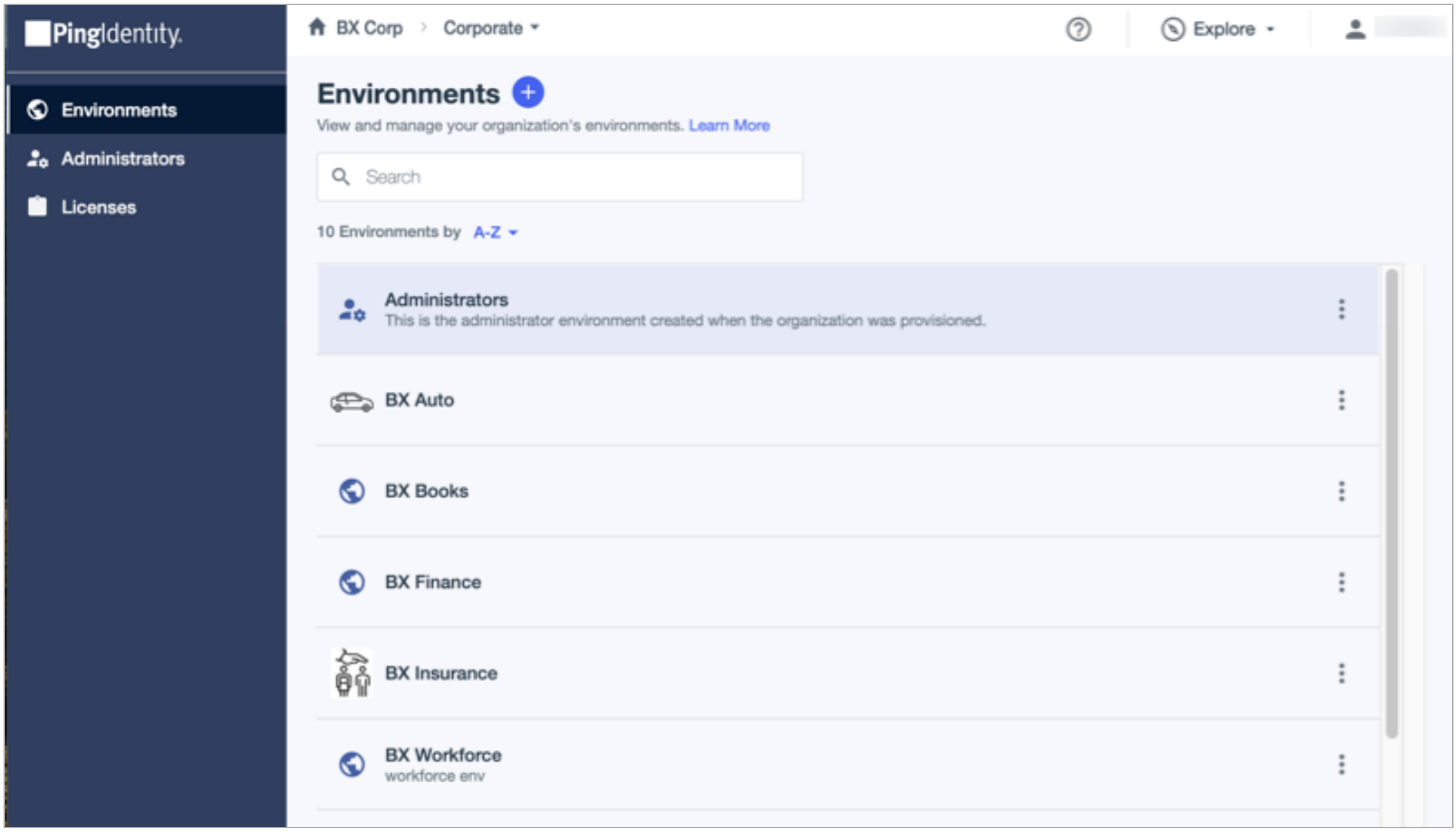
- Documentation, the API, code examples, data sheets, and videos for each product and service
- Interactive wizards that make it easy to build custom solutions and configure the Ping platform for any cloud environment scenario

To access the admin console for your organization, sign on to your account from either pingidentity.com or support.pingidentity.com and complete a few simple steps. Learn more in Accessing the PingOne admin console.

Environments page

The first time you access the admin console, the **Environments** page displays and lists the environments to which you have access. If you have the Organization Admin role, you'll see all of the environments in your organization.

> **Note**
>
> Subsequent sign ons take you to the admin console for the environment you last accessed. To return to the **Environments** page, click the Ping Identity logo on the sidebar or the **Home** icon at the top of the console.



Most organizations include an **Administrators** environment for keeping your administrator users separate from your end users. This environment is pinned to the top of the list.

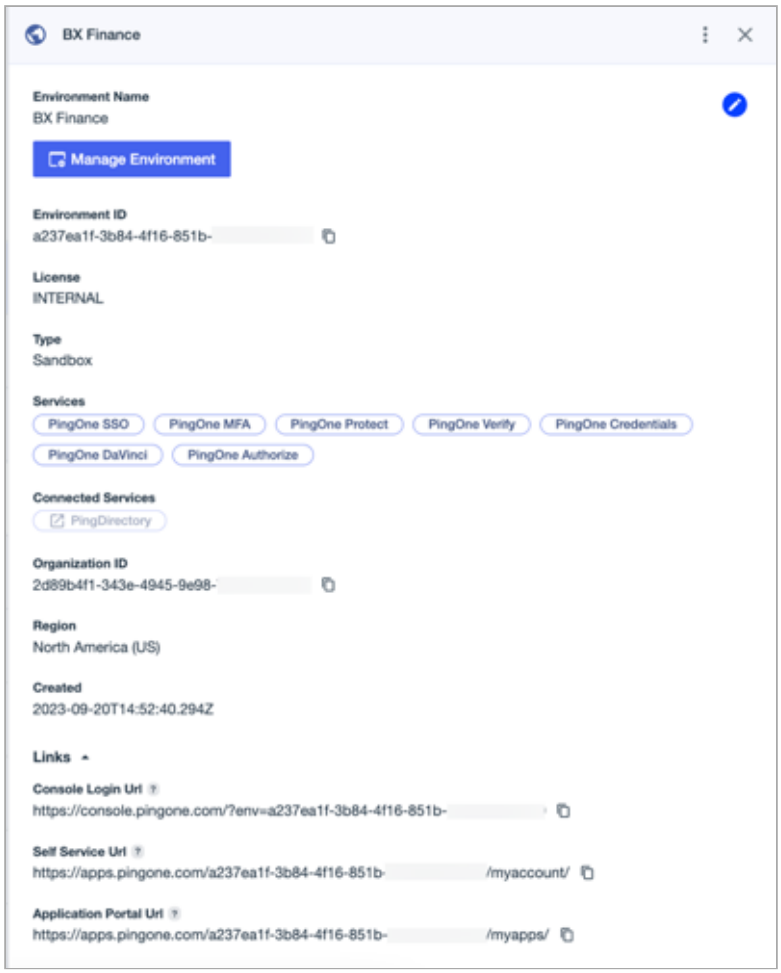
Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Older organizations might not have an **Administrators** environment by default, or the **Administrators** environment might be called something else. Whether or not you have an **Administrators** environment, you should manage all administrators in their own environment to separate them from end users and improve the security posture of your organization.

Use a combination of the search box and the sorting options to locate the environment you want quickly.

> **Note**
>
> The **Administrators** environment stays at the top of the list, regardless of the sort order you choose. However, if you enter search criteria that does not match the **Administrators** environment, it's not displayed in the search results.

Click an environment in the list to open the details pane.



To access the dashboard for a particular service or connected product in the environment, click the service or product name under **Services** or **Connected Services**.

> **Note**
>
> If a connected product or service is not configured, it's grayed out and a tooltip indicates that it requires configuration.

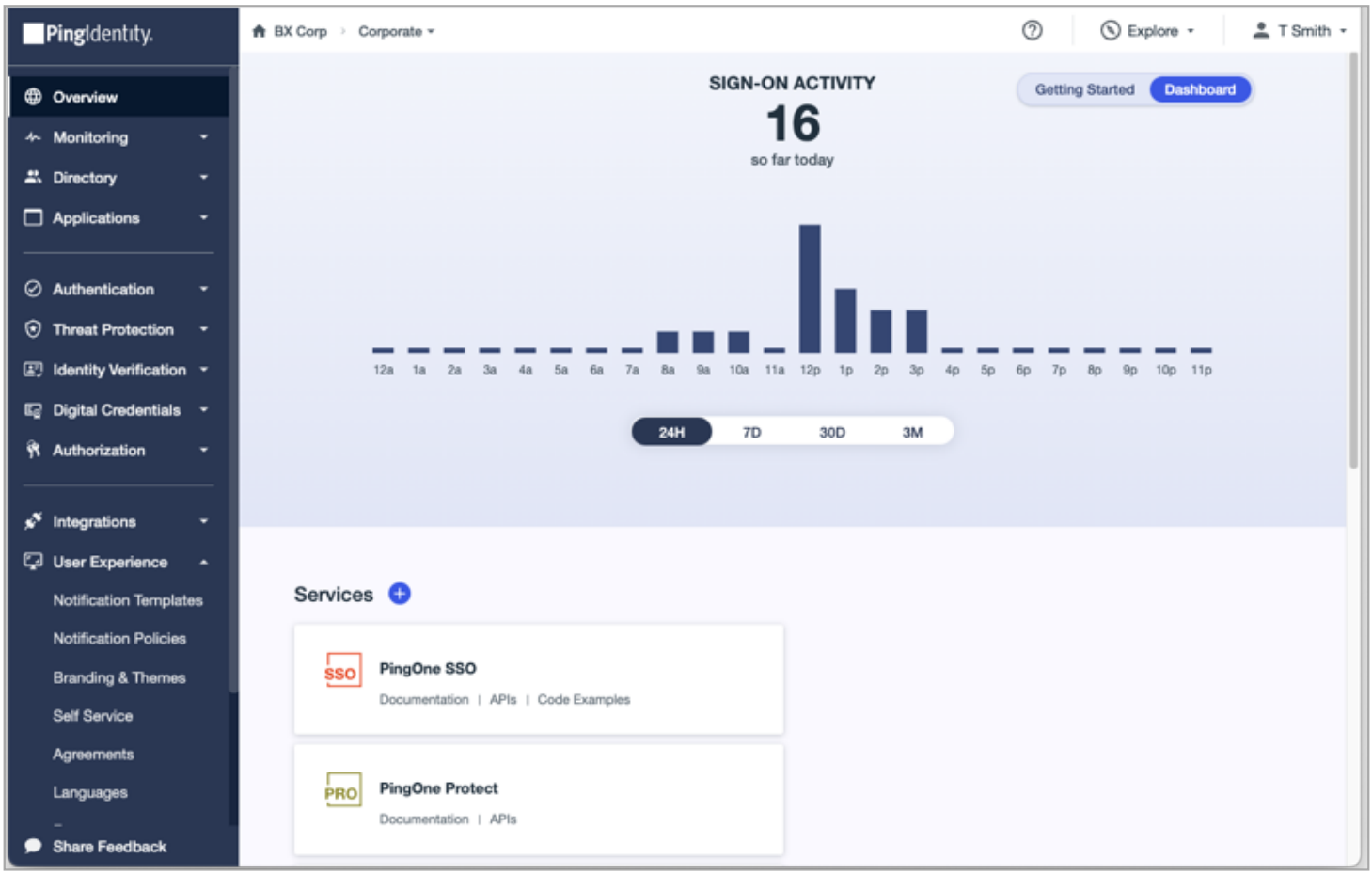
Copyright © 2025 Ping Identity Corporation

Click **Manage Environment** to go to the **Overview** page for the environment, which includes:

- A list of the products and services included in the environment
- A graph showing the activity that has occurred within the environment (if the environment contains PingOne services)
- Links to documentation, APIs, and code examples for each product and service in the environment

The menu options in the sidebar vary depending on which products and services are included in the environment.

The following example shows all of the services and most of the top-level menus.



More information

Learn more about the PingOne APIs in the PingOne Platform API Reference.

Learn more about configuring applications in Editing an application.

Learn more about authorization flows in Authorization flow by grant type, OpenID Connect/OAuth 2, and Flows.

Copyright © 2025 Ping Identity Corporation

Accessing the PingOne admin console

The PingOne admin console is the main point of entry for administrators in PingOne. The first time you access the admin console, you must register a multi-factor authentication (MFA) method because MFA is required for access. After you sign on the first time, the **Environments** page displays a list of environments to which you have access. If you have the Organization Admin role, all the environments in your organization are listed. Subsequent sign-ons will take you to the admin console for the environment you last accessed.

Before you begin

Ensure that you:

- Are an administrator of a PingOne environment.
- Set the username for your PingOne administrator account as your email address.
- Verify your email address in PingOne.

To access the PingOne admin console home page:

Steps

1. Go to pingidentity.com and click **Sign On**.
2. Enter your email address and click **Continue**.
   - If this is your first time signing on from a browser, an email is sent to your email address with a verification link. Click the link to verify your email address.
   - If you have multiple administrator identities associated with the same email address, a list of environments associated with those identities across all regions displays. Select the environment that you want to access.

     > **Note**
     > Environments that have expired licenses are flagged in the list of your environments. To extend a license, contact Ping Identity Sales at https://www.pingidentity.com/en/company/contact-sales.html.
3. Follow the authentication steps for your environment.

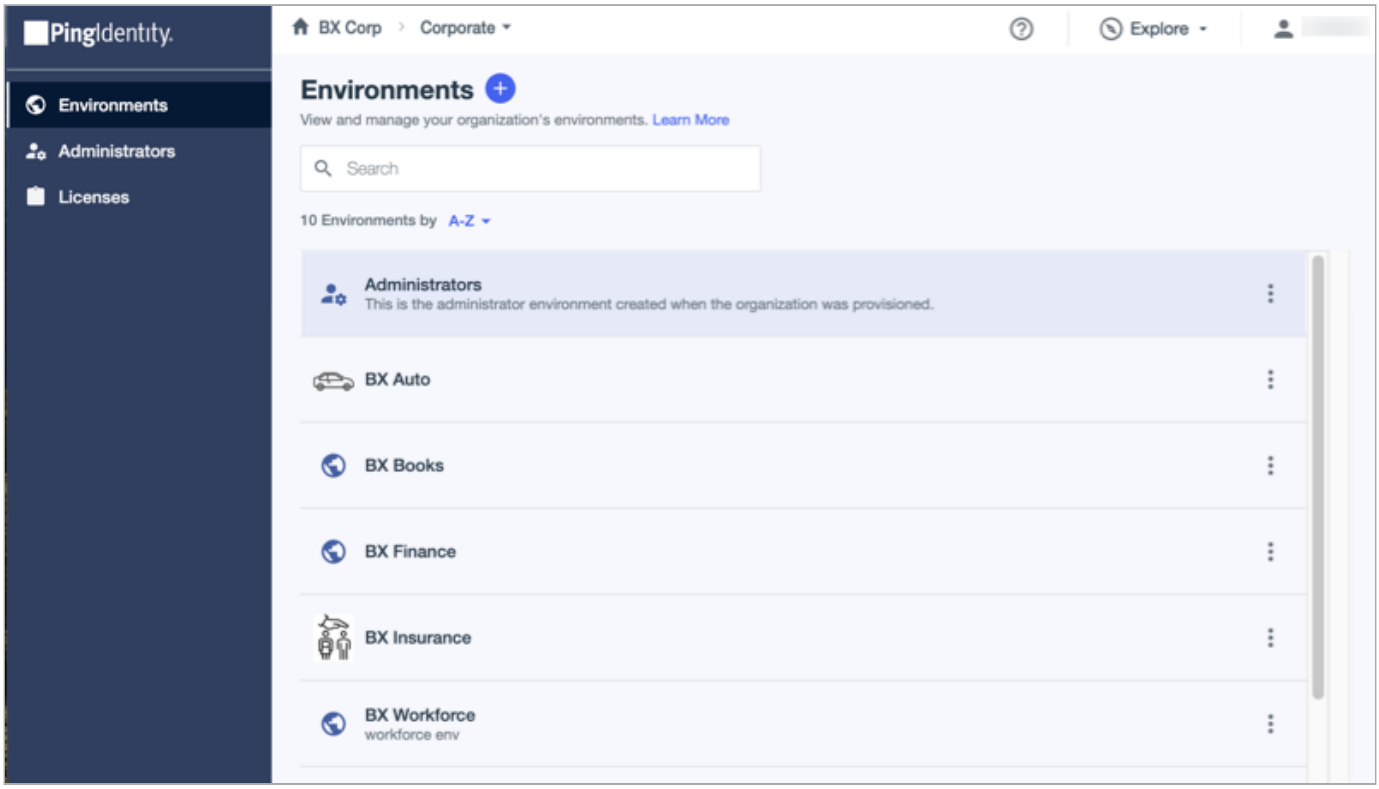
   If you are unable to sign on, contact your administrator for further assistance. You can also sign on using your direct console login URL. Learn more in Administrators: Managing your PingOne environment.

   > **Note**
   > Administrators must sign on again after 30 minutes of inactivity in the admin console. MFA is required if the last sign-on is older than 12 hours. These settings are not configurable.

   Result:

   The **Environments** page opens and lists the environments to which you have access. If this is your first time accessing this page, you're asked if you would like to take a quick tour of the admin console.

Copyright © 2025 Ping Identity Corporation



Starting a PingOne trial

Signing up for a 30-day free trial version is a great way to experience the power of PingOne for yourself.

About this task

Your trial organization includes:

- One trial license.
- Up to five environments in one region, including the Administrators environment, which is created when the new trial starts.
- An administrative user who has all the roles necessary to manage the organization and add other administrators.
- Up to 1000 active identities for the duration of the trial.

Even if you already have a PingOne license, you can still start a PingOne trial and evaluate the services available. Follow the appropriate set of instructions:

- Existing customers
- New customers

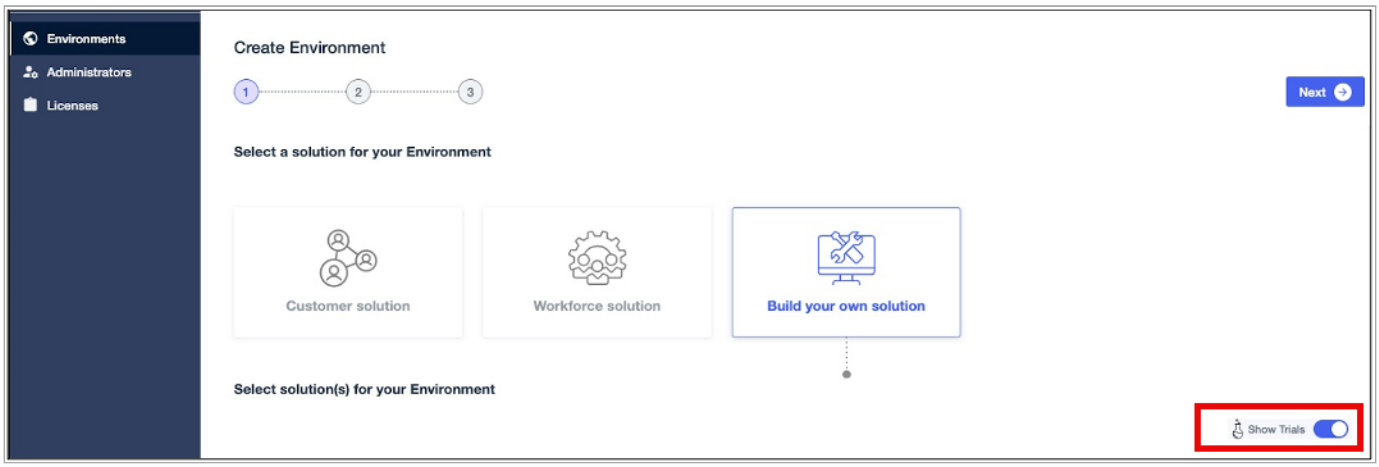
Existing customers

To sign up for the 30-day free trial, create a new PingOne environment in your organization and add the services that you want to evaluate.

Copyright © 2025 Ping Identity Corporation

Steps

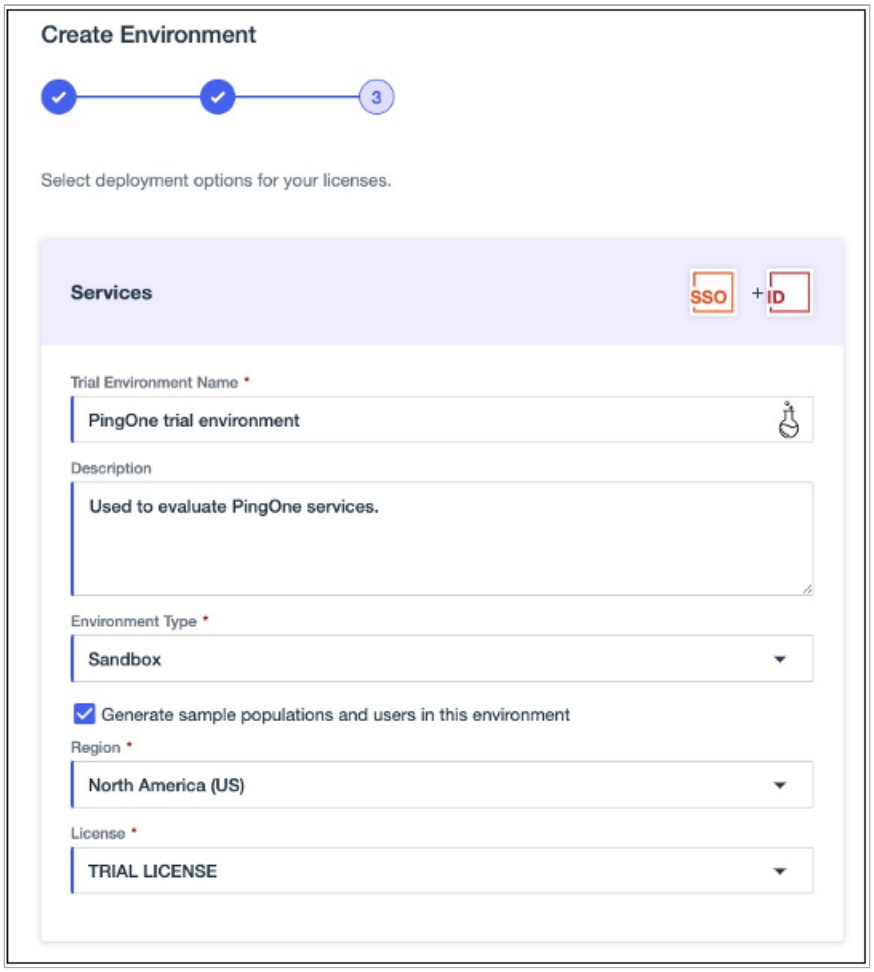
1. Sign on to your PingOne environment, access the **Environments** page, and click **+** to create a new environment.
2. On the **Create Environment** page, select the type of solution you want to build and click **Next**.
3. Ensure that the **Show Trials** toggle is on.



4. Select the services that you want to add to the environment and click **Next**.
5. Define your environment by entering the following:

Field	Description
Environment Name	A unique identifier for the environment.
Environment Description (optional)	A brief description of the environment.
Environment Type	Select **Sandbox**.
Generate sample populations and users in this environment	Select this checkbox to generate two populations and 40 sample users in the new environment.
Region	Select the region available in the list, which is determined by your PingOne organization.
License	Select **Create new trial license**.

Copyright © 2025 Ping Identity Corporation



6. Click **Finish**.

Result:

The new environment is created in your PingOne organization, and a new trial license is issued. The **Environments** page displays. You'll also be able to see the new license listed on the **Licenses** page.

New customers

To sign up for the 30-day free trial, provide your name, business email address, and verify it. You will receive access to a new PingOne organization and be prompted to sign on with the credentials you create during registration.

Steps

1. Go to pingidentity.com and click **Try Ping** on the right side of the page.

2. To activate your trial, check your email inbox and click **Verify Email** in the email sent to you.

Copyright © 2025 Ping Identity Corporation

3. Enter your first and last name, job title, and phone number in the appropriate fields. Note that you will be granted the Organization Admin role by default, which allows you to create, update, and delete environments and configure your organization to meet your needs.
4. Select the region available in the list, which is determined by your PingOne organization.

> **Important**
>
> PingOne data centers are available all over the world. For optimum performance, use the data center closest to your geographic region. Learn more in Organizations.

5. Create a password, select the checkbox to agree to the terms and conditions, and click **Start Trial**.
6. Enter the username and password you just created and click **Sign On**.
7. You're required to enroll in MFA to enhance your account security. Click **Continue**.
8. Select the MFA method that you want to use to authenticate:
   - **Email**: You'll provide your email address, receive an email with a passcode, and enter the passcode to sign on.
   - **Authenticator App**: You'll access the mobile authenticator app, receive a passcode, and enter the passcode to sign on.
   - **Passkey**: You'll create a passkey on your device using a biometric sensor or PIN and use that sensor or PIN to sign on.

Result:

After you complete the registration process, you'll be redirected to the **Environments** page, where you can begin creating identity solutions that meet your specific needs.

Next steps

Now, you can either add other administrators to the Administrators environment or create a new environment. Learn more in Managing administrators and Creating an environment.

Creating an environment

One of the first things you should do after you start a PingOne trial or purchase a PingOne license is to create an environment. A setup assistant guides you through this process.

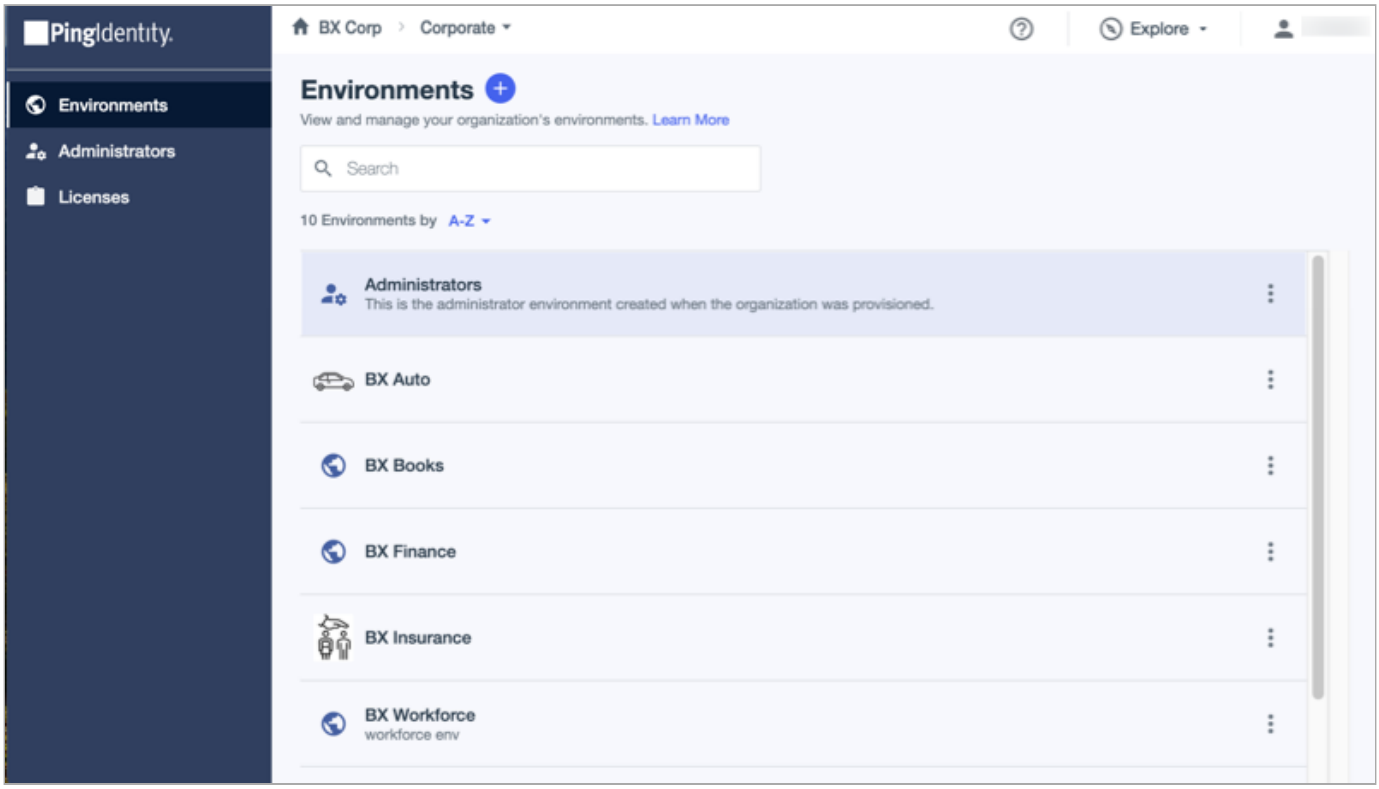
About this task

> **Note**
>
> You must have the Organization Admin role or a custom role with equivalent permissions to create an environment.

Steps

1. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page.
2. Click the **+** icon.

Copyright © 2025 Ping Identity Corporation

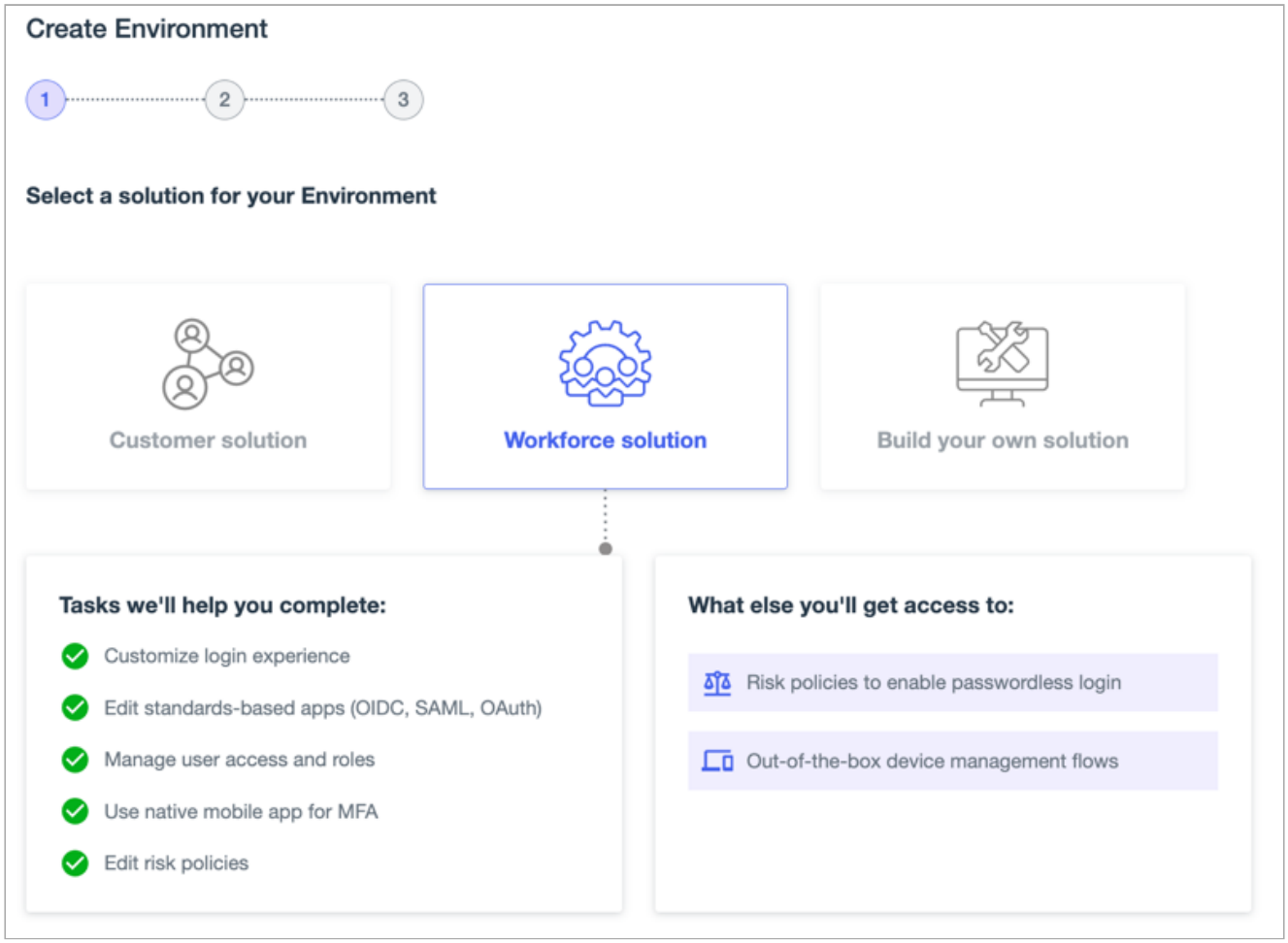


Result:

The **Create Environment** setup assistant starts.

3. Select the type of solution that you want to support in this environment.

Copyright © 2025 Ping Identity Corporation



Option	Description
Customer solution	Select to design registration and subsequent sign-on experiences for your customers and test them in a sample application tailored to your industry.
Workforce solution	Select to design single sign-on experiences for your employees, partners, and vendors.
Build your own solution	Select to choose from all of our services and products to build a hybrid solution that fits your unique use case.

4. Click **Next**.

   The services that will be deployed to your new environment are listed.

5. Click **Next**.

6. Define your environment by entering the following:

Copyright © 2025 Ping Identity Corporation

Field	Description
Environment Name	A unique identifier for the environment.
Description (optional)	A brief description of the environment.
Environment Type	Select **Sandbox** or **Production**. Sandbox environments are typically used for configuration and testing before deployment. Production environments are typically used for live configurations that are deployed for real-world use. Learn more about environment types in Sandbox and Production environments.
Generate sample populations and users in this environment	Select this checkbox to generate two populations and 40 sample users in the new environment.
Region	The appropriate geographical region for the environment. The list shows only regions that are included with your license. **Important** You can't change the region after the environment has been created.
License	Select the license to use for this environment. The available licenses for your organization are shown in the **License** list. For more information, see Licenses and Platform Limits.
Include a solution designer to easily design and test experiences (optional)	Customer and Workforce solutions only. If selected, after you create your environment, a solution designer opens and walks you through the process of designing your experiences.
Choose Your Industry (optional)	Customer solutions only. If you make a selection, PingOne creates a sample app tailored to the industry selected.

7. Click **Finish**.

Result

The new environment is created in your PingOne organization.

If you chose to build a customer or workforce solution, and selected the solution designer option, the solution designer opens and guides you through the process of designing and testing registration and sign-on experiences in less than 5 minutes.

If you did not select the solution designer option, or if you built your own solution, the **Environments** page opens. Locate your new environment by sorting the list alphabetically or by date created, or enter the environment name in the search box.

Building a customer solution

With your PingOne trial, you can quickly design registration and subsequent sign-on experiences for your customers and test them in a sample application tailored to your industry.

Copyright © 2025 Ping Identity Corporation

Steps

1. Click **Get Started**, either from the message you receive after creating your environment or from the top of the page.
2. On the **Welcome** page, click **Create a Customer Solution**.
3. On the **Tailor your experiences** page, select the industry to model the solution for, or click **Skip** to design experiences that can be used in any industry.

   Available industries include:

   - **Retail**
   - **Financial Services**
   - **Manufacturing**
   - **Healthcare**
   - **Education**
   - **Government**
   - **Realty**
   - **Pharmacy**
   - **Airline**
   - **Hotels**

   Result:

   You see a sample application in the middle of the page and the solution designer on the left side of the page.

Next steps

Create a registration experience for the application.

Copyright © 2025 Ping Identity Corporation

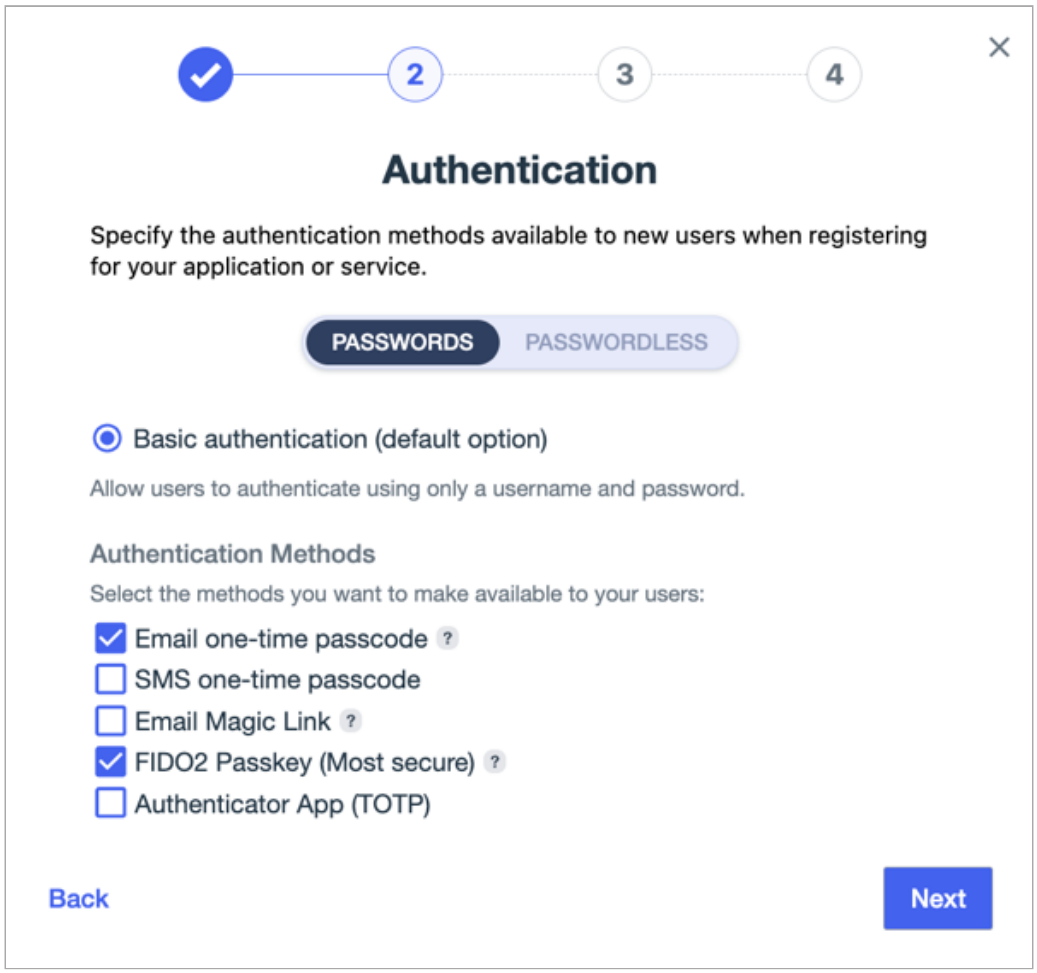
Passwords

Creating a registration experience that uses passwords
About this task

In a registration experience that uses passwords, users sign on using a password, possibly also using multi-factor authentication (MFA).

Steps

1. Click **Passwords** on the toggle at the top of the **Select your registration experience** window.



2. (Optional) Select **Require MFA** to require users to enroll in MFA during registration.

   If you do not select this option, users can enroll in MFA later.

3. (Optional) Select **Include terms of service agreement** to require users to consent to an agreement before creating an account.

4. Click **Next**.

5. Select the MFA methods you want to support for users.

Copyright © 2025 Ping Identity Corporation

Choose from:

- **Email one-time passcode**: User receives a one-time passcode (OTP) at the email address entered during registration. The user can also enter a second email address for MFA.
- **SMS one-time passcode**: The user receives an OTP at the mobile phone number entered during registration.
- **Email Magic Link**: The user receives a link for sign on at the email address entered during registration.
- **FIDO2 Passkey (Most secure)**: The user can register a FIDO2-compliant MFA method, such as biometrics, for authentication.
- **Authenticator App (TOTP)**: The user receives a prompt sent to a supported authenticator app, such as Google Authenticator.

> **Note**
>
> If any of these options aren't enabled, they aren't supported by your default MFA policy. Edit the policy to include the options you want to enable. Learn more in MFA policies.

6. Click **Next**.
7. Follow the instructions for the profile management and account recovery steps in the setup assistant.

   Result:

   You receive a notification when your registration experience is ready to test.

8. On your sample application, test the registration experience that you designed by clicking **Sign up**.

   Result:

   You've run a DaVinci flow to create a new user in your environment and validated that they are able to sign on.

9. To test the sign-on experience that you designed, click **Sign On** using the credentials of the user that you created.

> **Note**
>
> If you don't currently have access to PingOne DaVinci and you're ready to explore its potential, click **Learn about DaVinci** in the solution designer sidebar in the **Orchestrate & Integrate** section. You can also click **Request DaVinci** to complete a form and connect with a Sales representative who can enable DaVinci access for your trial environment.

Copyright © 2025 Ping Identity Corporation

Passwordless

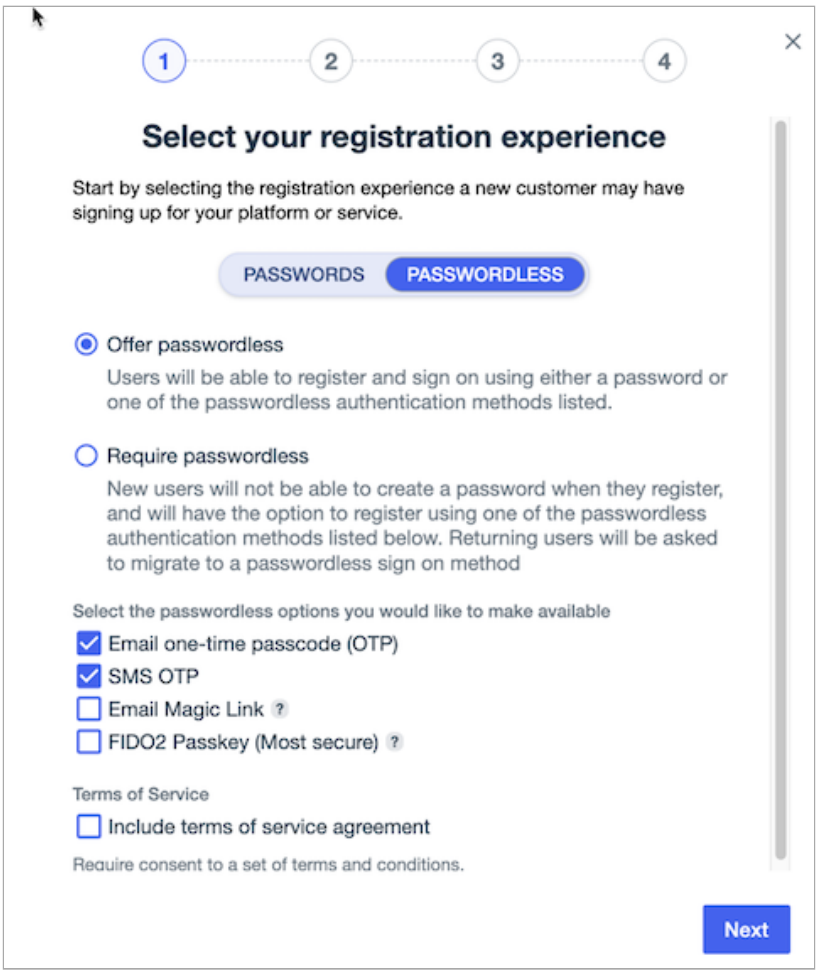
Creating a passwordless registration experience
About this task

In a passwordless registration experience, users sign on using their device, one-time passcode (OTP), biometrics, or other options. Passwords can be permitted as well depending on environment settings.

> **Note**
>
> Learn more about our passwordless solution in PingOne for Customers Passwordless.

Steps

1. Click **Passwordless** on the toggle at the top of the **Select your registration experience** window.



2. Select a passwordless registration option.

   Choose from:

   - **Offer passwordless**: Existing users can sign on with passwords but are prompted to add a non-password authentication method. New users automatically use passwordless authentication.
   - **Require passwordless**: All users must use passwordless authentication.

3. Select one or more methods for passwordless authentication.

Copyright © 2025 Ping Identity Corporation

4. (Optional) Select **Include terms of service agreement** to require users to consent to an agreement before creating an account.
5. Follow the instructions for the profile management and account recovery steps in the setup assistant.

   Result:

   You receive a notification when your registration experience is ready to test.
6. On your sample application, test the registration experience that you designed by clicking **Sign up**.

   Result:

   You've run a DaVinci flow to create a new user in your environment and validated that they are able to sign on.
7. To test the sign-on experience that you designed, click **Sign On** using the credentials of the user that you created.
8. To modify these experiences, select different options in the solution designer and continue to test them in your sample application until you're satisfied.
9. Continue to explore and customize your PingOne trial.

   You can update user information, password policies, and agreements using the solution designer.

   > **Note**
   >
   > If you don't currently have access to PingOne DaVinci and you're ready to explore its power, click the **Try DaVinci** link at the bottom of the solution designer on the left side of the page.

Building a workforce solution

With your PingOne trial, you can quickly design single sign-on experiences for your employees, partners, and vendors.

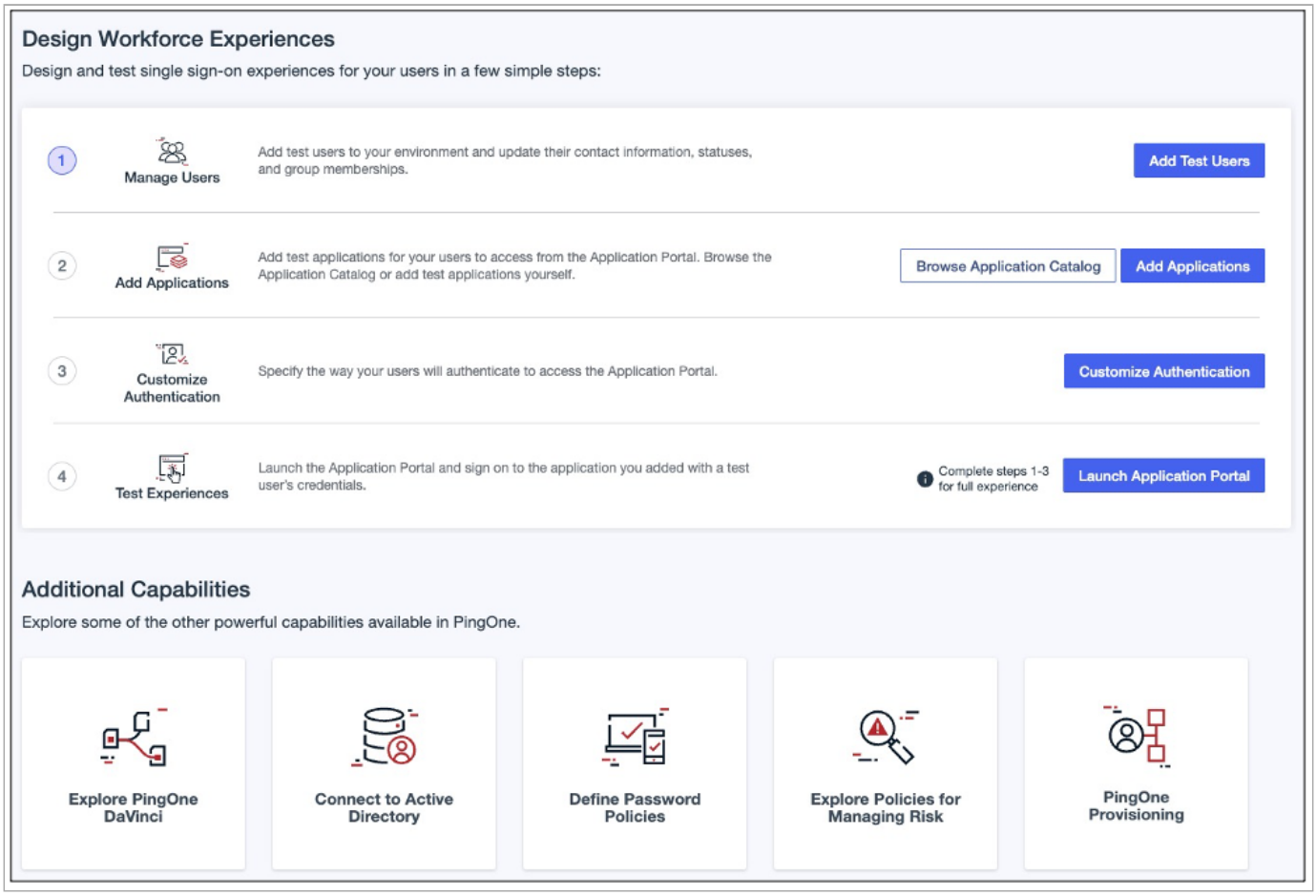
About this task

After creating a new workforce environment, the solution designer opens, which will walk you through the process of designing your experiences. To return to the designer in the future, click **Get Started** at the top of the page.

Steps

1. The solution designer outlines the steps involved in this process. Start by clicking **Add Test Users** to add test users to your environment.

Copyright © 2025 Ping Identity Corporation



The **Add Users** page opens. If you chose to have PingOne generate test users and populations to your environment, you'll see them listed on this page.

Follow the steps outlined in the online guide to add a test user to the environment.

2. On the second step, you can browse the Application Catalog to see which applications are available in the environment or click **Add Applications** to add a new application to the environment. An online guide walks you through the process.

3. On the third step, select the type of authentication experience you want your users to have when they sign on to your application or service for the first time and click **Save**.

   Choose between:

   - **User name and password**: Require your users register with a username and password.
   - **Username, password, and MFA with the PingID app**: Requires users to provide their username, password, and additional verification through the PingID app.
   - **Risk-based MFA**: Requires users to provide their username and password, and an additional verification factor if risk signals are detected.
   - **Passwordless - FIDO2 (Biometrics, Security Keys)**: Transition to passwordless authentication. Requires users to initially provide their usernames and passwords and authenticate with MFA. Then, they can register devices to enable biometric or security key authentication.

Copyright © 2025 Ping Identity Corporation

4. To test the user sign-on experience, click **Launch Application Portal** and sign on to the application with a test user's credentials.
5. To modify these experiences, select different options in the solution designer and continue to test them until you're satisfied.
6. Continue to explore and customize your PingOne workforce trial, and explore the additional capabilities highlighted at the bottom of the page.

Building solutions

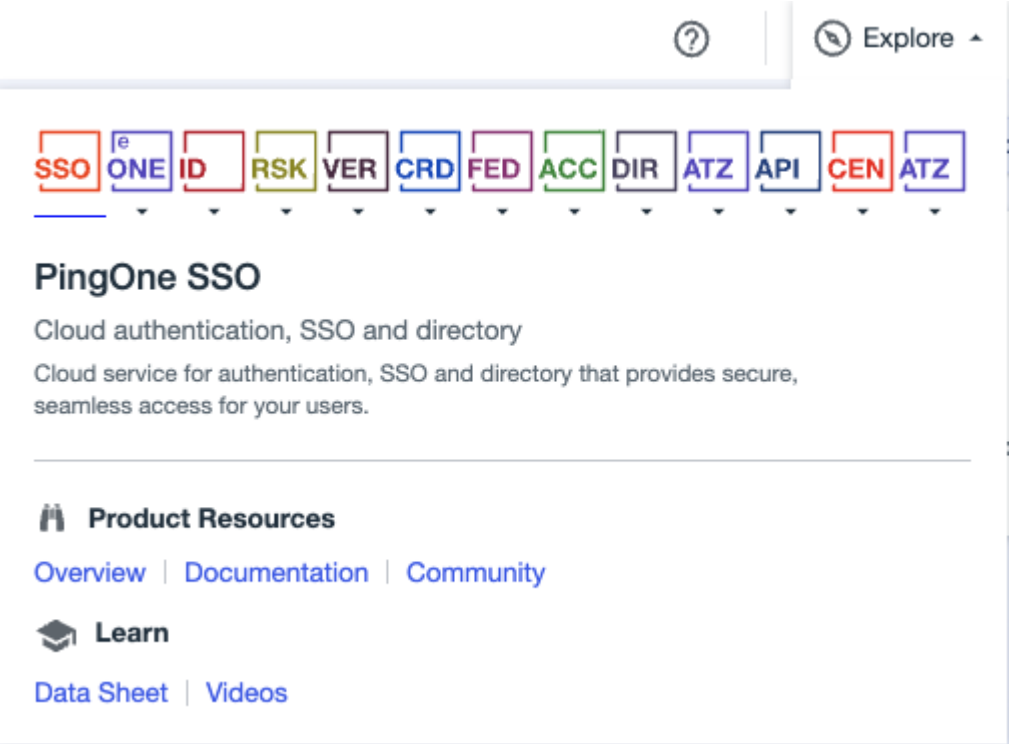
If you have an organization administrator role, you can build powerful identity solutions in minutes. Choose one of the packaged solutions or build your own.

Regardless of whether your solution includes one software product, one service, or a collection of products and services, wizards guide you through the process of creating new environments for the products and services you select, and instructions are provided for deploying each component.

See the following topics:

- Adding environments
- Deploying products and services

For descriptions of each product and service available, click the **Explore** tab. Select a product or service icon to review its description and to access documentation, APIs, code examples, data sheets, and videos for that product or service.



Adding environments

The first step in building an identity solution is adding an environment to organize your Ping products and services.

Copyright © 2025 Ping Identity Corporation

Before you begin

Determine what type of solution you're building. Filter the products and services by the type of audience you serve with your identity and access management solution:

Customer solutions

Help you create sign-on experiences for your clients and consumers. Products and services relevant to serving your clients and consumers are added to the environment.

Workforce solutions

Help you create sign-on experiences for your organization's employees. Products and services relevant to serving your employees and partners are added to the environment.

Build your own solution

Allows you to build a hybrid solution by selecting from all available products and services.

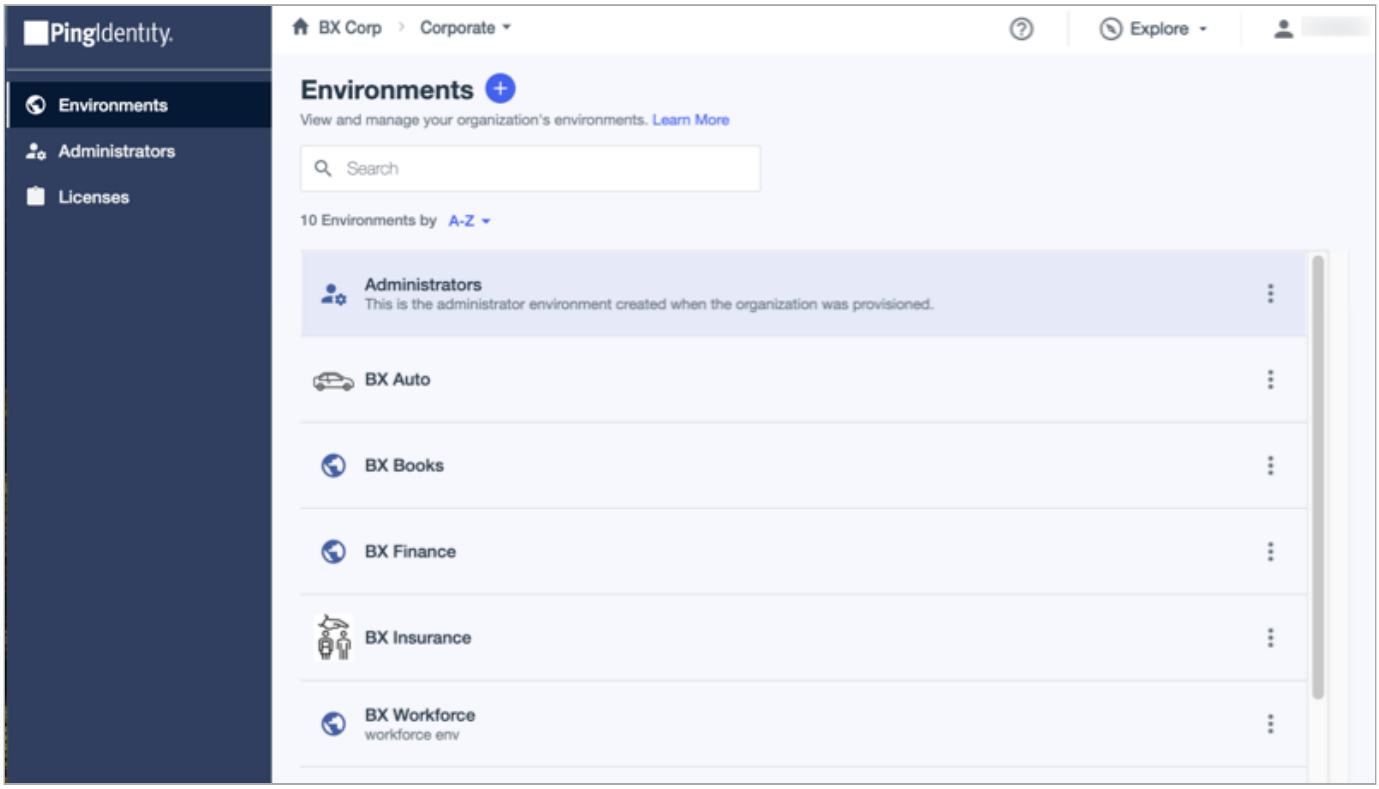
> **Important**
>
> When you select **Customer solution** or **Workforce solution**, a combination of preselected services designed to support your customer or workforce use cases is added to the environment. If your license does not cover the services that are included, you can select **Build your own solution** to select other available products and services.

When you select a solution, you might also want to consider how you want that solution to be deployed. PingOne for Enterprise and PingOne are multi-tenant cloud solutions that do not require additional setup or deployment after the environment in which they reside is created.

Steps

1. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page.
2. Click the **+** icon.

Copyright © 2025 Ping Identity Corporation



Result:

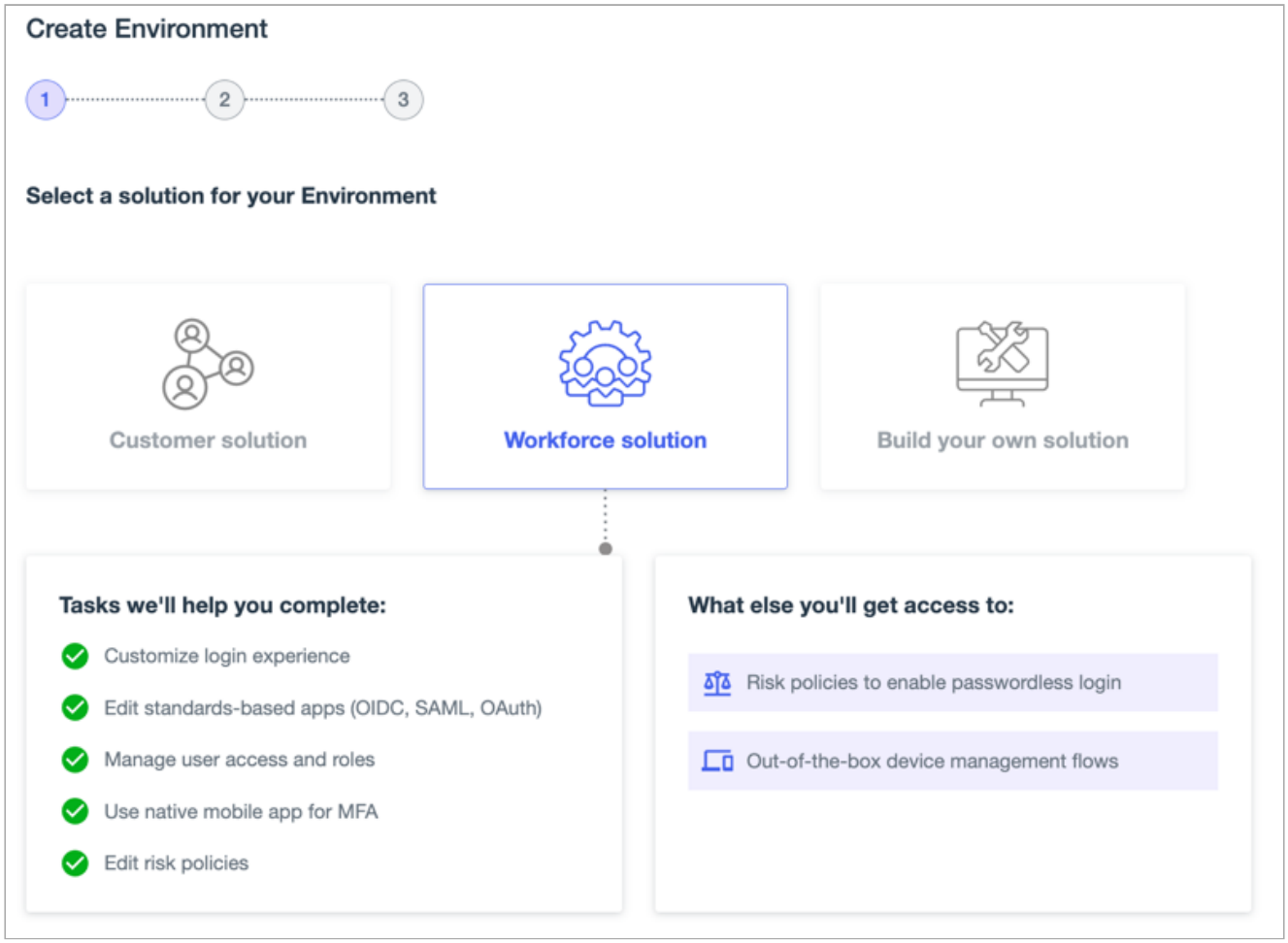
The **Create Environment** setup assistant starts.

3. To indicate whether you are building a customer solution, workforce solution, or custom solution, select the appropriate option.

   Result:

   Create Environment lists the main tasks that can be completed using the solution type.

Copyright © 2025 Ping Identity Corporation



4. Click **Next**.

   The services that will be deployed to your new environment are listed.

5. To add or remove them from your solution, select and deselect products and services as necessary, then click **Next**.

   Many of your selections are deployed automatically, but you might be asked how to deploy a connected product. Answer the questions to the best of your ability. You can change them later.

6. Define your environment by entering the following:

Field	Description
Environment Name	A unique identifier for the environment.
Description (optional)	A brief description of the environment.
Environment Type	Select **Sandbox** or **Production**. Sandbox environments are typically used for configuration and testing before deployment. Production environments are typically used for live configurations that are deployed for real-world use. Learn more about environment types in Sandbox and Production environments.

Copyright © 2025 Ping Identity Corporation

Field	Description
Generate sample populations and users in this environment	Select this checkbox to generate two populations and 40 sample users in the new environment.
Region	The appropriate geographical region for the environment. The list shows only regions that are included with your license. **Important** You can't change the region after the environment has been created.
License	Select the license to use for this environment. The available licenses for your organization are shown in the **License** list. For more information, see Licenses and Platform Limits.
Include a solution designer to easily design and test experiences (optional)	Customer and Workforce solutions only. If selected, after you create your environment, a solution designer opens and walks you through the process of designing your experiences.
Choose Your Industry (optional)	Customer solutions only. If you make a selection, PingOne creates a sample app tailored to the industry selected.

Result

The new environment is created in your PingOne organization.

If you chose to build a customer or workforce solution, and selected the solution designer option, the solution designer opens and guides you through the process of designing and testing registration and sign-on experiences in less than 5 minutes.

If you did not select the solution designer option, or if you built your own solution, the **Environments** page opens. Locate your new environment by sorting the list alphabetically or by date created, or enter the environment name in the search box.

Next steps

Deploy your solution. Learn more in Deploying products and services.

Deploying products and services

After creating an environment for your Ping products and services, set up the products and services.

Steps

1. On the **Environments** page, select the environment that you just created.

   Result:

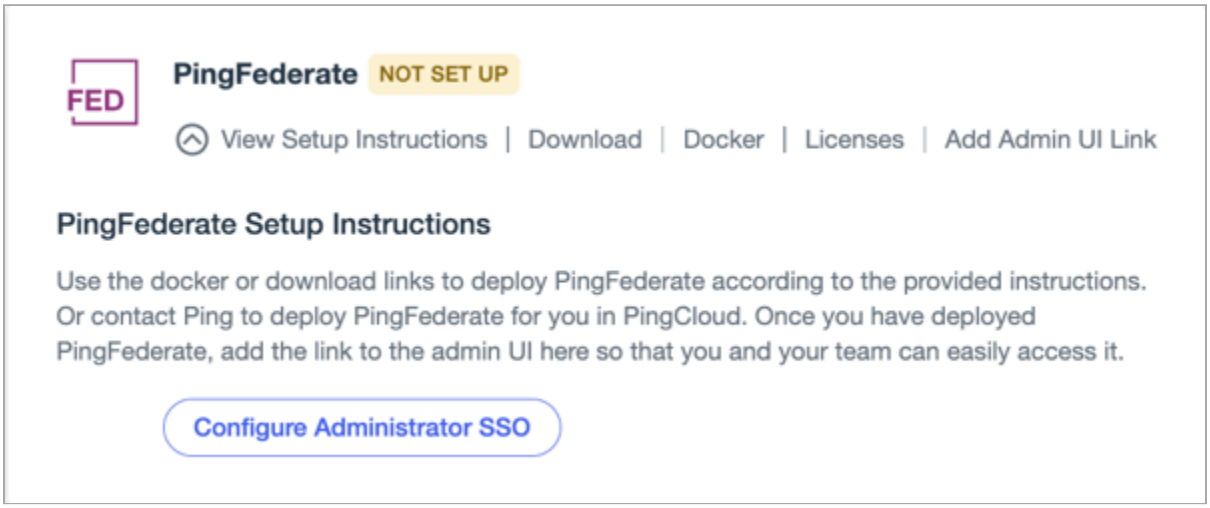
   The environment details pane opens and lists the products and services that are included in the environment, along with details such as the environment ID, environment type, URLs for the environment, license information, and so on. If setup is incomplete for a product, it's grayed out, and a tooltip indicates that configuration is needed.

2. Click **Manage Environment** to go to the **Overview** page for the environment.

Copyright © 2025 Ping Identity Corporation

3. In the **Services** section, locate the service that requires configuration, expand **View Setup Instructions**, and complete the setup.

   The ways in which you set up products and services vary. The following example displays the instructions for setting up PingFederate.



   Cloud software products are most easily deployed using Docker images, so click the **Docker** link and complete the appropriate steps. Learn more about deploying Ping products using Docker on the Ping Identity DevOps site.

   > **Note**
   >
   > - PingOne for Enterprise and PingOne services do not require additional setup or deployment after the environment in which they reside is created. PingOne for Enterprise environments are created as part of the procurement process or can be created in a trial using the sign up link.
   > - PingOne services are deployed automatically based on what is selected when the environment is added.
   > - When you add other Ping products to your environment, you can set up single sign-on and centralize management through PingOne.

Managing administrators

If you use PingOne as your identity provider, have administrator security enabled with PingOne or a hybrid authentication source, and you have the appropriate permissions, you can invite other administrators to register for PingOne.

Or, if you're an administrator with the appropriate permissions, you can add new administrators yourself and define their permissions using roles.

Complete the appropriate set of steps:

- Inviting administrators to register
  - Accepting the administrator account registration invitation
- Adding administrators
  - Completing the administrator account registration

Copyright © 2025 Ping Identity Corporation

> **Note**
> To prevent privilege escalation, you cannot create an administrator user if you do not have administrator privileges.

Inviting administrators to register

You can invite administrators to register with PingOne using their name and email address. These users receive an email containing a verification code, as well as a link to complete the registration process.

You can also set an expiration time on the invitation. The maximum time allowed is 24 hours.

Before you begin

To invite other administrators to access PingOne, you must use PingOne as your identity provider, have administrator security enabled with PingOne or a hybrid authentication source, and have the appropriate permissions.

Steps

1. In the PingOne admin console for the Administrators environment, go to **Directory > Users** and select **Invite Admin** from the **Users** list.
2. Enter the user's email address and first and last name in the appropriate fields.
3. Specify when you want the invitation to expire in the **Invitation Expires** field and click **Next**.
4. On the **Available responsibilities** tab, select the administrator roles you want the new administrator to have for each environment, such as **Environment Admin**, **Identity Data Admin**, or **Organization Admin**.

   > **Note**
   > You cannot assign privileges greater than those you are assigned. Best practice is to assign only the roles necessary for new administrators to do their jobs. Learn more in Administrator Roles and Managing user roles.

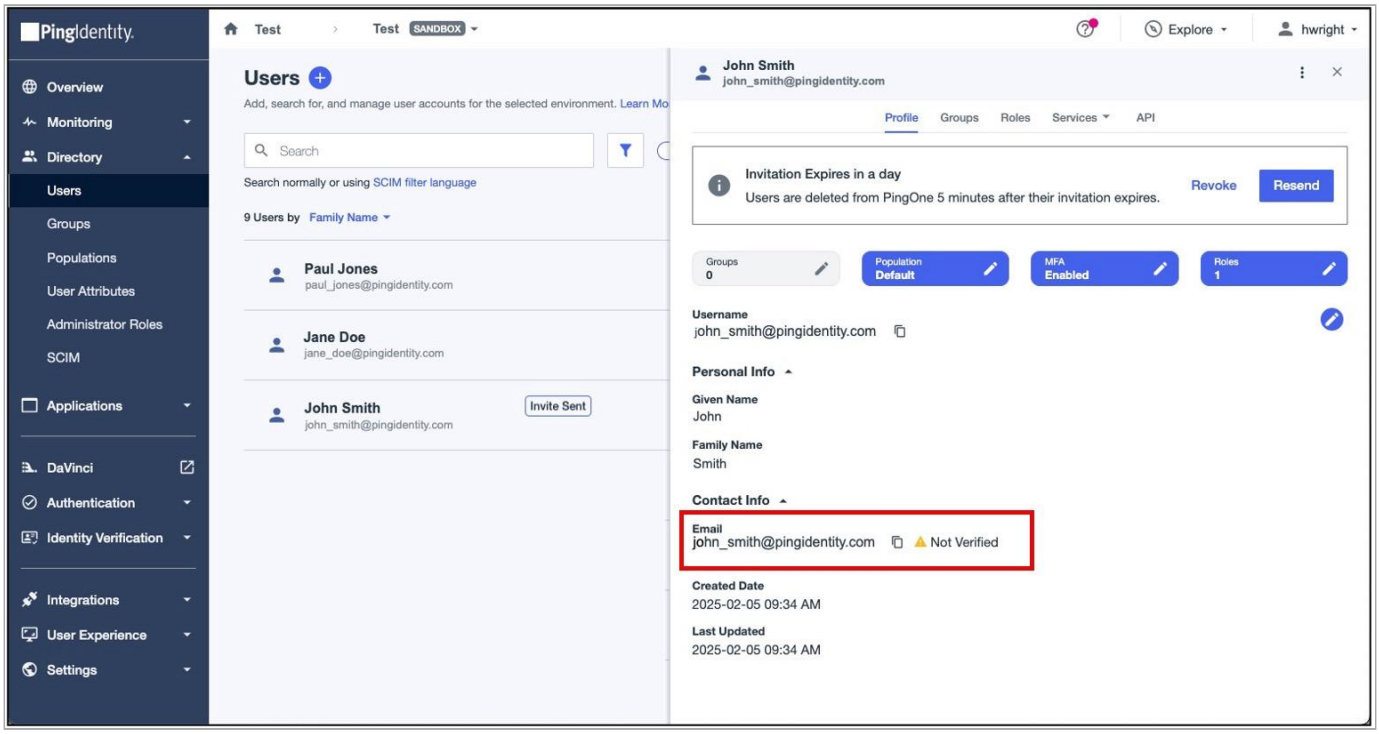
5. Click **Send Invitation**.

   Invitations display on the **Users** page. The toggle indicates whether the invitation is still active. Click the user to view details about the invitation.

6. (Optional) If you want to revoke the invitation or resend it with a new authentication code, click **Revoke** or **Resend**.

   > **Note**
   > The administrator's email address is not yet verified, but will be when the administrator accepts the invitation.

Copyright © 2025 Ping Identity Corporation



Next steps

The new administrator accepts the invitation and signs on to the admin console.

Accepting the administrator account registration invitation

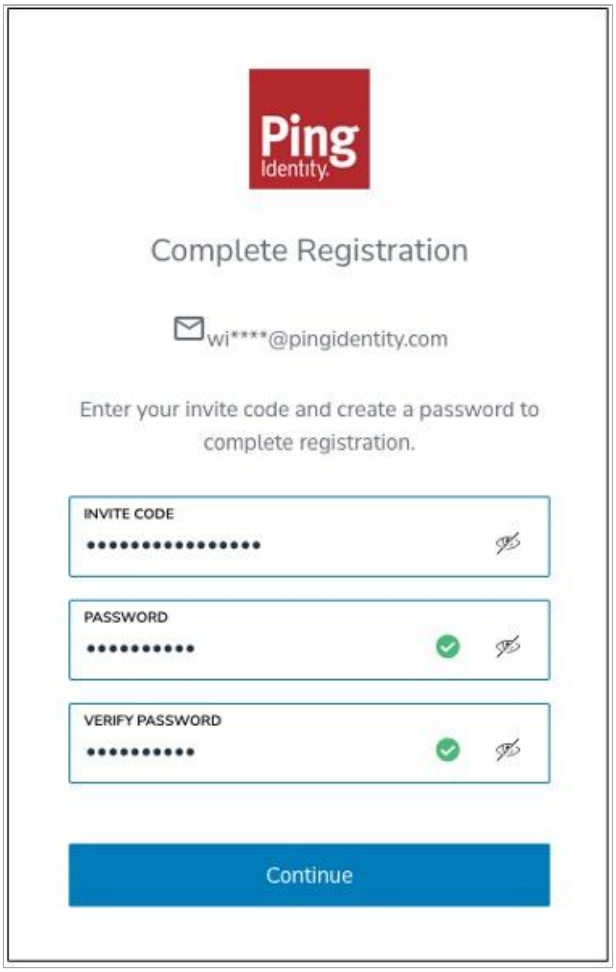
When you receive an email indicating that you were added as an administrator in PingOne, copy the invite code and paste it into PingOne to complete the registration process.

Steps

1. Click **Complete Registration** on the email you received.
2. On the sign-on page, enter your PingOne username.
3. Click the **Complete Registration** button.
4. Copy the invite code from the email and paste it into the **Invite Code** field.

> **Warning**
>
> If you enter an incorrect invite code five times, you will be locked out of the account and the invitation will need to be sent again.

Copyright © 2025 Ping Identity Corporation



5. Enter and verify a new password for the account and click **Continue**.

   Result:

   You are signed on to the PingOne admin console.

Adding administrators

You can designate an existing user as an administrator or create a new administrator user.

> **Note**
> To prevent privilege escalation, you cannot create an administrator user if you do not have administrator privileges.

Steps

1. In the Administrators environment, go to **Directory** > **Users** and browse or search for the user you that want to make an administrator.

   > **Note**
   > To create a new user with administrator privileges, click the **+** icon. Learn more in Adding a user. All administrator users should be maintained in the Administrators environment.

Copyright © 2025 Ping Identity Corporation

2. Click the user entry to open the user details panel.
3. On the **Roles > Administrator Roles** tab, click **Grant roles**.
4. Select an administrator role, such as **Environment Admin**, **Identity Data Admin**, or **Organization Admin**.

> **Note**
> You cannot assign privileges greater than those you are assigned. When you are determining which role to assign, consider the role that has the minimum permissions necessary for the administrator to perform their job responsibilities. Scope that role according to the levels at which the administrator should have this access. Learn more in Administrator Roles and Managing user roles.

5. Click **Save**.
6. On the **Profile** tab, click **Verify** to send a verification email to the user.

> **Note**
> All administrator users must verify their email address.

7. Go to **Settings > Environment Properties** and copy the **Console Login URL**.
8. Contact the new administrator and provide them with the following:
    - Their PingOne user name, if different from their email address.
    - The **Console Login URL** from the previous step.
    - (Optional) A temporary password for the console (if you set one up when you created the user).
    - The instructions for Completing the administrator account registration

Next steps

The new administrator completes their account registration.

Completing the administrator account registration

When you receive an email indicating that you were added as an administrator in PingOne, verify your email address and update your password to complete the registration process.

Before you begin

You should have received the following information from the PingOne administrator who added you as an administrator:

- Your PingOne user name if it is different from your email address.
- The **Console Login URL** for the environment that you are being added to.
- (Optional) A temporary password.

Steps

1. Go to the PingOne console using the URL you received from the administrator.

Copyright © 2025 Ping Identity Corporation

2. Enter your PingOne **Username**.
3. Update your **Password**.

   Choose from:

   - If you received a temporary password, enter it and create a new password when prompted.
   - Click **Forgot Password**, enter your PingOne username on the **Password Reset** window, and click **Submit**.

     An email containing a recovery code is sent to the email address associated with your PingOne user account. Paste the code where indicated on the **Enter New Password** window. Create a new password and click **Save**.

     Result:

   You are signed on to the PingOne administrator console.
4. On **Verify Email Address**, click **Verify**.

   Result:

   A new verification code is sent to your email address.
5. Paste the verification code where indicated and click **Confirm**.

Result

Your administrator account registration is complete.

Managing administrator roles

You can assign built-in or custom administrator roles to individual users or to groups.

> **Important**
>
> Learn more about built-in roles and creating and managing custom roles in Administrator Roles and Custom role scenarios before you start assigning roles to administrators.

Managing roles individually

About this task

Use the **Users** page to add roles to a user.

Steps

1. In PingOne, go to the **Administrators** environment.

   > **Note**
   >
   > Older organizations might not have an **Administrators** environment by default. To separate administrators from end users and improve security posture, you should manage all administrators in their own environment.
2. Go to **Directory → Users** and browse or search for the user that you want to edit.
3. Browse for an existing user or create a new one.

Copyright © 2025 Ping Identity Corporation

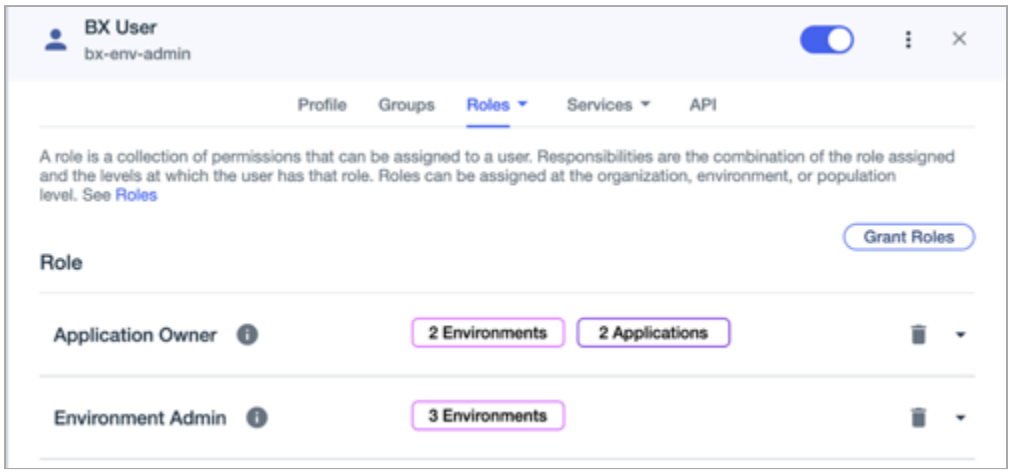
Learn more in Adding a user.

4. Click the user entry to open the user details panel.

5. Click the **Roles** > **Administrator Roles** tab.

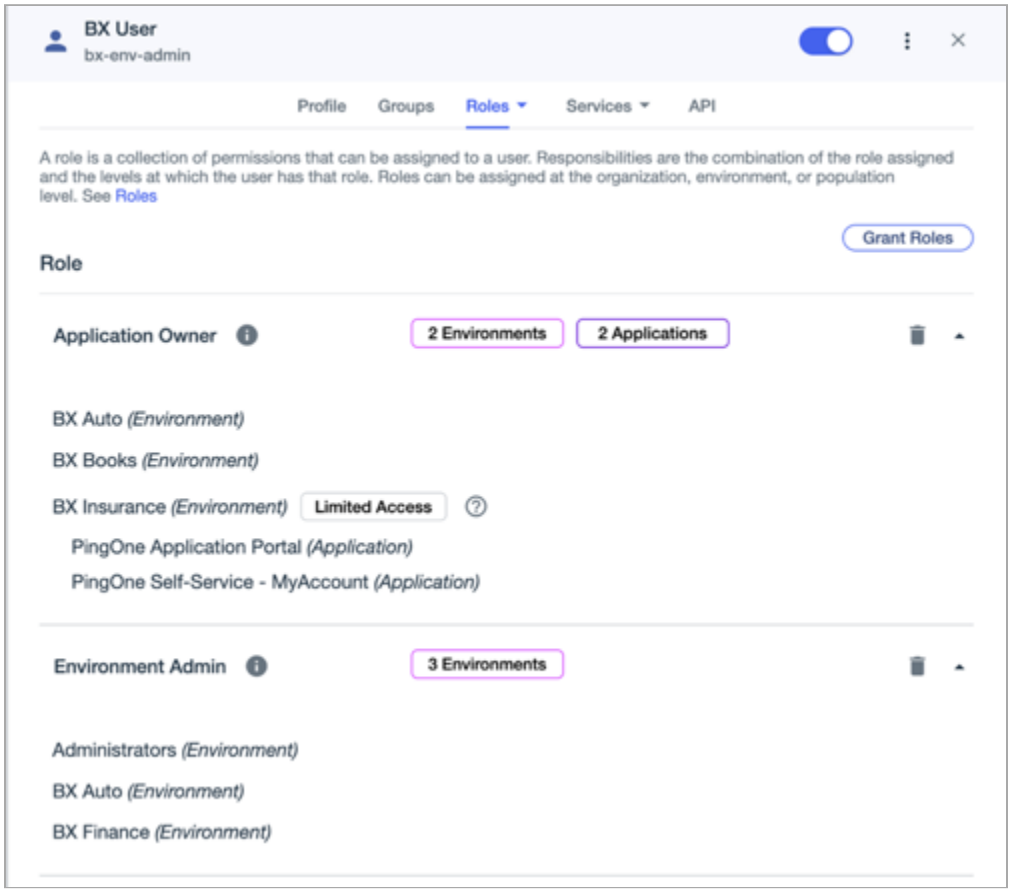
   If roles are assigned, they're listed here with information about where those roles apply. For example, in the following image, **BX User** has the **Application Owner** role in two environments. Because the role is assigned at the environment level, they have the role over all of the applications in those environments. In a third environment, they have the role over only two applications. They also have the **Environment Admin** role, and they have that role in three environments.

> **Note**
>
> You can assign administrator roles to users, groups, applications, or PingFederate gateway integrations.



> **Tip**
>
> Click the **Info** icon to view the permissions associated with the role. Click the down arrow on the right to view the list of environments or populations for which the role is assigned.

Copyright © 2025 Ping Identity Corporation



6. Click **Grant Roles**.

   The **Available Responsibilities** tab lists the roles that you are allowed to assign and the environments for which you are allowed to assign them. A responsibility is the combination of the role assignment and the level, or scope, at which the role is applied. Depending on the role, it could be assigned at the organization, environment, population, or application level.

   The **Granted Responsibilities** tab lists any roles that are currently assigned.

7. On the **Available Responsibilities** tab, click the role that you want to assign or change and perform any combination of the following:

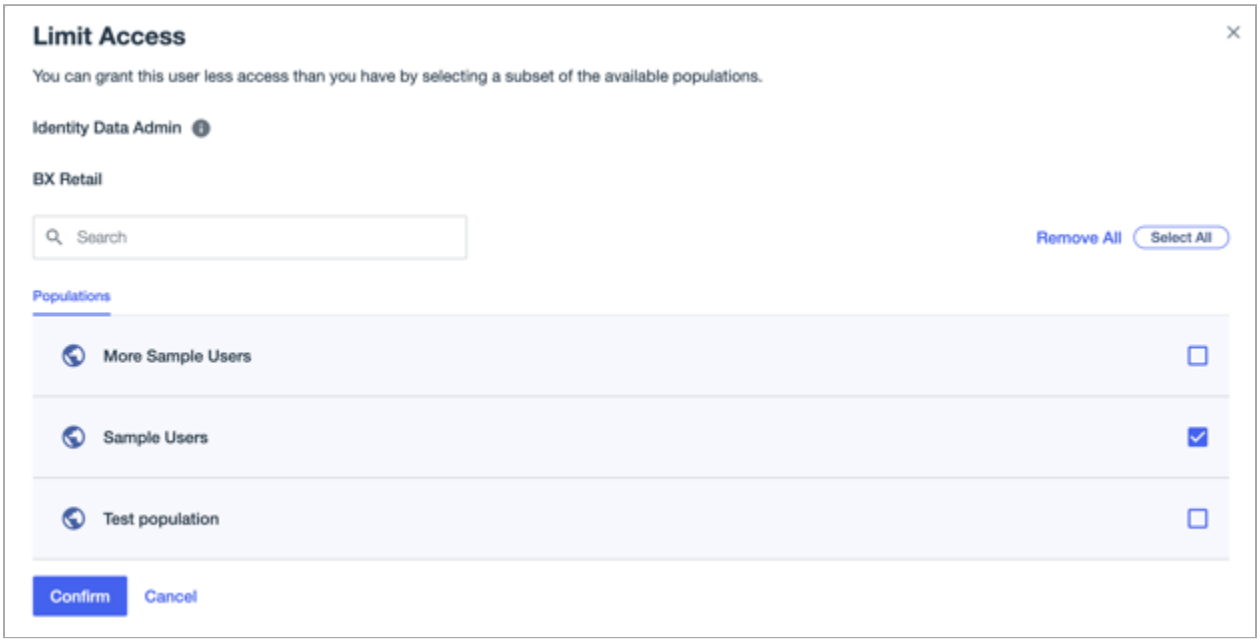
   1. To assign the role, select the checkboxes next to the applicable environments.

      > **Tip**
      >
      > Click **Select All** or **Remove All** to select or clear all available responsibilities.

   2. To remove a role assignment, clear the checkboxes next to the applicable environments.

   3. To grant this access for only a portion of the environment, click the **Reduce Access** icon ( ), select a subset of the available applications or populations on the **Limit Access** page, and click **Confirm**.

Copyright © 2025 Ping Identity Corporation



> **Note**
>
> You can grant only roles that are assigned to you or that confer the permissions needed to assign that role to others. For example, if you do not have the Environment Admin role, you cannot assign the Environment Admin role to others (and that role will not be listed under **Available Responsibilities**). However, if you have the Identity Data Admin role, you can assign either the Identity Data Admin role or the Identity Data Read Only role to others.
> Learn more about the permissions associated with each role in Roles.

8. Click **Save**.

Result

The role assignments that you selected are listed on the **Granted Responsibilities** tab.

Managing roles using groups

Use the **Groups** page to add roles to a group.

Assigning roles to groups allows you to:

- Manage roles for multiple users at once.
- Apply role changes in bulk.
- See users that have a certain role by viewing group members.

For security reasons, only static groups can have roles assigned to them. That is, you can't assign roles to groups that have members included based on a filter or rule. With a dynamic group, you might inadvertently add users to the group that would inherit role assignments. For more information, see Static and dynamic groups.

When adding users to groups that have roles assigned, be careful not to inadvertently assign a role to a user by adding them to a group. If a user has a role from being in a group, remove the user from the group to remove the role. If a user has a role assigned to them individually, you can remove the role from the user.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> - You can assign only roles that are assigned to you, or that are assignable by those roles. For example, the Identity Data Admin role has permissions that allow it to assign the Identity Data Admin Read Only role. Therefore, if you are assigned the Identity Data Admin role, you can assign that role or the Identity Data Admin Read Only role to a group.
> - An admin might not have permissions to assign roles but can add or remove users from a group that has role assignments. In other words, one admin can assign roles to a group, and a different admin can add or remove users from that group.
> - You cannot assign roles to a group that you are a member of.
> - You cannot add or remove yourself from a group that has roles assigned to it.
> - Roles assigned to a group will not affect roles that are assigned to a user individually.
> - You can assign roles in up to 500 groups.

Managing group roles

About this task

Assign roles to groups of administrators using the **Groups** page.

Steps

1. In PingOne, go to the **Administrators** environment.

   > **Note**
   >
   > Older organizations might not have an Administrators environment by default. We recommend that you manage all administrators in their own environment to separate administrators from end users and improve security posture.

2. Go to **Directory > Groups**.

3. Browse for an existing group or create a new one. Learn more in Creating a group.

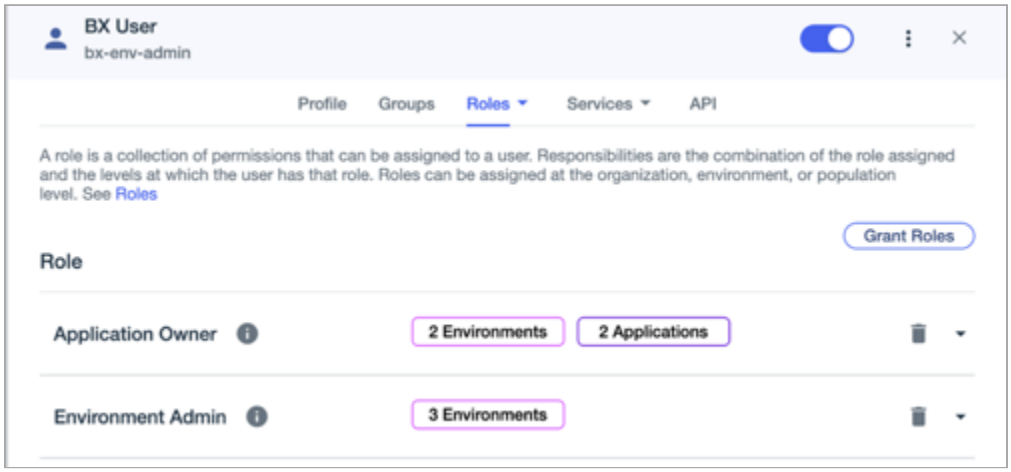
4. Click the group entry to open the details panel.

5. Click the **Roles** > **Administrator Roles** tab.

   If roles are assigned, they're listed here with information about where those roles apply. For example, in the following image, **BX User** has the **Application Owner** role in two environments. Because the role is assigned at the environment level, they have the role over all of the applications in those environments. In a third environment, they have the role over only two applications. They also have the **Environment Admin** role, and they have that role in three environments.

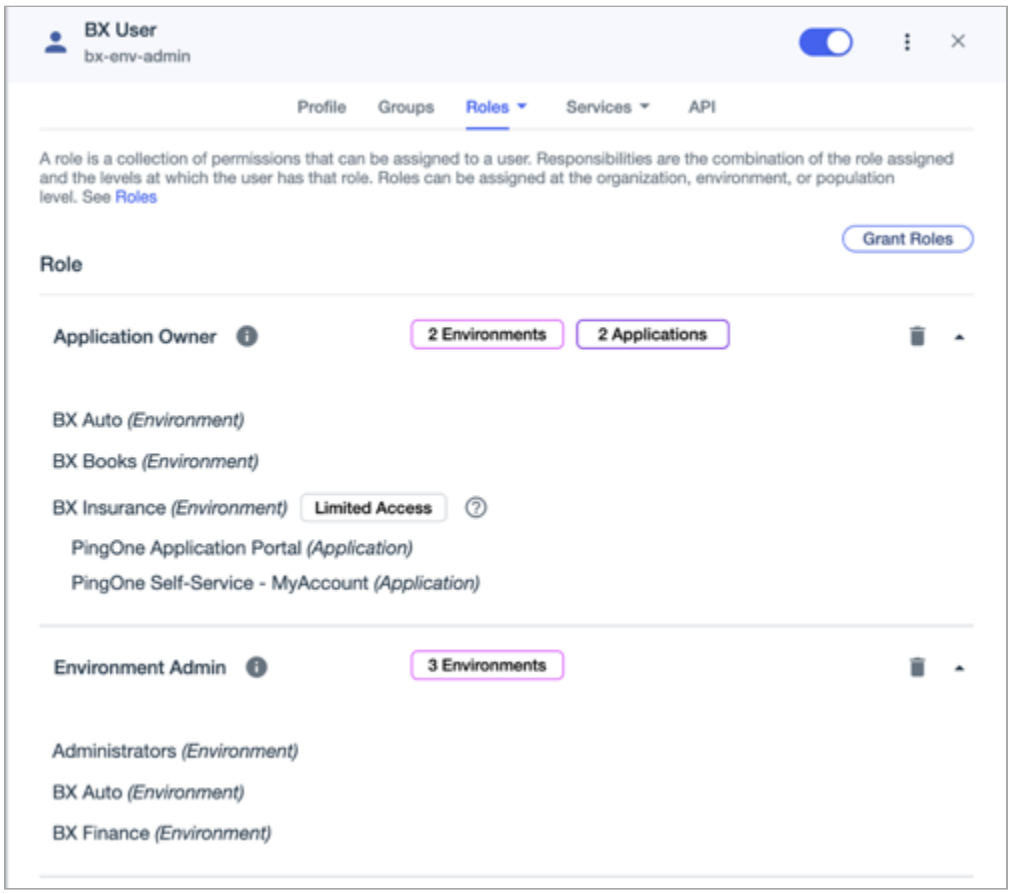
   > **Note**
   >
   > You can assign administrator roles to users, groups, applications, or PingFederate gateway integrations.

Copyright © 2025 Ping Identity Corporation



Tip

Click the **Info** icon to view the permissions associated with the role. Click the down arrow on the right to view the list of environments or populations for which the role is assigned.



6. Click **Grant Roles**.

   The **Available Responsibilities** tab lists the roles that you are allowed to assign and the environments for which you are allowed to assign them. A responsibility is the combination of the role assignment and the level, or scope, at which the role is applied. Depending on the role, it could be assigned at the organization, environment, population, or application level.

   The **Granted Responsibilities** tab lists any roles that are currently assigned.

Copyright © 2025 Ping Identity Corporation

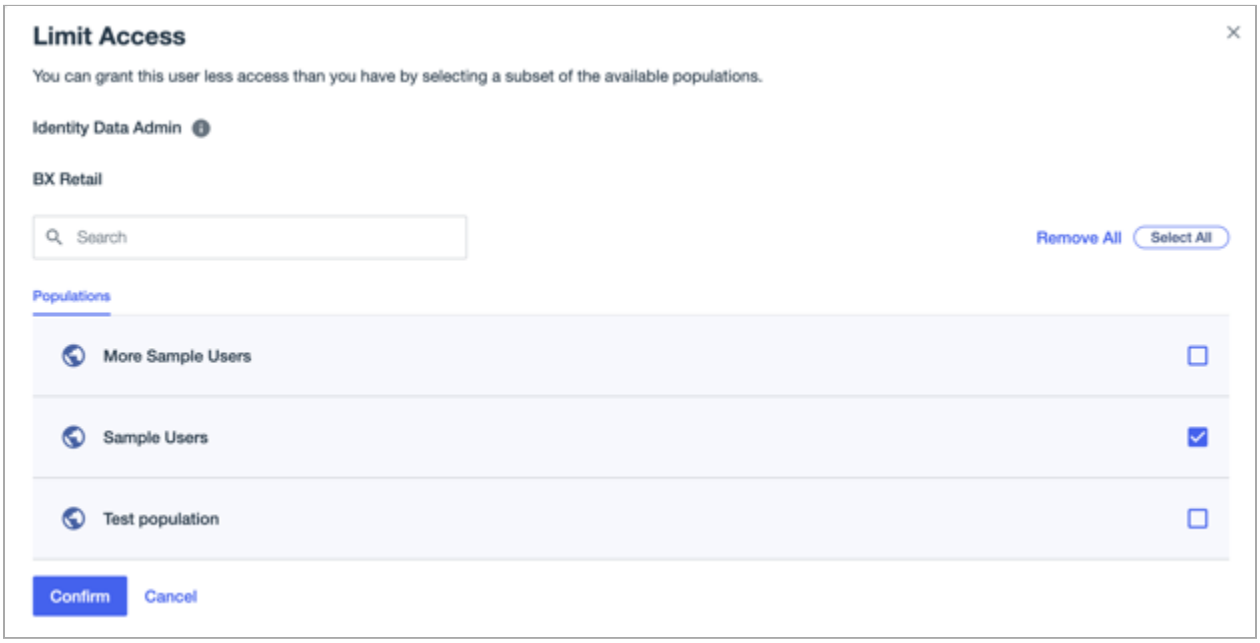
7. On the **Available Responsibilities** tab, click the role that you want to assign or change and perform any combination of the following:

    1. To assign the role, select the checkboxes next to the applicable environments.

    > **Tip**
    >
    > Click **Select All** or **Remove All** to select or clear all available responsibilities.

    2. To remove a role assignment, clear the checkboxes next to the applicable environments.

    3. To grant this access for only a portion of the environment, click the **Reduce Access** icon ( ), select a subset of the available applications or populations on the **Limit Access** page, and click **Confirm**.



> **Note**
>
> You can grant only roles that are assigned to you or that confer the permissions needed to assign that role to others. For example, if you do not have the Environment Admin role, you cannot assign the Environment Admin role to others (and that role will not be listed under **Available Responsibilities**). However, if you have the Identity Data Admin role, you can assign either the Identity Data Admin role or the Identity Data Read Only role to others.
> Learn more about the permissions associated with each role in Roles.

8. Click **Save**.

Result

The role assignments that you selected are listed on the **Granted Responsibilities** tab.

Managing administrator roles using external groups

Before you begin

Ensure that you have one administrator user with direct sign-on access to PingOne. Add this user to the Administrators environment to keep them separate from your end users.

> **Note**
>
> This task uses *PingOne Admin User* to refer to this user.

About this task

You can leverage just-in-time provisioning and use external groups, such as those in an identity store accessed through an external identity provider (IdP), to manage administrator role assignment in PingOne.

For example, you configure PingOne to use an external IdP with Active Directory (AD) as the identity store. You then create a group in the Active Directory identity store. You add users to this group and provision it to PingOne to ensure that these users have access to PingOne with the appropriate roles.

To use an external group to manage administrator roles in PingOne:

Steps

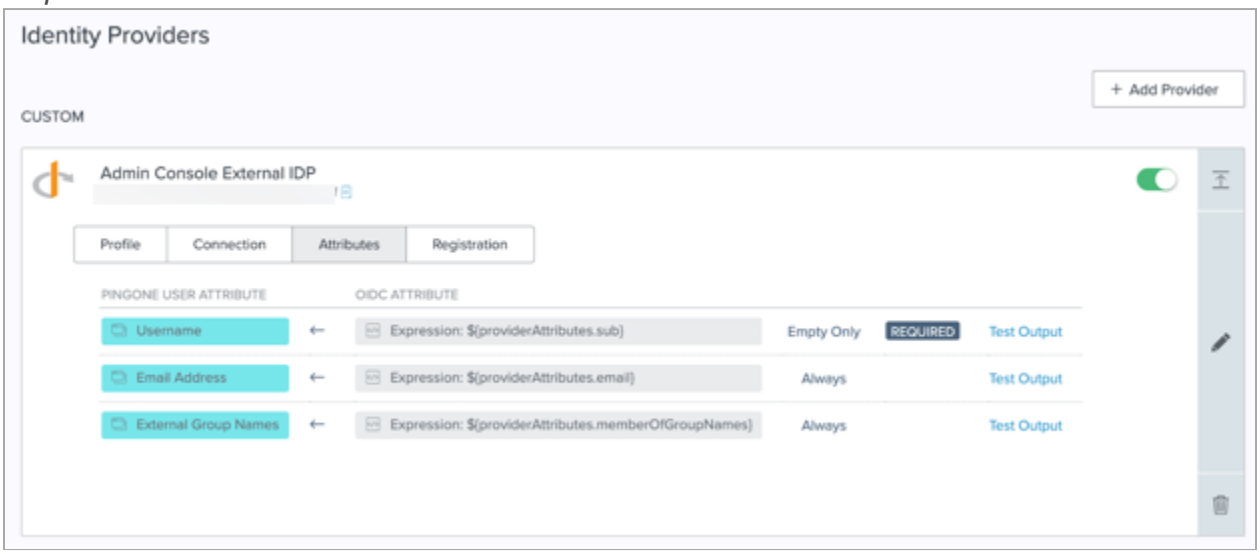
1. Add a custom OIDC or SAML external IdP in PingOne.

   > **Note**
   >
   > Managing roles using external groups is currently supported only for custom OIDC or SAML external IdPs.

   When you get to the step for mapping attributes, you must map at least the following PingOne user attributes to the corresponding attributes for the identity provider:

   - **Username**
   - **Email Address**
   - **External Group Names**

   Example:



   The values in the previous image are for example purposes only. The external attribute names will vary depending on the provider.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Set **Update Condition** for the **Email Address** and **External Group Names** attributes to **Always**. This ensures that these attributes are updated in PingOne whenever they are updated in the external IdP and that their access and permissions are always in sync.

Map additional attributes as needed.

> **Note**
>
> When authenticating into PingOne from an external IdP, ensure that you enable MFA as part of your authentication policy.

2. Create the applicable groups in your external identity store.
3. During the initial group set up, add the *PingOne Admin User* to each external group that you want to provision to PingOne.

> **Note**
>
> You can add more users, but at a minimum each group must contain one user with direct access to PingOne before you continue. The process for adding users to groups depends on the external identity store that you are using. Follow the steps in the documentation for your identity store.

4. Sign on to PingOne as the *PingOne Admin User*.

   Result:

   The external groups are provisioned to PingOne using just-in-time provisioning.

   Learn more in Just-in-time provisioning of external groups.

5. Assign the appropriate admin roles to the groups in PingOne.

   Learn more on the **Using groups** tab in Managing roles using groups.

> **Important**
>
> You must assign at least one role to each group, or the users will be unable to sign on to PingOne.
> These roles are assigned to all users currently in the group and to any users added to the group in the future.

6. Add users to the external group in the external identity store as needed to ensure that they can access PingOne with the appropriate role assignments.

   Similarly, remove users from the external group to remove their access to PingOne or to move them to a group with different role assignments.

Next steps

You should audit the users in your external directory regularly to ensure that their group membership and level of access is correct.

Copyright © 2025 Ping Identity Corporation

PingOne SSO

Using SSO, users can sign on to all their applications and services with one set of credentials. It gives employees, partners, and customers secure, one-click access from anywhere, on any device, and it reduces the number of separate accounts and passwords they need to manage.

SSO is made possible by a centralized authentication service that all apps (even third-party) can use to confirm a user's identity. Identity standards like SAML, OAuth, and OpenID Connect allow for encrypted tokens to be transmitted securely between the server and the apps to indicate that a user has already been authenticated and has permission to access the additional apps.

Getting started

- Getting started with PingOne SSO
- Set up single sign-on

Tutorials

- Add branding to PingOne forms
- Add a SAML application
- Build a custom sign-on policy
- Create a group
- Control user access

Integrations and Connectors

- Ping Identity Integration Directory
- PingOne Gateway connectors
- PingOne provisioning connectors

Copyright © 2025 Ping Identity Corporation

Developer resources

- Get started with PingOne
- Check out PingOne developer tools
- Explore the sample applications

Troubleshooting

- Audit logs
- System status
- Identify provisioning issues

Getting started with PingOne SSO

The first time you start PingOne, sign on with the default credentials that were set up during provisioning. The initial configuration includes a default organization, environment, and population. You can create additional environments, populations, and users for those populations.

About this task

After you start PingOne, you can set up your applications to work with PingOne. PingOne manages access to those applications and ensures that authorized users have access to the applications that they need.

PingOne uses an organization-based model to define tenant accounts and their related entities. The organization is the top-level identifier and defines your entire enterprise within the platform.

By default, your organization includes an `Admin` license, which contains an Admin environment and Administrators population. The Administrators population contains the initial administrator user. You should create all administrators in the Administrators population to make it easier to manage them and to help prevent privilege escalation.

Your organization also includes a `Trial` license and an End-User Sandbox environment that contains two populations and some sample users.

Next steps

These tasks can help you get started setting up PingOne for your organization:

- To sign on, see Administrators: Managing your PingOne environment.
- To replace the default Ping Identity logo with the logo for your organization, see Editing environment branding.

Copyright © 2025 Ping Identity Corporation

- To add applications for your users, see Adding an application.
- To add an authentication policy, see Adding an authentication policy.
- To manage certificates, see Adding a certificate and key pair.
- To add an external identity provider, see External IdPs.
- To find answers to common questions, see the Support and Community portal.

Setting up single sign-on

To have the best experience, you can set up single sign-on (SSO) from the PingOne admin console to all of your Ping products and services.

You can also use SSO with your PingOne account to access support resources. Find answers to common questions, create a support case, access training, and more in the Support and Community portal.

> **Note**
>
> If your email address is already verified with PingOne, you'll automatically be routed to sign on with your PingOne account.

PingOne to PingAccess

- Set up SSO to PingAccess

PingOne to PingCentral

- Set up SSO to PingCentral

PingOne to PingDirectory

- Set up SSO to PingDirectory

PingOne to PingFederate

- Set up SSO to PingFederate

Copyright © 2025 Ping Identity Corporation

PingOne to PingOne Advanced Identity Cloud

- Set up SSO to PingOne Advanced Identity Cloud

PingOne to PingOne for Enterprise or PingID

- Set up SSO to PingOne for Enterprise or PingID

Setting up SSO to PingAccess

To set up single sign-on (SSO) access from the PingOne admin console to PingAccess, configure PingOne and PingAccess, and then test the sign-on experience.

Before you begin

Ensure that you have:

- A licensed version of PingAccess
- A PingOne account

Configuring PingOne for SSO in PingAccess

About this task

To configure PingOne for SSO in PingAccess:

Steps

1. In the PingOne admin console, add a new attribute for PingAccess administrator roles:
    1. Go to **Directory > User Attributes** and click **+**.
    2. In the **Add Attribute** panel, select **Declared** and click **Next**.

       Declared attributes maintain the values of the claims that authorize access to other products.
    3. Enter the following information:
        - **Name**: `PingAccess-Role` (this value is case sensitive)
        - **Display Name**: `PingAccess Role`
        - **Description** (optional): Enter a brief description of this attribute that distinguishes it from others.
    4. Click **Save**.

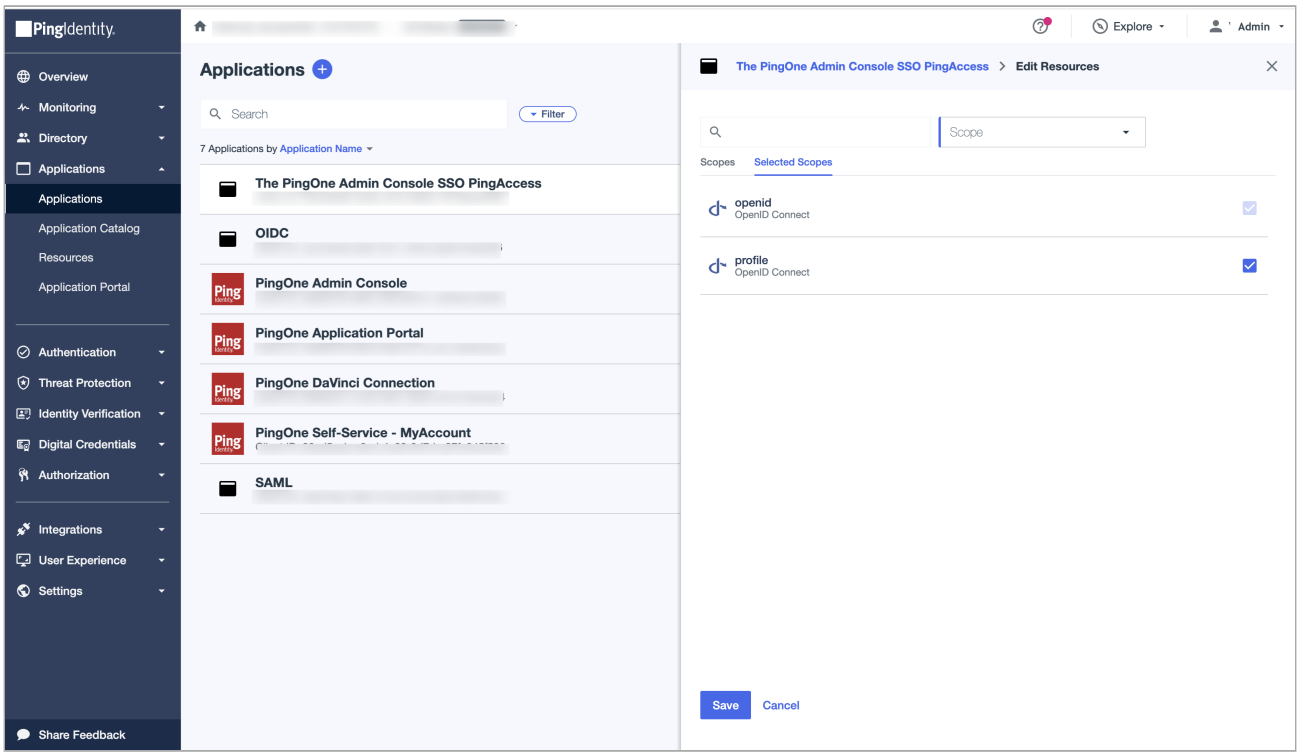
Copyright © 2025 Ping Identity Corporation

2. Create a new connection:

    1. Go to **Applications > Applications** and click **+**.
    2. In the **Add Application** panel, enter the following information:
        - **Application Name**: A name that helps you recognize this connection, such as `The PingOne Admin Console SSO PingAccess`.
        - **Description** (optional): A brief description of this application that distinguishes it from others.
    3. For **Application Type**, select **OIDC Web App** and click **Save**.
    4. In the application details panel, on the **Configuration** tab, click the **Pencil** icon.
    5. Locate the **Redirect URIs** field and enter the appropriate URL.

        Example:

        For example, `https://<FQDNofPAServer>:9000/pa/oidc/cb`, where <FQDNofServer> is the machine name or fully qualified domain name of your PingAccess server, such as `https://localhost:9000/pa/oidc/cb`.
    6. Click **Save**.
    7. On the **Resources** tab, click the **Pencil** icon.
    8. In the **Scopes** list, locate the **profile** scope and select the checkbox to add it to the **Selected Scopes** section.



    9. Click **Save**.
    10. On the **Attribute Mappings** tab, click the **Pencil** icon.
    11. Click **+ Add** and add the following attribute mapping:

Copyright © 2025 Ping Identity Corporation

Attributes	PingOne Mappings
`PingAccess Role`	**PingAccess Role**

12. Click **Advanced Configurations**.
13. For the attributes you just mapped, select the **Required** checkbox.
14. Click **Save**.

3. To enable the application, click the toggle at the top of the details panel to the right (blue).

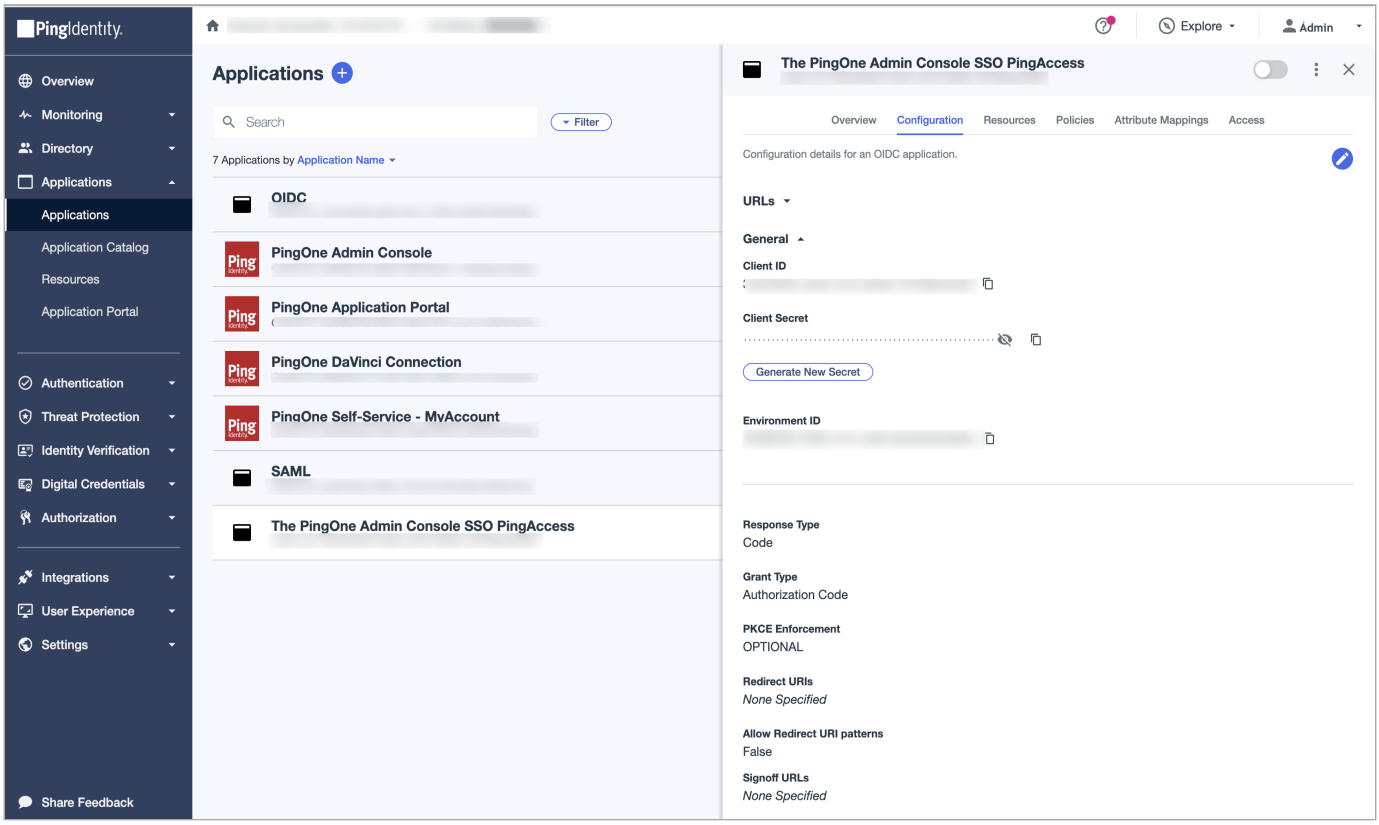
> **Note**
> You can disable the application by clicking the toggle to the left (gray).

4. Add a new PingAccess administrator and define their role and responsibilities.
    1. Go to **Directory** > **Users** and click **+**.
    2. On the **Add User** panel, enter a username for a PingAccess administrator with the Administrator role assigned in PingAccess and select a population to which the administrator should belong.

       Learn more in Admin UI SSO authentication in the PingAccess documentation.
    3. Click **Save**.
    4. In the **Profile** tab, click the **Pencil** icon and, in the **Custom Attributes** section, click **+ Add**.
    5. In the **New Attribute** list, select **PingAccess Role** and enter `fullAdmin`.
    6. Click **Save**.
    7. In the user details panel, go to the **Roles** > **Administrator Roles** tab, and click **Grant Roles**.
    8. In **Available Responsibilities**, click **Environment Admin** and select the checkboxes for the organizations and environments where the administrator should have this role.
    9. Click **Save**.
    10. Click the **More Options** (⋮) icon and select **Reset Password**.
    11. Select **Force password reset on next sign on**.
    12. Click **Save**.
5. Go to **Applications** > **Applications** and locate the application you created earlier.
6. Click the application entry to open the details panel.
7. On the **Configuration** tab, review the configuration information.

> **Tip**
> You need this configuration information to configure PingAccess for SSO, so keep this browser window open.

Copyright © 2025 Ping Identity Corporation



Configuring PingAccess

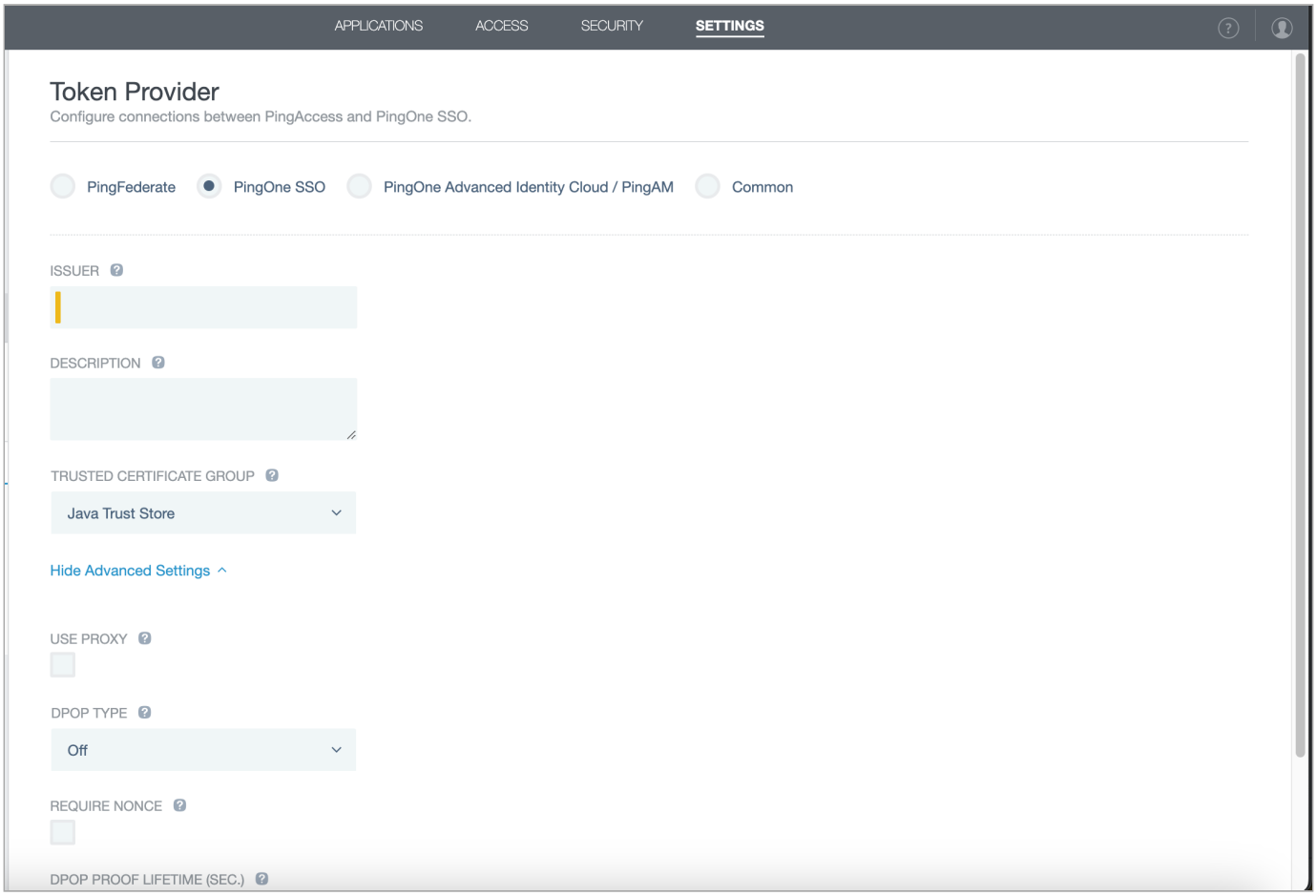
After configuring PingOne for SSO, configure PingAccess.

Steps

1. In the PingAccess administrative console, go to **Settings** > **System** > **Token Provider**.
2. On the **Token Provider** page, select **PingOne SSO** as the token provider.
3. In the **Issuer** field, enter the **Issuer ID** for the connection you created in PingOne.

   You can find this URL on the **Overview** tab of the application in PingOne.

Copyright © 2025 Ping Identity Corporation



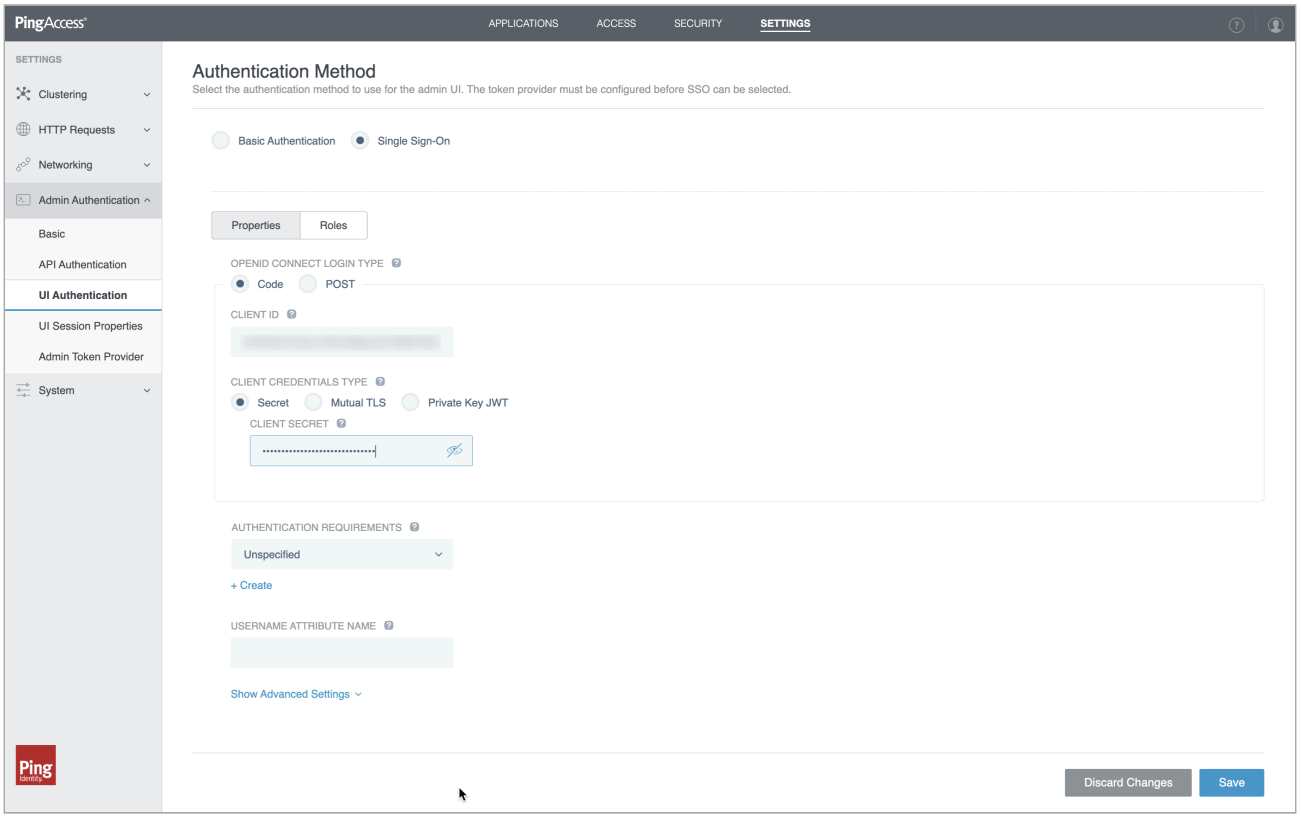
Learn more in Configuring PingOne in the PingAccess documentatation.

4. Go to **Settings > Admin Authentication > UI Authentication**.
5. On the **Authentication Method** page, select **Single Sign-On** and enter or edit the following:
    1. For **OpenID Connect Login Type**, select **Code**.
    2. In the **Client ID** field, enter the **Client ID** for the connection you created in PingOne.

       You can find **Client ID** on the **Overview** tab of the application in PingOne.
    3. For **Client Credentials Type**, select **Secret** and enter the **Client Secret** for the connection you created in PingOne.

       You can find **Client Secret** on the **Overview** tab of the application in PingOne.
    4. Click **Save**.

Copyright © 2025 Ping Identity Corporation



Learn more in Admin UI SSO authentication in the PingAccess documentation.

Testing SSO to PingAccess

After configuring PingOne and PingAccess, test SSO to PingAccess.

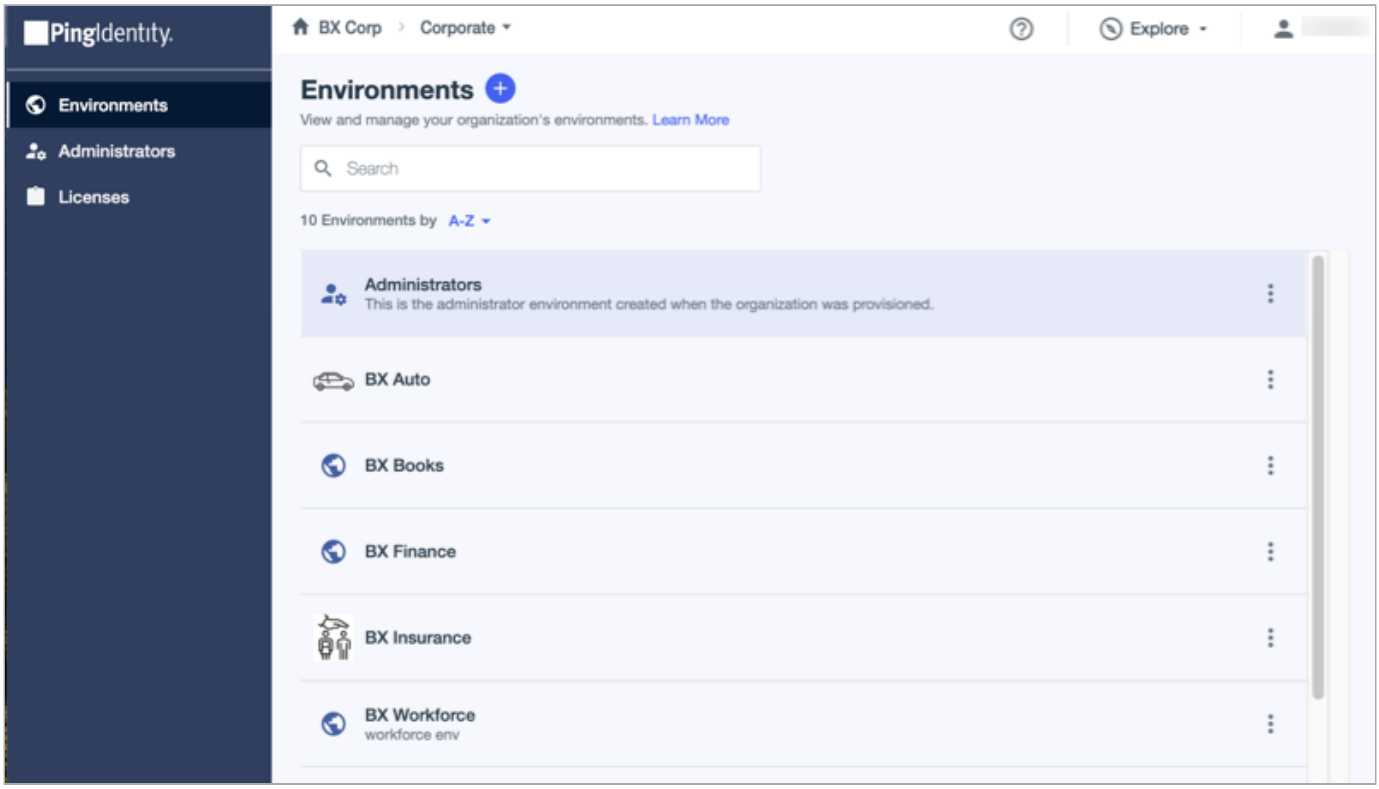
Steps

1. In the PingOne admin console, click the **Ping Identity** logo.

   Result:

   The admin console displays the environments to which you have access.

Copyright © 2025 Ping Identity Corporation



2. On the **Environments** page, click the environment to open the details panel.
3. Click **Manage Environment** to go to the **Overview** page for the environment.
4. In the **Services** section, click the **PingAccess** icon.

   Result:

   The PingAccess administrative console opens.

   Troubleshooting:

   If the OpenID Connect (OIDC) token provider is unreachable:

   1. Review the reason for the failure in the `pingaccess.log` file.
   2. Enable the default administrator authentication by setting the `admin.auth` property in the `<PA_HOME>/conf/run.properties` file.

      Learn more in Editing `run.properties` to disable SSO in the PingAccess documentation.
   3. In the PingAccess administrative console, edit the admin UI SSO or token provider settings to address the issue.
   4. In the `run.properties` file, set `admin.auth` back to `default`.

Copyright © 2025 Ping Identity Corporation

run.properties

```
#-----------------------------------------------------------------------------

admin.port=9000
admin.bindAddress=0.0.0.0
admin.ssl.protocols=${tls.default.protocols}
admin.ssl.ciphers=${tls.default.cipherSuites}
admin.acceptors=1
admin.backlog=512
admin.httptransport.coreThreadPoolSize=5
# 0 means allow PingAccess to calculate the appropriate number of I/O threads for the host
admin.httptransport.ioThreads=0
admin.httptransport.maxThreadPoolSize=-1
admin.httptransport.socketTimeout=30000

# Set to native to override the administrator authentication method.
admin.auth=default

admin.reuseAddress=true
#max body length in a request for admin API expressed in MBs
admin.max.request.bodylength=15

# maximum number of sessions for the admin UI when admin SLO is not enabled
admin.ui.max.sessions=100

# Specifies how exported sensitive data should be encrypted.
# Valid values are:
#
#   MASTER_KEY - (default) Use the system default/master key.
#
#   PORTABLE_INSECURE - Use a randomly-generated key for each export, and include it in the
```

5. Restart PingAccess to test.

Setting up SSO to PingCentral

To set up single sign-on (SSO) access from the PingOne admin console to PingCentral, configure PingOne and PingCentral and test the sign-on experience.

Before you begin

Ensure that you have:

- A licensed version of PingCentral
- A PingOne account
- A text editor or terminal

> **Important**
>
> When SSO is enabled for PingCentral, auto-provisioning is also enabled, which currently causes sign-on issues. New users are created during this process even if those users already have PingCentral accounts.

Copyright © 2025 Ping Identity Corporation

Configuring PingOne for SSO in PingCentral

Steps

1. In the PingOne admin console, add a new attribute to PingCentral administrator roles:
    1. Go to **Directory** > **User Attributes** and click **+**.

       Result:

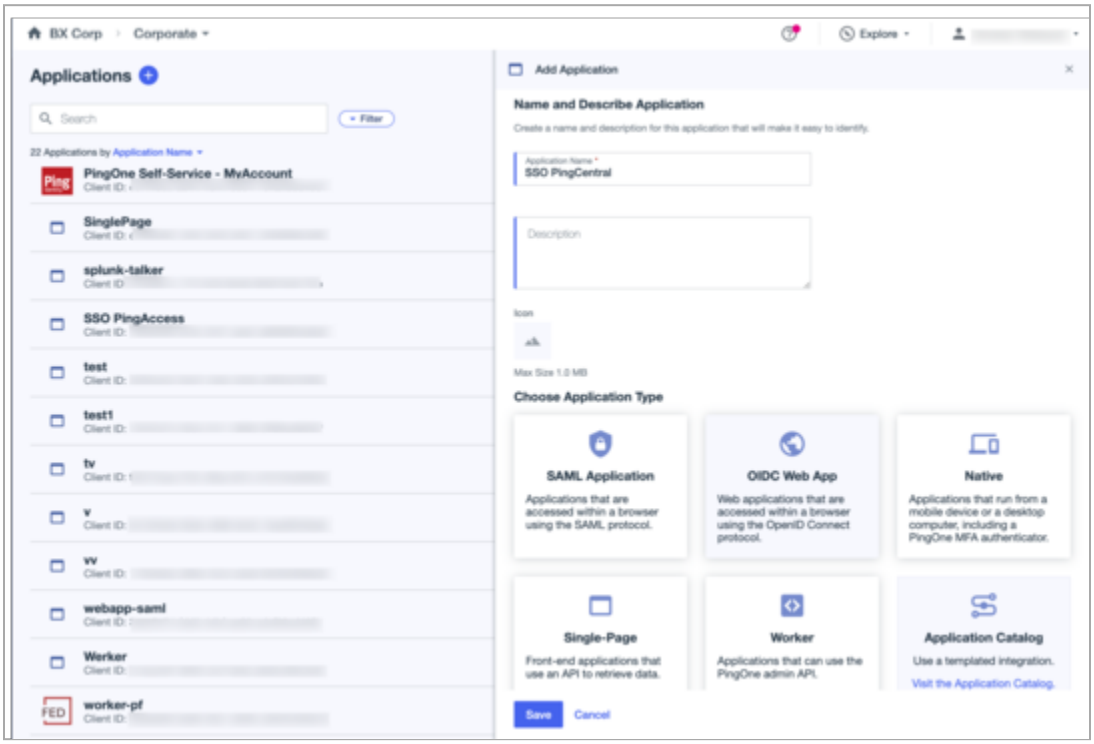
       The **Add Attribute** panel opens.
    2. In the **Add Attribute** panel, select **Declared** and click **Next**.

       Declared attributes maintain the values of the claims that authorize access to other products.
    3. Enter the following information:
        - **Name**: `PingCentral-Role` (this value is case sensitive)
        - **Display Name**: `PingCentral Role`
        - **Description** (optional): Enter a brief description of this attribute that distinguishes it from others.
    4. Click **Save**.
2. Create a new connection:
    1. Go to **Applications** > **Applications** and click **+**.

       Result:

       The **Add Application** panel opens.
    2. Enter the following information:
        - **Application Name**: Enter a name that helps you recognize this connection, such as `PingOne administrator console SSO PingCentral`.
        - **Description** (optional): Enter a brief description of this application that distinguishes it from others.
    3. For **Application Type**, select **OIDC Web App** and click **Save**.

Copyright © 2025 Ping Identity Corporation



4. In the application details panel, on the **Configuration** tab, click the **Pencil** icon.
5. Locate the **Redirect URIs** field and enter the appropriate URL.

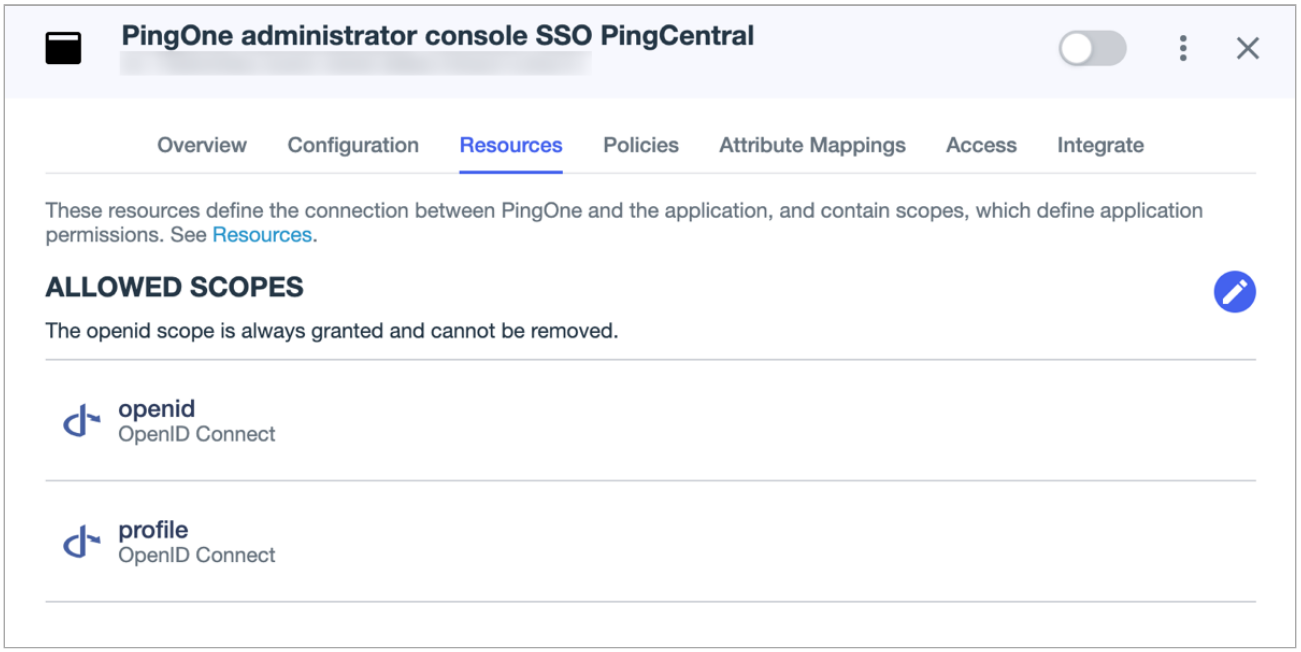
   Example:

   For example, `https://<FQDNofServer>:9022/login/oauth2/code/pingcentral`, where <FQDNofServer> is either the machine name or fully qualified domain name of your PingCentral server, such as `https://localhost:9022/login/oauth2/code/pingcentral`.

6. Click **Save**.
7. On the **Resources** tab, click the **Pencil** icon.
8. In the **Scopes** list, locate **Profile** scope and select the checkbox to add it to the **Allowed Scopes** section.

> **Note**
>
> The `openid` scope is included by default.

Copyright © 2025 Ping Identity Corporation



9. Click **Save**.
10. On the **Attribute Mappings** tab, click the **Pencil** icon.
11. Click **+ Add** and add the following attribute mapping:

Attributes	PingOne Mapping
`PingCentral Role`	**PingCentral Role**

12. Click the **Advanced Configurations** button.
13. For the **PingCentral Role** attribute, select the **Required** checkbox.
14. Click **Save**.

3. To enable the application, click the toggle at the top of the details panel to the right (blue).

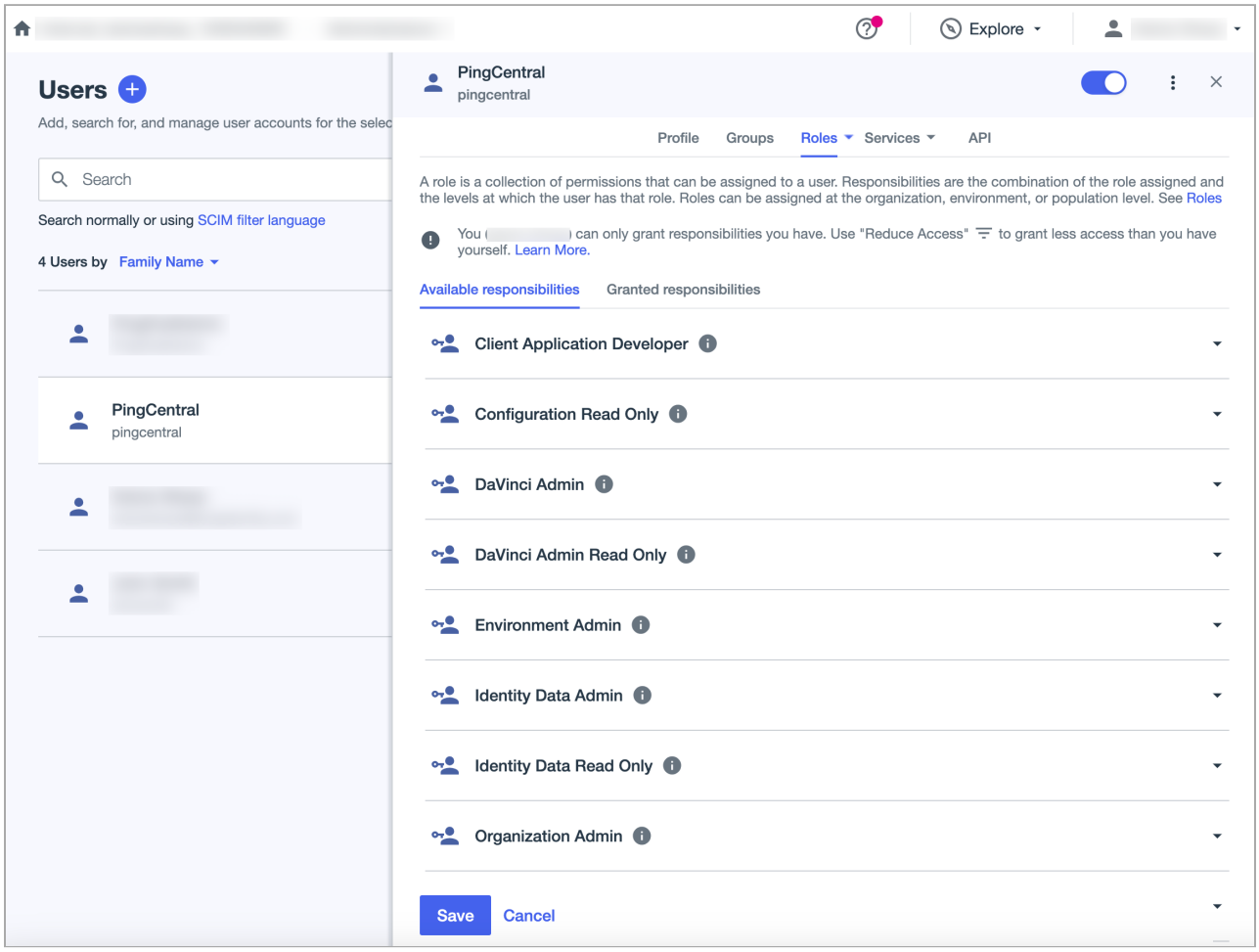
> **Note**
>
> You can disable the application by clicking the toggle to the left (gray).

4. Add a new PingCentral administrator in PingOne and define their role and responsibilities.
    1. In the PingOne admin console, go to **Directory** > **Users** and click **+**.
    2. On the **Add User** panel, enter the following information:
        - **Given Name** and **Family Name** (optional): Enter the user's name in these fields.
        - **Username**: Enter a username for the PingCentral administrator who has the **IAM Admin** role.
    3. Click **Save**.

Copyright © 2025 Ping Identity Corporation

4. In the user details panel, on the **Roles** tab, click **Grant Roles**.

5. In **Available Responsibilities**, click **Client Application Developer** and select the checkboxes for the organizations and environments where the administrator should have this role.



6. Click **Identity Data Admin** and select the checkboxes for the organizations and environments where the administrator should have this role.

7. Click the **More Options** (⋮) icon and select **Reset Password**.

8. Select **Force Password reset on next sign on**.

9. Click **Save**.

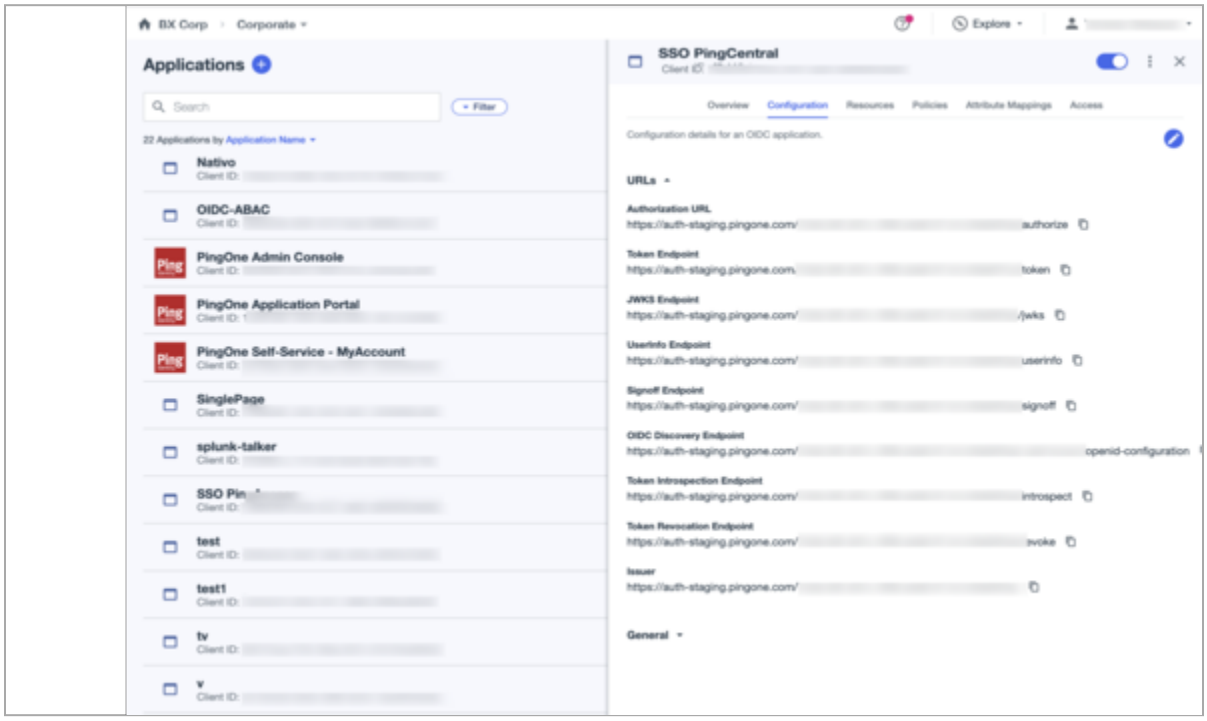
5. Go to **Applications > Applications**, and locate the application you created earlier.

6. Click the application entry to open the details panel.

7. On the **Configuration** tab, review the configuration information.

> **Tip**
>
> You need this configuration property information to configure PingCentral for SSO, so keep this browser window open.

Copyright © 2025 Ping Identity Corporation



Configuring PingCentral

After configuring PingOne for SSO, configure PingCentral.

Steps

1. In a text editor, open the `<pc-path>conf/application.properties` file.
2. Use the configuration information on the **Applications** page in the PingOne admin console to update the following values in the `application.properties` file.

> **Note**
>
> Watch for unwanted line breaks when pasting values into this file.

PingOne attribute	`application.properties` file attribute	Attribute	Example
	pingcentral.sso.oidc.enabled	true	`pingcentral.sso.oidc.enabled=true`
Issuer	pingcentral.sso.oidc.issuer-uri	Issuer	`pingcentral.sso.oidc.issuer-uri=https://auth.pingone.com/3c2f30a3-7a92-406e-b8f2-6a181e56f46b/as`
Client ID	pingcentral.sso.oidc.client-id	Client ID	`pingcentral.sso.oidc.client-id=5be9323a-e953-4aa6-8db3-5f4113a73f83`

Copyright © 2025 Ping Identity Corporation

PingOne attribute	`application.properties` file attribute	Attribute	Example
Client Secret	pingcentral.sso.oidc.client-secret	Client Secret	`pingcentral.sso.oidc.client-secret=cigVeh5py8IC2~ViGMmM3sslpYyMLCWr5SnmjXwvHUG-r4CYjtoOMAlNSPqZ4bc9`

3. Save and close the file.
4. Restart PingCentral.

Testing SSO to PingCentral

After configuring PingOne and PingCentral, test the sign-on experience to PingCentral.

Steps

1. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page and browse or search for the applicable environment.
2. On the **Environments** page, click the environment to open the details panel.
3. Click **Manage Environment** to go to the **Overview** page for the environment.
4. In the **Services** section, click the **PingCentral** icon.

   Result:

   The PingCentral admin console opens.

Setting up SSO to PingDirectory

To set up single sign-on (SSO) access from the PingOne admin console to PingDirectory, configure PingOne and PingDirectory and test the sign-on experience.

Before you begin

Ensure that you have:

- A PingDirectory server that accepts LDAPS connections

  This server will host the admin console that is being configured for SSO.

- The host name and port for the PingDirectory server
- A PingOne account

  Learn more in Getting started with PingOne SSO.

- A PingOne environment that includes PingDirectory.

  Learn more in Adding an environment and Adding a service to an environment.

Copyright © 2025 Ping Identity Corporation

> **Note**
> When creating a new PingOne environment, select **Customer solution** for the environment type.

About this task

During this process, you'll:

- Set up matching users between PingOne and the PingDirectory environments to allow the server's `All Admin Users` identity mapper to map the PingOne ID token to a Directory Server LDAP user.
- Set up the OpenID Connect (OIDC) application in PingOne.
- Configure the PingOne admin console and PingDirectory server.

Linking PingOne to PingDirectory

Configure a link to connect PingOne and PingDirectory.

Before you begin

Ensure that you have the values for host name and port for the PingDirectory server. Contact the PingDirectory administrator for these values.

Steps

1. In the PingOne admin console, go to the **Overview** page.
2. Locate the **PingDirectory** tile and click **Add Admin UI Link**.
3. For **Admin URL**, enter `https://<hostname>:<port>/console/login`.

   Replace <hostname> and <port> with the values for the PingDirectory server.

   > **Tip**
   > You can specify the LDAP server to bind to by using the query parameters `ldap-hostname` and `ldaps-port` when the administrative console is configured for SSO. By binding to the LDAP server, you can use a single console instance to administer multiple PingDirectory servers. An LDAPS scheme is always assumed because an encrypted connection is always required for SSO. Using these parameters, you can specify the URL as follows:
   >
   > ```
   > https://<hostname>:<port>/console?ldap-hostname=<my-ldap-host>&ldaps-port=<my-ldaps-port>
   > ```

4. Click **Save**.

Configuring matching administrator accounts

Set up user accounts for the users you want to have SSO access to PingDirectory. You can repeat this procedure for multiple user accounts.

Steps

1. In the PingOne admin console, go to **Directory** > **Users**.

Copyright © 2025 Ping Identity Corporation

2. Locate the user you want to configure and click the user entry to open the details panel.
3. On the **Profile** tab, copy the following values to a secure location:
   - **Username**
   - **Given name**
   - **Family name**
4. Open a terminal window.
5. Run the following `dsconfig` command.
   1. Replace <pd_install> with the PingDirectory version.
   2. Replace the <Username>, <GivenName>, and <FamilyName> variables with the values you copied from the PingOne user details panel.

```
~/<pd_install>/dsconfig create-root-dn-user --user-name <Username> \
  --set first-name:<Given Name> \
  --set last-name:<Family Name>
```

Adding the OIDC application to PingOne

In PingOne, add an OIDC application that connects to PingDirectory.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and click **+**.
2. Enter the following:
   - **Application Name**: Enter a name that helps you recognize this connection, such as `PingDirectory Administrative Console`.
   - **Description** (optional): Enter a brief description of this application that distinguishes it from others, such as `Application for the PingDirectory Administrative Console`.
3. In the **Choose Application Type** section, select **OIDC Web App**.
4. Click **Save**.
5. Click the application entry to open the details panel.
6. On the **Configuration** tab, click the **Pencil** icon.
7. Enter or edit the following values:

Field	Description
Response Type	Select the **Code** checkbox.
Grant Type	Select the **Authorization Code** checkbox.

Copyright © 2025 Ping Identity Corporation

Field	Description
Redirect URIs	Enter `https://<hostname>:<port>/console/oidc/cb` and replace the variables with the values for the PingDirectory server hostname and port. To find the port, run the **`status`** command from the `bin` directory. `Step 0.0.0.0:11443 : HTTPS  : Enabled  : HTTPS Connection Handler`
Token Endpoint Authentication Method	Select **Client Secret Basic** in the list.

> **Note**
> Learn more about configuring OIDC applications in Editing an application - OIDC.

8. On the **Attribute Mappings** tab, click the **Pencil** icon.
9. For the default `sub` attribute, select `UserName` in the **PingOne Mappings** list.
10. Click **Save**.
11. To enable the application, click the toggle at the top of the details panel to the right (blue).

> **Note**
> You can disable the application by clicking the toggle to the left (gray).

Configuring the application in PingDirectory

Modify the `config` file in PingDirectory to add the PingOne admin console.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and click the application you created to open the details panel.
2. On the **Configuration** tab, copy the following values to a secure location:
   - **Issuer**
   - **Client ID**
   - **Client Secret**
3. Locate the PingDirectory `config` file at:

```
PingDirectory/config/sample-dsconfig-batch-files/enable-pingone-admin-console-sso.dsconfig
```

4. Make a copy of the `config` file and leave the original file intact.
5. Open the copy of the `config` file in a text editor.

Copyright © 2025 Ping Identity Corporation

6. Replace the variables with the values you copied from PingOne.

```
# Create an ID token validator suitable for verifying ID tokens generated
# by the PingOne service. The "All Admin Users" identity mapper will be used
# to match users that authenticate with PingOne to either root DN users or
# topology admin users defined in the server configuration.
dsconfig create-id-token-validator \
--validator-name "PingOne ID Token Validator" \
--type ping-one \
--set enabled:true \
--set "identity-mapper:All Admin Users" \
--set evaluation-order-index:1 \
--set issuer-url:<PING_ONE_APPLICATION_ISSUER_URL>

[...]

# Configure the Administrative Console with your application's client
# credentials and issuer URI.
dsconfig set-web-application-extension-prop \
--extension-name Console \
--set sso-enabled:true \
--set oidc-client-id:<PING_ONE_APPLICATION_CLIENT_ID>  \
--set oidc-client-secret:<PING_ONE_APPLICATION_CLIENT_SECRET>  \
--set oidc-issuer-url:<PING_ONE_APPLICATION_ISSUER_URL>
```

7. Run the following `dsconfig` command.

```
dsconfig --batch-file \
    enable-pingone-admin-console-sso-copy.dsconfig \
    --no-prompt
```

Testing SSO to PingDirectory

Test the SSO experience from the PingOne admin console.

Steps

1. In the PingOne admin console, click **Overview**.
2. In the **Services** section, locate the **PingDirectory** tile.
3. Click **PingDirectory**.

   Result:

   A PingOne sign-on page opens.

4. Sign on using the credentials for a PingDirectory admin user.

Result

The PingDirectory server administrative console opens.

Copyright © 2025 Ping Identity Corporation

Setting up SSO to PingFederate

To set up single sign-on (SSO) access for administrators from the PingOne admin console to the PingFederate administrative console, configure PingOne and PingFederate and test the sign-on experience.

Before you begin

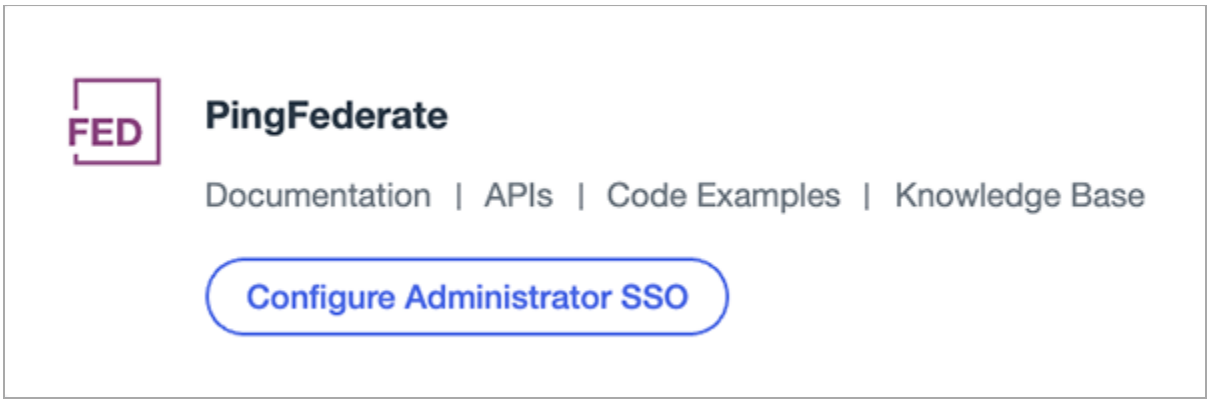
Ensure that you have:

- A licensed version of PingFederate 10.1.2 or later
- A PingOne account
- A text editor or terminal
- The Environment Admin role assigned in PingOne

> **Important**
>
> For PingOne users to use SSO to PingFederate, they must have one or more PingFederate-related roles in PingOne. You can assign roles in the PingOne admin console. Learn more in Administrator Roles and Managing user roles.

Steps

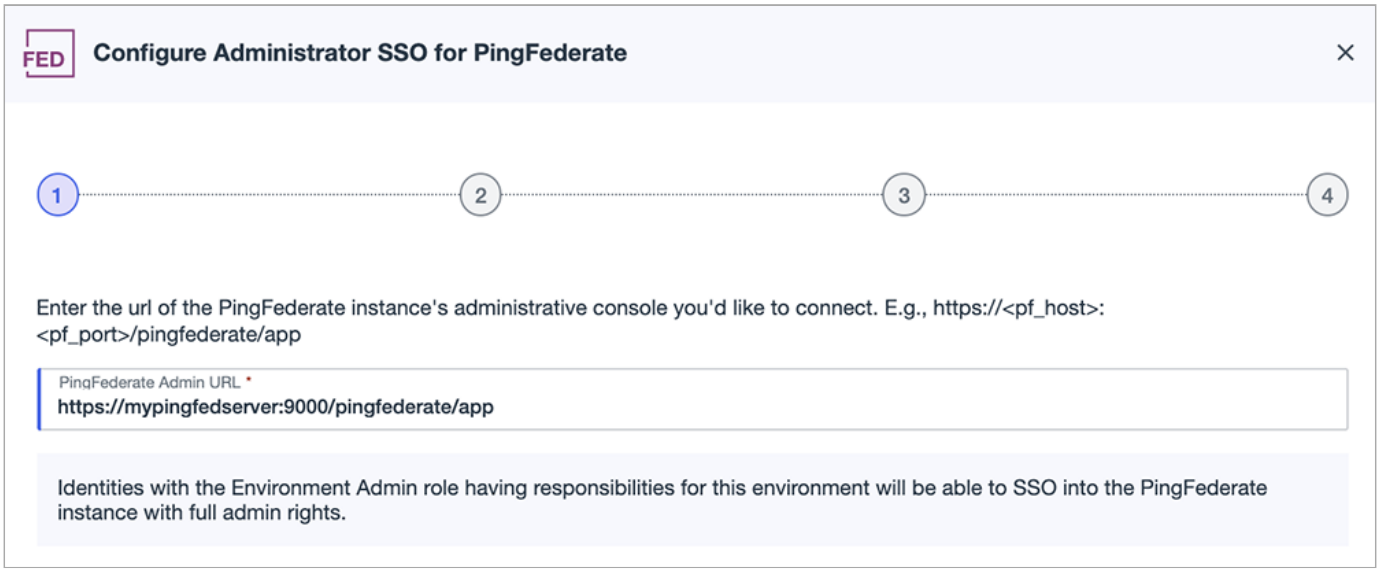
1. In the PingOne admin console, go to the **Overview** page.
2. Locate the **PingFederate** tile and click **Configure Administrator SSO**.



3. Enter the URL for the PingFederate administrative console.

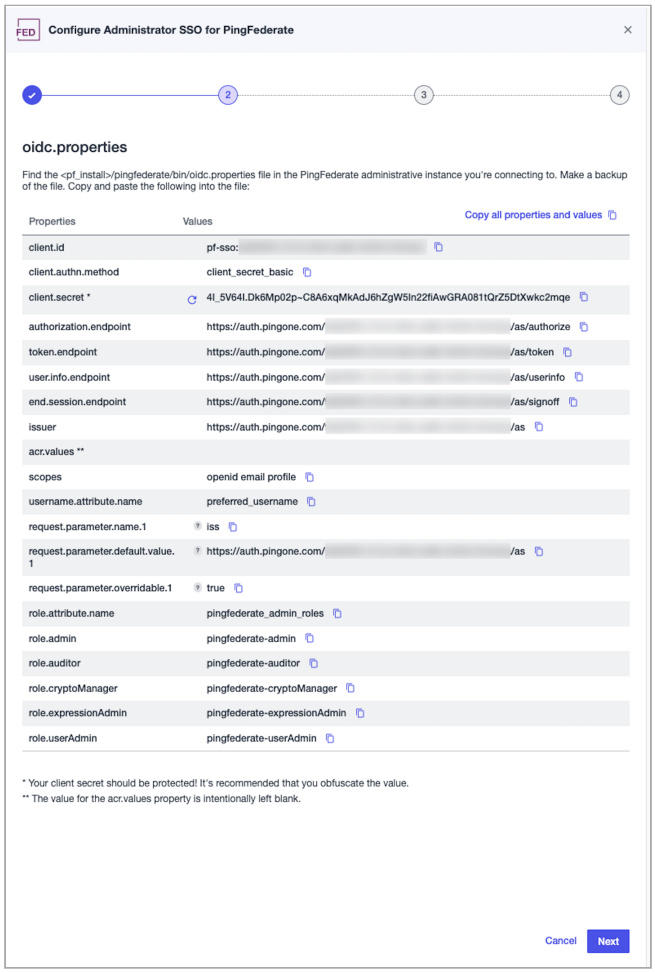
   Example:

   ```
   https://<pf_host>:<pf_port>/pingfederate/app
   ```



4. Click **Save and Continue**.

5. Copy the provided OpenID Connect (OIDC) settings to the `oidc.properties` file on the PingFederate administrative server.



Copyright © 2025 Ping Identity Corporation

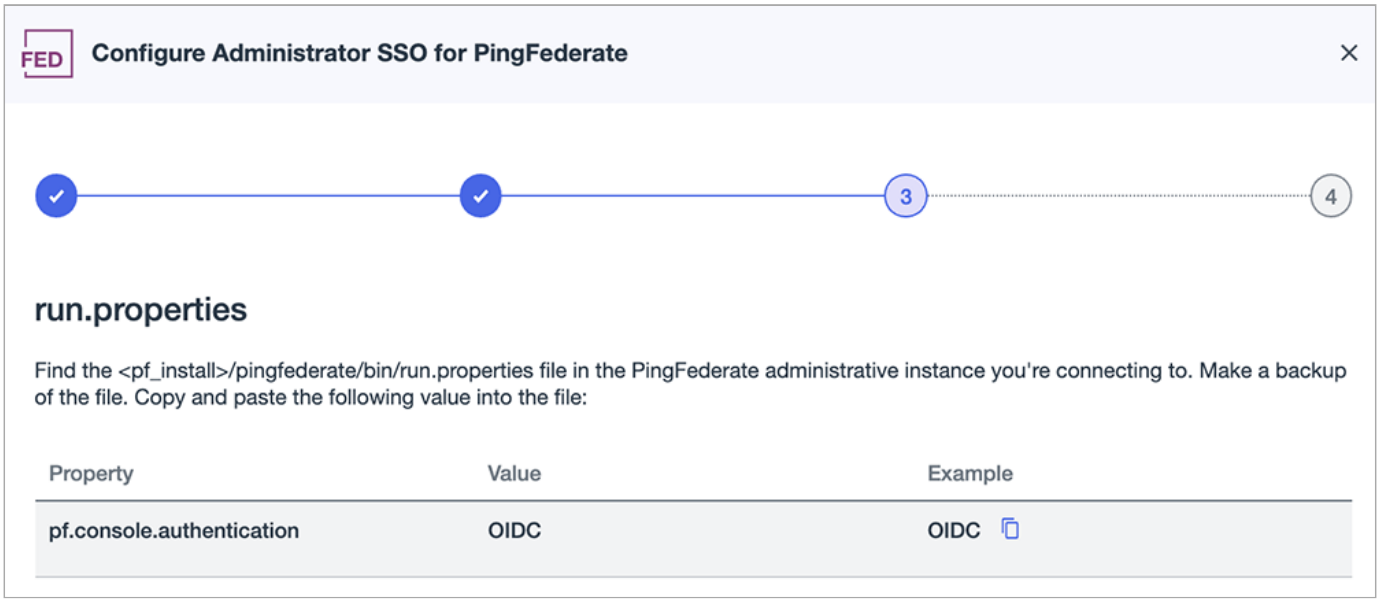
The following three unique parameters allow administrators to use SSO into PingFederate 11.2 or later from any PingOne environment if they have the proper administrator roles assigned for the environment. Learn more in Administrator Roles.

> **Note**
>
> For PingFederate 11.1 or earlier, the administrator's identity must exist in the same PingOne environment as the SSO configuration, and these parameters can't be used.

Request Parameter	Value
`request.parameter.name.1`	The request parameter's name. The value is `iss`. This field is required. Do not use URL encoding for the name.
`request.parameter.default.value.1`	The default value of the request parameter. The value is the authorization endpoint of the current environment if the administrator identity resides in the current environment. ◦ If this parameter isn't included in the request, the default value is included in the authorization request. ◦ If this parameter isn't included in the request, and no default value is specified, the parameter isn't included in the authorization request. ◦ This field is optional when `request.parameter.overridable.1` is set to `true`.
`request.parameter.overridable.1`	Specifies whether the request parameter can be overridden at runtime. The value is set to `true`, which allows the administrator identity's home environment to override the value. This field is optional. Possible values are `true` or `false`. If not specified, the default is `false`. If this property is set to `false`, the `request.parameter.default.value.1` is always included in the authorization request and can't be overridden.

6. Click **Next**.
7. Copy the provided `run.properties` file attribute value to the `run.properties` file on the PingFederate administrative server.

Copyright © 2025 Ping Identity Corporation



8. Click **Next**.
9. Click **Close**.

10. Restart the PingFederate server.

Testing SSO to PingFederate

After configuring PingOne and PingFederate, test the sign-on experience to PingFederate.

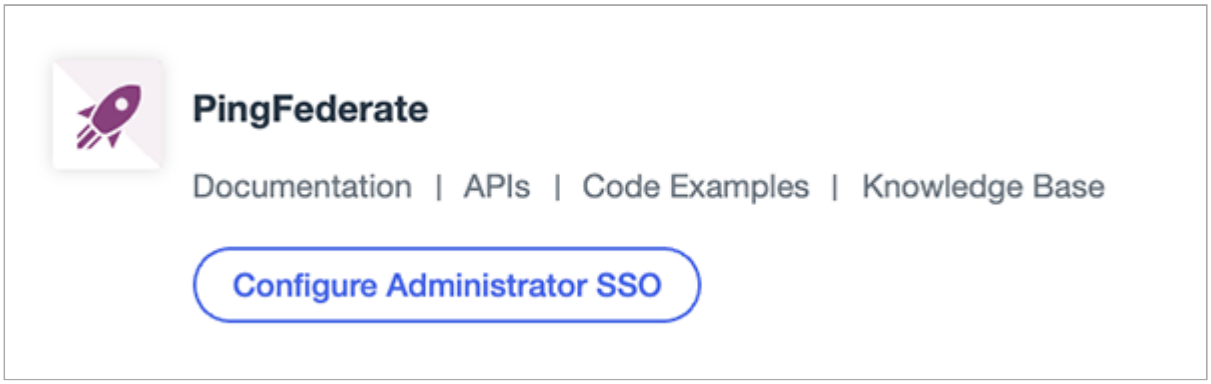
Before you begin

You must have a PingFederate-related role to perform this task. Learn more in Administrator Roles.

Steps

- In the PingOne admin console, on the **Overview** page, locate the **PingFederate** tile and click the **PingFederate** icon.

Copyright © 2025 Ping Identity Corporation



Result:

The PingFederate administrative console opens.

Setting up SSO to PingOne Advanced Identity Cloud

To set up single sign-on (SSO) access for administrators from the PingOne admin console to PingOne Advanced Identity Cloud, configure PingOne with each Advanced Identity Cloud tenant environment and test the sign-on experience.

Before you begin

Ensure that you have:

- A PingOne account
- A separate environment added to your PingOne account for each Advanced Identity Cloud tenant environment for which you want to set up SSO access from PingOne

  Learn more in Creating an environment.
- The following admin roles assigned in each PingOne environment and corresponding Advanced Identity Cloud tenant environment:
  - PingOne: Identity Data Admin, Environment Admin, and PingOne Advanced Identity Cloud Super Admin

    Learn more in Administrator Roles and Managing user roles.
  - Advanced Identity Cloud: Super Admin

    Learn more about assigning admin roles in Tenant administrator settings.

> **Important**
>
> Because Advanced Identity Cloud is made up of several individual tenant environments, you must complete the configuration steps for each Advanced Identity Cloud tenant environment.

Adding PingOne Advanced Identity Cloud to an environment

About this task

Add Advanced Identity Cloud to your existing environment.

Copyright © 2025 Ping Identity Corporation

Steps

1. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page and browse or search for the applicable environment.
2. On the **Environments** page, click the environment to open the details panel.
3. Click **Manage Environment** to go to the **Overview** page for the environment.
4. In the **Services** section, click **+**.
5. Click **+ Add** next to **PingOne Advanced Identity Cloud** and any other products or services that you want to add to the environment.
6. Click **Finish**.

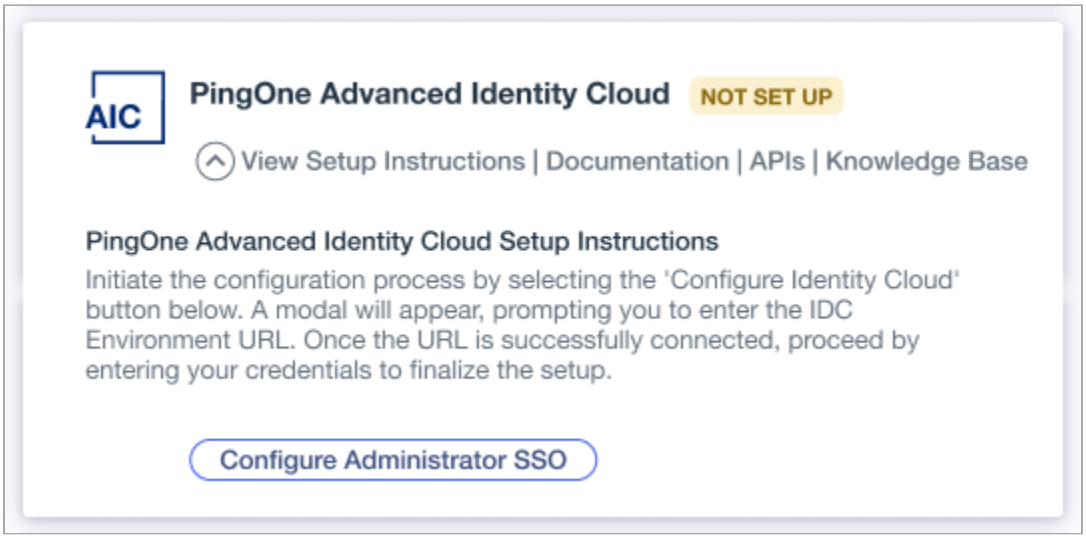
Configuring SSO to PingOne Advanced Identity Cloud

About this task

After adding Advanced Identity Cloud to your environment, configure SSO from the PingOne admin console.

Steps

1. In the PingOne admin console, in the **Environments** list, click the environment with Advanced Identity Cloud and click **Manage Environment**.
2. On the **Overview** page, locate the **PingOne Advanced Identity Cloud** tile and click **Configure Administrator SSO**.



3. In the **Configure PingOne Advanced Identity Cloud** window, enter the URL for the Advanced Identity Cloud administrative tenant.

   The URL must end with .forgerock.io or .forgeblocks.com. Learn more in Tenant administrator sign-on in the Advanced Identity Cloud documentation.

4. In the **Direct Sign-On Environment** list, select the environment that administrators must be associated with when authenticating directly from Advanced Identity Cloud using the **Sign in with PingOne** option.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Any administrator with an appropriate Advanced Identity Cloud role from any environment in PingOne can use SSO into Advanced Identity Cloud from PingOne.

5. Click **Connect**.

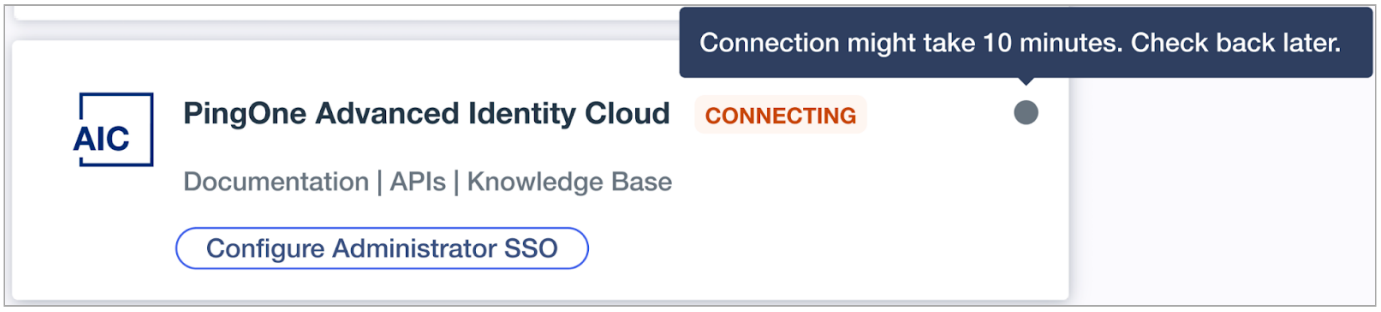
   Result:

   PingOne opens a new browser tab with the Advanced Identity Cloud sign-on screen.

6. Go to the new browser tab and enter your Advanced Identity Cloud credentials to complete setup.

   Result:

   PingOne creates a connection to Advanced Identity Cloud. It can take up to 10 minutes to complete the connection.



Testing SSO to PingOne Advanced Identity Cloud

About this task

After configuring PingOne and Advanced Identity Cloud, test the SSO experience.

Steps

1. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page and browse or search for the applicable environment.
2. On the **Environments** page, click the environment to open the details panel.
3. In the **Connected Services** section, click **PingOne Advanced Identity Cloud**.

Result

The Advanced Identity Cloud admin UI opens.

Inviting additional PingOne Advanced Identity Cloud administrators

About this task

After verifying the connection and gaining SSO access to the Advanced Identity Cloud tenant, the PingOne Advanced Identity Cloud Super Admin can invite additional Advanced Identity Cloud Super Admins and Tenant Admins to access the Advanced Identity Cloud tenant.

Copyright © 2025 Ping Identity Corporation

Steps

- In the PingOne admin console, add admins with SSO access to the tenant.

  These users can be assigned either the Advanced Identity Cloud Super Admin or Advanced Identity Cloud Tenant Admin role for the Advanced Identity Cloud tenant.

Next steps

Repeat the configuration steps for each Advanced Identity Cloud tenant environment for which you want to set up SSO access from PingOne.

Setting up SSO to PingOne for Enterprise or PingID

If your organization has set up PingOne for Enterprise, you can use single sign-on (SSO) from the PingOne admin console to the PingOne for Enterprise tenant. This allows organizations with multiple instances of PingOne for Enterprise or PingID to keep track of each environment without having to use a unique email address for each sign-on.

Before you begin

To set up SSO to PingOne for Enterprise, you must have the Organization Admin role assigned in PingOne. Learn more in Administrator Roles.

About this task

You'll use SSO to PingOne for Enterprise by selecting the **Enable SSO** option on the sign-on page. Although user mapping is accomplished by an administrator signing on with an email address and password, SSO is set up using OpenID Connect (OIDC).

Steps

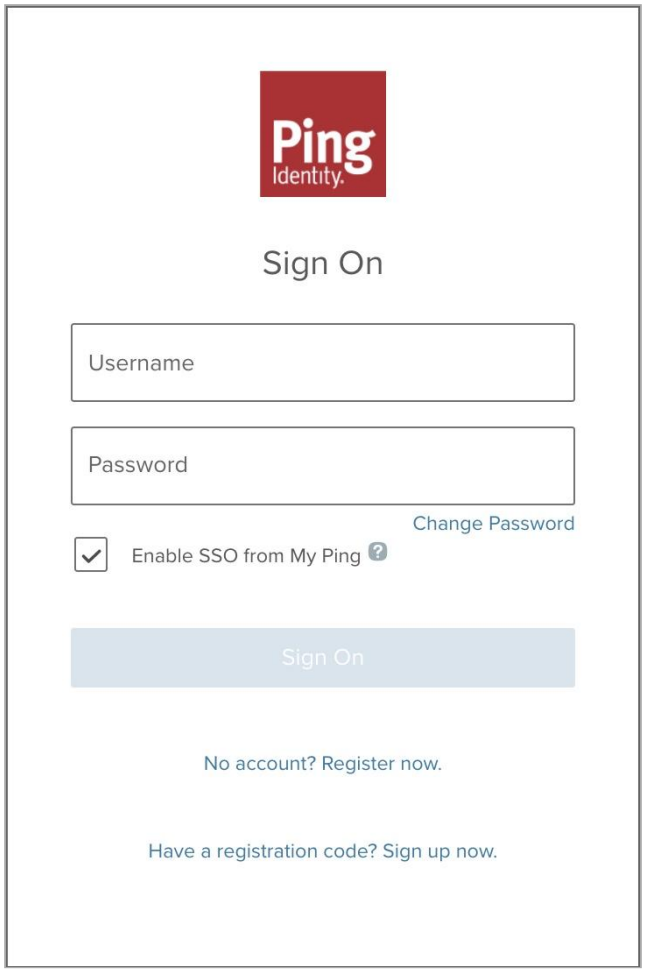
1. In the PingOne admin console, go to the **Overview** page.
2. In the **Services** section, click the **PingOne for Enterprise** icon or **PingID** icon.

   > **Note**
   >
   > If you don't see the **PingOne for Enterprise** or **PingID** icons, your organization doesn't have those services configured. Learn more in Building solutions.

   Result:

   The **Sign On** window opens.

Copyright © 2025 Ping Identity Corporation



3. Enter your username and password.
4. Select the **Enable SSO from My Ping** checkbox.

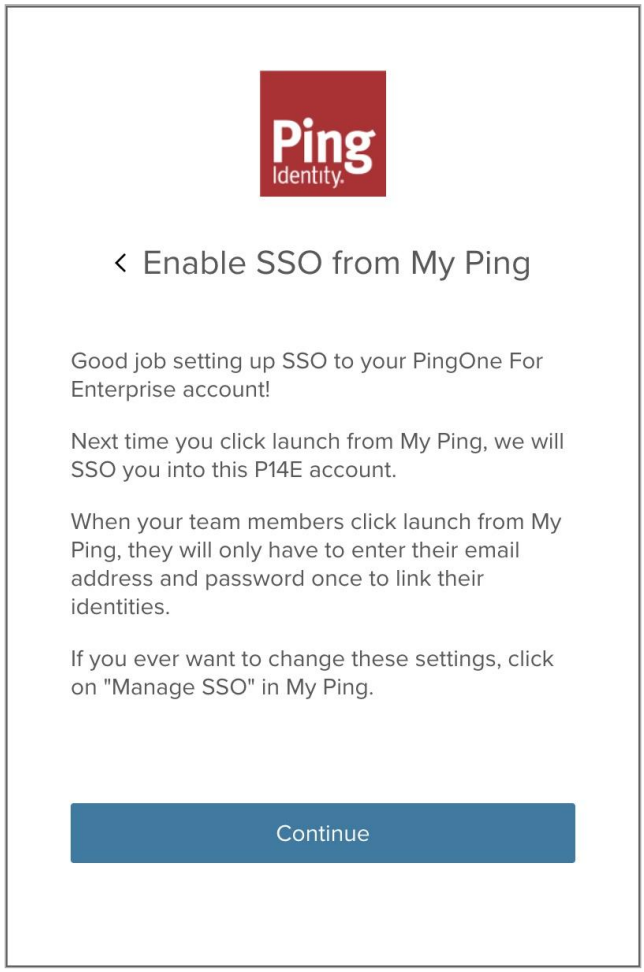
> **Note**
> This checkbox displays only if you have an Organization Admin role.

5. Click **Sign On**.

   Result:

   You see the following message:

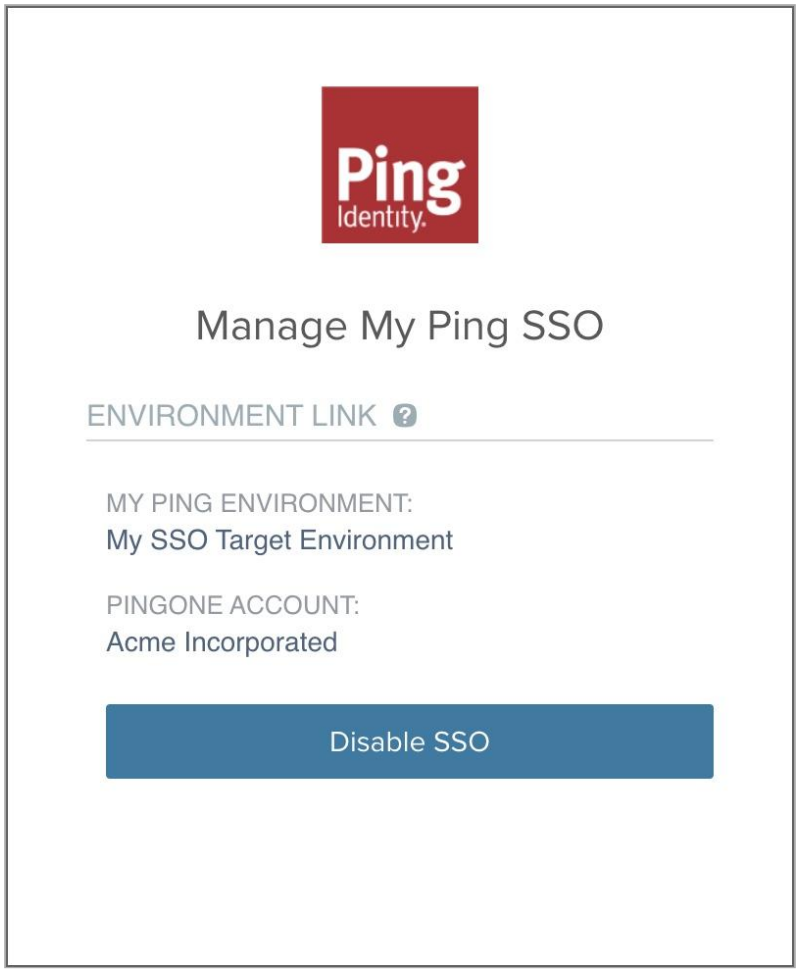
Copyright © 2025 Ping Identity Corporation



6. Click **Continue**.
7. To remove the SSO link to your account or map to a different account, click the **Manage SSO** link.

   The **Manage SSO** link allows you to unlink your username.
8. If you have the Organization Admin role and you want to unlink the environment for all administrator users, click **Disable SSO**.

Copyright © 2025 Ping Identity Corporation



Strong Authentication (MFA)

Multi-factor authentication (MFA) is a service that enables Customer and Workforce users to securely authenticate using a range of authentication methods.

Copyright © 2025 Ping Identity Corporation

Getting started with strong authentication (MFA)

What do you want to do?

- Start a PingOne trial
- Create an new environment for strong authentication (MFA)
- Integrate an existing PingID account or PingOne environment for MFA

What do you want to know?

- What is strong authentication (MFA)?
- Overview of authentication methods
- What is the difference between PingID and PingOne MFA?
- What is a typical strong authentication (MFA) workflow?

Configuring strong authentication

- Configure strong authentication methods
- Configure an MFA policy for strong authentication
- Create an Authentication policy
- Configure PingID policy
- Configure PingID Offline MFA
- Configure a passwordless Windows login application in PingOne
- Strong authentication (MFA) integrations
- Strong authentication monitoring and dashboards

Copyright © 2025 Ping Identity Corporation

Managing PingID in PingOne

- Manage PingID devices through MyAccount
- Bypass MFA for a specific user
- PingID language support
- PingID user life cycle management

Troubleshooting

- Audit logs
- System status
- Knowledge Base

Developer resources

- Get started with PingOne APIs
- PingOne Platform API Reference - PingOne MFA
- PingOne MFA Native SDK

Further resources

All other actions are managed by the PingID admin portal. Learn more in the PingID Administration Guide

Copyright © 2025 Ping Identity Corporation

Licenses and Platform Limits

PingOne licenses define the entitlements a customer has the right to use. That is, which PingOne services, in what quantities, and for what period of time.

If you sign up for Try Ping at www.pingidentity.com/en/try-ping.html, you'll get an organization and two licenses that are valid for 30 days.

- Admin license. Contains the entitlements for user administration and sign-on functionality to the Admin Portal.
- Trial license. Allows the customer to evaluate the functionality of all PingOne services for 30 days.

If you purchase one or more services, you will get a paid license to replace the trial license.

PingOne services are additive and can be used in various combinations to create a single solution. The PingOne platform operates on the principle of one license per environment, so to use multiple products in the same environment, your license must include all the products you want to use together. For more information, see Standard license types or contact Ping Identity Sales at www.pingidentity.com/en/company/contact-sales.html.

Viewing your licenses

Use the **License** page to view the details of your PingOne license and usage. Unlike some other software products, PingOne licenses are not contained in a file, but are records tracked directly in the Admin Portal.

Steps

1. Click the Ping Identity logo in the upper left side of the PingOne admin console.
2. Click **Licenses**.

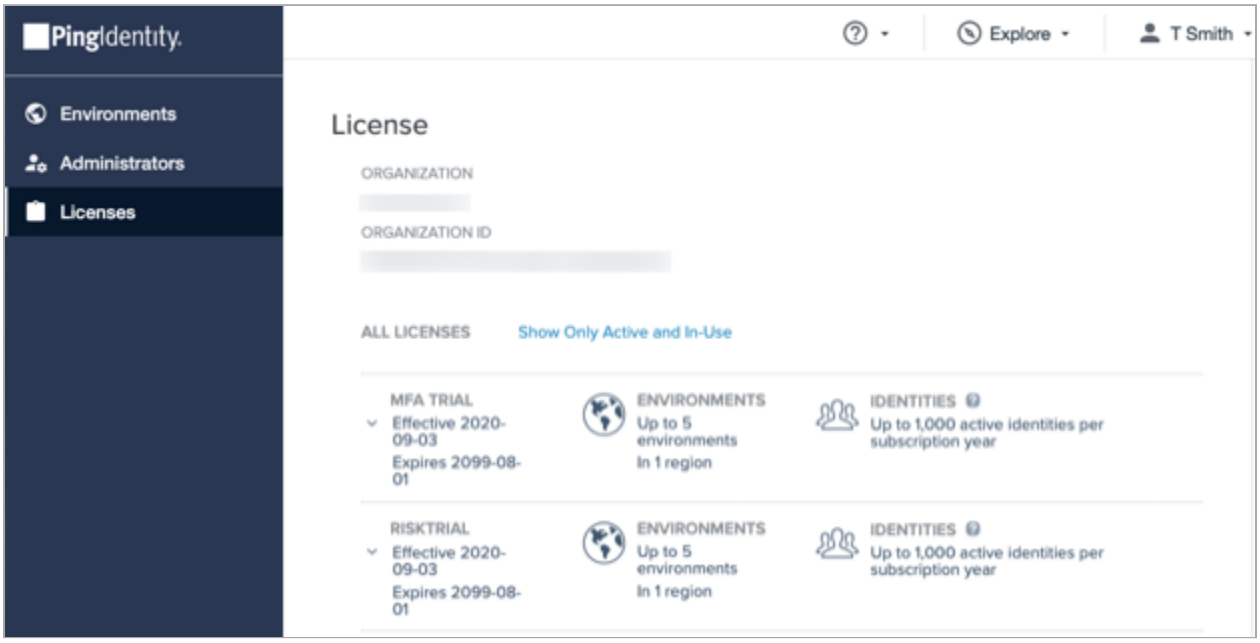
> **Note**
>
> The list shows only active licenses by default. To see expired licenses, click the **Show All Licenses** link.

Result

PingOne license details include:

- Identities
- Environments
- Expiration
- Renewal

Copyright © 2025 Ping Identity Corporation



License assignment

If you have more than one active license, use the **Licenses** page to change the association between your environments and your licenses.

A license can be associated with multiple environments, but an environment can be associated with only one license. Expanding the details on a license shows the environments to which that license is currently assigned.

The license details can help you determine if you need to purchase separate PingOne solutions, such as one for workforce and one for external customers. You can reassign licenses by clicking the **Re-assign** icon for the appropriate environment and then selecting a different active license. PingOne will not allow you to reassign an environment to a license that does not contain enough services.

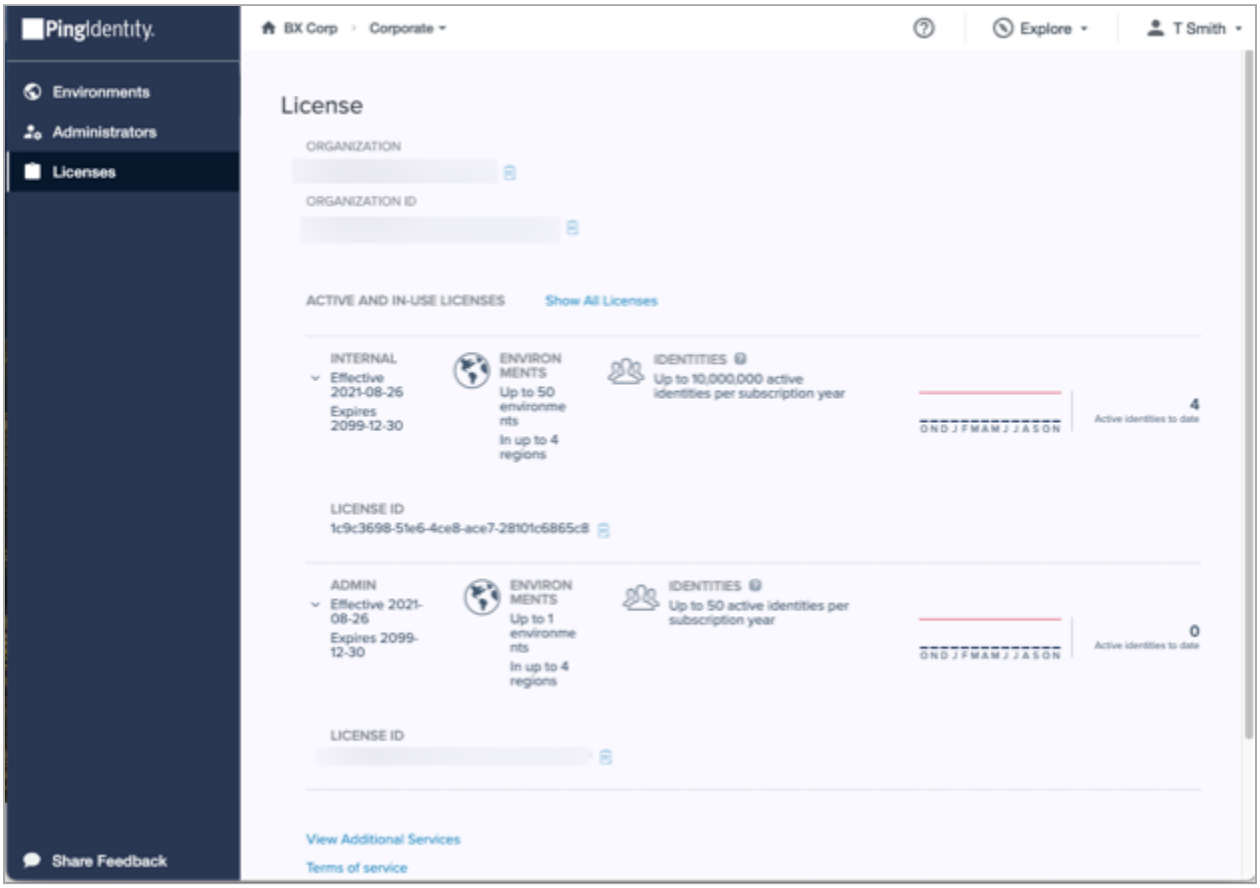
Each license supports a specific number of environments that can be associated with it at any given time. You will see a warning if you exceed that limit.

You can also assign licenses from the **Licenses** page. The console shows only licenses that are sufficient for the set of PingOne services that are configured for the selected environment. You cannot choose a license that includes fewer services than the environment is using.

For example, if you create a solution under a trial license using both MFA and Protect functionality, when you try to assign a paid license to that environment, the only licenses that are shown are those that entitle at least MFA and Protect features. Because an MFA-only license would be insufficient, it would not show in the list.

> **Note**
>
> You cannot change the license associated with the **Administrators** environment.

Copyright © 2025 Ping Identity Corporation



> **Note**
>
> You can also see the license assigned to an environment on the **Environments** page by going to **Settings > Environment Properties**.

Standard license types

PingOne includes several different types of licenses.

License name	Description
ADMIN	Includes all the features needed to administer the PingOne Admin Console, such as creating environments and users within environments. An Admin environment is automatically created for each trial.
TRIAL	Allows the customer to evaluate the functionality of all PingOne services for 30 days. The trial license is created by signing up for Try Ping at www.pingidentity.com/en/try-ping.html.
SOLUTION	Includes no PingOne services; but can enable a PingOne environment for integrating non-PingOne products.

Copyright © 2025 Ping Identity Corporation

License name	Description
JIT_TRIAL	Intended for customers that have paid licenses, but want to try other products within the organization. The JIT trial license is automatically generated when a new environment is created, if one or more trial services are selected for the environment.
Other license packages	All paid services have licenses corresponding to the service name.
Combo licenses	A single license that contains entitlements for multiple services, so that the services can be used together in a single environment. The name of the license shows the services it contains.

License FAQ

The following section contains common questions and answers about PingOne licenses.

I just purchased a PingOne Service, why am I being told I cannot add that service to my environment?

Ensure that the environment is associated with the new license. For example, if you have a PingOne MFA license and purchase PingOne Protect as an additional service, to add Protect features into the MFA solution, your MFA license would have had to be upgraded to be an MFA-Protect license. A new Protect-only license is not enough, because you cannot assign more than one license to an environment.

If the new license does not include all of the other services you are using in that environment, contact Ping Identity Sales at www.pingidentity.com/en/company/contact-sales.html.

I have paid services, but now want to try another service

You can create a trial environment for any product in combination with your paid services by creating a new environment. Select the paid services you want to use, then select the **View Trials** slider to see all the services you do not have licensed. Adding trial services to an environment will generate a 30-day trial license.

I just purchased a PingOne Service, but I still see a banner saying my license has expired

Ensure that the environment is associated with the new license. See License assignment. If the message persists, you might have other environments that are still associated with the earlier license. You can associate those environments with the new license or any other current license you might have that provides the same set of PingOne services.

I can't create any more environments

Licenses define limits for the maximum number of environments that it can be assigned to. If you need to create additional environments, contact Ping Identity Sales at www.pingidentity.com/en/company/contact-sales.html.

I can't create any more identities

Licenses have a soft limit and a hard limit for the maximum number of identities you can create. User limits are based on the total number of identities across all of the environments assigned to a license. Learn more in Licenses and identity limits.

Copyright © 2025 Ping Identity Corporation

Licenses and identity limits

Ping Identity products have specific licensing limits that offer crucial protection for both customers and Ping Identity. Use the following information to understand the various licensing constraints associated with Ping Identity products and navigate and optimize their usage within the defined boundaries.

PingOne

A PingOne license includes a soft limit and a hard limit for the maximum number of identities. A license can be assigned to one or more environments, and user limits are based on the total number of identities across all of the environments assigned to a license.

The soft limit is usually 12 times the licensed Monthly Active Users (MAU) or Average Annual Users (AAU) of yourPingOnesubscription. You can continue to add users when you've reached the soft limit, but the system will display a warning message.

The hard limit is 10% more than the soft limit, up to the maximum limit of 50 million identities. This strict limit serves as a hard cap that you can't exceed unless you have obtained explicit, written approval from Ping Identity. The need for this exception might arise if your subscribed MAU would theoretically allow for a hard limit exceeding 50 million identities, based on your contracted service levels. When you hit your license's hard limit or reach 50 million identities, whichever is lower, you can no longer add users without contacting Ping Identity Sales to change your license.

Example

If your licensed MAU is 1 million, the soft limit for your license is 12 million users. The hard limit is 13.2 million users.

- **Approaching limit**: At 10.8 million users, or 90% of the soft limit for your license, the admin console displays a warning message stating that you are at 90% of your allowed users. At this point, you can continue to add users.
- **Limit reached**: When you reach the soft limit of 12 million users, the admin console displays another warning message stating that you have reached 100% of your allowed users. You can still add users.
- **Limit exceeded**: When you reach 13.2 million users, which is the hard limit for the license, the admin console displays a message stating that you can no longer add users and must upgrade your license.

To receive email notifications when you are approaching these limits, configure the following alerts in **Monitoring > Alerts**:

- **Approaching User License Limit**: Triggers an alert when you reach 90% of the soft limit for your license.
- **User License Limit Reached**: Triggers an alert when you reach 100% of the soft limit for your license.
- **User License Limit Exceeded**: Triggers an alert when you reach the hard limit for the license and can no longer add users.

Learn more in Alerts.

PingOne Authorize

PingOne Authorize is licensed by identities, and a fair-use transaction allowance is defined for each identity tier. The fair-use transaction allowance corresponds to the total number of licensed identities specified in your PingOne subscription.

For some authorization use cases (for example, when permissions are checked for every page access or operation), the volume of authorization events can be significantly higher than the volume of authentication events. The fair-use transaction allowance provides you and Ping Identity with a shared expectation about the volume of authorization traffic. If this limit isn't sufficient, contact Ping Identity Sales about increasing the monthly allowance.

Copyright © 2025 Ping Identity Corporation

PingOne DaVinci

PingOne DaVinci is licensed by identities and transactions based on flow invocations. Your limits will be based on one of the following two license types.

Licensed by identities

PingOne DaVinci is licensed by identities as MAU or AAU with a fair-use transaction allowance as defined in the Product terms and conditions.

The fair-use transaction allowance corresponds to the total number of licensed identities specified in your PingOne DaVinci subscription. The fair use transaction allowance provides you and Ping Identity with a shared expectation about the volume of DaVinci traffic. If the identities or fair-use limits aren't sufficient, contact Ping Identity Sales about increasing the allowance.

Licensed by transactions (flow-based)

A flow invocation occurs each time a flow (a series of one or more connector executions) is initiated in DaVinci. If a flow launches one or more subflows, the subflows do not count as additional invocations. Only the initial invocation is counted.

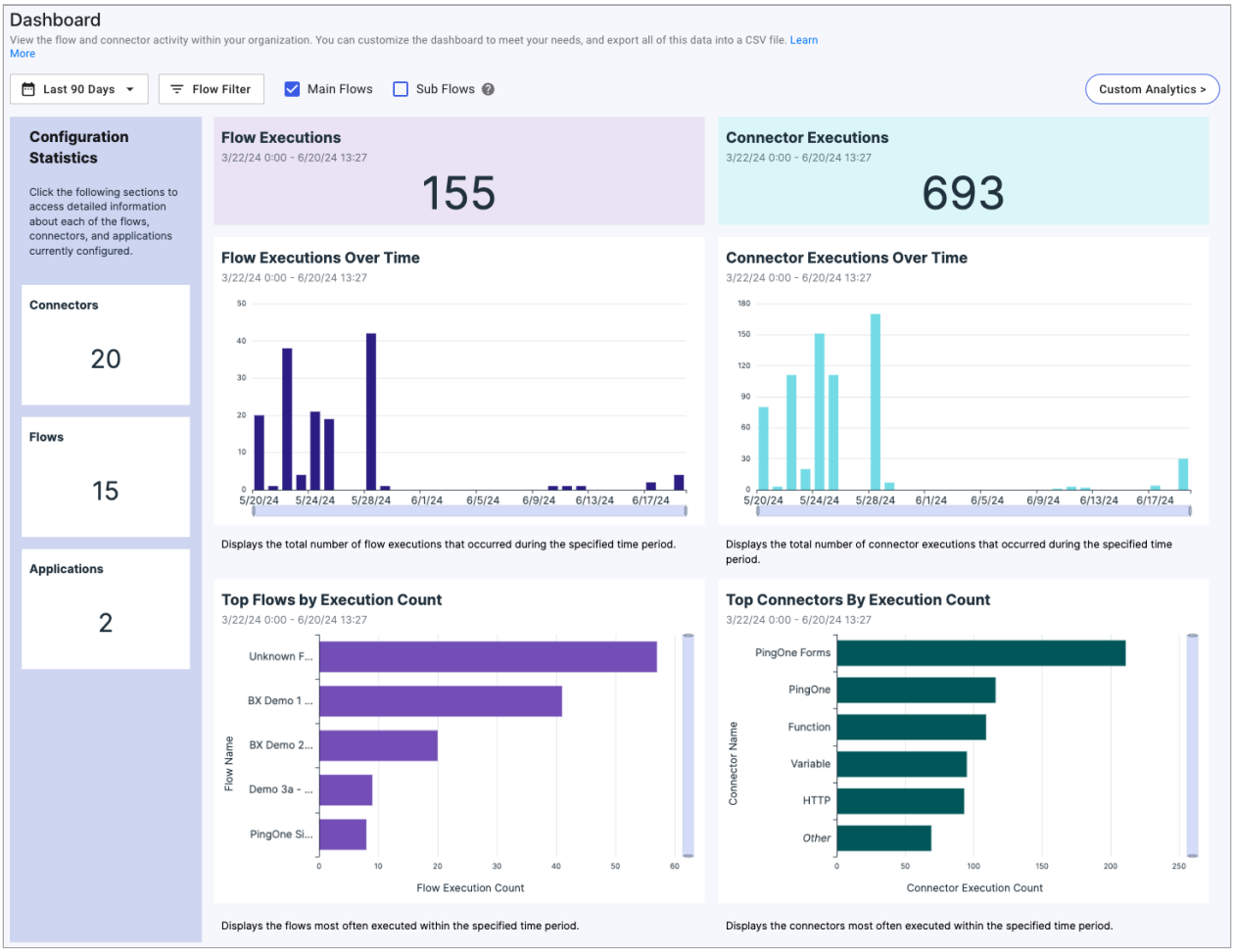
> **Note**
>
> In the product dashboard and your license, a flow invocation is represented as a flow execution, and each flow invocation counts as a flow execution.

The flow-based license comes with a fair-use transaction limit of 80 connector executions (previously referred to as API calls) per flow. There is no distinction between the types of connector executions. Ping Identity reserves the right to negotiate per-invoked flow pricing for PingOne DaVinci in the event that usage exceeds flow or connector execution volume limits set in the license. If the limit isn't sufficient, contact Ping Identity Sales about increasing volume limits as your usage increases. Learn more in DaVinci Usage Terms.

The DaVinci license shows your flow-based entitlements per subscription year.

The DaVinci dashboard shows the number of flow executions and connector executions that have occurred in a single environment. Use the total of all environment metrics to determine usage against the entitlements.

Copyright © 2025 Ping Identity Corporation



PingOne for Customers Passwordless

PingOne for Customers Passwordless is a solution bundle that is licensed by transactions based on flow invocations (learn more in the PingOne DaVinci section). It includes using PingOne Protect, PingOne SSO (including Directory), and PingOne MFA in PingOne DaVinci. This solution bundle requires usage of each product only through DaVinci flows.

PingOne standard platform limits

The PingOne platform includes default limits to ensure secure and reliable access for all of our customers.

> **Note**
>
> This is not a comprehensive list of all usage limits on PingOne. Limits on this list are subject to change. If you experience issues or have questions that aren't addressed in the following tables, contact your solution architect or open a support case in the Ping Identity Support Center.

Transactions

Type	Limit
HTTP API request header size	6 KB

Copyright © 2025 Ping Identity Corporation

Type	Limit
HTTP API requests per source IP	100 requests per second
SMS messages	50 per day per user
Email messages	50 per day per user
Gateway requests	500 per second per gateway instance
Webhook delivery	500 messages of 1 KB each per POST, 72 POSTs per second

Identity data

Type	Limit
Custom attribute schema	Maximum of 200 string attributes and 200 JSON attributes
Combined size of custom string and custom JSON attributes	Maximum is determined by the current, cumulated size of the user profile, which must not exceed 16 KB. Learn more in Custom attributes in the PingOne API documentation.

Administration

Type	Limit
Admin groups	500
Role assignments per admin group	3500
Population level role assignments	250
Role assignments per user or Worker application	3500 roles
Application level role assignments	250

Copyright © 2025 Ping Identity Corporation

Environments, populations, and groups

Type	Limit
Environments	Varies by subscription plan: • Trial plan max: 5 per organization • Platform max: ◦ 500 active environments per organization ◦ 100 environments in "Delete Pending" status per organization For limits specific to your plan, contact Support or your solution architect.
Populations	10,000 per environment
Groups	100,000 per environment
Nested groups	250 nested groups per group This limit includes the combination of nesting levels plus the number of groups at each level.
Identities	1 million per environment for trial plans, up to 50 million per environment depending on your contract
Group memberships	10,000 per identity. Due to size limits on ID tokens, the number of groups returned in a token could be lower.
PingOne Advanced Services or PingID deployments	100 per organization

Sign-on policies

Type	Limit
Sign-on policies	100 per environment
Steps/actions	21 per policy

Applications

Type	Limit
Applications (including Application Portal Links)	1000 per environment
Application attribute mappings	100 per application
Sign-on policies or DaVinci flow policies	20 per application

Copyright © 2025 Ping Identity Corporation

Type	Limit
Terms of service text	32,000 characters per revision text
Virtual server IDs (SAML applications)	200 per application

Configuration

Type	Limit
Custom domains	Paid plans only
Email customization	Paid plans only
Webhooks	50 per environment
Email trust domains	50 per environment
Themes	100 per environment
Forms	100 per environment

DaVinci flow limits

Property	Limit	Description
Resource	100	Your environment can contain a maximum of 100 of each entity type. This limitation applies to flows, variables, and connections, but not to end users. Each flow is limited to 100 stored versions.
API payload	10 MB	The maximum payload size for any API call (such as POST, GET, or DELETE) made within a flow.
Number of nodes that can be run per flow invocation	Twice the number of nodes in the flow or 70, whichever is higher	Maximum number of nodes that can be run. This limit is distinct for each flow, so if a flow launches a subflow, both flows can run a number of nodes up to this limit.
Flow timeout	Default is 5 minutes. Maximum possible is 2 days.	A timeout value for the entire flow, beginning when the flow is invoked. Editable for each flow. Learn more in Editing flow settings.

Copyright © 2025 Ping Identity Corporation

Property	Limit	Description
Flow HTTP response timeout	Default is 15 seconds. Maximum possible is 120 seconds.	A timeout value for any HTTP call made by any node in the flow. Editable for each flow. Learn more in Editing flow settings.
Node payload	1 - 10 MB (depending on the node)	The maximum size of the payload sent by a node to future nodes.

Learn more in DaVinci flow limits.

Identity providers (IdPs)

Type	Limit
IdPs	1000 per environment
IdP discovery rules	200

Gateways

Type	Limit
Gateways	20 gateways per environment
User Types	20 user types per LDAP gateway

Provisioning

Type	Limit
Revisions	1000 per environment
Stores	4196 per environment
Rules	4196 per environment
Mappings	4196 per environment

PingOne Authorize

Type	Limit
Unnamed versions	500 per environment

Copyright © 2025 Ping Identity Corporation

Type	Limit
Named versions	100 per environment
Version data size	7 MB per version
User-defined entities or configurations	4000 per environment
Managed entities or configurations	6000 per environment
Decision endpoints	30 per environment
Recent decisions	20 per decision endpoint
Service caching	Service response size: 1 MB Time to live: 24 hours maximum Learn more about service limits in Service configuration constraints.
API services	25 per environment
API operations	25 per API service
Application roles	128 per environment
Application resources	128 per environment
Application permissions	128 per environment
Application permission assignments	1024 per role

PingOne MFA

Type	Limit
Active devices	20 per user

PingOne Verify

Type	Limit
Hourly authentications	3 attempts per hour
Daily authentications	10 attempts per day

Ping Identity customers are not limited by how many verify transactions they perform. However, each of their users is limited by how many document authentications they perform.

Copyright © 2025 Ping Identity Corporation

PingOne Platform logging and reporting

PingOne includes various auditing and reporting tools for admins to monitor events in their PingOne environments.

Use the information in this section to understand the various types of logs and reporting, and options for collecting and accessing log data.

You can retrieve logs through the **Audit** page, by using webhooks, or through the API. You can also use the **Dashboards** page, the **Alerts** page, and the PingOne App for Splunk to monitor your PingOne environment.

Audit

Use the **Audit** page in the PingOne admin console to run queries on events and actions in the PingOne environment. You can limit the results to a specified time range and define which items to include in the report. PingOne maintains logs for 90 days by default.

To retain PingOne data for longer than 90 days, set up webhooks to stream the data to your own repository and configure your own retention policy. Learn more in Webhooks.

Historical dashboard data and administration configuration change data is retained for two years. Additionally, PingOne DaVinci and DaVinci flow data is not governed by this retention policy.

Learn more in Audit.

Webhooks

Use the **Webhooks** page in the PingOne admin console to set up subscriptions.

When an event of interest occurs in PingOne, the event is pushed from PingOne to a third-party monitoring system. Webhooks are available in a Splunk-friendly format, a New-Relic-friendly format, and the Ping activity format, which is a versatile, generic JSON format also used by the PingOne API for accessing event data.

Learn more in Webhooks.

PingOne API

Use the PingOne `User Activities` API to monitor user activities in PingOne. The service uses stream processors that listen to `users` and `login_attempts` events. These events are collected and presented by time period.

Learn more in User activities in the PingOne Platform API Reference.

PingOne App for Splunk

Use the PingOne App for Splunk to correlate your PingOne webhook data into a meaningful dashboard. Create custom dashboards and reports, monitor activity data, and analyze event data over time.

Learn more in Installing the PingOne app for Splunk.

Copyright © 2025 Ping Identity Corporation

Dashboards

Use the **Dashboards** page in the PingOne console to view and monitor activities for a particular service. Each capability, such as Authentication, Authorization, Identity Verification, and so on, has its own dashboard.

Learn more in Dashboards.

Alerts

Use the **Alerts** page in the PingOne console to set up alert messages based on the status of certain resources. The alerts are limited to events related to certificates, key pairs, and gateways.

Learn more in Alerts.

PingOne Services logging and reporting

In addition to the core PingOne platform logging, each PingOne service includes a variety of logs that administrators can use to monitor their environments.

PingOne DaVinci logging

PingOne DaVinci includes manual logging, a Flow Analytics connector, and a Webhook connector. Learn more in:

- Debugging and Analytics
- Flow Analytics Connector
- Webhook Connector
- Dashboard

PingOne Protect logging

For PingOne Protect, you can use the native logging in the PingOne admin console. You can also view real-time data on the **Threat Protection Dashboard**. Learn more in Threat Protection Dashboard.

PingOne SSO and PingOne Directory logging

For PingOne SSO, you can use the native logging in the PingOne admin console. You can also view real-time data on the **Authentication Dashboard**. Learn more in Authentication dashboard.

PingOne Verify logging

For PingOne Verify, you can use the native logging in the PingOne admin console. You can also view real-time data on the **Identity Verification Dashboard**. Learn more in Identity Verification Dashboard.

PingOne Verify also includes webhooks and metrics through the PingOne API. Learn more in:

- Subscriptions in the PingOne Platform API Reference

Copyright © 2025 Ping Identity Corporation

- Verification Metrics in the PingOne Platform API Reference

PingOne MFA logging

For PingOne MFA, you can use the native logging in the PingOne admin console. You can also view real-time data on the **MFA Dashboard**. Learn more in MFA dashboard.

PingOne MFA also includes device logs that you can access through the PingOne API. Learn more in MFA Device Authentications in the PingOne Platform API Reference.

PingOne Authorize logging

For PingOne Authorize, you can use the native logging in the PingOne admin console. You can also view real-time data on the **Authorization Dashboard**. Learn more in:

- PingOne Authorize event monitoring
- Authorization Dashboard

Copyright © 2025 Ping Identity Corporation

PingOne Tutorials

These tutorials guide you through common tasks in PingOne and its associated services. When you complete a tutorial, you can test the result.

PingOne

PingOne tutorials guide you through common configuration tasks.

- Customize the look and feel of PingOne authentication pages: Learn how to customize the look and feel of your sign-on form to align with your organization's theme.
- Add a SAML application: Learn how to quickly add your SAML application for access through PingOne.
- Build a custom sign-on policy: Learn how to configure a custom sign-on policy that fits your organization.
- Create a group: Learn how to create a group with either manual or dynamic membership to better manage your users.
- Control user access: Learn how to control user access to specific applications and resources using groups.
- Add custom attributes to a user: Learn how to add custom attributes to your users to determine the types of data that are stored for each user in PingOne.
- Configure a multi-factor authentication experience using PingOne and PingID: Learn how to develop a simple multi-factor authentication (MFA) experience using PingOne and PingID.
- Configure a basic passwordless login experience using PingOne and PingOne MFA: Learn how to develop a basic passwordless login experience using PingOne and PingOne MFA.
- Sync users between two environments: Learn how to synchronize users between two different PingOne environments using a Worker app and SCIM provisioning.

PingOne Authorize

Authorization tutorials guide you through the capabilities of PingOne Authorize.

- Build dynamic authorization policies: Learn how to use the dynamic authorization capabilities of PingOne Authorize.
- Manage API access: Learn how to use the API Access Management capabilities of PingOne Authorize.

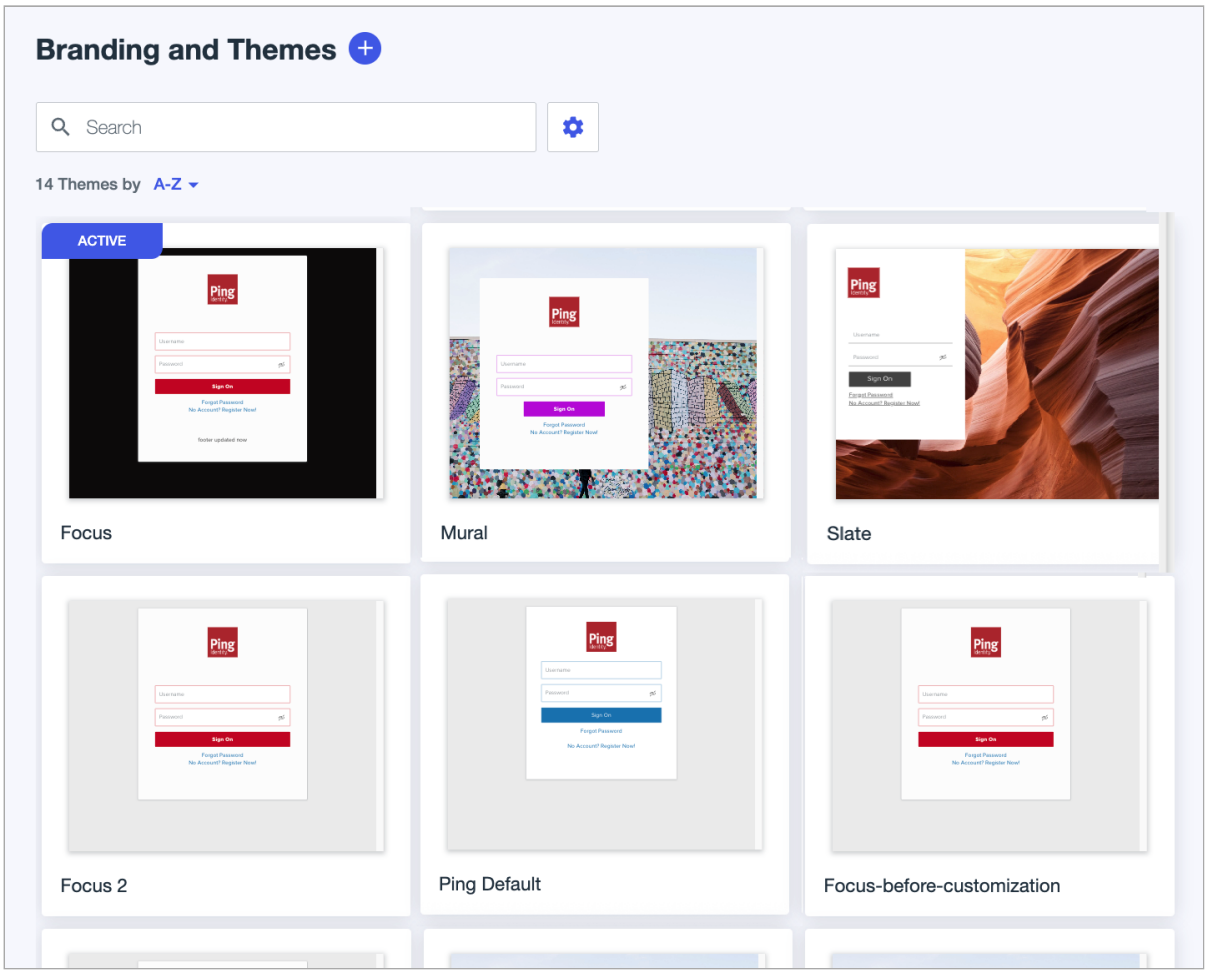
Copyright © 2025 Ping Identity Corporation

Customize the look and feel of PingOne authentication pages

This tutorial walks you through ways to customize your PingOne authentication experience to better align with your organization's brand. In this tutorial, you'll change the look and feel of registration and sign-on forms in PingOne by applying your own branding and making stylistic changes using a theme.

Steps

1. In the PingOne admin console, go to **User Experience** > **Branding and Themes**.



2. Click the ⚙ icon to open the **Global Settings** panel.

   These settings apply to all themes in the environment.

3. Enter or edit the branding details:

   - **Company name**: The name of your company as you want it to appear to end users.

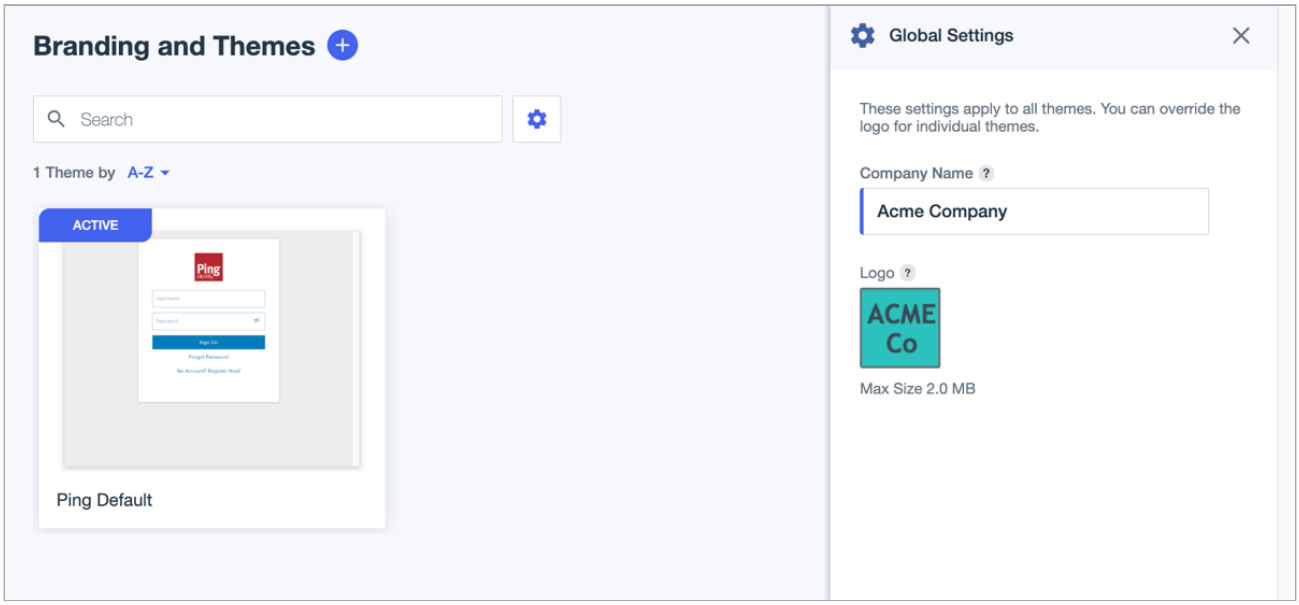
     Enter `Acme Company`.

   - **Logo**: An image to represent the environment to end users.

Copyright © 2025 Ping Identity Corporation

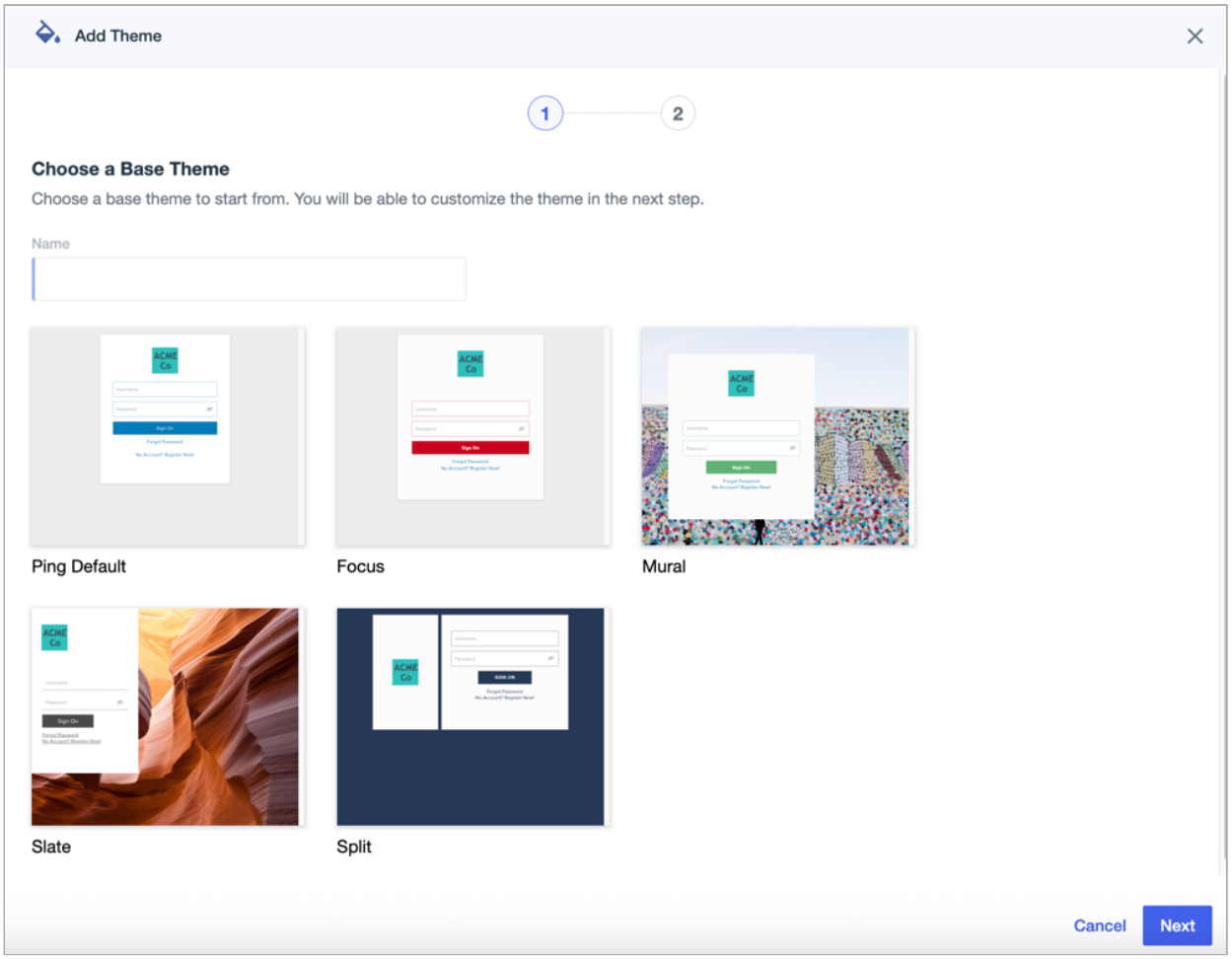
Click the image and select **Upload a New Image** to upload an image from your computer to use as the Acme Company logo. This logo is used when you create a new theme, but doesn't apply to existing themes.

> **Note**
>
> The maximum logo size is 2 MB.



4. Click **Save**.
5. Click the **+** icon to add a new theme.
6. On the **Choose a Base Theme** page, click **Slate**.

Copyright © 2025 Ping Identity Corporation



You can see that the logo for the base themes matches what you uploaded in **Global Settings**.

7. In the **Name** field, enter `Acme Theme`.

8. Click **Next** and select the tabs on the **Customize** page to review and change settings for the different page types.

   Page previews display in the left panel, and you configure settings in the **Theme Styles** panel on the right. The previews update in real time as you make changes to the settings. To switch between previews for desktop or mobile devices, click the **Desktop** or **Mobile** icon ( ).

9. Let's update a few settings for the sign-on and registration forms:

   1. Click the **Authentication Policy** tab.

   2. In the right panel, locate the **Button** section, select **Button Fill** and select one of the preconfigured color options.

      For the purposes of this tutorial, we selected aqua. Notice the color of the button in the preview panel changes to match your selection.

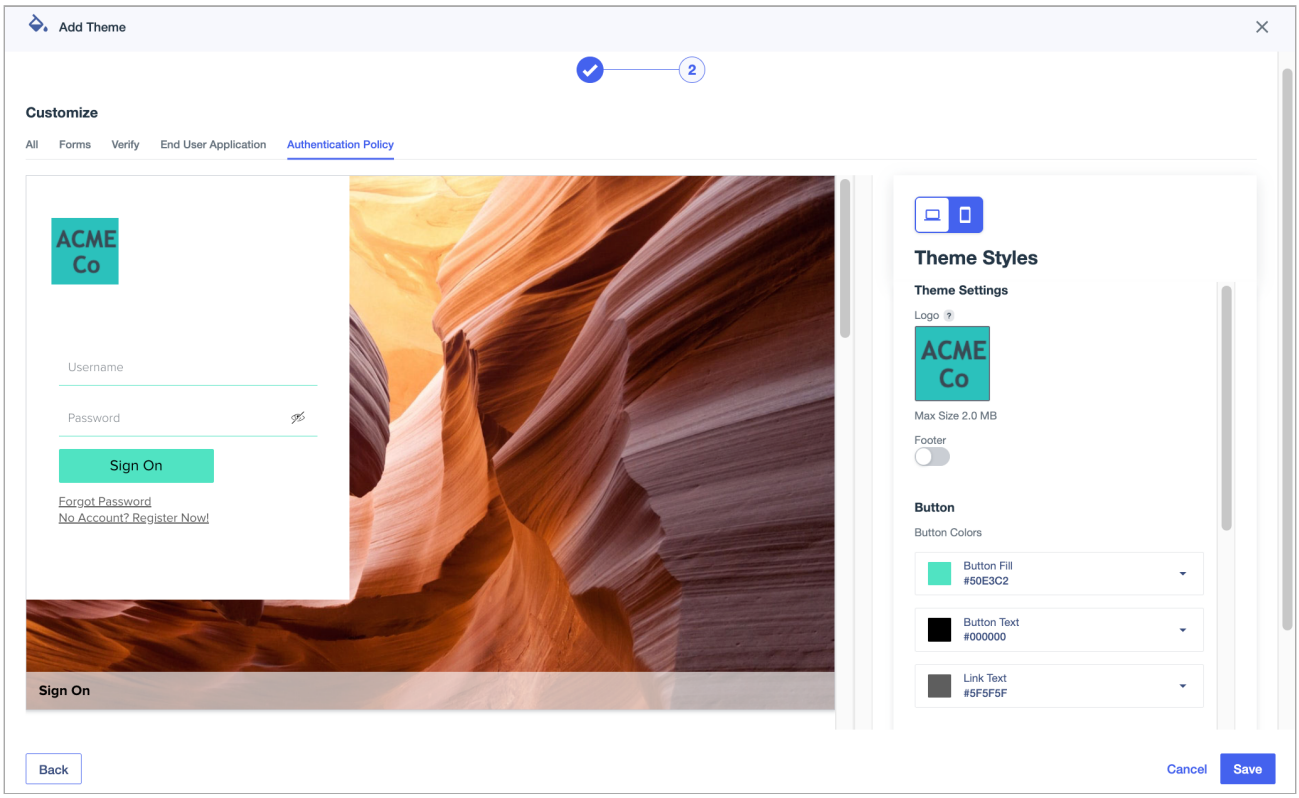
      Click outside of the color picker to return to the settings panel.

   3. Click **Button Text** and select another color.

      The color of the text inside the button update based on your selection.

Copyright © 2025 Ping Identity Corporation

For the purposes of this tutorial, we selected black.

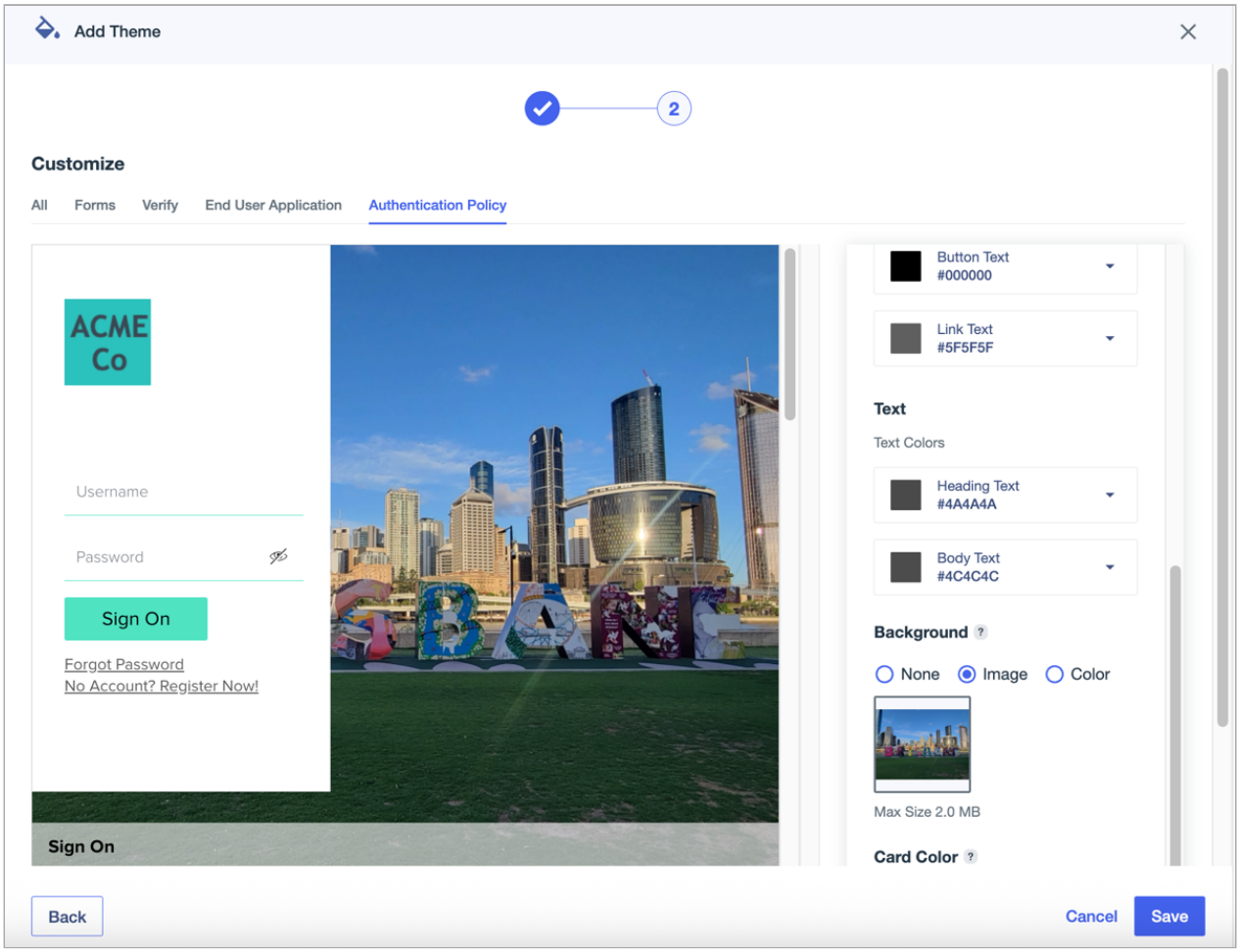


4. Scroll to the **Background** section, click the image, and select **Upload New Image**.
5. Select an image on your computer and click **Open**.

   Result:

   The background image for the theme updates.

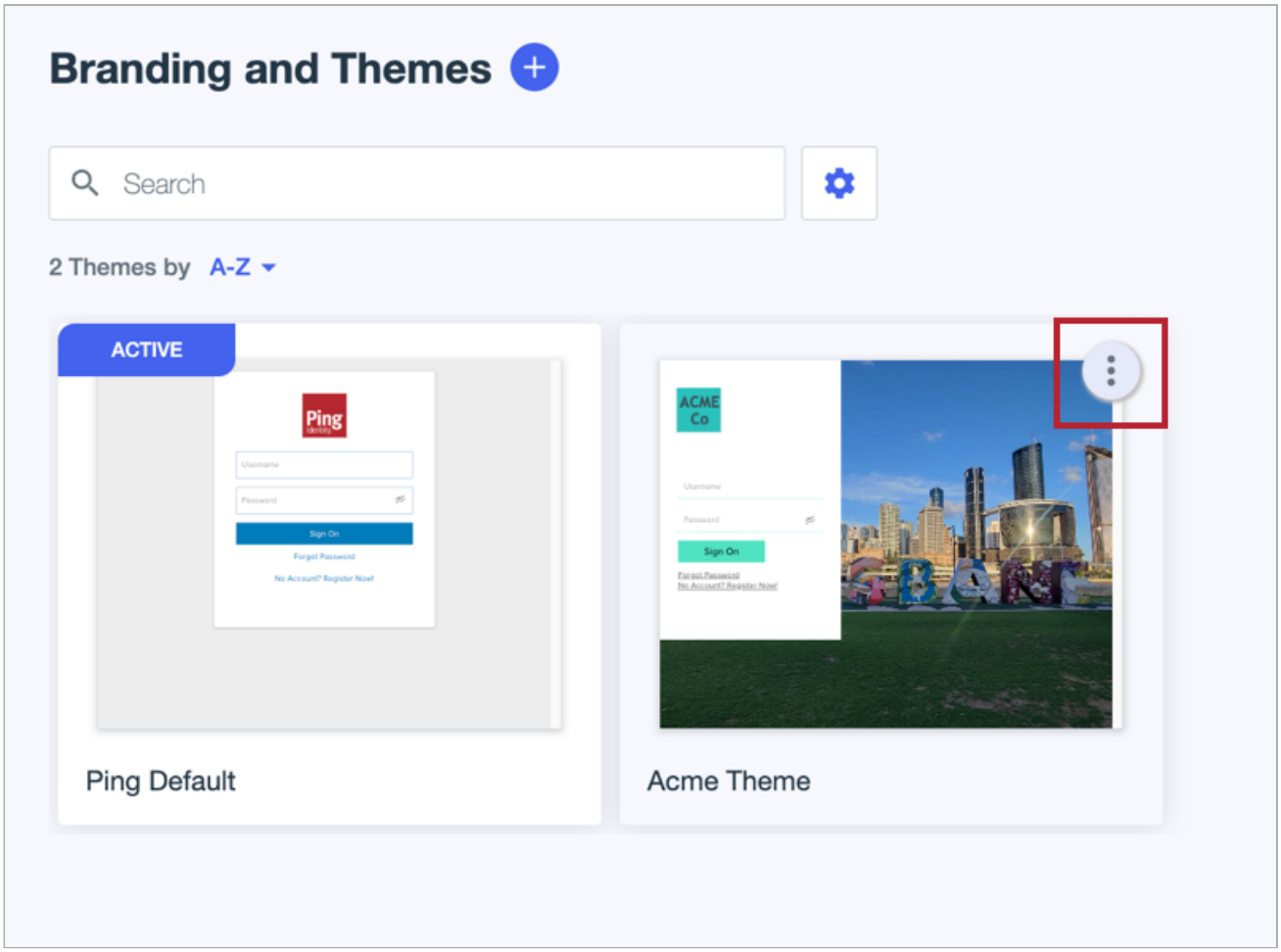
Copyright © 2025 Ping Identity Corporation



10. Click **Save**.

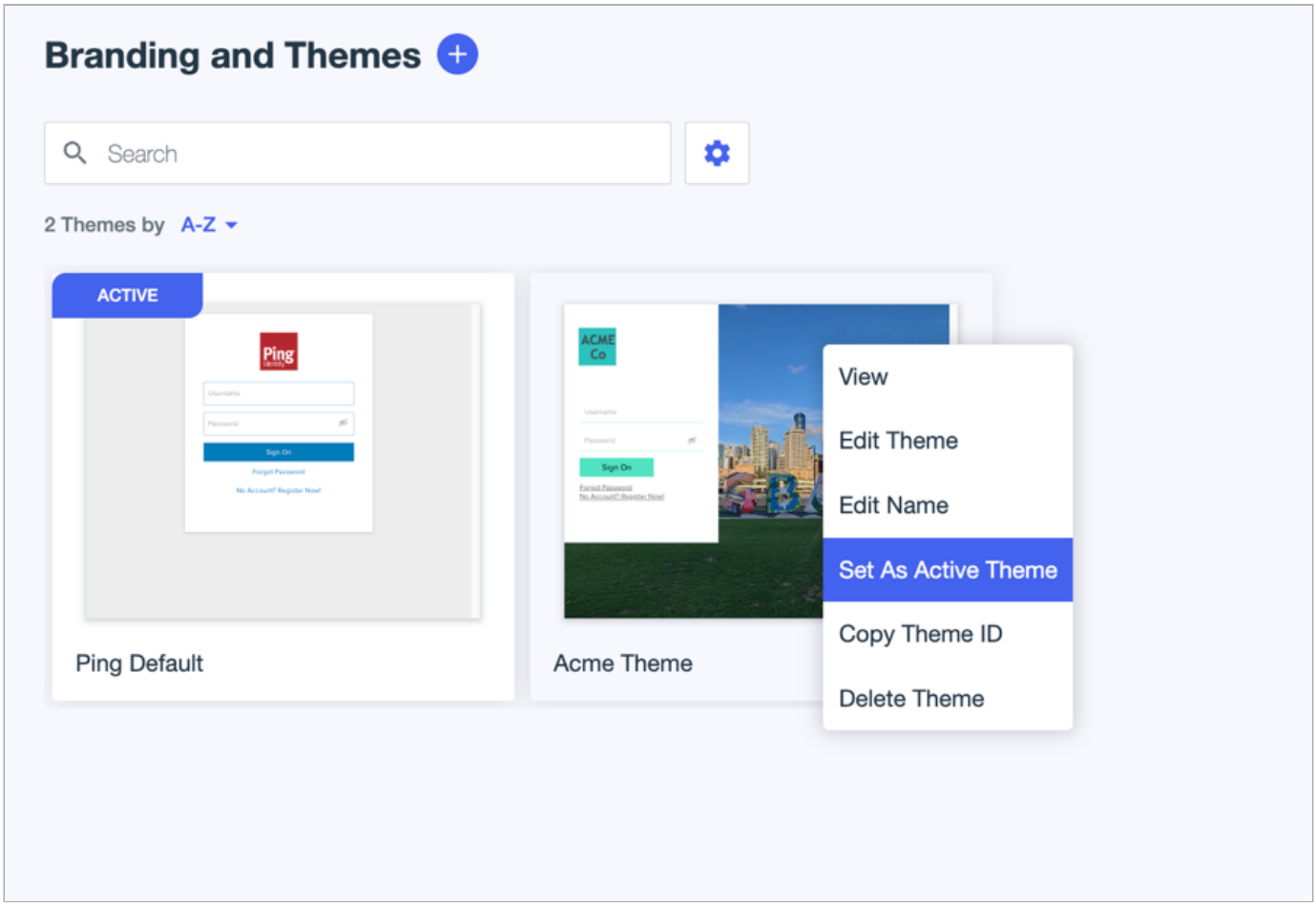
11. On the **Branding and Themes** page, hover over the **Acme Theme** to display the **More Options** (⋮) icon in the right corner.

Copyright © 2025 Ping Identity Corporation



12. Click the **More Options** (⋮) icon and select **Set As Active Theme**.

Copyright © 2025 Ping Identity Corporation



Result

Acme Theme is now the active theme for the environment.

> **Note**
>
> It can take up to 5 minutes for the new theme to appear to end users.

Learn More

Learn more about the many options for theme configuration in Branding and themes.

Add a SAML application

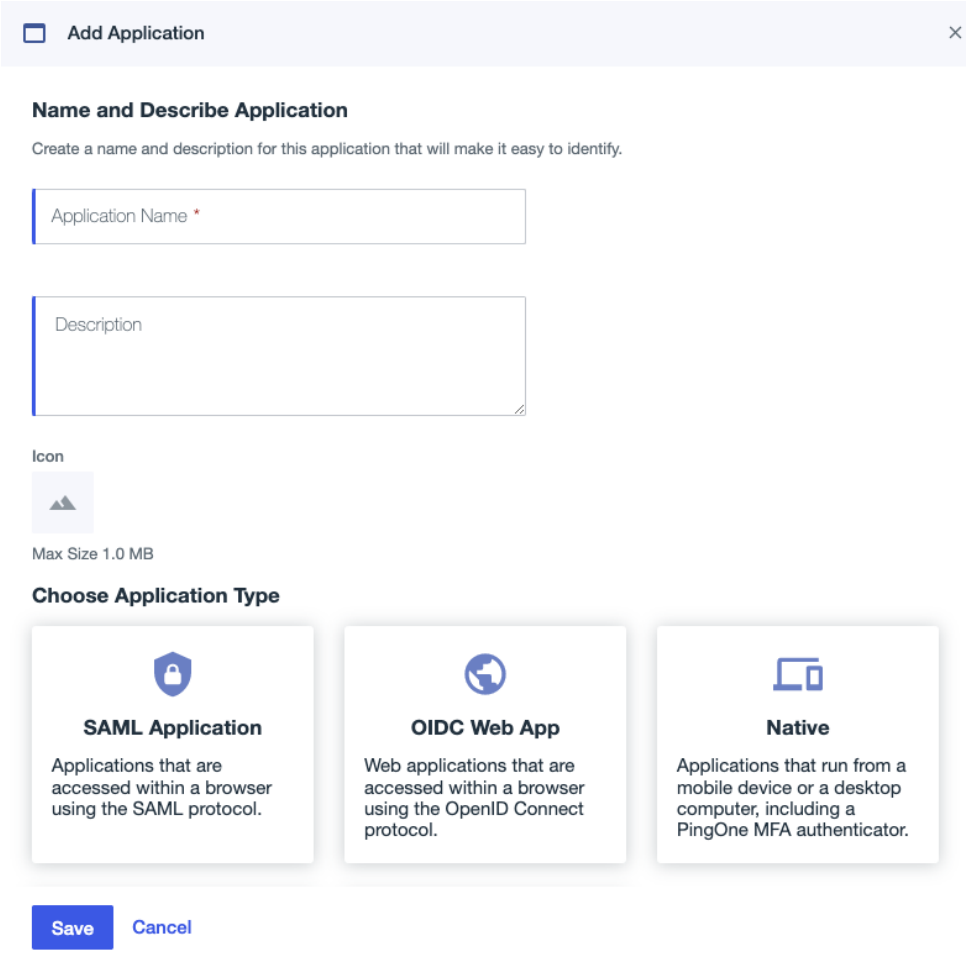
Learn how to add your SAML application in PingOne.

About this task

This tutorial walks you through the addition of your SAML application in PingOne so that you can customize and control access.

Copyright © 2025 Ping Identity Corporation

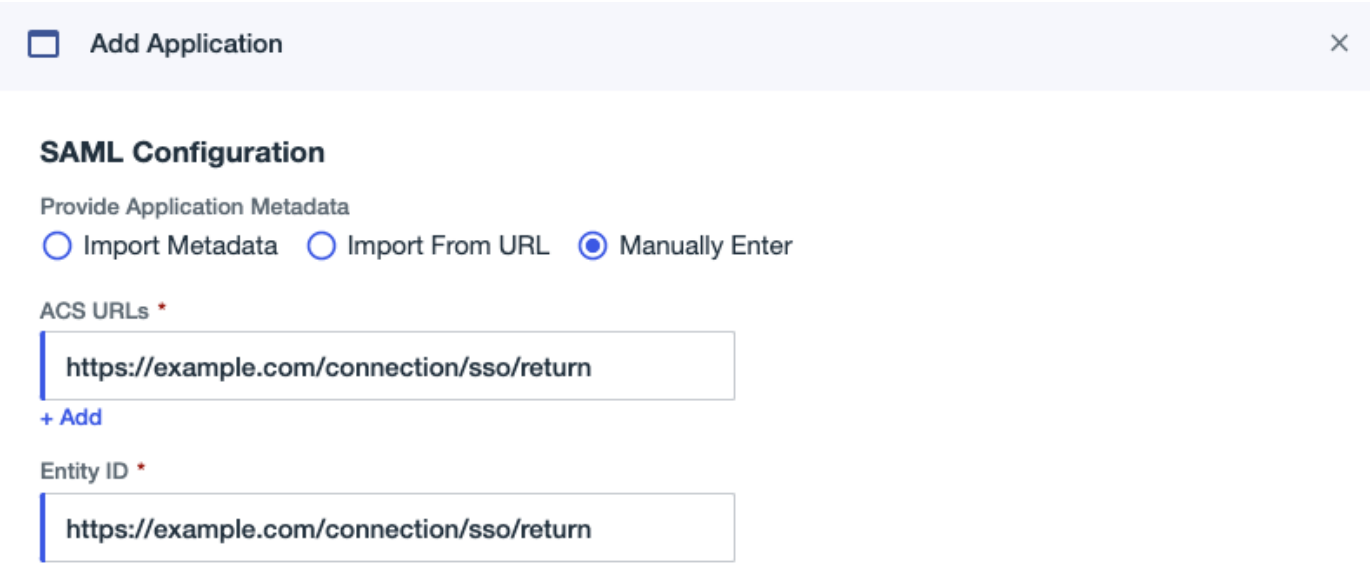
Steps

1. Go to **Applications** > **Applications**.
2. 

   Click the **+** icon.
3. Create the application profile by entering the following:
   - **Application name**: A unique identifier for the application.
   - **Description** (optional): A brief characterization of the application.
   - **Icon** (optional): A graphic representation of the application. Use a file up to 1MB in JPG, JPEG, GIF, or PNG format.
4. For **Choose application type**, click **SAML application**.

Copyright © 2025 Ping Identity Corporation

5. Click **Configure**.



6. For **SAML configuration**, select **Manually enter**.

> **Note**
>
> Alternatively, you can select **Import Metadata** to import the configuration settings from a local SAML configuration file or **Import From URL** to import the configuration from an internet address.

7. Enter the **ACS URL**.

> **Note**
>
> The assertion consumer service (ACS) URL is a location to which single sign-on (SSO) tokens are sent.

8. Enter the **Entity ID**.

> **Tip**
>
> The entity ID is a unique identifier for your application. For example, `my_app` .

9. Click **Save**.

10. On the **Applications** page, click the slider on the right to enable the application.

> **Note**
>
> You can review the configuration by clicking the application entry to open the details panel. You can also specify more options, like attribute mapping. See Editing an application - SAML.

Next steps

To test the application, go to the **Configuration** tab and copy the **Initiate Single Sign-on URL**. Paste the URL into a new private browser window, access the page, and sign on.

Copyright © 2025 Ping Identity Corporation

> **Tip**
> This task requires that at least one user account be created. For more information, see Adding a user.

Build a custom sign-on policy

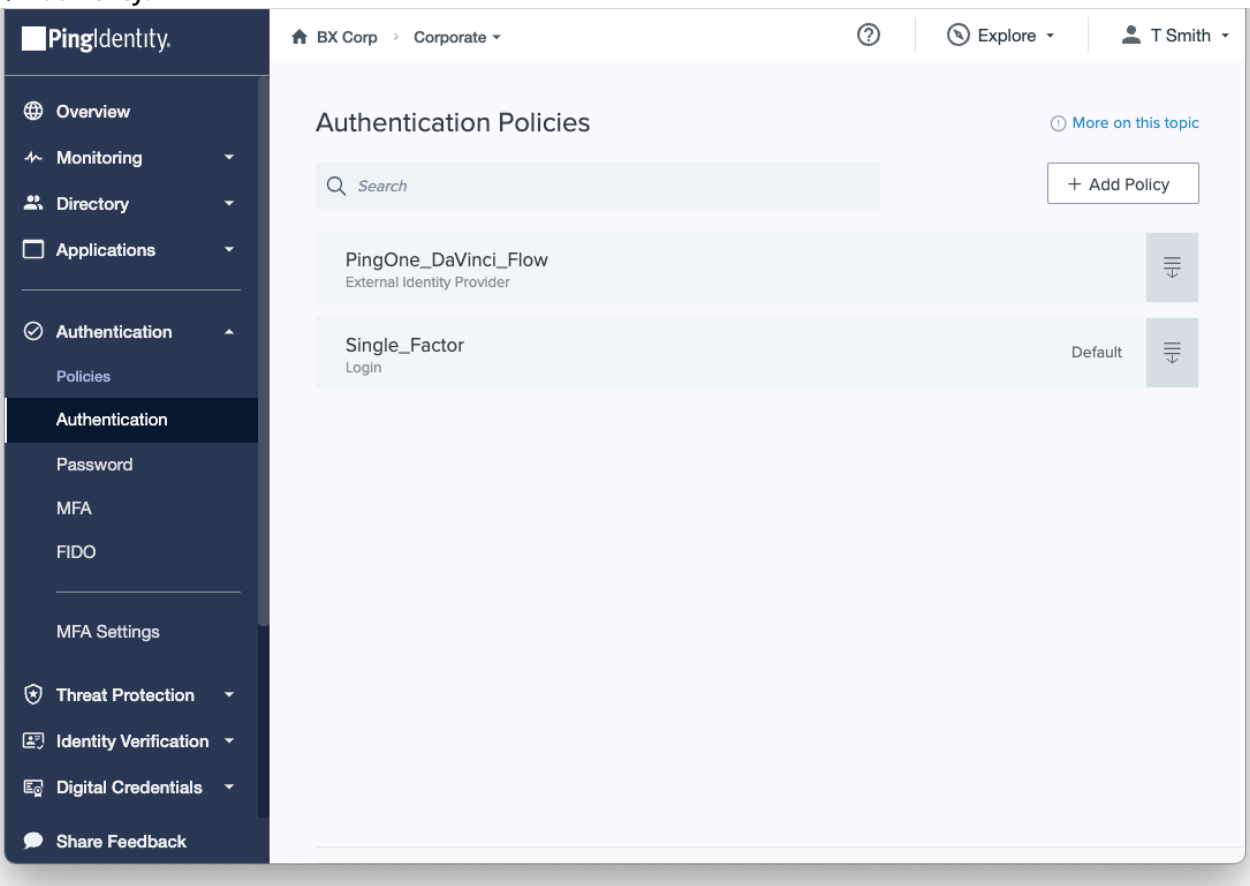
Learn how to build a custom sign-on policy that uses multifactor authentication.

About this task

This tutorial walks you through the creation of a multifactor authentication sign-on policy that you can apply to an application to secure access.

Steps

1. Go to **Authentication** > **Authentication**.
2. Click **+ Add Policy**.



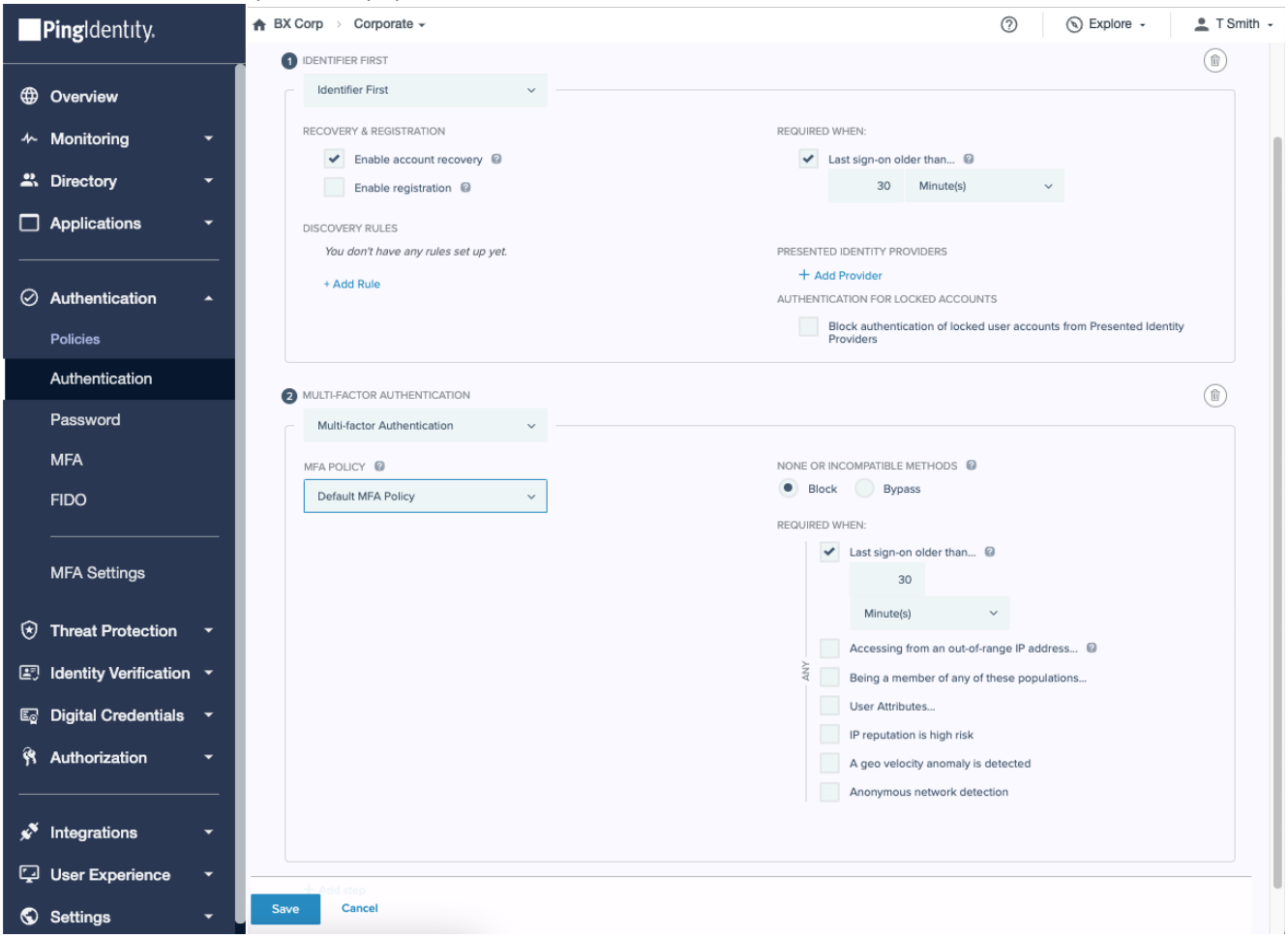
3. Enter a **Policy Name**.
4. Select a **Step Type** of **Identifier First**.
5. Click **Add Step**.

Copyright © 2025 Ping Identity Corporation

6. Select a **Step Type** of **Multi-factor Authentication**.

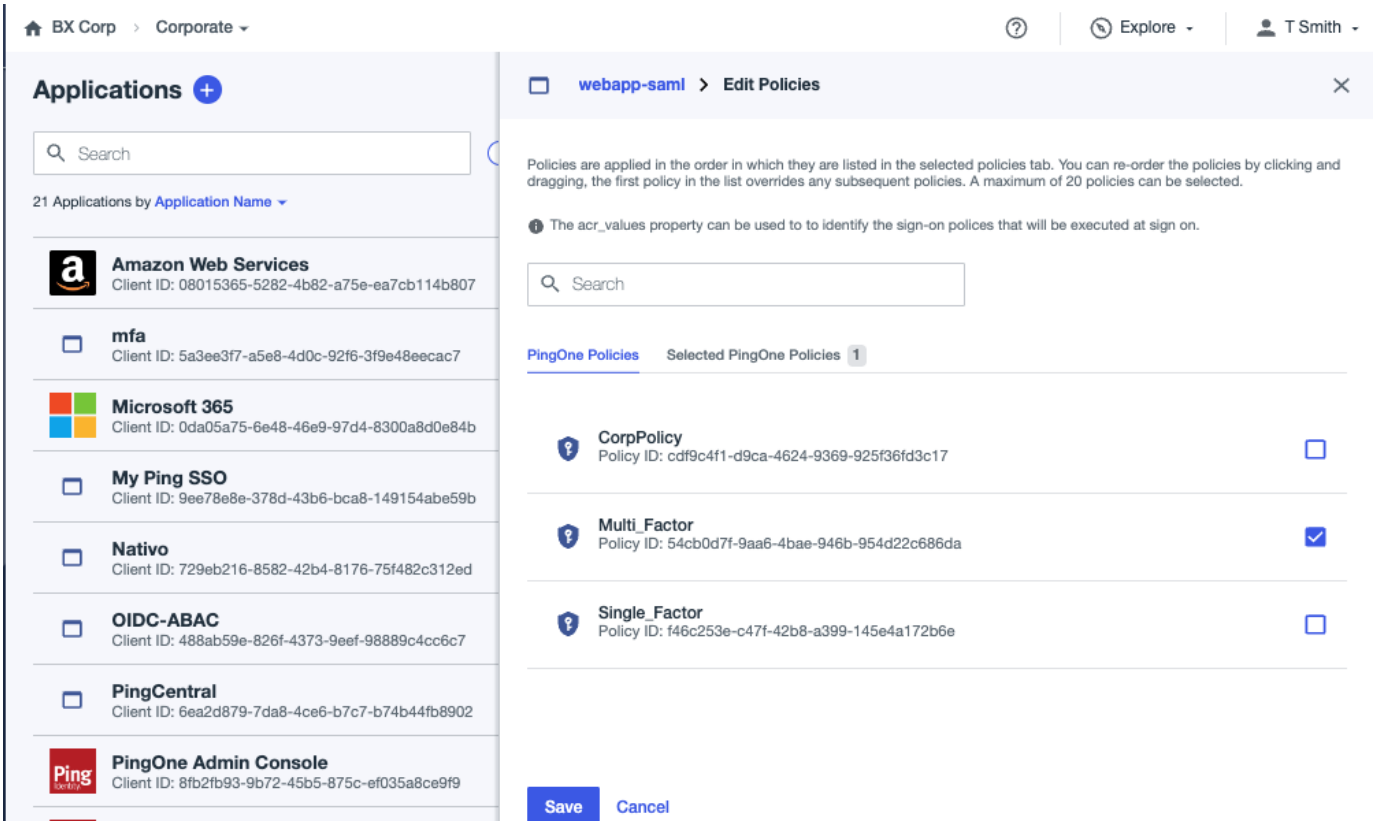
7. For **MFA Policy**, select **Default MFA Policy**.

8. Optionally, specify **Required When** criteria for the policy. For example, you can specify that the policy is required when users are member of a particular population.



9. To test the policy, assign it to an application on the application's **Policy** tab and access the application.

> **Tip**
>
> To learn how to add and access an application, see the Add a SAML application tutorial.



Create a group

Learn how to create a group to better manage your users and to provide improved access control to your applications.

About this task

This tutorial walks you through the creation of a group that you can use to better manage access to your applications. You can create groups with a manually specified membership or by specifying criteria that dynamically adds users when a match is found.

> **Note**
>
> To add users either manually or dynamically, you must first add a user.

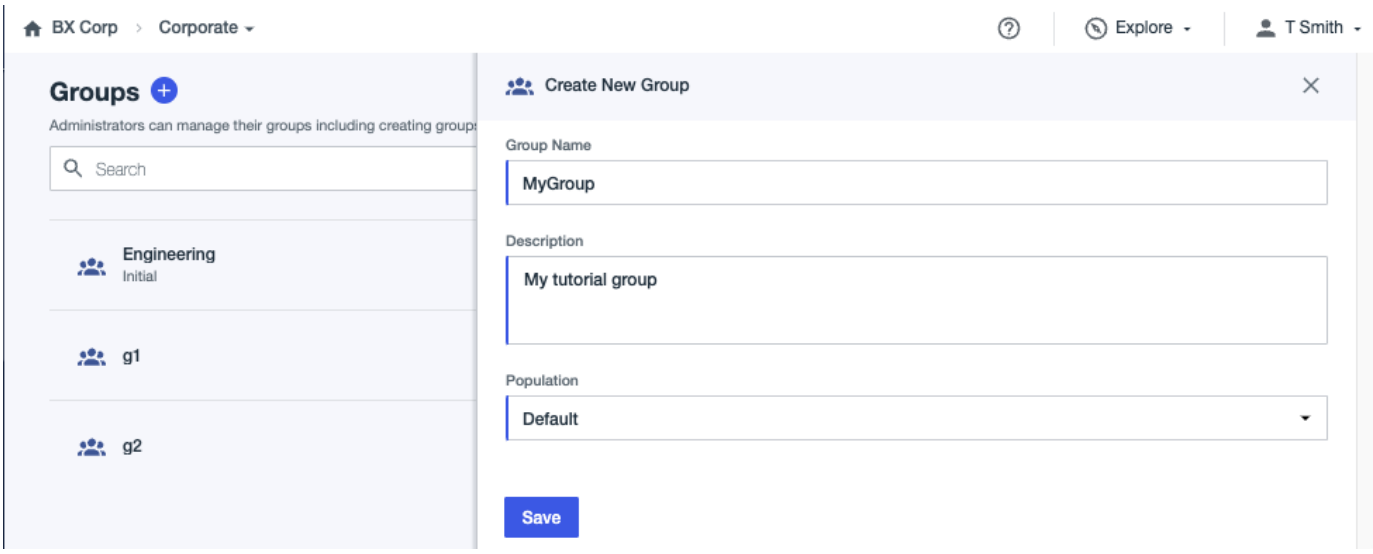
Steps

1. Go to **Directory** > **Groups**.
2. Click **+** to add a group.
3. Enter the following information:
   - **Group name**. A name for the group. The name must be unique within the environment for environment groups, and unique within a population for population groups.
   - **Description** (optional). A brief characterization of the group.

Copyright © 2025 Ping Identity Corporation

- **Population** (optional). The population in which the group will be created. Users with the *Environment Admin* role can create groups at the environment level, but users with the *Identity Admin* role must assign a group to a population for which they are an *Identity Admin*. If you select a population, the group can contain users from that population only.

4. Click **Finish & Save**.



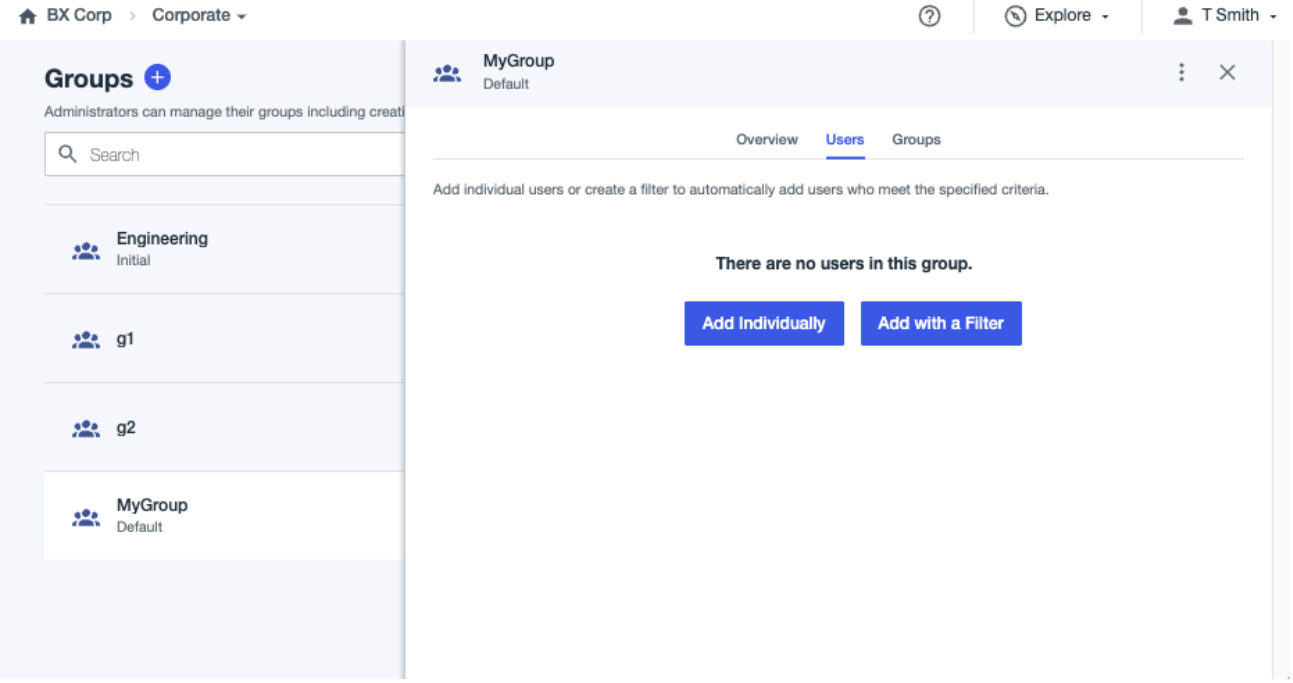
5. Click the **Members** tab.

6. Do one of the following:

   Choose from:

   - To add users from a list, click **+ Add members manually**. See Adding or removing users manually from the Groups page.

- To create a filter to determine group membership, click **+ Add members dynamically**. See Adding or removing users dynamically from the Groups page.



Control user access

Learn how to control user access to your applications using groups.

About this task

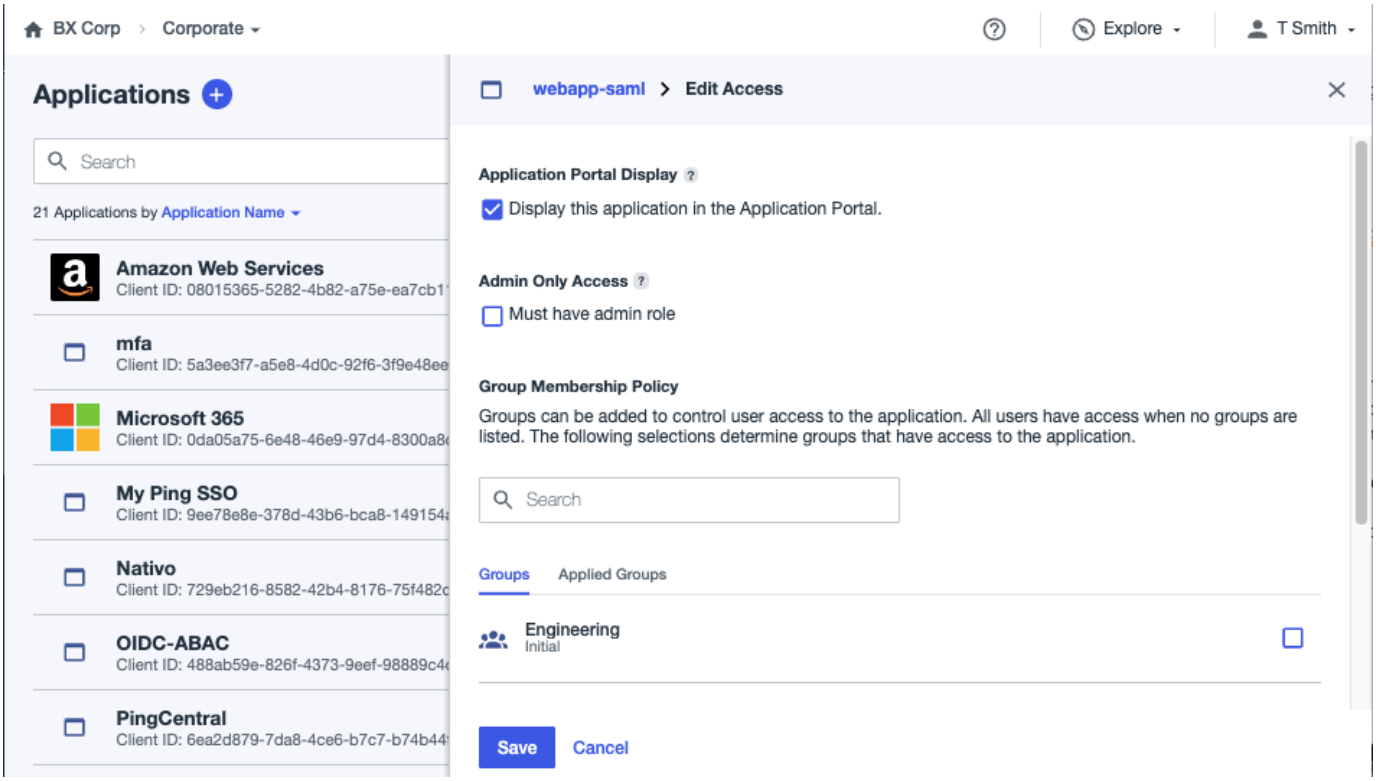
This tutorial walks you through the configuration of application access control using groups. When no groups are applied to an application, all users have access. Learn more in Application access control and Configuring application access control.

> **Note**
>
> To complete this tutorial, you must first create a group.

Steps

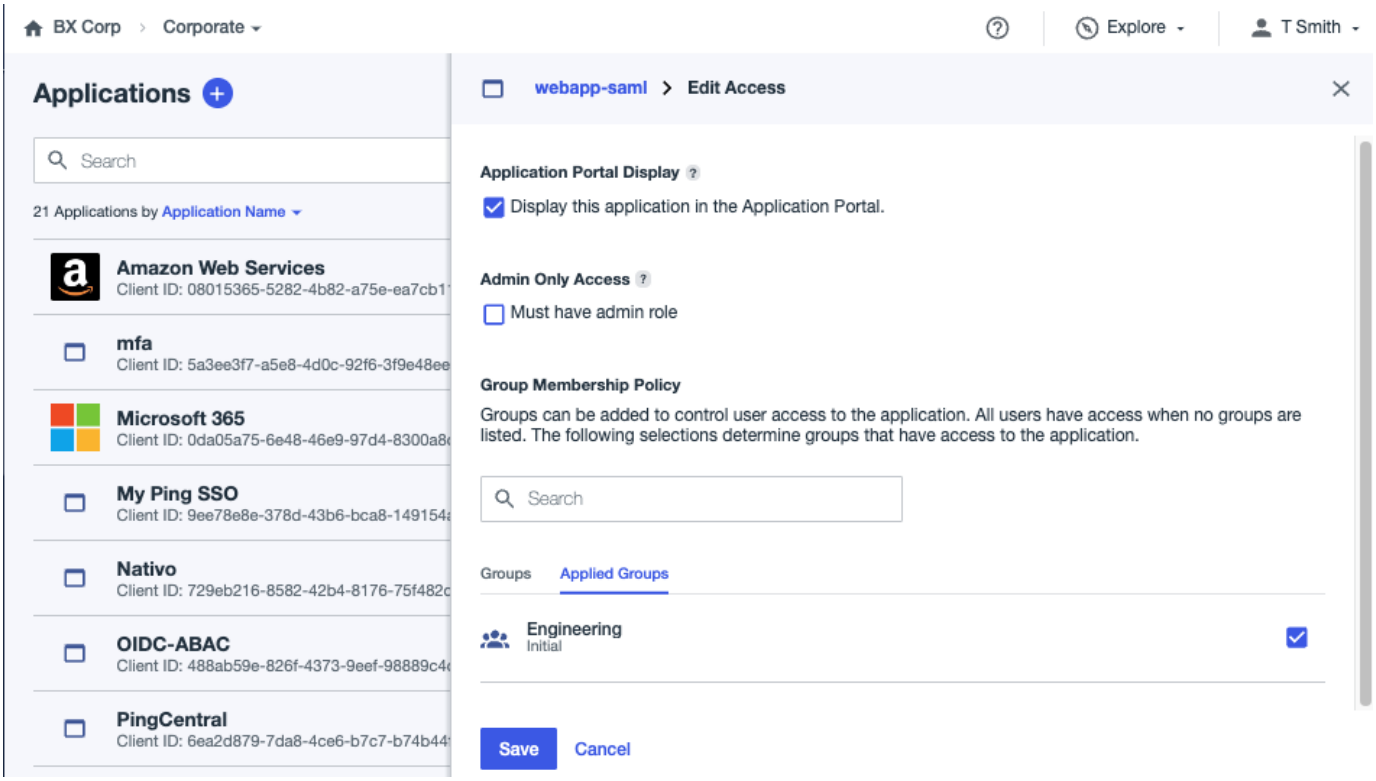
1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the application you want to configure.
2. Click the application entry to open the details panel for the application.
3. On the **Access** tab, click the **Pencil** icon.

Copyright © 2025 Ping Identity Corporation



4. To add a group to the access list, select its checkbox.

5. Click **Save**.



6. To test access control, try accessing the application with a user in the applied group and another who's not a member of the group.

Copyright © 2025 Ping Identity Corporation

Add custom attributes to a user

Learn how to add custom attributes to a user.

Before you begin

> **Note**
>
> To complete this tutorial, you must first add a user.

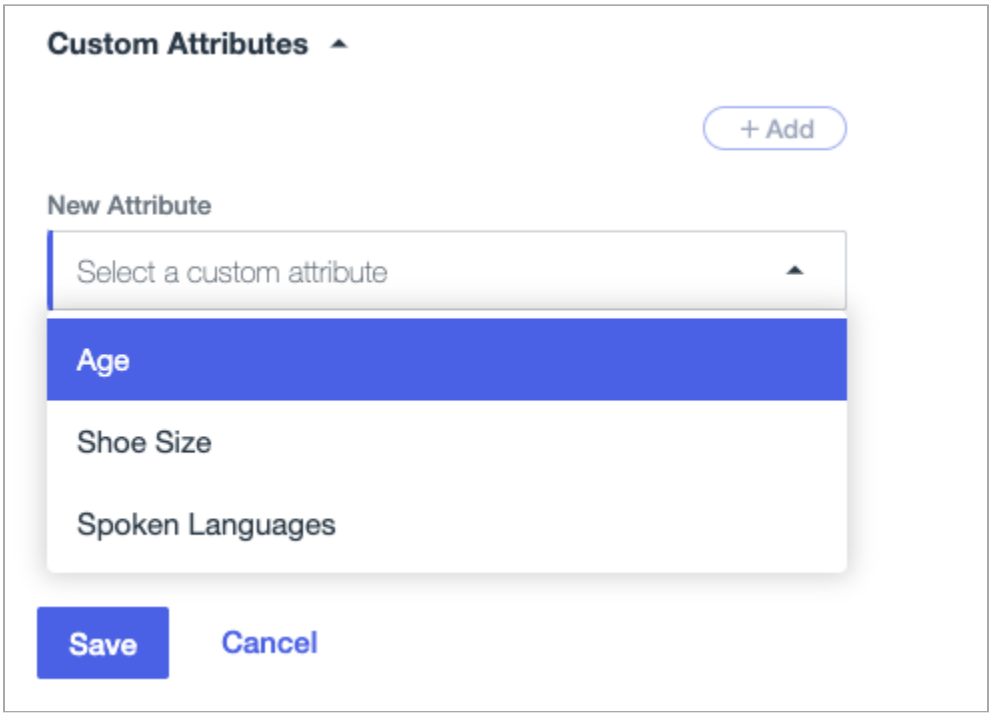
About this task

Adding custom attributes to a user determines the types of data that are stored for each user.

Steps

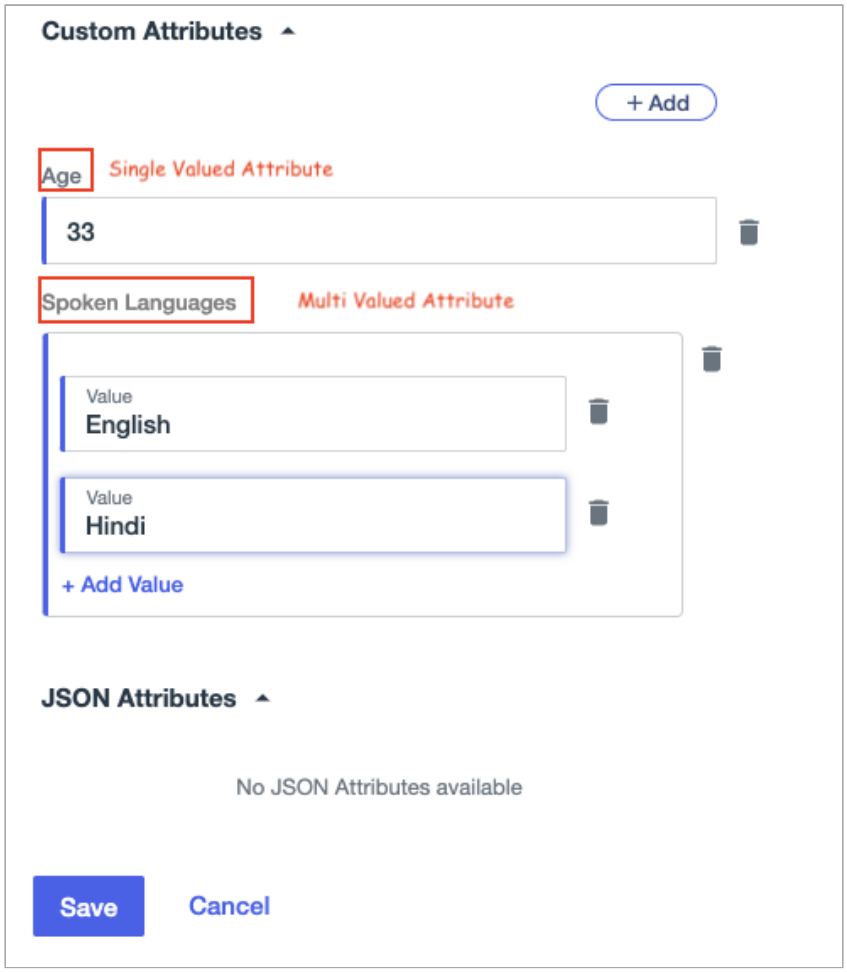
1. Go to **Directory** > **Users**.
2. Locate the user that you want to add a custom attribute to.

   You can browse or search for users.
3. Click the **More Options** (⋮) icon and click **Edit User**.
4. To add a custom attribute, scroll down to the **Custom Attributes** section.
5. Click **+ Add**.
6. In the **New Attributes list**, select a custom attribute.



7. Enter the value of the custom attribute.

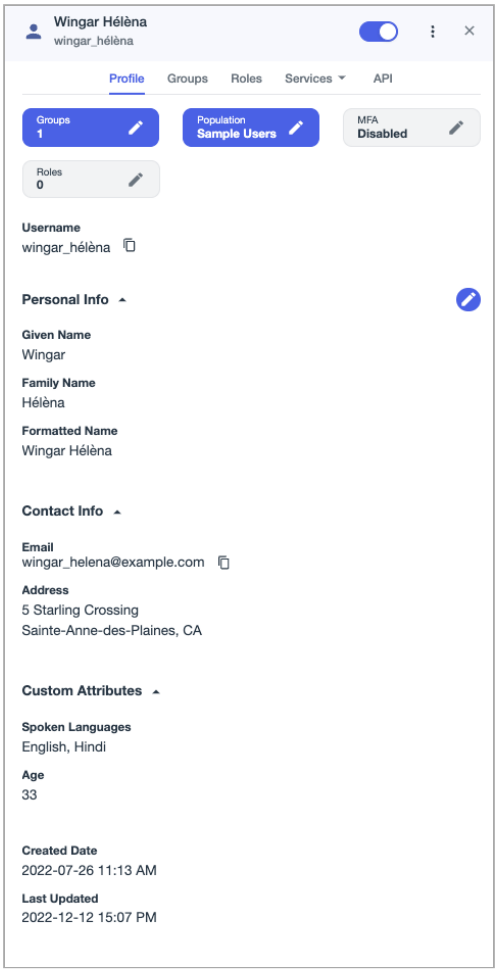
Copyright © 2025 Ping Identity Corporation



8. Click **Save**.

> **Note**
>
> You can view the attributes that you added in the **Custom Attributes** section of the user's **Profile** tab. This includes multi-value attributes and JavaScript Object Notation (JSON) object attributes.

Copyright © 2025 Ping Identity Corporation



Sync users between two environments

Learn how to set up a SCIM connection from one PingOne environment to another. You'll use the SCIM protocol to synchronize users between the two environments.

Create two environments and a Worker app

Create two environments that PingOne will synchronize, and a Worker application that will handle the synchronization.

Steps

1. Create the following two environments in PingOne:
    - P1-User-Source
    - P1-User-Destination

    Learn more in Adding an environment.

2. Go to the **P1-User-Destination** environment.

Copyright © 2025 Ping Identity Corporation

3. Go to **Applications > Applications** and create a new Worker Application with the following configuration:
    - **Grant type**: Client Credentials
    - **Token Endpoint Authentication Method**: Client Secret Basic

    Learn more in Adding an application.

4. Use the toggle to enable the new Worker application.
5. In the application details panel, click the **Roles**tab and add the **Identity Data Admin role** to your worker app

    Learn more in Configuring roles for a worker application.

6. In the application details panel, click the **Configuration** tab. Copy the following values to a secure location to use when making a provisioning connection:
    - **Token Endpoint**
    - **Client ID**
    - **Client Secret**
    - **Environment ID**

Create users and a group

:page-aliases:getting_started_with_pingone:p1_mfa_creating_a_user.adoc Create several users to be provisioned, and a group to identify them.

Steps

1. Go to the **P1-User-Source** environment.
2. Go to **Directory > Users**.
3. Create several users for provisioning.
4. Populate the following attributes for each user:
    - Email Address
    - Given Name
    - Family Name
5. Go to **Directory > Groups**.
6. Create a group called **Provisioning Users** and add any two users to that group.

    For more information, see Managing group membership.

Create a provisioning connection

Create a provisioning connection to define the source and target for provisioning.

Before you begin

Copyright © 2025 Ping Identity Corporation

Locate the values that you copied in Create two environments and a Worker app.

Steps

1. Go to the **P1-User-Source** environment.
2. Go to **Integrations > Provisioning**.
3. Click the **+** button and then click **New Connection**.
4. For connection type, select **Identity Store**.
5. Locate the **SCIM** tile and then click **Select**.
6. Click **Next**.
7. Enter a name and description. Click **Next**.
8. On the **Authentication** step, enter the following values:
   - **SCIM Base URL**: https://scim-api.pingone.*<region>*/environments/*<envID>*/v2

     Replace *<region>* with the appropriate value for your geographic region, such as .com, .ca, or .eu. For more information, see IP address and domain reference. Replace *<envID>* with the value you copied when you created the Worker app.
   - **Users Resource**: /Users
   - **SCIM Version**: 2.0
   - **Groups Resource**: /Groups
   - **Authentication Method**: OAuth 2 Client Credentials
   - **OAuth Token Request**: Paste the **Token Endpoint** value that you copied from Create two environments and a Worker app.
   - **OAuth Client ID**: Paste the **Client ID** value that you copied from Create two environments and a Worker app.
   - **OAuth Client Secret**: Paste the **Client Secret** value that you copied from Create two environments and a Worker app.
   - **Auth Type Header**: Select **OAuth Client Credentials**
9. Click **Test connection** to verify that PingOne can establish a connection to the SCIM resource.

   Result:

   If there are any issues with the connection, a **Test Connection Failed** dialog box opens. Click **Continue** to resume the setup with an invalid connection.

   > **Important**
   >
   > You cannot use the connection for provisioning until you have established a valid connection to SCIM. To retry, click **Cancel** in the **Test Connection Failed**dialog box and repeat step 8.

   Troubleshooting:

Copyright © 2025 Ping Identity Corporation

Learn more about troubleshooting your connection in Troubleshooting Test Connections Failure.

10. On the **Configure preferences** page, enter the user filter and the action to take when deprovisioning users.

    The filtering parameters are optional.

Option	Description
User filter expression	Determines how the connection uses the specified **User Identifier** to match existing users in the target identity store to the users being provisioned from the source identity store. Learn more in SCIM filter expressions.
User identifier	The identifier for the user filter expression.
Custom Attribute Schema URNs (optional)	A comma-delimited list of schema URNs to define a location for custom attributes. Use this option if the SCIM provider does not follow the standard naming convention for schema extensions in which custom attributes are defined. That is, URNs of the form `urn:ietf:params:scim:schemas:extension:<Organization Name>:2.0:User`.
Allow users to be created	Determines whether to create a user in the target identity store when the user is created in the source identity store.
Allow users to be updated	Determines whether to update user attributes in the target identity store when the user is updated in the source identity store.
Allow users to be disabled	Determines whether to disable a user in the target identity store when the user is disabled in the source identity store.
Allow users to be deprovisioned	Determines whether to deprovision a user in the target identity store when the user is deprovisioned in the source identity store.
Remove action	The action to take when removing a user from the target identity store.
Deprovision on rule deletion	Determines whether to deprovision users if the associated provisioning rule is deleted.

11. Click **Save**.

12. Use the toggle to enable the new connection.

Copyright © 2025 Ping Identity Corporation

> **Important**
>
> You cannot enable the new connection until you add the Identity Data Admin role to your worker app. Learn more in Configuring roles for a worker application.

Create a provisioning rule

Create a provisioning rule to identify which identities will be provisioned.

Steps

1. Go to the **P1-User-Source** environment.
2. Go to **Integrations** > **Provisioning**.
3. Click the **+** button and then click **New Rule**.
4. Enter a name for the rule.
5. On the **Configuration** tab, click the **Target** button, then select the SCIM connection you created in Create a provisioning connection.
6. Click **Save**.
7. On the **Configuration** tab, click the **User Filter** button, then click the pencil icon.
8. Set the filter to **Group Names**- **Contains**- **Provisioning Users**.
9. Click **Save**.
10. On the **Configuration** tab, click the **Attribute Mapping** button.
11. Verify the default attribute mappings.
12. On the rule overview page, use the toggle to enable the rule, which will initiate the provisioning process.

Verify the sync operation

After you have set up a connection and a rule, you can use the Sync summary and the Audit page to confirm that the sync is working.

Steps

- Do one of the following:
  - To use the **Sync summary**, click the rule entry to open the rule details panel.
  - To use the **Audit** page, go to **Monitoring** > **Audit**.

  For more information, see Viewing sync status.

Result

In the **P1-User-Source** environment, any users in the **Provisioning Users** group will be provisioned to the **P1-User-Destination** environment. You can add or remove users from the group to see the changes synchronized between the two PingOne environments.

Copyright © 2025 Ping Identity Corporation

Next steps

You can add or remove users from the group to see the changes synchronized between the two PingOne environments.

Integrate PingOne with a Node.js Express app

In this tutorial, you configure a Node.js application running Express to connect to your PingOne instance using OpenID Connect (OIDC).

You can then authenticate as a user and obtain both an access and ID token.

Time to success: 10 minutes

Before you begin

To complete this tutorial you must have:

- An OIDC Web application in PingOne configured with the following settings:
  - **Response Type**: Code
  - **Grant Type**: Authorization Code
  - **Redirect URIs**: http://localhost:3000/callback
  - **Token Endpoint Authentication Method**: Client Secret Basic

    > **Tip**
    >
    > As a starting point, use the **Getting Started Application** built into all customer solution environments when you select the **Include a solution designer to easily design and test experiences** checkbox. Learn more in Building solutions.

    Learn more in Adding an application and Editing an application - OIDC.
- Node.js v18.7.1 or later.
- A user created in your environment. Learn more in Adding a user.

Step 1. Download and initialize the sample app

We provide a sample app project that you can download and configure to connect to PingOne quickly and easily.

The project uses `npm` to manage the packages it requires, such as Express and Dotenv.

Download the sample app

Clone the Git repository or download a `.zip` archive to obtain the sample app source code:

Copyright © 2025 Ping Identity Corporation

Clone with Git

- *From the command line, clone the sample repo using Git:*

```
git clone https://github.com/pingidentity/generic-sample-apps.git
```

- *Navigate to the root of the sample using the following command:*

```
cd express-authorization-code % npm start
```

- *Run the following command to download and install the required packages and modules:*

```
npm install
```

Download a .zip archive

- *In a browser, go to https://github.com/pingidentity/generic-sample-apps.git.*
- *Select **Code**, and then click **Download ZIP**.*
- *Extract the contents of the `.zip` archive to a folder on your computer. For example `{generic-sample-apps}`.*

Initialize the sample app

The sample app requires a number of packages, which you can install by using npm:

1. Navigate to the express authorization code folder in the root directory using the following command:

   ```
   cd express-authorization-code
   ```

2. Run the following command to download and install the required packages and modules:

   ```
   npm install
   ```

   Example:

   The result resembles the following:

Copyright © 2025 Ping Identity Corporation

```
`~/PingOneNodeExpressSample $ npm install

added 134 packages, and audited 135 packages in 3s

19 packages are looking for funding
run `npm fund for details

found 0 vulnerabilities`
```

Step 2. Configure the sample app

Add the code and configuration the app needs to connect to PingOne:

1. In the PingOne admin console, go to **Applications > Applications**, and select the application to use for this tutorial.
2. On the **Integrate tab**, select the following:
   - In **Authorization Flows**, ensure that **Authorization Code** is selected.
   - In **Language Framework**, select **Express**.

     > **Note**
     >
     > This tutorial is for Express only. Selecting **Ping SDK for JavaScript** creates a different snippet. Go to JavaScript Tutorials for detailed instructions and links to the sample app.

   - If you've enabled custom domains, in the **Domain Path** list, select one of the following:
     - **Base**: Select to use the default *.pingone.com domain.
     - **Custom**: Select to use the custom domain configured for the environment.
3. Click the **Copy to clipboard** icon to copy the code snippet.

   The code is preconfigured with the environment settings the app requires for a connection, excluding the client secret.

   Example:

   ```
   `PingOne Express Authorization Code Flow
   PINGONE_AUTH_ENDPOINT="https://auth.pingone.com/####-####-####-####-######/as/authorize"
   PINGONE_TOKEN_ENDPOINT="https://auth.pingone.com/######-####-####-####-#########/as/token"
   PINGONE_SIGNOFF_ENDPOINT="https://auth.pingone.com/#######-####-####-####-############/as/signoff"
   PINGONE_CLIENT_ID="########-####-####-####-##########"
   PINGONE_CLIENT_SECRET="{{PINGONE_CLIENT_SECRET}}"
   REDIRECT_URI="http://localhost:3000/callback"
   PINGONE_SCOPES="openid"`
   ```

4. Open the application and folder in the IDE.
5. Paste the code from the PingOne console into the `.env` file, replacing the `# Replace with Snippet` string.
6. Save the `.env` file.

Step 3. Test the sample app

Copyright © 2025 Ping Identity Corporation

You can now run the sample app, which starts a server at http://localhost:3000 by default.

1. Navigate to the express authorization code folder in the root directory using the following command:

```
cd express-authorization-code
```

2. Run the following command to build the project and start the local server:

```
npm start
```

Example:

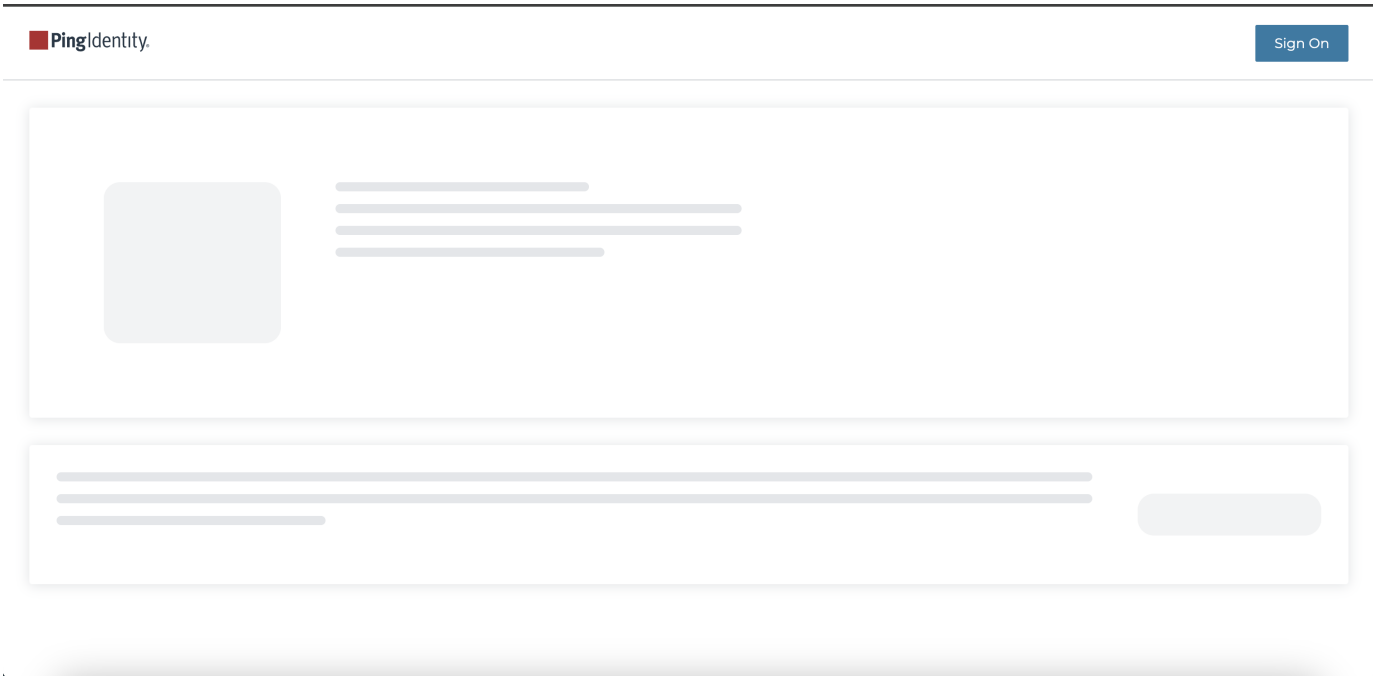
The result resembles the following:

```
express-authorization-code % npm start


> node-ex-website@1.0.0 start
> node server.js

Server listening on port 3000`
```

3. In a browser, go to http://localhost:3000/.

Result:

A wireframe for the application opens:



4. Click **Sign On**.

Result:

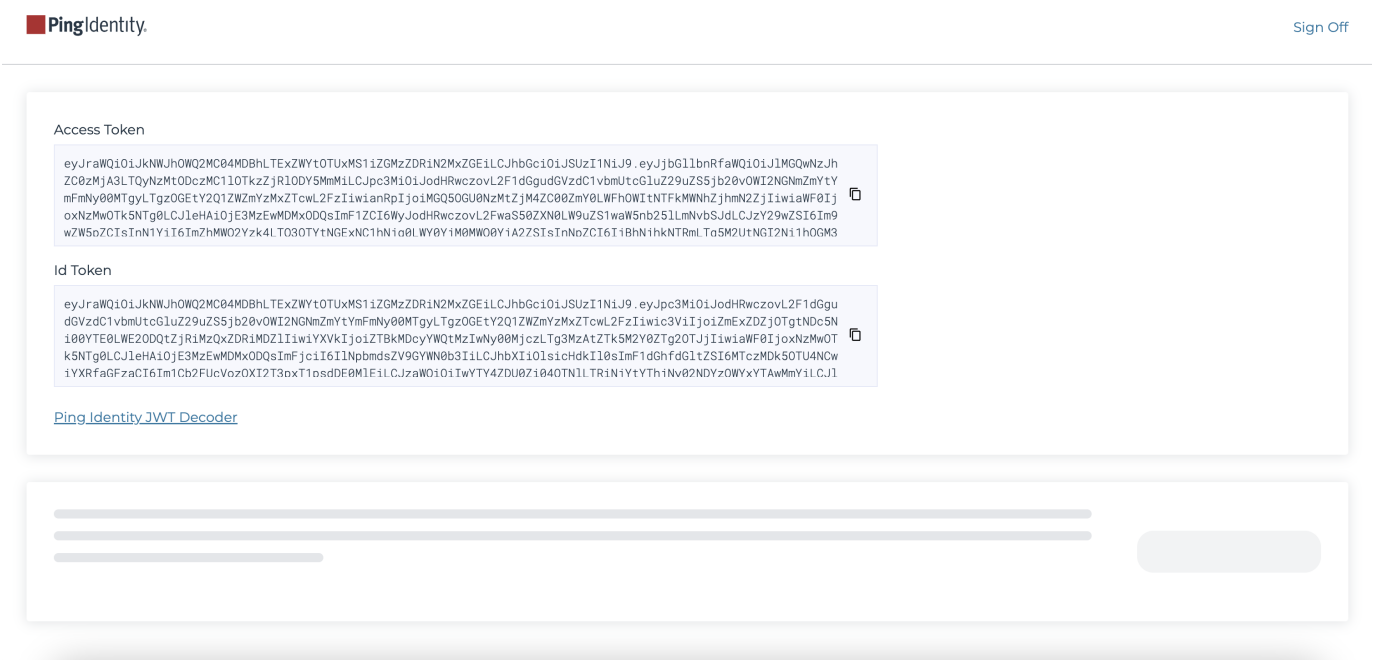
Copyright © 2025 Ping Identity Corporation

The PingOne sign-on page opens.

5. Enter a known user's credentials and click **Sign On**.

   Result:

   PingOne verifies the credentials and redirects the browser to the sample app, which opens a wireframe profile page that includes the access and ID tokens:



> **Tip**
>
> Copy a token value and inspect its contents using the Ping Identity JWT Decoder.

6. To revoke the tokens and sign the user off of PingOne, click **Sign Off**.

Result

You have successfully added PingOne-backed sign on and sign off to a Node.js app running Express.

Next steps

- You can easily change the sign-on experience by changing the authentication policy the application uses without rebuilding the sample app.
- Learn more in Authentication policies for applications.
- Learn more about what you can do with the tokens you obtained during the OIDC in The Essential OAuth Primer. To see how PingFederate uses OAuth 2.0 and OIDC, download the OAuth Playground (requires sign on).

Troubleshooting redirect URI mismatch errors

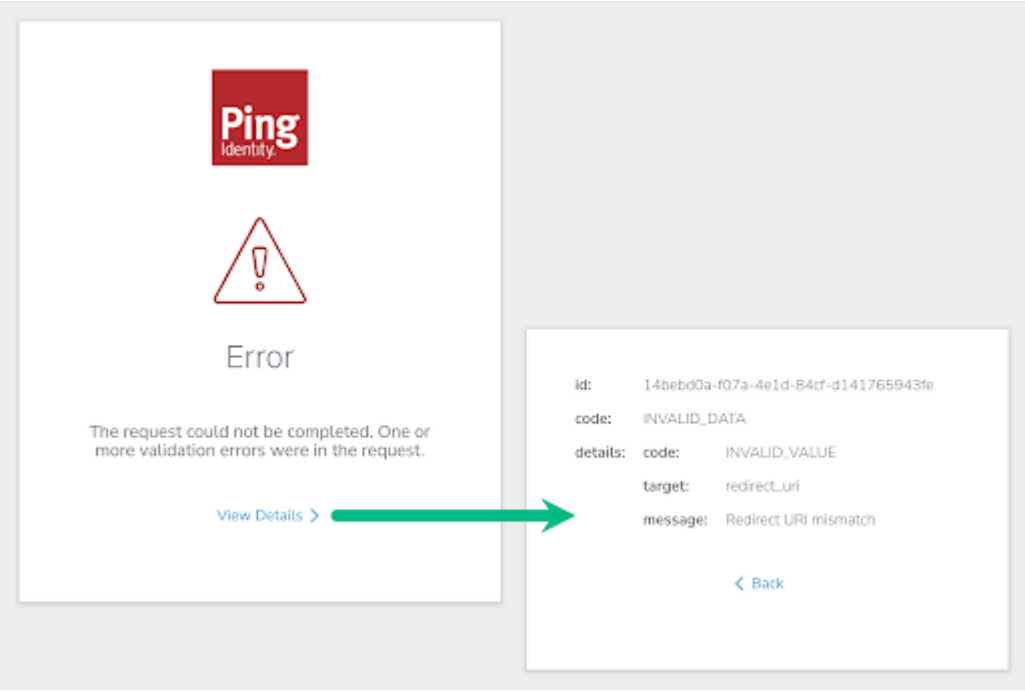
Try the tips and workarounds in the following section if you encounter a redirect URI mismatch error.

How to fix "Redirect URI mismatch" errors

Copyright © 2025 Ping Identity Corporation

The sample application sends a `redirect_uri` parameter when contacting the PingOne instance. If the value doesn't match a value configured in the web app in PingOne, you receive the following error:

```
The request could not be completed. One or more validation errors were in the request.
```



To resolve the issue:

1. In the PingOne admin console, go to **Applications** > **Applications** and select the application the sample is using.
2. On the **Configuration** tab, ensure that the **Redirect URIs** property contains http://localhost:3000/callback.
3. In an IDE or text editor, open the `.env` file in the root folder of the sample app.
4. Ensure the `REDIRECT_URI` property exactly matches the value in PingOne and is surrounded with double quotes: `"http://localhost:3000/callback"`.

Configure a multi-factor authentication experience using PingOne and PingID

This document demonstrates a simple multi-factor authentication (MFA) experience using PingOne and PingID. By the end of this document, you will have experienced MFA both from the administrator's perspective of configuration, and the end user's perspective of usage.

> **Note**
>
> For API operations on a PingID workforce implementation hosted via a PingOne environment, use the PingID APIs. See PingID API overview in the PingID API documentation.

To configure an MFA experience using PingOne and PingID, follow these steps:

1. Start a PingOne trial.

Copyright © 2025 Ping Identity Corporation

2. Add a new environment.
3. Add an existing PingID tenant to a new PingOne environment.
4. Create demo users.
5. Create a group with dynamic membership.
6. Create a web application.
7. Perform the user simulation.
8. Access the application portal.
9. Review the synchronization of users in PingID.

Starting a PingOne trial

Signing up for a 30-day free trial version is a great way to experience the power of PingOne for yourself.

About this task

Your trial organization includes:

- One trial license.
- Up to five environments in one region, including the Administrators environment, which is created when the new trial starts.
- An administrative user who has all the roles necessary to manage the organization and add other administrators.
- Up to 1000 active identities for the duration of the trial.

Even if you already have a PingOne license, you can still start a PingOne trial and evaluate the services available. Follow the appropriate set of instructions:

- Existing customers
- New customers

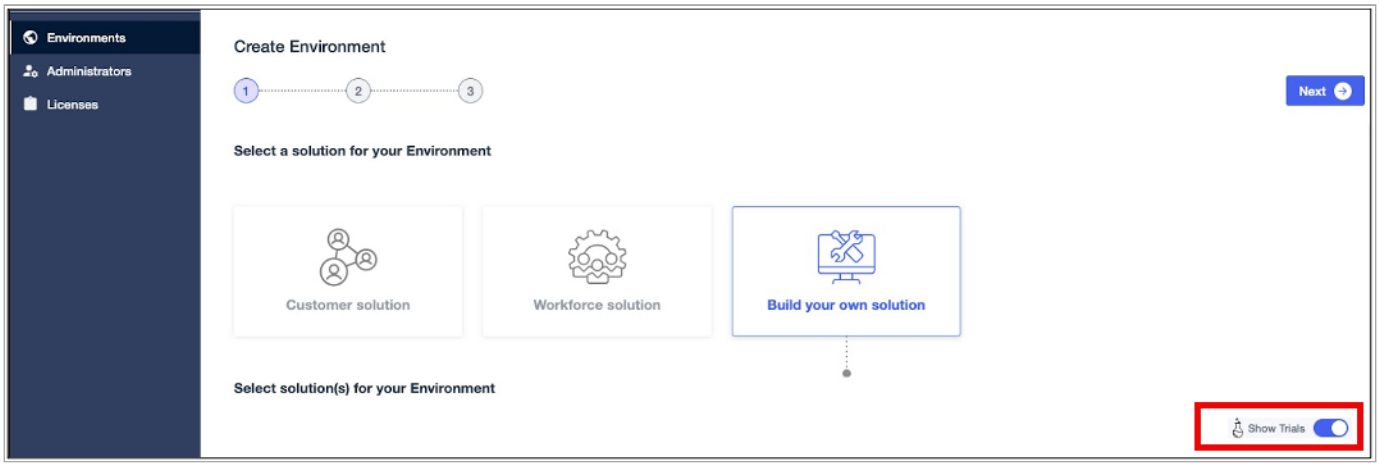
Existing customers

To sign up for the 30-day free trial, create a new PingOne environment in your organization and add the services that you want to evaluate.

Steps

1. Sign on to your PingOne environment, access the **Environments** page, and click **+** to create a new environment.
2. On the **Create Environment** page, select the type of solution you want to build and click **Next**.
3. Ensure that the **Show Trials** toggle is on.

Copyright © 2025 Ping Identity Corporation

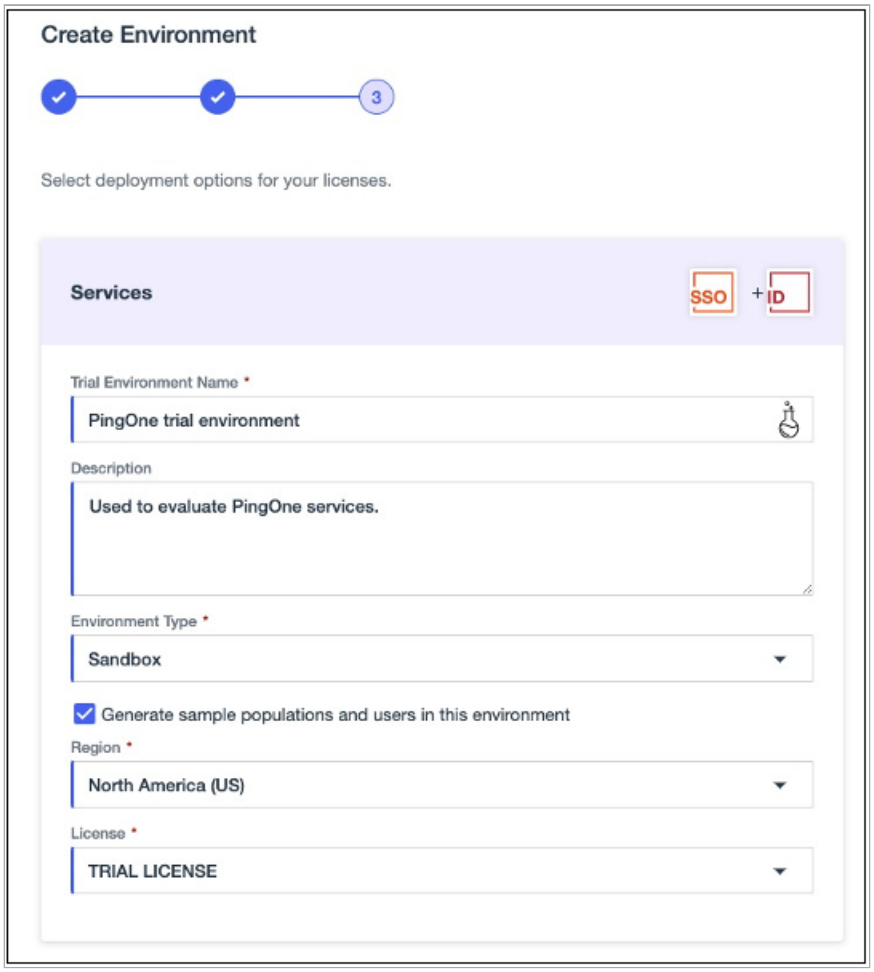


4. Select the services that you want to add to the environment and click **Next**.

5. Define your environment by entering the following:

Field	Description
Environment Name	A unique identifier for the environment.
Environment Description (optional)	A brief description of the environment.
Environment Type	Select **Sandbox**.
Generate sample populations and users in this environment	Select this checkbox to generate two populations and 40 sample users in the new environment.
Region	Select the region available in the list, which is determined by your PingOne organization.
License	Select **Create new trial license**.

Copyright © 2025 Ping Identity Corporation



6. Click **Finish**.

Result:

The new environment is created in your PingOne organization, and a new trial license is issued. The **Environments** page displays. You'll also be able to see the new license listed on the **Licenses** page.

New customers

To sign up for the 30-day free trial, provide your name, business email address, and verify it. You will receive access to a new PingOne organization and be prompted to sign on with the credentials you create during registration.

Steps

1. Go to pingidentity.com and click **Try Ping** on the right side of the page.

2. To activate your trial, check your email inbox and click **Verify Email** in the email sent to you.

Copyright © 2025 Ping Identity Corporation

3. Enter your first and last name, job title, and phone number in the appropriate fields. Note that you will be granted the Organization Admin role by default, which allows you to create, update, and delete environments and configure your organization to meet your needs.

4. Select the region available in the list, which is determined by your PingOne organization.

> **Important**
>
> PingOne data centers are available all over the world. For optimum performance, use the data center closest to your geographic region. Learn more in Organizations.

5. Create a password, select the checkbox to agree to the terms and conditions, and click **Start Trial**.

6. Enter the username and password you just created and click **Sign On**.

7. You're required to enroll in MFA to enhance your account security. Click **Continue**.

8. Select the MFA method that you want to use to authenticate:

   - **Email**: You'll provide your email address, receive an email with a passcode, and enter the passcode to sign on.
   - **Authenticator App**: You'll access the mobile authenticator app, receive a passcode, and enter the passcode to sign on.
   - **Passkey**: You'll create a passkey on your device using a biometric sensor or PIN and use that sensor or PIN to sign on.

Result:

After you complete the registration process, you'll be redirected to the **Environments** page, where you can begin creating identity solutions that meet your specific needs.

Next steps

Now, you can either add other administrators to the Administrators environment or create a new environment. Learn more in Managing administrators and Creating an environment.

Adding a new environment

To create a multi-factor authentication (MFA) experience, create an environment that includes PingOne and PingID.

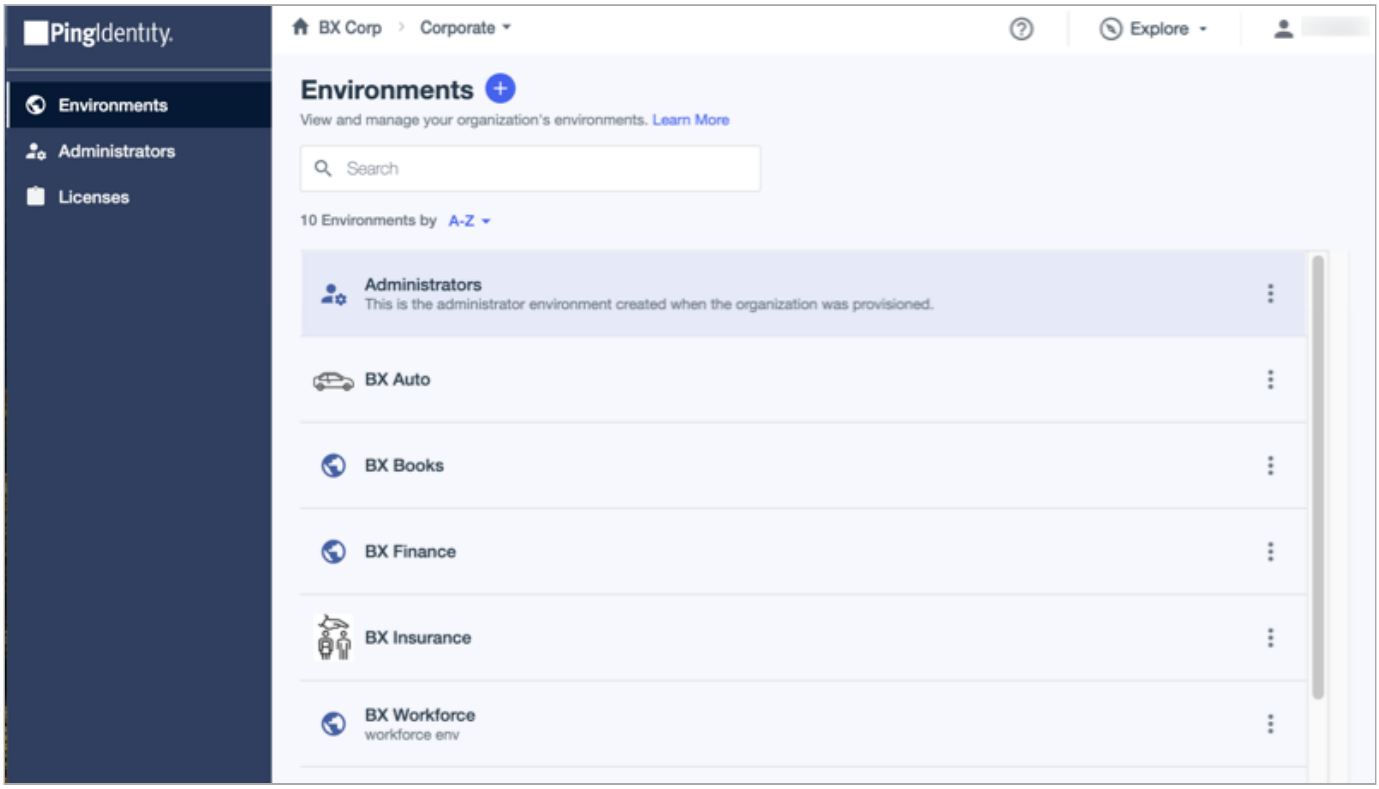
Steps

1. Sign on to the PingOne admin console.

2. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page.

3. Click the **+** icon.

Copyright © 2025 Ping Identity Corporation

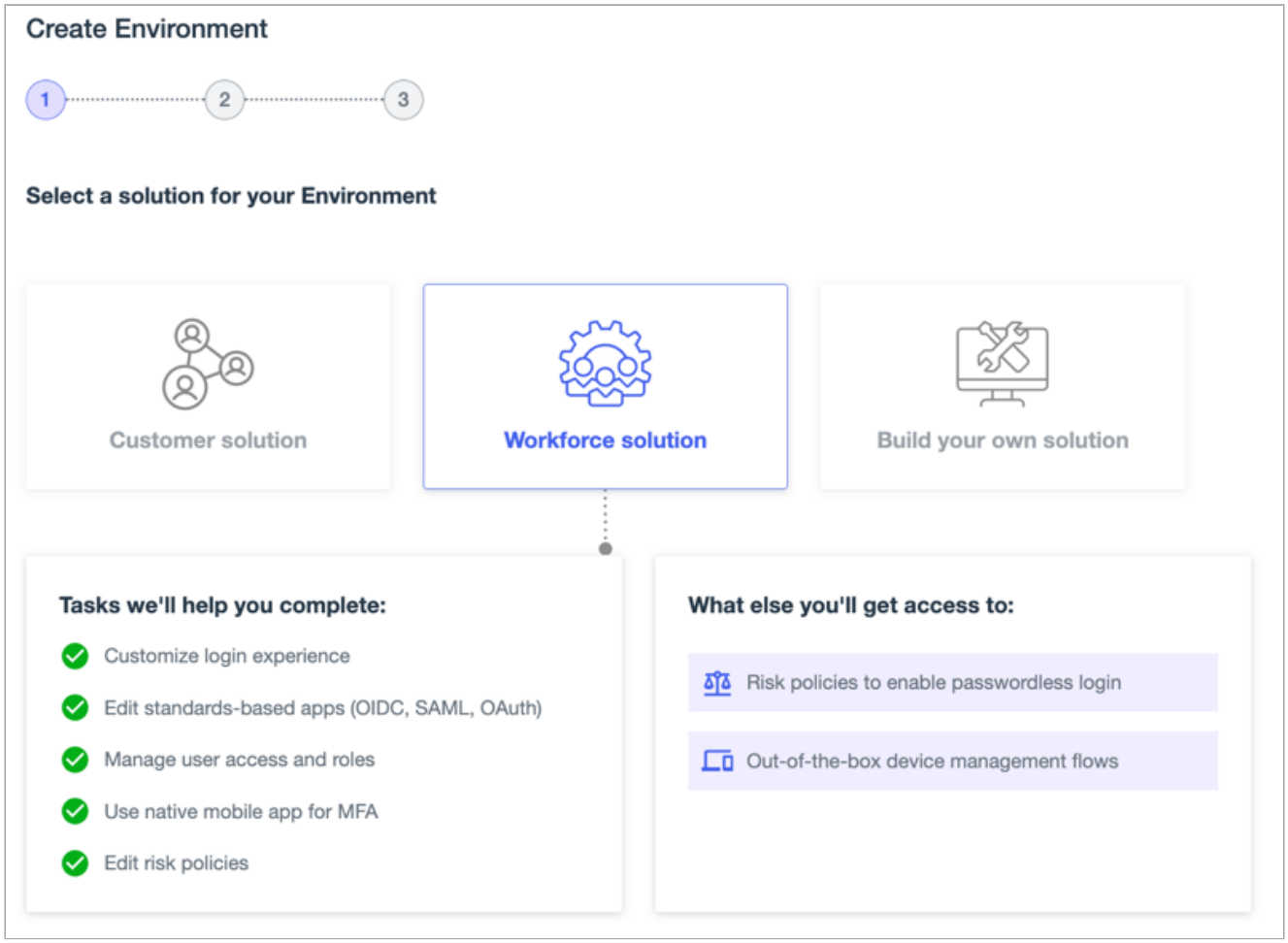


Result:

The **Create Environment** setup assistant starts.

4. On the **Create Environment** page, under **Select a solution for your Environment**, select **Workforce solution**.

Copyright © 2025 Ping Identity Corporation



5. Click **Next**.

   The services that will be deployed to your new environment are listed.

6. Click **Next**.

7. Define your environment by entering the following:

Field	Description
Environment Name	A unique identifier for the environment.
Description (optional)	A brief description of the environment.
Environment Type	Select **Sandbox** or **Production**. Sandbox environments are typically used for configuration and testing before deployment. Production environments are typically used for live configurations that are deployed for real-world use. Learn more about environment types in Sandbox and Production environments.
Generate sample populations and users in this environment	Select this checkbox to generate two populations and 40 sample users in the new environment.

Copyright © 2025 Ping Identity Corporation

Field	Description
Region	The appropriate geographical region for the environment. The list shows only regions that are included with your license. **Important** You can't change the region after the environment has been created.
License	Select the license to use for this environment. The available licenses for your organization are shown in the **License** list. For more information, see Licenses and Platform Limits.
Include a solution designer to easily design and test experiences (optional)	Customer and Workforce solutions only. If selected, after you create your environment, a solution designer opens and walks you through the process of designing your experiences.
Choose Your Industry (optional)	Customer solutions only. If you make a selection, PingOne creates a sample app tailored to the industry selected.

8. Click **Finish**.

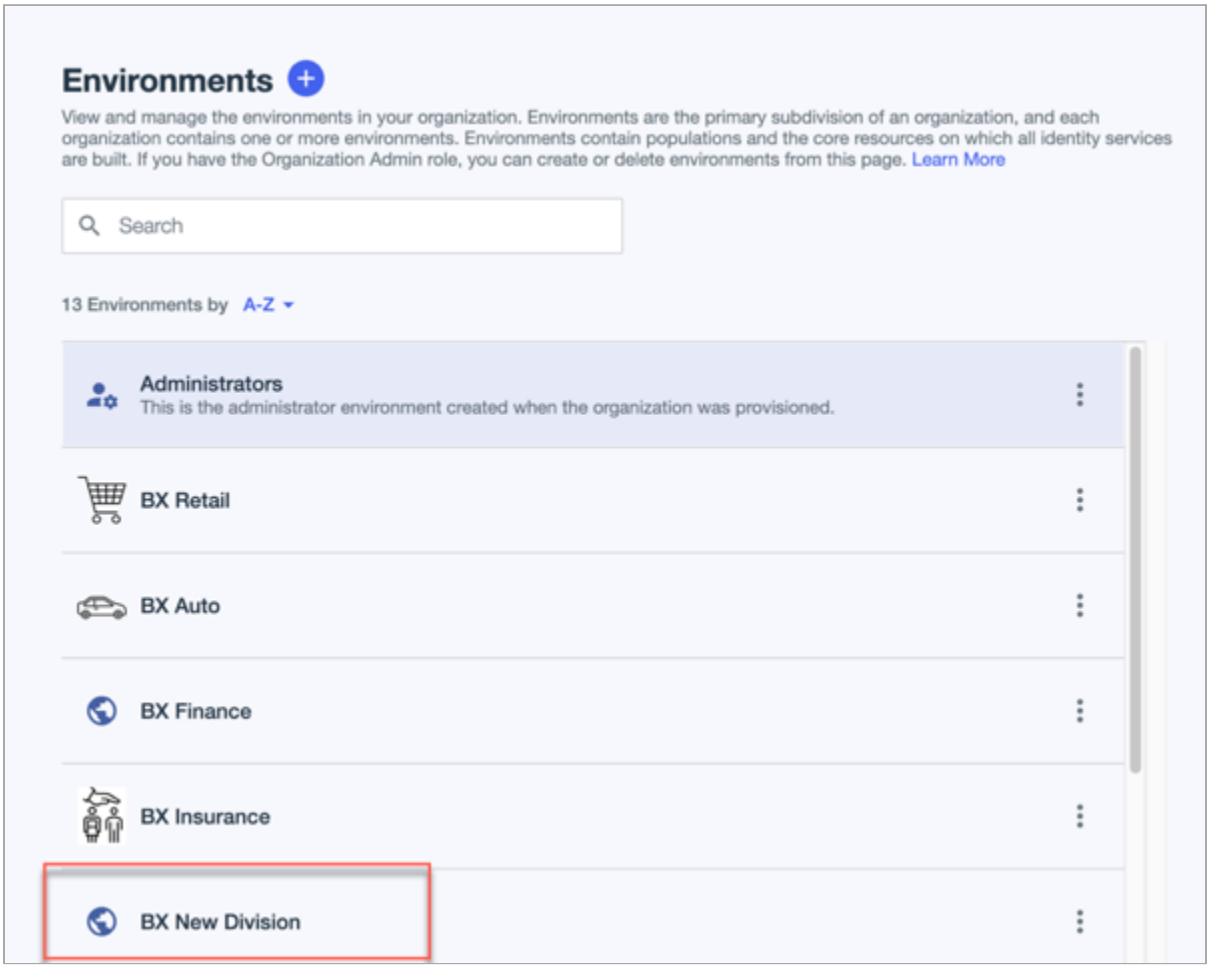
   Result:

   The new environment is created in your PingOne organization.

   If you selected the solution designer option, the solution designer opens and guides you through the process of designing and testing registration and sign-on experiences in less than 5 minutes.

   If you did not select the solution designer option, the **Environments** page opens. Locate your new environment by sorting the list alphabetically or by date created, or enter the environment name in the search box.

Copyright © 2025 Ping Identity Corporation

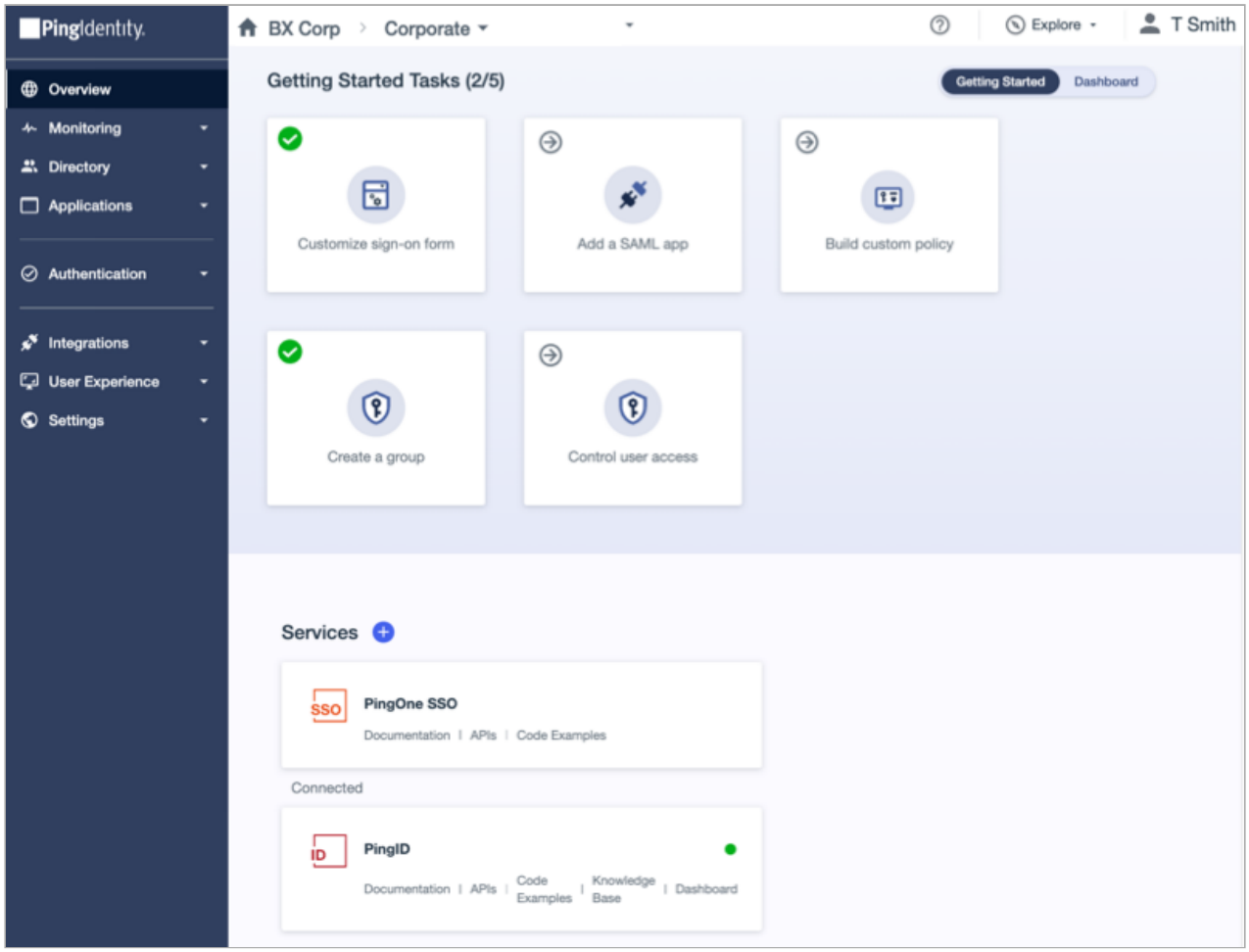


9. On the **Environments** page, click the environment to open the details panel.
10. Click **Manage Environment** to go to the **Overview** page for your environment.

    Result:

    The **Overview** window of your new environment displays PingOne SSO, PingID, and potentially other products in the **Services** section. The green dot in the **PingID** tile indicates that PingID has been deployed.

Copyright © 2025 Ping Identity Corporation



Next steps

Continue by Creating demo users.

Adding an existing PingID tenant to a new PingOne environment

If you have a separate PingID tenant, you can easily integrate it with your PingOne environment.

Before you begin

This task describes the steps required to add an existing PingID tenant to a PingOne environment. In order to add an existing PingID tenant, the following conditions must be met:

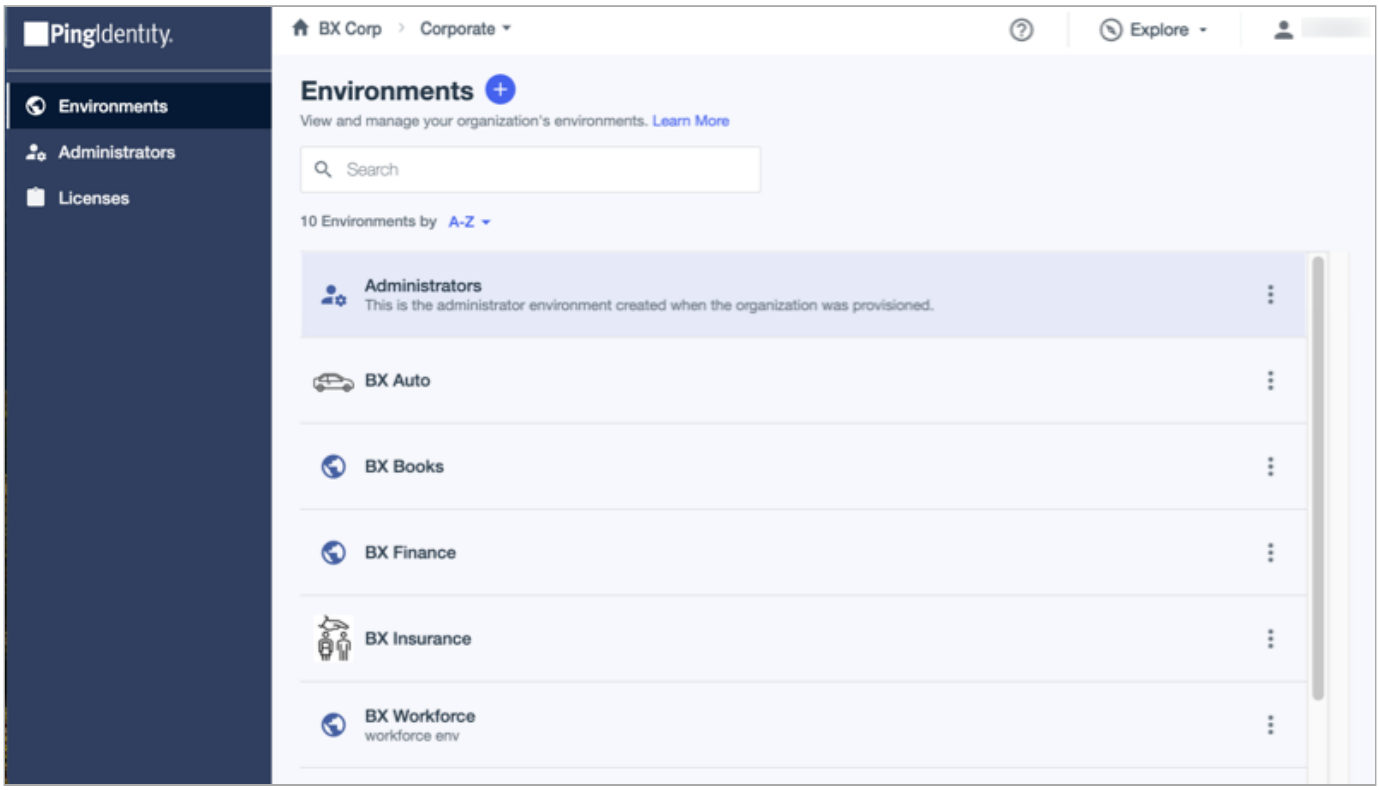
- You must have a full PingOne license. This option is not available with a trial license.
- Your PingID license must support a connection to PingOne.

> **Note**
>
> Learn more in Licenses and Platform Limits.

Steps

1. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page.

2. Click the + icon.



Result:

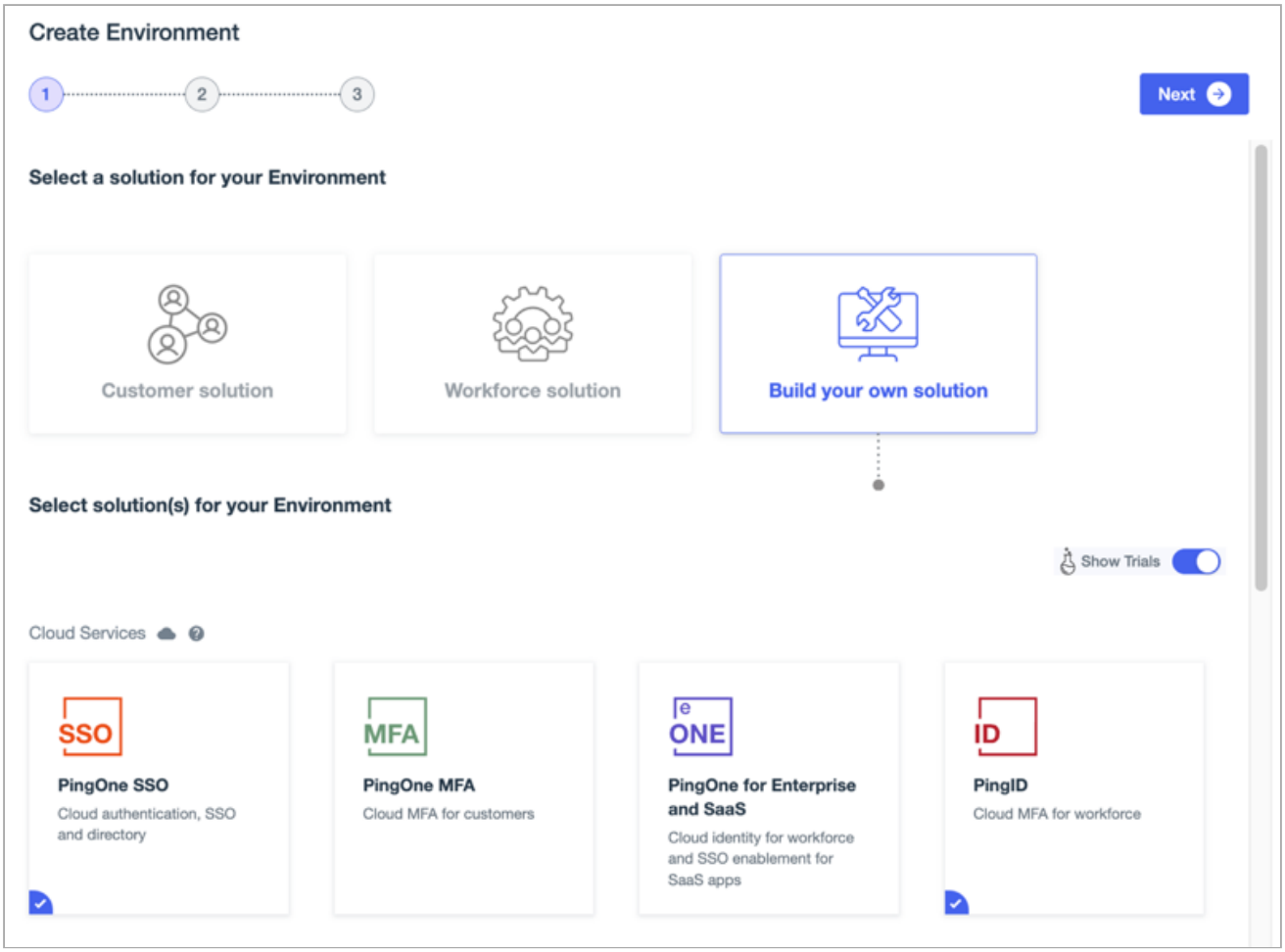
The **Create Environment** setup assistant starts.

3. In the **Select a solution for your Environment** section, click **Build your own solution**.

4. Click the **Show Trials** toggle.

5. In the **Select a solution for your Environment** section, select the **PingOne SSO** and **PingID** services.

Copyright © 2025 Ping Identity Corporation



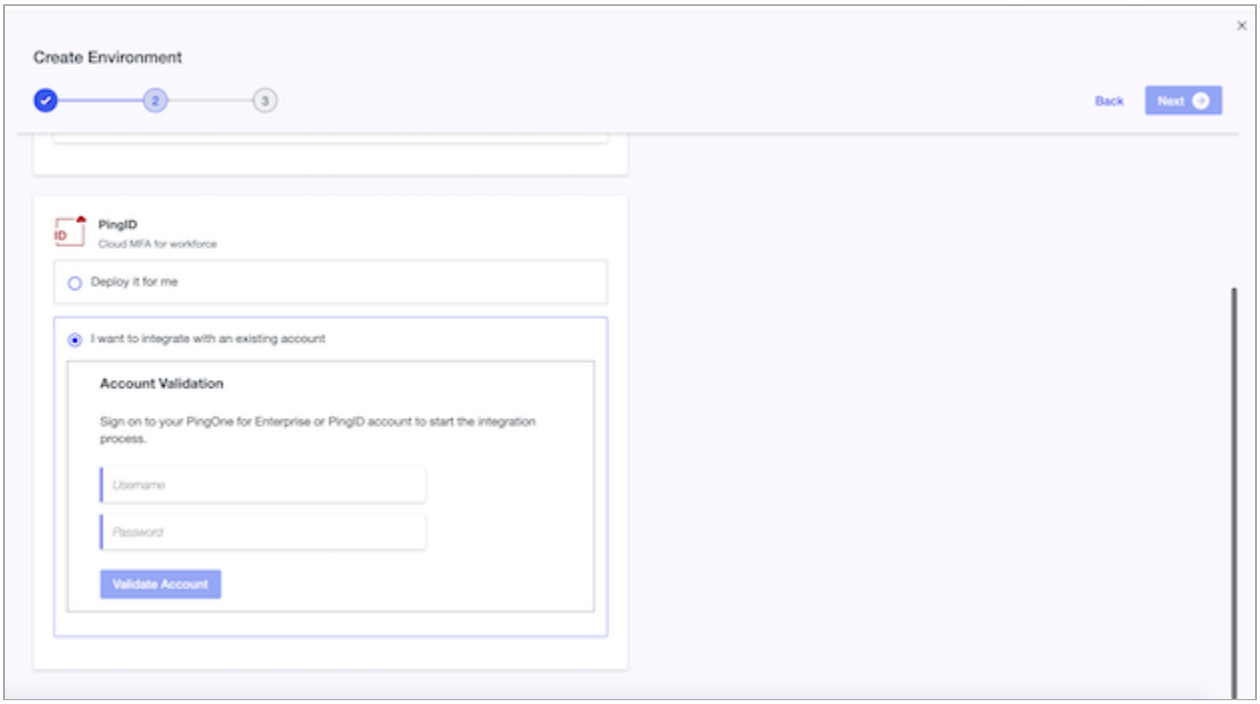
6. Click **Next**.

7. On the **PingID** tile, click **I want to integrate with an existing account**.

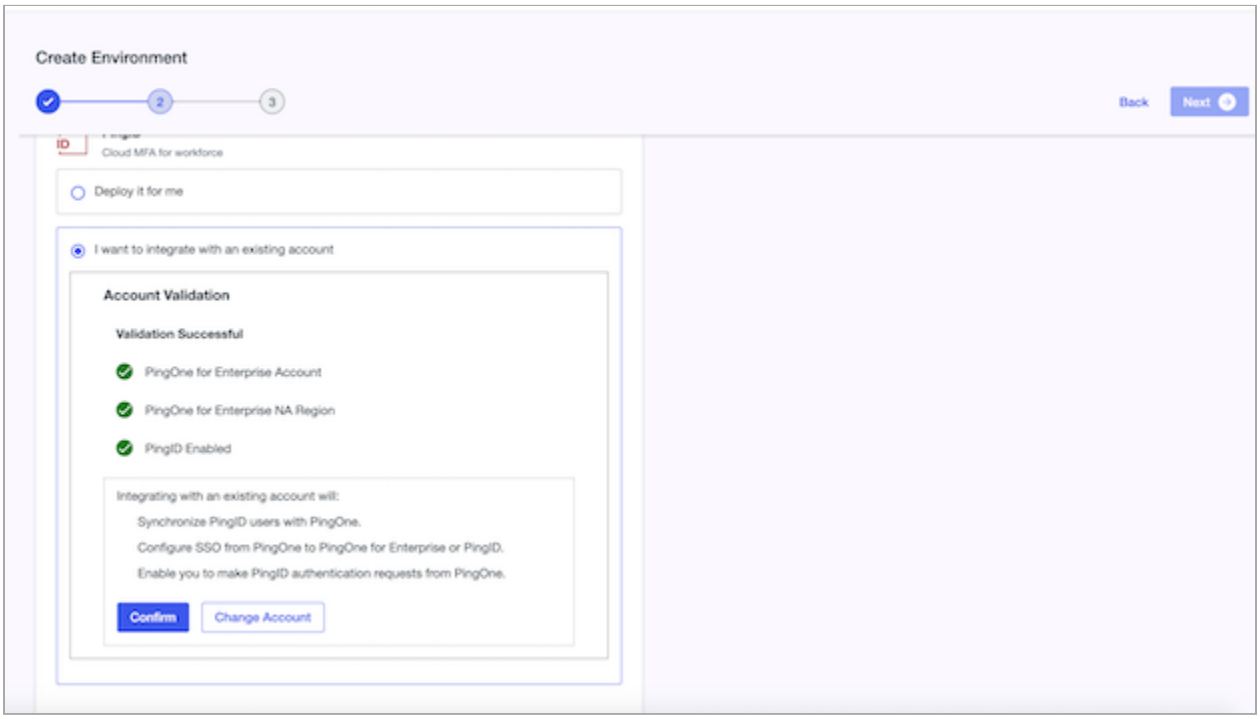
8. In the **Username** and **Password** fields, enter the administrator credentials for your existing PingID tenant.

9. Click **Validate Account**.

Copyright © 2025 Ping Identity Corporation



10. After PingOne has validated your account, click **Confirm**.



11. Click **Next**.

12. Define your environment by entering the following:

Field	Description
Environment Name	A unique identifier for the environment.

Copyright © 2025 Ping Identity Corporation

Field	Description
Description (optional)	A brief description of the environment.
Environment Type	Select **Sandbox** or **Production**. Sandbox environments are typically used for configuration and testing before deployment. Production environments are typically used for live configurations that are deployed for real-world use. Learn more about environment types in Sandbox and Production environments.
Generate sample populations and users in this environment	Select this check box to generate two populations and 40 sample users in the new environment.
Region	The appropriate geographical region for the environment. The list shows only regions that are included with your license. **Important** You can't change the region after the environment has been created.
License	Select the license to use for this environment. The available licenses for your organization are shown in the **License** list. Learn more in Licenses and Platform Limits.

13. Click **Finish**.

Result

The new environment is created in your PingOne organization and is listed on the **Environments** page.

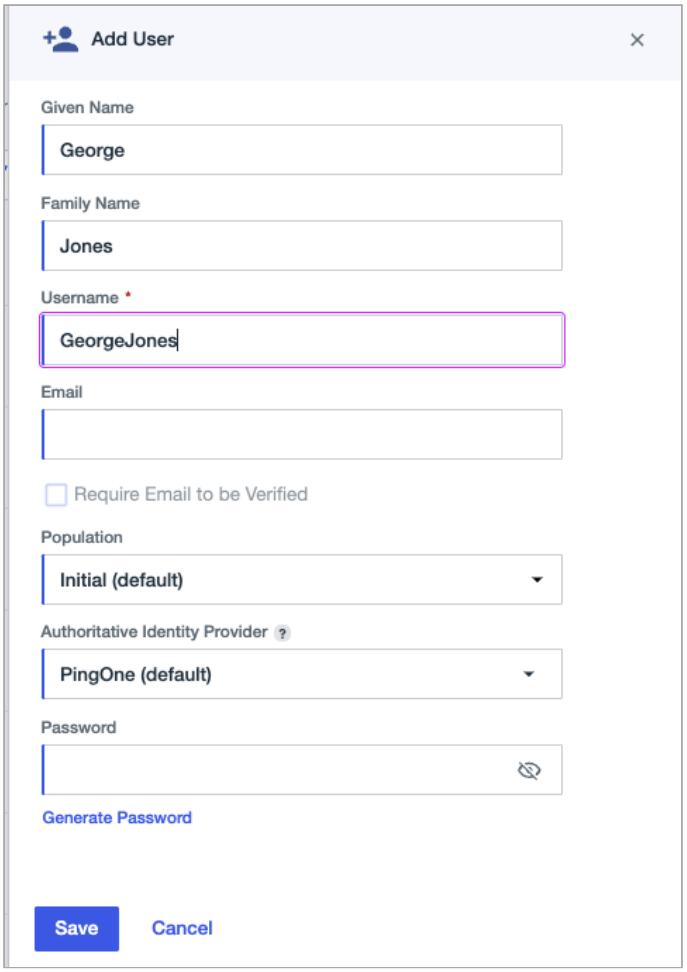
Creating demo users

This task walks you through the creation of users that you'll use later for the user simulation.

Steps

1. Go to **Directory** > **Users**.
2. On the **Users** page, click the **+** icon.
3. In the **Add User** panel, enter a **Given Name** of `George` and a **Family Name** of `Jones`.
4. Enter a **Username** of `GeorgeJones`.

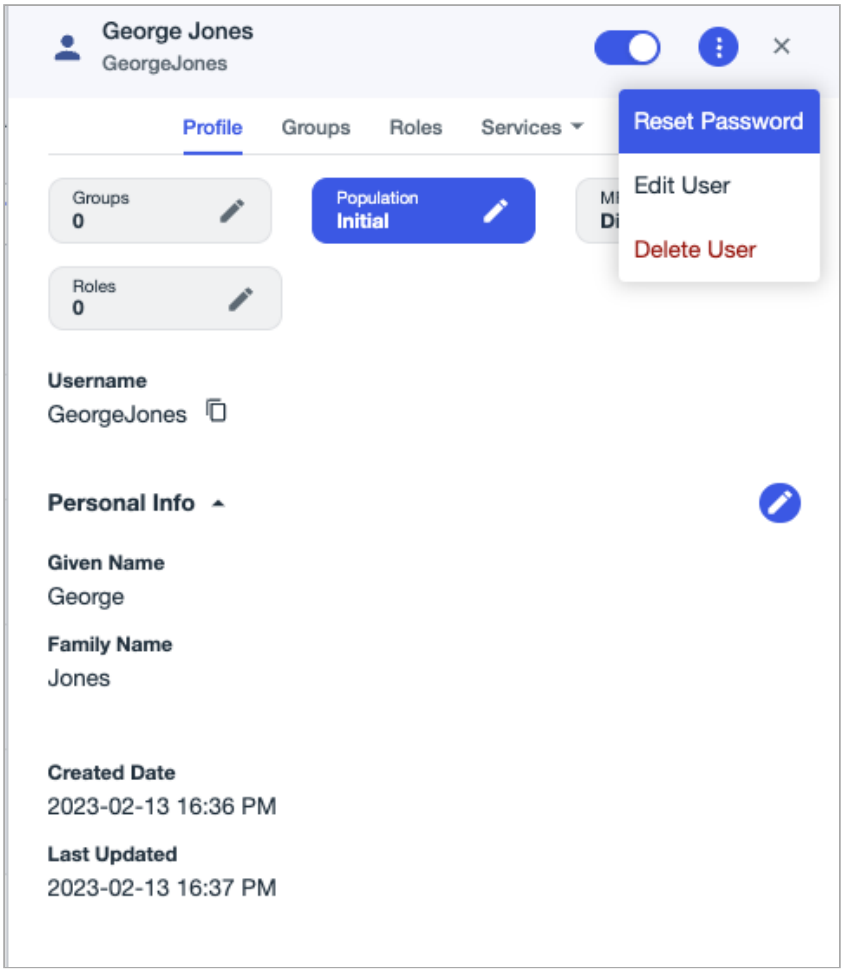
Copyright © 2025 Ping Identity Corporation



5. Click **Save**.

6. On the details panel for the user George Jones, click the options menu and then click **Reset Password** to create a temporary password so that George can log in to the web application that we'll create later.

Copyright © 2025 Ping Identity Corporation



7. Click the + icon, and repeat these steps to create another user with the **Given Name** `Sally`, **Family Name** `Smith`, and **Username** `SallySmith`.

8. Add another user with **Given Name** `Lucy`, **Family Name** `Greene`, and **Username** `LucyGreene`.

Next steps

Continue by Creating a group with dynamic membership.

Creating a group with dynamic membership

Creating groups for your users is not required, but groups are useful for organizing users who share the same criteria such as job title, region, and so on.

About this task

As part of this demo, you can experience group based access control during the user simulation. For the purposes of this demo, creating a group is optional.

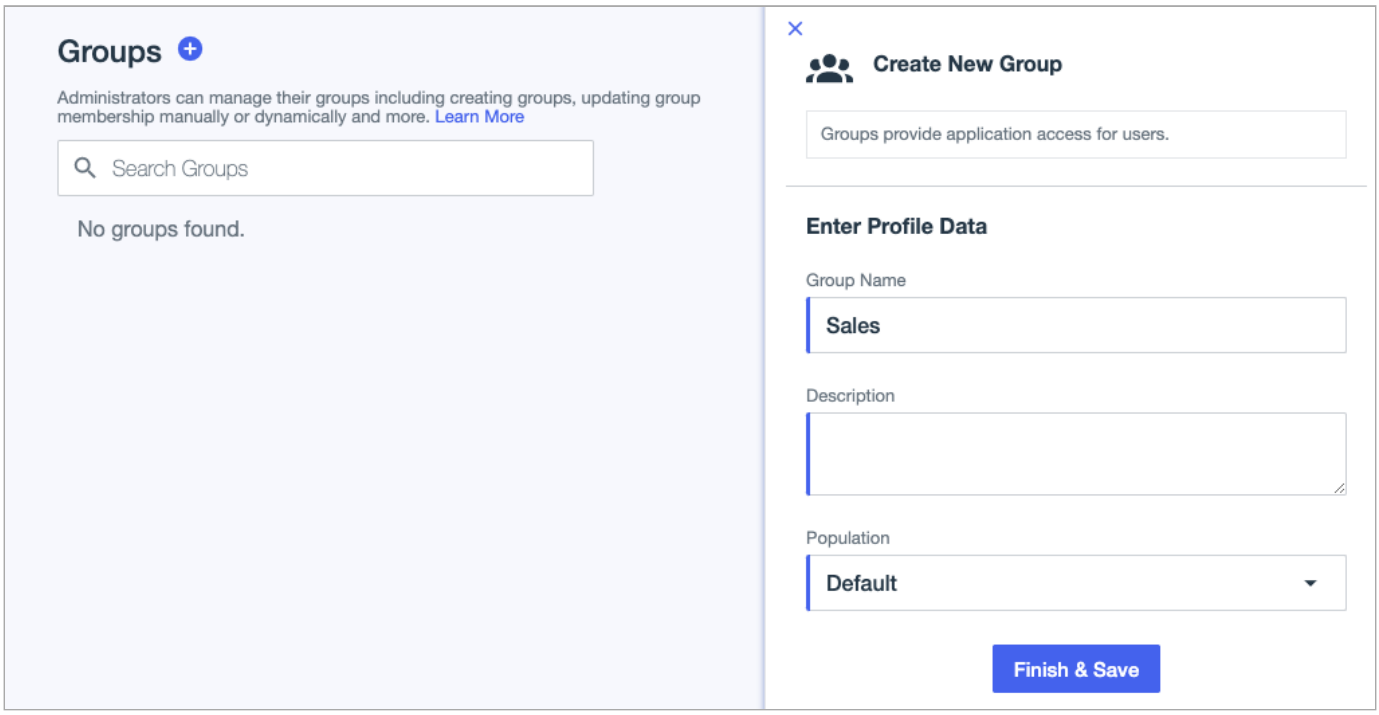
Steps

1. Go to **Directory** > **Groups**.

2. Click the + icon.

Copyright © 2025 Ping Identity Corporation

3. In the **Create New Group** panel, enter a **Group Name**, and select **Default** in the **Population** list.

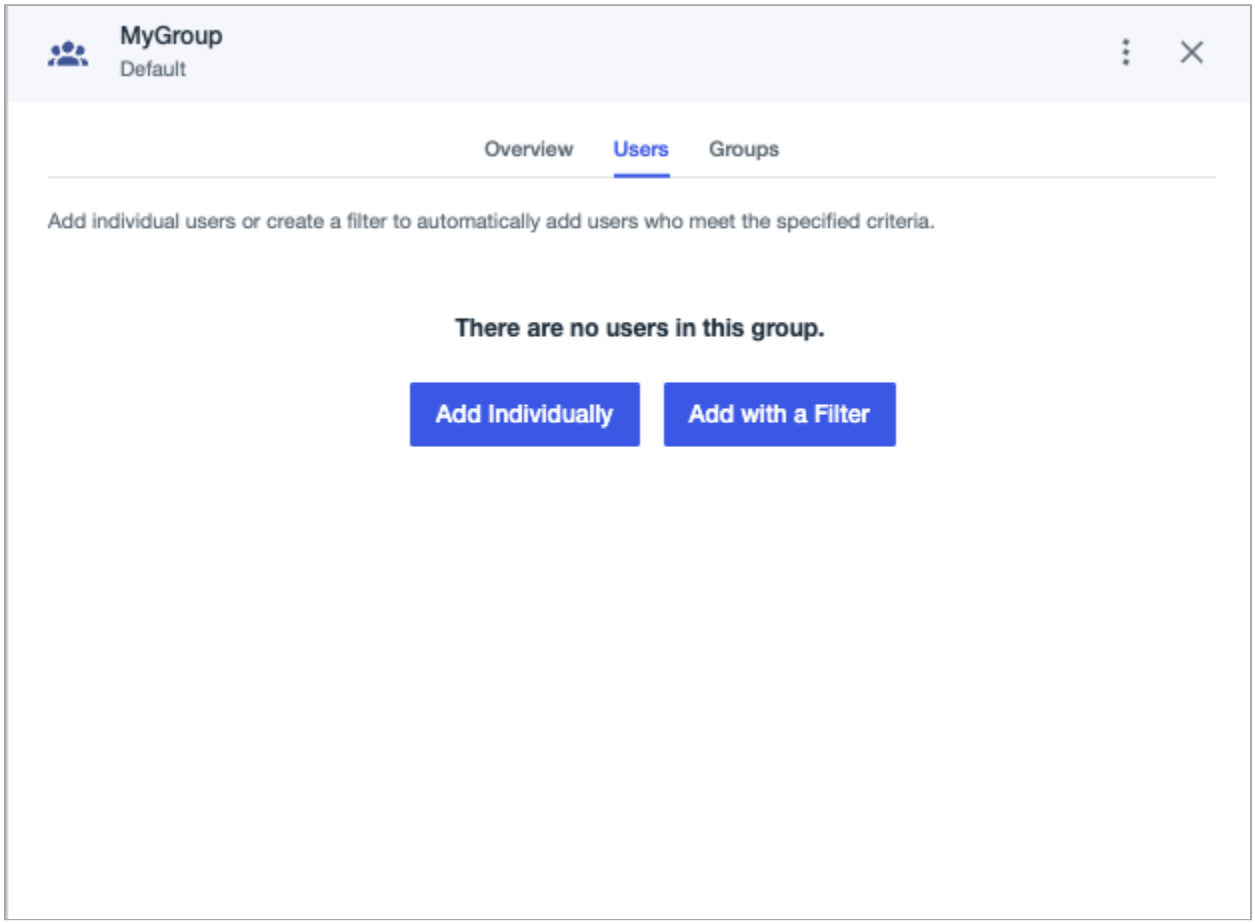


4. Click **Finish & Save**.

5. Click your new group to show the summary panel.

6. Click the **Users** tab.

Copyright © 2025 Ping Identity Corporation

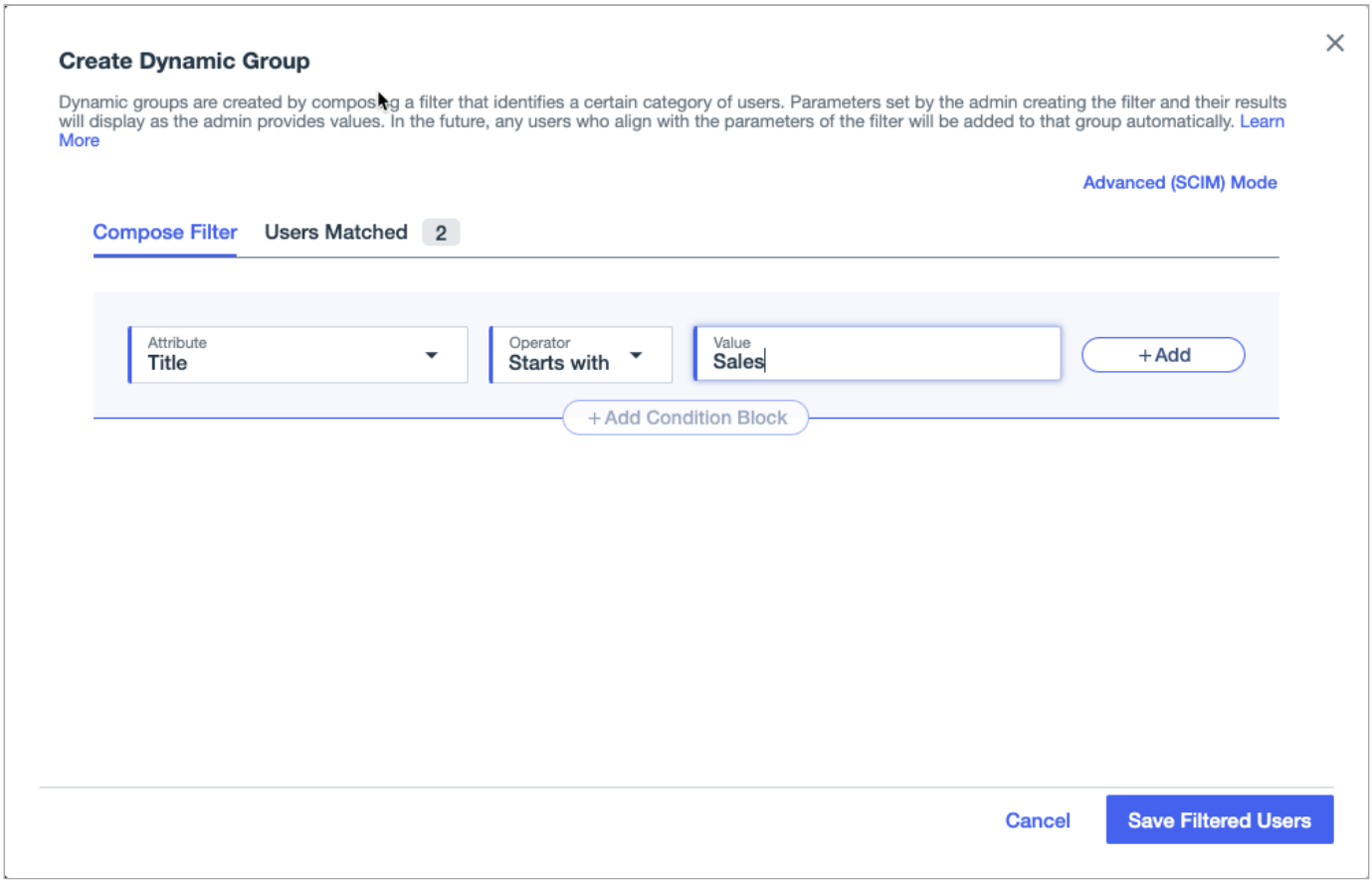


You can add members either individually or through a filter. For this example, we'll dynamically add users to the Sales group who have titles starting with "Sales."

7. Click **Add with a Filter**.

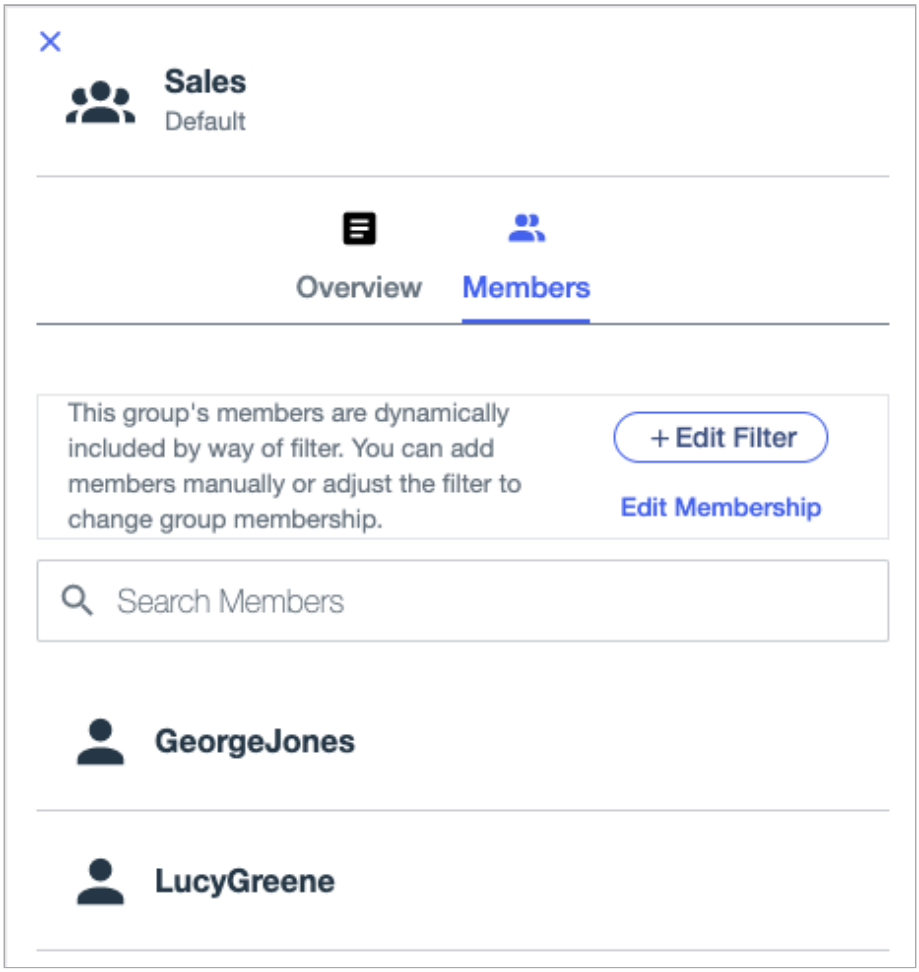
8. In the **Attribute** list, select **Title**, in the **Operator** list, select **Starts with**, and in the **Value** field, enter `Sales`. **Click Save Filtered Users**.

Copyright © 2025 Ping Identity Corporation



As you can see, George and Lucy have been added to the Sales group.

Copyright © 2025 Ping Identity Corporation



Next steps

Continue by Creating a web application.

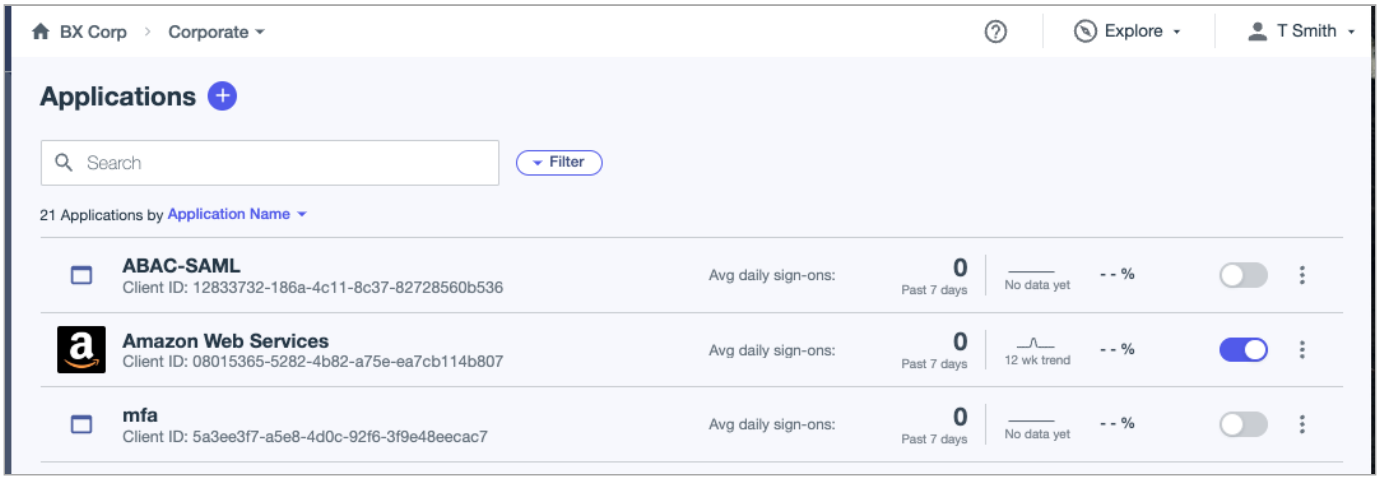
Creating a web application

Now that we've added our environment, and created new users and a group, we'll create a web application that uses a SAML connection.

Steps

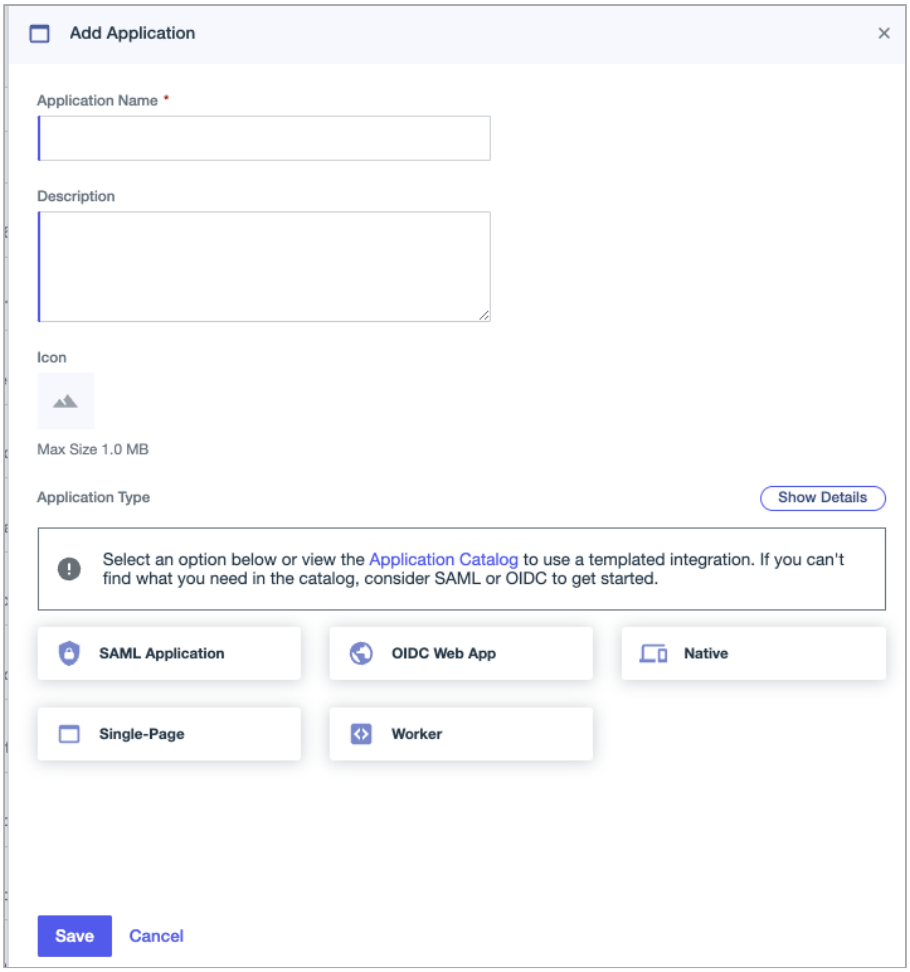
1. Go to **Applications** > **Applications**.
2. In the **Applications** window, click the **+** button.

Copyright © 2025 Ping Identity Corporation



3. In the **Add Application** panel, enter an **Application Name**, an optional **Description**.

> **Tip**
>
> Add an icon for your application so that it is easy to identify on the Application Portal.

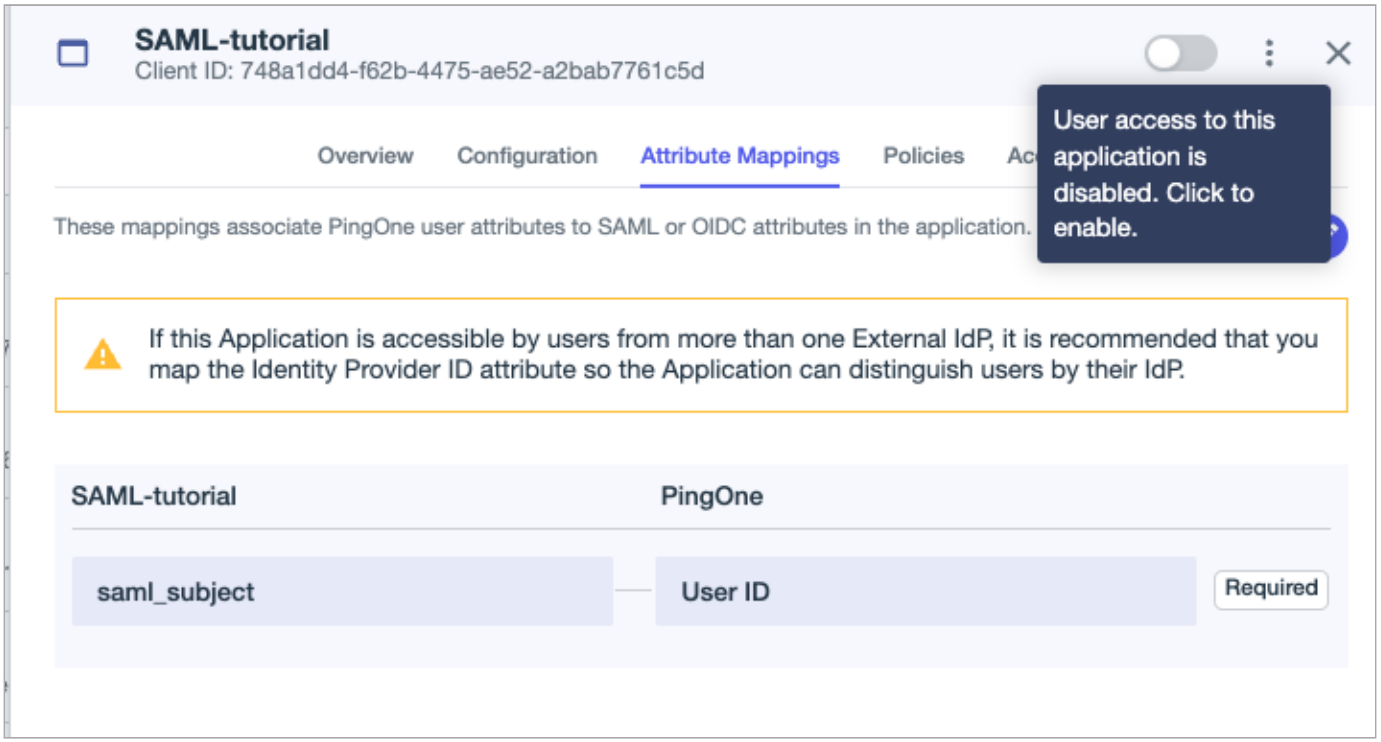


4. Click **SAML Application** and then click **Configure**.

5. For SAML Configuration, select **Manually Enter**.

Copyright © 2025 Ping Identity Corporation

6. Enter the following:
   - **ACS URLs**: `https://decoder.pingidentity.cloud/saml`
   - **Entity ID**: `pingidsamldecoder`
7. Click **Save**.
8. At the top of the panel, click the toggle to enable the application.



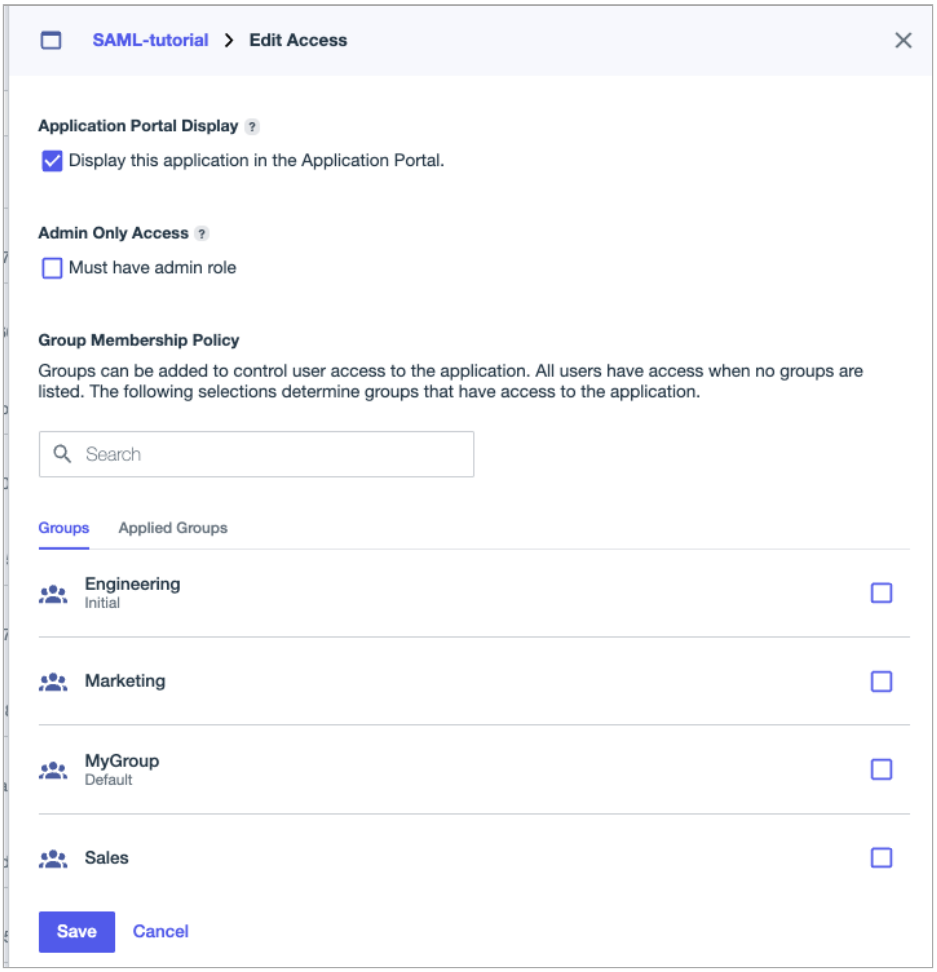
Limiting access to the application

We'll now limit access to the application to the Sales group.

Steps

1. Go to **Applications > Applications**. Locate your application and click the application entry to open the details panel.
2. Click the **Access** tab and then click the pencil icon.
3. Under **Groups**, select the check box for the **Sales** group.

Copyright © 2025 Ping Identity Corporation



4. Click **Save**.

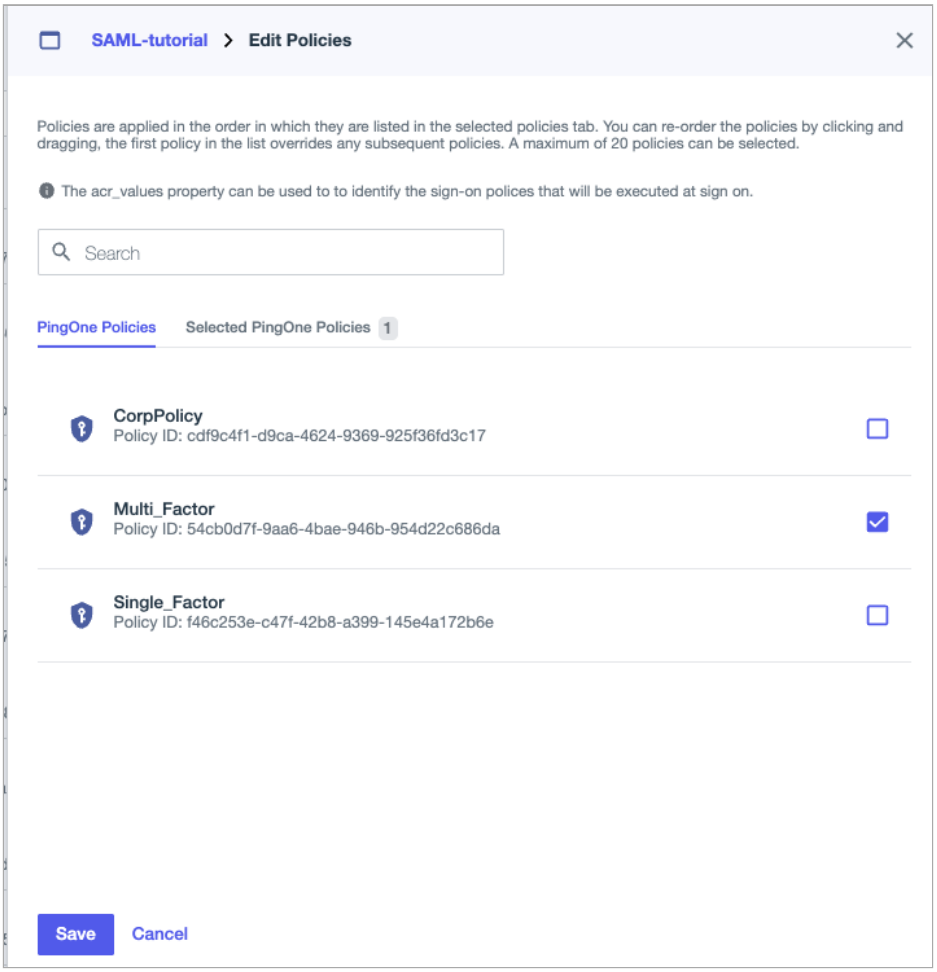
Assigning the Multi_Factor authentication policy to the application

We'll now assign the Multi-factor authentication policy to your web application. The application should still be open for edit.

Steps

1. Go to **Applications > Applications**. Locate your application and click the application entry to open the details panel.
2. Click the **Policies** tab and then click the pencil icon.
3. Under **PingOne Policies**, select the check box for the **Multi_Factor** policy.

Copyright © 2025 Ping Identity Corporation



4. Click **Save**.

Optional: Configuring PingID policy

You can configure the default PingID policy to add additional authentication methods and other policy criteria. For more information on PingID policy, see PingID documentation.

Steps

1. Go to **Authentication > Authentication**.
2. Expand the **Multi_Factor** policy and click the pencil icon to edit it.
3. In the **PingID Authentication step**, click the link to **Configure now**.
4. Configure the PingID policy and then click **Save**.

Next steps

Continue this demo by Performing the user simulation.

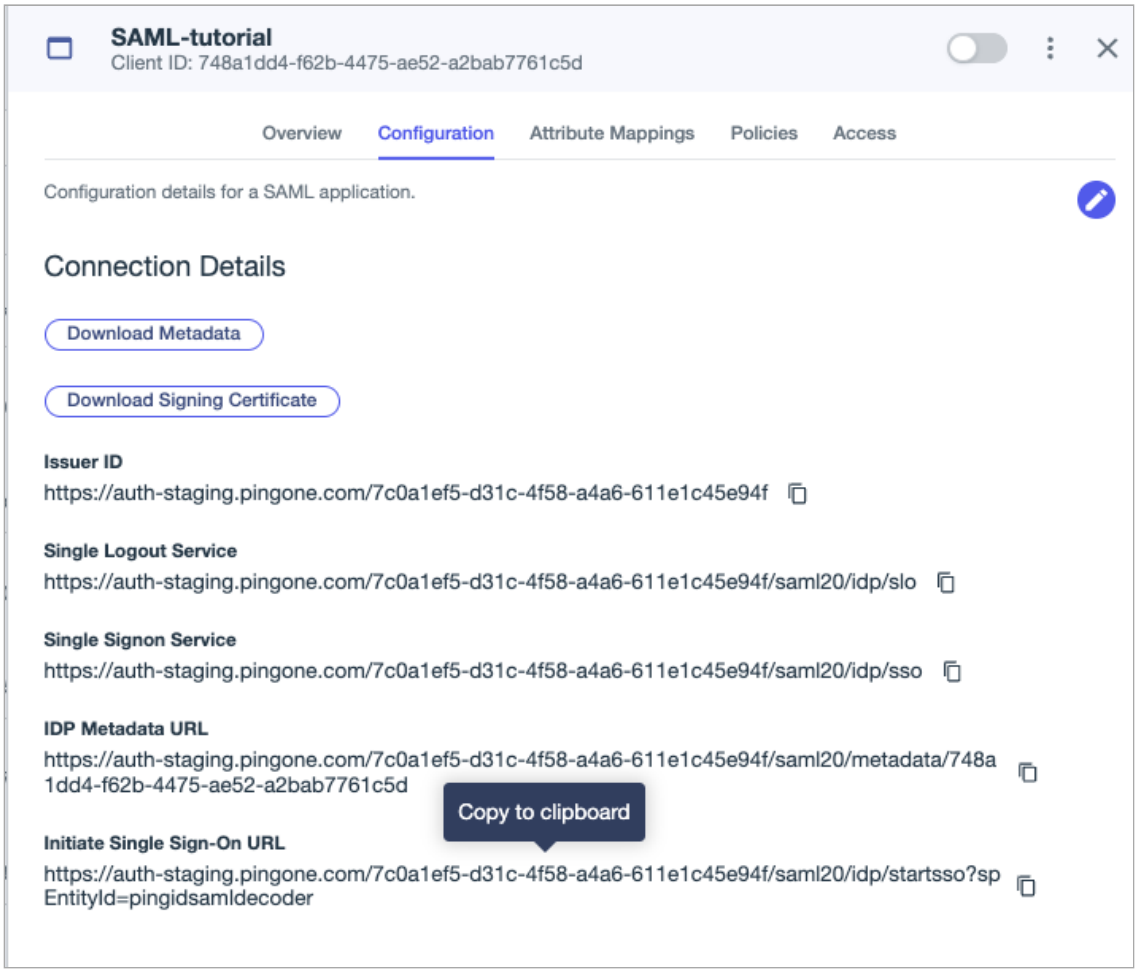
Copyright © 2025 Ping Identity Corporation

Performing the user simulation

The user simulation illustrates how to sign on to Ping Identity as a new user, create a new password, and access and install the PingID app on your mobile device.

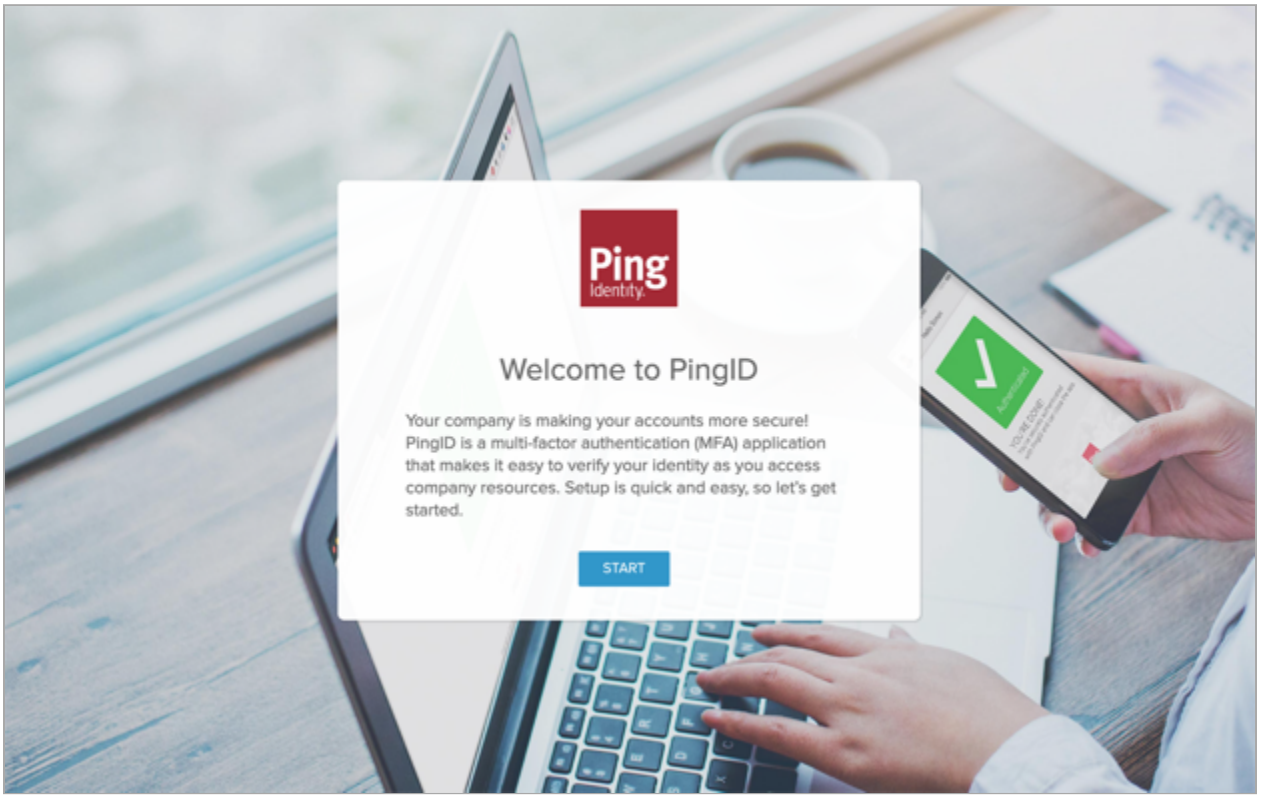
Steps

1. Go to **Applications > Applications**. Locate your application and click the application entry to open the details panel.
2. Click the **Configuration** tab, then copy the **Initiate Single Sign-on URL**.

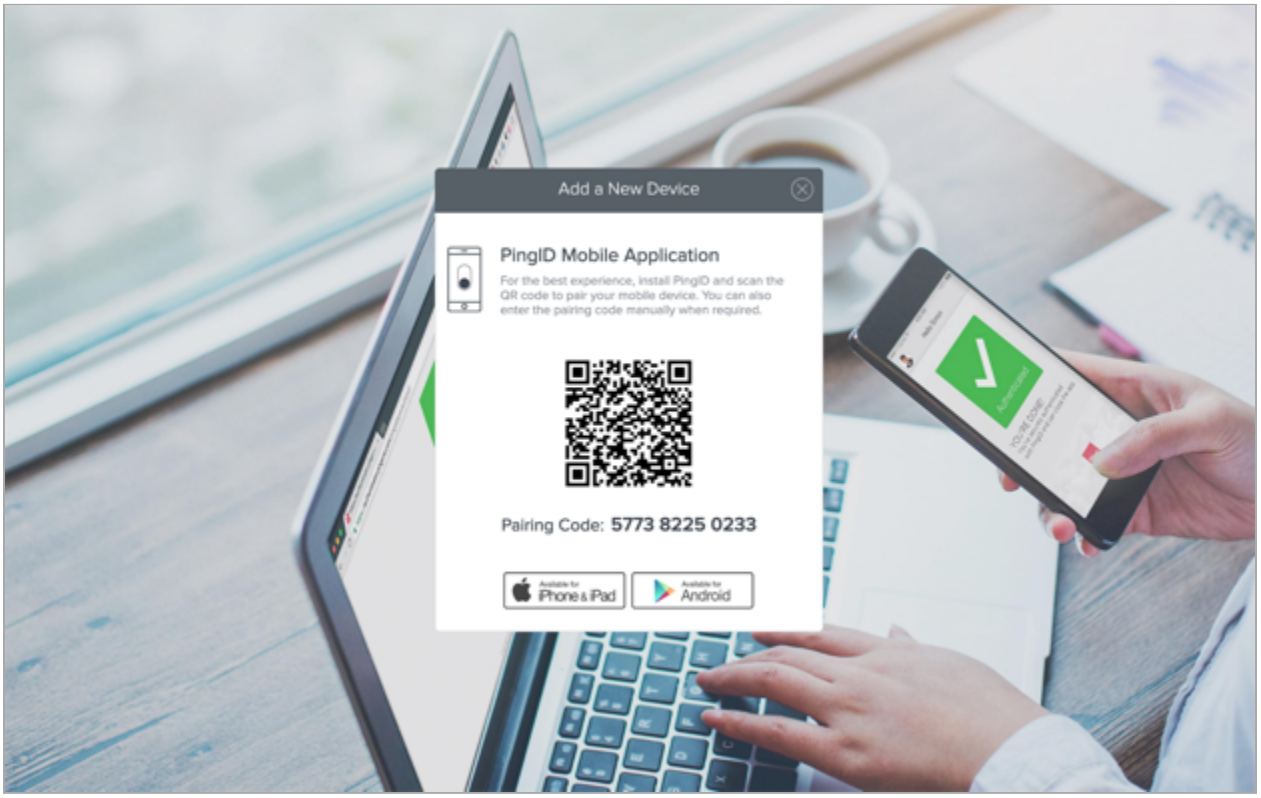


3. Open an incognito window in your browser, and go to the URL you copied.
4. Sign on as GeorgeJones using the temporary password.
5. Create a new password, and click **Save**. You should see the following PingID window.

Copyright © 2025 Ping Identity Corporation



6. Click **Start**. The following screen appears:



7. **Optional:** If PingID is not installed on your mobile device, scan the QR code with your camera to open the download location for your device type. If required, install the app.

Copyright © 2025 Ping Identity Corporation

8. **Optional:** If the app is installed, scan the QR code or enter the Pairing Code manually.
9. After your device has been successfully paired, you will receive an authentication request. Acknowledge this authentication request.

10. To sign on as other users, close and reopen your incognito browser, and then return to the **Initiate Single Sign-on URL** from step 1.

    Result:

    If you have tested with all 3 users, you will note that both George and Lucy are permitted access to the resource. Sally, however, is denied access to the resource because she does not have a title that starts with the word "Sales".

Next steps

Congratulations! You've just configured and tested a multi-factor authentication experience.

Complete this demo by Reviewing the synchronization of users in PingID.

Accessing the application portal

Review each user's available applications by accessing the Application Portal.

Steps

1. Go to **Applications > Applications**.
2. Expand the **PingOne Application Portal** application.
3. Click the **Policies** tab, and click the **Pencil** icon to edit.

Copyright © 2025 Ping Identity Corporation

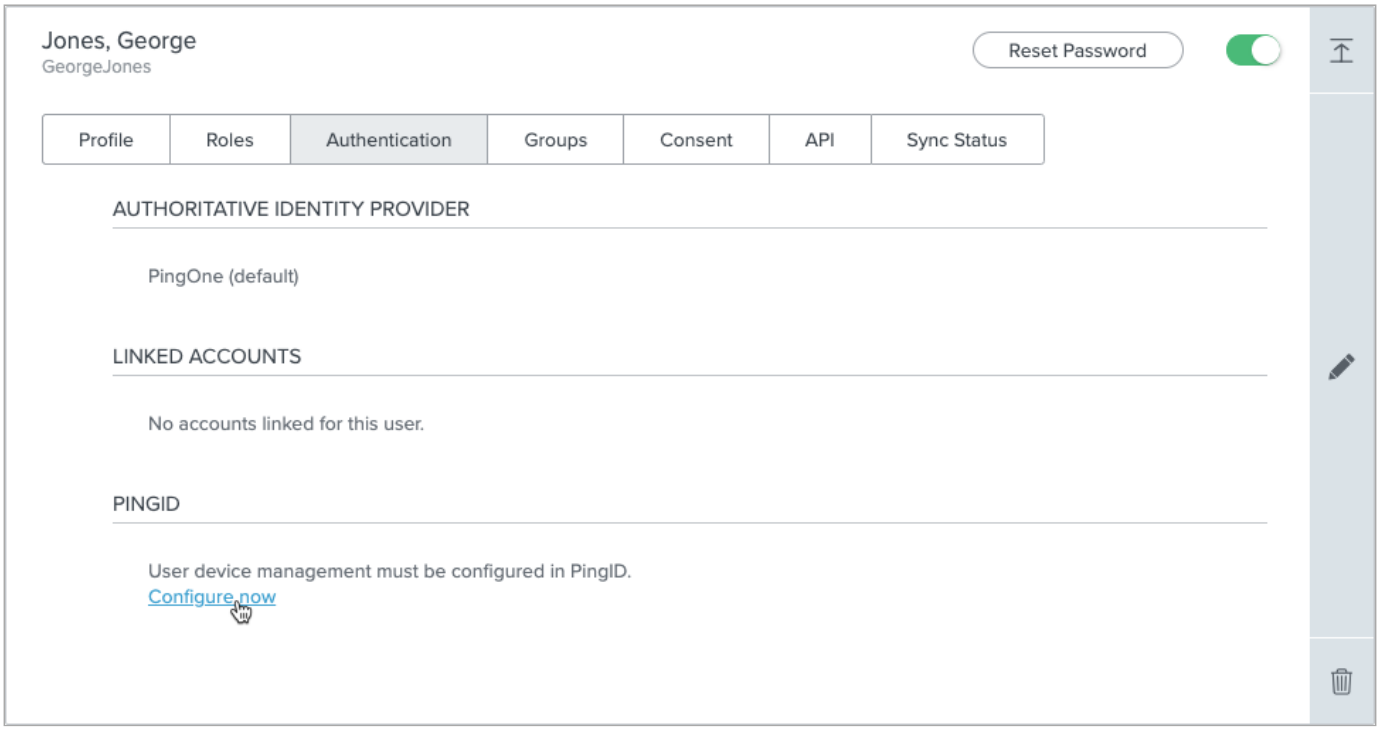
4. Click **+** to add **Multi_Factor** to**Applied Policies**.
5. Click **Save**.
6. Go to **Environment → Properties**.
7. Click the **Application Portal URL**.
8. Sign on with each user to review the applications that are available to them.

Reviewing the synchronization of users in PingID

You can access the PingID configuration portal to manage your PingID users.

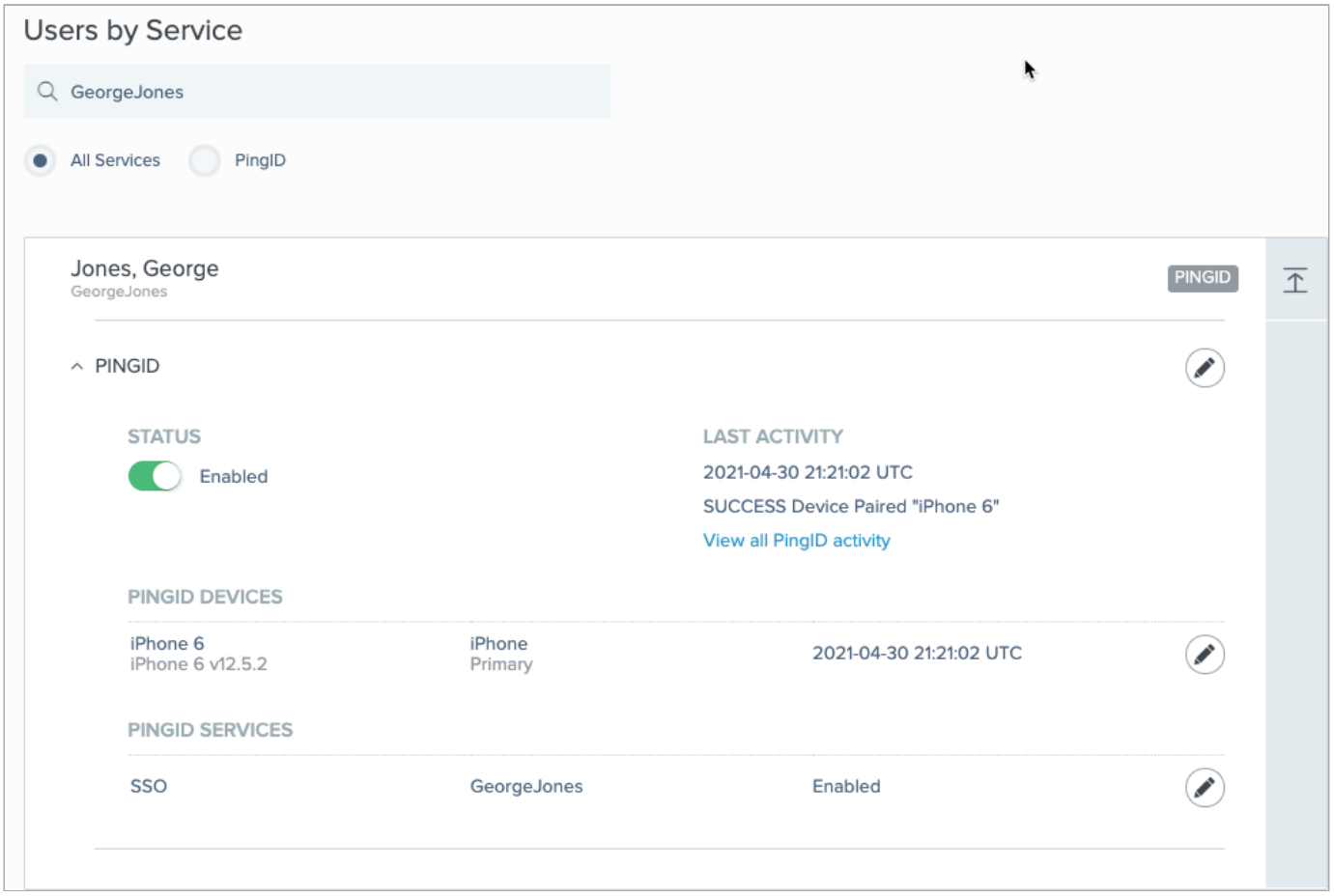
Steps

1. Go to **Directory** > **Users**.
2. Locate the user you want to manage, and click the user entry to open the details panel.
3. Click the **Authentication** tab, and click **Configure now** under **PingID**.



4. In the **Users by Service** window, you can see the status of the user, disable or remove them if needed, unpair their device, and click a link to view all of their PingID activity.

Copyright © 2025 Ping Identity Corporation



Configure a basic passwordless login experience using PingOne and PingOne MFA

This document demonstrates a basic passwordless login experience using PingOne and PingOne MFA.

By the end of this document, you will have experienced multi-factor authentication (MFA) both from the administrator's perspective of configuration, and the end user's perspective of usage.

To configure a basic passwordless login experience using PingOne and PingOne MFA, follow these steps:

1. Start a PingOne trial.
2. Create an environment.
3. Create a registration application.
4. Create a login application.
5. Create a registration policy.
6. Create a passwordless login policy.
7. Create a group with dynamic membership.

Copyright © 2025 Ping Identity Corporation

8. Copy the sign-on URLs.
9. Simulate a registration and successful login.
10. Simulate a registration and access control-based login failure.
11. Access the application portal.

Starting a PingOne trial

Signing up for a 30-day free trial version is a great way to experience the power of PingOne for yourself.

About this task

Your trial organization includes:

- One trial license.
- Up to five environments in one region, including the Administrators environment, which is created when the new trial starts.
- An administrative user who has all the roles necessary to manage the organization and add other administrators.
- Up to 1000 active identities for the duration of the trial.

Even if you already have a PingOne license, you can still start a PingOne trial and evaluate the services available. Follow the appropriate set of instructions:

- Existing customers
- New customers

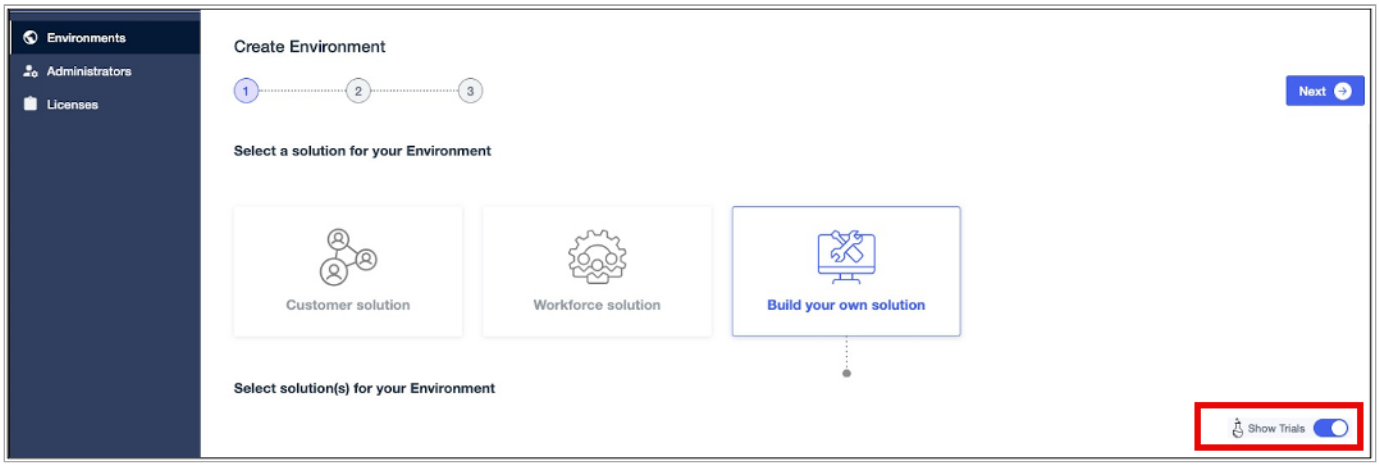
Existing customers

To sign up for the 30-day free trial, create a new PingOne environment in your organization and add the services that you want to evaluate.

Steps

1. Sign on to your PingOne environment, access the **Environments** page, and click **+** to create a new environment.
2. On the **Create Environment** page, select the type of solution you want to build and click **Next**.
3. Ensure that the **Show Trials** toggle is on.

Copyright © 2025 Ping Identity Corporation

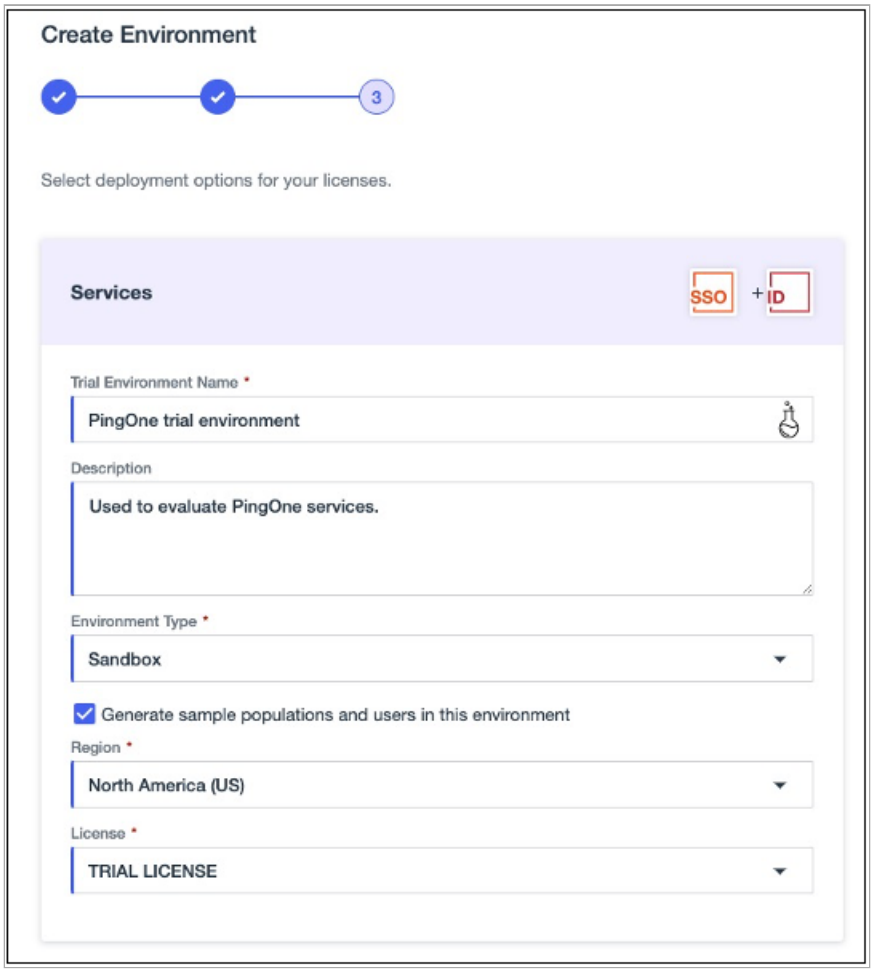


4. Select the services that you want to add to the environment and click **Next**.

5. Define your environment by entering the following:

Field	Description
Environment Name	A unique identifier for the environment.
Environment Description (optional)	A brief description of the environment.
Environment Type	Select **Sandbox**.
Generate sample populations and users in this environment	Select this checkbox to generate two populations and 40 sample users in the new environment.
Region	Select the region available in the list, which is determined by your PingOne organization.
License	Select **Create new trial license**.

Copyright © 2025 Ping Identity Corporation



6. Click **Finish**.

Result:

The new environment is created in your PingOne organization, and a new trial license is issued. The **Environments** page displays. You'll also be able to see the new license listed on the **Licenses** page.

New customers

To sign up for the 30-day free trial, provide your name, business email address, and verify it. You will receive access to a new PingOne organization and be prompted to sign on with the credentials you create during registration.

Steps

1. Go to pingidentity.com and click **Try Ping** on the right side of the page.

2. To activate your trial, check your email inbox and click **Verify Email** in the email sent to you.

Copyright © 2025 Ping Identity Corporation

3. Enter your first and last name, job title, and phone number in the appropriate fields. Note that you will be granted the Organization Admin role by default, which allows you to create, update, and delete environments and configure your organization to meet your needs.

4. Select the region available in the list, which is determined by your PingOne organization.

> **Important**
>
> PingOne data centers are available all over the world. For optimum performance, use the data center closest to your geographic region. Learn more in Organizations.

5. Create a password, select the checkbox to agree to the terms and conditions, and click **Start Trial**.

6. Enter the username and password you just created and click **Sign On**.

7. You're required to enroll in MFA to enhance your account security. Click **Continue**.

8. Select the MFA method that you want to use to authenticate:

   - **Email**: You'll provide your email address, receive an email with a passcode, and enter the passcode to sign on.
   - **Authenticator App**: You'll access the mobile authenticator app, receive a passcode, and enter the passcode to sign on.
   - **Passkey**: You'll create a passkey on your device using a biometric sensor or PIN and use that sensor or PIN to sign on.

Result:

After you complete the registration process, you'll be redirected to the **Environments** page, where you can begin creating identity solutions that meet your specific needs.

Next steps

Now, you can either add other administrators to the Administrators environment or create a new environment. Learn more in Managing administrators and Creating an environment.

Adding an environment

The first thing you should do after you start a PingOne trial or purchase a PingOne license is create an environment. A setup assistant guides you through this process.

About this task

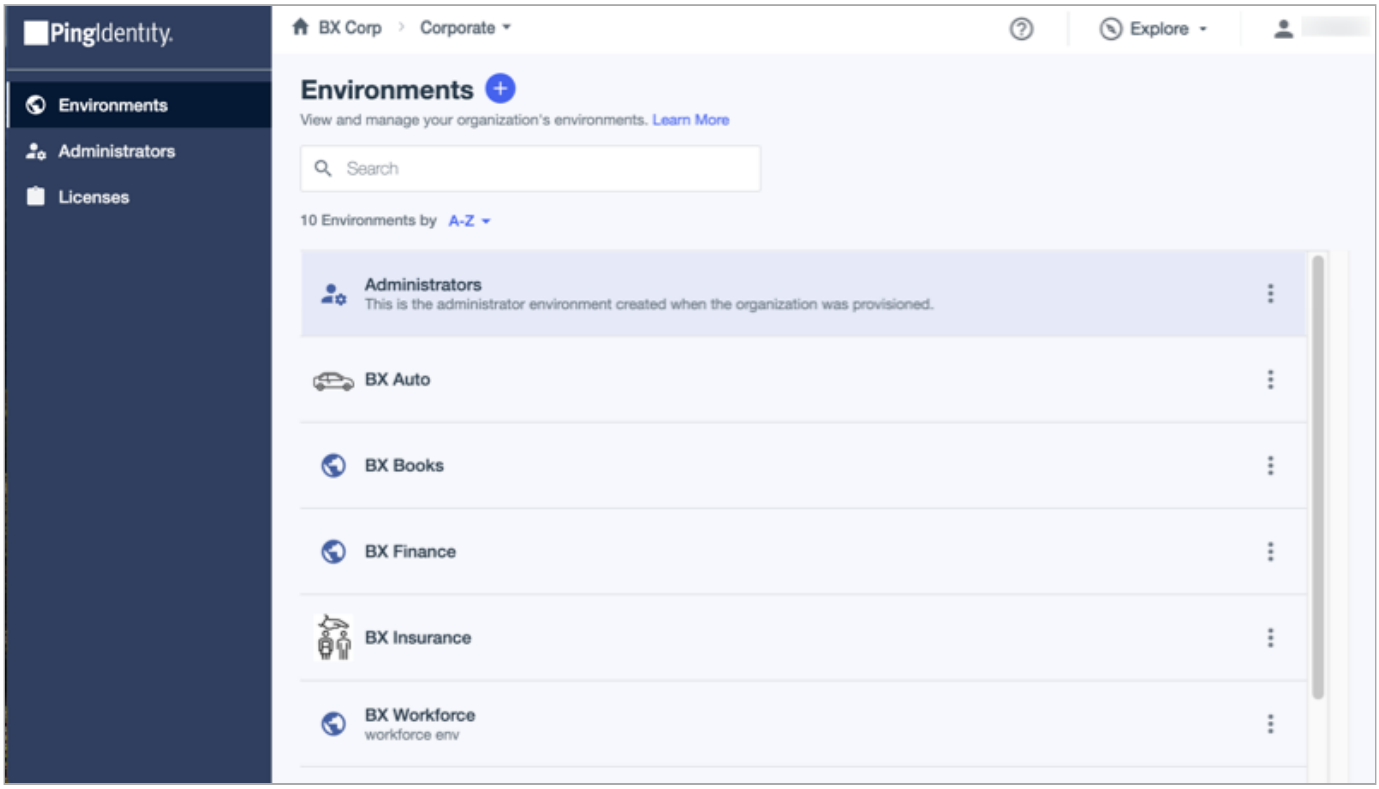
> **Note**
>
> You must have the Organization Admin role or a custom role with equivalent permissions to create an environment.

Steps

1. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page.

2. Click the **+** icon.

Copyright © 2025 Ping Identity Corporation

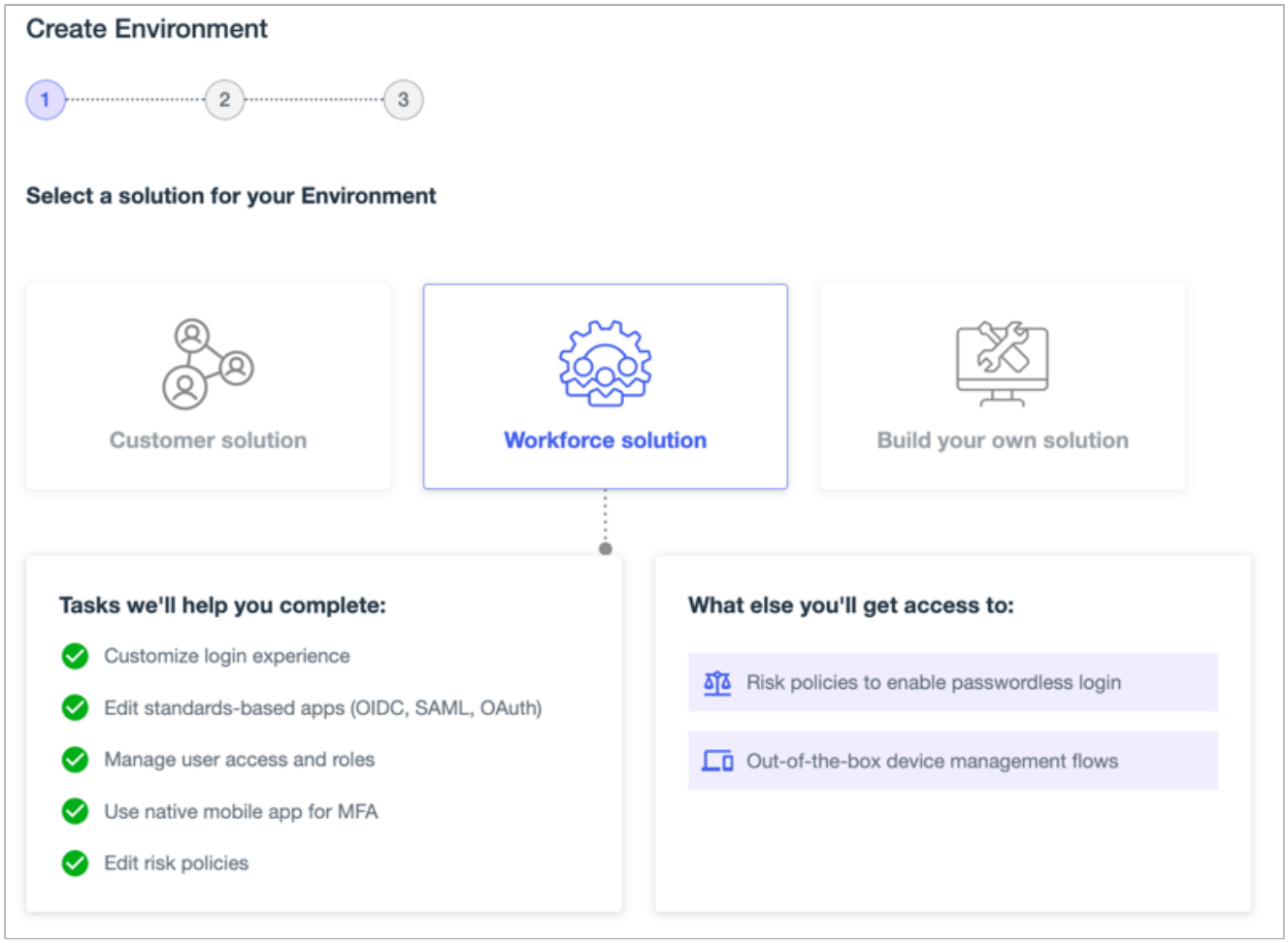


Result:

The **Create Environment** setup assistant starts.

3. Select the type of solution that you want to support in this environment.

Copyright © 2025 Ping Identity Corporation



Option	Description
Customer solution	Select to design registration and subsequent sign-on experiences for your customers and test them in a sample application tailored to your industry.
Workforce solution	Select to design single sign-on experiences for your employees, partners, and vendors.
Build your own solution	Select to choose from all of our services and products to build a hybrid solution that fits your unique use case.

4. Click **Next**.

   The services that will be deployed to your new environment are listed.

5. Click **Next**.

6. Define your environment by entering the following:

Copyright © 2025 Ping Identity Corporation

Field	Description
Environment Name	A unique identifier for the environment.
Description (optional)	A brief description of the environment.
Environment Type	Select **Sandbox** or **Production**. Sandbox environments are typically used for configuration and testing before deployment. Production environments are typically used for live configurations that are deployed for real-world use. Learn more about environment types in Sandbox and Production environments.
Generate sample populations and users in this environment	Select this checkbox to generate two populations and 40 sample users in the new environment.
Region	The appropriate geographical region for the environment. The list shows only regions that are included with your license. **Important** You can't change the region after the environment has been created.
License	Select the license to use for this environment. The available licenses for your organization are shown in the **License** list. For more information, see Licenses and Platform Limits.
Include a solution designer to easily design and test experiences (optional)	Customer and Workforce solutions only. If selected, after you create your environment, a solution designer opens and walks you through the process of designing your experiences.
Choose Your Industry (optional)	Customer solutions only. If you make a selection, PingOne creates a sample app tailored to the industry selected.

7. Click **Finish**.

Result

The new environment is created in your PingOne organization.

If you chose to build a customer or workforce solution, and selected the solution designer option, the solution designer opens and guides you through the process of designing and testing registration and sign-on experiences in less than 5 minutes.

If you did not select the solution designer option, or if you built your own solution, the **Environments** page opens. Locate your new environment by sorting the list alphabetically or by date created, or enter the environment name in the search box.

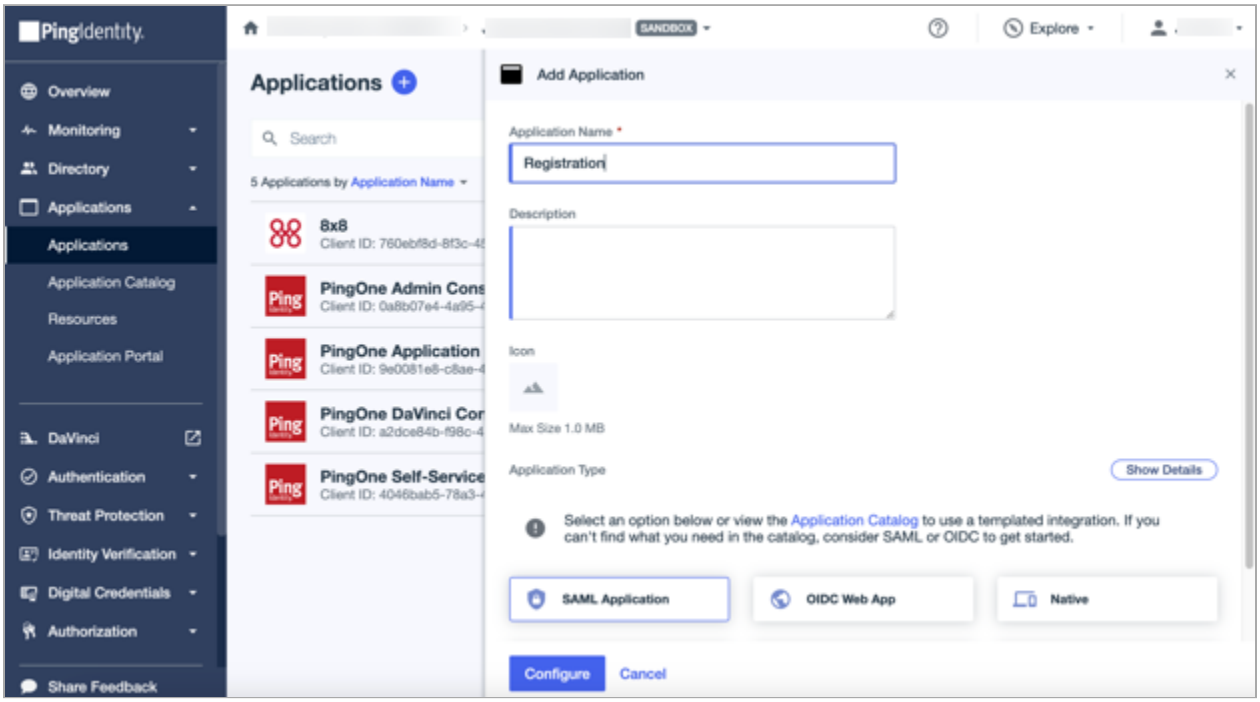
Creating a registration application

Create an application that your users can use to register.

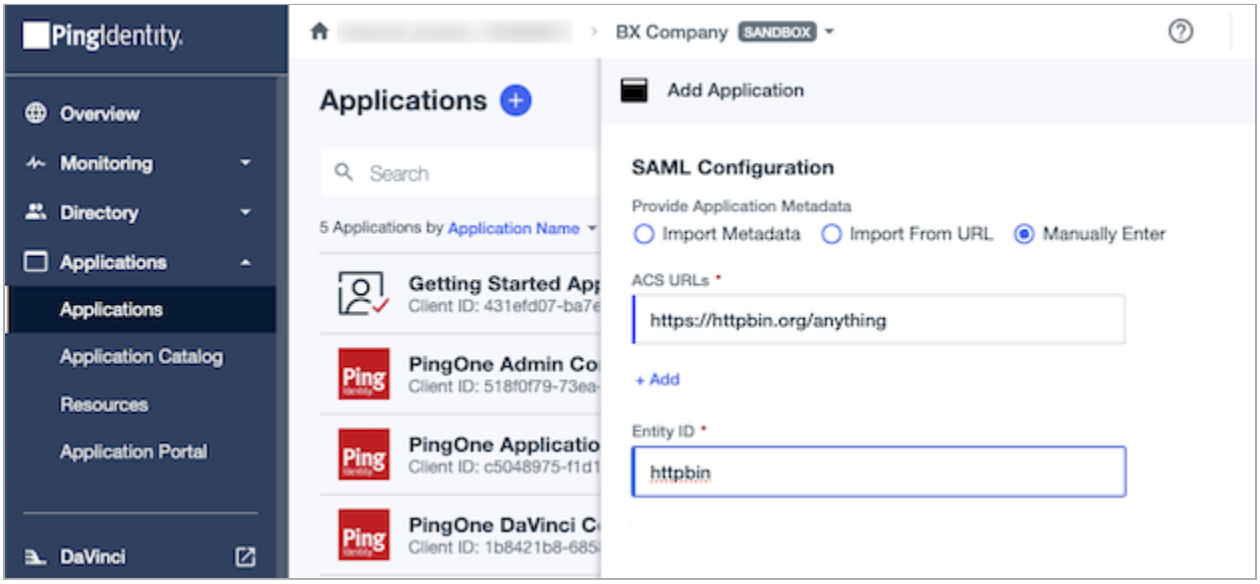
Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Applications > Applications**.
2. Click the **+** icon.
3. In the **Application Name** field, enter `Registration`.
4. Click **SAML Application**, and then click **Configure**.



5. Click **Manually Enter**.
6. In the **ACS URLs** field, enter `https://httpbin.org/anything`.



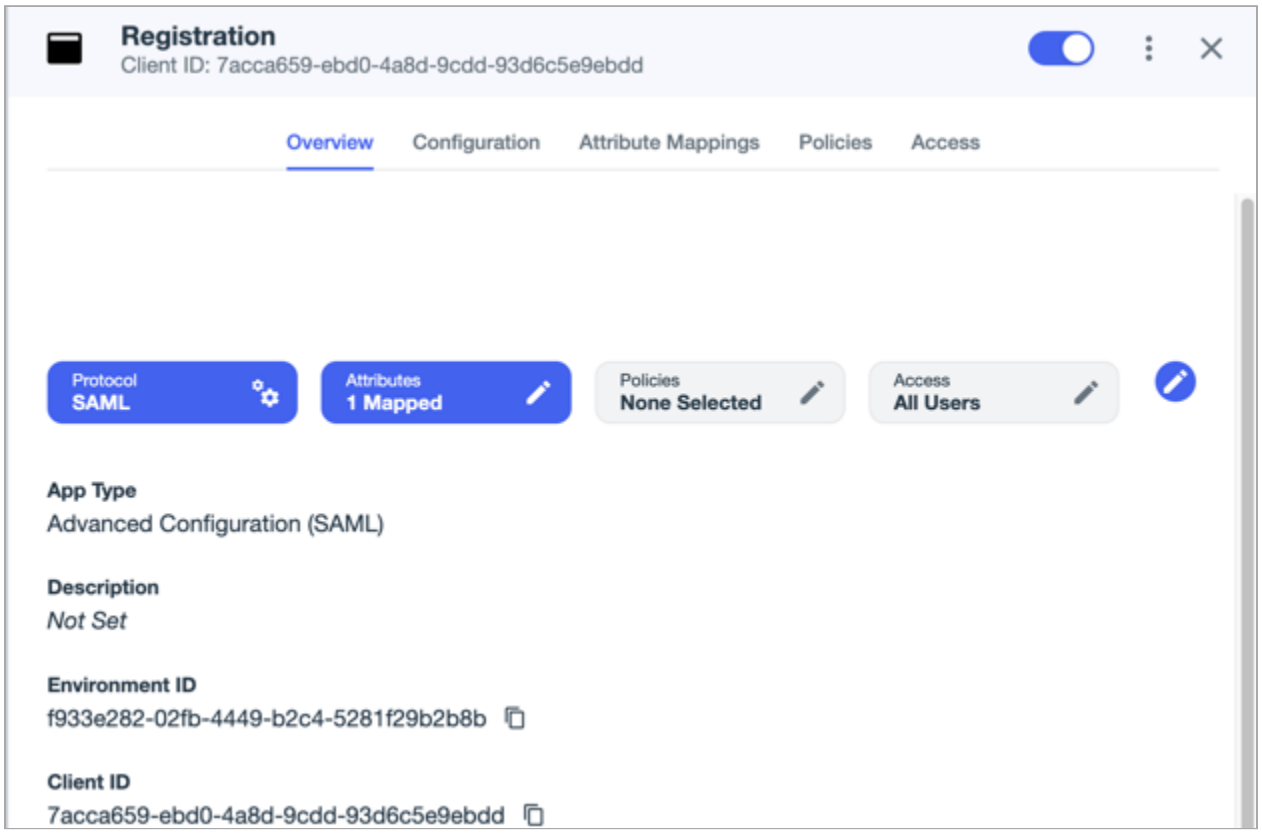
7. In the **Entity ID** field, enter `httpbin`, and then click **Save**.

Copyright © 2025 Ping Identity Corporation

Result:

PingOne adds the application the **Applications** list.

8. Click the **Configuration** tab, and then click the **Pencil** icon.
9. In the **Assertion Validity Duration (in seconds)** field, enter `180`.
10. Click **Save**.
11. In the **Applications** list, click the toggle in the top right to enable the application.



Next steps

Continue by Creating a login application.

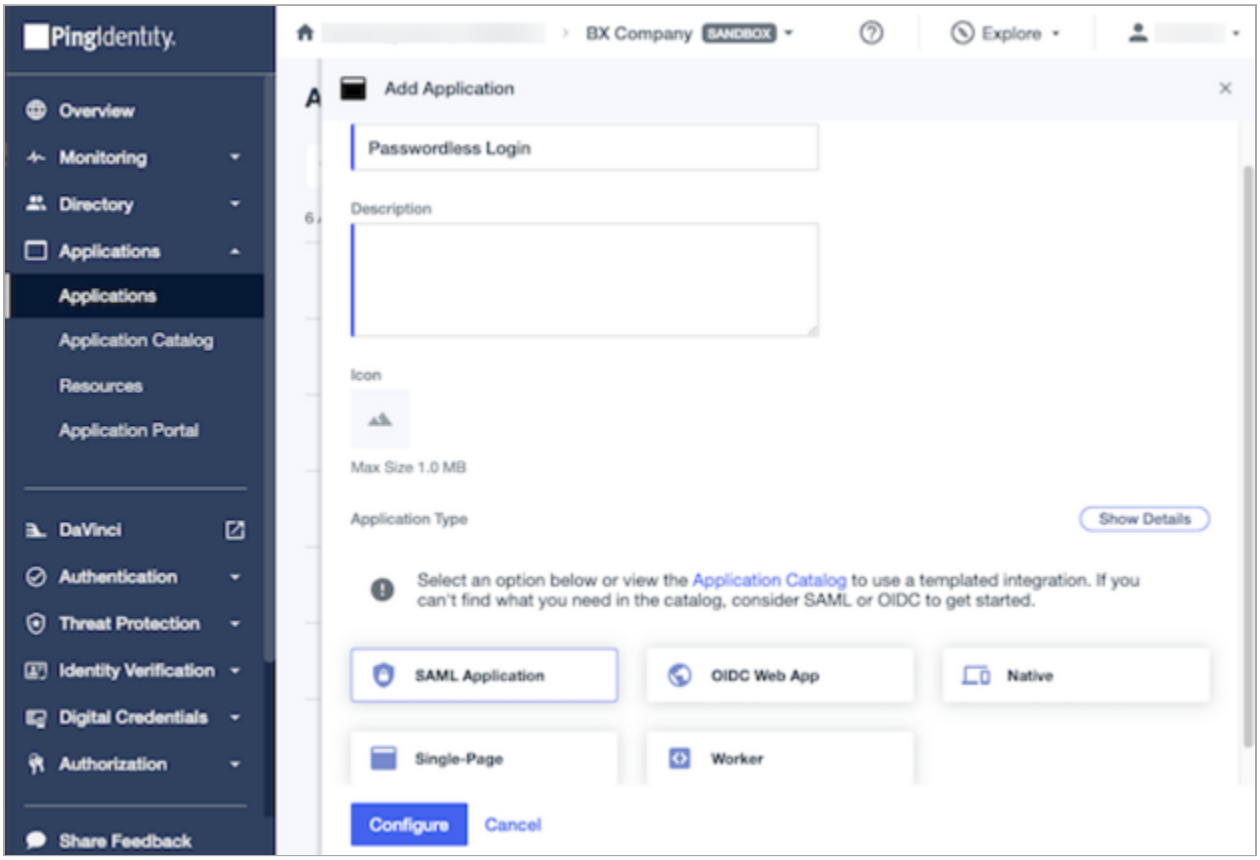
Creating a login application

Create an application that your users can use to log in.

Steps

1. Go to **Applications** > **Applications**.
2. Click the **+** icon.
3. In the **Application Name** field, enter `Passwordless Login`. Optionally, add a **Description** and an **Icon**.
4. Click **SAML Application**, and then click **Configure**.

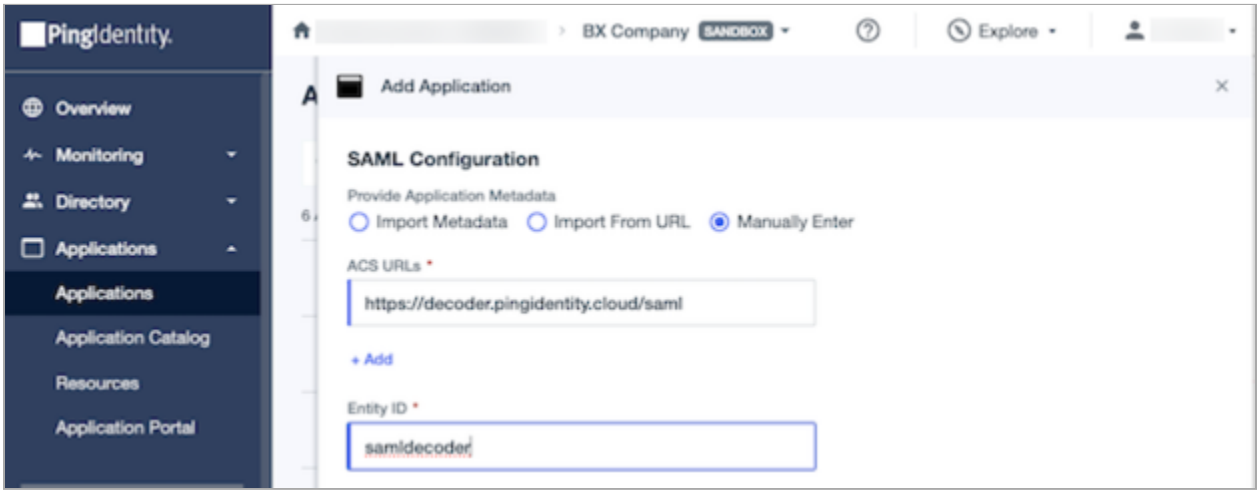
Copyright © 2025 Ping Identity Corporation



5. Click **Manually Enter**.

6. In the **ACS URLs** field, enter `https://decoder.pingidentity.cloud/saml`.

7. In the **Entity ID** field, enter `samldecoder`, and click **Save**.



Result:

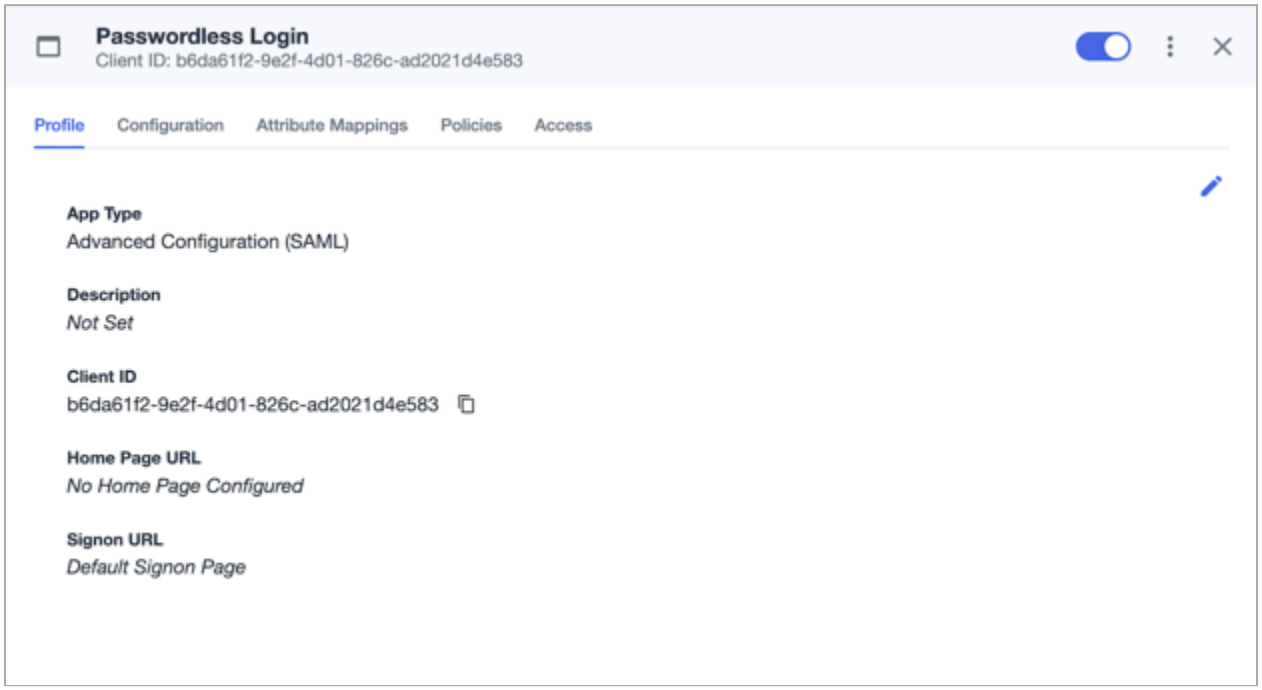
PingOne adds the application to the **Applications** list.

8. Click the **Configuration** tab, and then click the **Pencil** icon.

9. In the **Assertion Validity Duration (in seconds)** field, enter `180`.

Copyright © 2025 Ping Identity Corporation

10. Click **Save**.
11. Click the toggle in the top right to enable the application.



Next steps

Continue by Creating a registration policy.

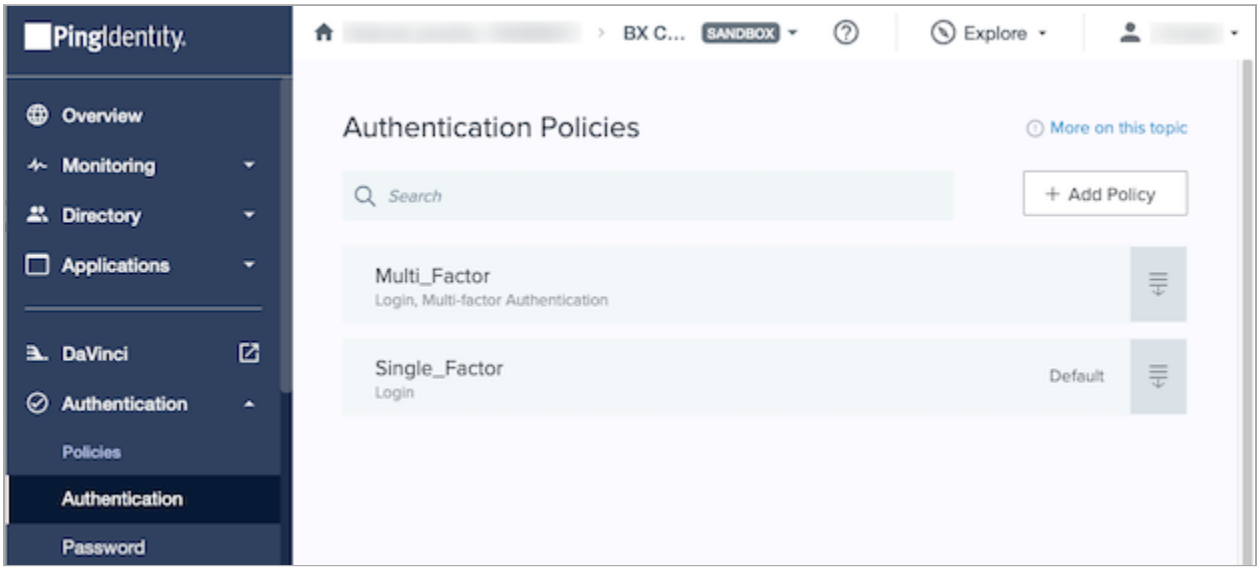
Creating a registration policy

Create a policy that includes a registration step so that users can create a user account.

Steps

1. Go to **Authentication > Authentication**.
2. Click **Add Policy**.

Copyright © 2025 Ping Identity Corporation

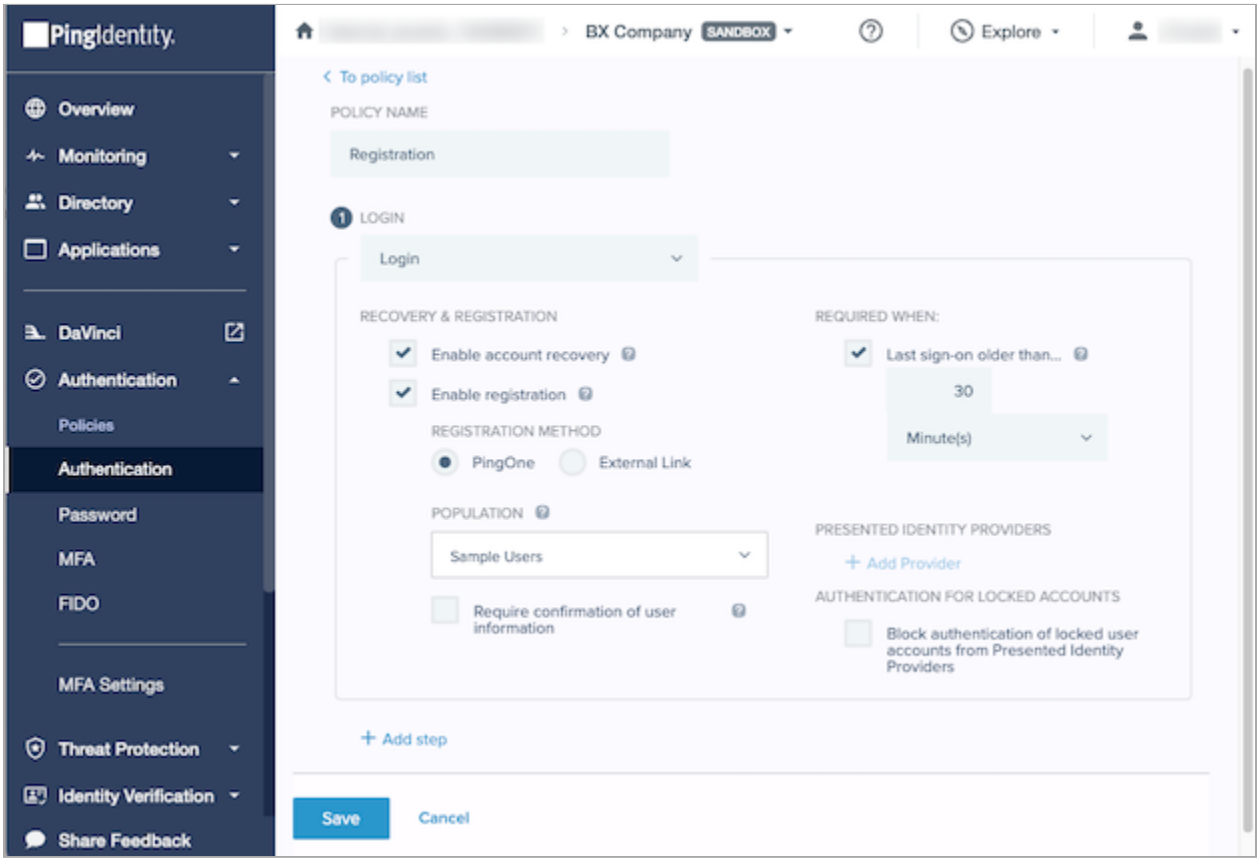


3. In the **Policy Name** field, enter `Registration`.

4. From the **Step Type** list, select **Login**.

5. Select the **Enable Registration** check box.

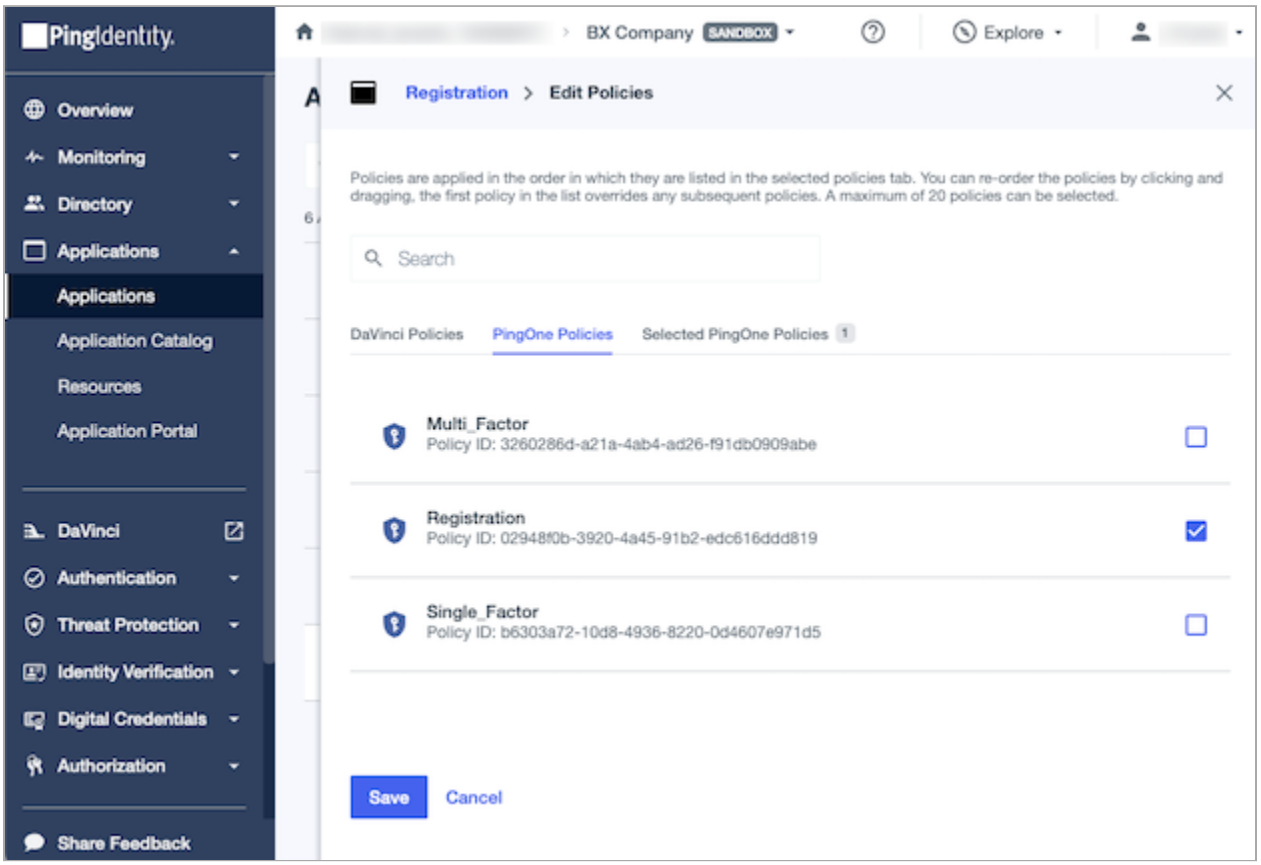
6. From the **Population** list, select **Default**.



7. Click **Save**.

Copyright © 2025 Ping Identity Corporation

8. Go to **Applications** > **Applications**.
9. Expand the **Registration** application and click the **Pencil** icon.
10. Click the **Policies** tab.
11. Click **+** or drag the **Registration** policy to the **Applied Policies** column.



12. Click **Save**.

Next steps

Continue by Creating a passwordless login policy.

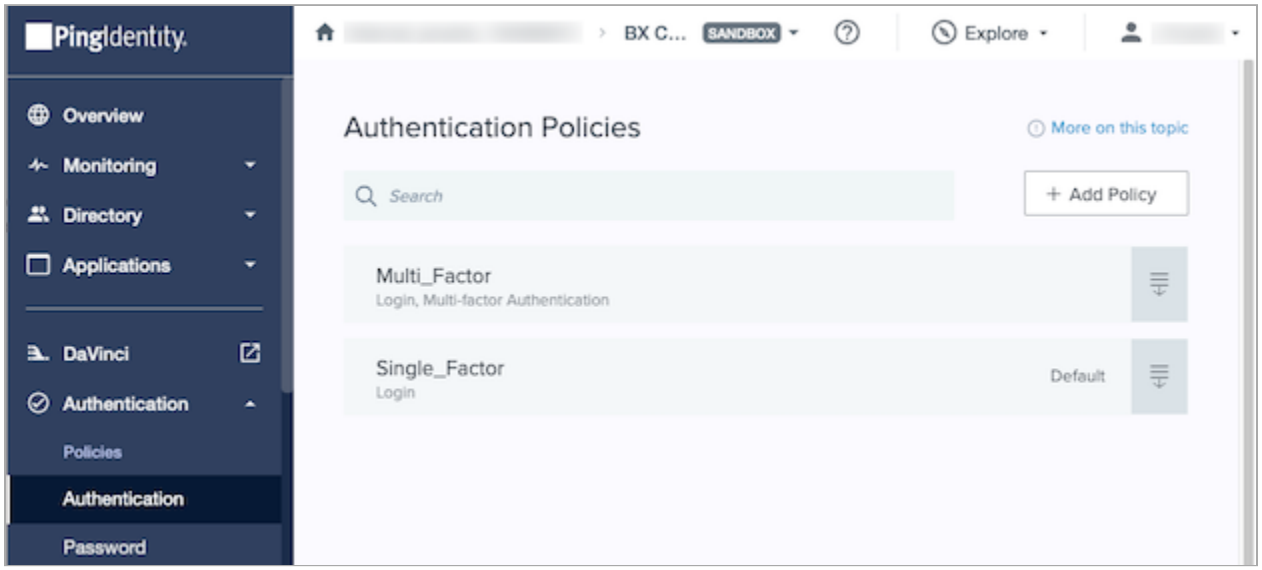
Creating a passwordless login policy

Create a login policy that allows users to log in with a one-time passcode (OTP) delivered via SMS.

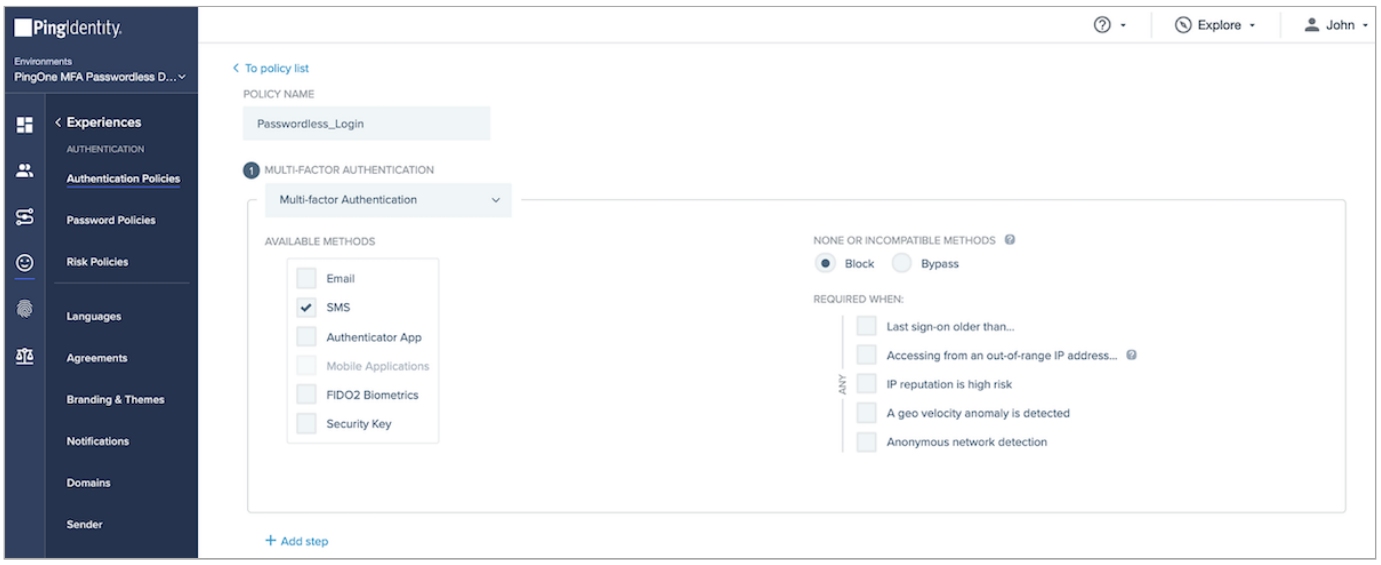
Steps

1. Go to **Authentication** > **Authentication**.
2. Click **Add Policy**.

Copyright © 2025 Ping Identity Corporation



3. In the **Policy Name** field, enter `Passwordless_Login`.
4. From the **Step Type** list, select **Multi-factor Authentication**.
5. Under **Available Methods**, select the **SMS** check box.



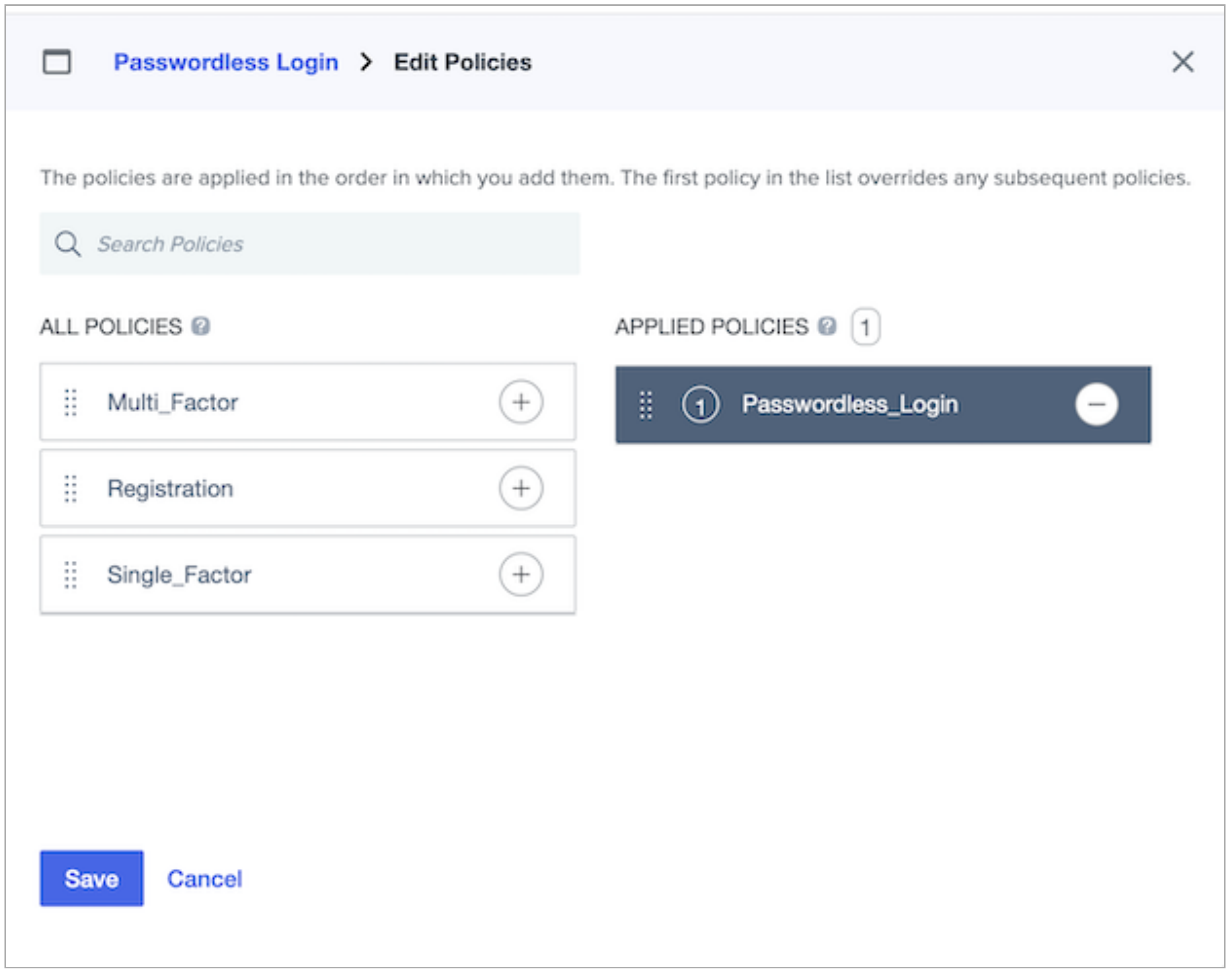
6. Click **Save**.

   Result:

   PingOne saves the policy and returns you to the **Policies** list.

7. Go to **Applications** > **Applications**.
8. Expand the **Passwordless Login** application.
9. Click the **Policies** tab and click the **Pencil** icon.
10. Click **+** or drag the **Passwordless_Login** policy to the **Applied Policies** column.

Copyright © 2025 Ping Identity Corporation



11. Click **Save**.

Next steps

Continue by Creating a group with dynamic membership.

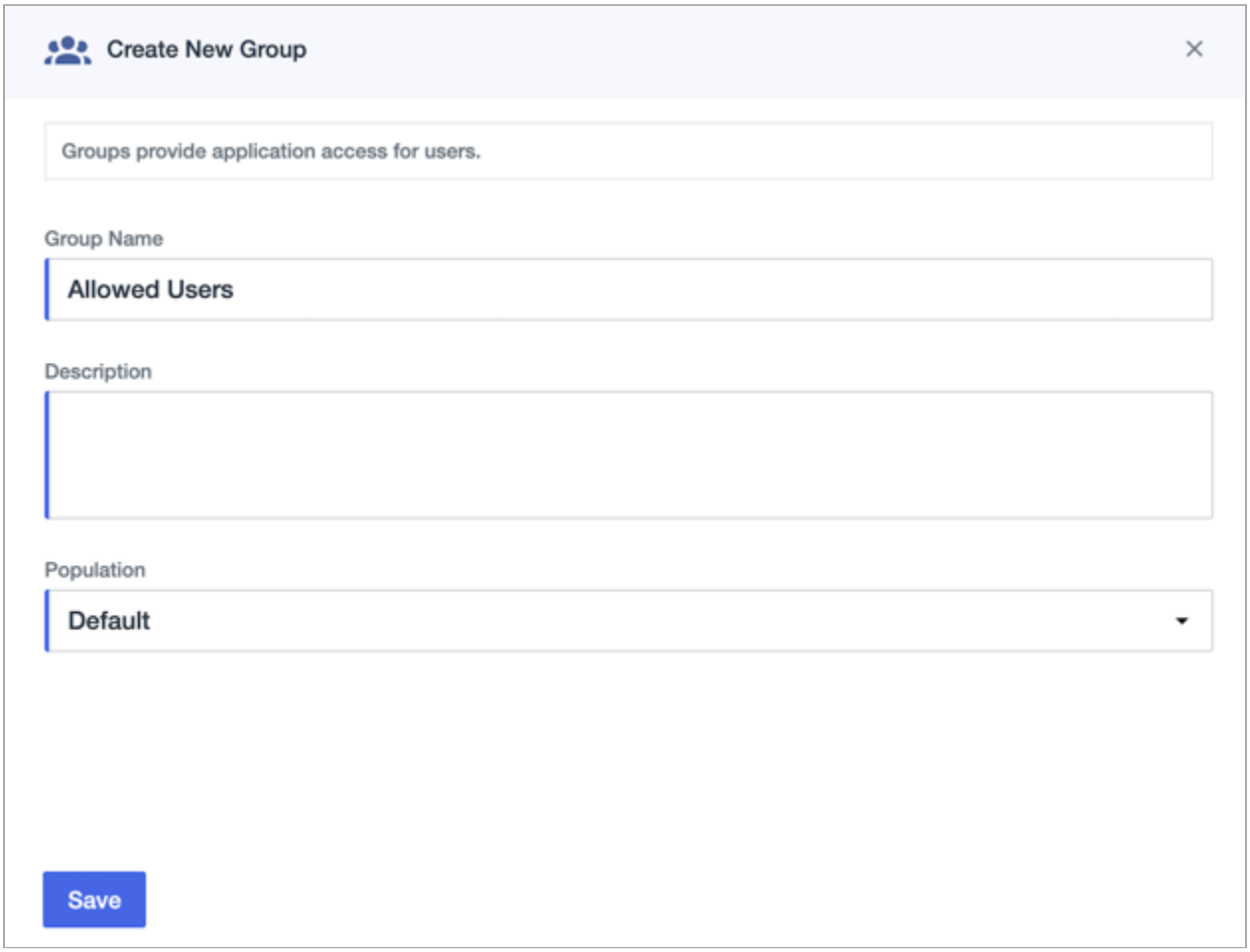
Creating a group with dynamic membership

Create a group that features dynamic membership. Use this group to limit access to the application based on group membership.

Steps

1. Go to **Directory** > **Groups**.
2. To add a new group, click **+**.
3. In the **Group Name** field, enter `Allowed Users`.
4. From the **Population** list, select **Default**.
5. Click **Save**.

Copyright © 2025 Ping Identity Corporation



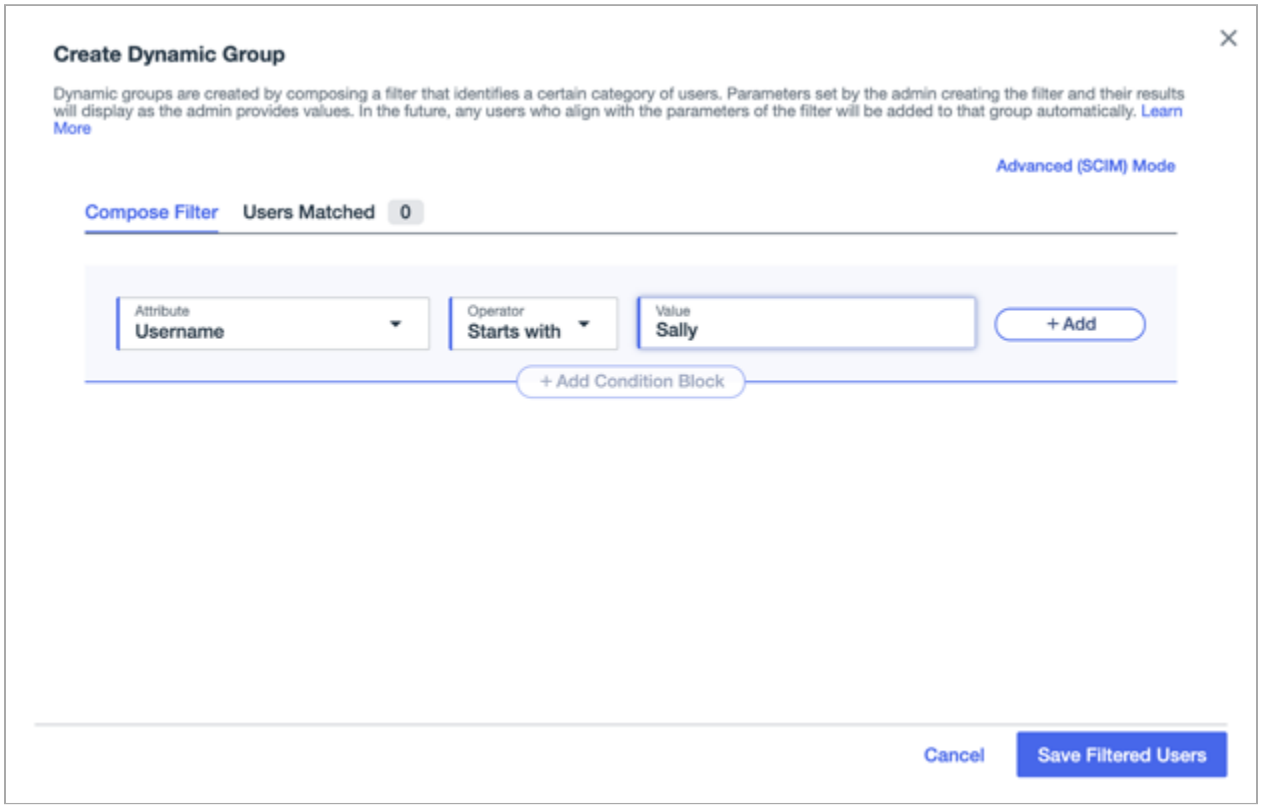
Result:

PingOne creates the user group and displays it in the **Groups** list.

6. In the configuration panel, click **Users**.
7. Click **Add Users with a Filter**.
8. In the **Create Dynamic Group** dialog, enter the following group criteria:

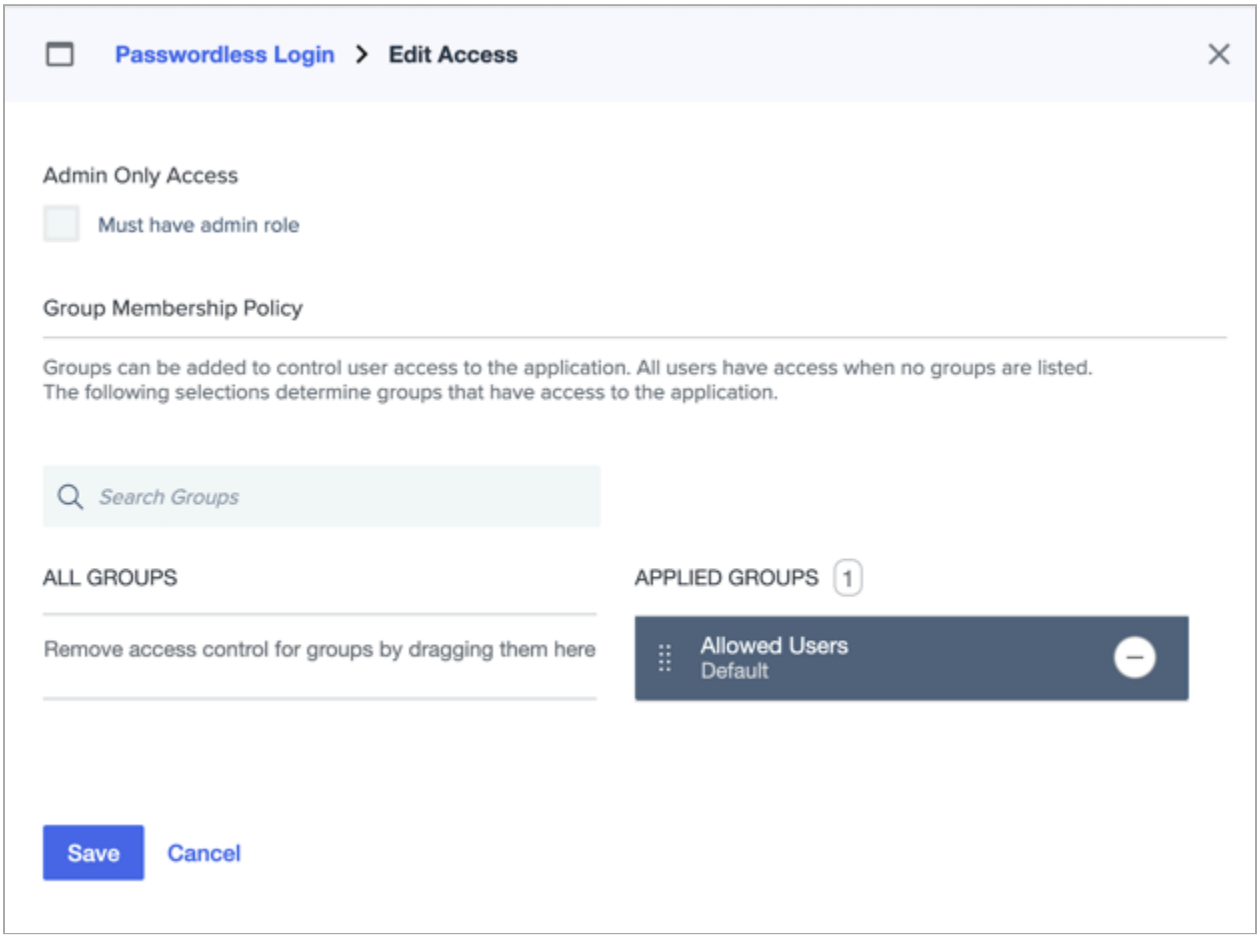
Field	Value
Attribute	**Username**
Operator	**Starts with**
Value	`Sally`

Copyright © 2025 Ping Identity Corporation



9. Click **Save Filtered Users**.
10. Go to **Applications** > **Applications**.
11. Expand the **Passwordless Login** application.
12. Click the **Access** tab and click the **Pencil** icon.
13. Click **+** or drag the **Allowed Users** group to the **Applied Groups** column.
14. Click **Save**.

Copyright © 2025 Ping Identity Corporation



Next steps

Continue by Copying the sign-on URLs.

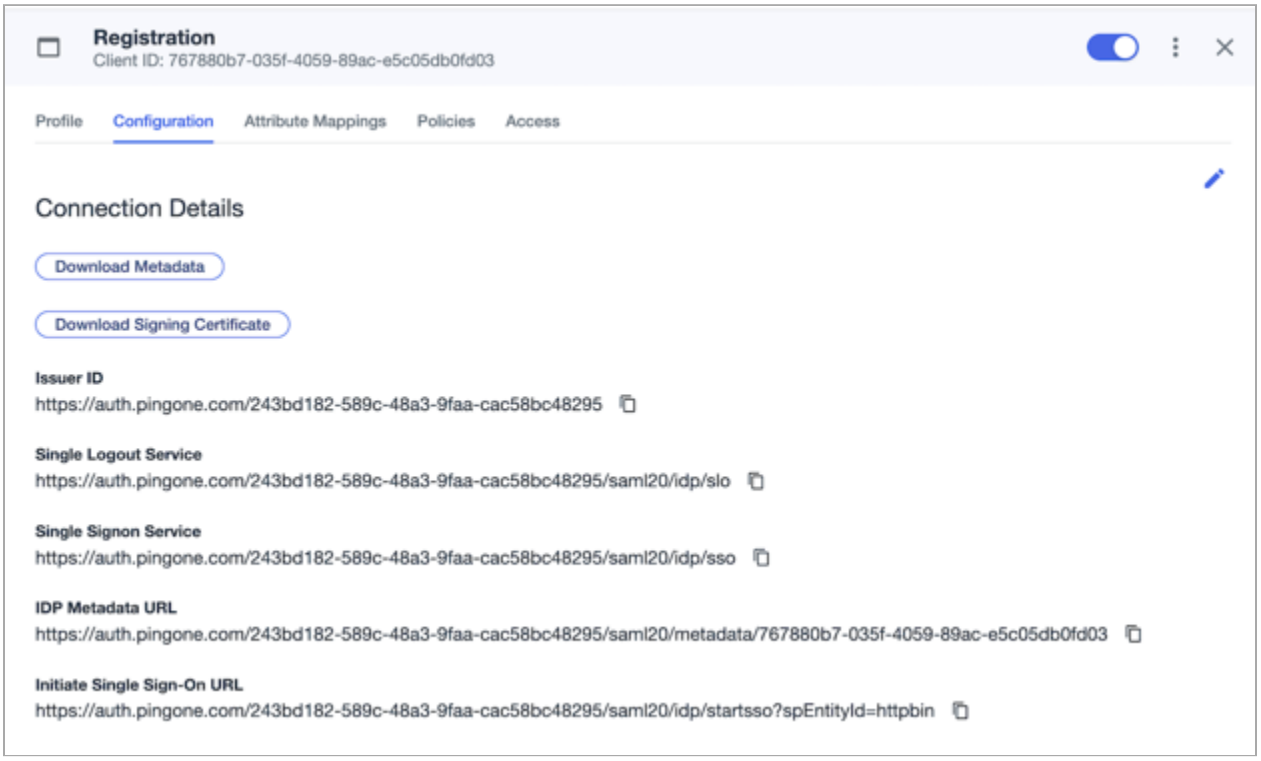
Copying the sign-on URLs

Copy the sign-on URLs into a text editor so that you can quickly complete this demo.

Steps

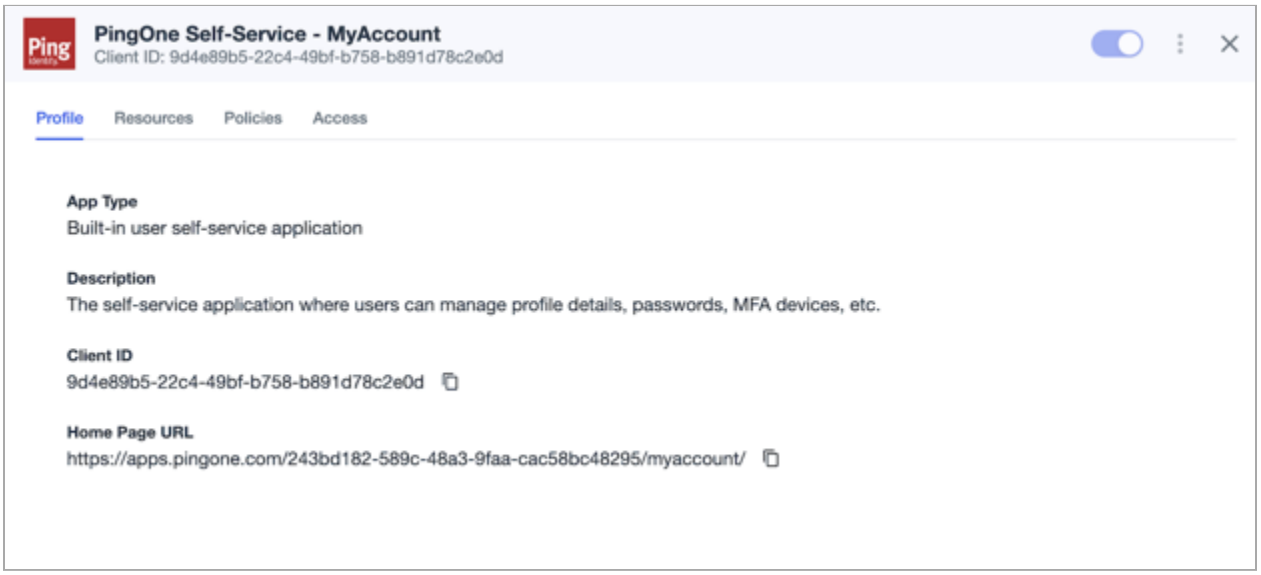
1. Go to **Applications > Applications**.
2. Expand the **Registration** application and click the **Configuration** tab.
3. Copy the **Initiate Single Sign-On URL** and paste it into a text editor.

Copyright © 2025 Ping Identity Corporation



4. Expand the **PingOne Self-Service** application.

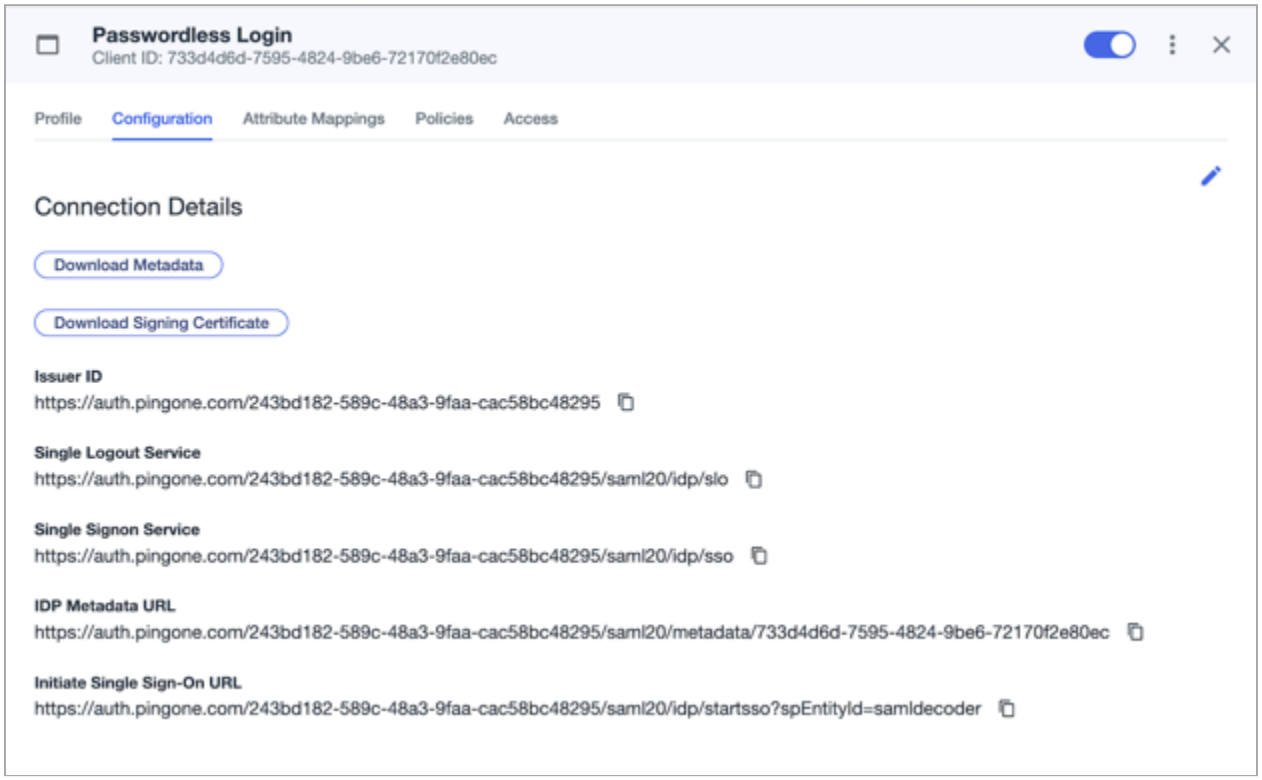
5. Copy the **Home Page URL** and paste it into a text editor.



6. Expand the **Passwordless Login** application and click the **Configuration** tab.

7. Copy the **Initiate Single Sign-On URL** and paste it into a text editor.

Copyright © 2025 Ping Identity Corporation



Next steps

Continue by Simulating a registration and successful login.

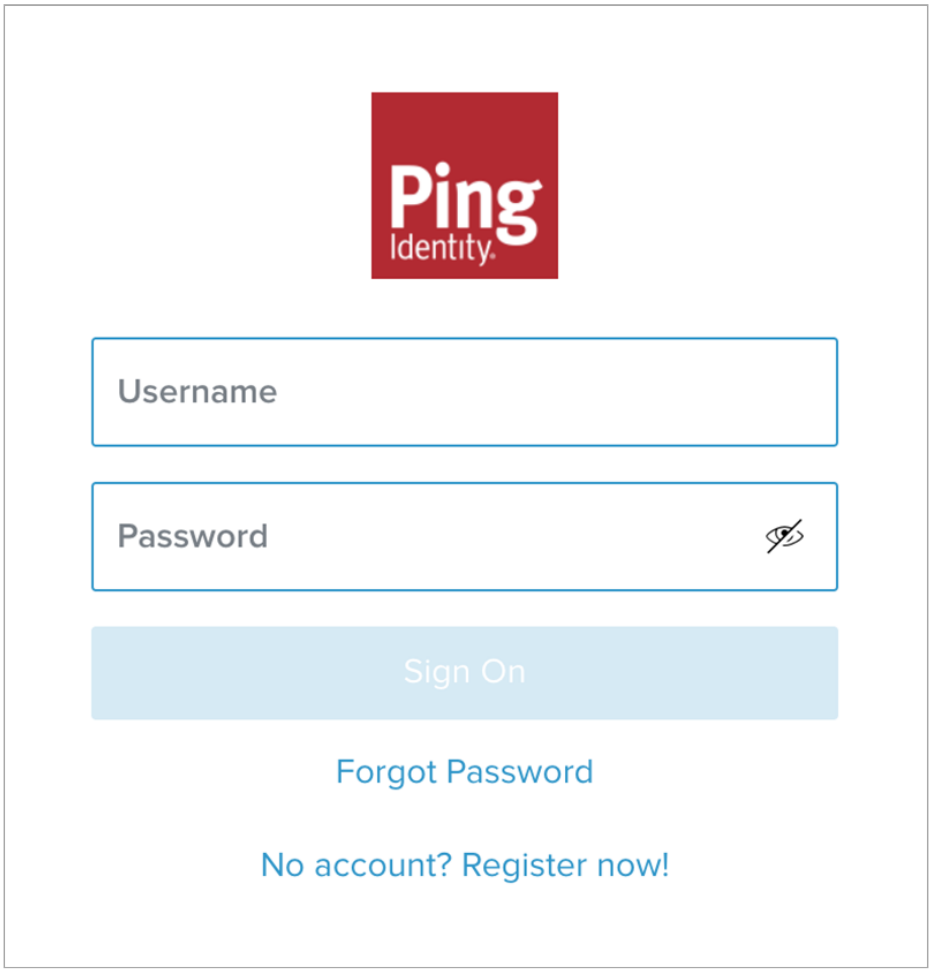
Simulating a registration and successful login

Simulate a user registration and a successful login to the application.

Steps

1. In an incognito or private browser window, go to the Initiate Single Sign-On URL for the **Registration** application.
2. Click **No account? Register now!**.

Copyright © 2025 Ping Identity Corporation



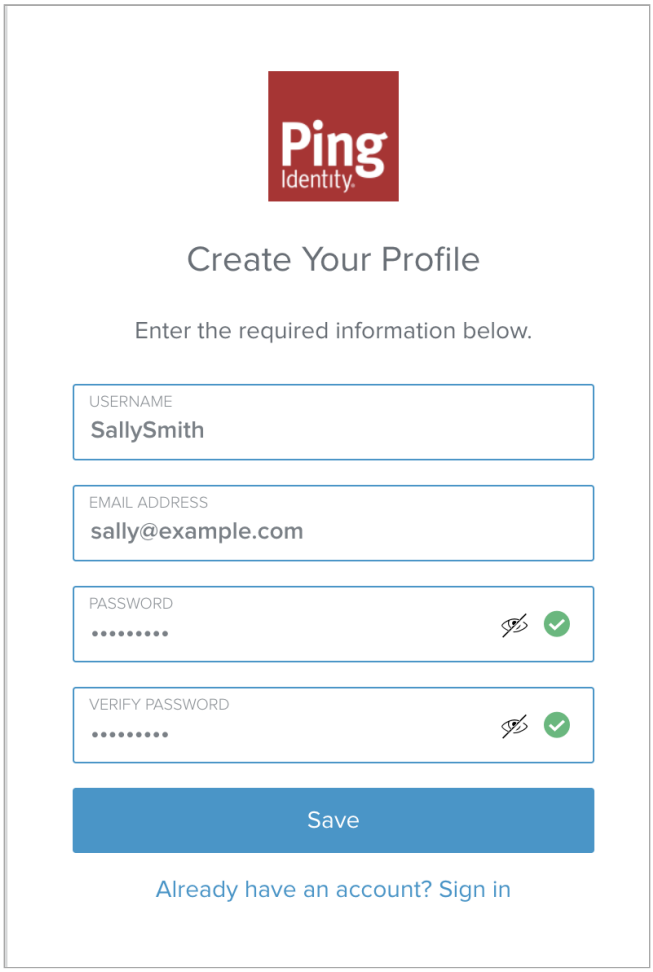
3. Register a new user 'Sally Smith'.

    1. In the **Username** field, enter `SallySmith`.

    2. In the **Email Address** field, enter a valid email address.

    3. In the **Password** and **Verify Password** fields, enter a password for this user.

Copyright © 2025 Ping Identity Corporation



4. Click **Save**.

   Result:PingOne will send a verification email to the address you entered.

5. In the **Verification Code** field, enter the verification code emailed to you.

6. Click **Verify**.

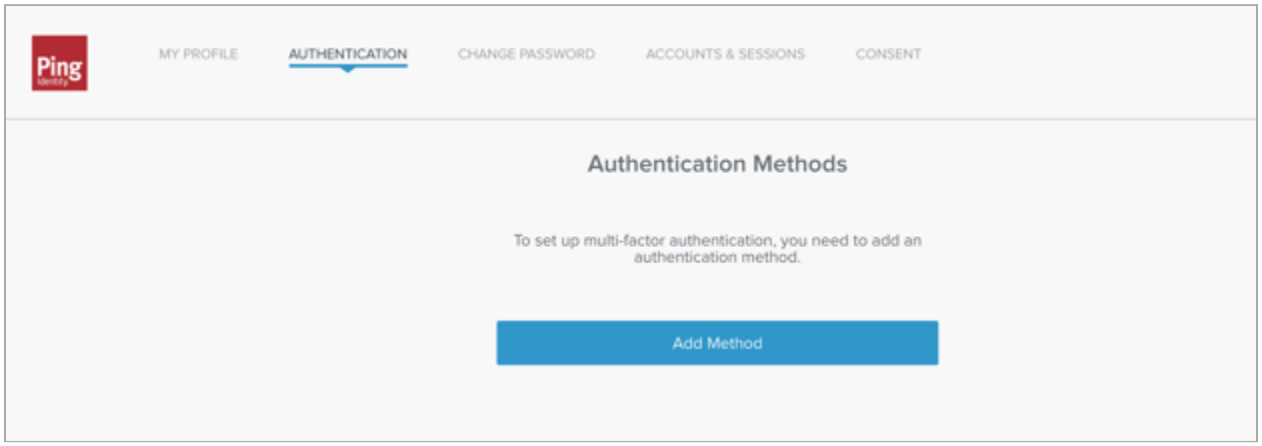
7. Close the incognito window.

4. Open a new incognito window and go to the PingOne Self-Service application Home Page URL.

5. In the **Username** and **Password** fields, enter the credentials for Sally Smith.

6. Go to **Authentication → Add Method**.

Copyright © 2025 Ping Identity Corporation



7. Click **Text message**.
8. In the **Phone Number** field, enter a phone number for PingOne to send a one-time passcode (OTP).
9. Click **Next**.

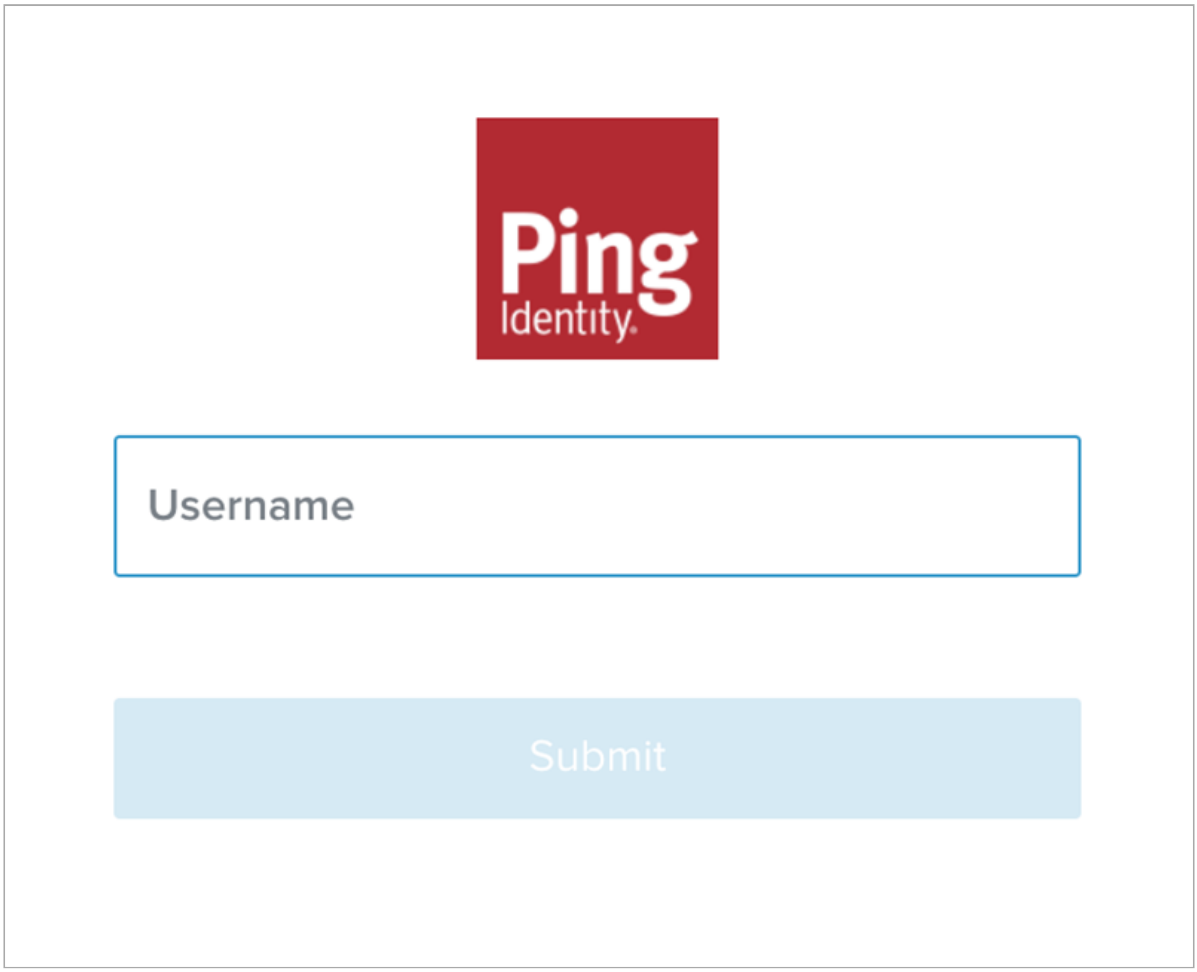
   Result:

   PingOne will send an SMS message with a verification code.
10. In the **Verification code** field, enter the verification code.
11. Click **Finish**.

    Result:

    The user is able to authenticate using SMS.
12. Open a new incognito window and go to the Passwordless Login application Initiate Single Sign-On URL.
13. In the **Username** field, enter `SallySmith`.

Copyright © 2025 Ping Identity Corporation



14. Click **Submit**.

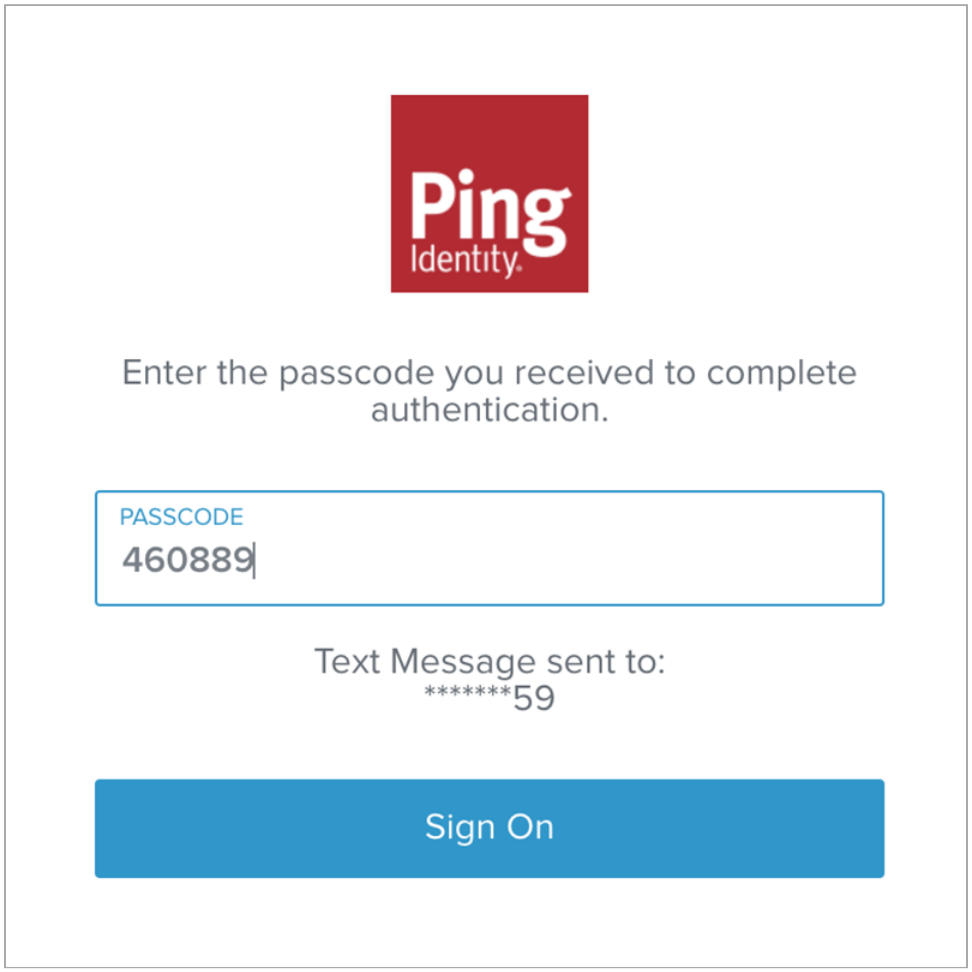
    Result:

    PingOne will send you a text message with a passcode.

15. In the **Passcode** field, enter the passcode.

16. Click **Sign On**.

Copyright © 2025 Ping Identity Corporation



Result:

You are authenticated to the PingOne **SAML Decoder** page.

Next steps

Continue by Simulating a registration and access control-based login failure.

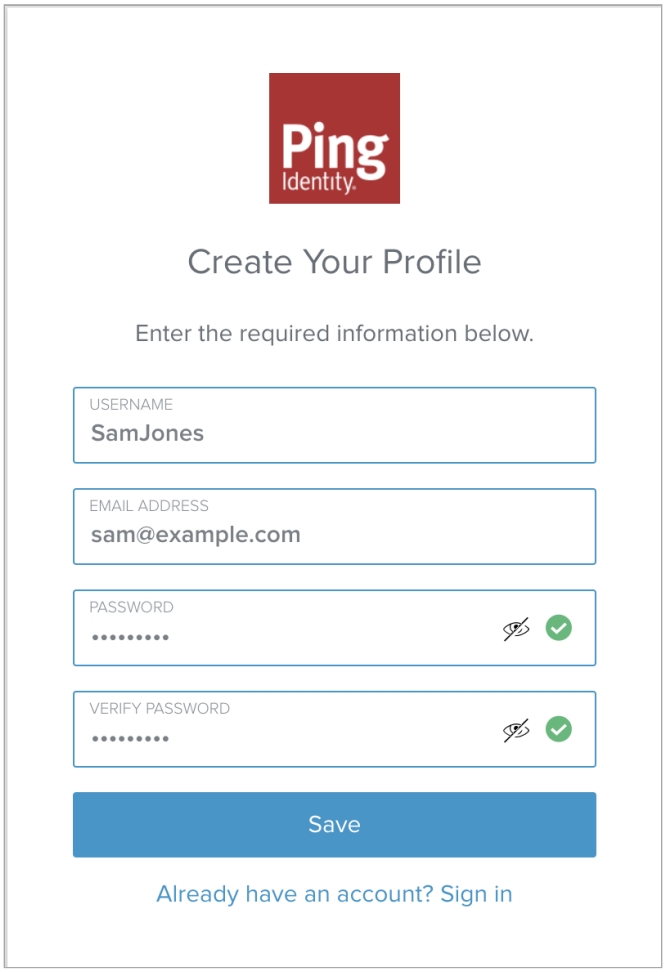
Simulating a registration and access control-based login failure

Simulate a user registration and an access control-based login failure.

Steps

1. In an incognito or private browser window, go to the Initiate Single Sign-On URL for the **Registration** application.
2. Click **No account? Register now**.
3. Register a new user 'Sam Jones'.
    1. In the **Username** field, enter `SamJones`.
    2. In the **Email Address** field, enter a valid email address.
    3. In the **Password** and **Verify Password** fields, enter a password for this user.

Copyright © 2025 Ping Identity Corporation



4. Click **Save**.

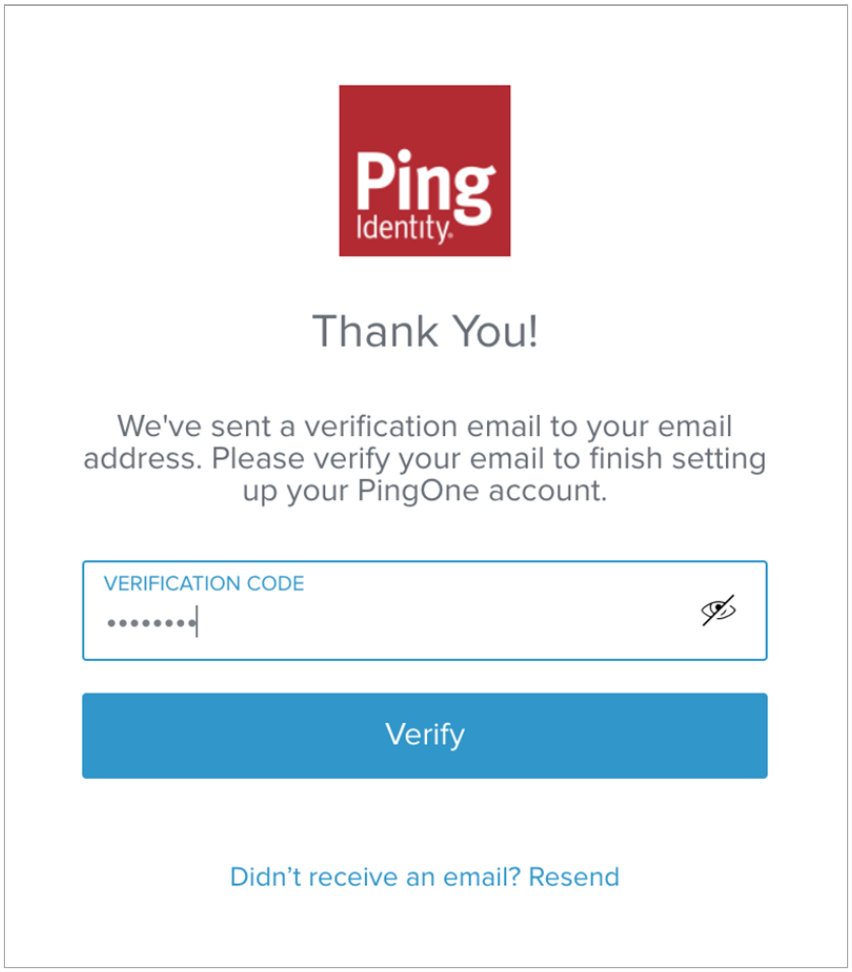
   Result:

   PingOne will send a verification email to the address you entered.

5. In the **Verification Code** field, enter the verification code emailed to you.

6. Click **Verify**.

Copyright © 2025 Ping Identity Corporation

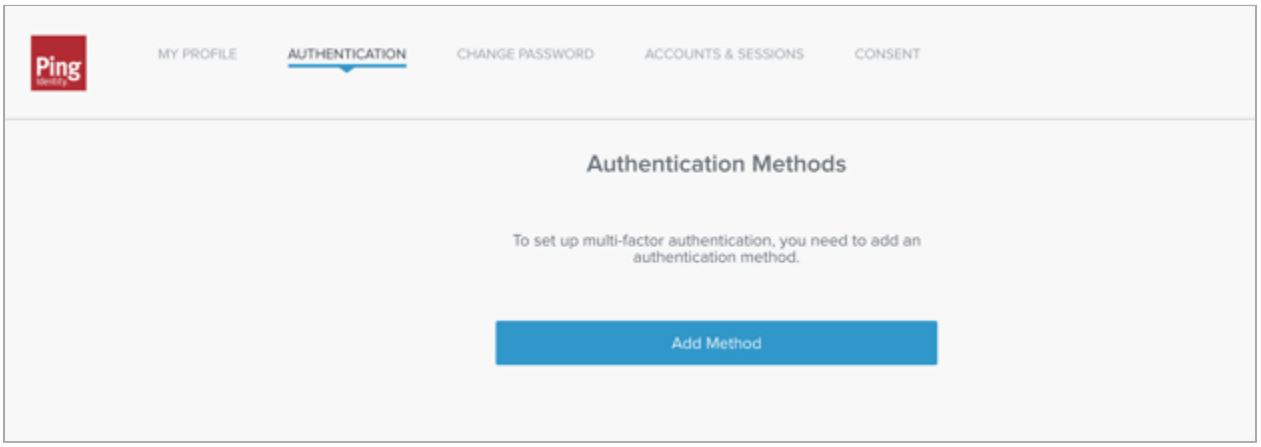


7. Close the incognito window.

4. Open a new incognito window and go to the PingOne Self-Service application Home Page URL.

5. In the **Username** and **Password** fields, enter the credentials for Sam Jones.

6. Go to **Authentication → Add Method**.



7. Click **Text message**.

8. In the **Phone Number** field, enter a phone number for PingOne to send a one-time passcode (OTP).

Copyright © 2025 Ping Identity Corporation

9. Click **Next**.

   Result:

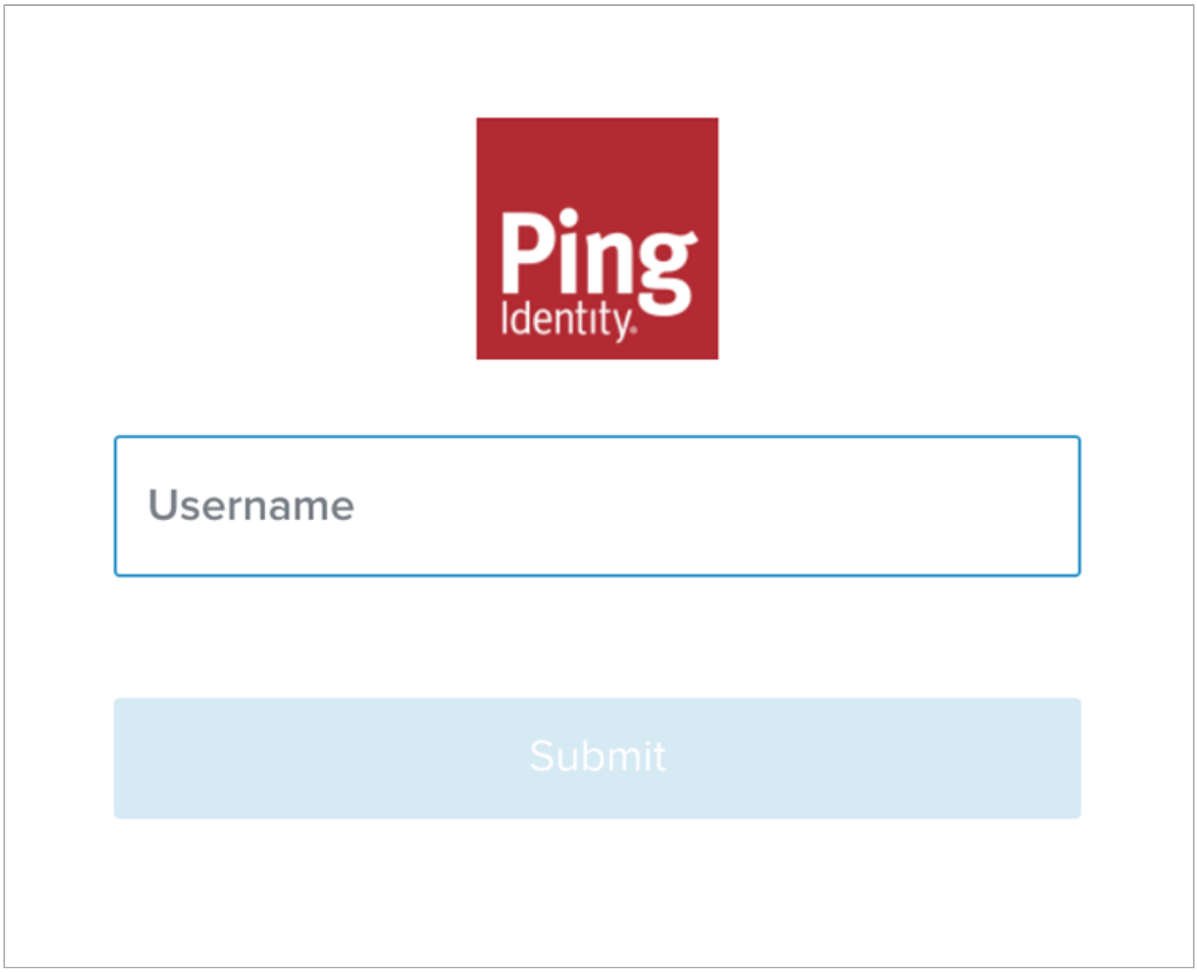
   PingOne will send an SMS message with a verification code.

10. In the **Verification code** field, enter the verification code.
11. Click **Finish**.

    Result:

    The user is able to authenticate using SMS.

12. Close the incognito window.
13. In a new incognito window, go to the Passwordless Login application Initiate Single Sign-On URL.
14. In the **Username** field, enter `SamJones`.



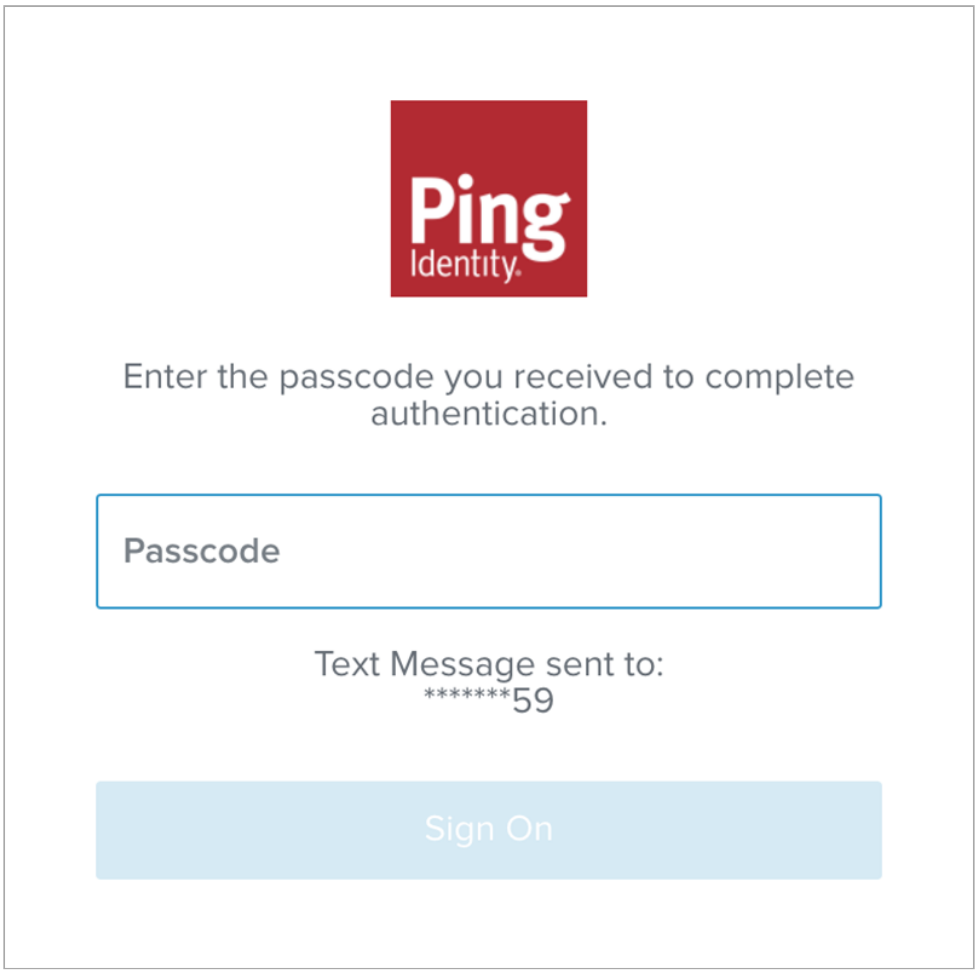
15. Click **Submit**.

    Result:

    PingOne will send you a text message with a passcode.

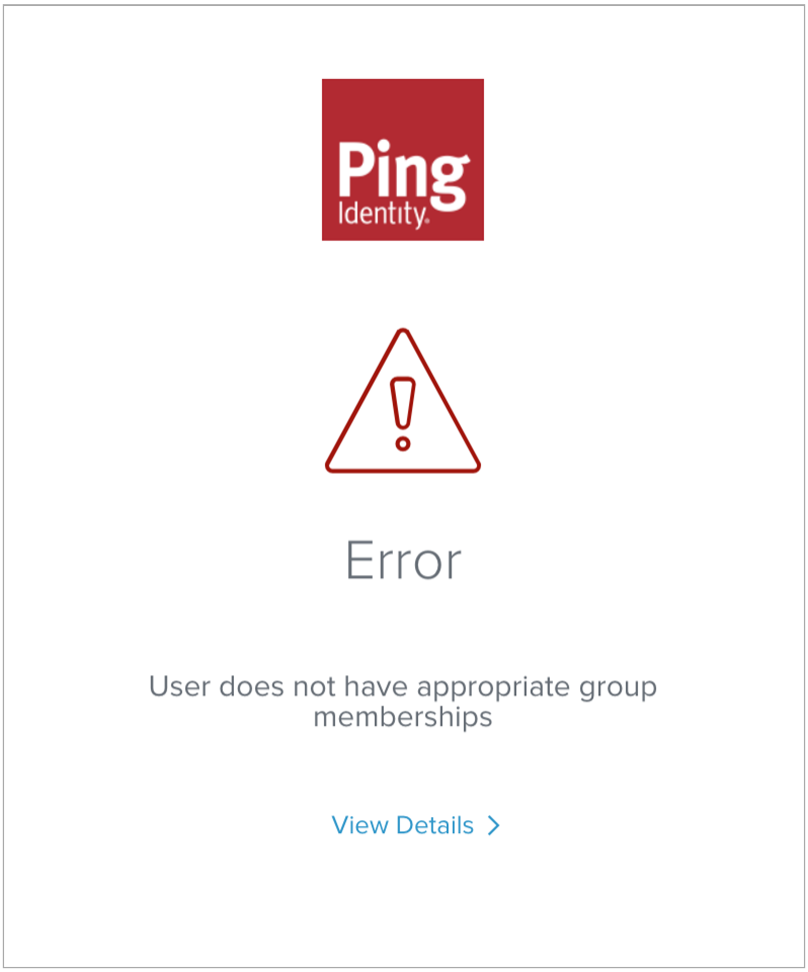
Copyright © 2025 Ping Identity Corporation

16. In the **Passcode** field, enter the passcode.



17. Click **Sign On**.

Copyright © 2025 Ping Identity Corporation



Result:

PingOne displays the following error message:

```
User does not have appropriate group memberships
```

Next steps

Congratulations! You've just configured and tested a passwordless login experience!

Accessing the application portal

Review each user's available applications by accessing the Application Portal.

Steps

1. Go to **Applications** > **Applications**.
2. Expand the **PingOne Application Portal** application.
3. Click the **Policies** tab, and click the **Pencil** icon to edit.
4. Click **+** to add **Multi_Factor** to**Applied Policies**.

Copyright © 2025 Ping Identity Corporation

5. Click **Save**.
6. Go to **Environment → Properties**.
7. Click the **Application Portal URL**.
8. Sign on with each user to review the applications that are available to them.

Copyright © 2025 Ping Identity Corporation

PingOne Use Cases

Learn how to configure PingOne with other Ping products and selected third-party products to enable you to better run your security business.

Configuring PingOne as an external IdP in ZIdentity

You can configure PingOne as an external identity provider (IdP) to enable single sign-on (SSO) to ZIdentity using the OpenID Connect (OIDC) authentication protocol.

Learn more in Configuring PingOne as an External IdP in the ZIdentity documentation.

Securing your APIs using PingOne and Amazon Verified Permissions

Reduce the time your developers spend securing APIs using permissions based on role-based access control (RBAC) by using PingOne as your identity provider (IdP) and Amazon Verified Permissions (AVP) as your permissions manager.

PingOne is a cloud-based identity as a service (IDaaS) framework for secure identity access management that uses an organization-based model to define tenant accounts and their related entities within the PingOne platform.

AVP is a fine-grained authorization service that accelerates application development by decoupling authorization logic from business logic. It uses the Cedar policy language to write authorization policies and allows developers to build applications faster by externalizing authorization and centralizing policy management.

This use case walks through how configuring AVP to secure access to application APIs hosted on the Amazon API Gateway for identities managed in PingOne. AVP will automatically create the Cedar policies that determine which APIs a user is permitted to call based on their PingOne group membership. When the user authenticates with PingOne, their group membership is included in the OIDC token that PingOne generates. AVP then compares the user's group memberships in the OIDC token to the Cedar policies and either allows or denies access to the API accordingly.

Goals

After completing this use case, you'll know how to configure AVP to secure access to your API for identities managed in PingOne.

What you'll do

In PingOne, you'll:

1. Create an OpenID Connect (OIDC) web application.
2. Create two example users.
3. Create two example groups.

In Amazon Web Services (AWS), you'll:

1. Create an example REST API and deploy the API to the Amazon API Gateway.
2. Configure AVP to secure access to your API for identities managed in PingOne.

Copyright © 2025 Ping Identity Corporation

Before you begin

In PingOne, each organization contains one or more tenants, known as environments, which define separate working domains within an organization.

To set up this use case, you'll need:

- A PingOne organization. Learn more in Starting a PingOne trial.
- A PingOne environment that includes the PingOne SSO service.
- An AWS account with access to the API Gateway and AVP services.

Tasks

Creating and configuring an OIDC application in PingOne

Create and configure an OIDC web application to manage using PingOne SSO.

1. In the PingOne admin console, go to **Applications** > **Applications** and click the **+** icon.
2. In the **Application Name** field, enter a unique identifier for the application.

   For example, `AVP app`.
3. (Optional) In the **Description** field, enter a brief description of the application.

   For example, `Use this application to verify sign on using Amazon Verified Permissions`.
4. (Optional) Click **Icon** to upload an image to represent the application.

   > **Note**
   > Use a file up to 1MB in JPG, JPEG, GIF, or PNG format.
5. For **Application Type**, click **OIDC Web App**.
6. Click **Save**.

   The details panel for the application opens.
7. On the **Overview** tab, copy the following values and save them to a secure location. You'll need these values when you configure AVP:

   1. In the **General** section, copy the values for **Client ID** and **Client Secret**.
   2. In the **Connection Details section**, copy the **Issuer ID**.
8. On the **Configuration** tab, click the **Pencil** icon.
9. In the **OIDC Settings** section, in the **Redirect URIs** field, enter the address to which PingOne will forward the OIDC response after verification.

Copyright © 2025 Ping Identity Corporation

For example, `https://oauth.pstmn.io/v1/browser-callback`.

10. Click **Save**.

11. On the **Attribute Mappings** tab, click the **Pencil** icon

12. Click **+ Add** and add a new custom attribute as follows:

    1. In the **Attributes** column, enter `group`.

    2. In the **PingOne Mappings** column, select **Group Names**.

13. Click **Save**.

14. (Optional) On the **Policies** tab, click the **Pencil** icon, select the authentication policies for the application, and click **Save**.

    Learn more in Authentication policies for applications and Applying authentication policies to an application.

15. (Optional) On the **Access** tab, click the **Pencil** icon, configure the access settings for your application, and click **Save**.

    Learn more in Application access control.

    > **Note**
    >
    > If you selected **Response Type = Code** and **Grant Type = Authorization Code**, there's also an **Integrate** tab that you can use to test your configuration. Learn more in Integrate PingOne with a Node.js Express app and Integrate Ping SDK for JavaScript with PingOne.

16. On the **Applications** page, browse or search for the application you just created and click the toggle to enable it.

    > **Note**
    >
    > The application can't be used until it is enabled.

Creating example users and groups in PingOne

Create two example users and groups to use for testing the AVP policies. As configured, user Alice will have full permissions to the example API, whereas user Bob will have restricted permissions.

1. In the PingOne admin console, go to **Directory** > **Users** and click the **+** icon.

2. For the first user, enter the following information:

    1. In the **Username** field, enter `alice`.

    2. In the **Population** list, select the population to which you want to add the user.

    > **Note**
    >
    > All users must belong to a population. If you don't have a population configured in your environment, you must create one. Learn more in Managing populations.

Copyright © 2025 Ping Identity Corporation

   3. In the **Password** field, enter a password for the user.
   4. Click **Save**.
3. For the second user, enter the following information:
   1. In the **Username** field, enter `bob`.
   2. In the **Population** list, select the population to which you want to add the user.
   3. In the **Password** field, enter a password for the user.
   4. Click **Save**.
4. Go to **Directory** > **Groups** and click the **+** icon.
5. For the first group, enter the following information:
   1. In the **Group Name** field, enter `AVP_Admin`.
   2. Click **Save**.
   3. On the **Groups** page, locate the **AVP_Admin** group and click it to open the details panel.
   4. On the **Users** tab, click **Add Individually**.
   5. In the **All Users** list, select the checkbox next to **alice** and click **Save**.
6. For the second group, enter the following information:
   1. In the **Group Name** field, enter `AVP_User`.
   2. Click **Save**.
   3. On the **Groups** page, locate the **AVP_User** group and click it to open the details panel.
   4. On the **Users** tab, click **Add Individually**.
   5. In the **All Users** list, select the checkbox next to **bob** and click **Save**.

Creating an example API in AWS

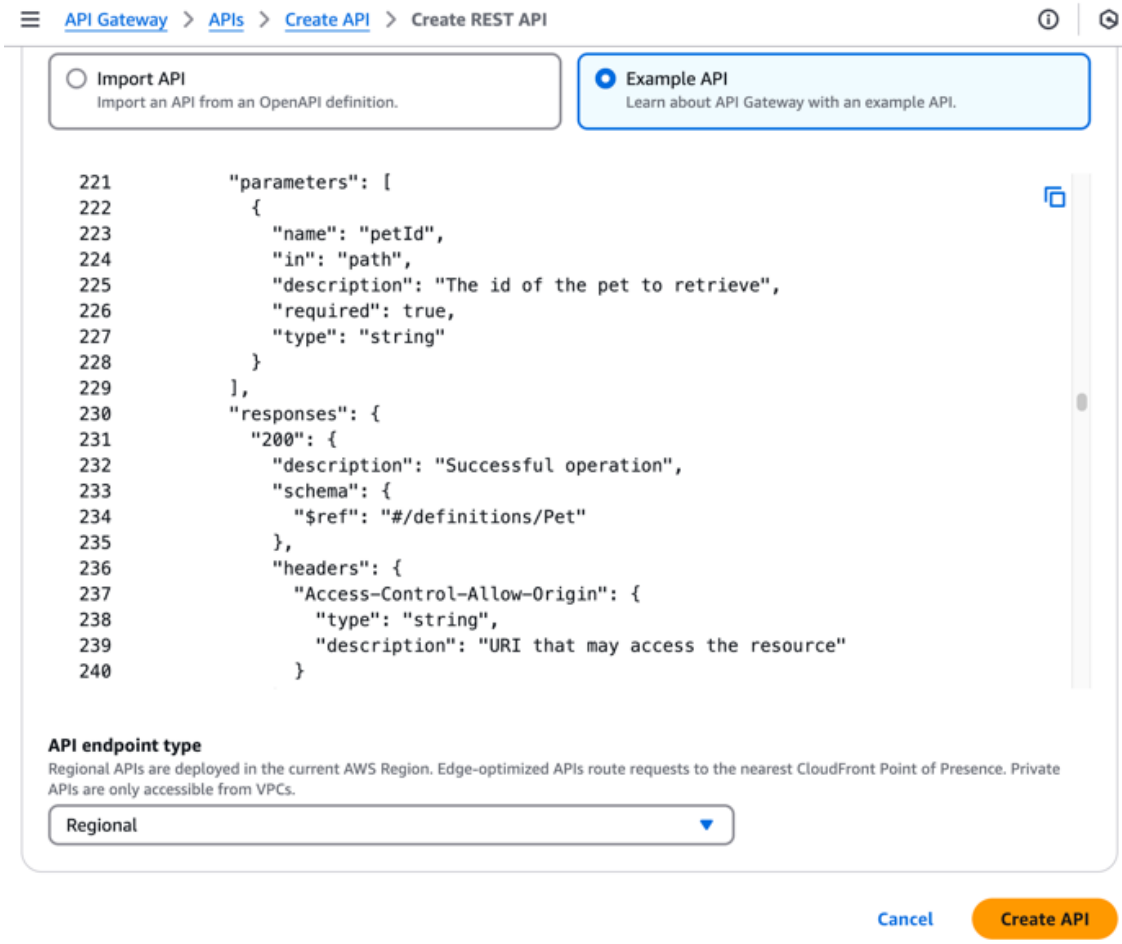
Now you'll create an example API to secure with AVP.

1. Sign on to the AWS Management Console.
2. Go to **API Gateway**.

   > **Note**
   > If **API Gateway** is not listed in your console, use the search bar to find it. Learn more about API Gateway in the Amazon API Gateway Developer Guide.

3. Click **Create API**.
4. Scroll to **REST API** and click **Build**.
5. Select **Example API**, and then click **Create API**.

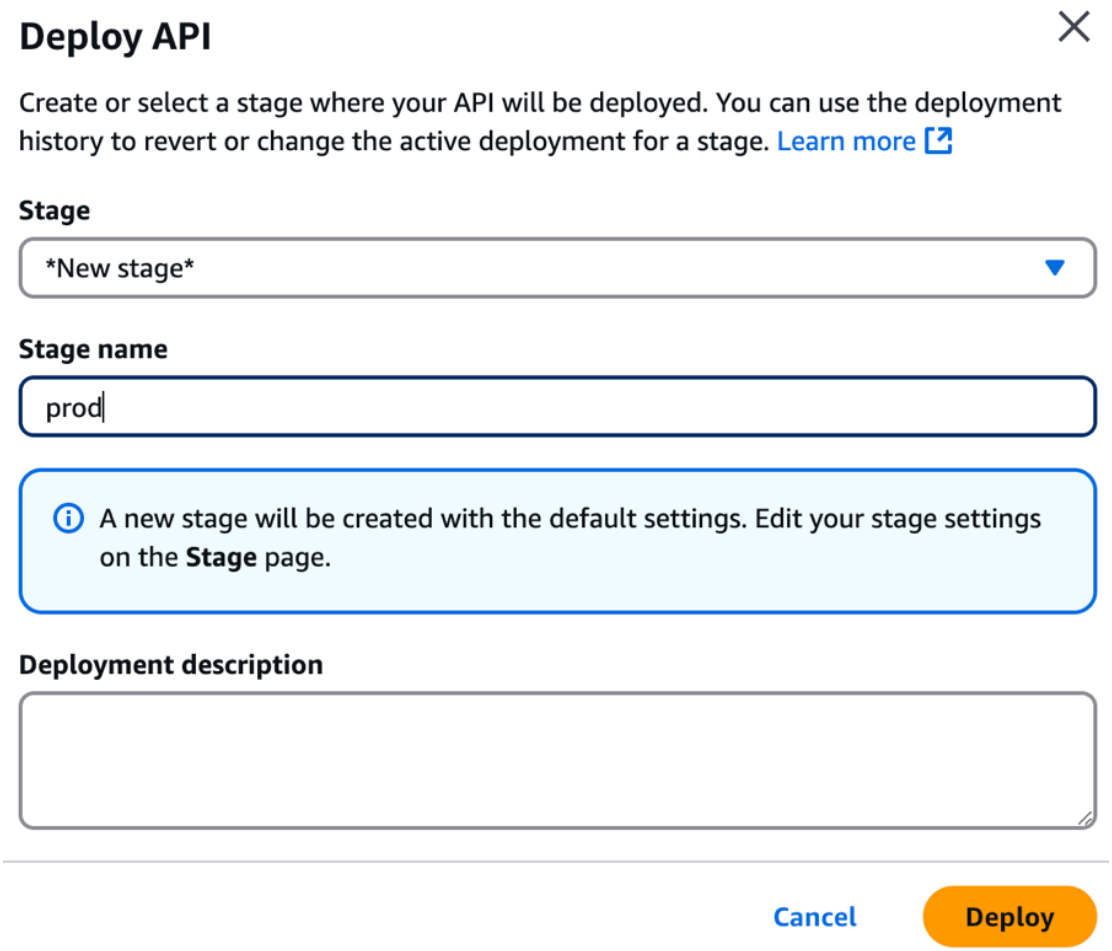
Copyright © 2025 Ping Identity Corporation



Result

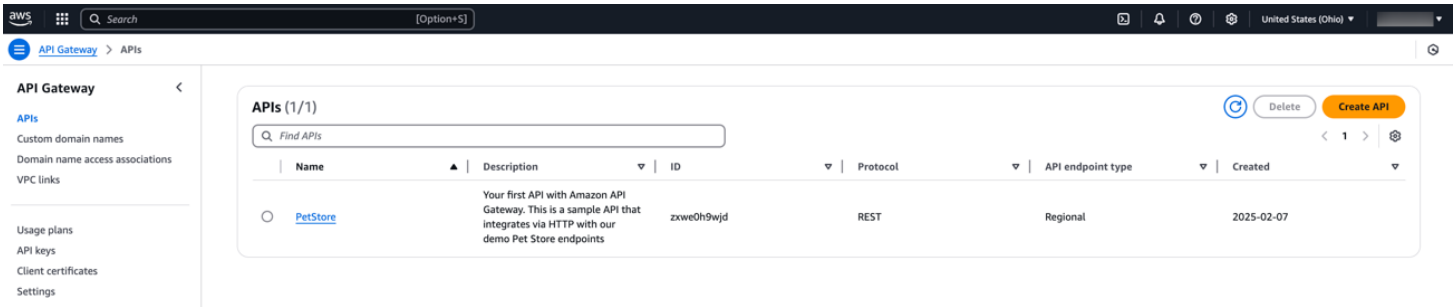
A message displays that states the API creation was successful.

6. Click **Deploy API**.
7. On the **Deploy API** modal, from **Stage**, select ***New Stage***.
8. In the **Stage name** field, enter `prod`.
9. Click **Deploy**.



Next Steps

View details about your API in the AWS Management Console by going to **API Gateway > APIs**.



Creating an Amazon Verified Permissions policy store

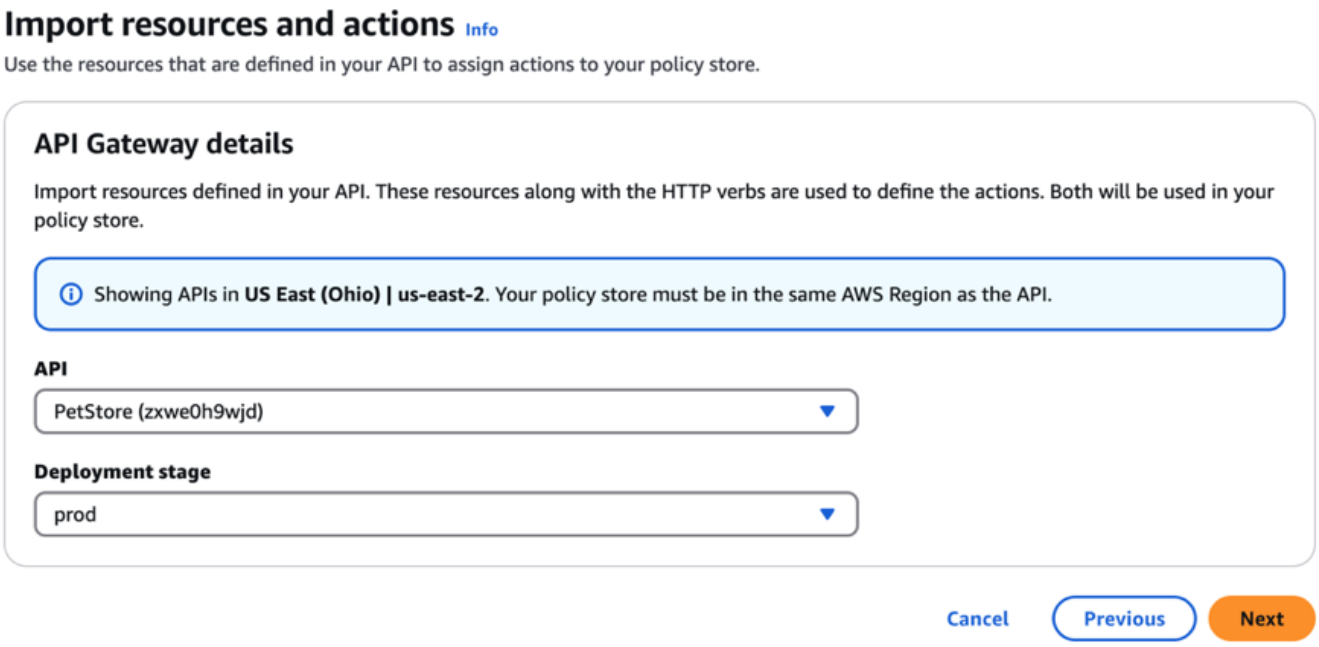
Next you'll create an AVP policy store and configure it to protect your API.

1. In the AWS Management Console, go to **Amazon Verified Permissions > Policy stores**.

> **Note**
>
> If **Amazon Verified Permissions** isn't listed in your console, use the search bar to find it. Learn more in the Amazon Verified Permissions User Guide.

Copyright © 2025 Ping Identity Corporation

2. Click **Create new policy store**.
3. In the **Starting options** section, select **Set up with API Gateway and an identity provider**.
4. Click **Next**.
5. On the **Import resources and actions** page, in the **API Gateway details** section, for **API**, select the API you created previously.
6. For **Deployment stage**, select **prod**.

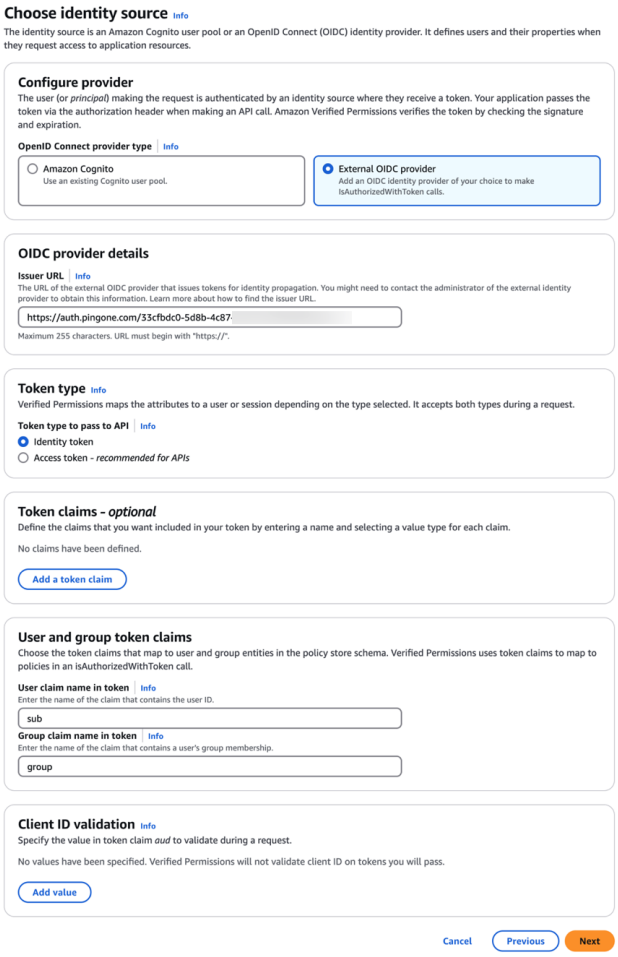


7. Click **Next**.
8. On the **Choose identity source** page, in the **Configure provider** section, select **External OIDC provider**.
9. In **OIDC provider details**, enter the **Issuer ID** URL you copied from the **Overview** tab when you created your OIDC application in PingOne.
10. For **Token type**, select **Identity token**.

> **Note**
>
> **Access token** will also work, but PingOne only includes the `group` claim in identity tokens, not in access tokens. When making API calls, use the **Identity token** type to ensure the AVP policies are applied correctly.

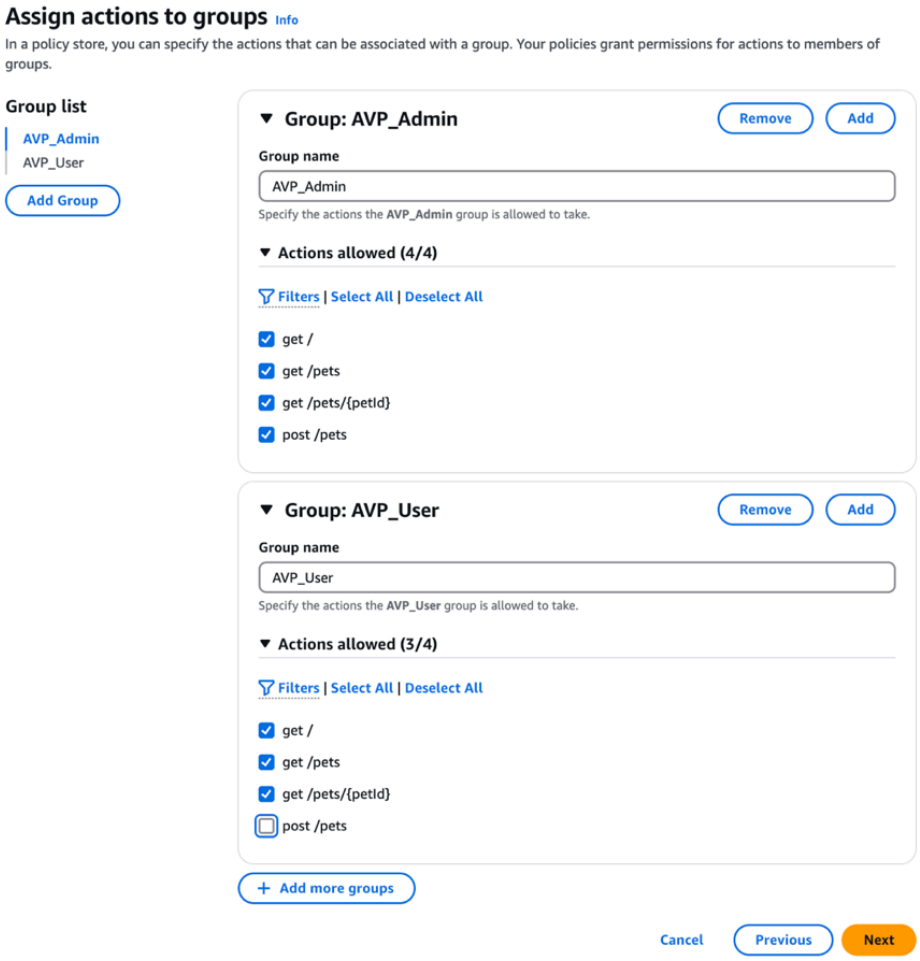
11. In **User and group token claims**, ensure that the values in **User claim name in token** and **Group claim name in token** match what you configured on the **Attribute Mappings** tab when you created your OIDC application in PingOne.

Copyright © 2025 Ping Identity Corporation



12. Click **Next**.
13. In **Assign actions to groups**, in the **Group name** field, enter `AVP_Admin`.
14. In **Actions allowed**, click **Select All** to give users in this group full permissions to the API.
15. Click **+ Add more groups**.
16. In the **Group Name** field, enter `AVP_User`.
17. In **Actions allowed**, clear the checkbox next to **post/pets** to give users in this group restricted permissions to the API.

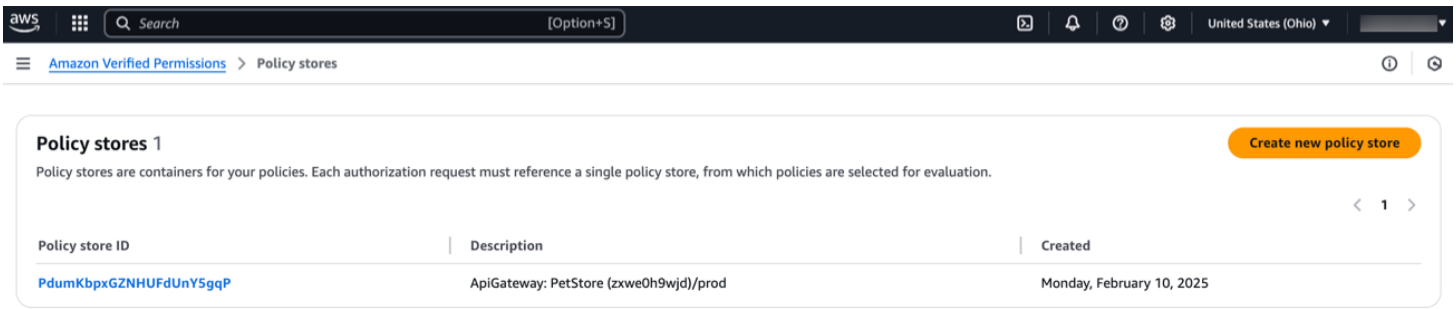
Copyright © 2025 Ping Identity Corporation



18. Click **Next**.
19. On **Deploy app integration**, for **Start authorizing for API**, select **Now, automatically**.
20. Click **Create policy store**.

Result

A message displays indicating that you successfully created the policy store. View details about your policy store in the AWS Management Console by going to **Amazon Verified Permissions > Policy Stores**.



Setting up PingOne SSO and PingID as the external MFA provider for Microsoft Entra ID

Microsoft Entra ID allows customers to use an external authentication provider for multi-factor authentication (MFA) through external authentication methods (EAMs). In this use case, you'll learn how to set up Entra ID, PingOne SSO, and PingID to support an EAM in Entra ID.

Set up an EAM in Entra ID if:

- Entra ID is the identity provider (IdP).
- The users reside in a managed domain in Entra ID.

  Learn more in Create and configure a managed domain in the Entra ID documentation.
- PingOne is the external authentication provider.

> **Note**
>
> If you added a Microsoft 365 application to PingOne using the application catalog and completed the PowerShell cmdlets to set up PingOne as the federated IdP for the domain in Entra ID, an EAM isn't required for MFA. Instead, you can add an MFA claim in the Microsoft 365 application to communicate to Entra ID that PingOne will handle MFA. Learn more in Using WS-Fed or SAML 1.1 federated IdP in the Entra ID documentation.

The high-level process of signing on with an EAM works as follows, with PingOne and PingID acting as the external authentication provider:

1. A user opens an application protected by Entra ID and is prompted to complete first-factor MFA in Entra ID.
2. Entra ID determines that another factor needs to be satisfied, such as if a conditional access policy requires MFA.
3. The user chooses the applicable EAM as second-factor MFA.
4. Entra ID sends an OpenID Connect (OIDC) authentication request to PingOne (the external authentication provider in this use case).
5. PingOne initiates MFA for the user.
6. The user completes the MFA requirement using the PingID app.
7. PingOne returns an ID token to Entra ID in the authentication response.
8. Entra ID validates the ID token and signs the users on to the application.

Learn more about EAMs in the Microsoft Entra MFA external method provider reference in the Entra ID documentation.

Goals

After completing this use case, you'll know how to:

- Configure Microsoft Entra ID to support an EAM for MFA.
- Add Entra ID as an external IdP in PingOne.

Copyright © 2025 Ping Identity Corporation

- Set up PingID as the MFA solution for Entra ID users.

What you'll do

In Microsoft Entra ID, you'll configure three components:

1. Add and configure an application.
2. Create an EAM.
3. Add a conditional access policy.

In PingOne, you'll configure the following:

1. Create a population for Entra ID users.
2. Create a Microsoft IdP connection.

Overview

The high-level process of signing on with an EAM works as follows, with PingOne and PingID acting as the external authentication provider:

1. A user opens an application protected by Entra ID and is prompted to complete first-factor MFA in Entra ID.
2. Entra ID determines that another factor needs to be satisfied, such as if a conditional access policy requires MFA.
3. The user chooses the applicable EAM as second-factor MFA.
4. Entra ID sends an OIDC authentication request to PingOne (the external authentication provider in this use case).
5. PingOne initiates MFA for the user.
6. The user completes the MFA requirement using the PingID app.
7. PingOne returns an ID token to Entra ID in the authentication response.
8. Entra ID validates the ID token and signs the users on to the application.

Learn more about EAMs in the Microsoft Entra MFA external method provider reference in the Entra ID documentation.

Goals

After completing this use case, you'll know how to:

- Configure Microsoft Entra ID to support an EAM for MFA.
- Add Entra ID as an external IdP in PingOne.
- Set up PingID as the MFA solution for Entra ID users.

Copyright © 2025 Ping Identity Corporation

What you'll do

In Microsoft Entra ID, you'll configure three components:

1. Add and configure an application.
2. Create an EAM.
3. Add a conditional access policy.

In PingOne, you'll configure the following:

1. Create a population for Entra ID users.
2. Create a Microsoft IdP connection.
3. Add an authentication policy and OIDC application to handle external authentication requests from Entra ID.
4. Add a second authentication policy to redirect users to Entra ID for OIDC authentication.

The last step is configuring PingID as the EAM for Entra ID.

Before you begin

PingOne is a cloud-based identity as a service (IDaaS) framework for secure identity access management that uses an organization-based model to define tenant accounts and their related entities within the PingOne platform. Each organization contains one or more tenants, known as environments, which define separate working domains within an organization.

To set up this use case, you'll need:

- A PingOne organization. Learn more in Starting a PingOne trial.
- A PingOne environment with the PingOne SSO and PingID services added.

  Create a new environment as follows, depending on whether you're already using PingID:

  - If you aren't using PingID already or if you want to create a new PingID account, create a new PingID environment in PingOne.
  - If you're using PingID currently and want to use your existing PingID account, integrate a PingID account with a new PingOne account. You should also follow these steps if you've previously integrated PingID with Microsoft Entra ID using custom controls. Learn more about integrating PingID with Entra ID in the PingID documentation.
- A Microsoft Entra account with an active subscription and an Entra tenant.

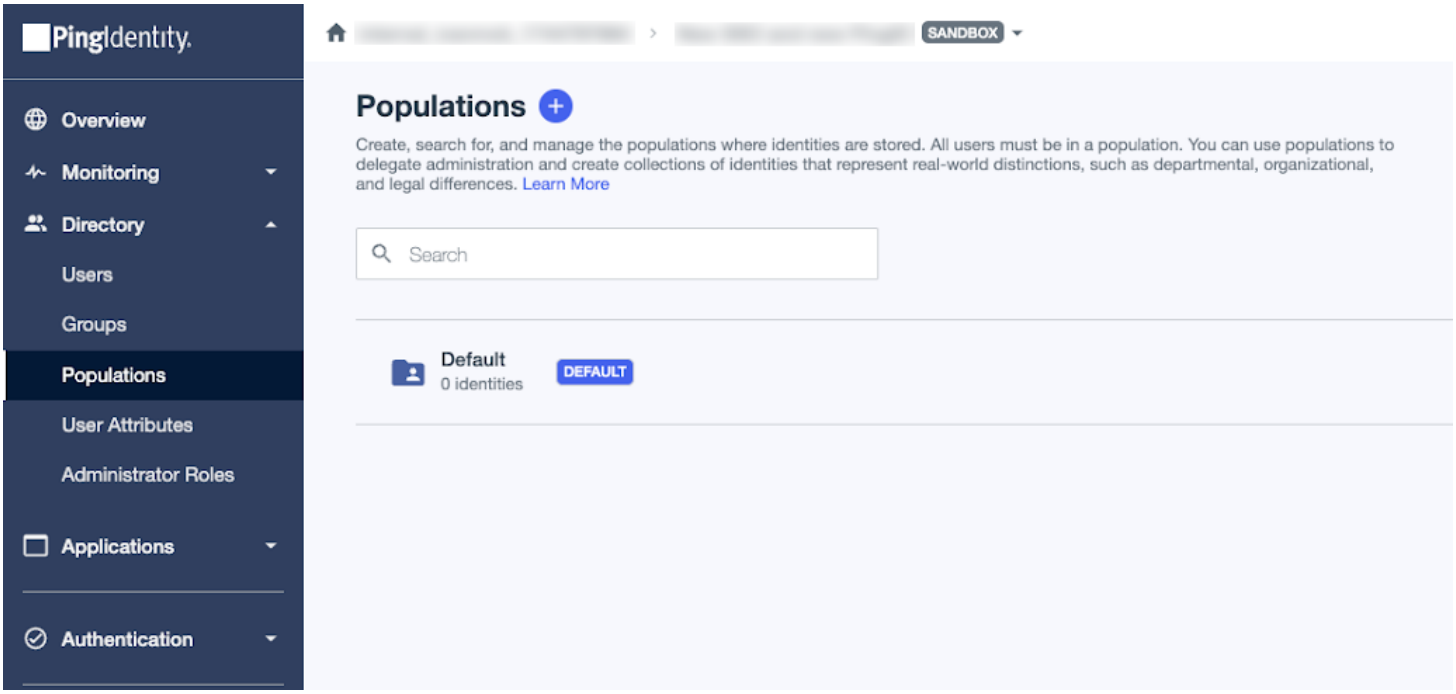
Tasks

New PingID accounts: Creating a population for Microsoft Entra ID users

If you created a new PingID environment in PingOne, your new environment includes a population named **Default**. Learn more in Creating a new PingOne environment with MFA.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If you integrated an existing PingID account with a new PingOne account, skip to Existing PingID accounts: Creating a population for Microsoft Entra ID users and changing the default population.

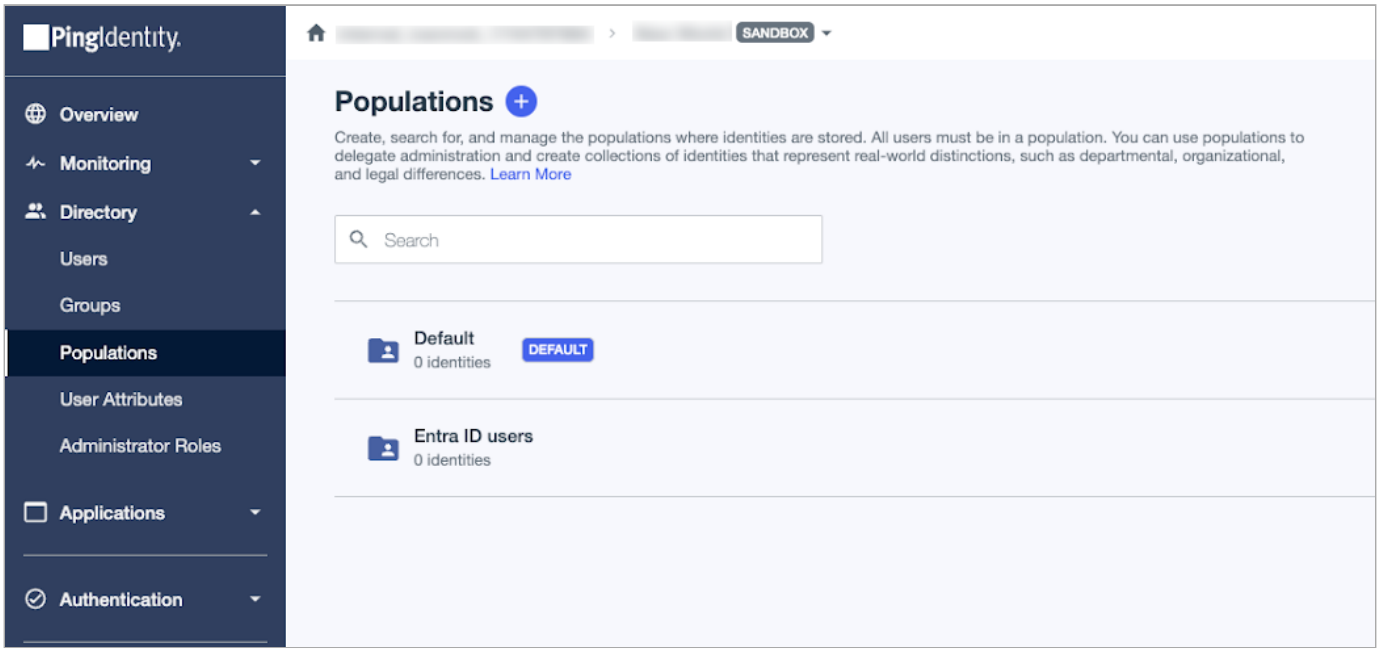


When you configure an EAM for Microsoft Entra, you'll need to create a new population in PingOne for users coming from Entra ID.

Steps

1. In the PingOne admin console, go to **Directory** > **Populations**.
2. Click the **+** icon to add a new population.
3. Enter the following:
    1. **Population Name**: A unique label for the population, such as `Entra ID users`.
    2. **Description** (optional): A brief description of the population.
    3. **Default Population** (optional): Don't select this checkbox in this scenario unless you want to specify this population as the new default population.
4. Click **Save**.

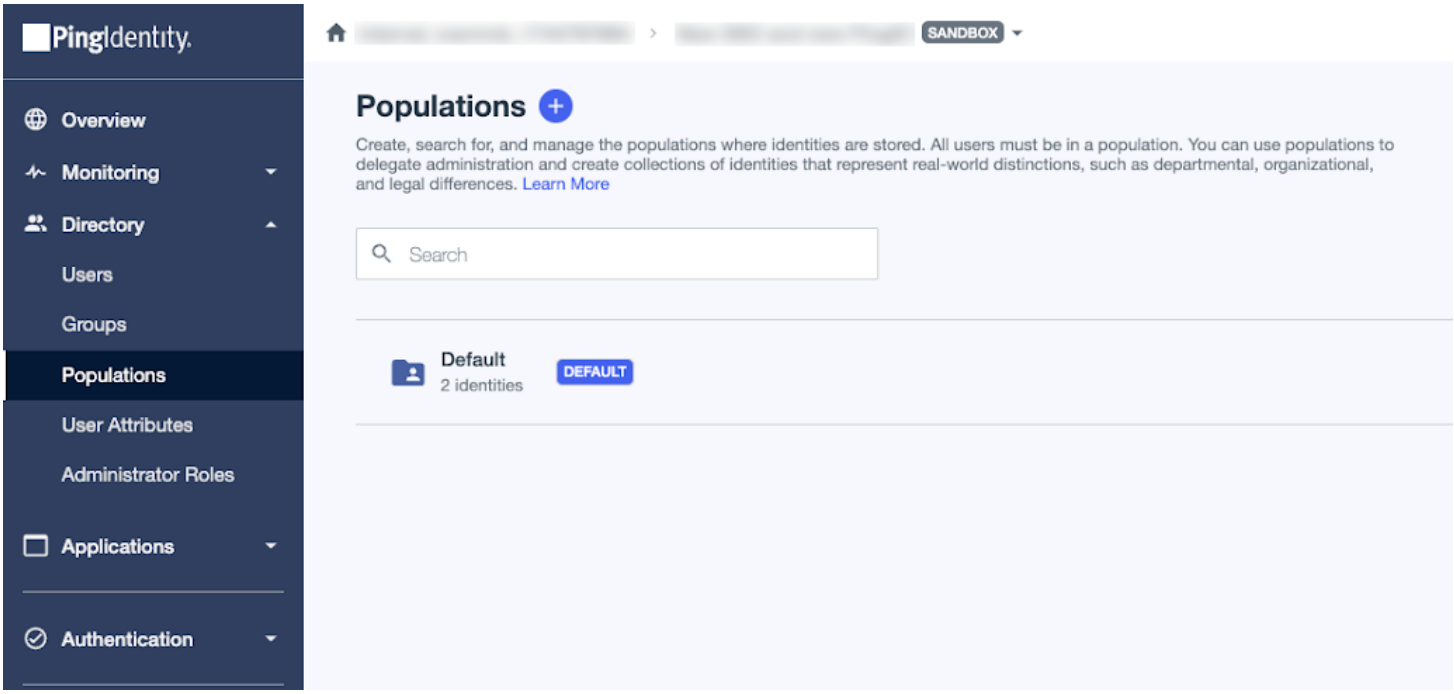
Copyright © 2025 Ping Identity Corporation



Existing PingID accounts: Creating a population for Microsoft Entra ID users and changing the default population

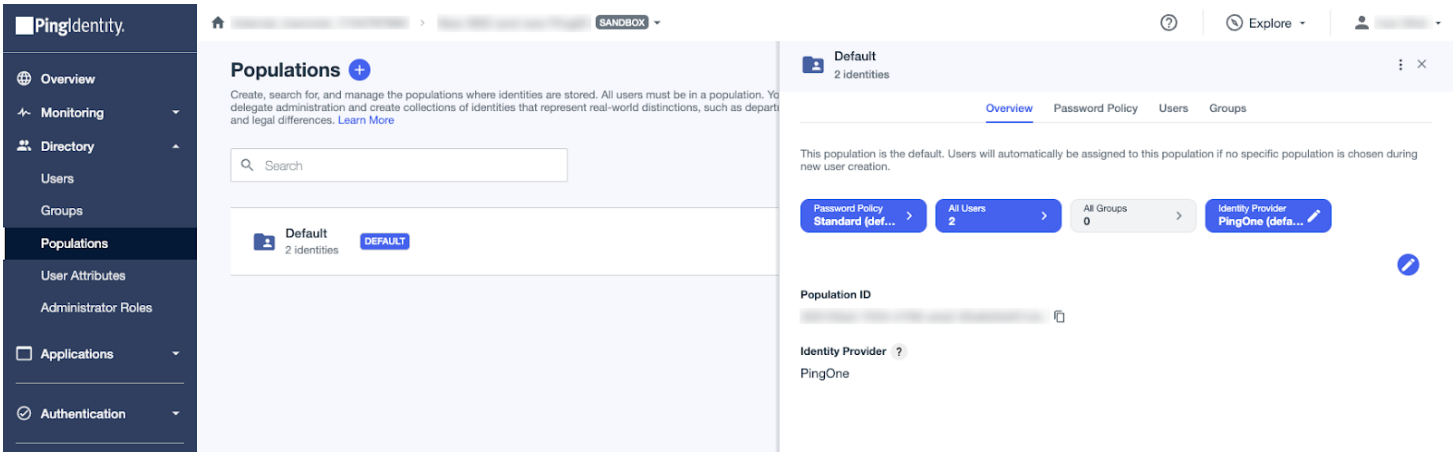
If you integrated your PingID account with a new PingOne account, your new environment includes a population named **Default** with users from PingID assigned to this population. The following image shows the **Default** population with two users from PingID.

> **Note**
>
> If you created a new PingID environment in PingOne, follow the steps in New PingID accounts: Creating a population for Microsoft Entra ID users.



By default, the **Identity Provider** for this population is set to **PingOne**. You'll update this setting as part of this process.

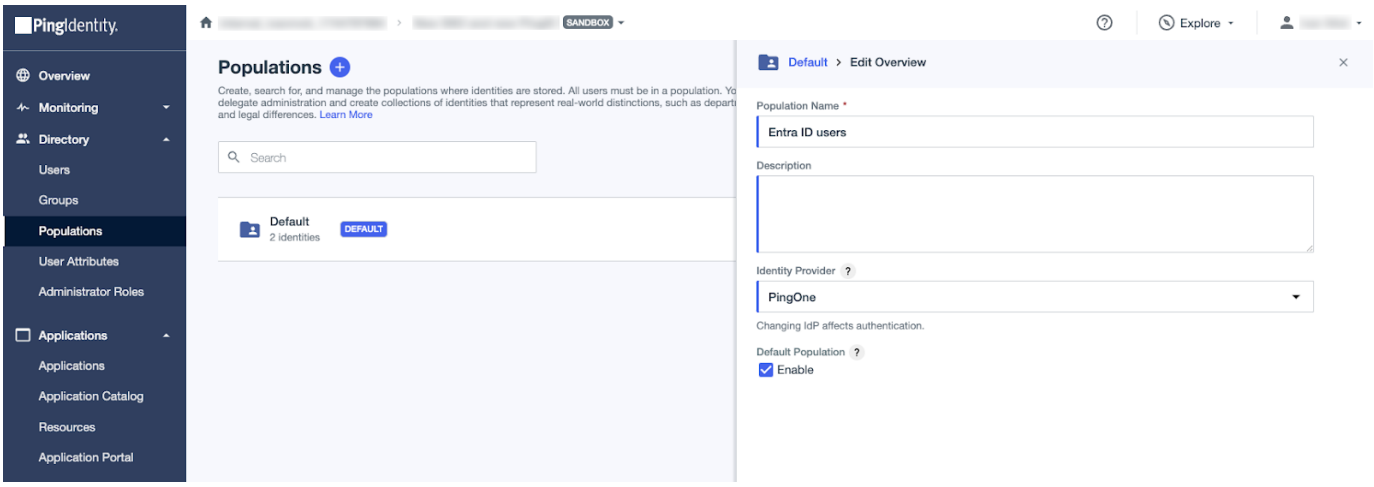
Copyright © 2025 Ping Identity Corporation



Because you could have a future scenario where users in this environment aren't coming from Microsoft Entra ID, you should rename the **Default** population, create a new population for users coming from Entra ID, and set the new population as the default population.

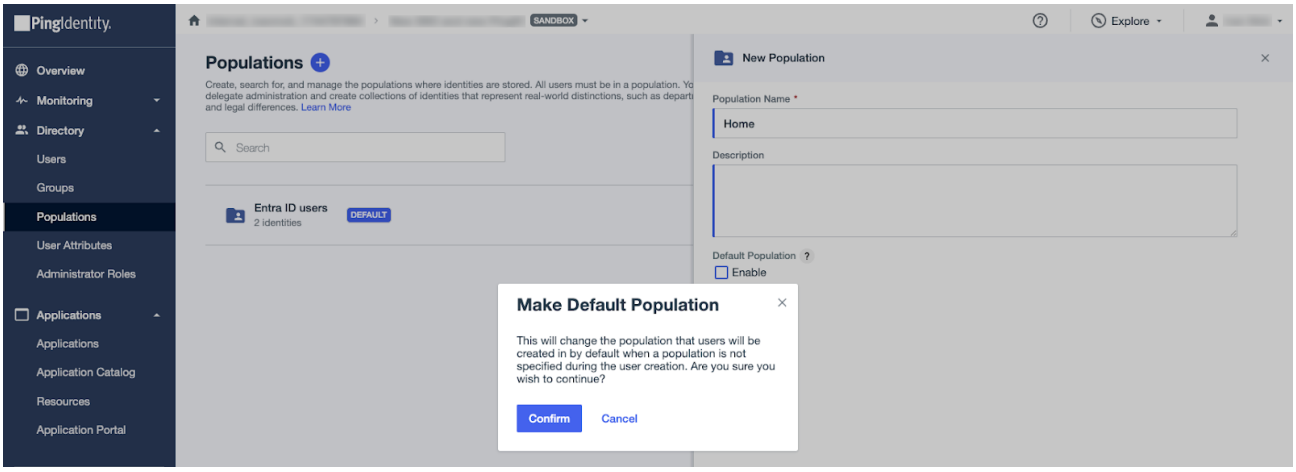
Steps

1. In the PingOne admin console, go to **Directory** > **Populations**.
2. Click the **Default** population, and then click the **Pencil** icon to edit the population.
3. Change **Population Name** from **Default** to a new name, such as `Entra ID users`.



4. Click **Save**.
5. To create a new population, click the **+** icon.
6. Enter the following:
    1. **Population Name**: A unique label for the population, such as `Home`.
    2. **Description** (optional): A brief description of the population.
    3. **Default Population**: Select the **Enable** checkbox to set this population as the new default population.
    4. In the confirmation modal, click **Confirm** to make this population the new default population.

Copyright © 2025 Ping Identity Corporation

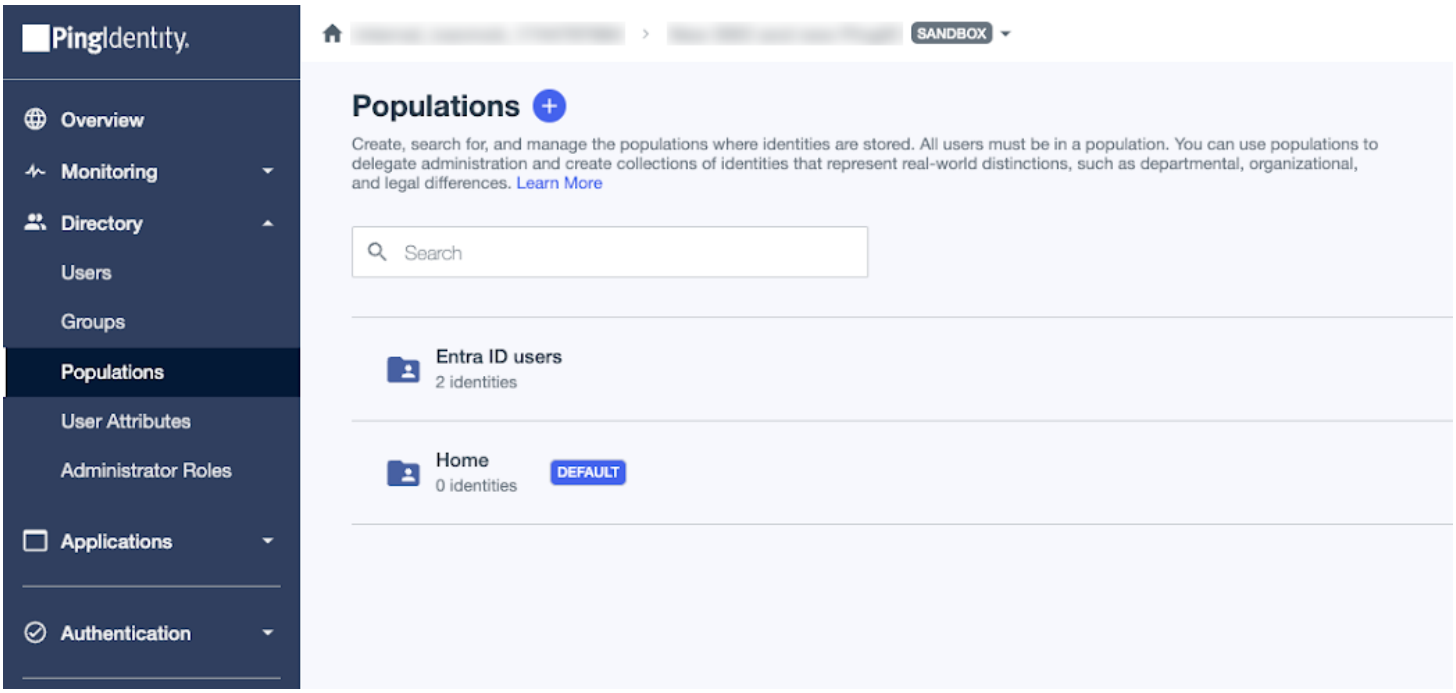


7. Click **Save**.

Result

You now have two populations in your environment:

1. **Entra ID users**: Users from PingID are assigned to this population. This is also the population where future Entra ID users will be assigned when Entra ID redirects users to PingOne for MFA. This population was previously named **Default** and was previously set as the default population.
2. **Home**: This population is the new default population and was created for future scenarios where users aren't coming from Entra ID.



Registering your application with Microsoft

To configure an EAM, register an application in Microsoft Entra. Learn more in Quickstart to registering an app in the Microsoft Entra documentation.

Before you begin

Copyright © 2025 Ping Identity Corporation

Ensure that you have:

- A Microsoft Entra account with an active subscription
- An Entra tenant

Steps

1. Go to the Microsoft Entra admin center and sign on to your account.

   If you don't have a Microsoft Entra account, you can create one now.

2. On the left, expand **Identity > Applications**.
3. Click **App registrations**.
4. At the top, click **New registration**.
5. In the **Name** field, enter a user-facing display name for the application.
6. For **Supported account types**, select **Accounts in this organizational directory only (Ping Identity only - Single tenant)** or **Accounts in any organizational directory and personal Microsoft accounts**, depending on the needs of your organization.

   Select the **Single tenant** option if you're working with only identities from your environment.

7. Under **Redirect URI**, select **Web** as the platform and enter the authorization URL of your PingOne environment.

   > **Tip**
   >
   > You can find this URL on the **Overview** tab of any OIDC application in the PingOne admin console in the **Connection Details** section.

   The format is `<issuer>/authorize`.

   Example 1: `https://auth.pingone.<region>/<envID>/as/authorize`

   Example 2: `https://<customDomain>/as/authorize` if you set up a custom domain. Learn more in Setting up a custom domain.

8. Click **Register**.

Enabling the implicit grant

After registering an application in Entra, enable the implicit grant type for your application to support an EAM.

Steps

1. Go to the Microsoft Entra admin center.
2. In the **App registrations** section, select your application.
3. Go to **Manage > Authentication**.
4. In the **Implicit grant and hybrid flows** section, select the **ID tokens** checkbox.
5. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Getting the client ID and client secret for your application and the tenant ID of your Entra tenant

When you register your application with Microsoft, Microsoft generates an application (client) ID and application secret for the application.

Microsoft also generates a directory (tenant) ID for each Microsoft Entra tenant. You'll copy these values and enter them into PingOne.

Steps

1. Go to the Microsoft Entra admin center.
2. In the **App registrations** section, select your application.
3. On the left, click **Certificates & secrets**.
4. In the **Client secrets** section, click **+ New client secret**.
5. Enter the following:
    1. **Description**: A brief description of the client secret.
    2. **Expires**: Select the duration of the certificate, based on the needs of your organization.
6. Click **Add**.
7. In the **Client secrets** section, locate the value for the applicable secret and copy it to a secure location.
8. On the left, click **Overview**.
9. Locate the **Application (client) ID** and copy it to a secure location.
10. Locate the **Directory (tenant) ID** and copy it to a secure location.

Setting up API permissions

Using an EAM with Microsoft Entra requires certain API permissions that you'll need to enable in your application.

Steps

1. Go to the Microsoft Entra admin center.
2. In the **App registrations** section, select your application.
3. On the left, click **API permissions**.
4. Click **+ Add a permission**.
5. Click **Microsoft Graph**.
6. Click **Delegated permissions** and expand **Openid permissions**.
7. Select the `openid` and `profile` permissions.

> **Note**
>
> `User.Read` is included by default and should remain selected.

Copyright © 2025 Ping Identity Corporation

8. Click **Application permissions**, expand **User**, and select the `User.Read.All` permission.

> **Note**
>
> If you don't intend to retrieve many attributes from Microsoft Entra ID and populate them into PingOne, you can select the `User.ReadBasic.All` permission instead of the `User.Read.All` permission.
> Both of these permissions require admin consent.

9. To grant admin consent, click **Add permissions**.
10. Click **Grant admin consent for <your Entra tenant>**.

Adding Microsoft as an identity provider in PingOne

Configure the IdP connection in PingOne.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs**.
2. Click **+**.
3. Click **Microsoft**.
4. Click **Next**.
5. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.

   > **Note**
   >
   > You can't change the **Icon** and **Sign-on button**, in accordance with the provider's brand standards.

6. Click **Next**.
7. On the **Configure IDP Connection** page, enter the following information:
   - **Client ID**: The application ID from the IdP that you copied earlier. You can find this information on the Microsoft Entra admin center.
   - **Client secret**: The application secret from the IdP that you copied earlier. You can find this information on the Microsoft Entra admin center.
   - **Callback URL**: Copy the **Callback URL** to a secure location. You'll provide this value to the IdP later.
   - **Tenant ID**: The tenant ID of your Entra tenant that you copied earlier. You can find this information on the Microsoft Entra admin center.
8. Click **Next**.

Copyright © 2025 Ping Identity Corporation

9. Define how the PingOne user attributes are mapped to IdP attributes. Learn more in Mapping attributes.
    - Leave the default PingOne user profile attributes and the external IdP attributes:
        - **Preferred Username** (from Microsoft) as the source of the PingOne **Username**
        - **Email** (from Microsoft) as the source of the PingOne **Email Address**
    - To add an attribute, click **+ Add**.
    - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
    - Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
        - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
        - **Always**: Always update the PingOne directory attribute.
10. Click **Save**.
11. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
>
> You can disable the IdP by clicking the toggle to the left (gray).

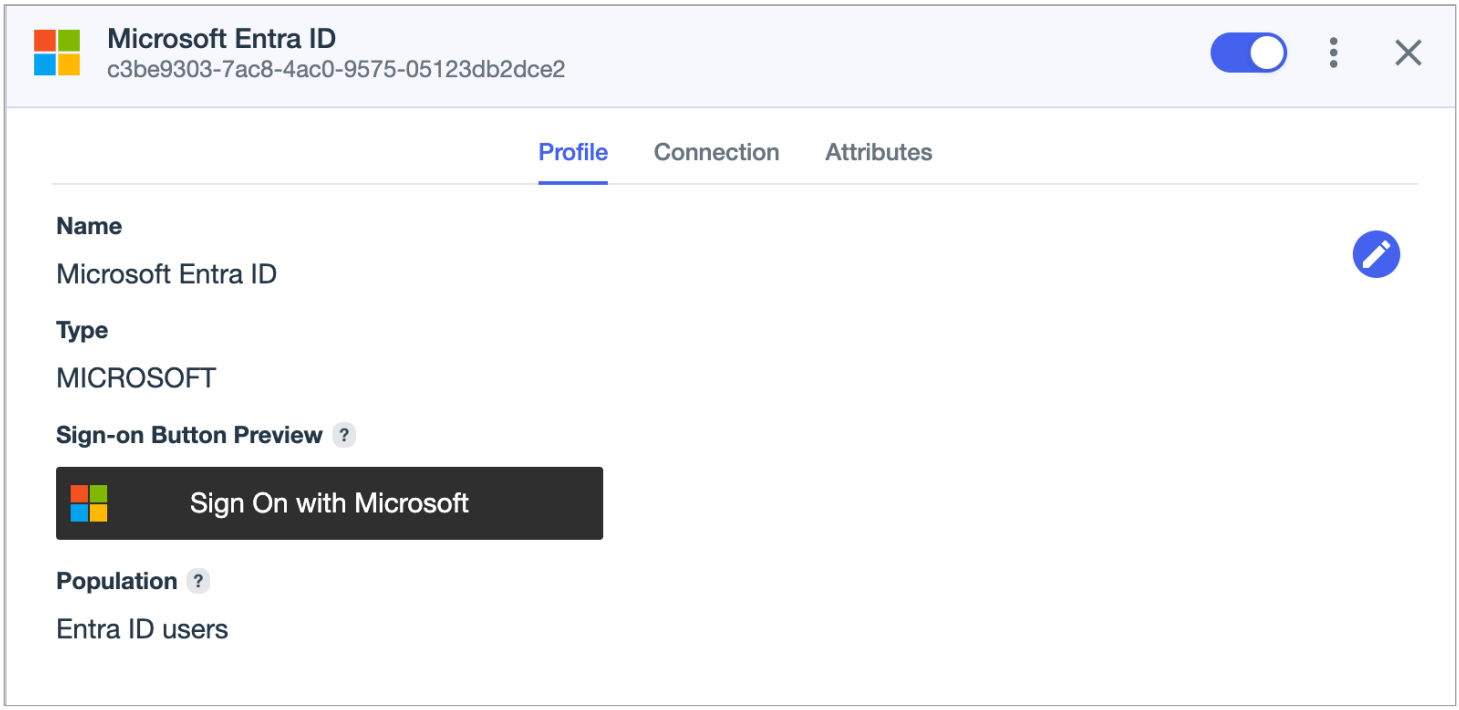
12. Click the connection in the **External IdPs** list to expand the connection details.
13. On the **Profile** tab, click the **Pencil** icon.
14. For **Population**, select the population that you previously created for Entra ID users.

> **Note**
>
> - If you created a new PingID environment in PingOne, use the population that you created in New PingID accounts: Creating a population for Microsoft Entra ID users.
> - If you integrated your PingID account with a new PingOne account, use the population that you created in Existing PingID accounts: Creating a population for Microsoft Entra ID users and changing the default population.

15. Click **Save**.
16. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
>
> You can disable the IdP by clicking the toggle to the left (gray).

Copyright © 2025 Ping Identity Corporation



Updating the population

After creating your connection to Microsoft, update the **Identity Provider** setting for the population that you created for users coming from Entra ID.

The **Identity Provider** setting is used as the runtime fallback IdP for users in the population who don't have an authoritative IdP configured in their user profile. Updating the population is especially important if you integrated your PingID account with a new PingOne account because those user profiles are created in PingOne without an authoritative IdP set. If the user is removed from the population, the IdP set in the population no longer applies to them.

Steps

1. In the PingOne admin console, go to **Directory** > **Populations**.
2. Click the population that you previously created for Entra ID users.
3. Click the **Pencil** icon.
4. In the **Identity Provider** list, select the IdP that you previously created in Adding Microsoft as an identity provider in PingOne.
5. Click **Confirm** in the modal, and then click **Save**.

Adding an authentication policy for Entra ID external authentication

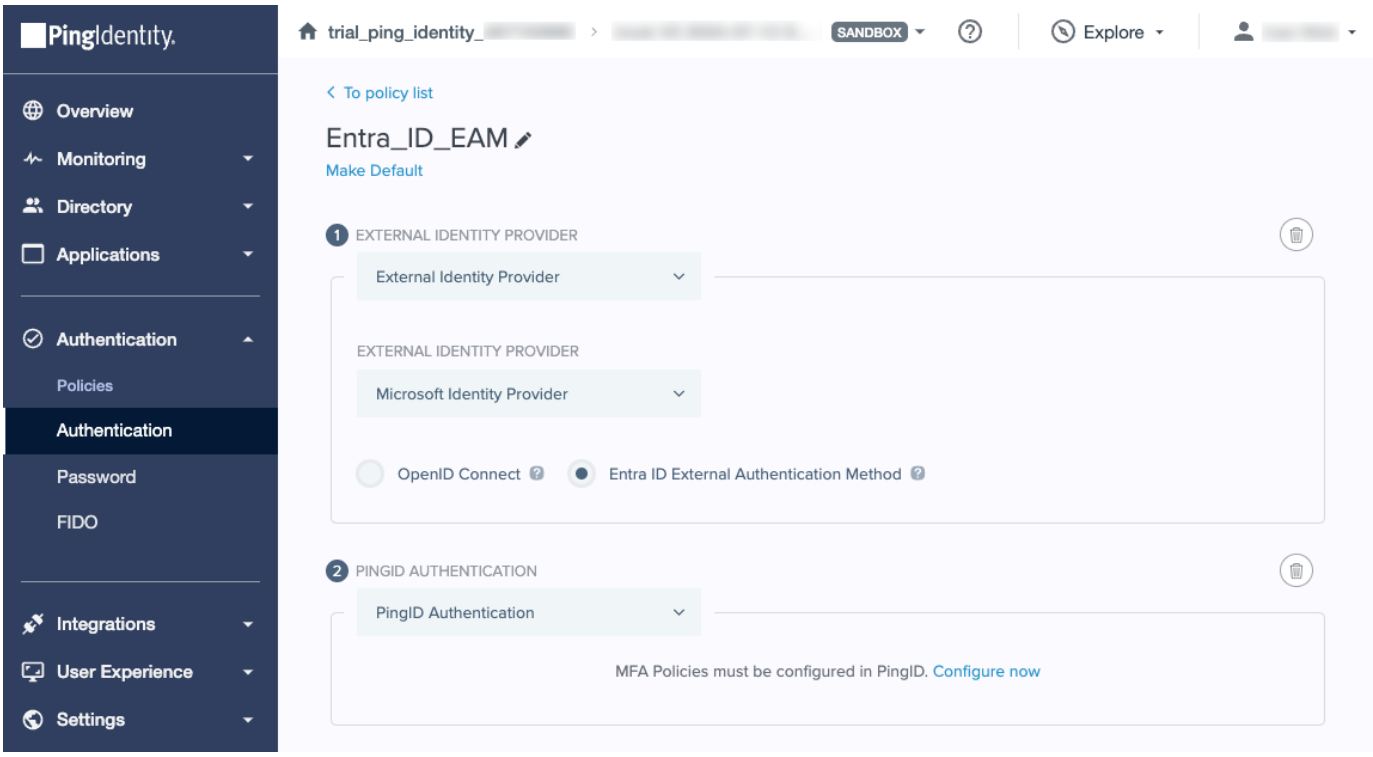
Add the Microsoft IdP to an authentication policy followed by an MFA step.

Steps

1. In the PingOne admin console, go to **Authentication** > **Authentication**.
2. Click **+ Add policy** and enter a name for the policy.

Copyright © 2025 Ping Identity Corporation

3. For the first step:
    1. In the **Step Type** list, select **External Identity Provider**.
    2. In the **External Identity Provider** list, select your Microsoft IdP.
    3. For **Policy Purpose**, select the **Entra ID External Authentication Method** option.
4. Click **+ Add step**.
5. For the second step, in the **Step Type** list, select **PingID Authentication**.



6. Click **Save**.

Configuring the OIDC application

Configure an OIDC application to handle authentication requests from Microsoft Entra ID.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications**.
2. Click **+** to add an application.
3. Enter the following:
    1. **Application name**: A unique identifier for the application.
    2. **Description** (optional): A brief description of the application.
    3. **Icon** (optional): A graphic representation of the application. Use a file up to 1 MB in JPG, JPEG, GIF, or PNG format.
4. For **Application Type**, select **OIDC Web App**.

Copyright © 2025 Ping Identity Corporation

5. Click **Save**.
6. On the **Configuration** tab, click the **Pencil** icon, and enter or edit the following:
    1. For **Response Type**, clear the default **Code** checkbox and select **ID Token**.
    2. For **Grant Type**, clear the default **Authorization Code** checkbox and select **Implicit**.
    3. For **Redirect URIs**, enter `https://login.microsoftonline.com/common/federation/externalauthprovider`.
    4. Click **Save**.
7. On the **Policies** tab, click **+ Add Policies**.
8. On the **PingOne Policies** tab, select the authentication policy that you created to handle external authentication requests from Entra ID.
9. Click **Save**.
10. To enable the application, click the toggle at the top of the details panel to the right (blue).

    > **Note**
    > You can disable the application by clicking the toggle to the left (gray).

11. Click the application entry to open the details panel.
12. On the **Overview** tab, copy the following PingOne application details to add in the Microsoft Entra admin center:
    - In the **General** section, copy the **Client ID** to a secure location.
    - In the **Connection Details** section, copy the **OIDC Discovery Endpoint** to a secure location.

Creating an external authentication method in Microsoft Entra

After creating the OIDC application in PingOne and copying the application ID, OIDC discovery endpoint, and client ID, create an EAM in Microsoft Entra.

Steps

1. Go to the Microsoft Entra admin center.
2. On the left, go to **Protection > Authentication methods**.
3. Click **Add external method**.
4. Enter the following:
    1. **Name**: Enter a name for the EAM.
    2. **Client ID**: Enter your PingOne application's client ID that you copied earlier.
    3. **Discovery Endpoint**: Enter the **OIDC Discovery Endpoint** that you copied earlier. The format is `<issuer>/.well-known/openid-configuration`.
    4. **App ID**: Enter the ID of the Microsoft Entra application that you copied previously. You can find the application ID in the Microsoft Entra admin center.

Copyright © 2025 Ping Identity Corporation

5. Click **Request permission**.

   The browser opens a new window for you to sign on with your Microsoft Entra admin credentials.

6. Review the requested permissions and click **Accept** if you agree.
7. In the **Enable and target** section, configure whether you want to include a subset of your users or all users.
8. Click the **Enable** toggle to enable the EAM.

Creating a conditional access policy in Microsoft Entra

Configure a conditional access policy in Microsoft Entra to define authentication requirements for users accessing applications.

> **Note**
>
> If your Microsoft Entra tenant contains other conditional access policies that use custom controls to initiate MFA, ensure those policies don't apply to the same users, groups, and applications that you select in this conditional access policy. Otherwise, your users could be prompted multiple times for MFA.

Steps

1. Go to the Microsoft Entra admin center.
2. On the left, go to **Protection** > **Conditional Access**.
3. Click **Policies**.
4. Update an existing policy or create a new policy.
5. Configure the following:
   1. **Name**: Enter a name.
   2. **Users**: Select the same users and groups that you selected in your EAM.
   3. **Target resources**: Select the applications to which you want to apply this conditional access policy.
   4. **Grant**:
      1. Click **Grant access**.
      2. Select the **Require multifactor authentication** checkbox.
      3. Click **Select**.
   5. **Enable policy**: Select **On** to turn on the policy.
6. Click **Save**.

Configuring PingID as the external authentication method

Configure a PingID policy to process user MFA requests coming from the PingOne application that you created to handle Microsoft Entra requests.

Steps

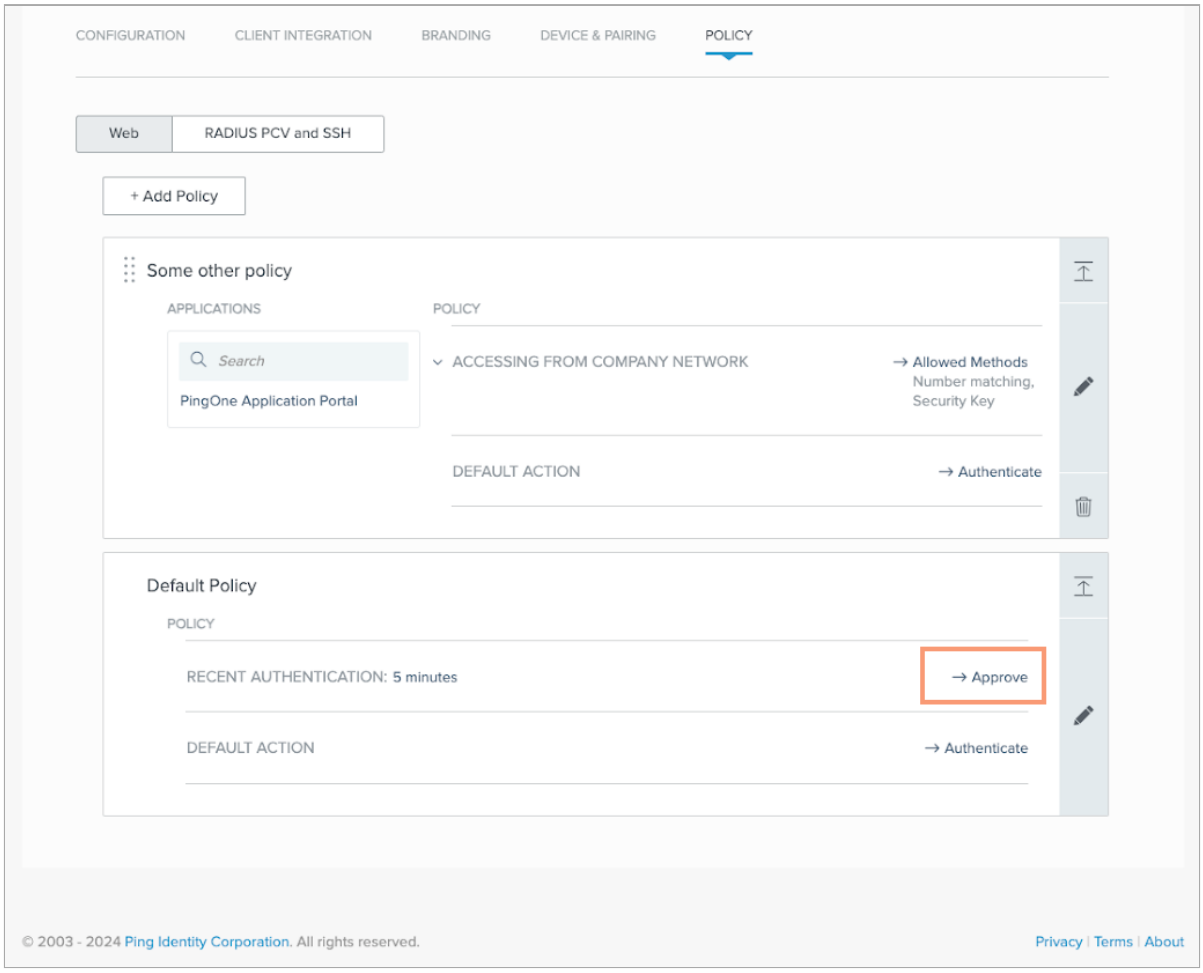
1. In the PingID admin portal, go to **Setup** > **PingID** and click the **Configuration** tab.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If you selected **Enable** for **Enforce Policy**, you might need to create an additional PingID policy. Learn more in the next step.

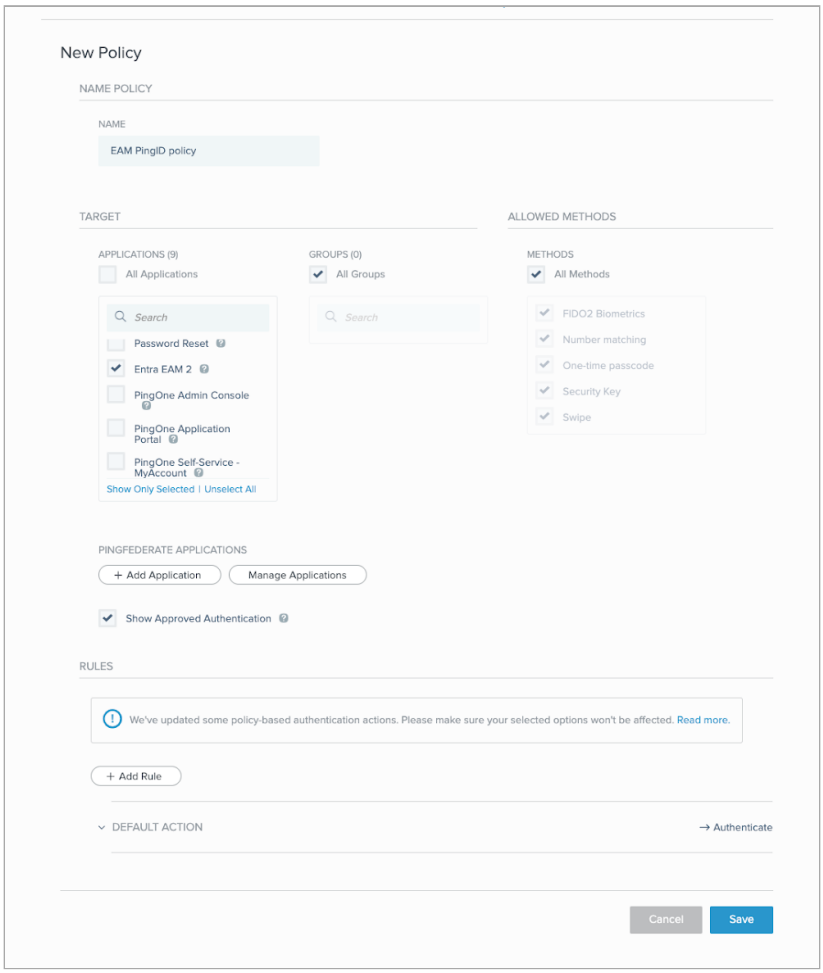
2. Click the **Policy** tab, and on the **Web** tab, expand and review each policy.

> **Note**
>
> Microsoft Entra ID doesn't allow MFA bypasses from an EAM and requires always prompting the user to complete MFA. If you have a policy that can apply to all applications and that has a rule with an action of **Approve**, you must create a new policy for the PingOne application. Examples of such policies include Recent Authentication or Accessing from Company Network.



1. To add a new policy, click **Add Policy**.
2. Enter a name for the policy, such as `EAM PingID policy`.
3. In the **Target** section, in the **Applications** list, select the PingOne application that you previously created.
4. For **Groups**, select all applicable groups.
5. (Optional) In the **Allowed Methods** section, select the authentication methods you want to allow.

6. Click **Save**.



Result:

The new policy becomes the first PingID policy, which works as a Microsoft Entra ID EAM. PingID will use this new policy when processing MFA requests coming from the PingOne application that you created to handle Microsoft Entra ID requests.

3. In a scenario where a user forgot or lost their mobile phone and can't use the PingID app for MFA, you can allow a user to bypass MFA with PingID for a specificed period of time, such as 8 hours.

    1. In the PingOne admin console, go to **Directory > Users**.
    2. Browse or search for the applicable user, and click the user entry to open the details panel.
    3. In the list for the **Services** tab, select **Authentication**.
    4. Scroll down to the **Integrations** section, click the **More Options** icon, and select **Bypass**.
    5. In the **Bypass** window, select the desired amount of time from the **Allow bypass of PingID authentication on SSO for** list and click **Bypass**.

Copyright © 2025 Ping Identity Corporation

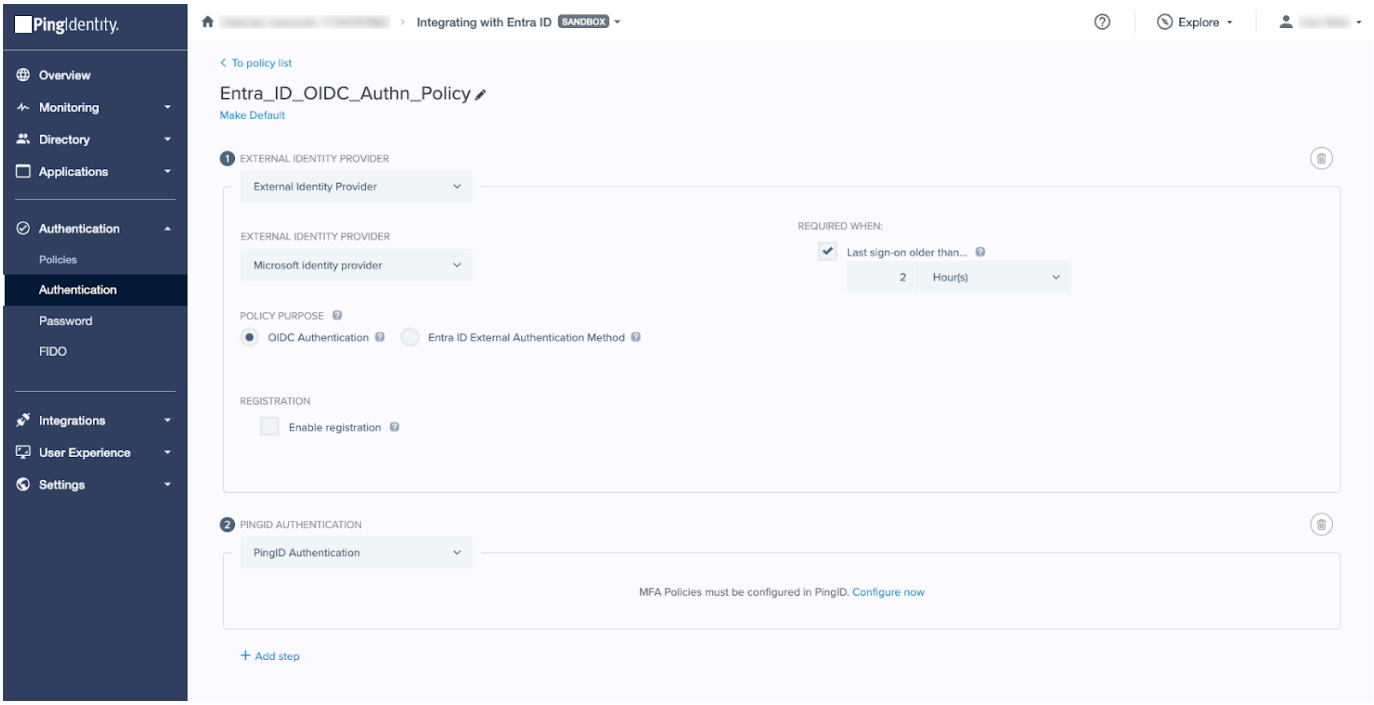
> **Note**
>
> Because Microsoft Entra ID requires the third-party MFA provider to specify the MFA method used and doesn't accept MFA bypasses as an acceptable MFA method, you must also configure bypass in the Microsoft Entra admin center. Learn more about configuring conditional access in the Microsoft Entra documentation.

Adding an authentication policy for OIDC authentication

If you want to allow users to sign on to the **PingOne Self-Service - MyAccount** application to manage their MFA methods or to other applications you've added to PingOne, you must create an authentication policy for OIDC authentication using the same Microsoft IdP connection.

Steps

1. In the PingOne admin console, go to **Authentication** > **Authentication**.
2. Click **+ Add policy** and enter a name for the policy.
3. For the first step:
    1. In the **Step Type** list, select **External Identity Provider**.
    2. In the **External Identity Provider** list, select your Microsoft IdP. This is the same Microsoft IdP you selected in Adding an authentication policy for Entra ID external authentication.
    3. For **Policy Purpose**, select the **OIDC Authentication** option.
4. If you want to prompt users for MFA, click **+ Add step**, and for the second step, select **PingID Authentication** in the **Step Type** list.



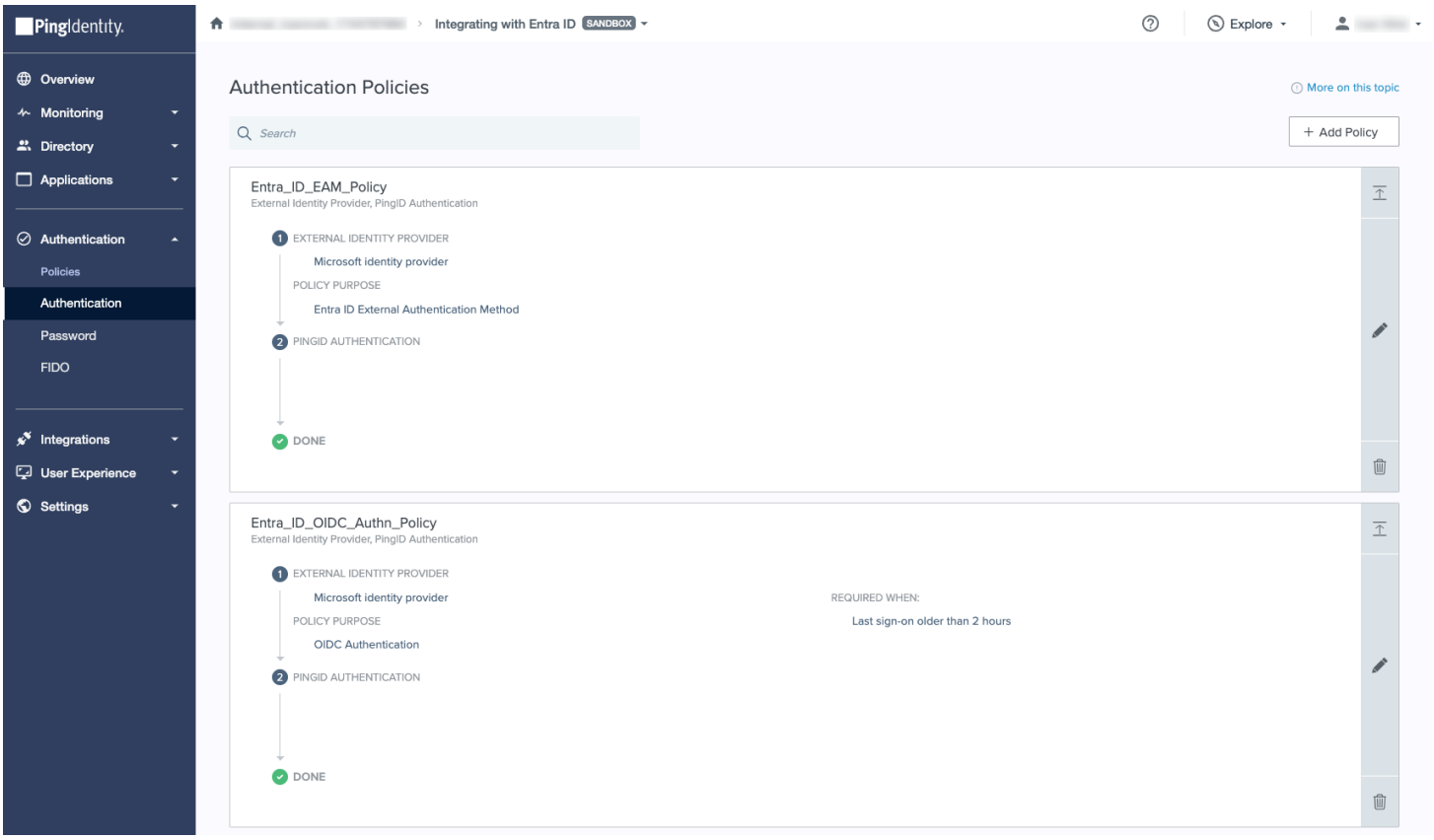
5. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Result:

You now have two authentication policies:

- An authentication policy for users authenticating with PingOne as the EAM for Microsoft Entra
- An authentication policy for OIDC authentication to allow users to sign on to other applications



Adding the callback URL to the Microsoft Entra admin center

If you created an authentication policy for OIDC authentication, you must also add the callback URL from the Microsoft IdP connection to the application you registered in the Microsoft Entra admin center.

Steps

1. In the PingOne admin console, go to **Integrations > External IdPs** and locate the Microsoft IdP that you created previously.
2. Click the IdP to open the details panel.
3. Click the **Connection** tab.
4. Copy the **Callback URL**.

   The following examples show the URL format:

   Example 1: `https://auth.pingone.<region>/<envID>/rp/callback/microsoft`

   Example 2: `https://<customDomain>/rp/callback/microsoft`
5. Go to the Microsoft Entra admin center.

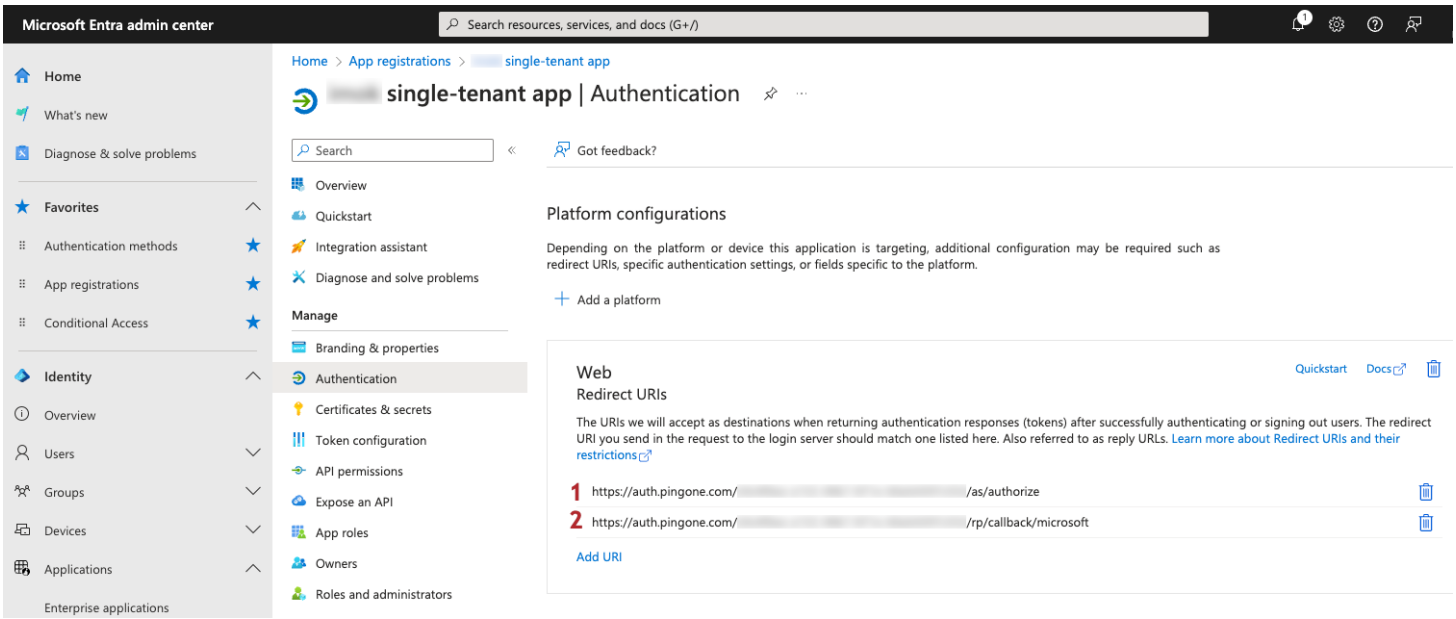
Copyright © 2025 Ping Identity Corporation

6. In the **App registrations** section, select your application.
7. On the left, click **Authentication**.
8. Go to **Platform configurations** > **Web** > **Redirect URIs**, and click **Add URI**.
9. Paste the **Callback URL** that you copied from the PingOne admin console.
10. Click **Save**.

Result

The **Redirect URIs** section displays both URLs you've added:

1. Authorization URL
2. Callback URL



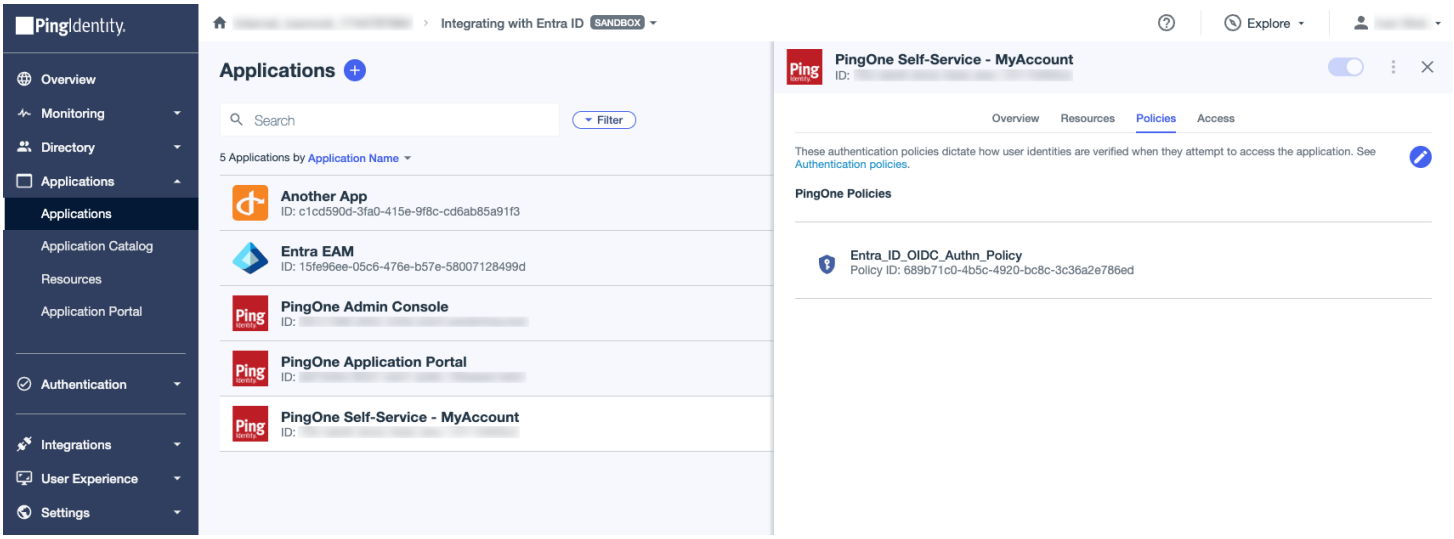
Assigning the OIDC authentication policy to an application in PingOne

After you create an authentication policy for OIDC authentication and add the callback URL to the application in Microsoft Entra, assign the OIDC authentication policy to applicable applications in PingOne, such as the **PingOne Self-Service - MyAccount** application or other applications you've added.

Steps

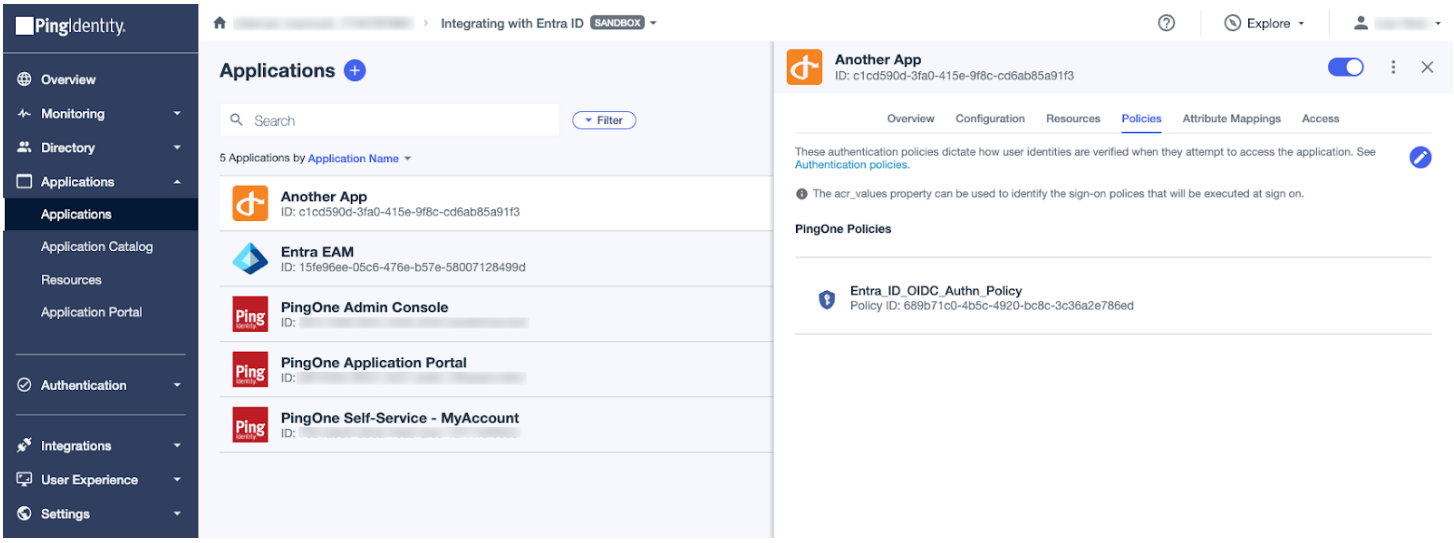
1. In the PingOne admin console, go to **Applications** > **Applications**.
2. Select the relevant application.
3. On the **Policies** tab, click **+ Add policies**.
4. On the **PingOne Policies** tab, select the OIDC authentication policy.
5. Click **Save**.

Copyright © 2025 Ping Identity Corporation



Next steps

Repeat these steps for any other applications to which you want users to be able to sign on, for example **Another App** in the following screenshot.



Validation

Now that you've set up an EAM in Microsoft Entra ID and configured PingOne and PingID as the external MFA provider, you're ready to validate that your Entra ID users can use PingID to complete MFA.

1. Open a new browser window in incognito mode.
2. In the Microsoft Entra admin center, locate the application you added to the conditional access policy that requires MFA and click the URL for the application.

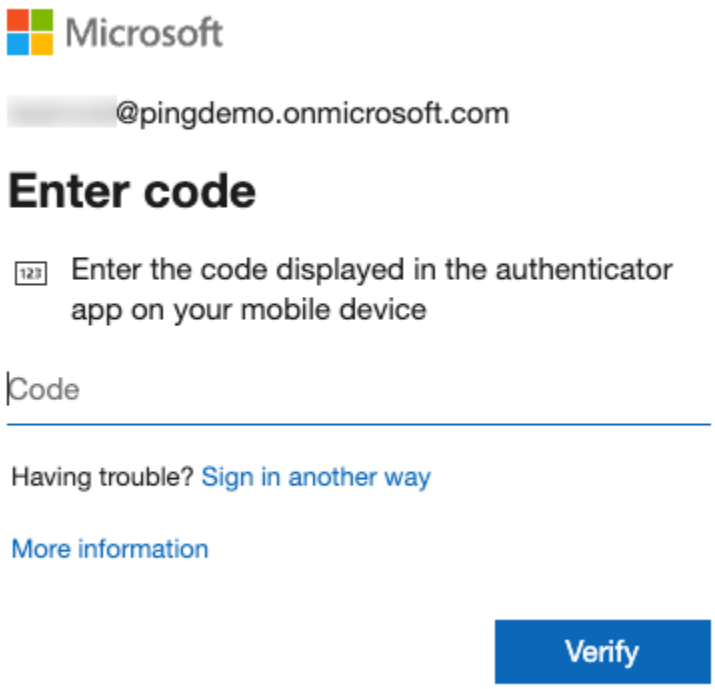
   In this example, **My Apps** at https://myapps.microsoft.com.
3. Sign on to the application and complete the first-factor authentication at Microsoft using a test user's credentials.

   Result:

Copyright © 2025 Ping Identity Corporation

If you, as an Entra ID admin, have activated system-preferred MFA and included the test user as the target user, and if the test user has installed and successfully used the system-preferred MFA method, Entra ID prompts the user to complete MFA action based on what Entra thinks is the most secure method.

In this example, the test user has installed and used both Microsoft Authenticator and verification code by text message, so Entra ID prompts the user to enter the code from Microsoft Authenticator.



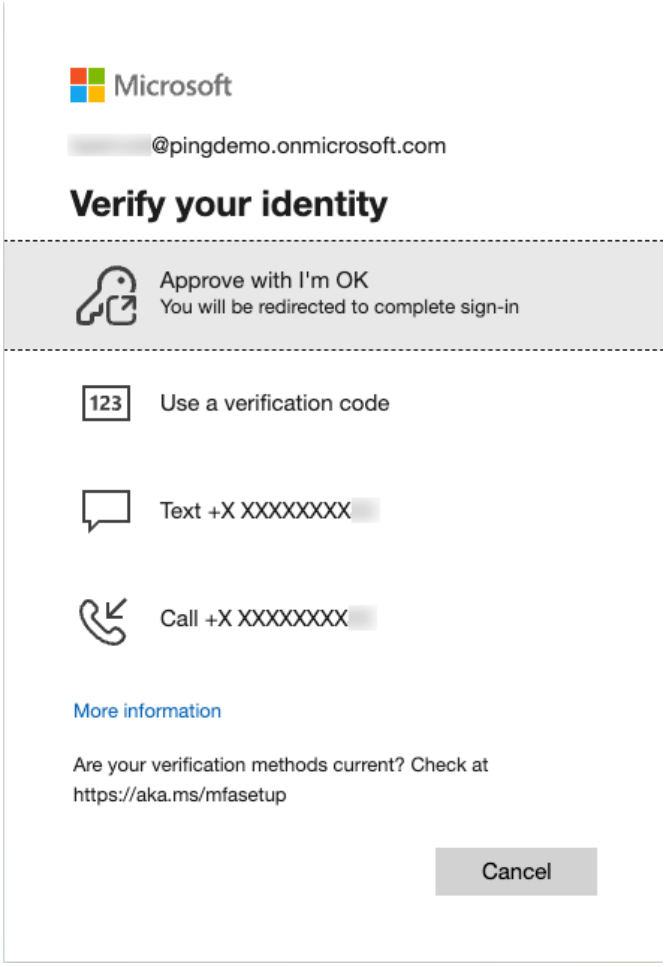
> **Note**
>
> If you haven't activated system-preferred MFA, the user won't see the **Enter code** page and is prompted to verify their identity.

4. To use your EAM, click **Sign in another way** at the bottom of the **Enter code** window.

   Result:

   After selecting **Sign in another way** or if system-preferred MFA doesn't apply, Entra ID displays the **Verify your identity** page.

Copyright © 2025 Ping Identity Corporation



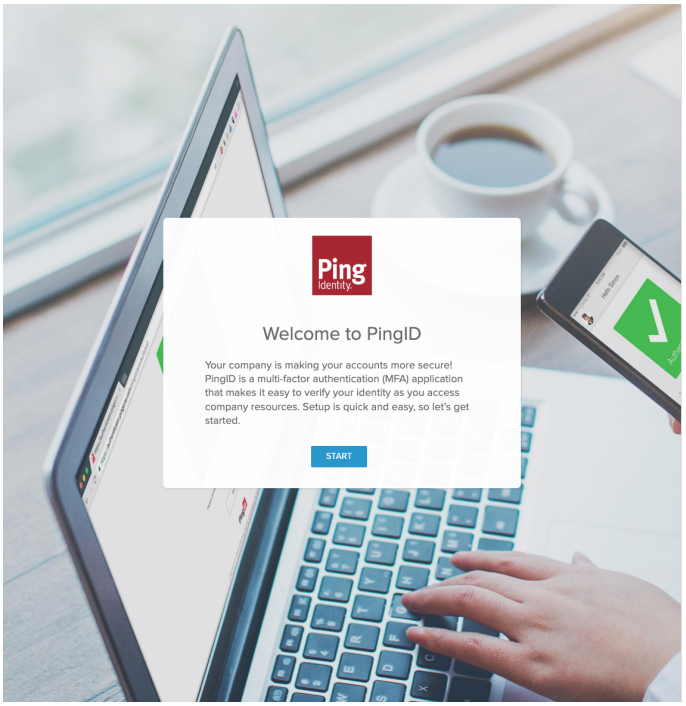
5. Select the EAM.

   Result:

   Entra ID redirects the browser to PingOne.

6. If the test user hasn't yet paired the PingID app, they're shown a **Welcome to PingID** page. Click **Start** to start the pairing process.

Copyright © 2025 Ping Identity Corporation



Result:

After pairing, the PingID app prompts the user to complete the MFA requirement.

7. After PingID is paired for the test user, complete the MFA prompt from the PingID app.

   Result:

   PingOne returns an ID token to Entra ID, and Entra ID processes the ID token and signs the test user on to the application.

8. Sign out of the application.

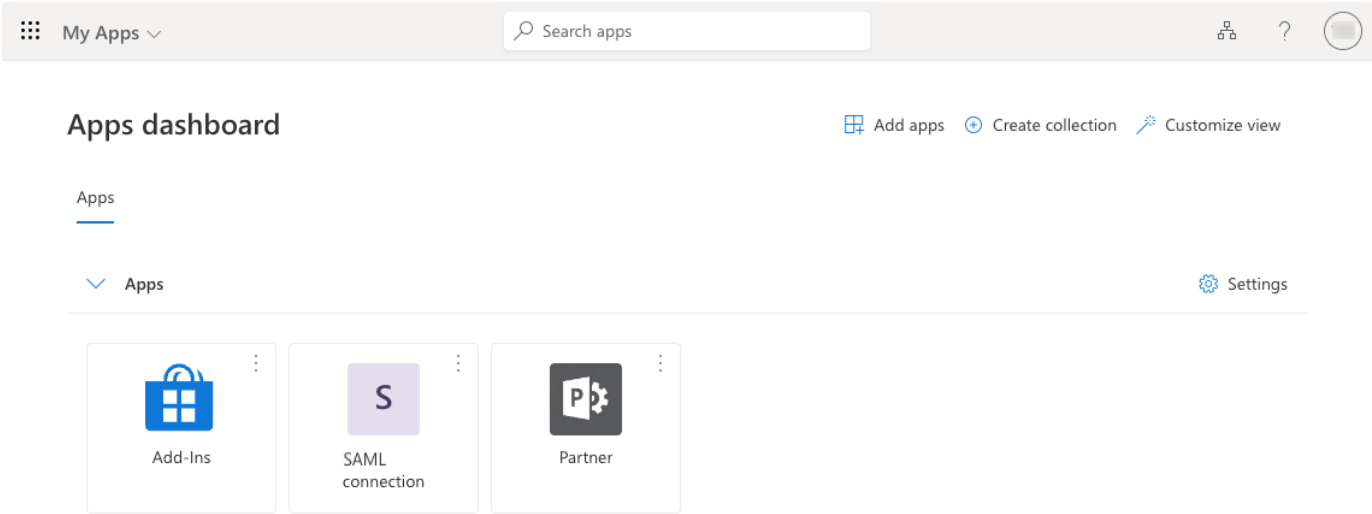
9. In the Microsoft Entra admin center, locate the same application and authenticate to the application again as the test user.

   Result:

   This time, PingID shouldn't prompt the test user to pair a device. Instead, the PingID app should prompt the test user to complete the MFA requirement.

   When the test user completes the MFA requirement, PingOne returns an ID token to Entra ID, and Entra ID processes the ID token and signs the test user on to the application.

Copyright © 2025 Ping Identity Corporation



Setting up PingOne SSO, DaVinci, and PingID as the external MFA provider for Microsoft Entra ID

Microsoft Entra ID allows customers to use an external authentication provider for multi-factor authentication (MFA) through external authentication methods (EAMs). In this use case, you'll learn how to set up Entra ID, PingOne SSO, DaVinci, and PingID to support an EAM in Entra ID.

Set up an EAM in Entra ID if:

- Entra ID is the identity provider (IdP).
- The users reside in a managed domain in Entra ID.

  Learn more in Create and configure a managed domain in the Entra ID documentation.
- PingOne is the external authentication provider.

> **Note**
>
> If you added a Microsoft 365 application to PingOne using the application catalog and completed the PowerShell cmdlets to set up PingOne as the federated IdP for the domain in Entra ID, an EAM isn't required for MFA. Instead, you can add an MFA claim in the Microsoft 365 application to communicate to Entra ID that PingOne will handle MFA. Learn more in Using WS-Fed or SAML 1.1 federated IdP in the Entra ID documentation.

The high-level process of signing on with an EAM works as follows, with PingOne and PingID acting as the external authentication provider:

1. A user opens an application protected by Entra ID and is prompted to complete first-factor MFA in Entra ID.
2. Entra ID determines that another factor needs to be satisfied, such as if a conditional access policy requires MFA.
3. The user chooses the applicable EAM as second-factor MFA.
4. Entra ID sends an OpenID Connect (OIDC) authentication request to PingOne (the external authentication provider in this use case).

Copyright © 2025 Ping Identity Corporation

5. PingOne initiates MFA for the user.
6. The user completes the MFA requirement using the PingID app.
7. PingOne returns an ID token to Entra ID in the authentication response.
8. Entra ID validates the ID token and signs the users on to the application.

Learn more about EAMs in the Microsoft Entra MFA external method provider reference in the Entra ID documentation.

Goals

After completing this use case, you'll know how to:

- Configure Microsoft Entra ID to support an EAM for MFA.
- Add Entra ID as an external IdP in PingOne.
- Set up PingID as the MFA solution for Entra ID users.

What you'll do

In Microsoft Entra ID, you'll configure three components:

1. Add and configure an application.
2. Create an EAM.
3. Add a conditional access policy.

In PingOne, you'll configure the following:

1. Create a population for Entra ID users.
2. Create a Microsoft IdP connection.

In DaVinci, you'll configure two flows:

1. Add a flow to handle external authentication requests from Entra ID.
2. Add a second DaVinci flow to redirect users to Entra ID for OIDC authentication.

The last step is configuring PingID as the EAM for Entra ID.

Before you begin

PingOne is a cloud-based identity as a service (IDaaS) framework for secure identity access management that uses an organization-based model to define tenant accounts and their related entities within the PingOne platform. Each organization contains one or more tenants, known as environments, which define separate working domains within an organization.

To set up this use case, you'll need:

- A PingOne organization. Learn more in Starting a PingOne trial.
- A PingOne environment with the PingOne SSO, DaVinci, and PingID services added.

Copyright © 2025 Ping Identity Corporation

Create a new environment as follows, depending on whether you're already using PingID:

- If you aren't using PingID already or if you want to create a new PingID account, create a new PingID environment in PingOne.
- If you're using PingID currently and want to use your existing PingID account, integrate a PingID account with a new PingOne account. You should also follow these steps if you've previously integrated PingID with Microsoft Entra ID using custom controls. Learn more about integrating PingID with Entra ID in the PingID documentation.

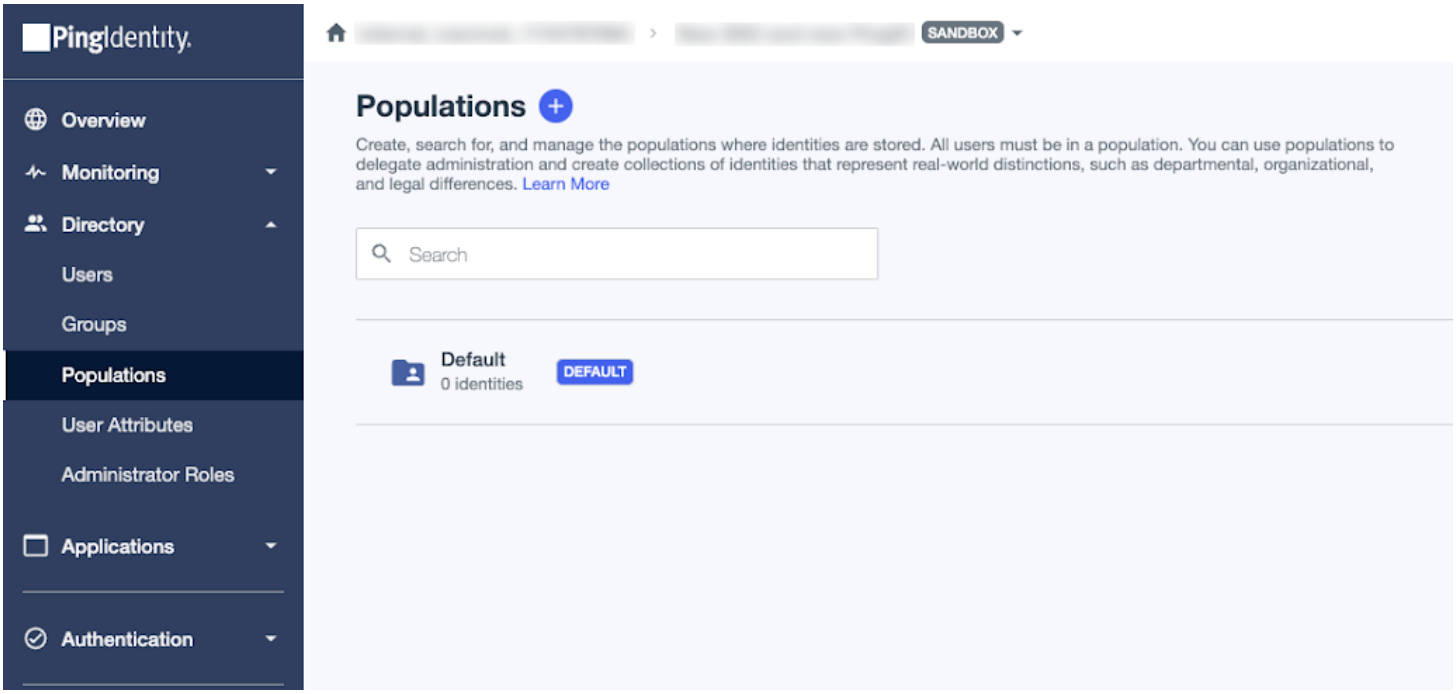
- A Microsoft Entra account with an active subscription and an Entra tenant.

Tasks

New PingID accounts: Creating a population for Microsoft Entra ID users

If you created a new PingID environment in PingOne, your new environment includes a population named **Default**. Learn more in Creating a new PingOne environment with MFA.

> **Note**
>
> If you integrated an existing PingID account with a new PingOne account, skip to Existing PingID accounts: Creating a population for Microsoft Entra ID users and changing the default population.



When you configure an EAM for Microsoft Entra, you'll need to create a new population in PingOne for users coming from Entra ID.

Steps

1. In the PingOne admin console, go to **Directory** > **Populations**.
2. Click the **+** icon to add a new population.

Copyright © 2025 Ping Identity Corporation

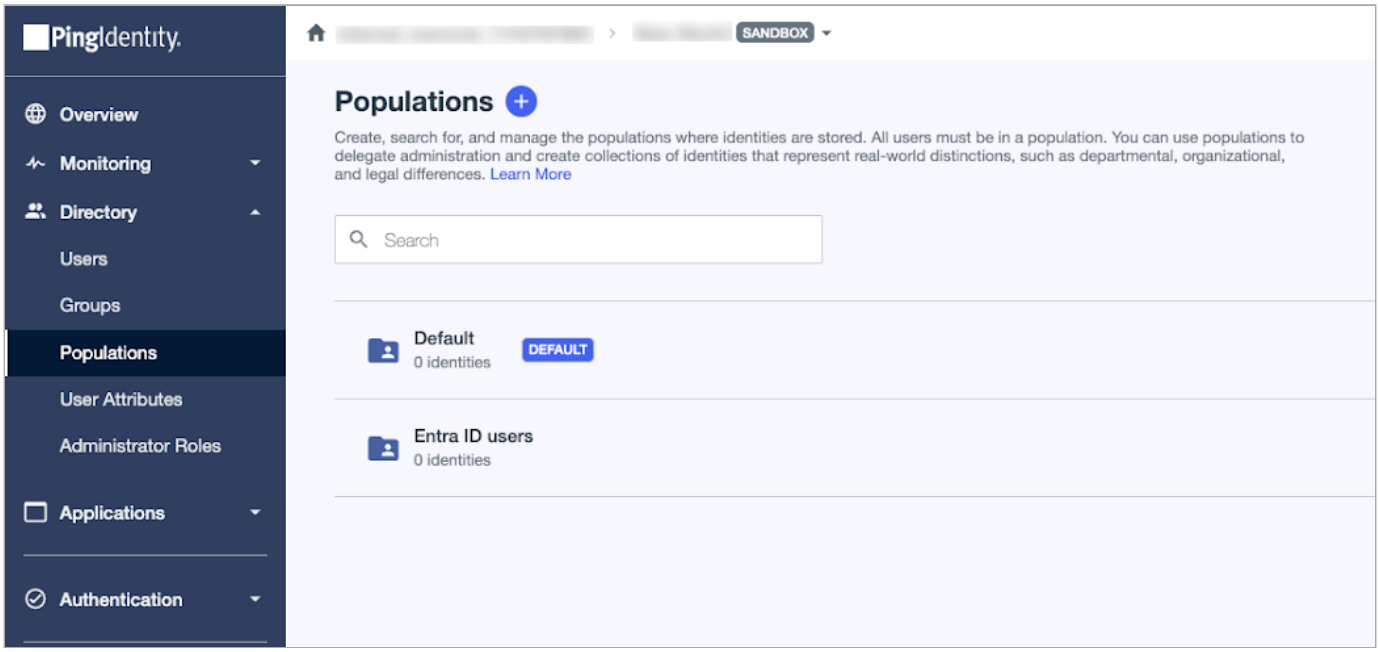
3. Enter the following:

    1. **Population Name**: A unique label for the population, such as `Entra ID users`.

    2. **Description** (optional): A brief description of the population.

    3. **Default Population** (optional): Don't select this checkbox in this scenario unless you want to specify this population as the new default population.

4. Click **Save**.

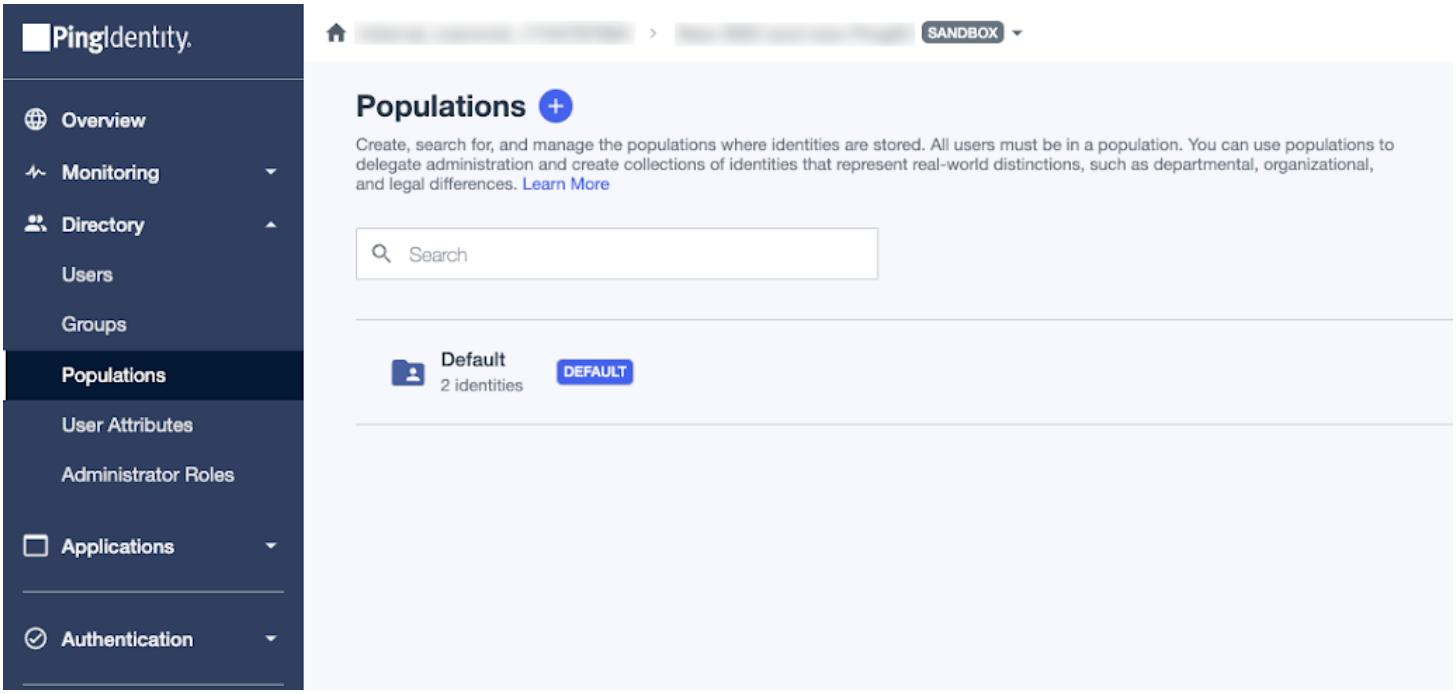


Existing PingID accounts: Creating a population for Microsoft Entra ID users and changing the default population

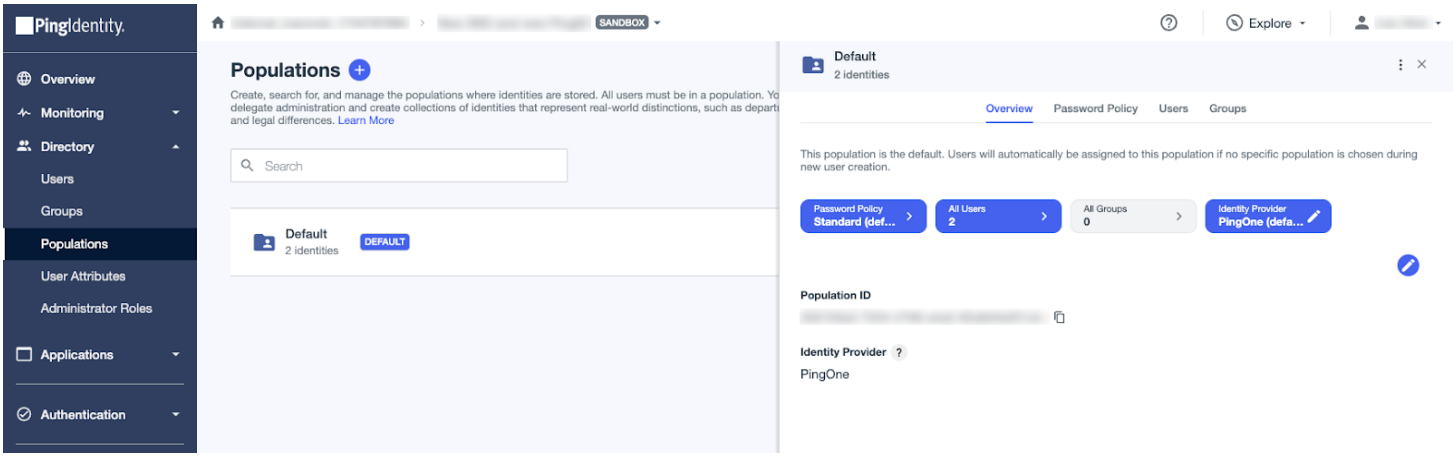
If you integrated your PingID account with a new PingOne account, your new environment includes a population named **Default** with users from PingID assigned to this population. The following image shows the **Default** population with two users from PingID.

> **Note**
>
> If you created a new PingID environment in PingOne, follow the steps in New PingID accounts: Creating a population for Microsoft Entra ID users.

Copyright © 2025 Ping Identity Corporation



By default, the **Identity Provider** for this population is set to **PingOne**. You'll update this setting as part of this process.

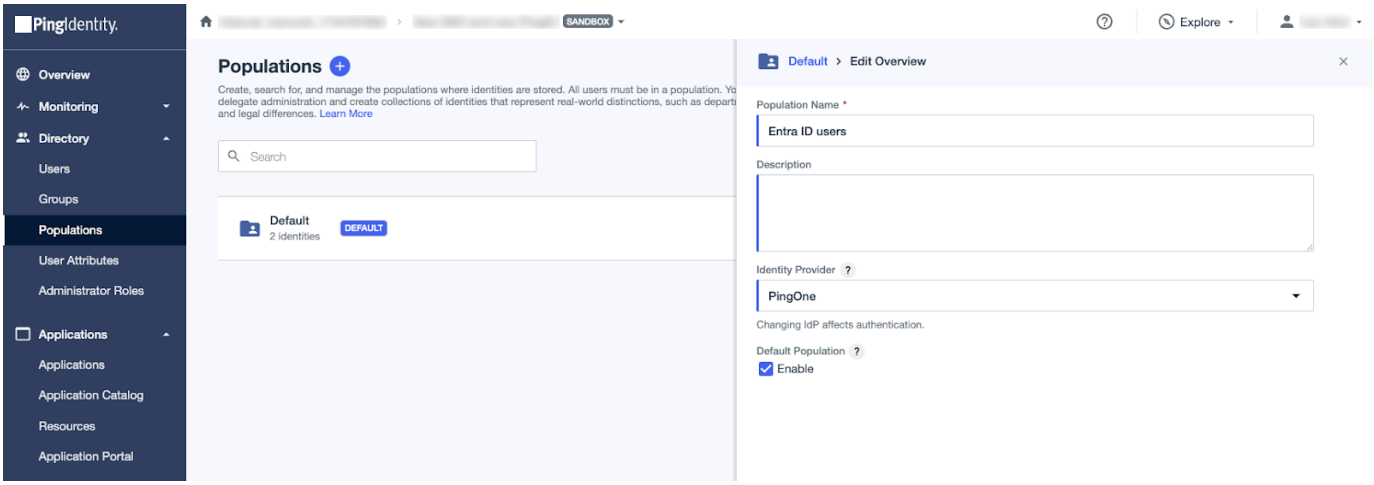


Because you could have a future scenario where users in this environment aren't coming from Microsoft Entra ID, you should rename the **Default** population, create a new population for users coming from Entra ID, and set the new population as the default population.

Steps

1. In the PingOne admin console, go to **Directory** > **Populations**.
2. Click the **Default** population, and then click the **Pencil** icon to edit the population.
3. Change **Population Name** from **Default** to a new name, such as `Entra ID users`.

Copyright © 2025 Ping Identity Corporation



4. Click **Save**.

5. To create a new population, click the **+** icon.

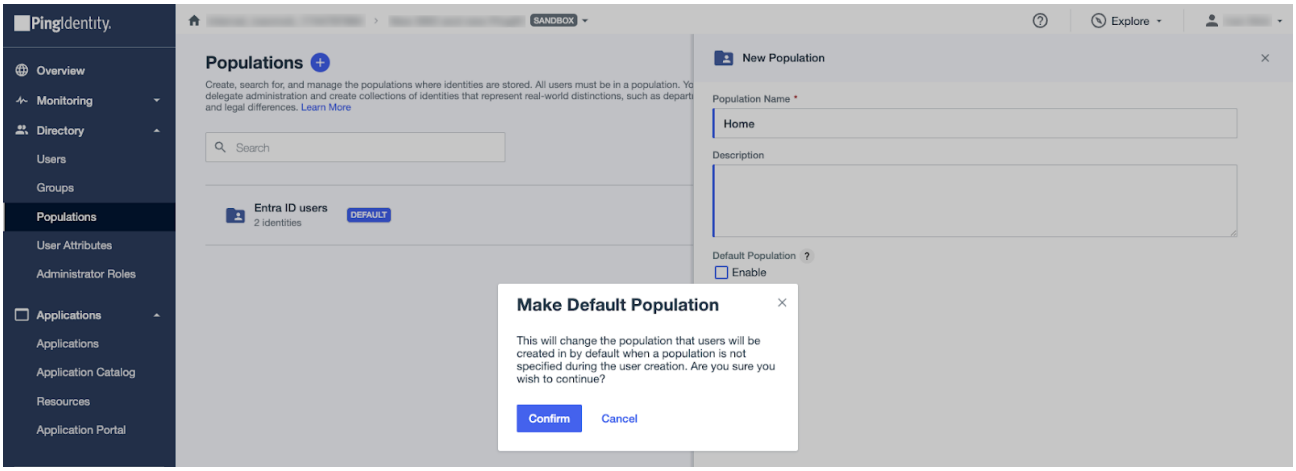
6. Enter the following:

    1. **Population Name**: A unique label for the population, such as `Home`.

    2. **Description** (optional): A brief description of the population.

    3. **Default Population**: Select the **Enable** checkbox to set this population as the new default population.

    4. In the confirmation modal, click **Confirm** to make this population the new default population.



7. Click **Save**.

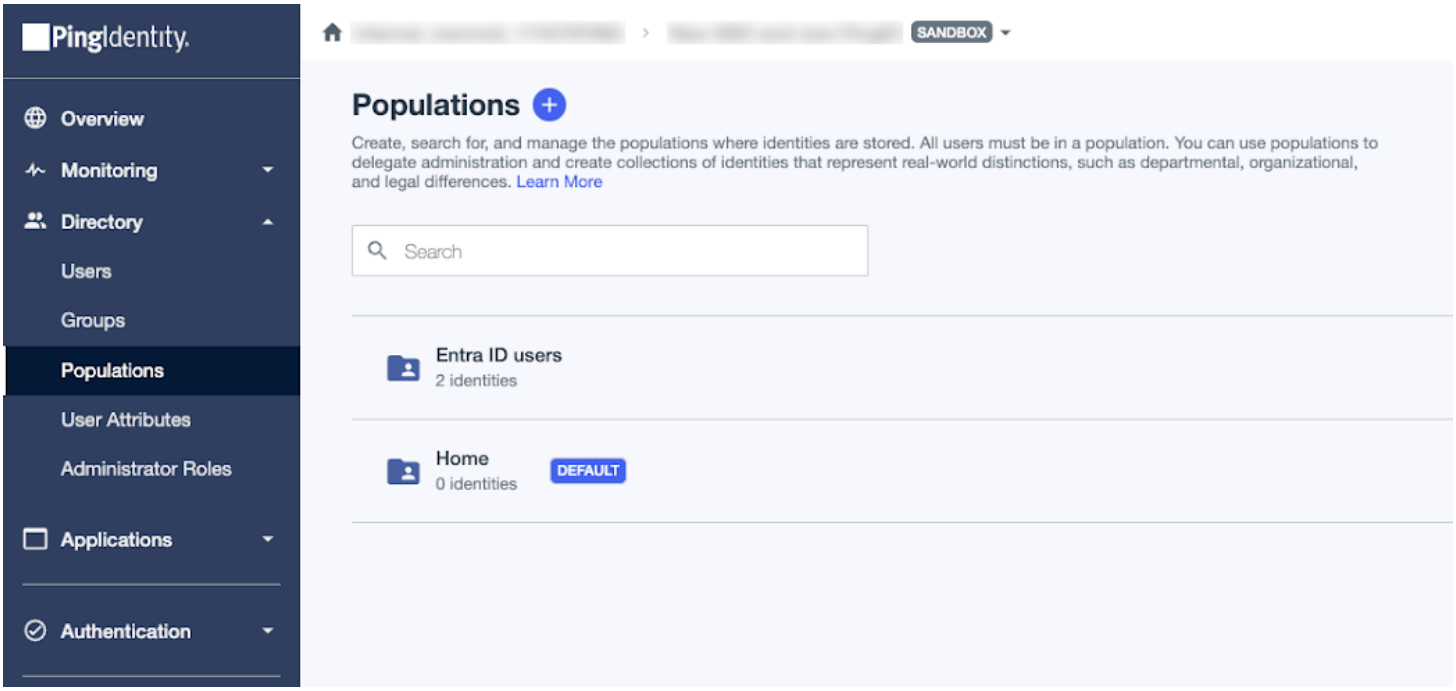
Result

You now have two populations in your environment:

1. **Entra ID users**: Users from PingID are assigned to this population. This is also the population where future Entra ID users will be assigned when Entra ID redirects users to PingOne for MFA. This population was previously named **Default** and was previously set as the default population.

2. **Home**: This population is the new default population and was created for future scenarios where users aren't coming from Entra ID.

Copyright © 2025 Ping Identity Corporation



Registering your application with Microsoft

To configure an EAM, register an application in Microsoft Entra. Learn more in Quickstart to registering an app in the Microsoft Entra documentation.

Before you begin

Ensure that you have:

- A Microsoft Entra account with an active subscription
- An Entra tenant

Steps

1. Go to the Microsoft Entra admin center and sign on to your account.

   If you don't have a Microsoft Entra account, you can create one now.

2. On the left, expand **Identity > Applications**.
3. Click **App registrations**.
4. At the top, click **New registration**.
5. In the **Name** field, enter a user-facing display name for the application.
6. For **Supported account types**, select **Accounts in this organizational directory only (Ping Identity only - Single tenant)** or **Accounts in any organizational directory and personal Microsoft accounts**, depending on the needs of your organization.

   Select the **Single tenant** option if you're working with only identities from your environment.

7. Under **Redirect URI**, select **Web** as the platform and enter the authorization URL of your PingOne environment.

Copyright © 2025 Ping Identity Corporation

> **Tip**
>
> You can find this URL on the **Overview** tab of any OIDC application in the PingOne admin console in the **Connection Details** section.

The format is `<issuer>/authorize`.

Example 1: `https://auth.pingone.<region>/<envID>/as/authorize`

Example 2: `https://<customDomain>/as/authorize` if you set up a custom domain. Learn more in Setting up a custom domain.

8. Click **Register**.

Enabling the implicit grant

After registering an application in Entra, enable the implicit grant type for your application to support an EAM.

Steps

1. Go to the Microsoft Entra admin center.
2. In the **App registrations** section, select your application.
3. Go to **Manage** > **Authentication**.
4. In the **Implicit grant and hybrid flows** section, select the **ID tokens** checkbox.
5. Click **Save**.

Getting the client ID and client secret for your application and the tenant ID of your Entra tenant

When you register your application with Microsoft, Microsoft generates an application (client) ID and application secret for the application.

Microsoft also generates a directory (tenant) ID for each Microsoft Entra tenant. You'll copy these values and enter them into PingOne.

Steps

1. Go to the Microsoft Entra admin center.
2. In the **App registrations** section, select your application.
3. On the left, click **Certificates & secrets**.
4. In the **Client secrets** section, click **+ New client secret**.
5. Enter the following:
    1. **Description**: A brief description of the client secret.
    2. **Expires**: Select the duration of the certificate, based on the needs of your organization.
6. Click **Add**.
7. In the **Client secrets** section, locate the value for the applicable secret and copy it to a secure location.

Copyright © 2025 Ping Identity Corporation

8. On the left, click **Overview**.
9. Locate the **Application (client) ID** and copy it to a secure location.
10. Locate the **Directory (tenant) ID** and copy it to a secure location.

Setting up API permissions

Using an EAM with Microsoft Entra requires certain API permissions that you'll need to enable in your application.

Steps

1. Go to the Microsoft Entra admin center.
2. In the **App registrations** section, select your application.
3. On the left, click **API permissions**.
4. Click **+ Add a permission**.
5. Click **Microsoft Graph**.
6. Click **Delegated permissions** and expand **Openid permissions**.
7. Select the `openid` and `profile` permissions.

> **Note**
>
> `User.Read` is included by default and should remain selected.

8. Click **Application permissions**, expand **User**, and select the `User.Read.All` permission.

> **Note**
>
> If you don't intend to retrieve many attributes from Microsoft Entra ID and populate them into PingOne, you can select the `User.ReadBasic.All` permission instead of the `User.Read.All` permission.
> Both of these permissions require admin consent.

9. To grant admin consent, click **Add permissions**.
10. Click **Grant admin consent for <your Entra tenant>**.

Adding Microsoft as an identity provider in PingOne

Configure the IdP connection in PingOne.

Steps

1. In the PingOne admin console, go to **Integrations > External IdPs**.
2. Click **+**.
3. Click **Microsoft**.
4. Click **Next**.

Copyright © 2025 Ping Identity Corporation

5. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.

     > **Note**
     > You can't change the **Icon** and **Sign-on button**, in accordance with the provider's brand standards.

6. Click **Next**.
7. On the **Configure IDP Connection** page, enter the following information:
   - **Client ID**: The application ID from the IdP that you copied earlier. You can find this information on the Microsoft Entra admin center.
   - **Client secret**: The application secret from the IdP that you copied earlier. You can find this information on the Microsoft Entra admin center.
   - **Callback URL**: Copy the **Callback URL** to a secure location. You'll provide this value to the IdP later.
   - **Tenant ID**: The tenant ID of your Entra tenant that you copied earlier. You can find this information on the Microsoft Entra admin center.
8. Click **Next**.
9. Define how the PingOne user attributes are mapped to IdP attributes. Learn more in Mapping attributes.
   - Leave the default PingOne user profile attributes and the external IdP attributes:
     - **Preferred Username** (from Microsoft) as the source of the PingOne **Username**
     - **Email** (from Microsoft) as the source of the PingOne **Email Address**
   - To add an attribute, click **+ Add**.
   - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
   - Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
     - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
     - **Always**: Always update the PingOne directory attribute.
10. Click **Save**.
11. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

    > **Note**
    > You can disable the IdP by clicking the toggle to the left (gray).

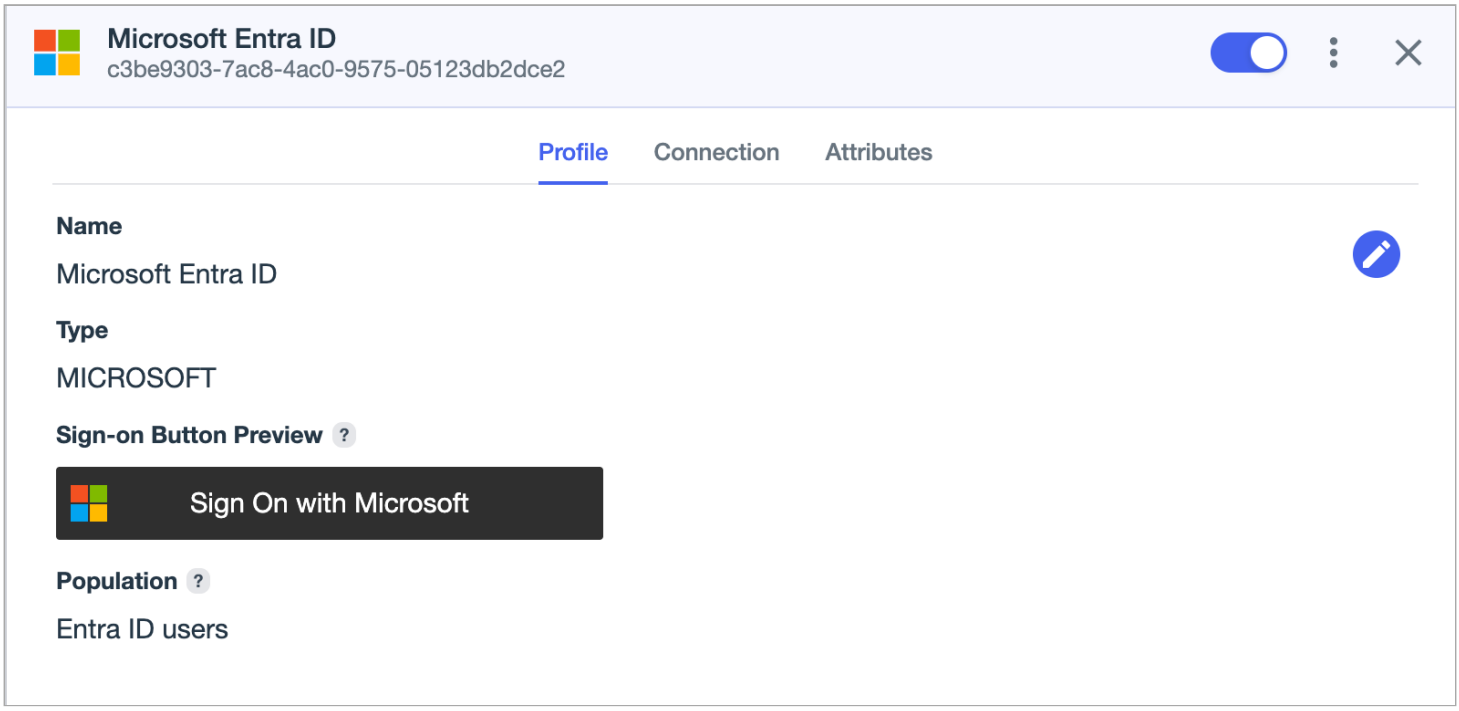
Copyright © 2025 Ping Identity Corporation

12. Click the connection in the **External IdPs** list to expand the connection details.
13. On the **Profile** tab, click the **Pencil** icon.
14. For **Population**, select the population that you previously created for Entra ID users.

> **Note**
>
> - If you created a new PingID environment in PingOne, use the population that you created in New PingID accounts: Creating a population for Microsoft Entra ID users.
> - If you integrated your PingID account with a new PingOne account, use the population that you created in Existing PingID accounts: Creating a population for Microsoft Entra ID users and changing the default population.

15. Click **Save**.
16. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
>
> You can disable the IdP by clicking the toggle to the left (gray).



Updating the population

After creating your connection to Microsoft, update the **Identity Provider** setting for the population that you created for users coming from Entra ID.

The **Identity Provider** setting is used as the runtime fallback IdP for users in the population who don't have an authoritative IdP configured in their user profile. Updating the population is especially important if you integrated your PingID account with a new PingOne account because those user profiles are created in PingOne without an authoritative IdP set. If the user is removed from the population, the IdP set in the population no longer applies to them.

Copyright © 2025 Ping Identity Corporation

Steps

1. In the PingOne admin console, go to **Directory > Populations**.
2. Click the population that you previously created for Entra ID users.
3. Click the **Pencil** icon.
4. In the **Identity Provider** list, select the IdP that you previously created in Adding Microsoft as an identity provider in PingOne.
5. Click **Confirm** in the modal, and then click **Save**.

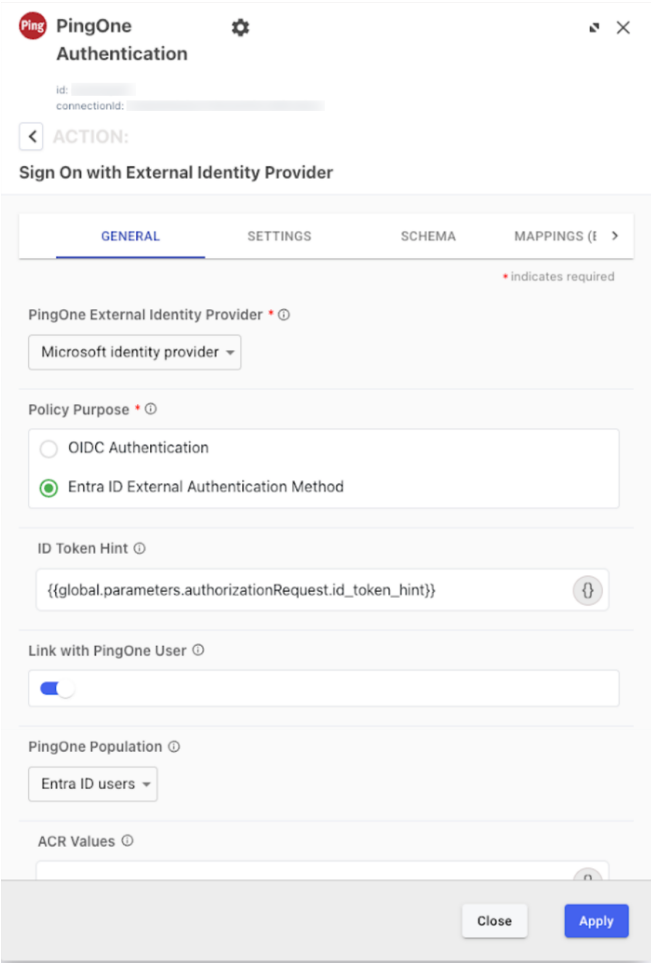
Adding a DaVinci flow and flow policy for Entra ID external authentication

Download and configure the DaVinci Entra ID EAM sample flow to handle external authentication requests from Entra ID.

Steps

1. Download the Entra ID EAM & OIDC Authentication Reference Flow from the Ping Library and extract the contents of the `.zip` archive to a folder on your computer.
2. In DaVinci, go to the **Flows** tab.
3. Click **+ Add Flow** and select **Import Flow**.
4. Upload the `entra-id-external-authentication-reference-flow.json` file from the sample flow `.zip` file and click **Import**.
5. Configure the **Entra ID external authentication method (EAM) - Sign On with External Identity Provider** node:
    1. Click the node to open the configuration settings.
    2. On the **General** tab, in the **PingOne External Identity Provider** list, select the Microsoft IdP you created in Adding Microsoft as an identity provider in PingOne.
    3. Make sure the following default configurations are set:
        - **Policy Purpose** is set to **Entra ID External Authentication Method**.
        - **ID Token Hint** is set to `{{global.parameters.authorizationRequest.id_token_hint}}`.
        - The **Link with PingOne User** toggle is enabled (blue).
    4. In the **PingOne Population** list, select the applicable population.
        - For new PingID accounts, learn more in New PingID accounts: Creating a population for Microsoft Entra ID users.
        - For existing PingID accounts, learn more in Existing PingID accounts: Creating a population for Microsoft Entra ID users and changing the default population.

Copyright © 2025 Ping Identity Corporation



5. Click **Apply**.

6. Review the default configuration settings for the **Mint Tokens - Return Success Response** node:

   1. Click the node to open the settings.

   2. On the **General** tab, make sure **User ID** is mapped to `id` from the **Entra ID external authentication method (EAM) - Sign On with External Identity Provider** node.

   3. Make sure **Custom Authentication Methods** is mapped to `entraIdAmr` from the **Map PingID AMR Value - Custom Function** node.

   4. Click **Apply**.

7. Add a DaVinci flow policy for the sample flow:

   1. Go to the **Applications** tab and click **+ Add Application**.

   2. In the **Name** field, enter a name for the application and click **Create**.

   3. To edit the application, select the application in the **Applications** list.

   4. On the **Flow Policy** tab, click **+ Add Flow Policy**.

   5. In the **Policy Name** field, enter a name for the flow policy.

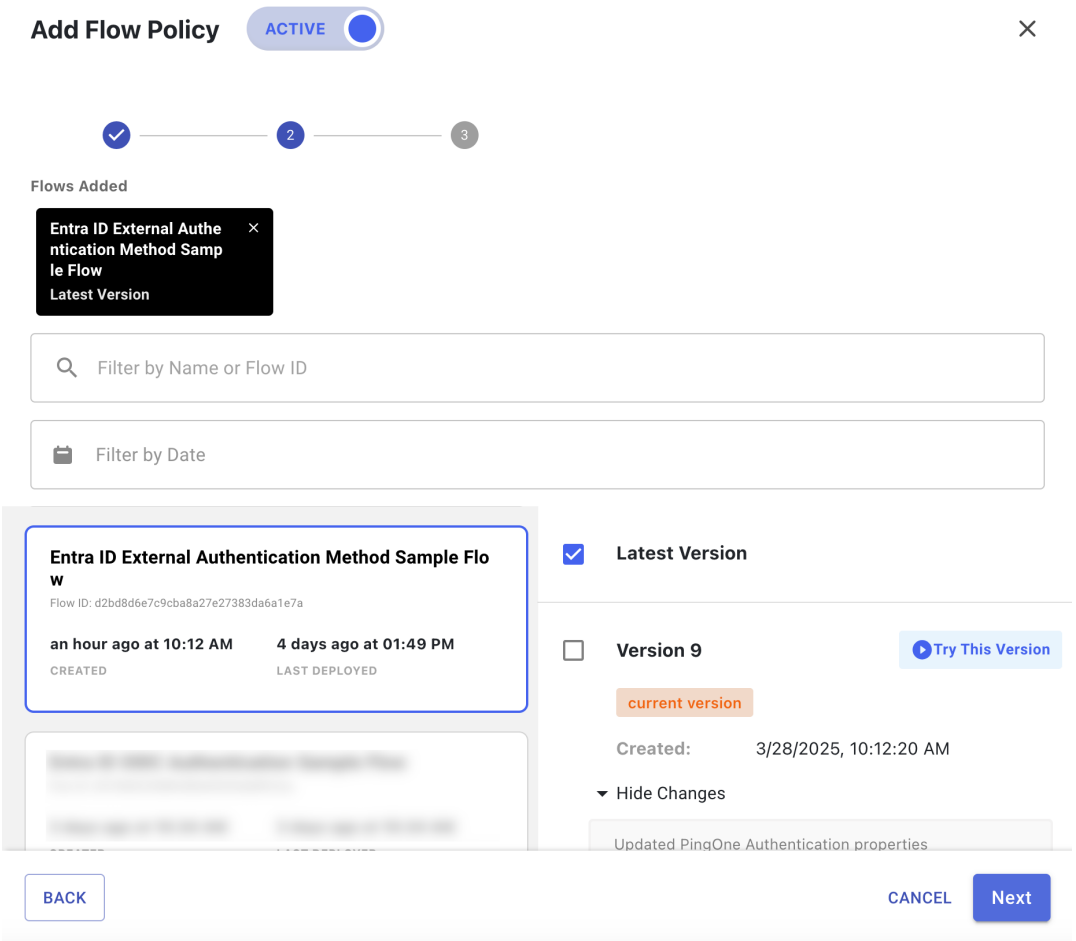
Copyright © 2025 Ping Identity Corporation

6. Select **PingOne Flow Policy** to enable flows in the policy to be launched directly through PingOne.

> **Note**
>
> This option can't be changed after the flow policy is created. PingOne flow policies can only include flows and flow versions that have the **PingOne Flow** setting enabled. Learn more in Configuring a flow policy.

7. Click **Next**.

8. In the flow list, click **Entra ID External Authentication Method Sample Flow** and select one or more versions of the flow to use.



9. Click **Next**.

10. (Optional) Add weight distribution and analytics information for each flow and flow version. Learn more in Configuring a flow policy.

11. Click **Create Flow Policy**.

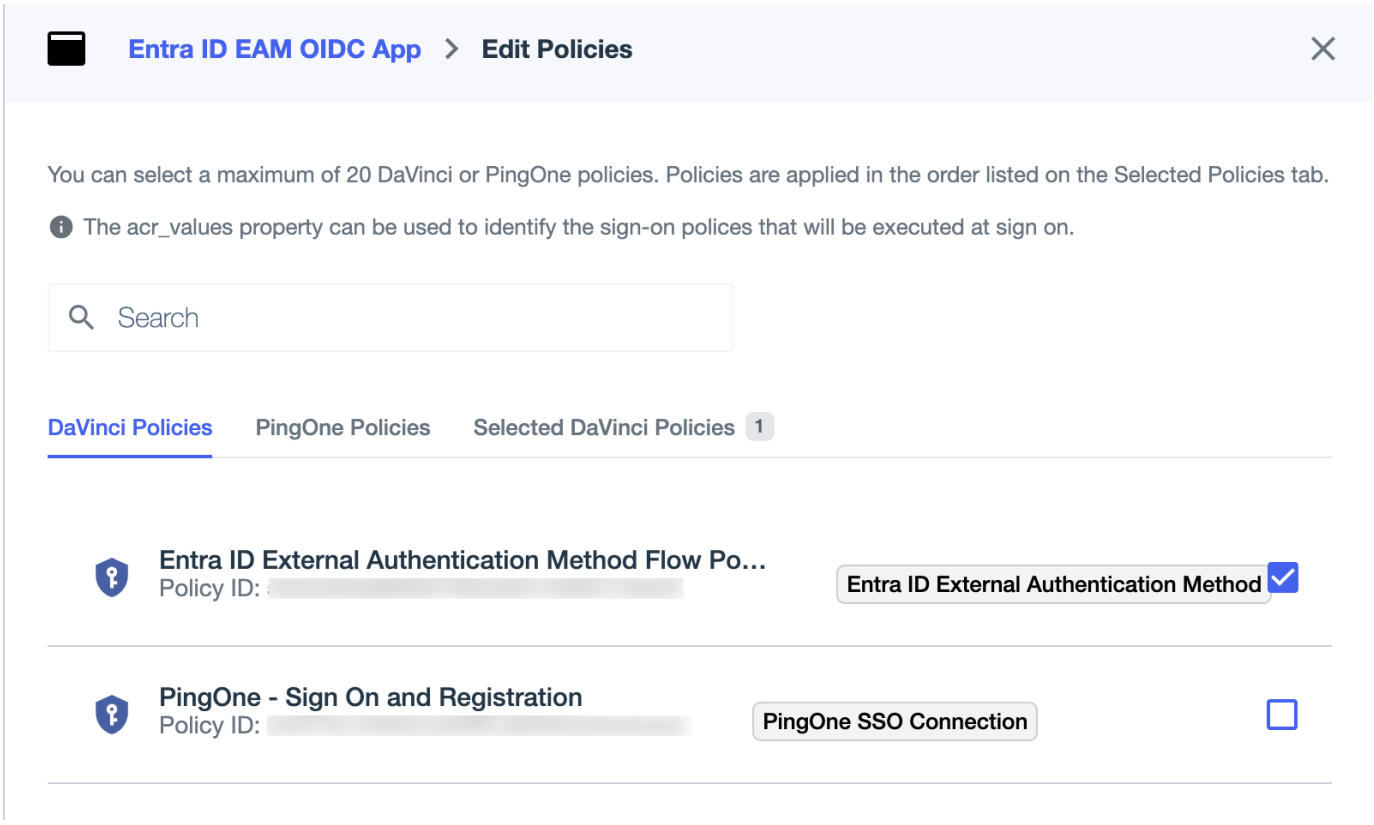
Configuring the OIDC application

Configure an OIDC application to handle authentication requests from Microsoft Entra ID.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications**.
2. Click **+** to add an application.
3. Enter the following:
    1. **Application name**: A unique identifier for the application.
    2. **Description** (optional): A brief description of the application.
    3. **Icon** (optional): A graphic representation of the application. Use a file up to 1 MB in JPG, JPEG, GIF, or PNG format.
4. For **Application Type**, select **OIDC Web App**.
5. Click **Save**.
6. On the **Configuration** tab, click the **Pencil** icon, and enter or edit the following:
    1. For **Response Type**, clear the default **Code** checkbox and select **ID Token**.
    2. For **Grant Type**, clear the default **Authorization Code** checkbox and select **Implicit**.
    3. For **Redirect URIs**, enter `https://login.microsoftonline.com/common/federation/externalauthprovider`.
    4. Click **Save**.
7. On the **Policies** tab, click **+ Add Policies**.
8. On the **DaVinci Policies** tab, select the DaVinci flow policy that you created to handle external authentication requests from Entra ID.

Copyright © 2025 Ping Identity Corporation



9. Click **Save**.
10. To enable the application, click the toggle at the top of the details panel to the right (blue).

> **Note**
>
> You can disable the application by clicking the toggle to the left (gray).

11. Click the application entry to open the details panel.
12. On the **Overview** tab, copy the following PingOne application details to add in the Microsoft Entra admin center:
    - In the **General** section, copy the **Client ID** to a secure location.
    - In the **Connection Details** section, copy the **OIDC Discovery Endpoint** to a secure location.

Creating an external authentication method in Microsoft Entra

After creating the OIDC application in PingOne and copying the application ID, OIDC discovery endpoint, and client ID, create an EAM in Microsoft Entra.

Steps

1. Go to the Microsoft Entra admin center.
2. On the left, go to **Protection** > **Authentication methods**.
3. Click **Add external method**.

4. Enter the following:
    1. **Name**: Enter a name for the EAM.
    2. **Client ID**: Enter your PingOne application's client ID that you copied earlier.
    3. **Discovery Endpoint**: Enter the **OIDC Discovery Endpoint** that you copied earlier. The format is `<issuer>/.well-known/openid-configuration`.
    4. **App ID**: Enter the ID of the Microsoft Entra application that you copied previously. You can find the application ID in the Microsoft Entra admin center.
5. Click **Request permission**.

   The browser opens a new window for you to sign on with your Microsoft Entra admin credentials.
6. Review the requested permissions and click **Accept** if you agree.
7. In the **Enable and target** section, configure whether you want to include a subset of your users or all users.
8. Click the **Enable** toggle to enable the EAM.

Creating a conditional access policy in Microsoft Entra

Configure a conditional access policy in Microsoft Entra to define authentication requirements for users accessing applications.

> **Note**
>
> If your Microsoft Entra tenant contains other conditional access policies that use custom controls to initiate MFA, ensure those policies don't apply to the same users, groups, and applications that you select in this conditional access policy. Otherwise, your users could be prompted multiple times for MFA.

Steps

1. Go to the Microsoft Entra admin center.
2. On the left, go to **Protection** > **Conditional Access**.
3. Click **Policies**.
4. Update an existing policy or create a new policy.
5. Configure the following:
    1. **Name**: Enter a name.
    2. **Users**: Select the same users and groups that you selected in your EAM.
    3. **Target resources**: Select the applications to which you want to apply this conditional access policy.
    4. **Grant**:
        1. Click **Grant access**.
        2. Select the **Require multifactor authentication** checkbox.
        3. Click **Select**.

Copyright © 2025 Ping Identity Corporation

5. **Enable policy**: Select **On** to turn on the policy.

6. Click **Save**.

Configuring PingID as the external authentication method

Configure a PingID policy to process user MFA requests coming from the PingOne application that you created to handle Microsoft Entra requests.

Steps

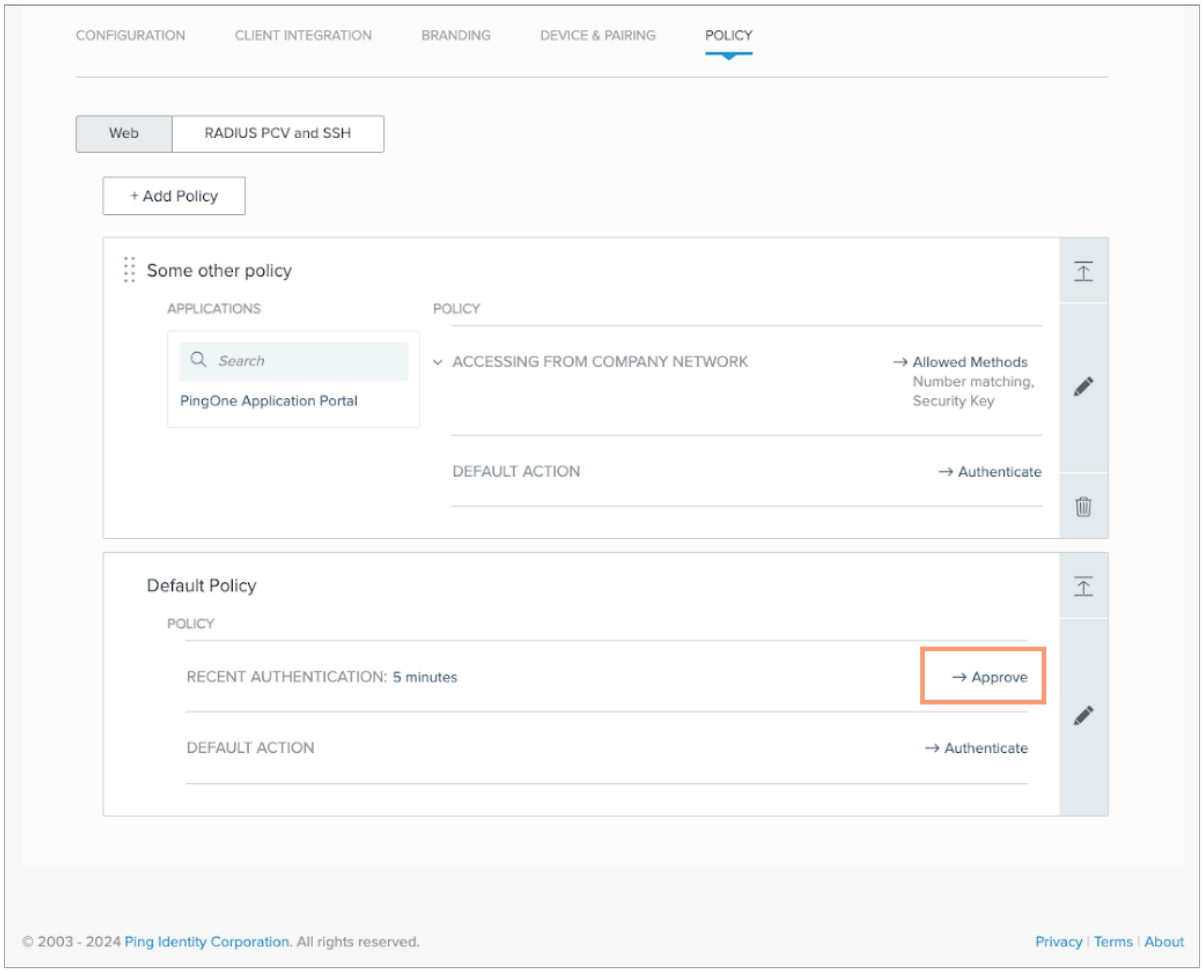
1. In the PingID admin portal, go to **Setup** > **PingID** and click the **Configuration** tab.

> **Note**
>
> If you selected **Enable** for **Enforce Policy**, you might need to create an additional PingID policy. Learn more in the next step.

2. Click the **Policy** tab, and on the **Web** tab, expand and review each policy.

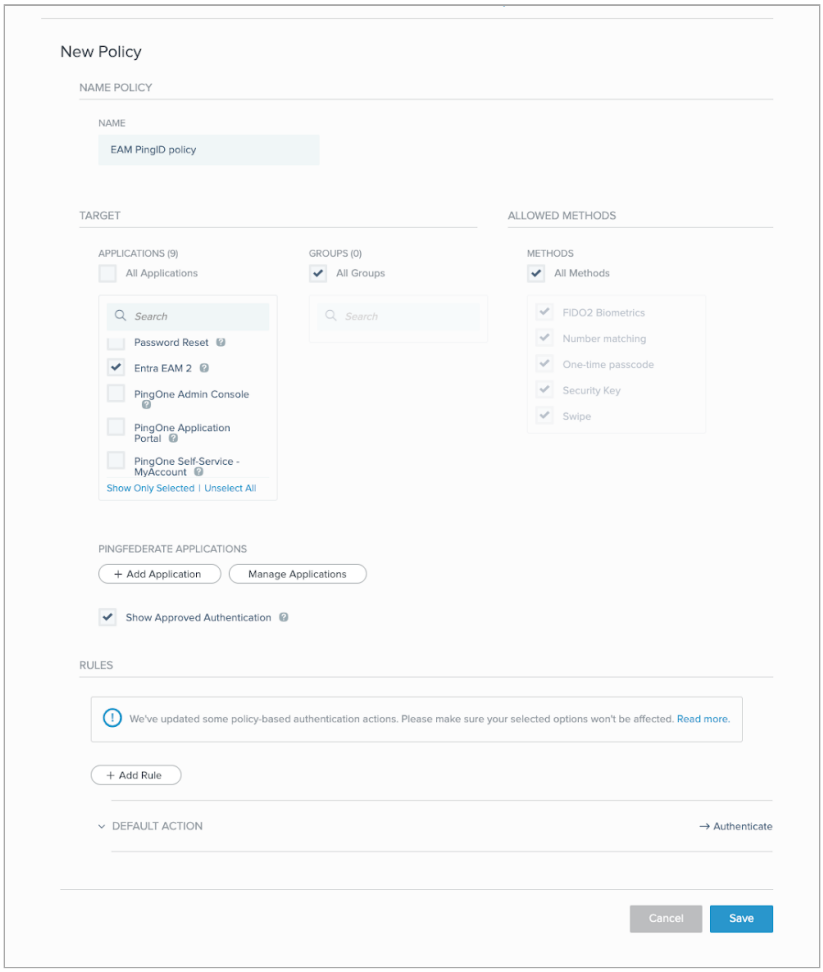
> **Note**
>
> Microsoft Entra ID doesn't allow MFA bypasses from an EAM and requires always prompting the user to complete MFA. If you have a policy that can apply to all applications and that has a rule with an action of **Approve**, you must create a new policy for the PingOne application. Examples of such policies include Recent Authentication or Accessing from Company Network.

Copyright © 2025 Ping Identity Corporation



1. To add a new policy, click **Add Policy**.
2. Enter a name for the policy, such as `EAM PingID policy`.
3. In the **Target** section, in the **Applications** list, select the PingOne application that you previously created.
4. For **Groups**, select all applicable groups.
5. (Optional) In the **Allowed Methods** section, select the authentication methods you want to allow.
6. Click **Save**.

Copyright © 2025 Ping Identity Corporation



Result:

The new policy becomes the first PingID policy, which works as a Microsoft Entra ID EAM. PingID will use this new policy when processing MFA requests coming from the PingOne application that you created to handle Microsoft Entra ID requests.

3. In a scenario where a user forgot or lost their mobile phone and can't use the PingID app for MFA, you can allow a user to bypass MFA with PingID for a specificed period of time, such as 8 hours.

    1. In the PingOne admin console, go to **Directory > Users**.
    2. Browse or search for the applicable user, and click the user entry to open the details panel.
    3. In the list for the **Services** tab, select **Authentication**.
    4. Scroll down to the **Integrations** section, click the **More Options** icon, and select **Bypass**.
    5. In the **Bypass** window, select the desired amount of time from the **Allow bypass of PingID authentication on SSO for** list and click **Bypass**.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Because Microsoft Entra ID requires the third-party MFA provider to specify the MFA method used and doesn't accept MFA bypasses as an acceptable MFA method, you must also configure bypass in the Microsoft Entra admin center. Learn more about configuring conditional access in the Microsoft Entra documentation.

Adding a DaVinci flow and flow policy for OIDC authentication

If you want to allow users to sign on to the **PingOne Self-Service - MyAccount** application to manage their MFA methods or to other applications you've added to PingOne, you must create a DaVinci flow and flow policy for OIDC authentication using the same Microsoft IdP connection.

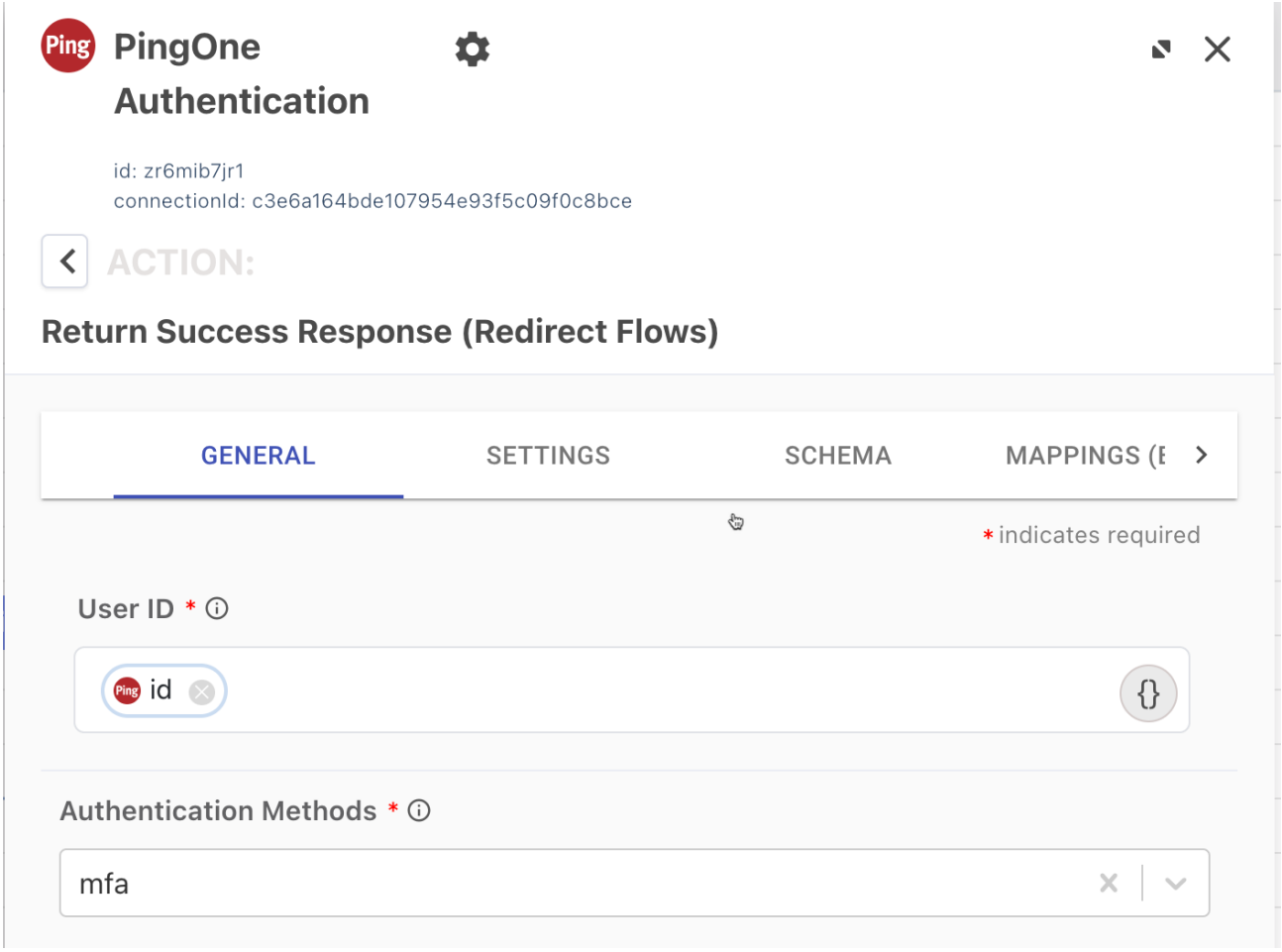
Before you begin

Make sure you've downloaded the Entra ID EAM & OIDC Authentication Reference Flow from the Ping Library and extracted the contents of the `.zip` archive to a folder on your computer. Learn more in Adding a DaVinci flow and flow policy for Entra ID external authentication.

Steps

1. In DaVinci, go to the **Flows** tab.
2. Click **+ Add Flow** and select **Import Flow**.
3. Upload the `entra-id-oidc-authentication-flow.json` file from the sample flow `.zip` archive and click **Import**.
4. Configure the **Entra ID OIDC authentication - Sign On with External Identity Provider** node:
    1. Click the node to open the configuration settings.
    2. In the **PingOne External Identity Provider** list, select the same Microsoft IdP you used in the **Entra ID External Authentication Method Sample Flow**.
    3. Make sure **Policy Purpose** is set to **OIDC Authentication**.
    4. Make sure the **Link with PingOne User** toggle is enabled (blue).
    5. In the **PingOne Population** list, select the same population you used in the Entra ID External Authentication Method Sample Flow.
    6. Click **Apply**.
5. Review the default configuration settings for the **Mint Tokens - Return Success Response** node:
    1. Click the node to open the configuration settings.
    2. On the **General** tab, make sure **User ID** is mapped to `id` from the **Entra ID OIDC authentication - Sign On with External Identity Provider** node.
    3. In the **Authentication Methods** list, make sure **mfa** is selected.

Copyright © 2025 Ping Identity Corporation



4. Click **Apply**.

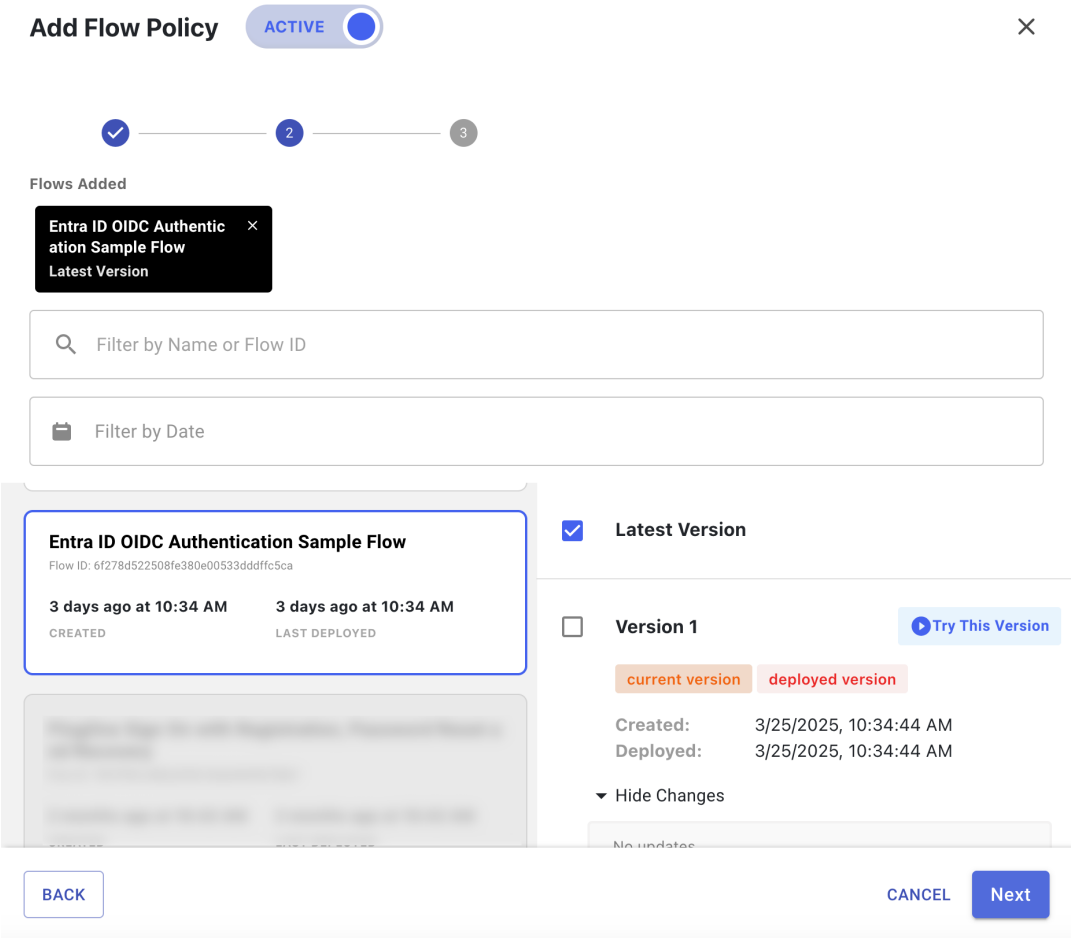
6. Add a DaVinci flow policy for the sample flow:

   1. Go to the **Applications** tab and click **+ Add Application**.
   2. In the **Name** field, enter a name for the application and click **Create**.
   3. To edit the application, select the application in the **Applications** list.
   4. On the **Flow Policy** tab, click **+ Add Flow Policy**.
   5. In the **Policy Name** field, enter a name for the flow policy.
   6. Select **PingOne Flow Policy** to enable flows in the policy to be launched directly through PingOne.

   > **Note**
   >
   > This option can't be changed after the flow policy is created. PingOne flow policies can only include flows and flow versions that have the **PingOne Flow** setting enabled. Learn more in Configuring a flow policy.

   7. Click **Next**.
   8. In the flow list, click **Entra ID OIDC Authentication Sample Flow** and select one or more versions of the flow to use.

Copyright © 2025 Ping Identity Corporation



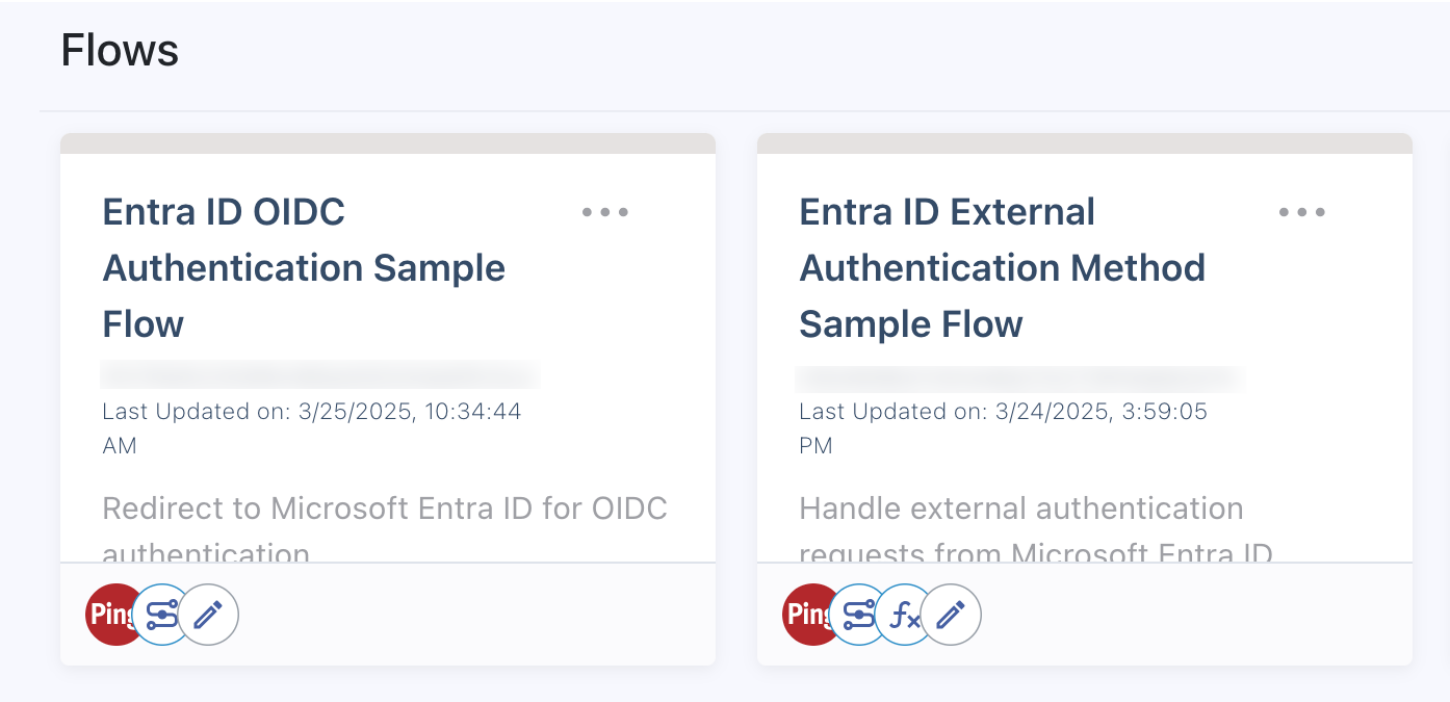
9. Click **Next**.
10. (Optional) Add weight distribution and analytics information for each flow and flow version. Learn more in Configuring a flow policy.
11. Click **Create Flow Policy**.

Result:

You now have two DaVinci flows:

- A flow for users authenticating with PingOne as the EAM for Microsoft Entra
- A flow for OIDC authentication to allow users to sign on to other applications

Copyright © 2025 Ping Identity Corporation



Adding the callback URL to the Microsoft Entra admin center

If you created an authentication policy for OIDC authentication, you must also add the callback URL from the Microsoft IdP connection to the application you registered in the Microsoft Entra admin center.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and locate the Microsoft IdP that you created previously.
2. Click the IdP to open the details panel.
3. Click the **Connection** tab.
4. Copy the **Callback URL**.

   The following examples show the URL format:

   Example 1: `https://auth.pingone.<region>/<envID>/rp/callback/microsoft`

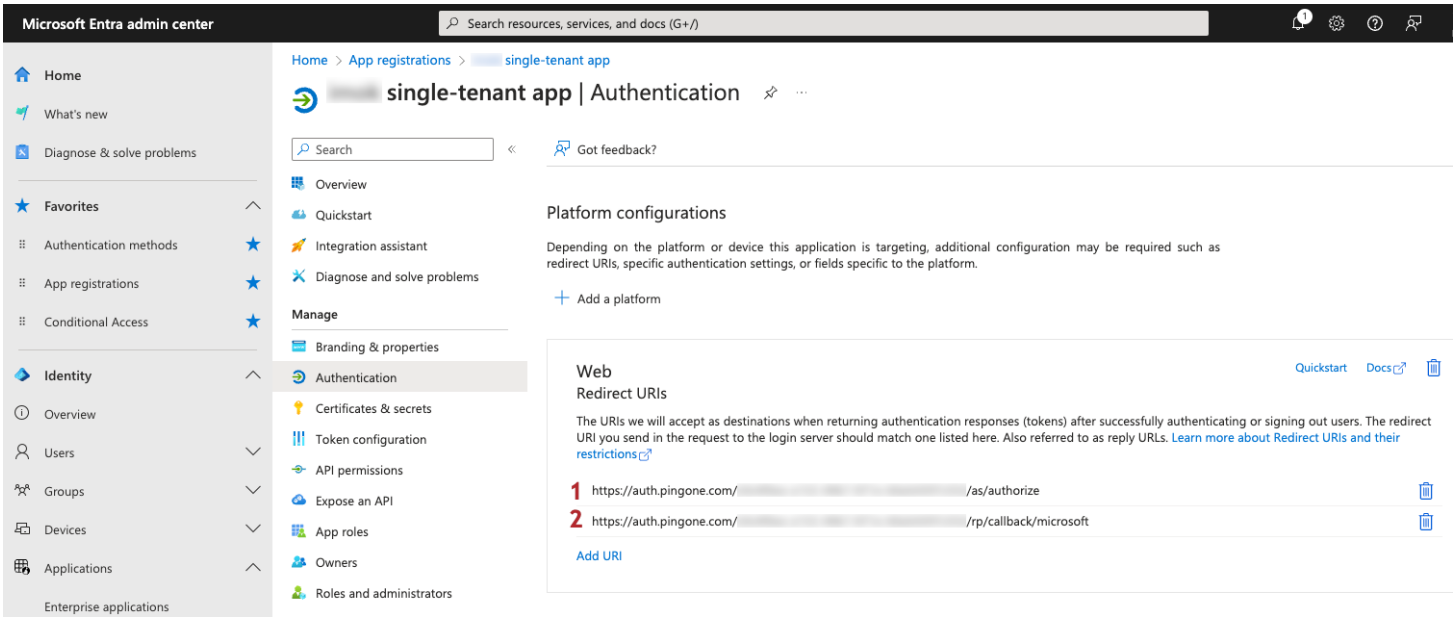
   Example 2: `https://<customDomain>/rp/callback/microsoft`
5. Go to the Microsoft Entra admin center.
6. In the **App registrations** section, select your application.
7. On the left, click **Authentication**.
8. Go to **Platform configurations** > **Web** > **Redirect URIs**, and click **Add URI**.
9. Paste the **Callback URL** that you copied from the PingOne admin console.
10. Click **Save**.

Result

Copyright © 2025 Ping Identity Corporation

The **Redirect URIs** section displays both URLs you've added:

1. Authorization URL
2. Callback URL



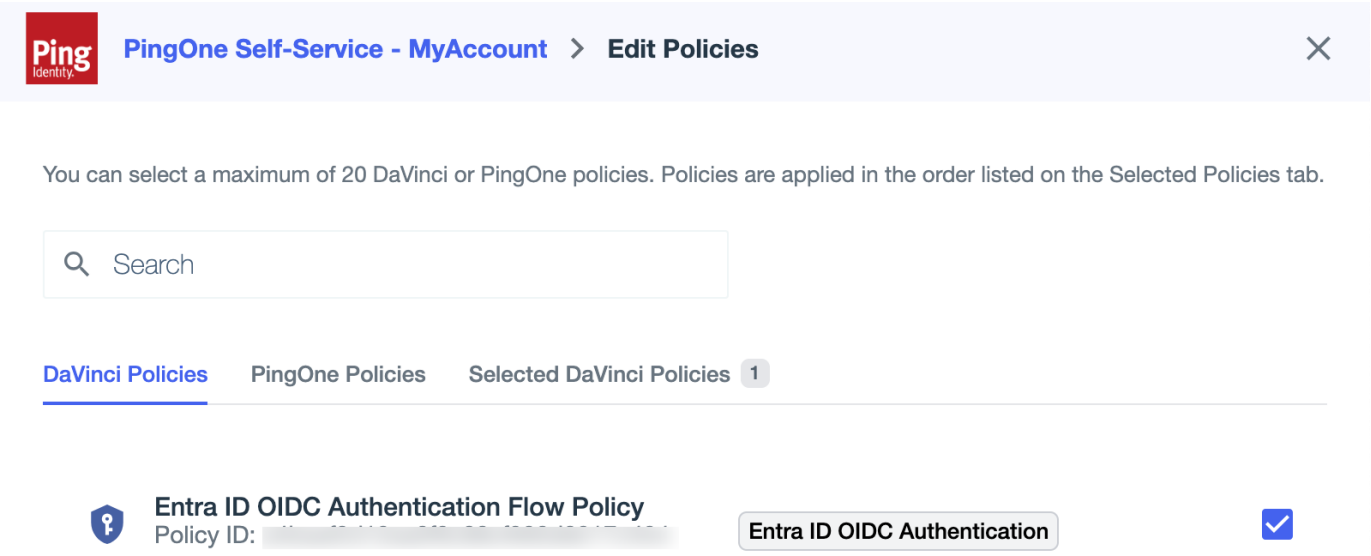
Assigning the DaVinci OIDC flow policy to an application in PingOne

After you create a DaVinci flow and flow policy for OIDC authentication and add the callback URL to the application in Microsoft Entra, assign the DaVinci OIDC flow policy to applicable applications in PingOne, such as the **PingOne Self-Service - MyAccount** application or other applications you've added.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications**.
2. Select the relevant application.
3. On the **Policies** tab, click **+ Add policies**.
4. On the **DaVinci Policies** tab, select the DaVinci OIDC flow policy that you created in Adding a DaVinci flow and flow policy for OIDC authentication.

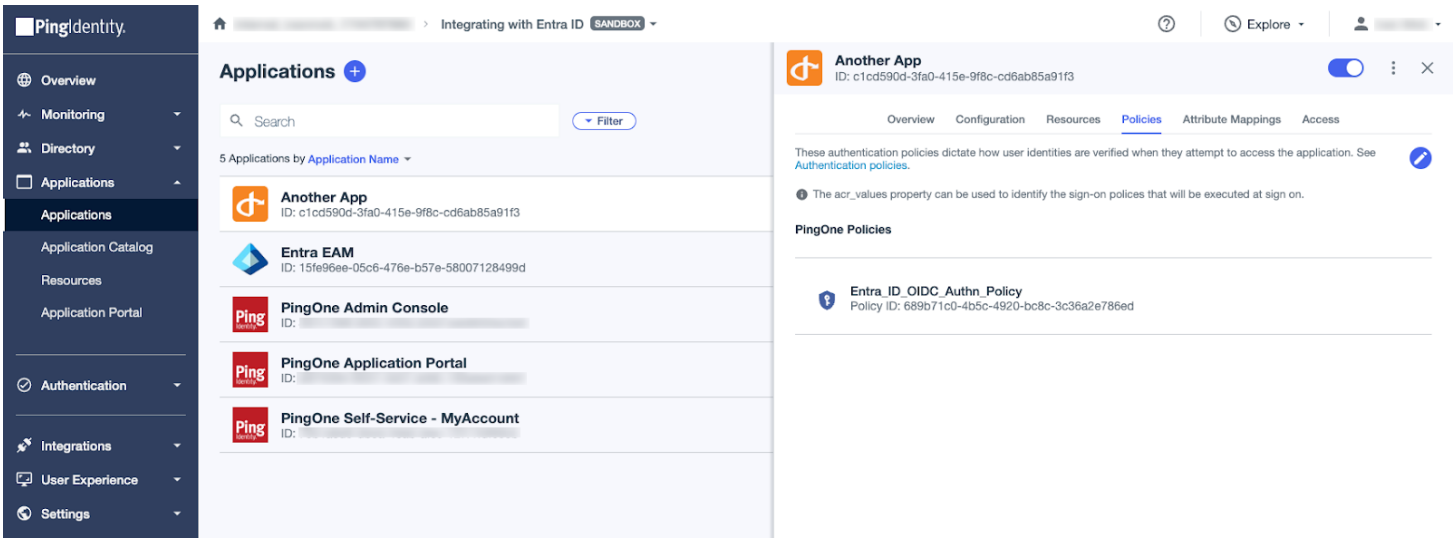
Copyright © 2025 Ping Identity Corporation



5. Click **Save**.

Next steps

Repeat these steps for any other applications to which you want users to be able to sign on, for example **Another App** in the following screenshot.



Validation

Now that you've set up an EAM in Microsoft Entra ID and configured PingOne and PingID as the external MFA provider, you're ready to validate that your Entra ID users can use PingID to complete MFA.

1. Open a new browser window in incognito mode.
2. In the Microsoft Entra admin center, locate the application you added to the conditional access policy that requires MFA and click the URL for the application.

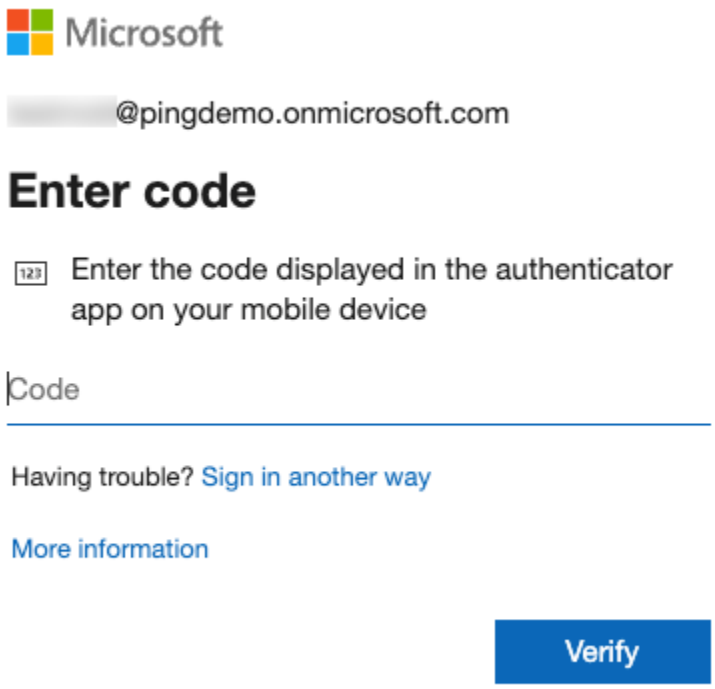
   In this example, **My Apps** at https://myapps.microsoft.com.

3. Sign on to the application and complete the first-factor authentication at Microsoft using a test user's credentials.

   Result:

   If you, as an Entra ID admin, have activated system-preferred MFA and included the test user as the target user, and if the test user has installed and successfully used the system-preferred MFA method, Entra ID prompts the user to complete MFA action based on what Entra thinks is the most secure method.

   In this example, the test user has installed and used both Microsoft Authenticator and verification code by text message, so Entra ID prompts the user to enter the code from Microsoft Authenticator.



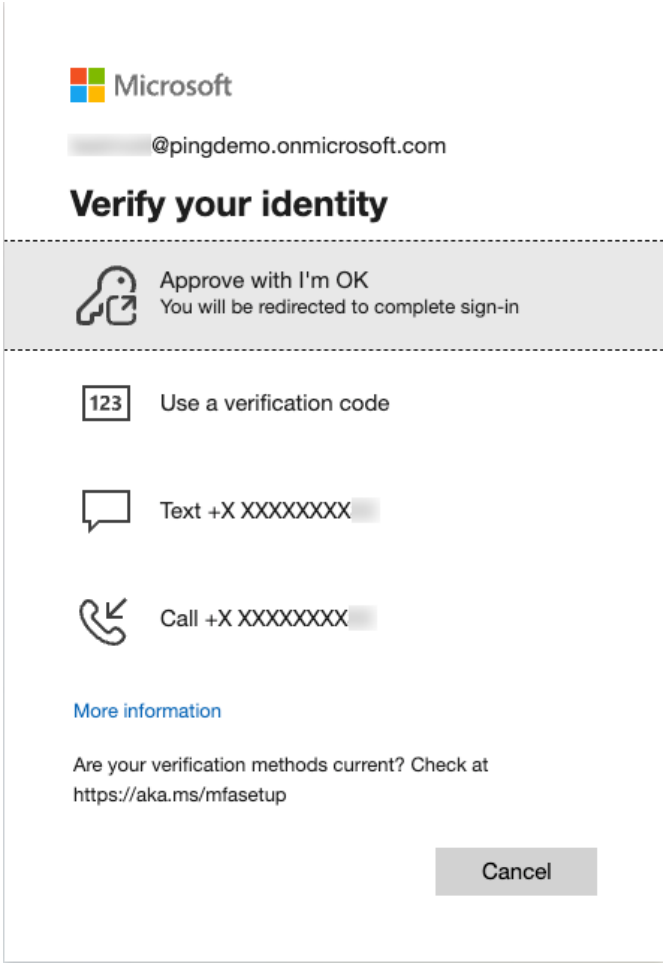
> **Note**
>
> If you haven't activated system-preferred MFA, the user won't see the **Enter code** page and is prompted to verify their identity.

4. To use your EAM, click **Sign in another way** at the bottom of the **Enter code** window.

   Result:

   After selecting **Sign in another way** or if system-preferred MFA doesn't apply, Entra ID displays the **Verify your identity** page.

Copyright © 2025 Ping Identity Corporation



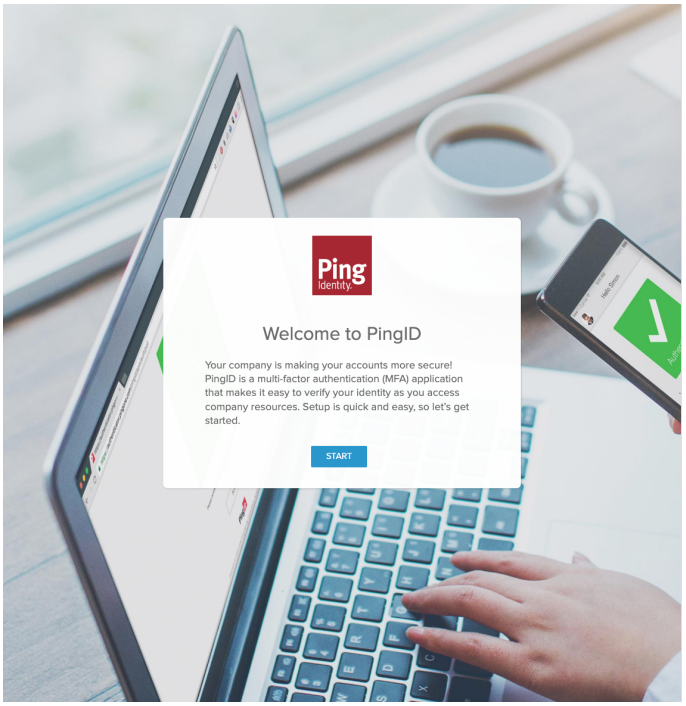
5. Select the EAM.

   Result:

   Entra ID redirects the browser to PingOne.

6. If the test user hasn't yet paired the PingID app, they're shown a **Welcome to PingID** page. Click **Start** to start the pairing process.

Copyright © 2025 Ping Identity Corporation



Result:

After pairing, the PingID app prompts the user to complete the MFA requirement.

7. After PingID is paired for the test user, complete the MFA prompt from the PingID app.

   Result:

   PingOne returns an ID token to Entra ID, and Entra ID processes the ID token and signs the test user on to the application.

8. Sign out of the application.

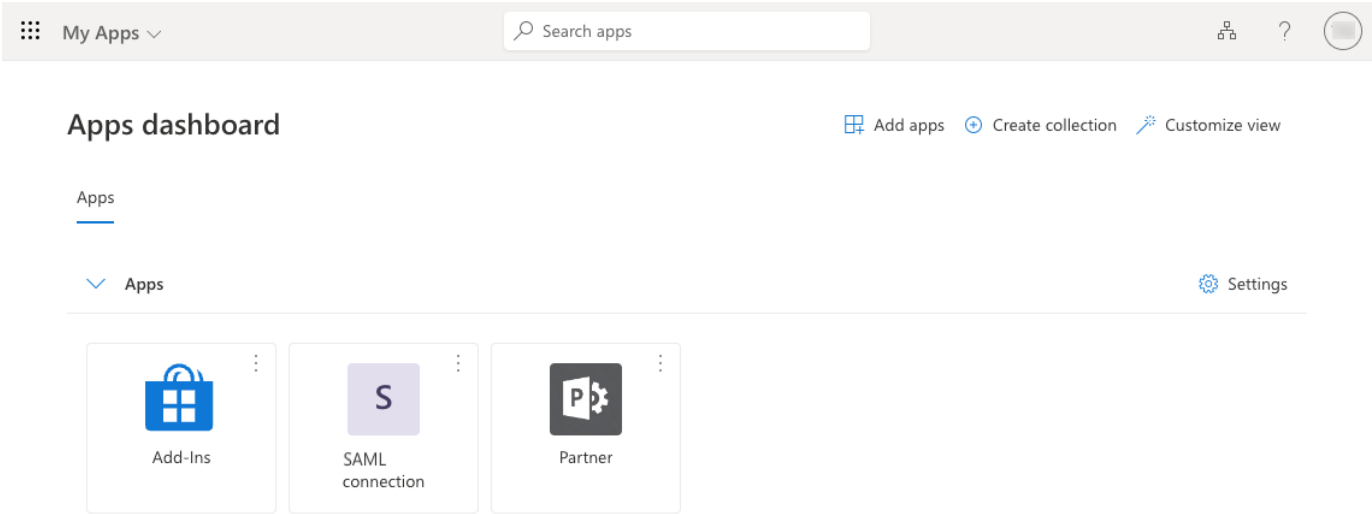
9. In the Microsoft Entra admin center, locate the same application and authenticate to the application again as the test user.

   Result:

   This time, PingID shouldn't prompt the test user to pair a device. Instead, the PingID app should prompt the test user to complete the MFA requirement.

   When the test user completes the MFA requirement, PingOne returns an ID token to Entra ID, and Entra ID processes the ID token and signs the test user on to the application.

Copyright © 2025 Ping Identity Corporation



Using PingGateway no-code application and API protection

PingGateway connects to PingOne as a single sign-on (SSO) provider. This integrates web applications, APIs, and microservices with PingOne without modifying the applications or the containers where they run.

PingGateway runs as reverse proxy gateway calling on PingOne for authentication and authorization. In deploying PingGateway, you protect APIs and applications as they are without changing them.

The PingGateway declarative configuration model gives you the flexibility to serve many use cases without the need to write or change code.

Learn more in the PingGateway documentation.

Copyright © 2025 Ping Identity Corporation

PingOne Expression Language

PingIdentity.

PingOne supports the Spring Expression Language (SpEL) version 5.1. SpEL is a powerful expression language used for querying and manipulating an object graph at runtime. Learn more in SpEL framework.

The PingOne expression language is an augmentation of SpEL. The PingOne expression language syntax is similar to Unified EL and offers additional features, such as method invocation, through the libraries described in this section.

Learn more about SpEL functionality in PingOne in:

- Using the expression builder
- Samples
- Expressions and concatenation
- Arrays and lists
- Maps and objects
- Operators
- Collection operations
- Disabled and restricted SpEL features
- Variables
- Custom library functions
- Null safe usage
- References

Using the expression builder

Use the expression builder to create expressions and test the results of those expressions. You can also use expressions to manipulate data, concatenate strings, and build arrays.

The expression builder uses the PingOne expression language to identify and access user attributes in the PingOne directory or other external applications or directories.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the application to which you want to add an attribute mapping.
2. Click the application entry to open the details panel.
3. On the **Attribute Mappings** tab, click the **Pencil** icon.
4. Click the **Gear** icon next to an attribute mapping to open the **Build and Test Expression** modal. Learn more in Mapping attributes.
    - Enter an expression that identifies the attribute you want to map.
    - To verify an expression and see sample data, click **Test Expression**.

Copyright © 2025 Ping Identity Corporation

- To toggle between expression values and JSON, click **Edit JSON** or **Edit Values**.
- For sample expressions and reference information, click **View Documentation**.

5. Click **Save**.
6. On the **Attribute Mappings** tab, click **Save**.

Samples

Use these sample expressions to build attribute mappings with the PingOne expression builder.

Sample user model

The examples in this section use the following model:

```
{
  "user": {
    "name": {
      "given": "John",
      "family": "Doe"
    },
    "role": "SA",
    "memberOfGroupNames": ["Admin", "User"],
    "groupDNs": [
      "CN=Devs,CN=Users,DC=malibu,DC=gl,DC=lab",
      "CN=Admins,CN=Users,DC=malibu,DC=gl,DC=lab"
    ]
  }
}
```

Literal expressions

Expression	Result
`'FirstName'`	`FirstName`
`"User"`	`User`
`1`	`1`
`true`	`true`

Copyright © 2025 Ping Identity Corporation

Expression	Result
`{'USER'}`	`['USER']`
`{'firstName': 'John'}`	`{ "firstName": "John" }`

String concatenation

Expression	Result
`'FirstName' + ', ' + 'LastName'`	`FirstName, LastName`
`user.name.given + ', ' + user.name.family`	`John, Doe`

Generate a user alias by concatenating parts of first and last name

Expression	Result
`#string.substring(user.name.given, 0, 1)` `#string.substring(user.name.family, 0, 4)`	`JDoe`

Extract the domain name from an email address

Expression	Result
`#regex.findAllMatches('user01@test.com', '(?⇐@)[^.]+')`	`[test]`

Output the date as a string in a certain format

Expression	Result
`#datetime.format('2021-01-01T10:15:00Z', 'EEEE, dd MMMM; h:mm a')`	`Friday, 01 January; 10:15 AM`

Copyright © 2025 Ping Identity Corporation

Replace a value based on a predefined set of options

Expression	Result
`user.name.given + ' ' + user.name.family + ', ' + \ {'PM': 'Product Manager', 'SA': 'Software Architect'} [user.role] ?: 'Unknown'`	`John Doe, Software Architect`

Change the contents of `memberOfGroupNames` *array to upper case*

Expression	Result
`user.memberOfGroupNames.![#string.upperCase(#this)]`	`[ "ADMIN", "USER" ]`

Use string concatenation to transform the contents of `memberOfGroupNames` *array to a group*

Expression	Result
`user.memberOfGroupNames.!['CN=' + #this ',DC=example,DC=com']`	`[ "CN=Admin,DC=example,DC=com", "CN=User,DC=example,DC=com" ]`

Extract group names from an array of group DNs

Expression	Result
`user.groupDNs.![#regex.replaceAll(#this, '(CN=)(.?),.', '$2')]`	`[ "Devs", "Admins" ]`

Accessing property names with non-alphanumeric characters

If a property name contains any characters other than alpha-numeric characters and underscores (`_`), use the map access format instead of dot notation.

The examples in this section use the following model:

Copyright © 2025 Ping Identity Corporation

```
{
    "providerAttributes": {
        "full-name": "John Doe",
        "http://www.schema.com/samples/userId": "jdoe00",
        "Email Address": "johndoe00@test.com"
    },
    "custom-attributes": {
        "email": "johndoe00@test.com"
    }
}
```

Property names with hyphens or dashes

Expression	Result
`providerAttributes['full-name']`	`John Doe`

Properties with URI or URL based names

Expression	Result
`providerAttributes['http://www.schema.com/samples/userId']`	`jdoe00`

Property names with blank spaces

Expression	Result
`providerAttributes['Email Address']`	`johndoe00@test.com`

Property roots with hyphens or dashes

Expression	Result
`#root['custom-attributes'].email`	`johndoe00@test.com`

Virtual server IDs for SAML applications

When using virtual server IDs for SAML applications to connect to multiple environments in one connection, you can protect against unauthorized access by adding an attribute mapping using the expression builder to compare the virtual server ID invoked by the request against an attribute and populate a required attribute accordingly.

Copyright © 2025 Ping Identity Corporation

For example, for two populations accessing the same SAML application, you can make sure only authorized users can access the application by configuring a different virtual server ID for each population and adding an expression to the application, such as:

```
(
       (context.requestData.virtualServerId eq 'IdP1' and
       user.population.id eq '<populationID1>')
       or
       (context.requestData.virtualServerId eq 'IdP2' and
       user.population.id eq '<populationID2>')
)? user.username : null
```

where `IdP1` and `IdP2` are the respective virtual server IDs, and `populationID1` and `populationID2` are example population IDs from **Directory > Populations** in the PingOne admin console.

If a user from the intended population (`populationID1`) accesses the application using an identity provider (IdP)-initiated single sign-on (SSO) URL for the virtual server ID configured for that population (`IdP1`), PingOne populates the `saml_subject` attribute with the username and redirects the browser with a SAML assertion to the application's ACS endpoint. If a user uses an IdP-initiated SSO URL for the virtual server ID configured for a population to which they don't belong, PingOne populates the `saml_subject` attribute with `null` and returns an error message. Learn more about using virtual server IDs in Editing an application - SAML.

Expressions and concatenation

Property reference expressions

Property reference expressions are the most common expression pattern to refer to a JSON object property using dotted syntax, `object.property1` , or map access syntax, `object[property]` .

Any property that begins with a letter and only contains letters, numbers or underscores can be accessed using dot notation or map access syntax, for example:

- `user.accountId`
- `user.name.given`
- `user['accountId']`
- `user['name']['given']`

If a property contains a character other than the ones mentioned previously, such as a hyphen or dollar sign, it can only be accessed using the map access syntax, for example `user.name['full-name']` or `providerAttributes['amountIn$']` .

Literal expressions

PingOne supports literal expressions in the form of strings, numeric values, boolean, and null.

Strings are delimited by single quotation marks. To put a single quotation mark itself in a string, use two single quotation mark characters around it. For example, `'''string'''` returns `'string'` .

Copyright © 2025 Ping Identity Corporation

Numeric literals used directly in expressions must adhere to Java standards, such as adhering to min and max limits and using `l` or `L` for long literals. Numeric literals are also subject to the Java floating point rounding issues.

Expression type	Example
String in double quotes	`"Hello"`
String in single quotes	`'Hello'`, `'''Hello'''`
Numbers	`1`, `8.57`, `34533535454345L`
Boolean	`true` or `false`

String concatenation

You can use the `+` operator to concatenate values. You must include a leading and trailing space around the operator.

For example, `user.name.family + ', ' + user.name.given` or `'Hi' user.name.given`.

> **Note**
>
> Because it's missing a leading space, `'Hi'+ user.name.given` will return an error.

Arrays and lists

You can build arrays for the following primitives:

- byte
- short
- int
- long
- float
- double
- char
- boolean

For example, `new <type>[<size>]` or `new <type>[] {<comma-separated values>}`.

You can use lists such as `{<comma-separated values>}`.

> **Note**
>
> Lists can contain both non-primitives and primitives.

Copyright © 2025 Ping Identity Corporation

Access arrays and lists using `[index]`.

Array or list type	Example
int array	`new long[4]`
float array	`new float[4]`
Array initializer	`new int[] {1,2,3,4}`
2-dimensional array (cannot have initializer)	`new int[2][2]`
Initializing and accessing array	`new int[] {1,2,3,4} [0]`
Accessing array property	`contacts[0]`
Empty list	`{}`
Integer list	`{1,2,3,4}`
String list	`{'List', 'of', 'Strings'}`
Accessing list element	`{'List', 'of', 'Strings'}[1]`
List with property references	`{user.name.given, user.name.family}`

Maps and objects

Define a map or object in the same way as a JSON object. Access a map using `[]`, or access an object using dot notation. For example, `{'<key>': <value>}`.

If the property key contains any characters other than alphanumeric characters or underscores, you must access it using `[]`. Null keys are discarded.

Map or object keys can be quoted or unquoted. If an unquoted key only contains alphanumeric characters or underscores, it is considered a literal. Otherwise, it is treated as an expression or data model property reference.

If a top level root property needs to be used as a map key which doesn't have the dot operator, use the internal variables `#root` or `#this`, as shown in the examples.

> **Note**
>
> The following examples are formatted with line breaks for readability, however expressions cannot contain line breaks or new line characters.

Copyright © 2025 Ping Identity Corporation

Command	Example

Define a map or object	***Using quoted keys***
	`{ 'userId': 100001, 'name': { 'first': user.name.given, 'last': user.name.family }, 'departmentIds': new int[] {101, 102} }`
	Using unquoted keys
	`{ userId: 100001, name: { first: user.name.given } }`
	Using a top level property value as key using `#root`
	`{ #root.externalId: 100001 }`
	Using a top level property value as key using `#this`
	`{ #this.externalId: 100001 }`

Empty map or object	`\{:}`
Access a map	`{ 'userId': 100001, 'name': { 'first': user.name.given, 'last': user.name.family }, 'departmentIds': new int[] {101, 102} }['name']['first']`

Copyright © 2025 Ping Identity Corporation

Command	Example

Access an object	`{ 'userId': 100001, 'name': { 'first': user.name.given, 'last': user.name.family }, 'departmentIds': new int[] {101, 102} }.name.first`
	
	Note
	Object access against literals causes an error if an incorrect or missing property is accessed, as shown in the following example:
	`{ 'name': { 'first': user.name.given, 'last': user.name.family } }.name.middle`

Operators

Operators are constructs used to manipulate individual data items and data sets. These include arithmetic, comparison, and logical operations.

Relational operators

The following relational operators are supported by using standard operator notation:

- Equal
- Not equal
- Less than
- Less than or equal to
- Greater than
- Greater than or equal to

Each symbolic operator can also be specified as a purely alphabetic equivalent that is case insensitive.

> **Note**
> All operator notations except for `!` require a leading and trailing space.

Copyright © 2025 Ping Identity Corporation

Alphabetic relational operator	Examples

• `lt`
• `<`
	`5 lt 12`
	`5 < 12`
	`user.activeDays < 30`
	Note
	Because the operator is missing a leading and trailing space, `user.activeDays<30` is incorrect.

• `le`
• `⇐`
	`6 le 6`
	`6 ⇐ 6`
	`user.activeDays ⇐ 30`

• `gt`
• `>`
	`12 gt 5`
	`12 > 5`
	`user.activeDays > 30`

• `ge`
• `>=`
	`12 ge 5`
	`12 >= 5`
	`user.activeDays >= 30`

• `eq`
• `==`
	`5 eq 5`
	`5 == 5`
	`user.activeDays == 30`

• `ne`
• `!=`
	`6 ne 5`
	`6 != 5`
	`user.activeDays != 30`

• `not` • `!`	`not (4 > 3)` `!(user.activeDays < 30)`
`matches`	Checks if a value matches the regular expression pattern. `'name' matches '[a-z]+'`

Logical operators

> **Note**
> All logical operator notations except for `!` require a leading and trailing space.

Logical operator	Example
`and`	`5 > 3 and 4 ⇐ 4`
`or`	`5 > 3 or 4 < 3`
• `not` • `!`	`5 < 13 and not (4 < 3)` `5 > 6 and ! 4 < 14`

Mathematical operators

All the following operators used for binary operation require a leading and trailing space.

Mathematical operator	Description

`+`	Add numbers or concatenate if one of the operands is a string.
	`5 + 6`
	`'Test' + 3`
	Note
	Because one of the operands is a string, it will return a string concatenation.
	`user.loginAttempts + user.logoutAttempts`
	Note
	Because the operator is missing a leading and trailing space, `5+6` is incorrect.

`-`	Subtraction
	`7 - 5`
	`user.totalLicenses - user.activeLicenses`
	Note
	Because the operator is missing a leading and trailing space, `7-5` is incorrect.

`*`	Multiplication
	`3 * 5`
	`user.avgLoginsPerMonth * 12`

`/`	Division
	`12 / 3`
	`user.totalLogins / 12`

`%`	Modulus: Get remainder after division `7 % 4`
`^`	Exponential Power `2 ^ 3`, which is equivalent to `(2 * 2 * 2)`

Copyright © 2025 Ping Identity Corporation

Ternary operator

You can use the ternary operator to perform single line if-then-else logic expressions.

```
user.enabled ? 'Active' : 'Inactive'
```

Elvis operator

The Elvis operator is a short form for the Operators for null checks. This operator requires a leading and trailing space.

You can rewrite `user.id != null ? user.id : 'N/A'` as `user.id ?: 'N/A'`.

Collection operations

You can use collection operations to transform existing collections.

Collection selection

You can transform an existing collection by selecting a subset based on filtering criteria, which results in a new collection.

`<Collection>.?[<Filter Criteria Expression>]` becomes a new collection.

In addition to returning a filtered collection, you can extract the first or last entry in a collection matching the filter criteria.

`<Collection>.^[<Filter Criteria Expression>]` returns the first element matching the filter criteria.

`<Collection>.$[<Filter Criteria Expression>]` returns the last element matching the filter criteria.

Selection	Input	Output
From an array or collection of numbers, select only the even numbers	`{1,2,3,4,5,6,7,8,9,10}.?[#this % 2 == 0]`	`[2,4,6,8,10]`
From an array or collection of numbers, select the first even number	`{1,2,3,4,5,6,7,8,9,10}.^[#this % 2 == 0]`	`2`
From an array or collection of numbers, select the last even number	`{1,2,3,4,5,6,7,8,9,10}.$[#this % 2 == 0]`	`10`

For the following input data model, the table following the data model describes possible selections.

Copyright © 2025 Ping Identity Corporation

```
{
    "user": {
        "contacts": [
            {
                "info": "user01@test.com",
                "primary": false,
                "type": "email"
            },
            {
                "info": 9876512345,
                "primary": true,
                "type": "phone"
            },
            {
                "info": 9876511111,
                "primary": false,
                "type": "phone"
            }
        ]
    }
}
```

Selection	Input	Output
Select all contact info of type `phone`	`user.contacts.?[type == 'phone']`	`{ "info": 9876512345, "primary": true, "type": "phone" }, { "info": 9876511111, "primary": false, "type": "phone" }`
Select the first primary contact info	`user.contacts.?[primary]`	`{ "info": 9876512345, "primary": true, "type": "phone" }`

Collection projection

You can transform an existing collection by applying transformations on the input collection's data or by selecting specific data, which results in a new collection containing entirely different data sets.

`<Collection>.![<Projection Expression>]` becomes a new collection.

For the following input data model, the table following the data model describes possible projections:

Copyright © 2025 Ping Identity Corporation

```
{
    "user": {
        "contacts": [
            {
                "info": "user01@test.com",
                "primary": false,
                "type": "email"
            },
            {
                "info": 9876512345,
                "primary": true,
                "type": "phone"
            },
            {
                "info": 9876511111,
                "primary": false,
                "type": "phone"
            }
        ]
    }
}
```

Projection	Input	Output
Transform to a list of contact types only	`user.contacts.![type]`	`["email", "phone", "phone"]`
Extract all primary info attributes	`user.contacts.?[primary].![info]`	`[9876512345]`
Extract the primary info attribute as a different object format	`user.contacts.?[primary].![{'primaryContact': info}]`	`[{"primaryContact": 9876512345}]`

Disabled and restricted SpEL features

Array declaration and initialization

You can only declare primitive arrays. Use List for both primitive and non-primitive arrays.

Type (T) operator

This feature is disabled along with the restriction on Java class usage.

instanceof operator

This feature is disabled along with the restriction on Java class usage.

Assignment operator

All external data used in the expression through external property references are read only.

Copyright © 2025 Ping Identity Corporation

Static and Instance methods

None of the static or instance methods in the Java API are accessible in expressions.

Operators

A leading and trailing space is required for the binary operators, as explained in the Operators section.

Safe Navigation (?.) Operator

The Safe Navigation operator is disabled because PingOne's expression language already attempts safe navigation internally when accessing object properties, except for object literals similar to the Safe Navigation operator (`?.`). This allows access to child properties against a parent object without errors, even if the parent object is null.

For example, `user.address.city` returns null if either `user` or `address` is null.

Variables

`#root` and `#this` variables

`#root` refers to the root context and `#this` refers to the current evaluation context object. Both are internal variables.

You can also use these variables to access any data model property references available to you. For example, `user.name.given`, `#root.user.name.given`, or `#this.user.name.given`.

`#root` is useful in the following scenarios:

- Defining a map key with a base property name's value. Learn more in Maps and objects.
- Accessing a property from the root context from within array or collection operations, such as projections or filtering, which is outside the current evaluation context. For example, `user.memberOfGroupNames.![#root.user.email + ' - ' + #this]`.

`#this` is useful within array or collection operations, such as projections or filtering, especially when the collections contain string, boolean, or number types instead of objects. For example, `user.memberOfGroupNames.![#string.upperCase(#this)]`.

Within the projection operator, `#this` refers to the array element being iterated. If `user.memberOfGroupNames` is a string array, `#this` represents each string element being iterated within the projection operator.

Authentication JWT variables

You can use variables to retrieve information from the token endpoint authentication JSON Web Token (JWT) and authentication method itself for access token and ID token fulfillment. Expressions are supported when using the private key JWT and client secret JWT token endpoint authentication methods. Learn more in Token endpoint authentication methods.

Use variables in expressions to retrieve information in the following configurations:

- Custom resources to fulfill access tokens
- OpenID Connect (OIDC) resources to fulfill ID tokens
- OIDC-based applications to override ID token fulfillment

Copyright © 2025 Ping Identity Corporation

The following variables are available in the expression builder:

Variable	Description
`#root.context.requestData.clientAssertion`	The authentication JWT payload sent by the application at the token endpoint.
`#root.context.requestData.clientAssertion.<property>`	The value of `<property>` from the authentication JWT payload sent by the application at the token endpoint.
`#root.context.requestData.clientAssertionHeader`	The authentication JWT header sent by the application at the token endpoint.
`#root.context.requestData.clientAssertionHeader.<property>`	The value of `<property>` from the header of the authentication JWT sent by the application at the token endpoint.
`#root.context.requestData`	The authentication JWT header and payload sent by the application at the token endpoint.
`#root.context.appConfig.tokenEndpointAuthMethod`	The token endpoint authentication method of the requesting application. Learn more in Token endpoint authentication methods. Possible values are: • `PRIVATE_KEY_JWT` • `CLIENT_SECRET_JWT` • `null` if the application isn't configured to use either `PRIVATE_KEY_JWT` or `CLIENT_SECRET_JWT`. Learn more in Null safe usage.

Custom properties

You can use the following custom property types with authentication JWT variables:

Custom Property Type	Description
String or numeric value	Add the custom property to the variable to access the value. For example, if the payload contains a property named custom1, add `custom1` to the payload variable: `#root.context.requestData.clientAssertion.custom1`.
Array	Add the custom property followed by `[n]` to the variable to access the nth element, where n starts with 0 for the first element. For example, `#root.context.requestData.clientAssertion.custom1[n]`.
Nested JSON object	Add the custom property followed by `.x` or `['x']` to the variable, where x is the nested property name. For example, `#root.context.requestData.clientAssertion.custom1.x` or `#root.context.requestData.clientAssertion.custom1['x']`.

Copyright © 2025 Ping Identity Corporation

Custom library variables

Additional internal variables are available for use in expressions, which are references to the custom libraries covered in Custom library functions.

The following variable references are available to custom libraries:

Reference	Description
`#string`	Function for string-based operations.
`#data`	Functions for processing arrays.
`#datetime`	Functions for parsing and processing date values. All input and output dates are in ISO 8601 format.
`#regex`	Functions using regular expressions.
`#crypto`	Functions for crypto operations, such as hashing and more in the future.

Custom library functions

Use the following custom library functions to process data in strings, arrays, and collections.

String library

You can perform string-related operations within an expression using the following library.

String	Description	Input	Output
`boolean isNotEmpty(String <input>)` where `<input>` is the string to check.	Returns `true` if the input string is not empty (`""`) and not null.	1. `#string.isNotEmpty('InputData')` 2. `#string.isNotEmpty('')`	1. `true` 2. `false`
`boolean isNotBlank(String <input>)` where `<input>` is the string to check.	Returns `true` if the input string is not empty (`""`), not null and not white space only.	1. `#string.isNotBlank('InputData')` 2. `#string.isNotBlank(' ')`	1. `true` 2. `false`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`String upperCase(String <input>)` where `<input>` is the string being converted to upper case.	Converts all characters to uppercase. Returns all characters in upper case if input is not null. Returns `null` if input is null.	`#string.upperCase('john')`	`JOHN`
`String lowerCase(String <input>)` where `<input>` is the string being converted to lower case.	Converts all characters to lowercase. Returns all characters in lower case if input is not null. Returns `null` if input is null.	`#string.lowerCase('LOWER')`	`lower`
`String trim(String <input>)` where `<input>` is the string being trimmed.	Removes white space from the start and end of `string` if input is not null. Returns `null` if input is null.	`#string.trim(' No Padding ')`	`No Padding`
`String substring(String <input>, int <start>, int <end>)` where: • `<input>` is the string to get the substring from • `<start>` is the position to start from • `<end>` is the exclusive position to end at	Gets a substring from the input string starting from the start position and up until the end position, not including the end position. You can use a negative value to start or end *n* characters from the end of the string. All position counting is zero-based. If start is not to the left of end, `""` is returned. Returns `null` if input is null.	1. `#string.substring('example input for substring demo', 8, 13)` 2. `#string.substring('example input for substring demo', -24, 13)` 3. `#string.substring('example input for substring demo', -24, -19)`	1. `input` 2. `input` 3. `input`
`boolean startsWith(String <input>, String <prefix>)` where: • `<input>` is the string to check • `<prefix>` is the prefix to match at the start of the input string.	Checks if the input string starts with the specified prefix and the comparison is case sensitive. Returns `true` if the input string starts with the prefix with the same case or if both are null.	`#string.startsWith('InputData', 'In')`	`true`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`boolean endsWith(String <input>, String <suffix>)` where: • `<input>` is the string to check • `<suffix>` is the suffix to match at the end of the input string	Checks if the input string ends with the specified suffix and the comparison is case sensitive. Returns `true` if input string ends with the suffix with the same case or if both are null.	`#string.endsWith('InputData', 'Data')`	`true`
`String[] split(String <input>, String <separators>)` where: • `<input>` is the string to split • `<separators>` are the characters to be used as delimiters to split the input string	Splits the provided text into an array based on the specified separators. Returned array won't contain any separators. A null separator splits on white space. Returns `null` if input is null.	`#string.split('Administrator, User, Guest', ', ')`	`["Administrator", "User", "Guest"]`
`String join(Array <values>, String <separator>)` where: • `<values>` is the array containing the values to be joined. • `<separator>` is the delimiter to use when joining the values in the input array. A null separator is treated as an empty string.	Joins the elements of the provided array into a single string containing the provided elements separated by the provided separator. Returns the joined string or `null` if the array is null.	`#string.join(\{'Administrator', 'User', 'Guest'}, ', ')`	`Administrator, User, Guest`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`int indexOf(String <input>, String <searchStr>, int <fromIndex>)` where: • `<input>` is the string to search against • `<searchStr>` is the string to find • `<fromIndex>` is the start position in the input string to start the search from	Finds the first index of the search string within the input string. A negative start position is treated as zero, and a start position greater than the input string length only matches an empty search. An empty search string (`""`) always matches. Returns `-1` if a match is not found.	`#string.indexOf('To find and return index or return -1', 'return', -1)`	`12`
`int lastIndexOf(String <input>, String <searchStr>, int <fromIndex>)` where: • `<input>` is the string to search against • `<searchStr>` is the string to find • `<fromIndex>` is the start position in the input string to begin the search from	Finds the last index within the input string. Search starts from the start position and continues backwards. A negative start position is treated as zero, and a start position greater than the input string length searches the entire string backwards. Returns `-1` if a match is not found.	`#string.lastIndexOf('To find and return index or return -1', 'return', 50)`	`28`
`int length(String <input>)` where `<input>` is the string to find the length of.	Returns the length of the input string or `0` if *input* is null.	`#string.length('Input')`	`5`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`String replace(String <input>, String <searchStr>, String <replacement>, int <max>)` where: • `<input>` is the string to be searched against to be replaced in. • `<searchStr>` is the string to be matched and replaced. • `<replacement>` is the string to be replaced with. • `<max>` is the maximum number of times replacement should be done. If `-1`, all matched values will be replaced.	Replaces all occurrences of `searchStr` within `input` according to the `replacement` and `max` values. A null reference passed to this method is a no-op.	`#string.replace('input values replaced by input replacement', 'in', 'out', -1)`	`output values replaced by output replacement`
`int compare(String <str1>, String <str2>, boolean <ignoreCase>)` where: • `<str1>` is the string to compare against • `<str2>` is the string to compare • `<ignoreCase>` determines whether the comparison is case-sensitive.	Compares two strings lexicographically. Returns `0` if `str1` is equal to `str2` or both are null. Returns a negative number if `str1` is less than `str2`. Returns a positive number if `str1` is greater than `str2`.	`#string.compare('Input', 'INPUT', true)`	`0`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`Number asInt(String <input>, Number <defaultIfNullOrInvalid>)` where: • `<input>` is the string representation of an integer number • `<defaultIfNullOrInvalid>` is the default value to be used if the string input is null, not a valid number, or out of range for integers	Parses the string argument as a signed decimal integer (min `-2147483648` and max `2147483647`). The characters in the string must all be decimal digits, except that the first character can be an ASCII minus sign (`-`) to indicate a negative value or an ASCII plus sign (`+`) to indicate a positive value. If input is null or not a valid integer, `defaultIfNullOrInvalid` is returned.	1. `#string.asInt('12', 0)` 2. `#string.asInt('NaN', 0)` 3. `#string.asInt('9876543210123456789', 0)`	1. `12` 2. `0` 3. `0`
`Number asLong(String <input>, Number <defaultIfNullOrInvalid>)` where: • *<input>* is the string representation of a Long number • *<defaultIfNullOrInvalid>* is the default value to be used if string input is null, not a valid number, or out of range for Longs	Parses the string argument as a signed decimal long (min `-9223372036854775808` and max `9223372036854775807`). The characters in the string must all be decimal digits, except that the first character can be an ASCII minus sign (`-`) to indicate a negative value or an ASCII plus sign (`+`) to indicate a positive value. If input is null or not a valid Long, `defaultIfNullOrInvalid` is returned.	1. `#string.asLong('12', 0)` 2. `#string.asLong('NaN', 0)` 3. `#string.asLong('9876543210123456789', 0)`	1. `12` 2. `0` 3. `0`
`Number asBigInt(String <input>, Number <defaultIfNullOrInvalid>)` where: • *<input>* is the string representation of a BigInteger number • *<defaultIfNullOrInvalid>* is the default value to be used if string input is null, not a valid number, or out of range for BigInteger	Translates the decimal string representation of a BigInteger into a BigInteger. The string representation consists of an optional minus sign followed by a sequence of one or more decimal digits. The character-to-digit mapping is provided by Character.digit. If input is null or not a valid Big Integer, `defaultIfNullOrInvalid` is returned.	1. `#string.asBigInt('1234567890987654321', 0)` 2. `#string.asBigInt('NaN', 0)`	1. `1234567890987654321` 2. `0`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`Number asFloat(String <input>, Number <defaultIfNullOrInvalid>)` where: • *<input>* is the string representation of a Float number • *<defaultIfNullOrInvalid>* is the default value to be used if string input is null, not a valid number, or out of range for Floats	Parses the string argument as a signed decimal float. If input is null, not a valid Float, or Infinity, `defaultIfNullOrInvalid` is returned.	1. `#string.asFloat('12.5', 0)` 2. `#string.asFloat('NaN', 0)` 3. `#string.asFloat('1234567899876543210123456789987654321019.12', 0)`	1. `12.5` 2. `0` 3. `0`
`Number asDouble(String <input>, Number <defaultIfNullOrInvalid>)` where: • *<input>* is the string representation of a Double number • *<defaultIfNullOrInvalid>* is the default value to be used if string input is null, not a valid number, or out of range for doubles	Parses the string argument as a signed decimal double. If input is null, not a valid number within the range of Double, or Infinity, `defaultIfNullOrInvalid` is returned.	1. `#string.asDouble('123456789987654321012345678998765432 1019.12', 0)` 2. `#string.asDouble('NaN', 0)`	1. `123456789987654321012345678998765432 1019.12` 2. `0`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`Number asBigDecimal(String <input>, Number <defaultIfNullOrInvalid>)` where: • *<input>* is the string representation of a BigDecimal number • *<defaultIfNullOrInvalid>* is the default value to be used if string input is null, not a valid number, or out of range for BigDecimal	Translates the string representation of a BigDecimal into a BigDecimal. The string representation consists of an optional sign, (`+` or `-`), followed by a sequence of zero or more decimal digits (the integer), optionally followed by a fraction, optionally followed by an exponent. The fraction consists of a decimal point followed by zero or more decimal digits. The string must contain at least one digit in either the integer or the fraction. The exponent consists of the character `e` or `E` followed by one or more decimal digits. The value of the exponent must lie between `-Integer.MAX_VALUE (Integer.MIN_VALUE+1)` and `Integer.MAX_VALUE`, inclusive. If input is null or not a valid BigDecimal, `defaultIfNullOrInvalid` is returned.	1. `#string.asBigDecimal('1234567890987654321.14', 0)` 2. `#string.asBigDecimal('NaN', 0)`	1. `1234567890987654321.14` 2. `0`
`String asBase64Encoded(String <input>)` where *<input>* is the string to be encoded.	Encodes the input string into a new string using the Base64 encoding scheme. Returns the encoded string if input is not empty, or else input is returned as-is.	`#string.asBase64Encoded('Test Value for encoding')`	`VGVzdCBWYWx1ZSBmb3IgZW5jb2Rpbmc=`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`String asBase64Decoded(String <input>)` where <*input*> is the Base64 encoded string to be decoded.	Decodes a Base64 encoded string into a new string using the Base64 encoding scheme. Returns the encoded string if input is not empty, or else input is returned as-is. This will return null if the input string is not in the valid Base64 schema.	`#string.asBase64Decoded('VGVzdCBWYWx1ZSBmb3IgZW5jb2Rpbmc=')`	`Test Value for encoding`
`String asUrlEncoded(String <input>)` where <*input*> is the string to be encoded.	Translates a string into application/x-www-form-urlencoded format using UTF-8 encoding scheme. Returns the encoded string if input is not empty, or else input is returned as-is.	`#string.asUrlEncoded('username=johndoe+admin')`	`username%3Djohndoe%2Badmin`
`String asUrlDecoded(String <input>)` where <*input*> is the URL encoded string to be decoded.	Decodes an application/x-www-form-urlencoded string using UTF-8 encoding scheme. Returns the decoded string if input is not empty, or else input is returned as it is. Returns null if the input string cannot be decoded due to any illegal characters.	`#string.asUrlDecoded('username%3Djohndoe%2Badmin')`	`username=johndoe+admin`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`String format(String <format>, String… <args>)` where: • *<format>* is the format supported by java.util.Formatter • *<args>* are the arguments referenced by the format specifiers in the format string. If there are more arguments than format specifiers, the extra arguments are ignored. The number of arguments is variable and can be zero	Returns a formatted string using the specified format string and arguments. Returns null if a format string contains an illegal syntax, a format specifier that is incompatible with the given arguments, insufficient arguments given the format string, or other illegal conditions.	1. `#string.format('UserId: %s, Full Name: %s, %s', 'johndoe','John', 'Doe')` 2. `#string.format('Hex for 10 is %X', 10)`	1. `UserId: johndoe, Full Name: John, Doe` 2. `Hex for 10 is A`
`String uuidAsBase64Guid(String <input>, String <defaultIfNullOrInvalid>)` where: • *<input>* is a string representation of a UUID. Invalid if not compatible with regex `/[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}/` • *<defaultIfNullOrInvalid>* is the default value to be used if input is null or not a valid UUID	Translates the string representation of a UUID to a GUID in Base64 format. If input is null or not a valid UUID, *<defaultIfNullOrInvalid>* is returned.	1. `#string.uuidAsBase64Guid('7754d487-1fc3-4206-9e95-ce012f1586e5', null)` 2. `#string.uuidAsBase64Guid('invalid', 'lZkqAJgEv0ueGKboT/JFVg==')`	1. `h9RUd8MfBkKelc4BLxWG5Q==` 2. `lZkqAJgEv0ueGKboT/JFVg==`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`String firstNonEmpty(String <value1>, String… <value2…10>)` where: • *<value1>* is the input value to test. Can be null or empty • *<value2…10>* are additional and optional input values to test. Can be null or empty	Returns the first value in the input values which is not empty ('') or null. If all input values are null or empty, then null is returned. There must be at least one input value and the rest are optional. You can enter a maximum of 10 input values.	1. `#string.firstNonEmpty(null, '', 'firstNonEmpty', 'secondNonEmpty')` 2. `#string.firstNonEmpty('', '')`	1. `firstNonEmpty` 2. `null`
`String firstNonBlank(String <value1>, String… <value2…10>)` where: • *<value1>* is the input value to test. Can be null, empty or blank. • *<value2…10>* are additional and optional input values to test. Can be null, empty or blank	Returns the first value in the input values which is not empty ('), null or whitespace only. If all input values are null, empty or blank then null is returned. There must be at least one input value and the rest are optional. You can enter a maximum of 10 input values.	1. `#string.firstNonBlank(null, '', ' ', 'firstNonEmpty', 'secondNonEmpty')` 2. `#string.firstNonBlank('', ' ', '')`	1. `firstNonEmpty` 2. `null`

Date and time library

You can parse, format, and process the date and time within an expression. Dates use the ISO 8601 format in UTC.

Examples of valid dates:

- 2023-01-01T23:59:59Z
- 2023-01-01T23:59:59.123Z
- 2023-01-01T23:59:59.123456Z
- 2023-01-01T23:59:59+800

Default output formats are in UTC:

- 2023-01-01T23:59:59.001Z

Copyright © 2025 Ping Identity Corporation

- 2023-01-01Z
- 23:59:59Z

> **Note**
>
> If you input the ISO 8601 format incorrectly, the system returns `null`.
> This library accepts DateTime with millisecond precision greater than 3, but the output always truncates to millisecond precision of 3.
> Additional input formats not documented above are not officially supported and subject to change without notice.

String	Description	Input	Output
`String addDays(String <inputDate>, int <days>)` where: • `<inputDate>` is the date in a supported ISO 8601 format. • `<days>` is the number of days to add. Can be negative to decrement.	Adds a number of days to the date represented by a supported ISO 8601 string representation and returns the new date in the default ISO 8601 output format. Returns `null` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, or has an invalid date range or values.	1. `#datetime.addDays('2021-01-31T01:01:01Z', 1)` 2. `#datetime.addDays('2021-03-01Z', -1)`	1. `2021-02-01T01:01:01.000Z` 2. `2021-02-28T00:00:00.000Z`
`String addMonths(String <inputDate>, int <months>)` where: • `<inputDate>` is the date in a supported ISO 8601 format. • `<months>` is the number of months to add. Can be negative to decrement.	Adds a number of months to the date represented by a supported ISO 8601 string representation and returns the new date in the default ISO 8601 output format. Returns `null` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, or has an invalid date range or values.	1. `#datetime.addMonths('2020-12-31T01:01:01.001Z', 2)` 2. `#datetime.addMonths('2021-02-28T01:01:01Z', -1)`	1. `2021-02-28T01:01:01.001Z` 2. `2021-01-28T01:01:01.000Z`
`String addYears(String <inputDate>, int <years>)` where: • `<inputDate>` is the date in a supported ISO 8601 format. • `<years>` is the number of years to add. Can be negative to decrement.	Adds a number of years to the date represented by a supported ISO 8601 string representation and returns the new date in the default ISO 8601 output format. Returns `null` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, or has invalid date range or values.	`#datetime.addYears('2021-01-31T01:01:01Z', 1)`	`2022-01-31T01:01:01.000Z`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`String addHours(String <inputDate>, int <hours>)` where: • `<inputDate>` is the date in a supported ISO 8601 format. • `<hours>` is the number of hours to add. Can be negative to decrement.	Adds a number of hours to the date represented by a supported ISO 8601 string representation and returns the new date in the default ISO 8601 output format. Returns `null` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, or has an invalid date range or values.	`#datetime.addHours('2020-12-31T23:59:59.001Z', 3)`	`2021-01-01T02:59:59.001Z`
`String addMinutes(String <inputDate>, int <minutes>)` where: • `<inputDate>` is the date in a supported ISO 8601 format. • `<minutes>` is the number of minutes to add. Can be negative to decrement.	Adds a number of minutes to the date represented by a supported ISO 8601 string representation and returns the new date in the default ISO 8601 output format. Returns `null` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, or has an invalid date range or values.	`#datetime.addMinutes('2021-01-31T23:59:59Z', 10)`	`2021-02-01T00:09:59.000Z`
`String addSeconds(String <inputDate>, int <seconds>)` where: • `<inputDate>` is the date in a supported ISO 8601 format. • `<seconds>` is the number of seconds to add. Can be negative to decrement.	Adds a number of seconds to the date represented by a supported ISO 8601 string representation and returns the new date in the default ISO 8601 output format. Returns `null` if `inputDate` is null, empty, blank, not a supported ISO 8601 format or has invalid date range or values.	`#datetime.addSeconds('2021-02-28Z', 1)`	`2021-02-28T00:00:01.000Z`
`int getDayOfMonth(String <inputDate>)` where `<inputDate>` is the date in a supported ISO 8601 format.	Returns day-of-month, a value from `1` to `31` for valid input or `-1` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, or has an invalid date range or values.	`#datetime.getDayOfMonth('2021-01-31T23:59:59Z')`	`31`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`int getMonth(String <inputDate>)` where `<inputDate>` is the date in a supported ISO 8601 format.	Returns the month from `1` to `12` for valid input or `-1` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, or has an invalid date range or values.	`#datetime.getMonth('2021-02-28Z')`	`2`
`int getYear(String <inputDate>)` where `<inputDate>` is the date in a supported ISO 8601 format.	Returns value for the year for valid input or `-1` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, or has an invalid date range or values.	`#datetime.getYear('2021-01-31T23:59:59Z')`	`2021`
`int getHour(String <inputDate>)` where `<inputDate>` is the date in a supported ISO 8601 format.	Returns the hour of the day as a value between `0` and `23` for valid input or `-1` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, or has an invalid date range or values.	`#datetime.getHour('2021-01-31T23:59:59Z')`	`23`
`int getMinute(String <inputDate>)` where `<inputDate>` is the date in a supported ISO 8601 format.	Returns the minute of the hour as a value between `0` to `59` for valid input or `-1` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, or has an invalid date range or values.	`#datetime.getMinute('2021-01-31T23:59:59Z')`	`59`
`int getSecond(String <inputDate>)` where `<inputDate>` is the date is ISO 8601 format.	Returns the second of the minute as a value between `0` to `59` for valid input or `-1` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, or has an invalid date range or values.	`#datetime.getSecond('2020-12-30T23:59:59.001Z')`	`59`
`String now()`	Obtains the current date-time in default ISO 8601 output format.	`#datetime.now()`	*<Current date and time in default ISO 8601 format>*

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`String toDateTime(int <year>, int <month>, int <dayOfMonth>, int <hour>, int <minute>, int <second>)` where: • `<year>` is the year to represent • `<month>` is the month-of-year to represent, from `1` (January) to `12` (December) • `<dayOfMonth>` is the day-of-month to represent, from `1` to `31` • `<hour>` is the hour-of-day to represent, from `0` to `23` • `<minute>` is the minute-of-hour to represent, from `0` to `59` • `<second>` is the second-of-minute to represent, from `0` to `59`	Obtains the date and time from the provided year, month, day, hour, minute, and second and returns valid date and time in default ISO 8601 output format. Returns `null` if the value for any field is incorrect or out of range, such as day-of-month being invalid for the provided month or year.	`#datetime.toDateTime(2021, 1, 31, 10, 15, 0)`	`2021-01-31T10:15:00.000Z`
`String toDate(String <inputDate>)` where `<inputDate>` is the date in a supported ISO 8601 format.	Transforms the date and time in a supported ISO 8601 format to a UTC date in the format `yyyy-MM-ddX`. Returns `null` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, or has an invalid date range or values.	`#datetime.toDate('2021-02-28Z')`	`2021-02-28Z`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`String toTime(String <inputDate>)` where `<inputDate>` is the date in a supported ISO 8601 format.	Transforms the date and time in a supported ISO 8601 format to a UTC time in the format `HH:mm:ss[.SSS]X`. Returns `null` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, or has an invalid date range or values.	`#datetime.toTime('2021-01-31T23:59:59Z')`	`23:59:59Z`
`String format(String <inputDate>, String <pattern>)` where: • `<inputDate>` is the date in a supported ISO 8601 format. • `<pattern>` is a valid pattern supported by Java 8 DateTimeFormatter.	Transforms the date and time in a supported ISO 8601 format to the date and time in the specified format. Returns `null` if the input `dateTime` or format is not valid. For more information, see the available formats in the Reference section. Returns `null` if `inputDate` is null, empty, blank, not a supported ISO 8601 format, has invalid date range or values, or if pattern is null or invalid.	1. `#datetime.format('2021-01-01T09:15:00Z', 'EEEE, dd MMMM; h:mm a')` 2. `#datetime.format('2021-02-28Z', "QQQQ 'of year' yyyy")`	1. `Friday, 01 January; 9:15 AM` 2. `1st quarter of year 2021`
`int compare(String <inputDateTime1>, String <inputDateTime2>)` where: • `<inputDateTime1>` is the primary date-time in a supported ISO 8601 format to compare with • `<inputDateTime2>` is the other date-time in a supported ISO 8601 format to compare to **Note** Both values are treated as null if null, empty, blank, or not a supported ISO 8601 format.	Compares this date and time to another date and time, including the chronology. Returns `0` if they are the same, a negative number if the former date is earlier, and a positive number if the former date is later.	1. `#datetime.compare('2021-01-01T00:00:00Z', '2021-01-01T00:00:00Z')` 2. `#datetime.compare('2021-01-01T00:00:01Z', '2021-01-01T00:00:00Z')`	1. `0` 2. `1`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`Number daysBetween(String <inputDateTime1>, String <inputDateTime2>, Number <defaultIfNotDate>)` where: • *<inputDateTime1>* is the primary date-time in a supported ISO 8601 format to compare with • *<inputDateTime2>* is the other date-time in a supported ISO 8601 format to compare to • *<defaultIfNotDate>* is the default value to return if either of the input date-time are null, empty, blank or not a supported ISO 8601 format **Note** *<inputDateTime1>* and *<inputDateTime2>* are treated as null if null, empty, blank, or not a supported ISO 8601 format.	Calculates the number of days between input dates. The result is negative if *<inputDateTime2>* is before *<inputDateTime1>*. If either of the input date-time are null, empty, blank or not a supported ISO 8601 format, the value provided for *<defaultIfNotDate>* is returned.	1. `#datetime.daysBetween('2021-01-01T00:00:00Z', '2021-01-01T08:45:00Z', -1)` 2. `#datetime.daysBetween('2021-01-01T00:00:01Z', '2021-01-03T10:30:00Z', -1)` 3. `#datetime.daysBetween('2021-01-03T00:00:01Z', '2021-01-01T10:30:00Z', -1)`	1. `0` 2. `2` 3. `-2`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`Number weeksBetween(String <inputDateTime1>, String <inputDateTime2>, Number <defaultIfNotDate>)` where: • *<inputDateTime1>* is the primary date-time in a supported ISO 8601 format to compare with • *<inputDateTime2>* is the other date-time in a supported ISO 8601 format to compare to • *<defaultIfNotDate>* is the default value to return if either of the input date-time are null, empty, blank, or not a supported ISO 8601 format **Note** *<inputDateTime1>* and *<inputDateTime2>* are treated as null if null, empty, blank, or not a supported ISO 8601 format.	Calculates the number of weeks between input dates. The result is negative if *<inputDateTime2>* is before *<inputDateTime1>*. If either of the input date-time are null, empty, blank or not a supported ISO 8601 format, the value provided for *<defaultIfNotDate>* is returned.	1. `#datetime.weeksBetween('2021-01-01T00:00:00Z', '2021-01-01T08:45:00Z', -1)` 2. `#datetime.weeksBetween('2021-01-01T00:00:01Z', '2021-01-15T10:30:00Z', -1)` 3. `#datetime.weeksBetween('2021-01-15T00:00:01Z', '2021-01-01T10:30:00Z', -1)`	1. `0` 2. `2` 3. `-2`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`Number monthsBetween(String <inputDateTime1>, String <inputDateTime2>, Number <defaultIfNotDate>)` where: • *<inputDateTime1>* is the primary date-time in a supported ISO 8601 format to compare with • *<inputDateTime2>* is the other date-time in a supported ISO 8601 format to compare to • *<defaultIfNotDate>* is the default value to return if either of the input date-time are null, empty, blank, or not a supported ISO 8601 format **Note** *<inputDateTime1>* and *<inputDateTime2>* are treated as null if null, empty, blank, or not a supported ISO 8601 format.	Calculates the number of months between input dates. The result is negative if *<inputDateTime2>* is before *<inputDateTime1>*. If either of the input date-time are null, empty, blank or not a supported ISO 8601 format, the value provided for *<defaultIfNotDate>* is returned.	1. `#datetime.monthsBetween('2021-01-01T00:00:00Z', '2021-01-01T08:45:00Z', -1)` 2. `#datetime.monthsBetween('2021-01-01T00:00:01Z', '2021-02-01T10:30:00Z', -1)` 3. `#datetime.monthsBetween('2021-02-01T00:00:01Z', '2021-03-01T10:30:00Z', -1)`	1. `0` 2. `1` 3. `1`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`Number yearsBetween(String <inputDateTime1>, String <inputDateTime2>, Number <defaultIfNotDate>)` where: • *<inputDateTime1>* is the primary date-time in a supported ISO 8601 format to compare with • *<inputDateTime2>* is the other date-time in a supported ISO 8601 format to compare to • *<defaultIfNotDate>* is the default value to return if either of the input date-time are null, empty, blank, or not a supported ISO 8601 format **Note** *<inputDateTime1>* and *<inputDateTime2>* are treated as null if null, empty, blank, or not a supported ISO 8601 format.	Calculates the number of years between input dates. The result is negative if *<inputDateTime2>* is before *<inputDateTime1>*. If either of the input date-time are null, empty, blank or not a supported ISO 8601 format, the value provided for *<defaultIfNotDate>* is returned.	1. `#datetime.yearsBetween('2021-01-01T00:00:00Z', '2021-01-01T08:45:00Z', -1)` 2. `#datetime.yearsBetween('2021-01-01T00:00:01Z', '2022-01-01T10:30:00Z', -1)` 3. `#datetime.yearsBetween('2022-01-01T00:00:01Z', '2021-01-01T10:30:00Z', -1)`	1. `0` 2. `1` 3. `-1`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`String periodBetween(String <inputDateTime1>, String <inputDateTime2>, String <defaultIfNotDate>)` where: • *<inputDateTime1>* is the primary date-time in a supported ISO 8601 format to compare with. The value is inclusive. • *<inputDateTime2>* is the other date-time in a supported ISO 8601 format to compare to. The value is exclusive. • *<defaultIfNotDate>* is the default value to return if either of the input date-time are null, empty, blank, or not a supported ISO 8601 format. **Note** *<inputDateTime1>* and *<inputDateTime2>* are treated as null if null, empty, blank, or not a supported ISO 8601 format.	Calculates the period between input dates represented as amount of time in years, months, and days using ISO 8601 period format `P[nY][nM][nD]`. The letter `P` starts the period, `n`] is an integer representing the number of years, months, and days, represented by `Y`, `M`, and `D`, respectively. A zero period is represented as zero days, or `P0D`. The result is negative if *<inputDateTime2>* is before *<inputDateTime1>*. If either of the input date-time is null, empty, blank or not a supported ISO 8601 format, the value provided for *<defaultIfNotDate>* is returned. The period is calculated by removing complete months, then calculating the remaining number of days, adjusting to ensure that both have the same sign. The number of months is then split into years and months based on a 12 month year.	1. `#datetime.periodBetween('2021-01-01T00:00:00Z', '2021-01-01T00:00:00Z', -1)` 2. `#datetime.periodBetween('2021-01-01Z', '2022-02-11Z', -1)`	1. `P0D` 2. `P1Y1M10D`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`String toUnixTimestamp(String <inputDateTime>)` where *<inputDateTime>* is the date-time in a supported ISO 8601 format. **Note** *<inputDateTime>* is treated as null if null, empty, blank, or not a supported ISO 8601 format.	Transforms the date-time in a supported ISO 8601 format to the number of seconds from the epoch of 1970-01-01T00:00:00Z. This returns null if *<inputDateTime>* is null, empty, blank, or not a supported ISO 8601 format.	1. `#datetime.toUnixTimestamp('2020-12-31Z')` 2. `#datetime.toUnixTimestamp('2020-12-31T23:59:59Z')` 3. `#datetime.toUnixTimestamp('2020-12-31T23:59:59.001Z')`	1. `1609372800` 2. `1609459199` 3. `1609459199`
`String fromUnixTimestamp(Number <epochSeconds>)` where *<epochSeconds>* is the number of seconds from the epoch of 1970-01-01T00:00:00Z.	Builds date-time using the number of seconds from the epoch of 1970-01-01T00:00:00Z to a UTC date-time in default ISO 8601 format. Returns null if *<epochSeconds>* is null.	`#datetime.fromUnixTimestamp(1609459199)`	`2020-12-31T23:59:59.000Z`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output

`String parse(String <inputDateTime>, String <format>, Object <options>)` where:
• *<inputDateTime>* is the date with or without time to parse in a format other than ISO 8601
• *<format>* is the custom format supported by Java DateTimeFormatter used for the specified *<inputDateTime>*
• *<options>* is an optional JSON object with default values for allowed date-time fields which cannot be obtained from the *<inputDateTime>* format. Supported fields are `zoneid` - if *<inputDateTime>* doesn't contain any zone information, users can configure the `zoneid` to be used in the input options JSON, or else UTC will be used.
Note
<inputDateTime> is treated as null if null, empty, blank, or not a supported ISO 8601 format.
	Parses *<inputDateTime>* in a format other than ISO 8601 as specified by *<format>*, and uses any default values specified in *<options>* if required to transform it to a date-time in ISO 8601 format.
	Will return null if *<inputDateTime>*:
	• Is null
	• Is not in a valid format
	• Cannot be transformed to ISO 8601 if it lacks any required fields such as day, month, or year
	• Any of those fields are out of range
		Parsing date with format yyyy-MM-dd without zone information which uses UTC as default zone
		`#datetime.parse('2022-01-01', 'yyyy-MM-dd', null)`
		Parsing date with format yyyy-MM-dd without zone information but with zone defaults configured using options
		`#datetime.parse('2022-01-01', 'yyyy-MM-dd', \{'zoneid': 'America/Vancouver'})`
		Parsing date with format yyyy-MM-dd z with zone information
		`#datetime.parse('2022-01-01 PST', 'yyyy-MM-dd z', null)`
		Parsing date with format dd/MM/yyyy HH:mm:ss without zone information which uses UTC as default zone
		`#datetime.parse('03/12/2021 09:30:45', 'dd/MM/yyyy HH:mm:ss', null)`
			1. `2022-01-01T00:00:00.000Z`
			2. `2022-01-01T08:00:00.000Z`
			3. `2022-01-01T08:00:00.000Z`
			4. `2021-12-03T09:30:45.000Z`

Copyright © 2025 Ping Identity Corporation

`String toDateTimeInTimezone(String <inputDateTime>, String <timezone>, String <pattern>)`
where:
• *<inputDateTime>* is the date in a supported ISO 8601 format.
• *<timezone>* is a valid zone ID supported by Java 8. Parsing matches the zone ID as follows:
1. If the zone ID equals `Z`, the result is UTC.
2. If the zone ID consists of a single letter, the zone ID is invalid.
3. If the zone ID equals `GMT`, `UTC`, or `UT`, then the result is a timezone with the same ID and rules equivalent to UTC.
 	
Zone IDs must match regular expression characters. If the zone ID is not in the Java 8 configured set of IDs, it is invalid. The detailed format of the region ID depends on the group supplying the data. The default set of data is supplied by the IANA Time Zone Database (TZDB).
	Transforms the date-time in a supported ISO 8601 format to date-time in the specified timezone in the required format if specified, or the default format `yyyy-MM-dd'T'HH:mm:ss[.SSS]Z`.
	Will return null if:
	• *<inputDateTime>* is null, empty, or blank
	• *<inputDateTime>* is not a supported ISO 8601 format, or has invalid dates or values
	• *<timezone>* or *<pattern>* are null or invalid
		Change time zone to America/Vancouver with default pattern
		`#datetime.toDateTimeInTimezone('2023-01-01T04:30:30.000Z', 'America/Vancouver', null)`
		Change time zone to +100 with default pattern
		`#datetime.toDateTimeInTimezone('2023-01-01T04:30:30Z', '+0100', null)`
		Change time zone to America/Vancouver with custom pattern
		`#datetime.toDateTimeInTimezone('2023-01-01T04:30:30.123Z', 'America/Vancouver', 'dd-MM-YYYY hh:mm a')`
			1. `2022-12-31T20:30:30-0800`
			2. `2023-01-01T05:30:30.000+0100`
			3. `31-12-2022 08:30 PM`

String	Description	Input	Output
IANA TZDB has region IDs of the form *<area>/<city>*, such as `Europe/Paris` or `America/New_York`. This is compatible with most IDs from Time Zone. * *<pattern>* is a pattern supported by Java 8 DateTimeFormatter. For available formats, see the References section. **Note** *<inputDateTime>* is treated as null if null, empty, blank, or not a supported ISO 8601 format.			

Data library

You can process data in arrays and collections using the following library.

Note

When using a collection format, some of the following methods which perform operations between two arrays or collections determine data type automatically based on Java defaults. For example, `3` is treated as integer, `3.5` as a double and `c` as a string. However, array comparison is based on the array data types.

`#data.containsAll(new int[] {2,4,6,8,10}, new int[] {2,8})` returns as true because both are int arrays.

`#data.containsAll(new int[] {2,4,6,8,10}, {2,8})` returns as true because the first argument is an int array and the second argument uses int by default.

`#data.containsAll(new float[] {2.1,4.1,6.1,8.1,10.1}, {2.1,8.1})` returns as false because the first argument is a float array and the second argument is a double, which is the default for floating point numbers.

`#data.containsAll(new double[] {2.1,4.1,6.1,8.1,10.1}, {2.1,8.1})` returns as true because the first argument is a double array and the second argument is treated as a double by default.

`#data.containsAll({2.1,4.1,6.1,8.1,10.1}, {2.1,8.1})` returns as true because both arguments are collections and use the default data types.

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`int indexOf(Array <srcArray>, <valueToFind>)` where: • `<srcArray>` is the array to search through • `<valueToFind>` is the value to find.	Finds and returns the index of the `valueToFind` in the input array. Returns `-1` if not found or if `srcArray` is null.	1. `#data.indexOf(new int[] {2,4,6,8,10}, 6)` 2. `#data.indexOf({'This', 'is', 'String', 'collection'}, 'is')`	1. `2` 2. `1`
`boolean isNotEmpty(Array <srcArray>)` where `<srcArray>` is the array to check.	Checks if the input array is not empty and not null.	1. `#data.isNotEmpty(new int[] {2,4,6,8,10})` 2. `#data.isNotEmpty({'This', 'is', 'String', 'collection'})`	1. `true` 2. `true`
`boolean containsAll(Array <srcData>, Array <searchData>)` where `<searchData>` is the array of values to be searched for in the `<srcData>` array.	Returns true if all elements of `searchData` are contained in `srcData`.	1. `#data.containsAll(new int[] {2,4,6,8,10}, new int[] {2,8})` 2. `#data.containsAll(new int[] {2,4,6,8,10}, {2,8})` 3. `#data.containsAll({2,4,6,8,10}, {2,9})` 4. `#data.containsAll(new float[] {2.1,4.1,6.1,8.1,10.1}, {2.1,8.1})` 5. `#data.containsAll(new double[] {2.1,4.1,6.1,8.1,10.1}, {2.1,8.1})`	1. `true` 2. `true` 3. `false` 4. `false` 5. `true`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`boolean containsAny(Array <srcData>, Array <searchData>)` where `<searchData>` is the array of values to be searched for in the `<srcData>` array.	Returns `true` if there is at least one common element in both arrays.	1. `#data.containsAny({2,4,6,8,10}, {2,9,11})` 2. `#data.containsAny(new int[] {2,4,6,8,10}, {2,9,11})` 3. `#data.containsAny({2,4,6,8,10}, new int[] {1,9})`	1. `true` 2. `true` 3. `false`
`Array removeAll(Array <srcData>, Array <dataToRemove>)` where `<dataToRemove>` is the array of values to be removed from the `<srcData>` array.	Removes the elements in `dataToRemove` from `srcData` and returns a new array.	1. `#data.removeAll(new int[] {2,4,6,8,10}, new int[] {2,6,11})` 2. `#data.removeAll({2,4,6,8,10}, {2,6,11})`	1. `[4,8,10]` 2. `[4,8,10]`
`Array retainAll(Array <srcData>, Array <dataToRetain>)` where: • *<srcData>* is the array from which values are to be removed • `<dataToRetain>` is the array of values to be retained if they also exist in `<srcData>`	Retains only the elements that exist in both `srcData` and `dataToRetain`.	1. `#data.retainAll(new int[] {2,4,6,8,10}, new int[] {2,6,11})` 2. `#data.retainAll({2,4,6,8,10}, new int[] {2,6,11})`	1. `[2,6]` 2. `[2,6]`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`Array union(Array <array1>, Array <array2>)` where: • `<array1>` is the first array to which elements will be added to • `<array2>` is the second array whose elements will be appended to first array.	Returns a new array containing the second array appended to the first array.	1. `#data.union(new int[] {2,4,6,8,10}, new int[] {1,10,11})` 2. `#data.union(new int[] {2,4,6,8,10}, {1,10,11})`	1. `[2,4,6,8,10,1,10,11]` 2. `[2,4,6,8,10,1,10,11]`
`int size(Array <inputArray>)` where `<inputArray>` is the array for which the size is determined.	Returns the size of the input array.	1. `#data.size(new int[] {2,4,6,8,10})` 2. `#data.size({2,4,6,8,10})`	1. `5` 2. `5`
`boolean equals(Array <array1>, Array <array2>)` where `<array1>` is the first array which is compared against `<array2>`.	Tests two arrays for value-equality and returns `true` if both arrays have the same size and all corresponding pairs of elements in the two arrays are equal.	1. `#data.equals(new int[] {2,4,6,8,10}, new int[] {2,4,6,8,10})` 2. `#data.equals({2,4,6,8,10}, new int[] {2,4,6,8,10})`	1. `true` 2. `true`

Regex library

You can use regular expressions in operations with the following library.

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`String replaceFirst(String <input>, String <regex>, String <replacement>)` where: • `<input>` is the string to search and replace in • `<regex>` is the regular expression to which this string is to be matched • `<replacement>` is the string to be substituted for the first match	Replaces the first substring of the text string that matches the given regular expression with the given replacement. A null reference passed to this method is a no-op and returns `null`.	1. `#regex.replaceFirst('upper case', '()( +)([a-z])', '$1_$3')` 2. `#regex.replaceFirst('upper case AND lower case', '()( +)([a-z])', '$1_$3')`	1. `upper_case` 2. `upper_case AND lower case`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`String replaceAll(String <input>, String <regex1>, String <replacement1>, …, String <regexN>, String <replacementN>)` where: • `<input>` is the string to search and replace in • `<regex1>` is the regular expression to which this string is to be matched • `<replacement1>` is the string to be substituted for each match • `<regex[2…N]>` is an optional additional regular expression to which this string is to be matched • `<replacement[2…N]>` is an optional additional string to be substituted for each match. If replacement is missing, the corresponding regex string won't be altered. **Note** The first pair of find-replace arguments are mandatory and the rest are optional.	Replaces each substring of the text string that matches the given regular expression with the given replacement. You can use this for 1 or more find and replace options. The first pair of find-replace arguments are mandatory and the rest are optional.	1. `#regex.replaceAll('upper case AND lower case', '()(+)([a-z])', '$1_$3')` 2. `#regex.replaceAll('numeric data to be replaced with textual data [1, 2]', 'to be', '', '1', 'one', '2', 'two')`	1. `upper_case AND lower_case` 2. `numeric data replaced with textual data [one, two]`

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`boolean matches(String <input>, String <regex>)` where: • `<input>` is the string to be matched with • `<regex>` is the regular expression to which the string is matched	Checks if the entire input string matches the regex pattern. If a null is passed as input, it returns `false`.	`#regex.matches('upper case', '()( +)([a-z])')`	`true`
`Array findAllMatches(String <input>, String <regex>)` where: • `<input>` is the string to search in • `<regex>` is the regular expression to which the string is matched	Find all matching substrings in the input string matching the regex pattern.	`#regex.findAllMatches('upper case AND lower case', '()( +)([a-z])')`	`["upper case", "lower case"]`

Crypto library

You can perform crypto operations such as hashing using the following library.

Copyright © 2025 Ping Identity Corporation

String	Description	Input	Output
`String hmacHexDigest(String <data>, String <key>, String <algorithm>)` where: • `<data>` is the string value to be hashed and must not be null • `<key>` is the string secret key to use and must not be null • `<algorithm>` is the hashing algorithm to use and must not be null **Note** Supported algorithms are HmacMD5, HmacSHA1, HmacSHA224, HmacSHA256, HmacSHA384, and HmacSHA512.	Creates a hash for the required data with Hashed Message Authentication Code (HMAC) using the specified secret key and cryptographic hashing function algorithm. Returns the hash or digest as a string containing only hexadecimal digits. Supported algorithms for hashing functions are HmacMD5, HmacSHA1, HmacSHA224, HmacSHA256, HmacSHA384, and HmacSHA512.	`#crypto.hmacHexDigest('data', 'secretKey', 'HmacMD5')`	`6659dfc3b860b836c087e3fd82c0d16b`

Core library

You can perform basic conditional expressions using if-else and switch alternatives.

Copyright © 2025 Ping Identity Corporation

String	Description
`Any ifelse(Boolean <condition>, Any <value>, Boolean <elseifCondition<1…10>>, Any <elseifValue<1…10>>, Any <elseValue>)` where: • `<condition>` is the primary If conditional expression which should evaluate to a boolean value. If it is not boolean, every attempt will be made to convert it to a boolean value. • `<value>` is the value to use if the primary condition evaluates to true. • `<elseifCondition<1…10>>` is an elseIf conditional expression which should evaluate to a boolean value. If it is not boolean, every attempt will be made to convert it to a boolean value. The elseIfValue should always follow the elseIf condition. • *<elseifValue<1…10>>* is the value to use if the related elseIf condition evaluates to true. • *<elseValue>>* is the value to use if none of the conditions evaluate to true.	Library function for an If-Else statement. Expressions provided for If and elseIf conditions should evaluate to a boolean value and if not, every attempt will be made to convert the evaluated value to boolean. If the condition evaluates to a Number, any value greater than 0 will be treated as True, or else false. If the condition evaluates to a String, the values `true`, `on`, `y`, `t`, `yes` are treated as true irrespective of the case, and otherwise false. If the condition evaluates to something other than Boolean, Number or String, it will be treated as false. The If statement and elseIf statement is a pair: a condition and a value to be used if condition evaluates to true. The elseIf statements are optional, and can enter 0 to 10 elseIf statements as needed. The elseValue to be used if no condition evaluates to true is also optional and is always the last parameter in the method.

Copyright © 2025 Ping Identity Corporation

String	Description
`Any switchExpr(Any <valueToFind>, Any <choiceToMatch1>, Any <valueToReturn1>, Any <choiceToMatch<2…10>>, Any <valueToReturn<2…10>>, Any <defaultValue>)` where: • `<valueToFind>` is the value against which all the choices are compared with to identify the match. • `<choiceToMatch1>` is the choice to match. • `<valueToReturn1>` is the value to use or return if the valueToFind matches the corresponding valueToMatch. • *<choiceToMatch<2...10>>* are additonal and optional choices to match. • *<valueToReturn<2...10>>* is the value to use or return if the valueToFind matches the corresponding choiceToMatch<n>. • *<defaultValue>* is the value to use if no matching choice is found for valueToFind. If this is not provided, null is returned.	Library function for a switch statement. A *<valueToFind>* is compared against 1 or more choices to match (*<choiceToMatch<1...10>>*). If a match is found, the value corresponding to the matched choice (*<valueToReturn<1...10>>*) is returned. If no match is found, *<defaultValue>* is returned if provided, or else null. *<choiceToMatch<n>>* and *<valueToReturn<n>>* are a pair and there should be a minimum of 1 pair and not exceed 10 pairs. A default value can be provided as the last parameter to the method.

Copyright © 2025 Ping Identity Corporation

Examples

String	Input
`Any ifelse(Boolean <condition>, Any <value>, Boolean <elseifCondition<1…10>>, Any <elseifValue<1…10>>, Any <elseValue>)`	`{ user: { type: "User" } } #core.ifelse(user.type == 'Administrator', 'Full Access', user.type == 'User', 'Restricted Access', 'No Access')` returns `Restricted Access` `{ user: { memberOfGroupIDs: ["User"], type: "Dev" } } #core.ifelse(#data.indexOf(user.memberOfGroupIDs, 'Administrator') >= 0, 'Full Access', #data.indexOf(user.memberOfGroupIDs, 'User') >= 0, #core.ifelse(user.type == 'SRE', 'Power Access', user.type == 'Dev', 'Debugging Access', 'Read Access'), 'No Access')` returns `Debugging Access`

`Any switchExpr(Any <valueToFind>, Any <choiceToMatch1>, Any <valueToReturn1>, Any <choiceToMatch<2…10>>, Any <valueToReturn<2…10>>, Any <defaultValue>)`	`{ user: { type: "Administrator" } } #core.switchExpr(user.type, 'Administrator', 'Full Access')`
	returns `Restricted Access`
	`{ user: { type: "User" } } #core.switchExpr(user.type, 'Administrator', 'Full Access', 'User', 'Restricted Access', 'No Access')`
	returns `Restricted Access`

Copyright © 2025 Ping Identity Corporation

Null safe usage

Using property references that might be null in expressions can lead to unexpected results. This topic contains examples and how to handle them.

The examples in this topic use the following data model:

```
{
  "user": {
    "name": {
      "given": "John",
      "family": "Doe"
    }
}
```

String concatenation

Issue

Because `user.name.middle` is null, the expression `user.name.given + ', ' + user.name.middle + ', ' + user.name.family` returns `John, null, Doe`.

Solution to concatenate only non-null values

`#string.join({user.name.given, user.name.middle, user.name.family}, ', ')` returns `John, Doe`.

Issue

Because `user.age` is null and the other operand is numeric, the expression `3 + user.age` returns an error.

Solution to avoid errors using an Elvis operator to add a default value

`3 + (user.age ?: '')` returns `3`.

Creating an array using nullable values

Issue

The newly created array `{user.externalId}` returns `[ null ]`.

Solution to remove nulls from the newly created array

`#data.removeAll({user.externalId}, {null})` returns `[]`.

Ternary operator

Issue

Because `user.enabled` is null, the expression `user.enabled ? 'Active' : 'Inactive'` returns an error.

Copyright © 2025 Ping Identity Corporation

Solution to avoid errors using an Elvis operator to add a default value

`(user.enabled ?: false) ? 'Active' : 'Inactive'` returns `Inactive`.

References

Spring Expression Language

See the SpEL Language Reference.

DateTimeFormatter patterns

The following common pattern symbols are extracted from Java documentation. For a complete list, see Class DateTimeFormatter.

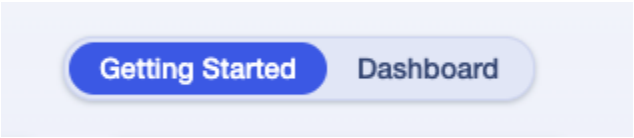
Symbol	Meaning	Examples
`y`	year-of-era	`2004`; `04`
`D`	day-of-year	`189`
`M`	month-of-year	`07`; `Jul`; `July`; `J`
`d`	day-of-month	`10`
`q`	quarter-of-year	`03`; `Q3`; `3rd quarter`
`W`	week-of-month	`4`
`E`	day-of-week	`Tue`; `Tuesday`; `T`
`a`	am-pm-of-day	`PM`
`h`	clock-hour-of-am-pm (1-12)	`12`
`K`	hour-of-am-pm (0-11)	`0`
`k`	clock-hour-of-am-pm (1-24)	`1`
`H`	hour-of-day (0-23)	`0`
`m`	minute-of-hour	`30`
`s`	second-of-minute	`55`

Copyright © 2025 Ping Identity Corporation

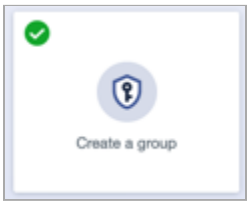
Overview page

The **Overview** page shows a summary of the environment, an overview of sign-on activity, and tutorials you can complete.

In the upper right corner of the panel, you can toggle between **Getting Started** and **Dashboard**.



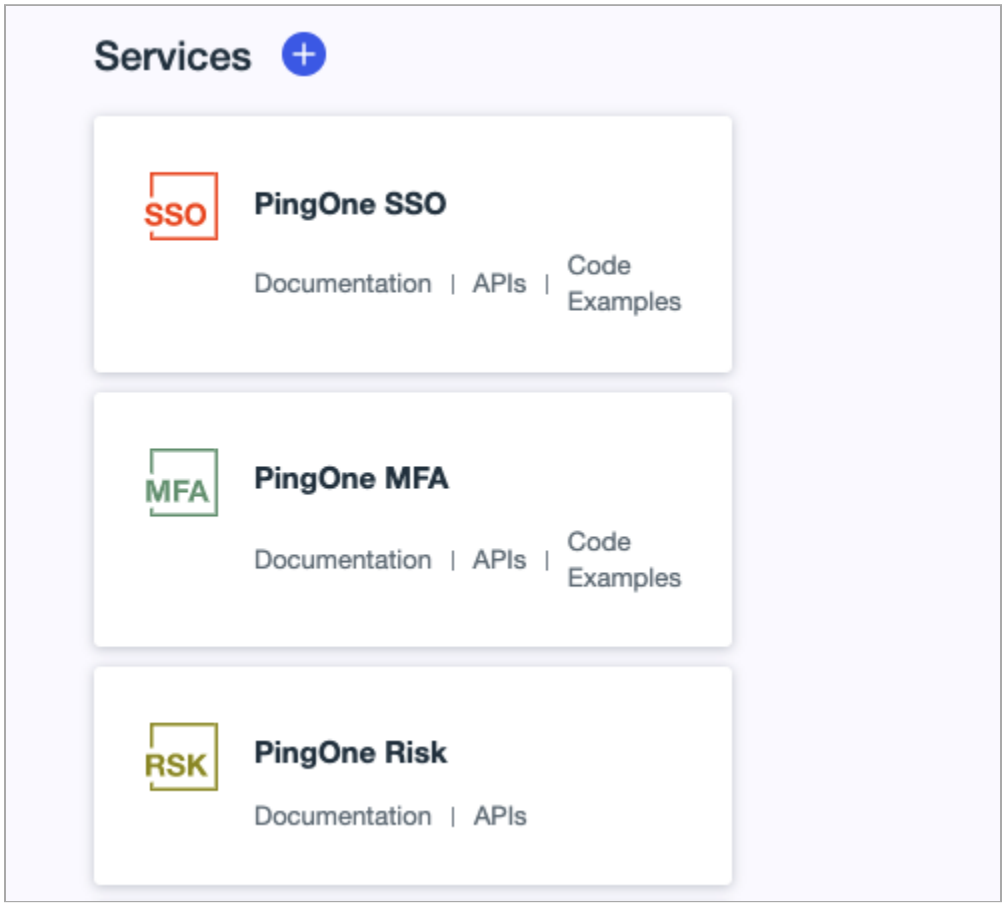
When displayed, the **Getting Started Tasks** section shows a list of tutorials for common tasks. Completed tutorials are noted with a check mark.



When the **Dashboard** toggle is enabled, the page shows a summary of sign on activity for the selected time period.

The **Services** section shows a list of current services, and an option to add services to your current PingOne environment.

Copyright © 2025 Ping Identity Corporation



For detailed information about a service, see the dashboard for the specific service, such as Authentication, MFA, or Protect.

Copyright © 2025 Ping Identity Corporation

Monitoring

The **Monitoring** branch provides access to the platform and services dashboards, as well as to the **Audit** and **Alerts** pages.

For more information, see the following topics:

Dashboards

Audit

Alerts

Dashboards

Dashboards contains the different dashboards for PingOne and your configured PingOne services.

PingOne

- Authentication Dashboard: View a summary of sign-on activity for the selected environment.
- User Demographics Dashboard: View a summary of user demographic profiles and activity for the selected environment.

PingOne Services

Note

You'll only see dashboards for the services you have.

- Authorization Dashboard: View a summary of metrics generated by requests to PingOne Authorize decision endpoints.
- DaVinci Dashboard: View a summary of DaVinci flow and connector usage.
- MFA Dashboard: View a summary of current user activity for the selected environment.
- Threat Protection Dashboard: View a summary of real-time PingOne Protect risk data.
- Identity Verification Dashboard: View a summary of PingOne Verify transaction activity.

Copyright © 2025 Ping Identity Corporation

Authentication dashboard

The Authentication dashboard shows a summary of sign-on activity through PingOne sign-on policies for the selected environment.

> **Note**
>
> The Authentication dashboard does not include DaVinci transactions.

You can limit the data to a specific time range, such as the current day, the current week, the current month, or the previous three months.

The graph at the top of the page shows sign-on activity at a glance, including the number of successful user sign-ons for the current day, and a graph showing the number of successful sign-ons and the number of failed sign-ons for the specified period.

Cards

The cards show the following information:

MFA adoption

The current percentage of MFA-enabled users. Select a timeframe of 30 days, 12 weeks, or 1 year to see the evolution of the MFA adoption rate. This information can help administrators visualize trends and inform decisions.Hover over the area chart to see exact information on rate and date for a particular point in time. The back of the card shows a snapshot of historical rates.

Total identities

The number of active users for the specified period.

Total password resets

The number of times users have requested password resets over the specified period.

The cards show a graphical view on one side and a list view on the other. Click the icon on the top right of the card to toggle between views.

Sign-ons by day/hour

The **Sign-ons by day/hour** shows relative authentication activity by hour of the day and day of the week. The color variations show usage trends throughout an average week.

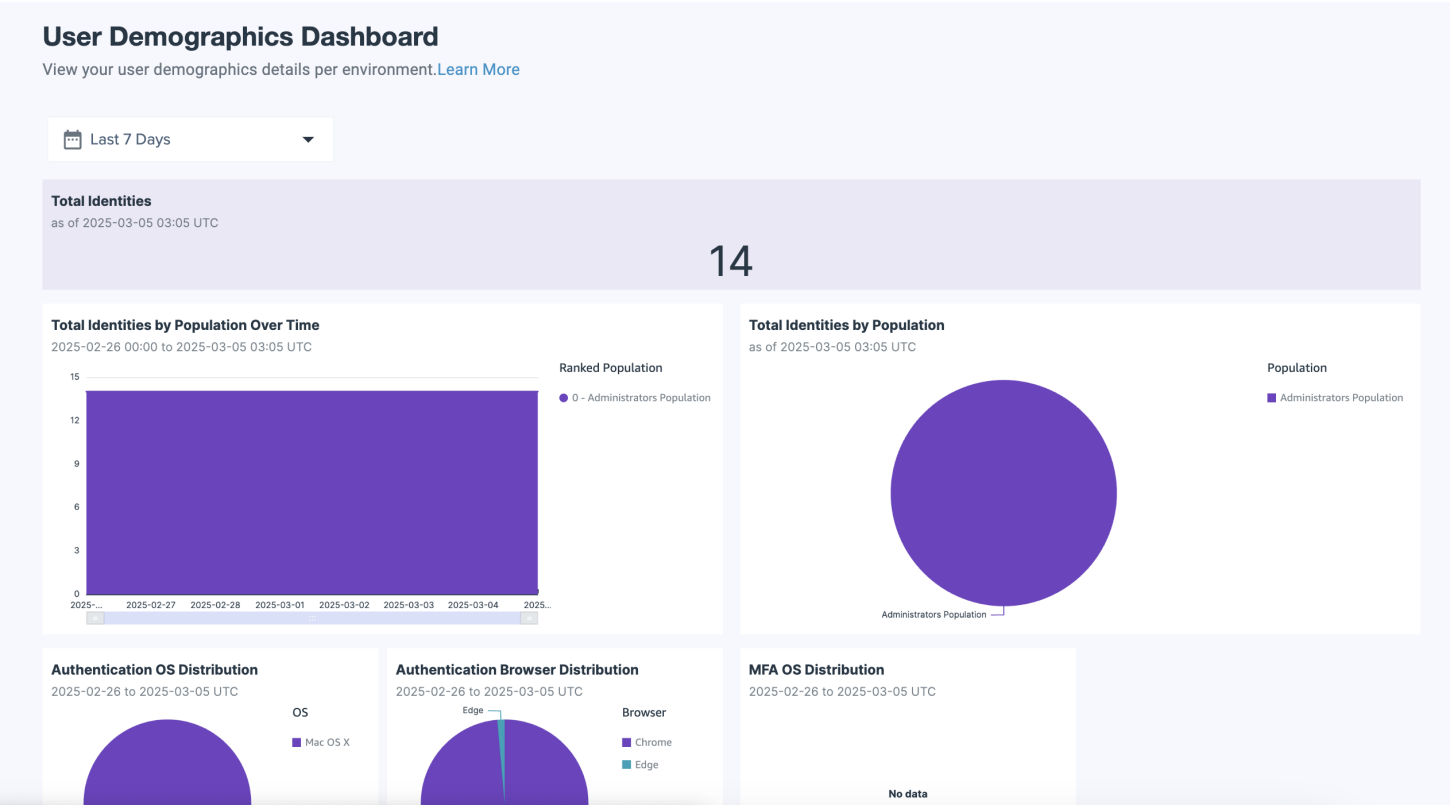
Hover over the map to see the actual average of sign-ons to more accurately quantify the variation between periods. You can use this information to better understand users' habits as well as identify periods of interest, such as typical highs and lows.

User Demographics Dashboard

The **User Demographics Dashboard** shows a summary of user demographic profiles and activity for the selected environment.

To access the **User Demographics Dashboard**, in the PingOne admin console, go to **Monitoring > User Demographics**.

Copyright © 2025 Ping Identity Corporation



Filters

You can limit the data to:

- **Today**
- **From Yesterday**
- **Last 7 Days** (Default)
- **Last 30 Days**
- **Last 90 Days**
- **This Month**
- **Last Month**
- **Custom Range**

> **Note**
>
> Data older than 180 days is not available for filtering. You can only select dates within a 6 month window.
> The charts are always shown in UTC time, regardless of the selection.

Charts

Use the following controls to adjust the charts:

Icon	Name	Description
	Maximize	Expands the chart to fill the dashboard. To minimize the chart, click the icon again.
	Menu options	Options can vary for different types of charts: • **View summary data**: Displays chart data as a table. • **Export to CSV**: Exports chart data to CSV or Excel format, depending on the type of chart.

Total Identities

Displays the total count of identities in the environment at the current date and time.

> **Note**
> The **Total Identities** and **Total Identities by Population** charts are not affected by the date filter. They always display current data, regardless of the selected date range.

Total Identities by Population Over Time

Displays the daily changes in the total count of identities, broken down by population groups over time. This chart shows how the identity count changes, indicating trends in different populations.

The top 10 populations by number display in the chart distribution. All other populations are cumulatively counted under **Other**.

Total Identities by Population

Displays the current distribution of identities by population.

Authentication OS Distribution

Displays the distribution of authentication attempts by the operating system for the selected time period.

> **Note**
> Updates for **Authenticate OS Distribution** and **Authenticate Browser Distribution** happen once a day at midnight, UTC. Depending on your time zone, these updates might not be visible for you at the end of the day.

Authentication Browser Distribution

Displays the distribution of authentication attempts by browser distribution for the selected time period.

> **Note**
> **Authentication OS Distribution** and **Authentication Browser Distribution** charts only display data for single sign-on (SSO) and do not include multi-factor authentication (MFA). The MFA dashboard has the mobile Authentication OS distribution chart.

DaVinci OS Distribution

Displays the distribution of DaVinci usage by operating system for the selected time period.

Copyright © 2025 Ping Identity Corporation

DaVinci Browser Distribution

Displays the distribution of DaVinci usage by browser for the selected time period.

Protect OS Distribution

Displays the distribution of successful Protect risk evaluations by Operating System for the selected time period.

Protect Browser Distribution

Displays the distribution of successful Protect risk evaluations by browser distribution for the selected time period.

MFA OS Distribution

Displays the distribution of MFA attempts by operating system for the selected time period.

MFA dashboard

The MFA dashboard shows a summary of current user activity for the selected environment.

You can limit the data to a specific time range, such as the current day, the past week to date, the past month to date, or the past six months.

The graph at the top of the page shows MFA activity at a glance, including the number of successful and failed authentications for the specified period.

Click any of the dashboard charts for a more detailed display with filters.

Chart Name	Description
Enrollments chart	Total enrolled new users
Enrollments by type chart	Distribution of enrolled new users by authentication type
SMS/Voice chart	Usage and cost breakdown of SMS and voice authentications and enrollments
User Devices	User devices by authentication method, and mobile app users by app version
Authentications by type chart	Distribution ratios of authentications by authentication type

MFA dashboard chart types

The charts are all interactive. You can:

- Hover over any colored area of a pie or bar chart to see additional details.
- Move the pointer horizontally on a line chart to see the plotted value.
- Click on the period bar to change the reporting period: Last year, last 6 months, last month, last week, or last day.

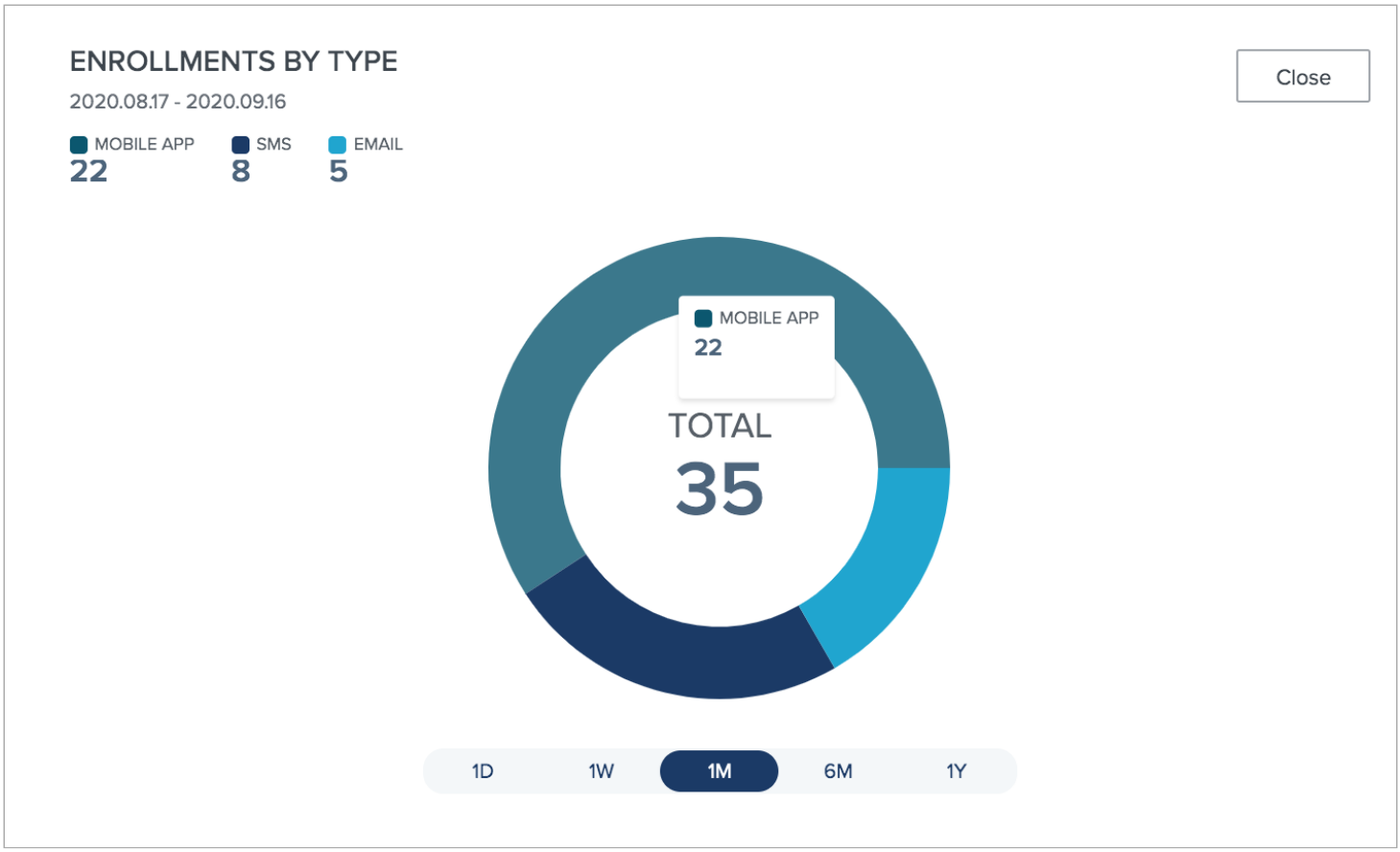
Copyright © 2025 Ping Identity Corporation

- Use a filter to change a chart appearance. The diagrams below and in subsequent sections are representative examples. Try the filters to see what works best for you.

Filtered charts offer additional information. Typical cases are shown below.

Pie charts

If you hover over a colored segment of the chart, the underlying value appears.



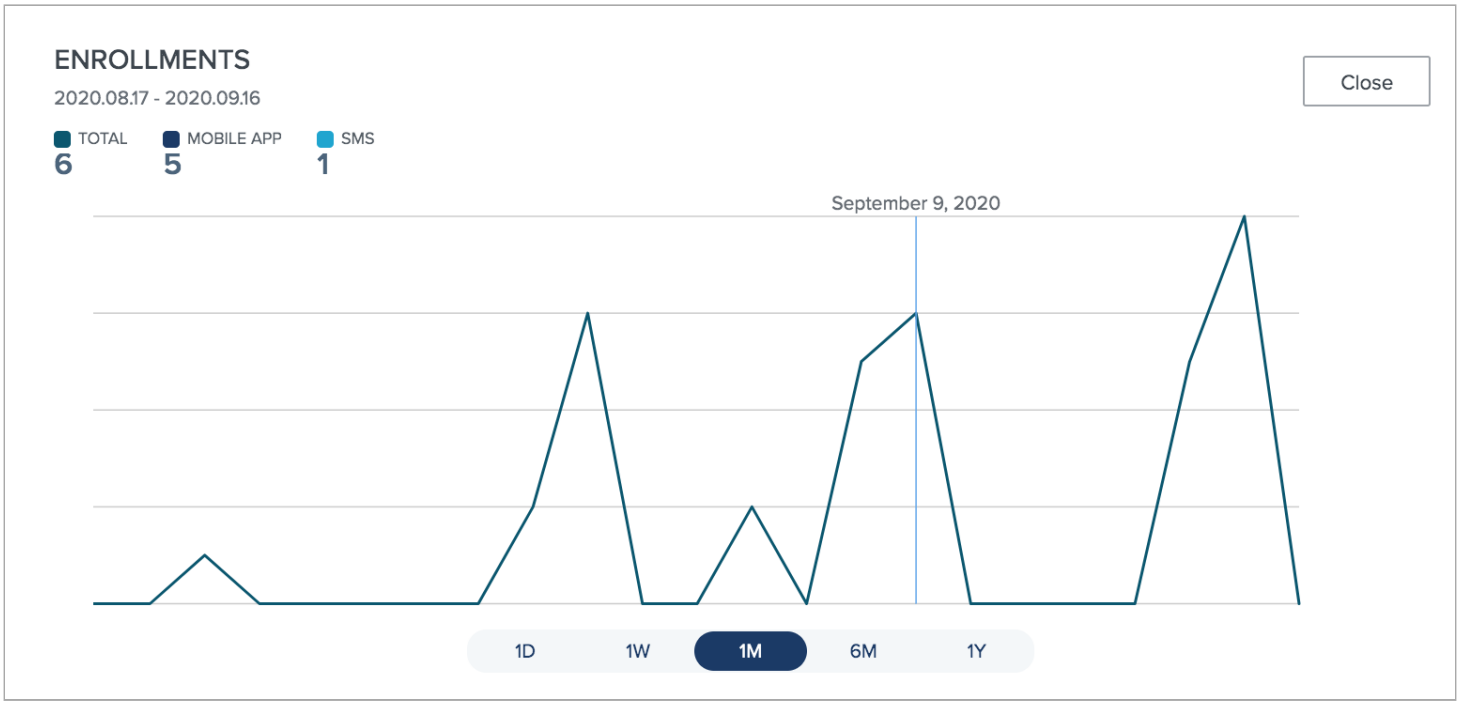
Bar charts

If you hover over a bar, you'll see a vertical line showing that it has focus and an underlying value. At the top left, the values narrow down to those of the focused date. For example:

Copyright © 2025 Ping Identity Corporation

Line graphs

If you move the pointer horizontally, you see a vertical line at a date point, and the date is displayed. At the top left, the values narrow to those of the focused date. For example:



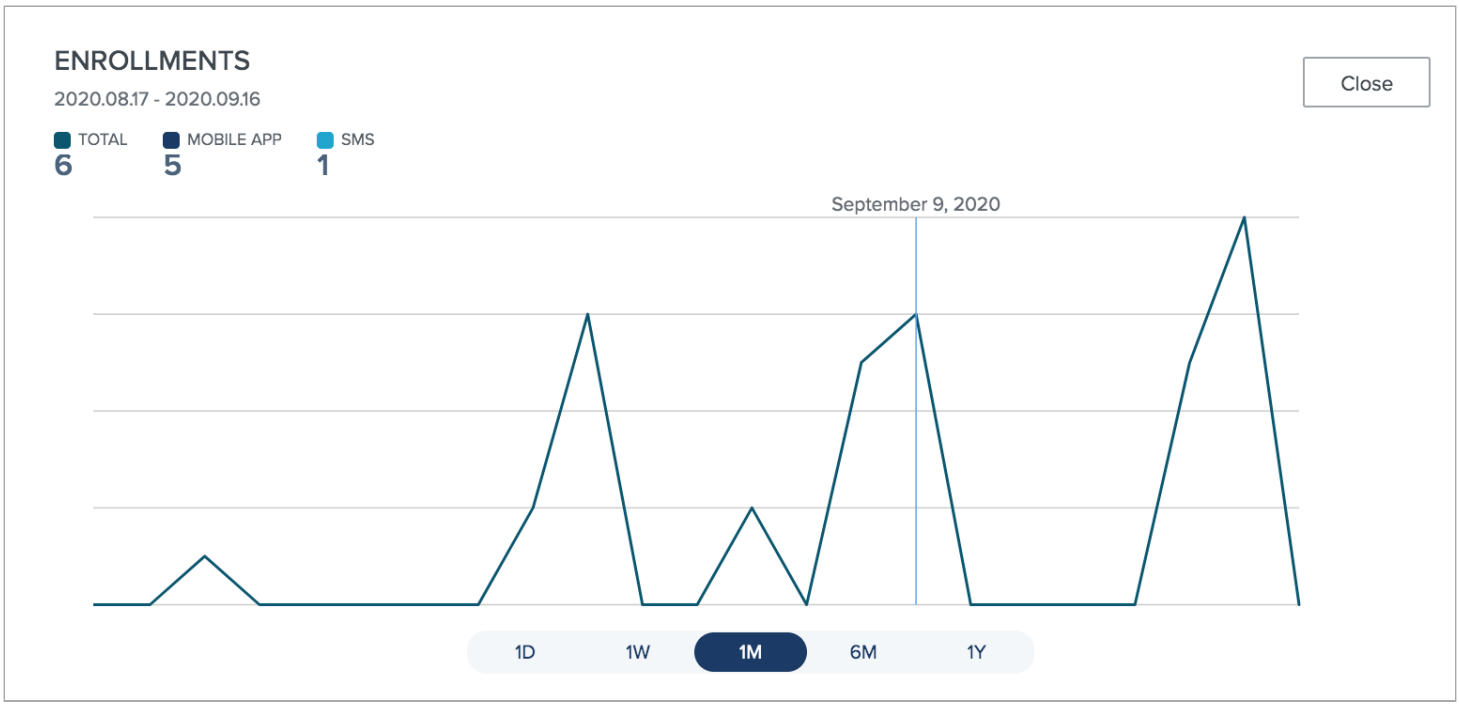
Copyright © 2025 Ping Identity Corporation

PingOne MFA Dashboard - disclaimer

- Data displayed on the **SMS/Voice** chart is based on SMS and voice calls sent by the Twilio or Syniverse service. Data is aggregated based on Twilio or Syniverse report logs and represented with an approximation of the cost. Some differences could apply between chart data and the final billing amount.
- PingOne does not provide SMS/Voice costs data for custom provider accounts that are not natively supported (unlike Twilio and Syniverse that are natively supported).
- Data refresh rate is subject to a 15-minute delay.

Enrollments chart

The **Enrollments** chart shows the number of new enrollments over the specified period.



The following filters are available:

Authentication method

Select or clear the authentication method check boxes to view enrollment data for specified authentication methods.

iOS/Android

Select or clear the **iOS** or **Android** check boxes to view enrollment data for specified mobile platforms.

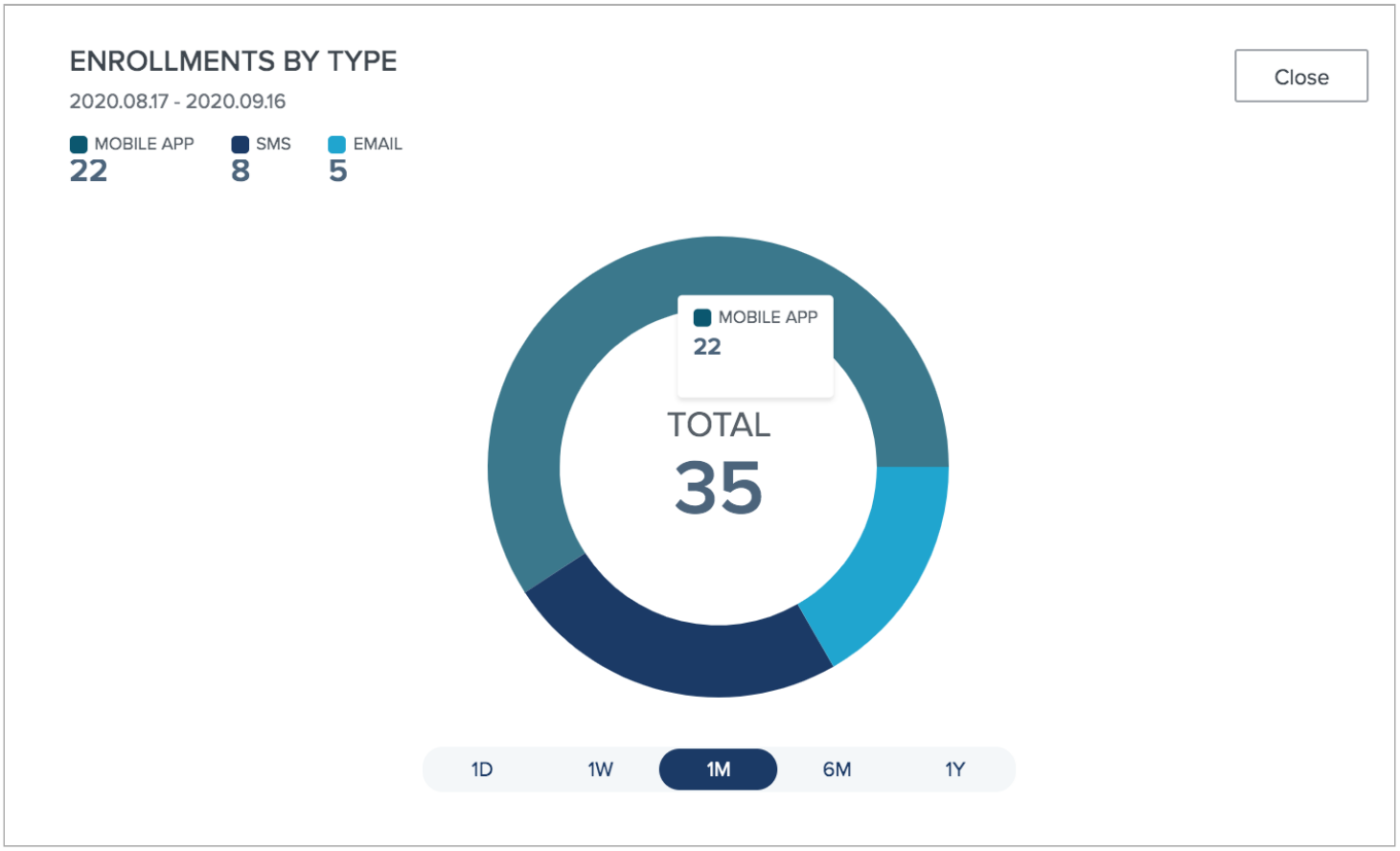
Date range

Enter the **Start date** and **End date** to view enrollment data for a specified date range. The default dates are the day, week, month, or six month period selected.

Copyright © 2025 Ping Identity Corporation

Enrollments by type chart

The **Enrollments by type** chart shows the distribution ratios of new enrollments by authentication type, for the specified period.



The following filters are available:

Authentication method

Select or clear the authentication method check boxes to view enrollment data by authentication type, for the specified authentication methods.

iOS/Android

Select or clear the **iOS** or **Android** check boxes to view enrollment data by authentication type, for the specified mobile platforms.

Amount/Percent

Select either:

- **Amount** to view the number of enrollments per authentication type.
- **Percent** to view the enrollments per authentication type as percentages of the total.

Copyright © 2025 Ping Identity Corporation

Date range

Enter the **Start date** and **End date** to view enrollment data for a specified date range. The default dates are the day, week, month, or six month period selected.

SMS/Voice chart

The **SMS/Voice** chart shows the usage and cost breakdown of SMS and voice authentications and enrollments, for the specified period.

The following filters are available:

Cost/Usage

Select one or both:

- **Cost** to view the costs of successful or failed SMS and voice authentications or enrollments.
- **Usage** to view the number of successful or failed SMS and voice authentications or enrollments.

SMS/Voice

Select one or both:

- **SMS** to view the costs or usage of SMS authentications or enrollments.

Copyright © 2025 Ping Identity Corporation

- **Voice** to view the costs or usage of voice authentications or enrollments.

Success/Failure

Select one or both:

- **Success** to view the costs or usage of successful SMS and voice authentications or enrollments.
- **Failure** to view the costs or usage of failed SMS and voice authentications or enrollments.

Notification Type

Select one of the following:

- **Authentication** to view the costs or usage of successful or failed SMS and voice authentications.
- **Registration** to view the costs or usage of successful or failed SMS and voice enrollments.
- **General** to view the costs or usage of successful or failed SMS and voice notifications sent by the PingOne Notifications Connector.
- **All**: View the cost or usage of successful or failed SMS and voice notifications for all notification types.

Country

Select a specific country or **All** countries to view the specified usage or cost breakdowns of SMS and voice authentications or enrollments for the period.

Date range

Enter the **Start date** and **End date** to view enrollment data for a specified date range. The default dates are the day, week, month, or six month period selected.

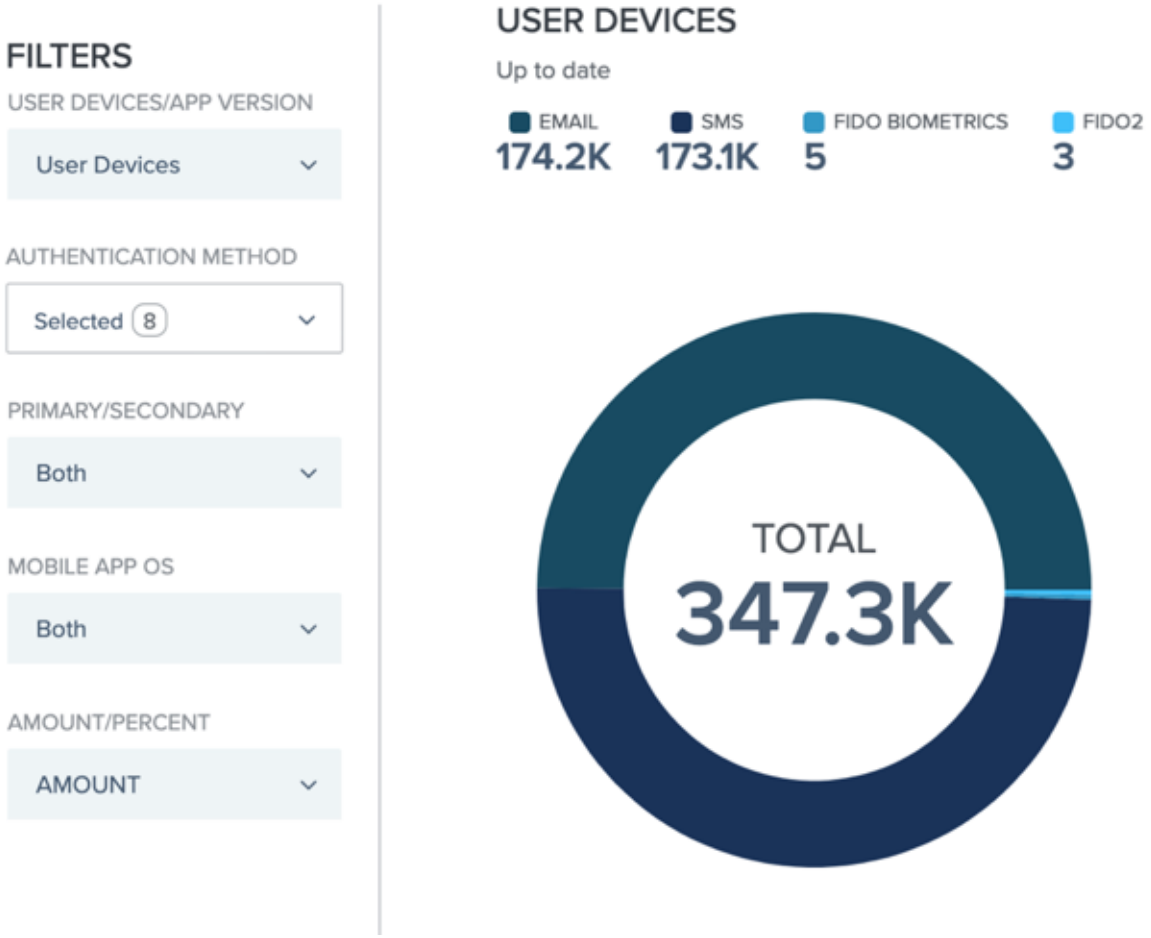
User devices and app version charts

The **User Devices** chart enables you to view current information for user devices per authentication method, and mobile app users per app version.

Use the **User Devices/App Version** filter to select the chart type that you want to view.

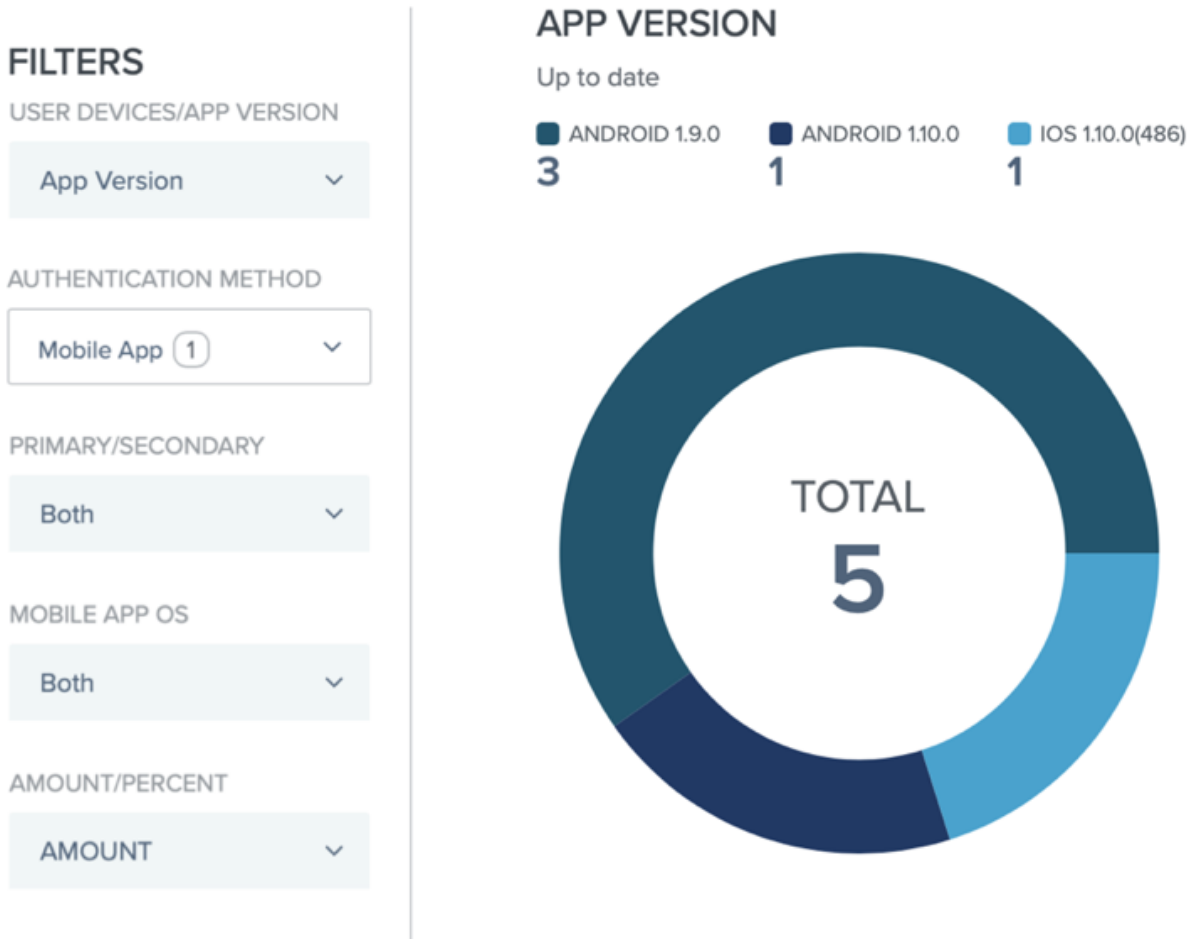
User Devices chart: view devices used by authentication method.

Copyright © 2025 Ping Identity Corporation



App Version chart: view mobile applications by version.

Copyright © 2025 Ping Identity Corporation



The filter options available vary depending on which chart you select:

Authentication method

Select the authentication methods you want to include in the results. For the App Version chart, only **Mobile app** is relevant.

Primary/Secondary

- **Primary** to view data for devices defined as the user's primary device only.
- **Secondary** to view data for devices defined as the user's secondary devices only.
- **Both** to include both primary and secondary devices.

Mobile app OS

View data per mobile OS. Select either:

- **iOS** to view data for iOS devices only.
- **Android** to view data for Android devices only.
- **Both** to view data for iOS and Android devices.

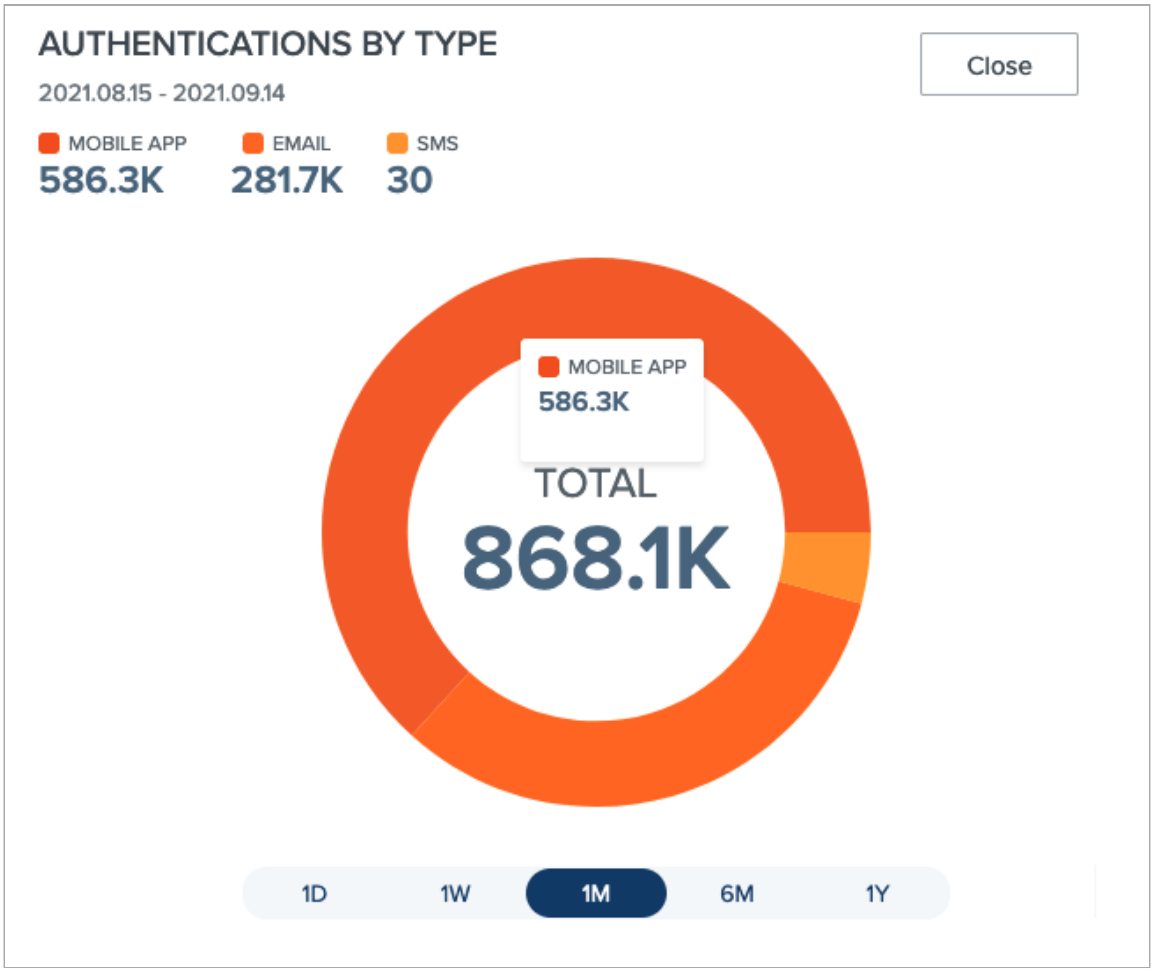
Copyright © 2025 Ping Identity Corporation

Amount/Percent

View data by either the number of devices, or the percentage of the total number of devices.

Authentications by type chart

The **Authentications by type** chart shows the distribution ratios of authentications by authentication method, for the specified period.



The following filters are available:

Authentication method

Select or clear the authentication method check boxes to view authentication data by authentication method, for the specified methods.

Success/Failure

Select one or both:

- **Success** to view successful authentications.
- **Failure** to view failed authentications.

Copyright © 2025 Ping Identity Corporation

iOS/Android

Select or clear the **iOS** or **Android** check boxes to view authentication data by authentication method, for the specified mobile platforms.

Amount/Percent

Select either:

- **Amount** to view the number of authentications per authentication method.
- **Percent** to view the authentications per authentication method as percentages of the total.

Date range

Enter the **Start date** and **End date** to view authentication data for a specified date range. The default dates are the past day, week, month, six month, or year period selected.

Audit

PingOne logs all actions performed in the admin console. Go to **Monitoring** > **Audit** to view a summary of these actions.

You can limit the results to include only a specified time range and time zone, and define which items to include in the report. PingOne keeps audit logs for 90 days by default.

To retain PingOne data for longer than 90 days, set up webhooks to stream the data to your own repository and configure your own retention policy. Learn more in Webhooks.

Historical dashboard data and administration configuration change data is retained for two years. Additionally, PingOne DaVinci and DaVinci flow data is not governed by this retention policy.

Learn more about auditing in PingOne in Running an audit report and Audit parameters.

You can find more information about PingOne logging and reporting capabilities in PingOne Platform logging and reporting.

Running an audit report

You can run reports to see a summary of actions performed in the PingOne admin console.

> **Note**
>
> You can find a complete list of events logged in PingOne in Audit Reporting Events in the PingOne API documentation.

Steps

1. In the PingOne admin console, go to **Monitoring** > **Audit**.
2. Enter the report parameters:
    - **Time Range**: Limit the report results to a specified range of time.
    - **Filter type**: Limit the results to a particular type, user, or resource.

Copyright © 2025 Ping Identity Corporation

- **Selected fields**: Specify which columns appear in the results list.
- **Time zone**: Specify the time zone to be used for the results list. The timestamp shows the date and time for the selected time zone.
- **Secondary Filter Type**: Specify a secondary filter to limit the results to a particular type, user, or resource. You must specify a primary filter type before you can select a secondary filter type.

3. Click **Run**.

Next steps

To rearrange the columns in the report summary, drag the column heading to the desired position.

To view the details of an event, click **View** in the **Details** column.

Audit parameters

Use audit parameters to specify the details of your search results.

Time Range

Relative

A time range relative to the current time. Under **Within**, select a number and a time period. For example, **3 weeks**.

Specific date

A time range with a specified start and end date, such as “March 27 to April 10.”

Filter type

Limit the search results based on the specified parameters.

Resource ID

Find activities by resource ID.

Correlation ID

Find activities by correlation ID. When an HTTP request is received, it is assigned a correlation ID. You can use the correlation ID to associate HTTP responses with messages in the event log.

Event type

Find activities by event type. Select an event type from the list. You can find a complete list of events logged in PingOne in Audit Reporting Events in the PingOne API documentation.

User ID (Actor)

Find activities that were performed by a particular user, by user ID.

Copyright © 2025 Ping Identity Corporation

User name (Actor)

Find activities that were performed by a particular user, by user name.

Client (Actor)

Find activities that were performed by a particular client. Select a client from the **Filter** list. The list of clients varies depending on your configuration.

Resource population

Find activities that were performed in resources within a particular population. Select a population from the list.

Resource type

Find activities that were performed on a particular type of resource. Select a resource from the list.

Population

Find activities that were performed on a particular population.

User

Find activities that were performed on a particular user.

Application

Find activities that were performed by a particular client application.

Selected fields

Specify which fields appear in the results list.

Timestamp

The date and time of the event. The format is: MM/DD/YYYY HH:mm:ss.

Event name

A unique identifier for the event.

Description

A brief description of the event.

Client

The client that performed the event.

User identity

The user for which the event was performed.

Population

The population for which the event was performed.

Copyright © 2025 Ping Identity Corporation

Resource type

The type of resource for which the event was performed.

Secondary filter type

Specify a secondary filter for your results.

> **Note**
>
> You must specify a primary filter type before you can select a secondary filter type.

Alerts

PingOne can deliver alert messages based on the status of certain resources.

Because alerts are configured per environment, you can have different alerts for different environments, such as staging and production. PingOne filters duplicate alerts so that administrators don't receive multiple redundant alerts.

PingOne supports a number of alert types, including certificate and key expiration alerts, user license limit alerts, and so on. For a complete list of alerts, go to **Monitoring → Alerts → +** in the PingOne admin console.

See:

- Viewing alerts
- Adding an alert
- Editing an alert
- Deleting an alert

Learn more about all logging and reporting capabilities in PingOne, in PingOne Platform logging and reporting.

Viewing alerts

Use the **Alerts** page to view and manage alerts for your current environment.

Steps

1. Go to **Monitoring** > **Alerts**.

   The **Alerts** page shows the alerts that are currently configured for your environment.

2. Browse or search for the alert that you want to view, and click an alert entry to open the details panel.

   The alert details panel shows the following:

   #### *Include alerts*

   The event types that will trigger the alert.

Copyright © 2025 Ping Identity Corporation

Email Addresses

The email addresses to which the alert will be sent.

Send Via

The alert channel to be used to deliver the alert. Currently, only email is supported.

Adding an alert

To enable alerts, you must configure an alert for the current environment. An alert includes information about which events trigger an alert and which email addresses will receive the alert.

Steps

1. Go to **Monitoring** > **Alerts**.
2. Click the **+** icon and configure the following:
   - **Name**: A unique name for the alert.
   - **Email Addresses**: The addresses to which the alert will be sent. You can specify individual email addresses or mailing lists.

     > **Tip**
     > If you have entered multiple email addresses, you can copy them to the clipboard after saving a new rule or when viewing an existing alert so that you can use them for additional rules that you want to create.

   - **Alert Types**: Select the event types that will trigger the alert.

     > **Note**
     > One of the triggers for the **Data Quality Issue** alert is the absence of data from the PingOne Signals (Protect) SDK. If you have activated this alert but have chosen not to implement the Signals SDK in your applications, you will occasionally receive email notifications regarding this missing data.

3. Click **Save**.

Editing an alert

Use the **Alerts** page to edit an existing alert.

Steps

1. Go to **Monitoring** > **Alerts**, and browse or search for the alert that you want to edit.
2. Click the alert that you want to edit to open the details panel.
3. Click the **Pencil** icon, and enter or edit the following:
   - **Name**: A unique name for the alert.

Copyright © 2025 Ping Identity Corporation

- **Email Addresses**: The addresses to which the alert will be sent. You can specify individual email addresses or mailing lists.

  > **Tip**
  >
  > Copy the email addresses to the clipboard if you want to use the same set of email addresses for a different alert.

- **Alert Types**: The event types that will trigger the alert.

4. Click **Save**.

Deleting an alert

Use the **Alerts** page to remove alerts that you no longer need.

Steps

1. Go to **Monitoring > Alerts**.
2. Locate the alert that you want to delete.
3. Click the details icon, and then click **Delete Alert**.
4. In the confirmation message, click **Delete**.

Copyright © 2025 Ping Identity Corporation

Directory

The **Directory** branch contains the **Users**, **Groups**, **Populations**, **User Attributes**, and **Administrator Roles** pages.

See:

Users

Groups

Populations

User Attributes

Administrator Roles

Users

Users are the unique identities that interact with the applications and services in the environment to which the user is assigned. You can use the **Users** page to manage users in your environment.

An identity is the full representation of a user profile, including the identity's relationships, roles, and attributes. If users are managed in an external identity provider, in PingOne MFA a user is a local instance of the unique identity that interacts with the applications and services of a specified environment.

Learn more

- Viewing users
- Searching for users
- Adding a user
- Editing a user
- Resetting a user password

Viewing users

Use the **Users** page to view and manage all users in your organization.

Steps

1. In the PingOne admin console, go to **Directory** > **Users** and browse or search for the user you want to view.

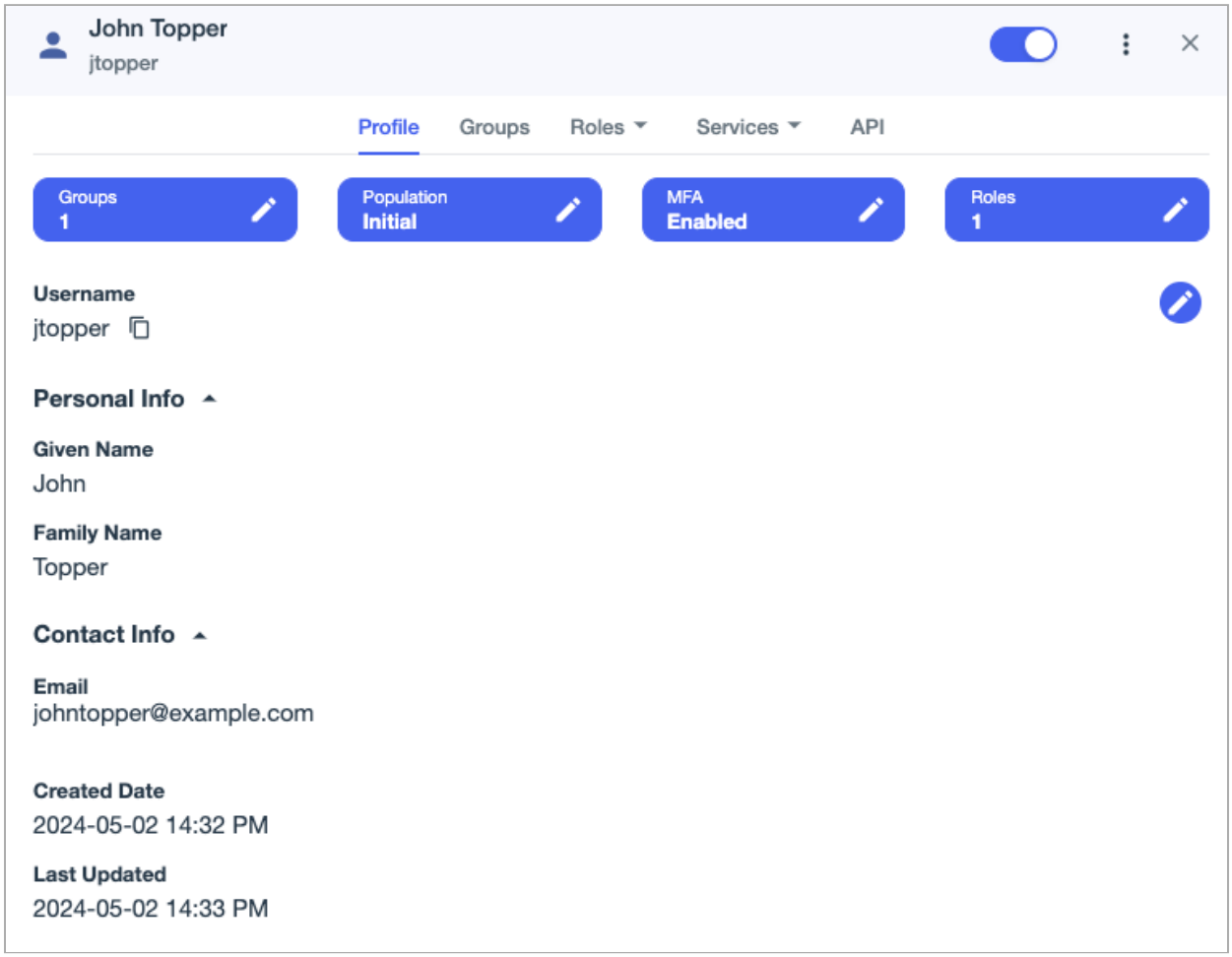
   You can narrow your search to a particular population. Learn more in Searching for users.

2. Click the user entry to open the user details panel.

Result

The user details panel shows specific information for the user.

Copyright © 2025 Ping Identity Corporation



Profile

Shows name, user name, and other contact information for the user. You can also see when the user identity was created and updated.

Groups

Shows group membership for the user. Learn more in Groups.

Roles > Administrator Roles

Shows the PingOne administrator roles that are currently assigned to the user. Administrator roles are collections of permissions for managing access to resources in the PingOne admin console, such as organizations, environments, and identities. Learn more in Administrator Roles.

Roles > Application Roles

Shows the application roles that are currently assigned to the user. In PingOne environments that include the PingOne Authorize service, application roles help you manage access to the application resources developed by your organization's engineering teams. Learn more in Application roles.

Copyright © 2025 Ping Identity Corporation

Services > Authentication

Shows details about authentication methods, as well as identity providers and linked accounts.

- **Status**: Shows whether MFA is enabled for the user.
- **Methods and devices**: Shows the authentication methods for the user, such as email, mobile, or SMS. You can see when an authentication method was paired, and remove or block a particular authentication method. If an end user has renamed an authentication method, it will appear here.
- **Authoritative identity provider**: Shows the current identity provider for the user and the origin of the user. The latter includes the information from the LDAP gateway, such as user type and password authority, if the user was migrated through it.
- **Sessions**: Shows current and recent sessions for the user. A session defines a set of user activity within PingOne applications. Learn more in Managing a user's sessions.
- **Linked accounts**: Shows any external accounts, such as Google or Apple, linked to the PingOne user account.

Services > Consent

Shows the most recent agreement to which the user has consented.

Services > Credentials

Use this tab to view or revoke a credential for the current user. Learn more in Managing a user's credentials.

Services > ID verification

If you have set up ID verification, use this tab to enable ID verification for the current user, reset the verification status, or manually approve a user. Learn more in PingOne Verify.

Services > Sync status

If you have set up provisioning for the user, this tab shows details about syncing with external identity stores. Learn more in Provisioning.

The following list shows the possible states for each identity:

- **Healthy**: The user account was successfully synced to the target identity store.
- **Partial sync**: The user account exists in the target identity store, but the user attributes were not fully synced. Ensure that the **Allow users to be updated** option is selected in the provisioning connection.
- **Not synced**: The user account does not exist in the target identity store. Ensure that the **Allow users to be created** option is selected in the provisioning connection.
- **Sync failure**: The user account was not synced to the target identity store because of an error. Check the configuration of the provisioning connection.

API

Shows user information in a format that is easy for application developers to use.

Copyright © 2025 Ping Identity Corporation

Searching for users

Use search parameters and filtering to find users in your organization.

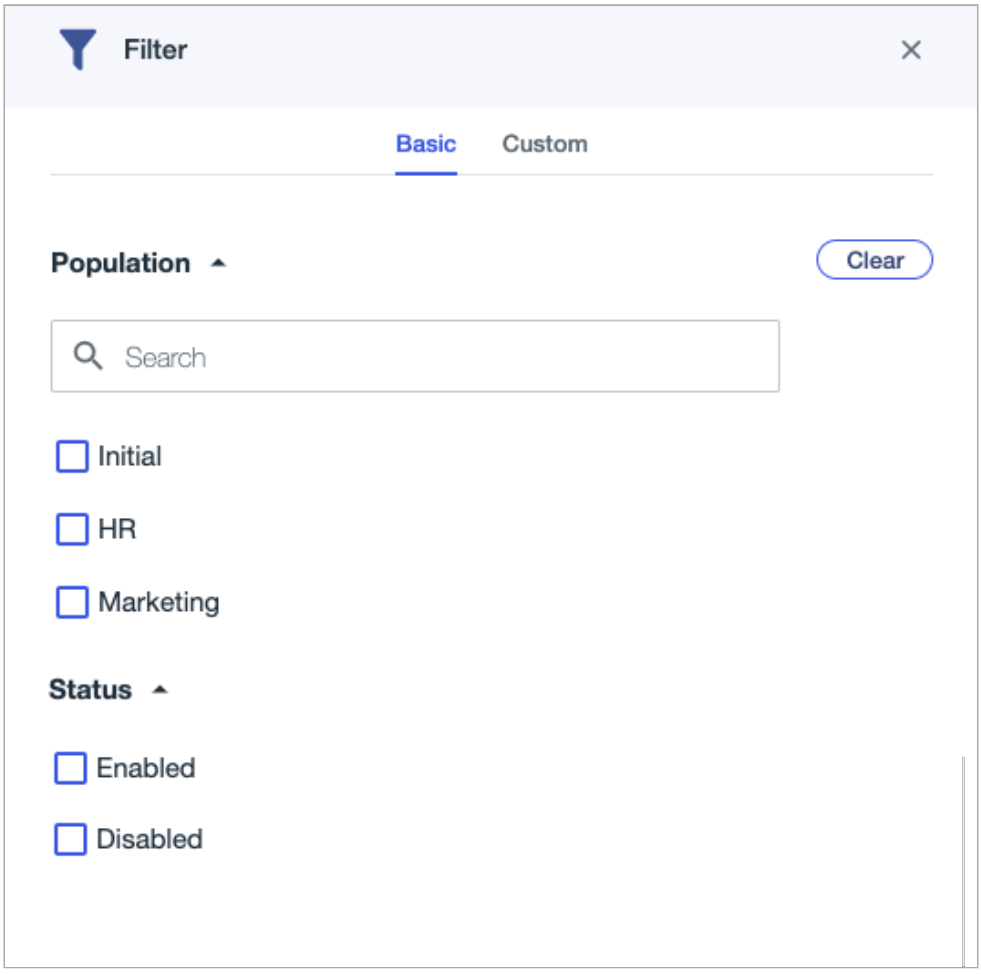
Searching for users

1. Go to **Directory → Users**.
2. In the **Search** field, enter the desired search terms. You can enter plain text or SCIM queries. For more information, see SCIM filter language.

The results list is updated as you enter the search query. You can sort the results by family name (last name), given name (first name), or time that the user was last modified.

Filtering on population or status

1. Go to **Directory → Users**.
2. In the **Search** field, enter the desired search terms.
3. To the right of the search box, click the Filters icon.



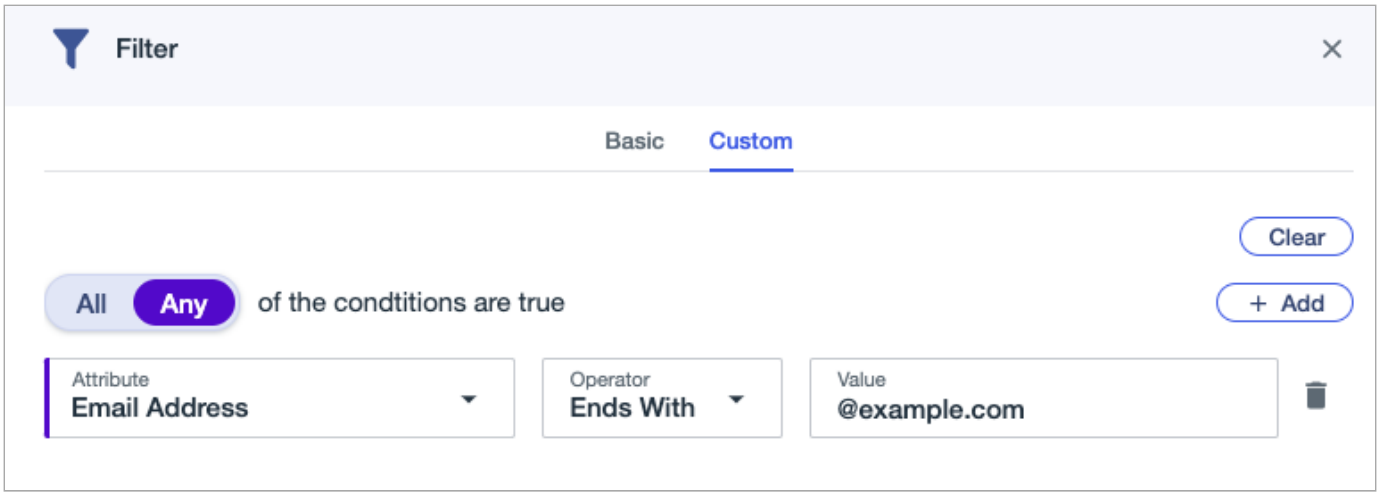
Copyright © 2025 Ping Identity Corporation

4. Do one or more of the following:
   - To filter by population, select one or more populations from the list.
   - To filter by status, select **Enabled** or **Disabled** from the list.
   - To clear all filters, click **Clear**.

The results list is updated as you enter the search query. You can sort the results by family name (last name), given name (first name), or time that the user was last modified.

Filtering on custom attributes

1. Go to **Directory → Users**.
2. In the **Search** field, enter the desired search terms.
3. To the right of the search box, click the Filters icon.
4. In the **Filter** panel, click the **Custom** tab.
5. Define the filter to specify the identities you are searching for. For more information, see Example user filters.



6. Enter the first condition:
   - Select **All** or **Any** to determine how the linked conditions will be evaluated: Boolean logical `AND` or `OR`.
   - **Attribute**. The user attribute to filter on.
   - **Operator**. Select `Equals`, `Starts with`, `Ends with`, or `Contains`.
   - **Value**. Enter the appropriate value.
7. If needed, click **+ Add** to add another condition or condition set.
8. Click **Apply**.

The results list is updated as you enter the search query. You can sort the results by family name (last name), given name (first name), or time that the user was last modified.

Copyright © 2025 Ping Identity Corporation

Viewing developer information for a user

You can use the API tab to access user information in a format that's easy for application developers to use. Use the PingOne admin console to access this information without having to make an API call.

1. Go to **Directory → Users**.
2. Locate the appropriate user. You can browse or search for users. See Searching for users.
3. Click the user entry to open the user details panel.
4. Click the **API** tab.

The API tab shows general information about the user, such as user ID, environment ID, and the URL at which the user data can be found. If a custom user schema is used, the data is available in JSON format. To access the data in JSON format, click **Copy to clipboard**.

Adding a user

Use the **Users** page to add users to the directory.

About this task

> **Important**
>
> In environments using PingFederate as the identity provider, adding a user in PingOne does not create the user in the PingFederate user directory. The ability to create a user in PingOne is provided as an option for MFA testing.

> **Note**
>
> If your environment is set up with custom user attributes, the user fields might not match the ones described here.

Steps

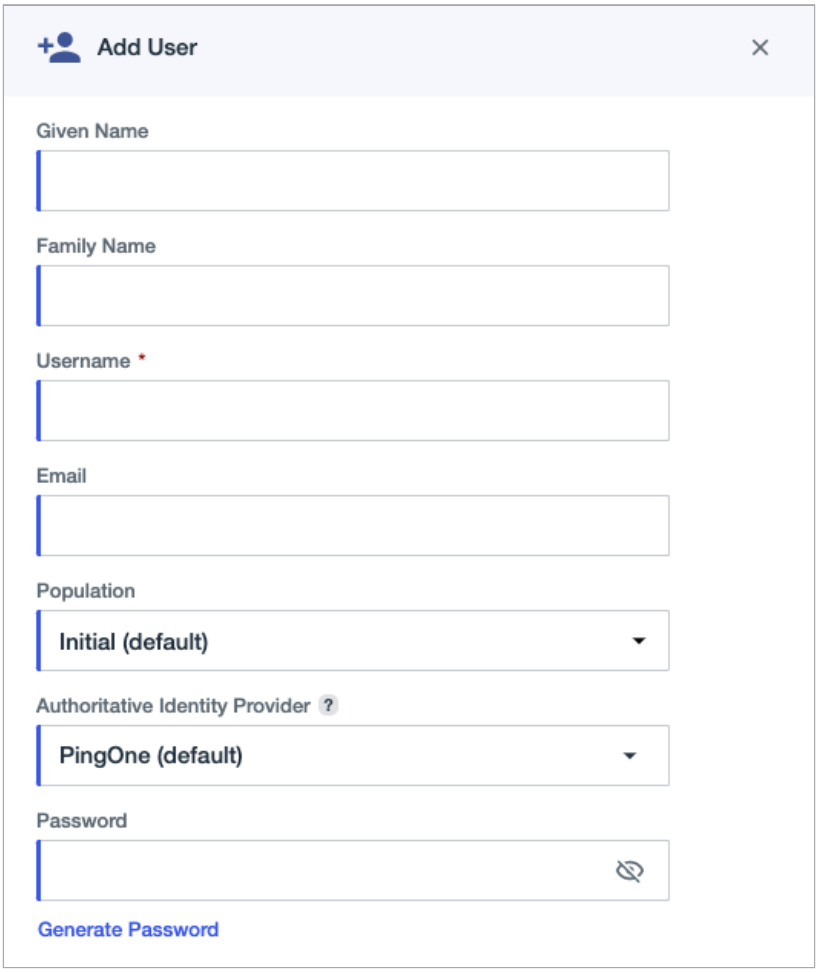
1. Go to **Directory → Users**.
2. Click the **+** icon.
3. Enter the following information.

Field	Description
Given name	The user's first name.
Family name	The user's last name.

Copyright © 2025 Ping Identity Corporation

Field	Description
Username	A unique identifier for the user. **Note** In a workforce environment, you cannot change usernames after they have been set. **Important** Do not use sensitive personal information (SPI) in usernames. SPI includes details such as political or religious affiliations, race, ethnicity, sexual orientation, medical or criminal history, and personal identification numbers such as Social Security numbers.
Email	A valid email address for the user.
Population	The population to which the user should belong. If you don't specify a population, the user will be added to the default population. For more information, see Populations.
Authoritative identity provider	If you have configured an external identity provider, select it from the list. An authoritative identity provider has authority over user records and credentials. For more information, see Authoritative identity providers.
Password	An initial password for the user. Click **Generate password** to have PingOne create a strong password for you. Click the eye icon to show the password in clear text.

Copyright © 2025 Ping Identity Corporation



4. Click **Save**.

Result

The user is created in the PingOne directory. You can edit a user profile after it has been created. See Editing a user.

Managing user roles

A role is a collection of permissions that you can assign to a user or group. Add, remove, or limit the scope of roles for PingOne users on the **Users** page.

You can manage two kinds of roles:

- Administrator roles grant access to specific PingOne capabilities. Learn more about the capabilities of each administrator role in Administrator Roles.
- Application roles grant access to features and API resources in applications developed by your organization. Learn more in Application roles.

Copyright © 2025 Ping Identity Corporation

Administrator roles

Assigning administrator roles

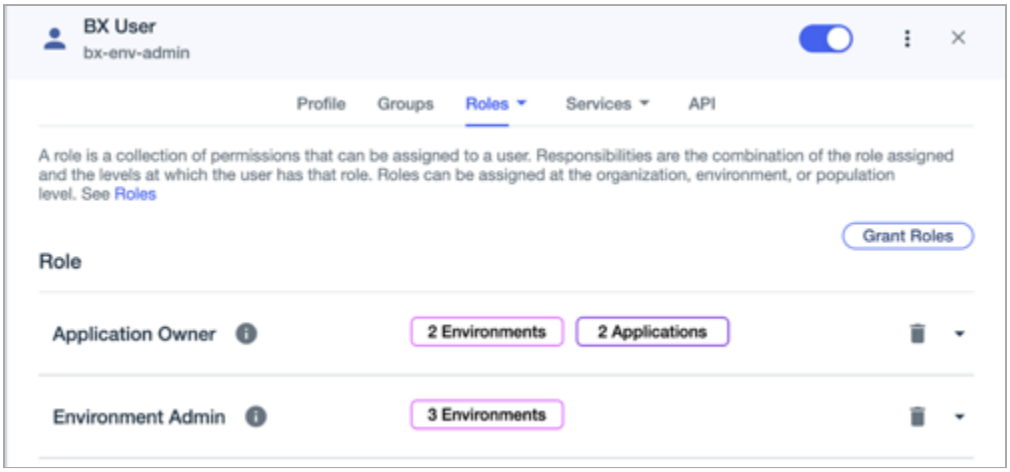
Assign administrator roles on the **Users** page in the directory.

Steps

1. Go to **Directory → Users** and browse or search for the user that you want to edit.
2. Click the user entry to open the user details panel.
3. Click the **Roles** > **Administrator Roles** tab.

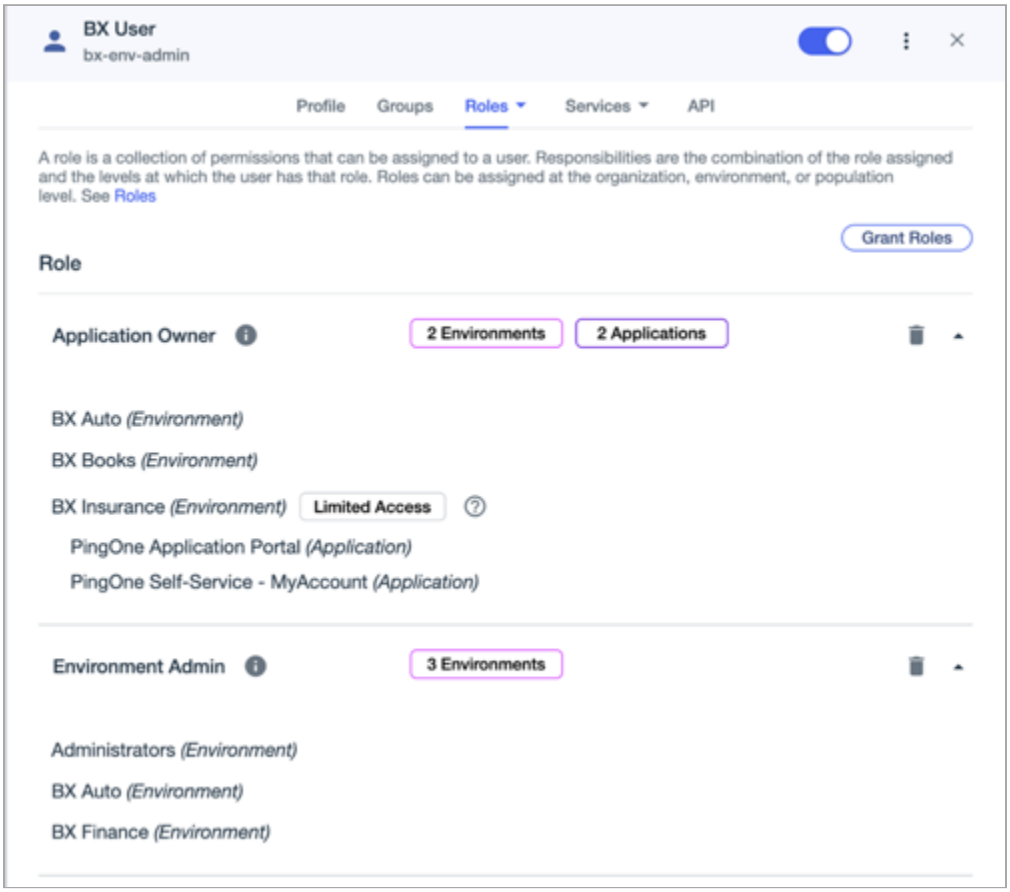
   If roles are assigned, they're listed here with information about where those roles apply. For example, in the following image, **BX User** has the **Application Owner** role in two environments. Because the role is assigned at the environment level, they have the role over all of the applications in those environments. In a third environment, they have the role over only two applications. They also have the **Environment Admin** role, and they have that role in three environments.

   > **Note**
   >
   > You can assign administrator roles to users, groups, applications, or PingFederate gateway integrations.



   > **Tip**
   >
   > Click the **Info** icon to view the permissions associated with the role. Click the down arrow on the right to view the list of environments or populations for which the role is assigned.

Copyright © 2025 Ping Identity Corporation



4. Click **Grant Roles**.

   The **Available Responsibilities** tab lists the roles that you are allowed to assign and the environments for which you are allowed to assign them. A responsibility is the combination of the role assignment and the level, or scope, at which the role is applied. Depending on the role, it could be assigned at the organization, environment, population, or application level.

   The **Granted Responsibilities** tab lists any roles that are currently assigned.

5. On the **Available Responsibilities** tab, click the role that you want to assign or change and perform any combination of the following:

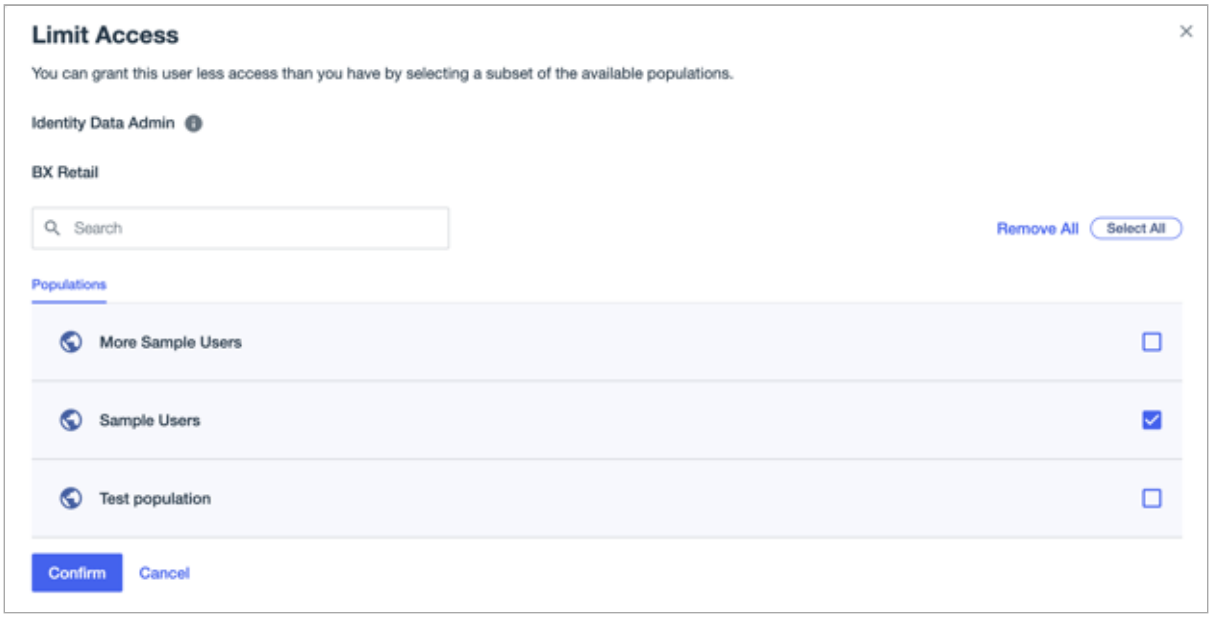
   1. To assign the role, select the checkboxes next to the applicable environments.

      > **Tip**
      >
      > Click **Select All** or **Remove All** to select or clear all available responsibilities.

   2. To remove a role assignment, clear the checkboxes next to the applicable environments.

   3. To grant this access for only a portion of the environment, click the **Reduce Access** icon ( ), select a subset of the available applications or populations on the **Limit Access** page, and click **Confirm**.

Copyright © 2025 Ping Identity Corporation



> **Note**
>
> You can grant only roles that are assigned to you or that confer the permissions needed to assign that role to others. For example, if you do not have the Environment Admin role, you cannot assign the Environment Admin role to others (and that role will not be listed under **Available Responsibilities**). However, if you have the Identity Data Admin role, you can assign either the Identity Data Admin role or the Identity Data Read Only role to others.
> Learn more about the permissions associated with each role in Roles.

6. Click **Save**.

Result

The role assignments that you selected are listed on the **Granted Responsibilities** tab.

Related links

- Administrator Roles

Copyright © 2025 Ping Identity Corporation

Application roles

Assigning application roles

Assign application roles on the **Users** page in the directory.

About this task

Follow these steps to assign application roles to users after you create application roles.

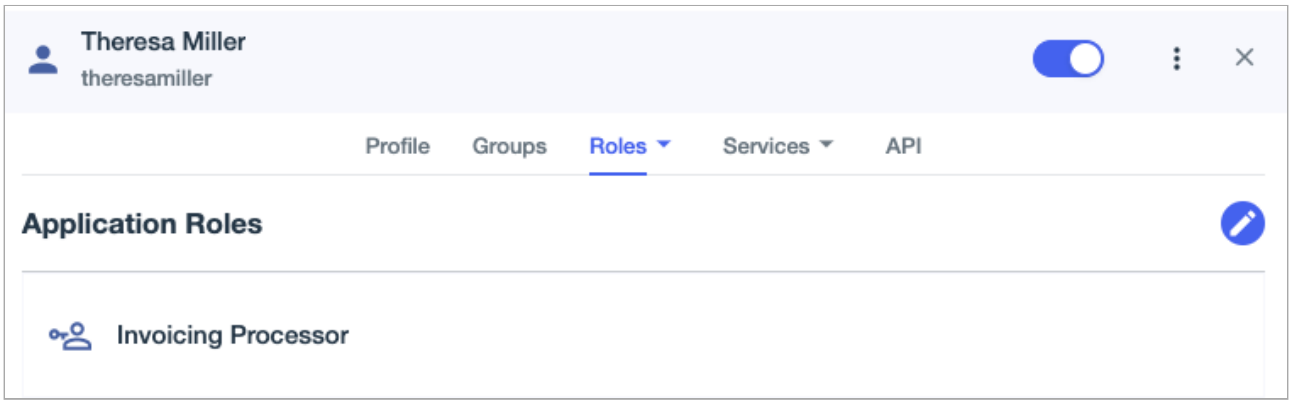
> **Note**
> The user assigning application roles must have the Identity Data Admin administrator role.

Steps

1. Go to **Directory → Users** and browse or search for the user to whom you want to assign a role.
2. Click the user entry to open the user details panel.
3. Click the **Roles → Application Roles** tab.

   If the user has assigned roles, they're listed here. For example, the image shows that **Theresa Miller** already has the **Invoicing Processor** role.

   > **Note**
   > You can assign application roles at the environment level.

4. Do one of the following.

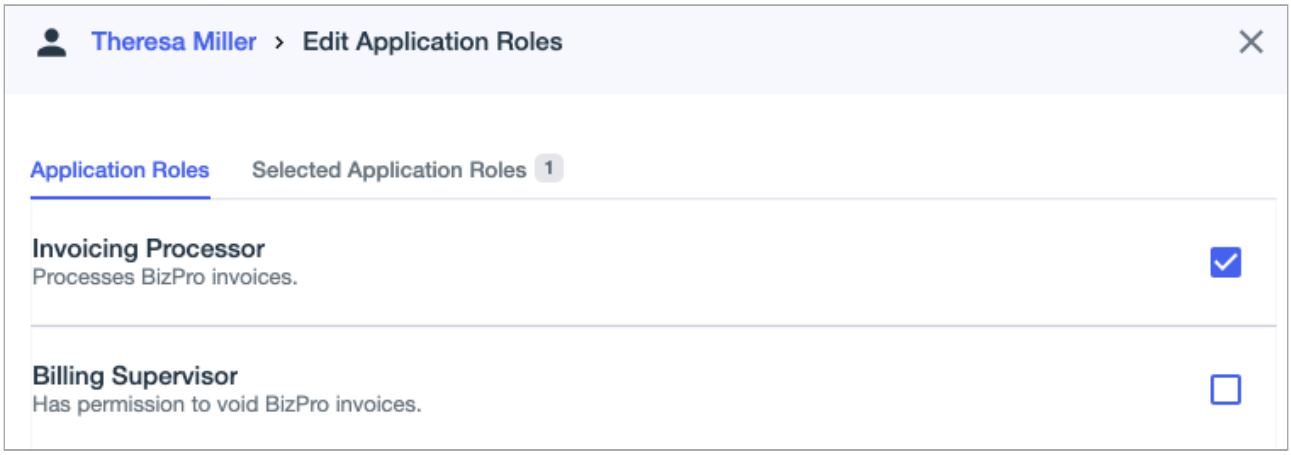
   Choose from:

   - If the user has assigned roles, click the **Pencil** icon.
   - If the user doesn't have assigned roles, click **Grant Application Roles**.

     Result:

     The **Application Roles** tab lists the roles that you can assign. The **Selected Application Roles** tab lists the roles, if any, that are currently assigned to the user.

Copyright © 2025 Ping Identity Corporation



5. On the **Application Roles** tab, select or clear the relevant checkboxes to assign or unassign roles.

   For example, you might assign Theresa the Billing Supervisor role while Melissa, the billing supervisor, is on vacation.

6. Click **Save**.

Editing a user

Use the **Users** page to edit users in the directory. The fields differ slightly based on your configuration.

Copyright © 2025 Ping Identity Corporation

Customer

Editing a user - Customer

Use the **Users** page to edit users in the directory.

Steps

1. In the PingOne admin console, go to **Directory** > **Users** and browse or search for the user that you want to edit.
2. Click the user entry to open the user details panel.
3. On the **Profile** tab, enter or edit the user's personal information, contact information, identity information, photo, or preferences.

   > **Important**
   > Do not upload photos that contain biometric data or other sensitive personal information. The PingOne directory doesn't support secure file storage for photos.

4. On the **Groups** tab, enter or edit group membership. Click **+ Add** to add the user to a group.

   Learn more in Groups.

5. Edit user roles.

   Choose from:

   - On the **Roles** > **Administrator Roles** tab, click the **Delete** icon to unassign roles that determine actions admins can take in PingOne. To assign a role, click **Grant Roles**.
   - On the **Roles** > **Application Roles** tab, click the **Pencil** icon or click **Grant Application Roles** to assign or unassign roles that determine access to features and API resources in applications developed by your organization.

     Learn more in Managing user roles.

6. On the **Services** > **Authentication** tab, enter or edit authentication information.
   - For **Multi-factor authentication**, click the toggle to enable or disable MFA.
   - Under **Methods and Devices**:
     - Click a device entry to show the date and time that the device was paired. If the device is a mobile device, and if logs have ever been sent from the device, the date, time, and Support ID of the most recent logs are shown.
     - To unpair a device, click the **More Options (⋮)** icon for the device and then select **Unpair**.
   - Under **Authoritative identity provider**, PingOne shows any configured external identity providers. To change the authoritative identity provider, click the **More Options (⋮)** icon and then select **Edit**.

     Learn more in Authoritative identity providers.

   - Under **Linked accounts**, PingOne shows any external accounts, such as Google or LinkedIn, that are linked to the user profile. To unlink an external account, click the **More Options (⋮)** icon and then select **Unlink**.
7. On the **Services** > **Consent** tab, view any agreements that the user has consented to.

Copyright © 2025 Ping Identity Corporation

8. On the **Services** > **Credentials** tab, if a user has a credential issued to them, view the credential and its status.

   Learn more in Managing a user's credentials

9. On the **Services** > **ID verification** tab (PingOne Verify only), PingOne shows verification status for the user. View the verification history, reset verification status, or manually approve a user.

   Learn more in PingOne Verify.

10. On the **Services** > **Sync status** tab, view the sync status for any provisioning connections.

    Learn more in Provisioning.

11. On the **API** tab, view technical information about the user, such as user ID, environment ID, and the URL at which the user data can be found.

Copyright © 2025 Ping Identity Corporation

Workforce

Editing a user - Workforce

Use the **Users** page to edit users in the directory.

> **Note**
>
> If you have a PingID account connected to your environment, the `Username` attribute cannot be edited.

Steps

1. Go to **Directory → Users** and browse or search for the user that you want to edit.
2. Click the user entry to open the user details panel.
3. On the **Profile** tab, enter or edit the user's personal information, contact information, identity information, photo, or preferences.

   > **Important**
   >
   > Do not upload photos that contain biometric data or other sensitive personal information. The PingOne directory doesn't support secure file storage for photos.

4. On the **Groups** tab, enter or edit group membership. Click **+ Add** to add the user to a group.

   Learn more in Groups.

5. Edit user roles.

   Choose from:

   - On the **Roles → Administrator Roles** tab, click the **Delete** icon to unassign roles that determine actions admins can take in PingOne. To assign a role, click **Grant Roles**.
   - On the **Roles → Application Roles** tab, click the **Pencil** icon or click **Grant Application Roles** to assign or unassign roles that determine access to features and API resources in applications developed by your organization.

   Learn more in Managing user roles.

6. In the **Services** list, select **Authentication** and enter or edit authentication information.

   - For **Multi-factor authentication**, click the toggle to enable or disable MFA.
   - To bypass MFA for SSO, under **Multi-Factor Authentication**, click **Allow MFA bypass** and then in the **Bypass** popup window, select the bypass duration and click **Bypass**.

     The bypass time remaining, and a **Resume** link are shown. Click **Resume** to resume MFA for the selected user.

   - Under **Methods and Devices**:

     - Click a device entry to show the date and time that the device was paired. If the device is a mobile device, and if logs have ever been sent from the device, the date, time, and Support ID of the most recent logs are shown.

Copyright © 2025 Ping Identity Corporation

        - To unpair a device, click the **More Options (⋮)** icon for the device and then select **Unpair**.

    - Under **Authoritative identity provider**, PingOne shows any configured external identity providers. To change the authoritative identity provider, click the **More Options (⋮)** icon and then select **Edit**.

  Learn more in Authoritative identity providers.

    - Under **Linked accounts**, PingOne shows any external accounts, such as Google or LinkedIn, that are linked to the user profile. To unlink an external account, click the **More Options (⋮)** icon and then select **Unlink**.

    - Under **Integrations**, select the services that should be enabled for the user. To disable or bypass a service, click the **More Options (⋮)** icon and then select **Disable** or **Bypass**. Bypassing a service suspends the need for a user to authenticate using the secondary authentication method for a specified amount of time.

7. On the **Services → Consent** tab, PingOne view any agreements that the user has consented to.

8. On the **Services → ID verification** tab (PingOne Verify only), PingOne shows verification status for the user. View the verification history, reset verification status, or manually approve a user.

   Learn more in PingOne Verify.

9. On the **Services → Sync status** tab, view the sync status for any provisioning connections.

   Learn more in Provisioning.

10. On the **API** tab, view technical information about the user, such as user ID, environment ID, and the URL at which the user data can be found.

Managing a user's devices and services

In environments that use multi-factor authentication (MFA), administrators can manage a user's MFA devices and service from the **Users** page.

About this task

From the **Users** page, you can remove a device, enable or disable a device, and bypass an authentication service. For example, you can bypass secondary authentication for a specified amount of time if a user loses or damages the MFA device that is paired with PingOne.

Steps

1. Go to **Directory → Users**.

2. Locate the user you want to edit. You can browse or search for users.

3. Click the user entry to open the user details panel.

4. Click **Services** and then **Authentication**.

5. Do one or more of the following:

Copyright © 2025 Ping Identity Corporation

Choose from:

- To change the default device, in the **Methods and Devices** section, locate the appropriate authentication method. Click the **More Options (⋮)** icon and then click **Make primary**.
- To show when the device was paired, locate the appropriate authentication method in the **Methods and Devices** section.
- To unpair a device, in the **Methods and Devices** section, locate the appropriate authentication method. Click the **More Options (⋮)** icon and then click **Unpair**.
- To block a device, in the **Methods and Devices** section, locate the appropriate authentication method. Click the **More Options (⋮)** ivon and then click **Block**. After you block a device, the **Block** option in the menu is replaced with an **Unblock** option.
- To bypass MFA:
  - To bypass MFA for SSO: In the **Multi-Factor Authentication** section, click **Allow MFA bypass** and then in the **Bypass** modal, select the bypass duration and click **Bypass**.

    The bypass time remaining and a **Resume** link are shown. Click **Resume** to resume MFA for the selected user.
  - (Workforce only) To disable a specific service, in the **Integrations** section, locate the appropriate service. Click the **More Options (⋮)** icon and then click **Disable**.
  - (Workforce only) To bypass a specific service, in the **Integrations** section. locate the appropriate service. Click the **More Options (⋮)** icon and then click **Bypass**. In the list, select the duration to bypass the service. After the specified time elapses, PingOne resumes the service automatically.
- To configure PingID settings, click **Configure Now**. Learn more about PingID settings in PingID User Life Cycle Management in the PingID documentation.

6. Click **Save**.

Managing a user's credentials

You can view and revoke a user's credentials from the **Users** page.

> **Note**
>
> Learn more about Creating a credential in PingOne Credentials.

Steps

1. In the PingOne admin console, go to **Directory > Users** and browse or search for the user that has the credential you want to view or revoke from.
2. Click the user entry to open the user details panel.
3. Click the **Services** tab and then **Credentials**.

   If a user has a credential issued to them, they're listed here with the following status:

   - **Active**: A credential is issued and appears in the digital wallet.

Copyright © 2025 Ping Identity Corporation

- **Pending**: A credential is issued but isn't in the digital wallet yet.
- **Revoked**: A credential is revoked and appears as revoked in the digital wallet.

4. (Optional) To revoke a credential:
    1. Next to the credential that you want to revoke, click the **More Options** (⋮) icon, and then click **Revoke**.
    2. Click **Revoke** in the **Revoke credential** dialog box.

User Devices report

You can view and export reports that list the details of MFA devices, such as the username and user ID associated with the device, using a number of device-related filters. For example, you can generate a report listing all email devices or a report containing all of the devices whose phone number starts with a certain country code.

Steps

1. In your PingOne environment, go to **Directory → Users**.
2. Click the **User Devices Report** button at the top of the page.

   Result:

   The table shows basic information for each device, such as the associated username and the device type.
3. Use the **Filter** button to filter the data displayed, based on one or more of the following criteria: device type, MFA status, user ID, email address, phone number. For email address and phone number, you can specify the whole address/number or use the **starts with** option. When you use the **equals** option, the search is case-sensitive. When you use the **starts with** option, the search is not case-sensitive.
4. If you want to export the displayed data to a file:
    1. Click **Generate Report**.
    2. Select **Generate CSV** or **Generate JSON**.
    3. When the export is finished, copy the displayed password, which you will need to open the `.zip` file that contains the requested output, and then click**Download CSV**/ **Download JSON**.

   The generated file is available for up to two hours. If you want to generate another report within this time period, change the filters applied to the data.

Enabling consent updates

To allow users to view and update their consents, an administrator must enable the `Manage OAuth Consents` option for the self-service application. Selecting this option enables the **Application** section under **Consents** and enables the end user to revoke any OAuth consent by showing the trash can icon for each consent.

Steps

1. Go to **User Experience → Self Service**.
2. Click the pencil icon.

Copyright © 2025 Ping Identity Corporation

3. Select the **Manage OAuth Consents** check box. Selecting this option enables the following two scopes for the self-service application.
    - `p1:read:oauthConsents` Allows the user to view their OAuth consents.
    - `p1:update:oauthConsents` Allows the user to revoke their OAuth consents.
4. Click **Save**.

Enabling end users to view consents

To allow end users to view their consents, but not revoke them, add the `p1:read:oauthConsents` scope to the self-service application.

Steps

1. Go to **Applications → Applications**.
2. Locate the **PingOne Self-Service - MyAccount** application, and click the application entry to open the details panel.
3. Click the **Resources** tab and then click the pencil icon.
4. Add `p1:read:oauthConsents` to the **Allowed scopes** column.
5. Click **Save**.

Viewing consents for a user

From the **Consents** tab, you can view the agreements that a particular user has consented to. Agreements can include terms and conditions, as well as permissions for an application. For example, an end user can allow an application to access their profile or email address.

Steps

1. Go to **Directory → Users**.
2. Locate the user you want to view. You can browse or search for users.
3. Click the user entry to open the user details panel.
4. Click **Services → Consent**.
5. Do one or more of the following:
    - To view a consent, locate the appropriate consent, and then click **Terms of service**.
    - To revoke a consent that the user has already agreed to, locate the appropriate consent, and then click the trash can icon. In the confirmation message, click **Revoke Access**.

Enabling or unlocking a user account or device

Learn how to enable a user's account. If a user account or device is locked or disabled, you can unlock it or enable it from the user details page.

Copyright © 2025 Ping Identity Corporation

About this task

A user account can have one or more authentication method or device paired with the account. A user's account can become locked, and sometimes the authentication method or device paired with the user's account can also become locked. This section describes how to unlock a user account, and any devices paired with the account.

- A user account can be locked out if a user has more than five incorrect password attempts within 15 minutes.
- A user account and the methods and devices associated with the account might be locked because of incorrect MFA authorization actions, such as entering an incorrect one-time password, or declining push confirmations on a mobile device. The duration of the device lock is defined by the MFA policy.

Tip

If an authentication methods or device is locked, a **Locked** icon is shown in the Method and Devices table in the relevant user's profile.

For information about user account lock settings, see Configuring MFA settings. For information about MFA device settings, see MFA policy.

To unlock an MFA method or device for a specific user:

Steps

1. Go to **Directory → Users**.
2. Locate the user you want to enable, disable, or unlock. You can browse or search for users.
3. In the user list, click the toggle to enable, disable, or unlock the user account.

Note

You cannot lock a user account manually, but you can disable it.

4. To unlock the MFA method or device for a specific user:
    1. In the user list, click the user entry.
    2. Click **Services → Authentication**.
    3. Next to the device that you want to unlock, click **More Options**, and then click **Unlock**.

Copyright © 2025 Ping Identity Corporation

Deleting a user

Use the **Users** page to remove user accounts that you no longer need. You can also disable a user account instead of deleting it. See Enabling or unlocking a user account or device.

Steps

1. Go to **Directory → Users**.
2. Locate the user you want to delete. You can browse or search for users.
3. On the right side of the user entry, click the three dots options menu and then click **Delete user**.
4. In the confirmation message, select the **I understand and want to continue** checkbox and then click **Delete**.

Managing user sessions

User sessions provide access to applications and resources in PingOne.

In a user's identity details, the **Authentication** tab shows recent user sessions with time, application (browser agent), device, and location.

Managing a user's sessions

About this task

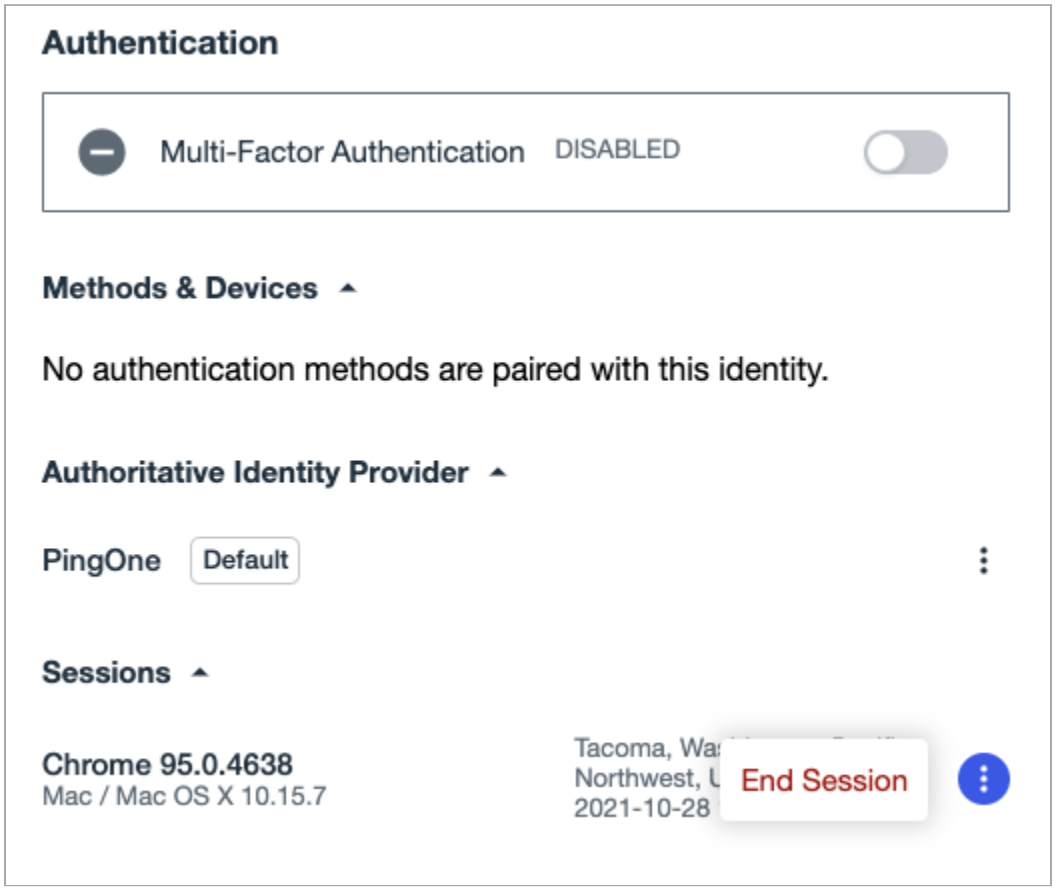
You can delete recent sessions for a particular user. Deleting a recent session will sign the user out of PingOne. You can delete a session if you detect suspicious activity, for example.

> **Note**
> You can't delete your own session if it is the current session. Sign off to end your current session.

Steps

1. Go to **Directory → Users**.
2. Locate the appropriate user. You can browse or search for users.
3. Click the user entry to open the user details panel.
4. Click **Services** and then **Authentication**.
5. Locate the appropriate session, then click the three dots options menu, and then click **End session**.

Copyright © 2025 Ping Identity Corporation



> **Note**
>
> If an administrator ends the current session for a user, the user might retain access to the self-service application until their current token expires. This is typically five minutes, but might be longer depending on how the token duration is configured.

Managing your own user sessions

Before you begin

Sign off to end your current session.

About this task

You can use the self-service application to manage your own sessions. You can delete your own sessions, but not the current session. You can delete a session if you detect suspicious activity, for example.

Steps

1. In the upper right corner of the page, click your name and then click **Profile**.
2. Click the **Accounts & Sessions** tab.
3. Locate the appropriate session.
4. Click **Sign off**.

Copyright © 2025 Ping Identity Corporation

Changing a user's population

Use the **Users** page to move a user to a different population.

Steps

1. Go to **Directory → Users**.
2. Locate the user that you want to move to a different population. You can browse or search for users.
3. Click the user entry to open the user details panel.
4. Under **Profile**, click **Population**.
5. In the **Population** list, select the new population for the user.
6. Click **Save**.

Verifying an email address for a user

For additional security, or to satisfy an authentication policy, you can require a user's email address to be verified.

About this task

To verify an email address, PingOne sends an eight-digit code to the specified email address. The user then enters the code into the PingOne self-service application to verify the address. Alternatively, developers can use the PingOne API to create a custom application for email validation. See POST Verify User in the PingOne Platform API Reference.

> **Note**
>
> Existing users will not be required to verify their email address, unless an admin has started the verification process. Start the verification process by clicking the **Verify email** link for a particular user. After an admin starts the verification process, the user details will show **Not verified** until the user finishes verification.

Steps

1. Go to **Directory → Users**.
2. Locate the appropriate user. You can browse or search for users.
3. Click the user entry to open the details panel.
4. On the right side, click the three dots options menu and then click **Verify email**.

   > **Note**
   >
   > If the user does not have an email address as part of their profile, the **Verify email** option will not appear.

Result

PingOne sends a verification code to the configured email address. The user can then use the verification code to verify their email address in the PingOne self-service application or custom application, if configured.

Copyright © 2025 Ping Identity Corporation

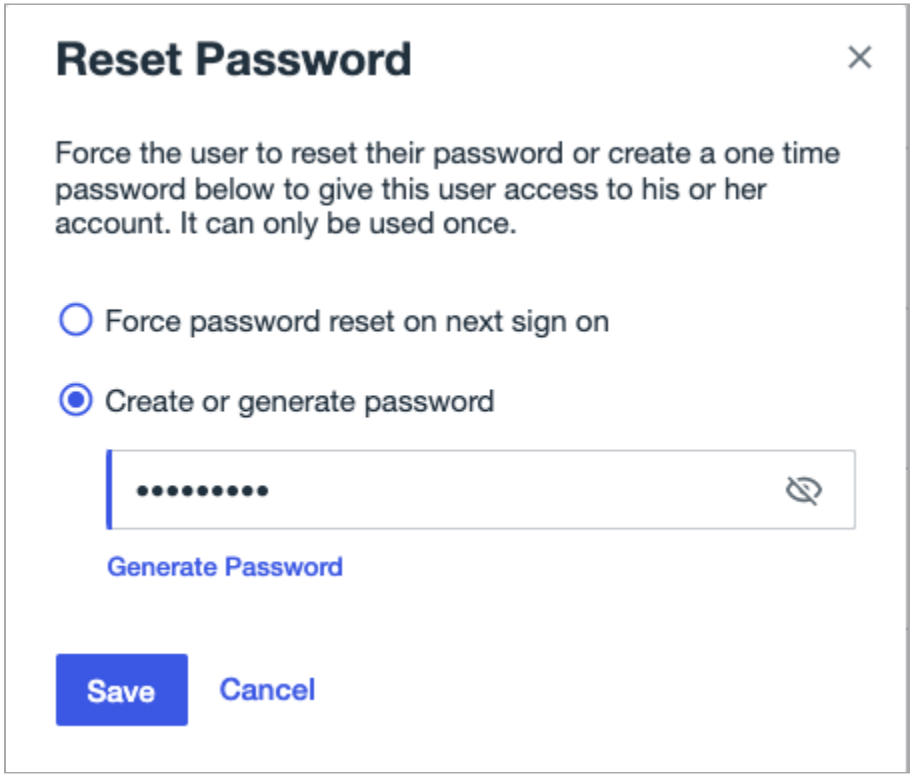
In the user details, the email address will appear as verified. If the user changes their email address, or if an admin starts the verification process again, the email address will have to be verified again.

Resetting a user password

Use the **Users** page to reset a user password. When you reset a user's password, you can create a new password for the user, or force the user to choose a new password the next time they sign on.

Steps

1. Go to **Directory → Users**.
2. Locate the user whose password you want to reset. You can browse or search for users.
3. On the right side of the user entry, click the three dots options menu and then click **Reset Password**.
4. In the **Reset Password** window, select one of the following:
   - **Force password reset on next sign on**. The user will be prompted to change their password the next time they sign on.
   - **Create or generate a password**. Enter a temporary password or click **Generate Password** to have PingOne create a secure password. Copy the password if needed.



5. Click **Save**.

Copyright © 2025 Ping Identity Corporation

SCIM filter language

The SCIM is an open standard for managing user identity information across applications or identity domains. You can use the SCIM filter language to build a user query.

The following example is a simple query to find a user by username:

```
username eq "christy"
```

You can join filter expressions by using the `and` and `or` operators and grouping them in parentheses. For example, to find all users who have a family name of `Smith` and a first name that starts with the letter `W`, use the following query:

```
(name.family eq "Smith") and (name.given sw "W")
```

For a full list of operators and supported attributes, see the following table.

Operator	Definition	Description
eq	equals	The attribute and operator values are identical. Supported attributes: • accountId • address.streetAddress • address.locality

Copyright © 2025 Ping Identity Corporation

Operator	Definition	Description
sw	starts with	The entire operator value is a substring of the attribute value, starting at the beginning of the attribute value. This criterion is satisfied if the two strings are identical. Supported attributes: • Custom attributes of type STRING • accountId • address.streetAddress • address.locality • address.region • address.postalCode • address.countryCode • email • enabled • externalId • locale • mobilePhone • name.formatted • name.given • name.middle • name.family • name.honorificPrefix • name.honorificSuffix • nickname • photo.href • preferredLanguage • primaryPhone • timezone • title • type • username
ew	ends with	The entire operator value is a substring of the attribute value, starting at the end of the attribute value. This criterion is satisfied if the two strings are identical. Supported attributes: • email • name.family • name.given
co	contains	The entire operator value is a substring of the attribute value, anywhere in the attribute value. This criterion is satisfied if the two strings are identical. Supported attributes: • name.family • name.given

Copyright © 2025 Ping Identity Corporation

Operator	Definition	Description
and	logical AND	Logical AND for building compound expressions in which both expressions are true.
or	logical OR	Logical OR for building compound expressions in which either expression is true.

These SCIM operators are not supported:

- `ne` (not equal)
- `pr` (present, is a non-empty or non-null value)
- `gt` (greater than)
- `ge` (greater than or equal to)
- `lt` (less than)
- `le` (less than or equal to)
- `not` (logical NOT)

Groups

Using groups to organize a collection of user identities can make it easier to manage access to applications. See Application access control.

About groups

You can create groups within an environment or within a population. However, after a group is created, the following conditions apply:

- You cannot move the group:
  - From one population to another
  - From a population to an environment
  - From an environment to a population
- Users that are removed from a population are also removed from the corresponding population-level group.
- End users cannot add or remove themselves from groups.

> **Note**
>
> You can have up to 100,000 groups per environment, and each group can have an unlimited number of users. A single user can belong to up to 10,000 groups.

Copyright © 2025 Ping Identity Corporation

About groups and populations

Groups and populations are both used to organize users, but they differ in several ways.

A user can belong to multiple groups, but only one population. A population is a fundamental organizational unit, while groups offer more fine-grained control. For example, you could use a population to contain all your employees and use a group to define subsets, such as Marketing, HR, Contractors, or US Employees.

A population-level group can contain users from that population only, but an environment-level group can contain users from different populations in the same environment.

Related links

- Populations
- Viewing group membership
- Managing group membership
- SCIM filter language

Internal and external groups

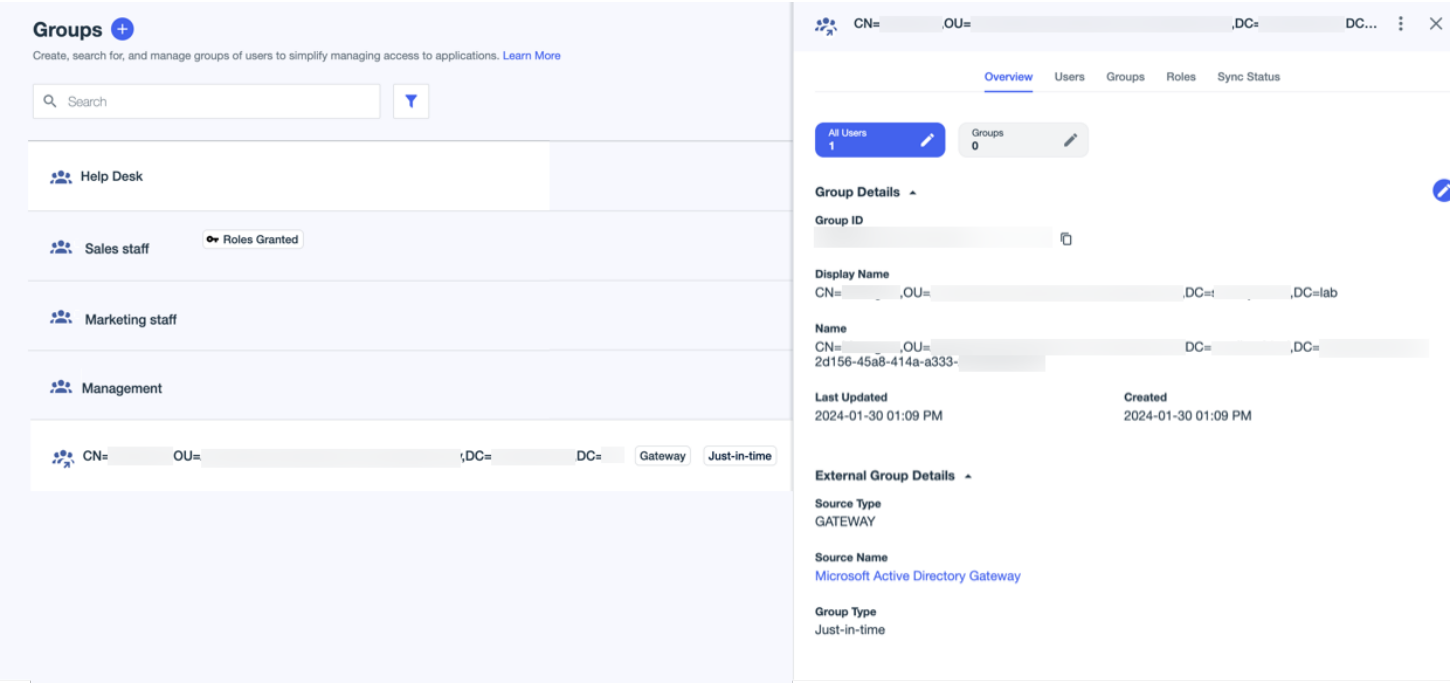
In PingOne, you can have internal groups, which are created and managed in PingOne, or external groups, which are created through a connection to an external identity provider (IdP) or Lightweight Directory Access Protocol (LDAP) gateway.

Internal groups are indicated on the **Groups** page with the **Internal Group** icon ( ) and are fully managed in PingOne. You can add, remove, and edit users directly.

You can create internal groups at the population level or the environment level. Administrators who are assigned roles scoped only to the population level can create groups for those populations only and cannot create groups at the environment level.

External groups are indicated on the **Groups** page with the **External Group** icon ( ) and with badges that indicate how the groups are provisioned (for example, **Just-in-time**) and from where they are sourced (for example, **External IdP** or **LDAP Gateway**). You can view the group membership for external groups in PingOne, but you can't add group members. Group membership is managed by the corresponding IdP or gateway from which the group originates. You can remove users, but the user might be added back into the group automatically the next time the group is synced with the source.

Copyright © 2025 Ping Identity Corporation



Static and dynamic groups

In PingOne, you can create static groups, dynamic groups, or a combination of both.

With static groups, you add or remove group members manually.

With dynamic groups, members are added based on rules. You'll set up an expression or filter to determine which users should be included in the group. If you change the filter criteria for a dynamic group, users will be added or removed automatically based on the current criteria in the filter. Likewise, as user attributes change to match or not match the filter, a user will be implicitly added or removed from the group.

Dynamic groups also allow you to add users directly. You can manually add users that do not match the SCIM filter.

For more information, see Creating a group and Managing group membership.

Dynamic group examples

You can use a custom filter to define dynamic internal groups, as in the following examples.

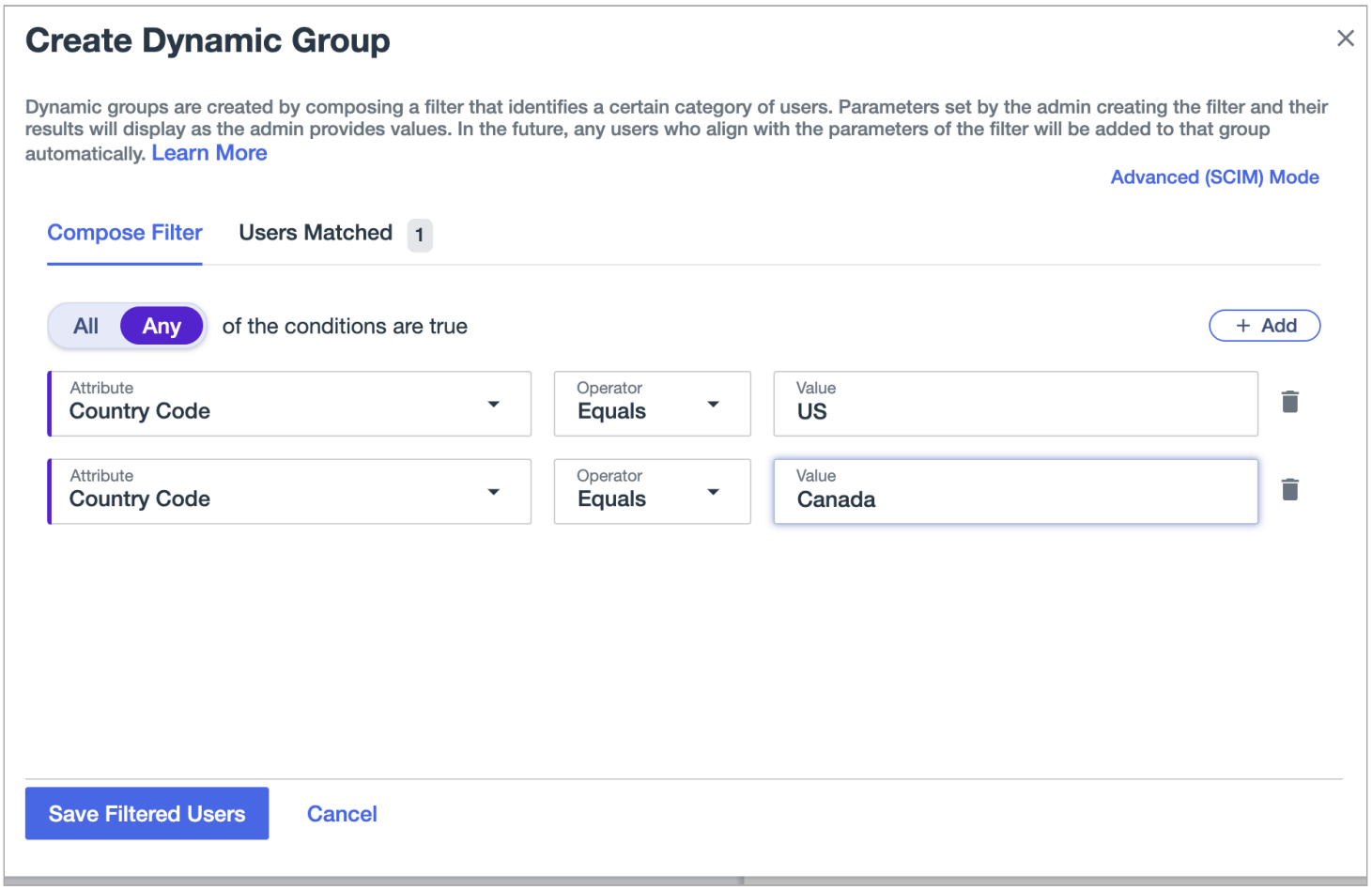
> **Note**
>
> This topic is not applicable to external group membership. External group membership is managed through the source from which the group originates.

Example 1

Filter with a simple **Any**. Include users from the following country codes:

- Country Code Equals `US`

- Country Code Equals `CA`

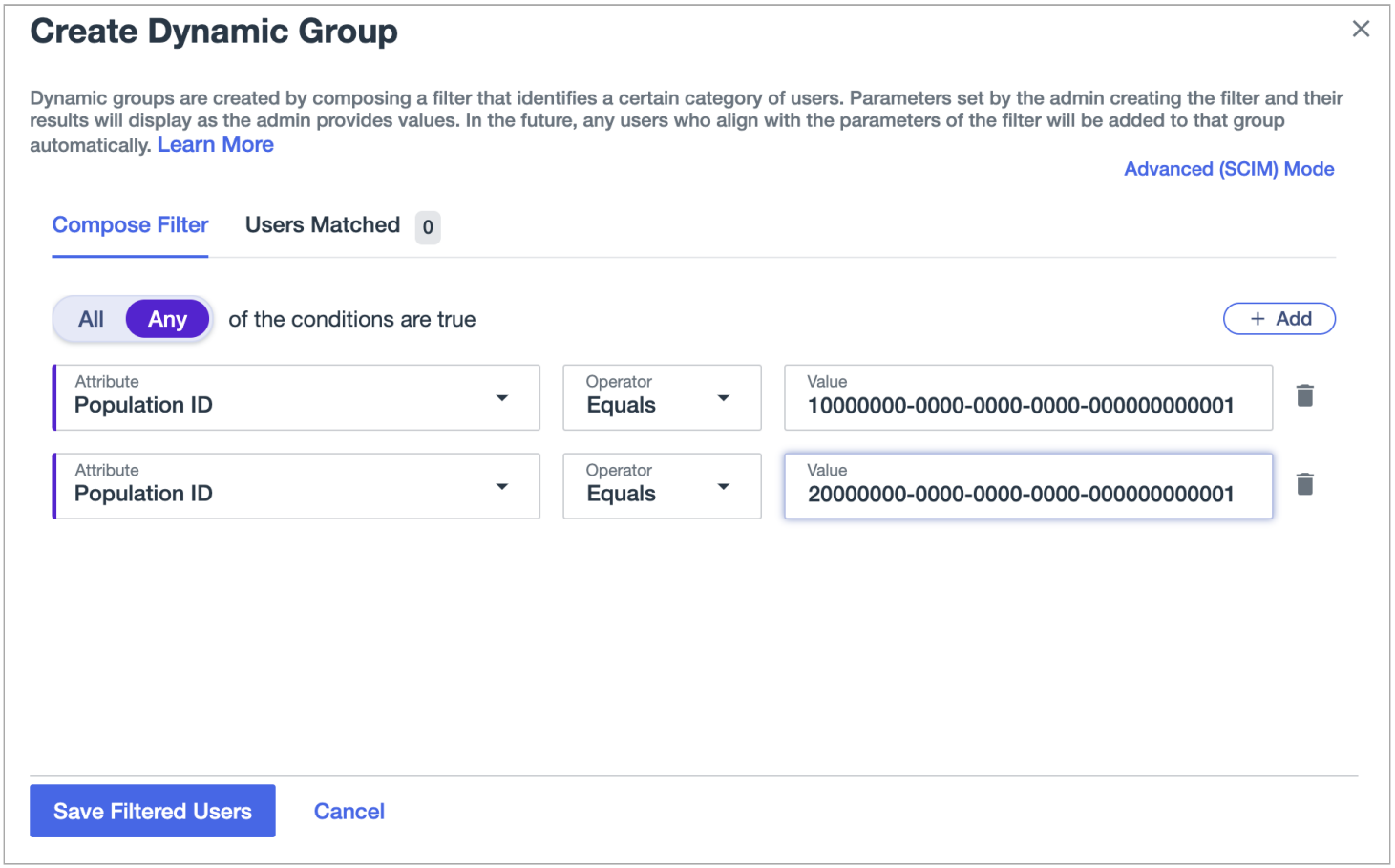


Example 2

Filter with a simple **Any** using UUIDs. Include users from the following populations:

- Population ID Equals `10000000-0000-0000-0000-000000000001`
- Population ID Equals `20000000-0000-0000-0000-000000000001`

Copyright © 2025 Ping Identity Corporation

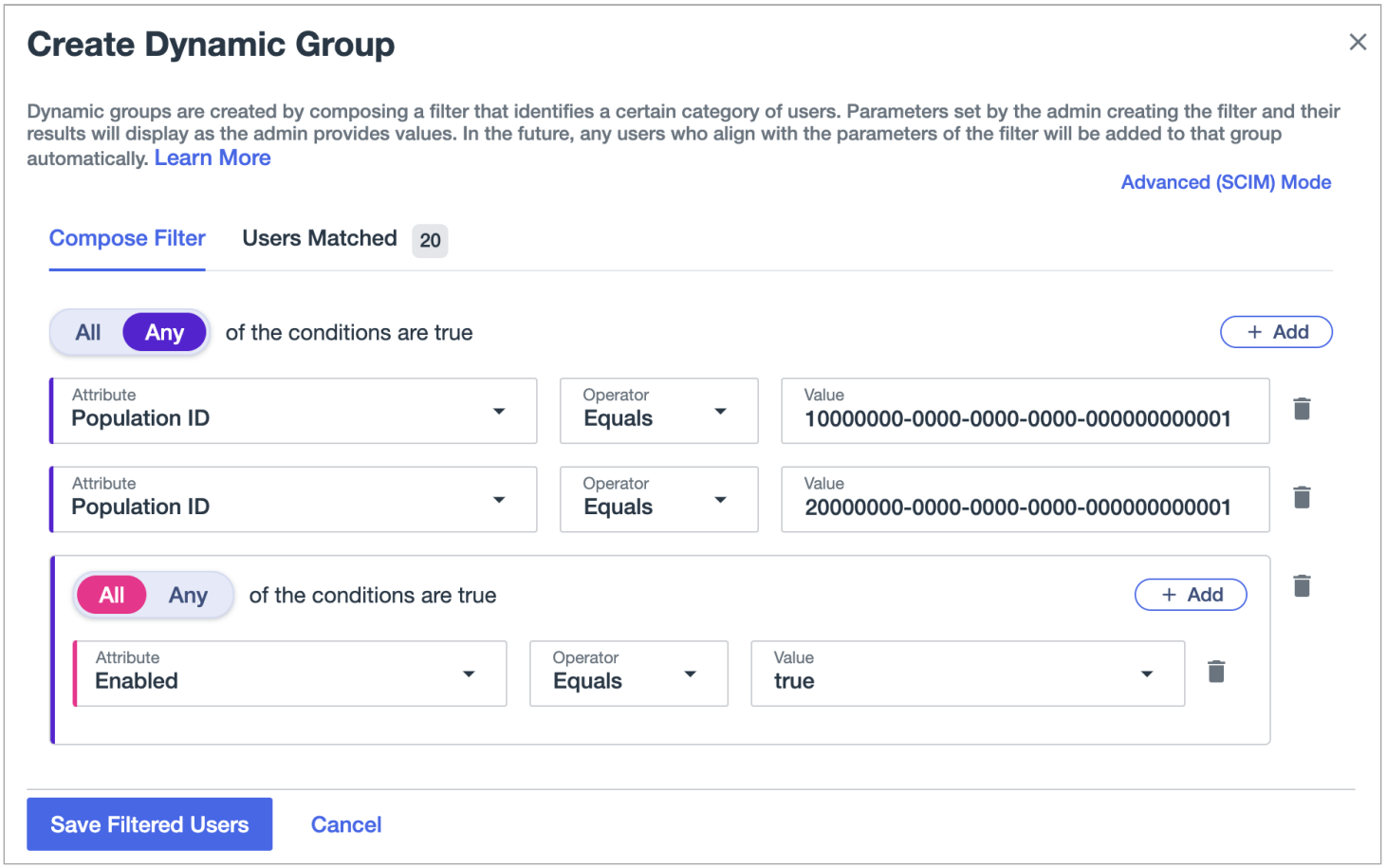


Example 3

Filter with an **Any** and **All**. Include enabled users from the following populations:

- Population ID Equals `10000000-0000-0000-0000-000000000001`
- Population ID Equals `20000000-0000-0000-0000-000000000001`
- Enabled Equals `True`

Copyright © 2025 Ping Identity Corporation

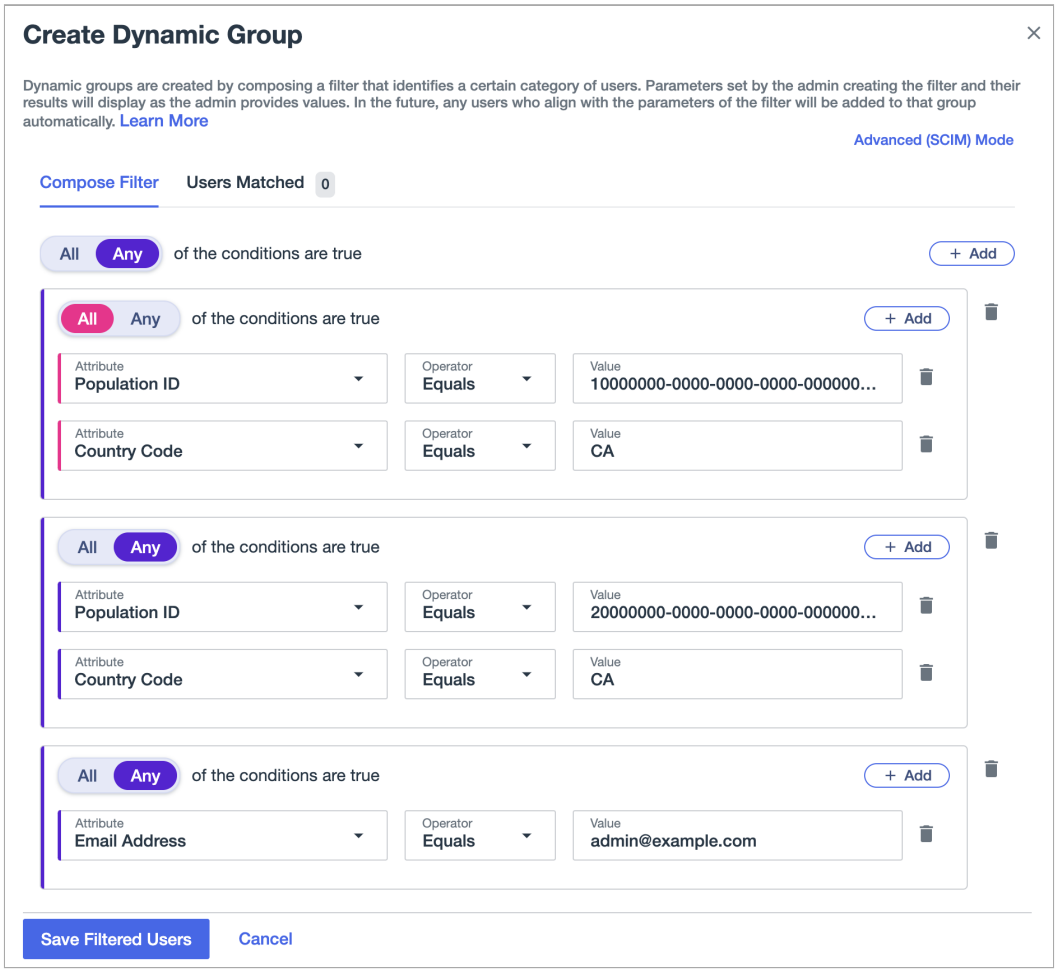


Example 4

Filter with an **All** and several **Any**. Include users from either of two populations in Canada, as well as a user with a particular email address.

- Population ID Equals `10000000-0000-0000-0000-000000000001`
- Country Code Equals `CA`
- Population ID Equals `20000000-0000-0000-0000-000000000001`
- Country Code Equals `CA`
- Email Address Equals `admin@example.com`

Copyright © 2025 Ping Identity Corporation

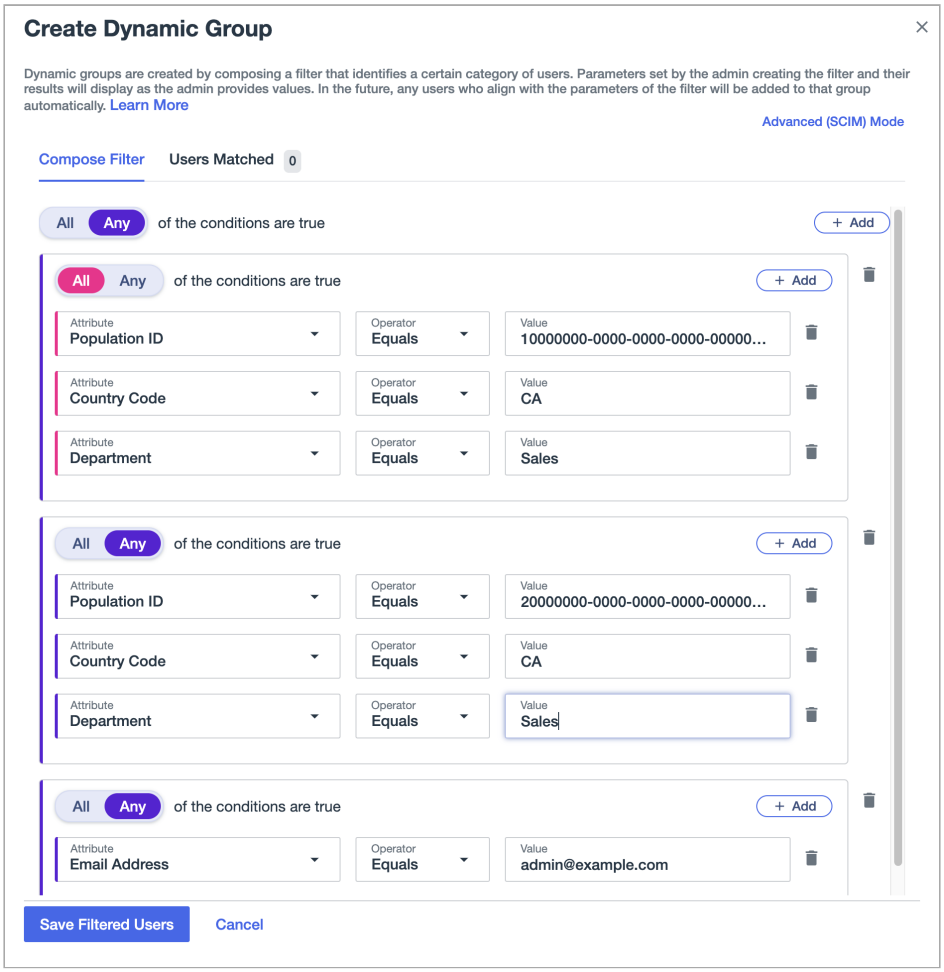


Example 5

Filter with an **All** and several **Any**. All users from either of two populations that are in the US and also in the Sales department, as well as a user with a particular email address. Note that the Department attribute is a custom attribute.

- Population ID Equals `10000000-0000-0000-0000-000000000001`
- Country Code Equals `US`
- Department Equals `Sales`
- Population ID Equals `20000000-0000-0000-0000-000000000001`
- Country Code Equals `US`
- Department Equals `Sales`
- Email Address Equals `admin@example.com`

Copyright © 2025 Ping Identity Corporation



Learn more in Managing group membership.

Nested groups

A nested group is a group that is a member of another group.

Use nested groups to allow inheritance of membership and application access from one group to its subgroups. For more information, see Application access control.

> **Note**
>
> You cannot nest an environment-level group inside a population-level group.

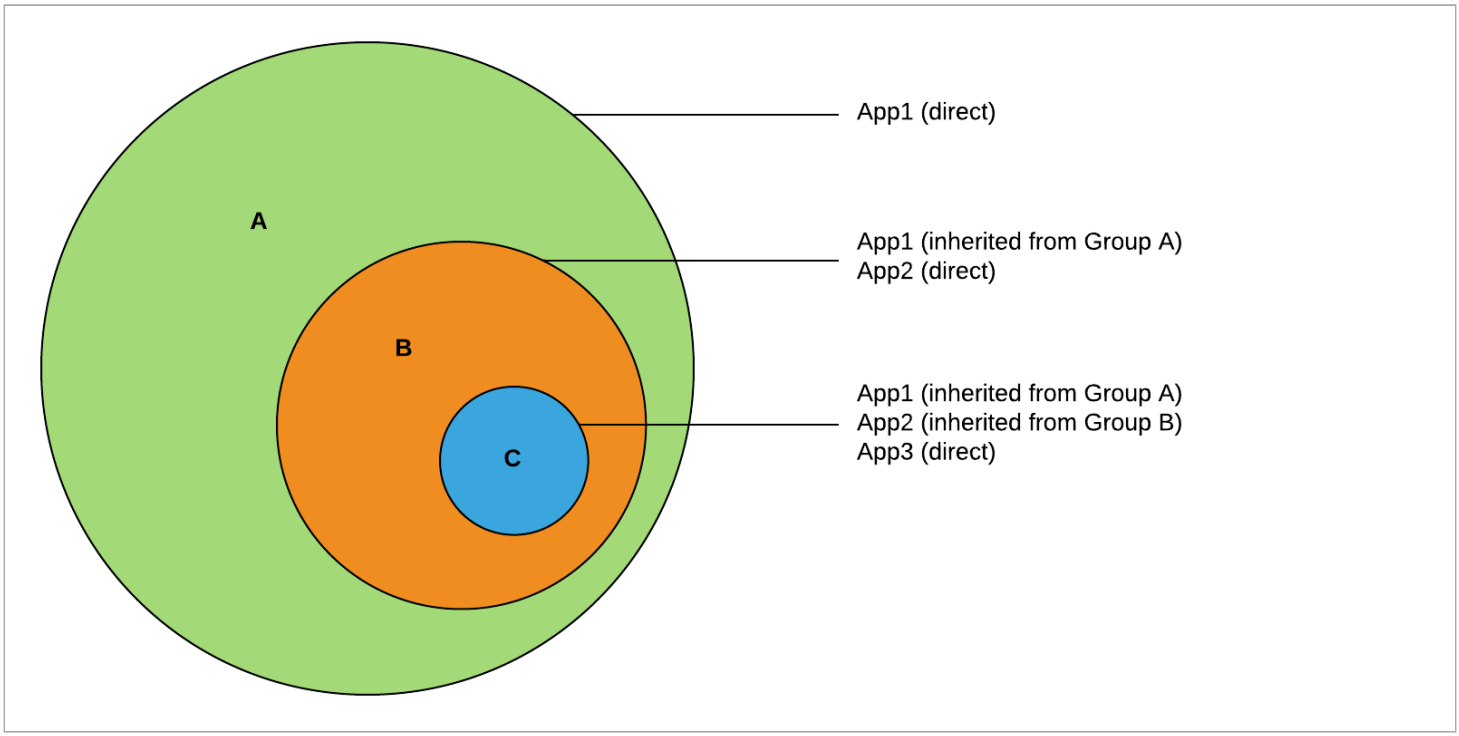
For example, assume an environment has three groups: Group A, Group B, and Group C. Each group has access to a single application: Group A has access to App1, Group B has access to App2, and Group C has access to App3.

If you nest Group B inside of Group A, and Group C inside of Group B, then application access will be as follows:

- Group A has access to App1.
- Group B has access to App1 and App2.
- Group C has access to App1, App2, and App3.

The following diagram illustrates this example.

Copyright © 2025 Ping Identity Corporation



Circular references

You can also nest groups inside their subgroups. Continuing the previous example, if you add Group A as a subgroup of Group C, creating a circular reference, then all three groups will have access to all three applications.

For more information, see Creating a nested group, Removing a nested group, and Managing group membership.

Group roles

To make permissions management easier, you can assign roles to groups and individual users.

Using group roles, you can:

- Manage roles for multiple users at once.
- Apply role changes in bulk.
- See users that have a certain role by viewing group members.

You can use roles to manage permissions for groups of administrators. Learn more in Managing administrators.

For security reasons, only static groups can have roles assigned to them. That is, you can't assign roles to groups that have members included based on a filter or rule. With a dynamic group, you might inadvertently add users to the group that would inherit role assignments. Learn more in Static and dynamic groups.

When adding users to groups that have roles assigned, be careful not to inadvertently assign a role to a user by adding them to a group. If a user has a role from being in a group, remove the user from the group to remove the role. If a user has a role assigned to them individually, you can remove the role from the user.

Copyright © 2025 Ping Identity Corporation

Note

- You can assign only roles that are assigned to you, or that are assignable by those roles. For example, the Identity Data Admin role has permissions that allow it to assign the Identity Data Admin Read Only role. Therefore, if you are assigned the Identity Data Admin role, you can assign that role or the Identity Data Admin Read Only role to a group.
- An admin might not have permissions to assign roles but can add or remove users from a group that has role assignments. In other words, one admin can assign roles to a group, and a different admin can add or remove users from that group.
- You cannot assign roles to a group that you are a member of.
- You cannot add or remove yourself from a group that has roles assigned to it.
- Roles assigned to a group will not affect roles that are assigned to a user individually.
- You can assign roles in up to 500 groups.

Learn more in Creating a group and Managing group membership.

Viewing groups

Use the **Groups** page to view the existing groups in the directory.

About this task

Note

You must have the Identity Data Admin role to create or edit groups. With the Identity Data Read Only role, you can view groups and group membership, but you can't create or edit groups.
Groups provisioned from an external source are indicated with the **External Group** icon ( ) and with badges that indicate how the groups are provisioned (for example, **Just-in-time**) and from where they are sourced (for example, **External IdP** or **LDAP Gateway**.

Steps

1. In the PingOne admin console, go to **Directory > Groups** and browse or search for the group that you want to view.
2. Click the group entry to open the details panel.

Result

The group details panel shows information about the group on the following tabs:

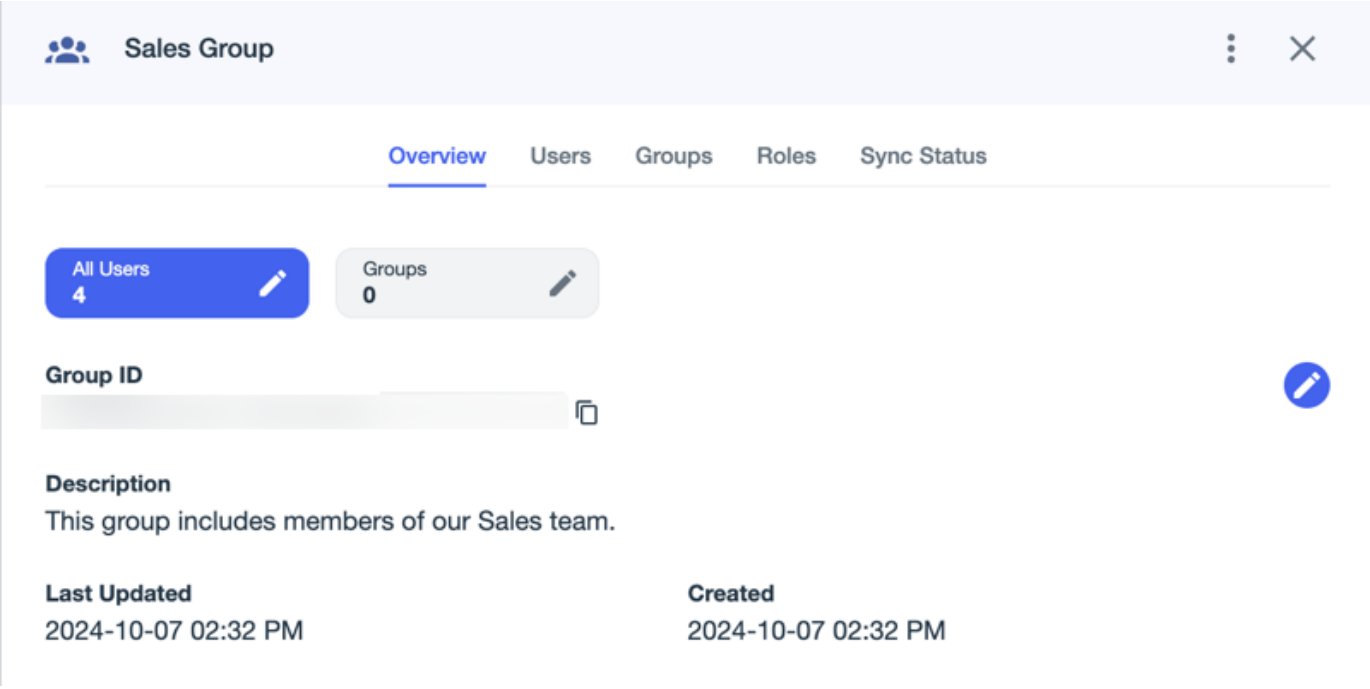
Overview

The **Overview** tab shows the name, description, and summary for the group, including the number of identities in the group, the group ID, custom properties stored as key-value pairs, and other details about the group, such as when it was created and last updated.

The information displayed depends on whether you are viewing an internal group or an external group.

Copyright © 2025 Ping Identity Corporation

Internal groups



Group ID

The ID for the group in PingOne.

Description

A description of the group. If this field is not visible, a description wasn't provided.

Display Name

The name of the group as it's displayed on the **Groups** page and in other areas of PingOne.

Population

Population groups only. The name of the population associated with the group. If this field is not visible, the group was created at the environment level.

Last Updated

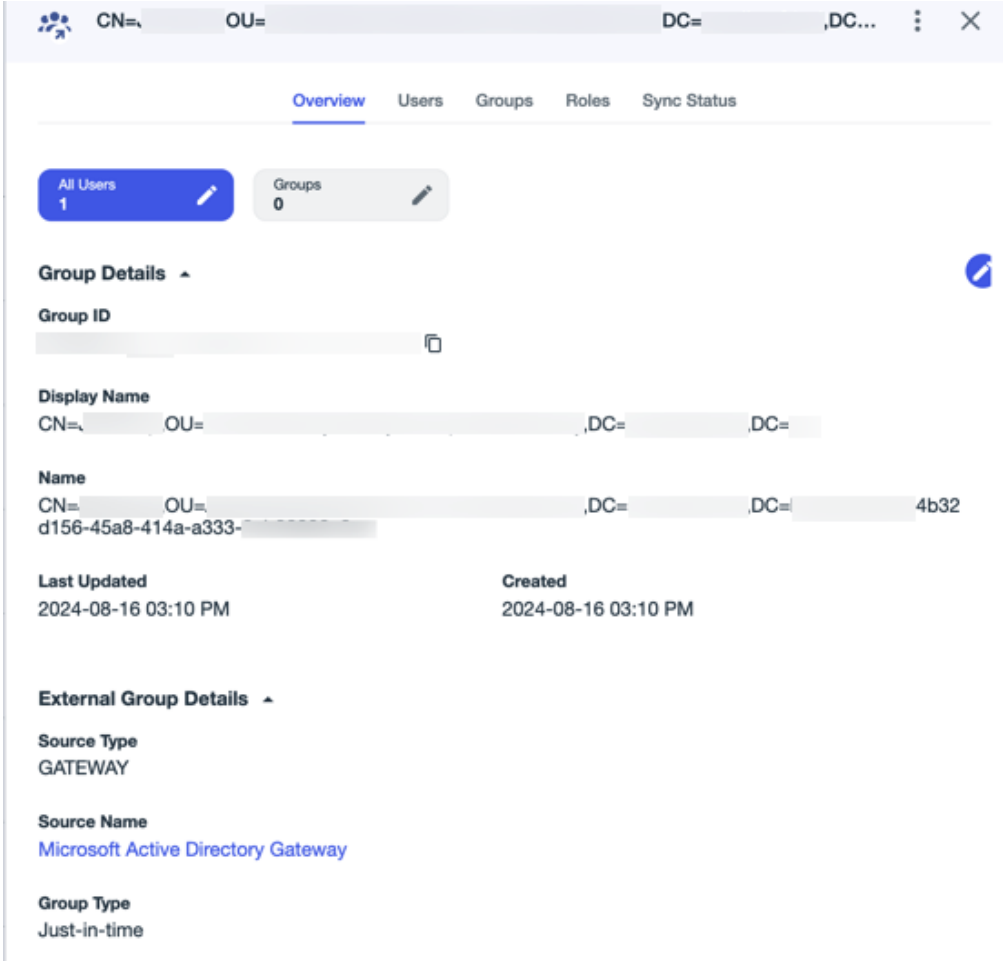
The date of the most recent change made to the group.

Created

The date the group was created.

Copyright © 2025 Ping Identity Corporation

External groups



Group ID

The ID for the group in PingOne.

Description

A description of the group. If this field is not visible, a description wasn't provided.

Display Name

The name of the group as it's displayed on the **Groups** page and in other areas of PingOne.

Name

To maintain unique group names, PingOne shows a slightly different group name for groups that were provisioned from an external source. The group name is based on the external group name and the source of the group in the format `<group-name>|<group-source>|<group-ID>`. For example, `CN=Accounting,OU=People,DC=local|GATEWAY|23bd87do1-041d-nrnn-05bjb90d9`. Learn more in Just-in-time provisioning of external groups.

Last Updated

The date of the most recent change made to the group.

Copyright © 2025 Ping Identity Corporation

Created

The date the group was created.

External Group Details

This section includes the following information about the external group:

Source Type

The source type from which the group originates, either **External IdP** or **LDAP Gateway**.

Source Name

The name of the source in PingOne. Clicking the name takes you to the configuration page for the IdP or gateway.

Group Type

The type of external group, based on how it is provisioned.

Original External Group Name

The name of the group as it appears in the source from which it originates.

Users

The **Users** tab shows the current members of the group.

> **Note**
>
> The **Direct** label indicates that a user or group belongs to the group directly, rather than belonging to a group within that group or matching a filter.

Groups

The **Groups** tab shows any nested groups in the group.

Roles

The **Roles** tab shows any roles that have been assigned to the group. Learn more in Administrator Roles.

Sync Status

If the group is referenced in any provisioning rules, the sync status information for that group is shown here. Learn more in Sync status.

Viewing group membership

You can view group membership on the **Groups** page or on the **Users** page.

About this task

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> You must have the Identity Data Admin role or a custom role with equivalent permissions to create or edit groups. With the Identity Data Read Only role, you can view groups and group membership, but you can't create or edit groups.

Groups page

Viewing group membership on the Groups page

The **Groups** summary page shows the current members of a group.

Steps

1. In the PingOne admin console, go to **Directory > Groups** and browse or search for the group that you want to view.
2. Click the group entry to expand the details panel.
3. Click the **Users** tab.

   The current members are listed. You can browse or search for members.

Users page

Viewing group membership on the Users page

The User details page shows group membership for a particular user.

Steps

1. In the PingOne admin console, go to **Directory > Users** and browse or search for the user that you want to view.
2. Click the **Groups** tab.

   The list shows current group membership. You can also add the user to an existing group. Learn more in Managing group membership.

Searching for groups

Use search and filtering to find existing groups in your organization.

About this task

You can filter groups by external source, such as an external identity provider (IdP) or Lightweight Directory Access Protocol (LDAP) gateway, and by population.

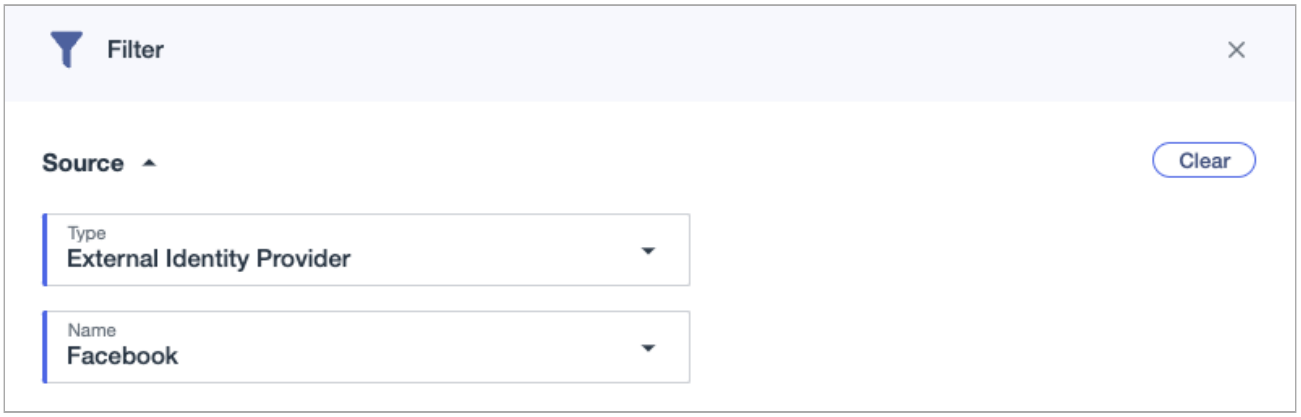
Copyright © 2025 Ping Identity Corporation

Steps

1. In the PingOne admin console, go to **Directory > Groups**.
2. To search for groups, enter the full name or display name in the search bar.
3. To filter the groups list:
    1. To the right of the search bar, click the **Filter** icon.
    2. In the **Filter** panel, under **Source**, select **Type** to filter groups from one of the following external sources:
        - **Gateway**
        - **External Identity Provider**

    > **Note**
    > Groups provisioned from an external source display a badge showing the source of the group. Learn more about external group sources in Just-in-time provisioning of external groups.

    3. For **Name**, select a source name from the list of available external sources.

    4. Under **Population**, search for or select one or more populations to filter your results.

    > **Note**
    > To clear all filters, click **Clear**.

Result

The results list updates as you enter search terms and select filtering criteria. You can click the group name to open the group details panel.

Managing groups

Create groups, manage group membership, and edit existing groups.

Creating a group

About this task

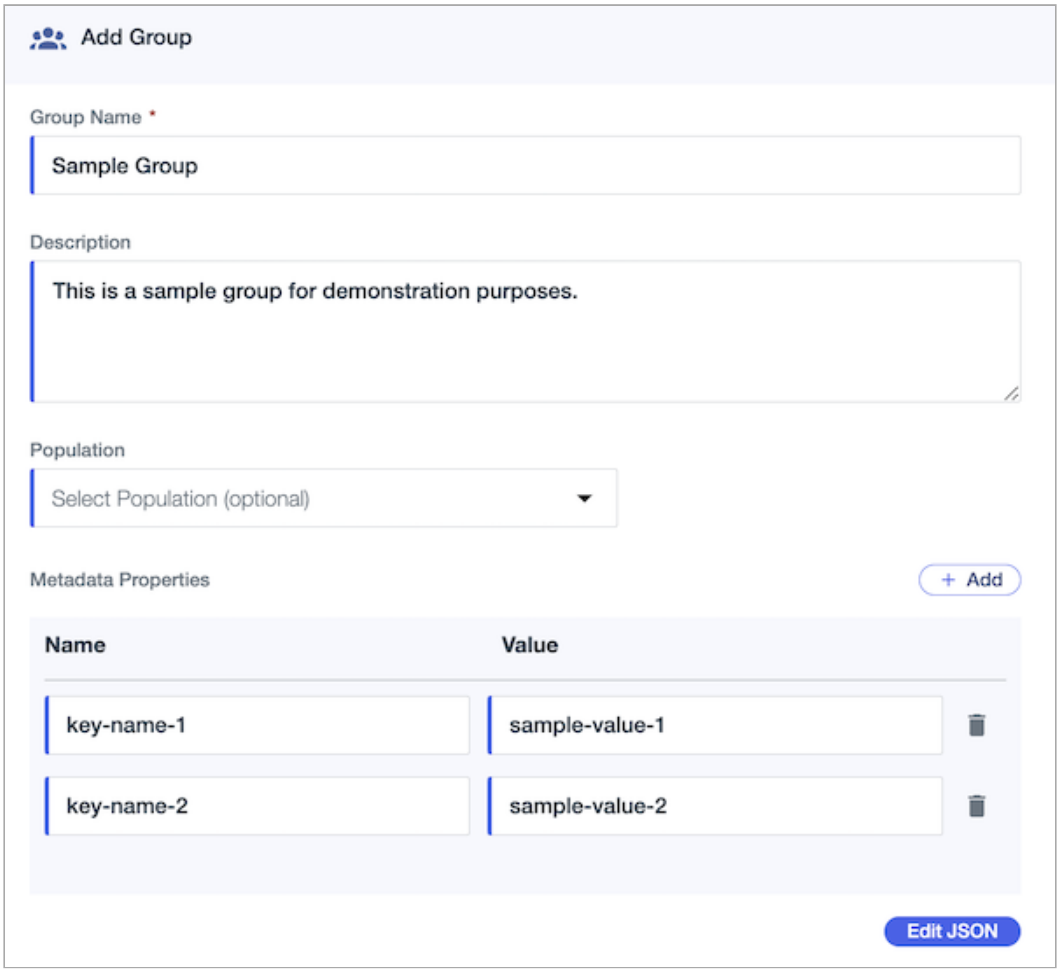
Use the **Groups** page to create groups. You can create static and dynamic groups. Learn more in Static and dynamic groups.

> **Note**
>
> You must have the Identity Data Admin role to create or edit groups. With the Identity Data Read Only role, you can view groups and group membership, but you can't create or edit groups.

Steps

1. In the PingOne admin console, go to **Directory** > **Groups**.
2. Click the **+** icon.
3. Enter the following:
    - **Group Name**: A name for the group. The name must be unique within the environment for environment groups, and unique within a population for population groups.
    - **Description** (optional): A brief description of the group.
    - **Population** (optional): The population in which the group will be created. Users with the **Environment Admin** role can create groups at the environment level, but users with the **Identity Admin** role must assign a group to a population for which they are an **Identity Admin**. If you select a population, the group can contain users from that population only.
    - **Metadata Properties** (optional): Custom metadata properties associated with the group, represented as key-value pairs. To add properties, either:
        - Enter the **Name** and **Value** in the corresponding fields.

Copyright © 2025 Ping Identity Corporation



- If you want to add complex properties that include JSON object values, or directly write properties as JSON, click **Edit JSON** and add the key-value data in the editor.

To switch back to the field view, click **Edit Key-Value-Pairs**.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> - To define more than 10 custom properties, you must use the JSON editor.
> - If you define fewer than 10 properties in the JSON editor, the **Overview** tab displays them in the **Name** and **Value** columns. Otherwise, they are displayed as JSON.
> - If you include a JSON object for any property value in the JSON editor, the **Overview** tab displays the properties as JSON.

4. Click **Save**.

Next steps

Add members to your group.

Managing group membership

About this task

You can define group members manually, dynamically, or using a combination of both.

To include members dynamically, you create a filter that defines which users should be in the group. If you create a dynamic group, you can still add users to the group manually.

Steps

1. In the PingOne admin console, go to **Directory** > **Groups** and browse or search for the group to which you want to add users.
2. Click the group entry to open the details panel.
3. On the **Users** tab, follow the instructions for your preferred method.

> **Note**
>
> You can't add users to an external group in PingOne. Group membership is managed by the group source. You can remove users, but the user might be added back into the group automatically the next time the group is synced with the source.

Copyright © 2025 Ping Identity Corporation

Manually from Groups

Adding or removing users manually from the Groups page
About this task

Use the **Groups** details page to add or remove members manually. You can also add users to a group from the **Users** details page.

Steps

1. In the PingOne admin console, go to **Directory** > **Groups** and browse or search for the group to which you want to add users.
2. Click the group entry to open the details panel.
3. On the **Users** tab, click **Add Individually**.

   > **Note**
   > If the group already has users, click the **Pencil** icon, and then click **Edit Users**.

4. Click the **All Users** tab.

   Result:

   All available users are shown in the **All Users** list.

5. Do one or more of the following:
   - To add a user, select the checkbox for the appropriate user.
   - To remove a user, clear the checkbox for the appropriate user.

   > **Note**
   > If a user is a member of a group because of a filter match, the user is shown in the **Members** list. However, you can't manually remove a member of a dynamic group. To remove a user from a dynamic group, change the filter criteria or modify user attributes to no longer match the filter criteria.
   > Additionally, you can't add users to an external group in PingOne. Group membership is managed by the group source. You can remove users, but the user might be added back into the group automatically the next time the group is synced with the source.

6. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Dynamically from Groups

Adding or removing users dynamically from the Groups page

Use the **Groups** details page to add or remove members dynamically based on a filter.

If new users are added, or existing users are updated, the group membership is updated automatically based on the criteria in the filter. If you create a dynamic group, you can still add users to the group manually.

Steps

1. In the PingOne admin console, go to **Directory** > **Groups** and browse or search for the group to which you want to add users.
2. Click the group entry to expand the details panel.
3. Click the **Users** tab, and then click **Add with a Filter**.

   > **Note**
   > If the group already has users, click the **Pencil** icon, and then click **Edit Users Filter**.

4. In the **Create Dynamic Group** window, define the filter that will determine group membership.

   For examples of filter expressions, see Dynamic group examples.

5. Enter the first condition:

   Attribute

   The user attribute to filter on.

   > **Note**
   > Boolean attributes support the `Equals` operator only, because they are either true or false.

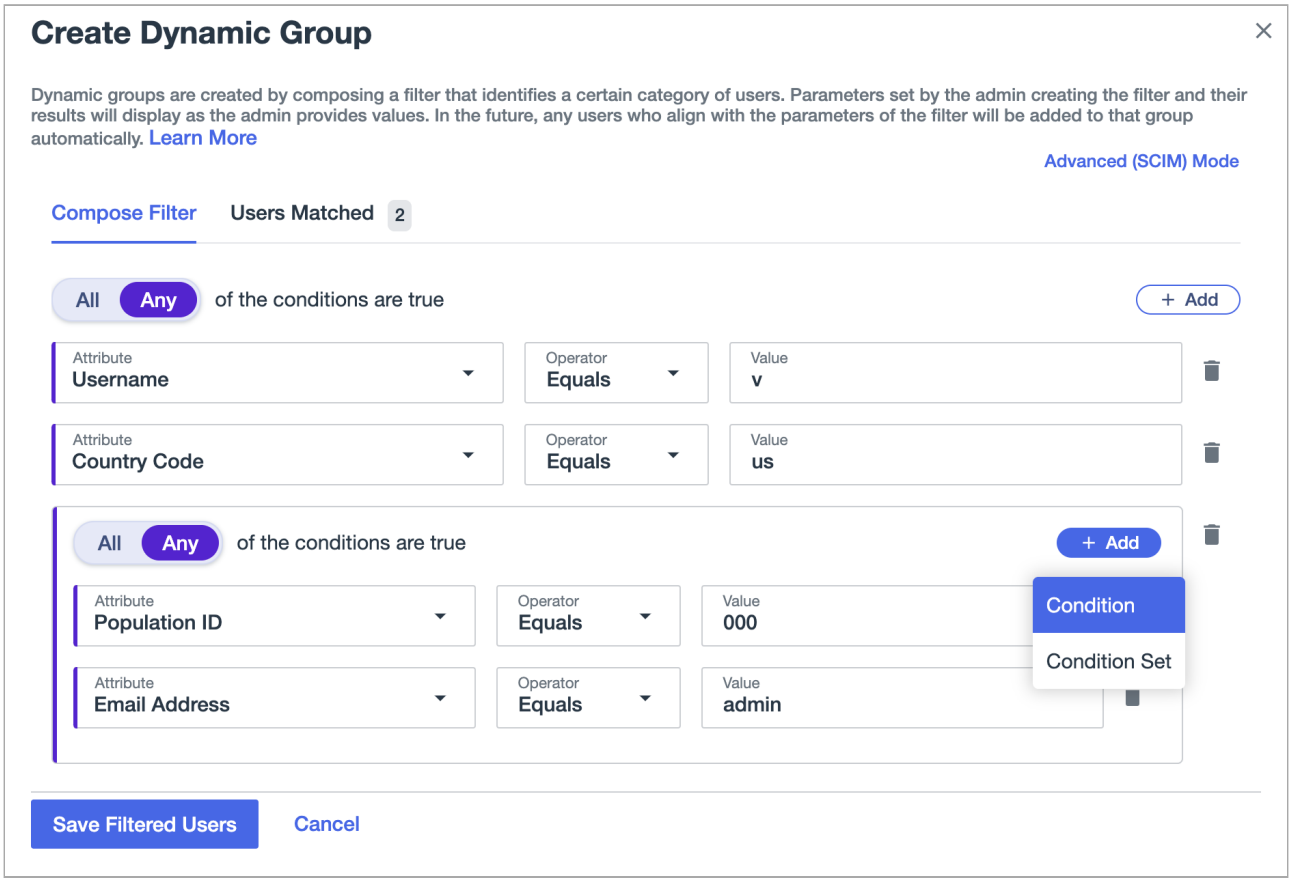
   Operator

   Select **Equals**, **Starts with**, **Ends with**, or **Contains**.

   Value

   Enter the appropriate value.

Copyright © 2025 Ping Identity Corporation



6. If needed, click **+ Add**, and then click **Condition** to add another condition.
7. Select **All** or **Any** to determine how the linked conditions will be evaluated: Boolean logical All or Any.

> **Note**
>
> All filters in the same condition block must use the same logical operator.

8. Continue adding conditions or condition blocks as needed.
9. Click **Save Filtered Users**.

   Result:

   The group is updated with any users that match the expression. If the filter is invalid, you see an error message and no users are added to the group.

10. Click the **Users Matched** tab to see the list of filtered users.

Copyright © 2025 Ping Identity Corporation

Manually from Users

Adding or removing users manually from the Users page

Use the **Users** page to manually add or remove users from a group.

Steps

1. In the PingOne admin console, go to **Directory** > **Users** and browse or search for the user you want to add or remove from a group.
2. Click the user entry to open the details panel.
3. Click the **Groups** tab.

   The list shows current group membership.
4. Click the **Pencil** icon.
5. Do one or more of the following:

   Choose from:

   - To add the user to a group, select the checkbox next to the group name.
   - To remove a user from a group, clear the checkbox next to the group name.

   > **Note**
   >
   > If a user is in a group due to a filter match, you can't directly remove the user from a dynamic group. To remove a user from a dynamic group, change the filter criteria or modify user attributes to no longer match the filter criteria.
   > Additionally, you can't add users to an external group in PingOne. Group membership is managed by the group source. You can remove users, but the user might be added back into the group automatically the next time the group is synced with the source.
6. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Using Advanced SCIM Mode

Adding users using the Advanced (SCIM) Mode editor
About this task

If you prefer to create a SCIM filter directly, you can use Advanced (SCIM) mode to determine which users should be in a group.

If new users are added, or existing users are updated, the group membership is updated automatically based on the criteria in the filter. If you create a dynamic group, you can still add users to the group manually.

Steps

1. In the PingOne admin console, go to **Directory > Groups** and browse or search for the group to which you want to add users.
2. Click the group entry to expand the details panel.
3. Click the **Users** tab, and then click **Add with a Filter**.

   > **Note**
   > If the group already has users, click the **Pencil** icon, and then click **Edit Users Filter**.

4. In the Create Dynamic Group window, click **Advanced (SCIM) mode**.

   > **Note**
   > If you have defined a filter in Basic mode, the filter will appear as a SCIM filter, although some complex SCIM filters cannot be displayed in Basic mode.

5. Enter a SCIM filter expression to define members of the group. Learn more in SCIM filter language.
6. Click **Save Filtered Users**.

   Result:

   The group is updated with any users that match the expression. If the filter is invalid, an error message will appear and no users will be added to the group.

7. Click the **Users matched** tab to see the list of filtered users.

Creating a nested group

Before you begin

You must create the groups before you can nest them. For more information, see Nested groups and Creating a group.

About this task

Use the **Groups** page to nest groups within other groups.

Copyright © 2025 Ping Identity Corporation

Steps

1. In the PingOne admin console, go to **Directory > Groups** and browse or search for the group to use as the parent group.
2. Click the group entry to expand the details panel.
3. On the **Groups** tab, do one of the following:

   Choose from:

   - If the parent group doesn't have any nested groups, click **Manage Groups**.
   - If the parent group already has nested groups, click the **Pencil** icon.
4. Select the checkbox next to the group that you want to nest.
5. Click **Save**.

Removing a nested group

About this task

Use the **Groups** page to remove a nested group from a parent group.

Steps

1. In the PingOne admin console, go to **Directory > Groups** and browse or search for the group to use as the parent group.
2. Click the group entry to expand the details panel.
3. Click the **Groups** tab.
4. Click the **Pencil** icon and clear the checkbox next to the group you want to remove.
5. Click **Save**.

Managing group roles

About this task

Roles are a collection of permissions that can be assigned to a user or group. You can add, remove, or limit the scope of roles for groups from the **Groups** page. Group role assignment is a convenient way to manage administrator access. Learn more about the capabilities of each role in Administrator Roles.

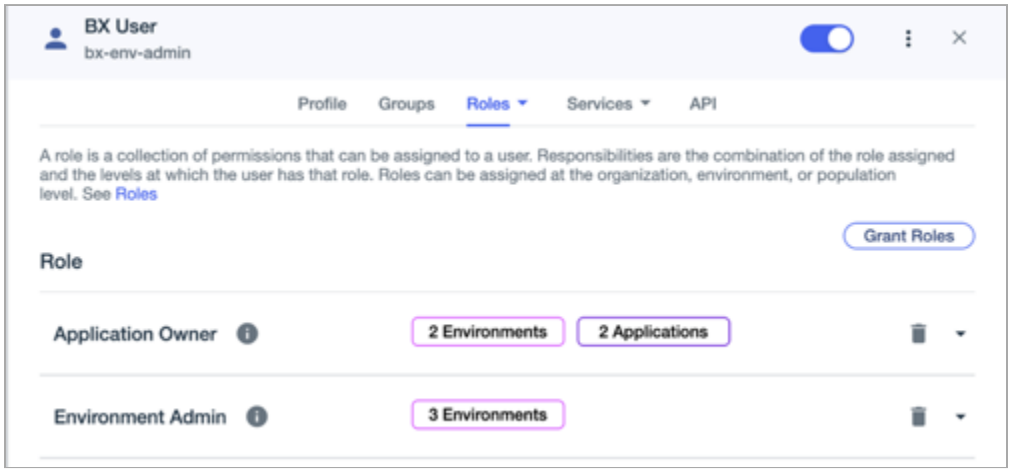
Steps

1. In the PingOne admin console, go to **Directory > Groups**.
2. Click an existing group entry to open the details panel, or create a new group.
3. Click the **Roles** > **Administrator Roles** tab.

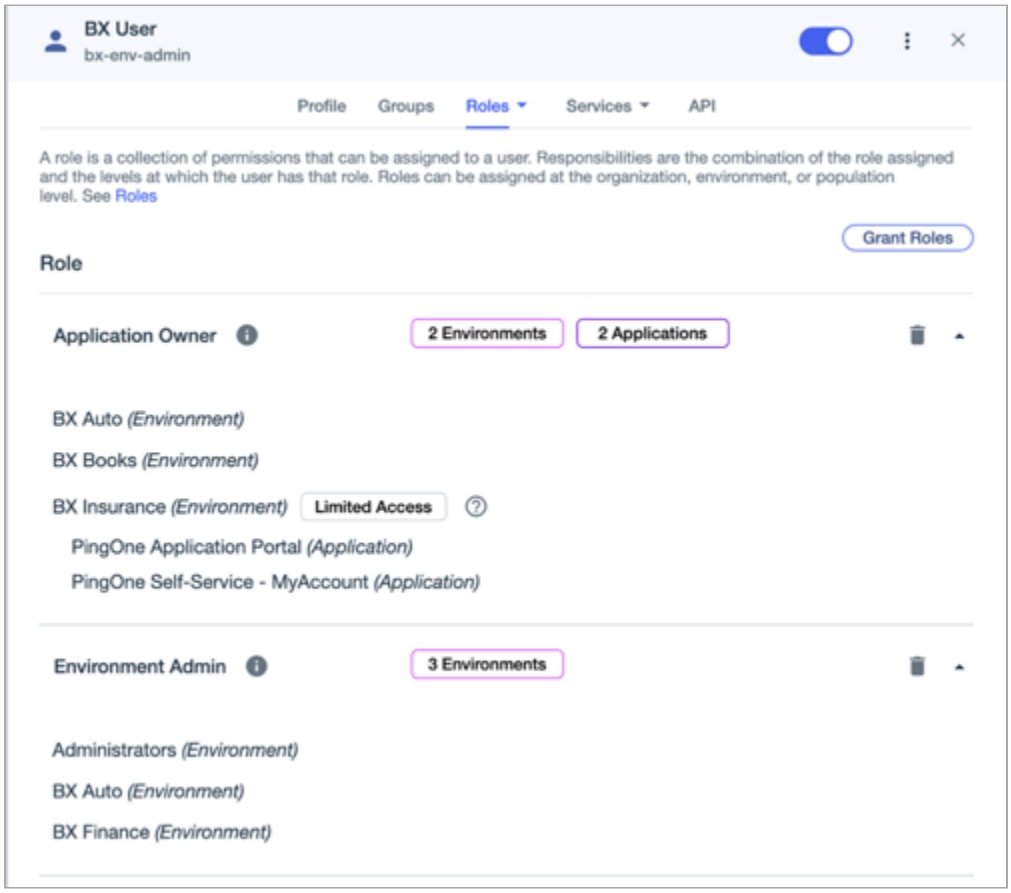
   If roles are assigned, they're listed here with information about where those roles apply. For example, in the following image, **BX User** has the **Application Owner** role in two environments. Because the role is assigned at the environment level, they have the role over all of the applications in those environments. In a third environment, they have the role over only two applications. They also have the **Environment Admin** role, and they have that role in three environments.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> You can assign administrator roles to users, groups, applications, or PingFederate gateway integrations.



> **Tip**
>
> Click the **Info** icon to view the permissions associated with the role. Click the down arrow on the right to view the list of environments or populations for which the role is assigned.



4. Click **Grant Roles**.

Copyright © 2025 Ping Identity Corporation

The **Available Responsibilities** tab lists the roles that you are allowed to assign and the environments for which you are allowed to assign them. A responsibility is the combination of the role assignment and the level, or scope, at which the role is applied. Depending on the role, it could be assigned at the organization, environment, population, or application level.

The **Granted Responsibilities** tab lists any roles that are currently assigned.

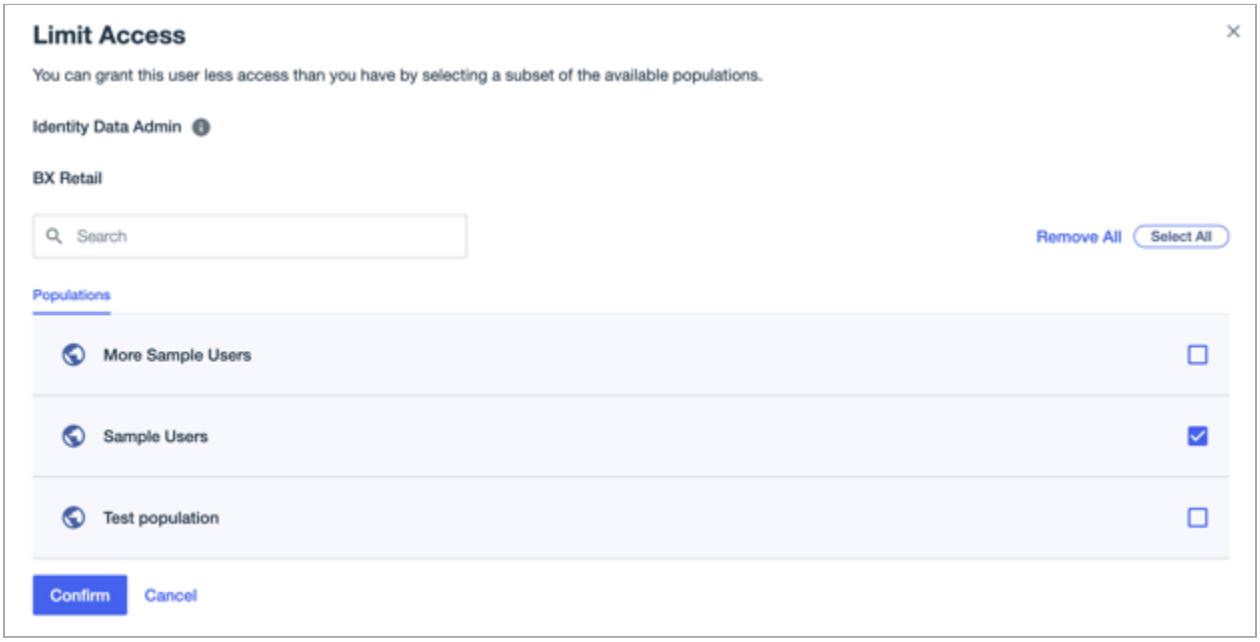
5. On the **Available Responsibilities** tab, click the role that you want to assign or change and perform any combination of the following:

    1. To assign the role, select the checkboxes next to the applicable environments.

    > **Tip**
    >
    > Click **Select All** or **Remove All** to select or clear all available responsibilities.

    2. To remove a role assignment, clear the checkboxes next to the applicable environments.

    3. To grant this access for only a portion of the environment, click the **Reduce Access** icon ( ), select a subset of the available applications or populations on the **Limit Access** page, and click **Confirm**.



> **Note**
>
> You can grant only roles that are assigned to you or that confer the permissions needed to assign that role to others. For example, if you do not have the Environment Admin role, you cannot assign the Environment Admin role to others (and that role will not be listed under **Available Responsibilities**). However, if you have the Identity Data Admin role, you can assign either the Identity Data Admin role or the Identity Data Read Only role to others.
> Learn more about the permissions associated with each role in Roles.

6. Click **Save**.

Result

The role assignments you selected are listed on the **Granted Responsibilities** tab.

Copyright © 2025 Ping Identity Corporation

Next steps

Learn more about role assignment using external groups in Managing administrator roles using external groups.

Editing a group

About this task

Use the **Groups** page to edit existing groups in the PingOne Directory.

Steps

1. In the PingOne admin console, go to **Directory > Groups** and browse or search for the group you want to edit.
2. Click the group entry to expand the details panel.
3. On the **Overview** tab, edit the group name, description, or metadata properties. Learn more in Creating a group.
4. On the **Users** tab, edit the group membership. You can add users manually, dynamically, or a combination of both. Learn more in Managing group membership.

   > **Note**
   >
   > You can't add users to an external group in PingOne. Group membership is managed by the group source. You can remove users, but the user might be added back into the group automatically the next time the group is synced with the source.

5. On the **Groups** tab, edit the nested groups. Learn more in Nested groups.
6. On the **Roles** tab, edit the group roles. Learn more in Group roles.
7. Click the **X** in the upper right to close the group details panel.

Deleting a group

About this task

Use the **Groups** page to remove a group you no longer need.

Steps

1. In the PingOne admin console, go to **Directory > Groups** and browse or search for the group you want to delete.
2. On the right side of the group entry, click the **More options (⋮)** icon and then click **Delete**.
3. In the confirmation message, click **Delete**.

Just-in-time provisioning of external groups

PingOne can provision group membership from an external source, such as an identity provider (IdP) or Lightweight Directory Access Protocol (LDAP) gateway. Just-in-time (JIT) group provisioning occurs as part of the authentication process.

These groups are labeled with a **Just-in-time** badge on the **Groups** page.

Copyright © 2025 Ping Identity Corporation

External IdPs

If the IdP includes group membership information in its Security Assertion Markup Language (SAML) assertions, ID tokens, or `UserInfo` responses, you can map this information into PingOne. You can populate the information one time or every time the user signs on.

Groups created through an external IdP are labeled with both the **Just-in-time** badge and an **External IdP** badge.

LDAP gateway

When defining a user type, you can map group membership information into PingOne. By default, PingOne populates this information one time. When you enable the **Update PingOne user attributes as users sign on** option, user attributes update each time a user signs on successfully through the LDAP gateway client.

Groups created through an LDAP gateway are labeled with both the **Just-in-time** badge and an **LDAP Gateway** badge.

> **Note**
>
> Because Kerberos authentication is a cloud-only operation, users authenticating with the Kerberos protocol will not trigger an update in their user records.

Learn more about updating group membership through LDAP gateways during sign on in Adding a user type.

Limitations

The following are known limitations to JIT group provisioning:

- (LDAP gateway only) When a group is nested inside another group, and a user is a member of the nested group but not the parent group, PingOne provisions only the nested group based on direct group membership.

  For example, there are two groups: group A (the parent group) and group B (the nested group). If a user is a member of group B (Group A → Group B → User), provisioning only occurs for group B (the nested group), not group A (the parent group).

- You can't change the **Group Display Name** in PingOne.
- If a group name is changed, PingOne considers it a new group. The user is removed from the old group and added to the new group.
- If a user was provisioned to a group in PingOne, you can manually remove the user from the group in PingOne. However, the JIT provisioning feature might add them back to the group later if they were not also removed at the external source.
- Users cannot be added to an external group directly from PingOne.

Related information

Learn more in:

- Mapping the group attribute from an LDAP gateway
- Mapping the group attribute from an external identity provider
- Including external groups in an application
- Managing administrator roles using external groups

Copyright © 2025 Ping Identity Corporation

Populations

A population defines a set of users and can help you make user management simple.

For example, you can create a population for similar types of users, such as those in a particular region or job function, and assign those users a unique password policy.

All users are assigned to a population, and you must have at least one population before you can create users. You can move individual users to a different population, but an individual user can't belong to more than one population simultaneously.

Learn more in Managing populations.

Default populations

You can configure any population as the default population. When creating a user through the console or API, PingOne adds the user to the default population unless you specify a population. Learn more in Managing populations.

Roles and populations

You can assign administrator roles for managing populations. For example, you can give an administrator user the Identity Admin role for a particular population so that the administrator can manage identities in that population but not in other populations. Learn more in Administrator Roles.

Managing populations

PingOne allows you to organize users into populations to simplify user and policy management.

Click the appropriate tab for instructions on:

- Viewing your existing populations and their details
- Adding a new population
- Making changes to a population
- Deleting an unused population

Copyright © 2025 Ping Identity Corporation

Viewing populations

Viewing populations

Use the **Populations** page to view populations in PingOne.

Steps

1. In the PingOne admin console, go to **Directory** > **Populations** and browse or search for the population that you want to view.
2. Click the population entry to open the details panel.

Result

The population details panel shows information about the population on the following tabs:

Overview

The **Overview** tab shows general information about the population.

Field	Description
Population Name	A unique label for the population.
Description	A brief description of the population, if one was entered.
Population ID	A unique identifier for the population. **Tip** You can click the **Copy** icon to copy the population ID to the clipboard.
Identity Provider	The default identity provider (IdP) for the population if one was selected. When nothing else is selected, PingOne is used as the default IdP during the runtime. Click the title to go to the specific identity provider. If your IdP isn't enabled, the word **Disabled** displays next to the title. Manage your IdPs from **Integrations** > **External IdPs**.

Configuration

The **Configuration** tab displays information about settings that apply only to DaVinci. These settings are not used in sign-on policies.

Field	Description
Alternative Identifiers	A domain, ID, or custom value used to identify the population.
Language	The preferred language for this population. Learn more in Languages. **Note** If a population doesn't have a selected language, the default language for the environment is used.

Copyright © 2025 Ping Identity Corporation

Field	Description
Theme	The default branding theme for this population. Learn more in Branding and themes and Adding a theme. **Note** If a population doesn't have a selected theme, the active theme for the environment is used.

Password Policy

The **Password Policy** tab shows detailed information about the password policy in use for the population.

Field	Description
Password Policy	The password policy assigned to the population. Click the link to go to the **Password Policies** page.
Description	A brief description of the password policy.
Password Policy ID	The ID of the password policy assigned to the population. Click the password ID to copy it to the clipboard.
Password Requirements	The requirements for the password. For example, the password must be 12 characters long, or it requires special characters.
Password Policy Rules	The password rules for the policy. For example, a rule that requires the user change their password every 6 months.
Account Lockout Rules	The lockout rules for the account. For example, after five incorrect password entries, the user is locked out for a period of time.

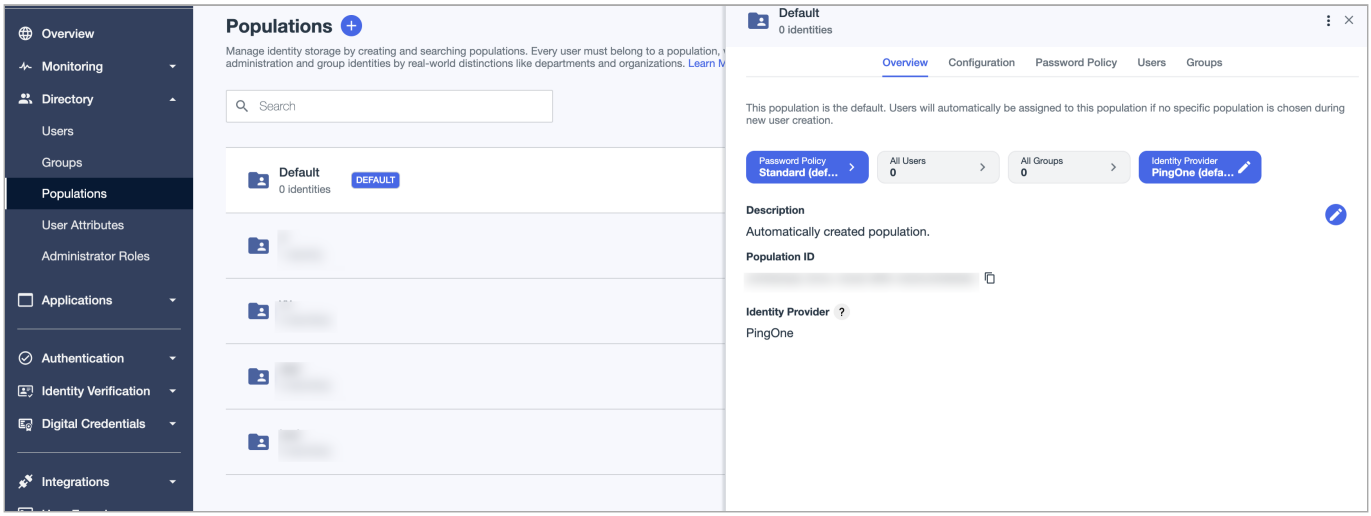
Users

The **Users** tab shows the list of users currently in the population.

Groups

The **Groups** tab shows the list of groups currently in the population.

Copyright © 2025 Ping Identity Corporation



Adding a population

Adding a population

Use the **Populations** page to add a population in PingOne.

Steps

1. In the PingOne admin console, go to **Directory** > **Populations**.
2. Click the **+** icon to add a population.
3. Enter the following:

Field	Description
Population Name	A unique label for the population.
Description (optional)	A brief description of the population.
Default Population	Select the checkbox to specify the current population as the default population. Users created without a specified population are added to the default population. **Note** If you are changing the default population, PingOne shows a confirmation message. Click **Confirm**.

4. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Editing a population

Editing a population

Use the **Populations** page to edit existing populations.

Steps

1. In the PingOne admin console, go to **Directory** > **Populations** and browse or search for the population you want to edit.
2. Click the population entry to open the details panel.
3. On the **Overview** tab, click the **Pencil** icon, edit or enter the following, then click **Save**:

Field	Description
Population Name	A unique label for the population.
Description (optional)	A brief description of the population.
Identity Provider (optional)	The default IdP for the population. **Note** If you are changing the default IdP, PingOne shows a confirmation message. Validate the IdP configuration to avoid lockout and click **Confirm**. This setting is used at runtime for users in the population who do not have **Authoritative Identity Provider** configured in their user profile, and only for as long as they remain in the population. When a user doesn't have an IdP configured in their user profile, the default IdP from the population PingOne is used. If **Authoritative Identity Provider** is set on the user profile, that setting is used to authenticate the user. The user profile setting is not updated or changed by the setting on the population. You must have the Identity Data Admin role or a custom role with equivalent permissions to configure this setting. Learn more in Authoritative identity providers.
Default population	Select the checkbox to specify the current population as the default population. Users created without a specified population are added to the default population. **Note** If you change the default population, PingOne shows a confirmation message. Click **Confirm**.

4. (Optional) On the **Configuration** tab, click the **Pencil** icon, edit or enter the following, then click **Save**.

Copyright © 2025 Ping Identity Corporation

> **Note**
> These settings apply only to DaVinci and aren't used in sign-on policies.

Field	Description
Alternative Identifiers	A domain, ID, or custom value used to identify the population.
Language	The preferred language for this population. Learn more in Languages. **Note** If you don't select a language, the default language for the environment is used.
Theme	The default branding theme for this population. Learn more in Branding and themes and Adding a theme. **Note** If you don't select a theme, the active theme for the environment is used.

5. (Optional) On the **Password Policy** tab, the **Standard** default policy shows. Click the **Pencil** icon, select a different password policy that is configured in your environment, then click **Save**.

   Learn more in Password policies.

6. (Optional) On the **Users** tab, browse or search for a user. Click the **More Options** (⋮) icon and click **Manage User Profile**.

   Result:

   The **Users** page opens, and the user details panel shows.

   Learn more in Changing a user's population.

   > **Note**
   > Users are added to the default population when a population isn't specified during the new user creation.

7. (Optional) On the **Groups** tab, browse or search for a group. Click the **More Options** (⋮) icon and click **Manage Group**.

   Result:

   The **Groups** page opens, and the group details panel shows.

   Learn more in Managing groups.

8. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Deleting a population

Deleting a population

Use the **Populations** page to remove populations that you no longer need.

Before you begin

- To delete a population, you must have the Environment Admin role or a custom role with equivalent permissions.
- You must remove all users from a population before you can delete it.

Steps

1. In the PingOne admin console, go to **Directory** > **Populations** and browse or search for the population you want to delete.
2. On the right side of the population entry, click the **More options** (⋮) icon and then click **Delete**.
3. On the confirmation message, click **Delete**.

User Attributes

User attributes determine the types of data that are stored for each user, such as name, address, account number, or email address. You can specify the attributes that are applied to users in your directory.

You can have up to 200 custom string attributes and JSON attributes in an environment.

Attribute access control

Some PingOne platform self-management scopes allow organizations to specify which user profile attributes are accessible to end users.

An administrator might want to prevent end users from seeing or modifying particular attributes that should remain private, such as custom attributes for entitlements, internal foreign keys, account status information, or any profile data that should not be exposed to an individual user. With access control scopes, organizations can store additional private data in the user profile without risk that the end user can see the data.

These access control scopes designate a specific set of user attributes, which is often a subset of attributes that the user is allowed to read or update. For example, a `p1:update:user:email-only` scope could remove all other user schema attributes except the user's email address. A user with this scope could update only their email address. All other visible attributes would not allow modification.

Related links

- Configuring attribute access control

Copyright © 2025 Ping Identity Corporation

Viewing user attributes

You can view user attributes in your environment.

About this task

Use the **Attributes** page to view the configured attributes for your environment.

Steps

1. Go to **Directory → User Attributes**.
2. Browse or search for the user attributes that you want to see configuration details for.

   You can scope your search by selecting **All**, **Core**, **Standard**, or **Custom** from the list.
3. **Optional:** To show attributes that are currently disabled, click **Show disabled attributes**.

Result

The **User Attributes** page shows a list of the configured attributes and their status.

Adding user attributes

You can add a user attribute to your environment.

About this task

Use the **Attributes** page to add a user attribute to your environment.

Steps

1. Go to **Directory → User Attributes**.
2. Click the **+** icon.
3. Select the attribute that you want to add: **Declared** or **JSON**.

   Declared attributes are string attributes that applications can access through the PingOne API or the PingOne console.

   Declared attributes can be:

   - Unique
   - Multivalued
   - Enumerated
   - Validated (Regex)

   JSON attributes are structured attributes that applications can access through the PingOne API or the PingOne console. Resources can use JSON attributes in their attribute mappings. You can use these attributes to pass complex information to applications through an access token.

Copyright © 2025 Ping Identity Corporation

JSON attributes can be:

- Multivalued
- Validated (JSON Schema)

4. Click **Next**.
5. Enter the following information:
   - **Name**: A unique identifier for the attribute.
   - **Display name**: The name of the attribute as you want it to look in the user interface.
   - **Description**: A brief characterization of the application.
6. Select the configuration options for the attribute:
   - **Enforce unique values**: Require that attribute values be unique across the environment.
   - **Allow multiple values**: Allow the attribute to support multiple values:
     - When a multi-valued attribute is mapped as part of an OIDC or OAuth flow, then the claim will be an array of values.
     - When a multi-valued attribute is mapped as part of a SAML flow, then the multi-valued attribute will be a multi-valued SAML attribute in the SAML assertion. See Mapping attributes.
   - **No Validation**: No validation is needed.
   - **Enumerated Values**: Allow the attribute to have enumerated values.
   - **Regex Validation**: Requires that the attribute have a testable expression. Enter the following information to test an expression:
     - **Expression**: A unique identifier for the attribute.
     - **Description**: A brief characterization of the attribute.
     - **Values**: Examples of values that match or do not match the expression.

   > **Note**
   > After you create an attribute that is multi-valued, you cannot change it to single-valued.

7. Click **Save**.

Related links

- Mapping attributes

Editing user attributes

You can edit existing user attributes in your environment.

About this task

Core and Standard attributes are system provided attributes. While core attributes cannot be edited or disabled, standard attributes have a limited editing ability. Use the **Attributes** page to edit an existing user attribute.

Steps

1. Go to **Directory → User Attributes**.
2. Locate the attribute that you want to edit by browsing or searching for it.

   Choose from:

   - Click the **More Options** (⋮) icon and then click **Edit Attribute**.
   - Click the attribute that you want to edit, and then click the pencil icon.

3. Select the configuration options for the attribute:
   - **Enforce unique values**: Require that attribute values be unique across the environment.
   - **Allow multiple values**: Allow the attribute to support multiple values:
     - When a multi-valued attribute is mapped as part of an OIDC or OAuth flow, then the claim will be an array of values.
     - When a multi-valued attribute is mapped as part of a SAML flow, then the multi-valued attribute will be a multi-valued SAML attribute in the SAML assertion. See Mapping attributes.
   - **No Validation**: No validation is needed.
   - **Enumerated Values**: Allow the attribute to have enumerated values.
   - **Regex Validation**: Requires that the attribute have a testable expression. Enter the following information to test an expression:
     - **Expression**: A unique identifier for the attribute.
     - **Description**: A brief characterization of the attribute.
     - **Values**: Examples of values that match or do not match the expression.

     > **Note**
     > After you create an attribute that is multi-valued, you cannot change it to single-valued. Not all attribute properties can be edited in the PingOne console.

4. Click **Save**.

Related links

- Mapping attributes

Mapping attributes

You can map PingOne user attributes to SAML or OIDC attributes to and from external applications, resources, identity providers, and provisioning connections.

Copyright © 2025 Ping Identity Corporation

For example, you could map `Email Address` in PingOne to `NameID` in an application.

> **Note**
>
> When mapping multivalued attributes to and from PingOne, consider the following conditions.
>
> - If you map a multivalued PingOne attribute to an attribute for an external application, the claim in the token or the attribute in the assertion will be multivalued.
> - If you map an external attribute to a PingOne attribute, PingOne will evaluate the mapping as follows:
> - If you map an external multivalued attribute to a multivalued PingOne attribute, PingOne will add all values to the PingOne attribute.
> - If you map an external multivalued attribute to a single-valued PingOne attribute, PingOne uses only the first value of the external multivalued attribute.
> - If you map an external single-valued attribute to a multivalued PingOne attribute, PingOne will take the single value and add it to the multivalued PingOne attribute to create a multivalued attribute containing one value.
>
> For more information about the expression builder, see Using the expression builder.

Using attribute mapping

You can map PingOne attributes to attributes in your application, resource, identity provider, or provisioning connection.

- Locate the object in which you want to map attributes.

  The specifics of attribute mapping vary based on the object that you are editing. For more information, see:

  - Editing an application
  - Editing a resource
  - Editing an identity provider
  - Editing a provisioning rule

Disabling or enabling a user attribute

If you don't want to delete a user attribute, you can disable it.

Steps

1. To disable a user attribute, go to **Directory → User Attributes**.
   1. Locate the user attribute that you want to disable by browsing or searching for it.
   2. To disable the user attribute, click the toggle.
2. To enable a user attribute, go to **Directory → User Attributes**.
   1. Click **Show disabled attributes.**
   2. Locate the user attribute that you want to enable.
   3. To enable the user attribute, click the toggle.

Copyright © 2025 Ping Identity Corporation

Viewing the user attribute schema

You can view or copy the user attribute schema.

About this task

Use the **Attributes** page to view or copy the user attribute schema.

Steps

1. Go to **Directory → User Attributes**.
2. To the right of the **+** icon, click the **More Options** (⋮) icon, and then click **View Schema**.

Result

The **View Schema** page opens. You can view the schema in either JSON or CSV format.

Characters supported in PingOne user attributes

The characters supported in user attributes in PingOne vary depending on the attribute. Learn more in the following table.

Attribute	Supported characters
Email Address	Uppercase and lowercase English letters: A-Z; a-z
	Arabic numerals: 0-9

Copyright © 2025 Ping Identity Corporation

Attribute	Supported characters
	The following symbols: • Exclamation mark (!) • Pound sign (#) • Dollar sign ($) • Ampersand (&) • Single quote (') • Asterisk (*) • Period (.) • Left and right parentheses ( ) • Comma (,) • Left and right angle brackets (< >) • Backslash (\) • Left and right square brackets ([ ]) • Colon (:) • Semicolon (;) • At sign (@) • Plus sign (+) • Slash (/) • Equals sign (=) • Question mark (?) • Caret (^) • Underscore (_) • Backtick (`) • Right and left curly brackets ({ }) • Pipe (|) • Tilde (~) • Dash (-)
	Unicode characters between \u0080 and \uFFF

	Double quotes (") if they meet the following criteria:
	• Must be used before the At sign (@)
	  ◦ Valid: "helloworld"@example.com
	  ◦ Invalid: helloworld@"example".com
	• Must be separated by periods (.)
	  ◦ Valid: hello."world"@example.com
	  ◦ Invalid: hello"world"@example.com
	• Must be paired correctly
	  ◦ Valid: "helloworld"@example.com
	  ◦ Invalid: helloworld"@example.com
	• Characters after @ must be a properly formatted domain name

Copyright © 2025 Ping Identity Corporation

Attribute	Supported characters

• **Username**
• **Name**
  ◦ **Formatted**
  ◦ **Given Name**
  ◦ **Middle Name**
  ◦ **Family Name**
  ◦ **Honorific Prefix**
  ◦ **Honorific Suffix**
• **Nickname**
• **Account ID**
• **Title**
• **Type**
• **Address**
  ◦ **Locality**
  ◦ **Region**
  ◦ **Postal Code**
	All characters in the following Unicode general categories:
	• L - Letter
	  ◦ Lu
	  ◦ Ll
	  ◦ Lt
	  ◦ Lm
	  ◦ Lo
	• M - Mark
	  ◦ Mn
	  ◦ Mc
	  ◦ Me
	• N - Number
	  ◦ Nd
	  ◦ Nl
	  ◦ No
	• P - Punctuation
	  ◦ Pc
	  ◦ Pd
	  ◦ Ps
	  ◦ Pe
	  ◦ Pi
	  ◦ Pf
	  ◦ Po
	• S - Symbol
	  ◦ Sm
	  ◦ Sc
	  ◦ Sk
	  ◦ So
	• Z - Separator
	  ◦ Zs
	  ◦ Zl
	  ◦ Zp

Copyright © 2025 Ping Identity Corporation

Attribute	Supported characters

• **Address**
  ◦ **Street Address**
	All characters in the following Unicode general categories:
	• L - Letter
	  ◦ Lu
	  ◦ Ll
	  ◦ Lt
	  ◦ Lm
	  ◦ Lo
	• M - Mark
	  ◦ Mn
	  ◦ Mc
	  ◦ Me
	• N - Number
	  ◦ Nd
	  ◦ Nl
	  ◦ No
	• P - Punctuation
	  ◦ Pc
	  ◦ Pd
	  ◦ Ps
	  ◦ Pe
	  ◦ Pi
	  ◦ Pf
	  ◦ Po
	• S - Symbol
	  ◦ So
	• Z - Separator
	  ◦ Zs

• **Address** ◦ **Country Code**	Two-letter country codes as listed in ISO 3166-2. Three-letter country codes are not supported. **Note** Any string of two uppercase letters is allowed, which means it is possible to enter a value that does not correspond to a country. For example, ZQ is valid in this attribute, but is not a valid country code.

Copyright © 2025 Ping Identity Corporation

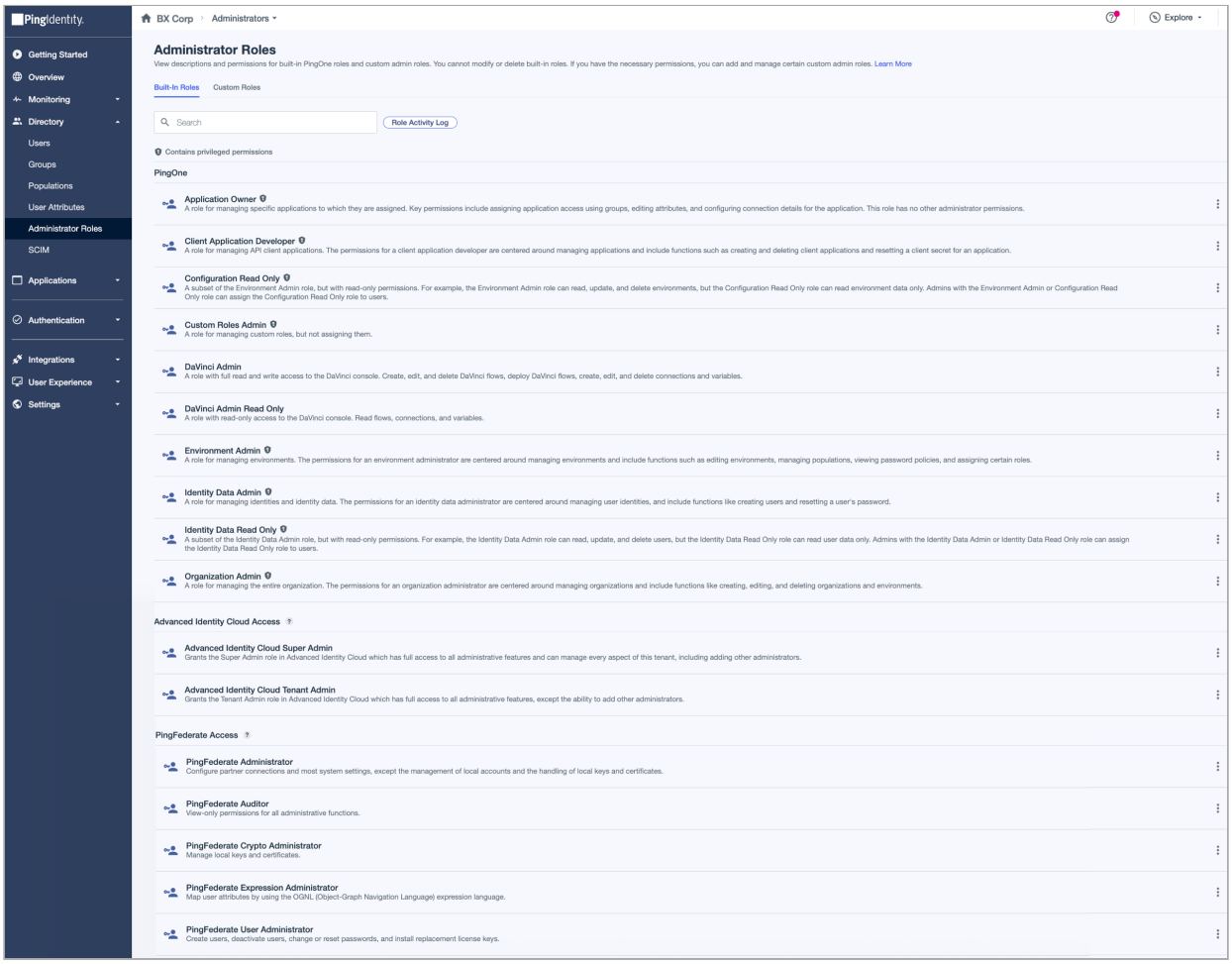
Attribute	Supported characters
• **Primary Phone** • **Mobile Phone**	All characters in the following Unicode general categories: • L - Letter ◦ Lu ◦ Ll ◦ Lt ◦ Lm ◦ Lo • M - Mark ◦ Mn ◦ Mc ◦ Me • N - Number ◦ Nd ◦ Nl ◦ No • P - Punctuation ◦ Pc ◦ Pd ◦ Ps ◦ Pe ◦ Pi ◦ Pf ◦ Po • S - Symbol ◦ Sm ◦ Sc ◦ Sk ◦ So • Z - Separator ◦ Zs **Note** To allow for the many different ways phone numbers are written around the world, the selection of characters that are valid in this attribute is fairly broad. However, this also means that it is possible to enter a value that does not correspond to a valid phone number. The following list contains examples of different phone number formats: • USA: +1 512 555 1212 • USA: +1-512-555-1212 • USA: (512) 555-1212 • Germany: (30) 1234 5678 • Australia: +61 3 1234 5678

Copyright © 2025 Ping Identity Corporation

Attribute	Supported characters
Custom Attributes	Because administrators can define custom attributes that are set to **No Validation** or to a custom **Regex Validation**, supported characters will vary. If the attribute is set to use **No Validation**, all Unicode characters are supported. If the custom attribute is set to use **Regex Validation**, the **Expression** field supports all Unicode characters. The characters allowed by the expression defined in this field are the supported characters for the custom attribute.

Administrator Roles

An administrator role is a collection of permissions that you can assign to a user, application, or connection. Administrator roles give PingOne administrators access to resources in the PingOne admin console and determine the actions they can take in PingOne.



There are two types of administrator roles in PingOne:

- **Built-in roles**

  PingOne provides several built-in administrator roles, such as Environment Admin, Application Owner, and Organization Admin. These roles provide access to a wide variety of resources at multiple levels within PingOne.

Copyright © 2025 Ping Identity Corporation

There are also built-in roles that are used to enable single sign-on (SSO) to other Ping products, such as PingOne Advanced Identity Cloud or PingFederate, and determine the administrator's level of access in those products.

You can't modify built-in administrator roles.

- **Custom roles**

  You can create custom administrator roles to delegate administration of particular resources in an environment and provide least-privileged access to those resources. These roles are environment-specific and consist of a limited set of permissions that can be edited by administrators who have one of the following roles:

  - Organization Admin
  - Custom Roles Admin
  - A custom role with permissions equivalent to the Custom Roles Admin. Learn more in Adding a custom administrator role.

  Like built-in roles, custom roles can be assigned to an individual user, group, worker application, or PingFederate Gateway for a specified level in PingOne. Depending on the environment in which the role is created, a custom role can be assigned at the organization level, environment level, or population level.

  If you want users from multiple environments to have access to the same custom administrator role, you must create the role in each of those environments.

Roles with the **Privileged** icon ( ) include permissions that either provide access to sensitive information, such as personal user data, or allow the bearer to perform actions that could significantly impact the organization, such as deleting an environment. These permissions should be assigned sparingly.

> **Best practice**
>
> Review the permissions associated with the role before you assign the role.

- Learn more about assigning admin roles to users in Managing user roles.
- Learn more about assigning admin roles to a user group in Group roles.
- You can also assign admin roles to worker applications. Learn more in Configuring roles for a worker application.
- Learn more about the permissions associated with built-in administrator roles in PingOne Role Permissions.

Built-In Roles tab

PingOne provides the following built-in administrator roles.

Click a role to open the details pane and view additional details about the role, including the levels to which it can be applied, for example, Environment or Application, and the permissions it includes. Built-in roles cannot be modified, but you can clone a built-in role to use it as the basis for a new custom role that you can modify.

Copyright © 2025 Ping Identity Corporation

Built-in PingOne administrator roles

Role	Description
Application Owner	A role for managing specific applications to which they are assigned. Key permissions include assigning application access using groups, editing attributes, and configuring connection details for the application. This role has no other administrator permissions.
Client Application Developer	A role for managing API client applications. The permissions for a client application developer are centered around managing applications and include functions such as creating and deleting client applications and resetting a client secret for an application.
Configuration Read Only	A subset of the Environment Admin role with read-only permissions only. For example, the Environment Admin role can read, update, and delete environments, but the Configuration Read Only role can read environment data only. Administrators with the Environment Admin or Configuration Read Only role can assign the Configuration Read Only role to users.
DaVinci Admin	(Only applicable for PingOne environments that include the PingOne DaVinci service.) A role that gives PingOne administrators full read and write access to the DaVinci console. Create, edit, and delete DaVinci flows, deploy DaVinci flows, create, edit, and delete connections and variables. The user adding DaVinci to an environment is given the DaVinci Admin role.
DaVinci Admin Read Only	(Only applicable for PingOne environments that include the PingOne DaVinci service.) A role that gives PingOne administrators read-only access to the DaVinci console. Read flows, connections, and variables.
DaVinci Admin	A role with full read and write access to the DaVinci console. Create, edit, and delete DaVinci flows, deploy DaVinci flows, create, edit, and delete connections and variables.
Environment Admin	A role for managing environments. The permissions for an environment administrator are centered around managing environments and include functions such as editing environments, managing populations, viewing password policies, and assigning certain roles.

Copyright © 2025 Ping Identity Corporation

Role	Description
Help Desk Admin	A role for managing user MFA methods and devices and resolving account lockouts. The permissions for a Help Desk Admin are centered around enabling the administrator to help end users successfully authenticate with PingOne and include functions such as resetting passwords and adding or updating MFA methods and devices configured in the user record.
Identity Data Admin	A role for managing identities and identity data. The permissions for an identity data administrator are centered around managing user identities, and include functions like creating users and resetting a user's password.
Identity Data Read Only	A subset of the Identity Data Admin role, but with read-only permissions. For example, the Identity Data Admin role can read, update, and delete users, but the Identity Data Read Only role can read user data only. Administrators with the Identity Data Admin or Identity Data Read Only role can assign the Identity Data Read Only role to users.
Organization Admin	A role for managing the entire organization. The permissions for an organization administrator are centered around managing organizations and include functions like creating, editing, and deleting organizations and environments.

Advanced Identity Cloud Access

For PingOne environments that include SSO to PingOne Advanced Identity Cloud, PingOne includes Advanced Identity Cloud-specific roles. These roles give PingOne administrators access to Advanced Identity Cloud and determine their level of access.

Role	Description
Advanced Identity Cloud Super Admin	A role for managing the Advanced Identity Cloud tenant with all administrator permissions, including adding administrators.
Advanced Identity Cloud Tenant Admin	A role for managing the Advanced Identity Cloud tenant with most administrator permissions, except adding administrators.

PingFederate Access

For PingOne environments that include SSO to PingFederate, PingOne includes PingFederate-specific roles. These roles give PingOne administrators access to PingFederate and determine their level of access to PingFederate.

Copyright © 2025 Ping Identity Corporation

Role	Description
PingFederate Administrator	Configure partner connections and most system settings, except the management of local accounts and the handling of local keys and certificates.
PingFederate Auditor	View-only permissions for all administrative functions. **Note** If a user has the PingFederate Auditor role in addition to another PingFederate role, during SSO to PingFederate, the Auditor role is stripped out and only the other role remains. For example, if you have the PingFederate Auditor and PingFederate Administrator roles, when you SSO to PingFederate, the PingFederate Auditor role is removed, and you will have only the PingFederate Administrator role.
PingFederate Crypto Administrator	Manage local keys and certificates.
PingFederate Expression Administrator	Map user attributes by using the OGNL (Object-Graph Navigation Language) expression language.
PingFederate User Administrator	Create users, deactivate users, change or reset passwords, and install replacement license keys.

Custom Roles tab

If there are custom roles in the environment, they are listed on the **Custom Roles** tab.

Custom administrator role restrictions

Custom administrator roles have certain restrictions that don't apply to the built-in administrator roles:

- Custom administrator roles are not currently supported in PingOne DaVinci.
- Custom administrator roles created in the **Administrators** environment can be assigned at the organization level to users, groups, applications, and gateways in the **Administrators** environment.

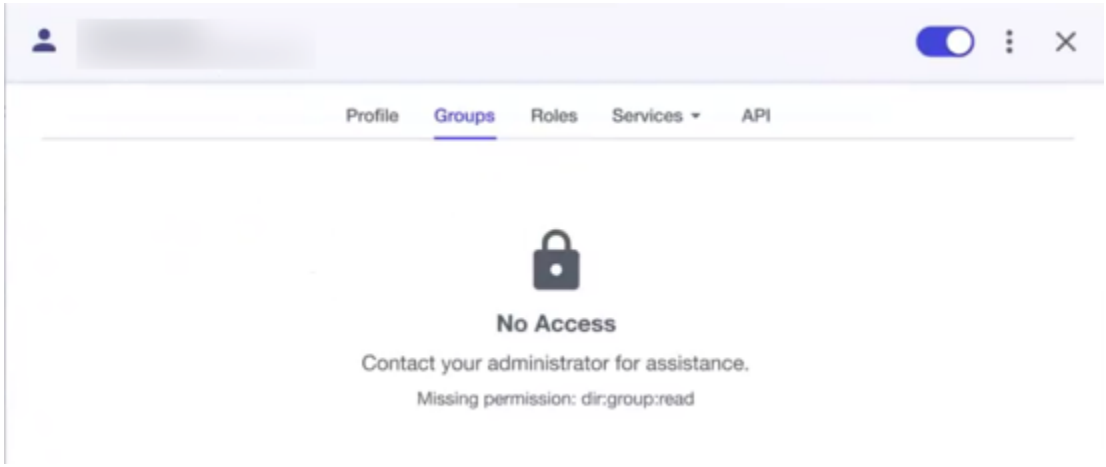
> **Note**
> For the purposes of this documentation, the **Administrators** environment is the environment in your organization that is assigned the ADMIN license. If you renamed your **Administrators** environment, or if you assigned your ADMIN license to a different environment, that environment acts as your **Administrators** environment.
> If you have issues with your ADMIN license, contact Ping Identity Support. The ADMIN license is required for access to certain functionality in PingOne, including some aspects of custom roles.

Copyright © 2025 Ping Identity Corporation

- Custom roles created in any environment other than the **Administrators** environment can't be assigned at the organization level. These roles can only be assigned against resources within the environment in which they were created or over the entire environment.
- Administrators with the Custom Roles Admin role can create custom roles, but only users with the roles selected in the **Assignable by** field for each custom role can assign that role.

> **Important**
>
> We are performing ongoing testing to ensure that all combinations of permissions work as expected for all of the pages in the PingOne admin console. However, it is possible that, at release time, certain combinations have not yet been tested. If you create a custom role, assign it, and find that certain pages do not load properly, know that we are continuing to test, and will resolve all issues. Make a note of the page that didn't load properly, and try again in a few weeks.

If missing permissions are preventing the page from loading properly, a message similar to the following appears.



Related links

- Viewing role details

Viewing role details

Use the **Administrator Roles** page to view details about the roles in your environment.

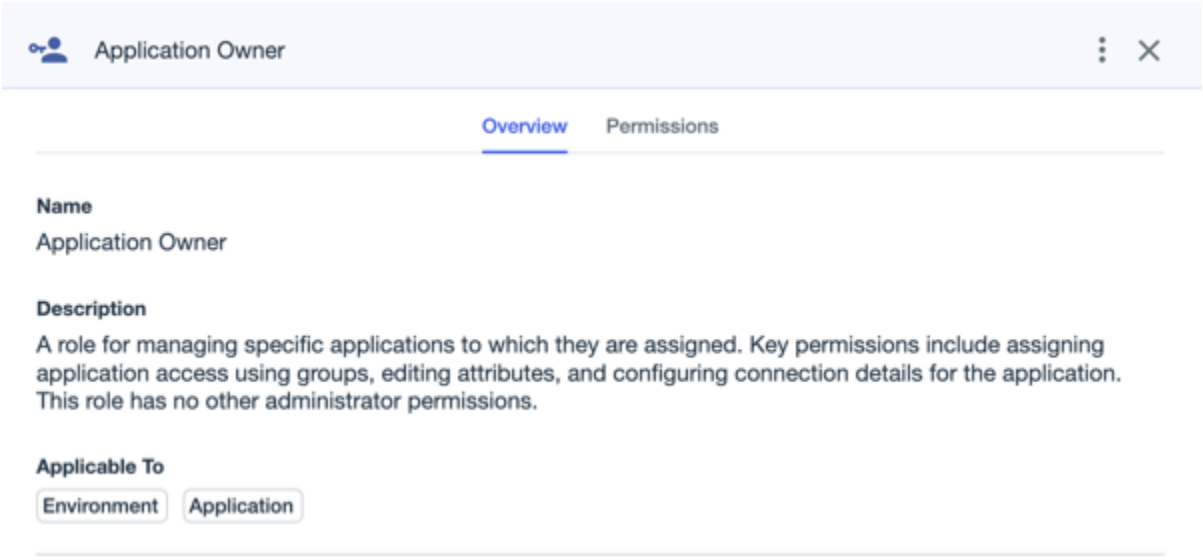
Steps

1. Go to **Directory** > **Administrator Roles** and browse or search for the role you want to view.
2. Click one of the tabs:
   - **Built-In Roles**: View the roles provided by PingOne.
   - **Custom Roles**: View any custom roles that have been created in the environment.
3. Click a role to open the details panel.

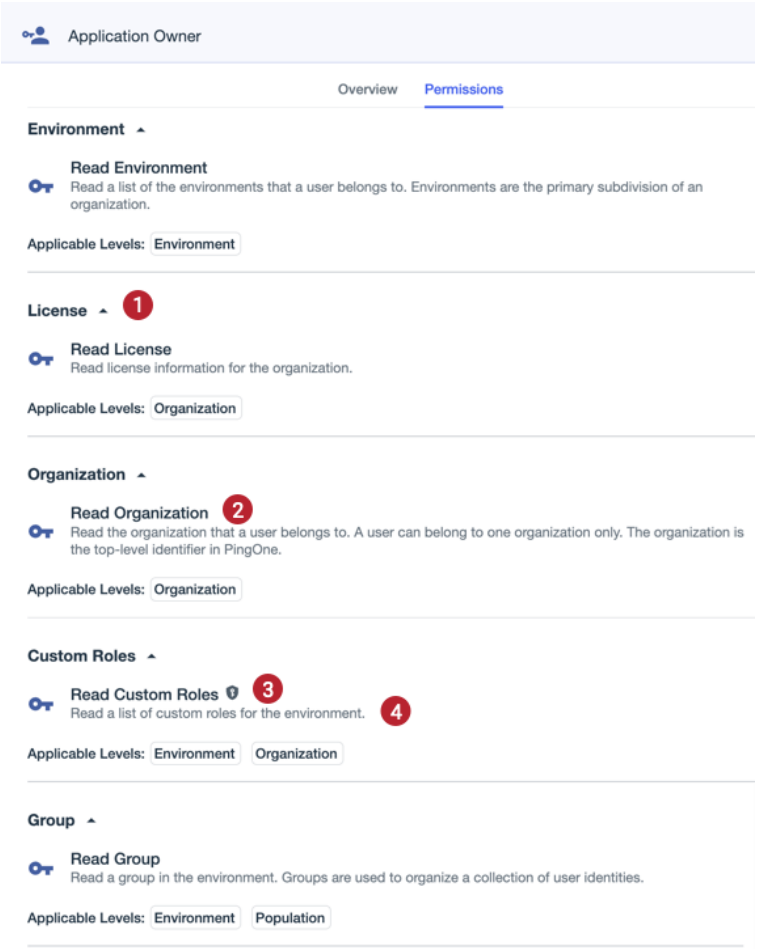
   The **Overview** tab includes the role name and description and the levels at which the role can be assigned.

   For example, **Environment** or **Application**.

Copyright © 2025 Ping Identity Corporation



4. Click the **Permissions** tab to view all of the permissions included in the role.



Copyright © 2025 Ping Identity Corporation

Permissions information:

1. **Category**: Permissions are grouped by category. The categories are based on the area of PingOne to which the permission relates. For example, the **Read License** permission is in the **License** category. The order of the categories is based on the sidebar navigation in PingOne.
2. **Permission name**: The name of the permission is a combination of what the permission enables the user to do (read, update, delete, and so on) and what PingOne resource they can do it to (applications, groups, licenses, and so on).
3. **Sensitive Permission icon** ( ): This icon indicates that the permission either provides access to sensitive information, such as personal user data, or allows the bearer to perform important actions that could negatively impact the organization, such as deleting an environment.
4. **Permission description**: Detailed information providing more context about what the permission allows.

> **Note**
>
> PingOne built-in administrator roles include many permissions. You can collapse the categories and use the scroll bar to view more permissions.

Adding a custom administrator role

Use the **Administrator Roles** page to add custom roles to the environment.

Before you begin

You must have one of the following roles to create a custom role:

- Organization Admin
- Custom Roles Admin
- A custom role with permissions equivalent to the Custom Roles Admin

Steps

1. In the sidebar, click the Ping Identity logo to open the **Environments** page.
2. Click the environment in which you want to add the new custom role and click **Manage Environment**.
3. Go to **Directory > Administrator Roles** and click the **Custom Roles** tab.
4. Click **Add Custom Role**.

> **Note**
>
> If you are creating this role outside of the **Administrators** environment, the role can be assigned only against resources within this environment or to the entire environment.

5. From **Initial Permissions**, select a basis for the new role.
    - **Permissions Sets**
        - **No Permissions**: Start building a new role without any permissions included.

Copyright © 2025 Ping Identity Corporation

- **Essential Permissions**: Start building a new role with the minimum set of permissions needed for the role to be usable.

- **Roles**

  Select an existing role to use as the basis for the new role. Permissions included in the role are added to the new role. You can add or remove permissions as needed in the following steps. You can use a built-in role or custom role as the basis for a new role.

  > **Note**
  >
  > You can use only roles that are assigned to you or that confer the permissions needed to assign that role to others.

  > **Best practice**
  >
  > Use an existing role as the basis for the new role, then remove the permissions you don't want the new role to have and add other permissions as needed. If you build a role without any starting permissions, users with that role could have issues accessing required functionality in the admin console. In some cases, the admin console might not load properly.

6. Enter a **Name** for the new role.

   > **Note**
   >
   > The role name must be unique within the environment.

7. (Optional) Enter a **Description** for the new role.

   > **Tip**
   >
   > **Best Practice:** Enter information about the intended use of the role in your description.

8. In **Assignable by**, select the roles that are allowed to assign this role to others.

9. In the **Advanced** section, you can restrict the role assignment so that it can only be assigned at a particular level.

   For example, if you want a role to be assigned only to manage individual populations in an environment but not the entire environment, select **Population**.

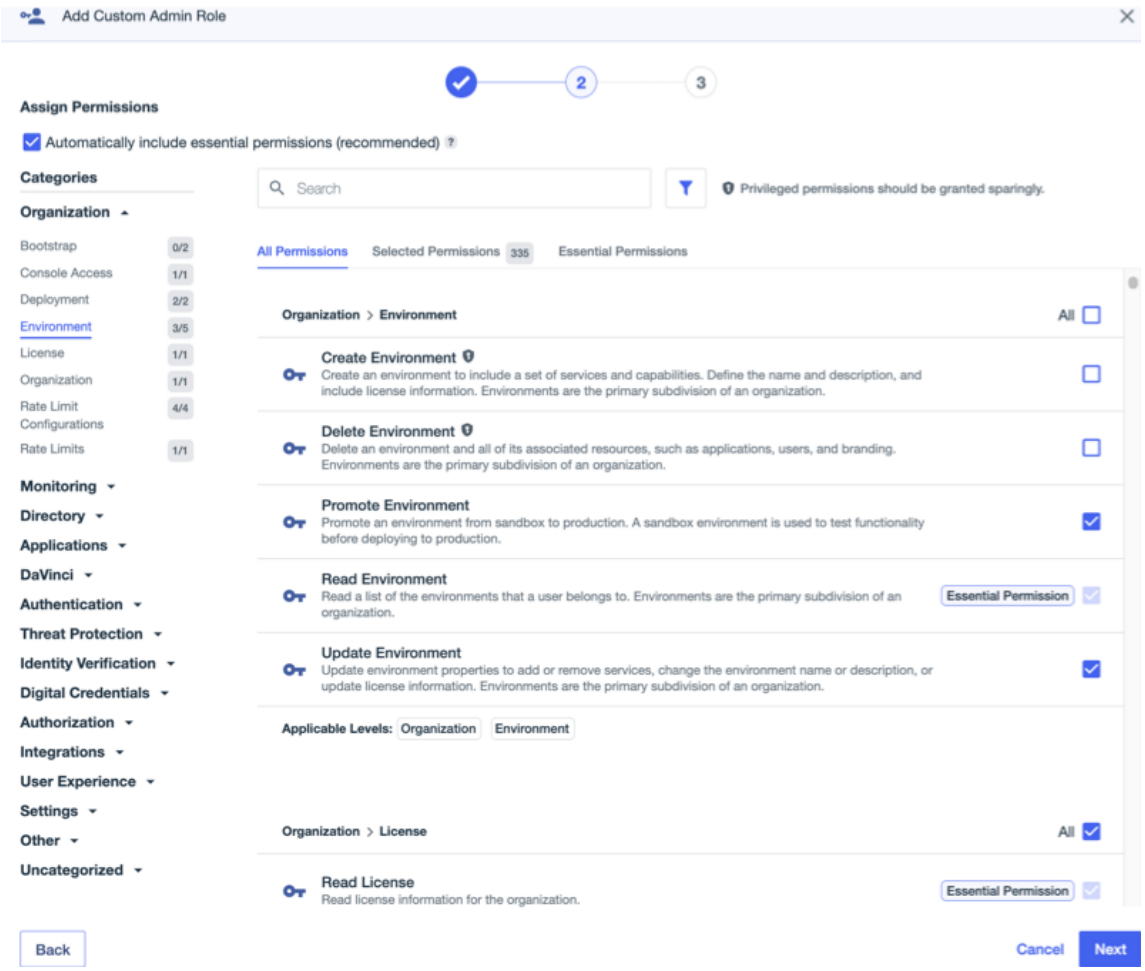
   > **Note**
   >
   > If you are creating this role in any environment other than the **Administrators** environment, you cannot enable the role to be assigned at the **Organization** level.

10. Click **Next**.

11. Add or remove permissions as needed.

    > **Tip**
    >
    > Leave **Automatically include essential permissions (recommended)** selected to ensure that your role has the minimum permissions needed to function properly.

Copyright © 2025 Ping Identity Corporation



The **Selected Permissions** tab lists the permissions that are currently selected for the role. The number in the tab header tells you how many permissions are currently associated with the role. The previous image shows a role with 335 permissions.

There are several ways to locate permissions you want to add to or remove from the role:

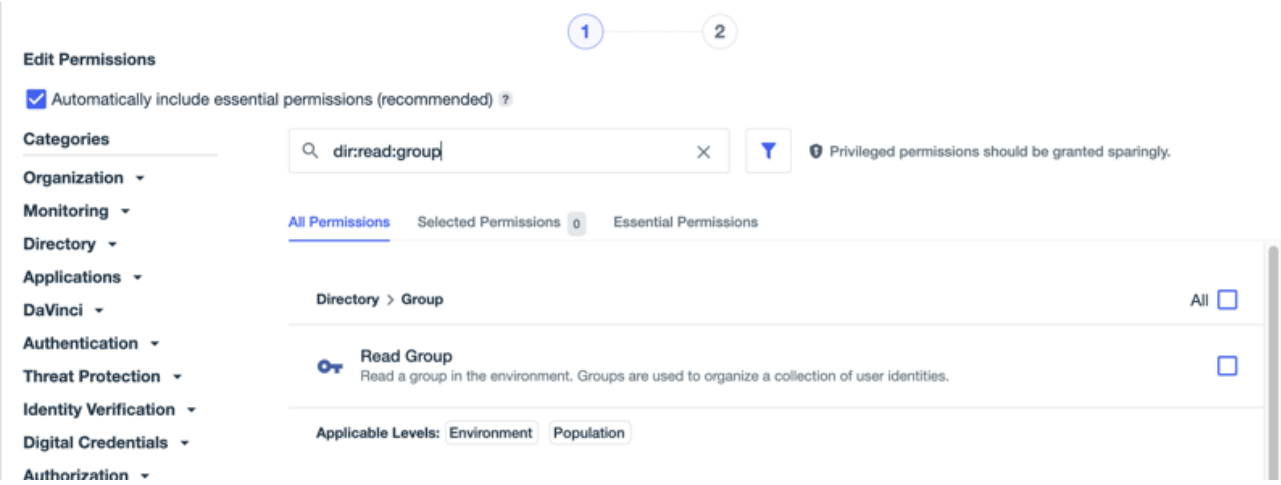
- Using the **Categories** list: In the left pane, permissions are organized under top-level categories that mirror the sidebar navigation pane in PingOne. Expand a top-level category to view the related categories and locate the permissions you want to add or remove from this role.

  The first number next to the category name indicates how many permissions in that sub-category are selected for inclusion in the role. The second number indicates the total number of permissions in that category. For example, in the previous screenshot, the current role configuration includes three of the permissions in the **Environment** category, and that category contains five permissions total. Click a category to view the permissions included in the category, including the permission name and a detailed description of what actions the permission allows the bearer to perform in PingOne.

- Using the **Search** functionality: The search looks for your criteria in the permission name or detailed description.

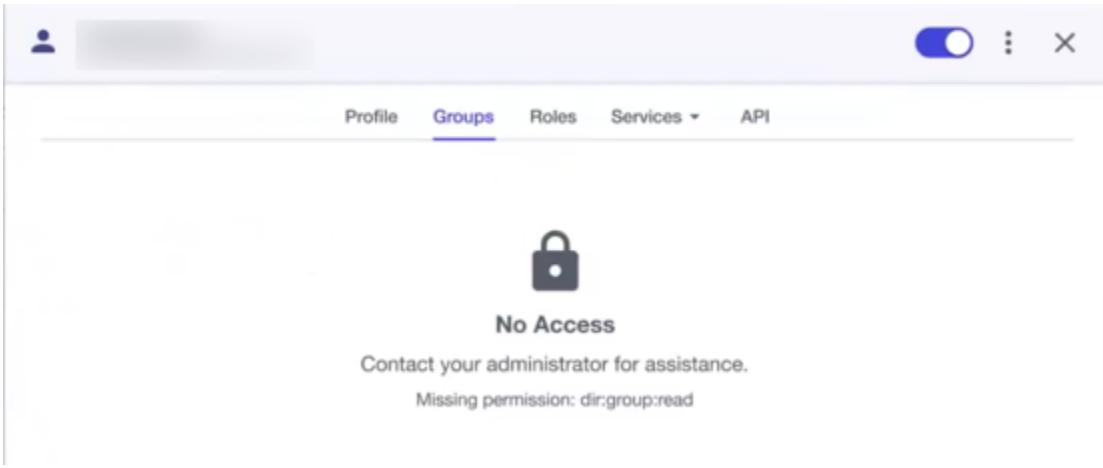
  You can also search for a permission using the permission identifier, for example `dir:read:group`. The identifier is a three-part, colon-delimited string that represents the category, action, and resource to which the permission applies. For the previously mentioned identifier, `dir` represents the **Directory** category, `read` is the action, and `group` is the resource.

Copyright © 2025 Ping Identity Corporation



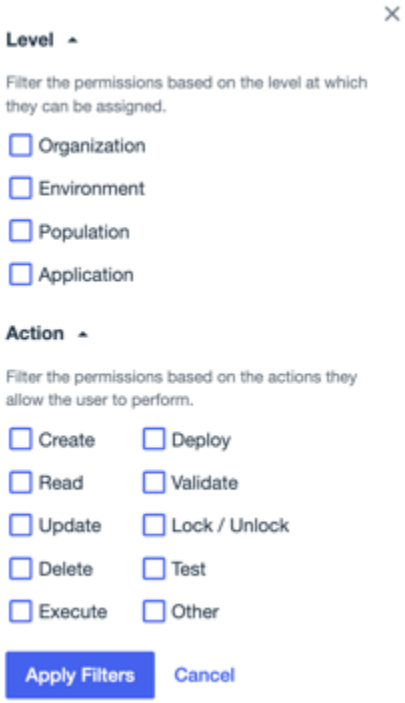
Learn more about the identifiers for permissions in PingOne Permissions by Identifier in the API documentation.

> **Note**
>
> The string identifier is also used when a user tries to access an environment resource in PingOne, but does not have the appropriate permissions for access. A message uses the string identifier to indicate that they are missing a necessary permission. That string can be sent to an administrator to search for and update the user's permissions if needed.



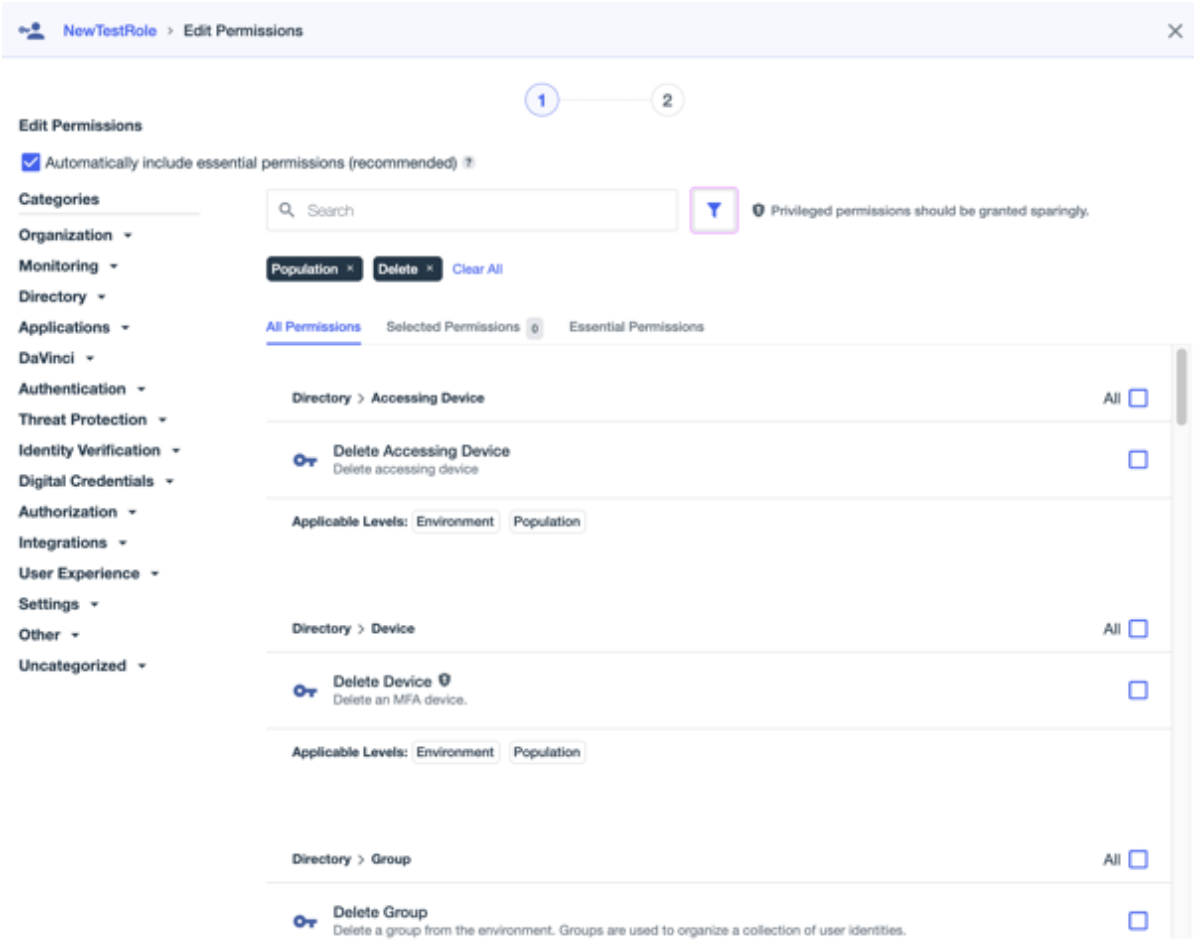
- Using the **Filter**: Click the **Filter** icon to find permissions based on the level at which they apply or the actions they permit.

Copyright © 2025 Ping Identity Corporation



For example, select **Population** and **Delete** to find all permissions that can be applied at the population level and that allow the bearer to delete resources.

Copyright © 2025 Ping Identity Corporation



Badges below the **Search** box indicate the filters that are selected. Click the **X** on a badge to remove the filter condition. Click **Clear All** to remove all conditions.

- Using a combination of the search functionality and the filters.

> **Tip**
>
> To find a permission that you want to remove from the role, perform searches and filtering on the **Selected Permissions** tab. To find a permission you want to add, perform searches and filtering on the **All Permissions** tab.

12. Click **Next**.

    If you included privileged permissions in the role, you are prompted to confirm that you want to include them. Click **Continue** to include them, or click **Cancel** to go back and remove them from the role.

> **Caution**
>
> Privileged permissions should be selected sparingly and only after careful consideration of the potential impact.

13. Review the role on the next page and click **Save**.

Result

Copyright © 2025 Ping Identity Corporation

The role is added to the **Custom Roles** tab on the **Administrator Roles** page and can now be assigned to users, groups, applications, or connections.

Custom role scenarios

Your organization wants you to create two custom roles for Support personnel. You are assigned the Custom Roles Admin role, and you have that role at the Organization level. This means that you can create custom roles in all of the environments in the organization. These roles will be assigned and used in different ways in the three scenarios that follow.

The first role, Support Level 2, is an advanced role for help desk employees. We'll create this role first, because we want it to exist when we create the Support Level 1 role. This role includes all of the permissions we will include in the Support Level 1 role, but also includes permissions for creating, reading, updating, and deleting users, locking user accounts, resetting user passwords, and assigning administrator roles to users. This role can be assigned by users with the Identity Data Admin role.

> **Note**
>
> Without a custom role, you would need to assign, at a minimum, the built-in Identity Data Admin role to give a user the permissions they need to perform these tasks. That role contains a total of 160 permissions, many of which you might not need or want a support user in this capacity to have.

The second role, Support Level 1, is an entry-level role for help desk employees and users with the role should only be able to read user records, and reset user passwords. This role can be assigned by users with the Identity Data Admin or the Support Level 2 roles.

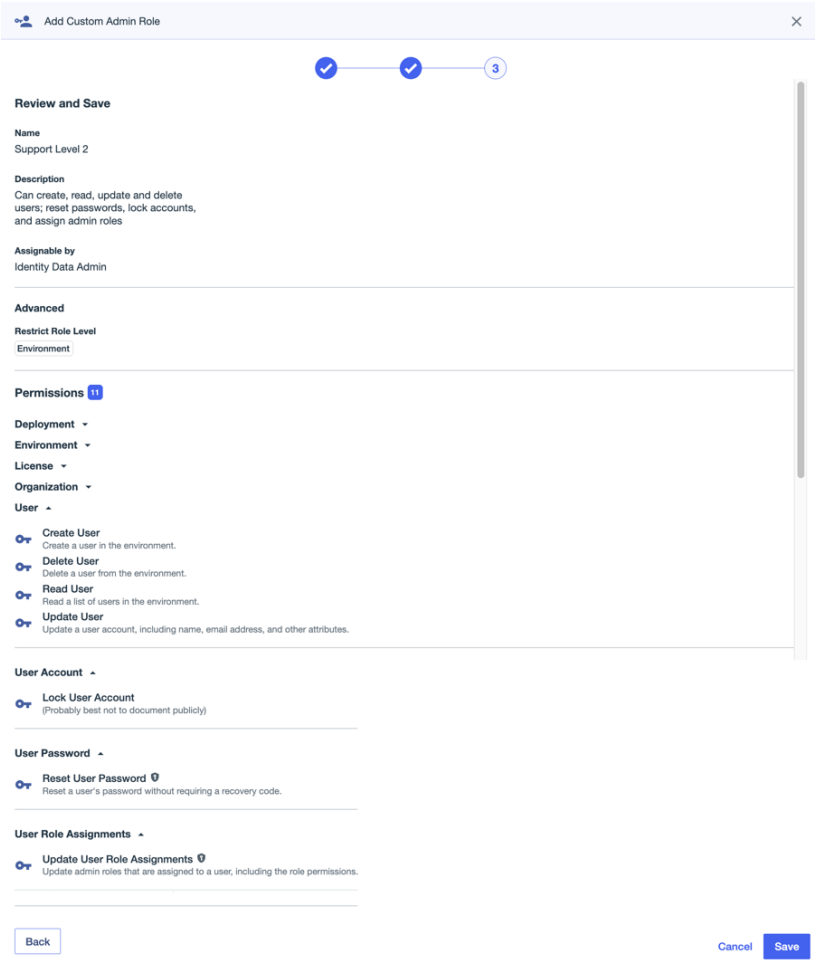
> **Note**
>
> Again, without custom roles, this user would require the built-in Identity Data Admin role at a minimum, because that is the role with the fewest permissions that includes the Reset User Password permission.

You create these roles in the **Administrators** environment, because that's the environment in which administrator identities should be created. You select to include the essential permissions. There are currently four essential permissions, so the number of selected permissions is four plus the number of permissions you select manually. For example, you add seven permissions to the Support Level 2 role, so that role now has 11 total permissions assigned.

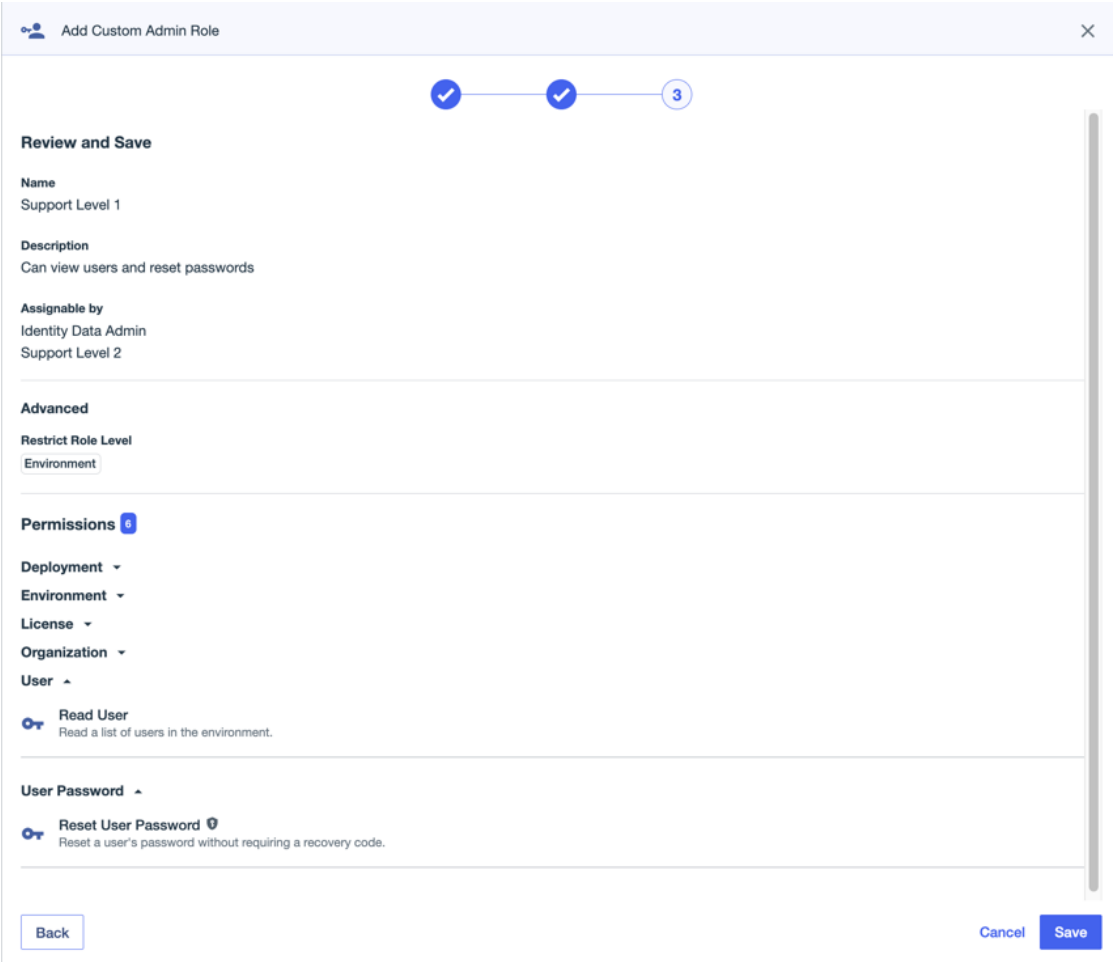
New roles created

Support Level 2 role summary

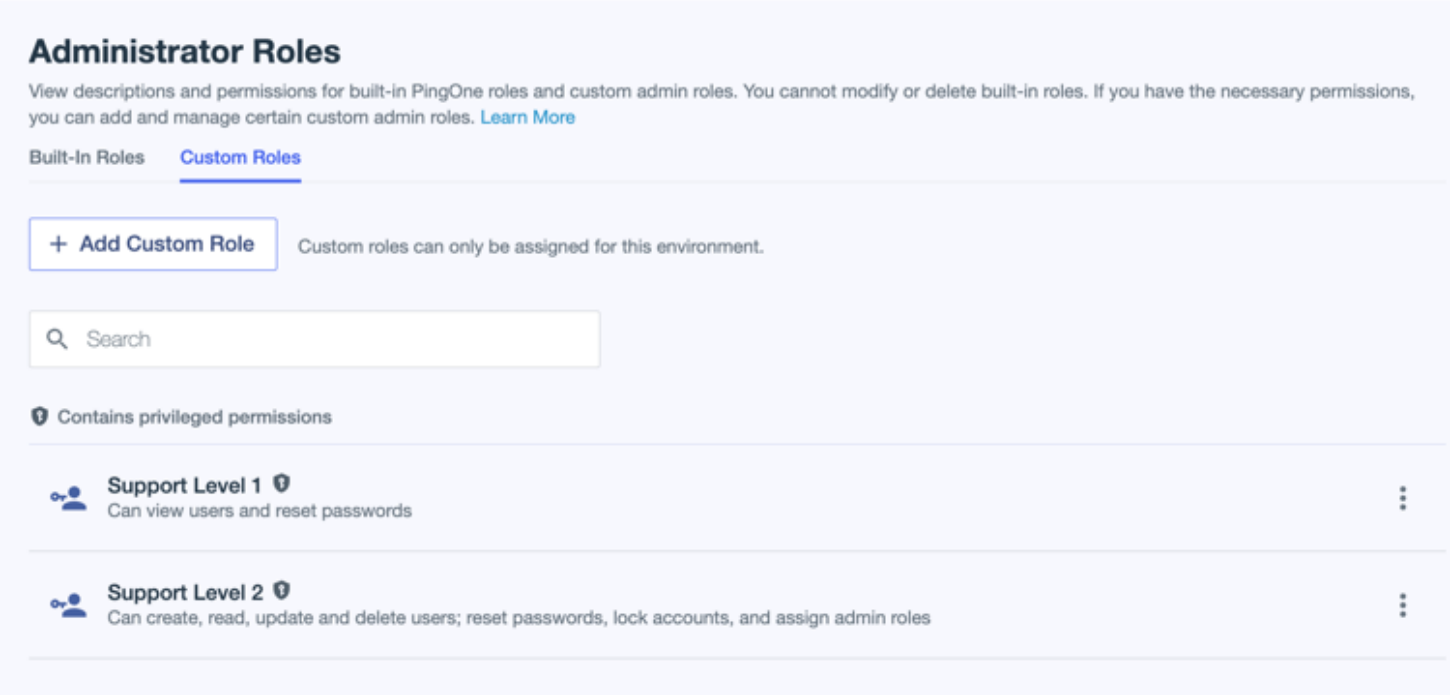
Copyright © 2025 Ping Identity Corporation



Support Level 1 role summary



New roles displayed on Custom Roles tab of Administrator Roles page



Copyright © 2025 Ping Identity Corporation

> **Note**
>
> The following scenarios show administrators assigning custom roles to users, but you can also assign custom roles to groups, worker applications, or PingFederate gateways, just like built-in roles.

Scenario 1: Custom role assignment within a single environment

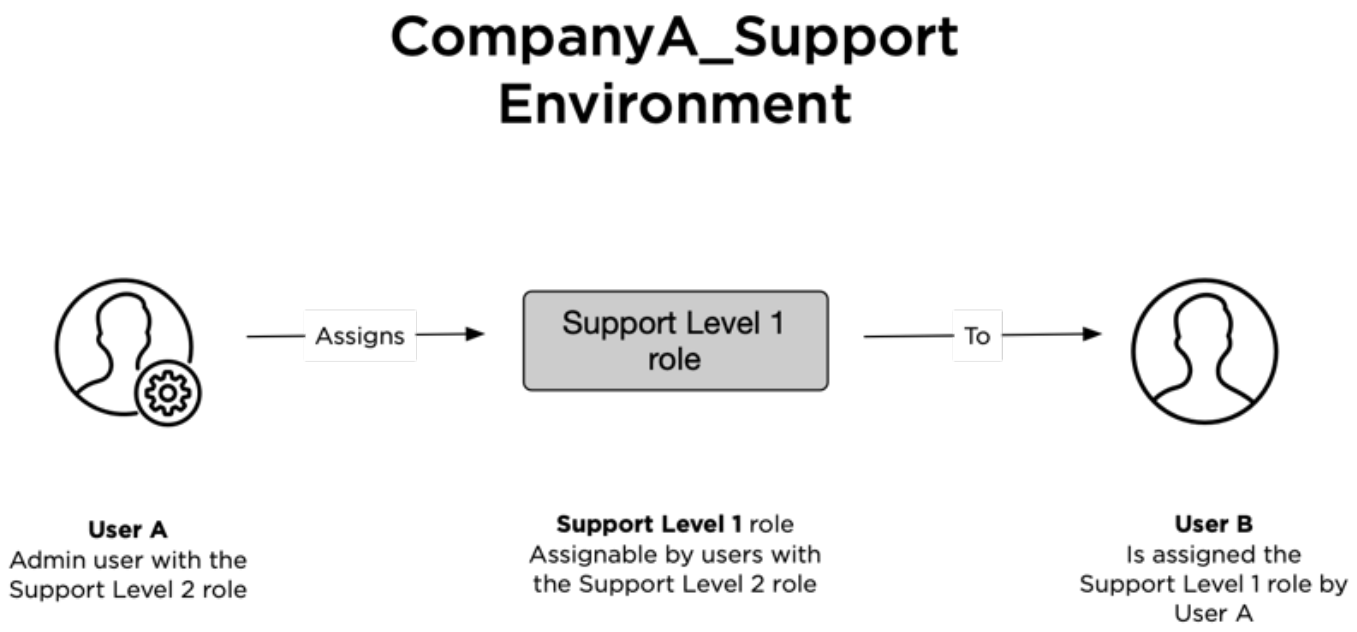
The goal of this scenario is for a user in an environment to assign a custom role to another user in the same environment.

If two users exist in the same environment, and you create a custom role in that environment, a user with the applicable **Assignable by** role can assign the custom role to another user in the same environment.

In this scenario:

- User A has the Support Level 2 role in the CompanyA_Support environment.
- User B is also in the CompanyA_Support environment.
- Administrators with the Support Level 2 role can assign the Support Level 1 role.
- User A assigns the Support Level 1 role to User B.

> **Note**
>
> Because this is not the **Administrators** environment, User A can’t assign the role at the organization level or to any environment resource outside of the CompanyA_Support environment.



Scenario 2: Custom role assignment from the Administrators environment

The goal of this scenario is to assign custom roles to two administrators and allow them to manage different environments in the organization.

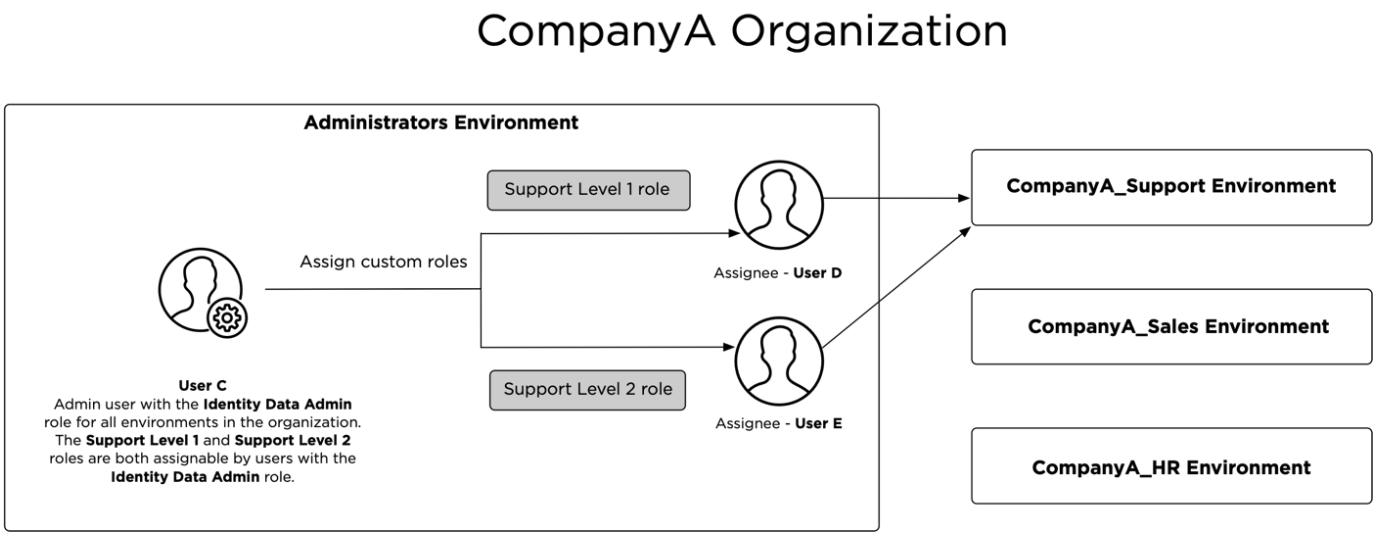
Copyright © 2025 Ping Identity Corporation

To assign the Support Level 1 or Support Level 2 roles to users over multiple environments or the entire organization, the roles must be created in the **Administrators** environment. The general role assignment rules apply, which means:

- The user who is going to assign the custom role must exist in the Administrators environment.
- This user must have a role that can assign the new custom role.
- This user must have that role scoped over the environments in which you want them to be able to assign users to manage with the new custom role.

In this scenario:

- User C exists in the **Administrators** environment. They are assigned the Identity Data Admin role for all environments in the organization. The Identity Data Admin role can assign both the Support Level 1 and Support Level 2 roles.
- Because User C has the Identity Data Admin role for all of the environments in the organization, they can assign the Support Level 1 and Support Level 2 roles to users over any environment in the organization.
- User D and User E also exist in the **Administrators** environment.
- User C assigns the Support Level 1 role to User D and the Support Level 2 role to User E. Both are scoped to the CompanyA_Support environment.



Scenario 3: Custom role assignment for delegated administration of another environment

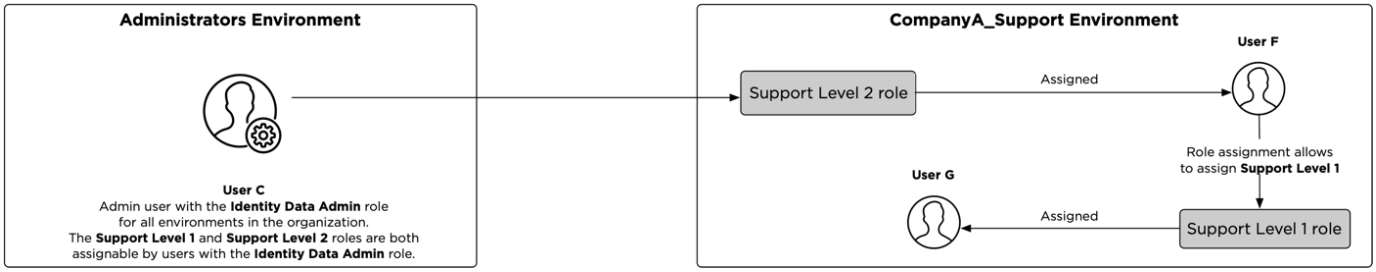
The goal of this scenario is for an administrator with a built-in role to assign custom support roles to users that are in a different environment.

In this scenario:

- User C exists in the **Administrators** environment. They are assigned the Identity Data Admin role for all environments in the organization.
- User F and User G exist in the CompanyA_Support environment.
- Both the Support Level 1 and Support Level 2 roles are created in the **CompanyA_Support** environment. These roles are assignable by the Identity Data Administrator role.

Copyright © 2025 Ping Identity Corporation

- Because User C has the Identity Data Admin role for all of the environments in the organization, they can assign the Support Level 2 role to User F in the CompanyA_Support environment.
- User F can then assign the Support Level 1 role to User G because Support Level 1 role is assignable by either the Identity Data Admin or the Support Level 2 role, and the users both exist in the CompanyA_Support environment.

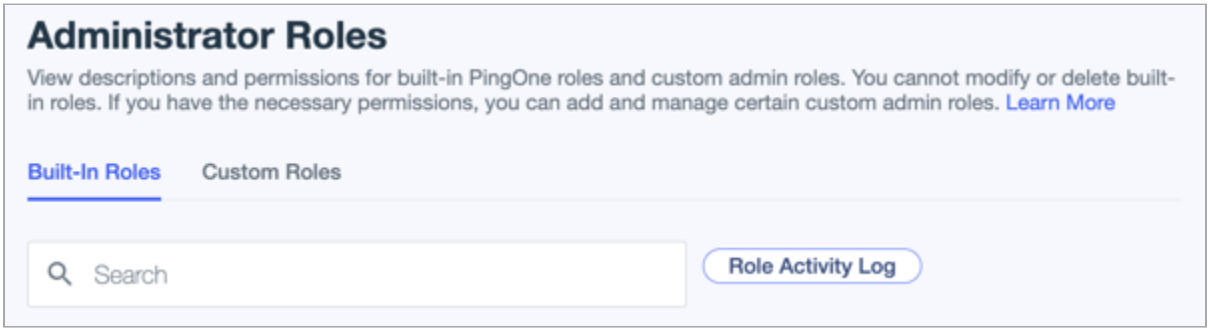


Viewing administrator role events

Administrator roles can give the bearer considerable control over environment resources, so best practice is to closely monitor role assignment activity. You can generate an audit report that's already configured to include only role assignment event information directly from the **Administrator Roles** page.

Steps

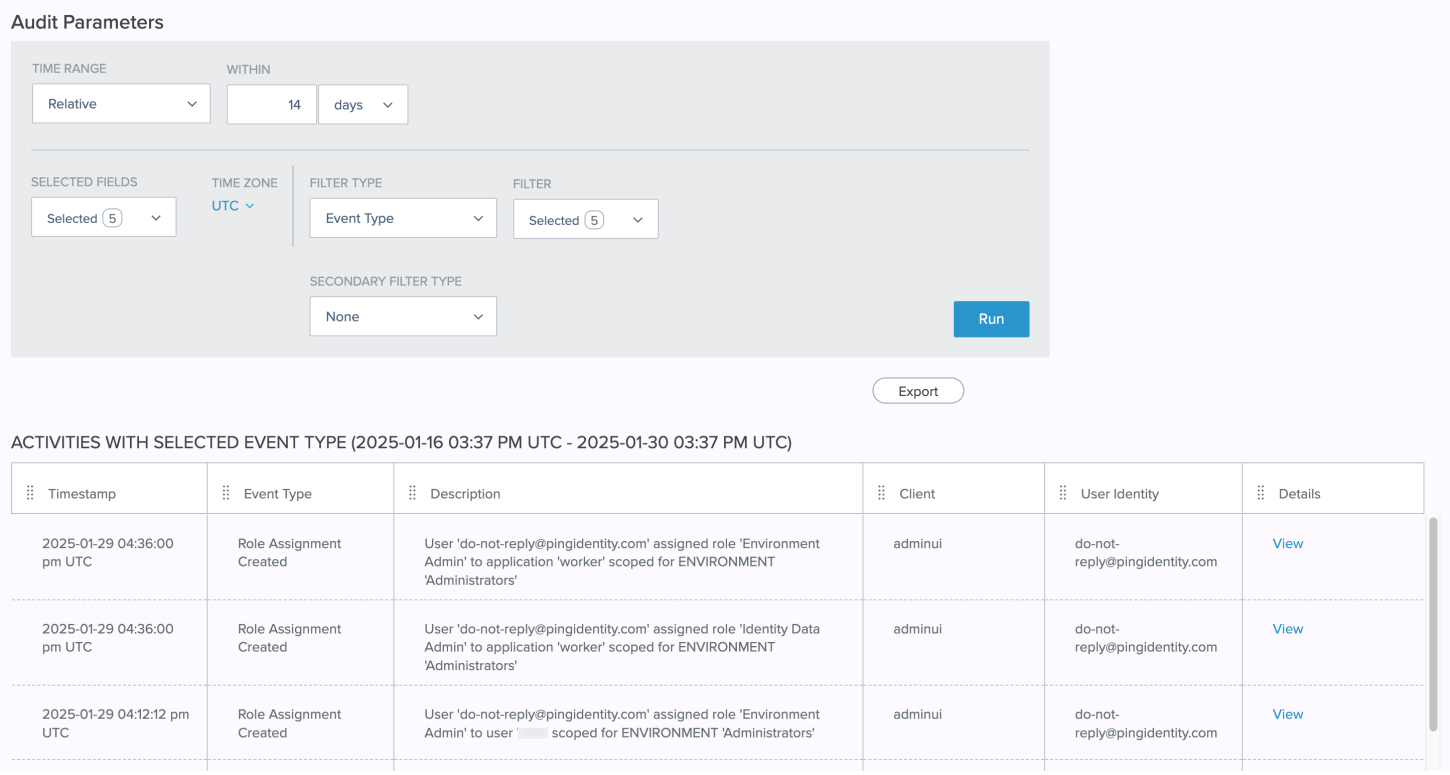
1. In the PingOne admin console, go to **Directory** > **Administrator Roles**.
2. Click **Role Activity Log**.



Result

The audit report opens and is filtered to show only role events that occurred within the last 14 days.

Copyright © 2025 Ping Identity Corporation



The **Description** column includes detailed information for each role event. The information included depends on the event type, but could include the following:

- Whether a role assignment was created (assigned to a user) or deleted (removed from a user).
- The scope, or level, at which the role assignment change was made. For example, environment, organization, population, or application.
- The name of the role that prompted the event. For example, Environment Admin, Application Owner, and so on. This might also be the name of a custom role.
- The name of the administrator who performed the action.

> **Note**
>
> You can set additional parameters or change the time range and run the report again to look for different information. Learn more in Audit parameters.

Learn more

- Running an audit report
- Administrator Roles

Group roles

To make permissions management easier, you can assign roles to groups and individual users.

Copyright © 2025 Ping Identity Corporation

Using group roles, you can:

- Manage roles for multiple users at once.
- Apply role changes in bulk.
- See users that have a certain role by viewing group members.

You can use roles to manage permissions for groups of administrators. Learn more in Managing administrators.

For security reasons, only static groups can have roles assigned to them. That is, you can't assign roles to groups that have members included based on a filter or rule. With a dynamic group, you might inadvertently add users to the group that would inherit role assignments. Learn more in Static and dynamic groups.

When adding users to groups that have roles assigned, be careful not to inadvertently assign a role to a user by adding them to a group. If a user has a role from being in a group, remove the user from the group to remove the role. If a user has a role assigned to them individually, you can remove the role from the user.

Note

- You can assign only roles that are assigned to you, or that are assignable by those roles. For example, the Identity Data Admin role has permissions that allow it to assign the Identity Data Admin Read Only role. Therefore, if you are assigned the Identity Data Admin role, you can assign that role or the Identity Data Admin Read Only role to a group.
- An admin might not have permissions to assign roles but can add or remove users from a group that has role assignments. In other words, one admin can assign roles to a group, and a different admin can add or remove users from that group.
- You cannot assign roles to a group that you are a member of.
- You cannot add or remove yourself from a group that has roles assigned to it.
- Roles assigned to a group will not affect roles that are assigned to a user individually.
- You can assign roles in up to 500 groups.

Learn more in Creating a group and Managing group membership.

Copyright © 2025 Ping Identity Corporation

Applications

The **Applications** branch contains the **Applications**, **Application Catalog**, **Resources**, and **Application Portal** pages.

See the following:

- Applications
- Application catalog
- Resources
- Application portal

Applications

You can add applications to your environment so that PingOne can manage access to the applications.

When you add an application, PingOne creates a client ID for the application, which is a unique identifier for the application and cannot be changed.

> **Note**
>
> To enable or disable an application, click the toggle in the **Applications** list.

PingOne supports several application types. Use the application type that best fits your requirements.

SAML application

A browser-based application with a server-side component, such as .NET web apps, JSP/Java, Node.js, or Ruby on Rails. SAML applications typically have functions similar to desktop applications, and use SAML for authentication.

- Adding an application
- Editing an application - SAML

OIDC Web application

A browser-based application with a server-side component, such as .NET web apps, JSP/Java, Node.js, or Ruby on Rails. OIDC web applications typically have functions similar to desktop applications, and use OIDC for authentication.

- Adding an application
- Editing an application - OIDC

Native application

An application that's installed and run directly on the local operating system, like Java, Objective-C, Swift, or React. Native applications are typically intended for mobile devices. Native applications use OIDC for authentication. A native application can be used as both an accessing application and as an authenticating application for MFA.

- Adding an application
- Editing an application - Native

Copyright © 2025 Ping Identity Corporation

Single page application

A browser-based application that runs on the front-end with no server-side component, such as Sencha Touch, AngularJS, and React. A single page application runs on the client side after it loads, so it can't keep a client secret. Single page applications use OIDC for authentication.

- Adding an application
- Editing an application - Single page

Device authorization

An application that allows a device to obtain authorization from the user through a second device, such as a smartphone. Device authorization is typically used for applications that run on an input-constrained, Internet-connected device, such as a smart TV.

- Adding an application
- Editing an application - Device authorization

Worker

An administrator application that can have the same roles as human administrators. Worker applications are configured with the client credentials grant type by default, but can be configured to support multiple grant/response types, just like the other application types. Worker applications use OIDC for authentication.

You can use Worker applications to create a userless service application that can perform administrator functions. The role assignments determine which functions the application can do. The Worker application can also perform administrator functions with the role of its user. To do this, give the application an additional grant type, which is used instead of the role assignments.

Worker applications can use a user-based grant type (`implicit` or `authorization_code`). With this configuration, you can assign only OIDC scopes to the application. When getting a token using a user-based grant type, the user's role assignments are used. When getting a token using the `client_credentials` grant type, the application's role assignments are used.

> **Note**
>
> Worker apps can't be used to facilitate end-user sign-ons, but they can be used to sign on users that have roles.

- Adding an application
- Editing an application - Worker

Viewing application details

Use the **Applications** page to view details for applications that are managed by PingOne.

Steps

1. Go to **Applications** > **Applications**.

   You can also search for applications or narrow your search to a particular application type.

Copyright © 2025 Ping Identity Corporation

Result:

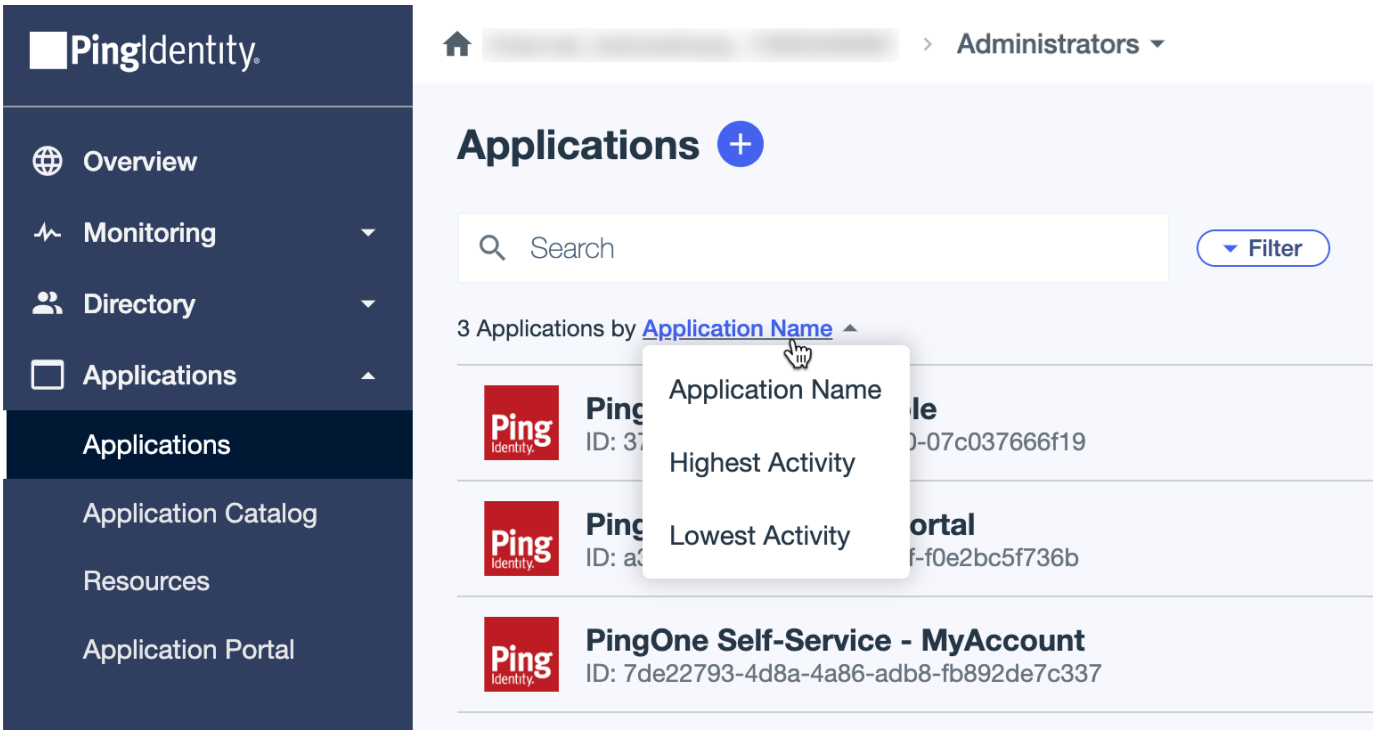
The **Applications** page shows a list of configured applications as well as the client ID and average daily sign-ons for each application.

> **Note**
>
> The **Applications** list also shows the system applications: **PingOne Admin Console**, **PingOne Application Portal**, and **PingOne Self-Service Application - MyAccount**.

2. (Optional) To go to the reporting page and run a report on the relevant authentication events, click the 12-week trend.

   Learn more in Viewing sign-on statistics by application.

3. To sort by application name, highest activity, or lowest activity, click **Application Name** at the top of the **Applications** list.



4. To open the details panel for a particular application, click the application entry.

   The application details panel shows several tabs, but the tabs vary depending on the type of application. For example, only worker applications have the **Roles** tab. Learn more about the different application types in Applications.

   The application details panel includes the following tabs, depending on the type of application:

Overview

General

General information about the application. Use this page to see your application details at a glance. Learn more in Editing an application.

- **App Type**: The type of application that was selected when the app was added, such as SAML, OpenID Connect (OIDC), Native, or Single page.

Copyright © 2025 Ping Identity Corporation

- **Description** (optional): A brief description of the application.
- **Environment ID**: The environment to which the application was added. Use the **Copy to clipboard** icon to copy the environment ID.
- **Client ID**: The unique identifier for the application. Use the **Copy to clipboard** icon to copy the client ID.
- **Client Secret** (OIDC applications only): A secret code that is shared between the application and PingOne. You might need this value to get an access token or to integrate your application with other applications. Keep the client secret confidential.
- **Home Page URL**: The default home page for the application.
- **Signon URL**: The URL to which the application requests that the end user be redirected to sign on.

Connection Details

- Endpoints needed to set up or configure the application. For example, **OIDC Discovery Endpoint** for OIDC applications or **Initiate Single Sign-On URL** for SAML applications.

Configuration

Configuration details that are specific to the type of application. For example, an OIDC application shows the authorization URL and token endpoint, among others, and a SAML application shows the ACS URLs and single logout (SLO) endpoints, among others. Learn more in Editing an application.

Resources

Scopes for the application. The **Resources** tab does not apply to SAML applications. Learn more in Resources.

Policies

Authentication policies associated with the application. Learn more in Authentication policies for applications.

Attribute mappings

Associations between PingOne user attributes and SAML or OIDC attributes in the application. For example, `Email Address` in PingOne could be mapped to `NameID` in a SAML application. Learn more in Mapping attributes.

Access

Groups that can access the application. Learn more in Groups.

Roles (Worker applications only)

Role assignments for the application. Roles are used to assign permissions to a worker application. Learn more in Administrator Roles.

Mobile (Native applications only)

Push notification methods for the application, typically an authenticator application on a mobile device. Learn more in Editing an application - Native.

Copyright © 2025 Ping Identity Corporation

Viewing sign-on statistics by application

The **Applications** page shows sign-on statistics for each application in the form of a 7-day average and 12-week trend chart. You can use this information to identify usage irregularities and application popularity as well as to identify risks associated with disabling an application.

Steps

1. Go to **Applications** > **Applications**.

   You can also search for applications or narrow your search to a particular application type.

2. To go to the reporting page and run a report on the relevant authentication events, click the 12-week trend.

Result

The **Applications** page shows a list of configured applications as well as the client ID and average daily sign-ons.

Adding an application

Add applications to your environment so that PingOne can manage access to the applications.

About this task

Use the **Applications** page to add an application to be managed by PingOne. Learn more about the different types of applications in Applications.

> **Note**
>
> Some application settings can only be configured after the application is created. Learn more in Editing an application.

PingOne supports the following application types:

- SAML
- OIDC
- Native
- Single page
- Device authorization
- Worker

Steps

1. Go to **Applications** > **Applications**.
2. Click the **+** icon.
3. Create the application profile by entering the following:
   - **Application name**: A unique identifier for the application.

Copyright © 2025 Ping Identity Corporation

- **Description** (optional): A brief description of the application.
- **Icon** (optional): A graphic representation of the application. Use a file up to 1MB in JPG, JPEG, GIF, or PNG format.

4. Choose the **Application Type**. Learn more in Applications.

   You can also choose Application Catalog to use a templated integration.

5. If you're creating a **SAML Application**, click **Configure**, and then specify the details of the connection between the application and PingOne.

   You can enter the values manually, or import them from a file or URL.

   Choose from:

   - Import the configuration details from an XML metadata file. Select **Import Metadata**. Click **Select a File** and then select an XML metadata file on your file system. Click **Open**.

     The configuration values are populated based on the information in the metadata file.

     > **Note**
     > If the metadata file does not specify all the configuration values, you must enter the missing values manually.

   - Import the configuration details from a metadata URL. Select **Import from URL**. Enter the URL and then click **Import**.

     > **Note**
     > The URL must be a valid absolute URL.

     The configuration values are populated based on the information from the URL.

   - Enter the configuration details manually. In the **ACS URLs** field, enter the Assertion Consumer Service (ACS) URLs. You must specify at least one URL, and the first URL in the list is used as the default.

   In the **Entity ID** field, enter the service provider entity ID used to look up the application. The Entity ID is a required property and is unique within the environment.

6. Click **Save**.

7. To enable the application, click the toggle at the top of the details panel to the right (blue).

   > **Note**
   > You can disable the application by clicking the toggle to the left (gray).

Next steps

After the application is created, you can edit the application settings, configure application policies, and control application access. Learn more in Editing an application, Applying authentication policies to an application, and Application access control.

Copyright © 2025 Ping Identity Corporation

Editing an application

Use the **Applications** page to modify applications that you've already added to PingOne.

About this task

The details of editing an application vary based on the type of application you're editing.

Learn more about the different types of applications in Applications. If you're creating a new application, learn more in Adding an application.

You can edit the following application types:

- SAML
- OpenID Connect (OIDC)
- Native
- Single page
- Worker
- Device authorization

Editing an application - SAML

Use the **Applications** page to edit existing SAML applications.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the application that you want to edit.
2. Click the application entry to open the details panel.
3. On the **Overview** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Application Name	A unique identifier for the application.
Description (optional)	A brief description of the application.
Icon (optional)	A pictorial representation of the application. Use a file up to 1MB in JPG, JPEG, GIF, or PNG format.
Home Page URL	The default home page for the application.

Copyright © 2025 Ping Identity Corporation

Field	Description
Signon URL	The URL to which the application redirects the end user for sign-on. **Note** If you created this application using the **Application Catalog** page, you can enable advanced configuration options. Click the **Enable Advanced Configuration** button to access all application settings on the **Configuration** tab.
Display Virtual Server ID	If **Allow Virtual Server IDs** is enabled on the **Configuration** tab, select a virtual server ID in the list to obtain the connection endpoints for the selected virtual server ID. If selected, the **Issuer ID**, URLs, and metadata file update based on the selected virtual server ID. If blank, PingOne uses the default virtual server ID. On the **Configuration** tab, you can enable, add, delete, and set the default virtual server ID.

4. On the **Configuration** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
ACS URLs	The assertion consumer service URLs. You must specify at least one URL. The first URL in the list is used as the default. If the service provider includes the optional `AssertionConsumerServiceURL` element in authentication requests, the incoming value must match one of the URLs defined here.
Signing Key	The certificate that confirms that requests, responses, and assertions actually came from the service provider (SP). Select the appropriate certificate from the list of available RSA or EC certificates. Learn more in Adding a certificate and key pair. Select whether to sign assertions, responses, or both. Select the algorithm to use for signing metadata. If you select an RSA signing certificate, the options are RSA_SHA256, RSA_SHA384, and RSA_SHA512. If you select an EC signing certificate, the options are SHA256_ECDSA, SHA384_ECDSA, and SHA512_ECDSA.

Copyright © 2025 Ping Identity Corporation

Field	Description
Encryption	If selected, the assertions PingOne sends to the SAML application are encrypted. **Note** Available for SAML 2.0 applications only. Select the algorithm for encrypting the assertions, either AES_128 or AES_256 (recommended). Import a certificate or select an existing one from the list of available certificates. Learn more in Adding a certificate and key pair.
Entity ID	The SP entity ID used to look up the application. This is a required property and is unique within the environment.
SLO Endpoint	The URL of the single logout (SLO) service. PingOne redirects the browser to this location when it needs to send an SLO message to the service provider. Learn more in SAML 2.0 single logout.
SLO Response Endpoint (optional)	The URL of the SLO response service. You can use this option if you have a separate service for SLO responses. If this value is blank, PingOne sends responses to the SLO endpoint.
SLO Window	Defines how long PingOne can exchange logout messages with the application, specifically a `LogoutRequest` from the application, after the initial request. PingOne can also send a `LogoutRequest` to the application when SLO is initiated by the user from other session participants, such as an application or identity provider (IdP). This setting is per application. This logout is separate from the user session logout that revokes all tokens. The minimum value is 1 hour and the maximum is 24 hours. You should start with a value of 2 hours and then fine tune as needed.
SLO Binding	The SAML binding used by the application. The default is **HTTP POST**. Select **HTTP Redirect** as needed.

Copyright © 2025 Ping Identity Corporation

Field	Description
Subject NameID format	A string that specifies the format of the subject `NameID` attribute in the SAML assertion. Options are: ◦ `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified` (default). The subject `NameID` is not specified. Use this format if you are not sure which format to use. ◦ `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`. The subject `NameID` is in the form of an email address. ◦ `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`. The subject `NameID` is an opaque unique identifier for a user that retains the same value over time. ◦ `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`. The subject `NameID` is a randomly generated identifier. A different value is used for each single sign-on (SSO) for a given user.
Assertion Validity Duration	The maximum amount of time that an assertion is valid (in seconds).
AuthnStatement Session Validity Duration	Update this value (in seconds) if the SAML application requires a different `SessionNotOnOrAfter` attribute value in the `AuthnStatement` element than the `NotOnOrAfter` value set by the **Assertion validity duration** setting.
Target Application URL	This option is required by some applications as the target URL. It's used in IdP-initiated SSO for deep linking. The application URL is passed in the `RelayState` parameter by the IdP.
Enforce Signed Authentication Request	If selected, PingOne accepts only signed SAML requests and rejects unsigned SAML requests. Verifying the digital signature enables PingOne to validate the authenticity and integrity of the SAML request. This can help mitigate data tampering attacks on attributes, such as the `RequestedAuthnContext` element in `AuthnRequest`. Learn more in RequestedAuthnContext.
Verification Certificate	A certificate that confirms that the SAML assertions actually came from the sender. Select or import the appropriate certificate. The list shows the certificates that are available. Learn more in Adding a certificate and key pair.

Copyright © 2025 Ping Identity Corporation

Field	Description
Select Policy based on RequestedAuthnContext	If selected, and if the `RequestedAuthnContext` value is an exact match to one of the configured policies, PingOne invokes the policy. Otherwise, it returns an error to the application. Learn more in RequestedAuthnContext.
Allow Virtual Server IDs	If enabled, allows you to add one or more custom virtual server IDs to identify your server differently when connecting to the same SAML application in different scenarios, such as from different environments or for different populations. ◦ To enable virtual server IDs, select the checkbox and enter an ID in the **Virtual Server IDs** field. ◦ To add additional virtual server IDs, click **+ Add Virtual Server ID**. The first virtual server ID becomes the default. ◦ To change the default, click the **More Options** (⋮) icon next to the applicable ID and click **Make Default**. If not enabled, PingOne uses the default server ID based on the PingOne domain or custom domain, if configured, in the application URLs. If at least one virtual server ID is configured, PingOne uses the default virtual server ID in the application URLs. You can select the virtual server ID on the **Overview** tab to obtain URLs for each virtual server ID. When using virtual server IDs to connect to multiple environments in one connection, you can protect against unauthorized access by adding an attribute mapping using the expression builder to compare the virtual server ID invoked by the request against an attribute and populate a required attribute accordingly. Learn more in Sample expression for virtual server IDs.

Copyright © 2025 Ping Identity Corporation

Field	Description
CORS Settings	Specifies the CORS options for the application. Learn more in Cross-origin resource sharing. ◦ **Allow any CORS-safe origin** (default): Allows the application to access resources from a domain that is CORS-safelisted, according to the Fetch specification. ◦ **Allow specific origins**: Allows the application to access resources from a specific domain. ■ **Allowed origins**: Specifies the allowed origin domains for CORS. You can specify a domain pattern or a valid IPv4 address. If you use a domain pattern, you can specify one wildcard to match incoming requests. **Note** You cannot use the wildcard on the domain name. For example, the following search patterns are valid: ■ `https://*.test.com` ■ `https://www.app*.test.com` The following patterns are not valid: ■ `https://test*.com` ■ `https://www.app.test*.com` ◦ **Disallow all origins**: Don't allow the application to access resources from a cross-origin domain. **Note** After you make changes to the **CORS Settings**, it can take several minutes for the new settings to take effect, due to time-to-live configuration on the resource.

5. On the **Attribute mappings** tab, click the **Pencil** icon, select a PingOne user attribute, and map it to an attribute in the application. Learn more in Mapping attributes.

    1. Enter a SAML attribute and then select the corresponding PingOne attribute from the list.

    2. Click the **More Options** (⋮) icon to configure `nameFormat` for the SAML attribute. To use a name format other than `Subject`, select an option from the list.

    If you don't select an option, PingOne uses the `basic` format as default. The options are:

    ■ **uri**: The attribute follows the convention for URI references. The interpretation of the URI content is application specific.

    ■ **basic**: The strings in the attribute must be drawn from the values belonging to the primitive type `xs:Name`.

Copyright © 2025 Ping Identity Corporation

- **unspecified**: The attribute can be any format. The interpretation of the content is application specific.

3. Click the **Gear** icon to use the expression builder to build an attribute mapping. Learn more in Using the expression builder.

4. Select **Required** to define the attribute as required for the application.

6. On the **Policies** tab, click the **Pencil** icon and select the authentication policies for the application.

   If you have a DaVinci license, you can select PingOne policies or DaVinci flow policies, but not both. If you don't have a DaVinci license, you'll see PingOne policies only.

   To add one or more PingOne authentication policies, click the **PingOne Policies** tab. If the application was previously configured with one or more DaVinci flow policies, click **Deselect all other Policies** to remove them from the application and select the PingOne authentication policies you want to apply to the application. PingOne authentication policies are applied in the order in which they appear in the list. Click the **Selected PingOne Policies** tab, reorder the policies as needed, and click **Save**.

   To add one or more DaVinci flow policies, click the **DaVinci Policies** tab. If the application was previously configured with one or more PingOne authentication policies, click **Deselect all other Policies** to remove them from the application and and select the DaVinci flow policies you want to apply to the application. PingOne applies the first DaVinci flow policy in the list. Click the **Selected DaVinci Policies** tab, reorder the policies as needed, and click **Save**.

   When invoking an IdP-initiated SSO request from PingOne, the **Initiate Single Sign-On URL** can optionally include the `flowPolicyId` HTTP request parameter to indicate the desired PingOne authentication policy by its name or the ID of the desired DaVinci flow policy that PingOne should use to authenticate the user. The specified policy must be added to the application. Learn more in Identity Provider Initiated SSO in the PingOne API documentation.

   When processing an SP-initiated SSO request PingOne receives from the application, the application can include the `RequestedAuthnContext` element in its authentication request to indicate the desired PingOne authentication policy by its name or the ID of the desired DaVinci flow policy that PingOne should use to authenticate the user. The application must have **Select Policy based on RequestedAuthnContext** enabled on the **Configuration** tab, and the specified policy must be added to the application.

   Learn more in Authentication policies for applications.

7. On the **Access** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Application portal display	Determines whether an application icon appears in the application portal even if the user is allowed to access the application in the application portal based on the group membership policy. Learn more in Application access control.

Copyright © 2025 Ping Identity Corporation

Field	Description
Admin only access	Specifies that a user with an administrator role is required to access the application. The user must have one of the following roles: ◦ `Organization Admin` ◦ `Environment Admin` ◦ `Identity Data Admin` ◦ `Client Application Developer`
Group membership policy	Select the group membership policy for the application. Learn more in Groups.

8. Click **Save**.
9. To enable the application, click the toggle at the top of the details panel to the right (blue).

> **Note**
> You can disable the application by clicking the toggle to the left (gray).

Related links

- Editing an application - OIDC
- Editing an application - Native
- Editing an application - Single page
- Editing an application - Device authorization
- Editing an application - Worker

Editing an application - OIDC

Use the **Applications** page to edit existing OpenID Connect (OIDC) applications.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the application that you want to edit.
2. Click the application entry to open the details panel.
3. On the **Overview** tab, click the **Pencil** icon, and enter or edit the following:

Field	Description
Application Name	A unique identifier for the application.
Description (optional)	A brief description of the application.

Copyright © 2025 Ping Identity Corporation

Field	Description
Icon (optional)	A pictorial representation of the application. Use a file up to 1 MB in JPG, JPEG, GIF, or PNG format.
Home Page URL	The default home page for the application.
Signon URL	The URL to which the application redirects the end user for sign-on. **Important** To avoid issues with third-party cookies in some browsers, we recommend that you use a custom domain to give your PingOne environment the same parent domain as your authentication application. Learn more in Domains.

4. On the **Configuration** tab, click the **Pencil** icon, and enter or edit the following:

Field	Description
Client ID	The unique identifier for the application.
Client Secret	The shared secret for the application. Ensure that you protect the client secret and store it in a secure location. To update the client secret, click **Generate New Secret**. To revoke the previous client secret, click **Revoke Previous Client Secret**. Learn more in Rotating the client secret for an application.
Environment ID	The identifier for the environment that contains the application.
Response Type	Select **Code**, **Token**, or **ID Token** for the response type. Learn more in Response types.
Grant Type	Select **Authorization Code**, **Implicit**, **Client Credentials**, or **Refresh Token**, for the grant type. Learn more in Grant types.
PKCE Enforcement	Select a value for PKCE code challenge enforcement. This value determines how the application creates the code challenge from the code verifier. Learn more in PKCE enforcement. **Note** PKCE enforcement is available for Authorization Code grant type applications only.

Copyright © 2025 Ping Identity Corporation

Field	Description
Refresh Token Configuration	Select this option to enable the Refresh Token grant type. You can specify the following: ***Refresh Duration*** The lifetime of the refresh tokens. If a value is not provided, the default value is `2592000`, or 30 days. Valid values are between `60` and `2147483647`. ***Refresh Token Rolling Duration*** How long the application can use the refresh token grant type to obtain a new access token and a new refresh token after the most recent user authentication event. If a value is not provided, the refresh token is valid forever. Valid values are between `60` and `2147483647`. **Note** The refresh token rolling duration must be longer than the refresh token duration. ***Refresh Token Rolling Grace Period*** The amount of time that a rolled refresh token remains valid if the client failed to receive an updated one during a roll. Valid values are between `0` and `86400` seconds. A value of `0` means that a refresh token becomes invalid after it's rolled.
Redirect URIs	The address to which PingOne forwards the OIDC response after authentication. **Note** The **Redirect URI** cannot contain a fragment component, such as `#some data`. Learn more in Redirection endpoint in the IETF documentation.
Allow Redirect URI patterns	Use a wildcard for flexibility in managing redirect URIs. Learn more in Redirect URIs.
Token Endpoint Authentication Method	Select one of the following: ◦ **None** ◦ **Client Secret Basic** ◦ **Client Secret Post** ◦ **Client Secret JWT** ◦ **Private Key JWT**

Copyright © 2025 Ping Identity Corporation

Field	Description
JSON Web Key Set Method	Select **JWKS URL** or **JWKS**. Provide either the URL where PingOne can retrieve the JSON Web Key Set (JWKS) or the web key set itself. You can paste the JSON in one line or multiple lines. **JWKS Method** is required for an application to send asymmetrically signed request objects. To use **Private Key JWT** for **Token Endpoint Authentication Method**, PingOne reuses the same JWKS URL or JWKS to process the private key JSON Web Token (JWT). **Note** ◦ If **Token Endpoint Authentication Method** is set to **Private Key JWT**, you must provide the **JWKS Method**. ◦ If **Token Endpoint Authentication Method** is set to **None**, **Client Secret Basic**, **Client Secret Post**, or **Client Secret JWT**, if the **JWKS Method** is not provided and the application sends an RS256/384/512-signed request object to PingOne, PingOne returns an error.
Require Pushed Authorization Request	Require the application to send its authorization requests directly to PingOne, without going through the browser, which can safeguard sensitive information from end-user devices. If **Require Pushed Authorization Request** is not selected, the application can send plain authorization requests or pushed authorization requests, but pushed authorization requests are not required. Learn more in Pushed authorization requests.
Pushed Authorization Request Reference Timeout	Specify how long the pushed authorization request should be valid. The default value is 60 seconds.
Initiate Login URI	The application's login initiation endpoint for third-parties to begin the sign-on process for the application. If provided, PingOne redirects users to this URI to initiate SSO to PingOne. The application is responsible for implementing the relevant OIDC flow when the **Initiate Login URI** is requested. Learn more in Initiating Login from a Third Party in the OIDC specification. This URI is required if you want the application to show in the PingOne Application Portal. Learn more in Application portal.
Target Link URI	The URI for the application. If provided, PingOne redirects application users to this URI after the user is authenticated. The `target_link_uri` parameter value in `Initiate Single Sign-On URL` is also updated with the value specified here.
Signoff URLs	The URLs to which the browser can be redirected after a logout has been performed. If you include a `post_logout_redirect_uri` query parameter in the `/signoff` request, with the same value that was set in the application, the browser will redirect the user to the matching URL.

Copyright © 2025 Ping Identity Corporation

Field	Description
Request Parameter Signature Requirement	Specify how the application sends the optional `request` parameter in its authorization requests. Click **Compare Options** for a description of the different settings. ◦ **Default**: Allows the application to send authorization requests with or without the `request` parameter. If using the `request` parameter, the application must include a digital signature. ◦ **Allow unsigned request parameters**: Allows the application to send authorization requests with or without the `request` parameter. If using the `request` parameter, the application has the option to include a digital signature or not. ◦ **Require signed request parameters**: Requires the application to use the `request` parameter and include a digital signature of it in its authorization requests. Learn more in Request Parameter Signature Requirement.
Additional Refresh Token Replay Protection	Outside of the optional rolling grace period, refresh tokens are intended for one-time use. For increased security, enable this option so that PingOne can invalidate both access and refresh tokens when a refresh token is reused. Learn more in Refresh token rotation.
OpenID Connect Session Management	Facilitate OIDC session management by allowing applications in the same browsing mode, such as private or normal browsing mode, to monitor the PingOne user session. Only applications running in the same browsing mode can monitor the PingOne user session. To use this option, your PingOne environment must be configured with a custom domain, such as `sso.example.com`, and the applications must be accessible under that domain. For example, `apps.example.com/app1` and `apps.example.com/app2` or `app1.example.com` and `app2.example.com`. Learn more in Setting up a custom domain. When enabled, the `session_state` parameter is included in the PingOne authorization response with the session status, such as `unchanged`, `changed`, or `error`. Learn more in OIDC session management in the PingOne API documentation and Best practices: Session management. **Note** ◦ The default idle timeout is 30 days. To set an idle timeout of fewer than 30 days: 1. Build a PingOne DaVinci flow that includes the Return Success Response (Redirect Flows) node from the PingOne Authentication connector. 2. In the Return Success Response (Redirect Flows) node, set the **Idle Timeout** value to the desired amount of time, such as 5 minutes. 3. Assign the flow to the applicable applications. ◦ If a user session is deleted because of a PingOne session API request or is purged by the system, it doesn't trigger a `changed` response.

Copyright © 2025 Ping Identity Corporation

Field	Description
Include the x5t parameter in the header of access tokens, ID tokens, and JWT-based refresh token	Select for PingOne to include the `x5t` header parameter in access tokens, ID tokens, and JWT-based refresh tokens. Enable this option if the application, custom resource, or both require the `x5t` parameter in the digital signature verification process.
Terminate User Session by ID Token	Enable this option to allow the application to send requests for PingOne to terminate end-user sessions at the `/idpSignoff` endpoint using only the ID token. The audience claim value in the ID token must match the client ID of the application so that PingOne can identify the session to be terminated. The application is not required to have access to the session token cookie. Learn more in the PingOne API documentation.
CORS Settings	Specifies the CORS options for the application. Learn more in Cross-origin resource sharing. ◦ **Allow any CORS-safe origin** (default): Allows the application to access resources from a domain that is CORS-safelisted, according to the Fetch specification. ◦ **Allow specific origins**: Allows the application to access resources from a specific domain. ■ **Allowed origins**: Specifies the allowed origin domains for CORS. You can specify a domain pattern or a valid IPv4 address. If you use a domain pattern, you can specify one wildcard to match incoming requests. **Note** You cannot use the wildcard on the domain name. For example, the following search patterns are valid: ■ `https://*.test.com` ■ `https://www.app*.test.com` The following patterns are not valid: ■ `https://test*.com` ■ `https://www.app.test*.com` ◦ **Disallow all origins**: Don't allow the application to access resources from a cross-origin domain. **Note** After you make changes to the **CORS Settings**, it can take several minutes for the new settings to take effect, due to time-to-live configuration on the resource.

5. On the **Resources** tab, click the **Pencil** icon and select the checkboxes to add appropriate OAuth scopes for the application. Click the **Selected scopes** tab to see the scopes that are currently selected for the application.

   The OAuth scopes determine the resources that the application can access. If you add OIDC scopes here, the application inherits the attributes associated with that scope.

Copyright © 2025 Ping Identity Corporation

If the application uses the Refresh Token grant type, add the `offline_access` scope to enable the application to request a refresh token from PingOne on a per-request basis. For example, when the application needs a refresh token, it includes the `offline_access` scope in its request, and PingOne includes a refresh token in its token response. However, when the application doesn't need a refresh token, it doesn't include the scope in the request, and PingOne therefore doesn't include a refresh token in its token response. If the `offline_access` scope is not added to an application that uses the Refresh Token grant type, PingOne always includes a refresh token in its token response, whether the application needs a refresh token or not.

To customize the lifetime of access tokens for applications, you must configure a custom resource, set the desired access token lifetime, and then add those scopes to the application. Learn more in Customizing access token lifetime.

6. On the **Policies** tab, click the **Pencil** icon and select the authentication policies for the application.

   If you have a DaVinci license, you can select PingOne policies or DaVinci flow policies, but not both. If you don't have a DaVinci license, you'll see PingOne policies only.

   To add one or more PingOne authentication policies, click the **PingOne Policies** tab. If the application was previously configured with one or more DaVinci flow policies, click **Deselect all other Policies** to remove them from the application and select the PingOne authentication policies you want to apply to the application. PingOne authentication policies are applied in the order in which they appear in the list. Click the **Selected PingOne Policies** tab, reorder the policies as needed, then click **Save**.

   To add one or more DaVinci flow policies, click the **DaVinci Policies** tab. If the application was previously configured with one or more PingOne authentication policies, click **Deselect all other Policies** to remove them from the application and and select the DaVinci flow policies you want to apply to the application. PingOne applies the first DaVinci flow policy in the list. Click the **Selected DaVinci Policies** tab, reorder the policies as needed, then click **Save**.

   For OAuth-based applications, you can specify another policy in the `acr_values` parameter in the authorization request. The `acr_values` parameter specifies the sign-on policies that PingOne should use for authentication. You can include any policies assigned to the application. Specify either a single DaVinci policy by flow policy ID or one or more PingOne policies by name, separated by spaces or the encoded space character `%20`. For example, `acr_values=d1210a6b0b2665dbaa5b652221badba2` or `acr_values=Single_Factor%20Multi_Factor`.

   Learn more in Authentication policies for applications.

7. On the **Attribute Mappings** tab, click the **Pencil** icon, select a PingOne user attribute, and map it to an attribute in the application that you're adding.

   Learn more in Customizing OIDC attributes for an application.

   1. Enter an application attribute and then select the corresponding PingOne attribute from the list.
   2. Click the **Gear** icon to use the expression builder to build an attribute mapping.

      Learn more in Using the expression builder.

8. On the **Access** tab, click the **Pencil** icon and enter or edit the following:

Copyright © 2025 Ping Identity Corporation

Field	Description
Application portal display	Determines whether an application icon appears in the application portal even if the user is allowed to access the application in the application portal based on the group membership policy. Learn more in Application access control.
Admin only access	Specifies that a user with an administrator role is required to access the application. The user must have one of the following roles: ◦ `Organization Admin` ◦ `Environment Admin` ◦ `Identity Data Admin` ◦ `Client Application Developer`
Group membership policy	Select the group membership policy for the application. Learn more in Groups.

9. Click **Save**.
10. To enable the application, click the toggle at the top of the details panel to the right (blue).

> **Note**
> You can disable the application by clicking the toggle to the left (gray).

> **Note**
> If you selected **Response Type = Code** and **Grant Type = Authorization Code**, there is also an **Integrate** tab that you can use to test your configuration. Generate code snippets from this tab and copy them into a web application so that you can ensure that the authorization and authentication configuration is working as intended.
> Learn more in Integrate PingOne with a Node.js Express app and Integrate Ping SDK for JavaScript with PingOne.

Related links

- Editing an application - SAML
- Editing an application - Native
- Editing an application - Single page
- Editing an application - Device authorization
- Editing an application - Worker

Editing an application - Native

Use the **Applications** page to edit existing native applications.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the application that you want to edit.
2. Click the application entry to open the details panel.
3. On the **Overview** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Application Name	A unique identifier for the application.
Description (optional)	A brief description of the application.
Icon (optional)	A pictorial representation of the application. Use a file up to 1MB in JPG, JPEG, GIF, or PNG format.
Home Page URL	The default home page for the application.
Signon URL	The URL to which the application redirects the end user for sign-on. **Important** To avoid issues with third-party cookies in some browsers, we recommend that you use a custom domain to give your PingOne environment the same parent domain as your authentication application. Learn more in Domains.

4. On the **Configuration** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Client ID	The unique identifier for the application.
Client Secret	The shared secret for the application. Ensure that you protect the client secret and store it in a secure location. To update the client secret, click **Generate New Secret**. To revoke the previous client secret, click **Revoke Previous Client Secret**. Learn more in Rotating the client secret for an application.
Environment ID	The identifier for the environment that contains the application.
Response Type	Select **Code**, **Token**, or **ID Token** for the response type. Learn more in Response types.

Copyright © 2025 Ping Identity Corporation

Field	Description
Grant Type	Select **Authorization Code**, **Implicit**, **Client Credentials**, **Device Authorization** or **Refresh Token** for the grant type. Learn more in Grant types.
PKCE Enforcement	Select a value for PKCE code challenge enforcement. This value determines how the application creates the code challenge from the code verifier. Learn more in PKCE enforcement. **Note** PKCE enforcement is available for Authorization Code grant type applications only.
Device authorization configuration	Select this option to enable the Device Authorization grant type. You can specify the following: ***Device Path ID (optional)*** Specifies a unique identifier within an environment for a device authorization grant flow to provide a short identifier to the application. The string can contain letters, numbers, hyphens, and underscores and can be up to 50 characters. **Note** PingOne ignores **Device Path ID** if **Device Custom Verification URI** is configured. ***Device Custom Verification URI (optional)*** Specifies an optional custom verification URI. Learn more in Device custom verification URIs. ***Device Authorization Timeout (required)*** The lifetime, in seconds, of the `user_code` and `device_code`. The default value is 600 seconds and the maximum value is 3600 seconds. ***Device Polling Interval (required)*** The minimum amount of time, in seconds, that the client should wait between polling requests to the token endpoint. The default value is 5 seconds, and the maximum value is 60 seconds. Learn more in Device authorization.

Copyright © 2025 Ping Identity Corporation

Field	Description
Refresh Token configuration	Select this option to enable the Refresh Token grant type. You can specify the following: ***Refresh token duration*** The lifetime of the refresh tokens. If a value is not provided, the default value is `2592000`, or 30 days. Valid values are between `60` and `2147483647`. ***Refresh token rolling duration*** How long the application can use the refresh token grant type to obtain a new access token and a new refresh token after the most recent user authentication event. If a value is not provided, the refresh token is valid forever. Valid values are between `60` and `2147483647`. **Note** The refresh token rolling duration must be longer than the refresh token duration. ***Refresh token rolling grace period*** The amount of time that a rolled refresh token is still valid in the event that the client failed to receive an updated one during a roll. Valid values are between `0` and `86400` seconds. A value of `0` means that a refresh token becomes invalid after it's rolled.
Redirect URIs	The address to which PingOne forwards the OIDC response after authentication. **Note** The **Redirect URI** cannot contain a fragment component, such as `#somedata`. Learn more in Redirection endpoint in the IETF documentation.
Allow Redirect URI patterns	Use a wildcard for flexibility in managing redirect URIs. See Redirect URIs.
Token Endpoint Authentication Method	Select one of the following: ◦ **None** ◦ **Client Secret Basic** ◦ **Client Secret Post** ◦ **Client Secret JWT** ◦ **Private Key JWT**

Copyright © 2025 Ping Identity Corporation

Field	Description
JSON Web Key Set Method	Select **JWKS URL** or **JWKS**. Provide either the URL where PingOne can retrieve the JSON Web Key Set (JWKS) or the web key set itself. You can paste the JSON in one line or multiple lines. **JWKS Method** is required for an application to send asymmetrically signed request objects. To use **Private Key JWT** for **Token Endpoint Authentication Method**, PingOne reuses the same JWKS URL or JWKS to process the private key JSON Web Token (JWT). **Note** ◦ If **Token Endpoint Authentication Method** is set to **Private Key JWT**, you must provide the **JWKS Method**. ◦ If **Token Endpoint Authentication Method** is set to **None**, **Client Secret Basic**, **Client Secret Post**, or **Client Secret JWT**, if the **JWKS Method** is not provided and the application sends an RS256/384/512-signed request object to PingOne, PingOne returns an error.
Require Pushed Authorization Request	Require the application to send its authorization requests directly to PingOne, without going through the browser, which can safeguard sensitive information from end-user devices. If **Require Pushed Authorization Request** is not selected, the application can send plain authorization requests or pushed authorization requests, but pushed authorization requests are not required. Learn more in Pushed authorization requests.
Pushed Authorization Request Reference Timeout	Specify how long the pushed authorization request should be valid. The default value is 60 seconds.
Initiate Login URI	The application's login initiation endpoint for third-parties to begin the sign-on process for the application. If provided, PingOne redirects users to this URI to initiate SSO to PingOne. The application is responsible for implementing the relevant OIDC flow when the **Initiate Login URI** is requested. Learn more in Initiating Login from a Third Party in the OIDC specification. This URI is required if you want the application to show in the PingOne Application Portal. Learn more in Application portal.

Copyright © 2025 Ping Identity Corporation

Field	Description
Target Link URI	The URI for the application. If provided, PingOne redirects application users to this URI after the user is authenticated. The `target_link_uri` parameter value in `Initiate Single Sign-On URL` is also updated with the value specified here.
Signoff URLs	The URLs to which the browser can be redirected after a logout has been performed. If you include a `post_logout_redirect_uri` query parameter in the `/signoff` request, with the same value that was set in the application, the browser will redirect the user to the matching URL.
Request Parameter Signature Requirement	Specify how the application sends the optional `request` parameter in its authorization requests. Click **Compare Options** for a description of the different settings. ◦ **Default**: Allows the application to send authorization requests with or without the `request` parameter. If using the `request` parameter, the application must include a digital signature. ◦ **Allow unsigned request parameters**: Allows the application to send authorization requests with or without the `request` parameter. If using the `request` parameter, the application has the option to include a digital signature or not. ◦ **Require signed request parameters**: Requires the application to use the `request` parameter and include a digital signature of it in its authorization requests. Learn more in Request Parameter Signature Requirement.
Additional Refresh Token Replay Protection	Outside of the optional rolling grace period, refresh tokens are intended for one-time use. For increased security, enable this option so that PingOne can invalidate both access and refresh tokens when a refresh token is reused. Learn more in Refresh token rotation.

Copyright © 2025 Ping Identity Corporation

Field	Description
OpenID Connect Session Management	Facilitate OIDC session management by allowing applications in the same browsing mode, such as private or normal browsing mode, to monitor the PingOne user session. Only applications running in the same browsing mode can monitor the PingOne user session. To use this option, your PingOne environment must be configured with a custom domain, such as `sso.example.com`, and the applications must be accessible under that domain. For example, `apps.example.com/app1` and `apps.example.com/app2` or `app1.example.com` and `app2.example.com`. Learn more in Setting up a custom domain. When enabled, the `session_state` parameter is included in the PingOne authorization response with the session status, such as `unchanged`, `changed`, or `error`. Learn more in OIDC session management in the PingOne API documentation and Best practices: Session management. **Note** ◦ The default idle timeout is 30 days. To set an idle timeout of fewer than 30 days: 1. Build a PingOne DaVinci flow that includes the Return Success Response (Redirect Flows) node from the PingOne Authentication connector. 2. In the Return Success Response (Redirect Flows) node, set the **Idle Timeout** value to the desired amount of time, such as 5 minutes. 3. Assign the flow to the applicable applications. ◦ If a user session is deleted because of a PingOne session API request or is purged by the system, it doesn't trigger a `changed` response.
Include the x5t parameter in the header of access tokens, ID tokens, and JWT-based refresh token	Select for PingOne to include the `x5t` header parameter in access tokens, ID tokens, and JWT-based refresh tokens. Enable this option if the application, custom resource, or both require the `x5t` parameter in the digital signature verification process.

Copyright © 2025 Ping Identity Corporation

Field	Description
Terminate User Session by ID Token	Enable this option to allow the application to send requests for PingOne to terminate end-user sessions at the `/idpSignoff` endpoint using only the ID token. The audience claim value in the ID token must match the client ID of the application so that PingOne can identify the session to be terminated. The application is not required to have access to the session token cookie. Learn more in the PingOne API documentation.
CORS Settings	Specifies the CORS options for the application. Learn more in Cross-origin resource sharing. ◦ **Allow any CORS-safe origin** (default): Allows the application to access resources from a domain that is CORS-safelisted, according to the Fetch specification. ◦ **Allow specific origins**: Allows the application to access resources from a specific domain. ■ **Allowed origins**: Specifies the allowed origin domains for CORS. You can specify a domain pattern or a valid IPv4 address. If you use a domain pattern, you can specify one wildcard to match incoming requests. **Note** You cannot use the wildcard on the domain name. For example, the following search patterns are valid: ■ `https://*.test.com` ■ `https://www.app*.test.com` The following patterns are not valid: ■ `https://test*.com` ■ `https://www.app.test*.com` ◦ **Disallow all origins**: Don't allow the application to access resources from a cross-origin domain. **Note** After you make changes to the **CORS Settings**, it can take several minutes for the new settings to take effect, due to time-to-live configuration on the resource.

5. On the **Resources** tab, click the **Pencil** icon and select the check boxes to add appropriate OAuth scopes for the application. Click the **Selected scopes** tab to see the scopes that are currently selected for the application.

   The OAuth scopes determine the resources that the application can access. If you add OIDC scopes here, the application inherits the attributes associated with that scope.

Copyright © 2025 Ping Identity Corporation

If the application uses the Refresh Token grant type, add the `offline_access` scope to enable the application to request a refresh token from PingOne on a per-request basis. For example, when the application needs a refresh token, it includes the `offline_access` scope in its request, and PingOne includes a refresh token in its token response. However, when the application doesn't need a refresh token, it doesn't include the scope in the request, and PingOne therefore doesn't include a refresh token in its token response. If the `offline_access` scope is not added to an application that uses the Refresh Token grant type, PingOne always includes a refresh token in its token response, whether the application needs a refresh token or not.

6. On the **Policies** tab, click the **Pencil** icon and select the authentication policies for the application.

   If you have a DaVinci license, you can select PingOne policies or DaVinci flow policies, but not both. If you don't have a DaVinci license, you'll see PingOne policies only.

   To add one or more PingOne authentication policies, click the **PingOne Policies** tab. If the application was previously configured with one or more DaVinci flow policies, click **Deselect all other Policies** to remove them from the application and select the PingOne authentication policies you want to apply to the application. PingOne authentication policies are applied in the order in which they appear in the list. Click the **Selected PingOne Policies** tab, reorder the policies as needed, then click **Save**.

   To add one or more DaVinci flow policies, click the **DaVinci Policies** tab. If the application was previously configured with one or more PingOne authentication policies, click **Deselect all other Policies** to remove them from the application and and select the DaVinci flow policies you want to apply to the application. PingOne applies the first DaVinci flow policy in the list. Click the **Selected DaVinci Policies** tab, reorder the policies as needed, then click **Save**.

   For OAuth-based applications, you can specify another policy in the `acr_values` parameter in the authorization request. The `acr_values` parameter specifies the sign-on policies that PingOne should use for authentication. You can include any policies assigned to the application. Specify either a single DaVinci policy by flow policy ID or one or more PingOne policies by name, separated by spaces or the encoded space character `%20`. For example, `acr_values=d1210a6b0b2665dbaa5b652221badba2` or `acr_values=Single_Factor%20Multi_Factor`.

   Learn more in Authentication policies for applications.

7. On the **Attribute Mappings** tab, click the **Pencil** icon and select a PingOne user attribute and map it to an attribute in the application that you are adding.

   Learn more in Customizing OIDC attributes for an application.

   1. Enter an application attribute and then select the corresponding PingOne attribute from the list.
   2. Click the **Gear** icon to use the expression builder to build an attribute mapping.

      Learn more in Using the expression builder.

8. On the **Access** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Application portal display	Determines whether an application icon appears in the application portal even if the user is allowed to access the application in the application portal based on the group membership policy. Learn more in Application access control.

Copyright © 2025 Ping Identity Corporation

Field	Description
Admin only access	Specifies that a user with an administrator role is required to access the application. The user must have one of the following roles: ◦ `Organization Admin` ◦ `Environment Admin` ◦ `Identity Data Admin` ◦ `Client Application Developer`
Group membership policy	Select the group membership policy for the application. Learn more in Groups.

9. On the **Mobile** tab, click the **Pencil** icon and allow mobile authentication for the app:

Option	Description
Android	Configure the app for Android by providing the package name for Google Play Services, the package name and app ID for Huawei Mobile Services, or both.
iOS	Provide the bundle ID as registered in the app store.

After you have enabled mobile authentication, you can configure any of the following:

1. Allow push notifications by providing the following information:

   - For Android apps that use Google Play Services, provide the JSON file that represents your Firebase Admin SDK private key.
   - For Android apps that use Huawei Mobile Services, provide the OAuth 2.0 client ID and client secret.
   - For iOS, provide the team ID, authentication token signing key, and key ID (as provided by Apple to your organization).

     After you save the push credentials, you can use the **Send Test** button to test them. You have to supply the push token issued by Google, Huawei, or Apple.

2. Turn on device integrity checking to prevent the use of compromised devices for pairing or authentication.

   You can enable device integrity checking separately for Android and iOS. For Android, you must choose between **Google Verification** and **Internal Verification**. Using internal verification will not count against your Google API call quota. You must provide the following additional information, depending on the type of verification you selected:

   - **Google verification** - select the JSON file that represents your **Service Account Credentials**
   - **Internal verification** - enter the **Decryption Key** and **Verification Key** from your Google Play Services account

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If an application appears in multiple environments, make sure to provide the same verification credentials and specify the same cache duration for the application in each of the environments. If these settings do not match, unexpected behavior can result. In such cases, you will also see an error message in the audit log. You will see a similar message if you provided incorrect credentials.

3. If your organization is using the PingOne MFA SDK to allow authentication with a QR code in certain flows, in **Universal / App Link**, enter the link or URI scheme that the application should use for this purpose, depending on which deep-linking mechanism the app developers used.
4. Use the **Passcode Refresh Duration** field to specify the amount of time a passcode should be displayed before being replaced with a new passcode.
5. Use **Number Matching Options** to specify how number matching authentication should be presented to users - whether they should select the displayed number from a group of three numbers, or whether you want to require that they actually enter the number that was shown. Note that to use number matching in an application, you must enable the **Number Matching** option in the relevant MFA policy.

+

> **Note**
>
> - The package name, app ID, bundle ID, and push notification settings cannot be modified after they have been saved for the application.
> - If you do not have the necessary license for making changes on the **Mobile** tab, a lock icon displays below the tab name. If you click the lock, a message appears explaining how to obtain the required license. If you previously had a valid license and defined mobile authentication settings for the app, they remain visible on the tab, but you cannot modify the settings or add to them.

10. Click **Save**.
11. To enable the application, click the toggle at the top of the details panel to the right (blue).

> **Note**
>
> You can disable the application by clicking the toggle to the left (gray).

Related links

- Editing an application - SAML
- Editing an application - OIDC
- Editing an application - Single page
- Editing an application - Device authorization
- Editing an application - Worker

Copyright © 2025 Ping Identity Corporation

Editing an application - Single page

Use the **Applications** page to edit existing single page applications.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the application that you want to edit.
2. Click the application entry to open the details panel.
3. On the **Overview** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Application Name	A unique identifier for the application.
Description (optional)	A brief description of the application.
Icon (optional)	A pictorial representation of the application. Use a file up to 1 MB in JPG, JPEG, GIF, or PNG format.
Home Page URL	The default home page for the application.
Signon URL	The URL to which the application redirects the end user for sign-on. **Important** To avoid issues with third-party cookies in some browsers, we recommend that you use a custom domain to give your PingOne environment the same parent domain as your authentication application. Learn more in Domains.

4. On the **Configuration** tab, click the **Pencil** icon, and enter or edit the following:

Field	Description
Client ID	The unique identifier for the application.
Client Secret	The shared secret for the application. Ensure that you protect the client secret and store it in a secure location. To update the client secret, click **Generate New Secret**. To revoke the previous client secret, click **Revoke Previous Client Secret**. Learn more in Rotating the client secret for an application.
Environment ID	The identifier for the environment that contains the application.

Copyright © 2025 Ping Identity Corporation

Field	Description
Response Type	Select **Code**, **Token**, or **ID Token** for the response type. Learn more in Response types.
Grant Type	Select **Authorization Code**, **Implicit**, **Client Credentials**, or **Refresh Token** for the grant type. Learn more in Grant types.
PKCE Enforcement	Select a value for PKCE code challenge enforcement. This value determines how the application creates the code challenge from the code verifier. Learn more in PKCE enforcement. **Note** PKCE enforcement is available for Authorization Code grant type applications only.
Refresh Token Configuration	Select this option to enable the Refresh Token grant type. You can specify the following: ***Refresh Duration*** The lifetime of the refresh tokens. If a value is not provided, the default value is `2592000`, or 30 days. Valid values are between `60` and `2147483647`. ***Refresh Token Rolling Duration*** How long the application can use the refresh token grant type to obtain a new access token and a new refresh token after the most recent user authentication event. If a value is not provided, the refresh token is valid forever. Valid values are between `60` and `2147483647`. **Note** The refresh token rolling duration must be longer than the refresh token duration. ***Refresh Token Rolling Grace Period*** The amount of time that a rolled refresh token is still valid in the event that the client failed to receive an updated one during a roll. Valid values are between `0` and `86400` seconds. A value of `0` means that a refresh token becomes invalid after it's rolled.
Redirect URIs	The address to which PingOne forwards the OIDC response after authentication. The Redirect URI cannot contain a fragment component, such as `#somedata`. Learn more in Redirection endpoint in the IETF documentation.

Copyright © 2025 Ping Identity Corporation

Field	Description
Allow Redirect URI patterns	Use a wildcard for flexibility in managing redirect URIs. See Redirect URIs.
Token Endpoint Authentication Method	Select one of the following: ◦ **None** ◦ **Client Secret Basic** ◦ **Client Secret Post** ◦ **Client Secret JWT** ◦ **Private Key JWT**
JSON Web Key Set Method	Select **JWKS URL** or **JWKS**. Provide either the URL where PingOne can retrieve the JSON Web Key Set (JWKS) or the web key set itself. You can paste the JSON in one line or multiple lines. **JWKS Method** is required for an application to send asymmetrically signed request objects. To use **Private Key JWT** for **Token Endpoint Authentication Method**, PingOne reuses the same JWKS URL or JWKS to process the private key JSON Web Token (JWT). **Note** ◦ If **Token Endpoint Authentication Method** is set to **Private Key JWT**, you must provide the **JWKS Method**. ◦ If **Token Endpoint Authentication Method** is set to **None**, **Client Secret Basic**, **Client Secret Post**, or **Client Secret JWT**, if the **JWKS Method** is not provided and the application sends an RS256/384/512-signed request object to PingOne, PingOne returns an error.
Require Pushed Authorization Request	Require the application to send its authorization requests directly to PingOne, without going through the browser, which can safeguard sensitive information from end-user devices. If **Require Pushed Authorization Request** is not selected, the application can send plain authorization requests or pushed authorization requests, but pushed authorization requests are not required. Learn more in Pushed authorization requests.
Pushed Authorization Request Reference Timeout	Specify how long the pushed authorization request should be valid. The default value is 60 seconds.

Copyright © 2025 Ping Identity Corporation

Field	Description
Initiate Login URI	The application's login initiation endpoint for third-parties to begin the sign-on process for the application. If provided, PingOne redirects users to this URI to initiate SSO to PingOne. The application is responsible for implementing the relevant OIDC flow when the **Initiate Login URI** is requested. Learn more in Initiating Login from a Third Party in the OIDC specification. This URI is required if you want the application to show in the PingOne Application Portal. Learn more in Application portal.
Target Link URI	The URI for the application. If provided, PingOne redirects application users to this URI after the user is authenticated. The `target_link_uri` parameter value in `Initiate Single Sign-On URL` is also updated with the value specified here.
Signoff URLs	The URLs to which the browser can be redirected after a logout has been performed. If you include a `post_logout_redirect_uri` query parameter in the `/signoff` request, with the same value that was set in the application, the browser will redirect the user to the matching URL.
Request Parameter Signature Requirement	Specify how the application sends the optional `request` parameter in its authorization requests. Click **Compare Options** for a description of the different settings. ◦ **Default**: Allow the application to send authorization requests with or without the `request` parameter. If using the request parameter, the application must include a digital signature. ◦ **Allow unsigned request parameters**: Allow the application to send authorization requests with or without the `request` parameter. If using the `request` parameter, the application has the option to include a digital signature or not. ◦ **Require signed request parameters**: Require the application to use the `request` parameter and include a digital signature of it in its authorization requests. Learn more in Request Parameter Signature Requirement.

Copyright © 2025 Ping Identity Corporation

Field	Description
Additional Refresh Token Replay Protection	Outside of the optional rolling grace period, refresh tokens are intended for one-time use. For increased security, enable this option so that PingOne can invalidate both access and refresh tokens when a refresh token is reused. Learn more in Refresh token rotation.
OpenID Connect Session Management	Facilitate OIDC session management by allowing applications in the same browsing mode, such as private or normal browsing mode, to monitor the PingOne user session. Only applications running in the same browsing mode can monitor the PingOne user session. To use this option, your PingOne environment must be configured with a custom domain, such as `sso.example.com`, and the applications must be accessible under that domain. For example, `apps.example.com/app1` and `apps.example.com/app2` or `app1.example.com` and `app2.example.com`. Learn more in Setting up a custom domain. When enabled, the `session_state` parameter is included in the PingOne authorization response with the session status, such as `unchanged`, `changed`, or `error`. Learn more in OIDC session management in the PingOne API documentation and Best practices: Session management. **Note** ◦ The default idle timeout is 30 days. To set an idle timeout of fewer than 30 days: 1. Build a PingOne DaVinci flow that includes the Return Success Response (Redirect Flows) node from the PingOne Authentication connector. 2. In the Return Success Response (Redirect Flows) node, set the **Idle Timeout** value to the desired amount of time, such as 5 minutes. 3. Assign the flow to the applicable applications. ◦ If a user session is deleted because of a PingOne session API request or is purged by the system, it doesn't trigger a `changed` response.

Copyright © 2025 Ping Identity Corporation

Field	Description
Include the x5t parameter in the header of access tokens, ID tokens, and JWT-based refresh token	Select for PingOne to include the `x5t` header parameter in access tokens, ID tokens, and JWT-based refresh tokens. Enable this option if the application, custom resource, or both require the `x5t` parameter in the digital signature verification process.
Terminate User Session by ID Token	Enable this option to allow the application to send requests for PingOne to terminate end-user sessions at the `/idpSignoff` endpoint using only the ID token. The audience claim value in the ID token must match the client ID of the application so that PingOne can identify the session to be terminated. The application is not required to have access to the session token cookie. Learn more in the PingOne API documentation.

Copyright © 2025 Ping Identity Corporation

Field	Description
CORS Settings	Specifies the CORS options for the application. Learn more in Cross-origin resource sharing. ◦ **Allow any CORS-safe origin** (default): Allows the application to access resources from a domain that is CORS-safelisted, according to the Fetch specification. ◦ **Allow specific origins**: Allows the application to access resources from a specific domain. ■ **Allowed origins**: Specifies the allowed origin domains for CORS. You can specify a domain pattern or a valid IPv4 address. If you use a domain pattern, you can specify one wildcard to match incoming requests. **Note** You cannot use the wildcard on the domain name. For example, the following search patterns are valid: ■ `https://*.test.com` ■ `https://www.app*.test.com` The following patterns are not valid: ■ `https://test*.com` ■ `https://www.app.test*.com` ◦ **Disallow all origins**: Don't allow the application to access resources from a cross-origin domain. **Note** After you make changes to the **CORS Settings**, it can take several minutes for the new settings to take effect, due to time-to-live configuration on the resource.

5. On the **Resources** tab, click the **Pencil** icon and select the check boxes to add appropriate OAuth scopes for the application. Click the **Selected scopes** tab to see the scopes that are currently selected for the application.

   The OAuth scopes determine the resources that the application can access. If you add OIDC scopes here, the application inherits the attributes associated with that scope.

   If the application uses the Refresh Token grant type, add the `offline_access` scope to enable the application to request a refresh token from PingOne on a per-request basis. For example, when the application needs a refresh token, it includes the `offline_access` scope in its request, and PingOne includes a refresh token in its token response. However, when the application doesn't need a refresh token, it doesn't include the scope in the request, and PingOne therefore doesn't include a refresh token in its token response. If the `offline_access` scope is not added to an application that uses the Refresh Token grant type, PingOne always includes a refresh token in its token response, whether the application needs a refresh token or not.

Copyright © 2025 Ping Identity Corporation

6. On the **Policies** tab, click the **Pencil** icon and select the authentication policies for the application.

   If you have a DaVinci license, you can select PingOne policies or DaVinci flow policies, but not both. If you don't have a DaVinci license, you'll see PingOne policies only.

   To add one or more PingOne authentication policies, click the **PingOne Policies** tab. If the application was previously configured with one or more DaVinci flow policies, click **Deselect all other Policies** to remove them from the application and select the PingOne authentication policies you want to apply to the application. PingOne authentication policies are applied in the order in which they appear in the list. Click the **Selected PingOne Policies** tab, reorder the policies as needed, then click **Save**.

   To add one or more DaVinci flow policies, click the **DaVinci Policies** tab. If the application was previously configured with one or more PingOne authentication policies, click **Deselect all other Policies** to remove them from the application and and select the DaVinci flow policies you want to apply to the application. PingOne applies the first DaVinci flow policy in the list. Click the **Selected DaVinci Policies** tab, reorder the policies as needed, then click **Save**.

   For OAuth-based applications, you can specify another policy in the `acr_values` parameter in the authorization request. The `acr_values` parameter specifies the sign-on policies that PingOne should use for authentication. You can include any policies assigned to the application. Specify either a single DaVinci policy by flow policy ID or one or more PingOne policies by name, separated by spaces or the encoded space character `%20`. For example, `acr_values=d1210a6b0b2665dbaa5b652221badba2` or `acr_values=Single_Factor%20Multi_Factor`.

   Learn more in Authentication policies for applications.

7. On the **Attribute Mappings** tab, click the **Pencil** icon and select a PingOne user attribute and map it to an attribute in the application that you are adding.

   Learn more in Customizing OIDC attributes for an application.

   1. Enter an application attribute and then select the corresponding PingOne attribute from the list.
   2. Click the **Gear** icon to use the expression builder to build an attribute mapping.

      Learn more in Using the expression builder.

8. On the **Access** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Application portal display	Determines whether an application icon appears in the application portal even if the user is allowed to access the application in the application portal based on the group membership policy. Learn more in Application access control.
Admin only access	Specifies that a user with an administrator role is required to access the application. The user must have one of the following roles: ◦ `Organization Admin` ◦ `Environment Admin` ◦ `Identity Data Admin` ◦ `Client Application Developer`

Copyright © 2025 Ping Identity Corporation

Field	Description
Group membership policy	Select the group membership policy for the application. Learn more in Groups.

9. Click **Save**.
10. To enable the application, click the toggle at the top of the details panel to the right (blue).

> **Note**
> You can disable the application by clicking the toggle to the left (gray).

Related links

- Editing an application - SAML
- Editing an application - OIDC
- Editing an application - Native
- Editing an application - Device authorization
- Editing an application - Worker

Editing an application - Worker

Use the **Applications** page to edit existing worker applications.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the application that you want to edit.
2. Click the application entry to open the details panel.
3. On the **Overview** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Application Name	A unique identifier for the application.
Description (optional)	A brief description of the application.
Icon (optional)	A pictorial representation of the application. Use a file up to 1 MB in JPG, JPEG, GIF, or PNG format.
Home Page URL	The default home page for the application.

Copyright © 2025 Ping Identity Corporation

Field	Description
Signon URL	The URL to which the application redirects the end user for sign-on. **Important** To avoid issues with third-party cookies in some browsers, we recommend that you use a custom domain to give your PingOne environment the same parent domain as your authentication application. Learn more in Domains.

4. On the **Configuration** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Client ID	The unique identifier for the application.
Client Secret	The shared secret for the application. Ensure that you protect the client secret and store it in a secure location. To update the client secret, click **Generate New Secret**. To revoke the previous client secret, click **Revoke Previous Client Secret**. Learn more in Rotating the client secret for an application.
Environment ID	The identifier for the environment that contains the application.
Response Type	Select **Code**, **Token**, or **ID Token** for the response type. Learn more in Response types.
Grant Type	Select **Authorization Code**, **Implicit**, **Client Credentials**, or **Refresh Token** for the grant type. Learn more in Grant types.
PKCE Enforcement	Select a value for PKCE code challenge enforcement. This value determines how the application creates the code challenge from the code verifier. Learn more in PKCE enforcement. **Note** PKCE enforcement is available for Authorization Code grant type applications only.
Redirect URIs	The address to which PingOne forwards the OIDC response after authentication. The Redirect URI cannot contain a fragment component, such as `#somedata`. Learn more in Redirection endpoint in the IETF documentation.

Copyright © 2025 Ping Identity Corporation

Field	Description
Allow Redirect URI patterns	Use a wildcard for flexibility in managing redirect URIs. See Redirect URIs.
Signoff URLs	The URL to which the application requests that the browser be redirected using the `post_logout_redirect_uri` parameter after a logout has been performed.
Token Endpoint Authentication Method	Select one of the following: ◦ **None** ◦ **Client Secret Basic** ◦ **Client Secret Post** ◦ **Client Secret JWT** ◦ **Private Key JWT**
JSON Web Key Set Method	Select **JWKS URL** or **JWKS**. Provide either the URL where PingOne can retrieve the JSON Web Key Set (JWKS) or the web key set itself. You can paste the JSON in one line or multiple lines. **JWKS Method** is required for an application to send asymmetrically signed request objects. To use **Private Key JWT** for **Token Endpoint Authentication Method**, PingOne reuses the same JWKS URL or JWKS to process the private key JSON Web Token (JWT). **Note** ◦ If **Token Endpoint Authentication Method** is set to **Private Key JWT**, you must provide the **JWKS Method**. ◦ If **Token Endpoint Authentication Method** is set to **None**, **Client Secret Basic**, **Client Secret Post**, or **Client Secret JWT**, if the **JWKS Method** is not provided and the application sends an RS256/384/512-signed request object to PingOne, PingOne returns an error.
Require Pushed Authorization Request	Require the application to send its authorization requests directly to PingOne, without going through the browser, which can safeguard sensitive information from end-user devices. If **Require Pushed Authorization Request** is not selected, the application can send plain authorization requests or pushed authorization requests, but pushed authorization requests are not required. Learn more in Pushed authorization requests.

Copyright © 2025 Ping Identity Corporation

Field	Description
Pushed Authorization Request Reference Timeout	Specify how long the pushed authorization request should be valid. The default value is 60 seconds.
Initiate Login URI	The application's login initiation endpoint for third-parties to begin the sign-on process for the application. If provided, PingOne redirects users to this URI to initiate SSO to PingOne. The application is responsible for implementing the relevant OIDC flow when the **Initiate Login URI** is requested. Learn more in Initiating Login from a Third Party in the OIDC specification. This URI is required if you want the application to show in the PingOne Application Portal. Learn more in Application portal.
Target Link URI	The URI for the application. If provided, PingOne redirects application users to this URI after the user is authenticated. The `target_link_uri` parameter value in `Initiate Single Sign-On URL` is also updated with the value specified here.
Signoff URLs	The URLs to which the browser can be redirected after a logout has been performed. If you include a `post_logout_redirect_uri` query parameter in the `/signoff` request, with the same value that was set in the application, the browser will redirect the user to the matching URL.
Request Parameter Signature Requirement	Specify how the application sends the optional `request` parameter in its authorization requests. Click **Compare Options** for a description of the different settings. ◦ **Default**: Allow the application to send authorization requests with or without the `request` parameter. If using the request parameter, the application must include a digital signature. ◦ **Allow unsigned request parameters**: Allow the application to send authorization requests with or without the `request` parameter. If using the `request` parameter, the application has the option to include a digital signature or not. ◦ **Require signed request parameters**: Require the application to use the `request` parameter and include a digital signature of it in its authorization requests. Learn more in Request Parameter Signature Requirement.

Copyright © 2025 Ping Identity Corporation

Field	Description
Additional Refresh Token Replay Protection	Outside of the optional rolling grace period, refresh tokens are intended for one-time use. For increased security, enable this option so that PingOne can invalidate both access and refresh tokens when a refresh token is reused. Learn more in Refresh token rotation.
OpenID Connect Session Management	Facilitate OIDC session management by allowing applications in the same browsing mode, such as private or normal browsing mode, to monitor the PingOne user session. Only applications running in the same browsing mode can monitor the PingOne user session. To use this option, your PingOne environment must be configured with a custom domain, such as `sso.example.com`, and the applications must be accessible under that domain. For example, `apps.example.com/app1` and `apps.example.com/app2` or `app1.example.com` and `app2.example.com`. Learn more in Setting up a custom domain. When enabled, the `session_state` parameter is included in the PingOne authorization response with the session status, such as `unchanged`, `changed`, or `error`. Learn more in OIDC session management in the PingOne API documentation and Best practices: Session management. **Note** ◦ The default idle timeout is 30 days. To set an idle timeout of fewer than 30 days: 1. Build a PingOne DaVinci flow that includes the Return Success Response (Redirect Flows) node from the PingOne Authentication connector. 2. In the Return Success Response (Redirect Flows) node, set the **Idle Timeout** value to the desired amount of time, such as 5 minutes. 3. Assign the flow to the applicable applications. ◦ If a user session is deleted because of a PingOne session API request or is purged by the system, it doesn't trigger a `changed` response.

Copyright © 2025 Ping Identity Corporation

Field	Description
Include the x5t parameter in the header of access tokens, ID tokens, and JWT-based refresh token	Select for PingOne to include the `x5t` header parameter in access tokens, ID tokens, and JWT-based refresh tokens. Enable this option if the application, custom resource, or both require the `x5t` parameter in the digital signature verification process.
Terminate User Session by ID Token	Enable this option to allow the application to send requests for PingOne to terminate end-user sessions at the `/idpSignoff` endpoint using only the ID token. The audience claim value in the ID token must match the client ID of the application so that PingOne can identify the session to be terminated. The application is not required to have access to the session token cookie. Learn more in the PingOne API documentation.

Copyright © 2025 Ping Identity Corporation

Field	Description
CORS Settings	Specifies the CORS options for the application. Learn more in Cross-origin resource sharing. ◦ **Allow any CORS-safe origin** (default): Allows the application to access resources from a domain that is CORS-safelisted, according to the Fetch specification. ◦ **Allow specific origins**: Allows the application to access resources from a specific domain. ■ **Allowed origins**: Specifies the allowed origin domains for CORS. You can specify a domain pattern or a valid IPv4 address. If you use a domain pattern, you can specify one wildcard to match incoming requests. **Note** You cannot use the wildcard on the domain name. For example, the following search patterns are valid: ■ `https://*.test.com` ■ `https://www.app*.test.com` The following patterns are not valid: ■ `https://test*.com` ■ `https://www.app.test*.com` ◦ **Disallow all origins**: Don't allow the application to access resources from a cross-origin domain. **Note** After you make changes to the **CORS Settings**, it can take several minutes for the new settings to take effect, due to time-to-live configuration on the resource.

5. On the **Resources** tab, click the **Pencil** icon and select the check boxes to add appropriate OAuth scopes for the application. Click the **Selected scopes** tab to see the scopes that are currently selected for the application.

   The OAuth scopes determine the resources that the application can access. If you add OIDC scopes here, the application inherits the attributes associated with that scope.

   If the application uses the Refresh Token grant type, add the `offline_access` scope to enable the application to request a refresh token from PingOne on a per-request basis. For example, when the application needs a refresh token, it includes the `offline_access` scope in its request, and PingOne includes a refresh token in its token response. However, when the application doesn't need a refresh token, it doesn't include the scope in the request, and PingOne therefore doesn't include a refresh token in its token response. If the `offline_access` scope is not added to an application that uses the Refresh Token grant type, PingOne always includes a refresh token in its token response, whether the application needs a refresh token or not.

Copyright © 2025 Ping Identity Corporation

6. On the **Policies** tab, click the **Pencil** icon and select the authentication policies for the application.

   If you have a DaVinci license, you can select PingOne policies or flow policies, but not both. If you don't have a DaVinci license, you'll see PingOne policies only.

   To add one or more PingOne authentication policies, click the **PingOne Policies** tab. If the application was previously configured with one or more DaVinci flow policies, click **Deselect all other Policies** to remove them from the application and select the PingOne authentication policies you want to apply to the application. PingOne authentication policies are applied in the order in which they appear in the list. Click the **Selected PingOne Policies** tab, reorder the policies as needed, then click **Save**.

   To add one or more DaVinci flow policies, click the **DaVinci Policies** tab. If the application was previously configured with one or more PingOne authentication policies, click **Deselect all other Policies** to remove them from the application and and select the DaVinci flow policies you want to apply to the application. PingOne applies the first DaVinci flow policy in the list. Click the **Selected DaVinci Policies** tab, reorder the policies as needed, then click **Save**.

   For OAuth-based applications, you can specify another policy in the `acr_values` parameter in the authorization request. The `acr_values` parameter specifies the sign-on policies that PingOne should use for authentication. You can include any policies assigned to the application. Specify either a single DaVinci policy by flow policy ID or one or more PingOne policies by name, separated by spaces or the encoded space character `%20`. For example, `acr_values=d1210a6b0b2665dbaa5b652221badba2` or `acr_values=Single_Factor%20Multi_Factor`.

   Learn more in Authentication policies for applications.

7. On the **Attribute Mappings** tab, click the **Pencil** icon and select a PingOne user attribute and map it to an attribute in the application that you are adding.

   Learn more in Mapping attributes.

   1. Enter an application attribute and then select the corresponding PingOne attribute from the list.
   2. Click the **Gear** icon to use the expression builder to build an attribute mapping.

      Learn more in Using the expression builder.

8. On the **Access** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Admin only access	Specifies that a user with an administrator role is required to access the application. The user must have one of the following roles: ◦ `Organization Admin` ◦ `Environment Admin` ◦ `Identity Data Admin` ◦ `Client Application Developer`
Group membership policy	Select the group membership policy for the application. Learn more in Groups.

9. On the **Roles** tab, click the **Pencil** icon and select the roles for the worker application.

Copyright © 2025 Ping Identity Corporation

Worker apps have no roles by default. After the application is created, you can add or remove roles as needed, up to the level of your roles as a user. You cannot assign roles that you do not have. Learn more in Configuring roles for a worker application.

10. Click **Save**.
11. To enable the application, click the toggle at the top of the details panel to the right (blue).

> **Note**
> You can disable the application by clicking the toggle to the left (gray).

Related links

- Editing an application - SAML
- Editing an application - OIDC
- Editing an application - Native
- Editing an application - Single page
- Editing an application - Device authorization

Editing an application - Device authorization

Use the **Applications** page to edit existing device authorization applications.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the application that you want to edit.
2. Click the application entry to open the details panel.
3. On the **Overview** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Application Name	A unique identifier for the application.
Description (optional)	A brief description of the application.
Icon (optional)	A pictorial representation of the application. Use a file up to 1 MB in JPG, JPEG, GIF, or PNG format.
Home page URL	The default home page for the application.

Copyright © 2025 Ping Identity Corporation

Field	Description
Signon URL	The URL to which the application requests that the end user be redirected to for sign-on. **Important** To avoid issues with third-party cookies in some browsers, we recommend that you use a custom domain to give your PingOne environment the same parent domain as your authentication application. Learn more in Domains.

4. On the **Configuration** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Client ID	The unique identifier for the application.
Client Secret	The shared secret for the application. Ensure that you protect the client secret and store it in a secure location. To update the client secret, click **Generate New Secret**. To revoke the previous client secret, click **Revoke Previous Client Secret**. Learn more in Rotating the client secret for an application.
Environment ID	The identifier for the environment that contains the application.
Response type	Select **Code**, **Token**, or **ID Token** for the response type. Learn more in Response types.
Grant Type	Select **Device Authorization** and **Refresh Token** for the grant type. Learn more in Grant types.

Copyright © 2025 Ping Identity Corporation

Field	Description
Device authorization configuration	Select this option to enable the Device Authorization grant type. You can specify the following: ***Device Path ID (optional)*** Specifies a unique identifier within an environment for a device authorization grant flow to provide a short identifier to the application. The string can contain letters, numbers, hyphens, and underscores and can be up to 50 characters. **Note** PingOne ignores **Device Path ID** if **Device Custom Verification URI** is configured. ***Device Custom Verification URI (optional)*** Specifies an optional custom verification URI. Learn more in Device custom verification URIs. ***Device Authorization Timeout (required)*** The lifetime, in seconds, of the `user_code` and `device_code`. The default value is 600 seconds and the maximum value is 3600 seconds. ***Device Polling Interval (required)*** The minimum amount of time, in seconds, that the client should wait between polling requests to the token endpoint. The default value is 5 seconds, and the maximum value is 60 seconds. Learn more in Device authorization.
Refresh Token configuration	Select this option to enable the Refresh Token grant type. You can specify the following: ***Refresh token duration*** The lifetime of the refresh tokens. If a value is not provided, the default value is `2592000`, or 30 days. Valid values are between `60` and `2147483647`. ***Refresh token rolling duration*** How long the application can use the refresh token grant type to obtain a new access token (and a new refresh token) after the most recent user authentication event. If a value is not provided, the refresh token is valid forever. Valid values are between `60` and `2147483647`. **Note** The refresh token rolling duration must be longer than the refresh token duration. ***Refresh token rolling grace period*** The amount of time that a rolled refresh token is still valid in the event that the client failed to receive an updated one during a roll. Valid values are between `0` and `86400` seconds. A value of zero means a refresh token becomes invalid after it's rolled.

Copyright © 2025 Ping Identity Corporation

Field	Description
Redirect URIs	The address to which PingOne forwards the OIDC response after authentication. **Note** The Redirect URI cannot contain a fragment component, such as `#somedata`. Learn more in Redirection endpoint in the IETF documentation.
Allow Redirect URI patterns	Use a wildcard for flexibility in managing redirect URIs. See Redirect URIs.
Token Endpoint Authentication Method	Select one of the following: ◦ **None** ◦ **Client Secret Basic** ◦ **Client Secret Post** ◦ **Client Secret JWT** ◦ **Private Key JWT**
JSON Web Key Set Method	Select **JWKS URL** or **JWKS**. Provide either the URL where PingOne can retrieve the JSON Web Key Set (JWKS) or the web key set itself. You can paste the JSON in one line or multiple lines. **JWKS Method** is required for an application to send asymmetrically signed request objects. To use **Private Key JWT** for **Token Endpoint Authentication Method**, PingOne reuses the same JWKS URL or JWKS to process the private key JSON Web Token (JWT). **Note** ◦ If **Token Endpoint Authentication Method** is set to **Private Key JWT**, you must provide the **JWKS Method**. ◦ If **Token Endpoint Authentication Method** is set to **None**, **Client Secret Basic**, **Client Secret Post**, or **Client Secret JWT**, if the **JWKS Method** is not provided and the application sends an RS256/384/512-signed request object to PingOne, PingOne returns an error.
Require Pushed Authorization Request	Require the application to send its authorization requests directly to PingOne, without going through the browser, which can safeguard sensitive information from end-user devices. If **Require Pushed Authorization Request** is not selected, the application can send plain authorization requests or pushed authorization requests, but pushed authorization requests are not required. Learn more in Pushed authorization requests.
Pushed Authorization Request Reference Timeout	Specify how long the pushed authorization request should be valid. The default value is 60 seconds.

Copyright © 2025 Ping Identity Corporation

Field	Description
Initiate Login URI	The application's login initiation endpoint for third-parties to begin the sign-on process for the application. If provided, PingOne redirects users to this URI to initiate SSO to PingOne. The application is responsible for implementing the relevant OIDC flow when the **Initiate Login URI** is requested. Learn more in Initiating Login from a Third Party in the OIDC specification. This URI is required if you want the application to show in the PingOne Application Portal. Learn more in Application portal.
Target Link URI	The URI for the application. If provided, PingOne redirects application users to this URI after the user is authenticated. The `target_link_uri` parameter value in `Initiate Single Sign-On URL`, as shown as part of the application configuration in the PingOne console, is also updated with the value specified here.
Signoff URLs	The URLs to which the browser can be redirected after a logout has been performed. If you include a `post_logout_redirect_uri` query parameter in the `/signoff` request, with the same value that was set in the application, then the browser will redirect the user to the matching URL.
Request Parameter Signature Requirement	Specify how the application sends the optional `request` parameter in its authorization requests. Click **Compare Options** for a description of the different settings. ◦ **Default**: Allow the application to send authorization requests with or without the `request` parameter. If using the request parameter, the application must include a digital signature. ◦ **Allow unsigned request parameters**: Allow the application to send authorization requests with or without the `request` parameter. If using the `request` parameter, the application has the option to include a digital signature or not. ◦ **Require signed request parameters**: Require the application to use the `request` parameter and include a digital signature of it in its authorization requests. Learn more in Request Parameter Signature Requirement.
Additional Refresh Token Replay Protection	Outside of the optional rolling grace period, refresh tokens are intended for one-time use. For increased security, enable this option so that PingOne can invalidate both access and refresh tokens when a refresh token is reused. Learn more in Refresh token rotation.

Copyright © 2025 Ping Identity Corporation

Field	Description
OpenID Connect Session Management	Facilitate OIDC session management by allowing applications in the same browsing mode, such as private or normal browsing mode, to monitor the PingOne user session. Only applications running in the same browsing mode can monitor the PingOne user session. To use this option, your PingOne environment must be configured with a custom domain, such as `sso.example.com`, and the applications must be accessible under that domain. For example, `apps.example.com/app1` and `apps.example.com/app2` or `app1.example.com` and `app2.example.com`. Learn more in Setting up a custom domain. When enabled, the `session_state` parameter is included in the PingOne authorization response with the session status, such as `unchanged`, `changed`, or `error`. Learn more in OIDC session management in the PingOne API documentation and Best practices: Session management. **Note** ◦ The default idle timeout is 30 days. To set an idle timeout of fewer than 30 days: 1. Build a PingOne DaVinci flow that includes the Return Success Response (Redirect Flows) node from the PingOne Authentication connector. 2. In the Return Success Response (Redirect Flows) node, set the **Idle Timeout** value to the desired amount of time, such as 5 minutes. 3. Assign the flow to the applicable applications. ◦ If a user session is deleted because of a PingOne session API request or is purged by the system, it doesn't trigger a `changed` response.
Include the x5t parameter in the header of access tokens, ID tokens, and JWT-based refresh token	Select for PingOne to include the `x5t` header parameter in access tokens, ID tokens, and JWT-based refresh tokens. Enable this option if the application, custom resource, or both require the `x5t` parameter in the digital signature verification process.
Terminate User Session by ID Token	Enable this option to allow the application to send requests for PingOne to terminate end-user sessions at the `/idpSignoff` endpoint using only the ID token. The audience claim value in the ID token must match the client ID of the application so that PingOne can identify the session to be terminated. The application is not required to have access to the session token cookie. Learn more in the PingOne API documentation.

Copyright © 2025 Ping Identity Corporation

Field	Description
CORS Settings	Specifies the CORS options for the application. Learn more in Cross-origin resource sharing. ◦ **Allow any CORS-safe origin** (default): Allows the application to access resources from a domain that is CORS-safelisted, according to the Fetch specification. ◦ **Allow specific origins**: Allows the application to access resources from a specific domain. ■ **Allowed origins**: Specifies the allowed origin domains for CORS. You can specify a domain pattern or a valid IPv4 address. If you use a domain pattern, you can specify one wildcard to match incoming requests. **Note** You cannot use the wildcard on the domain name. For example, the following search patterns are valid: ■ `https://*.test.com` ■ `https://www.app*.test.com` The following patterns are not valid: ■ `https://test*.com` ■ `https://www.app.test*.com` ◦ **Disallow all origins**: Don't allow the application to access resources from a cross-origin domain. **Note** After you make changes to the **CORS Settings**, it can take several minutes for the new settings to take effect, due to time-to-live configuration on the resource.

5. On the **Resources** tab, click the **Pencil** icon and select the check boxes to add appropriate OAuth scopes for the application. Click the **Selected scopes** tab to see the scopes that are currently selected for the application.

   The OAuth scopes determine the resources that the application can access. If you add OIDC scopes here, the application inherits the attributes associated with that scope.

   If the application uses the Refresh Token grant type, add the `offline_access` scope to enable the application to request a refresh token from PingOne on a per-request basis. For example, when the application needs a refresh token, it includes the `offline_access` scope in its request, and PingOne includes a refresh token in its token response. However, when the application doesn't need a refresh token, it doesn't include the scope in the request, and PingOne therefore doesn't include a refresh token in its token response. If the `offline_access` scope is not added to an application that uses the Refresh Token grant type, PingOne always includes a refresh token in its token response, whether the application needs a refresh token or not.

6. On the **Policies** tab, click the **Pencil** icon and select the authentication policies for the application.

   If you have a DaVinci license, you can select PingOne policies or DaVinci flow policies, but not both. If you don't have a DaVinci license, you'll see PingOne policies only.

Copyright © 2025 Ping Identity Corporation

To add one or more PingOne authentication policies, click the **PingOne Policies** tab. If the application was previously configured with one or more DaVinci flow policies, click **Deselect all other Policies** to remove them from the application and select the PingOne authentication policies you want to apply to the application. PingOne authentication policies are applied in the order in which they appear in the list. Click the **Selected PingOne Policies** tab, reorder the policies as needed, then click **Save**.

To add one or more DaVinci flow policies, click the **DaVinci Policies** tab. If the application was previously configured with one or more PingOne authentication policies, click **Deselect all other Policies** to remove them from the application and and select the DaVinci flow policies you want to apply to the application. PingOne applies the first DaVinci flow policy in the list. Click the **Selected DaVinci Policies** tab, reorder the policies as needed, then click **Save**.

For OAuth-based applications, you can specify another policy in the `acr_values` parameter in the authorization request. The `acr_values` parameter specifies the sign-on policies that PingOne should use for authentication. You can include any policies assigned to the application. Specify either a single DaVinci policy by flow policy ID or one or more PingOne policies by name, separated by spaces or the encoded space character `%20`. For example, `acr_values=d1210a6b0b2665dbaa5b652221badba2` or `acr_values=Single_Factor%20Multi_Factor`.

Learn more in Authentication policies for applications.

7. On the **Attribute Mappings** tab, click the **Pencil** icon and select a PingOne user attribute and map it to an attribute in the application that you are adding.

   Learn more in Customizing OIDC attributes for an application.

   1. Enter an application attribute and then select the corresponding PingOne attribute from the list.
   2. Click the **Gear** icon to use the expression builder to build an attribute mapping.

      Learn more in Using the expression builder.

8. On the **Access** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Application portal display	Determines whether an application icon appears in the application portal even if the user is allowed to access the application in the application portal based on the group membership policy. Learn more in Application access control.
Admin only access	Specifies that a user with an administrator role is required to access the application. The user must have one of the following roles: ◦ `Organization Admin` ◦ `Environment Admin` ◦ `Identity Data Admin` ◦ `Client Application Developer`
Group membership policy	Select the group membership policy for the application. Learn more in Groups.

9. Click **Save**.

Copyright © 2025 Ping Identity Corporation

10. To enable the application, click the toggle at the top of the details panel to the right (blue).

> **Note**
> You can disable the application by clicking the toggle to the left (gray).

Related links

- Editing an application - SAML
- Editing an application - OIDC
- Editing an application - Native
- Editing an application - Single page
- Editing an application - Worker

Configuring web applications

You can configure web applications for Strong Authentication customer use cases.

Configuring a web application includes the following steps:

- Creating a web application
- Associating an authentication policy with a web app

Creating a web application

A web application is a browser-based application with a server-side component, such as .NET web apps, JSP/Java, Node.js, or Ruby on Rails.

About this task

Web applications typically have functions similar to desktop applications. Web applications can use Security Assertion Markup Language (SAML) or OpenID Connect (OIDC) for authentication.

A web application includes the following configuration:

Create App Profile	The application name and description.
Configure	The application's redirect URL.
Grant Access	To your application (for your customers to trigger authentication requests).
Attribute Mapping	Map your PingOne user-defined attributes to the corresponding application attributes for accessibility between users and your app.

Copyright © 2025 Ping Identity Corporation

Every user authentication event occurs in the context of a SAML or OIDC application. When you invoke multi-factor authentication (MFA) through an OIDC request, you must provide a client ID, which is the ID of your web application.

A worker app is used to make backend calls. In contrast, a web app (or native app or single page app) is required for invoking an authentication flow.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications**.
2. Click **+**.

   Result:

   The **Add Application** panel opens.
3. Enter an appropriate **Application Name** and a **Description**.

   Example:

   For example, the application name `Getting Started Web OIDC App`.
4. In **Choose Application Type**, click **OIDC Web App**.
5. Click **Save**.

   Result:

   The details panel opens. Applications are granted OAuth scopes so that they can access PingOne platform resources.
6. To configure the application URL, click the **Configuration** tab, then click the **Pencil** icon.
7. In the **Redirect URIs** field, enter your application's redirect URL (for example, `https://example.com`).
8. Click **Save**.
9. To grant access to your application, click the **Access** tab and click the **Pencil** icon.
10. Click **+** to select the groups.
11. Click **Save**.
12. Click the **Resources** tab, and click the **Pencil** icon.
13. Enter `profile` in the **Search Scopes** field

    > **Note**
    >
    > This filters the list of resource types so that only the Open ID **profile** scope remains visible in the scopes selection list.

14. On the **Profile Scope**, click the **+** icon or drag it out to the **Allowed Scopes**.
15. Click **Save**.
16. To map your PingOne user-defined attributes to your corresponding application attributes, click the **Attribute Mappings** tab, and click the **Pencil**icon.

Copyright © 2025 Ping Identity Corporation

17. Click **+ Add** and fill in the **Attributes**and corresponding **PingOne Mappings** fields.
18. Click **Save**.
19. At the top right of the web application's profile, click the toggle to enable it.

> **Tip**
>
> You can find more information and additional configuration options in Adding an application.

Associating an authentication policy with a web app

Depending on the sensitivity of information and processing capabilities of each application, an organization can determine that multi-factor authentication (MFA) requirements for some applications are more stringent than for others.

PingOne provides the capability to define multiple MFA sign-on policies. You can configure one application to use a particular sign-on policy and another application to use a different policy.

The authentication flow is configured at the application level through a sign-on policy. If you don't assign a sign-on policy to your web application, it uses the environment's default sign-on policy. You can create multiple sign-on policies and associate them with different OpenID Connect (OIDC) applications.

You can also associate multiple sign-on policies with a single application. Policies are applied in the order in which they appear in the list. PingOne evaluates the first policy in the list first. If the requirements of the policy are not met, PingOne moves to the next policy in the list.

Copyright © 2025 Ping Identity Corporation

Console

Associating your authentication policy with your web app console

Before you begin

Before assigning your authentication policy with a web app, first create the application. Learn more in Configuring web applications.

About this task

You can find information about how to perform this task from the API in POST: Step 3: Assign the sign-on policy to an application.

Steps

1. Go to **Applications > Applications**.
2. Locate your web application and click it to open the details panel.
3. Click the **Policies** tab.
4. Click the **Pencil** icon to enter edit mode.
5. In the **PingOne Policies** list, locate the policy you created in the previous step.

   Example:

   For example, **MFA-only**.
6. Select the checkbox for the appropriate policy.
7. Click **Save**.

Next steps

Create a user

Copyright © 2025 Ping Identity Corporation

API alternative

Associating your authentication policy with your web app API alternative
About this task

Application developers can use the API operations to associate a sign-on policy with an application.

Steps

- Use the access token generated through the worker app and the following `POST` operation to assign the new authentication policy to an application:

```
POST https://api.pingone.com/v1/environments/{{envId}}/applications/{{appID}}/
signOnPolicyAssignments
```

See POST: Step 3: Assign the sign-on policy to an application.

Next steps

Create a user

Deleting an application

You can remove an application that you no longer need.

About this task

> **Note**
> To delete an application, you must have the `Client Application Developer` role.

Steps

1. Go to **Applications** > **Applications**.
2. Locate the application you want to delete. You can browse or search for applications.
3. Click the application entry to open the details panel.
4. In the upper right, click the three dots options menu, and then click **Delete**.
5. In the confirmation message, click **Delete**.

System applications

PingOne includes several applications that are part of the PingOne platform.

PingOne includes the following system applications:

- **PingOne Admin Console**

Copyright © 2025 Ping Identity Corporation

- **PingOne Application Portal**
- **PingOne Self-Service - MyAccount** (learn more in Self Service.)

You can assign sign-on policies to these system applications to control who can access them. You can disable the self-service app, but not the admin console. If you disable the self-service application, no end users can sign on to it, but administrators can. You can't disable the self-service app using the **Enable** toggle for the application. Instead, go to the application details and select **Must have admin role**. Learn more in Application access control.

> **Note**
>
> The **PingOne Admin Console** application uses a system policy configured in **Settings > Administrator Security** instead of the default policy. You can't assign a different policy to the admin console. Learn more in Administrator security.

You can find the system applications on the **Applications** page. Learn more in Application access control.

Device custom verification URIs

Device authorization applications can use a device custom verification URI to present a shorter URL that is easier for the user to enter.

> **Note**
>
> Device custom verification URIs can be configured for applications for which the **Device Authorization** grant type is enabled. For more information, see Grant types.

Instead of presenting the user with a PingOne URL, such as https://auth.pingone.com/device/082dba86-d36e-413e-85b4-ee499a5cea55, a device custom verification URI provides them with a shorter URL, for example https://example.com/device, that's easier to enter or remember.

When you configure your device authorization application in PingOne, you can define this URI using the **Device Custom Verification URI** setting. If you configure the **Device Custom Verification URI** setting, the response from PingOne returns the URL as configured. If you do not use this setting, the generated device custom verification URI follows these rules:

Response URL formats

Custom domain configured for the environment?	Device Path IDconfigured?	Format of URL returned from PingOnePingOne
Yes	Yes	URL returned by PingOne is in one of the following formats: • https://*<customDomain>*/device/*<devicePathId>* • https://*<customDomain>*/device/*<devicePathId>*?user_code=*<userCode>*

Custom domain configured for the environment?	Device Path IDconfigured?	Format of URL returned from PingOnePingOne
Yes	No	URL returned by PingOne in one of the following formats: • https://*<customDomain>*/device • https://*<customDomain>*/device?user_code=*<userCode>*
No	Yes	URL returned by PingOne is in one of the following formats: • https://auth.pingone.*<region>*/*<envId>*/device/*<devicePathId>* • https://auth.pingone.*<region>*/*<envId>*/device/*<devicePathId>*?user_code=*<userCode>*

Important

The URLs for the Device Custom Verification URI and for the redirect are generated based on the inbound initial authorize call. For more information, see Configuring a redirect for a device custom verification URI.
For example, if the custom domain for the environment is example.com, but the initial call is from https://auth.pingone.com/*<envID>*/as/device_authorization, then the generated device custom verification URI will have a format of https://auth.pingone.com/*<envId>*/device/*<devicePathId>*.
If the initial call is from https://example.com/as/device_authorization, the generated device custom verification URI will have a format of https://example.com/device/*<devicePathId>*.

Related links

- Editing an application - Device authorization

Configuring a redirect for a device custom verification URI

If the **Device Custom Verification URI** setting is configured for a device authorization application, the administrator must configure a redirect to which PingOne forwards the OIDC response after authentication.

About this task

The format of the redirect depends on a combination of two factors:

- Is a custom domain configured for the environment?
- Is the **Device Path ID** configured for the application?

Steps

- Configure your redirects based on the information in the following table:

Copyright © 2025 Ping Identity Corporation

Redirect formats for device custom verification URI

Custom domain configured for the environment?	Device Path IDconfigured?	Valid formats for redirects
Yes	Yes	◦ https://*<customDomain>*/device/*<clientId>*?user_code=*<userCode>* ◦ https://*<customDomain>*/device/*<clientId>* ◦ https://*<customDomain>*/device/*<devicePathId>*?user_code=*<userCode>* ◦ https://*<customDomain>*/device/*<devicePathId>* ◦ https://*<customDomain>*/device?user_code=*<userCode>* ◦ https://*<customDomain>*/device
Yes	No	◦ https://*<customDomain>*/device/*<clientId>*?user_code=*<userCode>* ◦ https://*<customDomain>*/device/*<clientId>* ◦ https://*<customDomain>*/device?user_code=*<userCode>* ◦ https://*<customDomain>*/device
No	Yes	◦ https://auth.pingone.*<region>*/device/*<clientId>*?user_code=*<userCode>* ◦ https://auth.pingone.*<region>*/device/*<clientId>* ◦ https://auth.pingone.*<region>*/device/*<devicePathId>*?user_code=*<userCode>* ◦ https://auth.pingone.*<region>*/device/*<devicePathId>* ◦ https://auth.pingone.*<region>*/device?user_code=*<userCode>* ◦ https://auth.pingone.*<region>*/device
No	No	◦ https://auth.pingone.*<region>*/device/*<clientId>*?user_code=*<userCode>* ◦ https://auth.pingone.*<region>*/device/*<clientId>* ◦ https://auth.pingone.*<region>*/device?user_code=*<userCode>* ◦ https://auth.pingone.*<region>*/device

Note

The *clientId* path is safer because that value does not change (*devicePathId* can change). In addition, a redirect to `/device` without a *clientId* or *devicePathId* is not recommended because the application's configured sign-on policy can't be used. However, if you use the same **Device Custom Verification URI** value for two separate applications, then a redirect to `/device` is needed, and the flow uses the environment's default sign-on policy.

Example:

Copyright © 2025 Ping Identity Corporation

For example, if the custom domain for the environment is set to `acme-corporation.com`, the **Device Custom Verification URI** for the application is set to `https://acme.com/go`, and the client ID for the application is `c78dbdd0-cc2c-42fa-b275-486503c30d2b`, the workflow is:

1. The end user enters the short URL, such as `https://acme.com/go`, in a browser to start the activation flow.
2. Outside of PingOne, the administrator has configured the following redirect to redirect the browser and start the device authorization flow: `https://acme-corporation.com/device/c78dbdd0-cc2c-42fa-b275-486503c30d2b`.
3. In PingOne, the flow redirects to https://acme-corporation.com/signon?flowId=03f3581c-7fee-4bf5-adb1-ed056d31ce91 to start the PingOne flow.

Next steps

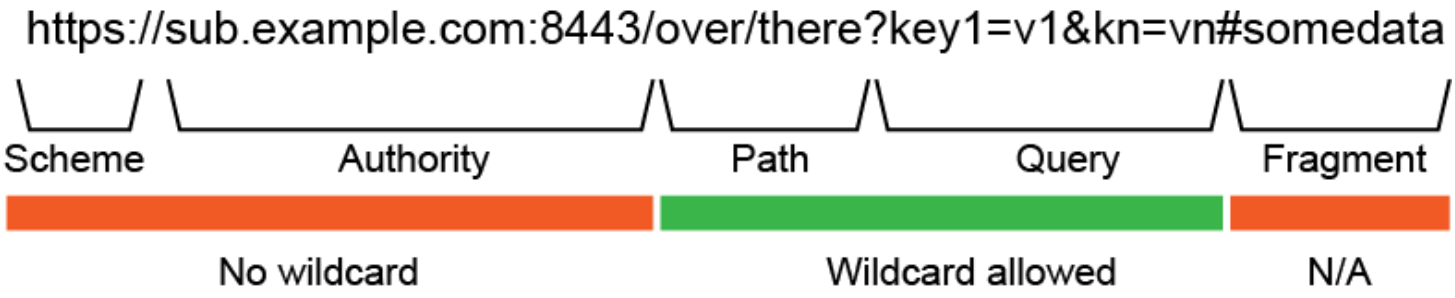
For more information about configuring your device authorization application, see Editing an application - Device authorization.

Redirect URIs

A redirect URI is the address to which PingOne forwards the OIDC response after authentication. For flexibility in configuring the redirect URI, you can use wildcards and loopback IP redirects.

Wildcards in redirect URIs

You can choose to allow a wildcard in the Redirect URI. Rather than entering an exact URI, you can use a wildcard to include multiple paths using one entry. Use wildcards in the path and query portions of the URI, that is, the portion of the URI after the authority. Only one wildcard is allowed per URI. The `*` operator is the only supported wildcard. For more information, see Editing an application.



Example

An application is configured with a **Redirect URI** entry of:

```
https://www.example.com/th*/callback
```

redirect_urivalue in the authorization request	Result
`https://www.example.com/this/callback`	PingOne accepts the provided `redirect_uri` value because `this` matches the `th*` pattern.

Copyright © 2025 Ping Identity Corporation

redirect_urivalue in the authorization request	Result
`https://www.example.com/that/callback`	PingOne accepts the provided `redirect_uri` value because `that` matches the `th*` pattern.
`https://www.example.com/oidc/callback`	PingOne rejects the provided `redirect_uri` value because `oidc` does not match the `th*` pattern. PingOne returns `Redirect URI mismatch` to the application.

> **Note**
> For security reasons, we recommend that you use a hardcoded URL (exact match), but the wildcard option can give you flexibility if you need it.

Loopback IP redirect URIs

PingOne supports any valid port for loopback IP redirect URIs. Native applications that can open a port on the loopback network interface without needing special permissions can use the loopback interface to receive the OAuth redirect.

To use a loopback URI, specify the **Authority** URL as a loopback IP address or `localhost`, and the port that the client is listening on. The **Scheme** must be HTTP or HTTPS. For more information, see Loopback Interface Redirection in the OAuth 2.0 for Native Apps RFC.

Example 1

An application is configured with a **Redirect URI** entry of:

```
http://127.0.0.1/cb
```

redirect_urivalue in the authorization request	Result
`http://127.0.0.1/cb`	PingOne accepts the provided `redirect_uri` value because it is an exact match.
`http://127.0.0.1:8080/cb`	PingOne accepts the provided `redirect_uri` value because port 8080 is a valid port.
`http://127.0.0.1:80/cb`	PingOne accepts the provided `redirect_uri` value because port 80 is a valid port.
`https://127.0.0.1/cb`	PingOne rejects the provided `redirect_uri` value because `https://` does not match the expected scheme of `http:/`. PingOne returns `Redirect URI mismatch` to the application.

Example 2

An application is configured with a **Redirect URI** entry of:

Copyright © 2025 Ping Identity Corporation

```
http://127.0.0.1:8080/cb
```

redirect_urivalue in the authorization request	Result
`http://127.0.0.1:8080/cb`	PingOne accepts the provided `redirect_uri` value because it is an exact match.
`http://127.0.0.1:9080/cb`	PingOne rejects the provided `redirect_uri` value because port 9080 does not match the expected port 8080. PingOne returns `Redirect URI mismatch` to the application.
`http://127.0.0.1:80/cb`	PingOne rejects the provided `redirect_uri` value because port 80 does not match the expected port 8080. PingOne returns `Redirect URI mismatch` to the application.

Application access control

Use application access control to define access to applications through roles and groups.

For each application, specify the conditions that must be met by an authenticating user to access an application. You can use application access control with all types of applications.

> **Note**
>
> You can define application permissions to control access to custom-developed application features after users authenticate. Learn more in Application permissions.

Role type

Specifies that a user with an administrator role is required to access the application. The user must have one of the following roles:

- Organization Admin
- Environment Admin
- Identity Data Admin
- Client Application Developer

Learn more in Administrator Roles. If no option is selected, an administrator role is not required to access the application.

Group type

Specifies that a user must be a member of a particular group or groups to access the application. If you have two or more groups, you can specify how group access is applied:

- **Any**: The user must be a member of at least one of the specified groups.
- **All**: The user must be a member of all specified groups.

Copyright © 2025 Ping Identity Corporation

If no option is selected, group membership is not required to access the application. If an existing group is removed from the environment, then any members of the group might no longer have access to the application, depending on their other group memberships and how group evaluation is configured.

Application portal

Determines whether an application icon appears in the application portal if the user would see the application in the application portal based on the group membership policy.

For example, you could use this option if the SSO flow is being triggered through means other than on the application portal or because you are creating multiple application deep links that will be shown in the application portal rather than the actual application. Learn more in Application portal.

Configuring application access control

Use application access control to define access to applications through roles and groups. For each application, specify the conditions that must be met by an authenticating user to access an application. You can use application access control with all types of applications.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the application you want to configure.
2. Click the application entry to open the details panel for the application.
3. On the **Access** tab, click the **Pencil** icon.
4. For **Admin Only Access**, to specify whether an administrator role is required to access the application, select the **Must have admin role** checkbox.

   Available roles are:

   - **Organization Admin**
   - **Environment Admin**
   - **Identity Data Admin**
   - **Client Application Developer**

     Learn more in Administrator Roles.
5. For **Group Membership Policy**, specify the groups that can access the application by searching or browsing for the group.

   The list is updated as you enter the search criteria. Do one or more of the following:

Option	Description
Add a group to the access list	On the **Groups** tab, select the checkbox for a group name to add it to the **Applied Groups** list.
Remove a group from the access list	On the **Applied Groups** tab, clear the checkbox for the group name you want to remove.

Copyright © 2025 Ping Identity Corporation

Option	Description
Require any group membership	If you apply two or more groups, select **User is a member of any applied group** to require the user to be a member of any of the applied groups to access the application.
Require all group membership	If you apply two or more groups, select **User must be a member of all applied groups** to require the user to be a member of all applied groups to access the application.

> **Note**
> If you remove an existing group from the environment, then any members of the group lose access to the configured application.

6. Click **Save**.

Auditing access events

You can use the **Audit** page to see a summary of user access events related to application access control.

Steps

1. In the PingOne admin console, go to **Monitoring** > **Audit**.
2. For **Time Range**, select the desired time span.
3. For **Filter Type**, select **Event Type**.
4. For **Filter**, select one of the following:
    - **User Access Allowed**: The user accessed the resource successfully.
    - **User Access Denied**: The user was denied access to the resource.
5. Click **Run**.

Next steps

- In the **Activities** list, see the **Description** column for specific events.
- In the **Details** column, click **View** to see more detailed information about the event.

Authentication policies for applications

You can configure which authentication policies should be used for a particular application.

An application can have zero or more associated authentication policies that determine how users are authenticated. The number of sign-on policies assigned to an application also controls how the authentication steps progress.

If you have a DaVinci license, you can select PingOne policies or DaVinci flow policies, but not both. If you don't have a DaVinci license, you can only assign PingOne policies.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> The PingOne admin console uses a system policy configured in **Settings** > **Administrator Security** instead of the default authentication policy. You can't assign a different policy to the admin console.
> Learn more in Administrator security.

Policies are applied in the order in which you add them. The first policy in the list overrides any subsequent policies. The default policy is always used if no policies are applied to an application.

Learn more about assigning a sign-on policy to an application in Applying authentication policies to an application.

> **Note**
>
> If an application is assigned only one authentication policy, such as the Passwordless sign-on policy, then the application uses only that policy. If the application is assigned multiple policies, it uses policies in the order they appear in the list.

No authentication policy assignments

Applications that aren't assigned an authentication policy use the environment's default authentication policy to authenticate users. Every environment has one authentication policy configured as its default policy. If the environment's default authentication policy changes, then the application uses the updated default policy.

One authentication policy assignment

Applications that are assigned one authentication policy always use that policy to authenticate users. For example, if the application is assigned the `Single_Factor` authentication policy, the application always uses this basic authentication method that prompts users to enter a username and password to authenticate the account.

Two or more authentication policy assignments

If an application is assigned two or more authentication policies, the authentication flow uses the policy with the highest priority first. If authentication is successful, the authentication flow is complete. If authentication fails, the flow initiates the authentication policy with the next highest priority. If authentication fails again, the authentication flow initiates the next authentication policy. The authentication flow continues until one of the assigned policies is completed successfully or all policies have been tried and failed.

Applying authentication policies to an application

Authentication policies define sign-on requirements for accessing an application.

Before you begin

Add an authentication policy in PingOne. Learn more in Adding an authentication policy and Authentication policies.

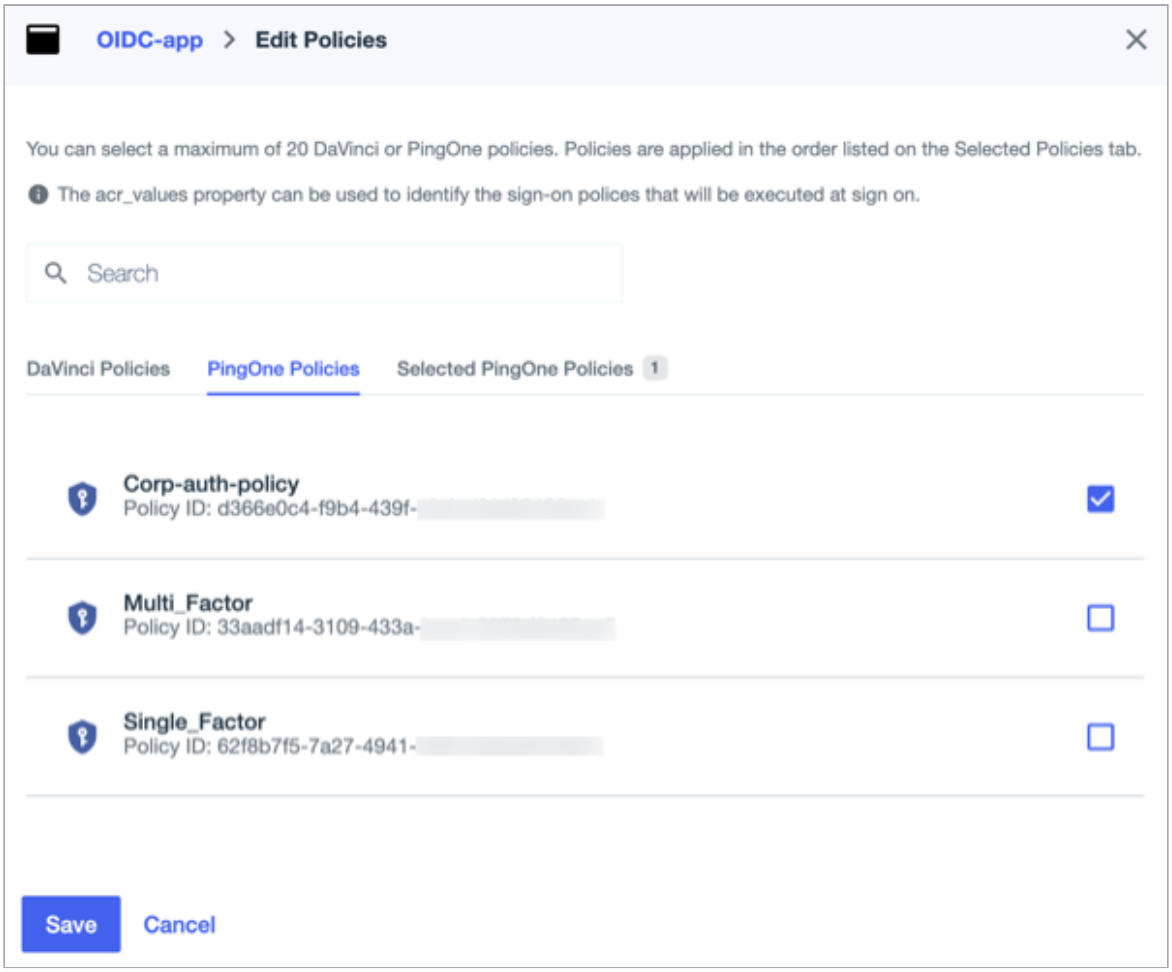
> **Note**
>
> The PingOne admin console uses a system policy configured in **Settings** > **Administrator Security** instead of the default authentication policy. You can't assign a different policy to the admin console.
> Learn more in Administrator security.

Copyright © 2025 Ping Identity Corporation

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the application you want to edit.
2. Click the application entry to open the **Details** panel.
3. On the **Policies** tab, click the **Pencil** icon.
4. Select the checkbox for the policy that you want to apply.

> **Note**
>
> You can select a maximum of 20 policies, and the policies are applied in the order listed on the **Selected Policies** tab.
> If you have a DaVinci license, you can select PingOne policies or DaVinci flow policies, but not both. If you don't have a DaVinci license, can only see and select PingOne policies.



5. (Optional) Go to the **Selected PingOne Policies** or **Selected DaVinci Policies** tab and drag and drop the policies to change the order in which they are applied.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> There is only one **Selected Policies** tab. The tab name displayed depends on whether you are using DaVinci flow policies or PingOne policies.

6. Click **Save**.

Viewing OIDC attributes for an application

Use the application details panel to view the current attribute mappings for an OIDC application.

Steps

1. Go to **Applications** > **Applications**.
2. Locate the application you want to view. You can browse or search for applications, or narrow your search to a particular application type
3. Click the application entry to open the details panel.
4. Click the **Attribute mappings** tab.

   PingOne shows the current attribute mappings for the OIDC application.

   ### *Custom attributes*

   Attributes that are mapped for the OIDC application. Applications can override the inherited global attributes with custom attributes.

   ### *Inherited global attributes*

   Attributes that are mapped as part of the OIDC resource on the **Resource** page. You can create custom attributes as a global setting, and applications will inherit the attribute mappings for any claims they need. Applications can override the inherited global attributes with custom attributes.

Next steps

To modify attribute mappings, see Customizing OIDC attributes for an application.

Customizing OIDC attributes for an application

About this task

In your PingOne Admin console, use the application details panel to customize the current attribute mappings for an OIDC application. Applications can override the inherited global attributes with custom attributes that you want included during runtime.

For example, if you're adding an OIDC app to PingOne, and the application owner requires the user's birthdate, which isn't a default mapping value, you can add birthdate to the OIDC application's Attribute Mappings configuration, sourcing it from something such as a custom user attribute that you've defined. Then, when the application asks for the profile OIDC scope at runtime, PingOne can include birthdate in the ID token and the UserInfo response.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Applications > Applications**.
2. Locate the application you want to view. You can browse or search for applications, or narrow your search to a particular application type
3. Click the application entry to open the details panel.
4. Click the **Attribute mappings** tab and then click the pencil icon to edit.

   PingOne shows the current attribute mappings for the OIDC application.

   ### *Custom attributes*

   Attributes that are mapped for the OIDC application. Applications can override the inherited global attributes with custom attributes.

   ### *Inherited global attributes*

   Attributes that are mapped as part of the OIDC resource on the **Resource** page. You can create custom attributes as a global setting, and applications will inherit the attribute mappings for any claims they need. Applications can override the inherited global attributes with custom attributes.

5. Do one or more of the following:
   - To edit an existing attribute, select the OIDC attribute and the desired PingOne mapping.

     > **Note**
     > Attributes with a blue background are part of the OIDC specification. You cannot delete the default attributes, but you can map them to new attributes in PingOne. PingOne will ignore an attribute if the PingOne mapping is blank.

   - To add an attribute, click the **+ Add** button. Enter an OIDC attribute and the desired PingOne mapping. Click the gears icon to use advanced expressions. See Using the expression builder.
   - To delete an attribute, click the trash can icon for the appropriate attribute.
   - To use the advanced configuration editor, click **Advanced configuration**. See Using the advanced configuration editor.
6. Click **Save**.

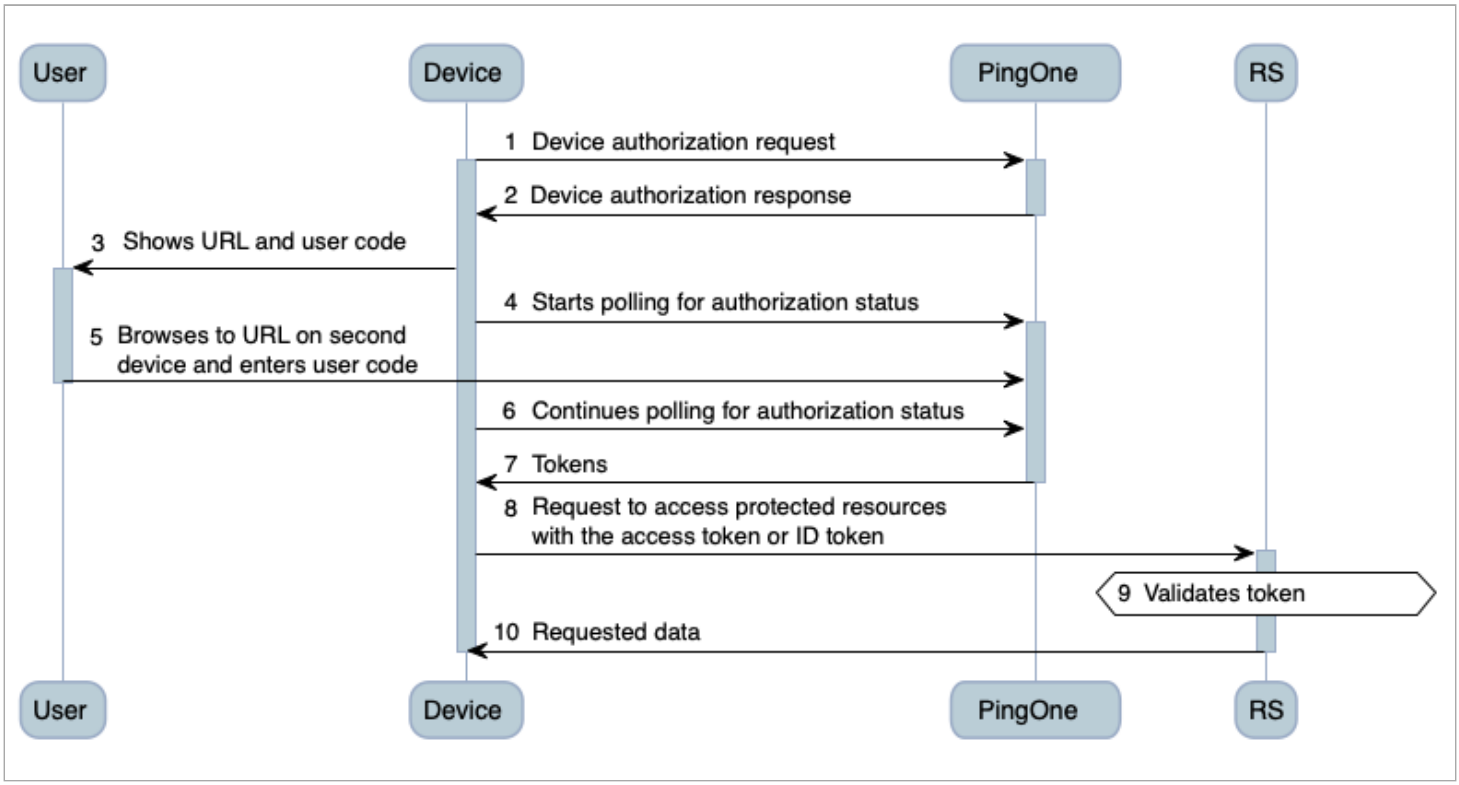
Device authorization

The OAuth device authorization grant type allows a user to grant authorization to the device client using a browser on a second device, typically a smartphone or computer.

This grant type is typically used to access a protected resource through a device that lacks a browser or has limited user input capabilities, such as a smart TV or appliance.

The device authorization grant process takes place between the user, device, PingOne authorization server, and the Resource Server (RS). Learn more about the grant type in the OAuth 2.0 Device Authorization Grant specification.

Copyright © 2025 Ping Identity Corporation



1. The device sends a device authorization request to PingOne, the authorization server at its device authorization endpoint.
2. PingOne returns a device authorization response. Among other parameters, the response contains a device code, a user code, and a verification URI.
3. The device provides the verification URI in a query parameter and instructions to the user, as in the following example:

```
Using a browser on another device, visit:
https://www.example.com
Enter the code:
HVF7-B4KW
```

4. The device starts sending token requests to PingOne to poll whether the user has completed the authorization process.

> **Important**
>
> The token request must include the device authorization grant type, `urn:ietf:params:oauth:grant-type:device_code` , the device code, and the user code.
> For each token request it receives, PingOne returns a response. The payload varies depending on the authorization status.

5. The user completes the authorization process by:
    1. Going to the verification URI on a second device that has a browser, such as a smartphone or a computer.
    2. Fulfilling the authentication requirements.
    3. Entering the user code or confirming a prepopulated user code.

Copyright © 2025 Ping Identity Corporation

4. Approving or denying the scope of permissions requested by the device.

6. The device continues polling PingOne for an authorization status.
7. PingOne validates the user code and provides the device with an access token (and an ID token if applicable) in the token response.

   If the user denies the scope of permissions, PingOne provides the device with a relevant error message in the token response.

8. The device provides the access token to the resource server to access protected resources.
9. The resource server validates the access token.
10. The resource server provides the requested data to the device.

Related links

- Editing an application - Device authorization
- Device custom verification URIs

Sample browser redirect flow

The user turns on their smart TV and starts a streaming app called ShowMe for the first time.

1. The ShowMe app sends a device authorization request to PingOne.
2. PingOne returns a device authorization response to the ShowMe app.

   The device authorization response includes the verification URI, the user code (activation code), and the device code, among other response parameters.

The ShowMe app then:

1. Presents the user code and verification URI through a QR code, a short URL, or both.
2. Prompts the user to scan the QR code to open the verification URI or enter the short URL on a smartphone, tablet, or computer.
3. Starts polling PingOne at the token endpoint with the device code it received from PingOne. PingOne returns an authorization pending message to the ShowMe app in the token responses until the user completes the next step.

The user:

1. Opens the verification URI on their smartphone, tablet, or computer.
2. Completes the authentication process.
3. Confirms the activation code that's shown on the smart TV.
4. Authorizes the request.

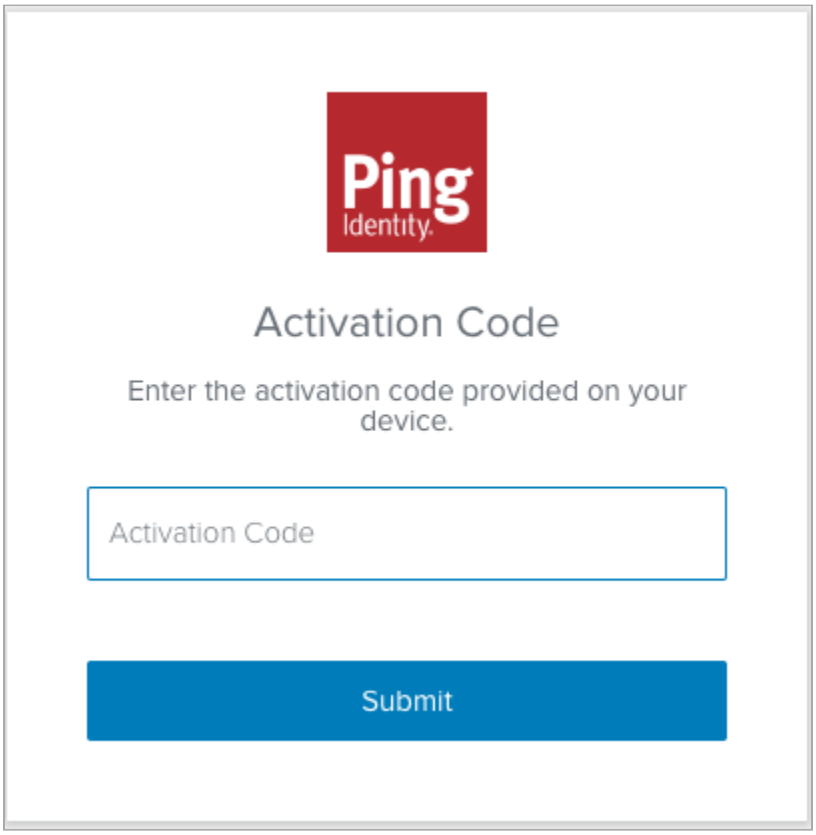
When the user authorizes the request, PingOne returns security tokens to the ShowMe app the next time it sends a token request.

Copyright © 2025 Ping Identity Corporation

Sample user interactions

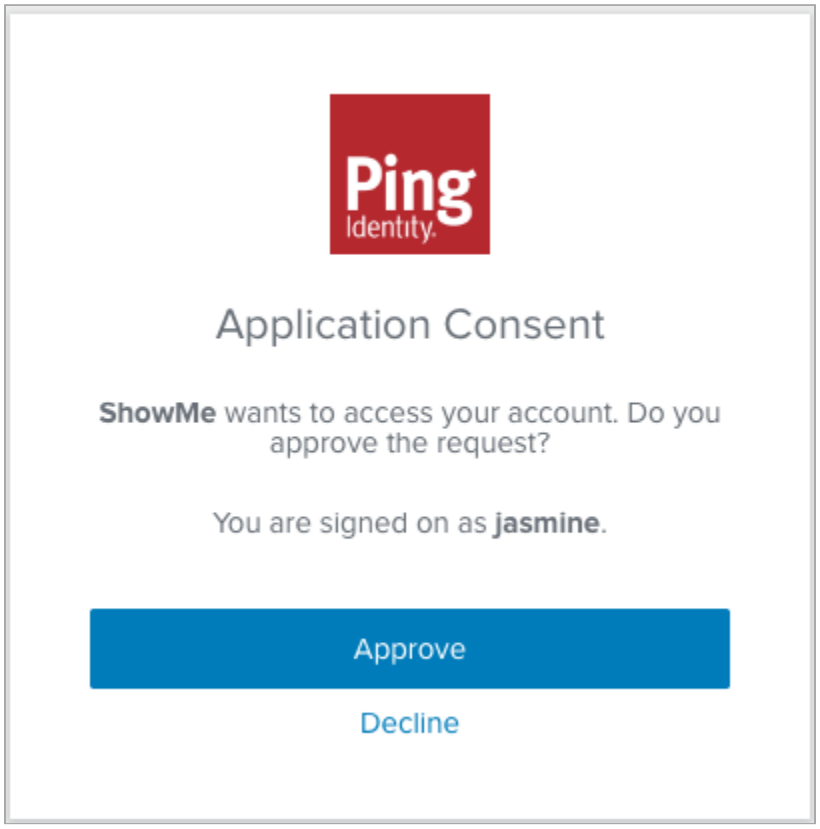
When the user opens the verification URI on the smartphone, tablet, or computer, the short URL redirects the browser to PingOne. PingOne prompts the user to complete the authentication process.

If the user completes the authentication process successfully, PingOne prompts the user to enter the activation code.

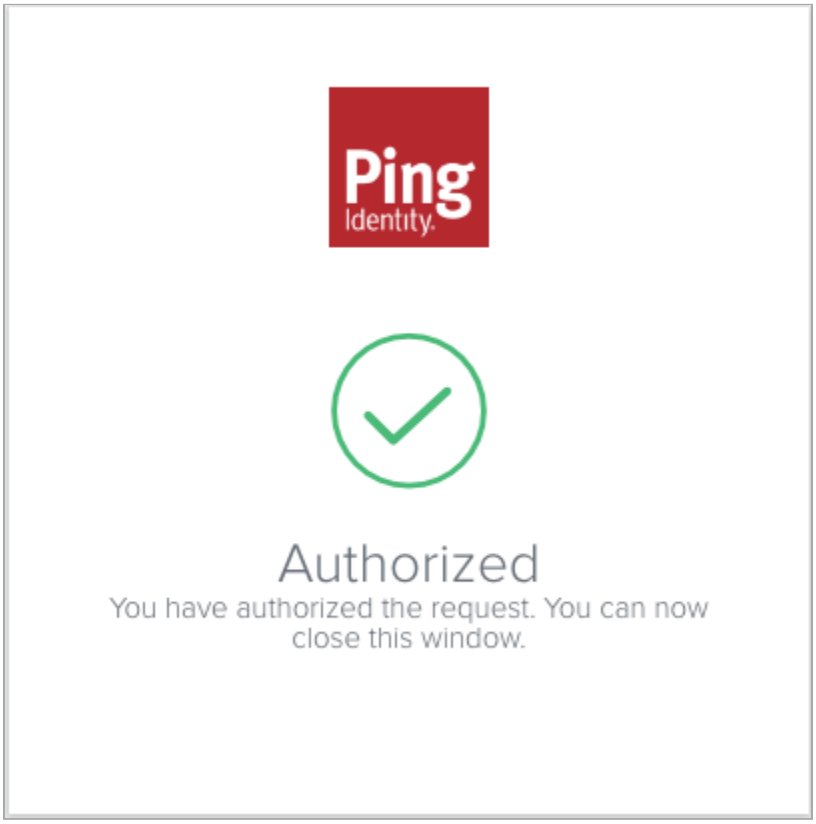


If the user enters the correct code shown by the streaming app on the smart TV, PingOne then prompts the user to authorize the request. The **Application Consent** page shows the name of the application and the authenticated user.

Copyright © 2025 Ping Identity Corporation



If the user approves the request, PingOne shows a message stating that the request is authorized. The user can then close the browser.



Copyright © 2025 Ping Identity Corporation

The next time the ShowMe app polls PingOne at the token endpoint, PingOne returns an access token and ID token if it's requested.

Request Parameter Signature Requirement

In PingOne, you can specify how an application sends the optional `request` parameter in its authorization requests. The application can send authorization requests with or without the `request` parameter, and with or without an optional digital signature.

You can choose a more secure option, a more flexible option, or a balance between the two. For more information, see https://openid.net/specs/openid-connect-core-1_0.html#JWTRequests.

In PingOne, you can choose from the following options when configuring an OIDC-based application:

Default

Allow the application to send authorization requests with or without the request parameter as defined in the OpenID specification. When using the request parameter, the application must include a digital signature. This option provides a balance of security and flexibility.

Require signed request parameters

Require the application to use the request parameter as defined in the OpenID specification and include a digital signature in its authorization requests. This option provides the most security.

Allow unsigned request parameters

Allow the application to send authorization requests with or without the request parameter as defined in the OpenID specification. When using the request parameter, the application has the option to include a digital signature or not. This option provides the most flexibility.

The following table shows a comparison of the different options.

Selection	Authentication request	Signed request	Unsigned request
Default	Yes	Yes	
Require signed request parameters		Yes	
Allow unsigned request parameters	Yes	Yes	Yes

Related links

- Editing an application - OIDC
- Editing an application - Native
- Editing an application - Single page

Copyright © 2025 Ping Identity Corporation

Pushed authorization requests

Applications can use a pushed authorization request (PAR) to securely initiate authorization flows. A PAR allows applications to send their authorization requests directly to PingOne, without going through the browser, which safeguards sensitive data from end-user devices.

With a PAR, an application can push an authorization request payload to PingOne with a direct back-channel request, which is a more secure method of sending sensitive data, such as personally identifiable information, than sending it with a browser on the front channel.

The authorization request payload contains parameters that are `application/x-www-form-urlencoded` formatted. PingOne can accept all parameters that usually make up an authorization request and any additional parameters needed for client authentication. It also can accept signed requests.

> **Note**
>
> - PingOne will not accept PAR requests that are larger than 1 MB.
> - PingOne accepts requests through HTTP POST only.

After PingOne validates the request and saves the payload, it returns the `request_uri` parameter as a reference to the payload. The response also indicates the lifetime of the request URI. The default lifetime is 60 seconds.

The application then uses the front channel to request an authorization code or token, sending the `request_uri` parameter to PingOne. PingOne uses the request URI to look up the request payload and continue the authorization flow. PingOne accepts a particular request URI only once.

For more information about the PAR protocol, see OAuth 2.0 Pushed Authorization Requests on the IETF website.

PAR and application types

PAR secures authorization requests, so PAR applies to the Authorization Code grant type and the Implicit grant type. In PingOne, each application type has its own default grant type. The following table shows PAR availability by application type.

App type	Grant type configured when the application was created	Can the app send a PAR to PingOnePingOne?
OIDC Web App	Authorization Code	Yes
Native	Authorization Code Implicit	Yes
Single-page	Implicit	Yes

Copyright © 2025 Ping Identity Corporation

App type	Grant type configured when the application was created	Can the app send a PAR to PingOnePingOne?
Worker	Client credentials	No. A non-interactive Worker app using the Client credentials grant type sends token requests to the token endpoint only. A non-interactive Worker app does not send authorization requests. However, you can configure a Worker app to use a user-based grant type, such as Authorization Code or Implicit. An interactive app can therefore send authorization requests and PARs to PingOne.

Related links

- Editing an application - OIDC
- Editing an application - Native
- Editing an application - Single page

RequestedAuthnContext

`RequestedAuthnContext` is an optional element in a SAML 2.0 `AuthnRequest`. `AuthnContextClassRef` and `AuthnContextDeclRef` are valid sub-elements in `RequestedAuthnContext`.

Administrators can control whether PingOne should determine the authentication method based on the `RequestedAuthnContext` element. This per-application option, `Policy Selection based on RequestedAuthnContext`, is for SAML 2.0 applications only and is disabled by default.

When the option is disabled, PingOne ignores the `RequestedAuthnContext` element.

When the option is enabled, PingOne evaluates the `RequestedAuthnContext` element as follows:

RequestedAuthnContext with AuthnContextClassRef and AuthnContextDeclRef elements

If both `AuthnContextClassRef` and `AuthnContextDeclRef` are found inside `RequestedAuthnContext`, PingOne returns an error to the application, according to the SAML 2.0 specification.

RequestedAuthnContext is a match

If the application is configured with one or more policies, and if the first `AuthnContextClassRef` element value (or the first `AuthnContextDeclRef` value) is an exact match to one of the configured policies, PingOne invokes that policy.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> - For a PingOne policy, the element value must match the policy name exactly.
> - For a DaVinci policy, the element value must match the policy ID exactly.
> - PingOne ignores the second and any subsequent element values.

RequestedAuthnContext is not a match

If the application is configured with one or more policies, and if the first `AuthnContextClassRef` element value (or the first `AuthnContextDeclRef` value) is not an exact match to one of the configured policies, PingOne returns an error to the application.

RequestedAuthnContext without a policy

If the application is not configured with any policy, and if either `AuthnContextClassRef` or `AuthnContextDeclRef` is provided, because the first `AuthnContextClassRef` element value (or the first `AuthnContextDeclRef` value) is never an exact match to `no policy`, PingOne returns an error to the application.

Related links

- Editing an application - SAML

Cross-origin resource sharing

Cross-origin resource sharing (CORS) allows devices on one domain to access resources on another domain.

You can use this feature if your application references third-party resources, such as cross-origin images, scripts, and stylesheets. CORS defines how a browser and server can interact to determine whether it is safe to allow a cross-origin request. You can specify an exact domain name, a domain name with a wildcard, or an IP address.

For more information, see:

- Editing an application - OIDC
- Editing an application - SAML

Refresh token rotation

PingOne can offer additional security by invalidating access tokens when a refresh token is reused.

Some flows allow applications to obtain refresh tokens. However, there can be some security implications of handling refresh tokens in the browser.

When using a refresh token, confidential clients also have to authenticate. Public clients, such as browser-based applications, do not authenticate during the Refresh Token flow. So in a typical front-end application, refresh tokens issued to front-end web applications are bearer tokens.

In practice, this means that if an attacker manages to steal a refresh token from a front-end application, they can use that token in a Refresh Token flow. To counter such attacks, the OAuth 2.0 specification mandates that browser-based applications apply a security measure known as refresh token rotation.

Copyright © 2025 Ping Identity Corporation

When refresh token rotation is enabled for an application, refresh tokens can be used only once. Every time the client uses a refresh token, the authorization server issues a new access token and a new refresh token. When the application wants to run another Refresh Token flow, it uses the refresh token that was issued most recently.

When an application uses a refresh token, it always receives a new refresh token for next time. As a result, refresh tokens are used only once.

However, if an attacker uses malicious code to steal an application's refresh token, the application won't be aware that the refresh token has been stolen, so it will keep using the refresh token to obtain new access tokens (and refresh tokens). The attacker, who has stolen a refresh token, also wants to get a new access token (and refresh token). As a result, either the attacker or the client application will use a refresh token for the second time.

Refresh token reuse likely indicates that a second party is trying to use a stolen refresh token. In response to this reuse, the authorization server immediately revokes the reused refresh token, along with all descendant tokens.

For more information, see A Critical Analysis of Refresh Token Rotation in Single-page Applications on the Ping Identity blog.

For information about configuring refresh tokens, see Editing an application - OIDC.

Rotating the client secret for an application

For security reasons, you should change an application's client secret on a regular basis. If you think the client secret might have been compromised, you should change it immediately.

After you update a client secret in PingOne, you must ensure that all applications that use the secret are updated. You can retain the previous client secret to give application owners time to update the secret without causing sign-on errors for their users. Use the PingOne admin console or the PingOne API to change a client secret.

> **Note**
>
> Client secrets apply only to OIDC-based applications.

For more information, see:

- Viewing the client secret for an application
- Generating a client secret for an application
- Revoking a client secret for an application
- To use the PingOne API to rotate a client secret, see Application secret in the PingOne Platform API Reference.

Viewing the client secret for an application

You can use the PingOne console to get the client secret for an existing OpenID Connect application without having to make an API call.

About this task

> **Note**
>
> Client secrets apply only to OIDC-based applications.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Applications > Applications** and browse or search for the application.
2. Click the application entry to open the details panel.
3. Click the **Configuration** tab, and locate the **General** section.
4. Locate the **Client Secret** section. Click the **Eye** icon next to **Client Secret** or **Previous Client Secret** to make the secret readable.
5. To copy the client secret, click **Copy to clipboard**.

> **Note**
>
> To rotate a client secret, see Generating a client secret for an application.

Generating a client secret for an application

For security reasons, you should change the client secret for OIDC-based applications on a regular basis. For more information, see Rotating the client secret for an application.

About this task

> **Note**
>
> Client secrets apply only to OIDC-based applications.

Steps

1. Go to **Applications > Applications** and browse or search for the application.
2. Click the application entry to open the details panel.
3. Click the **Configuration** tab, and locate the **Client Secret** section.
4. Click **Generate New Secret**.
5. From **Retain Previous Secret**, select how long to retain the previous client secret:

   Choose from:

   - **Retain for 1 Day**: The previous secret expires 24 hours after the creation of the new secret.
   - **Retain for 7 Days**: The previous secret expires 7 days after the creation of the new secret.
   - **Retain for 30 Days**: The previous secret expires 30 days after the creation of the new secret. 30 days is the maximum retention period.
   - **Retain for custom duration**: Configure the secret to expire after a custom time frame. For example, 14 days.

     > **Note**
     >
     > You cannot set the retention period for longer than 30 days.

Copyright © 2025 Ping Identity Corporation

- **Do Not Retain Previous Secret**: The previous secret expires immediately. Application users might experience sign-on errors until the application is updated to use the new secret.

> **Important**
>
> This setting cannot be changed. If you are not sure how long you should retain the previous client secret, select **Retain for 30 Days**. If you do not need to keep the previous secret for that long, you can revoke it manually before the retention period expires. For more information, see Revoking a client secret for an application.

6. Select **I understand and would like to continue**. Click **Confirm**.

Result

PingOne generates a new client secret for the application.

Revoking a client secret for an application

When you generate a new client secret for an OIDC-based application that has an existing client secret, you have the option to retain the previous secret for a certain period of time. If you no longer need the previous secret before it is set to expire, you can revoke it manually from the application's configuration tab.

About this task

Client secrets apply only to OIDC-based applications.

> **Note**
>
> For security purposes, revoke the previous client secret as soon as you know it is no longer needed.

Steps

1. Go to **Applications > Applications** and browse or search for the application for which you want to revoke the client secret.
2. Click the application entry to open the details panel.
3. Click the **Configuration** tab, and locate the **Previous Client Secret** section.

> **Note**
>
> If the previous client secret already expired or was not retained, this section does not appear.

4. Click **Revoke Previous Client Secret**.

> **Important**
>
> This action cannot be undone.

5. In the confirmation message, select **I understand and would like to continue**. Click **Confirm**.

Result

The previous secret is revoked. Users must have the new client secret to access the application.

Copyright © 2025 Ping Identity Corporation

Including external groups in an application

You can create attribute mappings for groups from external identity providers. If the application is accessible for users from multiple external identity providers, map the group name so that the application can differentiate users by identity provider.

Steps

1. Go to **Applications > Applications**.
2. Browse or search for the application that you want to edit.
3. Click the application entry to open the details panel.
4. Click the **Attribute Mapping** tab, and then click the pencil icon.
5. Click **+ Add**.
6. Add the following attribute mappings:

Application attribute	PingOne mapping
user.memberOfGroupsIDs	Group IDs
user.memberOfGroupsNames	Group Names

7. Click **Save**.

For more information, see Just-in-time provisioning of external groups.

Using the advanced configuration editor

The advanced configuration editor shows a detailed view for attribute mapping, giving you the ability to specify scopes, delivery method, and whether an attribute is required.

Steps

1. Go to **Applications > Applications**.
2. Locate the application you want to view. You can browse or search for applications, or narrow your search to a particular application type
3. Click the application entry to open the details panel.
4. Click the **Attribute mappings** tab and then click the pencil icon to edit.
5. Click the **Advanced configuration** button.
6. Do one or more of the following:
   - To edit an existing attribute, select the **OIDC attribute** and the desired PingOne mapping.
   - To add an attribute, click the **+ Add** button. Enter an application attribute and the desired PingOne mapping. Click the gears icon to use advanced expressions. See Using the expression builder.

Copyright © 2025 Ping Identity Corporation

- To define a scope for the attribute, select a scope from the **Scope** list.
- To define how the attribute is delivered to the application, select **UserInfo** or **ID Token**.
- To define an attribute as required, select the **Required** check box.
- To delete an attribute, click the trash can icon for the appropriate attribute.

7. Click **Save**.

Configuring roles for a worker application

Worker applications have no roles by default. After the application is created, you can add or remove roles as needed, up to the level of your roles as a user. That is, you cannot assign roles that you do not have, or do not have permission to assign.

About this task

> **Note**
>
> If you create a Worker app through the PingOne API, the app inherits your roles by default. Use the `assignActorRoles` parameter to create a Worker app with minimal roles. Learn more in Create Application - OIDC - Worker App in the PingOne Platform API Reference.

Steps

1. Go to **Applications > Applications** and browse or search for the application that you want to edit.

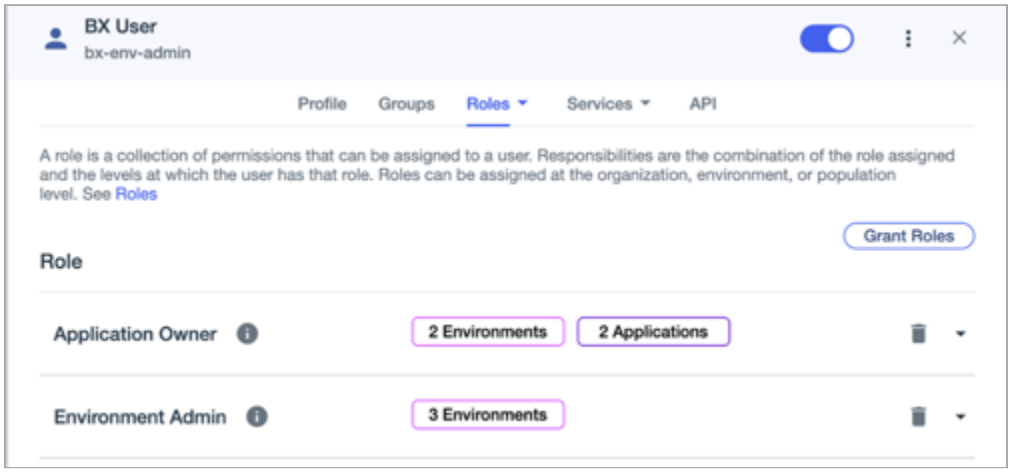
   > **Note**
   >
   > You can apply administrator roles to Worker applications only. To view the specific permissions for each role, go to **Directory → Administrator Roles**. Click a role to see its details. Learn more in Administrator Roles.

2. Click the application entry to open the details panel.
3. Click the **Roles** > **Administrator Roles** tab.

   If roles are assigned, they're listed here with information about where those roles apply. For example, in the following image, **BX User** has the **Application Owner** role in two environments. Because the role is assigned at the environment level, they have the role over all of the applications in those environments. In a third environment, they have the role over only two applications. They also have the **Environment Admin** role, and they have that role in three environments.

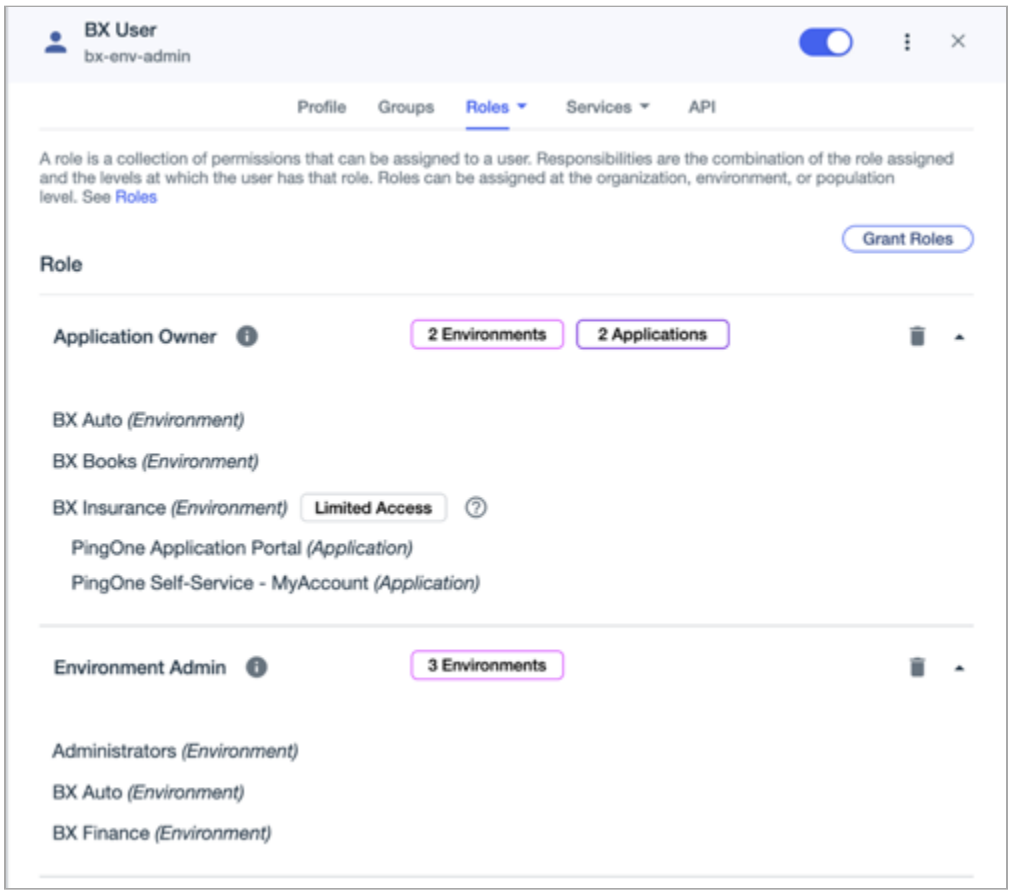
   > **Note**
   >
   > You can assign administrator roles to users, groups, applications, or PingFederate gateway integrations.

Copyright © 2025 Ping Identity Corporation



Tip

Click the **Info** icon to view the permissions associated with the role. Click the down arrow on the right to view the list of environments or populations for which the role is assigned.



4. Click **Grant Roles**.

   The **Available Responsibilities** tab lists the roles that you are allowed to assign and the environments for which you are allowed to assign them. A responsibility is the combination of the role assignment and the level, or scope, at which the role is applied. Depending on the role, it could be assigned at the organization, environment, population, or application level.

   The **Granted Responsibilities** tab lists any roles that are currently assigned.

Copyright © 2025 Ping Identity Corporation

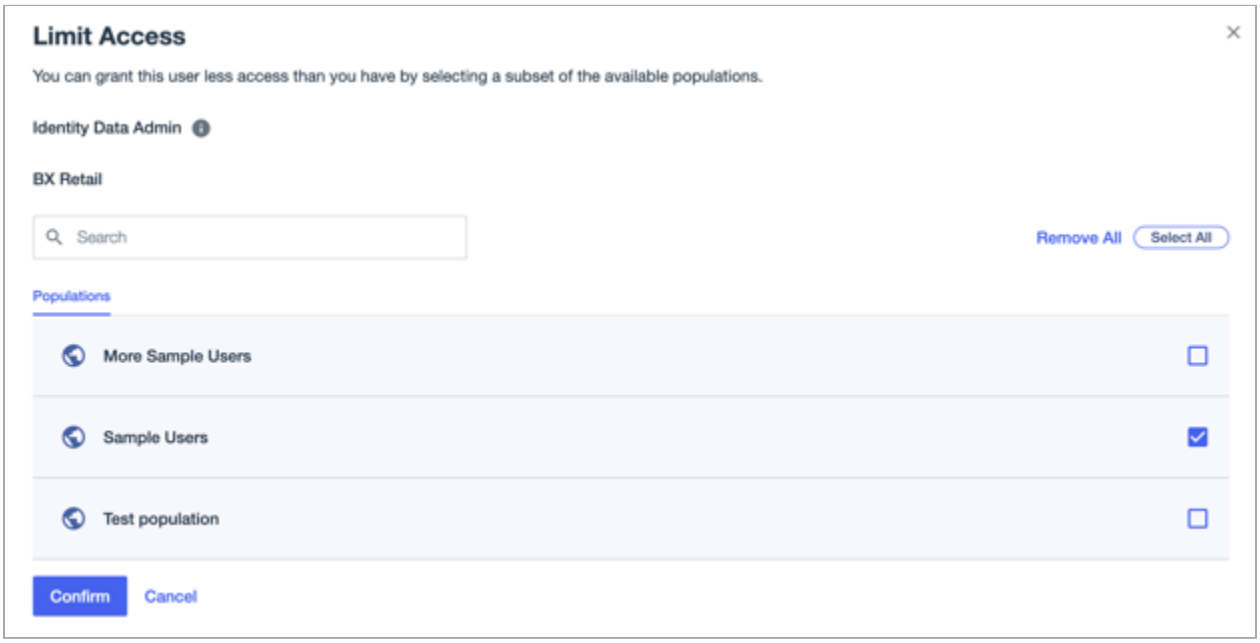
5. On the **Available Responsibilities** tab, click the role that you want to assign or change and perform any combination of the following:

    1. To assign the role, select the checkboxes next to the applicable environments.

    > **Tip**
    >
    > Click **Select All** or **Remove All** to select or clear all available responsibilities.

    2. To remove a role assignment, clear the checkboxes next to the applicable environments.

    3. To grant this access for only a portion of the environment, click the **Reduce Access** icon ( ), select a subset of the available applications or populations on the **Limit Access** page, and click **Confirm**.



    > **Note**
    >
    > You can grant only roles that are assigned to you or that confer the permissions needed to assign that role to others. For example, if you do not have the Environment Admin role, you cannot assign the Environment Admin role to others (and that role will not be listed under **Available Responsibilities**). However, if you have the Identity Data Admin role, you can assign either the Identity Data Admin role or the Identity Data Read Only role to others.
    > Learn more about the permissions associated with each role in Roles.

6. Click **Save**.

Result

The role assignments you selected are listed on the **Granted Responsibilities** tab.

Viewing scopes for an application

View scopes per application.

Copyright © 2025 Ping Identity Corporation

About this task

- OAuth scopes control what data is shared with third party applications. For example, you can accept or reject sharing an end user's profile or email address with an application.
- PingOne API Self-management scopes are applicable to users only. Self-management scopes specified identify the resources that end users can access to perform self-management actions. See also Self Service and PingOne API self-management scopes.

Steps

1. Go to **Applications > Applications**.

   You can also search for applications, or narrow your search to a particular application type.

2. Locate the application you want to view, and then click the application entry to open the details panel.
3. Click the **Resources** tab.

Result

The Allowed scopes list shows the application permissions. To edit the scopes, see Editing scopes for an application.

Editing scopes for an application

Edit scopes per application.

About this task

- OAuth scopes control what data is shared with third party applications. For example, you can accept or reject sharing an end user's profile or email address with an application.
- PingOne API Self-management scopes are applicable to users only. Self-management scopes specified identify the resources that end users can access to perform self-management actions. See also Self Service and PingOne API self-management scopes.

Steps

1. Go to **Applications > Applications**.

   You can also search for applications, or narrow your search to a particular application type.

2. Locate the application you want to view, and then click the application entry to open the details panel.
3. Click the **Resources** tab and then click the pencil icon.
4. Select the OAuth scopes for the application. Click and drag scopes in the left column to add them to the **Allowed Scopes** column on the right.
5. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Customizing access token lifetime

When defining a custom resource in PingOne, you can customize the access token lifetime as needed and add relevant scopes. The access token lifetime defaults to 1 hour.

About this task

When defining an OpenID Connect (OIDC)-based application, you can specify the resources that the application can request access to by adding the relevant scopes to the application. When an application requests an access token from PingOne so that it can access a custom resource, the application sends the required scopes in the request. The lifetime of the access token is determined by the access token lifetime set in that custom resource.

Steps

1. Go to **Applications > Resources**.
2. Click the **+** icon.
3. For **Create resource profile**, enter the following information:
    - **Resource name**: A unique identifier for the resource.
    - **Audience** (optional): The intended audience for the resource. If you don't provide a value, PingOne will default to the resource name.
    - **Description** (optional): A brief characterization of the resource.
    - **Access token time to live**: The maximum time that the access token will be valid for use in the application, in seconds.
4. Click **Next**.
5. For **Attributes**, map resource attributes to user attributes in PingOne.
    1. Enter a resource attribute and then select the corresponding PingOne attribute from the list.
    2. To add an attribute, click the **+ Add** button.
6. Click **Next**.
7. For **Scopes**, configure the appropriate scopes for the resource. Each resource can have one or more scopes. To add a scope, click **+ Add scope**. Enter the following:
    - **Scope name**: The name of the scope to be used for this resource. Scopes are defined by the resource server.
    - **Description** (optional): A brief description of the scope.
8. Click **Save**.
9. To add the scope to an application, go to **Applications > Applications**, and browse or search for the appropriate application.
10. On the **Resources** tab, click the **Pencil** icon.
11. Locate the scope that you previously added to your resource and click the checkbox next to the scope.
12. Click **Save**.

Copyright © 2025 Ping Identity Corporation

SAML 2.0 single logout

PingOne supports SAML 2.0 single logout (SLO), which enables users to sign off from multiple participants in a single action. Participants are the identity provider (IdP) and the service provider (SP), and are referred to as partners of each other. SLO is most common in workforce deployments, in which employees can sign off from multiple applications in a single operation.

This section describes the benefits, behaviors, and limitations of SAML 2.0 SLO.

> **Note**
>
> - SAML applications and IdPs can trigger SLO only if:
> - An SLO endpoint is configured.
> - The user interacts with the application or IdP within the configured SLO window.
> Learn more about the SLO settings in Editing an application - SAML.
> - Signing off from a SAML application or IdP with the conditions described above doesn't trigger PingOne to send logout requests to OpenID Connect (OIDC) or Microsoft 365 applications the user has signed on to in the same PingOne user session.
> - Signing off from an OIDC or Microsoft application doesn't trigger SAML 2.0 SLO.
> - The default sign-off method for the PingOne application portal and PingOne Self-Service - MyAccount is OIDC logout. You can change the sign-off method to SAML 2.0 SLO as needed. Learn more in Configuring the application portal and Configuring the self-service portal.

SLO scenarios

You can use SAML 2.0 SLO in several different scenarios:

SP-initiated SLO

For SP-initiated SLO, PingOne is the IdP, and the partner is the SP with a SAML application in PingOne. If the partner supports SP-initiated SLO, an application can send logout requests to PingOne.

IdP-initiated SLO

For IdP-initiated SLO, the partner is the IdP, and PingOne is the SP with an external IdP connection to the partner. If the partner supports IdP-initiated SLO, the IdP can send logout requests to PingOne.

PingOne-initiated SLO

For PingOne-initiated SLO, if PingOne is the IdP, and if the SP supports IdP-initiated SLO, PingOne can send logout requests to the SP. If PingOne is the service SP, and the IdP supports SP-initiated SLO, PingOne can also send logout requests to the SP.

To start a PingOne-initiated SLO request, the browser sends an HTTP GET request to either of the following URLs:

- https://auth.pingone.<region>/<envID>/saml20/startslo
- https://<customDomain>/saml20/startslo (Only if a custom domain has been configured. Learn more in Setting up a custom domain.)

Copyright © 2025 Ping Identity Corporation

SLO traffic

SLO messages (requests and responses) are transported through the browser. PingOne supports two SLO bindings that define how messages are transported:

- POST (default)
- Redirect

SLO behavior

Generally speaking, when a participant initiates a SAML 2.0 SLO request, based on the user's action, requests and responses are exchanged among all participating partners. The goal is to sign the user off from all partners.

When PingOne is a participant, and it receives an SLO request, if PingOne is aware of other participants, PingOne sends an SLO request to each participant in a sequence after each successful SLO response PingOne receives. When no participants remain, PingOne honors the original SLO request and returns a successful SLO response to the participant that originally sent the request.

When PingOne is the initiator, the SLO process works similarly. However, the SLO should finish with PingOne when it receives the last successful SLO response.

The chain succeeds when each participant completes its share of the SLO process. The chain breaks when one participant fails to complete the SLO request.

When SLO fails, the participant is supposed to return the browser to the initiator with an error message. If the participant is unable to do so, the participant would typically show a message directly to the user. In either case, the user can close the browser and optionally clear the browsing data, such as cache and cookies, to terminate sessions from all participants.

Applications and SLO

If the SP supports SLO, enter the SLO endpoint in the SAML application. This is the endpoint at the SP where it receives SLO requests. If the SP wants to receive SLO responses at a different endpoint, enter that as the SLO response endpoint. The SLO binding defaults to POST and also supports Redirect.

Because SLO can time out if one participant fails to send an SLO message, you can configure how long PingOne should send or receive SLO messages to and from an application since the initial request. This per-application flexibility allows you to fine-tune SLO experiences for your users.

External IdPs and SLO

SAML 2.0 external IdPs work the same way as SAML 2.0 applications. If the IdP supports SLO, enter the SLO endpoint in the external IdP configuration. This is the endpoint at the IdP where it receives SLO requests. If the IdP wants to receive SLO responses at a different endpoint, enter that as the SLO response endpoint. The SLO binding defaults to POST and also supports Redirect.

Because SLO can time out if one participant fails to send an SLO message, you can configure how long PingOne should send or receive SLO messages to and from a SAML 2.0 external IdP since the initial request. This per-external IdP flexibility allows you to fine-tune SLO experiences for your users.

Related links

- Adding an identity provider - SAML

Copyright © 2025 Ping Identity Corporation

- Editing an application - SAML

PKCE enforcement

You can use PKCE (Proof Key for Code Exchange) to secure applications, especially native mobile applications, that might otherwise be susceptible to an authorization code interception attack.

For more information about PKCE, see RFC7636.

> **Note**
>
> PKCE enforcement is available for Authorization Code grants only and applies only to applications that use such grants.

PingOne includes the following options for PKCE enforcement:

Optional

PKCE `code_challenge` is optional, and any code challenge method is acceptable.

Although permitted, avoid using the plain challenge method because the code challenge could be observed by an attacker on the device or in the http request.

Required

PKCE `code_challenge` is required, but any code challenge method is acceptable.

Although permitted, avoid using the plain challenge method because the code challenge could be observed by an attacker on the device or in the http request.

S256_required

PKCE `code_challenge` must use SHA 256 encoding for the code challenge method.

The SHA 256 method protects against eavesdroppers observing or intercepting the `code_challenge` because the challenge cannot be used without the code verifier value.

For more information about SHA 256 base encoding, see section 4.2 of RFC7636.

To enable PKCE enforcement in your application, see Editing an application - Native.

Editing custom ID token mappings

You can customize the content of an OpenID Connect (OIDC) ID token by adding custom attributes and their values.

The claim defined by the mapping is returned in the ID token, regardless of the scopes specified in the authorization request. For example, if you want to include a user's account ID in ID tokens associated with the specified OIDC application, you can map the user's account ID to the `accountId` PingOne user attribute.

You can map PingOne user attributes or static attributes to custom attributes in the application you are adding.

Copyright © 2025 Ping Identity Corporation

Mapping PingOne attributes

You can map PingOne attributes to custom attributes in your application. For example, you could map `account ID` in PingOne to `User ID` in the application.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the application for which you want to map attributes.

   You can also add an application. Learn more in Adding an application.

2. Click the application entry to open the details panel for the application.
3. On the **Attribute Mappings** tab, click the **Pencil** icon.
4. Click **+ Add**.
5. Enter the following:
   - **Attributes**: Enter the custom application attribute, such as `account ID`.
   - **PingOne Mappings**: Select an attribute in the list, such as `User ID`. You can browse or search for attributes.
6. If the value is a required attribute for the application, select the **Required** checkbox.

   > **Note**
   >
   > If you request an ID token with a claim that is marked as required but doesn't have a value, PingOne will return an error. If the value is not marked as required and doesn't have a value, the property will be omitted from the token.

7. To use the expression builder, click the **Gear** icon. Learn more in Using the expression builder.
8. Click **Save**.

Mapping static attributes

Some service providers require global values for all users to be passed in the assertion. You can use PingOne to map these keys to fixed values.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the application for which you want to map attributes.

   You can also add an application. Learn more in Adding an application.

2. Click the application entry to open the details panel for the application.
3. On the **Attribute Mappings** tab, click the **Pencil** icon.
4. Click **+ Add**.
5. Enter the following:
   - **Attributes**: Enter the custom application attribute, such as `Version`.

Copyright © 2025 Ping Identity Corporation

- **PingOne Mappings**: Enter a value, such as `2.0`.

6. To use the expression builder, click the **Gear** icon. Learn more in Using the expression builder.
7. Click **Save**.

Getting an access token

You can use the PingOne console to get the access token for an existing application. This allows you to get an access token without having to make an API call.

About this task

To get an access token, the following must be true:

- The application is enabled.
- The application has a grant type of `Client credentials`.
- The application has a token endpoint authentication method of `CLIENT_SECRET_BASIC` or `CLIENT_SECRET_POST`.
- The user has access to the client secret.
- For a worker application, the application has the appropriate role assignments. For non-worker applications, the application has the appropriate scopes.

Steps

1. Go to **Applications** > **Applications**.
2. Locate the application for which you want to get the access token. You can browse or search for applications.
3. Click the application entry to open the details panel.
4. Click the **Configuration** tab, and then click the pencil icon.
5. Click **Get Access Token**.

   On the **Access Token** window, you can select and copy the JSON, or click **Copy Access Token** to copy only the access token to your local clipboard.

Downloading IdP metadata for an application

PingOne generates a metadata file that contains configuration details for single sign-on (SSO). You can use the identity provider (IdP) metadata to share configuration information between the IdP and the service provider (SP). The metadata includes profile and binding support, connection endpoints, and certificate information.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the application for which you want to download the IdP metadata.
2. Click the application entry to open the details panel.

   Result:

Copyright © 2025 Ping Identity Corporation

The application details panel opens to the **Overview** tab.

3. For SAML applications with **Allow Virtual Server IDs** enabled, select a virtual server ID in the **Display Virtual Server ID** list to obtain the relevant metadata. Learn more in Editing an application - SAML.
4. Click **Download Metadata**.

Result

The file is saved to your local device storage.

> **Note**
>
> You can also download metadata for SAML IdPs. Learn more in Downloading metadata for SAML IdPs.

Response types

The response type determines whether an access token, an authorization code, or a JSON Web Token is returned by PingOne . The following OAuth 2.0 response types are supported by PingOne:

code

Returns an authorization code. The authorization code returned by the request is exchanged for an access token to complete the authorization.

token

Returns an access token. If the grant type is `implicit` or `client_credentials`, you can configure PingOne to return an access token.

id_token

Returns a JSON Web Token (JWT). If the grant type is `implicit`, you can configure PingOne to return a JWT containing a set of claims that represent the authentication state of a user.

Response mode values

The response mode determines how PingOne returns result parameters.

Specify the response mode using the `response_mode` request parameter. If `response_mode` is not present in a request, the default response mode is used.

PingOne supports a proprietary redirectless OAuth mode: pi.flow. This allows applications to request OAuth/OIDC tokens from PingOne and host the authentication UI in the applications without redirecting the user's browser to PingOne.

PingOne can respond back to the application's authorization request in one of four modes: `query`, `fragment`, `form_post`, and `pi.flow`.

query

Authorization Response parameters are encoded in the query string added to the `redirect_uri` when redirecting back to the application.

Copyright © 2025 Ping Identity Corporation

fragment

Authorization Response parameters are encoded in the fragment added to the `redirect_uri` when redirecting back to the application.

form_post

Authorization Response parameters are encoded as HTML form values that are auto-submitted in the browser, and are transmitted through HTTP POST to the application, with the result parameters being encoded in the body using the `application/x-www-form-urlencoded` format.

pi.flow

Specifies a redirectless flow with a flow object in the response. This allows applications to request OAuth/OIDC tokens from PingOne and host the authentication UI in the applications without redirecting the user's browser to PingOne. When authentication is complete, the app receives the auth code, access token, or ID token in a JSON response instead of a redirect.

Grant types

OAuth 2.0 and OpenID Connect define the authorization grant types by which a client application obtains an authorization grant in the form of an access token.

PingOne supports the following grant types:

Authorization code

This grant type is used by web applications. The authorization request generates an authorization code that is exchanged for an access token. An authorization code expires after 10 minutes.

Implicit

This grant type is intended for use by mobile applications or client-side web applications with no server-side component. The implicit grant type is for applications that cannot guarantee the confidentiality of the client secret.

Client credentials

This grant type is made directly to the token endpoint and is used to request an access token for either:

- Resources owned by the application rather than a user.
- Resources belonging to multiple end users.

Device authorization

This grant type allows a user to grant authorization to the device client using a browser on a second device, such as a smartphone or computer. The device authorization grant type is typically used to access a protected resource through a device that lacks a browser or has limited user input capabilities, such as a smart TV or appliance.

Copyright © 2025 Ping Identity Corporation

Refresh token

This grant type is used by applications to exchange a refresh token for an expired access token. It gives applications the ability to acquire a valid access token without additional user interaction. To obtain a refresh token along with an access token, the client must be configured with the `refresh_token` grant type and either the `authorization_code` grant type or the `device_authorization` grant type.

Token endpoint authentication methods

The token endpoint authentication method determines how PingOne authenticates applications at various endpoints, such as the token, token introspection, token revocation, and pushed authorization request endpoints. Learn more about token endpoint authentication methods in Client Authentication in the OpenID Connect (OIDC) specification.

PingOne supports the following token endpoint authentication methods:

CLIENT_SECRET_POST

Include the client credentials in the HTTP request body.

CLIENT_SECRET_BASIC

Include the client credentials using the HTTP Basic authentication scheme.

CLIENT_SECRET_JWT

Create a digitally signed JSON Web Token (JWT) using HS256, HS384, or HS512.

You can use expressions to retrieve information from the authentication JWT for token fulfillment. Learn more about using the expression builder in PingOne Expression Language and Variables.

PRIVATE_KEY_JWT

Create a digitally signed JWT using RS256, RS384, or RS512 with a private key owned by the application or resource server.

You can use expressions to retrieve information from the authentication JWT for token fulfillment. Learn more about using the expression builder in PingOne Expression Language and Variables.

Related links

- Grant types

Editing an application for the Microsoft Entra ID external authentication method

To connect PingOne as the external authentication provider for multi-factor authentication (MFA) in Entra ID, you must configure an OpenID Connect (OIDC) application to handle authentication requests from Microsoft Entra ID. When a user attempts to access an application configured in Microsoft Entra, the user authenticates first with Microsoft Entra ID and then is redirected to a third-party MFA provider, such as PingOne, for second-factor authentication.

You must also add a Microsoft identity provider (IdP). Learn more about configuring Entra ID as the IdP in Setting up PingOne SSO and PingID as the external MFA provider for Microsoft Entra ID.

Copyright © 2025 Ping Identity Corporation

Application catalog

The Application catalog contains popular applications that service providers have made available through PingOne.

After selecting an application from the catalog, follow the configuration instructions to add the application and make it available to your users.

Adding an application from the application catalog

Use the PingOne application catalog to configure single sign-on (SSO) for popular applications.

Steps

1. In PingOne admin console, go to **Applications** > **Application Catalog** and browse or search for applications.
2. Click the application entry to open the details panel.
3. For **Quick Setup**, enter the following information:
   - To change the application name, enter a new name in the **Name** field.

     > **Note**
     > The application name must be unique, and cannot be the same as any applications configured at **Applications** > **Applications**.

   - To change the icon for the application, click the icon image and select a new file.

     > **Note**
     > Some applications require additional configuration inputs, such as **AccountID**, **Domain Name**, or **Vanity URL**.

4. Click **Next**.
5. For **Map Attributes**, set up user attribute mapping from the application to PingOne.

   > **Note**
   > The required attributes for each application are pre-populated. In most cases, you won't need to alter the mappings.
   > Required attributes must be mapped before you can proceed to the next configuration tab.

   Choose from:

   - To change the attribute mapping, enter or select a new attribute in the **PingOne Mappings** list.
   - To designate the attribute as required, select the **Required** checkbox.
   - To use the expression builder or map the attribute to a literal string value, click the **Gear** icon. Learn more in Using the expression builder.
   - To delete an attribute mapping, click the **Delete** icon.

Copyright © 2025 Ping Identity Corporation

6. (Optional) To add a new attribute:
    1. Click **+ Add**.
    2. In the application field for the new attribute, enter the name of the attribute as it appears in the application.
    3. In the **PingOne Mappings** field for the new attribute, enter or select the PingOne attribute to map to.

       To use the expression builder or map the attribute to a literal string value, click the **Gear** icon. Learn more in Using the expression builder.
7. When you're finished mapping attributes, click **Next**.
8. For **Select Groups**, specify the groups that you want to have access to the application.

   > **Note**
   > By default, all users have access to the application. Assigning groups restricts application access to only those groups.

   Learn more in Groups.
9. Click **Save**.

   Result:

   The application is now configured for PingOne. There may be additional configuration necessary on the application side.
10. To see applications that have already been configured, click the **Configured** tab.
11. On the **Overview** tab, download or copy information required by the application to complete the SSO configuration.

    This information includes the following PingOne details:

    - Metadata
    - Signing certificate
    - **Issuer ID** URL
    - **Initiate Single Sign-on URL**
    - **Single Signon Service** URL
    - **IdP Metadata URL**

Next steps

After you configure the application, you can manage it from **Applications > Applications**.

To configure advanced application settings, go to the **Configuration** tab for the application to see all application settings, including but are not limited to:

- **ACS URLs**: The Assertion Consumer Service URLs.
- **Signing key**: The certificate that confirms that requests, responses, and assertions actually came from the application.
- **Entity ID**: The service provider (SP) entity ID used to look up the application.

Copyright © 2025 Ping Identity Corporation

- **SLO endpoint**: The SAML single logout endpoint URL.
- **Subject NameID format**: A string that specifies the format of the `Subject NameID` attribute in the SAML assertion.

Learn more about advanced settings in Editing an application.

Adding Microsoft 365 to the PingOne application portal

Use the application catalog to add Microsoft 365 to your application portal and connect the application to a Microsoft Entra ID domain.

PingOne supports the Microsoft 365 passive and active profiles for single sign-on (SSO):

Passive profile

Passive profile enables web browser SSO, where Microsoft 365 redirects the user's browser to PingOne for authentication, and the user provides their PingOne credentials.

If the PingOne environment is configured with an LDAP gateway, PingOne can validate the credentials against an on-premise LDAP server, such as Microsoft Active Directory (AD). If the LDAP gateway is configured with Kerberos authentication, the user can sign on seamlessly to Microsoft 365 using the Kerberos protocol.

Active profile

Active profile allows an application to collect the user's credentials and initiates an exchange with PingOne for a security token. The exchange uses the WS-Trust protocol to allow the user to access Microsoft 365.

Before you begin

You must have a Microsoft Azure account with a custom domain configured in Microsoft Entra ID as either of the following:

- Managed domain, where Entra ID is the identity provider (IdP) and manages authentication. In step 12, you'll change the domain to a federated domain and set up PingOne as the federated IdP for this domain.
- Federated domain, where Entra ID redirects users to a federated IdP for authentication. In step 12, you'll update Entra ID to use PingOne as the federated IdP for this domain.

Learn more about domains in Managing custom domain names in the Entra ID documentation.

> **Note**
>
> Each Microsoft 365 custom domain requires a unique `IssuerURI` value. To set up PingOne as the federated IdP for multiple domains, you must add a Microsoft 365 application for each domain.

Steps

1. In the PingOne admin console, go to **Applications** > **Application Catalog**.
2. In the **Search for applications** bar, enter `Microsoft 365`.
3. Click the **Microsoft 365** entry to open the details panel.

Copyright © 2025 Ping Identity Corporation

4. On the **Quick Setup** page, review the following:
   - **Name** (optional): Enter a new name to replace the default application name.
   - **Icon** (optional): Select a new image to replace the default application icon.
   - **Domain Name**: Enter the `<Custom Domain>` value from your Entra ID account. You can find your <Custom Domain> in the Microsoft Entra admin center by going to **Identity > Settings > Domain Names**.
   - **Subject NameIdentifier Format**: Select the value in the list to use for the `Subject NameIdentifier` attribute in the WS-Federation security token.

     Possible values are `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress` (default) or `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`.

     > **Note**
     > If the application is already configured, click **View in Applications list** to view the full configuration.

5. Click **Next**.
6. On the **Map Attributes** page, select the PingOne attributes to map to the required `ImmutableID`, `Subject`, and `UPN` Microsoft 365 attributes.

   > **Note**
   > **ImmutableID** uniquely identifies a user in Entra ID. You can find the **ImmutableID** value by running the **`Get-MsolUser`** command in PowerShell after you configure federation with Entra ID. Learn more about Get-MsolUser in the Microsoft documentation.
   > For **Subject**, the mapping attribute defaults to **Email Address** but can be configured to a different value.
   > For **UPN**, use an email address with a domain name that matches the domain name registered with Microsoft 365.

   - If your user identities are stored in the PingOne Directory, use the default mapping of `ImmutableID` to `ExternalID`. `ExternalID` is the user's **User ID** in PingOne.
   - If the Microsoft 365 users are migrated into PingOne from Entra ID through the LDAP gateway, and the source of the `ExternalID` is `objectGUID` or `ms-DS-ConsistencyGuid`, add an expression to the mapping configuration:
     1. Locate the `ImmutableID` mapping.
     2. Click the **Gear** icon to open the **Advanced Expression** modal.
     3. Enter the following expression:

        ```
        #string.uuidAsBase64Guid(user.externalId,null)
        ```

        Learn more in Using ms-DS-ConsistencyGuid as sourceAnchor in the Entra ID documentation.
     4. Click **Save**.

Copyright © 2025 Ping Identity Corporation

- You can create a custom PingOne user attribute instead of using `ExternalID`. Map `objectGUID` or `ms-DS-ConsistencyGuid` as the attribute source:

  1. Locate the `ImmutableID` mapping.
  2. Click the **Gear** icon to open the **Advanced Expression** modal.
  3. Enter the following expression:

     ```
     #string.uuidAsBase64Guid(user.customAttrName,null)
     ```

     where `customAttrName` represents the custom PingOne user attribute. You can also replace `null` with a custom value, such as an error.
  4. Click **Save**.

7. Click **Next**.
8. On the **Select Groups** page, click the name of the user groups that you want to have access to the application. You can browse or search for groups. Click the **Added** tab to see the groups that currently have access to the application.

   > **Note**
   >
   > By default, all users have access to the application. Assigning groups restricts application access to those groups only.

9. Click **Save**.
10. Click the **View in Applications list** link.
11. On the **Overview** tab, determine which cmdlets to use:

    Choose from:

    - If you've upgraded to Graph PowerShell, locate the **Microsoft Graph PowerShell cmdlets**.
    - If you haven't upgraded to Graph PowerShell, locate the **MSOnline cmdlets**.

12. Execute PowerShell cmdlets to configure PingOne as the federated IdP:

    Choose from:

    - **Entra managed domain**: Set up identity federation settings for the first time to use PingOne as the IdP.

      1. Locate either **Microsoft Graph PowerShell cmdlets** or **MSOnline cmdlets**, depending on your configuration.
      2. Click the **Copy to clipboard** icon for the appropriate section.

    - **Entra federated domain**: Update existing identity federation settings to use PingOne as the IdP.

      1. Locate either **Microsoft Graph PowerShell cmdlets** or **MSOnline cmdlets**, depending on your configuration.
      2. Click the **Copy to clipboard** icon for the appropriate section.

Copyright © 2025 Ping Identity Corporation

> **Tip**
>
> You might have to scroll to the right to see the **Copy to clipboard** icon.
> You might have to collapse the **Microsoft Graph PowerShell cmdlets** entry to see the **MSOnline cmdlets** entry.

13. Open Windows PowerShell.
14. In PowerShell, paste the copied commands and run them.

    These commands update the domain authentication in Entra ID to SSO. Learn more about the Microsoft cmdlets that are used in PingOne in the following topics in the Microsoft documentation:

    - Connect-MgGraph
    - New-MgDomainFederationConfiguration
    - Update-MgDomainFederationConfiguration
    - Connect-MsolService
    - Set-MsolDomainAuthentication
    - Set-MsolDomainFederationSettings

Next steps

- You can optionally enable Kerberos authentication for Microsoft 365 applications. Learn more in Enabling Kerberos authentication.
- Add an MFA claim in the Microsoft 365 application for PingOne to communicate to Entra ID that PingOne will handle MFA. Learn more in Configuring an authentication claim for the Microsoft 365 application.
- After you configure the application, you can manage it from **Applications** > **Applications**. Learn more in Editing an application.

Enabling Kerberos authentication

You can enable Kerberos authentication to provide end-users with a seamless sign-on experience if the Microsoft 365 users are migrated into PingOne from Active Directory (AD) through the LDAP Gateway and if your Microsoft 365 applications support the Active Profile sign in option.

Before you begin

You must have:

- An LDAP Gateway configuration with Kerberos authentication enabled
- At least one User Type configured
- A configured SPN in AD
- An LDAP Gateway deployed in the network where it can reach the targeted domain controllers

Copyright © 2025 Ping Identity Corporation

Steps

1. In PingOne, go to **Applications > Applications**.
2. Browse or search for the Microsoft 365 application and click the **Microsoft 365** entry to open the details panel.
3. Click **Enable Advanced Configuration** and click **Enable** when prompted.
4. In the **Configuration** tab, click the **Pencil** icon.
5. Select the **Enable Kerberos Authentication** check box.
6. Click **+Add Gateway User Type**.
7. Select a **Gateway** and a **User Type**.
8. Click **Save**.

Configuring an authentication claim for the Microsoft 365 application

If you set up a Microsoft 365 application to connect to a Microsoft Entra ID domain, PingOne is the federated identity provider (IdP) for users of the domain, and Entra ID redirects users to PingOne for authentication.

When users complete multi-factor authentication (MFA) with the federated IdP, such as PingOne, Entra ID expects the IdP to send an MFA claim to Entra ID to communicate that authentication has been completed. Add an MFA claim in the Microsoft 365 application in PingOne for Entra ID to consider MFA fulfilled.

> **Note**
> An external authentication method in Entra ID isn't required when the users reside in an Entra ID federated domain.

Before you begin

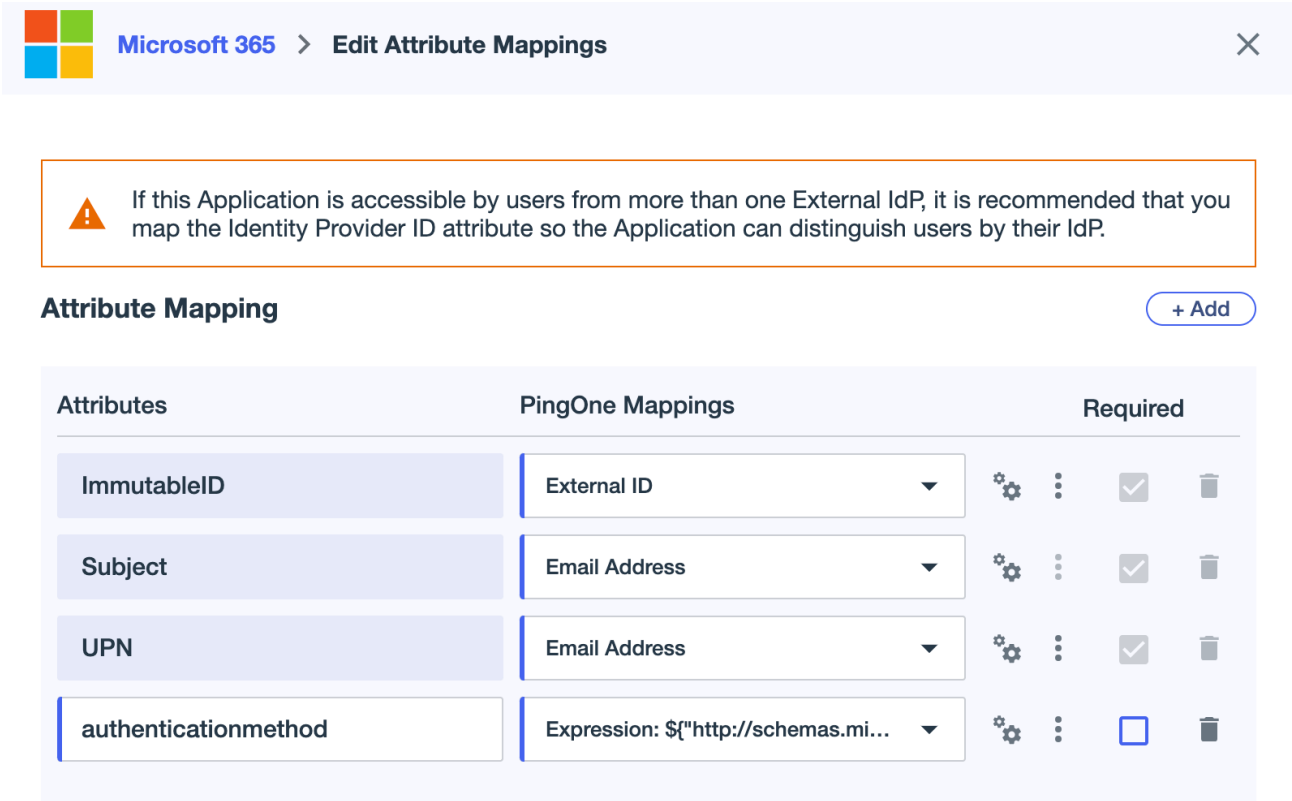
- Add Microsoft 365 to the application catalog and and complete the PowerShell cmdlets to set up PingOne as the federated IdP for the domain in Entra ID. Learn more in Adding Microsoft 365 to the PingOne application portal.
- Review Using WS-Fed or SAML 1.1 federated IdP in the Entra ID documentation.

Steps

1. In the PingOne admin console, go to **Applications > Applications** and click the **Microsoft 365 application** in the **Applications** list.
2. On the **Attribute Mappings** tab, click the **Pencil** icon.
3. Add a new attribute for the authentication method:
    1. Click **+ Add**.
    2. In the **Attributes** field, enter `authenticationmethod`.
    3. Click the **More Options** (⋮) icon and click **Update NameFormat**.
    4. In the **NameFormat** list, select **http://schemas.microsoft.com/ws/2008/06/identity/claims**.

Copyright © 2025 Ping Identity Corporation

5. Click **Update**.
6. Click the **Gear** icon to open the **Advanced Expression** modal.
7. Enter `"http://schemas.microsoft.com/claims/multipleauthn"` (with the quotation marks).



8. Click **Save**.

4. On the **Attribute Mappings** tab, click **Save**.

Result

Assertions from PingOne include the `authenticationmethod` attribute with the correct `AttributeNamespace` and `AttributeValue` attributes, and Entra ID honors the MFA status of the authenticated users from PingOne.

Adding Amazon Web Services to the PingOne application portal

Use the application catalog to add Amazon Web Services (AWS) to your application portal.

Steps

1. In PingOne, go to **Applications** > **Application Catalog**.
2. In the **Search for applications** field, enter `Amazon Web Services`.
3. Click the **Amazon Web Services** entry to open the details panel.

Copyright © 2025 Ping Identity Corporation

4. Review the following:
   - **Name**. Enter a new name to replace the default application name (optional).
   - **Icon**. Select a new image to replace the default application icon (optional).
   - **Entity ID**. The field is pre-populated with the correct value for AWS.
5. Click **Next**.
6. On the **Map Attributes** page, review the AWS to PingOne attribute mappings.

> **Note**
> Common attributes are pre-populated with the Security Assertion Markup Language (SAML) subject, the SAML role session name, and the SAML session duration. You must map any required attributes before you can continue.

Option	Description
To change an attribute mapping	Enter or select a new attribute in the PingOne Mappings list.
To add an attribute	Click **+ Add**. Enter the appropriate attribute mappings. To use the expression builder, or to map the attribute to a literal string value, click the **Gear** icon. For more information, see Using the expression builder.
To designate the attribute as required	Select the **Required** check box.
To delete an attribute mapping	Click the **Delete** icon.

7. Click **Next**.
8. For **Select Groups**, enter the name of the groups that you want to have access to the application.

> **Note**
> By default, all users have access to the application. Assigning groups restricts application access to only those groups.

9. Click **Save**.

   Result:

   The application is now configured for PingOne. You might have to perform additional configuration on the application side.

Next steps

To see applications that have already been configured, click the **Configured** tab on the **Application Catalog** page.

Copyright © 2025 Ping Identity Corporation

On the **Connection Details** page, you can download or copy metadata required by the application for single sign-on (SSO) configuration.

This information includes:

- PingOne metadata
- The PingOne signing certificate
- The PingOne Issuer ID Uniform Resource Locator (URL)
- The PingOne SSO Service URL
- The PingOne identity provider (IdP) Metadata URL
- The PingOne Initiate SSO URL

After you configure the application, you can manage it at **Applications > Applications**. For more information about advanced settings, see Editing an application.

Resources

Resources in PingOne represent web application endpoints (APIs) protected by OAuth 2 authorization services.

When you define an application in PingOne and specify its allowed scopes, you identify the resources that users can access when they sign on to that application.

> **Important**
>
> Connections to external resources must use open standards protocols.

Attributes

You can map PingOne user attributes to attributes in your resource. Learn more in Mapping attributes.

Scopes

Resources have scopes, and applications can request an access token that's associated with specific scopes when the token is granted. The endpoint enforces access through the encoded representation of the scopes in the access token. The endpoint decodes the token to determine the permissions allowed for the application.

Learn more about predefined PingOne resources in Resource scopes.

Permissions

With PingOne Authorize, you can use application permissions to set up role-based access control for API resources. A resource's application permissions control the kinds of actions users can perform on protected endpoints.

Learn more in Application permissions.

Copyright © 2025 Ping Identity Corporation

Resource scopes

The PingOne platform includes two predefined resources, `PingOne API`, which is a defined resource that represents the PingOne APIs, and `Open ID Connect`, which represents OIDC scopes.

You can use PingOne to define custom resources and their associated scopes. Custom resources can be associated with an application either exclusively or in addition to the platform's predefined resources.

> **Note**
>
> When an application is associated with both the PingOne resource and a custom resource, an authorization request cannot include scopes from both PingOne and the custom resource.
> For more information about getting unique access tokens for each API resource, see OAuth access token usage strategies for multiple resources.

OIDC scopes

OIDC scopes are used by an application during authentication to authorize access to user details, like name and email address. Scopes are a collection of claims. Each scope returns a set of user attributes, called claims.

You can define custom attributes for OIDC resources, as well as change the way they are delivered to the application: ID token, UserInfo endpoint, or both.

> **Note**
>
> Changes made to the Open ID resource will define the global configuration, which are inherited by applications. Applications can override the inherited global attributes with custom attributes. See Customizing OIDC attributes for an application.

Viewing resources

Use the **Resources** page to view resources in PingOne.

Steps

1. Go to **Applications** > **Resources**.
2. Browse or search for the resource you want to view.

   When you use the search bar, the results list is updated as you enter the query. The current resources are shown in the list.
3. Click a resource entry to open the details panel for the resource.

   The details panel includes the following tabs:

   - **Overview**: Shows general resource information, such as the resource ID, audience, access token TTL (time to live), token introspection endpoint, and client secret.
   - **Attributes**: Shows the resource attributes that are mapped to PingOne attributes. Learn more in Mapping attributes.

Copyright © 2025 Ping Identity Corporation

- **Scopes**: Shows the OIDC (OpenID Connect) scopes for the selected resource. Scopes define the permissions that the resource has, such as the ability to create a user or a population. Learn more in Resource scopes.
- **Permissions**: Shows the application permissions for the selected resource. These permissions control access to the kinds of actions users can perform on application resources. Learn more in Application permissions.

> **Note**
>
> To enable the **Permissions** tab, add PingOne Authorize to your environment.

Next steps

To edit a resource, click the pencil icon. Learn more in Editing a resource.

Adding a custom resource

Use the **Resources** page to add a custom resource to PingOne.

Steps

1. Go to **Applications** > **Resources**.
2. Click the **+** icon.
3. For **Create resource profile**, enter the following information:
   - **Resource name**: A unique identifier for the resource.
   - **Audience** (optional): The intended audience for the resource. If you don't provide a value, PingOne will default to the resource name.
   - **Description** (optional): A brief characterization of the resource.
   - **Access token time to live**: The maximum time that the access token will be valid for use in the application, in seconds.
4. Click **Next**.
5. For Attributes, map resource attributes to user attributes in PingOne.
   1. Enter a resource attribute and then select the corresponding PingOne attribute from the list.

      For example, you could map the `OIDC family_name` attribute to the PingOne `Family Name` attribute. You can add more attributes after you have created the custom resource. Learn more in Mapping attributes.
   2. Enter a resource attribute and then select the corresponding PingOne attribute from the list.

      Enter an OIDC attribute and the desired PingOne mapping. Click the **Gears** icon to use advanced expressions. Learn more in Using the expression builder.
   3. To delete an attribute, click the **Trash** icon for the appropriate attribute.

   Resources can use JSON attributes in their attribute mappings. You can use these attributes to pass complex information to applications through an access token. Learn more in Adding user attributes.
6. Click **Next**.

Copyright © 2025 Ping Identity Corporation

7. For **Scopes**, configure the appropriate scopes for the resource. Each resource can have one or more scopes. To add a scope, click **+ Add scope**. Enter the following:
   - **Scope name**: The name of the scope to be used for this resource. Scopes are defined by the resource server.
   - **Description** (optional): A brief description of the scope.
8. Click **Save**.

Next steps

You can add more scopes to the custom resource. Learn more in Editing a resource.

With PingOne Authorize, you can define application resources and permissions to set up role-based access control for the custom resource. Learn more in Application permissions and Editing a resource.

Editing a resource

Use the **Resources** page to modify existing resources in PingOne.

Steps

1. Go to **Applications > Resources** and browse or search for the resource that you want to edit.

   The results list updates as you enter the search query. The current resources are shown in the list.
2. Click a resource entry to open the details panel for the resource.
3. On the **Overview** tab, click the **Pencil** icon and enter or edit the following:

Field	Description
Resource Name	A unique identifier for the resource.
Audience (optional)	The intended audience for the resource. If you don't provide a value, PingOne defaults to the resource name.
Description (optional)	A brief description of the resource.
Access token time to live	The maximum time, in seconds, that the access token will be valid for use in the application.
Token introspection endpoint authentication method	Specifies how to authenticate using the client credentials for the application to which the token was issued. You can select from: ◦ `None` ◦ `Client secret basic` ◦ `Client secret post` ◦ `Client secret JWT` ◦ `Private key JWT` For `Private key JWT`, select **JWKS URL** or **JWKS**. Provide either the URL where PingOne can retrieve the JSON Web Key Set (JWKS) or the web key set itself.

Copyright © 2025 Ping Identity Corporation

4. On the **Attributes** tab, map resource attributes to user attributes in PingOne. Enter a resource attribute and then select the corresponding PingOne attribute from the list.

   Example:

   For example, you could map the `OIDC family_name` attribute to the PingOne `Family Name` attribute.

   1. (Optional) To add more attributes after you have created the custom resource, click **+ Add**. Enter an OIDC attribute and the desired PingOne mapping. Learn more in Mapping attributes. Click the **Gear** icon to use advanced expressions. Learn more in Using the expression builder.
   2. To delete an attribute, click the **Delete** icon for the appropriate attribute.

   > **Note**
   >
   > Resources can use JSON attributes in their attribute mappings. You can use these attributes to pass complex information to applications through an access token. Learn more in Adding user attributes.

5. On the **Scopes** tab, locate the scope you want to edit, and then click the **Pencil** icon. Enter or edit the **Scope name** and **Description**.

   1. (Optional) To add a scope, click **+ Add scope**, and enter the **Scope name** and **Description** and any mapped attributes to which you want the scope to have access.

6. (Optional) On the **Permissions** tab, click the **Include user permissions in Access Token** toggle to include application permissions in access tokens created for this resource.

   > **Note**
   >
   > To enable the **Permissions** tab, add PingOne Authorize to your environment.

   Permissions for the authenticated user will be included in the `p1.permissions` claim in the access token. Learn more in Application permissions.

7. (Optional) To add an application resource and permissions, click **+ Add Permissions**.

   Learn more in Adding application permissions.

8. To delete an application resource, click the **Delete** icon next to the application resource.

9. To edit an application resource, click the **Pencil** icon next to the application resource.

   Choose from:

   - Edit the application resource **Name** and **Description**.
   - To add a permission, click **+ Add**. Enter an **Action** and **Description** for the permission.
   - Edit the **Action** and **Description** for existing permissions.
   - To delete a permission, click the **Delete** icon next to the permission.

10. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Editing an OIDC resource

You can define the global attribute mappings and scopes for the OpenID Connect resource. These mappings are inherited by all OIDC applications by default. Applications can override the inherited global attributes with custom attributes that you want included during runtime. Learn more in Customizing OIDC attributes for an application.

Steps

1. Go to **Applications** > **Resources**.
2. Click the **OpenID Connect** entry to open the details panel.
3. On the **Attributes** tab, click the **Pencil** icon.
4. Review the OIDC attributes and their mapping to PingOne attributes.
   - To add an attribute, click the **+ Add** button. Enter an OIDC attribute and the desired PingOne mapping. Click the gears icon to use advanced expressions. Learn more in Using the expression builder.
   - To delete an attribute, click its **Delete**icon.

     > **Note**
     > Attributes with a blue background are part of the OIDC specification. You cannot delete the default attributes, but you can map them to new attributes in PingOne. PingOne will ignore an attribute if the PingOne mapping is blank.

5. Select the delivery method:
   - **ID token**. The attribute is delivered to the application in the ID token.
   - **UserInfo**. The attribute is delivered to the application from the UserInfo endpoint.

     > **Note**
     > PingOne enforces an ID token limitation of 25 values for a multivalued attribute. When this occurs, PingOne populates `[SIZE_LIMIT_EXCEEDED]` as the attribute value.
     > Use **UserInfo** to retrieve the data as needed.

6. Click the **Scopes** tab.
   - To add a scope, click **+ Add scope**. Enter the **Scope Name** and **Description**, and then select **Mapped Attributes** to assign to the scope.
   - To edit a scope, click the **Pencil** icon and select **Mapped Attributes** to assign to the scope.

     > **Note**
     > Assigning attributes to a scope allows an application to inherit these attributes, if the application has the resource and scope added to it. Learn more in Editing an application - OIDC.

7. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Deleting a resource

Use the **Resources** page to remove a resource that you no longer need.

About this task

> **Note**
>
> Deleting a resource might affect features in some applications. Make sure it is safe to delete a resource.

Steps

1. Go to **Applications** > **Resources**.
2. Locate the resource you want to delete. You can browse or search for resources.
3. Click a resource entry to open the details panel for the resource.
4. In the upper right, click the options menu (three dots) and then click **Delete**.
5. In the confirmation message, click **Delete**.

Rotating the client secret for a resource

For security reasons, you should change a resource's client secret on a regular basis. If you think the client secret might have been compromised, you should change it immediately.

After you update a client secret in PingOne, you must also update all resources that use the secret. You can retain the previous client secret to give resource owners time to update the secret without causing errors for their users. Use the PingOne admin console or the PingOne API to change a client secret.

For more information, see:

- Viewing the client secret for a resource
- Generating a client secret for a resource
- Revoking a client secret for a custom resource
- To use the PingOne API to rotate a client secret, see Resource secret in the PingOne Platform API Reference.

Viewing the client secret for a resource

You can use the PingOne console to get the client secret for an existing resource. This feature allows you to get a client secret without having to make an API call.

Steps

1. Go to **Applications** > **Resources** and browse or search for the resource.
2. Click the resource entry to open the details panel.

Copyright © 2025 Ping Identity Corporation

3. On the **Overview** tab, locate the **Client Secret** section. Click the **Eye** icon next to **Client Secret** or **Previous Client Secret** (custom resources only) to make the secret readable.
4. To copy the client secret, click **Copy to clipboard**.

> **Note**
> To rotate a client secret, see Generating a client secret for a resource.

Generating a client secret for a resource

For security reasons, you should change a resource's client secret on a regular basis. For more information, see Rotating the client secret for a resource.

Steps

1. Go to **Applications > Resources** and browse or search for the resource for which you want to generate the client secret.
2. Click the resource entry to open the details panel.
3. Click the **Overview** tab, and locate the **Client Secret** section.
4. Click **Generate New Secret**.
5. If you are generating a new secret for a custom resource, from **Retain Previous Secret**, select how long to retain the previous client secret:

   Choose from:

   - **Retain for 1 Day**: The previous secret expires 24 hours after the creation of the new secret.
   - **Retain for 7 Days**: The previous secret expires 7 days after the creation of the new secret.
   - **Retain for 30 Days**: The previous secret expires 30 days after the creation of the new secret. 30 days is the maximum retention period.
   - **Retain for custom duration**: Configure the secret to expire after a custom time frame. For example, 14 days.

     > **Note**
     > You cannot set the retention period for longer than 30 days.

   - **Do Not Retain Previous Secret**: The previous secret expires immediately. Users might experience sign-on errors until the resource is updated to use the new secret.

     > **Important**
     > This setting cannot be changed. If you are not sure how long you should retain the previous client secret, select **Retain for 30 Days**. If you do not need to keep the previous secret for that long, you can revoke it manually before the retention period expires. For more information, see Revoking a client secret for a custom resource.

6. Select **I understand and would like to continue**. Click **Confirm**.

Copyright © 2025 Ping Identity Corporation

Result

PingOne generates a new client secret for the resource.

Revoking a client secret for a custom resource

When you generate a new client secret for a custom resource that has an existing client secret, you have the option to retain the previous secret for a certain period of time. If you no longer need the previous secret before it is set to expire, you can revoke it manually from the configuration tab for the resource.

About this task

> **Note**
> For security purposes, revoke the previous client secret as soon as you know it is no longer needed.

Steps

1. Go to **Applications** > **Resources** and browse or search for the resource with the client secret that you want to revoke.
2. Click the resource entry to open the details panel.
3. On the **Overview** tab, locate the **Previous Client Secret** section.

   > **Note**
   > If the previous client secret already expired or was not retained, this section does not appear.

4. Click **Revoke Previous Client Secret**.

   > **Important**
   > This action cannot be undone.

5. In the confirmation message, select **I understand and would like to continue**. Click **Confirm**.

Result

The previous secret is revoked. Users must have the new client secret to access the resource.

Access tokens and ID tokens

Access tokens are credential strings that represent authorization to access a protected resource.

Client applications obtain access tokens by making OAuth 2 or OpenID Connect (OIDC) requests to an authorization server. Resource servers require clients to authenticate using access tokens.

Access tokens are obtained from the token endpoint, when using the client credentials grant type, or from the authorization endpoint, when using the implicit grant type. Access tokens are typically granted on behalf of a specific authenticated user. Tokens granted directly to applications are called application tokens.

Copyright © 2025 Ping Identity Corporation

Related links

- Customizing access tokens

Customizing access tokens

With PingOne, you can customize the content of access tokens by adding custom resource attributes and application permissions to the token. Use customized access tokens to convey additional information about token holders to applications.

About this task

> **Note**
> You cannot customize tokens for the two default resources, `OpenID Connect` and `PingOne API`.

Steps

1. Go to **Applications** > **Resources** and browse or search for the resource that you want to edit.
2. Click the resource entry to open the details panel for the resource.
3. To add custom attributes, click the **Attributes** tab, and then click the **Pencil** icon.
    1. Click **+ Add**.
    2. Enter the following:
        - **Attributes**: Enter the attribute value for the resource, such as `sub`.
        - **PingOne mappings**: Select an attribute in the list, such as `User ID`.

        > **Note**
        > Learn more about configuring the access token TTL (time to live) in Editing a resource.

    3. Continue adding attributes as needed.
4. To include application permissions in access tokens created for this resource, on the **Permissions** tab, click the **Include user permissions in Access Token** toggle.

    > **Note**
    > To enable the **Permissions** tab, add PingOne Authorize to your environment.
    > Learn more about defining application permissions in Adding application permissions.

    The `p1.permissions` claim in the access token will include permissions for the authenticated user.
5. Click **Save**.

Token introspection

Use token introspection to get detailed information about access tokens.

Copyright © 2025 Ping Identity Corporation

You can check the validity of access tokens, and find out which user and which scopes are associated with the token.

For more information about how to access the token introspection endpoint, see POST Token Introspection in the PingOne Platform API Reference.

Attribute access control

Some PingOne platform self-management scopes allow organizations to specify which user profile attributes are accessible to end users.

An administrator might want to prevent end users from seeing or modifying particular attributes that should remain private, such as custom attributes for entitlements, internal foreign keys, account status information, or any profile data that should not be exposed to an individual user. With access control scopes, organizations can store additional private data in the user profile without risk that the end user can see the data.

These access control scopes designate a specific set of user attributes, which is often a subset of attributes that the user is allowed to read or update. For example, a `p1:update:user:email-only` scope could remove all other user schema attributes except the user's email address. A user with this scope could update only their email address. All other visible attributes would not allow modification.

Related links

- Configuring attribute access control

Configuring attribute access control

You can configure individual scopes, such as `p1:read:user`, or sub-scopes, such as `p1:read:user:emailonly`.

About this task

You should configure access control scopes to include specific attributes explicitly, rather than using the default settings that allow all attributes, even new ones, to be read and updated. You can do this by creating sub-scopes for attributes that you want to allow, and assigning individual attributes to that scope.

Steps

1. Go to **Applications** > **Resources**.
2. Click the **PingOne API** entry to open the details panel.
3. Click the **Scopes** tab.
4. Locate an existing scope to edit and then click the pencil icon.
5. Select the attributes that the end user will be able to access.

   To add a sub-scope, click **+ Add scope** under the appropriate scope name and enter the scope suffix, such as `emailonly`, for the scope name, and then select the attributes that the end user will be able to access.
6. Click **Save**.

Related links

- Attribute access control

Copyright © 2025 Ping Identity Corporation

Application permissions

Application permissions allow you to control the types of actions that users can perform in your applications and APIs.

To implement access control based on permissions, commonly known as role-based access control (RBAC), define permissions for application features, then group these permissions into roles. Assigning roles to users grants access to features and API resources.

Application permissions and roles in PingOne help you centralize access control, making it easier to quickly and repeatedly assign permissions to users and adjust them as your business needs change.

> **Note**
>
> To use application permissions, you must have PingOne Authorize in your environment.

Resources and permissions

Applications are built on top of APIs, and application features are often represented as API operations. Accordingly, you define permissions against an API. **Application resources** are the things that you want to protect in your API or application.

An **application permission** specifies an action that a user can perform on an application resource. For example, if you have an invoicing application, you might define an invoice resource with permissions to view, create, pay, and void invoices. Learn more about this scenario in Adding application permissions.

Configuring application permissions

Complete the following steps to configure application permissions:

1. Add PingOne Authorize to your environment.
2. Add application permissions to a custom API resource.
3. Add application roles. This includes assigning permissions to roles, and then assigning roles to users.

Enforcing permissions

To enable your application to retrieve and enforce permissions, you can include the permissions claim in access tokens or use permissions-based rules.

Permissions claim in access tokens

To include permissions in access tokens, enable the **Include user permissions in Access Token** toggle on the **Permissions** tab for a custom resource. When the toggle is enabled, the `p1.permissions` claim is included in access tokens scoped to the custom resource.

- When an OAuth 2.0 client application requests an access token on behalf of a user, the claim is populated with the authenticated user's permissions. The application must be scoped to the custom resource. Permissions are not included in tokens obtained through the Client Credentials grant type.
- The claim is empty if the authenticated user isn't assigned to a role that has application permissions.

A resource server can use this JWT claim to identify the token holder's permissions in order to make authorization decisions.

Copyright © 2025 Ping Identity Corporation

> **Important**
>
> The `p1.permissions` claim increases access token size and the time required to generate a token. Use this type of permissions enforcement only if your organization doesn't require a large number of permissions.

The `p1.permissions` claim contains an array of strings. Each member of the array is a permission key, such as `invoices:read`. For example, consider a business application called BizPro that has invoicing capabilities. A decoded token for a BizPro user with permissions to read, write, and pay invoices looks something like this:

```
{
  "aud": [
    "BizPro Invoices API"
  ],
  "client_id": "2be7e2f8-02d8-46ca-9ebb-35e129a78452",
  "exp": 1702659466,
  "iat": 1702655866,
  "iss": "https://auth.pingone.com/672e060d-e6c9-49d9-81b8-22ac46e55c85/as",
  "p1.permissions": [
    "invoices:read",
    "invoices:write",
    "invoices:pay"
  ],
  "scope": "bizpro:invoices",
  "sid": "d11d5eb0-b2cb-4674-b4ef-2cdc211d379c",
  "sub": "c52cc34d-2f29-442d-adf8-00fc89f7bbd8",
}
```

You can use the token introspection endpoint to return information about claims in the access token. Learn more in the Token Introspection API documentation.

Permissions-based rules

If your organization has more extensive use cases that require a large number of permissions, you can define permissions-based rules that work with your API gateway to enforce entitlements.

After you configure application permissions, complete the following steps to define permissions-based rules for permissions enforcement:

1. Connect your API gateway to PingOne.
2. Register the API in order to enforce permissions.
3. Define access control rules for API operations.

Extending access control

When your organization's access control needs progress beyond static permissions, you can leverage real-time contextual information in your access control decisions. Fine-grained authorization policies can factor in a range of contextual attributes, such as user characteristics, risk signals, and environment properties such as location and time.

You can use PingOne's API Access Management custom policy capabilities in conjunction with application permissions to satisfy these access control requirements. Learn more in API services.

Copyright © 2025 Ping Identity Corporation

Adding application permissions

Define application permissions for the application resources that you want to protect.

Before you begin

- Add PingOne Authorize to your environment.
- Add a custom resource for your protected endpoints.

About this task

Application resources are features that users want to access, such as checking and savings accounts, an investment services add-on, or an invoicing module in a business application.

> **Note**
> PingOne platform resources, such as identities and PingOne APIs, are protected by PingOne platform roles and permissions. Application resources protect access to resources that are developed by your organization's engineering teams.

An application permission is the combination of an action and a resource. Think of permissions as actions that can be taken on a resource. Configure application permissions by assigning actions to application resources.

> **Note**
> You can add up to 128 application resources and 128 application permissions in each PingOne environment.

For example, consider a business application called BizPro that has invoicing capabilities. Endpoints for the associated invoicing API allow the following actions on the `invoices` resource:

- Read invoices: `GET /bizpro/invoices`
- Create an invoice: `POST /bizpro/invoices`
- Update an invoice: `PUT /bizpro/invoices/\{{invoiceId}}`
- Pay an invoice: `POST /bizpro/invoices/\{{invoiceId}}/pay`
- Void an invoice: `POST /bizpro/invoices/\{{invoiceId}}/void`

To control access to invoices, you create corresponding application permissions:

- `Invoices:Read`
- `Invoices:Write`
- `Invoices:Update`
- `Invoices:Pay`
- `Invoices:Void`

Steps

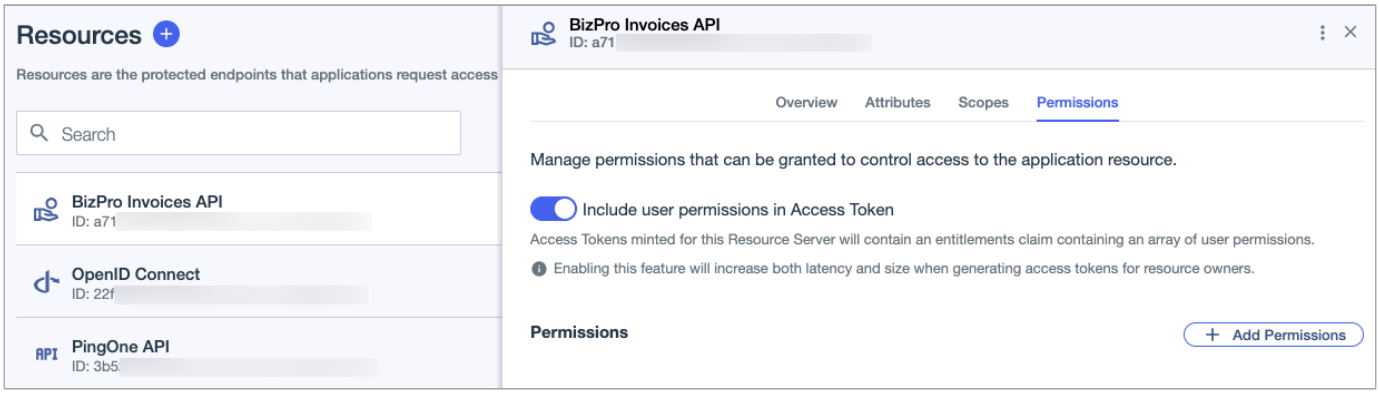
1. Go to **Applications** > **Resources** and browse or search for the custom resource for your protected endpoints.

Copyright © 2025 Ping Identity Corporation

2. Click the custom resource to open the details pane, then click the **Permissions** tab.

3. (Optional) To include user permissions in access tokens created for this custom resource, click the **Include user permissions in Access Token** toggle.

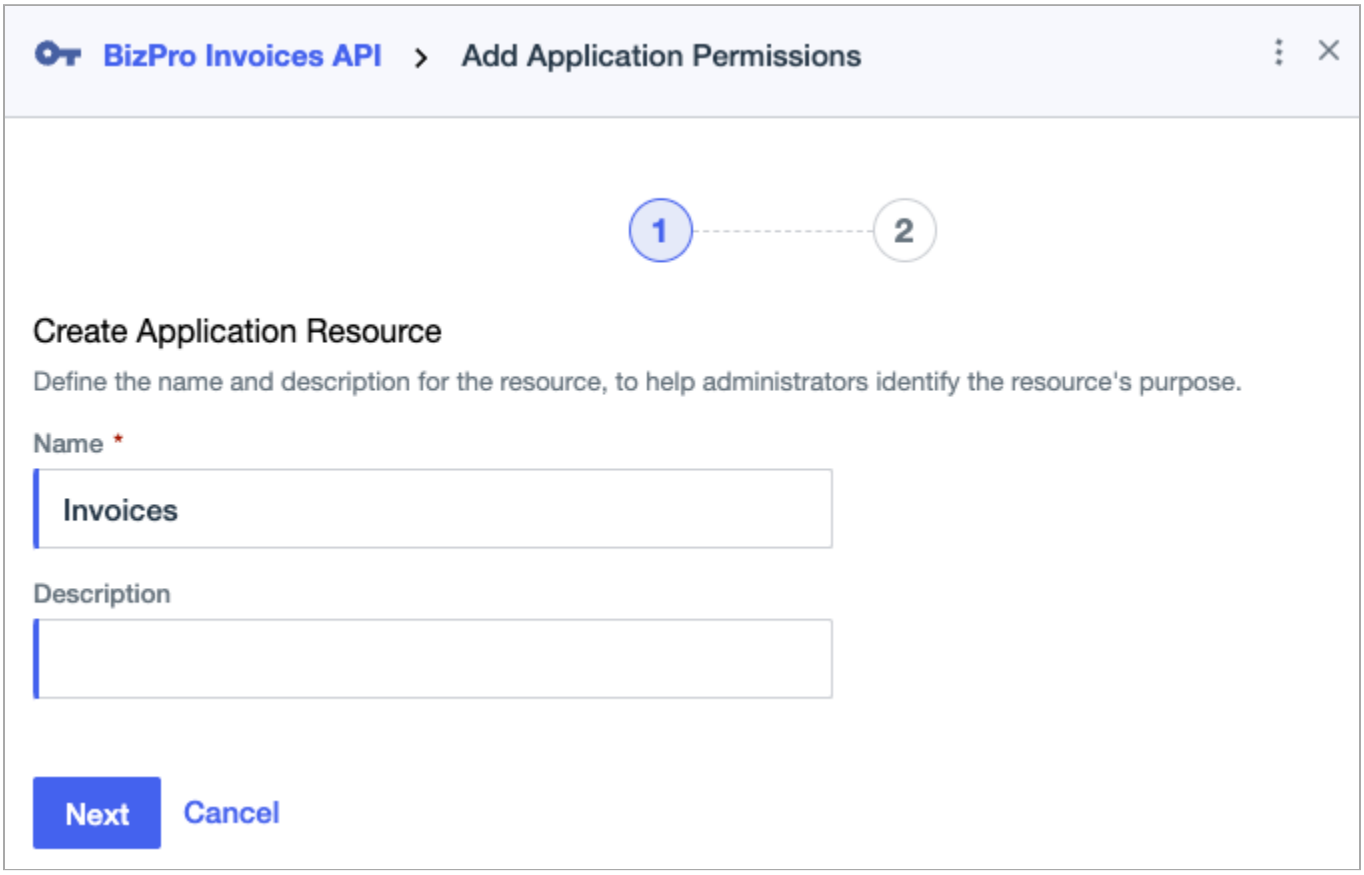
   Permissions for the authenticated user are included in the `p1.permissions` claim in the access token.



> **Note**
>
> If your organization requires a large number of permissions, consider using permissions-based rules for permissions enforcement. Learn more in Application permissions.

4. Click **+ Add Permissions**.

5. To create an application resource, enter a unique **Name** and an optional **Description**. Click **Next**.



Copyright © 2025 Ping Identity Corporation

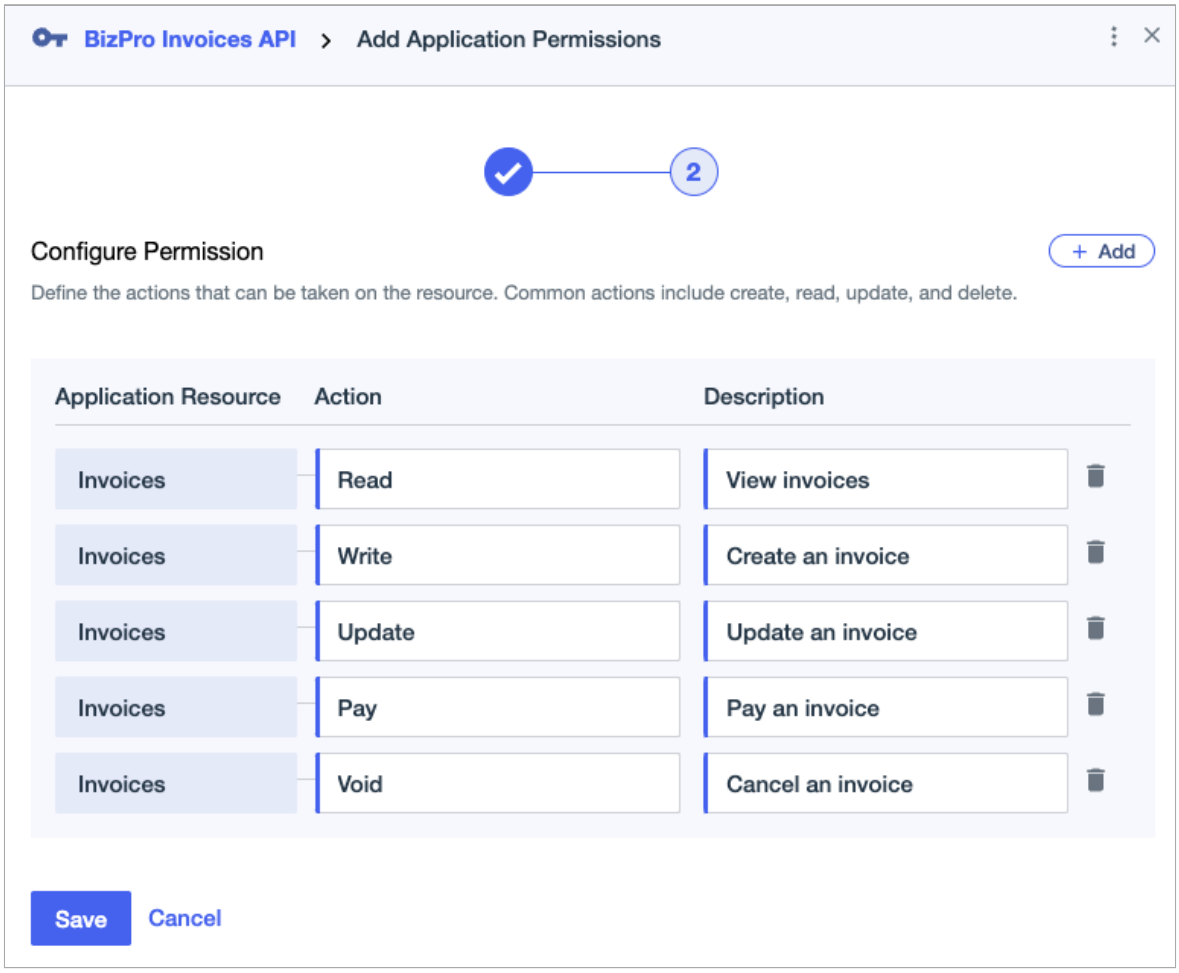
> **Note**
> The name can include Unicode letters, marks, numbers, spaces, forward slashes, dots, apostrophes, underscores, and hyphens, with a maximum length of 20 characters.

6. Configure permissions for the application resource:

   1. Click **+ Add** to add an **Action** that you want to protect with a permission.

      > **Note**
      > The action can include Unicode letters, with a maximum length of 20 characters.

   2. (Optional) Enter a **Description** for the action.



   3. To add more actions, click **+ Add**.

7. Click **Save**.

Next steps

Add application roles to simplify the assignment of application permissions to users. For example, David, an invoicing processor, might have permissions to create and pay invoices, while Melissa, the billing supervisor, can view and void invoices. Learn more in Adding an application role.

Copyright © 2025 Ping Identity Corporation

Application portal

The application portal shows the applications accessible to users through single sign-on (SSO) based on their group memberships. This includes SAML applications and OpenID Connect (OIDC) applications that have the `Initiate Login URI` configured. The applications that a user sees depend on the access controls for that application. Learn more in Adding an application.

> **Tip**
>
> To make an OIDC application available in the application portal, the application must have an `Initiate Login URI` configured. To add the URI to an existing application, go to the application's **Configuration** tab and enter the URI in the **Initiate Login URI** field. Learn more in Editing an application - OIDC.

You can also add links to other resources your users might find useful, such as status pages, user guides, and applications that aren't accessible through SSO, and select the sign-off method that PingOne uses when users sign off from the application portal. Learn more in Configuring the application portal.

Configuring the application portal

You can configure branding and theme options for the application portal and choose a sign-off method for end users.

Steps

1. In the PingOne admin console, go to **Applications** > **Application Portal**.
2. To apply the active environment theme to the application portal, select the **Apply active theme to Application Portal** checkbox. Learn more in Branding and themes.

   > **Tip**
   >
   > You can add links to resources your users might find helpful, such as status pages, user guides, and applications that aren't accessible through single sign-on (SSO). Learn more in Adding resource links to the application portal.

3. For **Sign Off Method**, choose either of the following for PingOne to use when end users sign off from the application portal:
   - **OIDC Logout** (default): Allow the end user to sign off from the application portal using OpenID Connect (OIDC) relying party (RP)-initiated logout. This option invalidates access tokens, refresh tokens, and ID tokens associated with the session. When selected, PingOne doesn't send SAML 2.0 single logout requests to SAML identity providers or applications.

     Learn more in the OIDC RP-Initiated Logout 1.0 documentation.
   - **SAML 2.0 Single Logout**: Initiate SAML 2.0 single logout when the user signs off from the application portal. Access tokens, refresh tokens, and ID tokens obtained during the session remain valid until they expire or are revoked.
4. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Applying authentication policies to the application portal

The application portal itself is an OpenID Connect (OIDC)-based application. Like other OIDC-based applications, you can configure an authentication policy for the application portal.

About this task

The authentication policy defines the sign-on requirements for accessing the application.

Default domain

By default, the application portal **Home Page URL** is https://apps.pingone.*<region>*/*<envId>*/myapps/

Custom domain

If you use a custom domain, the **Home Page URL** is https://*<customDomain>*/myapps/

For more information about how authentication policies are evaluated, see Authentication policies for applications.

To apply authentication polices to the application portal:

Steps

1. Go to **Applications > Applications** and click the **PingOne Application Portal** application to open the details panel.
2. Click the **Policies** tab, and then click the **Pencil** icon.
3. Select the policy that you want to apply.
4. Click **Save**.

Result

PingOne applies the selected policies to the **PingOne Application Portal** application. For more information about how authentication policies are evaluated, see Authentication policies for applications.

Next steps

To control which authentication policy is used when users access the portal, append the `policy` HTTP request parameter to the end of the URL for the application when you share the URL with users.

For example, the application portal is configured with three authentication policies named One, Two, and Three, and the policies are listed in that order on the **Policies** tab. You want a certain group of users to use policy Two when accessing the portal. Before you share the URL for the portal with these users, append the `policy` parameter to the URL as follows:

If you are using the default domain

https://apps.pingone.*<region>*/*<envId>*/myapps/**?policy=Two**

If you are using a custom domain

https://*<customDomain>*/myapps/**?policy=Two**

> **Note**
>
> To use a DaVinci flow policy instead of an authentication policy, use the policy ID for the `policy` parameter value.

Copyright © 2025 Ping Identity Corporation

If the policy name or ID does not match any configured policy, then PingOne returns an error.

Adding resource links to the application portal

You can add links to resources your users might find useful, such as status pages, user guides, and applications that are not accessible through SSO. You can add a link to any resource that has a URL.

Steps

1. Go to **Applications > Application Portal**.

   > **Note**
   >
   > To customize the branding and themes, see Configuring the application portal.

2. To add a link to a resource other than a SSO application, locate the **Links** section and then click **+**.
3. For **Profile details**, enter the following:
   - **Link name**. A name for the link as it will appear in the application portal.
   - **Description** (optional). A brief characterization of the link.
   - **Icon** (optional). A pictorial representation of the application. Use a file up to 1MB in JPG, JPEG, GIF, or PNG format.
   - **URL**. The URL to which the user will be directed. HTTP or HTTPS links are valid.
4. Click **Save**.

Next steps

You can edit the visibility settings after you create the link. The visibility settings determine which groups can access the link. See Editing a resource link.

Editing a resource link

You can edit a resource link to change the name, description, icon, URL, or visibility settings. The visibility settings determine which groups can access the link.

Steps

1. Go to **Applications > Application Portal**.
2. Under **Links**, locate the resource link you want to edit.
3. On the right, click the three dots options menu, and then click **Edit**.
4. For **Profile details**, click the pencil icon and enter or edit the following:
   - **Link name**. A name for the link as it will appear in the application portal.
   - **Description** (optional). A brief characterization of the link.
   - **Icon** (optional). A pictorial representation of the application. Use a file up to 1MB in JPG, JPEG, GIF, or PNG format.

Copyright © 2025 Ping Identity Corporation

- **URL**. The URL to which the user will be directed. HTTP or HTTPS links are valid.

5. Click the **Visibility** tab.
6. Do one of more of the following:
   - Select **Any** or **All** to determine whether the user must be a member of any defined group, or all defined groups.
   - To add a group, click the plus sign (**+**) for the appropriate group.
   - To remove a group, click the check mark for the appropriate group.

   > **Note**
   > If no groups are defined, then all users can access the link.

7. Click **Save**.

Deleting a resource link

You can remove a resource link that you no longer need.

Steps

1. Go to **Applications > Application Portal**.
2. Under **Links**, locate the resource link you want to delete.
3. On the right, click the three dots options menu, and then click **Delete**.
4. In the confirmation message, click **Delete**.

Copyright © 2025 Ping Identity Corporation

DaVinci

If you have a license for PingOne DaVinci, click **DaVinci** to open the DaVinci console.

DaVinci is an orchestration platform that lets you create flows using connections and logical operators. These flows guide users through defined processes that can present customized pages, modify values, or perform other actions.

Learn more in the PingOne DaVinci documentation.

Copyright © 2025 Ping Identity Corporation

Authentication

The **Authentication** branch provides access to your **Authentication**, **Password**, **MFA**, and **FIDO** policies.

You can also manage your **MFA Settings** from this branch.

For more information, see the following topics:

Authentication policies

Password policies

MFA policies

FIDO policies

MFA Settings

Authentication policies

Authentication policies dictate how the user's identity will be verified. For example, a single-factor authentication policy requires a single piece of evidence to verify a user's identity, such as a password. A multi-factor policy could require evidence to verify a user's identity, such as a TOTP authenticator app, FIDO2 biometrics, a push notification sent to the user's mobile device, or a one-time passcode sent over SMS, voice or email. You can also use multi-factor authentication to set up passwordless authentication. You can determine whether users who do not have any enrolled MFA devices are permitted to bypass the MFA flow, or are blocked from sign-on.

In PingOne MFA, and PingID, the multi-factor authentication step is the only policy step that the admin can configure. To enable configuration of additional steps, additional services must be added to the environment.

For each authentication policy, you can set a condition that determines whether the policy will be applied. For example, the Single_Factor policy can include a condition that requires users to sign on if the most recent sign-on occurred more than eight hours ago. If no conditions are specified, users will be required to sign on every time they access the application.

Viewing authentication policies

View the currently configured authentication policies.

Steps

- Go to **Authentication > Authentication**.

Result

The **Authentication Policies** window shows a list of current authentication policies, including details for single-factor and multi-factor authentication by default. Click the details icon to expand an entry and see details about the authentication policy.

Adding an authentication policy

You can add one or more authentication policy.

1. Go to **Authentication > Authentication**.

Copyright © 2025 Ping Identity Corporation

2. Click **+ Add Policy**.

3. Enter a policy name.

4. In the **Step Type** list, select the protocol for the first step:

Step Type	Description
Login	Requires only one piece of evidence to verify a user's identity, such as a username and password. Learn more in Adding a login authentication step.
Identifier First	Allows you to identify users before you authenticate them. Learn more in Adding an identifier first authentication step.
Multi-Factor Authentication (Customer only) or **PingID Authentication** (Workforce only)	Requires two pieces of evidence to verify a user's identity, such as a user name and password as well as a one-time passcode (OTP). You can also use multi-factor authentication (MFA) to set up passwordless authentication. Learn more in Adding a multi-factor authentication or PingID step and Setting up passwordless authentication.
External Identity Provider	Allows end users to access your applications by authenticating with the external identity provider (IdP). Learn more in Adding an external identity provider sign-on step.

5. (Optional) Click **Add Step** to add another step to the authentication policy.

   You can add any of the step types discussed previously, in addition to the following step types that can't be used for the first step in an authentication policy:

Step Type	Description
Progressive Profiling	Allows you to prompt a user for information to be added to their profile after the initial registration step. For example, you could prompt users to add their mobile phone number the next time they sign on. Learn more in Progressive profiling and Adding a progressive profiling step.
Agreement Prompt	Requires end users to consent to a terms of service agreement as part of a sign-on policy. Learn more in Agreements.

6. Continue adding steps as needed for your authentication policy.

Copyright © 2025 Ping Identity Corporation

7. Click **Save**.

> **Note**
>
> The first step in a policy can't have population or user attribute conditions. Additionally, if the second step in a two-step policy has conditions set, and you delete the first step so that the second step becomes the first, those conditions will be removed.

Adding a login authentication step

A single-factor authentication step requires only one piece of evidence to verify a user's identity, such as a username and password.

Steps

1. In the PingOne admin console, go to **Authentication** > **Authentication**.
2. Click **+ Add Policy** to create a new policy, or click the **Pencil** icon to edit an existing one.
3. Click **+ Add Step**.
4. In the **Step Type** list, select **Login**.
5. Enter or edit the recovery and registration settings.

Setting	Description
Enable account recovery	In case of a forgotten password, users can recover their accounts with a one-time passcode (OTP) sent over email.
Enable registration	Users can register their own accounts if a user record already exists. Select **PingOne Directory** to provision users to the PingOne user store. Select **External Link** to provision users to an external user store. PingOne will direct users to the **Registration Target URL** for registration, but PingOne will still be used for authentication.
Require confirmation of user information	If registration is enabled, requires end users to confirm the data that is linked with the third-party identity provider (IdP). The end user will have an opportunity to edit the information that the third-party IdP shares with PingOne, such as username, email address, first name, and last name.

6. Enter or edit the requirement conditions. If this condition is met, the user will be required to sign on.
   - **Last sign-on older than**: Requires users to sign on again if their previous sign-on is older than the configured value.
7. Enter or edit an external IdP. Click **+ Add Provider** and then select an IdP from the list. If an IdP doesn't appear on the list, the IdP might not be enabled. Learn more in Adding an external identity provider.

Copyright © 2025 Ping Identity Corporation

8. To prevent users from signing on if their PingOne user account is locked, select **Block authentication of locked user accounts from Presented Identity Providers**. If this option is cleared, users can sign on with their configured IdP credentials, but not their PingOne credentials.

9. Click **Save**.

Adding a multi-factor authentication or PingID step

An MFA policy requires two pieces of evidence to verify a user's identity, such as a user name and password as well as a one-time passcode (OTP) sent over SMS, voice or email, or a push notification to the user's mobile device. You can also use multi-factor authentication to set up passwordless authentication. Learn more in Setting up passwordless authentication.

Steps

1. Go to **Authentication** > **Authentication**.

2. Click **+ Add Policy** to create a new policy, or click the **Pencil** icon to edit an existing one.

3. Click **+ Add Step**.

4. Do either:

   - (Consumer only) In the **Step Type** list, select **Multi-Factor Authentication**.

   - (Workforce only) In the **Step Type** list, select **PingID Authentication**.

5. (Consumer only) In the **MFA Policy** list, select an MFA policy that has been defined for the environment. Learn more about defining MFA policies in MFA policies.

6. (Consumer only) **None or incompatible methods**:

   For MFA scenarios in which users attempt to sign on but do not have any enrolled MFA devices that comply with the permitted **Available Methods**, select a flow:

   - **Block**: Do not permit these users to sign on because they don't have a usable device for MFA.

   - **Bypass**: Allow users without a usable MFA device to bypass the MFA flow.

     To leverage the **Bypass** option, the user must already be authenticated, either by a password (login step) or by supplying a signed `login_hint_token` in the request object. Learn more in `login_hint_token` in the GET Authorize (Browserless and MFA Only Flows) operation in the PingOne Platform API Reference.

7. (Consumer only) Enter or edit the requirement conditions. If one or more of the following conditions are met, the user will be prompted to use a two-step authentication method.

   - **Last sign-on older than**: Requires users to sign in if their previous login is older than the configured value.

   - **Accessing from IP out of range**: Requires users to sign on if the request comes from an IP address outside of the specified range. Use CIDR notation to specify the IP address range.

   - **Being a member of any of these populations**: Requires users to sign on if the user belongs to the specified population or populations.

Copyright © 2025 Ping Identity Corporation

- **User attributes**: Requires users to sign om if they match a specified user attribute, such as postal code or user ID. For example, `Postal Code = 78750`. Select the checkbox, then click **+ Add attribute**. Enter the attribute and the appropriate value. If you have multiple attribute conditions, the policy will evaluate to true if any of the conditions are met (Boolean OR).
- **IP reputation is high risk**: PingOne collects and analyzes IP address data of authentication requests from the user's accessing device. An IP address is considered high risk if it may have recently been involved in malicious activities, such as DDoS attacks or spam activity. Select the checkbox to require MFA when authentication requests come from IP addresses with high risk scores.

  > **Note**
  >
  > The **IP reputation** option is a feature that is available only with a PingOne Protect or PingOne for Customers Passwordless license.

- **A geovelocity anomaly is detected**: PingOne analyzes location data from the user's accessing device. It determines whether travel time between a user's current login location and their previous login location is possible in the time frame that has elapsed since the previous login. Select the checkbox to require MFA when a geovelocity anomaly is detected.

  > **Note**
  >
  > The **Geovelocity anomaly** option is a feature that is available only with a PingOne Protect or PingOne for Customers Passwordless license.

- **Anonymous network detection**: PingOne collects and analyzes IP address data of authentication requests from the user's accessing device. Select the checkbox to require MFA when PingOne identifies an IP address as originating from an anonymous network such as an unknown VPN, proxy, or an anonymous communication tool such as Tor. Exclude IP addresses in the **Whitelist** by entering them in CIDR notation in a comma-separated list.

  > **Note**
  >
  > The **Anonymous network detection** option is a feature that is available only with a PingOne Protect or PingOne for Customers Passwordless license.

8. Click **Save**.

Adding an identifier first authentication step

To use identifier first authentication, add it as part of an authentication policy.

Steps

1. In the PingOne admin console, go to **Authentication > Authentication**.
2. Click **+ Add Policy** to create a new policy, or click the **Pencil** icon to edit an existing one.
3. Click **+ Add Step**.
4. In the **Step Type** list, select **Identifier First**.
5. Enter or edit the recovery and registration settings.

Copyright © 2025 Ping Identity Corporation

Setting	Description
Enable account recovery	In case of a forgotten password, users can recover their accounts with a one-time passcode (OTP) sent over email.
Enable registration	Users can register their own accounts if a user record already exists. Select **PingOne** to provision users to the PingOne user store. Select **External Link** to provision users to an external user store. PingOne will direct users to the **Registration Target URL** for registration, but PingOne will still be used for authentication.
Require confirmation of user information	If registration is enabled, requires end users to confirm the data that is linked with the third-party identity provider. The end user will have an opportunity to edit the information that the third-party identity provider (IdP) shares with PingOne, such as user name, email address, first name, and last name.
Discovery rules	Click **+Add rule** to add a rule, or **Edit rules** to modify an existing rule and complete the following fields: ◦ **Username Contains**: Enter a domain name to be evaluated by this rule. The rule will evaluate to true if the string contains any part of the provided value. > **Tip** > For increased security, be specific and enter multiple canonical domains, such as `@marketing.example.com` and `@payroll.example.com`. To add fewer entries, you could just enter `example.com`, and the rule would pick up both `@marketing.example.com` and `@payroll.example.com`, but that configuration might match users at unintended hosts. ◦ **Identity Provider**: Select the IdP to use for authentication if the rule is matched. Discovery rules are evaluated in the order they appear in the list. > **Note** > Users that don't match a discovery rule are authenticated against PingOne.

6. Enter or edit the requirement conditions.

   If this condition is met, the user will be required to sign on:

Last sign-on older than

Requires users to sign on if their previous sign-on is older than the configured value.

User attributes

Requires users to sign on if they match a specified user attribute, such as postal code or user ID. For example, `Postal Code = 78750`. Select the checkbox, then click **+ Add attribute**. Enter the attribute and the appropriate value. If you have multiple attribute conditions, the policy evaluates to true if any of the conditions are met (Boolean OR).

7. Enter or edit an external IdP. Click **+ Add Provider** and then select an identity provider from the list. If an IdP doesn't appear on the list, the IdP might not be enabled. Learn more in Adding an external identity provider.
8. To prevent users from signing on if their PingOne user account is locked, select **Block authentication of locked user accounts from Presented Identity Providers**. If this option is cleared, users can sign on with their configured IdP credentials, but not their PingOne credentials.
9. Click **Save**.

Related links

- Identifier first authentication
- Progressive profiling

Adding a progressive profiling step

To use progressive profiling, add it as part of an authentication policy.

About this task

> **Note**
> Because progressive profiling requires the user to be authenticated, it can't be the first step in the authentication policy. Create a login or multi-factor authentication step as the first step in the authentication policy.

Steps

1. Go to **Authentication > Authentication**.
2. Click **+ Add Policy** to create a new policy, or click the pencil icon to edit an existing one.
3. Click **+ Add Step**.
4. From the **Step Type** list, select **Progressive Profiling**.
5. Under Attributes, select a user attribute that you want to request. You can select any standard or custom string type attribute, including nested standard attributes (such as `name.family`), but not core or JSON type attributes.
6. Select **Required** if appropriate. If selected, the user will not be able to skip the prompt for requested information. The Skip button will not appear, and users will not be able to sign in until they provide the requested information. Be aware that this option may prevent users from signing in.
7. Click **Add attribute** to add another attribute (optional).

Copyright © 2025 Ping Identity Corporation

8. Enter the following information:
    - **Prompting text**. The text that the user will see before the requested profile information.
    - **Re-prompt every**. If the user skips entering the requested information, determines how soon the user will be prompted again. PingOne checks when the attributes were last updated by any progressive profiling action, such as a progressive profiling action or a progressive profiling form action. If all the attributes of the form have been updated within the specified time frame then the prompt will not be shown. This option applies to optional attributes only, because required attributes cannot be skipped.
    - **Show when: Another progressive profiling action has not already been shown**. If an authentication policy has multiple progressive profiling steps, show this step only if another progressive profiling step has not already been shown. This includes progressive profiling actions and progressive profiling form actions.
9. Click **Save**.

Related links

- Progressive profiling

Adding a terms of service prompt

You can require end users to consent to a terms of service agreement as part of a sign-on policy. For more information, see Agreements.

Steps

1. Go to **Authentication > Authentication**.
2. Click **+ Add Policy** to create a new policy, or click the pencil icon to edit an existing one.
3. Click **+ Add Step**.
4. From the **Step Type** list, select **Agreement prompt**.
5. Select the appropriate terms of service agreement. For information about creating a terms of service agreement, see Agreements. You can also preview the agreement to see how it will appear to end users.
6. Click **Save**.

Result

PingOne updates the authentication policy to include the selected terms of service agreement.

Adding an external identity provider sign-on step

If you configure an external identity provider (IdP) as part of a sign-on policy, end users can access your applications by authenticating with the IdP.

About this task

There are several ways an external IdP can be invoked to authenticate users. The external IdP sign-on step does so as a result of administrator declared policy, and the user is not given a choice. Learn more in External IdPs.

Copyright © 2025 Ping Identity Corporation

Depending on the sign-on policy, end users might bypass the PingOne sign-on prompt and be redirected to an external IdP to authenticate. A different sign-on policy could have end users use the PingOne sign-on prompt and then be redirected to an external IdP for second-factor authentication. The user must exist in PingOne, but the IdP manages authentication.

When using Microsoft as the external IdP, you must choose whether the policy is intended to authenticate users through the OpenID Connect (OIDC) protocol or to support an external authentication method (EAM) in Microsoft Entra ID.

Before you begin

- Set up a connection to your IdP.
- To support an EAM in Microsoft Entra ID, set up a connection to Microsoft.

Steps

1. Go to **Authentication** > **Authentication**.
2. Click **+ Add policy** to create a new policy, or click the **Pencil** icon to edit an existing one.
3. Click **+ Add step**.
4. In the **Step type** list, select **External identity provider**.
5. In the **External identity provider** list, select the IdP that will handle user authentication.
6. If Microsoft is selected for **External identity provider**, for **Policy Purpose**, select a method for users to authenticate:
   - **OIDC Authentication**: Select this option if you want users to authenticate with Microsoft using the OIDC protocol.
   - **Entra ID External Authentication Method**: Select this option if you want users to authenticate first with Microsoft Entra ID and then with PingOne as the external provider for multi-factor authentication (MFA). If you choose this option, skip to step 10.
7. Enter or edit the registration settings:

Setting	Description
Enable registration	Users can register their own accounts if a user record already exists.
Population	Specify which population will contain the newly registered users.
Require confirmation of user information	If enabled, this option requires end users to confirm the data that is linked with the third-party IdP. The end user will have an opportunity to edit the information that the third-party IdP shares with PingOne, such as user name, email address, first name, and last name.

8. Enter or edit the requirement condition.

   If this condition is met, the user will be required to sign on.

   - **Last sign-on older than**: Requires users to sign on again if their previous sign on is older than the configured value.

Copyright © 2025 Ping Identity Corporation

9. Enter or edit the IdP settings.

> **Note**
>
> These options are available only if you have an IdP sign-on step as a secondary step after a sign-on step that includes an IdP.

Setting	Description
Required authentication level	For SAML and OIDC identity providers, PingOne sends the `RequestedAuthnContext` or `acr_values` parameter to the specified IdP to indicate how the IdP should authenticate the user. This is commonly used to tell the IdP to use MFA, for example, to ensure the right level of authentication depending on the sensitivity of the target application.
Pass user context to provider	For SAML and OIDC identity providers, PingOne can be configured to include some user information in the authentication request. The information to include is determined as follows: ◦ If the user is linked to the IdP, pass the `external id` for the user. ◦ If the user is not linked to the IdP, and is identified in a previous sign-on step or existing session, pass the PingOne `username` for the user. ◦ If the user does not have an existing session, either from a previous transaction, or from completing a sign-on step before the external IdP step in the sign-on policy, pass the `loginHint` if it was received from the downstream application.

10. If the **Entra ID External Authentication Method** option is selected for **Policy Purpose**, click **+ Add step** and select **PingID Authentication** from the **Step type** list.

11. Click **Save**.

Next steps

If you're configuring an EAM in Microsoft Entra ID, add an OIDC application in PingOne and assign your authentication policy to your application. Learn more in Editing an application for the Microsoft Entra ID external authentication method.

Related links

- Adding a login authentication step
- Adding a multi-factor authentication or PingID step
- Adding an identifier first authentication step

Copyright © 2025 Ping Identity Corporation

Editing an authentication policy

Use the **Authentication** page to modify existing authentication policies in PingOne.

Editing a single-factor authentication policy

A single-factor authentication policy requires only one piece of evidence to verify a user's identity, such as a username and password.

1. In the PingOne admin console, go to **Authentication > Authentication**.
2. For **Single_Factor**, click the **Details** icon to expand the policy and then click the **Pencil** icon.
3. Enter or edit the **Login** settings:

Setting	Description
Enable account recovery	In case of a forgotten password, users can recover their accounts with a one-time passcode (OTP) sent through email.
Enable registration	Users can register their own accounts whether or not a user record already exists. Select **PingOne** to provision users to the PingOne user store. Select **External Link** to provision users to an external user store. PingOne directs users to the **Registration Target URL** for registration, but PingOne is still used for authentication.
Last sign-on older than	Requires users to sign on again if their previous sign-on is older than the configured value. **Note** The PingOne admin console uses a system policy that doesn't allow you to change this setting. The administrator must reauthenticate if they've been inactive for more than 30 minutes. If the administrator is active in the console within the 30-minute period, the session refreshes and reauthentication isn't necessary. MFA is required every 12 hours.

4. Enter or edit an external identity provider (IdP). Click **+ Add Provider** and then select an IdP from the list. If an IdP doesn't appear in the list, it might not be enabled. Learn more in Adding an external identity provider.
5. To prevent users from signing on if their PingOne user account is locked, select **Block authentication of locked user accounts from Presented Identity Providers**. If you leave this option cleared, users can sign on with their configured IdP credentials but not their PingOne credentials.

Copyright © 2025 Ping Identity Corporation

6. Click **Save**.

Editing a multi-factor authentication policy

A multi-factor authentication (MFA) policy requires two pieces of evidence to verify a user's identity, such as a username and password and a push notification to the user's mobile device or an OTP sent through SMS, voice, or email.

> **Note**
> The first step in a policy can't have population or user attribute conditions. Additionally, if the second step in a two-step policy has conditions set, and you delete the first step so that the second step becomes first, those conditions are removed.

1. In the PingOne admin console, go to **Authentication** > **Authentication**.
2. For **Multi_Factor**, click the **Details** icon to expand the policy and then click the **Pencil** icon.
3. Enter or edit the **Login** settings:

Setting	Description
Enable account recovery	In case of a forgotten password, users can recover their accounts with an OTP sent through email.
Enable registration	Users can register their own accounts whether or not a user record already exists. Select **PingOne** to provision users to the PingOne user store. Select **External Link** to provision users to an external user store. PingOne directs users to the **Registration Target URL** for registration but PingOne is still used for authentication.
Population	If registration is enabled, select the population to which the end user will be added.
Require confirmation of user information	If registration is enabled, end users must confirm the data linked with the third-party IdP. The end user can edit the information that the third-party IdP shares with PingOne, such as username, email address, first name, and last name.
Last sign-on older than	Requires users to sign on again if their previous sign-on is older than the configured value.

4. In the **MFA Policy** list, select an MFA policy. Learn more in MFA policies.
5. For **None or incompatible methods**, choose the MFA flow to use for MFA scenarios when users attempt to sign on but don't have any enrolled MFA devices that comply with the permitted **Available Methods**:
   - **Block**: Don't permit these users to sign on because they don't have a usable device for MFA.
   - **Bypass**: Allow users without a usable MFA device to bypass the MFA flow.

Copyright © 2025 Ping Identity Corporation

To leverage the **Bypass** option, the user must already be authenticated by a password (**Login** step) or by supplying a signed `login_hint_token` in the request object. Learn more about `login_hint_token` in the GET Authorize (Browserless and MFA Only Flows) operation in the PingOne Platform API Reference.

6. Enter or edit the MFA conditions. If one or more of the following conditions are met, the user is prompted to use a two-step authentication method:
   - **Last sign-on older than**: The previous sign-on is older than the configured value.
   - **Accessing from IP out of range**: The request comes from an IP address outside of the specified range. Use CIDR notation to specify the IP address range.
   - **Being a member of any of these populations**: The user belongs to the specified population or populations.
   - **User Attributes**: Requires users to sign on if they match a specified user attribute, such as postal code or user ID. For example, `Postal Code = 78750`. Select the checkbox and enter the attribute and the appropriate value. To add additional attributes, click **+ Add attribute**. If you have multiple attribute conditions, the policy evaluates to true if any of the conditions are met (Boolean OR).
   - **IP reputation is high risk**: PingOne collects and analyzes IP address data of authentication requests from the user's accessing device. An IP address is considered high risk if it could have recently been involved in malicious activities, such as DDoS attacks or spam activity. Select the checkbox to require MFA when authentication requests come from IP addresses with high risk scores.

     > **Note**
     >
     > The **IP reputation** option is a feature that is available only with a PingOne Protect or PingOne for Customers Passwordless license.

   - **A geovelocity anomaly is detected**. PingOne analyzes location data from the user's accessing device. It determines whether travel time between a user's current sign-on location and their previous sign-on location is possible in the time frame that has elapsed since the previous sign-on. Select the checkbox to require MFA when a geovelocity anomaly is detected.

     > **Note**
     >
     > The **Geovelocity anomaly** option is a feature that is available only with a PingOne Protect or PingOne for Customers Passwordless license.

   - **Anonymous network detection**: PingOne collects and analyzes IP address data of authentication requests from the user's accessing device. Select the checkbox to require MFA when PingOne identifies an IP address as originating from an anonymous network, such as an unknown VPN, proxy, or an anonymous communication tool (for example, Tor). Exclude IP addresses in the **Whitelist** by entering them in CIDR notation in a comma-separated list.

     > **Note**
     >
     > The **Anonymous network detection** option is a feature that is available only with a PingOne Protect or PingOne for Customers Passwordless license.

7. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Next steps

You can add more steps to the authentication policy. Click **+ Add step**, select the step type, and enter the values for the selected type.

Learn more in:

- Adding a login authentication step
- Adding a multi-factor authentication or PingID step
- Adding an identifier first authentication step
- Adding a progressive profiling step
- Adding a terms of service prompt
- Adding an external identity provider sign-on step

FIDO2

FIDO2 (Fast IDentity Online) allows your applications to authenticate users using public key-based credentials.

PingOne supports the use of the FIDO2 protocol, and the PingOne FIDO2 server is a FIDO2 certified product.

You can add FIDO2 as an authentication method for your end users. To set up FIDO2, edit an existing authentication policy or create a new one. For more information, see Editing an authentication policy and Adding a multi-factor authentication or PingID step.

FIDO2 with PingOne provides many security benefits, such as protection against phishing, man-in-the-middle, and replay attacks. PingOne includes the following security measures from the FIDO2 specification:

- Based on public key cryptography
- Ensures that private keys remain on the FIDO2 device only
- Does not employ server-side shared secrets that could otherwise be compromised
- Isolates services from accounts

Users can authenticate with:

- FIDO2 biometrics, by using a gesture in a compatible device
- FIDO2 security keys

FIDO2 biometrics

With FIDO2 biometrics, end users can authenticate using biometrics on compatible devices. Supported devices include Windows Hello, Android OS 7.0 or later, MacOS, and iOS. For FIDO2 biometrics, the authentication method is bound to a particular device, unlike other methods such as SMS, voice and email.

Copyright © 2025 Ping Identity Corporation

> **Note**
> FIDO2 biometrics can be used for web-based authentication only through browsers that support platform authenticators.

FIDO2 security keys

A hardware-based security key can be used to authenticate users, often in sensitive environments or environments with limited device or phone access, such as hospitals, financial institutions, or federal buildings. FIDO2 security keys are backward compatible with U2F, enabling PingOne to support both FIDO2 and U2F security keys.

After you enable a security key as part of an authentication policy, the user can use it to authenticate. Pairing the device creates a trust between the security key and the user account, so it can be used for authentication.

> **Note**
> Security keys can be used for web-based authentication only through browsers that support WebAuthn.

FIDO policy

You can configure one or more FIDO policy and include it in your MFA policy. You can create a FIDO policy for the use of FIDO2 Biometrics and FIDO2 security keys. Create a FIDO policy to define which FIDO devices and authenticators can be used for registration and authentication purposes, and to enable usernameless and passwordless authentication. For more information, see FIDO policies.

Related links

- Adding a multi-factor authentication or PingID step
- Editing an authentication policy

Progressive profiling

With progressive profiling, you can prompt a user for information to be added to their profile after the initial registration step. For example, you could prompt users to add their mobile phone number the next time they sign in.

You can use progressive profiling to minimize the amount of information you request during initial registration. After registration is complete, you can require or request additional information from the user.

You can also set up multiple progressive profiling steps within the same authentication policy to separate the steps by priority or by type. For example, the first step might request a single higher priority item, like a mobile phone number, with a more frequent prompt. The second step might request more lower priority items, with a less frequent prompt. You can set up each item to be required or optional.

For more information, see Adding an authentication policy.

Identifier first authentication

With identifier first authentication, also known as identity discovery, you can identify users before you authenticate them. You can set up rules that will take different authentication actions based on who the user is.

Copyright © 2025 Ping Identity Corporation

If the user name matches a configured rule, the system sends the user to a particular external identity provider. If the user name doesn't match a configured rule, the system sends the user to the regular password flow. For example, you could set up a rule to send employees to one identity provider, and contractors to another identity provider.

For more information, see Adding an authentication policy.

Setting up passwordless authentication

You can use passwordless authentication to enable a higher level of assurance for users without requiring them to remember complex passwords. With a passwordless authentication policy, users can sign in with only a username and a one-time passcode that is delivered over email or text message, or a mobile push notification.

> **Important**
>
> - Before enabling passwordless authentication, ensure that you have set up and validated a MFA device for you and your users, because they will not be able to sign on without a second factor.
> - We strongly discourage setting a passwordless policy as the default password policy.

1. Go to **Authentication** > **Authentication**.
2. Click **+ Add Policy**.
3. Enter a descriptive name for the policy, such as `Passwordless`.
4. From the **Step Type** list, select **Multi-Factor Authentication**.
5. From the **MFA policy** list, select the appropriate MFA policy. For more information about setting up MFA policies, see MFA.
6. Click **Save**.

Setting the default authentication policy

Use the **Authentication** page to configure the default authentication policy in PingOne.

> **Note**
>
> The default authentication policy doesn't apply to the PingOne admin console. The admin console uses a system policy configured in **Settings** > **Administrator Security** instead of the default policy. You can't assign a different policy to the admin console.

Steps

1. In the PingOne admin console, go to **Authentication** > **Authentication** and browse or search for the policy that you want to set as the default.
2. Click the **Expand** icon to expand the policy, and then click the **Pencil** icon.
3. At the top of the page, under the policy name, click **Make Default**.

Copyright © 2025 Ping Identity Corporation

Resolving a lockout

In most cases, PingOne will not allow you to create an authentication policy that would lock you out of your account. However, if you find yourself locked out of your account or otherwise blocked, you can contact Ping Identity to unlock it.

Steps

- If you are unable to access your account, contact support@pingidentity.com.

Password policies

A password policy dictates the strength and complexity requirements for a password or passphrase. You can choose or define a policy that fits the needs of your organization.

PingOne allows you to assign password policies to populations and includes three built-in policy types. You can customize these policies or create new policies to meet the password requirements for users in the population. Learn more in the following tables.

The built-in password policies include:

- Standard (default): The standard password policy incorporates industry best practices for a typical password policy. The standard policy is the default policy when the environment is created. The default policy is applied to populations for which another password policy has not been selected. You can later choose a different password policy to use as the default.
- Passphrase: The passphrase policy encourages users to use a passphrase instead of a password for stronger authentication. A passphrase can be easier to remember and more secure because of its length.
- Basic: The basic password policy is a more relaxed standard that allows for maximum customer flexibility. Because users are not required to change their passwords, the basic policy can be less secure.

Learn more about viewing, adding, modifying, or deleting password policies in Managing password policies.

Password policy comparisons

Review the following tables to compare the different rules and restrictions applied by each built-in policy.

Password Character Restrictions

Character Restriction	Standard Policy	Passphrase Policy	Basic Policy
Not the same as current password (always enabled).	Yes	Yes	Yes
Is not an exact match for any of the attribute values in the user profile.	Yes	Yes	No

Copyright © 2025 Ping Identity Corporation

Character Restriction	Standard Policy	Passphrase Policy	Basic Policy
Not similar to current password. **Note** PingOne checks the Levenshtein distance between the two passwords to ensure they are not too similar. The Levenshtein distance counts the number of characters added to, removed from, or replaced from the old password to the new password. If the Levenshtein distance is less than 3, then the password will be rejected as too similar. For example, changing a password from `kitten` to `smitten` would have a Levenshtein distance of 2, and be rejected as too similar.	Yes	Yes	No
Not a common password.	Yes	Yes	Yes
Has a computational complexity of at least 7 days, based on the Gibson Research Corporation Password Haystacks concept.	No	Yes	No
No more than two consecutive repeated characters. For example, `good-apple` is acceptable but `goood-appple` is not.	Yes	No	No
At least five unique characters.	Yes	No	No
Between 8 and 255 characters.	Yes	No	Yes
At least one of the following special characters: ~!@#$%^&*()-_=+[]\{}|;:,.<>/?	Yes	No	Yes
At least one number.	Yes	No	Yes
At least one uppercase letter.	Yes	No	Yes
At least one lowercase letter.	Yes	No	Yes
No more than two or three sequential numbers (configurable). For example, `123` or `432` are not acceptable if set to `2`, but would be acceptable if set to `3`.	No	No	No
No more than two or three sequential letters (configurable). For example, `abc` or `dcb` are not acceptable if set to `2`, but would be acceptable if set to `3`.	No	No	No
No more than three sequential QWERTY keyboard characters. For example, `qwer`, `rewq`, `zxcv`, or `vcxz` are not acceptable.	No	No	No
No more than three sequential symbol row characters. For example, `~!@#` or `#@!~` are not acceptable.	No	No	No

Copyright © 2025 Ping Identity Corporation

Character Restriction	Standard Policy	Passphrase Policy	Basic Policy
Supports all printable UTF-8 characters.	Yes	Yes	Yes

Password Policy Rules

Policy Rule	Standard Policy	Passphrase Policy	Basic Policy
Previous passwords maintained in history for 1 year	6	6	None
Password expires after	182 days	Never	182 days
User can change their password after	1 day	1 day	Never

Account Lockout Rules

Lockout Rule	Standard Policy	Passphrase Policy	Basic Policy
Allowed failed attempts	After five failed attempts, the user is locked out	5	5
Automatic unlock period	Accounts locked after maximum failed attempts are unlocked after 15 minutes	15 minutes	15 minutes

Managing password policies

Use the **Password** page to manage password requirements and rules for your environment.

Click the corresponding tab for instructions about:

- Viewing all policies and policy details
- Adding a policy
- Modifying a policy
- Deleting a policy

Copyright © 2025 Ping Identity Corporation

View password policies

Viewing password policies

Use the **Password** page to view existing password policies in your environment.

Steps

1. In the PingOne admin console, go to **Authentication** > **Password**.
2. Click a policy to view the policy details.
   - The **Overview** panel shows a count of populations using the policy and provides a link to the **Populations** page.
   - The **Configuration** panel shows the configured rules and requirements for the policy.

Add a password policy

Adding a password policy

Use the **Password** page to add a password policy to your environment.

Steps

1. In the PingOne admin console, go to **Authentication** > **Password**.
2. Click the **+** icon to add a policy.
3. Enter a **Name** and **Description** for the policy, then click **Next**.
4. Choose a template for the policy and modify to fit password requirements for users in the population, if applicable.

   Choose from:

   - Standard
   - Passphrase
   - Advanced

     Learn more about the password rules and character restrictions included in each of the built-in password policies in Password policies.

   > **Note**
   > Modifying the **Standard** and **Passphrase** templates automatically creates an **Advanced** policy.

5. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Edit a password policy

Editing a password policy

Use the **Password Policies** page to edit existing password policies in your environment.

Steps

1. In the PingOne admin console, go to **Authentication** > **Password** and browse or search for the policy that you want to edit.
2. Click the **More Options** (⋮) icon for the policy and select **Edit Password Policy**.
3. Make the appropriate changes. Learn more about password policy settings in Password policies.
4. (Optional) Select **Set as default policy** to assign this password policy to any population for which a password policy is not explicitly selected.
5. Click **Save**.

Delete a password policy

Deleting a password policy

Use the **Password** page to remove existing password policies from your environment.

Steps

1. In the PingOne admin console, go to **Authentication** > **Password** and browse or search for the policy that you want to delete.
2. In the list on the right, select **Delete**.
3. When prompted, click **Delete** to confirm.

> **Note**
> You cannot delete a policy that is assigned to a population. If the password policy is in use, you must first assign a new password policy to the affected populations.

MFA policies

Use the **MFA Policies** page to create, update, or delete MFA policies. After creating an MFA policy, you can refer to it in any authentication or registration flow designed in PingOne, PingOne DaVinci, PingID, or the PingOne MFA API.

An MFA policy allows you to define and configure the authentication methods that you want to use in your authentication policy. The MFA policy is then added as an MFA step in your authentication policy.

Copyright © 2025 Ping Identity Corporation

An MFA policy includes the following configuration information:

- The authentication methods that the policy allows
- The configurations specific to the authentication method, such as how many failed passcode attempts are allowed and how long users should be blocked after passcode failure

Default MFA policy

When you create a new environment, a default MFA policy is added to the **MFA Policies** page automatically.

- PingOne MFA:

  You can modify the default policy. For PingOne MFA you can also create additional MFA policies. The default policy serves the following purposes:

- When defining an authentication policy in PingOne, you can add an MFA step and select the **Use Default Policy** option. This means that the authentication policy will use whatever MFA policy is currently set to be the default MFA policy for the environment.
- The DaVinci PingOne MFA connector includes a policy ID in its configuration. If you do not specify an MFA policy, the connector will use whatever MFA policy is currently set to be the default MFA policy for the environment.
- In the PingOne MFA API, there are calls that allow you to specify a particular MFA policy to use. In these situations, if you do not specify an MFA policy, the flow will use whatever MFA policy is currently set to be the default MFA policy for the environment.

Adding an MFA policy

Create a multi-factor authentication (MFA) policy and then add it as a step to your authentication policy.

For details about how to configure an MFA policy, see Configuring an MFA policy for strong authentication.

You can find more information in Updating an existing MFA policy to use FIDO2.

FIDO policies

FIDO policies define which FIDO devices and authenticators can be used for registration and authentication purposes. FIDO allows you to authenticate users using public key-based credentials.

PingOne supports the use of the WebAuthn standard, and the PingOne FIDO2 server is a FIDO2-certified product.

FIDO2 with PingOne provides many security benefits, such as protection against phishing and replay attacks. PingOne includes the following security measures from the FIDO2 specification:

- Based on public key cryptography
- Does not employ server-side shared secrets that could otherwise be compromised

Copyright © 2025 Ping Identity Corporation

- Isolates services from accounts

FIDO2 devices can include:

- FIDO2 biometrics and security keys.
- Passkeys. Passkeys allow cloud-synched credentials so that users can access their FIDO sign-in credentials on many of their accessing devices, even new ones, without having to re-enroll every device on every account.

FIDO2 devices and authenticators can be used for registration and authentication purposes and to enable usernameless and passwordless authentication.

You can also view, search, add, or delete FIDO devices in the **Global Authenticators Table**. Learn more in Managing the Global Authenticators Table.

FIDO2 integration modes

PingID supports the following FIDO2 integration modes:

- PingID's out of the box solution, using the PingID UI and the pingone.com domain. Learn more in:
  - Using Windows Hello for authentication
  - Using Apple Mac Touch ID for authentication
  - Using a security key (FIDO2) for authentication
  - Using Android biometrics for authentication
- API-based, using a custom UI that is not hosted by PingID, and a custom domain. Learn more in:
  - FIDO pairing workflow
  - FIDO authentication workflow
  - FIDO passwordless authentication workflow
- Hybrid mode, also API-based using a custom UI for registration that is not hosted by PingID, and PingID's default UI for authentication. This mode leverages the pingone.com domain. Learn more in PPM request for FIDO authentication with a hybrid UI.

Related links

- Adding a FIDO policy

Adding a FIDO policy

To enable authentication with FIDO2 devices, first create one or more FIDO policies.

About this task

> **Note**
>
> A small number of the options listed aren't available for use with PingID accounts that are integrated with **PingOne**. Learn more about Updating a PingID account to use a PingOne FIDO2 policy.

Copyright © 2025 Ping Identity Corporation

To enable authentication with FIDO2 devices:

1. Create a FIDO policy defining which FIDO devices are permitted and the desired behavior when registering and authenticating your users. This task is described in detail in this topic.
2. Include the FIDO policy in the relevant MFA policy. For PingOne MFA, you can find more information in MFA policies and for PingID, you can find more information in Configuring an MFA policy for strong authentication.
3. Ensure the MFA policy is included in the MFA step of the relevant Authentication policy. You can find more information in Adding a multi-factor authentication or PingID step.

> **Note**
>
> When creating an environment, the following out-of-the-box (OOTB) FIDO policies are created by default:
>
> - Passkeys (default)
> - Security key
>
> These policies represent best practice configurations for registration and authentication of the relevant devices. You can change the default policy if required.

Steps

1. Go to **Authentication → FIDO**.
2. On the **FIDO Policies** page, click the **+** icon.
3. In the **Name** field, enter a meaningful name for the policy.

   There is a 256 character maximum.
4. In the **Device Display Name**, select the format in which you want the device to be displayed on self-service registration and authentication windows.

   Choose from:

   - **Label**: Free text field. The device name that is not translated.
   - **Translatable Keys**: Select an option from the list of translatable keys. The key is translated into the relevant language.

     > **Note**
     >
     > The list of translatable keys can be modified on the **FIDO policy** page for the relevant language. The FIDO policy page should be updated in the **Self-Service** module and the **Sign On Policy**module. You can find more information in Languages.
5. In the **FIDO Device Aggregation** field, select either:

   Choose from:

   - **Yes**: During authentication, aggregate all FIDO devices paired with a user's account and present them to the user as a single authentication method. The user's OS selects the most appropriate FIDO device with which to authenticate.
   - **No**: Present each FIDO device to the user as a separate device during authentication.

Copyright © 2025 Ping Identity Corporation

6. In the **Relying Party ID** field, select the relevant Relying Party ID (RPID):
   - **PingOne** (default): Use the PingOne RPID (such as pingone.com).
   - **Custom Domain**: Use the active custom domain for the selected environment. Learn more about custom domains in Domains.

     > **Note**
     > This option is not currently available for PingID.

   - **Other**: Enter a valid domain.

     > **Note**
     > For **Sandbox** environments in PingOne, you can also use the value `localhost` .

7. In the **Discoverable Credentials** field, select one.

   Discoverable credentials make it possible for registered users to authenticate without providing credentials.

   Choose from:

   - **Discouraged**: Discoverable credentials are not used, even when supported by the FIDO device. In cases where use of discoverable credentials is required by the FIDO device itself, this setting does not override the device setting.
   - **Required**: Require the use of discoverable credentials. This option is required for usernameless authentication.
   - **Preferred** (default): Use discoverable credentials where possible.

8. In the **Authenticator Attachment** field, select the type of authenticator that can be used to register.

   Choose from:

   - **Platform**: Only allow the use of FIDO device authenticators that contain an internal authenticator (such as a face or fingerprint scanner).
   - **Cross-platform**: Allow use of cross-platform authenticators , that are external to the accessing device (such as a security key).
   - **Both** (default).

9. In the **Public Key Credential Hints** field, select the authenticator that you want to present to the user during pairing. The selection is considered as a 'hint' to the authenticator.

   > **Note**
   > When defining Public Key Credentials Hints, make sure the options you select do not conflict with the **Authenticator Attachment** value.

   - **Security Key**: The user is likely to use a security key. If selected, **Authenticator Attachment** should be set to **Cross-platform**.
   - **Client Device**: The user is likely to use a platform authenticator attached to a client device (such as Touch ID, Face ID or Windows Hello). If selected, **Authenticator Attachment** should be set to **Platform**.

Copyright © 2025 Ping Identity Corporation

- **Hybrid**: The user is likely to use a mobile device or tablet for cross-device authentication using a QR-code or bluetooth. If selected, **Authenticator Attachment** should be set to **Cross-platform**.

10. In the **User Verification** field, select one.

    User verification requires the user to perform a gesture (such as a public key credential, fingerprint scan, or a PIN code) when using their FIDO device.

    1. In the **User Verification** field, select either:

       - **Discouraged**: User verification is not performed, even when supported by the FIDO device. In cases where user verification is required by the FIDO device itself, this setting does not override the device setting.
       - **Required**: Only FIDO devices supporting user verification can be used.
       - **Preferred** (default): User Verification is performed if the user's FIDO device supports it, and it is skipped if it is not supported.

       > **Note**
       > For usernameless flows, **User Verification** must be set to **Required**.

    2. To apply user verification to authentication as well as registration, select the **Enforce during authentication** checkbox.

11. In the **Backup Eligibility** field, indicate whether you allow users to authenticate with a device that uses cloud-synced credentials, such as a passkey.

    Options are **Allow** or **Disallow**.

12. In the **User Display Name** area, do the following:

    1. Select up to six attributes that can be used to populate the **User Display Name** and place them in order of preference. The **User Display Name** is a human-readable name associated with the user's account.

       > **Note**
       > You can select any OOTB user profile attributes. The first attribute that contains valid data is used to populate the **User Display Name**. It is displayed to the user during registration and authentication.

    2. To help users identify their passkeys, you can include **Additional Display Information**. Select the relevant checkbox:

       - **Include Environment Name**
       - **Include Organization Name**

       This information displays on the popup window that appears when a user adds a passkey as an authentication method.

13. In the **Attestation Request** area:

    1. In the **Attestation Type** field, select specify the level of either:

       - **None**: Do not require attestation for FIDO devices.

Copyright © 2025 Ping Identity Corporation

- **Direct**: Audit or allow FIDO devices that comply with the defined Attestation Requirements.
- **Enterprise**: Verify that the device is an Enterprise FIDO device. Optionally, require the user to use a FIDO device that matches the **Custom Attribute Defining User's Serial Number**.
  - In the **Custom Attribute Defining User's Serial Number** field, select either:
    - **<custom attribute>**: Only allow users to register FIDO devices with a serial number that matches the value defined by the custom user attribute.

      Learn more about custom attributes in Add custom attributes to a user
    - **Not Defined**: Allow users to register enterprise FIDO devices regardless of the serial number.

> **Note**
> Windows login doesn't support the use of FIDO2 security keys with enterprise attestation.

2. In the **Attestation Requirements** field, select one of the following.

   Choose from:

   - **None**: Allow all FIDO devices and don't request attestation.
   - **Audit only**: Request attestation for auditing purposes only.
   - **Allow All Global**: Allow use of all FIDO devices listed in the Global Authenticators table and request attestation.
   - **Allow FIDO Certified Authenticators**: Only allow use of FIDO Certified devices, and request attestation.

     > **Note**
     > To add a FIDO device to the **Global Authenticators Table**, see Managing the Global Authenticators Table.

   - **Allow Specific Authenticators**: Allow use of only the devices specified. Select this option and then select the devices you want to use in the **Allowed Authenticators table** below the list.

3. To prevent users from authenticating with other devices that are already registered with their account, but are not included in the **Allow Specific Authenticators** list, select the **Enforce during authentication** check box.

   > **Note**
   > This option can be applied only to devices that included a FIDO resident key during the registration process.

14. In the **User Presence Timeout** field, define the amount of time the user has to perform a user presence gesture with their FIDO device before the request expires (the default is two minutes). The value is considered a hint because the browser's FIDO authenticator defines the actual timeout value.

15. Click **Save**.

    Result:

    The policy is added to the **Policy** list.

Copyright © 2025 Ping Identity Corporation

> **Tip**
> In the **Policy** list, click a policy to see a summary of the policy details in the right pane or edit an existing policy.

Next steps

Add the FIDO policy to the MFA step in the relevant Authentication policy. For information, see Adding a multi-factor authentication or PingID step.

Managing FIDO policies

You can edit, rename, or delete a FIDO policy. You can also change the default policy.

About this task
Steps

1. Go to **Authentication > FIDO**.

   Result:

   The **FIDO Policies** window opens showing a list of FIDO policies.

2. In the FIDO policies list, in the relevant row do any of the following:

Option	Description
Edit a policy	Select **More Options (⋮)** and edit the relevant fields.
Change default policy	Next to the policy you want to make the default policy, select **More Options (⋮)** and click **Make Default**.
Rename a policy	Select **More Options (⋮)** click **Rename**.
Delete a FIDO policy	Select **More Options (⋮)** and click **Delete**.

3. Click **Save**.

> **Tip**
> In the policy list, click a policy to see a summary of the policy details in the right pane or edit an existing policy.

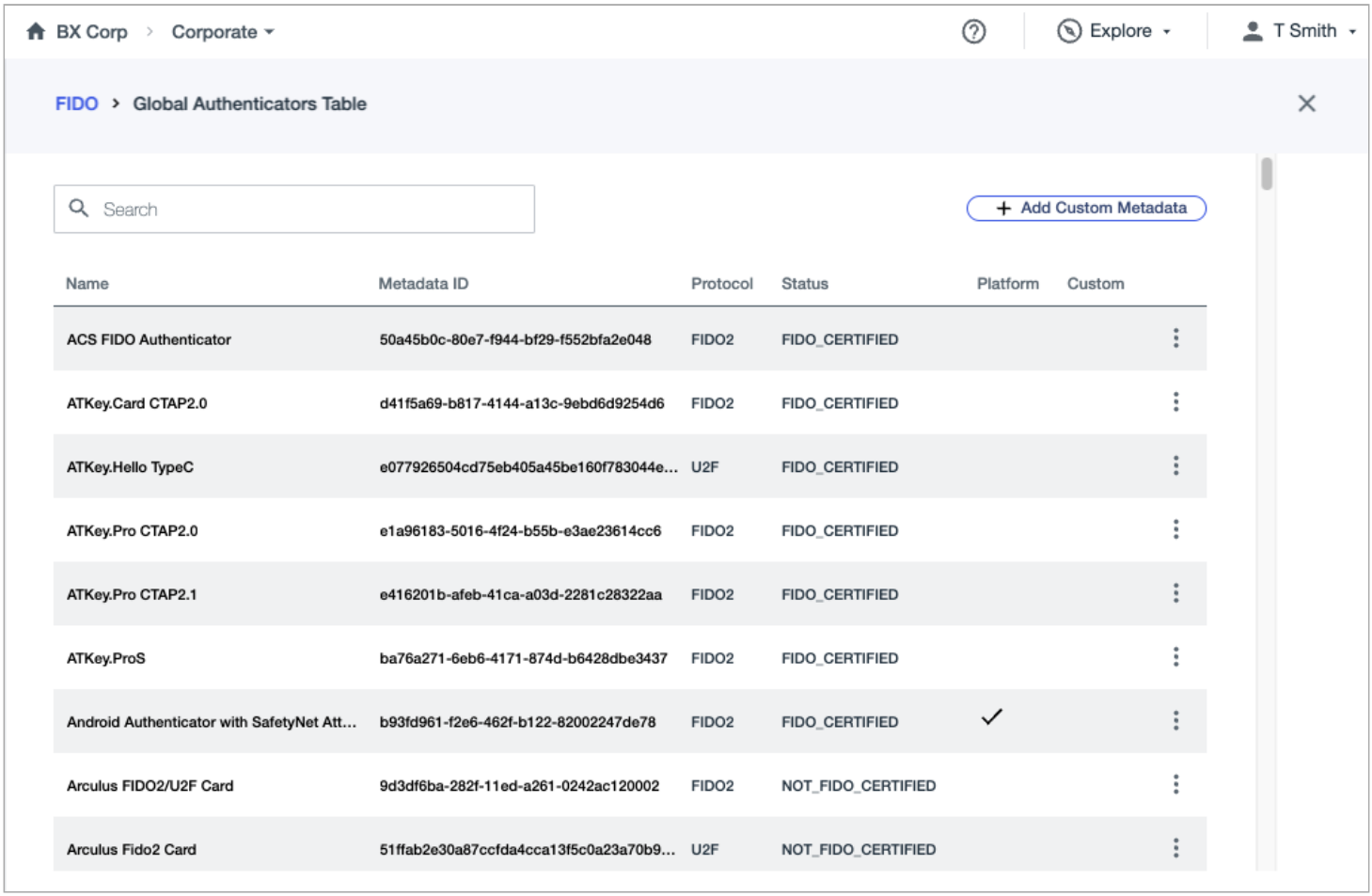
Managing the Global Authenticators Table

The **Global Authenticators Table** includes a list of devices obtained and regularly updated through the FIDO Alliance Metadata Service (MDS). Only devices listed in the **Global Authenticators Table** can be used in a FIDO policy.

About this task

The table also indicates which devices are **FIDO Certified** and the protocol supported for each device. You can add your own custom devices to the list. You can also download the metadata of an existing FIDO device and use it to create a custom entry.

Copyright © 2025 Ping Identity Corporation



Steps

1. Go to **Authentication > FIDO** and click the **Global Authenticators Table** link.
2. Do any of the following:

Option	Description
View device details	◦ In the relevant row, click the **More Options** (⋮) menu and select **View**. A popup window opens displaying the JSON for that device.
Download device details	◦ In the relevant row, click the **More Options** (⋮) menu, select **Download**, and save the JSON file that is created.
Add custom metadata	◦ Click **+ Add Custom Metadata** and select the JSON file that you want to add. Click **Open**. The device is added to the table. In the **Custom** column, a check mark indicates that it is a custom device.

Copyright © 2025 Ping Identity Corporation

Option	Description
Delete a custom device	◦ In the relevant row, click the **More Options** (⋮) menu and select **Delete**. **Note** You can delete only custom devices from the **Global Authenticators Table**.

MFA Settings

Use the **MFA Settings** page to configure the maximum number of MFA methods that a user can set up for authentication, authentication method selection, and account lockout settings.

Configuring MFA settings

You can define MFA settings for end users, such as the maximum number of methods that a user can set up for authentication, authentication method selection, as well as account lockout settings. These settings are applied at the environment level.

Steps

1. Go to **Authentication > MFA Settings**.
2. For **MFA status for new users**, specify whether MFA should be enabled by default for a user when their account is created.
3. For **Maximum allowed methods**, select the maximum number of authentication methods that users can set up for their accounts. The default is 5. Users can have multiple authentication methods using the same device. For example, an end user could have SMS, voice, biometrics, and an authenticator app all on a single mobile device.

   > **Note**
   > If you reduce the maximum value, existing methods are not affected. For example, if a user has four authentication methods set up, but you reduce the maximum number to three, the user won't have to remove an existing authentication method.

4. If some of your users will be pairing devices that have phone numbers with extensions, set the **Phone numbers with extensions** option to **Enabled**.
5. For **Account lockout**, enter or edit the following:
   - **Account lockout**: The maximum number of incorrect MFA authorization actions a user can attempt (such as entering an incorrect OTP or declining a push confirmation on a mobile device) before the account is locked.

     > **Note**
     > This value includes MFA authentication attempts across all configured devices.

   - **Account lockout duration**: The amount of time (in seconds) to keep the account locked after the failure count is exceeded. The account will automatically unlock after the specified time passes.

Copyright © 2025 Ping Identity Corporation

6. Select the type of key to use for pairing of devices: **12-digit numeric** key or **16-character alphanumeric** key.
7. Click **Save**.

Next steps

You can unlock or disable a user account on the user details page. Learn more in Enabling or unlocking a user account or device.

Step-up authentication for APIs

Step-up authentication enables you to require users to provide additional levels of authentication when they access sensitive API resources or perform high-risk actions.

Step-up authentication is also known as just-in-time authentication or route-based authentication. It allows your organization to reduce friction during the authentication experience while ensuring that sensitive resources are protected. For example, a bank might require only a basic level of authentication when customers view available banking products, but require an additional authentication method when they view their account balance or transaction history.

Step-up authentication has the following benefits:

- Balances a frictionless authentication experience with the need for increased security
- Limits MFA fatigue by asking for additional authentication only when it's needed
- Protects critical assets or high-risk resources that only certain users need to access
- Reassures users that their sensitive data is safe

When to use step-up authentication

Use step-up authentication when you want to guarantee that users are always required to provide an additional authentication factor when they try to access sensitive data or perform high-risk actions.

Specific kinds of API resources can be more sensitive than others, such as salary data, health records, or premium content. Before you allow a client to access these resources, you can use step-up authentication to require that:

- The user authenticated with a higher-level authentication policy
- The user authenticated recently

How is step-up authentication different from MFA?

With MFA, users must always present two or more authentication factors to verify their identity, such as a password and a one-time passcode (OTP) sent to their device.

With step-up authentication, users are allowed to access certain resources with one level of authentication, while more sensitive resources are protected by an additional level of authentication. Higher-level authentication is required only when it's needed.

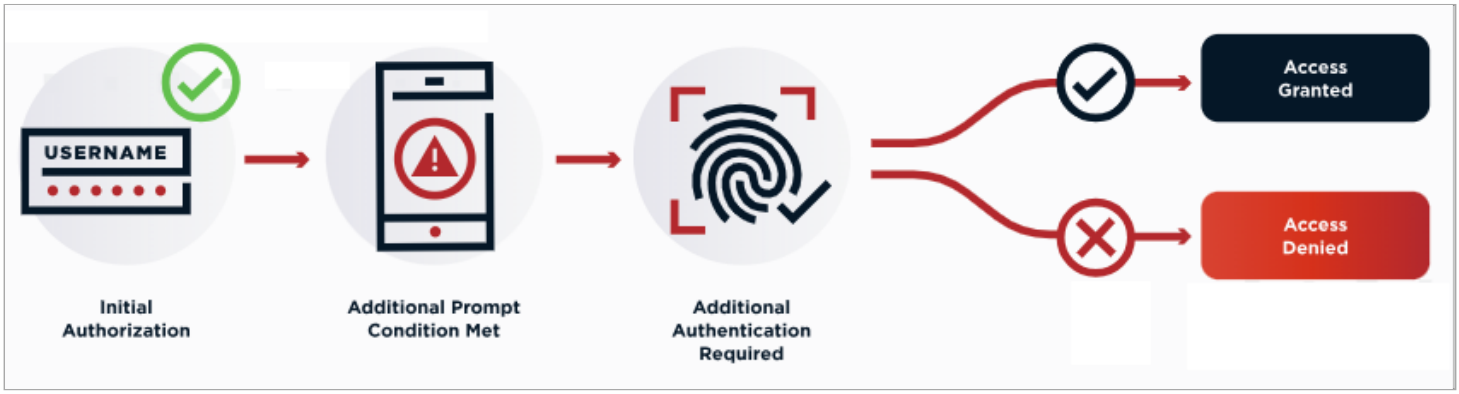
You can learn more about authentication levels in NIST authenticator assurance levels.

Copyright © 2025 Ping Identity Corporation

How it works

Step-up authentication uses PingOne in combination with your API gateway to require higher-level authentication for sensitive resources. You define authentication policies for an application with DaVinci or PingOne SSO, then use PingOne API Access Management in conjunction with your API gateway to protect your sensitive resources.

The following diagram and steps represent a typical step-up authentication flow:



1. A user accesses an application with a basic level of authentication.

   The authorization server issues an access token that the client application uses to request resources. For example:

   ```
   GET /secrets HTTP/1.1
   Host: example.com
   Authorization: Bearer eyJ0eX
   ```

   The access token includes claims related to authentication requirements:

   - `acr`: The name of the authentication policy used to satisfy the authentication event.
   - `auth_time`: The timestamp of the authentication event, expressed in epoch seconds.

2. The user requests access to a sensitive resource, meeting a condition that requires additional authentication.

   The resource server checks the `acr` and `auth_time` claims in the client's access token and determines that authentication requirements are not met. The resource server rejects the request and issues a challenge response. For example:

   ```
   HTTP/1.1 401 Unauthorized
   WWW-Authenticate: Bearer error="insufficient_user_authentication",
     error_description="A different authentication level is required",
     acr_values="strong_authentication_policy", max_age=300
   ```

   The challenge response includes the following details about authentication requirements:

   - `insufficient_user_authentication` error code: Tells the client that the user needs to reauthenticate.
   - `acr_values`: A list of acceptable authentication policies.

Copyright © 2025 Ping Identity Corporation

- `max_age`: The allowable elapsed time in seconds since the last active authentication event associated with the access token.

3. The user is prompted to reauthenticate with higher-level factors.
   - The client parses the challenge response. The error code indicates that the user needs to reauthenticate.
   - The client requests a new access token from the authorization server based on the `acr_values` and `max_age` provided in the challenge response. For example:

     ```
     GET /<envId>/as/authorize?
     client_id=<clientId>&scope=secret&response_type=code&redirect_uri=<redirectUri>&state=<state>&acr_values=
     Host: auth.pingone.com
     ```

   - The authorization server prompts the user to reauthenticate with the policy named in `acr_values`.

4. The user reauthenticates.

   If authentication is successful, the authorization server issues a new access token that includes the necessary claims.

5. If authentication is successful, the user requests access to the sensitive resource.
   - The client requests access to the sensitive resource with the new access token.
   - The resource server fulfills the request if the authentication policy matches the `acr_values` requested in the challenge response, or `max_age` is not exceeded.
   - The resource server denies the request if the authentication policy doesn't match the `acr_values` requested in the challenge response, or `max_age` is exceeded.

You can learn more about authentication challenges and bearer token usage in RFC 9470 and RFC 6750.

When you use PingOne for step-up authentication, PingOne SSO acts as the authorization server. PingOne API Access Management acts on behalf of the resource server to enforce authentication requirements and issue challenge responses when requirements aren't met.

Learn more in Setting up step-up authentication for APIs.

Setting up step-up authentication for APIs

Use step-up authentication in applications that require stronger authentication methods for access to sensitive resources.

To access an API resource, applications provide an access token. Step-up authentication uses the `acr` claim in the access token to ensure that users authenticate with a higher level of assurance when they access a sensitive API resource and the `auth_time` claim in the access token to ensure that they've authenticated recently. Learn more about step-up authentication for APIs.

Complete these high-level steps to set up step-up authentication.

Before you begin

Copyright © 2025 Ping Identity Corporation

To set up step-up authentication, you'll need:

- An API gateway that's integrated with PingOne Authorize. Learn more in PingOne Authorize API gateway integrations.
- A PingOne environment that includes the PingOne SSO and PingOne Authorize services.
- If you're using DaVinci authentication policies, your environment must include DaVinci.

Steps

1. Register your application in PingOne.

   > **Important**
   >
   > The **Application Type** must be **OIDC Web App**, **Native**, or **Single-Page**. Step-up authentication isn't supported for client applications that use the SAML or WS-Fed protocols.

2. Add the authentication policies you want to use for identity verification.

   Ensure that you have policies for basic authentication and for higher levels, such as MFA. You can use DaVinci or PingOne policies. Learn more in:

   - Adding a PingOne authentication policy
   - Creating a DaVinci authentication flow

3. Assign authentication policies to your application.

   > **Important**
   >
   > You can assign either DaVinci or PingOne policies to your application, but not both types at the same time.

4. Add an API service to register your protected API resources in PingOne.

   If you'll use custom policies for step-up authentication instead of basic rules, make sure that you enable custom policies for the API service.

5. Define API operations with basic rules for authentication policies and time since last authentication.

6. Deploy the API service.

Next steps

Configure your client application to handle 401 challenge responses with authentication policy (`acr_values`) and maximum authentication age (`max_age`) requirements. Your application should parse the challenge response, construct an appropriate OAuth 2.0 request, then try again with the new access token.

> **Important**
>
> Avoid getting caught in a loop if requests are repeatedly denied when authentication requirements aren't met.

Copyright © 2025 Ping Identity Corporation

Strong Authentication (MFA)

Multi-factor authentication (MFA) is a service that enables Customer and Workforce users to securely authenticate using a range of authentication methods.

Getting started with strong authentication (MFA)

What do you want to do?

- Start a PingOne trial
- Create an new environment for strong authentication (MFA)
- Integrate an existing PingID account or PingOne environment for MFA

What do you want to know?

- What is strong authentication (MFA)?
- Overview of authentication methods
- What is the difference between PingID and PingOne MFA?
- What is a typical strong authentication (MFA) workflow?

Configuring strong authentication

- Configure strong authentication methods
- Configure an MFA policy for strong authentication
- Create an Authentication policy
- Configure PingID policy
- Configure PingID Offline MFA
- Configure a passwordless Windows login application in PingOne
- Strong authentication (MFA) integrations
- Strong authentication monitoring and dashboards

Copyright © 2025 Ping Identity Corporation

Managing PingID in PingOne

- Manage PingID devices through MyAccount
- Bypass MFA for a specific user
- PingID language support
- PingID user life cycle management

Troubleshooting

- Audit logs
- System status
- Knowledge Base

Developer resources

- Get started with PingOne APIs
- PingOne Platform API Reference - PingOne MFA
- PingOne MFA Native SDK

Further resources

All other actions are managed by the PingID admin portal. Learn more in the PingID Administration Guide

Copyright © 2025 Ping Identity Corporation

Introduction to strong authentication (MFA)

Strong authentication allows administrators to require users to provide multiple verification factors before granting access. PingID provides a solution for Workforce scenarios, and PingOne MFA provides a solution for Customer scenarios.

A common security challenge is verifying that a user requesting access to a protected resource is who they claim to be and that they're permitted to access the requested resource. Protected resources use an authentication service to verify the requesting end user's authenticity.

Multi-factor authentication (MFA)

MFA is a process that uses two or more factors to verify an identity.

These factors include:

- Knowledge factors: Something you know, such as a username and password, a PIN, or the answer to a particular challenge. Considered weak authentication factors, knowledge factors pose a medium-to-high risk to vulnerability and exposure to unauthorized and unintended users.
- Possession factors: Something you have, such as an email address, phone number, hardware token, mobile device, or security key. Considered stronger than knowledge factors because they are mainly physical devices with a unique ID and should be secure in the possession of their owner.
- Inherent factors: Something you are, such as a biometric identifier like a fingerprint, voice, or face recognition. Considered the strongest authentication factors and pose the lowest risk to security vulnerability.

You can find a list of supported authentication methods in Overview of authentication methods. PingOne strong authentication (MFA) can be implemented for your:

- Customers (PingOne MFA): Secure authentication for customers of your organization.
- Workforce (PingID): Secure authentication for your organization's employees and contractors using PingID.

Overview of authentication methods

Learn about the multi-factor authentication (MFA) methods available for strong authentication.

Several authentication methods are available for strong authentication. Some are only for Workforce use cases, some are only for Customer use cases, and some can be used for both use cases.

Authentication methods are enabled and configured in the MFA policy. Learn more in Configuring an MFA policy for strong authentication.

Some authentication methods require additional configuration, and some have specific requirements and limitations. Learn more in Configuring strong authentication methods (MFA).

The following sections provide a summary of available authentication methods.

Copyright © 2025 Ping Identity Corporation

(Workforce only) PingID mobile app

Your workforce users can download an app to their mobile device and use it to sign on to your company services and applications with the added security of MFA. They can also use the app to verify their identity to an employer. The app provides several ways to authenticate and can be used when offline.

The app is fully configurable and includes a rich set of features, such as:

- Limiting the device type, OS, and app versions that can be used
- Preventing the use of rooted or jail-broken devices
- Enforcing version updates

It can also be used with Mobile Device Management (MDM).

Use PingID mobile app to authenticate using:

Biometrics: Fingerprint or Facial recognition

Biometrics authentication uses a device's native capability to scan and authenticate the user's fingerprint or face.

- Fingerprint authentication is supported on devices that support biometrics and are running the PingID mobile app on a supported OS.
- Authentication by facial recognition is model-dependent for Apple and Android devices. Learn more in iPhone and iPad models that support Face ID in the Apple documentation.

Both facial recognition and fingerprint authentication results are transparently passed through to the PingID app.

You can set the biometrics authentication rollout mode with the following settings:

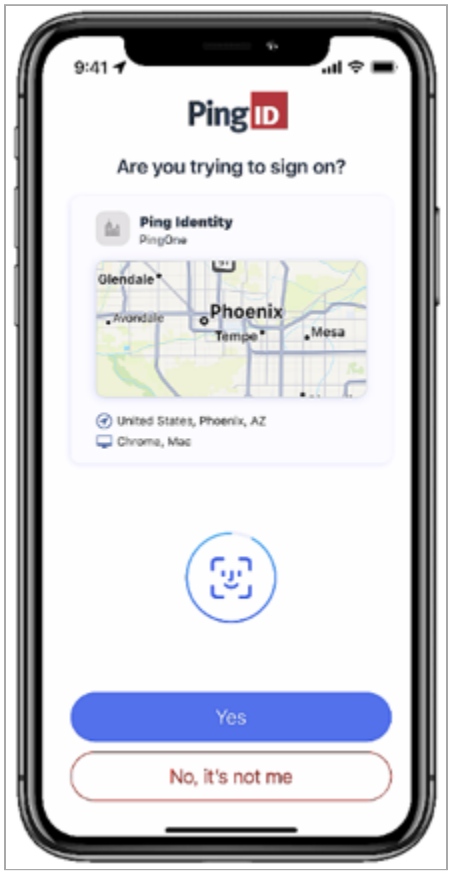
- Enable and disable mobile biometrics in the PingID Mobile App MFA policy settings.
- Define mobile biometrics settings in the PingID mobile application settings.

  Configure mobile biometrics as either:

  - **Preferred**: If mobile biometrics are defined on the user's device, the user must use them to authenticate. If the user doesn't have biometrics defined on the device, they are prompted to use the Approve method.
  - **Required**: Users must configure mobile biometrics on a supported device and can only use biometrics to authenticate. You can optionally allow iOS users to authenticate from the lock screen or use a one-time passcode (OTP) as a fallback if biometrics are not available.

  To prevent users with FaceID defined from authenticating by mistake, you can also configure PingID mobile app to explicitly request consent before each face scan is taken.

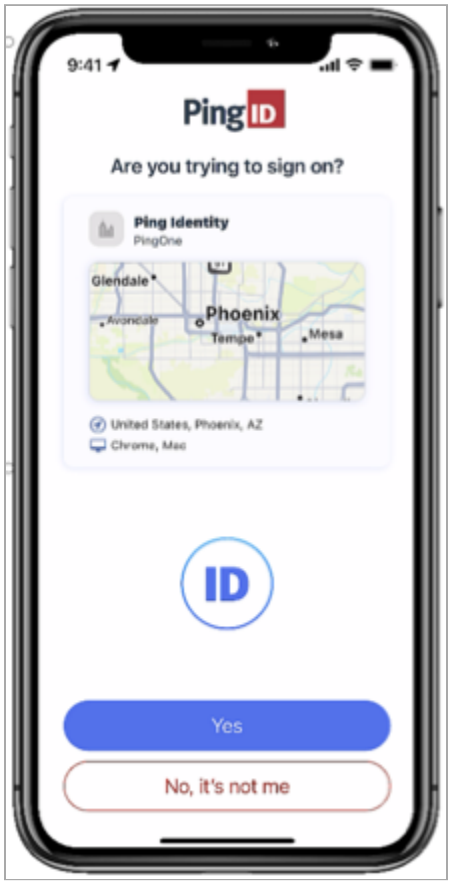
Copyright © 2025 Ping Identity Corporation



Approve a notification or Approve from Lock Screen

A push notification is sent to the user's device to let them know they need to authenticate. If PingID mobile app is open, they can tap **Yes** to authenticate. If their phone is locked, or if PingID mobile app is locked, the user might be able to authenticate from the lock screen. Long-tap the notification or swipe down and tap **Yes**.

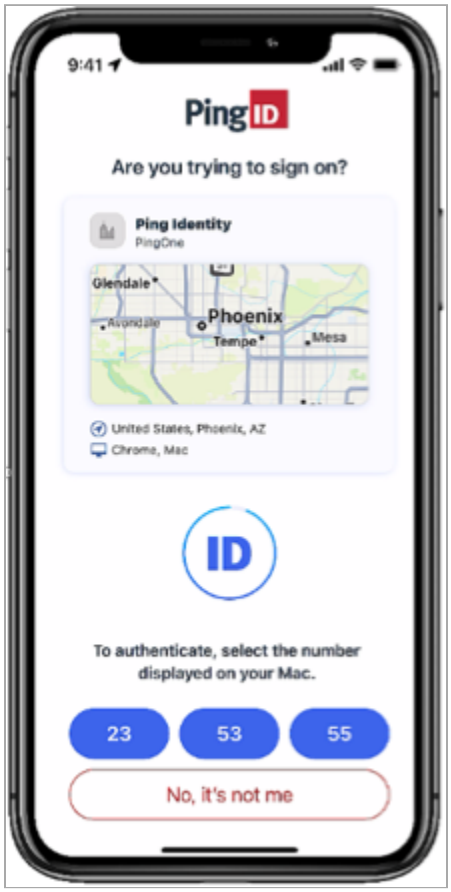
Copyright © 2025 Ping Identity Corporation



Copyright © 2025 Ping Identity Corporation

Number matching

You can require users to authenticate by selecting the number in PingID mobile app that matches the number displayed on the authenticating screen. This can be done as an additional authentication step as part of the mobile biometrics authentication or as its own authentication step. Number matching can also be performed from a user's smart watch.

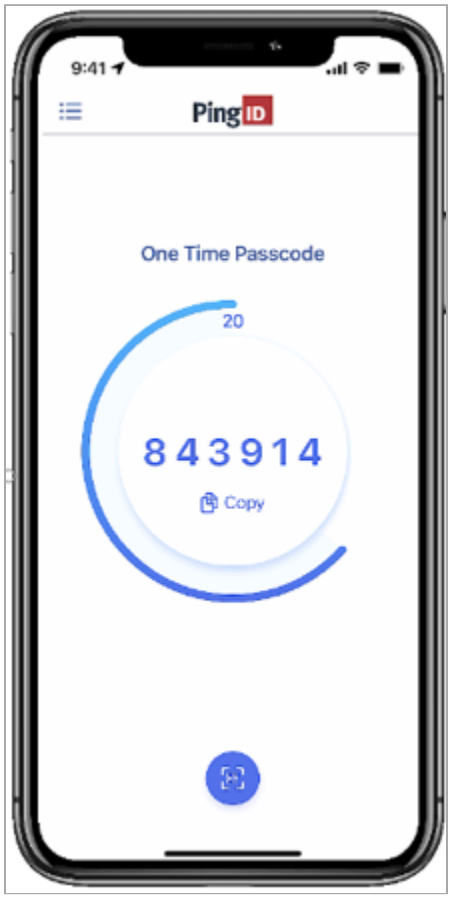


One-time passcode

PingID mobile app generates an OTP to enable users to authenticate when offline or unable to receive push notifications to your mobile device. Each OTP is unique, is valid for a limited time period, and can be used only once. When you open the PingID app, it generates a new OTP and displays a countdown timer showing when the current OTP is due to expire.

The OTP can be used for authentication in cases where the user's mobile is offline, such as when there is no network connection, or in any other use case set by the administrator as an organization's policy.

Copyright © 2025 Ping Identity Corporation



Smart Watch

If a user has a smart watch connected to their mobile device, the PingID mobile app automatically presents an authentication notification actions on the user's smart watch, asking the user if they are trying to sign on, with **Yes** or **No** options. This allows the user to authenticate without needing to access their device. A smart watch can also be used for number matching authentication.

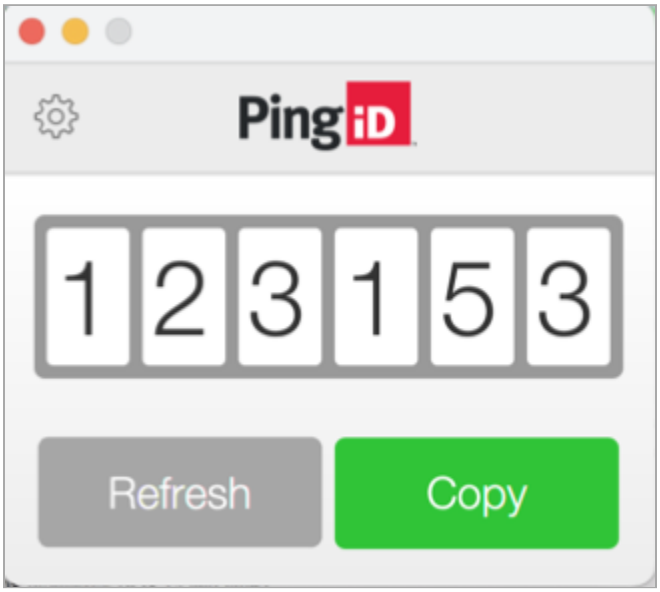
Manual Authentication (Offline authentication), and VPN access

PingID mobile app also provides the option for users to authenticate if they don't have internet access (offline authentication) or if they want to sign on to their organization's VPN.

(Workforce only) PingID desktop app

Your organization can enable users to download PingID desktop app to their Windows or Mac computer. They can use it to can generate an OTP with which to authenticate. Learn more in (Workforce Only) Configuring the PingID desktop application.

Copyright © 2025 Ping Identity Corporation



FIDO2

PingOne MFA and PingID support the FIDO2 authentication method. FIDO2 authentication allows users to authenticate using passkeys and other FIDO2-compatible authenticators. There are a wide range of devices that can be used as a passkeys.

Biometrics are supported for the following devices:

- Windows Hello
- Apple Mac (Touch ID)
- iOS biometrics (iOS 14 and later)
- Android biometrics (Android 7 and later)
- FIDO2 security keys
- Non-discoverable credentials (FIDO2 devices that are not defined as passkeys) are also supported. Users can take advantage of FIDO2 strong cryptographic authentication using built-in FIDO2 platform biometrics on their device.

Authenticator app

In both Workforce and Customer environments, you can enable use of a third-party authenticator app, such as Google Authenticator or Microsoft Authenticator. An authenticator app enables your users to authenticate by generating a standard Time-based One-Time Password (TOTP). This can be useful in many scenarios, for example:

- A workforce use case an organization cannot allow the PingID mobile app on their devices because PingID must be added to the allow list.
- You want users to use a single authenticator app and have users that must authenticate to multiple organizations.

(Workforce only) YubiKey (Yubico OTP)

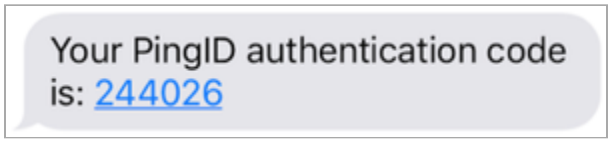
PingID workforce solutions support the use of a YubiKey with Yubico OTP capabilities as an authentication method. Select this method of authentication if you’ve distributed YubiKey hardware tokens to users who are not authenticating using a mobile device.

Copyright © 2025 Ping Identity Corporation

YubiKeys that are FIDO2 compliant can be used as either a YubiKey or a FIDO2 security key. Learn more in FIDO policies.

SMS and Voice authentication

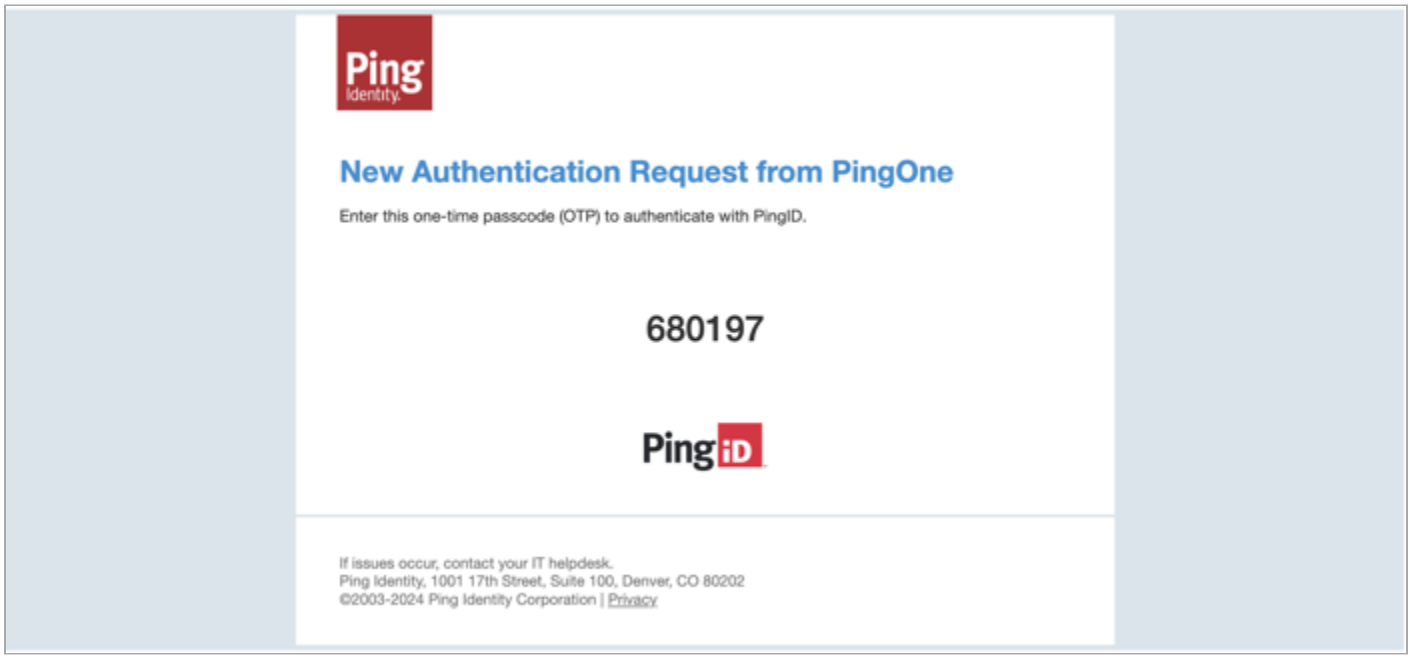
In both Workforce and Customer environments you can enable SMS or voice authentication. PingOne sends an OTP to the user's mobile device or landline phone using SMS or voice channels.



Learn more, including information about SMS and voice authentication and usage limits, in Configuring SMS and voice authentication.

Email authentication

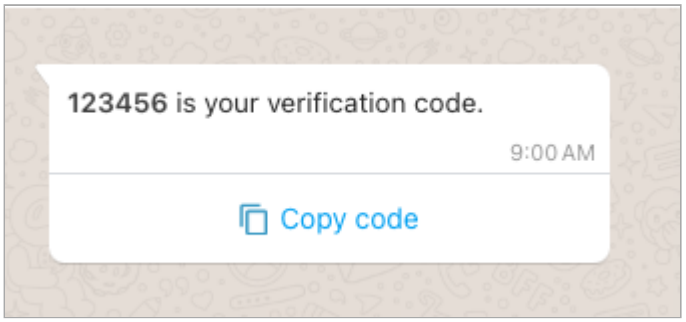
You can enable email authentication in Workforce and Customer environments. PingOne sends an OTP by email to the user's email address. Learn more in Configuring email authentication.



(Customer only) WhatsApp authentication

Enable and configure WhatsApp authentication to allow your users to receive a one-time passcode (OTP) by WhatsApp.

Copyright © 2025 Ping Identity Corporation



Learn more in (Customer Only) Configuring WhatsApp authentication

OATH token

Enable the use of OATH-compliant hard tokens to generate an OTP for secure authentication in Workforce or Customer environments.

Use hardware OATH tokens where there are no provisions for connection to the Internet, USB connections, or mobile phones. These connections could be disallowed for security reasons. Learn more in Configuring OATH token authentication.

Backup authentication

If a Workforce user forgets their device or their device is lost or stolen, they can authenticate using a backup device. The backup device available is defined by the information in your organization's directory and can include a personal email address or alternative phone number.

Backup authentication is configured in the PingID admin portal. Learn more in Configuring backup authentication methods.

What is the difference between PingID and PingOne MFA?

PingID is used to secure authentication for your organization's employees and contractors. PingOne MFA is used to secure authentication for your CIAM (Customer Identity and Access Management) use cases.

Workforce identities, and Customer identities are licensed differently, and require separate PingOne environments.

PingID: the workforce solution

Organizations are more likely to need to define more specific criteria for employee and contractor authentication and access to their systems. They are more likely to have more in-depth knowledge of:

- The authentication methods their employees are using.
- Information about the devices that their employees typically use to authenticate (and can create policies based on information such as IP reputation, and users authenticating from a new device).

Copyright © 2025 Ping Identity Corporation

Organizations can benefit from PingID to:

- Assert control over the type of device and range of authentication methods that their employees can use.
- Choose to limit use of less secure authentication methods, such as SMS and voice authentication.
- Use PingID policy to provide more frictionless authentication experiences for their trusted users, and require a step up to MFA or even block users authenticating in more risky scenarios.
- Benefit from a range of PingID integrations, including Windows login, and Windows login passwordless, Mac login, RADIUS Gateway (VPN), and SSH.

PingOne MFA - considering the customer

Your organization's customers or consumers are more likely to:

- Join from a wider and less predictable set of locations throughout the world.
- Use a wider set of devices and authentication methods.
- Tolerate less friction during enrollment and authentication.

PingOne MFA allows you to provide a wider range of device types to accommodate your customer's demographics and remove friction while maintaining security. PingOne MFA also allows you to provide strong authentication as part of your mobile application using the PingOne MFA mobile SDK.

Supported authentication methods

The following authentication methods are supported:

- PingOne MFA and PingID: FIDO2, Authenticator app, Email, SMS, and Voice authentication.
- PingID only: PingID mobile application, PingID desktop application, YubiKey OTP, OATH Token.
- PingOne MFA only: Mobile application integrated with the PingOne MFA SDK, WhatsApp.

Differences in policy usage

PingID is being transitioned to PingOne. Most PingID features are now available in PingOne. However to maintain a full set of PingID services during the transitional period, some features are still managed in the legacy PingID admin portal. During this transitional period, the following differences exist between PingOne MFA and PingID policies:

- Authentication policy: A default PingOne Authentication policy is created and it automatically includes the default MFA policy. The configuration options differ slightly for PingOne MFA and PingID. PingOne MFA also supports the use of multiple Authentication policies.
- MFA policy: PingOne MFA supports the use of multiple MFA policies. PingID supports the use of the default MFA policy only.
- FIDO2 policy: PingOne MFA supports the use of multiple FIDO2 policies. PingID supports the use of the default FIDO2 policy only.
- PingID authentication policy can be configured using the PingID web portal for PingID accounts only.

Copyright © 2025 Ping Identity Corporation

What is a typical strong authentication (MFA) workflow?

The main strong authentication (MFA) flows are the authentication and registration flows. The following list represents the high-level steps required to configure a PingOne environment to enable strong authentication for your SSO applications and covers both Workforce and Customer use cases.

1. Create an environment.
2. Create any applications to which you want to apply MFA. Learn more in Adding an application.
3. Perform general configurations. Learn more in MFA Settings.
4. Configure an MFA policy. Add and configure the the authentication methods that you want to enable.
5. Perform additional configurations for the specific authentication methods that you added.
6. Configure an authentication policy. For environments that are not integrated with DaVinci, configure an authentication policy.
7. (Workforce only) Configure PingID policy.
8. (Customer only) Create an application and Add MFA to the application in PingOne.
9. (Optional) Configure relevant integrations: Learn more in integrations for strong authentication.

Setting up an environment for strong authentication (MFA)

You can create a new PingOne environment and add multi-factor authentication (MFA) for Customer or Workforce use cases. You can also integrate an existing Workforce (PingID) account with a PingOne environment so that you can manage it through PingOne.

What do you want to do?

Follow the relevant instructions depending on the relevant use case.

Workforce and Customer:

- Create a new PingOne environment with MFA

Workforce only:

- Integrating a PingID account with a PingOne environment

Creating a new PingOne environment with MFA

To enable multi-factor authentication (MFA) for Customer or Workforce workflows, create a PingOne environment, add the relevant MFA service, and then add and configure any other services that you want to include.

About this task

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If you have an existing PingID environment and want to integrate it with a PingOne, follow the instructions in Integrating a PingID account with a new PingOne environment.

Steps

1. In the PingOne admin console, click **+** to add an environment, and then select either:
   - **Customer Solution** to get a preconfigured bundle that includes PingOne SSO, PingOne MFA, PingOne Protect, PingOne Verify, and DaVinci.
   - **Workforce Solution** to get a preconfigured bundle that includes PingOne SSO, PingID, PingOne Protect, and PingOne DaVinci.
   - **Build your own solution**: Select the solutions that you want to add to the environment. The options available depend on the license agreement you have.
2. In the **Services** window, enter the following information:
   - **Environment Name**: Enter a name for your PingOne environment.
   - **Description** (optional): Enter a description for the environment.
   - **Environment Type**: Select either **Sandbox** or **Production**
   - **Region**: Select the region that you want to create your environment.
   - **License**: Select the relevant license.
3. Click **Finish**.

Next steps

You can:

- In PingOne, add users. Learn more in Users. Learn more about allowing users to manage their account using MyAccount in Self Service.
- Configure an MFA policy including the relevant authentication methods.
- Learn about MFA authentication methods in Configuring strong authentication methods (MFA)

Integrating a PingID account with a PingOne environment

If you have an existing PingID accounts or PingOne environments, you can integrate them.

> **Important**
>
> Before performing any actions, read What you need to know before integrating or migrating a PingID account into a PingOne environment.

Choose the relevant option:

- Existing PingID account with a new PingOne environment

Copyright © 2025 Ping Identity Corporation

- Existing PingID account with an existing PingOne environment.
- Migrate PingID management from the web portal to PingOne environment. Only relevant if you integrated a PingID account with a PingOne environment before March 31, 2025.

After integrating a PingID account into a PingOne environment, consider common post-requisites.

What you need to know before integrating or migrating a PingID account into a PingOne environment

If you are integrating an existing PingID account into a PingOne environment, or migrating the management of your PingID account to PingOne read the following.

Service interruptions during migration

The migration process involves copying all user, device, and configuration data from the legacy PingID account to your PingOne environment. During this process, the following operations are temporarily suspended until migration is complete:

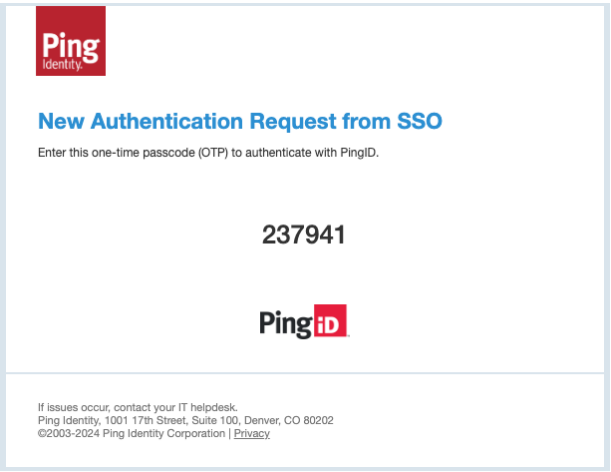
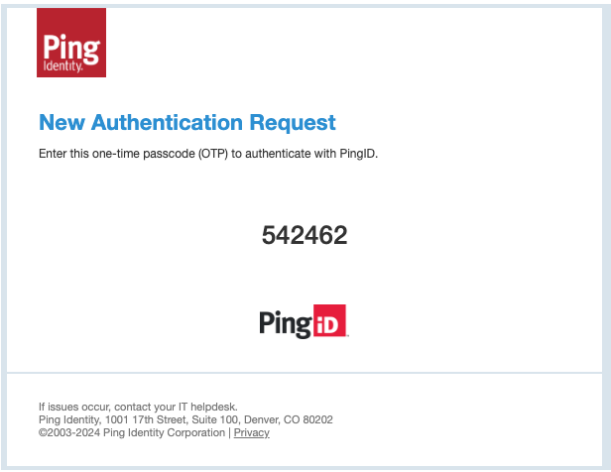
- MFA device management operations: Pair, Delete, Modify end-user or administrator MFA devices.
- User operations: Create, Delete, Update.
- All configuration changes within the legacy PingID admin portal and all configuration changes related to MFA in PingOne.

During migration end users can continue to authenticate with devices that are already paired with their account.

End-user experience changes

- Email notification templates:
  - Device Registration notification templates:
    - All templates relating to device registration and device authentication are automatically migrated to PingOne.
    - PingID custom templates for New Device Registration are automatically migrated to PingOne.
  - Strong authentication notification templates: When sending emails based on the strong authentication notification template, PingOne does not include the service provider (SP) name.

Copyright © 2025 Ping Identity Corporation

PingID template	PingOne template
	

  - Report Fraud notification templates: Only the default Fraud template is migrated to PingOne. If the Fraud template was customized in a PingID account, it is reset to the default template after migration.

- Device biometrics:

> **Note**
>
> As part of the migration process, the legacy PingID email notification template variable `${one-time-passcode}` is automatically updated to `${\otp}` in the equivalent PingOne email notification template.

In PingOne, device biometrics is always enabled for both iOS and Android devices. For PingID accounts where device biometrics is set to **Enabled** or **Required** for only one OS (iOS **or** Android), the configuration is expanded to include both OSs after PingID is integrated with PingOne.

- Device fallback behavior:

  - SMS quotas: If a user exceeds the configured SMS quota and SMS is their default authentication method, PingID would automatically fallback to the next authentication method on their list. In PingOne, the next time they attempt to authenticate, the Device Selection screen appears, allowing them to choose a different authentication method.

- Push notifications:

In PingOne environments, push notifications to mobile devices do not include the `spAlias` (the alias used to identify the authentication service).

- Web and RADIUS Gateway only:

If FIDO2, security key, or platform biometrics are configured as a user's primary authenticating device, and **Default to Primary** is also selected, if the accessing device does not support WebAuthn the **Device Selection** window presents a list of the user's paired devices, rather than falling back to the next authentication method in the list, as would otherwise be expected.

If you are using a RADIUS Gateway, you can solve this issue by performing additional configuration steps detailed in this Knowledgebase article.

Copyright © 2025 Ping Identity Corporation

- Locale configuration changes for SMS, voice, and email notifications:

  In the PingID admin portal, you could disable localizations. In PingOne SMS, Voice and Email notifications are always localized to supported languages in PingOne. If a user's browser is set to a language that is supported by PingOne that language is automatically applied.

- Regional support:

  PingOne environments created in the Canada region cannot support Strong Authentication for Workforce use cases (PingID service).

- MFA policy user account validation check:

  During authentication PingOne validates whether the user account is active. If the account is locked, the user is blocked from authenticating. In PingID this validation process did not exist. To overrride PingOne's account validation, in the MFA policy, select the **Skip user lock verification** checkbox.

Policy changes

There are several changes to the support of PingID policy rules when PingID is managed out of PingOne:

- Mobile OS version:

  The Mobile OS version rule is not supported in PingOne, and must be removed before migrating. The equivalent functionality can be configured directly in the **PingID mobile application** in the **Applications** page.

- Location-based rules:

  The location-based part of the following rules is not supported in PingOne, and must be removed from the following rules before migrating a PingID tenant to PingOne:

  - Access from the company network rule
  - Recently authenticating from office rule
  - Recent authentication from company network

- Limit push notifications rule:

  The Limit push notification rule is replaced by an equivalent configuration in the MFA policy. If your PingID account uses this rule, you'll have the opportunity to select the relevant MFA policy configuration during migration. Learn more about the Limit push notification configurations in PingOne in Configuring an MFA policy for strong authentication.

- Number matching:

  In PingOne environments, number matching is configured in the MFA policy. Learn more in in Configuring an MFA policy for strong authentication.

API changes

The following PingID APIs are not supported when PingID is managed out of PingOne:

- OATH token API

Copyright © 2025 Ping Identity Corporation

- User Management API:
  - EditUser
  - DeleteUser

It is recommended to use PingOne APIs after integrating a PingID account into PingOne, however all other PingID APIs will continue to function and can still be used.

IdP considerations

If PingFederate is the IdP

After integrating with PingOne, PingID accounts that were using the PingID provisioner must use the PingOne provisioner for user provisioning.

> **Note**
>
> When using PingOne provisioning, make sure **MFA Device Management** is set to **Do not manage**. Learn more in Adding attribute mapping for inbound provisioning.

After migration is complete, environments with PingFederate as their IdP should consider any post-migration changes that might be required for their environments.

For a list of common considerations, see Considerations after integrating or migrating a PingID account into a PingOne environment

If using PingOne for Enterprise with PingOne directory as the IdP

When integrating PingID with PingOne, admin user accounts from the PingOne for Enterprise directory cannot be migrated to a PingOne environment.

After completing the integration process, administrators must manually create the equivalent administrative user accounts in the PingOne administrators environment and assign those accounts the admin permissions necessary to manage the PingOne environment with which you integrated the PingID account.

> **Warning**
>
> When using PingOne directory as your IdP, if you want to change to a different IdP when migrating to PingOne, be aware that user account information from PingOne directory is not migrated, and would need to be recreated in the new IdP.

Learn more about PingOne administrator management in Managing administrators and Managing administrator roles.

Copyright © 2025 Ping Identity Corporation

User directory changes

After migration, PingOne usernames are immutable and cannot be changed. This is because the username that appears in the PingOne directory is used by the PingID service to identify the user.

Integrating a PingID account with a new PingOne environment

You can integrate an existing PingID account with a new PingOne environment.

Before you begin

> **Important**
>
> Before you begin, read What you need to know before integrating or migrating a PingID account into a PingOne environment.

> **Warning**
>
> Integration with a PingOne environment should be considered as a permanent change.
> After integration, unlinking yourPingID account from PingOne deletes the PingOne environment and can result in the deletion of the PingID account, with the following qualifications:
>
> - During the 14 day grace period following integration, you can unlink the PingID account and only the PingOne environment is deleted.
> - There is no grace period for PingOne environments that have updated FIDO devices to use the FIDO2 authentication method. In environments using FIDO2 authentication, deleting the PingOne environment also deletes the PingID account.

Before the integration process starts, PingOne performs several validations to ensure the PingID account is compatible with the PingOne environment. Before you start the integration process, you can do several checks to minimize the possibility of the validation failing. Make sure that:

- Your PingOne license covers the same number of users that exist in your PingID account and that your PingID account license is still valid.
- The PingOne environment that you create is in the same region as your PingID environment.
- The user accounts in your PingID environment do not include any duplicate users or usernames that contain unsupported characters. You'll have opportunity to fix issues during the PingID account validation process. Learn more about how to fix issues before you begin and find more detailed technical information in "Duplicate users found" error when attempting to connect a PingID environment to PingID in the Ping Identity Support Portal.
- Some policy rules are deprecated in PingOne. You'll need to remove them from the legacy PingID web portal before you start the integration:
  - Remove the Mobile OS version rule from any PingID polices.
  - Remove the location-based part of the following rules:
    - Access from the company network rule
    - Recent authentication from the office rule

Copyright © 2025 Ping Identity Corporation

        - Recent authentication from company network rule

    - In PingOne environments, the **Limit Push Notification Rule** is updated to a configuration in the MFA policy. If you have the rule defined in the PingID admin portal, you'll be asked to redefine it during the integration process.

About this task

Integrate your existing PingID account with a new PingOne environment so that you can:

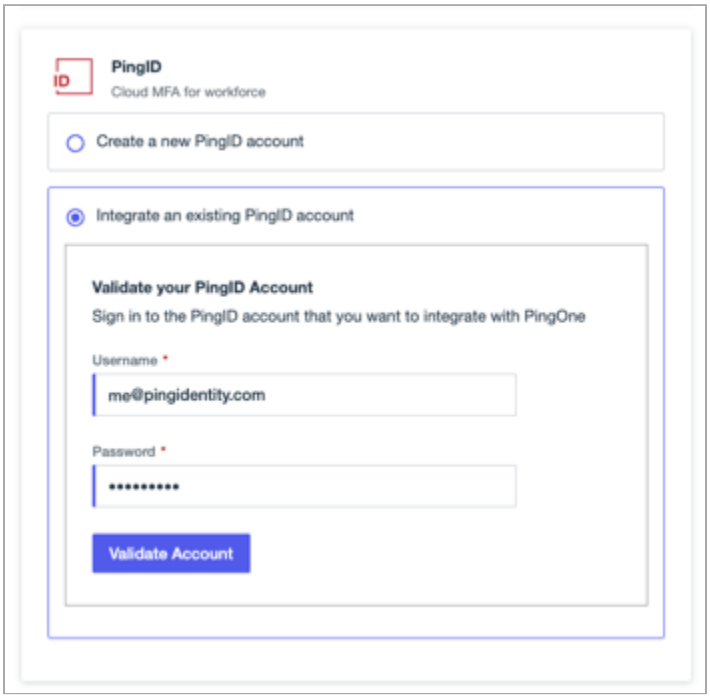
- Manage PingID users from PingOne
- Allow users to manage their devices using MyAccount.
- Apply a FIDO policy to PingID user accounts.
- Bring Your Own (BYO) SMS or Voice account
- Implement a Windows login passwordless flow.

If you want to create a new PingID environment, refer to Creating a new PingOne environment with MFA.

Steps

1. Start an PingOne trial.
2. To create a PingOne environment, in the PingOne admin console, go to **Add Environment** > **Build your own solution** > **PingID**, and then click **Next**.

   PingOne SSO is automatically included in the selection.



3. Select **Integrate an existing PingID account**, enter the user name and password for the PingID environment you want to integrate, and then click **Validate Account**.

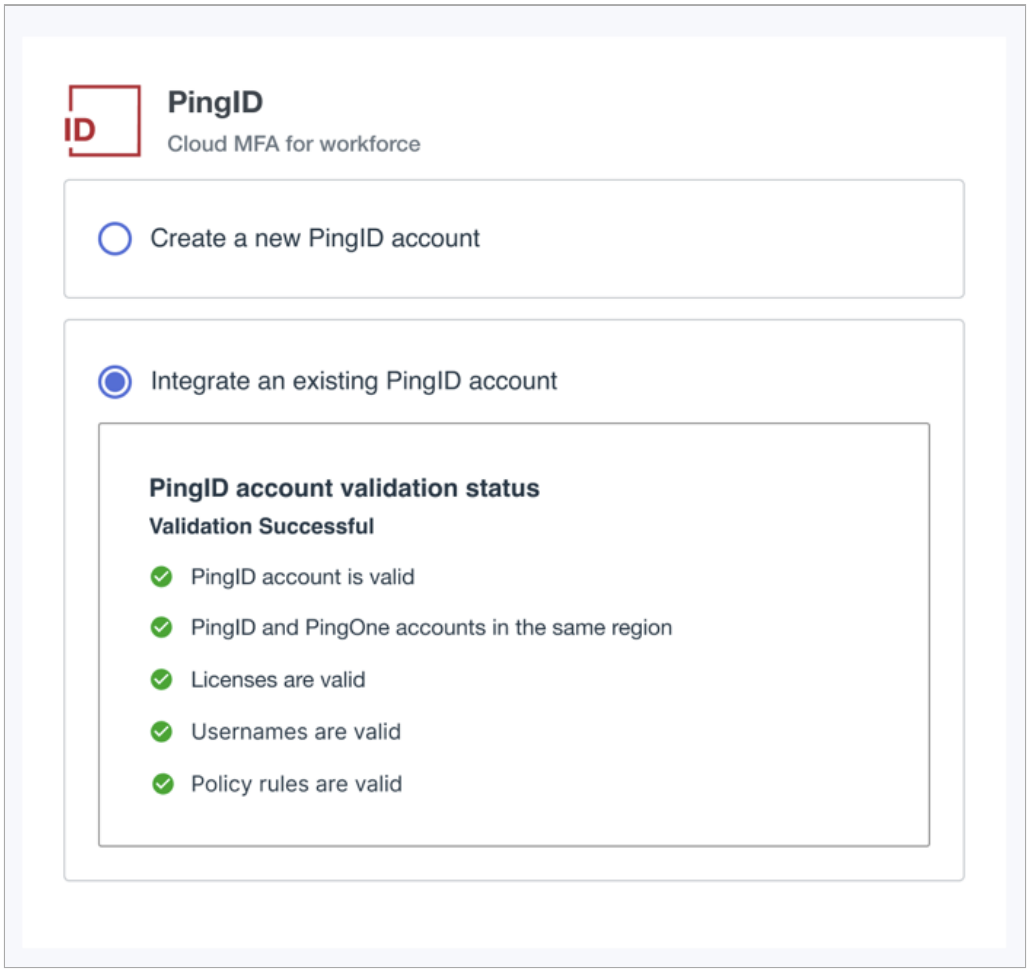
   PingOne performs a validation of your PingID and PingOne accounts.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> This step can take several minutes. Do not close the window during the validation process. If you need to fix any issues, follow the instructions in the validation wizard to fix them, and then rerun the validation.

Result:

You'll see the **Validation Successful** status.



4. Click **Next**, and then in the **Services** window enter the following information:
   - **Environment Name**: Enter a name for your PingOne environment.
   - **Description (optional)**: Enter a description for the environment.
   - **Environment Type**: Select either **Sandbox** or **Production**
   - **Region**: The region must match the region in which your PingID environment is located.
   - **License**: Select the relevant license.
5. Click **Finish**.

Result

Copyright © 2025 Ping Identity Corporation

You can now manage your users through PingOne. Although most of the PingID APIs are still supported, you should use the PingOne APIs when working out of PingOne. Learn more: What you need to know before integrating or migrating a PingID account into a PingOne environment.

Consider any post-requisites that might be required for your environment. Learn more in Considerations after integrating or migrating a PingID account into a PingOne environment.

Learn more about allowing your users to manage their devices using MyAccount in Self Service.

Learn more about creating and managing FIDO policies in FIDO policies.

Learn more about BYO Telephony in Using a custom provider account with PingOne.

Learn more about implementing a Windows login passwordless flow in Creating and configuring a passwordless Windows login application in PingOne.

Integrating an existing PingID account with an existing PingOne environment

You can integrate an existing PingID account with an existing PingOne environment.

Before you begin

> **Important**
>
> Before you begin, read What you need to know before integrating or migrating a PingID account into a PingOne environment.

> **Warning**
>
> Integration with a PingOne environment should be considered a permanent change. Make sure you connect the correct PingOne environment because after integration is complete this change cannot be rolled back.

Before the integration process starts, PingOne performs several validations to ensure the PingID account is compatible with the PingOne environment. Before you start the integration process, you can do several checks to minimize the possibility of the validation failing.

Make sure that:

- You have the necessary licenses:
  - Your PingOne license must cover the same number of unique user accounts that exist in your PingID account.

> **Note**
>
> The PingOne license must be sufficient to cover all user accounts unique to PingID that will be added to the PingOne environment.

- Your PingID account license must still be valid.

  To update a license, contact your Ping Identity representative.
  - The PingOne environment that you create is in the same region as your PingID environment.
  - PingOne MFA is not added as a service.

Copyright © 2025 Ping Identity Corporation

- Even if PingOne MFA is not added as a service, if the environment includes PingOne SSO, make sure that no paired MFA devices have been added to the PingOne environment.

  Learn more in User Devices report.

- For environments that use DaVinci flows, the PingOne MFA connector is not included in any existing flows.
- The user accounts in your PingID environment do not include any duplicate users or usernames that contain unsupported characters. You'll have the opportunity to fix issues during the PingID account validation process. Learn more about how to fix issues before you begin and find more detailed technical information in "Duplicate users found" error when attempting to connect a PingID environment to PingOne in the Ping Identity Support Portal.
- Some policy rules are deprecated in PingOne. You'll need to remove them from the legacy PingID web portal before you start the integration:

- Remove the Mobile OS version rule from any PingID polices. In PingOne, the functionality in this rule is provided by the Device Requirements. To ensure existing Mobile OS version rule functionality is migrated to PingOne:
  - Before migration, in the legacy PingID admin portal, go to **Device Requirements** section of the PingID application.
- Remove the *location-based* part of the following rules:
  - Access from the company network rule
  - Recent authentication from the office rule
  - Recent authentication from company network rule
- In PingOne environments, the **Limit Push Notification Rule** is updated to a configuration in the MFA policy. If you have the rule defined in the PingID admin portal, you'll be asked to redefine it during the integration process.

About this task

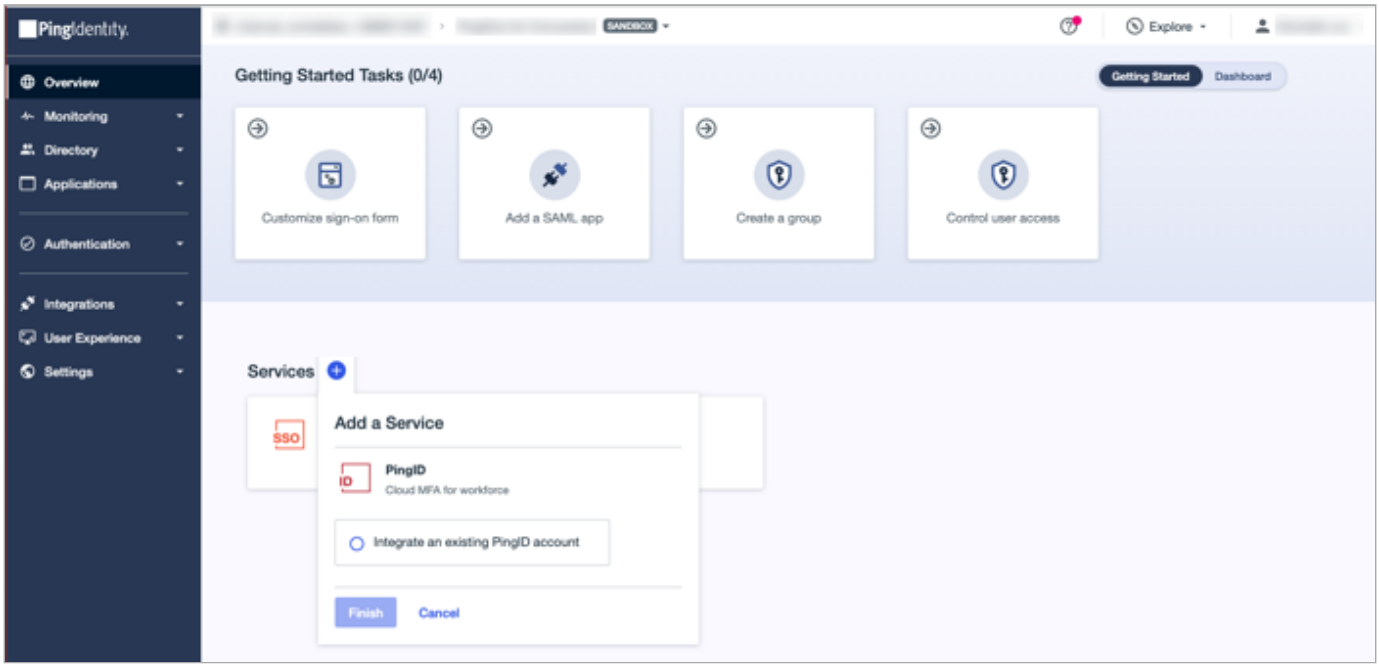
Integrate your existing PingID account with an existing PingOne environment so that you can:

- Manage PingID users from PingOne
- Allow users to manage their devices using MyAccount.
- Apply a FIDO policy to PingID user accounts.
- Bring Your Own (BYO) SMS or Voice account
- Implement a Windows login passwordless flow.

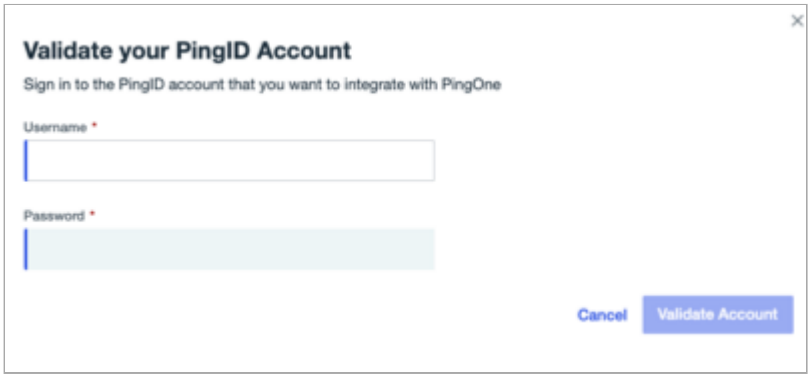
Steps

1. Go to the PingOne admin console, open the PingOne environment that you want to use and click the **Overview** tab.
2. In the **Services** area, click **+**, select **PingID**, and then select **Integrate an existing PingID account**.

> **Note**
>
> If the PingOne environment did not include PingOne SSO, it is added automatically.



3. Enter the username and password for the PingID account you want to integrate and then click **Validate Account**.



> **Note**
>
> - Do not close the window during the validation process, which can take several minutes.
> - The validation wizard lists any issues that cause the validation to fail. Some issues can be fixed during the validation process. Others, such as licensing issues, must be fixed independently. Fix all issues, then rerun the validation, if required.

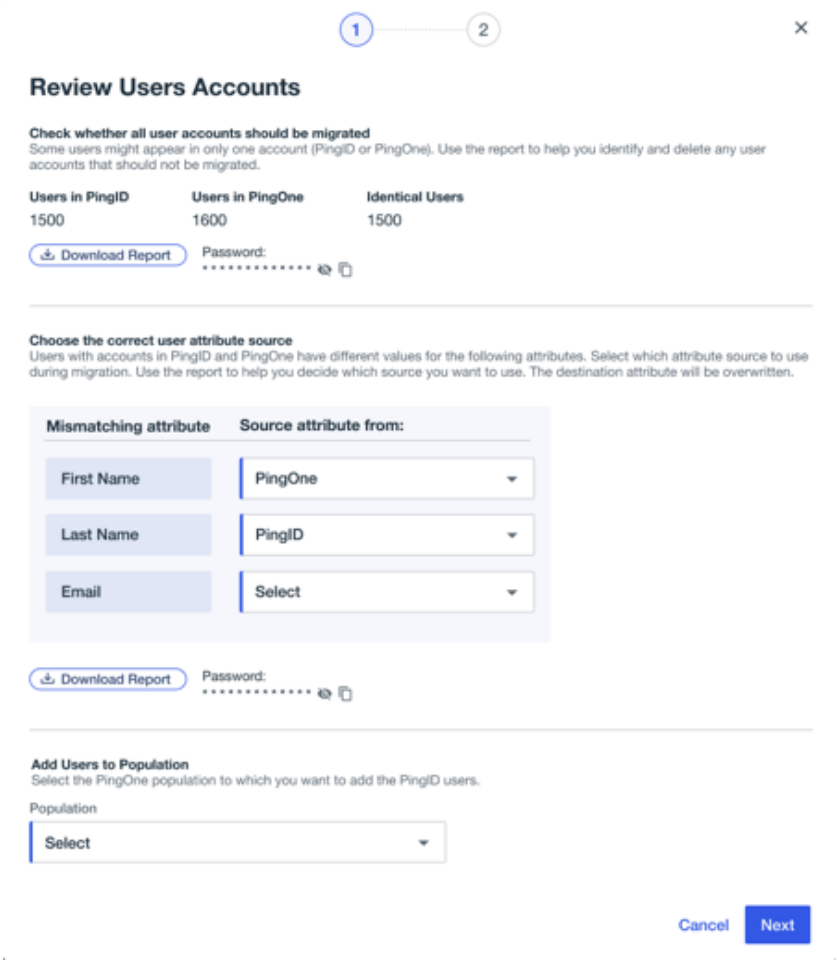
You'll see the **Validation Successful** status.

Copyright © 2025 Ping Identity Corporation

4. Click **Next**.

   PingOne performs a review of the user accounts in PingID and PingOne and provides a list of actions required before migration. It also provides a summary of the user distribution indicating the number of accounts that are unique to PingID or PingOne and the number that they have in common (Identical Users).

   The **Review User Accounts** window displays only the actions required that are relevant to your integration.



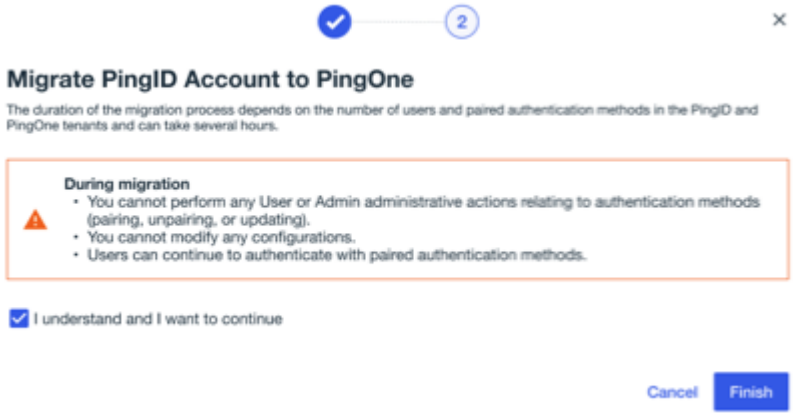
5. Perform the actions listed for the user accounts you want to integrate, and then click **Next**.

   - If you have user accounts that only appear in either PingID or PingOne, or have mismatching attributes within the same user account, you'll need to fix them. Click **Download** next to the relevant section to download a report to help you.

Copyright © 2025 Ping Identity Corporation

- For user accounts that are unique to PingID, select the population in which you want to create those user accounts in PingOne.

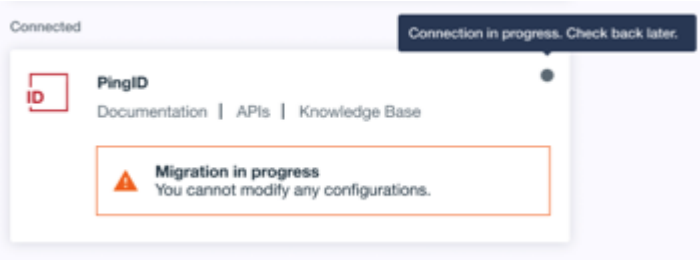
You'll see the **Migrate PingID Account to PingOne** window.



> **Important**
>
> - Migration can take several hours, depending on the number of users and paired authentication methods in the PingID and PingOne tenants. During migration, you can't perform user or admin administrative actions relating to authentication methods including pairing, unpairing, updating, or modify any configurations.
> - Users can continue to authenticate with authentication methods that are already paired.

6. Click **I understand and want to continue**, and then click **Finish**.

   You can check progress in the **Services** area of the **Overview** tab.



   When integration is complete, the PingID services status icon turns green.

> **Note**
>
> If the migration fails, a message shows indicating when you can retry migration (usually after 24 hours) and includes a link to the PingID migration report. View the report and fix any issues before you restart this procedure. If you require further help, contact your Ping Identity support representative.

Result

You can now manage your users through PingOne. Although most of the PingID APIs are still supported, you should use the PingOne APIs when working out of PingOne. Learn more in What you need to know before integrating or migrating a PingID account into a PingOne environment.

Copyright © 2025 Ping Identity Corporation

Consider any post-requisites that might be required for your environment. Learn more in Considerations after integrating or migrating a PingID account into a PingOne environment.

Learn more about allowing your users to manage their devices using MyAccount in Self Service.

Learn more about creating and managing FIDO policies in FIDO policies.

Learn more about BYO Telephony in Using a custom provider account with PingOne.

Learn more about implementing a Windows login passwordless flow in Creating and configuring a passwordless Windows login application in PingOne.

Migrating PingID management from the legacy PingID admin portal to a PingOne environment

If you integrated a PingID account with a PingOne environment before March 31, 2025, most of the management of the PingID environment is still performed by the legacy PingID admin portal. You'll need to manually migrate the management of that PingID environment and move it to PingOne.

Before you begin

> **Important**
>
> Before you begin, read What you need to know before integrating or migrating a PingID account into a PingOne environment.

Before the integration process starts, PingOne performs several validations to ensure the PingID account is compatible with the PingOne environment. Before you start the integration process, you can do several checks to minimize the possibility of the validation failing. Make sure that:

- Your PingOne license covers the same number of users that exist in your PingID account and that your PingID account license is still valid.
- The PingOne environment that you create is in the same region as your PingID environment.
- The user accounts in your PingID environment do not include any duplicate users or usernames that contain unsupported characters. You'll have opportunity to fix issues during the PingID account validation process. Learn more about how to fix issues before you begin and find more detailed technical information in "Duplicate users found" error when attempting to connect a PingID environment to PingID in the Ping Identity Support Portal.
- Some policy rules are deprecated in PingOne. You'll need to remove them from the legacy PingID admin portal before you start the integration:
  - Remove the Mobile OS version rule from any PingID polices.
  - Remove the location-based part of the following rules:
    - Access from the company network rule
    - Recent authentication from the office rule
    - Recent authentication from company network rule
  - In PingOne environments, the **Limit Push Notification Rule** is updated to a configuration in the MFA policy. If you have the rule defined in the PingID admin portal, you'll be asked to redefine it during the integration process.

Copyright © 2025 Ping Identity Corporation

- Read the topic about what you need to know before integrating a PingID account into a PingOne environment.

About this task

This procedure is only relevant for PingID accounts that were integrated with PingOne environment before November 19, 2024, and therefore still managed by the legacy PingID admin portal. Migrate management front the legacy PingID admin portal to ensure all PingID management capabilities that can potentially be performed from PingOne are moved to PingOne.

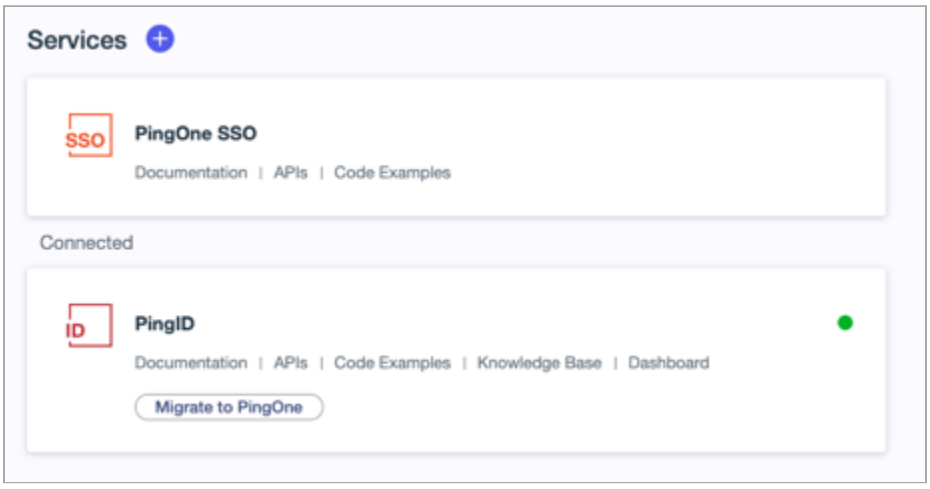
Important

- Then duration of this process is affected by the number of users in the PingID tenant and can take several hours. During migration, you cannot perform any actions that affect users' devices such as pairing, deleting, or updating devices, or edit any related configurations. Authentication flows are not affected by the migration.
- You can only attempt a migration once in a given 24-hour period.
- Some PingID policy rules are deprecated or updated in PingOne. To complete migration, you might be required to update, modify, or remove PingID policy rules. Details of actions required in the specific PingID account you are migrating are provided during the migration process, if applicable.

Steps

1. Sign on to the PingOne admin console.

   You'll see a **Migrate to PingOne** button next to the PingID account.



2. Click **Migrate to PingOne**.

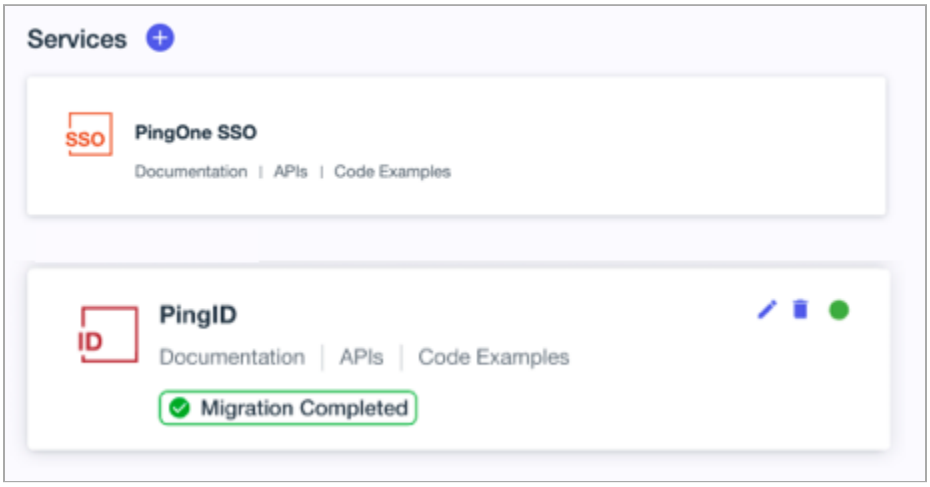
   Result:

   PingOne checks whether all the PingID policies are valid.

   A modal shows a warning message that this process will permanently move your PingID account to PingOne, and that the process might take several hours, during which it is not possible to edit any user configurations.

   At the end of the process you'll see confirmation that migration is complete.

Copyright © 2025 Ping Identity Corporation



3. Click **Next**, and then click **Finish**.

   Result

   You can now manage PingID authentication methods and associated configurations through PingOne.

Considerations after integrating or migrating a PingID account into a PingOne environment

After migrating your PingID account to a PingOne environment, consider the following post-requisites.

Enabling users to manage their devices using MyAccount when using an external IdP (such as PingFederate)

When using an external IdP, to enable your users to manage their devices using MyAccount, you'll need to do the following tasks in PingOne:

1. Add the IdP as an external IdP. Learn more in External IdPs.
2. Add the external IdP to an authentication policy. Learn more in Adding an authentication policy.
3. In the PingOne Self-Service - My Account application **Policies** tab, add the authentication policy that you created in the previous step.
4. Enable MyAccount. Learn more in Self Service.

Enable administrators to manage user devices

To provide administrators the permissions necessary to manage user devices from the PingOne admin portal, do the following:

1. In the Administrators environment in PingOne, manually create one or more Admin accounts.
2. Assign the admin accounts the permissions necessary to manage user devices for the PingOne environment with which you integrated the PingID account.

Configuring strong authentication methods (MFA)

This section describes the requirements, limitations, and configurations that are available for each authentication method.

Copyright © 2025 Ping Identity Corporation

To add an authentication method make sure you have already created:

- A PingOne account with the relevant services (Workforce or Customer).

Which authentication type do you want to add?

You can add one or more authentication method with which your users can authenticate. All authentication methods are enabled and configured in the MFA policy, but some authentication methods require additional configuration steps outside of the MFA policy. You can find details in the relevant sections:

- Workforce and Customer options:
  - FIDO2
  - Authenticator app
  - Email
  - SMS or voice
  - OATH token
- Workforce only (PingID):
  - PingID mobile app
  - PingID Desktop app
  - YubiKey
- Customer only (PingOne MFA):
  - Native mobile application
  - WhatsApp authentication

For Workforce environments, after configuring the relevant authentication methods, you can create and apply a PingID authentication policy.

Configuring mobile applications

You can can configure mobile applications for Customer and Workforce use cases.

Customer use case:

- Embed strong authentication into a native mobile application.
  1. Create a mobile application.
  2. Enable and configure the mobile application in the relevant MFA policy.
  3. Add a mobile app: Editing an application - Native
  4. Associate an authentication policy with a mobile app.

Copyright © 2025 Ping Identity Corporation

Workforce use case:

- Configure PingID mobile application for strong authentication

(Workforce Only) Configuring the PingID mobile application settings

PingID allows users to download an app to their mobile device and use it to sign on to your company services and applications with the added security of multi-factor authentication (MFA). They can also use it to verify their identity to an employer.

Before you begin

To add PingID mobile app as an authentication method, you need:

- A PingOne environment with the PingID service.

About this task

Configuring PingID mobile app as an authentication method for MFA includes the following steps:

1. Configure the MFA policy, including the PingID mobile app-specific configurations. Learn more in Configuring an MFA policy for strong authentication.
2. Configure the PingID mobile application in the **Applications** section of PingOne, as described in this procedure.

Steps

1. Go to **Applications > Applications**.
2. In the **Applications** list, select **PingID Mobile**.
3. On the **Configuration** tab, click the **Pencil** icon and edit the relevant fields described in the steps that follow this one.
4. In the **Mobile App authentication** area, under **Mobile Biometrics**, select the authentication behavior based on whether the user has biometrics (Fingerprint or Face). Select either:

   Choose from:

   - **Preferred**: If mobile biometrics are defined on the user's device, the user must use them to authenticate.
   - **Required**: Users must configure mobile biometrics on a supported device and can only use biometrics to authenticate.
   - (Optional) Select **Enable FaceID Consent on iOS:** to prevent users with FaceID defined from authenticating by mistake. When selected, the user is prompted to consent explicitly before each face scan is taken.
   - Select **Enable Notification Actions** to allow users to approve a notification request from the lock screen.
   - Select **Enable Device Passcode Fallback on iOS** to allow users to authenticate using the device passcode if biometrics authentication fails.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> - **Mobile Biometrics** configurations require **Biometrics** to be selected in the MFA policy. Learn more in MFA policy
> - For PingID mobile app 1.x users only, optionally select **Enable FaceID Consent on iOS:** to prevent users with FaceID defined from authenticating by mistake. When selected, the user is prompted to consent explicitly before each face scan is taken.

5. In the **Mobile App authentication** area, under **Number Matching Options**, select either:
   - **Select Number**: Display three numbers in PingID mobile app and prompt the user to tap the correct number.
   - **Enter Manually**: Display a text field in PingID mobile app and prompt the user to manually enter the correct number.

> **Note**
>
> - To enable this feature, **Number Matching** must be enabled in the MFA Policy. Learn more in Configuring an MFA policy for strong authentication.
> - This feature is supported by PingID mobile app 2.4 or later. Users running an earlier version are prompted to select a number, rather than entering the text manually.
> - Manual number matching is not supported by smart watches.

6. (Optional) In the **Mobile App authentication** area, enable the following options:
   - **Enable OTP Push Notification**: Send a push notification to users when they can only authenticate with an OTP. When they tap the notification, PingID mobile app opens automatically, displaying the current OTP.
   - **Display Authentication Information map**: Include a map with supporting information about the origin of the authentication request they receive with the push notification.
7. (Optional) In the **Mobile Management** area, enable the following options:
   - **Allow users to unpair or change device from the PingID mobile app**
   - **Allow authentication from lock screen for legacy Android devices** (Android Q or earlier)
   - **Require mobile app security PIN**: When selected, the user must enter a security PIN to access PingID mobile app. If selected, you must also define the security PIN-requirements, defining whether the security PIN must be 4 or 6 digits in length, and whether PingID mobile app PIN is always required or only when a device PIN or biometrics are not defined on the user's device. Learn more about PingID mobile app PIN requirements in PingID mobile app PIN requirements
8. In the **Mobile Notifications** section, you can choose to notify users when new PingID mobile app versions become available.

   Choose whether to make updates optional or mandatory and define from which version they appear.

   Choose from:

   - **Notify users of required mobile version updates**: Notify the user when a new version is available. The user must update to the new version to continue using PingID mobile app and cannot skip the update. If selected, for each OS, specify the minimum version from which update notifications should be sent. The default is **Latest**.

Copyright © 2025 Ping Identity Corporation

- **Notify users of optional version mobile updates**: Notify the user when a new version is available. The notification includes the option to skip the update and install it at a later date. If selected, for each OS, specify the minimum version from which update notifications should be sent. The default is **Latest**.

9. (Optional) To restrict the brand and model of mobile devices that can be used with PingID mobile app:
    1. In the **Mobile requirements** section, select **Select allowed and disallowed devices**.
    2. In the relevant **Brands** field, add one or more brands, and in the corresponding **Models** field, specify one or more models. If no model is selected, all models for that brand are selected.

    > **Note**
    > - If you choose the same device brand and model under both allowed and disallowed devices, then the disallowed selection takes precedence.
    > - These lists are continuously updated as new brands and models are introduced to the market.

10. To define the minimum operating system that a user's device (Android or iOS) must be running to authenticate with PingID mobile app:
    1. In the **Mobile requirements** section, select **Require device minimum operating system**.
    2. In the relevant list (**iOS** or **Android**), select the minimum OS version you want to allow.

    > **Note**
    > The list of supported operating systems is dynamic and can change as new versions are introduced. Discontinued support of older versions can also impact the minimum supported OS version.

11. To define the minimum version of PingID mobile app that a user must be running to authenticate:
    1. In the **Mobile requirements** area, select **Require minimum PingID version**
    2. In the relevant list (**iOS** or **Android**), select the minimum PingID mobile app version you want to allow.

    > **Note**
    > - Use this option if you want to require that your users have access to new features and the latest security benefits, or to disallow older versions of the PingID mobile app.
    > - The list of supported versions is dynamic and can change as new versions are introduced and support of older versions is discontinued.

12. To require a user's device to have a device lock enabled on their device to authenticate with PingID mobile app, in the **Mobile requirements** section, select **Require device lock to be enabled on device**.
13. To prevent users from authenticating with a rooted or jailbroken device, in the **Mobile requirements** section, select **Require the device not to be rooted or jailbroken**.
14. To enforce the use of a device that includes a hardware biometrics sensor, when pairing or authenticating with PingID mobile app, in the **Mobile requirements** section, select **Require the device to have biometric capabilities**.

Copyright © 2025 Ping Identity Corporation

15. To allow your organization's Mobile Device Management (MDM) to control activities of your users when using PingID mobile app:

    1. In the **Mobile requirements** section, select **Require Mobile Device Management**. A token is automatically generated in UUID format. Administrators can edit the key value if required.

    2. In the **Effective Date** field, enter a date by which you want the MDM requirement to be applied. Users are blocked from authenticating until the MDM system has distributed the token to all managed devices. The effective date should allow enough time for the MDM system to complete the distribution.

    3. Configure the organization's MDM system. You can find third-party MDM system configuration examples in Third-party MDM system configuration for PingID integration.

    > **Note**
    >
    > - You can also generate a new token, rotate a token, or revoke a token.
    > - Multiple keys can coexist, for example, for allowing time for rotating keys and the time it takes to phase in new keys and retire old ones. PingID checks all listed keys to verify a match with the key submitted in the authentication request. The MDM does not retain multiple values for the same token. Support for multiple keys is provided through PingID.
    >
    > Learn more in Managing MDM tokens.

16. Click **Save**.

PingID mobile app PIN requirements

As an extra layer of security, you can require users to enter a 4 or 6-digit PIN code to access the PingID mobile app.

Enable and configure a PingID mobile app PIN in the PingID mobile app settings. Learn more in (Workforce Only) Configuring the PingID mobile application settings.

You can require a PIN code to access PingID mobile app for:

- Devices that don't already have device biometrics or a device PIN code defined
- All devices

If this option is enabled:

- A user is prompted to create a PIN code when they pair the mobile app. The PIN code must include at least 3 or 4 different digits for PIN lengths of 4 and 6 digits, respectively. Digits must not be in ascending or descending sequence, such as 1234 or 4321.
- A user is prompted to enter the PIN code each time they launch the PingID app.
- The mobile app is locked after 3 minutes of inactivity, and the user is required to enter the PIN to unlock it.
- In the event of three consecutive incorrect PIN entries, the user is blocked from accessing the app for 2 minutes. This applies to both the PIN entry and the PIN change windows. Lockdown takes effect from the time of the lock, irrespective of whether the desktop app remains open or is closed and relaunched.
- The mobile app must be online for a user to pair the app. However, a user who is offline can still create a PIN, enter the PIN to access the mobile app, or change their PIN.

Copyright © 2025 Ping Identity Corporation

- The mobile app must be online for any change in PIN configuration to take effect, such as enabling or disabling the PIN or changing its length. The user can change their PIN from the PingID mobile app settings.
- If a user pairs the mobile app to more than one organization, the user must create only one PIN, according to the most restrictive organization requirements. For example:
  - If only one organization has enabled the **Mobile Security PIN** feature, the user is required to enter their PIN to use the mobile app for authentication to all organizations, including those which do not require the PIN.
  - If one organization requires a **4-Digit** PIN and a second organization requires a **6-Digit**, the user will be required to enter a 6-digit PIN.
- If the PIN code is already enabled, and the administrator changes the length of the PIN code required, users must first enter the app using the old PIN and then create a new PIN of the new length.
- It is not possible for the user to reset their PIN. If forgotten, to create a new PIN, the user must unpair their device, and then define their PIN code when pairing their device again.

If an administrator edits the PingID mobile app configuration to require a PIN code, changes are implemented at the user level according to the PingID version and the user flow:

- Users installing the PingID mobile app for the first time are asked to create a PIN during the mobile app pairing flow.
- Users are prompted to define a PIN code the next time they open the PingID mobile app when online.

PingID Mobile Device Management (MDM)

This section describes the steps to configure PingID's MDM integration, which verifies that devices connected through the PingID mobile app are managed by the organization's MDM infrastructure.

MDM is the administration of mobile devices, such as smartphones, tablet computers, and laptops. It can also be applied to desktop computers. Organizations can control activities of their employees by implementing MDM products or services.

MDM primarily deals with corporate data segregation, securing emails and corporate documents on mobile devices. MDM enforces corporate policies and supports the integration and management of mobile devices including laptops and hand-held devices of various categories.

Note

- PingID's MDM feature can only be used when the organization integrates with an MDM system.
- Two MDM systems cannot manage the same mobile device.
- This solution should work with any MDM system from the major vendors. PingID is officially supported with the following MDM solutions:
  - MobileIron
  - Workspace ONE UEM (formerly known as AirWatch)
  - Microsoft Intune

Copyright © 2025 Ping Identity Corporation

MDM integration flow

Integrating with an MDM involves the following steps:

1. Configure the PingID mobile application to include MDM and generate a token for MDM. Learn more in (Workforce Only) Configuring the PingID mobile application settings.
2. Configure the third-party MDM system for PingID integration.
    1. Generate and configure an APNS certificate for iOS in the MDM system. For example:
        - Installing an APNs certificate for iOS in Workspace ONE UEM
        - Installing an APNs certificate for iOS in MobileIron
        - Installing an APNs certificate for iOS in Microsoft Intune
    2. Configure Android for Work in the MDM system so that the PingID mobile app configuration can be pushed to managed mobile devices. For example:
        - Configuring Android for Work for Workspace ONE UEM
        - Configuring Android for Work for MobileIron
        - Configuring Android for Work for Microsoft Intune
    3. In the organization's MDM system, add PingID as a managed app and configure the token that was generated in PingOne admin portal. For example:
        - Configuring Workspace ONE UEM for PingID MDM integration.
        - Configuring MobileIron for PingID MDM integration
        - Adding the PingID mobile app for Microsoft Intune in iOS and Android.
3. After configuration, the MDM system distributes the token to its managed devices. During pairing and authentication, the PingID server compares the user's token with current active tokens, and the flow can only continue if there is a match between the user's token and a currently active PingID token.PingID permits administrators to define more than one active token.

Ongoing maintenance

As part of periodic MDM maintenance activities, you can generate new tokens for the PingID mobile app and revoke old tokens. Learn more in the following topics:

- PingID: You can generate a new token, rotate a token, or revoke a token. Learn more: Managing MDM tokens
- For the supported MDM systems:
    - Updating a PingID token in Workspace ONE UEM

Copyright © 2025 Ping Identity Corporation

Managing MDM tokens

Create, rotate, or revoke an MDM token.

- Creating a token:
  - Multiple keys can coexist, for example, for allowing time for rotating keys and the time it takes to phase in new keys and retire old ones. PingID checks all listed keys to verify a match with the key submitted in the authentication request.
  - The MDM does not retain multiple values for the same token. Support for multiple keys is provided through PingID.
  - The generated date following each token indicates the date and time of its creation.
- Revoking a token:
  - Organizational security policies might require periodic revocation of retired or obsolete tokens to prevent use of old tokens for authentication.
  - A minimum of one token must be retained. If you delete the only token, a new replacement token is automatically generated.
- Rotating a token:
  - Organizational security policies might require periodic rotation of MDM tokens to prevent use of old tokens for authentication.
  - To rotate a token, add a new token, distribute it to all managed devices, and then revoke the old token.

Generate an MDM token

Create an MDM token in the PingID application.

Steps

1. To manage MDM tokens, go to **Applications > Applications** > PingID Mobile* and click **Edit**.

   Result:

   In the **Mobile Requirements** area, under **Require mobile device management**, a list of MDM tokens is displayed.

2. Click **+Generate New Token** and copy the value of the new token key.
3. To update the token in the MDM system:
   1. Sign on to the MDM system, and go to the app configuration settings page.
   2. Update the **PINGID_MDM_TOKEN** token key.
   3. Delete the existing key value. In its place, paste the value of the new shared token key that you generated in the previous step.

Rotate an MDM token

You can rotate an MDM token.

Copyright © 2025 Ping Identity Corporation

About this task

To rotate an MDM token, generate a new MDM token, distribute it to all managed devices and then revoke the old token.

> **Caution**
>
> More than one token should coexist to permit token rotation without blocking users from authentication. If you have only one token and generate a new token by revoking the single listed token, all devices will be prevented from authenticating until the new token value is both updated in the MDM, and distributed to all devices. In such a case, consider setting the **Effective Date** to a future date to allow sufficient time for distribution of the new token to all devices.

Steps

1. Go to **Applications** > **Applications** > **PingID Mobile** and click **Edit**.

   Result:

   In the **Mobile Requirements** area, under **Require mobile device management**, a list of MDM tokens displays.

2. Click **+Generate New Token**, copy the value of the new token key, and then click **Save**.
3. Update the token key in the MDM system:
   1. Sign on to the MDM system, and go to the app configuration settings page.
   2. Update the **PINGID_MDM_TOKEN**.
   3. Delete the existing key value. In its place, paste the value of the new shared token key that you generated in the previous step.
4. Revoke the old MDM token:
   1. Go to **Applications** > **Applications** > **PingID Mobile** and click **Edit**.
   2. In the **Mobile Requirements** area, under **Require mobile device management**, next to the relevant token, click **Revoke**, and then click **Save**.

Revoke an MDM token

You can revoke an MDM token.

About this task

A minimum of one token must be retained. If you delete the only token, a new replacement token is automatically generated.

> **Important**
>
> At least one token must always exist. If you revoke the only token that exists, a new one is generated automatically. In such a case, all devices will be prevented from authenticating until the new token value is both updated in the MDM and distributed to all devices. Consider setting the **Effective Date** to a future date to allow sufficient time for distribution of the new token to all devices.

Steps

1. Go to **Applications** > **Applications** > **PingID Mobile** and click **Edit**.

Copyright © 2025 Ping Identity Corporation

Result:

In the **Mobile Requirements** area, under **Require mobile device management**, a list of MDM tokens displays.

2. Next to the relevant token entry, click **Revoke**, and then click **Save**.

Third-party MDM system configuration for PingID integration

Configuring any third-party mobile device management (MDM) system for the purpose of integrating with PingID typically requires the following steps:

1. Generate and configure an Apple Push Notification Service (APNS) certificate for iOS in the MDM system.
2. Configure Android for Work in the MDM system so that the PingID mobile app configuration can be pushed to managed phone sets.
3. In the organization's MDM system, add PingID as a managed app and configure the token that was generated in PingOne.

Examples of these configuration steps are available for the officially supported MDM systems:

- Configuring Workspace ONE UEM for PingID mobile app
- Configuring MobileIron for PingID
- Configuring Microsoft Intune for PingID

Configuring Workspace ONE UEM for PingID mobile app

To manage the PingID mobile app using Workspace ONE UEM (formerly known as AirWatch), you must apply several configuration settings.

The initial Workspace ONE UEM configuration comprises the following:

1. Installing an APNs certificate for iOS in Workspace ONE UEM
2. Configuring Android for Work for Workspace ONE UEM
3. Configuring Workspace ONE UEM for PingID MDM integration

Ongoing maintenance:

- Installing an APNs certificate for iOS in Workspace ONE UEM
- Configuring Android for Work for Workspace ONE UEM
- Configuring Workspace ONE UEM for PingID MDM integration

Ongoing maintenance

Copyright © 2025 Ping Identity Corporation

As part of MDM maintenance activities, new tokens for the PingID mobile app can be generated and old tokens revoked. Learn more in the following topics:

- Learn more about generating, rotating, or revoking an MDM token in PingOne in Managing MDM tokens.
- Learn more about token management in Workspace ONE UEM in Updating a PingID token in Workspace ONE UEM.

> **Note**
>
> This section documents use cases where PingID authenticating devices are managed by the Workspace ONE UEM MDM. If you want to use PingFederate to apply policies on accessing devices managed by Workspace ONE UEM, refer to the Workspace ONE UEM Integration Kit documentation.

Installing an APNs certificate for iOS in Workspace ONE UEM

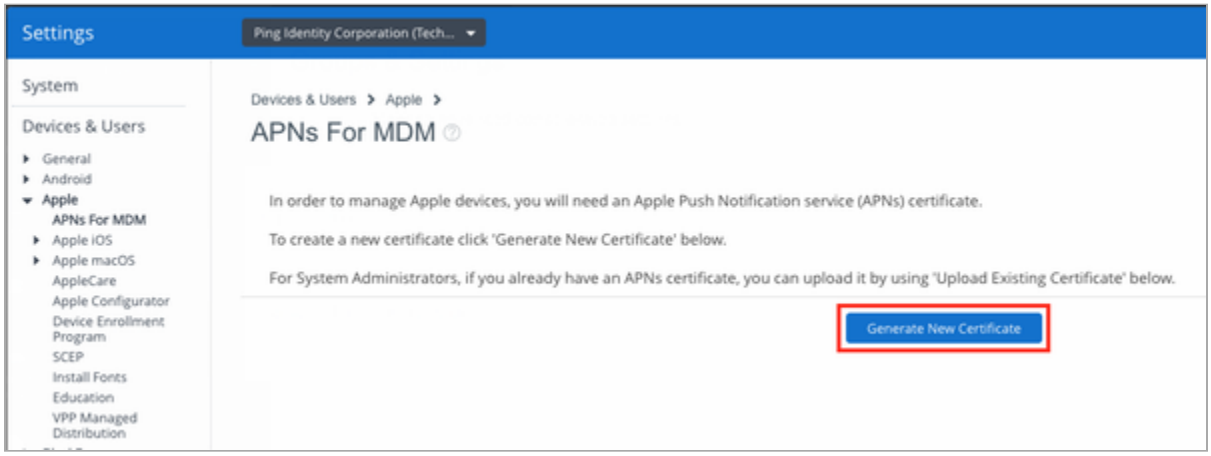
Install an Apple Push Notification service (APNs) certificate in Workspace ONE UEM.

About this task

To support iOS devices, an Apple mobile device management (MDM) certificate must be installed in the organization's MDM.

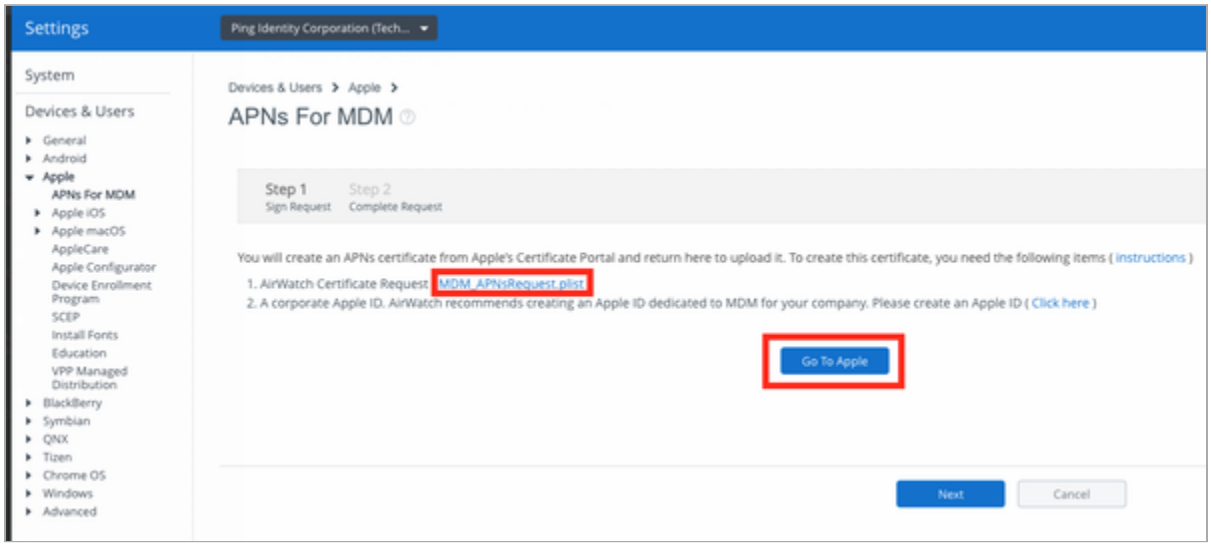
Steps

1. In the Workspace ONE UEM admin console, download an APNS certificate signing request (CSR):
    1. Go to **Settings** > **Apple** > **APNs for MDM**.
    2. Click **Generate New Certificate**.

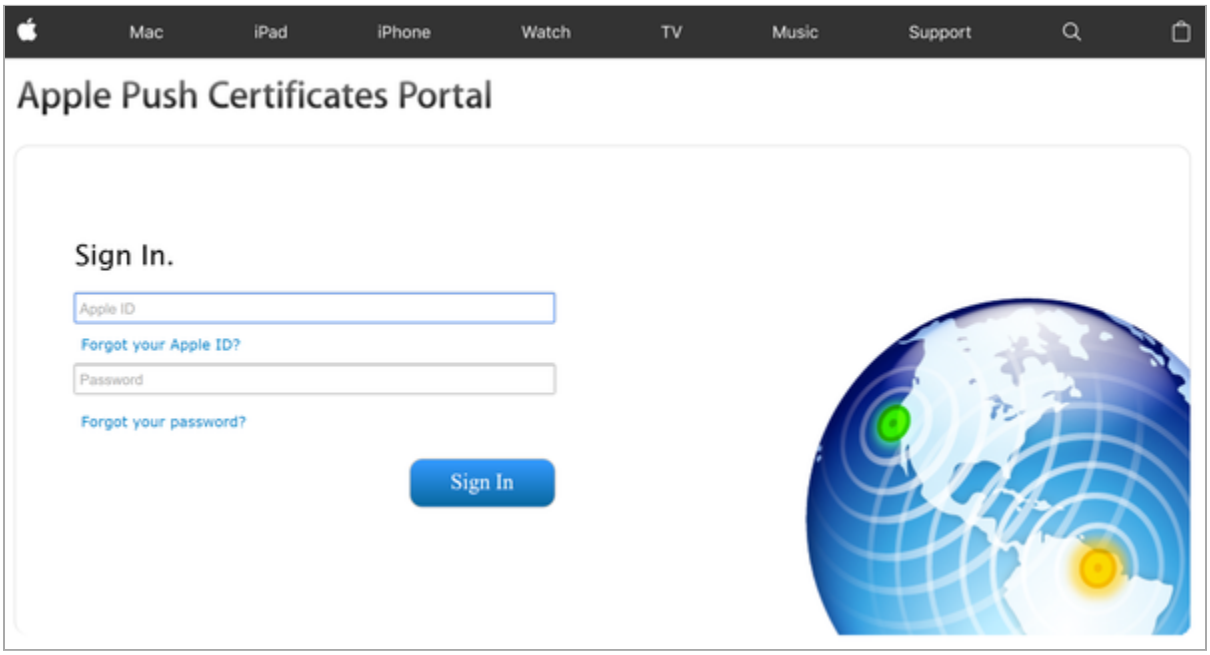


    3. Click **MDM_APNsRequest.plist**.
    4. Click **Go To Apple**.

Copyright © 2025 Ping Identity Corporation



2. Sign on to the Apple Push Certificates Portal.



3. Click **Create a Certificate** on either the **Get Started** window or the **Certificates for Third-party Servers** window.

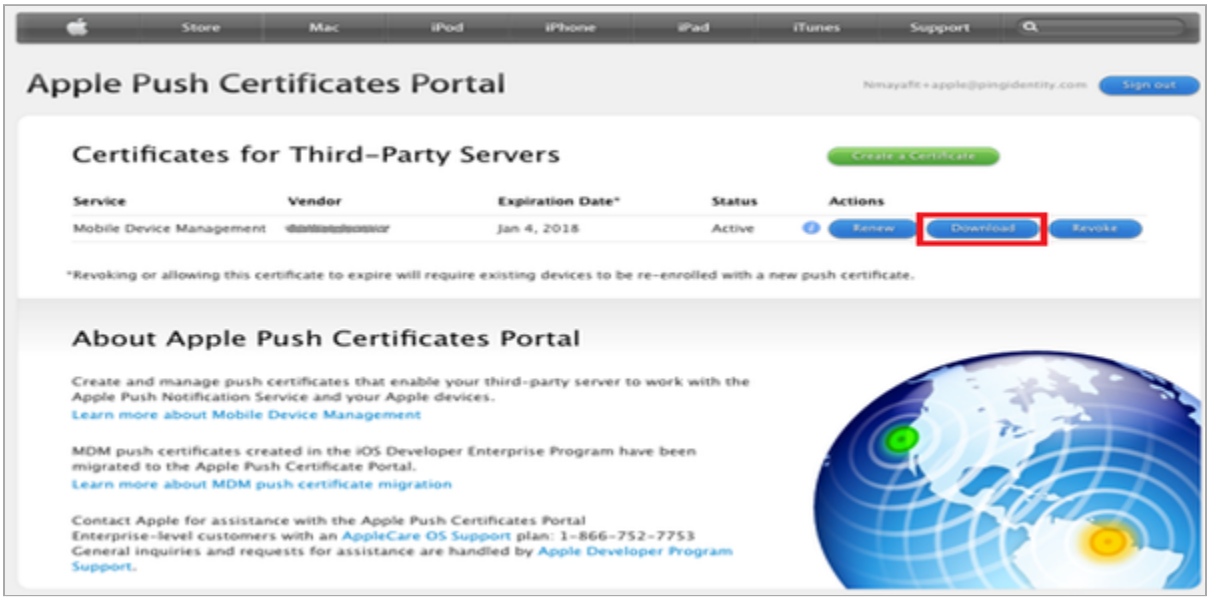
Note

If your organization does not yet have any Apple Push Certificates, the **Get Started** section is displayed. Otherwise, the **Certificates** list view window is displayed.

4. To browse for the CSR file created previously, click **Choose File**, and then click **Upload**.

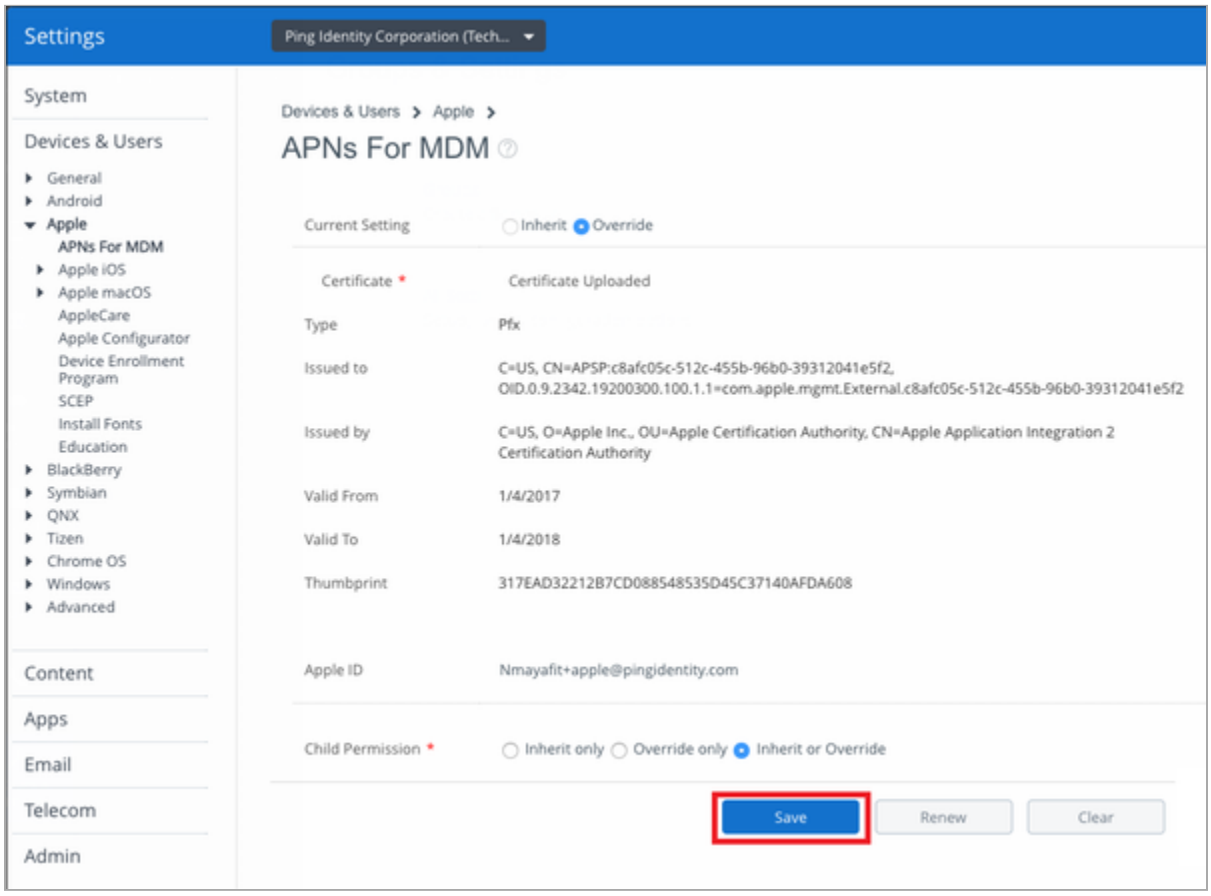
5. Click **Download**.

Copyright © 2025 Ping Identity Corporation



6. Upload the APNs certificate in Workspace ONE UEM:

   1. Go to **Devices & Users > Apple > APNs for MDM**.



   7. Click **Save**.

Configuring Android for Work for Workspace ONE UEM

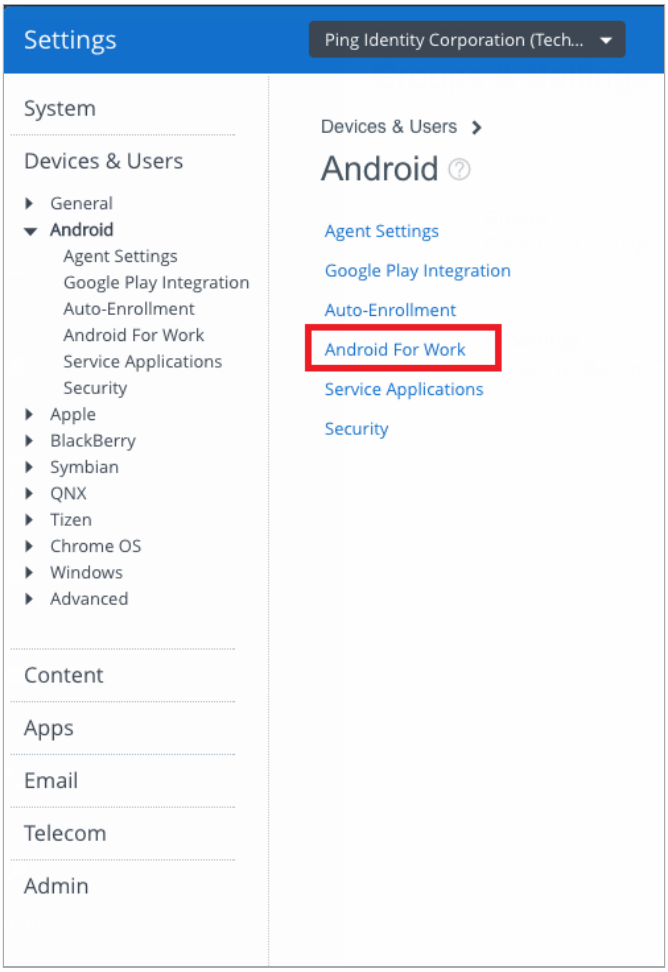
Configure Android for Work for the organization's mobile device management (MDM) so that the PingID mobile app configuration can be pushed to Android devices.

About this task

> **Note**
>
> This is an example configuration of Android for Work with G Suite. Android for Work can also be configured for MDM without G Suite.

Steps

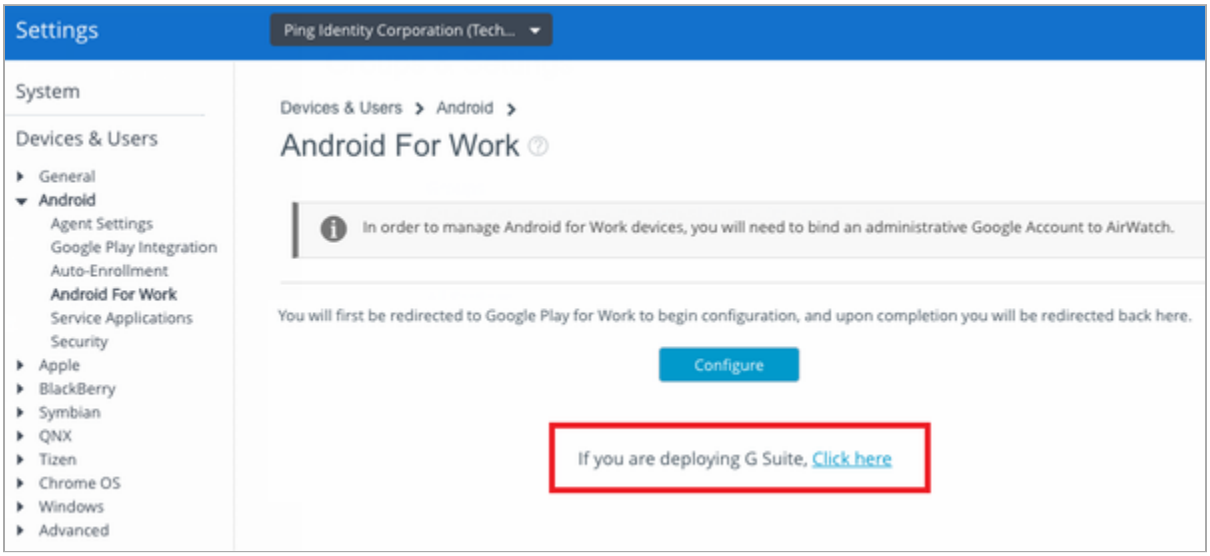
1. In Workspace ONE UEM, go to **Settings** > **Devices & Users** > **Android** > **Android For Work**.



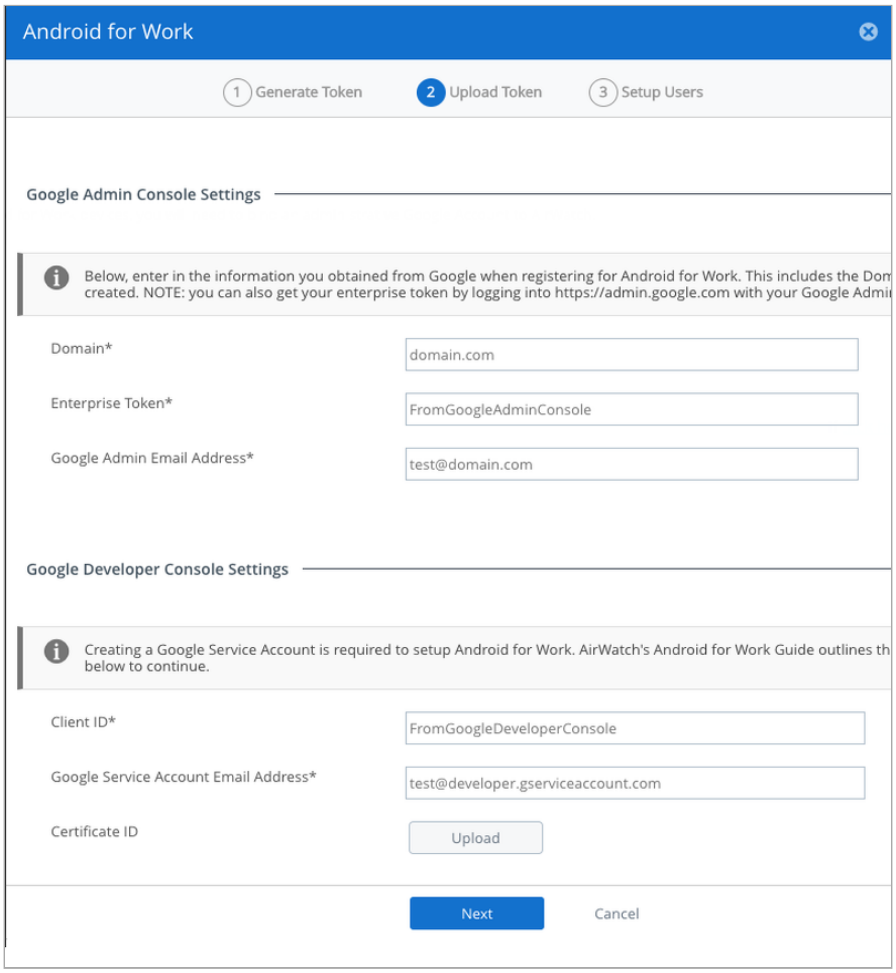
2. Click **Click here**.

   The browser redirects to G Suite, and on completion of the configuration, returns to Workspace ONE UEM.

Copyright © 2025 Ping Identity Corporation



3. In Workspace ONE UEM, in the **Android For Work** window, click **Configure**, and enter the required details.



Configuring Workspace ONE UEM for PingID MDM integration

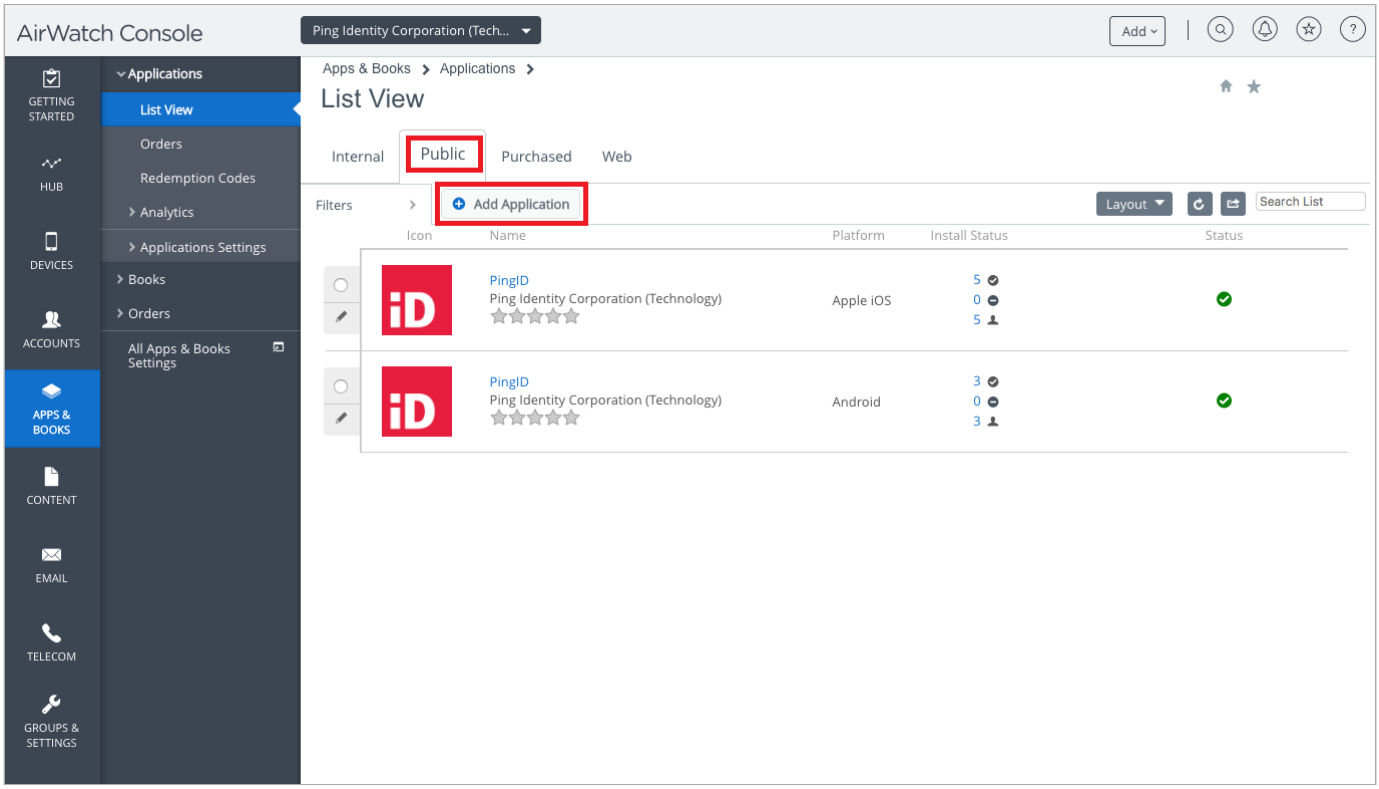
Configure PingID mobile app as a mobile device management (MDM) managed app in Workspace ONE UEM (formerly known as AirWatch).

About this task

> **Important**
>
> The procedure detailed here is the iOS example for the configuration of Workspace ONE UEM for PingID MDM integration. The procedure for Android is identical. If the organization's MDM manages both iOS and Android devices, configure and save the entire procedure separately for each platform.

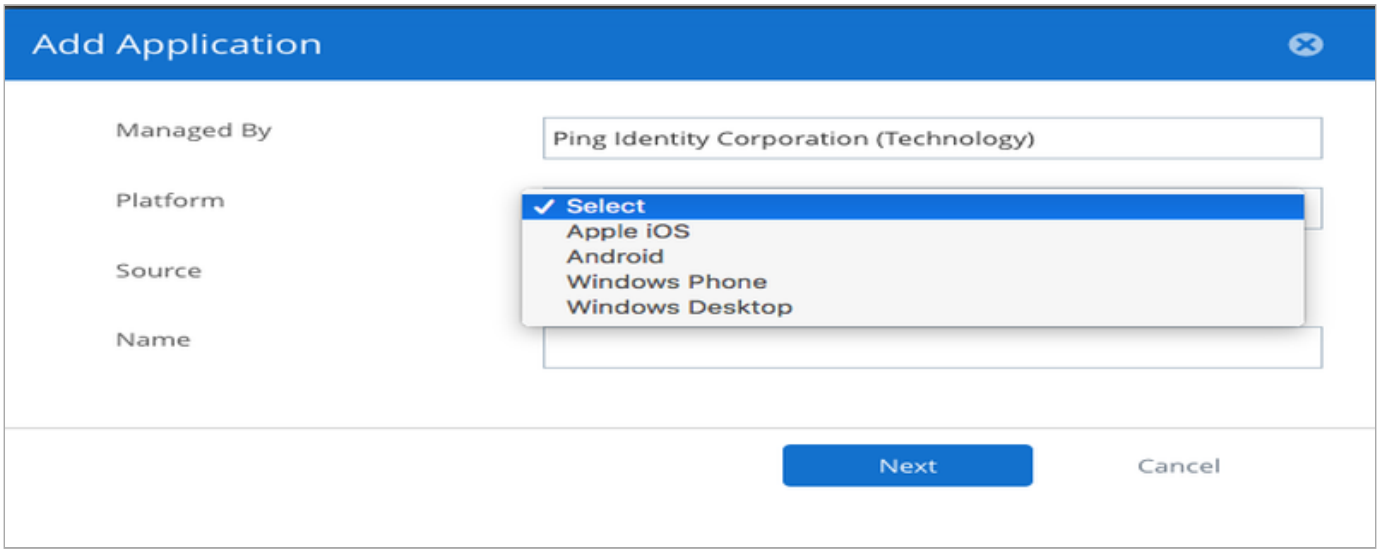
Steps

1. In the Workspace ONE UEM admin console, go to **Apps & Books** > **Applications** > **List View**
2. On the **Public** tab, click **Add application**.

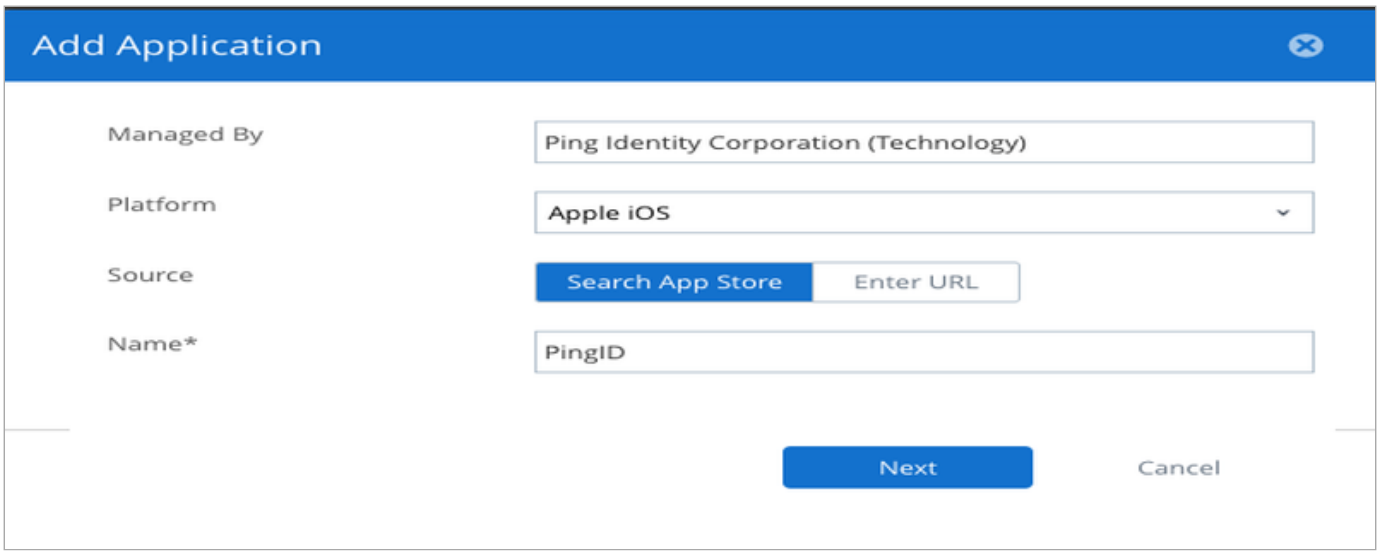


3. From the **Platform** list, select **Apple iOS**.

Copyright © 2025 Ping Identity Corporation



4. In **Source** field, click **Search App Store**.

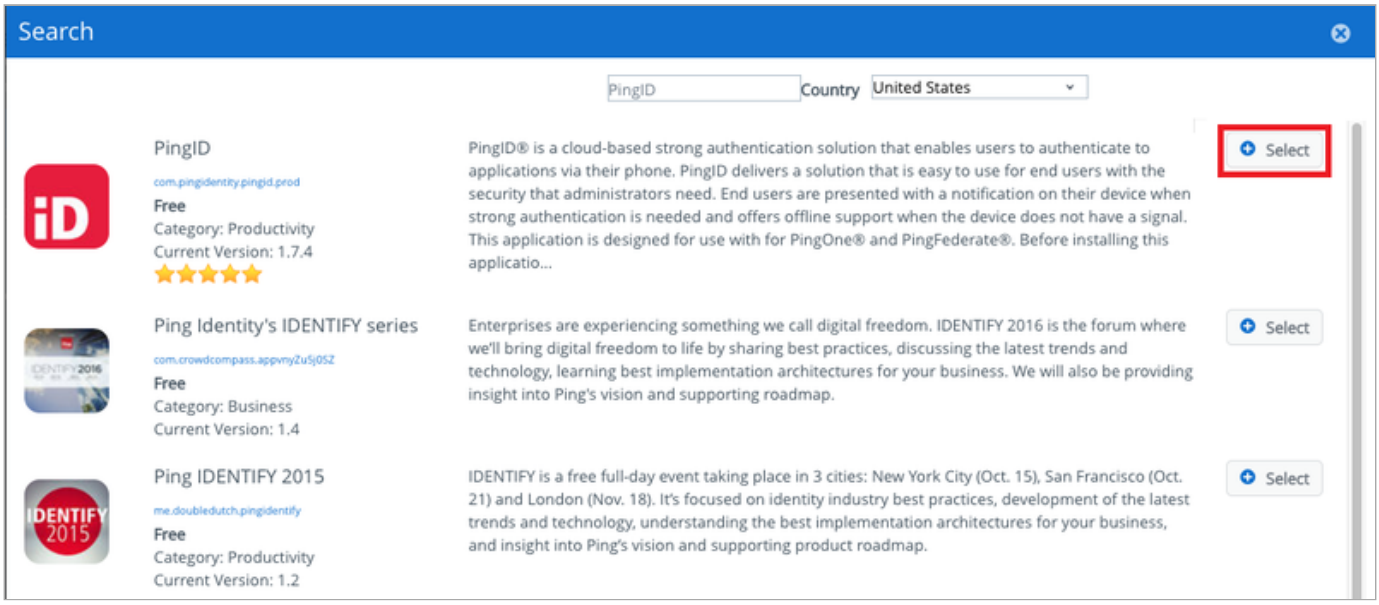


5. In **Name** field, enter `PingID`.

6. Click **Next**.

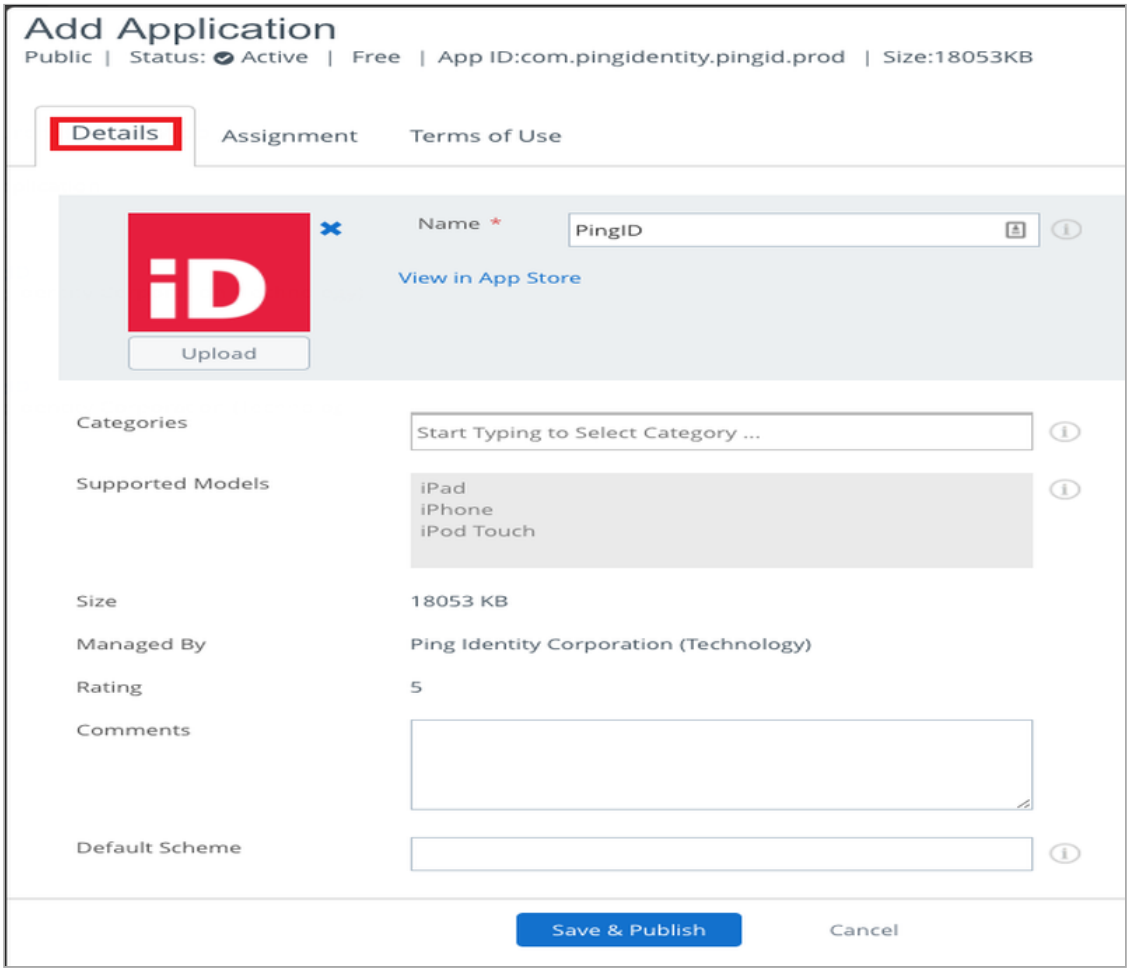
7. In the mobile app store, for the PingID mobile app, click **Select**.

Copyright © 2025 Ping Identity Corporation



Result:

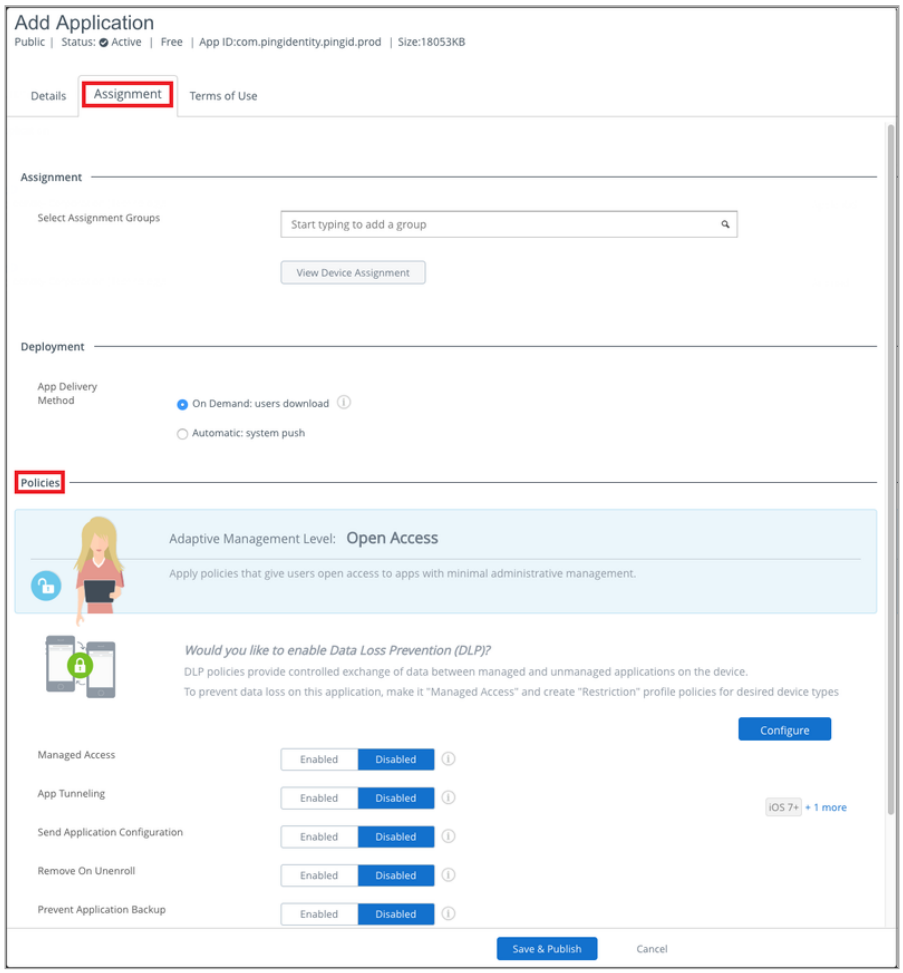
The PingID mobile app's details are displayed on the **Details** tab.



8. Click the **Assignment** tab.

Copyright © 2025 Ping Identity Corporation

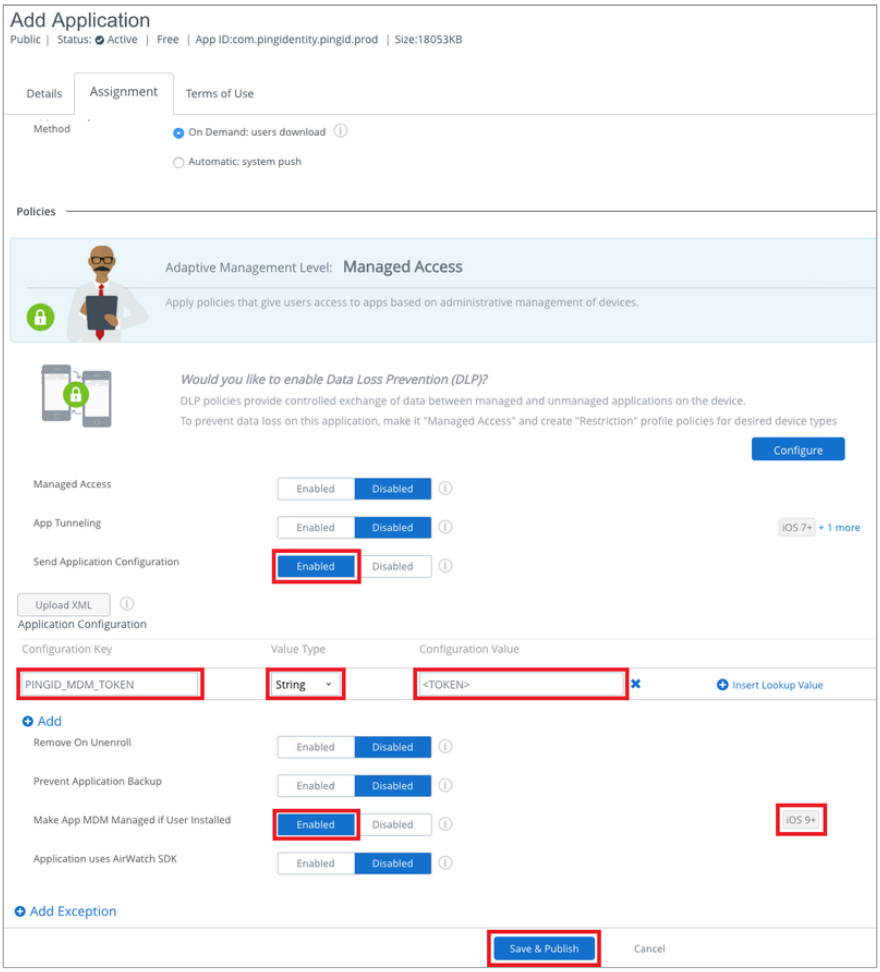
9. Go to the **Policies** section.



10. In the **Send Application Configuration** field, click **Enabled**.

    Result:

    The **Application Configuration** section displays.



11. In the **Application Configuration** section, enter the following parameter values:

Parameter	Value
Configuration Key	`PINGID_MDM_TOKEN`. **Note** ◦ For iOS, the value `PINGID_MDM_TOKEN` must be entered manually. ◦ For Android, the value `PINGID_MDM_TOKEN` is prepopulated.
Value Type	`STRING`
Configuration value	The token string value for MDM, as generated in the PingOne application configuration page.

12. In the **Make app MDM Managed If User Installed** field, click **Enabled**.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> This option transitions a non-managed app downloaded from the app store to a managed app. The user must approve it on their device.

> **Important**
>
> ***For Apple devices earlier than iOS 9 and Android devices***
>
> Users must execute the following steps:
>
> 1. Unpair the PingID mobile app on the iOS device.
> 2. Uninstall the PingID mobile app from the iOS device.
> 3. Reinstall the PingID mobile app, from the MDM's app catalog.
> 4. Pair the newly installed, MDM managed PingID mobile app.
>
> ***For Apple devices with iOS 9 and later***
>
> The user receives a notification on their device to approve the transition to MDM management. After user approval, the PingID mobile app installed on the iOS device is managed by the MDM.

13. Click **Save & Publish**.

> **Important**
>
> Repeat the entire configuration process for Android. The prerequisite to the Android app configuration is Configuring Android for Work for Workspace ONE UEM.

Updating a PingID token in Workspace ONE UEM

Update the token PingID managed app in Workspace ONE UEM for iOS

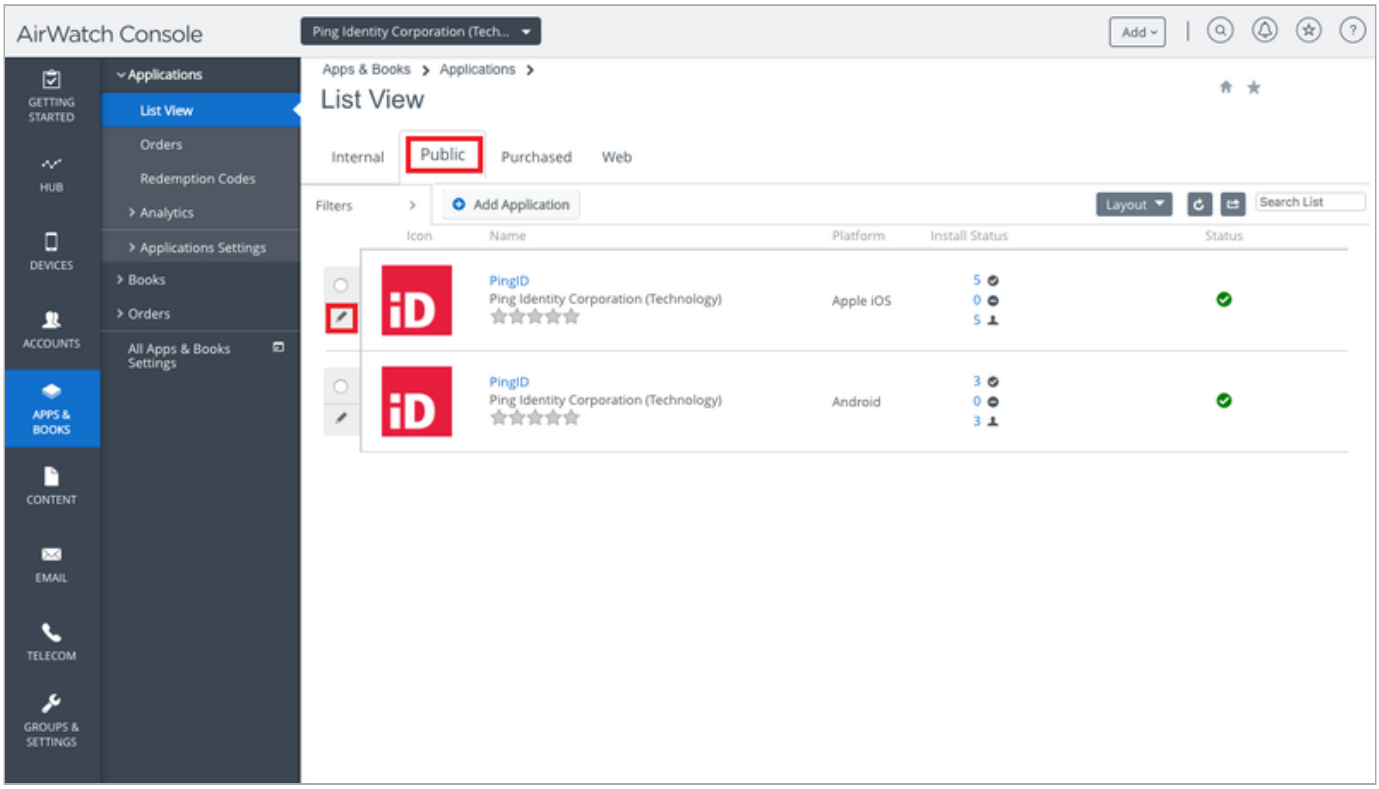
About this task

> **Important**
>
> You must configure and save the entire procedure separately for each platform.

Steps

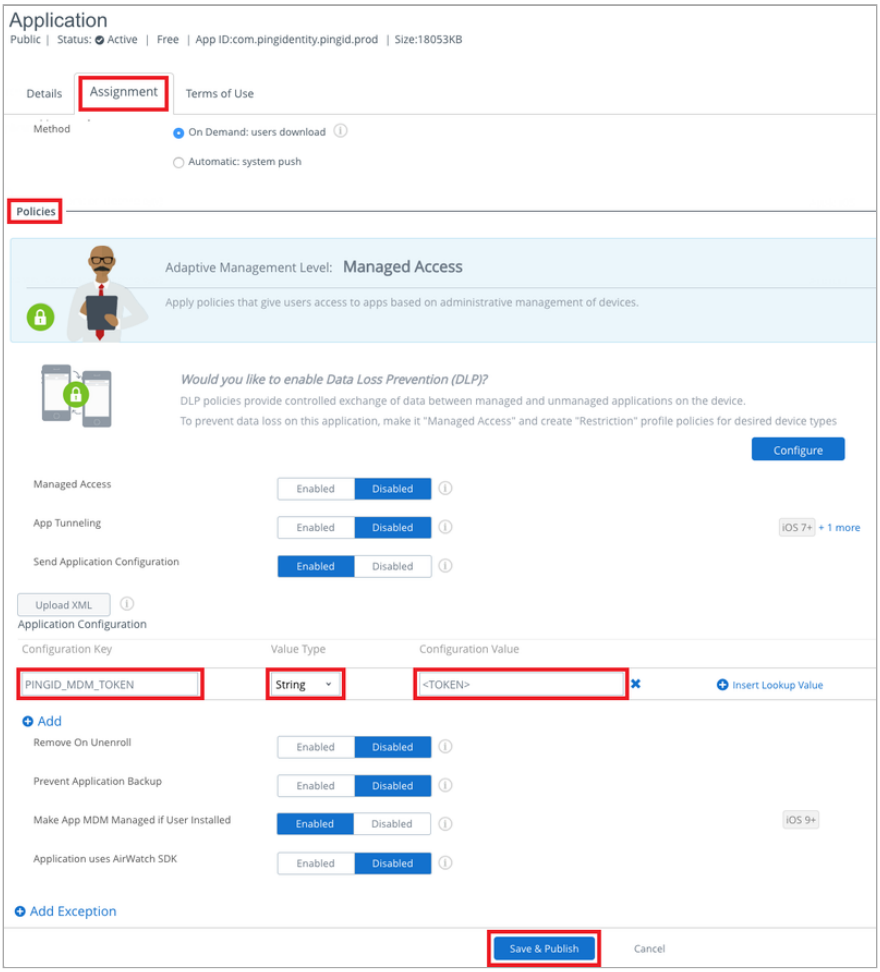
1. In the Workspace ONE UEM admin console, go to **Apps & Books → Applications → List View**.
2. On the **Public** tab, select the **PingID iOS** app to edit, and then click the **Pencil** icon.

Copyright © 2025 Ping Identity Corporation



3. Click the **Assignment** tab.

Copyright © 2025 Ping Identity Corporation



4. Go to the **Policies** section.

5. In the **Application Configuration** section, enter the following parameter values.

Parameter	Value
Configuration Key	`PINGID_MDM_TOKEN`. **Note** ◦ For iOS, the value `PINGID_MDM_TOKEN` must be entered manually. ◦ For Android, the value `PINGID_MDM_TOKEN` is prepopulated.
Value Type	`STRING`
Configuration value	The token string value for MDM, as generated in the PingOne application configuration page.

6. Click **Save & publish**.

Copyright © 2025 Ping Identity Corporation

> **Important**
>
> Repeat the entire process for Android.

Configuring MobileIron for PingID

To manage PingID mobile app using MobileIron, you must apply several configuration settings.

The initial MobileIron configuration comprises the following:

1. Installing an APNs certificate for iOS in MobileIron
2. Configuring Android for Work for MobileIron
3. Configuring MobileIron for PingID MDM integration

Ongoing maintenance

As part of mobile device management (MDM) maintenance activities, new tokens for the PingID mobile app can be generated and old tokens revoked. Learn more in the following topics:

- For PingID, learn more about generating, rotating, or revoking an MDM token in PingOne in Managing MDM tokens.
- For MobileIron, learn more in Updating a PingID token in MobileIron.

> **Note**
>
> The previous configuration steps are for use cases where PingID multi-factor authentication (MFA) authenticating devices are managed by the MobileIron MDM. In cases where PingFederate is used to apply policies on accessing devices managed by MobileIron, refer to the PingFederate MobileIron Integration Kit documentation.

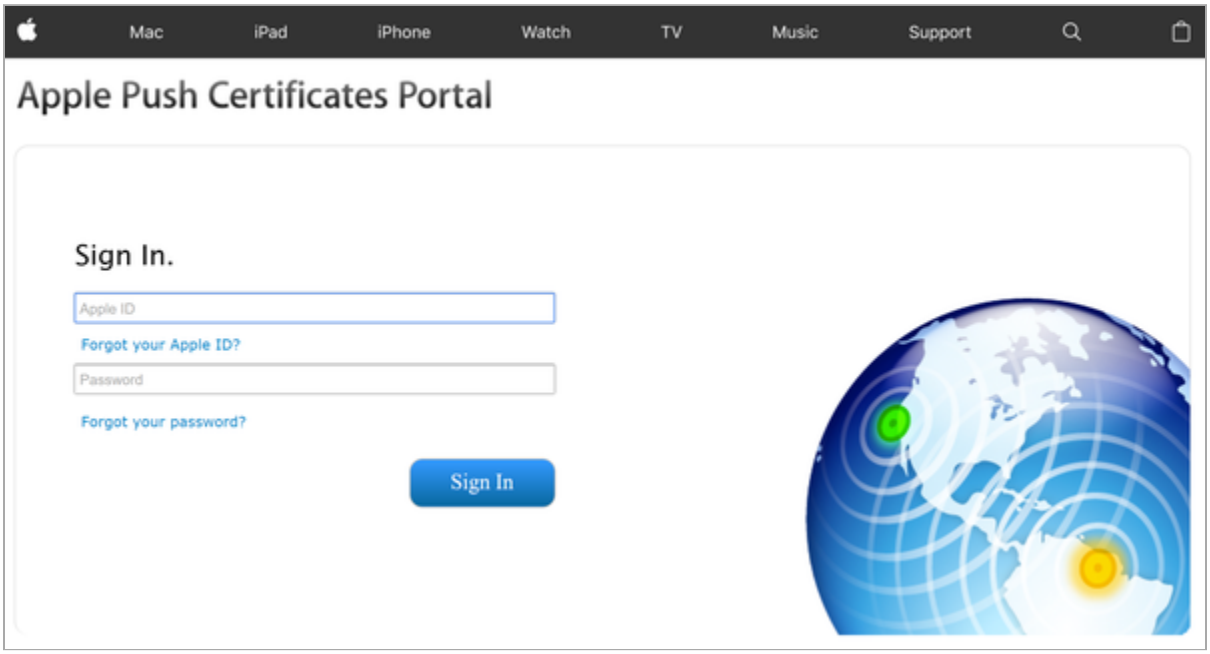
Installing an APNs certificate for iOS in MobileIron

To support iOS devices, install an Apple mobile device management (MDM) certificate in the organization's MDM.

Steps

1. In the MobileIron admin console, download an Apple Push Notification service (APNs) Certificate Signing Request (CSR):
    1. Go to **Admin > Apple/iOS > MDM Certificate > Download**.
    2. Click **Download File**.
2. Sign on to the Apple Push Certificates Portal.

Copyright © 2025 Ping Identity Corporation

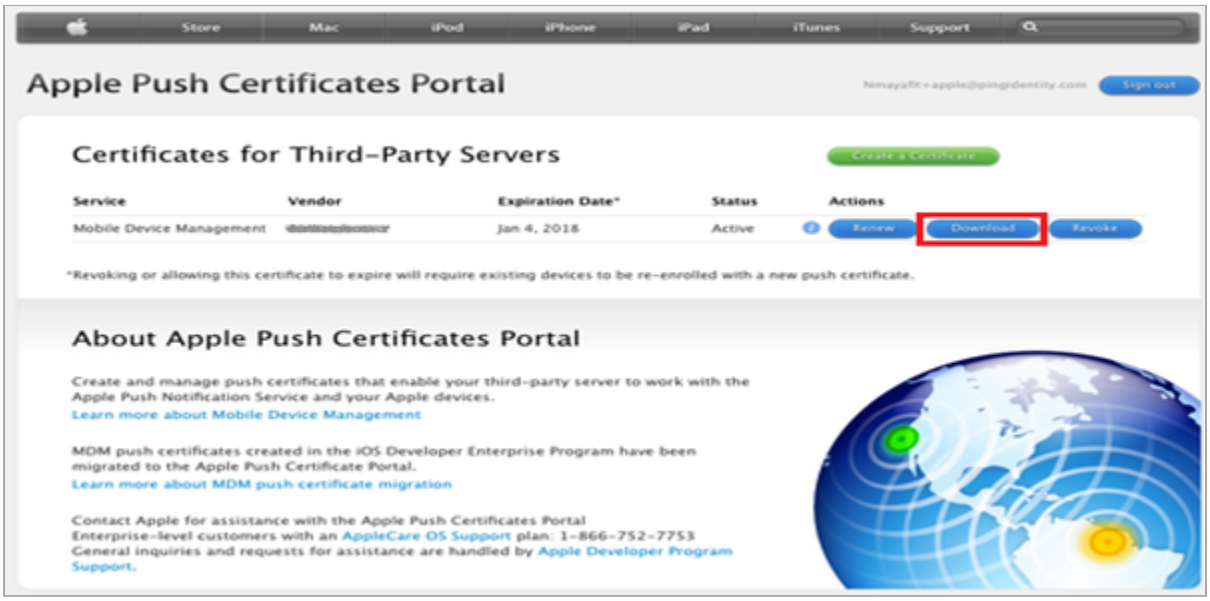


3. Click **Create a Certificate** on either the **Get Started** window, or the **Certificates for Third-party Servers** window.

> **Note**
>
> If your organization does not yet have any Apple Push Certificates, the **Get Started** section is displayed. Otherwise, the **Certificates** list view window is displayed.
>
>
>

4. To browse for the CSR file created earlier, click **Choose File**, and then click **Upload**.

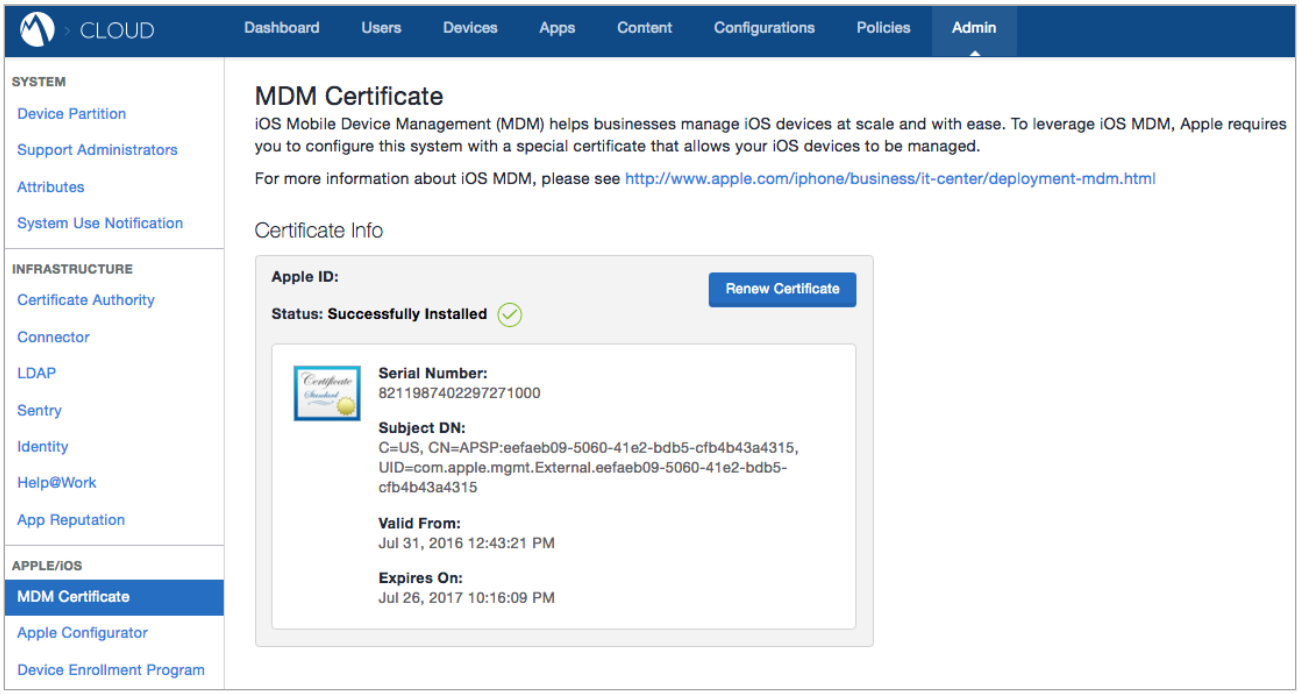
5. Click **Download**.



6. Upload the APNs certificate in MobileIron.

    1. Go to **Admin > Apple/iOS > MDM Certificate**.

Copyright © 2025 Ping Identity Corporation



7. Click **Save**.

Configuring Android for Work for MobileIron

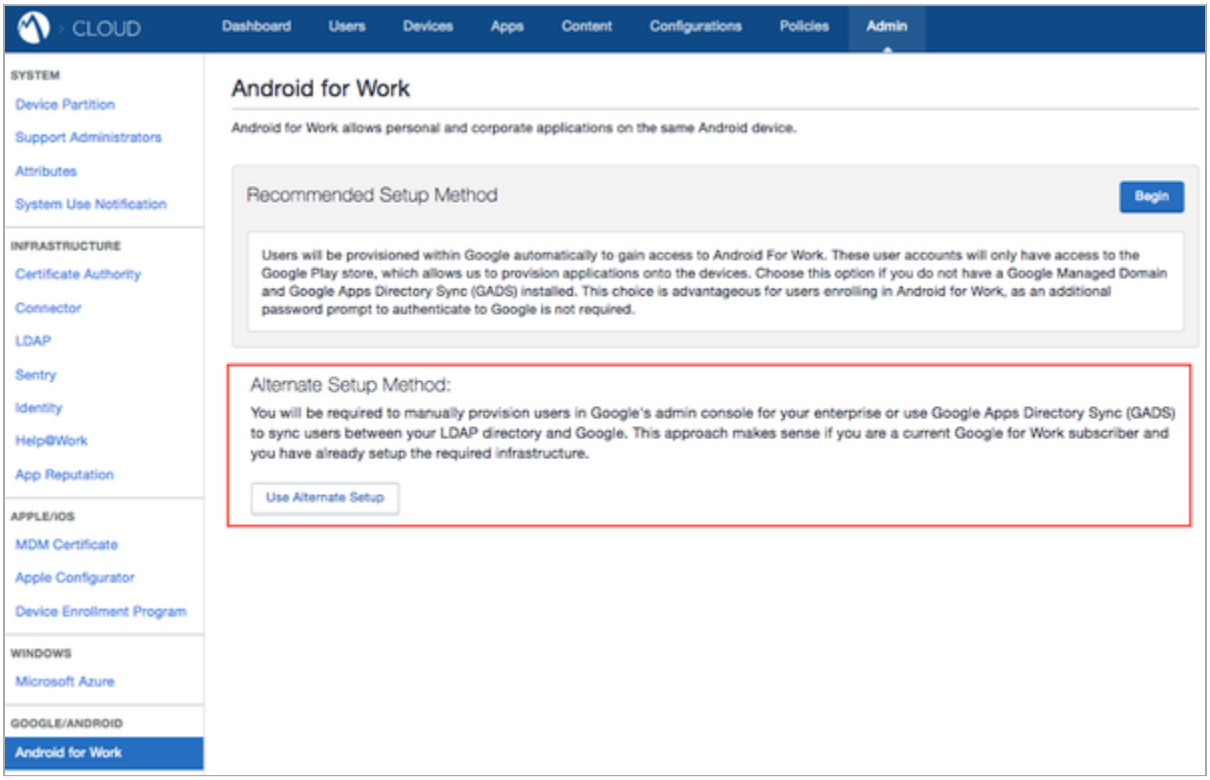
Configure Android for Work for the organization's mobile device management (MDM) so that the PingID mobile app configuration can be pushed to Android devices.

About this task

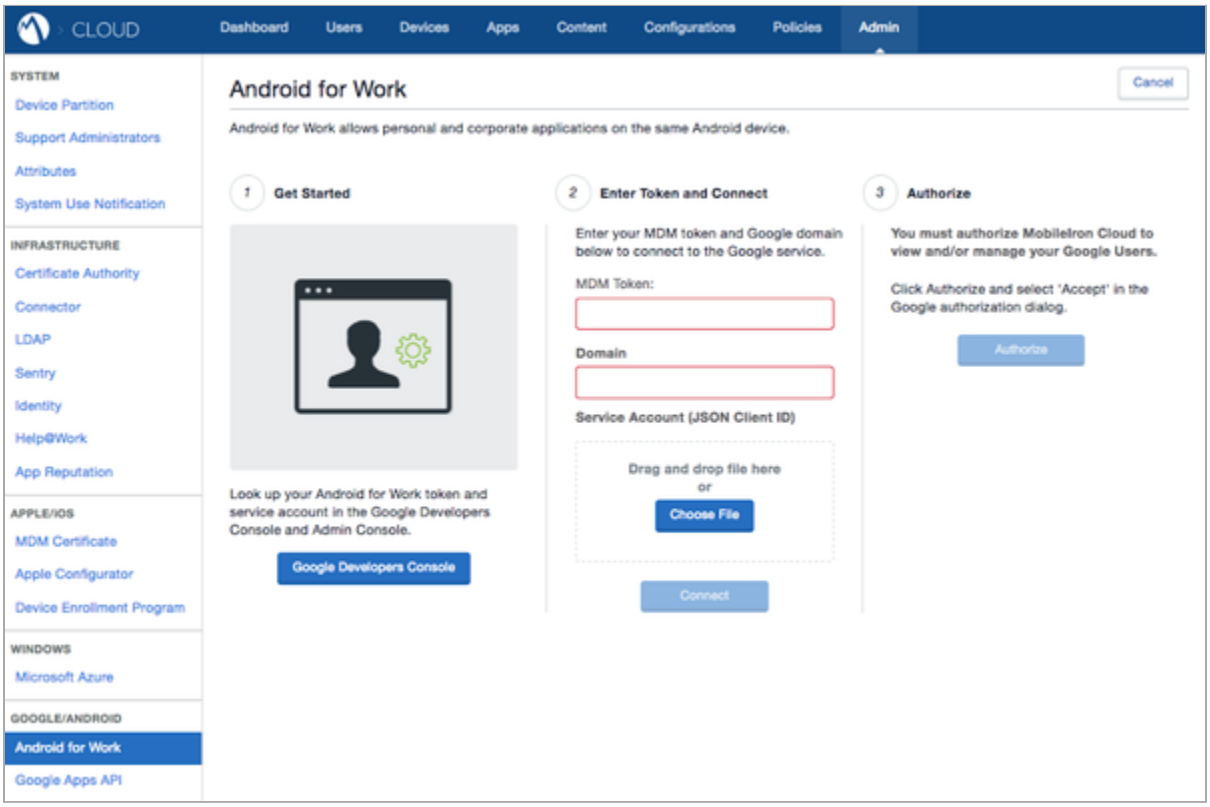
> **Note**
>
> This is an example configuration of Android for Work with G Suite. You can configure Android for Work MDM without G Suite.

Steps

1. Go to **Admin → Google/Android > Android for Work**, and then click **Use Alternate Setup**.



2. In the **Get Started** section, click **Google Developers Console**, and follow the on-screen instructions.



3. In MobileIron's admin portal, under **Enter Token and Connect**, connect to your organization's Google service.

4. In the **MDM Token** field, enter the token from the previous step.

Copyright © 2025 Ping Identity Corporation

5. In the **Domain** field, enter the domain by uploading the JSON file created earlier from the Google Developers Console, and click **Connect**.

6. To enable MobileIron to manage your Google users, click **Authorize**.

Configuring MobileIron for PingID MDM integration

Configure PingID mobile app as a mobile device management (MDM) managed app in MobileIron.

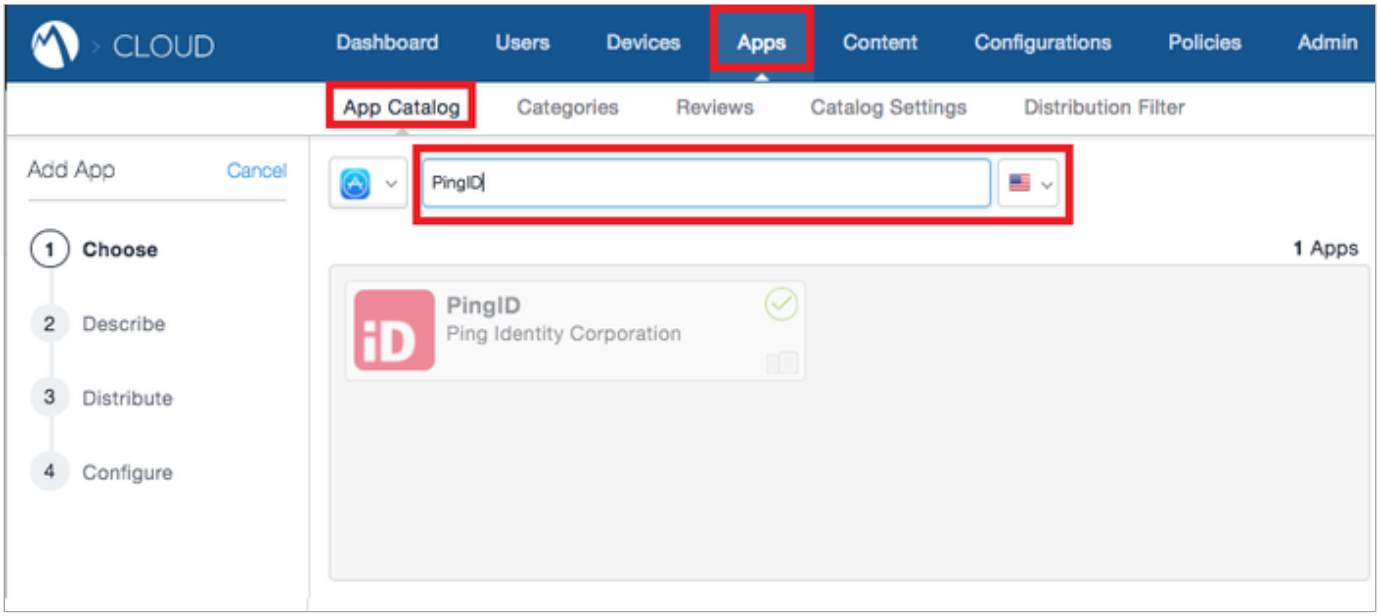
About this task

> **Important**
>
> The procedure detailed below is the iOS example for the configuration of MobileIron for PingID MDM integration. The procedure for Android is identical. If the organization's MDM manages both iOS and Android devices, configure and save the entire procedure separately for each platform.

Steps

1. In the MobileIron admin console, go to **Apps** > **App Catalog**.

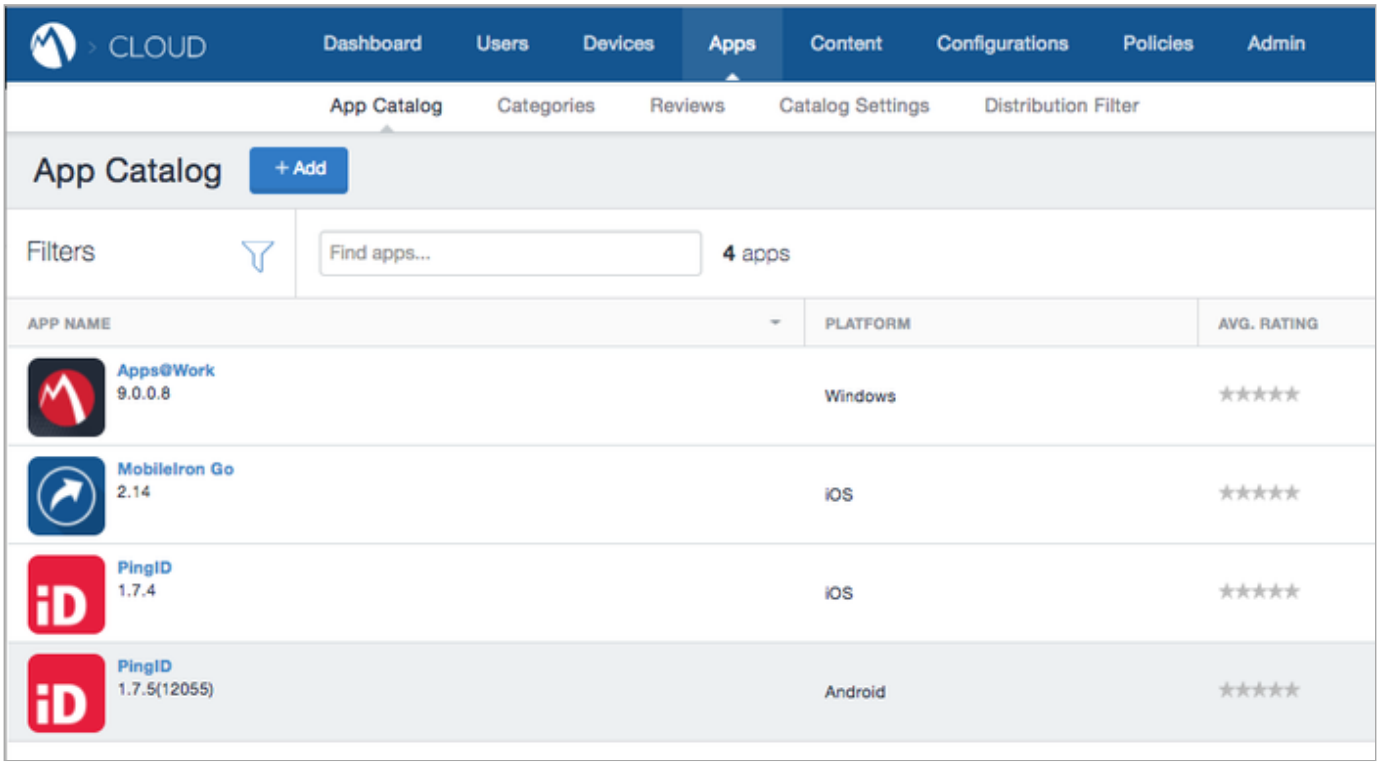
2. Choose the desired app store, and then search for PingID.



> **Note**
>
> The following steps describe the procedure for managing the PingID app for iOS. Repeat the procedure for the PingID app for Android.

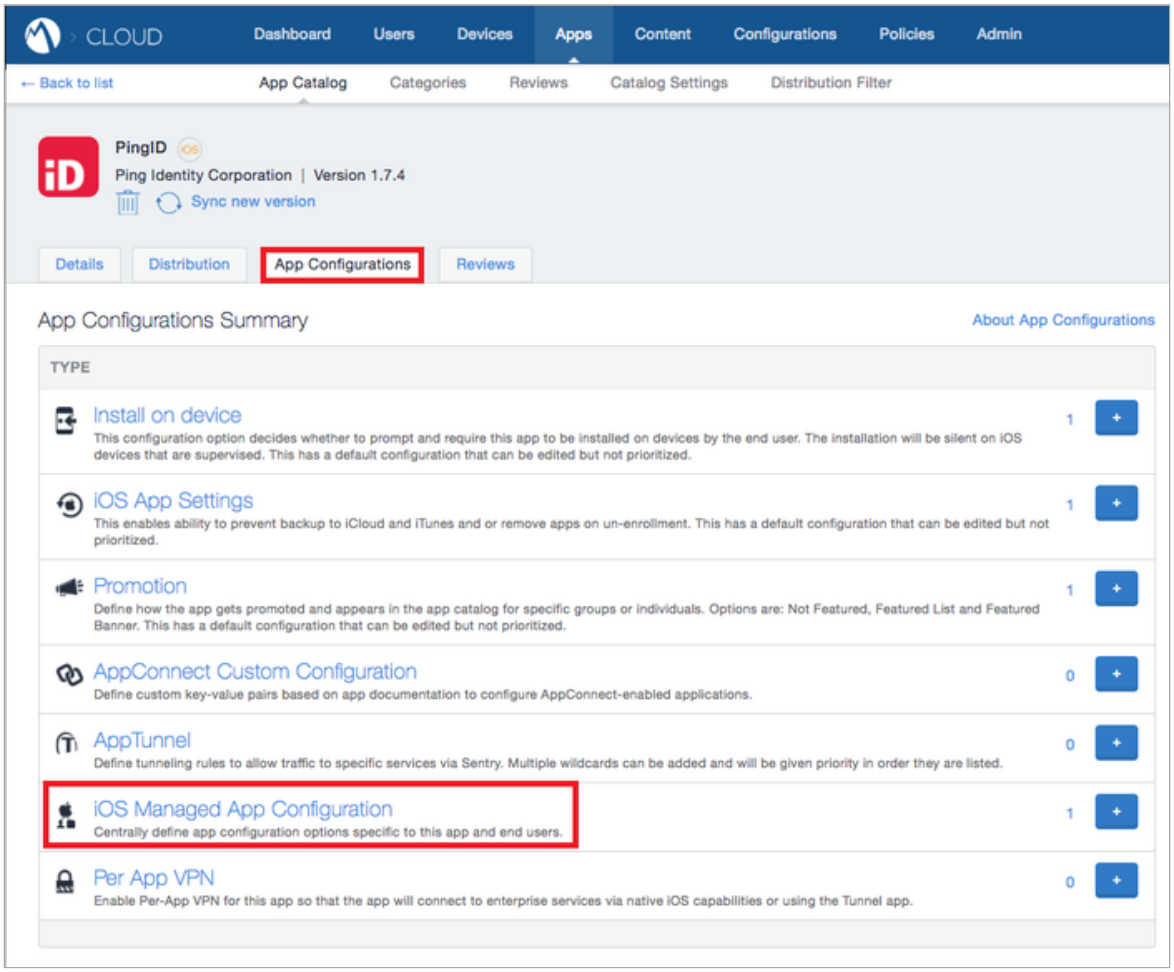
3. Select the PingID mobile app for iOS.

Copyright © 2025 Ping Identity Corporation

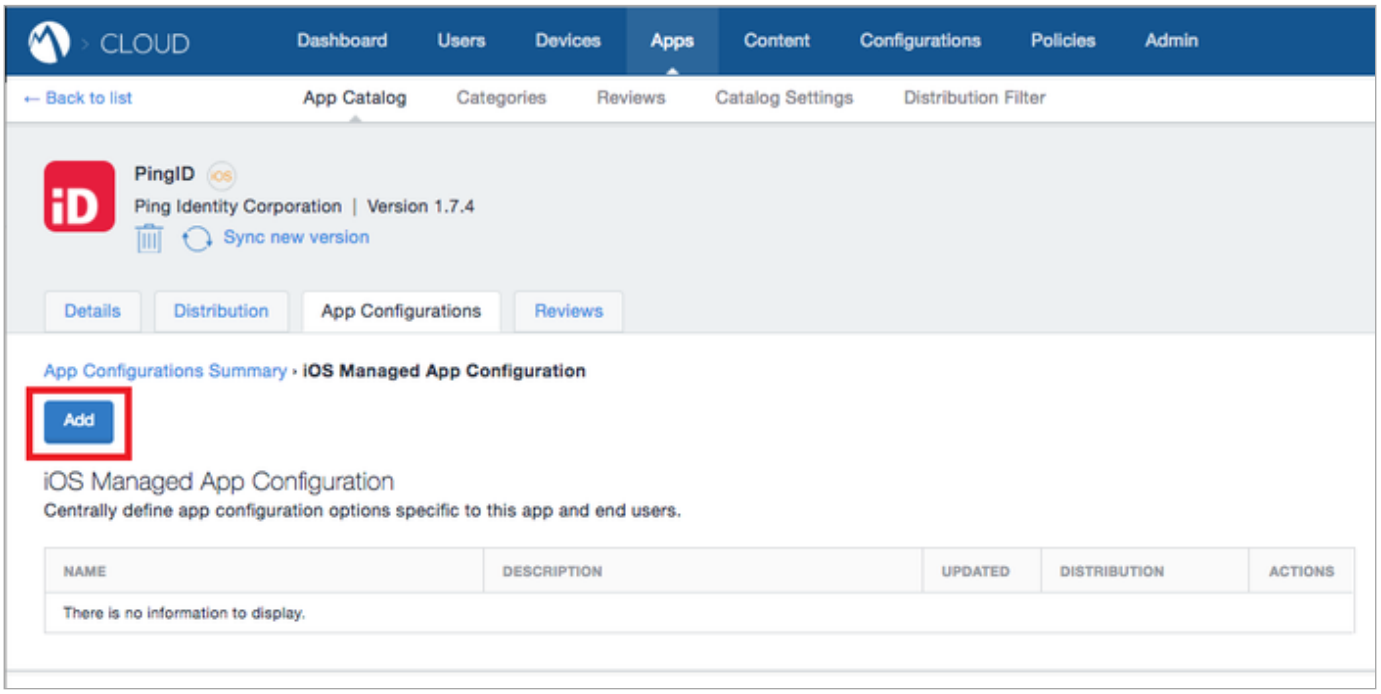


4. On the **App Configurations** tab, select **iOS Managed App Configuration**.

Copyright © 2025 Ping Identity Corporation

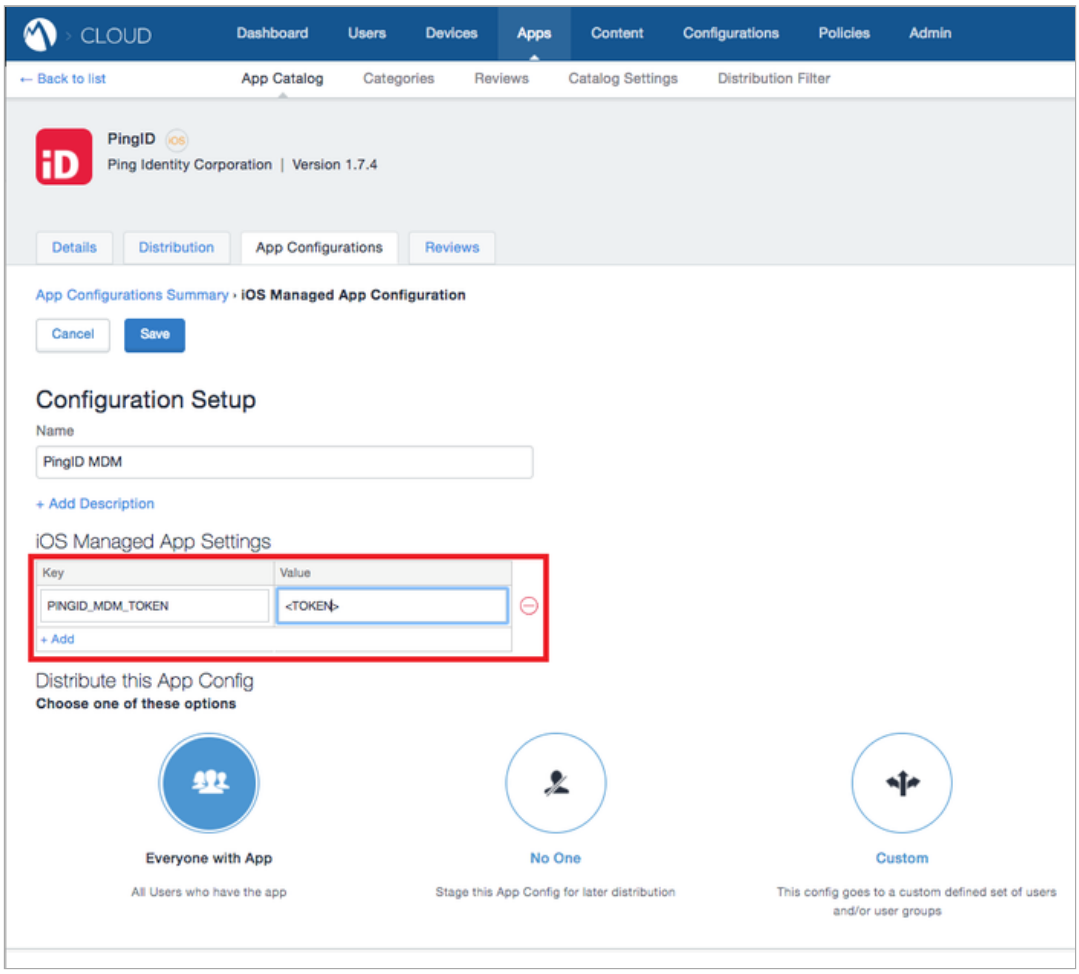

CLOUD
Dashboard
Users
Devices
Apps
Content
Configurations
Policies
Admin
← Back to list
App Catalog
Categories
Reviews
Catalog Settings
Distribution Filter
PingID
Ping Identity Corporation | Version 1.7.4
Sync new version
Details
Distribution
App Configurations
Reviews
App Configurations Summary
About App Configurations
TYPE
Install on device
This configuration option decides whether to prompt and require this app to be installed on devices by the end user. The installation will be silent on iOS devices that are supervised. This has a default configuration that can be edited but not prioritized.
1
iOS App Settings
This enables ability to prevent backup to iCloud and iTunes and or remove apps on un-enrollment. This has a default configuration that can be edited but not prioritized.
1
Promotion
Define how the app gets promoted and appears in the app catalog for specific groups or individuals. Options are: Not Featured, Featured List and Featured Banner. This has a default configuration that can be edited but not prioritized.
1
AppConnect Custom Configuration
Define custom key-value pairs based on app documentation to configure AppConnect-enabled applications.
0
AppTunnel
Define tunneling rules to allow traffic to specific services via Sentry. Multiple wildcards can be added and will be given priority in order they are listed.
0
iOS Managed App Configuration
Centrally define app configuration options specific to this app and end users.
1
Per App VPN
Enable Per-App VPN for this app so that the app will connect to enterprise services via native iOS capabilities or using the Tunnel app.
0

5. Click **Add**.


CLOUD
Dashboard
Users
Devices
Apps
Content
Configurations
Policies
Admin
← Back to list
App Catalog
Categories
Reviews
Catalog Settings
Distribution Filter
PingID
Ping Identity Corporation | Version 1.7.4
Sync new version
Details
Distribution
App Configurations
Reviews
App Configurations Summary › iOS Managed App Configuration
Add
iOS Managed App Configuration
Centrally define app configuration options specific to this app and end users.
NAME
DESCRIPTION
UPDATED
DISTRIBUTION
ACTIONS
There is no information to display.

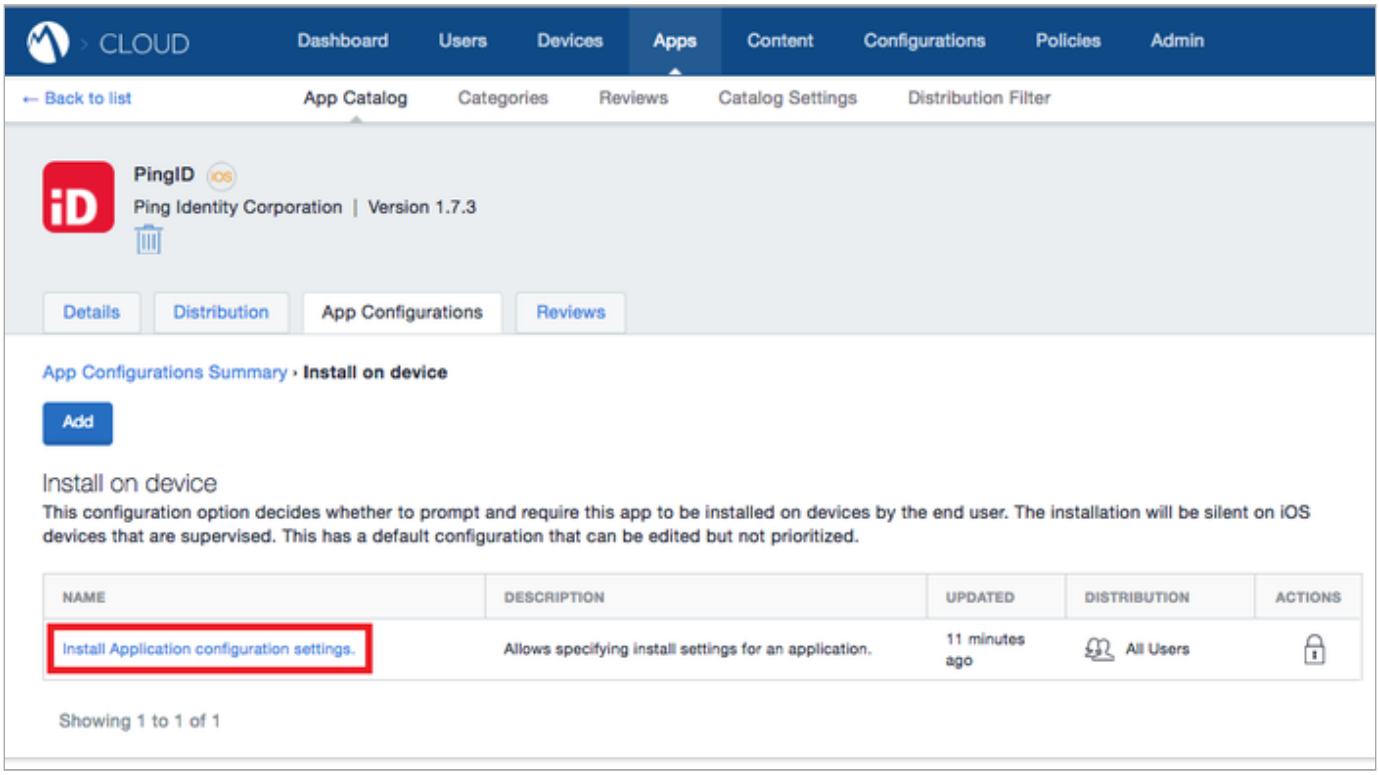
6. Enter the **Configuration Setup** parameter values.

Parameter	Value
Name	`PINGID_MDM_TOKEN`
Token value	The token string value for MDM, as generated inPingOne.



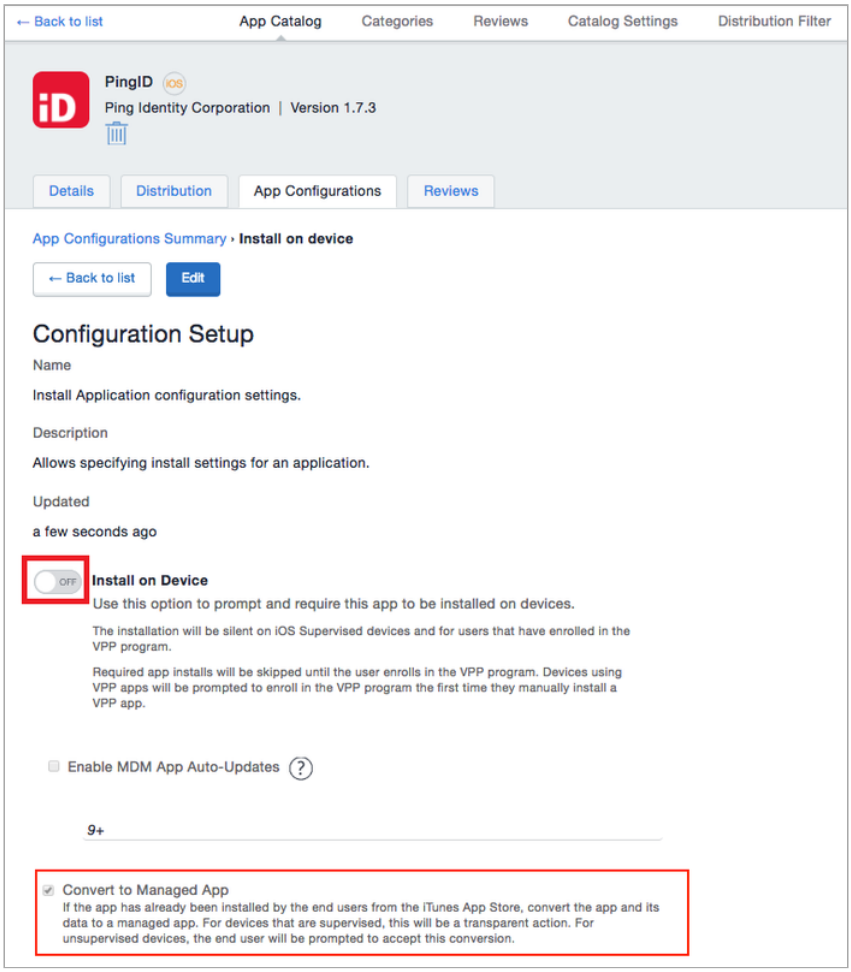
7. Click **Save**.
8. Click **Application Configurations Summary**.
9. Click **Install on device**.
10. Click **Install Application configuration settings**.

Copyright © 2025 Ping Identity Corporation



11. For iOS 9 and later, set the **Install on device** switch to **ON**.

12. Select the **Convert to Managed App** checkbox.



> **Note**
>
> This option transitions a non-managed app downloaded from the app store to a managed app. The user must approve it on their device.

> **Important**
>
> ***For Apple devices earlier than iOS 9 and Android devices***
>
> Users must execute the following steps:
>
> 1. Unpair the PingID mobile app on the iOS device.
> 2. Uninstall the PingID mobile app from the iOS device.
> 3. Reinstall the PingID mobile app from the MDM's app catalog.
> 4. Pair the newly installed, MDM managed PingID mobile app.
>
> ***For Apple devices with iOS 9 and later***
>
> The user receives a notification on their device to approve the transition to MDM management. After user approval, the PingID mobile app installed on the iOS device is managed by the MDM.

13. Click **Save/Update**.
    - When creating a new managed app entry, the button is marked **Save**.
    - When editing an existing entry, the button is marked **Update**.

Copyright © 2025 Ping Identity Corporation

> **Important**
>
> Repeat the entire configuration process for Android. The admin accesses the **Android for Work** options instead of **iOS Managed App Configuration**. The prerequisite to the Android app configuration is Configuring Android for Work for MobileIron.

Updating a PingID token in MobileIron

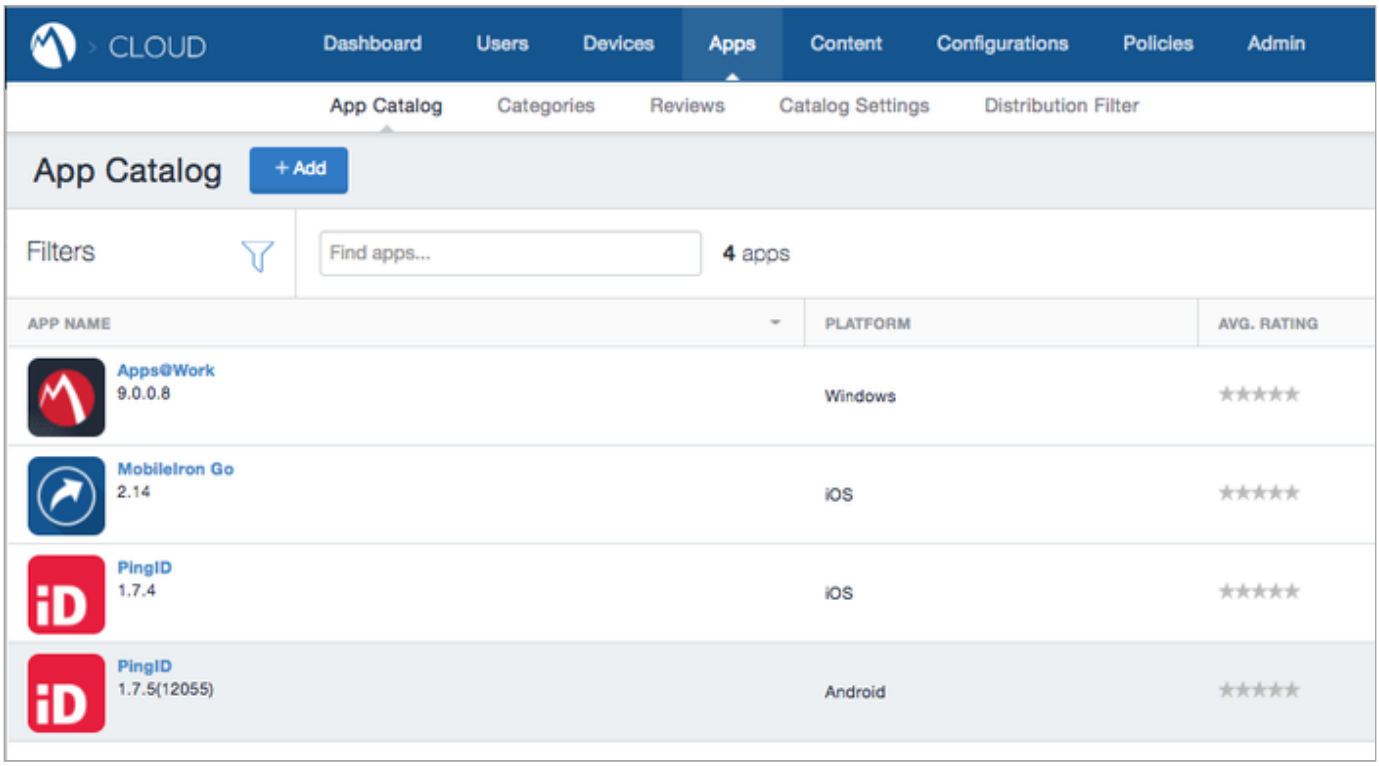
Update a PingID token in MobileIron

About this task

> **Important**
>
> The procedure detailed here is the iOS example for updating the token PingID managed app in MobileIron. The procedure for Android is identical. If the organization's mobile device management (MDM) manages both iOS and Android devices, configure and save the entire procedure separately for each platform.

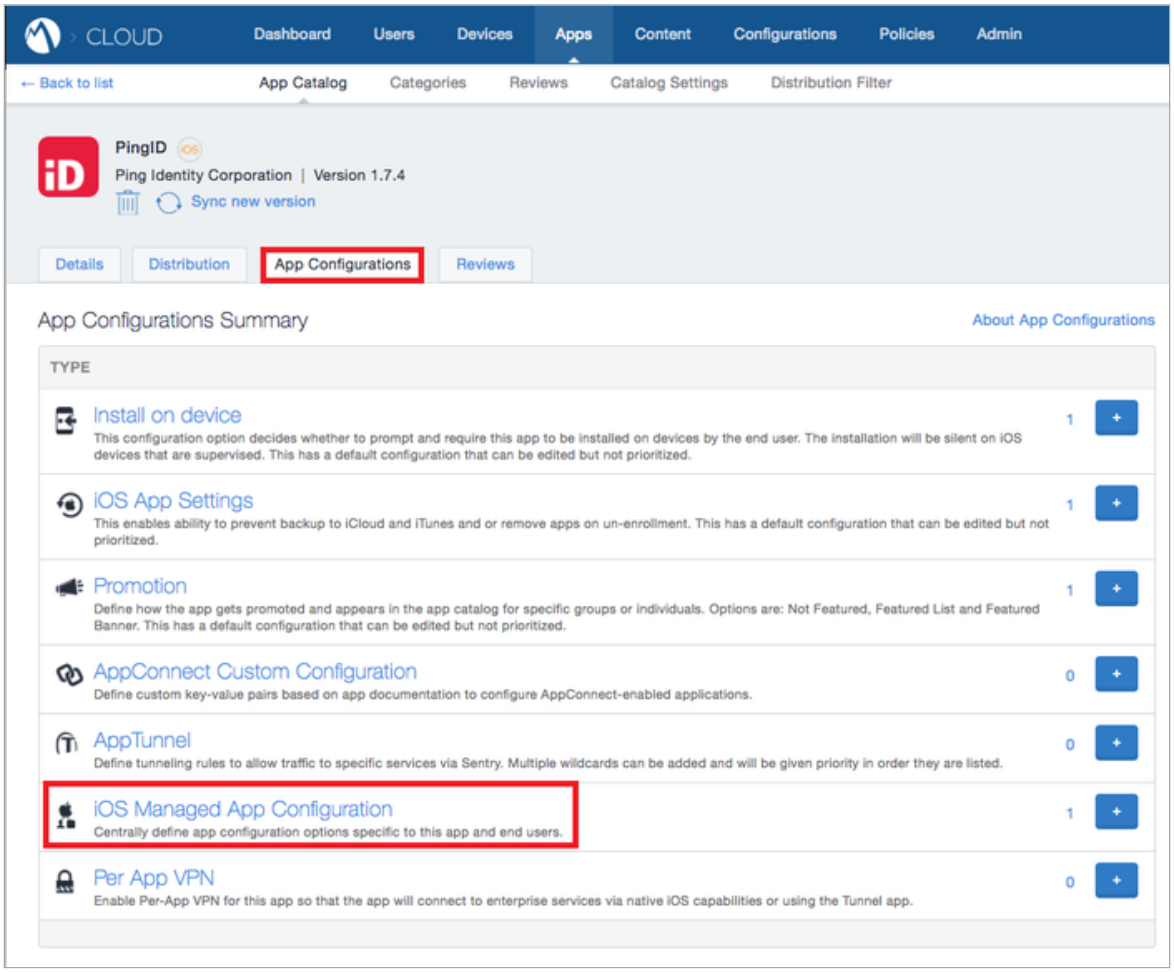
Steps

1. In the MobileIron admin console, go to **Apps → App Catalog**.
2. Select the PingID mobile app for iOS.



3. On the **App Configurations** tab, select **iOS Managed App Configuration**.

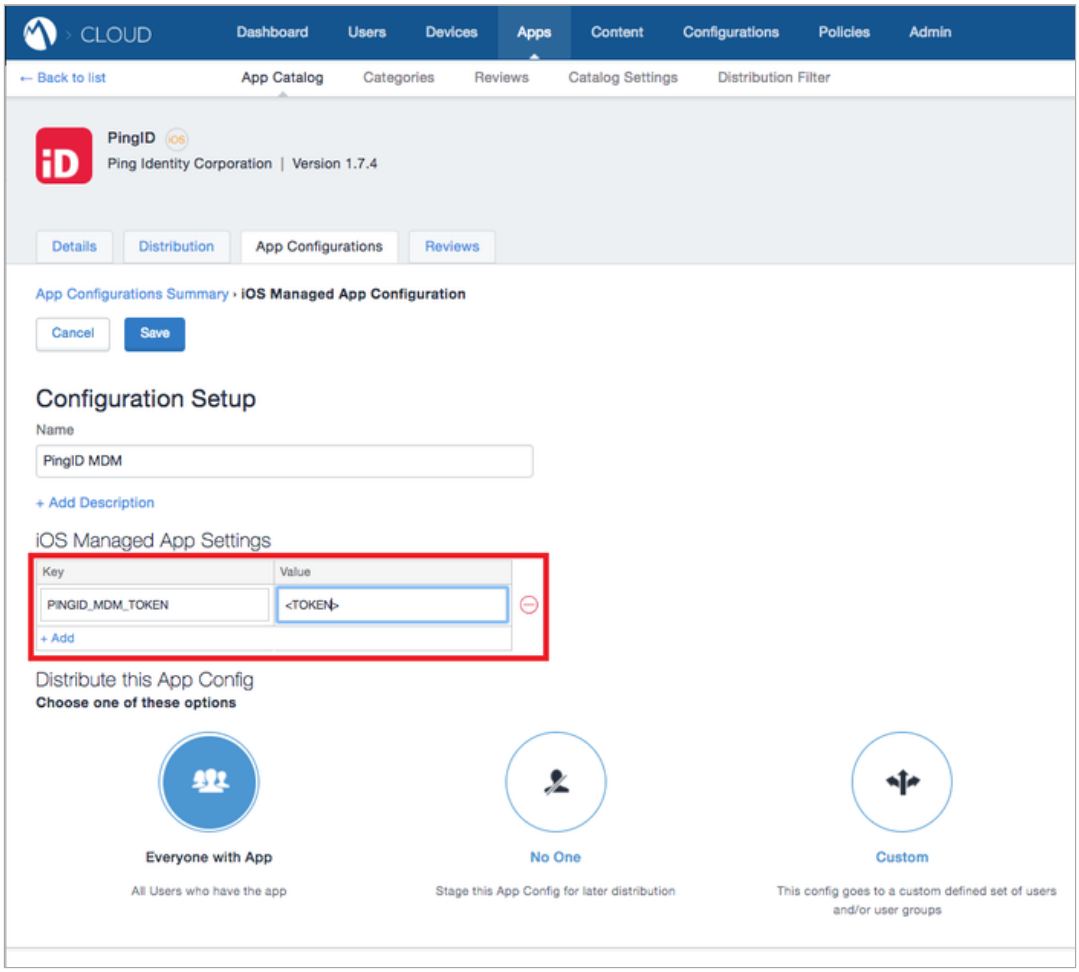
Copyright © 2025 Ping Identity Corporation



4. Update the **Configuration Setup** parameter values.

Parameter	Value
Name	`PINGID_MDM_TOKEN`.
Token value	The token string value for MDM, as generated in PingOne.

Copyright © 2025 Ping Identity Corporation



5. Click **Save**.

> **Important**
>
> Repeat the entire process for Android.

Configuring Microsoft Intune for PingID

To manage the PingID mobile app using Microsoft Intune, you must apply several configuration settings.

> **Note**
>
> The following steps are for use cases where PingID mobile authenticating devices are managed by Microsoft Intune mobile device management (MDM). In cases where PingFederate is used to apply policies on accessing devices managed by Microsoft Intune, refer to the Intune Integration Kit.

1. In Microsoft Intune, install an Apple Push Notification service (APNs) certificate for iOS. Learn more in Installing an APNs certificate for iOS in Microsoft Intune.

Copyright © 2025 Ping Identity Corporation

2. If your organization has iOS devices, add the PingID mobile app for iOS. Learn more in Adding the PingID mobile app for iOS in Microsoft Intune.
3. If your organization has Android devices, add the PingID mobile app for Android. Learn more in Adding the PingID mobile app for Android in Microsoft Intune.
4. Configure PingID mobile app configuration policies for Microsoft Intune. Learn more in Setting the PingID mobile app configuration policies for Microsoft Intune.

MDM maintenance:

As part of MDM maintenance activities for the PingID mobile app, you can generate new tokens and revoke old tokens. Learn more in the following:

- In PingID: In PingOne: Generate, rotate, or revoke an MDM token. Learn more in Managing MDM tokens.
- In Microsoft Intune: Learn more in Updating a PingID token in Microsoft Intune.

Installing an APNs certificate for iOS in Microsoft Intune

To ensure that PingID mobile app configurations can be pushed to iOS devices, install an Apple Push Notification service (APNs) certificate in Microsoft Intune.

Before you begin

Make sure you have your Apple ID.

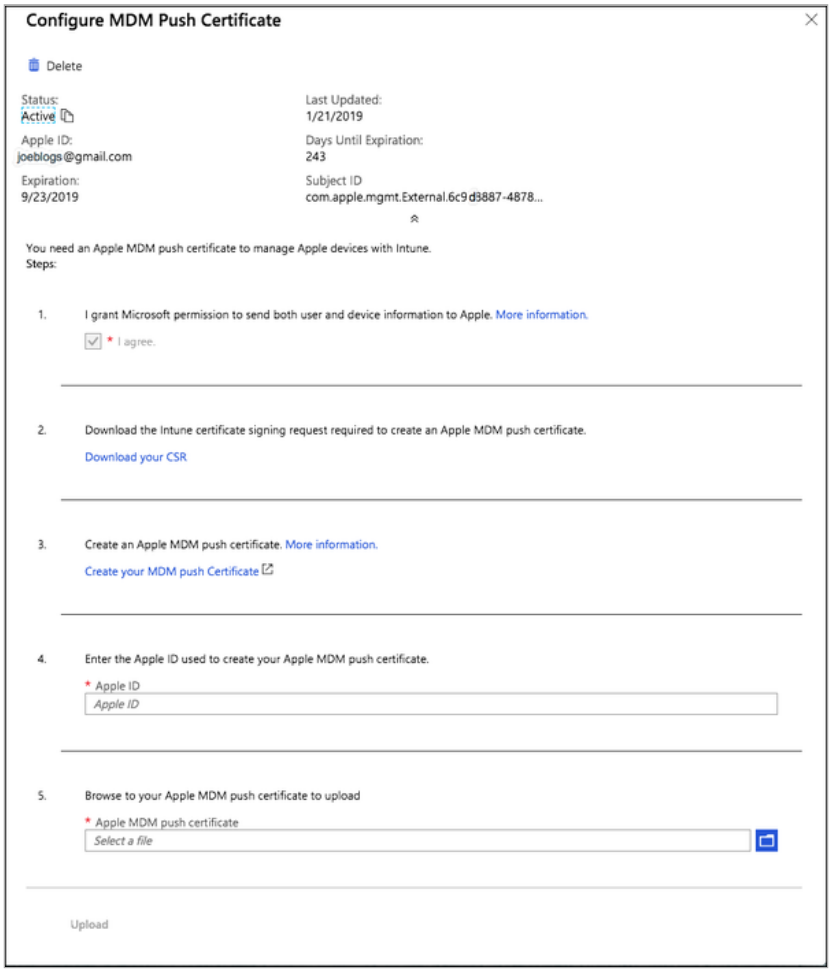
Steps

1. As a Global Administrator in the Microsoft Azure portal, go to **Intune > Device Enrollment > Apple Enrollment**, and then click **Apple MDM Push Certificate**.

   Result:

   The **Configure MDM Push Certificate** window is displayed.

Copyright © 2025 Ping Identity Corporation



2. In the **Configure MDM Push Certificate** window, complete the following fields.

    1. In section **1**, select the **I Agree** checkbox.

    2. In section **2**, click **Download Your CSR**.

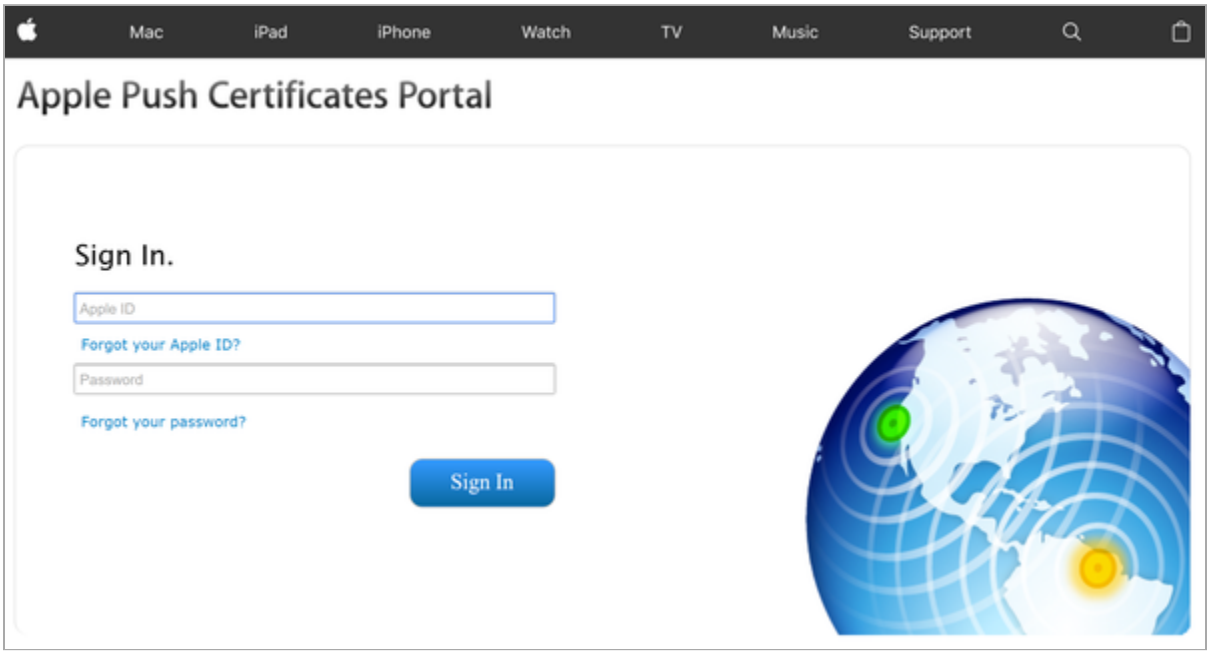
    3. In section **3**, click **Create Your MDM Push Certificate**.

    Result:

    The **Apple Push Certificates Portal** window opens in your browser.

3. Sign on to the Apple Push Certificates Portal.

Copyright © 2025 Ping Identity Corporation



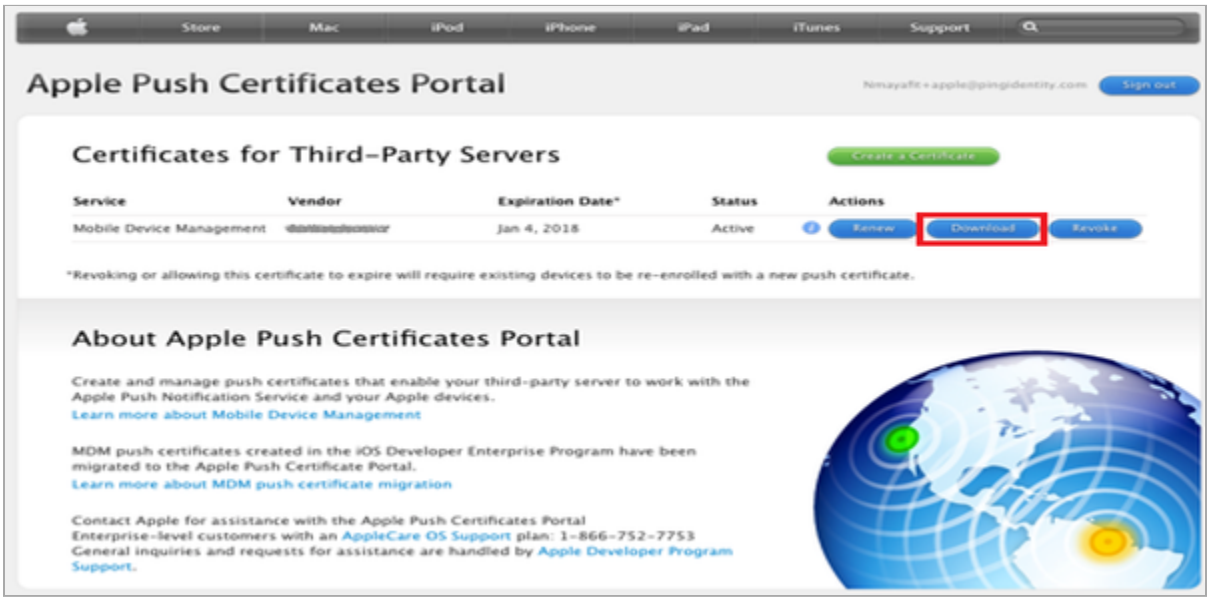
4. In either the **Get Started** section or the **Certificates for Third-Party Servers** section, click **Create a Certificate**.

> **Note**
>
> If your organization does not yet have any Apple Push certificates, the **Get Started** section is displayed. Otherwise, the **Certificates** list is displayed.

5. Click **Choose File** and browse for the certificate signing request (CSR) file you created previously, and then click **Upload**.

Copyright © 2025 Ping Identity Corporation

6. In the row of the new APNs certificate, click **Download**.



7. Return to the **Configure MDM Push Certificate** window and complete the following fields.

    1. In section **4**, enter your Apple ID.

    2. In section **5**, from the **Apple MDM Push Certificate** list, select your APNs certificate.

3. Click **Upload**, and then save your configuration.

Next steps

Add the PingID mobile app for iOS. Learn more in Adding the PingID mobile app for iOS in Microsoft Intune.

Configuring Android for Work for Microsoft Intune

To ensure that PingID mobile app configurations can be pushed to iOS devices, install an Apple Push Notification service (APNs) certificate in Microsoft Intune.

Before you begin

In the Intune dashboard, configure Android work profile devices. Learn more in Enroll device and create Android work profile in the Microsoft Intune documentation.

About this task

This is an example configuration of Android for Work without G Suite. You can also configure Android for Work for MDM with G Suite.

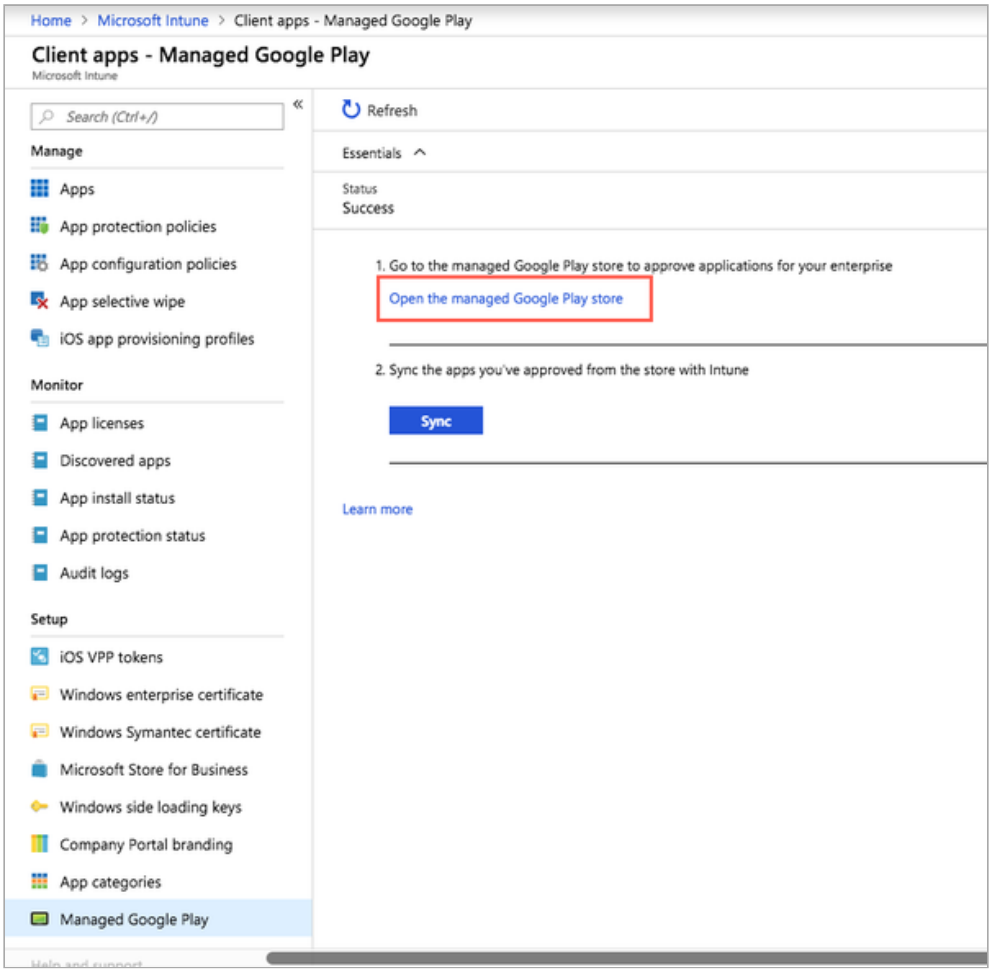
Steps

1. Go to the Microsoft Azure portal and sign on.
2. Go to **Intune** > **Home** > **Client Apps** > **Managed Google Play**.

   Result:

   The **Managed Google Play** window opens.
3. Click **Open the Managed Google Play Store**.

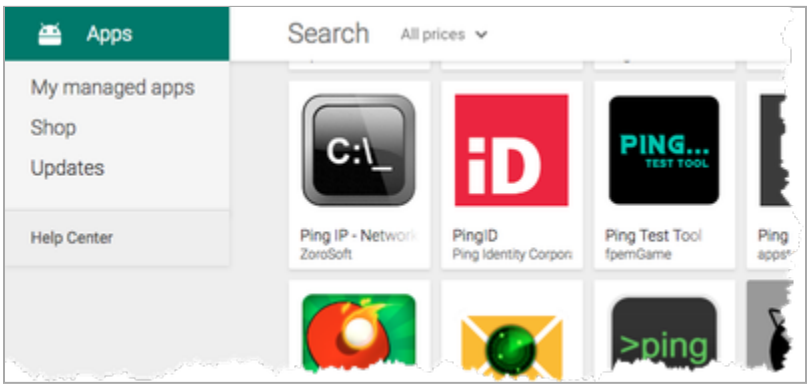
Copyright © 2025 Ping Identity Corporation



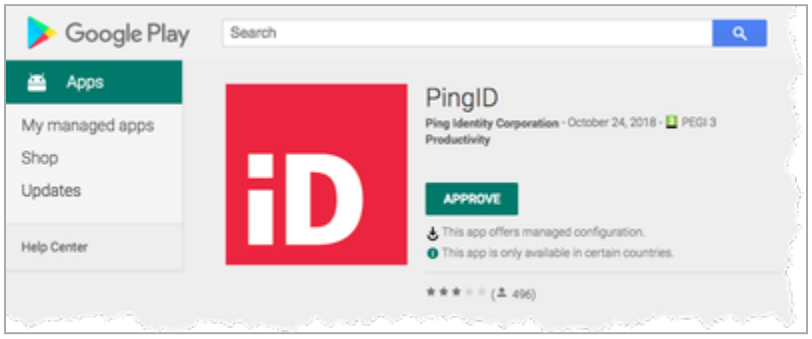
Result:

Google Play opens in a new browser tab or window.

4. Search for the PingID mobile app and select it.



5. Click **Approve**.

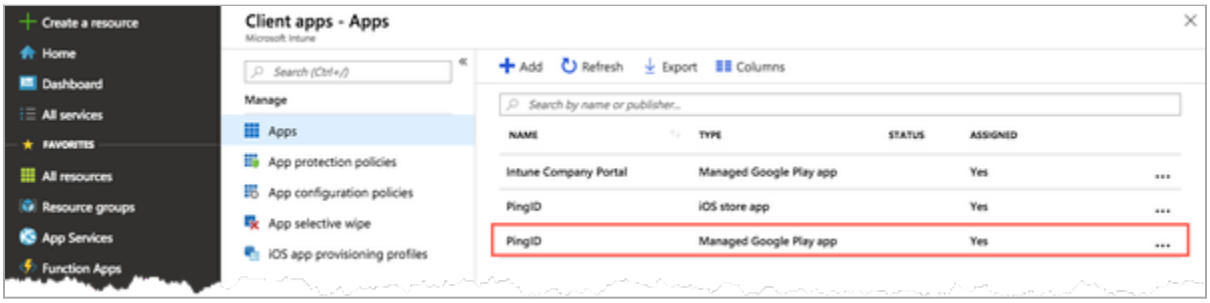


> **Note**
>
> You might need to sign on as a managed Google Play administrator.

Result:

The **Client Apps - Apps** window opens.

6. From the **Apps** list, click the PingID Google Play entry, and then from the left-hand menu, click **Assignments**.



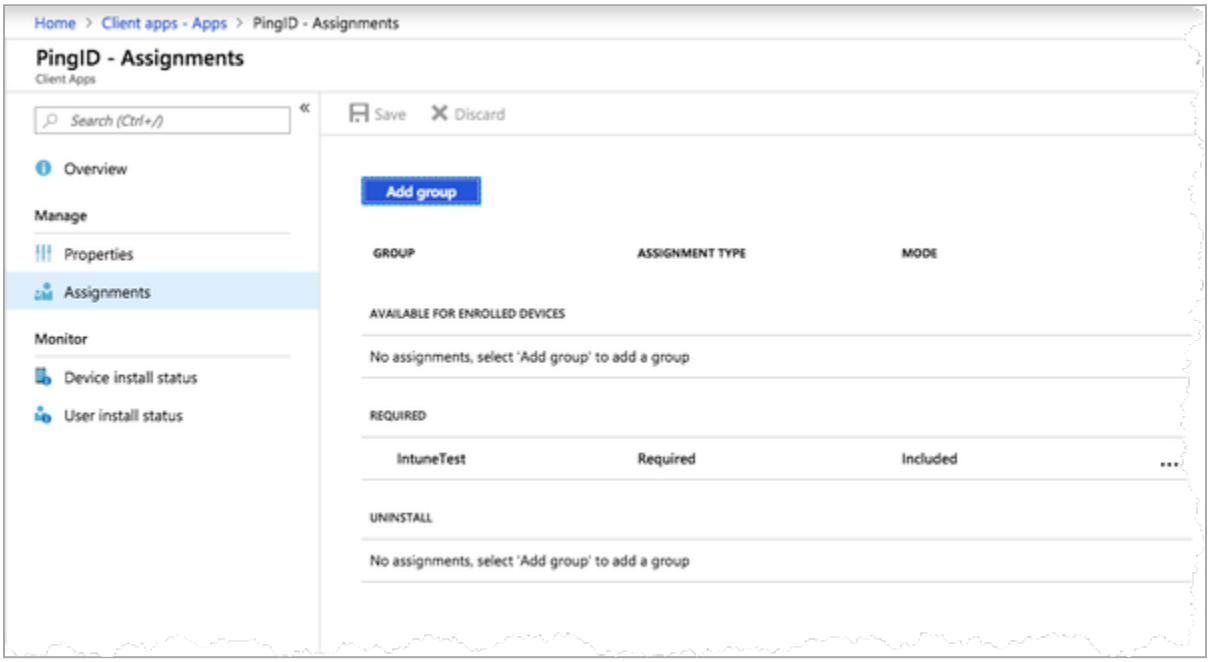
Result:

The **PingID - Assignments** window opens.

7. In the **PingID - Assignments** window, assign the PingID mobile app for Android to user groups.

   Learn more about creating, managing, and assigning apps to groups in the relevant Intune documentation.

Copyright © 2025 Ping Identity Corporation



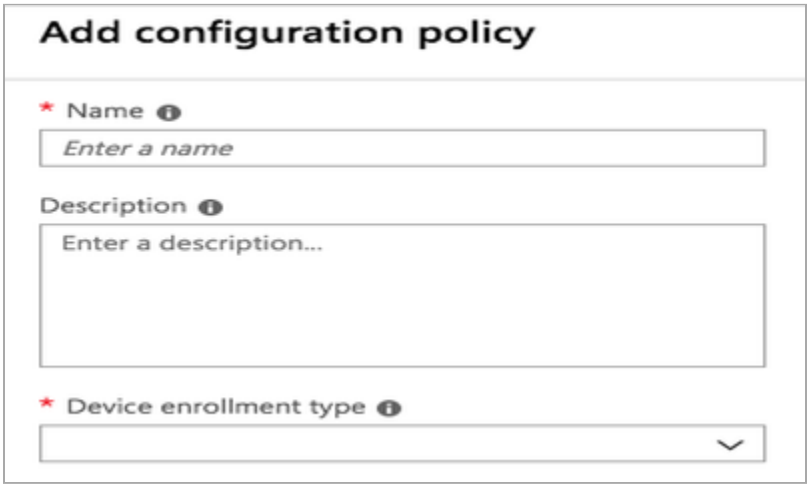
8. Go to **Intune > Client Apps > App Configuration Policies**, and then click **Add**.

   Result:

   The **Add Configuration Policy** window opens.

9. In the **Name** field, enter a name for the policy.

10. In the **Description** field, add a description.



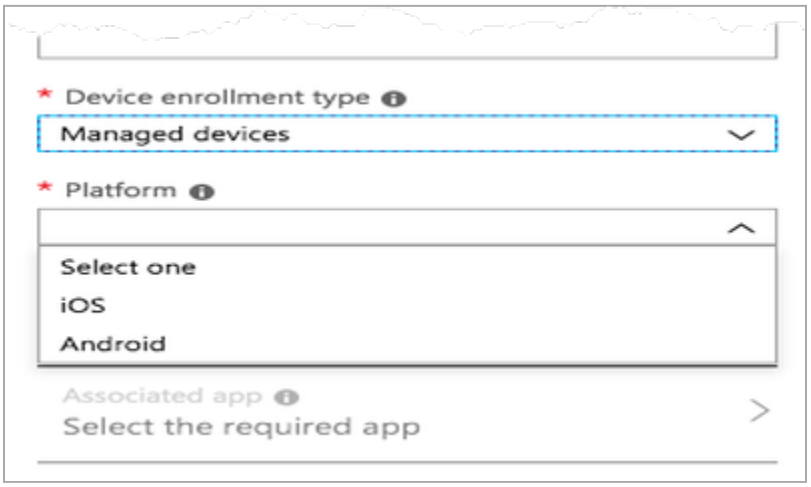
11. In the **Device Enrollment Type** list, select **Managed Devices**.

Copyright © 2025 Ping Identity Corporation

Result:

The **Platform** list is displayed.

12. From the **Platform** list, choose **Android**.



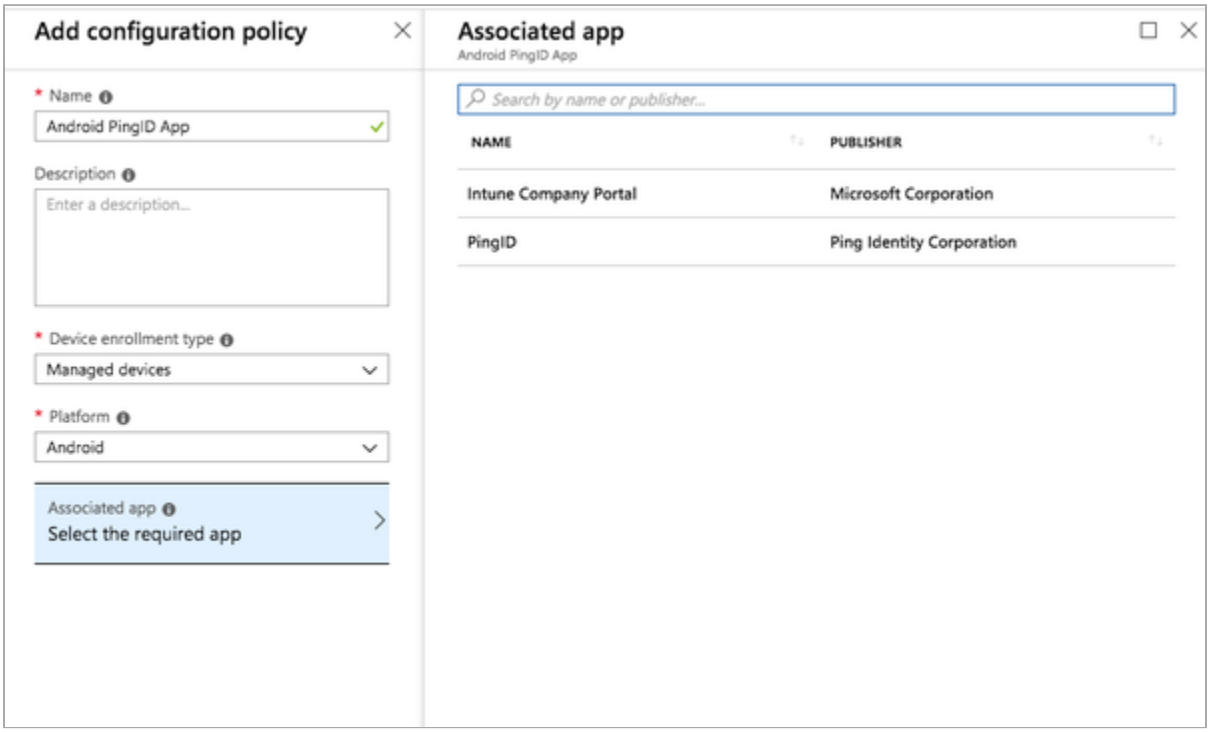
13. At the bottom of the window, click **Add**.

Result:

The **Associated App** tab is displayed.

14. On the **Associated App** tab, click **PingID**.

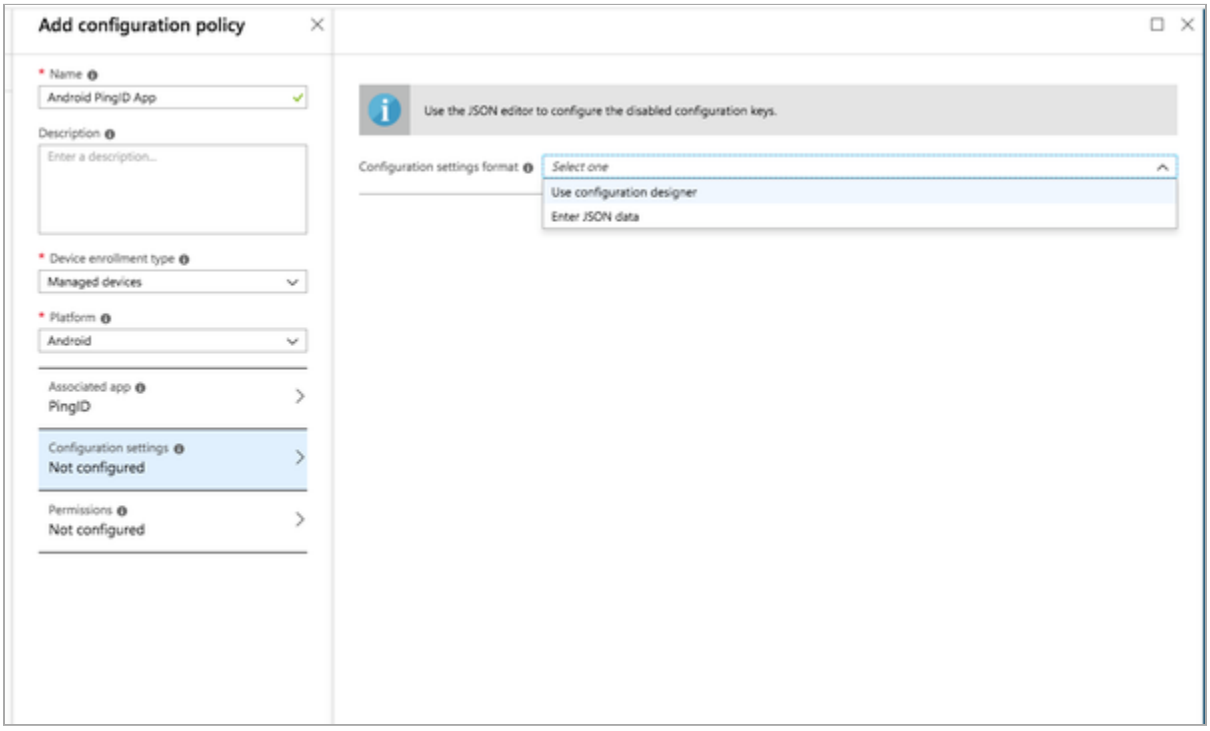
Copyright © 2025 Ping Identity Corporation



Result:

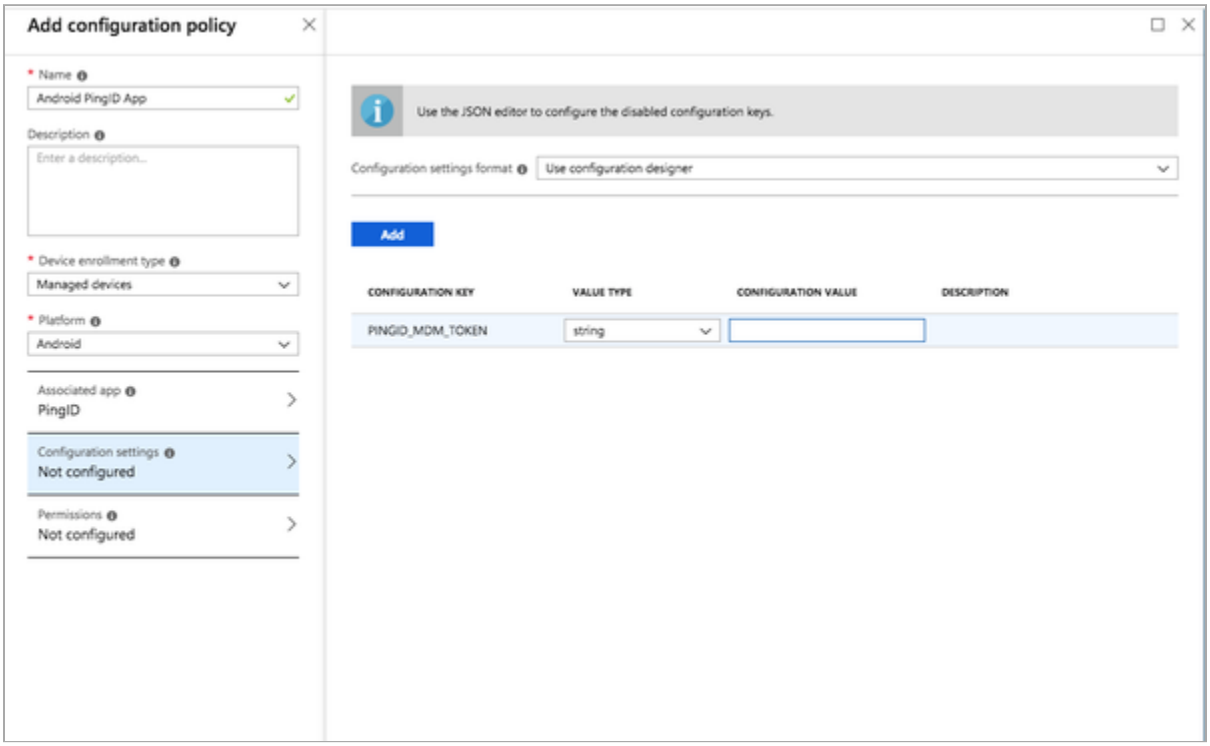
The **Configuration Settings** tab is displayed.

15. In the **Configuration Settings Format** list, select **Use Configuration Designer**.



16. In the **Configuration Value** field, enter the PingID MDM token, and then click **Add**.

    Learn more in (Workforce Only) Configuring the PingID mobile application settings.



Next steps

Learn more in Adding the PingID mobile app for Android in Microsoft Intune.

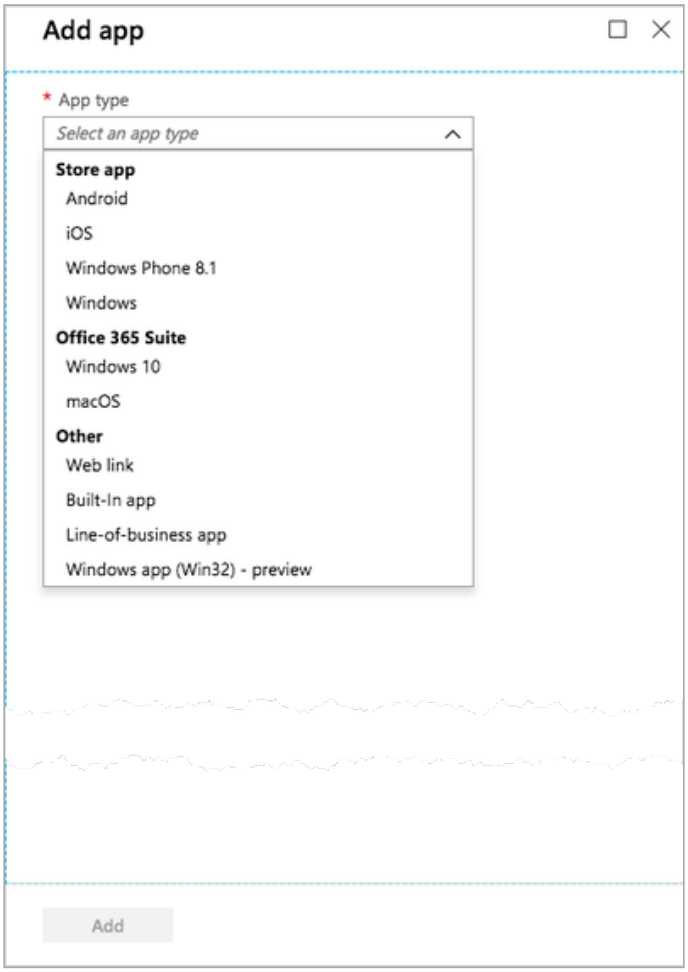
Adding the PingID mobile app for iOS in Microsoft Intune

Configure PingID mobile app as an MDM-managed app for iOS devices in Microsoft Intune.

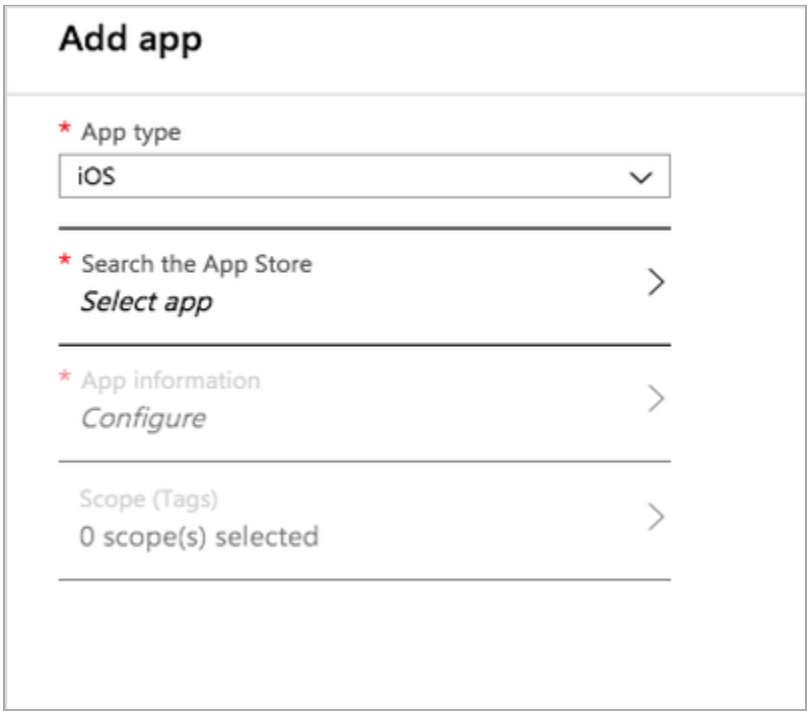
Steps

1. Go to the Microsoft Azure portal and sign on.
2. Go to **Intune → Client Apps > Apps > +Add > Add App**.
3. In the **App Type** list, select **iOS**.

Copyright © 2025 Ping Identity Corporation

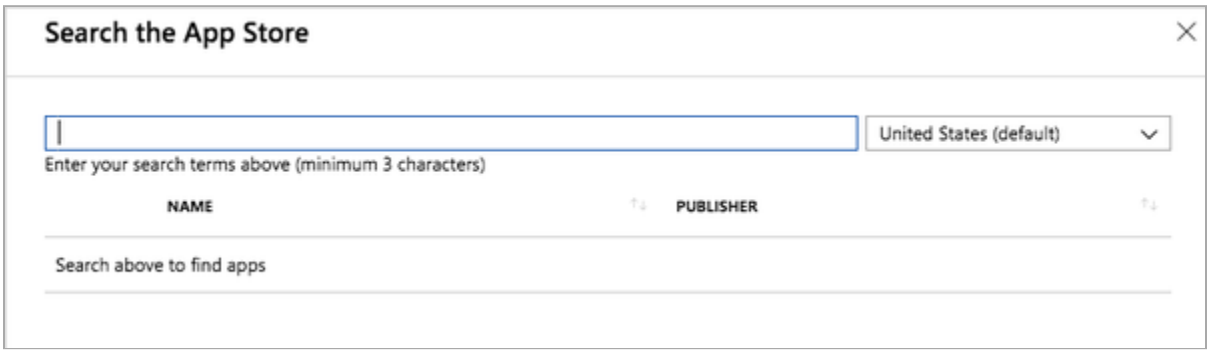


4. In the **Search the App Store** section, click **Select App**.



Result:

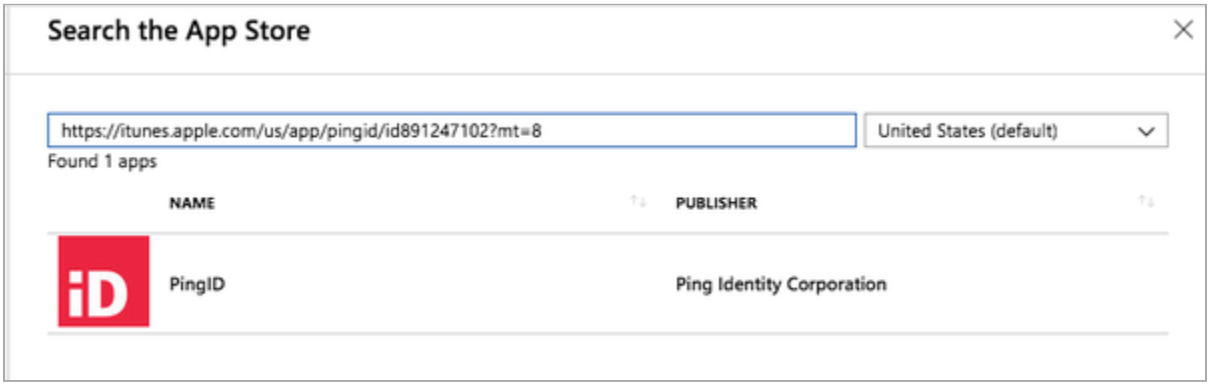
The **Search the App Store** window opens.



5. In the search field, enter the App Store URL for PingID mobile app: https://itunes.apple.com/us/app/pingid/id891247102?mt=8[].

   Result:

   The PingID mobile app app is displayed.



6. Click the PingID mobile app.

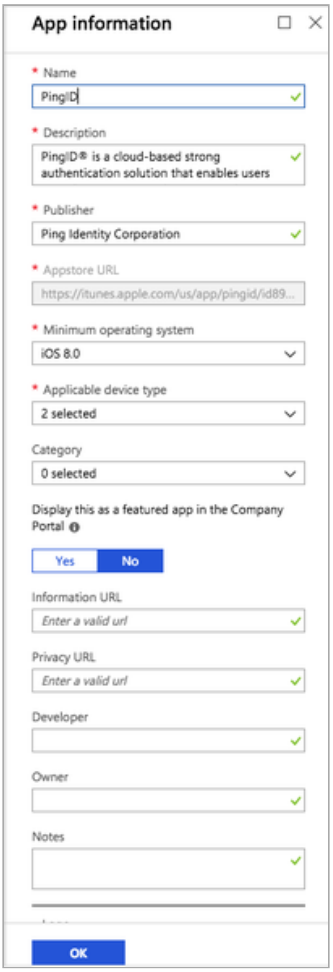
   Result:

   The **Add App** window opens with the **Configure** option enabled.

7. To open the **App Information** window, click **Configure**.

8. In the **App Information** window, make any required changes, and then click **OK**.

Copyright © 2025 Ping Identity Corporation



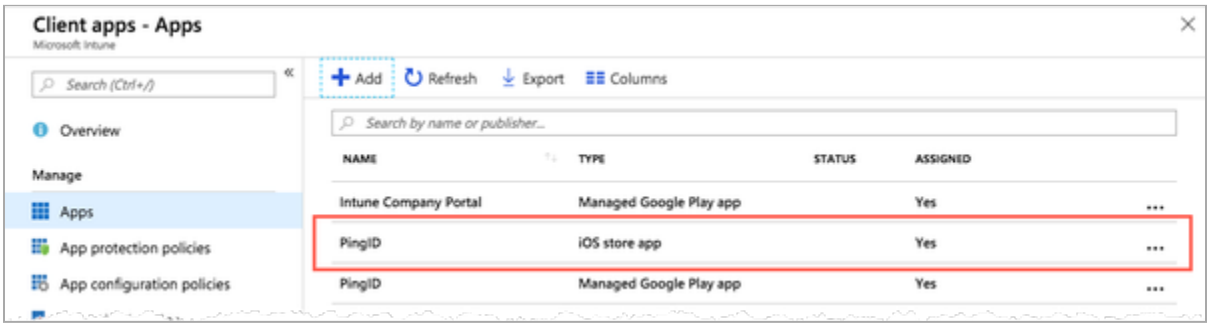
Result:

In the **Add App** window, the **Add** button is enabled.

9. In the **Add App** window, click **Add**.

Result:

Your app appears in the list of client apps.



Next steps

See Setting the PingID mobile app configuration policies for Microsoft Intune.

Adding the PingID mobile app for Android in Microsoft Intune

Configure PingID mobile app as an MDM-managed app for Android devices in Microsoft Intune to ensure that PingID mobile app configurations can be pushed to Android devices.

Before you begin

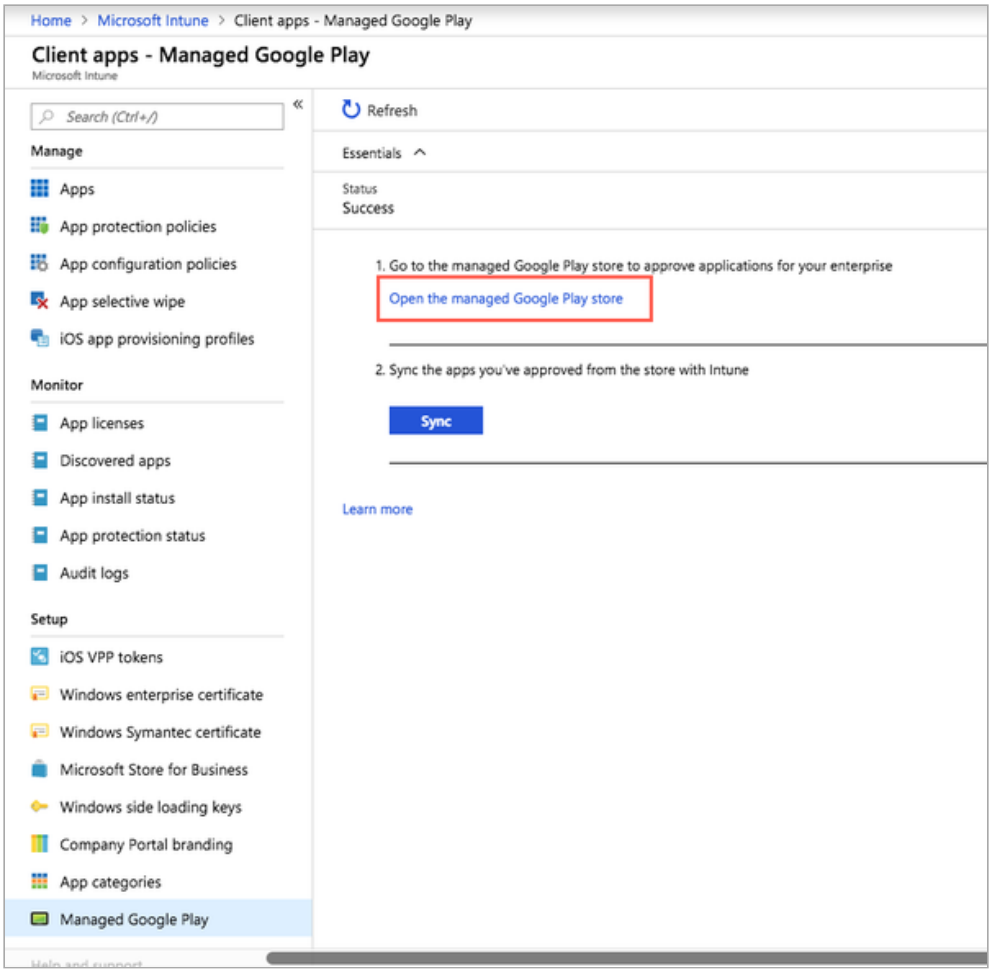
In the Intune dashboard, configure Android work profile devices. Learn more in https://docs.microsoft.com/en-us/intune/android-enterprise-overview.

About this task

This is an example configuration of Android for Work without G Suite. You can configure Android for Work for MDM with G Suite.

Steps

1. Go to the Microsoft Azure portal and sign on.
2. Go to **Intune > Home > Client Apps > Managed Google Play**.
3. In the **Client Apps - Managed Google Play** window, click **Open the Managed Google Play Store**.

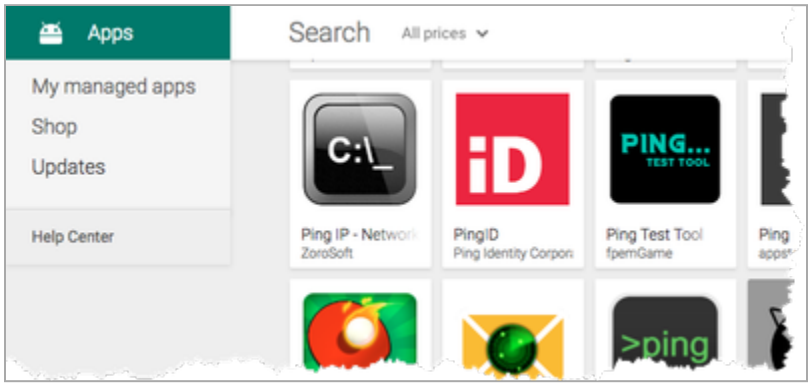


Result:

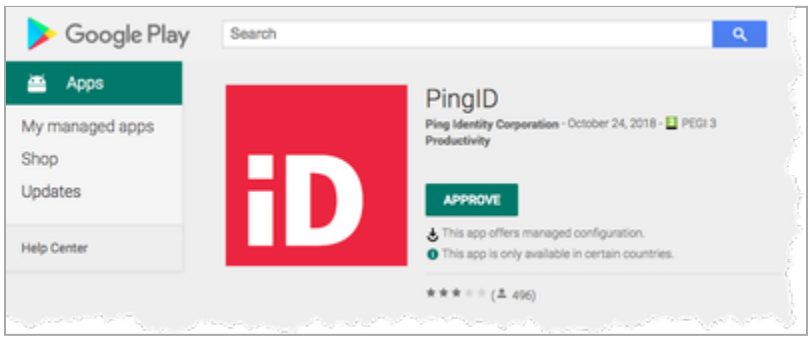
Google Play opens in a new browser tab or window.

4. Search for the PingID mobile app and select it.

Copyright © 2025 Ping Identity Corporation



5. Click **Approve**.

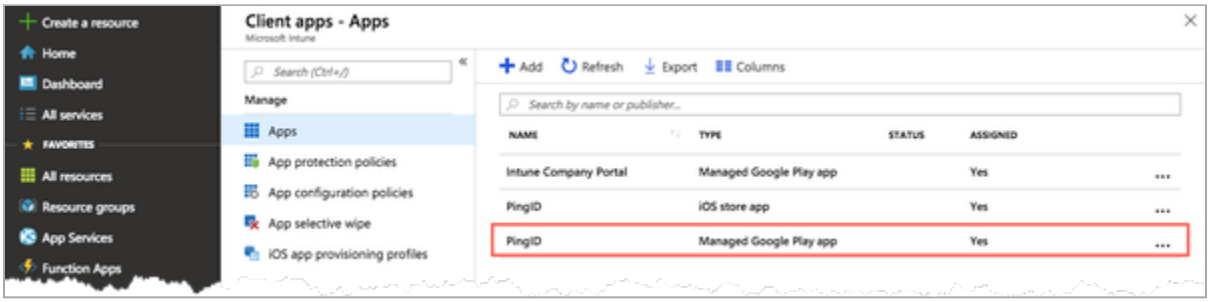


> **Note**
>
> You might be asked to sign on as a managed Google Play administrator.

Result:

The **Client Apps - Apps** window is displayed.

6. From the **Apps** list, select the PingID Managed Google Play app, and then from the left-hand menu, click **Assignments**.



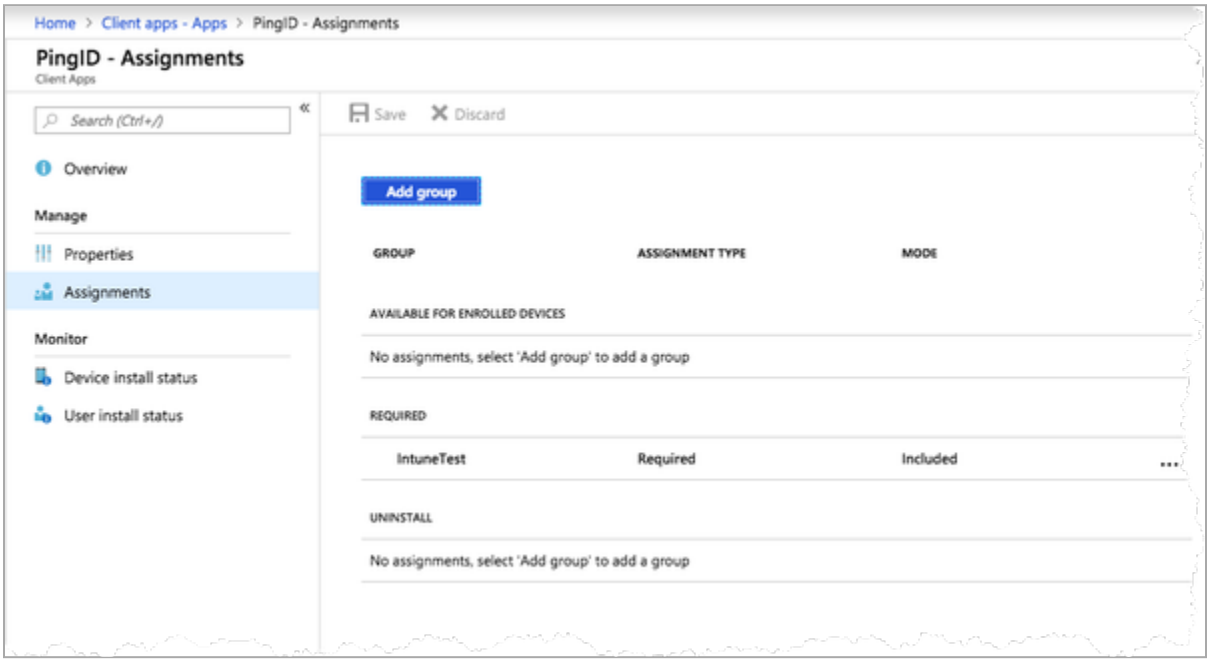
Result:

The **PingID - Assignments** window is displayed.

7. In the **PingID - Assignments** window, assign the PingID Android app to user groups.

   To create, manage and assign apps to groups, consult the relevant Intune documentation.

Copyright © 2025 Ping Identity Corporation



Next steps

Learn more in Setting the PingID mobile app configuration policies for Microsoft Intune.

Setting the PingID mobile app configuration policies for Microsoft Intune

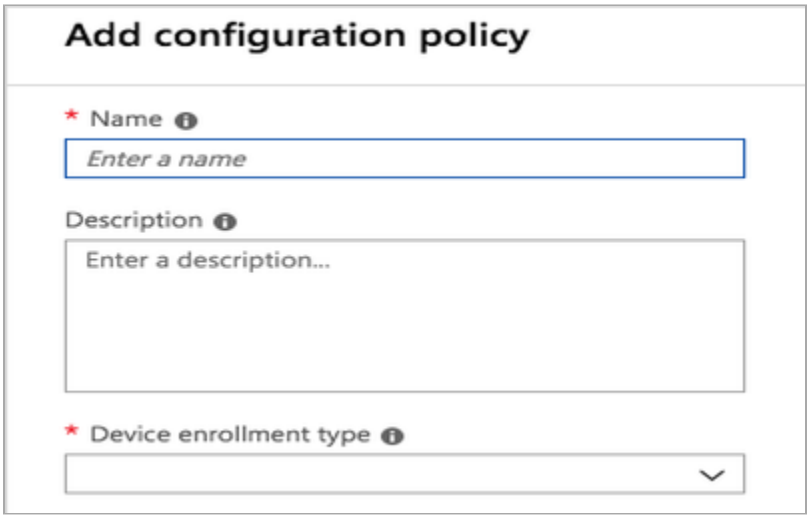
Configure the following procedure separately for iOS and Android.

Steps

1. Sign on to the Microsoft Azure portal.
2. Go to **Intune > Client Apps > App Configuration Policies > +Add**.

   Result:

   The **Add Configuration Policy** window is displayed.

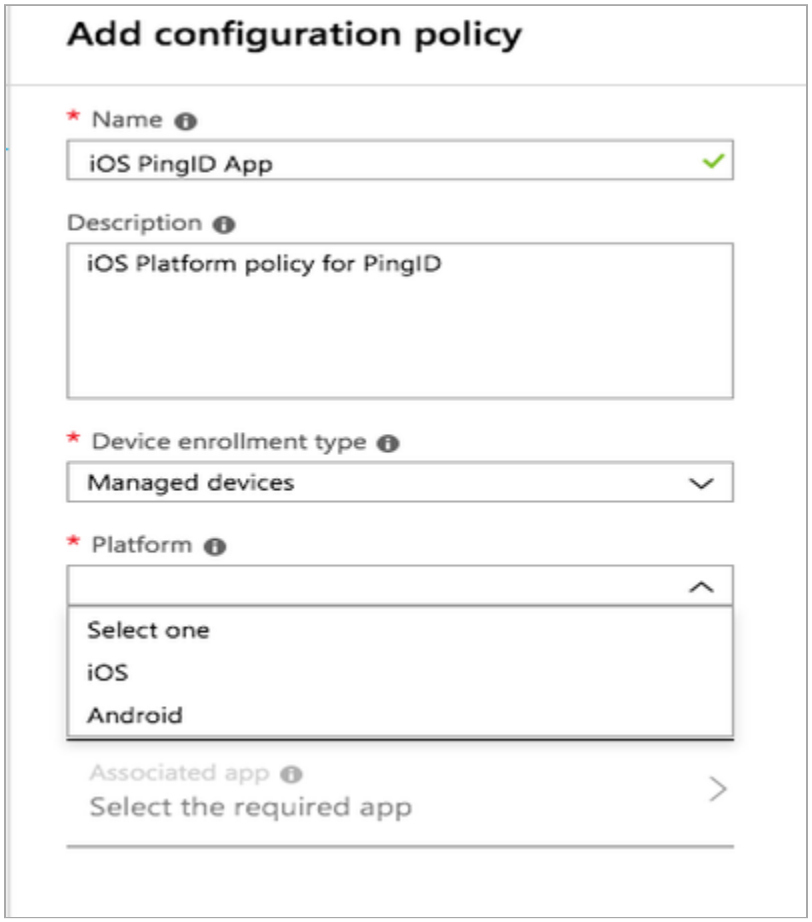


3. In the **Name** field, enter a policy name. In the **Description** field, enter a description.

Copyright © 2025 Ping Identity Corporation

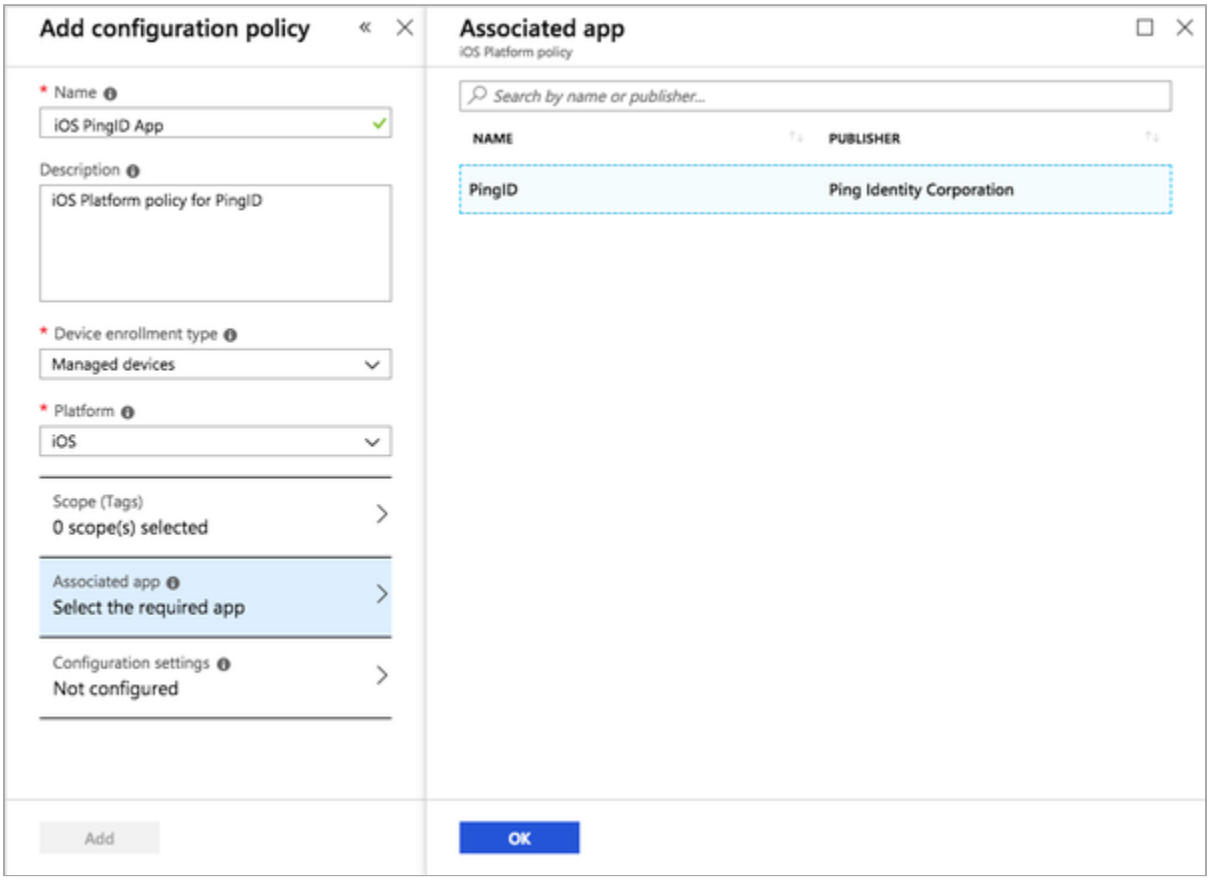
4. From the **Device Enrollment Type** list, select **Managed Devices**.

5. From the **Platform** list, select the relevant platform.



6. Click the **Associated App** section, and then in the **Associated App** pane, select **PingID**.

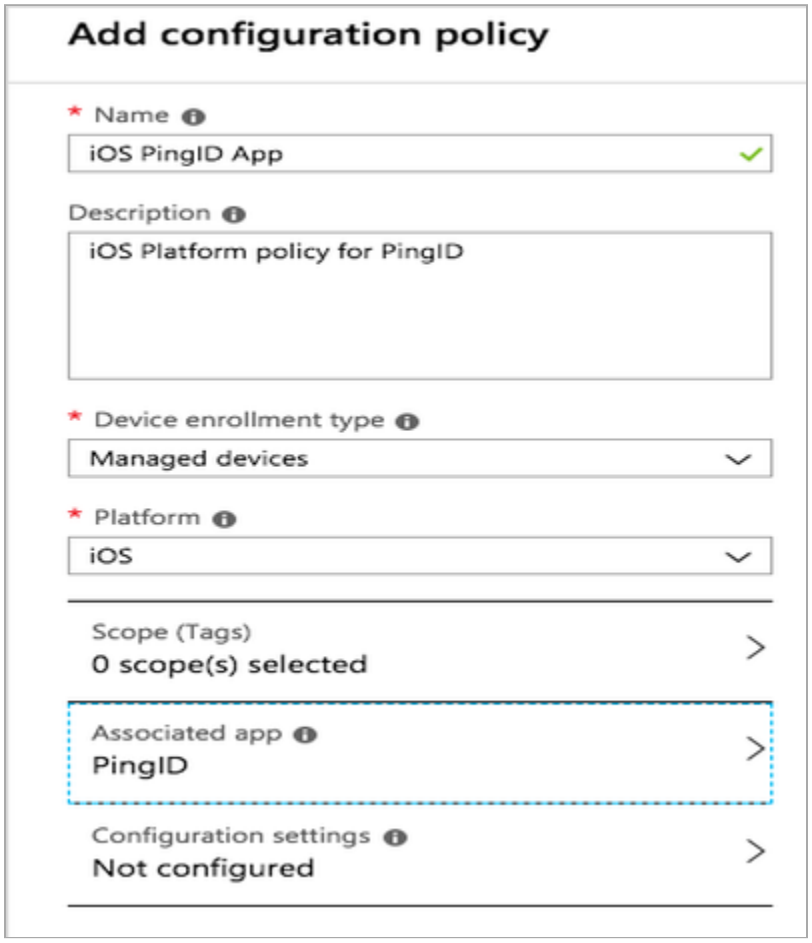
Copyright © 2025 Ping Identity Corporation



Result:

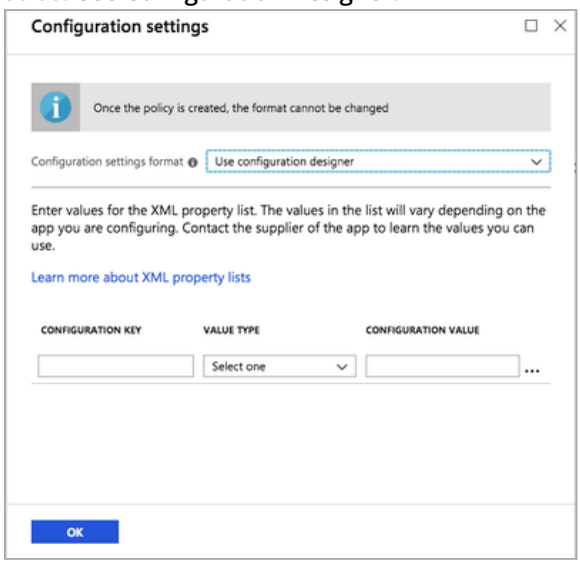
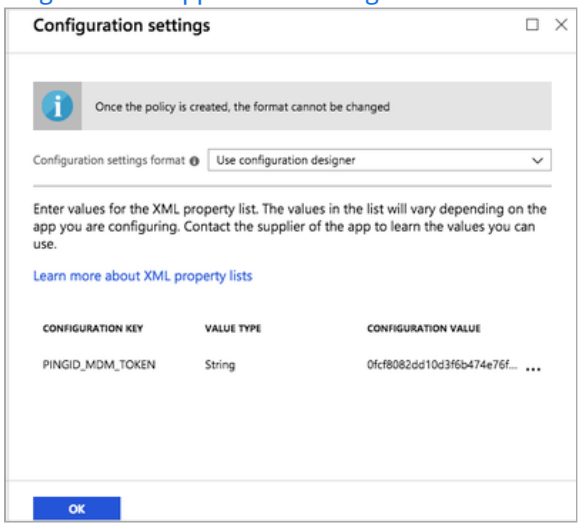
The **Associated App** section shows **PingID**.

Copyright © 2025 Ping Identity Corporation

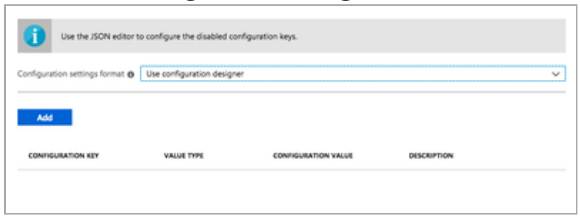
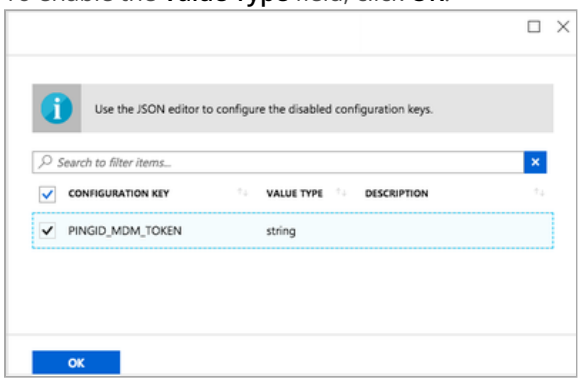
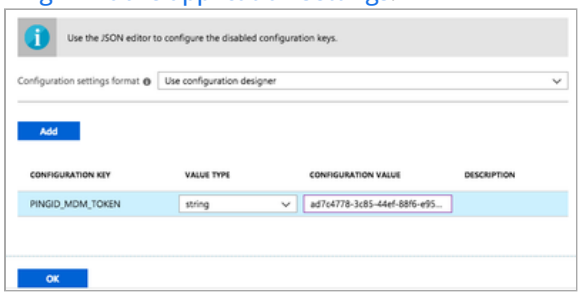


7. Click the **Configuration Settings** section, and then follow the steps according to the relevant operating system.

Copyright © 2025 Ping Identity Corporation

Operating System	Steps
iOS	1. From the **Configuration Settings Format** list, select **Use Configuration Designer**.  2. In the **Configuration Key** field, enter `PING_MDM_TOKEN`. 3. From the **Value Type** list, select **String**. 4. In the **Configuration Value** field, enter the MDM string generated in PingOne. For more information, see (Workforce Only) Configuring the PingID mobile application settings. 

Copyright © 2025 Ping Identity Corporation

Operating System	Steps
Android	1. From the **Configuration Settings Format** list, select **Use Configuration Designer**.  2. Click **Add**. 3. To enable the **Value Type** field, click **OK**.  4. From the **Value Type** list, select **String**. 5. In the **Configuration Value** field, enter the MDM string generated in PingOne. For more information, see (Workforce Only) Configuring the PingID mobile application settings. 

8. Click **OK**.

   Result:

   You are returned to the **Add Configuration Policy** window.

Updating a PingID token in Microsoft Intune

Configure the following procedure separately for iOS and Android.

Before you begin

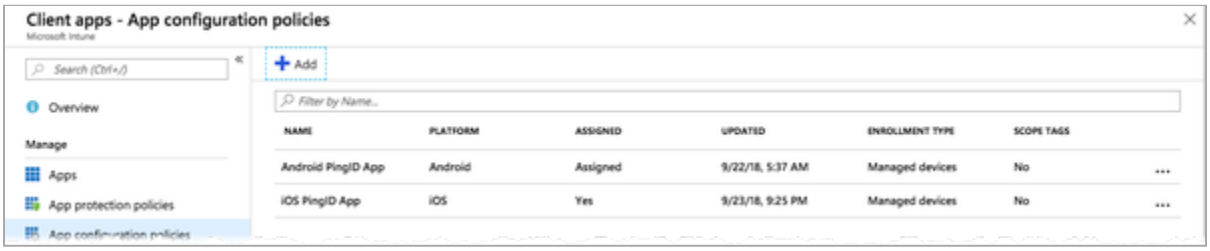
The PingID mobile app is configured for both iOS and Android.

Steps

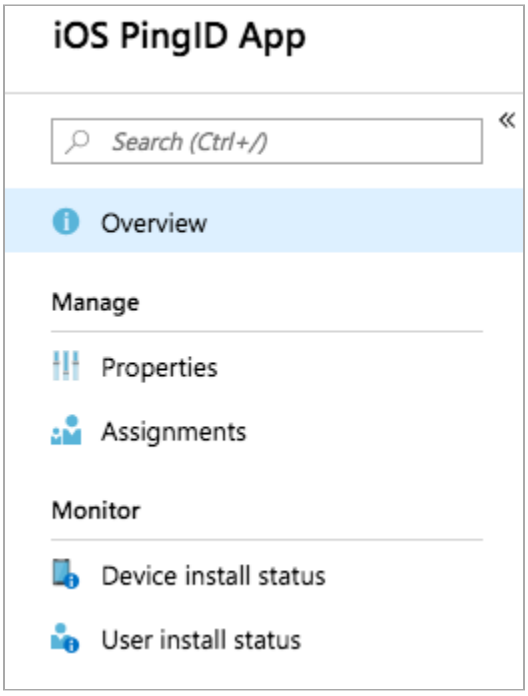
1. Go to the Microsoft Azure portal at https://portal.azure.com.
2. Go to **Intune → Client Apps → App Configuration Policies**.

   Result:

   The **Client Apps - App Configuration Policies** window is displayed.



3. Click the relevant **Android PingID App** or **iOS PingID App** entry.
4. Click **Properties**.



5. Follow the steps according to the relevant operating system.

Operating System	Steps
iOS	1. Click the **Configuration Settings** tab. 2. Enter the MDM string generated in PingOne between `<string>` and `</string>`. For more information, see (Workforce Only) Configuring the PingID mobile application settings.

Copyright © 2025 Ping Identity Corporation

Operating System	Steps
Android	1. Click the **Configuration Settings** tab. 2. From the **Value Type** list, select **String**. In the **Configuration Value** field, enter the MDM string generated in PingOne. For more information, see (Workforce Only) Configuring the PingID mobile application settings.

6. Click **OK**.

   Result:

   The changes are applied and the app dashboard window opens.

7. Click **Save**.

Configuring authenticator app authentication

You can use any third-party authenticator app that can generate a standard time-based one-time passcode (TOTP) for multi-factor authentication (MFA). Examples include Google Authenticator or Microsoft Authenticator.

Before you begin

To add an authenticator app as an authentication method, you need:

- A PingOne environment. The authentication policy should include the relevant MFA policy.

About this task

External authenticator apps are a useful solution in cases such as:

- A workforce organization that cannot allow the PingID mobile app on their devices, as PingID must be added to the allow list.
- An organization that wants to use a single authenticator app and has users that must authenticate to multiple organizations.

Users can use an authenticator app to access an account or application through the web, VPN, Mac login, or SSH. When authenticator app authentication is enabled, users can download the authenticator app of their choice and pair it with their PingOne account. Users can pair more than one authenticator app with their account.

Learn more about the user experience in the PingID End User Guide.

Steps

- Configure the authenticator app authentication method in the MFA policy. Learn more in MFA policy.

Configuring email authentication

You can enable email as an authentication method.

Copyright © 2025 Ping Identity Corporation

When email authentication is configured, and the user signs on to their account or app, they are sent an email with a one-time passcode (OTP) to authenticate with. The OTP is valid for up to 30 minutes.

- Learn how to configure email authentication in PingOne in Configuring an MFA policy for strong authentication.
- Learn how to configure supported languages in Languages.
- Learn how to create custom email templates in Notification templates.
- Learn how to limit the number of email notifications that can be sent per day in Notification Policies.
- Use the Sender page to configure your organization's SMTP email notification server. Learn more: Configuring a custom SMTP email notification server and Configuring trusted email addresses.
- Specify or restrict the user to a predefined email. Learn more:
  - (Workforce only): This is configured in the PingID Admin portal Pre-populating or restricting user registration data.
  - (Customer only): This option is only available for environments that are integrated with PingFederate, and is configured using the PingOne MFA adapter. Learn more: PingOne MFA IdP Adapter settings reference.

Workforce only:

- Learn how to add email as a backup authentication method in Configuring backup authentication methods.
- Learn more about the user experience in the PingID End User Guide.

Configuring FIDO2 authentication (Passkeys)

You can configure FIDO2 devices as an authentication method. FIDO2 devices include passkeys, FIDO2 biometrics, and security keys.

Before you begin

To add FIDO2 as an authentication method, you need:

- A PingOne environment. The authentication policy should include the relevant MFA policy.

> **Note**
>
> FIDO2 biometrics and security keys are legacy authentication methods and must be updated to support FIDO2 authentication. Learn more: Updating an existing MFA policy to use FIDO2, and for legacy PingID accounts, see Updating a PingID account to use PingOne FIDO2 policy for Passkey support.

About this task

Learn more about FIDO2 authentication in FIDO policies.

Adding FIDO2 as an authentication method involves the following steps:

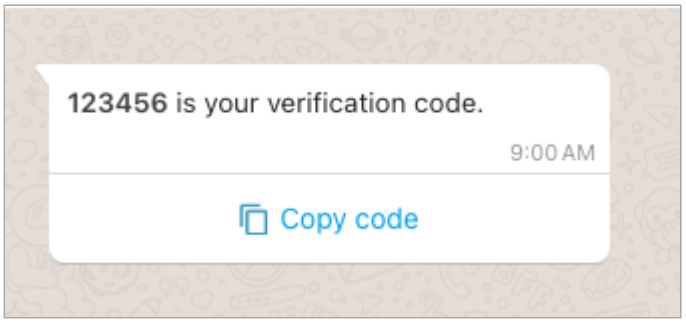
Steps

1. Configuring a FIDO2 policy.
2. Configure the MFA policy to include the FIDO2 authentication method, and include the relevant FIDO2 policy.

Copyright © 2025 Ping Identity Corporation

(Customer Only) Configuring WhatsApp authentication

Enable and configure WhatsApp authentication to allow your users to receive a one-time passcode (OTP) by WhatsApp.



Before you begin

To enable WhatsApp authentication, make sure you have a WhatsApp Business account that includes one or more WhatsApp messaging templates. You can find more details in Configuring a custom WhatsApp sender account.

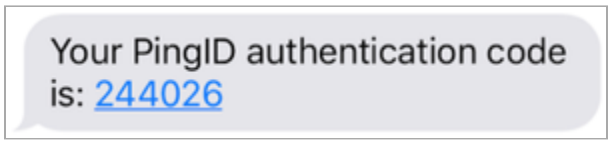
About this task

To configure WhatsApp authentication:

1. Add your WhatsApp Business account as a Sender in PingOne. Learn more in Configuring a custom WhatsApp sender account.
2. For each language you want to support, link a WhatsApp messaging template to the relevant PingOne Notification templates. Learn more in Notification Templates.
3. In the PingOne **MFA policy** enable WhatsApp as an authentication method. Learn more in Configuring an MFA policy for strong authentication.
4. (Optional) Configure a notification policy to limit the number of WhatsApp messages that can be sent per day or to limit their target locations. Learn more in Notification Polices.

Configuring SMS and voice authentication

You can enable SMS or voice authentication. When configured, a one-time passcode (OTP) is sent to the user's mobile device or landline phone, using SMS or telephony voice channels. The OTP is valid for up to 30 minutes.



- Learn how to configure SMS and voice authentication in Configuring an MFA policy for strong authentication.
- (Workforce only) Specify or restrict the user to a predefined phone number. Learn more: Pre-populating or restricting user registration data.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> For PingOne MFA, this is done using the PingOne MFA adapter.

- Create custom SMS or voice authentication templates. Learn more in Notification templates.
- Localize SMS messages and voice authentication calls:
  - Learn how to configure supported languages.
  - Learn how to limit the number of SMS or voice authentication notifications that can be sent per day in Notification Policies.
  - Learn how to use a custom SMS/Voice sender account with PingOne.

> **Note**
>
> To prevent users from registering their device for SMS or voice authentication, and allow existing users to continue to authenticate, you can disable **Allow Pairing** in the relevant MFA policy. This option is useful if you want to phase out SMS and voice authentication, in favor of more secure authentication methods. Learn more in Configuring an MFA policy for strong authentication.

Workforce only:

- Configure SMS or voice authentication as a backup authentication method. Learn more Configuring backup authentication methods.
  - Learn more about the user experience in the PingID End User Guide.

SMS and voice authentication conditions and limitations

The following list describes the conditions and limitations of SMS and voice authentication:

- SMS and voice usage limits are defined in the notification policy. Learn more: Notification Policies.
- Use of phone numbers with extensions must be enabled in MFA settings. Phone numbers with extensions are supported for voice calls. The phone number must be followed by a comma and the extension number. For example:
  - The phone number +12025550123 with the extension 2992 is entered as +12025550123,2992.
  - The extension can include the # or * characters. For example, +12025550123,#2992 or +12025550123,2992#.
  - If there is more than one extension, a comma should separate the extension and the nested extension. For example, +12025550123,#2992,#2991.
  - Each comma generates a 2-second pause. After the call is answered, the extension is dialed after 2 seconds. If a pause is required for longer than 2 seconds, add an additional comma for each additional 2-second pause. For example, in +12025550123,#2992,,,#2991, three commas generate a 6-second pause before the nested extension.
- Virtual numbers are not supported, and delivery success rates for virtual numbers are therefore likely to be lower than fixed numbers.
- Because of Chinese regulatory limitations, use of voice OTPs in China is disabled.

Copyright © 2025 Ping Identity Corporation

- In some cases, SMS OTPs in China may be blocked because of Chinese regulatory limitations. Therefore, it is recommended to use the Twilio Verify service in China. To enable this service, contact your Ping Identity sales representative.
- In India and Saudi Arabia, OTPs are sent by SMS in transactional mode.
- Twilio doesn't support the use of SMS OTPs in Iran. For users in Iran, if the first attempt to request an OTP using SMS fails due to this limitation, sending the request a second time triggers fallback to Vonage, which does support the use of SMS OTPs in Iran.
- Transactional SMS messages include PingID or PingOne MFA as part of the sender ID.
- Customers that are using Ping Identity's SMS default account might receive SMS messages from a pre-registered alphanumeric Sender ID. This is necessary in countries with regulations that require Ping Identity to use a pre-registered Sender ID. You can find a list of requirements by country in Twilio requirements and Vonage requirements.
- In countries that use alphanumeric sender IDs, sender IDs might vary depending on the SMS provider used.

> **Note**
>
> Voice authentication end users should change their voicemail password from their device default, or disable voicemail if using voice OTP authentication. An attacker could potentially direct an OTP voice call to a voicemail by calling the victim at the same time. In the event of an attack, the OTP will be recorded in the voicemail and will be subject to its password protection.

(Workforce Only) Configuring the PingID desktop application

PingID desktop app can be installed on a PC or Mac machine and used to generate a one-time passcode (OTP) with which to authenticate.

> **Note**
>
> Desktop app uses the HMAC-based one-time password (HOTP) algorithm to generate the OTP.

Users must be online to pair the PingID desktop app or change their PIN. However the desktop app can be used to generate an OTP even when the user is offline.

Before you begin

PingID desktop app is available for the following platforms and versions:

- Microsoft Windows 10 and 11
- Microsoft Windows Server 2016 and 2019
- Apple Mac OS X 11+

> **Important**
>
> The PingID desktop app does not run on an Apple Mac OSX virtual machine (VM).

The PingID desktop app requires a minimum of 155 MB RAM and 212 MB free disc space.

Learn more about the user experience in the PingID End User Guide.

Copyright © 2025 Ping Identity Corporation

Note

- Different end users using the same PC have different PingID accounts and undergo a unique authentication process. Each end user only sees their own organizations.
- When a user is registered to two different organizations, each organization's administrators can only see the details of their own organization's end users.
- Roaming user profiles:
  - Roaming user profiles are available from version 1.5.3 for the Windows desktop app.
  - To enable roaming user profiles, users must be unpaired and any previous installation of the desktop app must be uninstalled.
  - All terminals available for roaming users must have the desktop app installed with user roaming profiles support enabled.

Steps

Adding PingID desktop app as an authentication method includes the following steps:

1. Configure the MFA policy to include PingID desktop app. Learn more Configuring an MFA policy for strong authentication.
2. Optionally configure the PingID desktop app application if you want to:
   - Add a PIN to the PingID desktop app. This elevates security by preventing unauthorized users from accessing the PingID desktop app on an unlocked machine. Learn more in Configuring the PingID desktop app PIN.
   - Add a proxy. Learn more in Configure PingID Proxy for the PingID desktop app.

Configuring the PingID desktop app PIN

As an extra layer of security, you can require users to enter a 4 or 6-digit PIN code to access the PingID desktop app.

About this task

If you enable the PingID desktop app security PIN:

- Users are prompted to create a PIN code when they pair the desktop app. The PIN code must include at least 3 or 4 different digits for PIN lengths of 4 and 6 digits, respectively. Digits must not be in ascending or descending sequence, such as 1234 or 4321.
- Users are prompted to enter the PIN code each time they launch the PingID desktop app.
- The PingID desktop app is locked after 3 minutes of inactivity, and the user must enter the PIN to unlock it.
- In the event of three consecutive incorrect PIN entries, the user is blocked from accessing the app for 2 minutes. This applies to both the PIN entry and the PIN change windows. Lockdown takes effect from the time of the lock, no matter if the PingID desktop app remains open or is closed and relaunched.
- The PingID desktop app must be online for a user to pair the app. However, a user who is offline can still create a PIN, enter the PIN to access the desktop app, or change their PIN.
- The desktop app must be online for a change in PIN configuration to take effect, such as enabling or disabling the PIN or changing its length.

Copyright © 2025 Ping Identity Corporation

- If a user pairs the desktop app to more than one organization, the user must create only one PIN, according to the most restrictive organization requirements. For example:
  - If only one organization has enabled the **Desktop Security PIN** feature, the user is required to enter their PIN to use the desktop app for authentication to all organizations, including those which do not require the PIN.
  - If one organization requires a **4-Digit** PIN and a second organization requires a **6-Digit**, the user will be required to enter a 6-digit PIN.
- If the PIN code is already enabled, and the administrator changes the length of the PIN code required, users must first enter the app using the old PIN and then create a new PIN of the new length.

Steps

1. Go to **Applications > Applications**.
2. In the **Applications** list, select **PingID Desktop**.
3. On the **Configuration** tab, click the **Pencil** icon and then select the **Require desktop app security PIN** checkbox.
4. In the **Desktop Security PIN** section, click either **4-Digit** or **6-Digit** to indicate the PIN length.
5. Click **Save**.

   Result:

   If an administrator edits the PingID desktop configuration to require a PIN code, changes are implemented at the user level according to the PingID version and the user flow.

   - Users installing the PingID desktop app for the first time are prompted to create a PIN at the end of the desktop app pairing flow.
   - Users with the PingID desktop app 1.4 or later already paired are prompted to define a PIN code the next time they open the PingID desktop app while online.

Next steps

Add the MFA policy to the MFA step in the relevant Authentication policy. Learn more in Adding a multi-factor authentication or PingID step.

Configure PingID Proxy for the PingID desktop app

Configure the PingID desktop app to support proxy for all enterprise internal communication to the internet on enterprise desktop and laptop machines.

Before you begin

You can get latest version of the `SetProxyParams` script at https://github.com/pingidentity/pingid-desktop-application.

Steps

1. In PingOne, go to **Applications > Applications**.
2. In the **Applications** list, select **PingID Desktop**.
3. On the **Configuration** tab, click the **Pencil** icon.

Copyright © 2025 Ping Identity Corporation

4. To enable the use of PingID desktop app with the enterprise proxy, according to the mode configured in the `SetProxyParams` script, select the **Use proxy for desktop app** checkbox and then click **Save**.

> **Note**
>
> Even if the **Use Proxy For Desktop** setting is enabled enterprise-wide in the admin portal, administrators can require the desktop app installations on specific desktops and laptops to always work without a proxy.

5. Modify the `SetProxyParams` script, editing the relevant parameters.

> **Note**
>
> The `SetProxyParams` script is configured at machine level. If there are multiple instances of the desktop app installed on a machine, the setting of the `SetProxyParams` is applied to all instances.

Choose from:

- Restrictive mode: Forces users to use the desktop app with the enterprise proxy. The proxy toggle does not appear on the desktop app menu.
- Windows:

```
SetProxyParams.bat host port [username] [password] -r
```

- Mac:

```
sudo sh SetProxyParams.sh host port [username] [password] -r
```

- Permissive mode: Provides users an option to enable or disable use of the proxy from the desktop app menu, to accommodate authentication in different work modes, from within the enterprise network, or externally.
- Windows:

```
SetProxyParams.bat host port [username] [password]
```

- Mac:

```
sudo sh SetProxyParams.sh host port [username] [password]
```

- Disabled mode: Disables use of the desktop app with a proxy on specific devices.
- Windows:

```
SetProxyParams.bat disable
```

- Mac:

Copyright © 2025 Ping Identity Corporation

```
sudo sh SetProxyParams.sh disable
```

Where:

Parameter	Description
`host`	Proxy host IP address or host name.
`port`	Proxy port number.
`username`	Mandatory if the proxy requires credentials. Empty if the proxy does not require credentials.
`password`	Mandatory if the proxy requires credentials. Empty if the proxy does not require credentials.
`-r`	Mandatory for restrictive mode. Empty for permissive mode.

6. (Optional) Configure one of the following for PingID desktop app:
   - Proxy Auto Configuration (PAC). Learn more in Configuring Proxy Auto Configuration for the PingID desktop app
   - Kerberos proxy authentication. Learn more in Configuring Kerberos Proxy authentication for the PingID desktop app.
7. (Optional) To allow the PingID desktop app to work with a proxy, using a self-signed certificate or local CA-signed certificate:
   1. Ensure that the Java Development Kit (JDK) `keytool` utility is installed.
   2. Download a copy of the certificate that is installed on the proxy in DER format, and then save it to the local hard drive.
   3. Open the integrated terminal and navigate to the Java Runtime Environment (JRE) security directory inside the PingID root directory.

      The default paths are:

      - Windows: `C:\Program Files (x86)\Ping Identity\PingID\runtime\lib\security`
      - Mac: `/Applications/PingID.app/Contents/PlugIns/Java.runtime/Contents/Home/jre/lib/security`
   4. Add the certificate to the JRE certificate trust store.

      ```
      keytool -import -keystore cacerts -file <certificate file> -storepass changeit
      ```

Next steps

If you have not yet enabled and configured PingID desktop app as an authentication method in your MFA policy, you can find instructions in Configuring an MFA policy for strong authentication.

Copyright © 2025 Ping Identity Corporation

Configuring Proxy Auto Configuration for the PingID desktop app

Proxy Auto Configuration (PAC) enables you to manage networks that have multiple proxies so that you can configure different proxy servers for different URLs and replace proxies dynamically by editing and updating the PAC file.

Steps

1. On the relevant user's machine, configure the PAC URL:

   Choose from:

   - Windows:

     1. Go to **Start > Settings > Proxy** and then clear the **Automatically detect settings** checkbox.
     2. Select the **Use setup script** checkbox, enter the PAC file address, and click **Save**.

   - Mac:

     1. Go to **System Preferences > Network**, click **Advanced**, and then go to the **Proxies** tab.
     2. Select the **Automatic Proxy Configuration** checkbox.
     3. In the Proxy Configuration File **URL** field, enter the URL of the PAC file that you want to use. Click **OK**.

2. On the relevant user's machine, configure the PingID desktop app to work with PAC according to your operating system.

   Choose from:

   - Windows 32-bit: From the command line, enter `"C:\Program Files\Ping Identity\PingID\ProxyHelperSetup.exe" -pac`.
   - Windows 64-bit: From the command line, enter `"C:\Program Files(x86)\Ping Identity\PingID\ProxyHelperSetup.exe" -pac`.
   - Mac: In a terminal window, enter `sudo /Applications/PingID.app/Contents/MacOS/ProxyHelperSetup -pac`, and then enter the admin password when prompted.

3. Test the communication with the proxy server:

   1. Pair the PingID desktop app.
   2. Open the PingID log file.

      Result:

   If the PingID desktop app can communicate with PingID cloud server, the `Proxy configuration is PAC` entry appears during application startup. If there is no communication, indicated by an `unknown error` message when pairing the PingID desktop app, either the proxy is not working correctly, or there is a configuration problem.

Configuring Kerberos Proxy authentication for the PingID desktop app

The PingID desktop app supports proxy authentication using the Kerberos protocol, delegating the machine credentials for authentication to the organizational proxy.

Copyright © 2025 Ping Identity Corporation

About this task

The PingID desktop app supports proxy authentication using the Kerberos protocol, delegating the machine credentials for authentication to the organizational proxy. The HTTP client uses Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) to negotiate the authentication method.

When Kerberos is the agreed protocol, the client uses a ticket generated by the Key Distribution Center (KDC) for the proxy authentication that can be used multiple times. The Kerberos ticket expiry period can vary according to the KDC configuration.

Steps

1. Ensure that a Kerberos token is initialized on the user's operating system, and then from the command line or terminal window, run `klist` to verify that a valid Kerberos token is available.
2. From the command line or terminal window, enter the following command:

   Choose from:

   - Windows:

     ```
     "C:\Program Files(x86)\Ping Identity\PingID\ProxyHelperSetup.exe"
     <host> <port> -kerberos
     ```

   - Mac:

     ```
     sudo /Applications/PingID.app/Contents/MacOS/ProxyHelperSetup
     <host> <port> -kerberos
     ```

3. From the command line or terminal window, enter the following command to test Proxy Auto Configuration (PAC) with Kerberos.

   Choose from:

   - Windows:

     ```
     "C:\Program Files(x86)\Ping Identity\PingID\ProxyHelperSetup.exe"
     -pac -kerberos
     ```

   - Mac:

     ```
     sudo /Applications/PingID.app/Contents/MacOS/ProxyHelperSetup -pac -kerberos
     ```

(Workforce Only) Configuring YubiKey OTP authentication for PingID

YubiKey hard tokens can be used to generate a one-time passcode (OTP) with which to authenticate. YubiKeys can be paired for Yubico OTP authentication.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If your YubiKey is FIDO2 compliant, you can pair it as a passkey (FIDO2/U2F Security Key). For information about configuring a YubiKey as a passkey for FIDO2 authentication, see Configuring FIDO2 authentication (Passkeys)

A YubiKey hardware authenticator can be used in sensitive environments or for users working in environment with limited device or phone access, such as hospitals, financial institutions, or federal buildings.

The YubiKey hardware gives your enterprise a variety of form factors to allow the user to authenticate combined with the contextual awareness of PingID. YubiKey doesn't require a battery or network connectivity, so it's always on and accessible for MFA.

When YubiKey authentication is enabled, the user registers their personal YubiKey and pairs it with their PingID account. This creates a trust between the YubiKey and the user's account so they can use the YubiKey to authenticate during the sign on process.

Learn how to configure a YubiKey for use with PingID in PingOne in Configuring an MFA policy for strong authentication.

Learn more about the user experience in the PingID End User Guide.

> **Important**
>
> Find the YubiKey models that support Yubico OTP in the YubiKey products page.

Configuring OATH token authentication

You can enable OATH tokens as an authentication method in customer (PingOne MFA) or workforce (PingID) environments. When enabled, users can pair a supported OATH token to their account or app and use it to sign on to your company services and applications with the added security of multi-factor authentication (MFA).

Before you begin

To configure OATH tokens, you must have the following items from each token manufacturer and for each supplied token model:

- A token seed file. The seed file can be either:
  - A `.txt` file consisting of lines with a comma separating the token serial numbers and secret keys (without spaces)
  - A `.csv` file with the token serial numbers and secret keys in different cells (without spaces or commas)

    The secret keys are strings of hexadecimal digits.
- For each seed file, a single associated token type of either TOTP or HOTP.
- For TOTP types, a refresh interval of 30 - 60 seconds, and a hash algorithm of either SHA1, SHA256, or SHA512. The default values are 30 seconds, and SHA256 respectively.

> **Note**
>
> For HOTP types, a start counter can be appended as an additional field in the seed file. If absent, it defaults to 0.

Supported OATH tokens

Copyright © 2025 Ping Identity Corporation

Strong authentication supports hardware OTP tokens that are OATH compliant:

- HOTP SHA-1 devices
- TOTP SHA-1, SHA-256, and SHA-512 devices with 30 or 60 second OTP refresh intervals
- Any of the above devices that use a PIN code

Ping Identity doesn't:

- Sell hardware tokens
- Recommend any particular hardware token manufacturer

The following OATH tokens have been checked for use as an MFA authentication method.

Manufacturer	Model	Type
Feitian	Display card	TOTP-60-sec
Feitian	OTP c200	TOTP-60-sec
Feitian	Display card	HOTP
Gemalto	EZIO display card	TOTP-30-sec
HyperSecu	c100 token	HOTP
HyperSecu	Edge plus	TOTP-60-sec
HyperSecu	c200 token	TOTP-30-sec
HyperSecu	HyperOTP	TOTP-60-sec
HyperSecu	Edge plus	TOTP-30-sec
Protectimus	Protectimus TWO	TOTP-30-sec

About this task

You can use OATH hardware tokens to generate a one-time passcode (OTP) to authenticate. OATH hardware tokens can be useful in situations where users don't or can't have access to the internet, a USB connection, or a mobile device for security reasons.

Learn more about the user experience in the PingID End User Guide.

To add OATH tokens as an authentication method for MFA:

Steps

- Configure the MFA policy, including the OATH-specific configurations. Learn more in Configuring an MFA policy for strong authentication.

Copyright © 2025 Ping Identity Corporation

Configuring an MFA policy for strong authentication

Configure the multi-factor authentication (MFA) policy. Here you can add and configure the relevant authentication methods. You can then add the MFA policy as a step to your authentication policy.

Before you begin

- Optionally configure MFA general settings, including the maximum number of MFA methods allowed per user, authentication method selection, and account lockout settings. Learn more in MFA Settings.
- You can only create multiple MFA policies in a Customer (PingOne MFA) environment.
- (Customer only) Configure an authentication policy with an MFA step. Learn more in Authentication policies.

  > **Note**
  >
  > In a Workforce environment, the authentication policy is created automatically.

- Some authentication methods have configuration steps that you must complete in addition to configuring the MFA policy. Some of these additional configuration steps are compulsory (such as configuring an application for PingID mobile app or configuring a FIDO policy for FIDO2 authentication), and some are optional (such as configuring a notification template for SMS and voice authentication).

  Learn more about the configuration options, as well as any limitations or requirements for each authentication method, in Configuring strong authentication methods (MFA).

About this task

To create an MFA policy:

- Configure the relevant MFA policy settings for the authentication methods that you want to enable.
- If the authentication method requires additional configuration, make sure to complete the additional configuration steps, as outlined in this procedure.

Steps

1. Go to **Authentication > MFA**.
2. On the **MFA Policies** page, click the **+** icon.
3. In the **Name** field, enter a meaningful name for the policy.

   The maximum length is 256 characters.

4. In the **Method Selection** list, for users with more than one paired device, define which device is presented to the user for authentication. Select one.

   Choose from:

   - **User selected default**: Allow the user to authenticate with the device they selected as their default device.
   - **Prompt user to select**: If more than one method is available, when prompted to authenticate, the user is prompted to choose a device from the authentication methods they have paired to their account. Only authentication methods permitted by the relevant authentication policy are shown.

Copyright © 2025 Ping Identity Corporation

- (Workforce only) **Always display devices**: Even if the user has only one permitted authentication method paired with their account, the user is prompted to select an authentication method.

> **Note**
>
> The **Method Selection** setting isn't applied if you have enabled device authorization and the user is accessing an application from a trusted mobile device. It's also not applied if the user is trying to access the application with a browser that they have used for FIDO2 authentication in the past. In such cases, FIDO2 is used.

5. In the **Notification Policy** list, select the notification policy you want to apply to the MFA policy, or select **Use the default policy** to select the default notification policy defined for the environment. Learn more in Notification Policies.

6. In the **Send notification when new device paired** list, select how the user should be notified when a new device has been added to their account.

   Choose from:

   - **No notification**: User should not be notified.
   - **By email, else SMS**: By email (or by SMS if no email address available in the user profile).
   - **By SMS, else email**: By SMS (or by email if no phone number available in the user profile).

7. To apply the MFA policy during authentication, even if the user account is locked, select the **Skip user lock verification** checkbox.

8. If you have used the PingOne API to implement "remember me" functionality in your web applications so that users do not have to authenticate when accessing applications from a remembered device, use the **Remember Me Configurations** section to specify that the MFA policy should allow use of this option:

   1. Under **Remember Me Configurations**, select **Web Session**.
   2. Set the length of time that devices should be remembered (minimum 1 hour, maximum 90 days).

   > **Note**
   >
   > You can find instructions on implementing the "remember me" feature in Remembered Devices.

9. Enable and configure the authentication methods you want to provide for your users:

   1. Click **+ (Add Applications)**, select the name of the mobile application to use from those you have defined for the environment, and click **Save**. Learn more about creating an application in Applications.

      1. Define the following fields for the application:

         - **OTP & Push**: The mechanism that should be used to allow the user to authenticate.

           Choose from:

           - **Push**: Use only the standard push mechanism.
           - **OTP**: Use only OTPs.
           - **Push & OTP**: Use the standard push mechanism and allow OTP as a backup mechanism.

Copyright © 2025 Ping Identity Corporation

- **Push Notification Timeout**: The amount of time that a user has to respond to a push notification before it expires.
- **Allow Pairing**: To prevent users from pairing their device with this authentication method, clear the checkbox.
- **Device Integrity**: Define how authentication and registration attempts should proceed in the event that a device integrity check yields inconclusive results. Select **Permissive** if you want to allow the process to continue. Select **Restrictive** if you want to block the user in such situations.

  > **Note**
  >
  > The **Permissive/Restrictive** buttons are displayed only if device integrity checking is enabled for the application on the **Mobile** tab of the **Applications** definition page.

- **Number Matching**: Enable this option if you want the mobile push to require the user to match a number that they were shown when requesting access. To specify how the matching should be carried out, select one of the number matching options on the **Mobile** tab of the Application page for the relevant application.
- **Auto Enrollment**: Auto Enrollment means that the user can authenticate from an unpaired device, and the successful authentication results in the pairing of the device for MFA. To enable, select the checkbox.

  > **Note**
  >
  > To allow automatic enrollment even if the user does not have any existing paired devices, go to the authentication policy that you created. In the MFA step, verify that **None or Incompatible Methods** is set to **Bypass**. Learn more in Editing an authentication policy.

- **Device Authorization**: When enabled, the trusted device handles the authentication automatically, and no user involvement is required. This automatic mechanism is used only if the user is requesting access from the same device. To enable, select the checkbox.

  Select the **Device Authorization** checkbox and then choose one of the following options for **Extra Verification**:

  - **Disabled**: Do not use an extra verification step.
  - **Permissive**: A push is sent to the device to be handled automatically. If the push is not received, access is granted nonetheless.
  - **Restrictive**: A push is sent to the device to be handled automatically. If the push is not received, access is not granted.

- **Pairing Key Lifetime**: Indicate how much time an issued pairing key can be used until it expires.
- **Limit Push Notifications**: Use this option to help you prevent attacks based on repeated push notifications that lead users to eventually accept the request. Define the number of consecutive push notifications that can be ignored or rejected by a user within a defined period before push notifications are blocked for the application:

  - **Push Limit**: The number of notifications that can be declined or ignored (1 - 50).

Copyright © 2025 Ping Identity Corporation

- **Time Period**: Time period during which the notifications are counted towards the limit (1 minute - 120 minutes).
- **Lock Duration**: Duration for which the device is blocked (2 - 30 minutes).

> **Note**
>
> If you haven't already done so, configure the PingID mobile app. You can also do this after you finish configuring the MFA policy. Learn more in (Workforce Only) Configuring the PingID mobile application settings.

1. In the **Mobile Applications** section, configure the following fields:
   - **Passcode Failure Limit**: Define the maximum number of times that a one-time passcode (OTP) entry can fail.
   - **Lock Duration**: Set the amount of time that the authentication method is locked if the **Passcode Failure Limit** is exceeded. Accepted values range from 2 - 30 minutes.
   - **Rename device during pairing**: Select the checkbox to allow users to define a device nickname during the pairing flow.
2. Under **Add Applications**, **PingID mobile**, configure the following PingID mobile app-specific fields:
   - **Authentication request timeout**: Define the amount of time given before an authetication request times out.
     - **Device Timeout**: Defines the amount of time until the push notification reaches the device. The default is 25 seconds.
     - **Total Timeout**: Defines the amount of time the user has to complete the authentication request. The default is 40 seconds.

       Total Timeout must exceed **Device Timeout** by at least 15 seconds.
   - **Pairing Key Lifetime**: Indicate how much time an issued pairing key or QR code can be used until it expires. (Minimum 1 minute, maximum 48 hours).
   - **Allow Pairing**: Select the checkbox to allow users to pair PingID mobile app. To only allow users from specific IP addresses to pair PingID mobile application, in the list, select **Only these addresses**, and then enter the IP addresses in the format shown in the field.
3. **Limit Push Notifications**: Use this option to help you prevent attacks based on repeated push notifications that lead users to eventually accept the request. Define the number of consecutive push notifications that can be ignored or rejected by a user within a defined period before push notifications are blocked for the application:
   1. **Push Limit**: Number of notifications that can be declined or ignored (1 - 50).
   2. **Time Period**: Time period during which the push notifications are counted towards the push limit (minimum 1 minute, maximum 120 minutes).
   3. **Lock Duration**: Duration for which the device is blocked from authenticating. (1 second - 120 minutes.)

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Limiting the number of push notifications that can be declined or ignored can reduce the likelihood of a user acknowledging a malicious push notification as part of an MFA fatigue attack.

4. (Optional) Enable the following authentication options for users of PingID mobile app:

> **Note**
>
> Only the options that are enabled here are available as an Allowed Authentiation Method in PingID policy. You can find more information about PingID policy in Configuring PingID policy.

- **Push Notification**: Send push notifications to the user's device to notify them of an authentication request.
- **One-Time Passcode**: Allow the user to use a one-time passcode (OTP) to authenticate. The OTP can be used to authenticate even when offline.
- **Biometrics**: Allow the user to authenticate with their device biometrics, such as face or fingerprint authentication.
- **Number Matching**: Allow the user to authenticate by matching the number displayed on the user's accessing device with the corresponding number in PingID mobile app.

- In the **Allowed Authentication Methods** section, select the **Authenticator App** checkbox and then configure the following fields:
  - **Passcode Failure Limit**: Define the maximum number of times that OTP entry can fail (1 - 7).

    > **Note**
    >
    > - Authenticator App (TOTP) passcodes are valid for 30 seconds (refresh duration). However, to cover time synchronization issues, there is a grace period of 8 times the refresh duration in each direction. Taking the grace period into account, the passcode is valid for the base 30 seconds plus 8 x 30 = 240 seconds behind the time of issue and 240 seconds past the expiration time.
    > - In authentication flows that implement one-time authentication with the PingOne MFA API, users are not blocked after exceeding the configured passcode failure limit, even if you specify a blocking period in the MFA policy.

  - **Lock Duration**: The amount of time this authentication method is locked if the **Passcode Failure Limit** is exceeded (2 - 30 minutes).
  - **Allow Pairing**: To prevent users from pairing their device with this authentication method, clear the checkbox.
  - **Rename device during pairing**: Select the checkbox to allow users to define a device nickname during the pairing flow.
  - **Show application name**: To help users recognize which application the OTP displayed in their authenticator app is for, select this option and provide the text that should be displayed alongside the OTP. If you're using the same MFA policy for multiple applications, use a name that reflects the group of applications.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If you provide an application name, remember that users see the name that was in the MFA policy when they paired their device. If you subsequently update the application name in the MFA policy, the new name will be seen only by users who paired their device after the change was made.

- In the **Allowed Authentication Methods** section, select the **YubiKey** checkbox and then configure the following fields:
  - **Passcode Failure Limit**: Define the maximum number of times that OTP entry can fail (1 - 7).

    > **Note**
    >
    > In authentication flows that implement one time authentication with the PingOne MFA API, users are not blocked after exceeding the configured passcode failure limit, even if you specify a blocking period in the MFA policy.

  - **Lock Duration**: The amount of time this authentication method is locked if the **Passcode Failure Limit** is exceeded (2 - 30 minutes).
  - **Allow Pairing**: To prevent users from pairing their device with this authentication method, clear the checkbox.
  - **Rename device during pairing**: Select the checkbox to allow users to define a device nickname during the pairing flow.
- In the **Allowed Authentication Methods** section, select the **Email** checkbox, and then configure the following fields:
  - **Passcode Failure Limit**: Define the maximum number of times that OTP entry can fail (1 - 7).

    > **Note**
    >
    > In authentication flows that implement one-time authentication with the PingOne MFA API, users are not blocked after exceeding the configured passcode failure limit, even if you specify a blocking period in the MFA policy.

  - **Lock Duration**: The amount of time this authentication method is locked if the **Passcode Failure Limit** is exceeded (0 seconds - 30 minutes).
  - **Passcode Lifetime**: The amount of time the passcode is valid before it expires (maximum 30 minutes).

    > **Note**
    >
    > An OTP is valid for 30 minutes by default (refresh duration).

  - **Passcode Length**: Configure the length of the OTP (6 - 10 digits). The default is 6.
  - **Allow Pairing**: To prevent users from pairing their device with this authentication method, clear the checkbox.
  - **Rename device during pairing**: Select the checkbox to allow users to define a device nickname during the pairing flow.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> The following options are available for Workforce (PingID) accounts only:
>
> - To pre-populate or restrict user registration with user directory data, follow the instructions in Pre-populating or restricting user registration data
> - To configure email authentication as a backup authentication method, follow the instructions in Configuring backup authentication methods.

1. In the **Allowed Authentication Methods** section, select the checkbox for the relevant authentication method, and then configure the following fields for each method that you want to add:

   - **Passcode Failure Limit**: Define the maximum number of times that OTP entry can fail (1 - 7).

     > **Note**
     >
     > In authentication flows that implement one-time authentication with the PingOne MFA API, users are not blocked after exceeding the configured passcode failure limit, even if you specify a blocking period in the MFA policy.

   - **Lock Duration**: The amount of time this authentication method is locked if the **Passcode Failure Limit** is exceeded (0 seconds - 30 minutes).

   - **Passcode Lifetime**: The amount of time the passcode is valid before it expires (maximum 30 minutes).

     > **Note**
     >
     > An OTP is valid for 30 minutes by default (refresh duration).

   - **Passcode Length**: Configure the length of the OTP (6 - 10 digits). The default is 6.

   - **Allow Pairing**: To prevent users from pairing their device with this authentication method, clear the checkbox.

   - **Rename device during pairing**: Select the checkbox to allow users to define a device nickname during the pairing flow.

2. Configure all other SMS or voice-related configurations, including creating notification templates, limiting the number of SMS or voice messages that a user can send, localizing messages, and creating a custom sender account. Learn more in Configuring SMS and voice authentication

- In the **Allowed Authentication Methods** section, select the **WhatsApp** checkbox, and then configure the following fields.

  > **Note**
  >
  > You can only select the **WhatsApp** checkbox if your WhatsApp Business account is defined as sender in PingOne. Learn more in Configuring a custom WhatsApp sender account.

  - **Passcode Failure Limit**: Define the maximum number of times that OTP entry can fail (1 - 7).

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> In authentication flows that implement "one-time authentication" with the PingOne MFA API, users are not blocked after exceeding the configured passcode failure limit, even if you specify a blocking period in the MFA policy.

- **Lock Duration**: The amount of time this authentication method is locked if the **Passcode Failure Limit** is exceeded (2 - 30 minutes).
- **Passcode Lifetime**: The amount of time the passcode is valid before it expires (maximum 30 minutes).
- **Passcode Length**: Configure the length of the OTP (6 - 10 digits). The default is 6.
- **Allow Pairing**: To prevent users from pairing their device with this authentication method, clear the checkbox.
- **Rename device during pairing**: Select the checkbox to allow users to define a device nickname during the pairing flow.

> **Note**
>
> Two FIDO policies are available out-of-the-box. You can modify an existing policy or create additional FIDO policies. Learn more in FIDO policies.

- In the **Allowed Authentication Methods** section, select the **FIDO2** checkbox, and then configure the following fields.
  - **Failure Limit**: Define the maximum number of times that a FIDO attestation or assertion can fail.

    > **Note**
    >
    > The failure limit counts only attestations and assertions that reach the PingID server.

  - **Lock Duration**: Set the amount of time that the authentication method is locked if the **Failure Limit** is exceeded. Accepted values range from 2 - 7 minutes. Default value is 3 minutes.
  - In the **Allowed Authentication Methods** section, select **FIDO2** and in the **FIDO Policy** field, select the FIDO policy that you want to apply, or select **Use the default policy** to use the default FIDO policy.
  - **Allow Pairing**: To prevent users from pairing their device with this authentication method, clear the checkbox.
  - **Rename device during pairing**: Select the checkbox to allow users to define a nickname for the device during the pairing flow.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If you are editing an existing MFA policy that is using a deprecated FIDO Biometrics or Security Key authentication method, you'll need to replace it with the FIDO2 authentication method and reference an enhanced FIDO policy. Learn more in Updating an existing MFA policy to use FIDO2.

1. Configure the following fields:
   - **Pairing Key Lifetime**: Indicates the amount of time the pairing key and QR code remain valid before they expire. (Minimum 1 minute, maximum 48 hours).
   - **Allow Pairing**: Select the checkbox to allow users to pair PingID desktop app. To only allow users from specific IP addresses to pair PingID mobile application, in the list, select [.uicontrol**Only these addresses**, and then enter the IP addresses in the format shown in the field.
   - **Rename device during pairing**: Select the checkbox to allow users to define a device nickname during the pairing flow.
2. After you complete and save the MFA policy, add a proxy, and add a security PIN for PingID Desktop app in the PingID Desktop application settings. Learn more in (Workforce Only) Configuring the PingID desktop application.

1. In the **Allowed Authentication Methods** section, select the **OATH Token** checkbox, and then configure the following fields:
   - **Passcode Failure Limit**: Define the maximum number of times that OTP entry can fail (1 - 7).
   - **Lock Duration**: The amount of time this authentication method is locked if the **Passcode Failure Limit** is exceeded (0 seconds - 30 minutes).
   - **Allow Pairing**: To prevent users from pairing their device with this authentication method, clear the check box.
   - **Rename device during pairing**: Select the checkbox to allow users to define a device nickname during the pairing flow.
2. Click the **Configure OATH tokens** link. The OATH token configurations panel opens, showing a list of previously saved tokens. To add an OATH token, do the following:
   1. Click **Import Token**.
   2. In the **Import OATH Token** popup window, click **Choose File**, and navigate to the token seed file. For information about the token seed format, see Configuring OATH token authentication.
   3. Select the **Token Type**.

      > **Note**
      >
      > The token type and OTP length are applied to all entries in the imported file.

   4. If you selected a TOTP **Token Type**, select the **Algorithm** you want to use and the **Refresh Interval**.

      > **Note**
      >
      > The algorithm and refresh interval are applied to all entries in the imported file.

Copyright © 2025 Ping Identity Corporation

5. Click **Import**. The new tokens appear in the list.

> **Tip**
>
> - You can find a list of prerequisites and supported OATH tokens in Configuring OATH token authentication.
> - Make sure your OATH seed token is valid and is not already in use. If your seed file contains entries that duplicate an existing token, you'll see an `Incomplete Token Report` error.
> - To revoke one or more OATH tokens, select the checkbox next to the tokens you want to revoke, and then click **Revoke**.
> - To export token details to a downloadable .CSV file, select the checkbox next to the tokens you want to revoke, and then click **Export CSV**.

10. Click **Save**.

Result:

The policy is added to the **Policy** list.

> **Tip**
>
> In the **Policy** list, click a policy to see a summary of the policy details in the right pane or edit an existing policy.

Next steps

- If you haven't already, add the MFA policy to the MFA step in the relevant Authentication policy. Learn more: Adding a multi-factor authentication or PingID step. This is done automatically for PingID.
- Optionally configure Notification Templates to inform users about device pairing and strong authentication events. Learn more in Notification templates.

Updating an existing MFA policy to use FIDO2

If your MFA policy includes FIDO biometrics or security key authentication methods, you'll be asked to update your FIDO policy to the enhanced FIDO2 policy.

Before you begin

Note the following:

- FIDO2 authentication is supported in PingOne MFA and PingOne DaVinci.
- When updating your MFA policies to support the FIDO2 authentication method, you must also update:
  - All scripts that include the deprecated FIDO Biometrics and Security Key authentication methods.
  - All PingOne DaVinci flows that include the PingOne MFA Connector, and use the deprecated FIDO Biometrics and Security Key authentication methods.

Copyright © 2025 Ping Identity Corporation

Warning

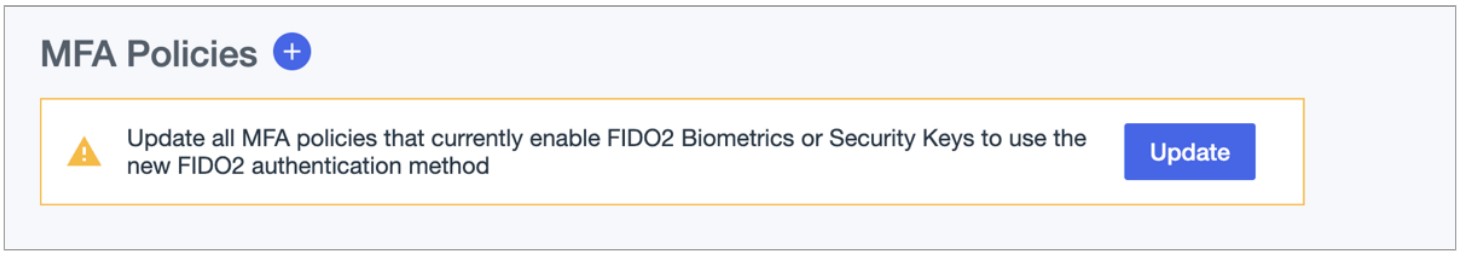
If you have integrated an existing PingID account with your PingOne environment, after updating FIDO devices to use the FIDO2 authentication method it is not possible to unlink the PingID account. Deleting the PingOne environment will also delete the PingID account.

About this task

As of June 20, 2023, FIDO biometrics and Security Key authentication methods are being phased out.

The FIDO2 authentication method replaces the deprecated FIDO biometrics and security key authentication methods and offers an expanded range of configurations and support for a wide range of FIDO authentication devices, including cloud-synced FIDO devices.

If your MFA policy references a FIDO policy with the deprecated authentication methods, you'll see a notice in the MFA page asking you to update the policy.



If you see this notice, follow these instructions to update your policy.

Note

- Updating the MFA policies to use the new FIDO2 authentication method inactivates the deprecated FIDO biometrics and security key authentication methods.
- After updating MFA policies to the new FIDO2 authentication method, the **Allow Pairing** checkbox is selected by default.

Steps

1. Go to **Authentication > MFA**.

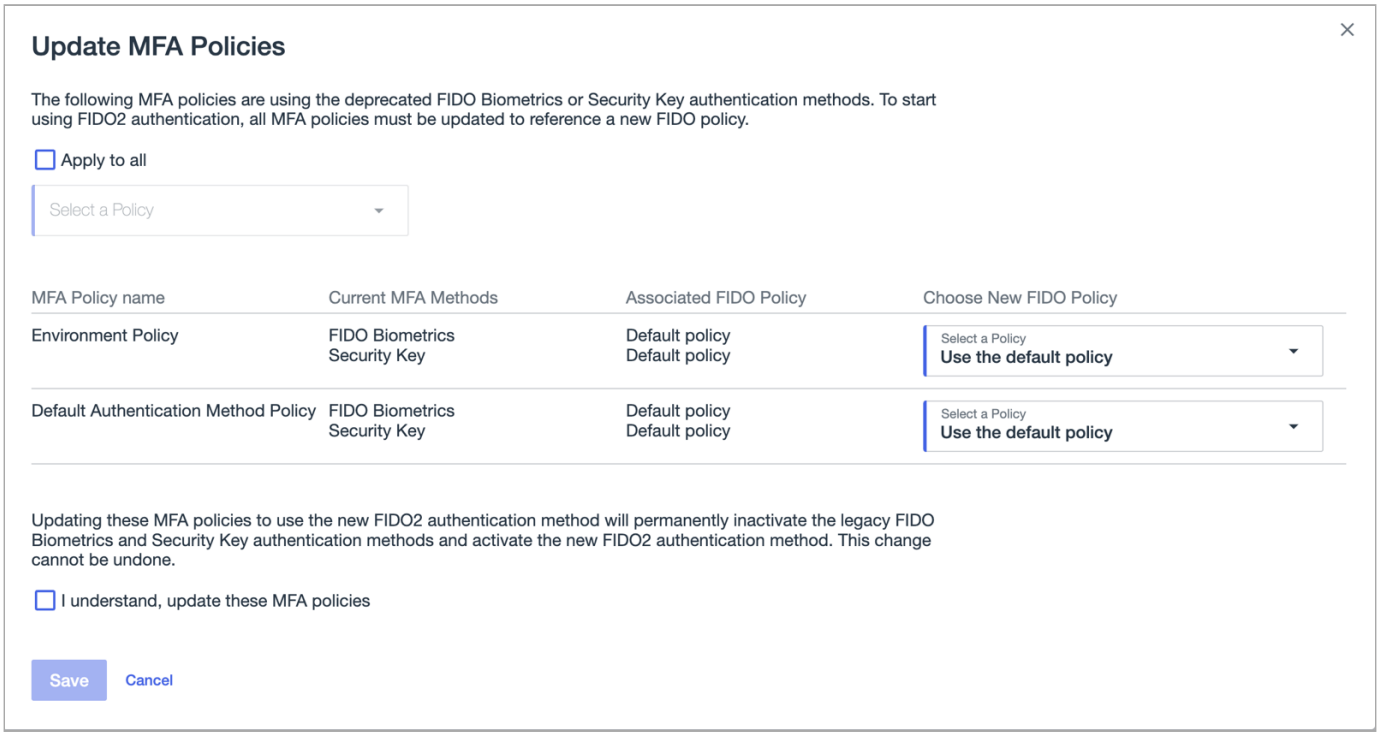
   If you must update your policy, first ensure that your FIDO2 policy is defined correctly for your organization. Learn more about configuring a FIDO2 policy in Adding a FIDO policy.

2. On the **MFA Policies** page, click **Update**.

   Result:

   The **Update MFA Policies** window opens, listing all of the MFA policies that currently include a deprecated FIDO policy.

Copyright © 2025 Ping Identity Corporation



3. Update the affected MFA policies.

   Choose from:

   - To update all affected MFA policies with the same enhanced FIDO policy, select the **Apply to all** checkbox, and then select the relevant enhanced FIDO policy from the list. The selected FIDO policy is applied to all MFA policies listed.
   - To update each MFA policy individually, for each MFA policy listed in the table, in the relevant row, select the enhanced FIDO policy in the **Choose New FIDO Policy** list.

   > **Note**
   >
   > To specify the default FIDO policy, select **Use the default policy**.

4. To complete the upgrade, click**I understand** and then click **Save**.

   Result:

   The FIDO2 biometrics and security key authentication methods are deactivated for the MFA policies listed, and FIDO2 authentication is activated.

Next steps

After updating your MFA policies, all scripts that rely on the deprecated FIDO Biometrics and Security Key methods, and all PingOne DaVinci flows that include the PingOne MFA Connector using one of these methods, should also be updated.

Copyright © 2025 Ping Identity Corporation

Strong authentication (MFA) integrations

You can integrate Customer (PingOne MFA) and Workforce (PingID) strong authentication (MFA) solutions with various platforms and solutions, including:

- API: If you want to use PingOne APIs, configure a worker app.
- DaVinci:
  - Learn more about using DaVinci in the DaVinci documentation.
  - For a list of relevant DaVinci flows, search for PingOne MFA in the Ping Identity Integration Directory.
  - (Customer only) Learn more about configuring the PingOne MFA connector in PingOne MFA connector.
  - (Workforce only) Learn more about configuring the PingID connector in PingID connector.
- PingFederate:
  - Customer only: To integrate PingOne MFA with PingFederate:
    1. Integrate PingOne with PingFederate. Learn more in Integrating with PingFederate.
    2. Configure the PingOne MFA Integration Kit in PingFederate. Learn more in PingOne MFA Integration Kit.
  - Workforce only: To integrate PingID with PingFederate:
    - Integrate PingID as an authentication solution with PingFederate either as a federation solution or as an identity bridge. Learn more in Integrate with PingID for PingFederate SSO in the PingID Administration Guide.
- Microsoft Entra ID:
  - Workforce only: Integrate PingID as an authentication solution for Microsoft Entra ID. This integration requires PingOne SSO. Learn more in Setting up PingOne SSO and PingID as the external MFA provider for Microsoft Entra ID.

PingID-specific integrations

You can integrate PingID with:

- **RADIUS Gateway**: Learn more in RADIUS gateways.
- **Windows login passwordless**: Learn more in Setting up Windows passwordless login.
- **Windows login**: Learn more in Integrating PingID with Windows login in the PingID Administration Guide.
- **Mac login**: Learn more in PingID integration for Mac login in the PingID Administration Guide.
- **SSH**: Learn more in Integrate PingID with SSH in the PingID Administration Guide.

Copyright © 2025 Ping Identity Corporation

Integrating with PingFederate

You can integrate PingFederate with PingOne MFA. The PingOne console has a built-in wizard for configuring a PingFederate connection. A PingFederate connection in PingOne MFA is actually a worker app with a specific configuration.

Before you begin

Make sure you've done the following:

- Created an application.
- Associated the application with an authentication policy that has an MFA step. Learn more in Authentication policies.

About this task

The wizard for creating a new PingFederate connection is an abridged worker app creation flow. Organizations using PingFederate as an identity provider (IdP) should implement this configuration.

> **Note**
> This configuration applies only if you are integrating PingOne MFA with PingFederate.

Steps

1. In the PingOne admin console, go to **Integrations** > **PingFederate**.
2. Click **+ Add Connection**.

   Result:

   The **Create Connection Profile** page opens.
3. Enter:
   - An appropriate **Connection Name**, such as `PingFederate Connection`
   - An optional **Description**
4. Click **Save and Continue**.

   Result:

   The **Establish Connection with PingFederate** page opens.
5. Copy the **Credentials** to your clipboard.
6. Click **Close**.

   Result:

   The new connection appears with the **New** mark on the **PingFederate Connections** page.
7. Go to the PingFederate administrative console and add the connection in PingFederate.

   Learn more in Connections to PingOne.

Next steps

Copyright © 2025 Ping Identity Corporation

Creating a web application

Configuring PingID policy

You can configure a PingID policy.

PingID policy is configured and managed in the PingID admin portal. You can find details in PingID authentication policy in the PingID Administration Guide.

> **Note**
>
> PingID device and pairing requirements are configured in the (Workforce Only) Configuring the PingID mobile application settings

Managing PingID in PingOne

Although many management tasks can be performed in PingOne, some PingID management tasks must still be done in the PingID admin portal. This section details information and tasks related to how to manage PingID in PingOne, indicating which tasks are performed in the PingID admin portal, and which tasks can be performed in PingOne. All PingOne MFA management tasks are performed in PingOne.

What would you like to do?

- Managing a user's devices and services
- Allow users to manage their PingID devices using MyAccount
- Configure PingID offline MFA
- Perform PingID life cycle management
- View PingID language support information
- Pre-populating or restricting user registration data

Accessing the legacy PingID admin portal from PingOne

About this task

If you have a PingID account integrated with a PingOne environment, most configurations are done in PingOne. However there are a limited number of administrative configurations (such as PingID policy) that are currently configured in the legacy PingID admin portal.

You can access the PingID admin poral directly from the PingOne environment home page.

Copyright © 2025 Ping Identity Corporation

Steps

- In PingOne, go to **Overview** and under **Services**, click the PingID icon. The legacy PingID admin portal opens.

> **Note**
>
> Fields that should be configured in PingOne are greyed out in the legacy PingID admin portal, and a link to the equivalent field in PingOne is provided.

Using MyAccount to manage PingID devices

Configure self-service options to allow your PingID users to manage their devices using the MyAccount app.

About this task

This section show you how to configure MyAccount to allow PingID workforce users from environments that are converged with PingOne to manage their devices.

Learn more about self-service configuration in Self Service.

Steps

1. Go to **User Experience > Self Service** and select **Edit**.
2. Select **Manage Authentication** and then select **Manage PingID Devices via MyAccount**.

> **Note**
>
> - Selecting **Manage PingID Devices via My account** also:
> - Enables the **Allow user actions according to granted authentication scopes** option in the MyAccount app **Resources** tab. This option provides users with a limited set of scopes until they authenticate.
> - Adds the MyAccount app to all PingID policies that already include Device Management.
> - To allow PingID users to manage their account with limited scopes, you must also ensure an MFA policy or MFA DaVinci flow policy is added to the MyAccount app.
> - Learn more about adding a policy to the app in Associating an authentication policy with a web app.
> - Learn more about disabling reduced scopes in Editing scopes for an application.
> - You can find information about PingOne API scopes and their function in PingOne self-management scopes.

PingID Offline MFA

PingID runs as a cloud service on the PingOne platform. To allow users to authenticate even if the PingID service is unreachable, PingID includes offline multi-factor authentication (MFA).

You need to configure offline MFA so that your users can take advantage of it in the event that PingID service is unreachable.

You can configure PingID offline MFA for the following use cases:

- Access through PingFederate single sign-on (SSO)
- Access through RADIUS password credential validator (PCV)

Copyright © 2025 Ping Identity Corporation

- Access through Windows login
- Access through Windows login (passwordless)
- Access through Mac login
- Access through the PingID integration with SSH

Below is an outline of the steps required to configure offline MFA for each of these cases. Links are provided to the detailed information for each case.

> **Note**
>
> - PingID policy rules that have been defined are not enforced when authenticating in offline mode.
> - Device requirements are taken into account when authenticating in offline mode.
> - Changes to the device list that occur during offline mode are updated in the user directory only when the user next authenticates online.

PingID offline MFA when authenticating through PingFederate single sign-on (SSO)

Offline MFA requires the following:

- A user directory to store user device information from PingID. Learn more in User directory for PingID Offline MFA.
- Unlimited Strength Java Cryptography Extension (JCE), which is required for supporting the 256-bit key size for cryptographic algorithms. Without it, the feature will return an exception related to the missing library and will not function.

When the PingID service is unreachable, after first-factor authentication, the user receives a QR code on an offline authentication screen.

To enable offline authentication, carry out the optional offline MFA step described in Installing the PingID Integration Kit for PingFederate, and configure offline MFA for the PingID Adapter as described in Configuring offline MFA (PingID Adapter).

When configuring the PingID Adapter for offline MFA, the most important option to configure is **Authenticating During Errors**, which can be set to one of:

- Bypass User
- Block User
- Passive Offline Authentication

> **Note**
>
> In addition to the standard options listed above, if you encounter a situation where PingID is down but the Passive Offline Authentication option is not prompting users to authenticate offline, you can select the **Enforce Offline Authentication** option for a limited time until the issue is resolved. This will force all your users to authenticate offline until you switch back to one of the standard options.

PingID offline MFA when accessing through RADIUS password credential validator (PCV)

When the PingID service is unreachable, after first-factor authentication, the user receives a 12-digit security key in the VPN client.

Copyright © 2025 Ping Identity Corporation

You can find detailed instructions on configuring offline MFA with PingID RADIUS PCV in Configuring offline MFA (RADIUS PCV).

> **Note**
>
> PingID offline MFA does not support RADIUS VPNs with no challenge.

When configuring offline MFA for the PingID RADIUS PCV, the most important option to configure is **Authentication During Errors**, which can be set to one of:

- Bypass User
- Block User
- Passive Offline Authentication

> **Note**
>
> In addition to the standard options listed above, if you encounter a situation where PingID is down but the Passive Offline Authentication option is not prompting users to authenticate offline, you can select the **Enforce Offline Authentication** option for a limited time until the issue is resolved. This will force all your users to authenticate offline until you switch back to one of the standard options.

PingID offline MFA when accessing through Windows login

When the PingID service is unreachable, after first-factor authentication, the user is prompted to authenticate using a security key or the PingID mobile app in offline MFA mode (manual authentication).

You can find detailed information about configuring offline MFA for Windows login in Installing the PingID integration for Windows login.

The behavior for offline situations is determined by the value provided for the `offlineAuthType` parameter when carrying out command-line installation of the integration with Windows login. You can set `offlineAuthType` to:

- 0 - do not allow MFA for offline authentication
- 1 - allow offline MFA using PingID mobile app only
- 2 - allow offline MFA using a FIDO2 security key only
- 3 - allow offline MFA using either PingID mobile app or a FIDO2 security key

PingID offline MFA when accessing through Windows login (passwordless)

When the PingID service is unreachable, after authentication is initiated, the user is prompted to authenticate using a security key or the PingID mobile app in offline MFA mode (manual authentication).

You can find details in the description of the **Offline Mode** option in Creating an authentication policy (Windows passwordless).

PingID offline MFA when accessing through Mac login

When the PingID service is unreachable, after first-factor authentication, the user is prompted to authenticate using a security key or the PingID mobile app in offline MFA mode (manual authentication).

You can find detailed information about configuring offline MFA for Mac login in Installing the PingID integration for Mac login.

Copyright © 2025 Ping Identity Corporation

The behavior for offline situations is determined by the value provided for the `offlineAuthType` parameter when carrying out command-line installation of the integration with Mac login. You can set `offlineAuthType` to:

- 0 - allow offline MFA with the PingID mobile app
- 1 - if the user does not have a paired PingID mobile app with their account, bypass MFA during login
- 2 - do not allow offline MFA

Offline MFA when using the PingID integration with SSH

When the PingID service is unreachable, after first-factor authentication, the user receives a 12-digit security key in the terminal window.

You can find detailed information in Enabling offline MFA in SSH integration.

The behavior for offline situations is determined by the value provided for the `fail_mode setting` in the configuration file, which can set to:

- `restrictive`
- `passive_offline_authentication`
- `permissive`

> **Note**
> In addition to the standard options listed above, if you encounter a situation where PingID is down but the `passive_offline_authentication` option is not prompting users to authenticate offline, you can select the `enforce_offline_authentication` option for a limited time until the issue is resolved. This will force all your users to authenticate offline until you switch back to one of the standard options.

User directory for PingID Offline MFA

PingID offline multi-factor authentication (MFA) supports storage of user authentication device details according to different user directory deployments.

User directory

PingID offline MFA can access device information stored in the directory's user object, or in a directory object separate from the user object, either in the same directory as the user object, or in a different directory.

> **Note**
> The PingID offline MFA feature is designed to work with directories from several vendors, including Active Directory, Oracle Directory, and Ping Directory.
> Directory setup scripts are provided for Active Directory as part of the PingID Integration Kit 2.0 and later. You must configure other directories manually.
> Learn more about directory configuration: Installing the PingID Integration Kit for PingFederate.

Scripts provided in the PingID Integration Kit 2.0 or later add the following attributes to the directory:

Copyright © 2025 Ping Identity Corporation

`pf-pingid-state`

The `pf-pingid-state` attribute holds the authentication state of the user during offline MFA.Administrators can use this attribute to bypass or block individual users.It is an optional attribute. When it is used, it must be coupled with the `user` object class on the main user directory. The optional values, `block` or `bypass`, stored in this attribute are managed by the administrator. For more information, see Configuring offline MFA (PingID Adapter) or Configuring offline MFA (RADIUS PCV).PingFederate only requires read access to the `pf-pingid-state` attribute.The value of the `pf-pingid-state` attribute is always stored in the user's object. You can assign a different name to the attribute using the setup script, within the limits permitted by the user directory.When PingID is offline, the identity provider checks the configuration.

- If the user's `pf-pingid-state` configuration is empty, the authentication flow continues.
- If `pf-pingid-state` is set to `bypass`, the user bypasses MFA.
- If `pf-pingid-state` is set to `block`, the user is blocked from logging in.

`pf-pingid-local-fallback`

The `pf-pingid-local-fallback` attribute holds the user's authentication devices list information.It is a mandatory attribute.The administrator must decide between:

- Adding the attribute to the `user` objectClass on the main user directory.
- Adding the attribute to a separate custom `pf-pingid-device` objectClass.

If you add `pf-pingid-local-fallback` to `pf-pingid-device`, you must decide which directory should hold the `pf-pingid-device` objects. These objects can be stored in the same directory as the users in a different location in the directory tree, or in an entirely separate directory. PingFederate configuration will vary according to the design you choose.

Multiple Adapter/PCV Instances: When running a single PingFederate server with multiple PingID tenants, the `pf-pingid-local-fallback` attribute cannot be linked to the user objectClass. It is mandatory to set up a separate custom `pf-pingid-device` objectClass. The location of the `pf-pingid-device` objects must be different for each Adapter/PCV instance.

If multiple Adapter/PCV instances use the same PingID tenant, there is no restriction on the `pf-pingid-local-fallback` attribute location.

For more information, see Installing the PingID Integration Kit for PingFederate. PingFederate will have read and write access to the `pf-pingid-local-fallback` attribute, because values stored in this attribute are managed by PingFederate.

Priority of parameter settings during the flow of PingID offline MFA

1. If the `Authentication During Errors` parameter is set to `Bypass` or `Block`, the user's `state` attribute is ignored during offline authentication. All users will either bypass PingID offline MFA or be blocked from authenticating, according to the `Authentication During Errors` setting.
2. If the `Authentication During Errors` parameter is set to `Passive` or `Enforce`, PingFederate checks the user's `state` attribute.

The user's `state` attribute is empty

If the user has a paired mobile device, the flow proceeds to offline MFA.If the user does not have a paired mobile device, the flow proceeds according to the setting in the `Users Without a Paired Device` parameter.

Copyright © 2025 Ping Identity Corporation

The user's `state` *attribute is set to* `Bypass`

The user will bypass PingID offline MFA.

The user's `state` *attribute is set to* `Block`

The user is blocked from authenticating.

Bypass MFA for a specific user

You can bypass multi-factor authentication (MFA) for a specific user for a specific duration. This suspends the requirement for a user to authenticate using their secondary authentication method for the specified amount of time.

Steps

1. Go to **Directory** > **Users** and browse or search for the user that you want to edit.
2. Click the user entry to open the user details panel.
3. In the **Services** list, select **Authentication** and enter or edit authentication information.
4. To bypass MFA for single sign-on (SSO), in the **Multi-Factor Authentication** section, click **Allow MFA bypass**, and then in the **Bypass** modal, select the bypass duration and click **Bypass**.

   The bypass time remaining and a **Resume** link are shown. Click **Resume** to resume MFA for the selected user.
5. (Workforce only) To bypass MFA for a specific service, in the **Integrations** section, next to the relevant service, click the **More Options (⋮)** icon and then select **Disable** or **Bypass**. Bypassing a service suspends the need for a user to authenticate using the secondary authentication method for a specified amount of time.

   > **Note**
   >
   > Audit events for bypassing a non-SSO service are only logged in the legacy PingID admin portal PingID report, and appear in the format `{service-name} bypass`

Pre-populating or restricting user registration data

For SMS, voice, and email authentication, you can pre-populate or restrict registration to corporate information that is already defined in your organization's user directory.

The following options are available:

Pre-Populate

When registering a device for email, or SMS and voice authentication, the email or phone number field pre-populated with the information defined in your user directory. The user can edit the information or replace it with a different address or phone number.

Copyright © 2025 Ping Identity Corporation

Restrict

When registering for PingID, the email, SMS, or voice field is pre-populated with the information defined in your user directory. The information is read-only and cannot be edited by the end user. If information in the user directory is missing or invalid for a specific device type, the user is not presented with the option to register with that device.

The configurations are applied during initial registration and during the registration of additional devices if you have enabled multiple-device capability.

This feature is configured in the PingID admin portal. Learn more in Pre-populating or restricting user registration data in the PingID Administration Guide.

PingID user life cycle management

This section details where to find information relating to PingID user life cycle management.

Managing the PingID user life cycle includes various tasks. While many tasks can be performed in PingOne Some tasks are still performed in the PingID web portal.

- Tasks performed in the web portal:
  - Configuring the PingID support message
  - Configuring the PingID enrollment settings
- Enabling or unlocking a user account or device
- Managing a user's devices and services includes:
  - View details of paired devices per user
  - Changing the user's default (primary) device
  - Unpair a device
  - Block a device
  - Disable a service
  - Bypass a service
- Provisioning users: When integrating with PingFederate, use the Provisioning Connector to create, update, disable and delete users in PingOne.

  Learn more about user management in PingOne: Users.

PingID branding and themes

This section details where to find information relating to branding and themes for PingID.

You can customize the default logo that appears on the PingID enrollment (registration) page and in the PingID mobile app. Learn more in Branding and themes and Editing environment branding.

Copyright © 2025 Ping Identity Corporation

PingID language support

PingID supports a wide variety of languages.

PingID mobile app and PingID clients support the following languages:

- French (EU)
- French (Canadian)
- German
- Japanese
- Chinese
- Dutch
- Italian
- Korean
- Portuguese
- Russian
- Thai
- Turkish
- Polish
- Czech
- Hungarian

The language displayed is defined as follows:

- **PingID mobile app**: According to the language defined in the user's mobile device language settings.
- **PingID authentication and registration screens**: According to the language settings of the web browser that is used.
- **SMS and Voice messages**: You can define the languages supported. The language displayed is according to the language settings of the web browser being used. Learn more in Enabling and customizing language localization for SMS authentication in PingID.

All other features are supported by the full list of PingOne supported languages. Learn more in Languages.

You can find information about the user experience in the PingID End User Guide.

Using the PingID Device Trust agent

Your risk policies can include the PingID Device Trust risk predictor if your users have installed the PingID Device Trust agent on their computers.

Copyright © 2025 Ping Identity Corporation

The PingID Device Trust predictor checks if a device is trusted by validating the trust created during the installation of the PingID Device Trust agent.

Use of the PingID Device Trust risk predictor requires a PingID license. Currently, to use the predictor you also need to have a PingOne Protect license.

Learn more about the PingID Device Trust risk predictor in PingID device trust.

> **Note**
> In terms of browser support, the trust agent currently does not work for users who are accessing applications from Safari.

Basic steps

To use the PingID Device Trust risk predictor in risk evaluations, perform the following steps:

- In a PingOne environment where a PingID account has been integrated:
  - Create a worker application.

    > **Note**
    > In this context, the worker application requires only the Accessing Device permissions, so for maximum security, it is recommended that you create a custom PingOne role that has only these permissions, and grant only that role to the worker application.

  - Add the PingID Device Trust risk predictor to one of your risk policies
- Using PingFederate (minimum version 11.3) or PingOne DaVinci, create a flow that uses the risk policy with the PingID Device Trust predictor, and carry out the additional configuration steps required.
- Ensure that the PingID Device Trust agent has been installed on your users' computers.

Designing flows with PingID Device Trust predictor in PingFederate

Before designing the flow:

- Download and install version 1.0.5 or higher of the PingOne Protect Integration Kit.
- Restart PingFederate

Designing the flow:

- In your HTML Form Adapter:

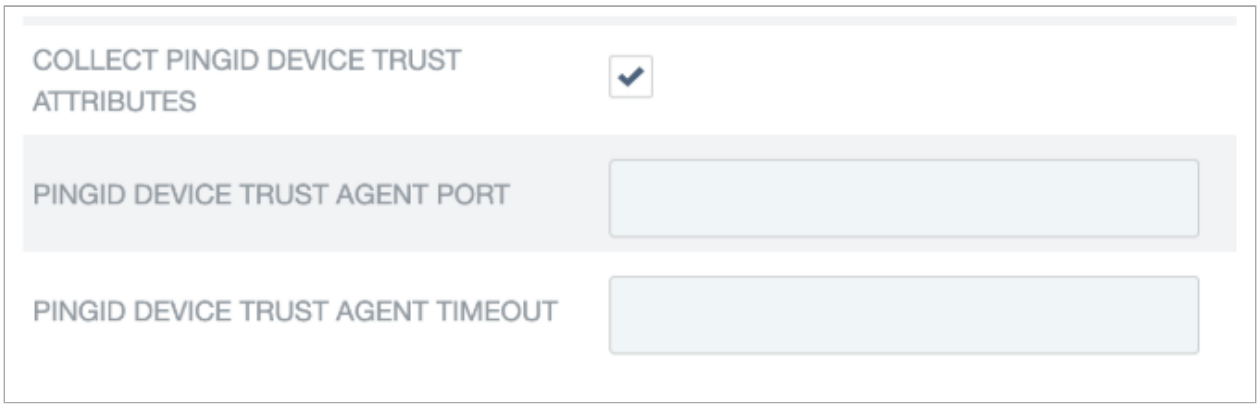
  1. Go to **Manage CAPTCHA and Risk Providers**.

     > **Note**
     > The steps in this section refer to the provider, but you can also enable and configure the PingID Device Trust agent in the configuration of the PingOne Protect Adapter.

  2. Select the existing PingOne Protect provider, or create a new one.

Copyright © 2025 Ping Identity Corporation

3. In the **Instance Configuration**, click **Show Advanced Fields** and then select **Collect PingID Device Trust attributes**.



4. If you don't want the agent to use the default port (9400), use the **PingID Device Trust agent port** field to specify the port to use.
5. If you don't want to use the default agent timeout (1000 ms), use the **PingID Device Trust agent timeout** field to specify the timeout to use.
6. Save.

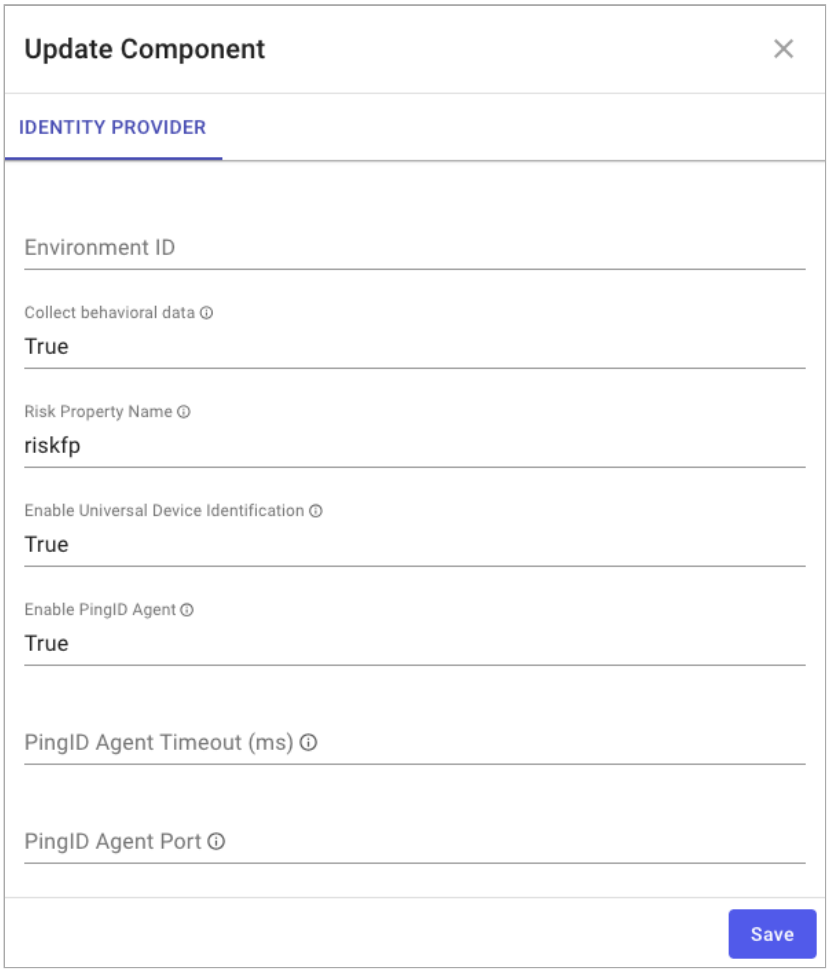
- Design your flow, using the possible risk evaluation responses for policies with the PingID Device Trust predictor.
- You can take into consideration both the risk level calculated for the trust predictor and the detailed data that is included in the response under `details.device.agent`. Note that the `details.device.agent` object is not included in the response if the risk level calculated for the trust predictor is HIGH. For details of the agent-related fields included in the response, see the Details data model table in the API documentation.

Designing flows with PingID Device Trust predictor in DaVinci

Carry out the following steps so that the risk evaluation in your flow receives the data from the trust agent:

- In your flow with risk evaluation, locate the HTTP connector where you added the **skrisk** component to the flow (as described in PingOne Protect Connector) and open the **Update Component** window for the **skrisk** component.

Copyright © 2025 Ping Identity Corporation



- Set **Enable PingID Agent** to True.
- If you don't want to use the agent timeout (1000 ms), use the **PingID Agent Timeout** field to specify the timeout to use.
- If you don't want the agent to use the default port (9400), use the **PingID Agent Port** field to specify the port to use.

> **Note**
>
> You can also enable and configure the PingID Device Trust agent using the PingOne Forms connector (**General** tab, after enabling **Device Profiling**).

- Continue designing your flow, using the possible risk evaluation responses for policies with the trust predictor.
- You can take into consideration both the risk level calculated for the trust predictor and the detailed data that is included in the response under `details.device.agent`. Note that the `details.device.agent` object is not included in the response if the risk level calculated for the Trust predictor is HIGH. For details of the agent-related fields included in the response, see the Details data model table in the API documentation.

Installing the PingID Device Trust agent on Windows computers

You can install the PingID Device Trust agent on a Windows computer with a GUI-based installation or with a command-line installation.

Copyright © 2025 Ping Identity Corporation

The GUI-based installation is provided only for testing purposes. Installation of the agent on user computers should be done only with the CLI installation.

At the moment, it is not possible to define a custom path for the installation. The agent will be installed to: `C:\Program Files\Ping Identity\PingID\Device Trust`

Installation requirements

- The user installing the agent must have administrator privileges for the computer.
- Users' computers must be running Windows 10 (64-bit) or Windows 11 and must support TPM 2.0.

GUI installation

- Download the GUI-based installation from the PingID download page.
- Run the downloaded .exe file to launch the installation wizard.
- On the first screen of the wizard (Device Trust Agent Settings), enter the mandatory information.
- If your company uses a proxy, click **Confgure Proxy** and enter the necessary proxy information.
- Click **Next** to proceed to the Optional Settings page
- If you want to run a custom script to provide the risk evaluation with additional data for the computer, enter the path to the relevant batch file. The use of custom scripts with the PingID Device Trust predictor is explained here.
- Use the Custom domain field if sign-on flows are going to be initialized from a domain other than the PingOne base domain.
- If you don't want the agent to listen on the default port - 9400, enter a different port number.

CLI installation

- Download the installation executable from the PingID download page.
- From the command-line, run the executable with the necessary parameters:

```
PingIdDeviceTrust_<version>.exe /LOG=intsllation.log /VERYSILENT /SUPPRESSMSGBOXES /PingOneBaseDomain="<PingOne base domain>" /EnvironmentID="<the environment id>" /ClientID="<the client id>" /ClientSecret="<the client secret>"   /NORESTART
```

Mandatory parameters

Parameter	Description
`PingOneBaseDomain`	The PingOne base domain, for example, pingone.com
`EnvironmentID`	The ID of the environment that contains the worker app and the risk policy
`ClientID`	The client ID for the worker app
`ClientSecret`	The client secret for the worker app

Copyright © 2025 Ping Identity Corporation

Optional parameters

Parameter	Description
`LOG`	The location of installation log file. If left out, no log file is created.
`Port`	Specify a port number if you don't want the agent to listen on the default port, 9400.
`ScriptFilePath`	The path to the relevant batch file if you want to run a custom script to provide the risk evaluation with additional data for the computer. The use of custom scripts with the PingID Device Trust predictor is explained here.
`CustomDomain`	If sign-on flows are going to be initialized from a domain other than the PingOne base domain, specify the domain.
`proxyAddress`	If your company uses a proxy, specify the address.
`proxyUserName`	If the proxy requires authentication, specify the username.
`proxyPassword`	If the proxy requires authentication, specify the password.
`VERYSILENT`	Should be included to prevent the display of UI elements such as progress window during CLI installation.
`SUPPRESSMSGBOXES`	Should be included to prevent the display of message boxes during CLI installation.
`NORESTART`	Include to prevent the computer from rebooting when the installation is complete.

Installing the PingID Device Trust agent on Mac computers

You can install the PingID Device Trust agent on a Mac computer with a GUI-based installation or with a command-line installation.

The GUI-based installation is provided only for testing purposes. Installation of the agent on user computers should be done only with the CLI installation.

At the moment, it is not possible to define a custom path for the installation. The agent will be installed to: `/usr/local/pingid/DeviceTrust`

> **Note**
> The user installing the agent must have administrator privileges for the computer.

GUI installation

- Download the Mac installation file from the PingID download page.
- Extract the individual files:
  - Package file: DeviceTrust.<version>.pkg

    - CLI installer: InstallPingIdDeviceTrust
    - Installer settings: devicetrust.installer.properties
- Copy the `devicetrust.installer.properties` file to the `/tmp` directory (this is currently not configurable - the installer looks for the properties file in `/tmp`)
- Update the `devicetrust.installer.properties` file with the values for the mandatory properties:
    - PingOneBaseDomain
    - EnvironmentID
    - ClientID
    - ClientSecret
- Specify values for any of the optional properties you want to use:
    - If your organization uses a proxy: ProxyAddress, ProxyUsername, ProxyPassword
    - If you want to run a custom script to provide the risk evaluation with additional data for the computer, set ScriptFilePath to the path to your script. The use of custom scripts with the PingID Device Trust predictor is explained here.
    - If sign-on flows are going to be initialized from a domain other than the PingOne base domain, set CustomDomain to that domain.
    - If you don't want the agent to listen on the default port - 9400, set Port to a different port number.
    - If you want more detailed information to be logged during installation, set LogLevel to 1.
- Launch the .pkg file to begin the installation.
- Click **Install**.

CLI installation

- Download the Mac installation file from the PingID download page.
- Extract the individual files:
    - Package file: DeviceTrust.<version>.pkg
    - CLI installer: InstallPingIdDeviceTrust
    - Installer settings: devicetrust.installer.properties
- From the command line, run the Mac installer, providing the necessary values for the parameters:

```
sudo ./InstallPingIdDeviceTrust "[-Package= full path to DeviceTrust .pkg]" "-PingOneBaseDomain=<PingOne base domain>" "-EnvironmentID=<EnvironmentID>" "-ClientID=<ClientID>" "-ClientSecret=<ClientSecret>" "[-ScriptFilePath=<ScriptFilePath>]" "[-Port=<Port>]" "[-CustomDomain=<CustomDomain>]" "[-ProxyAddress=<ProxyAddress>" "-ProxyUsername=<ProxyUsername>" "-ProxyPassword=<ProxyPassword>]"
```


Copyright © 2025 Ping Identity Corporation

Mandatory parameters

Parameter	Description
`Package`	The full path of the package file (.pkg). If not specified, the installer looks for the .pkg file in the current folder.
`PingOneBaseDomain`	The PingOne base domain, for example, pingone.com.
`EnvironmentID`	The ID of the environment that contains the worker app and the risk policy.
`ClientID`	The client ID for the worker app.
`ClientSecret`	The client secret for the worker app.

Optional parameters

Parameter	Description
`Port`	Specify a port number if you don't want the agent to listen on the default port, 9400.
`ScriptFilePath`	The path to the relevant batch file if you want to run a custom script to provide the risk evaluation with additional data for the computer. The use of custom scripts with the PingID Device Trust predictor is explained here.
`CustomDomain`	If sign-on flows are going to be initialized from a domain other than the PingOne base domain, specify the domain.
`ProxyAddress`	If your company uses a proxy, specify the address.
`ProxyUsername`	If the proxy requires authentication, specify the username.
`ProxyPassword`	If the proxy requires authentication, specify the password.
`LogLevel`	The level of logging carried out during installation and running of the agent. The default level is 0. To raise the logging level from Info to Debug, set LogLevel to 1.

To uninstall the PingID Device Trust agent, run the following command:

```
sudo /usr/local/pingid/DeviceTrust/bin/uninstall
```

Logging

Separate log files are created for installation of the agent and for the ongoing activity of the agent.

Copyright © 2025 Ping Identity Corporation

Log files on Windows

When installing on Windows, an installation log file is created if you included the /LOG parameter with the installation command. The value should be a full path.

For installation, the log level is set to DEBUG.

The path of the log file for the ongoing activity of the agent is `C:\Program Files\Ping Identity\PingID\Device Trust\logs\PingIdDeviceTrust.log`.

For the ogoing activity of the agent, the level is set to INFO. To raise the log level to DEBUG:

1. Open the Registry Editor.
2. Under HKEY_LOCAL_MACHINE\SOFTWARE\Ping Identity\PingId\DeviceTrust, add a new key of type *Dword32* called *LogLevel*.
3. Set the value of the new key to 1.
4. After making the change to the registry, restart the PingIDESVC service or restart the computer.

   To restore the logging level to INFO, change the value of the key to 0 and restart the PingIDESVC service or the computer.

> **Note**
>
> There is no mechanism to limit the log file size. So it's best not to leave the logging at DEBUG level for an extended period of time.

Log files on Mac

When installing on Mac, two installation log file are created:

- `/tmp/devicetrust.cliinstaller.log`
- `/tmp/devicetrust.install.log`

If an error occurred during installation, run the installation command again but set -LogLevel to 1. The log files will then contain more detailed information that you can use for debugging.

The path of the log file for the ongoing activity of the agent is `/usr/local/pingid/DeviceTrust/logs/PingIdDeviceTrust.log`.

If you encounter issues with the agent and want to raise the logging level of the activity log file to DEBUG, run the command:

```
sudo /usr/local/pingid/DeviceTrust/bin/install -LogLevel=1
```

To restore the logging level to INFO, run the command:

```
sudo /usr/local/pingid/DeviceTrust/bin/install -LogLevel=0
```


Copyright © 2025 Ping Identity Corporation

Custom scripts

When a risk evaluation is carried out using a policy that includes the PingID Device Trust predictor, the API response includes various device identification fields in the object `device.agent`. If you would like to include additional identifying information, you can specify the path of a local script when installing the trust agent on individual computers.

- The script should return a single string.
- In the API response returned for the risk evaluation, the string generated by the script is included as the value for the field `device.agent.customScript.output`.
- On Windows, the script should be a batch file.
- On Mac computers, the script should be a shell script.

The following example is a script that is run in order to pass a computer's third-party-generated ID to the risk evaluation.

```
@echo off
powershell.exe -command "[System.BitConverter]::ToString(((Get-ItemProperty 'HKLM:
\SYSTEM\CurrentControlSet\Services\ThirdPartyAgent\Sim').AG)).ToLower() -replace '-','' | ForEach-Object { Write-Host
-NoNewline $_ }"
exit 0
```

> **Note**
>
> If you are using a custom script, keep in mind that the time it takes for the script to run may affect user experience. You may also have to adjust the length of the agent timeout to prevent situations where the agent ends up returning an empty response.

Examples of risk evaluation response

Sample responses for predictor:

The following is an example response from a risk evaluation where the agent successfully verified the trusted device:

```
"trustedDevice": {
    "reason": "PingID Device trust verified successfully",
    "level": "LOW",
    "type": "DEVICE",
    "status": "TRUST_VERIFIED"
}
```

The following is an example response from a risk evaluation where the agent failed to verify the trusted device (due to factors such as an invalid signature):

Copyright © 2025 Ping Identity Corporation

```
"trustedDevice": {
    "reason": "PingID Device trust verification failed",
    "level": "HIGH",
    "type": "DEVICE",
    "status": "TRUST_VERIFICATION_FAILED"
}
```

The following is an example response from a risk evaluation where the agent was unable to verify the trusted device because the agent was not running or was unable to retrieve the JWT:

```
"trustedDevice": {
    "reason": "Not enough information to verify device trust",
    "level": "HIGH",
    "type": "DEVICE",
    "status": "NOT_AVAILABLE"
}
```

Agent-supplied information under device in risk evaluation API response

```
"device": {
    "agent": {
        "customScript": {
            "exitCode": 5,
            "output": "b90ce386-f74f-473c-bc27-f19b3569b8b5"
        },
        "loggedInUser": {
            "name": "jj",
            "objectSid": "objectSid",
            "domainName": "domainName"
        },
        "macAddress": [
            "0a-23-3b-fa-34-bb",
            "3d-21-fb-12-8b-h5",
            "ak-le-12-07-88-25"
        ],
        "os": {
            "name": "macOS",
            "version": "14.6.1"
        },
        "name": "mac-2CD4BNMD",
        "id": "94970C21-D879-6ACD-E208-99C6ECF9D7EA",
        "version": "0.1.0"
    },
    "os": {
        "name": "Mac OS X"
    },
    "browser": {
        "name": "Chrome"
    },
    "id": "Id-aeb87d04-9f59-4e68-aace-d7b211933a48",
    "estimatedDistance": 0
}
```


Copyright © 2025 Ping Identity Corporation

Strong authentication monitoring and dashboards

You can view dashboards and monitor MFA usage and events.

- View MFA dashboards. Learn more: MFA dashboard.
- Run an audit report. Learn more: Audit

> **Note**
>
> Legacy PingID reports can be viewed in the legacy PingID admin portal. Learn more: PingID reporting

Copyright © 2025 Ping Identity Corporation

Threat Protection using PingOne Protect

PingIdentity.

PingOne Protect helps prevent identity fraud by incorporating advanced features and real-time detection and enables customers to combat bad actors and address both password and multi-factor authentication (MFA) fatigue.

Getting started

- Introduction to PingOne Protect
- Getting started with PingOne Protect
- Start a PingOne trial

Tutorials

- Testing predictors
- Using third-party risk scores with PingOne Protect
- Evaluating staging policy risk data

Integrations and connectors

- PingOne Protect Integration Kit
- PingOne Protect connector
- PingGateway integration

Developer resources

- Get started with PingOne APIs
- PingOne Protect API reference
- PingOne Signals (Protect) SDK

Copyright © 2025 Ping Identity Corporation

Troubleshooting

- Audit logs
- System status

Introduction to PingOne Protect

PingOne Protect is a cloud-based service that applies machine learning and configurable, intelligent security policies to analyze user identity and detect potential threats.

PingOne Protect combines multiple internal and external risk factors to provide a single access point for calculating and retrieving risk scores. Use the user interface to create risk policies and configure the scores of various risk predictors into a single risk score. You can also view data and analytics on high-risk events and get in-depth insights on the authentication behavior of your users.

By implementing risk policies, you can control the authentication flow depending on the risk level. For example, you can force high-risk users to step up to stronger authentication or deny them access while providing a frictionless experience for trusted users.

PingOne Protect leverages the following predictors to learn user behavior and detect anomalies:

- Adversary-in-the-Middle

Copyright © 2025 Ping Identity Corporation

- Anonymous network detection
- Bot detection
- Device (new device and suspicious device)
- Email reputation
- Geovelocity anomaly
- IP reputation
- PingID device trust
- Traffic anomaly
- User-based risk behavior
- User location anomaly
- Velocity (user velocity and IP velocity)

> **Important**
>
> The suspicious device and bot detection predictors are only available if you have a license for PingOne Protect. If you have a PingOne Risk license, contact your account team for more details.

Learn more in PingOne Protect key concepts and the PingOne Protect Datasheet.

Getting started with PingOne Protect

Prevent account takeover, new account fraud, and multi-factor authentication (MFA) and password fatigue with PingOne Protect.

By evaluating multiple attack vectors, assigning risk scores, and providing insights, PingOne Protect triggers mitigation tools to block attacks and allow legitimate users to authenticate easily.

PingOne Protect allows enterprises to:

- Stop account takeover and new account fraud.
- Improve user experience by reducing MFA prompts and going passwordless.
- Create intelligent policies that aggregate multiple predictors and assign a risk score.

You can use PingOne Protect in user access, authentication, authorization, registration, and transaction flows.

The two basic elements used in the risk analysis process are predictors and risk policies:

Predictors

A predictor looks at a single factor, for example, whether or not a user is trying to authenticate from an anonymous network, and yields an estimated risk level. Learn more in Predictors.

Copyright © 2025 Ping Identity Corporation

Risk policy

A risk policy combines a number of individual risk predictors, looks at the risk level estimated for each of the predictors, and then yields an overall risk level of **Low**, **Medium**, or **High**. Learn more in Risk policies.

PingOne creates risk evaluations when a user initiates a flow, and the risk policy determines how the aggregated risk score from the risk evaluation should be translated into a final risk level. Learn more in Risk evaluations.

Threat Protection Dashboard

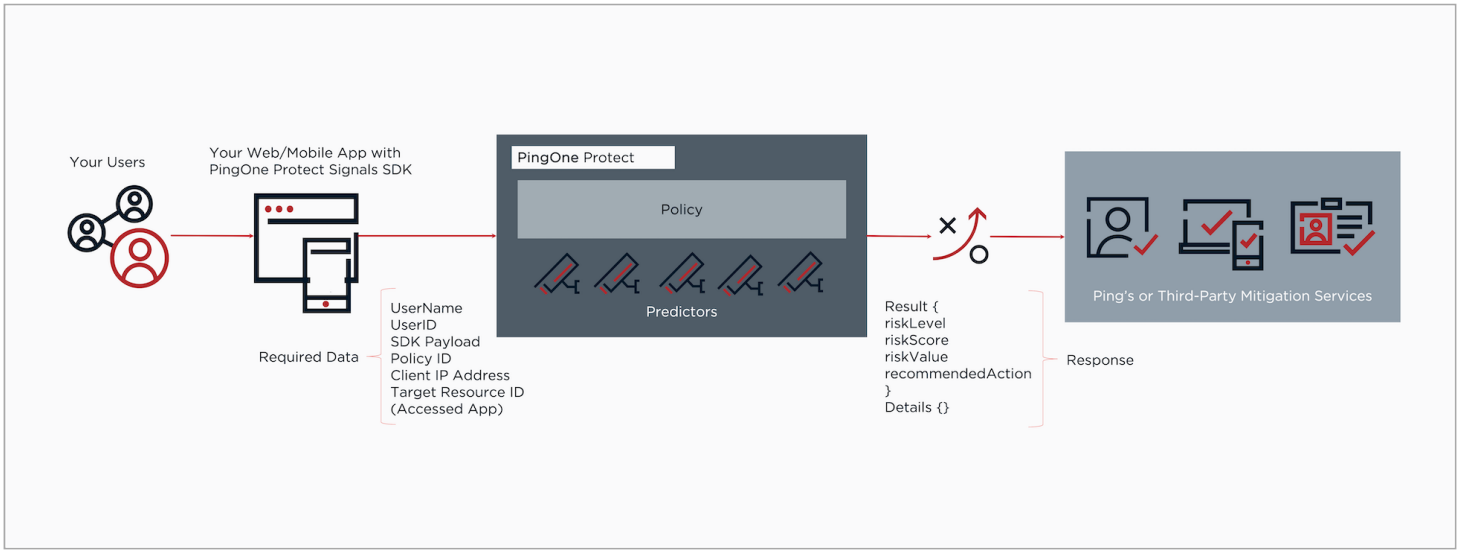
To help you assess how risk evaluations are impacting user flows, PingOne includes the **Threat Protection Dashboard**. The dashboard displays top-level information and includes a number of charts that you can use to get detailed information on specific aspects of the data.

Learn more in Threat Protection Dashboard.

How PingOne Protect works

PingOne Protect dynamically evaluates risk data and calculates a risk level. You can create risk policies to control the response that the end user receives depending on the risk level.

The following diagram shows how PingOne Protect works.



1. The user initiates the flow.

   Possible types of user flows are access, authentication, authorization, registration, or transaction. You can also specify a flow subtype to provide additional detail about the context of the flow, such as if the user performed a password reset or signed on with their username and password. Learn more about flow types and subtypes in the PingOne API documentation.

2. PingOne Protect evaluates risk levels based on various data points, such as network, location, device hardware and settings, behavioral biometrics, and more.

3. The PingOne Protect risk policy calculates the risk based on policy settings.

Copyright © 2025 Ping Identity Corporation

4. PingOne Protect returns a detailed response that includes data about the event, the user and their device, predictor results, and the risk policy result.

   Learn more in Risk evaluations.

   > **Note**
   >
   > You can use the PingOne API to configure and retrieve risk policies and evaluations. Learn more in the PingOne Protect API documentation.

   The policy result can include the following attributes:

   `result.level`

   The response always returns this attribute. Values can be `LOW`, `MEDIUM`, and `HIGH`.

   `result.score`

   The response always returns this attribute and includes the numeric score that the policy calculates. The score determines the risk level based on the policy threshold.

   `result.recommendedAction`

   The response might return this attribute based on the attack vector. This attribute enhances the risk level attribute and provides information on how the user flow should continue. Possible values are:

   - `BOT_MITIGATION`: You should take steps to handle a scenario where a bot is involved.
   - `AITM_MITIGATION`: You should take steps to mitigate the damage from an Adversary-in-the-Middle (AitM) attack. For an AitM attack, the user's credentials have been intercepted, so in addition to blocking the access request, you should lock the user's account until the password is changed.
   - `TEMP_EMAIL_MITIGATION`: The user has specified a disposable email address, which is an indication of a fraud attempt.
   - `DENY`: When a risk level of `HIGH` is calculated for a traffic anomaly predictor, you should deny access because the repeated risk evaluations are likely a sign of a brute force attack.

   `result.value`

   The response might return this attribute. `result.value` is free text that you can add to a policy override. Override rules are not necessary in most cases, but you can use them in scenarios that require blocking a user (for example, known IPs that you want to block).

   Learn more about policy overrides in Risk policies.

   You can find a full response example in PingOne Protect API documentation.

5. The risk policy makes a decision based on the response, and the user flow continues based on the decision.

Key concepts

To fully leverage the capabilities of PingOne Protect, familiarize yourself with the following key concepts:

- Introduction to risk policies

Copyright © 2025 Ping Identity Corporation

- Introduction to predictors
- Introduction to risk evaluations
- Introduction to using the PingOne API for risk evaluations

Introduction to risk policies

The risk policy looks at the risk level estimated for each of the predictors and then yields an overall risk level of **Low**, **Medium**, or **High**. When you define a user journey with the tools provided by Ping Identity, you decide which of your defined risk policies you would like to associate with that flow. For some situations, you might need to use a stricter risk policy, while for others, you might use a more lenient risk policy.

The default risk policy

When you add the PingOne Protect service to a PingOne environment, it includes a default risk policy. This is the recommended policy for your initial testing of risk evaluations.

The default risk policy has the following characteristics:

- It uses the **Scores** approach, which gives you a higher degree of control than the **Weights** approach.

  > **Important**
  >
  > **Weights** in risk policies have been deprecated for new PingOne environments but can still be used in existing environments.

- It includes all of the out-of-the-box predictors.
- It assigns a score of 50 for **High** risk for some of the predictors and a score of 75 for **High** risk for the remaining predictors. This is based on the premise that the IP-related predictors are less indicative of risky situations than the other predictors.

The risk level for each predictor type is calculated separately. Most predictor types require training and learn from successful events. You can also configure a fallback value for most predictor types to use if there is insufficient information to calculate a risk level.

Learn more in Predictors.

You can also create custom predictors that leverage external or processed data. Learn more in Adding custom predictors.

Staging policies

Staging policies allow you to fine tune and test risk policy changes before releasing changes to your production policy and does not affect your end users until you promote a staging policy to production.

Learn more in Creating and managing staging policies.

Custom risk policies

> **Important**
>
> Customize risk policies only after you've accumulated sufficient authentication data and analyzed it.

Use the **Risk Policies** page in PingOne to modify the default risk policy or create additional risk policies of your own. Learn more in Risk policies.

Copyright © 2025 Ping Identity Corporation

Introduction to predictors

Predictors are the basic building blocks that form risk policies. A predictor looks at a single factor, such as whether or not a user is trying to authenticate from an anonymous network. Each predictor yields an estimated risk level. For some predictors, the levels are **Low** and **High**. For other predictors, the levels are **Low**, **Medium**, and **High**.

PingOne Protect leverages the following risk predictors to learn user behavior and detect anomalies:

Predictor	Description
Adversary-in-the-Middle (AitM)	Checks the domain name that the user is trying to access in order to identify AitM attacks.
Anonymous network detection	Analyzes IP address data from a user's device to determine if the address is originating from any type of anonymous network, such as unknown VPNs, Tor, or proxies to mask the IP address.
Bot detection	Leverages advanced analysis of mouse, keyboard, touch, and mobile sensors, as well as device attributes, to detect non-human behavior, automated frameworks, recorders, and more.
Email reputation	Detects the use of disposable email addresses during registration.
Geovelocity anomaly	Analyzes location data to calculate if travel time between two session locations is physically possible.
IP reputation	Analyzes data from different intelligence sources to determine the probability an IP address is associated with malicious activity and to request stronger authentication to verify the user's identity.
IP velocity	Tracks the number of distinct IPs used per user.
New device	Takes into account the risk associated with users trying to access applications from unknown devices or devices that have not been used for sign-on in the recent past.
PingID device trust	Establishes device trust by collecting device information through the PingID device trust agent installed on an organization's workstations.
Suspicious device	Scrutinizes browser, operating system, and hardware attributes to identify suspicious settings or inconsistencies between these attributes collected from the device.
Traffic anomaly	Monitors users, devices, and sessions to detect traffic anomalies, such as a large number of risk evaluations requested for a single user within a short period of time or a large number of users per device during a given time period.
User-based risk behavior	Compares a transaction with the typical behavior of that specific user.
User location anomaly	Detects a user's sign-on location and checks it against previously saved authentication locations.

Copyright © 2025 Ping Identity Corporation

Predictor	Description
User velocity	Tracks the number of distinct users per IP.

Learn more about each predictor in Predictors.

Important

The PingOne Risk license allows you to use the following predictors in your risk policies. The remaining predictors require a PingOne Protect license.

- Anonymous network detection
- Geovelocity anomaly
- IP reputation
- IP velocity
- New device
- User-based risk behavior
- User location anomaly
- User velocity

To upgrade your license to PingOne Protect and gain access to the additional predictors, contact your account team for more details.

The risk level for each predictor type is calculated separately. Most predictor types require training and learn from successful events. You can configure a fallback value for most predictor types to use if there is insufficient information to calculate a risk level.

You can also create custom predictors that leverage external or processed data. Learn more in Customizing predictors.

Introduction to risk evaluations

Risk evaluations calculate the risk level and other risk-related details associated with an event. The PingOne Protect risk policy then calculates the risk based on policy settings and returns a detailed response that includes data about the event, the user and their device, predictor results, and the risk policy result. You can view the results from risk evaluations to see how your risk policy is performing.

Learn more about risk evaluations and how to use them in:

- Risk evaluations
- Updating completion status for risk evaluations
- Providing feedback for risk evaluations
- Reviewing risk evaluations

Introduction to using the PingOne API for risk evaluations

You can use the PingOne API to:

- Create and manage risk predictors
- Create and manage risk policies

Copyright © 2025 Ping Identity Corporation

- Create risk evaluations
- Update the completion status of risk evaluations to improve the accuracy of future risk evaluations

Learn more in the PingOne Protect section of the PingOne API documentation.

Trying PingOne Protect with a sample app

Before you begin

Sign up for a PingOne trial. Learn more in Starting a PingOne trial.

About this task

Signing up for a PingOne trial is a great way to experience the functionality of PingOne Protect with an automatically generated sample application. This sample app is a Ping-maintained application that allows you to design registration and sign-on experiences for your customers and test them in the app.

With your PingOne trial, you can try PingOne Protect and quickly and easily simulate risk events with the sample app to test how predictors work. The sample app allows you to test the capabilities of PingOne Protect in addition to other PingOne services, such as PingOne MFA and PingOne SSO, and can be tailored to your industry.

> **Note**
>
> Learn more about trying PingOne Protect in your existing PingOne user journey instead of with a trial in Getting up and running.

To try PingOne Protect with a sample app:

Steps

1. In the PingOne admin console, click **Add Environment**.
2. Select **Customer solution**, and click **Next**.

   > **Note**
   >
   > When you create a **Customer solution**, your new environment automatically includes the PingOne Protect service.

3. Click **Next** again to create the environment.
4. Enter the details for your environment, select the **Include a solution designer to easily design and test experiences** check box, and click **Finish**.

   Result:

   Your new PingOne environment is created and automatically opens.

5. Choose if you want to tailor your experience for your industry, or click **Skip**.

   Result:

   PingOne creates a sample app based on your selection. You can click **Get Started** to view the tour or close the tour pop-up window.

Copyright © 2025 Ping Identity Corporation

6. Test the predictors.

> **Note**
>
> The PingOne Protect capabilities are available in the **Authentication** flow of the sample app.

Getting up and running

Follow these steps to start using PingOne Protect as part of your user journeys.

While PingOne Protect provides many ways to customize predictors and to combine them in a risk policy, it also provides out-of-the-box predictors and a default risk policy that combines these predictors.

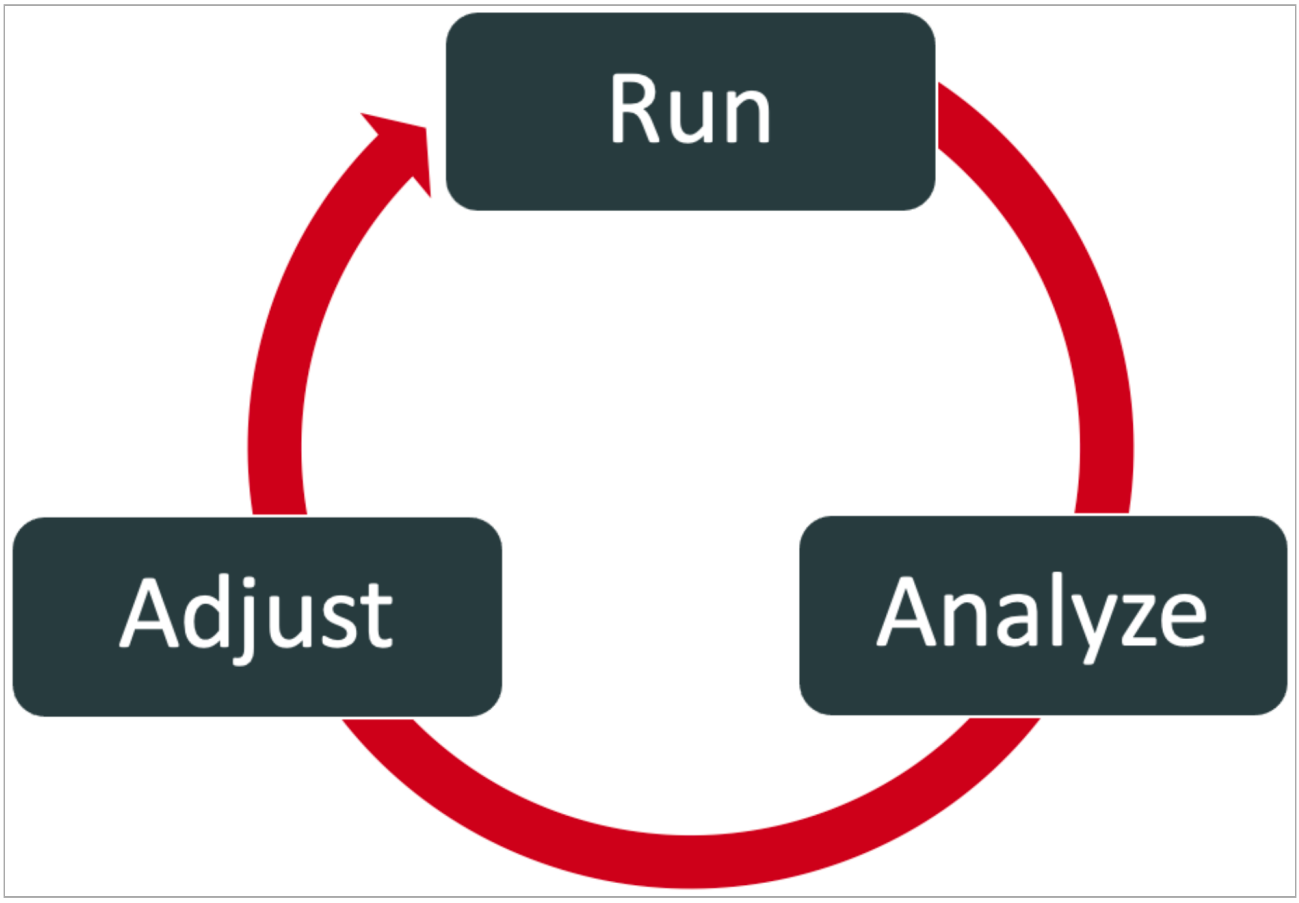
When you first start with PingOne Protect, the best approach is to use the default risk policy that is provided. After you've seen how this default policy affects the flow experience for your users, you can go back and fine-tune it by customizing individual predictors or creating multiple risk policies.

Because you'll use the default risk policy, your only task at the beginning is the integration of PingOne Protect with your user journey.

The main steps required to start using PingOne Protect are:

1. Integrate PingOne Protect into a user journey.
2. Configure the PingOne Signals (Protect) SDK.
3. Run and analyze your predictors:
    1. Run PingOne Protect to train the predictor models.
    2. Use the PingOne Protect dashboard to analyze the results.
    3. Adjust the scores for the predictors in the risk policy.

Copyright © 2025 Ping Identity Corporation



4. Repeat step 3 as needed.

Adding the PingOne Protect service to your environment

To get started, add the PingOne Protect service to your PingOne environment.

Before you begin

- If you don't have a PingOne account yet, start a PingOne trial.
- Make sure that you can sign on to the PingOne admin console.
- Add an environment to organize your services.
- Make sure that you have the Environment Admin and Identity Data Admin roles in your PingOne environment. Learn more in Managing user roles.

About this task

To add PingOne Protect to your environment:

Steps

1. In your PingOne environment, go to **Overview**.
2. Next to **Services**, click the **+** icon.
3. Click **+ Add** to add the **PingOne Protect** service.

Copyright © 2025 Ping Identity Corporation

4. In the **Add a Service** window, click **Finish**.

Result

PingOne Protect is displayed in the sidebar.

Integrating PingOne Protect with user journeys

After you add PingOne Protect to your environment, integrate PingOne Protect into a user journey.

Before you begin

You'll need a PingOne account with at least one environment that includes the PingOne Protect service. Learn more in Add an environment.

About this task

You can integrate your risk policy into a user journey in one of the following ways:

- Using the integration with PingFederate
- Building a custom flow with PingOne DaVinci
- Using the PingOne API
- Integrating with PingOne Advanced Identity Cloud

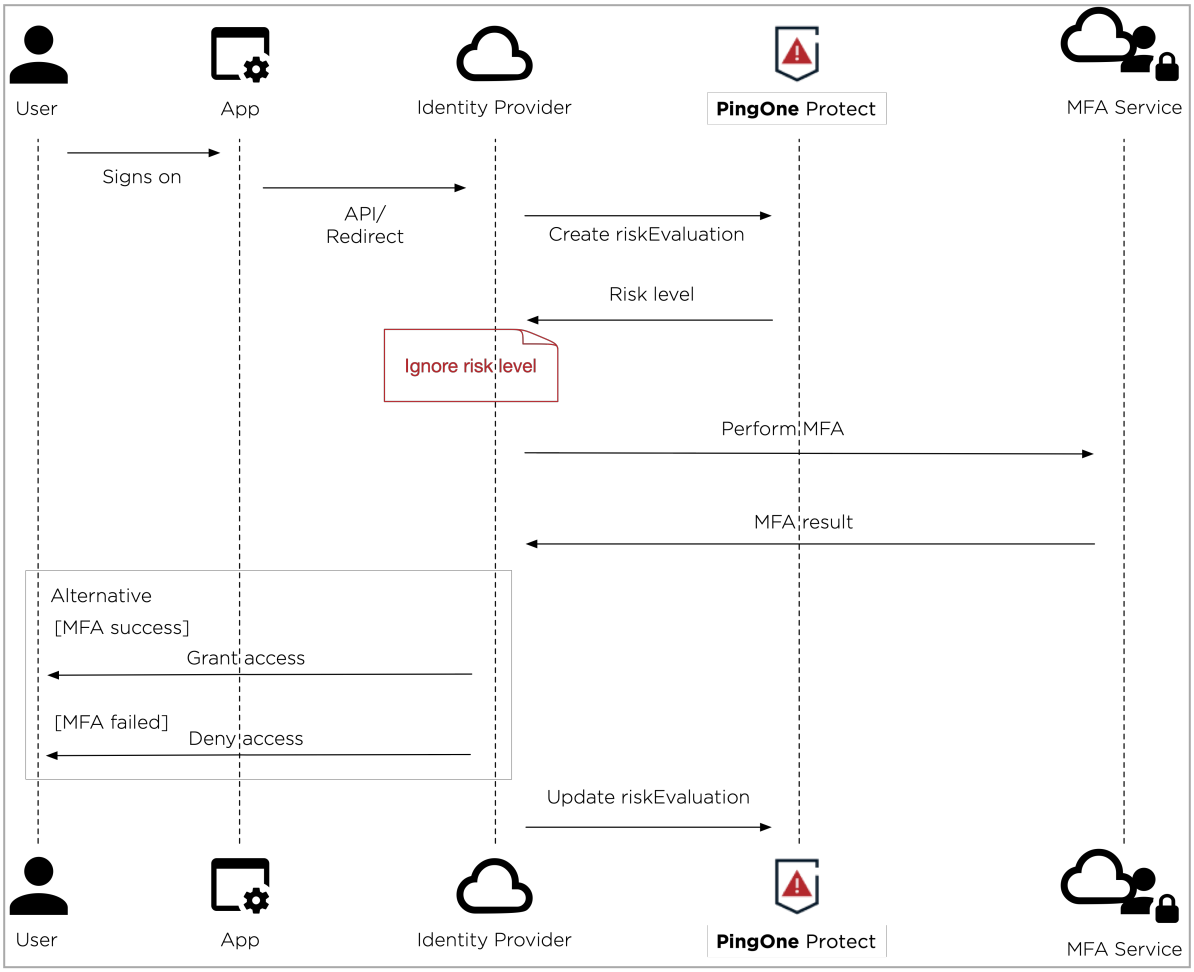
Regardless of the integration approach you use, the high-level steps are the same. The steps below use an authentication flow as an example for integration, but you can also use other user journeys, such as registration and authorization:

Steps

1. Integrate into an authentication flow.

   The following diagram shows a high-level overview of PingOne Protect integrated in silent mode into an example authentication flow.

Copyright © 2025 Ping Identity Corporation



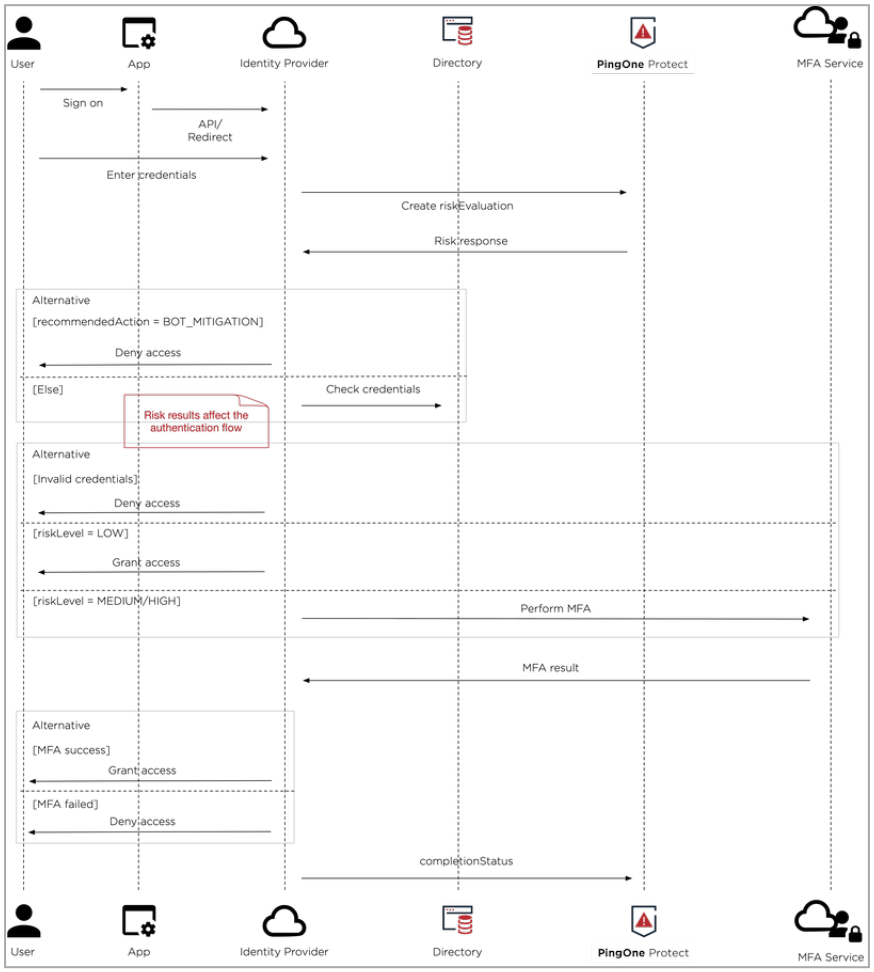
2. Send transaction feedback.
3. Configure a risk policy.

   The simplest approach is to use the default risk policy. You can also edit the default risk policy.

4. Add risk evaluation to your authentication flow.

   The following diagram shows an example of PingOne Protect integrated into an authentication flow with risk levels affecting the flow.

Copyright © 2025 Ping Identity Corporation



Copyright © 2025 Ping Identity Corporation

PingFederate

Using the PingOne Protect Integration Kit with PingFederate
Before you begin

Before proceeding, make sure PingFederate is installed. Learn more in Installing PingFederate.

Steps

1. Deploy the files for the type of integration kit you're using to your PingFederate directory:

   Choose from:

   - PingOne Protect Integration Kit
   - PingOne Risk Integration Kit

   > **Note**
   > The PingOne Protect Integration Kit 1.0 works with PingFederate 11.3 and later. The PingOne Risk Integration Kit will continue to support PingFederate versions 10.2 and later.

2. To allow PingFederate to communicate with PingOne, create a connection between PingOne and PingFederate.
3. To configure the integration kit, follow the steps in the documentation for the integration type that you selected in step 1.

Copyright © 2025 Ping Identity Corporation

DaVinci

Building a custom flow with PingOne DaVinci
Before you begin

Add PingOne DaVinci to your PingOne environment. Learn more in Adding an environment.

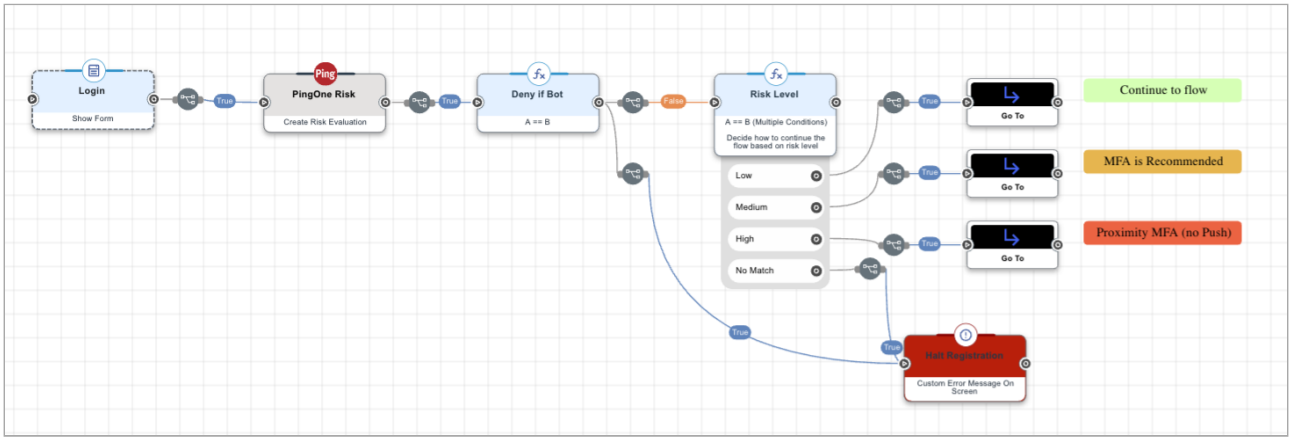
About this task

PingOne DaVinci is the graphic orchestration tool used for designing flows, such as user registration and authentication flows. Learn more about using PingOne DaVinci in the DaVinci documentation.

You can use the PingOne Protect connector to define different paths in an user journey flow, based on the result of a risk evaluation.

For example, you can use a risk evaluation connector before a MFA step, and then define different paths based on the risk score calculated:

- Skip the MFA challenge if low risk.
- Use a specific authentication method if user behavior data suggests medium or high risk.
- Block access completely in a high-risk situation, such as when the recommended action is equal to bot mitigation.



For examples of using the PingOne Protect connector in different types of flows, see the following templates in the Flow Library:

- PingOne - Sign On and Adaptive MFA
- PingID - MFA flow + Protect
- PingID - FIDO2 Passwordless + Protect

To use Protect connectors in a flow:

Steps

1. After you have added DaVinci to your PingOne environment, ensure any risk connectors you add to your flows already have been configured with the correct information for environment ID, client ID, and client secret.

   If you import a flow from a different PingOne environment, you must go to the settings for the Protect connector and update this information to reflect the environment where you're adding the flow.

Copyright © 2025 Ping Identity Corporation

2. Add two different Protect connectors to your flow by following the documentation for the PingOne Protect connector:

    1. Add a Protect connector with the Create Risk Evaluation capability.

       The response returns a final risk evaluation result - `High`, `Medium`, or `Low`. The Protect connector with the `Create Risk Evaluation` capability should be added at a point in the flow where you would like to base the next action on the risk score assigned, for example, show an MFA prompt for Medium or High, but automatically grant access if the risk is deemed Low.

    2. Add risk evaluation feedback to the flow by adding a Protect connector with the Update Risk Evaluation capability.

       This step is included after authentication has been completed, and it consists of sending an update with the final state of the transaction, such as `SUCCESS` or `FAIL`. The Update Risk Evaluation capability represents the system's ability to learn over time in order to improve results. You should always include an update connector in your flow because this step is essential for improving the accuracy of the machine learning models.

       > **Note**
       >
       > Flows may take users on different paths. Make sure to include a Protect connector with the Update Risk Evaluation capability at the end of each possible path.

Troubleshooting

If you are having issues with the PingOne Protect Connector, try the following:

- For each connector in the flow, make sure that all of the mandatory inputs have been provided.
- If you are using the `skrisk` component to include the data provided by the PingOne Signals (Protect) SDK, make sure that you have carried out the necessary steps.
- Use the Analytics feature to see where the flow stopped.
- Select the **Options** icon, and turn on **Show Node ID**. This will make it easier to identify the source of inputs and outputs.

Copyright © 2025 Ping Identity Corporation

API

Using the PingOne API
About this task

To integrate using the PingOne API:

Steps

1. Create a worker application and get an access token.

   Learn more in Adding an application and Getting an access token.

2. Add risk evaluation to your user flow.

   Learn more in the section on risk evaluation in the API reference.

   The response returns a final risk evaluation result of `High`, `Medium`, or `Low`.

3. Add risk evaluation feedback to the flow.

   This step is included after authentication has been completed, and it consists of sending an update with the final state of the transaction, such as `SUCCESS` or `FAIL`. This step is essential for improving the accuracy of the machine learning models. Learn more in PUT UPDATE Risk Evaluation in the API reference.

4. Modify the default risk policy or create one of your own risk policy set with the API.

Copyright © 2025 Ping Identity Corporation

PingOne Advanced Identity Cloud

Integrating with PingOne Advanced Identity Cloud
Before you begin

Make sure you have:

- A PingOne Advanced Identity Cloud administrator account
- A PingOne account

  Learn more in Starting a PingOne trial.
- The client ID and client secret for a PingOne environment
- A risk policy configured in PingOne (or use the default risk policy)
- A worker application with the Identity Data admin role assigned in PingOne

About this task

Advanced Identity Cloud is a comprehensive identity and access management (IAM) service that lets you deploy applications anywhere: on-premises, in your own private cloud, or in your choice of public cloud. With Advanced Identity Cloud, you can manage user journeys and take advantage of the PingOne Protect threat protection features by integrating the three PingOne Protect nodes into your journey.

Steps

1. Configure the PingOne Service in Advanced Identity Cloud.
2. Set up your user journey in Advanced Identity Cloud with the three PingOne Protect nodes in the journey:
   1. The PingOne Protect Initialize node to initialize the PingOne Protect Web SDK on the client device.
   2. The PingOne Protect Evaluation node to calculate the risk level and other risk-related details associated with an event.
   3. The PingOne Protect Result node to update the risk evaluation configuration or modify the completion status of the resource when the risk evaluation is still in progress.
3. Validate that the PingOne Protect Evaluation node is working by checking the PingOne **Audit** log for **Risk Evaluation Created** events.

Getting input from the PingOne Signals (Protect) SDK

Certain risk predictors, such as the **New Device** predictor, rely on supplemental risk-related information that is supplied by the PingOne Signals (Protect) SDK.

About this task

The default risk policy includes predictors that are dependent upon this input. To get reliable risk evaluations right from the start, you must carry out the steps to include the required code in your applications and include the information from the Signals SDK in your user journeys.

Copyright © 2025 Ping Identity Corporation

Steps

1. Add the required Signals SDK code into your web applications, Android applications, and iOS applications.

   Choose from:

   - PingOne Signals (Protect) SDK for Web
   - PingOne Signals (Protect) SDK for Android
   - PingOne Signals (Protect) SDK for iOS

2. Include the information from the Signals SDK in your flows using one of the following methods:

   Choose from:

   - PingOne Protect Integration Kit for PingFederate: Integrate device profiling with one of following:
     - PingOne Risk Integration Kit
     - PingOne Protect Integration Kit
   - PingOne Protect API: Create risk evaluations.
   - PingOne DaVinci: Include the PingOne Protect connector as part of a user flow.

Using third-party risk scores with PingOne Protect

The best threat protection often means leveraging multiple risk and fraud services. PingOne Protect allows administrators to send third-party data and other risk signal vendor scores, for example sending information from PingFederate whether a device is managed and not.

There are three steps to ingesting third-party risk data into PingOne Protect:

1. Send the third-party data to PingOne Protect by creating custom attributes to map the values to.
2. Validate that PingOne Protect received the third-party data.
3. Configure a custom predictor using the custom attributes.

   Custom predictors allow you to plug in external data sources and reference custom attributes. You can use custom predictors to determine a risk score for unmanaged devices or map third-party risk scores to high, medium, or low. You can also add custom predictors to risk policies, apply overrides, and view analytics in the dashboards.

Sending third-party data to PingOne Protect

PingOne Protect cannot invoke a third-party API directly, so the external data must be sent into the evaluation call from another service, and the values need to be mapped into custom attributes.

Depending on your identity service providers, there are multiple ways to send third-party data to PingOne Protect:

PingOne DaVinci

The most straightforward approach is using PingOne DaVinci to retrieve a third-party data feed and pass the response back into PingOne Protect. Use purpose-built PingOne DaVinci connectors to get risk evaluations from vendors such as Castle, LexisNexis, or Securonix. You can also configure a generic REST call to get risk information from other vendors.

Copyright © 2025 Ping Identity Corporation

Learn more in:

- PingOne Protect connector
- Setting up custom attributes
- Example connectors:
  - Castle connector
  - LexisNexis connector
  - Securonix connector
  - PingOne DaVinci HTTP connector (generic API call)

PingFederate

Use PingFederate integration kits to retrieve third-party data in combination with the PingOne Protect Integration Kit to configure custom attributes to map the data into PingOne Protect.

Learn more in:

- PingOne Protect Integration Kit
- Setting up custom attributes
- Example integration kits:
  - ID DataWeb Integration Kit
  - iovation Integration Kit
  - ThreatMetrix Integration Kit
  - Mobile device management (MDM) integration kits:
    - Intune Integration Kit
    - MobileIron Integration Kit
    - Workspace ONE UEM Integration Kit (formerly known as AirWatch)

PingOne API

Use the PingOne API to retrieve risk evaluations from third-party risk providers. You can add custom attributes to `event` objects by adding the attribute to the `event` object in the body of a risk evaluation request. Learn more in Risk evaluations.

PingOne Authorize

Use PingOne Authorize to call PingOne Protect for risk evaluations as part of a PingOne authorization policy. For more information, see Connecting to PingOne Protect.

Copyright © 2025 Ping Identity Corporation

Validating received third-party data in PingOne Protect

After you send the third-party data to PingOne Protect, validate that the data was received either using the PingOne admin console or the API:

- PingOne admin console: To view a risk evaluation, follow the steps in Reviewing risk evaluations.
- PingOne API: Create a risk evaluation and review the response. Learn more in the PingOne Protect API documentation.

> **Note**
> In a risk evaluation, the custom attributes appear in the `event {…}` section near the end of the JSON in a risk evaluation.

Configuring custom predictors using custom attributes

After sending third-party data and validating that it was received in PingOne, configure custom predictors that use the custom attributes that you previously created:

- PingOne admin console: Learn more in Adding custom predictors.
- PingOne API: Learn more in Custom risk predictors.

Running, analyzing, and adjusting your risk policy

To make informed decisions about how to fine-tune risk predictors and policies, you'll have to accumulate a certain amount of data on authentication attempts and how the risk evaluation impacts them.

About this task

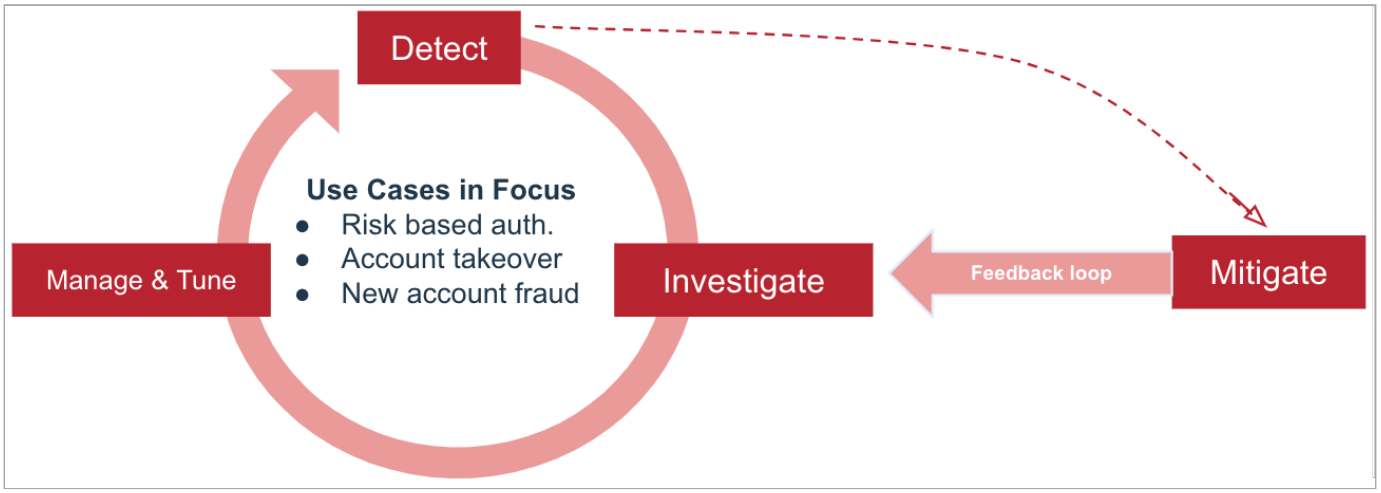
You should use the default risk policy for the initial period before you start customizing the policy or defining multiple risk policies.

Fine-tuning your policy is an iterative process and should follow this approach:

Steps

1. Train the risk models with production data for 1-3 weeks for workforce usage or 2-4 weeks for customer usage. This should be done with the default risk policy.
2. Use the **Threat Protection Dashboard** to analyze the results. Identify false positive results, meaning situations that are identified as **High** risk even though they are legitimate users. Check what is causing these false positives.
3. Adjust the scores for the different risk predictors in the risk policy to see if you can reduce the incidence of false positives.

Copyright © 2025 Ping Identity Corporation



Next steps

After you've familiarized yourself with how PingOne Protect works and have it running, refer to the following for next steps to deepen your understanding:

- To learn more about how the predictors work, you can test predictors by simulating risk events in a sample application.
- Learn more about customizing predictors that leverage external or processed data in Custom predictors and Adding custom predictors.
- Learn more about building and customizing your own risk policies in Risk policies.
- To test and fine-tune risk policy changes before promoting them into production, you can create a staging policy and view how your changes impact your users. Learn more in Evaluating staging policy risk data.

Risk policies

Risk policies determine how the various risk predictors are combined, and how the aggregated risk score should be translated into a final risk level of low, medium, or high.

You can modify the default risk policy or create additional custom risk policies of your own. After you have defined risk policies, you can use them as part of the integration with PingFederate, part of a flow designed with PingOne DaVinci, or part of a user journey built with the PingOne API.

Build risk policies on the **Risk Policies** page, which you can access from the **Threat Protection** menu.

When you build and customize a risk policy, you make decisions about the following:

- Which predictor types should be included when calculating the overall risk?

  When you create a new risk policy, it includes the following subset of the predictor types that PingOne supports:

  - Anonymous network detection
  - Geovelocity anomaly
  - IP reputation

Copyright © 2025 Ping Identity Corporation

- IP velocity
- New device
- User velocity
- User-based risk behavior
- User location anomaly

The scores assigned to the various predictors in the default risk policy are not uniform. The risk predictors that are not related to the detected IP are given a higher score because they are a better indication of serious risk.

You can also create custom risk predictors that analyze data that you provide. Learn more in Adding custom predictors.

> **Note**
>
> The default risk policy includes a **New Device** predictor. To have this predictor included in the actual risk evaluation, your authentication flow must provide information that can be used to identify individual devices. The best way to do this is to bring the information from the PingOne Signals (Protect) SDK. Having the predictor included in the risk evaluation can also be done by providing a persistent cookie as input.

- For each predictor type included, do you want to use the default predictor or one that you have customized?

  Customize predictors on the **Predictors** page.

- What method do you want to use to adjust the degree that each included predictor should be taken into account when calculating the overall risk score?

  There are two methods of combining the predictors (controlled with the switch at the top of the page):

Weights

Determines the relative weights that should be used when calculating the individual risk score for each predictor.

> **Important**
>
> **Weights** in risk policies have been deprecated for new PingOne environments but can still be used in existing environments.

Scores

Exercises more control over the overall calculation because you can specify an exact numerical score that should be assigned when PingOne Protect determines that there is a medium or high-risk level for a predictor.

- What specific weight or score should be assigned to each predictor included in the policy?

  This is relevant for both the weights and scores approaches, although the UI differs slightly between them.

- How should the aggregated risk score that was calculated be translated into a final risk level?

  Controls are provided on the **Risk Policies** page to map the aggregated risk score to the three categories that represent the final result of the risk analysis: low, medium, and high.

- Do you want to use overrides?

Copyright © 2025 Ping Identity Corporation

You can define overrides that assign a specific final risk level (low, medium, or high) based on a specific criterion, regardless of what the overall calculated risk score was. For example, you can define an override that states that if a geovelocity anomaly is detected, the final risk evaluation should be **High**, regardless of what the overall risk calculation score is.

> **Note**
>
> If you enter text in the **Note** field for overrides, the text is returned in the API response.

Best practices for risk policies

When you are first starting out with risk policies, it is recommended that you take advantage of the Risk Policy Assistant, which generates risk policies that match your organization's needs. On the basis of your responses to a number of basic questions, the assistant creates a new policy and assigns different scores to the various predictors to maximize the accuracy of your risk evaluations. To launch the Risk Policy Assistant, click the **Assistant** button.

Creating and managing staging policies

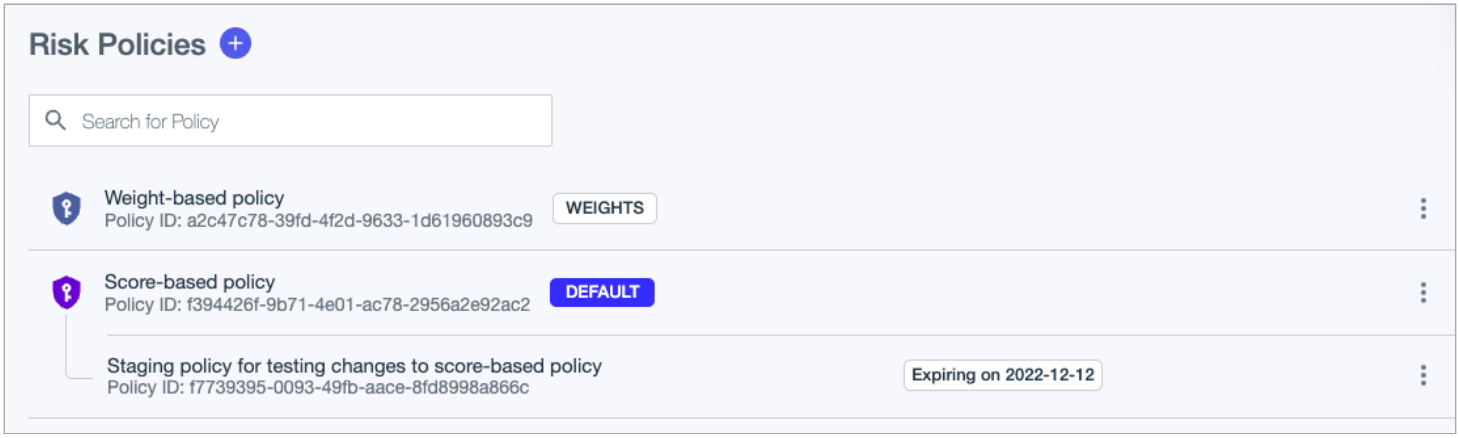
To test risk policy changes before putting them into production, you can create a staging policy that is associated with the risk policy that you're currently using.

About this task

When an evaluation event occurs for the production risk policy, the incoming risk data is also passed through the staging policy affiliated with the production policy, creating two sets of risk evaluation data: one for the production policy and one for its associated staging policy.

Staging policies are set to expire after 3 months, and the expiration date is displayed next to the risk policy name.

When a staging policy expires, incoming risk data is no longer passed through the staging policy for evaluation.



In the PingOne admin console, go to **Threat Protection** > **Risk Policies**:

Copyright © 2025 Ping Identity Corporation

Steps

- To create a staging policy, click the **More Options** (⋮) icon for the policy and select **Create staging policy**.

  Result:

  A policy editing window opens, and you can make the changes that you want to test.

- To promote the staging policy to production, click the **More Options** (⋮) icon for the policy, and select **Promote to production**.

  Result:

  When you promote a staging policy to production:

  - The settings in the staging policy are copied to production and replace the production policy settings. The policy name and ID remain the same.
  - The staging policy is deleted from the **Risk Policies** list.

  > **Note**
  > A staging policy can be promoted to production even if it has expired.

- To delete a staging policy, click the **More Options** (⋮) icon and select **Delete**.

Evaluating staging policy risk data

To test risk policy changes before actually putting them into production, you can create a staging policy that is associated with the risk policy that you are currently using.

Before you begin

Create a staging policy.

About this task

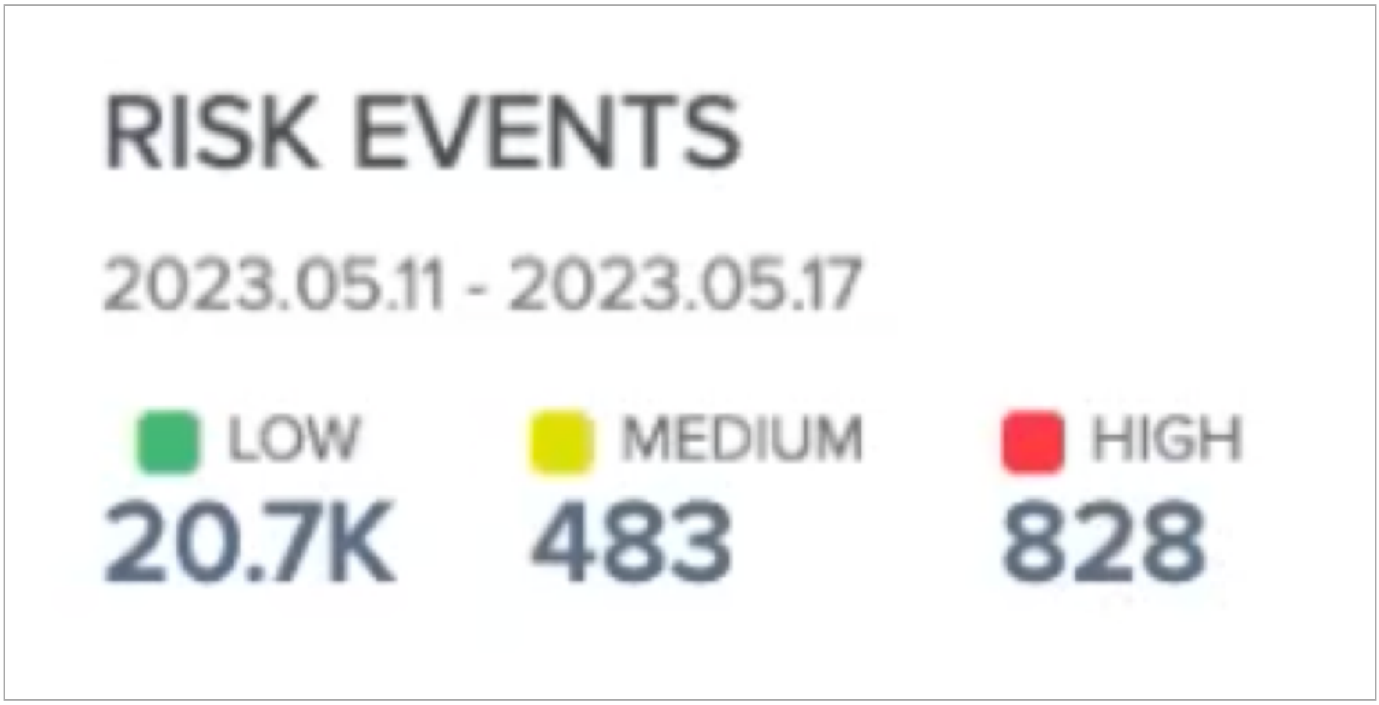
After creating your staging policy, you can view the risk data to determine how your policy changes affect end users.

To view risk data from a staging policy in the **Threat Protection Dashboard**:

Steps

1. Go to **Monitoring > Threat Protection**.
2. Click the **Risk Events** graph.
3. Review the total counts above the default graph, which shows only production event types.

Copyright © 2025 Ping Identity Corporation



4. Click the **Event Types** dropdown, and select both the **Production** and **Staging** checkboxes.

   Result:

   The graph refreshes to display risk event data from both production and staging risk policies.

5. Review the updated total counts to see how your staging policy affects each risk level.

6. Review the data in the drill-down table.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Only events that have triggered a specific risk predictor, such as geovelocity anomaly, or have an aggregated risk score of HIGH are shown.

1. Take note of the **Risk Policy** column to determine whether each risk event is associated with the production or staging policy. Check risk events specifically from the staging policy and review how the changes you made affect the data.

TIME	RISK POLICY	USER	RISK LEVEL	RISK SCORE	RISK LEVEL SOURCE	IP	COUNTRY	TARGET APPLICATION	USER AGENT
2023-05-17 15:41:21	Staging Corp Policy - Sc...		HIGH	80	AGGREGATED_SCORES		United States	Salesforce	Mozilla/5.0 (Macintosh; I...
2023-05-17 15:40:13	Corp Policy - Scoring	johndoe	HIGH	80	AGGREGATED_SCORES		United States	Salesforce	
2023-05-17 15:40:13	Staging Corp Policy - Sc...	johndoe	HIGH	80	AGGREGATED_SCORES		United States	Salesforce	
2023-05-17 15:30:34	Staging Corp Policy - Sc...		HIGH	120	AGGREGATED_SCORES		United States	Slack	Mozilla/5.0 (Macintosh; I...
2023-05-17 15:28:00	Staging Corp Policy - Sc...		HIGH	80	AGGREGATED_SCORES		United States	Gitlab	Mozilla/5.0 (Macintosh; I...
2023-05-17 14:57:42	Staging Corp Policy - Sc...		HIGH	80	AGGREGATED_SCORES		Canada	Salesforce	Mozilla/5.0 (iPhone; CP...

1. Scroll across to the **Predictors** column, and click **Details** in any risk event row to review the score for each configured predictor and the reason.

   Example:

   If you added the **New Device** predictor in your staging policy and do not use this predictor in your production policy, a risk event is triggered only in the staging policy when a user signs on with a new device. In the **Predictors Details** for this risk event, the **New Device** predictor shows a **High** score because the device has not been used recently. This allows you to test how your changes to the staging policy might affect users with real-time risk data passed from the production policy.

Next steps

Copyright © 2025 Ping Identity Corporation

Make any further adjustments to your staging policy if needed. After evaluating your staging policy, you can decide whether to promote the staging policy to production.

Predictors

When you add the PingOne Protect service to a PingOne environment, the environment includes one predictor of each basic type that's supported. For example, you could have one anonymous network predictor and one IP reputation predictor. The default name of the predictor is the name of the category.

PingOne Protect leverages the following risk predictors to learn user behavior and detect anomalies:

- Adversary-in-the-Middle (AitM)
- Anonymous network detection
- Bot detection
- Email reputation
- Geovelocity anomaly
- IP reputation
- IP velocity
- New device
- PingID device trust
- Suspicious device
- Traffic anomaly
- User-based risk behavior
- User location anomaly
- User velocity

You can also customize the default predictors and supplement the default predictors with predictors of your own using custom and composite predictors.

Learn more about how the predictors work in Testing predictors.

Copyright © 2025 Ping Identity Corporation

Important

The PingOne Risk license allows you to use the following predictors in your risk policies. The remaining predictors require a PingOne Protect license.

- Anonymous network detection
- Geovelocity anomaly
- IP reputation
- IP velocity
- New device
- User-based risk behavior
- User location anomaly
- User velocity

To upgrade your license to PingOne Protect and gain access to the additional predictors, contact your account team for more details.

Adversary-in-the-Middle (AitM)

Adversary-in-the-Middle (AitM) is a variant of Man-in-the-Middle attacks. In AitM, a malicious actor uses a reverse proxy to position themselves between a user and an online service to obtain user credentials and session tokens. This type of attack circumvents the protection provided by one-time passcode (OTP)-based multi-factor authentication (MFA) and is a common technique in phishing attempts.

The predictor checks the domain name that the user is trying to access in order to identify AitM attacks.

When the risk evaluation result indicates an AitM attack, you should both block the attempt to access the resource and lock the user account because the malicious actors have obtained the user's credentials. The account should be unlocked only after the user password has been changed.

Note

The PingOne Signals (Protect) SDK is required for the AitM predictor.

Anonymous network detection

Malicious actors typically use anonymous networks, such as unknown VPNs, Tor, and proxies, to mask their IP address. PingOne Protect analyzes IP address data from a user's device to determine if the address originates from any type of anonymous network. If so, the user can be prompted for step-up authentication or denied access.

You can configure a fallback value for this predictor type to use if there's insufficient information to calculate a risk level. PingOne Protect also supports creating an allow list of networks, ensuring that legitimate VPN users can access authorized resources.

Bot detection

Bot attacks are becoming more prevalent with malicious actors using a wide variety of attack vectors, from credential stuffing and brute force attacks to password spraying and fake accounts. PingOne Protect detects non-human behavior, automated frameworks, and recorders by analyzing mouse, keyboard, touch, and mobile sensors and device attributes. For example, if the predictor detects non-human behavior or an automated framework, it alerts as a high-risk event and recommends bot mitigation.

You can configure a fallback value for this predictor type to use if there's insufficient information to calculate a risk level.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> The PingOne Signals (Protect) SDK is required for the bot detection predictor.

Email reputation

The use of disposable email addresses is a common characteristic of fraudulent activity. The email reputation predictor detects the use of disposable email addresses during registration.

You can add the predictor to your risk policies, and you can also define a specific course of action if the `result.recommendedAction` field in the risk evaluation response equals `TEMP_EMAIL_MITIGATION`, such as blocking the registration attempt.

Geovelocity anomaly

Users frequently sign on to the same application from multiple locations throughout the day. A time lapse between two sign-on locations that is shorter than the time it would take to travel between the two points could indicate suspicious activity. PingOne Protect analyzes location data to calculate if travel time between two session locations is physically possible. If the elapsed time is calculated to be impossible, the user can be prompted with step-up authentication or denied access.

For example, if a user signs on to an application from the United States and then attempts to sign on again 2 hours later from Japan, the geovelocity anomaly predictor alerts on this anomaly.

You can configure a fallback value for this predictor type to use if there's insufficient information to calculate a risk level. You can customize a geovelocity anomaly predictor by creating an allow list of IP addresses for which these time and distance calculations should be ignored.

IP reputation

IP addresses that have been involved in malicious activities, such as distributed denial-of-service (DDoS) attacks or spam activity, are considered risky. The more frequently an IP address is used for malicious activities, the higher its risk score. If a user attempts to access an application that is associated with an IP address previously involved with suspicious activity, the probability of potentially risky behavior increases. PingOne Protect analyzes data from different intelligence sources to determine the probability an IP address is associated with malicious activity and to request stronger authentication to verify the user's identity.

You can configure a fallback value for this predictor type to use if there's insufficient information to calculate a risk level. You can also customize an IP reputation predictor by creating an allow list of IP addresses for which the IP reputation score should be ignored.

IP velocity

Compromised accounts can be associated with many different IP addresses. PingOne Protect detects the number of IP addresses a user is leveraging and alerts on anomalies. This predictor learns user behavior and dynamically adjusts the thresholds for each user. For example, if a user attempts to access their account from six different IP addresses within a short time frame, the IP velocity model detects an anomaly.

New device

New device predictors allow your risk policy to take into account the risk associated with users trying to access applications from unknown devices or devices that have not been used in the past 12 months.

Copyright © 2025 Ping Identity Corporation

The new device predictor identifies individual devices using the following attributes and checks for the attributes in the following order:

1. External device ID: If you want to maintain your own device IDs, you can assign external device IDs that are not managed by the PingOne Signals (Protect) SDK (for example, device serial number or mobile application installation ID).

   An example scenario where you might use external device IDs is if your mobile native app incorporates a WebView. In such cases, the mobile Signals SDK and the web Signals SDK provide different device IDs. By providing your own external device IDs, you have a consistent ID to identify devices. External device ID can be mapped through the API or in a DaVinci flow using the PingOne Protect connector.

2. Device ID: When you implement the Signals SDK, it generates and stores a device ID for each user device. If the SDK payload has been successfully sent to the risk evaluation, you see a `deviceID` field in the response to the `Create Risk Evaluation` API request.

3. Cookie + user agent: Set a persistent cookie and the user agent using the API, the PingOne Protect connector in a DaVinci flow, or PingOne Protect nodes in a PingOne Advanced Identity Cloud or PingAM user journey.

You can configure a fallback value for this predictor type to use if there's insufficient information to calculate a risk level. You can also set an activation date for the model to restart the learning process.

PingID device trust

With the rise in cybersecurity and data breaches, it's best practice for your organization to use a device trust process to safeguard your internal and customer data. The PingID device trust predictor allows PingOne to establish device trust with your organization's workstations, adds further security to your user sign-on flows, and reduces risk through the PingID device trust agent.

The PingID device trust agent is a lightweight application used in workforce use cases to add contextual data from your organization's workstations during user sign-on flows. To use the PingID device trust predictor in a PingOne Protect risk policy, you must install the PingID device trust agent on workstations from which your organization's employees sign on to corporate applications. The following contextual data can be added to flows:

- Operating system details, including type, version, patch level, and update status
- Device identification, including external device ID if you're using a third-party device hygiene system
- User authorization and authentication information on the device

Based on the information collected by the agent, PingOne Protect can establish device trust by determining if the device is known or unknown and includes the trust status in the risk evaluation response, such as `TRUST_VERIFIED` or `TRUST_VERIFICATION_FAILED`.

You can configure a fallback value for this predictor type to use if there's insufficient information to calculate a risk level.

Learn more in Using the PingID Device Trust agent.

> **Note**
>
> The PingID device trust predictor requires a PingID license.

Copyright © 2025 Ping Identity Corporation

Suspicious device

The suspicious device predictor checks for suspicious settings or mismatches between browser, operating system, and hardware attributes to detect emulators, super user permissions, virtual machines, mirroring applications, tampered devices and more. PingOne Protect detects suspicious devices by analyzing various data points, including:

- Operating system
- Browser type and version
- Hardware information
- Device settings

Using these data points, the predictor can differentiate between legitimate and suspicious devices and doesn't require any device history to detect anomalies. For example, the suspicious device predictor can detect attempts to attack with mobile emulators and flags such activity as high risk.

You can configure a fallback value for this predictor type to use if there's insufficient information to calculate a risk level.

You can also specify that the predictor requires that the payload from the Signals (Protect) SDK be provided as a signed JWT.

> **Note**
>
> The PingOne Signals (Protect) SDK is required for the suspicious device predictor.

Traffic anomaly

The traffic anomaly predictor detects traffic anomalies, such as brute force attacks, by monitoring various data points, including users, devices, and sessions. Currently, the predictor:

- Detects situations where there are a large number of risk evaluations requested for a single user within a short period of time
- Optionally can detect situations where the number of users per device during a given period of time is suspicious
- Flags these activities as high risk

The traffic anomaly predictor will eventually include additional rules, some of which you'll be able to enable or disable.

When a risk level of high is calculated for a traffic anomaly predictor, the `result.recommendedAction` field in the risk evaluation response returns the value `DENY`. In these situations, you should deny access because the repeated risk evaluations are likely a sign of a brute force attack.

User-based risk behavior

The user-based risk behavior model compares a transaction with the typical behavior of that specific user. For example, if a user accesses an application that they rarely use but is frequently used within the organization, user-based risk behavior detects an anomaly, but user risk behavior doesn't.

Copyright © 2025 Ping Identity Corporation

User-based risk behavior is a machine-learning model that continuously updates. The model learns each user's behavior from various data points, including:

- Operating system
- Browser type and version
- Activity time frame
- Geolocation (country)
- Application being accessed
- Device settings and characteristics

The machine-learning model characterizes abnormal activity as low, medium, or high risk. Thresholds for this predictor are dynamic and might change between different users. You can configure a fallback value for this predictor type to use if there's insufficient information to calculate a risk level.

> **Note**
>
> The PingOne Signals (Protect) SDK is required for the user-based risk behavior predictor type.

User location anomaly

User location anomaly predictors allow you to define a radius around the location of the previous successful sign-on attempts. If a sign-on attempt occurs at a location whose distance from the user's expected location is greater than the radius you defined, it's considered medium or high risk, depending on the extent of the deviation from the defined radius. This information can be used in authentication policies to reduce the risk of unintentional push notification approval and account takeover (ATO) attacks.

The default radius is 50 kilometers. The units for the radius can be set to miles or kilometers. The smallest radius that can be defined is 10 miles (16 KM) and the largest is 100 miles (160 KM).

You can also configure a fallback value to use if there's insufficient information to calculate a risk level.

User velocity

Stolen user accounts are becoming more common. A malicious user can have multiple sets of credentials originating from the same IP address. PingOne Protect detects the number of users originating from the same IP address and alerts on anomalies.

For example, if a workforce organization has 50 users who typically work from the same IP address at their office location, but 100 users attempt to authenticate from this IP address, the user velocity model alerts on this anomaly. Thresholds for this predictor are changed dynamically.

Customizing predictors

> **Important**
>
> Customize predictors only after you've accumulated sufficient event data and analyzed it.

Copyright © 2025 Ping Identity Corporation

When you define your own risk policies, you might be satisfied to use the out-of-the-box predictors provided and adjust the degree to which each predictor is taken into account. If you want to further refine the process, you can customize the individual predictors.

The PingOne Protect predictors can be:

- Customized instances of the basic predictor types
- Multiple risk predictors combined into a single composite predictor
- Custom predictors that use risk data from external sources

There are three ways to customize the predictors that can be included in risk policies:

Fine-tune out-of-the-box predictors

You can customize the out-of-the-box predictors by:

- Renaming the predictor
- Editing the settings contained in some predictors.

For example, for the **IP Reputation** predictor, you can modify the fallback decision value or add a list of IPs that should always be considered low risk.

In addition to changing the settings of some default predictors, you can create additional predictors of certain types. For example, you can create:

- A predictor of type **User Location Anomaly** called `Strict User Location Anomaly` with the distance set to 20 km and the fallback value set to **High** risk.
- A second predictor of type **User Location Anomaly** called `Lenient User Location Anomaly` with the distance set to 50 km and the fallback value set to **Medium** risk.

This makes it easy for you to include the strict predictor in a risk policy that you use for highly-sensitive applications and include the more lenient predictor in a risk policy that you use for less-sensitive applications.

Create composite predictors

Each out-of-the-box risk predictor represents a single risk factor. In some cases, you might need to combine multiple risk predictors and factors into a single predictor, such as when you're concerned about the use of an anonymous network only when a user location anomaly is also reported. This is where composite predictors come in.

In a composite predictor, you define conditions based on individual predictors, and you decide what level of risk should be assigned when the defined conditions are and are not met. Composite predictors can include both the standard predictor types provided and any custom predictors that you have created in addition to several risk factors, such as country and IP range.

In addition to taking into account the results of multiple individual risk predictors, you can include conditions that relate to the total number of predictors in a policy that were **Low**, **Medium**, or **High** risk.

Learn more in Adding composite predictors.

Copyright © 2025 Ping Identity Corporation

Create custom predictors

In addition to including the out-of-the-box predictors in a risk policy, you can create custom predictors to include other sources of risk in your risk policies.

Custom predictors can include the following types of comparisons:

- Numerical comparisons, using ranges you have defined for **Low**, **Medium**, and **High** risk
- Checking if an IP falls into a range of IPs that you have defined
- String-matching

Find descriptions of the types of information that you can include as a custom predictor in the fields for the details and event objects in the **Details data model** and **Event data model** tables in the Risk evaluations section of the PingOne API documentation. You can also refer to the sample response to see an example `Create risk evaluation` API request.

Learn more in Adding custom predictors.

Configuring predictors

You can configure and edit details and configuration settings for out-of-the-box, custom, and composite predictors at any time.

About this task

Most predictor types allow you to define a **Fallback Predictor Decision Value**, which is the risk level that should be assigned to the predictor if there is insufficient information to calculate the risk level. This can occur for a number of reasons, such as:

- The predictor is still in the training period.
- The basic information required (for example, the location of the user) can't be obtained.

To configure and edit a predictor:

Steps

1. In the PingOne admin console, go to **Threat Protection** > **Predictors**.
2. Click the predictor type to expand the predictor list, then click the specific predictor that you want to edit.
3. Edit the predictor details and configuration settings:
    - To edit **Display Name** and **Description**, click the **More Options** (⋮) icon and click **Rename**.
    - To edit configuration settings, click the **Pencil** icon and edit any of the following:

Copyright © 2025 Ping Identity Corporation

Predictor	Settings
Adversary-in-the-Middle (AitM)	Use the **Fallback Predictor Decision Value** list to select the risk level that this predictor should be assigned if there's insufficient information to calculate the risk level. Use the **Domain Allow List** field to provide a comma-separated list of the domains that are legitimate for your resources. These will be compared with the domains that your users are trying to access to verify that they were not the target of phishing attempts. If you don't specify one or more domains, PingOne Protect sets a short learning period to learn the domains that your users are accessing, and these domains are added to the allow list. The learned domains are displayed under **Domain Allow List**.
Anonymous Network Detection	Use the **Fallback Predictor Decision Value** list to select the risk level that this predictor should be assigned if there's insufficient information to calculate the risk level. In the **Allow List** field, enter the IP addresses for which anonymous network considerations should be ignored. This must be one or more ranges of IP addresses in classless inter-domain routing (CIDR) format, separated by commas, for example, `1.1.1.1/24, 1.1.2.1/12`. For IP addresses in IPv4 format, you can use IP ranges. For IP addresses in IPv6 format, you must add each address to the list individually.
Bot Detection	Use the **Fallback Predictor Decision Value** list to select the risk level that this predictor should be assigned if there's insufficient information to calculate the risk level. Use the **Track events without SDK payload** option to expand the types of bot activity that PingOne Protect can detect. To use this option, you must configure the PingOne Signals (Protect) SDK to pass the SDK payload into the risk evaluation.
Email Reputation	Use the **Fallback Predictor Decision Value** list to select the risk level that this predictor should be assigned if there's insufficient information to calculate the risk level.

Copyright © 2025 Ping Identity Corporation

Predictor	Settings
Geovelocity	Use the **Fallback Predictor Decision Value** list to select the risk level that this predictor should be assigned if there's insufficient information to calculate the risk level. In the **Allow List** field, enter the IP addresses for which anonymous network considerations should be ignored. This must be one or more ranges of IP addresses in CIDR format, separated by commas, for example, `1.1.1.1/24, 1.1.2.1/12`. For IP addresses in IPv4 format, you can use IP ranges. For IP addresses in IPv6 format, each address must be added to the list individually.
IP Reputation	Use the **Fallback Predictor Decision Value** list to select the risk level that this predictor should be assigned if there's insufficient information to calculate the risk level. In the **Allow List** field, enter the IP addresses for which anonymous network considerations should be ignored. This must be one or more ranges of IP addresses in CIDR format, separated by commas, for example, `1.1.1.1/24, 1.1.2.1/12`. For IP addresses in IPv4 format, you can use IP ranges. For IP addresses in IPv6 format, each address must be added to the list individually.
IP Velocity	You can't configure settings for the **IP Velocity** predictor.
New Device	Use the **Fallback Predictor Decision Value** list to select the risk level that this predictor should be assigned if there's insufficient information to calculate the risk level. Use the **Activation Date** field to specify a date when the learning process for the predictor should be restarted. You can use this in conjunction with the fallback setting to force strong authentication when moving the predictor to production. **Note** **Activation Date** uses UTC time.
PingID Device Trust	Use the **Fallback Predictor Decision Value** list to select the risk level that this predictor should be assigned if there's insufficient information to calculate the risk level.

Copyright © 2025 Ping Identity Corporation

Predictor	Settings
Suspicious Device	Use the **Fallback Predictor Decision Value** list to select the risk level that this predictor should be assigned if there's insufficient information to calculate the risk level. Use the **Signed SDK Payload is Required** option to specify that the predictor requires that the payload from the Signals (Protect) SDK be provided as a signed JSON Web Token (JWT). **Note** Before selecting this option for your predictor, verify that you've enabled the option to have the SDK payload provided as a signed JWT in the initialization code for the SDK. If you're using DaVinci flows, you can enable the signed JWT option when configuring the `skrisk` component in your flows. Learn more in the documentation for the web version of the Signals SDK and PingOne Protect DaVinci connector.
Traffic Anomaly	Use the **Fallback Predictor Decision Value** list to select the risk level that this predictor should be assigned if there's insufficient information to calculate the risk level. Use the **Users per Device** option to set the maximum number of users per device to be considered **Medium** and **High** risk for the specified timeframe.
User Location Anomaly	Use the **Fallback Predictor Decision Value** list to select the risk level that this predictor should be assigned if there's insufficient information to calculate the risk level. Enter the radius **Distance** and select the **Measurement** units (miles or kilometers).
User-Based Risk Behavior	Use the **Fallback Predictor Decision Value** list to select the risk level that this predictor should be assigned if there's insufficient information to calculate the risk level.
User Velocity	You can't configure settings for the **User Velocity** predictor.

4. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Adding predictors

Add additional predictors to a risk policy to identify possible fraudulent user behaviors.

About this task

PingOne Protect allows you to add additional predictors to the out-of-the-box predictors in a risk policy. You can add custom predictors, composite predictors, and additional versions of certain out-of-the-box predictors. Learn more in Predictors, Adding custom predictors, and Adding composite predictors.

When you create a new predictor, it's included by default in any subsequent risk policies you create.

When creating predictors, consider the following points regarding the relationship between the **Predictors** page and the **Risk Policies** page:

- When you create a new environment, it includes a default risk policy.
- When you first go to the **Predictors** page, you see the predictors that are included in the default risk policy.
- When you customize predictors, you see the change immediately in any risk policies that use the predictors that you modified.
- When you create new predictors, you can use them when you update existing risk policies or when you create new risk policies.

Most out-of-the-box predictors have settings you can configure. Learn more in Configuring predictors.

For most scenarios, you don't need to add additional out-of-the-box predictors, but there could be specific cirumstances when you need to add them. As an example scenario, you have a different risk policy for different user populations: one group of users travels frequently, and the other group never travels. In this scenario, you can add two **User Location Anomaly** predictors, each configured with a different radius distance and use the two predictors in different risk policies.

To add predictors:

Steps

1. In PingOne, go to **Threat Protection** > **Predictors**.
2. To add a new predictor, click the **+** icon.
3. For **Predictor**, choose the predictor type you want to add.

   > **Note**
   > You can only add additional predictors of certain predictor types.

4. In the **Display Name** field, enter a name for the predictor.

   The display name is used in the **Threat Protection Dashboard** and policy configuration.

5. In the **Compact Name** field, enter a short name that is returned in the API response.

   > **Note**
   > You can't change the compact name after it's been saved.

Copyright © 2025 Ping Identity Corporation

6. Configure the predictor.
7. Click **Save**.

Adding custom predictors

Custom predictors allow you to include risk-related data that isn't represented by any of the out-of-the-box risk predictors that PingOne Protect provides.

The data for a custom predictor can be:

- Information that PingOne Protect has, but isn't included in one of the standard predictors, such as the country where the user trying to access the resource is currently located
- External risk-related data that you provide as input, such as information on managed and unmanaged devices from PingFederate

You can define three types of custom risk predictors:

- IP range: Definition of risk levels associated with different IP ranges
- String matching: Definition of risk levels associated with different values of input provided as a string
- Numeric range: Definition of risk levels associated with different values of input provided as a number

Custom predictors are treated like the out-of-the-box predictors in terms of:

- Being able to add them to risk policies
- Viewing data for the predictors in the **Threat Protection Dashboard**
- Inclusion of the data in PingOne Audit logs

You can add a maximum of 15 custom predictors per environment.

Steps

1. In the PingOne admin console, go to **Threat Protection** > **Predictors**.
2. To add a new predictor, click the **+** icon.
3. For the predictor type, select **Custom**.
4. In the **Display Name** field, enter a name for the predictor.

   The display name is used in the **Threat Protection Dashboard** and policy configuration.
5. In the **Compact Name** field, enter a short name that will be returned in the API response.

   > **Note**
   > You can't change the compact name after it's been saved.
6. The **Attribute Mapping** field is used to point to the variable that will contain the data that's being used to determine high, medium, or low risk for the predictor. The field can take any of the following types of data:

Copyright © 2025 Ping Identity Corporation

Choose from:

- One of the fields included in the `details` object returned in the API response for risk evaluations, such as `details.country`. In this case, you would enter `${details.country}` in the **Attribute Mapping** field.
- One of the fields included in the `event` object included in the API request for risk evaluations, such as `event.browser.userAgent`. In this case, you would enter `${event.browser.userAgent}` in the **Attribute Mapping** field.
- Data that you're providing from an external source. You provide the data by including a new field in the `event` object in the `Create risk evaluation` API request, for example, `event.managedDevice`. In this case, you would enter `${event.managedDevice}` in the **Attribute Mapping** field.

  Learn more about the fields included in the `details` and `event` objects in the Details data model and Event data model tables in the Risk evaluation section of the PingOne API documentation.

  > **Note**
  >
  > If you defined a flow in DaVinci where custom attributes are provided as input to the risk evaluation, you must add `customAttributes` after `event` in the **AttributeMapping** field. For example, `${event.customAttributes.managedDevice}`.

7. In the **Fallback Predictor Decision Value** list, select a default risk level to use in case the attribute isn't provided.
8. In the **Risk Level Mapping** section:
   1. Select the type of input that's being provided for the comparison:
      - **Range** for numeric range input
      - **IP Ranges** for IP range input
      - **List Item** for string-matching input
   2. Enter the values that will be considered **Low**, **Medium**, and **High** risk.
      1. For string matching, enter one string in each text field.
      2. Click **Add List Item** if you want to provide more than one string for any of the three risk levels.

      > **Note**
      >
      > - If a value appears in more than one of the risk categories (**Low**, **Medium**, **High**), the more strict risk category is used for the value.
      > - For numeric input, the input is assigned to a specific risk level (**Low**, **Medium**, **High**) if it's greater than or equal to the **Min** value and less than the **Max** value.
9. Click **Save**.

Adding composite predictors

Each of the standard risk predictors represents a single risk factor. Use composite predictors to combine a number of risk predictors and factors into a single predictor, such as when you're concerned about the use of an anonymous network only when a user location anomaly is also reported.

Copyright © 2025 Ping Identity Corporation

About this task

You decide what level of risk you want to assign when the various conditions defined in the composite predictor are and are not met. Composite predictors can include both the standard predictor types provided and any custom predictors that you have created.

In addition to default and custom predictors, you can include the following risk factors in composite predictors:

- Country
- State
- IP range
- IP domain organization
- Internet service provider (ISP)
- Target resource name (target application)
- User groups
- User ID
- User name

As an example scenario for using composite predictors, you want the **Geovelocity** predictor to ignore a long list of IP addresses. The allow list can include up to 400 IP addresses for one predictor. If you need more than 400 IP addresses, you can add another **Geovelocity** predictor, combine the two predictors in a composite predictor (using the **All** operator), and add the composite predictor in the risk policy.

Steps

1. In the PingOne admin console, go to **Threat Protection** > **Predictors**.
2. To add a new predictor, click the **+** icon.
3. For the predictor type, choose **Composite**.
4. In the **Display Name** field, enter a name for the predictor.

   The display name is used in the **Threat Protection Dashboard** and policy configuration.
5. In the **Compact Name** field, enter a short name that is returned in the API response.

   > **Note**
   > You can't change the compact name after it's been saved.
6. Configure the criteria for the composite predictor.

   > **Note**
   > Predictor conditions are applied in order from top to bottom.

   1. To determine the conditions for each set of criteria, use **All**, **Any**, or **None**.

Copyright © 2025 Ping Identity Corporation

You can also nest sets of conditions.

2. Select a predictor type or risk factor, select an operator, and enter or select the value:
   - To use one value as the criterion, such as a single country, use the **Equals** or **Not Equals** operators.
   - To specify multiple values, such as a group of countries, use the **Is In** or **Not In** operators.
   - If you are using **User Groups** as a criterion, use the **Is In** or **Not In** operators to specify any number of groups and enter the names of the PingOne user groups to check what PingOne user groups the user belongs to.

     > **Note**
     > When you use the **Is In** or **Not In** operators to define a set of possible values for a risk factor that takes free text, such as **State**, provide the values as a comma-separated list.

   - If you are using **User ID** or **User Name** as a criterion, you can also use the **Contains** operator, which checks whether the User ID or User Name includes the specified substring. For example, you could check whether the User ID contains a certain domain name. The **Contains** operator is not case-sensitive.
3. (Optional) To add additional criteria, click **+ Item** to add a new criteria item, or **+ Group** to add a new group of criteria.
4. For **Risk Level Equals**, select **Low**, **Medium**, or **High** to determine the risk level result when the set of criteria is met.

   Example:

   In addition to taking into account the results of multiple individual risk predictors, you can include conditions that relate to the total number of predictors in a policy that were low, medium, or high risk.

   For example, you can create a composite predictor that specifies that the predictor should get a result of high risk if any of the following conditions are true:

   - **IP Reputation** is high risk.
   - **IP Velocity** is high risk.
   - Any three predictors in the policy being evaluated are found to be high risk.

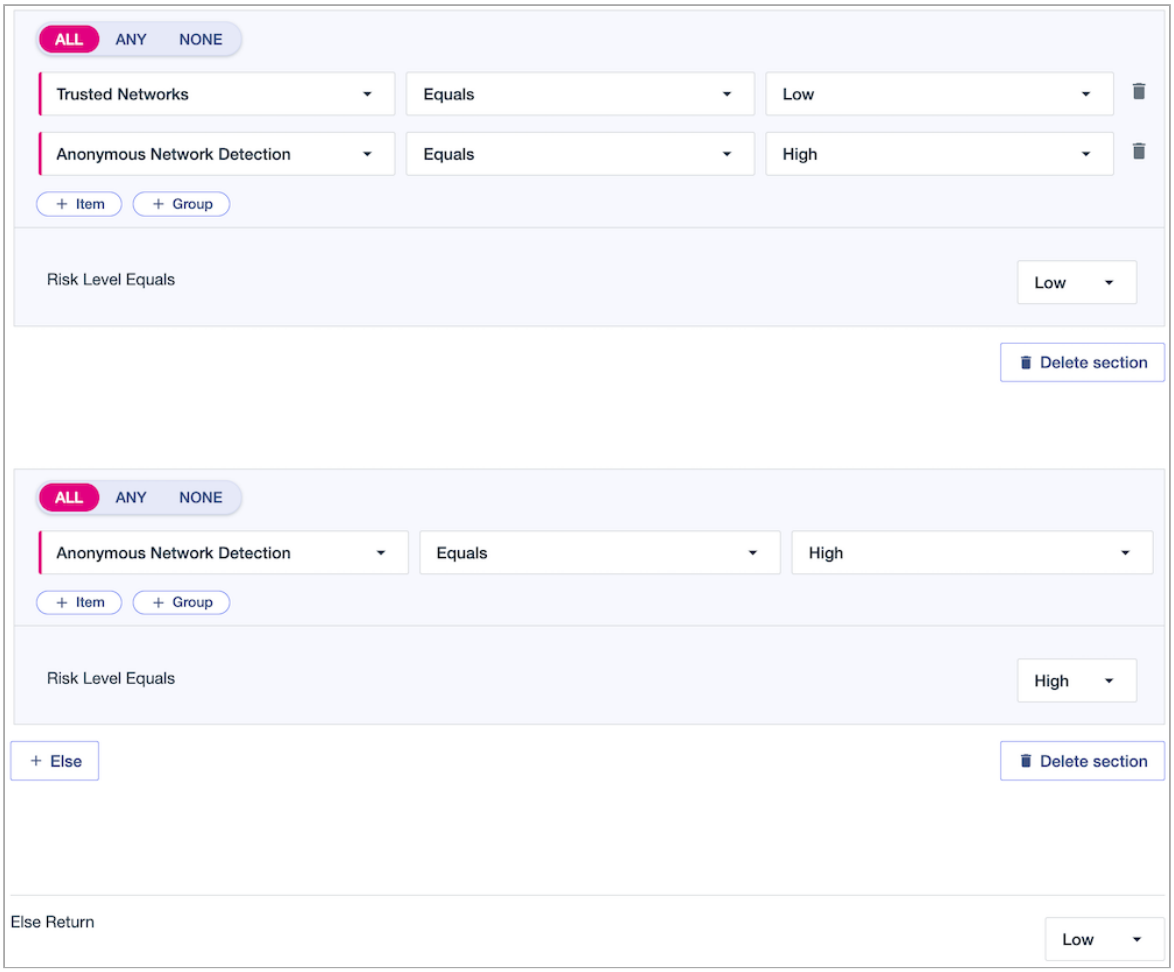
7. (Optional) Add additional conditions to evaluate if the first set of conditions is not met.
   1. Click **+ Else**.
   2. Configure the criteria and the risk level.

      > **Note**
      > You can configure up to three sets of conditions in a composite predictor.

8. (Optional) To configure the risk level result to assign if none of the defined conditions is met, select **Low**, **Medium**, or **High** for **Else Return** at the bottom of the page.

   > **Note**
   > The default value for **Else Return** is **None**.

Copyright © 2025 Ping Identity Corporation



9. Click **Save**.

Next steps

After a composite predictor yields a result, you can use the result in the same ways as the results of individual risk predictors:

- You can assign the predictor a score or weight to be used with the other predictors in your risk policy to calculate a final risk level.

> **Important**
>
> **Weights** in risk policies have been deprecated for new PingOne environments but can still be used in existing environments.

- You can define an override that uses the composite predictor so that in cases where the predictor conditions are met, you can directly assign a final risk level and ignore the other predictors in the risk policy.

Deleting a predictor

You can only delete additional predictors that you added. The default predictors can't be deleted.

Copyright © 2025 Ping Identity Corporation

Steps

1. In the PingOne admin console, go to **Threat Protection** > **Predictors**.
2. On the predictor that you want to delete, click the **More Options** (⋮) icon.
3. Click **Delete**.

Testing predictors

To test predictors, you can simulate risk events with a sample application in PingOne.

Before you begin

- You'll need a PingOne account and an environment with the PingOne Protect service. You can use an existing account or start a PingOne trial. Learn more in Starting a PingOne trial and Adding the PingOne Protect service to your environment.
- You can optionally use a sample app to test the risk predictors. Learn more about configuring an environment with a sample app in Trying PingOne Protect with a sample app.

About this task

Simulations allow you to deepen your understanding of how PingOne Protect detects different types of risk events. Learn more in PingOne Protect key concepts and Predictors.

Steps

- To test common predictors:

Predictor	Testing Steps
Geovelocity anomaly	1. Sign on to your account. 2. Sign on again with a Remote Desktop Protocol (RDP) in a server from a remote datacenter. You can alternatively have a colleague based in a different location sign on to the sample app with the same user.
New device	1. Sign on from one device. 2. Sign on again from another device.
Anonymous network detection	1. Use a public VPN/server or browser extension that hides your IP address. 2. Sign on.

Copyright © 2025 Ping Identity Corporation

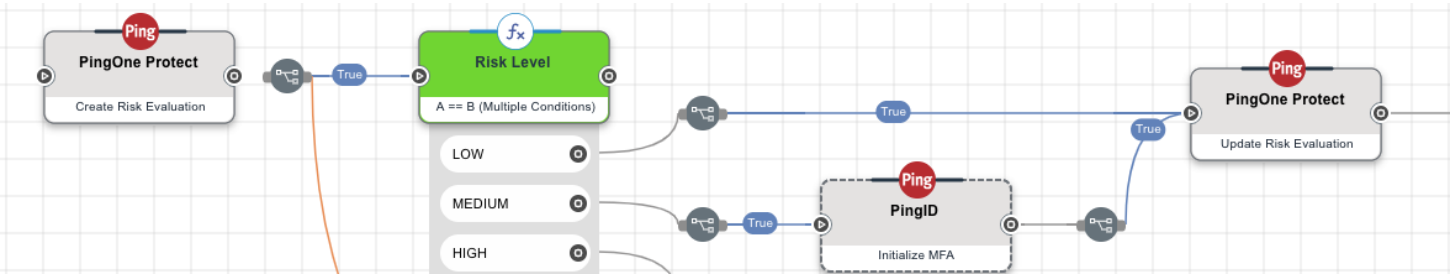
Predictor	Testing Steps
User-based risk behavior	1. Train the predictor by creating risk evaluations (such as signing on with the same user account several times and authenticating successfully each time). 2. Create a new risk evaluation (such as signing on again from a different browser or a different operating system if possible).

Risk evaluations

Risk evaluations calculate the risk level associated with an event. The risk evaluation uses the risk policy and the predictors included in the risk policy to determine a final risk level of low, medium, or high. Learn more in Risk policies.

Adding risk evaluation to a user flow

When you define a user journey, such as an authentication flow, you can include risk evaluations at relevant points in the flow. The risk evaluation is based on the risk policy that you specify for the evaluation. The following diagram shows a simplified sample flow using PingOne DaVinci that includes two steps related to risk evaluation.



1. Add a risk evaluation step at a point in the flow where you want the next action to be based on the calculated risk level. For example, you can design the flow to prompt the user to complete multi-factor authentication (MFA) for medium or high risk levels but automatically grant access for low risk level.

2. At the end of the flow, include a step to update the risk evaluation with the completion status of the flow (`SUCCESS` or `FAILED`). In the sample DaVinci flow, completion status indicates whether the user was able to successfully authenticate or not. Learn more in Updating completion status for risk evaluations.

Analyzing risk evaluation results

Review and analyze the results from risk evaluations to see how your risk policy is performing. After reviewing the results, you might need to fine-tune your risk policy, depending on your organization's needs and use cases. To make decisions on whether you need to adjust your risk policy, consider the following:

Your business goals

Should your risk policy be more permissive or more restrictive? This decision depends on your organization's needs, tolerance for fraud incidents, and overall revenue and user experience impacts.

Copyright © 2025 Ping Identity Corporation

How your risk policy is configured

How are various predictors configured as part of your risk policy? How are the final risk levels assigned? Learn more about questions to consider when creating and fine-tuning a risk policy in Risk policies.

The type of user flow

Is your risk policy used for an access, authentication, authorization, registration, or transaction flow? The type of user flow might affect the adjustments you make to a risk policy. You can also specify a flow subtype to provide additional detail about the context of the flow, such as if the user performed a password reset or signed on with their username and password. Learn more about flow types and subtypes in the PingOne API documentation.

You can also create different risk policies for different use cases. Learn more in Risk policies.

Additional identity mitigation tools

Should you use additional tools, such as MFA, identity verification, or knowledge-based authentication (KBA), in your user flow to prevent user identity fraud?

Learn more about how to:

- Update the risk evaluation completion status to improve the accuracy of future risk evaluations.
- Provide feedback on the accuracy of risk evaluations.
- View risk evaluations and determine if you need to fine-tune your risk policy.

Reviewing risk evaluations

Depending on your organization's goals and use cases, you should review and analyze risk evaluations to fine-tune your risk policy.

About this task

To review a risk evaluation:

Steps

1. View a risk evaluation.

   Choose from:

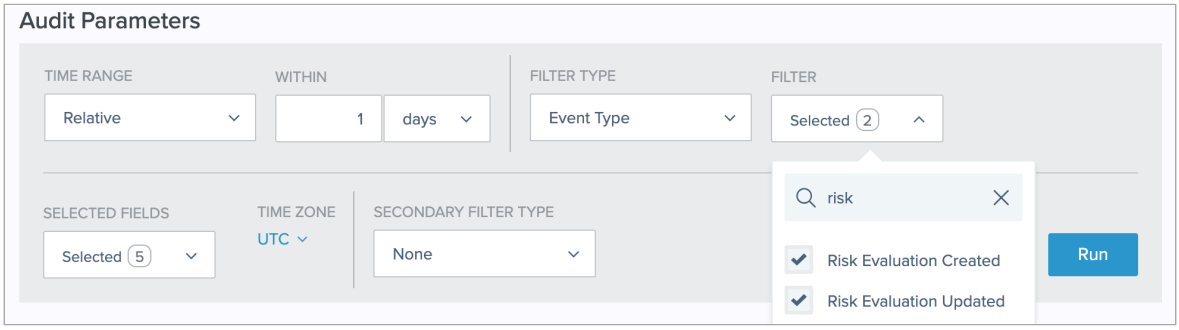
   - Using the API: You can find information about creating a risk evaluation in the PingOne Protect API documentation.
   - Using the PingOne admin console:

     1. In the PingOne admin console, go to **Monitoring > Audit**.
     2. Edit the **Time Range** and **Within** fields as needed.
     3. For **Filter Type**, select **Event Type**.
     4. For **Filter**, select **Risk Evaluation Created** and **Risk Evaluation Updated**.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> You can enter `risk` in the **Search Filter Type** field to view only risk-related event types.

You can find a complete list of events logged in PingOne in Audit Reporting Events in the PingOne API documentation.



5. Click **Run**.
6. To view the specific data and scores from an event, click **View** in the **Details** column in the report summary.

   Example:

   The following is an example response result from a risk evaluation:

```
"result": {
        "level": "HIGH",
        "score": 80.0,
        "source": "AGGREGATED_SCORES",
        "recommendedAction": "BOT_MITIGATION",
        "type": "VALUE"
}
```

2. In the response result section, review the following attributes in this order:

   1. `result.recommendedAction`

      Possible values are:

      - `BOT_MITIGATION`: If this attribute is included in the result, a bot was detected, and your policy's risk level returned `HIGH`. In this case, you should halt the user flow or route the user to an additional bot mitigation tool.

      > **Note**
      >
      > Make sure to set the bot detection predictor score higher than the overall **High risk threshold** in the risk policy. If the bot detection predictor score is not set higher than the **High risk threshold**, the risk policy result will not include the `recommendedAction: BOT_MITIGATION` attribute. Using this attribute allows you to test your risk policy or control the response from the risk policy instead of modifying the flow or code at the app level.

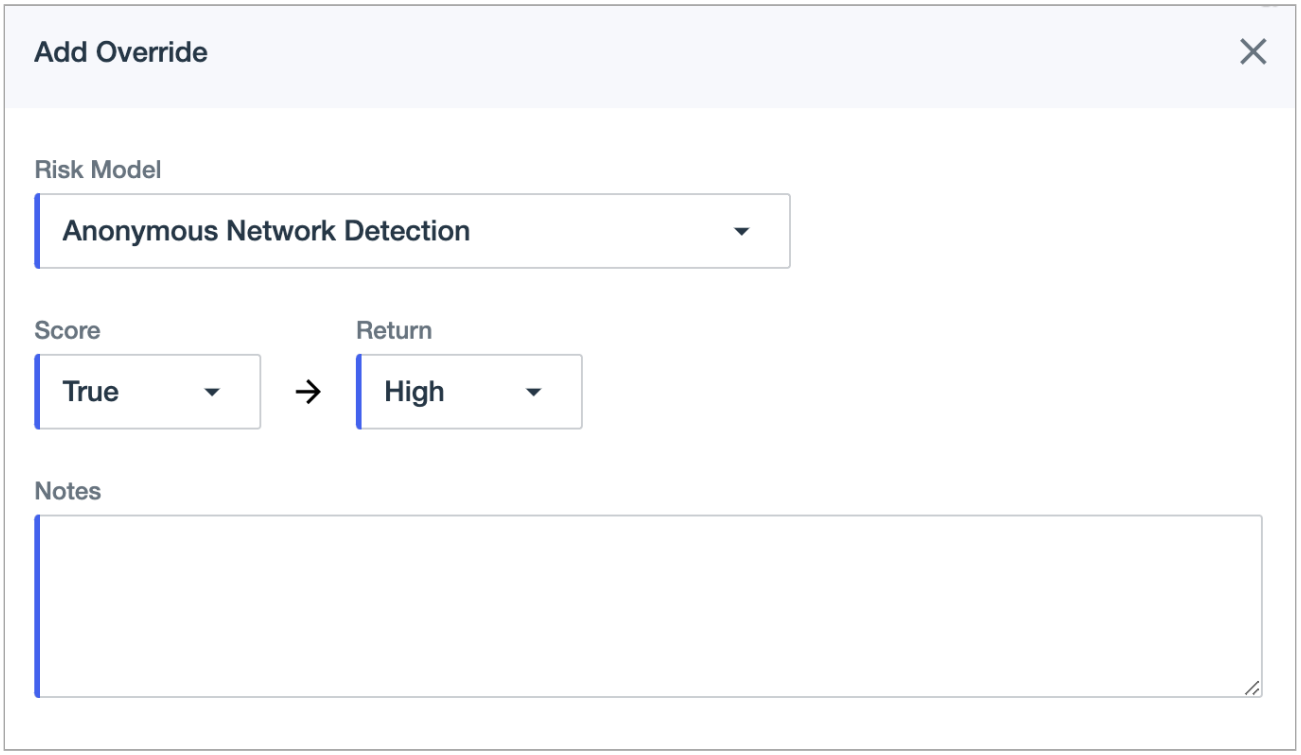
Copyright © 2025 Ping Identity Corporation

- `AITM_MITIGATION`: You should take steps to mitigate the damage from an Adversary-in-the-Middle (AitM) attack. For an AitM attack, the user's credentials have been intercepted, so in addition to blocking the access request, you should lock the user's account until the password is changed.
- `TEMP_EMAIL_MITIGATION`: The user has specified a disposable email address, which is an indication of a fraud attempt.
- `DENY`: When a risk level of `HIGH` is calculated for a traffic anomaly predictor, you should deny access because the repeated risk evaluations are likely a sign of a brute force attack.

2. `result.value`

   This attribute is included in the result when a risk policy has an override configured, and the **Notes** field of the override rule has free text entered.

   Check the value returned in the result against the **Notes** text entered in the override rule. If you don't use overrides for blocking events, you do not need to check this attribute.



3. `result.level`

   This attribute is always included in the response as one of three levels and affects the user flow as follows:

   - `LOW`: Continue the user flow without additional friction.
   - `MEDIUM`: Challenge the user with multi-factor authentication (MFA).

     You can decide to continue the user flow without challenging the user, depending on your use case, the user flow type, and how your risk policy is configured.
   - `HIGH`: Challenge the user with restrictive MFA.

Copyright © 2025 Ping Identity Corporation

The specific method you employ to challenge the user in a high-risk event depends on your use case and the type of MFA available to your users. It is not recommended to use the standard push MFA mechanism or block the user in this case.

4. `result.score`

   This numeric attribute is tied to `result.level` and can be used instead of or in conjunction with `result.level` for additional granularity.

   Example: You might decide to block based on the risk score, such as if `result.score` is greater than 250. Before making such a decision, review the **Threat Protection Dashboard** production data to see how your risk policy is currently performing.

   > **Note**
   >
   > If you want to block based on risk scores, check `result.score` before `result.level`.

   The following is an example user flow using `result.score` in conjunction with `result.level`:

   - If `result.score` is greater than 300, then block.
   - If `result.level` is `HIGH`, then restrictive challenge with MFA, such as with one-time passcode (OTP) or Fast IDentity Online (FIDO).
   - If `result.level` is `MEDIUM`, then challenge with MFA.
   - If `result.level` is `LOW`, then allow.

3. Analyze the response results to determine if the desired outcome occurs for various events and risk levels.

Next steps

After reviewing risk evaluations, you might need to fine-tune your risk policy, including how the various predictors are configured, the weights or scores assigned to the predictors, any override rules, and how the thresholds for the final risk level are set.

> **Important**
>
> **Weights** in risk policies have been deprecated for new PingOne environments but can still be used in existing environments.

You can also create a staging policy to test changes to your risk policy before putting them into production. Learn more in Creating and managing staging policies.

Updating completion status for risk evaluations

When PingOne Protect is integrated into a user journey, you can define different paths in the flow based on the risk evaluation response. For example, in an authentication flow, each risk evaluation created determines whether the user is granted access, challenged with multi-factor authentication (MFA), or denied access.

About this task

For every `Create Risk Evaluation` event in a user flow, PingOne Protect also requires an `Update Risk Evaluation` event that includes the flow completion status for the risk evaluation. Updating the flow completion status allows PingOne Protect to improve the accuracy of future risk evaluations and ensure protection against fraudulent access attempts.

Copyright © 2025 Ping Identity Corporation

Many of the predictors used in risk policies gradually learn characteristics from access attempts made by your users, such as where the user is physically located and what operating system they're using. This learning process can only take place if your flow provides the completion status to indicate which access attempts were made by legitimate users.

Steps

- Update the risk evaluation completion status for an event:

  Choose from:

  - PingOne API: Use the `completionStatus` property in the risk evaluation.
  - PingOne DaVinci: Add a PingOne Protect connector with the Update Risk Evaluation capability at the end of a user flow.
  - PingOne Advanced Identity Cloud: Add a PingOne Protect Result node to an Advanced Identity Cloud journey.
  - PingAM: Add a PingOne Protect Result node to a PingAM journey.
  - PingFederate: The PingOne Protect Integration Kit handles updating the risk evaluation automatically and does not require additional configuration.
  - For any other integration, make sure to include an Update Risk Evaluation event at the end of your user journey.

Result

After adding an `Update Risk Evaluation` event, `completionStatus` is updated as one of the following:

- `SUCCESS` when the user was granted access or passed the MFA challenge

  Only events with `completionStatus=SUCCESS` allow the predictors to learn.

- `FAILED` when the user was denied access or failed the MFA challenge.

  If a user is unable to successfully complete an event (for example, if their authentication failed), the risk evaluation for the event is updated as `completionStatus=FAILED`.

If `completionStatus` is not updated, the status remains `completionStatus=IN_PROGRESS`, and the predictor cannot learn from the event and stays in training mode.

Providing feedback for risk evaluations

You can provide feedback on the accuracy of risk evaluations using the `riskFeedback` endpoint in the PingOne API.

You can include feedback for one or multiple risk evaluations in each call. For each evaluation, you can specify a feedback category and a reason for including the evaluation in that category. This capability will also be added in the PingOne admin console in the future. Learn more in Providing feedback for risk evaluations in the API documentation.

Threat Protection Dashboard

The **Threat Protection Dashboard** provides a visual representation of real-time PingOne Protect data.

To access the **Threat Protection Dashboard**, in the PingOne admin console, go to **Monitoring > Threat Protection**.

Copyright © 2025 Ping Identity Corporation

Risk totals chart

The **Threat Protection Dashboard** shows the **Risk totals** chart, which summarizes all risk events analyzed in the selected time period. You can use the slider under the **Risk summary** chart to show data from the current day, past week, past month, or past six months. The columns in the chart rescale to show information over the selected time period. You can hover over a column to show the specific period it represents.

The columns in the chart rescale to show information over the selected time period. Each column is broken down into five sub-columns, defined at the top of the chart from left to right:

- The number of analyzed events
- The number of medium risk events
- The number of high risk events
- The number of high risk users
- The number of high risk IP addresses

In addition to the **Risk totals** chart, the **Threat Protection Dashboard** consists of the following graphs, each of which can be expanded for greater detail:

- Risk heat map
- Risk events
- High risk models

- Browser distribution
- OS distribution
- Top 20 high risk users
- Risky IP

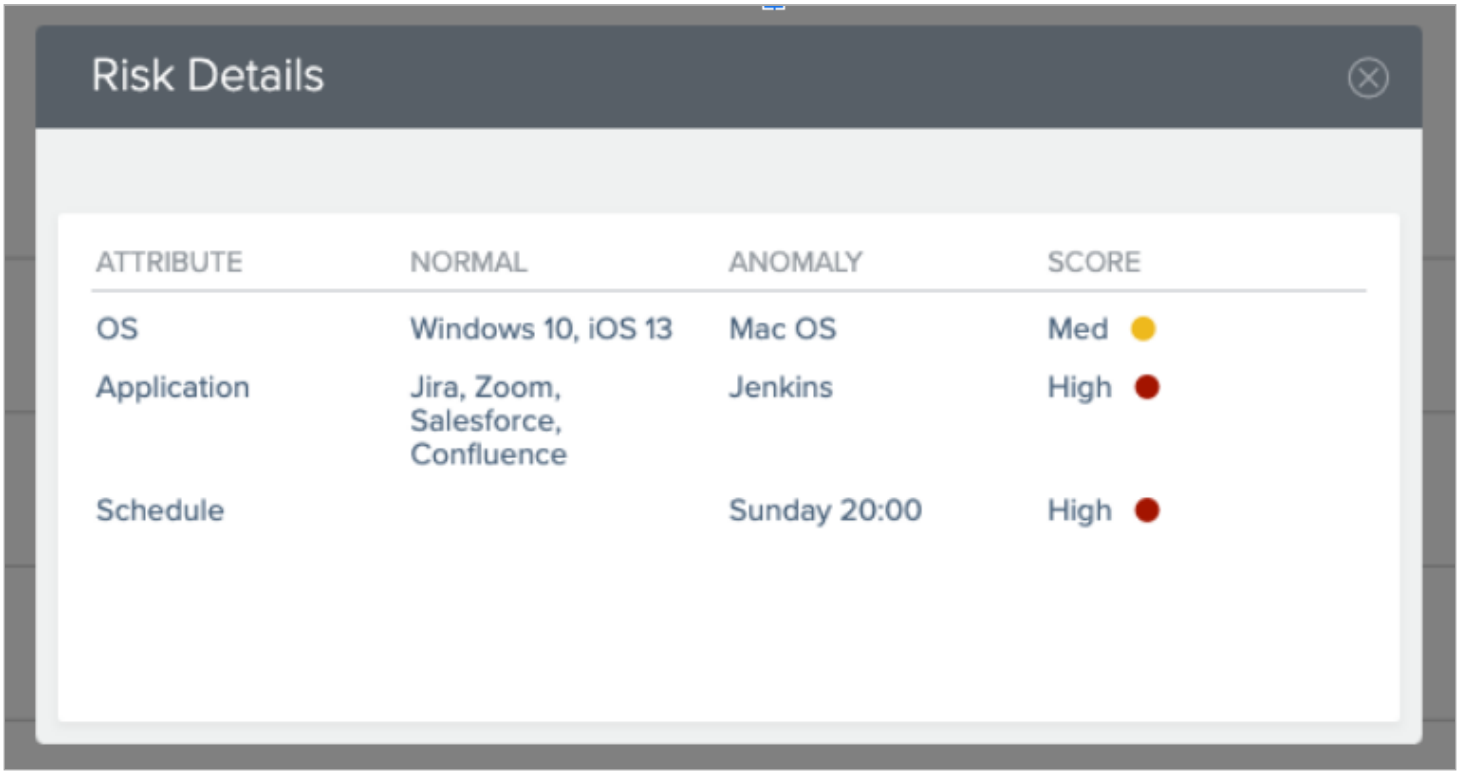
Risk details

> **Note**
>
> Only users with the `dir:read:user` permission can view the drill down table and user data.

In the monitored risk data tables, if the **User Based Risk Behavior** score is **Medium** or **High**, click the score to show the **Risk Details** window.

USER VELOCITY BY IP	IP VELOCITY BY USER	USER BASED RISK BEHAVIOR	USER BASED RISK BEHAVIOR REASON
LOW	LOW	HIGH	Unusual: OS, Browser Properties, Cou...
LOW	LOW	HIGH	Unusual: OS, Browser Properties, Cou...
LOW	LOW	HIGH	Unusual: OS, Browser Properties, Cou...

The **Risk Details** window compares values of the anomalous transaction to typical user behavior.

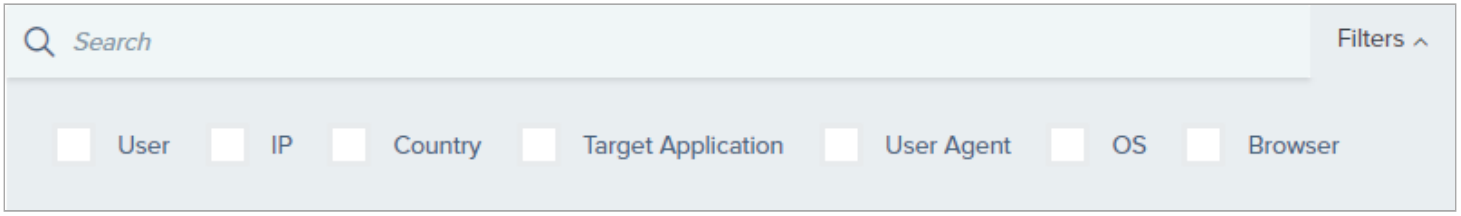


Copyright © 2025 Ping Identity Corporation

Column	Description
Attribute	The category of the anomalous transaction
Normal	Typical values of the transaction category, according to normal user behavior
Anomaly	The anomalous value in the transaction
Score	The risk level of the anomaly

Filtered searching

The filtered search bar appears above each table of risk data.



- Click **Filters** to toggle the list of filter options.
- Use the check boxes to select filters.
- If you enter free text without choosing at least one filter, the search displays all table rows containing the entered text.
- Wild card searches using an asterisk (`\*`) are not supported.
- A space is a significant character in a search string. For example, `Chrome<space>Mobile` works. `Chrome<space><space>Mobile` does not work.
- Use of quotation marks is not supported.
- The left-hand search filters operate first. Subsequent use of the filtered search bar produces a subset of the prior left-hand filter.

  For example, in the **Country** list, select **India**. The table shows results for India only.

  In the filtered search bar, select **OS** and enter `Android 10`. The table is reduced to show only users from India signing on from an Android 10 device.

  Learn more about the left-hand filters in Threat Protection Dashboard filters.

Threat Protection Dashboard filters

Use filters in the **Threat Protection Dashboard** charts to control the data displayed in the charts.

The following table lists all filters in the dashboard charts:

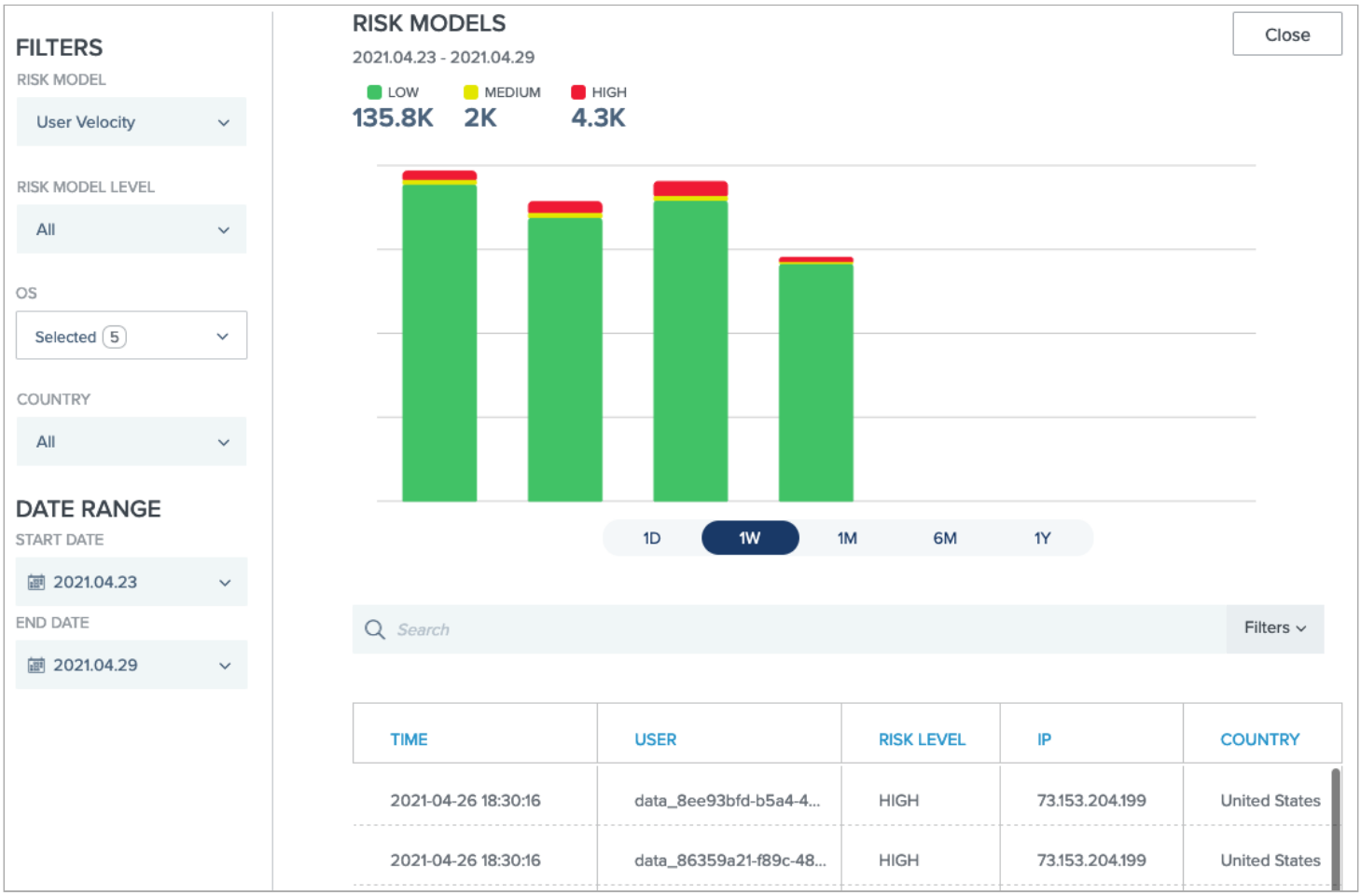
Copyright © 2025 Ping Identity Corporation

Filter	Description
Policy Name	Filters risk policies to be included in the chart. You can select multiple policies.
Event Type	Filters production and staging policy event types.
Flow Type	Filters the type of user flow: • Access: Verification of whether the user can access the relevant application, using tools such as PingAccess • Authentication: Authentication for sign-on or actions such as a password change • Authorization: Verification of whether the user is authorized to perform a specific action (for example, a profile change), using tools such as PingOne Authorize • Registration: Initial registration of an account • Transaction: Authentication performed during a purchase or other monetary transaction
Risk Level	Limits the results to a specific risk level.
High-Risk Model	Displays data from high-risk models.
Risk Model	Displays data from risk models. When you select a risk model from the list, the chart changes to show the risk level distribution of that risk model.
Risk Model Level	Limits the results to a specific risk level. The default value is **High**.
Amount/Percent	Displays the results as a number or percentage.
OS	Filters operating systems to be included in the chart.
OS/Family	Displays specific operating systems only.
Browser Family	Displays specific browser families only.
Country	Limits the results to a specific country.
User Name	Filters the data by specific users. All users are selected by default. **Note** The **User Name** selection only affects the drill-down table.
Date Range	Shows data from a custom time period.

Copyright © 2025 Ping Identity Corporation

Filter	Description
Period bar	Shows data from the current day, previous week, previous month, or previous six months.

The following image shows the filters available in one of the dashboard charts.



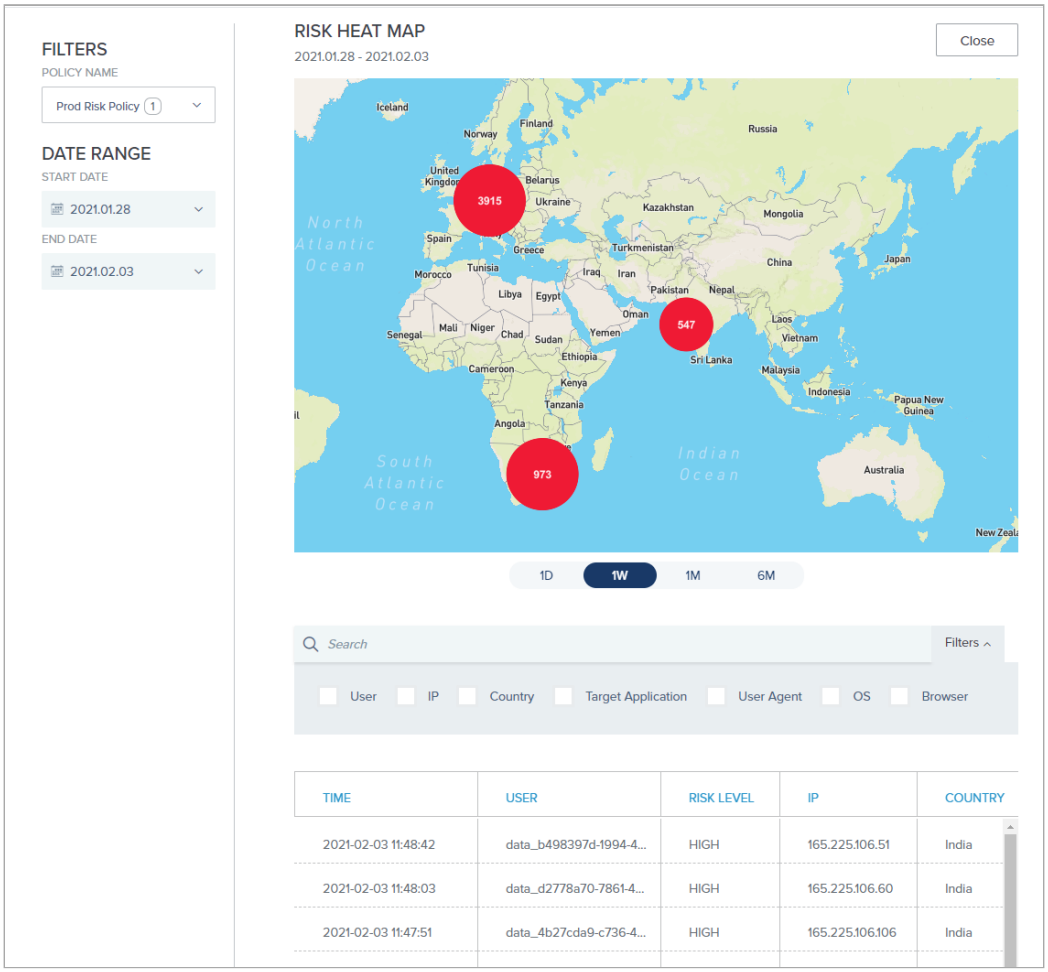
Risk heat map

The **Risk Heat Map** shows the location of high-risk events on a world map.

You can use the **Risk Heat Map** to determine where high-risk transactions have originated. The circles vary in size according to the number of high-risk transactions in that area.

To access the **Risk Heat Map**, go to **Monitoring > Threat Protection**.

Copyright © 2025 Ping Identity Corporation



Click on a circle or use the scroll function to zoom in on a location.

The drill-down table shows more detailed information about each high-risk event, such as the IP address and the target application.

Only events with an overall risk level of High are shown.

Scroll to the right to see additional columns. Learn more about using the filtered search bar in Filtered searching.

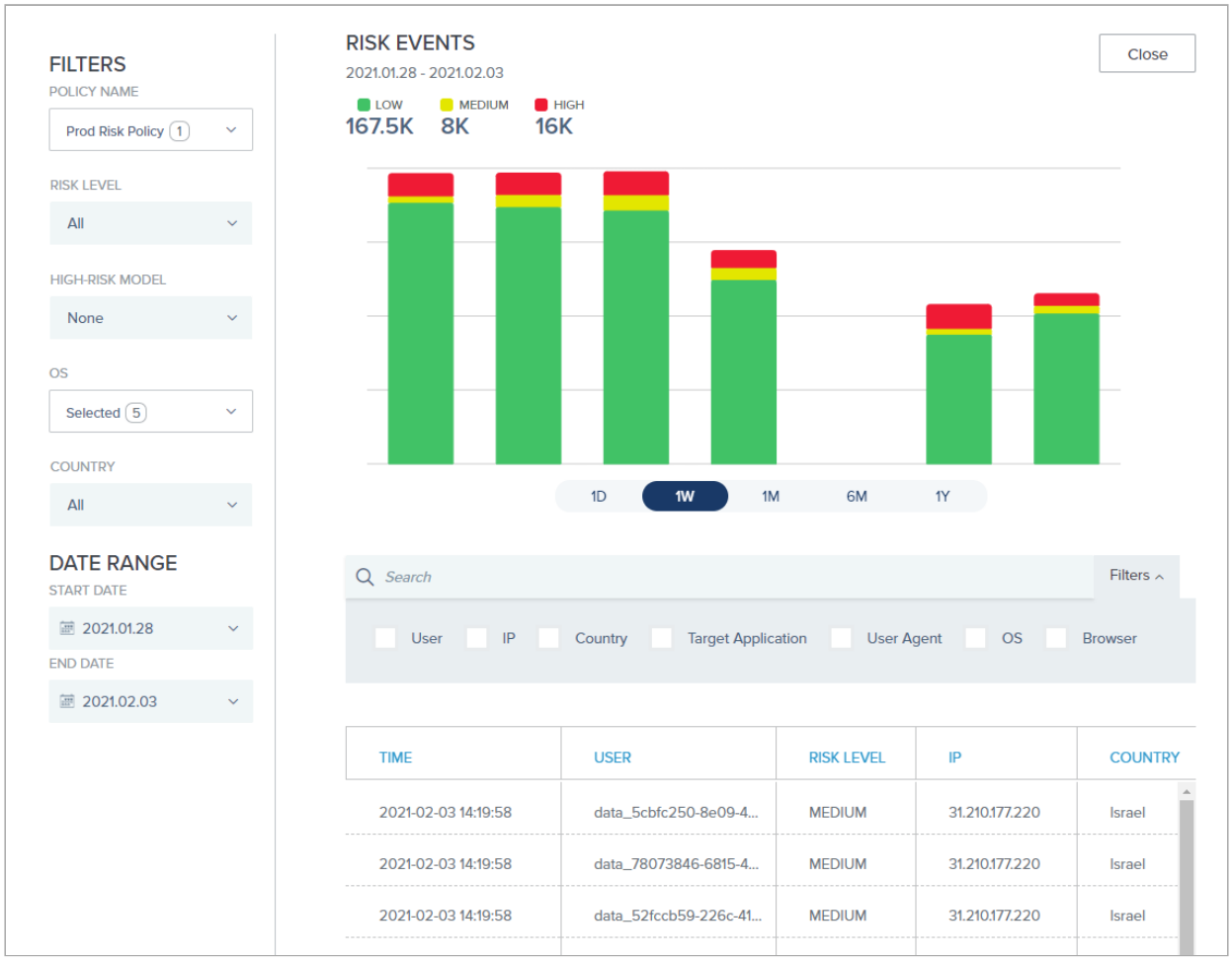
Zooming in on a location filters the results on the drill-down table. You can click a column header to sort the results by that value. Results are sorted by the **Time** column by default, with the most recent entries listed first.

Risk events

The **Risk Events** chart shows the distribution of risk levels in a given time period. The risk levels are determined by the selected risk policies.

To access the **Risk Events** dashboard, go to **Monitoring > Threat Protection**.

Copyright © 2025 Ping Identity Corporation



The drill-down table shows more detailed information about each risk evaluation event, such as IP address and target application.

Scroll to the right to see additional columns. Learn more about using the filtered search bar in Filtered searching.

Click a column header to sort the results by that value. Results are sorted by the **Time** column by default, with the most recent entries listed first.

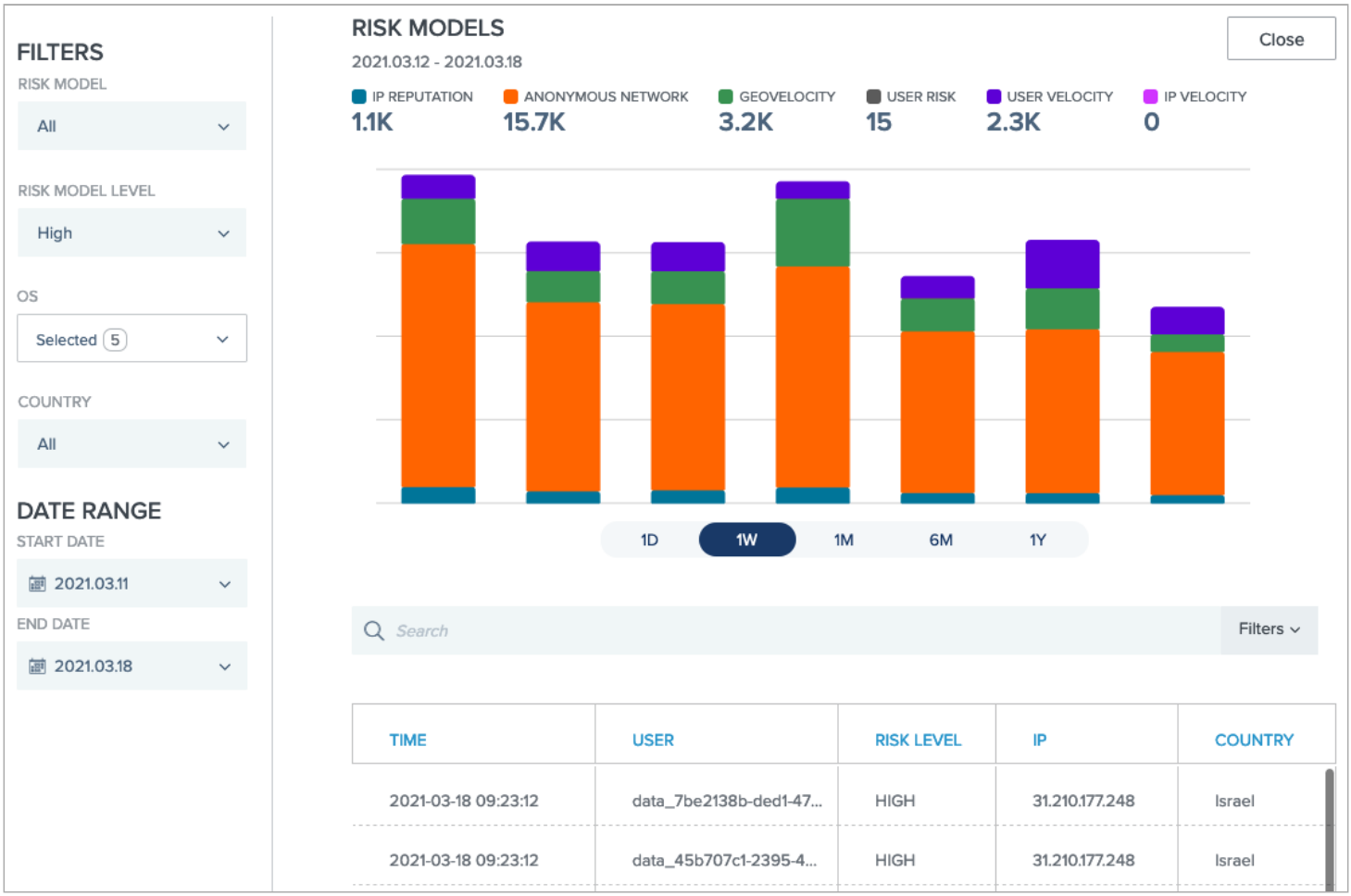
High risk models

The **High Risk Models** chart shows the distribution of each type of risk model, regardless of the configured risk policy.

You can use the **High Risk Models** chart to see which risk factors are most prevalent.

To access the **High Risk Models** chart, go to **Monitoring > Threat Protection**.

Copyright © 2025 Ping Identity Corporation



The drill-down table shows more detailed information about each risk evaluation event, including user, IP address, and target application.

Scroll to the right to see additional columns. Learn more about using the filtered search bar in Filtered searching.

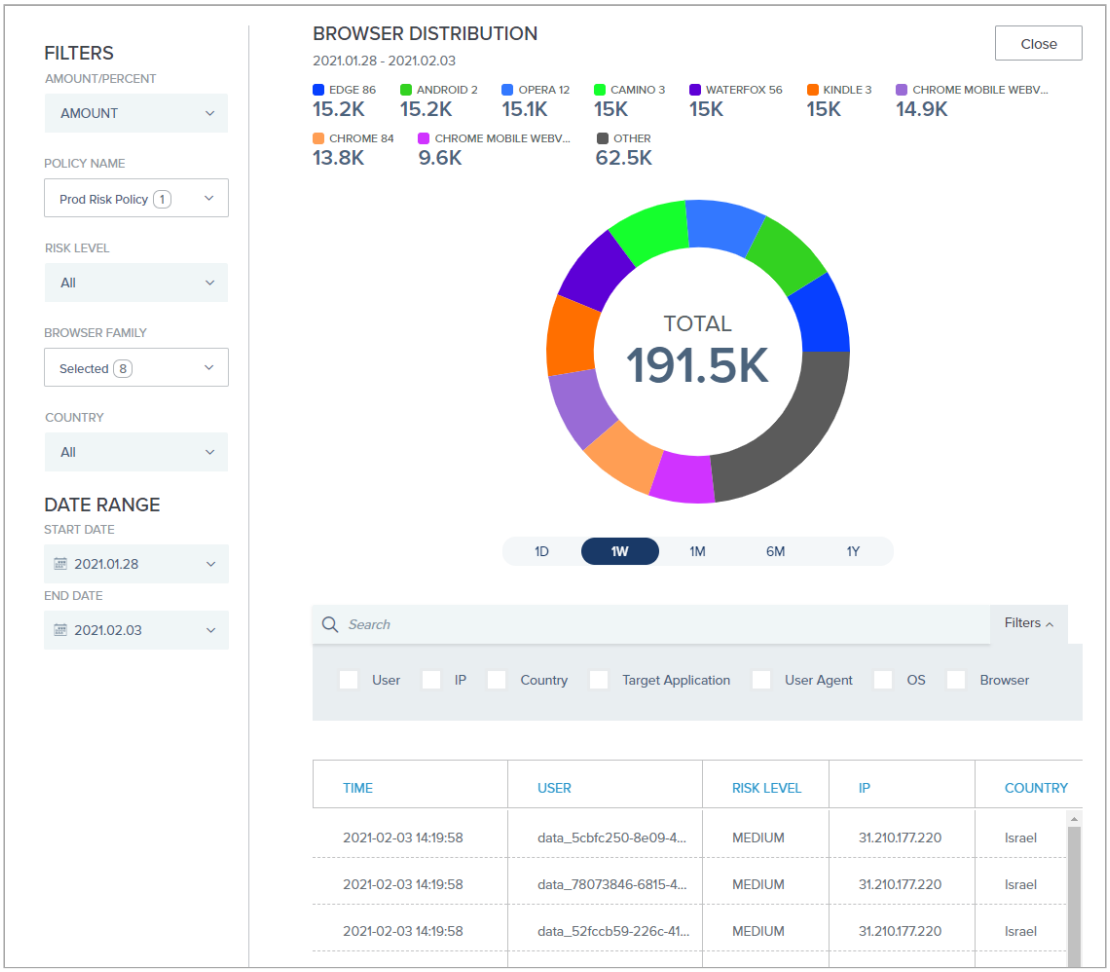
You can click a column header to sort the results by that value. Results are sorted by the **Time** column by default, with the most recent entries listed first.

Browser distribution

The **Browser Distribution** chart shows the number of recorded risk evaluations by user browser family.

To access the **Browser Distribution** chart, go to **Monitoring > Threat Protection**.

Copyright © 2025 Ping Identity Corporation



The drill-down table shows more detailed information about each risk evaluation event, such as IP address and target application.

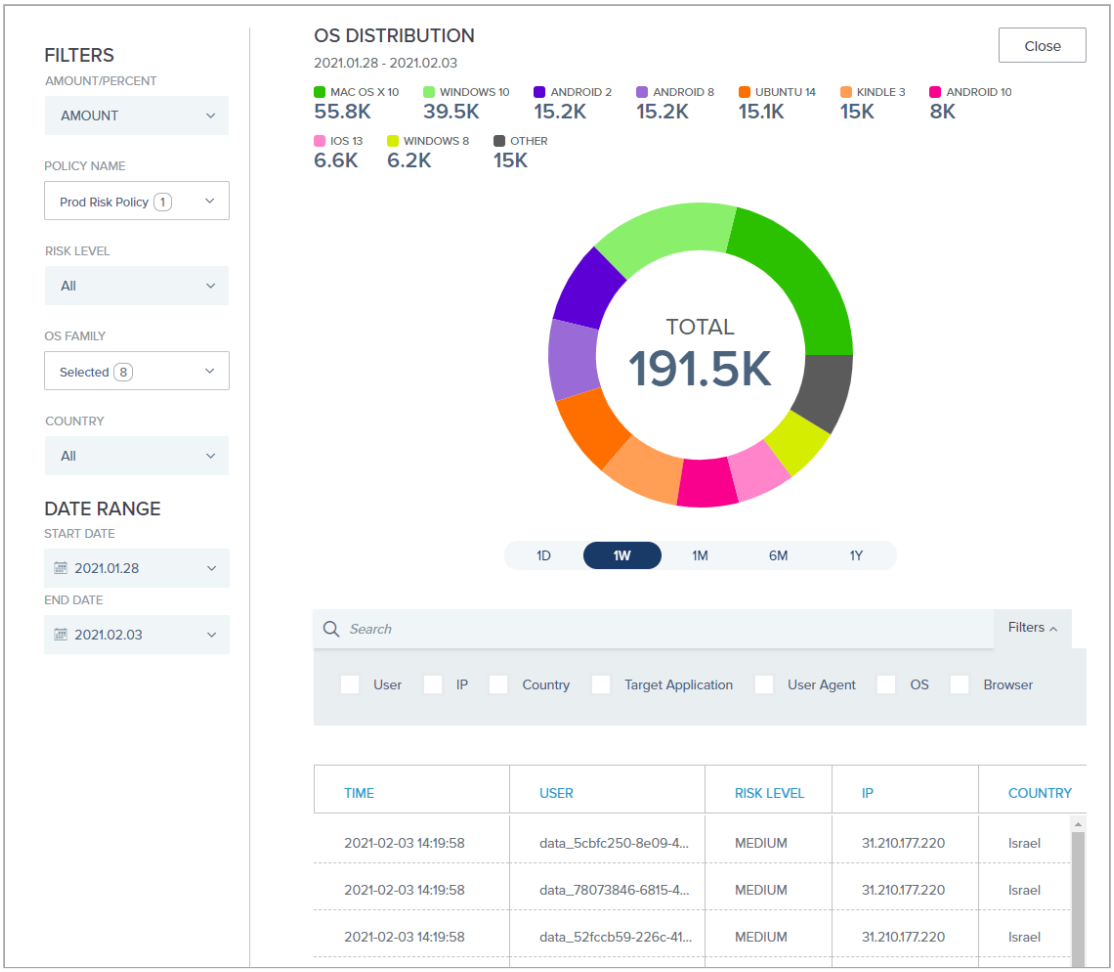
Scroll to the right to see additional columns. Learn more about using the filtered search bar in Filtered searching.

You can click a column header to sort the results by that value. Results are sorted by the **Time** column by default, with the most recent entries listed first.

OS distribution

The **OS Distribution** chart shows the number of recorded risk evaluations by user operating system type.

To access the **OS Distribution** chart, go to **Monitoring > Threat Protection**.



The drill-down table shows more detailed information about each risk evaluation event, such as IP address and target application.

Scroll to the right to see additional columns. Learn more about using the filtered search bar in Filtered searching.

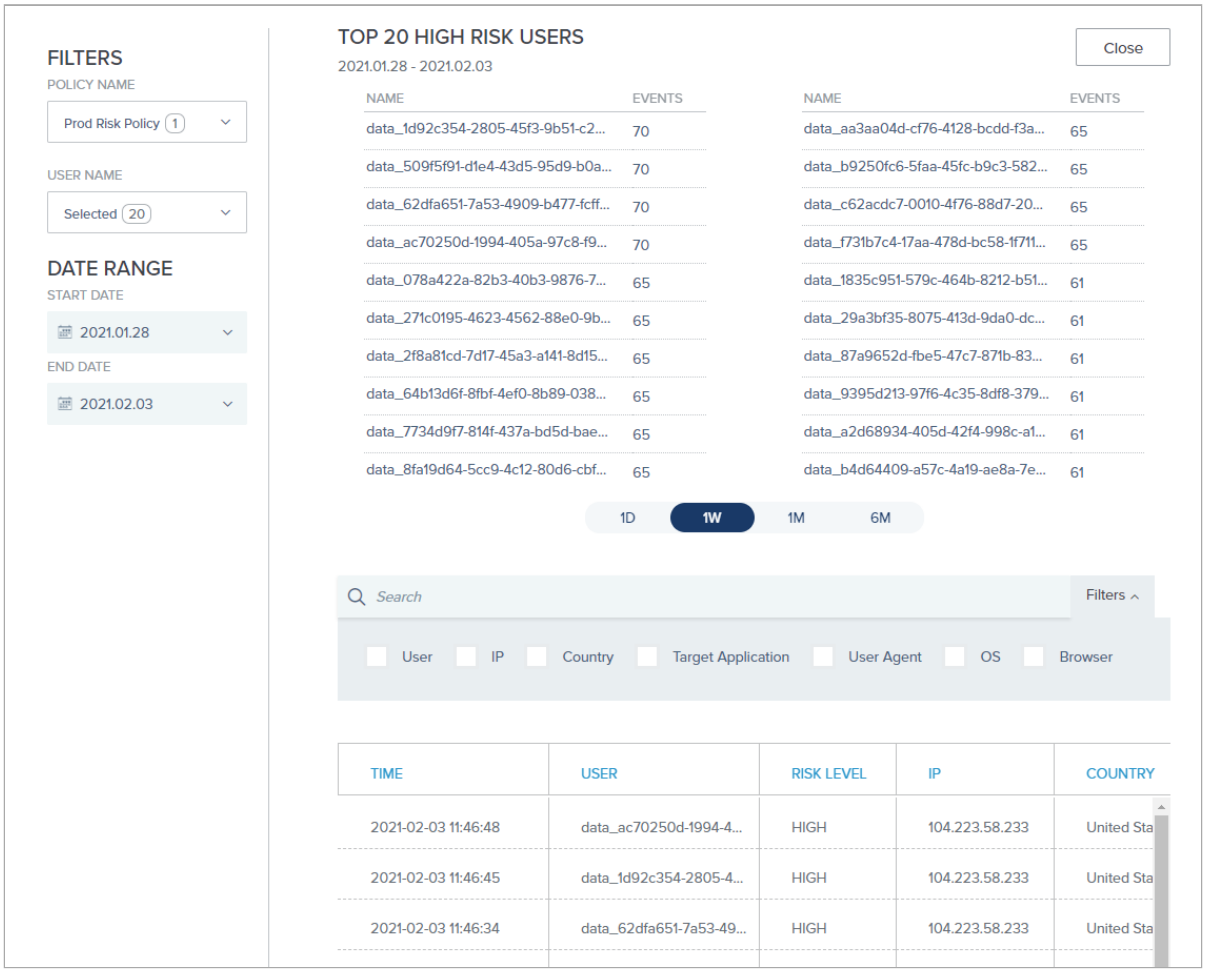
You can click a column header to sort the results by that value. Results are sorted by the **Time** column by default, with the most recent entries listed first.

Top 20 high risk users

The **Top 20 High Risk Users** chart shows the top 20 high-risk users and their respective number of high-risk events.

To access the **Top 20 High Risk Users** chart, go to **Monitoring > Threat Protection**.

Copyright © 2025 Ping Identity Corporation



The drill-down table shows more detailed information about each risk evaluation event for the user, such as IP address and target application.

Scroll to the right to see additional columns. Learn more about using the filtered search bar in Filtered searching.

You can click a column header to sort the results by that value. Results are sorted by the **Time** column by default, with the most recent entries listed first.

Risky IP

The **Risky IP** chart lists the high-risk IPs that have been encountered most frequently during risk evaluations. For each such IP, it shows the total number of events and information such as last location and internet service provider (ISP).

The chart also allows you to view detailed information for each of the risk evaluation events for the high-risk IPs.

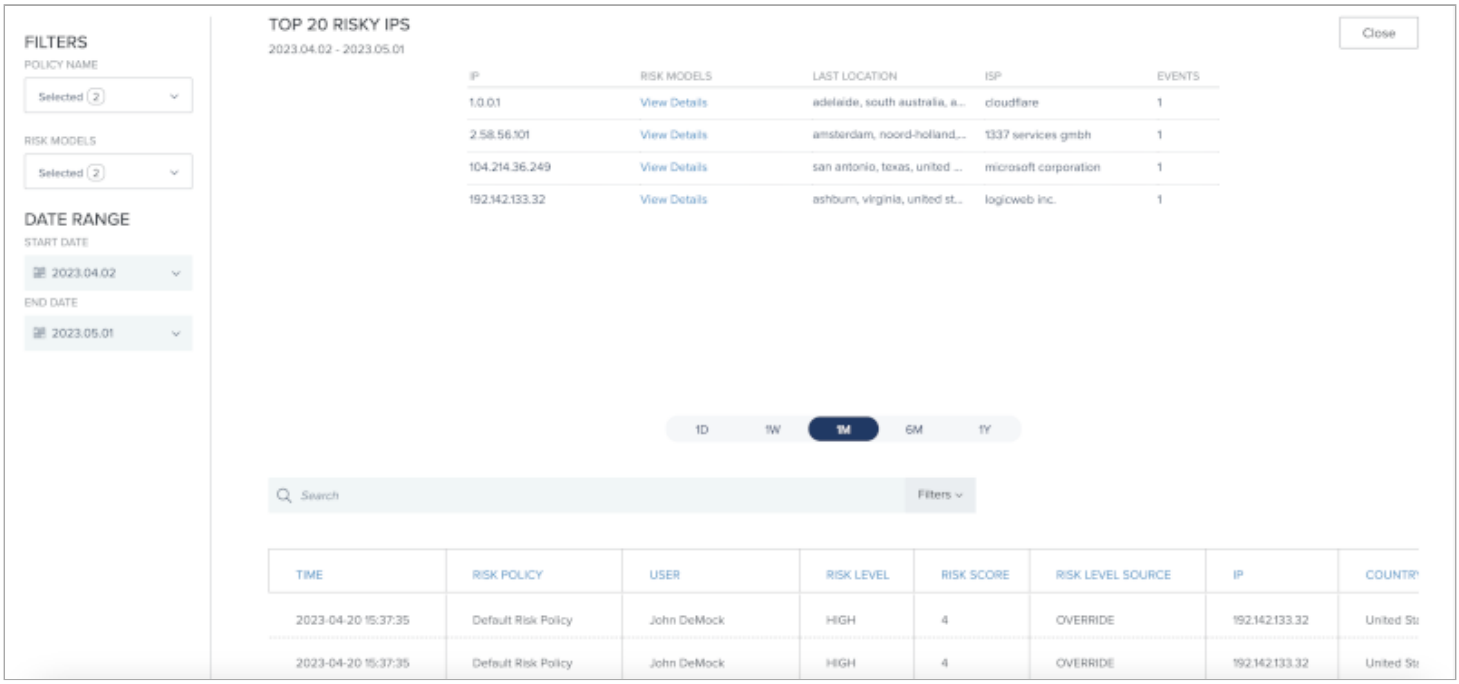
To display only a subset of the IPs or of the individual events, use the time period selector and the search bar.

To get a more exact date range, use the filter in the sidebar.

To see why an IP was categorized as high-risk, click **View Details**.

When you review the listed IPs, you might see that some IPs are categorized as high-risk, but they're IPs that you know are used by legitimate users. You can then add these IPs to the allow list in the relevant risk predictor, such as anonymous IP risk predictor, or define a composite predictor where you map the relevant ISP or IP range to low-risk level.

After you have added any IPs in the chart to the allow list, you can identify the high-risk IPs and deal with them in the framework of a risk policy or handle them with other tools that your organization uses.



PingOne Signals (Protect) SDK

You can use the PingOne Signals (Protect) SDK to obtain information for additional risk-related variables and then pass this information on to the risk evaluation.

Learn more in the Signals SDK documentation.

The Signals SDK can be used in conjunction with the PingOne Protect Integration Kit for PingFederate or PingOne Risk Integration Kit for PingFederate, with the PingOne Protect API, or as part of a flow designed with DaVinci.

Learn more about these different methods in:

- Integrating device profiling (PingOne Protect Integration Kit for PingFederate)
- Integrating device profiling (PingOne Risk Integration Kit for PingFederate)
- Creating risk evaluations (Protect API)
- PingOne Protect connector (DaVinci)

Copyright © 2025 Ping Identity Corporation

Best practices for PingOne Protect

Follow these recommendations to get the most out of PingOne Protect.

Risk policies

- When you add the PingOne Protect service to a PingOne environment, it includes a default risk policy. You should use this policy for your initial testing of risk evaluations. After you've seen how this default policy affects the flow experience for your users, you can go back and fine-tune it by customizing individual predictors. You can also create multiple risk policies.
- Train risk models with production data for 1-3 weeks for workforce usage or 2-4 weeks for customer usage. This should be done with the default risk policy.
- Use the PingOne Protect dashboards to analyze the risk evaluation results. Identify false positive results, meaning situations that are identified as High risk even though they are interactions with legitimate users.

  Identify the causes of these false positives. Adjust the scores for the different risk predictors in the risk policy to try to reduce the incidence of false positives.
- Use score-based policies rather than weight-based policies. Score-based policies provide more control over the overall calculation because you can specify an exact numerical score that should be assigned when PingOne Protect determines that there is a medium or high-risk level for a predictor.

  > **Important**
  >
  > **Weights** in risk policies have been deprecated for new PingOne environments but can still be used in existing environments.
- Before modifying an existing risk policy that is in use, use a staging policy to test how the changes will affect risk evaluations.

Risk evaluation results

When a risk evaluation is performed, the PingOne API returns detailed information in addition to the overall risk level that was calculated on the basis of the risk policy used. This information includes data about the event, the user and the device used, and the risk results for the individual predictors in the risk policy. You can take these supplemental details into account when determining how to proceed in the flow.

When deciding how a flow should proceed based on the risk evaluation response, consider:

- The type of flow, such as initial registration, ordinary authentication to access an application, or authentication prior to a monetary transaction
- The specific risk factors included in the risk policy that was used
- The type of business need, such as security needs vs. need for less friction in the user experience, or the frequency of fraud instances
- The various risk mitigation tools you have available, for example, MFA or knowledge-based authentication (KBA)

You can also use the detailed information in the response to better understand what led to the overall risk level and then fine-tune your risk policies.

Copyright © 2025 Ping Identity Corporation

The following are the key details returned in the response, ordered by level of importance.

Response detail	Recommendation
`result.recommendedAction`	In some cases, a specific course of action is recommended. For example, when the calculated risk level is HIGH and a bot is suspected, there is a recommendation to carry out the additional bot mitigation steps that your organization has available.
`result.value`	This field has a value only if you defined an override in your policy and included text in the **Notes** section.
`result.level`	The overall risk level calculated. • When the risk level is equal to LOW, the flow should probably continue without providing any additional friction for the user. • When the risk level is equal to MEDIUM, an MFA challenge should probably be issued, although in some scenarios, you may decide that even at this level there is no need for any additional friction. • When the risk level is equal to HIGH, you should present a challenge stronger than an ordinary MFA push. **Note** Because there are conditions where a HIGH risk level will be returned even for legitimate users, you should probably not block a user completely in such situations.
`result.score`	The raw risk score before the conversion to the LOW/MEDIUM/HIGH risk level. This provides a higher degree of granularity, and you can check how much the score exceeds the thresholds used for converting to risk level.

Predictors

- Ordinarily, you do not need to have more than one predictor of each type, for example User Location Anomaly. However, when you have different types of users, you might want to have multiple versions of the predictor so that you can use different versions in different risk policies.

  For example, if you have users who travel frequently, you could create one User Location Anomaly predictor that assigns a risk level of High if a user authenticates from outside the radius that you defined and create a second, more lenient User Location Anomaly predictor that can be applied to the users who travel frequently.

Copyright © 2025 Ping Identity Corporation

- If you use composite predictors, it will usually be to combine multiple types of predictors when you are interested in the interaction between them, such as assigning a risk level of High for authentications from an anonymous network only if there is also a user location anomaly.

  However, there are situations where you might want to combine multiple predictors of the same type. For example, a Geovelocity predictor allows you to compose an allow list of up to 400 IPs. To compose a larger list of allowed IPs, you can create a composite predictor that contains two different Geovelocity predictors.

Signals (Protect) SDK

- Implement the Signals (Protect) SDK in your applications. Certain risk predictors, such as the New Device predictor, rely on the supplemental risk-related information that is supplied by the Signals SDK.

Flows in DaVinci

- Each flow where you include a risk evaluation should include two different PingOne Protect connectors:
  - Add a connector with the `Create Risk Evaluation` capability at a point in the flow where you want to base the next action on the risk score assigned. For example, show an MFA prompt for MEDIUM or HIGH, but automatically grant access if the risk is deemed LOW.
  - Add a connector with the `Update Risk Evaluation` capability at a point in the flow after authentication has been completed. This capability represents the system's ability to learn over time in order to improve results. Always include an update connector in your flows because the learning mechanism is essential for risk evaluation precision.
- Use the `skrisk` component in your flow to automatically obtain the information from the Signals SDK.

  > **Note**
  >
  > This approach can only be used for web applications. For iOS or Android apps, you must manually implement the steps described in the SDK documentation, and then include in your flow a variable that represents the data obtained from the SDK.

- In the HTTP connector that you add before the connector that creates the risk evaluation, make sure that the `skrisk` component is at the beginning of the HTML template. All HTML tags that you add should be below the `skrisk` component in the **HTML Template** field.

Troubleshooting PingOne Protect

The following tips can help you solve problems that you have encountered when working with PingOne Protect.

I don't see the Bot Detection and Suspicious Device predictors

The Bot Detection and Suspicious Device predictors were added as part of the expansion to PingOne Protect. While you can still use the basic risk functionality with your existing PingOne Risk license, to use the new predictors, you must upgrade to a PingOne Protect license.

Copyright © 2025 Ping Identity Corporation

When creating a new environment, I don't see the option to add the PingOne Risk service

If you have a PingOne Protect license, the service to add is now called PingOne Protect.

Predictor does not return a risk level value. Reason given is "Not enough information to access risk score"

This might occur for a number of reasons:

- The predictor hasn't finished the required training period.
- Predictors learn only from successful transactions. Make sure that all your flows include updating the risk evaluation after the transaction has been completed. For the integration with PingFederate, this is handled automatically.
- The predictor is dependent upon input from the Signals (Protect) SDK, but the output from the SDK is missing. To resolve this issue, see the next section.

Risk evaluations that use predictors that are dependent upon input from the Signals (Protect) SDK do not seem to contain the output from the SDK

This occurs when the Signals SDK is not successfully loaded and run during the transaction.

The simplest way to check that the output from the SDK was received is to look at the API response for the evaluation and verify that it contains a value for `details.device.id`. You can also view the returned object in the entry for the event in the audit log in the PingOne admin console by going to **Monitoring > Audit**.

To help pinpoint the problem, use your browser's Developer tools while a transaction is carried out to confirm that the SDK was initialized and that the payload was generated. The **Console** tab of the Developer tools shows the relevant events or any errors that occur.

If you don't see the relevant events, take a look at the **Network** tab of the Developer tools to see why these scripts failed to load:

- `pingone-risk-profiling-signals-sdk.js`
- `pingone-risk-management-embedded.js`
- `signals-sdk.js`

The failure of the scripts to load can be because of browser plugins, network access rules, or company policies.

After the underlying issue has been addressed, try the risk evaluations again and use the **Console** tab to confirm that the SDK was successfully loaded and initialized.

I am having trouble with my PingOne DaVinci flow that includes risk evaluation

- You can find general tips on debugging DaVinci flows in Debugging and Analytics.
- If you have included the `skrisk` component in your flow, make sure that you have followed the instructions in PingOne Protect Connector.

Copyright © 2025 Ping Identity Corporation

I am having trouble with risk evaluations after installing and configuring the PingOne Protect Integration Kit (or PingOne Risk Integration Kit)

- Learn more about troubleshooting issues involving the PingOne Protect Integration Kit in the troubleshooting section for the integration kit.
- Learn more about troubleshooting issues involving the PingOne Risk Integration Kit in the troubleshooting section for the integration kit.

Fallback value is not being assigned correctly to one of my predictors

Verify that you did not select Medium as the fallback value for a predictor that is boolean in nature, such as geovelocity predictors. For such boolean predictors, you must set the fallback value to None, Low, or High.

Copyright © 2025 Ping Identity Corporation

Identity Verification using PingOne Verify

The PingOne Verify service lets you enable secure user verification based on a government-issued document and live face capture (a selfie).

Getting started

- What is PingOne Verify?
- Getting started with PingOne Verify

Tutorials

- Configuring PingOne Verify
- Enable user ID verification
- Reset a user's ID verification status
- Manually approve a user's ID
- Creating a verify policy

Integrations and Connectors

- Ping Identity Integration Directory
- PingOne Verify Integration Kit
- PingOne Verify Connector
- PingOne Verify AIC Node

DaVinci orchestration flows

- PingOne Verify Quickstart DaVinci Flow

Copyright © 2025 Ping Identity Corporation

Developer resources

- Get started with PingOne APIs
- PingOne Verify
- PingOne Verify Native SDKs
- Verify transactions
- Verify status

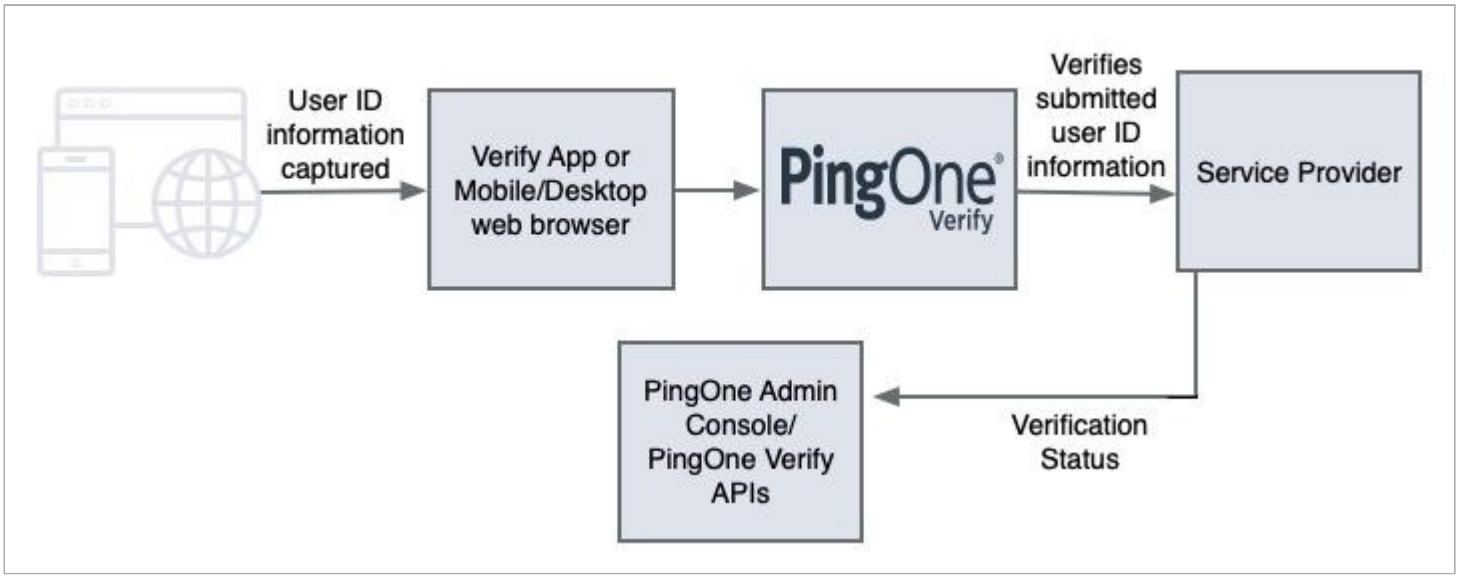
Troubleshooting

- Audit logs
- System status

Introduction to PingOne Verify

PingOne Verify service is a part of the PingOne Neo decentralized identity solution that enables secure user verification based on a government-issued document, live face capture (a selfie), and voice biometrics, ensuring users are who they claim to be. Learn more in PingOne Neo.

Copyright © 2025 Ping Identity Corporation



1. The user ID information is captured on a user's iOS or Android device using the customer-created Verify app or using a user's mobile web browser. User ID information can also be captured through the top 5 desktop browsers with an integrated camera or external web camera. After it has been captured, the user ID information is then sent to the PingOne ID Verification service.

   > **Note**
   >
   > Mobile and desktop web verification does not require a user to download the Verify app.

2. The PingOne ID Verification service interacts with a SP that verifies the submitted user ID information.
3. When a user's ID information is successfully verified, the PingOne ID Verification service approves the user authentication, and the verification status is available through the PingOne Verify APIs and the PingOne admin console.

Learn more in Identity Verification Dashboard.

> **Note**
>
> Only the ID verification status is retained by PingOne. Any personally identifiable information (PII data) passed to PingOne is deleted by the ID Verification service.
> Identity document verification uses two methods to extract personally identifiable information (PII): barcodes and optical character recognition (OCR). Learn more in A note extracted on data in the Verified Data API doc.

To set up and configure PingOne Verify, you'll use:

- The PingFederate admin console to configure the PingOne Verify Integration Kit
- A mobile or desktop web browser or the PingOne Verify mobile SDKs
- The PingOne admin console or the PingOne Verify REST APIs

Copyright © 2025 Ping Identity Corporation

PingOne Verify transactions flow

An authentication policy for PingOne Verify is configured in the PingFederate Integration Kit for PingOne Verify. The authentication policy can enable ID verification for all users in a PingOne environment. Learn more in the PingOne Verify Integration Kit.

1. When ID Verification is enabled for a user, the user's first attempts to sign on or register triggers the display of instructions from the mobile or desktop web browser or the customer Verify app created for the iOS or Android device.
2. The user is instructed to scan a QR code. This code links to an ID Verification transaction ID assigned to the user by the ID Verification service. The ID Verification service then sends the transaction ID to the mobile or desktop web browser or the customer Verify app on the user's device.
3. The customer Verify app then instructs the user to submit one of the following:
   - A photo of their driver license or a photo of their passport information page (the page containing their passport photo)
   - A live face photo (selfie)
   - A live sample of their voice

   > **Note**
   >
   > A live sample of the user's voice can also be recorded through a support call center and collected by the PingOne Verify APIs.
   > If the ID verification fails more than three times in a 1-hour period, the user must wait an hour before trying again.
4. The mobile or desktop web browser or the customer Verify app sends the collected data to the ID Verification service with the transaction ID received from the ID Verification service.
5. The ID Verification service then verifies the user information with the SP used for verification. When the ID Verification service receives the results from the SP:
   - The user's ID verification status is stored in PingOne. Only the ID verification status is retained. Any PII passed to PingOne is deleted by the ID Verification service.
   - For voice verification, PingOne removes identifying features from the user's raw voice sample to create a voice template. The voice template, or voiceprint, is stored in PingOne for future verifications.
   - If the ID verification wasn't successful, depending on the policies set in the PingOne Verify Integration Kit, a message and another QR code to scan are displayed in the customer Verify app or the mobile web browser. There is a limit of three attempts per user per hour.
6. For all subsequent attempts to SSO to PingOne, the authentication policy uses the ID Verification service to check the user's ID verification status stored in PingOne.

Custom domains

Because PingOne Verify supports custom domains, your domain name can appear in any browser-based user interface that's presented to end users. PingOne routes your domain name to the relevant PingOne services. Learn more in Domains.

Copyright © 2025 Ping Identity Corporation

Branding and themes

PingOne Verify supports branding and themes to easily change the look of your registration pages, sign-on pages, and verification pages for a particular environment. Learn more in Branding and themes.

Email and phone notifications templates

PingOne Verify supports email and phone notifications templates so that you can create a notification for end users to verify their email address or phone number. Learn more in Notification templates.

Metrics collection and messaging

PingOne Verify supports metrics collection and messaging for admin users to collect and audit PingOne Verify transaction events, such as the Verify App event. Learn more in Webhooks.

Language localization

PingOne Verify supports language localization so end users can interact with PingOne Verify in their preferred language. Learn more in Configuring PingOne Verify language localization.

Getting started with PingOne Verify

With PingOne Verify, you can integrate identity verification directly into your mobile app.

Using the PingOne Verify mobile SDK, you can prompt your customers to provide proof of identity, streamlining customer identity verification, while preventing fraud and abuse, by capturing live facial image and voice, scanning and validating government-issued identity documents, and confirming they match, all within your app.

Configuring PingOne Verify

Configure and integrate PingOne Verify into your user identity verification flow.

Before you begin

Regardless of the configuration method you choose, you'll need:

- A PingOne account with at least one environment that includes the PingOne Verify service. Learn more in Starting a PingOne trial and Creating an environment.
- A PingOne Verify policy. Learn more about configuring a policy in Creating a verify policy.

About this task

There are five ways to configure PingOne Verify:

- API integration
- PingOne DaVinci
- PingFederate Integration Kit

Copyright © 2025 Ping Identity Corporation

- Mobile SDK
- PingOne Advanced Identity Cloud and PingAM

The configuration method that you choose depends on your role.

Role	Configuration Method
Admins and developers	Typically use the PingOne REST API or PingOne DaVinci to get started quickly and test a verify transaction.
PingFederate admins	Use the PingFederate admin console to configure the PingOne Verify Integration Kit. PingFederate supplies the authentication policy and user verification status for PingOne Verify.
Mobile developers	Use the PingOne Verify mobile SDK (iOS or Android) to create the app your users employ for ID verification.
Advanced Identity Cloud and PingAM admins	Use verification nodes in an authentication journey.

Integrating PingOne Verify with user authentication journeys

Advanced Identity Cloud is a digital identity and access management (IAM) software as a service (SaaS) solution for any identity, workforce, or consumer.

PingAM software manages access to resources, such as web pages, applications, or web services, that are available over a network. PingAM centralizes access control by handling both authentication and authorization.

To take advantage of PingOne Verify features, you can integrate PingOne Verify nodes into your Advanced Identity Cloud and PingAM journeys. Learn more in Journeys.

Use the following nodes to integrate PingOne Verify with Advanced Identity Cloud and PingAM:

- PingOne Verify Evaluation node
- PingOne Verify Completion Decision node

> **Note**
>
> For self-managed deployments, these nodes are available only from PingAM 8.0 onwards. If you're using an earlier version of PingAM, use the corresponding Marketplace nodes.

Copyright © 2025 Ping Identity Corporation

PingOne API

Using the PingOne REST API
About this task

To configure PingOne Verify with the PingOne REST API:

Steps

1. Create your theme in PingOne Branding and themes to brand the PingOne Verify web experience for your end users.
2. (Optional) Use language localization to configure one or more languages and modify the PingOne Verify text fields that are presented to end users.
3. (Optional) If you enabled one-time passcode (OTP) through phone or email verification in your policy, create notification templates.
4. Trigger your first Verify transaction:
    1. Read Getting started with the PingOne APIs.
    2. Download the PingOne Postman collection.
    3. Note the variables you must value.
    4. Obtain a PingOne access token.

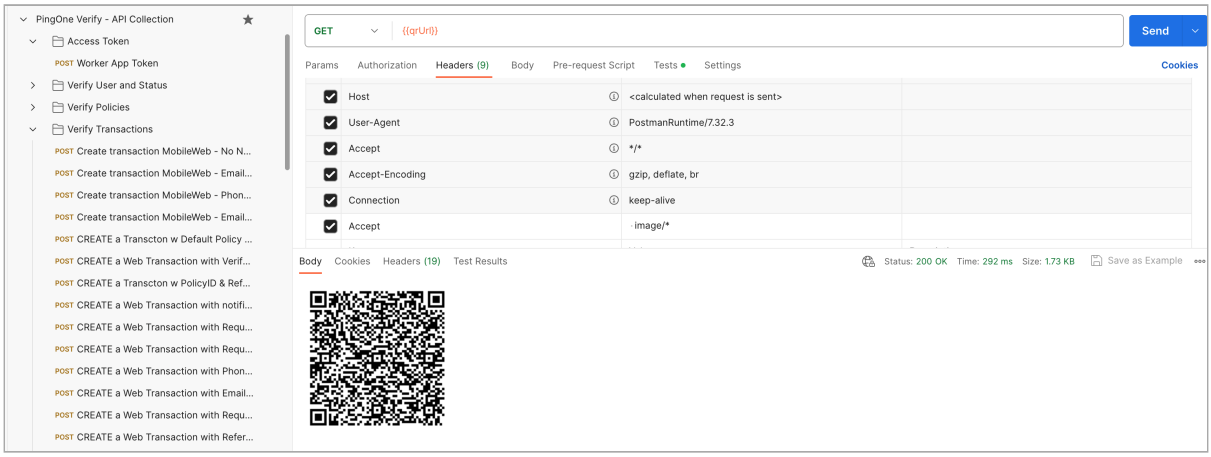
       Your *{{authPath}}* environment variable in Postman should begin with `auth.pingone`. See PingOne API domains to determine the correct *{{authPath}}* for your region. Note that nothing trails the domain in the *{{authPath}}* variable.
    5. Create a new Verify transaction with the Create Verify Transaction API call.

       Your *\{{apiPath}}* environment variable in Postman should begin with `api.pingone`. See PingOne API domains to determine the correct *\{{apiPath}}* for your region. Note that the trailing `/v1` is required (for example, `api.pingone.com/v1`).

       For more information, see PingOne API requests.

       Result:

       Postman renders a QR code.



6. Scan the QR code with a smartphone camera to try the mobile web flow.

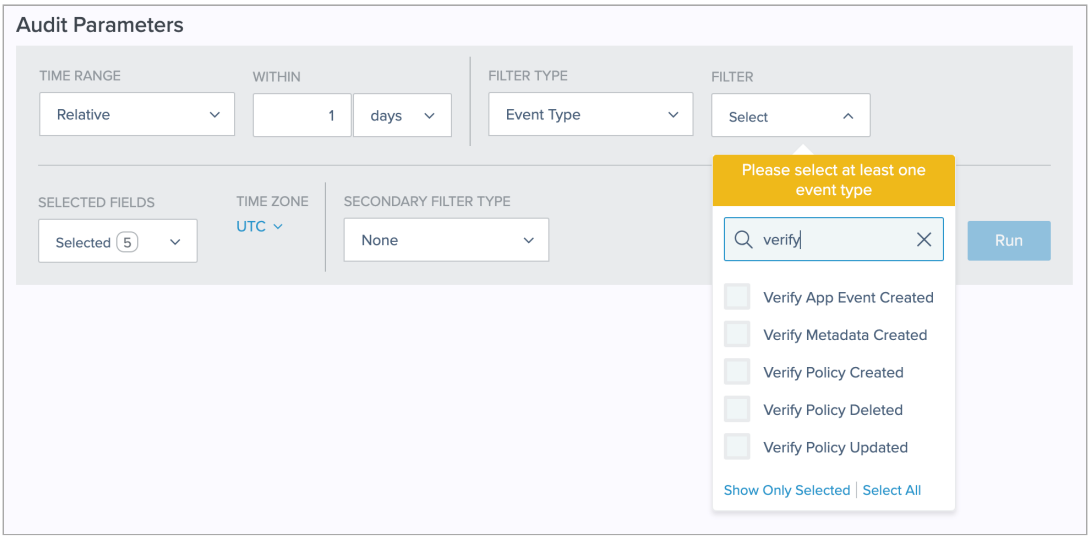
5. View the data submitted in the transaction and the scores returned from verification services.

   Choose from:

   - Using the API: Use the Verified Data and Meta Data endpoints.
   - Using the PingOne admin console:

     1. In PingOne, go to **Environment → Audit**.
     2. Edit the **Time Range** and **Within** fields as needed.
     3. For **Filter Type**, select **Event Type**.
     4. For **Filter**, enter `verify` in the **Search Filter Type** field.
     5. Select any of the **Verify** event types.

> **Note**
>
> You can find a complete list of events logged in PingOne in Audit Reporting Events in the PingOne API documentation.



Copyright © 2025 Ping Identity Corporation

6. Click **Run**.
7. To view the specific data and scores from an event, click **View** in the **Details** column in the report summary.

Copyright © 2025 Ping Identity Corporation

PingOne DaVinci

Using PingOne DaVinci
Before you begin

Add PingOne DaVinci to your PingOne environment. For more information, see Creating an environment.

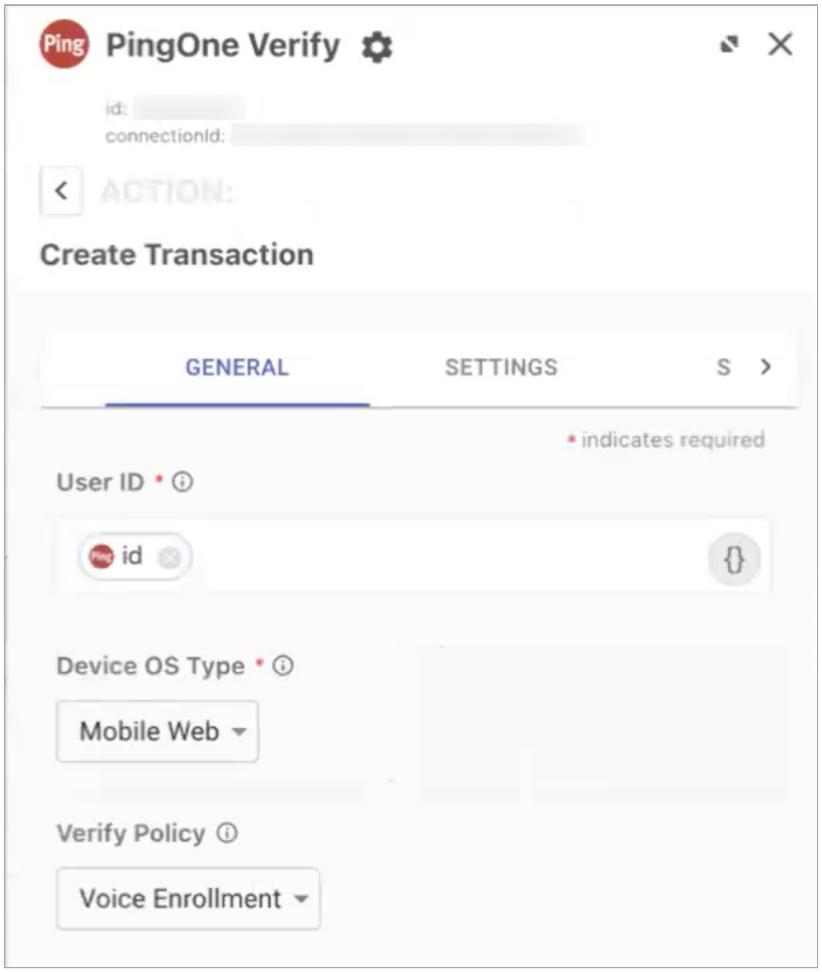
About this task

To configure PingOne Verify using PingOne DaVinci:

Steps

1. Create your theme in PingOne Branding and themes to brand the PingOne Verify web experience for your end users.
2. (Optional) Use language localization to configure one or more languages and modify the PingOne Verify text fields that are presented to end users.
3. (Optional) If you enabled OTP through phone or email verification in your policy, create notification templates.
4. Import a flow template in PingOne DaVinci by downloading it from the Integration Directory: PingOne Verify quick start flow template.
5. Update the flow with your PingOne Verify policy:
    1. Click the PingOne Verify `Create transaction` node in the flow.
    2. In the **Verify Policy** list, select the policy to use.

Copyright © 2025 Ping Identity Corporation

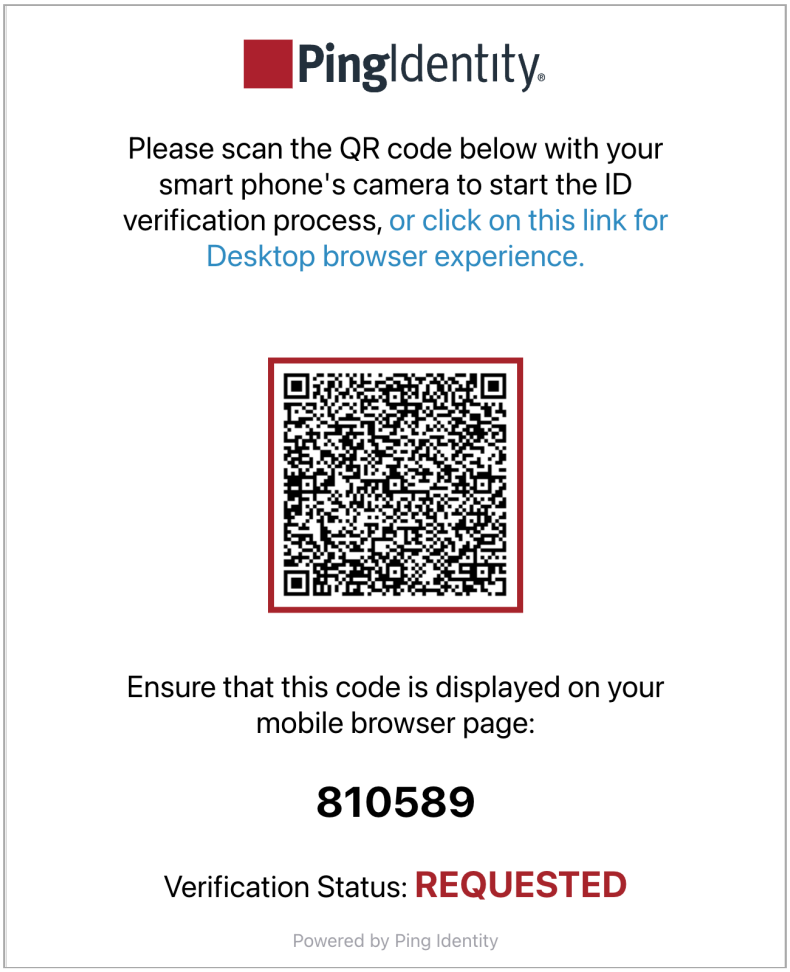


6. To run the flow and trigger a PingOne Verify transaction, click **Try Flow**.

   Result:

   PingOne DaVinci renders a QR code.

Copyright © 2025 Ping Identity Corporation



7. Scan the QR code on your mobile device to try the mobile web flow.
8. View the data submitted in the transaction and the scores returned from verification services.

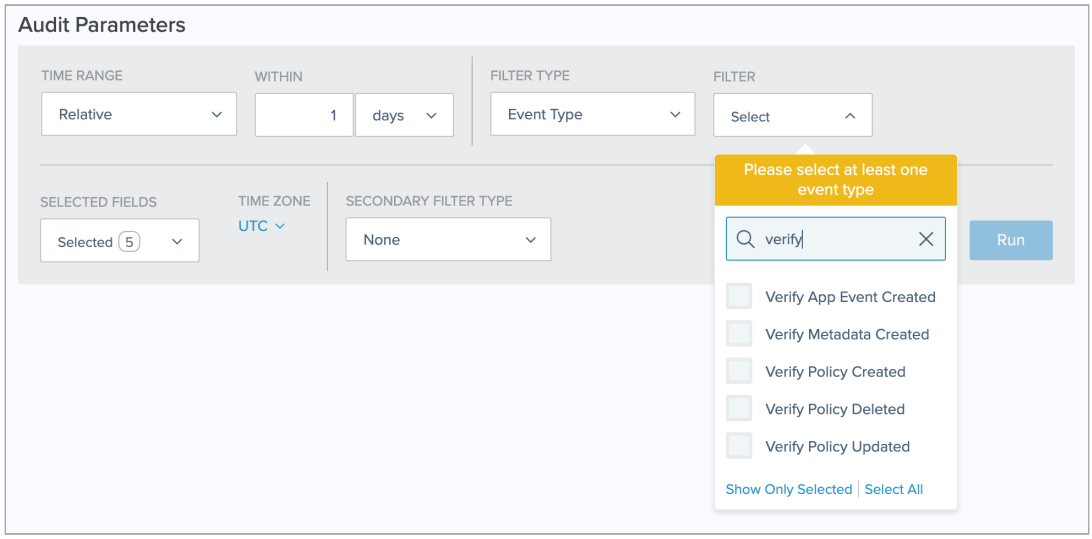
   Choose from:

   - Using the API: Use the Verified Data and Meta Data endpoints.
   - Using the PingOne admin console:

     1. In PingOne, go to **Environment → Audit**.
     2. Edit the **Time Range** and **Within** fields as needed.
     3. For **Filter Type**, select **Event Type**.
     4. For **Filter**, enter `verify` in the **Search Filter Type** field.
     5. Select any of the **Verify** event types.

     > **Note**
     >
     > You can find a complete list of events logged in PingOne in Audit Reporting Events in the PingOne API documentation.

Copyright © 2025 Ping Identity Corporation



6. Click **Run**.
7. To view the specific data and scores from an event, click **View** in the **Details** column in the report summary.

PingFederate

Using PingFederate
About this task

To use PingFederate to configure the PingOne Verify Integration Kit:

Steps

- Download PingFederate and the PingOne Verify Integration Kit from the PingFederate Downloads website.

> **Note**
> You'll need to work with your Ping Identity account team to start a trial license for PingFederate.

Learn more about getting started in the PingOne Verify Integration Kit documentation.

Copyright © 2025 Ping Identity Corporation

Mobile SDK

Using the PingOne Verify mobile SDK
About this task

Mobile application developers use the PingOne Verify mobile SDK for iOS and PingOne Verify mobile SDK for Android to create the PingOne Verify app for their users. The app is a self-service app for iOS or Android devices that guides the user through the process of taking photos of their ID and a selfie and submitting the photos to PingOne for verification.

To use the PingOne Verify mobile SDK:

Steps

1. Run the sample app from Github:
   - Running the sample app for iOS
   - Running the sample app for Android
2. Integrate the PingOne Verify mobile SDK into your own app:
   - Integrating the PingOne Verify SDK into your own app (iOS)
   - Integrating the PingOne Verify SDK into your own app (Android)

Copyright © 2025 Ping Identity Corporation

PingOne Advanced Identity Cloud and PingAM

Integrating with PingOne Advanced Identity Cloud and PingAM
Before you begin

Make sure you have:

- A PingOne Advanced Identity Cloud or PingAM account. Getting started with PingOne Advanced Identity Cloud.
- A PingOne account. Learn more in Starting a PingOne trial.
- A verify policy configured in PingOne (or use the default verify policy).
- A worker application with the Identity Data Admin role assigned in PingOne.

About this task

To take advantage of PingOne Verify features, you can integrate PingOne Verify nodes into your Advanced Identity Cloud and PingAM journeys. Learn more in Journeys.

Steps

1. Configure the PingOne service in Advanced Identity Cloud.
2. Set up your user journey in Advanced Identity Cloud or PingAM with PingOne Verify nodes in the journey:
   - The PingOne Verify Evaluation node to start a new identity verification with PingOne Verify.
   - The PingOne Verify Completion Decision node to check the status of the last verify transaction.
   - The PingOne Verify Authentication node to integrate biometric authentication functionality in your journey.
   - The PingOne Verify Proofing node to integrate verification functionality using Government ID, Facial Comparison, and Liveness in a journey.
3. Validate that the PingOne Verify Evaluation node is working by doing the following:
   1. Configure the node with **Store Verification Metadata** and **Store Verified Data** enabled.
   2. Use a Scripted Decision node to return the node state and make sure the values of the `pingOneVerifyMetadata`, `pingOneVerifyVerifiedData`, and `pingOneVerifyEvaluationFailureReason` properties are what you expect. You can also run the journey with Debugging enabled.
   3. Add message nodes attached to individual results outputs to understand the flow.
4. Validate that the PingOne Verify Completion Decision node is working by doing the following:
   1. Use logger messages in your Completion processing script to determine the processing goals and outcomes, and monitor the log.
   2. Evaluate the `nodeState` values of the PingOne Verify nodes that were set in the script using a Scripted Decision node that returns the nodeState, or with the Debugger enabled
   3. Add message nodes attached to individual results outputs to understand the flow.

Copyright © 2025 Ping Identity Corporation

Next steps

After you've familiarized yourself with how PingOne Verify works and have it running:

- Learn more about ID verification in:
  - Resetting a user's ID verification status
  - Manually approving a user's ID
- Learn more about your PingOne Verify license and the quota of transactions allowed in Viewing license information.

PingOne Verify key concepts

To fully leverage the capabilites of PingOne Verify, familiarize yourself with the following key concepts:

- Documentation authentication
- Face verification

PingOne Verify and documentation authentication

Document authentication in PingOne Verify uses machine learning and multiple verification checks to assess the validity of a document presented by a user.

What is machine learning and how is it used in document authentication?

Machine learning (ML) is a branch of artificial intelligence that allows computers to recognize patterns and make predictions based on data. In the context of document authentication (DocAuth), ML is employed to assess whether a document is genuine or fraudulent by comparing the features of the submitted document to a trained model.

Machine learning helps detect:

- Printed or photocopied documents
- Document tampering, such as changes to security features like holograms, text, or watermarks
- Subtle forgeries, such as improper alignment of text or altered photos

Models are trained on thousands of document samples to identify genuine versus fake documents, allowing for more accurate detection over time.

This continual learning process improves the accuracy of the verification system, particularly in high-volume regions where more document types are processed.

What are the steps for Automated Document Authentication?

The document authentication process in PingOne Verify is as follows:

1. **Capture document**: The user captures images of the front and back of their identity document, typically using a mobile device.

Copyright © 2025 Ping Identity Corporation

2. **Classify document**: The system classifies the document based on type (passport, driver license, and so on) and region of origin, using machine learning models trained on various document types.
3. **Compare to model**: The captured document is compared against the pre-trained model for that document type. The model checks for specific security features such as watermarks, barcodes, and holograms that must match what's expected for an authentic document.
4. **Check for tampering or forgery**: The system checks for signs of forgery or tampering, such as photocopied or altered documents, misaligned text, and improper security features.
5. **Extract data**: Relevant data (for example, name, date of birth, document number) is extracted using Optical Character Recognition (OCR) or, when available, directly from encoded barcodes like the PDF417 found on many driver licenses.
6. **Deliver result**: The result is delivered as either a successful authentication or a failure, accompanied by specific failure reasons if applicable (for example, "Document appears to be a photocopy" or "Expired ID").

Types of document authentication

PingOne Verify offers multiple types of document authentication methods:

Document authentication method	Definition
Automated	Machine learning models handle the entire authentication process without human intervention. This is the fastest, most scalable option and is ideal for most standard use cases.
Manual	In specific situations where additional review is needed, manual verification can be performed by a human agent who reviews the document based on its visual features.
Step-Up	In high-risk scenarios or when automated verification fails, users could be required to perform a step-up authentication. This can include re-verifying their identity through an additional document authentication check after the initial process.

What is a false positive? What is a false negative?

In machine learning and document authentication, the terms false positive and false negative are important for understanding the accuracy of the system:

Term	Definition
False positive	Occurs when a fraudulent or altered document is incorrectly flagged as valid by the system. For example, if someone submits a doctored ID and the system verifies it as genuine, that is a false positive. This represents a security risk as unauthorized individuals could gain access to sensitive systems.

Copyright © 2025 Ping Identity Corporation

Term	Definition
False negative	Occurs when a valid, legitimate document is incorrectly flagged as fraudulent or invalid. For example, if a user's authentic ID is not verified due to poor image quality or unusual document features, this is a false negative. This can cause frustration for legitimate users trying to verify their identity.

> **Note**
>
> PingOne Verify minimizes both false positives and false negatives through continuous improvement of its machine learning models, though some level of both is expected because of the complex nature of document verification across various regions and document types.

PingOne Verify and face verification

Face verification in PingOne Verify uses face matching, liveness detection, and injection attack detection to prevent fraud and ensure that the user presenting an ID is who they say they are.

What is face matching and how is it used in face verification?

PingOne Verify uses machine learning (ML) to detect the presence of a face in a government-issued document and compares it against a live selfie captured by the user. The system returns a confidence score indicating the likelihood that the faces match.

Face verification consists of two primary machine learning applications:

- **Face detection**: Determines if a face is present in an image, identifying its location, scale, and orientation.
- **Face comparison**: Evaluates whether two faces match, accounting for variations in expression, facial hair, and age.

PingOne Verify uses both face detection and face comparison to generate a reliable confidence score in face matching between the live selfie captured and the portrait of the ID document.

Presentation attacks and liveness detection

Presentation attacks are when fraudsters attempt to bypass verification and physically present an artificial face to the camera by using printed images, digital screens, video replays, or masks. The types of presentation attacks are:

Printed photo attack

A fraudster presents a high-quality printed image of the victim's face.

Screen replay attack

A digital screen displays an image or video of the victim's face.

3D mask attack

A realistic 3D mask of the victim's face is worn.

Liveness detection prevents presentation attacks. Presentation Attack Detection (PAD) determines whether the face being presented is a real, live person rather than a fake representation.

Copyright © 2025 Ping Identity Corporation

Liveness detection methods are categorized into:

- **Active liveness**: Requires user interaction, such as blinking, smiling, or turning the head. While effective, it introduces friction and can be bypassed with deepfake technology, a type of artificial intelligence (AI) that creates realistic-looking videos and images.
- **Passive liveness**: Requires no user interaction and detects fraud in a single image using AI-based analysis.

PingOne Verify uses single-frame passive liveness detection, eliminating friction while maintaining security. While PAD is effective against physical fraud, it doesn't protect against digital manipulation attacks, such as deepfakes, that don't rely on a physical medium.

Single-frame liveness

Presentation attacks are prevented by liveness detection. Single-frame liveness leverages computer vision to detect features in an image that are invisible to the human eye.

AI models analyze factors such as:

- Lighting inconsistencies
- Pixel distortions
- Image artifacts from screen displays or printed documents

A deep neural network, trained on real and fraudulent images, assigns a liveness confidence score based on these subtle characteristics.

Deepfakes and injection attack detection

In injection attacks, fraudsters bypass the camera entirely and inject synthetic or manipulated biometric data, such as a deepfake, directly into the system.

These attacks are more sophisticated and harder to detect because the fraudulent image isn't captured by the camera itself. Instead, it's digitally inserted into the verification process. The types of deepfakes and injection attacks are:

Virtual camera attack

A software-based camera injects pre-recorded images, deepfake videos, or synthetic faces instead of real-time captures.

External camera manipulation

Fraudsters use hardware-based techniques to feed a fake video or image into the system.

JavaScript code injection

Fraudsters modify browser code or install plugins to intercept and replace biometric data before it reaches the verification system.

Deepfake injection

AI-generated deepfake faces are directly fed into the biometric system instead of real faces.

Copyright © 2025 Ping Identity Corporation

How are injection attacks prevented?

Injection attack detection works by analyzing and securing the channel through which biometric data is captured, rather than relying on confidence scores that assess the authenticity of an image or video.

Injection attack detection focuses on how the image reaches the system. This is done by monitoring signals that verify whether the camera input is coming from a real device camera or if it was manipulated through software, such as virtual cameras or code injections. These checks include analyzing hardware properties, device-level security features, and integrity signals to detect tampering.

For example, if a virtual camera or an external application attempts to simulate a camera feed, PingOne Verify will recognize this and reject the transaction.

Because these signals provide binary yes or no verification rather than confidence scores, they offer a highly reliable, non-bypassable method of detecting and blocking deepfake and synthetic identity fraud at the source. By ensuring that only genuine, real-time camera captures are accepted, injection attack detection strengthens biometric security without introducing unnecessary friction for legitimate users.

Configuring PingOne Verify language localization

Use language localization to configure one or more languages and modify the PingOne Verify text fields that are presented to end users in notification and agreements.

Language location detects the user's browser locale and refers to the corresponding language pack in PingOne. Integrating PingOne language packs provides seamless localization and translation of Verify user interfaces, allowing users to interact with PingOne Verify in their preferred language. Learn more in Languages.

Steps

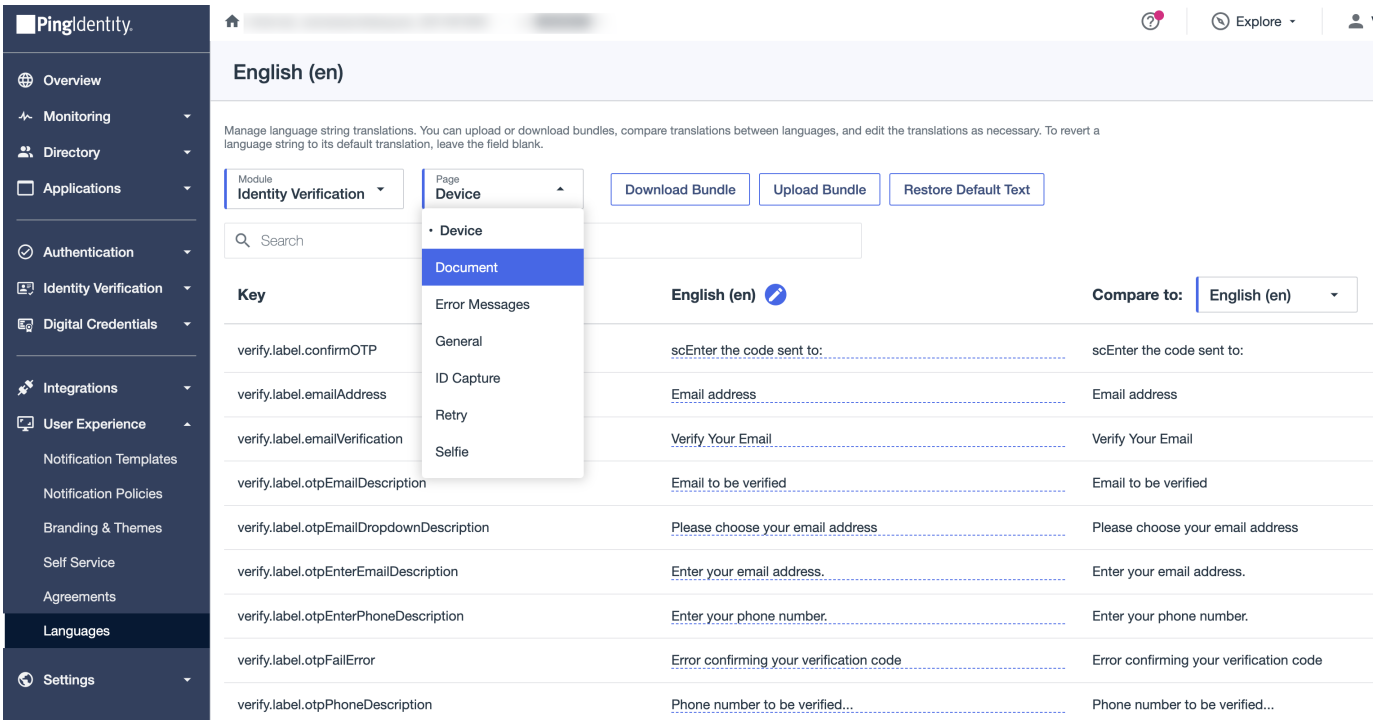
1. Go to **User Experience > Languages**.
2. Click your preferred language or add a language. Learn more in Adding a language.

   Result:

   The details panel opens.
3. In the **Module** list, select **Identity Verification**.
4. In the **Page** menu, select a page to view the associated keys.
5. The **Identity Verification** module includes the following pages:
   - **Device**
   - **Document**
   - **Error Messages**
   - **General**
   - **ID Capture**
   - **Retry**

Copyright © 2025 Ping Identity Corporation

- **Selfie**
- **Voice**



6. (Optional) Click **Compare to:** and select another language from the list to compare the text with a language other than the default language.
7. In the translation column, click the **Pencil** icon.
8. Edit the text in the translation field to your preferred translation.
9. Click **Save**.
10. In the upper right, click the toggle to enable the language.

> **Note**
>
> Learn more about downloading and uploading bundles in Downloading a language bundle and Uploading a language bundle.

PingOne Verify types of verification

PingOne Verify offers different types of verification to enable secure user verification.

Verification	Description
Government ID	Verification based on government-issued documents. For example, a driver license or a passport. Government ID verifications are, by default, run through an automated ID inspection system. When automated ID authentication is not supported or when it is not reliable, such as when the user submits poor quality image, verification can be replaced by manual ID inspection, or step-up (automated, then manual). Verification is performed on PingOne Verify transactions by default, unless a customized verify policy is assigned to the transaction when it's created. You can also verify users in India using their Aadhaar ID, a one-time passcode (OTP), and match the user's selfie against the Aadhaar registry. During this verification process, the standard document authentication flow (docauth) is bypassed and enhances the efficiency and reach of identity verification for users in India. Learn more in Creating a verify policy.
Facial Comparison Government ID	A live photo (selfie) compared with government ID documents for verification. Verification is performed on PingOne Verify transactions by default, unless a customized verify policy is assigned to the transaction when it's created. Learn more in Creating a verify policy.
Facial Comparison Reference Selfie	A new live photo (selfie) compared with a reference selfie sent by the admin through PingOne application programming interface (API) for verification. Verification is supported by the PingOne Verify DaVinci connector and the PingOne Verify PingFederate Integration Kit. Learn more in Verify transactions, PingOne Verify Connector, and PingOne Verify Integration Kit.
Liveness	A liveness check on the live photo (selfie) for verification. Verification is performed on PingOne Verify transactions by default, unless a customized verify policy is added to the transaction when it's created. Learn more in Creating a verify policy.
Phone	Phone verification using OTP. Verification can be enabled on the **Verify Policies** page.
Email	Email verification using OTP. Verification is enabled on the **Verify Policies** page.

Copyright © 2025 Ping Identity Corporation

Verification	Description
Voice	Voice verification using a voice sample. Voice verification has 2 steps: 1. Enrollment: The end user provides live voice samples by speaking a predetermined phrase into their device's microphone, or a customer support service or call center records an end user's voice on a phone call and submits the voice recording to the customer. **Note** PingOne stores voice templates abstracted from user voice samples. 2. Verification: The end user's voice is verified either by speaking the same phrase from enrollment into their device microphone or using a customer support service recording of the end user's voice. The support service can also send the user a link to verify their voice using a web-based flow. The voice sample is then compared to the user's voice template (created from previously captured voice samples) and verified using a voice recognition engine.
Manual ID inspection	Verification done by a manual review team to determine the authenticity, originality, and validity of a document. This verification is for circumstances where automated authentication isn't achievable (unsupported government ID type) or reliable, such as poor image quality. Manual ID inspection license can be configured and used as a complement to the default automated ID inspection system (multistep) or its replacement (direct-to-manual). **Note** Manual ID inspection requires an additional license to configure this verification through the PingOne admin console and the PingOne API.
AAMVA	Additional document verification provided by the American Association of Motor Vehicle Administrators (AAMVA) service through the Driver's License Data Verification (DLDV) service. Verification is enabled based on the active license capabilities your environment has. Learn more in US-based driver licenses in the PingOne developer documentation. **Note** AAMVA requires an additional license to configure this verification through the PingOne admin console or the PingOne API.

Copyright © 2025 Ping Identity Corporation

Verification	Description
Biographic matching	Biographic field values compared against attributes from the verified data of government-issued documents. These values are provided by the admin through PingOne APIs. Verification is also based on the result of PingOne Verify government ID verification. You can configure this verification through the PingOne API. **Note** Biographic matching results do not effect the final PingOne Verify verification status. Learn more in Create Verify Transaction (Biographic Matching) in the PingOne developer documentation.

ID verification

You can enable user ID verification, view a user ID verification status, reset a user's ID verification status, and manually approve a user's ID. All this can be done using the admin console or the PingOne REST API.

- Enabling user ID verification
- Viewing user ID verification
- Resetting a user's ID verification status
- Manually approving a user's ID

Enabling user ID verification

Enable user ID verification to require a user to go through the verification process when they register or sign on. You can enable ID verification using the PingOne admin console or the PingOne Verify REST API.

Copyright © 2025 Ping Identity Corporation

Console

Enabling user ID verification in the PingOne admin console

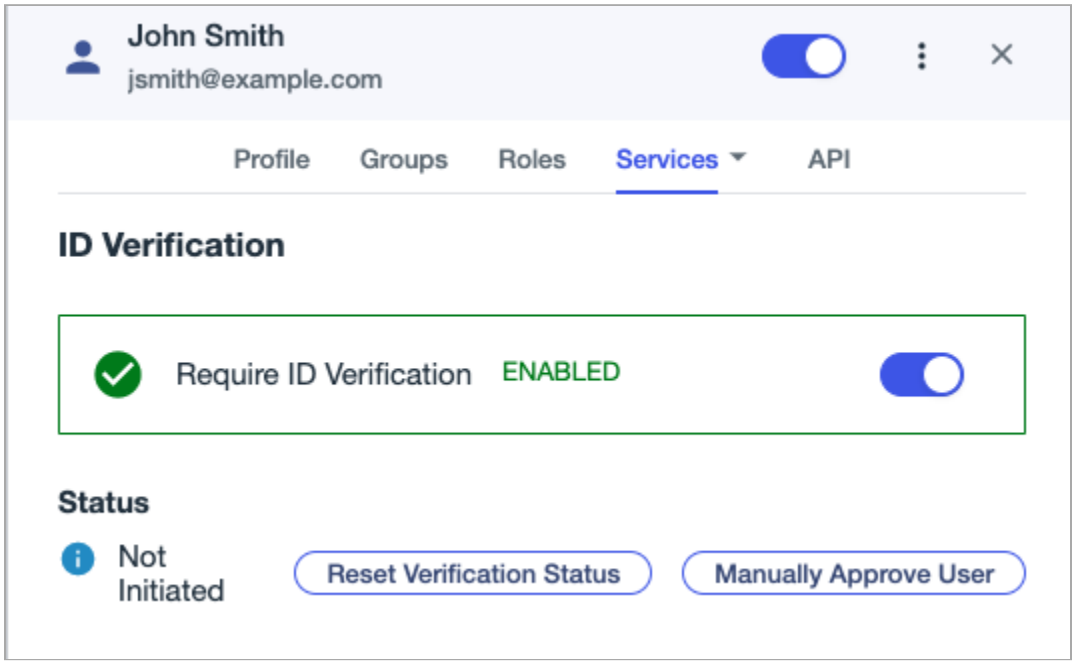
Steps

1. In the PingOne admin console, go to **Directory** > **Users**.
2. Locate the user you want to edit.

   You can browse or search for users.
3. Click the user entry to open the user details panel.
4. In the user details panel, click the **Services tab → ID Verification** to view the verification details for the user.

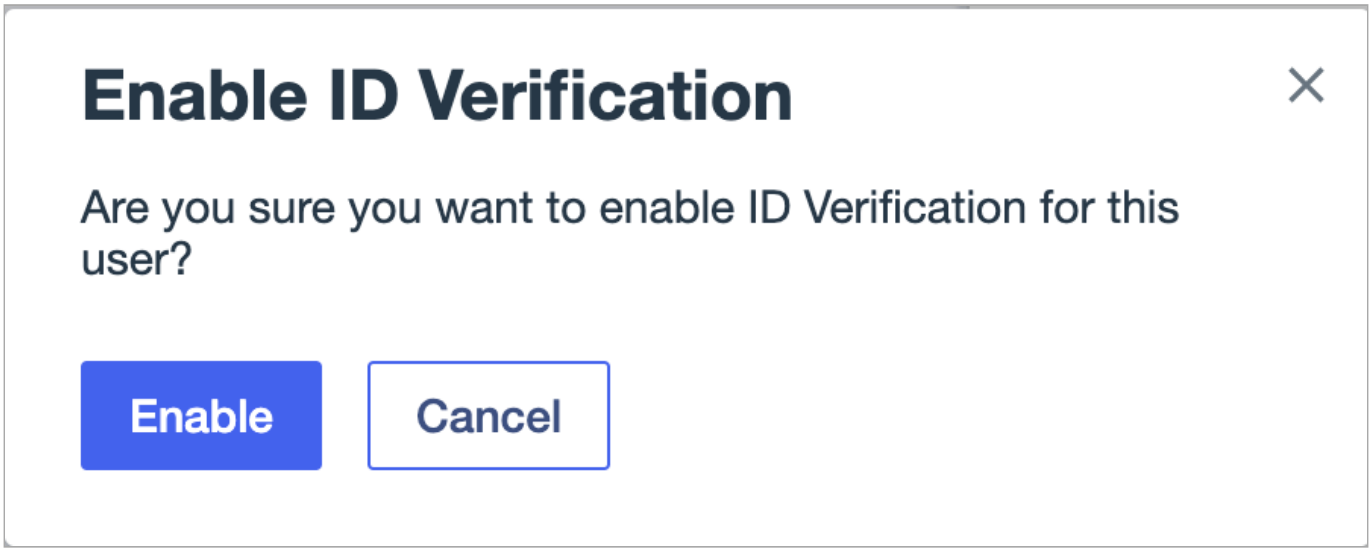
   > **Note**
   > This tab remains in place if ID verification was previously enabled for a user, but is now disabled.

5. Click the **Require ID Verification** toggle to enable ID verification for the user.



6. In the confirmation popup, click **Enable**.

Copyright © 2025 Ping Identity Corporation



Result

When the user attempts to sign on or register, instructions for ID verification are shown on their device. The connection to their device and the instructions displayed are created by the Verify app using the PingOne Verify SDK for iOS or Android devices. For more information, see PingOne Verify Mobile SDKs.

API

Enabling user ID verification with the PingOne Verify API
Steps

- Use the PingOne Verify REST API to make the following request:

```
POST /environments/{envID}/users/{userID}/verifyTransactions
```

For more information, see User verification in the PingOne Platform API Reference.

Result

When the user attempts to sign on or register, instructions for ID verification are shown on their device. The connection to their device and the instructions displayed are created by the Verify app using the PingOne Verify SDK for iOS or Android devices. For more information, see PingOne Verify Mobile SDKs.

Viewing user ID verification status

After you've configured ID verification, you can view a user's details to see their verification status. You can view user details in the PingOne admin console or through the PingOne Verify REST API.

Copyright © 2025 Ping Identity Corporation

Console

Viewing user ID verification status in the PingOne admin console

Steps

1. In the PingOne admin console, go to **Directory** > **Users**.
2. Locate the user you want to view.

   You can browse or search for users.
3. Click the user entry to open the user details panel.
4. In the user details panel, click the **Services tab → ID Verification** to view the verification details for the user.

   The **Status** section indicates the current state of the ID verification process for the user and can have one of the following values:

   ### *Not Initiated*

   The user must send their ID information for verification using the customer Verify app, either during registration or the next time the user signs on, depending on the configuration settings for the policy set in the PingOne Verify Integration Kit.

   ### *In Process*

   The ID verification service is in the process of receiving the user ID information sent with the ID verification transaction record, and attempting to validate the user ID information with the service provider.

   ### *Error*

   The user verification process encountered an error. The error message is shown in the **Status** section in the PingOne admin console and in the Verify app on the user's device.

   > **Note**
   >
   > If the ID verification fails more than three times in a 1-hour period, the user must wait an hour before trying again.

   ### *Successful*

   The user ID information has been validated by the service provider and verified by the ID verification service.

   The **Attempt Count** section shows the count of user ID verification attempts.

Copyright © 2025 Ping Identity Corporation

API

Viewing user ID verification status with the PingOne Verify API

Steps

- Use the PingOne Verify REST API to make one of the following requests:

  Choose from:

```
GET /environments/{envID}/users/{userID}/verifyTransactions
```

Returns all changes (transactions) in verification status for the user. For more information, see READ all ID verification transaction records for a user.

```
GET /environments/{envID}/users/{userID}/verifyTransactions/{transactionID}
```

Returns a specific change (transaction) in verification status for the user. For more information, see READ an ID verification transaction record for a user.

Resetting a user's ID verification status

At any stage in the ID verification process, you can choose to reset a user's verification status. You can reset the verification status in the PingOne admin console or through the PingOne Verify REST API.

About this task

You might reset a user's verification status if:

- There's an error and the user doesn't know what to do.
- The user verification process is hung in the `In Process` state.
- For any reason, you want to request the user to resubmit a successful verification.

Copyright © 2025 Ping Identity Corporation

Console

Resetting a user's ID verification status in the PingOne admin console

Steps

1. In the PingOne admin console, go to **Directory** > **Users**.
2. Locate the user you want to edit.

   You can browse or search for users.
3. Click the user entry to open the user details panel.
4. In the user details panel, click the **Services tab → ID Verification** to view the verification details for the user.
5. Click the **Reset Verification Status** button.

   Result:

   The **Status** changes to **Not Initiated**.
6. In the confirmation popup, click **Reset Verification Status**.

Result

The verification process restarts and sends a notification message to the user to resubmit their credentials for verification.

The user can resubmit their ID information from their device at the time of notification, or wait until the next time they sign on to PingOne.

If the user has previously completed a successful ID verification, the signed claim of their ID information still exists on their device. The user can just scan the new ID verification transaction record sent to their device. The customer Verify app then passes the existing signed certification to the ID verification service. The ID verification service validates the claim and changes the status of the user without having to contact the service provider for validation.

If you disable ID verification for a user that has previously completed a successful ID verification, the signed certification of their ID information also still exists on their device. Re-enabling ID verification for the user then follows the same process as described previously.

API

Resetting a user's ID verification status with the PingOne Verify API

Steps

- Use the PingOne Verify REST API to make the following request:

  ```
  DEL /environments/{envID}/users/{userID}/verifyTransactions/{transactionID}
  ```

  For more information, see DELETE an ID verification transaction record for a user.

Copyright © 2025 Ping Identity Corporation

Manually approving a user's ID

If automated user ID verification fails for any reason, you can manually approve a user's ID.

About this task

Manual approval allows the user to bypass the automated verification process and instead use admin-assisted verification. In this case, admins can rely on a custom defined identity verification process such as in-person or video-based conferencing to verify users. You can manually approve a user's ID in the PingOne admin console or through the PingOne Verify REST API.

Copyright © 2025 Ping Identity Corporation

Console

Manually approving a user's ID in the PingOne admin console

Steps

1. In the PingOne admin console, go to **Directory** > **Users**.
2. Locate the user you want to edit.

   You can browse or search for users.
3. Click the user entry to open the user details panel.
4. In the user details panel, click the **Services tab → ID Verification** to view the verification details for the user.
5. Click **View**, then **Manually Approve**.

> **Note**
>
> The **Manually Approve** option is not available for the following transactions with the status:
>
> - `Approved_Manually`
> - `Success`
> - `Approved_No_Request`

Result

The user ID is verified, and the user can register or sign on from their device.

Copyright © 2025 Ping Identity Corporation

API

Manually approving a user's ID with the PingOne Verify API

Steps

- Use the PingOne Verify REST API to make the following request:

```
PUT /environments/{envID}/users/{userID}/verifyTransactions/{transactionID}
```

For more information, see UPDATE an ID verification transaction record for a user.

Result

The user ID is verified, and the user can register or sign on from their device.

Verify policies

A PingOne Verify policy dictates what is required to verify a user.

Verify policies can require different types of user verification, such as an ID verification, facial comparison, or liveness. See the following:

- Creating a verify policy
- Managing a verify policy
- Deleting a verify policy

Creating a verify policy

A verify policy dictates what is required to verify a user, such as an ID verification, facial comparison, or liveness.

About this task

A verify policy allows you to create PingOne Verify transactions for different scenarios, such as:

- Choosing documents for verification during employee onboarding
- Selfie liveness and comparison during multi-factor authentication (MFA) in PingID using PingOne Verify
- Selfie match against the Aadhaar registry data for verification when an Indian Aadhaar ID is detected

Steps

1. In the PingOne admin console, go to **Identity Verification > Verify Policies**.

> **Note**
> A default verify policy based on your environment capabilities is listed.

Copyright © 2025 Ping Identity Corporation

2. Click the + icon.

3. Enter or edit the following:

Field	Description
Name	The policy's name.
Description	The policy's description.
Configuration	**Transaction Timeout**: Time period (in minutes) in which data can be collected after a transaction is created. The maximum transaction timeout is 30 minutes. **Data Collection Timeout**: Time period (in minutes) in which data can be collected after initiating verification from the UI. By default, the data collection timeout is set to 15 minutes. The maximum data collection timeout is 30 minutes. **Data Collection Only**: Click the toggle to enable data collection from a user without verification.

Copyright © 2025 Ping Identity Corporation

Field	Description
Government ID	Verification based on government-issued documents. For example, a driver license or a passport. Configure the following policy settings: ◦ **ID Verification**: Select **Required**, **Optional**, or **Disabled**. ◦ **Document Authentication Provider**: The provider used to authenticate government documents. Select **Mitek** (default) or **Veriff**. ◦ **Inspection Type**: Select the type of inspection performed on government-issued documents: ■ **Automatic**: AI-based analytics examine the ID document to determine if it's original and unaltered. ■ **Manual**: A human agent trained in document authentication examines the photo of the ID to determine its authenticity. ■ **Step-Up to Manual**: Automated inspection is tried first. If the document cannot be verified, the service switches to manual inspection. **Note** **Manual** and **Step-Up to Manual** inspection types require an additional license. ◦ **Government ID Retry Attempts**: The number of times a user can retry scanning an ID if the first attempt fails. Possible values for government ID retry attempts are 0 - 3. ◦ **Enable AAMVA**: Click the toggle to enable verification of ID information against the issuing agency database, the AAMVA Driver's License Data Verification (DLDV) service. ◦ **Fail Expired IDs**: Click the toggle to fail verification for expired IDs. ◦ **Enable Aadhaar Verification (India)**: Click the toggle to enable user verification through the Aadhaar registry. ◦ **OTP Attempts**: The number of times a user can enter the correct one-time passcode (OTP) that's sent to the phone number associated with their Aadhaar ID for verification. ◦ **Cooldown Duration (Seconds)**: A waiting period enforced after an OTP is sent to a user before they can request another one.
Facial Comparison	A live photo (selfie) compared with government ID documents or reference selfie for verification. Configure the following policy settings: ◦ **Facial Comparison**: Select **Required**, **Optional**, or **Disabled**. ◦ **Threshold**: The probability that selfies are likely to match with document images (facial comparison) or pass liveness checks (liveness). Select **Low**, **Medium**, or **High** threshold. **Note** Selfies are less likely to match or pass with a higher threshold.

Copyright © 2025 Ping Identity Corporation

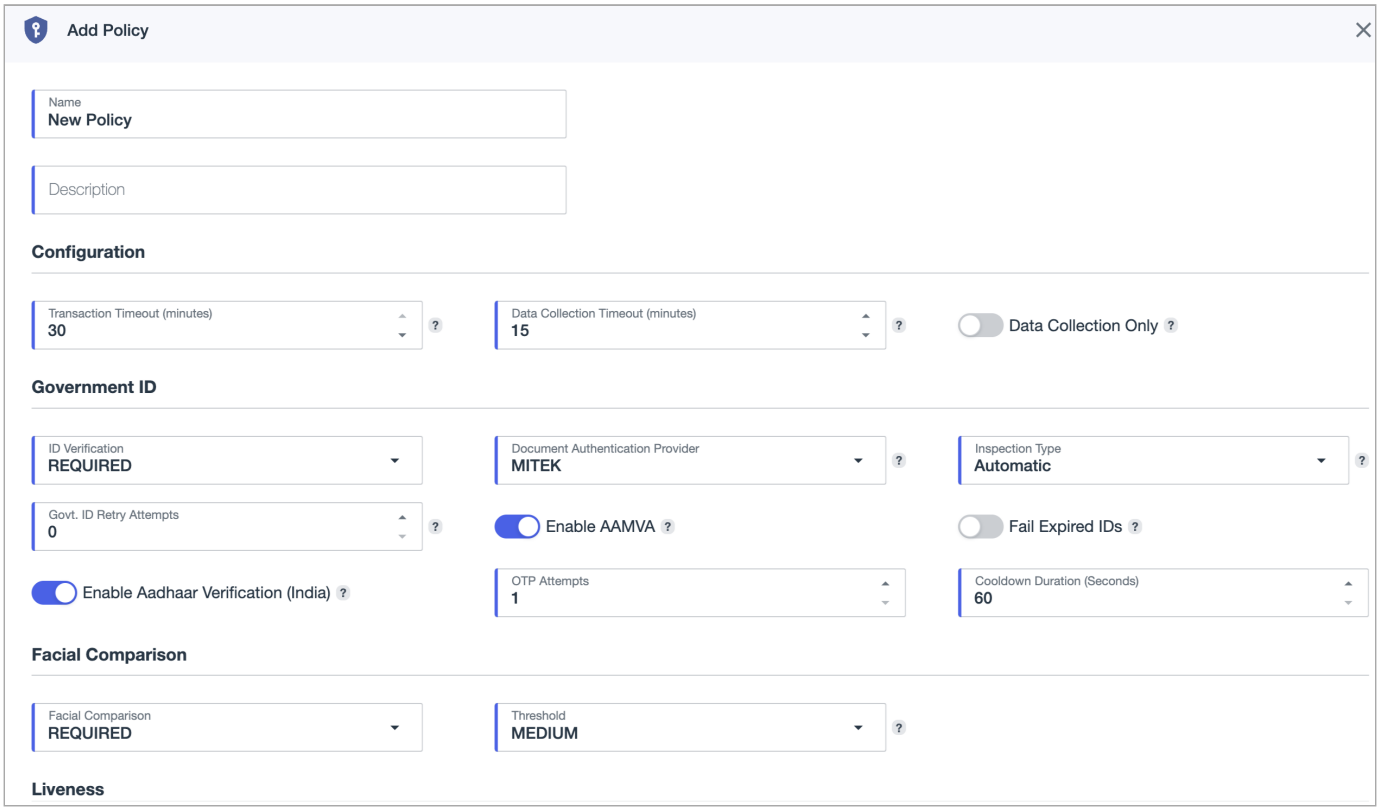
Field	Description
Liveness	A liveness check on the live photo (selfie) for verification. Configure the following policy settings: ◦ **Liveness**: Select **Required**, **Optional**, or **Disabled**. ◦ **Threshold**: The probability that selfies are likely to match with document images (facial comparison) or pass liveness checks (liveness). Select **Low**, **Medium**, or **High** threshold. ⓘ **Note** Selfies are less likely to match or pass with a higher threshold. ◦ **Selfie Retry Attempts**: The number of times a user can retake a selfie if the first attempt fails. Possible values for selfie retry attempts are 0 - 3.
Voice Verification	Verification using voice samples of the end user. There are two types of voice verification policies: enrollment and verification. ⓘ **Note** You must configure a separate enrollment policy and verification policy. Configure the following policy settings: ◦ **Voice Verification**: Select **Required**, **Optional**, or **Disabled**. ◦ **Enrollment**: Click the toggle to enable an enrollment policy. Disable for a verification policy. ◦ **Samples Required**: The number of voice samples the user must record for enrollment. ◦ **Voice Phrase**: Phrase the user repeats for enrollment or verification. You can configure custom phrases with the API. Learn more in Create Custom Voice Phrase in the PingOne developer documentation. ◦ **Comparison Threshold**: Voice samples are less likely to match with the voice template at higher thresholds. ◦ **Liveness Threshold**: Voice samples are less likely to pass liveness testing at higher thresholds. ◦ **Store Original Recordings**: Click the toggle to enable storing the original voice sample after a successful transaction. ◦ **Enhance Reference On Re-Enrollment**: Click the toggle to enhance the existing voice reference on re-enrollment. If disabled, the voice reference is replaced instead of enhanced with additional data. ◦ **Enhance Reference on Verification**: Click the toggle to enable improving the existing voice reference by adding a new template. ⓘ **Note** You can only enable or disable **Enhance Reference on Verification** if **Enrollment** is enabled.
Phone	**Phone Verification**: Select **Required**, **Optional**, or **Disabled**. **Create MFA Device**: Click the toggle to enable registration of a user's phone number as a trusted MFA device after successful OTP or web link verification.

Copyright © 2025 Ping Identity Corporation

Field	Description
Email	**Email Verification**: Select **Required**, **Optional**, or **Disabled** **Create MFA Device**: Click the toggle to enable registration of a user's email address as a trusted MFA device after successful OTP or web link verification.

Example:

An example configuration on the **Add Policy** page.



4. Click **Save**.

Result:

Your new policy is shown on the **Verify Policies** page.

Managing a verify policy

Edit, rename, or set your verify policy into the default policy.

Steps

- To edit a verify policy:
    1. In the PingOne admin console, go to **Identity Verification** > **Verify Policies**.
    2. Click the policy that you want to edit.

Copyright © 2025 Ping Identity Corporation

Result:

The **Policy Details** panel opens.

3. Click the **Pencil** icon.
4. Enter or edit the following configurations:

Field	Description
Name	The policy's name.
Description	The policy's description.
Configuration	**Transaction Timeout**: Time period (in minutes) in which data can be collected after a transaction is created. The maximum transaction timeout is 30 minutes. **Data Collection Timeout**: Time period (in minutes) in which data can be collected after initiating verification from the UI. By default, the data collection timeout is set to 15 minutes. The maximum data collection timeout is 30 minutes. **Data Collection Only**: Click the toggle to enable data collection from a user without verification.

Copyright © 2025 Ping Identity Corporation

Field	Description
Government ID	Verification based on government-issued documents. For example, a driver license or a passport. Configure the following policy settings: ■ **ID Verification**: Select **Required**, **Optional**, or **Disabled**. ■ **Document Authentication Provider**: The provider used to authenticate government documents. Select **Mitek** (default) or **Veriff**. ■ **Inspection Type**: Select the type of inspection performed on government-issued documents: ■ **Automatic**: AI-based analytics examine the ID document to determine if it's original and unaltered. ■ **Manual**: A human agent trained in document authentication examines the photo of the ID to determine its authenticity. ■ **Step-Up to Manual**: Automated inspection is tried first. If the document cannot be verified, the service switches to manual inspection. **Note** **Manual** and **Step-Up to Manual** inspection types require an additional license. ■ **Government ID Retry Attempts**: The number of times a user can retry scanning an ID if the first attempt fails. Possible values for government ID retry attempts are 0 - 3. ■ **Enable AAMVA**: Click the toggle to enable verification of ID information against the issuing agency database, the AAMVA Driver's License Data Verification (DLDV) service. ■ **Fail Expired IDs**: Click the toggle to fail verification for expired IDs. ■ **Enable Aadhaar Verification (India)**: Click the toggle to enable user verification through the Aadhaar registry. ■ **OTP Attempts**: The number of times a user can enter the correct one-time passcode (OTP) that's sent to the phone number associated with their Aadhaar ID for verification. ■ **Cooldown Duration (Seconds)**: A waiting period enforced after an OTP is sent to a user before they can request another one.

Copyright © 2025 Ping Identity Corporation

Field	Description
Facial Comparison	A live photo (selfie) compared with government ID documents or reference selfie for verification. Configure the following policy settings: ■ **Facial Comparison**: Select **Required**, **Optional**, or **Disabled**. ■ **Threshold**: The probability that selfies are likely to match with document images (facial comparison) or pass liveness checks (liveness). Select **Low**, **Medium**, or **High** threshold. **Note** Selfies are less likely to match or pass with a higher threshold.
Liveness	A liveness check on the live photo (selfie) for verification. Configure the following policy settings: ■ **Liveness**: Select **Required**, **Optional**, or **Disabled**. ■ **Threshold**: The probability that selfies are likely to match with document images (facial comparison) or pass liveness checks (liveness). Select **Low**, **Medium**, or **High** threshold. **Note** Selfies are less likely to match or pass with a higher threshold. ■ **Selfie Retry Attempts**: The number of times a user can retake a selfie if the first attempt fails. Possible values for selfie retry attempts are 0 - 3.

Copyright © 2025 Ping Identity Corporation

Field	Description
Voice Verification	Verification using voice samples of the end user. There are two types of voice verification policies: enrollment and verification. **Note** You must configure a separate enrollment policy and verification policy. Configure the following policy settings: ■ **Voice Verification**: Select **Required**, **Optional**, or **Disabled**. ■ **Enrollment**: Click the toggle to enable an enrollment policy. Disable for a verification policy. ■ **Samples Required**: The number of voice samples the user must record for enrollment. ■ **Voice Phrase**: Phrase the user repeats for enrollment or verification. You can configure custom phrases with the API. Learn more in Create Custom Voice Phrase in the PingOne developer documentation. ■ **Comparison Threshold**: Voice samples are less likely to match with the voice template at higher thresholds. ■ **Liveness Threshold**: Voice samples are less likely to pass liveness testing at higher thresholds. ■ **Store Original Recordings**: Click the toggle to enable storing the original voice sample after a successful transaction. ■ **Enhance Reference On Re-Enrollment**: Click the toggle to enhance the existing voice reference on re-enrollment. If disabled, the voice reference is replaced instead of enhanced with additional data. ■ **Enhance Reference on Verification**: Click the toggle to enable improving the existing voice reference by adding a new template. **Note** You can only enable or disable **Enhance Reference on Verification** if **Enrollment** is enabled.
Phone	**Phone Verification**: Select **Required**, **Optional**, or **Disabled**. **Create MFA Device**: Click the toggle to enable registration of a user's phone number as a trusted MFA device after successful OTP or web link verification.
Email	**Email Verification**: Select **Required**, **Optional**, or **Disabled** **Create MFA Device**: Click the toggle to enable registration of a user's email address as a trusted MFA device after successful OTP or web link verification.

5. Click **Save**.

Copyright © 2025 Ping Identity Corporation

- To rename a verify policy:

  1. In the PingOne admin conosole, go to **Identity Verification** > **Verify Policies**.
  2. Next to the relevant policy that you want to rename, click the **More Options** (⋮) icon, and then click **Rename**.

  3. In the **Name** field, enter a new name.
  4. Click **Save**.

- To set your verify policy as the default policy:

  1. In the PingOne admin console, go to **Identity Verification** > **Verify Policies**.
  2. Next to the relevant policy that you want to set as the default policy, click the **More Options** (⋮) icon, and then click **Make Default**.

     Result:

     You see a message asking if you are sure you want to select this as your default policy.

  3. Click **Save**.

     Result:

     A **Default** icon is added next to your policy name on the **Verify Policies** page.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Default policies can't be deleted. You must set a different policy as the default before you can delete a default policy.

Deleting a verify policy

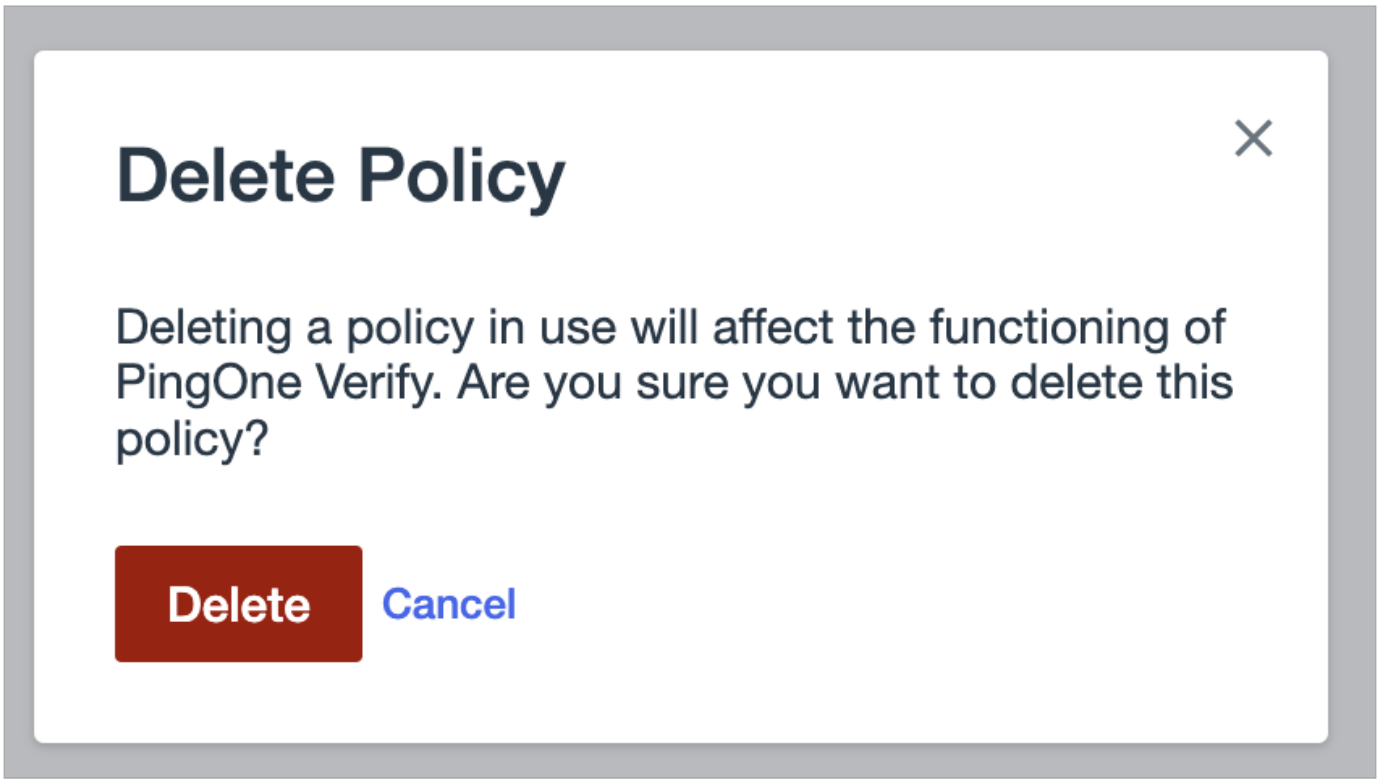
You can delete a verify policy from your **Verify Policies** page.

Steps

1. Go to **Identity Verification** > **Verify Policies**.
2. Next to the relevant policy that you want to delete, click the **More Options** (⋮) icon, and then click **Delete**.

   Result:

   You see a message asking if you're sure you want to delete the policy.

3. Click **Delete**.

   Result:

   Your policy is deleted and is no longer listed on the **Verify Policies** page.

Copyright © 2025 Ping Identity Corporation

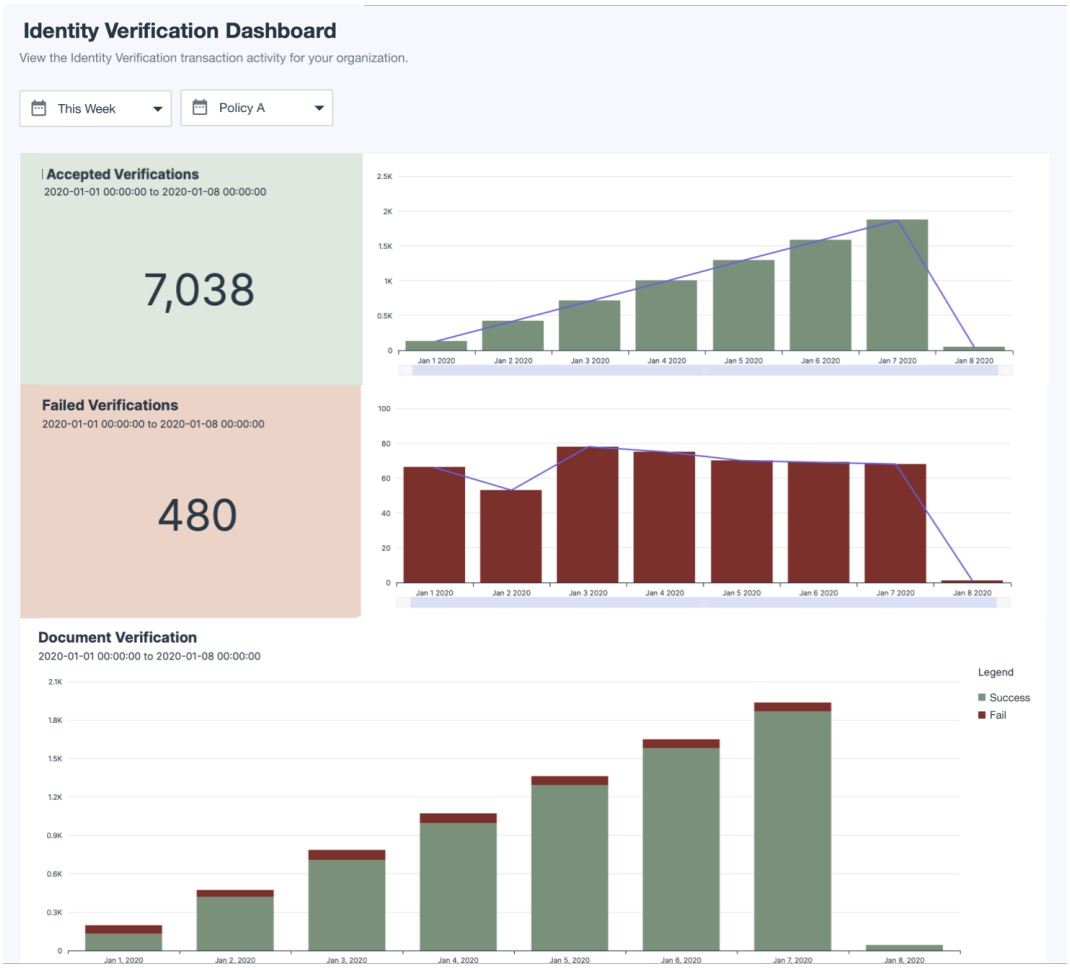
Identity Verification Dashboard

The **Identity Verification Dashboard** shows identity verification transaction activity for your organization.

Overview

To access the **Identity Verification Dashboard**, in the PingOne admin console, go to **Monitoring** > **Identity Verification**.

The **Identity Verification Dashboard** shows a summary of PingOne Verify transactions filtered by your choice of date, PingOne Verify policy, and accepted and failed verifications. You can use this information for managing both identify verification and the handling of accepted and failed verifications in the PingOne platform. Learn more about managing identity verification in Identity Verification using PingOne Verify.



Graphs

Accepted Verifications

The graph shows the total number of accepted verification transactions that occurred during a selected time period. A successful transaction means a user has been validated by the service provider and verified by the ID verification service. Hover over the bar graph to get more information.

Failed Verifications

The graph shows the total number of failed verification transactions that occurred during a selected time period. A failed transaction means a user has been rejected by the service provider or ID verification service. Hover over the bar graph to get more information.

Document Verification

The graph shows successful and failed documentation verification transactions that occurred during a selected time period.

Facial Verification

The graph shows successful and facial verification transactions that occurred during a selected time period. Facial verification checks for the liveness of the user and then compares the selfie with the user's picture on their government-issued ID.

> **Note**
>
> Data for this graph begins on February 27, 2024.

Viewing license information

The PingOne Verify license is transaction-based. Your license information shows the quota for the total number of transactions that are allowed. The transactions can take place in any time period, with the limit enforced by the ID verification service.

Steps

1. Click the Ping Identity logo in the upper left side of the PingOne admin console.
2. Click **Licenses**.

   > **Note**
   >
   > The list shows only active licenses by default. To see expired licenses, click **Show All Licenses**.

   If you have a currently active PingOne Verify license, the console shows the license quota and the current number of transactions used.

Next steps

To increase your license quota, click the **Please Contact Me** button. We'll contact you to answer any licensing questions and increase your license quota. For more information, see Licenses and Platform Limits.

Copyright © 2025 Ping Identity Corporation

Digital Credentials using PingOne Credentials

PingIdentity.

The PingOne Credentials service allows an issuer to create verifiable credentials that they can send to a compatible wallet app.

Getting started

- What is PingOne Credentials?
- Get started with PingOne Credentials
- Developing and registering the wallet app that runs the PingOne Neo SDK
- PingOne Credentials scenarios
- Customizing PingOne Credentials notification templates
- Creating a credential
- Editing a credential
- Revoking credentials

Integrations and connectors

- Ping Identity Integration Directory
- PingOne Credentials connector

Developer resources

- Get started with PingOne APIs
- PingOne Neo SDK
- PingOne Credentials
- Credential issuers

Copyright © 2025 Ping Identity Corporation

Introduction to PingOne Credentials

The PingOne Credentials service is a part of the PingOne Neo decentralized identity solution that allows an issuer to create verifiable credentials that they can issue to a compatible wallet app, eliminating cost and management of issuing physical credentials. Learn more in PingOne Neo.

The three parties that enable decentralized identity are:

Issuer

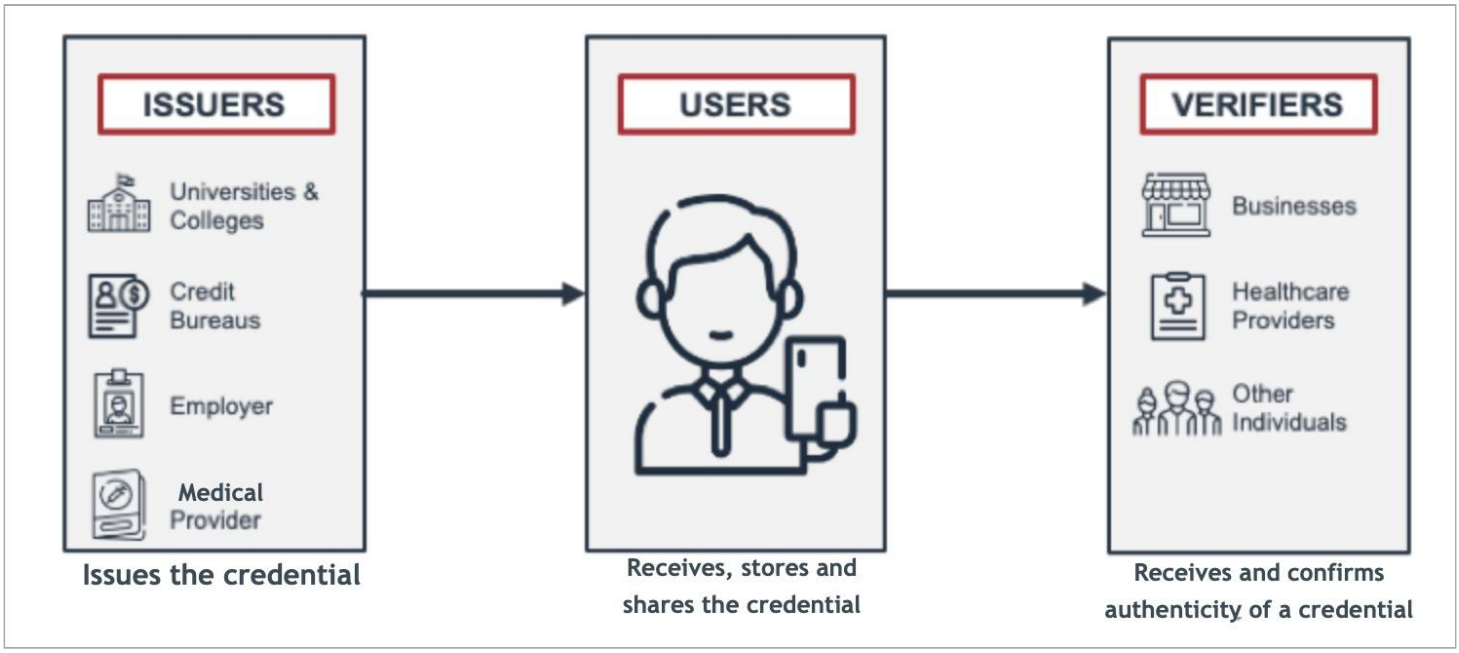
The proprietor and issuer of official sources of data, such as college transcripts, vaccination status, or employment history.

Verifier

Any individual or institution (service provider) with which a user chooses to share data that requires verification, such as sharing a driver license as proof of age or credit card information when applying for a loan.

User

An individual who matches the issuance rule of a group, population, or SCIM filter with a PingOne Credentials profile. Users can receive credentials from issuers, store them securely in their compatible wallet app, and use it to share their credentials with verifiers.



Issuers and verifiers can be any entity that the user engages with, such as a university, an insurance company, employer, health provider, or a financial institution.

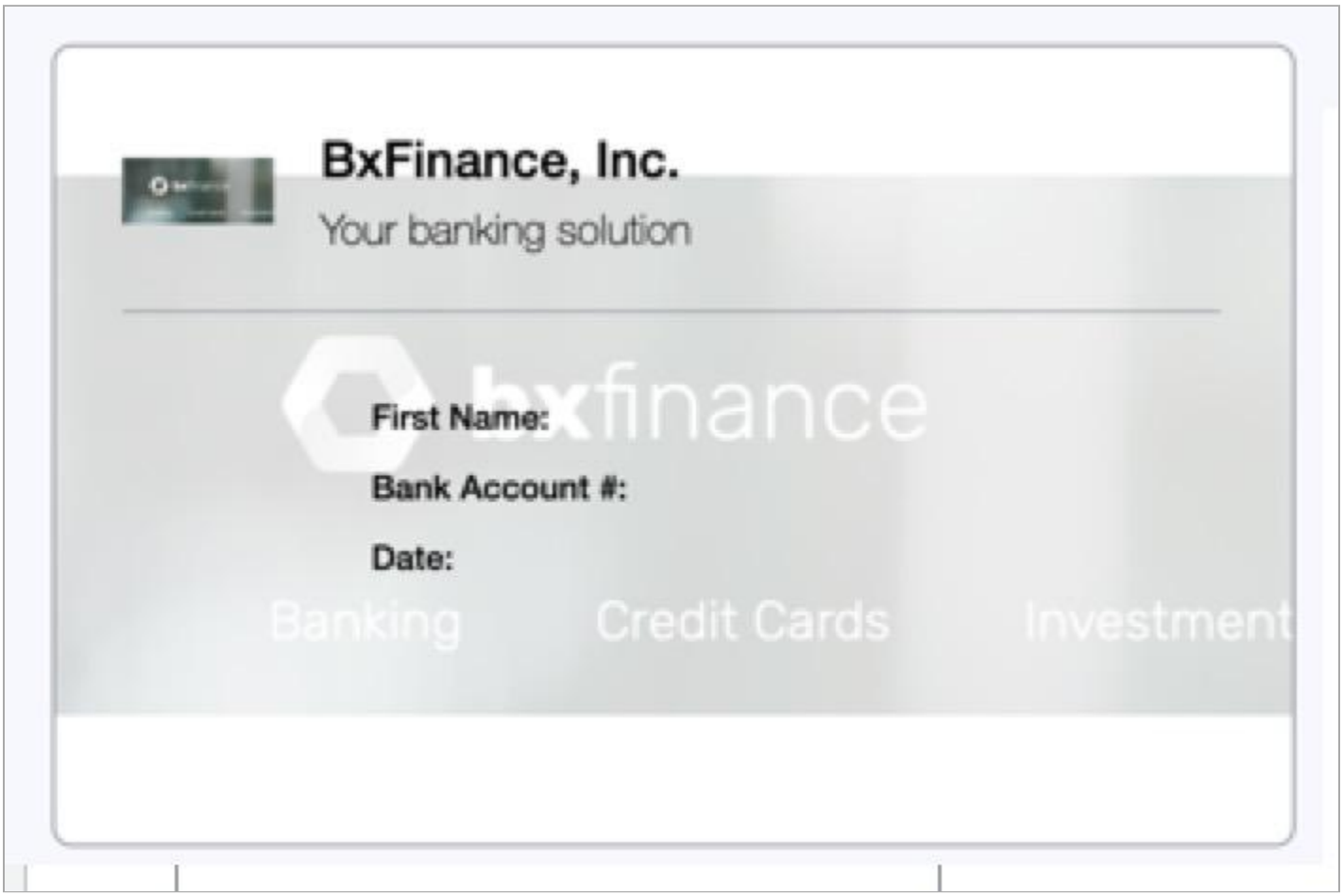
Users that need to receive or provide proof of a credential to these institutions might already have a record of their activity with that institution, which won't change. However, if the user needs to share that record with another entity, traditionally they must allow the other entity (a verifier) to contact the original institution (the issuer) to get the information and confirm that it's valid. This can be cumbersome, expensive, and time-consuming and could violate the user's privacy if not managed properly.

Copyright © 2025 Ping Identity Corporation

Using decentralized identity, it's possible for an issuer, such as a university or employer, to provide a verifiable credential about the user's qualifications or employment to the user in the form of a digital credential that the user can store in their compatible wallet app. Because the credential is always with the user, the user can share that information with the new business to seek employment. The potential employer can verify the data for its authenticity in real-time without contacting the issuer, so there's no further friction or exposure of privacy.

The issuer creates a credential in PingOne Credentials using the automated issuance rules that automatically issues a verifiable credential to all users who match a provided filter. The filter is based on Groups, Populations, or a SCIM filter. The issuer can also define individual fields on the credential in the form of key-value pairs to provide the appropriate details for the service credential they are offering to their users.

Credential details will vary according to the industry and the specific credentials the issuer wants to offer. For example, in addition to name and date of birth, an insurance company might want to provide the type of insurance, policy number, and expiry date. A bank might want to include the bank account number and date of issue, and a university might want to include the type of degree obtained.



The PingOne Credentials service maintains a unique private-key for each issuer within the PingOne environment. It uses the PingOne Neo SDK to allow creation of verifiable credentials in the backend.

To simplify the creation and issuance of credentials, PingOne Credentials wraps the API calls in a more consumable and user-friendly interface within the PingOne administrator console. This service also provides APIs that allow customers to interact programmatically and with additional customizations.

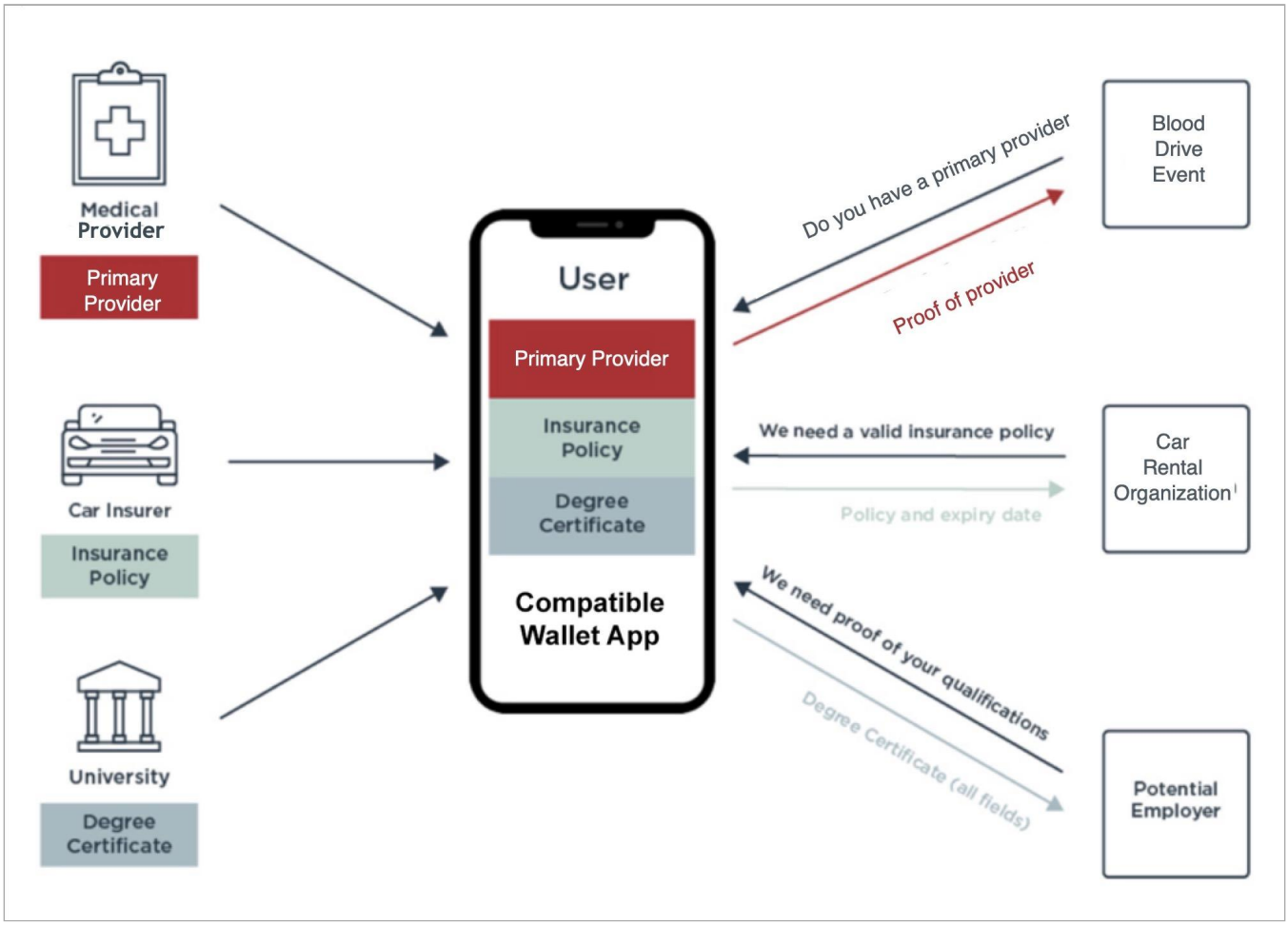
Copyright © 2025 Ping Identity Corporation

Credentials issued by this service can be shared:

- With other users through a compatible wallet app
- With custom QR codes that can be generated with the API calls

The following diagram shows examples of three different issuers, providing credentials to an individual user and the various ways a user can provide information to verifiers using these credentials:

- A medical provider issues a primary provider credential that includes details of the provider, date of last vaccination, and personal medical details. The user stores the certificate as a credential in their compatible wallet app. When a blood drive event requests proof of a primary care provider, the user can send it to them without providing all of the personal details it contains.
- A car insurer provides an insurance policy as a credential to a user. Credentials might include the user's ID, date of birth, and medical status, but when a car rental service asks for the user's insurance policy, the user can share just the policy number and expiry date.
- A university provides a degree certificate as a credential to the user. The user stores the credential in their compatible wallet app. The user can provide a potential employer with the full degree certificate (as well as any other qualifications their wallet app holds) immediately.



PingOne Credentials, along with a compatible wallet app, makes this verifiable exchange of data possible. You can use PingOne Credentials through the PingOne unified administrator console or through its API.

Copyright © 2025 Ping Identity Corporation

How PingOne Credentials works

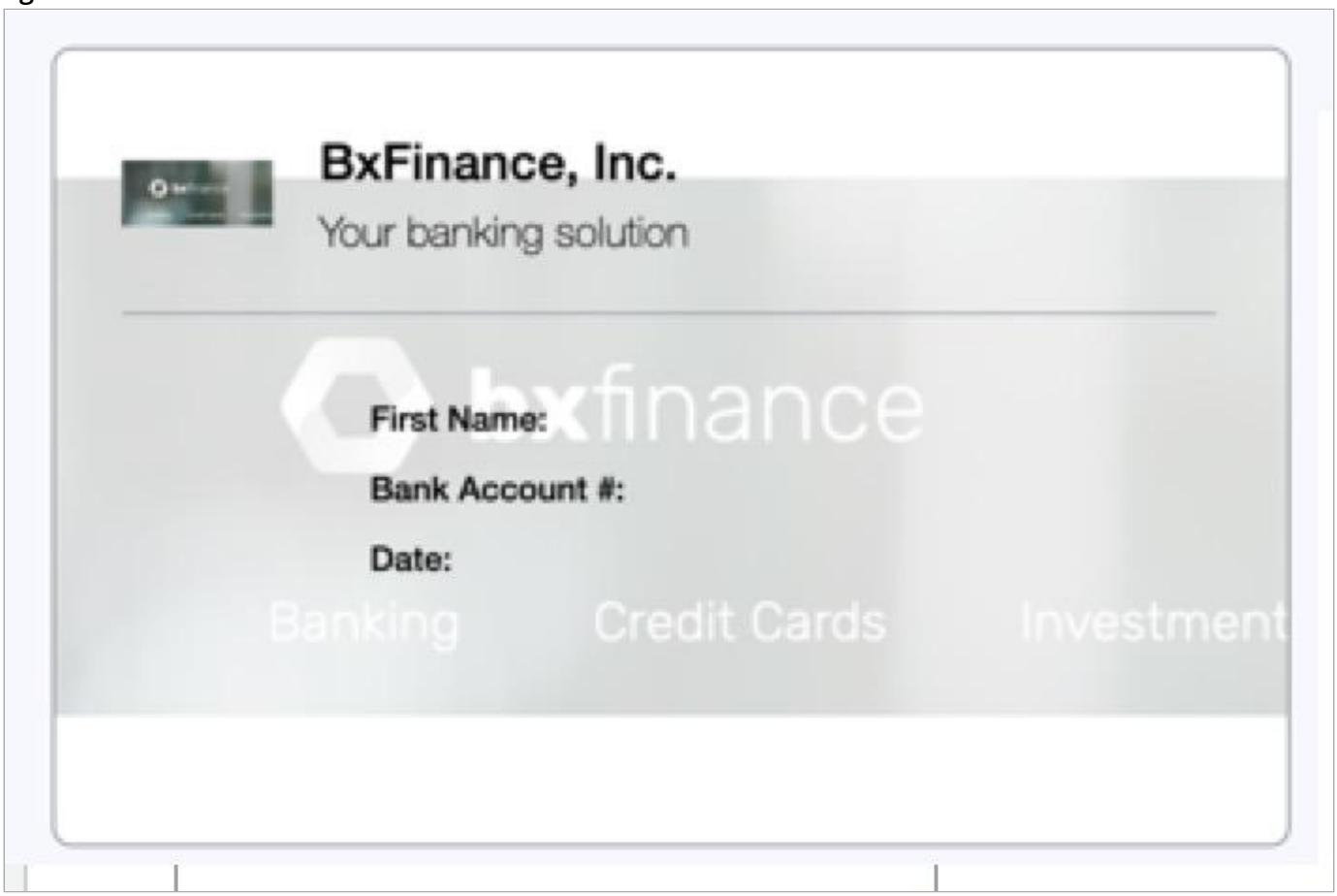
Users: Download a compatible wallet app and create a digital identity profile

Each user is invited to install and pair their digital wallet by installing a customer-developed app running the PingOne Neo SDK. An email or SMS notification can be sent to the user with a link that takes the users to a customer site that helps them install the customer app.

After the app is installed, clicking on the link prompts the user to complete digital wallet pairing. The SDK shares the application instance ID with PingOne Credentials and that is stored for future issued or revoked credentials.

Issuers: Create and issue a new credential in PingOne Credentials

Creating a credential



In PingOne Credentials, an issuer creates a new custom credential. A credential defines the field attributes required to issue a credential, the fields displayed on the credential, and an identifying logo and relevant branding. The field values can be supplied by the issuer or taken partly from both the issuer and the user, such as their selfie and verified first and last name.

> **Note**
>
> The credential can be used to issue a credential to any group or population listed in PingOne Credentials.

Copyright © 2025 Ping Identity Corporation

Issuing a credential to a user

1. The issuer creates a credential and uses the issuance rule to select a group, population, or uses a System for Cross-domain Identity Management (SCIM) filter to issue the credential to.
2. Credentials are automatically sent to a user who is a part of the issuance rule to their digital wallet.
3. If a user doesn't have a digital wallet, a message is sent to invite the user to download the app.
4. After downloading the app, the digital wallet is paired.
5. When the user accepts the credential, it's stored in their wallet app and can be shared with verifiers that request proof of a credential from a user.

Revoking a credential

An issuer can revoke a user's credentials remotely from PingOne Credentials. This ensures that wallet app credentials held by a user are always up-to-date.

Based on the issuance rule, revoking happens automatically for users if a directory attribute changes. For example, if a user is removed from the group, population, or SCIM filter, their credentials are revoked.

After a user's credential is revoked, if a user attempts to share credential data with a verifier, the verifier will see that the data is no longer valid by the issuer. The issuer can always reissue the credential to the user if necessary.

Verifiers: Verifying a credential

When asked for proof of a credential, such as age, valid license, or insurance, the user can share some or all of the information on a credential with a verifier. If the user approves a verifier's request, the user's compatible wallet app shares the specific data and the signed certifications with the verifier.

The verifier can then independently assert the validity of the data by checking whether the credential's digital signatures matches the issuer's public-key. This is done without requiring the verifier to communicate with the issuer directly. This creates a greater level of privacy for the user because the issuer never becomes aware of the user's interaction with the verifier. Additionally, the transaction can be done in real time.

PingOne Credentials example

As an issuer, BX Insurance Company, wants to issue a car insurance policy as a credential to their customers (users) digitally. They want to include the customer's picture, driver license ID, car insurance policy number, and the expiration date for the insurance policy.

The insurance company creates a credential in PingOne Credentials that includes the company logo, company branding, and all of the fields that they require for the type of insurance that they're issuing.

Copyright © 2025 Ping Identity Corporation

They use the credential to issue insurance policy digital credentials that the user stores in their compatible wallet app.

If the user wants to rent a car, they can share digital insurance credential details with the car rental company. Likewise, if the user is involved in a traffic accident, they can share details with the other driver (verifiers) to prove that they have insurance and to verify that their policy is valid.

If the user's insurance coverage stops before the expiration date specified during issuance, such as because of a lack of payment that renders the insurance invalid, BX Insurance Company can revoke the credential given to the user in real-time.

Sharing information from a digital wallet gives the verifiers the additional assurance that the information is up-to-date and represents the real-time status of the person's insurance, something that a paper copy can't provide.

PingOne Credentials allows BX Insurance Company to create numerous custom credentials for all the insurance policies that they want to cover, including:

- House insurance
- Health insurance
- Travel insurance
- Mortgages

After they create these credentials, they can issue them to their users.

Copyright © 2025 Ping Identity Corporation

PingOne Credentials scenarios

These scenarios provide high-level examples of how you can use PingOne Credentials.

The three scenarios that are covered are:

Creating and receiving credentials

Learn how a company can customize the credentials they issue to their customers and the notifications that customers receive.

Presenting and verifying a user credential

Learn how a user can provide proof of credentials to a provider of service (in this case, proof of insurance to a car rental company) and how the provider of service can then verify the user's credentials.

Revoking a credential and notifying a user

Learn how credentials can be revoked from a user's digital wallet app and how users can be notified that the credential was revoked. This scenario also covers how a user's credentials can be reissued.

Scenario: Creating and receiving a credential

In this scenario, a car insurance company, BX Insurance (the issuer) wants to customize an email invitation for digital wallet pairing and create a digital credential they can issue to their customer, John Smith (a user). Afterward, (in a second scenario) John is notified, downloads the digital wallet app, and receives the credential.

Scenario participants

The following parties are involved in this scenario:

Credential Issuer

BX Insurance

User

John Smith

Assumptions

BX Insurance (the credential issuer) meets the following requirements:

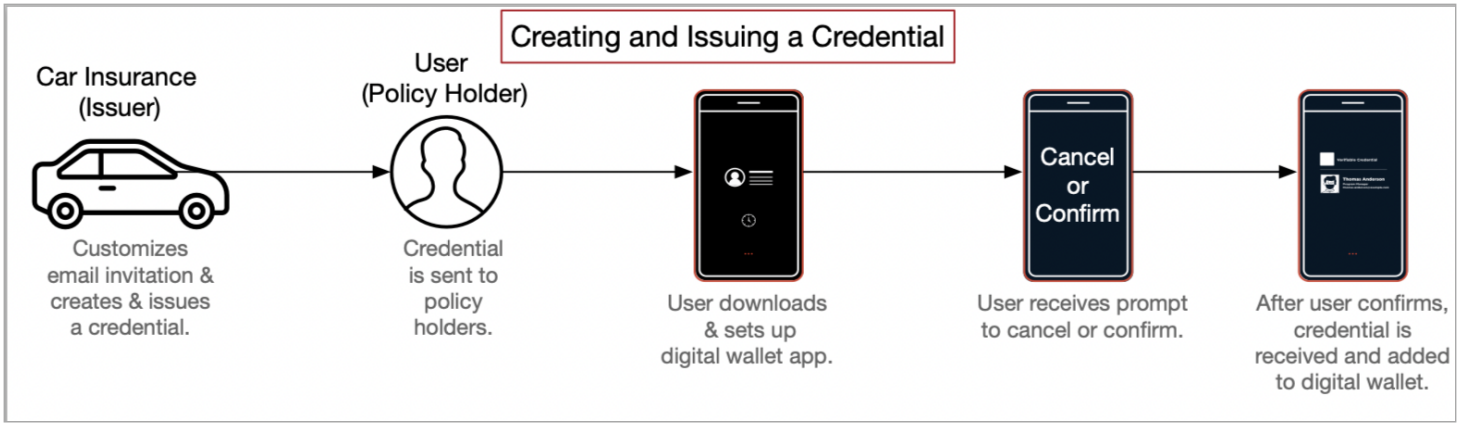
- PingOne Credentials, and PingOne MFA are available in the BX Insurance PingOne environment.
- BX Insurance has a group in their environment named **Current auto insurance subscribers**, and John Smith is a member of that group.

  For more information about creating a group, see Creating a group.
- A mobile developer for BX Insurance has developed and registered an app that runs the PingOne Neo SDK.
- A native application connection added in the BX Insurance environment registered the wallet app.

Copyright © 2025 Ping Identity Corporation

You can find more information about developing a sample app that runs the PingOne Neo SDK and adding a native application connection to register the wallet app in Developing and registering the wallet app that runs the PingOne Neo SDK.

Scenario



1. BX Insurance customizes an email invitation with the BX Insurance name with the text **To set up your BX Insurance Digital Wallet, click this link to download and set up the app**.
2. They create a new credential with the following attributes:
   - First and last name
   - Date of birth
   - Car insurance policy ID number
   - Policy expiration date
3. They select the group **Current auto insurance subscribers**, which John Smith is a part of, to issue the credential to.
4. They select the digital wallet application, save the credential, and then enable it, automatically sending the credential to John Smith.
5. John Smith receives the email invitation on his phone containing a link that says **To set up your BX Insurance Digital Wallet, click this link to download and set up the app**.
6. After clicking the link, he's redirected to the BX Insurance company app in the app store.
7. After he installs the app, the message `Please confirm to pair your wallet to receive a credential` appears.
8. John is presented the option to **Cancel** or **Confirm**.
9. After he taps **Confirm**, the BX Insurance credential is accepted and appears in his digital wallet.

Scenario: Presenting and verifying a user credential

In this scenario, John Smith (the user) wants to reserve a car from BX Rental Cars (the credential verification service) for his vacation next month. Before he can complete the reservation, BX Rental Cars requires that John provide proof that he has a car insurance policy that will be valid throughout the rental period.

Copyright © 2025 Ping Identity Corporation

Scenario participants

The following parties are involved in this scenario:

Credential issuer

BX Insurance

User

John Smith

Provider of a service

BX Rental Cars

Verifier service

The service BX Insurance contracts with for credential verification

Assumptions

BX Insurance (the credential issuer) meets the following requirements:

- PingOne Credentials and PingOne MFA are available in the BX Insurance PingOne environment.
- They created a credential type for the user data required to issue the credential. The credential type includes a connection to a digital wallet app that users can install and use to store their personal credentials.

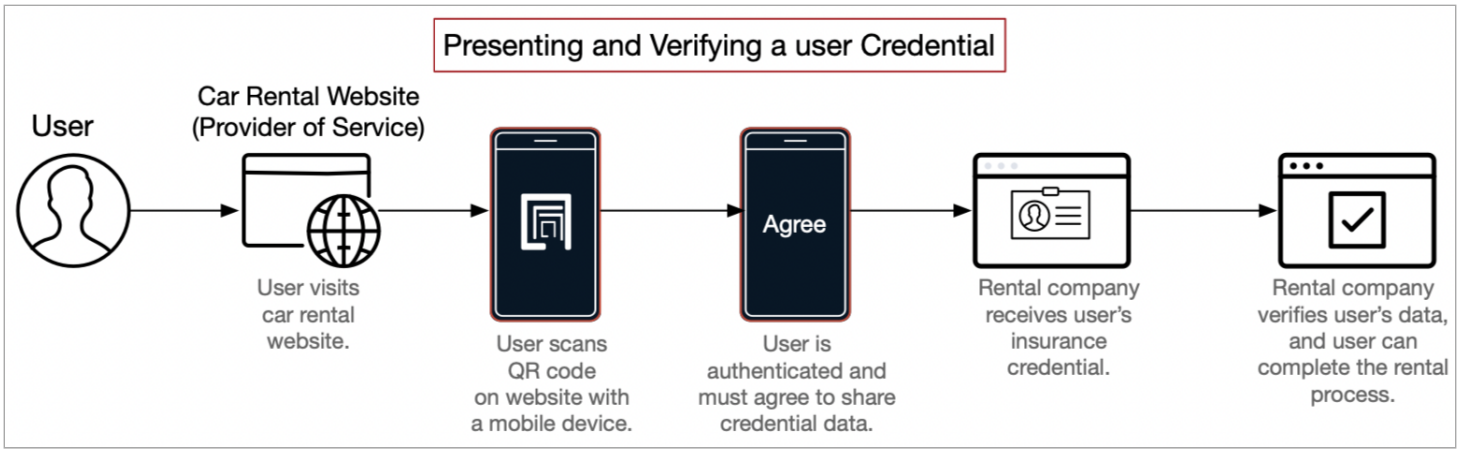
  For more information about creating a credentials template, see Creating a credential.
- BX Insurance customized the following credentials-related notification templates to inform users about the ongoing status of their credentials:
  - Digital Wallet Pairing
  - Credential Issued
  - Credential Revoked
  - Credential Updated

  For more information about notification templates, see Notification templates.

Additionally, John Smith has previously received his credential from BX Insurance, and it is stored in a compatible digital wallet app on his phone. For more information, see Scenario: Creating and receiving a credential.

Copyright © 2025 Ping Identity Corporation

Scenario



1. John visits the **Reservations** page of the BX Rental Cars website from his computer and starts a reservation request.
2. An API call is made from the website to the verifier service BX Rental Cars uses. This creates a new verification session and provides a QR code that BX Rental Cars displays on the screen for John to scan.
3. Using the wallet app on his phone, John scans the QR code.
4. Depending on how the wallet app is configured, John is authenticated by the app.
5. John sees that BX Rental Cars requires the following attributes from his BX Insurance credential:
    - First and last name
    - Date of birth
    - Car insurance policy ID number
    - Policy expiration date
6. Using the app, John agrees to share this data with BX Rental Cars.
7. The verifier service receives the credential, and checks the validity of the data using the public key that BX Insurance uploaded to the Verifiable Data Registry in PingOne Credentials.
8. After the data is verified, the data is delivered to the BX Rental Cars reservation site, and, meeting all of the requirements, John is permitted to complete his rental car reservation.

Scenario: Revoking a credential and notifying the user

In this scenario, John Smith (the user) decided he had a good experience with BX Rental Cars (the credential verification service) on his previous trip over the summer, and decides to rent with them again when he visits his family over the holidays. However, he missed both a notice from BX Insurance (the credential issuer) prompting him to renew his auto insurance and a later notification in his wallet app that his credential was revoked. He no longer has an active auto policy.

Scenario participants

The following parties are involved in this scenario:

Copyright © 2025 Ping Identity Corporation

Credential issuer

BX Insurance

User

John Smith

Provider of a service

BX Rental Cars

Verifier service

The service BX Insurance contracts with for credential verification

Assumptions

BX Insurance meets the following requirements:

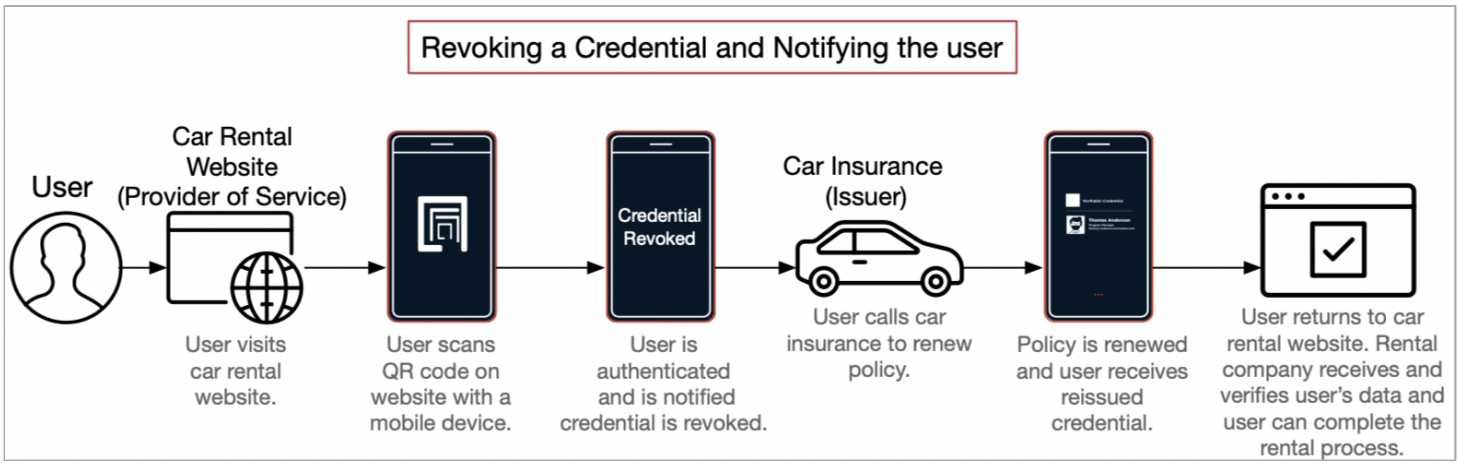
- PingOne Credentials and PingOne MFA are available in the BX Insurance PingOne environment.
- They created a credential type for the user data required to issue the credential. The credential type includes a connection to a digital wallet app that users can install and use to store their personal credentials.

  For more information about creating a credential type, see Creating a credential.
- The issuance rules for the credential type require that the user belong to the "Active Policy" group in PingOne. Membership in that group requires that the user's auto insurance policy is not expired.

  For more information about groups, see Groups.
- BX Insurance customized the Credential Revoked notification template to inform users when their credentials are revoked.

  For more information about notification templates, see Notification templates.

Scenario



1. John visits the **Reservations** page of the BX Rental Cars website from his computer and starts his new reservation request.

2. An API call is made from the website to the verifier service BX Rental Cars uses. This creates a new verification session and provides a QR code that BX Rental Cars displays on the screen for John to scan.
3. Using the wallet app on his phone, John scans the QR code.
4. Depending on how the wallet app is configured, John is authenticated by the app.
5. John sees a notification that his credential from BX Insurance was revoked. When John did not renew his auto policy, he was removed from the "Active Policy" group, invalidating his credential. He cannot complete his reservation.
6. John calls his BX Insurance agent, renews his policy, and pays for his policy extension.
7. After John's policy data updates, John is re-added to the "Active Policy" group and his credential from BX Insurance is reissued.
8. After receiving the updated credential and saving it to his wallet app, John returns to BX Rental Cars reservation site and is able to complete the reservation process.

For more information about revoking credentials, see Revoking a credential.

Getting started with PingOne Credentials

Learn how to get started with PingOne Credentials.

To try out issuance and verification demos for PingOne Credentials, learn more in PingOne Credentials issuance and PingOne Credentials verification test.

> **Note**
> These demos don't require any set up.

Before you begin

To get started with and access PingOne Credentials, you must have:

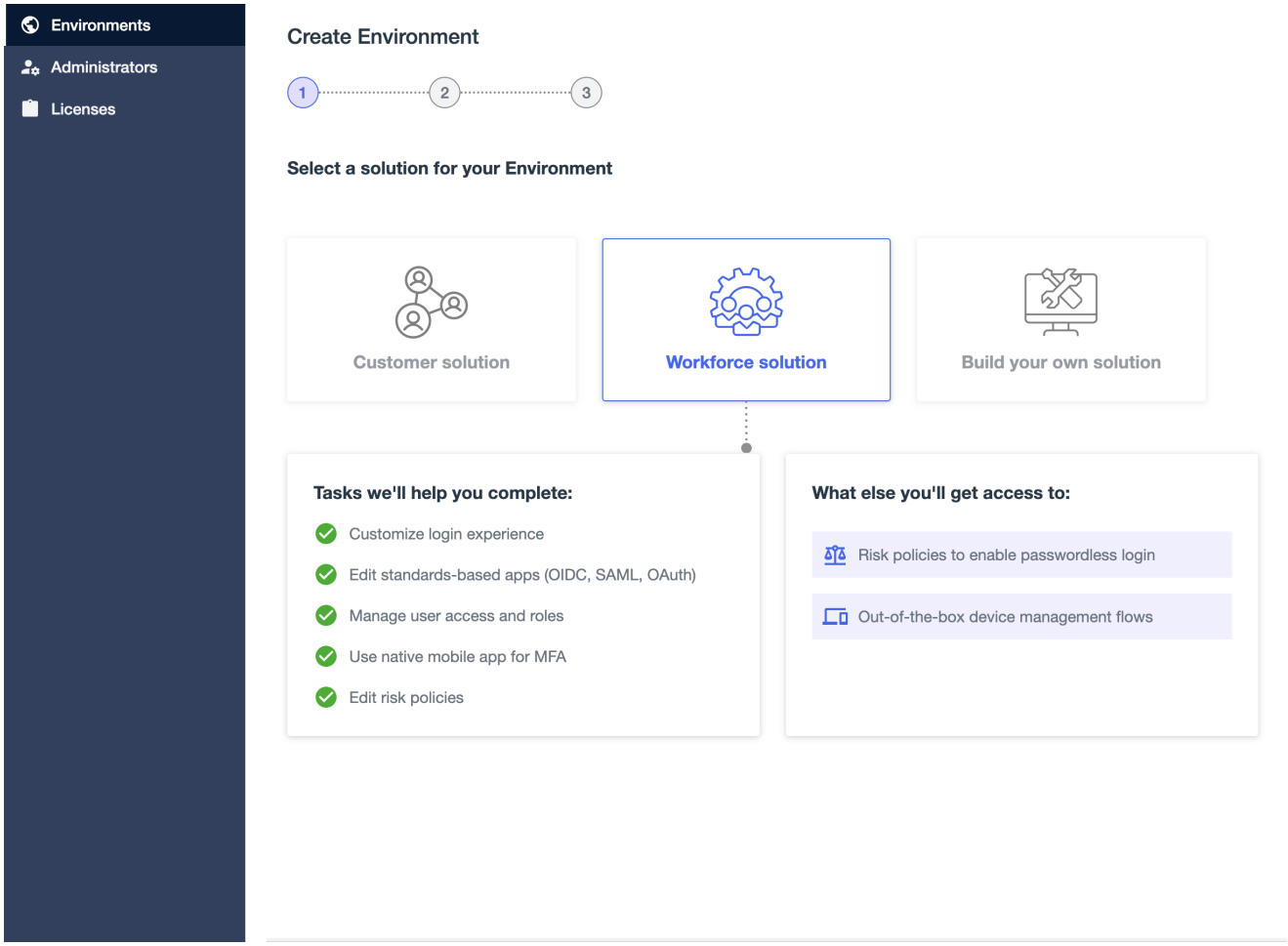
- A PingOne account. Learn more in Starting a PingOne trial.
- An environment with a workforce solution that includes PingOne Credentials, PingID, and DaVinci. Learn more in Building solutions.
- The PingID mobile app.

> **Note**
> For native integration, use the PingOne Neo SDK. Learn more in Developing and registering the wallet app that runs the PingOne Neo SDK.

To set up PingID as your digital wallet, you must have:

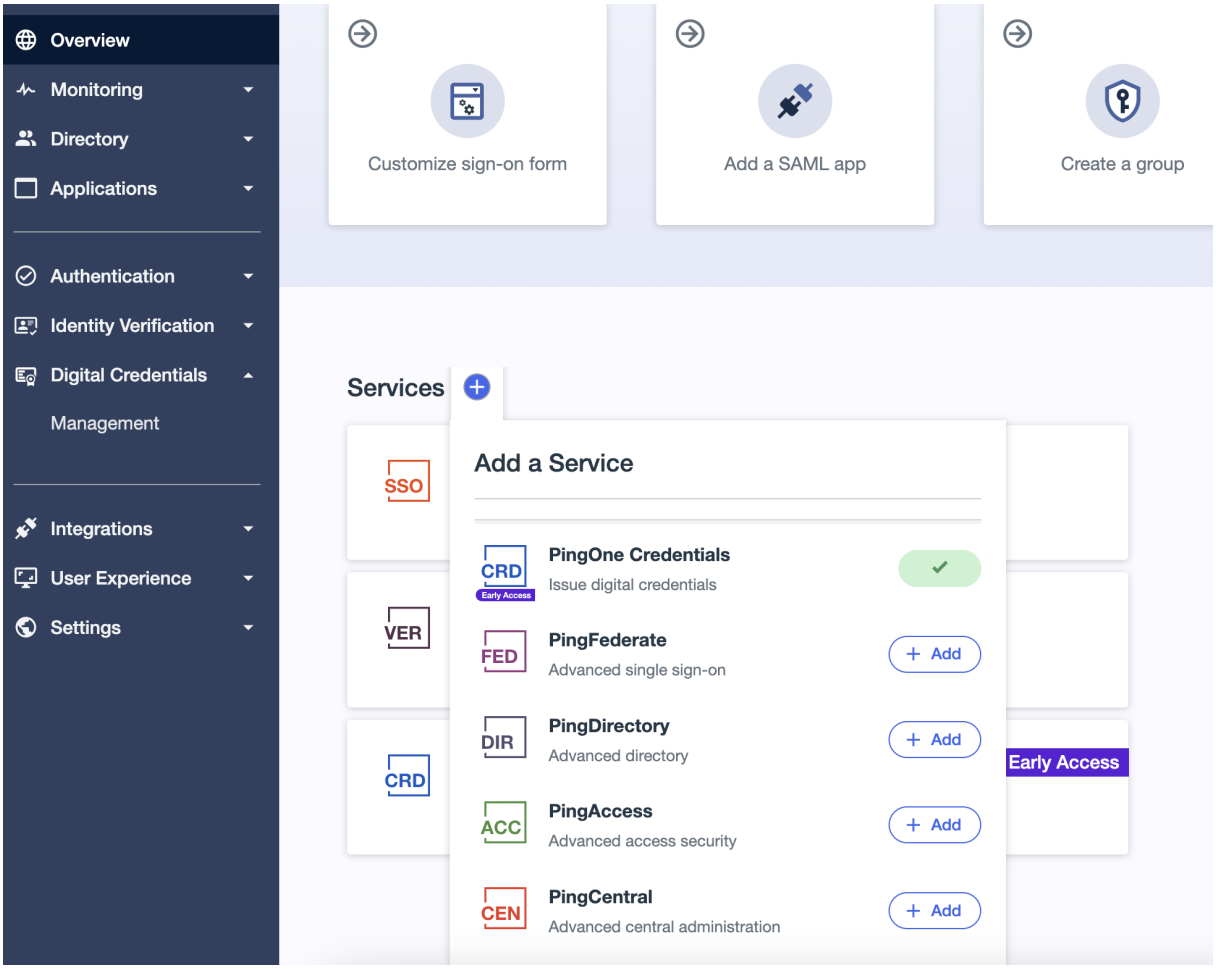
- The PingID mobile app.
- A new environment with a workforce solution. Learn more in Building solutions.

Copyright © 2025 Ping Identity Corporation

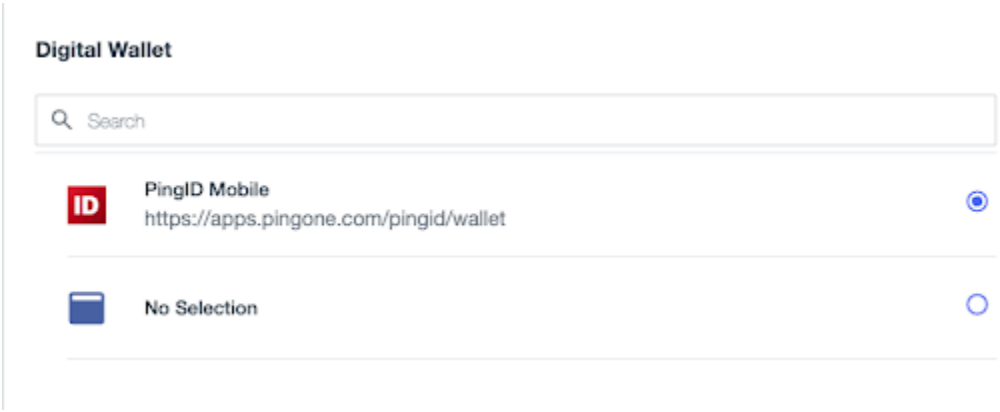


- The PingOne Credentials and DaVinci service in your environment.

Copyright © 2025 Ping Identity Corporation



- A credential. Learn more in Creating a credential. For compatibility with the DaVinci flows used for testing, the **Issue**, **Update**, and **Revoke** issuance rules should be set to **Periodic**, and the PingOne Credentials fields must include the following attributes:
    - **Name - Given Name**
    - **Name - Family Name**
    - **Title**
- PingID selected as your wallet. Learn more in Creating a credential.



Copyright © 2025 Ping Identity Corporation

To test pairing PingID and issuing a credential, you must:

1. Download the PingOne Neo Starter Flow - Setup a User Digital Wallet.
2. Import the flow using the instructions on how to import a flow in How to create a flow in the DaVinci documentation.
3. Launch the flow.

To test verifying a credential, you must:

1. Download the PingOne Neo Starter Flow - Verifiable Credential Presentation Request.
2. Import the flow using the instructions on how to import a flow in How to create a flow in the DaVinci documentation.
3. Launch the flow.

Developing and registering the wallet app that runs the PingOne Neo SDK

About this task

The mobile app guides the user through the process of accepting and sharing credentials. Each user is invited to install and pair their digital wallet by installing a customer-developed app running the PingOne Neo SDK.

Steps

1. Develop an app (for iOS or Android) that runs the PingOne Neo SDK, or embed the SDK into an existing app.

   Learn more in PingOne Neo SDK.

2. In the PingOne admin console, create a PingOne application to register your wallet app:

   1. Go to **Applications** > **Applications**.
   2. Click the **+** icon.

      Result:

      The **Add Application** panel opens.

   3. Enter the appropriate **Application Name** and **Description**.
   4. In the **Application Type** section, click **Native**.
   5. Click **Save**.

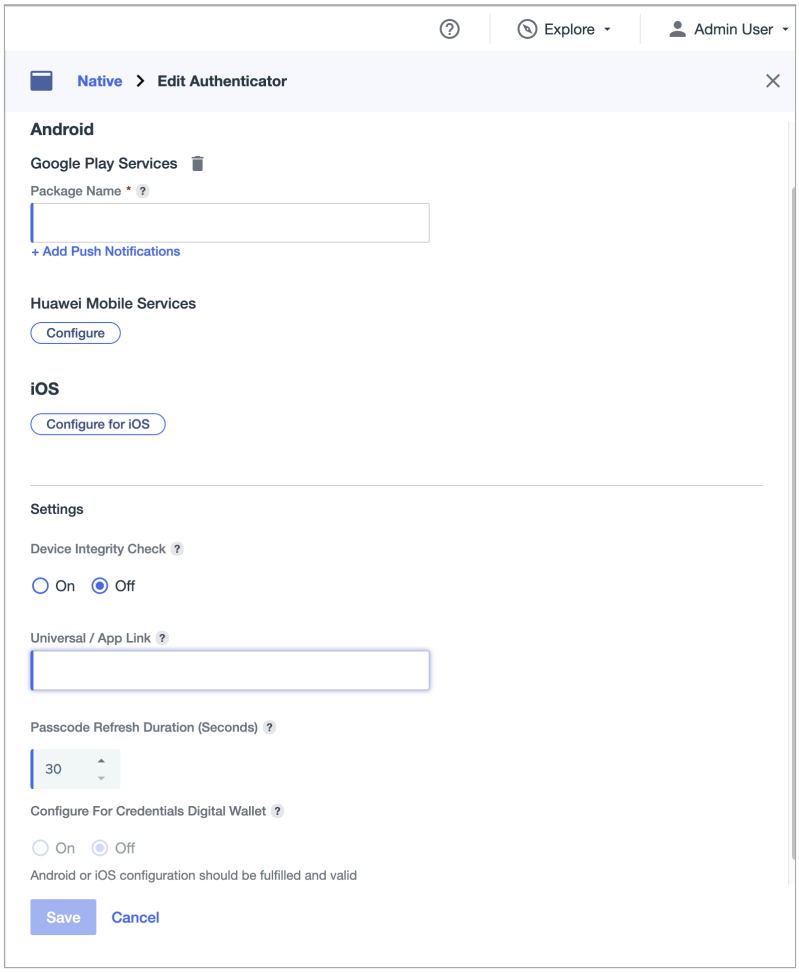
      Result:

   The details panel opens.

3. To configure the app, on the **Mobile** tab, click the **Pencil** icon:

   1. Click **Configure for Android** to configure the app for Android and provide the **Package Name** for Google Play Services or the **Package Name** and **App ID** for Huawei Mobile Services.
   2. Click **Configure for iOS** to configure the app for iOS and provide the **Bundle ID**, as registered in the app store.

Copyright © 2025 Ping Identity Corporation



4. **Optional:** To allow push notifications, click **+ Add Push Notifications**:

    1. For Android apps that use Google Play Services, enter a **Server Key**, as provided by FCM.

    2. For Android apps that use Huawei Mobile Services, enter a **OAuth 2.0 Client ID** and **Client Secret**.

    3. For iOS, enter the **Team ID**, **Select a file** for the**Authentication Token Signing Key**, and enter the **Key ID**, as provided by Apple to your organization.

5. In the **Settings** section:

    1. To turn on **Device Integrity Check**, click **On** to prevent the use of compromised devices for pairing or authentication.

    You can enable device integrity checking separately for Google play Services and iOS.

    1. Adjust the **Cache Duration**, the last device integrity check will be cached for a minimum of 1 minute or a maximum 48 hours.

    2. If your organization is using the PingOne MFA SDK to allow authentication with a QR code in certain flows, provide the relevant **Universal / App Link** or URI scheme that the application should use for this purpose, depending on which deep-linking mechanism the app developers used.

    3. Use the **Passcode Refresh Duration** field to specify the amount of time a passcode should be displayed before it's replaced with a new passcode.

Copyright © 2025 Ping Identity Corporation

4. To turn on **Configuration for Credentials Digital Wallet link**, click **On**, and enter a **Digital Wallet Link**.

> **Note**
> The **Package Name**, **App ID**, **Bundle ID**, and push notification settings cannot be modified after you save the application.

6. Click **Save.**

> **Note**
> To enable or disable your application in PingOne, click the toggle on the **Applications** page.

Customizing PingOne Credentials notification templates

Customize notification templates for PingOne Credentials notifications that end users receive.

Before you begin

You must have PingOne MFA in your environment.

> **Note**
> PingOne MFA provides the default notification templates.

About this task

PingOne Credentials notifications include:

Credential Issued

Notifications to end users when a credential is issued.

Credential Revoked

Notifications to end users when a credential is revoked.

Credential Updated

Notifications to end users when a credential is updated.

Digital Wallet Pairing

Notifications to end users to set up and pair a digital wallet app for storing credentials.

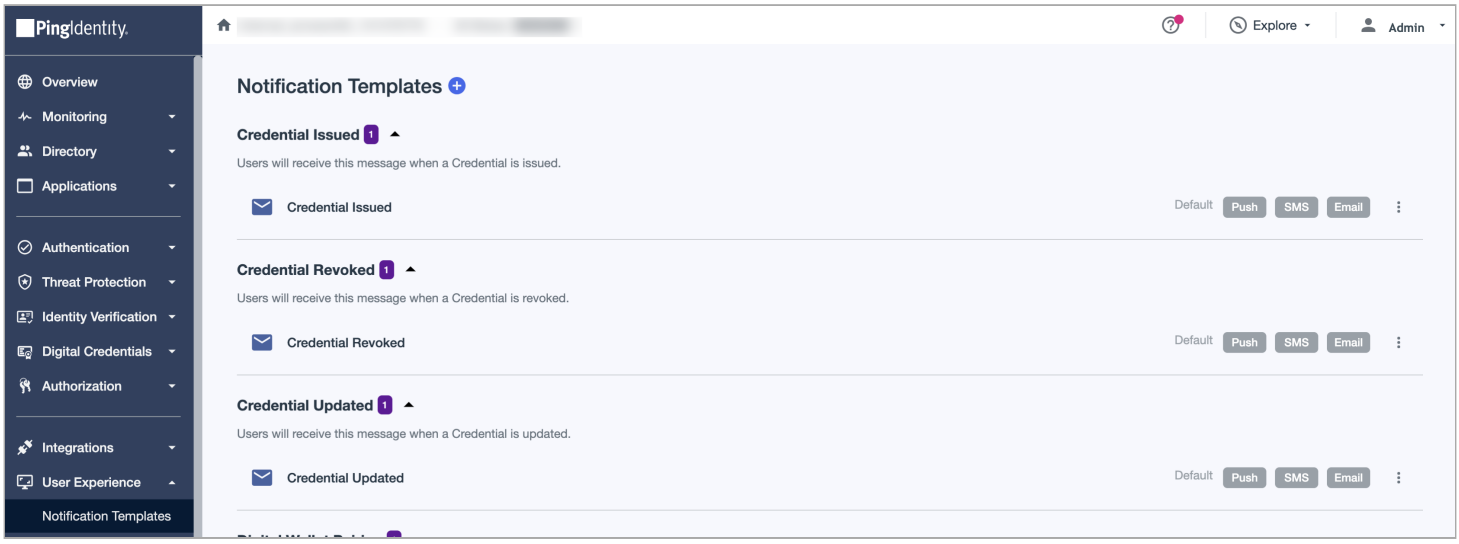
For more information about notification templates, see Notification templates and Editing a notification.

To customize notification templates for the notifications that groups or populations receive:

Steps

1. Go to **User Experience → Notification Templates**.

Copyright © 2025 Ping Identity Corporation

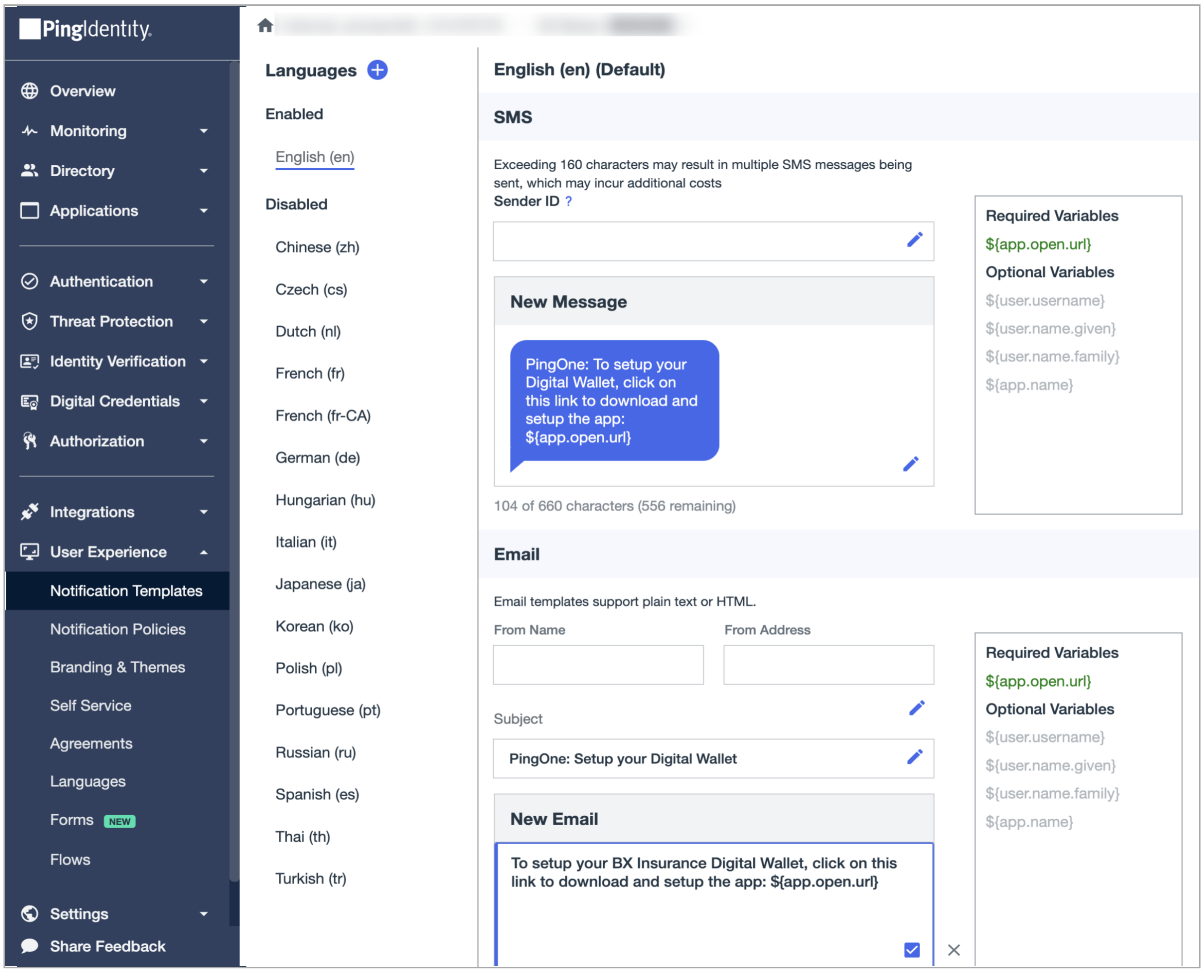


1. Click the **More Options (⋮)** icon for the notification template you want to customize.
2. Click **Edit**.
3. To edit a notification detail, click the **Pencil** icon for the field you want to edit.

   Example:

   For the **Digital Wallet Pairing** template, click the **Pencil** icon for the **New Email** field and enter a custom message, such as `To set up your BX Insurance Digital Wallet, click on this link to download and set up the app.`

Copyright © 2025 Ping Identity Corporation



4. Click the **Checkmark** icon to save your changes.

Credential management method comparison

The PingOne Credentials service offers Automated and API credential management options.

Automated credential management relies on the PingOne platform to automatically issue, edit, and revoke credentials. For example, if you configure a credential to issue to everyone in your PingOne population, a new user added to the PingOne directory automatically receives a credential. If a user is removed from the population, the credential is revoked. Learn more in Creating a credential.

API credential management uses the Credential APIs to issue, edit, and revoke credentials. API credential management requires you to set up listeners to respond to lifecycle events that happen in their external data source to know when to take the appropriate action on the user credential. Learn more in User Credentials.

Copyright © 2025 Ping Identity Corporation

	Definition	Integration	Pros	Cons	Choose if
Automated credential management	Automatically handles interactions between the directory of PingOne and the credential service to issue, edit, or revoke a credential.	Low integration level. Data sync is required to use attributes stored outside of PingOne Directory.	Automated credential management eliminates implementation complexity. PingOne takes care of all credential lifecycle events.	• Personal identifiable information (PII) is stored in PingOne. • Not suited if you have strict data residency or on-prem data residency needs.	You rely on the PingOne platform as your system of record.
API credential management	Uses APIs to issue, edit, or revoke a credential.	Complex integration level	Personal identifiable information (PII) is not stored in PingOne or subject to data residency concerns.	• More complex integration. • Credential lifecycle policy logic is the responsibility of the customer to maintain.	You have strict data residency requirements or existing data stores outside of PingOne

Creating a credential

Define the information that you want to collect from your customer and customize the look and feel of your credential.

About this task

- Customize a credential: Add a background, icon, and customize fonts and colors to create a credential with the branding that your customers know and trust.
- Customize data collection: Add directory attributes, date of issuance, or create alphanumeric text fields to capture more specific customer data. Specify which details appear on the credential and which details are collected as metadata only.
- Preview your credential in real time: When you edit the credential attributes, the card preview area shows your changes as you make them.

Before you begin

- Add PingOne Credentials to your environment.

Copyright © 2025 Ping Identity Corporation

- (Optional) Add PingID to your environment to add PingID as a digital wallet.

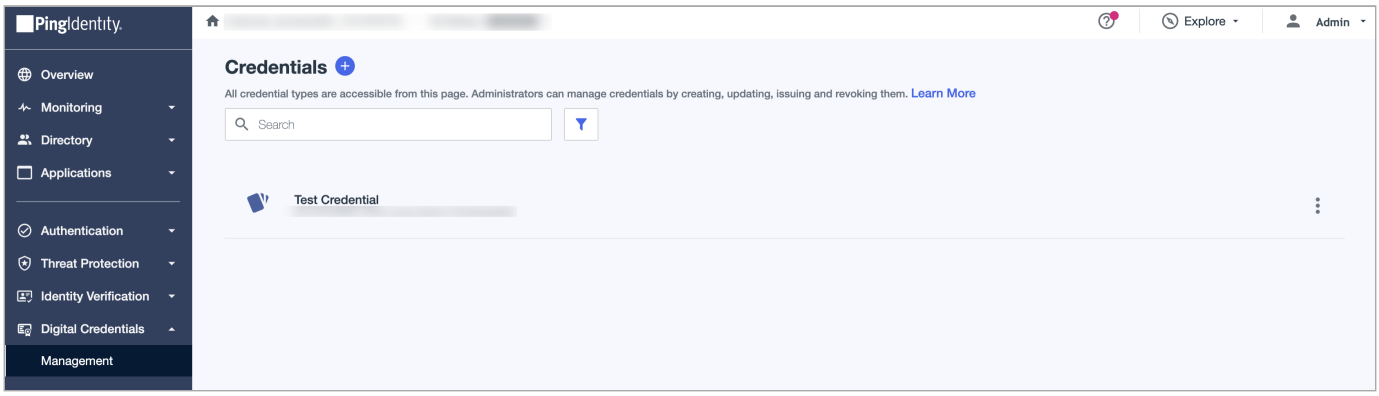
  You can add PingOne Credentials or PingID with a Workforce solution or build your own solution. Learn more in Adding a new environment and Building solutions.

Steps

1. In the PingOne admin console, go to **Digital Credentials** > **Management**.

   Result:

   The **Credentials** page opens, showing a list of any existing credentials.



2. Click the **+** icon.

   Result:

   The **New Credential** window opens.

3. Enter the following:

   > **Note**
   > As you edit attributes, the card preview updates in real time.

Credential Detail	Description
Name and **Subtitle**	Enter a **Name** and **Subtitle** that displays on the credential.
Theme	Configure the appearance of your credential. ◦ To add a logo, click the image under **Logo** and select the image file you want to use. ◦ To change or remove the existing **Logo**, hover over the logo image, click the **Camera** icon, and then click **Upload New Image** or **Remove Image**. **Note** Logo images must be smaller than 25 KB.

Copyright © 2025 Ping Identity Corporation

Credential Detail	Description
Card Styling	Select the **Card Color** and **Font Color** of your credential using the color picker or by entering an RGB value.
Card Background	◦ To add a background image, click the **Image** icon and select the image file you want to use. ◦ To remove an existing image, hover over the image, click the **Camera** icon, and then click **Upload New Image** or **Remove Image**. ◦ Move the **Transparency** slider to the left to increase the transparency of the background and increase the visibility of the credential text. **Note** Background images must be smaller than 50 KB.
Card Fields	Create fields from directory attributes. ◦ In the **Number of Columns** list, select the number of columns that you want to add to your credential. ◦ In the **Field Type** list, select an attribute that corresponds to a user directory attribute or select **Alphanumeric Text** to specify a static value in the credential. ◦ For **Field Title**, enter a title to display on your credential. ■ If **Alphanumeric Text** is selected for **Field Type**, enter a **Title** and **Value**. The value is a static value you provide and doesn't reference a directory attribute. ***Example:*** For **Title**, you can enter `Department`, and for **Value**, you can enter `Human Resources`. ◦ To add a new field, click **+ New Field**. ◦ To change whether a field is shown on the card, click the **Show label on card** ( ) icon. ◦ To make the field required, select the checkbox. ◦ To remove a field, click the **Delete** icon. ◦ To change the order in which the card fields are displayed, click and drag a field to the desired location.

4. Click **Next**.

5. On the **Rules** page, configure your issuance rules that state how often you want to **Issue**, **Update**, and **Revoke** credentials:

   - Click **On Demand** to apply staged changes manually through the API.

   - Click **Periodic** to apply staged changes every minute.

6. Click **Next**.

Copyright © 2025 Ping Identity Corporation

7. To issue your credential, on the **Issuance** page:

   Choose from:

   - Select **Groups** to choose a group that you want to issue credentials to.
   - Select **Populations** to choose a population that you want to issue credentials to.

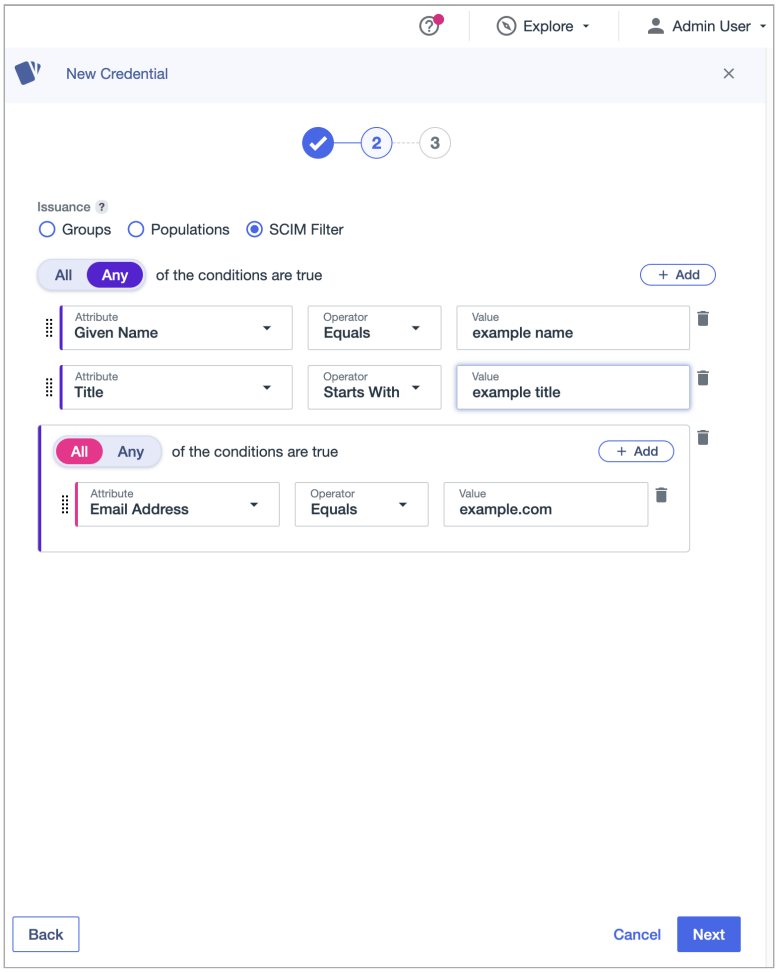
     > **Note**
     > If you select multiple groups or populations, a user has to be a member of at least one of those selected to be issued a credential.

   - Select **SCIM Filter** to create a filter that identifies a certain category of users to issue credentials automatically based on attributes from the PingOne Directory.

     1. Enter the first condition:
        - **Attribute**: Select an attribute.
        - **Operator**: Select **Equals**, **Starts with**, **Ends With**, or **Contains**.
        - **Value**: Enter the appropriate value.
     2. (Optional) Click **+ Add**, and then click **Condition** to add another condition or **Condition Set** to add a set of conditions.
     3. Select **All** or **Any** to determine how the linked conditions will be evaluated.

        > **Note**
        > To delete a condition, click the **Delete** icon.

Copyright © 2025 Ping Identity Corporation



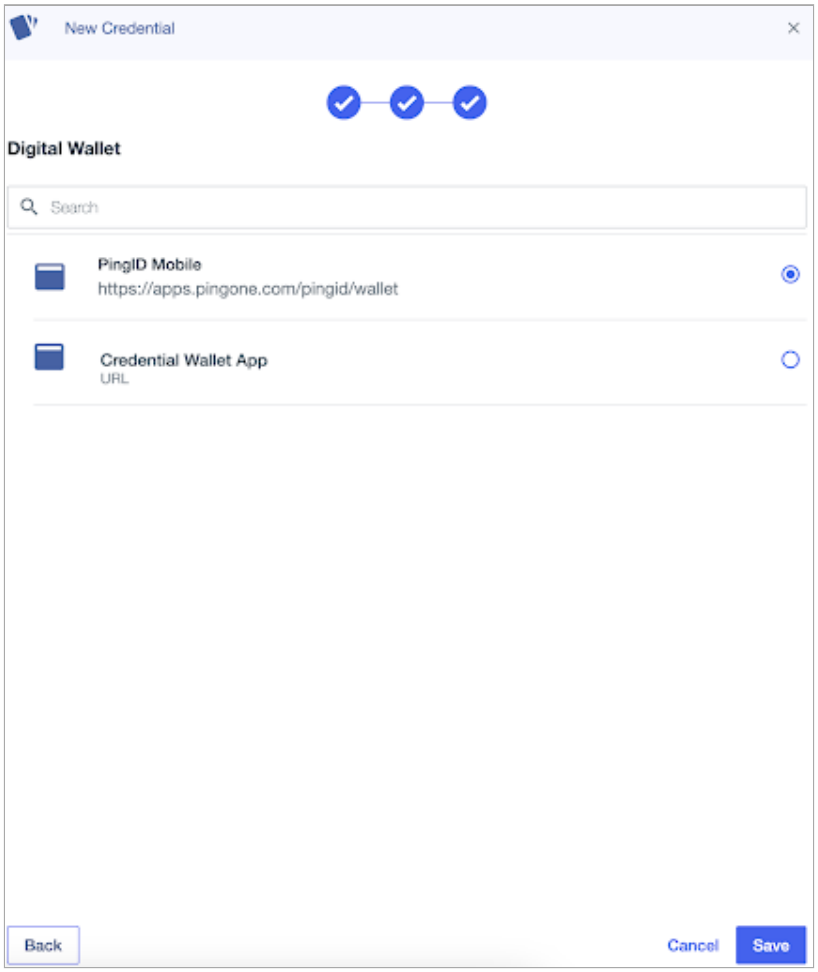
8. Click **Next**.

9. On the **Digital Wallet** page, click an application from the list or search for the application you want to use as a digital wallet.

> **Note**
>
> You can only select one application.

   - (Optional) To add a PingID digital wallet, select the PingID mobile application in the list or search for the application and then click to select it.
   - Click **No selection** to choose a digital wallet later.

Copyright © 2025 Ping Identity Corporation



10. Click **Save**.
11. To enable the credential, click the toggle on the **Credentials** page.

> **Note**
>
> You can find more information about viewing a user's assigned credential in the **Users** page in Managing a user's credentials.

Editing a credential

Edit the look and feel of your credential, the recipients of the credential, and the digital wallet.

Steps

1. In the PingOne admin console, go to **Digital Credentials** > **Management**.

   Result:

   The **Credentials** page opens, showing a list of your existing credentials.

2. For the credential you want to edit, click the credential, or click the **More Options** (⋮) icon and then click **Overview**.

3. To edit the credential, click the **Pencil** icon in the relevant section and edit any of the following as needed:
   - **Card**: The following table lists the details you can edit.

> **Note**
>
> Click on the **Download** ( ) icon on the credential to download an SVG file of your credential's template.

Credential Detail	Description
Name and **Subtitle**	Enter a **Name** and **Subtitle** that displays on the credential.
Theme	Configure the appearance of your credential. ■ To add a logo, click the image under **Logo** and select the image file you want to use. ■ To change or remove the existing **Logo**, hover over the logo image, click the **Camera** icon, and then click **Upload New Image** or **Remove Image**. **Note** Logo images must be smaller than 25 KB.
Card Styling	Select the **Card Color** and **Font Color** of your credential using the color picker or by entering an RGB value.
Card Background	■ To add a background image, click the **Image** icon and select the image file you want to use. ■ To remove an existing image, hover over the image, click the **Camera** icon, and then click **Upload New Image** or **Remove Image**. ■ Move the **Transparency** slider to the left to increase the transparency of the background and increase the visibility of the credential text. **Note** Background images must be smaller than 50 KB.

Copyright © 2025 Ping Identity Corporation

Credential Detail	Description
Card Fields	Create fields from directory attributes. ■ In the **Number of Columns** list, select the number of columns that you want to add to your credential. ■ In the **Field Type** list, select an attribute that corresponds to a user directory attribute or select **Alphanumeric Text** to specify a static value in the credential. ■ For **Field Title**, enter a title to display on your credential. ■ If **Alphanumeric Text** is selected for **Field Type**, enter a **Title** and **Value**. The value is a static value you provide and doesn't reference a directory attribute. ***Example:*** For **Title**, you can enter `Department`, and for **Value**, you can enter `Human Resources`. ■ To add a new field, click **+ New Field**. ■ To change whether a field is shown on the card, click the **Show label on card** ( ) icon. ■ To make the field required, select the checkbox. ■ To remove a field, click the **Delete** icon. ■ To change the order in which the card fields are displayed, click and drag a field to the desired location.

- **Rules**: Edit your issuance rules that state how often you want to **Issue**, **Update**, and **Revoke** credentials by selecting one of the following:
  - Click **On Demand** to apply staged changes manually through the API.
  - Click **Periodic** to apply staged changes every minute.
- **Issuance**: Edit the recipient of the credential by selecting one of the following:
  - **Groups**: Choose a group to which to issue the credential.
  - **Populations**: Choose a population to which to issue the credential.
  - **SCIM Filter**: Create a filter that identifies a category of users to which to issue the credential:
    - Select an **Attribute** and **Operator**, and enter a **Value**.
    - To add a new attribute, click **+ Add** and select **Condition** or **Condition Set**.
    - To remove a condition, click the **Delete** icon.
    - Click **All** or **Any** to determine how to filter using your attributes.

Copyright © 2025 Ping Identity Corporation

- **Digital Wallet**: To select an application, click the application from the list, or search for the desired application and then click to select it.
  - Click **No selection** to choose a digital wallet later.

4. Click **Update**.

Revoking a credential

You can revoke a credential if it is no longer valid and should be removed.

To revoke a credential, you change the issuance rule or SCIM filter. You can either remove or change the group, population, or SCIM filter so that the user doesn't match anymore.

> **Note**
>
> You can only delete a credential through the API.

You can also revoke a credential from a user in the **Users** page. Learn more in Managing a user's credentials.

To revoke credentials in PingOne Credentials:

Steps

1. In the PingOne admin console, go to **Digital Credentials** > **Management**.
2. Click the relevant credential.

   Result:

   The **Card Preview** window opens.

3. In the **Issuance** section, click the **Pencil** icon.

   Choose from:

   - Select **Groups** and clear the group to revoke credentials.
   - Select **Populations** and clear the population to revoke credentials.
   - Select **SCIM Filter**, and delete or edit conditions as needed to revoke permissions based on different criteria.

4. Click **Update**.

Result

Credentials for users no longer meeting the criteria are revoked.

Copyright © 2025 Ping Identity Corporation

Authorization using PingOne Authorize

PingOne Authorize is a cloud-based authorization service that controls what end users can see and do inside of applications and APIs.

PingOne Authorize allows organizations to centrally configure authorization requirements, ranging from simple rules to real-time, fine-grained policies. Centralized authorization enables Identity and Access Management (IAM) teams and stakeholders to collaborate and quickly adapt to new requirements, use cases, and regulations.

What's new?

- Integrate PingOne Authorize with Amazon CloudFront.
- Deploy policies on-premise with Authorize gateways.
- Protect sensitive API resources with Step-up authentication for APIs.
- Use custom OAuth parameters in HTTP service requests.
- Assign users to application roles.
- Add role-based permissions to access tokens.

Get started

- What is PingOne Authorize?
- What are PingOne environments?
- Start a PingOne trial
- Add PingOne Authorize to your PingOne environment

Tutorials

- Control access to all APIs on a service
- Control access to specific API operations
- Build your first dynamic authorization policy
- Control access to an API operation with a fine-grained policy

Copyright © 2025 Ping Identity Corporation

Use PingOne Authorize

- Define policy building blocks in the Trust Framework
- Build authorization policies
- Deploy authorization policies
- Examine authorization decisions
- Define your API in PingOne Authorize
- Define operations for protected actions

Integrations and connectors

API gateways

- Amazon Web Services integration
- Apigee integration
- Kong Gateway integration
- Kong Konnect integration
- PingGateway integration

DaVinci orchestration flows

- PingOne Authorize connector

Developer resources

- Get started with PingOne APIs
- Policy decision service API reference
- API Access Management API reference

Copyright © 2025 Ping Identity Corporation

Troubleshooting

- Audit logs
- Event monitoring
- System status
- Authorization Dashboard
- Troubleshoot API Access Management issues
- Troubleshoot Kong Gateway integration

Introduction to Authorization

PingOne Authorize is a cloud-based authorization service that controls what end users can see and do inside of applications and APIs.

Modern customer experiences demand sophisticated authorization controls balanced with continuous security, consistently applied across an exploding number of applications. PingOne Authorize allows organizations to centrally configure authorization requirements, ranging from simple rules to real-time, fine-grained policies. Rather than scatter control among IT infrastructure and application code, centralized authorization enables Identity and Access Management (IAM) teams and stakeholders to collaborate and quickly adapt to new requirements, use cases, and regulations.

PingOne Authorize has the following capabilities:

API Access Management

API Access Management addresses the needs of IAM teams by simplifying common API access control use cases and eliminating the guesswork of OAuth and OpenID Connect. Learn more in API Access Management.

Dynamic Authorization

Dynamic Authorization addresses the needs of application owners and stakeholders, empowering them to leverage real-time data in fine-grained policies that go well beyond identity and roles. PingOne Authorize can integrate with other PingOne services, such as PingOne Protect, and exploit information in a PingOne user profile to augment authorization events in real-time. Learn more in Dynamic authorization.

You can implement PingOne Authorize using either of these methods:

- Manage policies and authorization decisions entirely in PingOne. Use this method for centralized management of all of your authorization needs in Ping Identity's cloud.
- Manage policies and deployment services in PingOne and process authorization decisions in your organization's infrastructure, under your control. Use this method for high-volume, low latency authorization situations and when compliance and security considerations require on-premise deployment. Learn more in Authorize gateways.

Copyright © 2025 Ping Identity Corporation

Use the PingOne Authorize connector to make policy-based authorization decisions in your PingOne DaVinci flows. Learn more in PingOne Authorize Connector.

Learn about Ping Identity's entirely on-premise dynamic authorization solution in PingAuthorize.

Dynamic authorization

With dynamic authorization, centralized rules and policies control what users can see and do in your application. Policies evaluate context to determine access, including preferences, devices, risk scores, history, behaviors, transactions, and financial data. You can pull in additional signals in real-time when transactions are made.

Dynamic authorization offers significant benefits over role-based control:

Enhanced visibility and control

Replace hundreds of roles with a few policies that are centrally managed across sensitive applications. This streamlines your access management process and makes it easy to update and deploy policies across your organization.

Greater business agility

Take authorization out of your applications and centralize it to deliver a better user experience more quickly. Any stakeholder can collaborate on policy without code changes or application downtime. Your organization can react quickly to business challenges or changing regulatory requirements, increasing your agility and flexibility.

Improved security and regulatory compliance

Central monitoring and tracking of user activity and data access provides greater insight into user behavior and suspicious activities. Safeguard your sensitive data and address your customer's growing data privacy concerns by giving them greater control over and insight into their data and how it's used.

Lower costs

Bring new solutions to market faster because you don't have to wait for code changes on the backend. The capability to update your authorization logic in seconds allows your organization to focus on core competencies instead of access control.

How dynamic authorization works

Dynamic authorization externalizes access decisions to a decision service that determines what a user can see and do based on centrally managed policies and additional information gathered from information points. Attributes and rules are used in policies to instantiate business logic.

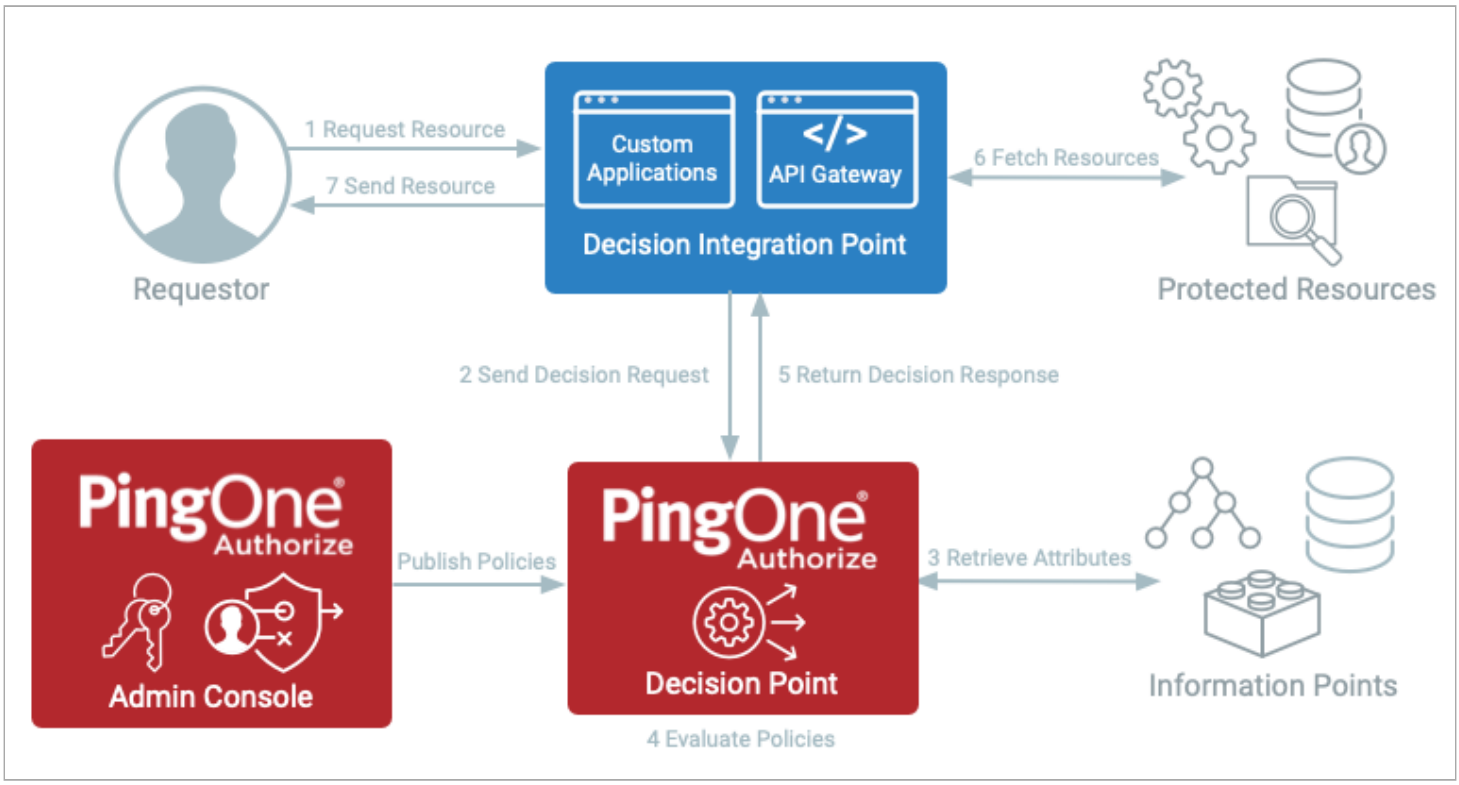
The following components are involved in dynamic authorization.

Component	Description
Admin console	Enables centralized authoring and management of policies, including a built-in decision endpoint for testing. This is sometimes known as a Policy Administration Point (PAP).

Copyright © 2025 Ping Identity Corporation

Component	Description
Decision integration point	Intercepts requests to protected resources and packages relevant information into a decision request, then sends the request to the decision service. Also passes the decision response back to the application. This is sometimes known as a Policy Enforcement Point (PEP). An API gateway is one type of decision integration point.
Decision service	Receives a decision request, evaluates the request against relevant policies, and returns a decision response that permits or denies access, or causes other systems to take additional actions. This is sometimes known as a Policy Decision Point (PDP), and in PingOne Authorize, it's part of the admin console.
Information point	Provides the decision service with additional information used to make an informed decision. This is sometimes known as a Policy Information Point (PIP). You define information points, such as data APIs, as attributes and services in the **Trust Framework**.

The following diagram shows a typical dynamic authorization request flow. Numbers in the diagram correspond to the steps that follow.



1. A user requests access to a protected resource through your application, such as viewing account details, accessing a database, or making a payment.
2. The decision integration point intercepts the user's request and builds a decision request with relevant information, such as attributes for the requestor's ID or account number. Then, the integration point sends the request to the decision service.

Copyright © 2025 Ping Identity Corporation

3. The decision service identifies targeted policies, which are authored and deployed using the admin console, that relate to protection of the resource, such as whether the account is active, or the user is a manager. Then the decision service calls out to registered information points to obtain extra information, such as the rest of the user information for that user ID.
4. The decision service evaluates relevant policies.
5. The decision service builds the decision response and sends it back to the decision integration point. The decision response includes a permit or deny decision and statements and advice that provide additional information for upstream applications to act on.
6. If the decision permits, the decision integration point fetches the protected resource. Based on presence statements, additional actions are triggered that allow contextually responsive user flows.
7. The decision integration point sends the resource to the requester with restrictions on the details and resources sent back that are based on the decision response.

API Access Management

API Access Management provides a simple way to manage access control while extending the authorization capabilities of your organization's API gateway.

With API Access Management, IAM teams centrally manage common access control use cases in PingOne, while enforcement is distributed to API gateways using Ping Identity integration kits. Now IAM teams can focus on authorization and access control, while IT architects and developers can focus on core API features.

Through centralized management and continuous evaluation of policy, you can have confidence that only the right users are accessing APIs, resources, and data.

API Access Management provides:

- Centralized, user-friendly configuration that smooths over the complexities of working with OAuth across multiple systems, with a powerful policy engine behind the scenes.
- Centralized visibility of API activity, including runtime auditing with a focus on authorization events.
- Coarse-grained access control that ensures only the right users and clients access API services.
- More granular access control for individual API operations, including rules based on group membership, authorized scopes, application permissions, the policy used for authentication, and the amount of time since authentication.
- Fine-grained access control for API services and operations through custom dynamic authorization policies.
- Advice statement processing for filtering and transformation of API request and response data.

API Access Management integrates with your API gateway to enforce access control policies on behalf of the API. Ping Identity provides integration kits for the following API gateways:

- Amazon Web Services
- Apigee
- Kong Gateway
- Kong Konnect

Copyright © 2025 Ping Identity Corporation

How API Access Management works

The following components are involved in API Access Management.

API Gateway

Your API gateway helps your organization manage the full lifecycle of APIs through design, development, testing, deployment, versioning, security, and analytics. To simplify authentication and authorization for the API services behind the API gateway, a Ping Identity integration kit installed in your API gateway connects to the HTTP Access Policy service in PingOne. Your API gateway acts as the policy enforcement point when policy decisions are provided by the HTTP Access Policy service at runtime.

Learn more about installing the integration kit for your API gateway in API gateway integrations.

Learn more about configuring the connection between your API gateway and PingOne in API gateways.

API service

API services are typically microservices and serverless functions developed by your organization to perform business or application functions. Access is routed through your API gateway to your API services. API gateways typically refer to API services as target APIs, upstream APIs, or backend APIs.

Using API Access Management, access control is managed centrally in PingOne Authorize, while enforcement is delegated to your API gateways. You can define operations with rules that control access to specific APIs within the API service.

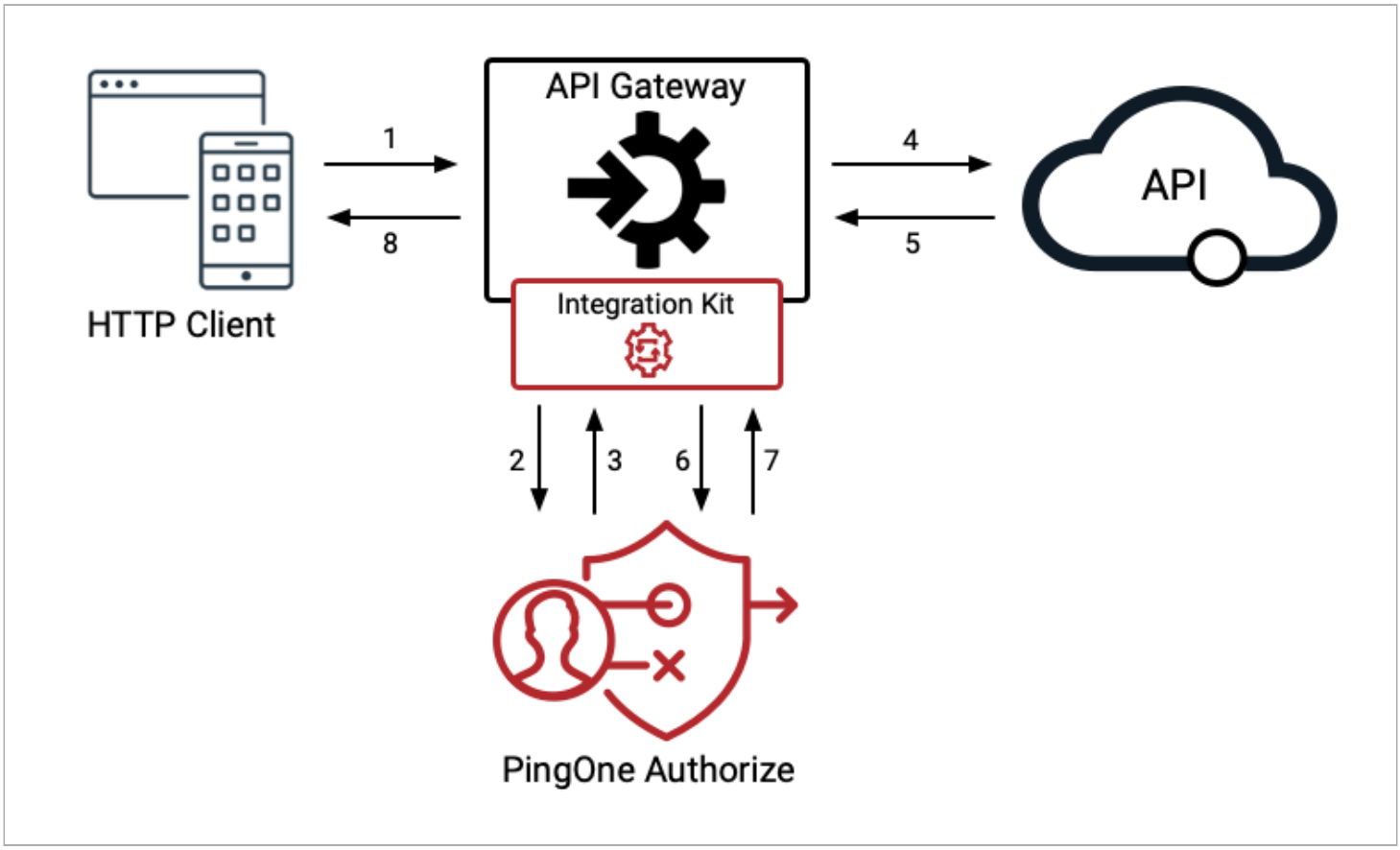
Learn more about configuring an API service and access control rules for a protected API in API services.

HTTP Access Policy Service

This PingOne Authorize runtime service provides the authentication and authorization decisions to your API gateway. Policy decisions are determined by evaluating the access control rules configured within the API services in PingOne Authorize.

The following diagram shows how traffic flows through an API gateway, PingOne Authorize, and a protected API. Numbers in the diagram correspond to the steps that follow.

Copyright © 2025 Ping Identity Corporation



1. The API Client makes a request to the API gateway.
2. The integration kit installed in the API gateway extracts fields from the API Client's request and sends them to the HTTP Access Policy service in PingOne Authorize for authorization.
3. PingOne Authorize evaluates the request, validates the authorization, then responds to the API gateway. The response can be an authentication or authorization error that is sent back to the client immediately, or a modified request that the API gateway sends to the backend API.
4. If authorized to proceed, the API gateway passes the original or modified API request to the backend API.
5. The backend API responds to the API gateway with the requested resource or result of the operation.
6. The integration kit in the API gateway extracts fields from the backend API's response and sends them to the HTTP Access Policy service in PingOne Authorize for processing.
7. PingOne Authorize responds to the processing request. The API response can be modified by authorization policy in PingOne Authorize.
8. The API gateway responds to the API Client with the original API response received from the backend API or the modified response received from PingOne Authorize.

Get started with PingOne Authorize

Learn more about setting up PingOne Authorize in your PingOne environment in Getting started with PingOne Authorize.

Copyright © 2025 Ping Identity Corporation

Use the tutorials to familiarize yourself with PingOne Authorize capabilities:

- Manage API access
- Build dynamic authorization policies

Getting started with PingOne Authorize

Set up your PingOne environment to get stared with PingOne Authorize.

Start by adding the PingOne Authorize service to your environment. When your environment includes PingOne Authorize, you're ready to use API Access Management.

Next, add a worker application that provides access to PingOne APIs and enables you to create dynamic authorization policies.

Adding the PingOne Authorize service to your environment

To get started with PingOne Authorize, add the service to your PingOne environment.

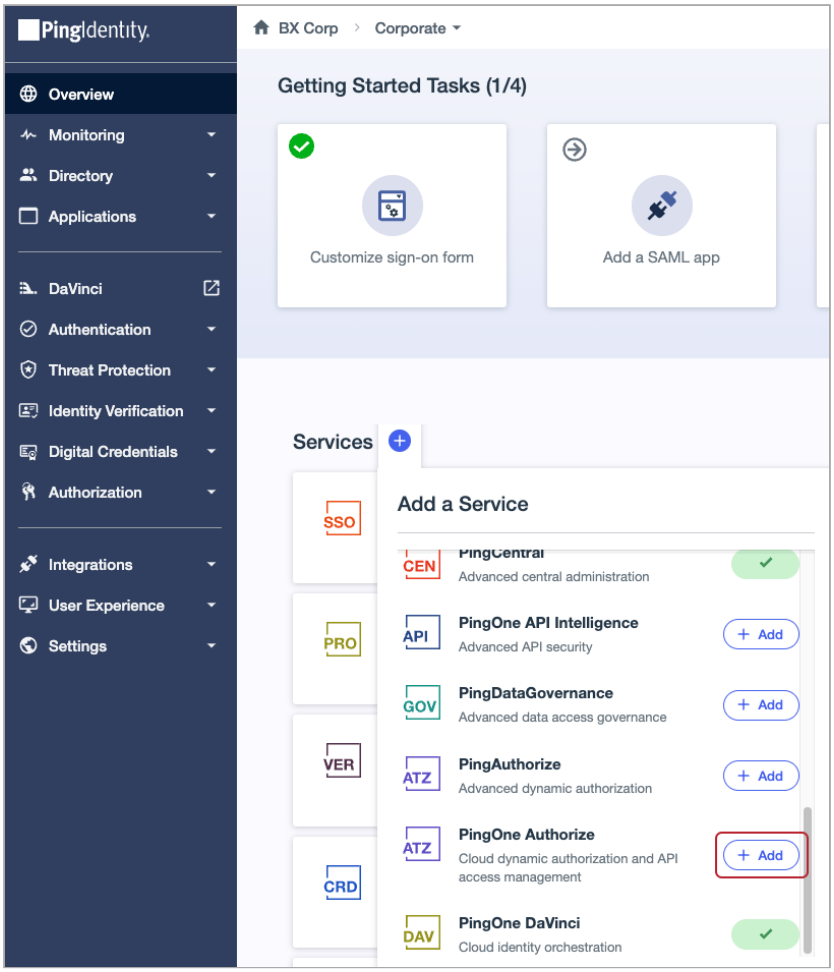
Before you begin

- If you don't have a PingOne account yet, start a PingOne trial.
- Make sure you can sign on to the PingOne admin console.
- Add an environment to organize your services.
- Make sure you have the Environment Admin and Identity Data Admin roles, or a custom role with equivalent permissions, in your PingOne environment. Learn more in Managing user roles.

Steps

1. In your PingOne environment, go to **Overview**.
2. Next to **Services**, click the **+** icon.
3. Click **+ Add** to add the **PingOne Authorize** service.

Copyright © 2025 Ping Identity Corporation



4. In the **Add a Service** window, click **Finish**.

   PingOne Authorize is displayed in the left navigation pane.

Adding a worker application for the PingOne Authorize service

After PingOne Authorize is in your PingOne environment, add a worker application to enable dynamic authorization API actions for the service.

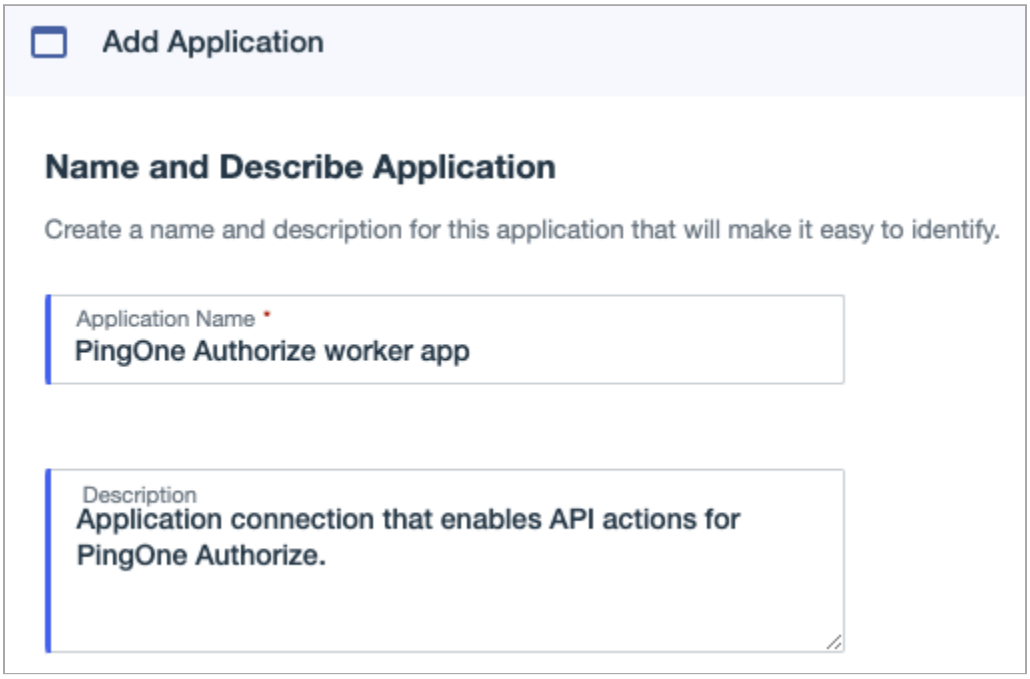
PingOne integrates with client applications through application connections that define access to PingOne resources. A worker application is a userless service application connection that can perform administrator functions. Access is encoded in the worker application's access token, which you submit with API requests. Learn more about how PingOne manages access to applications in Applications.

> **Note**
>
> You must assign the Environment Admin and Identity Data Admin roles, or a custom role with equivalent permissions, to the worker application after you create it. Learn more in Configuring roles for a worker application.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications**.

2. Click the + icon next to **Applications**.
3. For **Application Name** and **Description**, enter a unique identifier for the application and a brief characterization of the application.



4. For the **Application Type**, click **Worker**.
5. Click **Save**.

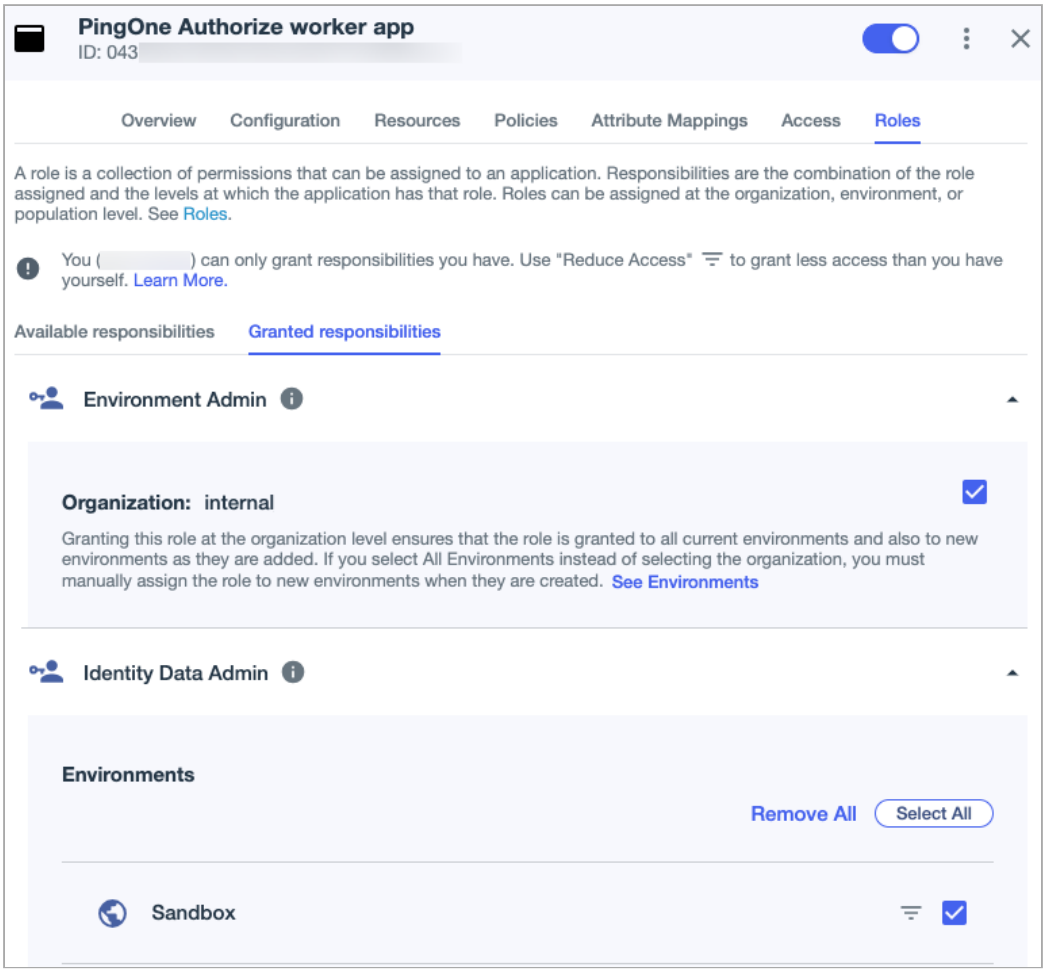
   Result:

   The **Applications** page displays your worker application.

6. On the **Roles** tab, click **Grant Roles**.
7. In **Available responsibilities**, select the following roles:
   - **Identity Data Admin** role for your environment
   - **Environment Admin** role for your organization, or for a specific environment

     The **Granted responsibilities** tab provides a simplified view of your selected roles.

Copyright © 2025 Ping Identity Corporation



8. Click **Save**.
9. (Optional) Configure the **Token Endpoint Authentication Method**.

   HTTP services that access PingOne APIs with the client credentials grant type expect credentials in the body of a token request (`client_secret_post`) instead of in the `Authorization` header (`client_secret_basic`).

   1. On the **Configuration** tab, click the ✎ icon.
   2. In the **Token Endpoint Authentication Method** list, select **Client Secret Post**.
   3. Click **Save**.
10. To enable the application, click the **Enable** toggle.

Next steps

Complete these tutorials to familiarize yourself with PingOne Authorize capabilities:

- Manage API access

Copyright © 2025 Ping Identity Corporation

- Build dynamic authorization policies

PingOne Authorize tutorials

Authorization tutorials guide you through the capabilities of PingOne Authorize.

Dynamic authorization

Learn how to build, test, and publish authorization policies and the **Trust Framework**.

- Build and publish your first authorization policy

API Access Management

Learn how to manage API access with an API gateway integration.

- Tutorial 1: Access control for managed API services
- Tutorial 2: Access control for specific API operations
- Tutorial 3: Fine-grained authorization for API operations

Build dynamic authorization policies

Use the tutorials to familiarize yourself with the dynamic authorization capabilities of PingOne Authorize.

Before you begin

- Make sure the PingOne Authorize service is in your environment.

> **Note**
> For this tutorial, you'll use PingOne Authorize, not PingAuthorize, so make sure you've added PingOne Authorize to your environment.

- Make sure you have a worker application connection for the PingOne Authorize service.
- Install Postman. You'll use a collection of Postman requests to simulate an application making decision requests.

Copyright © 2025 Ping Identity Corporation

Building your first dynamic authorization policy

Learn how to build your first dynamic authorization policy, from adding an attribute and a policy, through publishing the policy and making and examining decision requests.

You'll build a simple policy that walks through the dynamic authorization capabilities of PingOne Authorize. In this example use case, imagine you're a bank that wants to deny payments over 10,000 USD because they're sometimes fraudulent.

What you'll learn

- How to connect to data sources with attributes
- How to capture business logic in policies and test policy behavior
- How to iterate on policies through updates and retesting
- How to publish policies and set up decision endpoints
- How to make decision requests and examine recent decisions

Adding an attribute

Learn how to use the **Trust Framework** to add an attribute that you can use in a dynamic authorization policy.

About this task

You need to know the payment amount to determine if it's greater or less than $10,000 USD, so let's add an attribute for the amount to the Trust Framework.

The **Trust Framework** provides an enterprise-wide view of your data and service ecosystem. It's where your organization's technical people capture definitions for digital assets, services, and users across all domains in your organization, including:

- Attributes used in policies
- Connections to APIs
- Information points used as data sources for attributes

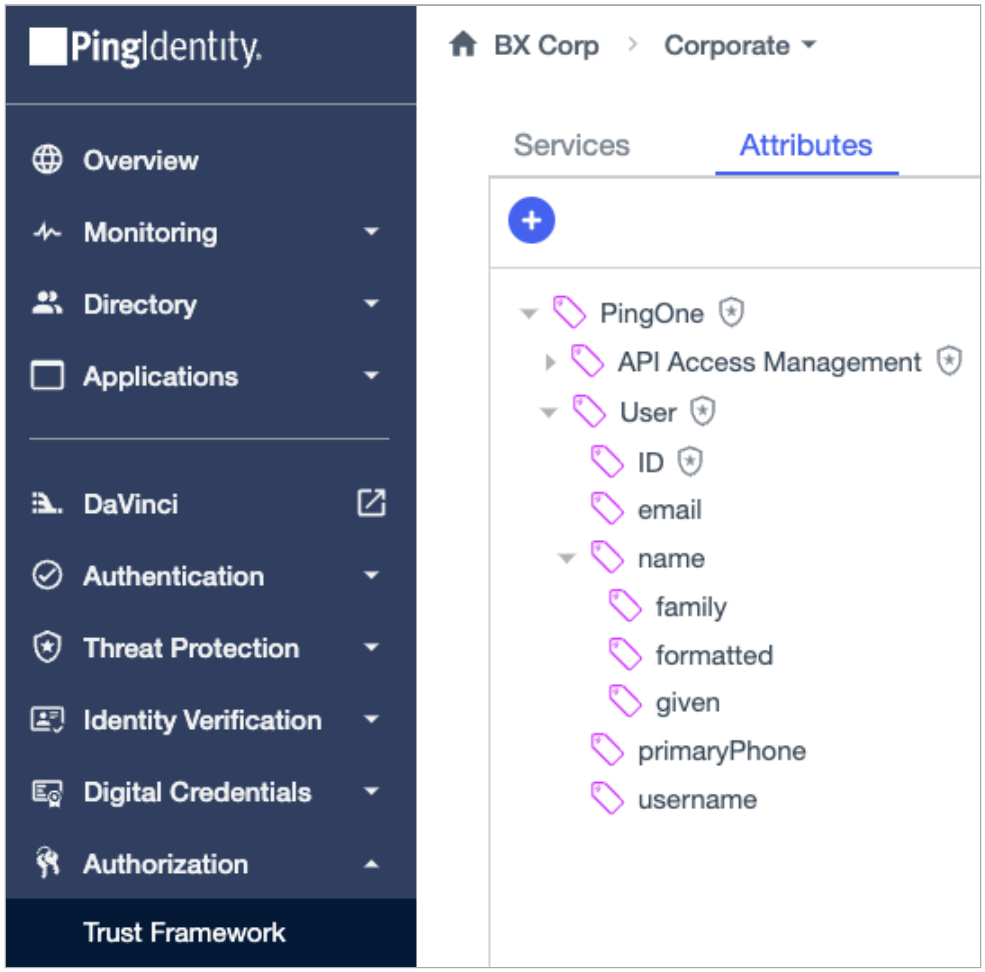
When you use business-friendly names to define resources in the **Trust Framework**, policy authors can easily refer to these resources without worrying about how the information is retrieved and populated.

Steps

1. In PingOne, go to **Authorization > Trust Framework**.
2. If it is not already displayed, click the **Attributes** tab.

   You can see the built-in User attributes that come with PingOne Authorize. You're going to add a new attribute for the amount.

Copyright © 2025 Ping Identity Corporation



3. Click the **+** icon and select **Add new Attribute**.

4. For the attribute **Name**, enter `Amount`.

> **Tip**
>
> If you selected another attribute before you added `Amount`, `Amount` is nested under the parent attribute. Nesting helps group related attributes together. To keep things simple, you won't nest the `Amount` attribute in this tutorial.

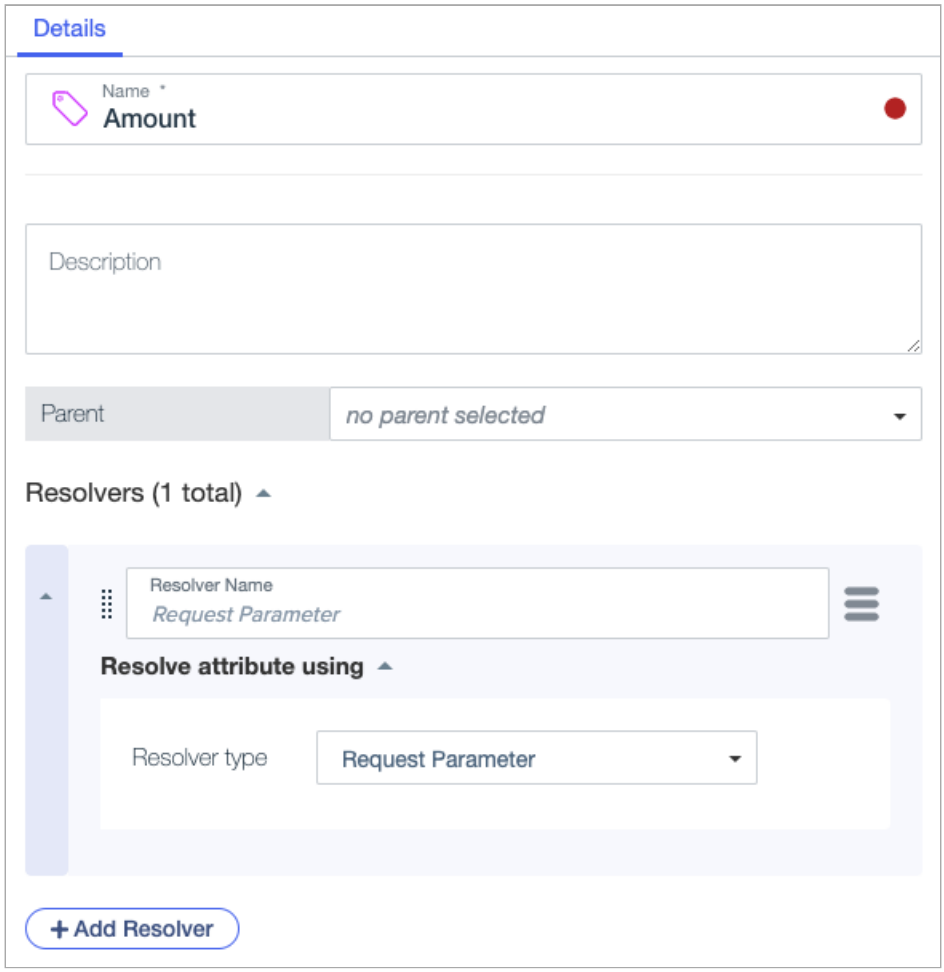
5. Verify that there is no **Parent** selected. If a parent exists, click the **Delete** icon to remove it.

   To get the payment amount, which is the value of the attribute, you'll add a resolver. Resolvers define where the initial data for an attribute comes from.

6. Click **+ Add Resolver**.

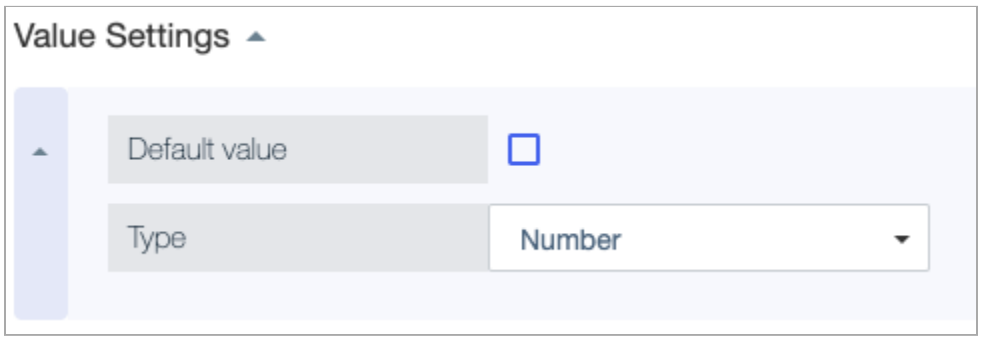
   Keep the default Resolver type of **Request Parameter** so that the value of your attribute comes from a parameter in the decision request. Later in the tutorial, you'll use a field in the decision request body to provide a value for the request parameter. So far your attribute looks like this.

Copyright © 2025 Ping Identity Corporation



Next let's make sure that the value of the attribute is a number.

7. In **Value Settings**, for the **Type**, select **Number**.

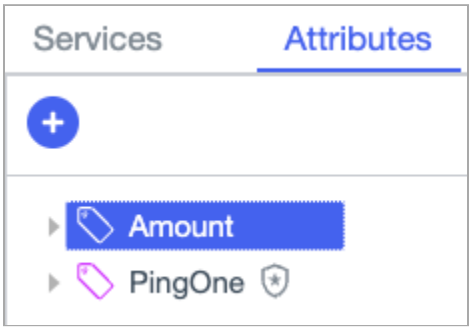


8. Click **Save Changes**.

   Result:

   Your new attribute is displayed in the attribute list.

Copyright © 2025 Ping Identity Corporation



Next steps

You used the **Trust Framework** to create a simple attribute that represents the payment amount. Now that you've added an attribute, you're ready to use the attribute in a policy.

Adding and testing a policy

Learn how to add and test a dynamic authorization policy that uses an attribute.

Adding a policy

About this task

Policies model business requirements into authorization logic. They're built by business analysts who understand your application requirements and the regulations you're complying with.

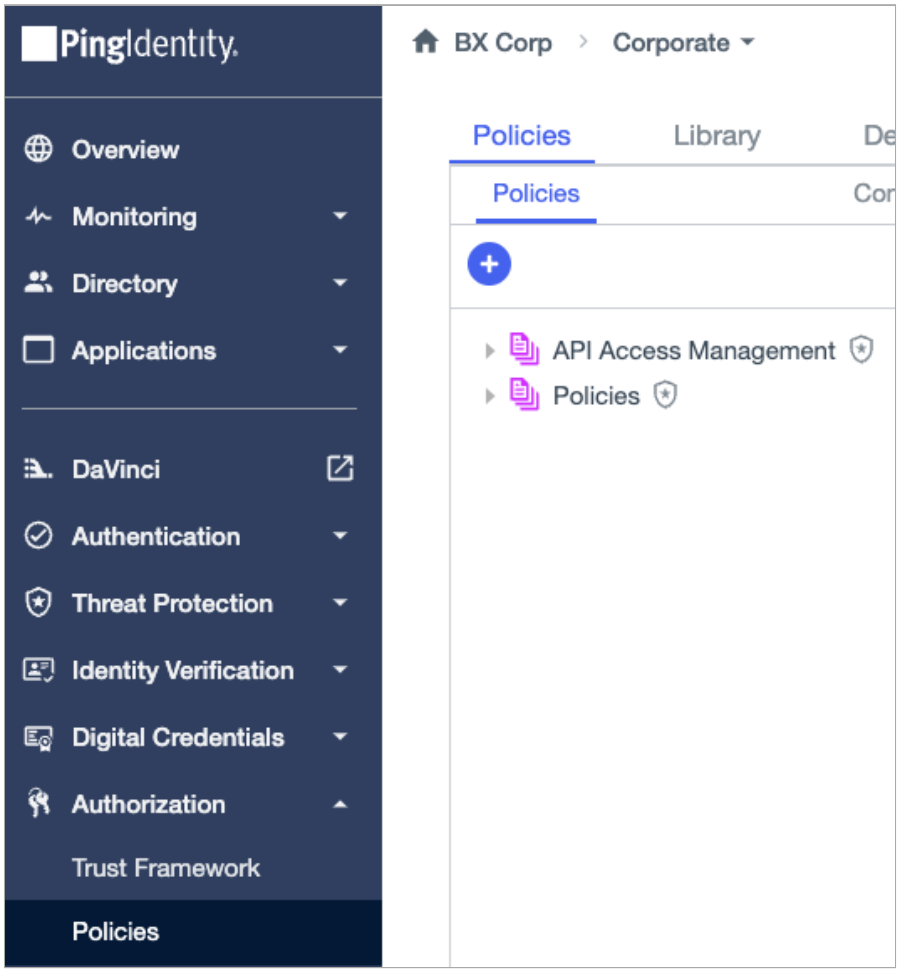
Let's add a policy that will deny payments over $10,000 USD.

Steps

1. Go to **Authorization** > **Policies**.

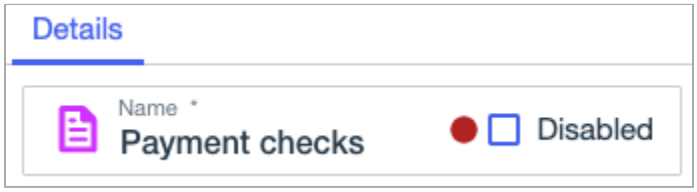
   On the **Policies** tab, you'll see the default policy set called **Policies**. Policy sets are like folders that you can use to group and organize policies. You're going to add your policy to the default policy set.

Copyright © 2025 Ping Identity Corporation



2. Select the root policy set **Policies**, then click the **+** icon and select **Add Policy**.
3. For the policy **Name**, enter `Payment checks`.

   The red dot on the right indicates that there are unsaved changes in the policy.



   Now you need a rule that defines the policy logic.

4. Click **+ Add Rule**.

   To keep things simple, leave out the description for now. When you develop your own policies, you can enter a description to document the underlying business case for the rule or the specific business policy the rule is enforcing.

5. For the rule **Name**, enter `Deny payments over 10000 USD`.
6. Because you want to deny certain payments, select **Deny** for the **Effect**.

   Let's make a comparison to determine if the payment amount is over $10,000 USD.

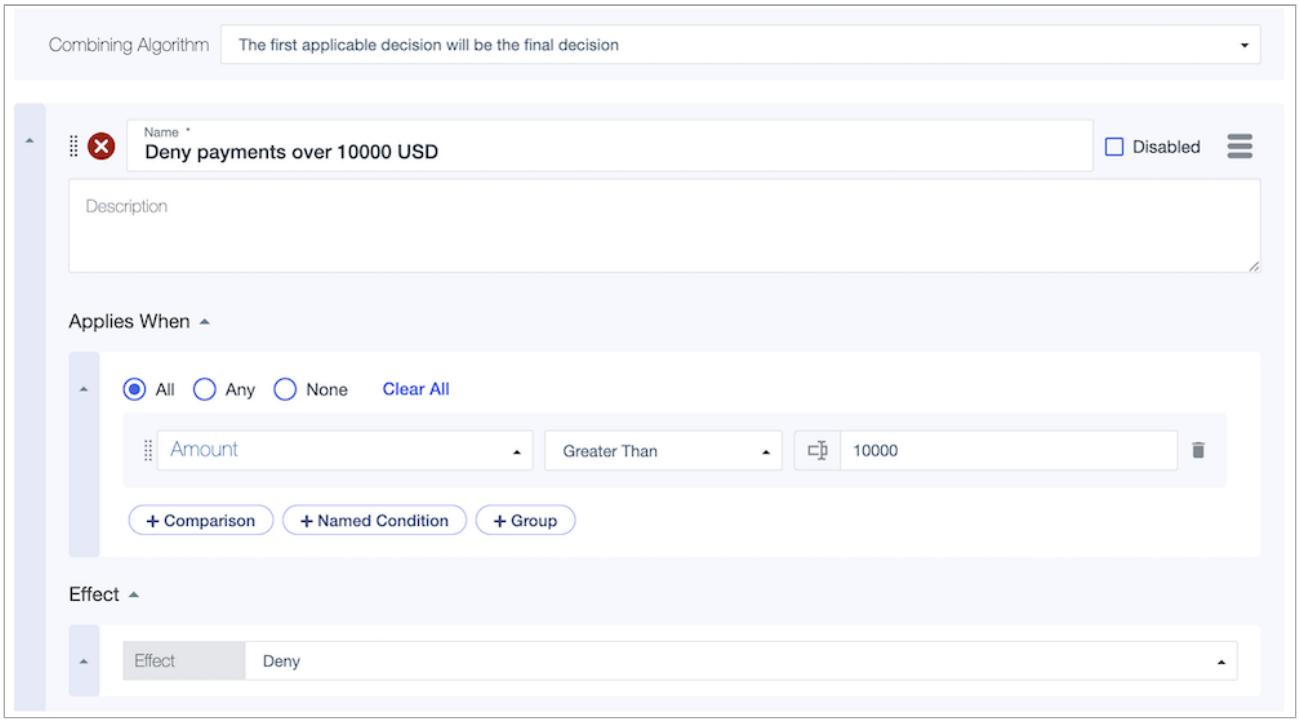
Copyright © 2025 Ping Identity Corporation

7. Click the hamburger menu next to the **Name** field and select **Add "Applies When"**.

    1. In the **Applies When** section, click **+ Comparison**.
    2. In **Select an attribute**, select **Amount**, which is the attribute that you added to the **Trust Framework**.
    3. For the comparator, select **Greater Than Or Equal**.
    4. For the constant value, enter `10000`.

    Result:

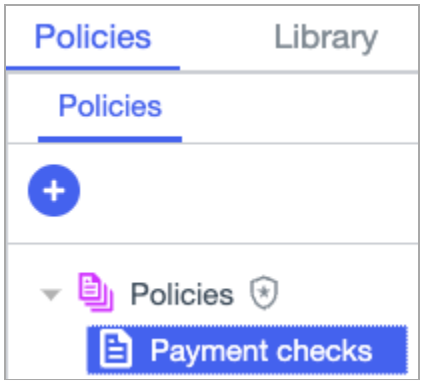
    Your rule looks like this.



8. Click **Save changes**.

    Result:

    Your new policy is displayed in the default policy set.



Copyright © 2025 Ping Identity Corporation

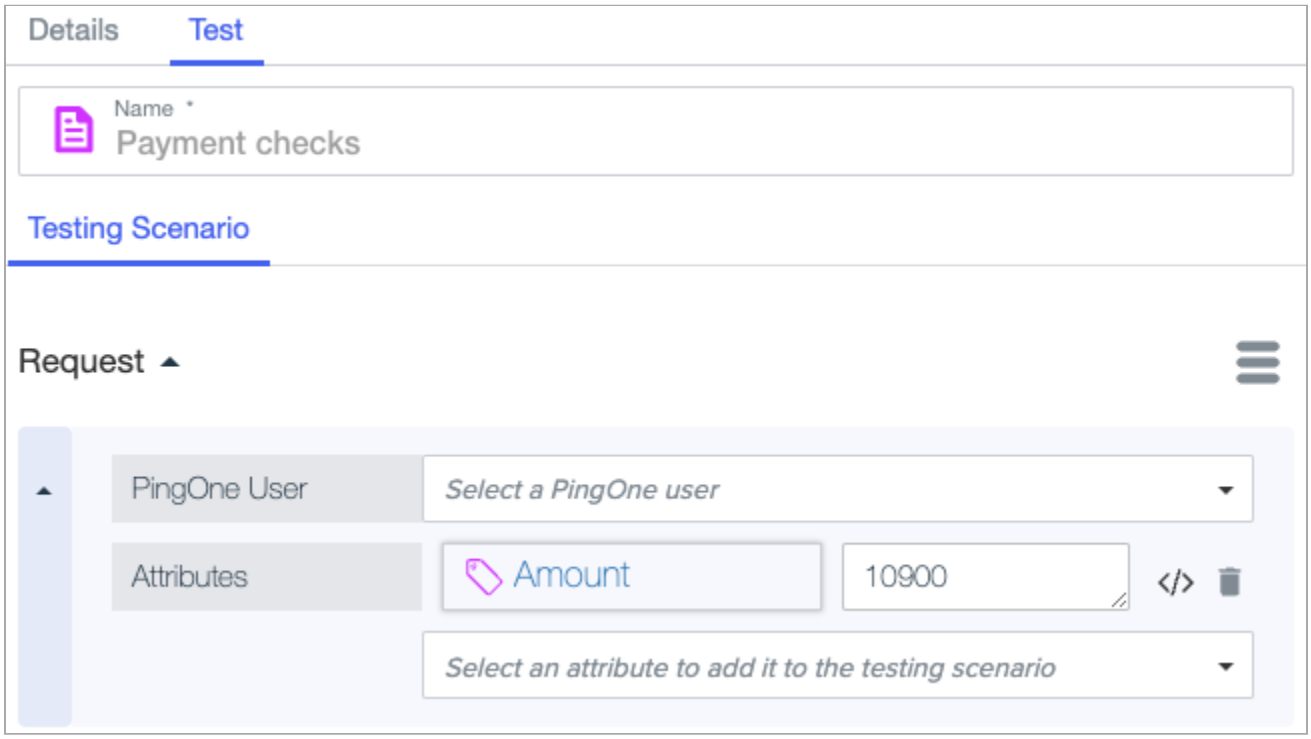
Testing the policy

About this task

Next you'll test your policy to make sure it does what you expect.

Steps

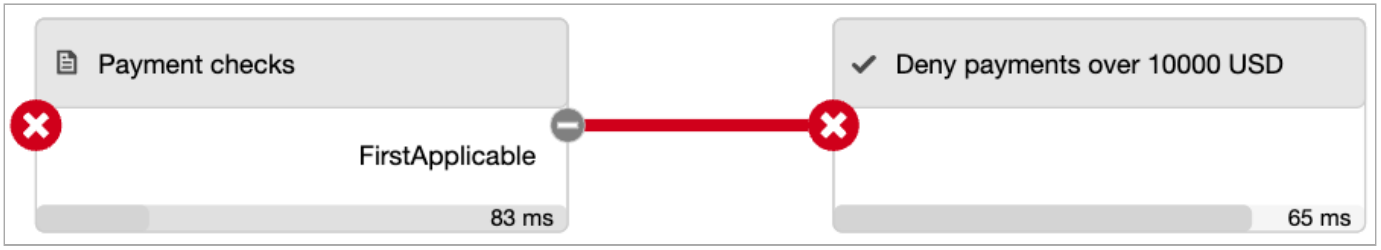
1. Go to **Authorization** > **Policies**, then select the **Payment checks** policy and click the **Test** tab.
2. In the **Request** section, in the **Attributes** list, select the **Amount** attribute and enter `10900` as the attribute value.



3. Click **Execute**.

   Result:

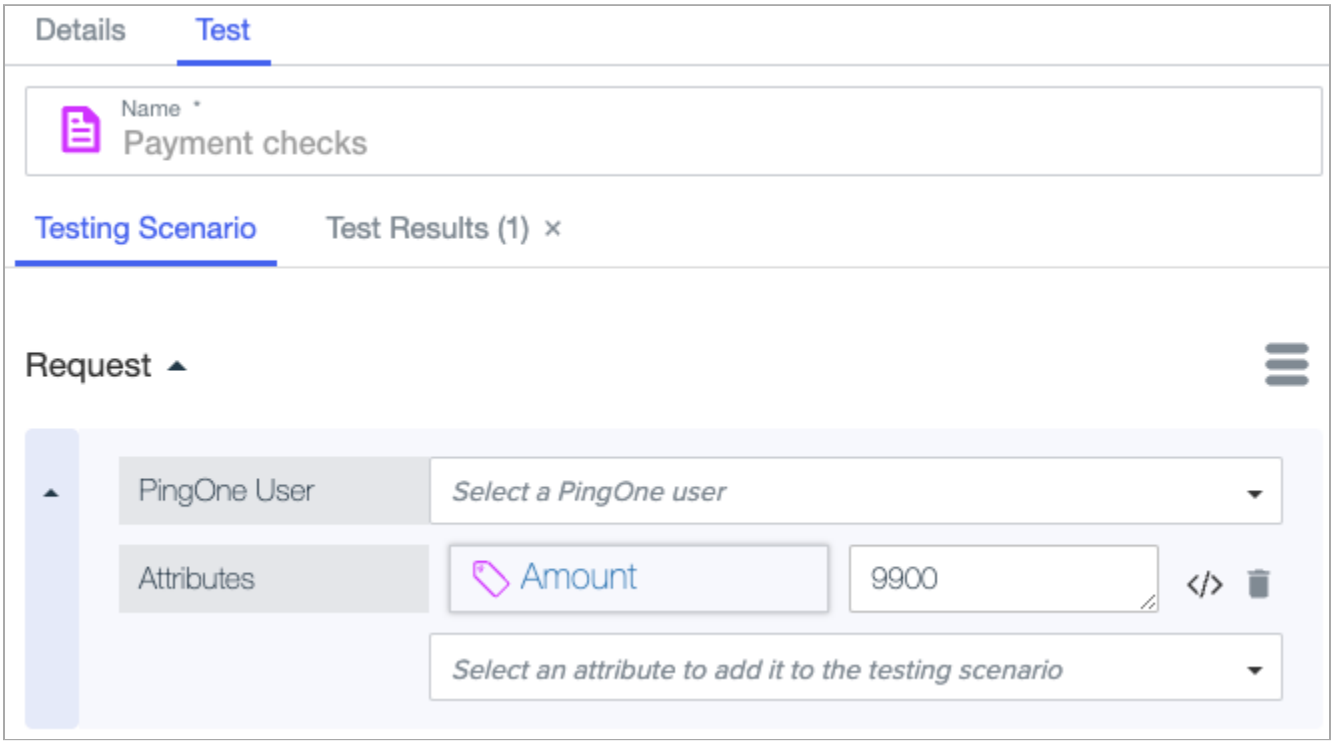
   The **Visualization** tab shows a deny result, as you'd expect, because the amount is over 10000. The policy is working.



   Now let's test a value less than 10,000 to see if the policy handles it.

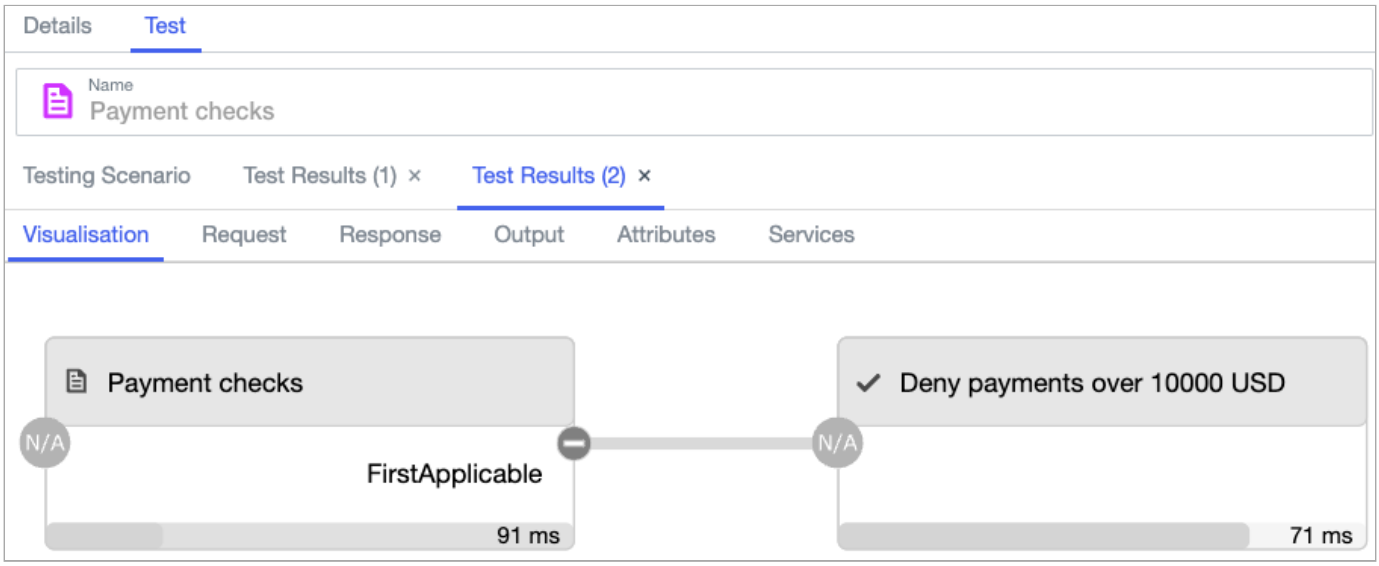
4. Click the **Testing Scenario** tab, enter `9900` as the attribute value, and click **Execute**.

Copyright © 2025 Ping Identity Corporation



Result:

A second **Test Results** tab is displayed that shows a result that's not applicable. Your rule only applies to amounts greater than or equal to 10000, so right now the rule doesn't apply to amounts less than 10000. This neutral decision indicates that the policy doesn't apply in this situation.



You have more work to do with your policy to account for amounts less than $10,000 USD.

Next steps

You used the amount attribute to build a basic policy with a rule that denies payments over $10,000 USD. Then you tested your policy and found that it doesn't account for payments less than $10,000 USD.

Let's update and retest the policy.

Copyright © 2025 Ping Identity Corporation

Updating and retesting a policy

Learn how to iterate a policy by updating and retesting it.

Updating the policy

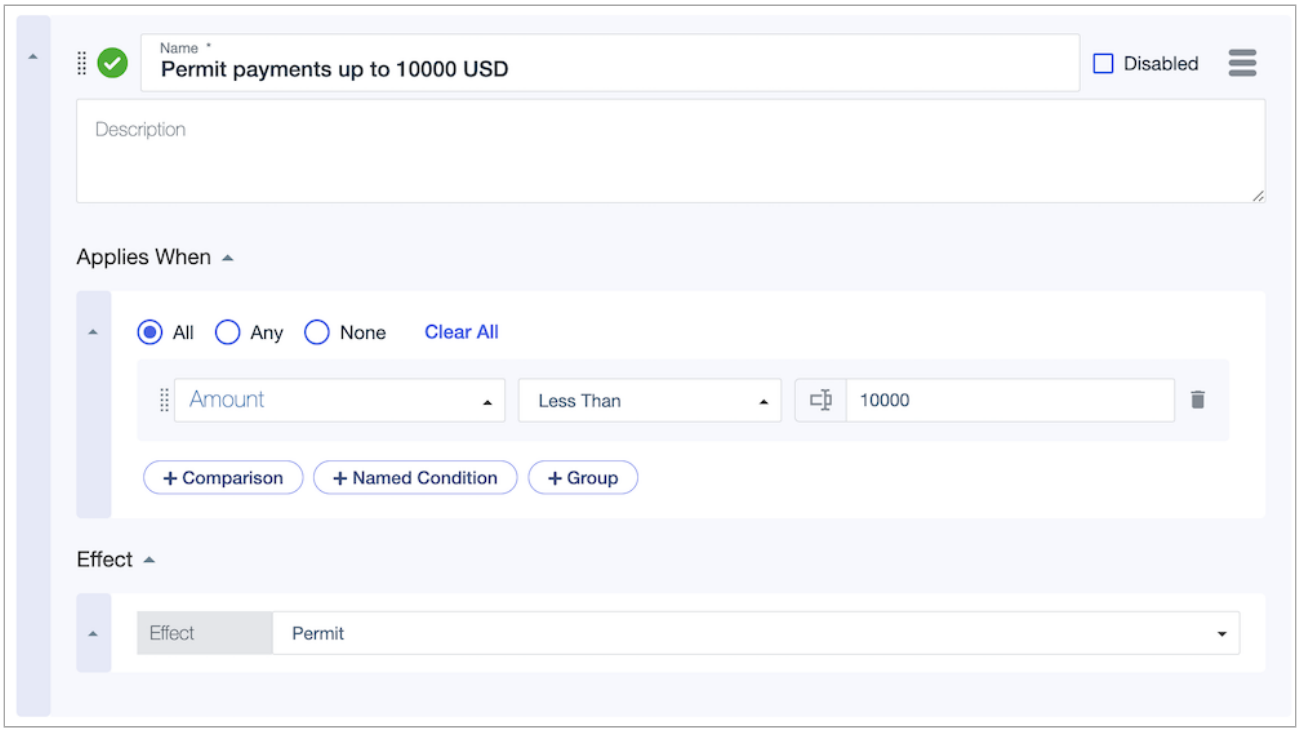
About this task

Let's add another rule to allow payments that are less than $10,000 USD.

Steps

1. Go to **Authorization** > **Policies** and make sure that the **Payment checks** policy is selected.
2. Click the **Details** tab, then click **+ Add Rule**.
3. For the rule **Name**, enter `Permit payments up to 10000 USD`.
4. Click the hamburger menu next to the **Name** field and select **Add "Applies When"**.
    1. In the **Applies When** section, click **+ Comparison**.
    2. In **Select an attribute**, select `Amount`, which is the same attribute you used before.
    3. For the comparator, select **Less Than**.
    4. For the constant value, enter `10000`.

    Your new rule looks like this.

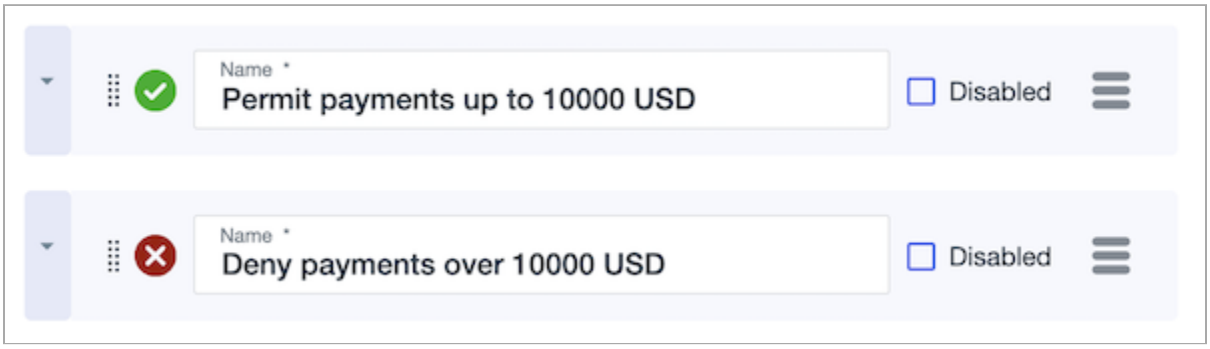


Copyright © 2025 Ping Identity Corporation

5. Click **Save changes**.

   Rules are evaluated in order from top to bottom. Let's move the permit rule so it's first.

6. Make sure that the rule is collapsed so that you only see the name, then click the drag bar to the left of the green check mark and reposition the permit rule above the deny rule.



   Now that there's a second rule, let's consider the combining algorithm. It determines how one or more rules are evaluated to make a decision. Instead of adding the permit rule, you could have used the combining algorithm alone to permit payments less than $10,000 USD. Let's change the combining algorithm as if you didn't already have the second rule.

7. For the **Combining Algorithm**, select **Unless one decision is deny, the decision will be permit**.

   For more details about combining algorithms, see Combining algorithms.

8. Click **Save changes**.

Retesting the policy

About this task

Let's test your policy again to make sure it handles payment amounts under $10,000 USD.

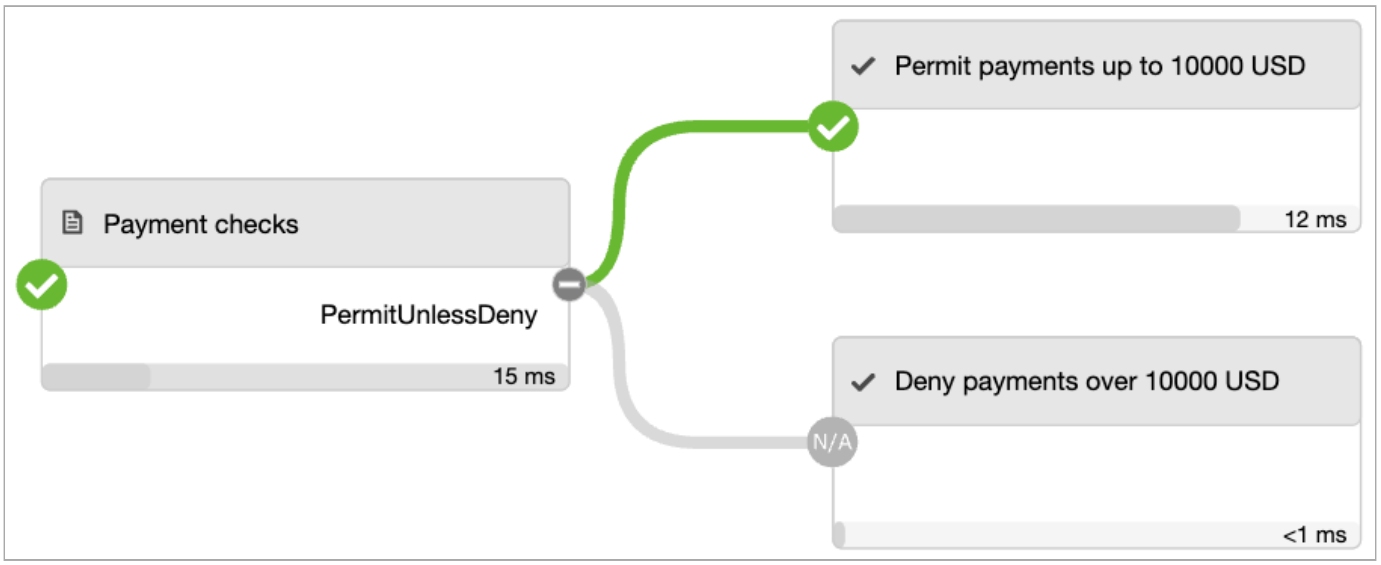
Steps

1. Go to **Authorization** > **Policies**, then select the **Payment checks** policy and click the **Test** tab.
2. In the **Request** section, in **Attributes**, enter `9900` as the value for the **Amount** attribute.
3. Click **Execute**.

   Result:

Copyright © 2025 Ping Identity Corporation

The **Visualization** tab shows a permit result, so now your policy handles amounts less than $10,000 USD. Your original rule for payments over $10,000 USD is not applicable because the amount is less than $10,000 USD.



Next steps

You added a second rule to your policy to account for payments less than $10,000 USD and used a combining algorithm. Then you retested your policy and found that it accounts for payments that are greater than or less than $10,000 USD.

So far, you've used the **Trust Framework** to create a basic attribute, then used the attribute in a policy with multiple rules and a combining algorithm. You've tested the policy and it does what you expect.

Now you're ready to publish your policy.

Publishing a policy and configuring an endpoint

Learn how to publish a policy to a decision endpoint and configure the endpoint.

Publishing a policy

About this task

Let's publish your changes to a decision endpoint so that you can make decision requests against a specific version of the policy. PingOne Authorize provides three decision endpoints to get you started: **Dev**, **Test**, and **Prod**. You've been working with the **Dev** endpoint so far.

Let's publish to the **Test** endpoint to make your new policy available for more rigorous testing.

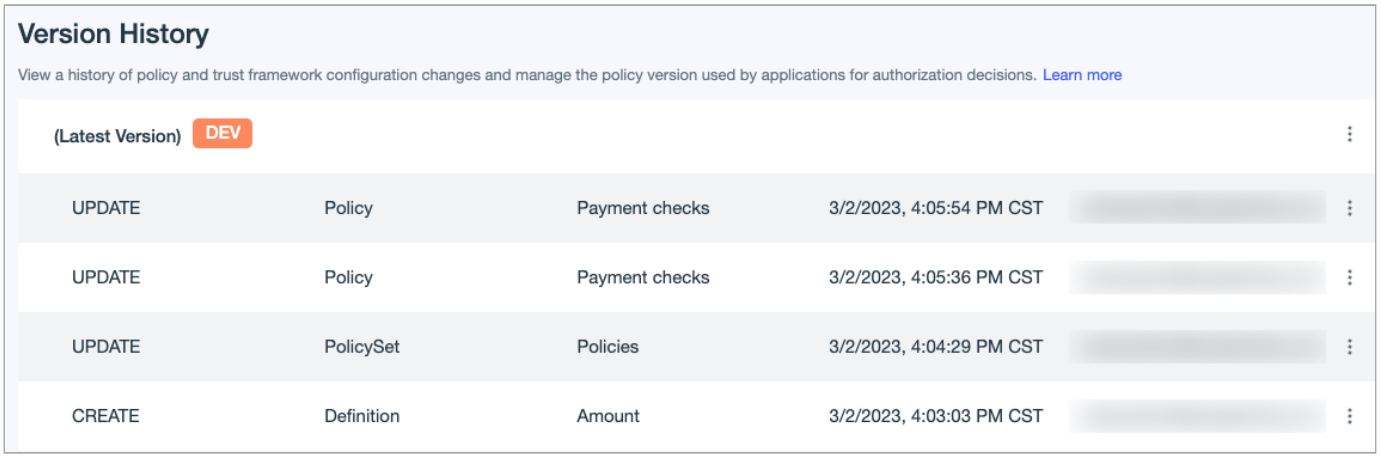
> **Important**
>
> Ensure that your policies and **Trust Framework** definitions are thoroughly tested before you publish them to the **Prod** endpoint and use them in production.

Copyright © 2025 Ping Identity Corporation

Steps

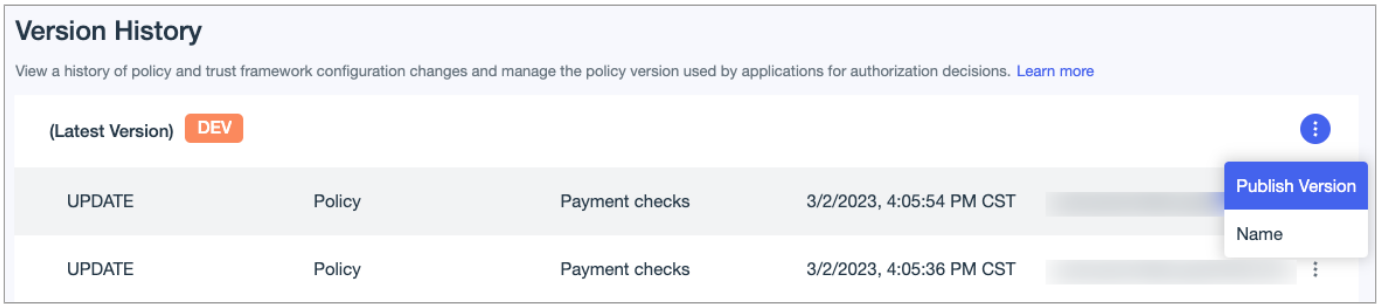
1. Go to **Authorization > Version History**.

   You see all the changes you've made, with the most recent changes listed first. The orange **Dev** icon indicates that you've been working with the development endpoint.



   Let's publish the latest version of your changes.

2. Click the **More Options (⋮)** icon to the right of **(Latest Version) Dev** and select **Publish Version**.

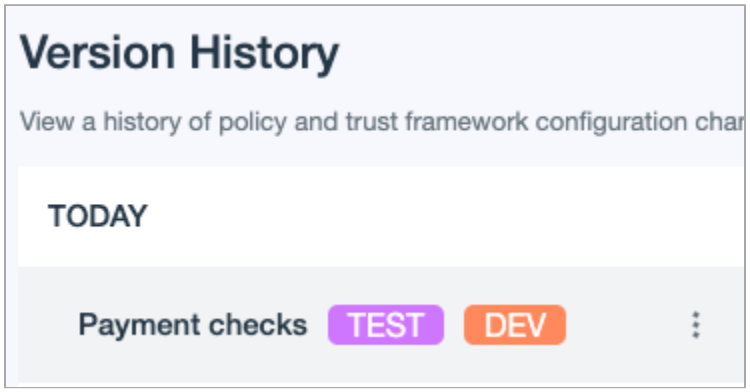


3. In the **Publish to** list, select the **Test** endpoint.
4. For the version **Name**, enter `Payment checks`.
5. Click **Publish**.

   Result:

   The version is now named and the pink **Test** icon indicates that it's published in **Test** in addition to **Dev**.

Copyright © 2025 Ping Identity Corporation



Setting up decision endpoints

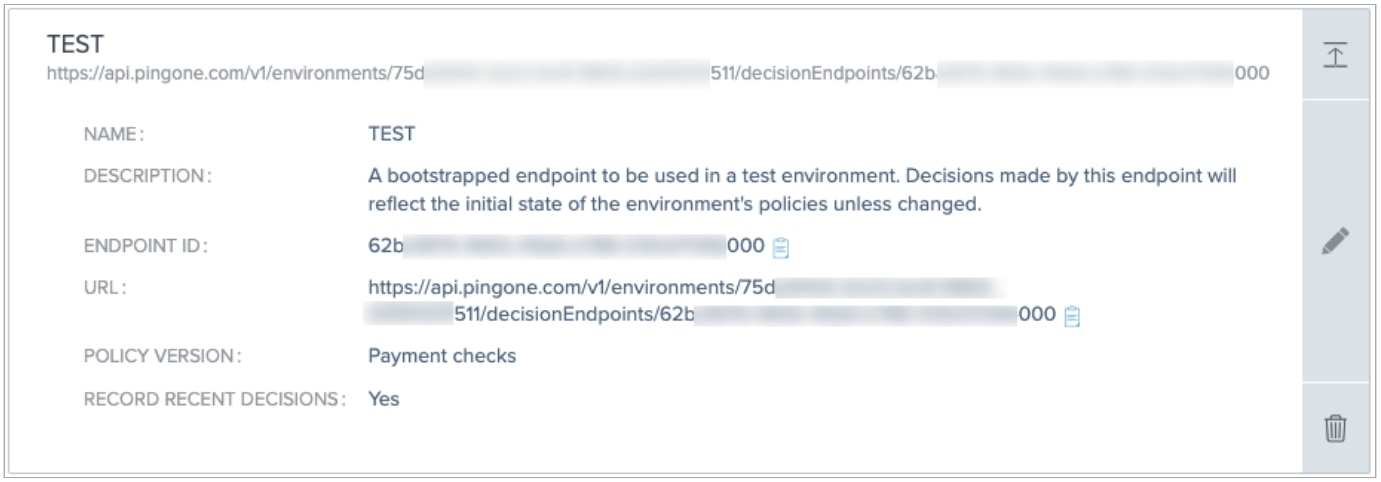
About this task

Let's take a look at the **Test** endpoint and set it up to record recent decisions.

You can configure a decision endpoint to keep track of recent decisions made during policy evaluation. This can cause a slower system response, so the setting is disabled by default. During policy development, enable this setting as a debugging tool to help you visualize and examine recent decisions.

Steps

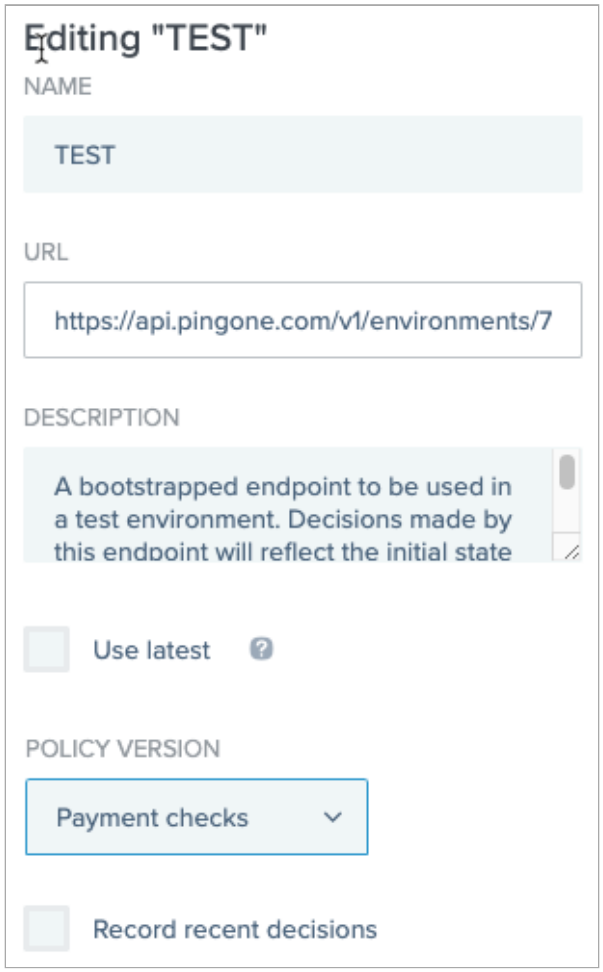
1. Go to **Authorization** > **Decision Endpoints**.
2. Expand the **Test** endpoint and click the **Pencil** icon.



Result:

The **Editing** window opens, and you can see that the endpoint is using the policy version that you published to it.

Copyright © 2025 Ping Identity Corporation



> **Note**
>
> If you're wondering about **Use latest**, this setting allows you to use the latest policy version instead of a specific named version. This republishes the latest version each time a request is made to the endpoint and can cause a slower system response. Don't enable this setting right now.

3. Select the **Record recent decisions** check box.

   When decision requests are made against your policy, this option keeps track of the last 20 decisions and allows you to examine those decisions in detail.

4. Click **Save**.

Next steps

You've published your policy to an endpoint where it can be tested and you've set up the **Test** endpoint to keep track of recent decisions.

Next, you'll make decision requests against your policy.

Making decision requests and examining recent decisions

Learn how policies are evaluated when an application makes decision requests and how you can examine the resulting decisions.

Copyright © 2025 Ping Identity Corporation

Making decision requests

About this task

You'll use Postman requests to simulate an application requesting decisions about payment amounts. To get started, let's walk through downloading a Postman collection and assigning values to variables used in the requests.

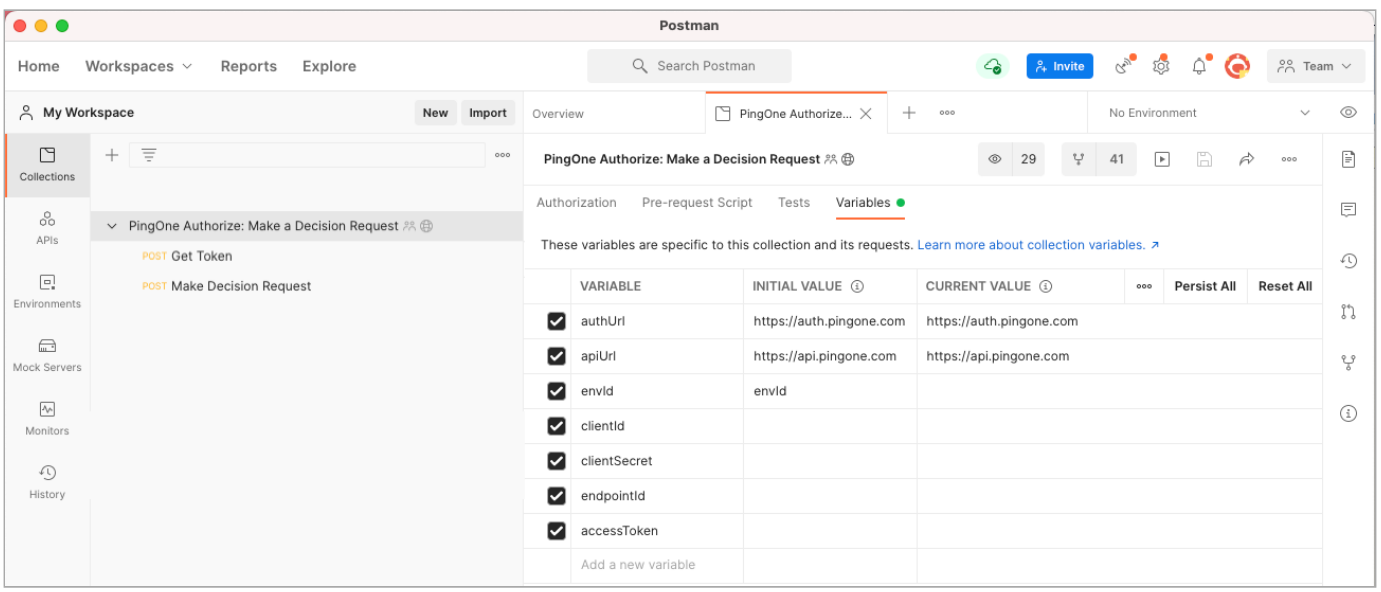
The PingOne platform requires an access token from your application before you can make calls to the API. You'll use a Postman request to get the access token, then you'll make decision requests.

Steps

1. Import a copy of the Postman collection:
    1. Click the **Run in Postman** button below.

    Run in Postman

    2. Click the **import a copy** link.
    3. If you use workspaces in Postman, select a workspace and click **Import**.
2. Go to **Collections** and click **PingOne Authorize: Make a Decision Request** to open the collection, then click the **Variables** tab.



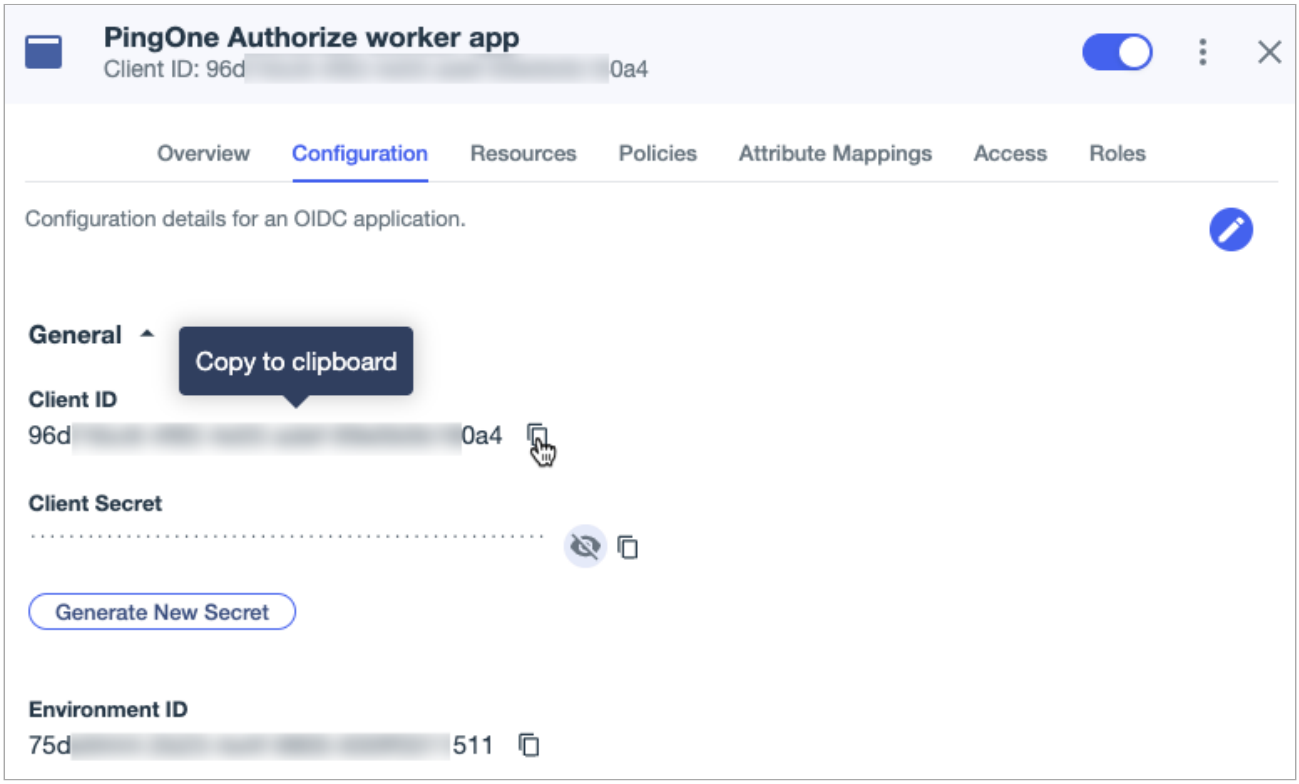
3. If you are outside of the North America (US) region, update the `authUrl` and `apiUrl` current values to use the data center closest to your geographic region.

Region	authUrl	apiUrl
Australia	https://auth.pingone.com.au	https://api.pingone.com.au
Canada	https://auth.pingone.ca	https://api.pingone.ca

Copyright © 2025 Ping Identity Corporation

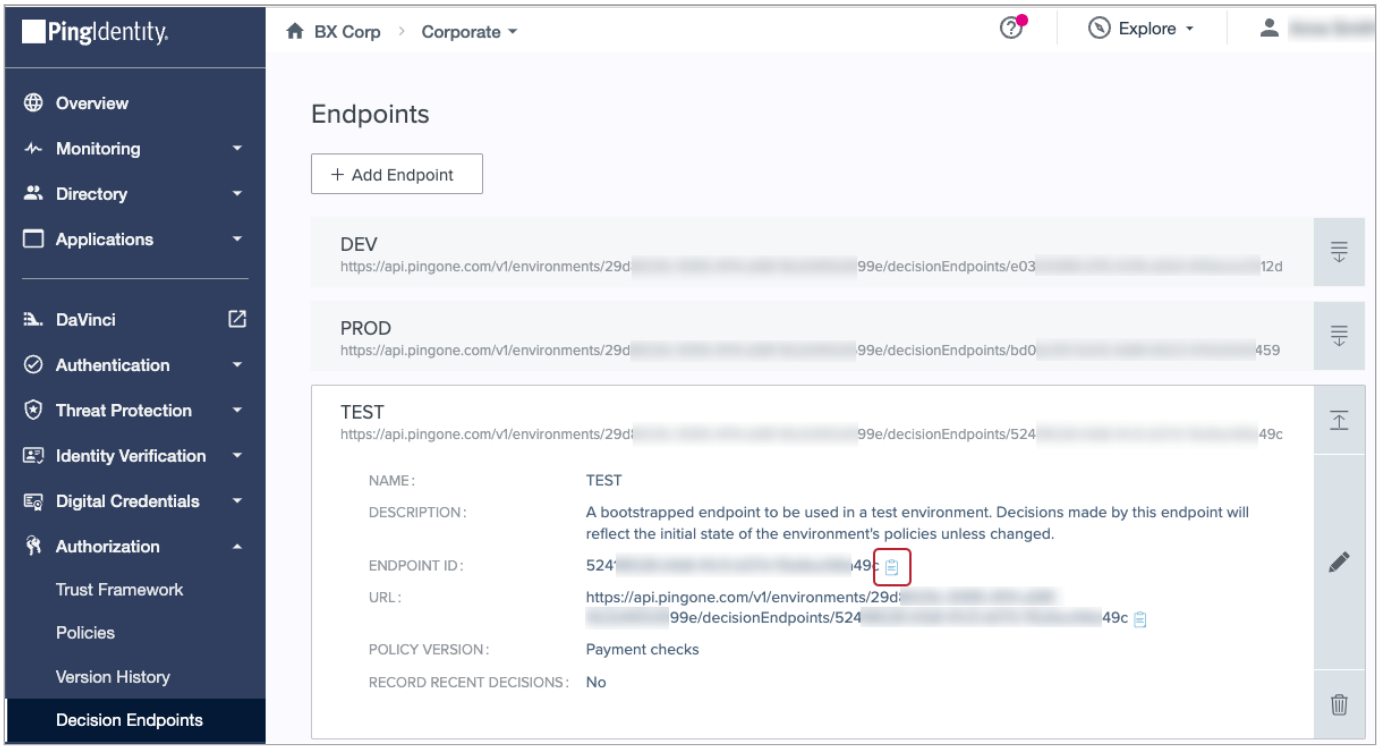
Region	authUrl	apiUrl
Europe	https://auth.pingone.eu	https://api.pingone.eu
Singapore	https://auth.pingone.sg	https://api.pingone.sg
Asia Pacific (legacy) **Note** Available only for existing .asia customers.	https://auth.pingone.asia	https://api.pingone.asia

4. In PingOne, go to **Applications** > **Applications**.
5. Click your worker application, then click the **Configuration** tab.
6. Copy the following values from the **General** section into the corresponding current values on the **Variables** tab in Postman:
   - **Client ID**: The Postman variable is `clientID`.
   - **Client Secret**: The Postman variable is `clientSecret`.
   - **Environment ID**: The Postman variable is `envId`.



7. Go to **Authorization** > **Decision Endpoints** and expand the **Test** endpoint.
8. Copy the **Endpoint ID** and paste it into the current value for **endpointId** in Postman.

Copyright © 2025 Ping Identity Corporation

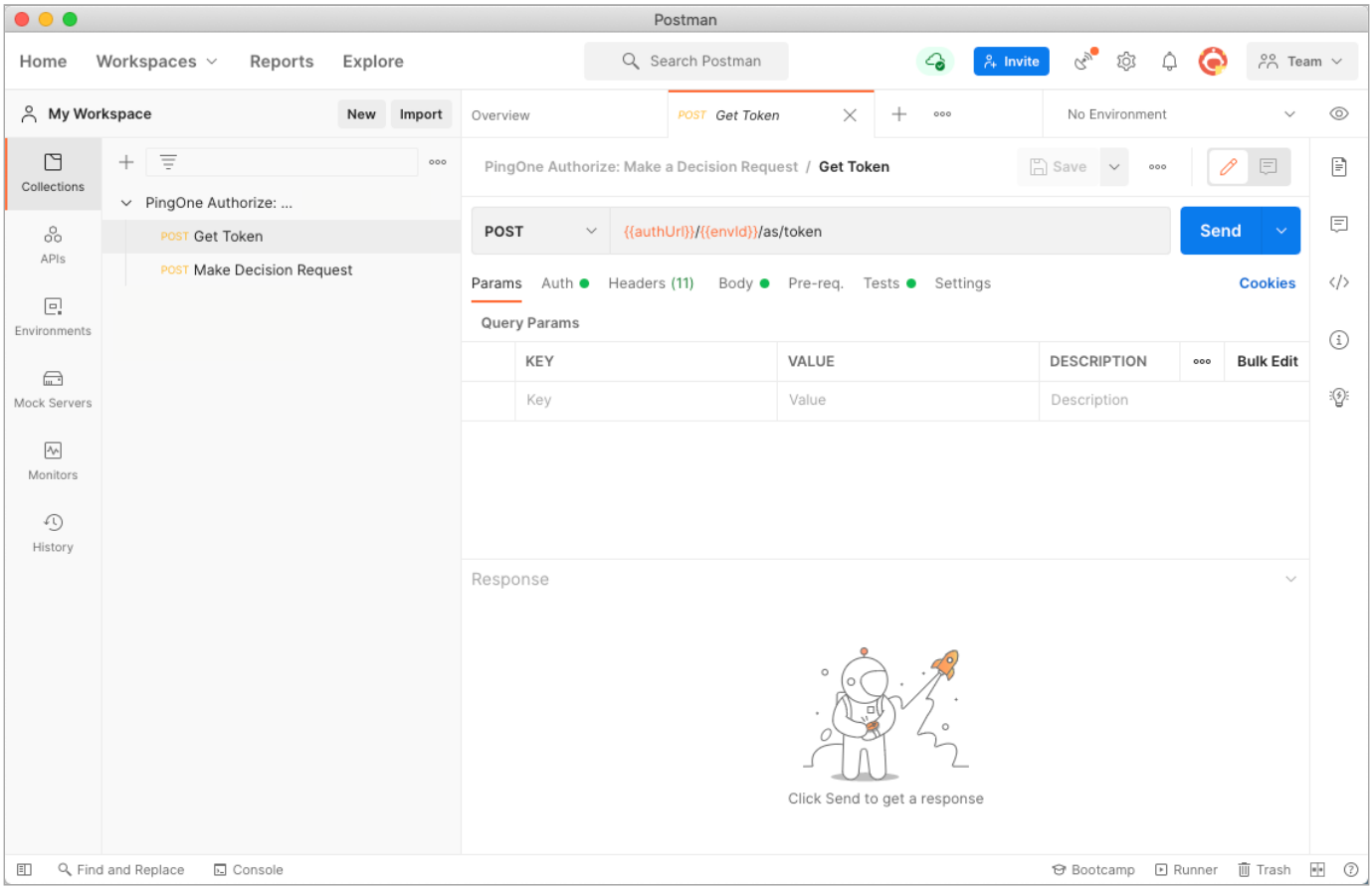


9. In Postman, click **Save** to save the current values you assigned.

   Result:

   Now you're ready to send a request to get an access token.

10. In Postman, select the **Get Token** request and click **Send**.



Result:

The access token is in the response.

```
"access_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6ImRlZmF1bHQifQ.
    rfjzIXJ7xpK271sIirrmiEfpsOnfTZ1xLEX9YO54ORhIDPjnlAWkf4FrA",
"token_type": "Bearer",
"expires_in": 3600
```

Now you're ready to make a decision request.

11. Select **Make Decision Request** and click the **Body** tab. Set the `Amount` parameter to `10990`.

Copyright © 2025 Ping Identity Corporation

PingOne Authorize: Make a Decision Request / **Make Decision Request**

POST {{apiUrl}}/v1/environments/{{envId}}/decisionEndpoints/{{endpointId}}

Params Authorization Headers (20) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL JSON

```
1 {
2     "parameters": {
3         "Amount": "10990"
4     }
5 }
```

12. Click **Send**.

    Result:

    The response body shows that the payment is denied according to our policy of denying payments greater than $10,000 USD.

Body

Pretty Raw Preview Visualize JSON

```
5     },
6     "timestamp": "2021-11-11T20:40:09.699Z",
7     "elapsedMicroseconds": 6147,
8     "status": {
9         "code": "OKAY"
10    },
11    "decision": "DENY"
12 }
```

Let's try a payment that's less than $10,000 USD.

13. Change the `Amount` value in the request body to `990` and click **Send**.

    Result:

    As you expect, the payment is permitted.

Copyright © 2025 Ping Identity Corporation

Body Cookies Headers (19) Test Results

Pretty Raw Preview Visualize JSON


```
5      },
6      "timestamp": "2021-11-11T19:25:33.467Z",
7      "elapsedMicroseconds": 5413,
8      "status": {
9          "code": "OKAY"
10     },
11     "decision": "PERMIT"
12 }
```


Result

You've simulated a couple of payment decision requests so that you have something to examine further.

Tutorial: examining recent decisions

About this task

Earlier, you configured the **Test** endpoint to keep track of recent decisions made during policy evaluation. You can use details about recent decisions to debug policy behavior during policy development.

> **Note**
>
> Recent decisions are a policy debugging tool, and are not intended for monitoring of authorization decisions in real time. You can examine the 20 most recent decisions made for an endpoint in the last 24 hours.

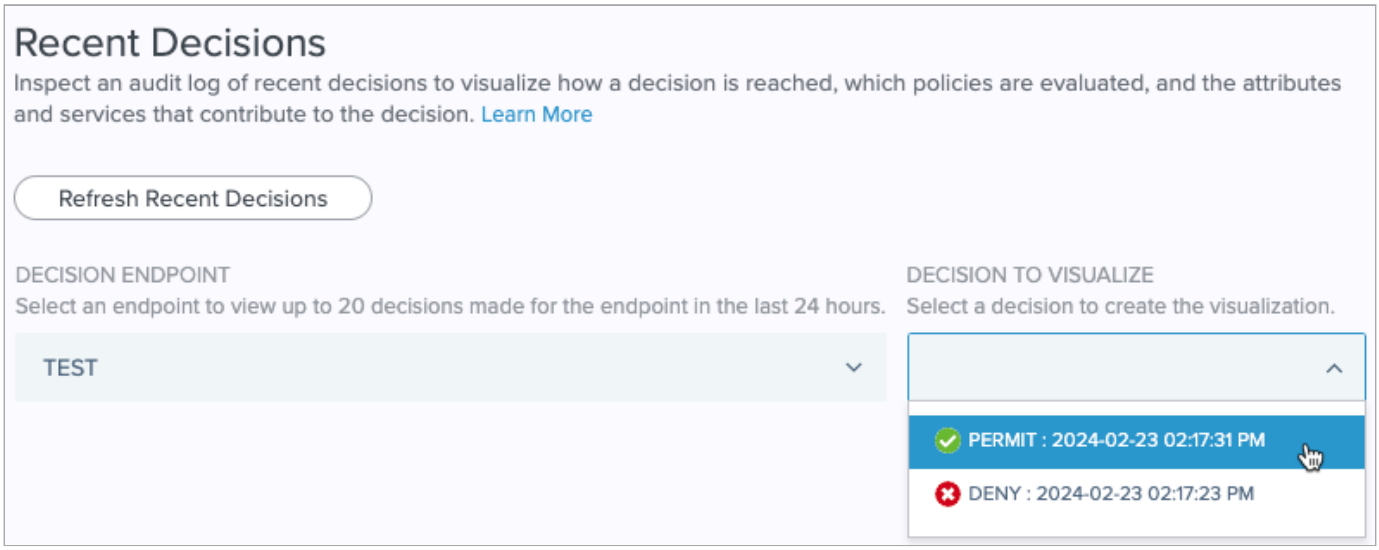
Let's examine recent decisions to make sure that the policy is handling payment requests correctly.

Steps

1. Go to **Authorization** > **Recent Decisions**.
2. In the **Decision Endpoint** list, select the **Test** endpoint.
3. In the **Decision to Visualize** list, select the first decision.

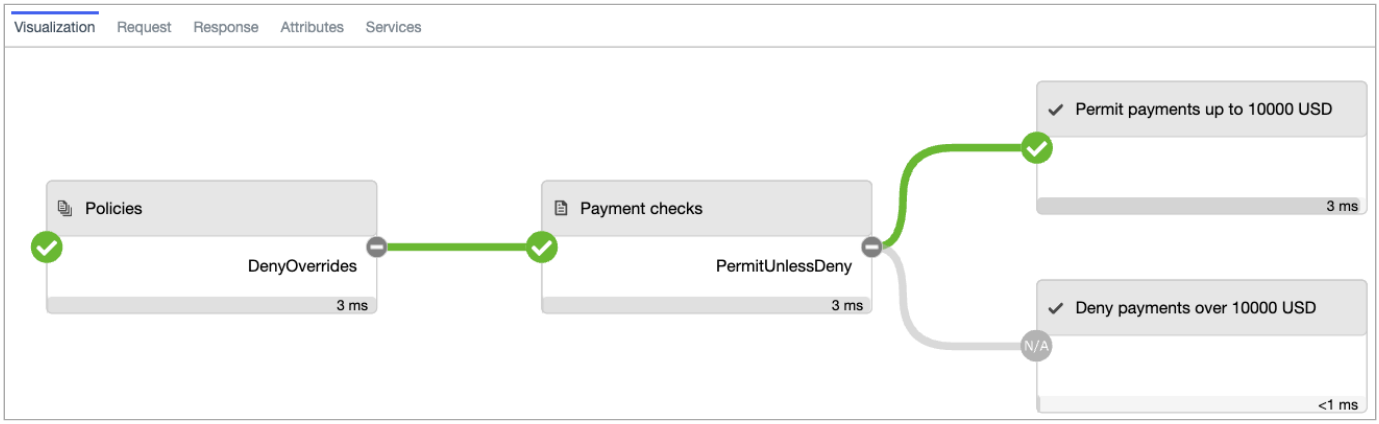
   This is the most recent decision.

Copyright © 2025 Ping Identity Corporation



4. Examine the decision flow to make sure that decisions are evaluated according to your expectations.

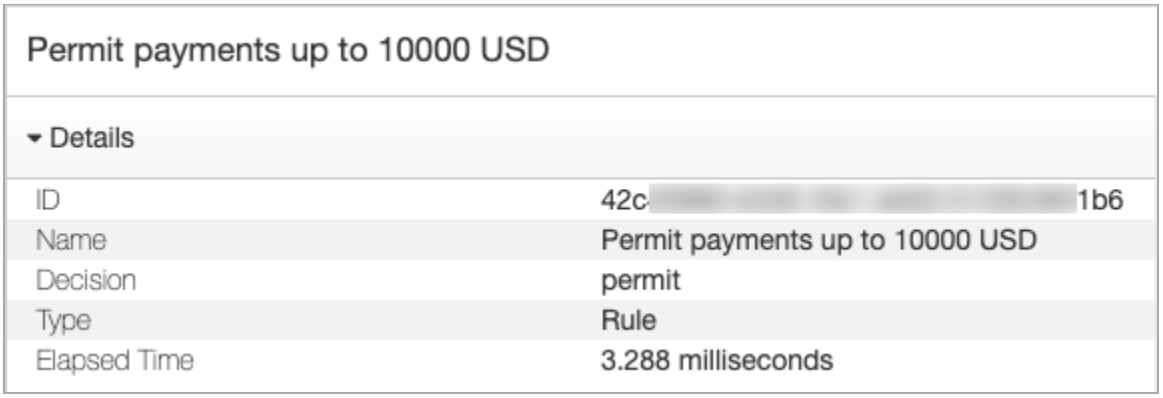
   The visualization is similar to what you saw when you tested your policy.



5. Click the **Permit payments up to 10000 USD** box to show more details.

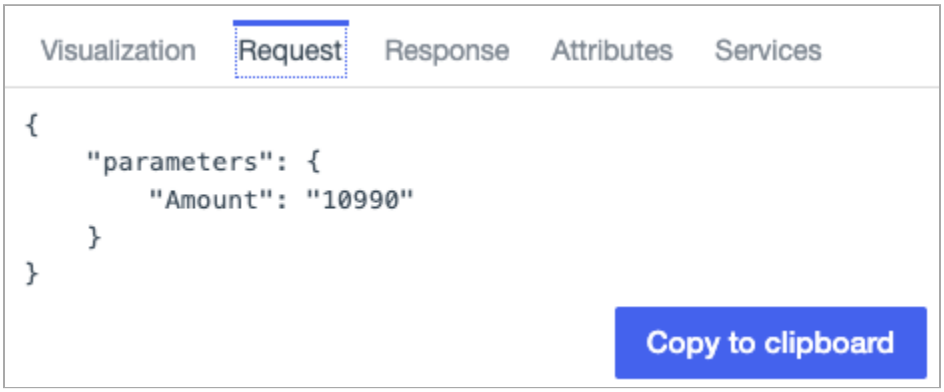
   Result:

   You can see that this represents your rule that permits payments up to $10,000 USD. The decision evaluated to `Permit` and it took 3.288 milliseconds.

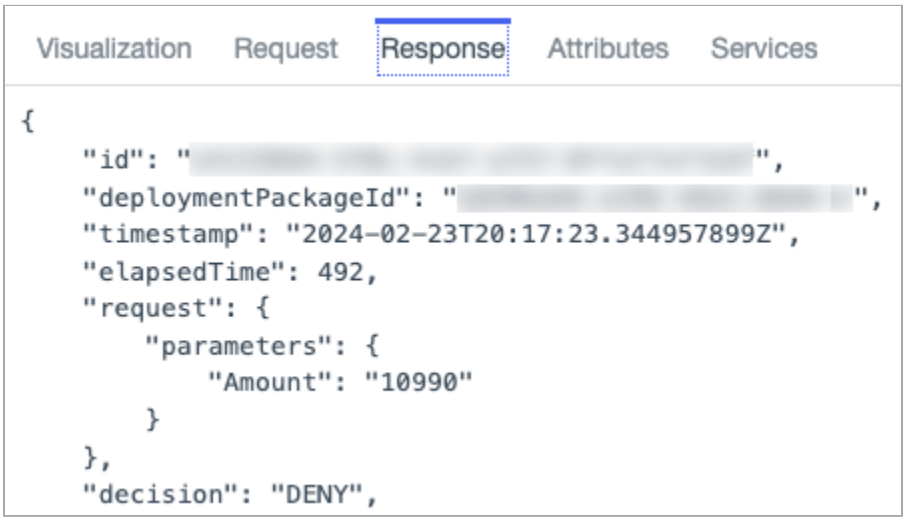


6. In the **Select Decision to Visualize** list, select the second decision and then examine the **Visualization** tab and the other tabs to make sure that everything looks as expected:

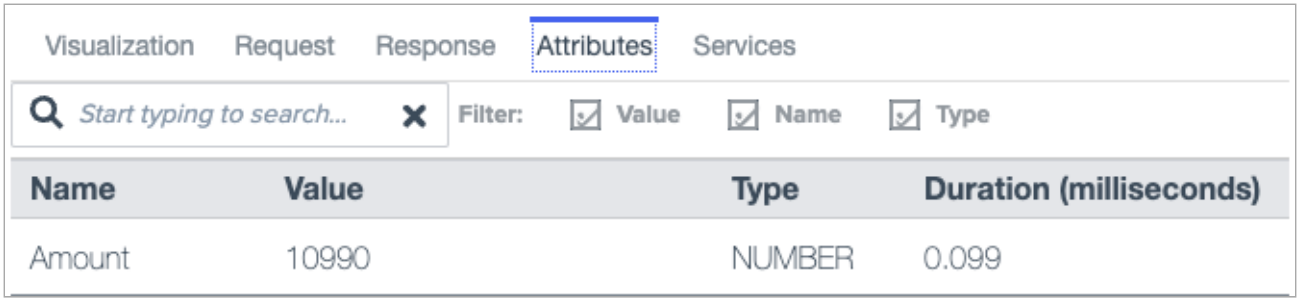
   1. Click the **Request** tab to review the JSON request sent to the decision service and confirm that the expected information was sent.



   2. Click the **Response** tab to review the complete, high-verbosity response for the decision, including expanded errors and other helpful information.



   3. Click the **Attributes** tab for details about the attribute used in the decision.



   Now that you've examined recent decisions for your named version, let's roll it out to production by publishing it to the **Prod** endpoint.

7. Go to **Authorization > Version History**.

Copyright © 2025 Ping Identity Corporation

8. For the **Payment checks** version, click the **More Options (⋮)** icon and select **Publish Version**.
9. In the **Publish to** list, select the **Prod** endpoint and click **Publish**.

   Result:

   The blue **Prod** icon indicates that the version is now published in **Prod** in addition to **Test** and **Dev**.

Result

Congratulations! You've built your first dynamic authorization policy, tested it, and rolled it out to production.

Manage API access

Use the tutorials to familiarize yourself with the API Access Management capabilities of PingOne Authorize.

Before you begin

Make sure:

- PingOne SSO and PingOne Authorize are in your environment. For more information, see Getting started with PingOne Authorize.

  > **Note**
  >
  > For this tutorial, you'll use PingOne Authorize, not PingAuthorize, so make sure you've added PingOne Authorize to your environment.

- If you're signing on as a user instead of an administrator, your user account has the Environment Admin and Identity Data Admin roles.
- You have Postman. You'll use a collection of Postman requests to get access tokens and make API calls.
- You have access to Docker and Docker Compose (included with Docker Desktop on Mac and Windows). You'll use Docker to spin up Kong Gateway for the tutorials.

In the following tutorials, you'll set up API access control through Kong Gateway:

- Tutorial 1: Access control for managed API services
- Tutorial 2: Access control for specific API operations
- Tutorial 3: Fine-grained authorization for API operations

Tutorial 1: Controlling access to APIs managed by an API service

Learn how to set up API Access Management in PingOne Authorize to provide protection and access control for APIs managed by an API service.

Copyright © 2025 Ping Identity Corporation

Imagine you're the publisher of Meme Game, an online game in which players compete with their friends to craft the funniest meme. You need to protect the APIs that compose the game so that only your browser-based client or mobile game client can access the APIs and other clients don't have access.

To do this, you'll configure applications and access control rules in PingOne and an authorization plugin for Kong Gateway. The plugin works with PingOne to handle the complexities of the OAuth and OpenID Connect protocols, making it easier for you to manage API access control across these systems.

What you'll learn

You'll learn how to:

- Configure the authorization plugin for Kong Gateway to connect the gateway to PingOne
- Create applications and managed API services in PingOne
- Configure which applications are authorized to connect to managed API services
- Demonstrate that only authorized clients are able to access the Meme Game APIs

What you'll do

Follow these steps to complete the tutorial:

- Set up your tutorial environment. The environment includes Kong Gateway configured to proxy REST API requests to the Meme Game API.
- Configure an application that doesn't have access to the Meme Game API and get an access token for the application.
- Configure the authorization plugin for Kong Gateway.
- Define a managed API service so that PingOne can help the API gateway enforce access control.
- Set up another application that has access to the Meme Game API.

Setting up your environment

To help you get started with API Access Management, we provide a Docker Compose project with everything you need.

About this task

The Docker Compose project includes Kong Gateway, a PostgreSQL database for gateway configuration, and the Ping Identity authorization plugin for Kong. The plugin is already installed.

Kong is configured to proxy REST API requests to the Meme Game API. This simple API is flexible enough to demonstrate several authorization use cases.

Copyright © 2025 Ping Identity Corporation

Note

- This project uses the enterprise version of Kong Gateway (not the open source version) in Free mode. By using this project, you agree to the terms of Kong's software license.
- The Meme Game API is publicly available and ready to use in PingOne Authorize tutorials. You don't need to install it.

You'll bring up this project and use cURL to make sure everything is working.

Caution

This project exposes Kong Manager and the Kong Admin API without any admin authentication. Be careful if you're running this project on a `docker-machine` exposed to the internet.

Steps

1. Clone the PingOne Authorize API Access Management Tutorials GitHub project.

   For example, clone the supporting files into a new `pingoneauthorize-api-tutorials` directory using HTTPS:

   ```
   git clone https://github.com/pingidentity/pingoneauthorize-api-tutorials.git && cd pingoneauthorize-api-tutorials
   ```

   This project requires three ports:

   - `KONG_ENGINE_HTTPS_PORT`: The runtime port for proxying REST API requests. By default, this is 8443.
   - `KONG_ADMIN_GUI_PORT`: The port for the Kong Manager UI. By default, this is 8002.
   - `KONG_ADMIN_API_PORT`: The port for the Kong Admin API. By default, this is 8001.

   If you need to use different ports, customize the ports for your environment in the `env-template.txt` file as follows. Skip the next step if you're okay with the defaults.

2. (Optional) Copy `env-template.txt` to `.env` and edit the file:

   ```
   cp env-template.txt .env
   vi .env
   ```

   When you finish editing the file, press Esc, and then exit the editor:

   ```
   :wq
   ```

3. If Docker Desktop is not running yet, start it.

4. Bring up the project:

   ```
   docker-compose up -d --build
   ```

Copyright © 2025 Ping Identity Corporation

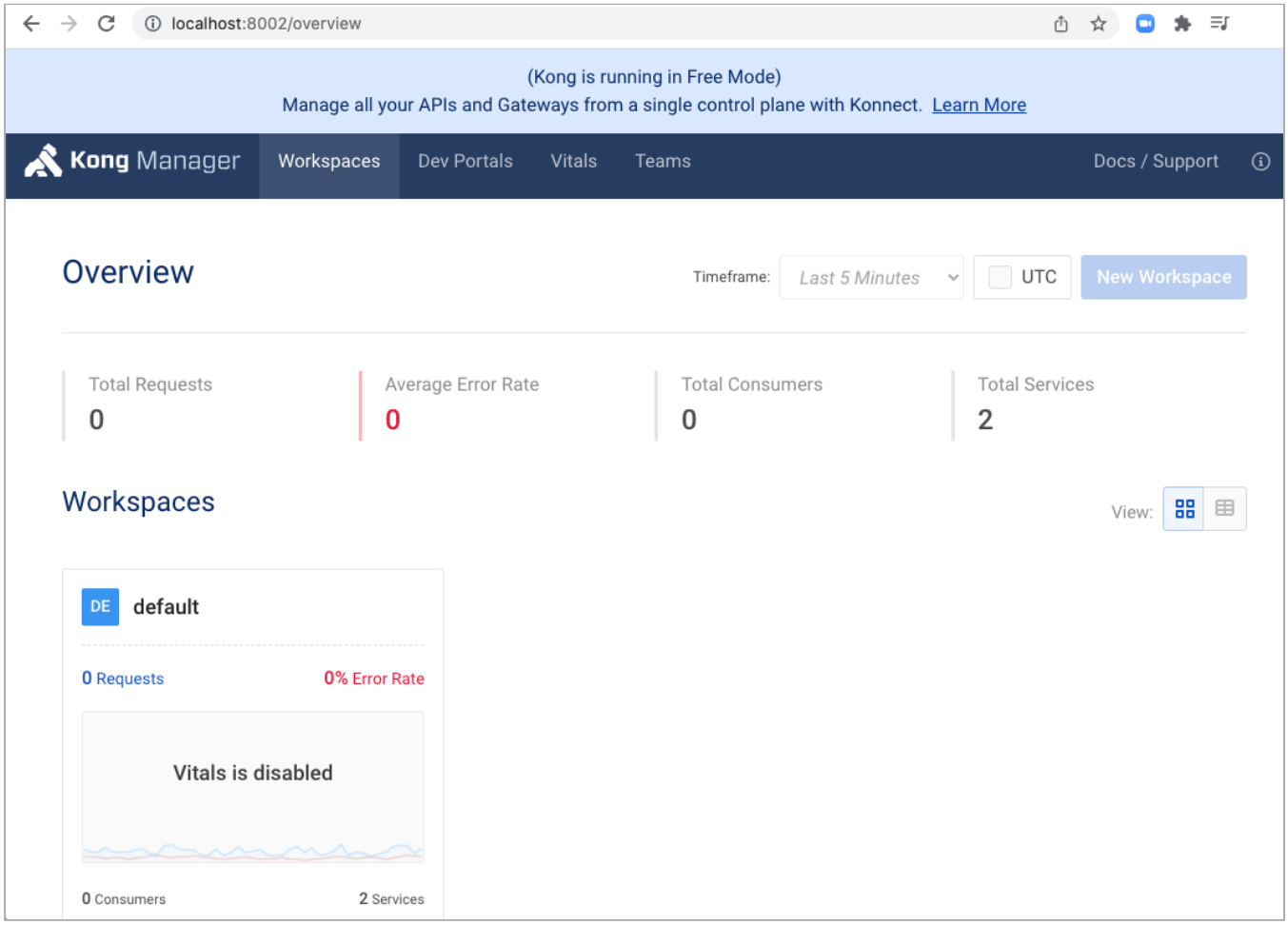
Result:

This creates the database and configures Kong.

5. To access Kong Manager, go to: http://localhost:8002.

> **Note**
>
> If you're not running on `localhost`, use your `docker-machine` name in the URL instead of `localhost`.

6. In Kong, click the **default** workspace.



7. Make sure Kong Gateway can connect to the Meme Game API:

```
curl -i --insecure --oauth2-bearer '{"sub":"user.0"}' https://localhost:8443/meme-game/api/v1/users/user.0/
answers
```

The connection might take a minute to come up. If the connection works, you'll see `HTTP/1.1 200 OK` and a JSON response. Not getting the right results? Learn more in Troubleshooting Kong Gateway integration with PingOne Authorize.

Copyright © 2025 Ping Identity Corporation

> **Tip**
>
> When you're finished with the tutorials and no longer need this environment, you can stop Kong and delete the PostgreSQL database. Don't do this yet!
>
> ```
> docker-compose down -v
> ```

Next steps

Your tutorial environment is set up and you're ready to add applications in PingOne. The first application you'll add is a banking application that doesn't have access to the Meme Game API.

Adding a banking application in PingOne

Learn how to create an application in PingOne that is granted access to a generic OAuth resource server. Later, you'll use this application to demonstrate protection against unauthorized access to a managed API service.

About this task

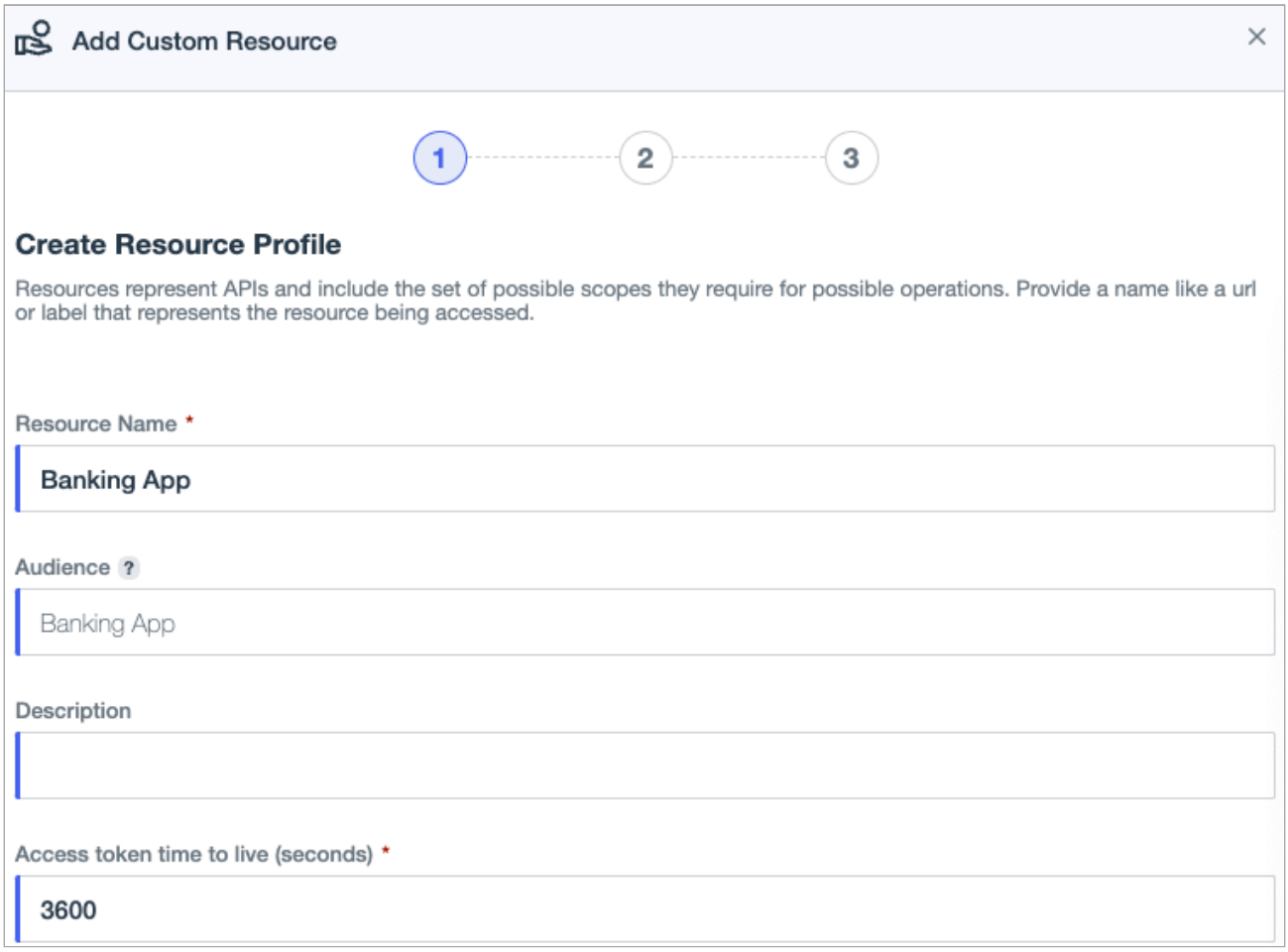
Create a banking application and its resources. You'll use the banking application to represent every other API client on the internet that doesn't have access to the Meme Game API.

First, add a banking resource in PingOne and give it an OAuth scope. Scopes determine the permissions for services that the application can access. Then, add a single page application in PingOne that represents your banking application. Grant permission for the banking application to access your banking resource.

Steps

1. Add the banking resource in PingOne:
    1. Go to **Applications** > **Resources** and click the **+** icon.
    2. For the **Resource Name**, enter `Banking App` as a unique identifier for the resource.

Copyright © 2025 Ping Identity Corporation



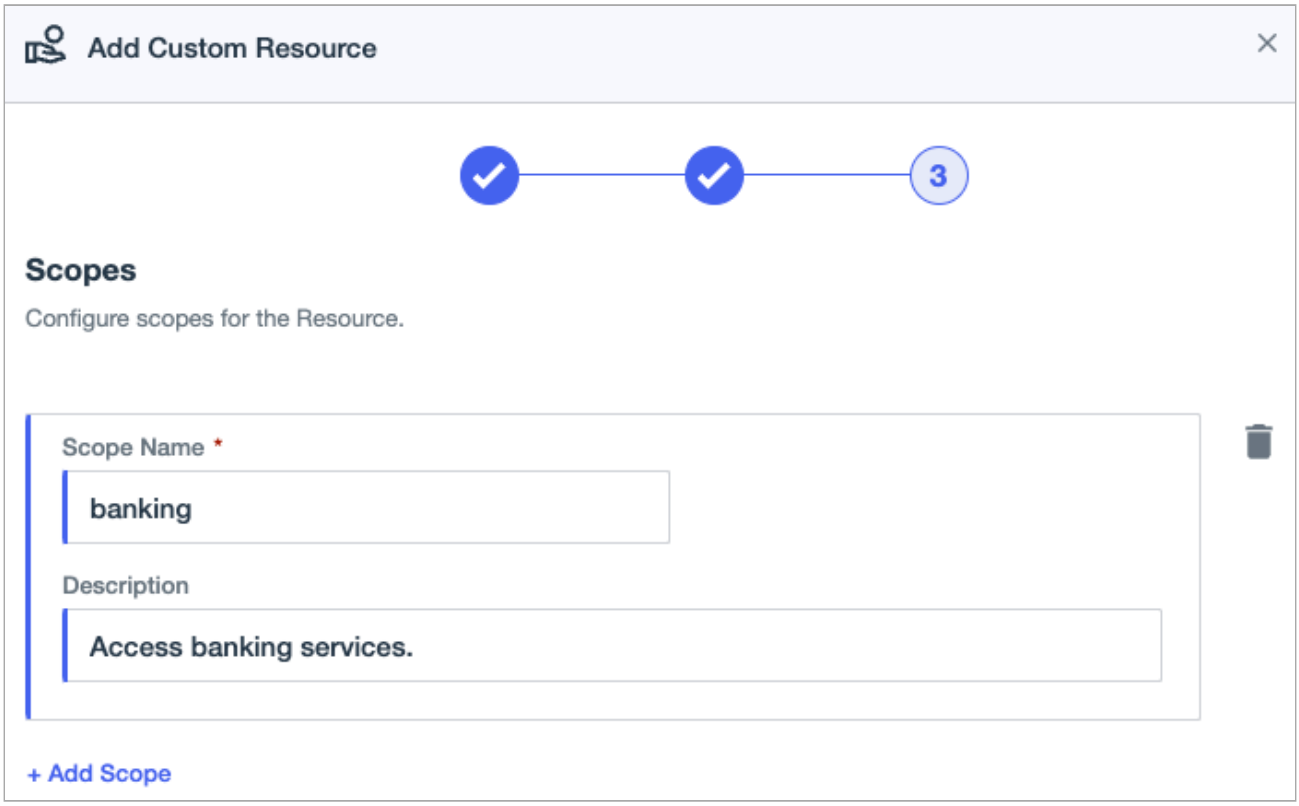
3. Click **Next**.

4. In **Attributes**, you don't need to configure any attribute mappings, so click **Next**.

5. To configure scopes, click **+ Add Scope**.

6. For the **Scope Name**, enter `banking` as an identifier for the scope, and then enter a meaningful **Description**.

Copyright © 2025 Ping Identity Corporation



7. Click **Save**.

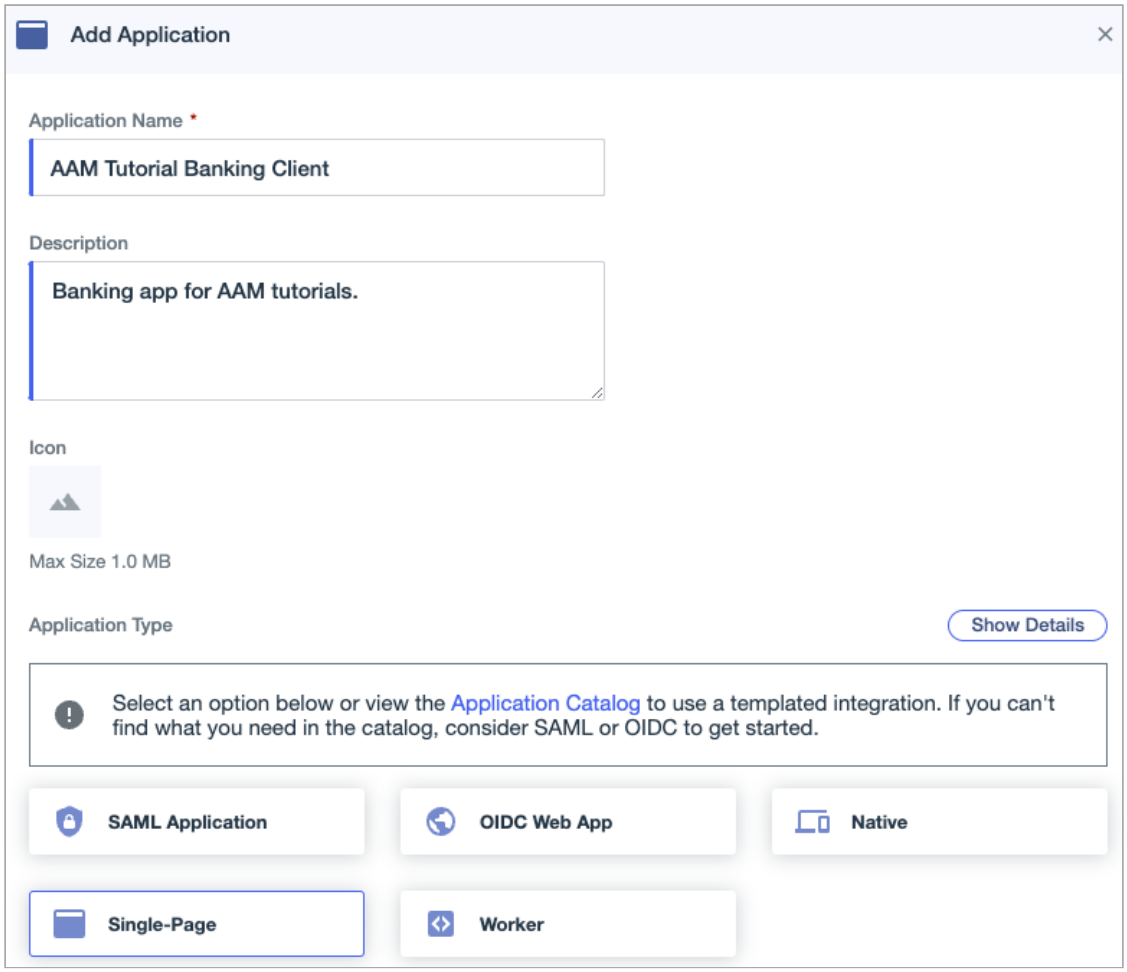
   Result:

   You're ready to add a single page banking application in PingOne.

2. Add the banking application in PingOne:

   1. Go to **Applications** → **Applications** and click the **+** icon to add an application.
   2. For the **Application Name**, enter `AAM Tutorial Banking Client` as a unique identifier for the application, and then enter a meaningful **Description**.
   3. For the **Application Type**, click **Single-Page**.

Copyright © 2025 Ping Identity Corporation



4. Click **Save**.

3. To enable the application, click the **Enable** toggle.

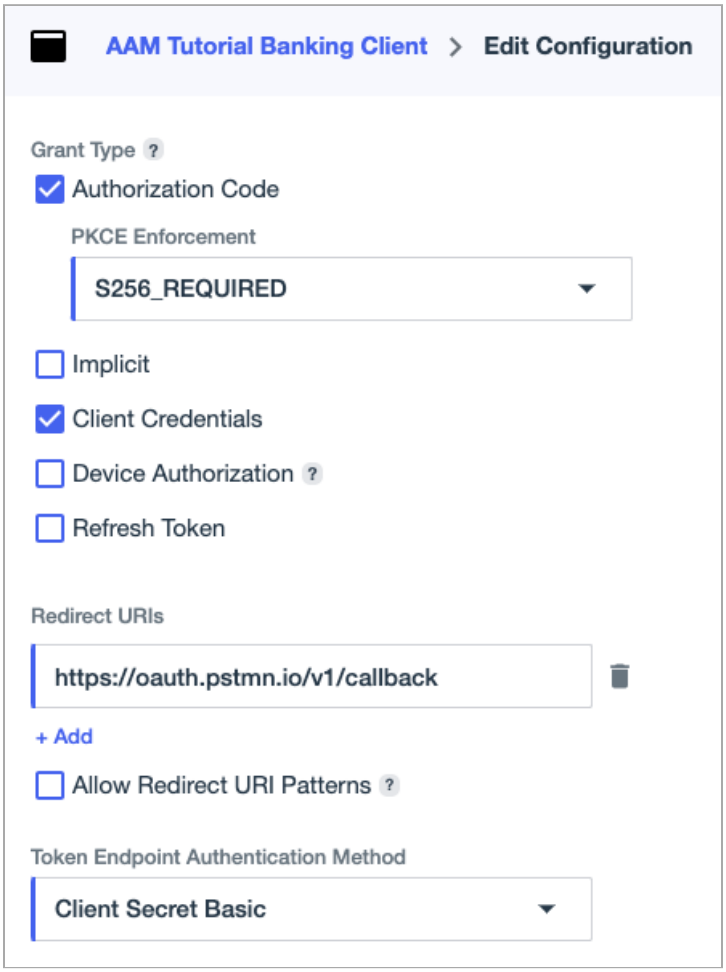
4. Configure the banking application to act as an API client without any notion of users.

   Later, this makes testing easier because you won't have to configure users.

   1. On the **Configuration** tab, click the **Pencil** icon.

   2. Under **Grant Type**, select the **Client Credentials** checkbox, and then in the **Token Endpoint Authentication Method** list, select **Client Secret Basic**.

Copyright © 2025 Ping Identity Corporation



3. For **Redirect URIs**, enter the following redirect:

   `https://oauth.pstmn.io/v1/callback`

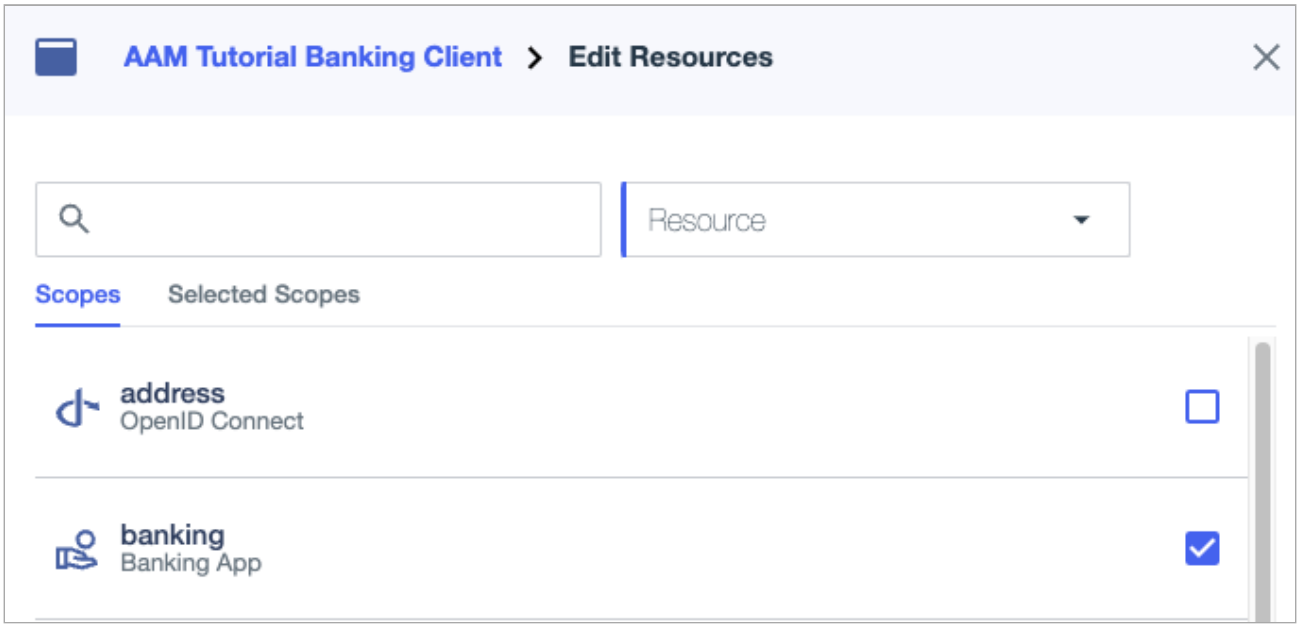
   This enables you to sign on as a user from Postman in a later tutorial.

4. Click **Save**.

5. Grant an OAuth scope to your application.

   This allows your application to access banking APIs.

   1. Click the **Resources** tab, and then click the **Pencil** icon.
   2. Select the **banking** checkbox.



3. Click **Save**.

   Keep the banking application open in PingOne for now. You'll need it in the next task.

Result

You added a single page application in PingOne to represent your banking application and configured it for access to the banking resource.

Next steps

You're ready to get an access token for the banking application so it can make calls to APIs.

Getting an access token

Get an access token with permissions for an OAuth resource server.

About this task

In order to make calls to an API, your application will provide an access token to the API resource server. You'll use Postman, acting as the banking application, to get the access token from PingOne.

To get started, let's walk through downloading the Postman collection and assigning values to variables used in the requests.

Steps

1. Import a copy of the Postman collection:

   1. Click the **Run in Postman** button below.

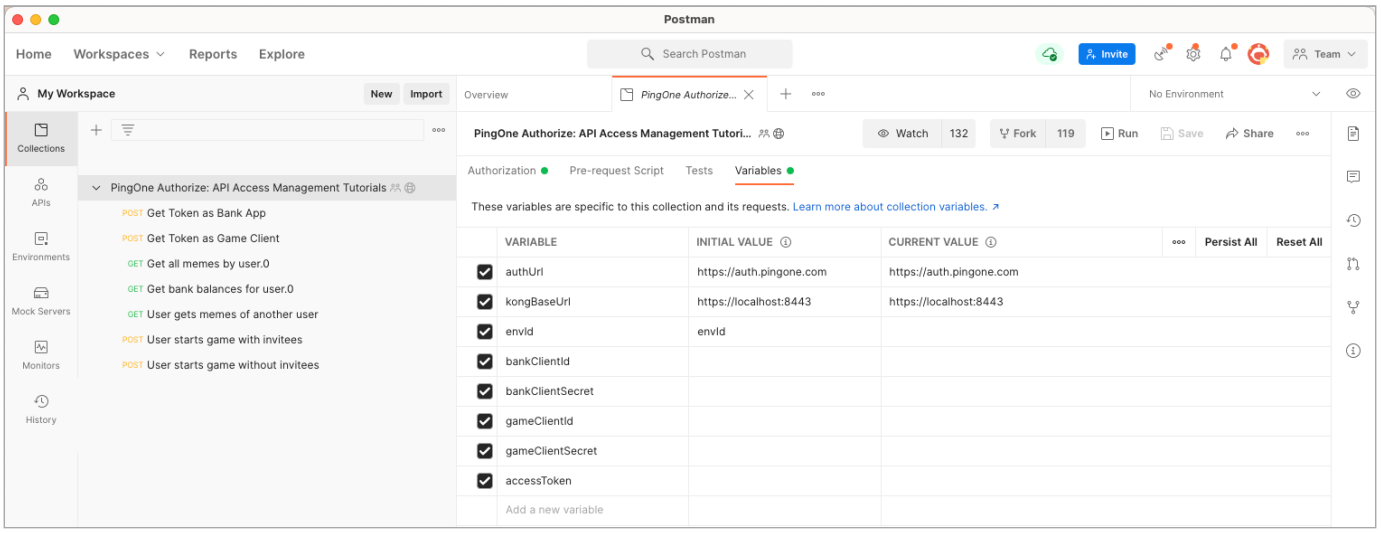
      Run in Postman

   2. Click the **import a copy** link.

   3. If you use workspaces in Postman, select a workspace and click **Import**.

Copyright © 2025 Ping Identity Corporation

2. Go to **Collections**, click **PingOne Authorize: API Access Management Tutorials** to open the collection, and then click the **Variables** tab.



3. If you are outside of the North America (US) region, update the current value of the `authUrl` to use the data center closest to your geographic region.

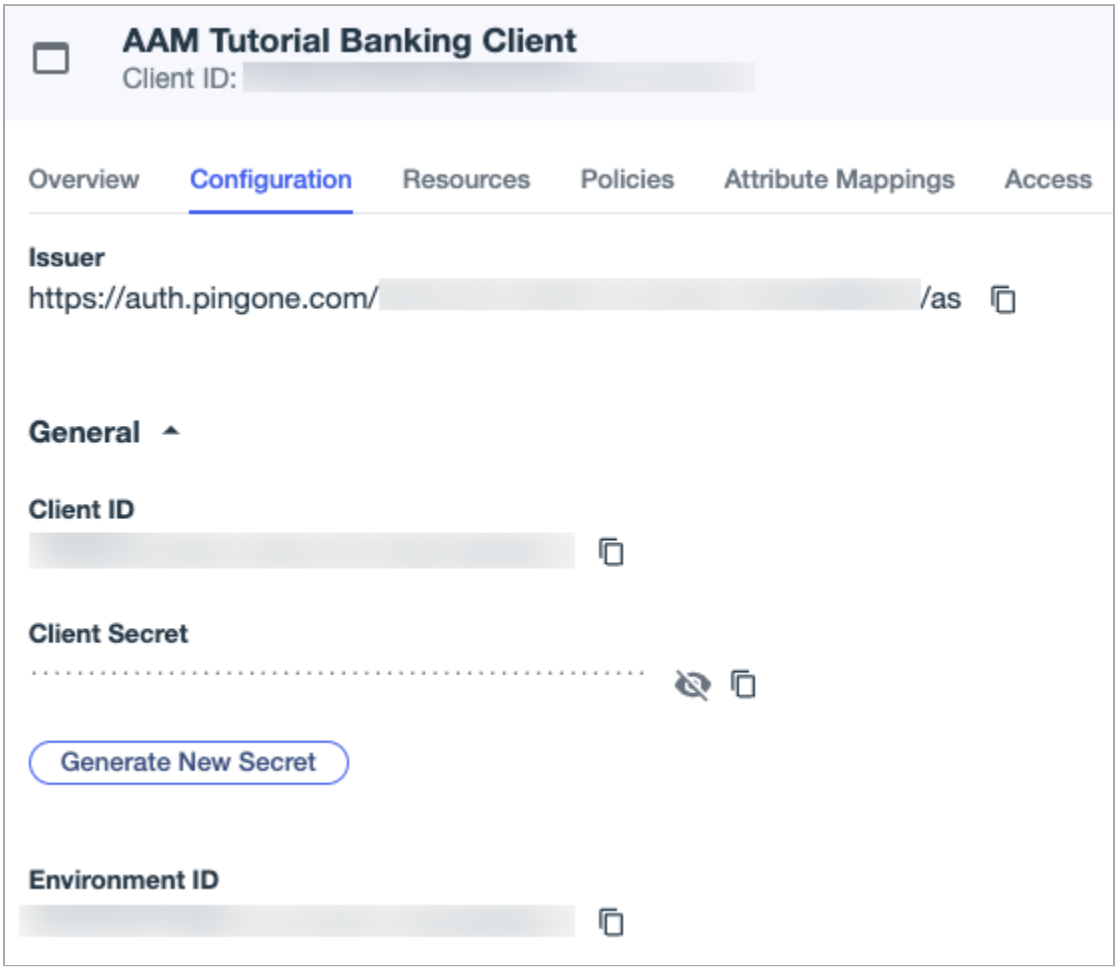
Region	authUrl
Canada	https://auth.pingone.ca
Europe	https://auth.pingone.eu
Australia	https://auth.pingone.com.au
Singapore	https://auth.pingone.sg
Asia Pacific (legacy) **Note** Available only for existing .asia customers.	https://auth.pingone.asia

4. On the **Configuration** tab of your **AAM Tutorial Banking Client** application in PingOne, copy the following values from the **General** section into corresponding current values on the **Variables** tab in Postman.

> **Tip**
>
> If you need to find the **AAM Tutorial Banking Client** application in PingOne, go to **Applications** > **Applications**. If you have trouble copying values in PingOne, refresh the browser.

- **Client ID**: The Postman variable is `bankClientId`.
- **Client Secret**: The Postman variable is `bankClientSecret`.
- **Environment ID**: The Postman variable is `envId`.

Copyright © 2025 Ping Identity Corporation

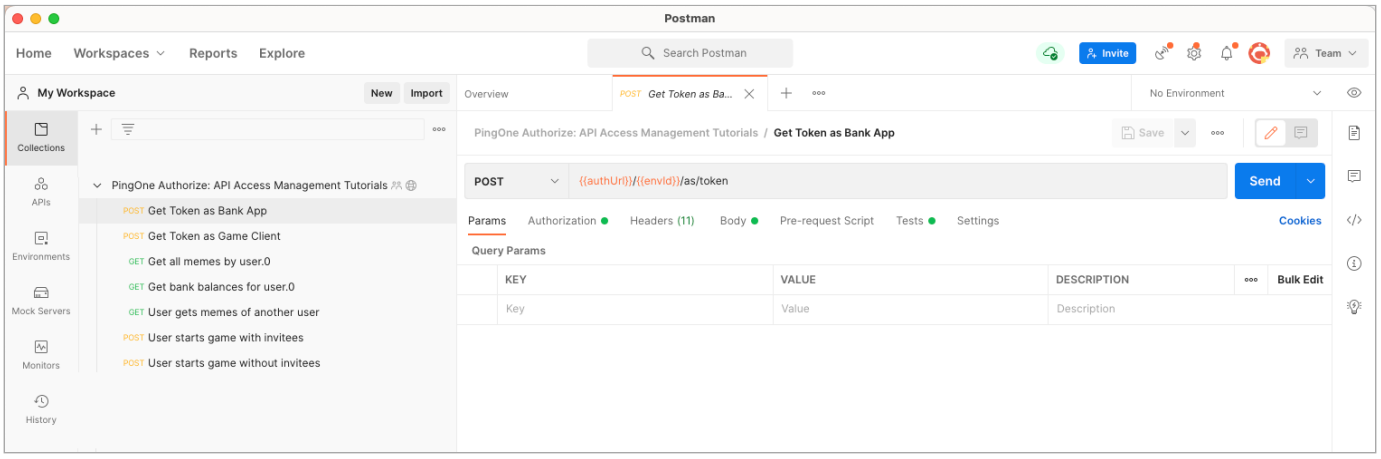


5. In Postman, click **Save** to save the current values you assigned.

   Result:

   You're ready to send a request to get an access token.

6. In Postman, select the **Get Token as Bank App** request and click **Send**.



The access token is in the response, and it has the banking scope.

Copyright © 2025 Ping Identity Corporation

```
"access_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6ImRlZmF1bHQifQ.
    [redacted]
"token_type": "Bearer",
"expires_in": 3600,
"scope": "banking"
```


Try a request to see if your banking application has access to the Meme Game API.

7. In Postman, select the **Get all memes by user.0** request and click **Send**.

   Result:

   You get a `200 OK` response. Your banking application has access because Kong Gateway isn't configured yet. Like most API gateways, Kong is configured initially with zero authorization rules by default.

   Troubleshooting:

   Not getting the right results? Learn more in Viewing API Access Management events in your PingOne environment audit log.

Result

You've granted access to the banking application in PingOne, but haven't enforced any access to resources in Kong Gateway yet.

Next steps

Configure the authorization plugin for Kong Gateway.

Configuring the authorization plugin for Kong Gateway

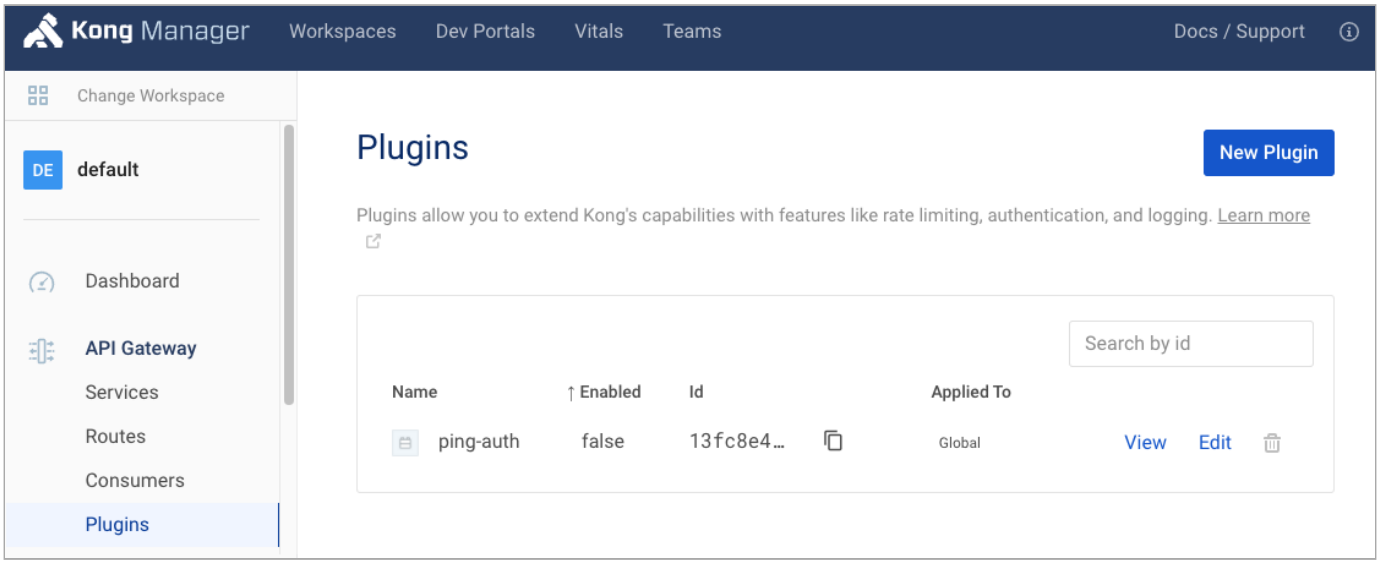
Learn how to configure the authorization plugin to set up a connection between Kong Gateway and PingOne.

Before you begin

Make sure the `pingoneauthorize-api-tutorials` container is running in Docker.

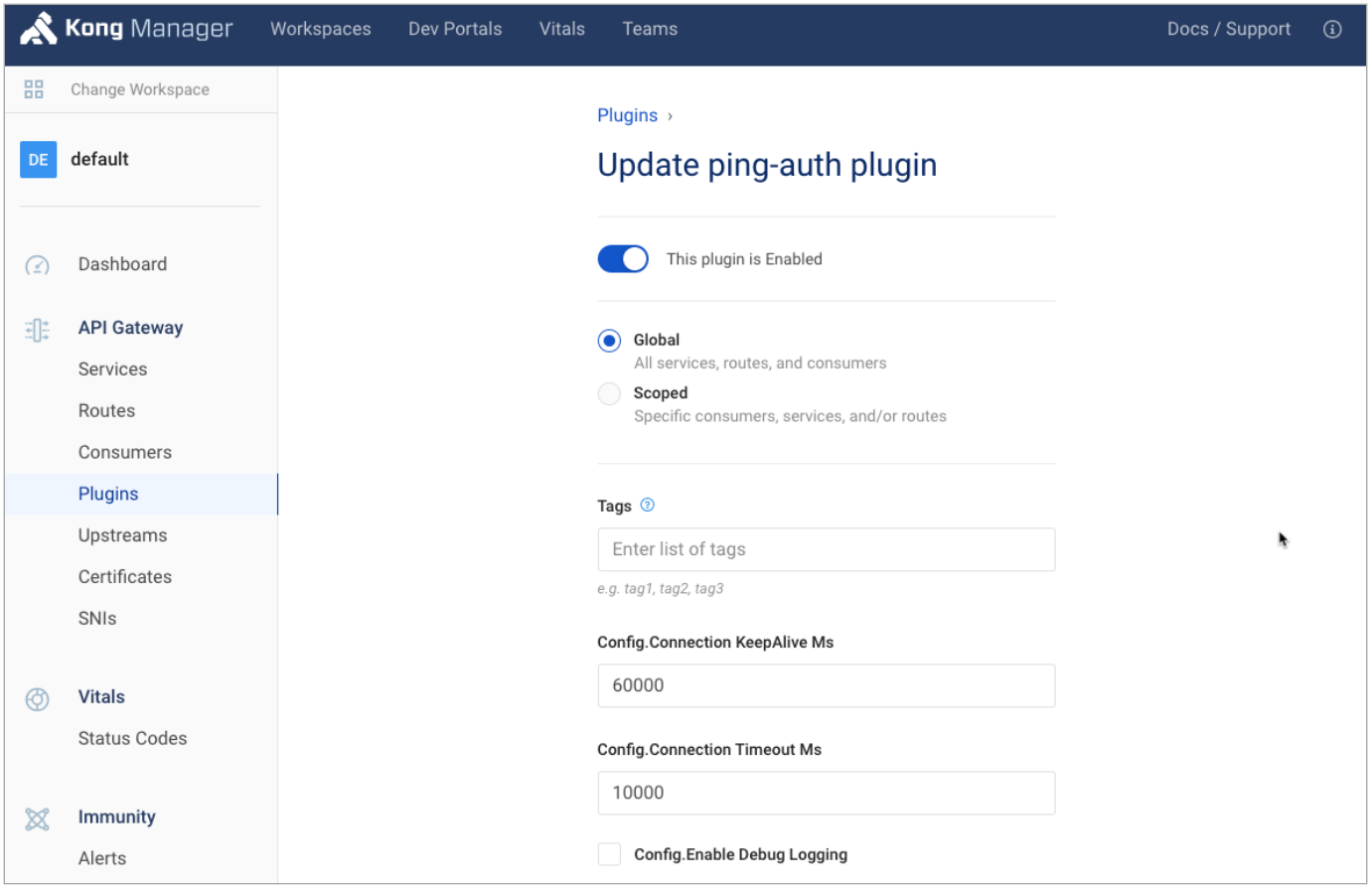
Steps

1. To access Kong Manager, go to http://localhost:8002.
2. Select the **default** workspace, and then click **Plugins**.



The `ping-auth` plugin is already installed in your tutorial environment. Now you'll configure it.

3. On the `ping-auth` line, click **Edit**.
4. On the **Update ping-auth plugin** page, click the toggle to enable the plugin.

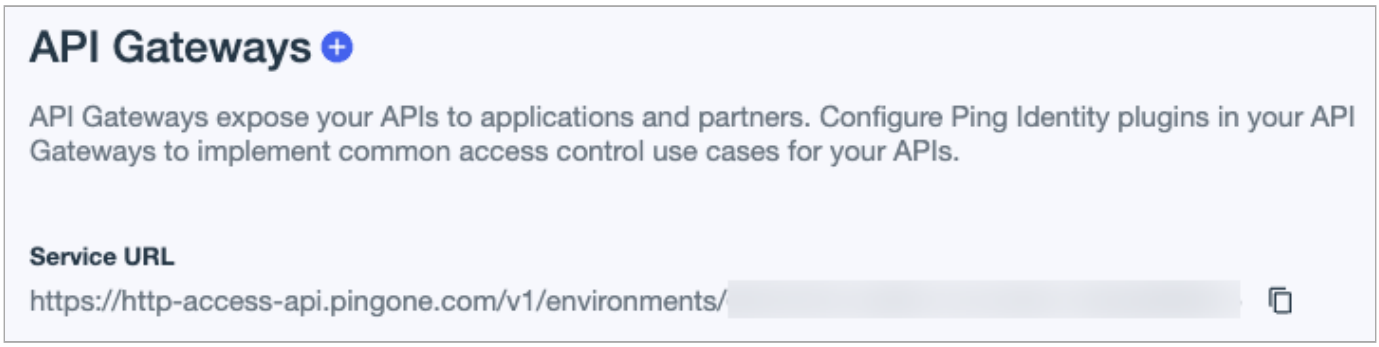


Next, you'll enter the service URL by copying it from PingOne Authorize.

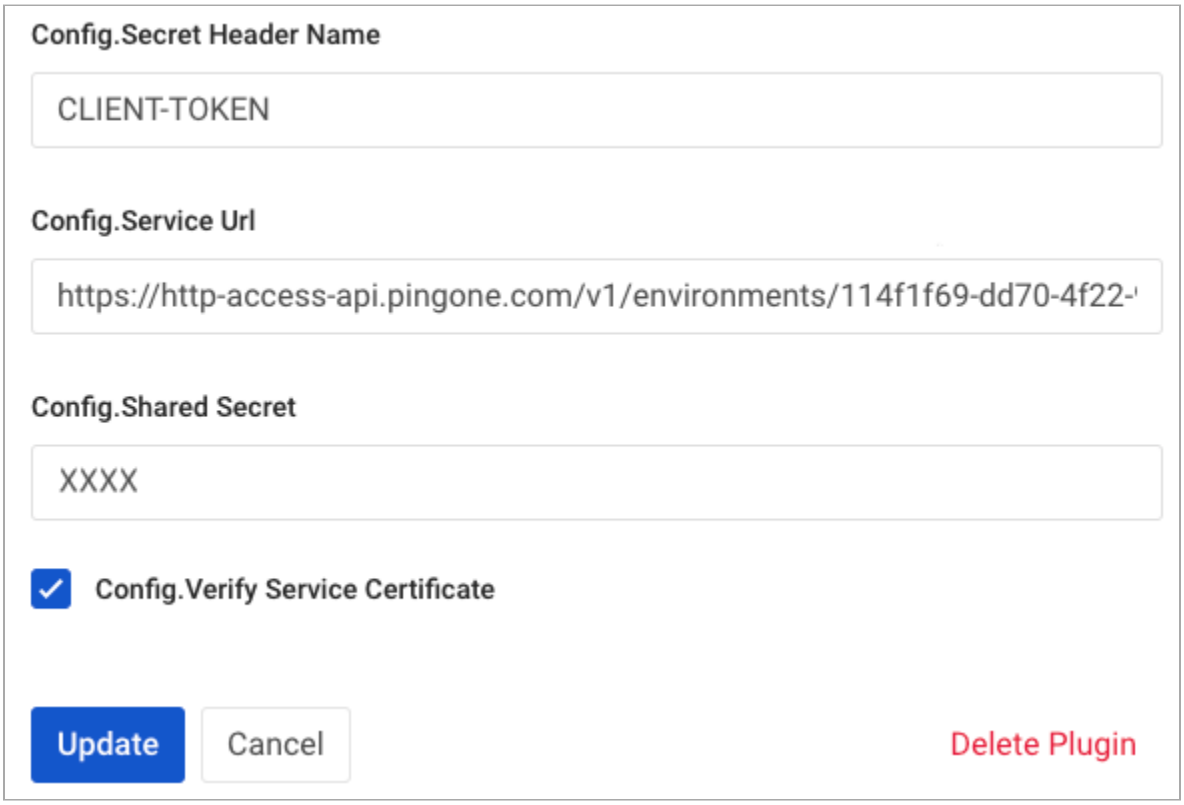
5. In PingOne, go to **Authorization > API Gateways**.

Copyright © 2025 Ping Identity Corporation

This is where you register the gateway and authorize it to work with PingOne.



6. Copy the **Service URL** and enter it in the **Config.Service Url** field in Kong Manager.

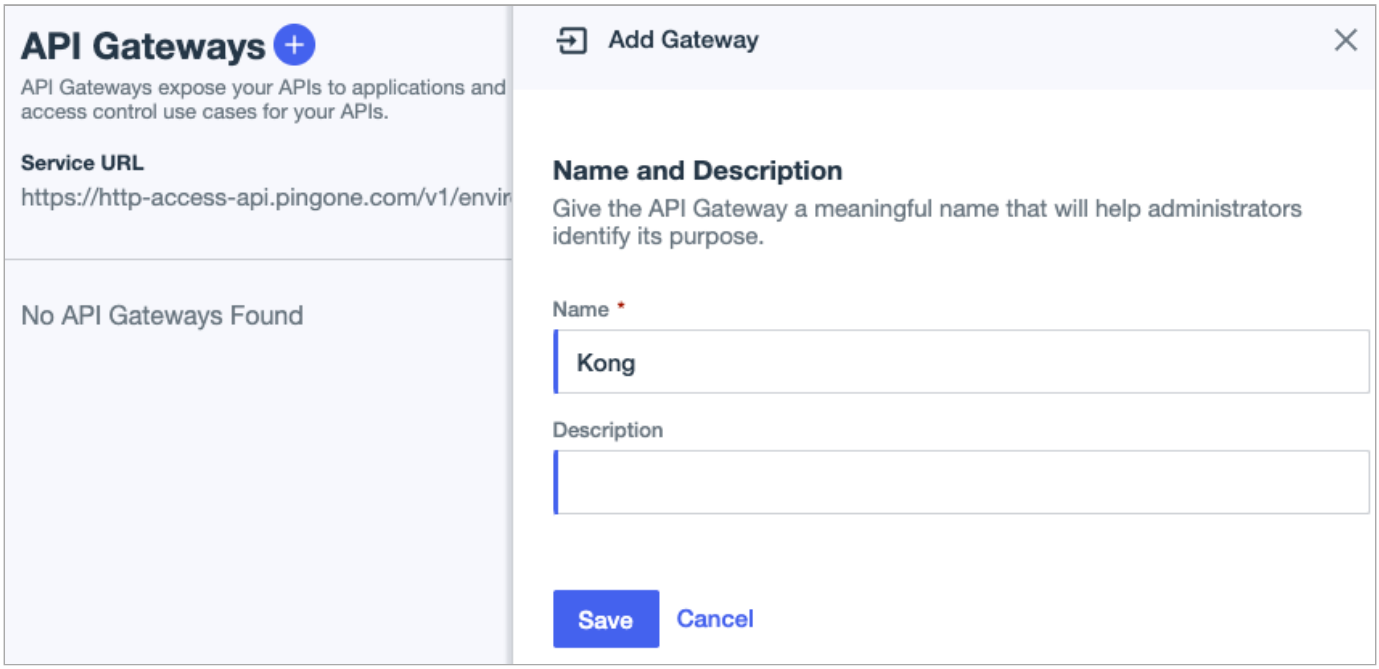


You need a credential to authorize Kong Gateway to connect to PingOne. First, add the gateway.

7. In PingOne, click the **+** icon next to **API Gateways** to add a gateway.

8. Enter `Kong` for the name of the gateway, and then click **Save**.

Copyright © 2025 Ping Identity Corporation

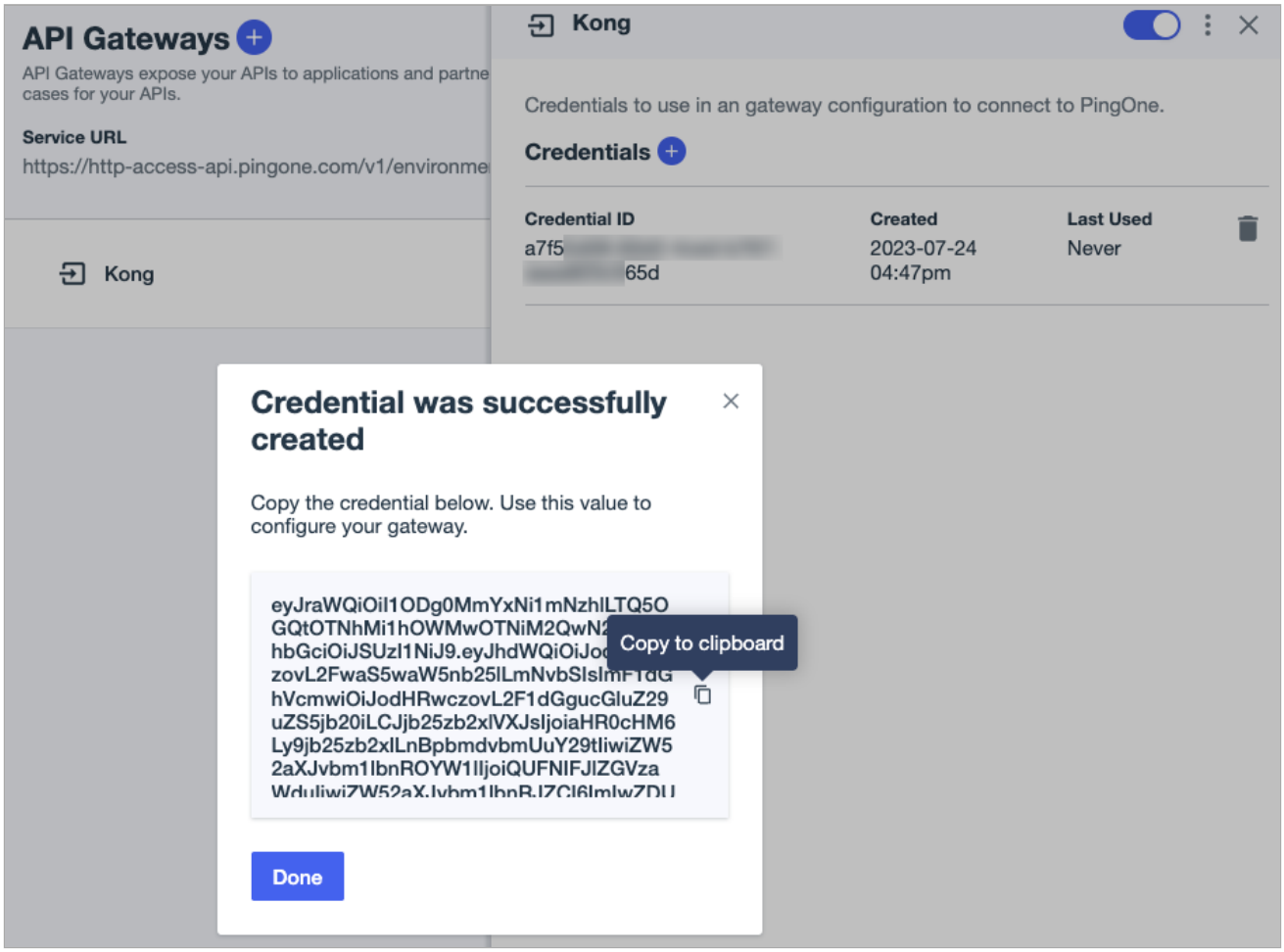


Next, you'll get the gateway credential to authorize Kong.

9. Click the **+** icon next to **Credentials** and copy the credential. Click **Done**.

> **Important**
>
> The gateway credential is the shared secret that authenticates the `ping-auth` plugin to PingOne Authorize. Version 1.2.0 of the plugin supports referenceable secrets. For security reasons, store the gateway credential in a vault supported by Kong. Learn more in Secrets Management and Environment Variables Vault in the Kong documentation.

Copyright © 2025 Ping Identity Corporation



10. In Kong Manager, enter the gateway credential in the **Config.Shared Secret** field.
11. Click **Update**, and then click **Update Plugin**.

    Result:

    Kong Gateway is configured to work with PingOne. Try the Postman request again to see if access has changed.

12. In Postman, select the **Get all memes by user.0** request and click **Send**.

    Result:

    You receive a `404 Not Found` error. This is because PingOne doesn't recognize the Meme Game API yet. By default, requests to unknown APIs fail closed, ensuring that access to an unknown API is blocked.

    Troubleshooting:

    Not getting the right results? Learn more in Viewing API Access Management events in your PingOne environment audit log.

Result

Now you have Kong Gateway connected to PingOne so that you can manage its access control behavior in PingOne.

Next steps

In the last step, the request was blocked because PingOne isn't configured to recognize the Meme Game API yet. Let's tackle that next.

Adding a managed API service for the Meme Game in PingOne

Learn how to define a managed API service in PingOne so that PingOne helps the API gateway enforce access control.

About this task

Instead of managing access control directly in Kong Gateway, you'll use an API service in PingOne to manage access control rules. PingOne, working with the authorization plugin, uses OAuth best practices to simplify management of API access control across these distributed systems.

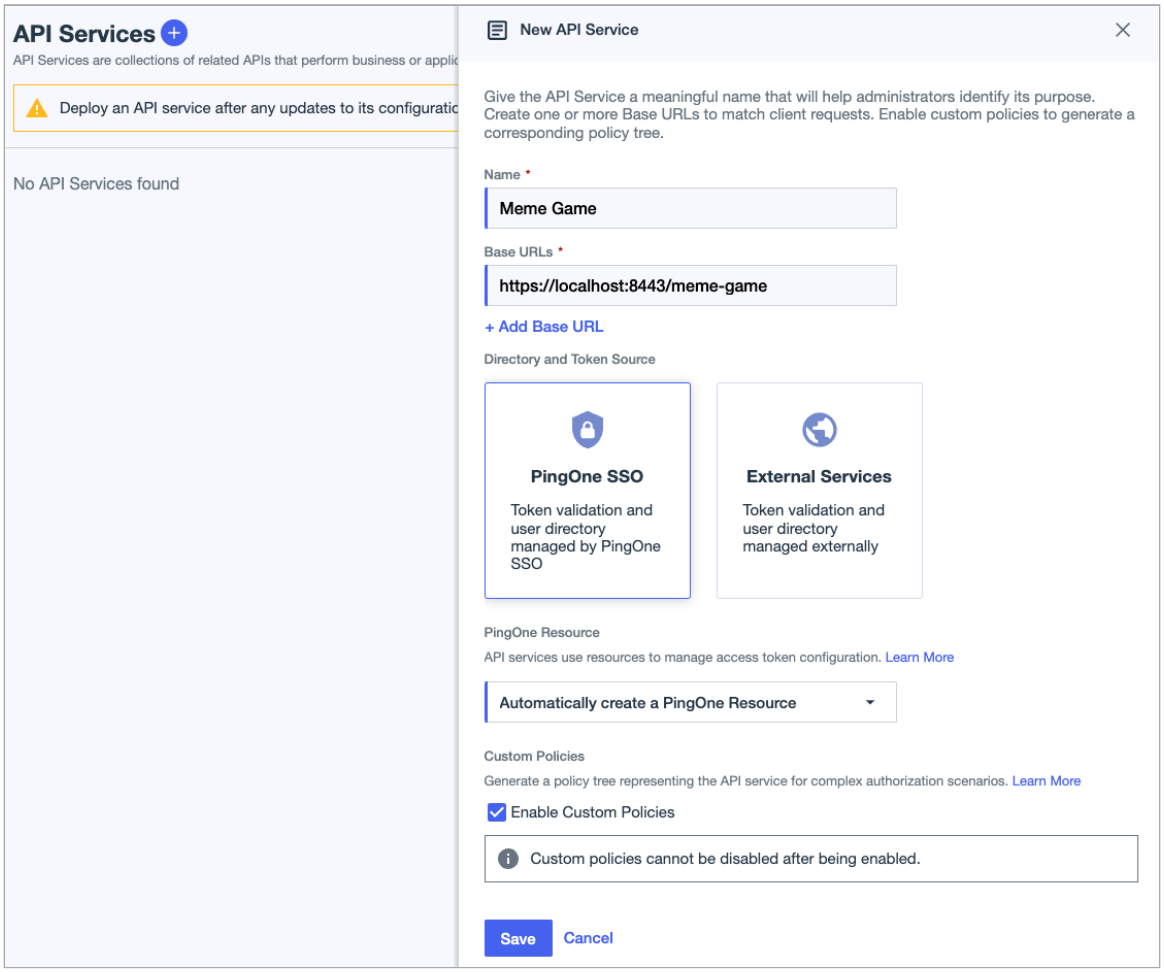
You'll define the Meme Game API in PingOne so that PingOne recognizes requests for this API and instructs Kong Gateway to protect access from unauthorized clients and allow access only from authorized clients.

Steps

1. In PingOne, go to **Authorization** > **API Services**.
2. Click the **+** icon next to **API Services** to add an API service.
3. For the service **Name**, enter `Meme Game`.
4. For **Base URLs**, enter `https://localhost:8443/meme-game`.

> **Note**
>
> If you're not running on `localhost`, use your `docker-machine` name in the URL instead of `localhost`. If you customized the ports, use the port for your environment instead of the default.

Copyright © 2025 Ping Identity Corporation



5. For the directory and token source, select **PingOne SSO**, if it is not already selected.

   This default option enables PingOne to manage user directory services and access token validation for the API service.

   > **Important**
   >
   > After you save the API service, you can't change this setting. If you want to switch to using external directory services, you must add a new API service configured with the **External Services** setting.

6. For the **PingOne Resource**, keep the default option to automatically create a PingOne resource.

   The resource establishes a relationship between the API service and PingOne in order to manage access token configuration. Resources created automatically will have the same name as the API service.

7. Select the **Enable Custom Policies** check box.

   Result:

   This will generate a policy tree for the API service, enabling you to create your own fine-grained authorization policies for the APIs managed by this API service. You'll add a custom policy in a later tutorial.

   > **Note**
   >
   > After you save the API service, you can't change this setting.

Copyright © 2025 Ping Identity Corporation

8. Click **Save**.

   Result:

   A corresponding Meme Game resource is successfully created.

9. To deploy the API service, click **Deploy**.

   Result:

   This creates a system-owned decision endpoint dedicated to the API service. This decision endpoint has the same name as the API service. Future deployments will publish any updates to the policy tree. PingOne is now configured to recognize the Meme Game API. Keep the API service open in PingOne. You'll need it in the next task.

   Try the Postman request again to see if your banking application can get memes.

10. In Postman, select the **Get all memes by user.0** request and click **Send**.

    Result:

    You get a `401 Unauthorized` error this time. That's because the access token is for your banking service, not the Meme Game.

    Troubleshooting:

    Not getting the right results? Learn more in Viewing API Access Management events in your PingOne environment audit log.

Result

Access to the Meme Game through Kong Gateway is now protected by PingOne, so unauthorized clients can't access the game.

Next steps

Create an application in PingOne that can access the Meme Game.

Adding a Meme Game application in PingOne

Learn how to create an application in PingOne that is granted access to a managed API service, then demonstrate authorized access to the API service.

About this task

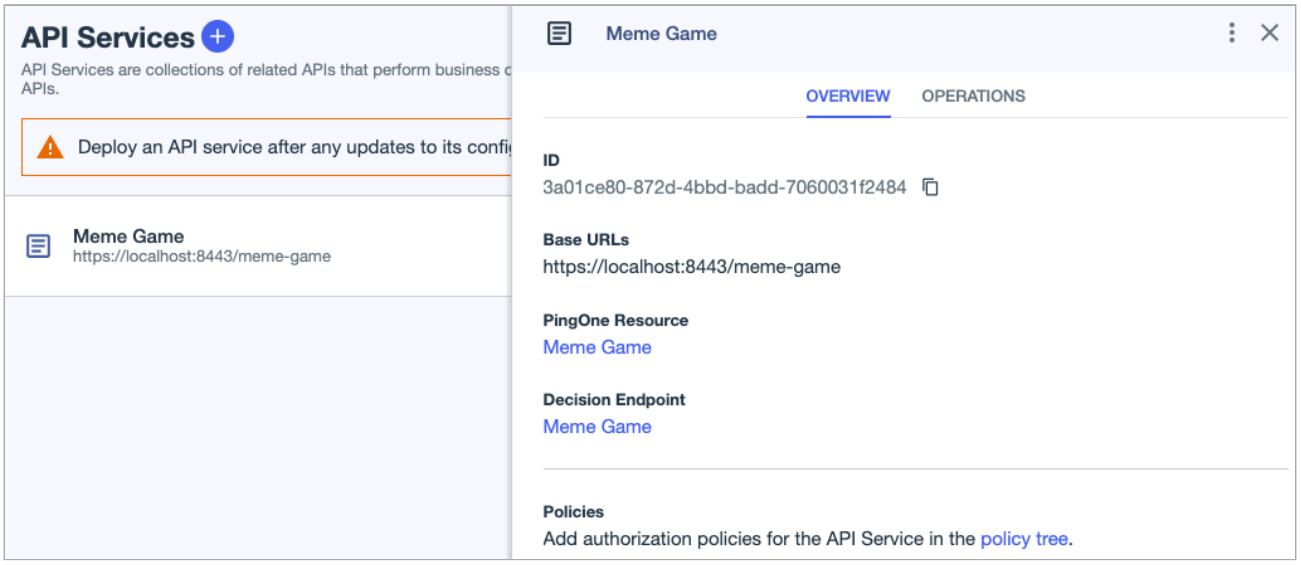
You'll create a Meme Game application in PingOne that has access to the Meme Game API. First, you'll add a scope to the Meme Game API service and use the scope to configure access to Meme Game APIs. Then, you'll add a single-page application that represents the browser-based game. Last, you'll grant permission for the Meme Game application to access the Meme Game API service.

Steps

1. Add a scope to the Meme Game API service:

   1. On the Meme Game API service **Overview** tab in PingOne, under **PingOne Resource**, click **Meme Game**.

Copyright © 2025 Ping Identity Corporation



> **Tip**
>
> If you need to find the Meme Game API service in PingOne, go to **Authorization** > **API Services**. This resource link is available because you created the resource automatically when you added the Meme Game API service.

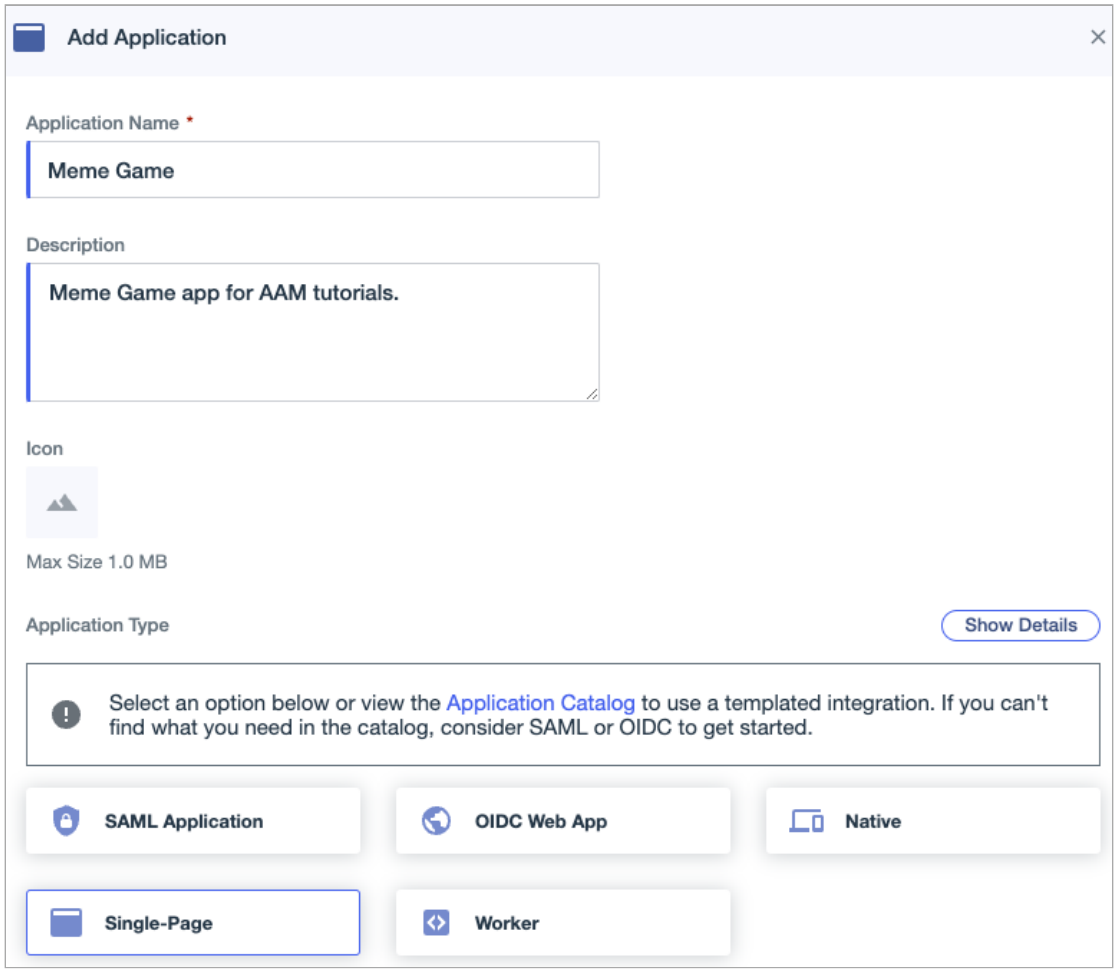
2. In **Applications** > **Resources**, on the **Scopes** tab, click **+ Add Scope**.
3. In the **Scope Name** field, enter `meme-game`.
4. Click **Save**.

   Result:

   Now you're ready to add the Meme Game application in PingOne.

2. Add a single-page application for the Meme Game:
   1. Go to **Applications** > **Applications** and click the **+** icon to add an application.
   2. For the **Application Name**, enter `Meme Game` as a unique identifier for the application, and then enter a meaningful **Description**.
   3. For the **Application Type**, select **Single-Page**.

Copyright © 2025 Ping Identity Corporation



4. Click **Save**.

3. To enable the application, click the **Enable** toggle.

4. Configure the Meme Game application to act as an API client without any notion of users.

   This will make testing easier later, because you won't have to configure users.

   1. On the **Configuration** tab, click the **Pencil** icon.

   2. Under **Grant Type**, select the **Client Credentials** checkbox, and then in the **Token Endpoint Authentication Method** list, select **Client Secret Basic**.

   3. For **Redirect URIs**, enter the following redirect:

      `https://oauth.pstmn.io/v1/callback`

      This enables you to sign on as a user from Postman in a later tutorial.

   4. Click **Save**.

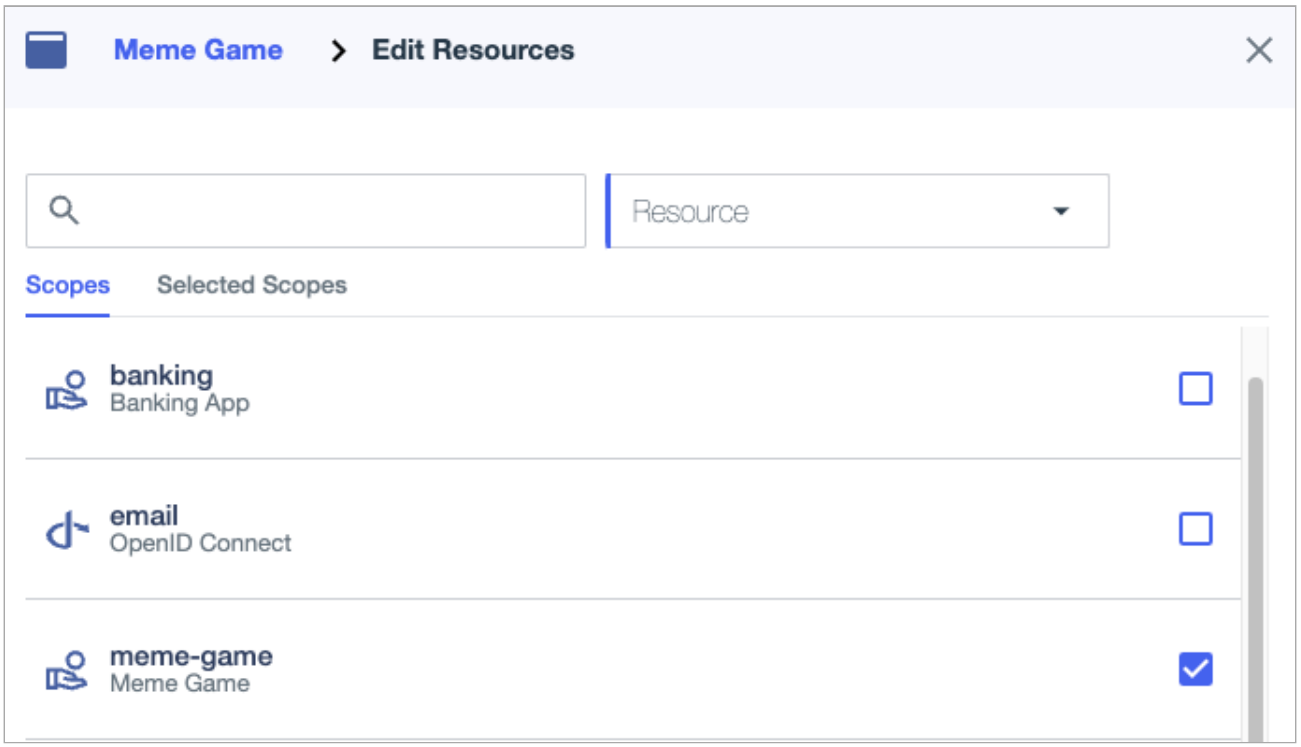
5. Grant an OAuth scope to your application.

   This allows your application to access Meme Game APIs.

   1. Click the **Resources** tab, and then click the **Pencil** icon.

Copyright © 2025 Ping Identity Corporation

2. Select the **meme-game** checkbox.



3. Click **Save**.

   Next, you'll populate variables in Postman for your new application.

6. Set up Postman and send requests:

   1. On the **Configuration** tab of the **Meme Game** application, copy the following values from the **General** section into corresponding current values on the **Variables** tab in Postman:

      - **Client ID**: The Postman variable is `gameClientId`.
      - **Client Secret**: The Postman variable is `gameClientSecret`.

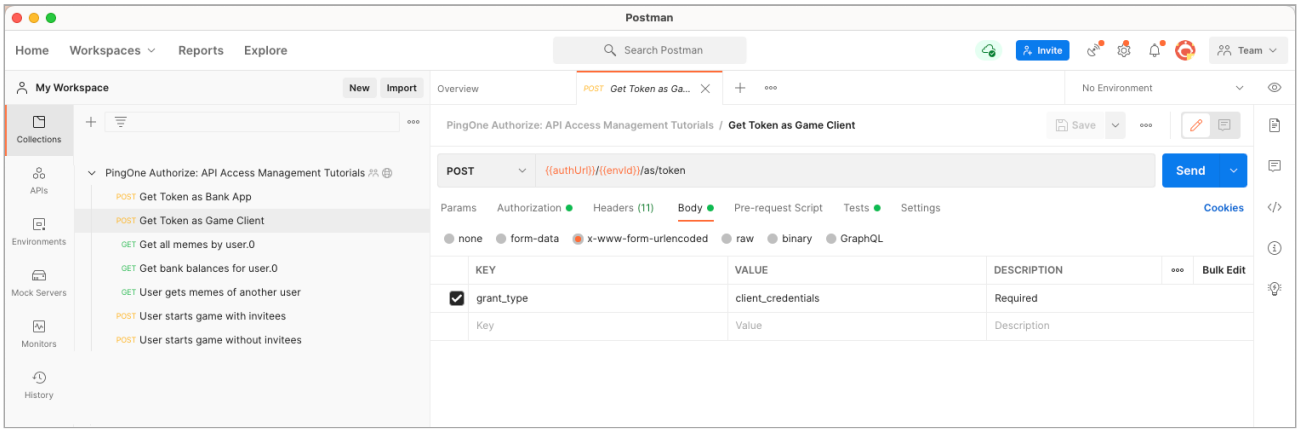
   2. In Postman, click **Save** to save the current values you assigned.

      Result:

      You're ready to send a request to get an access token.

   3. In Postman, select the **Get Token as Game Client** request and click **Send**.

Copyright © 2025 Ping Identity Corporation



Result:

The access token is in the response and it has the meme-game scope.


```
"access_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6ImRlZmF1bHQifQ.
    [redacted]
"token_type": "Bearer",
"expires_in": 3600,
"scope": "meme-game"
```


Postman, acting as the Meme Game application, has an access token for the Meme Game API. Try a Postman request to see if the Meme Game application can get memes.

4. In Postman, select the **Get all memes by user.0** request and click **Send**.

   Result:

   You get a `200 OK` response with data in the response body. You've configured access control for two applications: one that can access the Meme Game API and one that can't.

   Check the banking application again to make sure it can't access the Meme Game API now. First, get an access token for the banking application. Then, retry the request to get memes.

5. Select the **Get Token as Bank App** request and click **Send**.

   Result:

   Your access token has the banking scope.

6. Select the **Get all memes by user.0** request and click **Send**.

   Result:

Copyright © 2025 Ping Identity Corporation

You get a `401 Unauthorized` response.

Troubleshooting:

Not getting the right results? Learn more about troubleshooting in Viewing API Access Management events in your PingOne environment audit log.

Result

Congratulations! By configuring a plugin that connects Kong Gateway to PingOne, you've centralized the management of API access control in PingOne. Now you don't have to deal with the intricacies of OAuth or the risks of a distributed configuration for permissions and access control.

In this tutorial, you connected PingOne to Kong Gateway and configured applications and a managed API service in PingOne. By controlling which applications are authorized to connect to the managed API service, you demonstrated that only authorized clients are able to access managed APIs.

Next steps

Learn more about additional API Access Management capabilities of PingOne Authorize in the tutorial for user-based access control for specific API operations.

Tutorial 2: Controlling access to specific API operations

Learn how to configure API Access Management in PingOne Authorize to provide protection and access control for specific API operations.

Suppose there are two kinds of users in the Meme Game and they have different permissions:

- Game players compete with their friends to craft the funniest meme.
- Game administrators can review memes submitted by any user when they're flagged as inappropriate.

You need to allow administrators to review memes, but not allow players to review them. To do this, you'll configure users in PingOne, then define an API service operation to control permissions, and finally sign on as different users to demonstrate controlled access.

Before you begin, make sure you complete Tutorial 1: Controlling access to APIs managed by an API service to set up the environment you need for this tutorial.

What you'll learn

You'll learn how to:

- Configure users and groups in PingOne
- Protect API operations and control user permissions for privileged actions
- Demonstrate that only authorized users can perform protected actions

Copyright © 2025 Ping Identity Corporation

What you'll do

Follow these steps to complete the tutorial:

- Set up users and a group in PingOne.
- Define an API service operation and create a rule that gives only administrators access to the protected action.
- Sign on and review memes as an authorized administrator. Then sign on as an unauthorized player, demonstrating that players are prevented from reviewing memes.

Adding player and admin users for the Meme Game

Learn how to add users and groups in PingOne and use them for API access control.

Before you begin

Complete Tutorial 1: Controlling access to APIs managed by an API service to ensure you have:

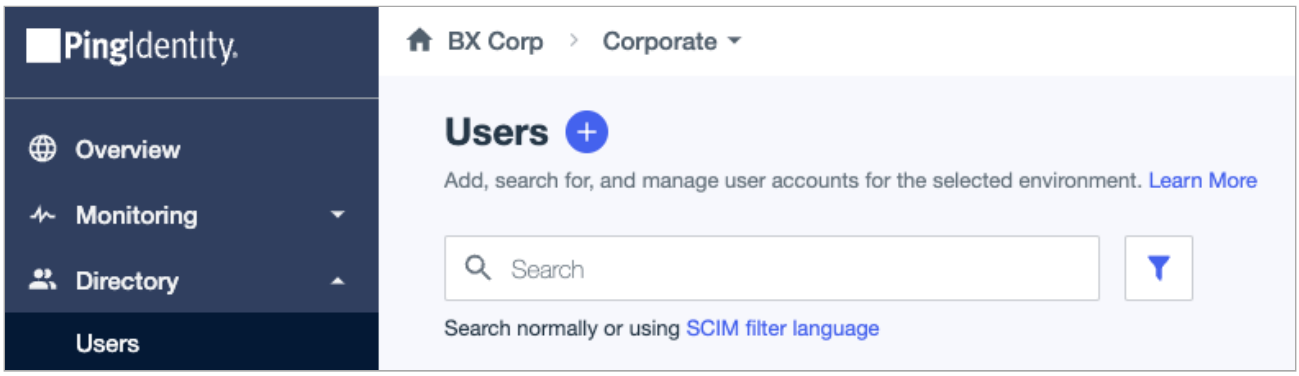
- Configured the authorization plugin to connect PingOne to Kong Gateway
- Defined a managed API service for the Meme Game
- Authorized Postman, acting as the game client, to access the Meme Game API

About this task

As the first step in controlling which users can review submitted memes, you'll create users in PingOne for the Meme Game administrator and the game player. Then, you'll create an administrator group that you'll use later to manage access to the API operation for reviewing memes.

Steps

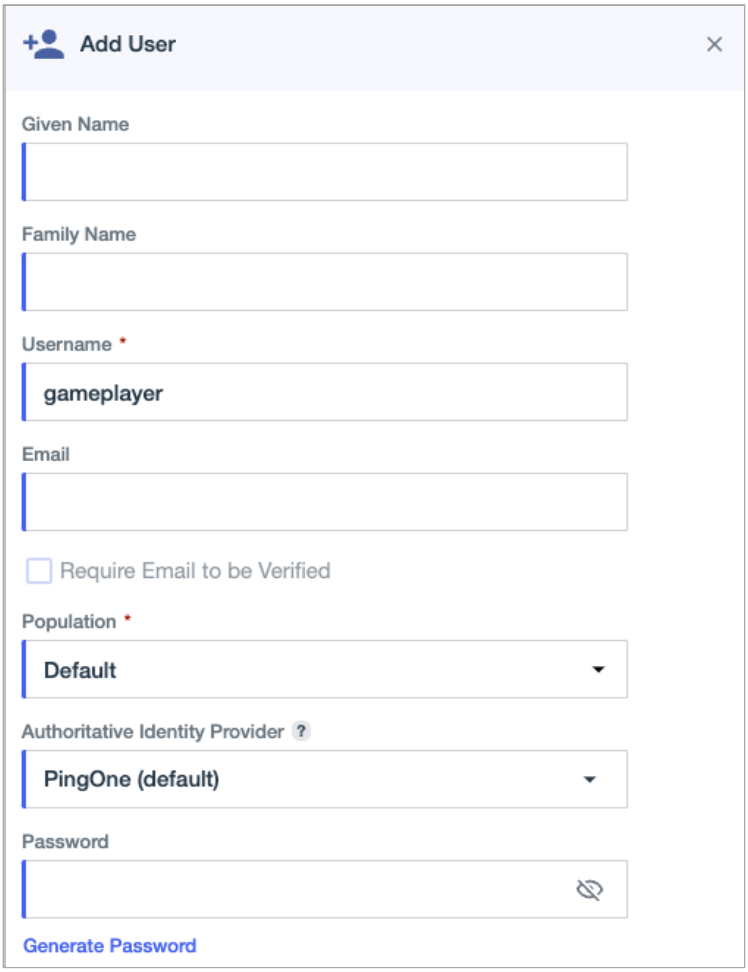
1. Add users:
    1. In PingOne, go to **Directory** > **Users** and click the **+** icon next to **Users**.



    First, you'll add the player.

    2. For **Username**, enter `gameplayer`.
    3. For **Population**, select **Default**, if it is not already selected.

Copyright © 2025 Ping Identity Corporation



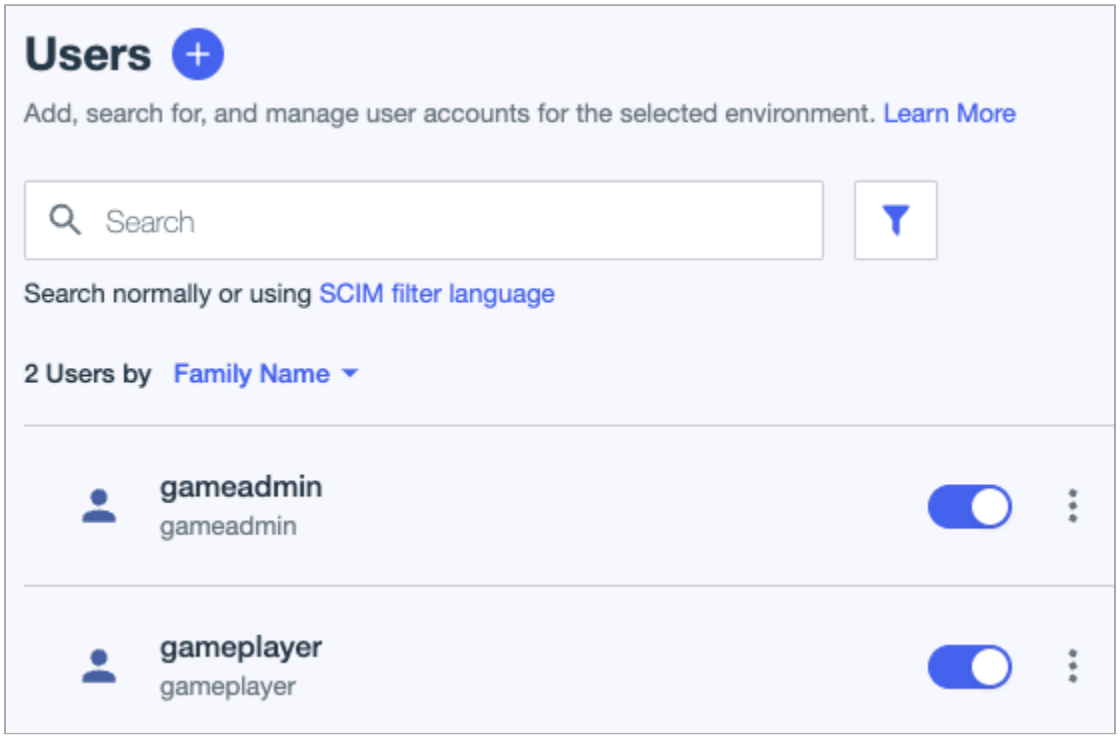
4. Click **Generate Password**, then click the **Eye** icon and copy the password to a convenient location. You'll need it later.
5. Click **Save**.

   Next, you'll add the administrator.
6. Click the **+** icon next to **Users**.
7. For **Username**, enter `gameadmin`.
8. Make sure the **Population** is **Default**.
9. Click **Generate Password**, then click the **Eye** icon and copy the password to a convenient location.
10. Click **Save**.

    Result:

    The **Users** page shows your users.

Copyright © 2025 Ping Identity Corporation

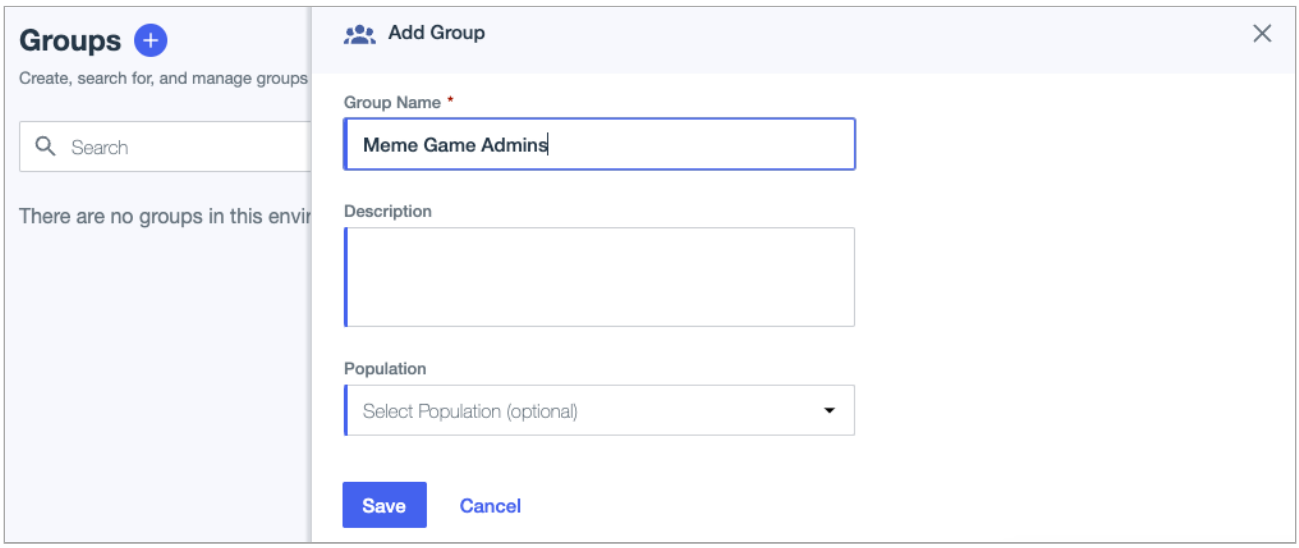


Next, you'll create a group for game administrators and add the **gameadmin** user to this group. Groups provide a way to organize a collection of users, making it easier to manage access to applications and operations.

2. Add a group:

   1. Go to **Directory** > **Groups** and click the **+** icon next to **Groups**.

   2. For the **Group Name**, enter `Meme Game Admins`, and then click **Save**.



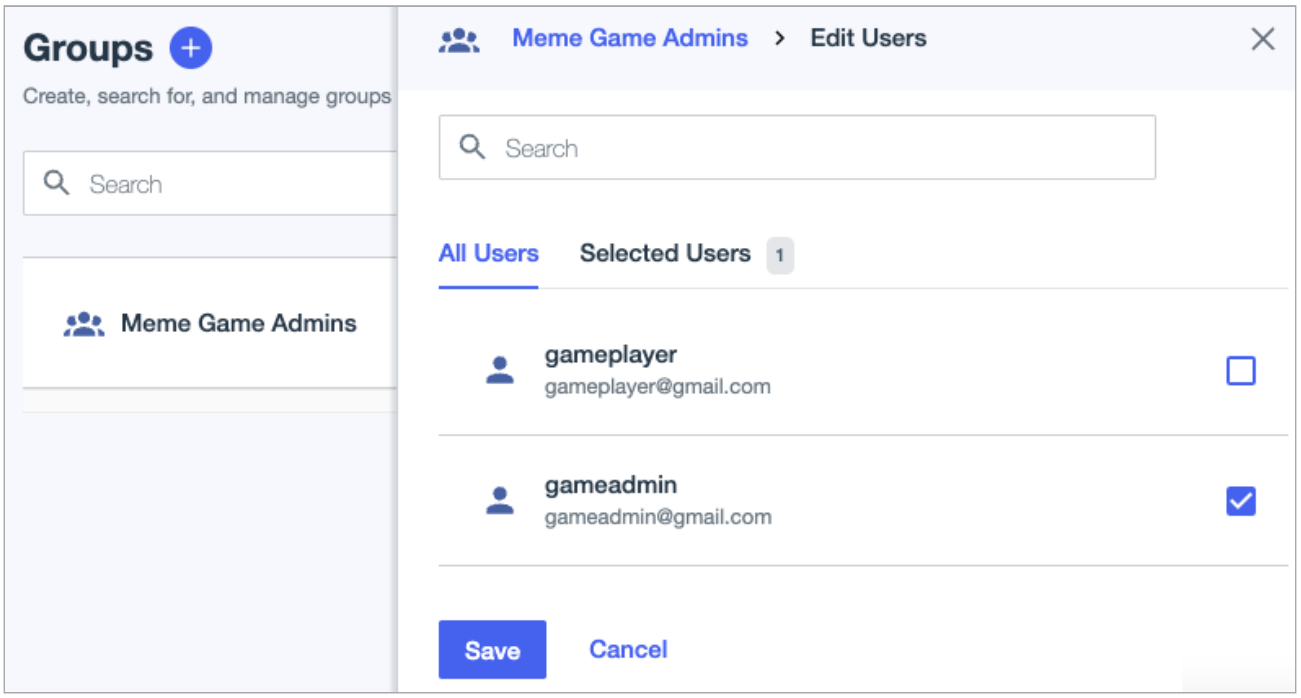
   3. Click the **Users** tab and then click **Add Individually**.

      Result:

      The **All Users** tab shows all available users.

Copyright © 2025 Ping Identity Corporation

4. Select the **gameadmin** check box.



5. Click **Save**.

   Result:

   The **gameadmin** user is now a member of the **Meme Game Admins** group.

Result

You've set up users and a group.

Next steps

Use the group in a rule to control access to an API operation.

Defining an operation for a privileged action

Learn how to add API service operations in PingOne and use rules to control access to operations.

About this task

Define an API service operation to match the API requests used to get another user's submitted memes. Then, create a rule to give only members of the **Meme Game Admins** group permission to perform the operation.

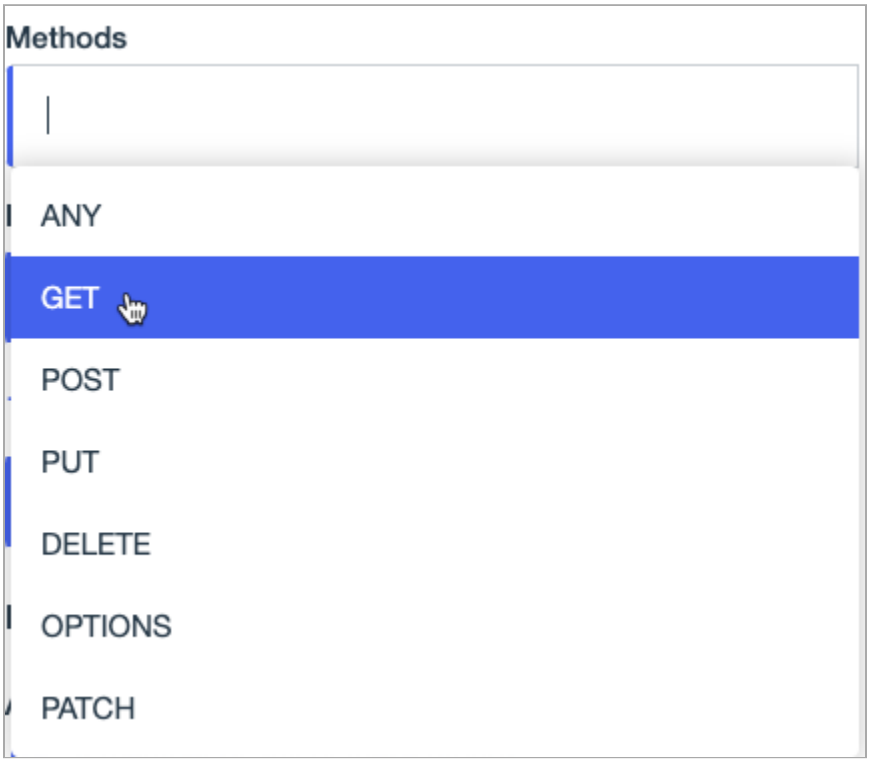
Steps

1. In PingOne, go to **Authorization > API Services**.
2. Click the **Meme Game** API service, and then click the **Operations** tab.
3. Click **Define Operation** to create a new operation.

Copyright © 2025 Ping Identity Corporation

4. Define a method and path combination that matches a client request to the API:

    1. Click **Methods**, and then select the GET method. Click outside the list of methods to close it.

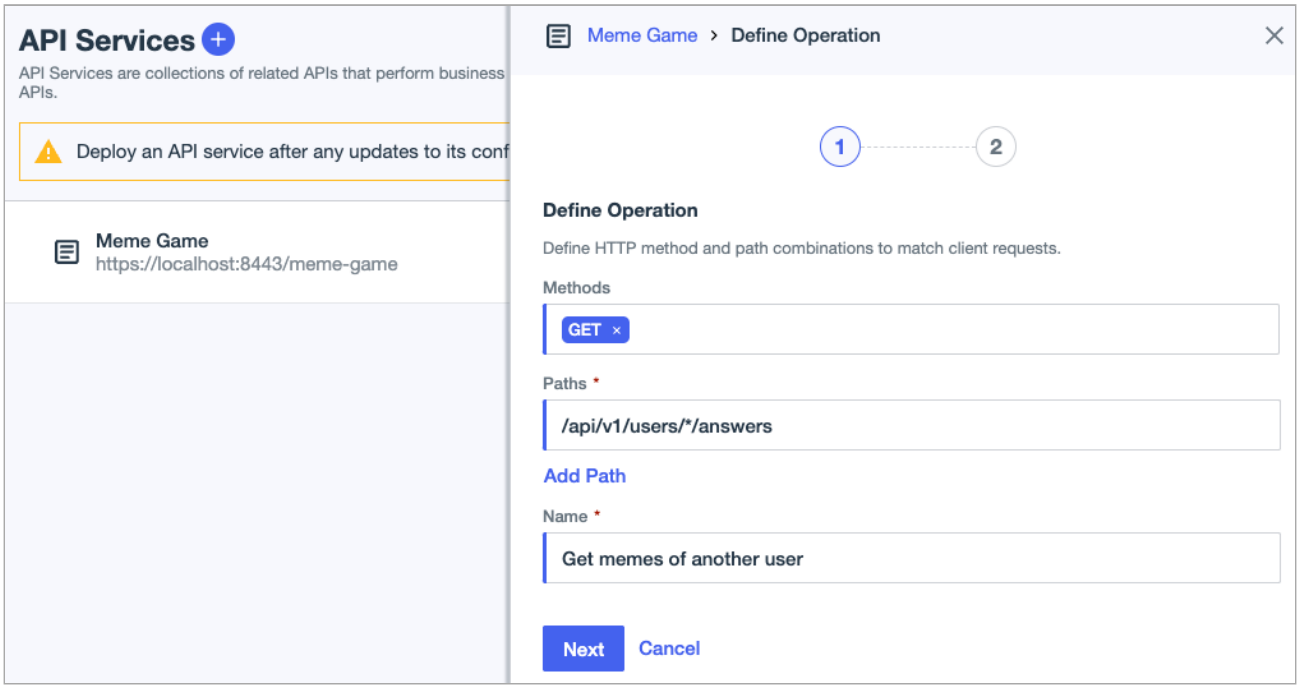
    2. For **Paths**, enter the following:

    `/api/v1/users/*/answers`

    This is the API path for getting a user's memes. The path must start with a slash (/). The asterisk (`*`) is a wildcard that represents any answers.

    3. For **Name**, enter `Get memes of another user`.

Copyright © 2025 Ping Identity Corporation

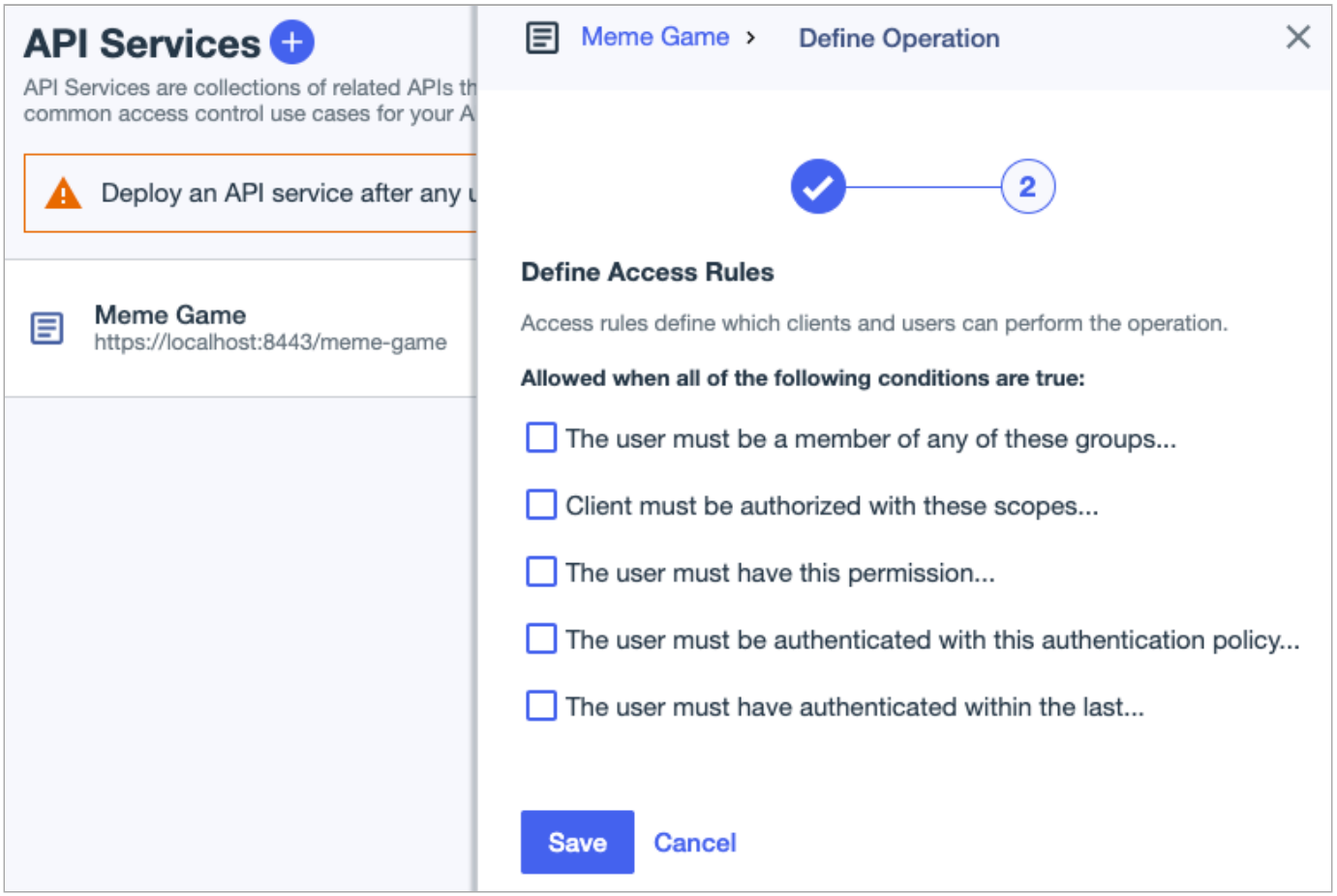


4. Click **Next**.

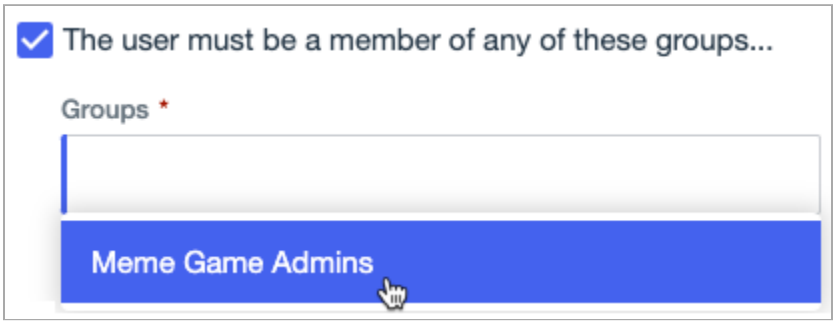
5. Define a basic rule that allows administrators to perform this operation:

   Basic rules grant access to protected operations based on factors such as group membership, authorized scopes, application permissions, the policy used for authentication, and the amount of time since authentication.

> **Note**
>
> In the next tutorial, you'll define a custom rule for an operation. Learn more about basic and custom rules in Defining operations for protected actions.



1. Select the **The user must be a member of any of these groups** check box.
2. Click **Groups**, and then select the **Meme Game Admins** group. Click outside the list of groups to close it.

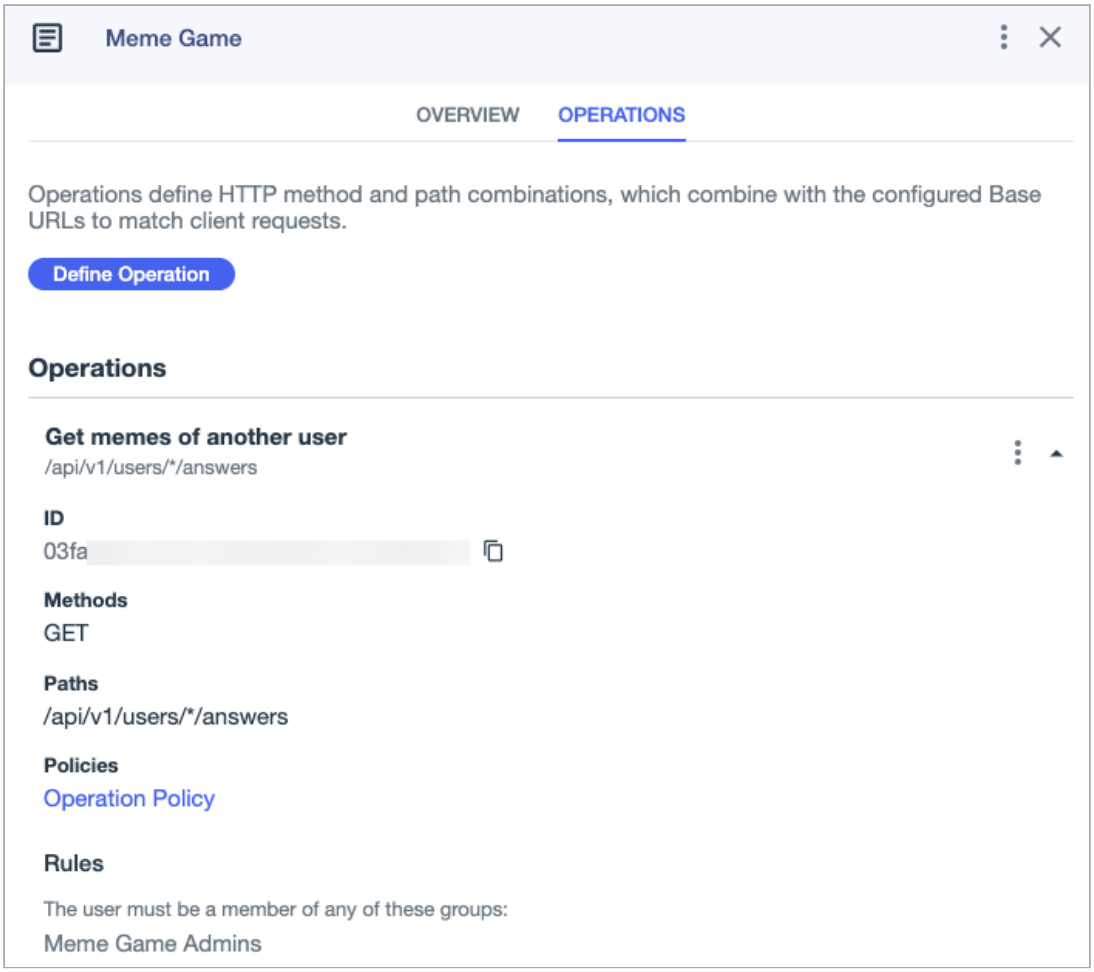


3. Click **Save**.

   Result:

   Now, only members of the **Meme Game Admins** group can call the **Get memes of another user** operation. This is what the operation looks like.

Copyright © 2025 Ping Identity Corporation



6. Click **Deploy** to deploy the new API service operation.

Result

You added an API service operation that controls access to an action and you gave members of the administrator group access to perform the action.

Next steps

Demonstrate how the API service enforces access control by allowing a request from administrators to review submitted memes and rejecting the request from players.

Getting memes of another user

Demonstrate access control for specific API operations by signing on as users with different permissions.

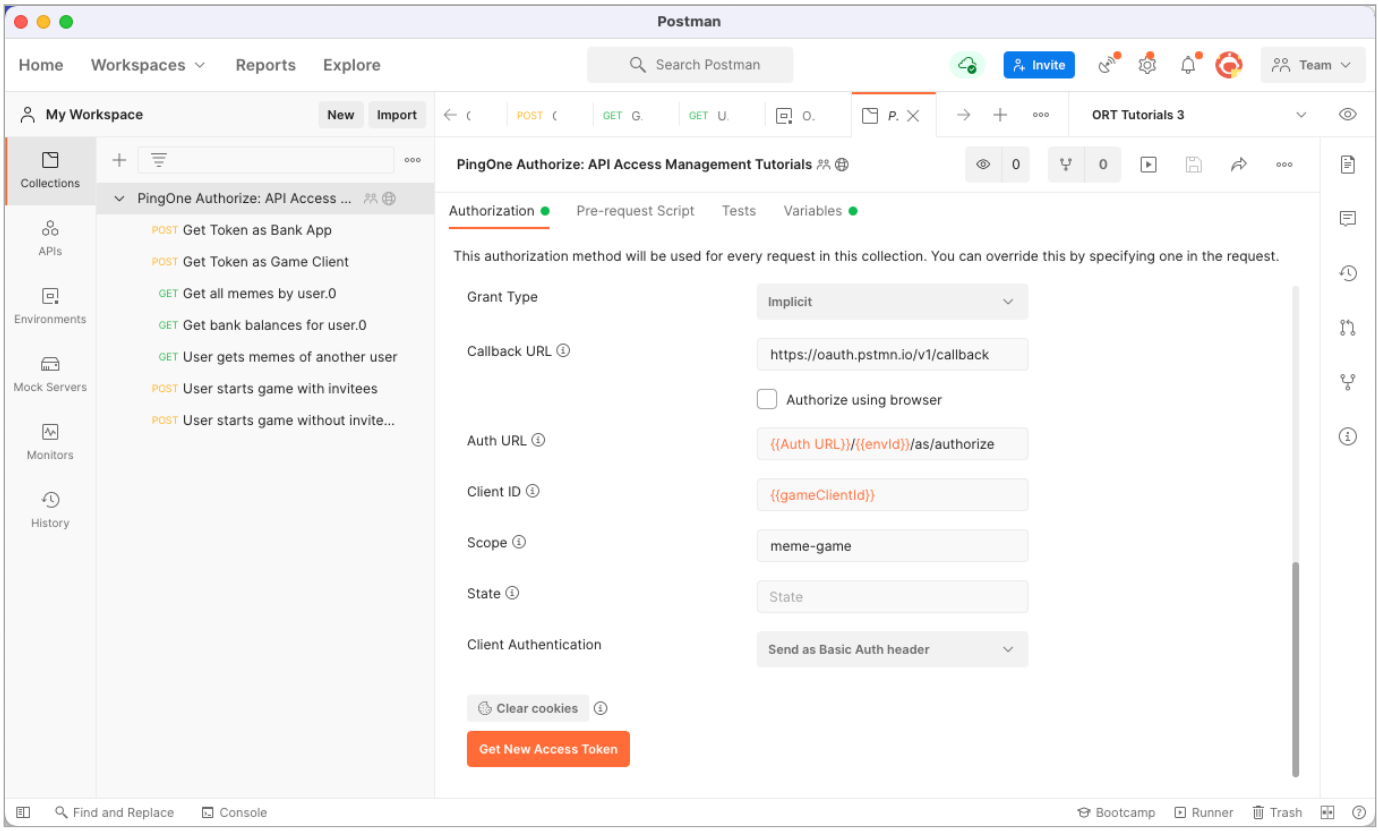
About this task

To act as a user, you'll use Postman's built-in ability to do OpenID Connect sign-on. Sign on as the game administrator and get an access token to allow Postman to act as the administrator. Then, repeat this for the game player. You'll demonstrate access control by sending a request to review submitted memes as the administrator and then as the player.

Copyright © 2025 Ping Identity Corporation

Steps

1. In Postman, go to **Collections** and click **PingOne Authorize: API Access Management Tutorials** to open the collection.



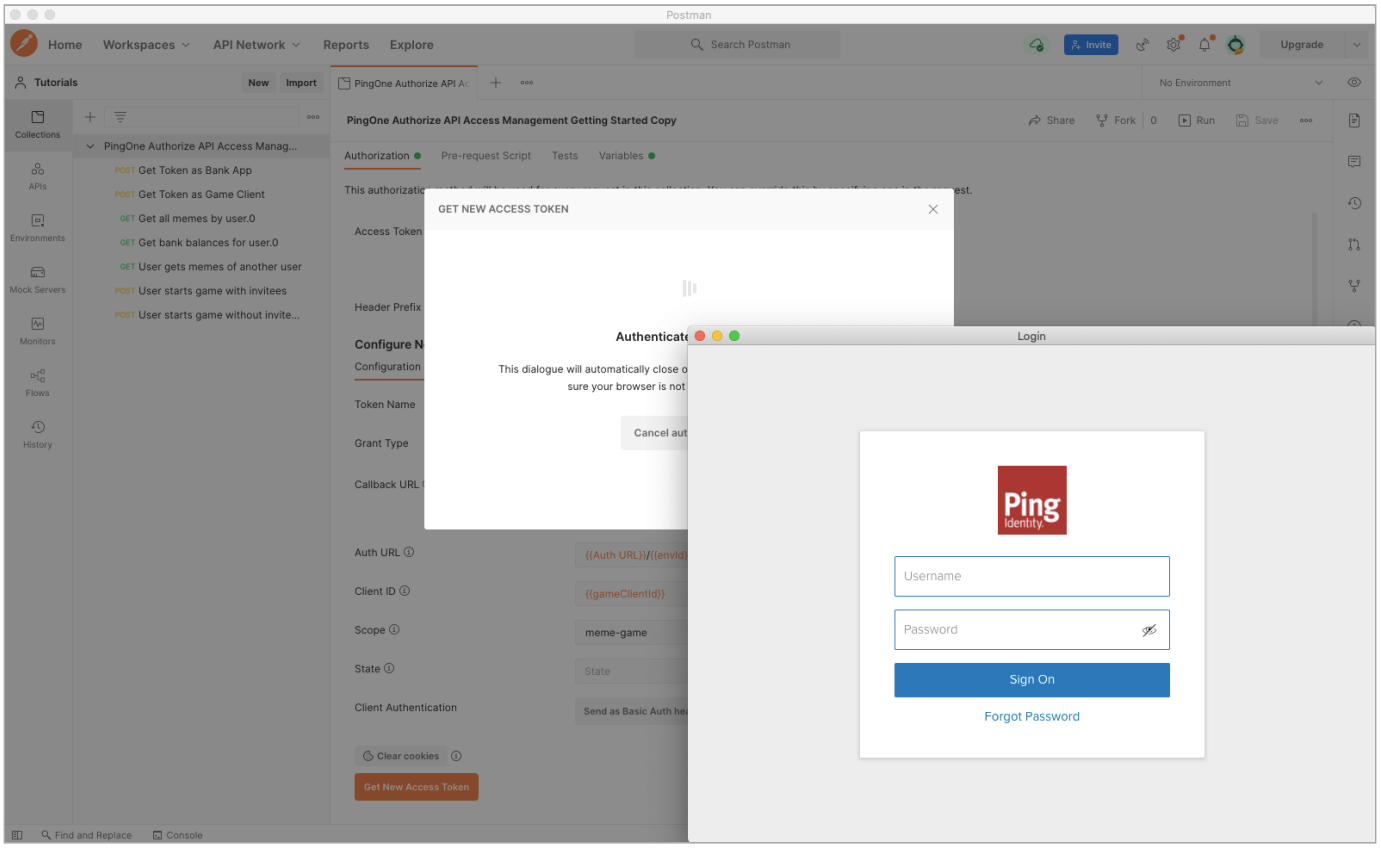
2. At the bottom of the **Authorization** tab, click **Clear cookies**.

3. Click **Get New Access Token**.

   Result:

   Postman launches the sign-on flow. You'll sign on as the gameadmin user with the password you saved earlier.

Copyright © 2025 Ping Identity Corporation



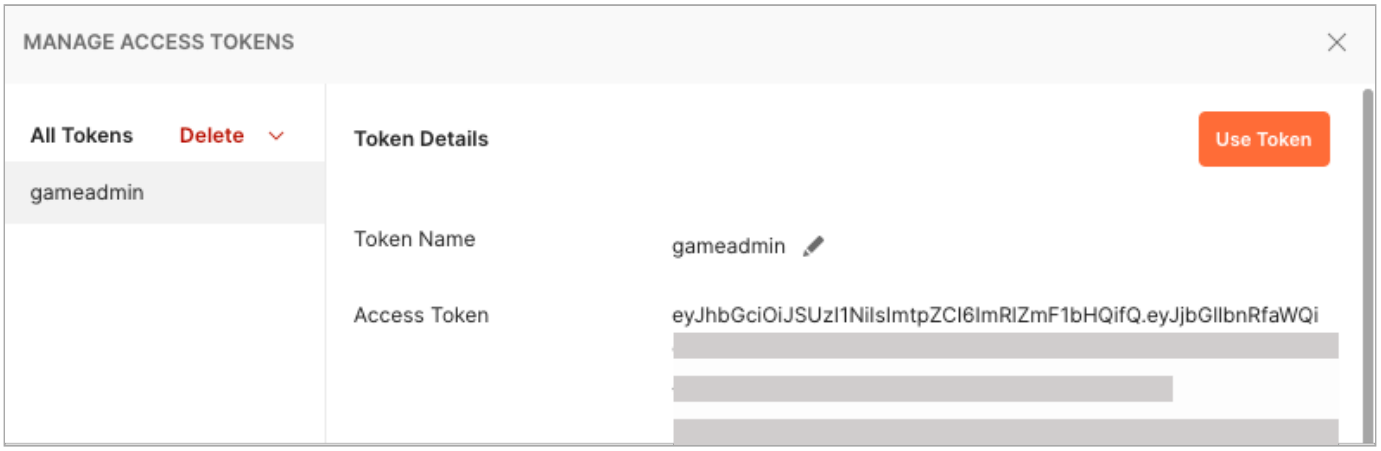
4. For the **Username**, enter `gameadmin`.
5. For the **Password**, enter the password you saved earlier. Click **Sign On**.

   Now you'll change the password for the **gameadmin** user.
6. For **Current Password**, enter the one-time password (OTP) again.
7. Enter a **New Password**, and then enter it again in **Verify New Password**.

   Copy the password to a convenient location. You'll need it to sign on later.
8. Click **Save**.
9. When authentication is complete, click **Proceed** or wait for the confirmation box to time out.
10. In **Manage Access Tokens**, click the **Pencil** icon and change the **Token Name** to `gameadmin`. Press Enter.

    This makes it easier to keep track of which user the token is for.

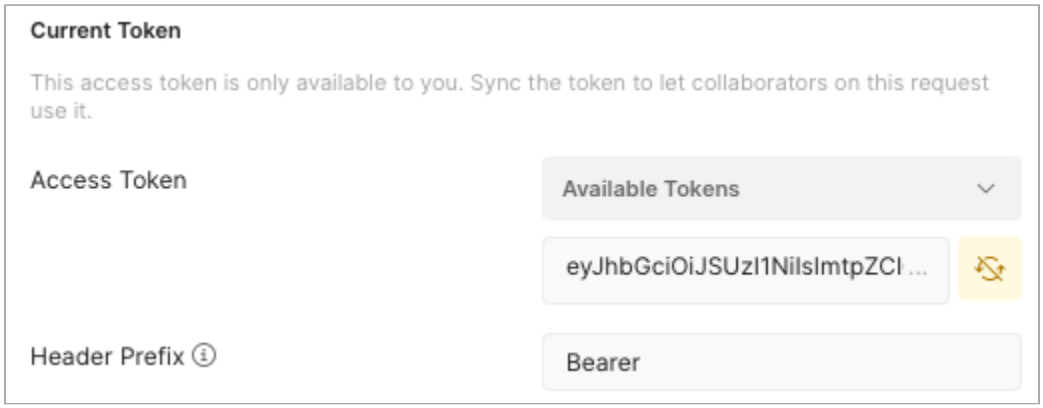
Copyright © 2025 Ping Identity Corporation



11. Click **Use Token**.

    Result:

    Now Postman has an access token to act as the gameadmin user.



    Try the request to review submitted memes as the administrator.

12. Select the **User gets memes of another user** request and click **Send**.

    Result:

    Success! You get a `200 OK` response with data in the response body.

    Now you'll get an access token to allow Postman to act as the gameplayer user.

13. To get an access token for the gameplayer user, repeat steps 1-11, with the following changes:

    1. In step 4, enter `gameplayer` for the **Username**.
    2. In step 10, change the **Token Name** to `gameplayer`.

       Result:

       Now you have an access token that allows Postman to act as the gameplayer user.

       Repeat the request to see if the player can review submitted memes

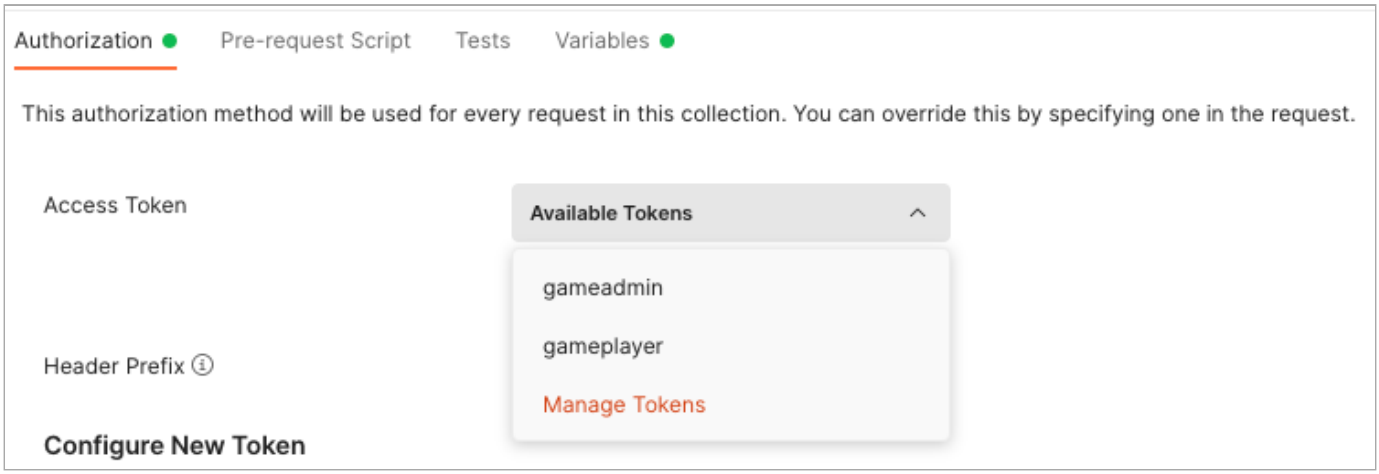
14. Select the **User gets memes of another user** request and click **Send**.

Copyright © 2025 Ping Identity Corporation

Result:

You get a `403 Forbidden` response. This demonstrates that the player can't review another user's submitted memes.

> **Tip**
>
> Because you have both tokens, you can have Postman act as the administrator or the player by selecting the corresponding token in the **Access Token** list on the **Authorization** tab.



Congratulations! You've demonstrated that only administrators can review submitted memes.

Troubleshooting:

Not getting the right results? Learn more in Viewing API Access Management events in your PingOne environment audit log.

Result

In this tutorial, you configured group-based access control for a protected API operation and demonstrated that only authorized users can perform the privileged action.

Tutorial 3: Fine-grained API authorization

Learn how to write a fine-grained custom policy in PingOne Authorize that authorizes an application interaction by comparing a combination of user attributes.

In the first tutorial, you configured PingOne Authorize and Kong Gateway to protect Meme Game APIs so that only an authorized client could access the APIs. You learned how PingOne Authorize hides the complexities of OAuth and OpenID Connect.

Now, suppose you are tasked with helping the Meme Game application team resolve a specific problem with an API. When starting a new game, the first player optionally invites other players using their email addresses. To prevent email spam, you'll create a policy that prevents a player from starting a new game with other players if the first player's email address comes from a generic domain.

In this custom policy, you'll authorize a specific application interaction by comparing a combination of attributes, in this case, the first player's email address and the invitee list. As with many custom policies, the business driver for this policy comes from outside the application team, specifically, the need to reduce email spam that impacts your organization's mail reputation.

Copyright © 2025 Ping Identity Corporation

Before you begin

Make sure:

- PingOne SSO and PingOne Authorize are in your PingOne environment. For more information, see Getting started with PingOne Authorize.
- You've completed Tutorial 1: Controlling access to APIs managed by an API service to set up the environment you need for this tutorial.

What you'll learn

You'll learn how to:

- Author custom policies for API operations
- Use user attributes in policies
- Extract attributes from API request bodies and use them in policies
- Test policies
- Examine recent decisions

What you'll do

Follow these steps to complete the tutorial:

- Add Meme Game users in PingOne.
- Define an API operation that requires custom policies.
- Add an attribute for the game invitee list.
- Create and test a policy that checks specific conditions for the API operation.
- Test the end-to-end use case using Postman.

Adding users for the Meme Game

Learn how to add users in PingOne with attributes you can use in policies.

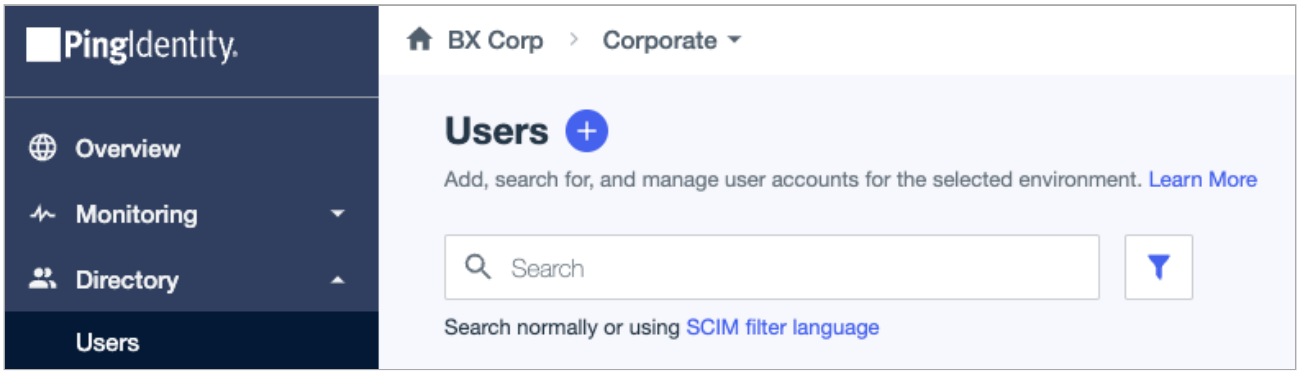
About this task

Before you create and test a policy that authorizes the conditions under which a user can start a new game, you'll need sample users for testing. Create a test user with an email address from a generic domain and another test user with an email address from a trusted domain.

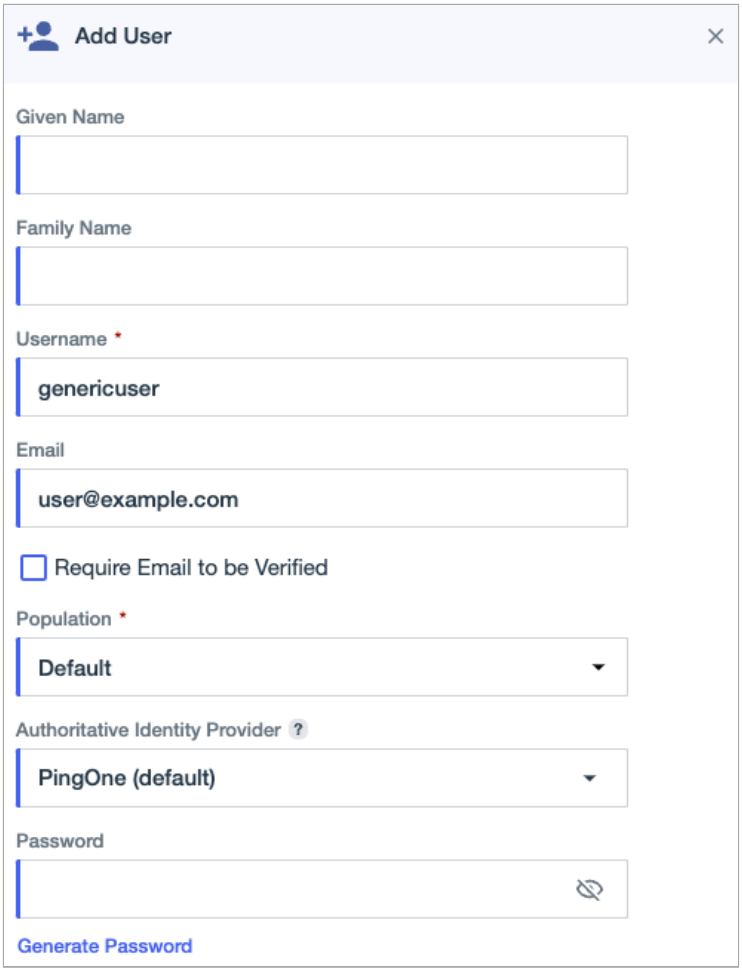
Steps

1. Add a user with an email address from a generic domain:
    1. In PingOne, go to **Directory** > **Users** and click the **+** icon next to **Users**.

Copyright © 2025 Ping Identity Corporation



2. For **Username**, enter `genericuser`.
3. For **Email**, enter `user@example.com`.
4. For **Population**, select **Default**, if it is not already selected.



5. Click **Generate Password**, then click the **Eye** icon and copy the password to a convenient location. You'll need it later.
6. Click **Save**.

Copyright © 2025 Ping Identity Corporation

2. Add a user with an email address from a trusted domain:
    1. Click the + icon next to **User**.
    2. For **Username**, enter `companyuser`.
    3. For **Email**, enter `example@pingidentity.com`.
    4. Make sure the **Population** is **Default**.
    5. Click **Generate Password**, then click the **Eye** icon and copy the password to a convenient location. You'll need it later.
    6. Click **Save**.

Result

You've added two users with email addresses from different domains. You'll use them later when testing your policy.

Next steps

Next, you'll define the API operation that requires a fine-grained authorization policy.

Defining an API operation that uses fine-grained policies

Learn how to add an operation that will use fine-grained custom policies in PingOne Authorize for access control.

About this task

Custom authorization policies in PingOne Authorize enable you to add more advanced API access rules that might require several iterations of configuration and testing before deployment. Custom policy authoring supports fine-grained logic and an iterative workflow.

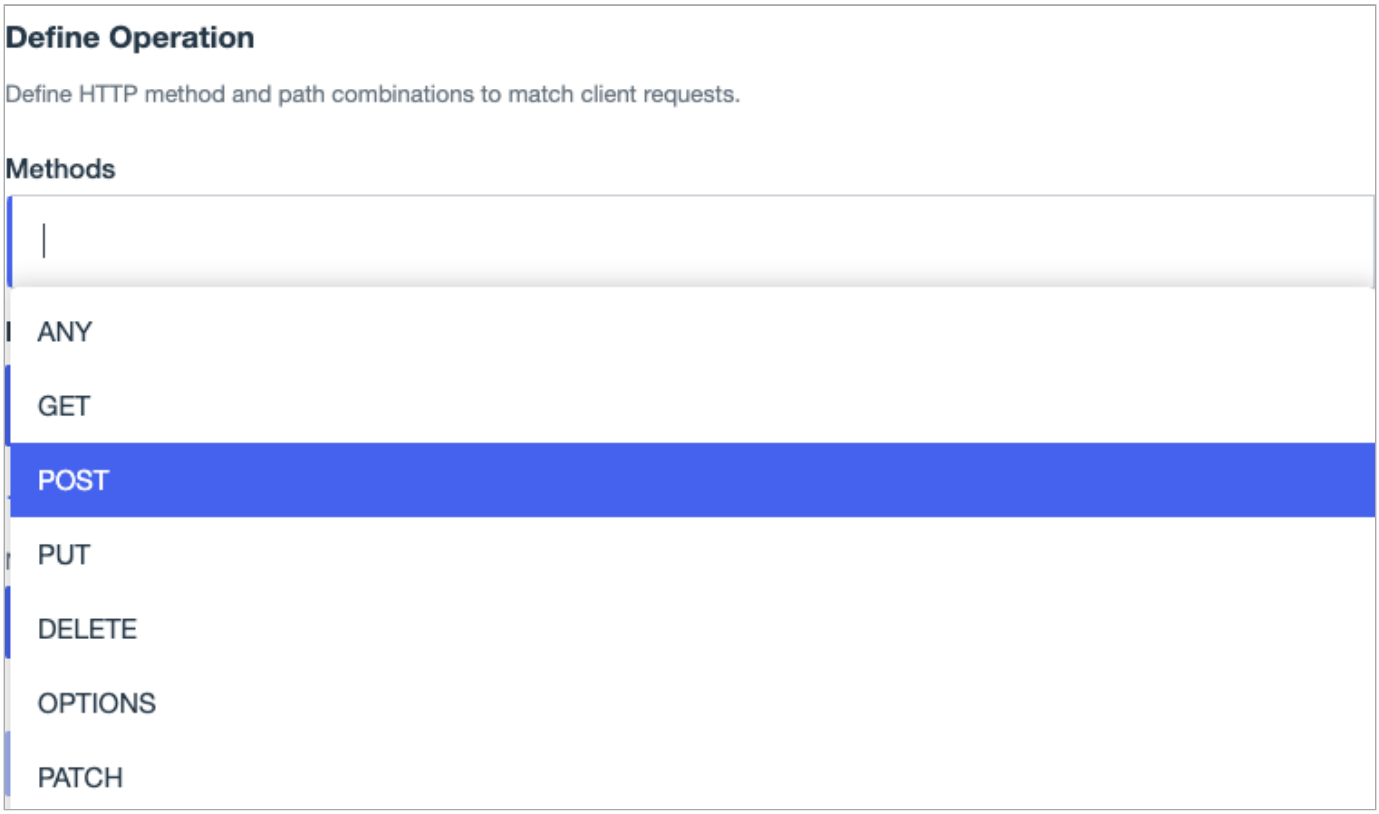
When you added the **Meme Game** API service in Tutorial 1: Adding a managed API service for the Meme Game in PingOne, you enabled custom policies for the API service. In this task, you'll create an API operation for the **Meme Game** API service that matches the API request used to start a new game. You'll create the custom policy in a later task.

Steps

1. In PingOne, go to **Authorization > API Services**.
2. Click the **Meme Game** API service, and then click the **Operations** tab.
3. Click **Define Operation** to create a new operation.

   First, define the operation by configuring a method and path combination that matches a client request to the API.
4. Click **Methods**, and then select the POST method. Press tab or click outside the list of methods to close it.

Copyright © 2025 Ping Identity Corporation



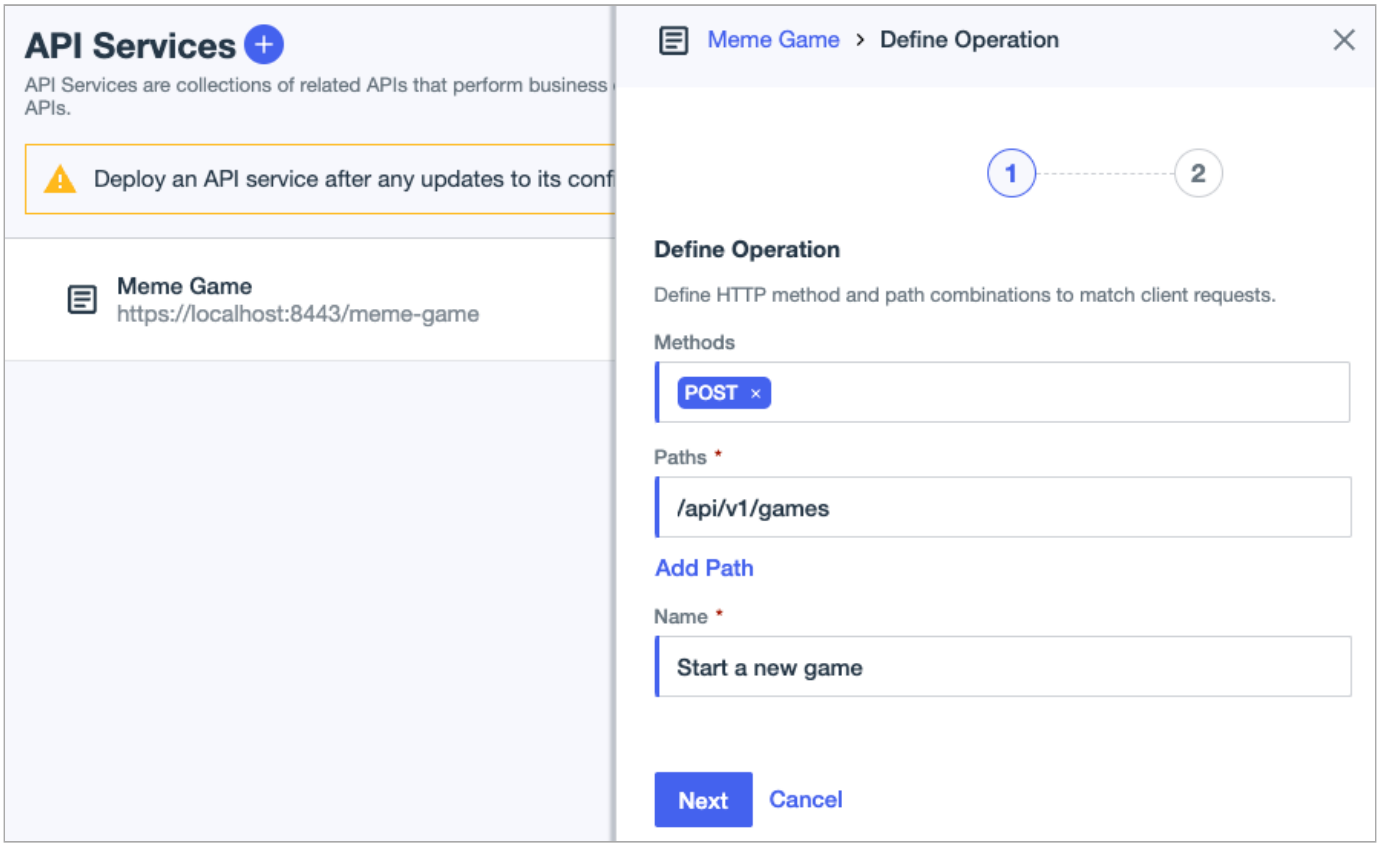
5. For **Paths**, enter the following:

   `/api/v1/games`

   This is the API path for starting a new game. The path must start with a slash (/).

6. For **Name**, enter `Start a new game`.

Copyright © 2025 Ping Identity Corporation



7. Click **Next**, and then click **Save**.

Result

You've defined an API operation that matches the API request used to start a new game.

Next steps

Next, you'll add attributes in the **Trust Framework** for your policy logic.

Adding a game invitee list attribute

Learn how to use the **Trust Framework** to add an attribute for the invitee list of other game players.

About this task

To create a policy that meets your business requirements, you'll need two attributes:

- To determine whether the user's email address comes from a generic domain, you'll use the built-in PingOne user **email** address attribute for the user authenticated to the application.
- To determine whether the user is inviting others to play the Meme Game, you'll create an attribute in the **Trust Framework** for the invitee list of other game players. You'll extract the invitee list from the API request body.

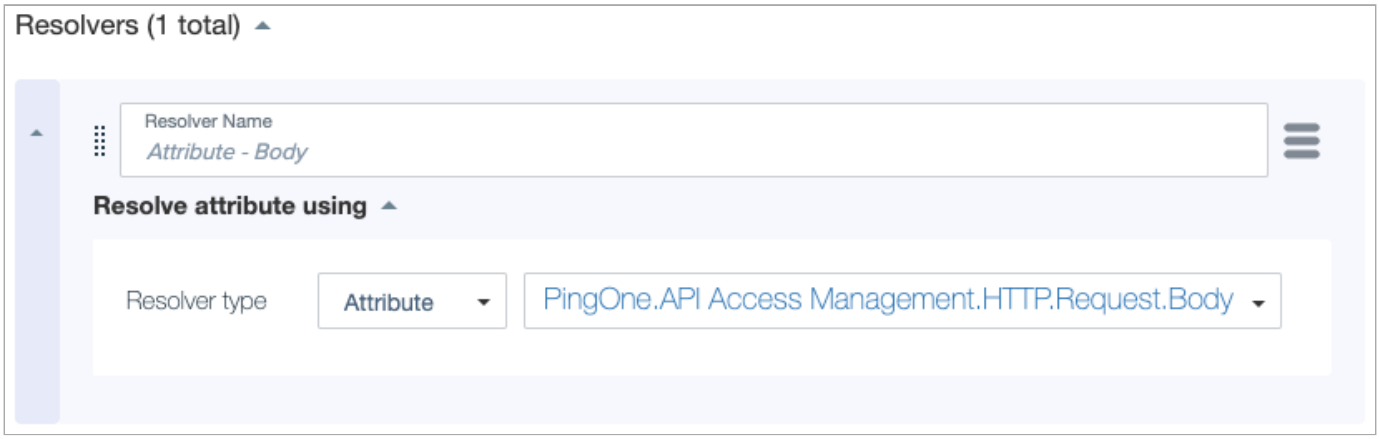
Steps

1. In PingOne, go to **Authorization > Trust Framework** and click the **Attributes** tab.

Copyright © 2025 Ping Identity Corporation

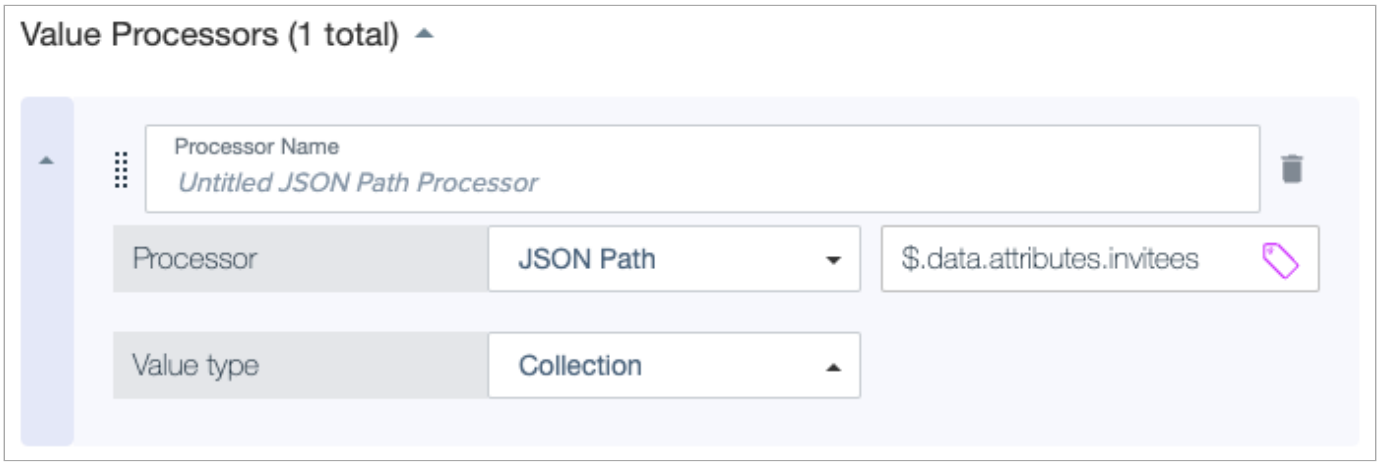
2. Click the + icon and select **Add new Attribute**.
3. For the attribute **Name**, enter `New game invitee list`.
4. Verify that there is no **Parent** selected. If a parent exists, click the **Delete** icon to remove it.
5. In the **Resolvers** section, click **+ Add Resolver**.
6. For the **Resolver Type**, select **Attribute**.
7. For **Select an attribute**, select **PingOne → API Access Management → HTTP → Request → Body**.

   This resolver returns the decision request body. For more information, see Resolvers.



8. Click **Value Processors** and then click **+ Add Processor**.
9. Make sure the **Processor** type is **JSON Path**.
10. Enter `$.data.attributes.invitees` in the input box for the JSON Path **Processor**.
11. For **Value Type**, select **Collection**.

    This processor extracts the invitee list from the decision request body. For more information, see Processors.



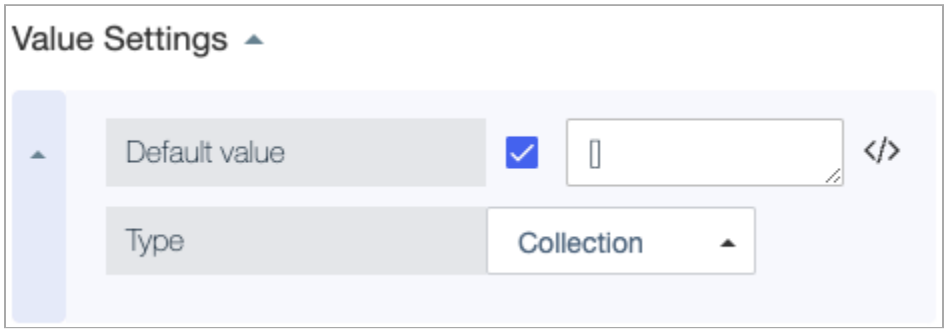
12. For **Value Settings**:

    1. Select the **Default value** check box, and then enter open and closing brackets ([]) for the default value.

Copyright © 2025 Ping Identity Corporation

This sets the default value to an empty collection, ensuring that the attribute resolves successfully if the invitee list is empty. For more information, see Value settings.

2. For the **Type**, select **Collection**.



13. Click **Save Changes**.

Result

You've added an attribute in the **Trust Framework** for the invitee list of other game players.

Next steps

Next, you'll put everything together in a custom policy that authorizes the specific conditions under which a user can start a game.

Adding a policy for the API operation

Learn how to add and test a custom policy in PingOne Authorize that uses API attributes.

About this task

It's time to put the previous steps together into a policy that addresses your business requirements. So far, you've defined an API operation that matches API requests used to start a new game, you have a built-in attribute for the authenticated user's email address, and you've created an attribute in the **Trust Framework** for the invitee list of other game players. Now, you'll create and test a policy that compares these three components to authorize the specific conditions under which a user can start a game.

Your business requirements:

- A user from a generic domain can play the game alone, to see how it works.
- A user from a generic domain cannot invite others to play with them.
- A user from a non-generic domain can play with or without inviting other players.

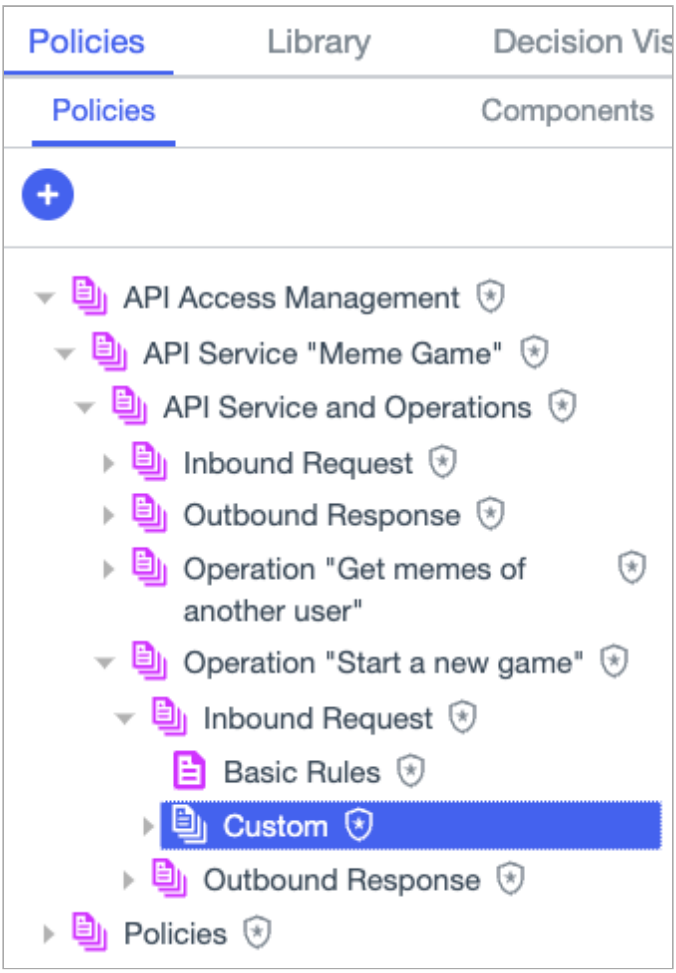
Steps

1. Add a policy that targets the API used when users start a new game:
    1. In PingOne, go to **Authorization > API Services** and click **Meme Game**.
    2. On the **Operations** tab, expand the **Start a new game** operation and copy the **ID** to a convenient location.

       You'll use it later for policy testing.
    3. Go to **Authorization > Policies**.

Copyright © 2025 Ping Identity Corporation

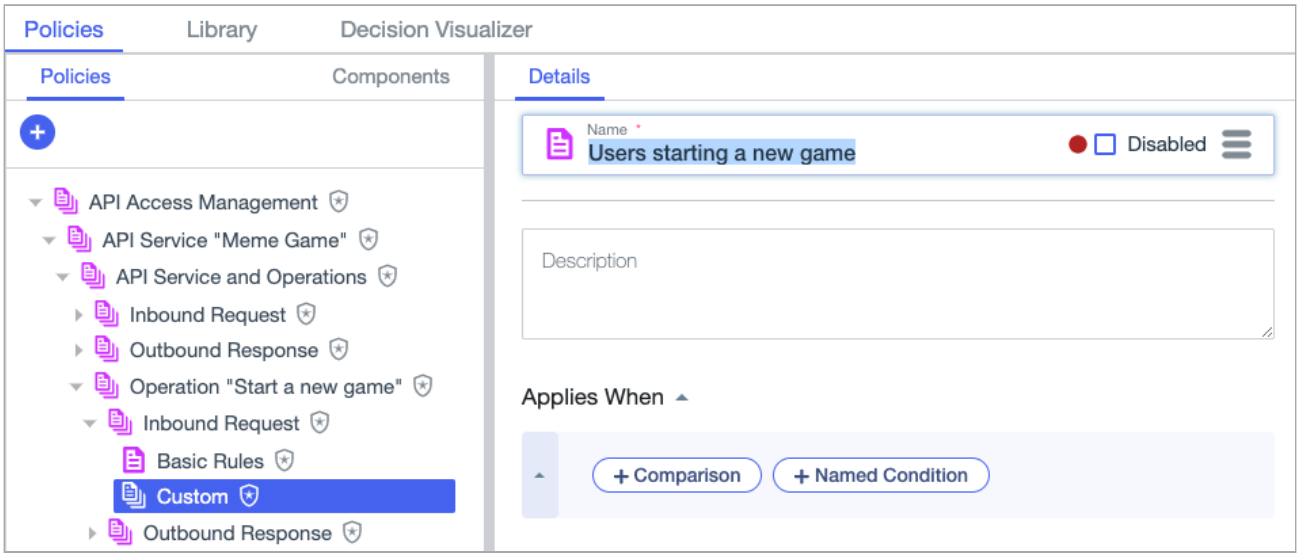
4. In the **API Access Management** policy set, select the **Inbound Request → Custom** policy set for the **Start a new game** operation.



This is where you add custom policies that target inbound requests for the API operation. The **Custom** policy set is owned by its parent operation, so there are restrictions around updating, moving, or deleting it, but you can add your own child policies.

5. Click the **+** icon and select **Add Policy**.

6. For the policy **Name**, enter `Users starting a new game`.



2. For the **Combining Algorithm**, select **Unless one decision is permit, the decision will be deny**.

   This ensures that only the specific combinations of attributes that the policy checks will be allowed to start a game. All other combinations will be denied.

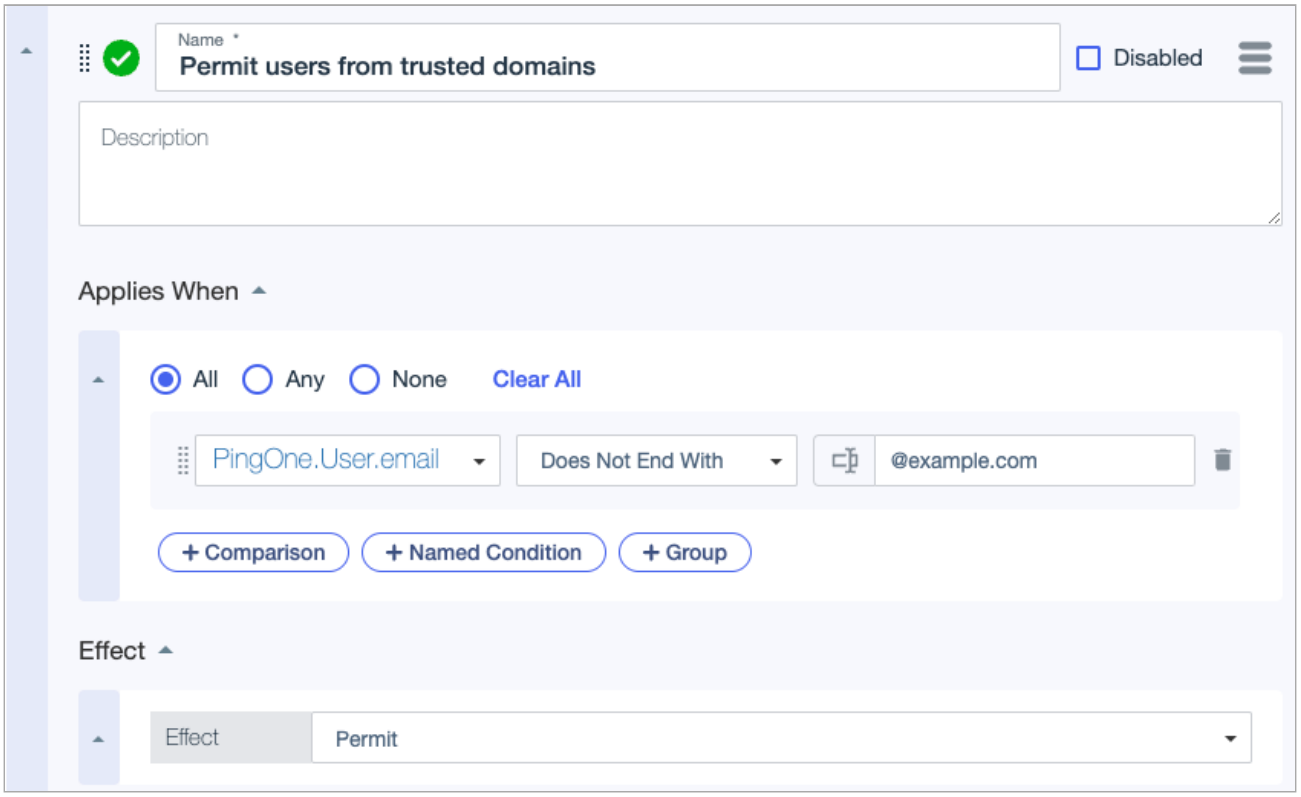
   Next, add rules to check whether the user's email address is from a generic domain.

   > **Note**
   >
   > To simplify this tutorial, you'll assert that the generic domain is example.com. In a real use case, you would use Authorization services in the **Trust Framework** to periodically obtain a current list of generic email domains.

3. Add a rule that permits users from non-generic domains:

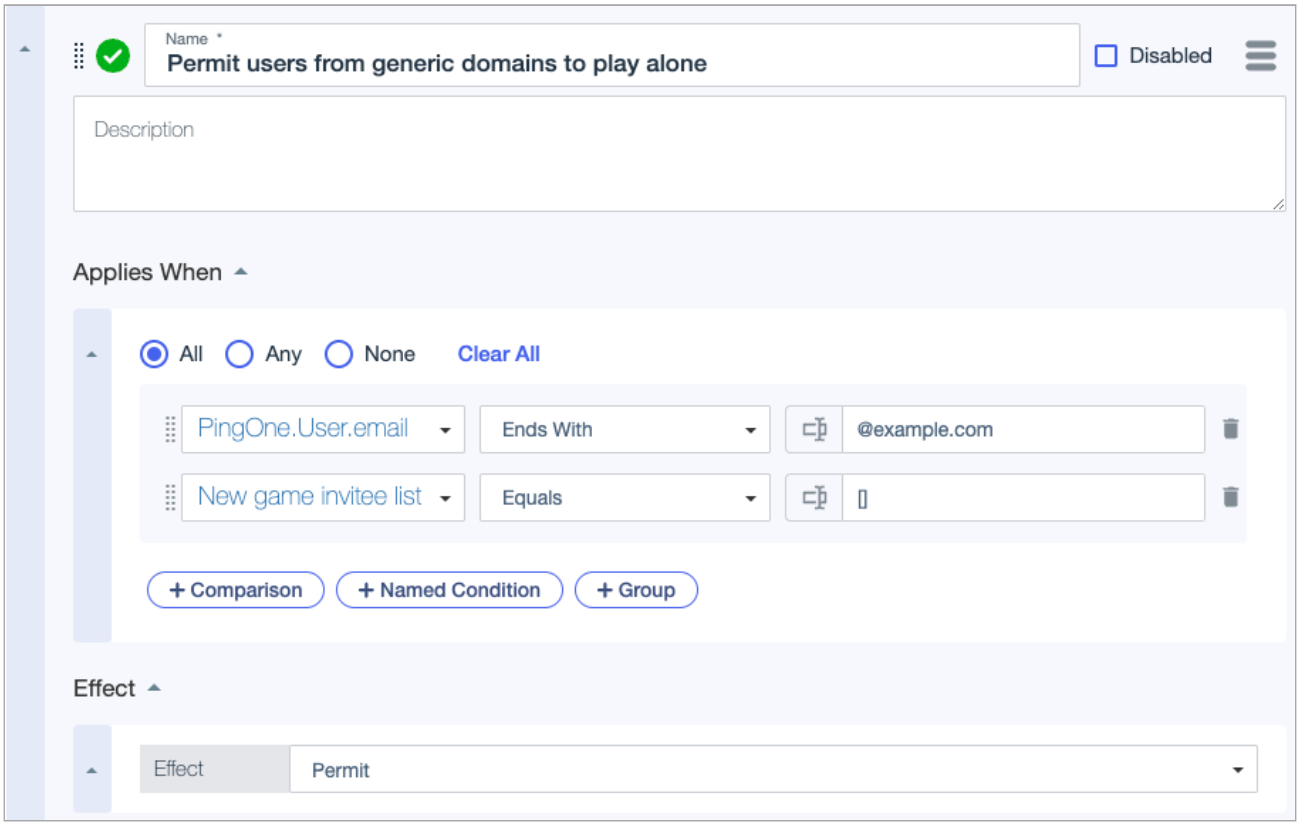
   1. Click **+ Add Rule**.
   2. For the rule **Name**, enter `Permit users from trusted domains`.
   3. Click the hamburger menu next to the **Name** field and select **Add "Applies When"**.
   4. In the **Applies When** section, click **+ Comparison**.
   5. In **Select an Attribute**, select **PingOne.User.email** (this is a built-in PingOne user attribute).
   6. For the comparator, select **Does Not End With**.
   7. For the constant, enter `@example.com`.

Copyright © 2025 Ping Identity Corporation



4. Add a rule that permits users from generic domains, but only if they play alone:
    1. Click **+ Add Rule**.
    2. For the rule **Name**, enter `Permit users from generic domains to play alone`.
    3. Click the hamburger menu next to the **Name** field and select **Add "Applies When"**.
    4. In the **Applies When** section, click **+ Comparison**.
    5. In **Select an Attribute**, select **PingOne.User.email**.
    6. For the comparator, select **Ends With**.
    7. For the constant, enter `@example.com`.
    8. To add another comparison, click **+ Comparison**.
    9. In **Select an attribute**, select **New game invitee list** (this is an attribute you created earlier).
    10. For the comparator, use the default **Equals**.
    11. For the constant, enter open and closed square brackets to signify an empty list with no invitees, `[]`.

Copyright © 2025 Ping Identity Corporation



12. Click **Save changes**.

    Next, you'll test the policy using testing features in **Policies**. The **Testing Scenario** defines a decision request and optional attribute and service overrides to serve as input for a test. Overrides let you test combinations of attributes without having to concern yourself with how the attributes are resolved at runtime. For example, you can test different values for the invitee list without having to form a properly formatted API request body.

5. Test the policy for the four combinations of users and invitees:

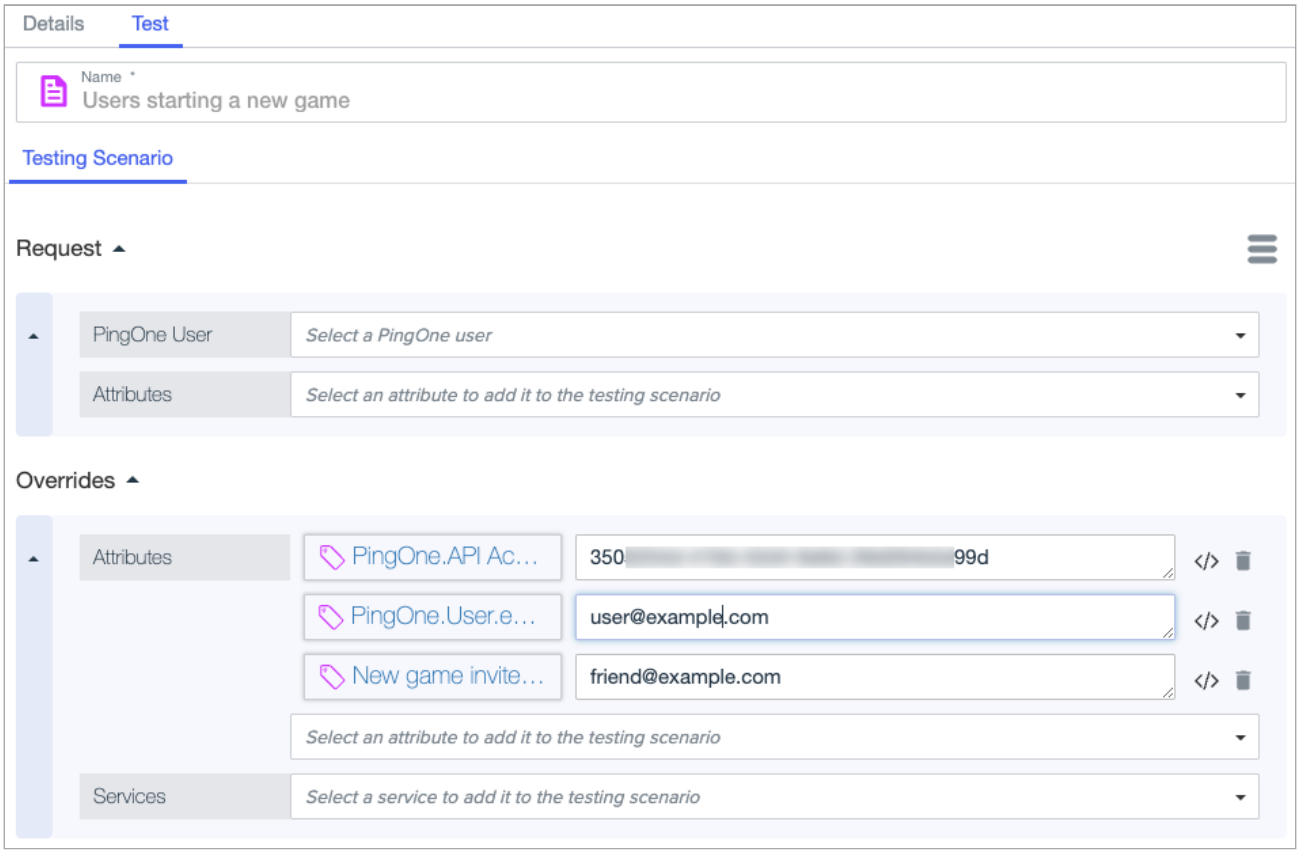
    1. Click the **Test** tab.

    2. In **Overrides**, for **Attributes**, select **PingOne → API Access Management → Operation → ID** and enter the same operation ID that you copied in step 1b.

    3. For the next attribute, select **PingOne.User.email** and enter the value `user@example.com`.

    4. For the last attribute, select **New game invitee list** and enter the value `friend@example.com`.

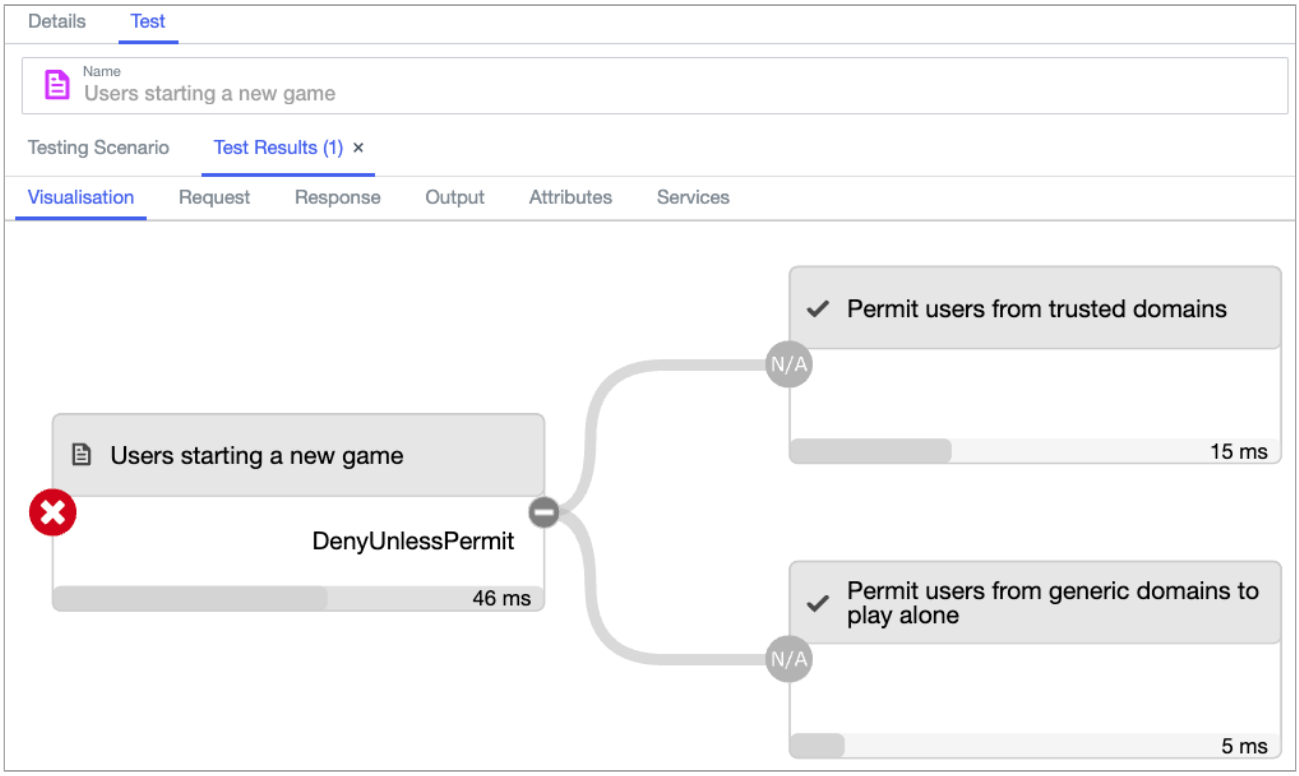
Copyright © 2025 Ping Identity Corporation



5. Click **Execute**.

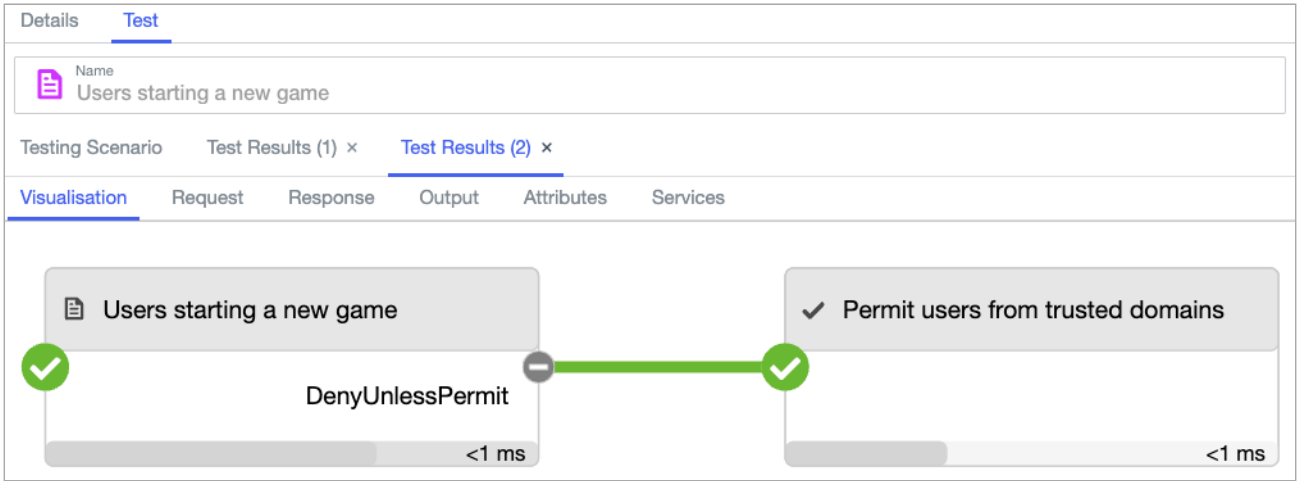
   Because neither rule evaluated as true, the policy resulted in a deny decision. This is the expected result because a user from a generic domain cannot invite others to their game. You can examine additional details for test results on the other tabs.

Copyright © 2025 Ping Identity Corporation



6. Repeat the test using different combinations of **PingOne.User.email** and **New game invitee list**.

   All other combinations should result in permit decisions. For example, change **PingOne.User.email** to `user@google.com` and the test will result in a permit decision, because the email address no longer has a generic domain.



   Now that you've tested your policy, it's ready to publish. You'll deploy the Meme Game API service to publish the latest version of the policy tree.

6. Go to **Authorization → API Services** and select the **Meme Game** API service.

7. Click **Deploy**.

Result

Copyright © 2025 Ping Identity Corporation

Your policy uses rules that compare the user's email address to the invitee list of other game players to meet requirements for the conditions under which a user can start a new game.

Next steps

Next, you'll test the end-to-end use case for starting new games by using Postman to simulate API requests from the Meme Game application.

Testing the end-to-end use case with Postman

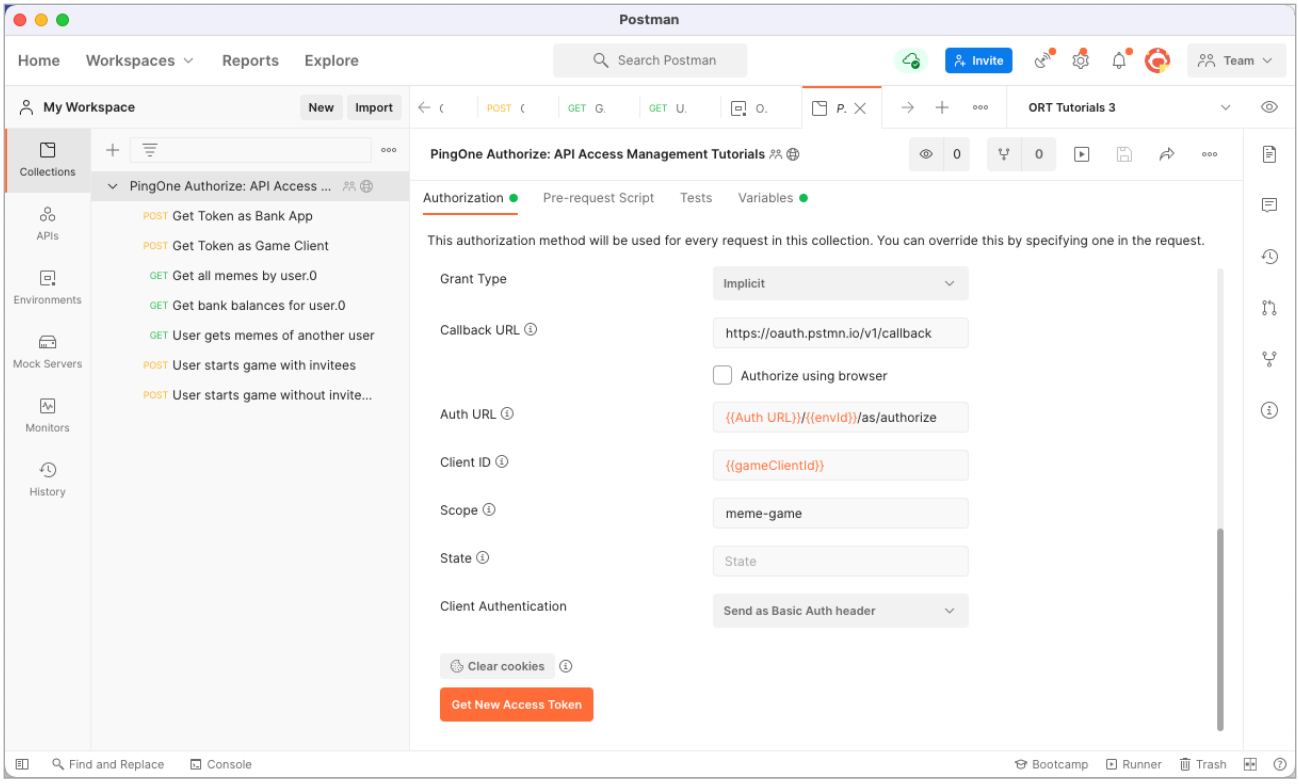
Learn how to test user access to the Meme Game by simulating API requests with Postman.

About this task

You'll use Postman to simulate a user authenticating to the game application and making API requests to start a new game. You'll demonstrate that the user whose email address comes from a generic domain is not allowed to start a game while inviting others, but they are allowed to start a game when playing by themselves. You'll also demonstrate that the user with an email address from a trusted domain is allowed to start games with or without inviting others.

Steps

1. Sign on as **genericuser**:
    1. In Postman, go to **Collections** and click **PingOne Authorize: API Access Management Tutorials** to open the collection.

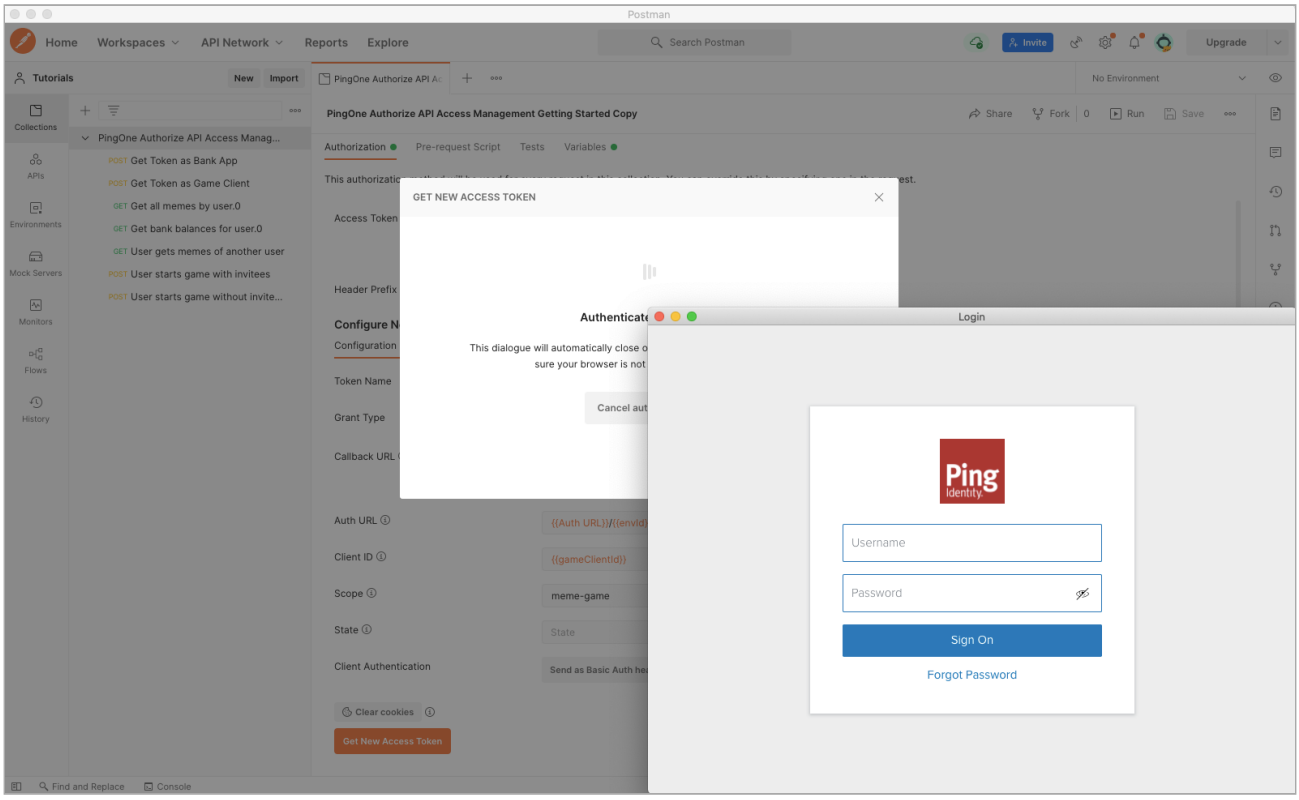


    2. At the bottom of the **Authorization** tab, click **Clear cookies**.
    3. Click **Get New Access Token**.

Copyright © 2025 Ping Identity Corporation

Result:

Postman launches the sign-on flow. You'll sign on as **genericuser** with the password you saved earlier.



4. For the **Username**, enter `genericuser`.
5. For the **Password**, enter the password you saved earlier. Click **Sign On**.

   Now, you'll change the password for **genericuser**.

6. For **Current Password**, enter the one-time passcode (OTP) again.
7. Enter a **New Password**, and then enter it again in **Verify New Password**.

   Copy the password to a convenient location. You'll need it to sign on later.

8. Click **Save**.
9. When authentication is complete, click **Proceed** or wait for the confirmation box to time out.
10. In **Manage Access Tokens**, click the **Pencil** icon and change the **Token Name** to `genericuser`. Press Enter.

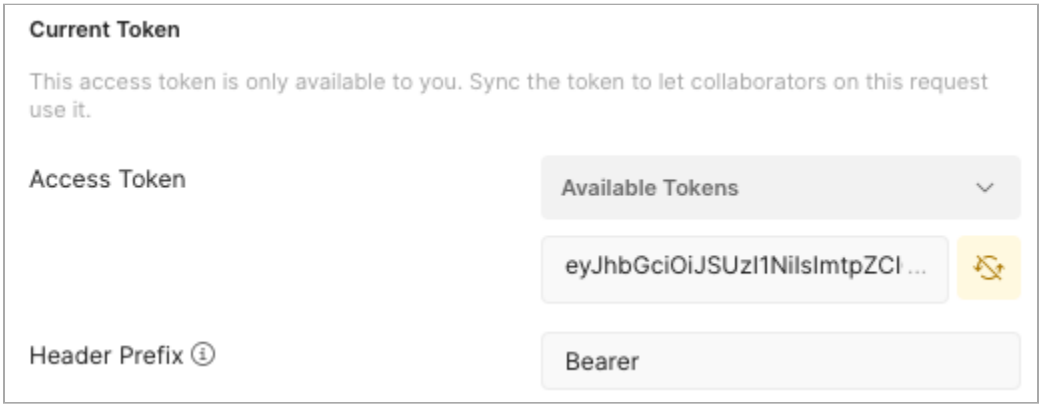
    This makes it easier to keep track of which user the token is for.

Copyright © 2025 Ping Identity Corporation

11. Click **Use Token**.

    Result:

    Now Postman has an access token to act as `genericuser`.



    Now, try to start games with and without invitees.

2. Select the **User starts game with invitees** request and click **Send**.

   Result:

   You get a `403 Forbidden` response. This demonstrates that a user whose email address is from a generic domain is not allowed to invite others to new games.

3. Select the **User starts game without invitees** request and click **Send**.

   Result:

   Success! You get a `201 Created` response with data in the response body. This demonstrates that a user whose email address is from a generic domain is only allowed to play the game by themselves.

   Now, you'll get an access token to allow Postman to act as **companyuser**.

4. To get an access token for **companyuser**, repeat step 1, with the following changes:

   1. In step 1d, enter `companyuser` for the **Username**.
   2. In step 1j, change the **Token Name** to `companyuser`.

Copyright © 2025 Ping Identity Corporation

Result:

You have an access token that allows Postman to act as the **companyuser**.

Repeat the requests to see if the user can start games and invite others.

> **Note**
>
> The meme-game.com API does not send invitation emails or store the email addresses of the invited list of users. Regardless, never send real email addresses in your testing with this API.

5. Select the **User starts game with invitees** request and click **Send**.

   Result:

   Success! You get a `201 Created` response.

6. Select the **User starts game without invitees** request and click **Send**.

   Result:

   Success! You get a `201 Created` response.

Result

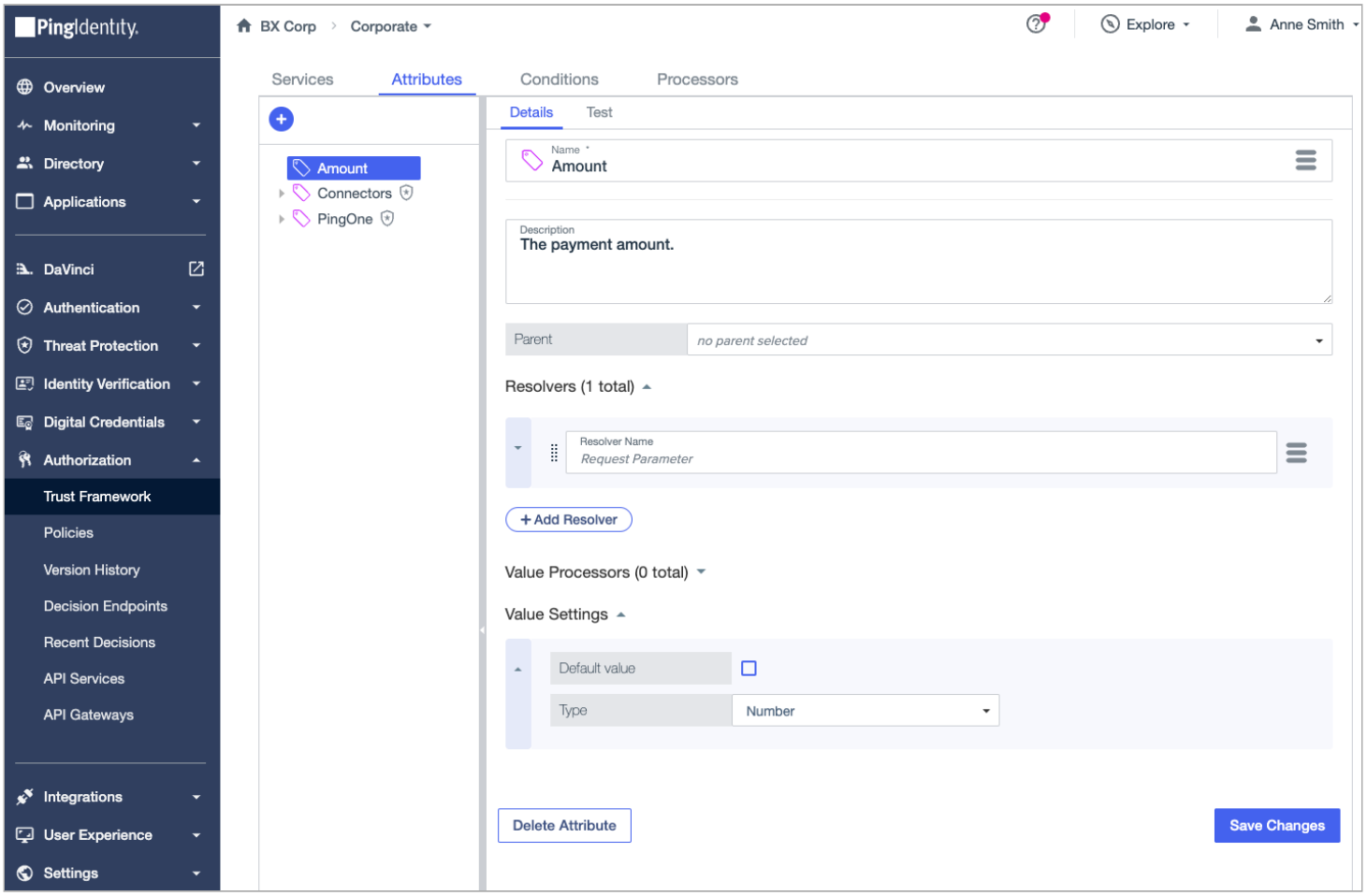
Congratulations! You created a custom authorization policy that meets your business requirements and you tested the policy.

Trust Framework

The PingOne Authorize **Trust Framework** is where you define the building blocks used in policies and access control decisions.

The **Trust Framework** provides an enterprise-wide view of your data and service ecosystem. It's where your organization's technical people capture definitions for digital assets, services, and users across all domains in your organization.

Copyright © 2025 Ping Identity Corporation



When you define these resources with business-friendly names, policy authors can use them in policies without worrying about how the underlying information is retrieved and populated.

Organize elements in the **Trust Framework** hierarchically in tree structures. You can branch the tree for each type of element up to 20 levels deep.

> **Note**
>
> You can define up to 4000 objects in each environment. This limit includes elements in the **Trust Framework** and also policies and rules. System-owned objects do not contribute to this limit.

Authorization attributes

PingOne Authorize attributes provide contextual information that informs fine-grained dynamic authorization decisions.

Attributes, like variables, have a name and store a value. Attribute values come from many sources, including:

- Constants defined in the **Trust Framework**.
- Information points that provide the decision point with information. These data sources, modeled as services in PingOne Authorize, are sometimes referred to as Policy Information Points (PIPs).

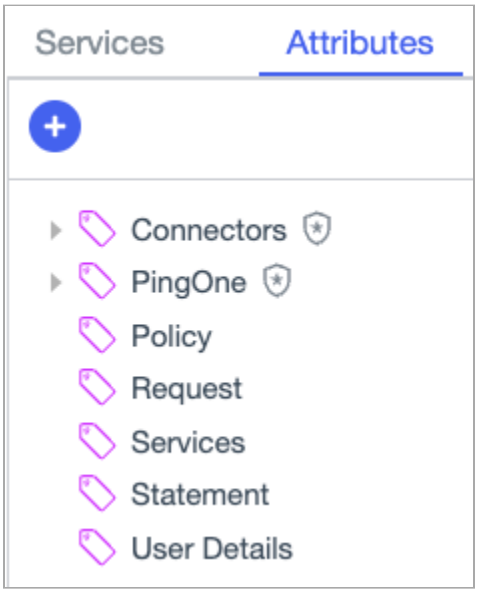
Copyright © 2025 Ping Identity Corporation

- Decision requests that package information coming from your application. For example, an attribute might correspond to an element of an HTTP request, such as the access token subject.
- JSON schema properties defined in another attribute.

Attribute hierarchy

Group attributes under parent attributes organized hierarchically in a tree structure. A simple and consistent structure can help your organization understand, update, and debug the **Trust Framework**.

In addition to the built-in **Connectors** and **PingOne** parent attributes, you might want to create parents for attributes used in policies, attributes that retrieve information from requests and services, attributes used in statements, and attributes that provide user details. You can also group attributes based on the decision flows they're used in, the actions they facilitate, and the teams that are responsible for them.



> **Note**
>
> You can define up to 4000 objects in each environment. This limit includes attributes and other elements in the **Trust Framework**. System-owned objects do not contribute to this limit.

Attribute components

You can use the following components in attributes. For more information, see Adding an authorization attribute.

Resolvers

Resolvers define source values for attributes. PingOne Authorize comes with built-in attributes that resolve PingOne identity and service information. Generated attributes resolve against other attributes to automatically extract properties from parent attributes.

Using a pull model, the decision point resolves attribute values only when they're needed during policy evaluation.

Copyright © 2025 Ping Identity Corporation

Processors

You can make the original value of an attribute available for use in policies, or you can manipulate the value using processors that convert an attribute value to a different format or extract a specific part of it, such as a specific part of an HTTP response.

You can use the transformed value in other attributes and in named conditions.

Value settings

Attributes have value settings that define the data type of the attribute and an optional default value.

Attribute testing

You can test attributes to validate their output values.

Adding an authorization attribute

Add attributes to provide data used in authorization policies and decision evaluations.

Before you begin

Consider how you will structure attributes in the **Attributes** tree and the naming conventions that you'll use.

About this task

> **Tip**
>
> Policy authors need to be able to build and manage policies without a deep understanding of the complex underlying data endpoints and data manipulation. When you add attributes, give them names that business users and policy authors will understand.

Steps

1. Add a new attribute:
    1. Go to **Authorization > Trust Framework** and click the **Attributes** tab.
    2. Click the **+** icon and select **Add new Attribute**.
2. Define general information for the attribute:
    1. Enter a unique **Name** for the attribute.

       To ensure that PingOne Authorize can resolve attribute references, the following characters are not allowed in the name:

       - Period (.)
       - Curly brackets ({ })
       - Pipe (|)
    2. For **Description**, enter information that describes the attribute's purpose.

Copyright © 2025 Ping Identity Corporation

The description is only visible on the **Attributes** tab, but it can help policy authors understand how to use the attribute in policies.

3. **Optional:** To nest the attribute under a parent attribute in the tree, select a **Parent** attribute.

   Nesting helps group related attributes together. You can move an attribute to another location in the tree by selecting a different parent attribute. To remove nesting, click the **Delete** icon and leave the **Parent** list blank.

3. **Optional:** Add resolvers that define where the attribute pulls information from.
4. **Optional:** Add value processors that transform the attribute's value.
5. **Optional:** Add value settings that define the attribute's data type and default value.
6. Click **Save changes**.

> **Note**
>
> You can copy an attribute for reuse by selecting **Make Copy** from the hamburger menu of that attribute. You cannot copy a portion of an attribute definition, with the exception of resolvers. You must copy the whole attribute definition to duplicate any of its content or manually copy the content between definitions.
> If you copy an attribute with child attributes, only the parent is duplicated.

Next steps

After you save the attribute, you can optionally add repetition settings that resolve the attribute's values from a collection.

Adding resolvers to an attribute

Optionally, add resolvers to define where an attribute pulls information from.

Before you begin

Add an attribute and configure the attribute's general settings.

Steps

1. Add a resolver to the attribute:

   1. In the **Resolvers** section, do one of the following:

      - Click **+ Add Resolver**.
      - Click **+ Add Parent Resolver**.

      > **Note**
      >
      > This is an optional shortcut that resolves the attribute against its parent. You can add a parent resolver if the attribute has a parent and doesn't already have a parent resolver. If you add a parent resolver, skip step 1c.

Copyright © 2025 Ping Identity Corporation

2. **Optional:** Update the **Resolver Name**.

   By default, the name is a combination of the resolver type and associated information, such as the attribute name for an **Attribute** resolver.

3. Select a **Resolver type**.

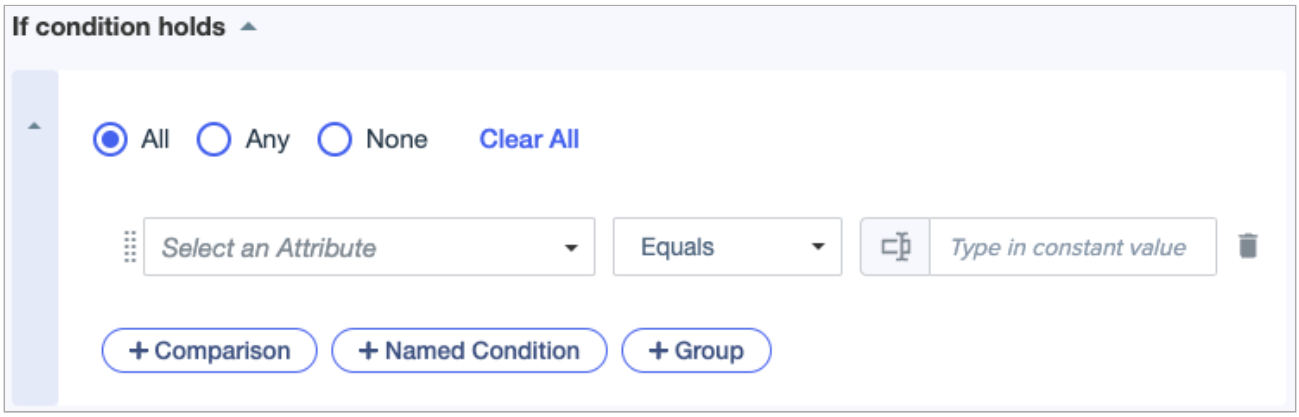
   For more information about resolver types, see Resolvers.

2. **Optional:** To invoke a resolver only under certain conditions, add conditions to the resolver:

   1. Click the hamburger menu next to the **Resolver Name** and select **Add Condition**.

      > **Tip**
      > You can remove a condition the same way.

   2. To add a comparison to the condition, click **+ Comparison**.



   3. Select an attribute to use in the comparison, select a comparator, and then enter a constant or click the **Switch to Attribute** ( ) icon to select an attribute.

When you select an attribute, you can select a property that's grayed out to generate an attribute that resolves against the parent attribute's JSON schema. If the property is nested, generate an attribute for the property above first, and then generate an attribute for the child property.

4. To nest a comparison under another comparison, click **+ Group**.

   Subgroups allow more permutations in comparisons. To remove nesting while keeping the comparison, click **Ungroup**.

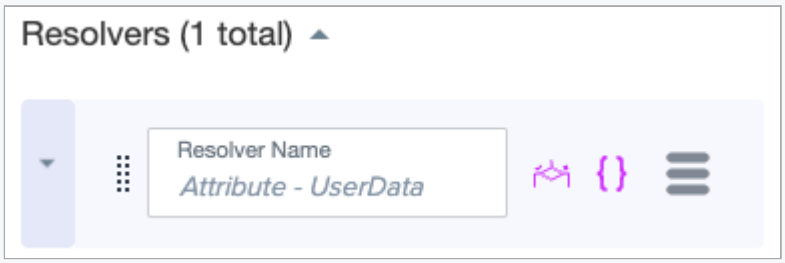
5. To select a named condition, click **+ Named Condition**, select a condition, and then select **is True** or **is False**.

6. To combine multiple conditions, named conditions, or groups, select one of the following options:

   - **All**: Invokes the resolver when all of the conditions are true. If one condition evaluates to false, evaluation stops and the remaining conditions are not executed. This is like adding an `AND` Boolean operator between conditions.
   - **Any**: Invokes the resolver when at least one of the conditions is true. If one condition evaluates to true, evaluation stops and the remaining conditions are not executed. This is like adding an `OR` Boolean operator between conditions.
   - **None**: Invokes the resolver when none of the conditions are true. This is like adding a `NOT` Boolean operator.

3. Add processors to transform the value returned by the resolver.

   For details, see Adding processors to an attribute.

> **Tip**
>
> Icons next to the **Resolver Name** field indicate at a glance whether a resolver has conditions, processors, or both.
>
> 
>
>
> You can copy resolvers defined in an attribute by selecting **Make Copy** from the hamburger menu of that resolver. Copying a resolver also copies any processors or conditions defined in that resolver.

Adding processors to an attribute

Optionally, define value processors to transform the value returned by an attribute, or the value returned by an attribute resolver.

Before you begin

Add an attribute and configure the attribute's general settings.

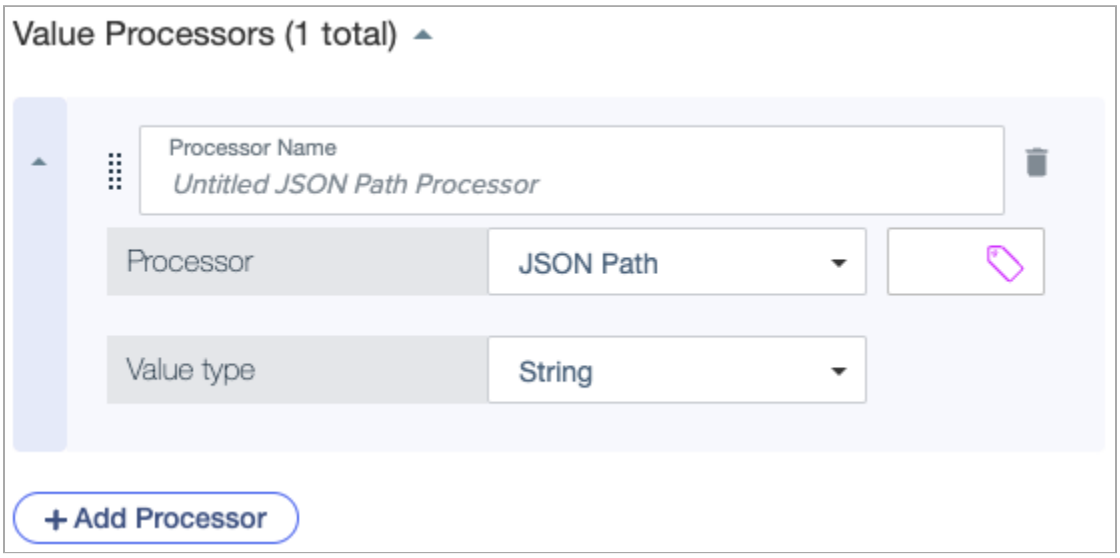
Copyright © 2025 Ping Identity Corporation

Steps

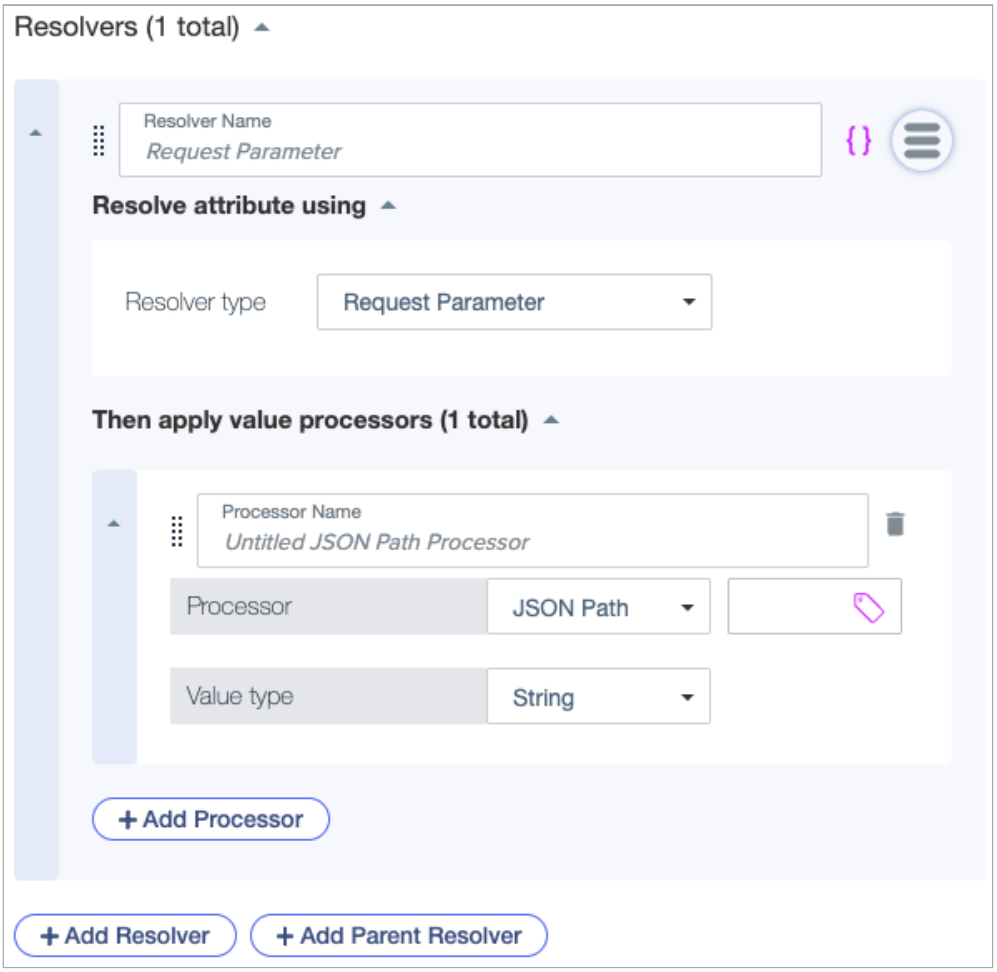
1. Do one of the following to add a processor to the attribute:

   Choose from:

   - To add a value processor, click the **Value Processors** section, and then click **+ Add Processor**.



   - To add a processor to an attribute resolver, in the **Resolvers** section, click the hamburger menu next to the **Resolver Name** field and select **Add Processing**.



2. **Optional:** Update the **Processor Name** field.
3. Select a **Processor** type, and then enter an expression for the processor.

   For details about processor types and expressions, see Processors. The **Label** ( ) icon indicates that you can reference attributes in the expression.

4. In the **Value type** list, select a data type for the transformed value returned after the expression is applied.

Adding value settings to an attribute

Define the attribute's data type and an optional default value for the attribute.

Before you begin

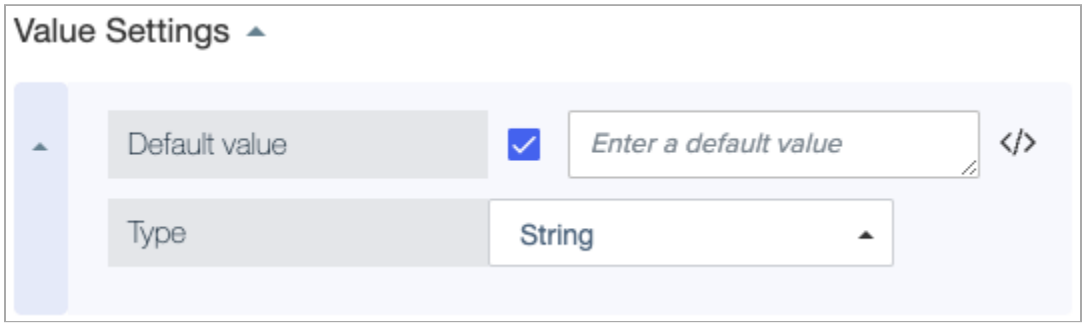
Add an attribute and configure the attribute's general settings.

Steps

1. **Optional:** In the **Value Settings** section, select the **Default value** check box, and then enter a default value.

   This provides the attribute with a value when it can't otherwise be resolved.

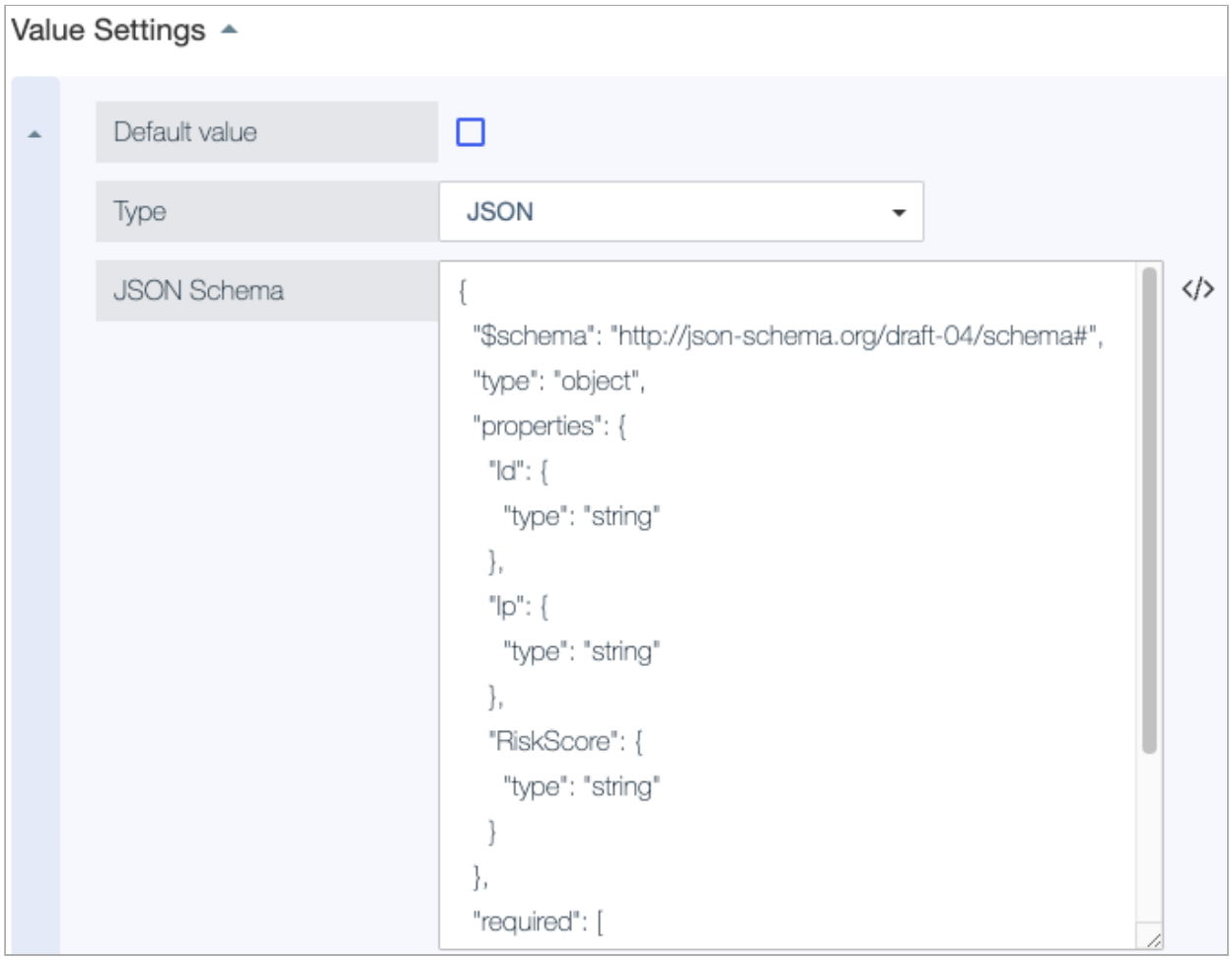
Copyright © 2025 Ping Identity Corporation



2. To constrain the set of allowable values for the attribute, select a data **Type**.

   For details, see Value settings.

3. **Optional:** If the data type is **JSON**, enter a valid **JSON Schema**.



> **Tip**
>
> You can generate attributes based on the schema.

Resolvers

Resolvers define where attributes pull information from.

An attribute can have one or more resolvers. Resolvers can be conditional. In addition, you can add a processor to a resolver to modify the attribute value.

PingOne Authorize resolves an attribute when the attribute value is used in a decision evaluation. Multiple resolvers are resolved in order of appearance in the attribute definition until one of them produces a value. You can drag collapsed resolvers to change their order. If a resolver fails to resolve successfully, processing moves on to the next resolver.

Learn more in Adding resolvers to an attribute.

Resolver types

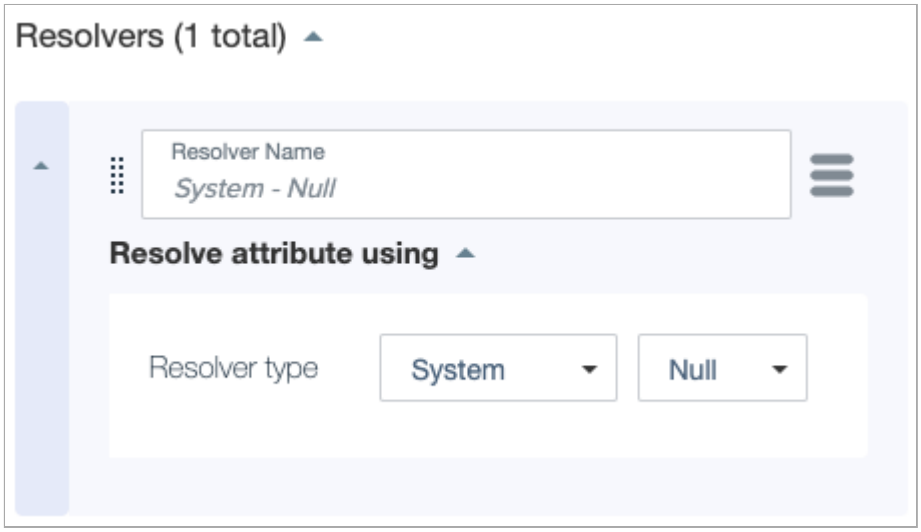
You can use the following types of resolvers:

Resolver type	Description
Attribute	Resolves an attribute from other attributes. This enables you to extract a child attribute or subset from an attribute that contains multiple pieces of information. For example, consider a `Customer.Name` attribute that returns the following JSON representation: `{ "firstname": "Andrew", "middlename": "James", "surname": "Martin" }` You can use an **Attribute** resolver to extract the surname. Create a `Customer.Name.Surname` attribute that resolves against the `Customer.Name` attribute. Then, add a JSON path processor to extract the `Surname` property of the JSON using the expression `$.fullname[0].surname`. • When an attribute has a defined JSON schema, you can generate attributes from schema properties. • When an attribute has a parent, you can click the **+ Add Parent Resolver** button to resolve the child attribute against its parent.
Constant	Takes a constant value defined on the resolver itself. The type and value of the constant are required. **Note** Constants undergo any value processing defined for the attribute.
Current Repetition Value	Resolves an attribute from a repetition source attribute. The source attribute's value setting must be **Collection**. You can use this resolver in attributes that have repetition settings.

Copyright © 2025 Ping Identity Corporation

Resolver type	Description
PingOne User	Resolves the attribute from the user ID provided in the decision request and returns the entire user object. This resolver uses the built-in PingOne User attribute without requiring any additional configuration. **Tip** When you run test scenarios for the attribute on the **Test** tab, use the **PingOne User** field to simulate a request from any user in the current environment.
PingOne User ID	Resolves the attribute from the user ID provided in the decision request and returns the ID. This resolver uses the built-in PingOne User ID attribute without requiring any additional configuration. **Tip** When you run test scenarios for the attribute on the **Test** tab, use the **PingOne User** field to simulate a request from any user in the current environment.
Request Parameter	Looks inside the decision request to determine whether the attribute has been provided by the caller. Specify the full name of the attribute, including any parents, in the request.
Service	Resolves the attribute by using a **Trust Framework** authorization services endpoint to invoke the service at runtime. The service might rely on other attributes being supplied to invoke the service.

Copyright © 2025 Ping Identity Corporation

Resolver type	Description
System	Uses the following standard system attributes without the need for any additional configuration: **`Current DateTime`** This returns the current system `datetime` according to the data type defined in the attribute's value settings. **Note** `Current DateTime` reflects local time for your organization's geographic region, which might differ from the user's geographic region. To determine local time for the user's geographic region: 1. Add an attribute that retrieves the user's timezone. 2. Add an attribute for the current date-time that uses the `Current DateTime` system resolver. 3. Add an attribute for local date-time with a Spring Expression Language (SpEL) value processor that uses the `toDateTimeInTimezone` function to transform the current date-time. Learn more about this function in Date and time library. Learn more in Example: Determining a user's local time. **`Null`** This returns no value. For example, you can use `Null` to compare the value of an attribute to an empty string. To check against a null value, create an attribute with a **System** resolver and a value of **Null**. 

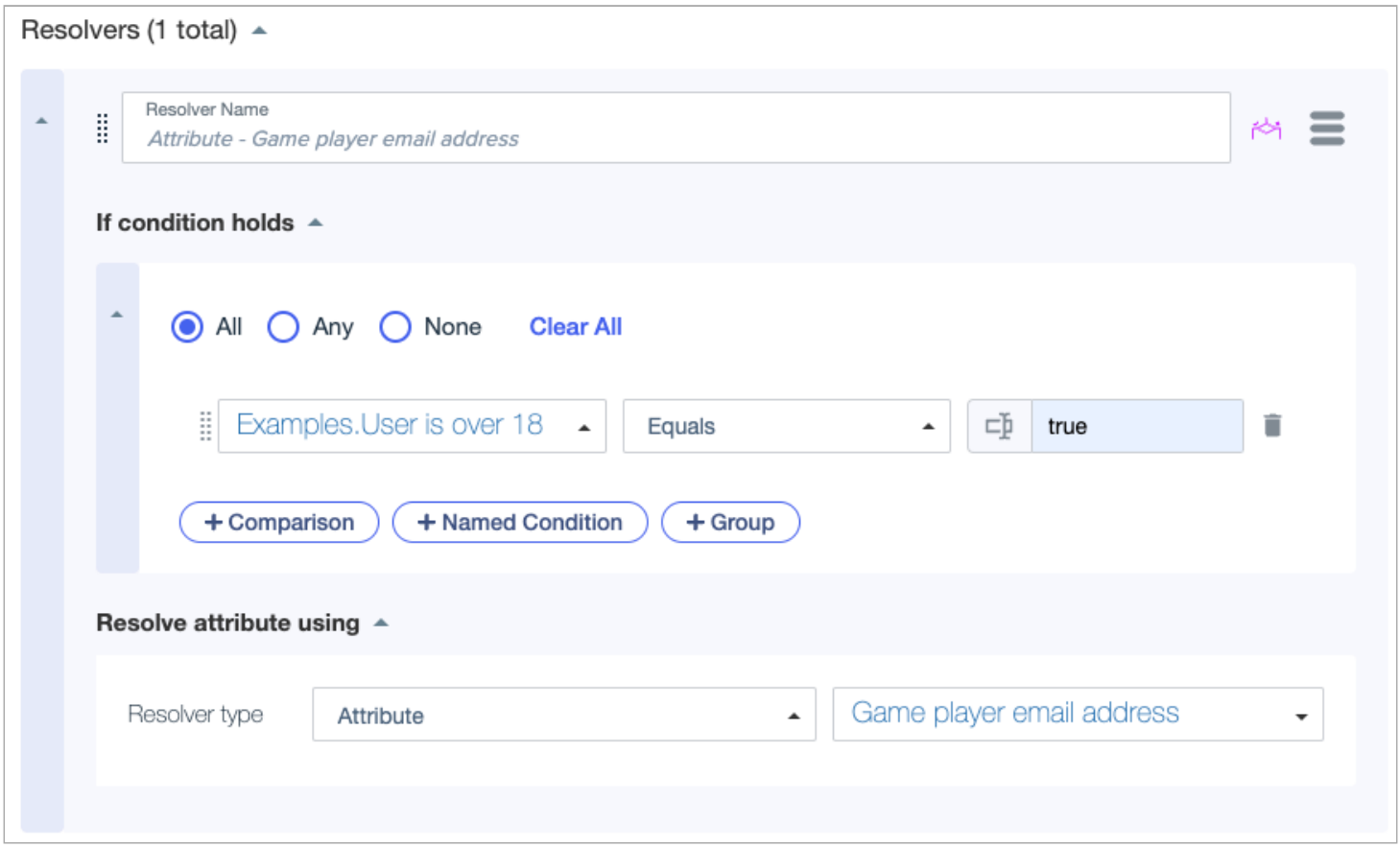
Conditional resolvers

Resolvers can have conditional logic that invokes the resolver only under defined conditions. As with other conditions in PingOne Authorize, you can add comparisons or named conditions, combine multiple conditions using **All**, **Any**, or **None**, and add subgroups.

Learn how to add conditions to resolvers in Adding an authorization attribute.

Copyright © 2025 Ping Identity Corporation

In the following example of a conditional resolver, the game player's email address is resolved only when the `User is over 18` attribute has a value of `true`.



Value processing for a resolver

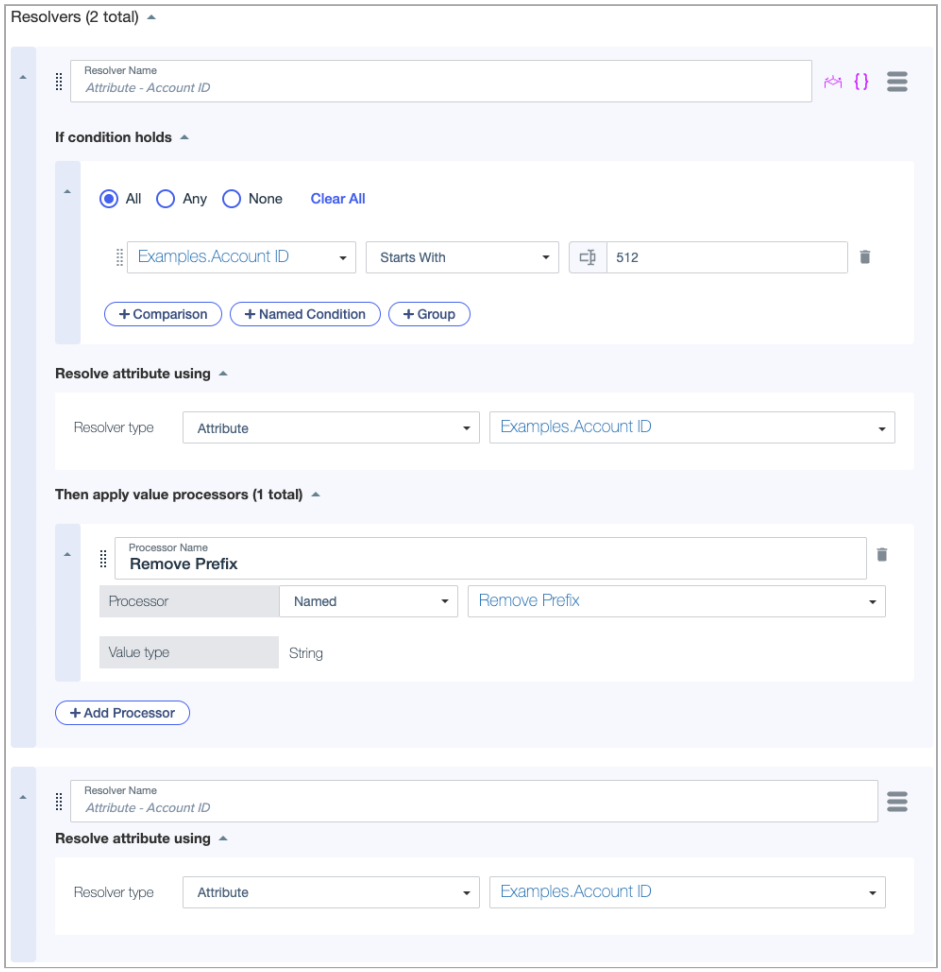
Resolvers can have value processors that extract details and modify data when the attribute value is being resolved. As with other processors, value processors for resolvers are processed in order, with each processor receiving the output of the previous processor.

Learn how to add processors to resolvers in Adding processors to an attribute.

Example: Removing an account prefix

Consider an account ID that has a standard prefix that you want to remove. In this example, a condition and a processor work together to identify and remove the prefix. A second resolver with no processing resolves account IDs that don't have the prefix.

Copyright © 2025 Ping Identity Corporation



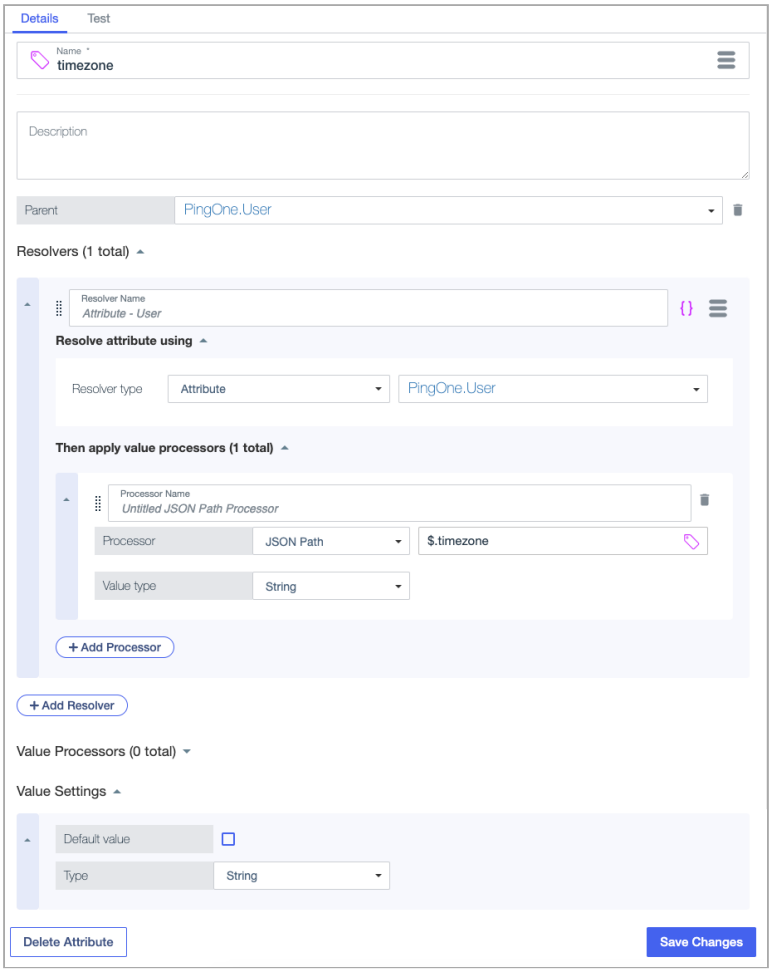
Example: Determining a user's local time

If a user is in a different geographic region than your system, you can use the `Current DateTime` system resolver and a SpEL processor to determine the user's local time.

1. Add an attribute that retrieves the user's timezone.

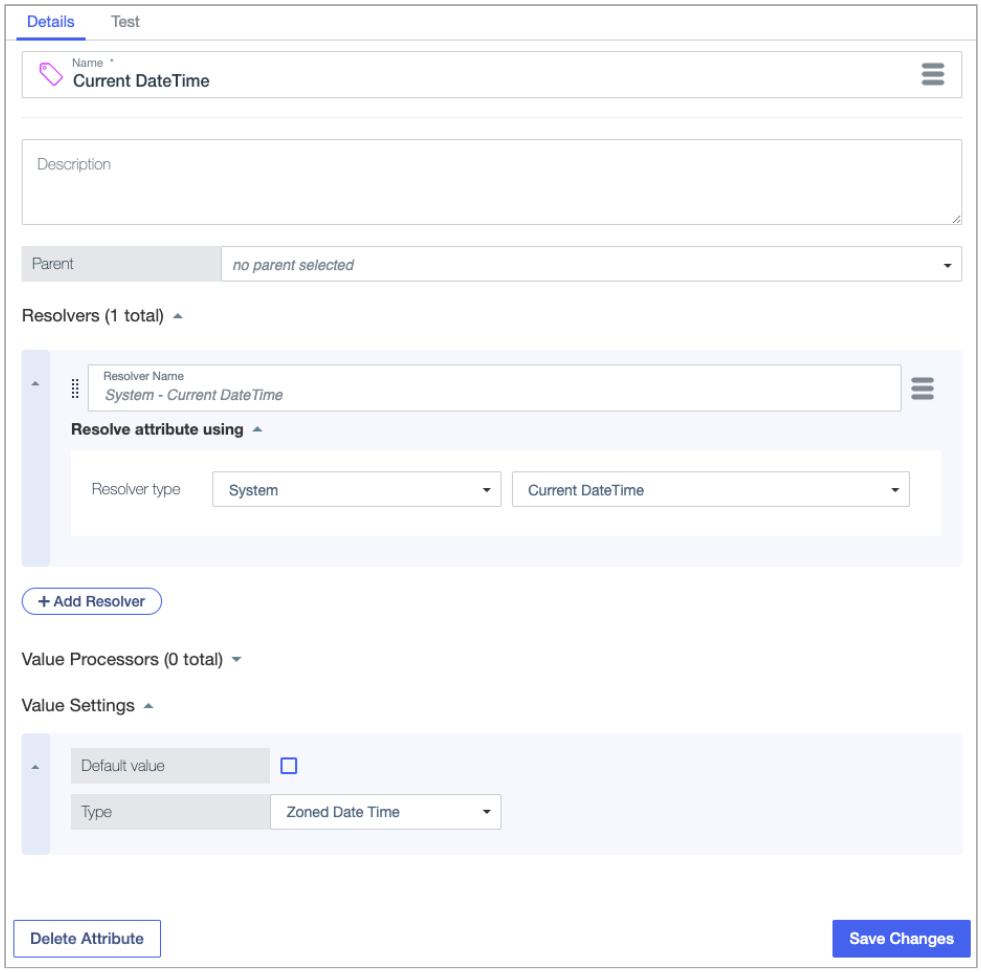
   For example, you can use a resolver and a processor to extract the **Timezone** property from the built-in **PingOne User** attribute, if the timezone is specified in the user's PingOne user profile.

Copyright © 2025 Ping Identity Corporation



2. Add an attribute for the current date-time that uses the `Current DateTime` system resolver.

> **Note**
>
> Make sure the attribute's value setting type is **Zoned Date Time**.



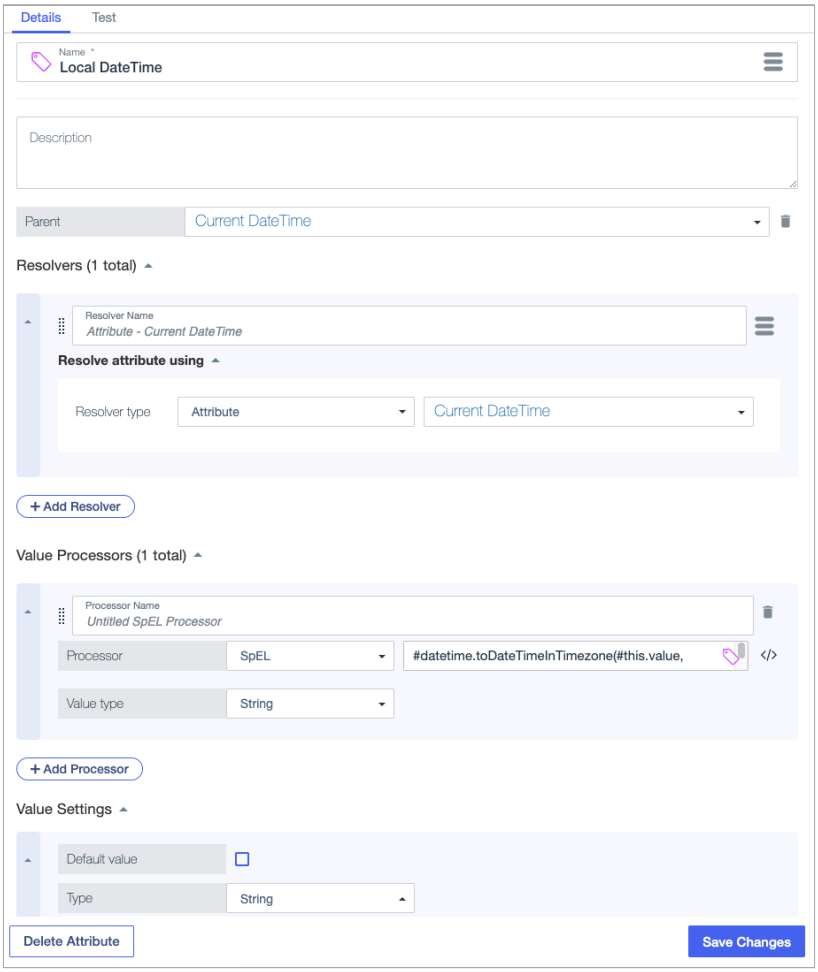
3. Add an attribute for local date-time with a SpEL value processor that uses the `toDateTimeInTimezone` function to transform the current date-time.

> **Tip**
>
> Learn more about the `toDateTimeInTimezone` function in Date and time library.

The following attribute resolves against the **Current DateTime** attribute, then uses a SpEL processor to convert the time to the user's local time with the following SpEL expression. The expression includes the timezone attribute that you added in step 1.

```
#datetime.toDateTimeInTimezone(#this.value, {{PingOne.User.timezone}}, 'yyyy-MM-dd HH:mm:ss')
```

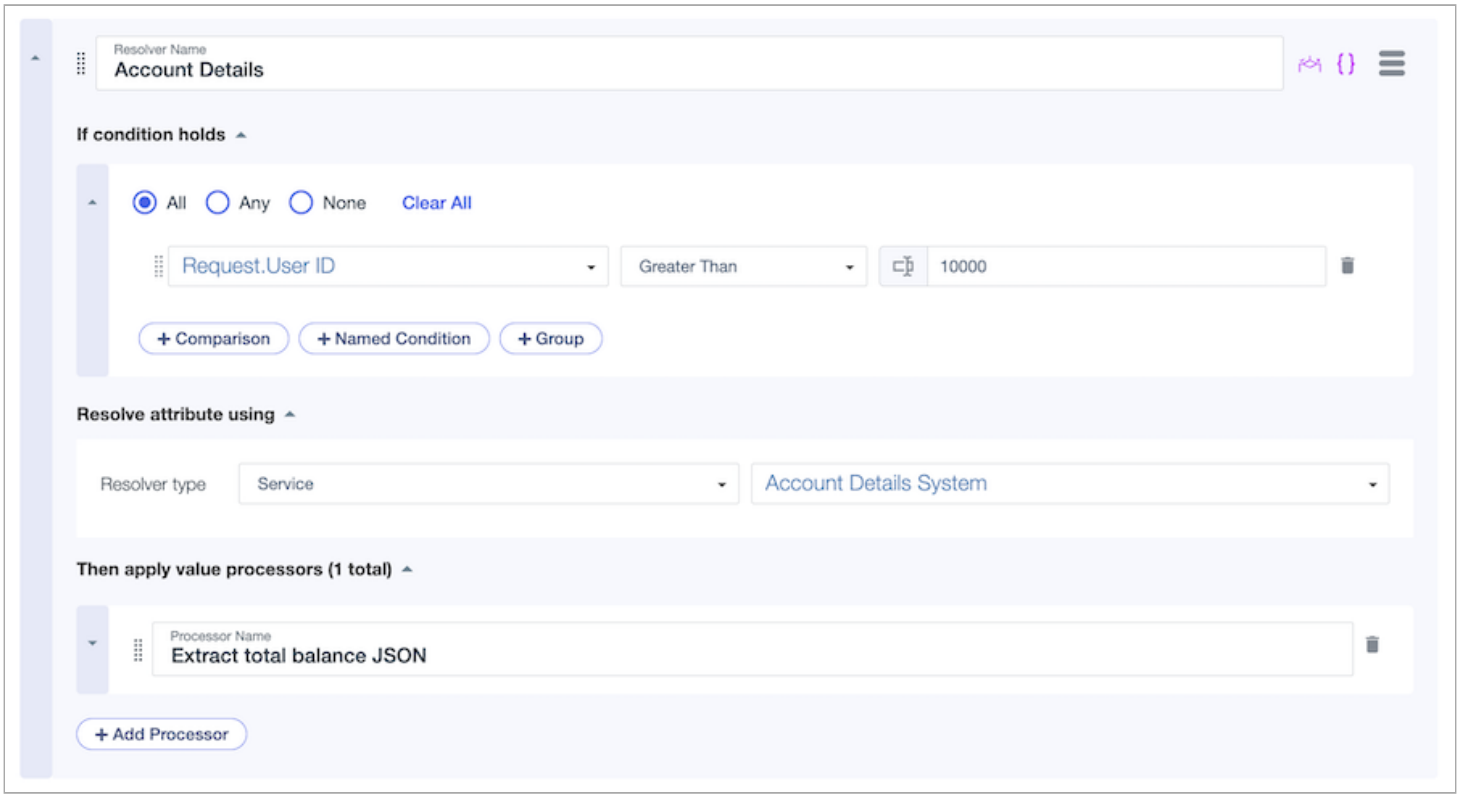

Copyright © 2025 Ping Identity Corporation

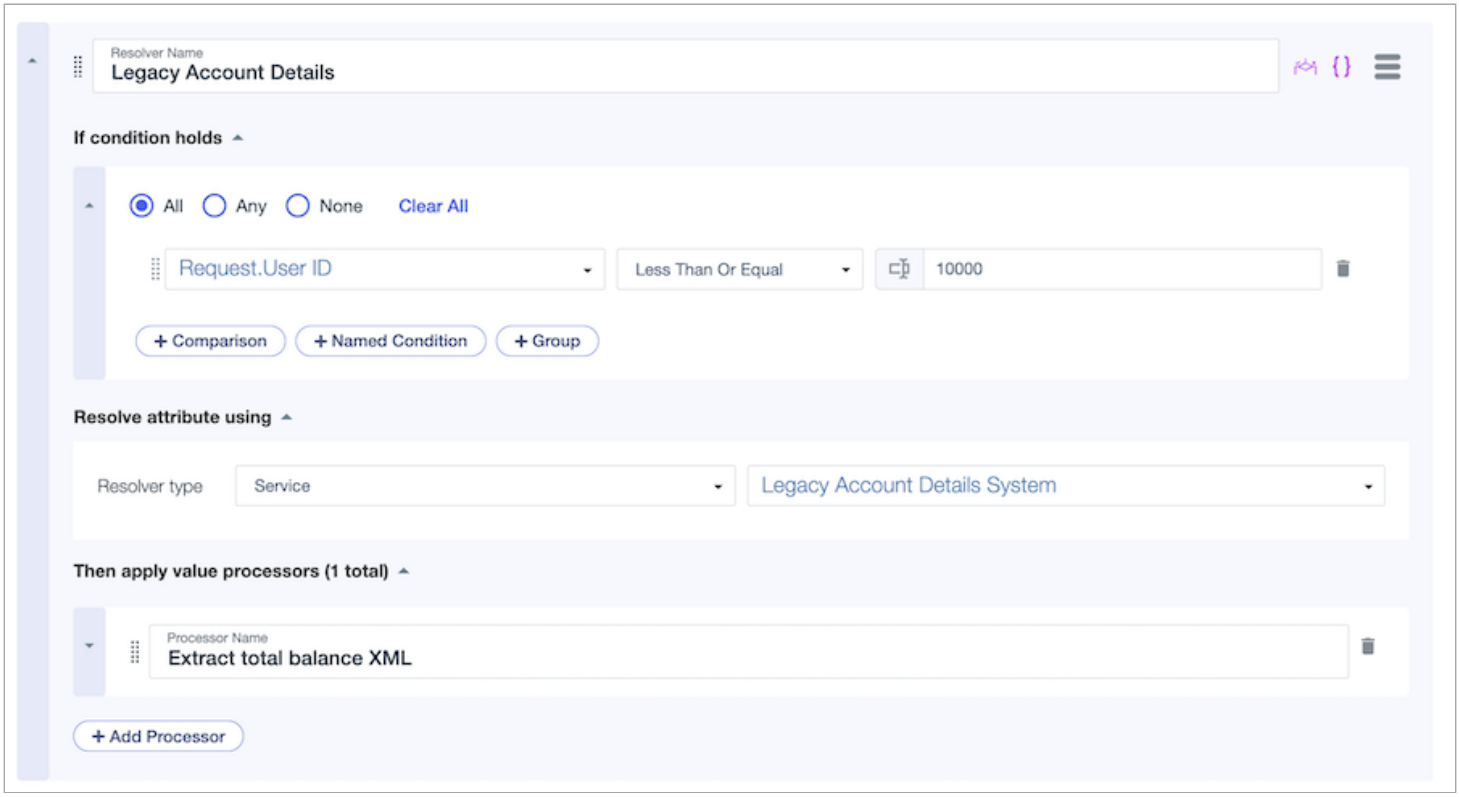


Example: Adding processors directly to resolvers

Adding value processors directly to resolvers, rather than to the attribute itself, can be useful when pulling data from distinct sources that require different formatting.

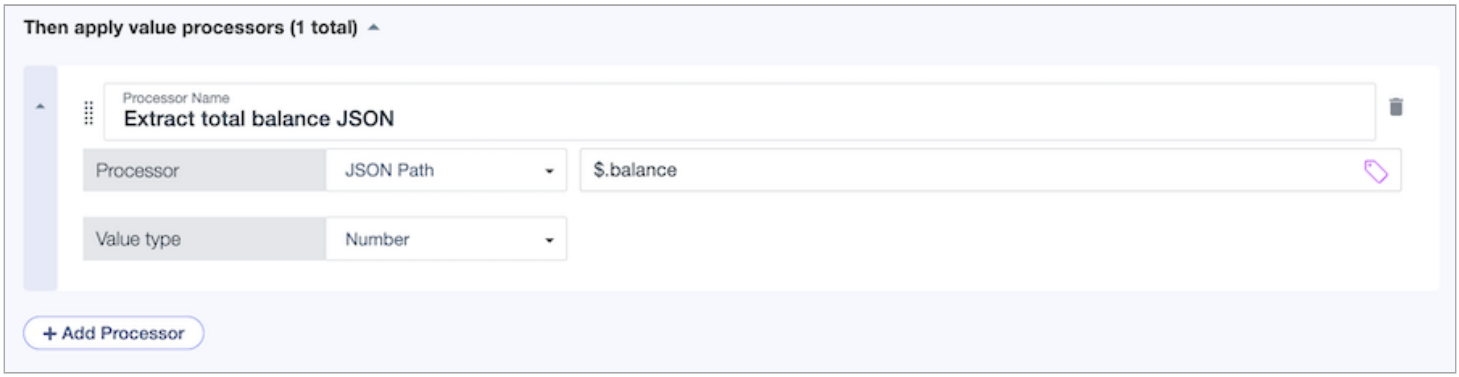
For example, consider a bank that wants to pull in user information either from a modern system or a legacy system to authorize transactions. These systems are represented by the **Account Details System** and **Legacy Account Details System** HTTP services, respectively. With the following resolver configuration, the decision service calls to the **Account Details System** service if the user ID is above `10000` (indicating a new user), or to the **Legacy Account Details System** service if the user ID is less than or equal to `10000` (indicating a legacy user):



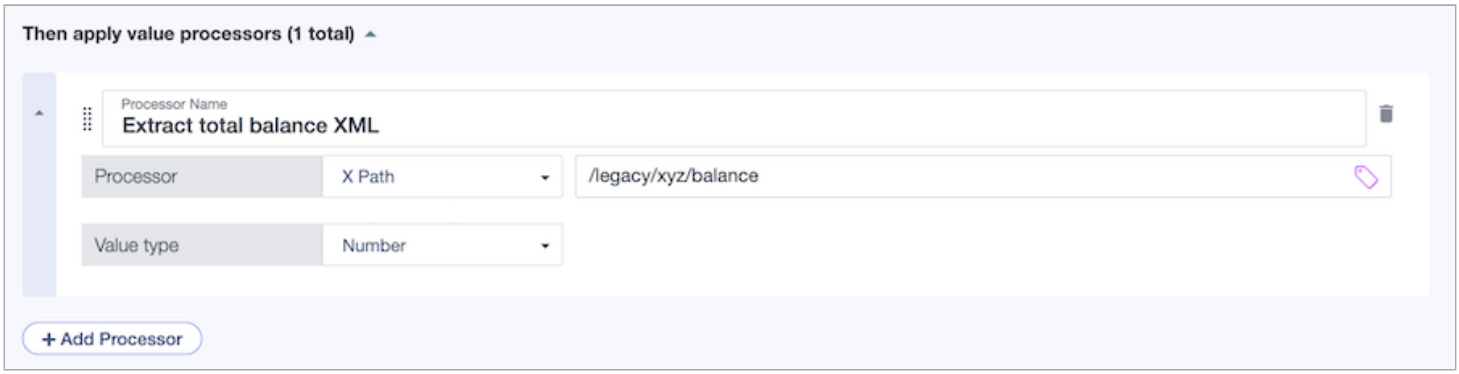


Data collected from the **Account Details System** service is formatted as JSON and requires a JSON Path processor defined on the **Account Details** resolver to extract a new user's total balance:

Copyright © 2025 Ping Identity Corporation



Data collected from the **Legacy Account Details System** service is formatted as XML and requires an X Path processor defined on the **Legacy Account Details** resolver to extract a legacy user's total balance:



After the decision service pulls in user data from either service, common value processing might be required regardless of where the data comes from. For example, suppose the bank has a 500 USD minimum for an active account and anything above that is available for transfers. The following SpEL processor subtracts 500 from the result of resolver processing to obtain the user's available balance for transfers:

Built-in attributes

The **Trust Framework** provides built-in attributes that enable you to use PingOne service and user profile data right out of the box.

Built-in attributes are nested under the **PingOne** parent attribute on the **Attributes** tab. PingOne Authorize owns the **PingOne** parent attribute and its children.

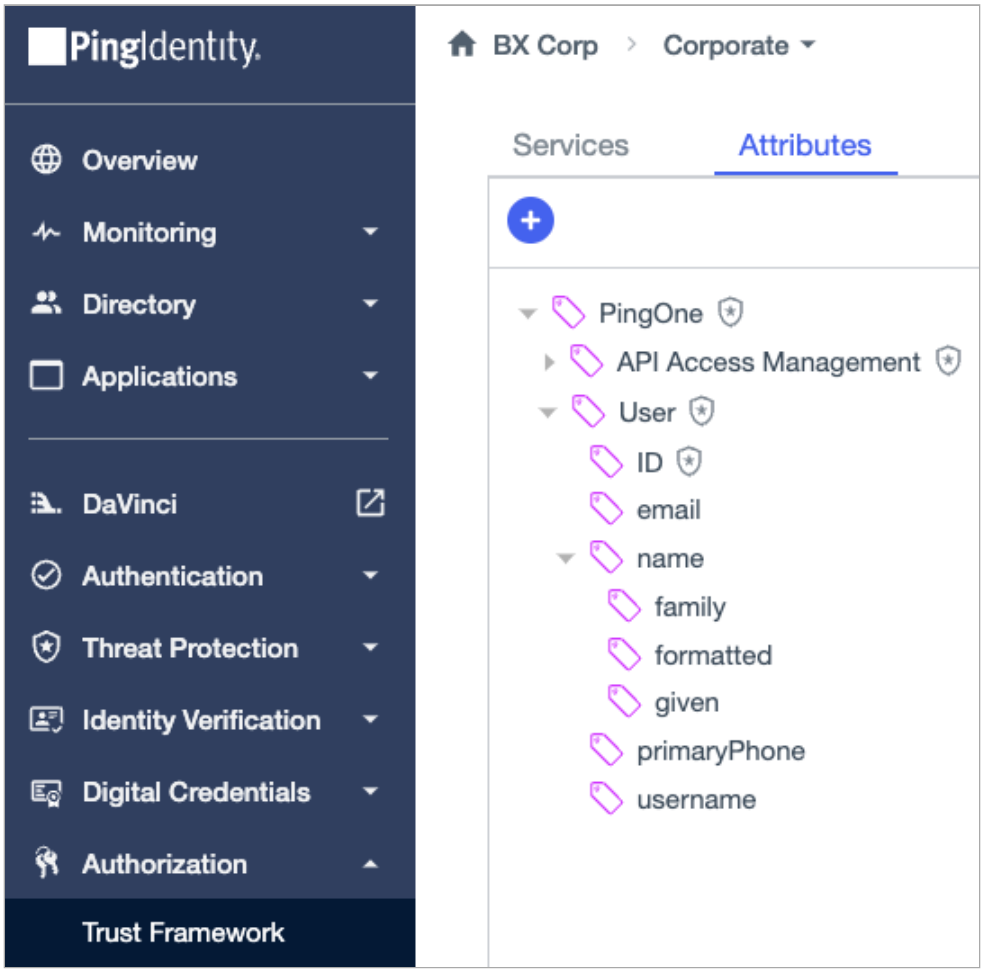
The **Shield** ( ) icon indicates that these attributes are system-owned and editing restrictions apply. You can't move, update, or delete these attributes. You can't nest your own attributes under the **PingOne** and user **ID** attributes. This ensures that built-in attributes are configured correctly and always available.

Copyright © 2025 Ping Identity Corporation

User attributes

Built-in **User** attributes model user identity information for use in other attributes and directly in policies. You can nest your own attributes under the **User** attribute.

> **Note**
>
> - To use built-in user attributes, make sure that the PingOne SSO service is enabled in your environment. This provides access to user profile information in the PingOne Directory.
> - These attributes resolve identities stored in the PingOne Directory and do not access user information in external identity stores. If you're using an external identity store, create your own user attributes that resolve against your identity store.
> - When you run test scenarios for these attributes on the **Test** tab, use the **PingOne User** field to simulate a request from any user in the current environment.



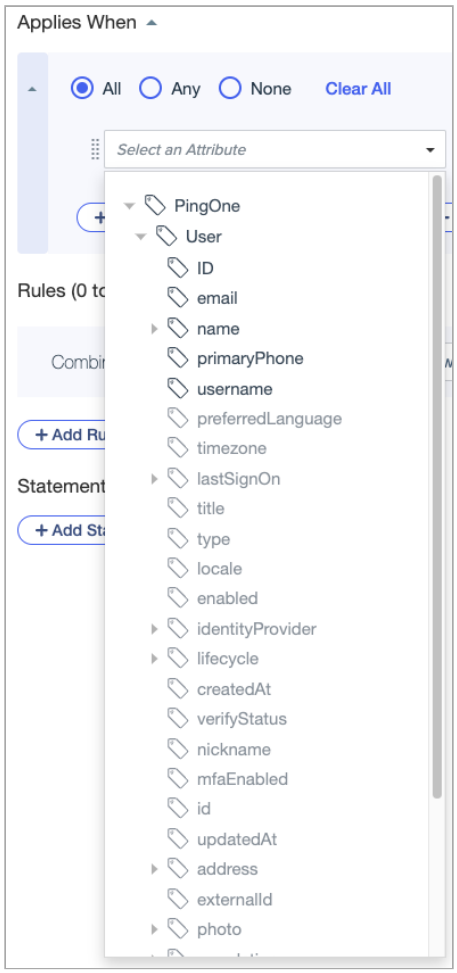
The following built-in user attributes resolve from the `userContext.userId` property of the decision request. These attributes are derived from properties of the PingOne user object. Learn more about the user object in Users data model.

Copyright © 2025 Ping Identity Corporation

Attribute	Data Type	Description
User	JSON	The `PingOne.User` attribute returns a JSON object that provides data about the identity requesting access to a resource. This attribute retrieves the PingOne user object through the `/environments/{envID}/users/{userID}` endpoint. Learn more about the **PingOne User** resolver in Resolvers.
ID	String	The `PingOne.User.ID` attribute returns the ID of the identity requesting access to a resource. Learn more about the **PingOne User ID** resolver in Resolvers.
email	String	The `PingOne.User.email` attribute returns the email address of the identity requesting access to a resource. This attribute uses a JSON Path processor to extract the user's email address from the `PingOne.User` attribute.
name	JSON	The `PingOne.User.name` attribute returns a JSON object that provides the name schema for the identity requesting access to a resource. This attribute uses a JSON Path processor to extract the user's name information from the `PingOne.User` attribute. As an example, consider a user called `Gregory Eric Jones` whose father has the same name.
family	String	The `PingOne.User.family` attribute returns the last name of the identity requesting access to a resource. This attribute uses a JSON Path processor to extract the user's last name, for example `Jones`, from the `PingOne.User.name` attribute.
formatted	String	The `PingOne.User.formatted` attribute returns the fully formatted name of the identity requesting access to a resource. This attribute uses a JSON Path processor to extract the user's formatted name, for example `Mr. Gregory E. Jones, II`, from the `PingOne.User.name` attribute.
given	String	The `PingOne.User.given` attribute returns the first name of the identity requesting access to a resource. This attribute uses a JSON Path processor to extract the user's first name, for example `Gregory`, from the `PingOne.User.name` attribute.
primaryPhone	String	The `PingOne.User.primaryPhone` attribute returns the main phone number of the identity requesting access to a resource. This attribute uses a JSON Path processor to extract the user's phone number from the `PingOne.User` attribute.
username	String	The `PingOne.User.username` attribute returns the username of the identity requesting access to a resource. This attribute uses a JSON Path processor to extract the username from the `PingOne.User` attribute.

Copyright © 2025 Ping Identity Corporation

Built-in user attributes comprise a subset of the standard and core PingOne user attributes available in **Directory > User Attributes**. You can generate attributes in PingOne Authorize for standard, core, and custom PingOne user attributes that are not already built-in, and use them in conditions, processors, and rules.



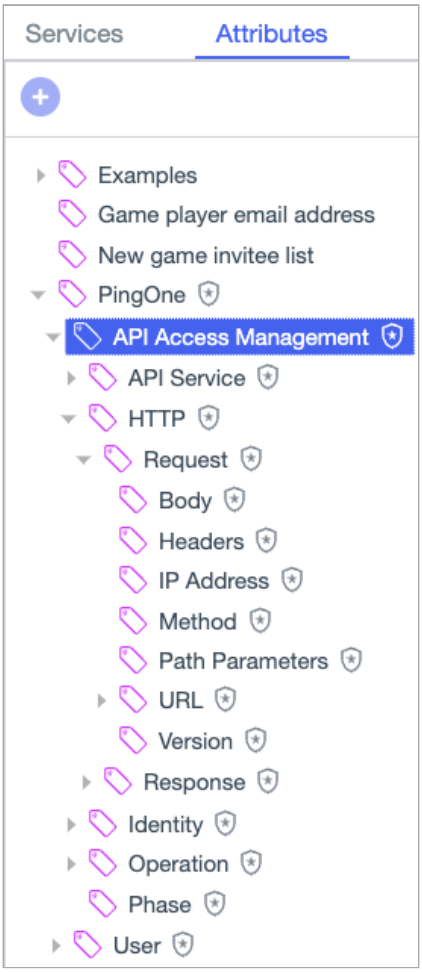
Changes made to PingOne user attributes, such as deleting an attribute or changing a custom attribute's description, do not affect the corresponding built-in or generated user attributes in PingOne Authorize, as long as they are in use. Deleting a PingOne user attribute deletes the corresponding attribute in PingOne Authorize if the attribute has no dependencies.

Changes made to built-in user attributes in PingOne Authorize do not affect the corresponding PingOne user attributes. For example, changing the name of the built-in **email** attribute to **emailAddress** in PingOne Authorize doesn't change the name of the associated PingOne **email** user attribute. The PingOne Authorize **emailAddress** attribute will continue to work as usual to resolve the user's email address.

API Access Management attributes

API Access Management attributes model API services and operations, HTTP requests and responses, and access tokens. PingOne Authorize generates these attributes when you enable custom policies for an API service.

Copyright © 2025 Ping Identity Corporation



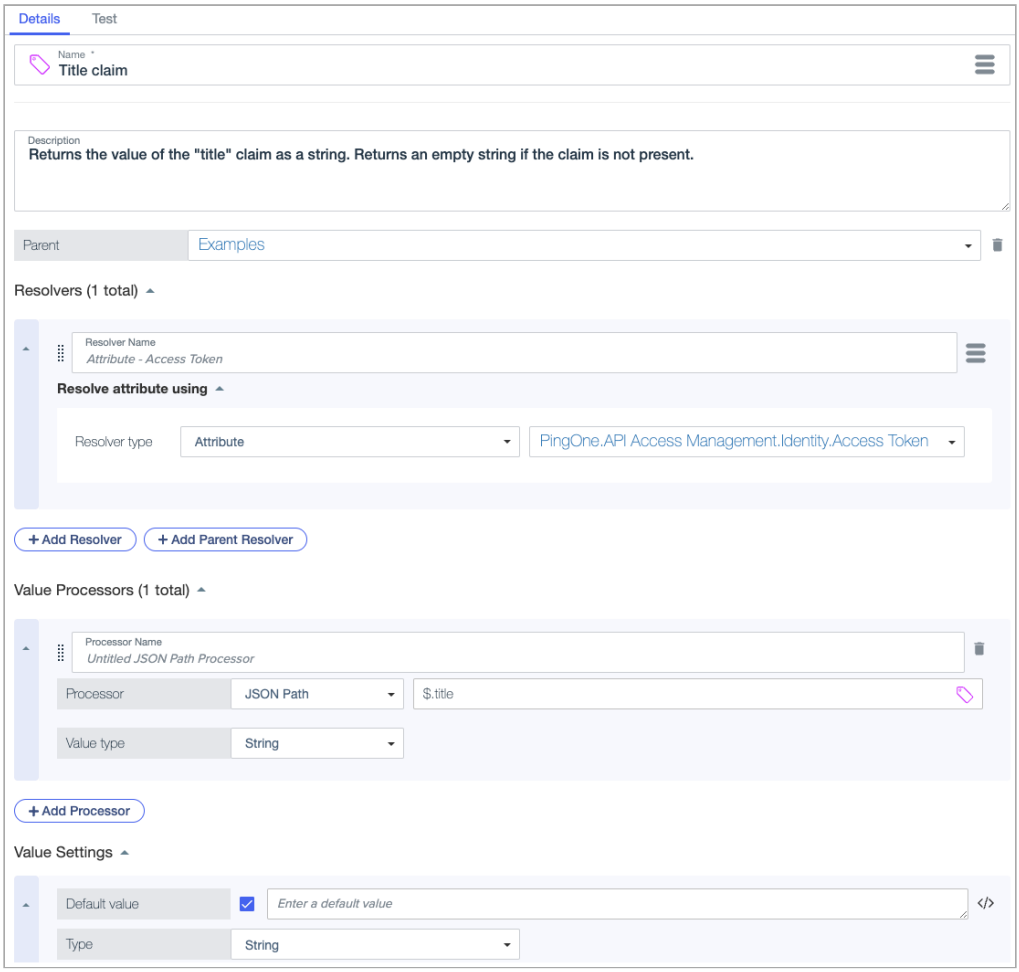
Creating attributes from built-in attributes

You can derive your own attributes from built-in API Access Management attributes, as shown in the following examples:

Custom access token claim attribute

In the following attribute, a value processor is used to resolve a custom claim called `title` from the built-in `PingOne.API Access Management.Identity.Access Token` attribute. To ensure that a token without the custom claim is resolved successfully, the attribute has an empty string as its default value. In this example, the claim's JSON data type is **String**. Access token claims can have other data types, including **Number** and **Collection**.

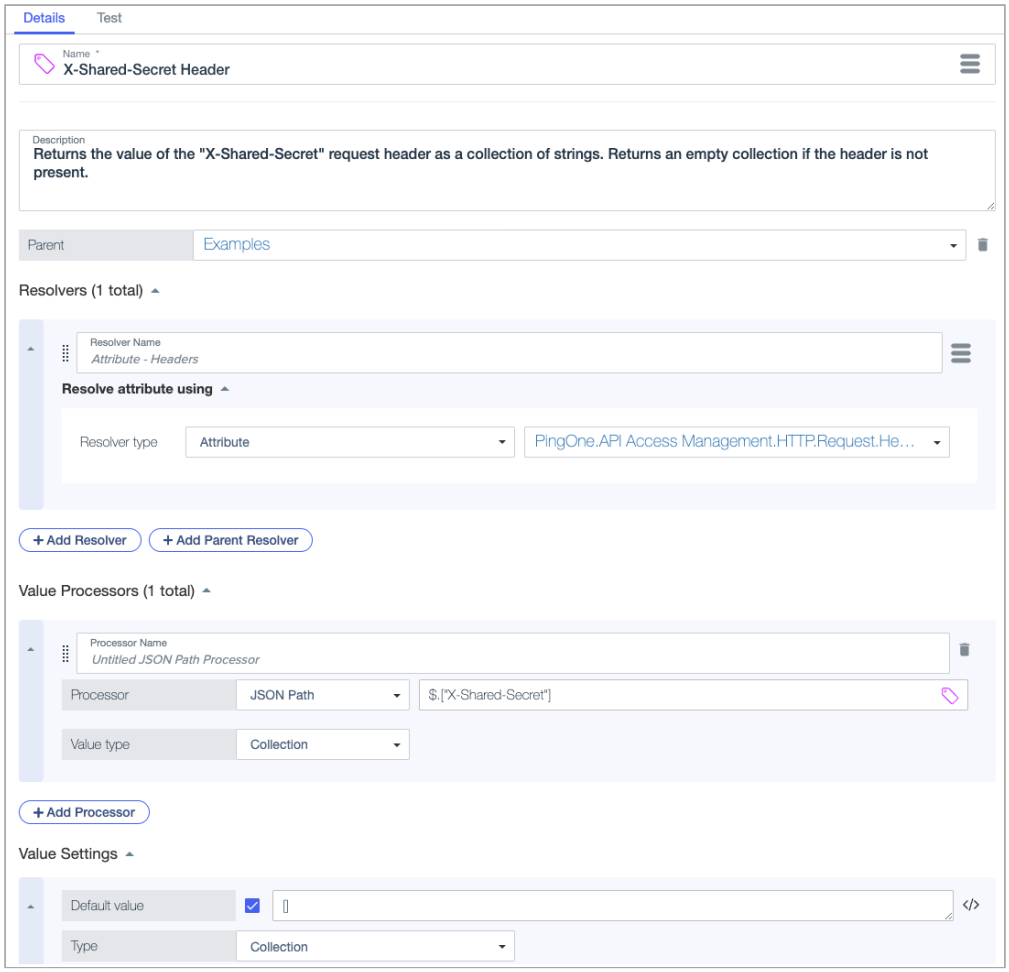
Copyright © 2025 Ping Identity Corporation



HTTP request header attribute

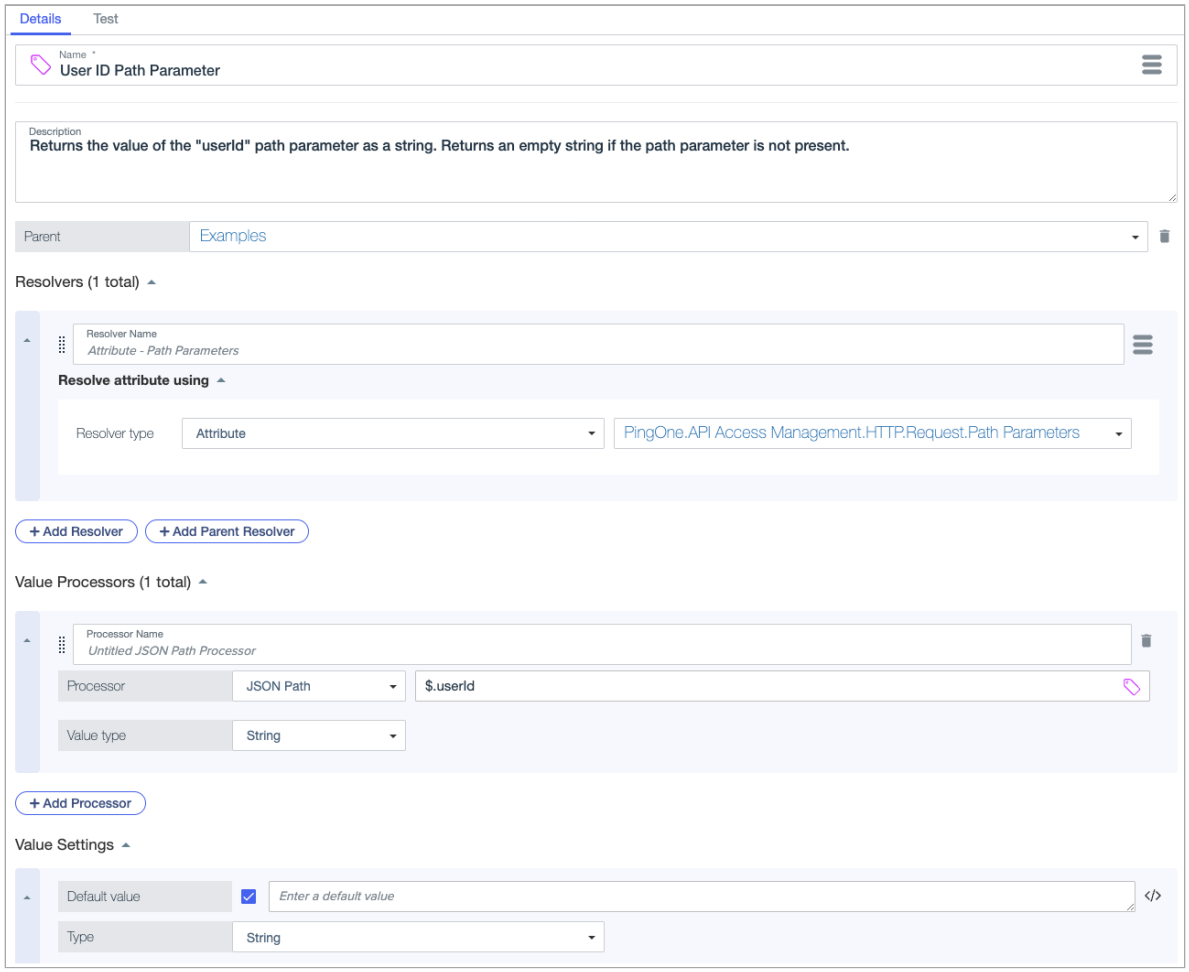
To allow policy authors to use a custom header in policies, you can define an attribute that extracts a custom header value from an HTTP request or response. In the following attribute, a value processor is used to resolve the `X-Shared-Secret` value from the built-in `PingOne.API Access Management.HTTP.Request.Headers` attribute as a collection. To ensure that a header without the custom value is resolved successfully, the attribute has an empty collection as its default value.

Copyright © 2025 Ping Identity Corporation



API operation path parameters

If an API operation path includes a parameter, you can define an attribute that allows policy authors to use the parameter in custom policies. For example, the following attribute extracts the user ID from a decision request that matches an API operation defined with the path `/records/user/{userId}`. For information about using this attribute in a policy, see Adding custom policies for API services and operations.



Step-up authentication attributes

The following attributes are used in basic access control rules for step-up authentication. You can also use them in custom policies. PingOne Authorize generates these attributes when you deploy an API service.

Attribute	Data Type	Description
Authentication Age	Number	The `API Access Management.Identity.Access Token.Authentication Age` attribute returns the number of seconds since the end user was authenticated. This attribute uses the `System Current DateTime` resolver and a SpEL processor to calculate the number of seconds since the **Authentication Time**.

Copyright © 2025 Ping Identity Corporation

Attribute	Data Type	Description
Authentication Policy	String	The `API Access Management.Identity.Access Token.Authentication Policy` attribute returns the authentication policy that was satisfied when the access token was issued. An authentication policy is also called an authentication context class reference (ACR). If the access token contains an `acr` claim, this attribute uses a JSON Path processor to extract the `acr` value from the `API Access Management.Identity.Access Token` attribute.
Authentication Time	Zoned Date Time	The `API Access Management.Identity.Access Token.Authentication Time` attribute returns the date and time when the end user was authenticated. If the access token contains an `auth_time` claim, this attribute uses a JSON Path processor to extract the date and time from the `API Access Management.Identity.Access Token` attribute. If the claim is missing from the token, the default value is January 1, 1970.

Generated attributes

When a JSON schema is defined in an attribute or service's value settings, you can generate child attributes that extract schema properties.

PingOne Authorize automatically resolves a generated attribute against the parent attribute or service and adds a JSON Path processor that extracts the JSON schema property.

You can generate attributes by selecting them in any field that allows attribute selection. If an attribute hasn't been generated for a property yet, the property is grayed out. Learn more in Generating an attribute.

If the parent attribute has nested JSON properties, you must generate attributes one level at a time. Generate the parent-level attribute first, then generate the child. For example, to generate a risk **level** attribute, you have to generate the **result** attribute first.

Copyright © 2025 Ping Identity Corporation

Nested attributes always resolve against the parent attribute directly above them in the tree, instead of the root-level attribute.

> **Note**
>
> If the JSON schema changes in the parent attribute, you must manually update any generated child attributes. PingOne Authorize does not do this automatically.

Connector attributes

When you connect to a PingOne service, PingOne Authorize automatically creates an attribute that resolves against the service. This attribute contains a JSON schema that you can use to generate additional attributes.

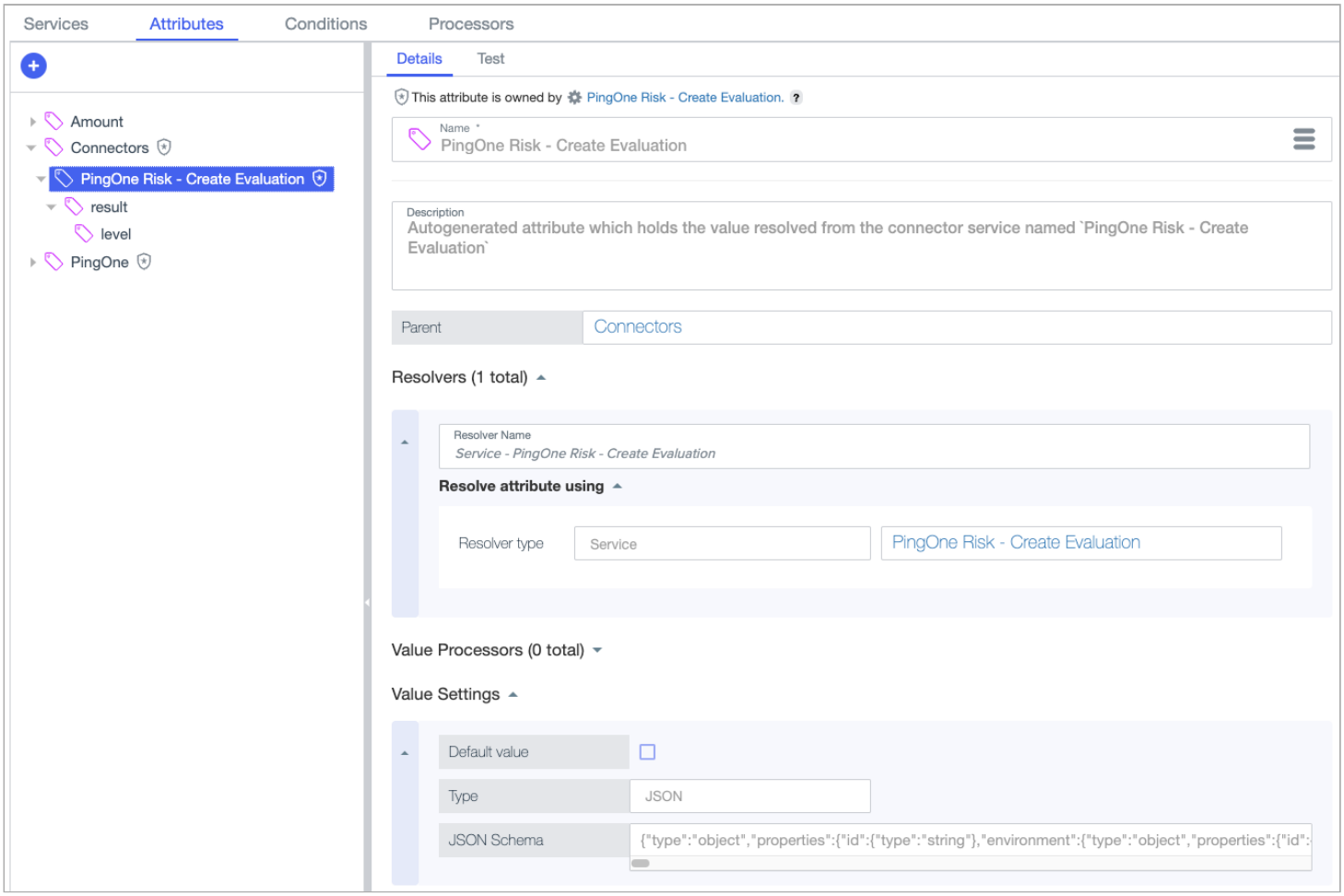
Connector attributes are nested under the **Connectors** parent attribute on the **Attributes** tab. PingOne Authorize owns the **Connector** parent attribute and the attributes nested directly under it that resolve against a service.

The **Shield** ( ) icon indicates that these attributes are system-owned and editing restrictions apply. You can't move, update, or delete these attributes. This ensures that connector attributes are configured correctly and always available.

You can nest your own attributes under connector attributes. When you delete a connector service, the generated attribute that resolves against the service is also deleted.

The following image shows an example of a system-owned connector attribute that resolves against the PingOne Protect service with additional child attributes that extract the risk level.

Copyright © 2025 Ping Identity Corporation



Generating an attribute

Generate attributes to extract JSON schema properties from parent attributes. Learn more in Generated attributes.

As example data for this task, consider the following JSON that represents a user in an external identity store:

```
{
  "Id": "my-id",
  "Ip": "217.145.198.92",
  "Name": "John Smith"
}
```

You'll create a parent attribute that stores this user information passed from a decision request, then generate child attributes that extract properties.

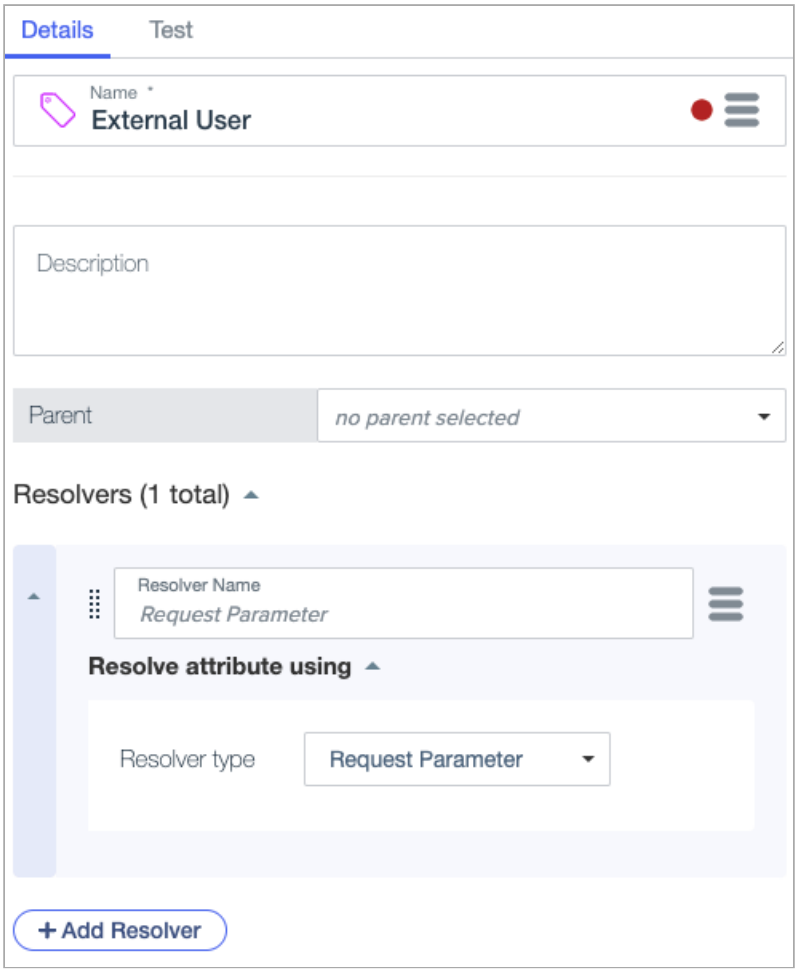
Steps

1. In the PingOne admin console, add an attribute that stores a JSON schema:
    1. Go to **Authorization > Trust Framework** and click the **Attributes** tab.
    2. Click the **+** icon and select **Add new attribute**, then enter a name for the attribute, such as `External User`.

Copyright © 2025 Ping Identity Corporation

3. To define where the attribute pulls information from, click **Resolvers**, and then click **+ Add Resolver**.

4. In the **Resolver type** list, select **Request Parameter**.



5. In the **Value Settings** section, select **JSON** in the **Type** list.

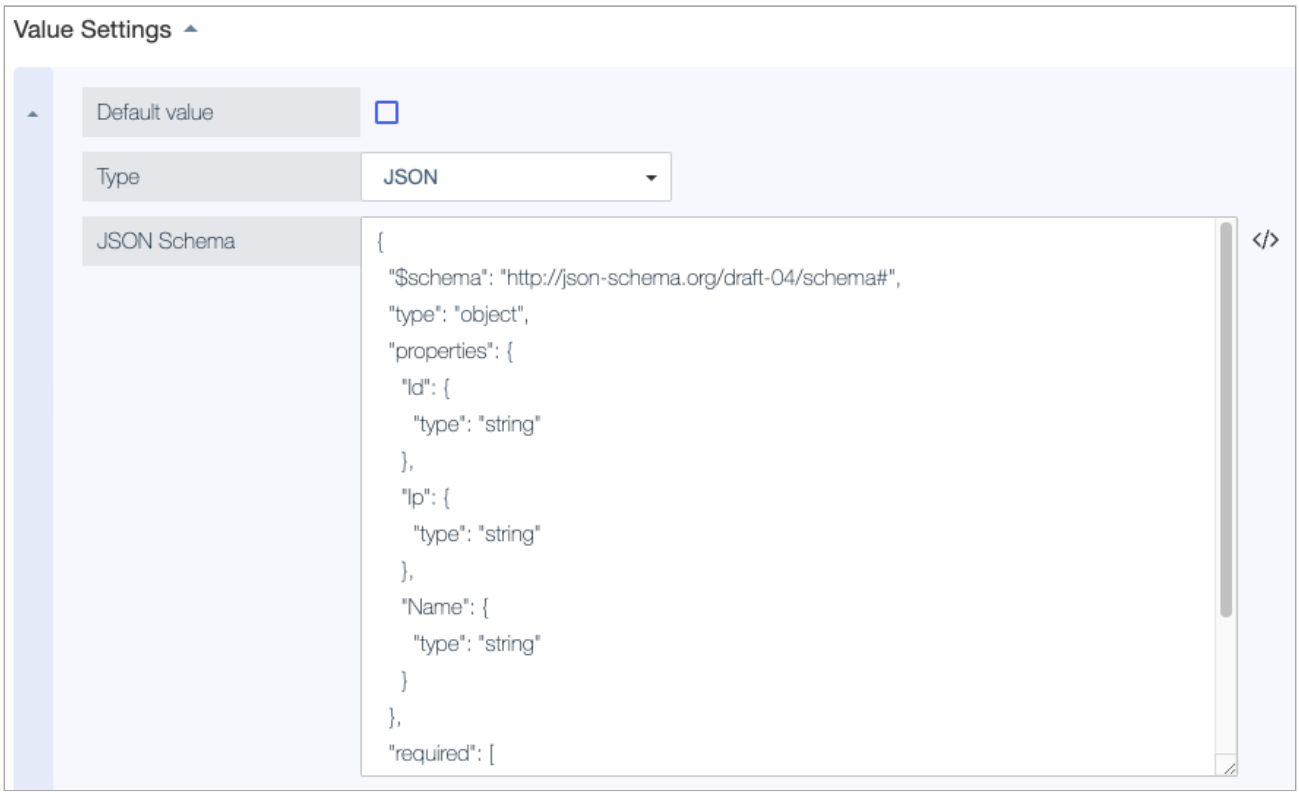
6. Use an online JSON schema generator to generate a schema for the example JSON that represents the external user.

   Example:

Copyright © 2025 Ping Identity Corporation

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "Id": {
      "type": "string"
    },
    "Ip": {
      "type": "string"
    },
    "Name": {
      "type": "string"
    }
  },
  "required": [
    "Id",
    "Ip",
    "Name"
  ]
}
```

7. Copy the resulting schema and enter it in the **JSON Schema** field.



> **Tip**
>
> To edit large JSON objects more effectively, open the code editor by clicking </>.

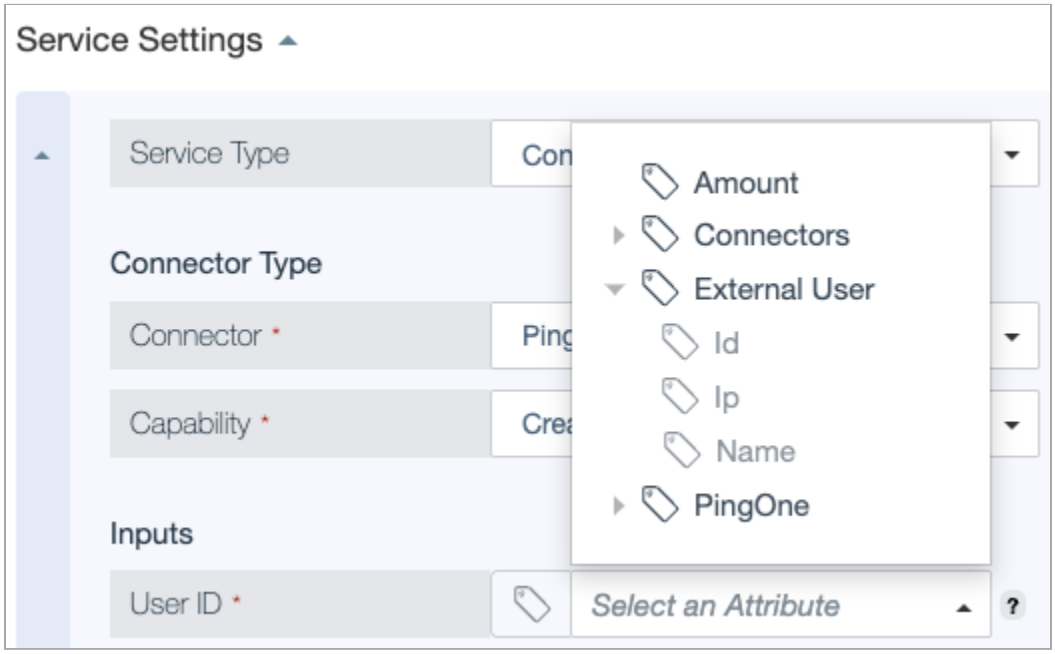
8. Click **Save Changes**.

2. Generate attributes based on the defined JSON schema.

For example purposes, you'll generate attributes for PingOne Protect connector service inputs.

1. Add a connector service forPingOne Risk. Enter a name, such as `External User Risk`, and then select the service type, and connector types.
2. In the **Inputs** section, click next to **User ID**, and then click the **Select an attribute** list.
3. Expand the **External User** parent attribute and select the **Id** property.

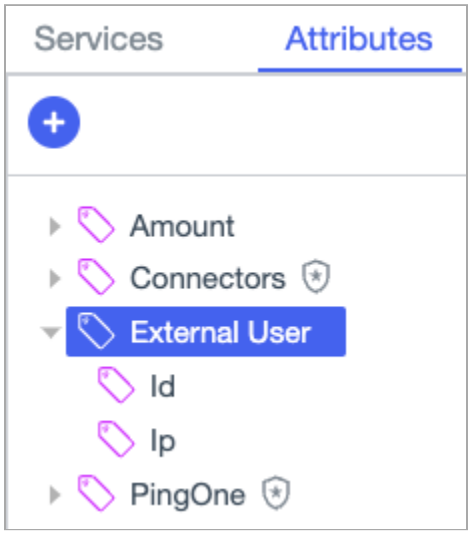
   If an attribute hasn't been generated for a property yet, the property is grayed out. When you select a property, PingOne Authorize adds an attribute that resolves against the parent attribute and a processor that extracts the property.



4. For **User Type**, enter `EXTERNAL`.
5. For **IP Address**, select the **External User → Ip** property to generate an attribute.
6. Click **Save changes**.

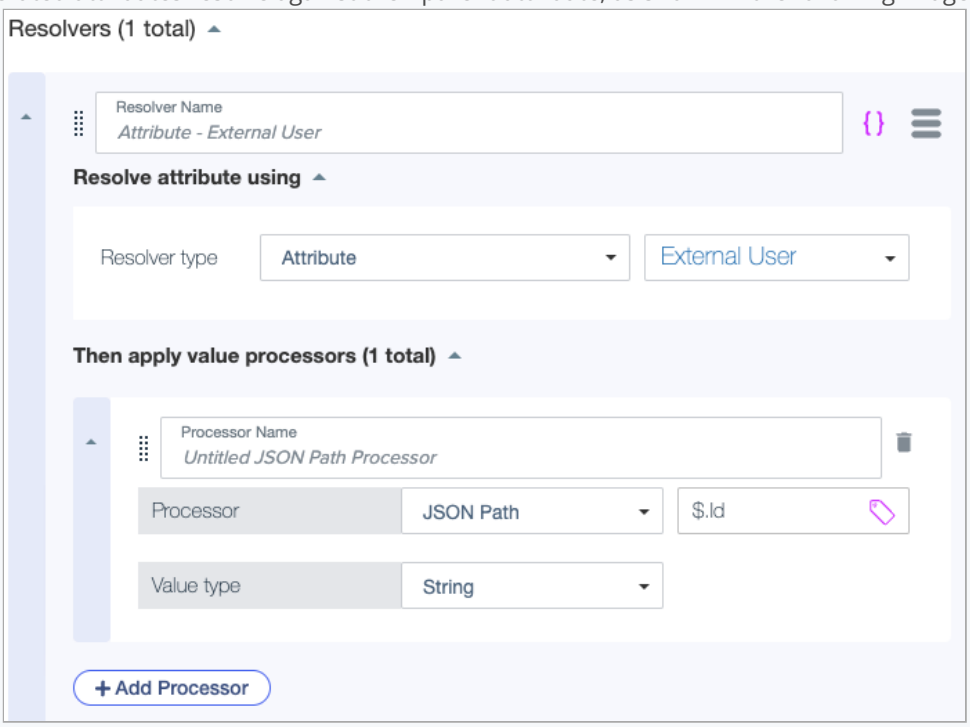
   Generated attributes are nested under the parent attribute on the **Attributes** tab.

Copyright © 2025 Ping Identity Corporation



Note

The generated attributes resolve against their parent attribute, as shown in the following image.



Interpolating authorization attributes

Attribute interpolation allows you to include attribute references in input fields and expressions.

About this task

PingOne Authorize resolves the value of the referenced attribute, replacing the attribute reference with the value itself. You can include text along with multiple attribute references. Use attribute interpolation in the following places:

- Fields that have the **Label** ( ) icon, such as service connector input fields

- JSON Path, SpEL, and X Path processors
- Statement payloads
- Inputs in REST service bodies

Steps

1. To open the attribute menu, enter two open curly brackets (`{{`) in a field that allows attribute interpolation.

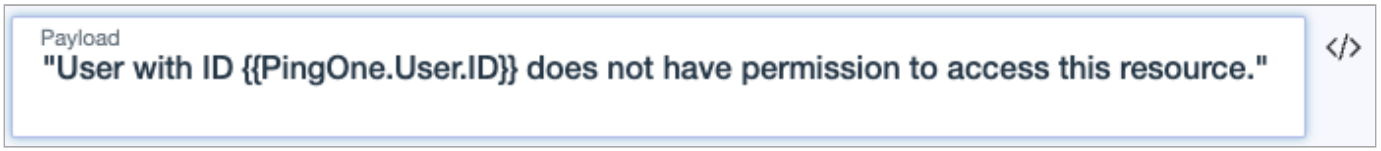
2. Enter the full path to the attribute, or select an attribute in the menu. To move to the next level in the menu, select **choose a nested attribute**.

3. To complete the reference, enter two closing curly brackets (`}}`) or select **}} complete expression** in the menu.

   Result:

   The following image shows an example of a completed attribute reference.

Copyright © 2025 Ping Identity Corporation



Adding repetition settings to an authorization attribute

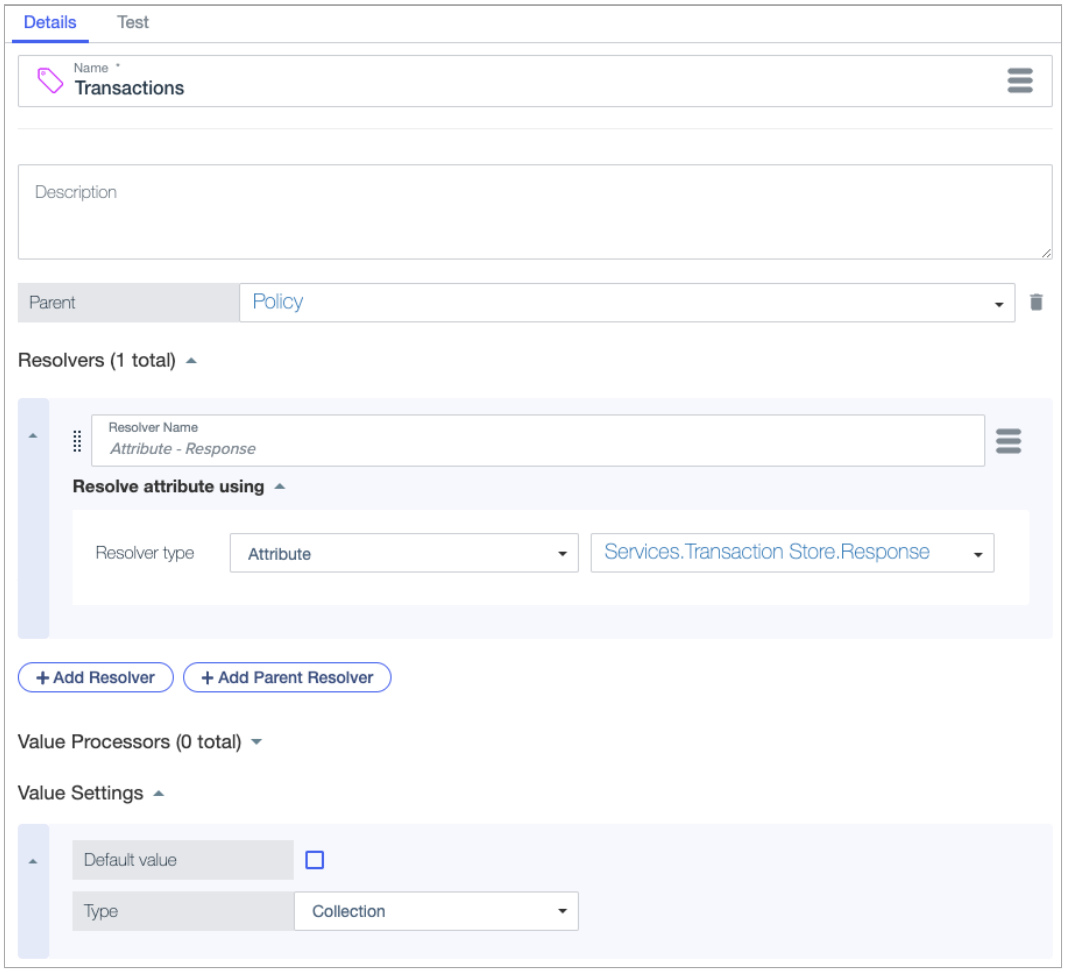
Add repetition settings to existing attributes to resolve attribute values from collections.

Before you begin

Add an attribute that serves as the repetition source.

> **Note**
>
> The value setting **Type** for the repetition source attribute must be **Collection**.

As an example, consider the following attribute that retrieves a collection of payment transactions from a service response. This attribute will serve as the repetition source for a repeating attribute that gets a transaction amount.



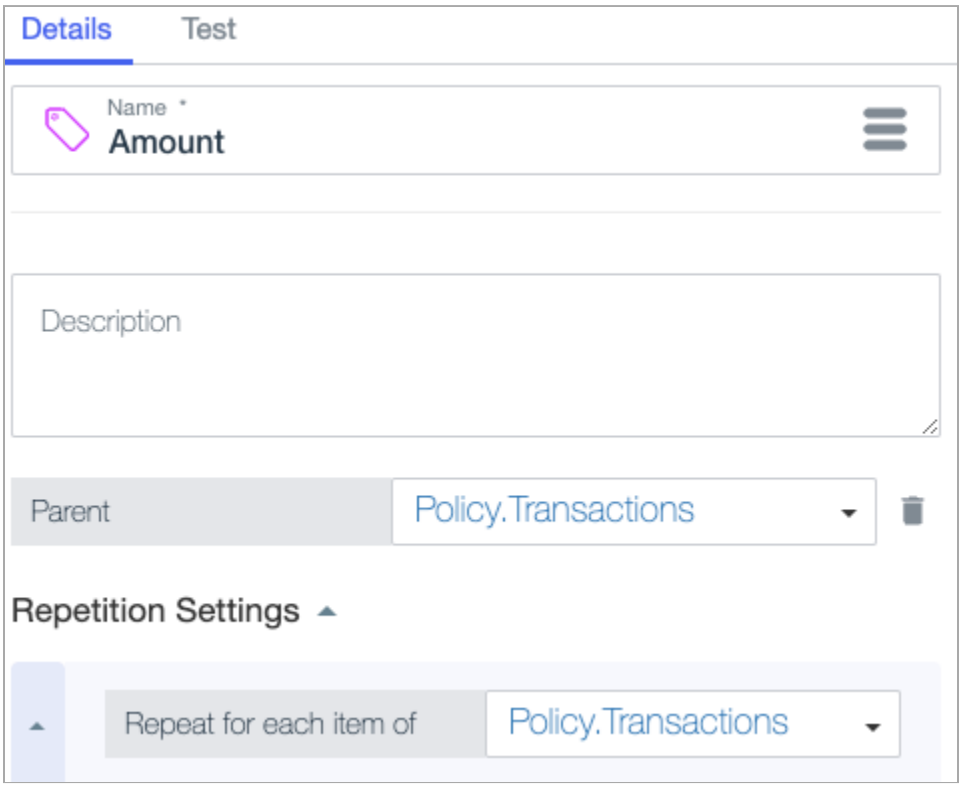
About this task

A repeating attribute requires a repetition source that points to a collection. To get values from each repetition of the collection, the repeating attribute must have a resolver set to **Current Repetition Value**.

> **Note**
>
> You can also use repeating attributes in named conditions and named processors. If an attribute uses a named condition or value processor, any repeating attributes referenced in the condition or value processor must have the same repetition source as the attribute itself.

Steps

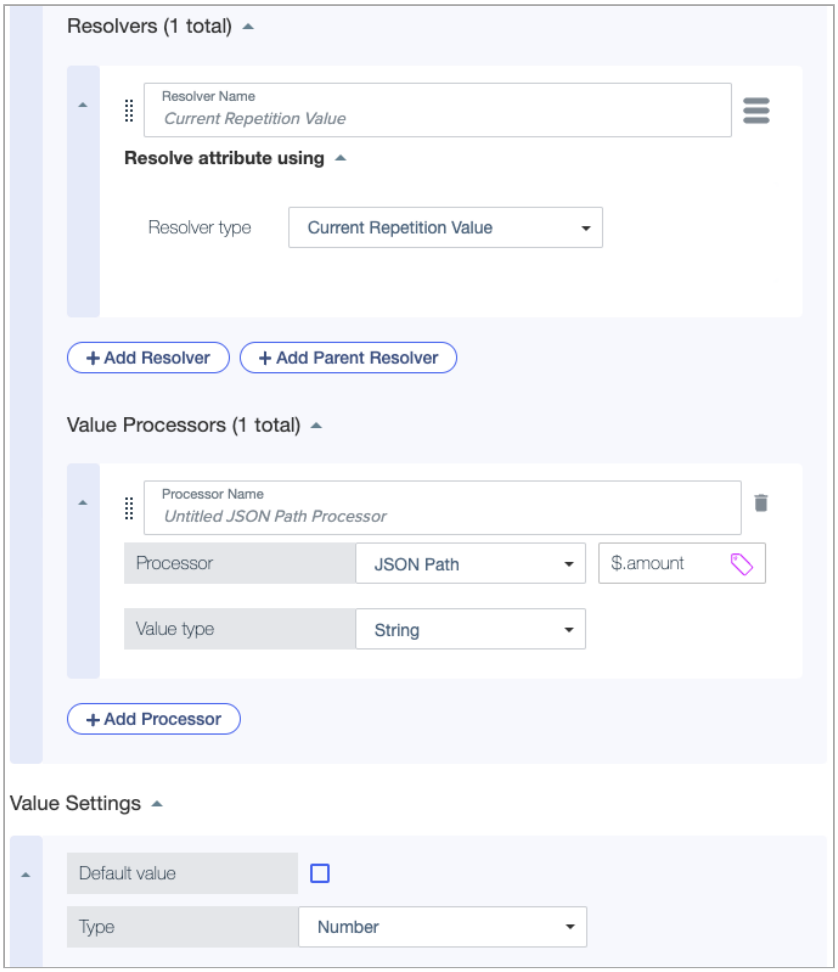
1. Go to **Authorization** > **Trust Framework** and click the **Attributes** tab.
2. Select the attribute to which you want to add repetition settings.
3. Click the hamburger menu in the **Name** field and select **Add repetition settings**.
4. In the **Repeat for each item of** list in the **Repetition Settings** section, select a repetition source attribute.



5. Expand **Resolvers** and click **+ Add Resolver**.
6. In the **Resolver type** list, select **Current Repetition Value**.

   This resolves the attribute against individual items in the collection.

Copyright © 2025 Ping Identity Corporation



7. Click **Save changes**.

Deleting an attribute

Delete PingOne Authorize attributes that you no longer need.

Before you begin

Before you delete an attribute, view dependents to see where the attribute is used and ensure that deleting the attribute doesn't introduce unintended consequences. You must remove references to the attribute before you can delete it.

About this task

> **Note**
>
> - You can't delete a generated attribute that resolves against a connector service. This type of attribute is automatically deleted when the associated connector service is deleted.
> - The **Shield** ( ) icon indicates that an attribute is system-owned and can't be deleted.

Steps

1. Go to **Authorization** > **Trust Framework** and click the **Attributes** tab.

2. Click the attribute that you want to delete.
3. Click **Delete Attribute**.
4. In the confirmation box, click **Yes**.

Authorization services

Services connect PingOne Authorize with data sources, such as APIs and information points, that provide information used to make context-aware authorization decisions.

Service connections augment authorization events with real-time data. Policy authors don't use information from a service directly in policies. Instead, services are a source of data for the attributes used in policy evaluations.

After you connect a service to PingOne Authorize, make sure that you add or generate attributes that store values resolved from the service. Learn more in Authorization attributes.

Service types

PingOne Authorize supports the following types of service connections.

HTTP services

These services connect to HTTP endpoints accessible over the public internet.

> **Note**
> If you're using an Authorize gateway for decision evaluations, you can make calls to on-premise services and information points in your organization's infrastructure. Learn more in Authorize gateways and Policies published to Authorize gateways.

HTTP services can send and receive text, JSON, and XML content. You can send custom headers with any request, and configure basic, bearer token, or OAuth 2.0 Client Credentials authentication methods for service-to-service authentication.

Connector services

These services consume information from other services provided by the PingOne platform. Learn more about attributes that are automatically generated when you connect to a PingOne service in Generating an attribute.

The PingOne Protect Connector service pulls in risk signals for use in authorization policies.

> **Note**
> This Connector service requires a PingOne Protect license.

LDAP Gateway services

These services connect to user information stored in external LDAP directories, such as PingDirectory, PingOne Advanced Identity Cloud (formerly ForgeRock Identity Cloud), or Microsoft Active Directory. You can use LDAP Gateway services for use cases such as:

- Retrieving a user's profile information

Copyright © 2025 Ping Identity Corporation

- Retrieving a user's groups

PingOne Authorize converts information received from an LDAP directory to JSON, making it easy to use this information in attributes and authorization policies.

Testing service integrations

On the **Test** tab for a service, you can test service integrations to validate output values.

Connecting a service

Connect PingOne Authorize to HTTP, PingOne Connector, or LDAP Gateway services to define data integrations.

Service connections in PingOne Authorize enable you to augment authorization events with real-time data. For example, you can use signals obtained from a risk service connection in a policy that determines whether a device requires step-up authentication.

Steps

1. In the PingOne admin console, go to **Authorization > Trust Framework**.
2. On the **Services** tab, click the **+** icon and select **Add New Service**.
3. Define general information for the service:
    1. Enter a unique **Name** for the service.

       The following characters are not allowed in the name:

       - Period (.)
       - Curly bracket ({ })
       - Pipe (|)
    2. (Optional) For **Description**, enter a description of the service's purpose.

       The description is only visible on the **Services** tab, but it can help policy authors understand how to use the service in policies.
    3. (Optional) To nest the service under a parent in the tree, in the **Parent** list, select a parent service.

       Nesting helps group related services together. You can move the service to another location in the tree by selecting a different parent service. To remove nesting, click the **Delete** icon and leave **Parent** blank.
4. Select a **Service Type**.

   Choose from:

   - **None**: This is for a parent service. Nest other services under a parent to help organize services in the tree structure. There are no additional settings to complete for this type of service. If you select **None**, skip to step 9.
   - **HTTP**: Connects to HTTP endpoints accessible over the public internet. Learn more about HTTP service settings in Connecting an HTTP service.
   - **Connector**: Connects to PingOne services. Learn more about Connector service settings in Connecting to PingOne Protect.

Copyright © 2025 Ping Identity Corporation

- **LDAP Gateway**: Connects to an external LDAP directory, such as PingDirectory, PingOne Advanced Identity Cloud, or Microsoft Active Directory. Learn more about LDAP Gateway service settings in Connecting an LDAP Gateway service.

5. (Optional) In the Value Settings section, define the data **Type** for the data returned by the service.
   - The default data type for HTTP services is **String**.
   - Because Connector services always return JSON, the default data type is **JSON**, and you cannot change it.
   - LDAP Gateway services return JSON.
6. (Optional) In the **Timeout Settings** section, enter a **Request Timeout** value if you want to change the number of milliseconds that PingOne Authorize waits for a service request to complete.

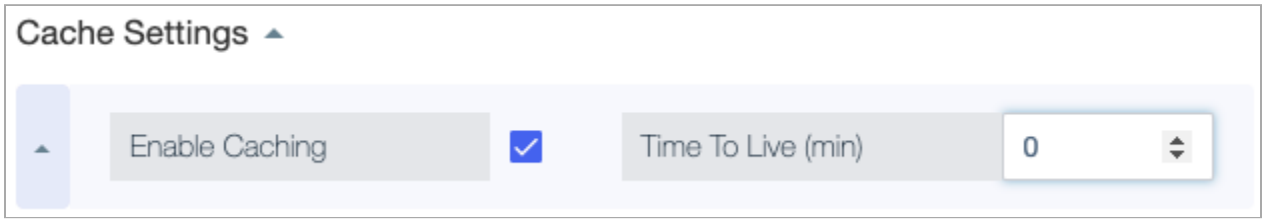
   The request timeout range is 0 - 3000 milliseconds and the default is 2000 milliseconds. If the timeout elapses before there is a successful service response, the service request is canceled, resulting in a timeout error.
7. (Optional) In the **Rate Limits** section, enter a **Requests per Second** value to change the maximum number of requests that decision points can make to the service per second.

   The default value is 1000000.

   > **Note**
   > The **Concurrent Requests** field has been deprecated and changing it has no effect.

8. (Optional) Enable caching for the service.

   Caching improves system performance by storing data returned from a service and reusing it on subsequent service requests until the cache expires.

   1. Select the **Enable Caching** checkbox.
   2. For **Time to Live**, enter the number of minutes that you want to store data retrieved from the service in the cache.

      The maximum value is 1440 minutes or 1 day.
9. Click **Save Changes**.

   > **Note**
   > You can copy a service for reuse by selecting **Make Copy** in the service's hamburger menu. If you copy a service with children, only the parent is duplicated.

Next steps

Test the service connection. Learn more in Testing Trust Framework elements.

Copyright © 2025 Ping Identity Corporation

Connecting an HTTP service

Configure HTTP settings to connect PingOne Authorize to an HTTP service.

Before you connect to an HTTP service, you can add attributes that store values for service settings, such as the endpoint URL for an HTTP request. Storing settings as attributes is useful if the values are dynamic, or if you want to use different values during testing. For example, during testing, you can override a production REST API used in an HTTP service with a test API.

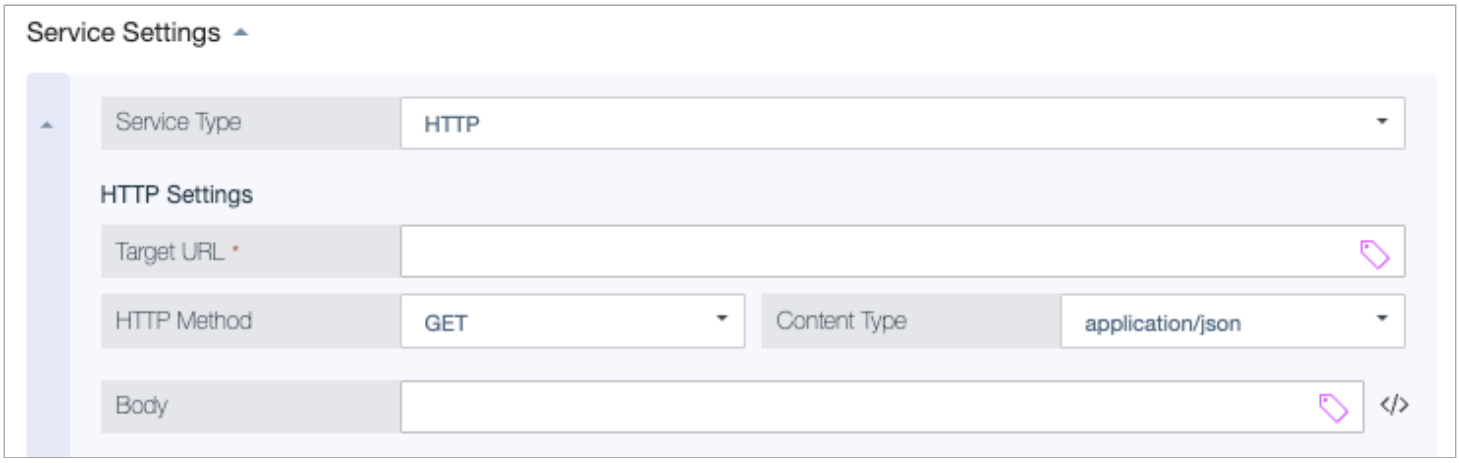
> **Important**
>
> If the service requires OAuth 2.0 Client Credentials authentication, you must add an attribute that stores the external service's client secret before you configure service settings. You can also add attributes that store other client credentials, such as the client ID and token endpoint.

After you finish configuring the service, test the service connection. To make the service response available in policies, add attributes that resolve against the service and process the response to extract required values.

Add a service, configure the following service settings, and then configure general settings to finish the service connection.

HTTP Settings

HTTP service requests can send and receive text, JSON, and XML content.



HTTP settings

Setting	Description
Target URL	The URL for the REST endpoint that the decision point accesses in the HTTP request. To include an attribute anywhere in the URL, wrap the full name of the attribute in double curly brackets. **Note** Because there is no URL encoding in service settings, use a PingOne expression language (SpEL) processor in the attribute definition to perform URL encoding. For example, you can use a SpEL processor similar to this in the attribute resolver: `#string.asUrlEncoded(#this.value)`
HTTP Method	The action performed in the HTTP request. Options are **GET**, **POST**, **PUT**, **DELETE**, and **HEAD**.
Content Type	The media type of the content in the HTTP request. Options are **application/json**, **application/xml**, **text/html**, and text.
Body	The body to send with the HTTP request. You can include attributes anywhere in the body, with no escaping, by wrapping the full name of the attribute in double curly brackets. **Note** You can configure HTTP headers to use additional authentication mechanisms. For example, you have full control over the `Authorization` header and other headers.

Headers

You can send any number of custom header key-value pairs with a request. To make the header dynamic, select an attribute for the header value.

To add a header:

1. Click **+ Header**.
2. Enter the header **Key**.

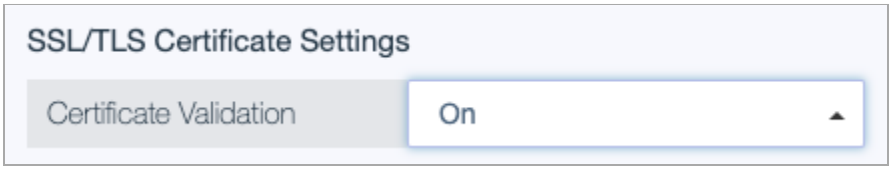
   The key is a fixed string.

Copyright © 2025 Ping Identity Corporation

3. For the header **Value**, enter a constant value or click to select an attribute.

SSL/TLS Certificate Settings

Certificate validation in PingOne Authorize allows you to enable or disable SSL and TLS certificates when connecting to SSL or TLS-based services.



SSL and TLS certificate settings apply when validating the certificate or certificate chain sent from the server. The following **Certificate Validation** options are available:

- **On**: Performs TLS validation when connecting to the service. Select this option when you connect to a service that has a certificate issued from a valid certificate authority. This setting is enabled by default.
- **Off**: Skips server certificate validation and allows initiation of the connection without validation.

HTTP authentication methods

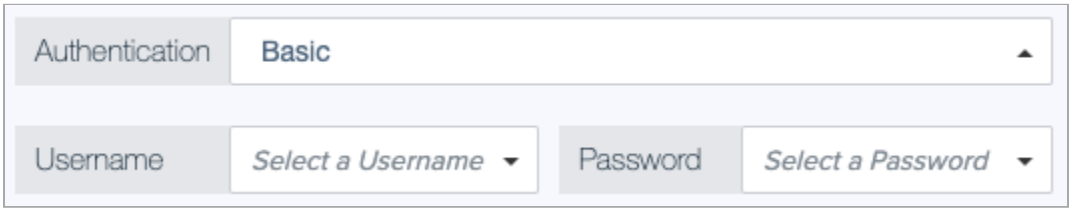
By default, no authentication method is selected for HTTP service requests. To authenticate such requests, you can use basic authentication with a username and password, a bearer token, or the OAuth 2.0 Client Credentials flow.

None

With this method, no authorization header is sent with the HTTP request. This is the default option.

Basic

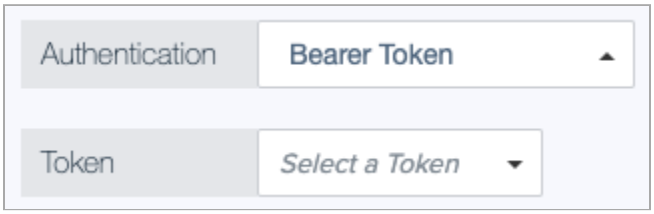
For basic authentication, provide a username and password.



Bearer Token

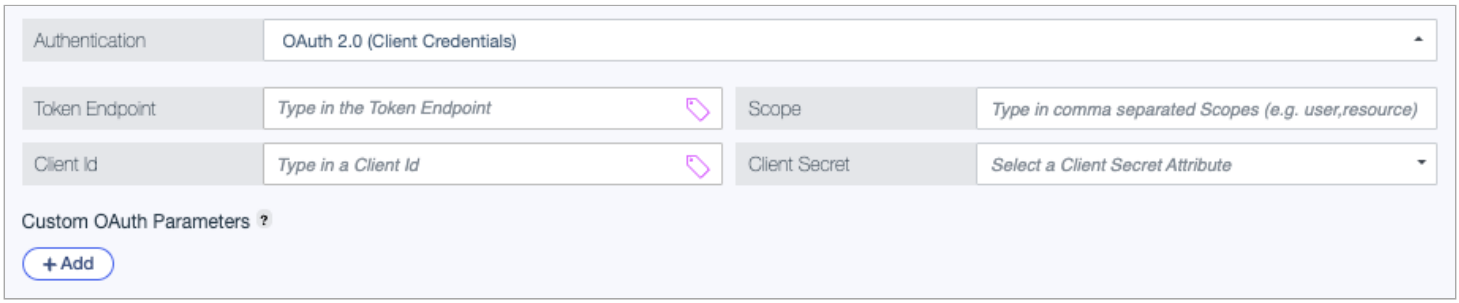
For bearer authentication with a static token, select an attribute that stores the authorization token to send with the HTTP request.

Copyright © 2025 Ping Identity Corporation



OAuth 2.0 (Client Credentials)

For authentication with the OAuth 2.0 Client Credentials flow, configure client credentials to exchange for an access token.



PingOne Authorize manages the authentication process as follows:

1. PingOne Authorize requests an access token for the external service by sending client credentials, including any scopes, in a POST request to the authorization server's token endpoint.

   PingOne Authorize always sends client credentials in the HTTP request body (`client_secret_post`) and doesn't support using the `Authorization` header (`client_secret_basic`).

   > **Important**
   >
   > If you're using an HTTP service to access PingOne APIs, configure your PingOne worker application to use `client_secret_post` to ensure that client credentials are sent in the body of the token request, as expected by the service.
   > If the worker application is configured to use `client_secret_basic` , requests for access tokens from PingOne Authorize will fail with an authentication error.

2. The authorization server validates the client credentials and provides an access token, which PingOne Authorize caches. When the external service no longer accepts this token, PingOne Authorize reuses the client credentials to get a new one.

3. In an HTTP service request, PingOne Authorize provides the access token in the `Authorization` header, authenticates with the HTTP service, and retrieves the requested information from the service.

Before you configure the following settings, add an attribute that stores the client secret. You can also add attributes that store other client credentials.

- **Token Endpoint**: The token endpoint URL for the authorization server that grants an access token. For example, `https://{domain}/oauth*/token` .
- **Scope** (optional): The scopes to request in the access token. Scopes are optional and can be used to limit the permissions of a token in the connected service. Separate scopes with commas and no spaces.
- **Client Id**: Enter the external service's unique client identifier, or select an attribute that stores this value.
- **Client Secret**: Select an attribute that stores the external service's client secret.

Copyright © 2025 Ping Identity Corporation

- **Custom OAuth Parameters** (optional): A list of custom key-value pairs representing additional parameters sent in the body of the token endpoint request. This level of customization is useful when integrating with authorization servers that enforce specific configuration constraints.

  The **Key** must be a fixed string. For the **Value**, enter a constant value or click to select an attribute.

> **Note**
>
> Custom OAuth parameters have the following constraints:
>
> - You can define up to 10 key-value pairs.
> - Keys cannot contain spaces in any position.
> - Keys must be between 1 - 128 characters in length.
> - You cannot use any of the following values as a key (case-sensitive):
> - `client_id`
> - `client_secret`
> - `scope`
> - `grant_type`

Value processors

You can define value processors to transform data returned by the HTTP service. Learn more in Processors.

Connecting to PingOne Protect

Establish a connection between PingOne Authorize and PingOne Protect to use risk signals in authorization policies and provide risk evaluation feedback.

Before you begin

- Make sure PingOne Protect is in your PingOne environment. Learn more in Getting up and running with PingOne Protect.
- If you're using an external user directory, create attributes that store values for service input settings, such as the ID and IP address of the user whose risk is being evaluated.

About this task

PingOne Protect monitors end-user requests and generates a risk score of low, medium, or high, based on user behavior and device context. Service Connectors enable you to include these risk assessments in dynamic authorization policies. For example, if a risk score is medium, the authorization policy might direct the user to complete step-up authentication with additional MFA methods. When the risk score is high, the policy might deny access to the resource.

Copyright © 2025 Ping Identity Corporation

PingOne Protect provides the capability to evaluate risk for a transaction, and the capability to provide feedback that improves risk models. Add a separate PingOne Protect service Connector in PingOne Authorize for each capability.

Configure the following Connector settings, then configure general settings to finish the service connection.

Steps

1. Add a service and select **Connector** as the **Service Type**.
2. For the **Connector** type, select **PingOne Protect**.
3. For **Capability**, select one of the following:

   Choose from:

   - **Create Risk Evaluation**: Evaluate risk for a specific transaction based on predictors and risk models.
   - **Update Risk Evaluation**: Provide feedback to PingOne Protect to improve the accuracy of the machine learning models. Perform this update after every risk evaluation.

   > **Note**
   > Changing the **Connector** type or **Capability** clears service settings. If you want to keep service settings, make sure you save the Connector before you change the type or capability.

4. Complete **Inputs** to define the API call to the PingOne Protect service.

   For each input, enter a constant or click to select an attribute. Constants are strings, but you can also enter numbers, enums, JSON objects, and attribute references. You can leave optional constants blank. If you switch to attribute selection, you must select an attribute, even if the input is optional.

   Learn more about the fields passed in the service request in Risk Evaluations.

Inputs	Description
User ID	ID of the user whose risk is being evaluated. If this is a PingOne user, make sure the ID belongs to a user in the current PingOne environment.
User Type	For PingOne users, enter `PING_ONE`. For users in an external directory, enter `EXTERNAL`. These are the only valid values for this input.
IP Address	The IP address of the user whose risk is being evaluated.
Application ID	Optional: ID for the application or resource the user wants to access.
Application Name	Optional: Name of the application or resource the user wants to access.
Session ID	Optional: Unique session ID for the transaction event.
Browser Data	Optional: An object that specifies browser fingerprint attributes. You can also use FingerprintJS to retrieve browser data.

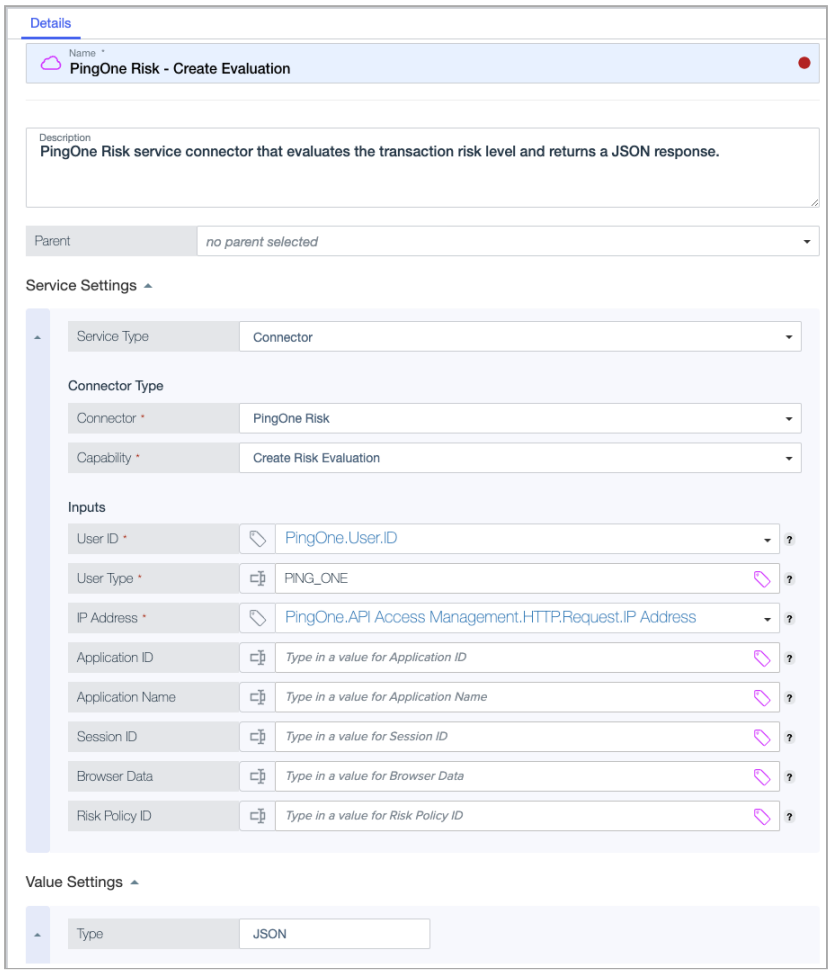
Copyright © 2025 Ping Identity Corporation

Inputs	Description
Risk Policy ID	Optional: The risk policy set used for the risk evaluation. If this is blank, the risk evaluation uses the default risk policy set for the current environment.
Completion Status	This input is for the **Update Risk Evaluation** capability. Status of the risk evaluation you're updating. Enter `SUCCESS` or `FAILED`. These are the only valid values for this input.
Risk Evaluation ID	This input is for the **Update Risk Evaluation** capability. The ID of the risk evaluation you're updating. You can generate an attribute for the ID from the service response.

Tip

Tooltips provide additional guidance for inputs. If you're having problems with invalid requests to PingOne Protect, make sure the service inputs are correct.

The following image shows an example PingOne Risk Connector service.

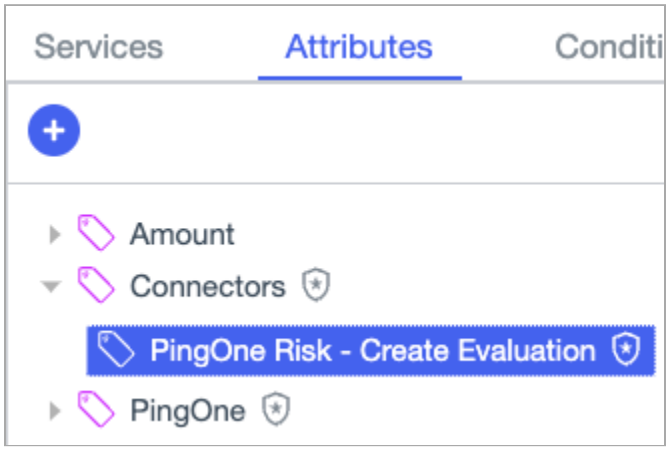


5. Finish general settings for the service.

Copyright © 2025 Ping Identity Corporation

Result

When you save the Connector service, PingOne Authorize automatically generates an attribute that resolves against the service. This attribute has the same name as the Connector service. Connector attributes are listed directly under **Connectors** on the **Attributes** tab in the **Trust Framework**.



You can generate child attributes from this attribute to extract service response values, such as the risk level, for use in authorization policies. When you update a Connector service, PingOne Authorize updates the generated Connector attribute associated with the service.

Connecting an LDAP Gateway service

Connect PingOne Authorize to a PingOne gateway to access user information stored in an external, on-premise LDAP directory.

Before you begin

You must configure an LDAP gateway connection to allow PingOne to communicate with the LDAP directory that contains the user information that you want to access.

About this task

PingOne gateways provide access to user identities and data stored in an external directory. After you configure an LDAP gateway connection in PingOne, add an **LDAP Gateway** service connection in PingOne Authorize to access user profile and group information stored in the on-premise LDAP directory.

> **Note**
> Only LDAP gateway connections are supported. You cannot connect to other gateway types, such as RADIUS Gateway.

PingOne Authorize converts user information retrieved from an LDAP Gateway service to JSON. The following is an example response from an LDAP Gateway service connection:

Copyright © 2025 Ping Identity Corporation

```
{
  "entries": [
    {
      "_dn": ["cn=Philip J. Wilson,ou=people,dc=example,dc=com"],
      "objectClass": ["inetOrgPerson","organizationalPerson","person","top"],
      "cn": ["Philip J. Wilson"],
      "sn": ["Wilson"],
      "description": ["Human"],
      "displayName": ["Wilson"],
      "employeeType": ["Loan Officer"],
      "givenName": ["Philip"],
      "mail": ["wilson@example.com"],
      "ou": ["Commercial Banking"],
      "uid": ["wilson"],
      "userPassword": ["xx"],
      "entryDN": ["cn=philip j. wilson,ou=people,dc=example,dc=com"],
      "entryUUID": ["3d7d9bfa-4d85-4414-94bc-ed9cfbe717b9"],
      "subschemaSubentry": ["cn=schema"],
      "creatorsName": ["cn=Internal Root User"],
      "createTimestamp": ["20230516132411.457Z"],
      "modifiersName": ["cn=Internal Root User"],
      "modifyTimestamp": ["20230516132411.457Z"]
    }
  ]
}
```


You can use JSON Path processors in attributes to extract the information that you require from the service response for use in authorization policies.

When you add an LDAP Gateway service, configure the following **LDAP Gateway** settings, then configure general settings to finish the service connection:

Steps

1. Go to **Authorization > Trust Framework** and add a service.
2. For the **Service Type**, select **LDAP Gateway**.
3. For **Gateway**, select the LDAP gateway connection that you set up in PingOne.
4. For the **Search Base DN**, enter the distinguished name for the directory information tree location where you want PingOne Authorize to start looking for user information.

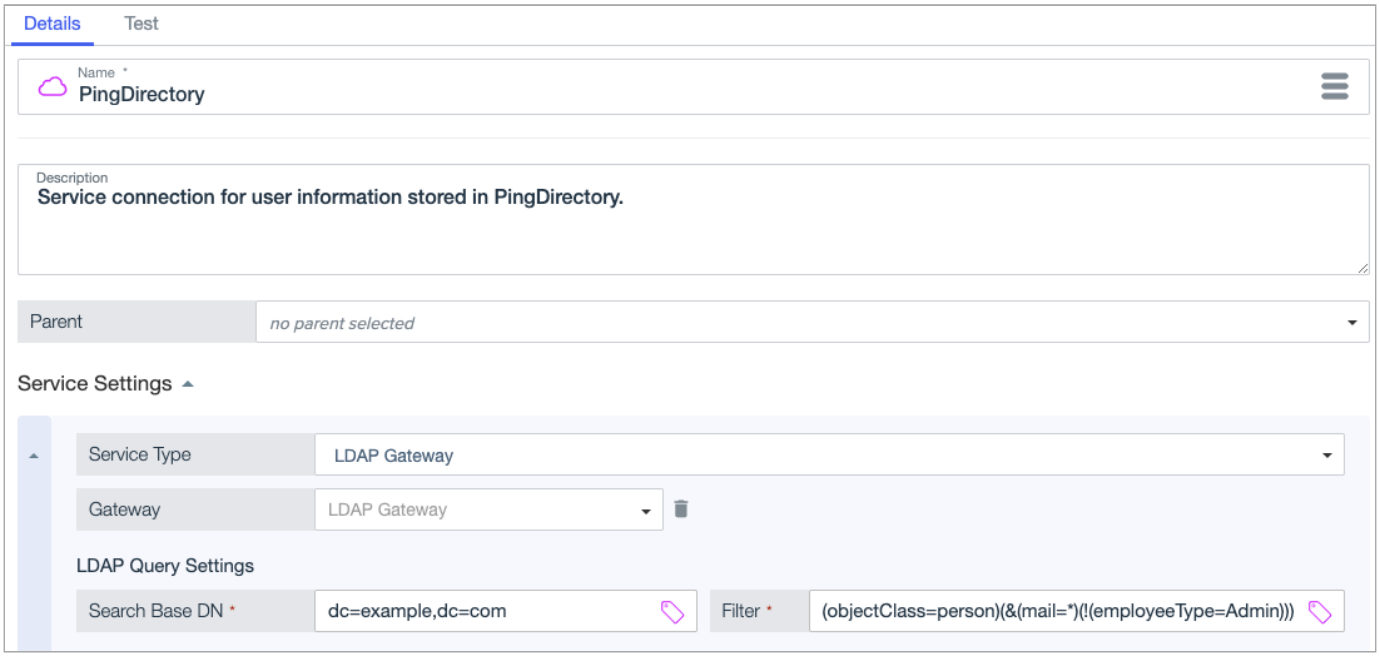
   Example:

   The search base in the following is the domain component example.com:

   ```
   dc=example,dc=com
   ```

5. To limit the scope of the results returned from the LDAP directory, enter a **Filter**.

Copyright © 2025 Ping Identity Corporation



Example:

This filter returns users that have email addresses, but are not administrators:

```
(objectClass=person)(&(mail=*)(!(employeeType=Admin)))
```

6. Finish general settings for the service.

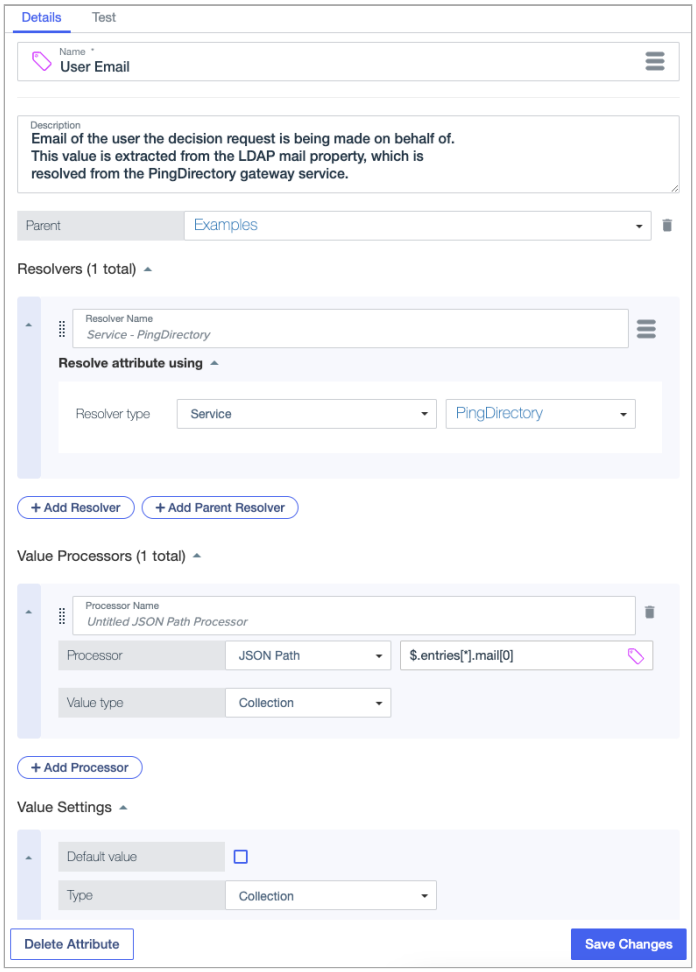
Next steps

After you configure the gateway connection, you can add attributes that extract information from the service response for use in authorization policies.

Example: Retrieve user profile information

The following attribute extracts user email addresses from the PingDirectory service. The JSON Path expression `$.entries[*].mail[0]` returns an array of mail strings, such as `["wilson@example.com"]`.

Copyright © 2025 Ping Identity Corporation



Example: Retrieve user groups

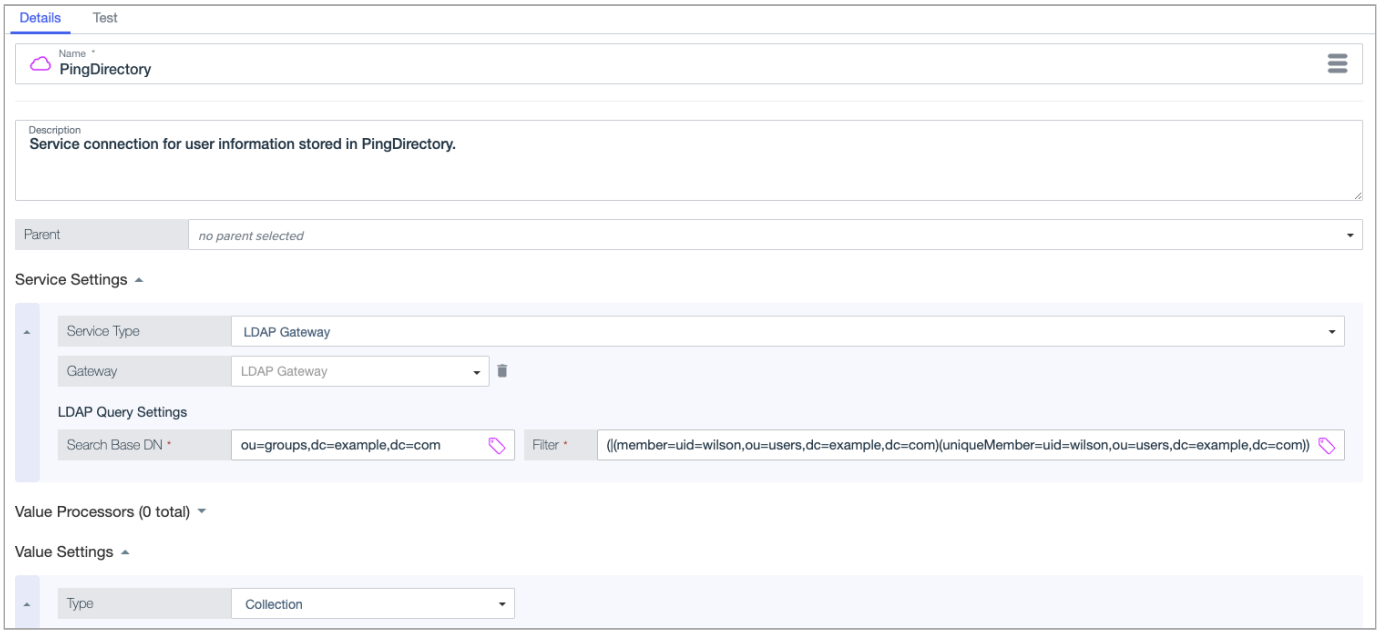
To retrieve a user's group memberships:

1. Set the **Search Base DN** in the PingDirectory service to `ou=groups,dc=example,dc=com`.
2. Enter a **Filter** to retrieve a list of groups for a particular user, such as Philip Wilson.

   This filter returns a list of the static groups to which Philip Wilson belongs.

```
(|(member=uid=wilson,ou=users,dc=example,dc=com)
(uniqueMember=uid=wilson,ou=users,dc=example,dc=com))
```

Copyright © 2025 Ping Identity Corporation



To retrieve all of the users that are a member of a group, such as loan officers, enter the following settings for the PingDirectory service:

- **Search Base DN**: `ou=people,dc=example,dc=com`
- **Filter**: `(isMemberOf=cn=loanAdmin,ou=groups,dc=example,dc=com)`

To retrieve a particular user if they are a member of a group, such as loan officers, enter the following settings for the PingDirectory service:

- **Search Base DN**: `uid=wilson,ou=people,dc=example,dc=com`
- **Filter**: `(isMemberOf=cn=loanAdmin,ou=groups,dc=example,dc=com)`

Authorization service caching

Caching improves decision evaluation performance by storing data retrieved from services for faster retrieval on subsequent service requests.

Caching improves latency and throughput by reducing the number of service calls the decision service makes to satisfy decision requests. A service is a good candidate for caching if service response values don't change very often.

If you're using an Authorize gateway for decision evaluations, go to Service caching for Authorize gateway instances.

How service caching works

When the decision service requests information from a service, it caches the service response if the data has not already been cached. On subsequent service requests, instead of invoking the service again, the decision service uses the cached data until the cache expires.

Copyright © 2025 Ping Identity Corporation

The cache key includes a hash of service settings and interpolated attribute values. The decision service invokes the service and caches the service response under a new key when a value in the service request changes. For example, when there's a new parameter in the request body, or an attribute value is resolving differently. The cache value contains the service response as strings.

PingOne Authorize maintains the service response in the cache for the period of time you define in the **Time to live** setting for a service. New cache keys are generated when you change any service setting and publish a new version. Returning to previous service settings might restore an older cache key and the previous version of the cache.

The service response size limit is 1 MB. Learn more about service limits in Service configuration constraints.

> **Important**
>
> Cache entries are stored in memory and do not persist during a restart or outage.

Configuring service caching

You can configure cache settings for individual services when you add or edit a service. For more information, see Connecting a service.

You cannot clear the cache manually.

> **Important**
>
> Service cache settings in PingOne Authorize override any cache control headers in the HTTP response. This can result in:
>
> - Caching when the headers indicate that the response shouldn't be cached
> - A delay in retrieving an updated service response because the cache isn't updated until it expires

Service configuration constraints

Service configuration constraints in PingOne Authorize help protect against potential vulnerabilities from service integrations.

The following table lists constraints for service integrations in PingOne Authorize. If a `ServiceExecutionException` occurs when a constraint is exceeded, an error message is listed in the table. You can review processing errors on the **Services** tab in Recent decisions.

Constraint type	Limit	Error message
Service request size	1 MB	`Request size is too large`
Service response size	1 MB	`Response size is too large`
Service timeout	3 seconds	
Service types	HTTPS only	
User-Agent header	Hidden	

Copyright © 2025 Ping Identity Corporation

Constraint type	Limit	Error message
Access to certain hosts	Not permitted	`Host is forbidden`
HTTP redirects	Not supported	`Redirects are not supported`
Service retries	Not supported	

Deleting a service

Delete PingOne Authorize services that you no longer need.

Before you begin

Before you delete a service, view dependents to see where the service is used and ensure that deleting the service doesn't introduce unintended consequences. You must remove references to the service, such as in attributes, before you can delete the service.

About this task

> **Note**
>
> When you delete a Connector service, the generated attribute associated with the service is also deleted. You can't delete the service if the associated Connector attribute is referenced in other attributes.

Steps

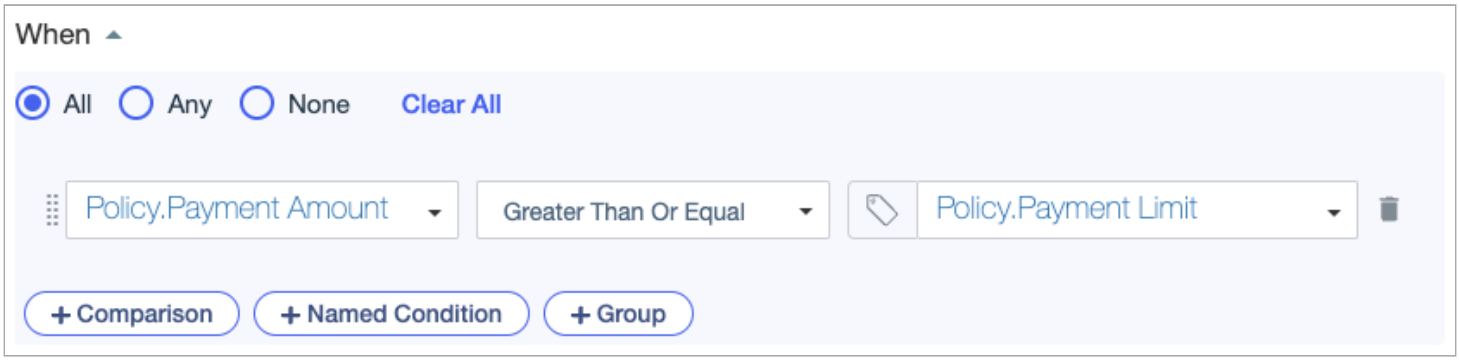
1. Go to **Authorization** > **Trust Framework** and click the **Services** tab.
2. Click the service you want to delete.
3. Click **Delete Service**.
4. In the confirmation box, click **Yes**.

Authorization conditions

Use conditions in PingOne Authorize attributes, rules, and policies to define authorization logic by comparing one thing to another. Conditions evaluate to either `true` or `false`.

You can compare attributes, constant values, and regular expressions in conditions. Conditions can also serve as targets that define when a policy or rule applies to a decision request. For example, you can target a rule so it applies when a payment amount is greater than or equal to a payment limit.

Copyright © 2025 Ping Identity Corporation



When you define a condition, on the left side, select an attribute that represents unknown or variable information to be validated. On the right side, enter known or predefined criteria in the form of an attribute or constant value. This keeps logical statements consistent regardless of what's being compared.

If there are multiple conditions, the decision service evaluates them in order from top to bottom according to the following options for combining conditions:

- **All** is like adding an `AND` Boolean operator between conditions. When one condition evaluates to false, evaluation stops and the remaining conditions are not executed.
- **Any** is like adding an `OR` Boolean operator between conditions. When one condition evaluates to true, evaluation stops and the remaining conditions are not executed.
- **None** is like adding a `NOT` Boolean operator between conditions. This invokes the condition when none of the conditions are true.

You can drag collapsed conditions to rearrange them and change the order in which they're evaluated.

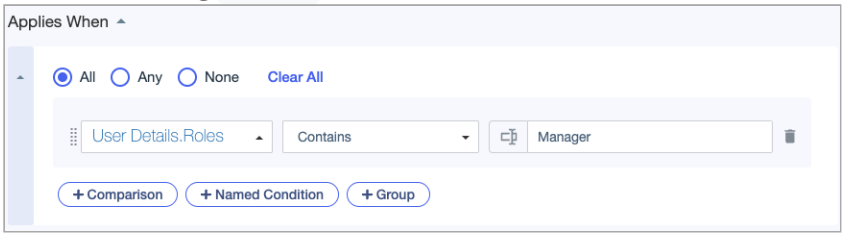
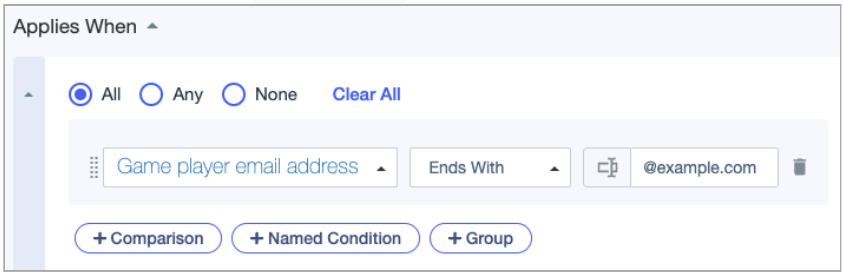
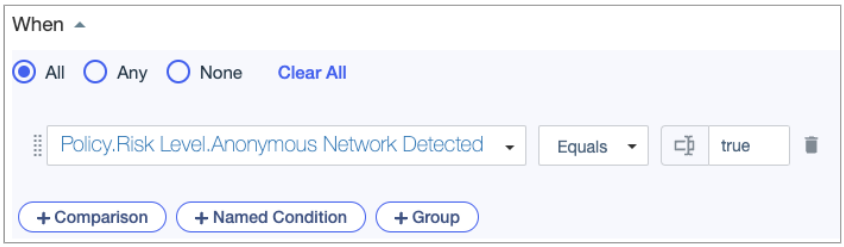
You can add conditions directly to resolvers and rules or define them on the **Conditions** tab as reusable named conditions.

Condition comparators

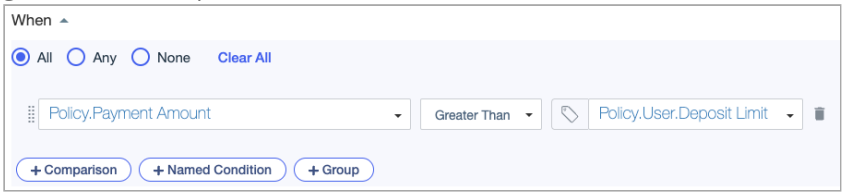
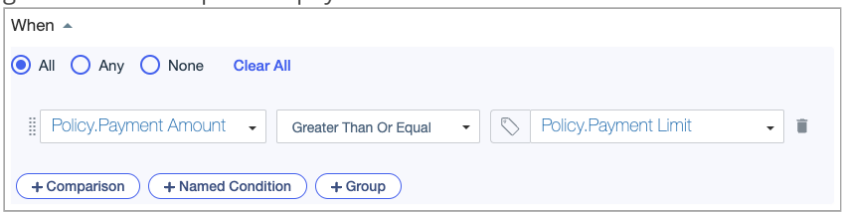
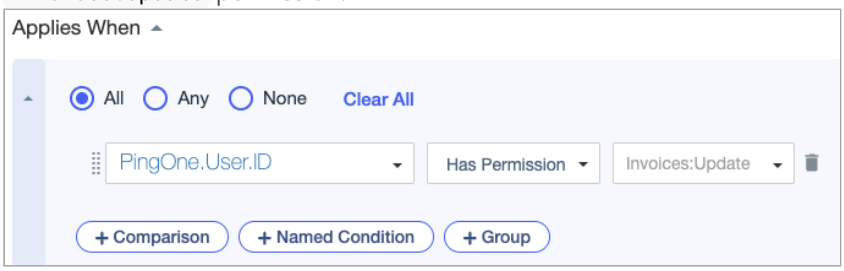
You can use the following comparators in condition comparisons.

> **Note**
>
> For simplicity, the table groups logical comparator pairs together, but you can only use one comparator at a time in a condition.

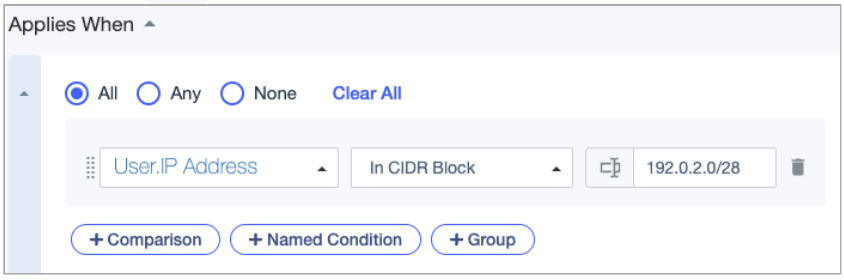
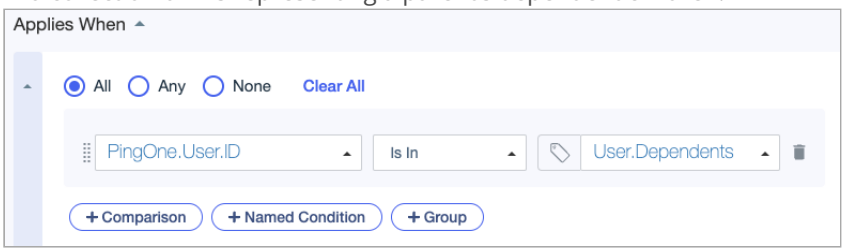
Copyright © 2025 Ping Identity Corporation

Comparator	Supported data types	Description
Contains **Does Not Contain**	Collection String	Checks whether a string or collection contains (or doesn't contain) another string. Use this comparator when you know part of a value that you want to check. For example, this condition evaluates to `true` if the user roles attribute contains the string `Manager`.  **Note** Matches for strings can differ from matches for collections. For example, the string `1234` contains the constant `23`, but the collection `[1234]` does not contain this constant. One possible matching collection for the constant `23` is `[21, 22, 23]`.
Ends With **Does Not End With**	String	Checks whether a string ends with (or doesn't end with) another string. For example, this condition evaluates to `true` if the user's email address ends with the domain `example.com`. 
Equals **Does Not Equal**	Boolean Collection Date Date Time Duration JSON Number Period String Time XML Zoned Date Time	Checks whether two values are equal (or not equal). For example, this condition evaluates to `true` if an anonymous network is detected. 

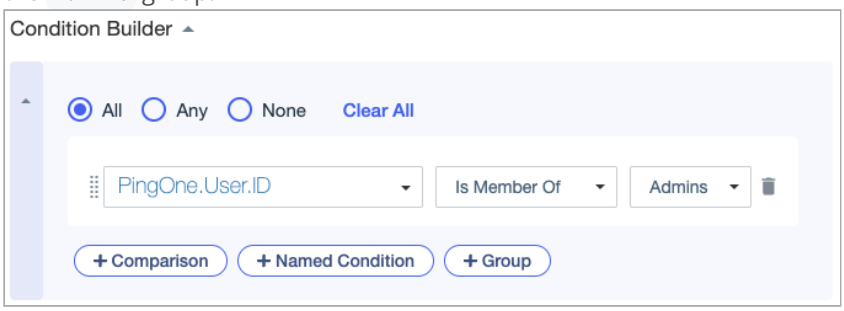
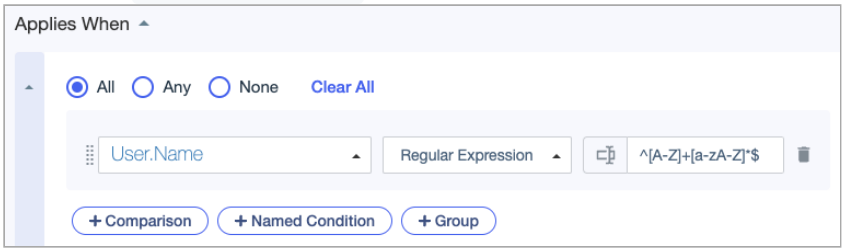
Copyright © 2025 Ping Identity Corporation

Comparator	Supported data types	Description
Greater Than **Less Than**	Boolean Date Date Time Duration Number String Time Zoned Date Time	Checks whether a value is greater than (or less than) another value. For example, this condition evaluates to `true` if a payment amount is greater than a deposit limit. 
Greater Than Or Equal **Less Than Or Equal**	Boolean Date Date Time Duration Number String Time Zoned Date Time	Checks whether a value is greater than or equal to (or less than or equal to) another value. For example, this condition evaluates to `true` if a payment amount is greater than or equal to a payment limit. 
Has Permission	String	Checks whether the PingOne user requesting access to a resource has a PingOne application permission. To check a permission in a comparison: 1. Select the **PingOne.User.ID** attribute. 2. Select the **Has Permission** comparator. 3. Select a PingOne permission from the list of application permissions that are available in the environment. For example, this condition evaluates to `true` if the user has the `Invoices:Update` permission.  **Note** This comparator relies on identity information provided by the PingOne SSO service. Make sure this service is deployed in your environment before you use this comparator.

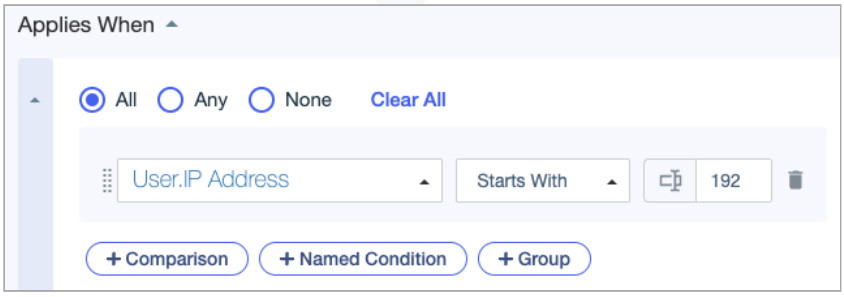
Copyright © 2025 Ping Identity Corporation

Comparator	Supported data types	Description
In CIDR Block **Not In CIDR Block**	String	Checks whether a user's IP address is in (or not in) an IP subnet range. IPv4 and IPv6 addresses are supported. To create a comparison: 1. Select an attribute that resolves to a valid IP address. 2. Select the **In CIDR Block** or **Not In CIDR Block** comparator. 3. Enter the IP address range as a constant or select an attribute that resolves to the IP address range. You must express the IP address range in Classless Inter-Domain Routing (CIDR) notation (the bitmask indicates the size of the routing prefix): `IP address/bitmask` For example, consider a condition that checks for IP addresses between 192.0.2.0 - 192.0.2.15. CIDR notation for this range is `192.0.2.0/28`. If the IP address attribute resolves to `192.0.2.1`, for example, the condition evaluates to `true`.  **Tip** For help expressing an IP address range in CIDR notation, use a CIDR calculator.
Is In **Is Not In**	Collection String	Checks whether a string or a collection is in (or not in) another collection. For example, this condition evaluates to `true` if the requesting user's ID is in a collection of IDs representing a parent's dependent children. 

Copyright © 2025 Ping Identity Corporation

Comparator	Supported data types	Description
Is Member Of **Is Not Member Of**	String	Checks whether the PingOne user requesting access to a resource is a member of (or not a member of) a PingOne group. To check for group membership in a comparison: 1. Select the **PingOne.User.ID** attribute. 2. Select the **Is Member Of** or **Is Not Member Of** comparator. 3. Select a PingOne group. You can search for groups. As you enter a search query, the group list shows matching results. For example, this condition evaluates to `true` if the user is a member of the `Admins` group.  **Note** These comparators rely on identity information provided by the PingOne SSO service. Make sure this service is deployed in your environment before you use these comparators.
Regular Expression	String	Checks whether a string matches a regular expression. For example, this condition evaluates to `true` if the user's name starts with a capital letter and only contains letters. The regular expression being matched is `^[A-Z]+[a-zA-Z]*$`. 

Copyright © 2025 Ping Identity Corporation

Comparator	Supported data types	Description
Starts With **Does Not Start With**	String	Checks whether a value starts with (or doesn't start with) another value. For example, this condition evaluates to `true` if the user's IP address starts with the network identifier `192`. 

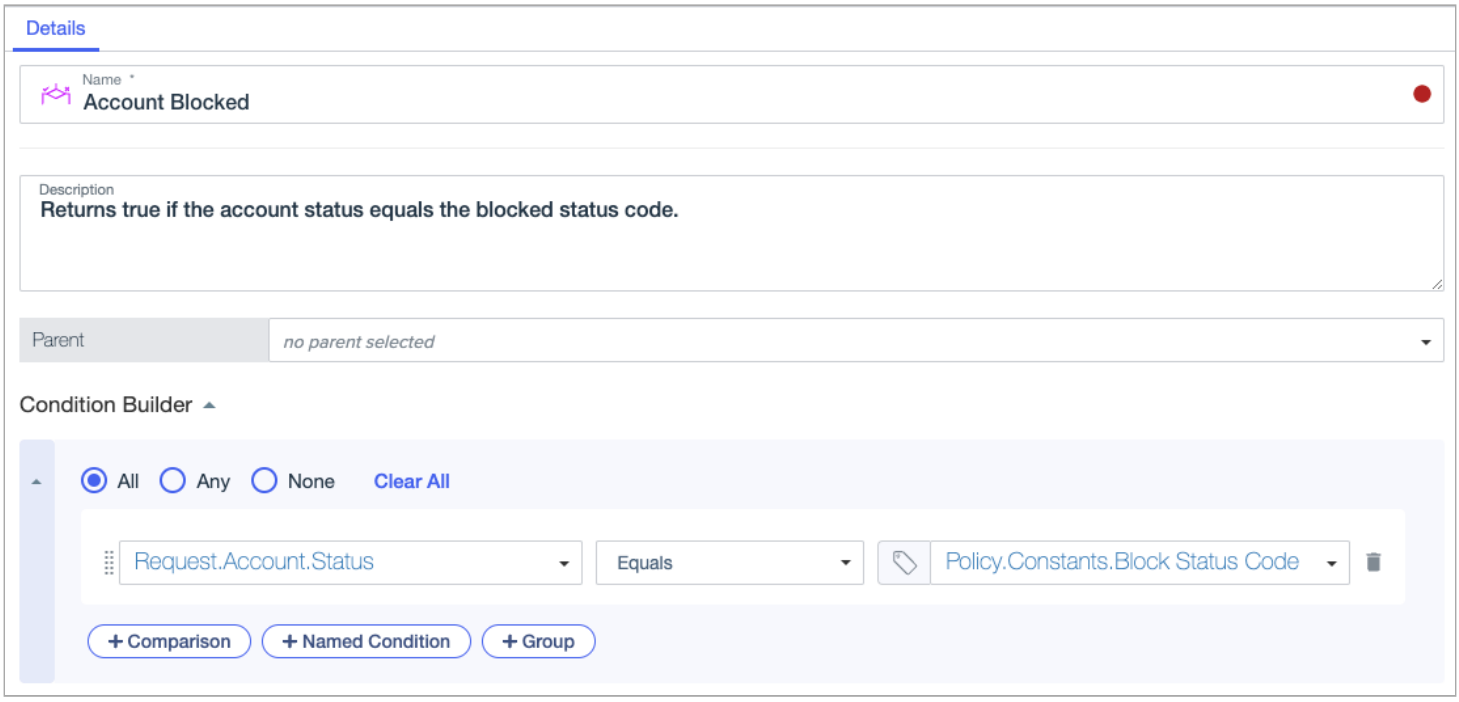
Adding a named authorization condition

Named conditions provide a way to reuse conditional logic across attributes and policies.

About this task

Named conditions can help provide consistency in authorization logic and minimize repetition throughout policies. You can use named conditions as components in more complicated condition expressions.

For example, consider a named condition that compares the account status received in a decision request to a status code to determine if the account is blocked. You can use this condition in multiple policies to check a user's account status.



Steps

1. Go to **Authorization** > **Trust Framework** and click the **Conditions** tab.

Copyright © 2025 Ping Identity Corporation

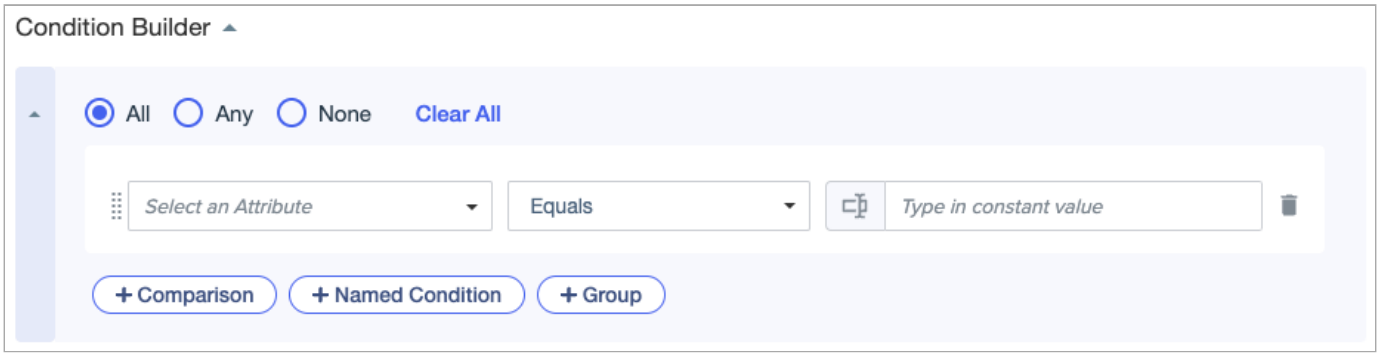
2. Click the + icon and select **Add new Condition**.
3. Define general information for the named condition:
    1. Enter a unique **Name** for the condition.

       The following characters are not allowed in the name:

       - Period (.)
       - Curly brackets ({ })
       - Pipe (|)
    2. **Optional:** For **Description**, enter information that describes the condition's purpose.
    3. **Optional:** To nest the condition under a parent in the tree, in the **Parent** list, select a parent condition.

       Nesting helps group related conditions together. You can move the condition to another location in the tree by selecting a different parent condition.

       To remove nesting, click the **Delete** icon and leave the **Parent** blank.
4. To add a comparison to the condition, click + **Comparison**.



5. Select an attribute to use in the comparison, select a comparator, and then enter a constant or click the **Switch to Attribute** ( ) icon to select an attribute.

> **Tip**
>
> When you select an attribute, you can select a property that's grayed out to generate an attribute that resolves against the parent attribute's JSON schema. If the property is nested, generate an attribute for the property above first and then generate an attribute for the child property.

6. To nest a comparison under another comparison, click + **Group**.

   Subgroups allow more permutations in comparisons. To remove nesting while keeping the comparison, click **Ungroup**.
7. To add a named condition, click + **Named Condition**, select a named condition, and then select **is True** or **is False**.
8. To combine multiple conditions, named conditions, or groups, select one of the following options.

Copyright © 2025 Ping Identity Corporation

Choose from:

- **All**: Invokes the condition when all of the conditions are true. If one condition evaluates to false, evaluation stops and the remaining conditions are not executed. This is like adding an `AND` Boolean operator between conditions.
- **Any**: Invokes the condition when at least one of the conditions is true. If one condition evaluates to true, evaluation stops and the remaining conditions are not executed. This is like adding an `OR` Boolean operator between conditions.
- **None**: Invokes the condition when none of the conditions are true. This is like adding a `NOT` Boolean operator.

9. Click **Save Changes**.

> **Note**
>
> You can copy a named condition defined on the **Conditions** tab for reuse by selecting **Make Copy** from the hamburger menu of that condition. If you copy a named condition with children, only the parent is duplicated. You can not copy a named condition at its point of use in a rule or policy.

Processors

Processors transform values returned from PingOne Authorize attributes and services.

Use processors to manipulate and transform data, including extracting details from structured data, or converting data to different formats.

Add processors directly to a resolver when you define attributes and services, or define them on the **Processors** tab as named processors to make them reusable.

> **Note**
>
> You can copy a processor defined on the **Processors** tab for reuse by selecting **Make Copy** from the hamburger menu of that processor. If you copy a processor with children, only the parent is duplicated.

You can use the following types of processors:

- Collection Filter
- Collection Transform
- JSON Path
- X Path
- SpEL
- Named

Set up a chain of one or more processors to transform an attribute value each time it is obtained from a resolver. The input to the first processor in the chain is the value that comes from the resolver. The input to subsequent processors is the previous processor in the chain. You can drag collapsed processors to rearrange their order.

Copyright © 2025 Ping Identity Corporation

> **Important**
>
> Processors have a type that indicates what the output data type should be after applying the expression. In attribute comparisons, data type mismatches are a common source of errors. Learn more about debugging these kinds of problems in Examining recent decisions.

Collection filter

When the data being processed has a value type of **Collection**, you can set a filter to examine each item in the collection and keep only the items that satisfy some condition. A collection filter uses a value processor to yield a `true` or `false` evaluation for each item in the collection. When `true`, the original item goes in the resulting collection. When `false`, it's omitted.

> **Important**
>
> To prevent errors, make sure that the data has a value type of **Collection** when you use a collection filter. For example, a common error in a chain of processors is defining data that is a JSON array as JSON in the previous processor.

Each item in the collection can optionally be preprocessed by one or more value processors before applying the condition. For example, suppose you received a collection of JSON objects from a service invocation and you want to filter the items by the `score` field. The input data might look like the following:

```
[
    { "name": "Alice", "role": "Sender",   "score": 72 },
    { "name": "Bob",   "role": "Receiver", "score": 36 },
    { "name": "Carol", "role": "Observer", "score": 47 },
    { "name": "Dave",  "role": "Attacker", "score": 99 }
]
```

A collection filter processor could achieve this by using a JSON Path preprocessor to extract the `score`:

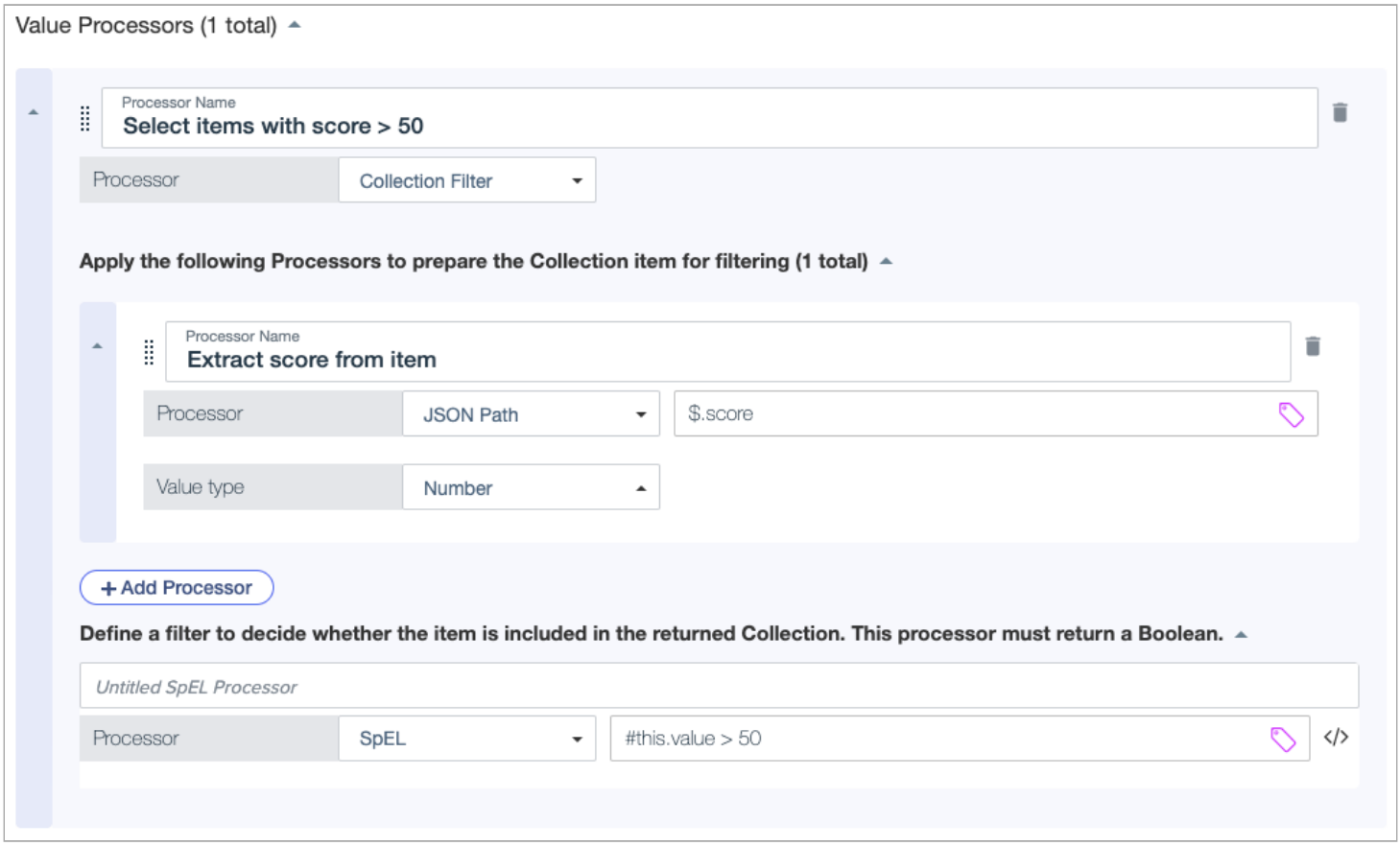
```
$.score
```

The following SpEL condition yields a true or false decision for each item:

```
#this.value > 50
```

Each list item is in turn passed through the preprocessor and the condition. The first item has score 72, which is greater than 50 so the condition yields true and the item is retained for the result collection. The second and third items have scores less than 50, so the condition yields `false` and these items are omitted. The final item also has a score higher than 50 and is retained.

Copyright © 2025 Ping Identity Corporation



The result of the collection filter is:

```
[
    { "name": "Alice", "role": "Sender",   "score": 72 },
    { "name": "Dave",  "role": "Attacker", "score": 99 }
]
```

The values produced by the preprocessing and condition are only used to determine inclusion. The final result of a collection filter consists of those original collection items that satisfied the predicate after preprocessing.

If the condition or preprocessing produces an error for any item in the input collection (for example, if a `score` field is missing or not a number in the source data), the whole collection filter is considered to have failed.

Collection transform

When the data being processed has a value type of **Collection**, you can set a transform to apply a processor or a sequence of processors to each item in the collection.

Assume that you have the following input collection:

Copyright © 2025 Ping Identity Corporation

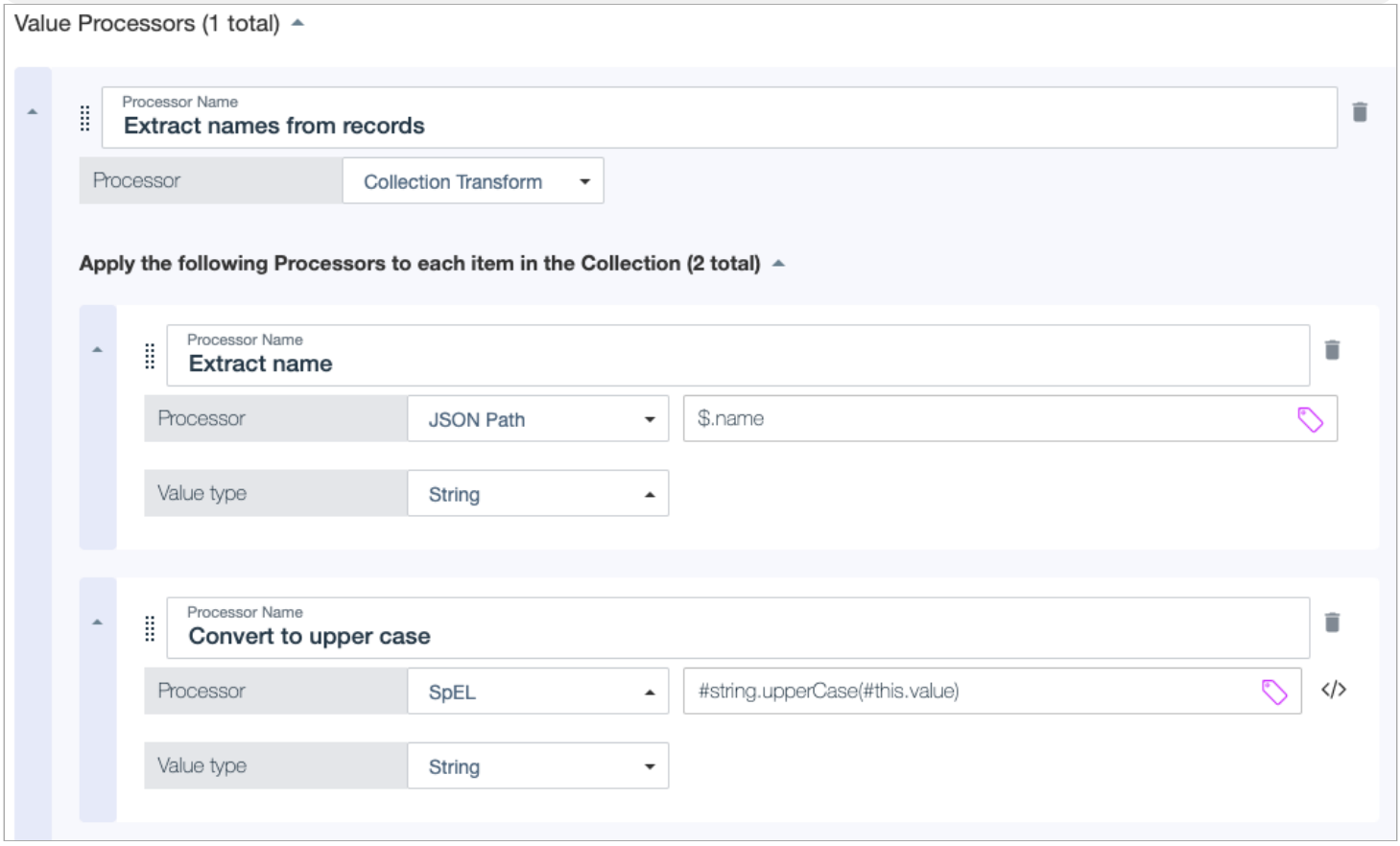
```
[
    { "name": "Alice", "role": "Sender",   "score": 72 },
    { "name": "Bob",   "role": "Receiver", "score": 36 },
    { "name": "Carol", "role": "Observer", "score": 47 },
    { "name": "Dave",  "role": "Attacker", "score": 99 }
]
```

The following JSON Path processor extracts the `name` field for each item:

```
$.name
```

This SpEL processor converts each `name` to upper case:

```
#string.upperCase(#this.value)
```



The resulting collection consists of just the extracted names converted to upper case, preserving the order of the original collection:

```
[ "ALICE", "BOB", "CAROL", "DAVE" ]
```

If the item processor produces an error for any item, the overall collection transform processor produces an error.

Copyright © 2025 Ping Identity Corporation

JSON Path

With JSON Path, you can extract data from JSON objects. For example, assume you have a service that resolves to the following JSON:

```
{
   "name": "Joe Bloggs",
   "requestedItems": [
      {
         "id": "b5f963fa-111e-49ff-994b-b89a20a2c1d5",
         "price": 125.00
      },
      {
         "id": "84e204dd-44f5-4a84-8e58-972c2a9c80b4",
         "price": 299.99
      }
   ]
}
```

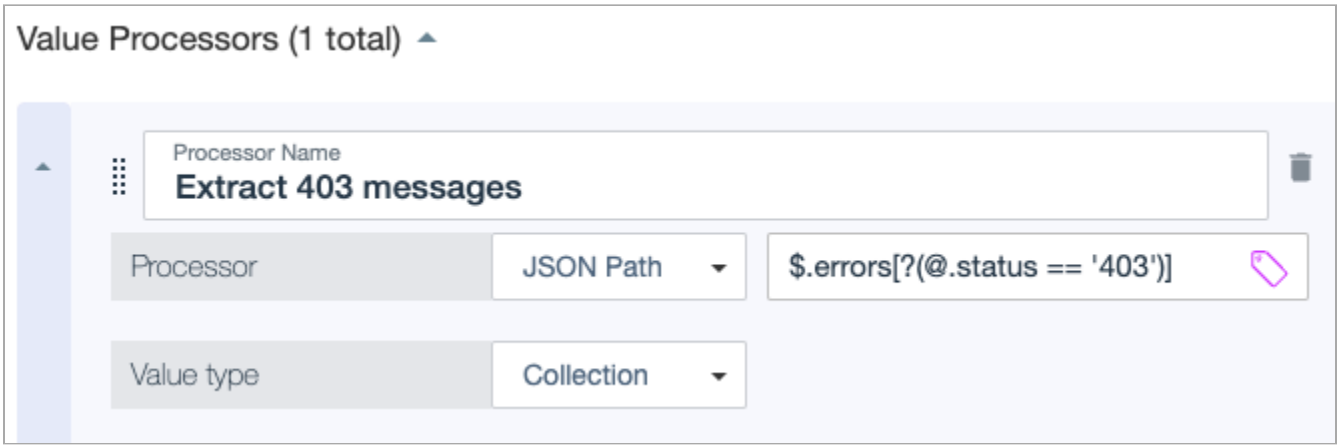
To extract the `price` fields of all requested items, we set the Value Processor to **JSON Path** with the expression `$.requestedItems[*].price`.

For another example, assume that you want to extract errors with a status of 403 from the following API response:

Copyright © 2025 Ping Identity Corporation

```
{
  "errors": [
    {
      "status": "403",
      "source": {
        "pointer": "/data/attributes/statements"
      },
      "detail": "Error 403 - Forbidden."
    },
    {
      "status": "403",
      "source": {
        "pointer": "/resources/lightwave"
      },
      "detail": "You don't have permission to access this resource."
    },
    {
      "status": "422",
      "source": {
        "pointer": "/data/attributes/volume"
      },
      "detail": "Volume does not, in fact, go to 11."
    },
    {
      "status": "500",
      "source": {
        "pointer": "/data/attributes/reputation"
      },
      "title": "The backend responded with an error",
      "detail": "Reputation service not responding after three requests."
    }
  ]
}
```

Set the Value Processor to **JSON Path** with the expression `$.errors[?(@.status == '403')]`.



The resulting collection consists of the extracted errors:

Copyright © 2025 Ping Identity Corporation

```
[
  {
    "status": "403",
    "source": {
      "pointer": "/data/attributes/statements"
    },
    "detail": "Error 403 - Forbidden."
  },
  {
    "status": "403",
    "source": {
      "pointer": "/resources/lightwave"
    },
    "detail": "You don't have permission to access this resource."
  },
]
```

For more information about JSON Path expressions, see https://github.com/json-path/JsonPath.

X Path

XPath is the XML-equivalent for JSON Path and follows a very similar syntax. For more information about XPath expressions, see the XPath tutorial on w3schools.com.

> **Note**
>
> PingOne Authorize policies only support the use of XPath 1.0. Functions added in later versions are not available.

SpEL

You can perform more complicated data processing with PingOne Expression Language, a customized derivation of the Spring Expression Language (SpEL). Expressions are applied directly to the resolved value.

For example, assume you want to search for a substring that matches the following regular expression:

```
\[[0-9]*\.[0-9]\]
```

Set the processor to **SpEL** and set the expression to the following:

```
matches(\[[0-9]*\.[0-9]\])
```

Interpolate attribute values directly into the SpEL expression using curly brackets, which can be useful if you want to combine multiple attribute values into a single value:

```
 {{Customer.Age}} - {{State.Drinking Age}} >= 0
```

You can concatenate interpolated attributes with strings in SpEL expressions. In the following example, a SpEL expression is used to dynamically concatenate a string with a user's account number to create a transaction verification message:

Copyright © 2025 Ping Identity Corporation

```
"Account " + {{Customer.AccountNumber}} + " has been charged."
```

> **Note**
>
> Be careful not to wrap an interpolated attribute with quotes.

PingOne's expression language differs from SpEL as follows:

- Some SpEL features are disabled or restricted. For example, `T(xyz)` syntax for invoking Java static functions is not supported. For more information, see Disabled and restricted SpEL features.
- References to the value being processed by the expression must use `#root.value` instead of `#root`. For more information, see Variables.
- Instead of invoking Java methods for handling data values, you must use the custom library functions provided by PingOne's expression language.

Learn more about SpEL in the official Spring Framework documentation.

Named

Named processors allow you to extract processor logic into a reusable component, which helps abstract some of the complexity when you define an attribute or a service. Also, it reduces repetition and allows commonly used logic to be updated in a single place.

Define named processors outside of an attribute on the **Processors** tab in the **Trust Framework**. You can also create inline value processors for attributes and services that co-exist with named processors.

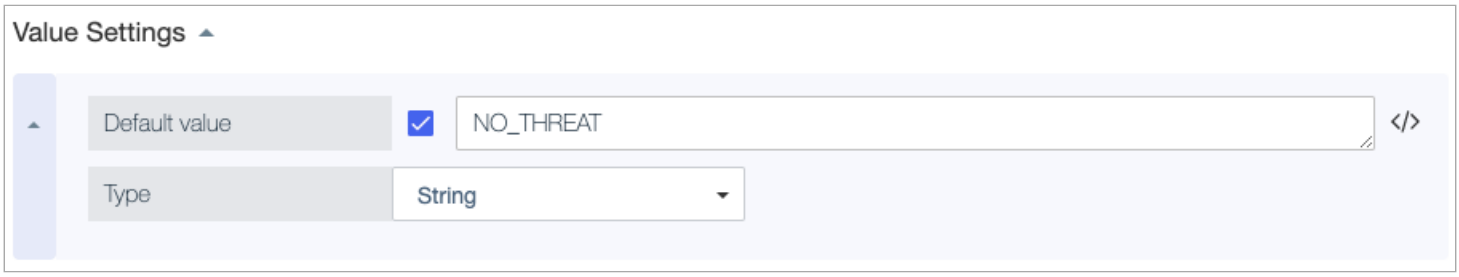
Value settings

Value settings enable you to define a data type for an authorization attribute or service and an optional default value for an attribute.

For information about adding value settings to an attribute, see Adding value settings to an attribute.

Default value

You can define a default value to provide an attribute with a value when it can't otherwise be resolved. This is optional. For example, with the following value settings, a risk level attribute resolves to the default value **NO_THREAT** under conditions in which it doesn't resolve to another value.



> **Note**
> An attribute with a default value and no resolvers acts as a constant that always resolves to the fixed default value.

Data type

The data type constrains the set of allowable attribute or service values and provides a predictable model for value processing and other data transformations.

The main data types for input and output data are **String** and **JSON**. All data types have conversions to and from a canonical string representation. You must use processors to convert other formats, such as date and time representations.

> **Important**
> Data type mismatches can be a common source of errors during attribute and service testing. Check for data type inconsistencies when you are building and testing the **Trust Framework**.

Attributes and services can have the following data types.

Data type	Description
Boolean	A simple true or false (case insensitive): • `True` can be represented in textual form, such as in default values or decision request parameters, as `true`, `yes`, or `1`. • `False` can be represented by `false`, `no`, or `0`. In value processing contexts, such as SpEL expressions, the value is a `java.lang.Boolean` instance.
Collection	An ordered collection of other value types. Only valid value types as described here can be members of collections. JSON-formatted arrays are valid textual representations of collections. In value processing contexts, a collection is a `java.util.Collection`. However, the objects contained are of an internal type. Use only the `get()` method to retrieve items by zero-based integer index. **Tip** To ensure a collection resolves successfully if it's empty, set the **Default value** to open and closing brackets: `[]`.
Date	A date, such as `23 April 2020`. The textual representation is ISO-8601, for example, `2020-04-23`. In value processing contexts, the value is a `java.time.LocalDate`. **Date** values can be converted to the following types: • **Date Time**: The time component becomes `00:00:00`. • **Zoned Date Time**: The time zone is assumed to be UTC.

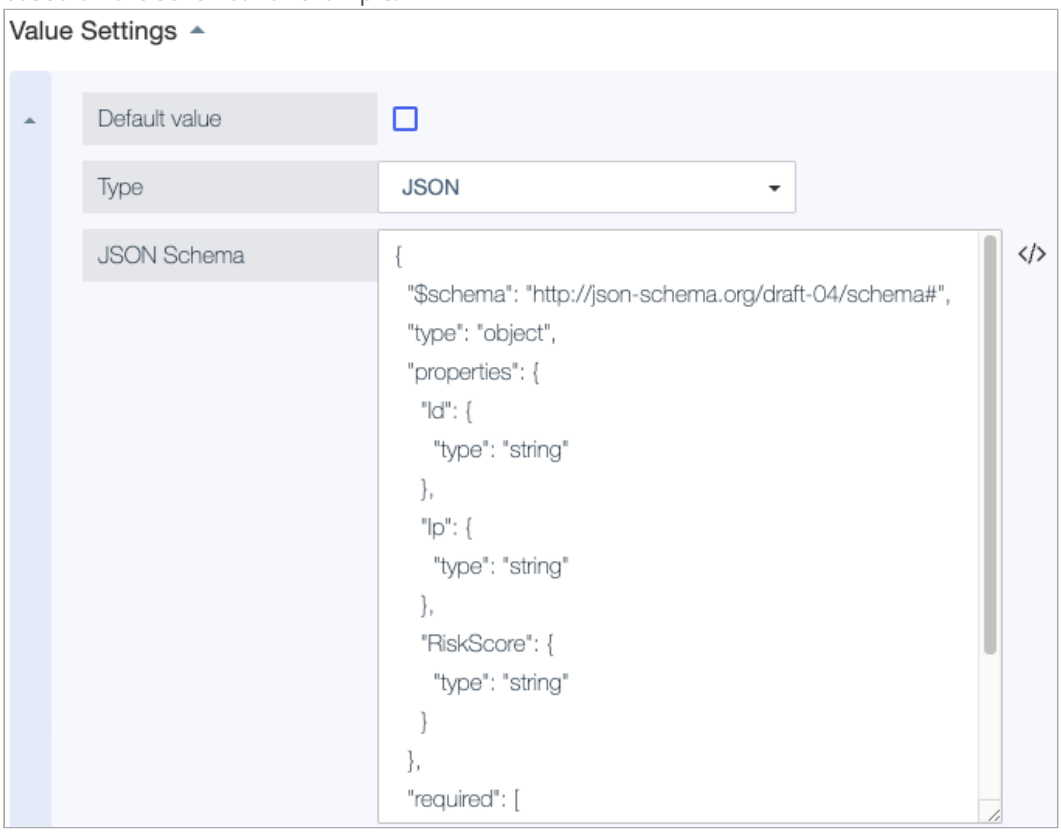
Copyright © 2025 Ping Identity Corporation

Data type	Description
Date Time	A date and time of day, such as `4:15 pm and 30 seconds on 23 April 2020`. The maximum resolution is microseconds. For example, `2020-04-23T16:15:30` or `2020-04-23T16:15:30.783239`. The textual representation is ISO-8601. In value processing contexts, the value is a `java.time.LocalDateTime`. **Date Time** values can be converted to the following types: • **Date** or **Time**: Dropping the appropriate information in each case. • **Zoned Date Time**: The time zone is assumed to be UTC.
Duration	A time duration expressible in seconds or a fraction of seconds. The textual representation is ISO-8601, for example: • `PT3H` for 3 hours • `PT2M45.836S` for 2 minutes and 45.836 seconds In value processing contexts, the value is a `java.time.Duration`. **Duration** values can't be converted to other types.

Copyright © 2025 Ping Identity Corporation

JSON

A JSON document. This is useful for bringing data into and out of the decision point. This is the only attribute type subject to JSON Path value processors. The textual representation is `JSON`. In value processing contexts, the value is a `java.util.Map` or `java.util.Collection`. Optionally, you can define a valid JSON Schema for an attribute and generate attributes based on the schema. For example:



> **Important**
> If the schema changes, you must update it manually in any generated child attributes.

Only simple JSON property definitions are supported. Complex object definitions, such as collections, are not supported. Limitations for the type keyword are as follows:

- Define the `type` keyword as a string. Arrays are not supported.
- PingOne Authorize recognizes the following types: `string`, `number`, `integer`, `object`, `array`, `boolean`.

  > **Note**
  > Define the keyword with a single type only. Multiple types and complex types are not supported.

- PingOne Authorize maps JSON property types to the following attribute types:
  - JSON type `string` is mapped to attribute type **String**.
  - JSON types `number` and `integer` are mapped to attribute type **Number**.
  - JSON type `object` is mapped to attribute type **JSON**.
  - JSON type `array` is mapped to attribute type **String**.

Copyright © 2025 Ping Identity Corporation

Data type	Description
	Note PingOne Authorize treats an `array` type value as an untyped object. You can't generate child attributes for this type. ◦ JSON type `boolean` is mapped to attribute type **Boolean**.
Number	A numeric value. Decimal integers and real numbers are supported, including scientific notation. In value processing contexts, the value is a `java.math.BigDecimal` instance.
Period	A time period expressible in calendar units, such as a number of days or months. The textual representation is ISO-8601, for example: • `P9Y` for 9 years • `P3M2D` for 3 months and 2 days In value processing contexts, the value is a `java.time.Period`. **Period** values can't be converted to other types.
String	Data that is not one of the other types is interpreted as UTF-8 text, stored internally as UTF-16. In value processing contexts, these values are `java.lang.String`.
Time	A time of day, such as `4:15 pm and 30 seconds`. The maximum resolution is microsecond. For example, `16:15:30`, `16:15:30.783`, and `16:15:30.783239` are all valid. The textual representation is ISO-8601. In value processing contexts, the value is a `java.time.LocalTime`. **Time** values can't be converted to other types.
XML	An XML document. This is useful for bringing data into and out of the decision point. This is the only data type subject to XPath value processors. The textual representation is XML. In value processing contexts, the value is an `org.w3c.Document`.
Zoned Date Time	A date and time of day with a time zone expressed as an offset from UTC. The textual representation is ISO-8601, for example, `2020-04-23T16:15:30.783+01:00`. In value processing contexts, the value is a `java.time.ZonedDateTime`. **Zoned Date Time** values can be converted to the following types, dropping information in each case: • **Date Time** • **Date** • **Time**

Testing Trust Framework elements

Test PingOne Authorize Trust Framework elements from end-to-end with tools that show the complete processing flow.

Copyright © 2025 Ping Identity Corporation

About this task

Testing enables you to validate the type conversion of policy information points (PIP) included in decision requests and the logical behavior of conditions. Although policy testing indirectly tests your Trust Framework elements, testing each Trust Framework element individually allows you to immediately view the output of element processing without needing to parse policy test results.

Use Trust Framework testing to:

- Verify attribute or service value settings.

  If you are testing an attribute with a value type other than `String`, the decision service must convert this attribute from a string provided in the request to the correct type. Testing an attribute or service allows you to verify that the formatting required for this conversion is correct.

- Test the behavior of value processors.

  The decision service's conversion of request parameters from strings to other data types, such as `Number`, might involve a chain of processors configured in the attribute definition. Testing an attribute allows you to determine whether such processing produces the desired outcome, before runtime.

- Test the behavior of resolvers.

  If you define multiple resolvers on an attribute, you can use testing to confirm the order in which the decision service checks these resolvers for a value.

- Test the logic of conditions.

  With testing, you can confirm that your conditional logic produces the desired outcome, before implementing that logic in your authorization policies.

Steps

1. Go to **Authorization → Trust Framework**.
2. Click the tab of the appropriate Trust Framework element type, select the element that you want to test, and then click the **Test** tab.
3. Define the test scenario:
   1. (Optional) To include a PingOne user ID as context in the decision request, search for a user in the **PingOne User** field.

      > **Important**
      > If you are testing an element that depends on the `PingOne.User` attribute, you must select a user to avoid a `MISSING_ATTRIBUTE` error.
      > The selected user must be defined in the current PingOne environment.

   2. In the **Attributes** list, select the attribute that you want to test and any other attributes that you want to include as request parameters, and provide sample values.

      > **Tip**
      > Click the angle brackets next to an attribute to display a JSON text editor.

Copyright © 2025 Ping Identity Corporation

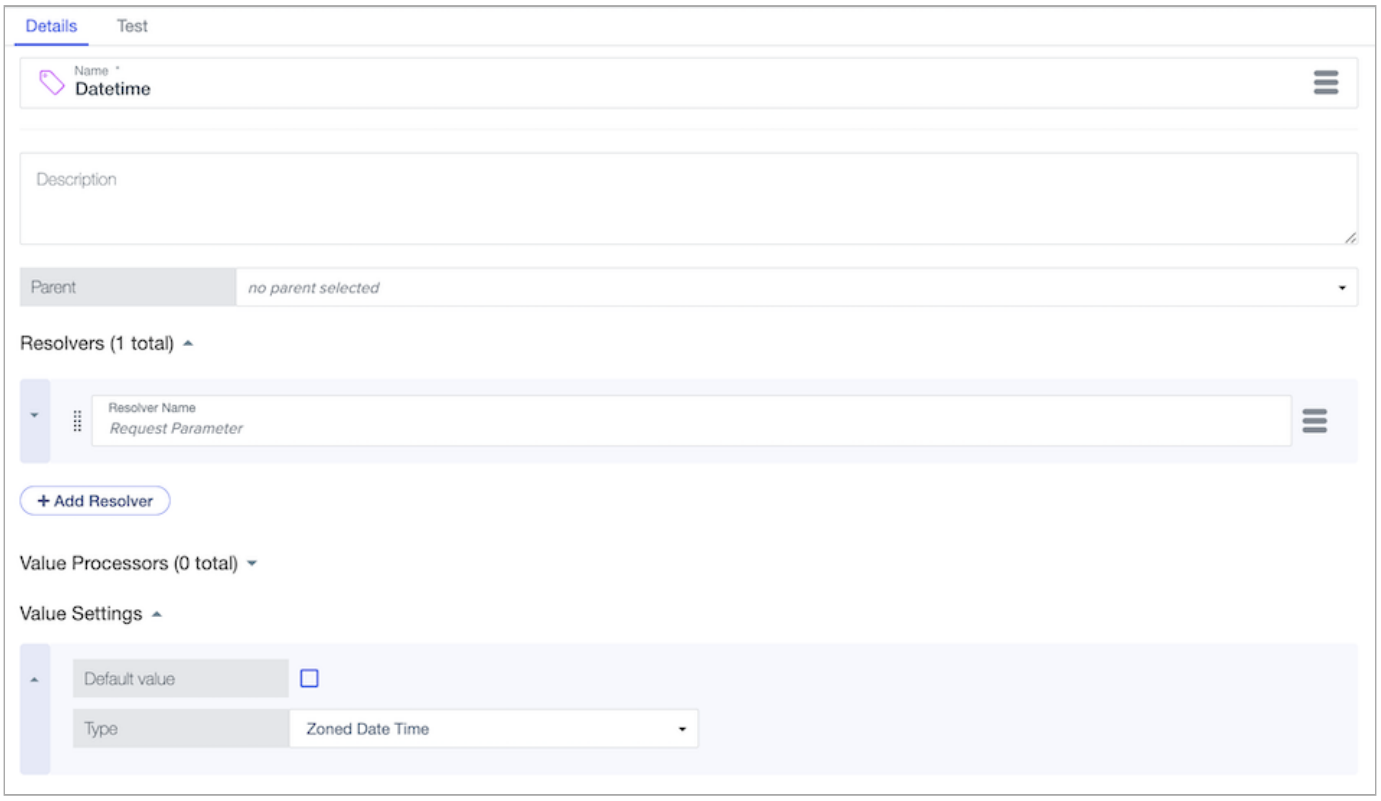
3. In the **Overrides** section, configure attribute and service values if you want to override those elements' default behavior.

   For example, if an attribute is defined with a request parameter resolver, and no value is specified in the test request, the decision service resolves that attribute from the **Overrides** configuration.

> **Note**
>
> You can also click the **Import JSON** button to define the test scenario with a JSON text editor.

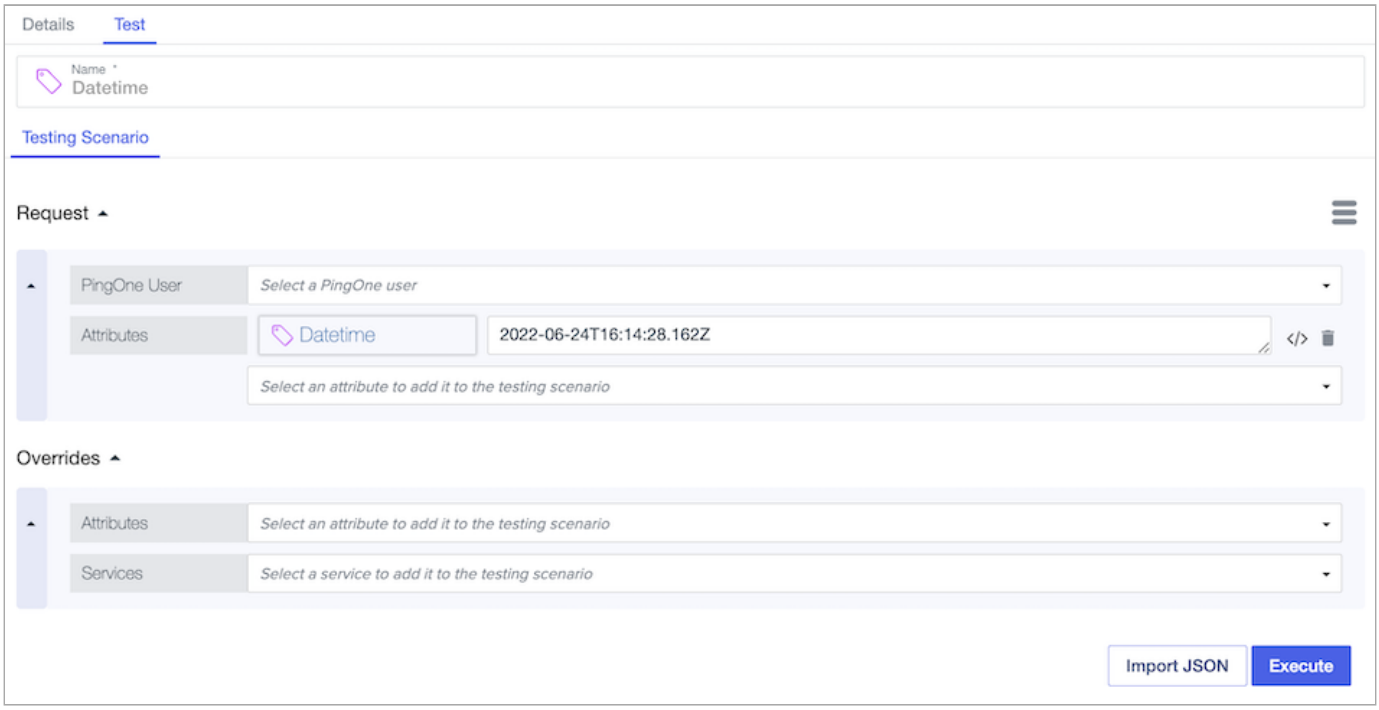
Example:

The **Datetime** attribute defined below has a value type of **Zoned Date Time**, resolves from a decision request parameter, and has no processors defined. Testing this attribute verifies whether the decision service can directly convert this attribute from a string.



The scenario below tests the **Datetime** attribute with an ISO 8601-formatted string as input:

Copyright © 2025 Ping Identity Corporation



4. Click **Execute**.

> **Note**
>
> If the test scenario exceeds 50 kB in size, sample values will not be stored in the local cache after executing the test request.

Result:

The **Output** tab displays the value and type of the attribute being tested, along with a **Copy to clipboard** button.

If the element being tested is of type **JSON**, the **Output** tab also displays a JSON text editor.

5. Click the other tabs for additional details:
   - **Request**: Shows the JSON request sent to the decision, allowing you to confirm the expected information was sent.
   - **Response**: Shows the complete, high-verbosity response for the decision, including expanded errors and other helpful information.

Copyright © 2025 Ping Identity Corporation

This tab can be helpful when troubleshooting value processing failures.

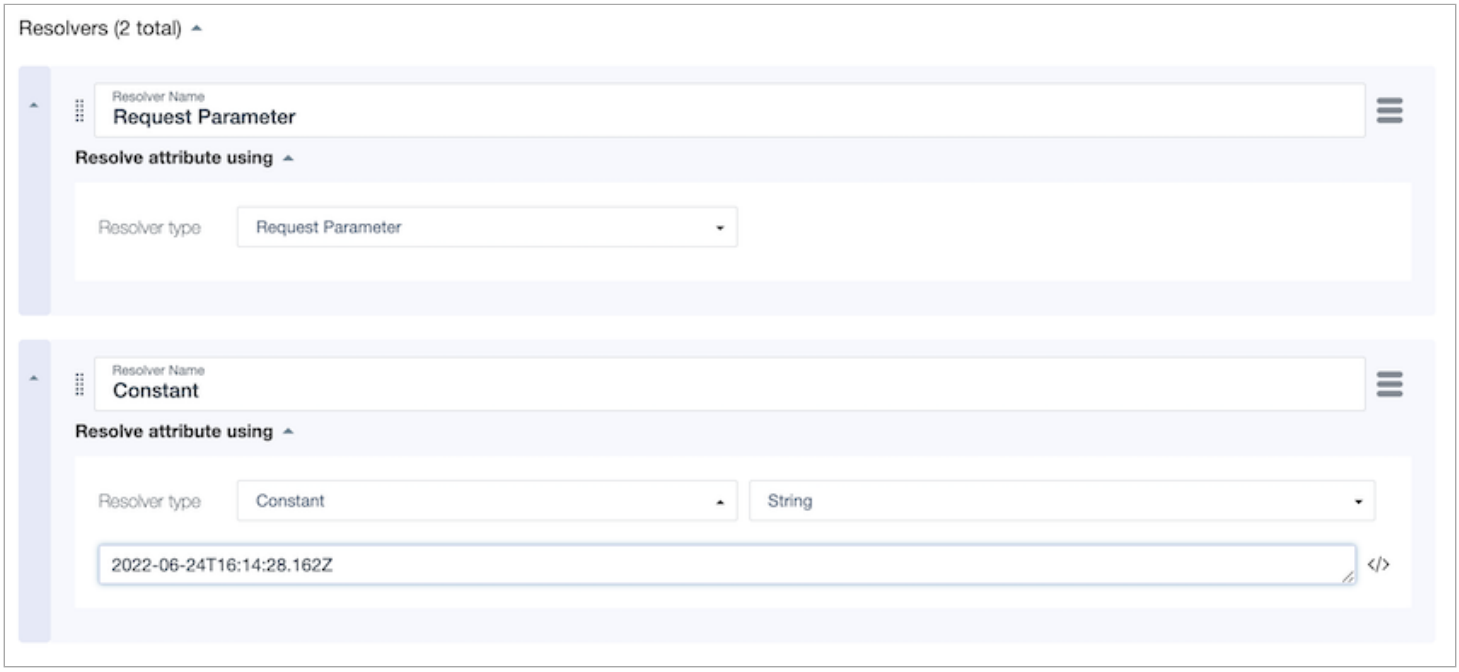
- **Attributes**: Shows details about the attributes used in the decision.
- **Services**: Shows details about the services used in the decision.

Examples

You can test additional Trust Framework elements with multiple value processors or resolvers.

Testing an attribute with multiple resolvers

The following example extends the **Datetime** attribute by adding a **Constant** resolver. The expected behavior is that the decision service first checks the decision request for a `Datetime` parameter to resolve the attribute from, and if there is no such parameter, the decision service resolves the attribute from a specified constant value.



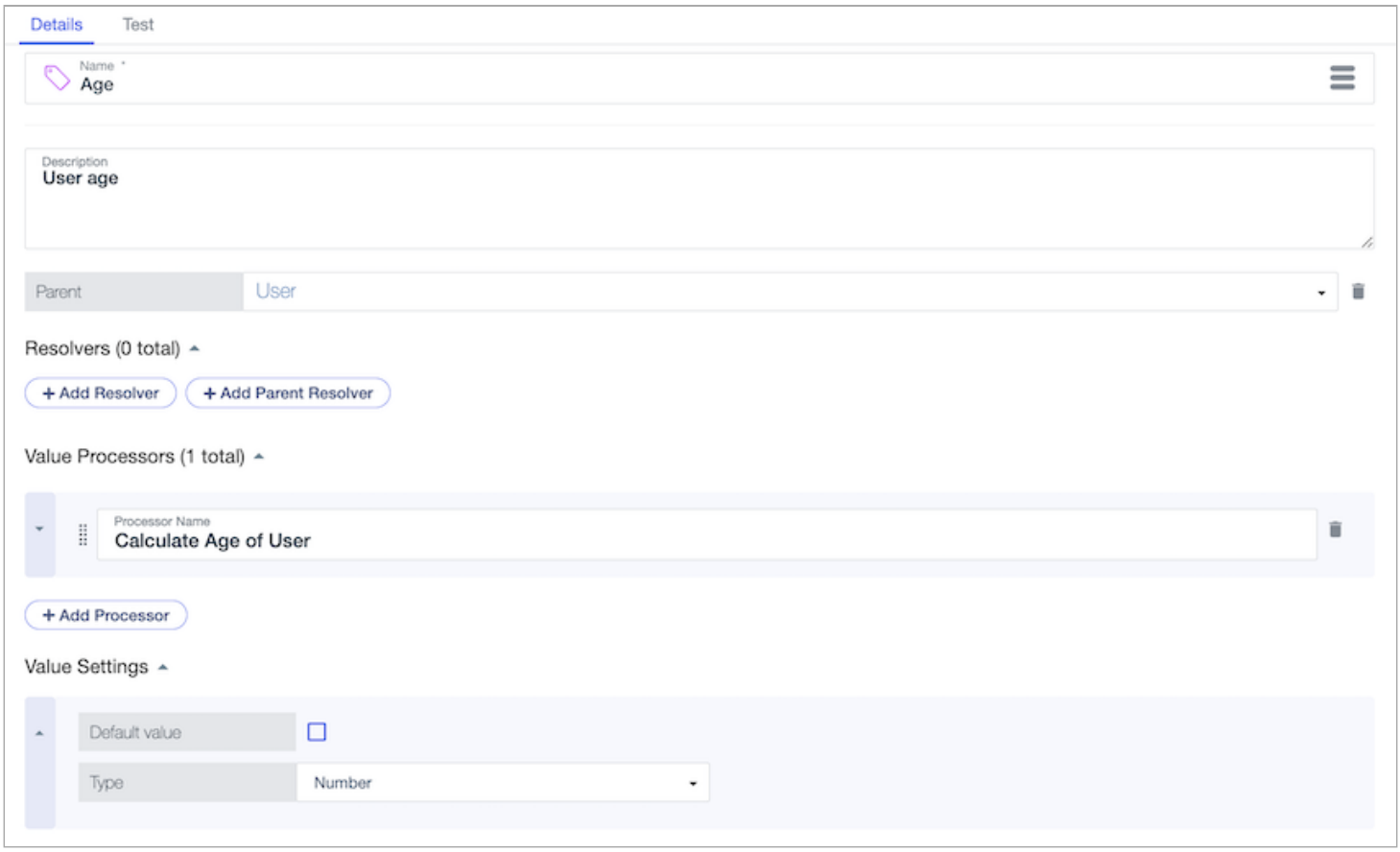
After executing the testing scenario without any parameters defined, you can check the `attributes.Datetime.resolvedBy` field under the **Response** tab to verify the order in which the decision service checks resolvers for attribute values.

Copyright © 2025 Ping Identity Corporation

```
},
"attributes": {
    "Datetime": {
        "id": "a865fbad-9621-46d4-bef4-d815636d65ed",
        "name": "Datetime",
        "successful": true,
        "consumedBy": [],
        "resolvedBy": [
            {
                "resolver": "request",
                "successful": false,
                "key": "Datetime",
                "valueProcessing": [],
                "error": {
                    "code": "MISSING_ATTRIBUTE",
                    "message": "Datetime"
                }
            },
            {
                "resolver": "constant",
                "successful": true,
                "valueProcessing": [],
                "value": "2022-06-24T16:14:28.162Z",
                "type": "STRING"
            }
```


Testing an attribute with multiple processors

The following example defines a **User.Age** attribute of type **Number**, which uses a series of processors to calculate a user's age:



Copyright © 2025 Ping Identity Corporation

The primary value processor, **Calculate Age of User**, defines three subordinate PingOne Expression Language processors that each use the **Datetime** attribute from above and a new **User.Date of Birth** attribute. The **User.Date of Birth** attribute is not connected to the built-in **PingOne.User** attribute.

- **Calculate year**:

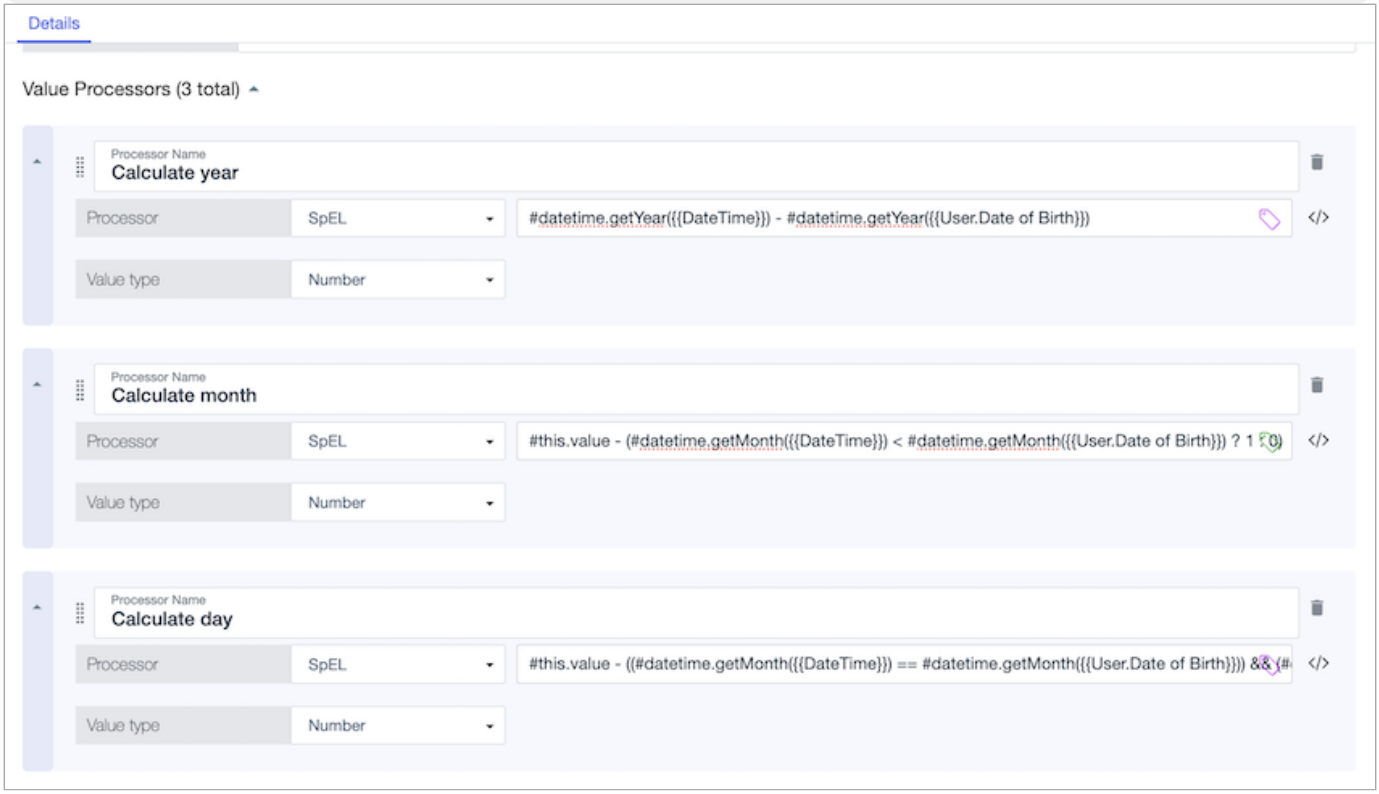
```
#datetime.getYear({{Datetime}}) - #datetime.getYear({{User.Date of Birth}})
```

- **Calculate month**:

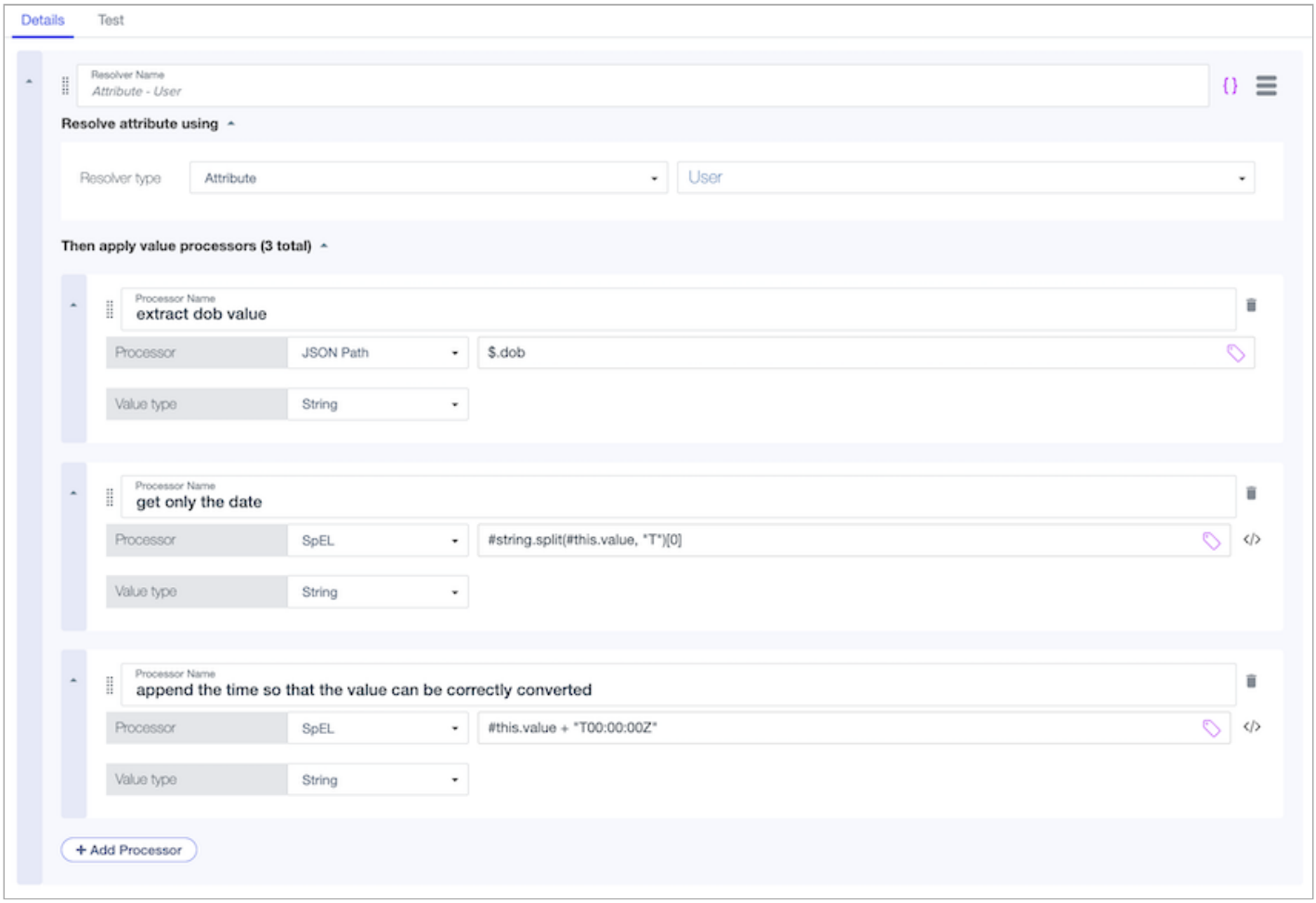
```
#this.value - (#datetime.getMonth({{Datetime}}) < #datetime.getMonth({{User.Date of Birth}}) ? 1 :
0)
```

- **Calculate day**:

```
#this.value - ((#datetime.getMonth({{Datetime}}) == #datetime.getMonth({{User.Date of Birth}})) &&
(#datetime.getDayOfMonth({{Datetime}}) < #datetime.getDayOfMonth({{User.Date of Birth}})) ? 1 : 0)
```

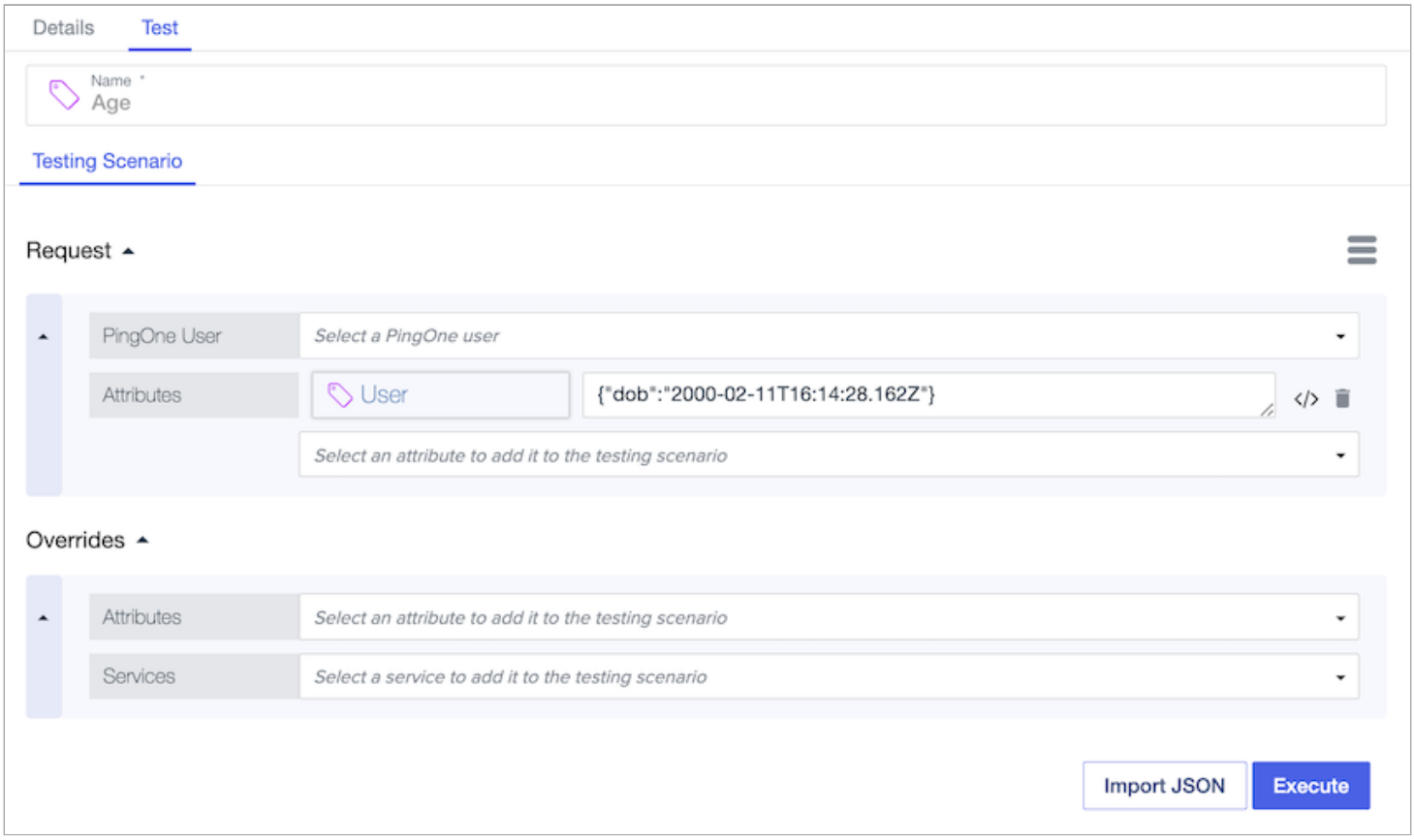


The decision service resolves the **User.Date of Birth** attribute from the **User** attribute and uses the following JSON Path and SpEL processors:

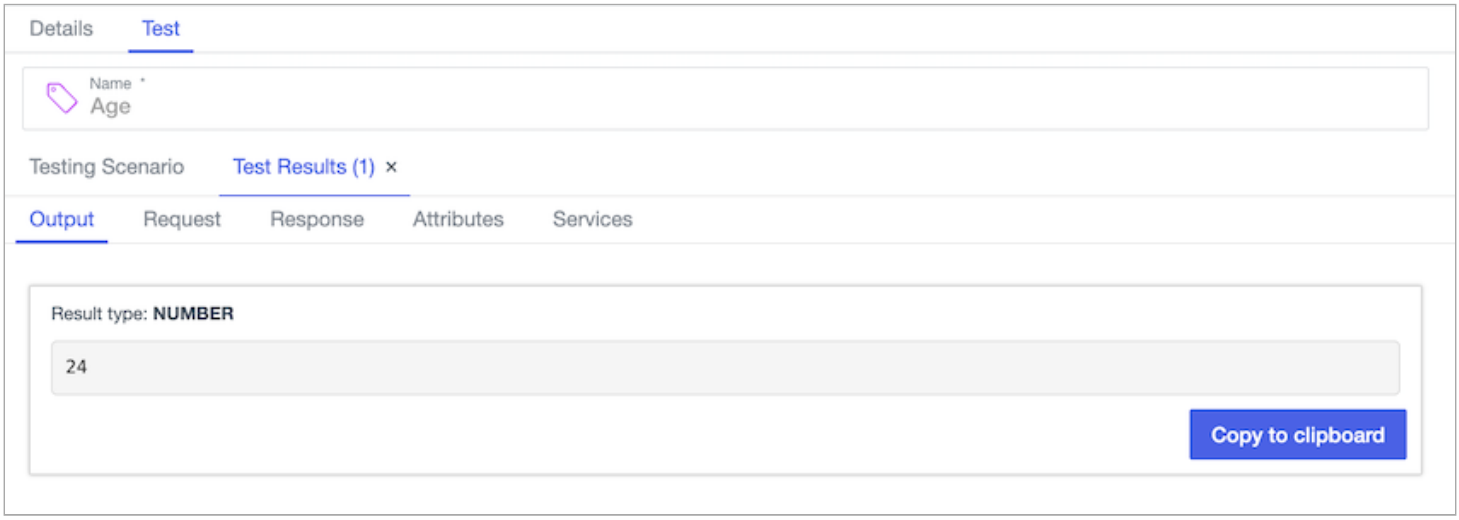


The following testing scenario verifies that the above chain of processing works as intended, where a user's birthday is February 11, 2000:

Copyright © 2025 Ping Identity Corporation



The test produces the following output as expected. Click the **Response** tab to view detailed processing steps.



Viewing dependents

Before you change a policy or an element in the PingOne Authorize **Trust Framework**, view dependents to see where the policy or element is used.

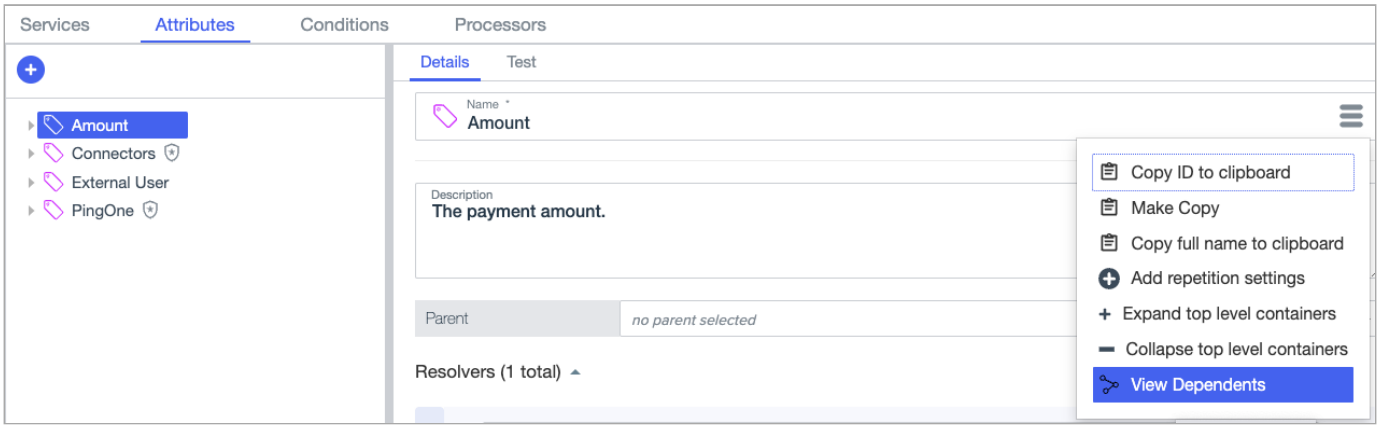
About this task

Viewing dependents helps ensure that updates don't introduce unintended consequences.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Authorization > Trust Framework** or **Authorization > Policies** and select an element or policy.
2. Click the hamburger menu in the **Name** field and select **View Dependents**.



Result:

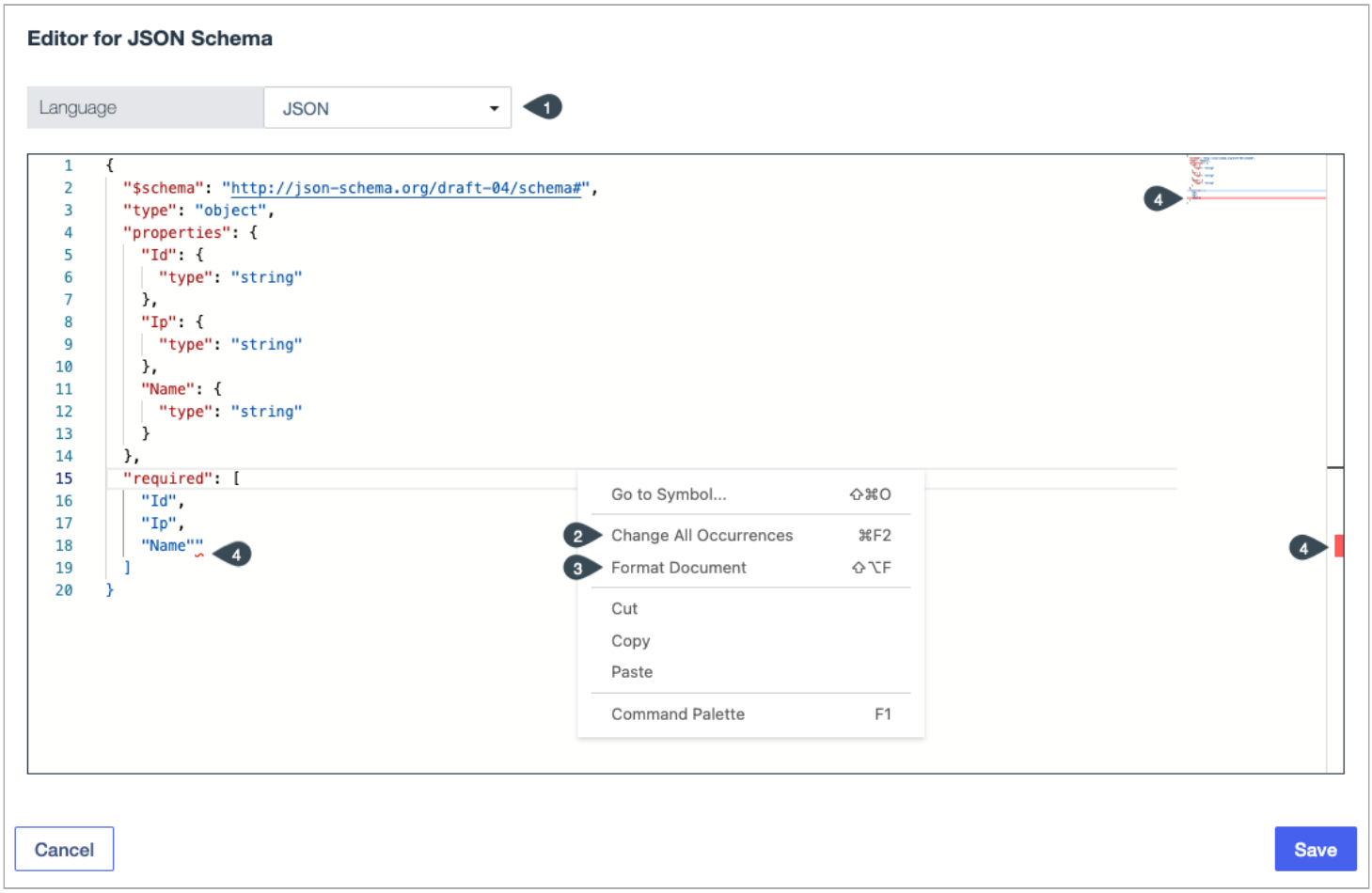
Dependents are shown in a new window.

Code editor

As you build and test your rules, policies, and **Trust Framework** definitions, you can use the code editor to write and review large blocks of content.

Click </> next to the field to open the Monaco-based code editor. Any content you've already added transfers to a modal window where you can continue working. The field's **Type** value determines the editor's **Language** value. If the **Type** value isn't JSON, HTML, or XML, the editor uses plain text.

Copyright © 2025 Ping Identity Corporation



The code editor has the following tools and options to help you quickly organize, navigate, and validate your work:

Language (1)

Change the content language while the editor is open. After saving your work and closing the editor, change the **Type** to permanently change the language of your content.

> **Note**
>
> Some context menu features are not available in all languages. We have focused on the JSON-enabled features here.

Change All Occurrences (2)

Save time and avoid manual errors by editing all of the case-sensitive matches of a highlighted term in one operation.

Format Document (3)

Quickly structure your content for clarity of hierarchy and relationships by automatically adding indents and line breaks.

Syntax validation (4)

Identify and resolve syntax errors as you're writing, allowing you to avoid unnecessary debugging and focus on the most valuable portions of your content. Look for validation indicators inline, in the scroll bar, or on the mini map. To see details about an error and hints on how to fix it, hover over the inline indicator and select **View Problem**.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Validation is only supported for JSON content and doesn't support interpolated values.

Auto-complete (not pictured)

Reduce repetitive typing and errors by using the auto-complete suggestions when available.

Find and replace (not pictured)

Make programmatic changes to your content using a find-and-replace tool that includes regex support.

Authorization policies

PingOne Authorize policies model business requirements into authorization logic using elements created in the **Trust Framework**.

Policies are built by business analysts who understand your application requirements and the regulations that you're complying with. Your organization imposes many conditions and constraints on access control. Policies capture these constraints in rules that define the circumstances under which users can access certain resources.

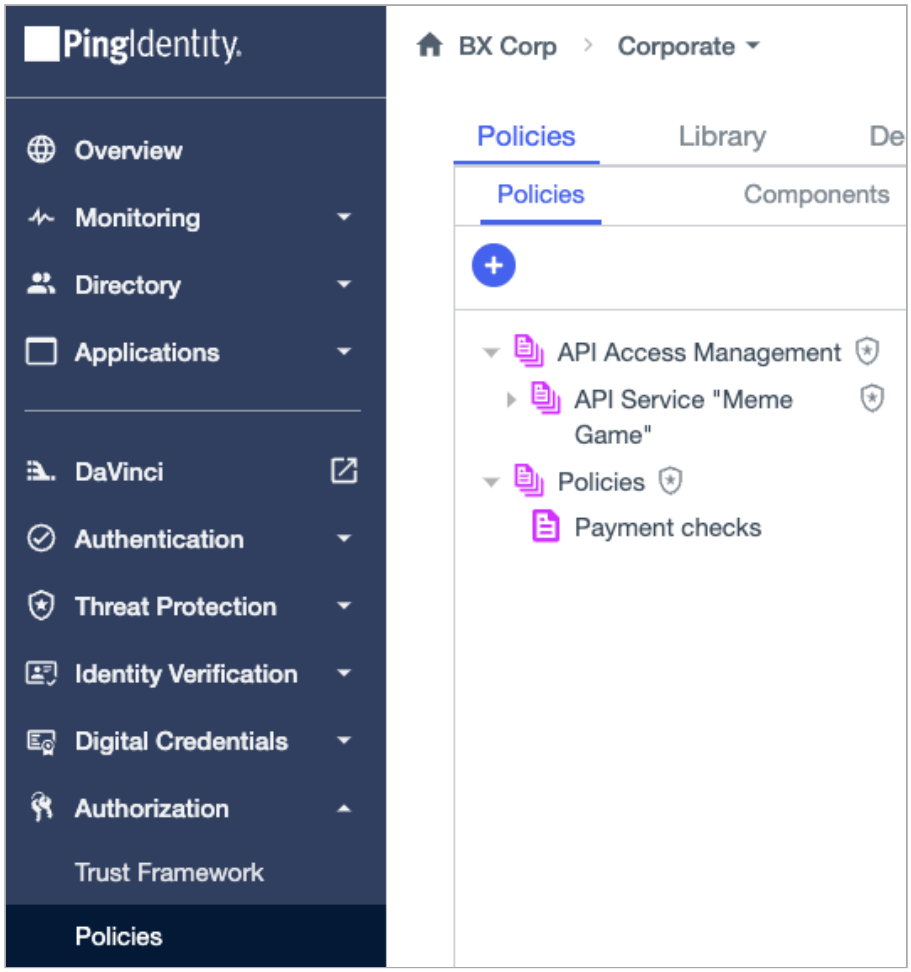
> **Note**
>
> If you're publishing policies to an Authorize gateway, learn more about policy best practices in Policies published to Authorize gateways.

Structuring policies

You can group policies using policy sets organized hierarchically in a tree structure. PingOne Authorize owns the **Policies** and **API Access Management** root policy sets.

The **Shield** ( ) icon indicates that these policy sets are system-owned and editing restrictions apply. You can't move or delete these policy sets. This ensures that they are configured correctly and always available.

Copyright © 2025 Ping Identity Corporation



Policies policy set

You can nest your own policy sets and policies under the **Policies** policy set:

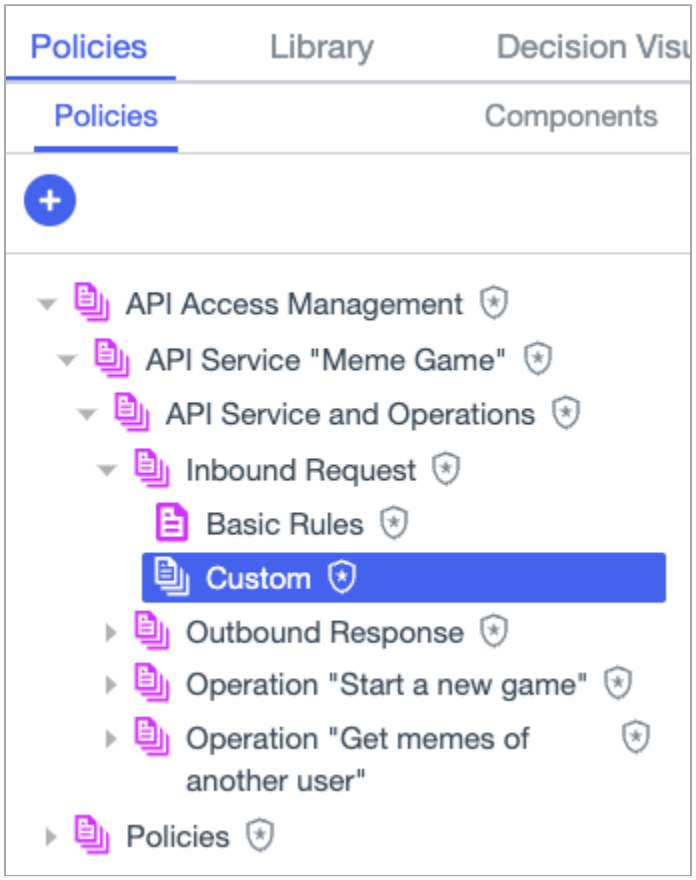
- Add a root policy set to contain all other policy sets. This is useful when you publish the policy tree to a decision endpoint.
- Branches can include policies and other policy sets as children. You can branch the policy tree up to 20 levels deep.
- Policies are evaluated in order from top to bottom in the tree. This allows you to control the order of execution using the structure of the tree.
- Place frequently used policies and policies for lightweight decisions near the top of the tree.

Learn more in Adding a policy or policy set.

API Access Management policy set

The **API Access Management** policy tree is generated when custom policies are enabled for an API service. The tree includes a policy set for each API service, with default policy sets nested under it. You can add your own policies under **Custom** policy sets in the tree.

Copyright © 2025 Ping Identity Corporation



The location of custom policies in the tree determines whether they are relevant to particular requests or responses. For example, a custom policy at the location selected in the image above would target any inbound request to the Meme Game API service. For more information, see Adding custom policies for API services and operations.

Policy components

Use the following components in policies and rules to capture authorization logic:

Conditions

Conditions define authorization logic by comparing one thing to another.

Targets

Targets use comparisons to enable the decision service to determine which policies or rules are relevant to a particular request.

Statements

Statements instruct the policy decision service to perform additional processing in conjunction with an authorization decision. In addition to allowing or blocking access to a resource, using statements, the decision service can attach information to decision responses and filter and transform API payloads.

Copyright © 2025 Ping Identity Corporation

Combining algorithms

To evaluate the overall decision of a policy, the decision service applies a combining algorithm. The algorithm determines how rules are combined to produce an authorization decision.

> **Note**
>
> You can define up to 4000 objects in each environment. This limit includes policies and rules, and also elements in the **Trust Framework**. System-owned objects do not contribute to this limit.

Testing policies

You can test policies from end-to-end with visualization tools that show the complete decision flow. For more information, see Testing policies.

Adding a policy or policy set

Add PingOne Authorize policies to define the circumstances under which users can access certain resources.

About this task

It's helpful to frame your policies in terms of what is permitted or denied.

Use policy sets to group policies and organize them hierarchically.

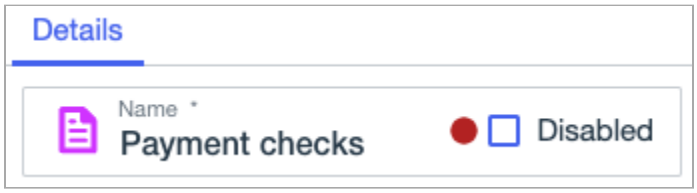
Steps

1. Go to **Authorization** > **Policies**.
2. Click the **+** icon and select one of the following:

   Choose from:

   - **Add Policy Set**: Add policy sets to logically group policies and other policy sets.
   - **Add Policy**: Add policies to logically group rules and other policies.
3. In the **Name** field, enter a name relevant to the business rule that you are modeling.

   > **Note**
   >
   > The red dot on the right indicates that the policy or policy set contains unsaved changes.



4. In **Applies When**, add targets to define when the policy is applied in decision requests.

Copyright © 2025 Ping Identity Corporation

> **Note**
> You cannot copy **Applies When** conditions for reuse in other policies or rules.

5. Add rules, conditions, and statements.

> **Note**
> Use the hamburger menu next to the rule **Name** field to add **Applies When** conditions and statements to rules.

6. **Optional:** Select the **Disable** check box to disable your policy or policy set.

   If you disable the policy, the decision engine skips it in evaluation and produces a `Not Applicable` decision.

> **Note**
> You can also disable rules. If a rule is unreachable because of the rule structure and combining algorithm, disabling that rule has no effect on the final decision.

7. Click **Save changes**.

> **Note**
> To copy a policy or rule for reuse, select **Make Copy** from the hamburger menu of that policy element. You cannot make copies of policy sets.
> If you copy policies containing **Library** rules or statements, those **Library** elements are reused in the new policy, not copied. For example, if you copy a policy that contains a custom rule, which in turn contains a **Library** statement, the rule is copied but the statement is reused.

Targets

Targets define the conditions under which policies and rules are applied to decision requests.

A target enables the decision service to determine which policies or rules are relevant to a particular request. You can use comparisons of attributes, constants, and named conditions in targets. You can also group conditions together. For example, you can target a rule so it applies when a payment amount is greater than or equal to a payment limit.

If the targeting condition is true, the rule or policy will be evaluated. Otherwise, the rule or policy is not applicable to the decision request. You can drag conditions to rearrange them and change the order in which they're evaluated.

> **Note**
> Policies and rules without targets apply to all decision requests.

Statements

Statements are directives that instruct the policy decision service to perform additional processing in conjunction with an authorization decision.

Copyright © 2025 Ping Identity Corporation

Without statements, your policies can tell the decision service to either permit or deny a decision request. With statements, you can include additional information in permit and deny decisions, such as adding response headers when the decision is permit and including a message when the decision is deny. For a statement to apply, the rule or policy must return a permit or deny decision. Statements aren't returned with decisions that are indeterminate or not applicable.

Statements enable you to be more expressive in your policies by allowing you to do things such as add or remove specific fields from requests and responses, return statement codes to DaVinci flows, update risk indicators, and provide authorized records for consent enforcement.

Statements are sometimes called advice and obligations. An obligation is an advice statement that must be fulfilled as a condition of authorizing the decision request.

Statements processed by the dynamic authorization decision service can return statement codes and attributes in decision responses. With an API gateway integration, the API Access Management HTTP Access Policy Service can enforce built-in statements that filter and transform inbound request and outbound response data. PingOne Authorize provides templates for these built-in statements.

For information about using statements in policies, see Adding statements to policies and rules.

Statement templates

PingOne Authorize provides statement templates that you can use in policies out of the box.

Statements templates in the **Library** enable you to easily add statements to policies. Each template includes a statement code, description, and example payload.

To ensure that statement templates are always available, you can't update or delete them. However, you can update a statement cloned from a template. Learn more about using statements in policies in Adding statements to policies and rules.

Built-in statements created from the templates listed below are processed by the API Access Management HTTP Access Policy Service and require an API gateway integration. You can only use these built-in statements in custom policies and rules for API services.

> **Note**
>
> The **Library** can also include other templates created by your organization for statements processed by the dynamic authorization decision service that don't require an API gateway integration.

This HTTP request/response pair is used in several of the examples that follow:

Copyright © 2025 Ping Identity Corporation

Request

```
POST /accounts HTTP/1.1
Host: bankingexample.com:1443
Content-Length: 56
Accept: application/json

{
"ID": "123456",
"amount": "999",
"type": "Savings"
}
```

Response

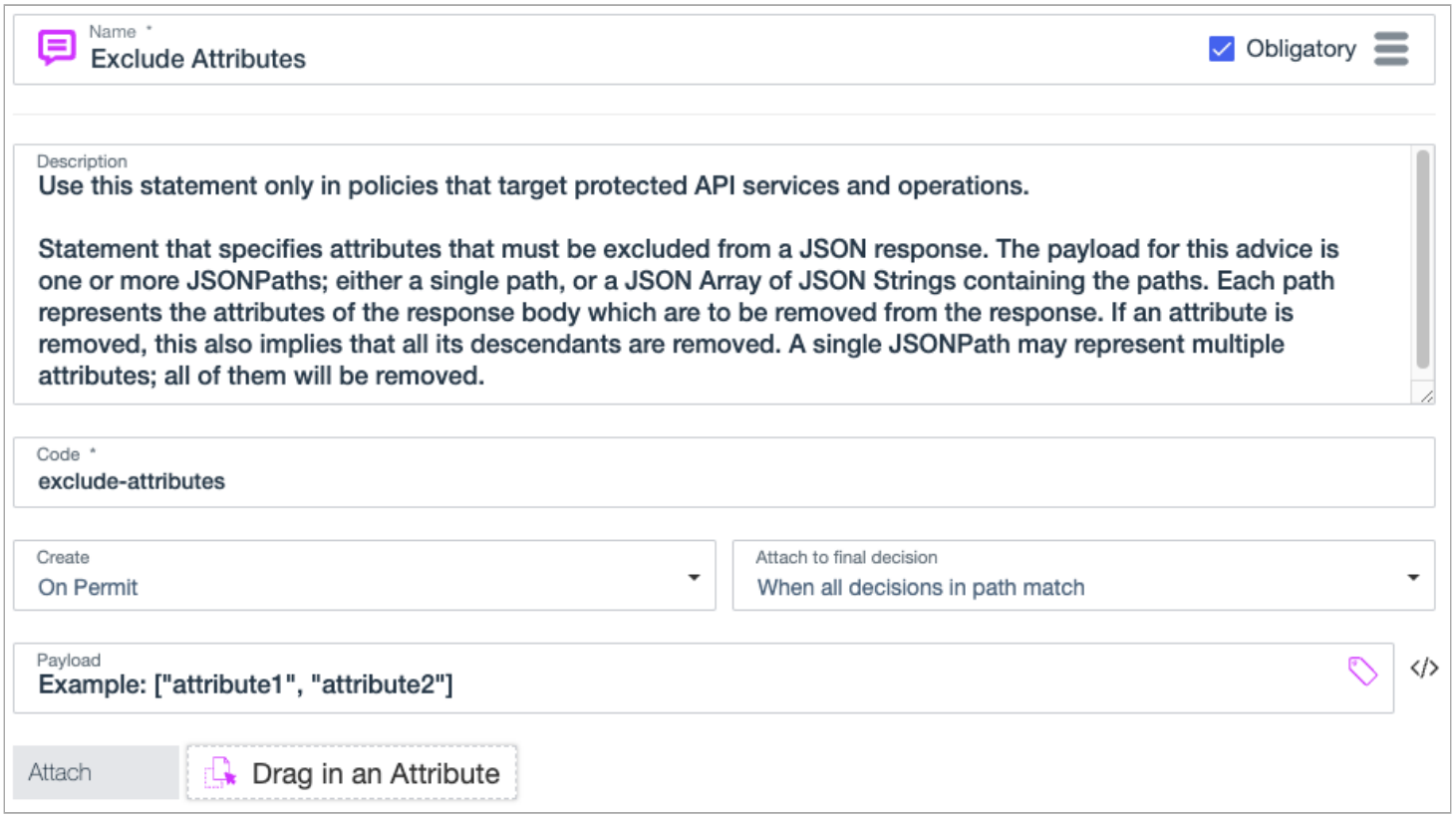
```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 56
Date: Mon, 17 Oct 13:17:18 GMT

{
"ID": "123456",
"amount": "999",
"type": "Savings"
}
```

Exclude attributes

Use the `exclude-attributes` statement to define a list of attributes to exclude from the HTTP response body in an inbound request or outbound response. This statement applies to permit decisions produced by custom API Access Management policies.

> **Tip**
>
> If your protected API is changing over time, consider using the `include-attributes` statement instead of the `exclude-attributes` statement. The `include-attributes` statement is a safer choice that continues to work when you add new attributes to your API.

Copyright © 2025 Ping Identity Corporation



Code

```
exclude-attributes
```

Payload

The payload for this statement is a JSON array of attribute names. This statement limits the attributes in the response body returned to the requester by removing attributes that are listed in the payload.

- If an attribute has descendants, they are also removed from the response body.
- If a single JSONPath expression represents multiple attributes, all of the represented attributes are removed from the response.

Format: `[ "attribute-to-exclude", "attribute-to-exclude" ]`

Example

The following payload instructs the decision service to remove the `amount` attribute from the HTTP response body.

Example payload: `[ "amount" ]`

Original body:

```
{
"ID": "123456",
"amount": "999",
"type": "Savings"
}
```

Copyright © 2025 Ping Identity Corporation

Modified body:

```
{
"ID": "123456",
"type": "Savings"
}
```

Include attributes

Use the `include-attributes` statement to define an allowed list of attributes to include in the HTTP response body in an inbound request or outbound response. This statement applies to permit decisions produced by custom API Access Management policies.

Code

```
include-attributes
```

Payload

The payload for this statement is a JSON array of attribute names. This statement limits the attributes in the response body returned to the requester by removing attributes that are not listed in the payload.

- If a listed attribute has ancestors, the response also includes the ancestors.
- If a single JSONPath expression represents multiple attributes, the response includes all of the represented attributes.

Copyright © 2025 Ping Identity Corporation

- If a policy result returns multiple instances of `include-attributes` statements, the response includes the union of all selected attributes.

Format: `[ "attribute-to-include", "attribute-to-include" ]`

Example

The following payload instructs the decision point to remove the `type` attribute from the HTTP response body.

Example payload: `[ "ID", "amount" ]`

Original body:

```
{
"ID": "123456",
"amount": "999",
"type": "Savings"
}
```

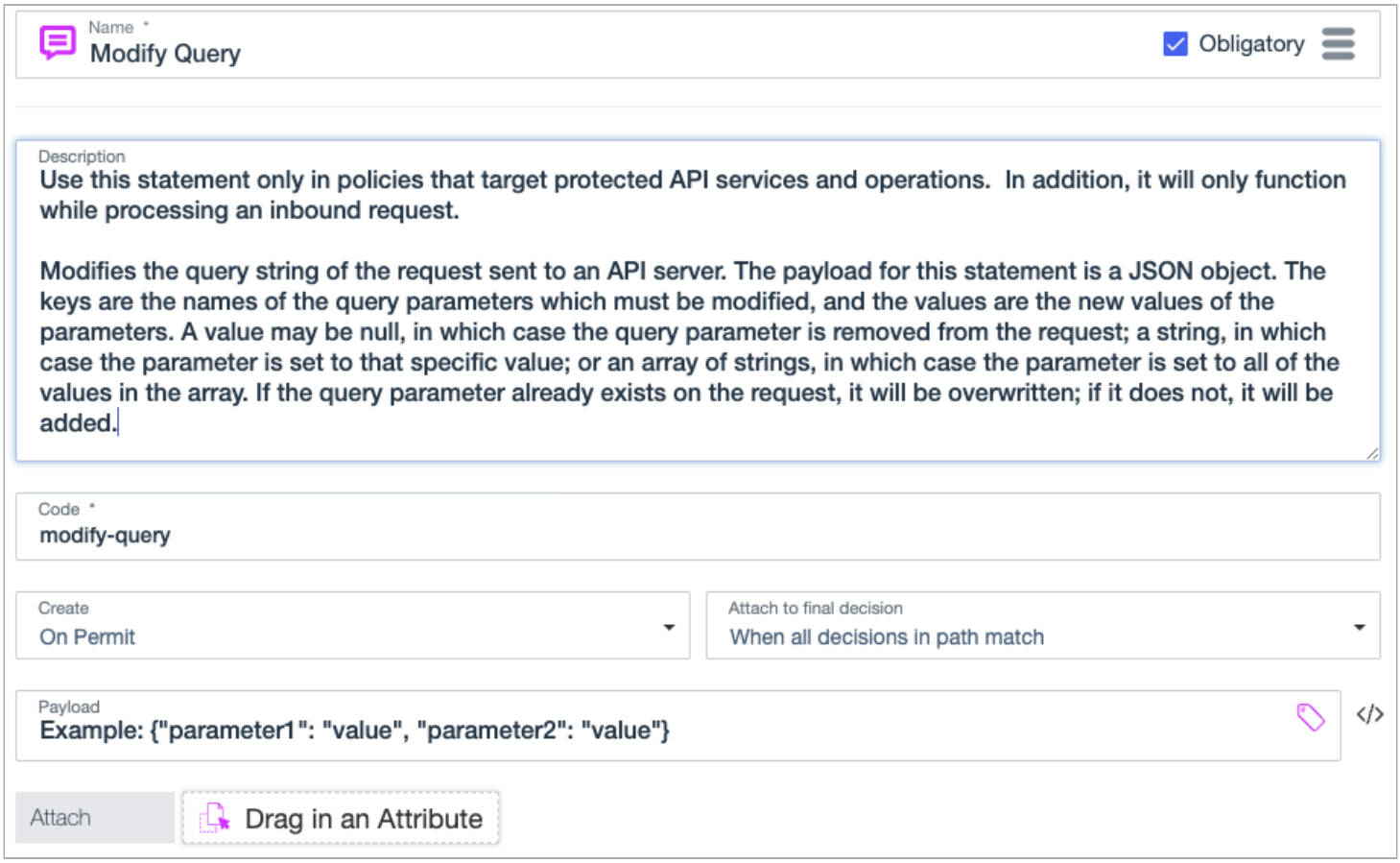
Modified body:

```
{
"ID": "123456",
"amount": "999"
}
```

Modify query

Use the `modify-query` statement to add, update, or remove request URL query parameters. This statement applies to permit decisions produced by custom API Access Management policies. This statement doesn't apply to outbound responses.

Copyright © 2025 Ping Identity Corporation



Code

```
modify-query
```

Payload

The payload for this statement is a JSON object that contains key-value pairs. For each pair, the key is the name of the query parameter to modify, and the value is the new value of the query parameter. The value can be:

- `null` : Removes the query parameter from the request.
- String: Sets the query parameter to that specific value.
- Array of strings: Sets the query parameter to all of the values in the array.

If the query parameter already exists in the request, the decision service overwrites it. If the query parameter does not already exist, the decision service adds it, unless the value is `null`.

Format: `{ "queryParameter": "parameter-value" }`

Example

The following payload instructs the decision service to modify a query parameter that returns 20 accounts at a time to return 10 instead.

Example payload: `{ "limit":"10" }`

Original request:

Copyright © 2025 Ping Identity Corporation

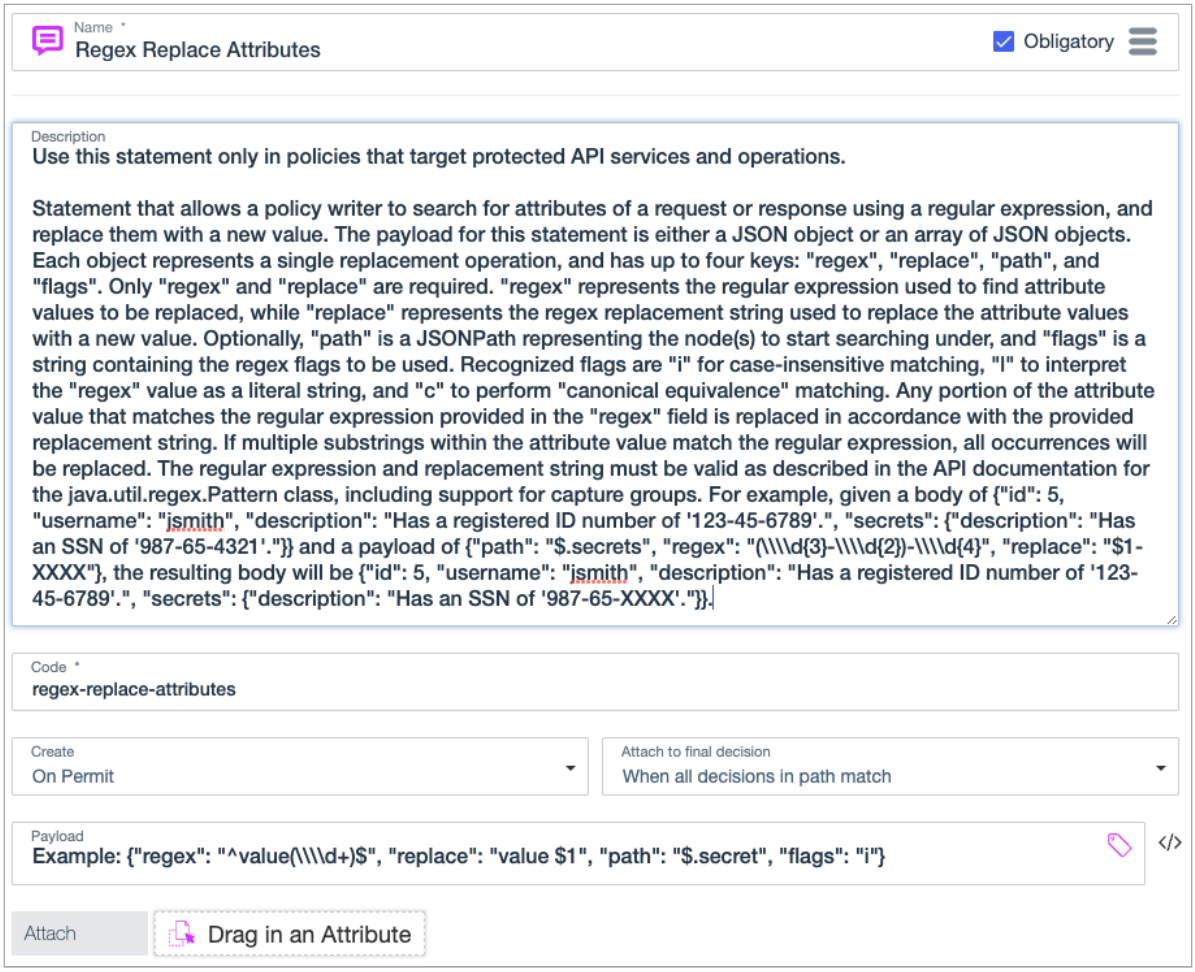
```
GET /accounts?limit=20 HTTP/1.1
Host: bankingexample.com:1443
Accept: application/json
```

Modified request:

```
GET /accounts?limit=10 HTTP/1.1
Host: bankingexample.com:1443
Accept: application/json
```

Regex replace attributes

Use the `regex-replace-attributes` statement to use regular expressions to search for and replace attribute values in the HTTP response body in an inbound request or outbound response. This statement applies to permit decisions produced by custom API Access Management policies.



Code

```
regex-replace-attributes
```

Payload

The payload for this statement is a JSON object that contains key-value pairs, or an array of JSON objects. Each JSON object represents a single replacement operation and has up to four keys:

- `path`: Optional. A JSONPath expression that represents the nodes to search under. The expression can point to objects, arrays, or strings in the body.
- `regex`: Required. The regular expression used to find the attribute values to replace.
- `replace`: Required. The regex replacement string used to replace the attribute value with a new value.
- `flags`: Optional. A string that contains any of the following recognized regex flags:
  - `i`: Performs case-insensitive matching.
  - `l`: Interprets the `regex` key's value as a literal string.
  - `c`: Performs canonical equivalence matching.

  You can combine flags. For example: "`il`".

The decision service replaces any portion of the attribute value that matches the regular expression in the `regex` key's value in accordance with the `replace` key's replacement string. If multiple substrings in the attribute value match the regular expression, the decision service replaces all occurrences.

The regular expression and replacement string must be valid, as described in the API documentation for the java.util.regex.Pattern class, including support for capture groups.

Format: `{ "path": "$.jsonPath", "regex": "regex", "replace": "replacement-value" }`

Example 1

The following payload instructs the decision service to replace the account type `Savings` with the account type `PremierSavings`.

Example payload:

```
{
"path":"$.type",
"regex":"^S[a-z]+s$",
"replace":"PremierSavings"
}
```

Original body:

```
{
"ID": "123456",
"amount": "999",
"type": "Savings"
}
```

Modified body:

Copyright © 2025 Ping Identity Corporation

```
{
"ID": "123456",
"amount": "999",
"type":"PremierSavings"
}
```

Example 2

The following payload instructs the decision service to mask the social security number.

Example payload:

```
{
"regex": "\\\\d{3}-\\\\d{2}-(\\\\d{4})",
"replace": "XXX-XX-$1"
}
```

As an alternative, you can use a different regular expression to do the same thing:

```
{
"regex": "[0-9]{3}-[0-9]{2}-([0-9]{4})",
"replace": "XXX-XX-$1"
}
```

Original body:

```
{
"name": "Jacob Andrews",
"age": "39",
"SSN": "123-45-6789"
}
```

Modified body:

```
{
"name": "Jacob Andrews",
"age": "39",
"SSN": "XXX-XX-6789"
}
```

Respond with authentication step-up challenge

Use the `auth-challenge` statement to implement step-up authentication challenges in policies that protect API services and operations. In step-up authentication, HTTP servers use the `WWW-Authenticate` response header to challenge OAuth 2.0 clients to provide sufficient credentials. Learn more about authentication challenges and bearer token usage in RFC 9470 and RFC 6750.

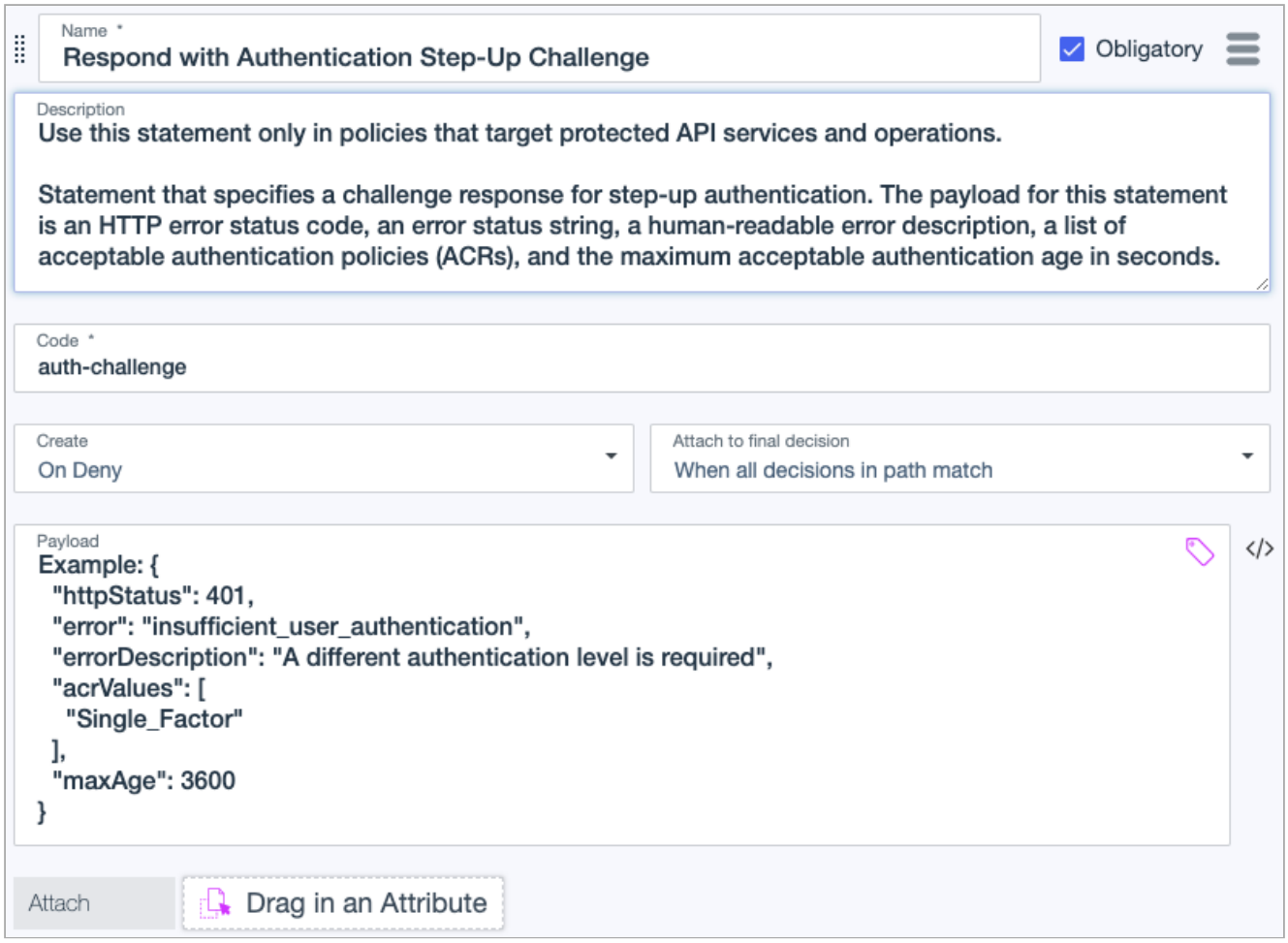
Copyright © 2025 Ping Identity Corporation

The `auth-challenge` statement:

- Applies to deny decisions produced by inbound decision requests only
- Adds the `WWW-Authenticate` header to deny responses

> **Note**
>
> This header isn't added to deny responses when you use the Amazon Web Services integration kit.

Learn more in Step-up authentication.



Code

```
auth-challenge
```

Payload

The payload for this statement is a JSON configuration object with the following properties:

Property	Type	Required	Description
`httpStatus`	Number	Required	The HTTP response status code to send to the client. Example: `401`

Copyright © 2025 Ping Identity Corporation

Property	Type	Required	Description
`scheme`	String	Optional	The challenge type. When this is not set, the default is `"Bearer"`.
`realm`	String	Optional	Provides the scope of protection as a hint to the end user about which credentials are needed.
`error`	String	Required	An error code. Standard error codes are defined by RFC 6749, RFC 6750, and RFC 9470. Example: `"insufficient_user_authentication"`
`errorDescription`	String	Optional	A human-readable error description for informational purposes that is meant for developers, not end-users. Example: `"A different authentication level is required"`
`errorUri`	String	Optional	An absolute URI that identifies a Web page explaining the error. Example: `"https://example.com/insufficient_user_authentication"`
`acrValues`	Array (String)	Optional	The authentication context class reference values, in order of preference, that the protected resource requires for the authentication event associated with the access token. Values are separated by spaces and can include the PingOne SSO policy name or DaVinci flow ID. **Note** If you are using PingOne as your identity provider (IdP), PingOne SSO only considers the first listed value in authorization requests. Other IdPs might support multiple values. `acrValues` provide authentication context that conveys information about how authentication takes place, such as the authentication methods or assurance level to meet. Example: `["Single_Factor"]`
`maxAge`	Number	Optional	The allowable elapsed time in seconds since the last active authentication event associated with the access token. Example: `3600`
`scopes`	Array (String)	Optional	An array of OAuth 2.0 scopes required to access the protected resource. Example: `["scope1","scope2"]`

Format:

Copyright © 2025 Ping Identity Corporation

```
{
  "httpStatus": 401,
  "error": "insufficient_user_authentication",
  "errorDescription": "Description",
  "acrValues": [
    "Authentication_Method"
  ],
  "maxAge": number of seconds
}
```

Example

The following payload instructs the decision service to construct an authentication challenge informing the requesting client that a different authentication level (multi-factor) and more recent authentication (within the last hour) are required.

Example payload:

```
{
  "httpStatus": 401,
  "error": "insufficient_user_authentication",
  "errorDescription": "A different authentication level is required. More recent authentication is required.",
  "acrValues": [
    "Multi_Factor"
  ],
  "maxAge": 3600
}
```

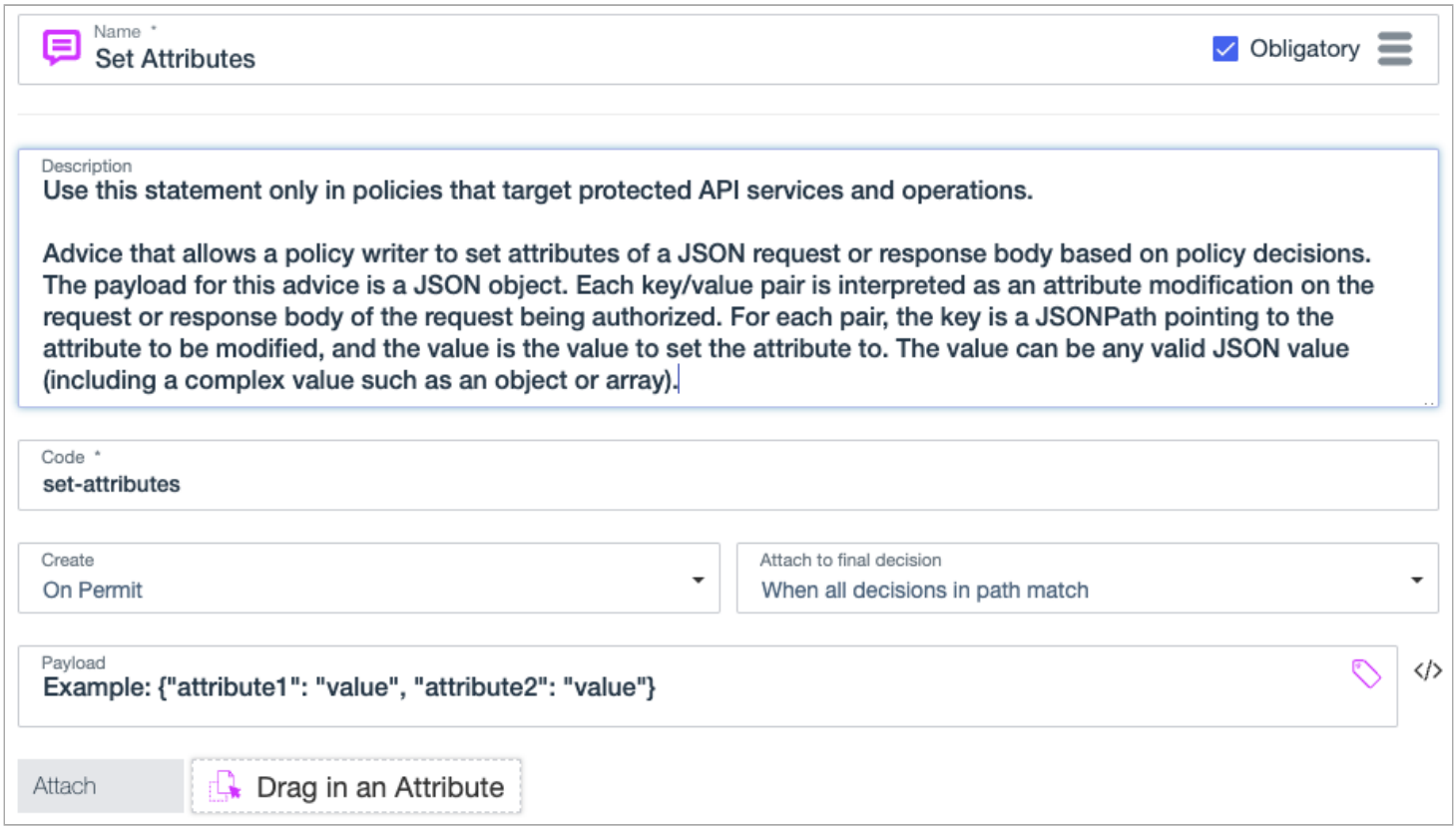
Example HTTP response status and `WWW-Authenticate` header value:

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer error="insufficient_user_authentication",
     error_description="A different authentication level is required. More recent authentication is required.",
     acr_values="Multi_Factor",
     max_age="3600"
```

Set attributes

Use the `set-attributes` statement to add, update, or remove attribute values in the HTTP response body in an inbound request or outbound response. This statement applies to permit decisions produced by custom API Access Management policies.

Copyright © 2025 Ping Identity Corporation



Code

```
set-attributes
```

Payload

The payload for this statement is a JSON object that contains key-value pairs. Each key-value pair is interpreted as an attribute modification on the request or response body of the request being authorized. For each pair, the key is a JSONPath expression that points to the attribute being modified, and the value is the new value for the attribute.

The value can be any valid JSON value, including a complex value such as an object or array. A `null` value removes the attribute from the HTTP body. Key-value pairs that do not already exist are added to the HTTP body, unless the value is `null`.

Format: `{ "$.jsonPath": "attributeValue" }`

Example

The following payload instructs the decision service to replace the account type `Savings` with the account type `PremierSavings`.

Example payload: `{ "$.type":"PremierSavings" }`

Original body:

```
{
"ID": "123456",
"amount": "999",
"type": "Savings"
}
```

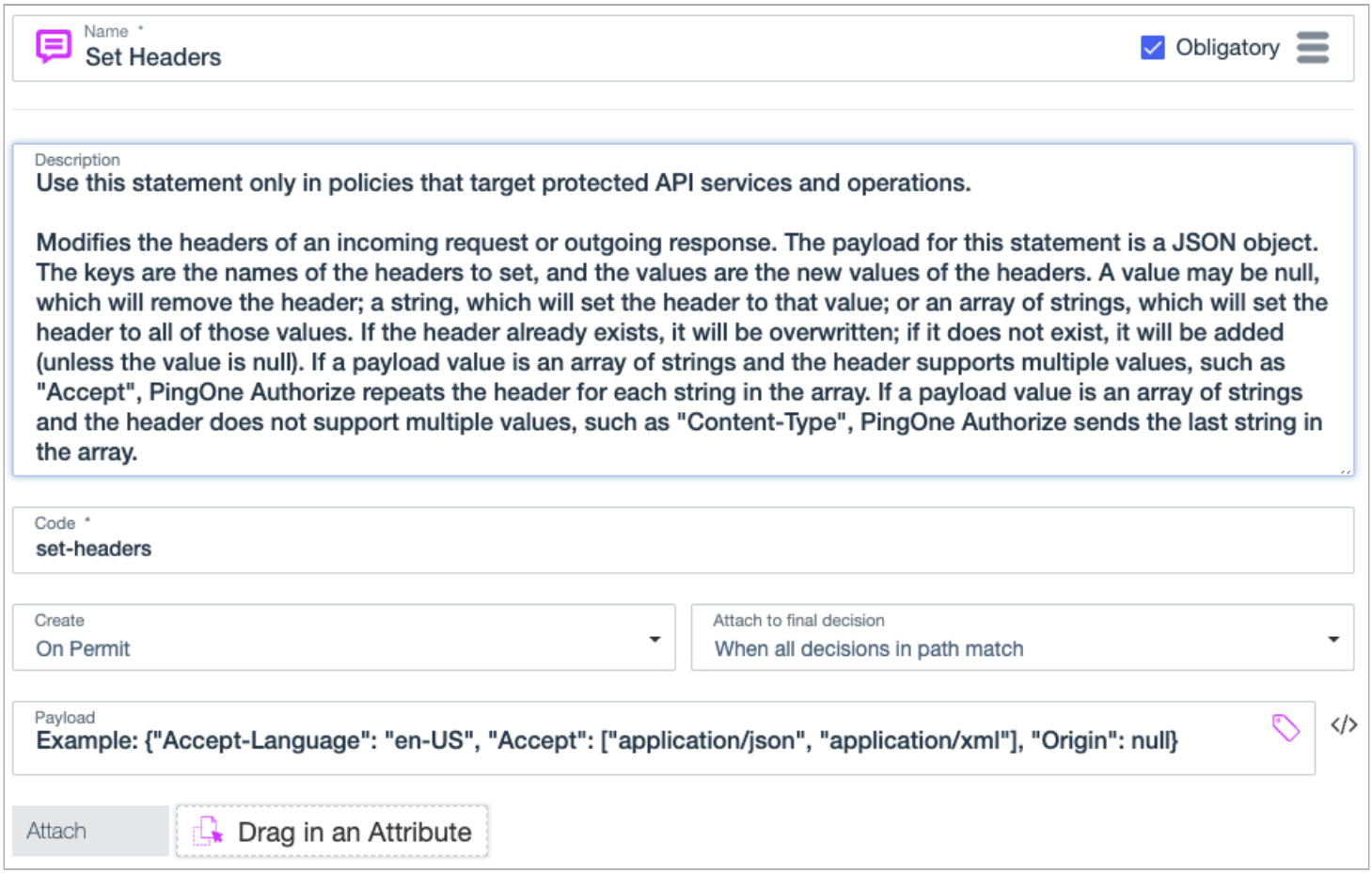
Copyright © 2025 Ping Identity Corporation

Modified body:

```
{
"ID":"123456",
"amount":"999",
"type":"PremierSavings"
}
```

Set headers

Use the `set-headers` statement to add, update, or remove HTTP request and response headers before they're returned to the API gateway. This statement applies to permit decisions produced by custom API Access Management policies.



Code

```
set-headers
```

Payload

The payload for this statement is a JSON object that contains key-value pairs. For each pair, the key is the name of the header field to set, and the value is the new value of the header field. The value can be:

- `null`: Removes the header field.
- A string: Sets the header field to that value.

Copyright © 2025 Ping Identity Corporation

- An array of strings: Sets the header field to all of the string values.

  If the header field supports multiple values, such as the `Accept` field, the decision service repeats the header field for each string in the array. If a header field doesn't support multiple values, such as the `Content-Type` field, the decision service sets the header field to the last string in the array.

If a header field already exists, the decision service overwrites it. If a header field doesn't already exist, the decision service adds it, unless the value is `null`.

Format: `{ "Header-Name": "header-value" }`

Example

The following payload instructs the decision service to add a custom request header.

Example payload: `{ "X-UserName": "user@bankexample.com" }`

Original headers:

```
Host: bankingexample.com:1443
Content-Length: 13
Accept: application/json
```

Modified headers:

```
Host: bankingexample.com:1443
Content-Length: 13
Accept: application/json
X-UserName: user@bankexample.com
```

Adding statements to policies and rules

Include statements in rules and policies to perform additional processing as part of an authorization decision.

About this task

You can add statements to the policy as a whole and to individual rules, or you can pull in statement templates from the **Library**.

> **Note**
>
> Some built-in statements require an API gateway integration and a policy or rule that targets an API service.

You can drag collapsed statements to rearrange them and change the order in which they are evaluated.

Steps

1. Go to **Authorization > Policies**, and click a policy or add a new policy.
2. Do one of the following to add a statement.

   Choose from:

   - In the **Statement** section, click **+Add Statement**.

Copyright © 2025 Ping Identity Corporation

- From the **Library** on the **Components** tab, drag a statement template into the **Statement** section. Statements pulled in from the **Library** are read-only. To make changes to the statement, click the hamburger menu next to the **Obligatory** check box and select **Replace with clone**.

> **Tip**
>
> - Changes you make to a clone don't affect the template in the **Library**.
> - You can add statements to individual rules the same way that you add them to policies. To add a statement to a rule, click the hamburger menu next to the rule **Name** field and select **Add Statement**. Then click **+ Add Statement** or drag a statement template from the **Library** to the **Statement** section in the rule.

3. Enter a **Name** and an optional **Description** for the statement.

4. **Optional:** If the statement must be fulfilled as a condition of authorizing the decision request, select the **Obligatory** check box.

   If the decision service can't fulfill an obligatory statement, the decision evaluation fails and the decision service returns an error to the client application. When a non-obligatory advice statement can't be fulfilled, the decision service logs an error and continues the decision evaluation.

5. Enter a statement **Code** to identify the type of statement.

   If you pulled in a statement template, use the default code populated from the template. Otherwise, enter your own code. For example, you can enter a code such as `MFA_REQ` or `APPROVE` to return a statement code to a DaVinci flow.

   For more information about built-in statement codes and payloads, see Statement templates.

6. In the **Create** list, select the kinds of decisions produced by the policy or rule that will create the statement.

   Statements can apply to `permit`, `deny`, `permit or deny`, or `indeterminate` decisions. Select **When Applicable** if the statement applies to any of these. This is the default option.

> **Tip**
>
> If you're using a built-in statement in a policy that targets protected API services and operations, make sure you select **On Permit**. If the policy or rule produces a deny decision, built-in statements are not processed.

Copyright © 2025 Ping Identity Corporation

7. In the **Attach to final decision** list, select an option for how the statement propagates through the decision tree and whether it is returned in the overall decision response.

   Choose from:

   - **When all decisions in path match**: The statement is returned when the decision for the rule or policy with which the statement is associated matches all decisions in the path. For example, when the decision for the rule with which the statement is associated is `permit`, and all decisions in the path are `permit`, the statement is returned. This is the default option.
   - **When final decision matches "Create" condition**: The statement is returned when the decision for the rule or policy with which the statement is associated matches the overall decision. For example, when the decision for the rule with which the statement is associated is `permit`, and the overall decision is `permit`, the statement is returned even if there are deny decisions in between.
   - **Always**: The statement is always returned, unless there's an error in the associated decision.

8. **Optional:** In the **Payload** field, enter JSON parameters that govern the actions that the decision point performs when it applies the statement.

   Payloads can include static or interpolated data and provide instructions for things such as filtering and transforming headers, query parameters, and request and response bodies. For payload examples, see Statement templates.

Copyright © 2025 Ping Identity Corporation

> **Tip**
>
> To experiment with JSONPath expressions, use a JSONPath evaluator, such as the JSONPath Online Evaluator.

9. **Optional:** To include attributes relevant to the statement in the decision response, drag one or more attributes from the **Components** tab to the **Attach** field.
10. **Optional:** To add the statement to the **Library** as a reusable component, click the hamburger menu next to the **Obligatory** check box and select **Add to library**.
11. Click **Save changes**.

Next steps

> **Note**
>
> To reuse a statement in other policies or rules, you can make a copy of it by selecting **Make Copy** from the hamburger menu of that statement. You can copy custom **Library** statements and statements in Library rules, but you cannot copy top-level, bootstrapped Library statements.
> You can copy any Library statement at its point of use. If you copy a Library statement in a rule or policy, the copy displays at the point of use and on the **Library** tab.

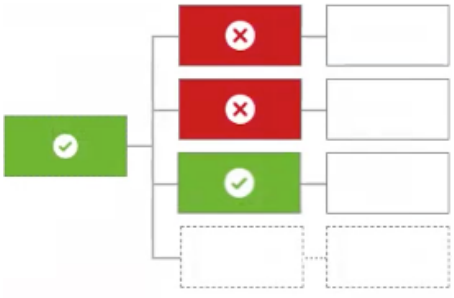
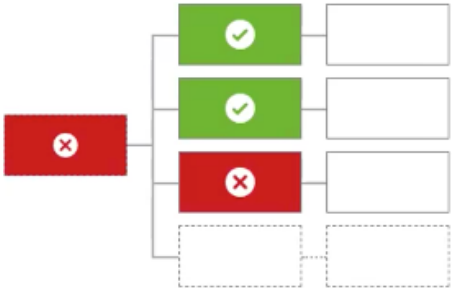
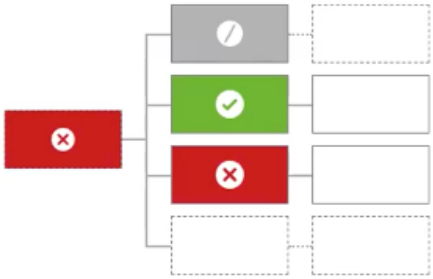
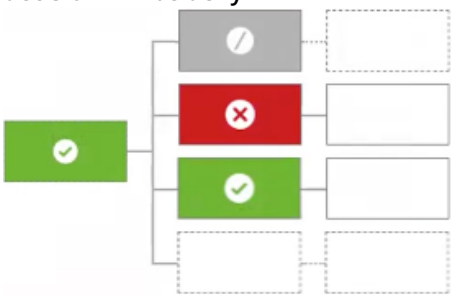
Combining algorithms

PingOne Authorize policies can combine multiple rules to produce a `Permit`, `Deny`, `Indeterminate`, or `Not Applicable` decision.

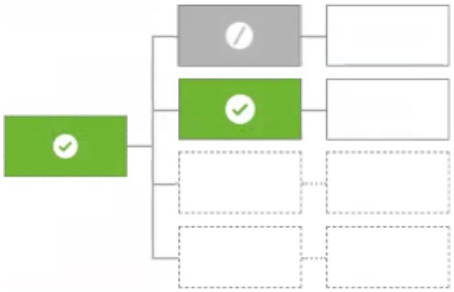
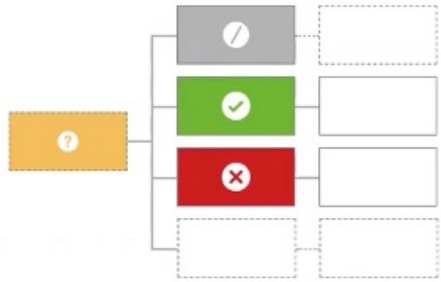
To evaluate the overall decision of a policy, the decision service applies a combining algorithm. The default algorithm for a new policy is **The first applicable decision will be the final decision**. This algorithm stops evaluating as soon as it reaches a decision that isn't `Not Applicable`.

The following table identifies available combining algorithms and describes their effects. The diagrams show one example of a decision evaluation for each combining algorithm; other evaluation paths are possible. The diagram legend is displayed before the table. The first column in each diagram represents the overall decision returned by the policy. The second column represents child decisions that produce the resulting policy decision.

Copyright © 2025 Ping Identity Corporation

Combining algorithm	Details
A single permit will override any deny decisions 	If any children produce the decision `Permit`, the policy returns `Permit` and stops evaluating rules. If no `Permit` is generated, all rules are evaluated. The policy returns `Indeterminate` if a child produces `Indeterminate`. Otherwise, the policy returns `Deny` if a child produces `Deny`. If none of the previous situations occur, the policy returns `Not Applicable`.
A single deny will override any permit decisions 	If any children produce the decision `Deny`, the policy returns `Deny` and stops evaluating rules. If no `Deny` is generated, all rules are evaluated. The policy returns `Indeterminate` if a child produces `Indeterminate`. Otherwise, the policy returns `Permit` if a child produces `Permit`. If none of the previous situations occur, the policy returns `Not Applicable`.
Unless one decision is deny, the decision will be permit 	The policy defaults to `Permit` unless any of its children produce the decision `Deny`. The evaluation of rules stops as soon as a `Deny` is produced.
Unless one decision is permit, the decision will be deny 	The policy defaults to `Deny` unless any of its children produce the decision `Permit`. The evaluation of rules stops as soon as a `Permit` is produced.

Copyright © 2025 Ping Identity Corporation

Combining algorithm	Details
The first applicable decision will be the final decision 	The decision engine evaluates the children in turn until one produces an applicable value of `Permit`, `Deny`, or `Indeterminate`. If the evaluation produces no applicable decisions, the policy returns `Not Applicable`.
Only one child may produce a decision. If more than one is produced, the result will be indeterminate 	The decision engine evaluates the children in turn. If at any point two children produce a decision other than `Not Applicable`, evaluation stops and the policy returns `Indeterminate`. If at any point a single child produces an `Indeterminate` decision, evaluation stops and the policy returns `Indeterminate`. If exactly one child produces an applicable decision, the policy uses it. If evaluation produces no applicable decisions, the policy returns `Not Applicable`.

Policy testing

PingOne Authorize allows you to test policies from end-to-end with visualization tools that show the complete decision flow.

You can test statement transformations using custom decision request parameters and simulated API requests and responses.

For more information, see:

- Testing policies
- Testing statement processing

Testing policies

Test PingOne Authorize policies from end-to-end with visualization tools that show the complete decision flow.

Steps

1. Go to **Authorization** > **Policies**.
2. Select the policy you want to test, and then click the **Test** tab.

Copyright © 2025 Ping Identity Corporation

3. Define the test scenario:

    1. (Optional) To include a PingOne user ID as context in the decision request, search for a user in the **PingOne User** field.

    > **Important**
    >
    > If you are testing an element that depends on the `PingOne.User` attribute, you must select a user to avoid a `MISSING_ATTRIBUTE` error.
    > The selected user must be defined in the current PingOne environment.

    2. In the **Attributes** list, select any attributes that you want to include as request parameters, and provide sample values.

    > **Tip**
    >
    > Click the angle brackets next to an attribute to display a JSON text editor.

    3. In the **Overrides** section, configure attribute and service values if you want to override those elements' default behavior.

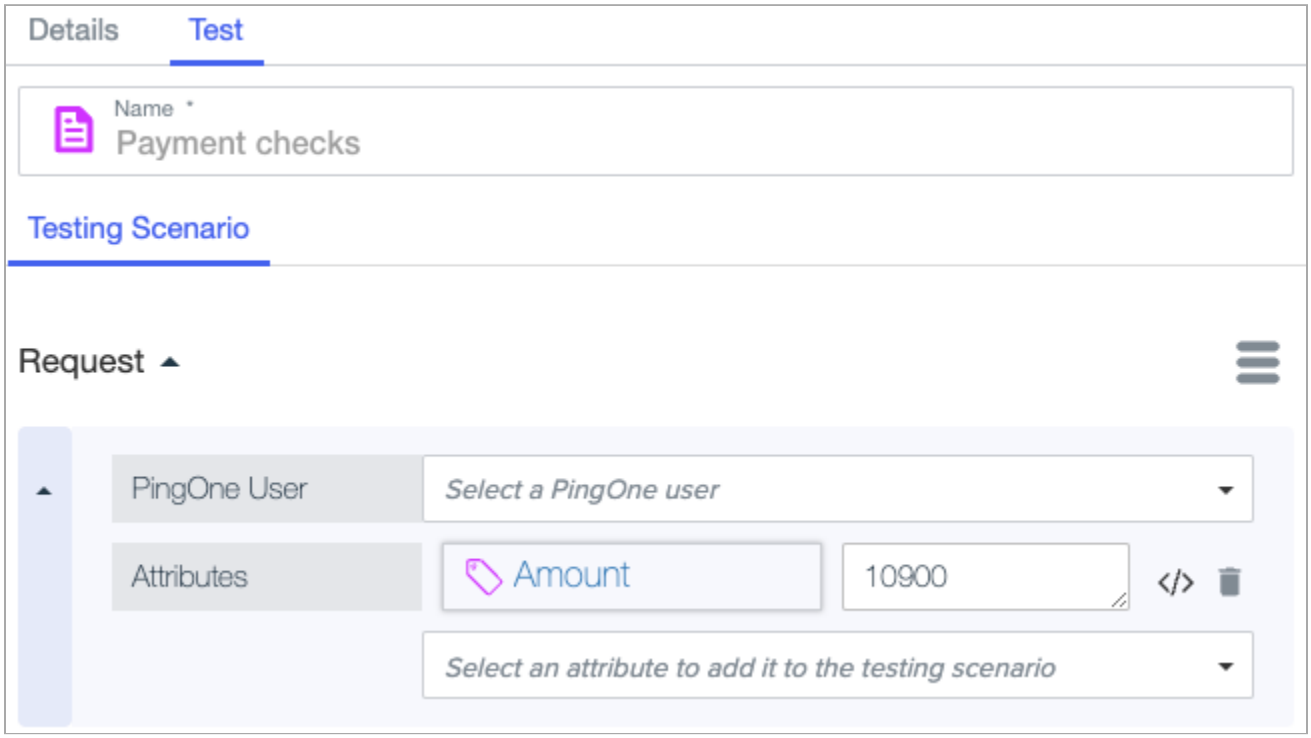
    For example, if an attribute is defined with a request parameter resolver, and no value is specified in the test request, the decision service resolves that attribute from the **Overrides** configuration.

> **Note**
>
> You can also click the **Import JSON** button to define the test scenario with a JSON text editor.

Example:

Using the **Payment checks** policy from the tutorials as an example, the following testing scenario uses the **Amount** attribute in a request to test whether the policy denies payments over 10,000 USD.

Copyright © 2025 Ping Identity Corporation



4. **Optional:** To process statements on a simulated API request or response, select the **Process Statements** check box.

   Learn more in Testing statement processing.

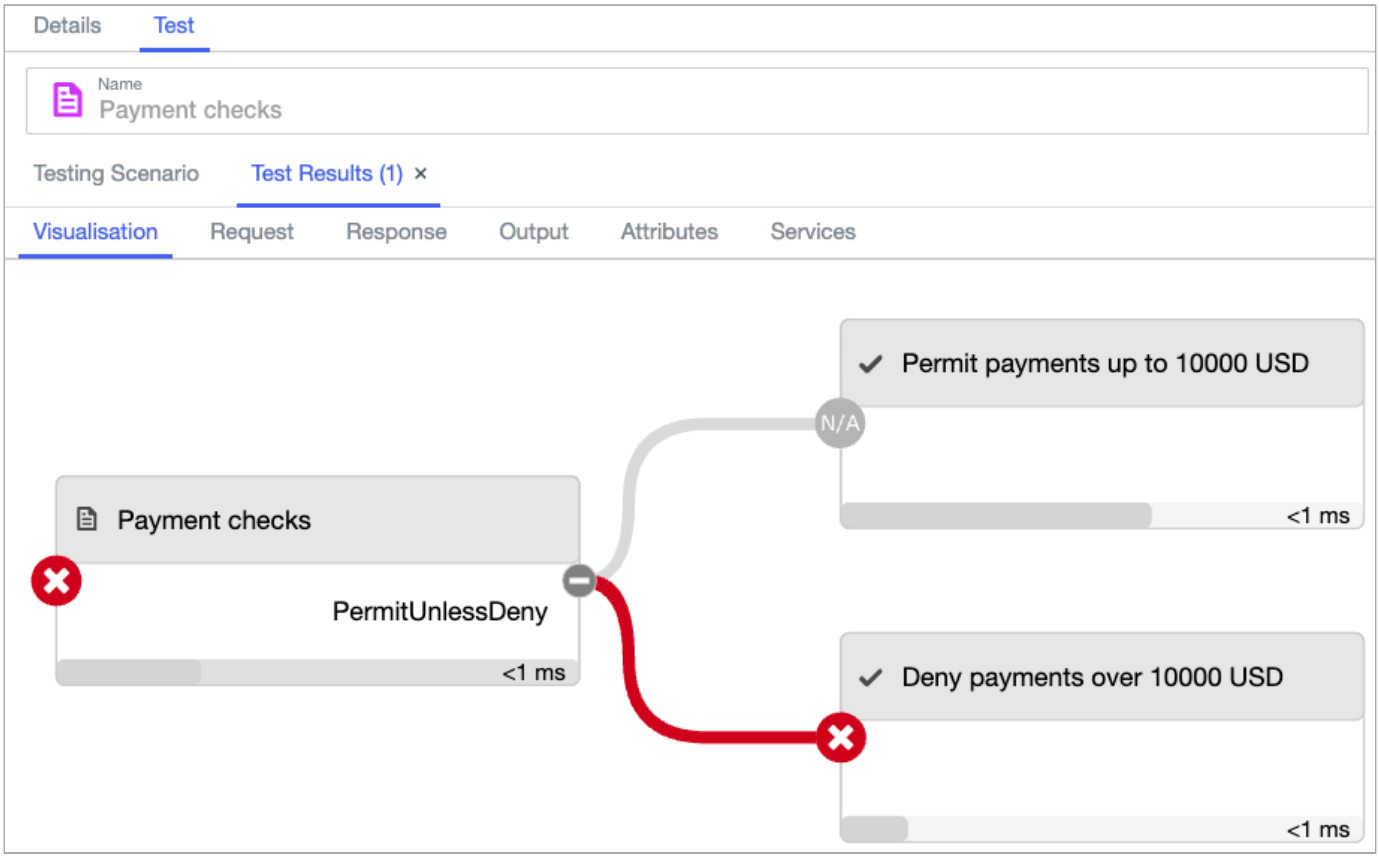
5. Click **Execute**.

> **Note**
>
> If the test scenario exceeds 50 kB in size, sample values will not be stored in the local cache after executing the test request.

Result:

The **Visualization** tab shows test results. As expected, the payment is denied.

Copyright © 2025 Ping Identity Corporation



6. Examine the decision flow to make sure decisions are evaluated according to your expectations.

   You can click any box in the flow to show more details.

7. Click the other tabs for additional details:

   - **Request** tab: Shows the JSON request sent to the decision service, allowing you to confirm that the expected information was sent.

     If you enabled statement processing, this tab also shows the API request or response.

   - **Response** tab: Shows the complete, high-verbosity response for the decision, including expanded errors and other helpful information.

     If you enabled statement processing, this tab also shows the transformed API request or response body and other statement processing details.

     > **Note**
     >
     > If the same comparison condition is attached to more than one rule in the policy subtree, the decision response only includes evaluation of the first occurrence of this condition. Despite only appearing once in the response, the decision service evaluates this condition wherever it is needed to make a decision. If the parent policy of the first instance of this condition is not applicable to the request, the decision response does not include evaluation of any rule containing this condition. This behavior is the same regardless of the rule's outcome (`Permit` , `Deny` , `Not Applicable`).

   - **Output** tab: Shows details about the decision, including the time it took to evaluate policies and rules.

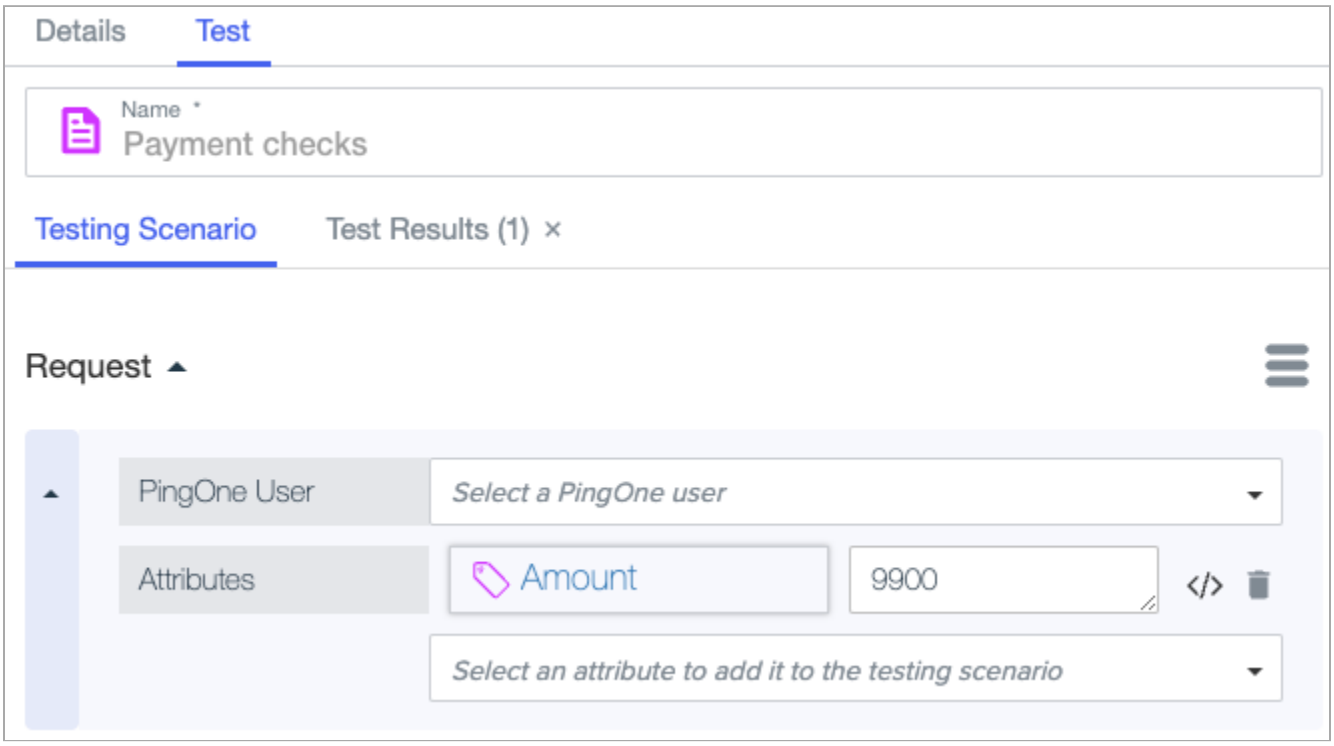
Copyright © 2025 Ping Identity Corporation

- **Attributes** tab: Shows details about the attributes used in the decision.
- **Services** tab: Shows details about the services used in the decision.
- **Processing Result** tab: Shows the transformed API request or response body with statements applied, along with any specified URI and headers. This tab is only displayed if you enabled statement processing.

8. To repeat the test using a different scenario, click the **Testing Scenario** tab, change the parameters, and then click **Execute**.

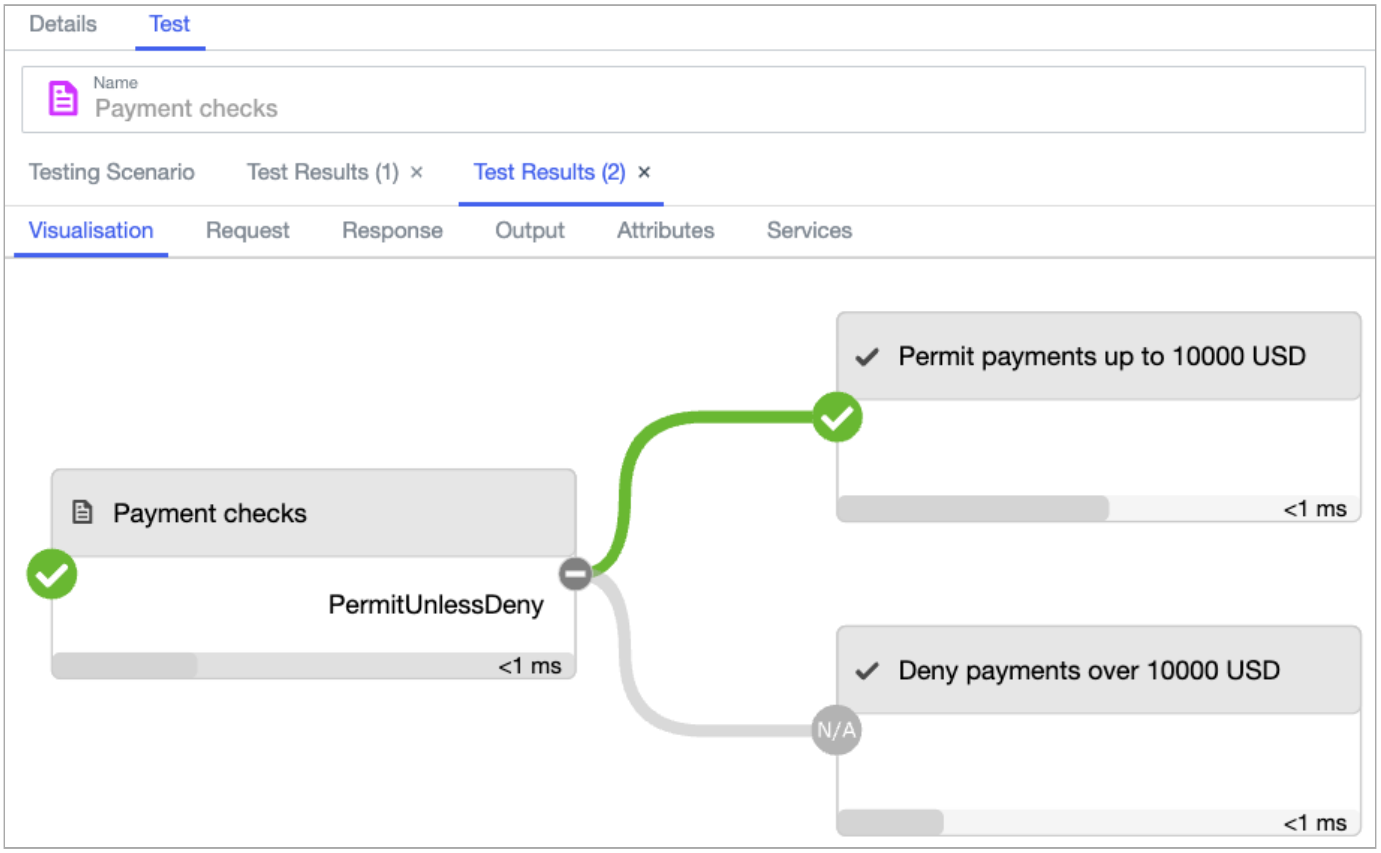
   Example:

   The following example tests an **Amount** value that is less than 10,000 USD.



A second **Visualization** tab shows test results. This time the payment is permitted. **Test Results** tabs are numbered to help you keep track of testing scenarios in the order in which they're run. If you delete a tab, for consistency, numbering remains the same for any remaining tabs.

Copyright © 2025 Ping Identity Corporation



Testing statement processing

When testing PingOne Authorize policies, you can enable statement processing to test API request and response transformations without using an external testing service.

Before you begin

Make sure you have defined an API service, as well as a custom policy with transformational statements protecting that service.

About this task

> **Note**
>
> PingOne Authorize only processes built-in statements defined in custom policies and rules for API services. For more information, see Statement templates.

Steps

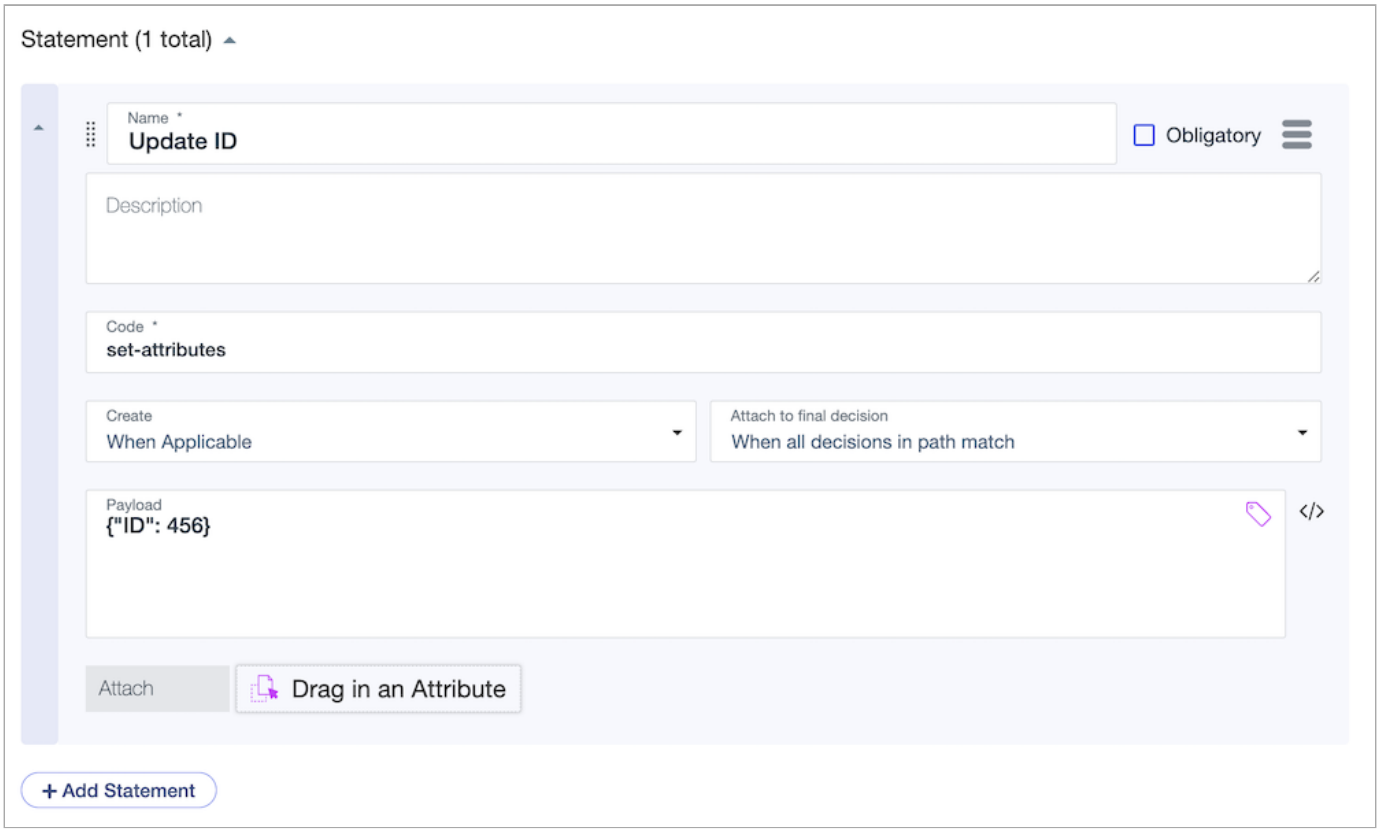
1. Go to **Authorization** > **Policies**.
2. Select the policy that you want to test, and then click the **Test** tab.
3. Define test parameters.
4. Select the **Process Statements** check box, and select **REQUEST** or **RESPONSE** depending on which stage of the API request flow you want to test.

Copyright © 2025 Ping Identity Corporation

5. In the **API Request** form, configure the testing scenario.

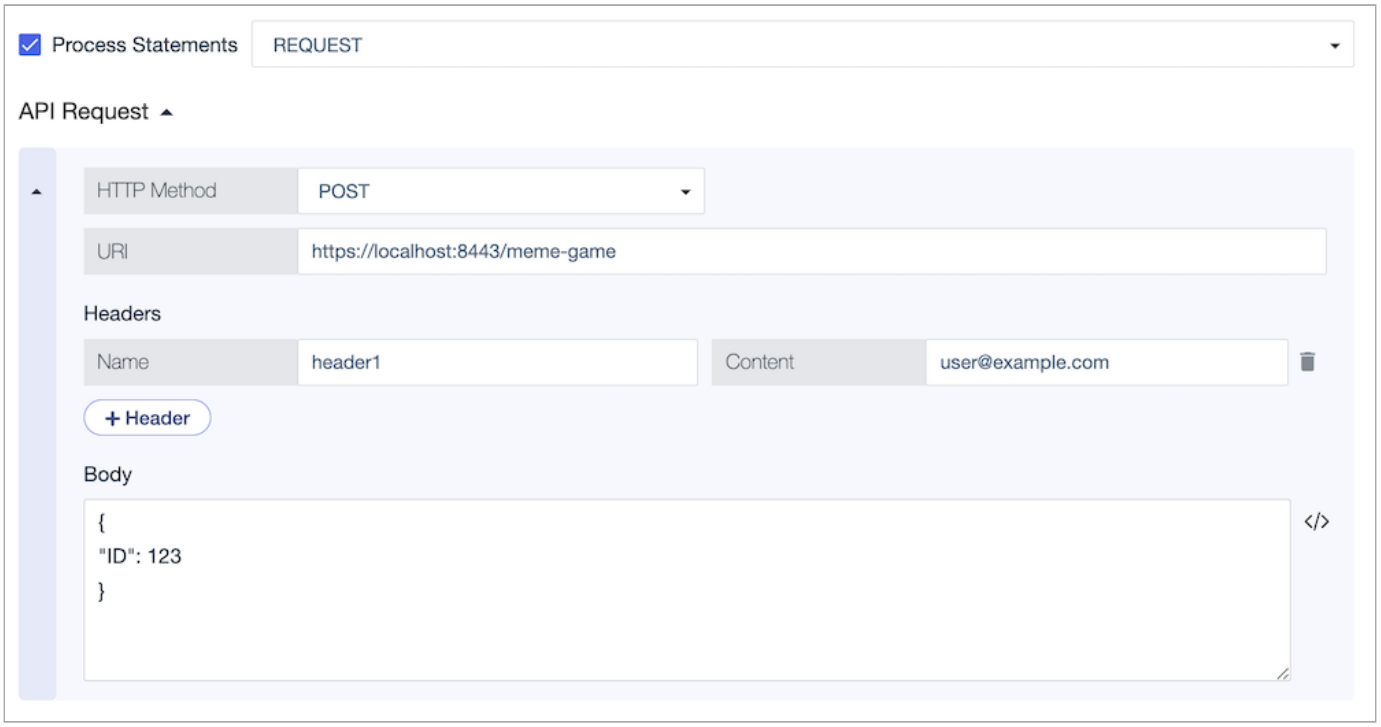
   Example:

   For example, consider the **Users starting a new game** policy from the tutorials. You can add a `set-attributes` statement to update the `ID` attribute in an API request.



   Then, use the following testing scenario to test the statement.

Copyright © 2025 Ping Identity Corporation

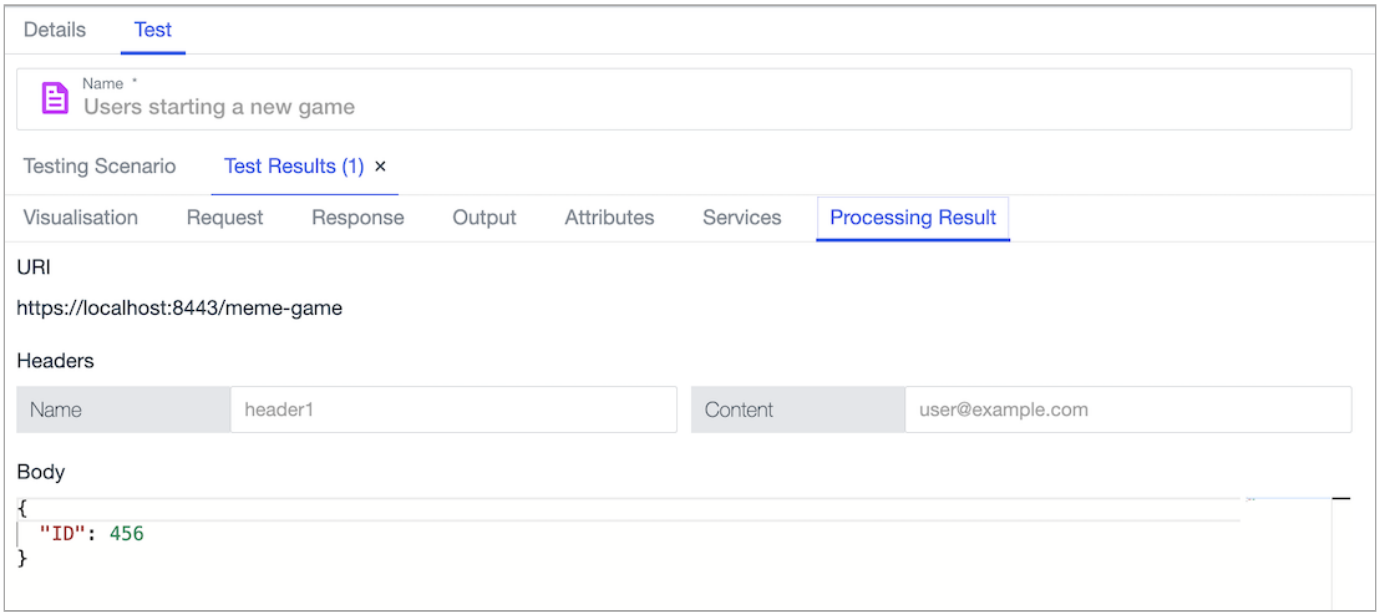


> **Note**
>
> Click the angle brackets next to the **Body** field to display a rich JSON text editor.

6. Click **Execute**.

   Result:

   The **Visualization** tab shows test results. The **Processing Result** tab displays the transformed API request or response body with statements applied, along with any specified URI and headers. This tab is only displayed if you enabled statement processing.



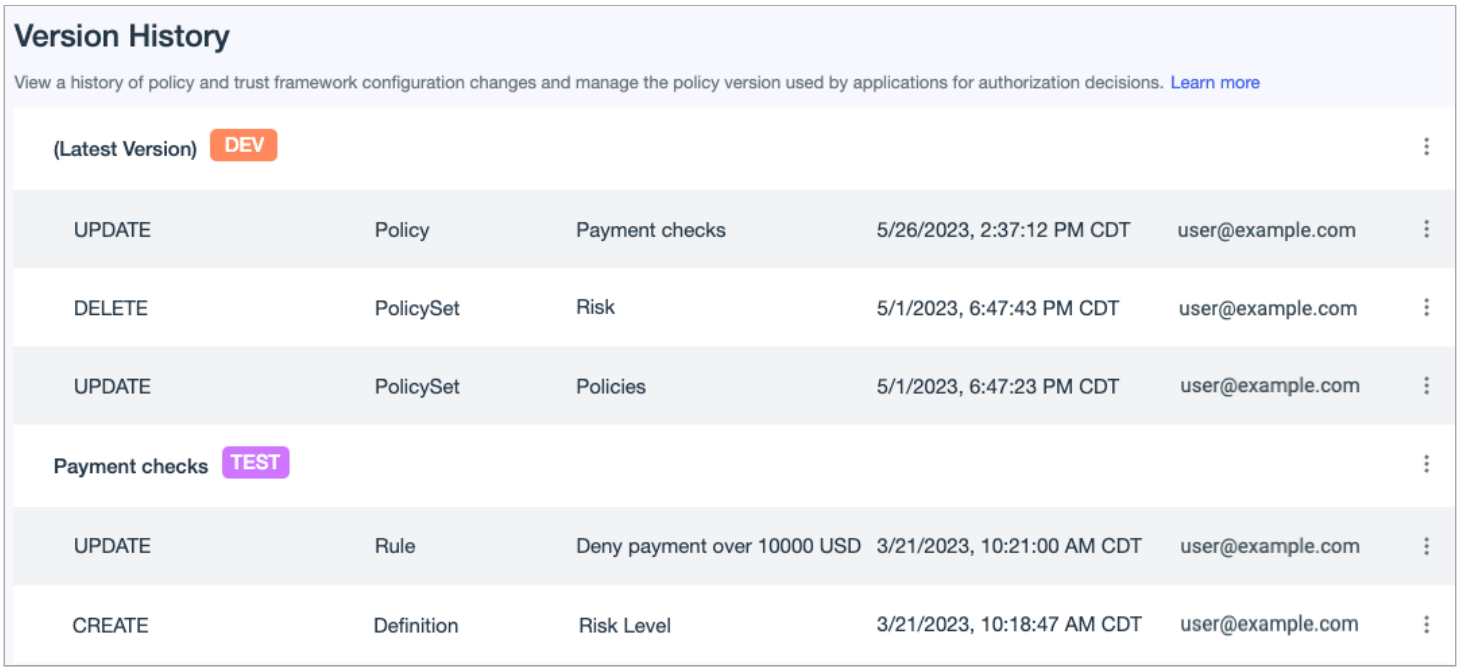
Copyright © 2025 Ping Identity Corporation

This tab also displays full and partial statement processing failures, including the code of the failed statement and a description of the failure.

Authorization version history

Version History provides a linear history of changes made to policies and **Trust Framework** definitions and enables you to publish versions to decision endpoints and Authorize gateways.

Versions are sorted to display the most recent changes first.



The following information is shown for each version:

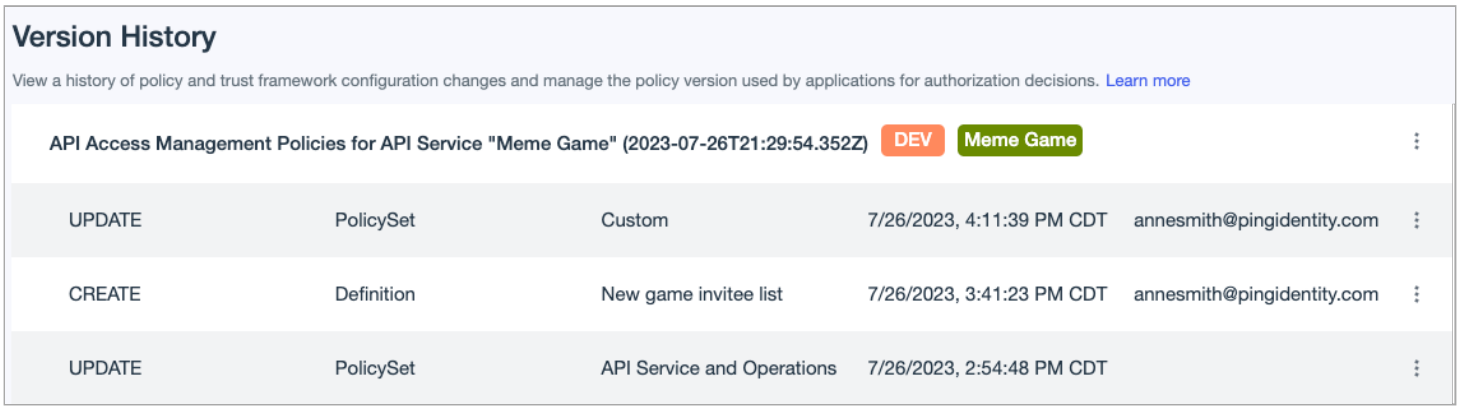
Column	Description
Action	The type of change made.
Object	The type of object that changed. This can be a policy, policy set, rule, statement, or definition. **Definition** includes changes to attributes, services, conditions, and processors.
Name	The name of the object that changed.
Timestamp	The date and time the change was made.
User	The email address of the user who made the change.

To help you track changes, you can name any version. When you reach policy development milestones, you can publish notable points in the version history to decision endpoints. When a named version is no longer published to any endpoints, you can remove the name from the version.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Each environment can have up to 100 named versions and 500 unnamed versions. The maximum data size for each version is 7 MB.

Changes to decision endpoints that have corresponding API services are listed under version names that begin with **API Access Management**.



> **Important**
>
> Do not rename these versions. Instead of publishing these versions, deploy the API service.

Naming an authorization version

Track notable updates to policies and **Trust Framework** definitions by giving them a version name. Learn more in Version history.

You can name a version whether you decide to publish the version or not. You can also change the name of a version. Version naming is optional.

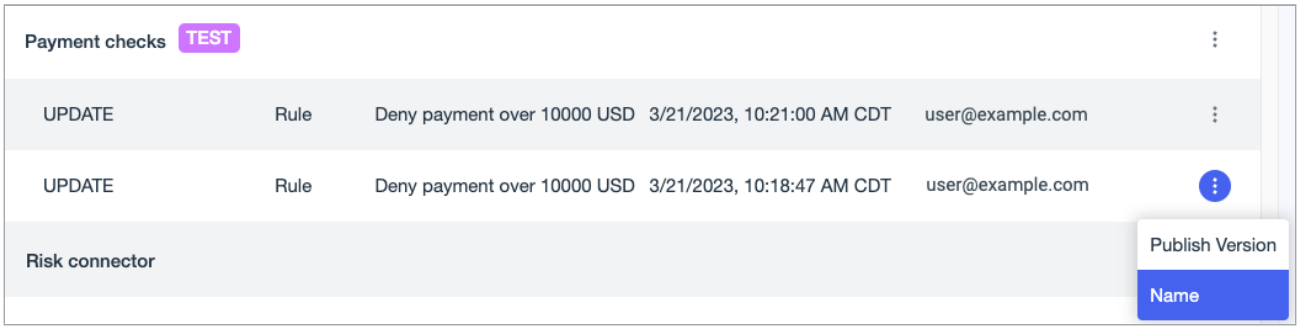
> **Important**
>
> Do not name or rename versions that begin with **API Access Management**. Instead, manage these versions by deploying the corresponding API service.

When a named version is no longer published to any endpoints, you can remove the name from the version. For example, you might remove the name from an older version after you deploy a new version that corrects errors in the older version.

Steps

1. To name a version:
    1. In the PingOne admin console, go to **Authorization** > **Version History**.
    2. Click the **More Options (⋮)** icon next to the version that you want to name and select **Name**.

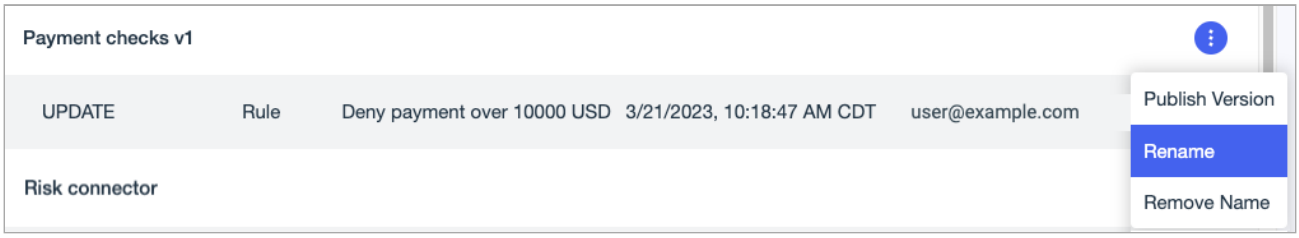
Copyright © 2025 Ping Identity Corporation



3. In the **Name Version** window, enter a version name, and then click **Name**.

2. To rename a version:

   1. Click the **More Options (⋮)** icon next to the version that you want to rename and select **Rename**.



   2. In the **Rename Version** window, change the version name, and then click **Rename**.

3. To remove a version name:

   1. Click the **More Options (⋮)** icon next to the version with the name that you want to remove and select **Remove Name**.

   2. In the **Remove Name** window, click **Remove Name**.

Publishing an authorization version

You can publish notable points in **Version History** to deploy policies and **Trust Framework** definitions to decision endpoints or to Authorize gateways.

Publishing a version is like saving a snapshot of your policies and **Trust Framework** definitions. The published version reflects the state of these objects at a specific point in time. Learn more in Version history.

By default, PingOne Authorize provides three decision endpoints for every environment: **Dev**, **Test**, and **Prod**. You can publish a version to multiple decision endpoints or Authorize gateways, but each decision endpoint can have only one version published to it at a time. The version is replaced each time you publish to an endpoint or an Authorize gateway. If an endpoint is set to use the latest version, updated versions are published to it automatically.

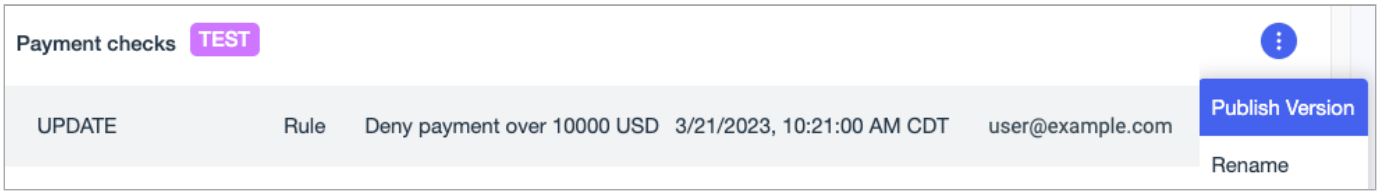
Use the following steps to publish versions to decision endpoints. To publish versions to Authorize gateways, go to Publishing policy versions to Authorize gateway instances.

> **Note**
>
> Ensure that your policies and **Trust Framework** definitions are thoroughly tested before you publish them to the **Prod** endpoint and use them in production.

Copyright © 2025 Ping Identity Corporation

Steps

1. In the PingOne admin console, go to **Authorization > Version History**.
2. Click the **More Options (⋮)** icon next to the version that you want to publish and select **Publish Version**.



> **Important**
>
> Do not publish versions with names that begin with **API Access Management**. Instead, deploy the API service to publish these changes.

3. In the **Publish to** list, select an endpoint.
4. For version **Name**, enter a name that makes the version easy to identify.

   If there's already a name, you can keep it or update it. The name is used as a tag in audit events.
5. Click **Publish**.

   Result:

   The version name and the endpoints that the version is published to are displayed in **Version History**.

Decision endpoints

Decision endpoints in PingOne Authorize provide development, testing, and production environments for the stages involved in policy deployment.

> **Tip**
>
> You can deploy policies to Authorize gateway instances in your organization's infrastructure instead of deploying to decision endpoints. Learn more in Authorize gateways and Publishing policy versions to Authorize gateway instances.

PingOne Authorize provides three default endpoints for deployment stages: **Dev**, **Test**, and **Prod**. You can add up to 30 endpoints in each environment and update or delete endpoints to suit your organization's needs.

> **Note**
>
> Endpoints that correspond to API services are required for API Access Management policy deployment. These endpoints are managed by the system and you can't delete them.

Copyright © 2025 Ping Identity Corporation

You can configure an endpoint to use the latest version of a policy or deploy a specific named version of a policy to the endpoint. When you use the latest version of a policy, any updates to the policy are published to the endpoint automatically. Because this compiles a publishing package each time a request is made to the endpoint and can cause a slower system response, **Use latest** is intended for policy development and debugging only. By default, the **Dev** stage endpoint is configured to use the latest version of a policy. You can change this setting or configure endpoints for other stages to use the latest version or specific versions of policies.

You can configure decision endpoints to keep track of the 20 most recent decisions made during the last 24 hours. It's helpful to enable this setting during policy development as a debugging tool so you can visualize and examine recent decisions. This can cause a slower system response, so the setting is disabled by default.

Event subscriptions, or webhooks, enable you to use third-party tools to monitor audit events for decision endpoints.

The PingOne API provides operations to create, read, update, and delete decision endpoint resources. It also provides an evaluation action to execute a decision request against a resource. Learn more about using the API in PingOne Authorize Policy Decision Service.

Adding a decision endpoint

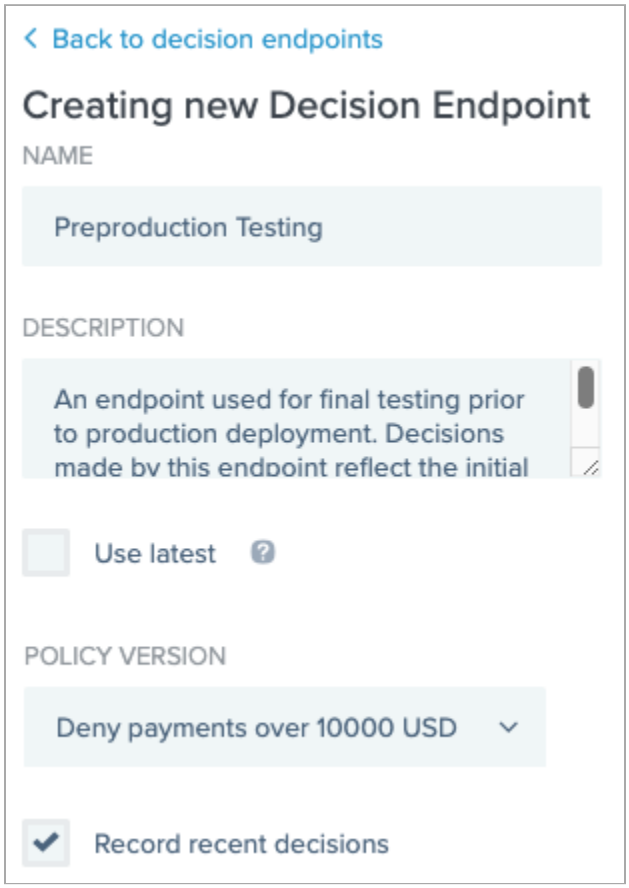
Add PingOne Authorize endpoints for stages that align with your organization's policy deployment process.

Steps

1. In the PingOne admin console, go to **Authorization > Decision Endpoints**.
2. Click **+ Add Endpoint**.
3. Enter an endpoint **Name** and a **Description** that reflects the endpoint's role in the deployment process.

   The maximum name length is 256 characters.

Copyright © 2025 Ping Identity Corporation



4. If you want to deploy a particular version of a policy to the endpoint, clear the **Use latest** checkbox and select the version in the **Policy Version** list.

   If you don't deploy a particular version, the endpoint uses the latest policy version. **Use latest** republishes the latest version each time a request is made to the endpoint and can cause a slower system response.

   > **Note**
   >
   > You should only enable **Use latest** during policy development and debugging.

5. Select the **Record recent decisions** checkbox to keep track of the last 20 recent decisions made for the endpoint during the last 24 hours.

   This allows you to visualize and examine recent decisions.

   > **Important**
   >
   > This can cause a slower system response. You should only enable this setting during policy development and debugging.

6. Click **Save**.

   Result:

   The new endpoint is added to the **Decision Endpoints** page. New endpoints are listed in alphabetical order after the three default endpoints.

Copyright © 2025 Ping Identity Corporation

Editing a decision endpoint

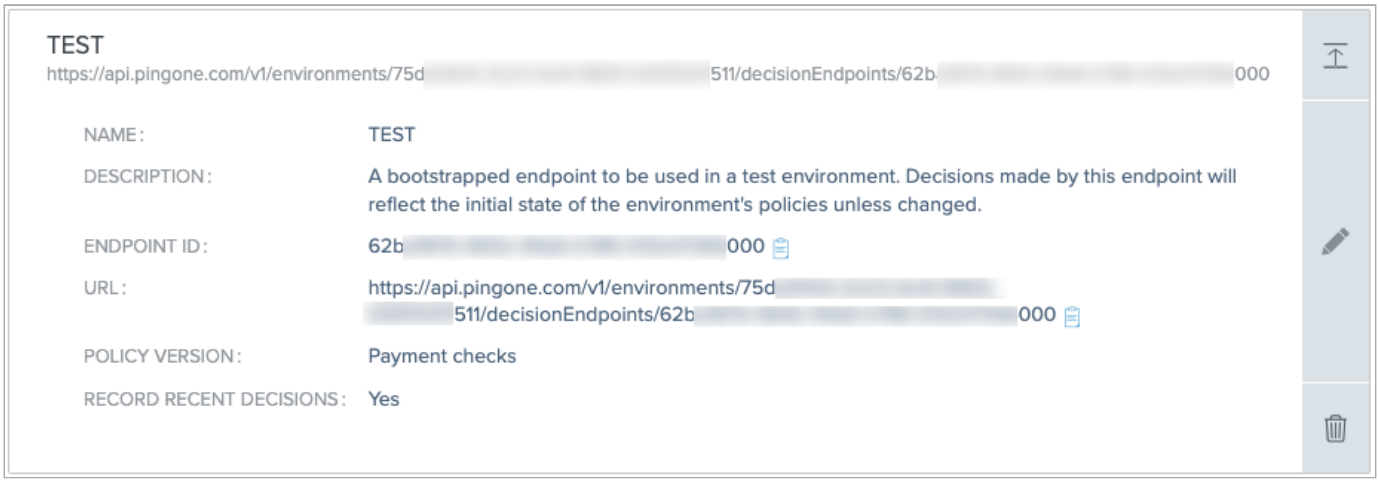
Edit PingOne Authorize endpoints to reflect changes in your organization's policy deployment process.

About this task

> **Tip**
>
> During policy development and debugging, you might want to select the **Record recent decisions** option so you can visualize and examine recent decisions.

Steps

1. In the PingOne admin console, go to **Authorization > Decision Endpoints**.
2. Expand the endpoint you want to edit and click the **Pencil** icon.



3. Add or edit the **Name**, **Description**, or other options.

   The maximum name length is 256 characters. Learn more about these options in Adding a decision endpoint.

   If you clear the **Record recent decisions** checkbox, recent decision requests are no longer tracked for the endpoint and decisions to visualize are removed from Recent decisions.

   > **Note**
   >
   > If the endpoint corresponds to an API service, it is managed by the system and **Record recent decisions** is the only option you can edit.

4. Click **Save**.

Deleting a decision endpoint

Delete PingOne Authorize endpoints for deployment stages that are no longer needed.

About this task

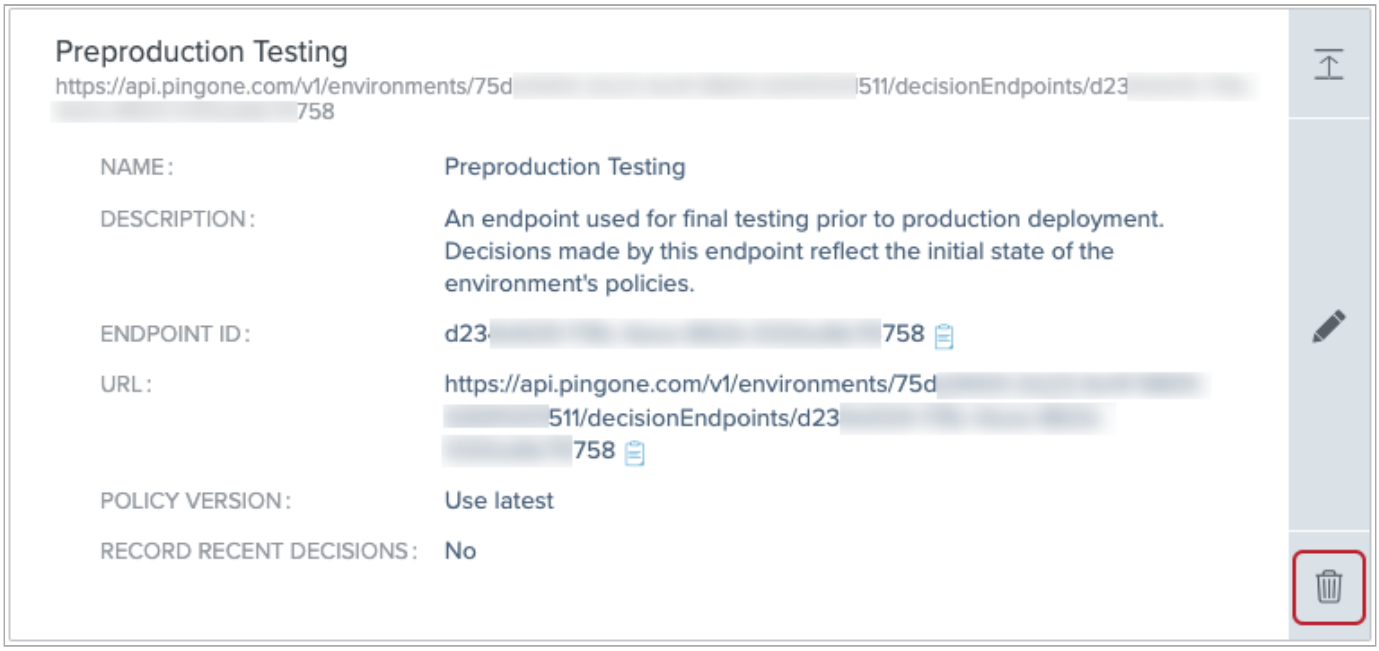
When you delete a decision endpoint, recent decisions for the endpoint are also deleted.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> You cannot delete a decision endpoint that corresponds to an API service. These endpoints are managed by the system and required for API Access Management policy deployment.

Steps

1. Go to **Authorization > Decision Endpoints**.
2. Expand the endpoint you want to delete and click the **Delete** icon.



3. In the **Delete Endpoint** window, click the check box to confirm that you want to delete the endpoint, then click **Delete**.

PingOne Authorize event monitoring

Event subscriptions, or webhooks, allow you to use third-party tools to monitor audit events for PingOne Authorize.

In PingOne, you can manage your event subscriptions in **Integrations > Webhooks**.

When you create a webhook, you can filter by the following event types to subscribe to the **Authorize Events** and **Decision Endpoint Events** you want to monitor. Learn more about creating and managing webhooks in Webhooks.

The same events are available in audit reports. Learn more about filtering events in audit reports in Audit.

Event type	Description
API Service Created	Triggered when an API service is created.
API Service Updated	Triggered when an API service is updated.
API Service Deployed	Triggered when an API service is deployed.

Copyright © 2025 Ping Identity Corporation

Event type	Description
API Service Deleted	Triggered when an API service is deleted.

Event type	Description
Authorize Attribute Created	Triggered when an attribute is created.
Authorize Attribute Updated	Triggered when an attribute is updated.
Authorize Attribute Deleted	Triggered when an attribute is deleted.

Event type	Description
Authorize Service Created	Triggered when a service is created.
Authorize Service Updated	Triggered when a service is updated.
Authorize Service Deleted	Triggered when a service is deleted.

Event type	Description
Authorize Condition Created	Triggered when a condition is created.
Authorize Condition Updated	Triggered when a condition is updated.
Authorize Condition Deleted	Triggered when a condition is deleted.

Event type	Description
Authorize Processor Created	Triggered when a processor is created.
Authorize Processor Updated	Triggered when a processor is updated.
Authorize Processor Deleted	Triggered when a processor is deleted.

Event type	Description
Authorize Policy Created	Triggered when a policy is created.
Authorize Policy Updated	Triggered when a policy is updated.
Authorize Policy Deleted	Triggered when a policy is deleted.

Copyright © 2025 Ping Identity Corporation

Event type	Description
Authorize Shared Advice Created	Triggered when shared advice is created.
Authorize Shared Advice Updated	Triggered when shared advice is updated.
Authorize Shared Advice Deleted	Triggered when shared advice is deleted.

Event type	Description
Authorize Shared Rule Created	Triggered when a shared rule is created.
Authorize Shared Rule Updated	Triggered when a shared rule is updated.
Authorize Shared Rule Deleted	Triggered when a shared rule is deleted.

Event type	Description
Authorize Tag Updated	Triggered when a tag is updated. The tag is the name given to a published version in Authorization version history.
Authorize Tag Deleted	Triggered when a tag is deleted.

Event type	Description
Decision Endpoint Created	Triggered when decision endpoints are created.
Decision Endpoint Updated	Triggered when decision endpoints are updated.
Decision Endpoint Deleted	Triggered when decision endpoints are deleted.
Decision Request Evaluated	Triggered when decision requests are evaluated. Provides: • The name and ID of the decision endpoint • The policy version deployed to the endpoint • The decision produced by the policy evaluation • The time elapsed to evaluate the decision request • The attributes marked for logging • The services invoked in the evaluation Decision Request Evaluated audit events are retained in PingOne audit logs for 90 days. **Tip** This filter produces a large volume of events. You might want to create a separate webhook for it.

Copyright © 2025 Ping Identity Corporation

Event type	Description
HTTP Request Policy Evaluated	Triggered when an HTTP request is evaluated. Provides: • The name and ID of the HTTP client • The name and ID of the API service • The decision produced by the policy evaluation • The method, headers, and request target included in the HTTP request • The name and ID of the API gateway (includes the name and version of the integration kit, if available) **Tip** This filter produces a large volume of events. You might want to create a separate webhook for it.
HTTP Response Policy Evaluated	Triggered when an HTTP response is evaluated. Provides: • The name and ID of the HTTP client • The name and ID of the API service • The decision produced by the policy evaluation • The status code and headers returned in the HTTP response • The name and ID of the API gateway (includes the name and version of the integration kit, if available) **Tip** This filter produces a large volume of events. You might want to create a separate webhook for it.

Learn more about the format of keys used in **Decision Request Evaluated** events in Event Types in the Policy Decision Authorization section of the PingOne Platform API Reference.

Recent decisions

Examine recent decisions in PingOne Authorize as part of the policy development and debugging process.

You can examine recent decisions for policies deployed to decision endpoints or to Authorize gateway instances. Learn more about recent decisions executed by gateway instances in Visualizing decisions made by Authorize gateway instances.

When the **Record recent decisions** option is enabled for a decision endpoint, PingOne Authorize keeps track of the last 20 decisions made by the decision service for that endpoint in the last 24 hours. This allows you to examine the decision flow and details about the attributes and services used in the decision.

> **Note**
> Recent decisions are a policy debugging tool, and are not intended for monitoring of authorization decisions in real time.

Copyright © 2025 Ping Identity Corporation

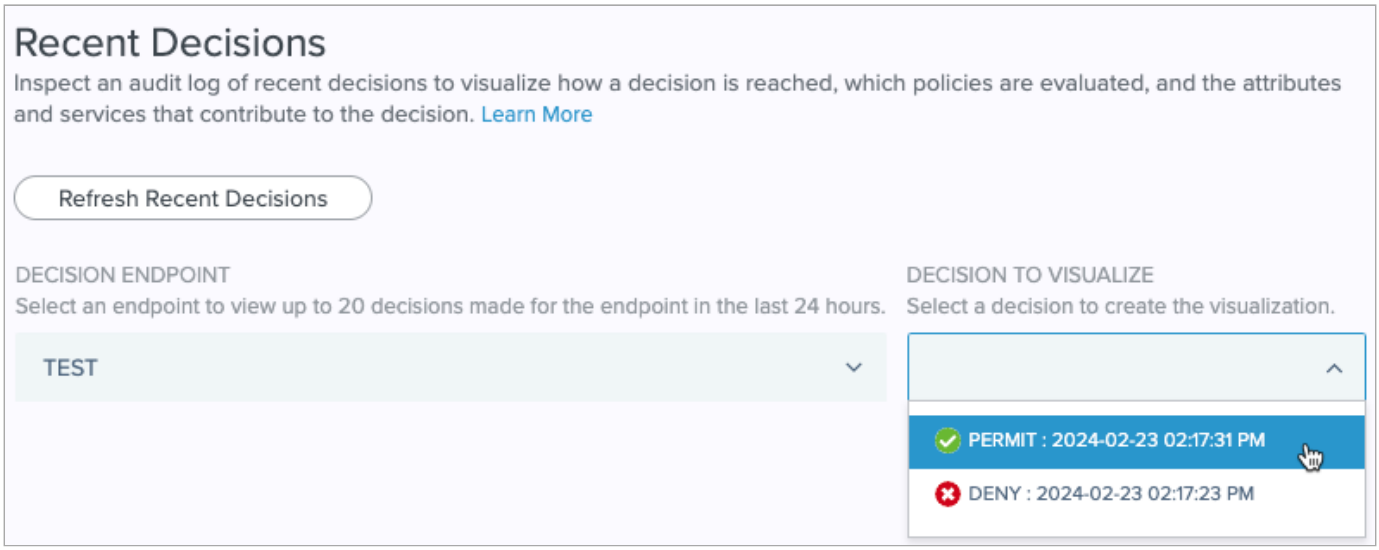
Examining recent decisions

When you develop and test policies in PingOne Authorize, examine the decision flow and other details about recent decisions to make sure the decision service is evaluating policies according to your expectations.

Steps

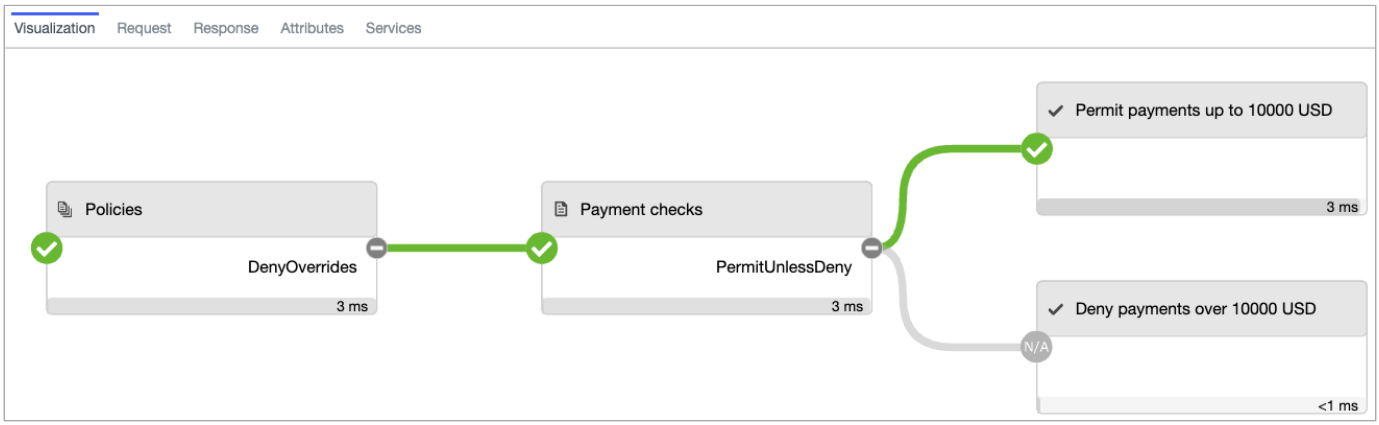
1. In the PingOne admin console, go to **Authorization > Recent Decisions**.
2. In the **Decision Endpoint** list, select the endpoint for which you want to examine recent decisions.
3. In the **Decision to Visualize** list, select a decision.

   The most recent decision is listed first.



> **Note**
>
> Click **Refresh Recent Decisions** at any time to update the list with the 20 most recent decisions made for the endpoint in the last 24 hours.

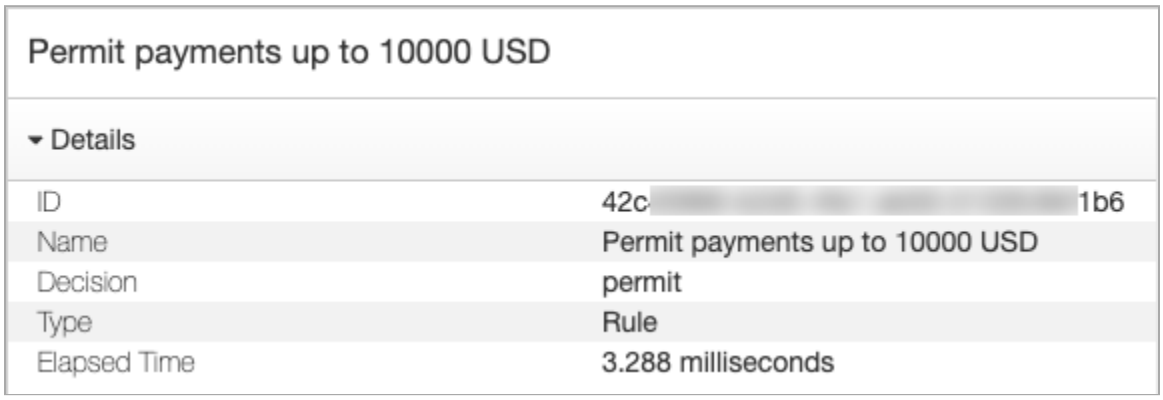
4. On the **Visualization** tab, examine the decision flow to make sure decisions are evaluated according to your expectations.



5. Click a box in the flow to show more details.

Copyright © 2025 Ping Identity Corporation

This example represents the rule that permits payments up to 10,000 USD. The decision evaluated to `Permit` and it took 3.288 milliseconds.



Permit payments up to 10000 USD

▾ Details

ID	42c[illegible]1b6
Name	Permit payments up to 10000 USD
Decision	permit
Type	Rule
Elapsed Time	3.288 milliseconds

6. Click the other tabs for additional details:
   - **Request** tab: Shows the JSON request sent to the decision service, allowing you to confirm that the expected information was sent.
   - **Response** tab: Shows the complete, high-verbosity response for the decision, including expanded errors and other helpful information.
   - **Attributes** tab: Shows details about the attributes used in the decision.
   - **Services** tab: Shows details about the services used in the decision.

API services

An API service is the fundamental unit of access control used in PingOne Authorize to represent the API that you want to protect.

Access control policies

To control access to your APIs, you can use built-in access control rules and custom policies. Built-in access control rules grant access based on:

- Authorized scopes
- User membership in groups
- User permissions
- Authentication policy
- Time since last authentication

Learn more about these rules in Defining operations for protected actions.

For more complex access control scenarios, you can define custom policies in the **API Access Management** policy tree. Learn more in Adding custom policies for API services and operations.

Copyright © 2025 Ping Identity Corporation

Token and user management

An API service groups related API operations into a protected domain, such as https://example-api-domain.com, that clients access with a single access token. When you define an API service, you can use PingOne to issue access tokens and manage users for the API service, or you can use external providers, such as PingFederate and PingDirectory.

PingOne token provider

If you use PingOne to issue tokens and manage users for the API service, PingOne Authorize works with PingOne resources and applications to manage access control for your API. You can configure access control rules that are tightly integrated with PingOne. You can also define custom policies that handle more complex authorization scenarios.

Each API service is associated with a PingOne resource. This resource is a representation of your API for OAuth authorization purposes. Resources have scopes that are used in access token configuration. Scopes determine which resources a client can access. PingOne Authorize uses scopes to:

- Ensure that the access token presented by a client was issued for your API. In this basic access control check, PingOne Authorize verifies that the audience claim in the access token for the client request matches the audience value configured for the API service's associated resource.

  > **Note**
  >
  > After you define an API service, make sure that you add a PingOne application that's allowed to access your protected API service. To allow access, grant the application the same scope that you configured for the API service.

- Determine the extent of access allowed to a client. For example, your API might require a `user:read` scope for reading user data and a `user:write` scope for modifying user data. You can configure a built-in access control rule to perform authorized scope checks.

When authorizing an HTTP request, if the request's access token includes a subject, PingOne Authorize automatically populates the built-in `PingOne.User` attribute with the requesting user's data.

External token providers

If you use external providers to issue tokens and manage users for the API service, you can define custom policies, but you can't use built-in access control rules. You must configure your API gateway to validate access tokens and pass verified claims to PingOne in the inbound request.

> **Important**
>
> When using an external token provider, PingOne Authorize relies on the API gateway for token validation and does not verify any matching claims.

With external providers, PingOne Authorize doesn't automatically provide identity information about the requesting user in built-in user attributes. Instead, if the request's access token includes a subject, you can use the `PingOne.API Access Management.Identity.Access Token.Subject` attribute to resolve user identity information from an external directory. Learn more in API Access Management attributes.

Copyright © 2025 Ping Identity Corporation

Policy deployment

Each API service has a system-owned decision endpoint that provides an environment for managing and deploying authorization policies relevant to the API service. The decision endpoint is created when you deploy the API service for the first time, and it has the same name as the API service. Learn more in Deploying an API service.

Defining your API in PingOne Authorize

Define a managed API service to represent your API so that PingOne Authorize can help your API gateway enforce access control.

Before you begin

Configure an API gateway integration kit to connect your API gateway to PingOne.

About this task

An API service allows PingOne Authorize to recognize requests for your API and instruct your API gateway to block access from unauthorized clients and allow access only from authorized clients.

An API service definition specifies:

- Pointers to the API and to specific parts of the API that you want to protect
- Whether directory services and access token validation for the API service are managed by PingOne or managed externally
- The PingOne resource associated with the API service (this is specified only when PingOne manages token validation)
- Whether custom access control policies for complex authorization scenarios are enabled for the API service

Learn more in API services.

> **Note**
> You can define up to 25 API services in each environment.

You must deploy the API service after you make configuration changes, such as updating settings, or adding or updating operations or custom policies.

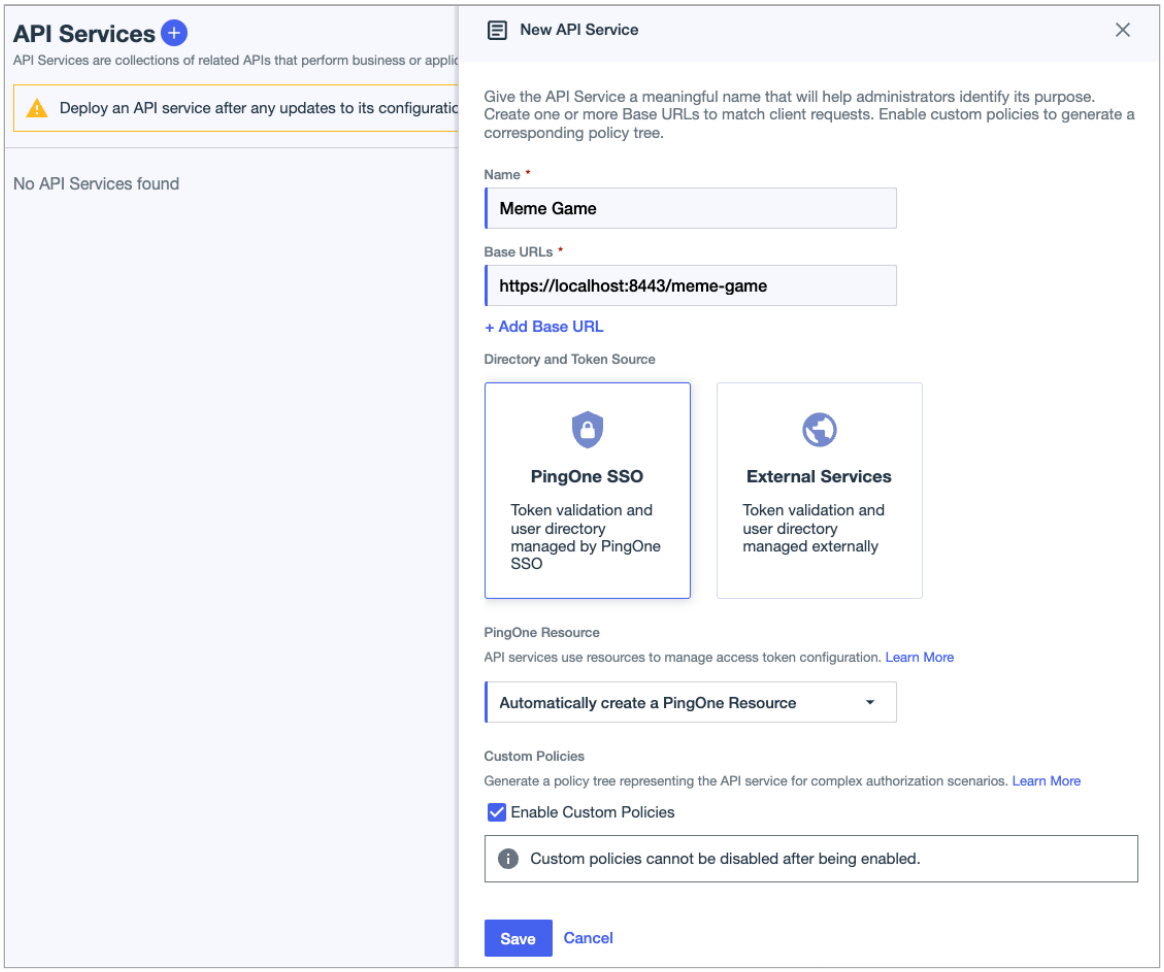
Steps

1. Go to **Authorization > API Services**.
2. Click the **+** icon next to **API Services** to add an API service.
3. For the **Name**, enter a name that identifies the API service.

   The name must be unique across all API services and resources.
4. Enter one or more **Base URLs** for the API represented by the API service.

   > **Tip**
   > You can enter multiple URLs to support aliases for the same service, such as a vanity URL in addition to the domain URL. To add another URL, click **+ Add Base URL**. URLs must be valid.

Copyright © 2025 Ping Identity Corporation



5. Select a user directory and token source.

   Choose from:

   - **PingOne SSO** (default): PingOne manages user directory services and access token validation for the API service.

     > **Important**
     >
     > If you're using the Amazon Web Services integration kit to enforce access control, the API service definition must use PingOne SSO as the directory and token source.

   - **External Services**: The API gateway manages access token validation services through external providers, such as PingFederate. This requires you to configure your API gateway to pass validated token claims to PingOne in decision requests.

     > **Important**
     >
     > After you save the API service, you can't change whether the directory and token source are managed by PingOne or by external providers.

6. Do one of the following.

Choose from:

- If you selected **External Services**, click **Save**. PingOne Authorize is now configured to recognize the API.
- If you selected **PingOne SSO**, complete the remaining steps.

7. Select a **PingOne Resource** from the list, or select the option to **Automatically create a PingOne Resource**.

   This resource is managed by the API service, and there are restrictions against deleting the resource while it's associated with an API service. Resources created automatically will have the same name as the API service.

8. To enable custom policies for the API service and its operations, select the **Enable Custom Policies** checkbox.

   Result:

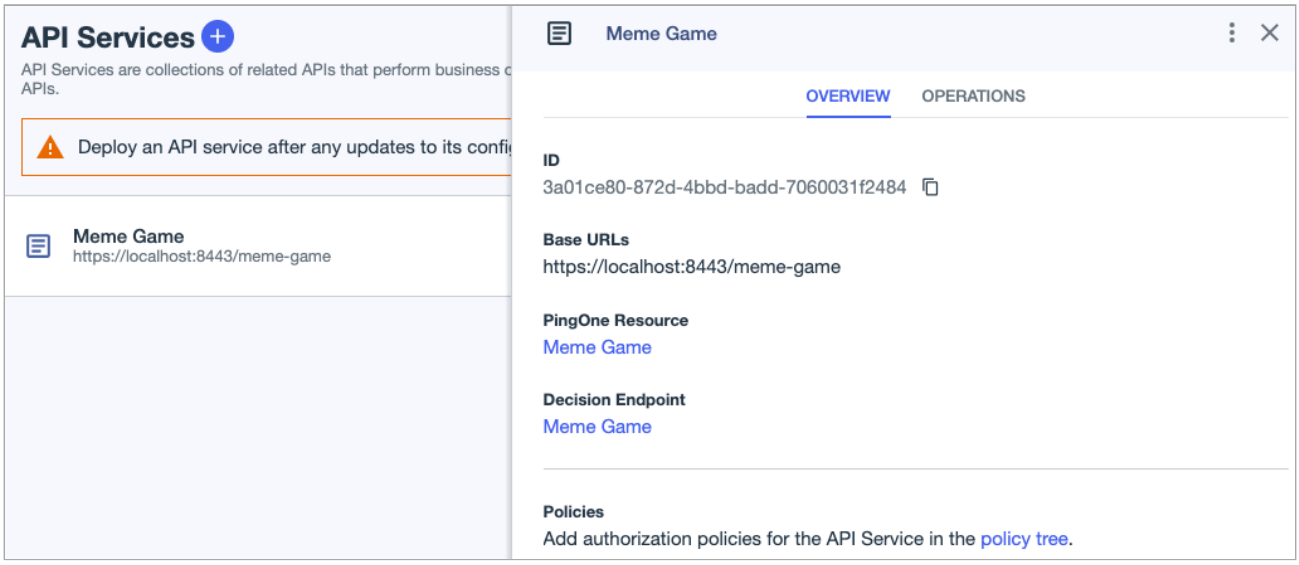
   This generates a policy tree for the API service, enabling you to add your own custom authorization policies for the APIs managed by this API service.

   > **Note**
   > After you save the API service, you can't change this setting. Custom policies are enabled by default if the API service uses **External Services** for token validation.

9. Click **Save**.
10. Click **Deploy**.
11. Add a scope to the **Meme Game** resource:

    The scope defines which resources an API client can access. An application requests a scope for the resource associated with an API service in order to set the audience for the access token.

    1. On the **Overview** tab, under **PingOne Resource**, click **Meme Game**.



    2. In **Applications > Resources**, click the **Scopes** tab, and then click **+ Add Scope**.
    3. In the **Scope Name** field, enter a name for the scope.

Copyright © 2025 Ping Identity Corporation

> **Tip**
> For consistency, use a lowercase version of the API service name and replace spaces with hyphens.

4. (Optional) Enter a description for the scope.
5. Click **Save**

12. Go to **Authorization > API Services**, select **Meme Game**, and then click **Deploy**.

    Result:

    PingOne Authorize is now configured to recognize the API.

Next steps

- If PingOne is managing user directory and access token validation services for the protected API service, add a PingOne application that is allowed to access the protected API service. To allow access, grant the application the same scope that you configured for the API service. Learn more in Editing scopes for an application.
- To configure built-in access control rules, define operations for protected API actions.
- For more complex access control scenarios, add custom policies for the API service.

Defining operations for protected actions

Operations in PingOne Authorize enable you to use built-in access control rules or custom policies to control access to API actions.

An API service operation is a method and path combination that matches a client request to the API. Add operations for API requests that you want to protect.

> **Note**
> You can define up to 25 operations for each API service in an environment.

When PingOne is managing user directory services and access token validation for an API service, you can define built-in access control rules and custom policies for an operation. When these services are managed externally, you can define custom policies for an operation, but you can't configure built-in access control rules.

Built-in access control rules

Built-in access control rules grant access to protected operations based on the following factors:

User membership in groups

Before you grant access based on group membership, you must add users and create groups in PingOne.

Authorized OAuth scopes

Scopes determine the resources that a client can access. For example, a banking application might use scopes to control the kinds of data shared with third-party applications.

Copyright © 2025 Ping Identity Corporation

Authorized permissions

Before you grant access based on permissions, you must define permissions for the application resources that you want to protect.

Authentication policy

This rule defines the authentication policy that the decision service requires when evaluating whether to allow access to the operation. The authentication policy provides context about the authentication method or assurance level required to get an access token for the protected resource.

You can use this rule to implement step-up authentication for the protected resource. Learn more in Step-up authentication.

Time since last authentication

This rule defines the maximum acceptable amount of time since the last authentication event used to get an access token for the protected resource. You can use this rule to implement step-up authentication for the protected resource.

> **Note**
>
> When you use the **authentication policy** and **time since last authentication** basic rules with the Amazon Web Services (AWS) integration kit, AWS doesn't return the full step-up challenge response. When these rules produce deny decisions, AWS returns a simple deny response with an HTTP status code.

PingOne Authorize automatically generates policies for built-in access control rules and deploys them when you deploy the associated API service.

> **Tip**
>
> You can get hands-on experience with defining access control rules for an API operation in Tutorial 2: Controlling access to specific API operations.

Custom policies

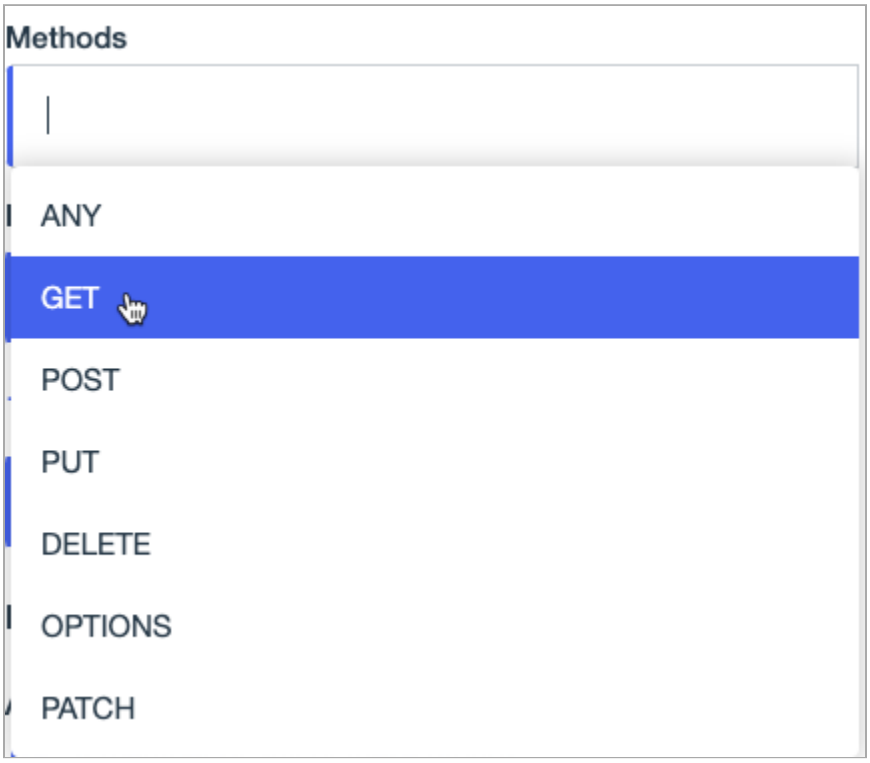
Custom policies handle more complex authorization scenarios, such as evaluating context by pulling in risk scores to determine access. You can enable custom policies when you define an API service or by editing the API service later.

The following steps provide information about configuring built-in access control rules for an operation. Learn more about custom policies in Adding custom policies for API services and operations.

Steps

1. Go to **Authorization > API Services**.
2. Select your API service, and then click the **Operations** tab.
3. To create a new operation, click **Define Operation**.
4. Click **Methods**, and then select one or more methods for the operation. Press Tab or click outside the list to close it.

Copyright © 2025 Ping Identity Corporation



5. Enter one or more API **Paths** for the operation.

   Paths must start with a slash (/) and match requests for resources and subresources exactly unless you use wildcards or parameters.

   - A single wildcard (*) represents one path segment.
   - A double wildcard (**) represents one or more segments at the end of the path.
   - Surround parameters with curly braces ({}). You can add attributes that represent path parameters to make them easy to use in custom policies. Learn more in API Access Management attributes.

   For examples of path definitions and matching requests for account resources and subresources, such as transactions, expand the following section. Only a few of the possible matches are shown for paths with wildcards. Learn more in Path Parameter Pattern Syntax.

Path	Examples of matching requests
`/accounts/{accountId}/transactions/*`	`/accounts/123/transactions` `/accounts/123/transactions/` `/accounts/123/transactions/456` `/accounts/123/transactions/details`
`/accounts/*/transactions/*`	`/accounts/123/transactions` `/accounts/123/transactions/` `/accounts/123/transactions/456` `/accounts/123/transactions/details`

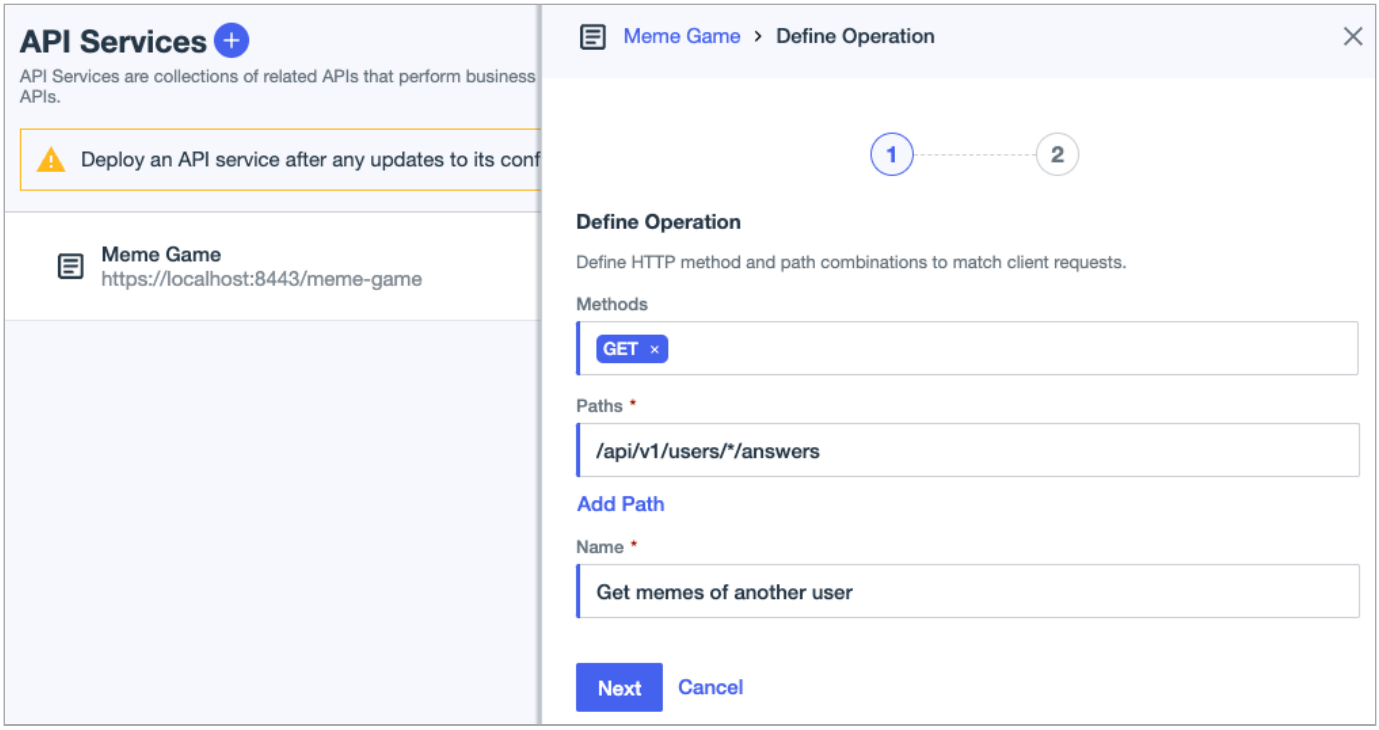
Copyright © 2025 Ping Identity Corporation

Path	Examples of matching requests
`/accounts/{accountId}/**`	`/accounts/123/transactions` `/accounts/123/transactions/` `/accounts/123/transactions/456` `/accounts/123/transactions/details` `/accounts/123/transactions/details/statement` `/accounts/123/settings`
`/accounts/{accountId}/transactions/`	`/accounts/123/transactions/` **Note** Matching requests must end with a slash (/).
`/accounts/{accountId}/transactions`	`/accounts/123/transactions` **Note** Matching requests must not end with a slash (/).

To add another path, click **+ Add Path**.

6. For **Name**, enter a name that describes the operation.

> **Note**
> You can change the default name, which consists of the method and path separated by **request for**.



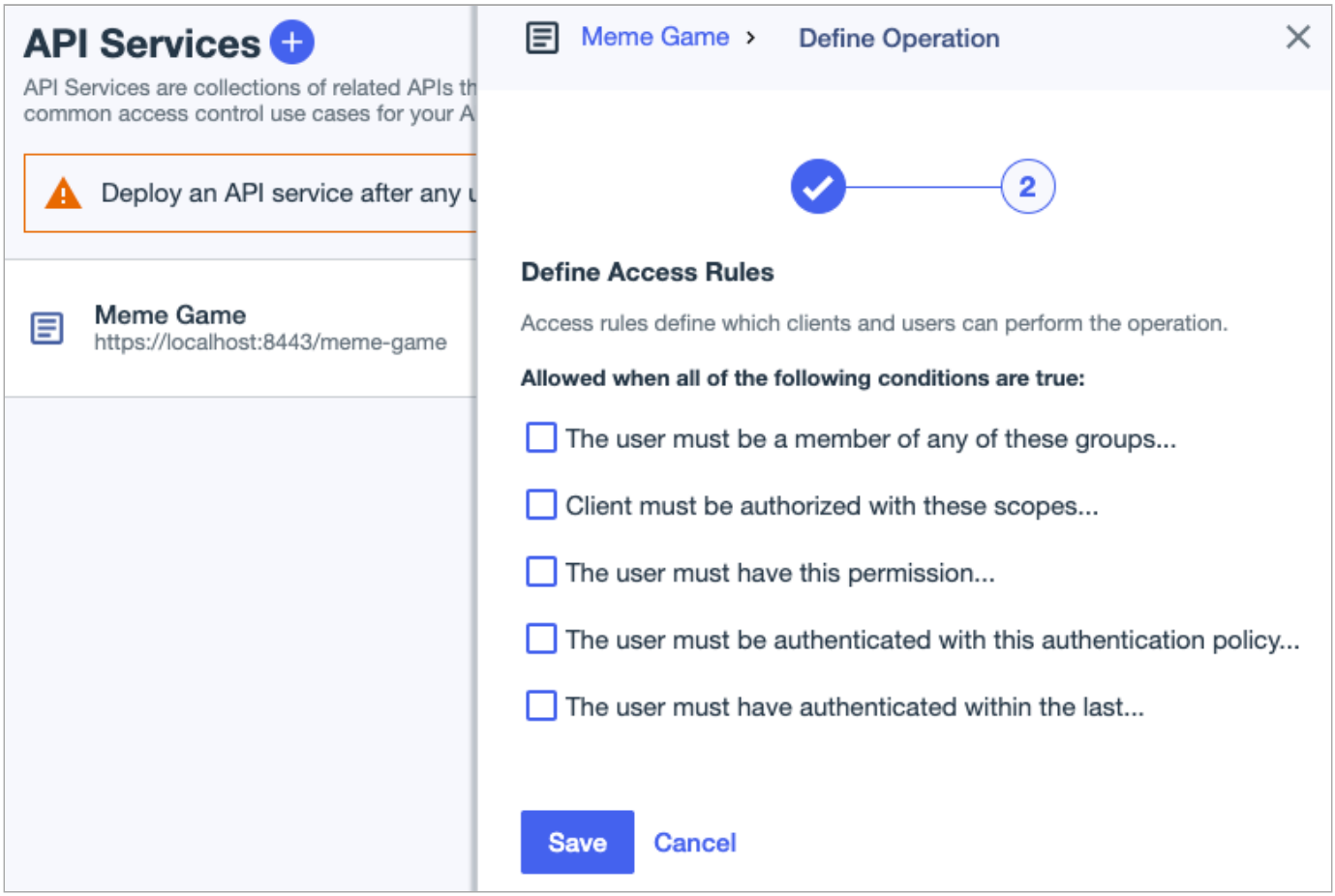
7. If user directory services and access token validation are managed externally for the API service, click **Save**, then click **Deploy**.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Built-in access control rules are not available in this situation. Instead, use your external providers, such as PingFederate and PingDirectory, to configure authorized scopes and user groups.

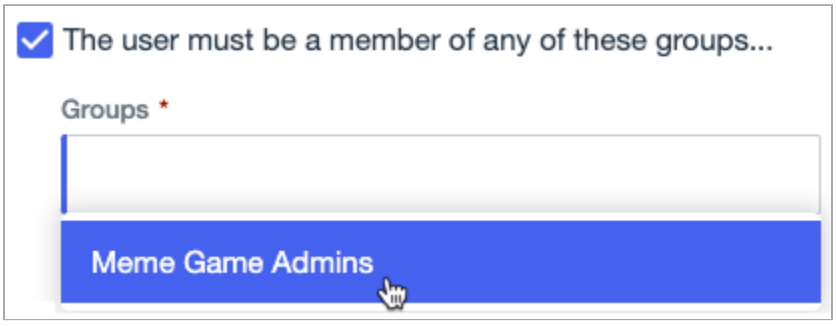
8. To define access control rules, click **Next**.

9. (Optional) Define a rule based on group membership:



1. Select the **The user must be a member of any of these groups** checkbox.

2. Click the **Groups** list, and then select one or more groups. Press Tab or click outside the list to close it.

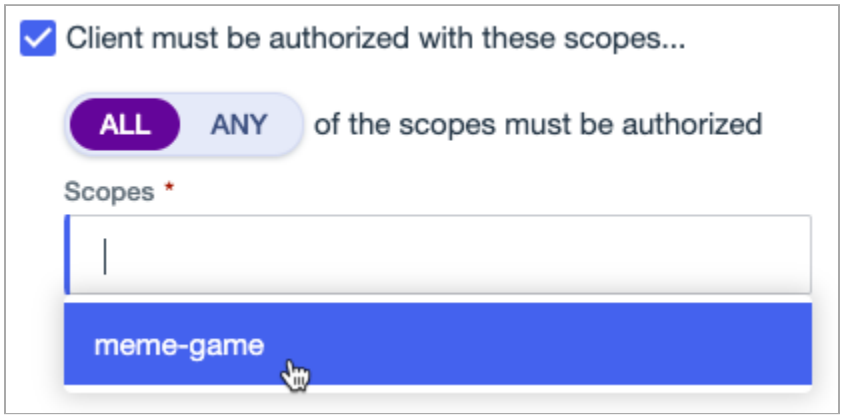


Copyright © 2025 Ping Identity Corporation

10. (Optional) Define a rule based on authorized scopes:

    1. Select the **Client must be authorized with these scopes** checkbox.

    2. Click the **Scopes** list, and then select one or more scopes. Press Tab or click outside the list to close it.



    3. (Optional) To add a new scope, in the **Scopes** list, enter the name of the scope, and then press Enter.

    4. Click the toggle to change whether all or any of the scopes must be authorized:

        - **All** (default): Allows access if a client is authorized for all of the scopes. This is equivalent to adding a Boolean AND operator between scopes.

        - **Any**: Allows access if a client is authorized for any of the scopes. This is equivalent to adding a Boolean OR operator between scopes.

        > **Note**
        >
        > **All** and **Any** have the same effect when there's only one scope.

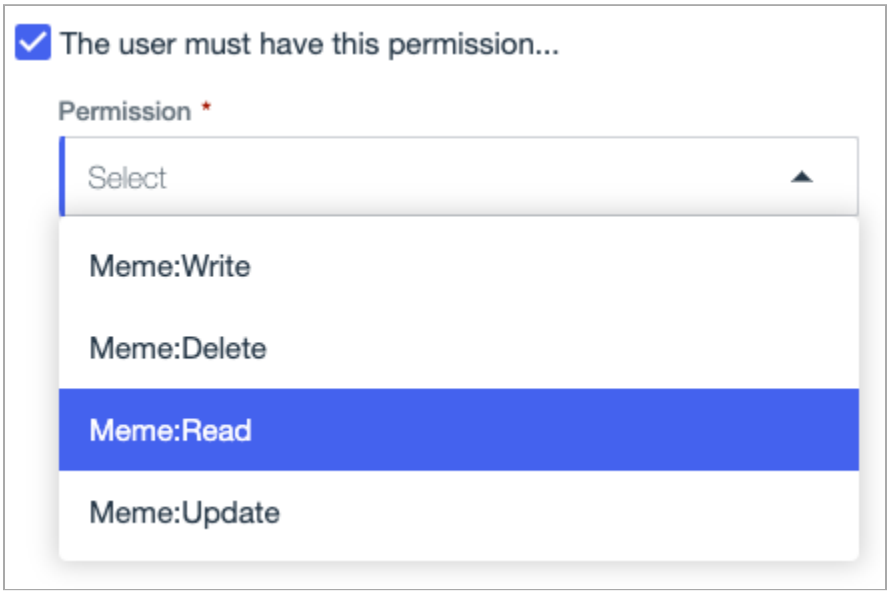
11. (Optional) Define a rule based on permissions:

    1. Select the **The user must have this permission** checkbox.

    2. Click the **Permission** list, and then select a permission.

    The list includes all of the permissions that are available for the PingOne resource associated with the API service.

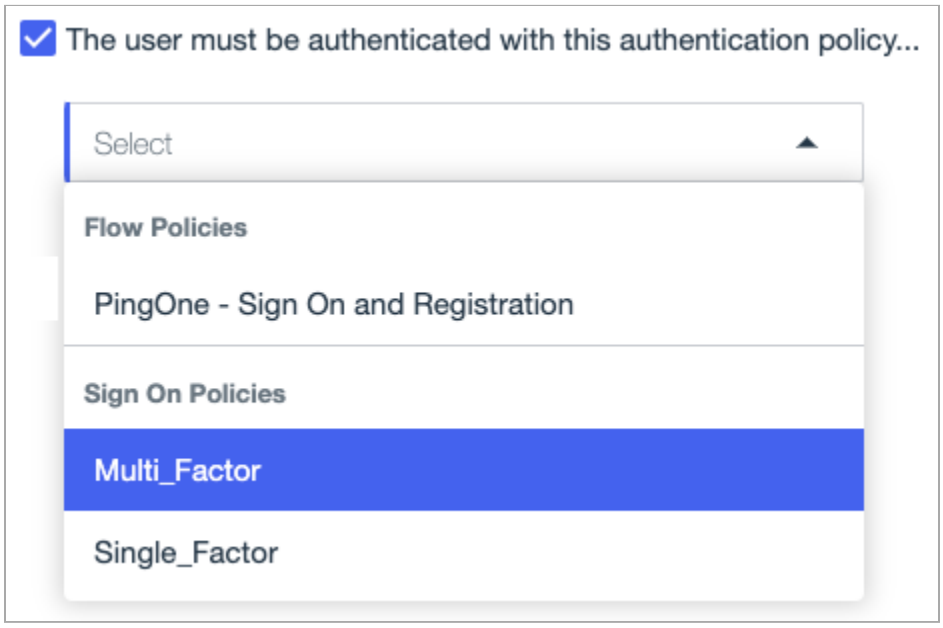
Copyright © 2025 Ping Identity Corporation



12. (Optional) Define a rule based on the authentication policy:

    1. Select the **The user must be authenticated with this authentication policy** checkbox.
    2. In the policy list, select a flow or sign-on policy.

       The list includes all of the authentication flows and sign-on policies that are available in the environment.



> **Note**
>
> If an authentication flow or sign-on policy is renamed or deleted, you must update this rule accordingly and redeploy the API service.

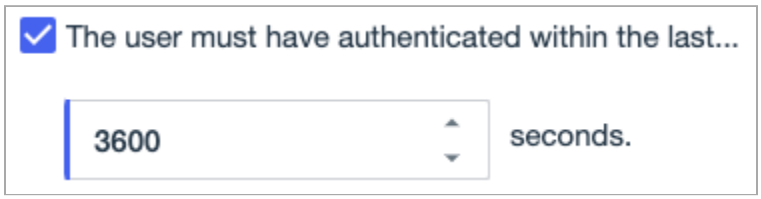
13. (Optional) Define a rule based on time since last authentication:

    1. Select the **The user must be authenticated within the last** checkbox.

Copyright © 2025 Ping Identity Corporation

2. Enter the maximum amount of time to allow since the last authentication event, in seconds.

   The number of seconds must be greater than 0.



14. Click **Save**.

15. Click **Deploy**.

Next steps

If you configured a scope-based rule for the operation, make sure that you grant the same scopes to your PingOne application to ensure that clients are allowed to access the API operation. To do this, edit the list of allowed scopes on the application's **Resources** tab. Learn more in Editing scopes for an application.

If you configured a permission-based rule for the operation, make sure that you assign permissions to roles, and assign roles to users.

Adding custom policies for API services and operations

With an API gateway integration, you can define custom policies that target inbound requests and outbound responses for API services and operations.

Before you begin

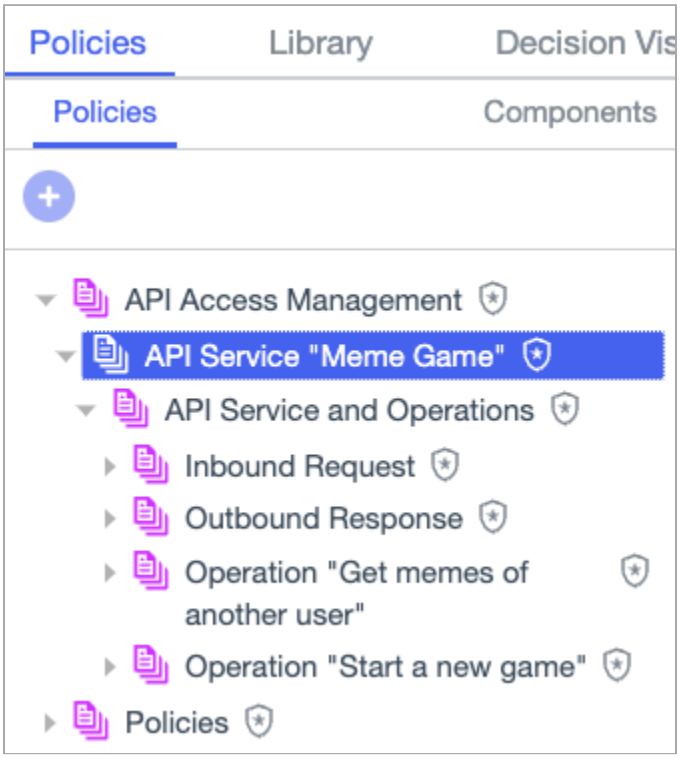
If custom policies are not enabled for your API service, enable them by clicking **Enable Custom Policies** on the API service's **Overview** tab.

About this task

Custom policies control access to APIs in complex authorization scenarios. When you enable custom policies for an API service, PingOne Authorize generates a policy tree for the API service. The tree structure is system-owned and reflects the API service and its operations. You can't modify the policy sets and policies in the tree, but you can add your own custom policies to **Custom** policy sets in the tree.

The tree structure is organized as follows.

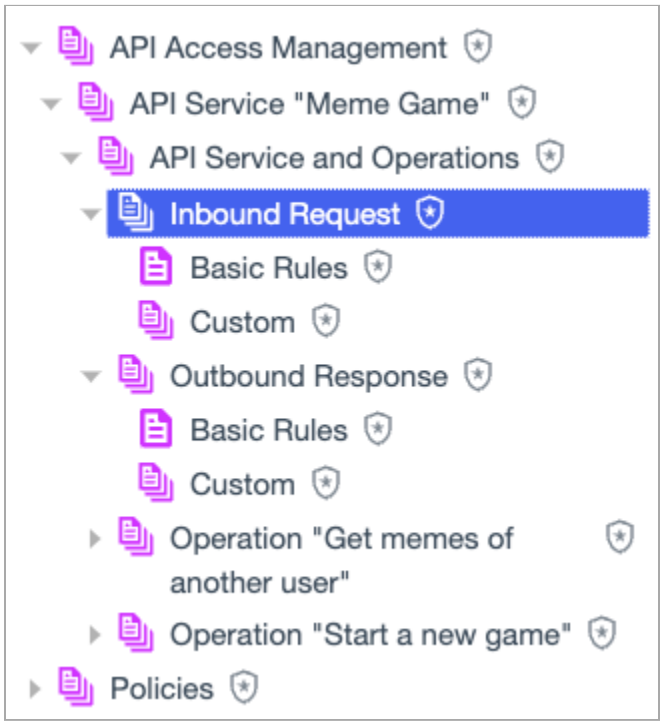
Copyright © 2025 Ping Identity Corporation



Top-level policy sets include:

- **API Service <*Name*>**: This is the top level policy set for the API service. It serves as a container for everything nested underneath it.
- **API Service and Operations**: This policy set ensures that combining algorithms work correctly for AAM rules and policies.

The next level contains the request and response policies and policy sets for each API service.

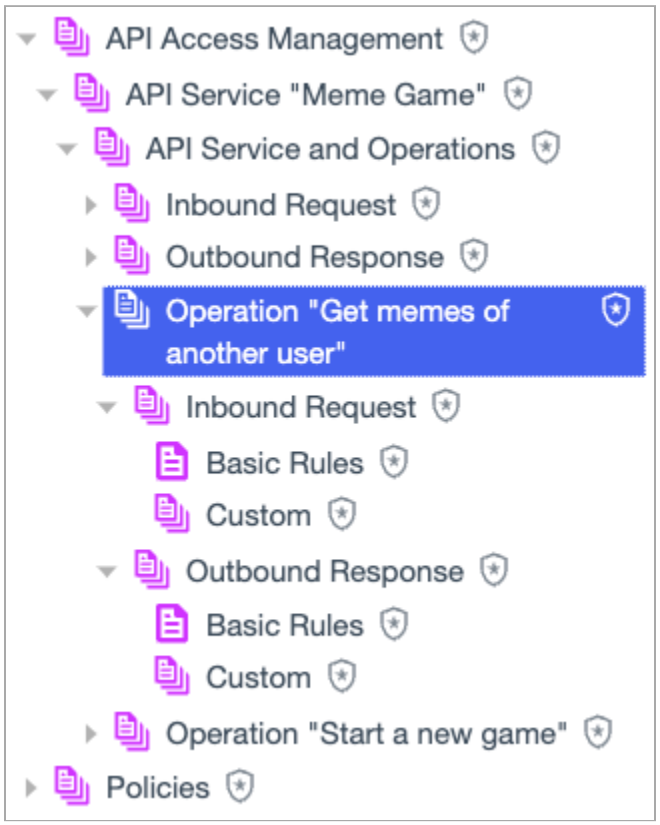


Copyright © 2025 Ping Identity Corporation

These include:

- **Inbound Request**: This policy set is a container for rules and custom policies that target inbound requests for the API service.
  - **Basic Rules**: This policy is reserved for rules generated by the system that target inbound requests for the API service. The rules are based on the API Service configuration.
  - **Custom**: This policy set is where you add your own custom policies that target inbound requests for the API service.
- **Outbound Response**: This policy set is a container for rules and custom policies that target outbound responses from the API service. Its children have the same structure as the **Inbound Request** policy set.

Each operation under the API service shares a similar structure.



Operation policies and policy sets include:

- **Operation <*Name*>**: This is the top level policy set for the operation. It serves as a container for everything nested underneath it.
- **Inbound Request**: This policy set is a container for rules and custom policies that target inbound requests for the specific operation.
  - **Basic Rules**: This policy stores group and scope-based rules that target inbound requests for the operation. The policy is generated automatically by the system when you add basic rules to an operation.
  - **Custom**: This policy set is where you add your own custom policies that target inbound requests for the operation.
- **Outbound Response**: This policy set is a container for rules and custom policies that target outbound responses from the specific operation. It has nested children for **Basic Rules** and **Custom** policies.

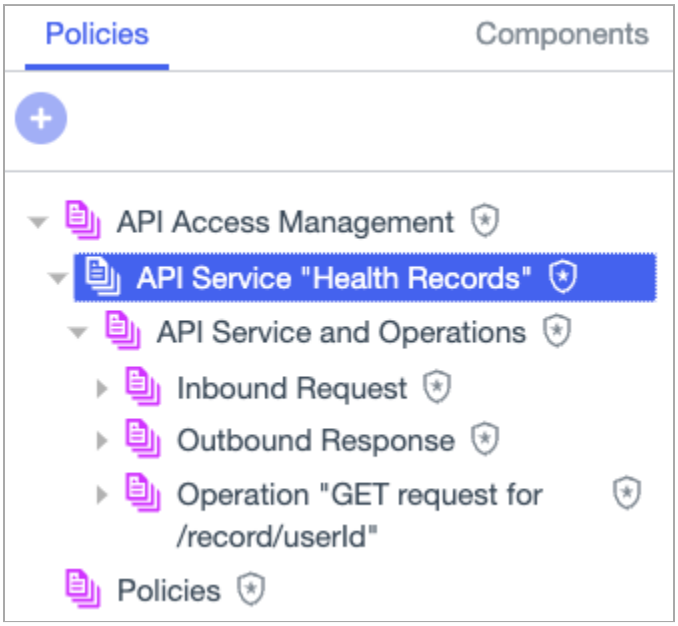
Copyright © 2025 Ping Identity Corporation

> **Note**
>
> For hands-on experience with writing a custom policy for an API operation, see Tutorial 3: Fine-grained API authorization.

Steps

1. Go to **Authorization > Policies**, and expand the **API Access Management** policy tree, then expand the policy tree for your API service.

   For example, consider an API service that protects health records and an API operation to get the records. You want to write a policy that allows a user to view only their own health records.



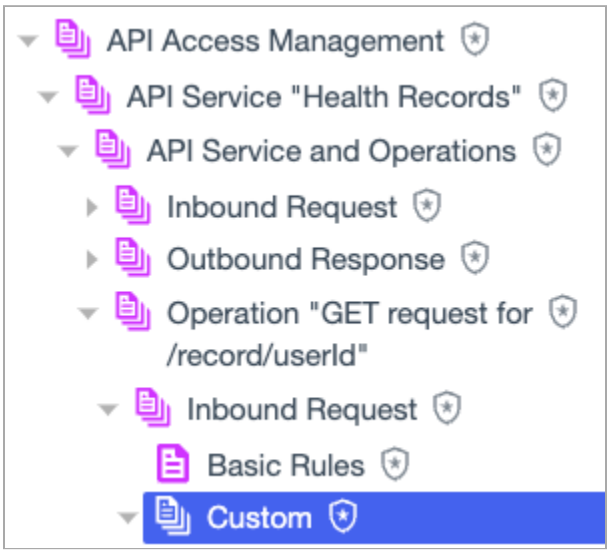
2. In the policy tree, select the **Custom** policy set nested under the request or response that you want the policy to target:

   Choose from:

   - API service **Inbound Request**: This is for policies that will be executed by any API call to any endpoint in the API service. For example, policies that control access based on user characteristics, such as account status or risk score, or whether certain scopes or claims are present in the access token, or whether requests are from certain IP address ranges.
   - API service **Outbound Response**: This is for policies that will modify responses to any API call in the API service. For example, a policy that rewrites the value of an attribute that appears in all responses, such as a URL that uses a private host name.
   - Operation **Inbound Request**: This is for policies that are restricted to specific endpoints. For example, a policy that requires an extra claim in the access token for a POST or PUT request, but not for a GET request, or a policy that constrains a search query to resources owned by the requester, such as allowing a user to view only their own health records.
   - Operation **Outbound Response**: This is for policies that modify responses to API calls to specific endpoints. For example, a policy that filters the attributes of JSON responses to remove sensitive fields that the API can return, such as information that a user hasn't consented to sharing with a requester.

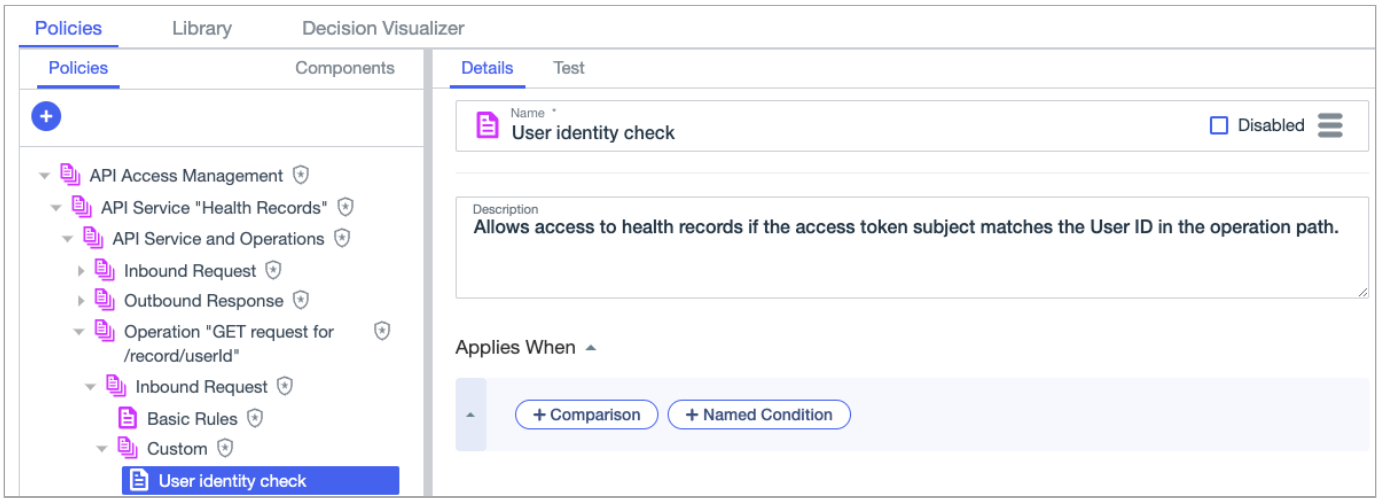
Copyright © 2025 Ping Identity Corporation

For the health records example, you would select the **Custom** policy set for inbound requests to the operation.



3. Click the **+** icon and select **Add Policy**.

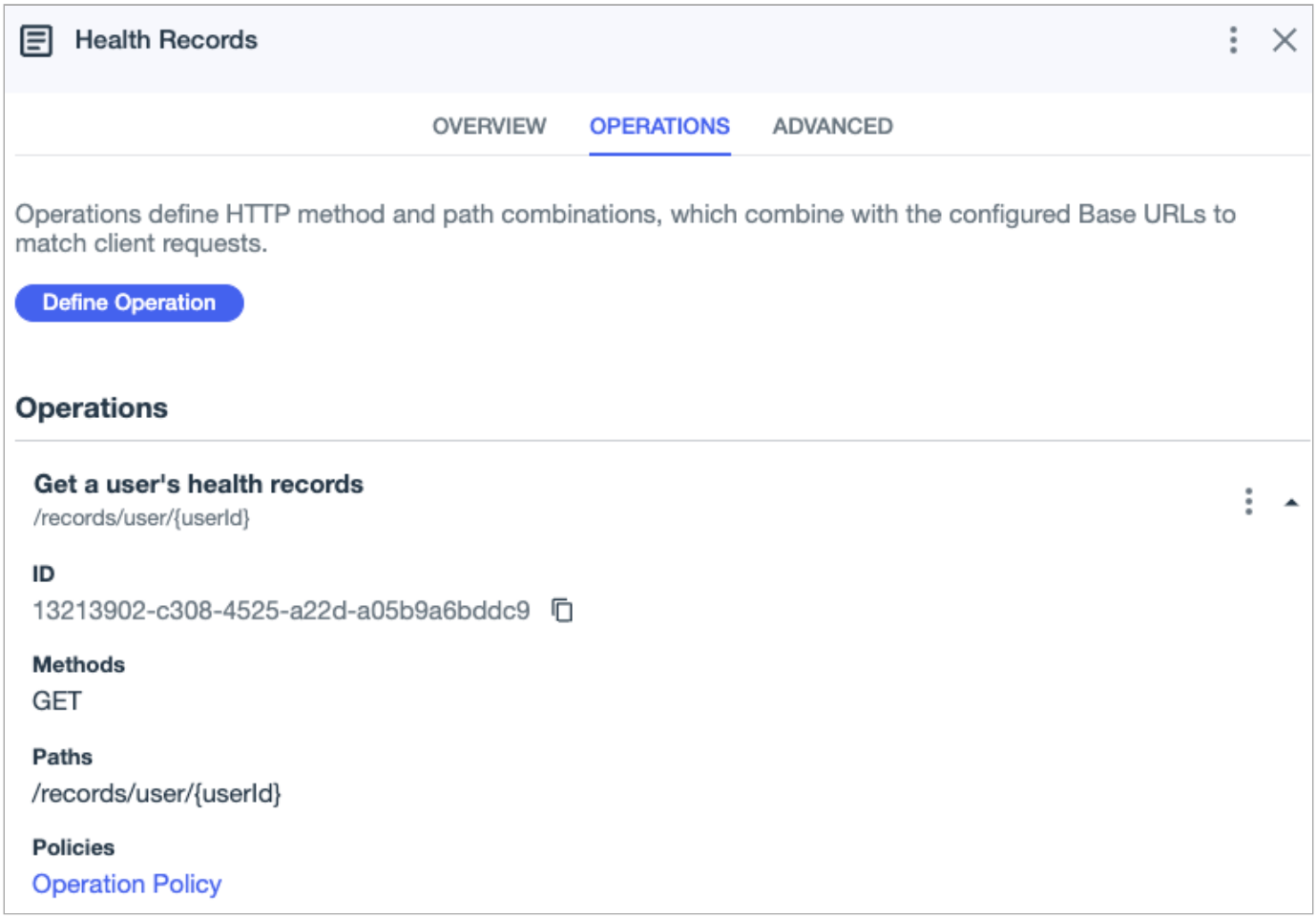
4. In the **Name** field, enter a name relevant to the business rule that you are modeling.



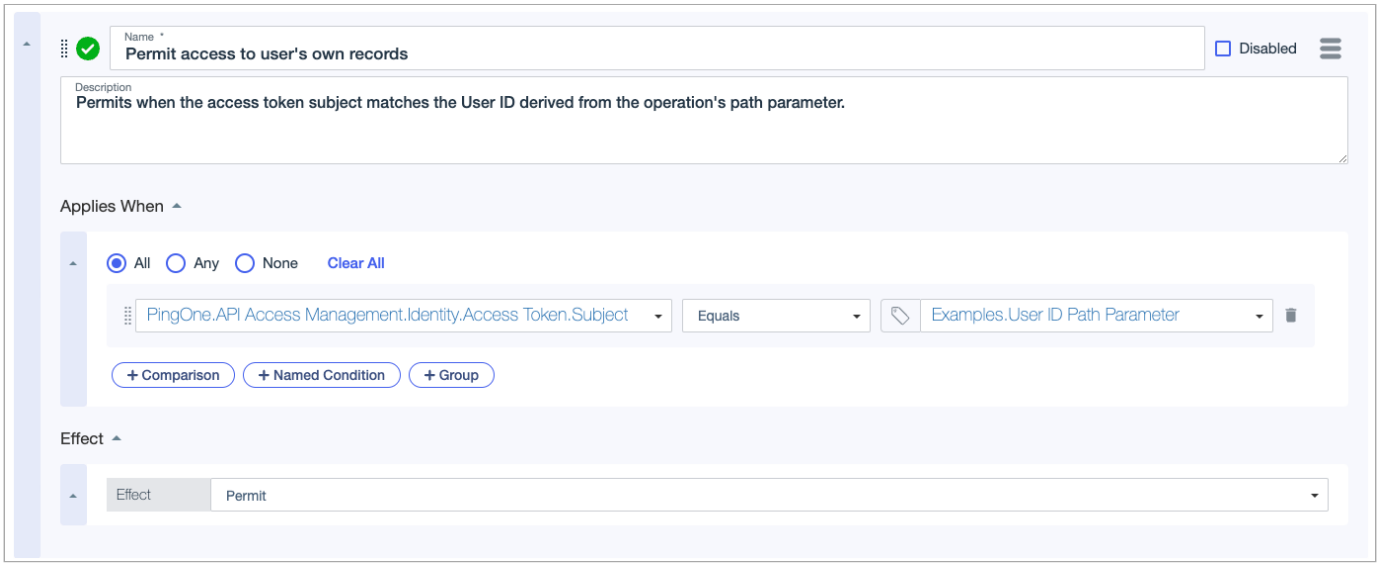
5. Add rules, conditions, and statements to the policy as needed.

For the health records example, consider the following API operation to get a user's health records:

Copyright © 2025 Ping Identity Corporation



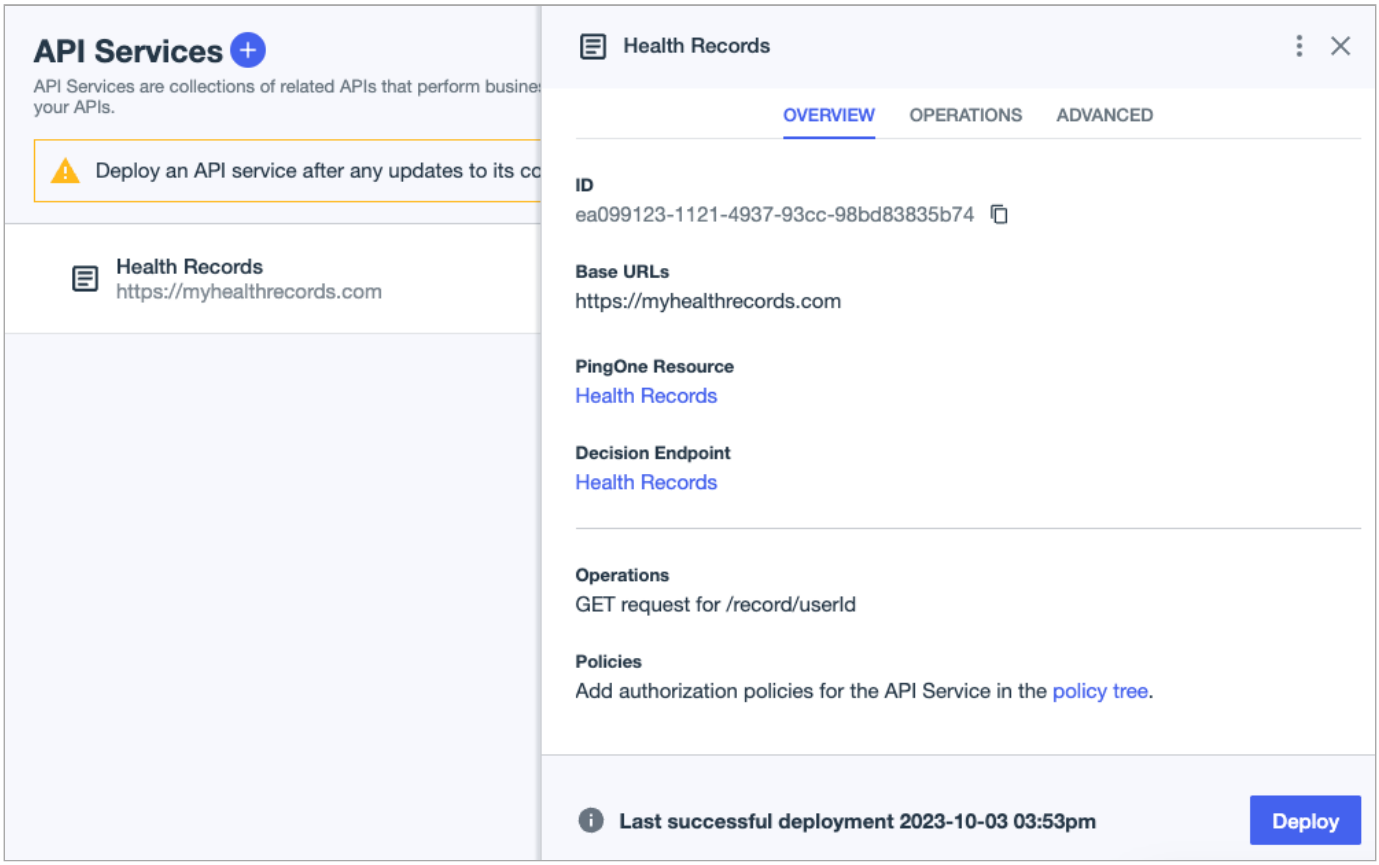
This rule allows access to health records only when the access token's subject claim matches the user ID in the request path. The attribute on the right hand side of the comparison represents the user ID path parameter in the API operation `/records/user/{userId}`. For more information about this attribute, see API Access Management attributes. For more information about accessing information about the requesting user from PingOne Directory or an external directory, see API services.



For more details about the components used in policies, see Authorization policies.

6. Click **Save changes**.

7. To deploy the policy, go to **Authorization** > **API Services**, and select the corresponding API service.



8. Click **Deploy**.

Deploying an API service

Deploy an API service after you make configuration changes, such as updating a setting, adding an operation, or updating attributes or custom policies.

About this task

Each API service has a system-owned decision endpoint that provides an environment for deploying the API service and its authorization policies. The decision endpoint is created when you deploy the API service for the first time, and it has the same name as the API service.

Deploying the API service also deploys the latest version of the **API Access Management** policy tree. This publishes basic and custom policies that target the API service and any operations.

> **Important**
>
> Do not use **Version History** to publish policies that target API services and operations. Instead, deploy the API service.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Authorization > API Services** and select the API service that you want to deploy.

   If the API service has already been deployed, a time stamp at the bottom of the page provides information about the last successful deployment.

2. Click **Deploy**.

Editing an API service

You can edit API service settings, operations, and rules. You can also configure scopes in basic rules.

Steps

1. Go to **Authorization > API Services**, click the **More Options (⋮)** icon next to the API service that you want to edit, and select **Edit**.

2. Update any of the following settings:

   1. (Optional) Change the API service **Name** or **Base URLs**.

   2. (Optional) To change the **PingOne Resource** associated with the API service, select a resource from the list, or select the option to **Automatically create a PingOne Resource**.

      This resource is managed by the API service and there are restrictions against deleting the resource while it's associated with an API service. Resources created automatically will have the same name as the API service. Learn more about resources in API services.

   3. Click **Save**.

3. To edit the API service's authorized scopes:

   Scopes determine the resources that a client can access.

   > **Note**
   >
   > If user directory services and access token validation are managed externally, use your external identity provider (IdP), such as PingFederate, to configure authorized scopes.

   1. On the **Overview** tab, under **PingOne Resource**, click the resource name.

   2. In **Applications > Resources**, click the **Scopes** tab.

   3. (Optional) Change a scope **Name** or **Description**.

   4. (Optional) To add a scope, click **+ Add Scope**, enter a **Name** and **Description** for the scope, and then click **Save**.

   5. (Optional) To edit a scope, click the **Pencil** icon next to the scope, change the **Name** or **Description**, and then click **Save**.

   6. (Optional) To remove a scope, click the **Delete** icon next to the scope, select the checkbox to confirm the deletion, and then click **Delete**.

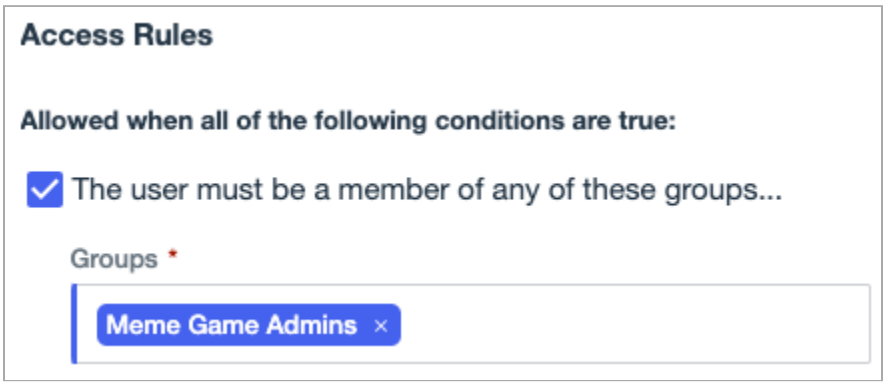
Copyright © 2025 Ping Identity Corporation

4. To add an operation, click the **Operations** tab, and then click **Define Operation**. Complete settings to define the operation.

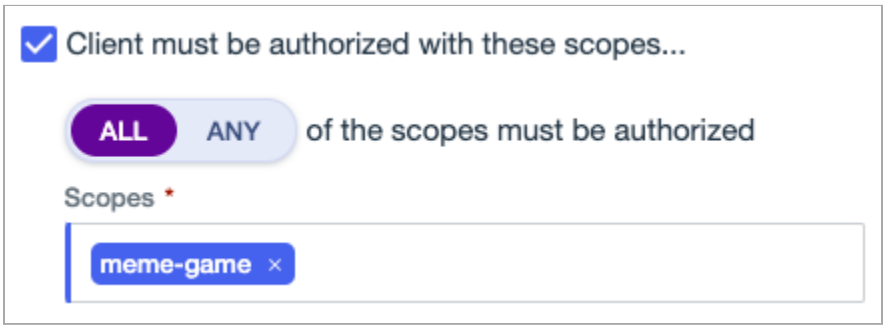
5. To edit an operation, click the **Operations** tab, click the **More Options (⋮)** icon next to the operation name, and then select **Edit Operation**:

    1. (Optional) Change **Methods**, **Paths**, or the operation **Name**.

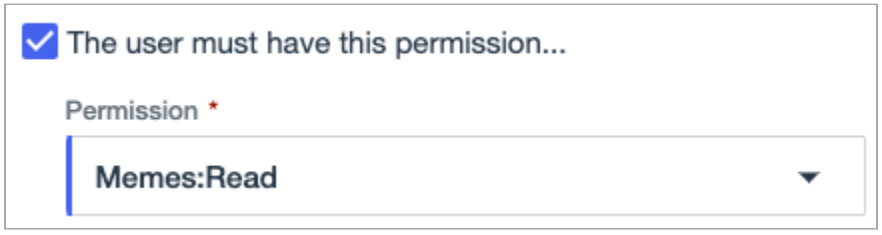
    2. (Optional) In **Access Rules**, change the **Groups** that are granted access to the operation.



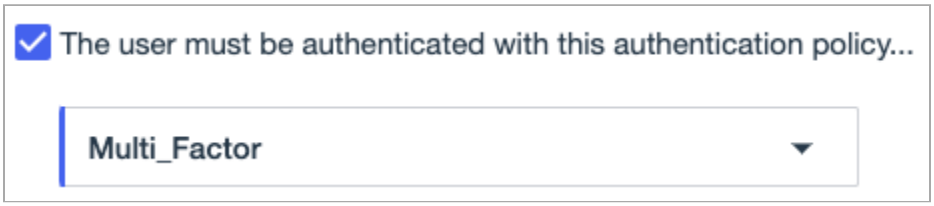
    3. (Optional) Change the scopes that must be authorized.



    4. (Optional) Change the permissions that the user must have.



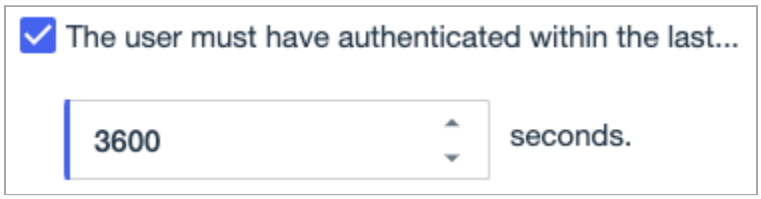
    5. (Optional) Change the required authentication policy.



Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If an authentication flow or sign-on policy is renamed or deleted, you must update this rule accordingly and redeploy the API service.

6. (Optional) Change the maximum amount of time to allow since the last authentication event.



7. Click **Save**.

6. To edit custom policies for the API service:

   1. Go to **Authorization > Policies** and select the policy in the **API Access Management** policy tree.

      You can edit any of the policies that are nested under **Custom** policy sets.

   2. Update the policy, and then click **Save changes**.

   3. Go to **Authorization > API Services** and select the API service.

   4. Click **Deploy**.

Deleting an API service or operation

Remove API services and operations that you no longer need.

About this task

Deleting an API service also deletes the corresponding decision endpoint, any operations and scopes defined for the API service, and the policy tree for the API service. You can also delete the associated PingOne resource.

Steps

1. Go to **Authorization > API Services**.

2. Click the API service that you want to delete or the API service that has the operation that you want to delete.

3. To delete an operation:

   1. Click the **Operations** tab.

   2. Click the **More Options (⋮)** icon next to the operation name, and then select **Delete Operation**.

   3. Select the **I understand and want to continue** check box.

   4. Click **Delete Operation**.

4. To delete the API service:

   1. Click the **More Options (⋮)** icon next to the API service name, and then select **Delete**.

Copyright © 2025 Ping Identity Corporation

2. Select one of the following:
   - **Delete the API service only**: Select this option to delete the API service, its decision endpoint, any operations and scopes, and policy tree. The PingOne resource associated with the API service will not be deleted.
   - **Delete the API service and the PingOne Resource**: Select this option to delete the API service, its decision endpoint, any operations and scopes, the policy tree, and the resource associated with the API service.
3. Select the **I understand and want to continue** check box.
4. Click **Delete**.

Troubleshooting API Access Management

The following resources can help you solve issues with API Access Management.

Solutions

API client HTTP 5xx errors

Likely cause

The API gateway might return HTTP 502 when there is misconfiguration or miscommunication between the Ping Identity gateway integration kit and the HTTP Access Policy Service in PingOne Authorize.

How to troubleshoot

The gateway integration kit logs warning messages to the API gateway error log when it encounters problems communicating with PingOne Authorize. For more information, see the integration kit documentation for your API gateway: Troubleshooting Kong Gateway integration with PingOne Authorize

API client HTTP 404 errors

Likely cause

The API gateway might return HTTP 404 to API clients when PingOne cannot match an API client's request to any of the Base URLs configured for an API service.

How to troubleshoot

PingOne Authorize produces events in your PingOne environment audit log to aid in troubleshooting HTTP 4xx errors. Learn more in Viewing API Access Management events in your PingOne environment audit log.

Details

The PingOne environment audit log will provide more detailed information. For example: `No API server defines policy for the URL`. The error message lists the URL sent by the API client to the API gateway. For example: `https://localhost:8443/meme-game/api/v1/users/user.0/answers`.

Copyright © 2025 Ping Identity Corporation

How to fix

Go to **Authorization > API Services**. Check the Base URL settings for the API service in question. If necessary, create an API service. Ensure that the Base URL for the API service matches the beginning of the URLs used by API clients when making requests for the API service through the API gateway.

API client HTTP 401 errors

Likely causes

The API gateway returns HTTP 401 to API clients when the API client's request cannot be authenticated or doesn't satisfy basic access control checks for an API service. For example, the API client attempts to invoke APIs in API service A using an OAuth Access Token issued for API service B. Or, the API client is using an old OAuth Access Token that has since expired.

How to troubleshoot

PingOne Authorize produces events in your PingOne environment audit log to aid in troubleshooting HTTP 4xx errors. Learn more in Viewing API Access Management events in your PingOne environment audit log.

Details

The PingOne environment audit log provides more detailed information. For example:

```
Request to the URL "https://example.com" denied due to an invalid OAuth access token.
```

The `www-authenticate` HTTP response header contains more information, such as `Token expired` or `Invalid audience`.

How to fix

Ensure that API clients properly manage their OAuth Access Tokens, including refreshing them or obtaining new tokens as necessary before tokens expire.

Other API client HTTP 4xx errors

Likely causes

The API gateway returns other HTTP 4xx errors to API clients when the API client's request doesn't satisfy access control rules configured for the API service or its API Operations in PingOne Authorize. For example, the API client attempts to invoke an API Operation that requires the user to be a member of a particular group in PingOne, but the user is not a member of that group.

How to troubleshoot

PingOne Authorize produces events in your PingOne environment audit log in order to aid in troubleshooting HTTP 4xx errors. Learn more in Viewing API Access Management events in your PingOne environment audit log.

You can trace recent authorization decisions to understand which access rules were not satisfied. Learn more in Viewing recent decisions for the API Access Management decision endpoint.

Copyright © 2025 Ping Identity Corporation

Details

The PingOne environment audit log provides more detailed information. For example:

```
Request to the URL "https://example.com" denied by policy evaluation.
```

The Recent Decisions visualization contains more information, including which rule wasn't satisfied and which attribute values were compared during policy evaluation. For more information, see Examining recent decisions.

How to fix

Ensure that API Operation access rules are properly configured to meet your application requirements. For group-based access control, ensure that the user is a member of one of the required groups. Also, ensure that the API client has been delegated authorization by a user, such as obtaining an OAuth Access Token using OAuth Code Flow.

Viewing API Access Management events in your PingOne environment audit log

Review audit activities in PingOne to verify that the API Access Management service is working properly or to troubleshoot any configuration problems.

About this task

When you make API requests to test configuration of API gateways, API Services, and resource operations, you can review runtime activity logs to ensure components are working correctly and to diagnose configuration problems. You can also check HTTP Access Policy management logs to review the status of actions performed on API Services.

Steps

1. In PingOne, go to **Monitoring > Audit**.
2. Run an audit report to show HTTP Access Policy events:
    1. For **Filter Type**, select **Event Type**.
    2. For **Filter**, select the following options:
        - **HTTP Request Policy Evaluated**
        - **HTTP Response Policy Evaluated**
    3. Click **Run**.
3. In the **Activities** table, in the **Details** column, click **View** to examine details for HTTP Access Policy events.

Parameter	Description
API server resources	The API server name and ID. Also the name and a link to the matched API operation. This information is contained in the `resources` field.
Gateway resources	The name and ID of the gateway that authenticated to the API, your environment ID, and a link to the gateway in the management API. This information is contained in the `actors.client` field.

Copyright © 2025 Ping Identity Corporation

Parameter	Description
Result	The status is either `SUCCESS` or `FAILED`. The description provides an explanation for the success or failure.
Policy evaluation result	Evaluation result codes and messages: ◦ `POLICY_EVALUATION_SUCCEEDED`: The request was evaluated successfully to produce a permit or deny decision. The message further explains the decision. ◦ `POLICY_EVALUATION_FAILED`: The request failed because of a policy evaluation error. ◦ `INVALID_GATEWAY_REQUEST`: The authorization plugin sent an invalid request to PingOne. ◦ `NO_POLICY_FOUND`: No matching API server was found to define the policy for the operation. ◦ `UNEXPECTED_ERROR`: An error occurred that doesn't fall under one of the other result codes. The HTTP response status code is also provided.
Authorization decision	The decision returned by the decision service for HTTP request events: ◦ `PERMIT` ◦ `DENY` ◦ `NOT_APPLICABLE` ◦ `INDETERMINATE`

4. Run another audit report to show API Service events:
    1. For **Filter Type**, select **Event Type**.
    2. For **Filter**, select the following options:
        - **API Service Created**
        - **API Service Deleted**
        - **API Service Deployed**
        - **API Service Updated**
    3. Click **Run**.
5. In the **Activities** table, in the **Details** column, click **View** to examine details for API Service events.

Parameter	Description
Actors	The client that performed the action. Also, the environment ID, the name and ID of the signed-on user, and a link to the user in the management API.
Action	The type of action performed and a brief description.

Copyright © 2025 Ping Identity Corporation

Parameter	Description
Resources	The type, ID, and name of the API Service. Also, the environment ID and a link to the API Service in the management API.
Result	The status is either `SUCCESS` or `FAILED`. The description provides an explanation for the success or failure.

Viewing recent decisions for the API Access Management decision endpoint

Trace recent authorization decisions to help troubleshoot problems with API Access Management rules and policies.

To help with troubleshooting, examine recent decisions for the decision endpoint associated with your API service. For more information, see Examining recent decisions.

API gateways

An API gateway in PingOne Authorize defines the connection between your API gateway and PingOne Authorize and authenticates your API gateway to PingOne.

Ping Identity provides integration kits for third-party API gateways that make it easier for you to manage access control in your APIs. Working with the integration kit in your API gateway, PingOne Authorize uses the best practices of OAuth to manage API access control across these distributed systems.

PingOne Authorize also integrates natively with PingGateway, enabling you to apply low-code access controls for APIs and web applications. Learn more about integrating PingOne Authorize with PingGateway in the PingGateway documentation.

For seamless policy-based access control for your HTTP APIs, configure an integration with PingOne Authorize to have your API gateway enforce authorization rules managed in PingOne Authorize. In addition to configuring an API gateway integration, you can edit or delete an API gateway, or rotate a gateway credential.

Learn more about how traffic flows through an API gateway and PingOne Authorize in How API Access Management works.

PingOne Authorize API gateway integrations

Connect your API gateway to PingOne Authorize to harness the power of API Access Management and dynamic authorization.

Ping Identity supports authorization and access management integrations with third-party API gateways through integration kits. PingOne Authorize also integrates natively with PingGateway. Integration with an API gateway enables policy evaluation through the HTTP Access Policy service in PingOne Authorize.

The following API gateways are supported:

- Amazon Web Services
- Apigee
- Kong Gateway
- Kong Konnect

Copyright © 2025 Ping Identity Corporation

- PingGateway

Integrating PingOne Authorize with Amazon Web Services

Ping Identity's integration kit for Amazon Web Services (AWS) extends AWS's authorization capabilities through an external policy evaluation service.

Integration with AWS allows centralized management of API access control and application protection in PingOne Authorize while delegating enforcement to AWS. Learn more about how this integration kit interacts with PingOne Authorize in How API Access Management works.

Install and configure the integration kit in AWS to enable management of access control rules in PingOne Authorize. The integration kit works with Amazon API Gateway or Amazon CloudFront.

To configure the integration kit:

- Set up an API gateway in PingOne Authorize

Choose one:

- Configure the integration kit as a Lambda authorizer that works with Amazon API Gateway.
- Configure the integration kit as a Lambda@Edge function that works with Amazon CloudFront.

> **Note**
>
> Version 1.4.0 of the integration kit supports integration with Amazon CloudFront.

Policy limitations

The integration kit supports all of the basic rules for controlling access to your protected API resources.

> **Note**
>
> Although you can use the **authentication policy** and **time since last authentication** basic rules to control access to sensitive resources, AWS doesn't return the full step-up challenge response. When these rules produce deny decisions, AWS returns a simple deny response with an HTTP status code.

The following limitations apply to using custom policies for API services and operations with this integration kit:

- PingOne Authorize only evaluates policies that target the inbound request.
- The built-in `PingOne.API Access Management.HTTP.Request.Body` attribute is not available for authorizing inbound requests.
- When PingOne Authorize permits an inbound request, no request transformations are applied before AWS forwards the request to the backend API.
- Headers set in policy aren't included in the AWS response to the client.
- In policies that use the `auth-challenge` statement, only the `httpStatus` payload property affects the response.

Copyright © 2025 Ping Identity Corporation

When deploying the integration kit with Amazon API Gateway, setting this property to `401` results in an `UNAUTHORIZED` response that defaults to a `401` status code. Any other value results in an `ACCESS_DENIED` response that defaults to a `403` status code. To learn how to modify the default status code, refer to Gateway responses in the Amazon API Gateway documentation.

- When deploying the integration kit with CloudFront, responses for deny decisions don't include response bodies.

Setting up PingOne Authorize for Amazon Web Services integration

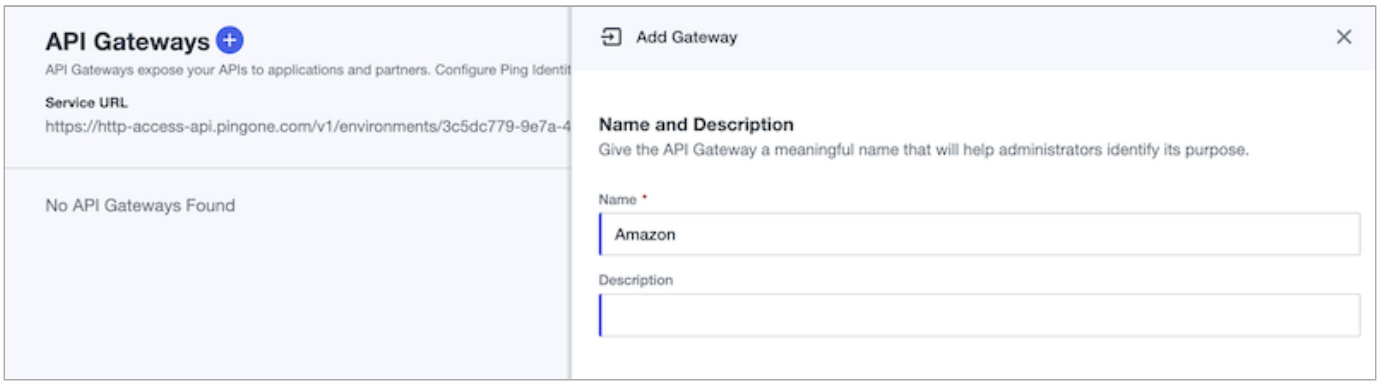
To allow Amazon Web Services (AWS) to use PingOne Authorize as an external runtime authorization policy service, set up an API gateway in PingOne that represents AWS. This will prepare PingOne Authorize to authenticate authorization requests from AWS.

Before you begin

Add PingOne Authorize to your PingOne environment. Learn more in Adding the PingOne Authorize service to your environment.

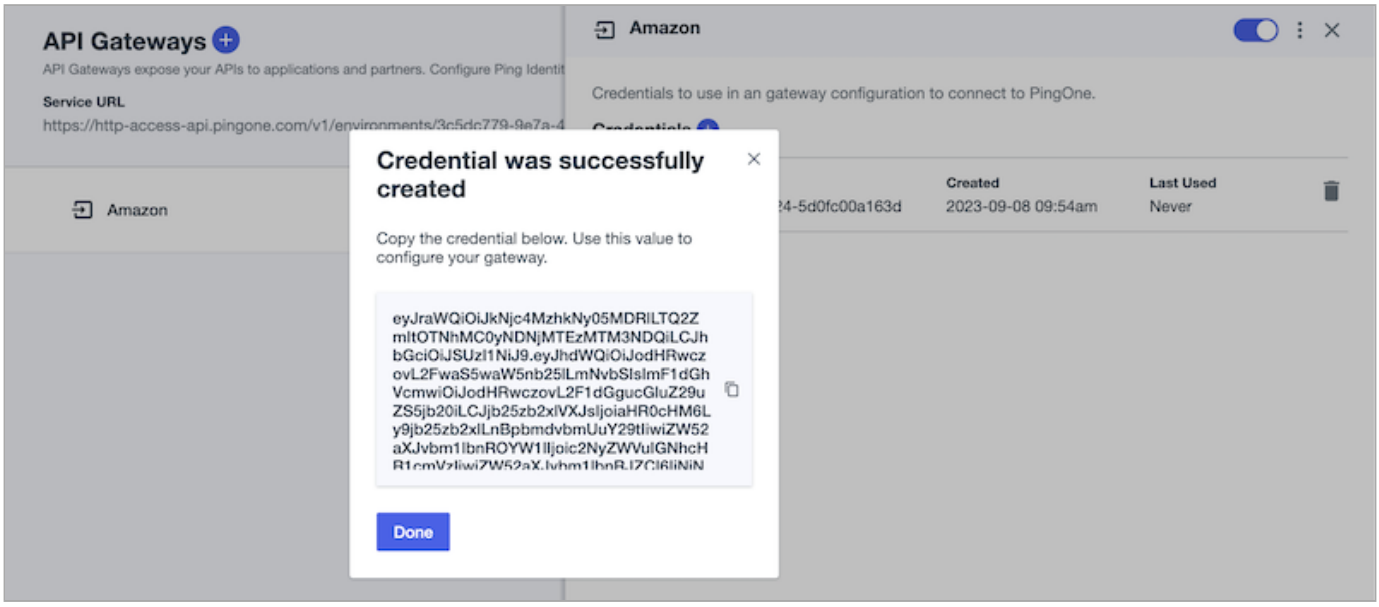
Steps

1. In PingOne, go to **Authorization** > **API Gateways**.
2. Copy the **Service URL** and save it somewhere convenient for later use.
3. To add a gateway, click the **+** icon next to **API Gateways**.
4. Enter a name for the gateway, such as `Amazon`. Click **Save**.



5. Click the **+** icon next to **Credentials**, copy the credential, and save it for later use.

Copyright © 2025 Ping Identity Corporation



6. Click **Done**.

Configuring Amazon API Gateway for PingOne Authorize integration

Deploy the Amazon Web Services (AWS) integration kit as a request parameter-based Lambda authorizer and configure it to integrate with PingOne Authorize and Amazon API Gateway.

When an API client sends a request, Amazon API Gateway invokes the Lambda authorizer to evaluate whether access should be granted. The authorizer calls PingOne Authorize to make an access decision based on your policy configurations.

- If access is allowed, Amazon API Gateway forwards the API client request to the backend REST API.
- If access is denied, Amazon API Gateway returns an appropriate HTTP status code and a reason for denial to the API client.

Before you begin

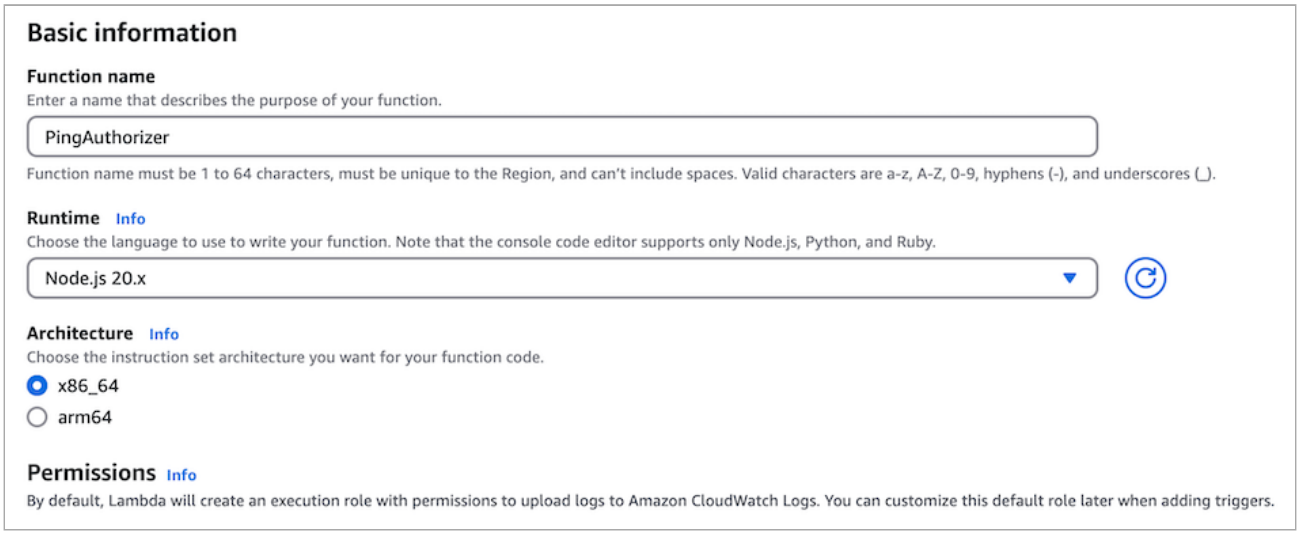
Ensure you have:

- A comfortable level of knowledge of the following interfaces and technologies (or access to developers as needed):
  - AWS Management Console
  - Lambda functions
  - Amazon API Gateway
- Sufficient permissions to create, edit, and publish Lambda functions and modify API endpoints.
- The AWS integration kit downloadable `.zip` archive. Download the integration kit from the Ping Identity Integration Directory.
- An understanding of policy limitations.

Copyright © 2025 Ping Identity Corporation

Steps

1. Create the Lambda function:
    1. Open the AWS Lambda console.
    2. Click **Create function**.
    3. Click **Author from scratch**.
    4. In the **Function name** field, enter a name.
    5. In the **Runtime** list, select **Node.js 20.x**.
    6. In the **Architecture** section, click **x86_64**.



    7. Click **Create function**.

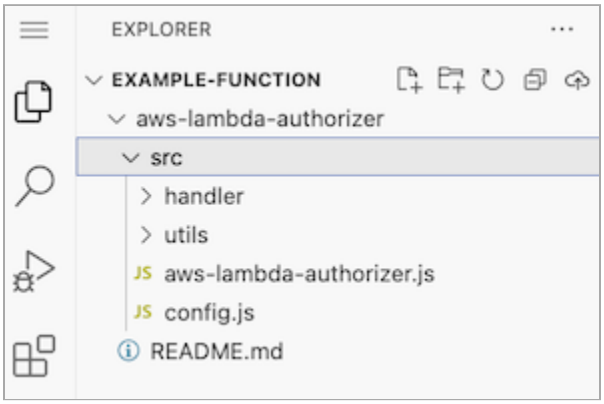
    Result:

    A page opens for your new Lambda function.

2. Upload the integration kit `.zip` archive and configure the environment variables:
    1. In the **Code source** section, select **.zip file** in the **Upload from** list.
    2. In the **Upload a .zip file** modal, click **Upload**. Select the integration kit `.zip` archive.
    3. Click **Save**.

    The Lambda code source should appear with these files uploaded:

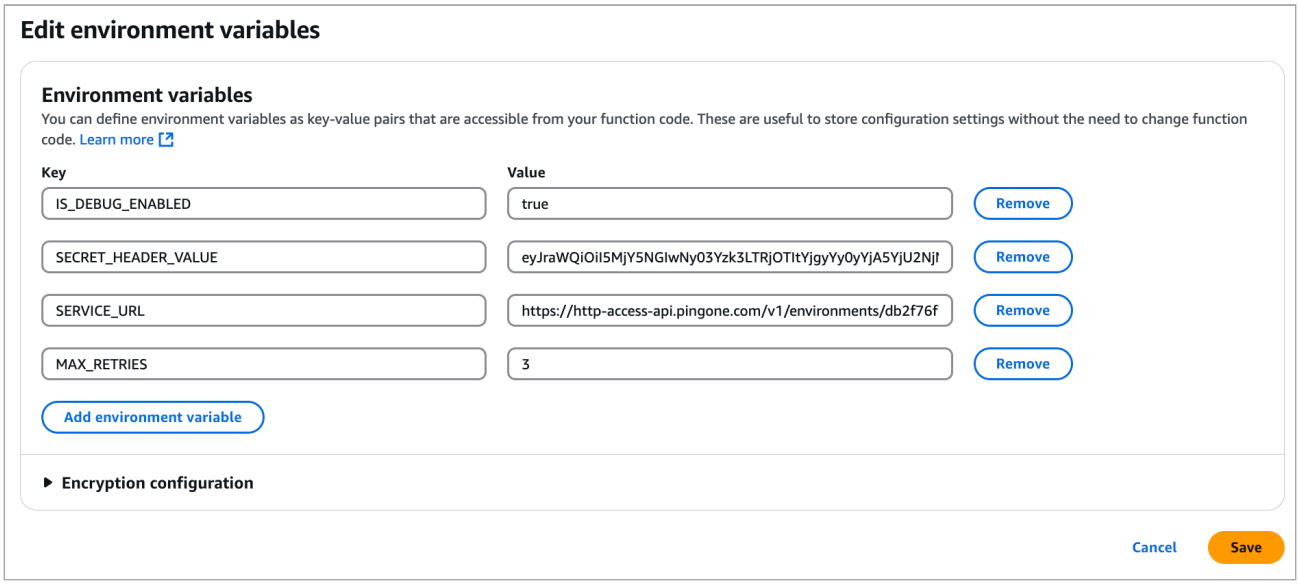
Copyright © 2025 Ping Identity Corporation



4. Scroll down, and in the **Runtime settings** section, click **Edit**.
5. In the **Runtime** list, select **Node.js 20.x**.
6. In the **Handler** field, enter `aws-lambda-authorizer/src/aws-lambda-authorizer.handler`.
7. Click **Save**.
8. Scroll up and click the **Configuration** tab.
9. In the left-hand navigation, click **Environment variables**, and then click **Edit**.
10. Add the following environment variables:

Environment variable	Value
`IS_DEBUG_ENABLED`	The value is `true` or `false` depending on whether debugging is required. Set this value to `false` in production environments.
`SECRET_HEADER_VALUE`	The gateway credential that you saved earlier in the PingOne console.
`SERVICE_URL`	The service URL that you saved in Setting up PingOne Authorize for Amazon Web Services integration.
`MAX_RETRIES`	Controls the number of connection retries that the integration kit performs when a PingOne Authorize request fails because of network errors or HTTP 5xx responses. The default is `1`.

Copyright © 2025 Ping Identity Corporation



11. Click **Save**.

    If you have already configured your backend API in AWS, skip to step 4.

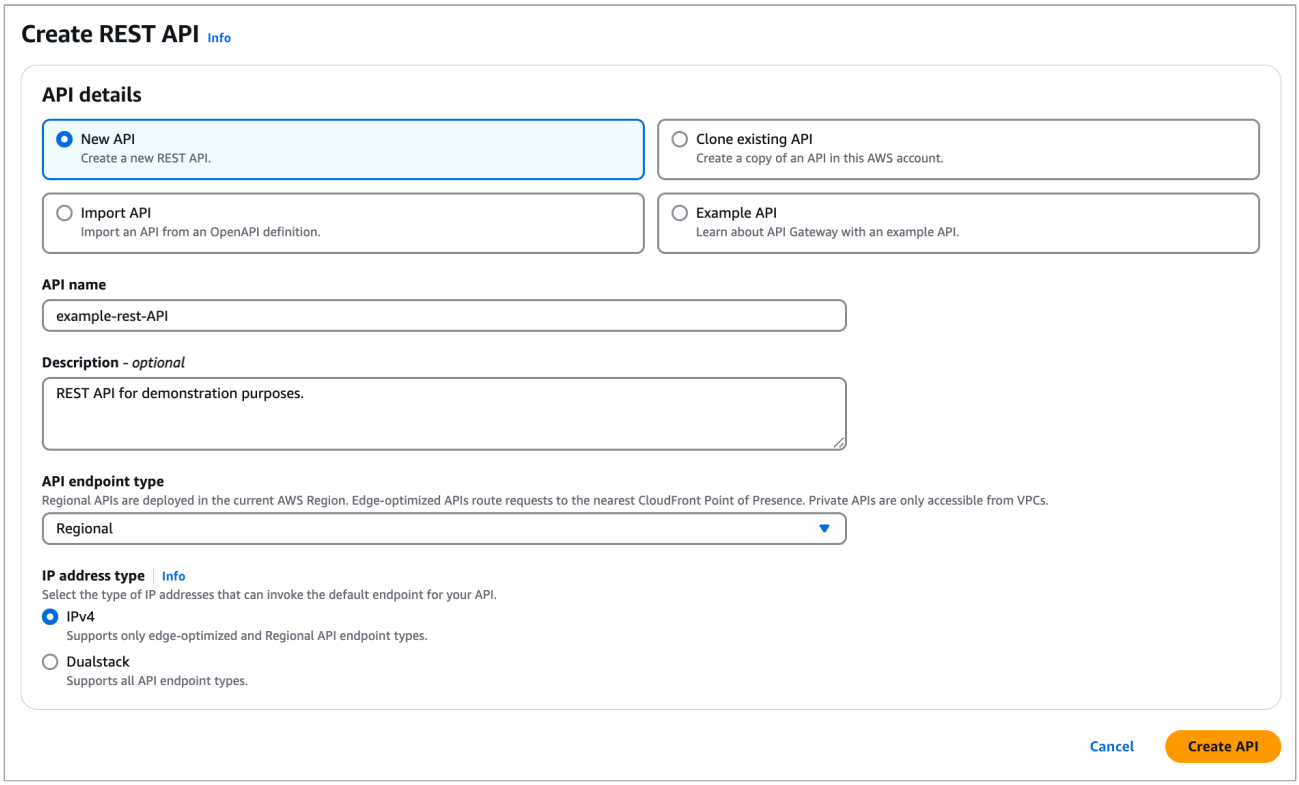
3. Configure a backend REST API:

    1. Open the AWS API Gateway console.
    2. Click **Create API**.
    3. In the **REST API** menu, click **Build**.

    > **Important**
    >
    > The AWS integration kit only supports and has only been tested with REST APIs.

    4. In the **API name** field, enter a name. Leave the rest of the default selections.

Copyright © 2025 Ping Identity Corporation



5. Click **Create API**.

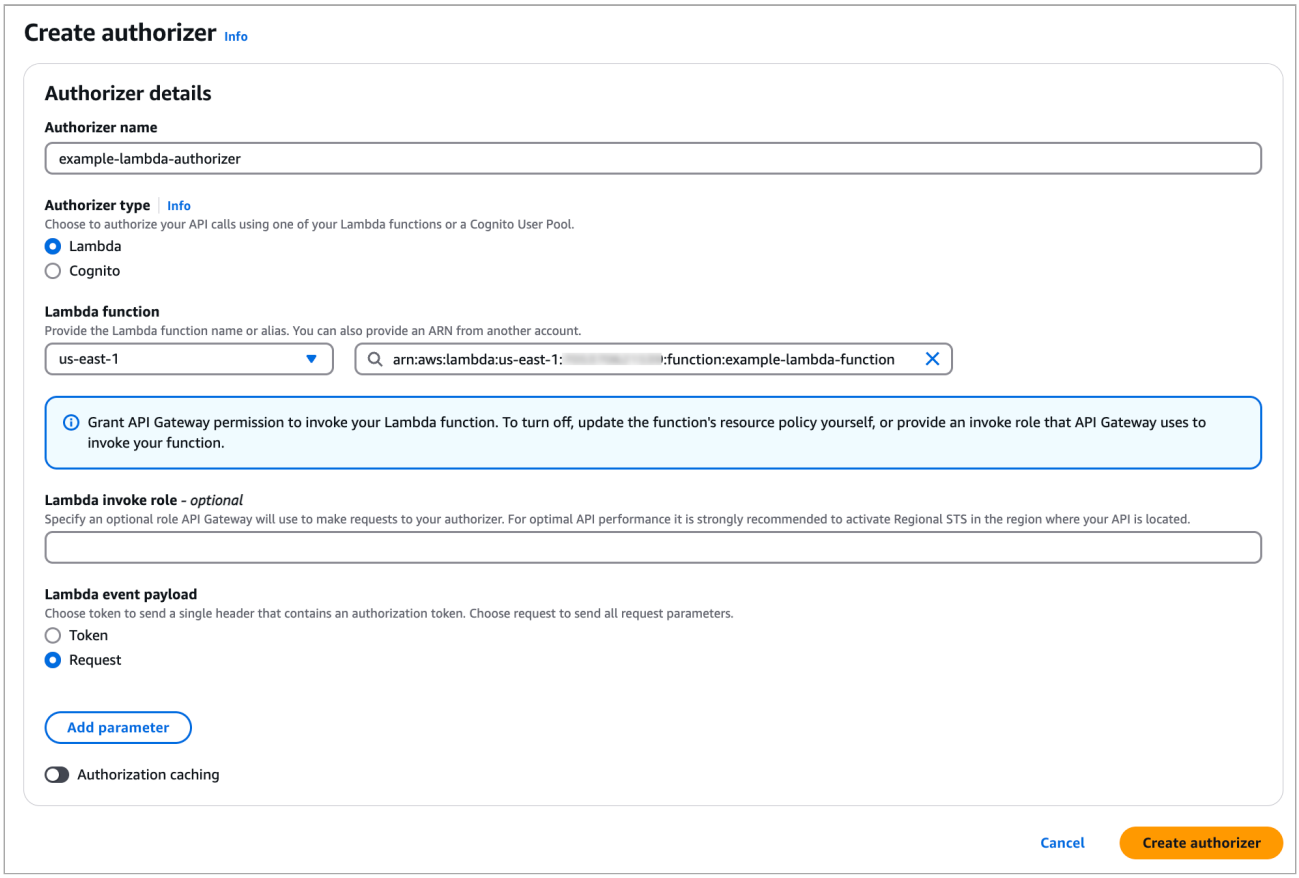
4. Configure Lambda authorizer using the Lambda function:

    1. On the page for your backend API, click **Authorizers** in the left-hand navigation.

    2. Click **Create Authorizer**.

    3. In the **Name** field, enter a name.

Copyright © 2025 Ping Identity Corporation



4. For the **Type**, click **Lambda**.
5. In the **Lambda Function** section, select your region and enter the name of the Lambda function that you created earlier.
6. Leave the **Lambda Invoke Role** field blank.

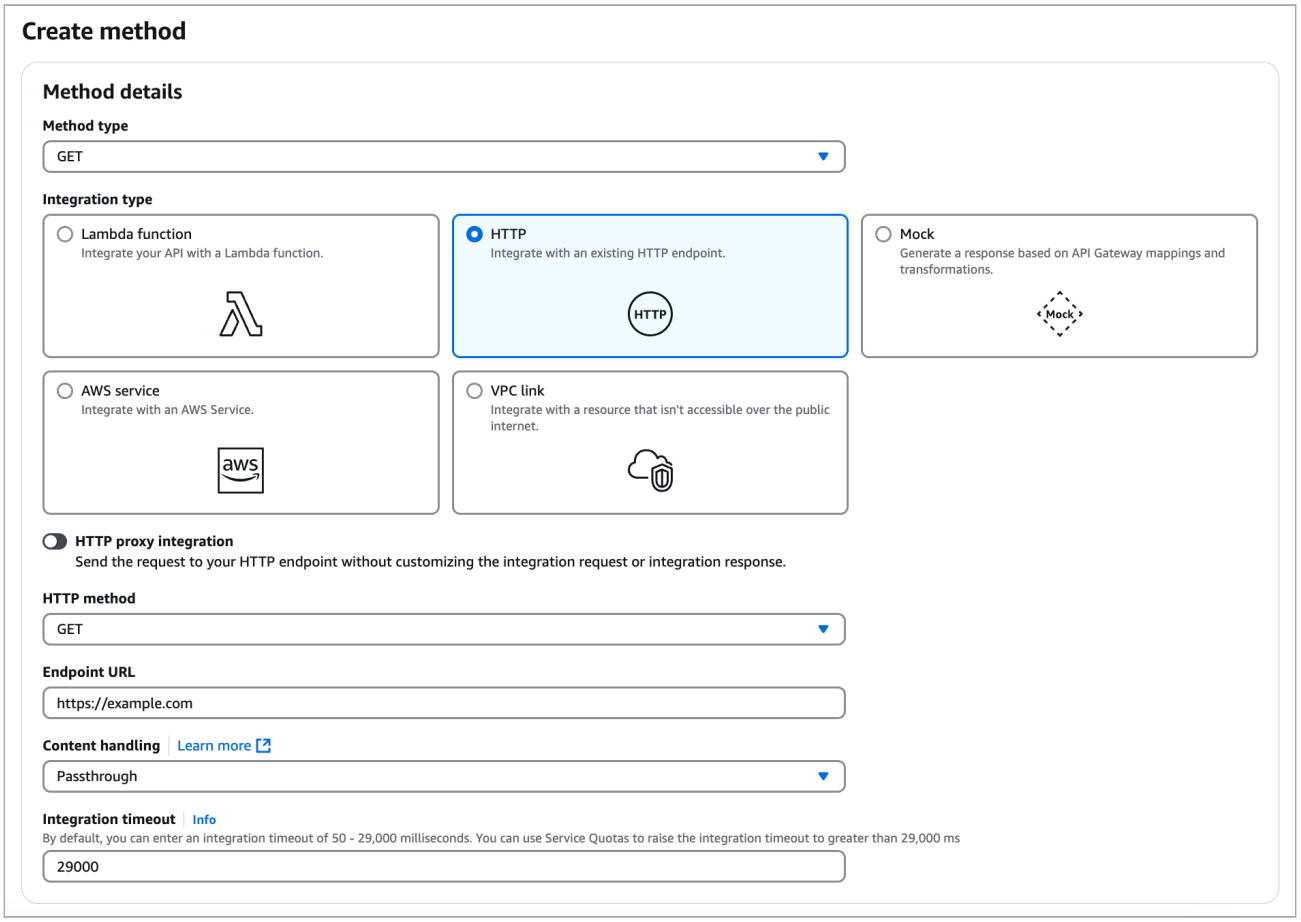
   By default, the Amazon API Gateway console sets a resource-based policy that grants the API Gateway permissions to invoke Lambda authorizer.
7. Under **Lambda Event Payload**, click **Request**.
8. Disable the **Authorization Caching** toggle.
9. Next to the **Identity source type** and **Key** fields, click **Remove**.
10. Click **Create authorizer**.

    You must repeat this Lambda configuration for each REST API that you want to protect with Lambda authorizer.

5. Assign an API method to Lambda authorizer and configure the integration point:
   1. On the page for your newly created backend API, click **Resources** in the left-hand navigation.
   2. Click **Create Resource**.
   3. Enter a name and path for your resource.
   4. Click **Create Resource**.

Copyright © 2025 Ping Identity Corporation

5. In the **Methods** section, click **Create Method**.
6. In the **Method type** list, select an API method.

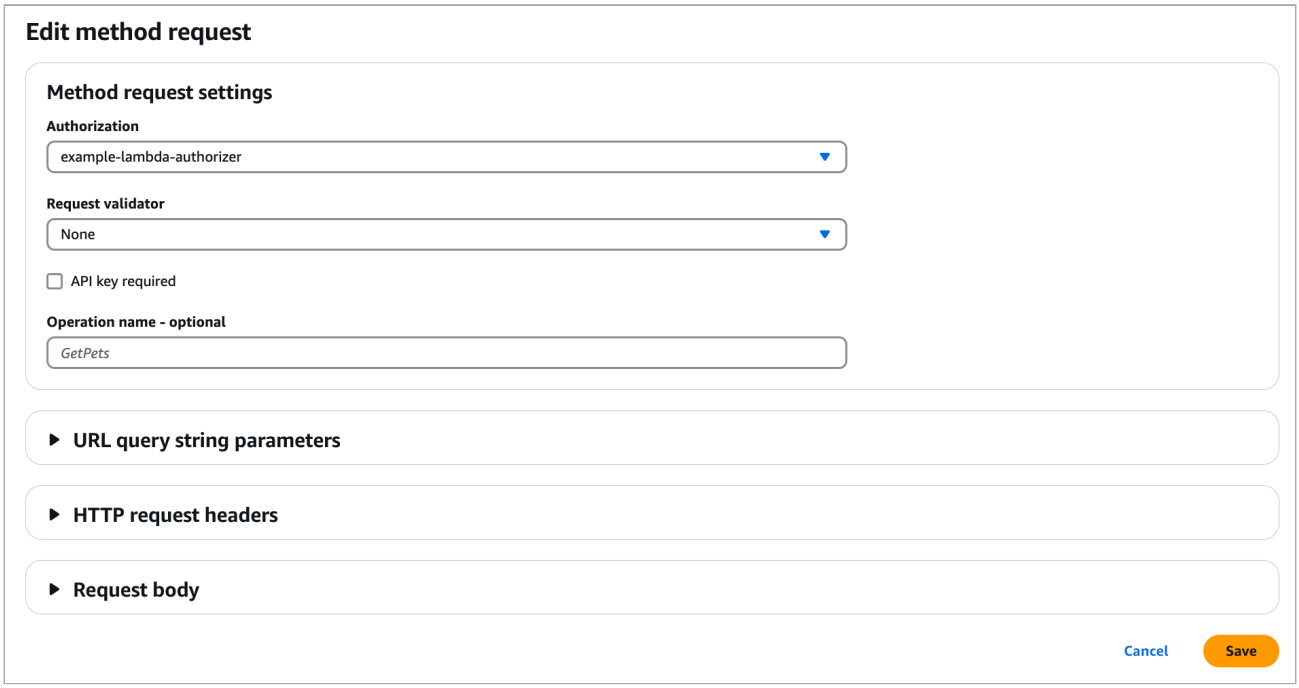


Resources in your API define one or more methods, such as `GET` or `POST`. Integrating these methods with Lambda authorizer means that any client API request of this method type is forwarded to the configured Lambda function.

You can define each resource and method individually, or use special resource and method types that apply to all incoming requests of a certain form. For example, the `ANY` method applies to all incoming requests.

7. For the **Integration type**, click **HTTP**.
8. In the **HTTP method** list, select a method corresponding to the method that you selected in step 5f.
9. In the **Endpoint URL** field, enter the endpoint to which the client API request is sent.
10. Keep the other default values and click **Save**.
11. Click the **Method Request** tab.
12. In the **Method request settings** section, click **Edit**.
13. In the **Authorization** list, select your lambda authorizer.

Copyright © 2025 Ping Identity Corporation



14. Click **Save**.

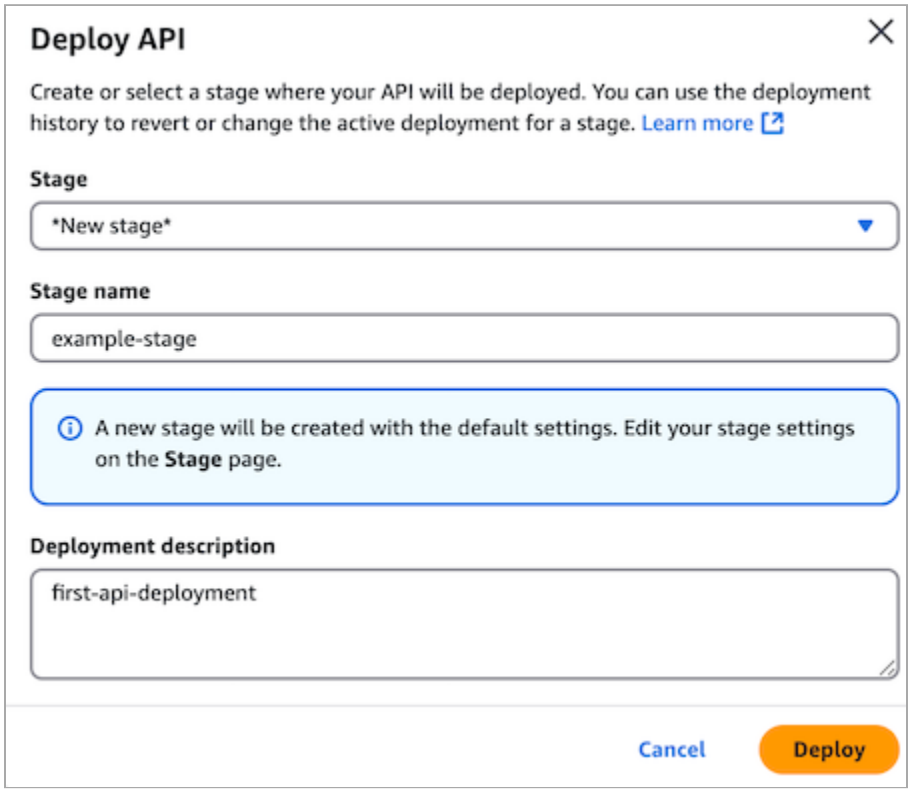
6. Deploy the API Gateway:

    1. On the page for your API, click **Resources** in the left-hand navigation.
    2. Click **Deploy API**.
    3. In the **Stage** list, do one of the following:

        Choose from:

        - Select an existing stage to deploy to.
        - Select **New Stage**. Enter a name and optional description for the stage.

Copyright © 2025 Ping Identity Corporation



4. Click **Deploy**.

Next steps

Define API services to represent your APIs so that PingOne Authorize can help your API gateway enforce access control. For more information, see Defining your API in PingOne Authorize.

> **Important**
>
> If you're using AWS to enforce access control, the API service definition must use PingOne SSO as the directory and token source.

Troubleshooting

To help track and debug issues related to your REST API, you can configure Amazon CloudWatch logging. Learn more in Set up CloudWatch logging for REST APIs in API Gateway in the Amazon API Gateway documentation.

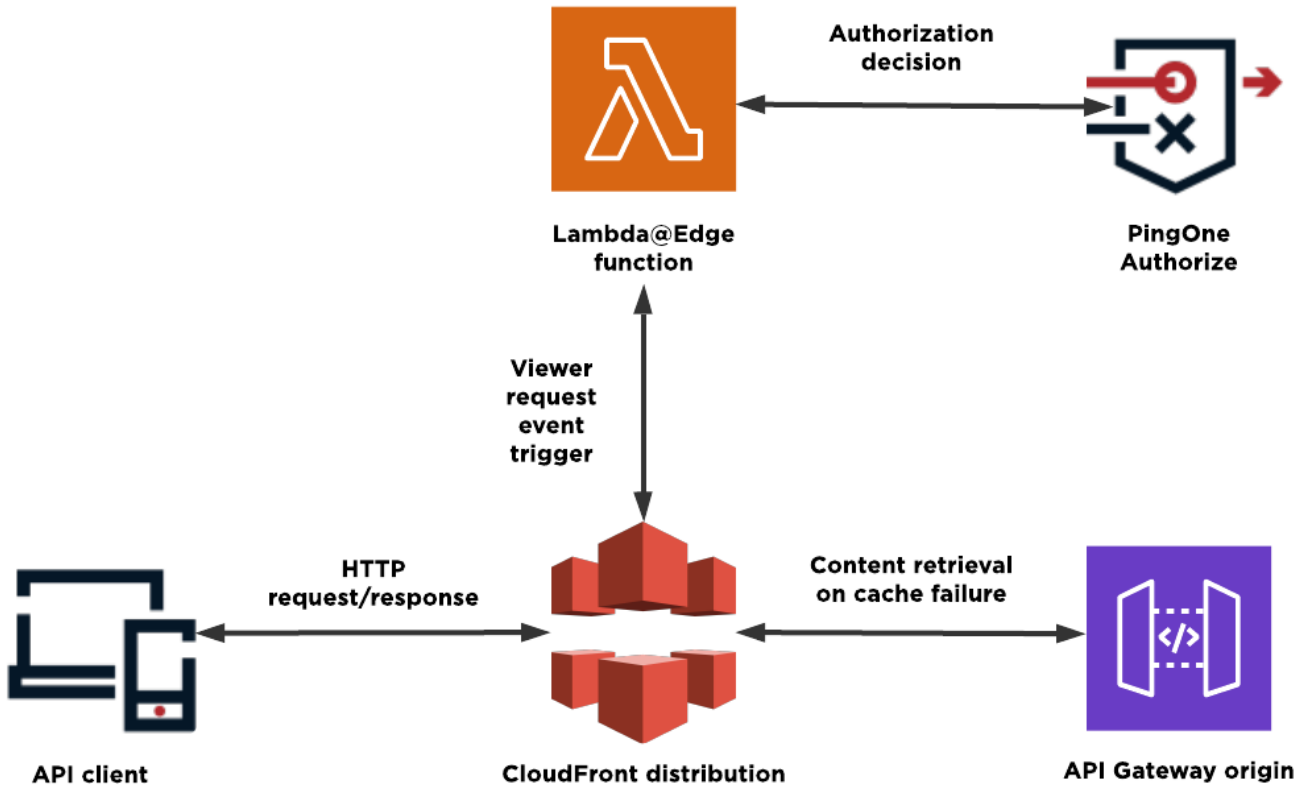
Configuring Amazon CloudFront for PingOne Authorize integration

Deploy the Amazon Web Services (AWS) integration kit as a Lambda@Edge function and configure it to integrate with PingOne Authorize and Amazon CloudFront.

Copyright © 2025 Ping Identity Corporation

Request flow

The following diagram and steps represent a typical request flow with CloudFront, a Lambda@Edge function, an API Gateway origin server, and PingOne Authorize:



1. The API client makes an HTTP request to the CloudFront distribution's domain.
2. The request is routed to a CloudFront edge location.
3. The Lambda@Edge function is invoked at the viewer request stage and processes the API client request.

   As part of this processing, the Lambda@Edge function calls PingOne Authorize for an authorization decision.

   - If authorized, the API client request proceeds to the next step.
   - If unauthorized, CloudFront sends a deny response to the API client, and the request terminates.
4. CloudFront forwards the request to the origin server.
5. The origin server processes the request and sends a response.
6. CloudFront decides whether to cache the response and sends the final response back to the API client.

Before you begin

Copyright © 2025 Ping Identity Corporation

To set up a CloudFront distribution and a Lambda@Edge function, you'll need:

- A comfortable level of knowledge of the following interfaces and technologies (or access to developers as necessary):
  - AWS Management Console
  - CloudFront
  - Lambda functions
- Sufficient permission to create, edit, and publish Lambda functions and CloudFront distributions.
- Version 1.4.0 or later of the AWS integration kit downloadable `.zip` archive. Download the latest integration kit from the Ping Identity Integration Directory.
- An understanding of policy limitations.

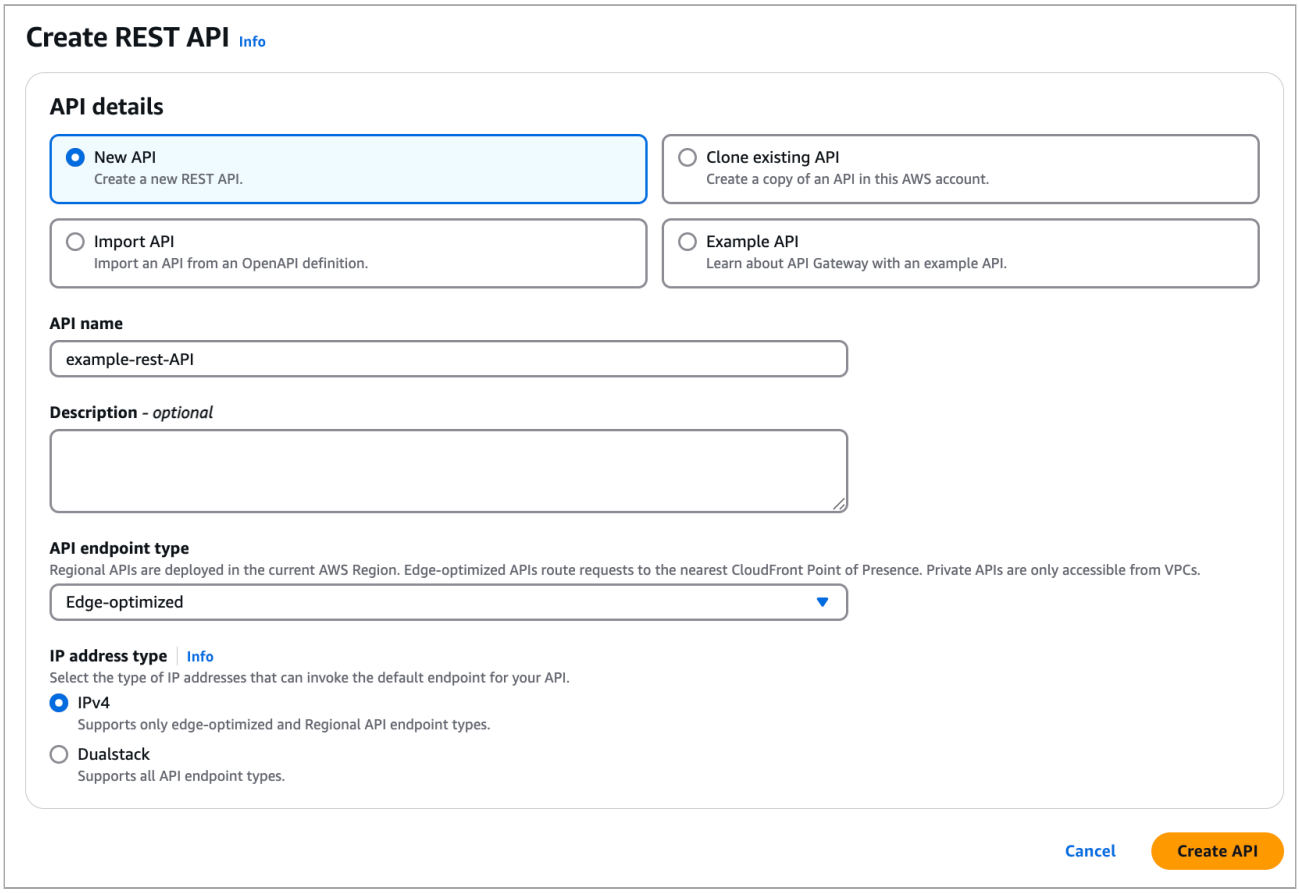
Configuring an API Gateway origin

Create and configure an Amazon API Gateway to serve as the origin for CloudFront.

Steps

1. Create a backend REST API:
   1. Open the AWS API Gateway console.
   2. Click **Create API**.
   3. In the **REST API** section, click **Build**.
   4. In the **API name** field, enter a unique name for your API.

Copyright © 2025 Ping Identity Corporation



5. In the **API endpoint type** list, select an endpoint type for your API.

   Learn more about the available endpoint types in API endpoint types for REST APIs in the Amazon API Gateway documentation.

6. Click **Create API**.

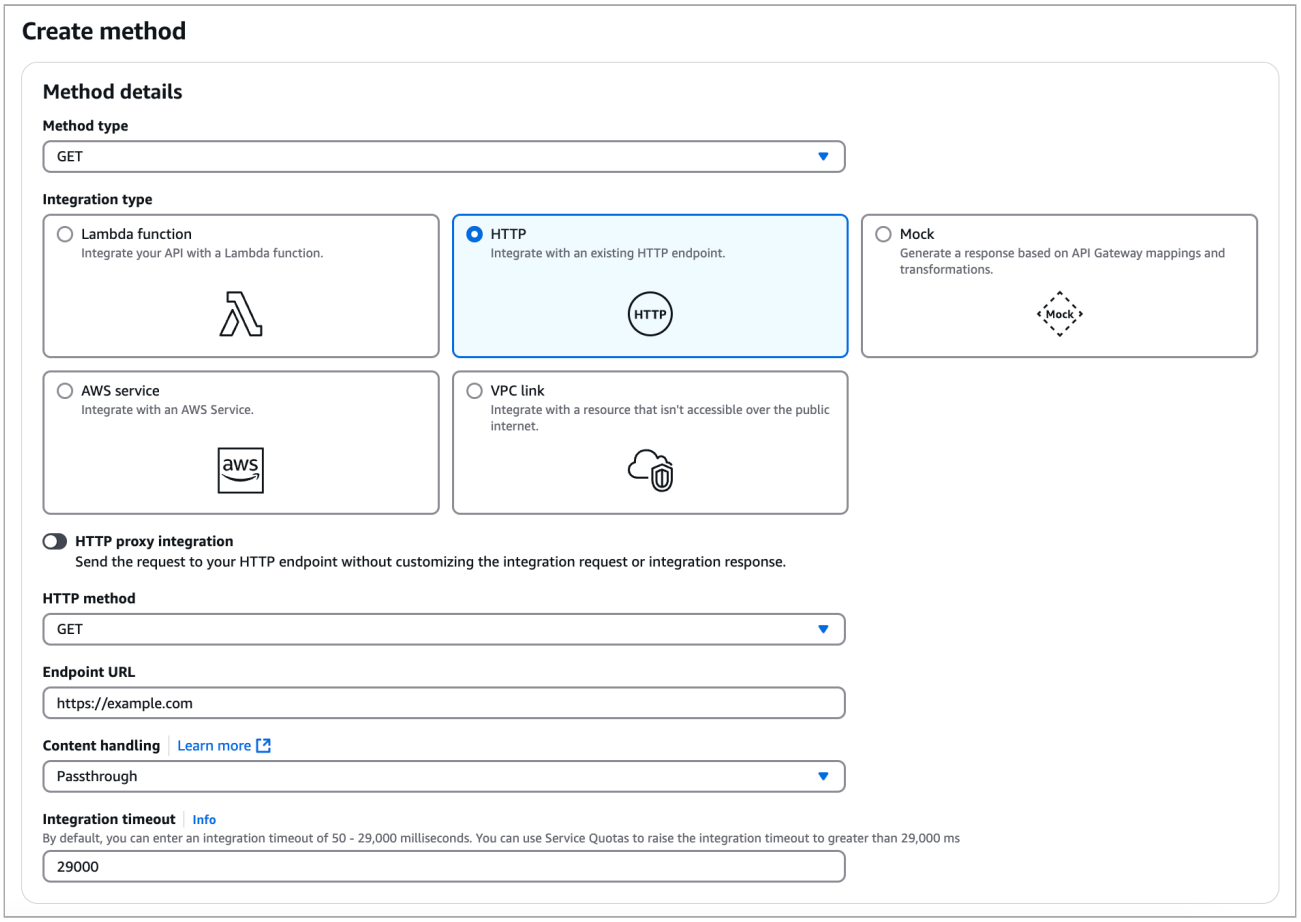
   Result:

   A page opens for your new API.

2. Create an API method:

   1. In the **Methods** section, click **Create method**.
   2. In the **Method type** list, select an API method.

Copyright © 2025 Ping Identity Corporation



3. Under **Integration type**, click **HTTP**.
4. Configure the rest of the method to meet your business needs.
5. Click **Create method**.

   Result:

   The page for your API opens with the new method defined.

3. Deploy your REST API:
   1. Click **Deploy API**.
   2. In the **Stage** list, select a deployment stage.
   3. (Optional) In the **Deployment description** field, enter a description.
   4. Click **Deploy**.
4. Go to **Stages** and select the deployed stage.
5. In the **Stage details** section, copy the **Invoke URL** for later use.

Copyright © 2025 Ping Identity Corporation

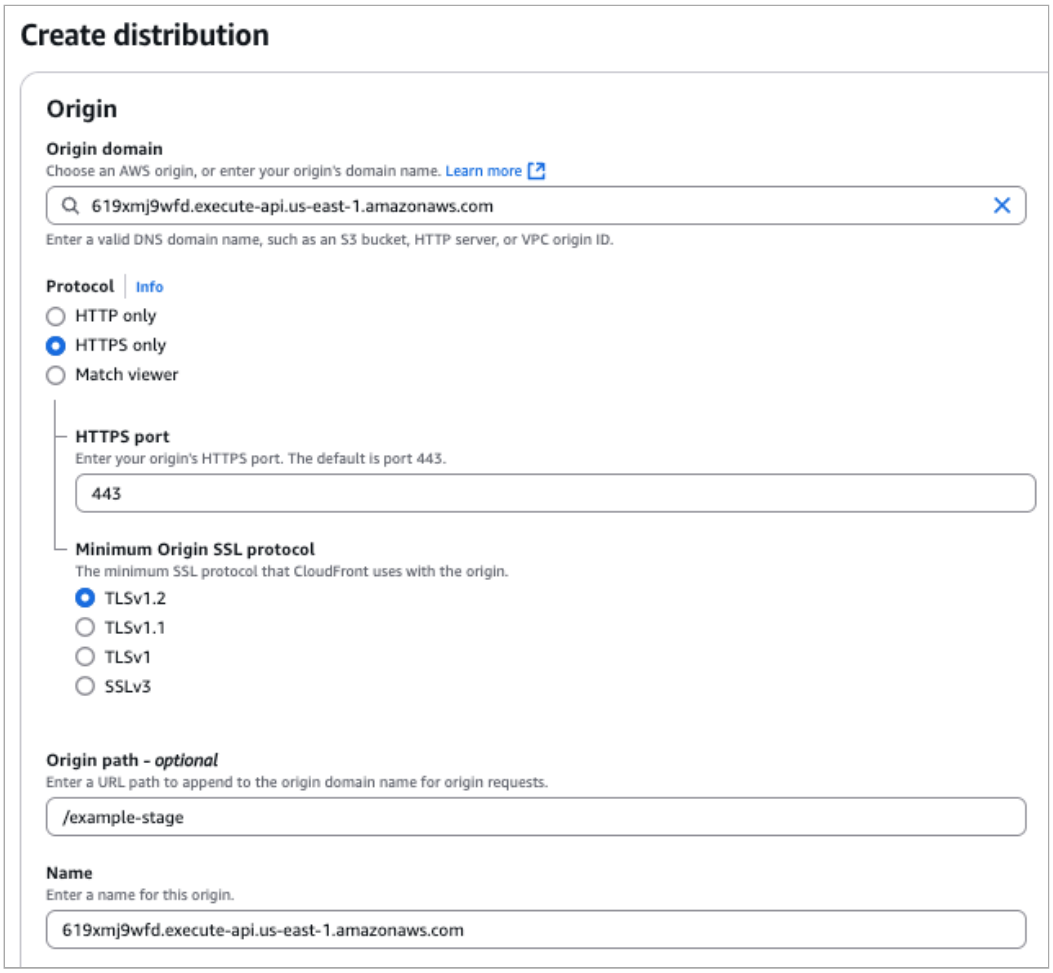
Configuring a CloudFront distribution

Create and configure a CloudFront distribution to define the origin servers from which CloudFront retrieves your API resources.

Steps

1. Open the AWS CloudFront console.
2. Click **Create distribution**.
3. Configure the origin settings:
    1. In the **Origin domain** field, paste the API invoke URL you copied earlier.

       The **Name** field is automatically populated with the origin domain name, and the **Origin path** field is automatically populated with the stage path.

    2. Under **Protocol**, click **HTTPS only**, and leave the default settings.
4. In the **Default cache behavior** section, configure caching to meet your business needs.
5. In the **Web Application Firewall (WAF)** section, click either **Enable security protections** or **Do not enable security protections**.

Copyright © 2025 Ping Identity Corporation

6. (Optional) To make it easier to find your CloudFront distribution later, add a **Description**.
7. (Optional) To enable CloudWatch logging for your CloudFront distribution, in the **Standard logging** section, click **On**, and then configure the settings to meet your business needs.
8. Click **Create distribution**.

> **Note**
>
> It might take a few minutes to deploy the CloudFront distribution. You can check the deployment status in the **Details** section of the distribution, under **Last modified**.

Configuring a Lambda@Edge function

Create a Lambda@Edge function and associate it with a CloudFront distribution.

Learn more about Lambda@Edge functions in Customize at the edge with Lambda@Edge in the CloudFront documentation.

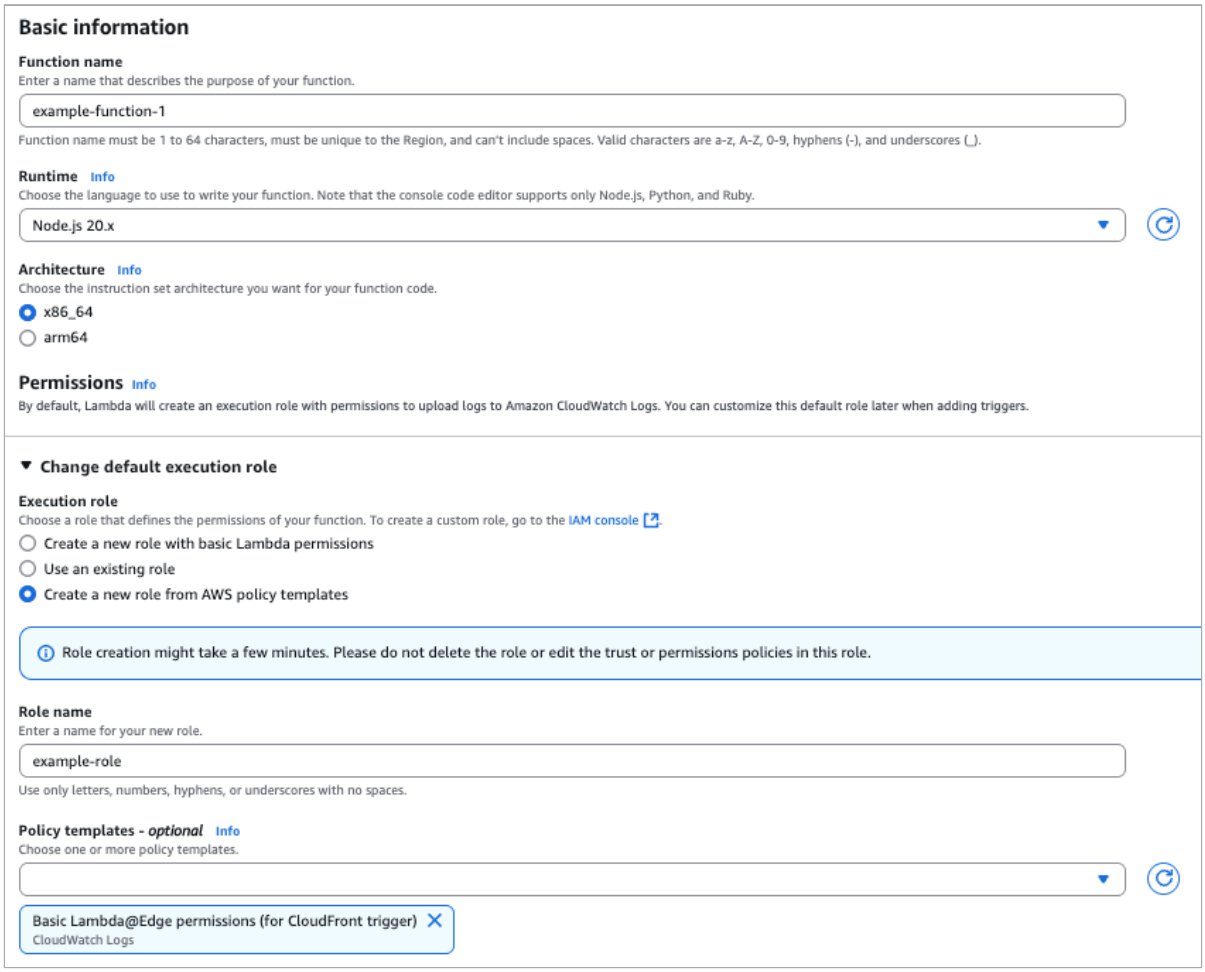
Steps

1. Create a Lambda function:
    1. Open the AWS Lambda console.

    > **Important**
    >
    > Make sure you're in the US East (N. Virginia) AWS region. You must be in this region to create Lambda@Edge functions.

    2. Click **Create function**.
    3. Click **Author from scratch**.
    4. In the **Basic information** section, in the **Function name** field, enter a unique name for the Lambda function.

Copyright © 2025 Ping Identity Corporation



5. In the **Runtime** list, select **Node.js 20.x**.
6. In the **Architecture** section, click **x86_64**.
7. Click **Change default execution role** to expand execution role settings.
8. Under **Execution role**, click **Create a new role from AWS policy templates**.
9. In the **Role name** field, enter a unique name for the execution role.
10. In the **Policy templates** search bar, enter `CloudFront` to filter the search results, and then select **Basic Lambda@Edge permissions (for CloudFront trigger)**.

    This policy template allows CloudFront to execute the Lambda function when a request matches the configured event trigger.
11. Click **Create function**.

    Result:

    A page opens for your new Lambda function.

2. Update the Lambda function source code:

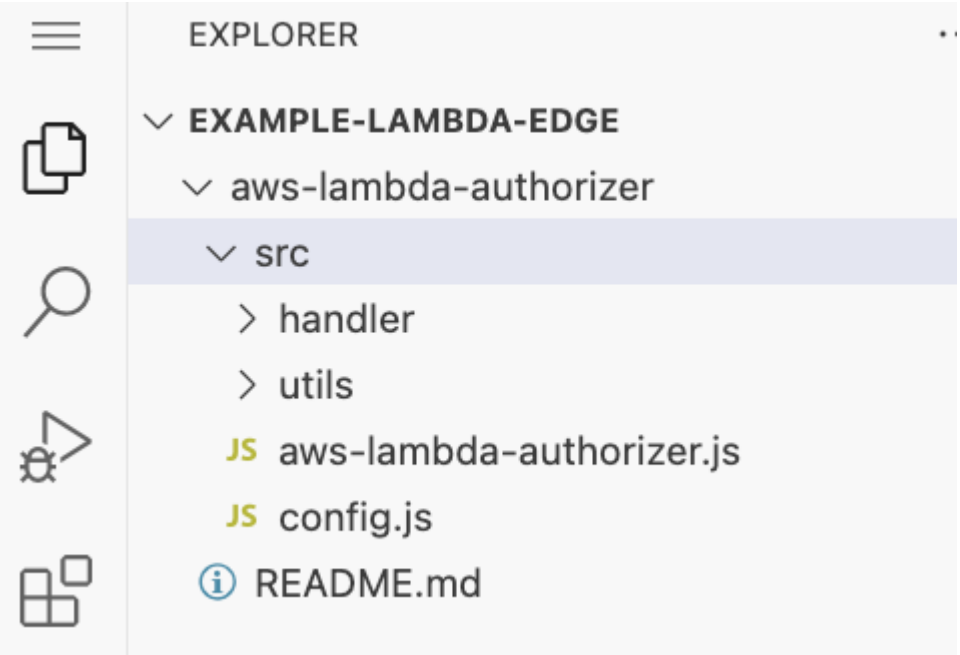
    1. Click the **Code** tab.

Copyright © 2025 Ping Identity Corporation

2. In the **Code source** section, in the **Upload from** list, select **.zip file**.
3. In the **Upload a .zip file** modal, click **Upload**, and then select the integration kit `.zip` archive in your local directory.
4. Click **Save**.

   Result:

   The Lambda source code should have these files uploaded:



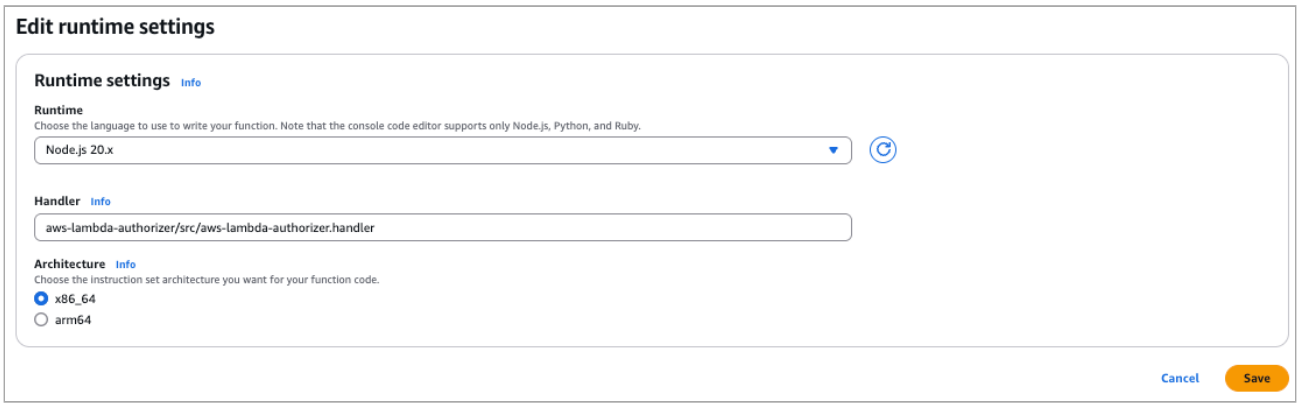
5. In the code source file explorer, expand the `src` folder, and then open the `config.js` file.
6. Update the following values:
   - `SECRET_HEADER_VALUE` : The gateway credential you saved in Setting up PingOne Authorize for Amazon Web Services integration. This value must be a string.
   - `SERVICE_URL` : The service URL you saved in Setting up PingOne Authorize for Amazon Web Services integration. This value must be a string.
   - `IS_DEBUG_ENABLED` : The value is `true` or `false` depending on whether debugging is needed. This value must be a Boolean, not a string. Set this value to `false` in production environments.
   - `MAX_RETRIES` : Controls the number of connection retries that the integration kit performs when a PingOne Authorize request fails because of network errors or HTTP 5xx responses. The default is `1` .

   Lambda@Edge doesn't support the use of environment variables for setting these values.
7. Click **Deploy**.

3. Update the Lambda function handler:
   1. Scroll down to the **Runtime settings** section and click **Edit**.

Copyright © 2025 Ping Identity Corporation

2. In the **Handler** field, replace the existing value with `aws-lambda-authorizer/src/aws-lambda-authorizer.handler`.

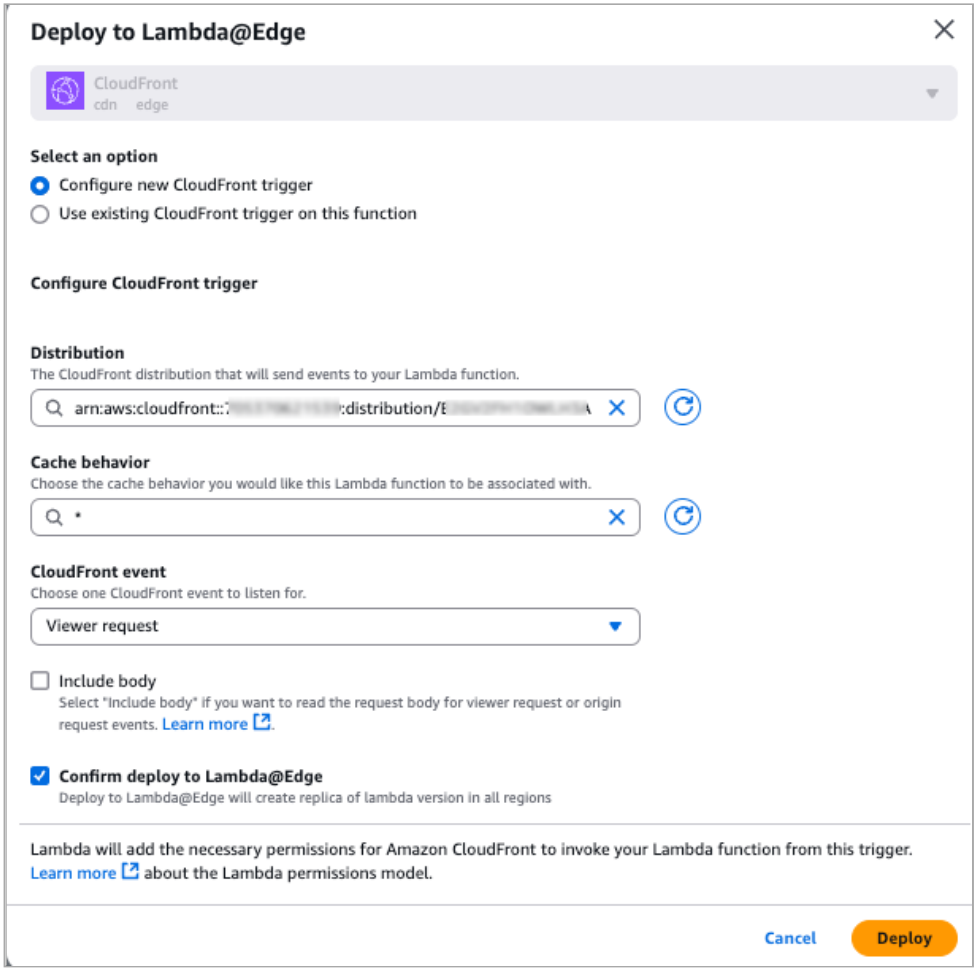


3. Click **Save**.

4. Deploy the Lambda function to Lambda@Edge:

   1. In the **Actions** list, select **Deploy to Lambda@Edge**.

   2. Click **Configure new CloudFront trigger**.



   3. In the **Distribution** list, select your CloudFront distribution.

Copyright © 2025 Ping Identity Corporation

> **Tip**
> If you added a description to your CloudFront distribution, you can enter this description to filter the search results.

4. In the **Cache behavior** list, select a cache behavior.
5. In the **CloudFront event** list, select **Viewer request**.
6. Select the **Confirm deploy to Lambda@Edge** checkbox.

5. Click **Deploy**.

   Result:

   Your Lambda@Edge function will now trigger with each viewer request made to the CloudFront distribution.

Next steps

Define API services to represent your APIs so that PingOne Authorize can help CloudFront enforce access control. Learn more in Defining your API in PingOne Authorize

> **Important**
> If you're using CloudFront and Lambda@Edge to enforce access control, the API service definition must use PingOne SSO as the directory and token source.

Troubleshooting

To track and debug issues related to your Lambda@Edge function and CloudFront distribution, you can configure Amazon CloudWatch logging. Learn more in Logging and monitoring in the CloudFront documentation.

Integrating PingOne Authorize with Apigee

Ping Identity's shared flow for Apigee extends Apigee's authorization capabilities through an external policy evaluation service.

Integration with Apigee allows centralized management of API access control and application protection in PingOne Authorize while delegating enforcement to Apigee. Learn more about how this integration kit interacts with PingOne Authorize in How API Access Management works.

Install and configure the integration kit in Apigee to enable management of access control rules in PingOne Authorize.

To configure the integration kit:

- Set up an API gateway in PingOne Authorize.
- Configure the PingAuth shared flow bundle in Apigee
- Attach the PingAuth shared flow on API proxies

Copyright © 2025 Ping Identity Corporation

Setting up PingOne Authorize for Apigee integration

To allow Apigee to use PingOne Authorize as an external runtime authorization policy service, set up an API gateway in PingOne that represents Apigee.

Before you begin

Add PingOne Authorize to your PingOne environment. For details, see Getting started with PingOne Authorize.

About this task

Prepare PingOne Authorize to authenticate authorization requests from Apigee.

Steps

1. In PingOne, go to **Authorization** > **API Gateways**.
2. Copy the **Service URL** and save it somewhere convenient for later use.
3. To add a gateway, click the **+** icon next to **API Gateways**.
4. Enter a name for the gateway, such as `Apigee`. Click **Save**.
5. Click the **+** icon next to **Credentials**, copy the credential, and save it for later use.
6. Click **Done**.

Configuring Apigee for PingOne Authorize integration

Install the PingAuth shared flow bundle in Apigee and configure it to integrate with PingOne Authorize.

Before you begin

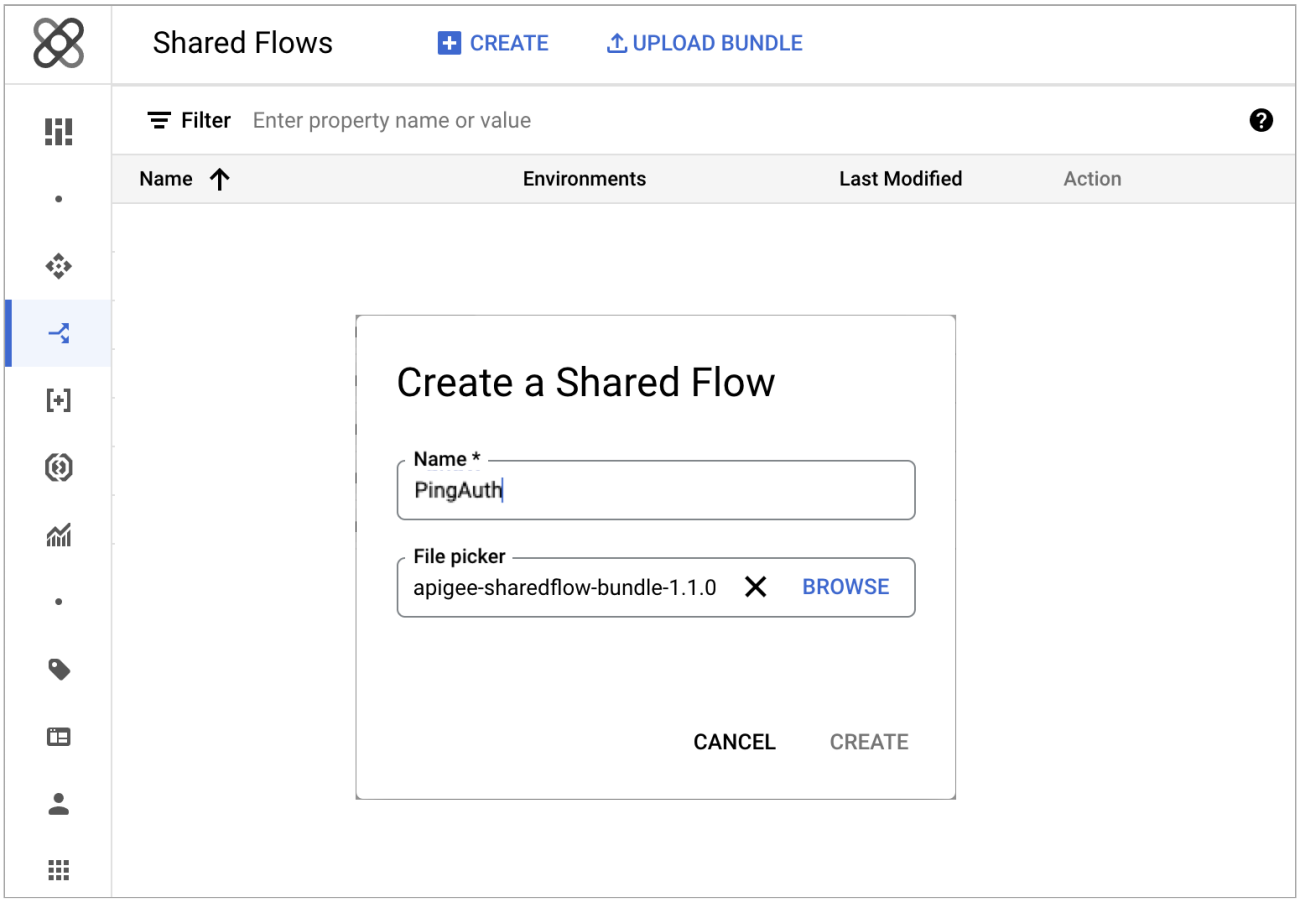
Ensure you have:

- A supported Apigee environment. The Ping Identity shared flow for Apigee supports Apigee Edge, Apigee Private Cloud, and Apigee X.
- The PingAuth Shared Flow Bundle `.zip` archive. Download the integration kit for Apigee from the Ping Identity Integration Directory.

Steps

1. Upload the shared flow bundle:
    1. In Apigee, go to **Develop → Shared Flows** and do one of the following:
        - In Apigee X, click **Upload Bundle**.
        - In Apigee Edge or Apigee Private Cloud, click **+Shared Flow**, and then click **Upload Bundle**.
    2. For the shared flow **Name**, enter `PingAuth`.
    3. In **File Picker**, browse to the PingAuth shared flow bundle zip file and select it.

Copyright © 2025 Ping Identity Corporation



4. Click **Create**.

2. In Apigee X, configure the connection to PingOne Authorize.

> **Note**
>
> Skip this step if you are using Apigee Edge or Apigee Private Cloud.
> Apigee X doesn't currently support managing the configuration values stored in key value maps in the Apigee interface. You must add these configuration values to the key value map policy. The key value map is created and the configuration values are added the first time the PingAuth shared flow is executed at runtime.

1. To access the PingAuth shared flow, go to **Develop → Shared Flows → PingAuth**.
2. Click the **Develop** tab and examine **Revisions** to make sure you are on the latest revision.
3. In the **Policies** panel on the left, click the **Load KVM Config** policy.
4. In the policy editor panel, remove the comment lines above and below the `InitialEntries` element.
5. Edit values for `service_host_port` and `service_base_path` to match the Service URL from the API Gateway you added in PingOne Authorize.

   For example, for Service URL:

   ```
   https://http-access-api.pingone.com/v1/environments/78b2c5b5-dead-f00d-beef-9f0ca3ae4486
   ```

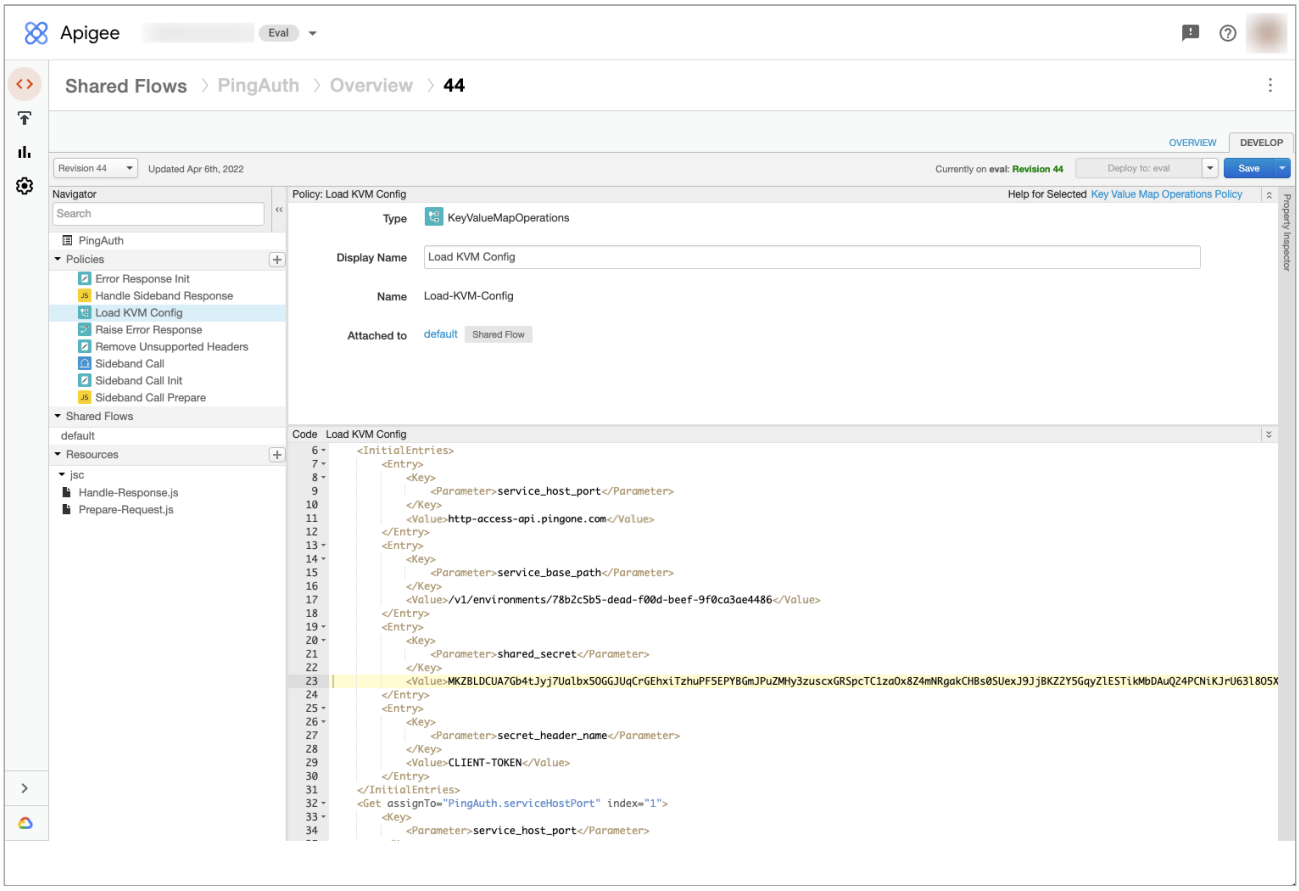
Copyright © 2025 Ping Identity Corporation

The `service_host_port` is `http-access-api.pingone.com`.

The `service_base_path` is `/v1/environments/78b2c5b5-dead-f00d-beef-9f0ca3ae4486`.

6. Edit the value for `shared_secret` to match the API Gateway credential you created in PingOne Authorize.

7. Click **Save**.



3. In Apigee Edge or Apigee Private Cloud, configure the connection to PingOne Authorize.

   Apigee Edge stores environment-specific configuration values in key value maps. This allows you to use the same policies across multiple deployment environments without any changes to the policies.

   1. Go to **Environment → Key Value Maps** and click **+Key Value Map**.

   2. Edit the key value map and click **Add Entry**.

   3. Add values using the key names `service_host_port` and `service_base_path` that match the Service URL from the API Gateway you added in PingOne Authorize.

      For example, for Service URL:

      ```
      https://http-access-api.pingone.com/v1/environments/78b2c5b5-dead-f00d-beef-9f0ca3ae4486
      ```

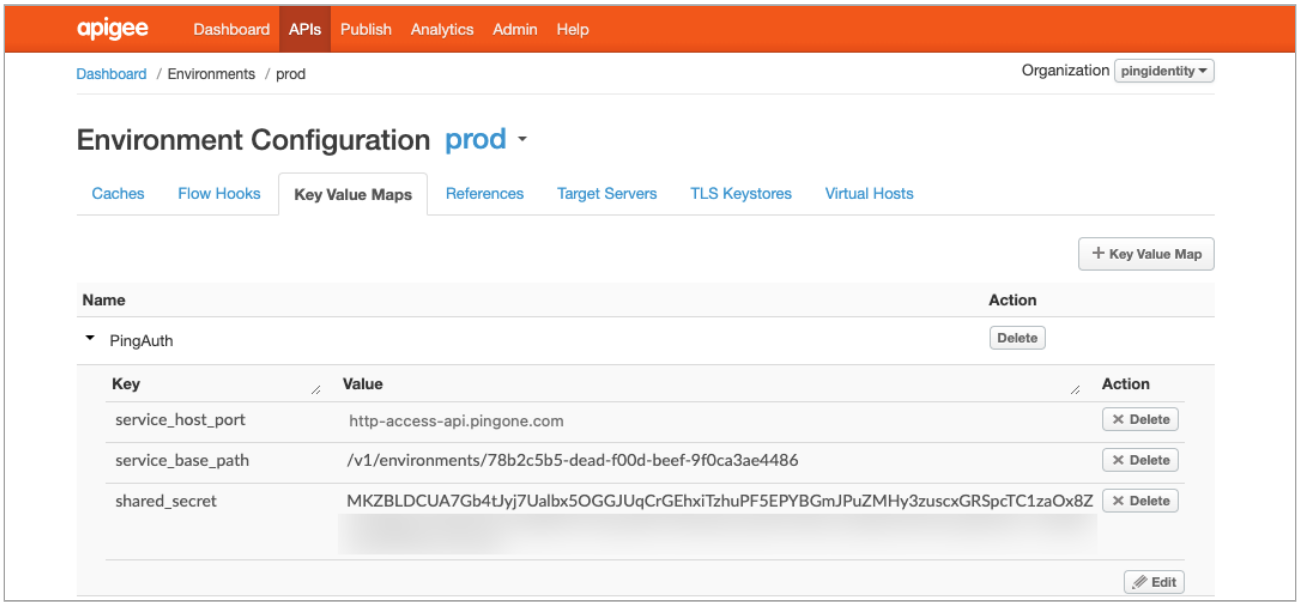
      The `service_host_port` is `http-access-api.pingone.com`.

      The `service_base_path` is `/v1/environments/78b2c5b5-dead-f00d-beef-9f0ca3ae4486`.

Copyright © 2025 Ping Identity Corporation

4. Add a value using the key name `shared_secret` that matches the API Gateway credential you created in PingOne Authorize.

5. Click **Save**.



4. Deploy the shared flow:

   1. To access the PingAuth shared flow, go to **Develop → Shared Flows → PingAuth**.

   2. Deploy the most recent revision of the shared flow to your environment.

Attaching the PingAuth shared flow to API proxies in Apigee

Configure the PingAuth shared flow on the API proxies where you want to use PingOne Authorize as the external authorization policy run-time service.

Steps

1. Add a Flow Callout policy:

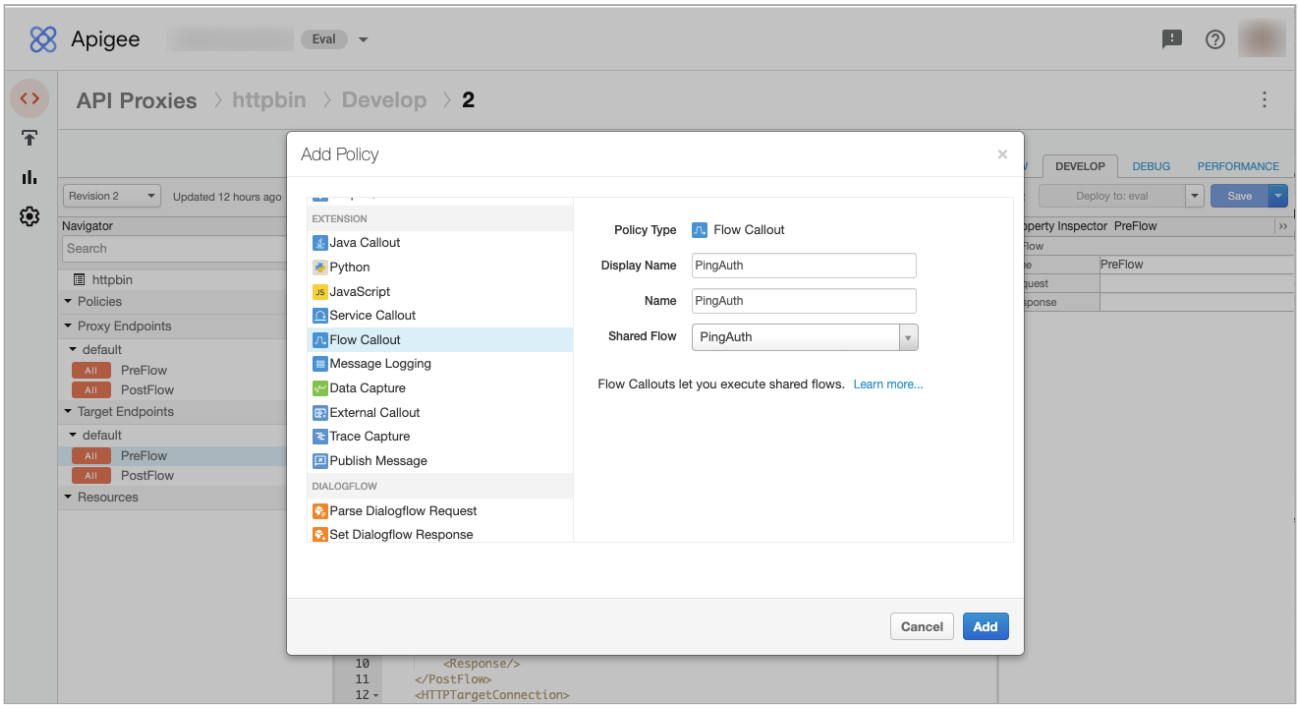
   1. In **Develop → API Proxies**, go to one of your APIs and click the **Develop** tab. Make sure you are on the latest revision of the proxy.

   2. In the left pane, for **Policies**, click the **+** icon to add a policy.

   3. In the **Add Policy** window, select the **Flow Callout** policy in the left pane, and then in the **Shared Flow** list, select **PingAuth**.

   4. Click **Add**.

Copyright © 2025 Ping Identity Corporation

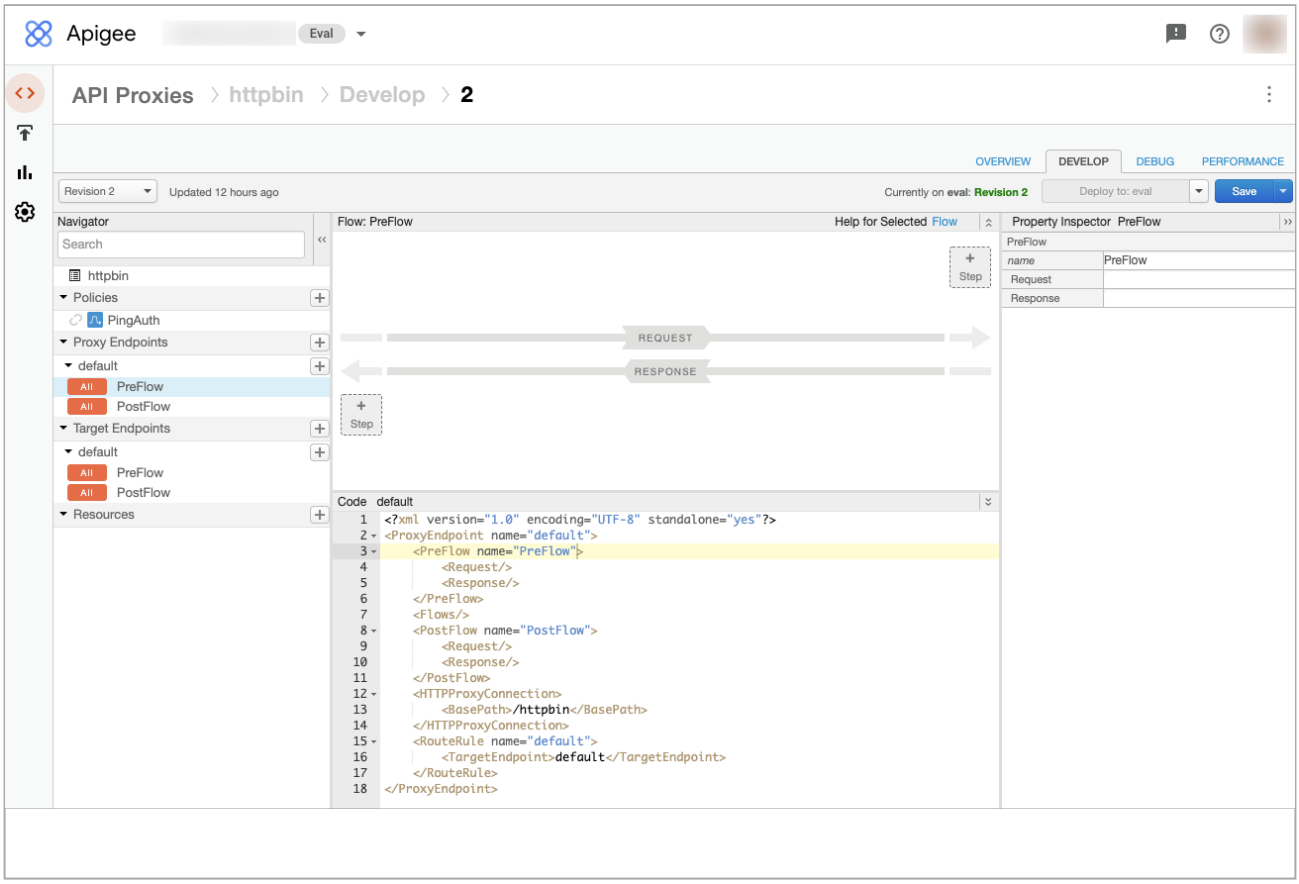


2. Attach the Flow Callout policy to flows.

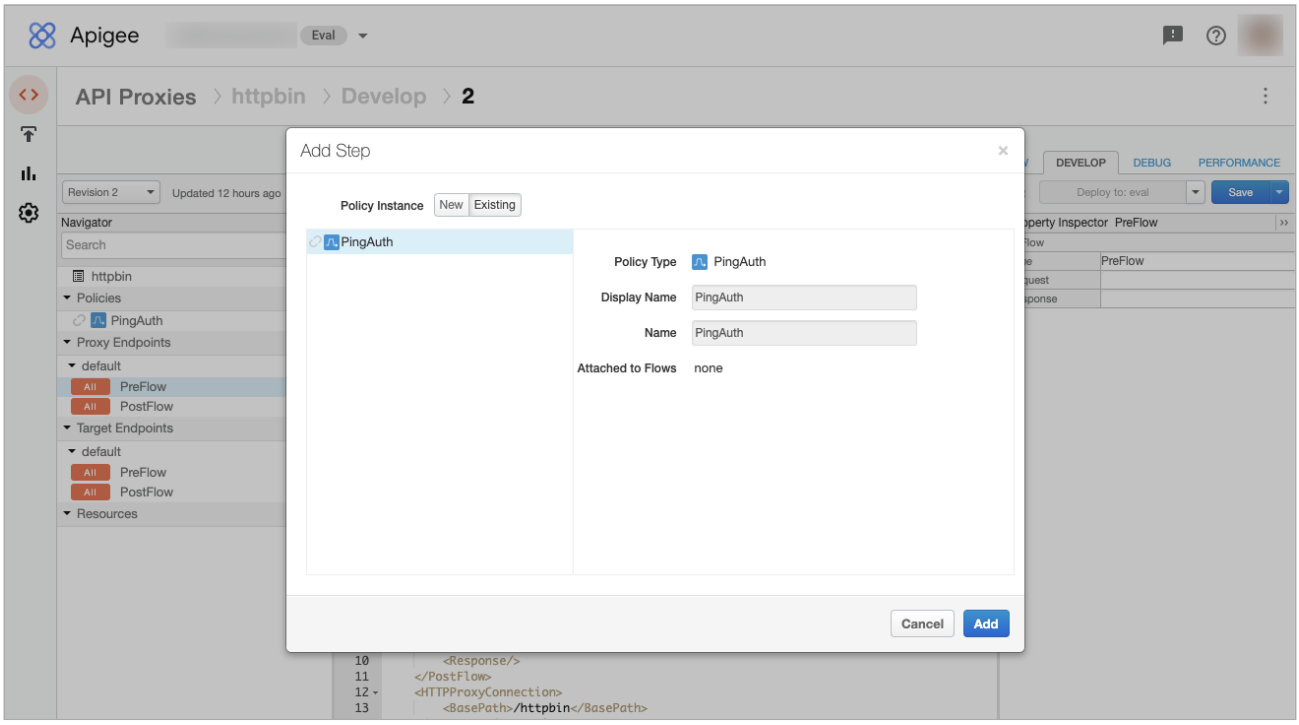
   Because PingOne Authorize is providing authentication and authorization that occurs before most other policies execute, integrate it in the preflow of the request to the proxy endpoint. For information about other ways to integrate PingOne Authorize, see Controlling how a proxy executes with flows in the Apigee documentation.

   1. In the left pane, for the **Proxy Endpoint**, click **PreFlow**, and then click **+ Step** to add a flow step to the **Request**.

Copyright © 2025 Ping Identity Corporation



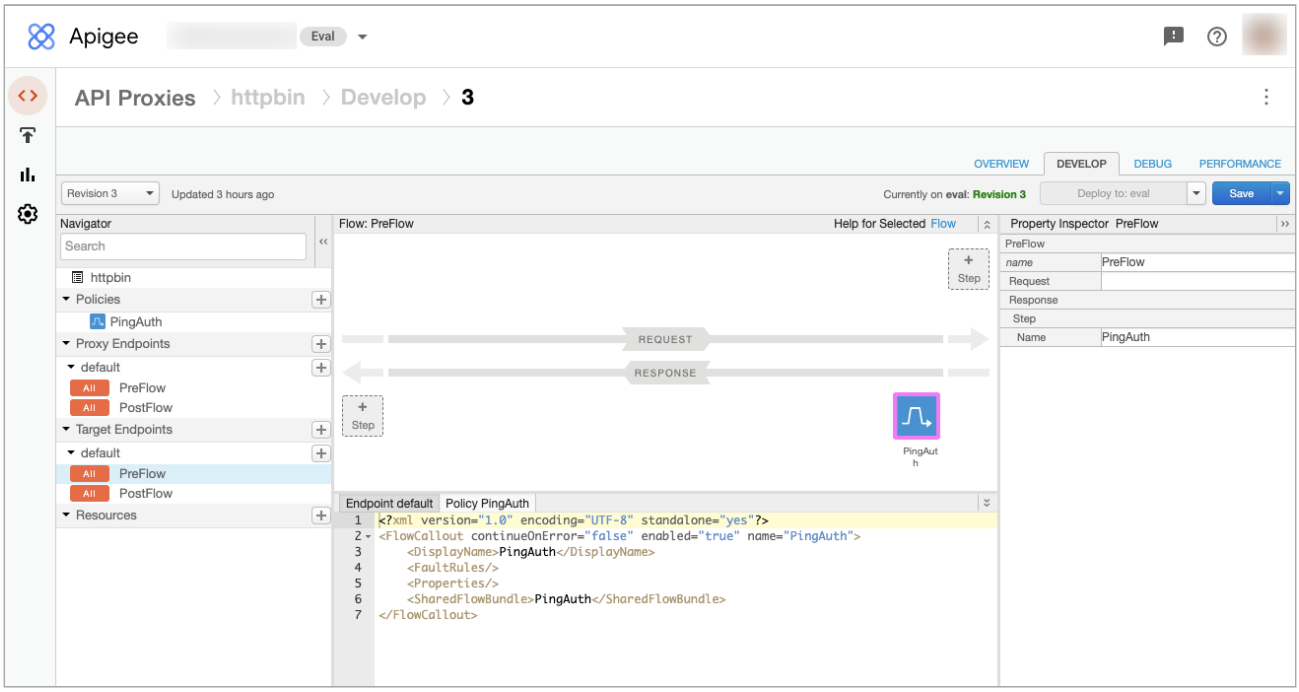
2. On the **Existing** tab, select the **PingAuth** Flow Callout policy, and then click **Add**.



3. In the left pane, for the **Target Endpoint**, click **PreFlow**, and then click **+ Step** to add a flow step to the **Response** flow.

4. On the **Existing** tab, select the **PingAuth** Flow Callout policy, and then click **Add**.

   This gives PingOne Authorize an early opportunity to process the API response from the target API before it's processed by Apigee.



3. Save and deploy the updated proxy.

Next steps

Define API services to represent your APIs so that PingOne Authorize can help your API gateway enforce access control. For more information, see Defining your API in PingOne Authorize.

Integrating PingOne Authorize with Kong Gateway

Ping Identity's integration kit for Kong extends Kong's authorization capabilities through an external policy evaluation service.

Integration with Kong Gateway allows centralized management of API access control and application protection in PingOne Authorize while delegating enforcement to Kong Gateway. Learn more about how traffic flows through Kong Gateway and PingOne Authorize in How API Access Management works.

Configure the integration kit in Kong Gateway to enable management of access control rules in PingOne Authorize. The integration kit works with Kong Gateway or Kong Konnect.

Note

- The `ping-auth` plugin has been tested with Kong Gateway 2.8.
- Support for Kong Konnect is available in version 1.0.8 and later of the `ping-auth` plugin.

Copyright © 2025 Ping Identity Corporation

To configure the integration kit:

1. Set up an API gateway in PingOne Authorize.
2. Configure the ping-auth plugin in Kong Gateway.

Important

The following are important usage notes for the Kong Gateway integration kit:

Transfer-encoding

A Kong limitation currently prevents the `ping-auth` plugin from supporting the `Transfer-Encoding` header, regardless of the value.

Logging limit

Because of Kong's log level limit, log messages are limited to 2048 bytes by default, which is less than the size of many requests and responses. Learn more in the OpenResty Reference documentation.

Request body limit

The `ping-auth` plugin might not receive client request bodies that exceed Kong's default buffer limit of 8 KB. If the request body is missing, check the `nginx_http_client_body_buffer_size` setting in `kong.conf` and increase its value to accommodate your maximum expected request body size. Learn more in nginx_http_client_body_buffer_size in the Kong documentation.

Learn more about Kong in the Kong Gateway documentation.

Setting up PingOne Authorize for Kong Gateway integration

To allow Kong Gateway to use PingOne Authorize as an external runtime authorization policy service, set up an API gateway in PingOne that represents Kong Gateway.

Before you begin

Add PingOne Authorize to your PingOne environment. Learn more in Getting started with PingOne Authorize.

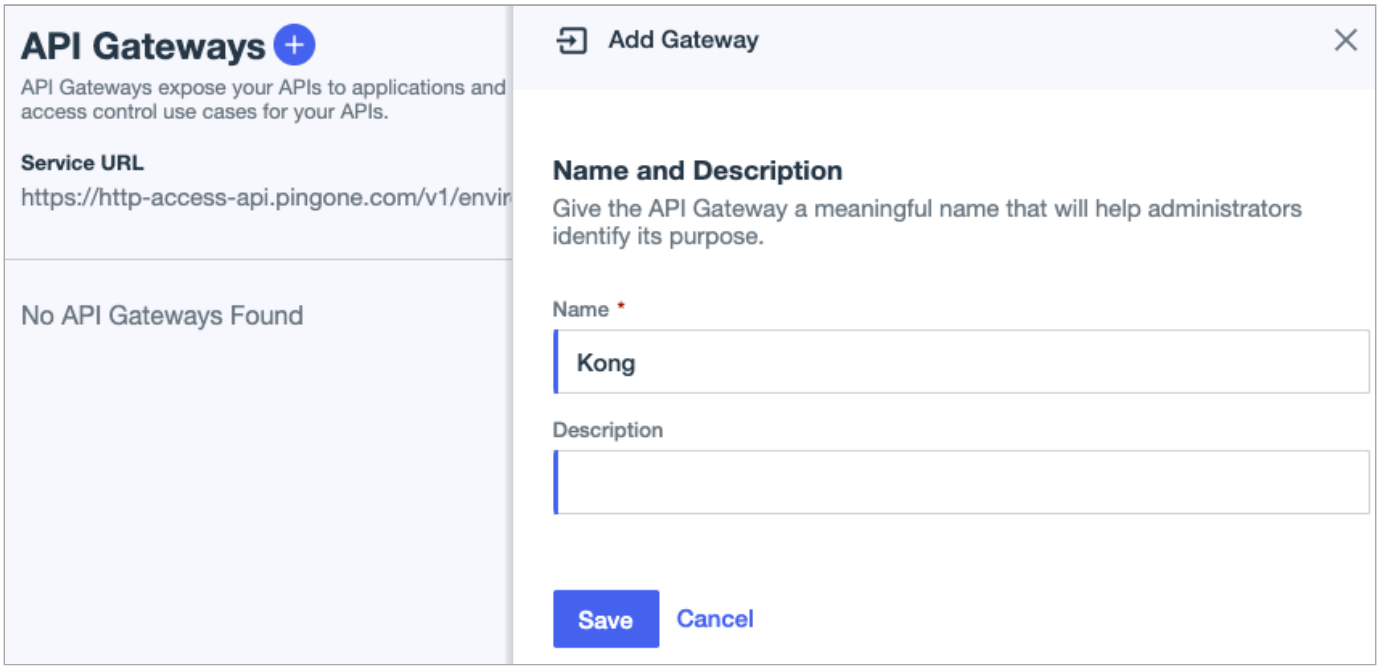
About this task

Prepare PingOne Authorize to authenticate authorization requests from Kong Gateway.

Steps

1. In the PingOne admin console, go to **Authorization** > **API Gateways**.
2. Copy the **Service URL** and save it somewhere convenient for later use.
3. To add a gateway, click the **+** icon next to **API Gateways**.
4. Enter a name for the gateway, such as `Kong`. Click **Save**.

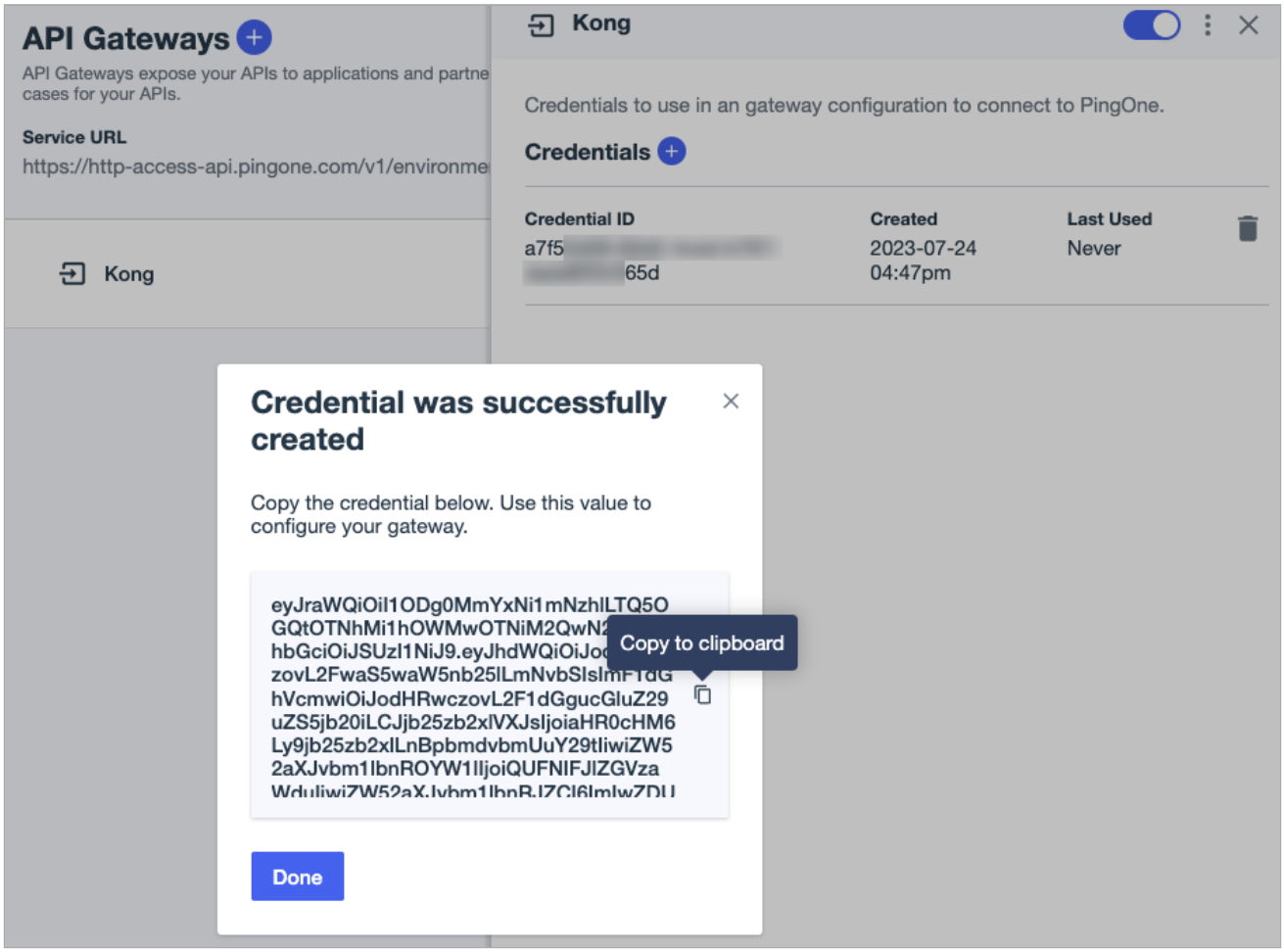
Copyright © 2025 Ping Identity Corporation



5. Click the **+** icon next to **Credentials**, copy the credential, and save it for later use.

> **Important**
>
> The gateway credential is the shared secret that authenticates the `ping-auth` plugin to PingOne Authorize. Version 1.2.0 of the plugin supports referenceable secrets. For security reasons, store the gateway credential in a vault supported by Kong. Learn more in Secrets Management and Environment Variables Vault in the Kong documentation.

Copyright © 2025 Ping Identity Corporation



6. Click **Done**.

Configuring Kong Gateway for PingOne Authorize integration

To integrate PingOne Authorize with Kong Gateway, install and configure the integration kit. You'll use LuaRocks to install the integration kit.

Steps

1. Run the following command to install the plugin:

   ```
   luarocks install kong-plugin-ping-auth
   ```

   Learn more in the Kong Gateway plugin installation documentation.

2. After installation, load the plugin into Kong by editing the `plugins = bundled,ping-auth` property in the `kong.conf` file.

   Alternatively, you can use the equivalent environment variable to set this property: `KONG_PLUGINS = bundled,ping-auth`.

3. Restart Kong Gateway to apply the plugin.

Copyright © 2025 Ping Identity Corporation

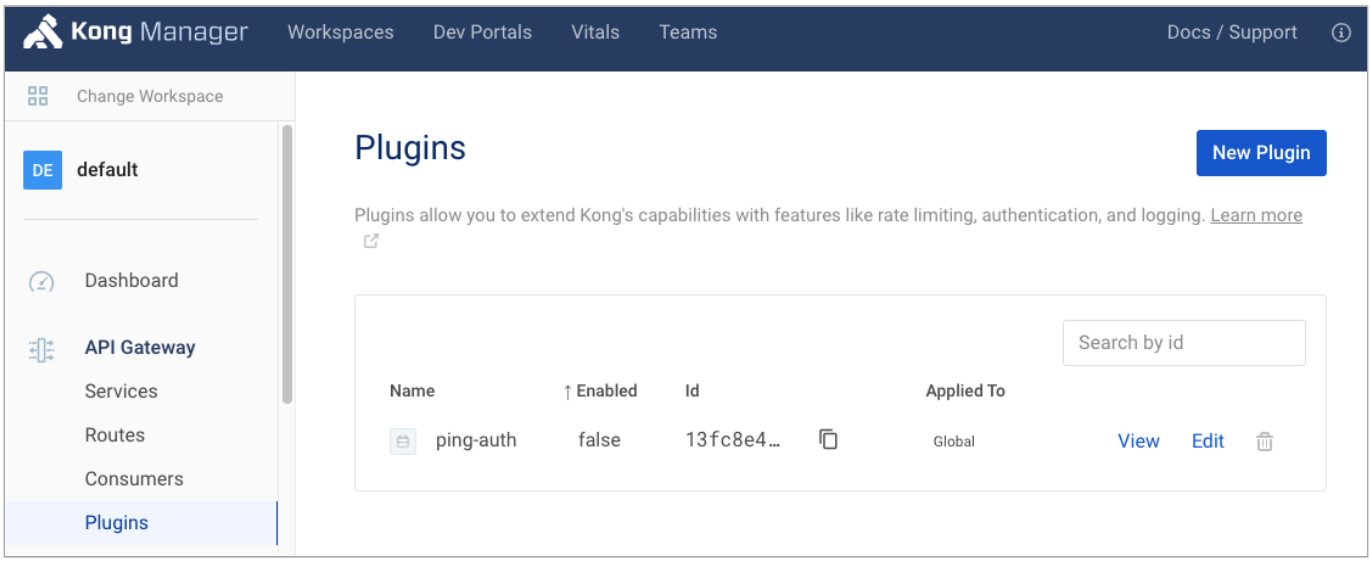
4. To verify that Kong loads the plugin successfully, check for the debug-level message `Loading plugin: ping-auth` in Kong's `error.log` file.

5. Use the Kong Gateway UI or API to complete the configuration.

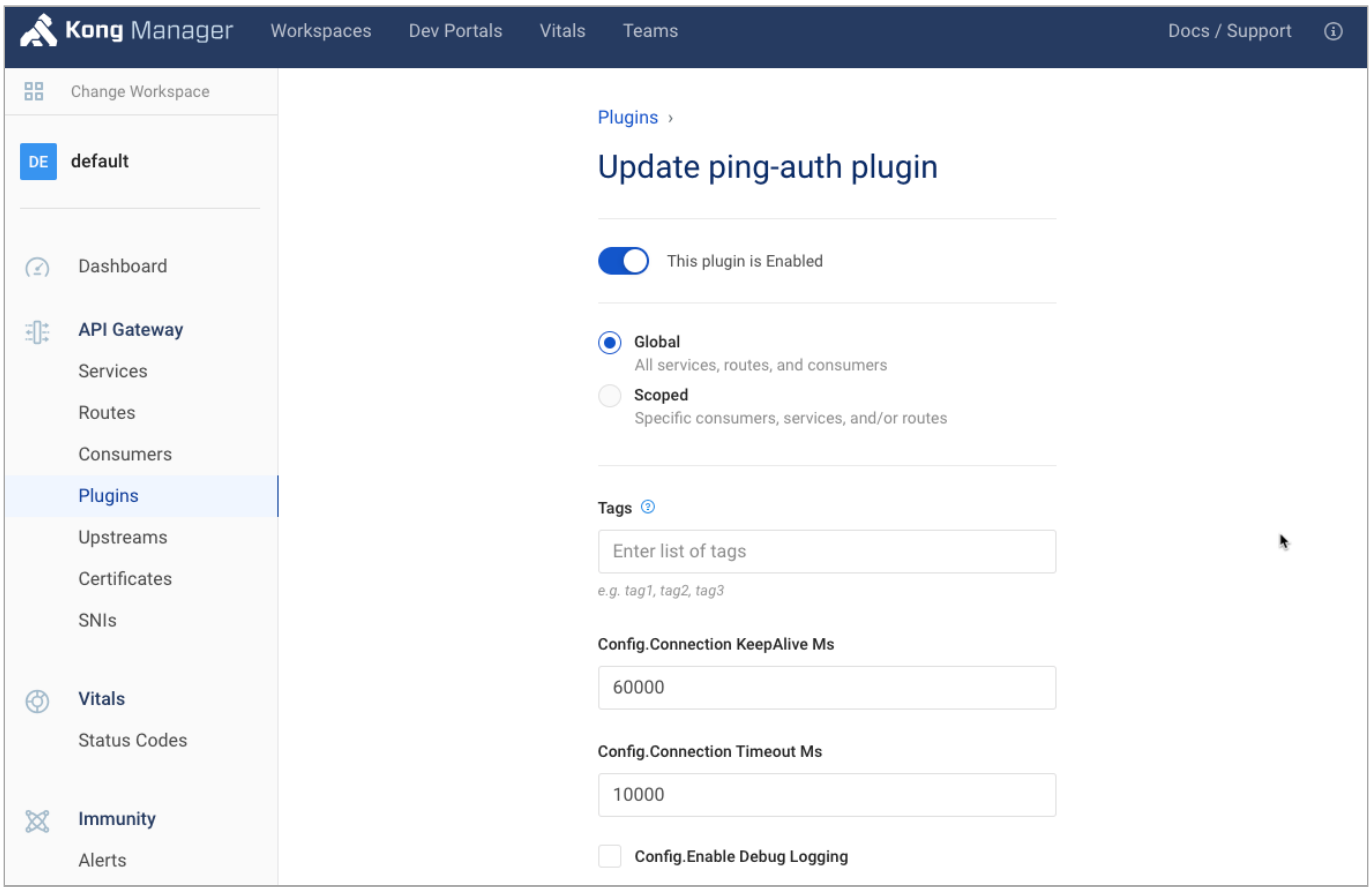
Copyright © 2025 Ping Identity Corporation

Kong Gateway UI

- *In Kong Manager, select the **default** workspace, and then click **Plugins**.*



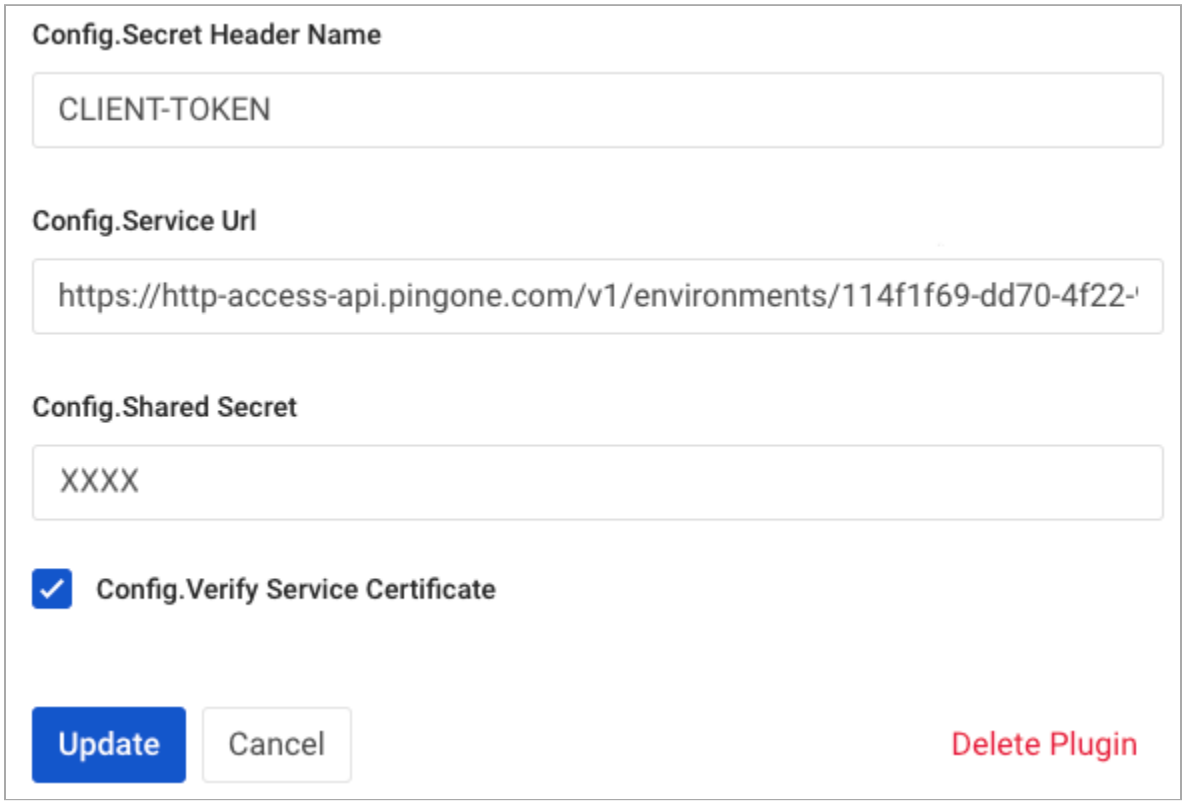
- *On the `ping-auth` line, click **Edit**.*
- *On the **Update ping-auth plugin** page, click the toggle to enable the plugin.*



Copyright © 2025 Ping Identity Corporation

- *(Optional) To enable the plugin for specific consumers, services, or routes, click **Scoped** and then enter **Service**, **Route**, and **Consumer** information as necessary.*
- *Paste the **Service URL** from the API gateway you added in PingOne Authorize into the **Config.Service Url** field.*

  This is the full URL of the Ping Identity policy provider.



- *In the **Config.Shared Secret** field, enter the API gateway credential you created in PingOne Authorize.*

> **Important**
>
> *The gateway credential is the shared secret that authenticates the `ping-auth` plugin to PingOne Authorize. Version 1.2.0 of the plugin supports referenceable secrets. For security reasons, store the gateway credential in a vault supported by Kong. Learn more in Secrets Management and Environment Variables Vault in the Kong documentation.*

- *(Optional) Configure additional options in Kong Manager:*

Option	*API Field Name*	*Description*
Config.Connection KeepAlive Ms	`connection_keepAlive_ms`	*The duration to keep the connection alive for reuse. The default is `6000` milliseconds.*
Config.Connection Timeout Ms	`connection_timeout_ms`	*The duration to wait before the connection times out. The default is `10000` milliseconds.*

Copyright © 2025 Ping Identity Corporation

Option	*API Field Name*	*Description*
Config.Enable Debug Logging	`enable_debug_logging`	*Controls if requests and responses are logged at the debug level. The default is* `false`*.* *For log messages to show in the* `error.log`*, you must set* `log_level = debug` *in* `kong.conf`*.*
Config.Verify Service Certificate	`verify_service_certificate`	*Controls whether the service certificate is verified. This is intended for testing purposes, and the default is* `true`*.*

- *Click* ***Update****, and then click* ***Update Plugin****.*

Copyright © 2025 Ping Identity Corporation

Kong Gateway API

- *Include the following JSON object in a POST request to https://<KONG_URL>/plugins:*

```
{
  "name": "ping-auth",
  "enabled": true,
  "config": {
    "service_url": "<service URL>",
    "shared_secret": "<shared secret>",
    "secret_header_name": "<shared secret header name>"
  }
}
```

  - `service_url`: *The **Service URL** from the API gateway you added in PingOne Authorize.*
  - `shared_secret`: *The API gateway credential you created in PingOne Authorize.*

    > **Important**
    >
    > *The gateway credential is the shared secret that authenticates the* `ping-auth` *plugin to PingOne Authorize. Version 1.2.0 of the plugin supports referenceable secrets. For security reasons, store the gateway credential in a vault supported by Kong. Learn more in Secrets Management and Environment Variables Vault in the Kong documentation.*

  - `secret_header_name`: *The name of the header in which the shared secret is provided. The default header name is* `CLIENT-TOKEN`.

    Learn more in the Kong Gateway Admin API documentation.

- *(Optional) Configure additional options:*

Option	*API Field Name*	*Description*
Config.Connection KeepAlive Ms	`connection_keepAlive_ms`	*The duration to keep the connection alive for reuse. The default is* `6000` *milliseconds.*
Config.Connection Timeout Ms	`connection_timeout_ms`	*The duration to wait before the connection times out. The default is* `10000` *milliseconds.*
Config.Enable Debug Logging	`enable_debug_logging`	*Controls if requests and responses are logged at the debug level. The default is* `false`. *For log messages to show in the* `error.log`*, you must set* `log_level = debug` *in* `kong.conf`.

Copyright © 2025 Ping Identity Corporation

Option	*API Field Name*	*Description*
Config.Verify Service Certificate	`verify_service_certificate`	*Controls whether the service certificate is verified. This is intended for testing purposes, and the default is* `true`.

Result

Kong Gateway is now configured to work with PingOne Authorize.

Next steps

Define a managed API service that represents your API so that PingOne Authorize can help your API gateway enforce access control. Learn more in Defining your API in PingOne Authorize.

Troubleshooting Kong Gateway integration with PingOne Authorize

The following resources can help you solve issues with the Kong Gateway integration for PingOne Authorize.

Solutions

API client HTTP 5xx errors

Likely cause

Kong Gateway might return `HTTP 502` when there is misconfiguration or miscommunication between the Ping Identity plugin for Kong Gateway and the HTTP Access Policy Service in PingOne Authorize.

How to troubleshoot

The plugin for Kong Gateway logs warning messages to the Kong Gateway error log when it encounters problems communicating with PingOne Authorize. For more information, see Troubleshooting resources.

Details

If the shared secret value doesn't match the API gateway credential in PingOne Authorize, the Kong error log message might indicate that the plugin received an `HTTP 401` error from PingOne Authorize, which is translated to a 5xx error sent to the API client. For example:

```
2022/03/28 16:19:49 [warn] 78#0: *85187 [lua] network_handler.lua:145: is_failed_request(): [ping-
auth] Sideband request denied with status code 401: The Gateway Token is invalid
```

Copyright © 2025 Ping Identity Corporation

If the service URL value doesn't match the service URL in PingOne Authorize, the Kong error log message might indicate that the plugin received an invalid response from the server. For example:

```
2022/03/28 16:19:49 [error] 78#0: *90929 [lua] access.lua:114: handle_response(): [ping-auth] Unable
to parse JSON body returned from policy provider. Error: Expected value but found T_END at character
1
```

If the request body exceeds Kong's default buffer size limit of 8 KB, the Kong error log message might indicate that the plugin received an invalid response from the upstream server. For example:

```
"code" : "Bad Request",
"message" : "Missing expected request body."
```

How to fix

Check the settings for **Shared Secret** and **Service URL** to ensure that they match your PingOne Authorize environment. If necessary, go to **Authorization > API Gateways** and generate a new credential, then copy the value to the shared secret setting in the Kong Gateway plugin configuration.

If the request body is missing, check the `nginx_http_client_body_buffer_size` setting in `kong.conf` and increase its value to accommodate your maximum expected request body size. Learn more in nginx_http_client_body_buffer_size.

API client HTTP 4xx errors

Likely causes

The API gateway might return 4xx errors to API clients in these situations:

- PingOne cannot match an API client's request to any of the Base URLs configured for an API service.
- The API client's request cannot be authenticated or doesn't satisfy basic access control checks for an API service.
- The API client's request doesn't satisfy access control rules configured for the API service or its API Operations in PingOne Authorize.

How to troubleshoot

Learn more about troubleshooting in Viewing API Access Management events in your PingOne environment audit log.

Troubleshooting resources

Enabling error logging in Kong Gateway

1. To view error log messages, configure Kong error logging.

   For more information, see the Kong Gateway Logging Reference documentation.

   For example, in a Docker environment, you can use the environment variable `KONG_PROXY_ERROR_LOG=/dev/stderr` to send the error log to the container console. This is the default setting in the API Access Management tutorials environment.

Copyright © 2025 Ping Identity Corporation

2. View the Kong Gateway error log.

   For example, in Docker:

```
docker-compose logs kong --follow
```

Enabling debug logging for the Kong Gateway plugin

Ping Identity Support might ask you to enable debug logging for the Kong Gateway integration kit. Changing these settings logs the full authorization request and response between the plugin in Kong Gateway and PingOne Authorize.

> **Warning**
> This could log sensitive and personally identifiable information (PII). Enable debug logging only when troubleshooting and disable it afterward.

1. Enable error logging in Kong Gateway. See step 1 in Enabling error logging in Kong Gateway.
2. To view debug messages, configure Kong error log verbosity.

   For more information, see the Kong Gateway Logging Reference documentation.

   For example, in a Docker environment, you can use the environment variable `KONG_LOG_LEVEL=debug` to set the verbosity.
3. To enable debug logging, edit settings for the `ping-auth` plugin and select the **Config.Enable Debug Logging** check box.
4. View the Kong Gateway error log.

   For example, in Docker:

```
docker-compose logs kong --follow
```

5. Look for messages that contain `ping-auth`.

   For example:

```
[ping-auth] Sending sideband request to policy provider
```

Integrating PingOne Authorize with Kong Konnect

Ping Identity's integration kit for Kong extends Kong's authorization capabilities through an external policy evaluation service.

Integration with Kong Konnect allows centralized management of API access control and application protection in PingOne Authorize while delegating enforcement to Kong Konnect. Learn more about how traffic flows through Kong Konnect and PingOne Authorize in How API Access Management works.

Configure the integration kit in Kong Konnect to enable management of access control rules in PingOne Authorize. The integration kit works with Kong Konnect or Kong Gateway.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> - For Kong Konnect integration, the `ping-auth` plugin has been tested with Kong Gateway 3.4.
> - Support for Kong Konnect is available in version 1.0.8 and later of the `ping-auth` plugin.

To configure the integration kit:

1. Set up an API gateway in PingOne Authorize.
2. Add the ping-auth plugin to your Kong Konnect control plane.
3. Upload ping-auth plugin files to each data plane node.
4. Configure the ping-auth plugin in Kong Konnect.

Learn more about adding custom Konnect plugins in the Kong Konnect documentation.

Setting up PingOne Authorize for Kong Konnect integration

To allow Kong Konnect to use PingOne Authorize as an external runtime authorization policy service, set up an API gateway in PingOne that represents Kong Konnect.

Before you begin

Add PingOne Authorize to your PingOne environment. Learn more in Getting started with PingOne Authorize.

About this task

Prepare PingOne Authorize to authenticate authorization requests from Kong Konnect.

Steps

1. In PingOne, go to **Authorization** > **API Gateways**.
2. Copy the **Service URL** value and save it for later use.

   You'll use this value to configure the `ping-auth` plugin in Kong Konnect.
3. To add a gateway, click the **+** icon next to **API Gateways**.
4. Enter a name for the gateway, such as `Kong Konnect`. Click **Save**.
5. Click the **+** icon next to **Credentials**, copy the credential, and save it for later use.

   > **Important**
   >
   > The gateway credential is the shared secret that authenticates the `ping-auth` plugin to PingOne Authorize. Version 1.2.0 of the plugin supports referenceable secrets. For security reasons, store the gateway credential in a vault supported by Kong. Learn more in Secrets Management in Konnect and Environment Variables Vault in the Kong documentation.
6. Click **Done**.

Copyright © 2025 Ping Identity Corporation

Configuring Kong Konnect for PingOne Authorize integration

For Kong Konnect to use PingOne Authorize as an external authorization policy runtime service, you must download, install, and configure the `ping-auth` plugin.

To configure the `ping-auth` plugin in Kong Konnect, you must:

- Add the ping-auth plugin to your control plane
- Upload files to data plane nodes
- Configure the ping-auth plugin in Konnect

Adding the ping-auth plugin to your control plane

Use the `ping-auth` plugin's `schema.lua` file to create the configurable object required by Konnect. Konnect uses this file to create a plugin entry in the plugin catalog for your control plane. If the plugin schema should be available in multiple control planes, add the schema individually to each one.

You can manage schemas for custom plugins through the Konnect UI or the Konnect Control Planes Config API.

Copyright © 2025 Ping Identity Corporation

Konnect UI

> **Note**
>
> The UI isn't available when using KIC in Konnect. Use the Konnect API instead.

Steps

1. Download version 1.0.8-1 or later of the `kong-plugin-ping-auth` src from https://luarocks.org/modules/pingidentity/kong-plugin-ping-auth.

   > **Note**
   >
   > Support for Kong Konnect is available in version 1.0.8 and later of the plugin.

2. Extract the `src.rock` file and store it on your local computer.

   Verify that you have the following files in the extracted `/kong-plugin/ping-auth` folder:

   - `access.lua`
   - `handler.lua`
   - `Network_handle.lua`
   - `response.lua`
   - `schema.lua`

3. In **Gateway Manager**, open a control plane.
4. In the sidebar, click **Plugins**, then click **New Plugin**.
5. On the **Custom Plugins** tab, click **Create** on the **Custom Plugin** tile.
6. Click **Select File**, then select the `schema.lua` file that you extracted in step 2.
7. Make sure your file displays correctly in the preview, then click **Save**.

Copyright © 2025 Ping Identity Corporation

Konnect API

When using the `/plugin-schemas` API, authenticate your requests with either a personal access token or a system account token by including it in the `Authorization` header:

```
--header 'Authorization: Bearer kpat_xgfT'
```

Steps

1. Upload the `schema.lua` file for your plugin using the `/plugin-schemas` endpoint:

   ```
   curl -i -X POST \
   https://{region}.api.konghq.com/konnect-api/api/runtime_groups/{controlPlaneId}/v2/plugin-schemas \
   --header 'Content-Type: application/json' \
   --data "{\"lua_schema\":  <your escaped Lua schema>}"
   ```

   Result:

   You should get an `HTTP 201` response.

2. To check that your schema was uploaded, use the following request:

   ```
   curl -i -X GET \
   https://{region}.api.konghq.com/konnect-api/api/runtime_groups/{controlPlaneId}/v1/available-plugins
   ```

   Result:

   This request returns an `HTTP 200` response with the schema for your plugin as a JSON object.

Uploading files to data plane nodes

About this task

After you upload the `ping-auth` plugin's schema to Konnect, upload the following files for the plugin to each Kong Konnect data plane node:

- `access.lua`
- `handler.lua`
- `Network_handle.lua`
- `response.lua`
- `schema.lua`

Copyright © 2025 Ping Identity Corporation

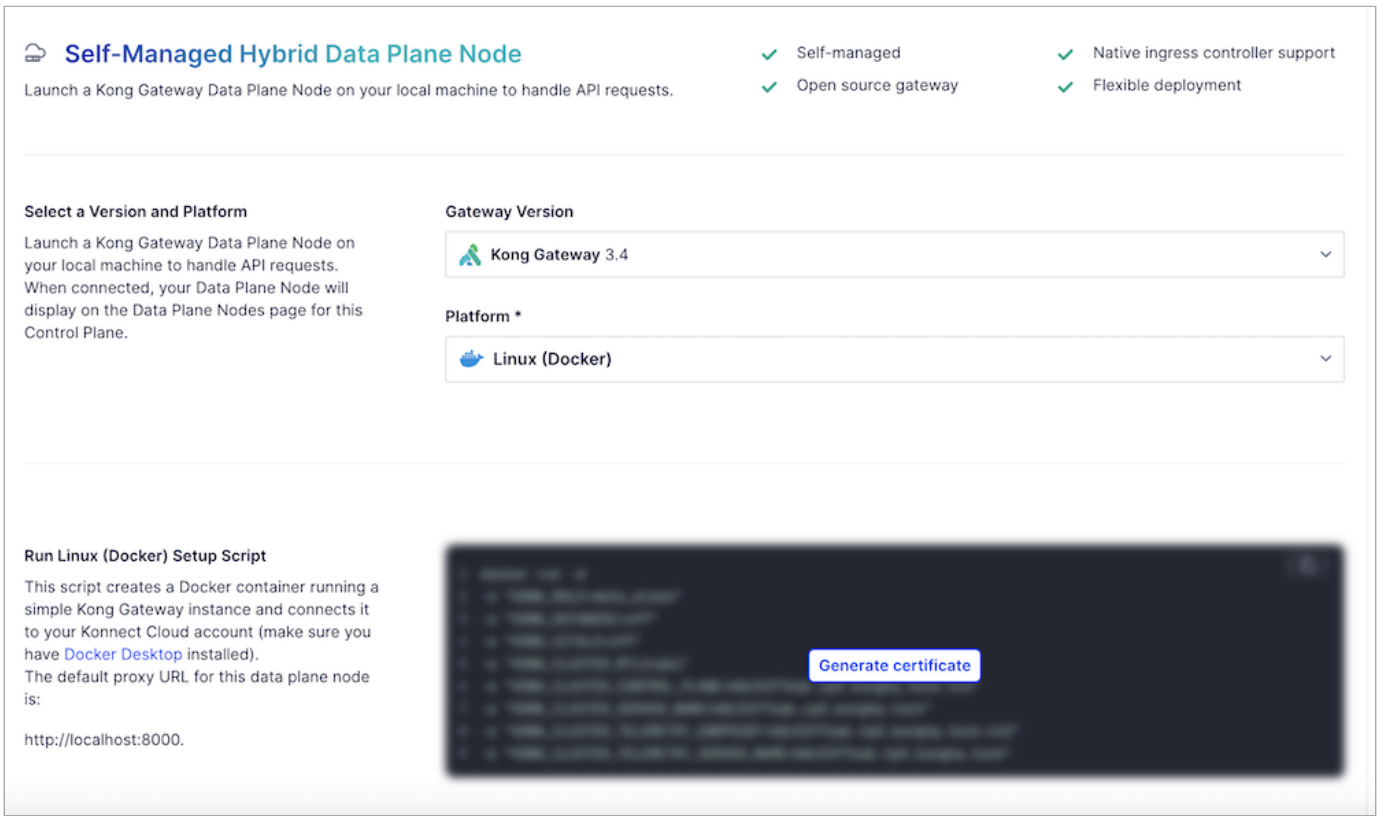
> **Important**
>
> If a data plane node doesn't have these files, the `ping-auth` plugin cannot run on that node.

Follow the Kong Gateway plugin deployment instructions to set up the plugin on each node. Instructions can vary depending on your platform. If you're running Kong Gateway on Docker, the following instructions are provided as an example.

Install the `ping-auth` plugin inside the Kong Konnect Docker container for each node. Copy or mount the plugin's source code into the container.

Steps

1. In your control plane, go to **Data Plane Nodes**, then click **New Data Plane Node**.
2. Select a **Platform**, for example **Linux (Docker)**, and **Generate a certificate**.



3. Copy the generated docker run command and add the following snippet to it.

   Substitute your own source and target paths.

   - The *<source_path>* is the location where you extracted the `ping-auth` plugin files. This is the parent folder that contains the `ping-auth` folder.
   - The *<target_path>* is where you keep custom Kong plugins. This is the path to the `ping-auth` plugin.

```
-v "/<source_path>/ping-auth:/<target_path>/ping-auth" \
-e "KONG_PLUGINS=bundled,ping-auth" \
-e "KONG_LUA_PACKAGE_PATH=/<target_path>/?.lua;;" \
```


Copyright © 2025 Ping Identity Corporation

4. To start a data plane node with the `ping-auth` plugin loaded, run the command.

   Example:

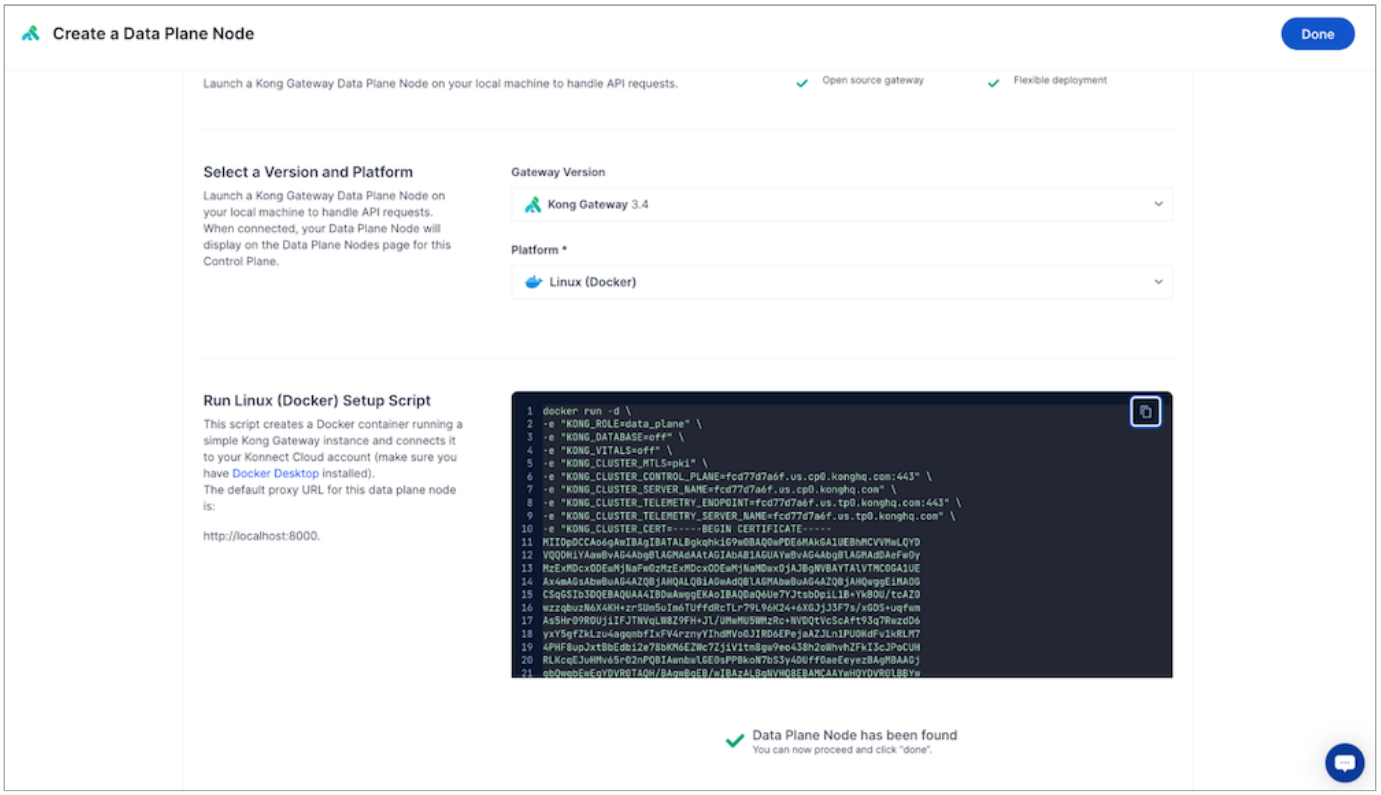
   For example, the command will look something like this, including the three snippet lines from the previous step. In this example, `plugins/kong` represents the *<source_path>* and `usr/local/share/lua/5.1/kong/plugins` represents the *<target_path>*.

```
docker run -d \
-v "/plugins/kong/ping-auth:/usr/local/share/lua/5.1/kong/plugins/ping-auth" \
-e "KONG_PLUGINS=bundled,ping-auth" \
-e "KONG_LUA_PACKAGE_PATH=/usr/local/share/lua/5.1/kong/plugins/?.lua;;" \
-e "KONG_ROLE=data_plane" \
-e "KONG_DATABASE=off" \
-e "KONG_VITALS=off" \
-e "KONG_NGINX_WORKER_PROCESSES=1" \
-e "KONG_CLUSTER_MTLS=pki" \
-e "KONG_CLUSTER_CONTROL_PLANE=<example>.cp0.konghq.com:443" \
-e "KONG_CLUSTER_SERVER_NAME=<example>.cp0.konghq.com" \
-e "KONG_CLUSTER_TELEMETRY_ENDPOINT=<example>.tp0.konghq.com:443" \
-e "KONG_CLUSTER_TELEMETRY_SERVER_NAME=<example>.tp0.konghq.com" \
-e "KONG_CLUSTER_CERT=<cert>" \
-e "KONG_CLUSTER_CERT_KEY=<key>" \
-e "KONG_LUA_SSL_TRUSTED_CERTIFICATE=system" \
-e "KONG_KONNECT_MODE=on" \
-p 8000:8000 \
-p 8443:8443 \
kong/kong-gateway:<version>
```

5. To confirm the Docker deployment, run the following command:

```
"docker logs [container id]"
```

Copyright © 2025 Ping Identity Corporation



Configuring the ping-auth plugin in Konnect

After you've uploaded the `ping-auth` plugin's schema to Konnect, configure the plugin in Gateway Manager or use the Kong API.

> **Caution**
>
> Test the operation of the `ping-auth` plugin before you use it in production.

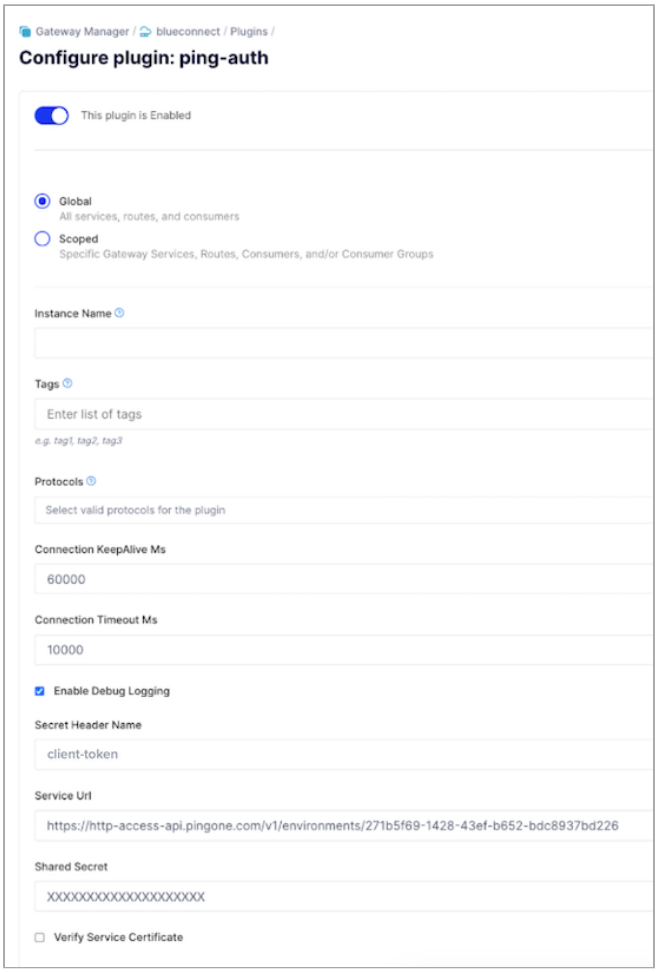
Copyright © 2025 Ping Identity Corporation

Konnect UI

Steps

1. In **Gateway Manager**, click **Plugins** in the sidebar, then click **New Plugin**.
2. On the **Custom Plugins** tab, click the **ping-auth** plugin.
3. (Optional) To enable the plugin for specific consumers, services, or routes, click **Scoped**, and then enter **Service**, **Route**, and **Consumer** information.
4. In the **Service Url** field, enter the API gateway service URL that you saved when you prepared PingOne Authorize for Konnect integration.
5. In the **Shared Secret** field, enter the credential that you saved earlier.

> **Important**
>
> The gateway credential is the shared secret that authenticates the `ping-auth` plugin to PingOne Authorize. Version 1.2.0 of the plugin supports referenceable secrets. For security reasons, store the gateway credential in a vault supported by Kong. Learn more in Secrets Management in Konnect and Environment Variables Vault in the Kong documentation.



6. Configure the following additional fields:

Option	API Field Name	Description
Connection KeepAlive Ms	`connection_keepAlive_ms`	The duration to keep the connection alive for reuse. The default is `60000` milliseconds.
Connection Timeout Ms	`connection_timeout_ms`	The duration to wait before the connection times out. The default is `10000` milliseconds.
Enable Debug Logging	`enable_debug_logging`	Controls whether requests and responses are logged at the debug level. The default is `false`. For log messages to show in `error.log`, you must set `log_level = debug` in `kong.conf`.
Verify Service Certificate	`verify_service_certificate`	Controls whether the service certificate is verified. This is intended for testing purposes, and the default is `true`.

7. Click **Save**.

Result

Kong Konnect is now configured to work with PingOne Authorize.

Copyright © 2025 Ping Identity Corporation

Kong API

Steps

1. Send the following in a POST request to `https://{region}.api.konghq.com/konnect-api/api/runtime_groups/{controlPlaneId}/plugins`:

```
{
  "name": "ping-auth",
  "enabled": true,
  "config": {
    "enable_debug_logging": true,
    "verify_service_certificate": false,
    "secret_header_name": "<shared secret header name>",
    "service_url": "https://<PingOne Server hostname>",
    "shared_secret": "<shared secret>"
  }
}
```

The following fields are required for this API request:

- `Secret_header_name`: The header name in which the shared secret is provided. You can provide additional configuration in accordance with the Kong API specification.
- `Service_url`: The full service URL of the API gateway in PingOne.

> **Tip**
> You saved the service URL when you prepared PingOne Authorize for Konnect integration. To find this credential in PingOne, go to **Authorization > API Gateways**.

- `Shared_secret`: The shared secret value to authenticate this plugin to PingOne.

> **Important**
> The gateway credential is the shared secret that authenticates the `ping-auth` plugin to PingOne Authorize. Version 1.2.0 of the plugin supports referenceable secrets. For security reasons, store the gateway credential in a vault supported by Kong. Learn more in Secrets Management in Konnect and Environment Variables Vault in the Kong documentation.

2. (Optional) Configure additional fields:

Option	API Field Name	Description
Connection KeepAlive Ms	`connection_keepAlive_ms`	The duration to keep the connection alive for reuse. The default is `60000` milliseconds.
Connection Timeout Ms	`connection_timeout_ms`	The duration to wait before the connection times out. The default is `10000` milliseconds.

Copyright © 2025 Ping Identity Corporation

Option	API Field Name	Description
Enable Debug Logging	`enable_debug_logging`	Controls whether requests and responses are logged at the debug level. The default is `false`. For log messages to show in `error.log`, you must set `log_level = debug` in `kong.conf`.
Verify Service Certificate	`verify_service_certificate`	Controls whether the service certificate is verified. This is intended for testing purposes, and the default is `true`.

Result

Kong Konnect is now configured to work with PingOne Authorize.

Editing an API gateway

You can edit the gateway name and description. You can also disable an API gateway.

Steps

1. Go to **Authorization > API Gateways**, and click the API gateway you want to edit.
2. To disable the gateway, click the toggle next to the API gateway name.
3. To edit the gateway, click the **More Options (⋮)** icon next to the API gateway name, and then select **Edit an API Gateway**.
4. Edit gateway settings.
5. Click **Finish & Save**.

Deleting an API gateway

Remove API gateways and credentials that you no longer need.

Steps

1. Go to **Authorization > API Gateways**, and click the API gateway you want to delete.
2. To delete a credential, click the **Delete** icon next to the credential.
3. To delete the API gateway, click the **More Options (⋮)** icon next to the API gateway name and then select **Delete**.
4. Select the **I understand and want to continue** check box, and then click **Delete**.

Copyright © 2025 Ping Identity Corporation

Rotating an API gateway credential

For security reasons, you should rotate an API gateway's credential on a regular basis.

About this task

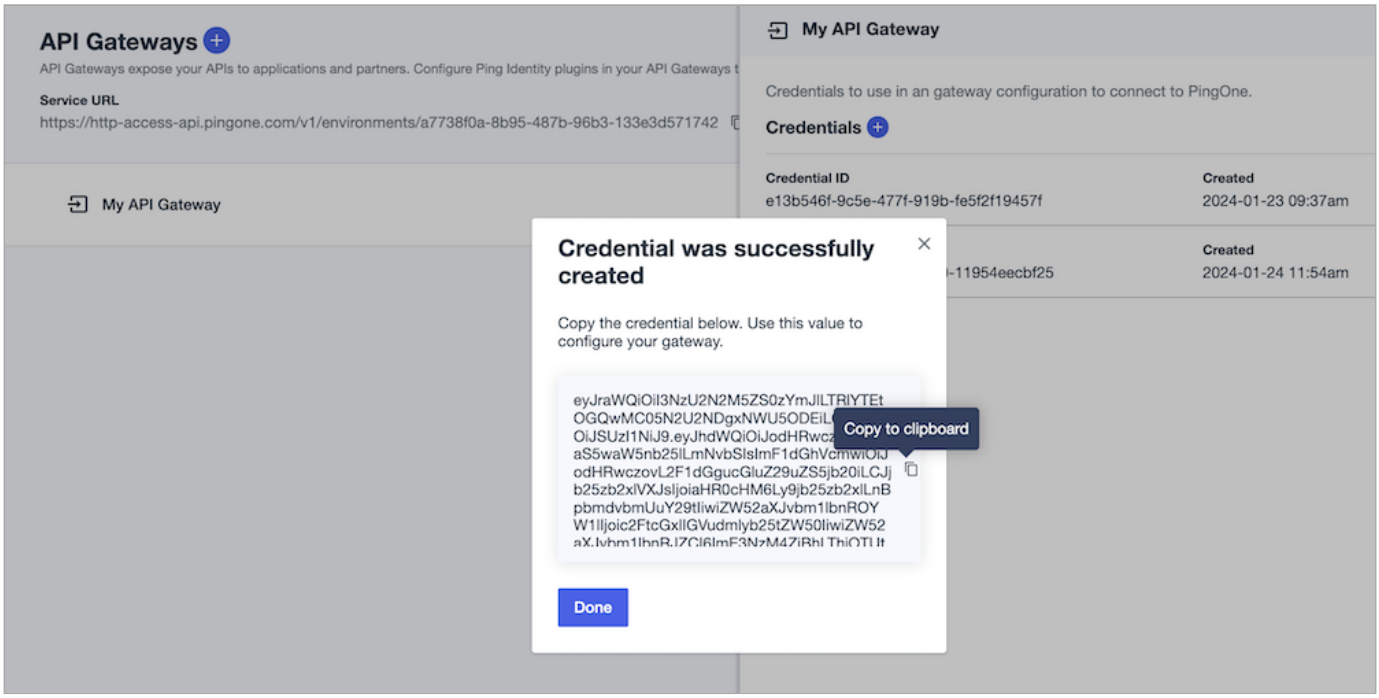
> **Important**
>
> If the credential might have been compromised, change it immediately.

An API gateway credential is a safeguard against requests from an unauthorized API gateway integration kit. After you create a credential and copy it to your Ping Identity integration kit, the credential is included in authorization requests made from the API Gateway to the HTTP Access Policy service. If the credential is absent or no longer valid, the HTTP Access Policy service automatically rejects the client API request.

You can use the PingOne Authorize console to create a new credential for an existing API gateway. This enables you to retrieve the credential without having to make an API call. After you create a new credential in PingOne Authorize, you must update all API gateway integration kits that use the credential. Retain the previous credential to give API gateway owners time to make updates without causing errors for users.

Steps

1. In PingOne, go to **Authorization → API Gateways**.
2. Click the API gateway with the credential that you want to rotate to open its details panel.
3. On the details panel, click the **+** icon next to **Credentials**, copy the credential and save it somewhere convenient, and then click **Done**.

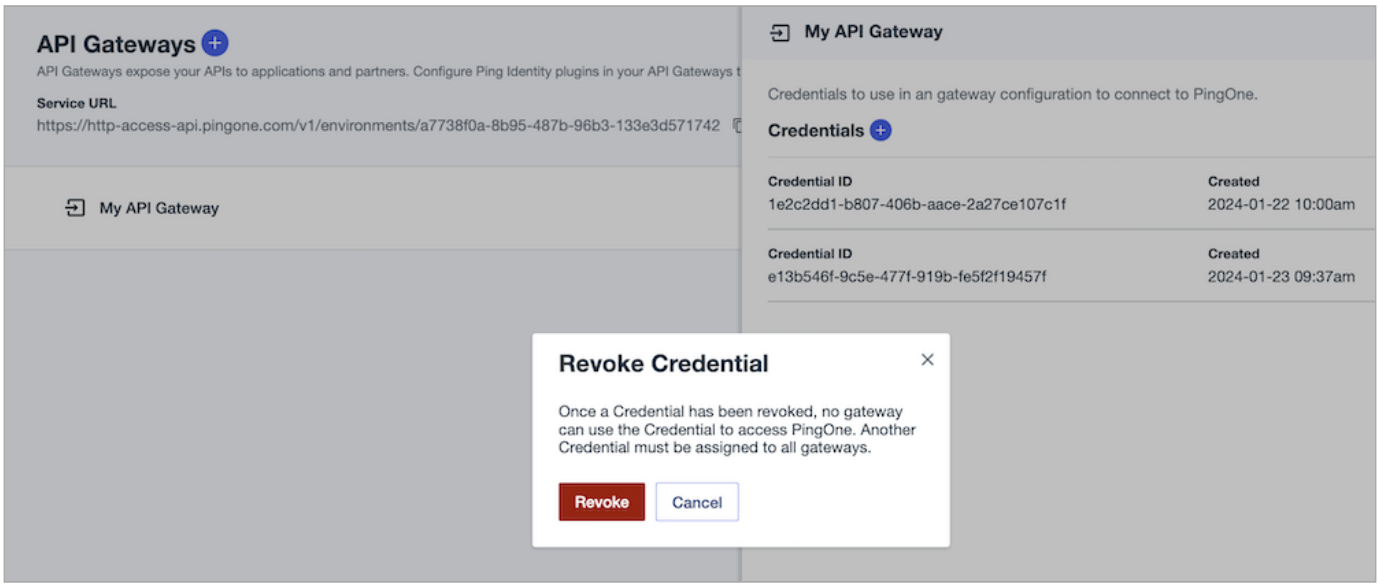


> **Note**
>
> The HTTP Access Policy service will accept both the old and new credentials. To prevent downtime, do not revoke the active gateway credential until after you update the integration kits.

4. Update each integration kit with the newly created gateway credential.

   Learn more about configuring your specific integration kit in API Gateway integrations.

5. In the details panel of your API gateway, click the **Delete** icon next to the old gateway credential, and then click **Revoke**.



Application roles

Application roles provide a way to group permissions by function and assign them to users.

Application roles are collections of application permissions. When you assign a user to a role, you grant the user all of the permissions for that role.

> **Note**
>
> PingOne administrator roles are collections of permissions that give PingOne admins access to resources in the PingOne admin console, such as organizations, environments, and identities.
> Application roles help you manage access to the application resources developed by your organization's engineering teams.

You can assign the same permission to multiple roles. For example, at a bank, both an account administrator and loan officer could have permission to view accounts.

You can also assign multiple roles to the same user. For example, at a small regional bank, Jim might be both an account administrator and a loan officer.

You can assign users to roles when you create an application role or when you edit a user. Learn more in Adding an application role and Managing user roles.

Copyright © 2025 Ping Identity Corporation

> **Note**
> Roles and permissions are currently scoped to an environment in PingOne.

Adding an application role

Add application roles to group application permissions by function, then control access to application resources by assigning roles to users.

Before you begin

- Add the application permissions that you want to grant to your roles.
- Add the users that you want to assign to roles.

About this task

Roles determine which permissions a user has. A user can perform an action on an application resource if they have a role with the associated permission.

> **Note**
> You can add up to 128 application roles in each PingOne environment.

Steps

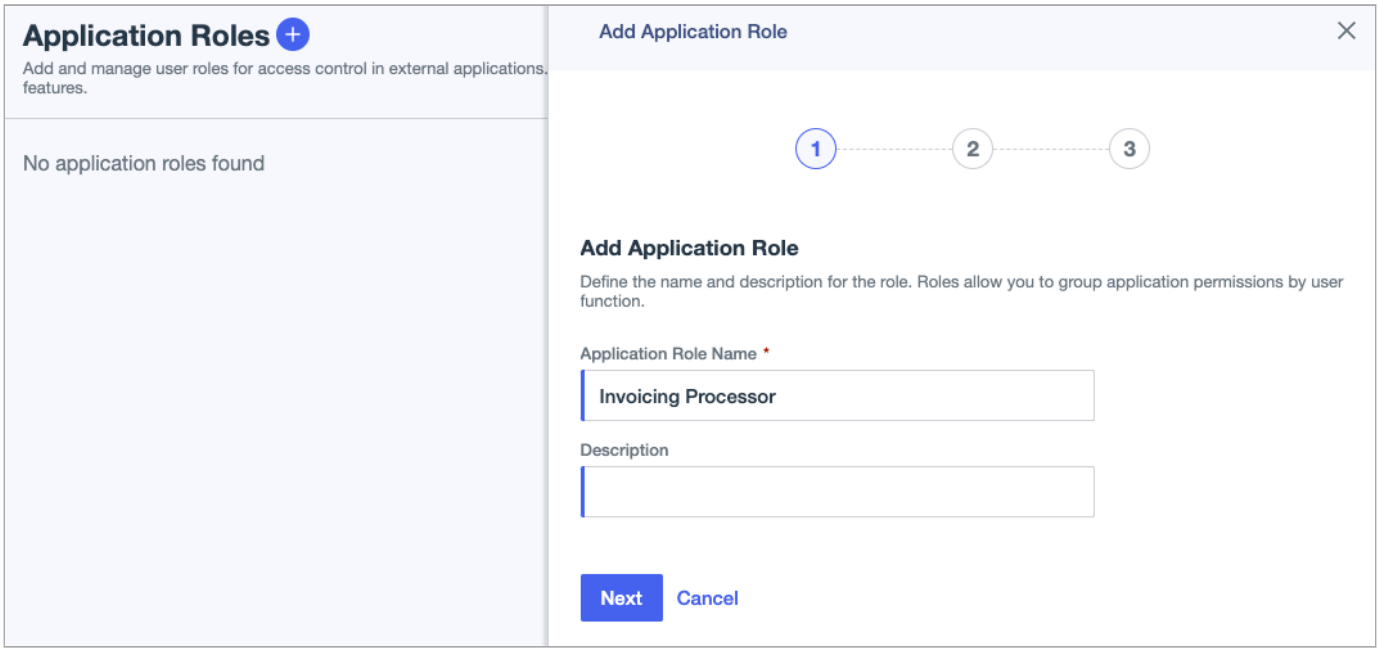
1. Go to **Authorization** > **Application Roles**.
2. Click the **+** icon next to **Application Roles**.
3. Enter a unique **Application Role Name** and an optional **Description**. Click **Next**.

   > **Note**
   > The name can include Unicode letters, marks, numbers, spaces, forward slashes, dots, apostrophes, underscores, and hyphens, with a maximum length of 20 characters.

   Example:

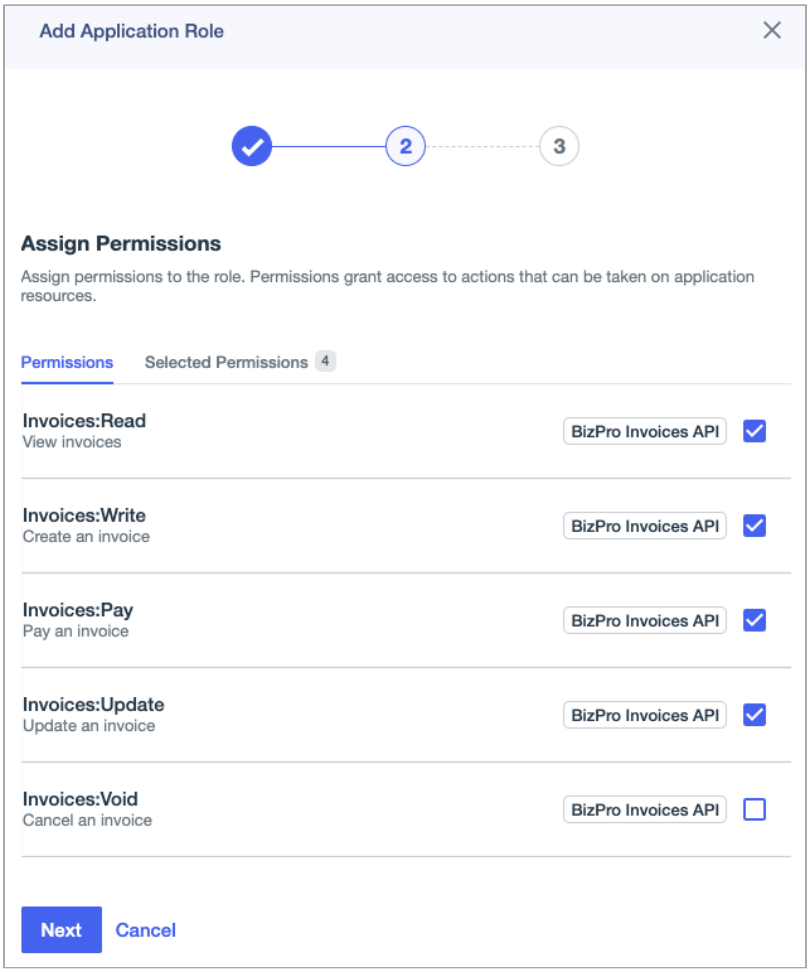
   For example, you could add an `Invoicing Processor` role for the BizPro invoicing application to give Invoicing Processors permissions to read, write, pay, and update invoices.

Copyright © 2025 Ping Identity Corporation



4. Select the permissions that you want to assign to the role.

   Permission names list the application resource and action separated by a colon. For reference, the PingOne resource associated with the application resource is displayed next to the checkbox.

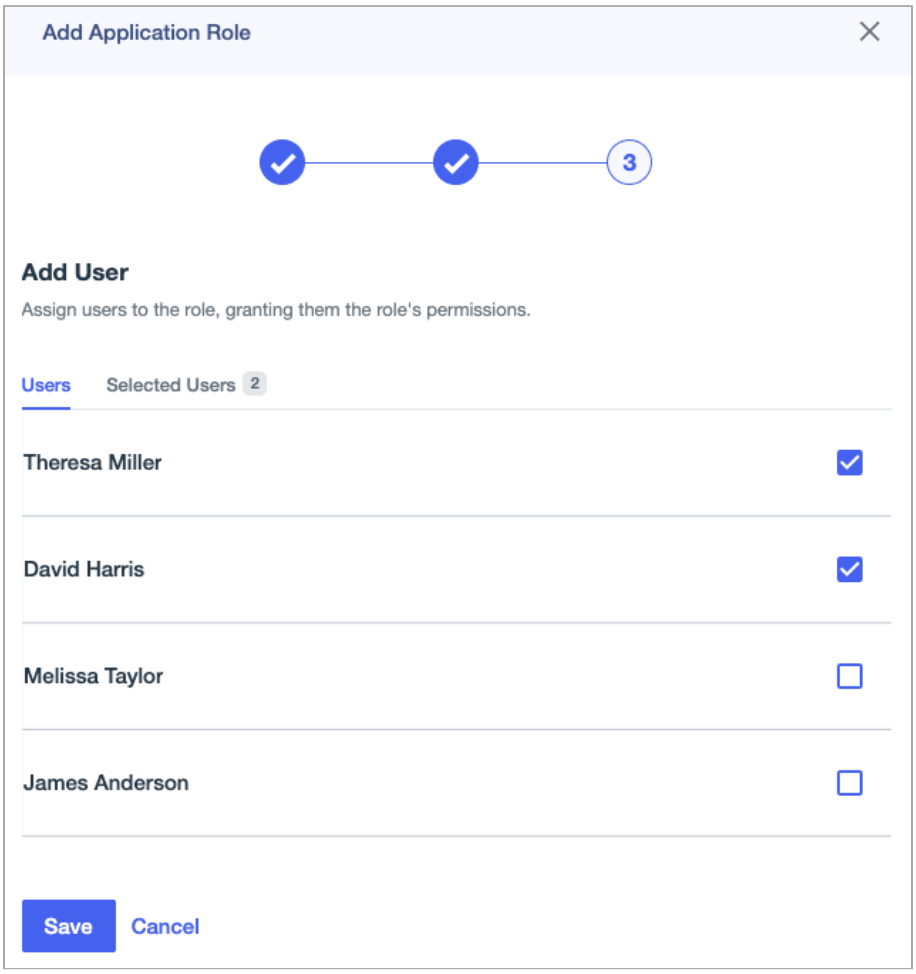


Copyright © 2025 Ping Identity Corporation

5. Click **Next**.
6. Select the users that you want to assign to the role.

   Result:

   Selected users will have the permissions that are assigned to the role.



7. Click **Save**.

Next steps

Add additional roles and assign users to grant them the permissions assigned to the roles.

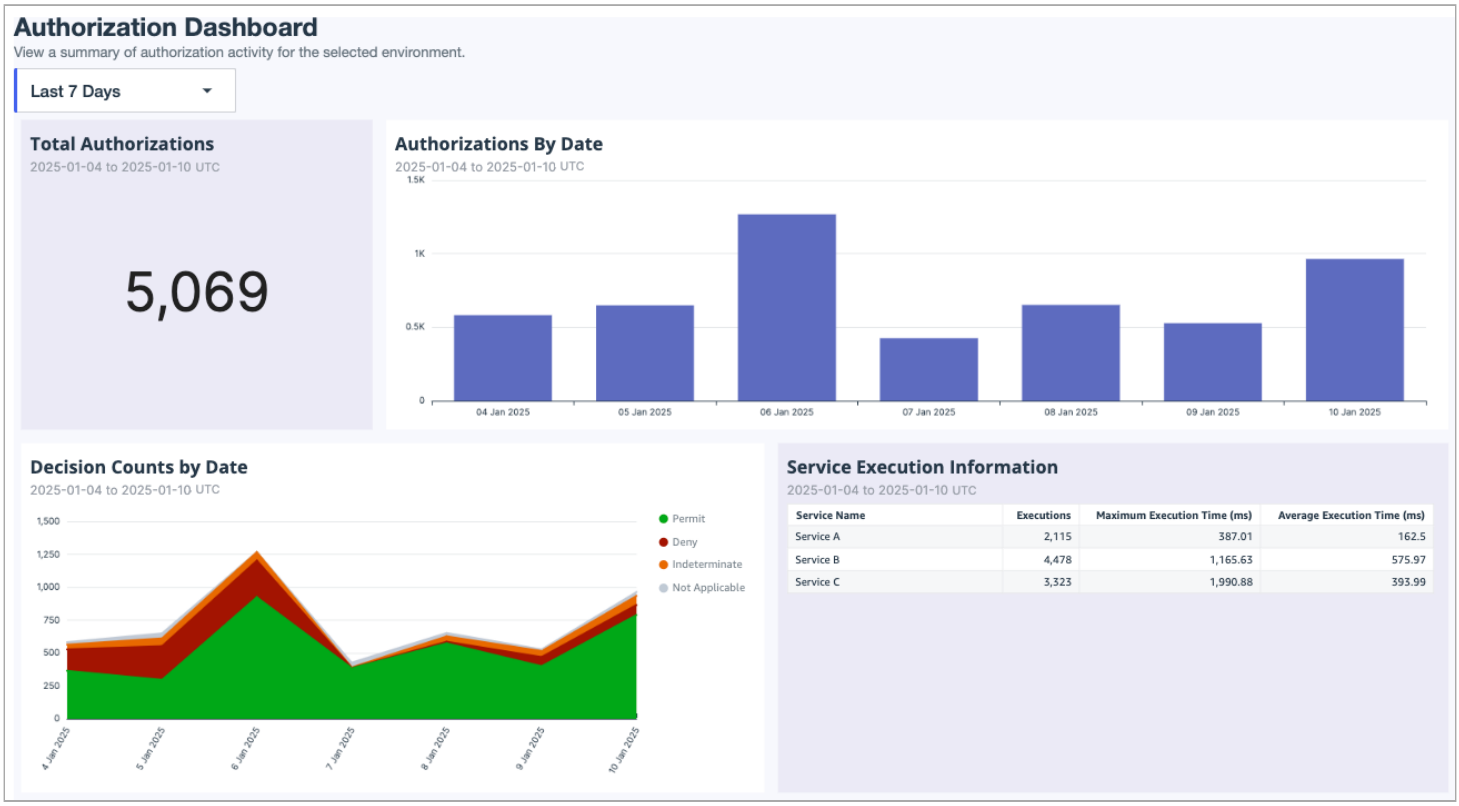
For example, in the BizPro invoicing application, Billing Supervisors might need permissions to read and void invoices. Add a `Billing Supervisor` role and assign the `Invoices:Read` and `Invoices:Void` permissions to it.

Authorization Dashboard

The **Authorization Dashboard** shows a summary of authorization activity generated by requests to PingOne Authorize decision endpoints.

To access the **Authorization Dashboard**, go to **Monitoring > Authorization**.

Copyright © 2025 Ping Identity Corporation



Filters

Use filters to refine the data displayed on the dashboard. You can limit data to a specific time range:

- **Today**: Displays data for the current day only.
- **From Yesterday**: Displays data for the previous day only.
- **Last 7 Days** (default): Displays data for the previous 7 days only.
- **Last 30 Days**: Displays data for the previous 30 days only.
- **This Month**: Displays data for the current calendar month only.
- **Last Month**: Displays data for the previous calendar month only.
- **Last 6 Months**: Displays data for the previous 6 months only.

This filter applies to all charts on the dashboard.

> **Note**
>
> PingOne aggregates data at regular intervals. It can take up to 30 minutes for decision requests to show up on the dashboard.

Charts

Use the following controls to adjust the charts:

Copyright © 2025 Ping Identity Corporation

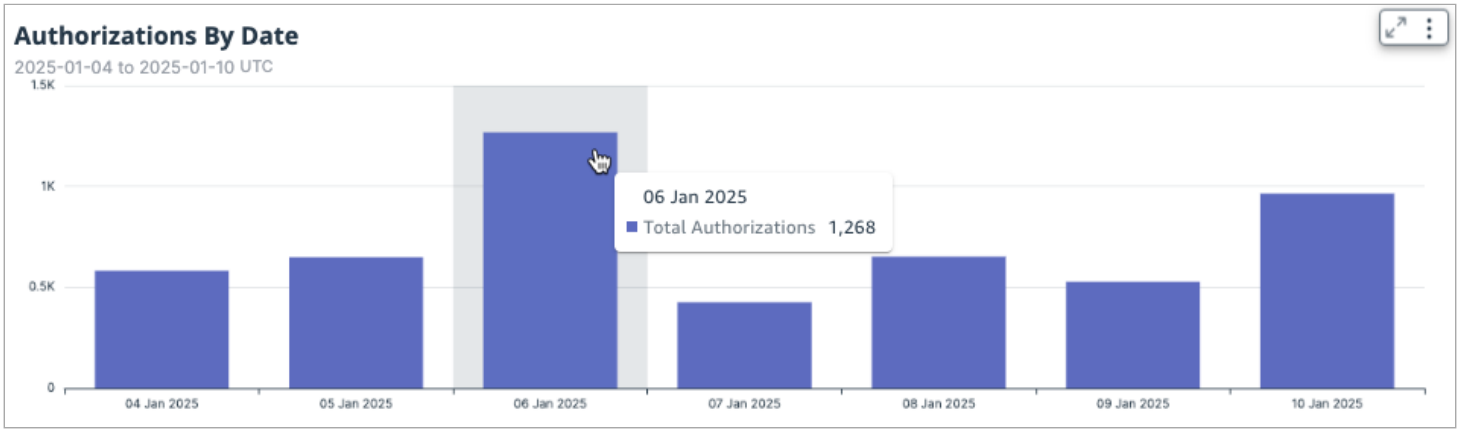
Icon	Name	Description
	Maximize	Expands the chart to fill the dashboard. To minimize the chart, click the icon again.
	Menu options	Options can vary for different types of charts: • **View summary data**: Displays chart data as a table. • **Export**: Exports chart data to CSV or Excel format, depending on the type of chart.
	Sort visual	Sorts the chart data in ascending or descending order.

Total Authorizations

Displays the total number of authorization decisions across all decision endpoints during the selected time period.

Authorizations by Date

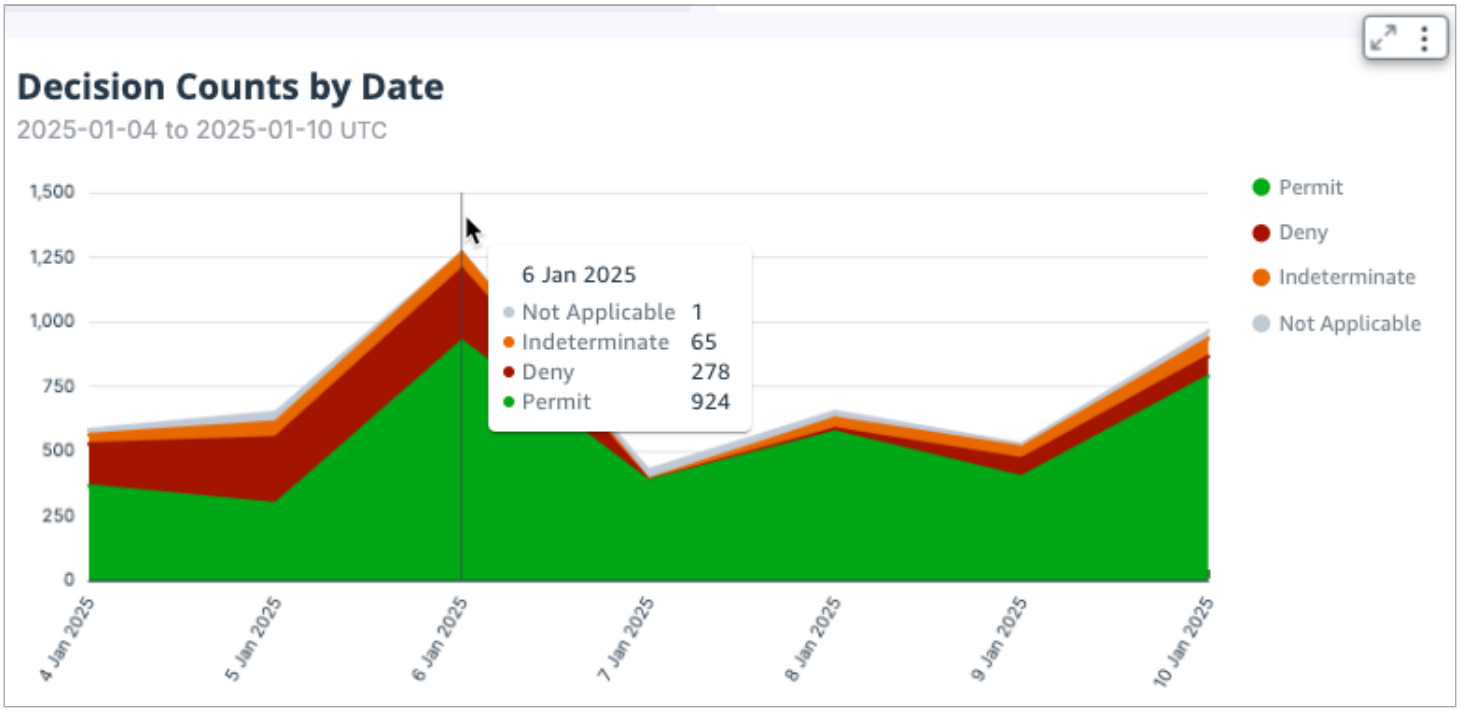
Displays a bar chart that shows the number of authorization decisions by date. Hover over a bar to display the number of authorizations on that date.



Decision Counts by Date

Displays a breakdown of permit, deny, indeterminate, and not applicable decision counts during the selected time period. Hover over the chart to display the number of decisions on that date by type.

Copyright © 2025 Ping Identity Corporation



Service Execution Information

Displays the number of requests made to policy information point services during the selected time period, including the maximum and average time in milliseconds that it took for the service to return a response.

Authorization API reference

PingOne Authorize APIs provide developers with tools to manage the following authorization resources:

- API Access Management services for authorization enforced through an API gateway
- Application resources and roles for role-based access control
- Authorization decisions, decision endpoints, and recent decisions
- Authorization policies, rules, and statements
- Trust Framework elements, including attributes, conditions, processors, and services

Learn more about authorization APIs in the PingOne Authorize API reference documentation.

Copyright © 2025 Ping Identity Corporation

Integrations

The **Integrations** branch contains the **External IdPs**, **Provisioning**, **Gateways**, **Webhooks**, and **PingFederate** pages.

For more information, see the following topics:

External IdPs

Provisioning

Gateways

Webhooks

PingFederate

External IdPs

With PingOne, you can use the PingOne user directory or an external identity provider (IdP).

Using an external IdP allows linked users to authenticate using the credentials provided by the external IdP. An external IdP includes mapping PingOne user attributes to attributes from the IdP.

You can also use an external IdP to secure the PingOne admin console. Learn more in Administrator security.

Approaches for external IdPs

There are several important differences in the way that IdPs can be used in PingOne authentication policies:

Login

Add an external IdP as part of a login step. At the sign-on prompt, the end user can enter a username and password or choose an external IdP to authenticate with, such as Google or Facebook. Learn more in Adding a login authentication step.

Identifier First

Add an identifier-first step to an authentication policy. The end user is prompted for an identifier, such as a username. The policy can then send the end user to a particular IdP based on rules evaluation of the identifier. Learn more in Identifier first authentication.

External Identity Provider

Add an external IdP step to an authentication policy. The end user is forwarded to an external IdP based on policy and without any interaction from the user. Learn more in Adding an external identity provider sign-on step.

Encryption

A SAML IdP can use one of your PingOne encryption certificates to encrypt SAML assertions for you.

If you want the IdP to use a specific encryption certificate, you can download it in the X509 PEM (`.crt`) format and send it to the IdP. Learn more in Downloading a certificate.

Copyright © 2025 Ping Identity Corporation

If you want the IdP to use the default encryption certificate, your metadata already contains it. Learn more in Downloading metadata for SAML IdPs.

When PingOne receives an encrypted assertion (a SAML response with an `EncryptedAssertion` element), it attempts to decrypt it with each encryption certificate in your environment starting with the default, followed by the rest of the encryption certificates.

When your encryption certificate nears expiration, you can add a new one and allow both the old and new certificate to be used. This allows all your IdPs to change to the new certificate at any time without downtime. When your default encryption certificate expires, you must change the default encryption certificate for your environment. Otherwise, the SAML metadata you provide to your IdPs contains the expired certificate and is not valid for most IdPs. You can change the default encryption certificate in the PingOne admin console. Learn more in Designating default keys.

PingOne supports the following standards:

- Encrypted assertion
- Multiple block encryption algorithms:
  - AES-128-CBC
  - AES-256-CBC
  - AES-128-GCM
  - AES-192-GCM
  - AES-256-GCM
  - Triple DES
- RSA-OAEP key transport algorithm

Viewing identity providers

Use the **External IdPs** page to view details for external identity providers (IdPs) that have been configured in PingOne.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs**.

   Result

   The **External IdPs** page shows a list of the configured IdPs.

2. Click an IdP to view details about the profile, connection, and attribute mappings.
3. To enable or disable an IdP, click the toggle in the **External IdPs** list.

> **Note**
>
> IdPs labeled with the **Administrator IDP** badge are used for authentication into the PingOne admin console and can't be disabled or deleted.

Next steps

Edit an identity provider.

Copyright © 2025 Ping Identity Corporation

Adding a vendor-specific identity provider in PingOne

Add a vendor-specific external identity provider (IdP) in PingOne to allow users to sign on to your applications using their existing credentials from services like Google, Apple, or LinkedIn. Adding an external IdP for a third-party vendor includes mapping PingOne user attributes to attributes from the IdP.

> **Note**
>
> To enable or disable an IdP, click the toggle in the **External IdPs** list.

Adding an identity provider - Amazon

Adding Amazon as an external identity provider (IdP) gives your users the option to sign on with Amazon when accessing your application.

Before you begin

Ensure that you have:

- A PingOne organization with an environment added. Learn more in Starting a PingOne trial.
- Added your application to PingOne. Learn more in Adding an application.
- An Amazon account.

Creating a security profile with Amazon

Before you can set up Amazon as an external IdP, you must create a security profile for your application. Learn more in Register for Login with Amazon.

Before you begin

Ensure that you have the following information for your application:

- Name
- Description
- Privacy notice URL
- Logo (optional)

Steps

1. Go to the Amazon Developer Console and sign on to your account.

   If you don't have an account you can create one now.

2. Click **Create a New Security Profile**.

Copyright © 2025 Ping Identity Corporation

3. Enter the following:
   - **Security Profile Name**: A unique identifier for the application, which will appear on the consent page when users agree to sign on with Amazon.
   - **Security Profile Description**: A brief description of the application.
   - **Privacy Notice URL**: The location of the privacy notice for your application.
   - **Consent Logo Image** (optional): The image that appears on the consent page to represent your application.
4. Click **Save**.

Enabling Login with Amazon

If you created a new security profile, `Login with Amazon` should be enabled by default. If you are adding an application to an existing security profile, enable `Login with Amazon`.

Steps

1. Go to the Amazon Developer Console.

   Result:

   You are asked to sign on to the Developer Console.
2. Click **Select a security profile**, then choose your security profile in the menu.
3. Click **Confirm**.
4. In the form that opens, enter a **Consent Privacy Notice URL**.

   This is the location of your application's privacy policy.
5. Click **Save**.

Getting the client ID and client secret

Copy the client ID and client secret from the Amazon Developer Console. You'll need these values when you add the application to PingOne.

Steps

1. Go to the Amazon Developer Console and locate the appropriate security profile.
2. Click **Web Settings**.
3. Copy the **Client ID** and **Client secret** to a secure location.

   You can always access these values on the Amazon Developer Console.

Adding Amazon as an identity provider in PingOne

Configure the IdP connection in PingOne.

Before you begin

Copyright © 2025 Ping Identity Corporation

You should have the following information ready:

- Client ID
- Client secret

Ensure that registration is enabled in the authentication policy. Learn more in Editing an authentication policy.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and click **+**.
2. Click **Amazon**.
3. Click **Next**.
4. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.

     > **Note**
     > You can't change the **Icon** and **Sign-on Button**, in accordance with the provider's brand standards.
5. Click **Next**.
6. Configure the connection and enter the following information:
   - **Client ID**: The application ID that you copied earlier from the IdP. You can find this information on the Amazon Developer Console.
   - **Client secret**: The application secret that you copied earlier from the IdP. You can find this information on the Amazon Developer Console.
   - **Callback URL**: Copy the **Callback URL** to a secure location. You'll provide this value to the IdP later.
7. Click **Next**.
8. Define how the PingOne user attributes are mapped to IdP attributes. Learn more in Mapping attributes.
   - Enter the PingOne user profile attribute and the external IdP attribute. Learn more about attribute syntax in Identity provider attributes.
   - To add an attribute, click **+ Add**.
   - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
   - Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
     - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
     - **Always**: Always update the PingOne directory attribute.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> You can map the following attributes provided by Amazon:
>
> - `email`
> - `name`
> - `user_id`
> - `postal_code`

9. Click **Save**.
10. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
>
> You can disable the IdP by clicking the toggle to the left (gray).

Adding the callback URL to the Amazon Developer Console

Copy the callback URL from the PingOne admin console and paste it in the Amazon Developer Console.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and browse or search for the appropriate IdP.
2. Click the IdP to open the details panel.
3. On the **Connection** tab, copy the **Callback URL** to a secure location.
4. Go to the Amazon Developer Console.
5. Select the appropriate profile.
6. Go to the **Web Settings** section.
7. For **Allowed Return URLs**, paste the value that you copied from the the PingOne admin console.
8. Click **Save**.

Next steps

- Add the IdP to your authentication policy.
- Apply the authentication policy to your application.

Adding an identity provider - Apple

Adding Apple as an external identity provider (IdP) gives your users the option to sign on with Apple when accessing your application.

Before you begin

Ensure that you have:

- A PingOne organization with an environment added. Learn more in Starting a PingOne trial.

Copyright © 2025 Ping Identity Corporation

- Added your application to PingOne. Learn more in Adding an application.
- An Apple account.

Creating an App ID

When you register your application, Apple generates an App ID to identify the application. You'll need this value to connect the application to PingOne.

Steps

1. Go to the Apple Developer site and sign on to your Apple Developer account.

   If you don't have an Apple Developer account, you'll need to create one.

2. Click **Certificates, Identifiers & Profiles**.
3. On the left, click **Identifiers** and then click the **+** icon.
4. In the **Register a New Identifier** section, select **App IDs**.
5. In the **Register an App ID** section, enter a value for the **Bundle ID**.
6. Copy the following values to a secure location:
   - **App ID prefix** (Team ID): Identifies your team or organization.
   - **Bundle ID**: Identifies a group of applications.
7. In the list of available capabilities, select **Sign in with Apple**.
8. Click **Continue and Register**.

Creating a Services ID

The Services ID identifies the particular instance of your application. The Services ID is equivalent to a client ID in PingOne.

Steps

1. On the Apple Developer site, sign on to your Apple Developer account and then click **Certificates, Identifiers & Profiles**.
2. In the **Register a New Identifier** section, select **Services ID**.
3. Enter the following information:
   - **Description**: A brief description of the application.
   - **Identifier**: The path to the application. This value will be used as the client ID in PingOne.
4. Click **Continue and Register**.
5. In the list, select the service you just created.
6. Select **Sign in with Apple** and click **Configure**.
7. Select the primary App ID and click the **+** icon.
8. Enter a value for **Domains and subdomains**.

Copyright © 2025 Ping Identity Corporation

This is the top-level domain for your application.

9. Leave the **Return URLs** blank for now.

   This is the path in your application that users are redirected to after they have authenticated with Apple. This value is equivalent to a callback URI. You'll enter this value after you set up your application in PingOne.

10. Click **Next**, and then click **Done**.

11. Click **Continue**, and then click **Save**.

Creating a private key

When you register your application, Apple generates a private key for client authentication. You'll need this value when you add the application to PingOne.

Steps

1. On the Apple Developer site, click **Certificates, Identifiers & Profiles**.
2. On the left, click **Keys**.
3. To register a new key, click the **+** icon.
4. Enter a value for **Key Name**.
5. Select **Sign in with Apple** and click **Configure**.
6. Select the primary App ID you created earlier.
7. Click **Save** and then click **Continue**.
8. Click **Register**.
9. Copy the **Key ID** to a secure location.

   You'll use this value when you add the IdP in PingOne.

10. To save the key to the local file system, click **Download**.

    The key is saved as a text file with a `.p8` file extension. The key will be used as the client secret signing key and its identifier will be used as the private key in PingOne.

    > **Important**
    >
    > You can download the key only once. Save the file to a secure location because the key is not saved in your developer account, and you won't be able to download it again. If the **Download** button is disabled, you already downloaded the key.

Configuring email communication

Configuring Apple for email communication allows users to set up an account and sign on to applications with their existing Apple ID, which is required for PingOne to communicate with users and for users to receive updates from Apple. Learn more in Configure private email relay service in the Apple Developer documentation.

Copyright © 2025 Ping Identity Corporation

Steps

1. On the Apple Developer site, click **Certificates, Identifiers & Profiles**.
2. On the left, click **More** and then click **Configure**.
3. Next to **Email Sources**, click the **+** icon.
4. For **Domains and subdomains**, enter `pingidentity.com`.
5. Click **Next**.
6. Click **Register** and then click **Done**.

Adding Apple as an identity provider in PingOne

Configure the IdP connection in PingOne.

Before you begin

Ensure that registration is enabled in the authentication policy. Learn more in Editing an authentication policy.

You should have the following information ready:

- App ID (Client ID)
- Client secret signing key
- Team ID
- Private key ID

Learn more in Creating an App ID and Creating a Services ID.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and click **+**.
2. Click **Apple**.
3. Click **Next**.
4. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.

     > **Note**
     > You can't change the **Icon** and **Sign-on Button** in accordance with the provider's brand standards.

5. Click **Next**.

Copyright © 2025 Ping Identity Corporation

6. Configure the connection and enter the following information:
   - **Service ID** (App ID): The application ID that you copied earlier from the IdP. You can find this information on the Apple Developer site.
   - **Private key**: The application secret that you copied earlier from the IdP. You can find this information on the Apple Developer site.
   - **Team ID**: A unique 10-character string generated by Apple that identifies your organization. The team ID is the prefix of the app ID.
   - **Private key ID**: Identifies the private key in the JSON Web Token (JWT). This JSON object is the client secret in PingOne.
   - **Callback URL**: Copy the **Callback URL** to a secure location. You'll provide this value to the IdP later.
7. Click **Next**.
8. Map the following PingOne attributes to Apple attributes:

PingOne attribute	Apple attribute
Given Name	providerAttributes.name.firstName
Family Name	providerAttributes.name.lastName

> **Important**
>
> Apple only sends an ID token with the first authentication using Sign in with Apple.
> Learn more about Sign in with Apple in Authenticating users with Sign in with Apple in the Apple documentation.

9. Map additional attributes as needed.

   Learn more in Mapping attributes.

> **Note**
>
> You can map additional attributes if they are in the ID token from Apple, such as `iss`, `iat`, `exp`, `aud`, `sub`, `nonce`, `nonce_supported`, `email`, and `email_verified`. Learn more about the JSON structure generated by Apple in Configuring your webpage for Sign in with Apple in the Apple documentation.

   - Enter the PingOne user profile attribute and the external IdP attribute. Learn more about attribute syntax in Identity provider attributes.
   - To add an attribute, click **+ Add**.
   - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
   - Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
     - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.

Copyright © 2025 Ping Identity Corporation

- **Always**: Always update the PingOne directory attribute.

10. Click **Save**.
11. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
> You can disable the IdP by clicking the toggle to the left (gray).

Adding the return URL to the Apple Developers site

Copy the callback URL from the PingOne admin console and paste it in the Apple Developers site.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and browse or search for the appropriate IdP.
2. Click the IdP to open the details panel.
3. Click the **Connection** tab.
4. Copy the callback URL to a secure location.
5. On the Apple Developer site, click **Certificates, Identifiers & Profiles**.
6. Select **Sign in with Apple** and click **Configure**.
7. Select the primary app ID and click the **+** icon.
8. For **Return URLs**, paste the **Callback URL** value that you copied earlier.
9. Click **Next**, and then click **Done**.

Next steps

- Add the IdP to your authentication policy.
- Apply the authentication policy to your application.

Adding an identity provider - Facebook

Adding Facebook as an external identity provider (IdP) gives your users the option to sign on with Facebook when accessing your application.

Before you begin

Ensure that you have:

- A PingOne organization with an environment added. Learn more in Starting a PingOne trial.
- Added your application to PingOne. Learn more in Adding an application.
- A Facebook account.

Copyright © 2025 Ping Identity Corporation

Registering your application with Facebook for Developers

Facebook generates an app ID and app secret for your application. You'll need these values to connect the application to PingOne.

Steps

1. Sign on to your Facebook Developer Account.

   If you haven't created a Facebook Developer Account, you can do so now.

2. At the top of the page, click **My Apps** and then click **Create app**.
3. Select the appropriate application type and then click **Continue**.
4. Enter the following information:
   - **App Display name**: The name you want to associate with this application ID.
   - **App Contact email**: The primary contact information for the application.
5. Click **Create app**, and then complete the security check, if required.

   Result:

   The application dashboard is displayed.

6. On the left side of the page, go to **Settings** > **Basic** and enter the following information:
   - **App domains**: The path in your application that users are redirected to after they have authenticated with Facebook.

     Leave **App domains** blank for now.

   - **Privacy policy URL** (optional): The URL that contains your privacy policy.
   - **Terms of service URL** (optional): The URL that contains your terms of service.
7. At the top of the page, locate the **App ID** and **App secret** and copy their values to a secure location.
8. Click **Save changes**.

Next steps

Learn more in Meta App Development.

Enabling Facebook login

You must enable Facebook login for your application if it's not enabled already.

Steps

1. Go to Facebook for Developers.
2. At the top of the page, click **My Apps**, and then select the appropriate app.
3. On the left side of the page, click **Products**
4. Locate the **Facebook login** card and click **Set up**.

Copyright © 2025 Ping Identity Corporation

5. Follow the instructions to set up Facebook login.

Adding Facebook as an identity provider in PingOne

Configure the IdP connection in PingOne.

Before you begin

Ensure that registration is enabled in the appropriate authentication policy. Learn more in Editing an authentication policy.

You should have the following information ready:

- App ID
- App secret

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and click **+**.
2. Click **Facebook**.
3. Click **Next**.
4. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.

     > **Note**
     > You can't change the **Icon** and **Sign-on button** in accordance with the provider's brand standards.
5. Click **Next**.
6. Configure the connection and enter the following information:
   - **App ID**: The application ID that you copied earlier from the IdP. You can find this information on the **Basic settings** page in the Facebook for Developers portal.
   - **App Secret**: The application secret that you copied earlier from the IdP. You can find this information on the **Basic settings** page on the Facebook for Developers portal.
   - **Callback URL**: Copy the **Callback URL** to a secure location. You'll provide this value to the IdP later.
7. Click **Next**.
8. Define how the PingOne user attributes are mapped to IdP attributes. Learn more in Mapping attributes.
   - Enter the PingOne user profile attribute and the external IdP attribute. Learn more about attribute syntax in Identity provider attributes.
   - To add an attribute, click **+ Add**.

Copyright © 2025 Ping Identity Corporation

- To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
- Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
  - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
  - **Always**: Always update the PingOne directory attribute.

9. Click **Save**.
10. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
> You can disable the IdP by clicking the toggle to the left (gray).

Adding the callback URL to Facebook for Developers

Copy the callback URL from the PingOne admin console and paste it in the Facebook for Developers login settings.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and browse or search for the appropriate IdP.
2. Click the IdP to open the details panel.
3. On the **Connection** tab, copy the **Callback URL** to a secure location.
4. Go to Facebook for Developers.
5. At the top of the page, click **My Apps**, and then select the appropriate app.
6. Go to **Facebook Login** > **Settings**.
7. For **Valid OAuth Redirect URIs**, paste the value that you copied from the PingOne admin console.

Next steps

- Add the IdP to your authentication policy.
- Apply the authentication policy to your application.

Adding an identity provider - GitHub

Adding GitHub as an external identity provider (IdP) gives your users the option to sign on with GitHub when accessing your application.

Before you begin

Ensure that you have:

- A PingOne organization with an environment added. Learn more in Starting a PingOne trial.
- Added your application to PingOne. Learn more in Adding an application.

Copyright © 2025 Ping Identity Corporation

- A GitHub account.

Creating your application on GitHub

Before you can set up GitHub as an external IdP, you must create an application on GitHub. GitHub generates a client ID and client secret for the application. Learn more in Creating an OAuth app in the GitHub documentation.

Steps

1. Go to GitHub and sign on to your account.

   If you don't have a GitHub account, you can create one now.

2. In the upper right, click your profile photo, and then click **Settings**.
3. On the left, click **Developer Settings**.
4. On the left, click **OAuth Apps**.
5. Click the **New OAuth App** button.

   > **Note**
   >
   > If you haven't created an app before, you'll see the button as **Register a new application**.

6. Enter the following:
   - **Application name**: The display name for the application.
   - **Homepage URL**: The full URL to your application home page.
   - **Application description**: A description for your application that all users will see.
   - **Authorization callback URL**: The path in your application that users are redirected to after they have authenticated with GitHub. Leave this value blank for now.
7. Leave the GitHub page open to return later and enter the `Authorization callback URL` after you have created the application in PingOne.

Adding GitHub as an identity provider in PingOne

Configure the IdP connection in PingOne.

Before you begin

Ensure that registration is enabled in the authentication policy you want to use. Learn more in Editing an authentication policy.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and click **+**.
2. Click **GitHub**.
3. Click **Next**.

Copyright © 2025 Ping Identity Corporation

4. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.

   > **Note**
   > You can't change the **Icon** and **Sign-on Button** in accordance with the provider's brand standards.

5. Click **Next**.
6. Copy the value for **Callback URL** to a secure location.
7. Leave the PingOne page open to return and enter the `Client ID` and `Client Secret` after you have created the application on GitHub.

Finishing creating the application on GitHub

Add the callback URL from the PingOne admin console to your application on GitHub.

Before you begin

Ensure you have copied the **Callback URL** from PingOne.

Steps

1. Go to the **Register a new OAuth application** page on GitHub.
2. For **Authorization callback URL**, enter the value for **Callback URL** that you copied from PingOne.
3. Click **Register application**.

Finishing adding the identity provider in PingOne

After you have registered the application with GitHub, copy the values for client ID and client secret and enter them into PingOne.

Before you begin

Ensure that you have copied the values for client ID and client secret from GitHub.

Steps

1. Return to GitHub and, in the **OAuth Apps** section, select the appropriate application.
2. Locate the **Client ID** and **Client Secret** and copy the values to a secure location.
3. In the PingOne admin console, configure the connection and enter the following information:
   - **Client ID**: The application identifier that you copied from the IdP. You can find this information on GitHub.
   - **Client Secret**: The application secret that you copied from the IdP. You can find this information on GitHub.
   - **Callback URL**: The URL to which the user will be redirected after authenticating.

Copyright © 2025 Ping Identity Corporation

4. Click **Next**.
5. Define how the PingOne user attributes are mapped to IdP attributes. Learn more in Mapping attributes.
    - Enter the PingOne user profile attribute and the external IdP attribute. Learn more about attribute syntax in Identity provider attributes.
    - To add an attribute, click **+ Add**.
    - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
    - Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
        - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
        - **Always**: Always update the PingOne directory attribute.

        You can map the following attributes provided by GitHub:
    - `Avatar URL`
    - `Blog`
    - `Company`
    - `Email`
    - `HTML URL`
    - `User ID`
    - `Location`
    - `Login`
    - `Name`
    - `Node ID`
    - `Site Admin`
    - `Type`
    - `URL`
6. Click **Save**.
7. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
>
> You can disable the IdP by clicking the toggle to the left (gray).

Next steps

- Add the IdP to your authentication policy.
- Add the authentication policy to your application.

Copyright © 2025 Ping Identity Corporation

Adding an identity provider - Google

Adding Google as an external identity provider (IdP) gives your users the option to sign on with Google when accessing your application.

Before you begin

Ensure that you have:

- A PingOne organization with an environment added. Learn more in Starting a PingOne trial.
- Added your application to PingOne. Learn more in Adding an application.
- A Google account.

Registering the application with Google

When you register your application, Google generates an app ID and app secret for the application. You'll need these values to connect the application to PingOne.

Steps

1. Go to the Google API Console.

   If you haven't created a Google account, you can do so now.

2. In the **Projects** list, select a project or create a new one.
3. On the left, click **Credentials**.
4. Click **Create credentials**, then select **OAuth client ID**.

   If you are prompted to configure an OAuth consent screen with information about your application, you can do that now.

5. Select the appropriate application type for your project and enter the following information:
   - **Name**: The name of the OAuth client ID, not the display name of the application.
   - **Authorized JavaScript origins**: The origin URI of the client application, for use with requests from a browser.
   - **Authorized redirect URIs**: (Leave this value blank for now.) The path in your application that users are redirected to after they have authenticated with Google.
6. Click **Create**.
7. On the **OAuth client** page, copy the client ID and client secret to a secure location.

   You can always access the client ID and client secret from the **Credentials** page in the API Console.

Next steps

Learn more in Setting up OAuth 2.0 in Google's API Console Help documentation.

Enabling the Google People API

You must enable the Google People API if it's not enabled already.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to the Google API Console.
2. In the **Projects** list, select a project or create a new one.
3. On the left, click **Library**.
4. Locate the **People API**.

   > **Tip**
   > If you need help finding the API, use the search field.

5. Click **Enable**.

Next steps

Learn more in Enable and disable APIs in Google's API Console Help documentation.

Adding Google as an identity provider in PingOne

Configure the IdP connection in PingOne.

Before you begin

Ensure that registration is enabled in the authentication policy. Learn more in Editing an authentication policy.

You should have the following information ready:

- Client ID
- Client secret

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and click **+**.
2. Click **Google**.
3. Click **Next**.
4. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.

     > **Note**
     > You can't change the **Icon** and **Sign-on Button** in accordance with the provider's brand standards.

5. Click **Next**.

Copyright © 2025 Ping Identity Corporation

6. Configure the connection and enter the following information:
   - **Client ID**: The application ID that you copied earlier from the IdP. You can find this information on the **Credentials** page on the Google Developers site.
   - **Client secret**: The application secret that you copied earlier from the IdP. You can find this information on the **Credentials** page on the Google Developers site.
   - **Callback URL**: Copy the **Callback URL** to a secure location. You'll provide this value to the IdP later.
7. Click **Next**.
8. Define how the PingOne user attributes are mapped to IdP attributes. Learn more in Mapping attributes.
   - Enter the PingOne user profile attribute and the external IdP attribute. Learn more about attribute syntax in Identity provider attributes.
   - To add an attribute, click **+ Add**.
   - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
   - Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
     - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
     - **Always**: Always update the PingOne directory attribute.
9. Click **Save**.
10. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
>
> You can disable the IdP by clicking the toggle to the left (gray).

Adding the callback URL to the Google API Console

Copy the callback URL from the PingOne admin console and paste it in the Google API Console.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and browse or search for the appropriate IdP.
2. Click the IdP to open the details panel.
3. On the **Connection** tab, copy the **Callback URL** to a secure location.
4. Go to the Google API Console.
5. In the **Projects** list, select the appropriate project.
6. Click **Credentials**.
7. In the **Application** list, click the appropriate application.

Copyright © 2025 Ping Identity Corporation

8. In the **Authorized redirect URIs** section, click **Add URI**, and paste the value that you copied from the PingOne admin console.

Next steps

- Add the IdP to your authentication policy.
- Apply the authentication policy to your application.

Adding an identity provider - LinkedIn

Adding LinkedIn as an external identity provider (IdP) allows your users to sign on with LinkedIn when accessing your application.

Before you begin

Ensure that you have:

- A PingOne organization with an environment added. Learn more in Starting a PingOne trial.
- Added your application to PingOne. Learn more in Adding an application.
- A LinkedIn account.

Registering the application with LinkedIn

LinkedIn generates a client ID and client secret for your application. You'll need these values to connect the application to PingOne.

Steps

1. Go to the LinkedIn Developers page.
2. Click **Create app**.

   You'll be prompted to sign on to your LinkedIn account.
3. Enter the following information:
   - **App name**: A unique name for the application. It must be fewer than 50 characters.
   - **LinkedIn Page**: The LinkedIn company page to be associated with your application.
   - **App logo**: The logo users see when they authenticate to your application.
4. Click **Create app**.
5. On the **Product** tab, locate **Sign In with LinkedIn using OpenID Connect** in the list of products and click **Request access**.
6. On the **Auth** tab, copy the **Client ID** and **Primary Client Secret** to a secure location.
7. In the **OAuth 2.0 Settings** section, you'll see an empty field for **Redirect URLs**, which is the path in your application that users are redirected to after they have authenticated with LinkedIn. Leave this value blank for now.

Learn more

Learn more in Sign in with LinkedIn using OpenID Connect in the Microsoft LinkedIn documentation.

Copyright © 2025 Ping Identity Corporation

Adding LinkedIn as an identity provider in PingOne

Configure the IdP connection in PingOne.

Before you begin

Ensure that registration is enabled in the authentication policy. Learn more in Editing an authentication policy.

You should have the following information ready:

- Client ID
- Client secret

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and click **+**.
2. Click **LinkedIn**.
3. Click **Next**.
4. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the identity provider.

     > **Note**
     > You can't change the **Icon** and **Sign-on button** in accordance with the provider's brand standards.
5. Click **Next**.
6. Configure the connection and enter the following information:
   - **Client ID**: The client ID that you copied earlier from the IdP. You can find this information on the **Auth** page on the LinkedIn Developers page.
   - **Client secret**: The application secret that you copied earlier from the IdP. You can find this information on the **Auth** tab on the LinkedIn Developers page.
   - **Callback URL**: Copy the **Callback URL** to a secure location. You'll provide this value to the IdP later.
7. Click **Next**.
8. Define how the PingOne user attributes are mapped to identity provider attributes. Learn more in Mapping attributes.
   - Enter the PingOne user profile attribute and the external IdP attribute. Learn more about attribute syntax in Identity provider attributes.
   - To add an attribute, click **+**.
   - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.

Copyright © 2025 Ping Identity Corporation

- Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
  - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
  - **Always**: Always update the PingOne directory attribute.

9. Click **Save**.
10. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
> You can disable the IdP by clicking the toggle to the left (gray).

Adding the callback URL to the LinkedIn Developer page

Copy the callback URL from the PingOne admin console and paste it into the LinkedIn Developers page.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and browse or search for the appropriate IdP.
2. Click the IdP to open the details panel.
3. Click the **Connection** tab.
4. Copy the **Callback URL** to a secure location.
5. Go to the LinkedIn Developers page.
6. In the **My Apps** list, select the appropriate application.
7. On the **Auth** tab, click the **Pencil** icon in the **OAuth 2.0 settings** section.
8. Click **+ Add redirect URL**.
9. Paste the callback URL that you copied from the PingOne admin console.
10. Click **Update**.

Next steps

- Add the IdP to your authentication policy.
- Apply the authentication policy to your application.

Adding an identity provider - LinkedIn (legacy)

Adding LinkedIn as an external identity provider (IdP) allows your users to sign on with LinkedIn when accessing your application.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> The legacy LinkedIn IdP has been deprecated, so you might be unable to connect with LinkedIn using a legacy connection. Consider using the OpenID Connect (OIDC)-based LinkedIn IdP connection. Learn more in Adding an identity provider - LinkedIn.

Before you begin

Ensure that you have:

- A PingOne organization with an environment added. Learn more in Starting a PingOne trial.
- Added your application to PingOne. Learn more in Adding an application.
- A LinkedIn account.

Registering the application with LinkedIn

LinkedIn generates a client ID and client secret for your application. You'll need these values to connect the application to PingOne.

Steps

1. Go to the LinkedIn Developers page.
2. Click **Create app**.

   You'll be prompted to sign on to your LinkedIn account.
3. Enter the following information:
   - **App name**: A unique name for the application. It must be fewer than 50 characters.
   - **LinkedIn Page**: The LinkedIn company page to be associated with your application.
   - **App logo**: The logo users see when they authenticate to your application.
4. Click **Create app**.
5. On the **Auth** tab, copy the **Client ID** and **Primary Client Secret** to a secure location.
6. In the **OAuth 2.0 Settings** section, you'll see an empty field for **Redirect URLs**, which is the path in your application that users are redirected to after they have authenticated with LinkedIn. Leave this value blank for now.

Learn more

Learn more in Sign in with LinkedIn in the Microsoft LinkedIn documentation.

Copyright © 2025 Ping Identity Corporation

Adding LinkedIn as an identity provider in PingOne

Configure the IdP connection in PingOne.

Before you begin

Ensure that registration is enabled in the authentication policy. Learn more in Editing an authentication policy.

You should have the following information ready:

- Client ID
- Client secret

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and click **+**.
2. Click **LinkedIn (Legacy)**.
3. Click **Next**.
4. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the identity provider.

     > **Note**
     > You can't change the **Icon** and **Sign-on button** in accordance with the provider's brand standards.
5. Click **Next**.
6. Configure the connection and enter the following information:
   - **Client ID**: The client ID that you copied earlier from the IdP. You can find this information on the **Auth** page on the LinkedIn Developers page.
   - **Client secret**: The application secret that you copied earlier from the IdP. You can find this information on the **Auth** tab on the LinkedIn Developers page.
   - **Callback URL**: Copy the **Callback URL** to a secure location. You'll provide this value to the IdP later.
7. Click **Next**.
8. Define how the PingOne user attributes are mapped to identity provider attributes. Learn more in Mapping attributes.
   - Enter the PingOne user profile attribute and the external IdP attribute. Learn more about attribute syntax in Identity provider attributes.
   - To add an attribute, click **+**.

Copyright © 2025 Ping Identity Corporation

- To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
- Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
  - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
  - **Always**: Always update the PingOne directory attribute.

9. Click **Save**.
10. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
> You can disable the IdP by clicking the toggle to the left (gray).

Adding the callback URL to the LinkedIn Developer page

Copy the callback URL from the PingOne admin console and paste it into the LinkedIn Developers page.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and browse or search for the appropriate IdP.
2. Click the IdP to open the details panel.
3. Click the **Connection** tab.
4. Copy the **Callback URL** to a secure location.
5. Go to the LinkedIn Developers page.
6. In the **My Apps** list, select the appropriate application.
7. On the **Auth** tab, click the **Pencil** icon in the **OAuth 2.0 settings** section.
8. Click **+ Add redirect URL**.
9. Paste the callback URL that you copied from the PingOne admin console.
10. Click **Update**.

Next steps

- Add the IdP to your authentication policy.
- Apply the authentication policy to your application.

Copyright © 2025 Ping Identity Corporation

Adding an identity provider - Microsoft

Adding Microsoft as an external identity provider (IdP) gives your users the option to sign on with their Microsoft accounts when accessing your application. Learn more in OIDC authentication.

To connect PingOne as the external authentication provider for multi-factor authentication (MFA) in Microsoft Entra ID, you'll need to add a Microsoft identity provider. Learn more in Entra ID external authentication method.

OIDC authentication

Adding Microsoft as an external identity provider (IdP) gives your users the option to sign on with their Microsoft accounts when accessing your application.

Registering your application with Microsoft

Register an application in Microsoft Entra. Learn more in Quickstart: Register an application with the Microsoft identity platform in the Microsoft Entra documentation.

Before you begin

Ensure that you have:

- A Microsoft Entra account with an active subscription
- An Entra tenant

Steps

1. Go to the Microsoft Entra admin center and sign on to your account.

   If you don't have a Microsoft Entra account, you can create one now.

2. On the left, expand **Identity** > **Applications**.
3. Click **App registrations**.
4. At the top, click **New registration**.
5. In the **Name** field, enter a user-facing display name for the application.
6. For **Supported account types**, select **Accounts in this organizational directory only (Ping Identity only - Single tenant)** or **Accounts in any organizational directory and personal Microsoft accounts**, depending on the needs of your organization.

   Select the **Single tenant** option if you're working with only identities from your environment.

7. Under **Redirect URI**, select **Web** as the platform and enter the authorization URL of your PingOne environment.

Copyright © 2025 Ping Identity Corporation

> **Tip**
>
> You can find this URL on the **Overview** tab of any OIDC application in the PingOne admin console in the **Connection Details** section.

The format is `<issuer>/authorize`.

Example 1: `https://auth.pingone.<region>/<envID>/as/authorize`

Example 2: `https://<customDomain>/as/authorize` if you set up a custom domain. Learn more in Setting up a custom domain.

8. Click **Register**.

Enabling the implicit grant

After registering an application in Entra, enable the implicit grant type for your application.

Steps

1. Go to the Microsoft Entra admin center.
2. In the **App registrations** section, select your application.
3. Go to **Manage** > **Authentication**.
4. In the **Implicit grant and hybrid flows** section, select the **ID tokens** checkbox.
5. Click **Save**.

Getting the client ID and client secret for your application

When you register your application with Microsoft, Microsoft generates an application (client) ID and application secret for the application.

You'll copy these values and enter them into PingOne.

Steps

1. Go to the Microsoft Entra admin center.
2. In the **App registrations** section, select your application.
3. On the left, click **Certificates & secrets**.
4. In the **Client secrets** section, click **+ New client secret**.

Copyright © 2025 Ping Identity Corporation

5. Enter the following:
    1. **Description**: A brief description of the client secret.
    2. **Expires**: Select the duration of the certificate, based on the needs of your organization.
6. Click **Add**.
7. In the **Client secrets** section, locate the value for the applicable secret and copy it to a secure location.
8. On the left, click **Overview**.
9. Locate the **Application (client) ID** and copy it to a secure location.

Setting up API permissions

Adding Microsoft as an external IdP requires certain API permissions that you'll need to enable in your application.

Steps

1. Go to the Microsoft Entra admin center.
2. In the **App registrations** section, select your application.
3. On the left, click **API permissions**.
4. Click **+ Add a permission**.
5. Click **Microsoft Graph**.
6. Click **Delegated permissions** and expand **Openid permissions**.
7. Select the following:
    - `email`
    - `offline_access`
    - `openid`
    - `profile`
    - `User.Read`

    > **Note**
    >
    > `User.Read` is included by default and should remain selected.

8. Click **Add permissions**.

Copyright © 2025 Ping Identity Corporation

Adding Microsoft as an identity provider in PingOne

Configure the IdP connection in PingOne.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs**.
2. Click **+**.
3. Click **Microsoft**.
4. Click **Next**.
5. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.

     > **Note**
     > You can't change the **Icon** and **Sign-on button**, in accordance with the provider's brand standards.
6. Click **Next**.
7. On the **Configure IDP Connection** page, enter the following information:
   - **Client ID**: The application ID from the IdP that you copied earlier. You can find this information on the Microsoft Entra admin center.
   - **Client secret**: The application secret from the IdP that you copied earlier. You can find this information on the Microsoft Entra admin center.
   - **Callback URL**: Copy the **Callback URL** to a secure location. You'll provide this value to the IdP later.
8. Click **Next**.
9. Define how the PingOne user attributes are mapped to IdP attributes. Learn more in Mapping attributes.
   - Leave the default PingOne user profile attributes and the external IdP attributes:
     - **Preferred Username** (from Microsoft) as the source of the PingOne **Username**
     - **Email** (from Microsoft) as the source of the PingOne **Email Address**
   - To add an attribute, click **+ Add**.
   - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.

Copyright © 2025 Ping Identity Corporation

- Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
  - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
  - **Always**: Always update the PingOne directory attribute.

10. Click **Save**.
11. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
> You can disable the IdP by clicking the toggle to the left (gray).

Adding the callback URL to the Microsoft Entra admin

Add the callback URL from the Microsoft IdP connection to the application you registered in the Microsoft Entra admin center.

Steps

1. In the PingOne admin console, go to **Integrations > External IdPs** and locate the Microsoft IdP that you created previously.
2. Click the IdP to open the details panel.
3. Click the **Connection** tab.
4. Copy the **Callback URL**.

   The following examples show the URL format:

   Example 1: `https://auth.pingone.<region>/<envID>/rp/callback/microsoft`

   Example 2: `https://<customDomain>/rp/callback/microsoft`
5. Go to the Microsoft Entra admin center.
6. In the **App registrations** section, select your application.
7. On the left, click **Authentication**.
8. Go to **Platform configurations > Web > Redirect URIs**, and click **Add URI**.
9. Paste the **Callback URL** that you copied from the PingOne admin console.
10. Click **Save**.

Next steps

- Add the Microsoft IdP to an authentication policy followed by an MFA step.

Copyright © 2025 Ping Identity Corporation

- Ensure that registration is enabled in the authentication policy. Learn more in Authentication policies and Add the authentication policy to your application.

Entra ID external authentication method

To connect PingOne as the external authentication provider for multi-factor authentication (MFA) in Entra ID, you must add a Microsoft identity provider (IdP). Learn more about configuring Entra ID as the IdP in Setting up PingOne SSO and PingID as the external MFA provider for Microsoft Entra ID.

Adding an identity provider - PayPal

Adding PayPal as an external identity provider (IdP) gives your users the option to sign on with PayPal when accessing your application.

Before you begin

Ensure that you have:

- A PingOne organization with an environment added. Learn more in Starting a PingOne trial.
- Added your application to PingOne. Learn more in Adding an application.
- A Paypal account

Registering your application with PayPal

Create your application with PayPal, and then copy the client ID and client secret.

Before you begin

Ensure that you have a PayPal account with an active subscription.

Steps

1. Go to PayPal for Developers and sign on to your account.

   If you don't have a PayPal account, you can create one now.

2. In the **My apps and credentials** section, click **Sandbox**.
3. In the **Rest API apps** section, click **Create app**.
4. In the **Application details** field, enter a name for the application, and then click **Create app**.
5. In the **Sandbox API credentials** section, copy the **Client ID** to a secure location.
6. In the **Secret** section, click **Show**.
7. Copy the client secret to a secure location.
8. In the **App feature options** section, select **Connect with PayPal**.

   You can clear the other options, unless your organization has a specific need for them.

Copyright © 2025 Ping Identity Corporation

9. Click **Save**.

Configuring scopes and options

On the PayPal for Developers site, configure the options for scope attributes, permissions, and customer consent.

Steps

1. Go to PayPal for Developers.
2. In the **Rest API apps** section, click your application name.
3. In the **Connect with PayPal** section, click **Advanced options**.
4. Select the following scope attributes:
   - `Full name`
   - `Email`
   - `Street address`
   - `City`
   - `State`
   - `Country`
   - `Postal code`
   - `Account verification status`
   - `PayPal account ID`
5. Under **Links shown on customer consent page**, enter the following:
   - **Privacy policy URL**: (Optional). The location of your organization's privacy policy.
   - **User agreement URL**: (Optional). The location of your organization's user agreement.
6. In the **Additional PayPal permissions** section, select **Enable customers who have not yet confirmed their email with PayPal to log in to your app**.
7. Click **Save**.

Adding PayPal as an identity provider in PingOne

Configure the IdP connection in PingOne.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and click **+**.
2. Click **PayPal**.
3. Click **Next**.

Copyright © 2025 Ping Identity Corporation

4. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.

     > **Note**
     > You can't change the **Icon** and **Sign-on Button** in accordance with the provider's brand standards.

5. Click **Next**.
6. Configure the connection and enter the following information:
   - **Client ID**: The application ID from the IdP that you copied earlier. You can find this information on the PayPal for Developers site.
   - **Client secret**: The application secret from the IdP that you copied earlier. You can find this information on the PayPal for Developers site.
   - **Environment**: The environment the configuration connects to. Click **live** or **sandbox**
   - **Callback URL**: Copy the **Callback URL** to a secure location. You'll provide this value to the IdP later.
7. Click **Next**.
8. Define how the PingOne user attributes are mapped to identity provider attributes. Learn more in Mapping attributes.
   - Enter the PingOne user profile attribute and the external IdP attribute. Learn more about attribute syntax in Identity provider attributes.
   - To add an attribute, click **+ Add**.
   - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
   - Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
     - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
     - **Always**: Always update the PingOne directory attribute.
9. Click **Save**.
10. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

    > **Note**
    > You can disable the IdP by clicking the toggle to the left (gray).

Registering the callback URL with PayPal

Copy the callback URL value from the PingOne admin console and enter it into the PayPal for Developers site.

Copyright © 2025 Ping Identity Corporation

Before you begin

Ensure that you have the callback URL from the PingOne admin console.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and browse or search for the appropriate IdP.
2. Click the IdP to open the details panel.
3. Click the **Connection** tab.
4. Copy the **Callback URL** and paste it in a secure location.
5. Go to PayPal for Developers.
6. In the **Rest API apps** section, click your application name.
7. In the **Sandbox app settings** section, locate **Return URL**.
8. Click **Show**.
9. For **Return URL**, enter the callback URL value that you copied from the PingOne admin console.
10. Click **Save**.

Next steps

- Add the IdP to your authentication policy.
- Apply the authentication policy to your application and ensure that registration is enabled in the authentication policy.

Adding an identity provider - X

Adding X as an external identity provider (IdP) gives your users the option to sign on with X when accessing your application.

Before you begin

Ensure that you have:

- A PingOne organization with an environment added. Learn more in Starting a PingOne trial.
- Added your application to PingOne. Learn more in Adding an application.
- An X account

Registering the application with X

To enable signing on with X, you must register your application with X.

Steps

1. Go to the X Developer site and sign on to your account.

   If you haven't created an X Developer account, you can do so now.

2. Click **Create an app**.

Copyright © 2025 Ping Identity Corporation

3. Enter the appropriate information.
4. Select **Enable sign in with X**.
5. Click **Create**.

Enabling email communication

Enable email communication to retrieve a user's email address from X.

Steps

1. Go to the X Developer site.
2. Select your application.
3. Click **Edit**, then click **Edit details**.
4. On the **Permissions** tab, click **Edit**.
5. Enable the **Request email addresses from users** option.
6. Click **Save**.

Getting the API key and API secret

When you register your application, X generates an API key to identify the application.

Steps

1. Go to the X Developer site.
2. Select your application.
3. On the **Keys and tokens** tab, copy the following values to a secure location:
    - **API key**: The consumer key that identifies the application.
    - **API secret key**: The consumer secret that secures the application.

Adding X as an identity provider in PingOne

Configure the IdP connection in PingOne.

Before you begin

Ensure that registration is enabled in the authentication policy. Learn more in Editing an authentication policy.

You should have the following information ready:

- API key
- API secret key

Learn more in Adding an identity provider - X.

Copyright © 2025 Ping Identity Corporation

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and click **+**.
2. Click **X**.
3. Click **Next**.
4. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.

     > **Note**
     > You can't change the **Icon** and **Sign-on Button** in accordance with the provider's brand standards.
5. Click **Next**.
6. Configure the connection and enter the following information:
   - **API key**: The consumer key that you copied earlier from the IdP. You can find this information on the X Developer site.
   - **API secret key**: The consumer secret that you copied earlier from the IdP. You can find this information on the X Developer site.
   - **Callback URL**: Copy the **Callback URL** to a secure location. You'll provide this value to the IdP later.
7. Click **Next**.
8. Define how the PingOne user attributes are mapped to IdP attributes. Learn more in Mapping attributes.
   - Enter the PingOne user profile attribute and the external IdP attribute. Learn more about attribute syntax in Identity provider attributes.
   - To add an attribute, click **+ Add**.
   - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
   - Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
     - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
     - **Always**: Always update the PingOne directory attribute.
9. Click **Save**.
10. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

Copyright © 2025 Ping Identity Corporation

> **Note**
> You can disable the IdP by clicking the toggle to the left (gray).

Adding the callback URL to the X Developer site

Copy the callback URL from the PingOne admin console and paste it in the X Developer site.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and browse or search for the appropriate IdP.
2. Click the IdP to open the details panel.
3. On the **Connection** tab, copy the **Callback URL** to a secure location.
4. On the X Developer site, select your application.
5. On the **App details** tab, for **Callback URL**, paste the value that you copied earlier.
6. Click **Save**.

Next steps

- Add the IdP to your authentication policy.
- Apply the authentication policy to your application.

Adding an identity provider - Yahoo

Adding Yahoo as an external identity provider (IdP) gives your users the option to sign on with Yahoo when accessing your application.

Before you begin

Ensure that you have:

- A PingOne organization with an environment added. Learn more in Starting a PingOne trial.
- Added your application to PingOne. Learn more in Adding an application.
- A Yahoo account

Creating the application with Yahoo

To enable signing on with Yahoo, create the application on the Yahoo Developers page. Yahoo generates a client ID and client secret to identify the application. Learn more in Getting Started in the OpenID Connect section of the Yahoo Developer site.

Steps

1. Go to the Yahoo Developer site and sign on to your account.

   If you haven't created a Yahoo Developer account, you can do so now.

2. Click the **Create an App** button.

Copyright © 2025 Ping Identity Corporation

3. Enter a name for the application.
4. For **Application type**, select **Web application**.
5. Leave **Redirect URI** blank for now.

   You will get this value from PingOne and enter it later.
6. In the **API Permissions** section, select **OpenID Connect Permissions**, and then select **Email** and **Profile**.
7. Leave the page open so you can return later to enter the **Redirect URI**.

Adding Yahoo as an identity provider in PingOne

Configure the IdP connection in PingOne.

Before you begin

Ensure that registration is enabled in the authentication policy. Learn more in Editing an authentication policy.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and click **+**.
2. Click **Yahoo**.
3. Click **Next**.
4. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.

     > **Note**
     > You can't change the **Icon** and **Sign-on Button** in accordance with the provider's brand standards.
5. Click **Next**.
6. Copy the value for **Callback URL** to a secure location.
7. Leave the page open so you can return later to enter the values for **Client ID** and **Client secret**.

Finishing creating the application with Yahoo

Add the callback URL from the PingOne admin console to your Yahoo application.

Before you begin

Ensure you have the callback URL from the PingOne admin console that you copied in Adding an identity provider - Yahoo.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to the Yahoo Developers page.
2. For **Callback URL**, enter the value that you copied from the PingOne admin console on the **Configure Connection** page.
3. Click **Create App**.

Finishing adding the identity provider in PingOne

After you have created the application with Yahoo, copy the values for client ID and client secret and enter them into PingOne.

Steps

1. Go to the Yahoo Developers page.
2. Copy the values for **Client ID** and **Client Secret** to a secure location.
3. In the PingOne admin console, finish configuring the Yahoo connection and enter the following information:
   - **Client ID**: The application ID that you copied from the IdP. You can find this information on the Yahoo Developers site.
   - **Client Secret**: The application secret that you copied from the IdP. You can find this information on the Yahoo Developers site.
   - **Callback URL**: The URL to which the user will be redirected after authenticating.
4. Click **Next**.
5. Define how the PingOne user attributes are mapped to IdP attributes. Learn more in Mapping attributes.
   - Enter the PingOne user profile attribute and the external IdP attribute. Learn more about attribute syntax in Identity provider attributes.
   - To add an attribute, click **+ Add**.
   - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
   - Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
     - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
     - **Always**: Always update the PingOne directory attribute.

       You can map the following attributes provided by Yahoo:

       - `sub`
       - `name`
       - `given_name`
       - `family_name`
       - `email`

Copyright © 2025 Ping Identity Corporation

- `picture`
- `nickname`
- `locale`

6. Click **Save**.
7. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
> You can disable the IdP by clicking the toggle to the left (gray).

Next steps

- Add the IdP to your authentication policy.
- Apply the authentication policy to your application.

Adding an identity provider - OIDC

You can use the generic OpenID Connect (OIDC) configuration to add any external identity provider (IdP) that follows the OIDC standard.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and click **+**.
2. Click **OpenID Connect**.
3. Click **Next**.
4. On the **Add External Identity Provider** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.
   - **Icon** (optional): An image to represent the IdP. Use a file up to 1 MB in JPG, JPEG, GIF, or PNG format. Use a 90 x 90 pixel image.
   - **Sign-on button** (optional): An image to use for the login button displayed to the end user. Use a 300 x 42 pixel image.
5. Click **Next**.
6. Enter the **Connection Details**:
   - **Client ID**: The application ID that is generated by the external IdP to which you are connecting.
   - **Client secret**: The application secret that is generated by the external IdP to which you are connecting.

Copyright © 2025 Ping Identity Corporation

- **Callback URL**: Copy the **Callback URL** to a secure location. You'll provide this value to the IdP later.

7. Enter the **Discovery Details**:

   - **Discovery document URI** (optional): The discovery endpoint from the external IdP. Enter the URL and then click **Use Discovery document** to populate the remaining settings in **Discovery Details** automatically. Learn more in Discovery document URI.
   - **Issuer**: The issuer to which the authentication is sent for the external IdP. This URL must use the `https` protocol.
   - **JWKS endpoint**: The URL that specifies the JSON Web Key Set (JWKS) endpoint for the external IDP. The JWKS endpoint includes public keys that can be used to verify JSON Web Keys (JWKs) from the IdP. This URL must use the `https` protocol.
   - **Authorization endpoint**: The URL that specifies the authorization endpoint for the external IdP. The client requests an authorization grant from the authorization endpoint. This URL must use the `https` protocol.
   - **Token endpoint**: The URL that specifies the token endpoint for the external IdP. The client presents its authorization grant to the token endpoint to obtain an access token and a refresh token when needed. This URL must use the `https` protocol.
   - **User information endpoint** (optional): The URL that specifies the `userInfo` endpoint for the external IdP. The client can present an access token to the `userInfo` endpoint to retrieve additional information about the user, including attributes. Clients can use this endpoint to retrieve profile information, preferences, and other user-specific information. This URL must use the `https` protocol.
   - **Token endpoint authentication method**: The authentication method to use for authenticating the external IdP. Select **None**, **Client Secret Basic**, or **Client Secret Post**.
   - **Requested scopes**: The scopes to include in the authentication request to the external IdP. Scope values are case sensitive. You can provide multiple scopes by separating them with a space.
   - **Proof Key for Code Exchange (PKCE)**: Select to use PKCE to secure communication with the IdP and help prevent authorization code interception attacks.

     This option is selected by default if **Discovery document URI** is configured and if the metadata from the provider includes the following:

     ```
     "code_challenge_methods_supported": [
     "plain",
     "S256"
     ]
     ```

     If **Discovery document URI** is not configured, or if the `code_challenge_methods_supported` metadata from the provider does not include `S256`, this option is cleared by default.

     Learn more about PKCE in RFC7636: Proof Key for Code Exchange by OAuth Public Clients on the Internet Engineering Task Force (IETF) website.

8. Click **Next**.

Copyright © 2025 Ping Identity Corporation

9. Define how the PingOne user attributes are mapped to IdP attributes. Learn more in Mapping attributes.
    - Enter the PingOne user profile attribute and the external IdP attribute. Learn more about attribute syntax in Identity provider attributes.
    - To add an attribute, click **+ Add**.
    - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
    - Select the update condition, which determines how PingOne updates its user directory with the values from the IdP:
        - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
        - **Always**: Always update the PingOne directory attribute.
10. Click **Save**.
11. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
>
> You can disable the IdP by clicking the toggle to the left (gray).

Next steps

Add the IdP to your authentication policy.

Discovery document URI

The Discovery document URI is a discovery endpoint that identifies the location of the OpenID Provider (OP), as well as metadata about its configuration. You can use the Discovery document URI to populate the configuration for the OP in PingOne.

The Discovery document URI has the following format:

```
<OpenID Provider's issuer value>/.well-known/openid-configuration
```

The URL must start with https:// according to the OpenID Connect (OIDC) Discovery 1.0 specification. Learn more in the OIDC documentation.

For example:

```
https://www.example.com/.well-known/openid-configuration
```

```
←---- OP issuer ----→←----- Spec defined path -----→
```


Copyright © 2025 Ping Identity Corporation

> **Tip**
>
> If you are connecting to PingOne DaVinci as an external identity provider, the discovery endpoint is one of the following, depending on whether you have a custom domain:
>
> ***Custom domain***
>
> `https://<customDomain>/davinci/.well-known/openid-configuration`
>
> ***Default domain***
>
> `https://auth.pingone.<region>/<envID>/davinci/.well-known/openid-configuration`

Learn more in Domains.

Adding an identity provider - SAML

You can use the generic SAML configuration to add an external identity provider (IdP) that follows the SAML standard.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and click **+**.
2. Click **SAML**.
3. Click **Next**.
4. On the **Create Profile** page, enter the following information:
   - **Name**: A unique identifier for the IdP.
   - **Description** (optional): A brief description of the IdP.
   - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.
   - **Sign-on Button** (optional): An image to be used for the sign-on button that the end user will see. Use a 300 x 42 pixel image.
   - **Icon** (optional): An image to represent the IdP. Use a file up to 1MB in JPG, JPEG, GIF, or PNG format.
5. Click **Next**.
6. On the **Configure PingOne Connection** page, enter the following:
   - **PingOne (SP) Entity ID**: The entity ID for the service provider (SP), which is used as the `Issuer` when PingOne sends a request to the external IdP. The IdP can also use this value to ensure that requests from the SP are valid. By default, this ID is based on the value you entered for **Name**.
   - **ACS Endpoint**: Shows the Assertion Consumer Service (ACS) URL. The ACS endpoint is where the single sign-on (SSO) tokens are sent. Copy this value and enter it into the IdP configuration.
   - **Signing Certificate**: The certificate that confirms that requests, responses, and assertions actually came from the SP. Select the appropriate certificate from the list of available RSA or EC certificates. Learn more about adding a certificate in Adding a certificate and key pair.

Copyright © 2025 Ping Identity Corporation

- **Signing Algorithm**: Select the algorithm to be used for signing metadata. If you selected an RSA signing certificate, the options are **RSA_SHA256**, **RSA_SHA384**, and **RSA_SHA512**. If you selected an EC signing certificate, the options are **SHA256_ECDSA**, **SHA384_ECDSA**, or **SHA512_ECDSA**.
- **Enable Signed Authentication Request**: Specifies whether the SAML authentication request will be signed when sending it to the IdP. If the external IdP is included in an authentication policy that will be used by applications that are accessed by a combination of default URLs and custom domains URLs, select this option.

7. Click **Next**.
8. On the **Configure IDP Connection** page, specify the details of the connection between the IdP and PingOne.

   You can enter the values manually or import them from a file.

   Choose from:

   - **Import Metadata**: Click **Select a file** and then select an XML metadata file on your file system. Click **Open**.

     > **Note**
     > If the metadata file doesn't specify all the configuration values, you must enter the missing values manually.

   - **Import from URL**: Enter the **Idp Metadata URL** and then click **Import**.

     > **Note**
     > The URL must be a valid absolute URL.

   - **Manually Enter**:
     - **SSO Endpoint**: Specifies the SSO endpoint for the authentication request. Only authentication requests can be sent to the SSO endpoint.
     - **IDP Entity ID**: Specifies the IdP's entity ID.
     - **SSO Binding**: Specifies the binding to use for the authentication request. Select **HTTP Post** or **HTTP Redirect**.
     - **SLO Endpoint**: The URL of the single logout (SLO) service. PingOne redirects the browser to this location when it needs to send an SLO message to the service provider. Learn more in SAML 2.0 single logout.
     - **SLO Response Endpoint**: The URL of the SLO. You can use this option if you have a separate service for SLO responses. If this value is blank, PingOne sends responses to the SLO endpoint.
     - **SLO Binding**: The SAML binding used by the application. The default is `HTTP POST`. Select `HTTP Redirect` as needed.
     - **SLO Window (in hours)**: Specify how long PingOne can exchange logout messages with the IdP, specifically a `LogoutRequest` from the IdP, since the initial request. PingOne can also send a `LogoutRequest` to the IdP when SLO is initiated by the user from other session participants, such as an application or another IdP. This setting is per IdP. The SLO logout is separate from the user session logout that revokes all tokens. The minimum value is 1 hour, and the maximum is 24 hours. You should start with a value of 2 hours and then fine tune as needed.

Copyright © 2025 Ping Identity Corporation

- **Verification Certificate**: A certificate that confirms that the SAML assertions actually came from the sender. Click **+ Import** or select the appropriate certificate. The list shows the available certificates. Click **+ Add** to add more certificates. Learn more in Adding a certificate and key pair.

9. Click **Next**.
10. Define how the PingOne user attributes are mapped to IdP attributes. Learn more in Mapping attributes.
    - Enter the PingOne user profile attribute and the external IdP attribute. Learn more about attribute syntax in Identity provider attributes.
    - To add an attribute, click **+ Add**.
    - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
    - Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
      - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
      - **Always**: Always update the PingOne directory attribute.
11. Click **Save**.
12. To enable the IdP, click the toggle at the top of the details panel to the right (blue).

> **Note**
>
> You can disable the IdP by clicking the toggle to the left (gray).

Next steps

Add the IdP to your authentication policy.

Editing an identity provider

Use the **External IdPs** page to edit an existing external identity provider (IdP).

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and browse or search for the IdP you want to edit.
2. Click the IdP to open the details panel.
3. On the **Profile** tab, click the **Pencil** icon and enter or edit the following information:
    - **Name**: A unique identifier for the IdP.
    - **Description** (optional): A brief description of the IdP.
    - **Population**: A population that overrides the authentication policy's registration population and enables just-in-time registration from the IdP.
    - **Icon** (optional): A pictorial representation of the IdP. Use a file up to 1 MB in JPG, JPEG, GIF, or PNG format.

Copyright © 2025 Ping Identity Corporation

- **Sign-on button** (optional): An image to be used for the login button that the end user will see. Use a 300 x 42 pixel image.

> **Note**
> You can't change the **Icon** and **Sign-on Button**, in accordance with the provider's brand standards.

4. Click **Save**.
5. On the **Connection** tab, click the **Pencil** icon and enter or edit the information as needed.

   These values vary depending on the type of external IdP you're editing.

> **Note**
> If you're using a custom domain, you can toggle the view between the custom and original URLs. The original and custom URLs will continue to work. Learn more in Domains.

6. Click **Save**.
7. On the **Attributes** tab, click the **Pencil** icon and enter or edit the attribute mappings, which define how the PingOne user attributes are mapped to IdP attributes. Learn more in Mapping attributes.
   - Enter the PingOne user profile attribute and the external IdP attribute. Learn more about attribute syntax in Identity provider attributes.
   - To add an attribute, click **+ Add**.
   - To use the advanced expression builder, click the **Gear** icon. Learn more in Using the expression builder.
   - Select the update condition, which determines how PingOne updates its user directory with the values from the IdP. The options are:
     - **Empty only**: Update the PingOne attribute only if the existing attribute is empty.
     - **Always**: Always update the PingOne directory attribute.
8. Click **Save**.
9. To enable or disable an IdP, click the toggle in the **External IdPs** list.

> **Note**
> IdPs labeled with the **Administrator IDP** badge are used for authentication into the PingOne admin console and can't be disabled or deleted.

Deleting an identity provider

Use the **External IdPs** page to remove an external identity provider (IdP) that you no longer need.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and browse or search for the IdP you want to delete.

Copyright © 2025 Ping Identity Corporation

2. Click the **More Options** (⋮) icon
3. Click **Delete**.
4. In the confirmation message, click **Delete**.

SAML 2.0 single logout

PingOne supports SAML 2.0 single logout (SLO), which enables users to sign off from multiple participants in a single action. Participants are the identity provider (IdP) and the service provider (SP), and are referred to as partners of each other. SLO is most common in workforce deployments, in which employees can sign off from multiple applications in a single operation.

This section describes the benefits, behaviors, and limitations of SAML 2.0 SLO.

> **Note**
>
> - SAML applications and IdPs can trigger SLO only if:
> - An SLO endpoint is configured.
> - The user interacts with the application or IdP within the configured SLO window.
> Learn more about the SLO settings in Editing an application - SAML.
> - Signing off from a SAML application or IdP with the conditions described above doesn't trigger PingOne to send logout requests to OpenID Connect (OIDC) or Microsoft 365 applications the user has signed on to in the same PingOne user session.
> - Signing off from an OIDC or Microsoft application doesn't trigger SAML 2.0 SLO.
> - The default sign-off method for the PingOne application portal and PingOne Self-Service - MyAccount is OIDC logout. You can change the sign-off method to SAML 2.0 SLO as needed. Learn more in Configuring the application portal and Configuring the self-service portal.

SLO scenarios

You can use SAML 2.0 SLO in several different scenarios:

SP-initiated SLO

For SP-initiated SLO, PingOne is the IdP, and the partner is the SP with a SAML application in PingOne. If the partner supports SP-initiated SLO, an application can send logout requests to PingOne.

IdP-initiated SLO

For IdP-initiated SLO, the partner is the IdP, and PingOne is the SP with an external IdP connection to the partner. If the partner supports IdP-initiated SLO, the IdP can send logout requests to PingOne.

PingOne-initiated SLO

For PingOne-initiated SLO, if PingOne is the IdP, and if the SP supports IdP-initiated SLO, PingOne can send logout requests to the SP. If PingOne is the service SP, and the IdP supports SP-initiated SLO, PingOne can also send logout requests to the SP.

To start a PingOne-initiated SLO request, the browser sends an HTTP GET request to either of the following URLs:

- https://auth.pingone.<region>/<envID>/saml20/startslo

Copyright © 2025 Ping Identity Corporation

- https://<customDomain>/saml20/startslo (Only if a custom domain has been configured. Learn more in Setting up a custom domain.)

SLO traffic

SLO messages (requests and responses) are transported through the browser. PingOne supports two SLO bindings that define how messages are transported:

- POST (default)
- Redirect

SLO behavior

Generally speaking, when a participant initiates a SAML 2.0 SLO request, based on the user's action, requests and responses are exchanged among all participating partners. The goal is to sign the user off from all partners.

When PingOne is a participant, and it receives an SLO request, if PingOne is aware of other participants, PingOne sends an SLO request to each participant in a sequence after each successful SLO response PingOne receives. When no participants remain, PingOne honors the original SLO request and returns a successful SLO response to the participant that originally sent the request.

When PingOne is the initiator, the SLO process works similarly. However, the SLO should finish with PingOne when it receives the last successful SLO response.

The chain succeeds when each participant completes its share of the SLO process. The chain breaks when one participant fails to complete the SLO request.

When SLO fails, the participant is supposed to return the browser to the initiator with an error message. If the participant is unable to do so, the participant would typically show a message directly to the user. In either case, the user can close the browser and optionally clear the browsing data, such as cache and cookies, to terminate sessions from all participants.

Applications and SLO

If the SP supports SLO, enter the SLO endpoint in the SAML application. This is the endpoint at the SP where it receives SLO requests. If the SP wants to receive SLO responses at a different endpoint, enter that as the SLO response endpoint. The SLO binding defaults to POST and also supports Redirect.

Because SLO can time out if one participant fails to send an SLO message, you can configure how long PingOne should send or receive SLO messages to and from an application since the initial request. This per-application flexibility allows you to fine-tune SLO experiences for your users.

External IdPs and SLO

SAML 2.0 external IdPs work the same way as SAML 2.0 applications. If the IdP supports SLO, enter the SLO endpoint in the external IdP configuration. This is the endpoint at the IdP where it receives SLO requests. If the IdP wants to receive SLO responses at a different endpoint, enter that as the SLO response endpoint. The SLO binding defaults to POST and also supports Redirect.

Because SLO can time out if one participant fails to send an SLO message, you can configure how long PingOne should send or receive SLO messages to and from a SAML 2.0 external IdP since the initial request. This per-external IdP flexibility allows you to fine-tune SLO experiences for your users.

Copyright © 2025 Ping Identity Corporation

When triggered, PingOne sends and processes logout requests to and from SAML 2.0 IdPs to which the user previously signed on using either of the following methods:

- A PingOne authentication policy (External IdP step)
- PingOne DaVinci (Sign On with External Identity Provider capability from the PingOne Authentication connector)

Downloading metadata for SAML IdPs

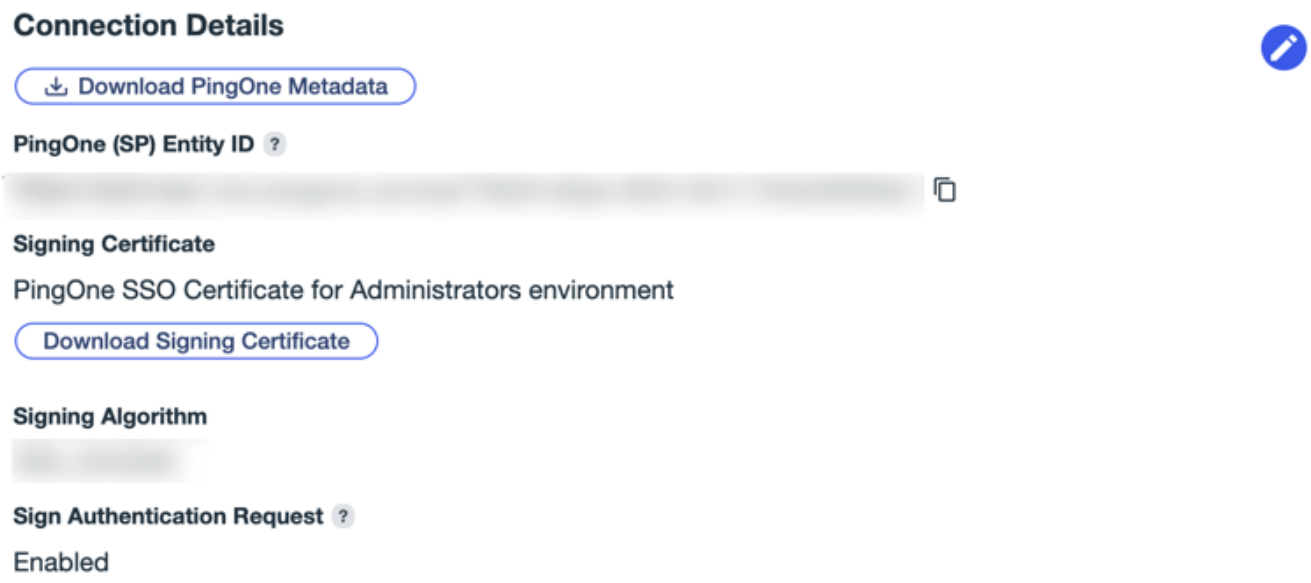
PingOne generates a metadata file that contains configuration details for external SAML identity providers (IdPs). You can use the IdP metadata to share configuration information between the PingOne and the IdP. The metadata includes configuration details and certificate information.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and browse or search for the IdP for which you want to download metadata.
2. Click the IdP to open the details panel.

   > **Note**
   > You can download metadata for SAML IdPs only.

3. On the **Connection** tab, click **Download PingOne Metadata**.



Result

The file is saved to your local device storage.

> **Note**
> You can also download IdP metadata for applications. Learn more in Downloading IdP metadata for an application.

Copyright © 2025 Ping Identity Corporation

Identity provider attributes

You can map user attributes from an external identity provider (IdP) to PingOne user attributes using the appropriate notation for SAML and JSON.

When mapping user attributes, use the `providerAttributes` prefix rather than `samlAssertion` as follows:

```
providerAttributes.<IdP attribute name>
```

For example, mapping the email attribute from Facebook to PingOne would look like this:

```
providerAttributes.email
```

> **Note**
>
> For external IdPs that pass attributes in JSON structure (all external providers except SAML), the syntax for mapping attributes that use JSON dot notation, such as `name.family`, must use square brackets and single quotes around the attribute name as follows:
>
> ```
> providerAttributes['name.family']
> ```

Mapping the group attribute from an external identity provider

If the external identity provider (IdP) includes group information in its security tokens (ID tokens from an OpenID Connect (OIDC) IdP or assertions from a Security Assertion Markup Language (SAML) IdP), you can add a mapping between the **External Group Names** attribute in PingOne and the inbound attribute name from the external IdP.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and browse or search for the appropriate IdP.
2. Click the IdP to open the details panel.
3. On the **Attributes** tab, click the **Pencil** icon.
4. Click **+ Add**.
5. For PingOne user profile attribute, select **External Group Names**.
6. For the external IdP attribute, enter the inbound attribute name from the external IdP.
7. For **Update condition**, select one of the following:
   - **Always**: Update the group information in PingOne every time the user authenticates from the external IdP.
   - **Empty only**: Update the group information in PingOne only if there is no value for the attribute in PingOne.
8. Click **Save**.

Learn more in Just-in-time provisioning of external groups.

Copyright © 2025 Ping Identity Corporation

Initiating SSO from PingOne

Configure single sign-on (SSO) initiated from PingOne to give users one-click access to the applications they need.

Configure a new SAML application or edit an existing one. Learn more in Editing an application - SAML.

Steps

1. In the PingOne admin console, go to **Applications > Applications** and browse or search for the appropriate application.
2. Click the application entry to open the details panel.
3. On the **Overview** tab, copy the **Initiate Single Sign-On URL**.

Next steps

You can save the **Initiate Single Sign-On URL** or embed it in an external application to launch the app and initiate SSO through PingOne.

Setting up IdP-initiated SSO

PingOne supports single sign-on (SSO) from an external SAML identity provider (IdP) to an application. If a user is already signed on with the IdP, they can access an application without having to sign on.

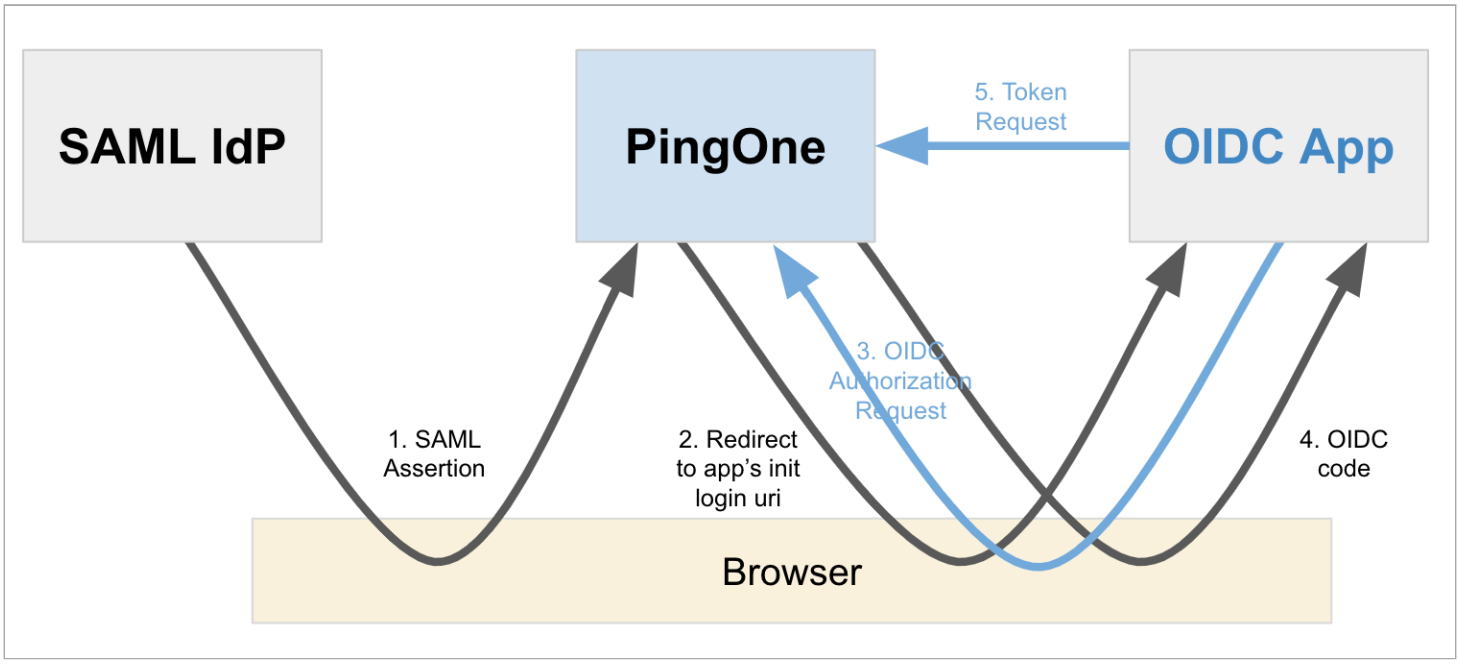
About this task

You'll configure the application in PingOne, and then configure the IdP to reference the application for IdP-initiated SSO. For OpenID Connect (OIDC) applications, you must first complete the configuration steps in Configuring an OIDC application. For SAML applications, skip to Enabling IdP-initiated SSO.

You'll need to configure the IdP to include the `RelayState` parameter with the target application ID when the IdP sends a SAML assertion to PingOne.

The following diagram shows the flow for an OIDC application:

Copyright © 2025 Ping Identity Corporation



Configuring an OIDC application

Add an **Initiate Login URI** in your OIDC application configuration. Learn more in Initiating Login from a Third Party.

Steps

1. In the PingOne admin console, go to **Applications** > **Applications** and browse or search for the OIDC application you want to edit.
2. Click the application entry to open the details panel.
3. On the **Configuration** tab, click the **Pencil** icon.
4. Enter the following:
   - **Initiate Login URI**: The URI to use for SSO to the application. PingOne redirects application users to this URI to initiate SSO to PingOne using OIDC. The `Initiate Login URI` is required if you want the application to appear in the PingOne application portal.
   - **Target Link URI** (optional): The URI for the application itself. PingOne redirects application users to this URI after the user is authenticated.

     > **Note**
     > If you don't specify a value for **Target Link URI**, you must include an `applicationUrl` in the `RelayState` during IdP-initiated SSO to this application (see step 2 in Enabling IdP-initiated SSO).
5. Click **Save**.
6. Click the **Profile** tab.
7. Locate the **Client ID** and copy it to a secure location.
8. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Enabling IdP-initiated SSO

In the external SAML IdP, enable IdP-initiated SSO. The specifics of the configuration vary depending on the IdP. Refer to the applicable IdP documentation for more information.

Before you begin

Make sure your application in PingOne has an authentication policy assigned that contains the external IdP initiating SSO. Learn more in Applying authentication policies to an application.

Steps

1. In the IdP, configure the `RelayState` parameter to contain the `applicationId` when the IdP sends an SAML assertion to PingOne.

   This is the **Client ID** copied from the application in PingOne.

   > **Note**
   >
   > For some applications, the `applicationId` is also known as the **Client ID**.

   Example:

   ```
   applicationId=bda4e692-84c2-4f90-8835-d28da695c748
   ```

2. (Optional) Include `applicationUrl` in the `RelayState`.

   Example:

   ```
   applicationId=bda4e692-84c2-4f90-8835-d28da695c748&applicationUrl=https://myapp.com/overview
   ```

   > **Note**
   >
   > If the target application is an OIDC application without a `target_link_uri` configured, include the `applicationUrl` in the `RelayState`. The `applicationUrl` is used only when `target_link_uri` is not configured.
   > The `RelayState` parameter should also be URL-encoded. The following are examples of the full parameter sent to PingOne:
   >
   > ```
   > RelayState=applicationId%3Dbda4e692-84c2-4f90-8835-d28da695c748
   > ```
   >
   > ```
   > RelayState=applicationId%3Dbda4e692-84c2-4f90-8835-
   > d28da695c748%26applicationUrl%3Dhttps%3A%2F%2Fmyapp.com%2Foverview
   > ```

Authoritative identity providers

An authoritative identity provider (IdP) is the IdP that has authority over user records and credentials and defines where a user normally authenticates. By default, PingOne is a user's authoritative IdP, meaning users authenticate with a PingOne username and password.

Copyright © 2025 Ping Identity Corporation

If a user authenticates from an external IdP that's different from their authoritative IdP set in PingOne, and they do not have an existing account link for that IdP, the user must link their account by signing on through the authoritative IdP first (for example, by entering their PingOne username and password). This creates an account link between the external IdP and the PingOne user. Learn more in Adding an external identity provider sign-on step.

> **Note**
>
> For a user to link their account with multiple external IdPs, their authoritative IdP must be set to PingOne. Account linking only applies when the user's authoritative IdP is PingOne.
> If a user's authoritative IdP is PingOne, but they don't have a PingOne password, the user can't sign on through an external IdP and can't link their account between the external IdP and PingOne. This can occur when users are created through an external integration that does not set an authoritative IdP or password, such as through the PingID or PingOne MFA adapters for PingFederate. This can also occur with any other custom integration that creates users without setting an authoritative IdP or password.

Setting the IdP

The authoritative IdP can be set either on the user or on a population in PingOne. Setting the authoritative IdP on a population means that all users in that population whose authoritative IdP is not set explicitly on the user record will use the authoritative IdP set on the population. If the user record does not include an authoritative IdP, and the user is not part a population that has an authoritative IdP applied, the authoritative IdP defaults to PingOne.

For example, if you're using the PingID or PingOne MFA adapters, users can be created by the adapters without an authoritative IdP or password, and they cannot sign on to PingOne. In this scenario, setting the authoritative IdP as PingFederate for that population applies the authoritative IdP to the users created by the adapters. Learn more in Adding a user and Managing populations.

You can change a user's authoritative IdP in the PingOne admin console or using the API. For example, if a user's authoritative IdP is PingOne but you want them to authenticate through an external IdP without needing a PingOne password, set their authoritative IdP to that external IdP. Learn more about using the API in Update User Identity Provider.

Just-in-time provisioning

With just-in-time (JIT) provisioning, you can automate user registration and account creation. If a user authenticates through an external IdP that has registration enabled, and the user doesn't already exist in PingOne, the user is automatically created through JIT provisioning without their authoritative IdP set to the external IdP.

+ Users that are JIT provisioned automatically have the authoritative IdP configured and linked with the user account at the IdP.

+ To enable JIT provisioning, you must select a population on the **Registration** tab for the external IdP. Learn more in Configuring an authoritative identity provider.

Identifier-first authentication

With identifier-first authentication, you can identify users before you authenticate them. If the user has an authoritative IdP, PingOne redirects the user to that IdP for authentication after they enter their email or username.

If a user account in PingOne is preregistered and the user authenticates through their authoritative IdP for the first time, PingOne links the user account without requiring the user to verify their account or password. If you use a login authentication step instead, users must choose their IdP from a list that you can configure. Learn more in Adding an identifier first authentication step and Adding a login authentication step.

Copyright © 2025 Ping Identity Corporation

Related links

- External IdPs
- Authentication policies
- Configuring an authoritative identity provider

Configuring an authoritative identity provider

You can configure an identity provider (IdP) as an authoritative IdP, which allows it to provision users without any registration or sign-on steps.

About this task

Set up an IdP as usual, edit the IdP to configure it as an authoritative IdP, and then specify which population should contain the provisioned users.

Before you begin

Set up an external IdP if you haven't already. Learn more in External IdPs.

Steps

1. In the PingOne admin console, go to **Integrations** > **External IdPs** and browse or search for the IdP that you want to edit.
2. Click the IdP entry to open the details panel.
3. On the **Profile** tab, click the **Pencil** icon.
4. In the **Population** list, select the population to which you want to provision users.

   Selecting a population enables just-in-time (JIT) provisioning for the configured IdP and overrides the population set in the authentication policy under **Enable registration**.
5. Click **Save**.

Viewing or changing the authoritative identity provider for a user

You can use the user details page to see information about a user's authentication configuration, including the authoritative identity provider (IdP).

Steps

1. In the PingOne admin console, go to **Directory** > **Users** and browse or search for the appropriate user.
2. Click the user you want to view to expand the details panel.
3. Go to the **Services** > **Authentication** tab.

   The current authoritative IdP is listed in the **Authoritative Identity Provider** section.
4. To change the authoritative IdP:

   1. In the **Authoritative Identity Provider** section, click the **More Options** (⋮) icon and click **Edit**.

Copyright © 2025 Ping Identity Corporation

2. In the **Authoritative Identity Provider** modal, select a different IdP in the list.
3. Click **Save**.

Provisioning

PingOne provisioning propagates user identity information from the PingOne directory to a target identity store, or from a source identity store to the PingOne directory.

The provisioning service continually synchronizes changes to and from the source and target identity stores. Provisioning events are triggered by any addition, change, or deletion of users or user information in the source identity store.

How do I use it?

You'll create a connection that defines the source or target identity store for identities. You can then set up rules to define which identities from the source identity store are provisioned. Rules define which users are provisioned and how attributes are mapped between the source identity store and the target identity store.

Rules include:

- **Source**. The connection to the source identity store.
- **Target**. The connection to the target identity store.
- **Filter**. Determine which identities are provisioned, based on factors such as population or user attributes.
- **Attribute mapping**. Map attributes from one identity store to another.

Related links

- Creating a SCIM connection
- Creating a Salesforce Communities connection
- Creating a Salesforce Leads and Contacts connection
- Creating an Aquera connection
- Creating a Workday connection
- Creating a Microsoft Azure Office 365 connection
- Creating a Zoom connection
- Creating a Slack connection
- Creating a ServiceNow connection
- Creating a Google Workspace connection
- Creating a GitHub EMU connection
- Creating an LDAP gateway provisioning connection

Copyright © 2025 Ping Identity Corporation

Inbound and outbound provisioning

You can use some connection types for outbound provisioning, some for inbound provisioning, and some for both.

For outbound provisioning, identities flow from PingOne to an external identity store. PingOne is the source and the external identity store is the target. For outbound provisioning, changes are near real-time. When there is a change to a user in PingOne, the target identity store is updated immediately.

For inbound provisioning, identities flow from an external identity store to PingOne. The external identity store is the source and PingOne is the target.

For inbound provisioning with the Workday provisioner, a polling mechanism checks the source identity store every 15 minutes. When there is a circuit breaker due to polling failure, reset is 12 hours. After 12 hours, the polling mechanism will attempt to run a full re-sync for the associated provisioning rule. For LDAP inbound poll failure, the reset is 30 minutes. Learn more about sync status in Sync Status and Viewing sync status.

We recommend that you use the SCIM provisioning connection for outbound provisioning only. For importing identities into PingOne, use the SCIM Users API. Learn more in Using the SCIM API to import users.

> **Note**
>
> PingOne must be either the source or target identity store.

The following table shows the connection type:

Identity store	Inbound	Outbound
SCIM	Yes	Yes
Salesforce	No	Yes
Salesforce Communities	No	Yes
Salesforce Leads and Contacts	No	Yes
Aquera	No	Yes
Workday	Yes	Yes
Microsoft Azure (Office 365)	No	Yes
Zoom	No	Yes
Slack	No	Yes
ServiceNow	No	Yes
Google Workspace	No	Yes
GitHub EMU	No	Yes

Copyright © 2025 Ping Identity Corporation

Identity store	Inbound	Outbound
LDAP Gateway	Yes	Yes

Outbound group provisioning

You can use group provisioning to sync a group along with its memberships to a software as a service (SaaS) application for access control management and other purposes.

Syncing groups is automatic. Memberships are synced based on the user filter criteria. In the group provisioning section, you can select groups to be provisioned to the target and users from those groups are provisioned based on the user filter criteria defined under the **User Filter** section of a provisioning rule.

For more information, see Configuring outbound group provisioning.

Viewing provisioning rules and connections

On the **Provisioning** page, you can view the currently configured provisioning connections and rules.

Steps

- Go to **Integrations → Provisioning**.

  The **Provisioning** page opens with the **Rules** and **Connections** tabs shown.

  - To see provisioning rules, click **Rules**. You can sort the list of rules by `Name`, `Last sync`, or `Creation date`.
  - To see provisioning connections, click **Connections**. You can sort the list of connections by `Name`, `Gateway`, or `Identity stores`.

Result

PingOne shows the rules and connections that have been created. Click an entry to show its details. The details panel page shows the following:

Rules details

Overview. General information about the provisioning connection, including name, description, and sync summary. For more information about the sync summary, see Viewing sync summary.

Configuration Summary. A visual representation of the provisioning rule, including the source identity store, user filter, group provisioning, attribute mapping, and target identity store. The configuration options shown on this page vary based on the target.

Configuration LDAP Setup (LDAP Gateway targets only). Shows details about the LDAP Gateway connection, including RDN Attribute and Base DN.

Connections details

Overview. General information about the provisioning connection, including name, description, and configured rules.

Copyright © 2025 Ping Identity Corporation

Configuration. Details about the connection, including authorization information that is unique to the connection type, as well as custom configuration options, such as provisioning and deprovisioning actions.

> **Note**
>
> Advanced provisioning actions are available only for connections that support outbound provisioning.

Related links

- Creating a SCIM connection
- Creating a Salesforce Communities connection
- Creating a Salesforce Leads and Contacts connection
- Creating an Aquera connection
- Editing a provisioning connection

Group provisioning FAQ

The following section contains common questions and answers about group provisioning.

How do I debug when group synchronization failed on the target?

To debug the group sync failure, on the sync summary, click the **Audit Logs** link to go to the **Audit** page. On the **Audit** page, you can view the audit report for any detailed error messages in the audit logs.

Review the **Provisioning Group Sync Failure** and **Provisioning Group Membership Failure** audit events to check which group or membership failed and the reason why it failed.

For additional debugging, use the **correlationId** in Splunk to find any `ERROR` or `WARN` logs. You can also check the status of the group on the **Group Provisioning** tab.

How do I know if there is a membership sync failure on a group that is part of a provisioning rule configuration?

If there is a membership sync failure, the sync summary shows the failure.

In the sync summary, click the **Audit Logs** link to go to the **Audit** page. On the **Audit** page, you can view the audit report for any detailed error messages in the audit logs.

Review the **Provisioning Group Sync Failure** and **Provisioning Group Membership Failure** audit events to check which group or membership failed and the reason why it failed.

You can also go to **Directory → Users → Sync Status** to check the membership sync status.

How do I debug when the Groups section of the sync summary reports failures?

To debug the group sync failure, click **Audit Logs** to go to the **Audit** page. On the **Audit** page, you can view the audit report for any detailed error messages in the audit logs.

Review the **Provisioning**, **Group Sync Failure**, and **Provisioning Group Membership Failure** audit events to check which group or membership failed and the reason why it failed.

Copyright © 2025 Ping Identity Corporation

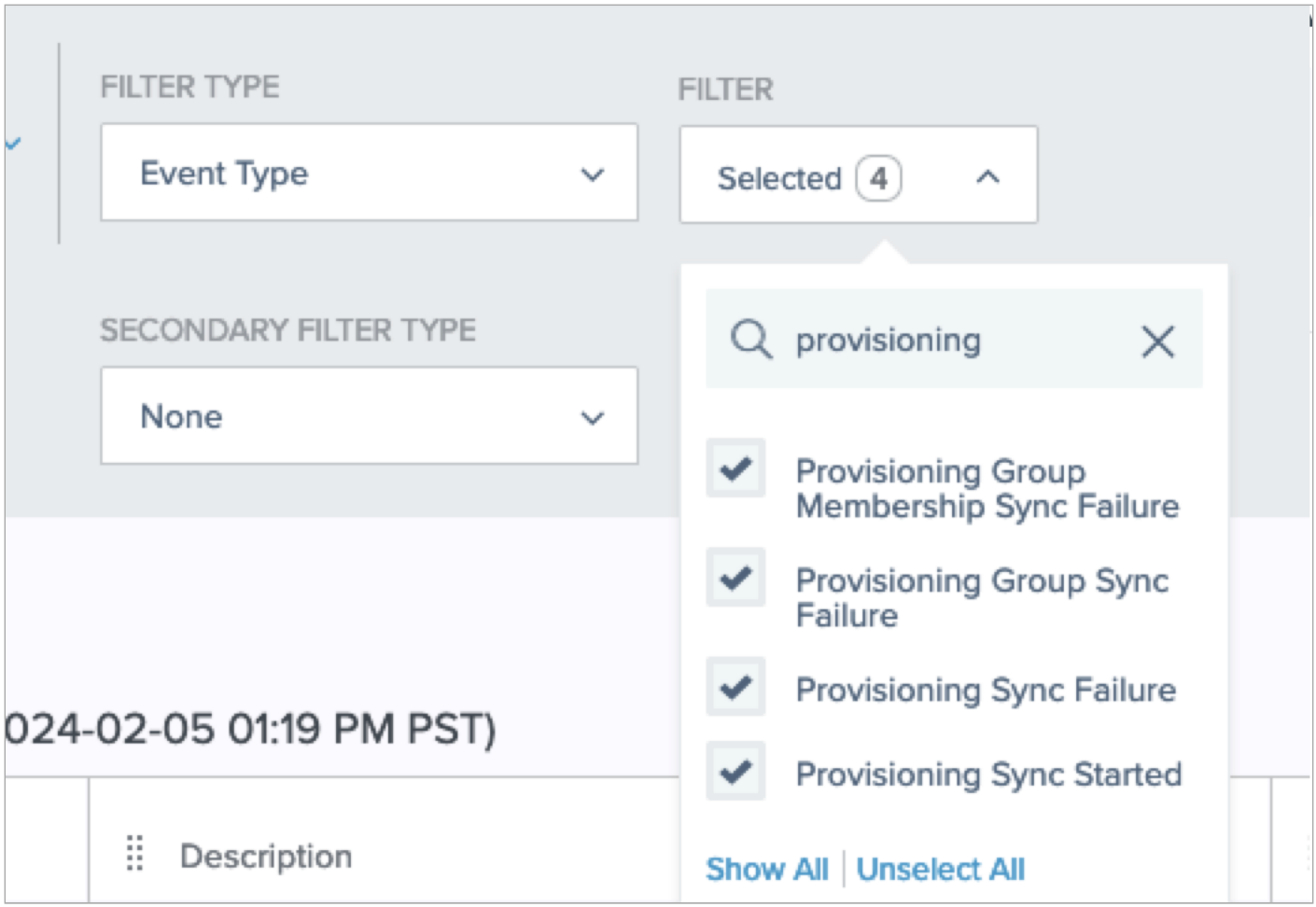
For additional debugging, use the **correlationId** in Splunk to find any `ERROR` or `WARN` logs. You can also check the status of the group on the **Group Provisioning** tab.

How do I filter for group provisioning sync events in the audit events?

To filter audit events for group provisioning sync events, in the **Filter** field, enter `provisioning`.

The available audit events for group provisioning are:

- **Provisioning Group Membership Sync Failure**
- **Provisioning Group Sync Failure**
- **Provisioning Sync Failure**
- **Provisioning Sync Started**



Is there a membership status in Directory → User ?

Yes. Learn more about membership status in Using user identity details to identify sync issues.

Can I see the status of a group in Directory → Groups ?

Yes. Learn more about group status in Using group identity details to identify sync issues.

Copyright © 2025 Ping Identity Corporation

Can I sync nested groups as part of a group provisioning?

Yes. However, you must select the child groups that you want to sync over.

> **Important**
>
> Selecting a parent group does not automatically provision its children. The provisioning service doesn't automatically provision all subgroups within a group (nested groups) unless selected explicitly.

What does the message `the target doesn't support group provisioning` mean?

At present, target systems Service Now, Zoom, LDAP Outbound, Salesforce Contacts, and Leads, do not support group provisioning. Only user provisioning is supported for these target systems.

What does the message `the target user id is unknown` mean?

The user has not been created in the target and could not be added to group memberships. Retry the sync after creating the user.

Are external groups that are synced using JIT supported for outbound group provisioning?

No. Syncing of JIT groups is not currently supported.

How many groups can I configure as part of a provisioning rule?

Provisioning supports 1000 groups to be synced to the target system.

Configuring provisioning

To configure provisioning, you'll create a connection to the appropriate identity store, then create a rule that determines how users will be provisioned.

You can use some connection types for outbound provisioning, some for inbound provisioning, and some for both. You can also use an LDAP Gateway connection to provision to and from LDAP directories such as Microsoft Active Directory or Ping Directory.

> **Note**
>
> Not all provisioning connection types support inbound provisioning. See Inbound and outbound provisioning.

Use the following steps to set up provisioning, depending on your configuration.

Outbound

1. Creating a connection
2. Creating an outbound rule
3. Adding attribute mapping for outbound provisioning
4. Adding a user filter
5. Viewing sync status

Copyright © 2025 Ping Identity Corporation

6. Configuring outbound group provisioning

Inbound

1. Creating a connection
2. Creating an inbound rule
3. Adding attribute mapping for inbound provisioning
4. Adding a user filter
5. Viewing sync status

Outbound using a Gateway

1. Creating a connection
2. Creating an outbound rule for a connection through an LDAP gateway
3. Adding attribute mapping for outbound provisioning
4. Adding a user filter
5. Viewing sync status

Inbound using a Gateway

1. Creating a connection
2. Creating an inbound rule for a connection through an LDAP gateway
3. Adding attribute mapping for inbound provisioning
4. Adding a user filter
5. Viewing sync status

Creating a connection

Create a connection using any of the supported provisioning connection types.

About this task

The connection defines the options for the connection, such as host configuration, authentication, and provisioning options. Some connections support inbound provisioning, some support outbound provisioning, and some support both. For more information, see Inbound and outbound provisioning.

For information about configuring each connection type, see:

Steps

- Creating a SCIM connection
- Creating a Salesforce connection

Copyright © 2025 Ping Identity Corporation

- Creating a Salesforce Communities connection
- Creating a Salesforce Leads and Contacts connection
- Creating an Aquera connection
- Creating a Workday connection
- Creating a Microsoft Azure Office 365 connection
- Creating a Zoom connection
- Creating a Slack connection
- Creating a ServiceNow connection
- Creating a Google Workspace connection
- Creating a GitHub EMU connection
- Creating an LDAP gateway provisioning connection

> **Note**
>
> PingOne must be either the source or target connection. You don't have to add PingOne as a connection type; it will be added automatically when you select the source or target connection. The connection must be enabled before you can use it in a rule.

Creating an outbound rule

Create a rule to define which users are provisioned and how attributes are mapped between PingOne and the external identity store.

About this task

If you are creating a rule for a connection through an LDAP gateway, see Creating an outbound rule for a connection through an LDAP gateway or Creating an inbound rule for a connection through an LDAP gateway.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **+** and then click **New rule**.
3. Enter a name and description for the rule. The rule name will appear in the list when you've completed and saved the rule.
4. Click **Create rule**.
5. On the **Configuration** tab, assign a source and target connection for the rule. Click the **Source** or **Target** icon. Under **Available connections**, click **+** to add a connection as a source or target. If you haven't created a connection yet, see Creating a connection. You can add disabled connections to a source or target, but the connection must be enabled to enable an associated rule.

Copyright © 2025 Ping Identity Corporation

> **Note**
> PingOne must be either the source or target connection. If you choose an external source connection, then PingOne will be selected automatically as the target connection, and vice versa.

6. Click **Save**.

Next steps

- To specify which identities are provisioned based on factors such as population, group, or other user attributes, follow the instructions in Adding a user filter.
- To map PingOne user attributes from an external identity store, follow the instructions in Adding attribute mapping for outbound provisioning.

Creating an inbound rule

Create a rule to define which users are provisioned to PingOne and how attributes are mapped between the external identity store and PingOne.

About this task

If you are creating a rule for a connection through an LDAP gateway, see Creating an inbound rule for a connection through an LDAP gateway.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **+** and then click **New rule**.
3. Enter a name and description for the rule. The rule name will appear in the list when you've completed and saved the rule.
4. Click **Create rule**.
5. On the **Configuration** tab, click the **Source** icon. Under **Available connections**, click **+** to add an appropriate connection as a source. If you haven't created a connection yet, see Creating a connection. You can add disabled connections to a source or target, but the connection must be enabled to enable an associated rule. PingOne will automatically be added as the target.

   > **Note**
   > Not all provisioning connection types support inbound provisioning.

6. Click **Save**.
7. On the **Configuration** tab, click the **Target** icon.
8. Click the **See Details** link and then click the pencil icon.
9. For **Actions**, enter or edit the following:
   - **Allow users to be created**. Determines whether to create a user in the PingOne user store when the user is created in the source identity store.

Copyright © 2025 Ping Identity Corporation

- **Allow users to be updated**. Determines whether to update user attributes in the PingOne user store when the user is updated in the source identity store.
  - **Allow users to be disabled**. When a user is disabled in the source identity store, PingOne disables the user in the PingOne identity store.
- **Allow users to be deprovisioned**. Determines whether to deprovision a user in the PingOne identity store when the user is deprovisioned in the source identity store.
- **Remove action**. Determines the action to take when removing a user from the source identity store.
  - **Delete**. When a user is deprovisioned from the source identity store, PingOne deletes the user in the PingOne identity store.
  - **Disable**. When a user is deprovisioned from the source identity store, PingOne disables the user in the PingOne identity store.
- **Deprovision on rule deletion**. Determines whether to deprovision users that were provisioned using this rule if the rule is deleted.

10. Click **Save**.

Next steps

- To specify which identities are provisioned based on factors such as active users or other source user attributes, follow the instructions in Adding a user filter.
- To specify additional options for onboarding new users, follow the instructions in Adding attribute mapping for inbound provisioning.

Creating an outbound rule for a connection through an LDAP gateway

Create a rule to define which users are provisioned and how attributes are mapped between PingOne and the LDAP directory.

Before you begin

- The RDN attribute that specifies the relative portion of the DN (distinguished name), which uniquely identifies the user in the LDAP directory.
- The Base DN that specifies where the users will be created in the LDAP directory.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **+** and then click **New rule**.
3. Enter a name and description for the rule. The rule name will appear in the list when you've completed and saved the rule.
4. Click **Create rule**.
5. Click the **Target** button, and then click the **+** icon for the appropriate gateway to add it as the target connection. PingOne Directory will be automatically added as the source.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If you haven't created the appropriate connection yet, see Creating an LDAP gateway provisioning connection. You can add disabled connections to a source or target, but the connection must be enabled to enable an associated rule.

6. Enter the following:
   - **RDN attribute**. Select the PingOne attribute that will map to the RDN attribute. The RDN attribute is the relative portion of the DN (distinguished name) that uniquely identifies the user in the LDAP directory

     > **Note**
     >
     > The default attributes are based on the directory type of the gateway used.
     > - For Active Directory, `RDN` defaults to `cn`. For Ping Directory, `RDN` defaults to `uid`.

   - **Base DN**. Specifies the location in the LDAP directory structure where users will be created. For more information, see Distinguished Names in the Microsoft LDAP documentation.
7. Click **Save**.

Next steps

- To specify which identities are provisioned based on factors such as population, group, or other user attributes, follow the instructions in Adding a user filter.
- To map PingOne user attributes from an external identity store, follow the instructions in Adding attribute mapping for outbound provisioning.

Creating an inbound rule for a connection through an LDAP gateway

For inbound gateway connections, you can configure an LDAP filter that specifies which users to provision.

Before you begin

Ensure that you have the Users Base DN that defines the users you want to provision. For inbound provisioning, it specifies the source of the users that will be imported into PingOne.

> **Note**
>
> For inbound provisioning rules, we recommend that you use the same Users Base DN value as the user type in the Gateway configuration. This enables users to be authenticated through the LDAP Gateway for syncing passwords. For more information, see Adding a user type.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **+** and then click **New rule**.
3. Enter a name and description for the rule. The rule name will appear in the list when you've completed and saved the rule.
4. Click **Create rule**.

Copyright © 2025 Ping Identity Corporation

5. Click the **Source** button, and then click the **+** icon for the appropriate gateway to add it as the source connection. PingOne will be automatically added as the target.

> **Note**
>
> If you haven't created the appropriate connection yet, see Creating a connection. You can add disabled connections to a source or target, but the connection must be enabled to enable an associated rule.

6. Enter the **Users Base DN**. The **Users Base DN** specifies the location in the LDAP directory structure where PingOne provisioning will search for users. For users to be found, they must be located under the Users Base DN.

   A stricter Users Base DN will match fewer users in the directory. For example, `ou=Users,dc=lab,dc=local` is more strict than `dc=lab,dc=local` because it will match only objects under the Users Organizational Unit.

7. Click **Save**.

Next steps

- To create an LDAP filter expression and define the users that will be provisioned, follow the instructions in Adding an LDAP filter.
- To specify additional options for onboarding new users, follow the instructions in Adding attribute mapping for inbound provisioning.

Adding a user filter

Add a user filter to specify which identities are provisioned, based on factors such as population, group, or other user attributes.

Steps

1. Go to **Integrations → Provisioning**.
2. Click the **Rules** tab.
3. Find the appropriate rule and click it to show the rule details.
4. Click the **Configuration** tab.
5. Click the **User filter** button.

> **Note**
>
> Inbound provisioning rules have an LDAP filter rather than a User filter. See Adding an LDAP filter.

6. Click the pencil icon to edit the filter.
7. Define the filter that determines which identities are provisioned. For more information, see Example user filters.
8. Enter the first condition:
   - Select **All** or **Any** to determine how the linked conditions will be evaluated: Boolean logical AND or OR.
   - **Attribute**. The user attribute to filter on.
   - **Operator**. Equals. Equals is the only operator supported at this time.

Copyright © 2025 Ping Identity Corporation

- **Value**. Enter the appropriate value.

> **Note**
>
> - If you select a group in the filter, then updating or deleting the group can cause the provisioning rule to re-sync.
> - If you select a group in the filter, the filter will include all users with any kind of membership in the group, whether direct, dynamic membership based on a user filter, or inherited from parent groups. For more information, see Groups.

9. If needed, click **Add +** to add another condition or condition set.
10. Continue adding conditions or condition sets as needed.
11. Click **Save**.

Next steps

- To map PingOne user attributes from an external identity store, follow the instructions in Adding attribute mapping for outbound provisioning.
- For workday inbound rule, see Workday attribute mapping.

Adding an LDAP filter

For inbound provisioning through an LDAP Gateway, create an LDAP filter expression to define the users that will be provisioned.

Steps

1. Go to **Integrations → Provisioning**.
2. Click the **Rules** tab.
3. Find the appropriate inbound rule and click it to show the rule details.
4. Click the **Configuration** tab.
5. Click the **LDAP filter** button.

> **Note**
>
> Outbound provisioning rules have a User filter rather than an LDAP filter. See Adding a user filter.

6. Click the pencil icon to edit the filter.
7. Enter or edit the filter to define the users to provision to PingOne. For more information, see LDAP filters.
8. Click **Save**.

Next steps

To specify additional options for onboarding new users, follow the instructions in Adding attribute mapping for inbound provisioning.

Copyright © 2025 Ping Identity Corporation

Example user filters

This section shows some example user filters to define users for provisioning.

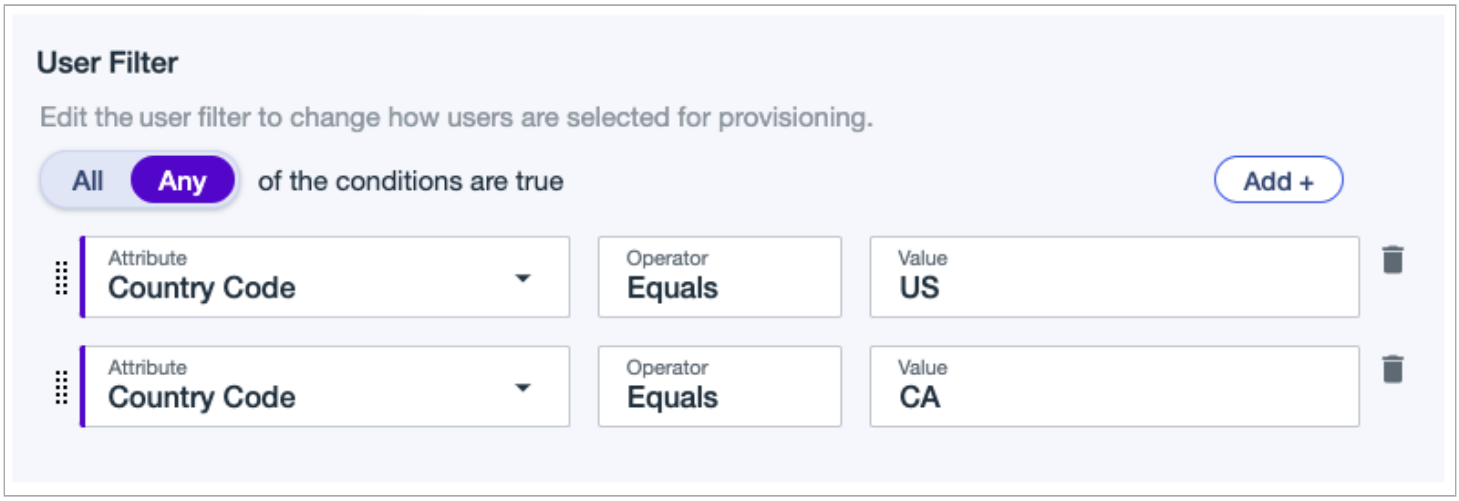
Example 1

A filter that includes users from the USA and Canada. Include users that match the following:

Country Code Equals **US**

OR

Country Code Equals **CA**



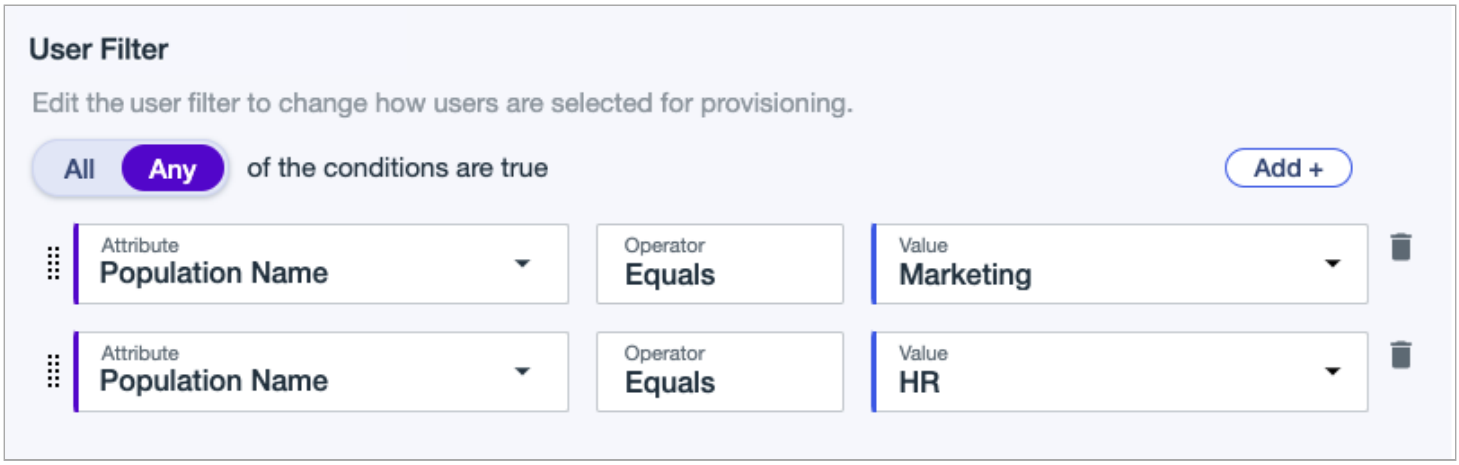
Example 2

A filter that includes users from the following populations:

Population Name Equals **Marketing**

OR

Population Name Equals **HR**



Copyright © 2025 Ping Identity Corporation

Example 3

A filter that includes enabled users from the following populations:

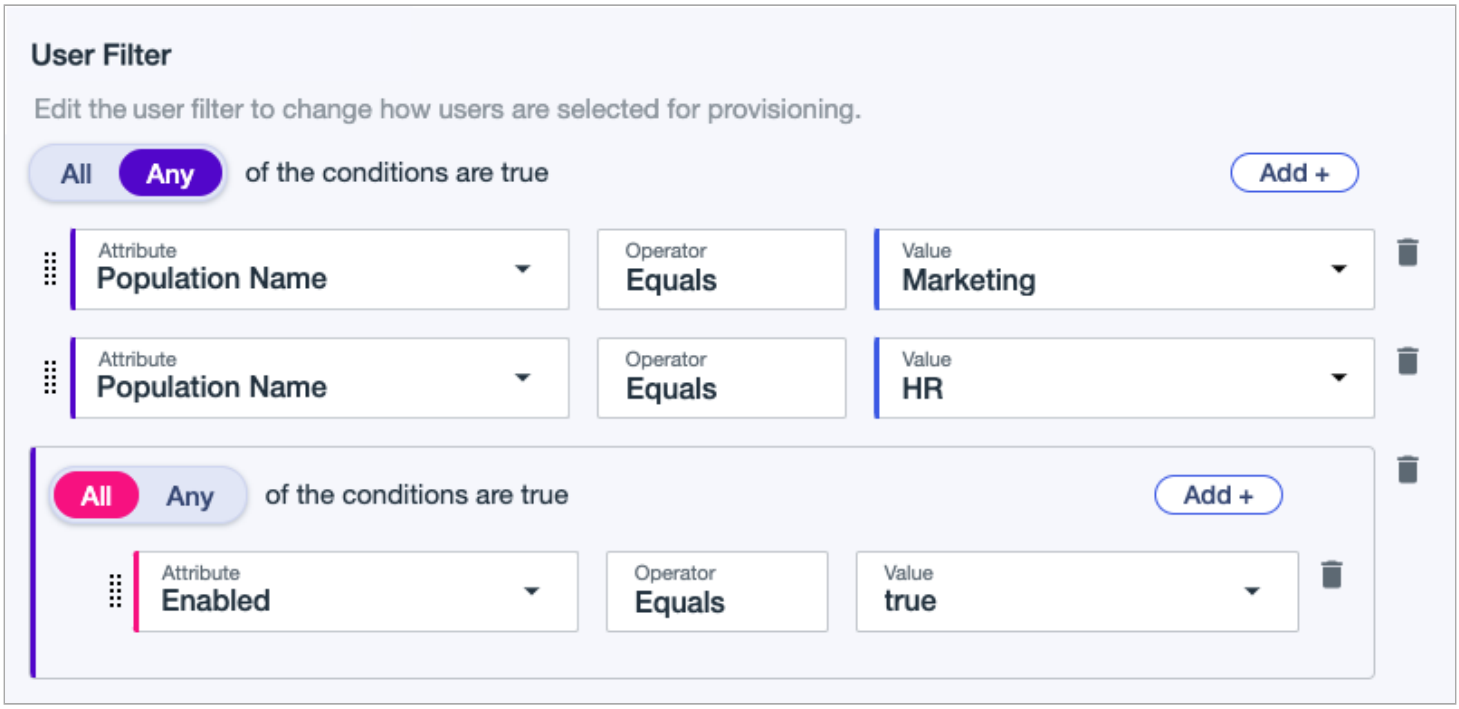
Population Name Equals **Marketing**

OR

Population Name Equals **HR**

AND

Enabled Equals **true**



Example 4

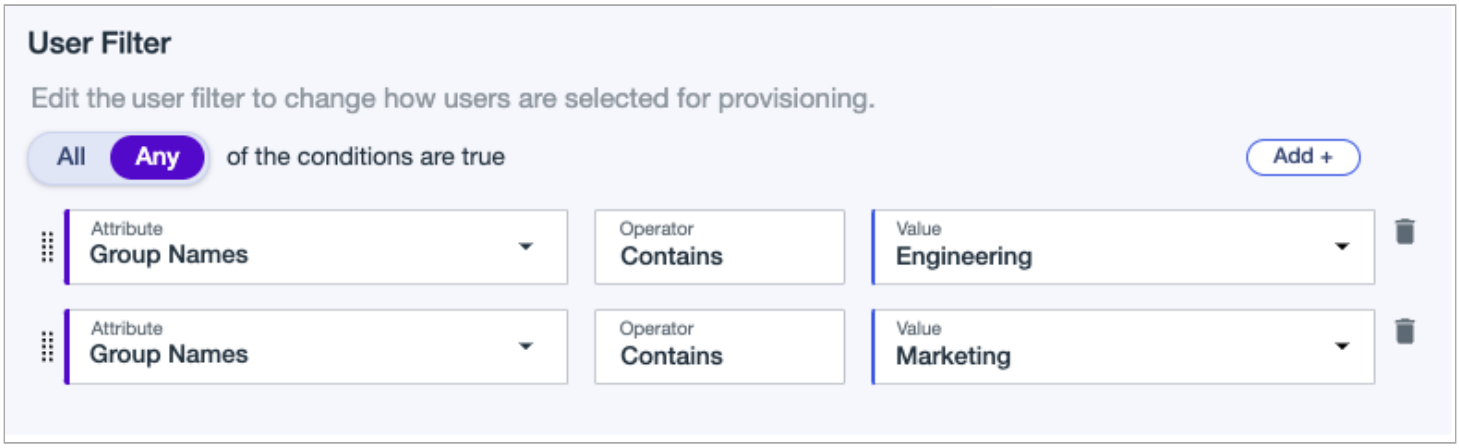
A filter that includes users from the Engineering and Marketing groups. Include users that match the following:

Group Names Contains **Engineering**

OR

Group Names Contains **Marketing**

Copyright © 2025 Ping Identity Corporation



Adding attribute mapping for outbound provisioning

You can map PingOne user attributes from attributes in an external identity store. For outbound provisioning, the mapping is applied to the attribute coming from the PingOne directory before it is saved to the target identity store.

Steps

1. In the PingOne admin console, go to **Integrations** > **Provisioning**.
2. On the **Rules** tab, find the appropriate rule and click it to show the details panel.
3. Click the **Configuration** tab.
4. Click **Attribute Mapping**.

   > **Important**
   >
   > You must have a source and target connection configured before you can set up attribute mapping.

5. Click the **Pencil** icon to edit the attribute mapping.
6. Review the attribute mappings for the configured identity store. The default attribute mappings for a particular identity store are provided. Learn more in Mapping attributes.

Option	Description
Add an attribute mapping	Click **+ Add**. Enter the source and target attribute.
Use the expression builder	Click the **Gear** icon. Learn more in Using the expression builder. You can also use list values in the expression builder to create advanced expressions, such as conditional statements.

Copyright © 2025 Ping Identity Corporation

Option	Description

Choose values from a picklist	Some attributes have metadata that define potential values.
	For example, for Salesforce attribute mapping, you can see a list of values from Salesforce in the form of a picklist. In the expression builder, enter a single quote to see potential values.
	You can use a switch statement or an if-else to evaluate an expression based on a pattern match.
	For example, to match an `accountId` attribute, enter the following in the expression builder:
	`#core.switchExpr(#root.accountId, '0000EXAMPLEID', 'Valid' , 'Invalid')`
	For a switch statement with multiple cases and a match, enter the following in the expression builder.
	`#core.switchExpr(#root.accountId, '0000EXAMPLEID1', 'Full Access', '0000EXAMPLEID2', 'Restricted Access' , '0000EXAMPLEID3', 'Read-only Access', 'No Access')`

Delete a mapping	Click the **Delete** icon.

> **Note**
>
> The default attributes are based on the directory type of the gateway used. For outbound provisioning, the `RDN` attribute defaults to `cn` for Active Directory.
> For inbound provisioning from Workday and SCIM identity stores, you can specify some additional options for onboarding new users. Learn more in Adding attribute mapping for inbound provisioning.

7. Click **Save**.

Adding attribute mapping for inbound provisioning

For inbound provisioning, you can specify additional options for onboarding new users.

The mapping is applied to the attribute coming from the source identity store before it is saved to the PingOne directory.

Steps

1. In the PingOne admin console, go to **Integrations** > **Provisioning**.
2. On the **Rules** tab, find the appropriate rule and click it to open the details panel.
3. Click the **Configuration** tab.

Copyright © 2025 Ping Identity Corporation

4. Click **Attribute Mapping**.

> **Important**
> You must have a source and target connection configured before you can set up attribute mapping.

5. Click the **Pencil** icon to edit the attribute mapping.
6. Review the attribute mappings for the configured identity store.

   The source attribute mappings for a particular identity store are provided. Learn more in Mapping attributes.

Option	Description
Add an attribute mapping	Click **+ Add**. Enter the source and target attributes.
Add a new source attribute	Enter the attribute name. In the list, select the `ADD:<attribute-name>` attribute. Map the added attribute to a target attribute.
Use the expression builder	Click the **Gear** icon. Learn more in Using the expression builder.
Delete a mapping	Click the **Delete** icon.

> **Note**
> Custom attributes created and mapped with the same name as an existing user sub attribute override the existing user sub attribute.
> For example, if you create a custom attribute called `country` and the user sub attribute `country` already exists, the custom attribute overrides it even if you configure the attribute with a different letter case.

7. Click **Next**.

   For inbound provisioning, you can specify additional options for onboarding new users. For inbound provisioning, the mapping is applied to the attribute coming from the source identity store before it is saved to the PingOne directory.

8. Enter the following as part of PingOne user onboarding:

Option	Description
Population	Select a population from the list. When users are synced to PingOne, they will be added to the specified population.

Copyright © 2025 Ping Identity Corporation

Option	Description
Authenticate via AD/LDAP	Specify whether to authenticate the user through the Active Directory or LDAP gateway user directory. If you select **Yes**, PingOne will be automatically set as the Authoritative identity provider. If you select **Yes**, specify a Gateway user type. If you select **No**, specify an Authoritative identity provider.
Authoritative Identity Provider	If you selected **No** for **Authenticate via AD/LDAP**, select the identity provider that will have authority over user records and credentials. PingOne is the default, but if you've configured another IdP you can select it here. Learn more in Authoritative identity providers. If you select PingOne as the **Authoritative identity provider**, specify the following options: ◦ **Set Password** (checkbox): Determine whether to specify a default password for new users. ◦ **Set Password** (field): Specify the default password in PingOne for users synced in from an external identity store as a source. Click **Set password**, then enter a literal value. You can also create a complex password using the functions in the expression builder. Learn more in Using the expression builder. **Note** You should use strong passwords, even for temporary passwords. ◦ **Reset their password on first login**: Force users to reset their password the first time they authenticate through PingOne.
Gateway User Type	If you selected **Yes** for **Authenticate via AD/LDAP**, select a gateway user type. The user type identifies users in the external directory. You must define a user type to use external authentication.

Copyright © 2025 Ping Identity Corporation

Option	Description
MFA Device Management	If your users have MFA devices that are managed by a PingOne service (for example, PingOne MFA and PingID), this setting controls how the inbound provisioner can impact those devices. Select from the following options. ◦ **Merge with devices in PingOne** (default): Select this option to add a device from the identity store into a user's existing device in PingOne. ◦ **Overwrite devices in PingOne**: Select this option to replace configured user devices in PingOne from the identity store. Only new devices mapped under attribute mappings are added. ◦ **Do not manage**: Select this option to disable device management. This option is recommended for users using PingID in the same environment and to avoid unexpected device unpairing from nickname conflicts. Inbound provisioning and PingID use the same device nicknames and cause device unpairing.

9. Click **Save**.

Authentication method management for inbound provisioning

Inbound provisioning manages all mapped email, voice, and SMS MFA attributes.

Nicknames

PingOne assigns nicknames to authentication methods (also called "devices"). The nicknames are used to identify authentication methods on user-facing pages, such as the **Device Selection** page.

Inbound provisioning uses nicknames when provisioning and synchronizing a user's authentication methods. The following are the managed nicknames used by inbound provisioning:

- `SMS 1`
- `SMS 2`
- `SMS 3`
- `Email 1`
- `Email 2`
- `Email 3`
- `Voice 1`

Copyright © 2025 Ping Identity Corporation

- `Voice 2`
- `Voice 3`

> **Important**
>
> The inbound provisioner might unpair existing MFA devices if an existing device has a name that matches a managed nickname, since they are assumed to be devices that the inbound provisioner should manage. In this case, where the managed nicknames are used by either PingID or manually entered, the recommended solution is to use the **Do not manage** option mentioned in Adding attribute mapping for inbound provisioning. It is also possible to give your MFA device a different nickname, as a workaround.

Mapping attributes to nicknames

Each device nickname is associated with one attribute on the **Attribute Mapping** tab of the provisioning rule. For example, the `Email 3` nickname holds the value of the `MFA Device Email 3` attribute.

You can map these attributes on the **Attribute Mapping** tab of the provisioning rule.

Synchronization

When synchronizing a user's authentication methods, inbound provisioning behaves as described in the following scenarios.

Synchronization scenarios

Scenario	Action
A device exists with a managed nickname, but the value does not match the value in the identity store.	The provisioner deletes and re-creates the device with the value from the identity store.
A value matches between PingOne and the identity store, but the device uses an unmanaged nickname.	The provisioner deletes and re-creates the device with the appropriate managed nickname.
A device exists with an unmanaged nickname and the value does not match the value in the identity store.	The provisioner does not make any changes.

Maximum number of authentication methods

Although inbound provisioning supports up to three SMS attributes, three email attributes, and three voice attributes, PingOne accepts a maximum of five authentication methods per user by default. You can adjust this in the PingOne settings.

Copyright © 2025 Ping Identity Corporation

Configuring outbound group provisioning

Use PingOne provisioning to sync groups along with its memberships out of PingOne to a connected *SaaS* application.

Before you begin

You must create a group in your PingOne admin console to select for outbound provisioning

> **Note**
>
> The recommended number of groups supported in a provisioning rule for outbound group provisioning is 1000. When syncing, you cannot sync external groups. This capability is limited to internal groups for outbound group provisioning.

Learn more in Creating a group.

About this task

The following provisioners support group provisioning:

- SCIM
- Salesforce workforce
- Salesforce communities
- Microsoft Azure Office 365
- Slack
- Google
- GitHub EMU

Membership type	Description
Group memberships	Memberships are a part of a group. Provisioners that support this: • Slack • SCIM • GitHub EMU
User memberships	Memberships are a part of a user. Provisioners that support this: • Google • Salesforce If there is an existing group with the same name on target, provisioning merges the group and its members.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Integrations → Provisioning**.
2. On the **Rules** tab, locate the rule that you want to use, and click the rule to open the details panel.
3. On the **Configuration** tab, click **Group Provisioning**.
   - To add groups, click **Add Groups**.
   - To search groups, enter a group name in the **Search Group Name** field.
   - To edit groups, click the **Pencil** icon and select a group in **All Groups**.
   - To remove a group, clear the check-box for the group in **All Groups.**
   - To view provisioned groups, click **Selected groups**.
   - To accept a merge or overwrite memberships when a group with the same name exists on the target, click the checkbox next to **I understand and want to continue**, in the **Merge Group Memberships** or **Overwrite Group Memberships** modal.

     > **Note**
     >
     > Merging or overwriting memberships only applies to SCIM, Slack and GitHub EMU provisioning connections. Learn more in Creating a Slack connection, Creating a SCIM connection, and Creating a GitHub EMU connection.

4. Click **Save**.

Enabling or disabling a connection

You must enable a connection before you can use it in a rule.

Steps

1. Go to **Integrations → Provisioning**.
2. Click the **Connections** tab.
3. Find the appropriate entry and click it to show the details panel.
4. In the upper right, click the toggle switch to enable or disable the connection.

Result

The toggle moves to the left (gray) when disabled, to the right (green) when enabled.

Enabling or disabling a rule

You must enable a rule before you can use it for provisioning. If you enable a rule then users will be provisioned based on the attribute mapping and filter criteria for the rule. If you disable a rule then all provisioning based on that rule will stop.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Integrations → Provisioning**.
2. Click the **Rules** tab.
3. Find the appropriate entry and click it to show the details panel.
4. In the upper right, click the toggle switch to enable or disable the rule.

Result

The toggle moves to the left (gray) when disabled, to the right (green) when enabled.

Sync status

The sync status shows the sync summary and current status of users and groups of a provisioning connection.

Sync updates

Sync updates occur when there is a change at the source on a user, group, or membership if the target supports group provisioning. The provisioning service updates the user at the target and keeps the source and target in sync.

Sync frequency

Sync frequency depends on the provisioner and is not configurable.

For outbound provisioning, changes are near real-time. When there is a change to a user in PingOne, the target identity store is updated immediately.

For inbound provisioning with Workday, a polling mechanism checks the source identity store every 15 minutes. When there is a circuit breaker due to polling failure, the reset is 12 hours. After 12 hours, the polling mechanism will attempt to run a full re-sync for the associated provisioning rule. For LDAP inbound poll failure, the reset is 30 minutes.

Learn more about inbound and outbound provisioning in Inbound and Outbound Provisioning.

To see your sync status, see Viewing sync status.

Identity store	Inbound	Outbound	Sync Frequency
SCIM	No	Yes	Real-time
Salesforce	No	Yes	Real-time
Salesforce Communities	No	Yes	Real-time
Salesforce Leads and Contacts	No	Yes	Real-time
Aquera	No	Yes	Real-time

Copyright © 2025 Ping Identity Corporation

Identity store	Inbound	Outbound	Sync Frequency
Workday	Yes	Yes	Users are retrieved from the source identity store using a polling mechanism. For every subsequent update, polling occurs every 15 minutes.
Microsoft Azure (Office 365)	No	Yes	Real-time
Zoom	No	Yes	Real-time
Slack	No	Yes	Real-time
ServiceNow	No	Yes	Real-time
Google Workspace	No	Yes	Real-time
GitHub EMU	No	Yes	Real-time
LDAP Gateway	Yes	Yes	For inbound sync, users are retrieved from the source identity store using a polling mechanism. For every subsequent update, polling occurs every 2 - 3 minutes. For outbound sync is real-time

Viewing sync status

Use the **Provisioning** page to see the sync status for a provisioning connection.

Steps

1. Go to **Integrations → Provisioning**.
2. On the **Rules** tab, locate the appropriate rule entry, and click it to open the details panel.

> **Note**
> The rule must be enabled for the sync summary to be visible. Learn more in Enabling or disabling a rule.

Result

The **Sync summary** section shows details about current sync operations, such as last successful sync and sync failures. If you notice synchronization failures for a provisioning connection, use the information in the following tables to identify any issues.

Copyright © 2025 Ping Identity Corporation

The information in the summary differs slightly based on the type of provisioning connection.

Outbound provisioning

Item	Description
Sync summary	Shows details about current sync operations.
Audit logs	To review audit logs, click **Audit logs**.
Resync	Click **Resync** to resync a particular rule. Re-syncing occurs to all entities, users and groups. Any entities out of sync will be in sync with the source.
Users	The current status of users, such as `Active`, `Inactive`, or `Failed`.
Last sync	The date of the most recent sync from the target.
Impacted	The total number of users targeted by the rule.
Success	The total number of impacted users fully synced to the target.
Unsynced	The total number of impacted users for which an account does not exist at the target and the user was not synced.
Partial Synced	The total number of impacted users for which an account does exist at the target but might be out of sync.
Failed	The total number of impacted users not synced due to an error.
Groups	The current status of groups, such as `Active`, `Inactive`, or `Failed`.
Impacted	The total number of groups targeted by the rule.
Success	The number of groups fully synced to the target identity store.
Failed	The number of groups that were not synced to the target identity store or that contain group members that were not synced.

Copyright © 2025 Ping Identity Corporation

Inbound provisioning

Item	Description
Sync summary	The current status of the rule, such as `Active`, `Inactive`, or `Failed`.
Last sync	The date and time of the most recent sync operation.
Last poll	The last time that the source connection was polled for any changes.
Last write-back (Workday connections only)	The date and time of the most recent outbound (write-back) update.
Impacted users	The number of users that match the provisioning filter but might not have been provisioned yet.
Synced users	The number of users fully synced to the target user store. The user exists in the target data store and has been updated based on the attribute mapping of the rule.
Unsynced users	The number of users for which an account does not exist in the target user store, but the user was not synced.
Partial synced users	The number of users for which an account exists in the target user store, but the user attributes are not fully synced.
Sync failures	The number of users that were not synced due to error.
Write-back failures (Workday connections only)	The number of users that were not updated for outbound (write-back) updates.

Outbound provisioning sync summary examples

The following are outbound provisioning examples and their sync summaries.

Example	Sync Summary
When a provisioning rule is configured to a target that does not support group provisioning, the sync summary only presents stats on **Users**.	The sync summary has only one section: • **Users**
When a provisioning rule is configured to a target that does support group provisioning, the sync summary presents stats on **Users** as well as on **Groups**.	The sync summary has two sections: • **Users** • **Groups**

Copyright © 2025 Ping Identity Corporation

Example	Sync Summary
A provisioning rule is configured to sync two groups with two users in each, and users failed to sync on the target. In that case, because the users didn't get through, provisioning service records those users as a user **Failed** event.	The sync summary appears as follows: **Users** • **Impacted: 2** • **Failed: 2** **Groups** • **Impacted: 2** • **Success: 2** • **Failed: 0**
A provisioning rule is configured to sync five groups. All groups sync successfully, but one membership doesn't get updated on the target for one group. Provisioning service records that as a **Failed**event on membership under **Groups**.	The sync summary appears as follows: **Groups** • **Impacted: 5** • **Success: 4** • **Failed: 1**
A provisioning rule is configured to sync five users, and as part of your target connection, **Allow Users to be Created** is not checked. Provisioning service records those users as an **Unsynced** event.	The sync summary appears as follows: **Users** • **Impacted: 5** • **Success: 0** • **Partially Synced: 0** • **Unsynced: 5** • **Failed: 0**
A provisioning rule is configured to sync five users, and as part of your target connection, **Allow Users to be Updated** is not checked. There is an update made on only one user after the last successful sync. Provisioning service records that as a **Partially Synced** event.	The sync summary appears as follows: **Users** • **Impacted: 5** • **Success: 5** • **Unsynced: 0** • **Partially Synced: 1** • **Failed: 0**

Using reporting to identify sync issues

You can run a targeted report to identify general sync issues.

Steps

1. Go to **Monitoring → Audit**.
2. For Filter type, select **Event type**.

Copyright © 2025 Ping Identity Corporation

3. For Filter, select the following:
   - `Provisioning Sync Failure`
   - `Provisioning Identify Sync Failure`

   > **Note**
   > There are several other provisioning-related filters that you can also use depending on your issue.

4. Click **Run**.

Next steps

- In the results list, see the **Description** column for specific failures.
- In the **Details** column, you can click **View** to see more detailed information.

Using user identity details to identify sync issues

Use the details page to identify specific sync issues for a particular user or users.

Steps

1. Go to **Directory → Users**.
2. Locate the appropriate user. You can browse or search for users.
3. Click the user entry to open the details panel.
4. Click **Services → Sync Status**.

   > **Note**
   > Membership sync status shows for provisioners that support outbound group provisioning.

Next steps

See the **Sync Status** for specific failures. Sync failures are often due to errors with attribute mapping.

Using group identity details to identify sync issues

You can use the group details panel to identify specific sync issues for a particular group.

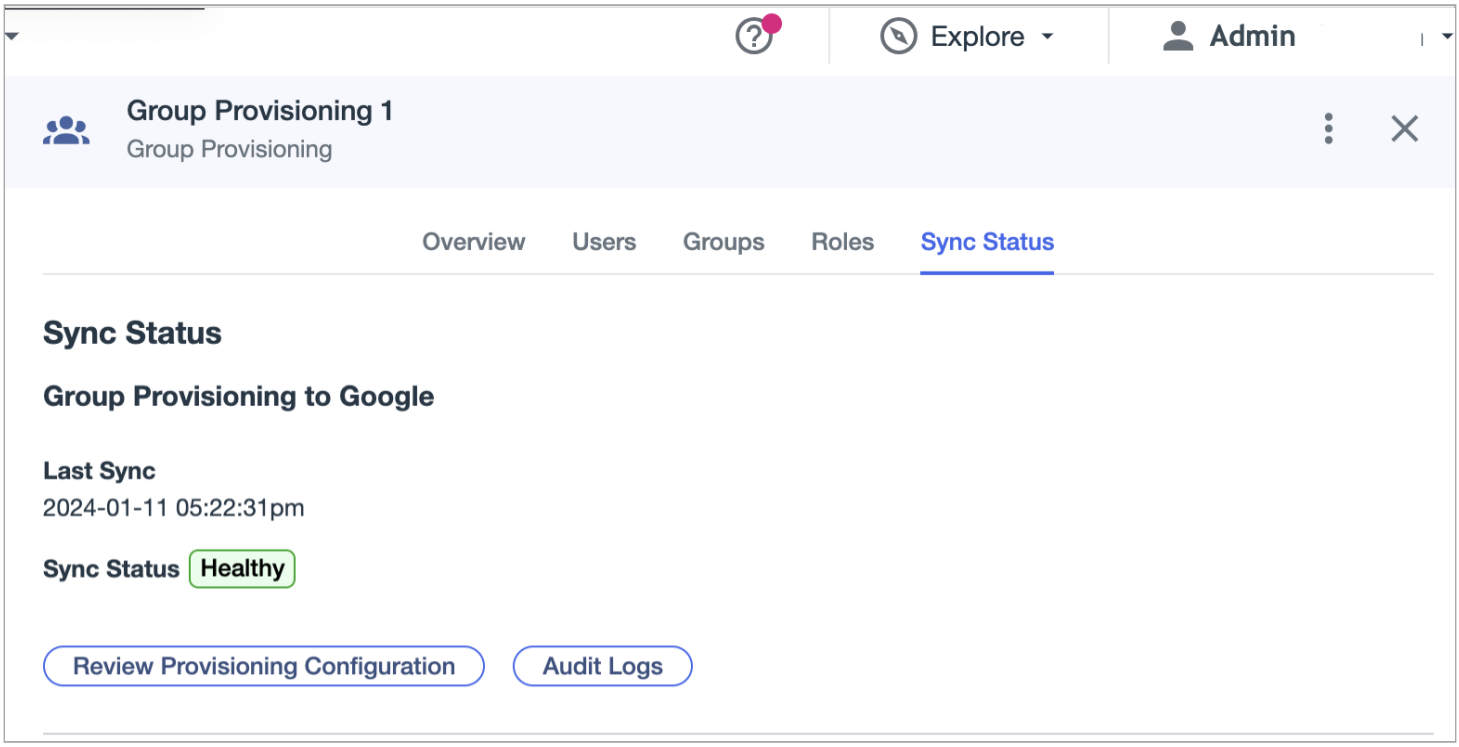
About this task

To view the sync status of a group:

Steps

1. Go to **Directory → Groups** and browse or search for the group.
2. Click the group entry to open the details panel.
3. Click **Sync Status**.

Copyright © 2025 Ping Identity Corporation



Next steps

See the **Sync Status** for specific failures.

Using audit logs to identify sync issues

Use the audit logs in the rule details panel to identify specific issues for a particular group.

Steps

1. Go to **Integrations → Provisioning**.
2. Click the **Rules** tab, locate the rule entry, and click it to show the details panel.

> **Note**
>
> The rule must be enabled for the sync summary to be visible. For more information, see Enabling or disabling a rule.

3. Click **Audit Logs**.

Result

An audit log with a pre-populated filter for the rule displays.

Provisioning configuration change resync behavior

When you change provisioning rule configurations, some changes trigger an automatic full resync, while other changes do not.

The following table describes the resync behavior for the provisioning rule configuration options:

Copyright © 2025 Ping Identity Corporation

Configuration option	Triggers a full resync
Name (connection) A unique identifier for the connection.	No
Description (connection) An optional brief characterization of the connection.	No
Configure Authentication (connection) Includes authentication details based on your connection. Changes to authentication configurations on a provisioning connection will trigger a resync.	Yes
Configure Preferences (connection) Includes preference details based on your connection. Updates to preferences configurations on a provisioning connection will trigger a resync.	Yes
Actions (connection) Changes to the advanced workflow actions won't trigger a resync. For example, when you see a user's sync status as **Partial Sync**, the **Allow Users to be Updated** option is disabled and prevents the user from being fully synced. Enabling**Allow Users to be Updated**does not automatically trigger a resync. Click **Resync,** to sync the rule and update the user on the target system. **Note** Manually clicking **Resync**, resyncs all users between the source and target that are part of the provisioning rule. Learn more in Sync Status	No
User Base DN (LDAP) Defines the users that you want to provision. For inbound provisioning, it specifies the source of the users that will be imported into PingOne. Provisioning supports syncing from LDAP directories. Whenever there are any changes made to a pre-defined Base DN, an auto re-sync will be triggered.	Yes
Name (rule) A unique identifier for the rule.	No
Description (rule) An optional brief characterization of the rule.	No

Copyright © 2025 Ping Identity Corporation

Configuration option	Triggers a full resync
User Filter A filter used to specify which identities are provisioned, based on factors such as population, group, or other user attributes.	Yes
LDAP Filter For inbound provisioning through an LDAP gateway, an LDAP filter expression defines the users that will be provisioned.	Yes
Attribute Mapping Maps PingOne user attributes from attributes in an external identity store. For outbound provisioning, the mapping is applied to the attribute coming from the PingOne directory before it's saved to the target identity store.	Yes
PingOne user onboarding For inbound provisioning, specifies additional options for onboarding new users. Learn more in Attribute mapping for inbound provisioning.	Yes
Group Provisioning Syncs groups along with their memberships out of PingOne to a connected SaaS application. Adding a new group or removing an existing group from the rule triggers a resync. Learn more in Configuring outbound group provisioning	Yes
Group Name A unique identifier for the group.	No
User attributes Determines the types of data that are stored for each user. **Note** When you update a user attribute that is not a part of attribute mapping, it does not trigger a resync. Learn more in Adding user attributes.	No **Note** When you update a user attribute that is not a part of attribute mapping in Workday, it triggers a sync for that particular user. Other users are not affected.
Resync Resyncing occurs to all entities, users, and groups. Any entities out of sync will be synchronized with the source. Click **Resync** to resync a particular rule.	Yes

Copyright © 2025 Ping Identity Corporation

Creating a SCIM connection

You can set up provisioning to or from a (System for Cross-domain Identity Management (SCIM) identity store. You can also use the PingOne API to set up inbound SCIM for user provisioning. For more information, see SCIM in the PingOne API Reference.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **+** and then click **New connection**.
3. On the **Identity Store** row, click **Select**.
4. Click **SCIM Outbound**, click **Select**, and then click **Next**.
5. Enter a name and description for this provisioning connection.

   The connection name appears in the provisioning list after you've saved the connection.
6. Click **Next**.
7. On the **Configure authentication** panel, enter the following
   - **SCIM base URL**: The fully qualified URL to use for the SCIM resources, such as `https://scim-example.com/v2/`.
   - **Users resource**: The endpoint for the SCIM `User` resource.
   - **SCIM version**: The SCIM version to use for the connection.
   - **Groups Resource**: The endpoint for the SCIM `Groups`
   - **Authentication method**: The SCIM authentication method to use for the connection.

     You can choose to use no authentication (**None**). For all other methods, additional entry fields are displayed, depending on the selected authentication method.

     > **Note**
     >
     > **Basic Authentication** provides limited security:
     > - The identity store configuration will have the provided Basic Auth credentials.
     > - The authentication scope is exactly that of the Basic Auth user, rather than some subset of the user data.
     >
     > If possible, you should use the **OAuth 2 Bearer Token** or **OAuth 2 Client Credentials** authentication methods.

     - **Basic Authentication**
       - **Basic Auth User**: Enter the Basic Auth user for the identity store.
       - **Basic Auth Password**: Enter the Basic Auth user password for the identity store.
       - **Auth Type Header**: Select **Basic**, **Bearer**, **OAuth Client Credentials**, or **Custom** (to supply your own header configuration).

         If you select **Custom**, the **Custom Header** entry field is displayed. Enter the custom header configuration.

Copyright © 2025 Ping Identity Corporation

> **Note**
> Custom headers added here will be added only as authorization headers in the request.

- **OAuth 2 Bearer Token**
  - **OAuth Access Token**: Enter the OAuth access token value supplied by the authorization server for the identity store.
  - **Auth Type Header**: Select **Basic**, **Bearer**, **OAuth Client Credentials**, or **Custom** (to supply your own header configuration).

    If you select **Custom**, the **Custom Header** entry field is displayed. Enter the custom header configuration.

> **Note**
> Custom headers added here will be added only as authorization headers in the request.

- **OAuth 2 Client Credentials**
  - **OAuth Token Request**: Enter the endpoint URL used to obtain an access token, such as `https://scim-example.com/as/token.oauth2`.
  - **OAuth Client ID**: Enter the client ID registered with the OAuth server for the provisioning identity store.
  - **OAuth Client Secret**: Enter the client secret value associated with the OAuth client ID.
  - **Auth Type Header**: Select **Basic**, **Bearer**, **OAuth Client Credentials**, or **Custom** (to supply your own header configuration).

    If you select **Custom**, the **Custom Header** entry field is displayed. Enter the custom header configuration.

> **Note**
> Custom headers added here will be added only as authorization headers in the request.

8. Click **Test connection** to verify that PingOne can establish a connection to the SCIM resource.

   Result:

   If there are any issues with the connection, a **Test Connection Failed** dialog box opens. Click **Continue** to resume the setup with an invalid connection.

   > **Important**
   > You cannot use the connection for provisioning until you have established a valid connection to SCIM. To retry, click **Cancel** in the **Test Connection Failed** dialog box and repeat step 7.

   Troubleshooting:

   Learn more about troubleshooting your connection in Troubleshooting Test Connections Failure.

9. In the **Configure preferences** and **Actions** sections, enter the user filter and the action to take when deprovisioning users.

   The filtering parameters are optional.

Copyright © 2025 Ping Identity Corporation

Option	Description
User filter expression	Determines how the connection uses the specified **User Identifier** to match existing users in the target identity store to the users being provisioned from the source identity store. Learn more in SCIM filter expressions.
User identifier	The identifier for the user filter expression.
Custom Attribute Schema URNs (optional)	A comma-delimited list of schema URNs to define a location for custom attributes. Use this option if the SCIM provider does not follow the standard naming convention for schema extensions in which custom attributes are defined. That is, URNs of the form `urn:ietf:params:scim:schemas:extension:<Organization Name>:2.0:User`.
Group membership handling	Determines whether to update or replace target groups with PingOne memberships. Select **Merge** or **Overwrite**. **Note** Merging or overwriting memberships only applies to SCIM, Slack, and GitHub EMU provisioning connections. **Important** There is a limitation when syncing groups and group memberships to AWS Identity Centre and Atlassian Cloud. Learn more in SCIM provisioning known limitations.
Allow users to be created	Determines whether to create a user in the target identity store when the user is created in the source identity store.
Allow users to be updated	Determines whether to update user attributes in the target identity store when the user is updated in the source identity store.
Allow users to be disabled	Determines whether to disable a user in the target identity store when the user is disabled in the source identity store.
Allow users to be deprovisioned	Determines whether to deprovision a user in the target identity store when the user is deprovisioned in the source identity store.
Remove action	The action to take when removing a user from the target identity store.

Copyright © 2025 Ping Identity Corporation

Option	Description
Deprovision on rule deletion	Determines whether to deprovision users if the associated provisioning rule is deleted.

10. Click **Save**.

Result

The SCIM provisioning profile is complete and is added to the list of provisioning profiles on the **Provisioning** page.

Next steps

To sync group members out of PingOne into a software as a service (SaaS) application, follow the instructions in Configuring outbound group provisioning.

SCIM provisioning features

Provision users from the PingOne identity store to a System for Cross-domain Identity Management (SCIM)-compliant identity store.

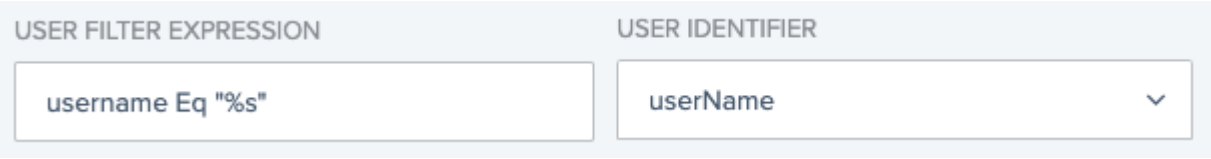
The provisioner offers the following features:

- Supports the SCIM 1.1 and 2.0 specifications
- User provisioning, including `create`, `update`, `disable`, and `delete`
- Supports SCIM core and enterprise attributes
- Basic authentication, OAuth 2 bearer token, and OAuth 2 client credentials authentication
- Supports SCIM overrides, such as filter expression, authorization header type, and users API path
- Ability to provision disabled user accounts
- Configurable deprovisioning actions
- Configurable group provisioning

SCIM filter expressions

Use SCIM filter expressions to define how the provisioner matches existing users in the target application to users in the identity store. The expression overrides the default filter expression that is set by the User Identifier field.

The user filter expression contains the attribute name, the operation, and the attribute value. The attribute value is represented by `"%s"` in the expression.



Copyright © 2025 Ping Identity Corporation

The `“%s”` variable stores the value of the user identifier. The value that you select in the User Identifier list, such as `userName` or `workEmail`, is used in the User Filter Expression and replaces the contents of the `"%s"` variable.

Example filter expressions:

- `username Eq "%s"`
- `email Co "%s"`

For more information, see the Filtering section in the SCIM 2.0 specification RFC 7644.

SCIM provisioning known limitations

The following are known issues or limitations with System for Cross-domain Identity Management (SCIM) user provisioning.

Service provider (SP) connections

- The `Unique User Identifier` cannot be changed in an SP connection configuration.

  To change to a different `Unique User Identifier`, delete the existing connection and then create a connection with the new `Unique User Identifier`.

- All SP connections with the same target must use the same `Unique User Identifier`.

  If multiple SP connections are created for the same target, every subsequent connection will use the `Unique User Identifier` configured in the first connection that was created.

Attributes

- The connector has a limit of one value per type (for example, home, work, and other) for multi-value attributes (for example, email, phone, and address).
- If the application does not specify type or primary information on multi-value attributes, unexpected behavior can occur.

  During an update, existing attributes on the application cannot be removed, and the desired value cannot be correctly set as primary.

- The provisioner cannot clear a user attribute after it is set.
- PingOne does not support multi-value attributes, so the first attribute value will be used.
- If the target application supports two email attributes and one attribute is empty, the provisioner populates both attributes with the email address and sets both as primary.

  This can produce unexpected effects in some target applications.

Other

- SCIM-compliant SPs might implement or interpret the SCIM standards differently, which can result in behavior that is not consistent with the intended use of the SCIM provisioner.
- When syncing groups and group memberships to AWS Identity Centre, you can encounter a `400 invalid` filter when a group’s name has a special character in a different language.

Copyright © 2025 Ping Identity Corporation

- When syncing groups and group memberships to Atlassian Cloud, renaming a group is not supported. Updating the Group Name causes a UI mismatch on the group's Sync Status(Healthy - for overwrite / Sync Failure - for merge). Adding and removing members continues to work.
- When provisioning users and groups to AWS Identity Center, you might encounter an error such as `The resource could not be modified. [prov_exception_msg] [SCIM004,]` .The SCIM Provisioner responds with the message `Request is unparsable, syntactically incorrect, or violates schema` .

> **Note**
>
> For AWS, every user must have a First name, Last name, Username, and Display name value specified. If any of these values are missing from a user, that user is not provisioned.
> Learn more about special characters that you must not use in attributes synchronized with SCIM in Limitations and ListUsers in the AWS documentation. The `<>;:%` SCIM filter expression is in the correct format as defined by AWS.

- When provisioning users and groups to Atlassian Cloud, the SCIM filter is `username eq "%s"` . If given an invalid SCIM filter, you might encounter an error such as `The resource could not be modified. [prov_exception_msg] [SCIM004]` .The SCIM Provisioner responds with the message `Resource [USER] invalid filter` .

Creating a Salesforce connection

Use a Salesforce connection to enable provisioning from PingOne to Salesforce.

Before you begin

Make sure that you have:

- An existing Salesforce account.
- The full domain for the Salesforce account.

> **Tip**
>
> You can find the domain in the URL when signed on to the account. For example, `<myCompanyName>.my.salesforce.com` .

- The client ID and client secret for the connected application. For more information, see Create a Connected App in the Salesforce documentation.
- The OAuth access token and refresh token for the connected application. Learn more in Getting an API access token from Salesforce.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **+** and then click **New connection**.
3. On the **Identity Store** line, click **Select**.
4. Click **Salesforce**, click **Select**, and then click **Next**.
5. Enter a name and description for the provisioning connection.

Copyright © 2025 Ping Identity Corporation

The connection name appears in the provisioning list after you save the connection.

6. Click **Next**.

7. On the **Configure authentication** panel, enter the values for the following fields:

Field	Value
Salesforce domain	The full domain for the Salesforce account. **Tip** You can find the domain in the URL when signed on to the account. For example, `<myCompanyName>.my.salesforce.com`.
Client ID	The **Consumer Key** value from Salesforce for the connected application. For more information, see Create a Connected App in the Salesforce documentation.
Client secret	The **Consumer Secret** value from Salesforce for the connected application.
OAuth access token	The access token from Salesforce for the connected application. **Tip** You can use the Ping Identity OAuth Configuration Service (OCS) to get the token. For more information, see Getting an API access token from Salesforce.
OAuth refresh token	The refresh token from Salesforce for the connected application.

8. Click **Test connection** to verify that PingOne can establish a connection to Salesforce.

Result:

If there are any issues with the connection, a **Test Connection Failed** dialog box opens. Click **Continue** to resume the setup with an invalid connection.

> **Important**
> You cannot use the connection for provisioning until you have established a valid connection to Salesforce. To retry, click **Cancel** in the **Test Connection Failed** dialog box and repeat step 7.

Troubleshooting:

Learn more about troubleshooting your connection in Troubleshooting Test Connections Failure.

Copyright © 2025 Ping Identity Corporation

9. On the **Configure preferences** panel, configure the following options:

Option	Description
Permission set management	Determines how to handle permission sets in the Salesforce identity store. Select **Merge with permission sets in Salesforce** or **Overwrite permission sets in Salesforce**. If you select **Merge with permission sets in Salesforce** and a permission set is added in the datastore, PingOne adds it to the user's existing permission sets in Salesforce. PingOne does not remove any permission sets added in Salesforce by other sources. If you select **Overwrite permission sets in Salesforce**, and a permission set is added or removed in the datastore, PingOne overwrites the user's permission sets in Salesforce with those from the datastore.
Allow users to be created	Determines whether to create a user in the Salesforce identity store when the user is created in the PingOne identity store.
Allow users to be updated	Determines whether to update user attributes in the Salesforce identity store when the user is updated in the PingOne identity store. **Note** If you clear the **Allow users to be updated** or **Allow users to be disabled** check boxes, the child options that depend on a user update will become unavailable.
Allow users to be disabled	Determines whether to disable a user in the Salesforce identity store when the user is disabled in the PingOne identity store.
Action when disabling users	Determines the action to take when deprovisioning users from the Salesforce identity store: ◦ **Disable**. When deprovisioning, PingOne disables the user. The user cannot sign on, and their data is not visible to other users in Salesforce. ◦ **Freeze**. When deprovisioning, PingOne freezes a user. The frozen user cannot sign on, but the user's data, such as profile and activity, is still visible to other users in Salesforce. For more information, see Freeze or Unfreeze User Accounts in the Salesforce documentation.

Copyright © 2025 Ping Identity Corporation

Option	Description
Allow users to be deprovisioned	Determines whether to deprovision a user in the Salesforce identity store when the user is deprovisioned in the PingOne identity store.
Remove action	Determines the action to take when removing a user from the Salesforce identity store.
Deprovision on rule deletion	Determines whether to deprovision users if the associated provisioning rule is deleted.

10. Click **Finish**.

Next steps

To sync group members out of PingOne into a software as a service (SaaS) application, follow the instructions in Configuring outbound group provisioning.

Salesforce attribute mapping

The following table lists common Salesforce attributes that can be mapped for user provisioning.

For a more complete list of Salesforce attributes, see Users in the Salesforce documentation.

Attribute	Description
Active	The status of the user account in Salesforce.
Alias	The user's short name used on list pages, reports, and other pages where the entire name does not fit. **Important** This value must be 8 characters or fewer.
Email	The user's email address.
Language Locale Key	The user's language.
Username	The user's PingOne username and Salesforce login. **Important** This value must be in the format of an email address.
Email Encoding Key	The email encoding. A default set of email encoding options is provided based on your Salesforce environment.
Last name	The user's last name.

Copyright © 2025 Ping Identity Corporation

Attribute	Description
Locale Sid Key	The locale of the user. A default set of options is provided based on your Salesforce environment.
Time Zone Sid Key	The user's timezone. A default set of options is provided based on your Salesforce environment.
Profile Id	The identifier associated with a user profile type in Salesforce. The profile determines the type of user and some permissions. See Profiles in the Salesforce documentation.
First name	The user's first name.

Creating a Salesforce Communities connection

You can set up provisioning for a connection to a Salesforce Communities identity store.

Before you begin

You should review the information about creating users and cloning community profiles in Salesforce Communities. For more information, see the Salesforce Communities integrations documentation.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **+** and then click **New connection**.
3. On the **Identity Store** line, click **Select**.
4. Click **Salesforce Communities**, click **Select**, and then click **Next**.
5. Enter a name and description for this provisioning connection. The connection name will appear in the list when you've completed and saved the connection.

   The connection name appears in provisioning the list after you save the connection.
6. Click **Next**.
7. On the **Configure authentication** screen, enter the following:

Field	Value
Salesforce domain	The full domain for the Salesforce account. **Tip** You can find the domain in the URL when lsigned on to the account. For example, `<myCompanyName>.my.salesforce.com`.

Copyright © 2025 Ping Identity Corporation

Field	Value
Client ID	The **Consumer Key** value from Salesforce for the connected application. For more information, see Create a Connected App in the Salesforce documentation.
Client secret	The **Consumer Secret** value from Salesforce for the connected application.
OAuth access token	The access token from Salesforce for the connected application. **Tip** You can use the Ping Identity OAuth Configuration Service (OCS) to get the token. For more information, see Getting an API access token from Salesforce.
OAuth refresh token	The refresh token from Salesforce for the connected application.

8. Click **Test connection** to verify that PingOne can establish a connection to Salesforce Communities.

   Result:

   If there are any issues with the connection, a **Test Connection Failed** dialog box opens. Click **Continue** to resume the setup with an invalid connection.

   > **Important**
   > You cannot use the connection for provisioning until you have established a valid connection to Salesforce Communities. To retry, click **Cancel** in the **Test Connection Failed** dialog box and repeat step 7.

   Troubleshooting:

   Learn more about troubleshooting your connection in Troubleshooting Test Connections Failure.

9. On the **Configure preferences** screen, enter the following:

Copyright © 2025 Ping Identity Corporation

Option	Description
Permission set management	Determines how to handle permission sets in the Salesforce Communities identity store. Select **Merge with permission sets in Salesforce** or **Overwrite permission sets in Salesforce**. If you select **Merge with permission sets in Salesforce** and a permission set is added in the data store, PingOne adds it to the user's existing permission sets in Salesforce Communities. PingOne does not remove any permission sets added in Salesforce Communities by other sources. If you select **Overwrite permission sets in Salesforce** and a permission set is added or removed in the data store, PingOne overwrites the user's permission sets in Salesforce Communities with those from the data store.
Allow users to be created	Determines whether to create a user in the Salesforce Communities identity store when the user is created in the PingOne identity store.
Allow users to be updated	Determines whether to update user attributes in the Salesforce identity store when the user is updated in the PingOne identity store. **Note** If you clear the **Allow users to be updated** or **Allow users to be disabled** check boxes, the child options that depend on a user update will become unavailable.
Allow users to be disabled	Determines whether to disable a user in the Salesforce Communities identity store when the user is disabled in the PingOne identity store.
Action when disabling users	Determines the action to take when deprovisioning users from the Salesforce Communities identity store: ◦ **Disable**. When deprovisioning, PingOne disables the user. The user cannot sign on, and their data is not visible to other users in Salesforce Communities. ◦ **Freeze**. When deprovisioning, PingOne freezes a user. The frozen user cannot sign on, but the user's data, such as profile and activity, is still visible to other users in Salesforce Communities. For more information, see Freeze or Unfreeze User Accounts in the Salesforce documentation.

Copyright © 2025 Ping Identity Corporation

Option	Description
Allow users to be deprovisioned	Determines whether to deprovision a user in the Salesforce Communities identity store when the user is deprovisioned in the PingOne identity store.
Remove action	Determines the action to take when removing a user from the Salesforce Communities dentity store.
Deprovision on rule deletion	Determines whether to deprovision users if the associated provisioning rule is deleted.

10. Click **Finish**.

Result

The Salesforce Communities provisioning connection is complete and is added to the list of provisioning connections on the **Provisioning** page.

Next steps

To sync group members out of PingOne into a software as a service (SaaS) application, follow the instructions in Configuring outbound group provisioning.

Salesforce Communities provisioning features

The Salesforce Communities provisioner offers the following features.

Provision users from the PingOne identity store to Salesforce Communities:

- Create users
- Update users
- Deprovision users

Customize provisioning options:

- Deprovision users with a freeze or disable action
- Provision disabled users
- Merge or overwrite permission sets

Group provisioning

- Sync a group and its members from PingOne to Salesforce Community.

Salesforce Communities attribute mapping

The following table lists common Salesforce Communities attributes that can be mapped for user provisioning.

Copyright © 2025 Ping Identity Corporation

For a more complete list of Salesforce attributes, see Users in the Salesforce documentation.

Attribute	Description
Account Id	The identifier associated with a company in Salesforce Communities. This field is required for Salesforce Communities users when provisioning customer and partner users.
Alias	The user's short name used on list pages, reports, and other pages where the entire name does not fit. Must be eight characters or less.
Email	The user's email address.
Email Encoding Key	The email encoding. A default set of email encoding options is provided based on your Salesforce environment.
First name	The user's first name.
IsActive	The status of the user account in Salesforce Communities.
Language Locale Key	The user's language.
Last name	The user's last name.
Locale Sid Key	The locale of the user. A default set of options is provided based on your Salesforce environment.
Profile Id	The identifier associated with a user profile type in Salesforce. The profile determines the type of user and some permissions. See Profiles in the Salesforce documentation.
Time Zone Sid Key	The user's timezone. A default set of options is provided based on your Salesforce environment.
Username	The user's username and Salesforce login. This value must be in the format of an email address.

Salesforce Communities known limitations

The following are known issues and limitations with Salesforce Communities user provisioning.

Attributes

- The provisioner cannot clear user attributes after they have been set.
- Multi-attribute values are not supported.

Copyright © 2025 Ping Identity Corporation

Deprovisioning

- When deprovisioning a Salesforce customer or partner user, the provisioning connector does not unlink the user from the associated contact.
- If a customer or partner user is unlinked in Salesforce from the associated contact, any changes to the user in the data store causes the provisioning connector to create a new user in Salesforce and link it to the existing contact.
- Guest users in Salesforce cannot be frozen. If **Freeze Users** instead of **Disable** is selected in your provisioning options, the guest user will not be disabled or frozen.

Refresh tokens

- Refresh token policy must be set to **Refresh token is valid until revoked** for OAuth because expiring refresh tokens are not supported.

Salesforce Communities

- The provisioner can link users to `customer` and `partner` business accounts, but not `person` accounts. For more information, see the Accounts page in the Salesforce documentation.

Group provisioning

- Syncing memberships is not supported for Salesforce Community. Admins can set up group provisioning on Salesforce communities to sync only groups from PingOne.

Creating a Salesforce Leads and Contacts connection

You can set up provisioning for a connection to a Salesforce Contacts identity store.

About this task

You can provision PingOne identities as Salesforce Leads, Contacts, or Users. You can also promote or demote identities from one group to another. For more information, see Manage Leads and Contacts.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **+** and then click **New connection**.
3. For **Identity Store**, click the **Select** button.
4. Under **Salesforce Leads and Contacts**, click **Select**, and then click **Next**.
5. Enter a name and description for this provisioning connection. The connection name will appear in the list when you've completed and saved the connection.
6. Click **Next**.

Copyright © 2025 Ping Identity Corporation

7. On the **Configure authentication** screen, enter the following:
   - **Salesforce domain**. The full domain for the Salesforce account. You can find the domain in the URL when logged into the account. For example, `myCompanyName.my.salesforce.com`.
   - **Client ID**. The Consumer Key from Salesforce for the connected application. For more information, see Create a Connected App in the Salesforce documentation.
   - **Client secret**. The Consumer Secret from Salesforce for the connected application.
   - **OAuth access token**. The access token from Salesforce for the connected application. You can use the Ping Identity OAuth Configuration Service (OCS) to get the token. For more information, see Getting an API access token from Salesforce.
   - **OAuth refresh token**. The refresh token from Salesforce for the connected application.
8. Click **Test connection** to verify that PingOne can establish a connection to Salesforce Leads and Contacts.

   Result:

   If there are any issues with the connection, a **Test Connection Failed** dialog box opens. Click **Continue** to resume the setup with an invalid connection.

   > **Important**
   >
   > You cannot use the connection for provisioning until you have established a valid connection to Salesforce Leads and Contacts. To retry, click **Cancel** in the **Test Connection Failed** dialog box and repeat step 7.

   Troubleshooting:

   Learn more about troubleshooting your connection in Troubleshooting Test Connections Failure.
9. On the **Configure preferences** screen, enter the following:
   - **Record type**. Specify the type of Salesforce Contact to create: Contact or Lead. For more information, see Leads and Contacts in the Salesforce documentation.
   - **Allow records to be deleted**. Determines whether to delete a user in the target identity store when the user is deleted in the source identity store.
   - **Allow users to be created**. Determines whether to create a user in the target identity store when the user is created in the source identity store.
   - **Allow users to be updated**. Determines whether to update user attributes in the target identity store when the user is updated in the source identity store.
   - **Allow users to be disabled**. Determines whether to disable a user in the target identity store when the user is disabled in the source identity store.
   - **Allow users to be deprovisioned**. Determines whether to deprovision a user in the target identity store when the user is deprovisioned in the source identity store.
   - **Remove action**. The action to take when removing a user from the target identity store.
   - **Deprovision on rule deletion**. Determines whether to deprovision users if the associated provisioning rule is deleted.

Copyright © 2025 Ping Identity Corporation

10. Click **Finish**.

Result

The Salesforce Contacts provisioning connection is complete and is added to the list of provisioning connections on the **Provisioning** page. If you see errors related to Salesforce provisioning, check for sync failures. See Viewing sync status.

Next steps

To define which users are provisioned and how attributes are mapped between PingOne and an external identity store, follow the instructions in Creating an outbound rule.

Salesforce Contacts provisioning features

The Salesforce Contacts provisioner offers the following features.

- Manage Leads and Contacts in Salesforce based on changes in an external datastore
- Enable the create, update, and delete capabilities independently

Manage Leads and Contacts

The provisioning connector synchronizes users from the PingOne datastore to Salesforce based on the `Email` attribute.

When you configure the attribute mappings in your service provider connection, you can set up synchronization by populating the `Email` attribute with a matching attribute from the datastore.

For example:

- In Salesforce, Janet's `Email` is `jsmith@example.com`.
- In your datastore, Janet's `mail` is `jsmith@example.com`.
- On the **Attribute Mapping** page, you map the `Email` attribute to `mail`.
- When the provisioning connector runs, the datastore user is provisioned with an `Email` of `jsmith@example.com`. This matches Janet's existing `Email` in Salesforce, so her information in the datastore is synchronized to her Salesforce account.

Lead and Contact record provisioning

Provisioning is triggered by any of the following:

- A user is added to the datastore group or filter that is targeted by the provisioning connector.

The target is determined in the provisioning connector configuration.

Lead and Contact record updates

Provisioning is triggered when a change occurs to a user attribute that is mapped in the provisioning connector configuration.

Copyright © 2025 Ping Identity Corporation

Lead and Contact record deprovisioning

Deletion is triggered by any of the following:

- A user is deleted from the user store.
- A user is disabled in the user store.
- A user is removed from the datastore group or filter that is targeted by the provisioning connector.

Salesforce Contacts attribute mapping

This section lists common attributes that can be mapped for provisioning to a Salesforce Contacts user store.

For a complete list of Salesforce attributes, see Users in the Salesforce documentation.

Attribute	Description
`Alias`	The user's short name used on list pages, reports, and other pages where the entire name does not fit. Must be eight characters or less.
`Email`	The user's email address.
`Email Encoding Key`	The email encoding. A default set of email encoding options is provided based on your Salesforce environment.
`First name`	The user's first name.
`IsActive`	The status of the user account in Salesforce Contacts.
`Language Locale Key`	The user's language.
`Last name`	The user's last name.
`Locale Sid Key`	The locale of the user. A default set of options is provided based on your Salesforce environment.
`Time Zone Sid Key`	The user's timezone. A default set of options is provided based on your Salesforce environment.
`Username`	The user's username and Salesforce login. This value must be in the format of an email address.

Salesforce Contacts known limitations

The following are known issues and limitations with Salesforce Contacts user provisioning.

Copyright © 2025 Ping Identity Corporation

Converted contacts and leads

When a Contact record is converted to a User in Salesforce:

- The Salesforce Contacts Connector can continue to update the Contact record, but changes are not reflected in the new User record.
- The Salesforce Contacts Connector cannot delete the Contact record. Instead, it shows the following error.

```
[{"message":"Your attempt
to delete jsmith could not be completed because it is associated with
the following portal users.: jsmith@example.com\n","errorCode":"DELETE_FAILED","fields":[]}]
```

When a Lead record is converted to another record type in Salesforce:

- The Salesforce Contacts Connector can still delete the Lead record, but cannot update it. Instead, it shows the following error.

```
"[{"message":"cannot reference converted lead",
"errorCode":"CANNOT_UPDATE_CONVERTED_LEAD", "fields":[]}]"
```

- If the Lead record is deleted from your data store but not deleted from Salesforce, and a new Lead is created in the directory with the same email address, the synchronization fails with the message above.

Attributes

The provisioning connector cannot clear user attributes after they have been set.

Certificates

Adding a new certificate to PingFederate's trusted certificate authority (CA) store for use in a secure LDAP (or LDAPS) connection requires a server restart when a secure LDAP connection has already been attempted or established.

Deprovisioning

After deleting an LDAP user account, the provisioner doesn't remove the user in the next provisioning cycle when Group DN is specified until a new user is added to the targeted group. This limitation is compounded when the **User Create** provisioning option is disabled. For more details, see SaaS provisioner does not remove the user when Group DN is specified in the Ping Identity Knowledge Base.

Performance

The Salesforce Connector dynamically retrieves data from the customer's Salesforce instance. Depending on your Salesforce environment, this could cause some delays when you create a provisioning connection to Salesforce.

Refresh tokens

The refresh token policy must be set to **Refresh token is valid until revoked** for OAuth because expiring refresh tokens are not supported.

Copyright © 2025 Ping Identity Corporation

Creating an Aquera connection

Use an Aquera provisioning connection to provision PingOne identities to an Aquera user store.

Before you begin

We recommend that you review the information about creating users in Aquera. For more information, see the Aquera User Guide.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **+** and then click **New connection**.
3. For **Identity Store**, click the **Select** button.
4. Under **Aquera**, click **Select** and then click **Next**.
5. Enter a name and description for this provisioning connection. The connection name will appear in the list when you've completed and saved the connection.
6. Click **Next**.
7. On the **Configure authentication** screen, enter the following:
   - **Aquera SCIM URL**. The fully qualified URL to use for the SCIM resources, such as https://api.aquera.io/scim/. You can find this information on your Aquera Applications page.
   - **Connection profile**. Select the authentication method to use: **Basic Auth** or **Bearer Token**. Additional fields are displayed, depending on the selected method.

     > **Note**
     > The type of authentication to use is determined by the target SaaS application configured in Aquera. When you set up an application in Aquera, you might be constrained by the authentication methods supported by a particular application. For example, certain applications might support OAuth tokens only, while others might support basic authentication only.

   - **Basic Auth**
     - **Basic Auth User**. The user name for the target SaaS application in Aquera. The user name is configured during the application setup in Aquera.
     - **Basic Auth Password**. The password for the target SaaS application in Aquera. The password is configured during the application setup in Aquera.
   - **Bearer token**
     - **OAuth Access Token**. Enter the OAuth access token value for the target SaaS application in Aquera.
8. Click **Test connection** to verify that PingOne can establish a connection to Aquera.

   Result:

Copyright © 2025 Ping Identity Corporation

If there are any issues with the connection, a **Test Connection Failed** dialog box opens. Click **Continue** to resume the setup with an invalid connection.

> **Important**
>
> You cannot use the connection for provisioning until you have established a valid connection to Aquera. To retry, click **Cancel** in the **Test Connection Failed** dialog box and repeat step 7.

Troubleshooting:

Learn more about troubleshooting your connection in Troubleshooting Test Connections Failure.

9. On the **Configure preferences** screen, enter the following:
   - **Allow users to be created**. Determines whether to create a user in the target identity store when the user is created in the source identity store.
   - **Allow users to be updated**. Determines whether to update user attributes in the target identity store when the user is updated in the source identity store.
   - **Allow users to be disabled**. Determines whether to disable a user in the target identity store when the user is disabled in the source identity store.
   - **Remove action**. Select **Delete** or **Disable**. Determines whether to remove or disable a user in the target identity store when the user is deleted in the source identity store.
   - **Deprovision on rule deletion**. Determines whether to deprovision users if the associated provisioning rule is deleted.
10. Click **Finish**.

Result

The Aquera provisioning connection is complete and is added to the list of provisioning connections on the **Provisioning** page.

Next steps

To define which users are provisioned and how attributes are mapped between PingOne and an external identity store, follow the instructions in Creating an outbound rule.

Aquera provisioning known limitations

The following are known issues and limitations with Aquera user provisioning.

Partial updates

If the downstream provisioning from Aquera is provisioning to a service provider that doesn't support partial update operations, you cannot disable a user on deprovisioning because deprovisioning will be converted to a partial update operation rather than a delete operation.

Copyright © 2025 Ping Identity Corporation

Creating a Workday connection

Use the **Provisioning** page to create a connection between a Workday identity store and PingOne.

Before you begin

Ensure that you have:

- An existing Workday tenant.
- The hostname for the Workday tenant. Learn more in Identifying your Workday hostname.
- An Integration System User account in Workday. Learn more in Creating a Workday Integration System User.
- A write-back provisioning in your configuration, learn more in Configuring write-back provisioning.
- Reviewed the limitations of the Workday provisioner. Learn more in Workday provisioner known limitations.
- An Integration System created in Workday to enter your Integration System IDs. Learn more in Creating a Workday Integration System with a Field Override Service.

Steps

1. Go to **Integrations > Provisioning**.
2. Click **+** and then click **New connection**.
3. Click **Select** for **Identity Store**.
4. On the **Workday** tile, click **Select**. Click **Next**.
5. Enter a name and description for this provisioning connection.
6. Click **Next**.
7. In the **Configure Authentication** section, enter the following:
   - **User name**: The Workday Integration System User account. Learn more in Creating a Workday Integration System User.
   - **Password**: The password for the Workday Integration System User account.
   - **Tenant ID**: The name of your Workday tenant. To find the tenant name, start Workday and go to **Edit Tenant Setup - Security**. The tenant name is shown in the list.
   - **API host**: The hostname, including subdomain, for your Workday tenant. For example, `<your_subdomain>.workday.com`. Learn more about finding the hostname in Identifying your Workday hostname.
8. Click **Test Connection** to verify that PingOne can establish a connection to Workday.

   Result:

   If there are any issues with the connection, a **Test Connection Failed** dialog box opens. Click **Continue** to resume the setup with an invalid connection.

Copyright © 2025 Ping Identity Corporation

> **Important**
>
> You can't use the connection for provisioning until you've established a valid connection to Workday. To retry, click **Cancel** in the **Test Connection Failed** dialog box and repeat step 7.

Troubleshooting:

Learn more about troubleshooting your connection in Troubleshooting Test Connections Failure.

9. Click **Next**.
10. In the **Configure Preferences** section, enter the **Integration system IDs** to sync custom attributes from your Workday Integration Systems. To find the Integration System IDs, view your Integration System in Workday and click the list next to **System ID**.

    > **Note**
    >
    > You can add mulitple Integration System IDs, separated by commas.

11. Click **Save**.

Result

The Workday provisioning connection is added to the list of connections on the **Provisioning** page.

Next steps

Define which users are provisioned and how attributes are mapped between PingOne and an external identity store. Learn more in Creating an inbound rule.

Learn more about adding custom attributes from Workday in Adding Custom attributes from Workday into PingOne.

Add custom attributes in Workday and sync them into PingOne. Learn more in Creating a Workday Integration System with a Field Override Service and Syncing custom attributes from Workday into PingOne.

Configuring write-back provisioning

You can configure write-back provisioning from PingOne to the Workday user directory. Use write-back provisioning to update certain user attributes in the Workday user directory. You enable write-back provisioning by setting attribute mappings to bi-directional.

Before you begin

- To enable write-back provisioning, you must first configure a Workday provisioning connection. See Creating a Workday connection.
- Configure permissions for the security group you created when you configured the Workday provisioning connection. See Configuring Business Process Security Policy permissions for write-back.

About this task

With bi-directional sync, if an attribute is changed in either directory, the other directory will be updated as well. Changes made in the Workday directory are updated on the next scheduled inbound sync, but changes made in the PingOne directory are updated immediately.

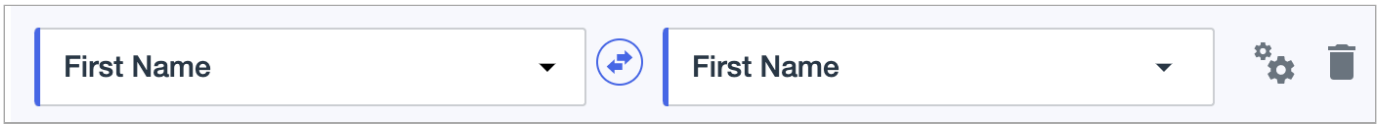
Copyright © 2025 Ping Identity Corporation

Only native source attributes can be used for write-back provisioning. You cannot use expressions and literal values for write-back provisioning. When you enable bi-directional mapping for an attribute, PingOne automatically adds the required `WID` (Worker ID) attribute to uniquely identify users within the Workday directory. `WID` is typically mapped to `External ID` in PingOne.

> **Note**
>
> Some attributes are dependent on other attributes for write-back provisioning. For example, to write back a `First Name` attribute, you must also set the following attributes to write-back: `Middle Name`, `Last Name`, and `Name Locale`. For more information, see Workday attribute mapping. Attributes that are set to write-back (bi-directional) are indicated by a double arrow on the attribute mapping page.

Steps

1. Go to **Integrations → Provisioning**.
2. Click the **Rules** tab.
3. Locate the existing Workday inbound provisioning rule, and click the entry to open the details panel.
4. Click the **Configuration** tab.
5. Click the **Attribute mapping** button, and then click the pencil icon.
6. Review the default mapped attributes and add any additional attributes.
7. Identify any attributes for write-back provisioning, and then click the directional arrow to toggle between inbound and bi-directional. The arrow changes to a double blue arrow to indicate bi-directional (write-back) provisioning.



> **Note**
>
> - Ensure that you have enabled write-back for all attributes in the same attribute grouping. For more information, see Workday attribute mapping.
> - Not all attributes support write-back. For attributes that do not support write-back, you will see the message `This attribute does not support write-back`.

8. Click **Save**.

Next steps

Viewing sync status

Identifying your Workday hostname

You'll need the Workday hostname to configure the Workday provisioning connection. You can find it in the WSDL file in your Workday tenant.

Copyright © 2025 Ping Identity Corporation

Steps

1. Start the Workday application.
2. In the Search bar, enter `Public Web Services` and click the report.
3. In the resulting screen, click the **...** button, point to **Web Service** and click **View WSDL** in the message.
4. In the WSDL file, locate `soapbind:address`.
5. Copy the hostname from the location element and paste it to a secure location.

> **Note**
>
> When setting up the provisioning connection, you'll use the hostname, including subdomain, for your Workday tenant. For example, `<your_subdomain>.workday.com`.

Creating a Workday Integration System User

For Workday provisioning, PingOne requires an Integration System User in Workday with a minimally scoped set of permissions. PingOne uses this user account to consume data from Workday through the Workday APIs.

Before you begin

You might already have a suitable Integration System User. If not, use the following procedure to add one.

About this task

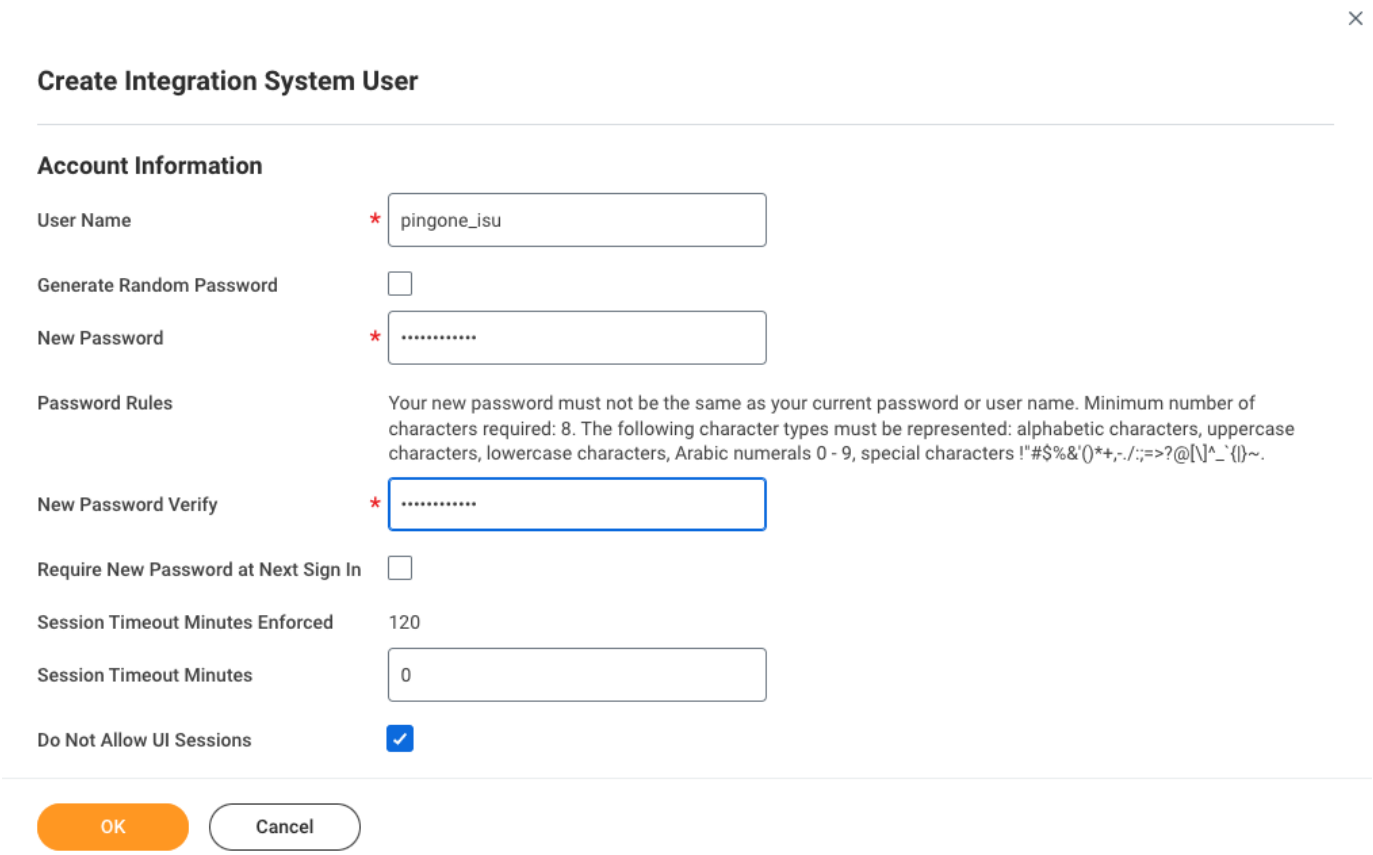
The Integration System User must be part of an Unconstrained Integration System Security Group with a series of `Get Only` Domain Security Policies granted to it to access the appropriate worker data. These domains relate to worker data about their employment status, home and work contact information, and organizations to which they belong.

Steps

1. Go to your Workday tenant and enter `create integration system user` in the search field.
2. Under **Tasks & Reports**, click **Create Integration System User**.
3. Enter a username and password for the new user.
4. Leave the **Require New Password at Next Sign In** option clear.
5. For **Session Timeout Minutes**, enter `0`. This option helps avoid any issues with PingOne related to timeouts.
6. Select **Do Not Allow UI Sessions** to prevent this user from signing into Workday.

Copyright © 2025 Ping Identity Corporation

7. Click **OK**.



Next steps

Adding the Integration System User to a Security Group

Adding the Integration System User to a Security Group

To ensure that the Integration System User can access the appropriate worker data, add it to an Unconstrained Integration System Security Group.

Before you begin

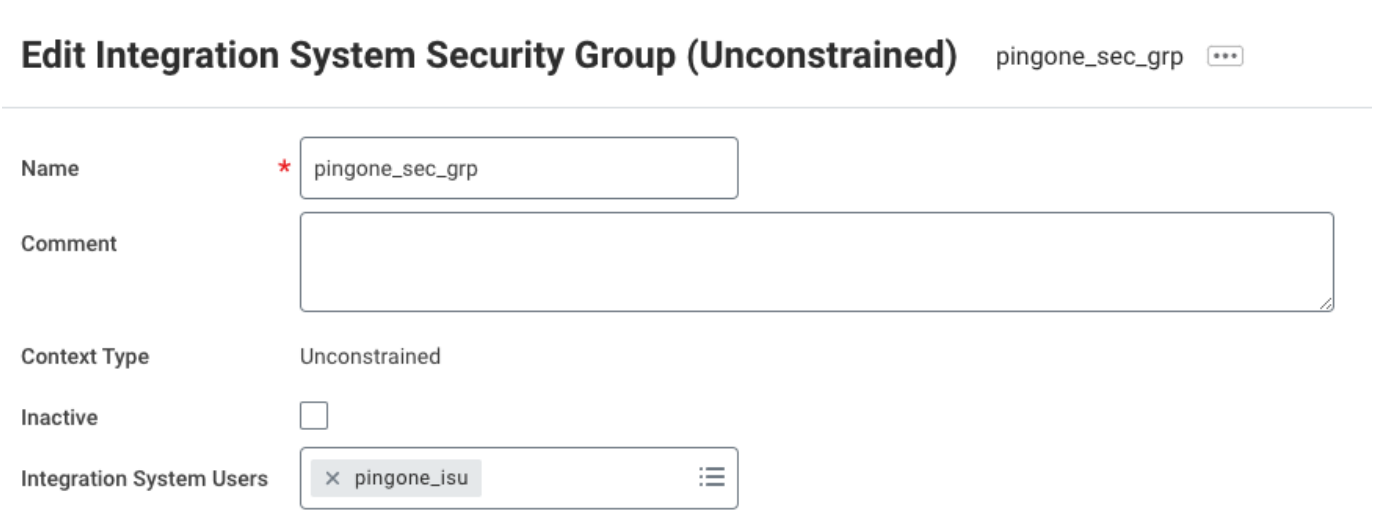
You might already have a suitable Security Group. If not, use the following procedure to add one.

Steps

1. Go to your Workday tenant and enter `create security group` in the search field.
2. Under **Tasks & Reports**, click **Create Security Group**.
3. For **Type of Tenanted Security Group**, select **Integration System Security Group (Unconstrained)**.
4. Enter a name for the security group.
5. Click **OK**.

Copyright © 2025 Ping Identity Corporation

6. On the **Edit Integration Security Group (Unconstrained)** screen, add the appropriate user to the group under **Integration System Users**. You can search or browse for the appropriate user.
7. Click **OK**.



Next steps

Configuring the Domain Security Policy Permissions for the Security Group

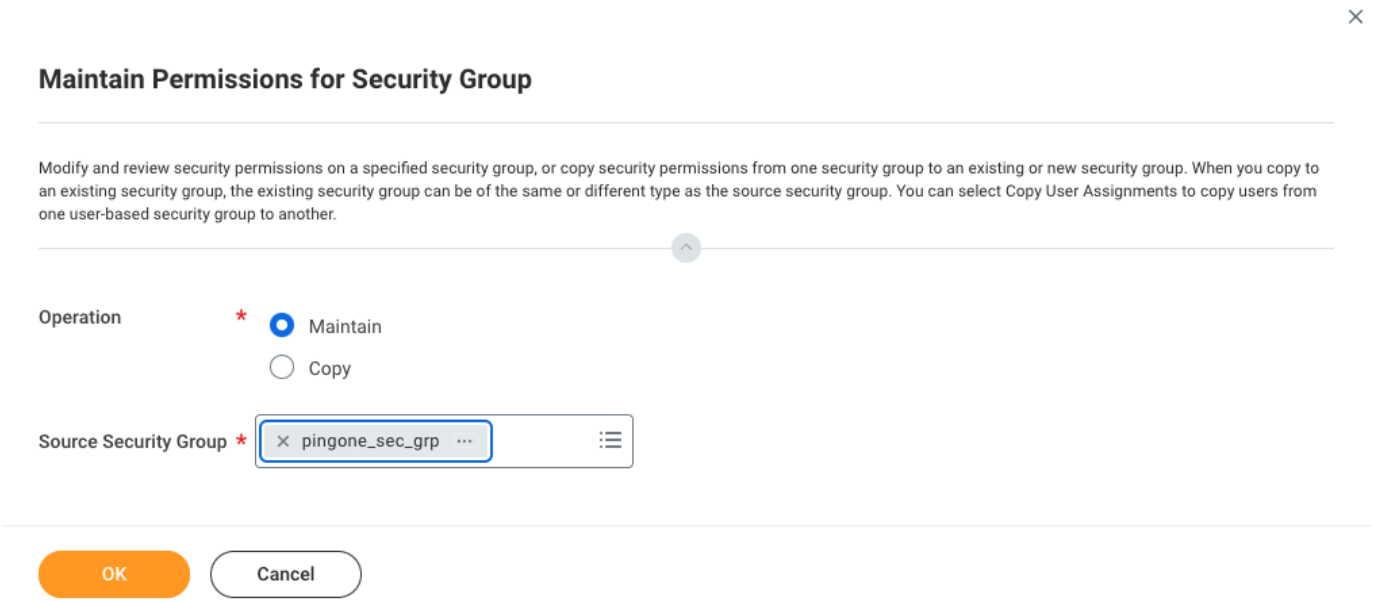
Configuring the Domain Security Policy Permissions for the Security Group

Edit the security group to ensure that it has the appropriate permissions.

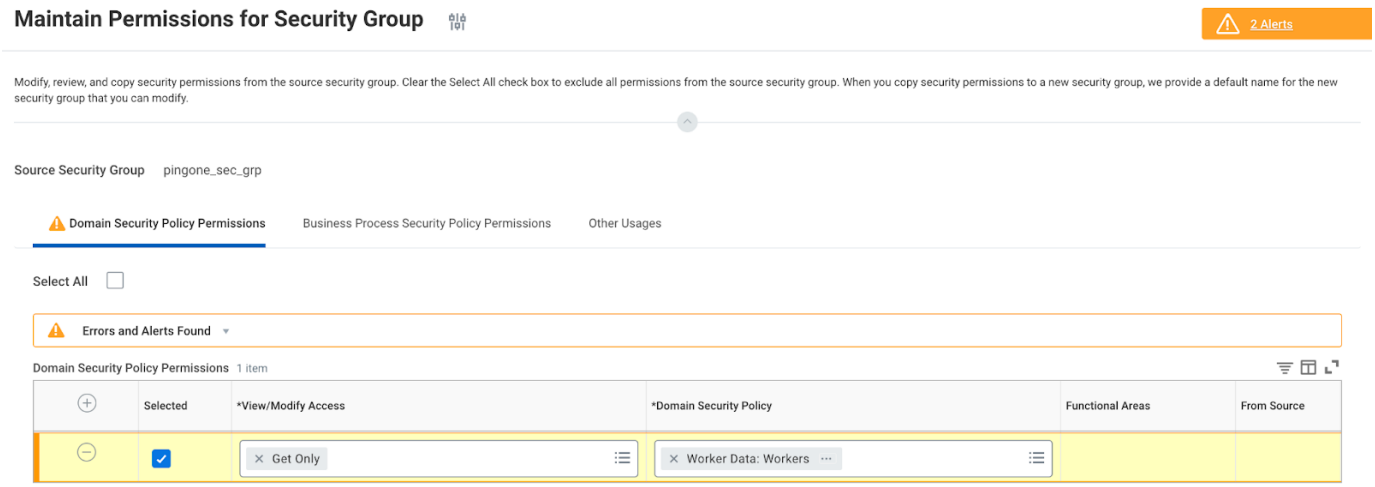
Steps

1. Go to your Workday tenant and enter `maintain permissions for the security group` in the search field.
2. Under **Tasks & Reports**, click **Maintain Permissions for Security Group**.
3. For **Operation**, click **Maintain**.
4. For **Source Security Group**, enter the name of the security group you created earlier.
5. Click **OK**.

Copyright © 2025 Ping Identity Corporation



6. On the next screen, under **Domain Security Policy Permissions**, add a separate row for each required Domain Security Policy. To add a new row click the **+** icon, enter the correct access level (`Get Only` in all cases) and the Domain Security Policy. Add the Domain Security Policy according to the following table.



Domain	Domain Security Policy
Get Only	Worker Data: Employment Data
Get Only	Person Data: Public Home Email Address Integration
Get Only	Person Data: Public Work Address Integration
Get Only	Worker Data: Organization Information
Get Only	Person Data: Public Work Email Address Integration

Copyright © 2025 Ping Identity Corporation

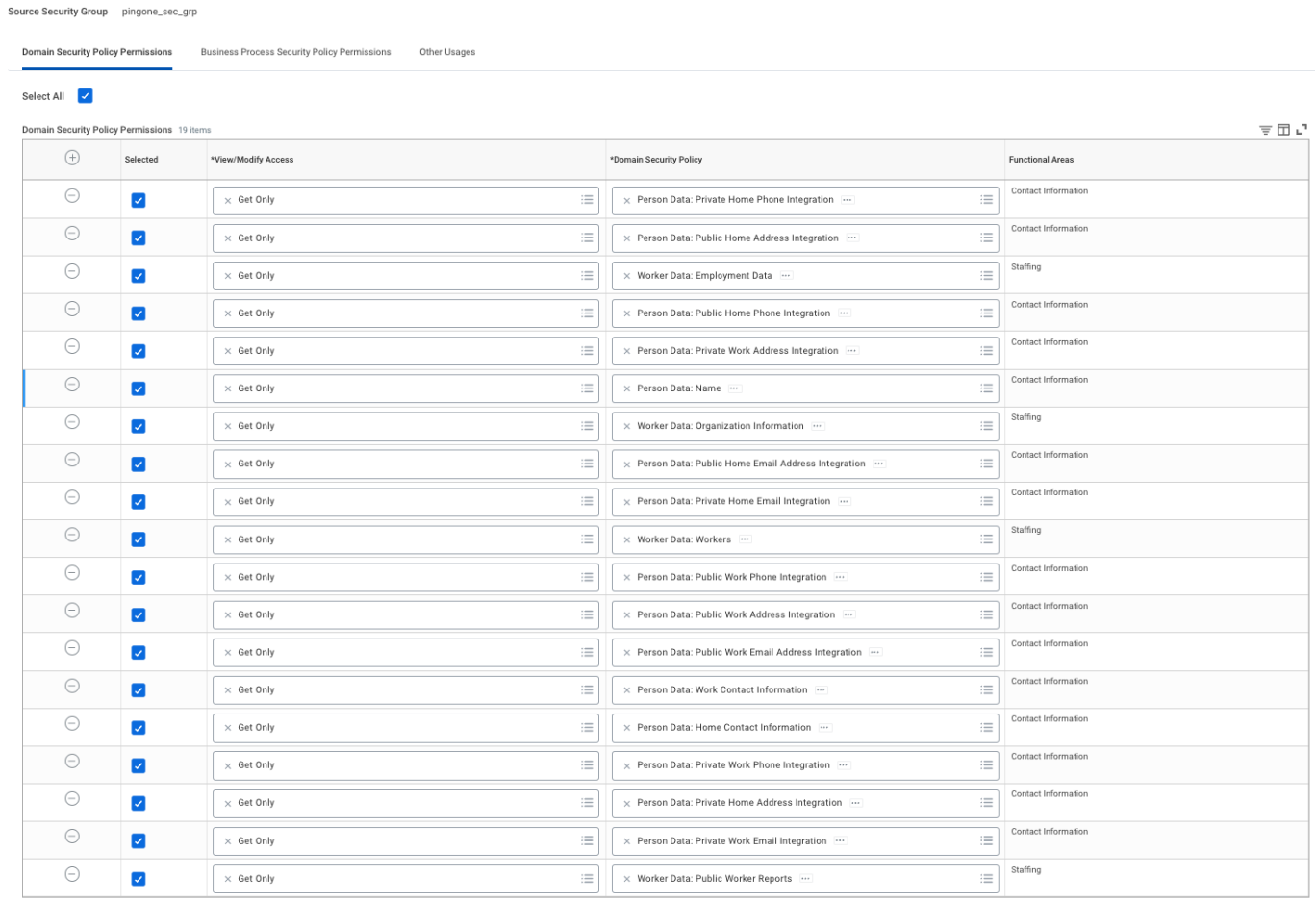
Domain	Domain Security Policy
Get Only	Person Data: Private Work Address Integration
Get Only	Worker Data: Workers
Get Only	Person Data: Private Work Phone Integration
Get Only	Person Data: Private Home Address Integration
Get Only	Person Data: Public Home Address Integration
Get Only	Person Data: Name
Get Only	Person Data: Work Contact Information
Get Only	Person Data: Public Home Phone Integration
Get Only	Person Data: Public Work Phone Integration
Get Only	Person Data: Home Contact Information
Get Only	Person Data: Private Work Email Integration
Get Only	Person Data: Private Home Phone Integration
Get Only	Person Data: Private Home Email Integration
Get Only	Worker Data: Public Worker Reports

7. Click **OK**.

8. Review that the permissions for the security group contain all the necessary Domain Security Policy options.

Copyright © 2025 Ping Identity Corporation

9. Click **Done**.



Next steps

Activating the Security Policy Changes

Configuring Business Process Security Policy permissions for write-back

For write-back, you must edit the security group to ensure that it has the appropriate permissions.

Steps

1. Go to your Workday tenant and enter `edit business process security policy` in the search field.
2. Under **Contact information**, click **Change legal name**.
3. Locate the **Web service** section and add the security group you created earlier.
4. Repeat this process for:
    - **Change Home Contact Information**
    - **Change Work Contact Information**
5. Click **OK**.

Copyright © 2025 Ping Identity Corporation

Next steps

Activating the Security Policy Changes

Activating the Security Policy Changes

After you have reviewed the permissions for the group, activate the security policy changes. If you don't activate the security policy changes, the Integration System User will not have the necessary permissions and PingOne will not be able to sync users from Workday.

Steps

1. Go to your Workday tenant and enter `activate pending security policy changes` in the search field.
2. Under **Tasks & Reports**, click **Activate Pending Security Policy Changes**.
3. Add a comment to describe the security changes and then click **OK**.
4. Review the pending security policy changes, then select the **Confirm** checkbox.
5. Click **OK**.

Next steps

After you have created the Integration System User, added the Integration System User to a security group, configured the Domain Security Policy Permissions for the group, and activated the Security Policy changes, you can create the Workday provisioning connection. See Creating a Workday connection.

Workday attribute mapping

The following table lists the default Workday attributes that can be mapped to PingOne user attributes for user provisioning.

Attribute	Description
Work email	The user's email address.
Username	The user's username and Workday login.
Active	The status of the user account in Workday.
First Name	The user's first (given) name.
Middle Name	The user's middle name.
Last Name	The user's last (family) name.

For inbound provisioning from Workday, LDAP Gateway, and SCIM identity stores, you can specify some additional options for onboarding new users. For more information, see Adding attribute mapping for inbound provisioning.

Copyright © 2025 Ping Identity Corporation

Attribute dependencies

When mapping attributes for write-back, some attributes are dependent on other attributes. For example, to configure a `Name` attribute, you must also include `First Name`, `Middle Name`, `Last Name`, and `Name Locale`.

The following table shows the dependent attribute groupings. That is, if you map one attribute in a group for write-back, you need to map them all.

Name grouping	First Name Last Name Middle Name Name Locale
Home address grouping	Home Street Address Line One Home Street Address Line Two Home Postal Code Home City Home Region Home Country
Home phone grouping	Home Phone Home Phone Country Home Phone Type
Work address grouping	Work Street Address Line One Work Street Address Line Two Work Postal Code Work City Work Region Work Country
Work phone grouping	Work Phone Work Phone Country Work Phone Type

These attributes can be mapped independently of one another.

- WID
- Work Email
- Home Email

Creating a Workday Integration System with a Field Override Service

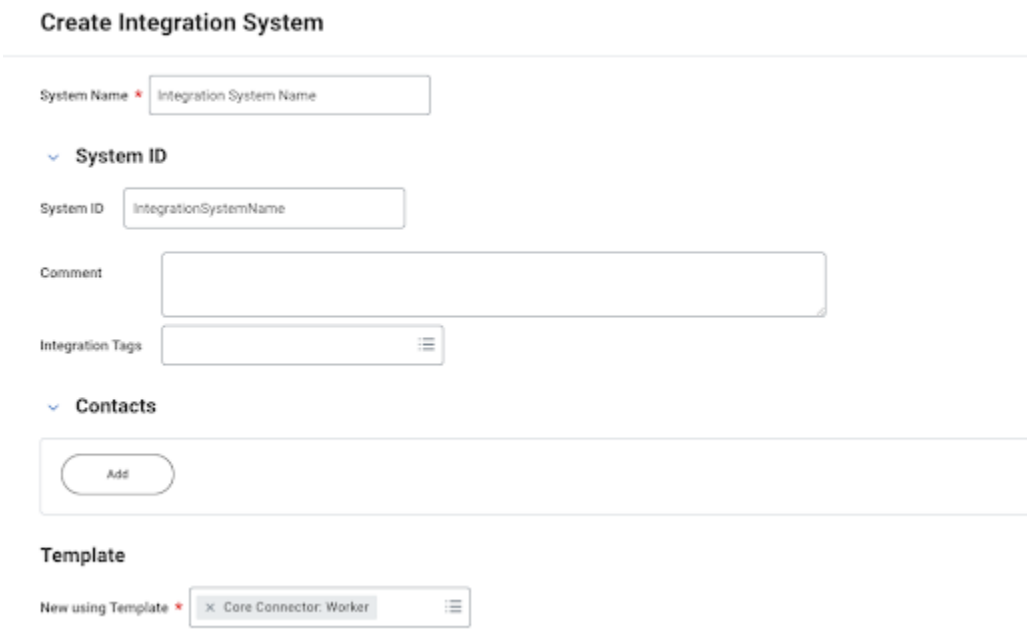
You can use Workday's Field Override Service to create and sync Workday custom attributes into PingOne. The Field Override Service simplifies and improves performance over custom reports.

To create a Field Override Integration System in Workday and add custom attributes to sync into PingOne as part of user onboarding:

Copyright © 2025 Ping Identity Corporation

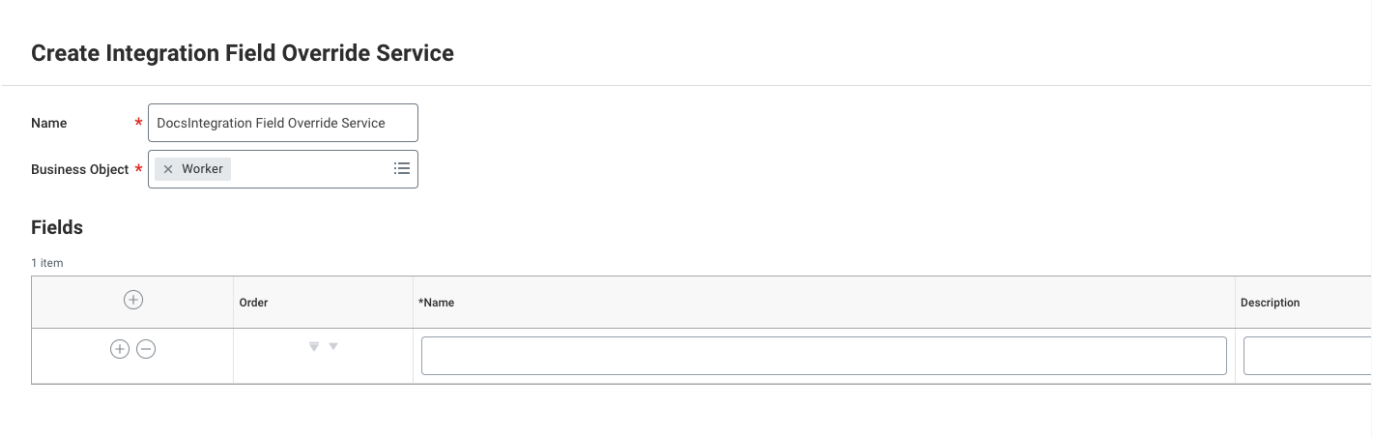
Steps

1. Sign on to your Workday account.
2. In the search bar, enter `Integration System`, and click **Create Integration System**.
3. Enter the following:
    - **System Name**: A name for your Integration System.
    - **Comment** (Optional): Add a comment.
    - **Template**: In the **New using template** list, select **Core Connector: Worker**.



4. Click **OK**.
5. On the **Configure Integration Services** page, in the **Custom Integration Services** section, click **+**.
6. Click **Create**.
7. In the list of services, select **Create Integration Field Override Service**.
8. Enter a name for the Field Override Service.
9. Select **Worker as the Business Object**.

Copyright © 2025 Ping Identity Corporation



10. To add fields:
    1. Enter a **Name**.
    2. (Optional) Enter a **Description**.
    3. To add more fields, click **+**.
11. Click **OK**.

    Result:

    Your integration system is created.
12. Click **OK** to return to the **View Integration System** page.
13. To configure the field mappings for your system:
    1. Click the **...** icon.
    2. Go to **Actions** > **Integration System** > **Configure Integration Field Overrides**.
    3. In the **Integration Service** list, select your system, and then click it to open the field mappings.
    4. Configure the mappings for your fields.
    5. Click **OK**.
14. Click **Done**.

> **Important**
>
> All custom properties are treated as strings.

Next steps

Add the integration System IDs from Worday to PingOne. Learn more in Adding Integration System IDs from Workday into PingOne.

Sync custom attributes from Workday to PingOne. Learn more in Syncing custom attributes from Workday into PingOne.

Copyright © 2025 Ping Identity Corporation

Adding Workday Integration System IDs to PingOne

To set up and update your provisioning settings and be able to sync custom attributes into PingOne, you need the Integration System IDs from Workday.

Before you begin

- Make sure you have an Integration System created in Workday with a Field Override Service to populate and map custom Workday attributes. Learn more in Creating a Workday Integration System with a Field Override Service.
- Make sure you have an Integration System user with permission to make the GET call on the custom attributes from Workday. Learn more in Adding the Integration System User to a Security Group and Configuring the Domain Security Policy Permissions for the Security Group.

Steps

1. Sign on to your Workday account.
2. In the search bar, enter `View your Integration System`.
3. In the list, select your Integration System.
4. Click **OK**.
5. Expand **System IDs**.
6. Copy the system IDs that you want to add to PingOne.
7. In PingOne, go to **Integrations** > **Provisioning**.
8. Click your applicable connection.
9. On the **Configurations** tab, click the **Pencil** icon.
10. In the **Configure Preferences** section, enter the **Integration System IDs** needed for syncing custom attributes from your Workday Integration System.

    > **Note**
    > The **Integration System IDs** field supports multiple system IDs, separated by commas.

11. Click **Save**.

Next steps

Sync your custom Workday attributes into PingOne. Learn more in Syncing custom attributes from Workday into PingOne

Syncing custom attributes from Workday into PingOne

Sync custom attributes from Workday into PingOne.

Before you begin

- Make sure you have an Integration System created in Workday with a Field Override Service to populate and map custom Workday attributes. Learn more in Creating a Workday Integration System with a Field Override Service.

Copyright © 2025 Ping Identity Corporation

- Make sure you added the Integration System IDs to your connection. Learn more in Adding Workday Integration System IDs to PingOne.
- Make sure you have an Integration System user with permission to make the GET call on the custom attributes from Workday. Learn more in Adding the Integration System User to a Security Group and Configuring the Domain Security Policy Permissions for the Security Group.
- Make sure you copy the custom attribute from Workday.

Steps

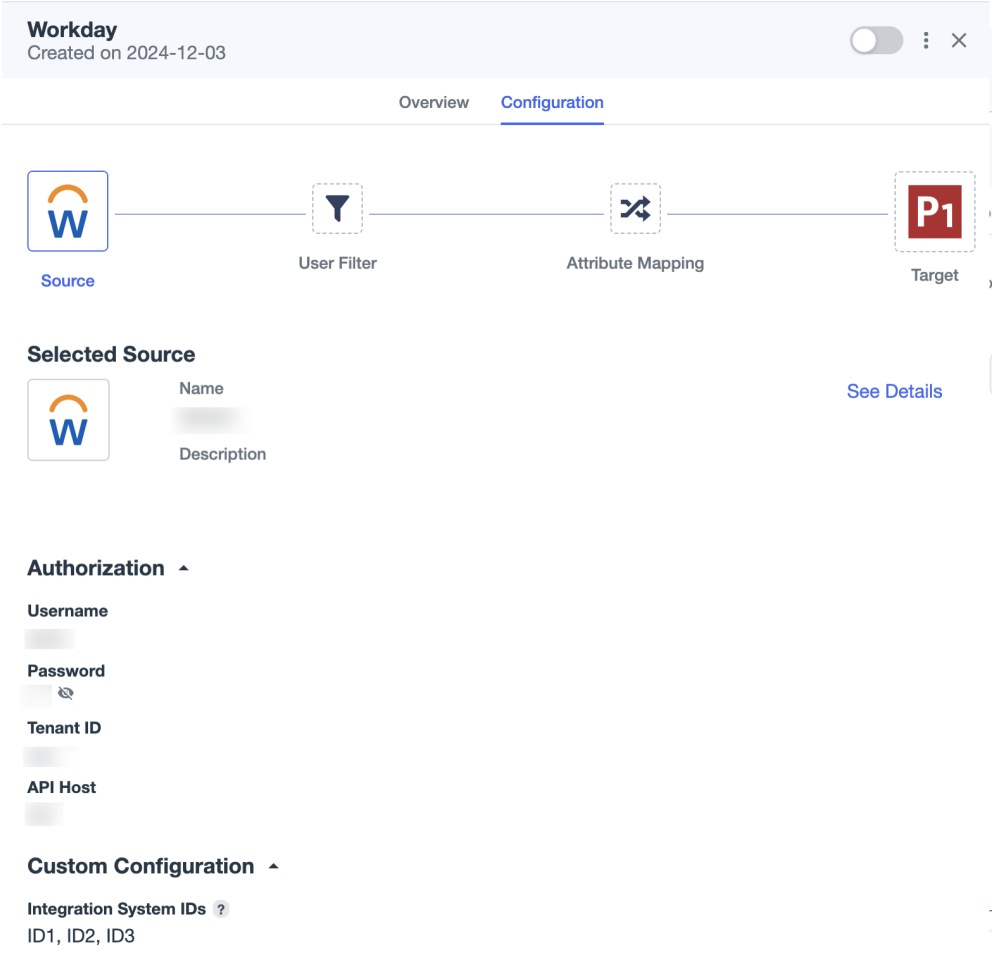
1. In the PingOne admin console, go to **Integrations** > **Provisioning**.
2. On the **Rules** tab, click the appropriate rule.

   Result:

   The details panel opens.

3. Click the **Configuration** tab.

> **Note**
>
> You should see the Integration System IDs you added when creating or editing a connection.



4. Click **Attribute Mapping**.
5. Click the **Pencil** icon to edit the attribute mapping.
6. Click **+ Add**.
7. Paste the custom attribute you copied from Workday.

> **Note**
>
> If the custom attribute has a value populated, the value appears with "ADD:" in front of the custom attribute name.

8. Map the added custom attribute you added to the target attribute.
9. Click **Save**.

Workday provisioner known limitations

The following are known limitations with Workday user provisioning.

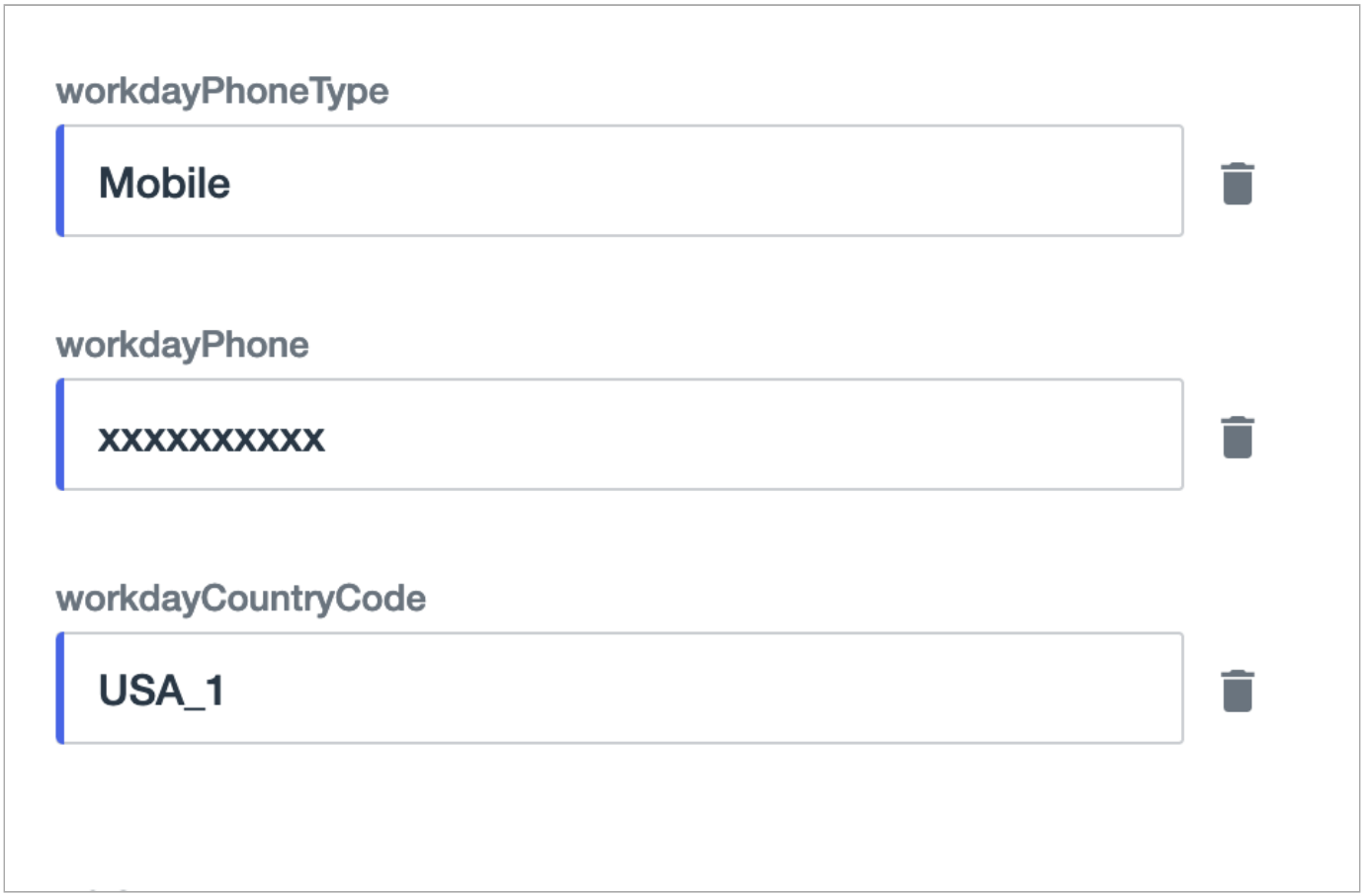
The PingOne Workday provisioner does not support the following Workday integration options:

- Contingent workers. Contingent or temporary worker user types are not supported by the PingOne provisioning Workday integration at this time. Only full time employee user types can be imported.
- Dynamic attributes. The PingOne provisioning Workday integration does not support dynamic attributes at this time.

Workday write-back provisioning has the following limitations:

- For write-back, you cannot create or delete users, you can update existing users only.
- Phone number country codes use an internal Workday format, so any modifications to the country code field require codes in that format.
- If there is a pending business process associated with any of the attributes configured for write-back, then write-back will fail. For example, if an admin updates a name attribute, Workday starts a business process in which another admin must approve that name change. If a write-back occurs while the name change is pending, then the write-back will fail.
- The `Country` attribute for addresses must be mapped to a custom attribute because Workday uses a different data format than PingOne. Use the three-letter country code (ISO 3166-1), followed by an underscore, and then the country calling code (international subscriber dialing code) for that country. The following example shows the Workday country code format for Canada.

Copyright © 2025 Ping Identity Corporation



- For custom attributes, you must have an Integration System user with permission to make the GET call on the custom attributes from Workday. For example, the attribute names `Hire_Date` and `Original_Hire_Date` require the permission `Worker Data: Current Staffing Information`. Learn more in Adding the Integration System User to a Security Group and Configuring the Domain Security Policy Permissions for the Security Group.

Creating a Microsoft Azure Office 365 connection

Use a Microsoft Azure Office 365 connection to enable provisioning from PingOne to the Microsoft Azure identity platform.

Before you begin

You should review the information about registering applications with the Microsoft identity platform. Learn more in Register an application with the Microsoft identity platform in the Microsoft documentation.

Make sure that you have:

- An Azure account that has an active subscription. Learn more in Microsoft's Create your Azure Free account.
- The tenant domain ID for the Azure account. You can find the tenant domain in the Azure portal. Go to the application properties and select **View endpoints**. Copy the ID from the URL under **Microsoft Azure AD Graph API Endpoint**.
- The client ID and client secret for the connected application. You can find the client ID and client secret in the Azure portal. Learn more in Register an application with the Microsoft identity platform in the Microsoft documentation.

Copyright © 2025 Ping Identity Corporation

- The following application permissions in your application:
  - `Application.ReadWrite.All`
  - `Group.ReadWrite.All`
  - `Organization.Read.All`
  - `User.ReadWrite.All`

  Learn more in Add permissions to access web APIs.

Steps

1. In PingOne, go to **Integrations → Provisioning**.
2. Click **+**, and then click **New connection**.
3. On the **Identity Store** line, click **Select**.
4. Click **Microsoft Azure (Microsoft 365)**, click **Select**, and then click **Next**.
5. Enter a name and description for the provisioning connection.

   Result:

   The connection name appears in the provisioning list after you save the connection.
6. Click **Next**.
7. On the **Configure authentication** panel, enter the values for the following fields:

Field	Value
Tenant domain ID	The tenant domain ID for the Azure account. You can find the tenant domain in the Azure portal. Learn more in Local tenant ID and primary domain.
Client ID	The client ID from Azure for the connected application. You can find the client ID and client secret in the Azure portal.
Client secret	The client secret from Azure for the connected application. You can find the client ID and client secret in the Azure portal.

8. Click **Test connection** to verify that PingOne can establish a connection to Azure.

   Result:

   If there are any issues with the connection, a **Test Connection Failed** dialog box opens. Click **Continue** to resume the setup with an invalid connection.

   > **Important**
   >
   > You cannot use the connection for provisioning until you have established a valid connection to Azure. To retry, click **Cancel** in the **Test Connection Failed** dialog box and repeat step 7.

Copyright © 2025 Ping Identity Corporation

Troubleshooting:

Learn more about troubleshooting your connection in Troubleshooting Test Connections Failure.

9. On the **Configure Preferences** pane, configure the following:

Option	Description
Remove Licenses when SKU ID is empty	Determines whether to remove a user's license from their account if you do not configure the **skuId** field in the rule's attribute mappings, or if the user's **skuId** field is cleared in the external identity store. ◦ **True**: When enabled, if you choose to not configure the **skuId** field in the rule's attribute mapping, the user's licenses will be removed from their account. ◦ **False** (default): When disabled, if you choose to not configure the **skuId** field in the rule's attribute mapping, the user's licenses will not be removed from their account. However, if you configure the **skuId** field in the rule's attribute mapping, and if the user's **skuId** field is cleared in the directory, the user's licenses will be removed from their account.
Allow users to be created	Determines whether to create a user in the Azure identity store when the user is created in the PingOne identity store.
Allow users to be updated	Determines whether to update user attributes in the Azure identity store when the user is updated in the PingOne identity store.
Allow users to be disabled	Determines whether to disable a user in the Azure identity store when the user is disabled in the PingOne identity store.
Allow users to be deprovisioned	Determines whether to deprovision a user in the Azure identity store when the user is deprovisioned in the PingOne identity store.
Remove action	Determines the action to take when removing a user from the Azure identity store. ◦ **Delete**: When a user is deprovisioned from the PingOne identity store, PingOne removes the user from the external identity store. ◦ **Disable**: When a user is deprovisioned from the PingOne identity store, PingOne disables the user in the external identity store.

Copyright © 2025 Ping Identity Corporation

Option	Description
Deprovision on rule deletion	Determines whether to deprovision users that were provisioned using this rule if the rule is deleted.

10. Click **Finish**.

Result

The Azure Office 365 provisioning connection is complete and is added to the list of provisioning connections on the **Provisioning** page.

> **Note**
> When you create the provisioning rule, make sure that you map a value for the `Password` attribute. You must map a value for `Password` before you can enable the rule. Learn more in Adding attribute mapping for outbound provisioning.

Next steps

To sync group members out of PingOne into a software as a service (SaaS) application, follow the instructions in Configuring outbound group provisioning.

Microsoft Azure Office 365 attribute mapping

The following table lists common Microsoft Azure Office 365 attributes that can be mapped for user provisioning.

Attribute	Description
password	A value for the user's initial password. The field can also be set to a static default value. This field is required when a user is created. It can not be updated, but you can force the user to update their password on their next sign on by setting `resetPassword` to `true`. **Note** The password must satisfy the minimum requirements of the user's password policy. We recommend using a strong password.
mailNickname	The mail alias for the user.
resetPassword	Determines whether a user must reset their password the next time they sign on. The default value is `true`, but it can be mapped to an attribute.
userPrincipalName	The user principal name (UPN) of the user. The UPN is an Internet-style login name for the user based on the Internet standard RFC 822.
immutableid	Associates a user ID with a user account in the Microsoft Azure identity store.
displayName	The name as it will look in the PingOne identity store.

Copyright © 2025 Ping Identity Corporation

Attribute	Description
accountEnabled	Determines whether a user account is enabled. The default value is `Enabled`.
surname	The last (family) name of the user.
givenName	The first name of the user.
usageLocation	Determines the location of license usage, which is required for licensing. Map to an attribute that contains the ISO-3166 formatted country (2-letter country code) of license usage. Required for users that will be assigned licenses due to a legal requirement to check the availability of services in various countries. Examples include: `US`, `JP`, and `GB`.

Creating a Zoom connection

Use a Zoom connection to enable provisioning from PingOne to the Zoom user directory.

Before you begin

We recommend that you review the Zoom documentation, including:

- Accessing SAML Response Logs
- SCIM2 API
- SCIM2 API User attributes

Make sure that you have:

- A Zoom system administrator account.
- The Account ID, Client ID, and Client secret for a Server-to-Server OAuth application. For more information, see Creating an application in Zoom.

> **Note**
>
> Zoom has deprecated the JWT app type. You should create new apps of Server-to-Server OAuth type. For more information, see the JWT App Type Deprecation FAQ in the Zoom documentation.

Steps

1. Go to **Integrations → Provisioning**.
2. Click the **+** icon and then click **New Connection**.
3. For **Identity Store**, click the **Select** button.
4. Under **Zoom**, click **Select** and then click **Next**.
5. Enter a name and description for this provisioning connection. The connection name will appear in the list when you've completed and saved the connection.
6. Click **Next**.

Copyright © 2025 Ping Identity Corporation

7. On the **Configure authentication** screen, enter the following information. For information about finding these values, see Creating an application in Zoom.
    - **SCIM URL**. The fully qualified URL for the SCIM resource, such as `https://api.zoom.us/scim2`.
    - **Authentication Method**. Select the available authentication method: **OAuth Bearer Token** for Server-to-Server OAuth applications. The configuration fields will change appropriately.
    - **OAuth Token URL** (OAuth only). The fully qualified URL for the token resource, such as `https://zoom.us/oauth/token`.
    - **OAuth Account ID** (OAuth only). The account ID to identify the connected Server-to-Server OAuth application in Zoom.
    - **OAuth Client ID** (OAuth only). The client ID to identify the connected Server-to-Server OAuth application in Zoom.
    - **OAuth Client Secret** (OAuth only). The credentials for the connected Server-to-Server OAuth application in Zoom.
8. Click **Test connection** to verify that PingOne can establish a connection to Zoom.

    Result:

    If there are any issues with the connection, a **Test Connection Failed** dialog box opens. Click **Continue** to resume the setup with an invalid connection.

    > **Important**
    >
    > You cannot use the connection for provisioning until you have established a valid connection to Zoom. To retry, click **Cancel** in the **Test Connection Failed** dialog box and repeat step 7.

    Troubleshooting:

    Learn more about troubleshooting your connection in Troubleshooting Test Connections Failure.
9. On the **Actions** screen, enter the following:
    - **Allow users to be created**. Determines whether to create a user in the Zoom user directory when the user is created in the PingOne identity store.
    - **Allow users to be updated**. Determines whether to update user attributes in the Zoom user directory when the user is updated in the PingOne identity store.
        - **Allow users to be disabled**. When a user is disabled in the PingOne identity store, PingOne disables the user in the external identity store.
    - **Allow users to be deprovisioned**. Determines whether to deprovision a user in the Zoom user directory when the user is deprovisioned in the PingOne identity store.
    - **Remove action**. Determines the action to take when removing a user from the Zoom user directory.
        - **Disable**. When a user is deprovisioned from the PingOne identity store, PingOne disables the user in the external identity store.
        - **Delete**. When a user is deprovisioned from the PingOne identity store, PingOne deletes the user in the external identity store.

Copyright © 2025 Ping Identity Corporation

- **Deprovision on rule deletion**. Determines whether to deprovision users that were provisioned using this rule if the rule is deleted.

10. Click **Finish**.

Next steps

To define which users are provisioned and how attributes are mapped between PingOne and an external identity store, follow the instructions in Creating an outbound rule.

Zoom provisioning features

Provision users from the PingOne identity store to a Zoom identity store.

The provisioner offers the following features:

- Manages users in Zoom based on changes in an external data store that is attached to PingOne.
- Creates, updates, and disables or deletes users.
- Enable the create, update, and disable or delete capabilities independently.
- Choose to disable or delete users when deprovisioning.

Creating an application in Zoom

Use the Zoom App Marketplace to create a connected application of Server-to-Server OAuth type. You'll copy the Account ID, Client ID, and Client secret, and enter them into PingOne to create a Zoom connection.

Steps

1. Sign on to the Zoom App Marketplace as an administrator.
2. On the navigation bar, click **Develop**, and then click **Build App**.

   > **Note**
   >
   > Zoom has deprecated the JWT app type. You should create new apps of Server-to-Server OAuth type. For more information, see the JWT App Type Deprecation FAQ in the Zoom documentation.

3. On the **Choose your app type** page, in the **Server-to-Server OAuth** tile, click **Create**.
4. On the **Create a Server-to-Server OAuth** page, in the **App Name** field, enter a name and click **Create**.

   Result:

   The **Account ID**, **Client ID**, and **Client Secret** for your new application are shown on the **App credentials** tab. Remember where this information is stored, because you'll need it to create a provisioning connection.

5. On the **Information** tab, add information about your app, such as a meaningful short description that will help others understand its purpose.
6. Scroll down and enter the company name, which is required to activate your app.

Copyright © 2025 Ping Identity Corporation

7. Scroll down to the **Developer Contact Information** section of the page, enter your name and email address in the appropriate fields. Click **Continue**.
8. On the **Feature** tab, enable the features you're interested in, such as events, team chats, and multi-platform support. Click **Continue**.
9. On the **Scopes** tab, click **+ Add Scopes**. On the **Add scopes** page, add the following scopes:
    - User scopes
        - **View and manage sub account's user information** (user:master)
        - **View all user information** (user:read:admin)
        - **View users information and manage users** (user:write:admin)
    - Account scopes
        - **View and manage sub accounts** (account:master)
        - **View account info** (account:read:admin)
        - **View and manage account info** (account:write:admin)
    - SCIM2 scopes
        - **Call Zoom SCIM2 API** (scim2)
10. Click **Done**, and then click **Continue**.
11. On the **Activation** page, click **Activate your app**.

Zoom attribute mapping

The following table lists common Zoom user attributes that can be mapped to PingOne user attributes for user provisioning.

Attribute	Description
Username	The user's unique username and Zoom login.
Given Name	The user's first name.
Family Name	The user's last name.
Email	The user's email address.
Phone	The phone number for the user, formatted as `+1 5125550123`.
Active	The status of the user account in Zoom.
User Type	The type of account for the user, such as `Basic`, `Pro`, or `Corp`.
Roles	Roles held by the user, such as `Student` or `Engineer`.

Copyright © 2025 Ping Identity Corporation

Attribute	Description
Title	The user's title, such as `Manager` or `CEO`.
Department	The user's department or work group, such as `Marketing`.
Organization	The user's organization, typically a company or school.
Locale	The user's default location for purposes of localizing things like currency, date and time format, or numerical representations.

Creating a Slack connection

Use a Slack connection to enable provisioning from PingOne to the Slack user directory.

Before you begin

Make sure that you have:

- A Slack Workspace Owner account. For more information, see Types of roles in Slack.
- The OAuth2 Access Token for the connected application. You can use the Ping Identity OAuth Configuration Service (OCS) to get the token. For more information, see Getting a Slack API access token.

You should review the provisioning information in the Slack documentation. For more infomration, see Manage members with SCIM Provisioning.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **+** and then click **New connection**.
3. On the **Identity Store** line, click **Select**.
4. Click **Slack**, click **Select**, and then click **Next**.
5. Enter a name and description for this provisioning connection.

   The connection name appears in the provisioning list after you save the connection.
6. Click **Next**.
7. On the **Configure authentication** panel, in the **OAuth2 Access Token** field, enter the access token from Slack for the connected application.

   You can use the Ping Identity OAuth Configuration Service (OCS) to get the token. For more information, see Getting a Slack API access token.
8. Click **Test connection** to verify that PingOne can establish a connection to Slack.

   Result:

Copyright © 2025 Ping Identity Corporation

If there are any issues with the connection, a **Test Connection Failed** dialog box opens. Click **Continue** to resume the setup with an invalid connection.

> **Important**
> You cannot use the connection for provisioning until you have established a valid connection to Slack. To retry, click **Cancel** in the **Test Connection Failed** dialog box and repeat step 7.

Troubleshooting:

Learn more about troubleshooting your connection in Troubleshooting Test Connections Failure.

9. In the **Configure Preferences** and **Actions** sections, enter the following:

Field	Description
Unique user identifier	Determines how to identify a unique user. Select `primaryEmail` or `userName`.
Group membership handling	Determines whether to update or replace target groups with PingOne memberships. Select **Merge** or **Overwrite**. **Note** Merging or overwriting memberships only applies to SCIM, Slack, and GitHub EMU provisioning connections.
Allow users to be created	Determines whether to create a user in the Slack user directory when the user is created in the PingOne identity store.
Allow users to be updated	Determines whether to update user attributes in the Slack user directory when the user is updated in the PingOne identity store.
Allow users to be deprovisioned	Determines whether to deprovision a user in the Slack user directory when the user is deprovisioned in the PingOne identity store.
Remove action	Determines the action to take when removing a user from the Slack user directory. ◦ **Disable**. When a user is deprovisioned from the PingOne identity store, PingOne disables the user in the external identity store.
Deprovision on rule deletion	Determines whether to deprovision users that were provisioned using this rule if the rule is deleted.

10. Click **Save**.

Next steps

Copyright © 2025 Ping Identity Corporation

To sync group members out of PingOne into a software as a service (SaaS) application, follow the instructions in Configuring outbound group provisioning.

Slack provisioning features

Provision users from the PingOne identity store to a Slack identity store.

The provisioner offers the following features:

- Supports all Slack plans, including Standard, Plus, and Enterprise Grid.
- Manages users in Slack based on changes in an external datastore:
  - Creates, updates, and disables users.
  - Enable the create, update, and disable capabilities independently.
  - Choose to disable users when deprovisioning.
- Supports outbound group provisioning.

Slack attribute mapping

The following table lists common Slack user attributes that can be mapped to PingOne user attributes for user provisioning.

Attribute	Description
userName	The user's username and Slack login.
displayName	The user's nickname in the PingOne identity store.
givenName	The user's first name.
familyName	The user's last name.
primaryEmail	The user's email address.
active	The status of the user account in Slack.

Slack provisioning known limitations

The following are known limitations with Slack user provisioning.

- Some user attributes in the Slack directory cannot be cleared after they are set.
- Membership sync status for a group shows success even if a disabled user is added to a group in group provisioning.

Copyright © 2025 Ping Identity Corporation

Creating a ServiceNow connection

Use a ServiceNow connection to enable provisioning from PingOne to the ServiceNow user directory.

Before you begin

Review the User administration information in the ServiceNow documentation.

Make sure that you have:

- Administrator access to a ServiceNow instance running a supported version.
- The username and password for the administrator account.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **+** and then click **New connection**.
3. For **Identity Store**, click the **Select** button.
4. Under **ServiceNow**, click **Select** and then click **Next**.
5. Enter a name and description for this provisioning connection. The connection name will appear in the list when you've completed and saved the connection.
6. Click **Next**.
7. On the Configure authentication screen, enter the following:
   - **ServiceNow URL**. The URL of your ServiceNow instance. For example, `https://yourinstance.service-now.com`.
   - **Username**. The administrator user for the ServiceNow instance.
   - **Password**. The password for the administrator user.
8. Click **Test connection** to verify that PingOne can establish a connection to ServiceNow.

   Result:

   If there are any issues with the connection, a **Test Connection Failed** dialog box opens. Click **Continue** to resume the setup with an invalid connection.

   > **Important**
   > You cannot use the connection for provisioning until you have established a valid connection to ServiceNow. To retry, click **Cancel** in the **Test Connection Failed** dialog box and repeat step 7.

   Troubleshooting:

   Learn more about troubleshooting your connection in Troubleshooting Test Connections Failure.

9. On the **Actions** screen, enter the following:
   - **Allow users to be created**. Determines whether to create a user in the ServiceNow user directory when the user is created in the PingOne identity store.

Copyright © 2025 Ping Identity Corporation

- **Allow users to be updated**. Determines whether to update user attributes in the ServiceNow user directory when the user is updated in the PingOne identity store.
  - **Allow users to be disabled**. Determines whether to disable a user in the ServiceNow user directory when the user is disabled in the PingOne identity store.
- **Allow users to be deprovisioned**. Determines whether to deprovision a user in the ServiceNow user directory when the user is deprovisioned in the PingOne identity store.
- **Remove action**. Determines the action to take when removing a user from the ServiceNow user directory.
  - **Disable**. When a user is deprovisioned from the PingOne identity store, PingOne disables the user in the external identity store.
- **Deprovision on rule deletion**. Determines whether to deprovision users that were provisioned using this rule if the rule is deleted.

10. Click **Finish**.

Next steps

To define which users are provisioned and how attributes are mapped between PingOne and an external identity store, follow the instructions in Creating an outbound rule.

ServiceNow default attributes

The following table shows the default ServiceNow user attributes that can be mapped to PingOne user attributes for user provisioning.

> **Note**
> This information shows typical attribute mappings, but you are free to map attributes however you like.

PingOne Directory attribute	Description	ServiceNow attribute
Username	The user's username and ServiceNow login. PingOne uses this value to synchronize pre-existing users in ServiceNow with PingOne.	Username
Given Name	The user's first (given) name. For example, "Barbara" in "Ms. Barbara Jane Jensen, III".	First Name
Family Name	The user's last (family) name. For example, "Jensen" in "Ms. Barbara Jane Jensen, III".	Last Name
Email Address	The user's email address.	Email
Enabled	The status of the user account in ServiceNow.	Active

Copyright © 2025 Ping Identity Corporation

ServiceNow supported attributes

The following table lists all the attributes that can be mapped for user provisioning to ServiceNow. For more information about these attributes, see Create a user in the ServiceNow documentation.

Attribute	Description
Username	The user's username and ServiceNow login. PingOne uses this value to synchronize pre-existing users in ServiceNow with PingOne.
Prefix	The user's honorific prefix, such as Ms., Mr., or Dr.. This attribute maps to introduction in ServiceNow.
FirstName	The user's first (given) name. For example, "Barbara" in "Ms. Barbara Jane Jensen, III".
MiddleName	The user's middle name. For example, "Jane" in "Ms. Barbara Jane Jensen, III".
LastName	The user's last (family) name. For example, "Jensen" in "Ms. Barbara Jane Jensen, III".
Email	The user's email address.
MobilePhone	The user's mobile phone number.
BusinessPhone	The user's business phone number.
HomePhone	The user's home phone number.
Roles	The user's role, such as Student or Faculty. This attribute supports multiple values. The ServiceNow Provisioner can assign only roles that are already assigned to the user account that you use for provisioning. The ServiceNow Provisioner does not create new roles, so the roles must already exist in ServiceNow.
Title	The user's business title, such as Software engineer.
Active	The status of the user account in ServiceNow.
LockedOut	If true, the user is locked out. The user account still exists in ServiceNow, but the user cannot sign on.
Password	The user's password. Passwords cannot be mapped from a source data store, so this field can be used to set a literal default value.
PasswordNeedsReset	If true, the user must change their password at the next sign-on.
EmployeeNumber	A string identifier, typically numeric or alphanumeric, assigned to a person, often based on order of hire or association with an organization.

Copyright © 2025 Ping Identity Corporation

Attribute	Description
Gender	The user's gender.
Manager	The Username that represents the manager for the user.
Department	The user's department or work group, such as "Sales".
Street	The user's street address.
City	The user's city or locale.
Zip	The user's ZIP code or postal code.
State	The user's state, province, or territory.
CountryCode	The user's country. Uses the two-character country code as defined by the ISO-3166-1 alpha-2 standard.
Location	The user's geographical location.
Timezone	The user's time zone. Uses the IANA time zone database format. For example, `America/Los_Angeles`. The ServiceNow provisioner can set only time zones that are already assigned to the user account that you use for provisioning. You might need to update the time zones in ServiceNow to account for other allowable values.
Language	The user's language. Uses the two-character language code as defined by the ISO 639-1 standard.
Notification	Determines whether to enable notifications. Select `Enable` or `Disable`.
TimeFormat	The user's time format. **Note** The ServiceNow Provisioner can set only time formats that are already assigned to the user account that you use for provisioning. For more information, see Global date and time field format in the ServiceNow documentation.
Photo	The user's photo.

ServiceNow provisioning features

The ServiceNow provisioning connection offers the following features:

Manages users in ServiceNow based on changes in an external datastore.

- Creates, updates, and disables users.

Copyright © 2025 Ping Identity Corporation

- Allows you to enable the create, update, and disable capabilities independently.
- Allows you to choose to disable users when deprovisioning.

ServiceNow provisioning known limitations

The following are known issues or limitations with the ServiceNow provisioning connection.

- When **Allow Users To be Disabled** is set to `false` but **Allow Users To Be Updated** is set to `true`, then any update to a disabled user, such as a name change, won't get propagated to ServiceNow. For updates to go through for a disabled user, both settings must be set to `true`.
- If the PingOne attribute `PhotoLink` is mapped to the ServiceNow attribute `Photo`, the URL can get truncated because the `maxLength` for the `Photo` attribute is `40`. We recommend that you manually upload the user photo on the ServiceNow console.
- If you delete a user in the PingOne console, the user will be disabled in the ServiceNow directory. In PingOne, `Disable` is the only option for **Remove action**. To delete a user, use the ServiceNow console.

Creating a Google Workspace connection

Use a Google Workspace connection to enable provisioning from PingOne to the Google Workspace user directory.

Before you begin

Review the Google Cloud documentation at Google Cloud documentation.

Make sure that you have:

- A Google Workspace project. For more information, see the Google Cloud admin console.
- Details for the connected application, such as application name, domain, OAuth client ID, and client secret. For more information, see Finding Google application details.
- Reviewed the Google Workspace provisioning known limitations.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **+** and then click **New Connection**.
3. On the **Identity Store** line, click **Select**.
4. Click **Google Workspace**, click **Select**, and then click **Next**.
5. Enter a name and description for the provisioning connection.

   The connection name is added to the **Connections** tab after you save the connection.
6. Click **Next**.
7. On the **Configure authentication** panel, enter the following information.

Copyright © 2025 Ping Identity Corporation

You can find the values on the Google Developer console. For more information, see Finding Google application details.

- **Application name**: The name of the connected application.
- **Domain**: The fully qualified domain name for the connected application.
- **OAuth client ID**: The application ID for the connected application.
- **OAuth client secret**: The application secret for the connected application.
- **OAuth access token**: The access token for the connected application.
- **OAuth refresh token**: The refresh token for the connected application.

8. Click **Test connection** to verify that PingOne can establish a connection to Google Workspace.

   Result:

   If there are any issues with the connection, a **Test Connection Failed** dialog box opens. Click **Continue** to resume the setup with an invalid connection.

   > **Important**
   > You cannot use the connection for provisioning until you have established a valid connection to Google Workspace. To retry, click **Cancel** in the **Test Connection Failed** dialog box and repeat step 7.

   Troubleshooting:

   Learn more about troubleshooting your connection in Troubleshooting Test Connections Failure.

9. On the **Actions** panel, enter the following:

Field	Value
Allow users to be created	Determines whether to create a user in the Google Workspace user directory when the user is created in the PingOne identity store.
Allow users to be updated	Determines whether to update user attributes in the Google Workspace user directory when the user is updated in the PingOne identity store.
Allow users to be disabled	When a user is disabled in the PingOne identity store, PingOne disables the user in the external identity store. **Note** You'll see this option only if you select **Allow users to be updated**.
Allow users to be deprovisioned	Determines whether to deprovision a user in the Google Workspace user directory when the user is deprovisioned in the PingOne identity store.

Copyright © 2025 Ping Identity Corporation

Field	Value
Remove action	Determines the action to take when removing a user from the Google Workspace user directory. **Note** You'll see this option only if you select **Allow users to be deprovisioned**. **Disable**:When a user is deprovisioned from the PingOne identity store, PingOne disables the user in the external identity store. **Delete**: When a user is deprovisioned from the PingOne identity store, PingOne deletes the user in the external identity store.
Deprovision on rule deletion	Determines whether to deprovision users that were provisioned using this rule if the rule is deleted.

10. Click **Finish**.

Next steps

To sync group members out of PingOne into a software as a service (SaaS) application, follow the instructions in Configuring outbound group provisioning.

Finding Google application details

Use the Google Developer Console to find the details for your connected application, such as client ID, client secret, access token, and refresh token.

Steps

1. Go to the Google Developer Console.
2. In the projects list, select a project or create a new one.
3. In the **Search** field, enter `Google Workspace`.
4. On the left navigation pane, click **Credentials**.
5. Under **OAuth 2.0 Client IDs**, click the appropriate application.
6. In the OAuth client window, copy the client ID and client secret to a secure location.

   You can always access the client ID and client secret from the **Credentials** page later if needed.

Google Workspace attribute mapping

The following table lists common Google Workspace user attributes that can be mapped to PingOne user attributes for user provisioning.

Copyright © 2025 Ping Identity Corporation

Attribute	Description
`Family Name`	The user's last name.
`Given Name`	The user's first name.
`Email Address`	The user's email address.
`Password`	The user's password.
`!enabled`	This attribute is used to maintain the status of the user account in Google Workspace. If the user is enabled in PingOne, then the sync enables the user in Google Workspace. If the user is disabled in PingOne, then the sync disables the user in Google Workspace.

> **Note**
> For outbound provisioning to Google Workspace, you must map the `addressFormatted` attribute for the user's address to appear in the Google Admin portal.

Google Workspace provisioning known limitations

The following are known issues or limitations with Google Workspace user provisioning.

- You can clear user attributes after setting them by sending an empty string value `onUpdate`.
- If a PingOne user has an invalid `addressCountry` value, Google Workspace might not provision the user properly.
- Changes to user attributes can take a few minutes to propagate to Google Workspace. However, in some cases, changes can take up to 24 hours to take effect. For more information, see How changes propagate to Google services.
- The `isAdmin` property can only be edited in the Make a user an administrator operation (makeAdmin method). If the property is edited in the user insert or update methods, the edit is ignored by the Google API service.
- When there is an existing group in Google with the same email ID and one member and PingOne has the same group with a different member, both the existing members and the new member are in Google after Provisioning.
- An update in membership in PingOne doesn't recreate a synced deleted group from Google.

Creating a GitHub EMU connection

Use a GitHub EMU (Enterprise Managed Users) connection to enable provisioning from PingOne to the GitHub EMU user directory.

Before you begin

Make sure that you have:

- A GitHub EMU tenant

Copyright © 2025 Ping Identity Corporation

- The Base URL for the GitHub EMU tenant, such as `https://api.github.com/scim/v2/enterprises/<enterprise_slug>`. For more information, see Creating an enterprise account in the GitHub documentation.
- The access token for the GitHub EMU tenant. For more information, see Getting a GitHub EMU access token.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **+** and then click **New connection**.
3. On the **Identity Store** line, click **Select**.
4. Click **GitHub EMU**, click **Select**,and then click **Next**.
5. Enter a name and description for the provisioning connection.

   The connection name is added to the **Connections** tab after you save the connection.
6. Click **Next**.
7. On the **Configure authentication** panel, enter the following:
   - **Base URL**: The fully qualified URL to use for the connected application, such as `https://api.github.com/scim/v2/enterprises/<enterprise_slug>`. For more information, see Creating an enterprise account in the GitHub documentation.
   - **Access Token**: The access token from GitHub EMU for the connected application. For more information, see Getting a GitHub EMU access token.
8. Click **Test connection** to verify that PingOne can establish a connection to GitHub EMU.

   Result:

   If there are any issues with the connection, a **Test Connection Failed** dialog box opens. Click **Continue** to resume the setup with an invalid connection.

   > **Important**
   >
   > You cannot use the connection for provisioning until you have established a valid connection to GitHub EMU. To retry, click **Cancel** in the **Test Connection Failed** dialog box and repeat step 7.

   Troubleshooting:

   Learn more about troubleshooting your connection in Troubleshooting Test Connections Failure.
9. In the **Configure preferences** and **Actions** sections, enter the following:

Copyright © 2025 Ping Identity Corporation

Field	Description
Group membership handling	Determines whether to update or replace target groups with PingOne memberships. Select **Merge** or **Overwrite**. **Note** Merging or overwriting memberships only applies to SCIM, Slack, and GitHub EMU provisioning connections.
Allow users to be created	Determines whether to create a user in the GitHub EMU user directory when the user is created in the PingOne identity store.
Allow users to be updated	Determines whether to update user attributes in the GitHub EMU user directory when the user is updated in the PingOne identity store.
Allow users to be disabled	When a user is disabled in the PingOne identity store, PingOne disables the user in the GitHub EMU user directory. **Note** Users who are disabled in PingOne are marked as suspended in the GitHub EMU identity store.
Allow users to be deprovisioned	Determines whether to deprovision a user in the GitHub EMU user directory when the user is deprovisioned in the PingOne identity store.
Remove action	Determines the action to take when removing a user from the GitHub EMU user directory. **Disable**: When a user is deprovisioned from the PingOne identity store, PingOne disables the user in the external identity store. **Delete**: When a user is deprovisioned from the PingOne identity store, PingOne removes the user in the external identity store.
Deprovision on rule deletion	Determines whether to deprovision users that were provisioned using this rule if the rule is deleted.

10. Click **Save**.

Next steps

To sync group members out of PingOne into a software as a service (SaaS) application, follow the instructions in Configuring outbound group provisioning.

Copyright © 2025 Ping Identity Corporation

Getting a GitHub EMU access token

Go to the GitHub EMU admin console and get an access token. Ensure that you have administrator privileges for the GitHub EMU admin console.

Steps

1. Go to the GitHub EMU admin console at `https://api.github.com/scim/v2/enterprises/<enterprise_slug>`, where *<enterprise_slug>* is your tenant name.
2. In the upper right, click your profile photo and then click **Settings**.
3. On the left, click **Developer settings**.
4. On the left, click **Personal access tokens**.
5. Click **Generate new token**. Select the `admin:enterprise` scope for the token. Click **Generate token**. Copy the token to a secure location. You'll enter this value in PingOne when you create the GitHub EMU provisioning connection.

GitHub EMU attribute mapping

The following table lists common GitHub EMU attributes that can be mapped for user provisioning.

Attribute	Description
Username (required)	The user's GitHub EMU username. According to GitHub, a username, including underscore and short code, must not exceed 39 characters. For more information, see About usernames for managed user accounts in the GitHub documentation.
Email (required)	The user's email address.
External ID (required)	Associates a user ID with a user account in the GitHub EMU user directory.
First Name	The user's first name.
Last Name	The user's last name.
Active	The status of the user account in the GitHub EMU user directory.
Formatted Name	The user's full name, including all middle names, titles and suffixes, formatted for display.
Display Name	A human-readable name for a user.

Copyright © 2025 Ping Identity Corporation

Attribute	Description
Roles	A list of the user's roles. For example, you could map the `Roles` attribute to `billing_manager` or `enterprise_owner`. For more information about role values, see Provision a SCIM enterprise user in the GitHub documentation. **Note** If a user doesn't have any roles assigned, they will be listed under the `Unaffiliated` section in GitHub EMU.

GitHub EMU provisioning features

The GitHub EMU provisioner offers the following features.

- Provision users from the PingOne identity store to GitHub EMU:
  - Create users
  - Update users
  - Deprovision users
- Customize provisioning options:
  - Deprovision users with a disable or delete action
- Outbound group provisioning

GitHub EMU provisioning known limitations

The following are known issues or limitations with GitHub EMU user provisioning.

- GitHub does not support provisioning a user with an initial disabled state.
- GitHub might enforce rate limiting for large numbers of users, such as more than 7000 users being provisioned at one time. For more information, see Rate limiting in the GitHub documentation.
- If a group exists in Github with the same group name from provisioning, then syncing fails.

Creating an LDAP gateway provisioning connection

Use a gateway connection to set up provisioning to or from an Active Directory or PingDirectory user store through a new or existing gateway configuration.

Before you begin

Copyright © 2025 Ping Identity Corporation

Ensure that you have:

- An existing gateway that is enabled and has a healthy connection. Learn more in Gateways. For provisioning through an LDAP Gateway, PingOne supports only Active Directory or PingDirectory user stores.

> **Note**
>
> For LDAP Gateways, you can configure inbound or outbound provisioning. RADIUS Gateways do not support provisioning.

- A gateway that is not configured for just-in-time (JIT) provisioning. You cannot enable the **Enable migration of new users upon first authentication** option if you want to use the gateway for outbound or inbound sync. Learn more in Adding a user type.
- For inbound provisioning, ensure that the LDAP Gateway is version 2.3.3 or later. Previous versions of the LDAP Gateway do not support inbound provisioning.
- For inbound provisioning, ensure that the service account reads deleted entries (cn=Deleted Objects) to keep PingOne in sync when objects are deleted in Active Directory.
- The service account can access all users in the specified Base DN.

> **Note**
>
> If the service account doesn't have access to deleted objects, such as a user that's been deleted, the service account can't detect that change.

- A gateway that makes outbound websocket connections to specific websocket endpoints. Learn more in Before configuring an LDAP gateway.
- A gateway that is able to establish an outbound connection to auth.pingone.com and api.pingone.com (or the equivalent URLs for your region). Learn more in PingOne URLs by geographic region.
- Established secure websocket connections on those relevant endpoints.

Steps

1. In the PingOne admin console, go to **Integrations** > **Provisioning**.
2. Click the **+** icon and then click **New connection**.
3. For **Gateway**, click **Select**.
4. Select an existing gateway or click **+ New Gateway** to set up a new gateway.

> **Important**
>
> The gateway must be active and have a valid connection to an LDAP directory. Learn more about creating a gateway in Gateways.

5. Click **Next**.

Copyright © 2025 Ping Identity Corporation

6. On the **Actions** page, enter the provisioning options. The following options apply only if the gateway provisioning connection is used in an outbound provisioning rule:
    - **Allow users to be created**: Determines whether to create a user in the LDAP user directory when the user is created in the PingOne identity store. By default, this option is not selected.
    - **Allow users to be updated** (default): Determines whether to update user attributes in the LDAP user directory when the user is updated in the PingOne identity store.
        - **Allow users to be disabled**: Determines whether to disable a user in the LDAP user directory when the user is disabled in the PingOne identity store.
    - **Allow users to be deprovisioned**: Determines whether to deprovision a user in the LDAP user directory when the user is deprovisioned in the PingOne identity store. By default, this option is not selected.
        - **Remove action**: Select **Delete** or **Disable**. Determines whether to remove or disable a user in the target identity store when the user is deleted in the PingOne identity store.
        - **Deprovision on rule deletion**: Determines whether to deprovision users if the associated provisioning rule is deleted.
7. Click **Finish**.

Next steps

- To define which users are provisioned from PingOne to LDAP and how attributes are mapped between PingOne and the LDAP directory, follow the instructions in Creating an outbound rule for a connection through an LDAP gateway.
- To configure an LDAP filter that specifies which users to provision from LDAP to PingOne, follow the instructions in Creating an inbound rule for a connection through an LDAP gateway.

Active Directory attributes

The following table lists common Active Directory attributes that can be mapped for user provisioning.

Attribute	Description
cn (Required)	The common name for the user account.
sAMAccountName (Required)	The user name for the user account.
Given Name	The first name of the user.
sn	The last name (surname) of the user.
Display Name	The name as it will appear in the PingOne identity store.
Mail	The email address for the user.
Mobile Number	The mobile telephone number for the user.
Telephone Number	The telephone number for the user.

Copyright © 2025 Ping Identity Corporation

Attribute	Description
Title	The user's title, such as Manager or CEO.
Active	The status of the user account.
Password	The password for the user.
ResetPassword	Determines whether a user must reset their password the next time they sign on. The default value is false, but it can be mapped to an attribute.
Street Address	The physical address for the user.
Postal Code	The ZIP code or postal code for the user.
l	The user's default location for purposes of localizing things like currency, date and time format, or numerical representations.
Country Abbreviation	The country code for the user.
st	The region for the user.

PingDirectory attributes

The following table lists common PingDirectory attributes that can be mapped for user provisioning.

Attribute	Description
uid (Required)	The user name for the user account. Typically mapped to `Username`.
sn (Required)	The last name (surname) of the user. Typically mapped to `Family Name`.
cn (Required)	The common name for the user account. Typically mapped to `Username`.
Given Name	The first name of the user.
Mail	The email address for the user.
Mobile Phone	The mobile telephone number for the user.
Telephone Number	The telephone number for the user.
Title	The user's title, such as Manager or CEO.
Active	The status of the user account.

Copyright © 2025 Ping Identity Corporation

Attribute	Description
Password	The password for the user.
Street Address	The physical address for the user.
Postal Code	The ZIP code or postal code for the user.
l	The user's default location for purposes of localizing things like currency, date and time format, or numerical representations.
st	The region for the user.
Preferred Language	The primary language for the user.

Default attribute mapping for inbound provisioning through an LDAP gateway

The following table lists the default attributes for Active Directory and PingDirectorythat can be mapped to PingOne user attributes for user provisioning.

Active Directory default attributes

Attribute	Description
sAMAccountName	The user's username.
sn	The user's last name (surname).
Given Name	The user's first (given) name.
Mail	The user's email address.
Active	The status of the user account in Active Directory.

PingDirectory default attributes

Attribute	Description
uid	The user's username.
Given Name	The user's first (given) name.
sn	The user's last name (surname).
Mail	The user's email address.

Copyright © 2025 Ping Identity Corporation

Attribute	Description
Active	The status of the user account in PingDirectory.

Known issues for provisioning through an LDAP gateway

The following are known issues or limitations with provisioning through an LDAP gateway.

- PingOne does not support concurrency for LDAP inbound provisioning using the same gateway connection, even with different User Base DNs.
- For bi-directional LDAP sync, ensure that the attribute mappings on both rules are identical.

> **Note**
> PingOne does not maintain directory hierarchy on outbound to be the same as inbound.

- In the expression builder, you can use only LDAP attributes that are part of the default attribute list. As a workaround, you can use the ADD feature to map the needed attribute and use it in the expression.
- The LDAP filter currently does lexicographical comparison for numeric values.
- In Active Directory, deleting an OU that contains users might not deprovision users in PingOne.
- PingOne does not support `moddn` operations.
- PingOne does not support updating the `uid` attribute value.

Editing a provisioning connection

You can edit an existing connection for more specific configuration of provisioning actions.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **Connections**.
3. Click a connection to open the details panel.
4. Click the **Overview** tab and then click the pencil icon.
5. Edit the Icon, Name, or Description as needed.

> **Note**
> You can't change the icon for PingOne Directory connections.

6. Click **Save**.
7. Click the **Configuration** tab and then click the pencil icon.

Copyright © 2025 Ping Identity Corporation

The configuration details vary depending on the type of connection you are editing. For more information, see Creating a connection.

8. Click **Save**.

Next steps

Check the connection to see if identities are being provisioned as expected. See Viewing sync status.

Editing a provisioning rule

You can edit an existing rule to change the custom filter and attribute mapping. You cannot change the source or target connection after a rule is created.

Steps

1. Go to **Integrations → Provisioning**.
2. Click **Rules**.
3. Click a rule to open the details panel.
4. Click the **Overview** tab.
5. In the upper right, click the **More Options** menu and then click **Edit Overview**.
6. Edit the **Name** or **Description** as needed.
7. Click **Save**.
8. Click the **Configuration** tab.
9. Do one of the following:
    - For outbound provisioning, click the **User Filter** button. Enter a filter to define the users that will be provisioned. For more information, see Adding a user filter.
    - For inbound gateway provisioning, click the **LDAP filter** button (optional). Enter an LDAP filter expression to define the users that will be provisioned. For more information, see LDAP filters.
    - For inbound provisioning from Workday and SCIM identity stores, you can specify some additional options for onboarding new users. See Adding attribute mapping for inbound provisioning.
    - For outbound provisioning to Google Workspace, you must map the `addressFormatted` attribute for the user's address to appear in the Google Admin portal. For more information, see Google Workspace attribute mapping.
10. Click the **Attribute Mapping** button. Review the attribute mappings. For more information, see Adding attribute mapping for outbound provisioning. For inbound provisioning, you can specify some additional options for onboarding new users. See Adding attribute mapping for inbound provisioning.
11. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Troubleshooting test connection failure

The following information applies to the various configuration error scenarios. You can use your connections details page, Splunk logs, or Postman to identify and resolve issues.

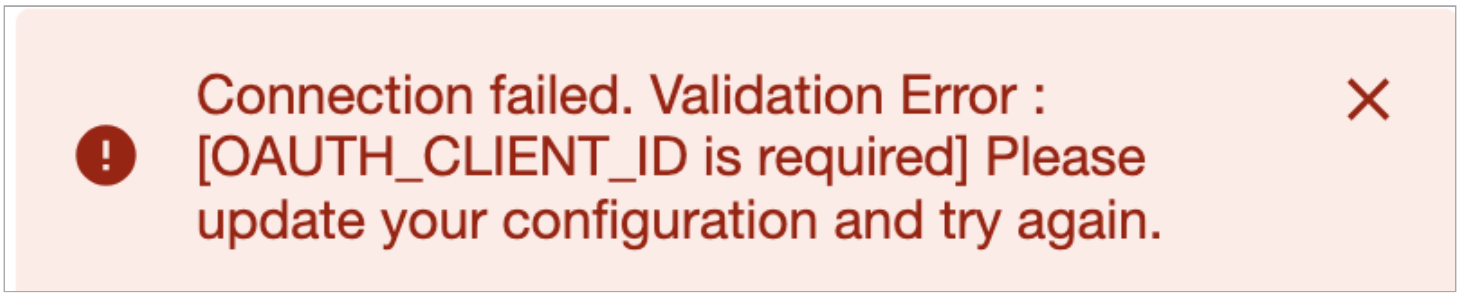
> **Note**
>
> If you are establishing a connection for the first time, make sure that you have a webhook to connect your PingOne environment to Splunk. This will help you troubleshoot your connection. Learn more in Installing the PingOne app for Splunk.

I am getting a validation error.

A validation error occurs if you didn't enter all required configurations in the **Configure Authentication** panel in your PingOne admin console.

Verify that you have entered all the necessary configurations for your connection and click **Test Connection**.

> **Note**
>
> Validation errors show the configuration that is required to have a successful connection, such as a Client ID, SCIM URL, and so on.

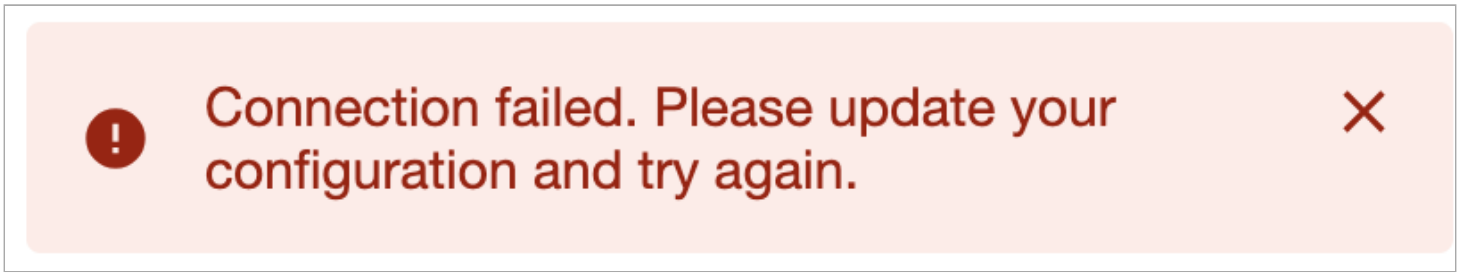


I entered all my configurations and am still getting an error message.

If you receive this error message and have entered all your configurations, it might be a problem with the configuration itself.

In your Splunk logs, check for any possible errors, such as a `400` or `500` error.

Reviewing a Splunk log can identify the error, such as a missing letter from your client ID or incorrect URL, and help you resolve it in the admin console.



What other testing can I do to troubleshoot a test connection failure?

For further testing your connection configuration, use the `POST: Test Configuration` call in Postman, as shown in the following cURL example. When you test this call, the response returned will include a success message or bad request message.

Copyright © 2025 Ping Identity Corporation

POST Test Connection Configuration

ENV

```
{{apiPath}}/environments/{{envID}}/propagation/stores/connection/status
```

The `POST /environments/{{envID}}/propagation/stores/connection/status` operation verifies identity store resource configuration in the specified environment resource. This operation uses the `application/vnd.pingidentity.connection.check+json` custom media type as the content type in the request header. This call is prospective; that is, you can test whether a proposed configuration will be accepted.

Headers

authorization	Bearer {{accessToken}}
content-type	application/vnd.pingidentity.connection.check+json

Body

raw (application/vnd.pingidentity.connection.check+json)

```
{
```

Example Request — Test Connection Configuration

Language - cURL

```
curl --location --request POST '{{apiPath}}/environments/{{envID}}/p
--header 'Authorization: Bearer {{accessToken}}' \
--header 'Content-Type: application/vnd.pingidentity.connection.chec
--data-raw '{
    "type": "scim",
    "name": "scim",
    "configuration": {
```

Example Response — 200 OK

P

Deleting a connection

Use the Provisioning page to remove a connection you no longer need.

Steps

1. Go to **Integrations → Provisioning**.
2. Click the **Connections** tab.
3. Find the appropriate entry and click it to show the details panel.
4. In the upper right, click the three dots menu and then click **Delete**. If you have a rule associated with a particular connection, you must remove the rule from the connection before you can delete the connection.

> **Important**
>
> No new users will be provisioned based on this connection. If you selected the `Deprovision on rule deletion` option when creating the rule, all users in the target user store that were provisioned using this rule will be deleted or disabled.

5. In the confirmation message, click **Delete**.

Result

The connection is removed from the list and permanently deleted.

Deleting a rule

Use the Provisioning page to remove a rule you no longer need.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Integrations → Provisioning**.
2. Click the **Rules** tab.
3. Find the appropriate entry and click it to show the details panel.
4. In the upper right, click the **More Options** menu and then click **Delete**.

> **Note**
> If the rule is associated with a particular connection, the rule will be removed from the connection when you delete the rule.

5. In the confirmation message, click **Delete**.

Result

The rule is removed from the list and permanently deleted. No new users will be provisioned based on this rule.

Using the SCIM API to import users

Use the SCIM API to import users into PingOne. The PingOne SCIM API acts as a translation layer that receives SCIM requests to then issue as equivalent PingOne API requests, and translates PingOne API responses to SCIM-compliant responses for the user.

> **Note**
> PingOne supports only version 2.0 of the SCIM standard.

Accessing the PingOne SCIM API

The URI for the PingOne SCIM API is

https://scim-api.pingone.com/environments/*{{envID}}*/v2/

where *{{envID}}* is the ID for the appropriate PingOne environment.

Using the /Users endpoint

Use the `/Users` endpoint to create, update, and delete users.

The URI for the `/Users` endpoint is *{{scimPath}}*/environments/*{{envID}}*/v2/Users

where

- *{{scimPath}}* is the regional domain for the PingOne SCIM service provider, such as https://scim-api.pingone.com or https://scim-api.pingone.eu.
- *{{envID}}* is the ID for the appropriate PingOne environment.

Copyright © 2025 Ping Identity Corporation

Examples

Create user

POST *{{scimPath}}*/environments/*{{envID}}*/v2/Users

Read one SCIM user

GET *{{scimPath}}*/environments/*{{envID}}*/v2/Users/*{{userID}}*

Read all SCIM users

GET *{{scimPath}}*/environments/*{{envID}}*/v2/Users

Delete SCIM user

DELETE *{{scimPath}}*/environments/*{{envID}}*/v2/Users/*{{userID}}*

You can use the `/DirectMappedUsers` endpoint to pass attributes exactly as they appear in the PingOne schema. You can pass any attributes, including custom attributes, by including the exact name of the attribute in the SCIM payload.

For more information, see SCIM in the PingOne API Reference.

Gateways

PingOne gateways act as a bridge between your on-premise infrastructure and PingOne.

You can create the following types of gateways:

Gateway type	Description
LDAP	Use LDAP gateways to: • Authenticate users in PingOne when their credentials are stored in an external directory • Migrate identities to the PingOne user store • Authenticate users via Kerberos
RADIUS	Authenticate users that are authenticating to a remote network access server.
Authorize	Evaluate authorization decisions on-premise while maintaining authorization policies centrally in PingOne.
PingGateway	Integrate web applications, APIs, and microservices with PingOne without modifying the application or the container where it runs. Built on a reverse proxy architecture, PingGateway enforces security and access control.

Copyright © 2025 Ping Identity Corporation

LDAP gateways

PingOne can use an LDAP gateway to authenticate and authorize user identities that are stored in an external directory.

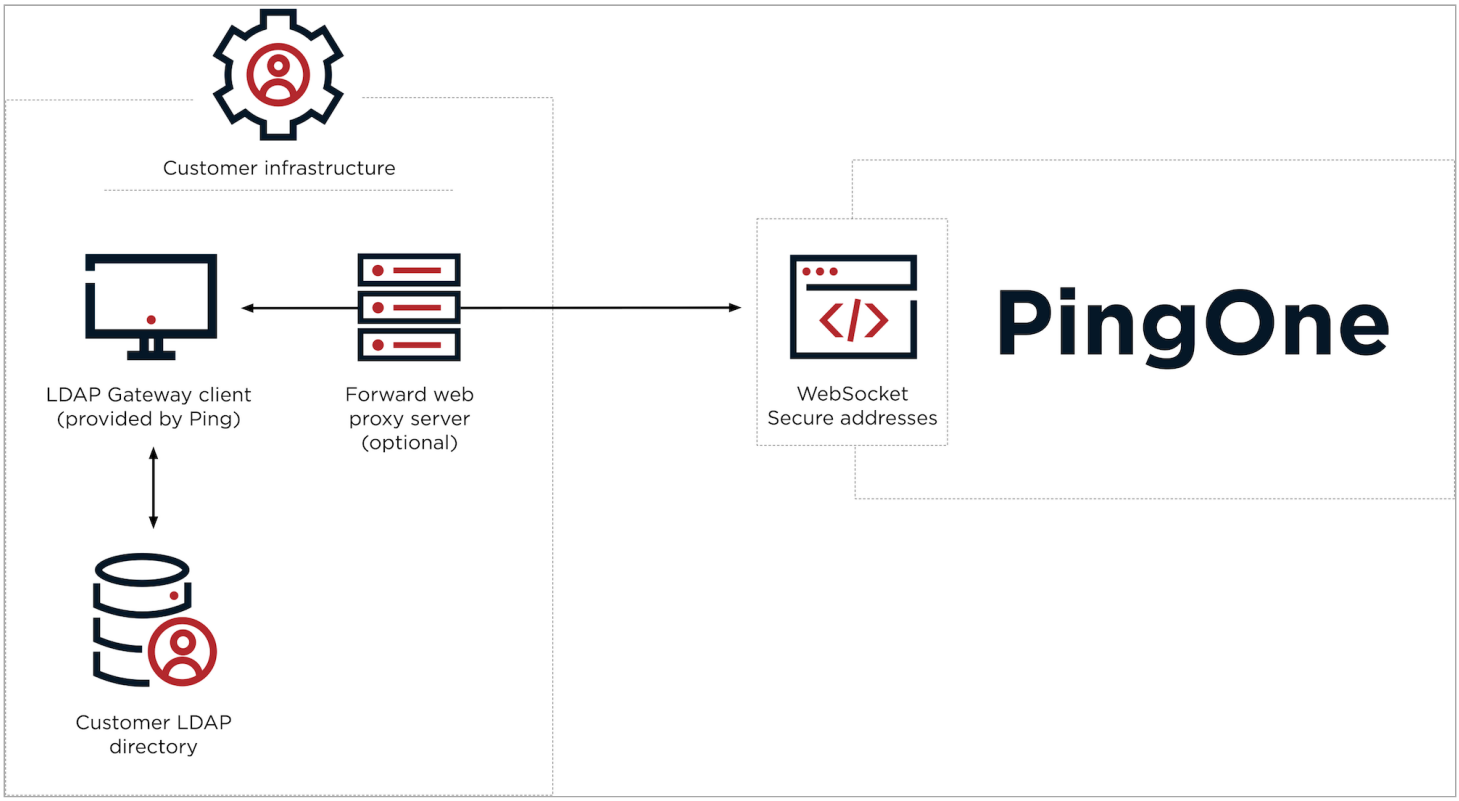
Use an LDAP gateway to:

- Authenticate users in PingOne when their credentials are stored in an external directory.
- Migrate identities to the PingOne directory when users initially sign on through the LDAP gateway client.
- Make authorization decisions using identity data stored in an external directory. For more information, see Connecting an LDAP Gateway service.

When a user signs on to PingOne, if PingOne finds the user in the PingOne directory, then the sign-on flow continues.

If PingOne doesn't find the user in the PingOne directory, and a gateway is configured, then PingOne checks the external user directory. If PingOne finds an identity matching the username and password, then it authenticates the user and can create the identity in the PingOne directory. Each user that is authenticated using a gateway can have their identities added to the PingOne directory.

The following diagram shows a high-level overview of how LDAP gateways work in PingOne. Beginning with the LDAP Gateway client application 3.2.0, you can optionally configure a forward web proxy server to handle WebSocket traffic between the gateway client and PingOne.



Supported directories

PingOne LDAP gateways support the following directories.

- PingDirectory

Copyright © 2025 Ping Identity Corporation

- Microsoft Active Directory, with or without Kerberos authentication

  Learn more in Kerberos authentication.

- Oracle Directory Server Enterprise Edition
- Oracle Unified Directory
- CA Directory
- IBM (Tivoli) Security Directory Server
- Any LDAP v3-compliant directory server

Before configuring an LDAP gateway

Before you set up an Lightweight Directory Access Protocol (LDAP) gateway, ensure that you have the following information.

Details about the directory

You'll need the following information about the LDAP directory:

- The host name and port for all server instances.
- A service account from the directory server that the PingOne gateway will use to access the directory (`bind DN` and `bind password`).

  Learn more about configuring the service account and granting the required permissions in Best practices for configuring Active Directory for LDAP gateways.

  > **Note**
  >
  > The service account must be able to search for users in the directory by username.

- Whether the directory instances support TLS and StartTLS. If the TLS certificates for the servers were signed by a non-default certificate authority (CA), you must have the CA's signing certificates available to upload to PingOne. Learn more in Importing an LDAP certificate to PingOne.
- A method for correlating a directory user with a PingOne user, including the base DN for issuing searches against the directory and the attribute that corresponds to the PingOne `username` attribute.

Docker

You can run the gateway in a Docker container or as a standalone Java or Windows application. If you plan to run the gateway in a Docker container, you must have Docker installed on the computer that will run the gateway.

System requirements

The computer, virtual machine, or Docker environment that will run the gateway should have the following resources dedicated to the gateway:

Copyright © 2025 Ping Identity Corporation

Resource	Requirement
Processor	Two CPUs or virtual CPUs
RAM	1 GB
Storage	1 GB

Java

Verify the Java version on the computer that will run the gateway. Ensure that you have one of the following versions:

- 17.0.8 or later
- 21 LTS or later

Gateway access

The gateway requires access to the LDAP directory server over the network as well as the ability to initiate outbound requests over the internet to establish a WebSocket Secure connection to PingOne.

The WebSocket Secure address varies depending on your region. Ensure that the gateway can access the WebSocket Secure address for your region, as listed in the following table.

If provisioning will be used, the gateway must be able to establish an outbound connection to the API endpoints for your region, as listed in the following table. Learn more in Creating an LDAP gateway provisioning connection.

Region	Address	API Endpoints
Australia	wss://gateways.pingone.com.au/ wss://gateways-ap-southeast-2.pingone.com.au/	auth.pingone.com.au api.pingone.com.au
Canada	wss://gateways.pingone.ca/ wss://gateways-ca-central-1a.pingone.ca/ wss://gateways-ca-central-1b.pingone.ca/	auth.pingone.ca api.pingone.ca
Europe	wss://gateways.pingone.eu/ wss://gateways-eu-central-1.pingone.eu/ wss://gateways-eu-west-1.pingone.eu/	auth.pingone.eu api.pingone.eu
North America (US)	wss://gateways.pingone.com/ wss://gateways-us-east-2.pingone.com/ wss://gateways-us-west-2.pingone.com/	auth.pingone.com api.pingone.com
Singapore	wss://gateways.pingone.sg/ wss://gateways-ap-southeast-1y.pingone.sg/ wss://gateways-ap-southeast-1z.pingone.sg/	auth.pingone.sg api.pingone.sg

Copyright © 2025 Ping Identity Corporation

Region	Address	API Endpoints
Asia Pacific (legacy) **Note** Available only for existing .asia customers.	wss://gateways.pingone.asia/ wss://gateways-ap-southeast-2.pingone.asia/	auth.pingone.asia auth.pingone.asia

PingOne user privileges

The administrator setting up the gateway must have the **Environment admin** role. To confirm, open the PingOne console, locate the administrator identity, and confirm its roles.

Forward web proxy server

You can configure the client application to use a forward web proxy server to handle WebSocket traffic between the gateway client and PingOne. You'll need to provide:

- The IP address and the port of the web proxy
- Access credentials if the web proxy requires authentication. An LDAP gateway client version of 3.3.0 or higher is required.

> **Note**
>
> - The web proxy server must support the WebSocket protocol.
> - Digest authentication does not support international characters.
> - Basic authentication requires configuration in the proxy server to support international characters.

Learn more about configuring a web proxy in Starting a gateway instance.

Kerberos

If you are using Kerberos for authentication with Active Directory, you'll need:

- Service Account User Principal Name
- Service Account Password
- Service Principal Name

  Learn more about configuring service principal names in Creating SPNs.

The Service Account must be configured with AES 128 bit or 256 bit encryption. To configure encryption in Kerberos:

1. Start Active Directory Users and Computers.
2. View the properties of the Service Account that you created for the gateway.
3. Click the **Account** tab.

Copyright © 2025 Ping Identity Corporation

4. In the **Account Options** section, select one or both of the following:
    - **Kerberos AES 128 bit encryption**
    - **Kerberos AES 256 bit encryption**

Learn more in Kerberos authentication.

Best practices for configuring Active Directory for LDAP gateways

This guide provides an overview of the recommended configuration for integrating AD with PingOne Lightweight Directory Access Protocol (LDAP) gateways, including setting up the service account with the required permissions and granting the permissions for user password changes and resets.

> **Note**
> These configurations in AD require LDAP Gateway client application 3.1.2 or later.

In this guide, the example gateway is used to manage users in the Employees organizational unit (OU):

Bind DN: `CN=Service Account,OU=ServiceAccounts,OU=PingOneLDAPGateway`

Search Base DN: `OU=Employees,OU=PingOneLDAPGateway`

Setting up the service account

About this task

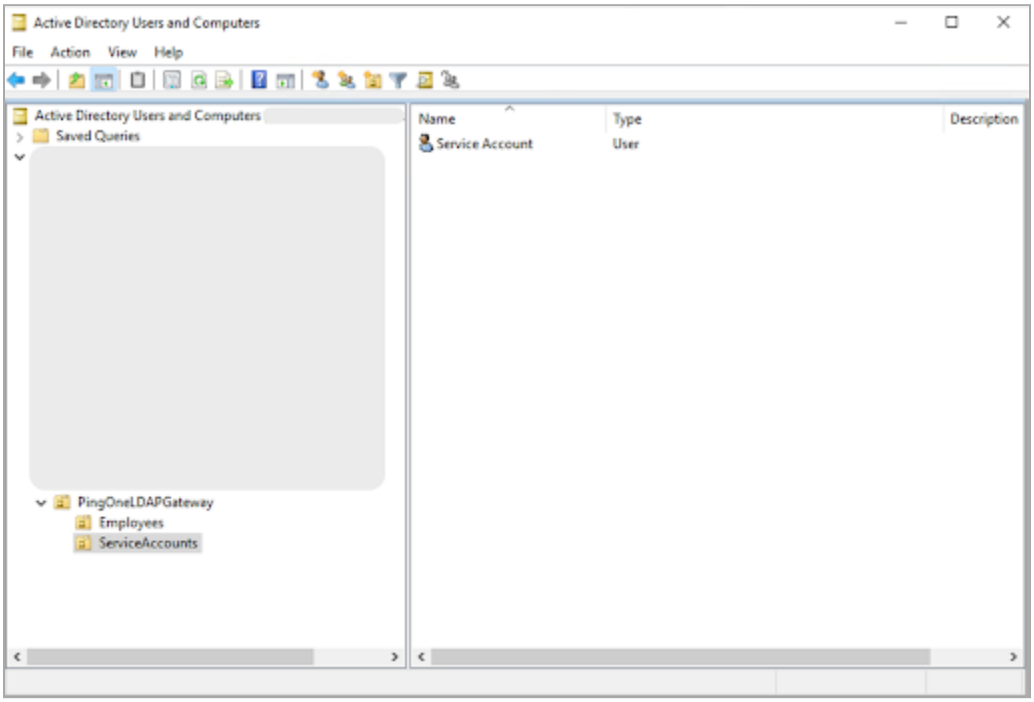
Set up the service account to manage permissions for the client:

Steps

1. Set the service account as the bind DN in the LDAP gateway.

    > **Note**
    > **Service Account** should be in a separate OU from the target users (**Employees** in this example).

Copyright © 2025 Ping Identity Corporation



2. Grant **Read** permissions for each Search Base DN in the gateway's user types.

3. For inbound provisioning through the LDAP gateway, ensure that the service account can read deleted entries (`cn=Deleted Objects`) to keep PingOne in sync when objects are deleted in AD:

   Choose from:

   - Make the service account an administrator.
   - Allow non-administrators to view the AD deleted objects container.

     Learn more in Let non-administrators view deleted objects container in the Microsoft documentation.

Granting user password permissions

About this task

Manage user password changes and resets by enabling users to change their own passwords and administrators to reset user passwords.

Instead of making changes to each user, AD also allows admins to apply permissions to whole hierarchies of users, such as an entire OU.

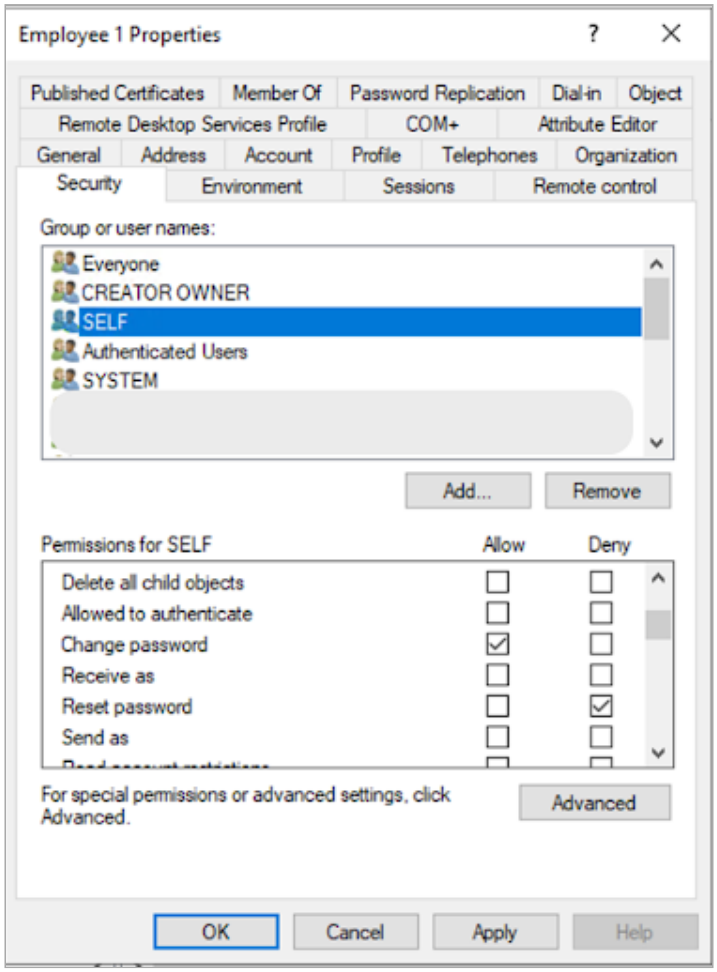
Steps

- To allow users to change their own passwords:

  1. Right-click on the user group or name to which you want to grant password permissions and click **Properties**.
  2. On the **Security** tab, select the **SELF** group of users, and select the **Allow** checkbox for **Change password** and the **Deny** checkbox for **Reset password**.
  3. Click **Apply** and then **OK**.

Copyright © 2025 Ping Identity Corporation

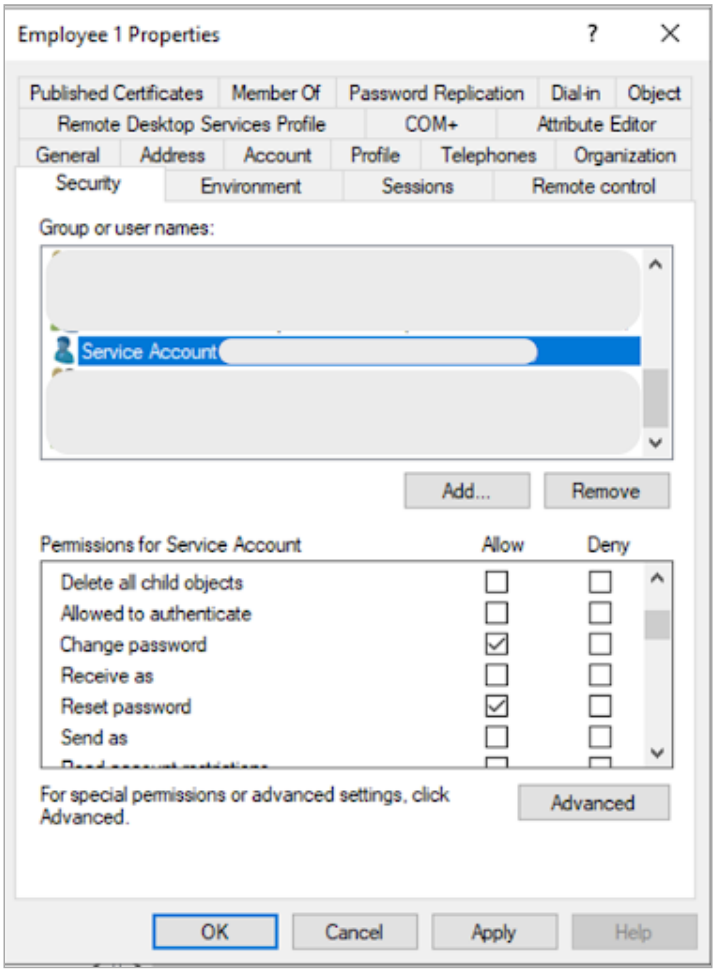
> **Note**
>
> To disable users from changing their own passwords, select the **Deny** checkbox for **Change password**.



- To allow admins to reset user passwords:

  1. Right-click the **Employee user object**, click **Properties**, and then click the **Security** tab.
  2. In the list of groups, select the **Service Account** and select the **Allow** checkbox for **Change password** and **Reset password**.

Copyright © 2025 Ping Identity Corporation



3. Click **Apply** and then **OK**.

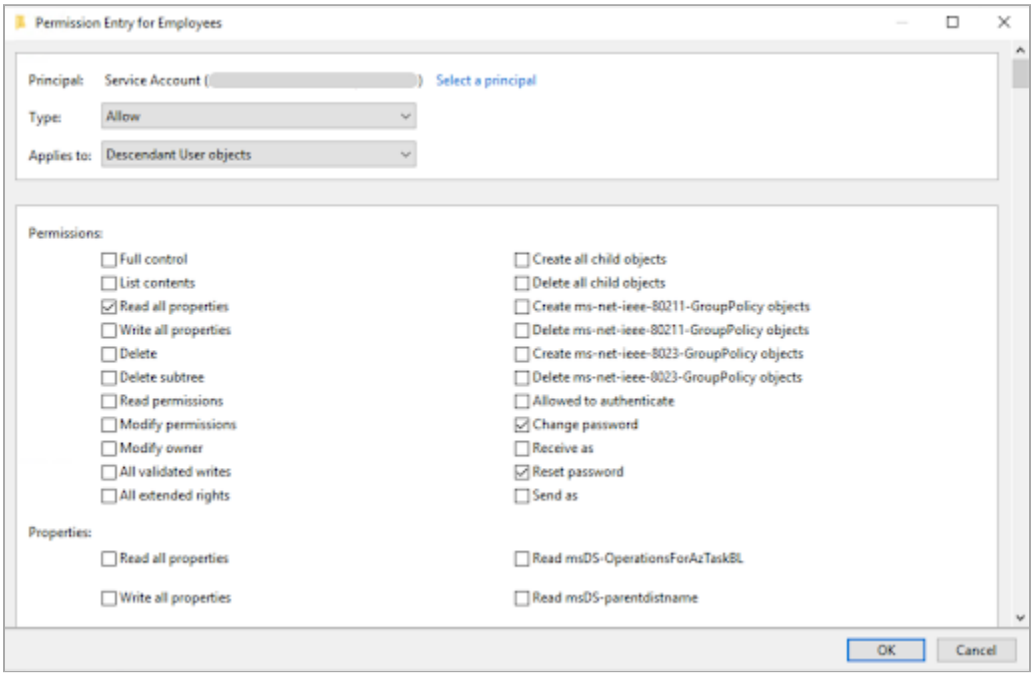
- To add permissions to an entire OU:

  1. Open **Active Directory Users and Computers**.
  2. Right-click on the OU of the target users (for example, **Employees**), and then click **Properties**.
  3. To create customizable permissions, click the **Security** tab, click **Advanced**, and then click **Add**.

     1. In the **Permission Entry** window, click **Select a principal**.
     2. Enter `Service Account` for object name and click **OK**.
     3. Clear the default permissions and then select the desired permissions.

        For example, the recommended permissions for a service account are:

        - **Read all properties**
        - **Change password**
        - **Reset password**



4. Click **OK**.

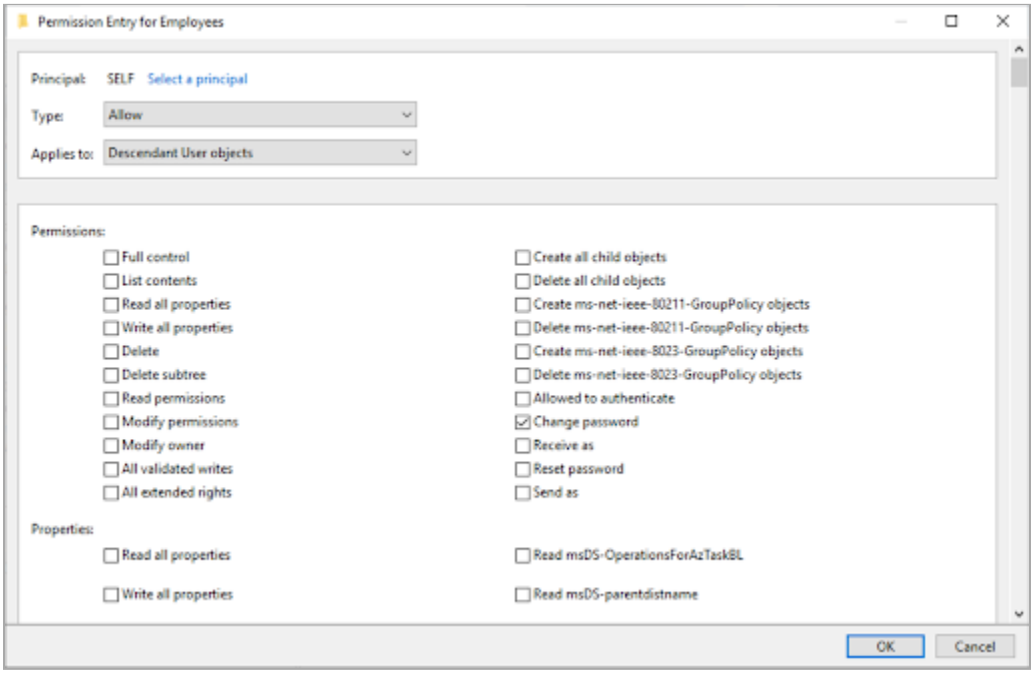
4. In the **Advanced Security Settings** window, click **Add**.

   1. In the **Permission Entry** window, click **Select a principal**.

   2. Enter `SELF` for object name and click **OK**.

   3. Clear the default permissions and then select the desired permissions.

      For example, the recommended permission for **SELF** is **Change password**.



   1. Click **OK**.

Copyright © 2025 Ping Identity Corporation

5. In the **Advanced Security Settings** window, click **Apply** and **OK**.
6. In the **Security** tab, click **Apply** and **OK**.

Importing an LDAP certificate to PingOne

Import your certificate authority (CA) certificate to PingOne to establish trust between PingOne and your Lightweight Directory Access Protocol (LDAP) gateway.

Before you begin

Contact your LDAP administrator to obtain the certificate from the CA that issues the certificates to their LDAP servers.

About this task

> **Note**
> Although you can import the LDAP certificate to PingOne, we recommend that you import the issuing CA certificate to ensure that the connection will continue to work if the LDAP certificate auto-renews.

Steps

1. Go to **Settings → Certificates and Key Pairs**.
2. Click **+ Add**, and then click **Import Key Pair/Cert**.
3. For **Usage type**, select **SSL/TLS**.
4. Click **Select a file** and locate the appropriate file on your local file system.
5. Select the file and then click **Open**.
6. In the **Import key pair certificate** window, click **Upload**.

Setting up an LDAP gateway

Set up a gateway connection by configuring a gateway in PingOne and downloading a gateway instance to run on-premise, adjacent to the LDAP directory.

About this task

You can then create an authentication policy that uses the gateway to migrate new users the first time they sign on. User objects can also be configured to use the gateway for credential validation using the PingOne Users API. Learn more in Manually migrating users to PingOne.

If you are using Microsoft Active Directory (AD), you can also set up Kerberos authentication. Learn more about setting up AD in Best practices for configuring Active Directory for LDAP gateways.

To set up a gateway:

Steps

1. Add an LDAP gateway.

Copyright © 2025 Ping Identity Corporation

2. Start a gateway instance.
3. Verify a gateway instance.
4. Add a user type.
5. **Optional:** Create an authentication policy that uses a gateway.
6. **Optional:** Add an authentication policy to an application.

Adding an LDAP gateway

An LDAP gateway connection allows PingOne to communicate with the LDAP directory.

About this task

> **Note**
> For gateway provisioning, PingOne supports only Active Directory or PingDirectory user stores. For more information, see Provisioning.

Steps

1. Go to **Integrations → Gateways**.
2. Click the **+** icon.
3. Enter the following:
   - **Name**: A name for the gateway. The name must be unique within the environment.
   - **Description**: (Optional). A brief characterization of the gateway.
   - **Gateway Type**: Select LDAP.
4. Click **Next**.
5. Enter connection information:
   - **LDAP Directory Type**: Specify the type of directory that the gateway will connect to. PingOne supports any LDAP v3-compliant directory server.

     > **Note**
     > If you select **Microsoft Active Directory**, you'll have the option to use Kerberos for authentication. See Kerberos authentication.

   - **LDAP Host Name**: Specify the IP address or hostname for the external directory server. Click **+ Add LDAP Host** to configure multiple servers for failover. PingOne will try to connect to the servers in the order they are listed. If the first server is unavailable, then PingOne will try to connect to the next server in the list.
   - **Port**: Specify the port that the external directory is located on. For standard LDAP connections, the default port is 389. For connections with TLS security, the default port is 636.

Copyright © 2025 Ping Identity Corporation

- **Follow LDAP Referrals**: Determines whether the LDAP Gateway client follows referrals it receives from LDAP servers.
- **Connection Security**: Select **TLS**, **StartTLS,**or **None** to configure the security options for the connection. **TLS** is the default selection and is recommended for better security.
- **Allow TLS connections with untrusted certificates**: Allow certificates that are signed by a certificate authority (CA) that is not well-known or trusted. A certificate could be untrusted if the certificate is expired, the hostname doesn't match what is specified in the certificate, or a certificate is self-signed.
- **Bind DN**: Specify the credential to be used to access the external directory. You can query the directory to get this value.
- **Bind Password**: Specify the password for the selected `Bind DN`.

  > **Note**
  >
  > The following options appear only if you selected **Microsoft Active Directory** for **Directory type**.

- **Enable Kerberos Authentication**: Determines whether to use Kerberos for authentication.
- **Service Account User Principal Name**: The UPN of a properly configured service account. The value must be in UPN format and is case-sensitive. For more information, see UPN format in the Active Directory documentation.

  > **Note**
  >
  > The Service Account UPN (User Principal Name) requires a proper SPN (Service Principal Name) and is case-sensitive. For more information, see Creating SPNs. For additional protection, we recommend adding MFA to the associated authentication policy. For more information, see Creating an authentication policy that uses the gateway and Adding a multi-factor authentication or PingID step.

- **Service Account Password**: The password for the service account.
- **Retain Previous Credentials**: Determines whether PingOne will remember credentials that were previously used to authenticate. If you change the service account credentials, PingOne will save the previous five service account credentials. This allows Kerberos requests issued with previous service account credentials to be validated for the specified amount of time. For more information, see Retaining credentials.
- **Retention Duration (Minutes)**: Specifies how long to keep the previous credentials, in minutes. The default value is 610.

6. Click **Save**.

   Result:

   PingOne generates a gateway credential, which the gateway uses to authenticate with PingOne.

   > **Note**
   >
   > A gateway credential is like a password, so keep it protected. For security reasons, PingOne does not store the generated gateway credentials, but you can always create a new one in the PingOne console. Multiple gateway instances can use the same gateway credential.

7. Copy the credential and paste it to a secure location.

Copyright © 2025 Ping Identity Corporation

You'll use the credential later when creating a gateway instance.

8. **Optional:** Click **Show me the Docker command** and copy it to a secure location.
9. Click **Done**.

Next steps

Starting a gateway instance

Adding a user type

A user type identifies categories of users in the external directory. You must define a user type in the gateway to use external authentication as part of your authentication policy.

About this task

You can bulk migrate users from an external directory and continue to have those PingOne users authenticate with the external directory as the password authority. In other words, password checks and password changes would still go through the external directory. See the **Select Password Authority** option in the following procedure.

> **Tip**
> You can pre-populate the fields with default values for the directory type you chose when you created the gateway. Click the **Use default values** button.

Steps

1. In the PingOne admin console, go to **Integrations** > **Gateways**.
2. Locate the appropriate gateway and then click the gateway name to expand the gateway details.
3. Click the **Lookup** tab.
4. Next to **User Types**, click the **+** icon.
5. To use the default values based on the type of LDAP directory that you selected when you created the gateway, click the **Use default values** button.
6. Enter or edit the following:
   - **User Type**: Enter a name for the set of users you're trying to look up. This field is a label for the user type you're creating, and typically identifies the category of users you are trying to import, such as `Employees`.
   - **Select Password Authority**: Select **PingOne** or **LDAP** for authentication. If you choose **PingOne**, PingOne will authenticate with the external directory the first time and then authenticate with PingOne for all subsequent sign-ons. Click **Help me decide** for more information.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> - If you change the password authority from LDAP to PingOne for an existing user type, the user's password is migrated from the LDAP directory to PingOne the next time the user signs on.
> - If you change the password authority from PingOne to LDAP for an existing user type, the user's password is removed from PingOne. Going forward, PingOne sends credential validation requests to the LDAP directory through the LDAP gateway.

- **Push password changes to LDAP**: If you selected **PingOne** as the password authority, select this option to have PingOne update the LDAP directory with the new password if a user changes their password in PingOne.
- **Enable password changes from PingOne**: If you selected LDAP as the password authority, select this option to allow users to change their password in PingOne. PingOne will update the LDAP directory with the new password.

  If you are running an Active Directory server, PingOne can change a user's password if the user's password expires or the **User must change password at next logon** option is selected. Enable this option to allow PingOne to change a user's password.
- **User Search LDAP Base DN**: Specify a path to the directory for the users that you want to authenticate. The LDAP gateway searches the entire subtree.
- **User Link Attributes**: Define the LDAP attributes that PingOne uses to link PingOne users with LDAP users when they sign on. For example, `dn` and `sAMAccountName`.

You can define multiple attributes if all users don't have the same unique attributes populated in the LDAP directory. PingOne searches for each defined attribute individually as an "OR" query from top to bottom until the correlating user is found. If multiple users are found for one user attribute, then PingOne searches for the next defined attribute.

- **Enable migration of new users upon first authentication**: Select this option to enable users without a PingOne user record to sign on based on the applicable authentication policy. When users sign on for the first time, PingOne creates user records based on the attribute mapping configuration.
- **LDAP Filter**: Specify an LDAP filter to identify the users that should be migrated to the PingOne directory.
- **Population**: When importing the identity to PingOne, add the identity to the specified population.
- **Update PingOne user attributes as users sign on**: Select this option to update user attributes in PingOne when users sign on successfully through the LDAP gateway client and when attribute changes are detected based on the LDAP server response. If an update fails for at least one user attribute, no attributes will be updated, and authentication will fail. Successes and failures are recorded in the PingOne audit log.

  You can find a complete list of events logged in PingOne in Audit Reporting Events in the PingOne API documentation.

  > **Note**
  >
  > - User attributes are not updated if the user authenticates with Kerberos.
  > - This option is only available when **Password Authority** is set to **LDAP**.

- **Map Attributes**: Map LDAP user attributes to PingOne attributes. For example, you could map the `mail` attribute in the LDAP directory to the `Email` attribute in PingOne. Learn more in Mapping attributes.

7. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Mapping the group attribute from an LDAP gateway

If the external directory includes group information in its security tokens, you can add a mapping between the **External Group Names** attribute in PingOne and the inbound attribute name from the external directory.

About this task

> **Note**
>
> For Lightweight Directory Access Protocol (LDAP) gateway connections, the group associated with the user is provisioned to PingOne only on the initial user migration.

Steps

1. Go to **Integrations** > **Gateways**.
2. Locate the appropriate gateway connection.
3. Click the gateway entry to open the gateway details panel.
4. On the **Lookup** tab, click the **More Options** (⋮) icon, and then click **Edit**.
5. In the **Map Attributes** section, click **+ Add Mapping**.
6. For **PingOne User Profile Attribute**, select **External Group Names**.
7. For the external directory attribute, enter the inbound attribute name from the external directory. For example, `memberOf` for Microsoft Active Directory, and `isMemberOf` for PingDirectory.
8. Click **Save**.

Next steps

When a user signs on the first time, if the user doesn't exist in PingOne, the gateway creates a user record in PingOne based on the mappings, including group membership. When you enable the **Update PingOne user attributes as users sign on** option, user attributes update each time a user signs on successfully through the LDAP gateway client. The groups associated with the user are also provisioned to PingOne each time the user signs on to PingOne.

Learn more in Adding a user type and Just-in-time provisioning of external groups.

Starting a gateway instance

You can run a standalone gateway as a Windows service, a standalone Java application, or a Docker container, with or without a forward web proxy server.

About this task

Copyright © 2025 Ping Identity Corporation

Note

- Stopping and starting a gateway instance does not cause any configuration issues, but the PingOne Gateway will not function until the instance is started again.
- Digest authentication does not support international characters.
- Basic authentication requires configuration in the proxy server to support international characters.

Learn more about starting a gateway instance in:

- Running a standalone gateway as a Windows service
- Starting a gateway instance as a standalone Java application
- Starting the gateway instance in a Docker container

Running a standalone gateway as a Windows service

You can run the PingOne Lightweight Directory Access Protocol (LDAP) gateway as a standalone Windows service. You'll do this by downloading a `.zip` archive from the PingOne admin console and adding the service to a computer running Windows. This functionality is available in LDAP Gateway version 2.3.0 and later.

Before you begin

- Set up an LDAP gateway. Learn more in Setting up an LDAP gateway
- If you have a valid gateway credential, have it ready. Alternatively, you can create a new credential on the **Overview** tab in the gateway details. Learn more in Creating or deleting a gateway credential.
- Install Java version 17.0.8 or later or Java version 21 LTS or later on the computer that will run the gateway.
- Create a `JAVA_HOME` system environment variable that points to the directory that contains the `bin` directory from the Java distribution.

Directory structure

Most extract utilities will extract the PingOne LDAP gateway software `.zip` archive files to a directory with a pattern of `pingone-ldap-gateway-<version>`. This directory structure is part of the `.zip` archive. For best results, do not rename the `pingone-ldap-gateway-<version>` directory.

The archive extracts the files with the following directory structure:

Parent directory

```
C:\Program Files\Ping Identity
```

LDAP Gateway directory

```
C:\Program Files\Ping Identity\pingone-ldap-gateway-<version>
```

Copyright © 2025 Ping Identity Corporation

`run.properties` *location*

```
C:\Program Files\Ping Identity\pingone-ldap-gateway-<version>\config
```

Batch files location

```
C:\Program Files\Ping Identity\pingone-ldap-gateway-<version>\bin\windows
```

Learn more in:

- Adding the LDAP gateway service
- Removing the LDAP gateway service
- Upgrading the PingOne LDAP Gateway

Adding the LDAP gateway service

Download the `.zip` archive and extract it to the computer that will run the gateway.

Steps

1. In the PingOne admin console, go to **Integrations** > **Gateways** and locate the appropriate gateway.
2. Click the gateway name to expand the gateway details.
3. Click the **Download** tab.
4. In the **Standalone** section, review the prerequisites and instructions.
5. In the **Instructions** section, click the download link for the gateway bundle.

   > **Note**
   >
   > If prompted, complete the sign-on process.

   Result:

   The download begins.

6. Extract the `.zip` archive to the computer that will run the gateway.

   We recommend that you use a common location as the parent directory, such as `C:\Program Files\Ping Identity`.

7. Follow the instructions in the `README.txt` file to:

   1. Configure the `run.properties` file, including providing the gateway credential information.

      The `run.properties` file is located in the `config` directory. For example, `C:\Program Files\Ping Identity\pingone-ldap-gateway-2.3.0\config`.

   2. (Optional) To configure an LDAP Gateway client application to use a forward web proxy server to handle traffic between the gateway and PingOne, in the `run.properties` file provide the relevant access information.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> - To add the web proxy details after installing the LDAP gateway client application as a Windows service, update the `run.properties` file, and then run the `bin/windows/reinstall-service.bat` file using an account with administrator privileges.
> - You must also configure the web proxy settings locally per each running instance. For example, if you're running two gateway client applications, you must configure web proxy settings in both instances.
> - Digest authentication does not support international characters.
> - Basic authentication requires configuration in the proxy server to support international characters.

8. Sign on to Windows with administrator privileges.
9. Start a command prompt or PowerShell.
10. Run the `install-service.bat` file without any parameters.

    By design, the `install-service.bat` file does not start the service automatically after completion. However, the service is configured to start automatically at the next and subsequent restarts of the Windows operating system.
11. In the Services system application, start the PingOne LDAP Gateway service.

Removing the LDAP gateway service

Use the following information to remove the PingOne LDAP Gateway service.

Steps

1. Sign on to Windows with administrator privileges.
2. Start the Services system application and stop the PingOne LDAP Gateway service.
3. Locate the `uninstall-service.bat` file.
    1. In the Services system application, locate the LDAP Gateway service.
    2. Right-click and select **Properties**.
    3. Note the **Path to executable** value.

       For example, if the value is

       `C:\Program Files\Ping Identity\pingone-ldap-gateway-2.3.0\bin\windows\ldap-gateway-windows-x86-64.exe -s C:\Program Files\Ping Identity\pingone-ldap-gateway-2.3.0\bin\windows\PingOneLdapGatewayService.conf`

       then you can find the `uninstall-service.bat` file in the `C:\Program Files\Ping Identity\pingone-ldap-gateway-2.3.0\bin\windows` directory.
4. Run the `uninstall-service.bat` file without any parameters. The underlying directories and files are not removed. Make backup copies and remove the files as needed.

Upgrading the PingOne LDAP Gateway

Copyright © 2025 Ping Identity Corporation

Use the following information to update the PingOne LDAP Gateway, such as from version 2.3.0 to version 2.3.1. You'll uninstall the old version before installing the new one.

Steps

1. In the PingOne admin console, go to **Integrations → Gateways**.
2. Click the appropriate gateway entry to open the details panel.
3. Click the **Download** tab.
4. Click the download link to download the ZIP archive for version 2.3.1.
5. Extract the ZIP archive to the computer that will run the gateway.

   We recommend that you use a common location as the parent directory, such as `C:\Program Files\Ping Identity`.
6. Configure the `run.properties` file, including providing the gateway credential information.

   The `run.properties` file is located in the `config` directory. For example: `C:\Program Files\Ping Identity\pingone-ldap-gateway-2.3.1\config`.
7. Uninstall the old version of the gateway before installing the new one.
   1. Start the Services system application and find the LDAP Gateway 2.3.0 service.
   2. Right-click and select **Properties**.
   3. Note the **Path to executable** value.

      For example, if the value is `C:\Program Files\Ping Identity\pingone-ldap-gateway-2.3.0\bin\windows\ldap-gateway-windows-x86-64.exe -s C:\Program Files\Ping Identity\pingone-ldap-gateway-2.3.0\bin\windows\PingOneLdapGatewayService.conf`

      then you can find the `uninstall-service.bat` file in the `C:\Program Files\Ping Identity\pingone-ldap-gateway-2.3.0\bin\windows` directory.
   4. **Optional:** Start the Services system application and stop the LDAP Gateway 2.3.0 service.
   5. Run the `uninstall-service.bat` file for the LDAP Gateway 2.3.0 service, without any parameters. The underlying directories and files are not removed. Make backup copies and remove the files as needed.
8. After you have uninstalled the old version, you can finish installing the new one.
   1. Locate the `install-service.bat` file for the LDAP Gateway 2.3.1 service.
   2. Run the `install-service.bat` file without any parameters.

      By design, the `install-service.bat` file does not start the service automatically after completion. However, the service is configured to start automatically at the next and subsequent restarts of the Windows operating system.
   3. In the Services system application, start the new PingOne LDAP Gateway 2.3.1 service.

Copyright © 2025 Ping Identity Corporation

Starting a gateway instance as a standalone Java application

Download a gateway bundle and run it on a local computer as a Java application.

Before you begin

- If you have a valid gateway credential, have it ready. Alternatively, you can create a new credential on the Overview tab in the gateway details. Learn more in Creating or deleting a gateway credential.
- Install Java version 17.0.8 or later or Java version 21 LTS or later on the computer that will run the gateway.
- Create a JAVA_HOME system environment variable that points to the directory that contains the bin directory from the Java distribution.

About this task

Run the application on a computer that can reach your LDAP directory and PingOne.

Steps

1. Go to **Integrations → Gateways** and locate the appropriate gateway.
2. Click the gateway name to expand the gateway details.
3. Click the **Download** tab.
4. In the **Standalone** section, review the prerequisites and instructions.
5. In the **Instructions** section, click the download link for the gateway bundle.

   > **Note**
   >
   > **If promted, complete the sign-on process.**

   Result:

   The download begins

6. Follow the instructions in the `README.txt` file to configure the `run.properties` file, including providing the gateway credential information.
7. Optional: To configure an LDAP Gateway client application to use a forward web proxy server to handle traffic between the gateway and PingOne, provide access information into the `run.properties` file.

   > **Note**
   >
   > - You must configure the web proxy settings locally per each running instance. For example, if you're running two gateway client applications, you must configure web proxy settings in both instances.
   > - Digest authentication does not support international characters.
   > - Basic authentication requires configuration in the proxy server to support international characters.

8. Sign on to the computer with administrator privileges.
9. At a command prompt, run the `bin\run.bat` file for Windows or the `bin/run.sh` file for Linux.

Copyright © 2025 Ping Identity Corporation

Next steps

Verify a gateway instance

Starting the gateway instance in a Docker container

About this task

Use the Docker command that you copied from PingOne to start a Docker container. Run the Docker container on a computer that can reach your LDAP directory and PingOne.

Before you begin

- If you have a valid gateway credential, have it ready. Alternatively, you can create a new credential on the **Overview** tab in the gateway details. Learn more in Creating or deleting a gateway credential
- Ensure that Docker is installed and the Docker Engine is running.

Steps

1. In the PingOne admin console, go to **Integrations → Gateways** and locate the appropriate gateway.
2. Click the gateway name to expand the gateway details.
3. Click the **Download** tab.
4. In the **Standalone** section, review the prerequisites and instructions.
5. In the **Instructions** section, copy the Docker command and paste it into a file or the command prompt.
6. If you agree to the terms of the license agreement, open the Docker command in a text editor and change `-e PING_IDENTITY_ACCEPT_EULA=no` to `-e PING_IDENTITY_ACCEPT_EULA=yes`.
7. Optional: To configure an LDAP Gateway client application to use a forward web proxy server to handle traffic between the gateway and PingOne, add access information to the Docker command.
   - `-e http_proxyHost=<HTTP_PROXY_HOST>`
   - `-e http_proxyPort=<HTTP_PROXY_PORT>`
   - `-e http_proxyUser=<HTTP_PROXY_USER>`
   - `-e http_proxyPassword=<HTTP_PROXY_PASSWORD>`
   - `-e http_proxyAuthenticationMethod=DIGEST (or BASIC)`

     `http_proxyHost` and `http_proxyPort` are required to use a web proxy. `http_proxyUser`, `http_proxyPassword`, and `http_proxyAuthenticationMethod` are required if the web proxy requires authentication.

Copyright © 2025 Ping Identity Corporation

> **Important**
>
> For `http_proxyAuthenticationMethod`, it's worth noting that BASIC (as in basic authentication) transmits access credentials without encryption. You should use DIGEST (as in digest authentication) because it uses a challenge-response mechanism and does not send the password in plain text.

> **Note**
>
> - You must configure the web proxy settings per each running instance. For example, if you're running two gateway client applications, you must configure web proxy settings in both instances.
> - Digest authentication does not support international characters.
> - Basic authentication requires configuration in the proxy server to support international characters.

8. At a command prompt, run the Docker command.

Next steps

Verify a gateway instance

Verifying a gateway instance

After you start the gateway instance, ensure that the gateway can connect to PingOne.

Steps

1. Go to **Integrations → Gateways**.
2. Locate the appropriate gateway.

> **Note**
>
> You can refresh the **Gateways** page to ensure that the information is current.

3. Review the gateway details to ensure that the gateway instance is healthy.

Configuring multiple gateway instances

For high-availability applications or scalability, you can configure multiple gateway instances. You can then run the Windows service, Docker container, or Java application on multiple servers.

When multiple gateway instances are connected to PingOne, PingOne maintains a list of the active gateway instances connection. PingOne will load balance based on each connection with lower load and latency. If a gateway instance is not available, it is excluded from the list of active gateway instances.

You can set up one PingOne gateway with one gateway credential, with multiple gateway instances that share the same credential. If needed, you can remove the credential from the PingOne gateway to stop all gateway traffic.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> We recommend that you use a different credential for each gateway instance. Using different credentials allows you to easily revoke access to individual gateway instances.

Creating or deleting a gateway credential

PingOne automatically creates a gateway credential when you add a gateway, but you can create additional credentials at any time. You can also delete a gateway credential.

About this task

> **Important**
>
> For optimal security, you should rotate gateway credentials periodically.

Steps

1. In the PingOne admin console, go to **Integrations** > **Gateways**.
2. To add a gateway credential:
    1. Click the appropriate gateway to display gateway details.
    2. On the **Overview** tab, click the **+** icon next to **Gateway credentials**.
    3. Verify that the credential was created and copy it to a secure location.

    > **Important**
    >
    > The credential is shown in the console only once. If necessary, you can retrieve existing credentials through the `Gateway Management API`. Learn more in Gateway Management in the PingOne Platform API Reference.

    4. Click **Done**.

    Result:

    The new credential is added to the list with a unique ID.
3. To delete a gateway credential:
    1. On the **Gateways** page, click the gateway that has the credential you want to delete.
    2. On the **Overview** tab, click the **Delete** icon (🗑) icon next to the credential.
    3. Select the **I understand and want to continue** checkbox.
    4. Click **Revoke**.

    After a credential is revoked, the gateway cannot use the credential to access PingOne.

Copyright © 2025 Ping Identity Corporation

Creating an authentication policy that uses the gateway

You can create or edit an authentication policy that end users use to sign on to PingOne. Learn more about authentication policies in Adding an authentication policy.

About this task

You can use an Lightweight Directory Access Protocol (LDAP) gateway to authenticate and authorize user identities stored in an external directory. You can then create an authentication policy that uses the gateway to migrate new users the first time they sign on.

An authentication policy with an added gateway with Kerberos configuration enables seamless single sign-on (SSO). If PingOne can't authenticate users through the Kerberos protocol, it presents users with a sign-on form. Learn more in Kerberos authentication.

Before you begin

- Set up an LDAP gateway with a user type configured. To enable seamless SSO authentication experience using the Kerberos protocol, enable Kerberos authentication in your LDAP gateway. Learn more in Setting up an LDAP gateway.
- Enable migration of new users in your gateway's user type. Learn more in Adding a user type.

Steps

1. In the PingOne admin console, go to **Authentication > Authentication** and search for an existing authentication policy or create a new one.
2. Click the **Details** icon to expand the policy, and then click the **Pencil** icon.
3. On a **Login** policy step, in the **Migrate Gateway Users Upon First Authentication** section, click **+ Add gateway user type**.
4. Enter the following:
   - **Gateway**: Select the gateway that connects to the external directory.
   - **User type**: Select the user type that authenticates with the external gateway through which PingOne finds the user to complete the authentication process.

   > **Note**
   > You can add multiple gateway and user-type configurations. PingOne validates user credentials against them sequentially.
   > You should add an multi-factor authentication (MFA) step to increase security. Learn more in Adding a multi-factor authentication or PingID step.

   > **Important**
   > You can only add user types where the **Migrate Gateway Users Upon First Authentication** option is enabled. After saving the authentication policy, don't remove the migration option from the selected user types as this policy configuration becomes uneditable until the migration option is re-enabled in those user types.

5. Click **Save**.

Next steps

Copyright © 2025 Ping Identity Corporation

Adding the authentication policy to an application

Adding the authentication policy to an application

Associate the authentication policy with an application so that users accessing the application will use the specified authentication policy. For more information, see Authentication policies for applications.

Steps

1. Go to **Applications → Applications**.
2. Locate the application you want to edit by browsing or searching for it.
3. Click the application entry to open the **Details** panel.
4. Click the **Policies** tab, and then click the **Pencil** icon.
5. Select the check box for the authentication policy that you want to apply for the application.

   The policies are applied in the order in which they appear in the list. PingOne evaluates the first policy in the list first. If the requirements of the policy are not met, PingOne moves to the next policy in the list.
6. Click **Save**.

Kerberos authentication

If you are using Microsoft Active Directory as your Lightweight Directory Access Protocol (LDAP) user store, you can use Kerberos for authentication. PingOne will authenticate users against the Active Directory user store using the Kerberos authentication protocol.

> **Note**
>
> Because Microsoft Active Directory is the only directory that supports Kerberos for authentication, when you add the gateway connection, select **Microsoft Active Directory** for **Directory type**. Learn more in Adding an LDAP gateway.

Known limitations

When an Active Directory user is a member of a large number of groups, they might receive a `413 Request Entity Too Large` response during Kerberos authentication. As a user is added to more groups, the size of the Kerberos ticket increases and can exceed the limitations of the PingOne infrastructure.

To resolve this:

- Remove the user from extraneous groups.
- Fallback to sign on with username and password when Kerberos fails.

Copyright © 2025 Ping Identity Corporation

End user authentication flow

With Kerberos authentication properly configured, the end user authentication flow behaves as follows:

- First, PingOne tries to authenticate the end user through Kerberos. This is a seamless experience and requires no user interaction.

  If Kerberos authentication succeeds, the login step is complete.

- If the authentication policy has an multi-factor authentication (MFA) step, the end user proceeds to MFA. When the end user completes all steps, PingOne redirects the browser to the target application.

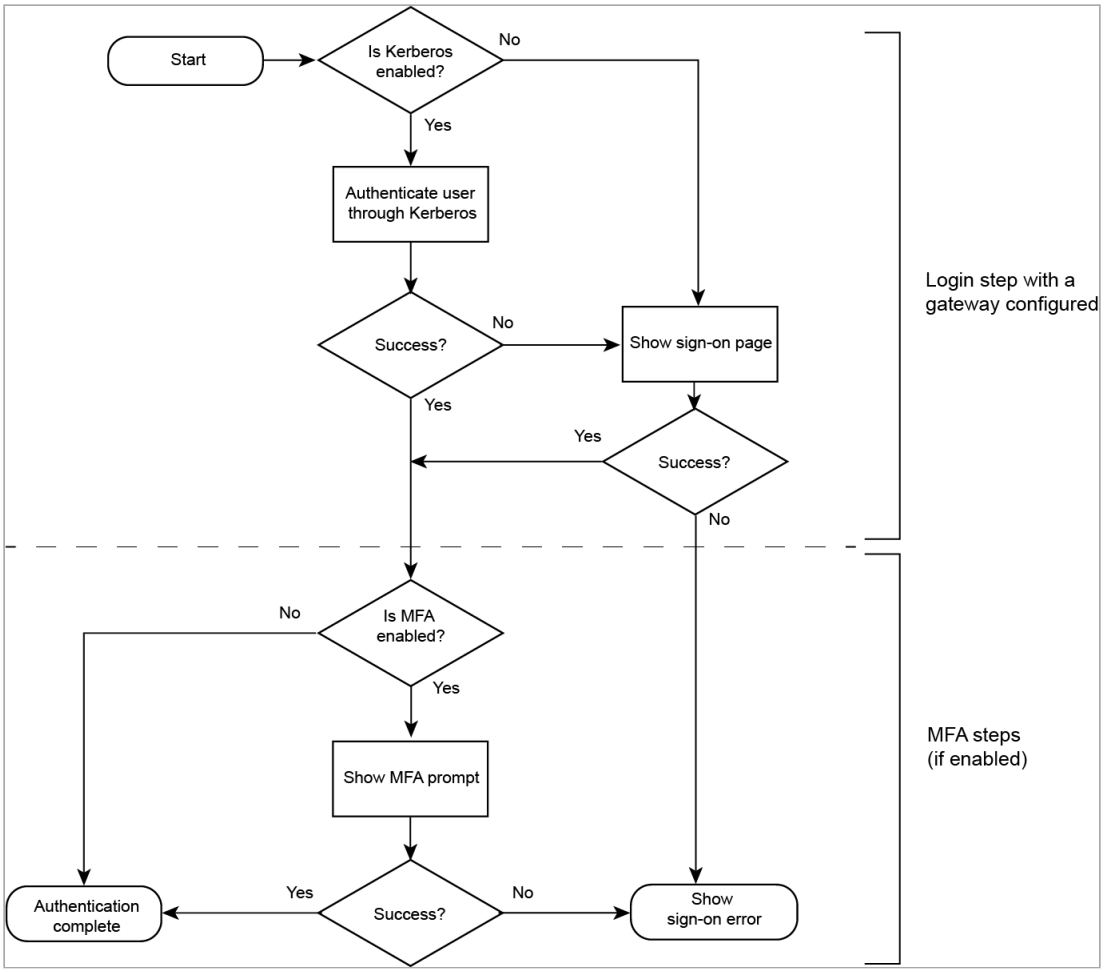
- If Kerberos authentication fails, PingOne tries to authenticate the end user by showing the sign-on page with user name and password fields.

  If the end user provides the correct credentials, the login step is complete.

- If the authentication policy has an MFA step, the end user will proceed to MFA. When the end user completes all steps, PingOne redirects the browser to the target application.

- If the end user fails to provide the correct credentials, PingOne returns a sign-on error to the browser.

The following illustration shows the authentication flow.



Creating SPNs

To enable Kerberos authentication, you must configure two service principal names (SPNs).

About this task

An SPN is a unique identifier of a service instance. SPNs are used by Kerberos to associate a service with a domain.

Use the Windows utility `setspn` to configure two SPNs for each PingOne region. To find the SPNs for various PingOne regions, see SPN reference.

> **Note**
> You can also use ADSI Edit to configure the SPN values.

The purpose of two SPNs is future proofing. Ping Identity will migrate its infrastructure in the coming months. Adding the second `HTTP/kerberos.pingone.com` SPN ensures that your configuration will continue to work after the migration.

Steps

1. On the domain controller, open a command prompt as an administrator.
2. Enter the following command `setspn -S HTTP/<regionalPingOneaddress> <sAMAccountName>`

   where `<regionalPingOneaddress>` is the SPN you want to add and `<sAMAccountName>` is the service account name that you want to update.

   > **Note**
   > When you run the `setspn` command, you must capitalize `HTTP` and follow it with a forward slash (`/`).
   > For example, `setspn -S HTTP/d3vol3lyj0eg62.cloudfront.net ping-one-kerberos-svc-account`
   > To find the SPNs for the different PingOne regions, or if you're using custom domains, see SPN reference.

SPN reference

The following table shows the service principal name (SPN) values for the various PingOne regions.

Region	SPN 1	SPN 2
Australia	HTTP/d17e9v8kuwbj1g.cloudfront.net	HTTP/kerberos.pingone.com.au
Canada	HTTP/d2zesjvkk5mc9z.cloudfront.net	HTTP/kerberos.pingone.ca
Europe	HTTP/d2g9q8z5merlnu.cloudfront.net	HTTP/kerberos.pingone.eu
North America (US)	HTTP/d3vol3lyj0eg62.cloudfront.net	HTTP/kerberos.pingone.com
Singapore	HTTP/dcfgtxahv7i2c.cloudfront.net	HTTP/kerberose.pingone.sg

Copyright © 2025 Ping Identity Corporation

Region	SPN 1	SPN 2
Asia Pacific (legacy) **Note** Available only for existing .asia customers.	HTTP/d17e9v8kuwbj1g.cloudfront.net	HTTP/kerberos.pingone.asia

Custom domains

If the environment is configured with a custom domain, only one SPN is required. The address varies depending on the DNS result. See the examples below for more information.

CloudFront examples

Example 1: DNS result from nslookup

```
c:\>nslookup -type=A sso.example.com
Step 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa
        primary name server = 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa
        responsible mail addr = (root)
        serial  = 0
        refresh = 28800 (8 hours)
        retry   = 7200 (2 hours)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
Server:  UnKnown
Address:  ::1Non-authoritative answer:
Name:    d3laihe2ro8a3z.cloudfront.net
Addresses:  65.8.10.10
          65.8.10.20
          65.8.10.30
          65.8.10.40
Aliases:  sso.example.com
          45ffcbe6-ec42-48d2-999e-89a7eae22ea9.edge1.pingone.com
```

Based on this DNS result from `nslookup`, in CloudFront the SPN address is `HTTP/d3laihe2ro8a3z.cloudfront.net`. This remains true regardless of the PingOne region.

Copyright © 2025 Ping Identity Corporation

Example 2: DNS result from dig

```
~$ dig sso.example.com A

; <<>> DiG 9.10.6 <<>> sso.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1344
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sso.example.com.        IN    A

;; ANSWER SECTION:
sso.example.com.    3526    IN    CNAME    45ffcbe6-ec42-48d2-999e-89a7eae22ea9.edge1.pingone.com.
45ffcbe6-ec42-48d2-999e-89a7eae22ea9.edge1.pingone.com.    86326 IN CNAME d3laihe2ro8a3z.cloudfront.net.
d3laihe2ro8a3z.cloudfront.net. 54 IN    A    65.8.10.10
d3laihe2ro8a3z.cloudfront.net. 54 IN    A    65.8.10.20
d3laihe2ro8a3z.cloudfront.net. 54 IN    A    65.8.10.30
d3laihe2ro8a3z.cloudfront.net. 54 IN    A    65.8.10.40

;; Query time: 30 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Fri Nov 25 14:02:32 PST 2022
;; MSG SIZE  rcvd: 221
```

Based on this DNS result from `dig`, in CloudFront the SPN address is `HTTP/d3laihe2ro8a3z.cloudfront.net`. This remains true regardless of the PingOne region.

Cloudflare examples

Example 1: DNS result from nslookup

```
c:\>nslookup -type=A sso.example.com
Server:  127.0.0.1
Address:  127.0.0.1#53

Non-authoritative answer:
sso.example.com canonical name = f97e2bbf-6680-44b6-a2cf-97aa0b4a4226.edge1.test-one-pingone.com.
f97e2bbf-6680-44b6-a2cf-97aa0b4a4226.edge1.pingone.com  canonical name =
92b8af3f-0d5b-4cc8-8460-8a35a26efc5e.ping-ccd.com.
Name:    92b8af3f-0d5b-4cc8-8460-8a35a26efc5e.ping-ccd.com
Address:  130.250.137.31
```

Based on this DNS result from `nslookup`, in Cloudflare the SPN address is `HTTP/92b8af3f-0d5b-4cc8-8460-8a35a26efc5e.ping-ccd.com`.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> This example assumes the organization resides in the North America (US) region. If your organization is in a different region, the end of the SPN would differ depending on that region:
>
> - North America (Canada): `ping-ccd.ca`
> - Europe: `ping-ccd.eu`
> - Australia: `ping-ccd.com.au`
> - Asia-Pacific: `ping-ccd.asia`
> - Singapore: `ping-ccd.sg`

Example 2: DNS result from dig

```
~$ dig sso.example.com A

; <<>> DiG 9.10.6 <<>> sso.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21003
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;sso.example.com.        IN    A

;; ANSWER SECTION:
sso.example.com.    98    IN    CNAME    f97e2bbf-6680-44b6-a2cf-97aa0b4a4226.pingone.com.
f97e2bbf-6680-44b6-a2cf-97aa0b4a4226.pingone.com.    86198 IN CNAME
92b8af3f-0d5b-4cc8-8460-8a35a26efc5e.ping-ccd.com.
92b8af3f-0d5b-4cc8-8460-8a35a26efc5e.ping-ccd.com. 98 IN    A    130.250.137.31

;; Query time: 31 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Jun 23 10:26:50 PDT 2025
;; MSG SIZE  rcvd: 361
```

Based on this DNS result from `dig`, in Cloudflare the SPN address is `HTTP/92b8af3f-0d5b-4cc8-8460-8a35a26efc5e.ping-ccd.com`.

> **Note**
>
> This example assumes the organization resides in the North America (US) region. If your organization is in a different region, the end of the SPN would differ depending on that region:
>
> - North America (Canada): `ping-ccd.ca`
> - Europe: `ping-ccd.eu`
> - Australia: `ping-ccd.com.au`
> - Asia-Pacific: `ping-ccd.asia`
> - Singapore: `ping-ccd.sg`

Copyright © 2025 Ping Identity Corporation

Configuring end user browsers

To support Kerberos authentication, you must add two trusted URIs to end user browsers.

The purpose of two URIs is future proofing. Ping Identity will migrate its infrastructure in the coming months. Adding the second URI ensures that your configuration will continue to work after the migration.

Custom domains

If the environment is configured with a custom domain, `auth.pingone.com` and `kerberos.pingone.com` are irrelevant. Instead, add the custom domain as the trusted URI.

Browser URI reference

When configuring end user browsers, use the following trusted URI values for the various PingOne regions.

Region	URI 1	URI 2
Australia	auth.pingone.com.au	kerberos.pingone.com.au
Canada	auth.pingone.ca	kerberos.pingone.ca
Europe	auth.pingone.eu	kerberos.pingone.eu
North America (US)	auth.pingone.com	kerberos.pingone.com
Singapore	auth.pingone.sg	kerberos.pingone.sg
Asia Pacific (legacy) **Note** Available only for existing .asia customers.	auth.pingone.asia	kerberos.pingone.asia

Configuring Mozilla Firefox

Configure Kerberos authentication for the Firefox browser.

Copyright © 2025 Ping Identity Corporation

Steps

1. Start the Firefox browser.
2. In the address bar, enter `about:config`.
3. If you are presented with a security warning, click **Accept the risk and continue**.
4. In the **Search** field, enter `network.negotiate-auth.trusted-uris` and then click the pencil icon.
5. Do one of the following:
   - If the environment is not configured with a custom domain, enter the two trusted addresses separated by a comma, and then click the check mark icon.
   - If the environment is configured with a custom domain, enter the custom domain and then click the check mark icon.

     For more information about the trusted URI values, see Configuring end user browsers.

Configuring Microsoft Edge

Ensure that the Microsoft Edge browser on the end user's system is configured to support Kerberos authentication. Use the Group Policy Management Editor to configure the browser.

Before you begin

To use the administrative template for Microsoft Edge, download it from the Microsoft website. For more information, see Configure Microsoft Edge policy settings.

Steps

1. Start the Group Policy Management Editor from Windows Administrative Tools.
2. Go to **Administrative Templates → Windows Components → Microsoft Edge → Internet Control Panel → Security Page → Site to Zone Assignment List → Show Contents**.
3. Do one of the following:
   - If the environment is not configured with a custom domain, in the **Show Contents** window, for **Value Name**, enter the first trusted address, and in the **Value** column, enter `1`. Enter the second trusted address, and in the **Value** column, enter `1`. Click **OK**. For more information about the trusted URI values, see Configuring end user browsers.
   - If the environment is configured with a custom domain, in the **Show Contents** window, for **Value Name**, enter the custom domain, and in the **Value** column, enter `1`. Click **OK**. For more information about the trusted URI values, see Configuring end user browsers.
4. Configure the Internet Zone options.

Copyright © 2025 Ping Identity Corporation

> **Note**
> The path to the Microsoft Edge settings can vary depending on your version of Windows.

1. Go to **User Configuration → Administrative Templates → Windows Components → Microsoft Edge → Internet Control Panel → Security Page → Internet Zone → Logon options**.
2. In the **Logon Options** window, for the **Logon options** list, select **Automatic logon with current user name and password**. Click **OK**.

5. Configure the Intranet Zone options.
   1. Go to **User Configuration → Administrative Templates → Windows Components → Microsoft Edge → Internet Control Panel → Security Page → Intranet Zone → Logon options**.
   2. In the **Logon Options** window, in the **Logon options** list, select **Automatic logon with current user name and password**. Click **OK**.

Configuring Google Chrome

Configure Kerberos authentication for the Google Chrome browser.

About this task

On Windows, Google Chrome uses the same configuration values as Microsoft Edge. For more information, see Configuring Microsoft Edge.

Retaining credentials

To ensure that end users can continue to authenticate through Kerberos if the service account password is changed, you can configure PingOne to retain the previous credentials for the service account for the specified time period.

Steps

1. Go to **Integrations → Gateways**.
2. Select the applicable gateway configuration.
3. Click the **Connection** tab and then click **Edit**.
4. Select the **Retain Previous Credentials** checkbox.
5. For **Retention Duration (Minutes)**, specify how long to keep the previous credentials, in minutes. The default value is 610. You can enter any value between 1 and 10,080.
6. Enter a new password into the **Service Account Password** field.
7. Click **Save**.

Copyright © 2025 Ping Identity Corporation

8. Ask the Active Directory admin to update the service account password in Active Directory. Shortly after the AD admin updates the password in AD, the INFO alert disappears from the PingOne admin console.

Clearing credentials

If you suspect that your credentials are out of date or compromised, you can clear all previously retained service account credentials.

Steps

1. Go to **Integrations → Gateways**.
2. Select the applicable gateway configuration.
3. Click the **Connection** tab and then click **Edit**.
4. Clear the **Retain Previous Credentials** checkbox.
5. Enter a new password into the **Service Account Password** field.
6. Click **Save**.
7. Ask the Active Directory admin to update the service account password in Active Directory. Shortly after the AD admin updates the password in AD, the INFO alert disappears from the PingOne admin console.

Manually migrating users to PingOne

If you have configured an Lightweight Directory Access Protocol (LDAP) gateway, you can use the PingOne API to programmatically provision users from the external LDAP directory.

About this task

Use the `POST CREATE User Import External Password` method with the relevant external password information.

Learn more in POST CREATE User Import External Password in the PingOne API documentation.

Troubleshooting an LDAP gateway instance

If the gateway instance is not healthy, use the information in this section to troubleshoot any issues.

The following information applies to the various gateway deployment scenarios. You can use the gateway details page, gateway logs, or Splunk reports to identify issues. Learn more in Verifying a gateway instance and Monitoring activity with Splunk.

I want to view the gateway application logs

You can view gateway client application logs to get detailed information about the gateway and the responses from your LDAP server. The method to do so varies depending on your gateway configuration.

Gateway as a standalone service

By default, log files are saved to the `./logs` directory on the computer running the gateway. Log files roll over by date.

Copyright © 2025 Ping Identity Corporation

To view the logs, go to the `./logs` directory. The logs are named `GatewayStandalone.yyyymmdd.log`

Gateway as a Windows service

By default, log files are saved to the `./logs` directory on the computer running the gateway. Log files roll over by date.

To view the logs, go to the `./logs` directory. The logs are named:

- `GatewayService.yyyymmdd.log`
- `GatewayWrapper.yyyymmdd.log`

> **Note**
> The `GatewayWrapper.yyyymmdd.log` file mirrors the console output of the standalone version, with additional logs.

Gateway as a Docker container

To view logs for a Docker container, run the following command:

```
docker logs _<container ID or name>_
```

My logs aren't showing enough information

You can enable verbose logging to get more detailed logs about the gateway and the responses from your LDAP server. The method to do so varies depending on your gateway configuration.

> **Note**
> The following steps were validated with PingOne LDAP Gateway client application version 2.3.3.

Gateway as a standalone service

By default, the log level is set to `INFO`, which includes errors and general information for the service. For more verbose logs, set the log level to `DEBUG`, which includes all possible information for the service.

1. If the PingOne LDAP Gateway service is running, stop it.
2. Locate the `./config/run.properties` file.
3. Locate the `LOG_LEVEL` parameter.
4. Change the parameter to `LOG_LEVEL=DEBUG`.
5. Restart the PingOne LDAP Gateway service.

You can also change the formatting of the console output.

1. If the PingOne LDAP Gateway service is running, stop it.
2. Locate the `./config/logback.xml` file.
3. Follow the instructions in the file to enable more detailed logs in the console.

Copyright © 2025 Ping Identity Corporation

4. Restart the PingOne LDAP Gateway service.

Gateway as a Windows service

Use the `LOG_LEVEL` parameter to configure the logging settings. By default, the log level is set to `INFO`, which includes errors and general information for the service. For more verbose logs, set the log level to `DEBUG`, which includes all possible information for the service.

1. Locate the `./config/run.properties` file.
2. Locate the `LOG_LEVEL` parameter.
3. Change the parameter to `LOG_LEVEL=DEBUG`.
4. Run `./bin/windows/reinstall-service.bat`.
5. Press the Windows + R keys.
6. Enter `services.msc` to open the Windows Services Controller.
7. Locate the PingOne LDAP Gateway service and start it.

The Ping Identity Gateway console opens and shows detailed logs.

Gateway as a Docker container

Use the `Dlogger.console.level` and `LOG_LEVEL` parameters to configure the logging settings.

Use the following Docker run command:

```
-e JAVA_OPTS="-Dlogger.console.level=DEBUG" -e LOG_LEVEL=DEBUG
```

> **Note**
> You can also use Splunk to monitor a gateway connection. Learn more in Monitoring activity with Splunk.

My connection is taking too long to resolve

If your connection is taking a long time, check the following:

- If the connection is configured with a string host name, try using an IP address instead.
- On the server that you want to connect to, ensure that the desired port is open.
- Ensure there aren't any routing issues in your infrastructure that could affect the ability of the gateway server to reach the LDAP server or Remote Authentication Dial-In User Service (RADIUS) client.
- Sometimes it can take several seconds for the connection information to be updated in the console user interface. Try refreshing the page to get the most current information.

I want to increase scalability

For high-availability applications or scalability, you can deploy multiple gateway instances. You can then run the Windows service, Docker container, or Java application on multiple servers.

Copyright © 2025 Ping Identity Corporation

When multiple gateway instances are connected to PingOne, PingOne maintains a list of the active gateway instance connection. PingOne will load balance based on each connection's current load, prioritizing sending traffic to the connections with lower load and latency. If a gateway instance is not available, it is excluded from the list of active gateway instances.

> **Note**
>
> Use a different credential for each deployed gateway instance. Using different credentials allows you to easily revoke access to individual gateway instances.

I'm getting a PKIX path building failed error

For LDAP gateway connections with provisioning, you might see the following error if the gateway connection is interrupted:

```
PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid
certification path to requested target
```

If this error occurs, check the following:

- Ensure that the LDAPS certificate was imported into PingOne correctly. Learn more in Importing an LDAP certificate to PingOne.

  1. Go to **Integrations → Gateways**, and click the gateway to open the details panel.
  2. Click the **Connections** tab, and then click **Edit**.
  3. Click the **Allow TLS connections with untrusted certifications** checkbox.
  4. Click **Save**.
  5. Re-test authentication.

  If authentication is successful when the gateway is set to ignore the LDAPS certificate, this confirms that there's an issue with the certificate that the LDAP server is presenting.

- Verify that traffic between the gateway and auth.pingone.com and api.pingone.com is uninterrupted (such as by proxies, firewalls, or SSL inspection). Learn more in Before configuring an LDAP gateway.

I'm getting a TSL certificate is not trusted error

When an LDAP gateway connects to an on-prem LDAP directory server, it establishes a secure connection using TLS, which encrypts traffic using a cipher suite.

The following possible errors can occur when there is a Cipher Suite mismatch, and the connection cannot be established:

```
The TLS certificate is not trusted. Attempting to reconnect. Please check the logs for more details or
visit https://www.pingidentity.com/en/permalinks/p1gateway-troubleshooting.html for more troubleshooting
help.
```

```
An error occurred while attempting to connect to server ldap.example.com:636:
IOException(LDAPException(resultCode=91 (connect error), errorMessage='An error occurred while attempting
to establish a connection to server ldap.example.com/<ipaddress>:636:SocketException(Connection reset)
```


Copyright © 2025 Ping Identity Corporation

```
An error occurred while attempting to connect to server ldap.example.com:636:
IOException(LDAPException(resultCode=91 (connect error), errorMessage='An error occurred while attempting
to establish a connection to server ldap.example.com/<ipaddress>:636:SSLHandshakeException(Received fatal
alert: handshake_failure)
```

If you get any of these errors, use the following steps:

1. Check the gateway client logs for a `HANDSHAKE_FAILURE` error and determine which cipher suites are supported by the LDAP server.
2. From the terminal, run the following command and replace ldap.example.com with the FQDN of your LDAP server:

   ```
   openssl s_client -showcerts ldap.example.com:636
   ```

   This gives you an output of the SSL-Session, including a TLS version and cipher value, such as ECDHE-RSA-AES256-GCM-SHA384
3. In Translating OpenSSL cipher suite names to IANA, find the correct IANA cipher suite name that matches the openssl cipher name.
4. Stop the gateway client if it is running.
5. Choose:
   - For Windows service:
     1. In `bin/windows/PingOneLdapGatewayService.conf`, in the `# Java additional parameters` section, add the following line:

        ```
        wrapper.java.additional.14=-
        Dcom.unboundid.util.SSLUtil.enabledSSLCipherSuites=<cipher suite>
        ```

     2. Re-install the Windows service.
   - For standalone Java:
     1. On Windows, add the following line to the Java command at the bottom of `run.bat`:

        ```
        -Dcom.unboundid.util.SSLUtil.enabledSSLCipherSuites=<cipher suite> ^
        ```

     2. On Linux or MacOS, add the following line to the Java command at the bottom of `run.sh`:

        ```
        -Dcom.unboundid.util.SSLUtil.enabledSSLCipherSuites=<cipher suite> /
        ```
   - For Docker:
     1. Add `e JAVA_OPS="-Dcom.unboundid.util.SSLUtil.enabledSSLCipherSuites=<cipher suite>"` to the Docker command

Copyright © 2025 Ping Identity Corporation

6. Start the gateway.

Troubleshooting LDAP authentication

Use the information in this section to troubleshoot any LDAP authentication issues.

Users receive an error when signing on or changing their password

A user receives the following error message when signing on or trying to change their password:

```
A system error occurred when accessing your account for authentication. Contact your administrator.
```

If this error occurs, check for the following:

- Check if the user's account needs to be updated in the external Lightweight Directory Access Protocol (LDAP) directory server. If you have an LDAP gateway configured, ensure that it's configured properly.
- If **Update PingOne user attributes as users sign on** is enabled in the PingOne admin console, check the audit logs for any update failures.

I'm getting an Active Directory password modify error

For LDAP gateway connections using Active Directory (AD), you might see password modify errors in your LDAP gateway client logs.

This error can appear as a failure to change a password using a service account in AD. The error appears as either of the following:

```
LDAP password change result requestId=be2f0fb3-a090-4bf5-ab9c-97a9e480f6e3,
resultCode=19 (constraint violation), resultDetails=LDAPResult(resultCode=19 (constraint violation),
diagnosticMessage='00000005: AtrErr: DSID-03191080, #1: 0: 00000005: DSID-03191080, problem 1005
(CONSTRAINT_ATT_TYPE), data 0, Att 9005a (unicodePwd)')
```

```
LDAP password change result requestId=be2f0fb3-a090-4bf5-ab9c-97a9e480f6e3,
resultCode=50 (insufficient access rights), resultDetails=LDAPResult(resultCode=50 (insufficient access
rights),
diagnosticMessage='00000005: SecErr: DSID-031A11B9, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0')
```

Learn more about the recommended configuration for the service account in AD in Best practices for configuring Active Directory for LDAP gateways.

How do I know if a user has entered an incorrect username?

If the LDAP gateway connects to AD, when the provided username cannot locate a user record in AD, look for two DEBUG messages similar to the following samples in the gateway client application log:

Copyright © 2025 Ping Identity Corporation

```
DEBUG 2024-10-10T13:06:30.495Z c.p.l.l.RawLdapSearchesThenOpRequestHandler - Processing
message=rawLdapSearchesThenOpRequest requestId=853ea174-6ccf-475d-9db3-a5f38edde100
searches=[SearchRequest(baseDN='CN=Users,DC=example,DC=local', scope=SUB, deref=NEVER, sizeLimit=0,
timeLimit=0, filter='(|(sAMAccountName=non-existent)(mail=non-existent))', attrs={*, +})]
```

```
DEBUG 2024-10-10T13:06:30.516Z c.p.l.r.internal.SerializationUtils - Search result has entryCount=0
The “non-existent” message and the “Search result has entryCount=0” message indicate the user has entered
an incorrect username (or the user record has been deleted in Active Directory).
```

If the LDAP gateway connects to PingDirectory, similar messages are also recorded to the gateway client application log.

How do I know if a user has entered an incorrect password?

If the LDAP gateway connects to AD, when the provided username is valid but the provided password is not, look for a DEBUG message similar to the following sample in the gateway client application log:

```
WARN  2024-10-11T14:09:25.545Z c.p.l.l.RawLdapSearchesThenOpRequestHandler - Received ldap result for
requestId=a8336c85-6980-4436-82a2-3f2fcdb3c454, resultCode=49 (invalid credentials),
resultDetails=BindResult(resultCode=49 (invalid credentials), messageID=3, diagnosticMessage='80090308:
LdapErr: DSID-0C090569, comment: AcceptSecurityContext error, data 52e, v4563 ',
hasServerSASLCredentials=false)
```

The `resultCode=49` message indicates the user has entered an incorrect password.

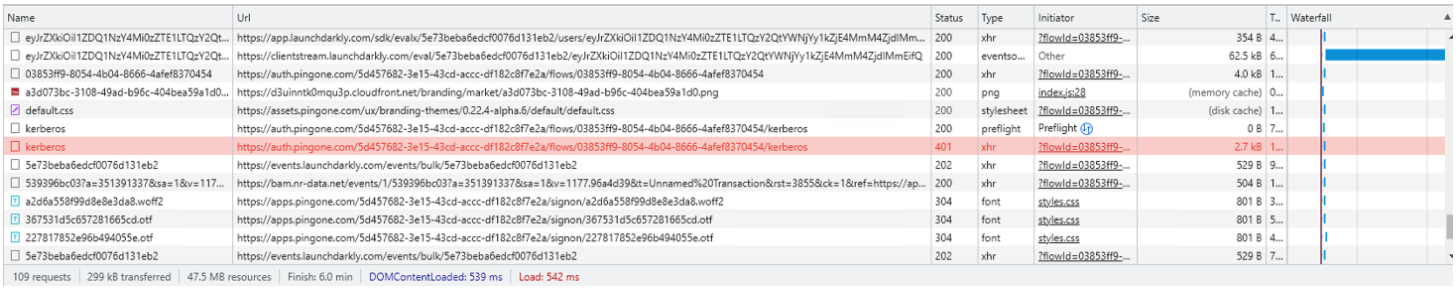
If the LDAP gateway connects to PingDirectory, a similar `resultCode=49` message is also recorded to the gateway client application log.

Troubleshooting Kerberos

I am unable to sign on using Kerberos through the PingOne gateway

If you’ve configured the PingOne gateway to support Kerberos authentication, but you’re still seeing a sign-on screen, check the audit logs for any Kerberos failures.

You can find a complete list of events logged in PingOne in Audit Reporting Events in the PingOne API documentation.



Name	Url	Status	Type	Initiator	Size	T...	Waterfall
eyJrZXkiOiI1ZDQ1NzY4Mi0zZTE1LTQzY2Qt...	https://app.launchdarkly.com/sdk/evalx/5e73beba6edcf0076d131eb2/users/eyJrZXkiOiI1ZDQ1NzY4Mi0zZTE1LTQzY2QtYWNjYy1kZjE4MmM4ZjdlMm...	200	xhr	?flowId=03853ff9-...	354 B	4...	
eyJrZXkiOiI1ZDQ1NzY4Mi0zZTE1LTQzY2Qt...	https://clientstream.launchdarkly.com/eval/5e73beba6edcf0076d131eb2/eyJrZXkiOiI1ZDQ1NzY4Mi0zZTE1LTQzY2QtYWNjYy1kZjE4MmM4ZjdlMmEifQ	200	eventso...	Other	62.5 kB	6...	
03853ff9-8054-4b04-8666-4afef8370454	https://auth.pingone.com/5d457682-3e15-43cd-accc-df182c8f7e2a/flows/03853ff9-8054-4b04-8666-4afef8370454	200	xhr	?flowId=03853ff9-...	4.0 kB	1...	
a3d073bc-3108-49ad-b96c-404bea59a1d0...	https://d3uinntk0mqu3p.cloudfront.net/branding/market/a3d073bc-3108-49ad-b96c-404bea59a1d0.png	200	png	index.js:28	(memory cache)	0...	
default.css	https://assets.pingone.com/ux/branding-themes/0.22.4-alpha.6/default/default.css	200	stylesheet	?flowId=03853ff9-...	(disk cache)	1...	
kerberos	https://auth.pingone.com/5d457682-3e15-43cd-accc-df182c8f7e2a/flows/03853ff9-8054-4b04-8666-4afef8370454/kerberos	200	preflight	Preflight	0 B	7...	
kerberos	https://auth.pingone.com/5d457682-3e15-43cd-accc-df182c8f7e2a/flows/03853ff9-8054-4b04-8666-4afef8370454/kerberos	401	xhr	?flowId=03853ff9-...	2.7 kB	1...	
5e73beba6edcf0076d131eb2	https://events.launchdarkly.com/events/bulk/5e73beba6edcf0076d131eb2	202	xhr	?flowId=03853ff9-...	529 B	9...	
539396bc03?a=351391337&sa=1&v=117...	https://bam.nr-data.net/events/1/539396bc03?a=351391337&sa=1&v=1177.96a4d39&t=Unnamed%20Transaction&rst=3855&ck=1&ref=https://ap...	200	xhr	?flowId=03853ff9-...	504 B	1...	
a2d6a558f99d8e8e3da8.woff2	https://apps.pingone.com/5d457682-3e15-43cd-accc-df182c8f7e2a/signon/a2d6a558f99d8e8e3da8.woff2	304	font	styles.css	801 B	3...	
367531d5c657281665cd.otf	https://apps.pingone.com/5d457682-3e15-43cd-accc-df182c8f7e2a/signon/367531d5c657281665cd.otf	304	font	styles.css	801 B	5...	
227817852e96b494055e.otf	https://apps.pingone.com/5d457682-3e15-43cd-accc-df182c8f7e2a/signon/227817852e96b494055e.otf	304	font	styles.css	801 B	4...	
5e73beba6edcf0076d131eb2	https://events.launchdarkly.com/events/bulk/5e73beba6edcf0076d131eb2	202	xhr	?flowId=03853ff9-...	529 B	7...	

109 requests | 299 kB transferred | 47.5 MB resources | Finish: 6.0 min | DOMContentLoaded: 539 ms | Load: 542 ms

```
{
"id" : "f0509c78-9d00-4c69-92e0-6528d7cd5494",
"code" : "ACCESS_FAILED",
"message" : "The request could not be completed. You do not have access to this resource.",
"details" : [ {
"code" : "INVALID_TOKEN",
"message" : "Kerberos ticket is invalid"
} ]
}
```

The `Kerberos ticket is invalid` error indicates the browser submitted a Kerberos ticket, but the ticket was invalid or otherwise unable to be processed.

This error occurs when:

The KDC isn't issuing tickets with AES Encryption

1. In Windows, open a command prompt and enter **`klist`**.

   There should be a ticket for the services for which you configured SPNs. For example, `HTTP/kerberos.pingone.com` and `HTTP/d3vol3lyj0eg62.cloudfront.net`.

   Learn more in Creating SPNs.

2. Check the KerbTicket Encryption Type.

   If the KerbTicket Encryption Type is set to RSADSI RC4-HMAC, it will not be supported by PingOne, as PingOne requires AES Encryption.

   1. On your server, in **Active Directory Users and Computers**, find the user account that is attempting to access PingOne using Kerberos.
   2. Right click the account and select **Properties**.
   3. Click the **Account** tab.
   4. In the **Account Options** section, select **This account supports Kerberos AES 256 bit encryption**.

   If there is a login error, you might need to purge existing Kerberos tickets.

3. To purge tickets:

   1. Open a command prompt and enter **`klist purge`**.
   2. Sign off from Windows and sign back on.
   3. Attempt Kerberos authentication.

Copyright © 2025 Ping Identity Corporation

> **Note**
> Discuss with your Active Directory admin the best way to ensure the Key Distribution Center (KDC) issues tickets using AES Encryption for all users.

The service account for the PingOne gateway isn't configured to use AES Encryption for Kerberos

1. In **Active Directory Users and Computers**, find the service account you've configured for the PingOne gateway Kerberos integration.
2. Right click the account and select **Properties**.
3. On the **Account** tab, in the **Account Options** section, select **This account supports Kerberos AES 256 bit encryption**.
4. Restart the gateway instance. Learn more in Starting a gateway instance.
5. Confirm that Kerberos sign-on working.

   If Kerberos authentication still isn't working, purge existing Kerberos tickets.
6. To purge tickets:
   1. Open a command prompt and enter `klist purge`.
   2. Sign off from Windows and sign back on.
   3. Attempt Kerberos authentication.
7. If Kerberos authentication still isn't working, you must reset the password for the service account. Then, repeat step 6.

A user is getting an HTTP error 431

Kerberos tickets containing user group information can exceed the PingOne header size limit, causing PingOne to return HTTP error 431 `Request Header Fields Too Large`.

> **Note**
> The PingOne header size limit is 6 KB

Reduce the number of groups the user is a member of so that the Kerberos ticket is smaller.

RADIUS gateways

The PingOne Remote Authentication Dial-In User Service (RADIUS) Gateway is a lightweight RADIUS server that acts as a bridge between an on-premise VPN or remote access system and PingOne.

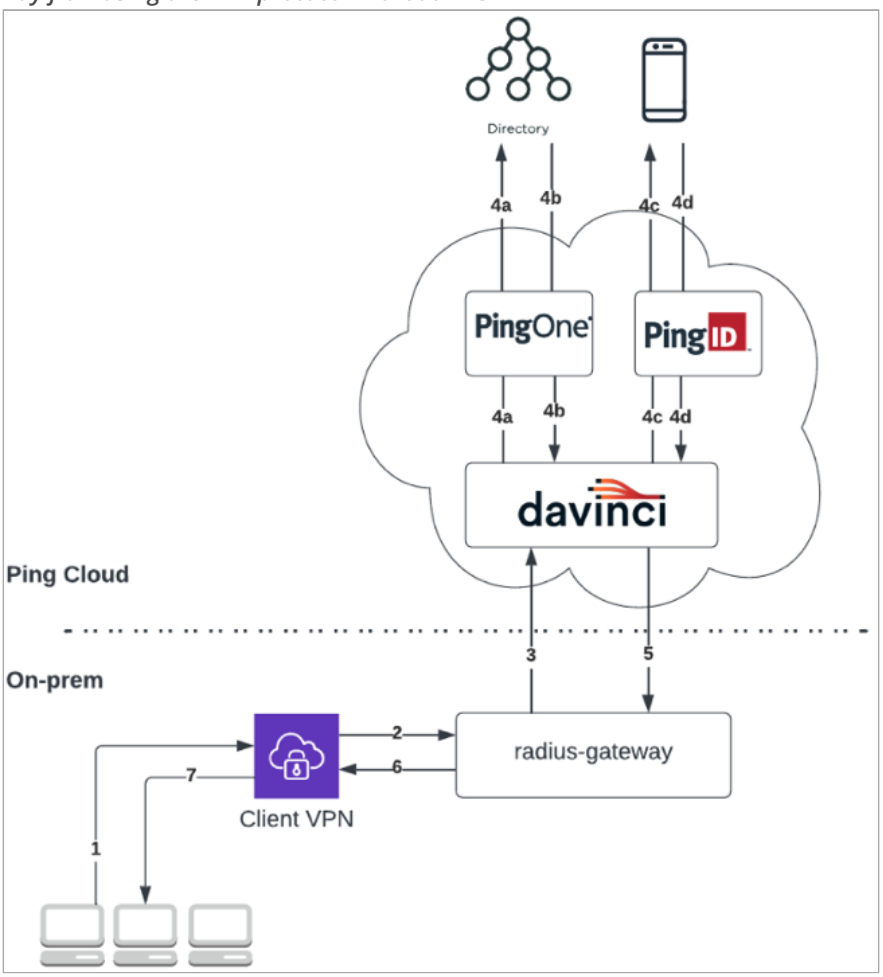
Copyright © 2025 Ping Identity Corporation

You can use a RADIUS gateway to orchestrate user authentication flows by leveraging the PingOne DaVinci orchestration engine. After you have configured a RADIUS gateway, users must follow a series of steps, as defined in your DaVinci flow, to gain access to your VPN. You can customize the DaVinci flow to include steps, such as user credential validation and multi-factor authentication (MFA).

The RADIUS gateway currently supports the PAP, MS-CHAP v2, and EAP-MSCHAPv2 protocols. You can also incorporate your Network Protocol Server (NPS) into a flow, if required. If an NPS is incorporated into the flow, after authenticating successfully, the NPS attributes are extracted from the authentication response and sent to the RADIUS client.

The following diagrams provide examples of a general RADIUS gateway authentication flow for each protocol using PingID mobile app to authenticate. The actual configuration varies depending on your organizational infrastructure considerations and policies.

Example of a RADIUS gateway flow using the PAP protocol without NPS



1. A user opens a VPN sign-on window and enters their username and password.
2. The VPN client sends their details to the RADIUS server running in the RADIUS gateway.
3. The RADIUS gateway initiates a DaVinci flow policy.
4. The DaVinci flow executes the following steps:
    1. DaVinci invokes the PingOne connector step to initiate credential validation.
    2. The user credentials are validated against a directory (in this example, PingOne Directory).

Copyright © 2025 Ping Identity Corporation

3. DaVinci invokes the PingID connector step and the PingID server initiates a second-factor authentication. The user receives a push notification to the relevant device.

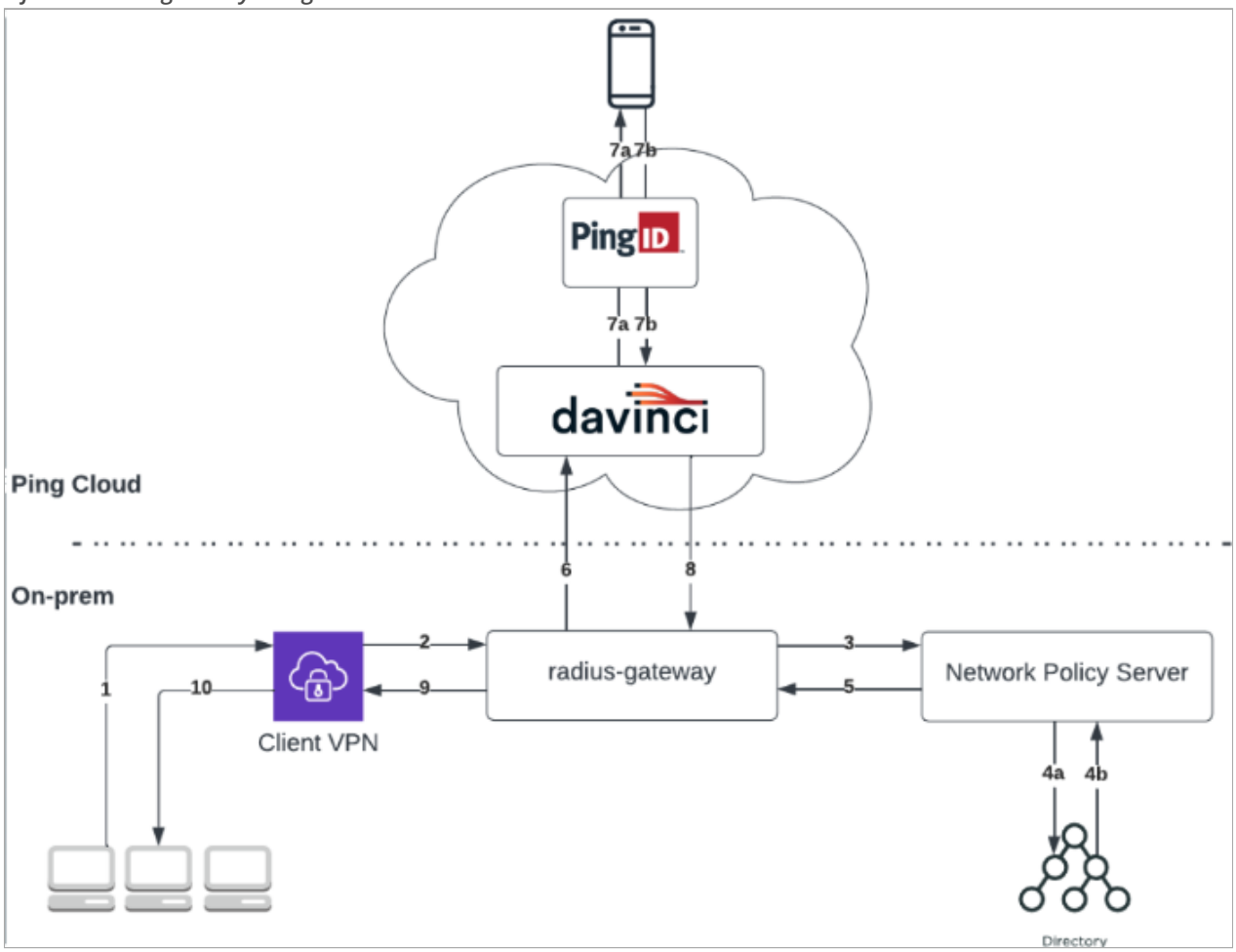
4. The user approves the push notification.

5. The DaVinci flow is finalized and a response is sent back to the RADIUS gateway.

6. The RADIUS gateway returns a response to the VPN.

7. The VPN forwards the response, granting or denying access to the user.

Example of the RADIUS gateway using NPS



This flow can be used with advanced protocols, such as MS-CHAP v2, or PAP.

1. A user opens a VPN sign-on window and enters their username and password.

2. The VPN client sends their details to the RADIUS server running in the RADIUS gateway.

3. The RADIUS gateway forwards the details to the NPS.

4. The NPS validates the user credentials against its directory.

5. The NPS returns the response to the RADIUS gateway.

6. If the credentials are correct, the RADIUS gateway initiates a DaVinci flow policy.

Copyright © 2025 Ping Identity Corporation

7. The DaVinci flow executes the following steps:
    1. DaVinci invokes the PingID connector step and the PingID server initiates a second factor authentication. The user receives a push notification to the relevant device.
    2. The user approves the push notification.
8. The DaVinci flow is finalized and a response is sent back to the RADIUS gateway.
9. The RADIUS gateway returns a response to the VPN.
10. The VPN forwards the response, granting or denying access to the user.

Before you begin configuring a RADIUS gateway

Before you start setting up a gateway, ensure that you have the following information.

Prerequisites

To enable communication between PingOne Remote Authentication Dial-In User Service (RADIUS) gateway and your RADIUS clients, you'll need:

- To add the PingOne DaVinci service to your PingOne environment.
- A RADIUS Client IP and Shared Secret for each RADIUS client.
- A DaVinci flow with a DaVinci policy. You should add the RADIUS gateway connector, the PingID connector, and use an out-of-the-box RADIUS gateway flow. Learn more in the PingOne RADIUS gateway connector documentation. Learn more about PingOne DaVinci policies in DaVinci flow policies.
- (Optional) If you want to perform multi-factor authentication (MFA) using PingID, you'll also need to configure the RADIUS gateway in a PingOne environment that has PingID linked as a service.
- RADIUS gateway currently supports PAP, MS-CHAP v2, and EAP-MSCHAPv2 protocols. If you want to use the MS-CHAP v2, or EAP-MS-CHAP v2 protocol, you need a Network Policy Server (NPS). You'll also need to enable users to enter an one-time passcode (OTP) with their username. Learn more in Enable users to enter an OTP with their username in MS-CHAP v2, or EAP-MSCHAPv2 mode.
- (Optional) When using the PAP protocol, you can also incorporate an NPS into a flow.

Docker

You can run the gateway in a Docker container or as a standalone Java application. If you plan to run the gateway in a Docker container, ensure that you have Docker installed on the computer that will run the gateway.

System requirements

The computer, virtual machine, or Docker environment that will run the gateway should have the following resources dedicated to the gateway:

- Processor: 2 CPUs or virtual CPUs
- RAM: 1 GB

Copyright © 2025 Ping Identity Corporation

- Storage: 1 GB

Gateway access

The gateway requires access to the RADIUS client over the network as well as the ability to initiate outbound requests over the internet to establish a WebSocket Secure connection to PingOne.

The WebSocket Secure address varies depending on your region. Ensure that the gateway can access the WebSocket Secure address for your region.

Region	Address
Australia	wss://gateways.pingone.com.au/ wss://gateways-ap-southeast-2.pingone.com.au/
Canada	wss://gateways.pingone.ca/ wss://gateways-ca-central-1a.pingone.ca/ wss://gateways-ca-central-1b.pingone.ca/
Europe	wss://gateways.pingone.eu/ wss://gateways-eu-central-1.pingone.eu/ wss://gateways-eu-west-1.pingone.eu/
North America (US)	wss://gateways.pingone.com/ wss://gateways-us-east-2.pingone.com/ wss://gateways-us-west-2.pingone.com/
Singapore	wss://gateways.pingone.sg/ wss://gateways-ap-southeast-1y.pingone.sg/ wss://gateways-ap-southeast-1z.pingone.sg/
Asia Pacific (legacy) **Note** Available only for existing .asia customers.	wss://gateways.pingone.asia/ wss://gateways-ap-southeast-2.pingone.asia/

PingOne user privileges

The administrator setting up the gateway should have the `Environment admin` role. To confirm, open the PingOne console, locate the administrator identity, and confirm its roles.

Enable users to enter an OTP with their username in MS-CHAP v2, or EAP-MSCHAPv2 mode

PingOne RADIUS Gateway with MS-CHAP v2 or EAP-MSCHAPv2 only works in no-challenge mode.

About this task

Copyright © 2025 Ping Identity Corporation

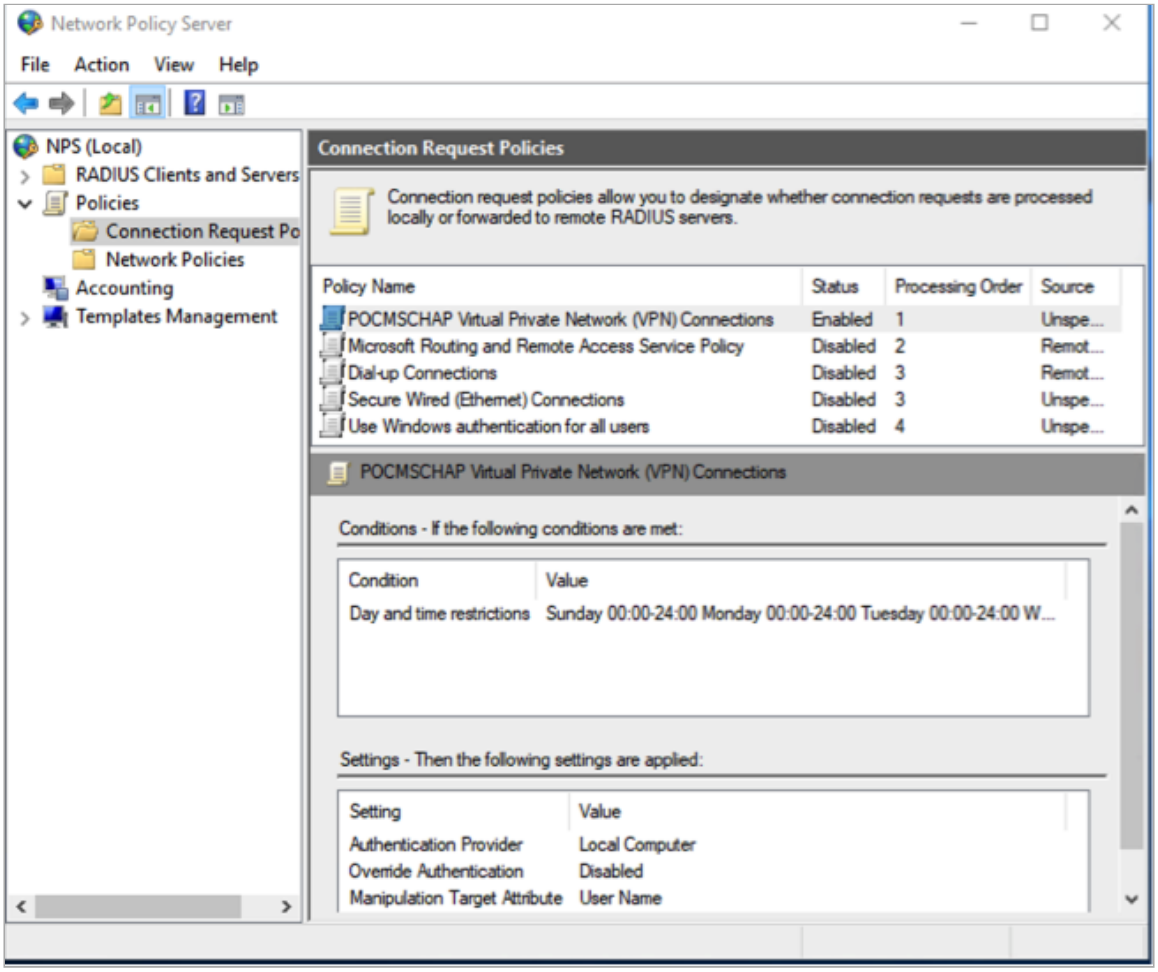
Your users can enter a one-time passcode (OTP) with their username when signing on in no-challenge mode. To do this, a custom separator should be added to the Network Policy Server (NPS). The same custom separator must also be configured in the DaVinci flow. Learn more in the PingOne RADIUS gateway connector documentation.

For example, adding a comma separator enables the user to enter the OTP in the format `<username>,OTP`. For user `John`, OTP `123456` is entered as `John,123456`.

To configure the NPS to enable users to enter an OTP together with their username:

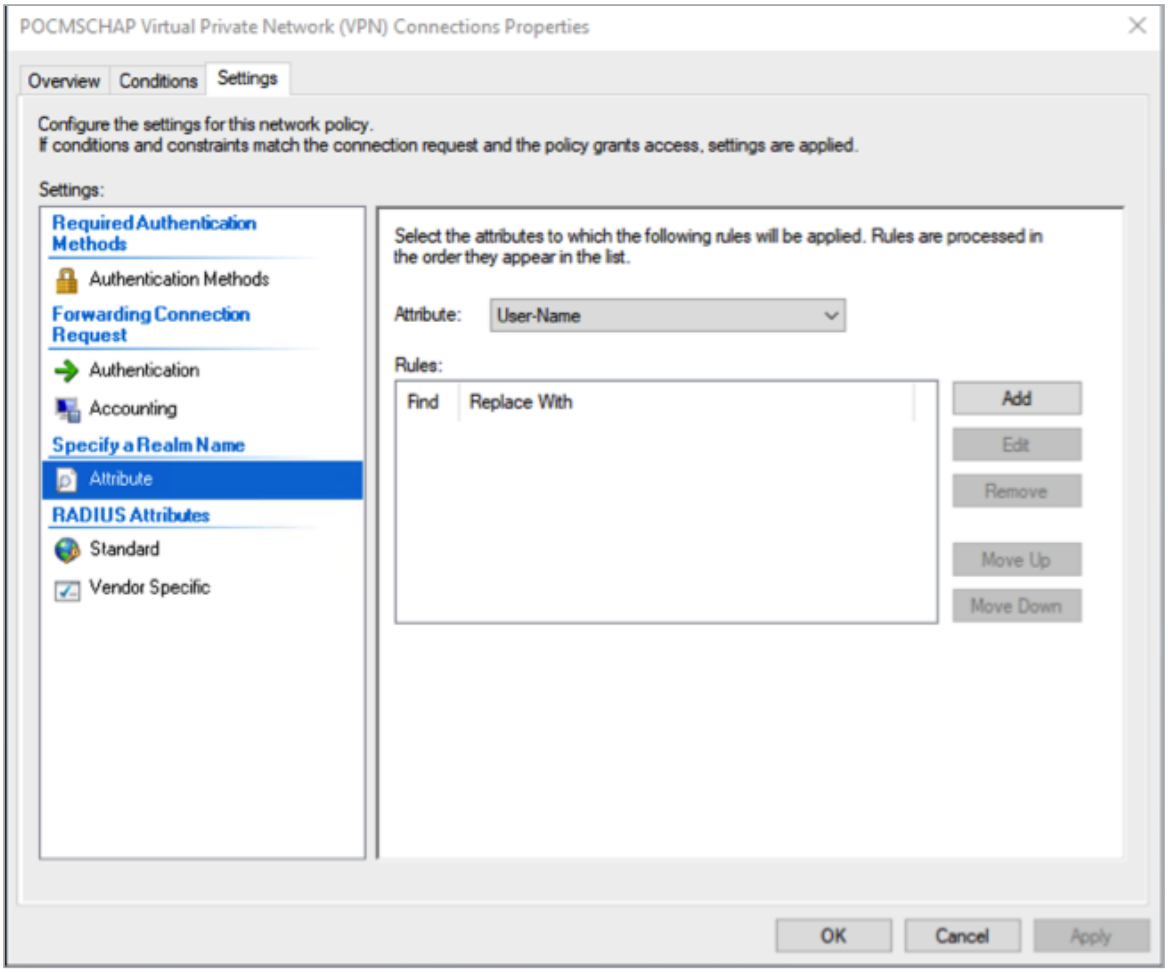
Steps

1. Sign on to the Windows server and open the **Network Policy Server** (NPS) configuration window.
2. In the **NPS** tree, under **Policies** click **Connection Request Policies**.



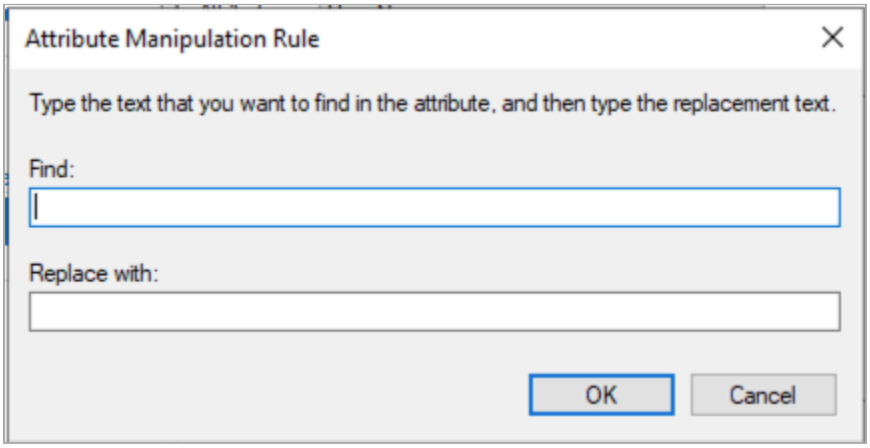
3. In the **Connection Request Policies** list, double-click your policy to view the policy properties.
4. On the **Settings** tab, in the **Specify a Realm Name** section, click **Attribute**.

Copyright © 2025 Ping Identity Corporation



5. In the **Attribute** list, select **User-Name**.

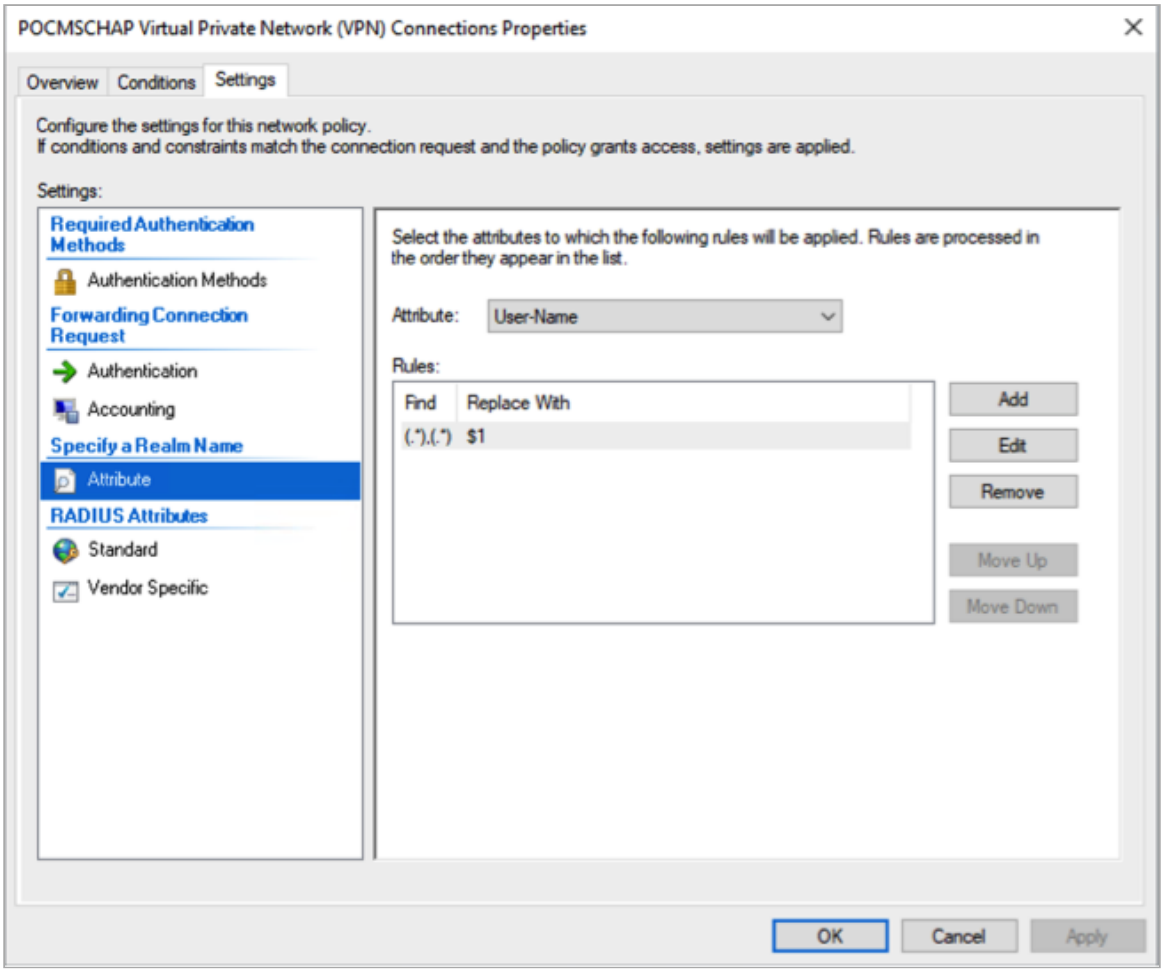
6. Click **Add**.



7. In the **Attribute Manipulation Rule** window, enter the following and then click **OK**:

   - **Find**: `(.)<custom separator>(.)`
   - **Replace with**: `$1`

Copyright © 2025 Ping Identity Corporation



Setting up a RADIUS gateway

Set up a Remote Authentication Dial-In User Service (RADIUS) gateway to simplify the control and management of your network by providing a centralized cloud-based way to monitor, manage, and troubleshoot your RADIUS authentication requests through a single platform.

About this task

To set up a RADIUS gateway:

Steps

1. Add a RADIUS gateway.
2. Starting a gateway instance.
3. Verifying a gateway instance.

Adding a RADIUS gateway

Add a RADIUS gateway to allow PingOne to communicate with your RADIUS clients.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Integrations → Gateways**.
2. Click the **+** icon.
3. Enter the following and click **Next**:
   - **Name**: A name for the gateway. The name must be unique within the environment.
   - **Gateway Type**: Select **RADIUS**.
   - **Description** (optional): A brief description of the gateway.
4. **Optional:** In the **Authentication Port** field, enter the relevant port number. The default is 1812.

   > **Note**
   > You must stop all active gateway instances before modifying the authentication port.

5. In the **DaVinci Policy ID** field, select the DaVinci Policy ID that you want to apply to the RADIUS gateway.
6. If you want to define a **Default Shared Secret**, enter it here.

   If no default is defined, you must enter a **Client Shared-Secret** for each **Client IP address** that you add.

   > **Note**
   > For security reasons, you should rotate the shared secret at least once a year.

7. **Optional:** To incorporate a Network Policy Server (NPS), configure the following settings:
   1. Select the **Use RADIUS Remote Network Policy Server** check box.
   2. Enter the relevant NPS **Server IP** and **Server port**.

      > **Note**
      > Because validation of the client IP shared secret is performed on the RADIUS gateway side and the NPS side, you must make sure the shared secret on the client matches the shared secret on the endpoint NPS.

8. In the **RADIUS clients** area, for each client that you want to add:
   1. Click **Add Client**.
   2. In the new row, enter the **Client IP address** of the VPN server or remote access system and the **Client Shared Secret**.

      If the **Client Shared Secret** field is left empty, the **Default Shared Secret** is used.

   3. (Optional) To mitigate the risk of a Blast-RADIUS attack, select the **RADIUS Security Enhancement** checkbox and then select either:
      - **Require Message-Authenticator**: RADIUS gateway requires this attribute in every client request, and also includes it as the first attribute in every RADIUS response.

Copyright © 2025 Ping Identity Corporation

- **Limit Proxy-State**: RADIUS Gateway ignores requests that contain one or more Proxy-State attribute if they do not include the **Message-Authenticator** attribute. This option should only be used for legacy clients that don't support sending the **Message-Authenticator** attribute and are not acting as a proxy client.

> **Note**
>
> Learn more about Blast RADIUS mitigations in the IETF article Deprecating Insecure Practices in RADIUS and RADIUS vulnerability CVE-2024-3596 in the Ping Identity Knowledge Base (requires sign-on).

9. Click **Save**.

   Result:

   The new gateway displays in the **Gateways** list. PingOne generates a gateway credential, which the gateway uses to authenticate with PingOne.

   > **Important**
   >
   > A gateway credential is like a password, so keep it protected. For security reasons, PingOne does not store the generated gateway credentials, but you can always create a new one in the PingOne console. Multiple gateway instances can use the same gateway credential.

10. Copy the credential and paste it to a secure location.

    You'll use the credential later when starting a gateway instance.

11. **Optional:** Click **Show me the Docker command** and copy it to a secure location.

12. Click **Done**.

Next steps

Start a gateway instance

Starting a gateway instance

You can run a standalone gateway as a Windows service, a standalone Java application, or a Docker container, with or without a forward web proxy server.

About this task

> **Note**
>
> - Stopping and starting a gateway instance does not cause any configuration issues, but the PingOne Gateway will not function until the instance is started again.
> - Digest authentication does not support international characters.
> - Basic authentication requires configuration in the proxy server to support international characters.

Copyright © 2025 Ping Identity Corporation

Starting the gateway instance in a Docker container

About this task

Use the Docker command that you copied from PingOne to start a Docker container. Run the Docker container on a computer that can reach your Remote Authentication Dial-In User Service (RADIUS) client and PingOne.

Steps

1. Ensure that Docker is installed and that the Docker Engine is running.
2. Locate the Docker command that you copied earlier.

   Learn more in Adding a RADIUS gateway.
3. Review the end user license agreement at www.pingidentity.com/en/legal/subscription-agreement.html.
4. If you agree to the terms of the license agreement, open the Docker command in a text editor and change `-e PING_IDENTITY_ACCEPT_EULA=no` to `-e PING_IDENTITY_ACCEPT_EULA=yes`.
5. At a command prompt, run the Docker command.
6. (Optional) To configure a RADIUS gateway client application to use a forward web proxy server to handle traffic between the gateway and PingOne, in the `run.properties` file provide the relevant access information:
   - `-e http_proxyHost=<HTTP_PROXY_HOST>`
   - `-e http_proxyPort=<HTTP_PROXY_PORT>`
   - `-e http_proxyUser=<HTTP_PROXY_USER>`
   - `-e http_proxyPassword=<HTTP_PROXY_PASSWORD>`
   - `-e http_proxyAuthenticationMethod=DIGEST (or BASIC)`

   `http_proxyHost` and `http_proxyPort` are required to use a web proxy.

   `http_proxyUser`, `http_proxyPassword`, and `http_proxyAuthenticationMethod` are required if the web proxy requires authentication. a

   > **Important**
   >
   > For `http_proxyAuthenticationMethod`, note that BASIC (as in basic authentication) transmits access credentials without encryption. You should therefore use DIGEST (digest authentication) because it uses a challenge-response mechanism and does not send the password in plain text.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> - You must configure the web proxy settings locally for each running instance. For example, if you are running two gateway client applications, you must configure web proxy settings for each instance separately.
> - For basic authentication to support international characters, the proxy server must also be configured to support international characters.
> - Digest authentication does not support the use of international characters.

Next steps

Verify a gateway instance

Starting a gateway instance as a standalone Java application

Download a gateway bundle and run it on a local computer as a Java application.

Before you begin

- If you have a valid gateway credential, have it ready. Alternatively, you can create a new credential on the Overview tab in the gateway details. Learn more in Creating or deleting a gateway credential.
- Install Java version 17.0.8 or later or Java version 21 LTS or later on the computer that will run the gateway.
- Create a JAVA_HOME system environment variable that points to the directory that contains the bin directory from the Java distribution.

About this task

Run the application on a computer that can reach your RADIUS client and PingOne.

Steps

1. Go to **Integrations → Gateways** and locate the appropriate gateway.
2. Go to **Integrations → Gateways** and locate the appropriate gateway.
3. Click the **Download** tab.
4. In the **Standalone** section, review the prerequisites and instructions.

   In the **Instruction** section, click the download link for the gateway bundle.

   > **Note**
   >
   > If prompted, complete the sign-on process.

   The download begins.
5. To configure the gateway:
   1. Extract the downloaded bundle and follow the instructions in the `README.txt` file.

Copyright © 2025 Ping Identity Corporation

2. To configure a RADIUS gateway client application to use a forward web proxy server to handle traffic between the gateway and PingOne, in the `run.properties` file, provide the relevant access information.

> **Note**
>
> - You must configure the web proxy settings locally for each running instance. For example, if you are running two gateway client applications, you must configure web proxy settings for each instance separately.
> - For basic authentication to support international characters, the proxy server must also be configured to support international characters.
> - Digest authentication does not support the use of international characters.

Next steps

Verify a gateway instance

Verifying a gateway instance

After you start the gateway instance, ensure that the gateway can connect to PingOne.

Steps

1. Go to **Integrations → Gateways**.
2. Locate the appropriate gateway.

> **Note**
>
> You can refresh the **Gateways** page to ensure that the information is current.

3. Review the gateway details to ensure that the gateway instance is healthy.

Configuring multiple gateways

For high-availability applications or scalability, you can configure multiple gateways. You can then run the Docker container or Java application on multiple servers.

When multiple gateways are configured, PingOne maintains a list of the active gateways and uses a round robin algorithm to route the request to the first available gateway instance. If a gateway is not available, it is excluded from the list of active gateways.

You can set up one PingOne logical gateway with one gateway credential, with multiple physical gateways that share the same credential. If needed, you can remove the credential from the logical gateway to stop all gateway traffic.

Creating or deleting a gateway credential

PingOne automatically creates a gateway credential when you add a gateway, but you can create additional credentials at any time. You can also delete a gateway credential.

About this task

Copyright © 2025 Ping Identity Corporation

> **Important**
> For optimal security, you should rotate gateway credentials periodically.

Steps

1. In the PingOne admin console, go to **Integrations** > **Gateways**.
2. To add a gateway credential:
    1. Click the appropriate gateway to display gateway details.
    2. On the **Overview** tab, click the **+** icon next to **Gateway credentials**.
    3. Verify that the credential was created and copy it to a secure location.

    > **Important**
    > The credential is shown in the console only once. If necessary, you can retrieve existing credentials through the `Gateway Management API`. Learn more in Gateway Management in the PingOne Platform API Reference.

    4. Click **Done**.

    Result:

    The new credential is added to the list with a unique ID.
3. To delete a gateway credential:
    1. On the **Gateways** page, click the gateway that has the credential you want to delete.
    2. On the **Overview** tab, click the **Delete** icon (🗑) icon next to the credential.
    3. Select the **I understand and want to continue** checkbox.
    4. Click **Revoke**.

    After a credential is revoked, the gateway cannot use the credential to access PingOne.

Running a standalone RADIUS gateway as a Windows service

You can run the PingOne RADIUS gateway as a standalone Windows service. You'll do this by downloading a PingOne LDAP gateway software `.zip` archive from the PingOne admin console and adding the service to a computer running Windows. This functionality is available in RADIUS Gateway 1.2 and later.

Before you begin

- Set up a Radius gateway. Learn more in Setting up a RADIUS gateway
- If you have a valid gateway credential, have it ready. Alternatively, you can create a new credential on the **Overview** tab in the gateway details. Learn more in Creating or deleting a gateway credential.
- Install Java version 17.0.8 or later or Java version 21 LTS or later on the computer that will run the gateway.

Copyright © 2025 Ping Identity Corporation

- Create a `JAVA_HOME` system environment variable that points to the directory that contains the `bin` directory from the Java distribution.

Directory structure

Most extract utilities will extract the PingOne RADIUS gateway software `.zip` archive files to a directory with a pattern of `pingone-radius-gateway-<version>`. This directory structure is part of the `.zip` archive. For best results, do not rename the `pingone-radius-gateway-<version>` directory.

The archive extracts the files with the following directory structure:

Parent directory

```
C:\Program Files\Ping Identity
```

RADIUS Gateway directory

```
C:\Program Files\Ping Identity\pingone-radius-gateway-<version>
```

run.properties location

```
C:\Program Files\Ping Identity\pingone-radius-gateway-<version>\config
```

Batch files location

```
C:\Program Files\Ping Identity\pingone-radius-gateway-<version>\bin\windows
```

Learn more in:

- Adding the RADIUS Gateway service
- Removing the RADIUS Gateway service
- Upgrading the PingOne RADIUS Gateway

Adding the RADIUS Gateway service

Download the ZIP archive and extract it to the computer that will run the gateway.

Steps

1. In the PingOne admin console, go to **Integrations → Gateways**.
2. Click the appropriate gateway entry to open the details panel.
3. Click the **Download** tab.
4. Click the download link to download the `.zip` archive.
5. Extract the `.zip` archive to the computer that will run the gateway. We recommend that you use a common location as the parent directory, such as `C:\Program Files\Ping Identity`.

Copyright © 2025 Ping Identity Corporation

6. Follow the instructions in the `README.txt` file to:

    1. Configure the `run.properties` file, including providing the gateway credential information. The run.properties file is located in the config directory. For example: `C:\Program Files\Ping Identity\pingone-radius-gateway-1.2.0\config`.

    2. (Optional) To configure a RADIUS Gateway client application to use a forward web proxy server to handle traffic between the gateway and PingOne, in the `run.properties` file provide the relevant access information.

    > **Note**
    >
    > - You must configure the web proxy settings locally for each running instance. For example, if you are running two gateway client applications, you must configure web proxy settings for each instance separately.
    > - For basic authentication to support international characters, the proxy server must also be configured to support international characters.
    > - Digest authentication does not support the use of international characters.

7. Sign on to Windows with administrator privileges.

8. Start a Command Prompt or PowerShell.

9. Run the `install-service.bat` file without any parameters. By design, the `install-service.bat` file does not start the service automatically after completion. However, the service is configured to start automatically at the next and subsequent restarts of the Windows operating system.

10. In the Services system application, start the PingOne RADIUS Gateway service.

Removing the RADIUS Gateway service

Use the following information to remove the PingOne RADIUS Gateway service.

Steps

1. Sign on to Windows with administrator privileges.

2. Start the Services system application and stop the PingOne RADIUS Gateway service.

3. Locate the `uninstall-service.bat` file.

    1. In the Services system application, locate the RADIUS Gateway service.

    2. Right-click and select **Properties**.

    3. Note the **Path to executable** value.

    For example, if the value is

    `C:\Program Files\Ping Identity\pingone-radius-gateway-1.2.0\bin\windows\radius-gateway-windows-x86-64.exe -s C:\Program Files\Ping Identity\pingone-radius-gateway-2.3.0\bin\windows\PingOneRadiusGatewayService.conf`

    then you can find the `uninstall-service.bat` file in the `C:\Program Files\Ping Identity\pingone-radius-gateway-1.2.0\bin\windows` directory.

Copyright © 2025 Ping Identity Corporation

4. Run the `uninstall-service.bat` file without any parameters. The underlying directories and files are not removed. Make backup copies and remove the files as needed.

Upgrading the PingOne RADIUS Gateway

Use the following information to update the PingOne RADIUS Gateway to a later version. You'll uninstall the old version before installing the new one.

Steps

1. In the PingOne admin console, go to **Integrations → Gateways**.
2. Click the appropriate gateway entry to open the details panel.
3. Click the **Download** tab.
4. Click the download link to download the ZIP archive for the version to which you want to upgrade.
5. Extract the ZIP archive to the computer that will run the gateway. We recommend that you use a common location as the parent directory, such as `C:\Program Files\Ping Identity`.
6. Configure the `run.properties` file, including providing the gateway credential information. The `run.properties` file is located in the `config` directory. For example: `C:\Program Files\Ping Identity\pingone-radius-gateway-<new-version>\config`.
7. Uninstall the old version of the gateway before installing the new one.
    1. Start the Services system application and find the RADIUS Gateway service that you are upgrading from.
    2. Right-click and select **Properties**.
    3. Note the **Path to executable** value.

       For example, if the value is `C:\Program Files\Ping Identity\pingone-radius-gateway-1.2.0\bin\windows\radius-gateway-windows-x86-64.exe -s C:\Program Files\Ping Identity\pingone-radius-gateway-1.2.0\bin\windows\PingOneRadiusGatewayService.conf`

       then you can find the `uninstall-service.bat` file in the `C:\Program Files\Ping Identity\pingone-radius-gateway-<old-version>\bin\windows` directory.
    4. Optional: Start the Services system application and stop the RADIUS Gateway <old-version> service.
    5. Run the `uninstall-service.bat` file for the RADIUS Gateway <old-version> service, without any parameters. The underlying directories and files are not removed. Make backup copies and remove the files as needed.
8. After you have uninstalled the old version, you can finish installing the new one.
    1. Locate the `install-service.bat` file for the RADIUS Gateway <new-version> service.
    2. Run the `install-service.bat` file without any parameters.

       By design, the `install-service.bat` file does not start the service automatically after completion. However, the service is configured to start automatically at the next and subsequent restarts of the Windows operating system.
    3. In the Services system application, start the new PingOne RADIUS Gateway <new-version> service.

Copyright © 2025 Ping Identity Corporation

Troubleshooting a RADIUS gateway instance

If the gateway instance is not healthy, use the information in this section to troubleshoot any issues.

The following information applies to the various gateway deployment scenarios. You can use the gateway details page, gateway logs, or Splunk reports to identify issues. Learn more in Verifying a gateway instance and Monitoring activity with Splunk.

I want to view the audit logs

You can view logs to get detailed information about the Gateway service. The method to do so varies depending on your gateway configuration.

Gateway as a standalone service

By default, log files are saved to the `./logs` directory on the computer running the gateway. Log files roll over by date.

To view the logs, go the `./logs` directory. The logs are named `GatewayStandalone.yyyymmdd.log`

Gateway as a Windows service

By default, log files are saved to the `./logs` directory on the computer running the gateway. Log files roll over by date.

To view the logs, go to the `./logs` directory. The logs are named:

- `GatewayService.yyyymmdd.log`
- `GatewayWrapper.yyyymmdd.log`

> **Note**
>
> The `GatewayWrapper.yyyymmdd.log` file mirrors the console output of the standalone version, with additional logs.

Gateway as a Docker container

To view logs for a Docker container, run the following command:

```
docker logs  _<container ID or name>_
```

My connection is taking too long to resolve

If your connection is taking a long time, check the following:

- If the connection is configured with a string host name, try using an IP address instead.
- On the server that you want to connect to, ensure that the desired port is open.
- Ensure there aren't any routing issues in your infrastructure that could affect the ability of the gateway server to reach the LDAP server or Remote Authentication Dial-In User Service (RADIUS) client.
- Sometimes it can take several seconds for the connection information to be updated in the console user interface. Try refreshing the page to get the most current information.

Copyright © 2025 Ping Identity Corporation

I want to increase scalability

For high-availability applications or scalability, you can deploy multiple gateways. You can then run the Windows service, Docker container, or Java application on multiple servers.

When multiple gateways are deployed, PingOne maintains a list of the active gateways and uses a round robin algorithm to route the request to the first available gateway instance. If a gateway is not available, it is excluded from the list of active gateways.

> **Note**
>
> Use a different credential for each deployed gateway instance. Using different credentials allows you to easily revoke access to individual gateways.

Authorize gateways

Authorize gateways combine the advantages of centralized policy administration with the benefits of on-premise decision evaluation and enforcement.

An Authorize gateway acts as a bridge between policy management components in PingOne and runtime gateway instances in your organization's infrastructure or cloud data center. Gateway instances have a small footprint and are easy to deploy across your staging pipelines.

Authorize gateways provide the following benefits:

Cloud administration of policies

Use the latest features of our admin console for policy authoring and management in one place, without the need to manage a policy administration point in your infrastructure.

Reduced latency

Minimize latency by deploying multiple gateway instances alongside the resources you are protecting.

Authorize gateways are ideal for high-volume, low latency situations, such as high-throughput transactions or API traffic. You can set up policy-enforcing applications and decision evaluation gateway instances in close proximity, and traffic doesn't need to flow through the PingOne platform.

Data residency

If compliance and security considerations make on-premise deployment a requirement for your application, gateway instances enable access to your on-premise datastores without exposing sensitive data outside of your organization's infrastructure.

Privacy for internal services

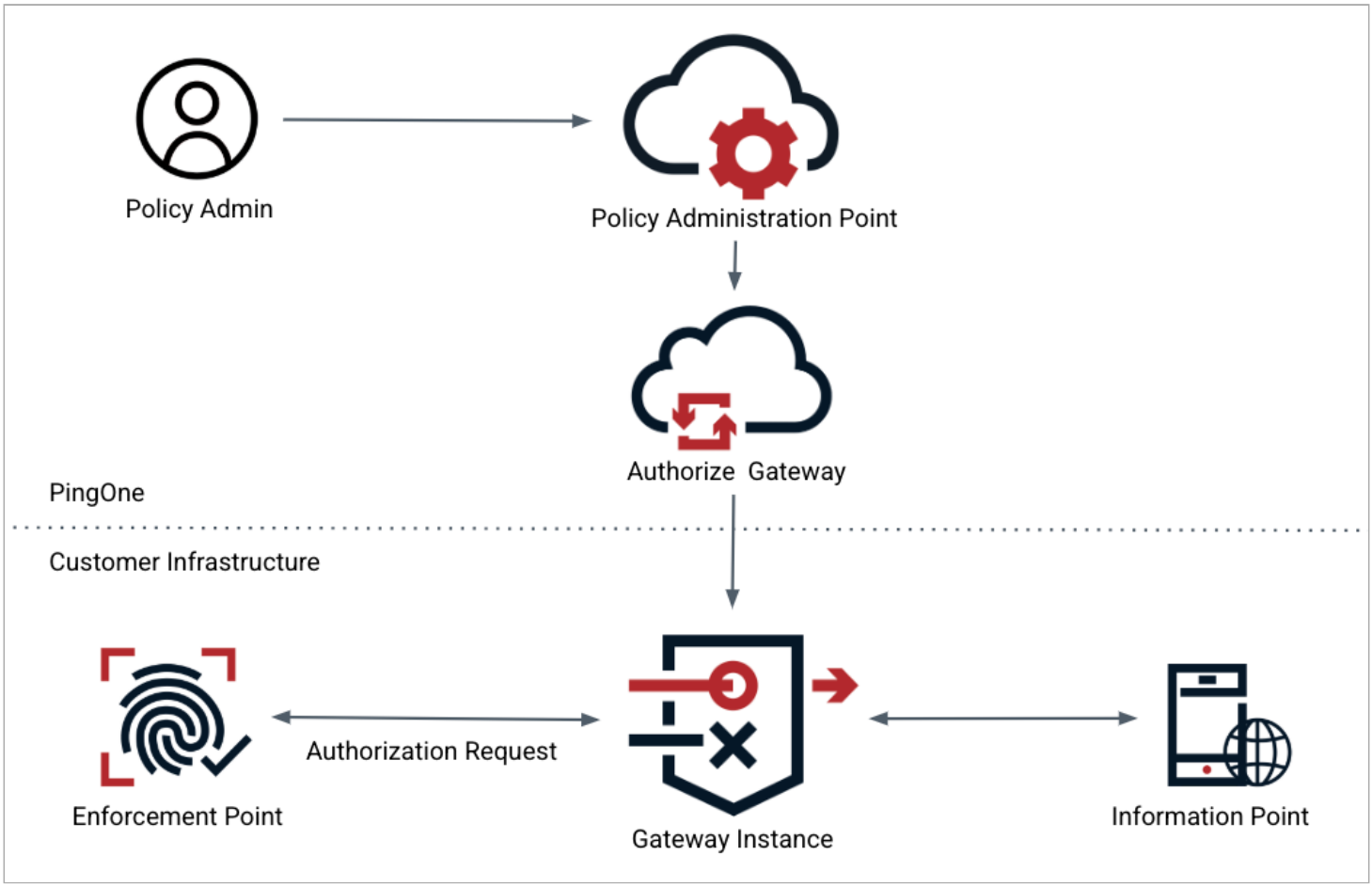
Decision evaluations use data stored in information points (HTTP services) that aren't exposed to the public internet.

How Authorize gateways work

With Authorize gateways, authorization decisions are processed within the boundaries of your network and under your control, while policy management and deployment services run in the PingOne cloud.

The following components are involved:

Copyright © 2025 Ping Identity Corporation



Management in PingOne

Component	Description
Policy administration point	PingOne Authorize serves as the centralized policy administration point where you configure and manage authorization policies and the attributes and services that provide context in authorization decisions.
Authorize gateway	The Authorize gateway communicates between PingOne and gateway instances in your organization's infrastructure. Use Authorize gateways to publish policy versions to gateway instances and keep them up to date.

Decision evaluations on-premise

Component	Description
Gateway instances	Authorize gateway instances evaluate policy versions published from PingOne in order to make authorization decisions. Gateway instances are distributed as containerized images, and they maintain a WebSocket Secure connection with the PingOne platform.

Copyright © 2025 Ping Identity Corporation

Component	Description
Information points	Information points are HTTP services that provide context for authorization decisions. Information points can be publicly available services or services maintained in your infrastructure.
Policy enforcement points	Enforcement points are applications that consume authorization decisions. They're maintained by your organization in your infrastructure.

A WebSocket Secure connection maintains two-way communication between Authorize gateways in PingOne and gateway instances in your infrastructure as follows:

- PingOne sends gateway configuration changes to gateway instances.
- Gateway instances send errors and alerts, error logs, health state, and metrics to PingOne.

> **Note**
>
> Error logs and metrics are collected for monitoring purposes only. This information isn't exposed in the PingOne admin console, except for CPU **% busy** and **Transaction time**.
> Gateway instances initiate the WebSocket connection, ensuring that you don't have to open inbound firewalls in your network to this traffic.

Authorize gateways use publicly authenticated HTTPS APIs in PingOne for the following:

- Token exchange to get an access token for PingOne APIs
- Downloading policy version deployment packages

Requirements for Authorize gateways

Before you deploy Authorize gateway instances in your organization's infrastructure, ensure that your systems meet the following requirements.

PingOne user privileges

The administrator setting up Authorize gateways must have the **Environment Admin** role in PingOne. This grants the **Authorize Gateway Deployment** permission required for working with Authorize gateways.

To confirm your roles, in the PingOne **Administrators** environment, go to **Directory > Users**, click the administrator identity, and confirm the roles on the **Roles** tab.

PingOne environment

Make sure the PingOne environment that you're using for self-managed deployments includes the PingOne SSO and PingOne Authorize services.

Learn more about setting up environments in Creating an environment.

Copyright © 2025 Ping Identity Corporation

Docker

To run a containerized Authorize gateway, you must have Docker installed on the machine that will run the gateway.

System requirements

The Docker environment that will run the Authorize gateway must have the following resources dedicated to the gateway:

Resource	Requirement
Processor	2 CPUs or virtual CPUs
RAM	1 GB
Storage	1 GB

Gateway access

The Authorize gateway requires the ability to initiate outbound requests over the internet to establish a WebSocket Secure connection and HTTPS connections to PingOne.

The WebSocket Secure address varies depending on your region. Ensure that the gateway can access the WebSocket Secure address for your region.

Region	Address	API Endpoints
Australia	wss://gateways.pingone.com.au/ wss://gateways-ap-southeast-2.pingone.com.au/	auth.pingone.com.au api.pingone.com.au
Canada	wss://gateways.pingone.ca/ wss://gateways-ca-central-1a.pingone.ca/ wss://gateways-ca-central-1b.pingone.ca/	auth.pingone.ca api.pingone.ca
Europe	wss://gateways.pingone.eu/ wss://gateways-eu-central-1.pingone.eu/ wss://gateways-eu-west-1.pingone.eu/	auth.pingone.eu api.pingone.eu
North America (US)	wss://gateways.pingone.com/ wss://gateways-us-east-2.pingone.com/ wss://gateways-us-west-2.pingone.com/	auth.pingone.com api.pingone.com
Singapore	wss://gateways.pingone.sg/ wss://gateways-ap-southeast-1y.pingone.sg/ wss://gateways-ap-southeast-1z.pingone.sg/	auth.pingone.sg api.pingone.sg

Copyright © 2025 Ping Identity Corporation

Region	Address	API Endpoints
Asia Pacific (legacy) **Note** Available only for existing .asia customers.	wss://gateways.pingone.asia/ wss://gateways-ap-southeast-2.pingone.asia/	auth.pingone.asia auth.pingone.asia

Setting up an Authorize gateway

Follow this process to deploy Authorize gateways in infrastructure managed by your organization.

You can use a bootstrapped version of authorization policies with your Authorize gateway. This enables you to set up components in your infrastructure before you build policies in the cloud.

To get started:

1. Make sure your systems meet requirements for self-managed deployments.
2. Add an Authorize gateway.
3. Start a gateway instance using Docker. This deploys a gateway instance in your infrastructure.
4. Build your authorization policies and set up attributes and services in the Trust Framework.
5. Publish policy versions to gateway instances.
6. Make decision requests to gateway instances.

Adding an Authorize gateway

Use an Authorize gateway to deploy authorization policy versions to gateway instances in your infrastructure and keep them up to date.

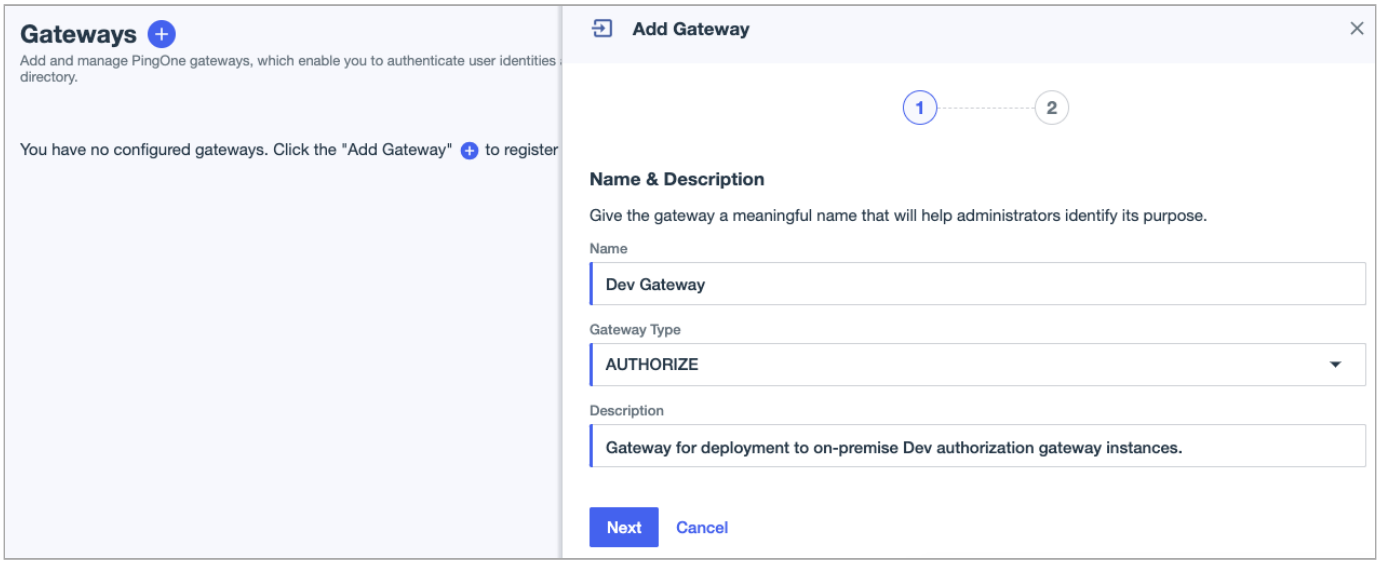
The Authorize gateway communicates between PingOne and gateway instances. The Authorize gateway consists of a PingOne cloud component and one or more gateway instances deployed in your organization's infrastructure. The downloadable runtime is available after you've added an Authorize gateway.

You can use separate Authorize gateways to represent your development, testing, and production environments for deploying authorization policies.

Steps

1. In PingOne, go to **Integrations** > **Gateways** and click the **+** icon to add a gateway.

Copyright © 2025 Ping Identity Corporation

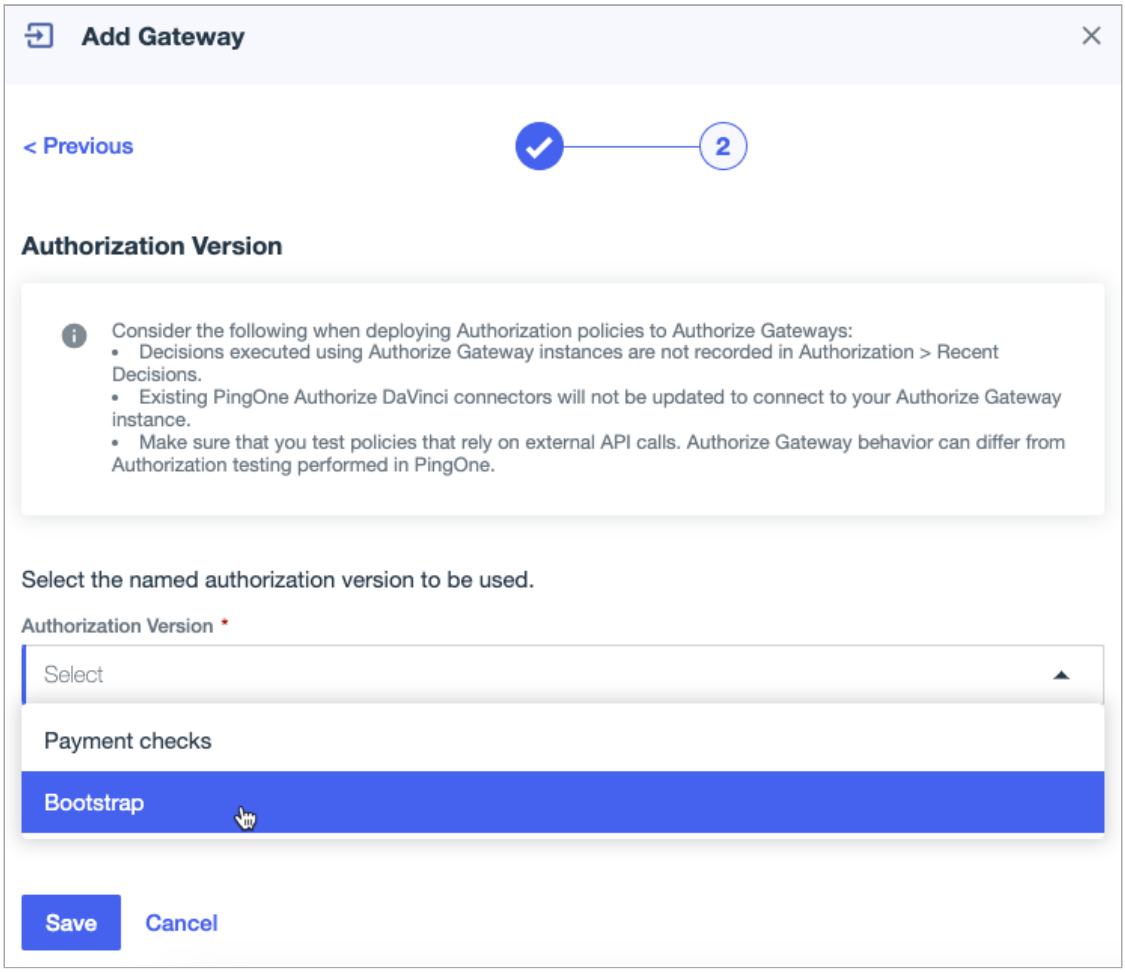


2. Enter the following:
   - **Name**: A name for the gateway. The name must be unique in this environment.
   - **Gateway Type**: Select **Authorize**.
   - **Description** (optional): A brief description of the gateway.
3. Click **Next**.
4. Select an **Authorization Version**.

   This is the policy and Trust Framework configuration that will be published to gateway instances and used to make authorization decisions. Each gateway instance associated with this Authorize gateway will use this authorization version.

   If you haven't set up policies and the Trust Framework yet, select **Bootstrap**.

Copyright © 2025 Ping Identity Corporation



5. Click **Save**.

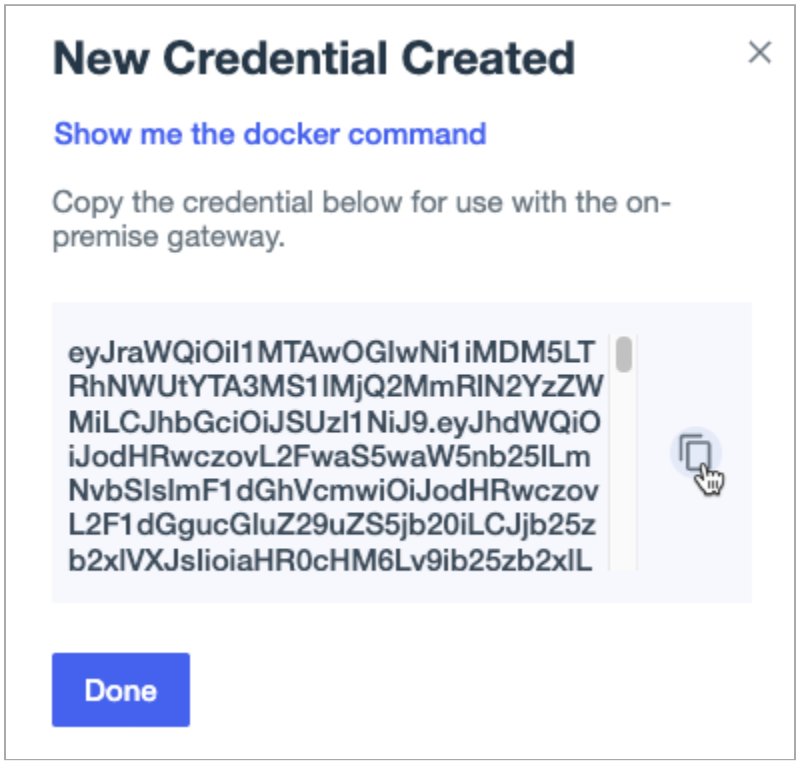
   PingOne generates a gateway credential. The gateway instance in your organization's infrastructure uses this credential to authenticate with PingOne.

   > **Important**
   >
   > A gateway credential is like a password, so keep it protected. For security reasons, PingOne does not store generated gateway credentials, but you can always create a new one in PingOne.
   > Multiple gateway instances can use the same gateway credential, and the credential doesn't expire.
   > To revoke a credential, click the **Delete** icon.

6. Copy the credential and save it in a secure location for later use.

   You'll use the credential later to connect gateway instances to PingOne.

Copyright © 2025 Ping Identity Corporation

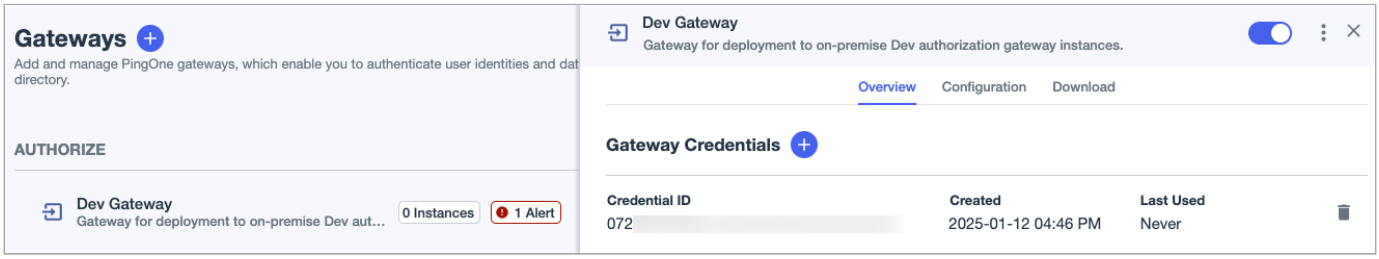


7. Click **Show me the Docker command** and copy the command to a secure location.

   You'll use the Docker command later to start a gateway instance.

8. Click **Done**.

   Your new Authorize gateway displays an alert reminding you that no gateway instances are connected yet.

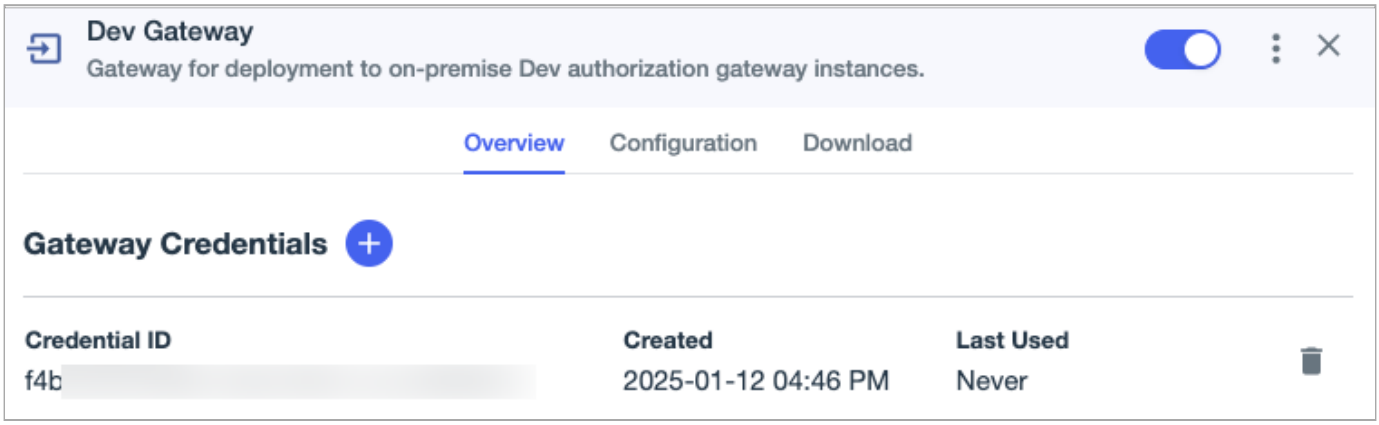


Result

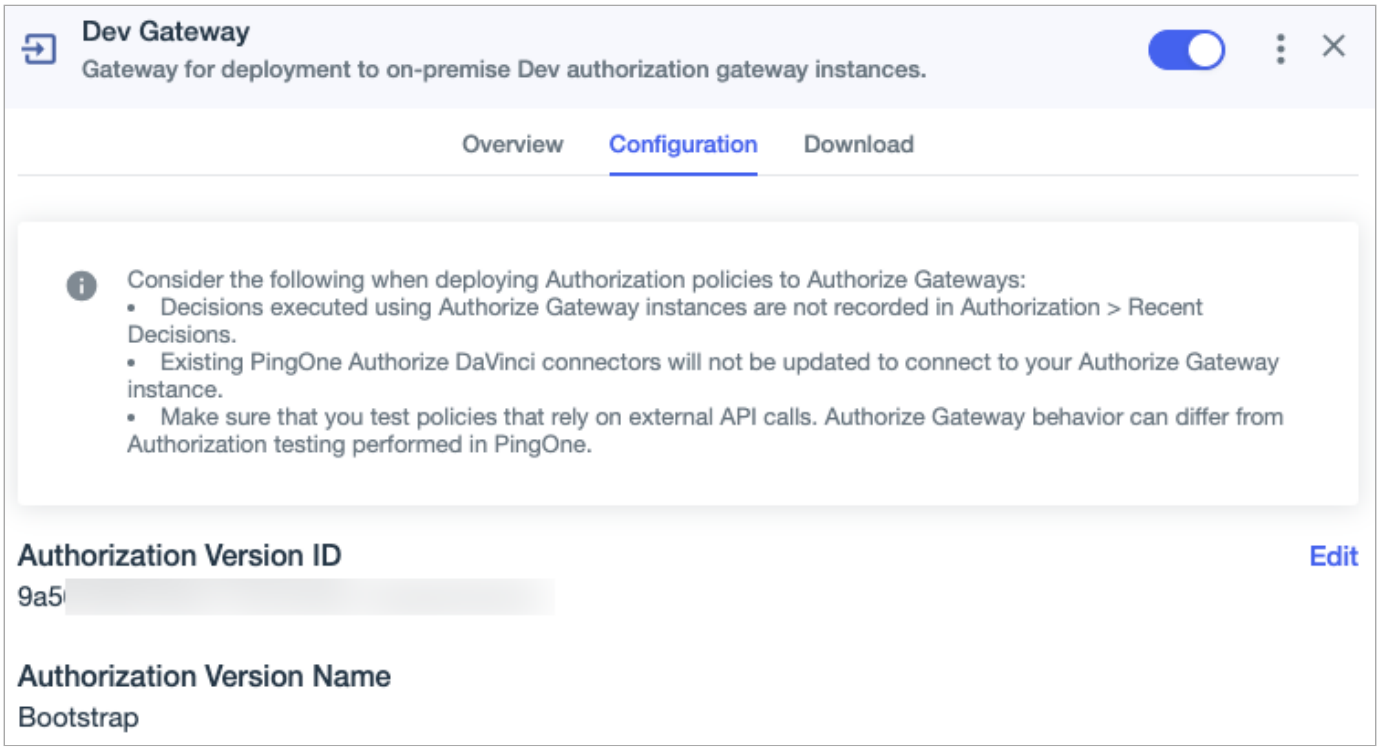
Explore the settings available for your new gateway:

- Header area: The toggle next to the gateway name allows you to enable or disable the gateway. Use the **More Options** (⋮) icon to edit gateway settings or delete the gateway.
- **Overview** tab: Allows you to add or delete gateway credentials. After you start a gateway instance, this tab also shows you the status and version of your gateway instances.

Copyright © 2025 Ping Identity Corporation

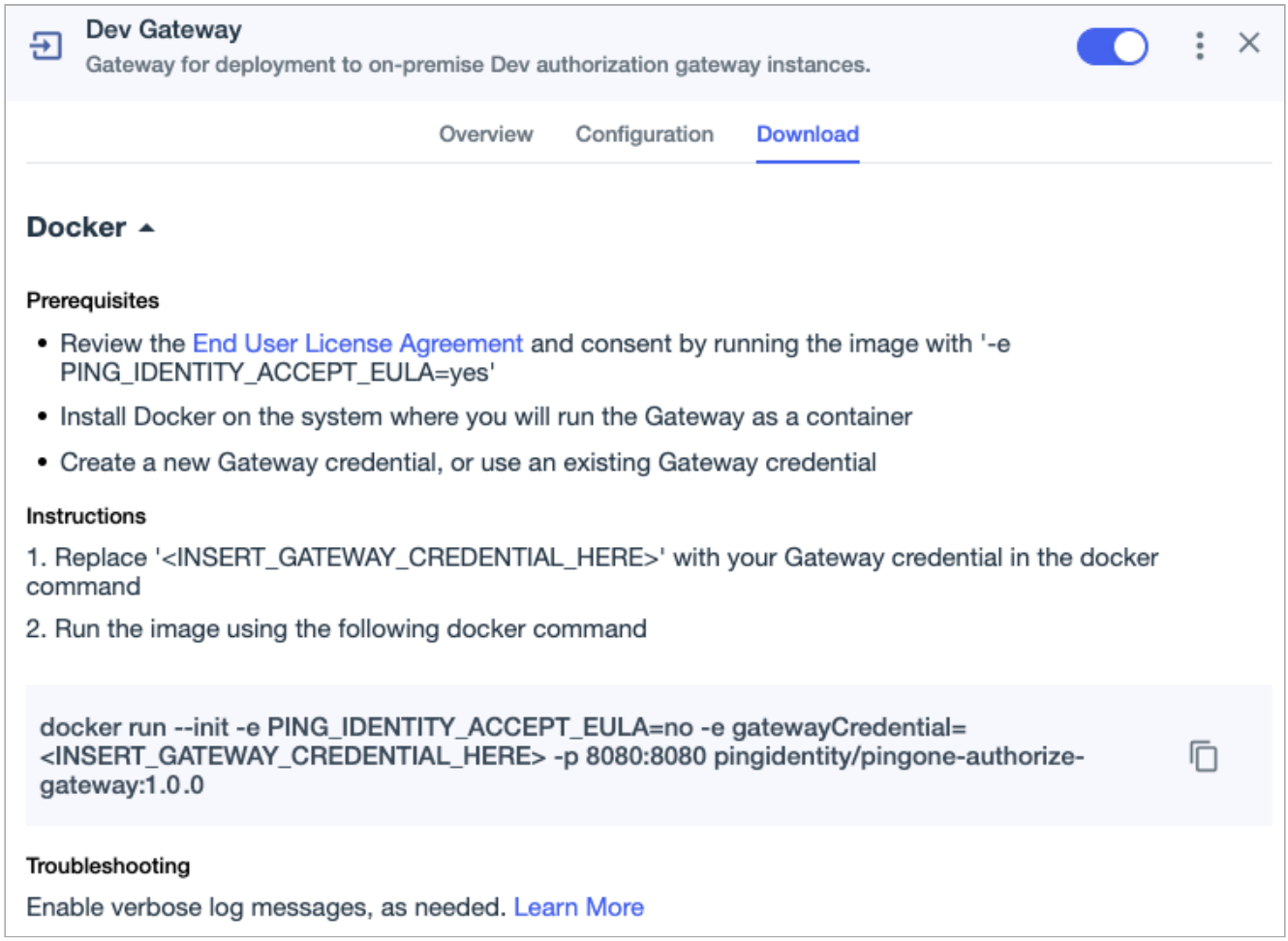


- **Configuration** tab: Allows you to edit the policy and Trust Framework version deployed to gateway instances.



- **Download** tab: Provides instructions and a command for running the gateway as a Docker container.

Copyright © 2025 Ping Identity Corporation



Next steps

Starting an Authorize gateway instance.

Starting an Authorize gateway instance

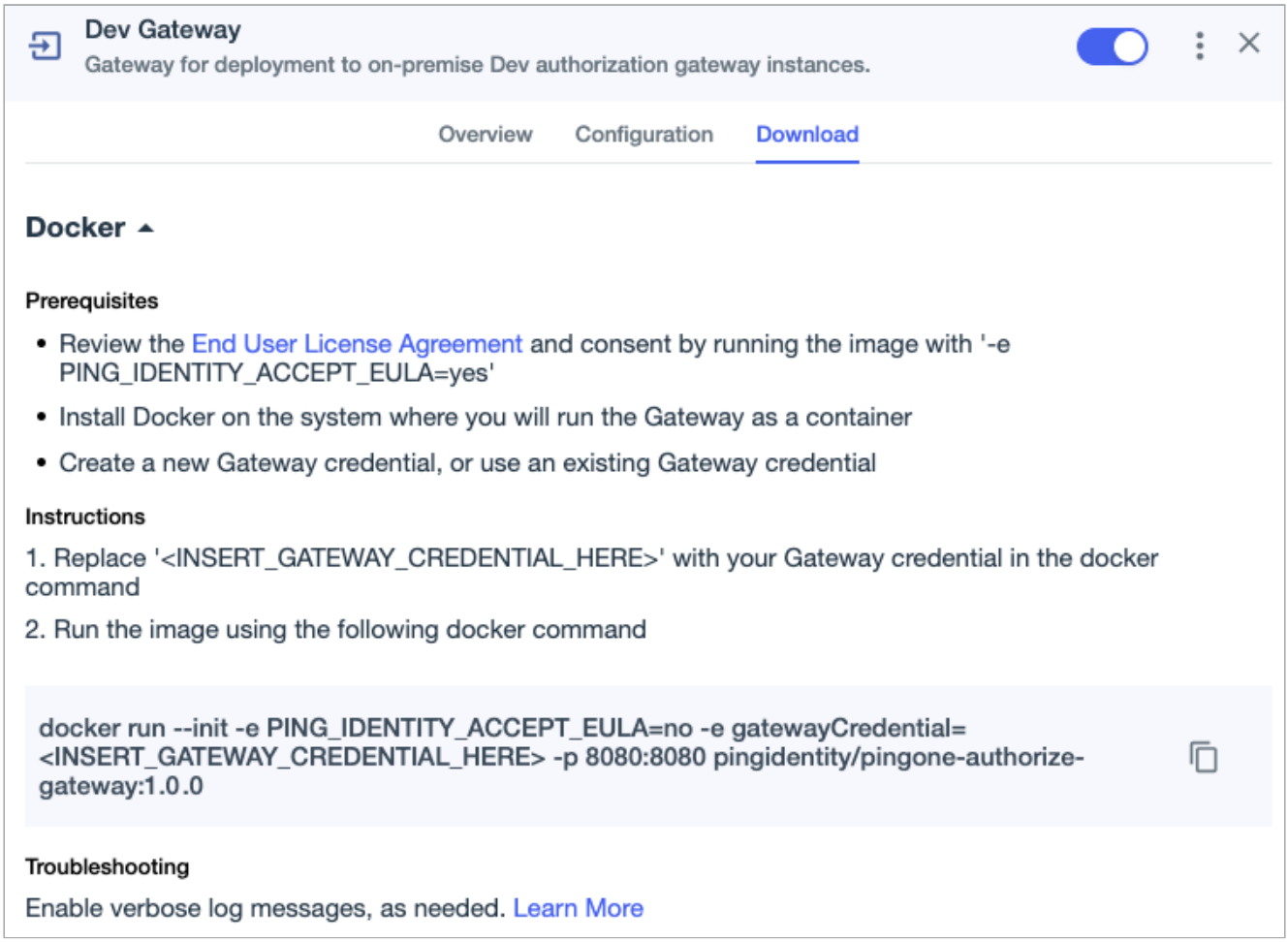
Follow these steps to deploy and start an Authorize gateway instance in your infrastructure.

Gateway instances evaluate policy versions published from PingOne in order to make authorization decisions. Gateway instances are distributed as containerized images, and they maintain a WebSocket connection with the PingOne platform.

> **Important**
>
> Make sure you install gateway instances on a system that can reach PingOne and any information points that will be used for authorization decisions.

To start a gateway instance, you'll use the Docker command that you copied earlier on the Authorize gateway **Download** tab.

Copyright © 2025 Ping Identity Corporation



Before you begin

- Ensure that Docker is installed and the Docker Engine is running.
- Review the end user license agreement at www.pingidentity.com/en/legal/subscription-agreement.html.

Steps

1. In the Docker command that you copied in step 7 of Adding an Authorize gateway, consent to the license agreement by changing `no` to `yes`:

   ```
   -e PING_IDENTITY_ACCEPT_EULA=yes
   ```

2. Replace `<INSERT_GATEWAY_CREDENTIAL_HERE>` with the gateway credential that you copied in step 6 of Adding an Authorize gateway.

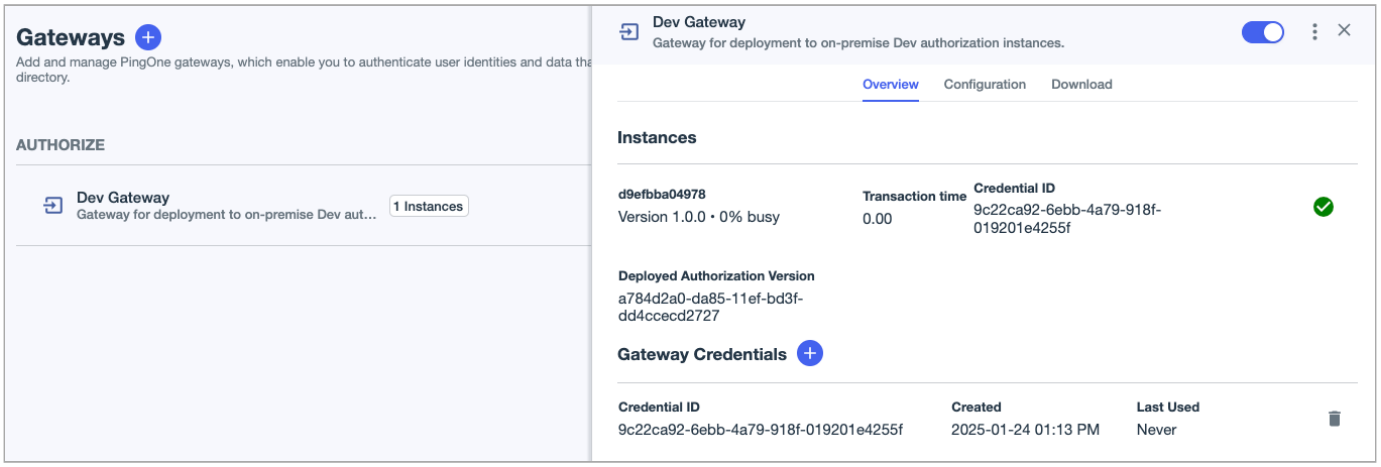
   The command should look something like this (line breaks are included for readability and are not necessary in your command):

   ```
   docker run --init \
     -e PING_IDENTITY_ACCEPT_EULA=yes \
     -e gatewayCredential=<your-gateway-credential> \
     -p 8080:8080 pingidentity/pingone-authorize-gateway:1.0.0
   ```

Copyright © 2025 Ping Identity Corporation

3. Run the command.

   The container starts and you have a connected gateway instance.



> **Note**
>
> If the gateway instance can't connect to PingOne, it won't start.

Next steps

- Start additional gateway instances in your infrastructure as needed for your organization's use cases. You can use multiple gateway instances to help handle traffic spikes, ensure high availability by avoiding a single point of failure, and for geographical distribution.
- Publishing policy versions to Authorize gateway instances.

Verifying an Authorize gateway instance

After you start a gateway instance, ensure that the gateway can connect to PingOne.

> **Important**
>
> When a gateway instance connects to PingOne, it stores configuration information in your organization's infrastructure. If the gateway instance loses its connection to PingOne, it uses stored configuration information to start up and might not be using the latest configuration version.

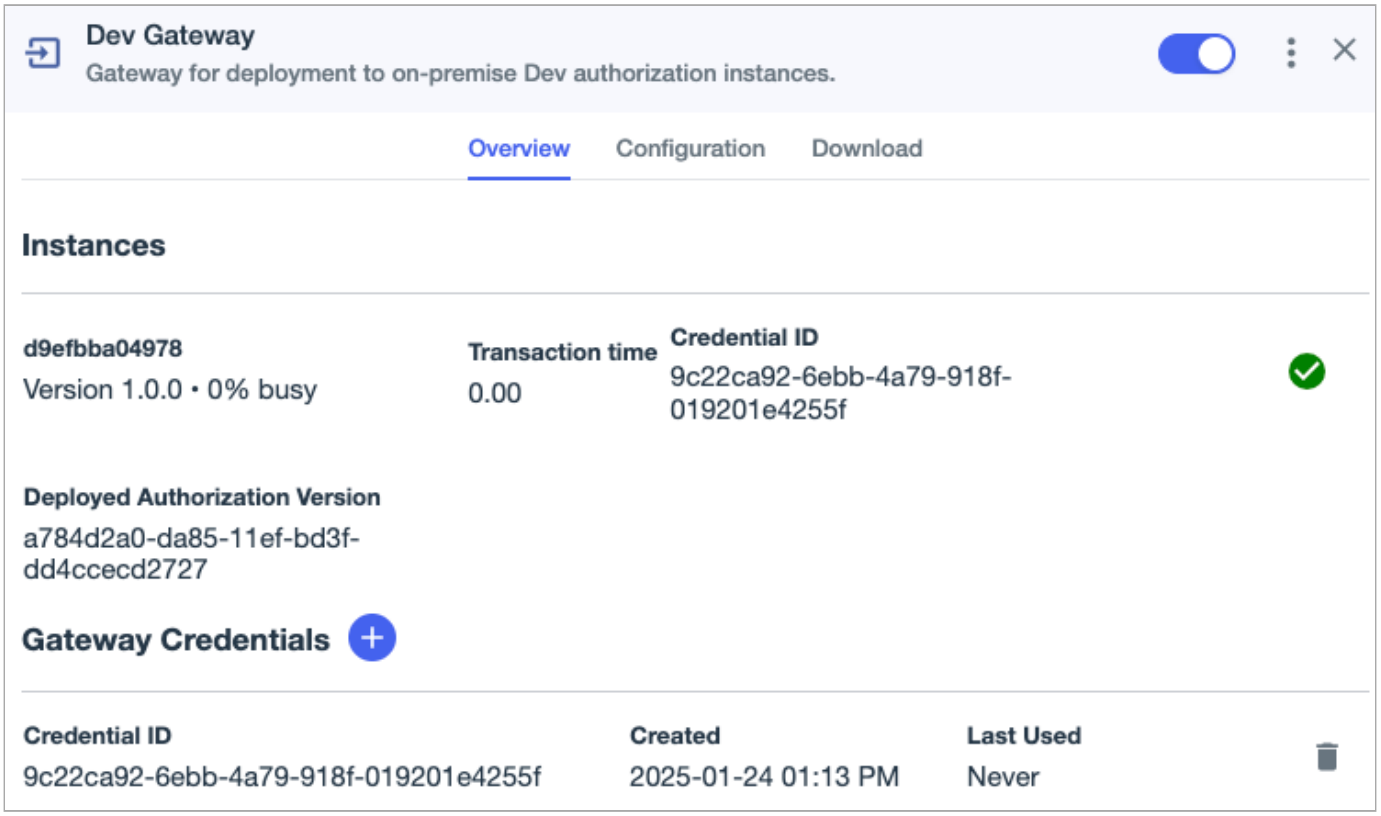
Steps

1. In the PingOne admin console, go to **Integrations** > **Gateways** and select the appropriate gateway.

   > **Note**
   >
   > You can refresh the **Gateways** page to ensure that the information is current.

2. Review gateway details to ensure that the gateway instance is healthy.

Copyright © 2025 Ping Identity Corporation



Configuring an Authorize gateway instance

Customize the environment and behavior of the gateway instance to suit your business needs.

Use the Docker `run` command or Docker Compose to pass configuration information to your gateway instance. You can configure decision logging, authentication, and service caching.

Copyright © 2025 Ping Identity Corporation

Docker run

Use the Docker `run` command

Steps

1. Stop the gateway instance container.
2. Using the `SPRING_APPLICATION_JSON` environment variable, modify the **`docker run`** command to include the relevant configuration object.

   For example, to configure decision logging for the gateway instance, the command should look something like this (line breaks are included for readability and are not necessary in your command):

   ```
   docker run --init \
     -e PING_IDENTITY_ACCEPT_EULA=yes \
     -e gatewayCredential=<your-gateway-credential> \
     -e SPRING_APPLICATION_JSON='{"decision-logging":[{"name":"debugLog","details":
   ["decisionTree"],"logged-attributes":["Amount"],"log-format":"%date{yyyy-MM-
   dd'\''T'\''HH:mm:ss.SSSXXX,UTC} [%logger] %msg%n"}]}' \
     -p 8080:8080 pingidentity/pingone-authorize-gateway:1.0.0
   ```

   Learn more about starting a gateway instance.

3. Run the command.

   The container starts with the relevant configuration enabled for the gateway instance.

Copyright © 2025 Ping Identity Corporation

Docker Compose

Use Docker Compose

With Docker Compose, you can manage the Docker application by configuring the application's services, networks, and volumes in a single, comprehensible YAML file. You can also start and stop all managed services with the **`docker compose up`** and **`docker compose down`** commands, respectively.

1. Stop the gateway instance container.
2. In the host server, create a `docker-compose.yml` file.

   For example:

   ```
   touch docker-compose.yml
   ```

   Learn more in the Docker Compose documentation.

3. In the newly created `docker-compose.yml` file, use the `environment.SPRING_APPLICATION_JSON` variable to pass in the relevant configuration object.

   For example, to configure decision logging for the gateway instance, the `docker-compose.yml` file should look something like this:

   ```
   services:
     authorize-gateway:
       image: pingidentity/pingone-authorize-gateway:1.0.0
       init: true
       environment:
         PING_IDENTITY_ACCEPT_EULA: "yes"
         gatewayCredential: <your-gateway-credential>
         SPRING_APPLICATION_JSON: |
           {
             "decision-logging": [
               {
                 "name": "debugLog",
                 "details": ["decisionTree"],
                 "logged-attributes": ["Amount"],
                 "log-format": "%date{yyyy-MM-dd'T'HH:mm:ss.SSSXXX,UTC} [%logger] %msg%n"
               }
             ]
           }
       ports:
         - "8080:8080"
   ```

4. From your gateway instance directory, start the application by running **`docker compose up`**.

   The container starts with the relevant configuration enabled for the gateway instance.

   Learn more about the Docker Compose CLI in How Compose works in the Docker Compose documentation.

Copyright © 2025 Ping Identity Corporation

Configuring multiple Authorize gateway instances

For high-availability applications or scalability, you can configure multiple gateway instances. You can then run the Docker container on multiple servers.

When multiple gateway instances are connected to PingOne, PingOne maintains a list of the active connections for each gateway. If a gateway instance isn't available, it's excluded from the list of active gateway instances.

You can set up an Authorize gateway with one gateway credential and have multiple gateway instances share the same credential. If necessary, you can remove the credential from the Authorize gateway to stop all gateway traffic. Removing the credential breaks the connection to PingOne, but it doesn't stop gateway instances or stop authorization requests from being served.

When there's no connection to PingOne, gateway instances continue to run with the last successful gateway configuration. Any new authorization versions won't be deployed to gateway instances that used the deleted credential.

> **Tip**
>
> Best practice is to use a different credential for each gateway instance. Using different credentials allows you to easily revoke access to individual gateway instances.

Authentication for Authorize gateway endpoints

To enhance security for certain endpoints, the gateway instance can enforce client authentication using a shared secret.

Shared secrets are enforced per gateway instance and not shared between instances. To define a shared secret, use one of the available configuration methods to pass the authentication JSON object to your gateway instance.

Example `authentication` object:

```
{
  "authentication": {
    "type": "sharedsecret",
    "keys": ["example-secret-key"]
  }
}
```

Configuration properties for the `authentication` object:

- `type` : A constant set to `sharedsecret` .
- `keys` : An array containing shared secrets as strings.

> **Note**
>
> Secret keys must be at least 128 bits.

To avoid service interruptions, the gateway instance allows authenticated endpoints to accept multiple, distinct shared secrets at the same time. This allows time to update the gateway instance's configuration to use a new shared secret.

For example:

Copyright © 2025 Ping Identity Corporation

```
{
  "authentication": {
    "type": "sharedsecret",
    "keys": ["example-secret", "example-secret-2"]
  }
}
```

After it's enabled, the gateway instance will require authentication for the following endpoints:

- `/api/authorize`
- `/actuator/state`
- `/actuator/metrics`
  - `/actuator/metrics/*`

Any request made to these endpoints must provide the configured shared secret with the `Authorization` header.

For example:

```
curl --location 'http://localhost:8080/api/authorize' \
  --header 'Authorization: Bearer example-secret' \
  --header 'Content-Type: application/json' \
  --data '
{
  "parameters": {
    "Amount": "990",
    "Account": "Basic checking",
    "Payment.consentId": "{{consentID}}"
  }
}'
```

> **Note**
>
> If you have defined multiple shared secrets for secret rotation, the `Authorization` header can include any of these secrets.

Authentication is not supported for the following endpoints:

- `/actuator`
- `/actuator/health`
  - `/actuator/health/liveness`
  - `/actuator/health/readiness`

Service caching for Authorize gateway instances

Caching improves decision evaluation performance and reduces latency by storing data retrieved from services for faster retrieval on subsequent service requests.

Copyright © 2025 Ping Identity Corporation

You can configure gateway instances with a Redis cache. Single instance and cluster (including AWS ElastiCache) Redis modes are supported.

> **Note**
>
> Redis Sentinel isn't supported.

Service caching uses a two-level cache to improve performance and minimize redundancy. A local in-memory cache acts as the level-one cache and the Redis instance acts as the level-two cache. When making a call to a service, the gateway instance tries to load the level-one cache entry. If the entry isn't found, the gateway instance calls the level-two cache. If no entry is found on either level, the gateway instance calls the service itself.

Cached values are per gateway instance and not shared between instances, but you can use the same Redis instance to point towards the same level-two cache. You cannot clear the in-memory cache manually.

Logging is provided for Redis cache connection status and health.

Service caching configuration

Using one of the available configuration methods, pass the `caching` JSON object into your gateway instance.

Example `caching` object:

```
{
  "caching": {
    "external": {
      "redis": {
        "uri": "redis://localhost:6379/0",
        "mode": "SINGLE_INSTANCE",
        "auth": {
          "username": "admin",
          "password": "password"
        }
      }
    }
  }
}
```

Configuration properties for the `caching` object:

Property	Description
`uri`	Required. Specifies connection details. In `CLUSTER` mode, all Redis instances are discovered automatically when you provide the URI for the master instance. For AWS ElastiCache, use `CLUSTER` mode and provide the ElastiCache address.

Copyright © 2025 Ping Identity Corporation

Property	Description
`mode`	Required. Specifies the Redis mode. Accepted values are `SINGLE_INSTANCE` or `CLUSTER`.
`auth`	Required only for `SINGLE_INSTANCE` mode. Specifies `username` and `password` authentication credentials.

Creating or deleting an Authorize gateway credential

PingOne automatically creates a gateway credential when you add a gateway, but you can create additional credentials at any time. You can also delete a gateway credential.

About this task

> **Important**
>
> For optimal security, you should rotate gateway credentials periodically.

Steps

1. In the PingOne admin console, go to **Integrations** > **Gateways**.
2. To add a gateway credential:
    1. Click the appropriate gateway to display gateway details.
    2. On the **Overview** tab, click the **+** icon next to **Gateway credentials**.
    3. Verify that the credential was created and copy it to a secure location.

    > **Important**
    >
    > The credential is shown in the console only once. If necessary, you can retrieve existing credentials through the `Gateway Management API`. Learn more in Gateway Management in the PingOne Platform API Reference.

    4. Click **Done**.

    Result:

    The new credential is added to the list with a unique ID.
3. To delete a gateway credential:
    1. On the **Gateways** page, click the gateway that has the credential you want to delete.
    2. On the **Overview** tab, click the **Delete** icon (🗑) icon next to the credential.
    3. Select the **I understand and want to continue** checkbox.
    4. Click **Revoke**.

    After a credential is revoked, the gateway cannot use the credential to access PingOne.

Copyright © 2025 Ping Identity Corporation

Upgrading an Authorize gateway instance

Take advantage of new policy features and enhancements by upgrading your gateway instance.

Deployment of policy versions to gateway instances could fail if the policy version includes features that aren't compatible with or supported by the current gateway instance version. When an attempt is made to deploy a policy version not supported by the gateway instance, the Docker container console for that instance logs a message such as:

```
Supported config versions are [1.0…1.0] but deployment of 2.0 was attempted
```

Upgrading a gateway instance ensures policy version compatibility and minimizes downtime by updating components such as the application code, image, configuration, and associated services.

Learn more about best practices for publishing policy versions in Policies published to Authorize gateways.

> **Best practice**
>
> To ensure a successful upgrade process, do the following:
>
> - Test the upgrade in a staging or pre-production environment.
> - Back up data and configurations before starting the upgrade.
> - Use strategies like blue-green deployment or rolling updates to minimize downtime.

Use the Docker `run` command or Docker Compose to upgrade your gateway instance.

Copyright © 2025 Ping Identity Corporation

Docker run

Use the Docker `run` command

Steps

1. Stop the gateway instance container.
2. To remove the old container and ensure the new gateway instance is deployed, run the **`docker rm <container-name>`** command.
3. Modify the docker **`run`** command to include the new gateway instance version.

   For example, to upgrade the gateway instance to version 1.1.0, the command should look something like this (line breaks are included for readability and are not necessary in your command):

   ```
   docker run --init \
     -e PING_IDENTITY_ACCEPT_EULA=yes \
     -e gatewayCredential=<your-gateway-credential> \
     -p 8080:8080 pingidentity/pingone-authorize-gateway:1.1.0
   ```

   > **Note**
   >
   > Use the same port mappings, volumes, and environment variables that were used in the original **`docker run`** command to ensure the new container behaves the same way.

4. Run the command.

Copyright © 2025 Ping Identity Corporation

Docker Compose

Use Docker Compose

Before you begin

Make sure you have installed Docker Compose.

Steps

1. To stop the gateway instance container, run the **`docker compose down`** command.
2. Update the image tag in the `docker-compose.yml` file to the desired version.

   For example, to upgrade the gateway instance to version 1.1.0, the `docker-compose.yml` file should look something like this:

   ```
   services:
     authorize-gateway:
       image: pingidentity/pingone-authorize-gateway:1.1.0
       init: true
       environment:
         PING_IDENTITY_ACCEPT_EULA: "yes"
         gatewayCredential: <your-gateway-credential>
       ports:
         - "8080:8080"
   ```

3. To remove the old container and ensure the new gateway instance is deployed, run the **`docker compose rm`** command.
4. To start the upgraded gateway instance, run the **`docker compose up`** command.
5. To verify the upgraded gateway instance is running correctly, run the **`docker inspect <container-name>`** command and check the image version.

Next steps

Publish new policy versions to your gateway instance.

Deleting an Authorize gateway

Remove Authorize gateways that you no longer need.

Steps

1. In PingOne, go to **Integrations > Gateways**.
2. Click the **More Options** (⋮) icon next to the gateway you want to delete and select **Delete**.
3. Select the **I understand and have confirmed that this gateway is not in use** checkbox.
4. Click **Delete**.

Copyright © 2025 Ping Identity Corporation

Policies published to Authorize gateways

Keep the following points in mind as you build policies and the Trust Framework configuration that you plan to publish to Authorize gateways.

The following features are not currently supported for Authorize gateway deployments:

- Calls to gateway instances from the PingOne Authorize DaVinci connector
- API Access Management in PingOne Authorize
- The **Authorization Dashboard** doesn't track metrics for decisions made by gateway instances.

Policies

You can use many of the policy authoring features available in PingOne Authorize. However, the following features are not yet supported:

- The **Has Permissions**, **Is Member Of**, and **Is Not Member Of** condition comparators in policies and rules
- Attributes listed under **PingOne** on the **Attributes** tab, including **User** and **API Access Management** attributes
- The **PingOne User** and **PingOne User ID** resolvers in attributes

Information points

You can make calls to information points and on-premise services directly from gateway instances. When you set up an HTTP service in PingOne, use URLs for your local or private services instead of public URLs.

The following features are not supported:

- You can't use a **Connector** type service to provide risk information to gateway instances.
- When testing services, you can't test calls to your local or private services. However, you can use overrides to mock the service response.

Publishing policy versions to Authorize gateway instances

You can publish policy and Trust Framework versions to gateway instances through **Version History** in PingOne or you can use an Authorize gateway.

Publishing a version is like saving a snapshot of your policies and Trust Framework definitions. The published version reflects the state of these objects at a specific point in time. Learn more in Authorization version history.

> **Note**
>
> You can also publish policy versions to cloud-based decision endpoints. However, decision endpoints don't provide the data residency and reduced latency benefits of gateway instances deployed in your organization's infrastructure.

Each gateway instance that is associated with the same Authorize gateway uses the authorization version published to that gateway. When you publish a version to an Authorize gateway, the authorization version deployment configuration is downloaded and stored locally with the gateway instance in your infrastructure.

Copyright © 2025 Ping Identity Corporation

Important

Publishing could fail if policies include features that aren't compatible with gateway instances, such as version differences or unsupported features. Learn more in Policies published to Authorize gateways.

Before you begin

- Build your authorization policies in PingOne. Learn more in Policies.
- Set up an Authorize gateway.
- Start an Authorize gateway instance.

Copyright © 2025 Ping Identity Corporation

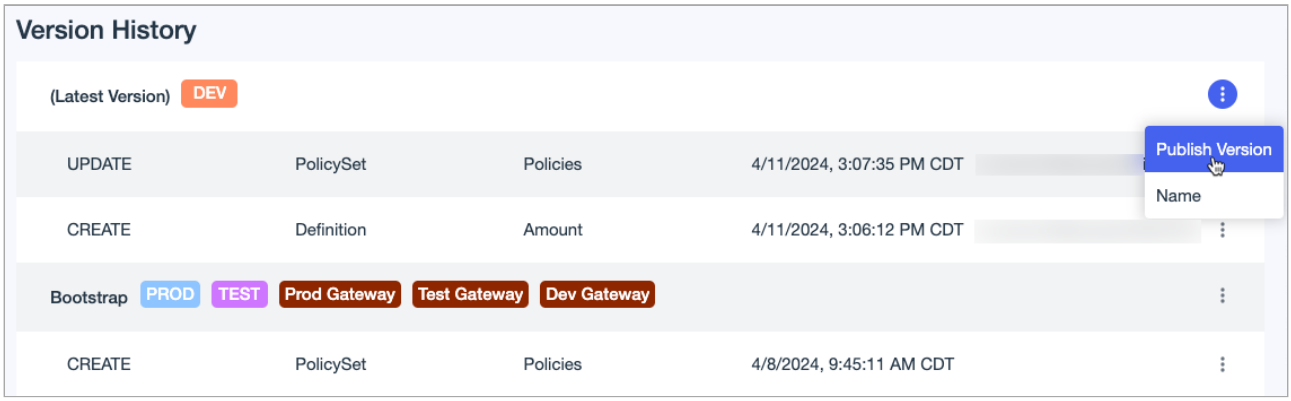
Version History

Publish a version in Version History

You can use **Version History** to publish authorization versions to gateway instances. This method enables you to view which versions are published to particular Authorize gateways.

Steps

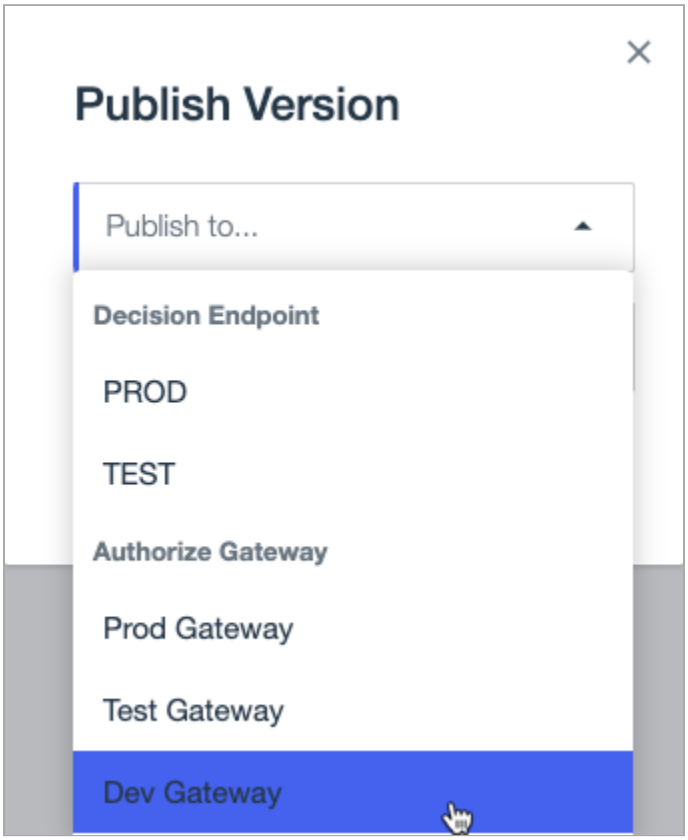
1. In the PingOne admin console, go to **Authorization > Version History**.
2. Click the **More Options** (⋮) icon next to the version you want to publish and select **Publish Version**.



In this example, the **Prod Gateway**, **Test Gateway**, and **Dev Gateway** Authorize gateways were created using the **Bootstrap** authorization version. You can also see that the **Prod** and **Test** cloud-based decision endpoints use the **Bootstrap** version, and that the **Dev** decision endpoint uses the latest policy version by default. You'll publish versions to Authorize gateways and not to cloud-based decision endpoints.

3. In the **Publish to** list, select an Authorize gateway.

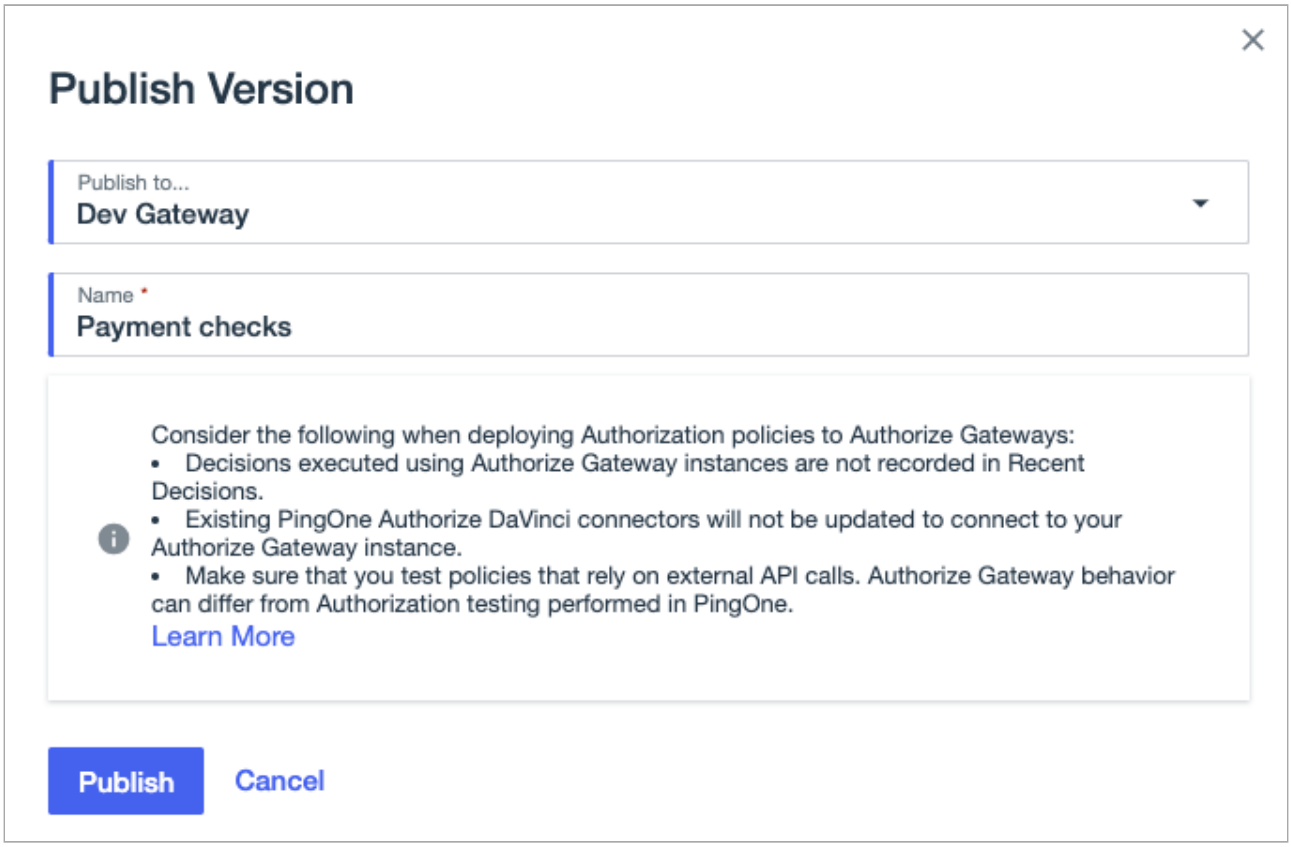
Copyright © 2025 Ping Identity Corporation



4. If you're publishing the latest version, which is unnamed, enter a **Name** that makes the version easy to identify.

   If you're publishing a version that's already named, you can use the existing name or change it.

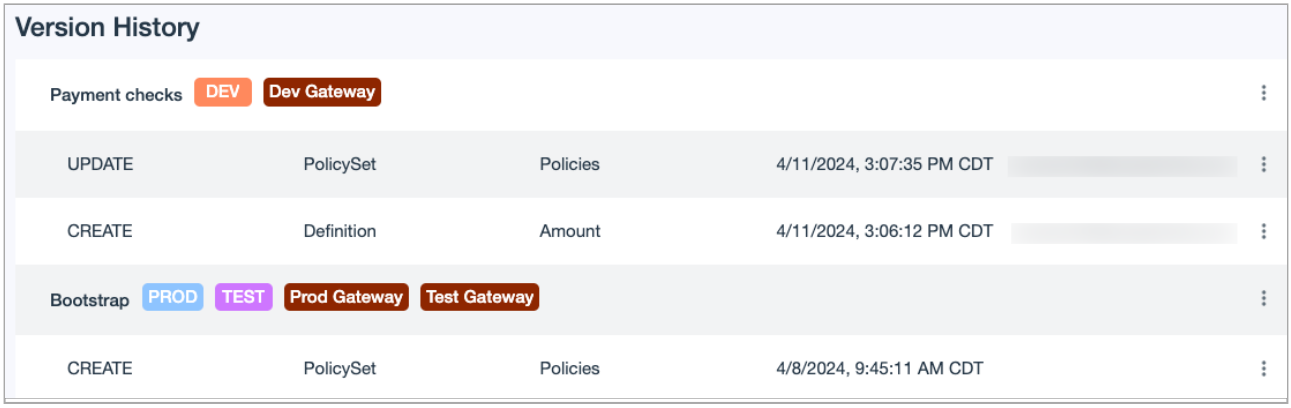
Copyright © 2025 Ping Identity Corporation



5. Click **Publish**.

   Result:

   The latest version is renamed and it is now published to the **Dev Gateway**, in addition to the **Dev** decision endpoint.



Copyright © 2025 Ping Identity Corporation

Authorize gateway

Select a version in an Authorize gateway

This method for publishing authorization versions to gateway instances provides a convenient way to change the version when you're editing a gateway.

Steps

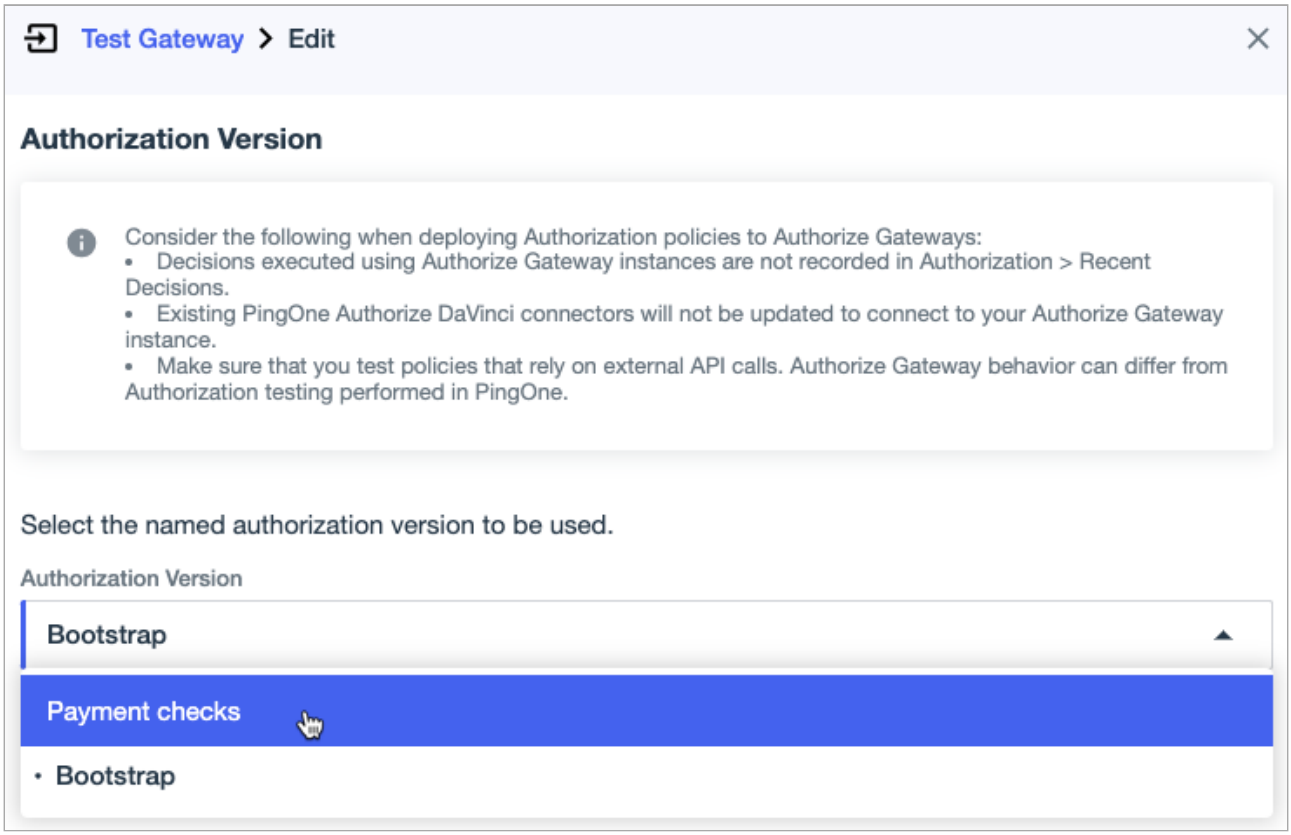
1. In the PingOne admin console, make sure that you've named an authorization version.

   As an example, you'll use the **Payment checks** version that you just published to the **Dev Gateway** and promote it to the **Test Gateway**.

2. Go to **Integrations** > **Gateways** and click the Authorize gateway you want to work with.

3. On the **Configuration** tab, click **Edit**.

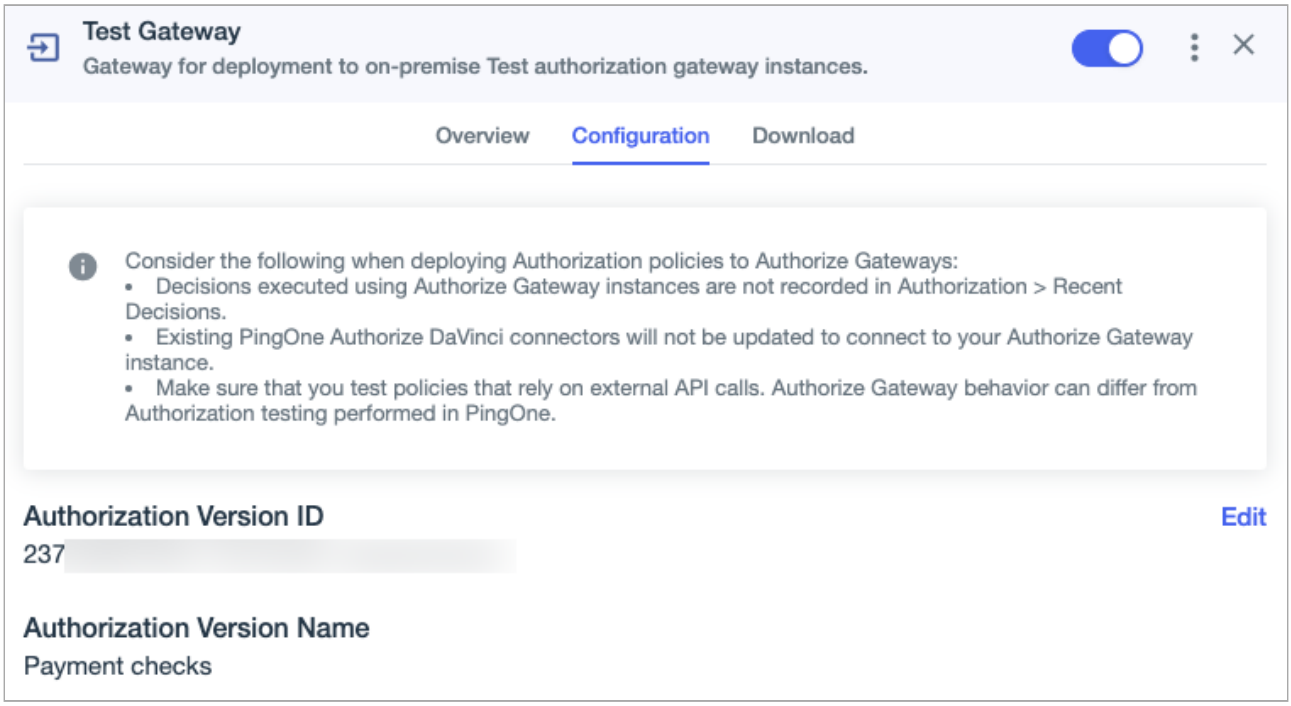
4. Select an **Authorization Version**.



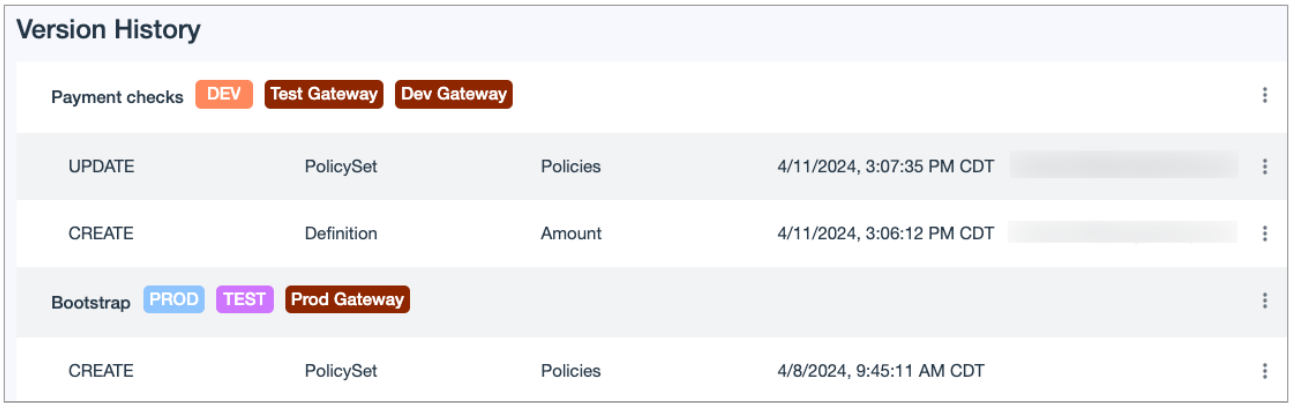
5. Click **Save**.

   This updates the authorization version that the gateway will download and deploy to any associated gateway instances.

Copyright © 2025 Ping Identity Corporation



Version History also reflects which policy version the Authorize gateway is using.



Making decision requests to Authorize gateway instances

Before you make decision requests to gateway instances in your organization's infrastructure, ensure that you've completed steps 1 - 5 in Setting up an Authorize gateway.

Use the `POST localhost:8080/api/authorize` operation to execute a decision request against a gateway instance. You can enforce client authentication on the `/api/authorize` endpoint by configuring a shared secret. Learn more in Authentication for Authorize gateway endpoints.

The request body requires the `parameters` property. Parameters consist of an attribute name and value separated by a colon. For example:

Copyright © 2025 Ping Identity Corporation

```
{
    "parameters": {
        "Amount": "990",
        "Account": "Basic Checking",
        "Payment.consentId": "{{consentID}}"
    },
}
```

Example request

```
curl --location 'http://localhost:8080/api/authorize' \
  --header 'Authorization: Bearer example-secret' \
  --header 'Content-Type: application/json' \
  --data '
{
  "parameters": {
    "Amount": "990"
  }
}'
```

Example response

```
{
   "id": "13234d13-7cc5-4394-a1a4-c685cbff4a5d",
   "authorizationVersion: {
       "id": "2027cfbe-4fcc-46f8-9c2f-d1f34983a43f"
    },
   "timestamp": "2024-04-25T21:56:53.572691726Z",
   "elapsedMicroseconds": 409,
   "status": {
       "code": "OKAY"
   },
   "decision": "PERMIT"
}
```

Visualizing decisions made by Authorize gateway instances

As part of the policy development and debugging process, you can examine recent decisions executed by gateway instances.

During policy development and testing, you can examine the decision flow and other details about recent decisions to make sure the gateway instance is evaluating policies according to your expectations.

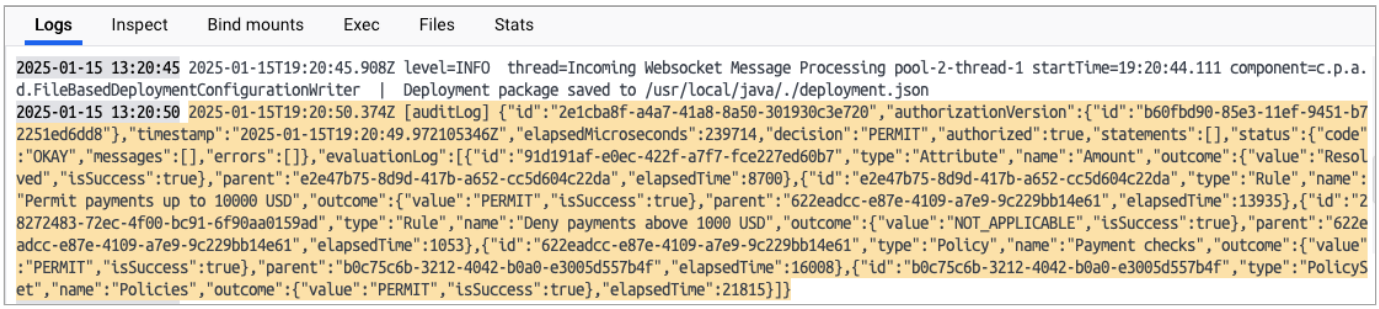
> **Note**
>
> In addition to examining authorization decisions, you can define cloud-based test scenarios on the **Test** tab to test your policies.

Steps

1. In Docker Desktop, go to **Containers** and select your gateway instance.

Copyright © 2025 Ping Identity Corporation

2. Click the **Logs** tab and copy the decision audit log entry that you want to visualize.



3. In the PingOne admin console, go to **Authorization > Policies**.

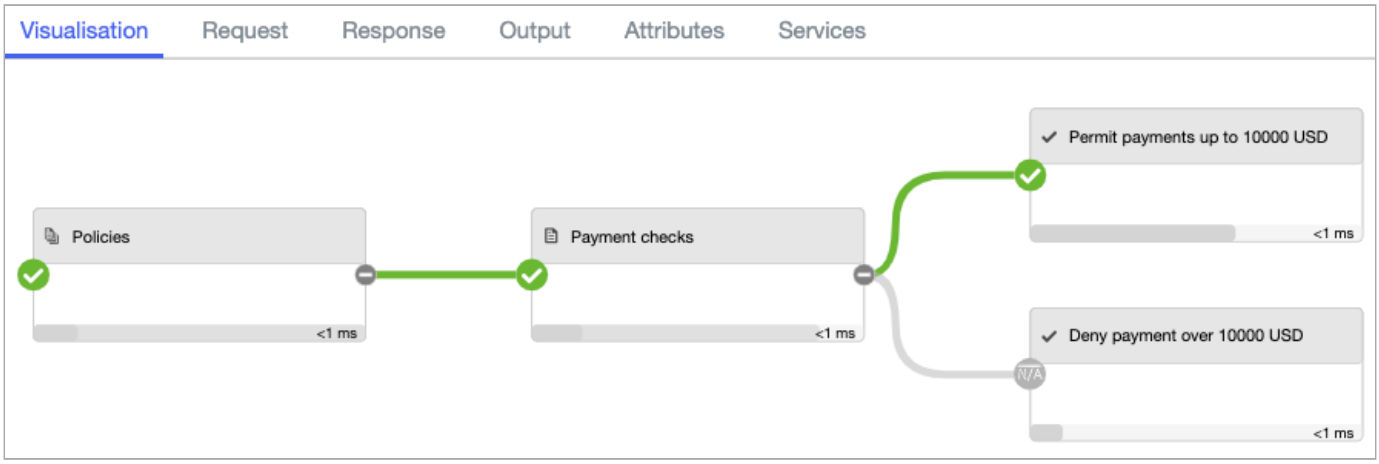
4. Click the **Decision Visualizer** tab.

5. In the **Paste Logs** field, paste the decision response from the gateway instance.

6. Click **Visualize**.

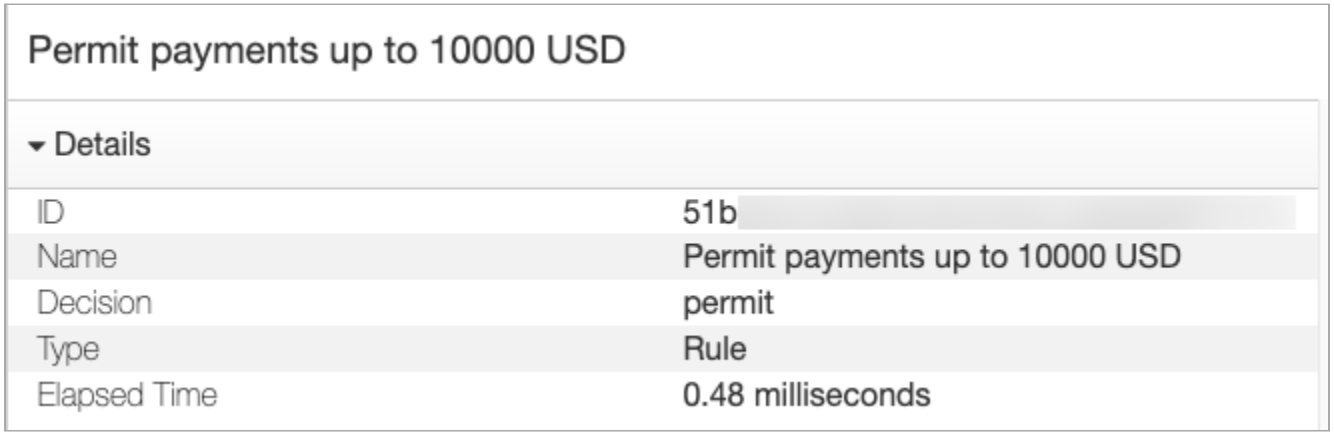
   On the **Visualization** tab, examine the decision flow to make sure decisions are evaluated according to your expectations.

Copyright © 2025 Ping Identity Corporation



7. Click a box in the flow to show more details.

   This example represents a rule that permits payments up to 10,000 USD. The decision evaluated as `permit` and took 0.48 milliseconds.



Permit payments up to 10000 USD

Details

ID	51b
Name	Permit payments up to 10000 USD
Decision	permit
Type	Rule
Elapsed Time	0.48 milliseconds

   Boxes in the decision flow don't include information about statements attached to the policy or rule outcome.

8. Click the other tabs for additional details:

   - **Request** tab: Shows the JSON request sent to the gateway instance, allowing you to confirm that the expected information was sent.

     To view details on this tab, include the request view in your decision log configuration.

   - **Response** tab: Shows the response for the decision.

     The `evaluationLog` field records the attributes and the outcome of each policy and rule used to produce the final decision response.

   - **Output** tab: Shows the time taken to evaluate each policy set, policy, and rule used in the final decision.

   - **Attributes** tab: Shows details about the attributes used in the decision.

   - **Services** tab: Shows details about the services used in the decision.

     To view details on this tab, include the services view in your decision log configuration.

Copyright © 2025 Ping Identity Corporation

Logging for Authorize gateway instances

Configure decision and service logging to help manage, troubleshoot, and optimize your Authorize gateway policies.

Decision logging

Decision logging provides detailed insights into how an Authorize gateway instance evaluates requests and makes decisions.

By default, decision log entries are written to the Docker container's console and include high-level details about attributes, services, and policy elements evaluated in the decision.

For example:


```
2025-01-15T19:20:50.374Z [auditLog]
{
  "id":"2e1cba8f-a4a7-41a8-8a50-301930c3e720",
  "authorizationVersion":{"id":"b60fbd90-85e3-11ef-9451-b72251ed6dd8"},
  "timestamp":"2025-01-15T19:20:49.972105346Z",
  "elapsedMicroseconds":239714,
  "decision":"PERMIT",
  "authorized":true,
  "statements":[],
  "status":{"code":"OKAY","messages":[], "errors":[]}
  "evaluationLog":[{"id":"91d191af-e0ec-422f-a7f7-
fce227ed60b7","type":"Attribute","name":"Amount","outcome":
{"value":"Resolved","isSuccess":true},"parent":"e2e47b75-8d9d-417b-a652-cc5d604c22da","elapsedTime":8700},
{"id":"e2e47b75-8d9d-417b-a652-cc5d604c22da","type":"Rule","name":"Permit payments up to 10000
USD","outcome":{"value":"PERMIT","isSuccess":true},"parent":"622eadcc-e87e-4109-
a7e9-9c229bb14e61","elapsedTime":13935},{"id":"28272483-72ec-4f00-
bc91-6f90aa0159ad","type":"Rule","name":"Deny payments above 1000 USD","outcome":
{"value":"NOT_APPLICABLE","isSuccess":true},"parent":"622eadcc-e87e-4109-a7e9-9c229bb14e61","elapsedTime":
1053},{"id":"622eadcc-e87e-4109-a7e9-9c229bb14e61","type":"Policy","name":"Payment checks","outcome":
{"value":"PERMIT","isSuccess":true},"parent":"b0c75c6b-3212-4042-b0a0-e3005d557b4f","elapsedTime":16008},
{"id":"b0c75c6b-3212-4042-b0a0-e3005d557b4f","type":"PolicySet","name":"Policies","outcome":
{"value":"PERMIT","isSuccess":true},"elapsedTime":21815}]
}
```


> **Note**
>
> To more easily consume logs, you can stream log data from the gateway instance to external destinations like Kafka or Splunk.

When developing and testing authorization policies published to gateway instances, you can configure the granularity of decision log views for enhanced visibility into which policies and rules were evaluated and which attributes or services were consumed in the process.

Copyright © 2025 Ping Identity Corporation

Decision logging configuration

Using one of the available configuration methods, pass the `decision-logging` JSON object into your gateway instance and override the default logging configuration.

Example `decision-logging` configuration object:

```
{
  "decision-logging": [
    {
      "name": "auditLog",
      "details": ["evaluationLog", "services", "request"],
      "logged-attributes": ["Amount","Payment.consentId"],
      "logFormat": "%date{yyyy-MM-dd'T'HH:mm:ss.SSSXXX,UTC} [%logger] %msg%n"
    }
  ]
}
```

Configuration properties for the `decision-logging` object:

- `name` (required): A unique name for the logger.

  Add this name to each log entry by including the `%logger` tag in the `log-format` configuration property.

- `details` (required): An array of logging views. Logging views determine the granularity of log entry data.

  You can include the following logging views in this array:

Logging view	Description
`request`	Includes the full decision request object.
`statements`	Includes any statements attached to the decision response.
`errors`	Includes any errors returned in the `status` field of the decision response.
`attributes`	Includes detailed resolution and value processing information for any attributes evaluated in the decision. By including this view, you can see attribute data after clicking the **Attributes** tab in the **Decision Visualizer**. Learn more in Visualizing decisions made by Authorize gateway instances.

Copyright © 2025 Ping Identity Corporation

Logging view	Description
`services`	Includes details for services invoked during policy evaluation. By including this view, you can see service data after clicking the **Services** tab in the Decision Visualizer. Learn more in Visualizing decisions made by Authorize gateway instances.
`evaluationLog`	Includes a list of policy elements evaluated in the decision.
`decisionTree`	Includes details for the evaluation flow of the policy tree.

> **Important**
>
> Selecting the `request`, `attributes`, or `services` logging views might log sensitive and personally identifiable information (PII). Enable these views only during testing and disable them afterward.

- `logged-attributes` (optional): An array of full names of attributes whose data type and value you want to be logged.

  If included, this property overrides configuration of the `attributes` logging view.

  > **Note**
  >
  > To obtain an attribute's full name, click the hamburger menu next to the attribute and select **Copy full name to clipboard**.

- `log-format` (optional): A string defining the format for log entries.

  If no format is specified, the log format defaults to `"%date{yyyy-MM-dd'T'HH:mm:ss.SSSXXX,UTC} [%logger] %msg%n"`.

  For example:

  ```
  2024-10-08-T22:16:51.239Z
  ```

  Learn more about customizing the log format in the logback documentation.

Examples

The following request asks whether the client is authorized to deposit 990 USD into a basic checking account:

Copyright © 2025 Ping Identity Corporation

```
curl --location 'http://localhost:8080/api/authorize' \
  --header 'Authorization: Bearer example-secret' \
  --header 'Content-Type: application/json' \
  --data '
{
  "parameters": {
    "Amount": "990",
    "Account": "Basic checking",
    "Payment.consentId": "{{consentID}}"
  }
}'
```

Given the above request and the `decisionTree` logging view configured, `debugLog` produces the following entry:

Copyright © 2025 Ping Identity Corporation

```
[2024-08-13 15:29:56,748]
{
  "id": "cda6fd43-e9ae-49de-b822-7479ef2f2b35",
  "deploymentPackageId": "42b99394-cbb0-46f9-8b9d-bca15cde330e",
  "timestamp": "2024-08-13T10:48:45.344117Z",
  "elapsedTime": 649161,
  "decision": "PERMIT",
  "authorised": true,
  "statements": [],
  "decisionTree": {
    "id": "9cf53282-0443-44a3-895a-1c413e190177",
    "nodeType": "PolicySet",
    "name": "Policies",
    "targets": [],
    "elapsedTime": 19914,
    "combiningAlgorithm": "FirstApplicable{}",
    "decision": "PERMIT",
    "attributes": {
        "Amount": {
            "id": "1a89a7b2-6034-48fa-ad45-6bb68e454bb5",
            "name": "Amount",
            "successful": "true",
            "elapsedTime": 0,
            "value": "permit",
            "type": "NUMBER"
        }
    }
    "applicableChildren": {
      "Payment checks": {
        "id": "014fa703-b5a4-4820-8744-2cb0c715fcfd",
        "nodeType": "Policy",
        "name": "Payment checks",
        "sequence": 1,
        "targets": [],
        "elapsedTime": 14765,
        "combiningAlgorithm": "FirstApplicable{}",
        "decision": "PERMIT",
        "applicableChildren": {
          "Permit payments up to 1000 USD": {
            "id": "1b9fd38e-5713-48f4-9bf1-5ea8d7b98493",
            "nodeType": "Rule",
            "name": "Permit payments up to 1000 USD",
            "sequence": 1,
            "targets": [],
            "elapsedTime": 13637,
            "decision": "PERMIT",
            "condition": {
              "less than or equal": {
                "lhs": {
                  "id": "1a89a7b2-6034-48fa-ad45-6bb68e454bb5",
                  "name": "Amount",
                  "value": 990,
                  "type": "NUMBER"
                },
```

```
                "rhs": {
                  "value": 1000,
                  "type": "NUMBER"
                }
              },
              "result": {
                "value": "true",
                "type": "BOOLEAN"
              }
            },
            "statements": []
          }
        },
        "statements": []
      }
    },
    "statements": []
  }
}
```

Using decision log entries, you can visualize the decision flow and other details about recent decisions to make sure the gateway instance is evaluating policies according to your expectations. Learn more in Visualizing decisions made by Authorize gateway instances.

> **Note**
>
> Although you can define multiple decision loggers, this isn't recommended for performance reasons.

Service call logging

When information points are slow to respond, it can lead to delays in evaluating policies or incorrect access decisions. Service call logs can help diagnose information point degradation by providing insight into service latency and availability.

By default, the Authorize gateway instance logs external service calls in the `SERVICE_AUDIT` component. The gateway instance will produce an additional log entry if the service response value is retrieved from a cache.

Examples

The following examples show `SERVICE_AUDIT` log entries for different types of service call results.

`HTTP 200; level=INFO`

The following example shows a `SERVICE_AUDIT` log entry for a successful HTTP service call:

```
2024-10-03T11:42:13.204Z level=INFO  thread=DefaultServiceExecution-Http Service-0 component=SERVICE_AUDIT
decisionRequestId=0e70aec0-ba0d-42a5-bfd9-673538b0a8be exchangeId=J9ggyeMm8utrLivF9fj-dw |  HTTP service
call: name=Payment Service, host=192.168.7.106, duration=14ms, configuredTimeout=2000ms, status=HTTP/1.1
200 OK
```

`HTTP 4XX, 5XX; level=INFO`

Copyright © 2025 Ping Identity Corporation

The following example shows a `SERVICE_AUDIT` log entry for an unsuccessful HTTP service call, due to a lack of authorization:

```
2024-10-03T11:47:48.280Z level=INFO  thread=DefaultServiceExecution-Http Service-0 component=SERVICE_AUDIT
decisionRequestId=a2bbdc25-5d15-4cfc-84b0-0ccf9378ce68 exchangeId=Yvg-p4Lyq2CKD2fsSHE7eQ |  Error invoking
HTTP service: name=Payment Service, host=192.168.7.106, duration=5ms, configuredTimeout=2000ms,
error=com.pingidentity.authorize.serviceexecution.ClientServiceExecutionException: Got unsuccessful status
code: 401, with body: {
  "message": "Unauthorized"
}
```

`HTTP 429; level=WARN`

The following example shows a `SERVICE_AUDIT` log entry for an unsuccessful HTTP service call, due to rate limits:

```
2024-10-03T11:45:50.598Z level=WARN  thread=DefaultServiceExecution-Http Service-0 component=SERVICE_AUDIT
decisionRequestId=d63629cc-d61f-41e7-8e68-52298a83b533 exchangeId=Wx-T-oESN6uxNRYeu158Tg |  Error invoking
HTTP service: name=Payment Service, host=192.168.7.106, duration=14ms, configuredTimeout=2000ms,
error=com.pingidentity.authorize.serviceexecution.ClientServiceExecutionException: Got unsuccessful status
code: 429, with body: {
  "message": "Too Many"
}
```

`level=WARN`

The following example shows a `SERVICE_AUDIT` log entry for an unsuccessful service call, due to the service timing out:

```
2024-10-03T11:50:19.540Z level=WARN  thread=DefaultServiceExecution-Payment Service-0
component=SERVICE_AUDIT decisionRequestId=0c907d84-f70d-4c82-893c-a8d0810bae37
exchangeId=jRPBjiXKEFoL06BuOjGieg |  Error invoking HTTP service: name=Payment Service, host=192.168.7.106,
duration=2004ms, configuredTimeout
```

Service cache hit

The following example shows a `SERVICE_AUDIT` log entry for a successful service cache hit:

```
2024-10-04T11:58:19.540Z level=INFO thread=DefaultServiceExecution-RandomUserService-0
component=SERVICE_AUDIT decisionRequestId=b7034567-08da-499g-9b1a-926b8571d565
exchangeId=85sC5rqIn_bPfvnU2u5Mgg | Cache hit for Payment Service: name=PaymentService, cacheKey=3c21d32a-
c432-4cf4-99e1-f9e04f32134a_E02083C34EBC29E4A2CD378F4755728, host=localhost
```

Webhooks

With webhooks, also known as subscriptions, you can use third-party tools to monitor events in PingOne.

Use PingOne to create and manage these event subscriptions. Subscriptions are push-based. When an event of interest occurs in PingOne, the event is pushed from PingOne to your monitoring system, such as Splunk, New Relic, and other SIEM systems.

You can find an overview of all logging and reporting capabilities in PingOne in PingOne Platform logging and reporting.

If the webhook target is offline, PingOne continues to retry and queue up all matching events.

Copyright © 2025 Ping Identity Corporation

If the webhook target is down for longer than 7 days, PingOne starts to lose events.

The webhook continues to retry the current event until a 200 response is returned. It doesn't move on to the next event until a 200 response has returned or the event has expired from Kafka.

> **Note**
> Events expire after 7 days.

Creating or editing a webhook

You can create a webhook to monitor events in PingOne.

Steps

1. In the PingOne admin console, go to **Integrations** > **Webhooks**.
2. Click **+ Add Webhook** or expand an existing webhook to edit it.
3. Enter a descriptive name for the connection.
4. Enter the **Destination** information.

   These settings configure the connection to the monitoring system.

   - **Destination URL**: The IP address or hostname of the application that you want to send data to.

     > **Note**
     > IPv6 addresses aren't supported.

   - **Format**: The format of the activity data. Select the format that is most easily consumed by your management system:
     - **Splunk**: A Splunk-friendly format.
     - **Ping Activity Format**: Use this format if the destination can't directly accept the Splunk or New Relic formats. It's a versatile, generic JSON format, which is the same format used by the PingOne API for accessing event data using Audit Activities. Learn more in the Subscription Action Types table in Subscriptions (webhooks) in the PingOne API documentation.
     - **New Relic**: A New Relic-friendly format.
   - **Certificates**: A certificate to ensure that the connection is secure. Browse existing certificates, or upload a new one.
   - **Allow TLS connection with untrusted certificates**: Select this option to allow a certificate that's not from a certificate authority (CA). PingOne certificates, and all certificates signed by the default CAs are trusted. This option is typically used for testing. Learn more in Certificates and key pairs.
   - **TLS Client Authentication Key**: Select a key to enable mutual TLS (mTLS). The key is used as a client credential to authenticate the webhook and must have a usage type of outbound mTLS. Learn more in Adding a certificate and key pair.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> To use a TLS client authentication key, you must disable the **Allow TLS connection with untrusted certificates** setting.

5. (Optional) To enter the headers information, click **Add Headers**:
   - **Basic authentication**: Enter a username and password for the destination system.
   - **Custom HTTP headers**: Specify additional information for the HTTP headers. Provide information in the form of key-value pairs. For example, you can define a custom Authorization header with a token instead of using basic authentication. This is the common method for modern security information and event management (SIEM) systems, such as Splunk and Sumo Logic.
6. Enter the **Filters** information.

   These settings determine which events are monitored. Select a category or a subset of events in that category.
   - **Event types**: Specify the types of events to monitor, such as user created, user deleted, and so on.

     You can find a complete list of events logged in PingOne in Audit Reporting Events in the PingOne API documentation.
   - **Tags**: Specify a tag to monitor.

     Admin Identity Event: An action taken by an administrator or API client on another administrator user, such as:
     - Creating or deleting an administrator user
     - Enabling or disabling an administrator user
     - Adding or removing roles from an administrator user
     - Changing a password for an administrator user
     - Changing username or email address for an administrator user
     - Enabling or disabling MFA for an administrator user
     - Pairing a new MFA device for an administrator user
     - Adding or removing linked accounts for an administrator user
   - **Applications**: Specify the applications in your PingOne environment that you want to monitor. You can include up to 10 applications.
   - **Populations**: Specify the populations in your PingOne environment that you want to monitor. You can include up to 10 populations.

     > **Note**
     >
     > For each filter, such as events, applications, or populations, the expression evaluates to `true` if any of the criteria are met (Boolean OR).
     > For multiple filters, the expression evaluates to `true` if all of the criteria are met (Boolean AND).
7. Enter the optional data.

Copyright © 2025 Ping Identity Corporation

Specify whether to include the IP address and User Agent strings in the report. Because IP addresses and User Agent strings can be considered sensitive data, you must manually select these options to include them in the report.

- **Include IP address**: Include the end user's IP address in the report. IP addresses are the client's IP address as it appears to the PingOne services. In some cases, this value is a proxy address rather than the actual client device address.
- **Include User Agent**: Include the User Agent String in the report. User Agent Strings are included if PingOne interacts with the user client when the client provides the string. The recorded value is exactly what was presented to PingOne by the client.

8. Click **Save**.

Deleting a webhook

You can remove a webhook connection that you no longer need.

Steps

1. Go to **Integrations → Webhooks**.
2. Locate the webhook that you want to delete.
3. Click the details icon to expand the webhook you want to delete.
4. Click the **Delete** icon to delete the webhook.
5. In the confirmation message, click **Delete**.

Enabling or disabling a webhook

If you don't want to delete a webhook, you can disable it.

About this task

When you disable a webhook, it no longer pushes events to the configured connection. When you re-enable a webhook, it collects events that were missed and pushes them to the monitoring system. Events accumulate for a maximum of 7 days. Events older than 7 days are removed.

Steps

1. Go to **Integrations → Webhooks**.
2. Locate the webhook that you want to enable or disable.
3. Click the toggle to enable or disable the webhook.

Result

The toggle moves to the left (gray) when disabled and to the right (green) when enabled.

Copyright © 2025 Ping Identity Corporation

PingFederate

Use a PingFederate connection to connect a PingFederate environment with the PingOne platform, which allows PingFederate to use PingOne services, such as PingOne MFA or PingOne Protect.

This connection allows the credentials for the PingFederate connection to be stored in PingOne. Each PingFederate connection has one or more credentials associated with it. The credential is generated in PingOne and then configured in PingFederate so that PingOne can authenticate the PingFederate additional service used by PingFederate. After you create a connection, you won't need to enter credentials or other connection details for each instance. The credentials never expire, but you can create new credentials and revoke old ones if you want to rotate the credentials.

You will generate a credential in PingOne and then copy it to PingFederate when you create the connection. During runtime, PingFederate uses the credential to access PingOne services.

Note

- You can create one or more credentials for each PingFederate connection. You typically won't need more than one credential other than during the credential-rotation period.
- You can create more than one PingFederate connection, but doing so means that multiple PingFederate environments are sharing the same PingOne environment.
- The setup and rotation process involves copying the credential from PingOne as the console presents it, pasting the credential into PingFederate when you are ready to create or update the PingOne connection in the PingFederate console.
- The credentials don't expire, but we recommend rotating them manually.

Learn more in Connections to PingOne in the PingFederate Administrator's Reference Guide.

Creating a connection

Create a connection profile and credential in PingOne, then use the credential in PingFederate to establish the connection.

Before you begin

To set up a connection between PingOne and PingFederate, you need access to the administrator consoles for both platforms.

Steps

1. In the PingOne admin console, go to **Integrations** > **PingFederate**.
2. Click the **+** icon.
3. Enter the following information:
   - **Name**: A unique identifier for the connection.
   - **Description** (optional): A brief description of the connection.
4. Click **Save**.

   Result:

Copyright © 2025 Ping Identity Corporation

PingOne generates a credential for the connection. PingFederate exchanges the credential for an access token that is used to call PingOne APIs.

5. In the **New Credential Created** window, click the **Copy to Clipboard** icon.

> **Important**
>
> After you leave this page, you cannot go back and copy the credential, so make sure to copy it now. If you're not going to complete the configuration now, you can paste the credential to a text file. You can also create a new credential later. Learn more in Editing a connection.

6. Click **Done**.

   Result:

   The new connection is added to the **PingFederate Connections** list.

Next steps

Adding the connection in PingFederate

Adding the connection in PingFederate

About this task

Go to the PingFederate administrative console and add the connection in PingFederate.

Learn more in Connections to PingOne.

Viewing connection details

Use the PingFederate **Connections** page to view existing connections from PingFederate to PingOne.

Steps

1. In the PingOne admin console, go to **Integrations** > **PingFederate**.

   Result:

   The connection entries show the connection name, description, and status toggle switch. Click the toggle to enable or disable the connection to PingFederate.

> **Note**
>
> You can disable a connection in PingOne or in PingFederate. The connection can be used only if it's enabled in both PingOne and PingFederate.

2. Click a connection entry to open the details panel, which shows more information about the connection, including the status of the connection, configuration details, and roles.

   The details panel shows the following information:

Copyright © 2025 Ping Identity Corporation

Overview

Shows the currently configured credentials, including credential ID, when the credential was created, and when the credential was last used. You can also revoke the credential from this tab.

Roles

Shows the roles that are currently configured for the connection. Learn more in Administrator Roles. The **Roles** tab also shows which PingOne environments the connection can access. Learn more in Editing a connection.

API

Shows the connection ID, environment ID, and API URL, which shows where you can find the JSON connection data. You can also click the **Copy to Clipboard** icon to copy the JSON data directly from PingOne.

Editing a connection

After you've created a connection, you can use the PingFederate **Connections** page to edit it, if needed.

Steps

1. In the PingOne admin console, go to **Integrations** > **PingFederate**.
2. Click a connection entry to open the details panel.
3. Do one or more of the following:
    - Edit the name and description.
    - Add or revoke credentials.
    - Add roles and responsibilities.

Editing the name and description

You can edit the name and description of an existing connection.

Steps

1. Click the appropriate connection to open the details panel.
2. Click the **More Options** (⋮) icon on the right and then click **Edit Name & Description**.
3. Enter or edit the values for **Name** and **Description**.
4. Click **Save**.

Adding or revoking credentials

You can add or revoke credentials for existing connections.

Steps

1. Click the appropriate connection to open the details panel.

Copyright © 2025 Ping Identity Corporation

2. Click the **Overview** tab.
3. Do one of the following:
   - To revoke a credential, click the **Delete** icon. In the confirmation message, select **I understand and want to continue**, and then click **Revoke**.
   - To add a credential, click the **+** icon. Click the **Copy to clipboard** icon to copy the credential, if necessary. Click **Done** to close the credential window.

> **Note**
>
> After you leave this screen, you can't go back and copy the credential, so ensure that you copy it now. If you aren't going to complete the configuration now, you can paste the credential to a text file.

Adding roles and responsibilities

You can add roles and responsibilities to existing connections. By default, the connection applies to the current environment. You can also add or remove environments from the connection.

Steps

1. Click the appropriate connection to open the details panel.
2. Click the **Roles** tab.
3. Do one of the following:
   - To remove a role, click the **Delete** icon next to the appropriate role. In the confirmation message, click **Remove**.
   - To add a role, click the **Grant Roles** button. Select a role to grant. Learn more in Administrator Roles. Add or remove responsibilities as needed. Responsibilities define the environments or organization that the connection can access. Click **Save**.

Deleting a connection

You can remove a connection that you no longer need.

Steps

1. In the PingOne admin console, go to ***Integrations** > **PingFederate**.

   Result:

   PingOne shows an entry for each existing connection.
2. For the connection you want to delete, click the **More Options** (⋮) icon and then click **Delete**.
3. In the confirmation message, select **I understand and want to continue**, and then click **Delete**.

Copyright © 2025 Ping Identity Corporation

User Experience

The **User Experience** branch contains the Notification Templates, Notification Policies, Branding and Themes, Self Service, Agreements, and Languages pages.

Learn more in:

Notification templates

Notification Policies

Branding and themes

Self Service

Agreements

Languages

Notification templates

Use notification templates to inform end users about certain events, such as device pairing and password resets.

PingOne provides the following notification types:

Credential Issued

Notifications to end users when a credential is issued.

Credential Revoked

Notifications to end users when a credential is revoked.

Credential Updated

Notifications to end users when a credential is updated.

Device Pairing

Notifications for setting up end user devices for strong authentication.

PingOne Verify Email Address and Phone Number Verification

Notifications for end users to verify their email address or phone number.

Digital Wallet Pairing

Notifications to end users to set up and pair a digital wallet app for storing credentials.

General

Multi-purpose notifications to create custom notifications for use with the PingOne Notifications Connector.

PingOne Verify ID Verification

Notifications for end users to provide identity documents.

Copyright © 2025 Ping Identity Corporation

Email Address Verification (Admin)

Notifications for PingOne administrators to verify their email address.

Email Address Verification (User)

Notifications for PingOne users to verify their email address.

Password Recovery

Notifications for end users who have forgotten their password and have started the `Forgot password` process.

Strong Authentication

Notifications for end users setting up strong authentication.

Transaction

Notifications for end users when strong authentication is required for transaction approval. For example, elevated security for a high value or high risk resource or service.

Verification code

Notification with a verification code sent to the email address in the user profile to verify the user account.

You can also create a notification policy to define the number of SMS or voice notification messages that can be sent per day. Learn more in Notification Policies.

Related links

- Viewing notification templates
- Adding a notification template
- Editing a notification template
- Reporting for notifications
- Notification Policies

Viewing notification templates

Use the **Notification Templates** page to view the currently configured notification templates. The delivery method (email, SMS, voice or push) for each notification type includes a template with default settings.

Steps

- In the PingOne admin console, go to **User Experience** > **Notification Templates**.

Result

The Notification Templates page shows a list of notification types and the number of notifications configured for each type, as well as the delivery method and languages configured for each notification. To see specific details about the notifications for each language and delivery method, edit the notification. Learn more in Editing a notification template.

Copyright © 2025 Ping Identity Corporation

Next steps

Adding a notification template

Editing a notification template

Adding a notification template

To add a notification template, you'll select a default notification template and customize it to meet the needs of your organization. New notifications are based on a default notification type.

> **Note**
> You must have the Environment Admin role to add and edit notification templates.

Steps

1. In the PingOne admin console, go to **User Experience > Notification Templates**.
2. Click **+**.
3. In the **Add Notification** window, enter the following:
   - **Type**: Select the purpose of the notification template. The options are **Device pairing**, **Strong authentication**, and **Transaction**. You can find more information on notification types in Notification templates.

     > **Note**
     > Multiple notifications variations are not supported for the Password Recovery and Verification Code templates.

   - **Name** (optional): A unique identifier for the notification template. The name appears in the notification template list to help administrators choose the appropriate template.
4. Click **Next**.

   > **Note**
   > To protect the email reputation scores for all of our customers, PingOne Trial licensees cannot use the built-in PingOne email domain (`@pingone.com`) to send email notifications with customized content. Paid licensees can customize the content, and Trial licensees can create custom email notification content when using their own SMTP server or custom email domains. Learn more in Setting up a trusted email domain and Configuring a custom SMTP email notification server.

5. Click **Save**.

Result

The notification template is added to the notification templates list.

Next steps

Edit the notification template as needed. Learn more in Editing a notification template.

Copyright © 2025 Ping Identity Corporation

Editing a notification template

You can edit existing notification templates to meet the needs of your organization.

- For email, SMS, voice, and push notifications, each notification type includes a template with default settings.
- For WhatsApp notifications, you must manually select the WhatsApp business account template that you want to use.

> **Note**
>
> You need the `Environment Admin` role to add and edit notifications.

Steps

1. In the PingOne admin console, go to **User Experience > Notification Templates**.
2. Locate the notification template you want to edit.
3. On the right of the notification template, click the details menu (three dots) and then click **Edit**.

   Result:

   The notification template opens in edit mode. If the notification has multiple delivery methods, you can edit them all on the same screen.

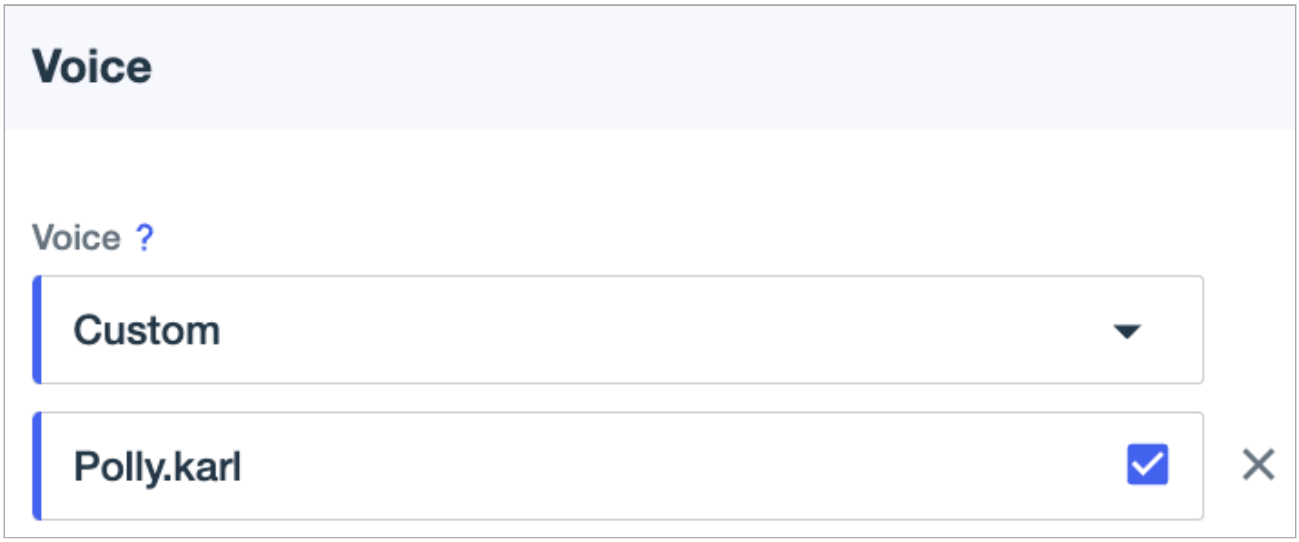
   > **Note**
   >
   > To protect the email reputation scores for all of our customers, PingOne Trial licensees cannot use the built-in PingOne email domain (`@pingone.com`) to send email notifications with customized content. Paid licensees can customize the content, and Trial licensees can create custom email notification content when using their own SMTP server or custom email domains. Learn more in Setting up a trusted email domain and Configuring a custom SMTP email notification server.

4. Enter or edit the content for each delivery method and language. Select the language on the left. Learn more about adding a language in Languages, and learn more about delivery methods and variables in Delivery methods and variables.

   > **Note**
   >
   > - Click the ✎ icon to edit a field. Click the **Checkmark** icon to save changes.
   > - Click **Restore default text** to undo any content changes you have made.
   > - Click **X** in the upper right to abandon changes and return to the notifications list.

5. SMS notifications only: If you defined a Twilio Verify server for sending PingOne notifications, use the **Twilio Verify Template** drop-down to select the Verify template that you want to use for the notification.
6. Voice notifications only:
   - To change the default voice, in the voice field, select a voice from the list. You can find a list of supported voices in Delivery methods and variables.
   - If you use a custom voice provider and want to add a custom voice, select **Custom**, and then enter the name of the custom voice in the field that appears below the custom field.

Copyright © 2025 Ping Identity Corporation



> **Note**
>
> Learn more about managing the languages supported for use with this notification template in Languages.

- If you defined a Twilio Verify server for sending PingOne notifications, use the **Twilio Verify Template** drop-down to select the Verify template that you want to use for the notification.

> **Note**
>
> If you do not select a template, the default Verify template is used. For voice notifications, if you select a different template, you must contact Twilio support to enable the use of alternative templates for your account since this Twilio feature is still in beta.

7. WhatsApp notifications only:

> **Note**
>
> - Before selecting a WhatsApp message template, you must define a custom WhatsApp Sender account. Learn more in: (Customer Only) Configuring WhatsApp as a sender
> - The WhatsApp message template (Category = Authentication) must be used, and is only supported by the PingOne Device Pairing and Strong Authentication templates.
> - The WhatsApp message text and translations are defined by WhatsApp and cannot be edited in PingOne.
> - If WhatsApp does not support a language that's defined in PingOne, the system language is used.

- In the **Device Pairing** and **Strong Authentication** templates, for each language that you want to support, select the relevant WhatsApp message template.

> **Note**
>
> The list of WhatsApp message templates that appear are those defined in your WhatsApp business account.

Copyright © 2025 Ping Identity Corporation

Delivery methods and variables

Delivery methods define the format of the message, and include details such as the subject, message content, and variables that you can use in the message content. Variables can represent things like a user name or one-time password. Some variables are optional and some are mandatory.

SMS

Notifications are sent as an SMS (short message service) text message.

Sender ID

You can configure a sender ID to be used instead of a telephone number for commercial use or to comply with regulations requiring SMSs to be sent as transactional and not promotional. For more information, see Configuring an SMS/Voice sender account with PingOne.

New message

The content of the message. Use up to 660 characters.

Variables

The required variable is *${otp}*. It must be included in the message content.The predefined optional variable is *$\{user.username}*. It can be included in the message content. The optional variable *$\{user.username}* is relevant only for the Strong Authentication, Device Pairing, and Transaction templates.

> **Note**
>
> On some templates, the initiator of the flow might provide dynamic variables that can be included in the message as well. For more information, see Dynamic variables in the PingOne Platform API Reference.

Email

Notifications are sent as a standard email message. You can replace the PingOne email service with your organization's SMTP server. See Configuring a custom SMTP email notification server.

> **Note**
>
> PingOne sends emails from dedicated IP pools, which ensures the high reputation, increased reliability and deliverability rate of PingOne emails. End users can whitelist these IP addresses to reduce the likelihood of potential issues with grey-listing or content blocking of PingOne services.

From Name

The name of the sender's email account that sends email notifications.

From Address

The email address of the sender's account that sends email notifications.

Reply-To Name

The name of the sender's email account to send replies.

Copyright © 2025 Ping Identity Corporation

Reply-To Address

The email address to send replies to the sender.

> **Note**
>
> - If you configure the environment to use the PingOne email service, you can only configure trusted email addresses in the **From Address** and **Reply-To Address** of the email notification template. See Configuring trusted email addresses.
> - If you configure the environment to use a custom email service, you can add any email (trusted or not-trusted) in the **From Address** and **Reply-To Address** of the email notification template.
> - It is the customer's responsibility to check that the email is trusted in their mail server.
> - If the environment is configured to use a custom email service, and you later reconfigure it to use the PingOne email service without removing non-trusted email addresses from the email notification template, depending on the environment definitions, the default environment email address will be either a trusted **From Address**, or it will be the PingOne email service's address.
> - The **Reply-To Address** for email notification templates is optional. If the **Reply-To Address** has a value, the **From Address** is mandatory .

Subject

The subject line of the email message.

New email

The content that appears in the message body. Use plain text or HTML.

Variables

The required variable is *${otp}*. It must be included in the subject or message body.The predefined optional variable is *$\{user.username}*. It can be included in the subject or message body. The optional variable *$\{user.username}* is relevant only for the Strong Authentication, Device Pairing, and Transaction templates.

> **Note**
>
> On some templates, the initiator of the flow might provide dynamic variables that can be included in the message as well. For more information, see Dynamic variables in the PingOne Platform API Reference.

Push

Notifications are sent as push notifications to the end user's device.

Title

The title of the push notification, up to 200 characters.

Push category

Select a category to control the type of banner that is displayed to the user:

- **Banner buttons**: The default banner - contains both Approve and Deny buttons.

Copyright © 2025 Ping Identity Corporation

- **No banner buttons**: When the user clicks the banner, they are taken to an application that contains the necessary approval controls.
- **Approve & open app**: When the Approve button is clicked, authentication is completed and the user is taken to the relevant application.

> **Note**
> To use the non-default banners, you must implement them in your application code, using the PingOne SDK.

New push

The content that appears in the body of the notification.

Variables

No required variables.The predefined optional variable is *$\{user.username}*. It can be included in the title or message body. The optional variable *$\{user.username}* is relevant only for the Strong Authentication, Device Pairing, and Transaction templates.

> **Note**
> On some templates, the initiator of the flow might provide dynamic variables that can be included in the message as well. For more information, see Dynamic variables in the PingOne Platform API Reference.

Voice

Notifications are sent to the end user's device as voice messages.

A voice notification consists of a voice and a locale. For example selecting Man voice and en_GB locale, results in notifications that are spoken in a male voice with an English accent.

You can add a voice from the voice dropdown, or select **Custom** to add a custom voice (see Editing a notification template). If PingOne or your provider do not support the voice in combination with the selected language or locale, PingOne selects an alternative voice that is supported.

Voice type

Specify the type of voice that the end user will hear. Voice types are vendor specific, and the closest-matching voice is selected, based on the vendor-compatible options available, as follows:

- Man or Woman: Select the most applicable voice, based on the gender selected and the user's locale that is defined.
- Best applicable: Select the most applicable voice, based on the user's locale.
- Custom (Twilio only): Specify the voice that you want to use.PingOne supports Man, Woman, and Polly voices only. For a list of relevant voices, see Text-to-Speech (TTS).

> **Note**
> To enhance stability, Ping Identity uses more than one voice call provider. Therefore the voice type used might vary between different authentication requests.

Copyright © 2025 Ping Identity Corporation

Message

The content of the voice message.

Variables

The required variable is *${otp}*. It must be included in the message.The predefined optional variable is *$\{user.username}*. It can be included in the message. The optional variable *$\{user.username}* is relevant only for the Strong Authentication, Device Pairing, and Transaction templates.

> **Note**
>
> On some templates, the initiator of the flow might provide dynamic variables that can be included in the message as well. For more information, see Dynamic variables in the PingOne Platform API Reference.

Elements

The following operational elements can be embedded in voice messages:

- `<pause1sec>` : Pauses the message narration for 1 second.

  > **Note**
  >
  > The `<pause1sec>` element cannot be modified. To pause for more than one second, add multiple `<pause1sec>` elements in succession. For example, `[.codeph] <pause1sec><pause1sec><pause1sec>` pauses the message narration for three seconds.

- `<sayCharValue> .. </sayCharValue>` : Reads the character name of each character of the enclosed string separately.
- `<repeatMessage val=x> .. </repeatMessage>` : Narrates the enclosed text `<val>` number of times.

In the following message example, `${otp}` is assigned the value `"123456"`, and `${email}` is assigned the value `"joe@bxz.com"` :

```
Hello <pause1sec> your authentication code is <sayCharValue>${otp}</sayCharValue> <repeatMessage val=2>I repeat your code is <sayCharValue>${otp}</sayCharValue></repeatMessage> <pause1sec> Mail <sayCharValue>${email}</sayCharValue> for help
```

The narrated message on the voice call sounds like:

```
HELLO <1 second silence> YOUR AUTHENTICATION CODE IS ONE TWO THREE FOUR FIVE SIX I REPEAT YOUR CODE IS ONE TWO THREE FOUR FIVE SIX I REPEAT YOUR CODE IS ONE TWO THREE FOUR FIVE SIX <1 second silence> MAIL JAY OH EE AT BEE EX ZEE DOT SEE OH EM FOR HELP
```

Reporting for notifications

To run a report to see when notifications were created, updated, or deleted:

Steps

1. In the PingOne admin console, go to **Monitoring > Audit**.
2. For **Time range**, enter the appropriate time span for the report.

Copyright © 2025 Ping Identity Corporation

3. For **Filter type**, select **Event type**.
4. For **Filter**, select one or more of the following. You can search or browse for event types.
   - **Content created**: One piece of content (with a specific ID) was created. A piece of content represents one message text option for a notification.
   - **Content deleted**: One piece of content (with a specific ID) was deleted. A piece of content represents one message text option for a notification.
   - **Content updated**: One piece of content (with a specific ID) was updated. A piece of content represents one message text option for a notification.
   - **Contents deleted**: All content within a variant type was deleted.
   - **Contents updated**: All content within a variant type was updated.
   - **Notification created**: A notification message was created.
   - **Notification updated**: A notification message was updated.
5. Click **Run**.

Notification Policies

Create a notification policy to limit the number of SMS, voice, WhatsApp, or email notifications that can be sent per day. To prevent the malicious use of notifications, you can also add a notification cooldown period during which users must wait before requesting another notification such as another one-time passcode (OTP).

About this task

When creating an environment, a notification policy is created by default. Workforce environments can only include a single notification policy. In a Customer environment, you can create multiple notification policies and change the default policy for the environment.

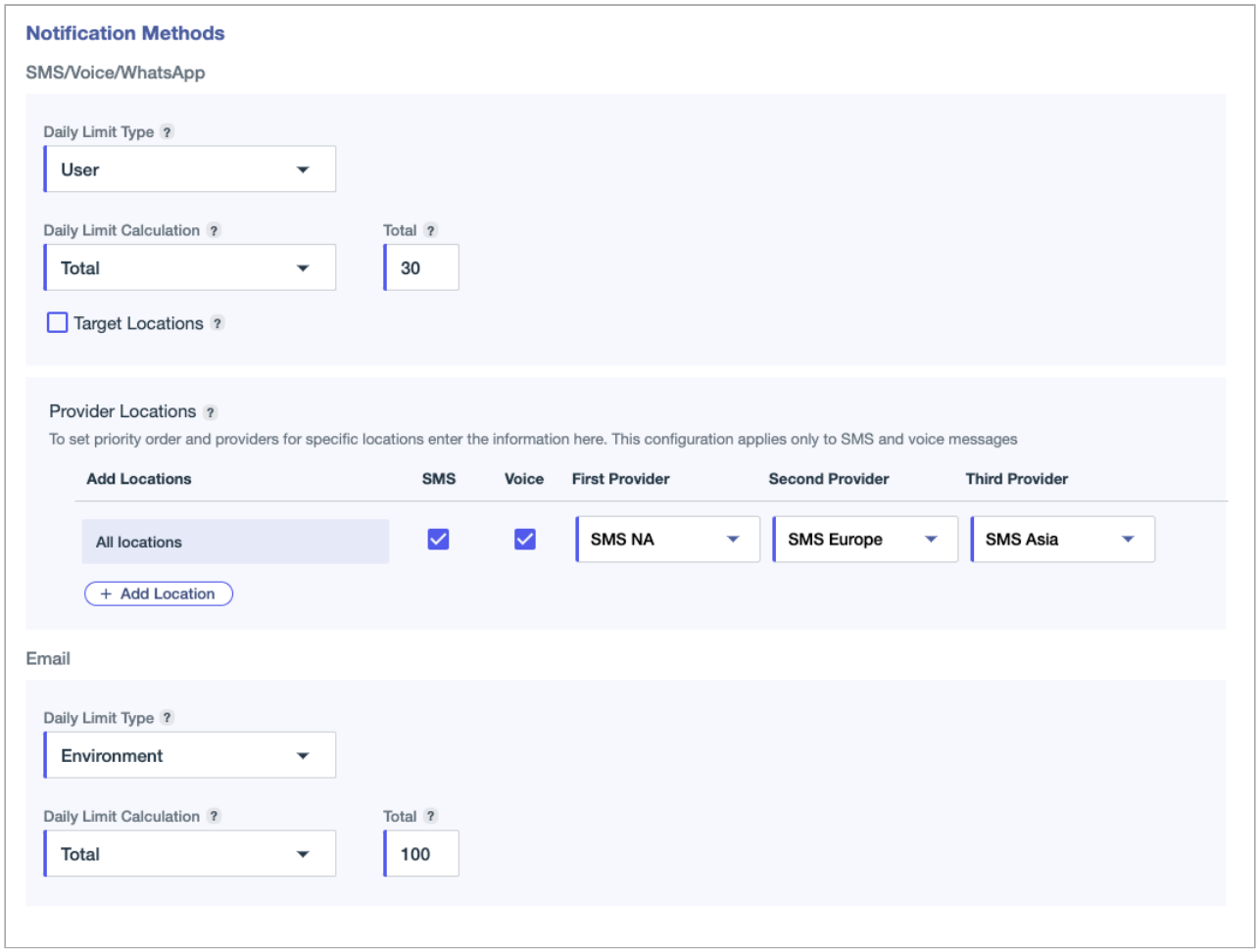
The limits in a notification policy can be per environment or per user. You can define a limit for the total number of notifications or separate limits for used and unused notifications. Used notifications are those to which users responded. Unused notifications are those that users received but did not use for registration or authentication.

> **Note**
>
> - The daily notification counters are reset every night at midnight UTC.
> - If you're sending your email notifications using the Ping Identity email service, there's a fixed maximum of 1.5 million email notifications per day for each environment.

Steps

1. In the PingOne admin console, go to **User Experience** > **Notification Policies**.
2. Click the policy you want to edit, then click the ✎ icon, or to add a new policy, click the + icon.

Copyright © 2025 Ping Identity Corporation



3. Enter a meaningful name for the policy (maximum 256 characters).
4. Use the **Daily Limit Type** list to specify whether the limit is per environment or per user.

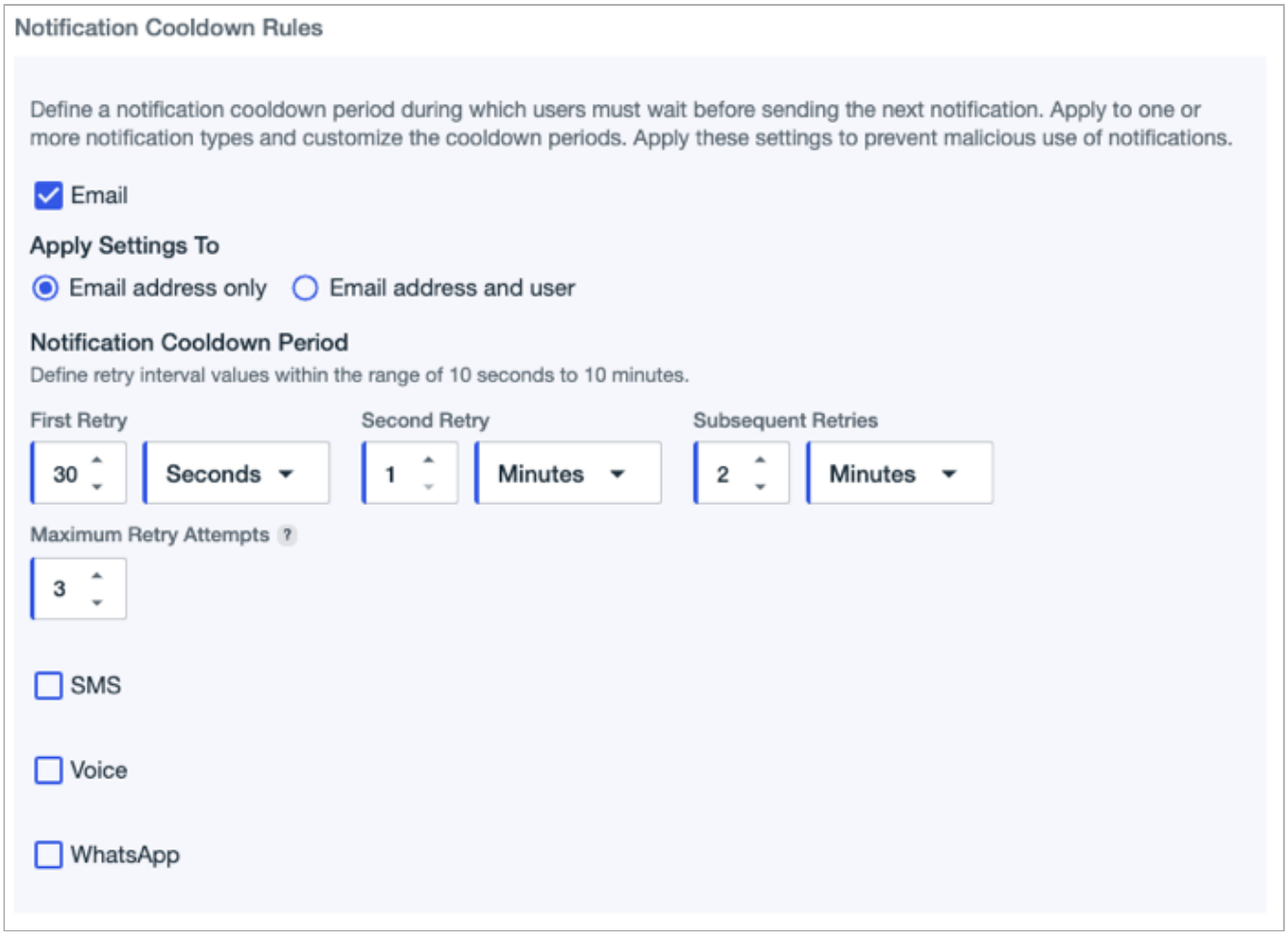
   Select **Unlimited** if you don't want to define a limit.
5. Use the **Daily Limit Calculation** field to specify whether you want to limit the total number of notifications or set separate limits for used and unused notifications.
6. Enter the **Total** number of notifications that can be sent per day or enter separate limits for used and unused notifications (possible values 1 - 50).

   > **Note**
   >
   > For a trial environment, the maximum number of notifications allowed per day is 100. For a licensed environment, there is no limit.
7. For SMS, voice, and WhatsApp notifications, you can use the **Target Locations** option to restrict the use of notifications to a subset of countries. After selecting **Target Locations**, use the **Select Locations** field to compose an allow list or deny list.
8. For SMS and voice notifications, if you've defined one or more custom servers or custom providers, you can specify the order of provider preference, based on availability. You can specify a single order for all geographic locations, or you can use the **Add Location** option to specify different provider preferences for different groups of countries. You can also specify separate provider preferences for SMS and voice.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If none of the providers specified for a given group of countries is enabled for a required notification method (SMS or voice), PingOne also checks if the default provider is enabled for that method. The default provider is the first provider listed on the **SMS/Voice** tab of the **Sender** page. If the default provider isn't enabled for that notification method, the message will not be sent.

9. To prevent the malicious use of notifications, in the **Notification Cooldown Rules** section define cooldown rules.



For each authentication method (**Email**, **SMS**, **Voice**, or **WhatsApp**), select the relevant checkbox and define the following:

1. For **Apply Settings To**, select either:
   - **Phone/Email only**: Apply the settings per phone number or email address even if it's used by more than one user.
   - **Phone/Email and user**: If more than one user receives notifications to the same phone number or email address, apply the settings separately to each user.
2. For **Notification Cooldown Period**, configure the retry intervals and maximum retry events:
   - Retry intervals: For up to three retry intervals, define the time period the user must wait before requesting another notification such as an OTP (minimum is 10 seconds, maximum is 10 minutes). The third interval is applied to all subsequent retries until the **Maximum Retry Attempts** limit is reached.

Copyright © 2025 Ping Identity Corporation

- **Maximum Retry Attempts**: Maximum number of attempts the user has to retry requesting another notification, such as an OTP, before the use of the email address or phone number is locked. The lock is applied for 30 mins or until the user successfully enters the correct passcode.

10. Click **Save**. The policy is added to the policy list.

> **Tip**
>
> In the policy list, click a policy to see a summary of the policy details in the right pane or edit an existing policy.

Next steps

You can select which notification policy you want to apply to an MFA policy. Learn more in Configuring an MFA policy for strong authentication.

Branding and themes

Use branding themes to quickly define a set of colors and images to best match your company's branding and easily change the look of standard authentication policy forms, the application portal, the self-service portal, PingOne forms, and identity verification pages for a particular environment.

Learn more

- Viewing a list of available themes
- Previewing a theme
- Editing environment branding
- Adding a theme
- Editing a theme
- Selecting an active theme
- Deleting a theme

Viewing a list of available themes

Use the **Branding and Themes** page to see available themes.

Steps

- In the PingOne admin console, go to **User Experience** > **Branding and Themes**.

Result

The **Branding and Themes** page shows a list of the configured themes for the environment.

You can browse or search for a specific theme. You can also sort the list of themes alphabetically or by last updated date.

Copyright © 2025 Ping Identity Corporation

Learn more

- Previewing a theme
- Selecting an active theme
- Adding a theme
- Editing a theme
- Deleting a theme

Previewing a theme

View a real-time rendering of your theme and see how it affects the appearance of different end-user pages in your environment.

Steps

1. In the PingOne admin console, go to **User Experience** > **Branding and Themes** and browse or search for the theme you want to view.
2. Click the theme you want to preview.

   The details panel for the theme opens. The **All** tab is selected by default and shows previews of every type of page affected by applying the selected theme. To preview a certain type of page, select the applicable tab and scroll to see the different pages in each category.

   To switch between previews for desktop or mobile devices, click the **Desktop** or **Mobile** icon ( ).

   - **Forms**

     Click the **Forms** tab to see how your theme affects the appearance of PingOne forms in your environment.

     > **Note**
     >
     > Select a form from the **Form Preview** list to preview how the theme affects a particular form. You can also click **Edit Form** to open the **Forms** page in a separate tab and make updates as necessary. Learn more in Forms.

   - **Verify**

     Click the **Verify** tab to see how your theme affects the appearance of identity verification forms in your environment.

   - **End User Application**

     Click the **End User Application** tab to see how your theme affects the appearance of system applications, such as the **Application Portal** and **Self-Service - MyAccount**.

   - **Authentication Policy**

     Click the **Authentication Policy** tab to see how your theme affects the appearance of sign-on and registration pages in your environment.

Copyright © 2025 Ping Identity Corporation

Learn more

- Selecting an active theme
- Adding a theme
- Editing a theme

Editing environment branding

Use the **Global Settings** panel to edit the branding options for existing environments. These settings determine the company name and logo that appear on end-user-facing pages in the user interface.

Steps

1. In the PingOne admin console, go to **User Experience** > **Branding and Themes**.
2. Click the **Gear** icon (⚙) to open the **Global Settings** panel.

   These settings apply to all themes in the environment.
3. Enter or edit the branding details:
   - **Company name**: The name of your company as you want it to appear to end users.
   - **Logo**: An image to represent the environment to end users.

     To add or change the image used for the logo, hover over the image, click the **Camera** icon (📷), and select **Upload New Image**. Select an image in `.jpg`, `.jpeg`, `.gif`, or `.png` format up to 2 MB in size.

     To delete a logo from a theme, click 📷 and select **Remove Image**.
4. Click **Save**.

Learn more

- Viewing a list of available themes
- Selecting an active theme
- Editing a theme

Adding a theme

PingOne delivers several built-in themes. Use the **Branding and Themes** page to add a theme to the current environment. The new theme uses your **Company Name** and **Logo** if you added them in **Global Settings**. Learn more in Editing environment branding.

Steps

1. In the PingOne admin console, go to **User Experience** > **Branding and Themes**.
2. Click the **+** icon.

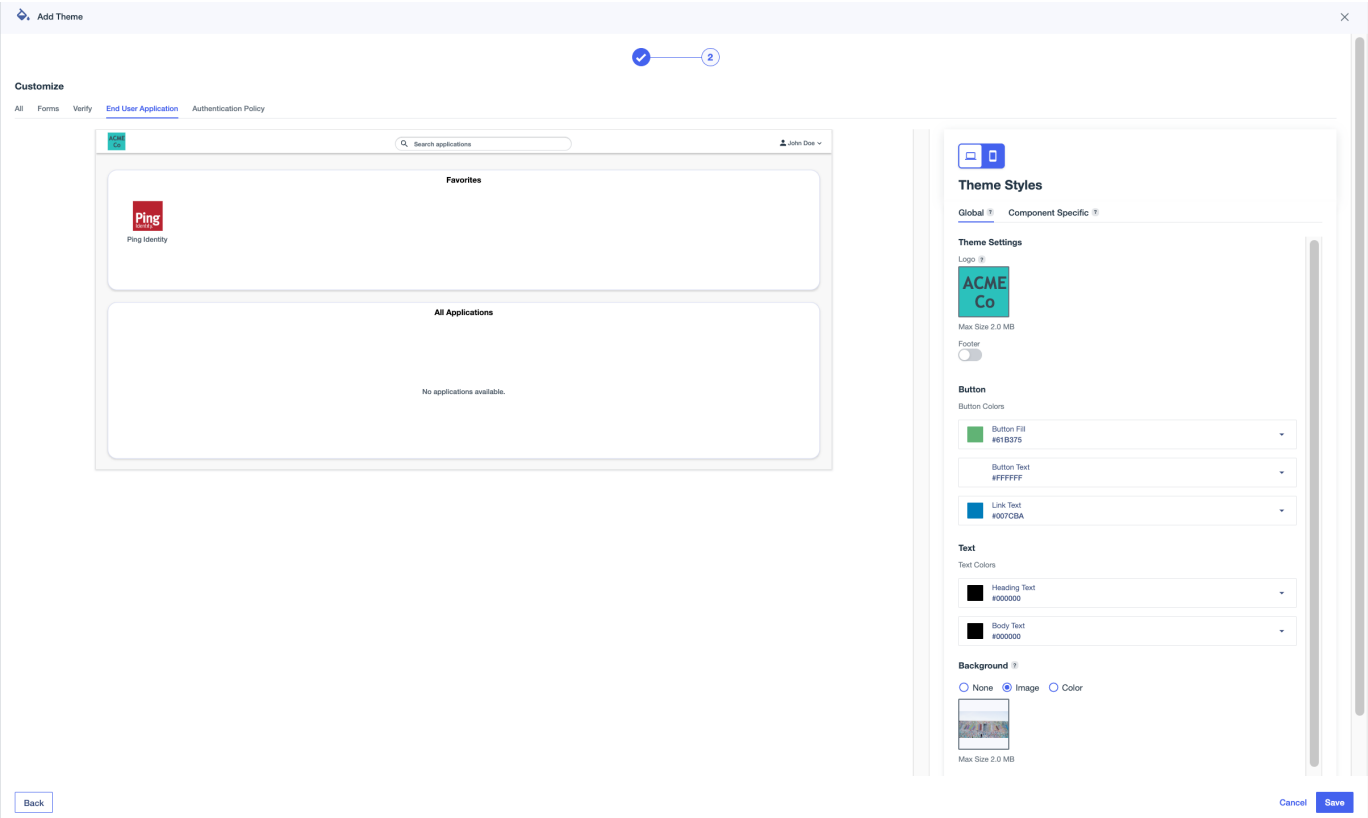
Copyright © 2025 Ping Identity Corporation

3. On the **Choose a Base Theme** page, click the theme you want to start with.

> **Note**
>
> When you select a base theme, PingOne generates a unique name for the new version. For example, if you select the **Focus** theme as your base theme, your new theme is named **Focus 1** by default. You can edit this name before you continue.

4. Click **Next** and select the tabs on the **Customize** page to change settings for the different page types.

   Page previews display in the left panel, and you configure settings in the **Theme Styles** panel on the right. The previews update in real time as you make changes to the settings. To switch between previews for desktop or mobile devices, click the **Desktop** or **Mobile** icon ( ).



> **Note**
>
> All page types include global theme settings, which apply across all components. Some page types also have **Component Specific** settings, which apply only to the specific component.

5. Click the **All** tab to edit global theme settings that apply to all pages that aren't affected by component-specific styles.

Copyright © 2025 Ping Identity Corporation

Setting	Description
Logo	An image to represent the environment. Hover over the box and click the **Camera** icon (📷) to upload an image. Select an image in `.jpg`, `.jpeg`, `.gif`, or `.png` format up to 2 MB in size. To change the image used for the logo, click 📷 and select **Upload New Image**. To delete a logo from a theme, click 📷 and select **Remove Image**.
Footer	Text that appears at the bottom of each page. Click the toggle to the right (blue) to enable footer text, then enter the text. You can include HTML in the footer, including the following elements and attributes: ◦ `a(href, target)` **Important** To use an `href`, you must include the protocol in the address, such as `ftp`, `http`, `https`, `mailto`, `tel`, or `sms`. ◦ `b` ◦ `blockquote(cite)` ◦ `br` ◦ `cite` ◦ `code` ◦ `dd` ◦ `dl` ◦ `dt` ◦ `em` ◦ `i` ◦ `li` ◦ `ol` ◦ `p` ◦ `pre` ◦ `q(cite)` ◦ `small` ◦ `span` ◦ `strike` ◦ `strong` ◦ `sub` ◦ `sup` ◦ `u` ◦ `ul`
Button	Configure the color of the buttons, such as the **Sign on** and **Save** buttons: ◦ **Button Fill**: The background color for the buttons. ◦ **Button Text**: The color of the text on the buttons. ◦ **Link Text**: The color of the text for links displayed on the buttons.
Text	The color of the text on the pages: ◦ **Heading Text**: The color of the text in headings. ◦ **Body Text**: The color of non-heading text.

Copyright © 2025 Ping Identity Corporation

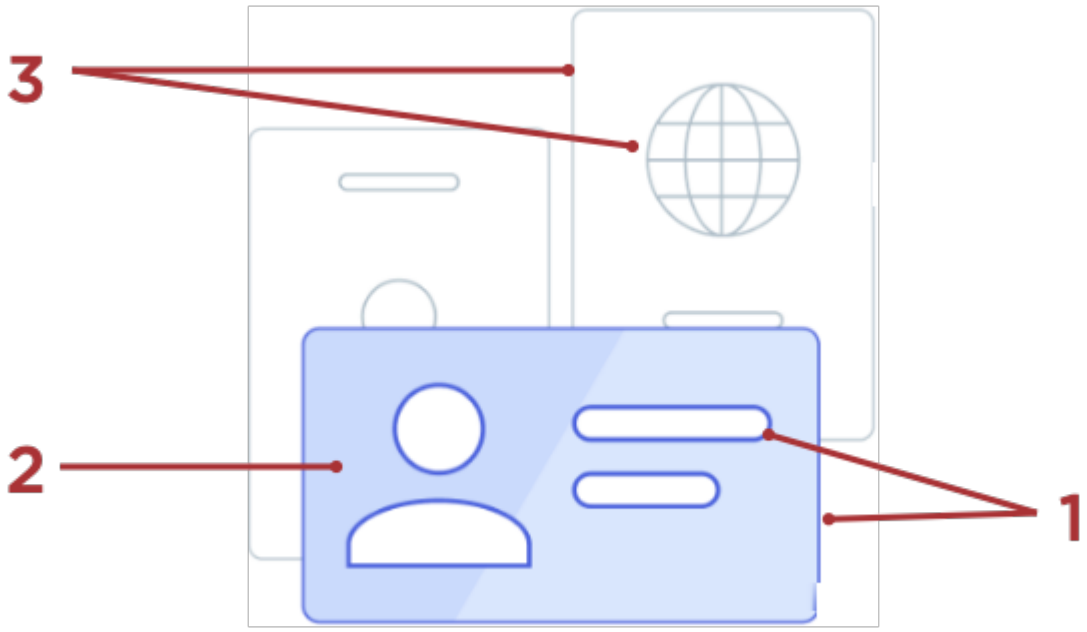
Setting	Description
Background	The background to use on each page. ◦ **None**: Do not use a background. ◦ **Image**: To use an image for the background, hover over the box and click the **Camera** icon (📷) to upload an image. Select an image in `jpg`, `jpeg`, `gif`, or `png` format up to 2 MB in size. To change the image used for the background, click 📷 and select **Upload New Image**. To delete a background image from a theme, click 📷 and select **Remove Image**. ◦ **Color**: Select a color to use for the background.
Card Color	The color of the box around form fields.

6. Click the **Forms** tab to edit global theme settings and preview the updated appearance of the PingOne forms in your environment.

> **Note**
>
> There are no component-specific styles for **Forms**.
> Your selections affect all forms, and can't be set at the form level, but you can select a form from the **Form Preview** list to preview it with theme styling applied. You can also click **Edit Form** to open the **Forms** page in a separate tab and make updates as necessary.
> Learn more in Forms.

7. On the **Verify** tab, click one of the tabs in the **Theme Styles** panel:
   - **Global**: Edit global theme settings and preview the updated appearance of identity verification pages.
   - **Component Specific**: Edit settings that only affect the appearance of the images on identity verification pages.

Copyright © 2025 Ping Identity Corporation



Setting	Description
Foreground Main (1)	The color used for the border around the front image and around the internal shapes in the front image.
Foreground Highlight (2)	The fill color used for the front image.
Background Outline (3)	The color used for the borders around the background images and around the internal shapes in the background images.

8. On the **End User Application** tab, click one of the tabs in the **Theme Styles** panel:
   - **Global**: Edit global theme settings and preview the updated appearance of system applications, such as the **Application Portal** and **Self-Service - My Account**.
   - **Component Specific**: Edit settings that only affect the appearance of system applications, such as the **Application Portal** and **Self-Service - My Account**.

Setting	Description
Background Color	The background color used for the application.

9. Click the **Authentication Policy** tab to edit global theme settings and preview the updated appearance of the sign-on and registration pages in your environment.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> There are no component-specific styles for **Authentication Policy**.

10. Click **Save**.

    The theme is added to the list on the **Branding and Themes** page.

> **Note**
>
> You can also customize an existing theme. Learn more in Editing a theme.

Next steps

Selecting an active theme

Editing a theme

PingOne delivers several built-in themes. Use the **Branding and Themes** page to modify the built-in themes or themes that you've added to the environment to better match your company's branding. The customized themes use your **Company Name** and **Logo** if you added them in **Global Settings**.

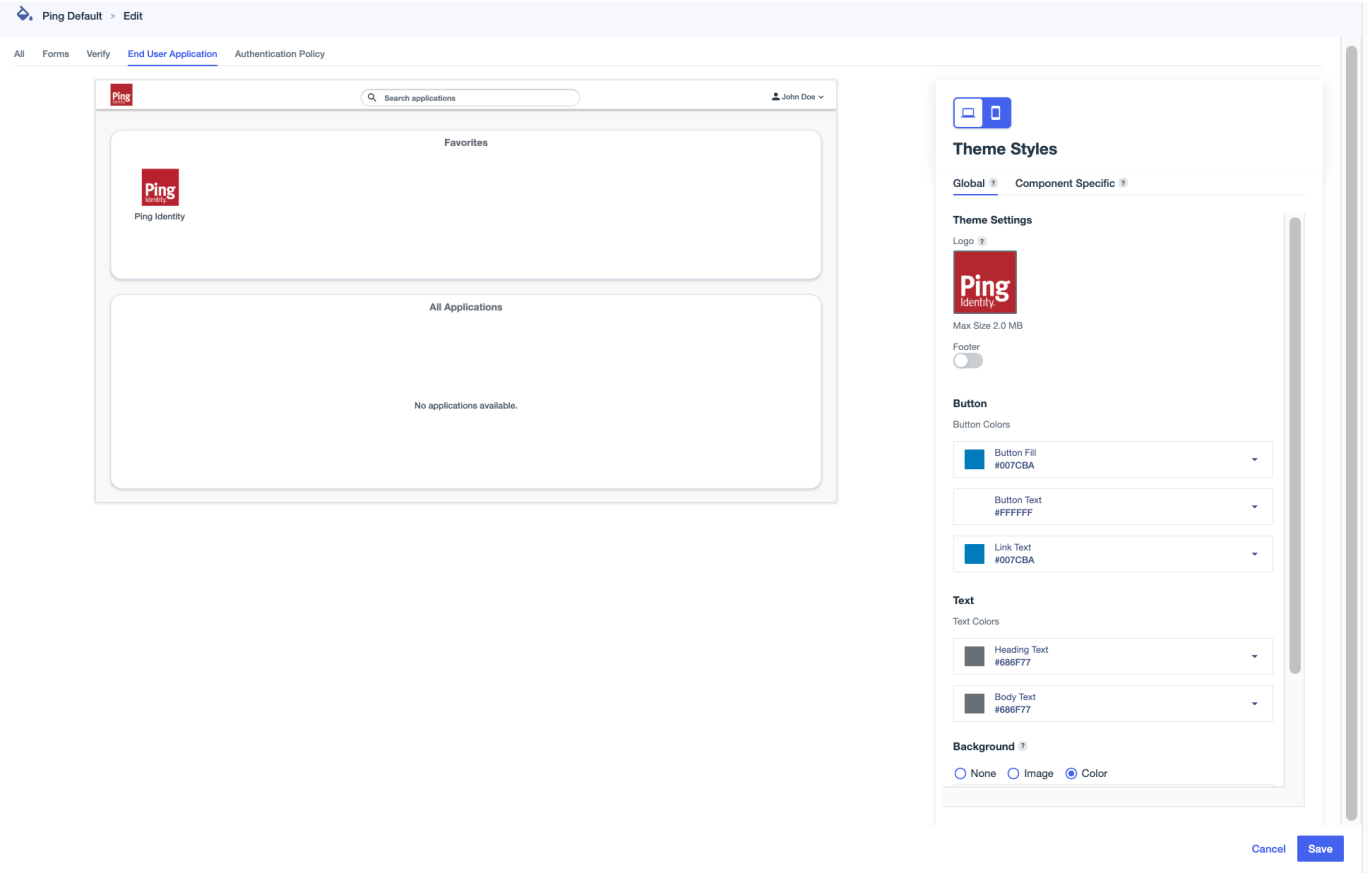
> **Important**
>
> If you edit a theme, you are responsible for ensuring that your customizations meet accessibility standards.

Steps

1. In the PingOne admin console, go to **User Experience** > **Branding and Themes** and browse or search for the theme you want to edit.
2. To change the theme name, click the **More options** (⋮) icon and select **Edit Name**.
3. Update the **Theme Name** and click **Save**.
4. To customize the other settings for the theme, click the **More options** (⋮) icon and select **Edit Theme**.

   Page previews display in the left panel, and you configure the settings in the **Theme Styles** panel on the right. The previews update in real time as you make changes to the settings. To switch between previews for desktop or mobile devices, click the **Desktop** or **Mobile** icon ( ).

Copyright © 2025 Ping Identity Corporation



> **Note**
>
> All page types include global theme settings, which apply across all components. Some page types also have **Component Specific** settings, which apply only to the specific component.

5. Click the **All** tab to edit global theme settings that apply to all pages that aren't affected by component-specific styles.

Setting	Description
Logo	An image to represent the environment. Hover over the box and click the **Camera** icon (📷) to upload an image. Select an image in `.jpg`, `.jpeg`, `.gif`, or `.png` format up to 2 MB in size. To change the image used for the logo, click 📷 and select **Upload New Image**. To delete a logo from a theme, click 📷 and select **Remove Image**.

Copyright © 2025 Ping Identity Corporation

Setting	Description
Footer	Text that appears at the bottom of each page. Click the toggle to the right (blue) to enable footer text, then enter the text. You can include HTML in the footer, including the following elements and attributes: ◦ `a(href, target)` **Important** To use an `href`, you must include the protocol in the address, such as `ftp`, `http`, `https`, `mailto`, `tel`, or `sms`. ◦ `b` ◦ `blockquote(cite)` ◦ `br` ◦ `cite` ◦ `code` ◦ `dd` ◦ `dl` ◦ `dt` ◦ `em` ◦ `i` ◦ `li` ◦ `ol` ◦ `p` ◦ `pre` ◦ `q(cite)` ◦ `small` ◦ `span` ◦ `strike` ◦ `strong` ◦ `sub` ◦ `sup` ◦ `u` ◦ `ul`
Button	Configure the color of the buttons, such as the **Sign on** and **Save** buttons: ◦ **Button Fill**: The background color for the buttons. ◦ **Button Text**: The color of the text on the buttons. ◦ **Link Text**: The color of the text for links displayed on the buttons.
Text	The color of the text on the pages: ◦ **Heading Text**: The color of the text in headings. ◦ **Body Text**: The color of non-heading text.

Copyright © 2025 Ping Identity Corporation

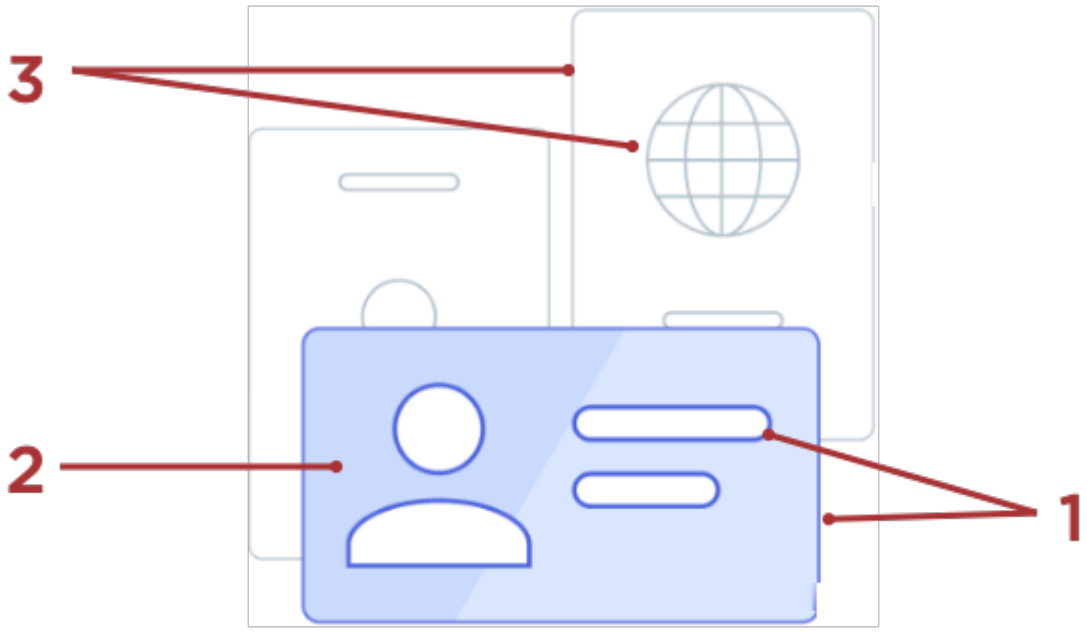
Setting	Description
Background	The background to use on each page. ◦ **None**: Do not use a background. ◦ **Image**: To use an image for the background, hover over the box and click the **Camera** icon (📷) to upload an image. Select an image in `jpg`, `jpeg`, `gif`, or `png` format up to 2 MB in size. To change the image used for the background, click 📷 and select **Upload New Image**. To delete a background image from a theme, click 📷 and select **Remove Image**. ◦ **Color**: Select a color to use for the background.
Card Color	The color of the box around form fields.

6. Click the **Forms** tab to edit global theme settings and preview the updated appearance of the PingOne forms in your environment.

> **Note**
>
> There are no component-specific styles for **Forms**.
> Your selections affect all forms, and can't be set at the form level, but you can select a form from the **Form Preview** list to preview it with theme styling applied. You can also click **Edit Form** to open the **Forms** page in a separate tab and make updates as necessary.
> Learn more in Forms.

7. On the **Verify** tab, click one of the tabs in the **Theme Styles** panel:
   - **Global**: Edit global theme settings and preview the updated appearance of identity verification pages.
   - **Component Specific**: Edit settings that only affect the appearance of the images on identity verification pages.

Copyright © 2025 Ping Identity Corporation



Setting	Description
Foreground Main (1)	The color used for the border around the front image and around the internal shapes in the front image.
Foreground Highlight (2)	The fill color used for the front image.
Background Outline (3)	The color used for the borders around the background images and around the internal shapes in the background images.

8. On the **End User Application** tab, click one of the tabs in the **Theme Styles** panel:
   - **Global**: Edit global theme settings and preview the updated appearance of system applications, such as the **Application Portal** and **Self-Service - My Account**.
   - **Component Specific**: Edit settings that only affect the appearance of system applications, such as the **Application Portal** and **Self-Service - My Account**.

Setting	Description
Background Color	The background color used for the application.

9. Click the **Authentication Policy** tab to edit global theme settings and preview the updated appearance of the sign-on and registration pages in your environment.

Copyright © 2025 Ping Identity Corporation

> **Note**
> There are no component-specific styles for **Authentication Policy**.

10. Click **Save**.

Next steps

Selecting an active theme

Selecting an active theme

Use the **Branding and Themes** page to apply an active theme to the current environment.

Steps

1. In the PingOne admin console, go to **User Experience** > **Branding and Themes** and browse or search for the theme that you want to use for the environment.
2. Click the **More Options** icon (⋮) and select **Set as Active Theme**.

   > **Note**
   > It can take up to 5 minutes for the new theme to appear to end users.

3. (Optional) To specify different branding for a particular form in the PingOne Forms connector, click the **More Options** (⋮) icon and select **Copy Theme ID**.

   Paste the ID into the configuration for the theme in DaVinci. Learn more in the PingOne Forms Connector documentation.

   > **Note**
   > The theme ID is also displayed on the details panel under the theme name.

Next steps

Customize a theme.

Deleting a theme

Use the **Branding and Themes** page to delete a theme you no longer need.

Steps

1. In the PingOne admin console, go to **User Experience** > **Branding and Themes** and browse or search for the theme you want to delete.
2. Click the **More Options** icon (⋮) and select **Delete Theme**.

Copyright © 2025 Ping Identity Corporation

> **Note**
> You can't delete the active theme.

3. On the **Confirm Delete** modal, click **Delete**.

Result

The theme is removed from the **Branding and Themes** page.

Self Service

Use the options on the **Self Service** page to determine what information appears to end users in the self-service portal, also known as the PingOne Self-Service - MyAccount app. For example, you might want to allow users to manage their own sessions or view agreements to which they've consented. Learn more in System applications.

You can find the following sections at **User Experience > Self Service** in the PingOne admin console:

- **Branding and Themes**: The options in this section define the look and feel of the self-service portal (MyAccount app). Learn more in Branding and themes.
- **Self Service**: The options in this section define the information that the end user sees in the self-service portal (MyAccount app), such as **Manage Authentication**, **View Agreements**, and **Change Password**. You can also select the **Sign Off Method** that PingOne uses when the end user signs off from the MyAccount app.

Learn more in Configuring the self-service portal.

Configuring the self-service portal

You can configure what information appears to end users in **Self Service**, also known as the PingOne Self-Service - MyAccount app. Learn more in System applications. You can also choose the sign-off method that PingOne uses when end users sign off from the MyAccount app.

Steps

1. In the PingOne admin console, go to **User Experience > Self Service**.
2. Click the **Pencil** icon.
3. Select or clear the following options as appropriate for your organization:

Setting	Description
Branding and Themes	
Apply Active Theme	Apply the branding and themes configured for the environment to the MyAccount app.
Show Footer	Show the theme's footer at the bottom of the MyAccount app.

Copyright © 2025 Ping Identity Corporation

Setting	Description
Self Service Section	
Manage Profile	Allow end users to edit their own profile attributes. If this option is enabled, end users can modify their profile details, such as name, address, and phone number. The specific attributes vary depending on the environment configuration.
Manage Authentication	Allow end users to manage their authentication methods, such as email, security key, text message, or authenticator app. **Important** Users should always include the country code when pairing a device. Phone formats across the globe are constantly expanding and changing. If the country code isn't included, issues might occur with message delivery. Choose from the following options: ◦ **Enable or Disable MFA**: Allow end users to enable or disable multi-factor authentication (MFA) for their account. This option is relevant for Customer Identity and Access Management (CIAM) users. ◦ **Manage PingID Devices via MyAccount**: Allow PingID users to manage their devices from the MyAccount app. This option is relevant for PingID workforce users from environments that are converged with PingOne. **Note** Selecting **Manage PingID Devices via My account** also: ■ Enables the **Allow user actions according to granted authentication scopes** option in the MyAccount app **Resources** tab. This option provides users with a limited set of scopes until they authenticate. ■ Adds the MyAccount app to all PingID policies that already include Device Management. ■ To allow PingID users to manage their account with limited scopes, you must also ensure an MFA policy or MFA DaVinci flow policy is added to the MyAccount app. ■ To add a policy to the app, refer to Associating an authentication policy with a web app. ■ To disable reduced scopes, refer to Editing scopes for an application. ■ Learn more about PingOne API scopes and their function in PingOne Self-management scopes. ◦ **None**: Do not enable either option.
Change Password	Allow end users to change their own passwords.

Copyright © 2025 Ping Identity Corporation

Setting	Description
Manage Linked Accounts	Allow end users to manage the linked accounts that are used during authentication.
Manage Sessions	Allow end users to view or sign off from PingOne sessions.
View Agreements	Allow users to see the agreements to which they've consented.
Manage OAuth Consents	Allow users to view and revoke OAuth consents to which they've agreed.
Sign Off Method	Determine which sign-off method PingOne uses when users sign off from the MyAccount app. Choose either of the following options: ◦ **OIDC Logout** (default): Allow the end user to sign off from the MyAccount app using OpenID Connect (OIDC) relying party (RP)-initiated logout. This option invalidates access tokens, refresh tokens, and ID tokens associated with the session. When selected, PingOne doesn't send SAML 2.0 single logout requests to SAML identity providers or applications. Learn more in the OIDC RP-Initiated Logout 1.0 documentation. ◦ **SAML 2.0 Single Logout**: Initiate SAML 2.0 single logout when the user signs off from the MyAccount app. Access tokens, refresh tokens, and ID tokens obtained during the session remain valid until they expire or are revoked.

4. Click **Save**.

Agreements

You can require end users to consent to an agreement that is part of a sign-on policy.

Whether to require consent is based on configuration settings and the user's consent history. If the user doesn't have any consents for any of the configured agreements, then PingOne will require the user to consent. End users can see their most recent consent in the self-service application. Administrators can use auditing to see a history of the consents that the end user has accepted. Learn more in Auditing for agreement consents.

You can configure an agreement for each language and locale. If there's no exact match, then PingOne defaults to the general language (without locale). If there is no language match, then PingOne uses the default language for the environment. You can find more information on adding languages in Languages.

For the localized agreement text, you can use any UTF-8 characters up to a maximum of 32,000 characters.

Viewing agreements

Use the **Agreements** page to view existing agreements.

Copyright © 2025 Ping Identity Corporation

Steps

1. In the PingOne admin console, go to **User Experience > Agreements**.
2. Click an agreement entry to open the details panel.

Result

The Agreement details page shows:

Overview tab

- **Name**: The name of the agreement.
- **Description**: A brief characterization of the agreement.
- **Reconsent every**: The duration of the agreement consent, that is, how often the user will have to re-consent to the agreement.
- **Languages**: The localized content that has been added for the agreement, including enabled and disabled languages. To modify, click **Edit localized content**.

API tab

- **ID**: The unique identifier for the agreement.
- **Environment ID**: The unique identifier for the environment that the agreement is configured for.
- **API URL**: The PingOne API endpoint that contains the agreement.
- **JSON**: The JSON object that represents the agreement.

Related links

- Adding an agreement
- Enabling or disabling an agreement

Adding an agreement

Use the **Agreements** page to create a new agreement. You can use agreements to prompt your users to consent to various policies. Learn more in Authentication policies.

Steps

1. In the PingOne admin console, go to **User Experience > Agreements**.
2. Click the **+** icon.
3. Enter the following information:
    - **Name**: A unique identifier for the agreement.
    - **Description** (optional): A brief characterization of the agreement.

Copyright © 2025 Ping Identity Corporation

- **Reconsent every**: Specify the duration of the agreement consent, that is, how often the user will have to reconsent to the agreement. Select **Never**, or select **Number of days** and enter a value.

4. Click **Save**.

Result

The agreement is created and added to the **Agreements** list.

Next steps

Adding a language to an agreement

Adding a language to an agreement

After you've created an agreement, add localized content to the agreement. If the content has already been added to the agreement, you can skip this step. One agreement can consist of multiple language versions of the agreement.

Steps

1. In the PingOne admin console, go to **User Experience** > **Agreements**.
2. In the **Agreements** list, locate the agreement you want to edit. Click the agreement entry to open the details panel.
3. On the **Overview** tab, click the **Edit Localized Content** button.
4. For **Languages**, click the **+** button. Learn more in Languages.
5. For **Language**, select the language that the agreement will use.
6. Click **Save**.

   Result:

   The language is added to the configured languages for the agreement.

Next steps

Creating localized content

Creating localized content

After you add a language version to an agreement, you can enter the localized text that makes up the agreement. Each time you modify the localized agreement content, the revision number is incremented. You configure each new revision to require re-consent, if needed.

Steps

1. In the PingOne admin console, go to **User Experience** > **Agreements**.
2. In the **Agreements** list, locate the agreement you want to edit. Click the agreement entry to open the details panel.
3. On the **Overview** tab, click the **Edit Localized Content** button.

Copyright © 2025 Ping Identity Corporation

4. On the left side, under **Languages**, click the language you want to edit.
5. Enter or edit the following information:
   - **Localized agreement title**: Enter or edit the title as it should appear in this language.
   - **Agreement format**: Specify the type of content for the agreement text: plain text or HTML. With HTML, you can style the agreement text and include hyperlinks. The following HTML elements are allowed: `a`, `br`, `p`, `b`, `i`, `em`, `h1`, `h2`, `h3`, `strong`.

     > **Note**
     > - Hyperlinks must use the `https` protocol.
     > - To set up a hyperlink that opens in a new browser window, add the `target="blank"` attribute to the `<a>` element. For example, `<a href="https://www.example.com" target="blank">Terms and conditions</a>`.
     > - The `<script>` element is not allowed.

   - **Localized Agreement Content**: Enter or paste the text of the agreement.
   - **Acceptance label**: The text that is displayed for the affirmative option. For example, `I accept`.
   - **Continue label**: The text that is displayed for the user to continue after accepting the agreement. For example, `Continue`.
   - **Don't accept label**: The text that is displayed for the negative option. For example, `I don't accept`.
   - **Effective date**: Specify when the agreement should go into effect.
   - **Require new consent**: Specify whether users will have to re-consent if the agreement is updated.
6. Click **Save**.

Next steps

Previewing an agreement

Previewing an agreement

After you have created an agreement, you can preview it to see how it will look to end users. The agreement will use the theme that is configured for your environment. Learn more in Branding and themes.

Steps

1. In the PingOne admin console, go to **User Experience > Agreements**.
2. In the **Agreements** list, locate the agreement you want to preview. Click the agreement entry to open the details panel.
3. On the **Overview** tab, click the **Edit Localized Content** button.
4. On the left side, under **Languages**, click the language you want to preview.
5. In the **Revision** list, select the revision you want to preview, and then click **Preview**.

   Result:

Copyright © 2025 Ping Identity Corporation

The agreement is displayed as it will appear to the end user using the theme that is configured for your environment.

Next steps

Enabling a language for an agreement

Enabling a language for an agreement

After you have created the localized agreement content, you can enable the appropriate languages for the agreement.

Steps

1. In the PingOne admin console, go to **User Experience** > **Agreements**.
2. In the **Agreements** list, locate the agreement for which you want to enable a language. Click the agreement entry to open the details panel.
3. On the **Overview** tab, click the **Edit Localized Content** button.
4. On the left side, under **Languages**, click the language you want to enable.
5. Click the toggle to enable the configured language. The toggle moves to the left (gray) when disabled and to the right (green) when enabled.

> **Note**
>
> Ensure that the language you selected is enabled for the current environment. Learn more in Languages.

Next steps

Enabling or disabling an agreement

Enabling or disabling an agreement

After you have created the localized agreement content and enabled the configured language, you can enable the agreement. If an agreement has existing consents, you cannot delete it because the history of user consents are preserved, but you can disable it.

Steps

1. In the PingOne admin console, go to **User Experience** > **Agreements**.
2. In the **Agreements** list, locate the agreement you want to enable or disable.
3. Click the toggle switch on the right to enable the agreement. The toggle moves to the left (gray) when disabled and to the right (green) when enabled.

> **Note**
>
> If you disable an agreement, it will no longer be part of the sign-on policy.

Copyright © 2025 Ping Identity Corporation

Next steps

Adding the agreement to the authentication policy

Adding the agreement to the authentication policy

To start gathering consents from end users, add the agreement to the appropriate authentication policy.

Steps

1. In the PingOne admin console, go to **Authentication** > **Authentication**.
2. Open the authentication policy you want to add the agreement to.
3. Click the icon to open the policy in edit mode.
4. Click **+ Add step**.
5. Select **Terms of service prompt**.
6. For **Terms of service agreement**, select the appropriate agreement. If the expected agreement isn't shown, it might not have been added. Learn more in Adding an agreement.
7. To see the agreement as it will appear to end users, click **Preview**.
8. Click **Save**.

Viewing previous revisions

To view previous versions of your agreement:

Steps

1. In the PingOne admin console, go to **User Experience** > **Agreements**.
2. In the **Agreements** list, locate the agreement you want to view. Click the agreement entry to open the details panel.
3. On the **Overview** tab, click **Edit Localized Content**.
4. On the left side, under **Languages**, click the language you want to preview.
5. In the **Revision** list, select the version you want to view.
6. Click the **Preview** button.

Deleting an agreement

You can delete an agreement that you no longer need. If an agreement has existing consents, you cannot delete it because the history of user consents are preserved. You can, however, disable it. Learn more in Enabling or disabling an agreement.

Copyright © 2025 Ping Identity Corporation

Steps

1. In PingOne admin console, go to **User Experience** > **Agreements**.
2. In the **Agreements** list, locate the agreement you want to delete.
3. On the right, click the three dots option menu and then click **Delete**.
4. In the confirmation message, click **Delete**.

Auditing for agreement consents

You can run an audit report to see more information about agreements, such as when an agreement was accepted or revoked. You can also use the **User details** page to see a user's consent history. Learn more in Viewing the consent history for a specific user.

Steps

1. In the PingOne admin console, go to **Monitoring** > **Audit**.
2. For **Time range**, enter the appropriate time span for the report.
3. For **Filter type**, select **Event type**.
4. For **Filter**, select one or more of the following. You can search or browse for event types.
   - **Agreement accepted**: An agreement was accepted by the end user.
   - **Agreement revoked**: An agreement was revoked by the end user.
5. To limit the report to a particular user, use a secondary filter with `User Name` or `User ID`.
6. Click **Run**.

Viewing the consent history for a specific user

You can view the **User details** page to see the consent history for a particular user. You can also use the **Audit** page to see a user's consent history. Learn more in Auditing for agreement consents.

Steps

1. In the PingOne admin console, go to **Directory** > **Users**.
2. Browse or search for the user you want to view.
3. Click the user entry to open the details panel.
4. Click **Services** > **Consent**.

Result

The **Consent** page shows the latest agreement to which the user has consented, including the agreement name, language, and date. Click **View** to see a preview of the agreement to which the user has consented.

Copyright © 2025 Ping Identity Corporation

Languages

You can configure one or more languages for the text that is presented to end users in notifications and agreements.

Add an entry for each language that you want to configure for an environment. Use a language-locale pair, such as `American English (en-US)`, to customize text for more specific language variants when you configure agreements.

PingOne uses the user's browser locale and `preferredLanguage` attribute, if set, to determine which language to present to a user. If there is no content configured for a user's requested language-locale pair, PingOne will show content for the default language configured for the environment.

Viewing languages

Use the **Languages** page to see the languages that are currently configured for your PingOne environment.

To view configured languages:

Steps

1. In the PingOne admin console, go to **User Experience** > **Languages**.

   Result:

   The configured languages are shown in the language list with the following labels:

   Default language

   The default language for your environment. If there is no other language that matches a user's language and locale, PingOne will use this language.

   Enabled languages

   Languages that have been added to PingOne and are ready for PingOne to use.

   Disabled languages

   Languages that have been added to PingOne, but are not currently enabled.

2. Click a language entry to open the details panel.

   > **Note**
   > You can view translatable keys, compare their translation between languages, and edit the translations.

Next steps

- Changing the default language
- Adding a language
- Configuring localized content

Copyright © 2025 Ping Identity Corporation

Changing the default language

Use the **Languages** page to change the default language.

The default language is the language that most users of your applications will see when they receive a notification or agreement.

To change the default language:

Steps

1. In the PingOne admin console, go to **User Experience** > **Languages**.
2. In the **Enabled languages** section, to the right of the language that you want to be the default language, click the **More Options** (⋮) icon, and then click **Make default**.
3. In the confirmation message, click **Confirm**.

> **Note**
>
> To set a language as the default language, it must be enabled and have no configuration issues, such as incomplete localized text. Learn more in Viewing languages and Enabling or disabling a language.

Adding a language

Use the **Languages** page to add a language to your PingOne environment.

To add a language to your environment:

Steps

1. In the PingOne admin console, go to **User Experience** > **Languages**.
2. At the top of the page, click the **+** icon.
3. In the **Languages** section, select a language from the list by browsing or searching for it.

> **Note**
>
> You can select a generic language, such as **English (en)**, or a language-locale pair, such as **US English (en-US)**. The languages in the list are preconfigured.

4. Click **Save changes**.

Next steps

Configuring localized content

Deleting a language

Use the **Languages** page to delete languages from your PingOne environment.

Copyright © 2025 Ping Identity Corporation

You can delete a language you no longer need. If you don't want to delete a language, you can disable it. Learn more in Enabling or disabling a language

Steps

1. In the PingOne admin console, go to **User Experience** > **Languages**.
2. In the list, locate the language you want to delete.

   > **Note**
   > You cannot delete the provided languages or the default language, but you can delete any custom language.

3. On the right side, click the **More Options** (⋮) icon and then click **Remove**.
4. In the confirmation message, click **Delete**.

Enabling or disabling a language

After you have configured the content for a language, enable it on the **Languages** page.

Instead of deleting a language, you can disable a language you don't need. If a language is disabled, you can't configure agreements or notifications in that language.

Steps

1. In the PingOne admin console, go to **User Experience** > **Languages**.
2. In the list, click the language you want to enable or disable.

   Result:

   The details panel for the selected language opens.

3. In the upper right, click the toggle.

   Result:

   The toggle moves to the left (gray) when disabled, and to the right (blue) when enabled.

Configuring localized content

Use the **Agreements**, **Notification Templates**, and **Forms** pages to set up localized content for each language.

Steps

- To set up localization for agreements, follow the steps for Creating localized content.
- To set up localization for notifications, follow the steps in Notification templates.
- To set up localization for PingOne Forms, follow the steps for Using translatable keys.

Copyright © 2025 Ping Identity Corporation

Next steps

Make sure that the appropriate language is enabled for that language to appear in end user sign-on screens. Learn more in Enabling or disabling a language.

Modifying translatable keys

You can create custom text for various user-facing screens in a particular language.

To modify the translation for a key:

Steps

1. In the PingOne admin console, go to **User Experience** > **Languages**.
2. In the list, click the language you want to edit.

   Result:

   The details panel for the selected language opens.
3. In the **Module** list, select a module to view the associated keys.

   > **Note**
   >
   > The module you select only displays the keys for that section of your PingOne environment.
4. In the **Page** list, select a page to view the associated keys.
5. (Optional) In the **Search** bar, enter a key to search for it.
6. (Optional) Click **Compare to:** and select another language from the list to compare with a language other than the default language.
7. Click the icon above the key translations.

   Result:

   You can now edit the fields for translations, and you see the **Save** and **Cancel** buttons at the bottom of the page.
8. Edit the text in the translation field to your preferred translation.
9. Click **Save**.

Next steps

Repeat the steps for any keys for which you want to provide a custom translation. After you have finished modifying translatable keys, ensure localization is configured. Learn more in Configuring localized content.

Deleting translatable keys

You can delete custom keys for a language. The deletion of translatable keys is only available for the English language.

Copyright © 2025 Ping Identity Corporation

> **Note**
> Default keys are disabled and cannot be deleted.

Steps

1. In the PingOne admin console, go to User Experience > Languages.
2. In the list, select a language to edit.

   Result:

   The details panel for the selected language opens.
3. In the **Module** list, select a module to view the associated keys.

   > **Note**
   > Key deletion is supported only for the **DaVinci** module.
4. In the **Page** list, select a page to view the associated keys.

   > **Note**
   > Key deletion is supported only for the **Custom Messages** page.
5. Click **Delete Keys**.

   Result:

   A **Delete Key** column of checkboxes is added to the right of the **Key** column.
6. In the **Delete Key** column, select the key or keys to delete.
7. Click **Delete** at the bottom of the list, then confirm deletion in the modal.

Result

The selected keys are deleted.

Adding a custom key for DaVinci

In addition to the Ping-provided default **Standard Fields**, you can create custom key-value pairs that provide translatable text for various user-facing screens in DaVinci. The addition of custom keys is only available for the English language.

To add a custom key:

Steps

1. In the PingOne admin console, go to **User Experience > Languages**.
2. Enable the languages for which you would like to add localized content.
3. Click **English (en)** to open the details panel so that you can add the necessary custom keys.

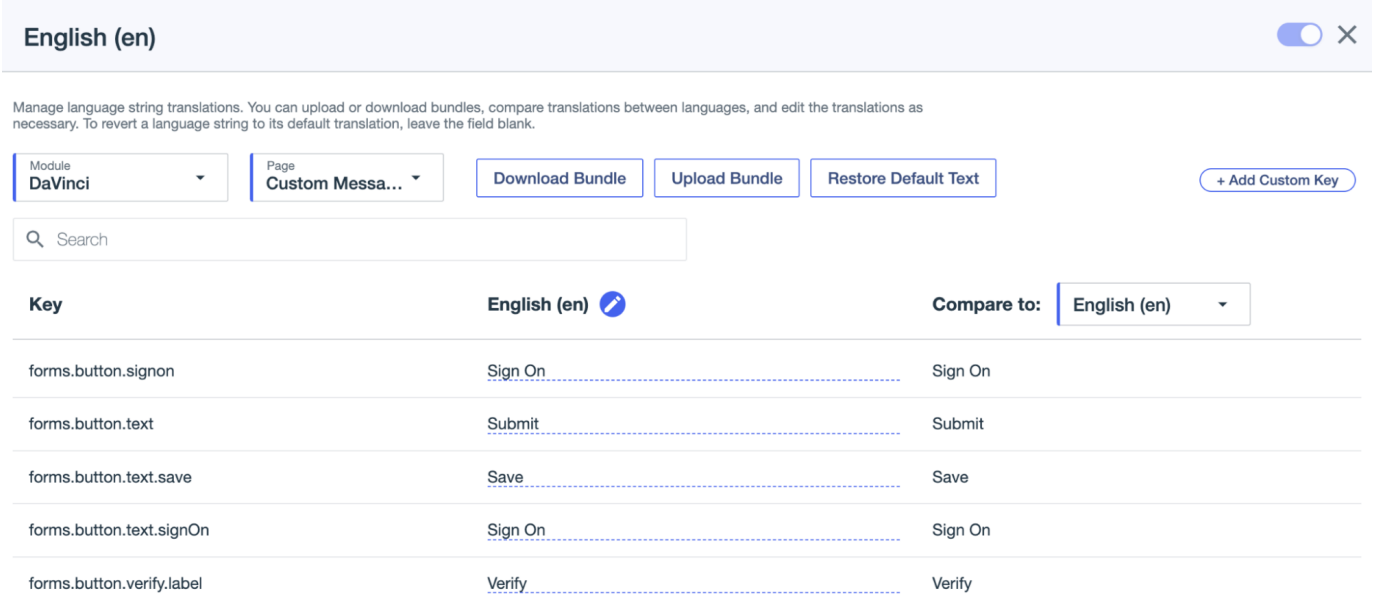
Copyright © 2025 Ping Identity Corporation

Result:

The details panel for the **English** language opens.

4. In the **Module** list, select the module to view the associated keys.

> **Note**
>
> When modifying keys for the module, both forms configured with PingOne Forms and custom HTML-based forms can use the translatable text.

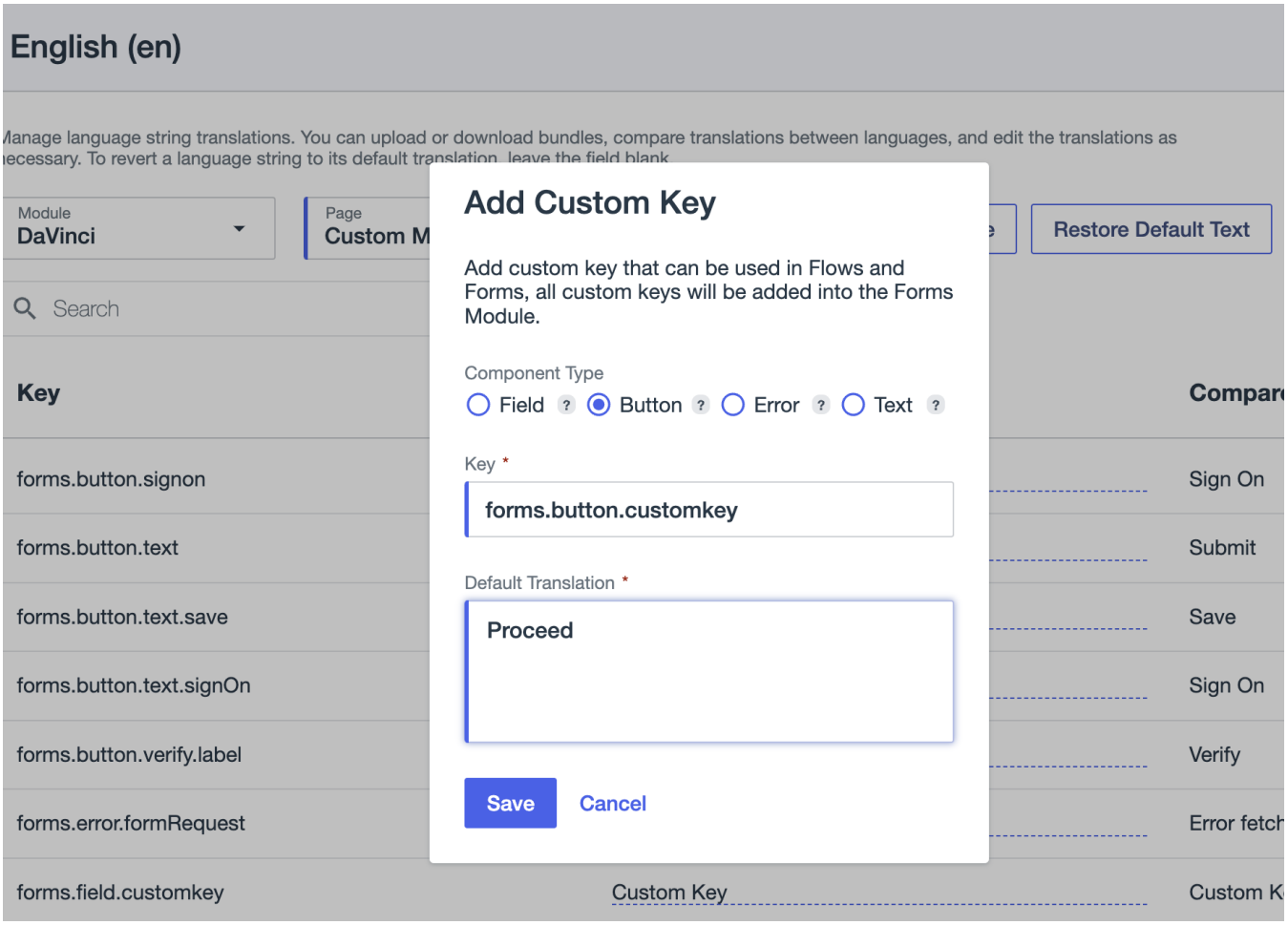


5. In the **Page** list, select the **Custom Messages** page to view the associated keys.

6. Click **+ Add Custom Key**.

7. Select the **Component Type**.

Copyright © 2025 Ping Identity Corporation



8. Change the generated unique **Key** value.

> **Note**
>
> - The key must start with a `forms.` prefix and can only contain letters, numbers, dashes, underscores, or dots.
> - The maximum of key-value pairs for the DaVinci **Custom Messages** section is limited to 500.

9. Add a **Default Translation** in English.

> **Note**
>
> The **Default Translation** cannot be more than 1024 characters.

10. Click **Save**.

Setting up DaVinci Forms for multi-language support

This use case covers how to set up the translatable text in forms with multiple langauges that will be translated based on the language settings in the end user's browser settings.

To set up forms for translations from English to another language:

Copyright © 2025 Ping Identity Corporation

Steps

1. To set up the desired languages with custom keys in **User Experience > Languages**:
    1. Enable the languages for which you would like to provide translations, such as **French**, **Chinese**, and **German**. Learn more in Enabling or disabling a language.
    2. Make sure that **English** is the default language. Learn more in Changing the default language.
    3. Export the default language **English** page. Learn more in Downloading a language bundle.
    4. Add any additional content in the CSV file for **English**.

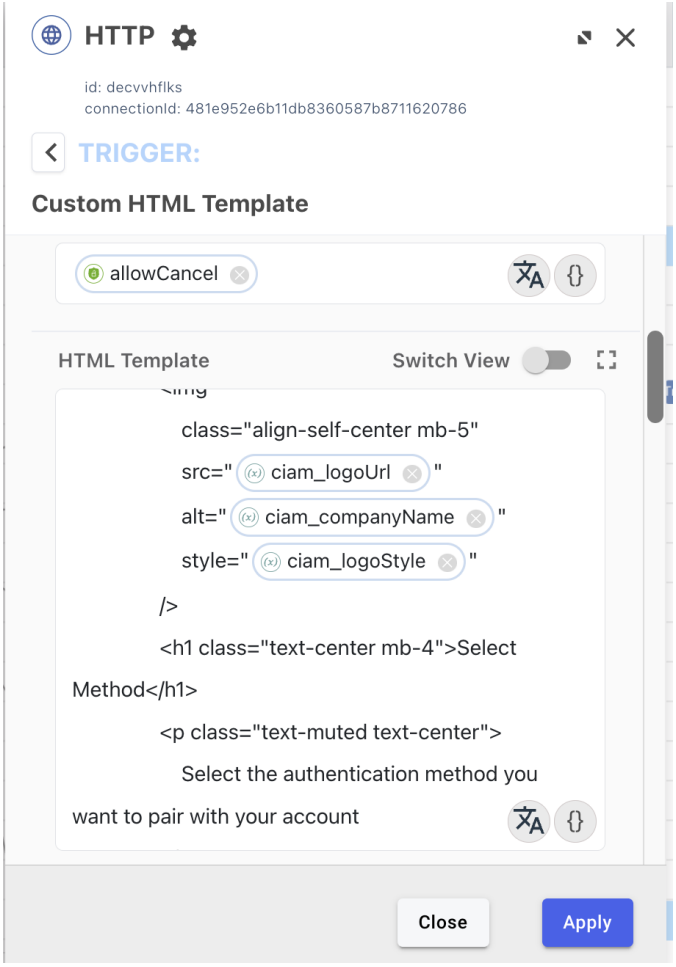
    > **Note**
    >
    > The **Key** must start with a `forms.` prefix and can only contain letters, numbers, dashes, underscores, or dots.

    5. Upload the bundle for **English** with the added key-value pairs.
    6. Export the content in the bundle for the translated language, such as **French**, **Chinese**, and **German**. Learn more in Uploading a language bundle.
2. Configure the PingOne Forms connector capabilities in a flow with the selected keys.

    For example, you can select the message keys for:

    - **Custom HTML Template** Forms using the HTTP connector

Copyright © 2025 Ping Identity Corporation



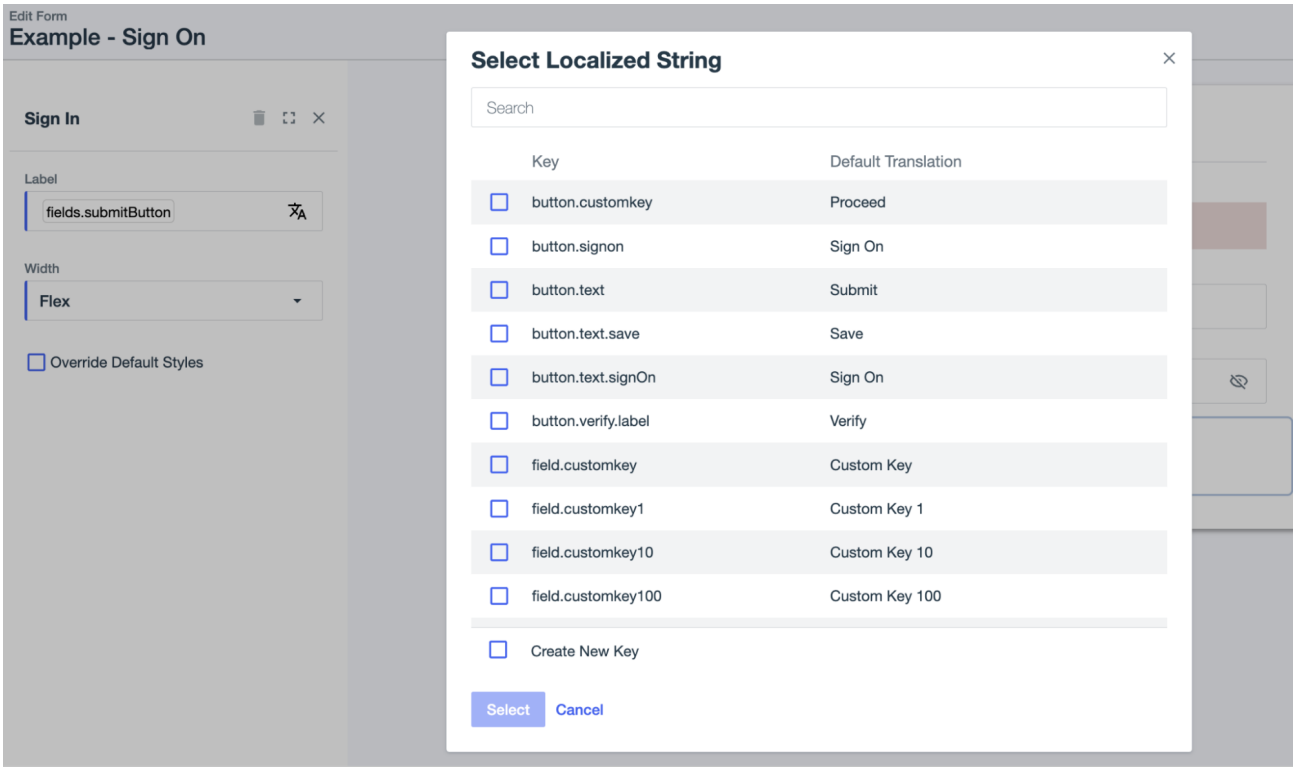
> **Note**
>
> Click the **Translation** ( ) icon. A modal with a list of the available keys and their default translations opens.

> **Note**
>
> Select the appropriate **Key**. To define a unique key and default translation, select **Create New Key**.

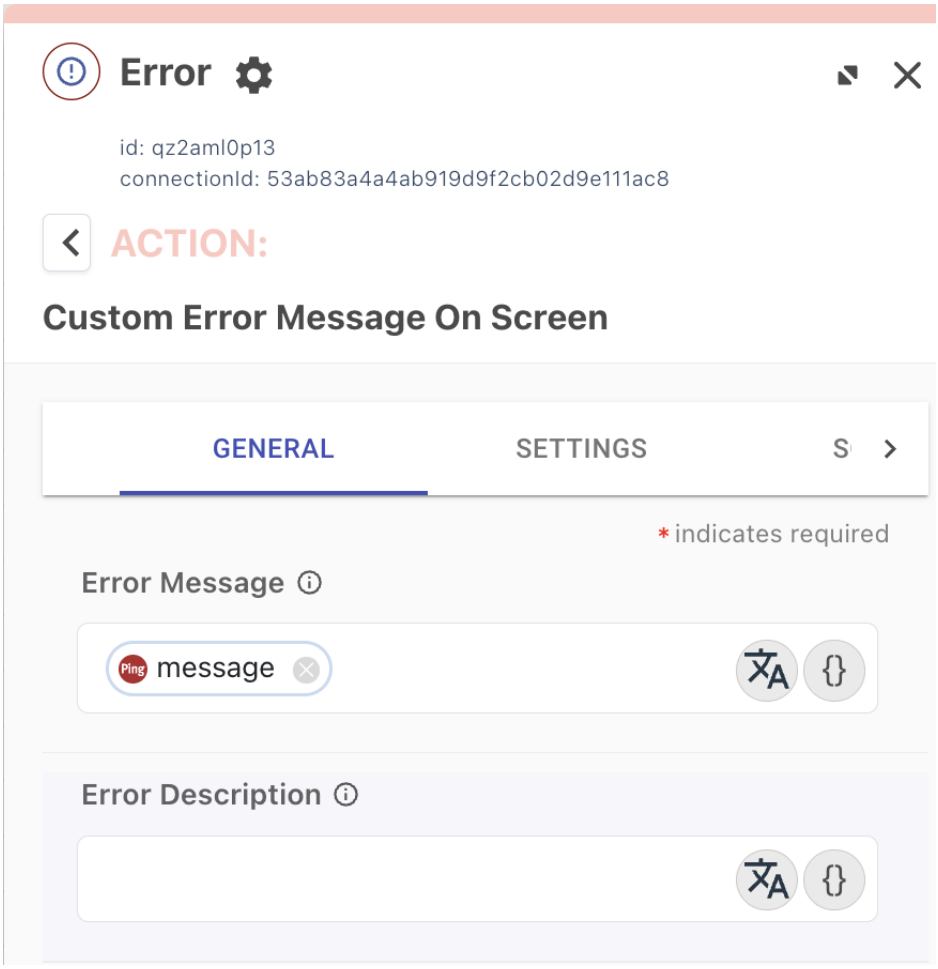
- PingOne Forms using the PingOne Forms connector

> **Note**
>
> Learn more in Using translatable keys.

Copyright © 2025 Ping Identity Corporation



- Custom error messages in the Error Message connector



When added in the flow, you will see the English texts for the keys. However, when the flow is executed in the browser, the texts associated with the keys will render in adherence with the default language of the end-user's browsers.

Downloading a language bundle

You can download a language bundle as a CSV file that contains the keys and associated text for that language. You can send this file to a translation service, and then import the translated content.

To download a complete language pack or for a particular page under a module:

Steps

1. To download the entire language pack for a particular language:
    1. In the PingOne admin console, go to **User Experience > Languages**.
    2. In the list, to the right of the language that you want to download the language bundle for, click the **More Options** (⋮) icon.
    3. Click **Download Bundle**.

Copyright © 2025 Ping Identity Corporation

2. To download the translatable keys for a particular page under a module:
    1. In the list, click the language you want to edit.

       Result:

       The details panel for the selected language opens.
    2. In the **Module** menu, select the module from which you would like to download the associated translatable keys.
    3. In the **Page** menu, select the page from which you would like to download translatable keys.
    4. Select **Download Bundle** at the top of the configuration panel.
    5. In the confirmation message, click **Download**.

Result

The bundle is saved the `Downloads` directory on your local file system.

Uploading a language bundle

You can import language bundles from a translation service for localizing languages that are not already available in PingOne. Uploading a bundle allows you to create new keys in English and update the translations for existing keys in English and other languages for the custom messages.

To import a language bundle:

Steps

1. To upload the entire language pack for a particular language:
    1. In the PingOne admin console, go to **User Experience** > **Languages**.
    2. In the list, to the right of the language for which you want to upload the language bundle, click the **More Options** (⋮) icon.
    3. Click **Upload Bundle**.
2. To upload the translatable keys for a particular page under a module:
    1. In the PingOne admin console, go to **User Experience** > **Languages**.
    2. In the list, select the language you want to edit.

       Result:

       The details panel for the selected language opens.
    3. In the **Module** list, select the module for which you would like to upload the associated translatable keys.
    4. In the **Page** list, select the page for which you would like to download the associated keys.
    5. Select **Upload Bundle** at the top of the configuration panel.
    6. In the modal, select **Select a file** and open the `CSV` file from your device.

Copyright © 2025 Ping Identity Corporation

7. Click **Upload**.

Next steps

Ensure that the uploaded language is enabled. Learn more in Enabling or disabling a language.

Forms

DaVinci Forms is a drag-and-drop form builder that allows you to create custom forms without having to write HTML.

Creating forms with DaVinci Forms and the PingOne Forms connector allows you to quickly include user-facing forms in your DaVinci flows. You can use templates to create forms for registration, sign-on password reset, and password recovery use cases, or create a custom form. Learn more in:

- Create custom forms
- Apply branding and themes
- Localize content with translatable keys

After you've created these forms in the **User Experience** > **Forms** section, you can implement them in your DaVinci flow with the PingOne Forms connector. You can find more information on the PingOne Forms connector in PingOne Forms connector.

Creating a form

Creating a form in PingOne allows you to provide branded user experiences through custom forms without writing custom HTML and quickly implement these forms in DaVinci with the PingOne Forms connector. After you create a form in **User Experience** > **Forms**, either by starting with a blank form or selecting a templated form, you can configure your form Form properties, Forms fields, and the Form toolbox.

In this example, you create a form using a template that is set up for your own branding and localization to be quickly included in a DaVinci flow.

Steps

1. Create a form in PingOne:
    1. In the PingOne admin console, go to **User Experience** > **Forms**.
    2. Click the **+** icon.
    3. In the **Form Name** field, enter a name for the form.

    > **Note**
    > This form name is used internally and is not displayed to users.

    4. (Optional) In the **Form Description** field, enter a description for the form.
    5. Select a **Form Usage**.
    6. Click **Add Form**.

Copyright © 2025 Ping Identity Corporation

Result:

A modal opens listing the available templates.

7. Select **Blank Form** to create a custom form or select a preconfigured form that's appropriate for your use case.

2. Configure your form with the Form properties, Form fields, and Form toolbox.
3. In the **User Experience > Branding and Themes** section, customize your form with branding and themes. Learn more in Branding and Themes.

> **Important**
>
> If you have customizations in DaVinci Forms as well as in **Branding and Themes**, the style configured in DaVinci Forms takes precedence over styles configured in **Branding and Themes**.

4. To support localization for the user-facing text in your form, add translatable keys in the configuration settings for the form. Learn more in Using translatable keys.
5. To implement the form in DaVinci, add and configure the PingOne Form connector in DaVinci. Learn more in PingOne Forms connector documentation.

Configuring a sign-on form

You can use forms created in **User Experience > Forms** to allow users to sign on with credentials, social login providers, or a magic link.

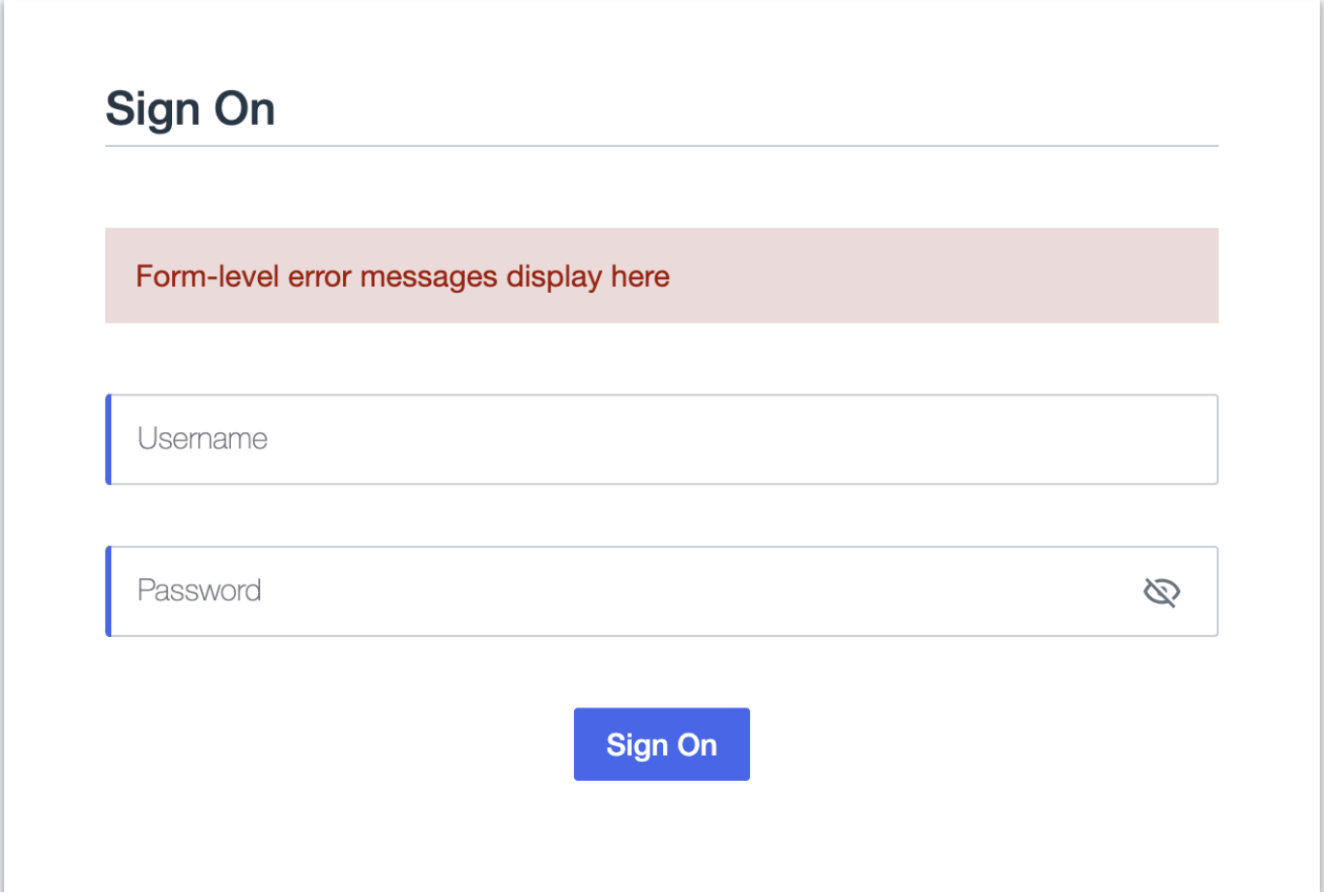
Creating a sign-on form with username and password

To configure a simple sign-on form to allow users to authenticate with their credentials:

Steps

1. In the PingOne admin console, go to **User Experience > Forms**.
2. Click the **+** icon and select the **Sign On** template.
3. (Optional) Customize the templated form using the form builder. Learn more in Form properties, Form fields, and Form toolbox.

Copyright © 2025 Ping Identity Corporation



4. Click **Save**.

Result

You can now use the form in your DaVinci flow with the PingOne Forms connector.

Creating a sign-on form with social login

Before you begin

In the PingOne admin console, go to **Integrations** > **External IdPs** and configure social login providers. Learn more in Adding a vendor-specific identity provider in PingOne.

> **Note**
> If you don't have social login providers configured in your PingOne environment, the **Social Login** component won't be available in the form builder.

Copyright © 2025 Ping Identity Corporation

Steps

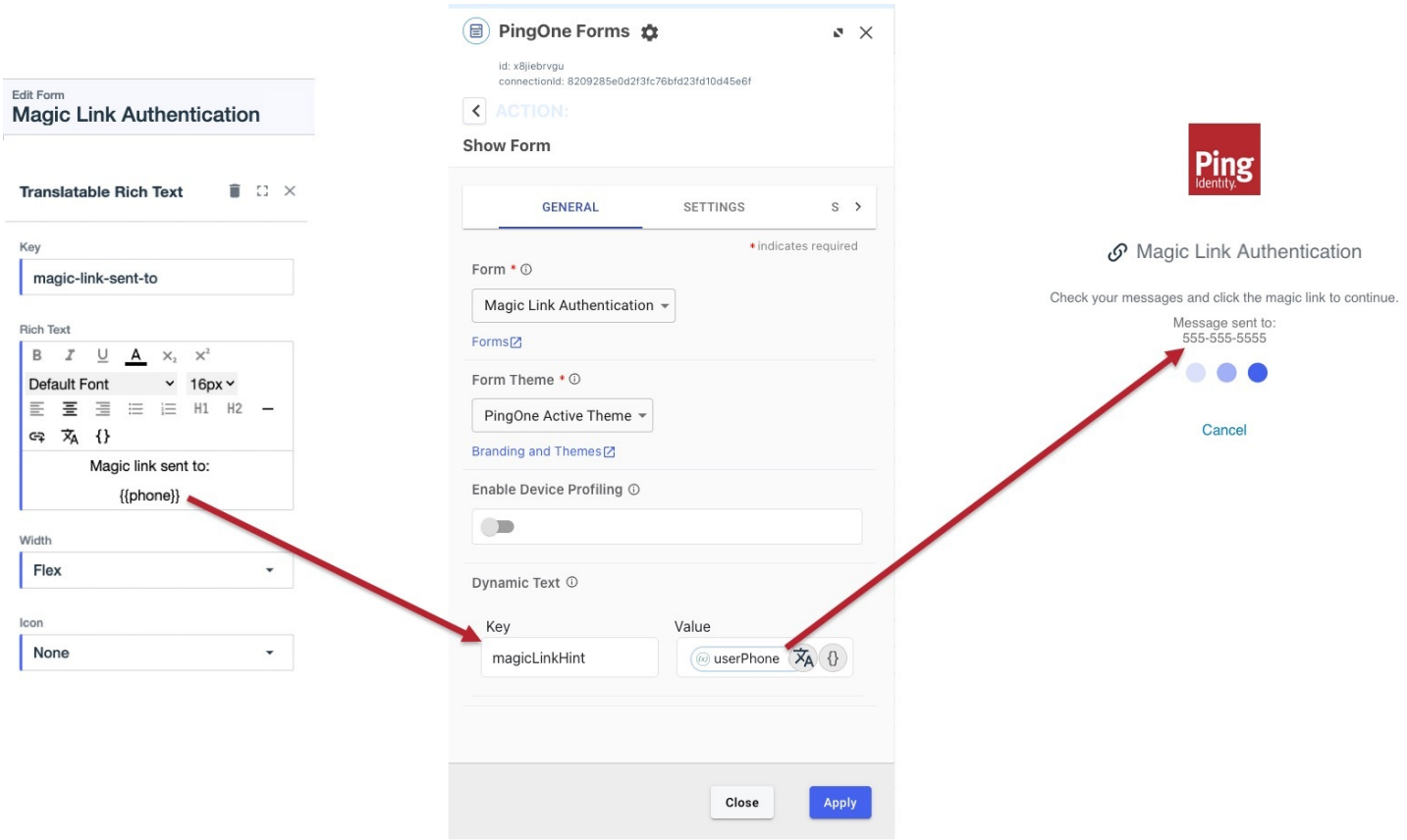
To configure a sign-on form with social login:

1. In the PingOne admin console, go to **User Experience** > **Forms**, click **+** and select the **Sign On** template.
2. Add a **Divider** component and optionally add a centered label, such as `OR`, to the divider.
3. Add one or more **Social Login** components below the divider to allow the end user to authenticate with social login.
4. (Optional) You can further customize the templated form in the form builder. Learn more in Form properties, Form fields, and Form toolbox.

Result

You can now use the form in your DaVinci flow with the PingOne Forms connector.

Creating a sign-on form with a magic link



To configure a sign-on form with magic link:

Steps

1. Create an email prompt form:
    1. In the PingOne admin console, go to **User Experience** > **Forms**.
    2. Click **+** and select **Blank Form**.
    3. In the **Form Name** field, enter a title for the form, such as `Sign On`.
    4. (Optional) Enter a **Form Description**.
    5. In **Fields** > **PingOne Attribute Fields** > **Contact**, drag an **Email** field onto the form.
    6. In the **Form Toolbox**, drag a **Submit Button** component onto the form.
2. Create a magic link prompt form:
    1. In the PingOne admin console, go to **User Experience** > **Forms**.
    2. Create a form with the **Magic Link Prompt** template.
    3. (Optional) Customize the templated form using the form builder. Learn more in Form properties, Form fields, and Form toolbox.
3. Configure the DaVinci flow:
    1. Add a Challenge connector node in your flow and create an out-of-band challenge flow pattern. Learn more about creating challenges in Challenge connector.
    2. Add a PingOne Forms connector node and select the **Show Form** capability.
    3. Toggle **Enable Polling** on and set it up to poll the challenge created earlier in the flow by the Challenge connector.
    4. In the **Dynamic Text** table, map the user's email address or phone number with the `magicLinkHint` **Key**.

Configuring a registration form

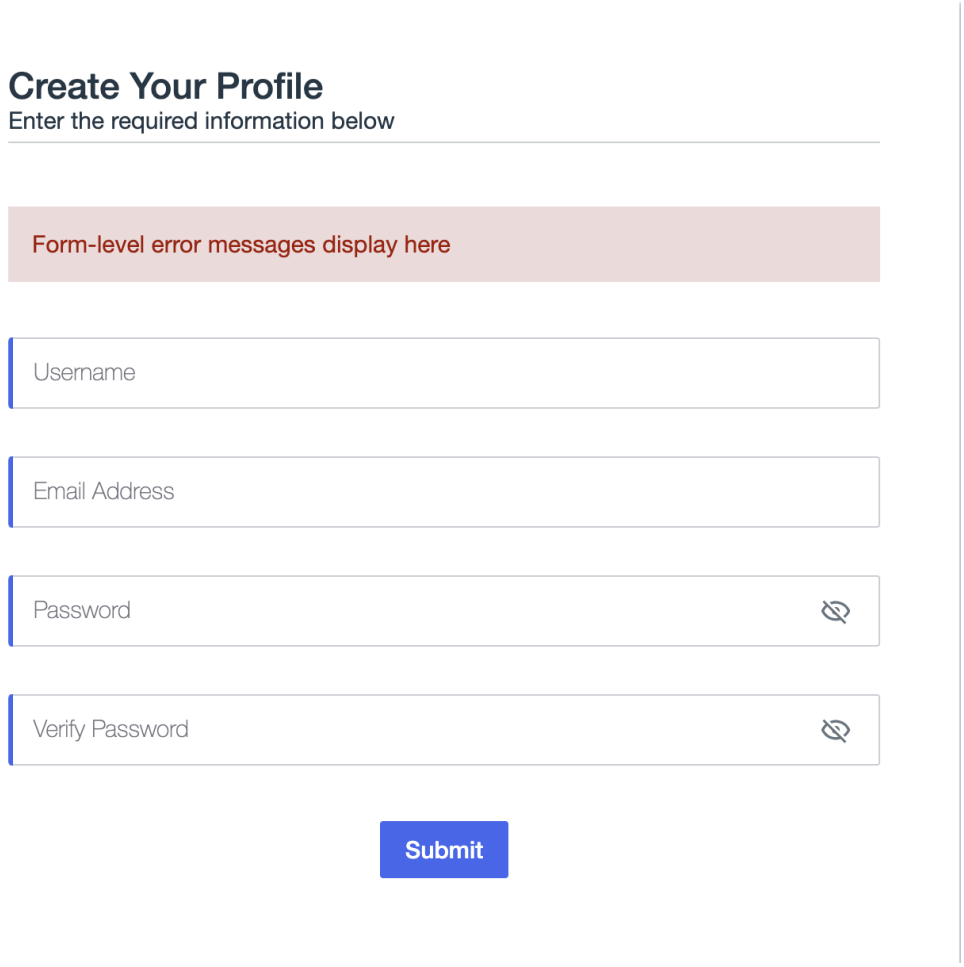
You can use forms created in **User Experience** > **Forms** to allow users to register and sign terms and conditions configured in **User Experience** > **Agreements**. You can find more information on configuring agreements for use in forms in Agreements.

To create a simple registration form with agreements:

Steps

1. In the PingOne admin console, go to **User Experience** > **Forms**.
2. Click the **+** icon and select the **Agreement** form.
3. (Optional) Customize the templated form using the form builder. Learn more in Form properties, Form fields, and Form toolbox.

Copyright © 2025 Ping Identity Corporation



Result

You can now use the form in your DaVinci flow with the PingOne Forms connector.

Configuring an MFA form

You can use forms created in **User Experience** > **Forms** to allow users to register and authenticate with multi-factor authentication (MFA), by one-time passcode (OTP), FIDO2, or an authenticator app.

Creating an MFA form with OTP

To create an MFA form for registration or authentication with OTP:

Steps

1. In the PingOne admin console, go to **User Experience** > **Forms**.

Copyright © 2025 Ping Identity Corporation

2. Click the + icon and select one of the following OTP templates:
    - **Email OTP Prompt - Registration**
    - **Email OTP Prompt - Authentication**
    - **Text Message OTP Prompt - Registration**
    - **Text Message OTP Prompt - Authentication**
    - **Voice OTP Prompt - Registration**
    - **Voice OTP Prompt - Authentication**
3. (Optional) Customize the templated form in the form builder.
4. Click **Save**.

Result

You can now use the form in your DaVinci flow with the PingOne Forms connector.

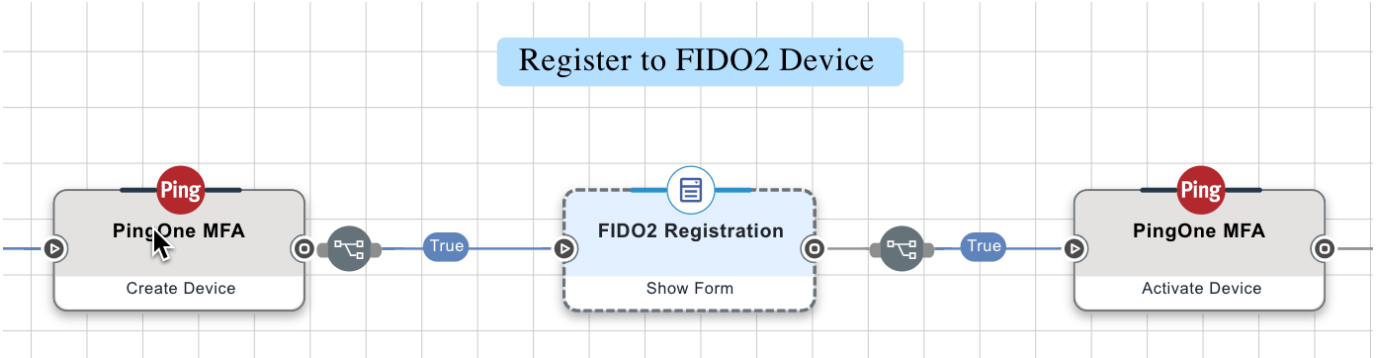
Creating an MFA form with FIDO2 registration

To configure FIDO2 in PingOne Forms for registration:

Steps

1. Create a FIDO2 form:
    1. In the PingOne admin console, go to **User Experience** > **Forms**.
    2. Click the + icon and select the **FIDO2 - Registration** template.
    3. (Optional) Customize the templated form in the form builder.
    4. Click **Save**.
2. In DaVinci, configure the flow.

Copyright © 2025 Ping Identity Corporation



1. Add a PingOne MFA connector node and select the **Create Device** capability.

> **Important**
>
> This connector is necessary for **Public Key Credential Creation** field in the following PingOne Forms connector.

2. In a subsequent node, add a PingOne Forms connector and select the **Show Form** capability, then select the FIDO2 registration form you created in **User Experience** > **Forms**.
3. In a subsequent node, add another PingOne MFA node and select the **Activate Device** capability.

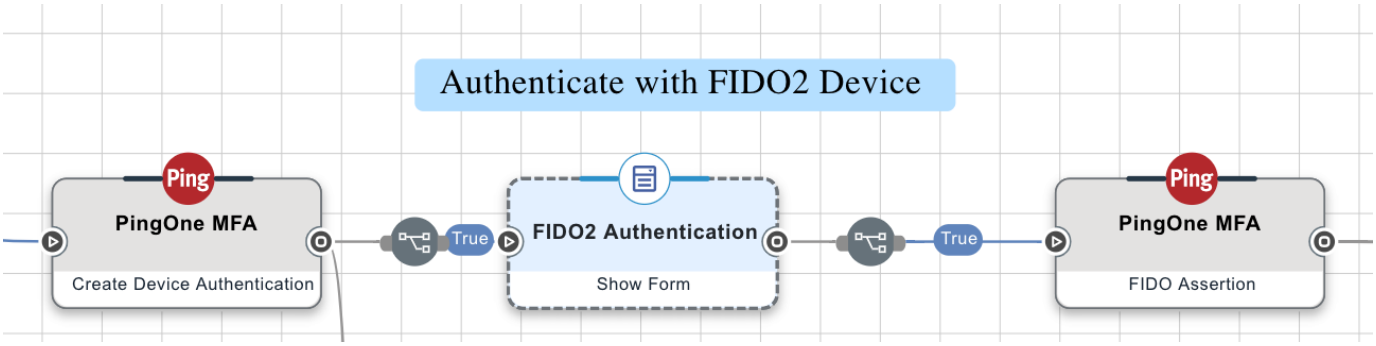
Creating an MFA form with FIDO2 authentication

To configure FIDO2 in PingOne Forms for authentication:

Steps

1. Create a FIDO2 form:
    1. In the PingOne admin console, go to **User Experience** > **Forms**.
    2. Click the **+** icon and select the **FIDO2 - Authentcation** template.
2. (Optional) Customize the templated form in the form builder.
3. Click **Save**.
4. Configure the DaVinci flow.

Copyright © 2025 Ping Identity Corporation



1. In your PingOne DaVinci flow, add a PingOne MFA connector and select the **Create Device Authentication** capability.

   > **Important**
   >
   > This connector is necessary for the **Public Key Credential Request** field in the following PingOne Forms connector.

2. In a subsequent node, add a PingOne Forms connector and select the **Show Form** capability, then select the FIDO2 authentication form you created in **User Experience > Forms**.

3. In a subsequent node, add another PingOne MFA node and select the **FIDO Assertion** capability.

Creating an MFA form with the authenticator app

To create a simple registration or authentication form with an authenticator app prompt:

Steps

1. In the PingOne admin console, go to **User Experience > Forms**.
2. Click the **+** icon and select either the **Authenticator App Prompt - Registration** or **Authenticator App Prompt - Authentication** form.
3. (Optional) Customize the templated form in the form builder.
4. Click **Save**.

Result

You can now use the form in your DaVinci flow with the PingOne Forms connector.

Copyright © 2025 Ping Identity Corporation

Using translatable keys

You can add translatable keys for any user-facing text in your forms, including the input field labels, button labels, and rich text. After adding these keys, the text can be translated based on the user's browser settings for preferred languages.

To add a translatable key:

Steps

1. In the PingOne admin console, go to **User Experience** > **Forms** and select a form.
2. In the **Edit Form** section, click on a section of your form that includes text to localize.

   Result:

   The element's configuration settings pane opens.
3. Click the **Translation** ( ) icon.

   Result:

   The **Select Localized String** modal opens with a list of the available keys and their default translations.
4. Select the appropriate **Key**.

   If you're adding translatable keys for a button, the appropriate **Key** is **Button.text**, where `Submit` is the default translation.
5. (Optional) To define a unique key and default translation, select **Create New Key**.
6. Click **Select**.

   Result:

   A key is added to the field with the **Translation** ( ) icon.
7. (Optional) Click the key and enter a custom default translation in the **Enter Default Translation** field. Click **Save**.

Next steps

Repeat the steps for elements in the form with user-facing text. After you have added translatable keys, you must configure which languages are enabled for translation in **User Experience** > **Languages**. Learn more in Enabling or disabling a language.

Using dynamic text

You can use dynamic text to show a value from your DaVinci flow in the form of read-only text. Dynamic text is useful for personalizing forms. For example, you can:

- Show user-specific information, such as "Welcome, Charlie."

Copyright © 2025 Ping Identity Corporation

- Show flow-specific information, such as "You have 3 attempts remaining."
- Create dynamic URLs, such as "To set your profile picture, edit your profile."

> **Important**
> Currently, this functionality is available only in the **Translatable Rich Text** component and field labels.

To use dynamic text to show user-specific information for a greeting message:

Steps

1. In a **Translatable Rich Text** component or the label property for a field, type **{{}}**.
2. Between the brackets, define the name **{{greetingName}}**.
3. Click **Save**.
4. In your DaVinci flow, add a PingOne Forms connector and select the **Show Form** capability. Select the form you saved.
5. In the **Dynamic Text** section, select a value from your flow that contains the user's first name for the **greetingName** key.
6. Click **Save** and run the flow.

Form properties

You can view and edit form properties on the **Properties** tab.

Property	Description
Form Name	The name of the form. This name is used internally and is not visible to the end user. This property is required.
Form Description	A description of the form. This description is used internally and is not visible to the end user.
Localization Display	PingOne localization support. Valid displays are: ***Display translations*** Displays all translated strings on the form. If custom strings exist, ensure that keys and translations for these strings are included to prevent partially translated forms from displaying. ***Display keys*** Displays the translation keys for all strings on the form. **Note** This option is typically used only for testing purposes. ***Display only the default language*** Displays the default language on the form without localization information.

Copyright © 2025 Ping Identity Corporation

Property	Description
Show "Required" field indicators	When selected, the form indicates the fields that the user must complete.
Show "Optional" field indicators	When selected, the form indicates the fields that are optional for the user. This property is selected by default.
Enable for text fields	When selected, autocomplete tools are enabled for text fields. This feature provides assistive tools to make the form more accessible for users.
Enable for password fields	When selected, autocomplete tools are enabled for password fields. This feature provides assistive tools to make the form more accessible for users.

Form fields

You can add any of the following fields on the **Fields** tab. After adding the fields, you can configure some of the field properties.

You can add additional user information categories by going to **Directory** > **User Attributes** in PingOne. After you add them, these new categories are available as field types.

> **Important**
>
> When a form is modified and saved, it could have an immediate impact on a production flow depending on how it's used in DaVinci. If you add new fields, you must go into the DaVinci flow and modify the mappings with new or updated fields.

Custom Fields

Field	Description
Checkbox List	A section with a list from which a user can select one or more options.
Combobox	A drop-down element for selecting from multiple possible values.
Dropdown	A drop-down element.
Password	A field for a user's password.
Phone Number Input	A field for a user's country code and phone number for validation.
Radio Button List	A section of options where a user can only select one.
Text Input	A field for a user's text input.

Copyright © 2025 Ping Identity Corporation

PingOne Attribute Fields

User Account

Field	Description
Username	The account username.
Password	A field that allows the user to enter their current PingOne password or set a new one. Enable **Verify Password** to require the user to confirm the new password. Enable **Show Password Requirements** to show requirements set by the environment's default password policy.
Current Password	A field that prompts the user to enter their current PingOne password for authentication.
New Password	A field that allows the user to set a new PingOne password. Enable **Verify Password** to require the user to confirm the new password. Enable **Show Password Requirements** to show requirements set by the environment's default password policy.
Recovery Code	The recovery code for the user's account. This field can be used with the **New Password** field for password recovery.
Type	The type of user. Must be `PING_ONE` or `EXTERNAL`. Use this field for forms that allow administrators to create users

Contact

Field	Description
Email Address	The user's email address.
Primary Phone	The user's primary phone number.
Mobile Phone	The user's mobile phone number.

Name

Field	Description
Formatted	The form of the user's name.
Given Name	The user's given name.
Middle Name	The user's middle name.
Family Name	The user's family name.
Nickname	The user's nickname.

Copyright © 2025 Ping Identity Corporation

Field	Description
Title	The user's title.
Honorific Prefix	The honorific prefix for the user's name.
Honorific Suffix	The honorific suffix for the user's name.

Language

Field	Description
Locale	The user's locale.
Preferred Language	The user's preferred language.

Address

Field	Description
Street Address	The street address.
City / Locality	The town or locale.
Region	The state or region.
Postal Code	The zip code or postal code.
Country Code	The three-digit country code.
Timezone	The user's time zone.

Photo

Field	Description
Photos Link	The URL for the user's photo.

Field properties

Clicking on a field already in your form displays the field properties in the sidebar.

Property	Description
Field Type	The type of field, such as **Text Input** or **Password**.

Copyright © 2025 Ping Identity Corporation

Property	Description
Key	The key value for the provided data. **Note** This property can only be edited for custom fields.
Label	The field label that's displayed for the end user.
Label Position	Configures whether the label displays inside the field or above the field. Valid positions are: • **Inside** • **Above**
Input Type	The type of input provided by the user. Valid types are: ***Text*** A text field with option validation. ***Password*** A password-specific field with optional confirmation. ***Dropdown*** A drop-down list with one or more options you can configure under **Options**. ***ComboBox*** A drop-down menu with one or more options you can configure under **Options**. ***Radio*** A set of radio buttons. ***Single Checkbox*** A single checkbox that can be configured to display as a checkbox or toggle. ***Checkbox*** A set of checkboxes with one or more options. ***Phone Number*** Turns field into a phone number input component.
Width	The width of the field. Valid values are: • **Flex** (fills the available space) • **25%** • **50%** • **75%**
Validation Type	If you selected **Text** as the input type, this option lets you validate the text. Valid values are: • **None** • **Custom** If you select **Custom**, the **Regex** and **Error Message** fields show. The **Regex** value is used to validate the text, and the **Error Message** value appears if the text is invalid.

Copyright © 2025 Ping Identity Corporation

Property	Description
Verify Password	If you selected **Password** as the input type, this checkbox adds a field to verify the provided password.
Field Required	This checkbox indicates that the field is required. The form properties determine whether optional or required fields are indicated.

Form toolbox

You can add any of the following components on the **Toolbox** tab to customize the layout and appearance of the form.

Tool	Description
Agreement	Select an agreement configured in **User Experience** > **Agreements** to present to a user.
Divider	A horizontal divider. Add optional text to your divider in the **Label** field and align the text with **Label Alignment**.
Empty Block	An empty space that can be moved and resized.
Error Display	A space that shows any form or flow-level errors.
Flow Button	A customizable button to include in a form.
Flow Link	A custom link to include in a form. For example, you can add a **Forgot Password** link for password reset.
Google reCAPTCHA v2	A Google reCAPTCHA tool can distinguish between human and automated accesses. You can customize the alignment, size, and theme of the reCAPTCHA tool. **Note** You must supply your environment with the **Site Key** and **Secret Key** from your Google account to enable this tool. Click **Global Google reCAPTCHA Settings** to view or update this information. This element can be included only on forms designed for use in flows.
Polling	An activity indicator. This component also enables polling functionality and configuration in the PingOne Forms connector.
QR Code	A scannable QR code. This component is useful for a variety of use cases, including prompting an end user to: • Open a website or app installer on their mobile device • Start an identity verification process on their mobile device • Pair a mobile app or authenticator for MFA

Copyright © 2025 Ping Identity Corporation

Tool	Description
Rich Text	A block of custom text. **Note** This legacy component will be deprecated in 2025. Use **Translatable Rich Text** instead.
Social Login	A social login button.
Translatable Rich Text	A block of custom text that can be translated. **Note** This field is preferred because it can be localized for end users. This field also supports an optional icon to the left of the text.
Submit Button	A submit button. The button is removable. Forms configured with MFA components don't require an additional submit button.
Show Hidden	When selected, displays any hidden elements.

MFA components

You can use MFA components to create MFA forms for device authentication, device registration, and FIDO2 registration or authentication in your PingOne DaVinci flow.

Tool	Description
MFA - Device Selection Authentication	Provides multiple authentication methods defined by the MFA policy or device list configured in your PingOne Forms connector.
MFA - Device Selection Registration	Provides multiple registration methods defined by the MFA policy or device list configured in your PingOne Forms connector.
FIDO2	A submit button for FIDO2 registration or authentication forms.

Copyright © 2025 Ping Identity Corporation

Settings

The **Settings** section contains information specific to an environment, including properties, administrator security, certificates and key pairs, custom domains, and SMTP servers.

Choose from one of the following topics:

- Environment properties
- Administrator security
- Certificates and key pairs
- Domains
- Sender

Environment properties

Use the **Environment Properties** page to view details about your environment, such as the assigned license, organization and environment IDs, and the URLs for the associated admin console and self-service and application portals.

Learn more about PingOne environment contents and uses in Environments.

In the PingOne admin console, go to **Settings** > **Environment Properties**. The following information is displayed:

General settings

Field	Description
Organization Name	The name of the organization.
Name	The name of the environment.
Description	A brief description of the environment.
License	The environment license details.
Environment ID	The environment ID.
Organization ID	The organization ID.
Type	The type of environment (**Sandbox** or **Production**).
Region	The geographical region to which the environment belongs.
Created	The date and time the environment was created.

Copyright © 2025 Ping Identity Corporation

URLs

Field	Description
Console Login URL	The URL used to sign on to the admin console for this environment.
Self-Service URL	The URL for end user access to the self-service portal for this environment.
Application Portal URL	The URL for end user access to the application portal.

Getting Started Guides

Administrators environment only. Display or hide the Administrators getting started guide on the **Environments** page.

Early Access Participation

View the early access features enabled in the environment. Learn more in Managing opt-ins for early access features in PingOne.

Viewing and switching environments

Use the **Environments** list to view the currently configured environments in your organization.

Steps

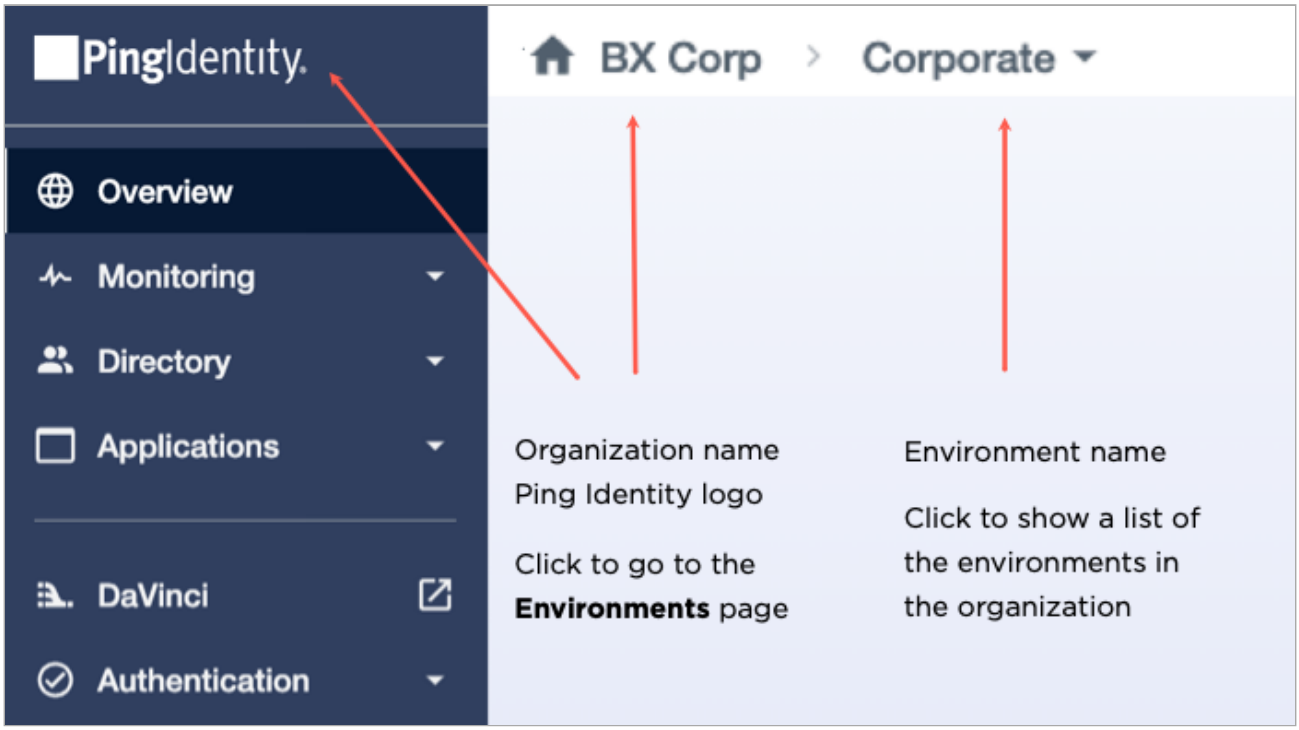
- To view your environments, do one of the following:

  Choose from:

  - On the top of the page, click the name of the current environment name to see the full list of environments in the organization.
  - Click the Ping Identity icon or the organization name to go to the **Environments** page.

> **Note**
>
> To search for an environment, enter the environment name in the **Search** field. You can also sort the environments alphabetically or by date created.

Copyright © 2025 Ping Identity Corporation



- To switch environments, select a different environment from the list.

Adding an environment

Add an environment to your organization from the **Environments** page using the setup assistant to guide you through the process.

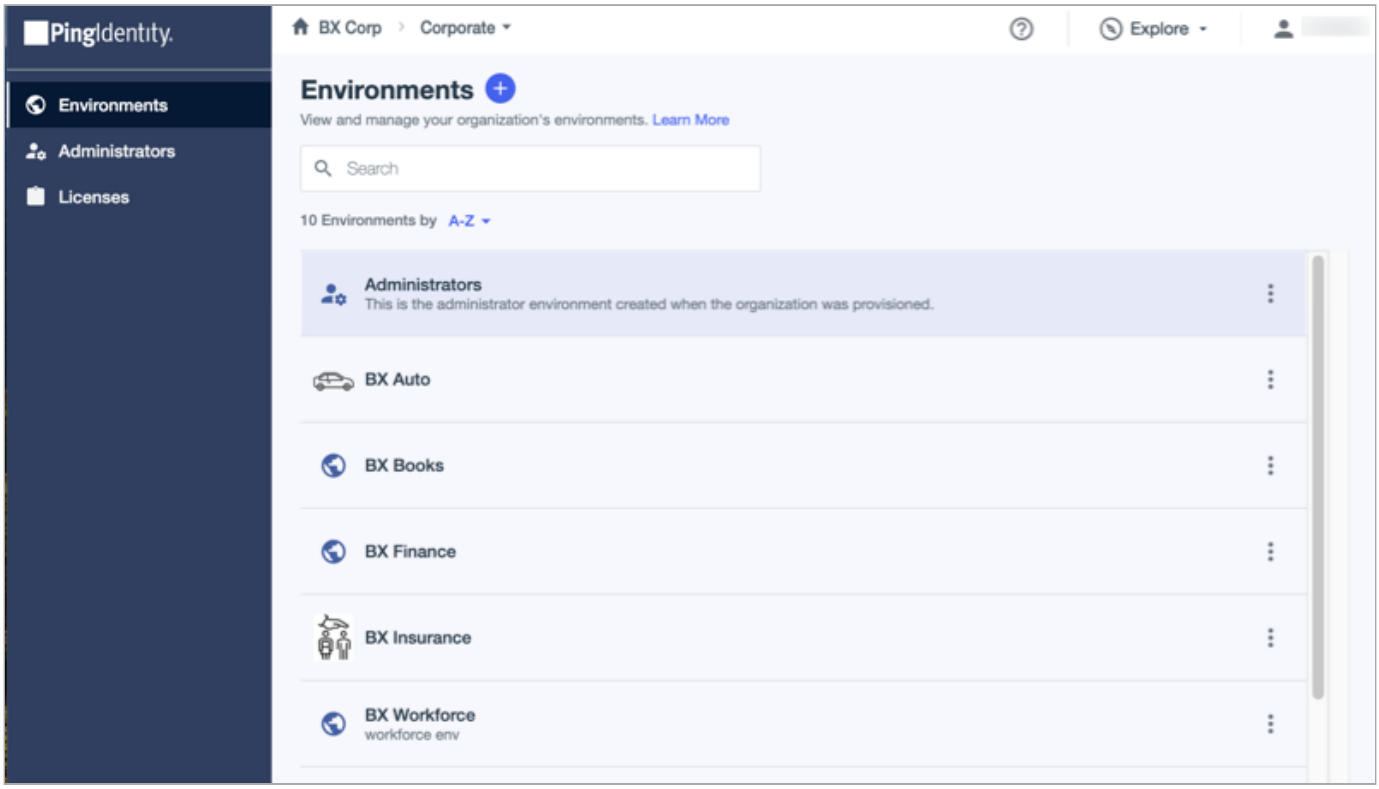
About this task

> **Note**
> You must have the Organization Admin role or a custom role with equivalent permissions to create an environment.

Steps

1. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page.
2. Click the **+** icon.

Copyright © 2025 Ping Identity Corporation

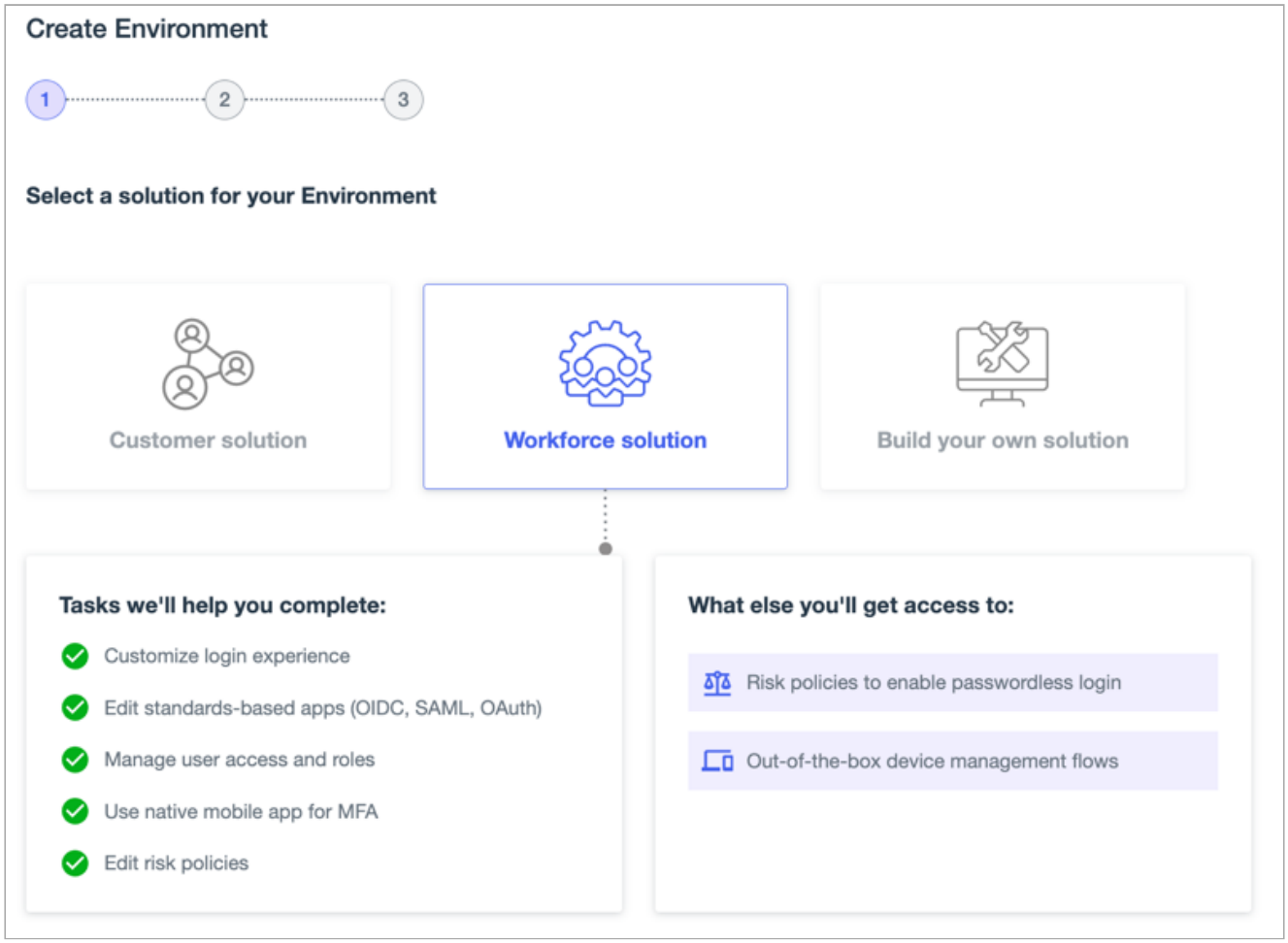


Result:

The **Create Environment** setup assistant starts.

3. Select the type of solution that you want to support in this environment.

Copyright © 2025 Ping Identity Corporation



Option	Description
Customer solution	Select to design registration and subsequent sign-on experiences for your customers and test them in a sample application tailored to your industry.
Workforce solution	Select to design single sign-on experiences for your employees, partners, and vendors.
Build your own solution	Select to choose from all of our services and products to build a hybrid solution that fits your unique use case.

4. Click **Next**.

   The services that will be deployed to your new environment are listed.

5. Click **Next**.

6. Define your environment by entering the following:

Copyright © 2025 Ping Identity Corporation

Field	Description
Environment Name	A unique identifier for the environment.
Description (optional)	A brief description of the environment.
Environment Type	Select **Sandbox** or **Production**. Sandbox environments are typically used for configuration and testing before deployment. Production environments are typically used for live configurations that are deployed for real-world use. Learn more about environment types in Sandbox and Production environments.
Generate sample populations and users in this environment	Select this checkbox to generate two populations and 40 sample users in the new environment.
Region	The appropriate geographical region for the environment. The list shows only regions that are included with your license. **Important** You can't change the region after the environment has been created.
License	Select the license to use for this environment. The available licenses for your organization are shown in the **License** list. For more information, see Licenses and Platform Limits.
Include a solution designer to easily design and test experiences (optional)	Customer and Workforce solutions only. If selected, after you create your environment, a solution designer opens and walks you through the process of designing your experiences.
Choose Your Industry (optional)	Customer solutions only. If you make a selection, PingOne creates a sample app tailored to the industry selected.

7. Click **Finish**.

Result

The new environment is created in your PingOne organization.

If you chose to build a customer or workforce solution, and selected the solution designer option, the solution designer opens and guides you through the process of designing and testing registration and sign-on experiences in less than 5 minutes.

If you did not select the solution designer option, or if you built your own solution, the **Environments** page opens. Locate your new environment by sorting the list alphabetically or by date created, or enter the environment name in the search box.

Editing an environment

Use the **Environment Properties** page to edit an existing environment and to view details about the current environment.

Before you begin

Copyright © 2025 Ping Identity Corporation

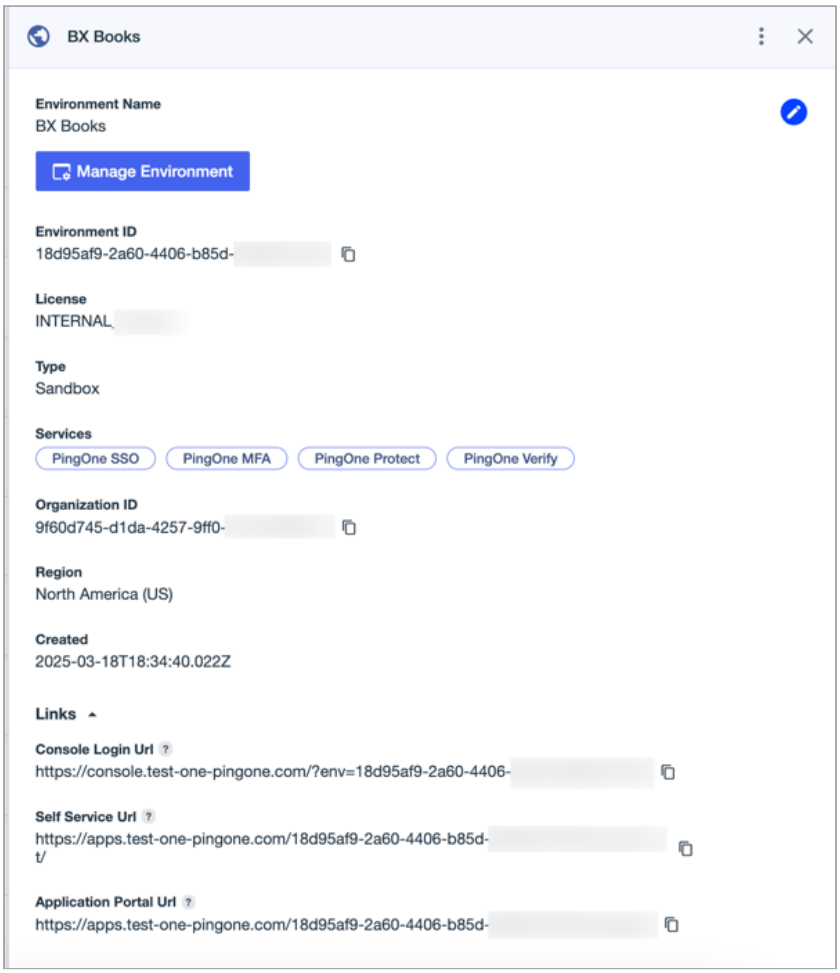
To edit an environment, you must have the Environment Admin role or a custom role with equivalent permissions.

Steps

1. Access the environment details page for the environment you want to edit by doing one of the following.

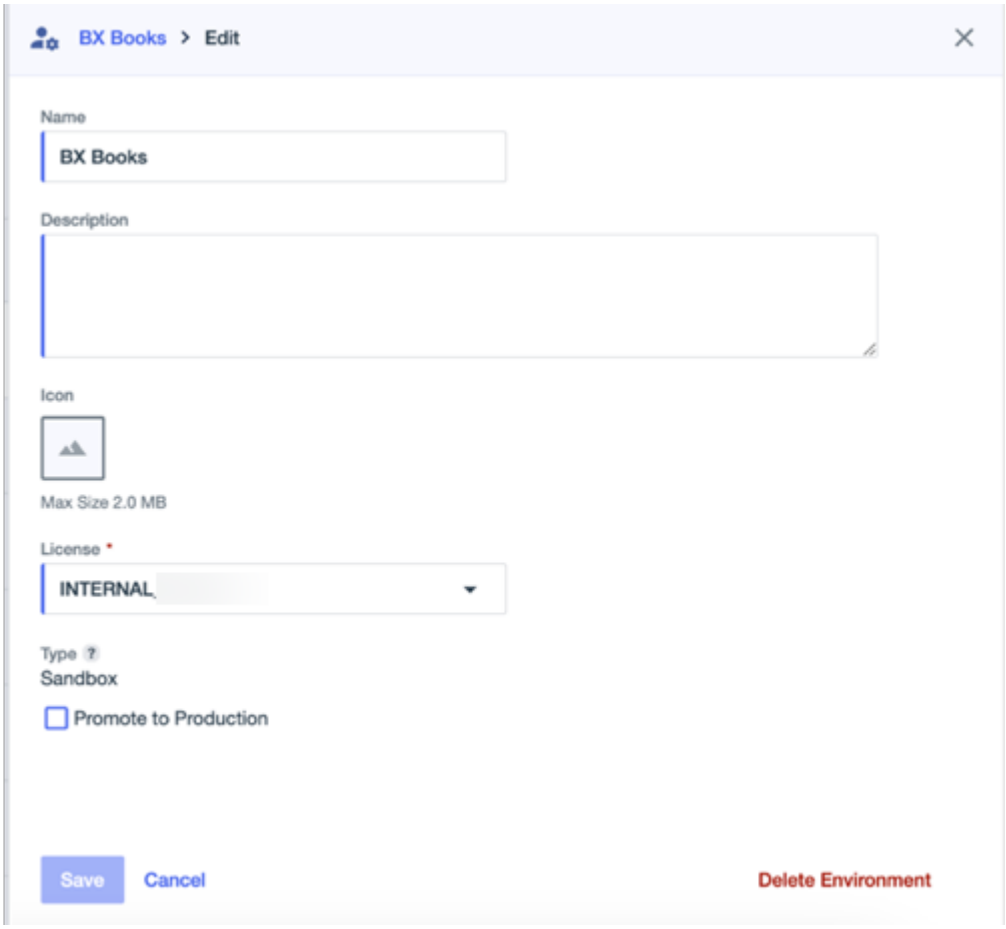
   Choose from:

   - If you're in the console for the environment that you want to edit, go to **Settings > Environment Properties**.
   - If you're not in the console for the environment that you want to edit, click the Ping Identity logo in the sidebar to open the **Environments** page and click the environment that you want to edit.



2. Click the **Pencil** icon to open the editing view.

Copyright © 2025 Ping Identity Corporation



3. Edit the following:

Field	Description
Environment Name	Change the unique identifier for the environment.
Description (optional)	Change the brief description of the environment.
Icon (optional)	To add or change the icon that displays in the **Environments** list, click in the **Icon** box and upload an image. Icons must be no larger than 2 MB.

Copyright © 2025 Ping Identity Corporation

Field	Description
License	Select a different license to use for this environment. The available licenses for your organization are shown in the **License** list. Learn more in Licenses and Platform Limits. **Note** Changing the license from one type to another can cause: ◦ Feature configurations to change or disappear altogether. This includes early access features that are available for opt-in or enabled in the environment. ◦ The need to manually reconfigure settings such as those for sign-on policies and schema attributes. Perform a hard refresh on the environment to see what features are available after changing the license assignment.
Type	If you have the Environment Admin role or a role with equivalent permissions, you can promote a Sandbox environment to Production by selecting the **Promote to Production** checkbox. **Note** If the **Type** is **Production**, you can't change it. Learn more about environment types in Sandbox and Production environments.

4. Click **Save**.

Managing opt-ins for early access features in PingOne

Some PingOne features are available early so that you can try them in your own environments and provide feedback before general availability. Opting in to a feature early lets you use the capability in real-world scenarios and test how it works with your specific environment configuration. You have full control over the features you enable and the environments in which you enable them, and you can remove features you opt in to from the environment at any time during the early access period.

> **Note**
> Not all features are enabled for early access. Additionally, early access features can be enabled only at the environment level. You can't enable an early access feature for the entire organization.
> Early access features related to services that aren't in the environment or that aren't allowable by the license assigned to the environment aren't available for opt-in. If you change the environment type or the license assigned to the environment, some early access features might be removed from the environment, and others might be available. You must perform a hard refresh in the browser to see the list of early access features available after making these changes.

Copyright © 2025 Ping Identity Corporation

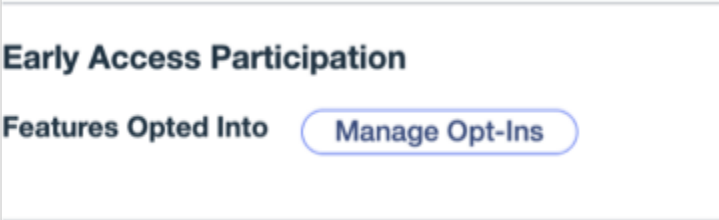
Before you begin

You must have one of the following administrator roles to manage early access features for an environment:

- Organization Admin
- Environment Admin
- A custom administrator role with equivalent permissions

Steps

1. In the PingOne admin console, go to **Settings** > **Environment Properties**.
2. Scroll to the **Early Access Participation** section and click **Manage Opt-Ins**.

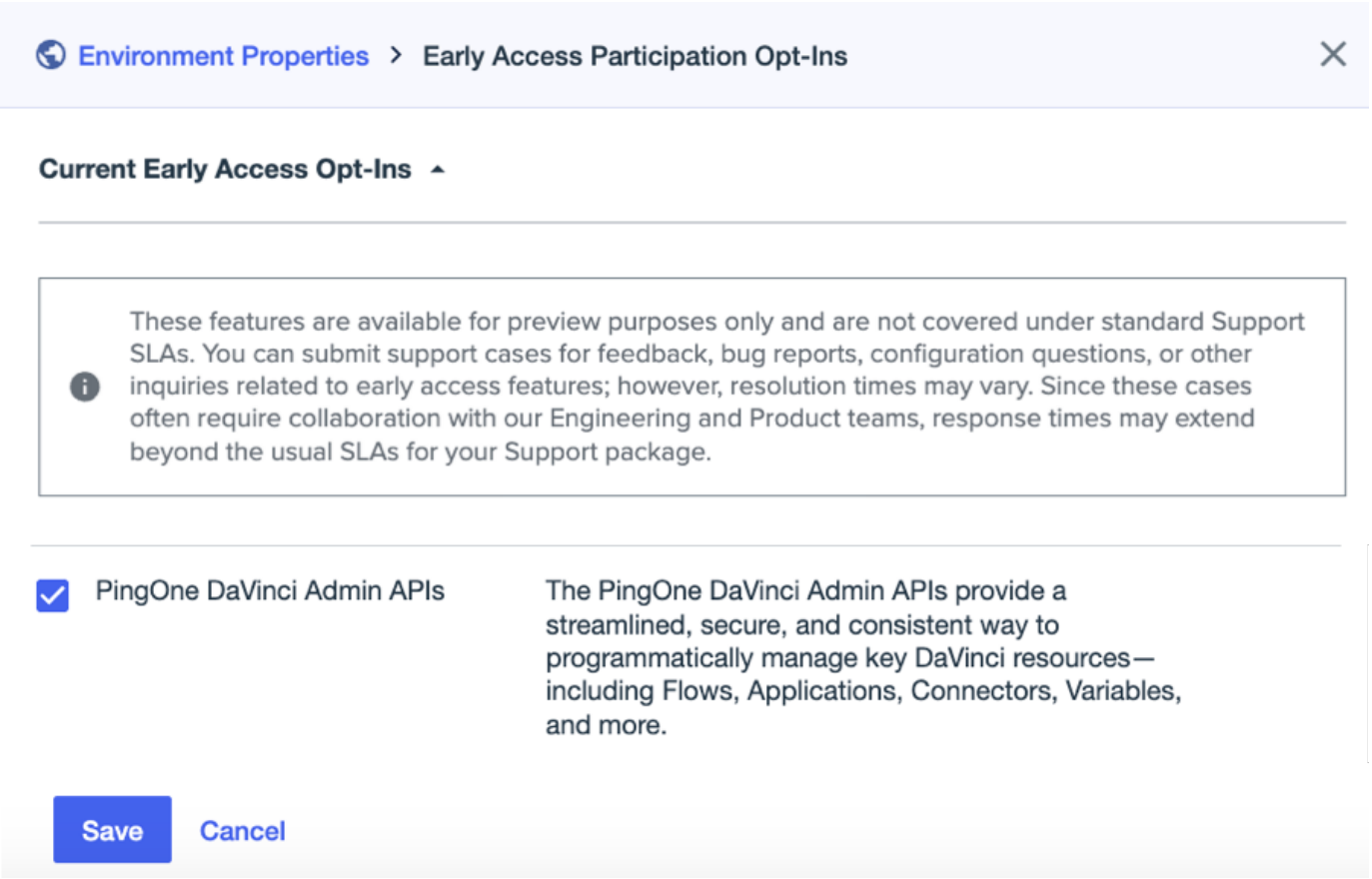


   Result

   A list of early access features that are available for the environment opens.

3. Select the checkboxes for features you want to enable, or clear the checkboxes for features you want to remove.

Copyright © 2025 Ping Identity Corporation



4. Click **Save**, and then click **Refresh** on the **Opt-Ins Updated** modal to see the updates in the admin console.

Result

The early access features you enabled are listed in the **Early Access Participation** section of the **Environment Properties** page and are now ready for use. If you removed a feature, it's no longer displayed in this list.

During the early access period, click **Feedback** to let Ping Identity know if the feature meets your expectations and use case requirements or what changes you might like to see. This early feedback helps Ping understand customer context and consider feature enhancements or new features for future development.

Learn more

Find draft documentation for early access features in the Early Access section of the PingOne documentation.

Adding an icon to an environment

Add an icon to an environment to easily find it on the **Environments** page.

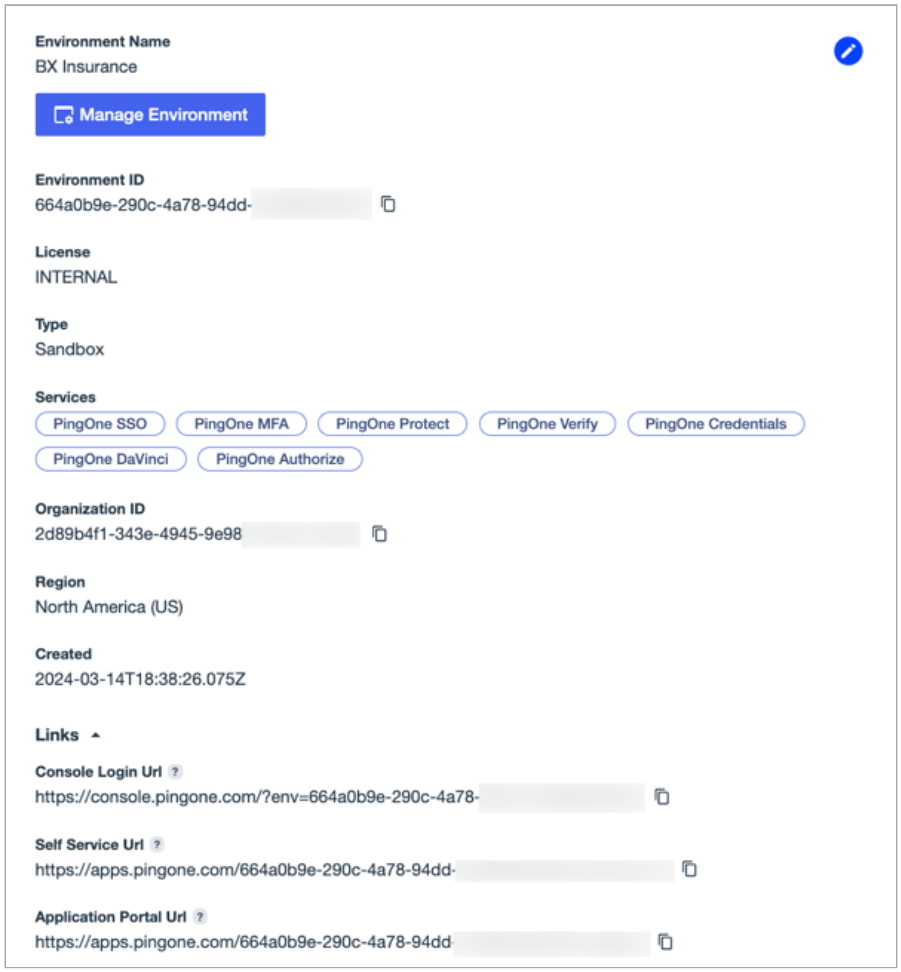
Steps

1. Access the environment details page for the environment to which you want to add an icon by doing one of the following.

Copyright © 2025 Ping Identity Corporation

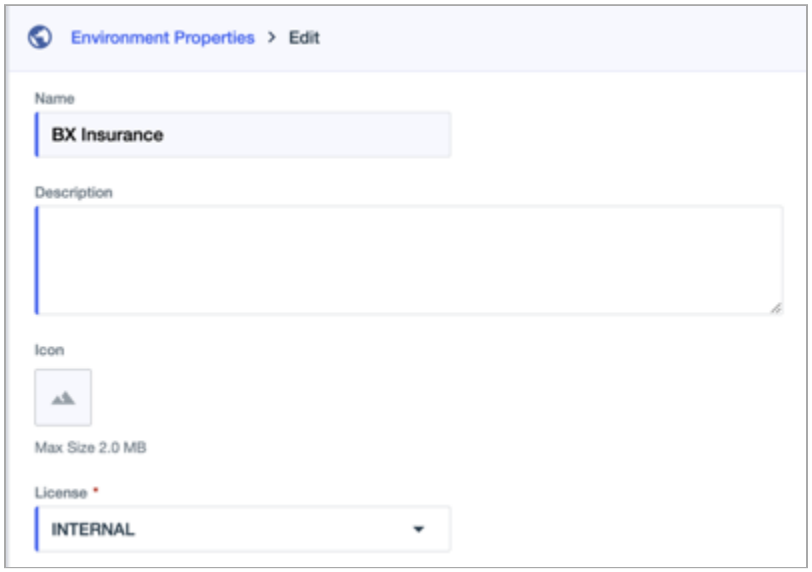
Choose from:

- If you are in the console for the environment that you want to edit, go to **Settings** > **Environment Properties**.
- If you're not in the environment that you want to edit, click the Ping Identity logo in the sidebar to open the **Environments** page and click the environment that you want to edit.



2. Click the **Pencil** icon.
3. Click the **Icon** box.

Copyright © 2025 Ping Identity Corporation



Result:

A file browser opens.

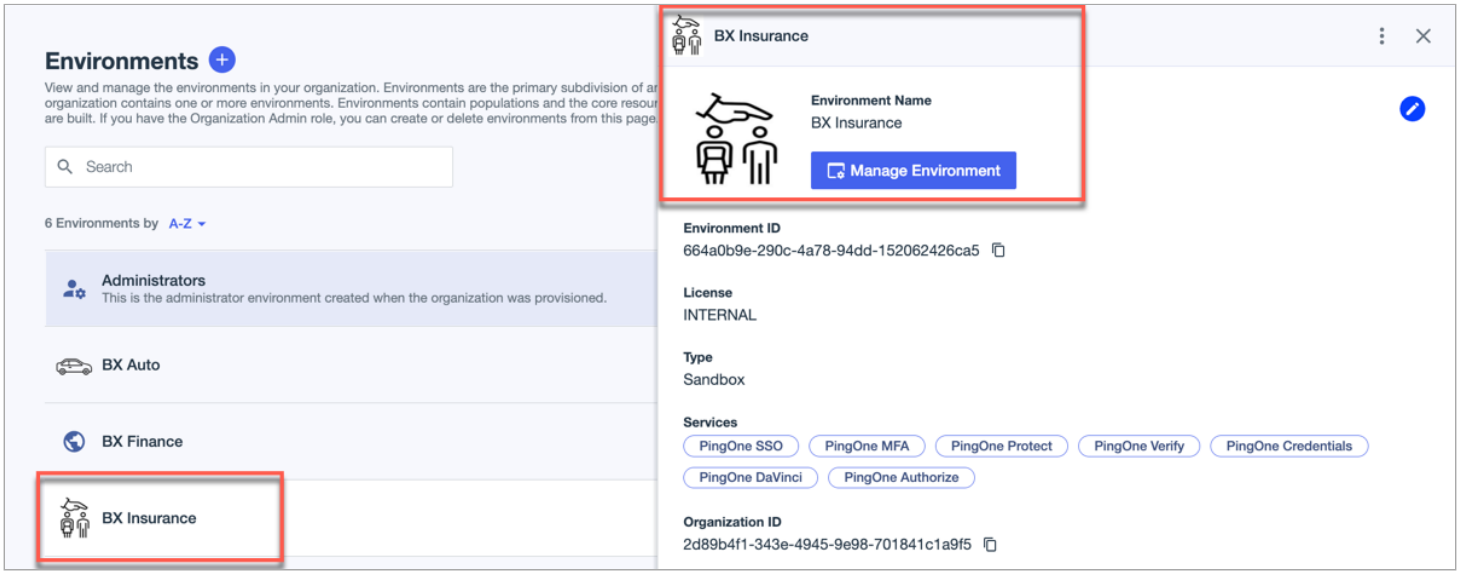
4. Browse for and select the icon you want to use and click **Open**.

> **Note**
>
> The maximum icon size is 2 MB.

5. Click **Save**.

Result

The icon is displayed in the environment details view and on the **Environments** page.



Deleting an environment

Use the **Environments** page to remove an environment that you no longer need.

Copyright © 2025 Ping Identity Corporation

The deletion process and result depends on whether you're deleting a Sandbox environment or a Production environment. Learn more in Sandbox and Production environments.

Deleting a Sandbox environment

To delete an environment, you must have the Organization Admin role or a custom role with equivalent permissions. Additionally, your identity must exist in a different environment than the one you're deleting.

Deleting a Sandbox environment removes all configurations and identity data, but logs and reports are retained for 90 days.

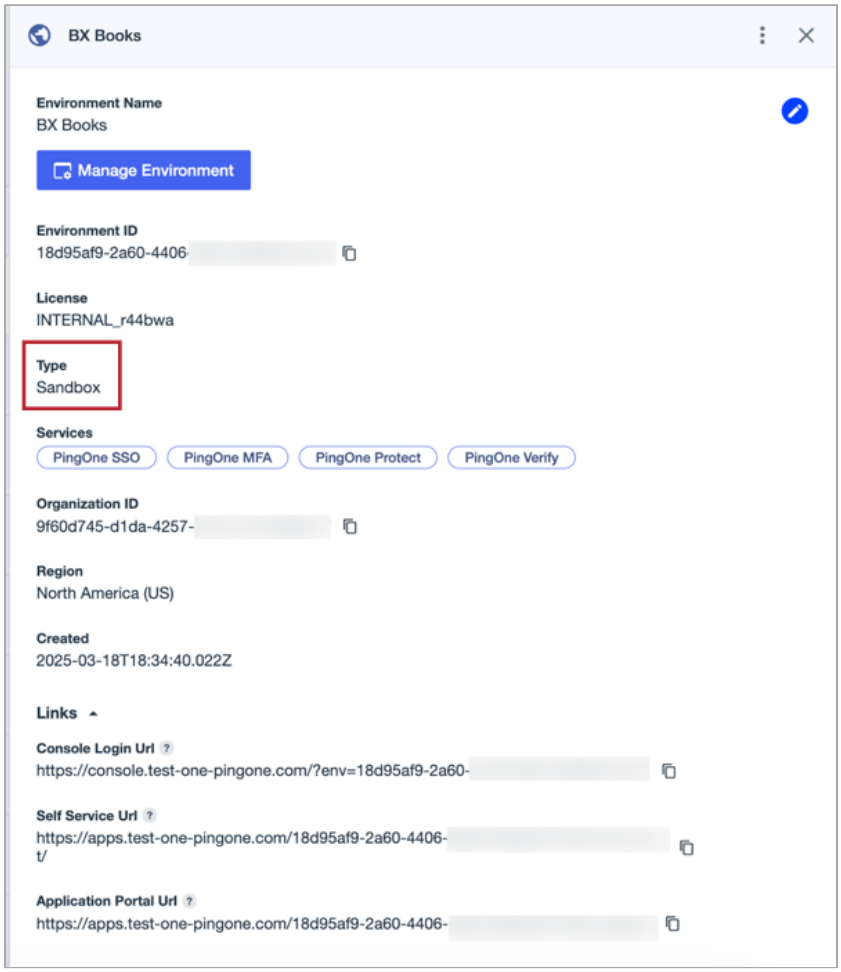
> **Important**
>
> Deleting a Sandbox environment is immediate, and the environment can't be recovered after deletion.

> **Best practice**
>
> If you have Sandbox environments that are used for production purposes, promote the environments to Production so that they can't be deleted immediately. Sandbox environments should only be used for testing. Learn more in Promoting a Sandbox environment to Production.

Steps

1. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page and browse or search for the applicable environment.
2. Click the environment to view the environment properties and verify that the environment is a Sandbox environment.

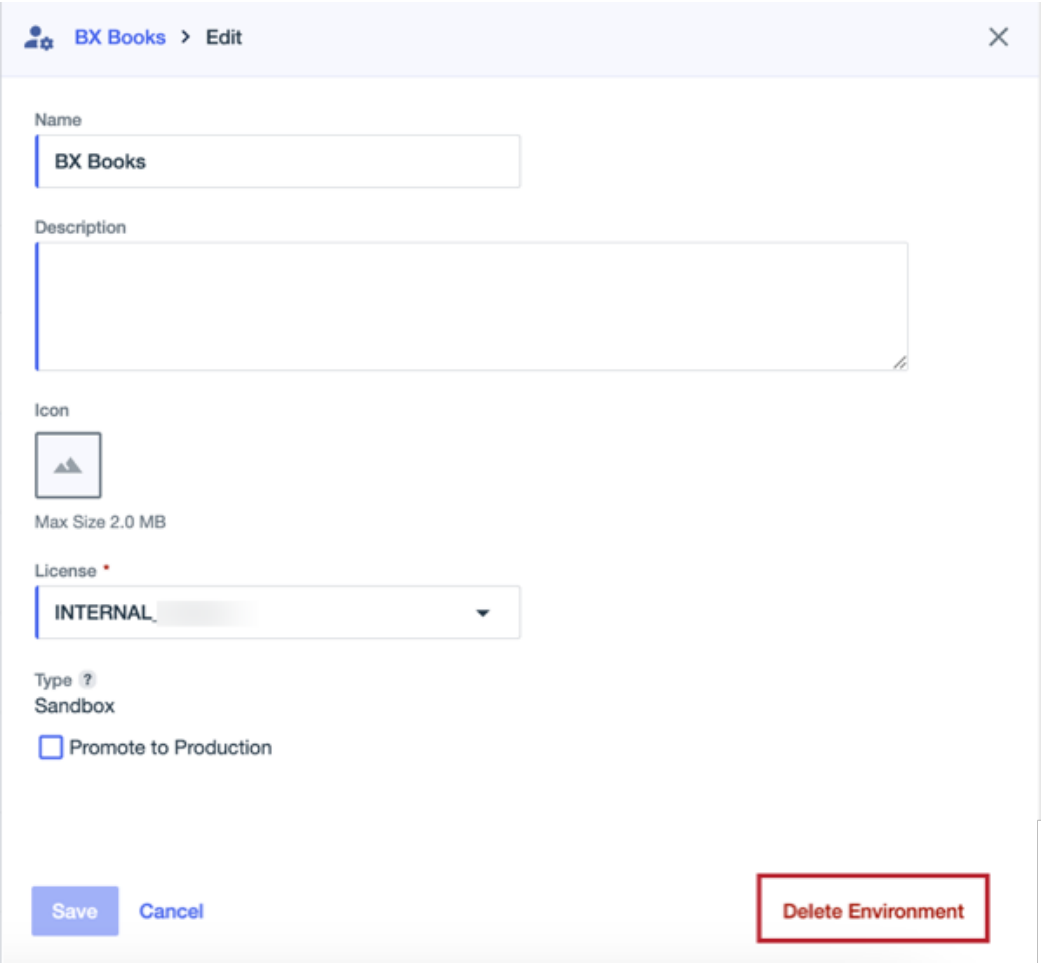
Copyright © 2025 Ping Identity Corporation



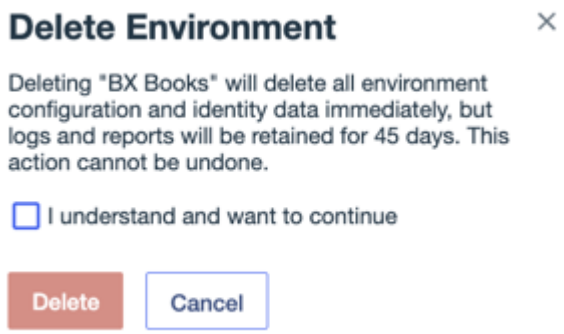
3. Click the **Pencil** icon to open the details panel.

4. Click **Delete Environment**.

Copyright © 2025 Ping Identity Corporation



5. On the **Delete Environment** modal, select **I understand and want to continue** and then click **Delete**.



Result

The environment is deleted immediately and removed from the **Environments** page.

Deleting a Production environment

To delete an environment, you must have the Organization Admin role or a custom role with equivalent permissions. Additionally, your identity must exist in a different environment than the one you're deleting.

When you delete a Production environment, the environment remains in a recoverable state for 30 days.

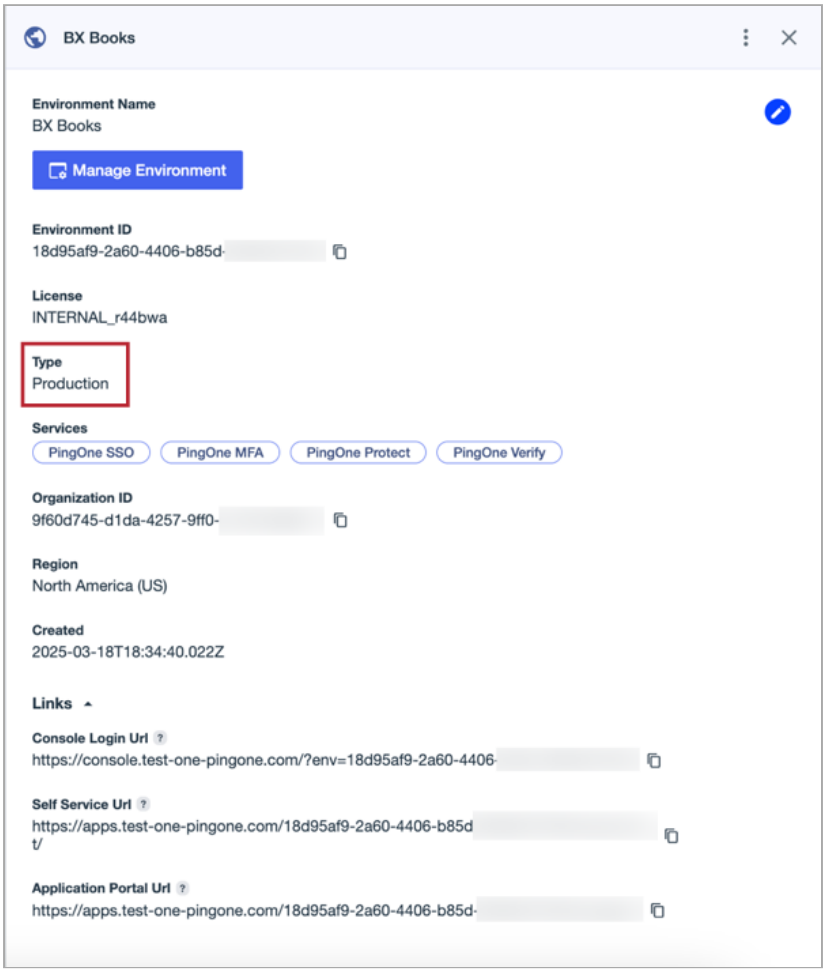
Copyright © 2025 Ping Identity Corporation

> **Important**
>
> At the end of the 30 days, the environment is permanently deleted and cannot be recovered.

When a Production environment is permanently deleted, all configuration and identity data is removed, but logs and reports are retained for 90 days.

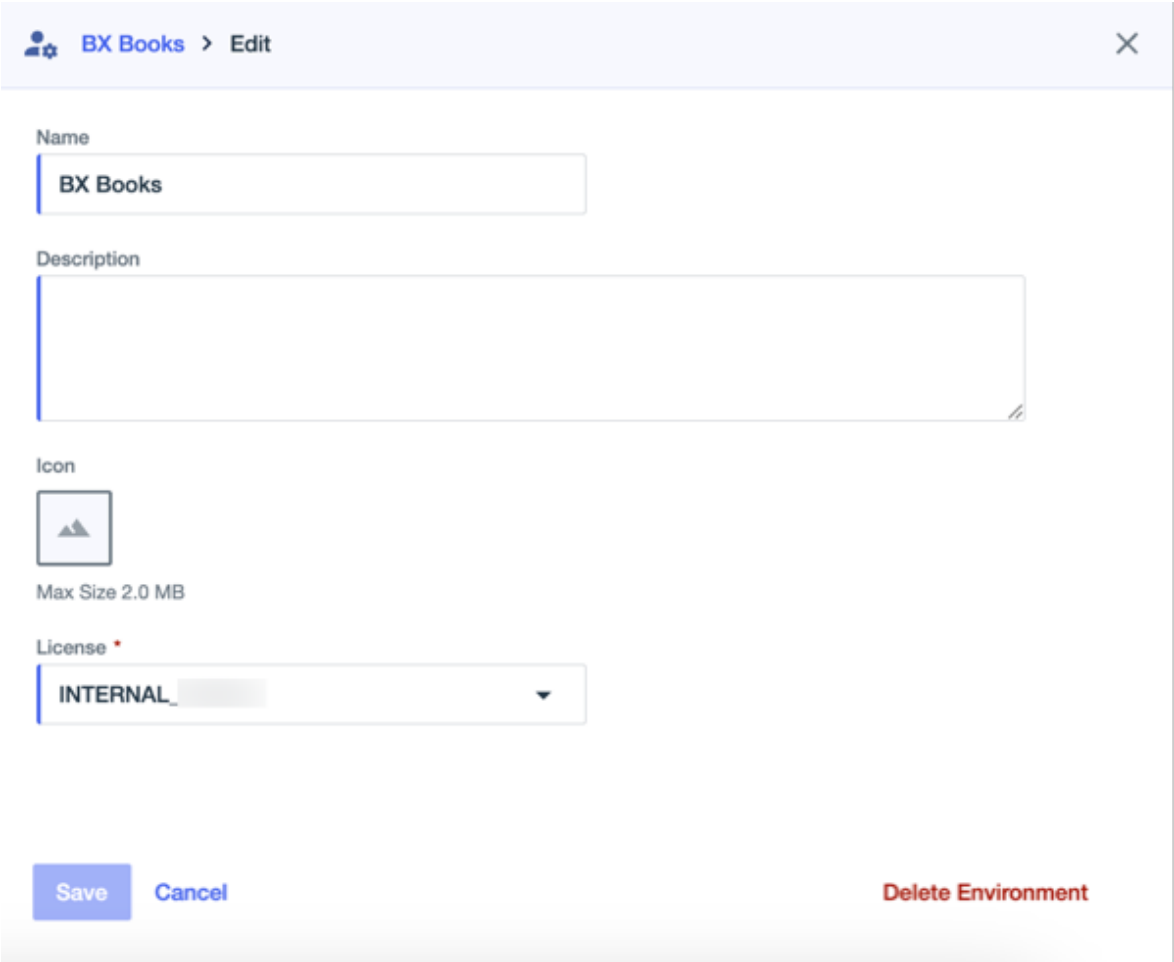
Steps

1. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page and browse or search for the applicable environment.
2. Click the environment to view the environment properties and verify that the environment is a Production environment.



3. Click the **Pencil** icon to open the details panel.
4. Click **Delete Environment**.

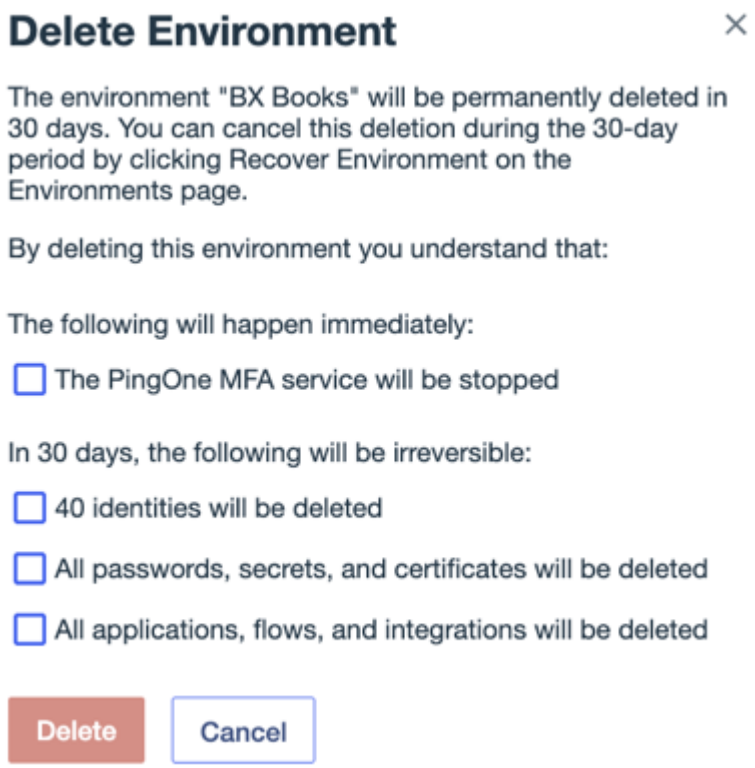
Copyright © 2025 Ping Identity Corporation



> **Note**
>
> Each environment in an organization must have a unique name. While a deleted production environment is in pending deletion status, you can't create an active environment with the same name. If you want to use the name of your deleted environment for a new environment in your organization, you must change the name of the environment before you create the new environment. If you don't change the name, you can't use that name for another environment until the environment with the same name is permanently deleted.

5. On the **Delete Environment** modal, review each disclosure statement and select the checkboxes to confirm that you understand what will be deleted. Then click **Delete**.

Copyright © 2025 Ping Identity Corporation



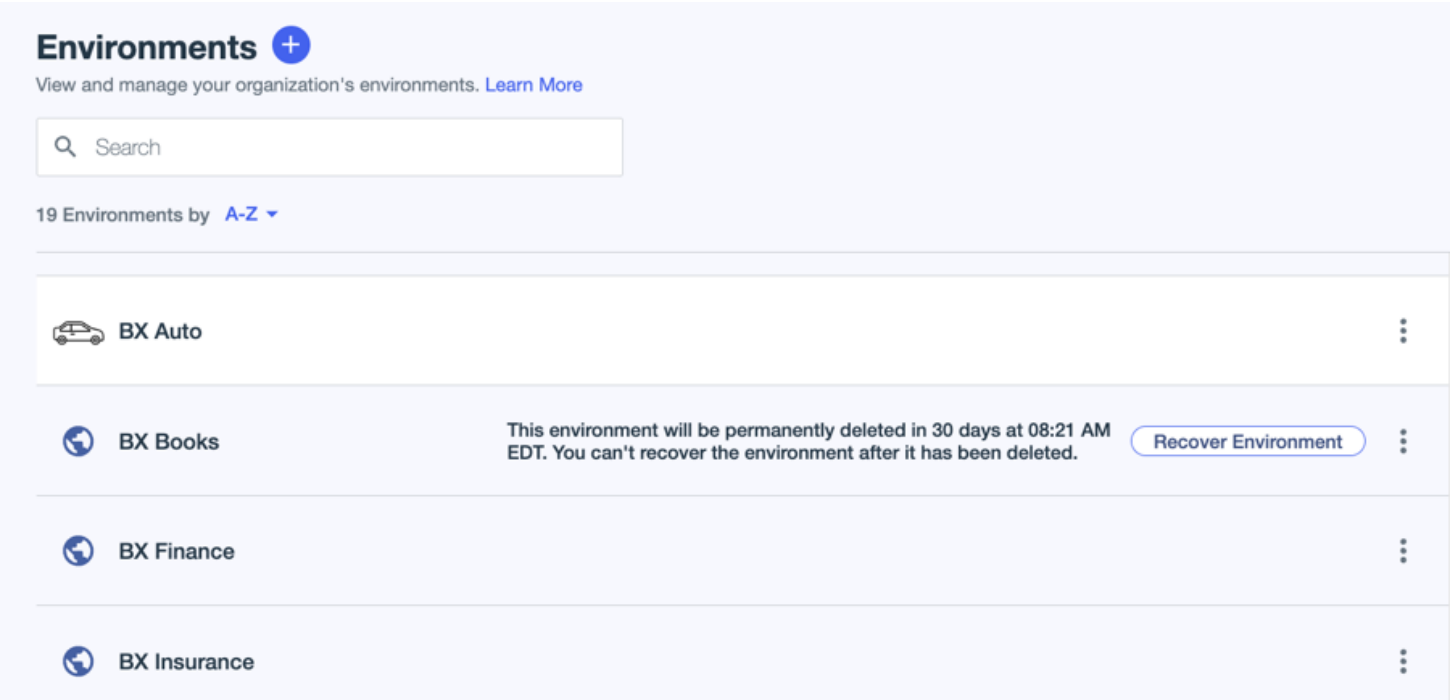
Result

The environment is moved into "Delete Pending" status for 30 days and is unusable during this period. An Environment Updated event is logged for auditing purposes. You can still view the environment details and make some configuration changes, but no other environment activity is logged while in this status.

Deleted Production environments remain on the **Environments** page and are indicated with a message that includes information about when the environment will be permanently deleted. If you access the environment, a banner along the top of the console also provides information about when the environment will be deleted. A message is also displayed in the environment details panel. These messages will count down until the date of permanent deletion.

You can restore the environment at any time during the 30-day period by clicking **Recover Environment**. Learn more in Recovering a deleted Production environment.

Copyright © 2025 Ping Identity Corporation



> **Note**
>
> Deleted Sandbox environments can't be recovered.

Recovering a deleted Production environment

You can recover a deleted Production environment at any time during the 30-day pending deletion period.

To recover an environment, you must have the Organization Admin role or a custom role with equivalent permissions.

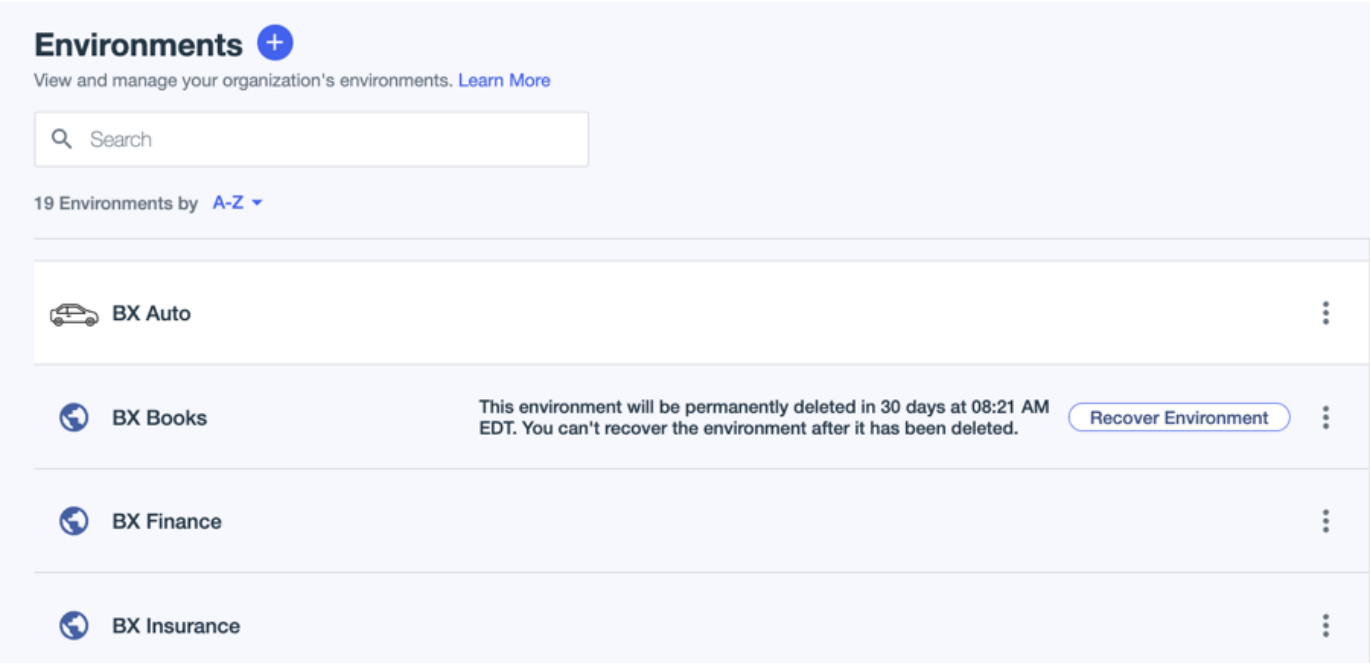
> **Important**
>
> You can't recover deleted Sandbox environments or Production environments that were deleted more than 30 days ago.

Steps

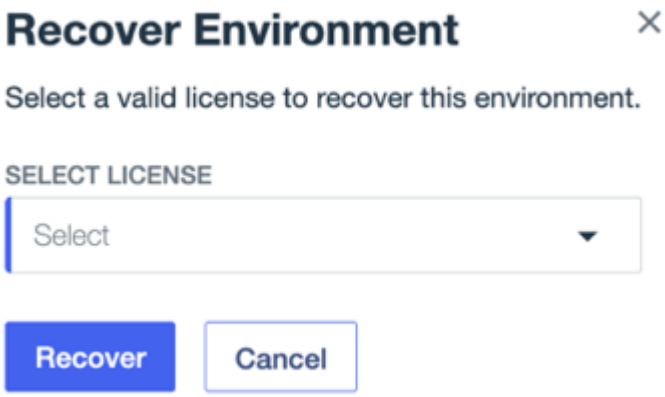
1. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page and browse or search for the applicable environment.

   Environments that have been deleted but are still in the 30-day pending deletion period are indicated with a message that includes information about when the environment will be permanently deleted.

Copyright © 2025 Ping Identity Corporation



2. Click **Recover Environment**.
3. On the **Recover Environment** modal, select a license to assign to the environment.

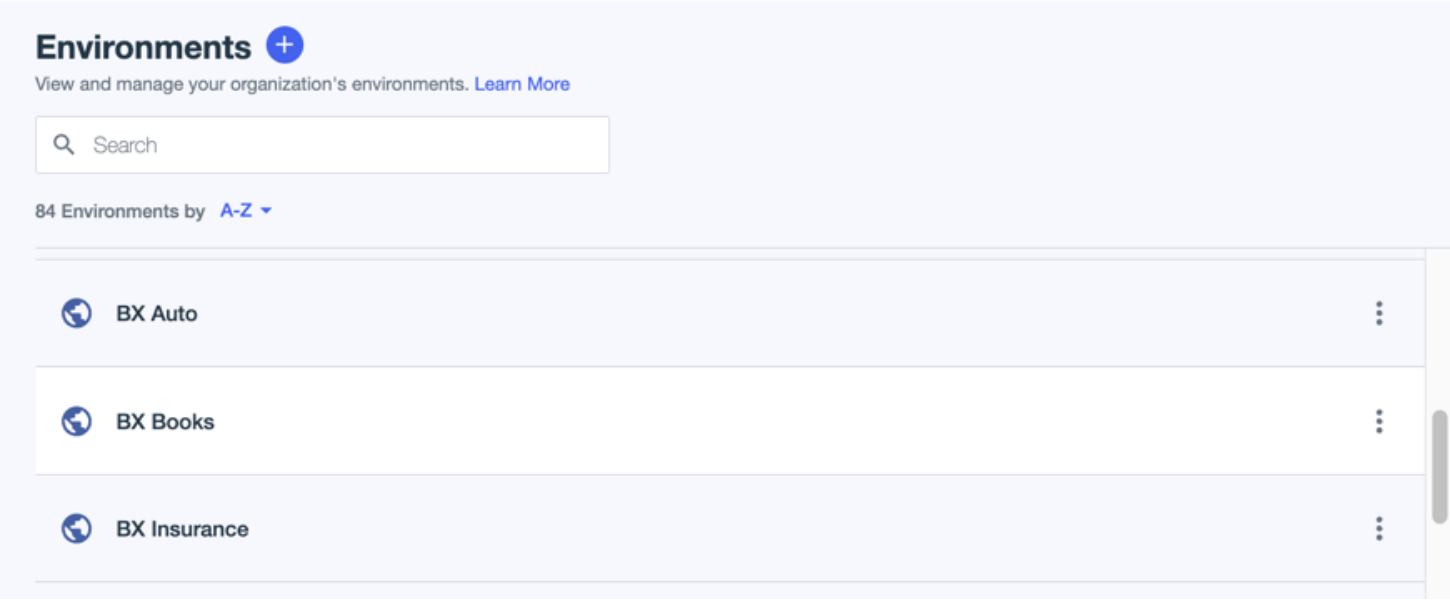


4. Click **Recover**.

Result

The environment is restored to full functionality. On the **Environments** page, the recovery information is removed.

Copyright © 2025 Ping Identity Corporation



Promoting a Sandbox environment to Production

Use the **Environment Properties** page to promote a Sandbox environment to Production.

> **Important**
>
> Promoting a Sandbox environment to Production is a permanent change and can't be reversed. You cannot demote a Production environment to Sandbox.

Before you begin

To promote an environment, you must have the Environment Admin role or a custom role with equivalent permissions.

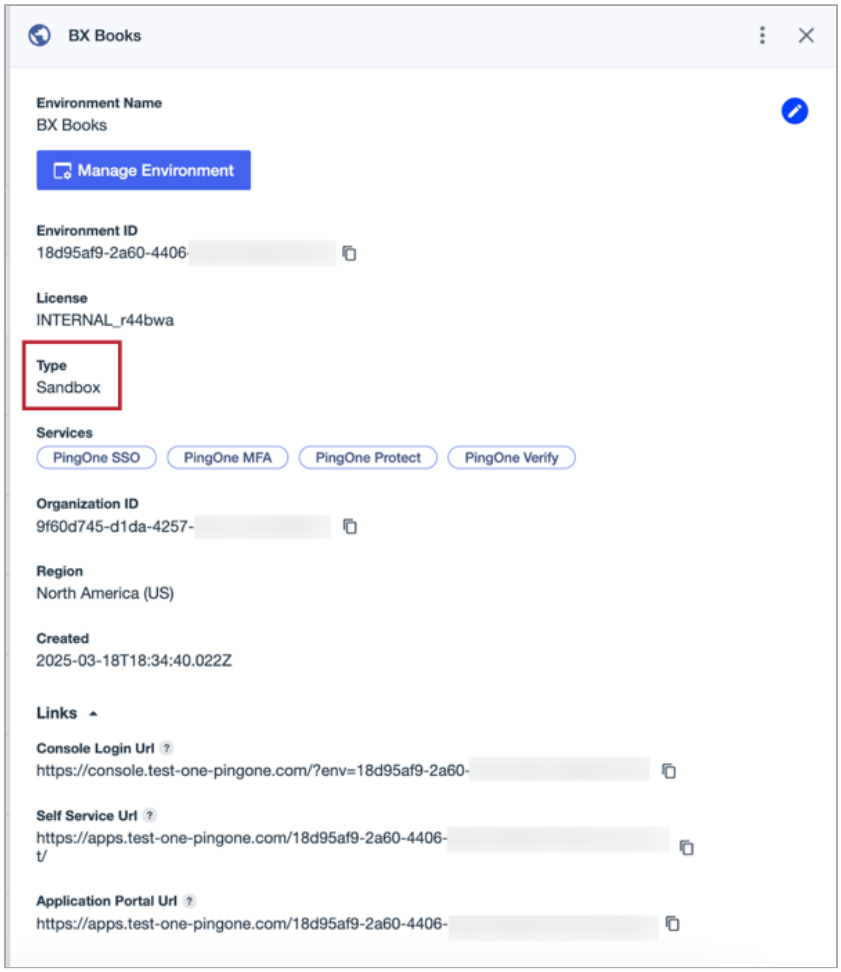
> **Note**
>
> If you have a trial license, you can't promote Sandbox environments to Production.

Learn more about environment types in Sandbox and Production environments.

Steps

1. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page and browse or search for the applicable environment.
2. Click the environment to view the environment properties and verify that the environment is a Sandbox environment.

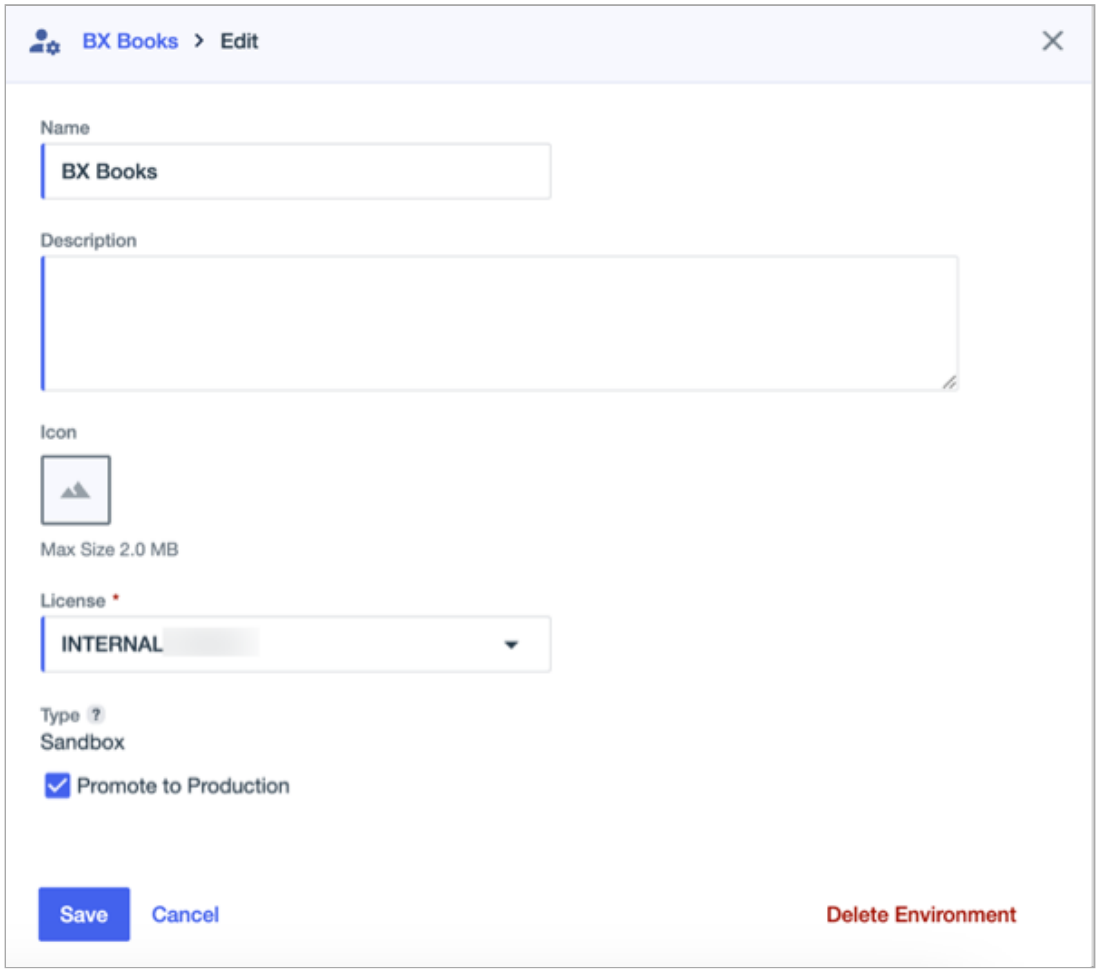
Copyright © 2025 Ping Identity Corporation



3. Click the **Pencil** icon.

4. At the bottom of the page, under **Type**, select the **Promote to Production** checkbox.

Copyright © 2025 Ping Identity Corporation



5. Click **Save**.
6. Click **Promote** on the **Promote to Production** modal to confirm the change.

> **Important**
>
> This action cannot be reversed.

Result

The environment is now a Production environment.

Adding a service to an environment

Use the **Overview** page to add services to an existing environment in your organization.

Steps

1. In the PingOne admin console sidebar, click the Ping Identity logo to open the **Environments** page and browse or search for the applicable environment.
2. On the **Environments** page, click the environment to open the details panel.
3. Click **Manage Environment** to go to the **Overview** page for the environment.

Copyright © 2025 Ping Identity Corporation

4. In the **Services** section, click the **+** icon.
5. Select the service that you want to add.
6. Click **+ Add** next to the service.
7. Follow the instructions in **Add a Service**.
8. Click **Finish**.

Administrator security

Security settings for administrators accessing the PingOne admin console are configured on the **Administrator Security** page.

Ping Identity requires MFA for all PingOne administrators as of June 1, 2025. Learn more in the PingOne administrators MFA requirement - FAQ.

Learn more

- Configuring administrator security
- Configuring administrator security - PingID

Configuring administrator security

Use the **Administrator Security** page to view or change the authentication settings for the PingOne admin console.

You can use PingOne, an external identity provider (IdP), or a combination of an external IdP and PingOne to provide secure access to the admin console.

> **Note**
> This topic only applies to environments that do not include PingID. If your environment includes PingID, go to Configuring administrator security - PingID.

Ping Identity requires multi-factor authentication (MFA) for all PingOne administrators.

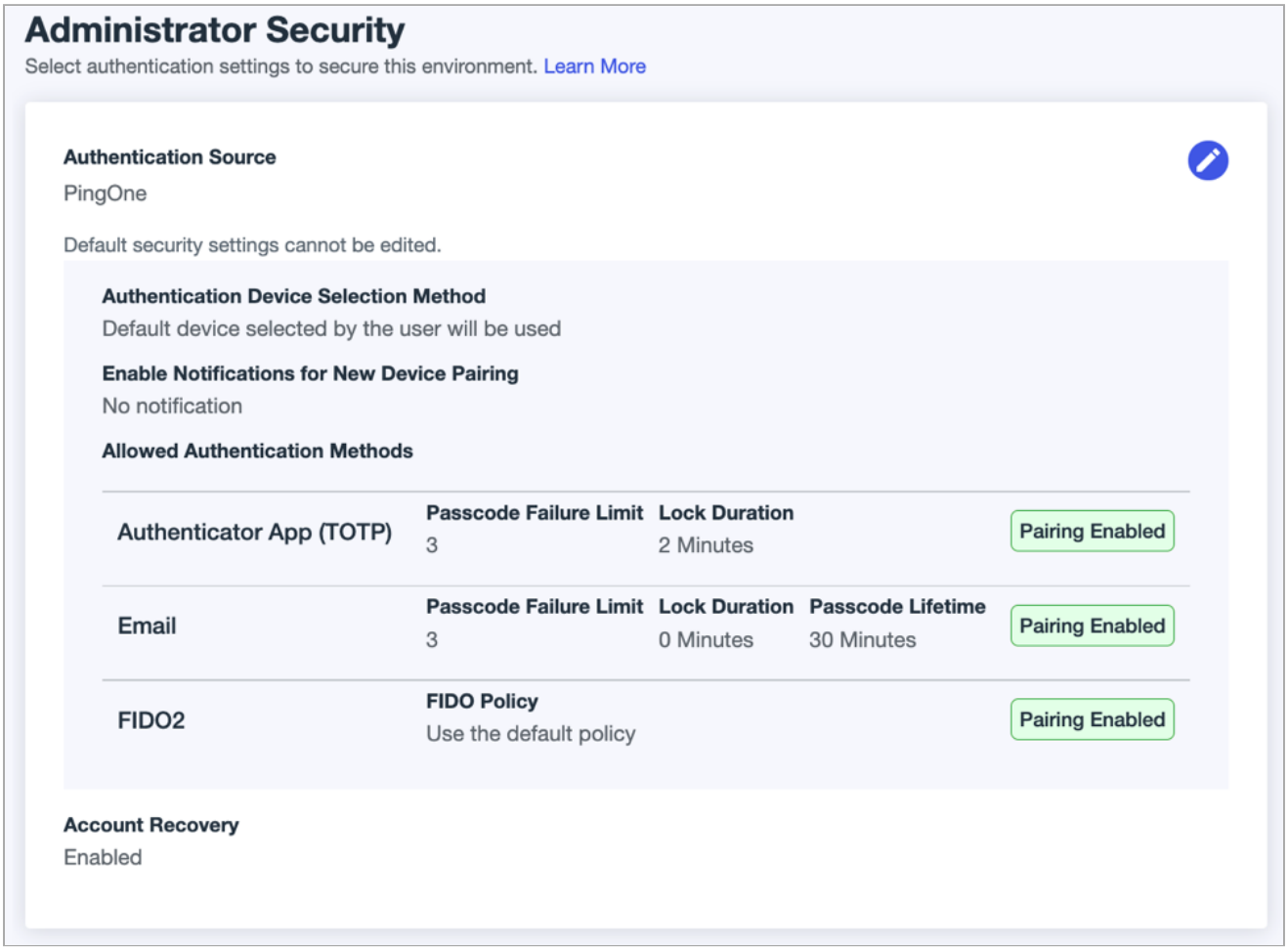
> **Note**
> Administrators must sign on again after 30 minutes of inactivity in the admin console. MFA is required if the last sign-on is older than 12 hours. These settings are not configurable.

You must have the Organization Admin role, Environment Admin role, or a custom role with equivalent permissions to configure **Administrator Security**.

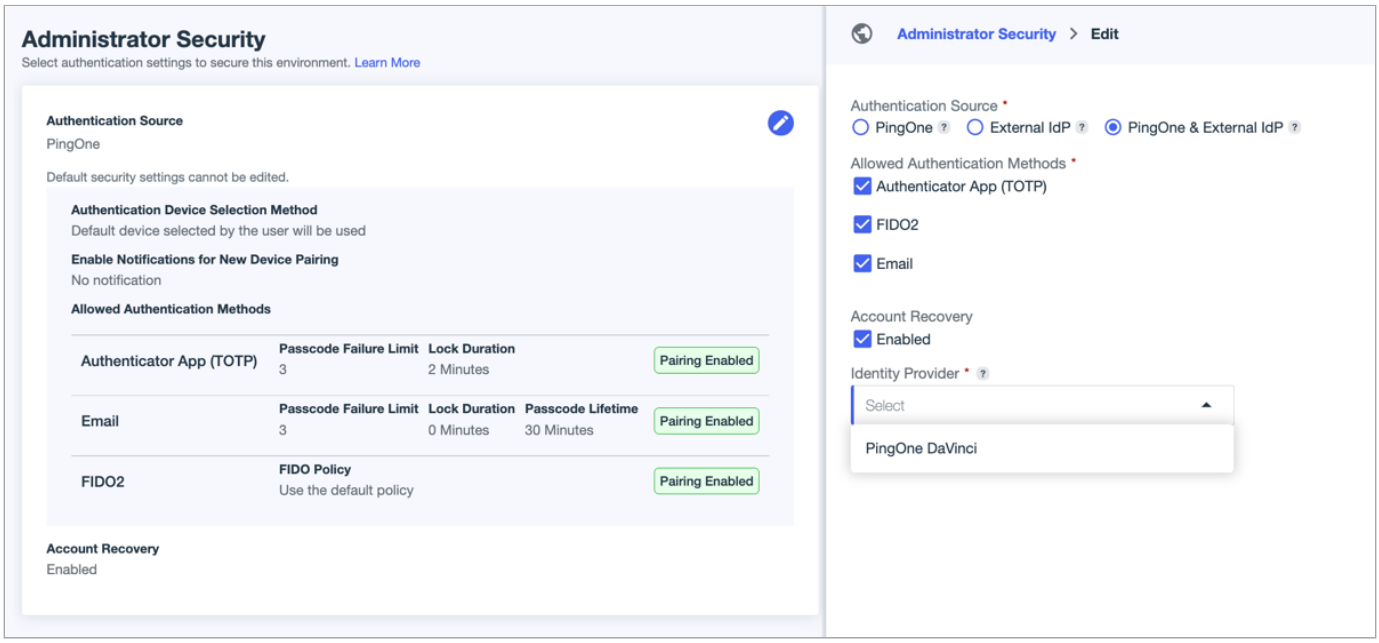
Steps

1. In the PingOne admin console, go to **Settings > Administrator Security**.

Copyright © 2025 Ping Identity Corporation



2. Click the **Pencil** icon to change the security settings.



3. For **Authentication Source**, select one of the following.

Choose from:

- **PingOne** (default): PingOne is used as the authentication source. A system-delivered authentication policy requiring MFA is enabled. You can't use a different authentication policy, but you can select which supported methods to use for MFA. Supported MFA methods include email, authenticator app (TOTP), and FIDO2. The first time an administrator signs on to the admin console, they're prompted to configure one of the methods you enable.

  > **Note**
  >
  > If you haven't updated the MFA policies for your environment to use FIDO2 instead of FIDO, you won't see the FIDO2 option on **Administrator Settings**. Learn more in Updating an existing MFA policy to use FIDO2.
  > FIDO isn't supported for new device registration during just-in-time (JIT) registration of administrators. If existing administrators have a registered FIDO device for MFA, that method is valid as long as your MFA policy is not updated to FIDO2.

- **External IdP**: This option is enabled only if you have configured at least one external IdP in your environment. The selected IdP is used as the authentication source for the admin console. If you select this option, ensure that your external IdP is configured to follow best practice security recommendations.

  You should also test the connection to ensure that it is configured correctly. Administrators will be unable to sign on if this connection is configured incorrectly.

  > **Note**
  >
  > You can't make changes to the IdP configuration from this page. Go to **Integrations** > **External IdPs** if you need to edit the connection. Learn more in Editing an identity provider.

- **PingOne & External IdP**: This option is enabled only if you've configured at least one external IdP in your environment. The selected IdP is used as the initial authentication source for the admin console. After the user authenticates through the IdP, PingOne sends a secondary authentication request unless you select **Limit MFA to specific populations** and require secondary authentication only for specific populations.

  Test the connection to the IdP to ensure that it is configured correctly. If the connection to the IdP fails, the administrator can sign on to PingOne directly, as long as they have valid credentials in PingOne.

4. Configure the applicable settings:

Setting	Description
Allowed Authentication Methods	**PingOne** and **PingOne & External IdP** only. Select at least one MFA method for verification. ◦ **Authenticator App (TOTP)** ◦ **FIDO2** ◦ **Email**

Copyright © 2025 Ping Identity Corporation

Setting	Description
Account Recovery	**PingOne** and **PingOne & External IdP** only. If selected, PingOne administrators who forget their password can recover their accounts with a one-time passcode (OTP) sent to their email. **Note** This setting applies only to the PingOne account and not to the external IdP. Account recovery for the external IdP is managed by the provider.
Identity Provider	**External IdP** and **PingOne & External IdP** only. Select the IdP to use for authentication. This IdP will be labeled with an **Administrator IDP** badge in **Integrations > External IdPs**. The IdP can't be disabled or deleted while assigned in **Administrator Security**. **Important** If you change the selected IdP, the settings for the new IdP are used for authentication. You should always test the connection configuration when you change this setting to ensure that administrators are able to sign on to PingOne.
Limit MFA to specific populations	**PingOne & External IdP** only. Select this checkbox to require a secondary authentication request from PingOne only for the populations you select in the **Populations Requiring MFA** list. Users in populations that aren't selected will authenticate only once, through the external IdP.

5. Click **Save**.

Configuring administrator security - PingID

Use the **Administrator Security** page to view or change the authentication settings for the PingOne admin console.

You can use PingID, an external identity provider (IdP), or a combination of external IdP and PingID. Some configuration might need to be done in the PingID console.

> **Note**
> This topic only applies to environments that include PingID. If your environment does not include PingID, go to Configuring administrator security.

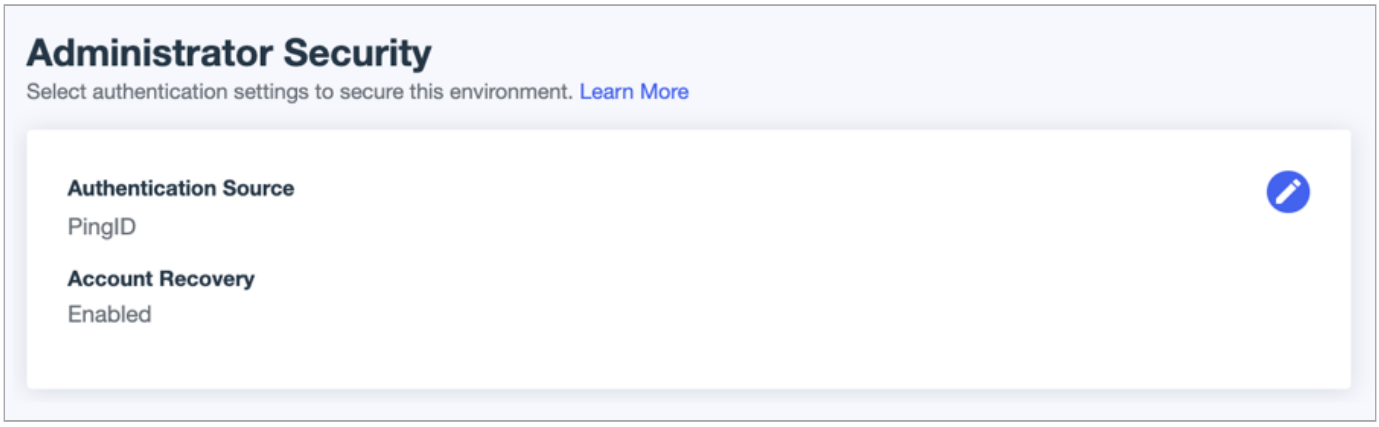
Ping Identity requires multi-factor authentication (MFA) for all PingOne administrators.

Copyright © 2025 Ping Identity Corporation

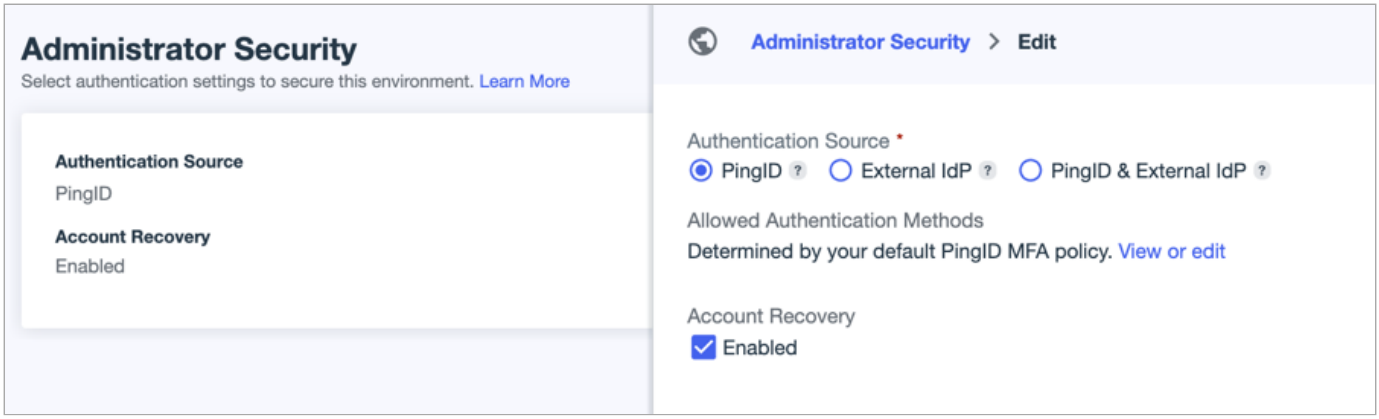
You must have the Organization Admin role, Environment Admin role, or a custom role with equivalent permissions to configure **Administrator Security**.

Steps

1. In the PingOne admin console, go to **Settings > Administrator Security**.



2. Click the **Pencil** icon to change the settings.



3. For **Authentication Source**, select one of the following.

   Choose from:

   - **PingID** (default): PingID is used as the authentication source. You configure the authentication policy and set the allowed MFA methods in the PingID console. Click **Configure Now** to open the PingID admin portal in a separate window and configure the authentication policy. Learn more in the Authentication Policy section of the PingID documentation.

     > **Note**
     >
     > If the environment was created after January 7, 2025, or if your PingID tenant was migrated to PingOne after March 31, 2025, the default MFA policy is managed from **Authentication > MFA** in PingOne. Learn more in Configuring an MFA policy for strong authentication.

   - **External IdP**: This option is enabled only if you have configured at least one external IdP in your environment. The selected IdP is used as the authentication source for the admin console. If you select this option, ensure that your external IdP is configured to follow best practice security recommendations.

Copyright © 2025 Ping Identity Corporation

You should also test the connection to ensure that it is configured correctly. Administrators will be unable to sign on if this connection is configured incorrectly.

> **Note**
> You can't make changes to the IdP configuration from this page. Go to **Integrations** > **External IdPs** if you need to edit the connection. Learn more in Editing an identity provider.

- **PingID & External IdP**: This option is enabled only if you have configured at least one external IdP in your environment. The selected IdP is used as the initial authentication source for the admin console. After the user authenticates through the IdP, PingID sends a secondary authentication request.

  Test the connection to the IdP to ensure that it is configured correctly. If the connection to the IdP fails, as long as the administrator has a recovery account in PingOne, the administrator can sign on to PingOne directly. PingID will then prompt them for secondary authentication.

4. Configure the applicable settings:

Setting	Description
Account Recovery	**PingID** and **PingID & External IdP** only. If selected, PingOne admins who forget their password can recover their accounts with a one-time passcode (OTP) sent to their email. **Note** This setting applies only to the PingID account and not to the external IdP. Account recovery for the external IdP is managed by the provider.
Identity Provider	**External IdP** and **PingID & External IdP** only. Select the IdP to use for authentication. This IdP will be labeled with an **Administrator IDP** badge in **Integrations** > **External IdPs**. The IdP can't be disabled or deleted while assigned in **Administrator Security**. **Important** If you change the selected IdP, the settings for the new IdP are used for authentication. You should always test the connection configuration when you change this setting to ensure that administrators are able to sign on to PingOne.

5. Click **Save**.

Certificates and key pairs

When you create a new environment, PingOne creates two default key pairs: one for signing and one for encryption.

Copyright © 2025 Ping Identity Corporation

The **Certificates and Key Pairs** page shows details about the cryptographic certificates and key pairs that are set up for your environment.

The default certificates include the following:

- Subject DN
- Serial number
- Issuer
- Issued date
- Expiration date

Viewing certificates and key pairs

Use the **Certificates and Key Pairs** page to view details about the certificates that are set up for your environment.

Steps

1. Go to **Settings** > **Certificates and Key Pairs**.

   You can browse or search for certificates.

2. Click the expand icon to see more information for each certificate.

   The certificate details page shows the following:

   ### *Details*

   - **Subject DN**: The subject distinguished name for the certificate. The subject DN includes attribute-value pairs, such as common name (CN), organizational unit (OU), organization (O), and country name ©.
   - **Serial**: The serial number, a unique identifier for the certificate that is generated by the certificate authority.
   - **Issuer**: The certificate authority that issued the certificate. The issuer value includes attribute-value pairs, such as CN, OU, O, and C.
   - **Issued date**: The date that the certificate was issued.

   ### *Applications*

   Lists applications that are currently using the certificate. To add a certificate to an application, Editing an application - SAML.

   ### *CSR*

   Use the CSR tab to generate certificate signing requests (CSRs) and import the certificate authority (CA) response. For more information, see Generating a CSR.

Adding a certificate and key pair

Use the Certificates and key pairs page to set up a certificate for your environment.

Copyright © 2025 Ping Identity Corporation

About this task

The certificate must be valid when you add it to PingOne. You cannot add a certificate before its validity period begins (the certificate's `NotBefore` date) or after it expires (the certificate's `NotAfter` date). The private key must be unencrypted. You cannot upload a private key that is protected by a password or passphrase. The certificate, private key, and certificate chain must all be PEM-encoded unless uploading a pkcs12 file format.

Steps

1. Go to **Settings** > **Certificates and Key Pairs**.
2. Click **+ Add** and then click **Create key pair**.
3. Enter the following information:

Option	Description
Common name	The server name that is covered by the certificate. It is typically made up of the domain name, such as `www.example.com`. Do not use special characters (?, $, % and so on), IP addresses, port numbers, or http:// or https:// in the common name.
Usage type	Certificates can be used for signing and verification, encryption, SSL, issuance, or outbound mTLS. Select the primary usage for this certificate.
Organization	The corporation, university, or government agency that is covered by the certificate. Use the legal name under which your organization is registered. Do not abbreviate or use any of these symbols: ! @ # $ % ^ * ( ) ~ ? > < / \.
Organization unit	A division within the primary organization, such as `Engineering` or `Human Resources`. If your organization is doing business as a trade name, you can specify the trade or DBA name in this field.
City	The city in which the organization is located. Do not use abbreviations. For example, spell `Saint Louis` rather than `St. Louis`.
State	The state or province in which the organization is located.
Country	The two-character ISO 3166-1 country code. For example, `US` for the United States.
Validity days	The number of days the key is valid, with a maximum of 730 days.

Copyright © 2025 Ping Identity Corporation

Option	Description
Key algorithm	The public key algorith with which to generate the public-provate key pair. Choose RSA (Rivest Shamir Adleman) or EC (Eliptic Curve).
Key size bits	The number of bits in the key's algorithm. The available values depend on the selected key algorithm.
Signature algorithm	The cryptographic algorithm used by the certification authority to sign the certificate. The available values depend on the selected key algorithm.

4. Click **Save and Finish**.

Importing a certificate and key pair

Use the **Certificates and Key Pairs** page to set up a certificate for your environment.

About this task

The certificate must be valid when you add it to PingOne. You cannot add a certificate before its validity period begins (the certificate's `NotBefore` date) or after it expires (the certificate's `NotAfter` date). The private key must be unencrypted. You cannot upload a private key that is protected by a password or passphrase. The certificate, private key, and certificate chain must all be PEM-encoded unless uploading a PKCS 12 file format.

Steps

1. Go to **Settings** > **Certificates and Key Pairs**.
2. Click **+ Add**, and then click **Import key pair/cert**.
3. Select the primary usage type for this certificate.

   Certificates can be used for signing and verification, encryption, or SSL.
4. Click **Select a file** and go to the appropriate file on your local file system.
5. Select the file and click **Open**.
6. In the **Import key pair certificate** window, click **Upload**.

Downloading a certificate

Use the **Certificates and Key Pairs** page to export a certificate with a public key from a key pair to your local file system.

Steps

1. Go to **Settings** > **Certificates and Key Pairs**.
2. Locate the key pair you want to download by browsing, filtering, or searching for available entries.

Copyright © 2025 Ping Identity Corporation

3. Click the details icon to expand the appropriate certificate.
4. Click the **Details** tab.
5. Click **Download certificate**.
6. Select the desired format: **X509 PEM (.crt)** or **Certificates PKCS7 DER (.p7b)**.

Result

The file is saved to your local file system.

Designating default keys

When you create an organization, PingOne includes a default signing key and default encryption key. You can designate different keys as the default signing key and default encryption key if needed. For example, if an existing key expires, you can designate a different key as default.

Steps

1. Go to **Settings** > **Certificates and Key Pairs**.
2. Locate the key you want to set as default.
3. Click the details icon to expand the appropriate key.
4. Do one of the following:
    - For a signing key, click **Make Default Signing Key**. In the confirmation message, click **Continue**.
    - For an encryption key, click **Make Default Encryption Key**. In the confirmation message, click **Continue**.

    > **Note**
    > You can't set expired keys as default.

Result

The default key is indicated with a **Default** label.

Assigning a key pair to an application

New applications automatically use the default key pair, but you can change the key pair that an existing application uses.

Steps

1. Go to **Settings** > **Certificates and Key Pairs**.
2. Locate the key you want to set as default.
3. Click the details icon to expand the appropriate key.
4. Click the **Applications** tab.
5. For the appropriate application, click **Reassign**.

Copyright © 2025 Ping Identity Corporation

6. In the **Reassign Key Pair** window, select the new key pair.

> **Note**
>
> If you change the default key, existing applications will continue to use the key that was assigned when the application was created.

Key rotation policy

PingOne uses key rotation to automatically generate new cryptographic keys at a particular interval. The default rotation is 90 days, which exceeds industry best practices.

Administrators can review and fine-tune key rotation policies by using the PingOne API. For more information, see Key rotation policies in the PingOne Platform API Reference.

A KRP applies to:

- OIDC Web apps
- Native apps
- Single-Page apps
- Custom apps created through the Management API. For more information, see Application operations in the PingOne API Reference.

> **Note**
>
> Although any OIDC-based application can be configured to use the KRP, if the application is configured with scopes from the PingOne API and if the application includes PingOne API scopes in its authorization requests, PingOne uses the PingOne default key to sign the access tokens.

Related links

- Viewing the signing key for an application
- Updating the key rotation for an application

Viewing the signing key for an application

Use the application details panel to view the current signing key for an application.

About this task

For new applications, PingOne automatically uses a key from the default KRP to sign access tokens and ID tokens. For applications created before the KRP feature was introduced, PingOne won't automatically use a key from the default KRP to sign access tokens and ID tokens. However, you can upgrade the application to the new KRP in the **Overview** tab in the application details panel.

Steps

1. Go to **Applications > Applications**.

Copyright © 2025 Ping Identity Corporation

2. Locate the application you want to view. You can browse or search for applications, or narrow your search to a particular application type.
3. Click the application entry to open the details panel.
4. Click the **Configuration** tab and locate the **General** section. The **Signing Key** setting shows which key the application is using. If the application is not using the key rotation policy, you can configure the application to do so. See Updating the key rotation for an application.

Updating the key rotation for an application

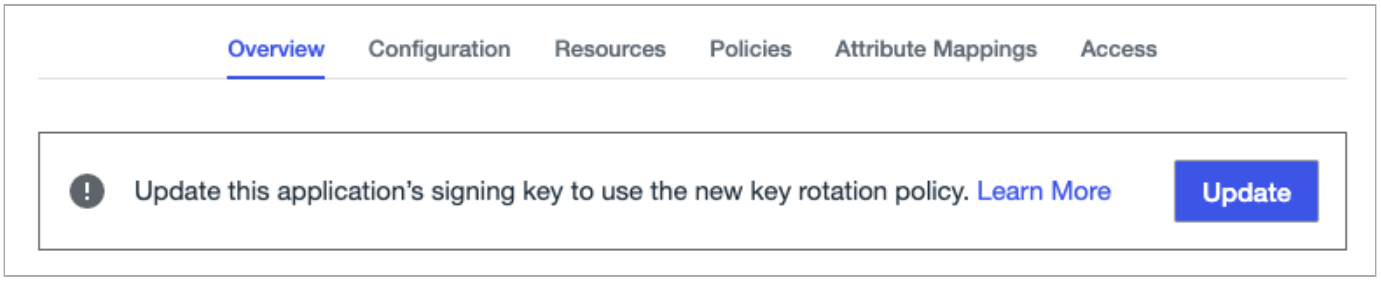
Use the application details panel to update the key rotation for an application.

About this task

For new applications, PingOne automatically uses a key from the default KRP to sign access tokens and ID tokens. For applications created before the KRP feature was introduced, PingOne won't automatically use a key from the default KRP to sign access tokens and ID tokens. However, you can upgrade the application to the new KRP in the **Overview** tab in the application details panel.

Steps

1. Go to **Applications** > **Applications**.
2. Locate the application you want to view. You can browse or search for applications, or narrow your search to a particular application type.
3. Click the application entry to open the details panel.
4. On the **Overview** tab, locate the banner at the top of the page. Click the **Update** button.



5. In the confirmation message, select **I understand and would like to continue**, and then click **Confirm**.

Converting PEM certificates to a different format

If needed, you can convert PEM certificates to a different format, such as PFX or PKCS#7.

Before you begin

You must have:

- The original private key that was used for the certificate
- A PEM (`.pem`, `.crt`, `.cer`) file

Copyright © 2025 Ping Identity Corporation

- OpenSSL

About this task

Certificates are commonly issued as PFX files, with the extension `.pfx` or `.p12`. If you have a certificate in another format, you can convert it to PFX and import it to PingOne.

The PKCS#7 or P7B format is stored in Base64 ASCII format and has a file extension of `.p7b` or `.p7c`. A P7B file contains certificates but not the private key.

Steps

1. Open a terminal window.
2. Run the command for the conversion you want to perform:

   Choose from:

   - PEM to PFX:

     ```
     openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -
     certfile more.crt
     ```

Syntax	Description
`openssl`	The command for executing OpenSSL.
`pkcs12`	The file utility for PKCS#12 files in OpenSSL.
`-export -out certificate.pfx`	Exports and saves the PFX file as `certificate.pfx.`
`-inkey privateKey.key`	Uses the private key file `privateKey.key` as the private key to combine with the certificate.
`-in certificate.crt`	Uses `certificate.crt` as the certificate to combine with the private key.
`-certfile more.crt`	(Optional) Use this option if you have more than one certificate you want to include in the PFX file.

   - PEM to PKCS#7:

     ```
     openssl crl2pkcs7 -nocrl -certfile certificate.crt -out certificate.p7b -outform DER
     ```

Syntax	Description
`openssl`	The command for executing OpenSSL.
`crl2pkcs7`	The file utility for PKCS#7 files in OpenSSL.

Copyright © 2025 Ping Identity Corporation

Syntax	Description
`-nocrl`	Specifies to not include a certificate revocation list (CRL) in the output file and to not read a CRL from the input file.
`-certfile certificate.crt`	Specifies a filename containing one or more certificates in PEM format. All certificates in the file are added to the PKCS#7 structure. You can use this option more than once to read certificates from multiple files.
`-out certificate.p7b`	Outputs the file as `certificate.p7b`.
`-outform DER`	Specifies the PKCS#7 structure output format. The distinguished encoding rules (DER) format is a DER-encoded CRL structure.

Generating a CSR

On the **Certificates and Key Pairs** page, you can generate a certificate signing request (CSR) and download it to your local file system.

About this task

A CSR is an encoded file you can send to the certificate authority to apply for a public key certificate. If granted, the certificate authority will send you a response. The public key in the response must match the public key of this certificate.

Steps

1. Go to **Settings** > **Certificates and Key Pairs**.
2. Locate the appropriate key pair by browsing, filtering, or searching for entries.
3. Click the details icon to expand the entry.
4. Click the **CSR** tab.
5. Click **Export CSR**.
6. Select the desired format: **X509 PEM (.csr)** or **PKCS10 DER (.p10)**.

Result

The file is saved to your local file system.

Related links

- Importing the CA response

Copyright © 2025 Ping Identity Corporation

Generating a CSR for a custom domain

If you use a custom domain, you need to create the custom domain resource in PingOne and import the SSL certificate used by the custom domain resource.

About this task

To implement a custom domain, you'll:

1. Create the custom domain resource. For example, `auth.acme.com`.
2. Create a CNAME record in the `acme.com` DNS for `auth.acme.com` that points to the canonical name when the custom domain was created.
3. If you don't have an SSL certificate, outside of PingOne, generate a certificate for `auth.acme.com` (a certificate request that's signed by a certificate authority), which results in a private key, certificate chain, and certificate.
4. Import the SSL certificate (chain, cert, private key).

Learn more about custom domains in Domains.

If you don't have an SSL certificate, create the trusted SSL certificate for the custom domain as follows:

Steps

1. Start **`openssl`** or install it if you haven't already.
2. Run the following **`openssl`** command.

   ```
   openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
   ```

3. Enter the following certificate signing request (CSR) information at the prompt:
   - Common Name (CN)
   - Organization
   - Organization Unit (OU)
   - City (or Locality)
   - State (or Province)
   - Country
4. Submit your CSR to a certificate authority (CA) for validation.

Result

After validation, the CA returns the trusted SSL certificate, which you can import to complete and enable the custom domain. Learn more in Adding an SSL certificate.

Copyright © 2025 Ping Identity Corporation

Importing the CA response

On the **Certificates and Key Pairs** page, you can import the CA response that you received from the certificate authority (CA). If you have applied for a public key certificate, the certificate authority will send you a response. You can import the CA response to PingOne. The public key in the response must match the public key of this certificate.

Steps

1. Go to **Settings** > **Certificates and Key Pairs**.
2. Locate the appropriate certificate by browsing or searching for certificates.
3. Click the details icon to expand the certificate.
4. Click the **CSR** tab.
5. In the **Import CA response** section, click **Choose**.
6. On the local file system, locate the CA response file.
7. Click **Open**.

Result

The file is imported to PingOne, and the key pair entry is updated to reflect the new issuer values in the CA response.

Related links

- Generating a CSR

Domains

With PingOne, you can configure a custom domain name for the browser-based user interface and other PingOne services.

With a custom domain name, you can route your own domain name to PingOne services, removing all references to `pingone` in the browser address bar. The end user sees the custom URL in their browser, such as `auth.example.com` instead of the default URL, such as `auth.pingone.com`.

All PingOne products and services with end-user interfaces support custom domains, except for the Admin Console.

Custom domains are owned and controlled by the administrator.

Setting up a custom domain

Before you create a CNAME record with your DNS manager, you must first create an entry for the custom domain in PingOne. PingOne provides a canonical name value that you will use to create a CNAME record for your domain name.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> You can configure one custom domain per environment.
> Custom domains created after March 17, 2025 will use Cloudflare instead of Amazon CloudFront. Contact your organization's network infrastructure team and direct them to review the Custom domain migration to Cloudflare support article for more information (sign on required). This post contains details about how to assess whether your network and firewall settings require updates to support the new infrastructure.

Before you begin

Before you begin, you'll need the following:

- An existing custom domain
- Access to your DNS manager
- A valid Secure Sockets Layer (SSL) certificate

Adding a custom domain

Add the custom domain to your PingOne environment.

Steps

1. In the PingOne admin console, go to **Settings** > **Domains**.
2. Click **+ Add Custom Domain**.
3. Enter the domain name, such as `auth.example.com` and click **Save**. PingOne validates the domain name to ensure that it is not already in use.

   Before the custom domain becomes active, PingOne requires that you provide an appropriate SSL certificate and point your custom domain to a PingOne-supplied canonical name using a CNAME record. The CNAME record proves that your custom domain is not already in use and directs requests to your custom domain through your PingOne environment.

Adding the CNAME to your DNS configuration

After you add the custom domain name, copy the canonical name from PingOne and add it to the CNAME record for your custom domain.

Steps

1. In the PingOne admin console, go to **Settings** > **Domains**.
2. Click **Verify domain**.
3. On the **Verify Custom Domain** modal, copy the **Canonical Name**.

   > **Note**
   >
   > Some DNS providers do not support a trailing period in the CNAME. If you are using one of these DNS providers, omit the trailing period from the CNAME record.

4. Add the Canonical Name to the CNAME record for your custom domain.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> The canonical name will not have a DNS resolution until you complete the steps in Verifying the custom domain name and Adding an SSL certificate.

Verifying the custom domain name

Ensure that you have added a CNAME record to your DNS configuration before starting this task. You cannot verify a custom domain until you update the DNS manager to add the CNAME record value, which consists of your domain name pointing to the canonical name that you copied from PingOne.

Steps

1. In the PingOne admin console, go to **Settings > Domains**.
2. Click **Verify domain**.
3. On the **Verify Custom Domain** modal, click **Verify**.

> **Note**
>
> The specifics of DNS configuration depend on your DNS manager. Changes to the DNS can take up to 24 hours to propagate through the internet, so you might need to click **Verify** multiple times over that period of time until the DNS record is found.

Result

PingOne verifies that the CNAME is associated with the custom domain name you entered. This association is needed to set up domain control and enable the functionality of a custom domain.

Adding an SSL certificate

To enable HTTPS for your custom domain, you need to add an SSL certificate from a certificate authority (CA). You can also use these steps to update a certificate that has expired. Learn more in Generating a CSR for a custom domain.

About this task

> **Note**
>
> - Do not use a self-signed certificate or a certificate signed by a CA that is internal to your own organization. Certificates must be signed by a globally trusted CA.
> - Minimum encryption of RSA-2048 or ECDSA-256 is required.
> - The certificate must be valid.
> - You can use wildcard and Subject Alternative Name (SAN) certificates, but they must match the domain name.
> - When reimporting a certificate, the key type and size cannot be changed.
> - If you want to change the key type or size, you must delete the custom domain and recreate it using the new certificate. Recreating the domain will also change the canonical name for the domain.

Steps

1. In the PingOne admin console, go to **Settings > Domains**.
2. Click **Add an SSL certificate**.

Copyright © 2025 Ping Identity Corporation

3. Enter the following information:
    - **Private key**. A PEM-encoded unencrypted private key that matches the certificate's public key.
    - **Certificate**. A PEM-encoded certificate to import.
    - **Intermediate certificates**. A PEM-encoded certificate chain. Do not include the end-entity certificate.
4. Click **Save**.

Testing the custom domain

Test your custom domain to ensure that it resolves to the correct location. After you add a certificate, it can take up to several hours for the changes to propagate through the network.

Steps

1. Open a web browser, and enter the address of your custom domain, such as `https://auth.example.com/myaccount`.
2. Verify that you are presented with the sign-on screen for your application or other appropriate resource.

Setting up a trusted email domain

You can configure PingOne to send emails on your organization's behalf from a trusted domain. Use PingOne to get the email domain trust records and add them to your DNS configuration. You can also set up DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF).

Before you begin

You'll need:

- An existing domain
- Access to your DNS manager

About this task

> **Note**
>
> - You can configure up to 50 trusted email domains per environment.
> - Learn more about configuring trusted email addresses for a trusted email domain in Configure trusted email addresses.
> - The `_pingoneemail` text record on the **Email Domain Verification** modal is optional, but it is a best practice to add this record to your DNS. If it isn't added, each sender email address you add must be verified separately through a verification email.

Adding the trusted email domain

You'll add the trusted email domain to your environment and then configure your DNS manager.

Steps

1. In the PingOne admin console, go to **Settings > Domains**.

Copyright © 2025 Ping Identity Corporation

2. Click **+ Add Email Domain**.
3. Enter the trusted email domain name, such as `auth.example.com` and click **Save**. PingOne validates the domain name to ensure that it is not already in use.

Adding the records to your DNS configuration

After you add the trusted email domain, copy the email domain trust records and add them to your DNS configuration. Ensure that you add the records as TXT records, not CNAME records.

Steps

1. In the PingOne admin console, go to **Settings** > **Domains**.
2. Locate the appropriate email domain name entry and click **Verify**.
3. In the **Email Domain Verification** modal, copy the email domain trust records to a secure location.
4. Go to your DNS manager and update it with the email domain entries you copied. You can leave the PingOne window open, or close it and return later.

> **Note**
>
> The specifics of DNS configuration depend on your DNS manager. We recommend that you wait at least 1 hour for the DNS changes to propagate through the internet, although it can take up to 24 hours.

Verifying the trusted email domain

Ensure that you have added the trust records to your DNS configuration before starting this task. You cannot verify a trusted email domain until you update the DNS manager to add the trust records.

Steps

1. In the PingOne admin console, go to **Settings** > **Domains**.
2. Locate the appropriate email domain name entry and click **Verify**.
   - A green checkmark indicates that the verification check succeeded.
   - A yellow exclamation point indicates that the verification check did not succeed. We recommend that you wait 1 hour and try again. Complete DNS propagation can take up to 24 hours.
3. Click **Close**.

The email domain name should show a green checkmark to confirm that it has been verified, and the **DKIM Setup** and **SPF Setup** buttons should be visible. If there is a yellow exclamation point next to the email domain name, click **Verify** to retry the verification process.

Setting up DKIM

After you've verified the trusted email domain, you can set up DKIM. DKIM authenticates email messages and prevents forged sender addresses.

Steps

1. In the PingOne admin console, go to **Settings** > **Domains**.

Copyright © 2025 Ping Identity Corporation

2. Locate the appropriate email domain name entry and click **DKIM Setup**.
3. Copy the email trust records.

> **Note**
>
> If you see multiple regions listed, such as EU-WEST-1, US-EAST-1, US-WEST-1, you should copy the CNAME records for all regions. This is required for Simple Email Service (SES) to sign messages, and can also allow messages to be sent from another region if there's a fault in the primary region.

4. Go to your DNS manager and update it with the DKIM entries you copied. Ensure that you add the records as CNAME records, not TXT records.
5. Return to the **DKIM Setup** modal and click **Verify**.
   - A green checkmark indicates that the verification check completed successfully.
   - A yellow exclamation point indicates that the verification check did not succeed. We recommend that you wait 1 hour and try again. Complete DNS propagation can take up to 24 hours.
6. Click **Close**.

Setting up SPF

You can set up SPF, which helps protect senders and recipients from spam, spoofing, and phishing. By adding an SPF record to your DNS, you can specify a list of senders approved to send email from your domain.

Steps

1. In the PingOne admin console, go to **Settings > Domains**.
2. Locate the appropriate email domain name entry and click **SPF Setup**.
3. Copy the email trust records.
4. Go to your DNS manager and update it with the SPF entries you copied.
5. Return to the **SPF Setup** modal and click **Verify**.
   - A green checkmark indicates that the verification check has completed successfully.
   - A yellow exclamation point indicates that the verification check has not succeeded. We recommend that you wait 1 hour and try again. Complete DNS propagation can take up to 24 hours.
6. Click **Close**.

Removing a custom domain or trusted email domain

If you no longer need a custom domain or trusted email domain, you can remove it.

Before you begin

If you remove a custom domain, your end users will no longer be able to access applications or other resources using the custom domain name. If you remove a trusted email domain, you will no longer be able to send email messages from the trusted domain.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Settings** > **Domains**.
2. Locate the custom domain or trusted email domain that you want to remove.
3. For the appropriate entry, click **Remove**.
4. In the confirmation message, click **Remove**.

Sender

Use the Sender page to configure your organization's SMTP server.

You can use the Ping Identity server or a custom server.

See:

Configuring a custom SMTP email notification server

Configuring trusted email addresses

Configuring an SMS/Voice sender account with PingOne

Configuring a custom SMTP email notification server

Use the Sender page to configure your organization's SMTP server.

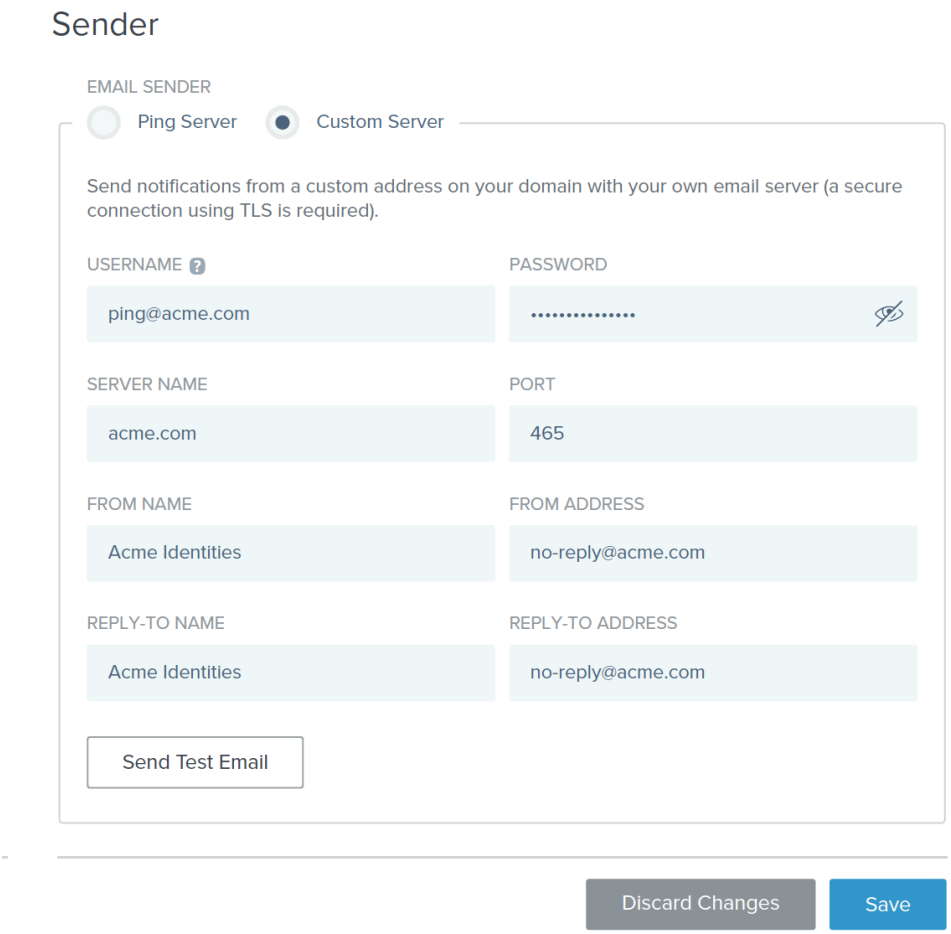
Steps

1. Go to **Settings** > **Sender**.
2. Click the **Email** tab.

   The default **Ping Server** details appear, until a **Custom Server** is configured for the organization. The **Ping Server** settings are not configurable.

   - **From Name**: The name that appears as the sender's name in the email message.
   - **From Address**: The email address that appears as the sender's email address in the email message.
   - **Reply-To Name**: The name that appears as the sender's reply-to name in the email message.
   - **Reply-To Address**: The email address that appears as the sender's reply-to address in the email message.
3. Select **Custom Server** to use the organization's SMTP server instead of the Ping Identity email service.

Copyright © 2025 Ping Identity Corporation



> **Note**
>
> Any edit changes on previously saved custom server fields requires re-entry of the **Password** field.

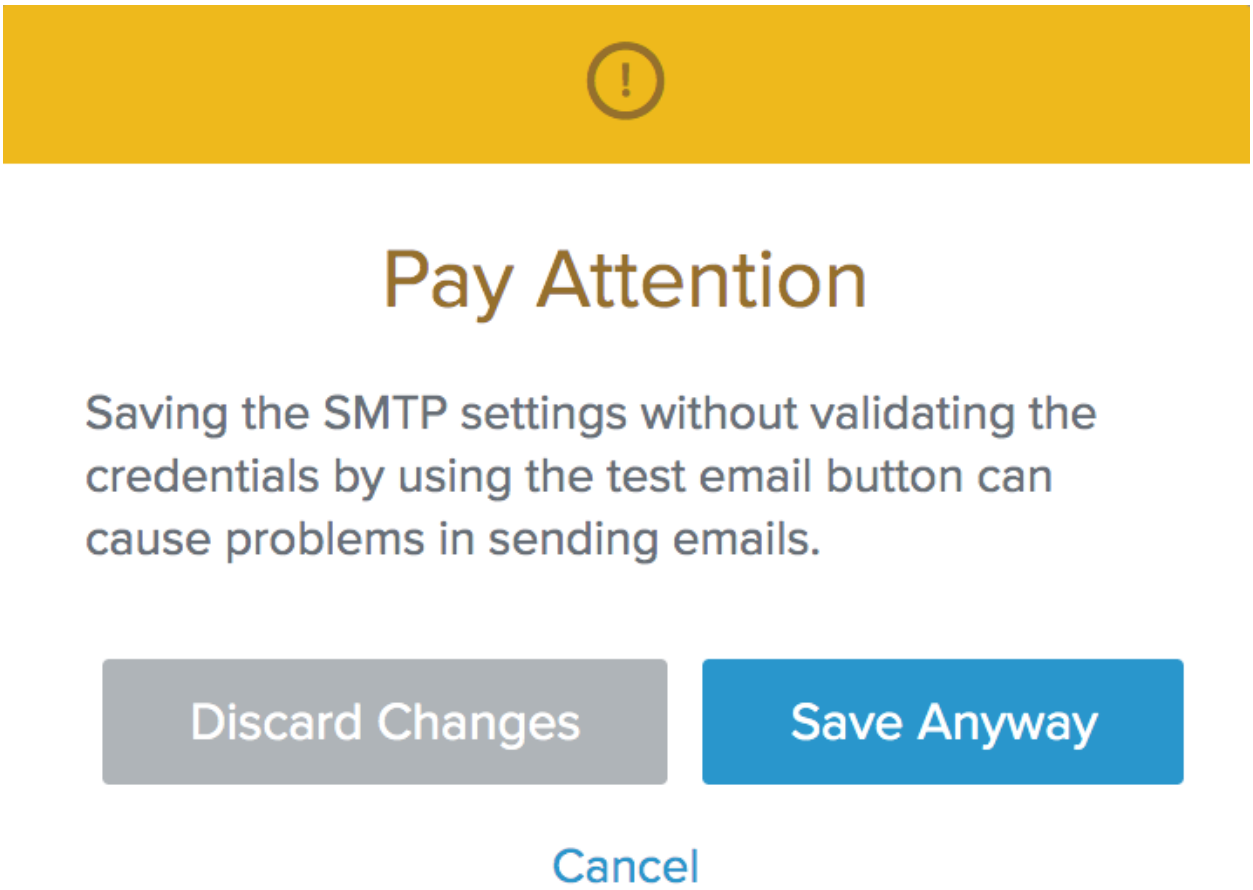
Field	Type	Description
Username	Mandatory	The organization's SMTP server's user name.
Password	Mandatory	The organization's SMTP server's password.
Server Name	Mandatory	The name of the organization's SMTP server.
Port	Mandatory	The port used by organization's SMTP server to send emails (default: 465). NOTE: The protocol used depends upon the port specified. If you specify port 25,587, or 2525, SMTP with STARTTLS is used. Otherwise, SMTPS is used.
From Name	Optional	The name that appears as the sender's name in the email message.

Copyright © 2025 Ping Identity Corporation

Field	Type	Description
From Address	Mandatory	The email address that appears as the sender's email address in the email message.
Reply-To Name	Optional	The name that appears as the sender's reply-to name in the email message.
Reply-To Address	Optional	The email address that appears as the sender's reply-to address in the email message.

4. Click **Save** to save your custom changes, or **Discard Changes** to abandon them.

   The **Pay Attention** pop-up opens.



   Choose from the following options:

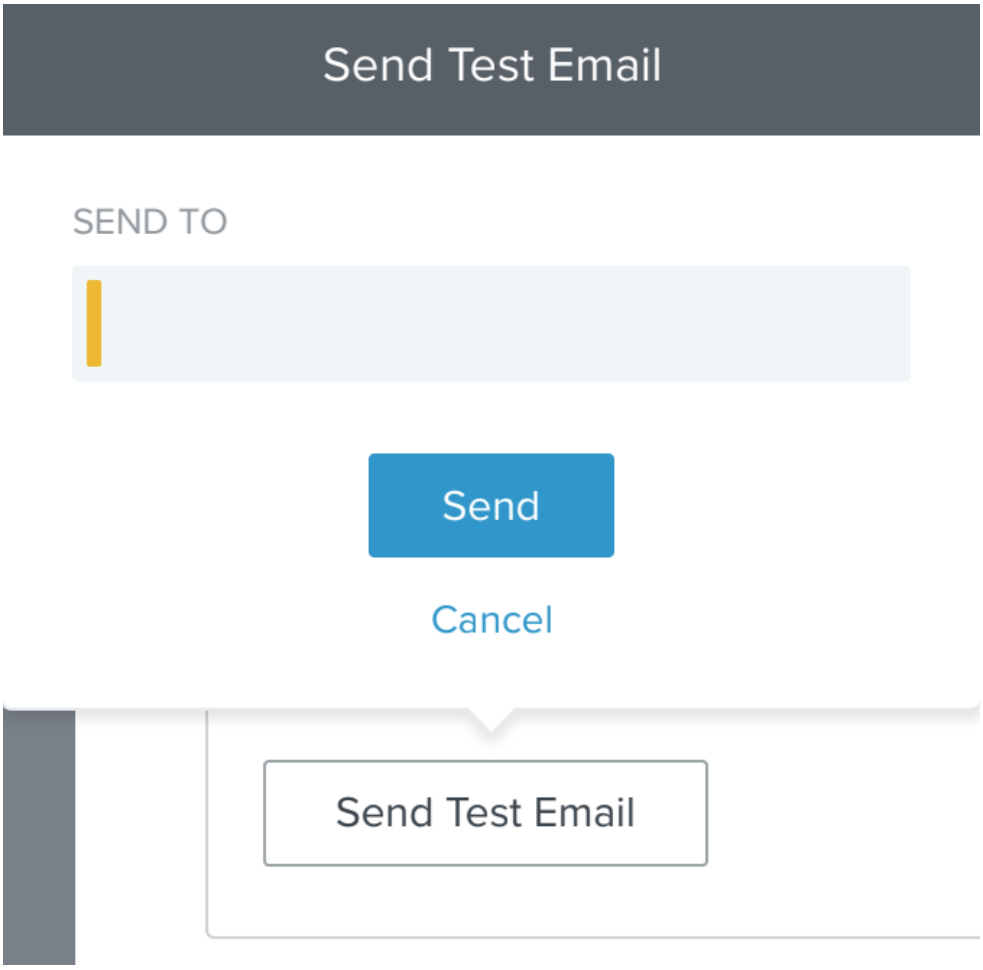
   - **Discard Changes** to keep the previous custom server settings.
   - **Save Anyway** to keep the new custom server configuration settings.

Copyright © 2025 Ping Identity Corporation

> **Important**
>
> When saving, authentication is not tested using the new credentials. We recommend following up with the **Send Test Email** step to confirm successful SMTP server configuration.

5. To test the SMTP server configuration, click the **Send Test Email** button.

   The **Send Test Email** dialog opens.



6. Enter a recipient email address in **Send to** and click **Send**.
7. Check the destination email box for the test email.

   PingOne returns one of the following status messages:

   - **Success**

     A test email was successfully sent to some.body@acme.com.

   - **Failure**

     Using the credentials you provided, we couldn't authenticate with your email server.

Copyright © 2025 Ping Identity Corporation

Using a custom email provider for notifications

To configure PingOne to use an external email service for sending notifications to your users:

1. Go to **Settings** > **Sender**.
2. On the **Email** tab, click the **Pencil** icon.
3. In the **Email Sender** section, click **Custom Provider**.

> **Note**
>
> You can only have a single sender defined for a PingOne environment. After you select **Custom Provider**, any previous email sender settings are erased.

4. For **Provider Name**, enter any name to identify the provider.
5. For **Authorization**:
   - If your authentication with the email provider uses a username and password, select **Basic** and enter the username and password.
   - If your authentication is based on the use of a bearer token, select **Bearer** and enter the token to use.
6. (Optional) Enter the **From Name** and **From Address** values you want to use in the notifications.
7. (Optional) Enter the **Reply-To Name** and **Reply-To Address** values you want to use in the notifications.
8. Provide the information required by your email provider's API:
   1. In the **Type** list, select **GET** or **POST** to specify the type of API request that should be sent.
   2. In the **URL** field, enter the endpoint for your email provider, for example, `https://api.example.com/email`.
   3. If the type is set to **POST**, define the body of the request by selecting one of the options in the **Body** list: **None**, **Form**, or **Raw**.
      - If you select **Form**, use **Key** and **Value** to enter field names and values.
      - If you select **Raw**, use the **Raw** field to enter the information that will be used for the body of the request. The body that you define must include the PingOne variables listed in **Required Variables**: `${from}`, `${to}`, and `${message}`.

      In both **Raw** and **Form** view, when you add one of the required variables to the body, it's highlighted in green in the list. You can also include in the body of the notification the variables listed in **Optional Variables**.
   4. If the type is set to **GET**, append the query parameters that the email provider's API requires to the URL. The URL must also include the required PingOne variables.
   5. Click **Add Header** to add whatever headers the email provider's API requires.
   6. After entering all of the information, click **Send Test Email** to send an email to verify that everything is working correctly.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> When you edit existing settings for the email service, the password is not displayed when the page is loaded. To send a test email, you must re-enter the password. Because **Password** is a mandatory field, **Save** is disabled until you re-enter the password.

9. Click **Save**.

> **Note**
>
> **Save** is disabled until you have filled in all the required fields and have included all the required variables in the body of the request.

Example: Using SendGrid as custom email provider for notifications

Follow these steps to have PingOne use SendGrid for sending notifications to users:

1. Go to **Settings** > **Sender**.
2. On the **Email** tab, click the **Pencil** icon.
3. In the **Email Sender** section, click **Custom Provider**.

> **Note**
>
> You can only have a single sender defined for a PingOne environment. Selecting **Custom Provider** erases any previous email sender settings.

4. For **Provider Name**, enter a name to identify your SendGrid configuration.
5. For **Authorization**, select **Bearer** and enter the token to use for your SendGrid account.
6. Enter the **From Address** to use in the notifications. This address must be a verified sender in SendGrid.
7. (Optional) Enter the **From Name** value you want to use in the notifications.
8. (Optional) Enter the **Reply-To Name** and **Reply-To Address** values you want to use in the notifications.
9. Provide the information required by the SendGrid API:
    1. In the **Type** list, select **POST**.
    2. In the **URL** field, enter `https://api.sendgrid.com/v3/mail/send`.
    3. For the body of the request, select **Raw**.
    4. In the **Raw** field, enter the following JSON:

```
{"personalizations":[{"to":[{"email":"${to}"}]}],"from":{"email":"${from}","name":"${from.name}"},"reply_to":{"email":"${reply-to}","name":"${reply-to.name}"},"subject":"${subject}","content":[{"type":"text/plain","value":"${message}"}]}
```


Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Some of the variables in this sample JSON are optional, for example, `${from.name}`. The variables required by PingOne are listed in the UI and in Using a custom email provider for notifications

5. Verify that the single header required by SendGrid is already shown `(content-type:application/json)`. If not, click **Add Header** and enter the header type and value.

6. After entering all of the information, click **Send Test Email** to send an email to verify that everything is working correctly. Enter the email address to send the test email to and click **Send**.

> **Note**
>
> If you're editing existing settings, the token is not displayed when the page is loaded. To send a test email, you must enter the token alongside the email address you specified for the test email.

10. Click **Save**.

> **Note**
>
> **Save** is disabled until you have filled in all the required fields and have included all the required variables in the body of the request.

Configuring trusted email addresses

Ping Identity can send trusted emails on your organization's behalf, from your organization's trusted domain. This option requires that you first Set up a trusted email domain for your environment, and then configure associated trusted email addresses.

About this task

> **Note**
>
> You can configure up to 10 trusted email addresses for each trusted email domain.

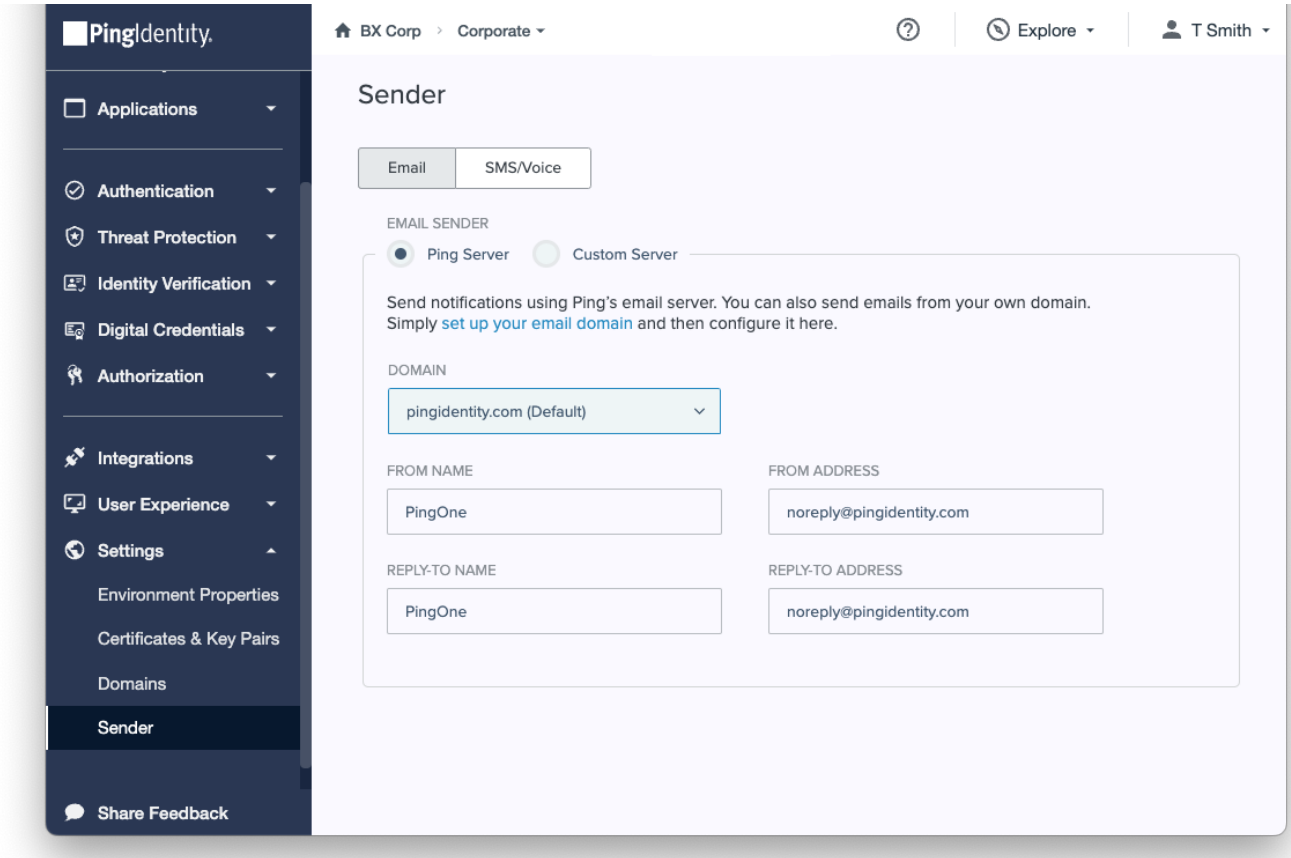
Steps

1. Go to **Settings** > **Sender**.

2. Click the **Email** tab.

3. Select **Ping Server**.

Copyright © 2025 Ping Identity Corporation



> **Note**
>
> The default **Ping Server** details are shown, until a trusted email domain and its associated addresses are configured, or alternatively, a **Custom Server** is configured for the organization. The **Ping Server** settings are configurable only when a trusted email domain is already configured.

- **Domain**: The email domain name. Default: `pingidentity.com`.
- **From Name**: The name that appears as the sender's name in the email message. Default: `PingOne`.
- **From Address**: The email address that appears as the sender's email address in the email message. Default: `noreply@pingidentity.com`.
- **Reply-To Name**: The name that appears as the sender's reply-to name in the email message. Default: `PingOne`.
- **Reply-To Address**: The email address that appears as the sender's reply-to address in the email message. Default: `noreply@pingidentity.com`.

4. Select your trusted email domain from the **Domain** dropdown.
5. Enter the sender details:
    1. **From Name**: Enter the name that should appear as the sender's name in the email message.
    2. **From Address**: Select an email address from the dropdown, or click **+ New Email Address** to open the **New Email Addresses** screen and create a new address.

Copyright © 2025 Ping Identity Corporation

In the **New Email Addresses** screen:

1. Enter the local-part (username) of the trusted email address, and click **Done**. If the `_pingoneemail` text record was not added to your DNS, you'll have to verify the email address by clicking **Next** and carrying out the remaining steps.
2. When you click **Next**, a verification code is mailed to the trusted email address, and the **Email Verification** screen opens.
3. Enter the verification code in the **Verification Code** field.
4. Click **Done**. If verification failed, or if no verification code email was received, click **Resend verification email** to retry.

6. Enter the reply-to details:
   1. **Reply-To Name**: Enter the name that should appear as the reply-to name in the email message.
   2. **Reply-To Address**: Select an email address from the dropdown, or click **+ New Email Address** to open the **New Email Addresses** screen and create a new address, as described for **From Address**.
7. Click **Save** to save your custom changes, or **Discard Changes** to abandon them.

(Customer Only) Configuring WhatsApp as a sender

To use WhatsApp as a strong authentication (MFA) method, you'll need to add your WhatsApp business account as a sender.

Before you begin

Before connecting your WhatsApp business account as a sender in PingOne, configure a WhatsApp business account in the Meta business and developer portals as follows:

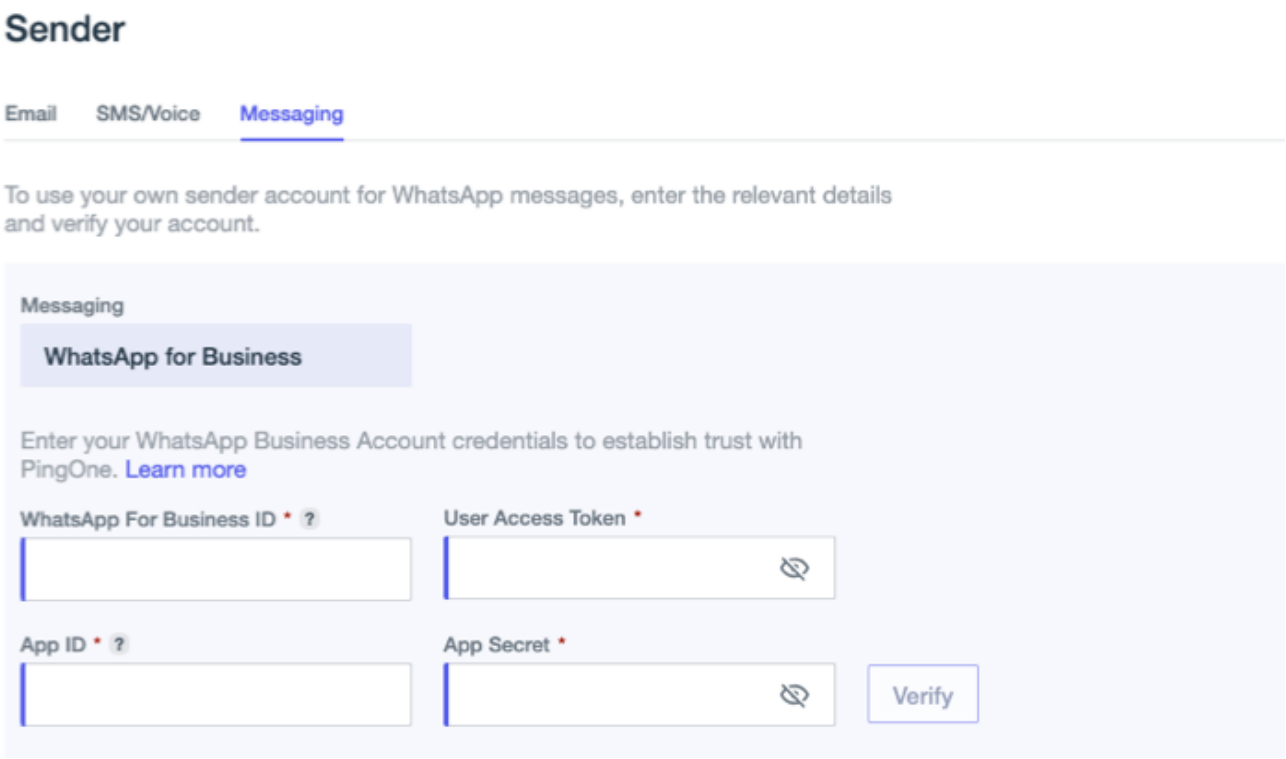
1. If you don't have one already, create a WhatsApp business account.
2. Create a WhatsApp application that includes at least one sender number.
3. In the WhatsApp business account, create a **System User** with the **Admin** System user role.
4. Assign the **System User** to the WhatsApp application.
5. Generate an access token, and then add the following scopes to the access token:
   - `business_management`
   - `manage_app_solution`
   - `whatsapp_business_management`
   - `whatsapp_business_messaging`
6. Get the **App ID** and **App Secret**. You can find the **App ID** and **App Secret** in the Developer portal **App settings**.
7. In the WhatsApp business account, create one or more WhatsApp message templates. The message templates must be of category **Authenticator**. The message template can be used to send notifications in PingOne.

Steps

Copyright © 2025 Ping Identity Corporation

To configure a custom WhatsApp sender:

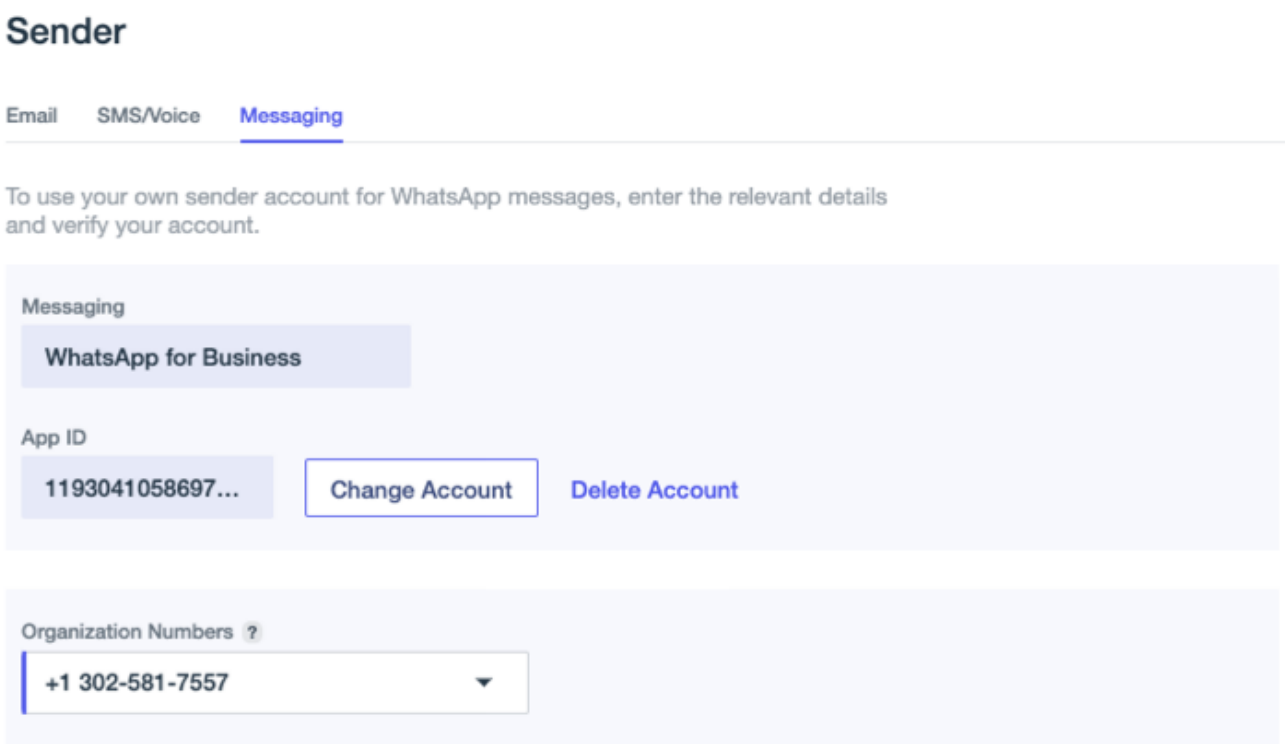
1. In the PingOne admin console, go to **Settings > Sender**.
2. On the **Messaging** tab, enter the following information, and then click **Create**:
   - **WhatsApp for Business ID**: Enter your organization's WhatsApp business account ID.
   - **User Access Token**: Enter the user access token that was generated from your WhatsApp business account.
   - **App ID**: Enter the app ID of the relevant WhatsApp application.
   - **App Secret**: Enter the app secret for the WhatsApp application in the format `<appid|apptoken>`.



PingOne verifies the WhatsApp business account details and displays the available WhatsApp sender numbers.

> **Important**
>
> Validation can take several minutes. Do not close the validation window until the validation is complete.

Copyright © 2025 Ping Identity Corporation



Result

The WhatsApp account is saved.

Next steps

Learn more about the additional steps required to add WhatsApp as an authentication method in (Customer Only) Configuring WhatsApp authentication

Configuring an SMS/Voice sender account with PingOne

If you have an existing Twilio or Syniverse account, you can configure PingOne to use it for SMS and voice notifications:

- Using a Twilio account with PingOne
- Using Twilio Verify with PingOne
- Using a Syniverse account with PingOne
- You can also view Sender IDs per country.

If you have an account with a provider that is not one of the providers natively supported by PingOne (Twilio, Twilio Verify, and Syniverse) you can configure PingOne to use it for SMS and voice notifications:

- Using a custom provider account with PingOne

Using a Twilio account with PingOne

If you have an existing Twilio account, you can configure PingOne to use it for SMS and voice notifications.

Copyright © 2025 Ping Identity Corporation

Keep the following points in mind:

- **Billing:** You must set up your Twilio billing arrangements before you can configure PingOne to use your account.
- **Multiple Twilio accounts:** If you have more than one Twilio account, you can only use one of them. If you have sub-accounts, you can use one of:
  - The main account
  - A single sub-account of the main account
- **Inactive Twilio Accounts:** It is the administrator's responsibility to delete a Twilio account configuration in PingOne if the account becomes inactive. See Managing a Twilio account in PingOne for deleting a custom Twilio account from PingOne.

To configure a Twilio account, go to Configuring a Twilio account for PingOne.

To manage a Twilio account, go to Managing a Twilio account in PingOne.

Configuring a Twilio account for PingOne

Use the information in this section to configure PingOne to use your Twilio account.

Before you begin

Ensure that you have your Twilio account SID and Auth Token. You can copy them as required from the Twilio dashboard. You should also have set up one or more origination phone numbers.

Steps

1. Go to **Settings** > **Sender**.
2. Select **SMS/Voice**.
3. Select **Custom Server**.

   > **Warning**
   > Selecting **Custom Server** will result in deletion of a custom provider if one was defined.

4. In the **Twilio Setup - Account** message, click **Setup**.

   > **Note**
   > The Twilio account applies across all PingOne applications of the environment.

5. To configure your Twilio account to work with PingOne:
   - **Account SID**: Enter the Twilio account SID.

     > **Note**
     > If the **SID** is shorter than 34 characters, an error message is displayed.

   - **Auth Token**: Enter the Twilio account's Auth Token.

Copyright © 2025 Ping Identity Corporation

6. Click **Verify Account**. That validates the account to PingOne and populates the **Origination Numbers** list from your Twilio account.

> **Note**
>
> - If the **Auth Token** is incorrect, an error message is displayed.
> - If there are no originating phone numbers in the Twilio account, it will not be validated to PingOne.

7. Click **Verify Account** to validate the account in PingOne and populate the Origination Numbers list from your Twilio account.

   If the account is successfully verified, the **Twilio Setup - Select Numbers** popup opens, showing all the origination phone numbers available to this Twilio account.

> **Note**
>
> If there are no origination numbers in the Twilio account, it will not be validated in PingOne.

8. In the **Twilio Setup - Select Numbers** message:

   1. Select at least one origination number to use.

      - Select the origination numbers to be used.
      - Click the **Show only selected**/**Show all** toggle to show only the marked phone numbers and hide the numbers that are not selected, or to show selected and unselected numbers.
      - Click **Select all** to select and mark all the origination numbers for this Twilio account.
      - Click **Unselect all** to deselect and unmark all the origination numbers for this Twilio account.

      > **Note**
      >
      > - If you intend to use both SMS and voice, all your selected numbers must support both SMS and voice.
      > - Twilio allows the use of sender IDs (in place of telephone numbers) for commercial use or to comply with regulations requiring SMSs to be sent as **transactional** and not **promotional**.
      > - Sender IDs defined in Twilio are not displayed. PingOne uses the actual phone numbers.
      > - Sender IDs are displayed according to the Sender IDs sent in the API requests.

   2. Select **Done** to continue with the configuration, or **Cancel**.

      Result:

      The **Origination Numbers** table displays.

   3. For **Toll-free** and **Short code** numbers, you can configure supported **Countries** for notification recipients:

      - Click in the **Countries** field. The **Configure countries** popup opens.
      - Click in the **Select countries** field to display the list of countries. Select a country from the list.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> - **Toll-free**: You can add multiple countries in the **Select countries** list. If no country is specified, the specified toll-free number can only be used to dispatch notifications to United States recipient numbers.
> - **Short code**: You can select only one country in the **Select countries** list. If no country is specified, the specified short code can only be used to dispatch notifications to United States recipient numbers.

9. In **Fallback to Default Account**, you can select **Syniverse** to use as a fallback if Twilio becomes unavailable for reasons explained in the following note.

> **Note**
>
> **Under fallback:**
> If PingOne receives an error during the message dispatch process that the used number is invalid, it retries using the fallback option.
> - If there was no way of originating the SMS or voice event with the tenant's own account, and you defined a fallback to Syniverse, the event will be originated from the fallback account.
> - The following errors will cause fallback:
> - All API errors (but not SMS delivery errors)
> - No origination number was found on the Twilio account
> - If a transaction was charged to a specific account, it does not imply that subsequent transactions will be charged to the same account. The account charged for each transaction is determined on an individual basis. Preference is always given to the custom account.

- **Syniverse**:

  Enter the Syniverse **Access Token** and select at least one **Origination Number**.

  1. Copy/paste your Syniverse **Access Token** to the indicated field.

     > **Note**
     >
     > The system uses your access token to connect to your Syniverse account.
     > Recommended: In your account in the Syniverse portal, define an application that is dedicated to PingOne traffic. Use this application for analyzing PingOne traffic throughput, and troubleshooting SMS or voice message despatch cases.

  2. Click the **Verify Account** button. That validates the account to PingOne and populates the **Origination Numbers** list from your Syniverse account.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> - If the **Access Token** is incorrect, an error message is displayed.
> - If your Syniverse account is not fully configured a yellow exclamation mark appears next to the **Access Token** field. If you click on it, the `Syniverse Not Configured` warning message appears.
> - If there are no originating phone numbers in the Syniverse account, it will not be validated to PingOne.
> - To configure your Syniverse account to work with PingOne:
> 1. Copy the URL from the **Address** field.
> 2. In your Syniverse account:
> - In the **Delivery Configuration**, paste the URL that you copied from the PingOne **Address** field.
> - Create 2 subscriptions: **SCG-Message** and **SCG-Voice-Calls**.
>
> See the Syniverse article How to setup a Webhook for Receiving Messages and Notifications for more information.
>
> These Syniverse configurations are required in order that Ping Identity's dashboards and reports will reflect complete and accurate data. Ping Identity will not be able to troubleshoot SMS or voice events related to Syniverse if these configurations are incomplete.

If the account was successfully verified, the display will change to show a list of originating numbers from Syniverse.

3. Select at least one originating telephone number to use.

10. Click **Save**.

11. To complete the setup process, click **I Agree** on the **Third-party Service Consent** message to confirm your legal consent.

> **Note**
>
> You will be asked for legal consent only when entering a new **SID**.

Managing a Twilio account in PingOne

Use the information in this section to manage your Twilio account.

About this task

Managing a Twilio account includes:

- Changing active organization numbers and fallback setting (as in Configuring a Twilio account for PingOne)
- Changing to another account
- Deleting the account

Steps

1. Go to **Settings** > **Sender**.
2. Click the **SMS/Voice** tab.

Copyright © 2025 Ping Identity Corporation

The custom Twilio account's configuration is displayed.

3. Select at least one originating telephone number to use.
4. You can change the **Fallback to Default Account** settings.
5. To switch to a different Twilio account, click **Change Account**. You will be offered the configuration window for a new account. Proceed as in Configuring a Twilio account for PingOne.
6. To delete the active custom account, click the **Custom Provider** radio button.
7. To save your settings, click **Save** at the bottom of the window.

Using Twilio Verify with PingOne

You can add a Twilio account to use Twilio Verify for sending PingOne notifications.

Steps

To start using Twilio Verify for PingOne notifications:

1. In the PingOne admin console, go to **Settings > Sender**.
2. Select **SMS/Voice**.
3. Click the **Pencil** icon.
4. Click **Custom Server**.
5. In the **Sms/Voice Sender** list, select Twilio Verify.
6. Enter the **Account Sid** for the Twilio account.
7. Enter the **Auth Token** for the Twilio account.
8. Enter the **Twilio Verify Service SID**.
9. Click **Save**.
10. In your Twilio account:
    1. Turn on the **Enable Custom Verification Code** option.
    2. Enable events for auditing Twilio Verify activity by following the steps in the Verify Events Onboarding Guide in the Twilio documentation. In the sink creation step, enter the following Ping URL in the **Destination** field: https://api.pingone.com/v1/environments/{environmentId}/notificationCallback/twilioVerify and select POST as the method.

> **Note**
>
> If you're in a Ping region other than North America, replace *api.pingone.com* in the URL with the relevant domain, as described in PingOne API domains in the PingOne developer documentation.

Copyright © 2025 Ping Identity Corporation

Next steps

After saving Twilio Verify as a notification sender, when you edit a notification template, the SMS section contains a list of all the Verify templates defined for the account. You can select the Verify template that you want to use for the notification. Learn more about configuring notification templates in Editing a notification template.

Using a Syniverse account with PingOne

If you have an existing Syniverse account, you can configure PingOne to use it for SMS and voice notifications.

Keep the following points in mind:

- **Billing:** You must set up your Syniverse billing arrangements before you can configure PingOne to use your account.
- **Multiple Syniverse accounts:** If you have more than one Syniverse account, you can only use one of them.
- **Inactive Syniverse Accounts:** It is the administrator's responsibility to delete a Syniverse account configuration in PingOne if the account becomes inactive. You can find information on deleting a Syniverse account from PingOne in Managing a Syniverse account in PingOne.

To configure a Syniverse account go to Configuring a Syniverse account for PingOne.

To manage a Syniverse account go to Managing a Syniverse account in PingOne.

Configuring a Syniverse account for PingOne

Use the information in this section to configure PingOne to use your Syniverse account.

Before you begin

Ensure that you have your Syniverse account Access Token. You can copy it as required from the Syniverse dashboard. You should also have set up one or more origination phone numbers.

About this task

> **Note**
> By enabling your Syniverse account, you are taking responsibility for dispatching SMS and voice messages.

Steps

1. Go to **Settings** > **Sender**.
2. Select **SMS/Voice**.
3. Select **Custom Server** to use the organization's Syniverse account.

   > **Warning**
   > Selecting **Custom Server** will result in deletion of a custom provider if one was defined.

4. In the **Syniverse Setup - Account** message, click **Setup**.

Copyright © 2025 Ping Identity Corporation

> **Note**
> A Syniverse account applies across all PingOne applications of the environment.

5. To configure your Syniverse account to work with PingOne:
    1. Copy the URL from the **Address** field.
    2. In your Syniverse account:
        1. In the **Delivery Configuration**, paste the URL that you copied from the PingOne **Address** field.
        2. Create 2 subscriptions: **SCG-Message** and **SCG-Voice-Calls**.

    See the Syniverse article How to setup a Webhook for Receiving Messages and Notifications for more information.

> **Note**
> These Syniverse configurations are required in order that Ping Identity's dashboards and reports will reflect complete and accurate data. Ping Identity will not be able to troubleshoot SMS or voice events related to Syniverse if these configurations are incomplete.

6. Copy/paste your Syniverse Access Token to the **Access Token** field.

> **Note**
> The system uses your access token to connect to your Syniverse account.
> Recommended: In your account in the Syniverse portal, define an application that is dedicated to PingOne traffic. Use this application for analyzing PingOne traffic throughput, and troubleshooting SMS or voice message despatch cases.

7. Click the **Verify Account** button. That validates the account to PingOne and populates the Origination Numbers list from your Syniverse account.

> **Note**
> - If the **Access Token** is incorrect, an `Invalid account information` error message will display.
> - If your Syniverse account is not fully configured a yellow exclamation mark appears next to the **Access Token** field. If you click on it, the `Syniverse Not Configured` warning message appears.
> - If there are no originating phone numbers in the Syniverse account, it will not be validated to PingOne.

If the account was successfully verified, the display will change to show a list of originating numbers from Syniverse.

8. In the **Syniverse Setup - Select Numbers** popup:
    1. Select at least one origination number to use.
        - Select the origination numbers to be used.
        - Click the **Show only selected**/**Show all** toggle to display only the marked phone numbers and hide the numbers that are not selected, or to display selected and unselected numbers.
        - Click **Select all** to select and mark all the origination numbers for this Twilio account.

Copyright © 2025 Ping Identity Corporation

- Click **Unselect all** to deselect and unmark all the origination numbers for this Twilio account.

> **Note**
>
> - If you intend to use both SMS and voice, all your selected numbers must support both SMS and voice.
> - Syniverse allows the use of sender IDs (in place of telephone numbers) for commercial use or to comply with regulations requiring SMSs to be sent as **transactional** and not **promotional**.
> - Sender IDs are displayed according to the Sender IDs sent in the API requests.

2. Select **Done** to continue with the configuration, or **Cancel**.

   Result:

   The **Origination Numbers** table displays.

3. For **Toll-free** and **Short code** numbers, you can configure supported **Countries** for notification recipients:

   - Click in the **Countries** field. The **Configure countries** popup opens.
   - Click in the **Select countries** field to display the list of countries. Select a country from the list.

> **Note**
>
> - **Toll-free**: You can add multiple countries in the **Select countries** list. If no country is specified, the specified toll-free number can only be used to dispatch notifications to United States recipient numbers.
> - **Short code**: You can select only one country in the **Select countries** list. If no country is specified, the specified short code can only be used to dispatch notifications to United States recipient numbers.

9. In **Fallback to Default Account**, select **Twilio** to use your Twilio account as a fallback if Syniverse becomes unavailable for reasons explained in the following note.

> **Note**
>
> **Under fallback:**
> If PingOne receives an error during the message dispatch process that the used number is invalid, it retries using another configured Syniverse number. After attempting to dispatch the message and receiving an error for all configured numbers, the fallback flow is triggered.
>
> - If there was no way of originating the SMS or voice event with the tenant's own Syniverse account and you defined a fallback, the event will be originated from the configured fallback account.
> - The following errors will cause fallback:
> - All API errors (but not SMS delivery errors).
> - No origination number was found on the Syniverse account.
> - If a transaction was charged to a specific account, it does not imply that subsequent transactions will be charged to the same account. The account charged for each transaction is determined on an individual basis. Preference is always given to the custom account.

- **Twilio**:

Copyright © 2025 Ping Identity Corporation

Enter the **Twilio Account SID**, **Auth Token** and select at least one **Origination Number**:

1. Copy/paste the Twilio account SID to the indicated field.

   > **Note**
   >
   > If the SID is shorter than 34 characters, an error message displays.

2. Copy/paste the Twilio **Auth Token** to the indicated field.
3. Click the **Verify Account** button. That validates the account to PingOne and populates the **Origination Numbers** list from your Twilio account.

   > **Note**
   >
   > - If the **Auth Token** is incorrect, an error message displays.
   > - If there are no originating phone numbers in the Twilio account, it will not be validated to PingOne.

   If the account is successfully verified, the display changes to show a list of originating numbers from Twilio.

4. Select at least one originating telephone number to use.

10. Click **Save**.
11. To complete the setup process, click **I Agree** on the **Third-party Service Consent** popup to confirm your legal consent.

> **Note**
>
> You will only be asked for legal consent when entering a new **Access Token**.

Managing a Syniverse account in PingOne

Use the information in this section to manage your Syniverse account.

About this task

Managing an account includes:

- Changing active originating numbers and fallback setting (as in Configuring a Syniverse account for PingOne)
- Changing to another account
- Deleting the custom account

Steps

1. Go to **Settings** > **Sender**.
2. Click the **SMS/Voice** tab.

   The custom Syniverse account configuration is displayed.

3. Select at least one originating telephone number to use.

Copyright © 2025 Ping Identity Corporation

4. You can change the **Fallback to Default Account** settings.
5. To switch to a different account, click **Change Account**. You will be offered the configuration window for a new account. Proceed as in Configuring a Syniverse account for PingOne.
6. To delete the active custom account, click the **Custom Provider** radio button.
7. To save your settings, click **Save**.

Using a custom provider account with PingOne

If you have an existing custom provider account that is not natively supported by PingOne (unlike Twilio and Syniverse that are natively supported), you can configure PingOne to use it for SMS and voice notifications.

When using a custom provider account with PingOne:

- **Billing**: You must set up your billing arrangements directly with your provider before you can dispatch notifications from your custom account with PingOne.

  > **Note**
  > PingOne does not provide SMS/Voice costs data for custom provider accounts.

- **Inactive Accounts**: It is the administrator's responsibility to delete a custom provider account configuration in PingOne if the account becomes inactive. See Managing a custom provider account in PingOne for deleting a custom account from PingOne.

To configure a custom provider account go to Configuring a custom notification provider for PingOne. See also tutorials for more specific use cases:

- Use Case: Configuring Telesign as a provider with PingOne.
- Use Case: Configuring Burst SMS as a provider with PingOne.
- Using a Twilio account with PingOne to support Twilio Studio flows.

To manage a custom provider account go to Managing a custom provider account in PingOne.

Configuring a custom notification provider for PingOne

Use the information in this section to configure PingOne to use a custom notification provider.

> **Note**
> You can define up to three custom notification providers. When defining more than one custom provider, keep in mind that the first provider on the **SMS/Voice** tab is the one that will be used to send notifications unless you specify one of the other providers in the notification policy you are using.

Steps

1. Go to **Settings** > **Sender**.
2. Click the **SMS/Voice** tab.

Copyright © 2025 Ping Identity Corporation

3. Select **Custom Provider** to use your organization's provider account.
4. **Provider Name**: Enter the name of your provider account.
5. From **Authorization**:

   Choose from:

   - **Basic**

     1. **User Name**: Enter the username for your custom provider account.
     2. **Password**: Enter the password for your custom provider account.

     > **Note**
     > When editing an existing configuration, you can click **Change Account** to enter a new password for the custom provider account.

   - **Bearer**: In **Token**, enter the token for your custom provider account.

6. **Origination**: Click **+ Add Sender Phone Number** to configure a sender phone number, and for each number entered, select the following:

   1. **Type**: Select the type of phone number

      - **Standard**: The sender **Number** must conform to the valid format of a full international phone number.
      - **Toll-free**: The sender **Number** should be a valid toll-free phone number (US only). It is the customer's responsibility to confirm that the number is toll-free.
      - **Short code**: The sender **Number** must conform to the valid format of a short code phone number (US only). It is the customer's responsibility to confirm that the number is a short code.

   2. **Countries**:

      For **Toll-free** and **Short code** numbers, you can configure supported **Countries** for notification recipients:

      - Click in the **Countries** field. The **Configure countries** popup opens.
      - Click in the **Select countries** field to display the list of countries. Select a country from the list.

      > **Note**
      > - **Toll-free**: You can add multiple countries in the **Select countries** list. If no country is specified, the specified toll-free number can only be used to dispatch notifications to United States recipient numbers.
      > - **Short code**: You can select only one country in the **Select countries** list. If no country is specified, the specified short code can only be used to dispatch notifications to United States recipient numbers.

   3. **Voice**: Mark the checkbox to configure the number to dispatch voice notifications.
   4. **SMS**: Mark the checkbox to configure the number to dispatch SMS notifications.

   Repeat this step to configure additional sender phone numbers.

Copyright © 2025 Ping Identity Corporation

7. **SMS**:

   To use a different custom provider to send SMS messages, configure this section.

   1. **Type**: Choose the type of operation to issue SMS notification requests to the associated vendor **URL** endpoint.
      - **POST** (default)
      - **GET**
   2. **URL**: The vendor endpoint that will receive SMS notification requests using the corresponding operation and request body.
   3. **Body** (optional): The request body format style for configuration maintenance.
      - **None**: The vendor endpoint receives SMS notification requests without a request body.
      - **Form**: The notification request body is in the form of key and value pairs. Click **+ Add Key, Value** for each new key and value pair that you want to enter.
      - **Raw**: Enter the notification request as free-form JSON text.

      > **Caution**
      > Changing the request body format style from **Form** deletes the request body's key and value pairs, and changing the format style from **Raw** deletes the request body's free-form JSON text.

      The customized body should include the variables: `"${from}"`, `"${to}"`, and `"${message}"`. Depending on vendor requirements, the `"${from}"` variable might be optional.

      The body can include:

      - ${locale} - locale
      - ${otp} - OTP

        You can also use dynamic variables in the Body section. For more information, see Dynamic variables in the PingOne Platform API Reference.
   4. **Headers**: Enter headers for the SMS notification request. Click **+ Add Header** for each new header you want to add. The header style assumes the same format style (key and value pair, or free text) according to the format you selected for the request body.
      - For JSON body format, set the header to `content-type=application/json`.
      - For x-www-form-urlencoded body format, set the header to `content-type=application/x-www-form-urlencoded`.
   5. **Plus sign**:
      - **Enabled** (default): Permit the standard number format for the sender and recipient numbers, including a leading plus sign.
      - **Disabled**: For configurations where the provider requires the sender and recipient numbers without a leading plus sign.
   6. Click **Send Test SMS** to check your configuration.

Copyright © 2025 Ping Identity Corporation

The **Send Test SMS** popup opens. Enter a destination phone number to test receiving an SMS notification from your configured custom provider.

1. In the **Send To** field, select the phone number's country, and enter the destination phone number.
2. Click **Send**.

   The **Send Test SMS** popup closes.
3. Verify that you've received a test notification on the destination phone.

8. **Voice**:

To use a different custom provider to send voice messages, configure this section.

1. **Type**: Choose the type of operation to issue voice notification requests to the associated **URL** endpoint.
   - **POST**
   - **GET**
2. **URL**: The vendor endpoint that will receive voice notification requests using the corresponding operation and request body.
3. **Body**: The request body format style for configuration maintenance.
   - **None**: The vendor endpoint receives voice notification requests without a request body.
   - **Form**: The notification request body is in the form of key and value pairs. Click **+ Add Key, Value** for each new key and value pair that you want to enter.
   - **Raw**: Enter the notification request as free-form JSON text.

   > **Caution**
   >
   > Changing the request body format style from **Form** deletes the request body's key and value pairs, and changing the format style from **Raw** deletes the request body's free-form JSON text.

   The customized body should include the variables: `"${from}"`, `"${to}"`, and `"${message}"`. Depending on vendor requirements, the `"${from}"` variable might be optional.

   In addition, the body can include the following optional variables:

   - ${voice} - the type of voice configured for notifications
   - ${locale} - locale
   - ${otp} - OTP
   - ${user.user.name} - user's username
   - ${user.name.given} - user's given name
   - ${user.name.family} - user's family name

   You can also use dynamic variables in the Body section. For more information, see Dynamic variables in the PingOne Platform API Reference.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> The `< repeatMessage>` and `<pause1sec>` tags are not supported for custom provider voice OTP messages. To add a pause in a custom provider voice message, use the **Preceding padding** (`"beforeTag"`) and **Succeeding padding** (`"afterTag"`) parameters, for example:

4. **Preceding padding**: Set a custom pause or padding before an OTP character, to leverage vendor capabilities when sending voice notifications. For example:

```
"beforeTag":"<Say>",
```

5. **Succeeding padding**: Set a custom pause or padding after an OTP character, to leverage vendor capabilities when sending voice notifications. For example:

```
"afterTag":"</Say> <Pause length=\"1\"/>"
```

6. **Headers**: Enter headers for the voice notification request. Click **+ Add Header** for each new header you want to add. The header style assumes the same format style (key and value pair, or free text) according to the format you selected for the request body.
   - For JSON body format, set the header to `content-type=application/json`.
   - For x-www-form-urlencoded body format, set the header to `content-type=application/x-www-form-urlencoded`.
7. **Plus sign**:
   - **Enabled** (default): Permit the standard number format for the sender and recipient numbers, including a leading plus sign.
   - **Disabled**: For configurations where the provider requires the sender and recipient numbers without a leading plus sign.
8. Click **Send Test Voice** to check your configuration.

   The **Send Test Voice** popup opens. Enter a destination phone number to test receiving a voice notification from your configured custom provider.

   1. In the **Send To** field, select the phone number's country, and enter the destination phone number.
   2. Click **Send**.

      The **Send Test SMS** popup closes.
   3. Verify that you've received a test notification on the destination phone.
9. Click **Save**.

> **Warning**
>
> If you previously configured a **Custom Server**, the settings are deleted when you save the custom provider settings.

Copyright © 2025 Ping Identity Corporation

10. To define additional custom providers, click **Add Provider**.

Use Case: Configuring Telesign as a provider with PingOne

About this task

Add Telesign as your organization's provider account.

Steps

1. Go to **Settings** > **Sender**.
2. Select **SMS/Voice**.
3. Select **Custom Provider**.

> **Warning**
> Selecting **Custom Provider** deletes any existing custom server configuration.

4. **Provider Name**: Enter a meaningful name for your Telesign provider account.
5. **Authorization**: Select **Basic** and then enter the following:
    1. **User Name**: Enter the Client ID for your Telesign provider account.
    2. **Password**: Enter the API key for your Telesign provider account.

    > **Note**
    > When editing an existing configuration, you can click **Change Account** to enter a new password for the custom provider account.

6. **SMS**:

   To use Telesign to send SMS messages, configure this section.

    1. **Type**: Select the **POST** operation to issue SMS notification requests to the associated vendor **URL** endpoint.
    2. **URL**: Enter the following URL `https://rest-api.telesign.com/v1/messaging`
    3. **Body**: The request body format style for configuration maintenance. In the list select **Form** and then add the following key and value pairs. Click **+ Add Key, Value** for each additional entry.

Key	Value
message_type	ARN
message	${message}
phone_number	${to}

Copyright © 2025 Ping Identity Corporation

> **Caution**
>
> Changing the the request body's format style from **Form** deletes the request body's key and value pairs, and changing the format style from **Raw** deletes the request body's free-form JSON text.

4. **Headers**: The Telesign header for the SMS notification requests is added by default.
5. **Plus sign**: Select **Enabled** to enable the standard number format for the sender and recipient numbers, including a leading plus sign.

7. **Voice**:

To use Telesign to send voice messages, configure this section.

1. **Type**: Select the **POST** operation to issue voice notification requests to the associated vendor **URL** endpoint.
2. **URL**: Enter the following URL `https://rest-api.telesign.com/v1/voice`
3. **Body**: The request body format style for configuration maintenance. In the list select **Form** and then add the following key and value pairs: Click **+ Add Key, Value** for each additional entry.

Key	Value
message_type	ARN
message	${message}
phone_number	${to}

> **Caution**
>
> Changing the the request body's format style from **Form** deletes the request body's key and value pairs, and changing the format style from **Raw** deletes the request body's free-form JSON text.

4. **Preceding padding**: Set a custom pause or padding before an OTP character, to leverage Telesign vendor capabilities when sending voice notifications. For example:

```
"beforeTag":"<Say>",
```

5. **Succeeding padding**: Set a custom pause or padding after an OTP character, to Telesign vendor capabilities when sending voice notifications. For example:

```
"afterTag":"</Say> <Pause length=\"1\"/>"
```

6. **Headers**: The Telesign header for the SMS notification requests is added by default.
7. **Plus sign**: Select **Disabled** to ensure a leading plus sign is not added to the sender and recipient numbers.

Copyright © 2025 Ping Identity Corporation

> **Note**
> Telesign does not support the use of a leading "+" in phone numbers for voice notifications.

8. Click **Save**.
9. Check your configuration:
    1. To check SMS configuration, in the **SMS** area, click **Send Test SMS** and in the popup window enter a destination phone number to test receiving an SMS notification from Telesign, and then click **Send**. A test SMS notification should be received on the destination phone.
    2. To check Voice configuration, in the **Voice** area, click **Send Test Voice** and in the popup window enter a destination phone number to send a Voice notification from Telesign, and then click **Send**. A test voice notification should be received on the destination phone.

Use Case: Configuring Burst SMS as a provider with PingOne

Add Burst SMS as your organization's provider account to send SMS notification messages.

About this task

To add Burst SMS as your organization's provider account:

Steps

1. Go to **Settings** > **Sender**.
2. Select **SMS/Voice**.
3. Select **Custom Provider**.

> **Warning**
> Selecting **Custom Server** deletes any existing custom provider configuration, if one exists.

4. **Provider Name**: Enter a meaningful name for your Burst SMS provider account.
5. **Authorization**: Select **Basic** and then enter
    1. **User Name**: Enter the username for your Burst SMS provider account.
    2. **Password**: Enter the password for your Burst SMS provider account.

    > **Note**
    > When editing an existing configuration, you can click **Change Account** to enter a new password for the custom provider account.

6. **Origination Number**: Click **+ Add Sender Phone Number** to configure a sender phone number. A new row is added. Enter the following information:
    1. **Sender Phone Number**: Enter the phone number that sends the notification. You can leverage shortcodes and toll-free numbers for increased throughput for US numbers.

Copyright © 2025 Ping Identity Corporation

2. **Phone Number Type**: Enter the type of phone number you are using:
   - **Standard**: The **Sender Phone Number** must conform to the valid format of a full international phone number.
   - **Toll-free**: The **Sender Phone Number** should be a valid toll-free phone number (US only). It is the customer's responsibility to confirm that the number is toll-free.
   - **Short code**: The **Sender Phone Number** must conform to the valid format of a short code phone number (US only). It is the customer's responsibility to confirm that the number is a short code.
3. Select the SMS checkbox to use the number for SMS call.

Repeat this step to configure additional sender phone numbers.

7. **SMS**:

   To use Burst SMS to send SMS messages, configure this section.

   1. **Type**: Select the **GET** operation to issue SMS notification requests to the associated vendor **URL** endpoint.
   2. **URL**: Enter the following URL: `https://api.transmitsms.com/send-sms.json?to=${to}&from={from}&message=${message}`
   3. **Plus sign**: Select **Enabled** to enable the standard number format for the sender and recipient numbers, including a leading plus sign.
8. Click **Save**.
9. To check SMS configuration, in the **SMS** area, click **Send Test SMS** and, in the modal, enter a destination phone number to test receiving an SMS notification from Burst SMS, and then click **Send**. A test SMS notification should be received on the destination phone.

Using a Twilio account with PingOne to support Twilio Studio flows

To use Twilio studio flows, configure Twilio as a custom provider and then define the specific flows that you want to use. You'll also need to configure the relevant PingOne notifications for use with the relevant Twilio flow.

Steps

1. Go to **Settings** > **Sender**.
2. Select **SMS/Voice**.
3. Select **Custom Provider**.

   > **Warning**
   > Selecting **Custom Provider** deletes any existing custom server configuration, if one exists.

4. **Provider Name**: Enter a meaningful name for your Twilio provider account.
5. **Authorization**: Select **Basic** and then enter
   1. **User Name**: Enter the Twilio Studio account `sid` as your username.

Copyright © 2025 Ping Identity Corporation

2. **Password**: Enter the Twilio Studio account token as your password.

> **Note**
> When editing an existing configuration, you can click **Change Account** to enter a new password for the custom provider account.

6. **Origination**: Click **+ Add Sender Phone Number** to configure a sender phone number, and for each number entered, select the following:

   1. **Type**: Select the type of phone number

      - **Standard**: The sender **Number** must conform to the valid format of a full international phone number.
      - **Toll-free**: The sender **Number** should be a valid toll-free phone number (US only). It is the customer's responsibility to confirm that the number is toll-free.
      - **Short code**: The sender **Number** must conform to the valid format of a short code phone number (US only). It is the customer's responsibility to confirm that the number is a short code.

   2. Select at least one of the **SMS** or **Voice** checkboxes to define which device type is directed to the studio flow.

   > **Note**
   > The studio flow defines the actual method that will be used to send the OTP (SMS, Voice, or other).

7. **SMS**:

   To direct SMS devices to the Twilio Studio flow, configure this section.

   1. **Type**: Select the **POST** operation to issue a POST request to the Twilio REST API.
   2. **URL**: Enter the full URL for the Twilio Studio flow you want to use: `https://studio.twilio.com/v2/Flows/<flowID>/Executions`
   3. **Body**: The request body format style for configuration maintenance. In the list, select **Form** and then add the following key and value pairs. Click **+ Add Key, Value** for each additional entry.

Key	Value
From	${from}
to	${to}
Parameter	${message} **Note** This takes the notification value defined in **Experiences → Notifications**. The message text is defined in the last step of this procedure.

Copyright © 2025 Ping Identity Corporation

> **Caution**
>
> When saving, be aware that changing the request body's format style from **Form** deletes the request body's key and value pairs, and changing the format style from **Raw** deletes the request body's free-form JSON text.

8. **Voice**:

   To use Twilio studio to send voice messages, configure this section.

   1. **Type**: Select the **POST** operation to issue voice notification requests to the associated vendor **URL** endpoint.
   2. **URL**: Enter the following URL, including the flow ID for the Voice communication flow from Twilio studio: `https://studio.twilio.com/v2/Flows/<flowID>/Executions`
   3. **Body**: The request body format style for configuration maintenance. In the list select **Form** and then add the following key and value pairs. Click **+ Add Key, Value** for each additional entry.

Key	Value
From	${from}
To	${to}
Parameters	${message} **Note** This takes the notification value defined in **Experiences → Notifications**. The message text is defined in the last step of this procedure.

> **Caution**
>
> When saving, be aware that changing the request body's format style from **Form** deletes the request body's key and value pairs, and changing the format style from **Raw** deletes the request body's free-form JSON text.

9. Click **Save**.
10. Go to **User Experience** > **Notification Templates** and for each notification type that you want to use with Twilio Studio:

    1. Right-click the**More options** icon and select **Edit**.
    2. In the **New Message** field for the relevant authentication method, enter `\{"OTP":${otp}}`

    > **Note**
    >
    > You can include additional parameters, such as username in the message. For example:
    >
    > ```
    > {"OTP":${otp}, "username":${username}}
    > ```

Copyright © 2025 Ping Identity Corporation

You can also use dynamic variables in the Body section. For more information, see Dynamic variables in the PingOne Platform API Reference.

11. Check your configuration:
    - To check SMS configuration, in the **SMS** area, click **Send Test SMS** and in the modal, enter a destination phone number to test receiving an SMS notification from Telesign, and then click **Send**. A test SMS notification should be received on the destination phone.
    - To check Voice configuration, in the **Voice** area, click **Send Test Voice** and in the modal, enter a destination phone number to send a Voice notification from Telesign, and then click **Send**. A test voice notification should be received on the destination phone.

Managing a custom provider account in PingOne

Use the information in this section to manage your custom provider.

About this task

Managing a custom notification provider account includes:

- Changing the account, active sender phone numbers, and notification request format, body, and headers. Learn more in Configuring a custom notification provider for PingOne
- Deleting the custom account

Steps

1. Go to **Settings** > **Sender**.
2. Click the **SMS/Voice** tab.

   The custom provider account's configuration is displayed.
3. You can change to a different provider account.
4. You can update, delete or add sender phone numbers.
5. You can change the notification request format, body and headers.
6. To delete the active custom account, click the **Custom Server** radio button.

   You are prompted to confirm that your custom provider settings will be lost if you change the type of sender.
7. To save your settings, click **Save**.

Sender IDs per country

Sender IDs is either a custom alphanumeric name (such as a company name), or numeric code, (such as a specific mobile phone number) that is displayed in the **From** field of SMS notifications sent by PingID server on behalf of your organization.

The Sender ID helps recipients to identify an SMS message as genuine, as it helps users recognize the sender and their brand. It is particularly useful when sending messages that don't require a response. When registered, sender IDs can also help prevent impersonation by scammers.

Copyright © 2025 Ping Identity Corporation

International regulations require all alphanumeric SenderIDs to be registered by country. These regulations dictate that SMSs sent by unregistered Sender IDs must be blocked.

The following table lists the countries in which Ping Identity has a registered SenderID use with Strong Authentication solutions (PingID and PingOne MFA).

Country	Registered SenderID (Vonage)	Registered SenderID (Twilio)
Afghanistan	-	Mobile Code
Armenia	-	PINGIDENTIT
Australia	PingCode	Ping Code
Bangladesh	Ping Code	Ping Code
Belarus	-	Ping Code
Benin	Ping Code	Mobile Code
Brazil	-	PING CODE
Cambodia	Ping Code	Mobile Code
Cameroon	-	Mobile Code
Congo	-	Mobile Code
Czech Republic	-	Ping Code
China	Mobile Code	-
East Timor	-	Ping Code
Egypt	Mobile Code	Ping Code
Ethiopia	Ping Code	Ping Code
Ghana	Ping Code	Mobile Code
Guinea	-	Mobile Code
Guinea-Bissau	Ping Code	Mobile Code
Hong Kong	-	Mobile Code
Indonesia	PingCode	Ping Code
Ivory Coast	-	Mobile Code

Copyright © 2025 Ping Identity Corporation

Country	Registered SenderID (Vonage)	Registered SenderID (Twilio)
Jordan	Ping Code	Ping Code
Kenya	Ping Code	-
Kuwait	Mobile Code	Ping Code
Liberia	Ping Code	Ping Code
Mexico	MobileCode	MobileCode
Morocco	Ping Code	MobileCode
Nigeria	-	Mobile Code
Oman	Ping Code	Ping Code
Philippines	-	PINGIDENTIT
Pakistan	Mobile Code	-
Qatar	Ping Code	Ping Code
Russia	Ping_Code	PingCode
Rwanda	-	Mobile Code
Saudi Arabia	Ping Code	Ping Code
Serbia	PingCode	-
Singapore	Ping Code	Ping Code
South Sudan	-	Mobile Code
Sri Lanka	Mobile Code	Ping Code
Sudan	-	Mobile Code
Swaziland	-	Mobile Code
Thailand	-	Ping Code
Turkey	Mobile Code	PingID
Uganda	-	Mobile Code
United Arab Emirates	Mobile Code	PingID

Copyright © 2025 Ping Identity Corporation

Country	Registered SenderID (Vonage)	Registered SenderID (Twilio)
Venezuela	Mobile Code	Ping Code
Vietnam	PINGIDENTIT	PINGIDENTIT
Zambia	-	Mobile Code

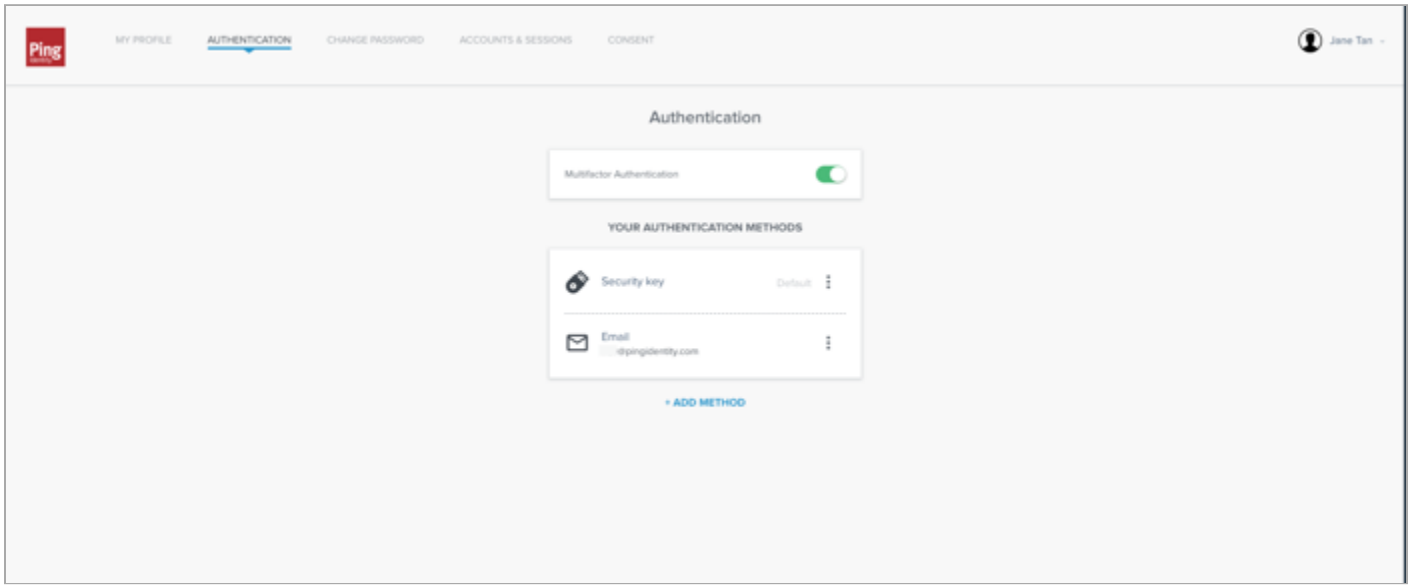
Copyright © 2025 Ping Identity Corporation

Managing your PingOne user profile

The PingOne self-service portal enables administrators and end users to manage their profile without contacting customer service.

This section is intended to introduce the functions available for the out-of-the-box PingOne user profile page and is intended for the following audiences:

- PingOne administrators: Learn how to manage your own account.
- PingOne administrators managing PingOne end users: Understand how your users can make use of the self-service options and use this guide as a basis for creating a guide for your own end users.



The options displayed in the PingOne user profile are identical for both administrators and end users, but they can be implemented differently to fit your use cases.

From the PingOne self-service page, users can:

- Update their profile
- Add or remove authentication methods
- Change their password
- View linked accounts, sessions, and consents

Administrators can view the same tabs on the profile page. Some options might not be relevant when managing their own account, such as linked profiles and consents.

> **Note**
>
> You should create and maintain separate PingOne environments for your administrators and your end users so that you can maintain multi-factor authentication (MFA) configurations, branding, and policies appropriate to each environment.

Copyright © 2025 Ping Identity Corporation

Administrators: Managing your PingOne environment

You can manage the multi-factor authentication (MFA) methods for your PingOne account, and change your password, if needed.

About this task

Each PingOne environment has three unique URLs:

URL	Purpose	Format
Console URL	URL to sign on to the console for administrators of one or more environments, depending on the permissions defined for the admin's role.	https://console.pingone.*<region>*/?env=*<environmentID>*
Self-service Url	URL for PingOne end users to access self-service functionality, such as changing a password, pairing a device, or editing their profile.	https://apps.pingone.*<region>*/*<environmentID>*/myaccount/
Application Portal Url	URL for end users to access their application portal.	https://apps.pingone.*<region>*/*<environmentID>*/myapps/

> **Tip**
>
> You can view these URLs from your PingOne account (**Settings → Environment Properties**). Make a note of them when you sign on for the first time.

You can edit your profile, change your password, and manage your MFA methods. The appearance of your PingOne profile page is the same as the UI available to your end users, however, some of the options listed are not applicable to an administrator account, such as linked account consents.

Steps

- To access your admin self-service profile, sign on to the PingOne admin console, and in the **Avatar** menu select one of the following.

  Choose from:

  - Profile: Go to the **Profile** tab to update your contact details including phone number, email address, and physical address.

    > **Note**
    >
    > To enable single sign-on (SSO) to Support from the **My Support Cases** option on the **Avatar** menu, you must have a verified email address in your profile. Your profile must also include you **First Name** and **Last Name**.

  - My MFA methods: Go to the **Authentication** tab to add one or more authentication method to securely sign on to your account or app.

Copyright © 2025 Ping Identity Corporation

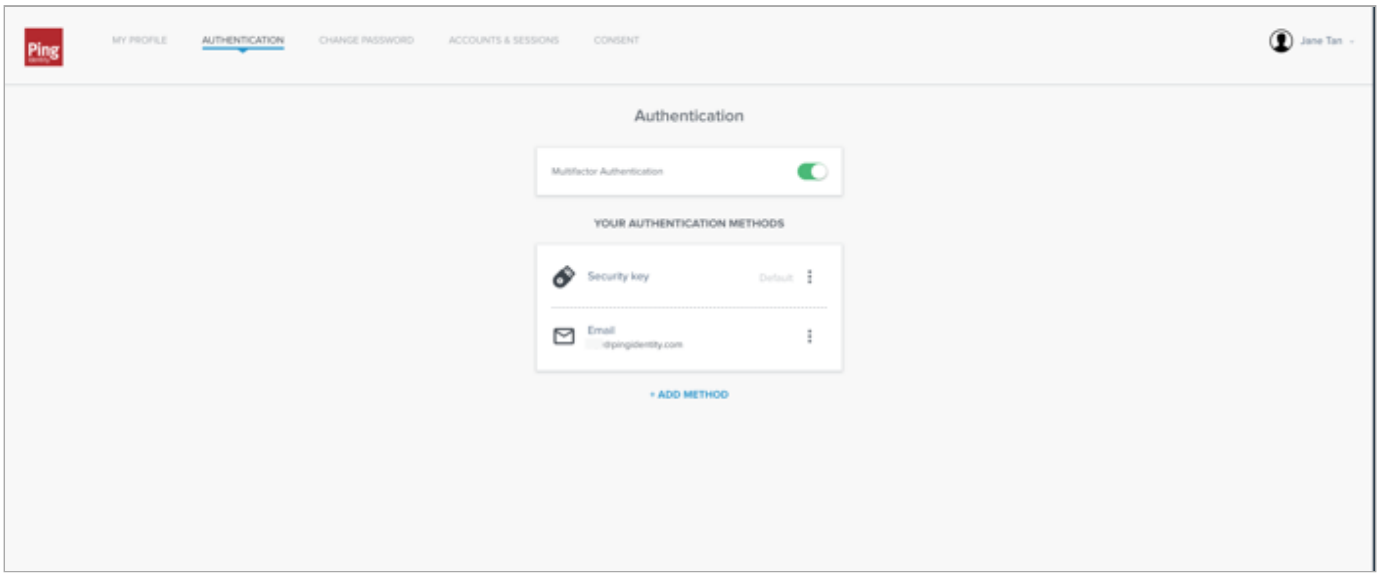
> **Note**
>
> Access to the PingOne admin console requires at least one registered MFA method. Supported methods include email, authenticator app (TOTP), and FIDO2. Learn more in Configuring administrator security.

- Change password: Go to the **Change Password** tab to change your own password.

> **Note**
>
> You can also access your profile using the self-service URL or from the **Avatar** menu in the application portal.

Result:

Your profile opens, showing the following tabs.



End users: Accessing your PingOne profile

Access the PingOne self-service portal to update your personal information, change your password, add MFA, view your accounts and sessions, and manage consents.

About this task

This section is intended for PingOne administrators to understand the options available to your end users when they access their self-service profile. Options available vary according to your configuration needs. The PingOne self-service portal enables your end users to:

- Edit their own profile
- Change their own profile
- Add or modify the mutli-factor authentication (MFA) methods from those defined by the admin
- View external accounts linked to their PingOne profile

Copyright © 2025 Ping Identity Corporation

- View any agreements for which they have given consent

The way an end user accesses their profile varies and can include:

> **Note**
>
> You should create and maintain separate PingOne environments for your administrators and your end users, so you can maintain MFA configurations, branding and policies appropriate to each environment.

Steps

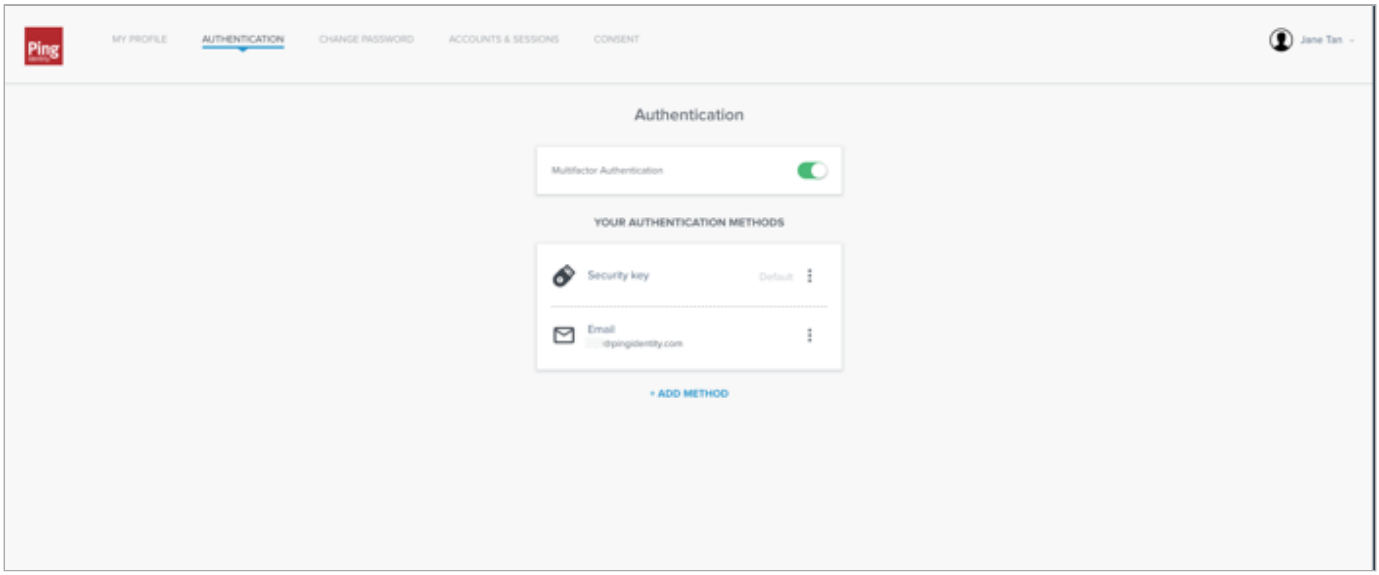
- Access your profile based on your use case:

  Choose from:

  - To access your profile using the self-service URL: In a web browser, enter the self-service URL you received from your organization.
  - For customer use cases: In your application, tap the relevant option.
  - For workforce use cases: From the application portal, in the **Avatar** menu, select **Devices**.

    Result:

    Your profile opens, showing the following tabs.



  - My profile: Update your contact details including phone number, email address, and physical address.
  - Authentication: Add one or more authentication method to securely sign on to your account or app.
  - Change password: Change your password yourself.
  - Accounts & sessions: View and manage linked accounts and open sessions.
  - Consents: View any agreements to which you have consented.

Copyright © 2025 Ping Identity Corporation

Editing your profile

Access your PingOne user profile to update your contact details and location information.

Before you begin

To access your PingOne profile, you'll need your PingOne self-service portal URL and password.

About this task

The out-of-the-box profile includes the user's basic contact and location information by default.

Steps

1. Go to your profile, click the **My Profile** tab, and then click **Edit Profile**.
2. Edit your details.

   The fields that appear are defined by your organization and might include:

   - **Contact** details: Your name, phone number, mobile number, and email address.

     > **Note**
     >
     > Administrators only: To enable SSO to Support from the **My Support Cases** option on the **Avatar** menu, you must have a verified email address in your profile. Your profile must also include your **First Name** and **Last Name**.

   - **Location**: Your physical location, including street name, city, state, and zip code.
3. Click **Save**.

   Result:

   The PingOne directory is updated with your changes.

Managing authentication methods

From your PingOne user profile you can add, rename, or delete one or more authentication methods. You can also define your default authentication method.

Before you begin

To enable users with more than one authentication method to define a default multi-factor authentication (MFA) method, you must enable the `User-selected default` option. See Configuring MFA settings.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> A user might not be able to use their default device for various reasons, such as:
>
> - If a user tries to authenticate from a mobile device and device authorization is allowed, then the device authorization occurs.
> - If a user has a FIDO device with an active session, this device is used to authenticate the user even if the user changes their default device.
> - If policy rules disallow the default device.

About this task

You can add different devices, such as a security key or phone biometrics for authentication. You can also add multiple authentication methods that use the same physical device. For example, you could set up MFA using SMS, voice, FIDO2 biometrics, and an authenticator app on a single mobile device. The devices available are defined by your organization.

> **Note**
>
> You should add at least two MFA methods. The methods listed are defined by your administrator, and might vary between environments.

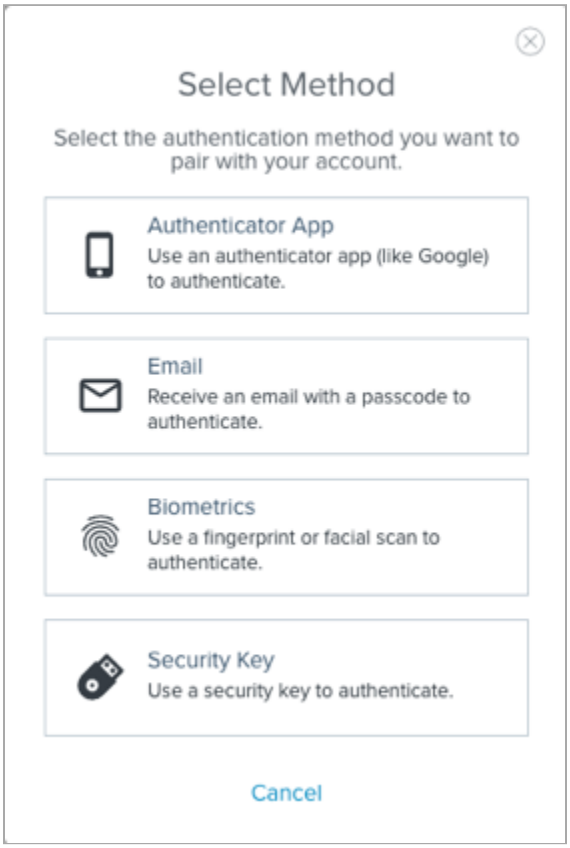
Steps

1. Go to your profile, click the **My Profile** tab, and then click the **Authentication** tab.
2. Click **Add Method**.

   Result:

   The **Select Method** window opens, listing the methods available for you to add.

Copyright © 2025 Ping Identity Corporation

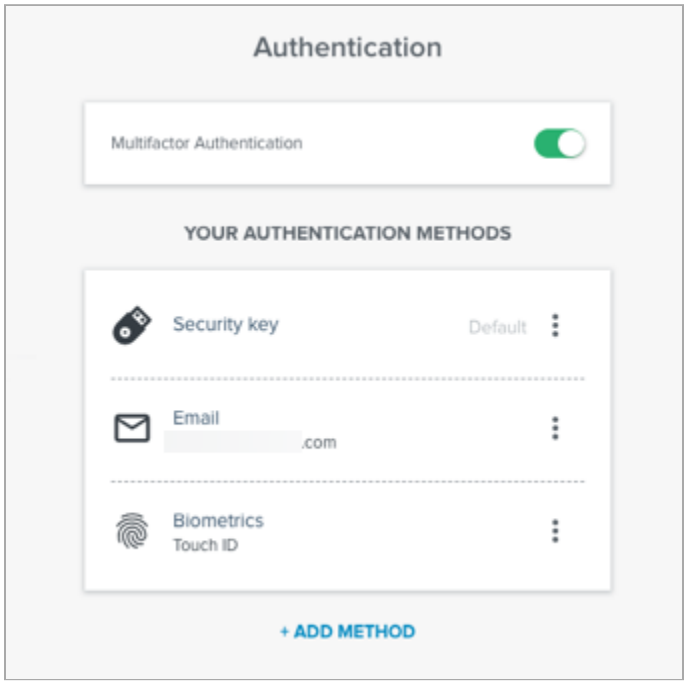


3. Select the authentication method you want to add and follow the instructions to pair that authentication method:
   - **Authenticator app**: Use a third-party authenticator application, such as Google Authenticator. Open the authenticator application and scan the QR code or enter the passcode. Click **Next**. Enter the passcode from the authenticator application to complete the device pairing.
   - **Text message**: Use a text message (SMS) with a one-time passcode (OTP) to authenticate. Enter the phone number and click **Next**. Enter the passcode you received to complete the device pairing.
   - **Voice**: Receive a voice call with a one-time passcode to authenticate. Enter the phone number and click **Next**. Enter the passcode you received to complete the device pairing.
   - **Email**: Use an email message with a one-time passcode to authenticate. Enter an email address and click **Next**. Enter the passcode you received to complete the device pairing.
   - **Mobile**: Use an application on your mobile device to authenticate. Select the mobile app for pairing your mobile device. Scan or enter the pairing key in the mobile app.
   - **FIDO2 biometrics**: Use FIDO2 biometrics on compatible devices to authenticate. On your device, sign on or enter your password to complete pairing.
   - **Security key**: Use a FIDO2 or U2F security key to authenticate. You will be prompted to authenticate with the security key.

   Result:

   The authentication method is listed on the **Authentication** tab in the **Your Authentication Methods** section. Repeat this step to add another authentication method, if required.

Copyright © 2025 Ping Identity Corporation



4. After adding an authentication method, you can optionally do the following:

Option	Description
Set a default authentication method	If you added more than one MFA method, to define your default method, click the hamburger menu next to the relevant MFA method and then click**Set As Default**. **Note** The devices available for authentication depend on your company policy, therefore your default device might not always be available for authentication.
Rename an authentication method	Click the hamburger menu next to the authentication method you want to set as default, and then click **Edit Name**. Enter a meaningful name for the authentication method, and click the checkmark. Names of up to 100 characters are supported.
Remove an authentication method	Click the hamburger menu next to the authentication method you want to remove, and then click **Remove**. **Important** Ensure that you leave at least one authentication method. If you remove all authentication methods, you might lock yourself out of the application.

Copyright © 2025 Ping Identity Corporation

Completing the administrator account registration

When you receive an email indicating that you were added as an administrator in PingOne, verify your email address and update your password to complete the registration process.

Before you begin

You should have received the following information from the PingOne administrator who added you as an administrator:

- Your PingOne user name if it is different from your email address.
- The **Console Login URL** for the environment that you are being added to.
- (Optional) A temporary password.

Steps

1. Go to the PingOne console using the URL you received from the administrator.
2. Enter your PingOne **Username**.
3. Update your **Password**.

   Choose from:

   - If you received a temporary password, enter it and create a new password when prompted.
   - Click **Forgot Password**, enter your PingOne username on the **Password Reset** window, and click **Submit**.

     An email containing a recovery code is sent to the email address associated with your PingOne user account. Paste the code where indicated on the **Enter New Password** window. Create a new password and click **Save**.

     Result:

   You are signed on to the PingOne administrator console.
4. On **Verify Email Address**, click **Verify**.

   Result:

   A new verification code is sent to your email address.
5. Paste the verification code where indicated and click **Confirm**.

Result

Your administrator account registration is complete.

Administrators: Verifying your own email address

Administrators must verify their own email address in PingOne.

About this task

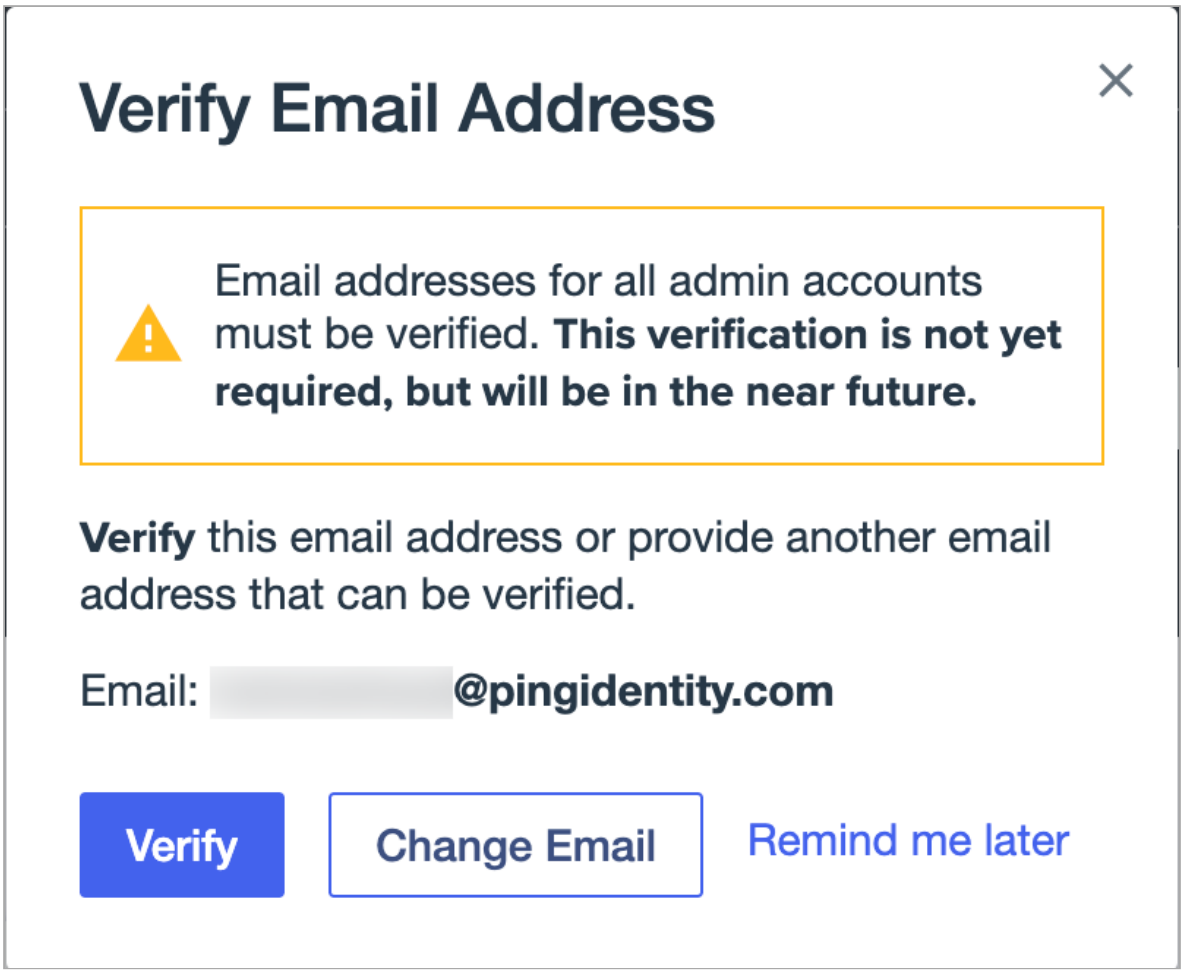
Copyright © 2025 Ping Identity Corporation

As an administrator, you should verify your email address using the PingOne admin console, but you can also use the PingOne self-service application to verify your email address. See End users: Verifying an email address.

To verify your email address with the admin console:

Steps

1. In PingOne, in the **Verify Email Address** popup window, click **Verify**.



Result:

PingOne sends a verification code to your email address.

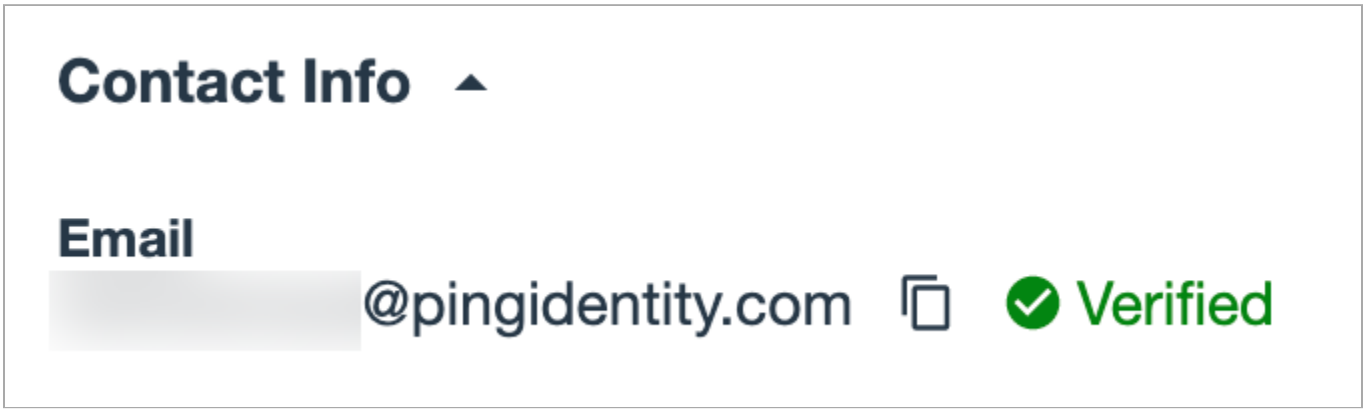
2. Go to the email from PingOne, copy the eight-digit verification code, and paste it into the **Verification Code** field.

> **Note**
> If you didn't receive an email or need to resend the code for any reason, click **Request Again**.

Result

Under your contact information, your email appears as verified. If you change your email address in your profile, you must verify it again.

Copyright © 2025 Ping Identity Corporation



End users: Verifying an email address

In certain situations, end users might be able to verify their own email address using the PingOne self-service application.

About this task

You might be required to verify your email address if you change your email address in your profile or if your administrator requires it.

To verify an email address as an end user:

Steps

1. Sign on to the PingOne self-service application.

   See End users: Accessing your PingOne profile.

2. Do one of the following:

   - If you have already received the verification email, then paste or enter the verification code.
   - If you haven't received the verification email, click **Verify** in the yellow banner. Go to your email application and locate the email from PingOne. Copy the eight-digit verification code, then paste or enter the code.

     > **Note**
     > If you don't see the yellow banner, you don't need to verify your email address.
     > If you didn't receive an email, or need to resend the code for any reason, click **Resend code**.

3. Click **Verify**.

Result

Under your contact information, your email shows as verified. If you change your email address in your profile, you must verify it again.

Changing your password

If you forget your password or want to change it, you can change it yourself from your PingOne profile.

Copyright © 2025 Ping Identity Corporation

Before you begin

To access your PingOne user profile, you'll need your PingOne environment URL and password.

> **Tip**
> You can also access yourPingOne user profile using the self-service URL for your environment.

Steps

1. Go to your profile, click the **My Profile** tab, and then click **Change Password**.
2. Enter the following information:
    - **Current password**
    - **New password**
    - **Confirm new password**
3. Click **Save**.

Managing accounts and sessions

View and manage accounts linked to your profile, and any open sessions.

Before you begin

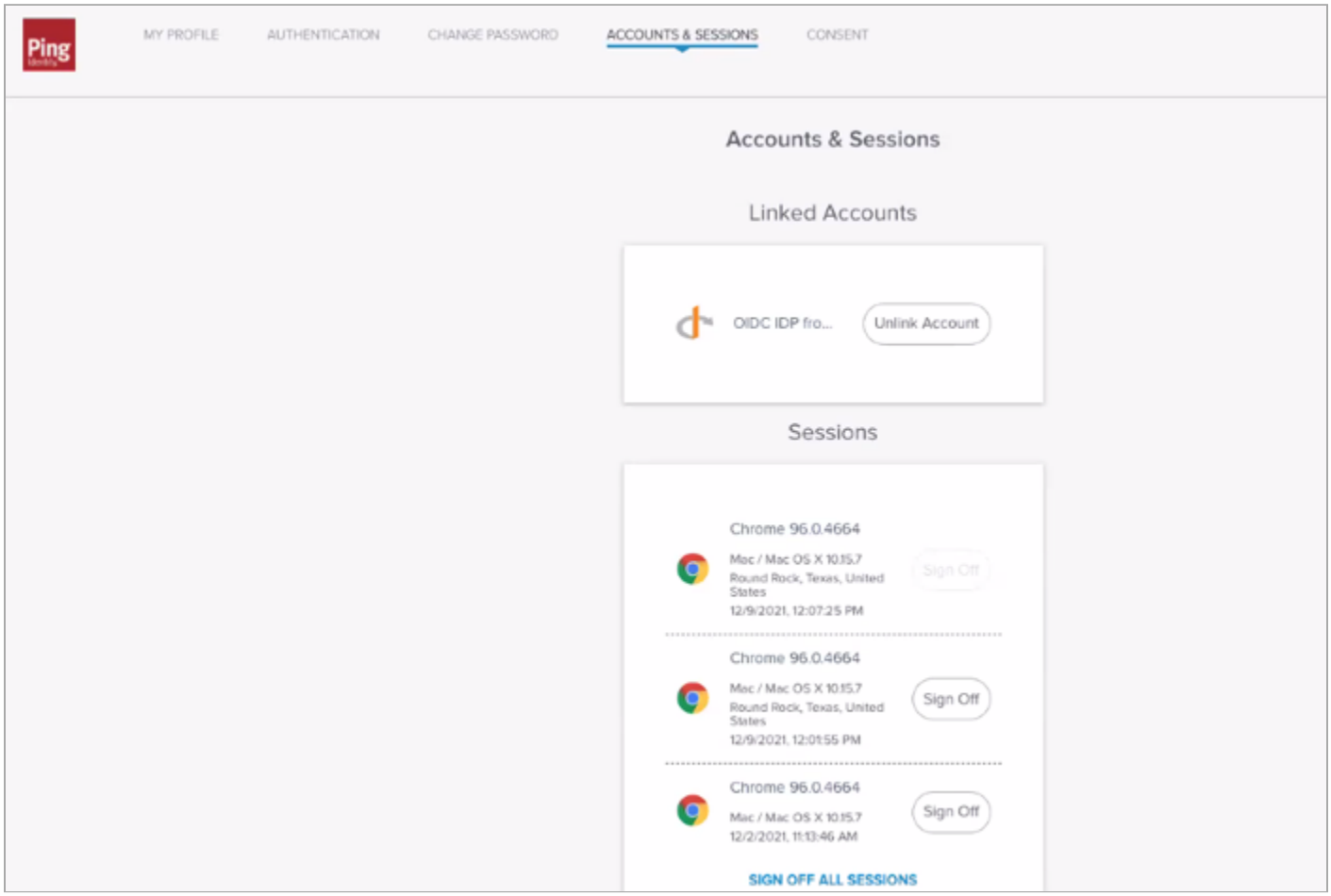
Administrators can allow their users to sign on using one or more external account profiles, such as Amazon, Facebook, or GitHub. When a user signs on using an external account, the account is listed in their profile, in the **Linked Account** section of the **Accounts & Sessions** tab. Users can view and manage their accounts from this tab.

About this task

You can view and manage:

- Linked accounts: The first time you sign on using a linked account, such as Facebook or LinkedIn, the account is linked to your profile.
- Sessions: Each time you sign on to your account or app, a new session is created. If you sign on using more than one device, you create multiple active sessions. Active sessions are displayed in the **Accounts & Sessions** tab and show details of the browser, device type, and the date and time at which the session started.

Copyright © 2025 Ping Identity Corporation



Steps

1. Go to your profile and click the **Accounts & Sessions** tab.

   Result:

   You see any linked accounts and any open sessions.

2. To unlink an external account:

   1. In the row next to the account that you want to unlink, click **Unlink Account**.

      Result:

      A confirmation window opens.

   2. Click **Unlink**.

      Result:

   The account is removed.

3. To sign off an open session:

   Choose from:

   - Sign off a single session: Next to the relevant entry, click **Sign Off**.

Copyright © 2025 Ping Identity Corporation

- Sign off all sessions: Click **Sign off all sessions**.

Managing consents

View or revoke any terms of service agreements that you consented to when accessing your account.

About this task

From the **Consents** tab, you can view all the agreements that you have consented to. Agreements can include terms and conditions, as well as permissions for an application. For example, you might allow an application to access your profile or email address.

Steps

1. Go to your profile. See End users: Accessing your PingOne profile.
2. Click the **Consent** tab.

   Result:

   You see a list of all agreements for which you've given your consent.

3. Do one or more of the following:

   - To view details of the agreement, click the **Eye** icon ( ) next to an entry.
   - To revoke an agreement that you have already consented to, click the trash can icon. In the confirmation message, click **Revoke Access**.

Copyright © 2025 Ping Identity Corporation

Developer Tools

Use the information in this section to find out more about developer tools, APIs, and integrating with other Ping Identity software.

- PingOne Platform API Reference
- Tools for developers
- Monitoring activity with Splunk
- Integrating with other Ping Identity software
- IP address and domain reference
- PingOne browser support

PingOne Platform API Reference

The PingOne API gives developers the tools to manage users and integrate enterprise and third-party applications with the PingOne identity and application management platform.

You can find the PingOne Platform API Reference at https://apidocs.pingidentity.com/pingone/platform/v1/api/.

Tools for developers

Ping Identity provides several tools that make it easy to get identity services such as authentication and SSO into your applications.

See the Developer Tools section in the Ping Identity Developer portal.

You can find the PingOne Native SDKs at https://apidocs.pingidentity.com/pingone/native-sdks/v1/api.

Monitoring activity with Splunk

Use Splunk to monitor PingOne activity data.

Installing the PingOne App for Splunk

The PingOne App for Splunk correlates your PingOne data into a meaningful dashboard. The app allows you to create custom dashboards and reporting, monitor activity data, and analyze event data over time.

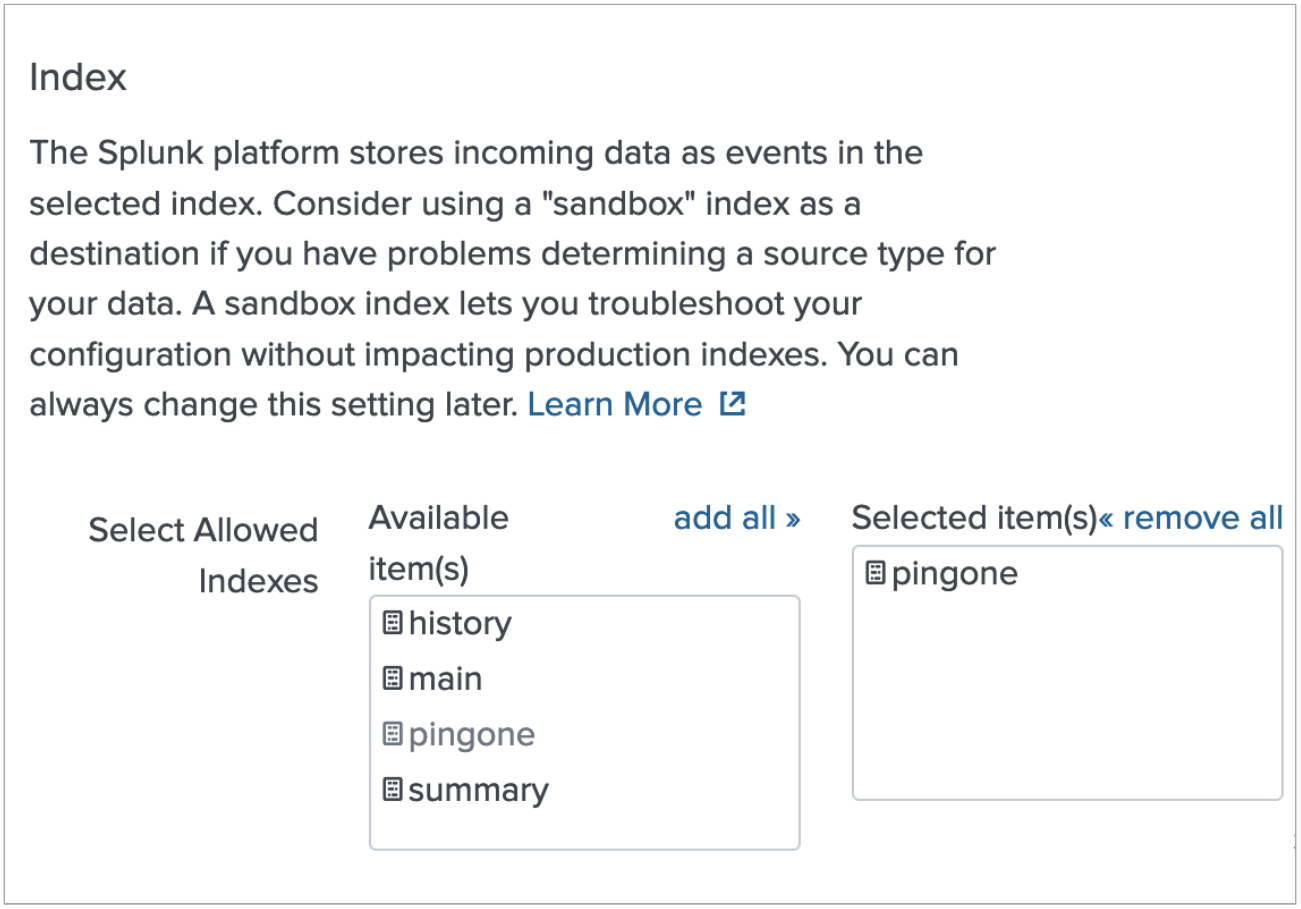
Before you begin

You must:

- Have a Splunk administrator account.
- Create a webhook to send your PingOne data to your Splunk instance. We recommend collecting the data in `index=pingone` so that the data model attached to the PingOne App for Splunk will automatically pick up the data.
    - Create a data input in Splunk to receive the webhook data from PingOne. In Splunk, click **Settings** > **Data inputs**.

Copyright © 2025 Ping Identity Corporation

- For **HTTP Event Collector**, click **+Add new**. Send the data to `index=PingOne`. Make sure to copy the token provided by Splunk. Learn more in the Splunk HTTP Event Collector documentation.



> **Note**
>
> To use a different index, refer to step 2 below to configure the PingOne App for Splunk to capture webhook data stored in other indexes.

- Create the webhook in PingOne and add a custom header, where you can enter the token provided by Splunk when you created the **HTTP Event Collector** input.

- Download the PingOne App for Splunk package in Splunkbase. Search for `PingOne` in Splunkbase to find the file.

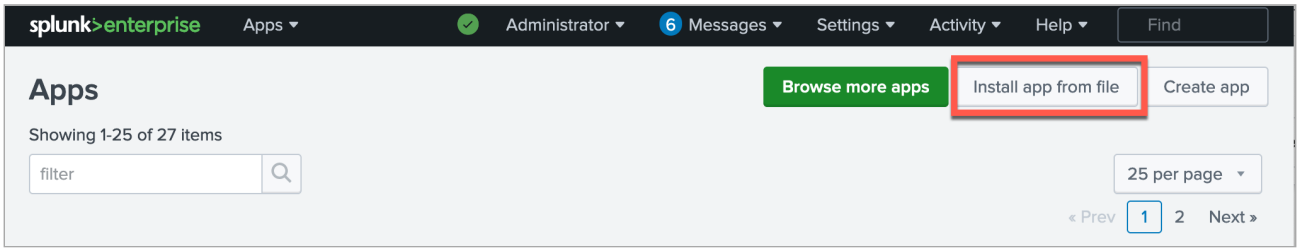
About this task

To install the PingOne App for Splunk:

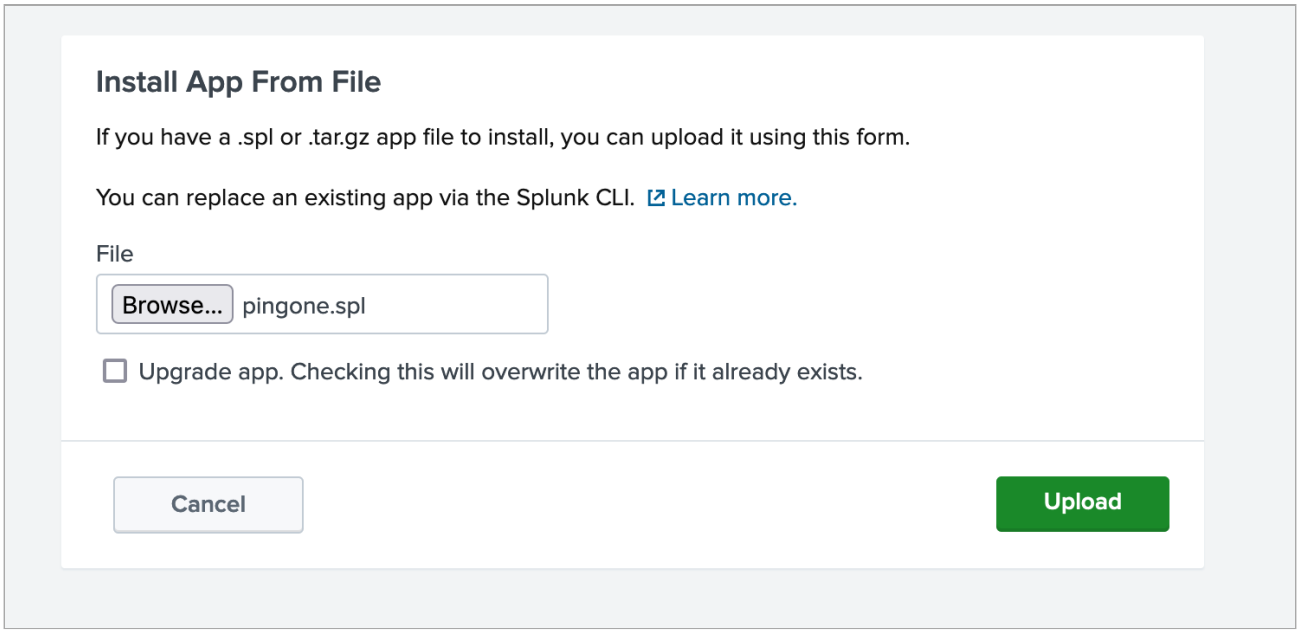
Steps

1. Sign on to Splunk and install the PingOne App for Splunk.
    1. Click **Apps** > **Manage Apps**.
    2. Click **Install app from file**.

Copyright © 2025 Ping Identity Corporation



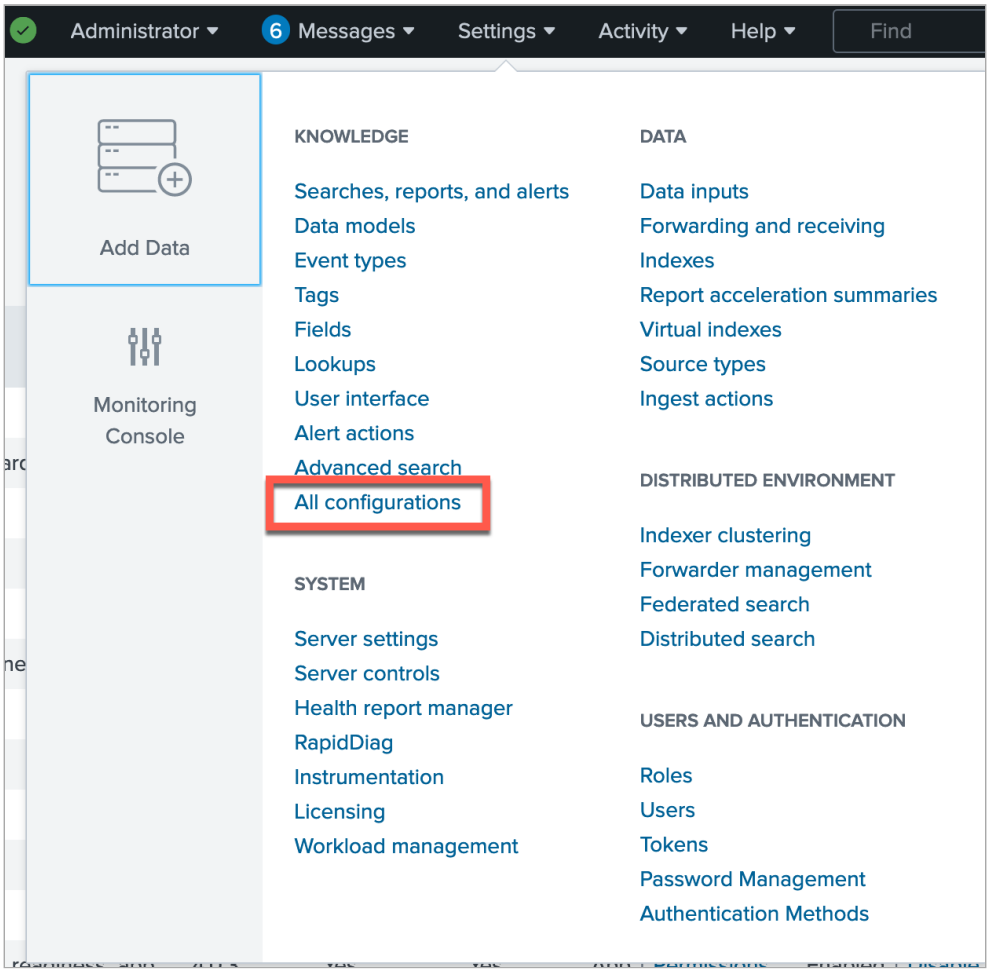
3. To upload the PingOne App for Splunk package file, click **Browse**, select the file, and then click **Upload**.



2. If your data is not in `index=pingone`, modify the macro to point to your data:

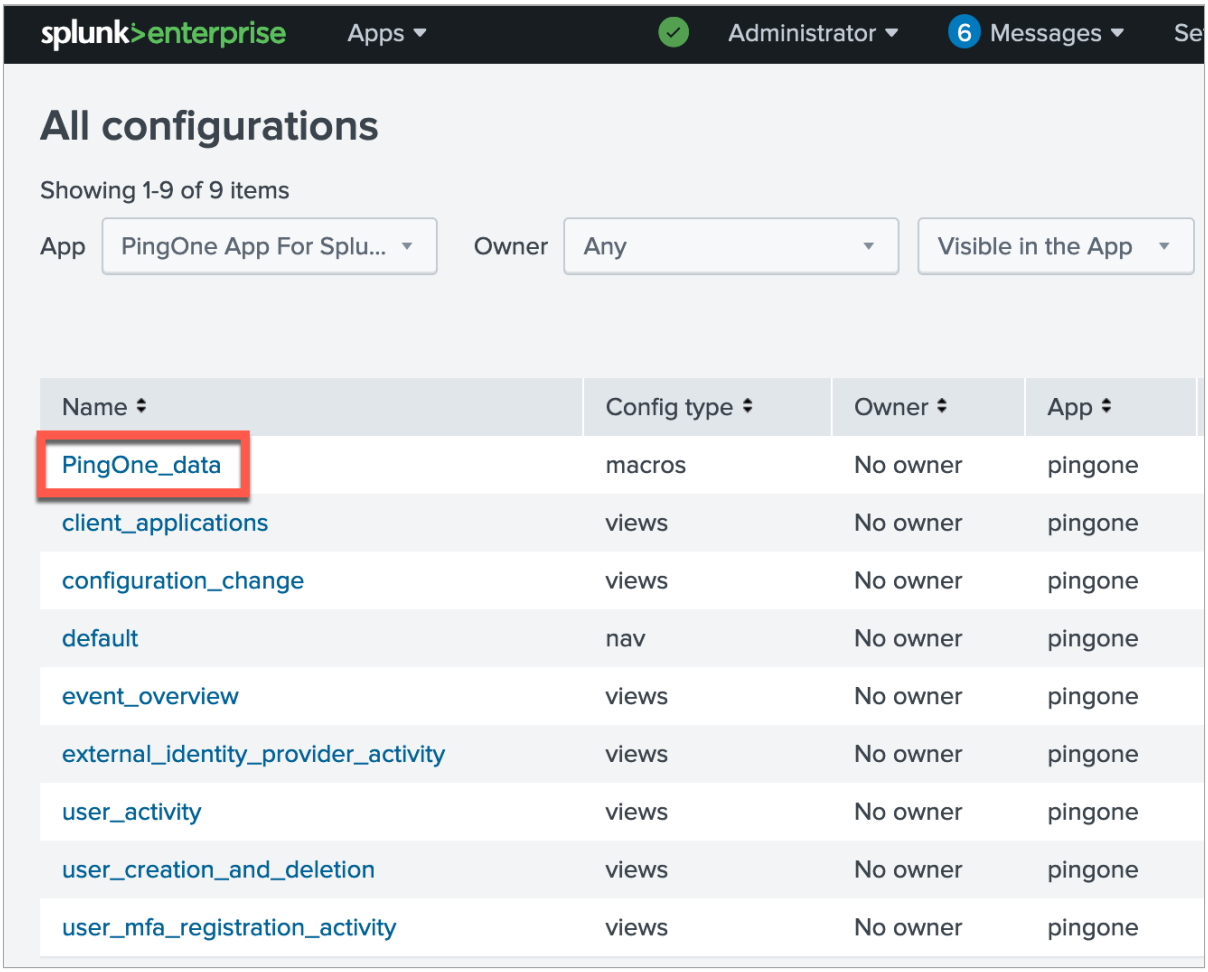
   1. Click **Settings** > **All configurations**.

Copyright © 2025 Ping Identity Corporation



2. For the **App** field, filter on **PingOne App for Splunk** configurations and select the **PingOne_data** macro.

Copyright © 2025 Ping Identity Corporation



3. To point the macro to your data, enter your index in the **Definition** box.

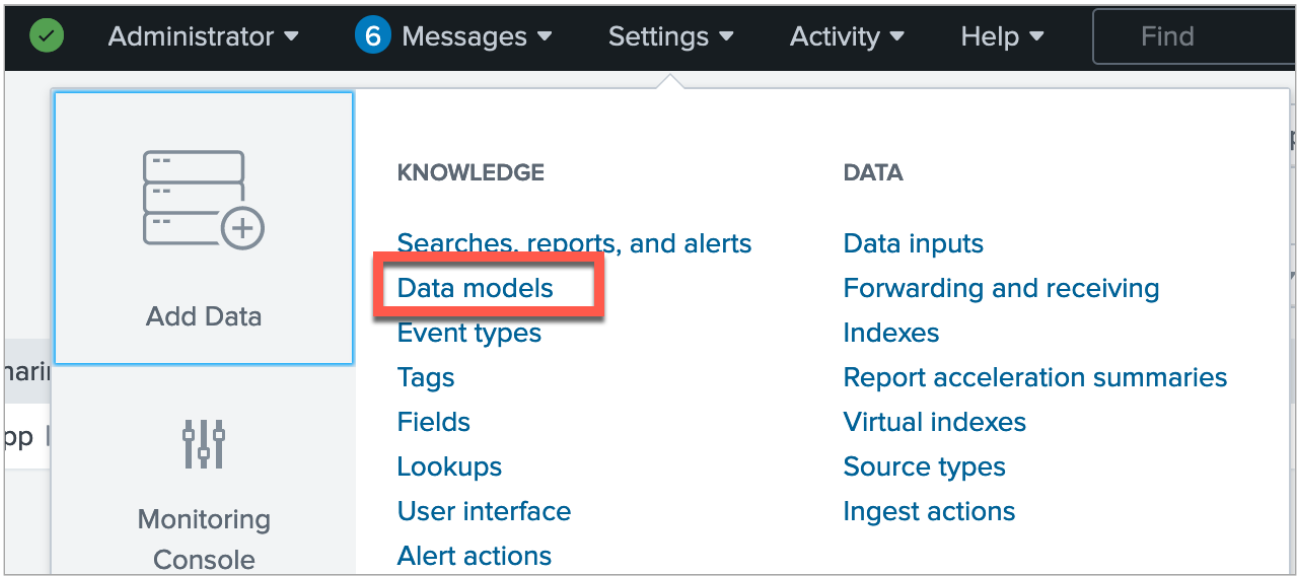
   The default is `index=PingOne`. Below is an example definition.

3. (Optional) Accelerate your data model to make a summary index of PingOne data.

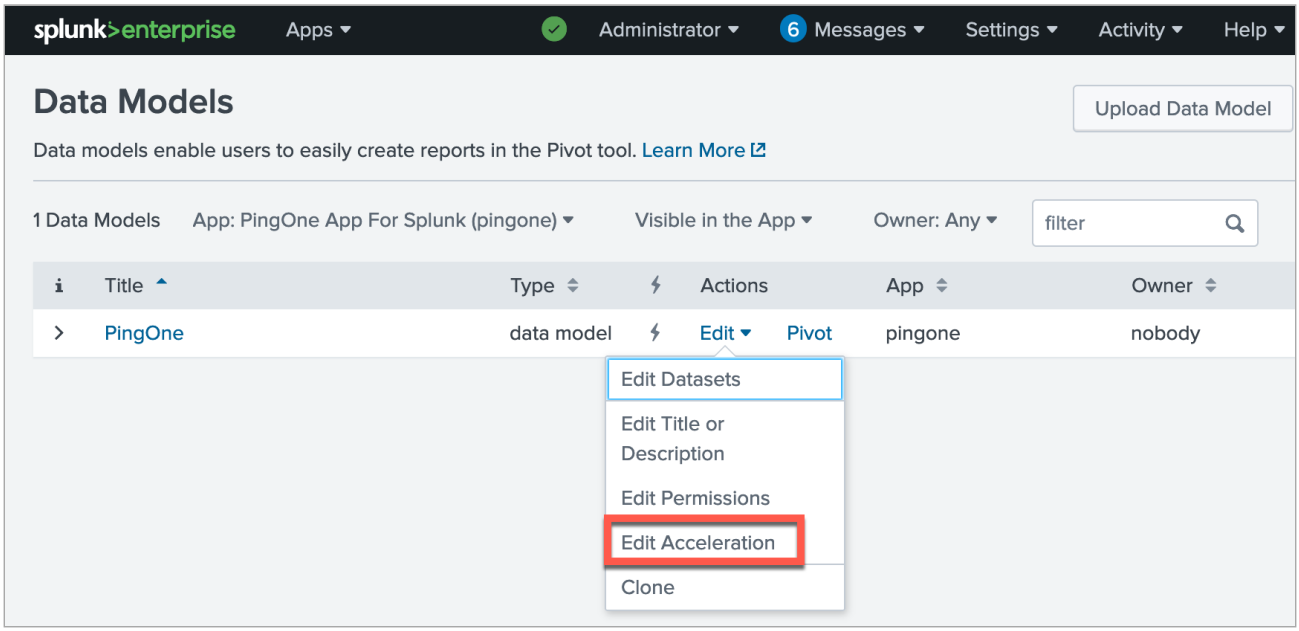
   The summary index results in more efficient population of the dashboards and allows you to populate the tables over larger time ranges.

   1. Go to **Settings** > **Data models**.

Copyright © 2025 Ping Identity Corporation



2. Click **Edit** > **Edit Acceleration** for the PingOne data model.

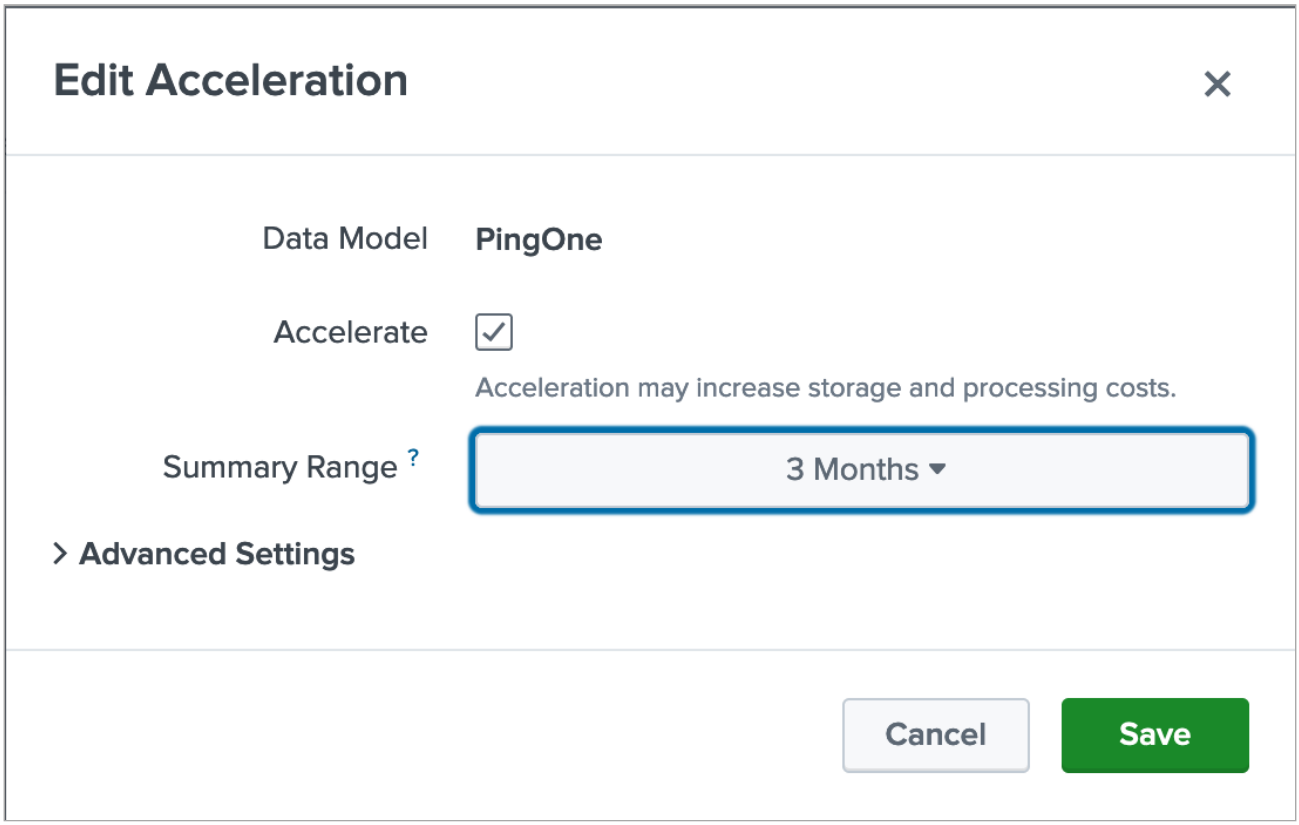


3. In the **Edit Acceleration** window, select the **Accelerate** checkbox.

4. Select a **Summary Range**. Click **Save**.

> **Note**
>
> The dashboards only display accelerated data through the summary range selected, so choose a time range accordingly.

Copyright © 2025 Ping Identity Corporation



> **Note**
>
> It will take time for the summary index to build.

Troubleshooting the PingOne App for Splunk

See the following information for help troubleshooting the dashboards in the PingOne App for Splunk.

Why do some of the graphs not populate?

If there are no results returned within the selected time range given, the dashboard widget shows as blank. If this activity is limited to one widget, such as a table or chart, on a dashboard, this likely means there were no relevant events to populate the chart.

Why do the Event Detail charts have a count listed?

The data model collects aggregate data, which is used to populate the dashboards. Because the data collected are not raw log events, it's possible for multiple matching events to be aggregated. As an example, if a user account was unlocked 3 times in a second by the same administrator, the count value would be 3.

How do the dashboard table fields translate from PingOne webhook JSON data?

In the PingOne App for Splunk prebuilt dashboards, the PingOne webhook JSON data translates to the following table headings.

Copyright © 2025 Ping Identity Corporation

JSON Key	Field Name
`action.type`	Action
`result.description`	Description
`result.status`	Status
`actors.client.id`	Client ID
`actors.client.environment.id`	Environment ID
`actors.client.name`	Client Application
`actors.user.id`	Actor ID
`actors.user.name`	Actor
`resources.name`	Target Resource
`action.type`	Action

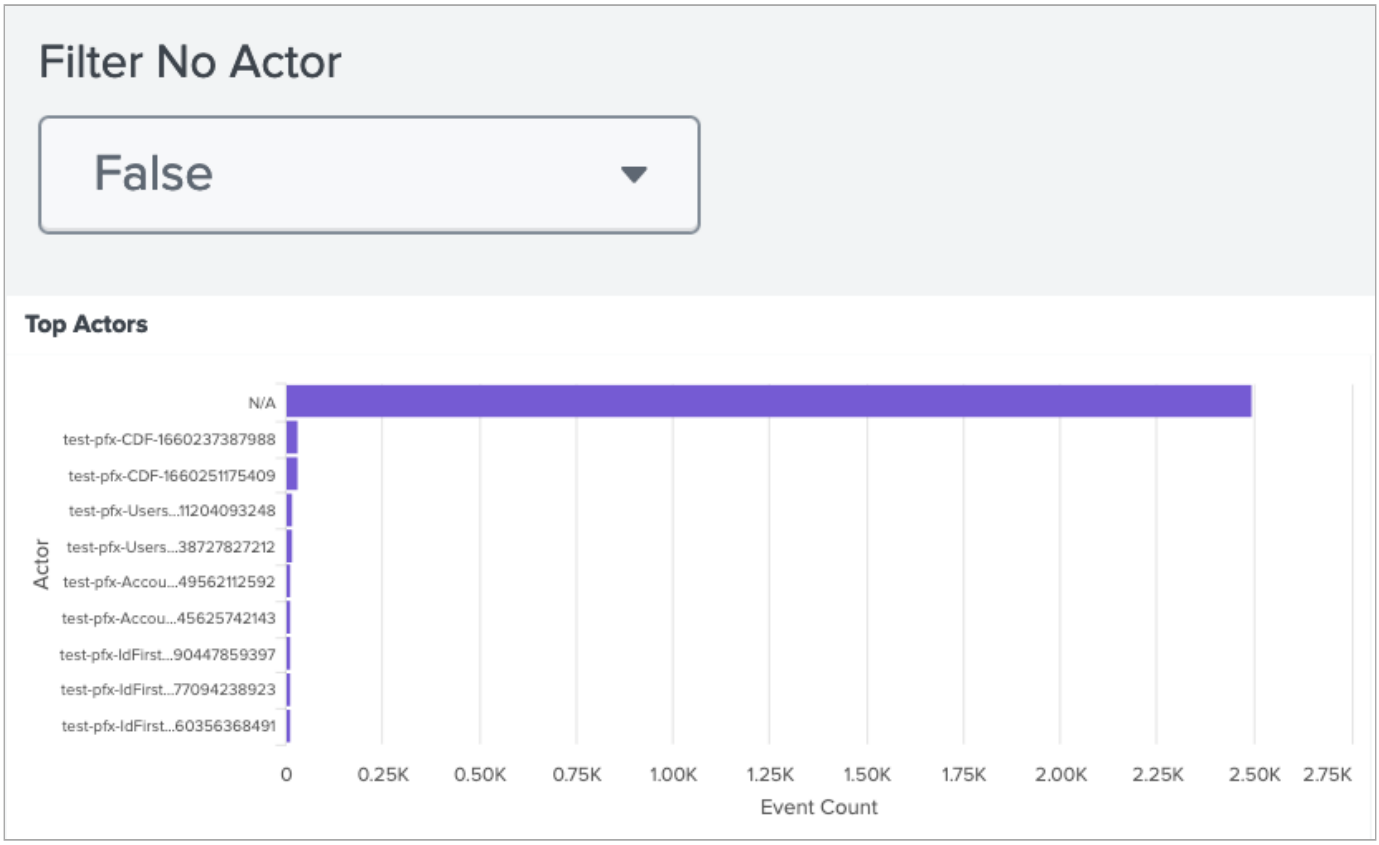
What does "N/A" mean when populated into a field such as Actor (actors.user.name)?

In this case, "N/A" means that no value was included with the event. For instance, if the activity was performed by a worker app instead of a user account, the corresponding event data would have an N/A value in the dashboard results.

Certain dashboards allow you to filter N/A values in the results. For the **User Activity** dashboard:

- If **Filter No Actor** is set to `False`, N/A values are displayed.

Copyright © 2025 Ping Identity Corporation



- If **Filter No Actor** is set to `True`, N/A values will be removed from the results.

Copyright © 2025 Ping Identity Corporation

Integrating with other Ping Identity software

PingOne can be integrated with other Ping Identity software, such as PingFederate and PingDataSync.

PingFederate

PingFederate is an enterprise federation server that enables user authentication and single sign-on. It serves as a global authentication authority that allows employees, customers and partners to securely access all the applications they need from any device. PingFederate can connect to PingOne for identity and authentication services.

By sending transaction information and an optional device profile to PingOne when a user signs on, PingFederate can get a security risk assessment for the sign-on event. Including the risk assessment in your PingFederate authentication policy allows you to dynamically adjust the user's authentication requirements each time they sign on.

You can use PingFederate to retrieve user attributes from PingOne and validate user credentials when a user tries sign-on.

You can also use the PingFederate provisioning engine to manage users in PingOne.

For more information, see the PingOne Integration Kit, the PingOne MFA Integration Kit, and the PingOne Protect Integration Kit.

PingDataSync

You can use PingDataSync to synchronize PingDirectory Server with PingOne. Using data synchronization, you can:

- Unify identity data across multiple data sources.
- Migrate identity data with zero downtime.
- Keep passwords, credentials, and profiles up to date.
- Choose fast, one-time migrations or ongoing bi-directional synchronizations.

For more information, see the PingDataSync Administration Guide.

IP address and domain reference

Use the information in this section to configure your network rules for PingOne. For PingOne to function correctly, you might need to configure your network to allow appropriate inbound and outbound traffic.

Inbound

PingOne provides services through several domains. The domains vary based on your organization's region. These domains are for traffic inbound to PingOne.

Add the following domains to your allow list to ensure that the services are available.

Copyright © 2025 Ping Identity Corporation

Region	Domain
Australia	api.pingone.com.au apps.pingone.com.au assets.pingone.com.au auth.pingone.com.au console.pingone.com.au http-access-api.pingone.au uploads.pingone.com.au uploads2.pingone.com.au
Canada	api.pingone.ca apps.pingone.ca assets.pingone.ca auth.pingone.ca console.pingone.ca http-access-api.pingone.ca uploads.pingone.ca uploads2.pingone.ca
Europe	api.pingone.eu apps.pingone.eu assets.pingone.eu auth.pingone.eu console.pingone.eu http-access-api.pingone.eu uploads.pingone.eu uploads2.pingone.eu
North America (US)	api.pingone.com apps.pingone.com assets.pingone.com auth.pingone.com console.pingone.com http-access-api.pingone.com uploads.pingone.com uploads2.pingone.com
Singapore	api.pingone.sg apps.pingone.sg assets.pingone.sg auth.pingone.sg console.pingone.sg http-access-api.pingone.sg uploads.pingone.sg uploads2.pingone.sg

Copyright © 2025 Ping Identity Corporation

Region	Domain
Asia Pacific (legacy) **Note** Available only for existing .asia customers.	api.pingone.asia apps.pingone.asia assets.pingone.asia auth.pingone.asia console.pingone.asia http-access-api.pingone.asia uploads.pingone.asia uploads2.pingone.asia

Note

The http-access-api.pingone.* domains handle requests from API gateway integration kits to PingOne Authorize API Access Management. Learn more about controlling access to your APIs in API Access Management.

Firewall settings for end users accessing PingOne from your network

If your organization uses a firewall that restricts inbound traffic, follow the specific procedures for the operating system and the firewall you use to add the LaunchDarkly domain to the allow list. Adding this domain supports feature flag release management for early access or beta features in PingOne.

Note

End users accessing PingOne from outside your organization's network do not need to enable this domain.

Region	Domain
North America - US	launchdarkly.com

Outbound

The static IP addresses are for traffic outbound from PingOne to other services. The static IP addresses are Production NAT Gateways in each region that are used to send traffic.

You should ensure that the static IP addresses are correctly tagged in your network infrastructure so they are not inadvertently blocked.

Learn more about the list of current IP addresses in PingOne IP Addresses on the Ping Identity Support page.

Note

You might be prompted to sign on to access the Ping Identity Support page.

PingOne browser support

PingOne is supported on the following browsers.

Copyright © 2025 Ping Identity Corporation

Note

The minimum supported resolution is 1000 x 600 pixels.

Browser	Version
Google Chrome	Three most recent major versions
Mozilla Firefox	Three most recent major versions
Apple Safari for MacOS	Two most recent major versions
Microsoft Edge	Two most recent major versions
Microsoft Internet Explorer	PingOne support for Internet Explorer 11 ended on January 31, 2023.

Note

For PingOne to function properly, JavaScript must be enabled in the browser.
Desktop applications that use embedded browsers are only supported if the embedded browser is supported. For example, some Windows applications use Internet Explorer as the embedded browser. Those applications aren't supported because PingOne doesn't support Internet Explorer.

Copyright © 2025 Ping Identity Corporation

Operational Status

For the operational status of all Ping Identity services, including PingOne, see the Ping Identity status page.

You can also choose to subscribe to alert notifications.

Copyright © 2025 Ping Identity Corporation