PingOne for Enterprise

August 8, 2025

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 for Enterprise . . . 9
Which PingOne am I using?. . . . 13
PingOne for Enterprise requirements and browser support. . . . 16
PingOne for Enterprise usage monitoring . . . 19
PingOne for Enterprise Release Notes . . . 21
Previous PingOne for Enterprises releases . . . 34
Previous PingOne SSO for SaaS Apps releases . . . 123
Previous AD Connect Releases . . . 133
PingOne for Enterprise . . . 151
Getting started . . . 153
Registering a PingOne for Enterprise account . . . 154
PingOne for Enterprise language support. . . . 155
PingOne for Enterprise identity repositories . . . 156
SSO with PingOne for Enterprise . . . 158
Federated SSO with PingOne for Enterprise . . . 159
Basic SSO (password vaulting). . . . 160
PingOne for Enterprise and SLO . . . 162
Initiating SSO in PingOne for Enterprise . . . 166
Connecting to an identity repository . . . 168
Select PingOne for Enterprise Directory . . . 169
Manage directory settings . . . 170
Configure the directory password policy . . . 170
Allow self registration for new directory users . . . 171
Manage directory attributes . . . 173
Add directory attributes . . . 174
Remove directory attributes . . . 174
View or renew directory API credentials . . . 174
Assign directory branding and designs . . . 175
PingOne for Enterprise Directory attributes. . . . 177
Connect to Active Directory . . . 179
How AD Connect works . . . 180
AD Connect in a DMZ . . . 182
Installing AD Connect. . . . 183
Assign AD Connect branding and designs . . . 186
Using IWA with browser clients . . . 187
AD Connect final setup . . . 189
AD Connect security best practices . . . 190
Installing AD Connect with IIS . . . 192
Customize the login, error, and password change windows in AD Connect for IIs . . . 194

Configure IWA for AD Connect with IIS . . . 197
Secure your AD Connect with IIS deployment . . . 198
Add trusted sites using Firefox settings . . . 200
High availability for AD Connect . . . 200
AD Connect for IIS final setup . . . 203
Updating AD Connect . . . 205
Auto-update AD Connect . . . 205
Manually Update AD Connect . . . 206
Troubleshoot an AD Connect update . . . 209
View and manage AD Connect agent nodes . . . 209
Configure logging in AD Connect . . . 210
Connect to PingFederate . . . 214
Configuring Provisioning for PingFederate . . . 217
Connect to OpenID Connect . . . 218
Connect to Azure . . . 220
Connect to ADFS . . . 223
Connect to Google . . . 225
Connecting to a custom SAML provider . . . 226
Creating advanced attribute mappings . . . 230
Managing applications . . . 234
Adding or updating a SAML application . . . 235
Configuring your OAuth settings . . . 238
Adding or updating an OIDC application . . . 241
Integrating an OIDC application . . . 245
OIDC application grant types . . . 254
Assign advanced attribute mappings . . . 255
Add or update an application using its SSO URL . . . 258
Add an application from the Application Catalog . . . 259
PingOne for Enterprise Application Catalog . . . 260
Achievers . . . 262
ADP Workforce . . . 265
Amazon Web Services . . . 268
Aquera . . . 273
Arena BOMControl . . . 276
Ariba . . . 278
Atlassian Cloud . . . 281
Bomgar . . . 286
Box . . . 289
Concur . . . 294
Cornerstone . . . 298
Coupa . . . 301
CylancePROTECT . . . 305
DocuSign . . . 309
Dropbox . . . 312

Egnyte . . . 316
Evernote . . . 321
Workplace by Facebook . . . 325
Github.com . . . 328
Kronos Workforce . . . 332
Lucidchart . . . 335
Microsoft 365 . . . 340
NetSuite . . . 346
New Relic . . . 350
PagerDuty . . . 353
Salesforce . . . 356
ServiceNow . . . 361
Sharefile . . . 365
Slack . . . 368
Smartsheet . . . 373
SuccessFactors . . . 377
Ultimate Software . . . 380
WebEx . . . 384
Workday . . . 388
Zendesk . . . 392
Zoom . . . 395
Add a Basic SSO (password vaulting) application . . . 402
Creating a custom application category . . . 402
Managing users . . . 403
Managing PingOne for Enterprise Directory users . . . 404
Add directory groups and entitlements . . . 405
Add directory users . . . 406
Approve new directory users . . . 407
Display directory user details . . . 408
Update directory user details . . . 411
Reset a user's password . . . 411
Disable directory users . . . 411
Delete directory users . . . 412
Validating user credentials with PingFederate . . . 412
Changing user passwords for PingFederate . . . 413
Managing users by group . . . 413
Adding user groups . . . 414
Authorize group access to applications . . . 415
Exporting a report of applications by group . . . 416
Delete groups . . . 416
Managing service users . . . 416
Temporarily hiding a user's service . . . 417
Bypassing a user's service . . . 417
Removing service users . . . 419

User provisioning in PingOne for Enterprise . . . 419
Authenticating users . . . 422
Create or update an authentication policy . . . 423
Disable an authentication policy . . . 425
Certificate management . . . 425
View certificate details . . . 426
Download or share a certificate . . . 427
Create a signing certificate . . . 427
Importing a certificate and key pair . . . 428
View and change certificate usage . . . 429
Updating a signing certificate . . . 429
Update a signing certificate for application connections . . . 430
Updating a signing certificate for an identity repository . . . 431
Check whether you need to update the PingOne for Enterprise universal certificate . . . 432
Sign a certificate using a CSR . . . 433
Updating a verification certificate . . . 433
Update an encryption certificate . . . 435
Delete a certificate . . . 436
Monitoring PingOne for Enterprise use . . . 436
Monitoring service activity . . . 436
Reports . . . 437
PingOne for Enterprise report types . . . 438
PingOne for Enterprise report event reference . . . 439
Run a predefined report . . . 444
Run a custom report . . . 445
Subscriptions . . . 446
Adding a Push subscription . . . 448
Add a Poll subscription . . . 450
Get the audit events for a Poll subscription . . . 451
Creating an Admin-API client . . . 454
Managing your administrators and account . . . 455
Assign administrative roles . . . 456
Assign Application Administrator applications . . . 457
Manage your user profile . . . 458
Editing administrative roles, permissions, and notifications . . . 459
Assign admin portal groups . . . 460
Configuring SSO to the PingOne for Enterprise admin portal . . . 460
SSO to the PingOne for Enterprise admin portal with multi-factor authentication . . . 461
SSO to the PingOne for Enterprise admin portal from PingFederate . . . 463
Assign branding and design . . . 464
Upgrade a PingOne for Groups account . . . 466
Using the PingOne for Enterprise dock
Introducing the PingOne for Enterprise dock . . . 466

Launch an application . . . 468
Manage your devices. . . . 468
Install the PingOne for Enterprise browser extension . . . 469
Change your privacy key . . . 470
Manage your Basic SSO passwords . . . 471
Configuring the dock when using an identity bridge. . . . 471
Configure the dock when using PingOne for Enterprise Directory . . . 474
Assign branding and design . . . 476
Add an app to a category . . . 479
Upgrade the PingOne for Enterprise dock . . . 479
Monitoring and modifying customer accounts. . . . 480
Display and search customer accounts . . . 480
Administer customer accounts . . . 481
Configuring customer account service settings . . . 481
Invite a new customer . . . 484
Creating a customer account . . . 485
Upgrade a customer account . . . 485
Suspend a customer account . . . 486
Change a customer ID or account name . . . 486
Reference
Administrative roles . . . 487
Error code reference . . . 489
PingOne for Enterprise security best practices . . . 498
PingOne for Enterprise use cases . . . 500
PingOne SSO for SaaS Apps . . . 500
PingOne SSO for SaaS Apps overview . . . 504
Update the PingOne SSO for SaaS Apps universal certificate . . . 505
Getting started . . . 506
Configure your account
Assign administrators . . . 507
Assign branding and design . . . 507
Manage your user profile . . . 509
Editing administrative roles, permissions, and notifications . . . 509
Configure SSO to the admin portal. . . . 510
Add a SaaS application . . . 512
Adding or updating a SAML-enabled application . . . 512
Adding or updating an OIDC application . . . 515
Add or update other applications . . . 518
PingOne for Enterprise and SLO . . . 521
Integrate an application. . . . 524
Integrating an OIDC application . . . 527
Using the global REST API client credentials . . . 537
Creating or editing application-specific credentials . . . 538
Creating or editing additional Connection API credentials . . . 539

Redirect users to PingOne SSO for SaaS Apps (SP-initiated SSO) . . . 540
Java Redirect Sample . . . 541
.NET Redirect Sample . . . 542
PHP Redirect Sample . . . 543
Ruby Redirect Sample . . . 544
Python Redirect Sample . . . 545
Perl Redirect Sample . . . 546
Process the PingOne SSO for SaaS Apps token exchange . . . 547
Java Token Exchange Sample . . . 549
.NET Token Exchange Sample . . . 552
PHP Token Exchange Sample . . . 555
Ruby Token Exchange Sample . . . 558
Python Token Exchange Sample . . . 558
Perl Token Exchange Sample . . . 561
Integrate an application hosted on multiple URLs . . . 564
Test your application
Testing your application using the built-in IdP . . . 565
Testing your application using PingOne for Enterprise . . . 566
Connect customers to your application . . . 568
Partner account applications . . . 569
Connect an application for a partner account . . . 569
Creating an invited SSO connection . . . 571
Application Catalog app connection . . . 571
Create a connection using the SSO self-service widget . . . 572
Create a connection using the Customer Connection API . . . 574
Creating a manual SAML connection . . . 574
Edit an invited customer connection . . . 576
Edit a managed customer connection . . . 577
Adding a new connection to an existing customer . . . 579
Finding theidpIdvalue . . . 579
Certificate management . . . 580
View certificate details . . . 581
Download or share a certificate . . . 582
Create a signing certificate . . . 582
Importing a certificate and key pair . . . 583
Associate certificates with a SAML application or customer IdP connection . . . 584
View certificate usage . . . 585
Updating a signing certificate . . . 585
Update a signing certificate for applications . . . 585
Update a signing certificate for a customer IdP . . . 586
Sign a certificate using a CSR . . . 587
Updating a verification certificate for an application or customer IdP connection . . . 587
Update an encryption certificate . . . 588
Delete a certificate . . . 588

Managing reports and subscriptions . . . 588
Reports. . . . 589
PingOne SSO for SaaS Apps report types . . . 589
PingOne SSO for SaaS Apps report event reference . . . 591
Subscriptions . . . 595
Manage partner accounts . . . 596
Configure partner account service settings . . . 597
Creating and administering a partner account . . . 599
Inviting a new customer . . . 600
Enable IdP discovery . . . 601
Reference . . . 601
PingOne SSO for SaaS Apps Customer Connection API . . . 601
About multiplexing . . . 612
PingOne SSO for SaaS Apps security best practices . . . 614
What is an idpId? . . . 615
Invited PingOne for Enterprise SSO . . . 616
Getting started with Invited PingOne for Enterprise SSO . . . 618

PingOne for Enterprise

PingOne for Enterprise is a cloud solution that lets you connect your workforce users to any SAML or OpenID Connect (OIDC) application with a single sign-on (SSO).

Note

If you have a PingOne SSO for SaaS Apps license, see PingOne SSO for SaaS Apps. If you're not sure which license you have, see Which PingOne am I using?.

PingOne for Enterprise release notes

- PingOne for Enterprise Release Notes

PingOne for Enterprise operational status

See Ping Identity Services for the operational status of all Ping Identity services, including PingOne for Enterprise. You can also choose to subscribe to alert notifications.

You can also connect to the following heartbeat endpoints to monitor PingOne for Enterprise operational status:

- SSO: https://sso.connect.pingidentity.com/sso/heartbeat
- Admin Portal: https://admin.pingone.com/web-portal/heartbeat

Get started with PingOne for Enterprise

- PingOne for Enterprise
- System requirements and browser support
- PingOne for Enterprise language support
- Register a PingOne for Enterprise account
- Connect to an identity repository
- SSO with PingOne for Enterprise
- Assign branding and design

Copyright © 2025 Ping Identity Corporation

Use PingOne for Enterprise

- Add and manage applications
- PingOne for Enterprise Application Catalog
- Add, delete, and manage users
- Configure authentication policies
- Manage certificates
- Monitor service activity with reports and subscriptions
- Manage your administrators
- Configure the dock
- PingOne for Enterprise use cases
- Administrative roles
- Security best practices

PingOne for Enterprise for Managed Service Providers

PingOne for Enterprise for Managed Service Providers includes all of the features of a standard PingOne for Enterprise account, plus additional functionality to manage your customer accounts.

- Monitor and manage customer accounts

Troubleshoot PingOne for Enterprise

- Error code reference
- Monitoring your usage for billing and licensing

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise

Learn more

- PingOne for Enterprise community forum
- PingOne for Enterprise support
- PingOne for Enterprise training (existing customers only)
- Partner portal (partners)

Copyright © 2025 Ping Identity Corporation

Which PingOne am I using?

This guide can help determine whether you are using PingOne or a version of PingOne for Enterprise, so that you can access the appropriate documentation and support.

PingOne or PingOne for Enterprise?

The PingOne Platform and PingOne for Enterprise are different products that use separate interfaces.

The best way to determine which product you're using is the URL that you use to access the administration portal.

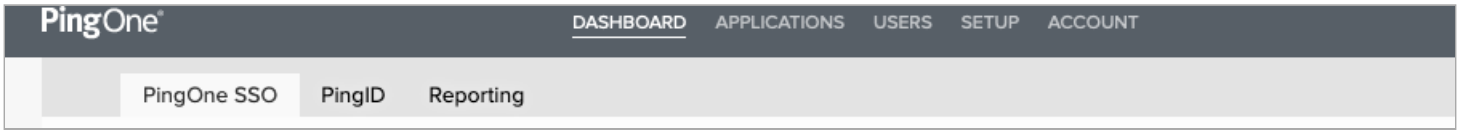
Product	Admin Console URL	Documentation Link
PingOne	console.pingone.com	PingOne
PingOne for Enterprise	admin.pingone.com	PingOne for Enterprise

There are four versions of PingOne for Enterprise with different capabilities to meet different use cases.

You can identify which version of PingOne for Enterprise you're using by looking at the top navigation bar.

PingOne for Enterprise

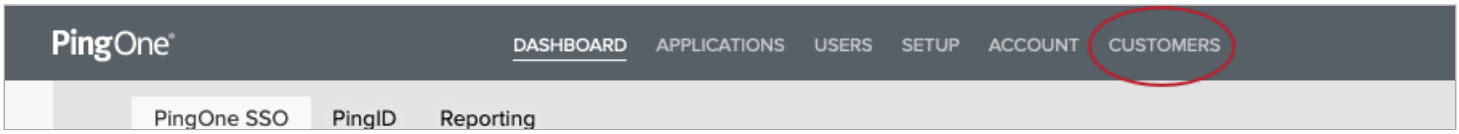
The top navigation bar on PingOne for Enterprise has menus for **Dashboard**, **Applications**, **Users**, **Setup**, and **Account**.



Learn more in the PingOne for Enterprise documentation.

PingOne for Enterprise for Managed Service Providers

PingOne for Enterprise for Managed Service Providers has an additional **Customers** menu on the right of the top navigation bar.

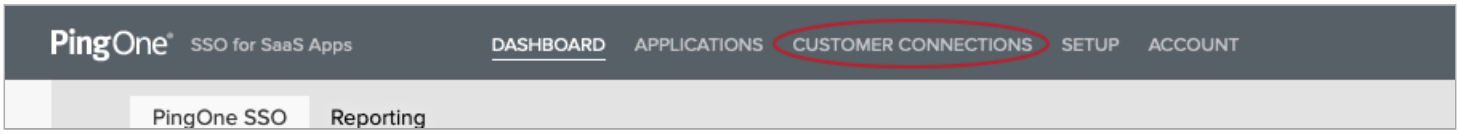


Learn more about managing customer accounts with PingOne for Enterprise for Managed Service Providers in Monitoring and modifying customer accounts

PingOne SSO for SaaS Apps

PingOne SSO for SaaS Apps has an additional menu for **Customer Connections** between **Applications** and **Setup** on the top navigation bar.

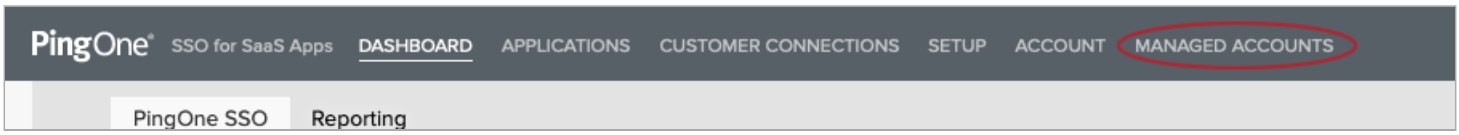
Copyright © 2025 Ping Identity Corporation



Learn more in the PingOne SSO for SaaS Apps documentation.

PingOne SSO for SaaS Apps with Managed Accounts

In addition to the **Customer Connections** menu, PingOne SSO for SaaS Apps with Managed Accounts has a **Managed Accounts** menu on the right of the top navigation bar.



Learn more in Manage partner accounts.

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise requirements and browser support

These requirements apply to all versions of PingOne for Enterprise and PingOne SSO for SaaS Apps.

Access requirements

The following URLs and ports must be accessible:

URL/Port	Purpose
Port 443	The default port for secure HTTP.
https://admin.pingone.com	Connect to your organization's PingOne for Enterprise account for administration and management purposes.
https://desktop.pingone.com https://desktop.pingone.eu https://desktop.pingone.com.au	Connect to the PingOne for Enterprise dock page for user SSO to applications. The page is a path following this URL and is unique to your organization.
https://authenticator.pingone.com https://authenticator.pingone.eu https://authenticator.pingone.com.au	The PingOne for Enterprise authenticator service.
https://sso.connect.pingidentity.com	The single sign-on (SSO) engine for PingOne for Enterprise. This URL is not regionalized.
https://login.pingone.com https://login.pingone.eu https://login.pingone.com.au	The sign-on engine for PingOne for Enterprise Directory and AD Connect.

Supported Browsers

Javascript must be enabled for all browsers.

PingOne dock is supported on both desktop and mobile displays, for all specified browser versions.

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 **Note** The PingOne for Enterprise browser extension is not supported on Safari.
Microsoft Edge	Two most recent major versions

Copyright © 2025 Ping Identity Corporation

Browser	Version
Microsoft Internet Explorer	PingOne for Enterprise support for Internet Explorer 11 ended on September 30, 2022.

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise usage monitoring

The following reports help you track single sign-on (SSO) usage, which partially determines your PingOne for Enterprise billing.

To run these reports, go to **Dashboard > Reporting**. For more information see Reports.

PingOne for Enterprise usage reports

SSO Summary

This report lists the number of SSO transactions by application during the specified time period. Because the report tracks SSO usage by application, the same user is counted multiple times if they access multiple applications. Therefore, the report total will be higher than your actual SSO usage.

SSO User Summary

This report lists all of the usernames that used SSO during the specified period. You can export the list to audit or count it. Deleting users from **Users by Service** deletes them from this report, but it doesn't delete them from Ping's historical records for billing and licensing purposes. Deleted users are restored to the report the next time they use SSO. For more information, see Temporarily hiding a user's service.

PingOne SSO for SaaS Apps usage reports

SSO Summary by Customer

This report lists the unique usernames that accessed each of your applications through PingOne SSO for SaaS Apps. Because the report tracks SSO usage by application, the same user is counted multiple times if they access multiple applications. Therefore, the report total will be higher than your actual SSO usage.

SSO User Count

This report provides a count of unique usernames that accessed your applications through PingOne SSO for SaaS Apps for each of your customers. Because this report counts totals for each customer rather than by application, you can use these numbers to determine exact SSO usage by customer. Summing these amounts gives you the total number of unique users, which will match Ping's internal usage numbers for billing and licensing purposes.

Subscriptions

You can also set up real-time SSO usage monitoring through the **Subscriptions** tab. Setting up an **SSO** subscription in PingOne for Enterprise or PingOne SSO for SaaS Apps allows you to send SSO events to your own external system so that you can track the number of unique users.

For more information, see Subscriptions.

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise Release Notes

New features and improvements in PingOne for Enterprise, PingOne for Enterprise for Managed Service Providers, PingOne SSO for SaaS Apps, PingOne SSO for SaaS Apps with Managed Accounts, and AD Connect.

May 2025

Users tab restored after migrating PingID

Info PingOne for Enterprise

We've restored the SSO functionality in the **Users** tab for accounts that have migrated their PingID tenant to PingOne. We've also added a banner linking you to the PingOne admin console where you can manage your migrated PingID tenant.

February 2025

Filter Users by Service search

New PingOne for Enterprise

We've added a feature that allows you to filter your search results by user attribute in the **Users by Service** window. You can now search by Subject, Email, or Name across all available services. The default attribute is Subject.

To search by Name, the input string must be in the format "last name, first name".

> **Note**
>
> To use the search filter, your account must not have the `SERVICE_USER_LEGACY` feature flag, which preserves legacy search behavior from before a PingOne for Enterprise update in April 2023.
> Your account only has this feature flag enabled if you requested it. If you're not sure whether you have this feature flag, or if you want it removed so you can access this new behavior, open a support case.
> The email and name filters can only filter user data that was newly created or updated after this feature was deployed (February 2025).

Learn more in Temporarily hiding a user's service, Bypassing a user's service, and Removing service users.

January 2025

Users tab remains after PingID integration with PingOne

Fixed PingOne for Enterprise

We've fixed a defect that caused the **Users** tab to remain available to the Service User Admin role after you integrate your PingID tenant with PingOne.

Integrating PingID with PingOne moves user management from PingOne for Enterprise to the PingOne admin console.

Learn more in the Users section of the PingOne documentation.

Copyright © 2025 Ping Identity Corporation

Sub-tenant admin access lock

Fixed PingOne for Enterprise PingOne SSO for SaaS Apps

We've fixed a defect in PingOne for Enterprise for Managed Service Providers and PingOne SSO for SaaS Apps with Managed Accounts that allowed administrative users to permanently lock their access to read-only when impersonating a sub-tenant.

October 2024

AWS IAM Identity Center Provisioner

Improved PingOne for Enterprise

We added the ability to update the `nickname` attribute for existing provisioned Amazon Web Services (AWS) single sign-on (SSO) users.

Learn more in Amazon Web Services.

PingOne Connector

Fixed PingOne for Enterprise

We fixed a defect that could cause delays in fetching an updated user schema.

The following known limitations apply:

- Clearing fields on updates is not supported.
- Multivalued attributes (e.g. emails or addresses) are not supported. Multiple values appear as a single array value in PingOne.
- Custom attributes are set when the user is initially created and are never updated.

May 2024

SCIM SaaS Provisioner

Fixed PingOne for Enterprise

Fixed a defect that caused a JSON parsing error when non-standard fields are present in the SCIM 2.0 Enterprise User Schema Extension.

The following known limitations apply:

- User attributes cannot be cleared after they have been set. They can only be updated.
- Outbound Group Provisioning and Memberships are not supported.
- Patch updates to SCIM-enabled target applications are not supported.

Copyright © 2025 Ping Identity Corporation

- There is a limit of one value per type (such as home, work, or other) for multivalue attributes such as `email`, `phone`, and `address`.
- Unexpected behavior may occur if the SaaS does not specify either type and primary information, or both type and primary information for multivalue attribute such as such as `email`, `phone`, and `address`. Also, existing SaaS attributes might not be removed during an Update, and the desired value might not be correctly set as primary.
- SCIM-compliant service providers can implement or interpret SCIM standards differently, which can result in behavior that is not consistent with the intended use of the SCIM SaaS Provsioner.

PingOne Connector

New PingOne for Enterprise

Added support for the Australia region.

The following known limitations apply:

- Clearing fields on updates is not supported.
- Multivalued attributes (e.g. emails or addresses) are not supported. Multiple values appear as a single array value in PingOne.
- Custom attributes are set when the user is initially created, and are never updated.

March 2024

Country data for SSO report

New PingOne for Enterprise

Added a new column to the SSO report listing the country where the SSO event originated.

To learn more, see PingOne for Enterprise report event reference.

November 2023

ServiceNow Connector 2.3

New PingOne for Enterprise

Added support for the Utah and Vancouver versions of ServiceNow.

The following known limitations apply:

- Outbound Group Provisioning and Memberships are not supported.
- User attributes cannot be cleared after they have been set. They can only be updated.
- When provisioning to ServiceNow, all user accounts in ServiceNow must have a `username` (User ID).

Copyright © 2025 Ping Identity Corporation

This is not a required field in ServiceNow, but it is required for provisioning to work due to the provisioner using this field to sync with preexisting users in ServiceNow. If a user in ServiceNow resolves to `sAMAccountName` (the "standard" mapping in the provisioning channel), then the accounts will be linked.

Currently if users exist in ServiceNow without a `username` that will cause errors in provisioning, resolve this by ensuring every user has this field populated even if they are not intended to be managed by the provisioner.

- When provisioning users, the `username` attribute must only contain URL-safe characters.
- When synchronizing roles with users, the role attribute must contain only URL-safe characters.
- If a new user is created with the same `username` as an existing user, a duplicate user will not be created. Instead, the existing user will be updated with any information in the create.
- Due to limitations with the ServiceNow API, a role can be added to a user, but not removed. This may cause a user's role in the source datastore to become out-of-sync with the user's role in ServiceNow.

  For more information, see Enable User Role Removal.
- When mapping the `roles` attribute, multiple additional calls to ServiceNow must be made to sync user role. This may impact provisioning performance.
- For departments that contain the `^` character in the name, the ServiceNow API causes the creation of multiple departments with the same name.
- For the `department` and `location` parameters, the ServiceNow API ignores capitalization. When provisioning a user that matches multiple departments or locations in ServiceNow (such as Accounting and accounting), PingFederate provisions the user with an empty department or location attribute and logs an error in `provisioner.log`.
- The `city` attribute mapping is not supported for the local repository.

For more information, see Adding ServiceNow to Your PingOne for Enterprise Dock.

July 2023

Webex Connector 2.3.0

New PingOne for Enterprise

Updated the **SiteID** configuration field to be optional.

For more information, see Adding WebEx to Your PingOne for Enterprise Dock.

Zoom Connector 1.3.3

New PingOne for Enterprise

Added support for Server-to-Server OAuth applications. This is an alternative method to create a connection to Zoom due to the deprecation of JSON Web Token (JWT) applications.

For more information, see Adding Zoom to Your PingOne for Enterprise Dock.

Copyright © 2025 Ping Identity Corporation

May 2023

Manual PingOne for Enterprise connections

Info PingOne SSO for SaaS Apps

It is no longer possible to connect a PingOne for Enterprise tenant and a PingOne SSO for SaaS Apps tenant by manually exchanging metadata. This kind of connection was never supported, and can cause duplicate entity ID errors.

You should always use an invited connection to connect your PingOne SSO for SaaS Apps application to PingOne for Enterprise.

April 2023

Users by Service search

Info PingOne for Enterprise

The Users by Service search behavior has changed from returning results that contain the search string to returning results that begin with the username.

For more information, see Monitoring service activity.

ServiceNow Tokyo

Improved PingOne for Enterprise

Added support for the Tokyo version of ServiceNow.

The following known limitations apply:

- Outbound Group Provisioning and Memberships are not supported.
- User attributes cannot be cleared after they have been set. They can only be updated.
- When provisioning to ServiceNow, all user accounts in ServiceNow must have a `username` (User ID).

  This is not a required field in ServiceNow, but it is required for provisioning to work due to the provisioner using this field to sync with preexisting users in ServiceNow. If a user in ServiceNow resolves to `sAMAccountName` (the "standard" mapping in the provisioning channel), then the accounts will be linked.

  Currently if users exist in ServiceNow without a `username` that will cause errors in provisioning, resolve this by ensuring every user has this field populated even if they are not intended to be managed by the provisioner.
- When provisioning users, the `username` attribute must only contain URL-safe characters.
- When synchronizing roles with users, the role attribute must contain only URL-safe characters.
- If a new user is created with the same `username` as an existing user, a duplicate user will not be created. Instead, the existing user will be updated with any information in the create.

Copyright © 2025 Ping Identity Corporation

- Due to limitations with the ServiceNow API, a role can be added to a user, but not removed. This may cause a user's role in the source datastore to become out-of-sync with the user's role in ServiceNow.

  For more information, see Enable User Role Removal.

- When mapping the `roles` attribute, multiple additional calls to ServiceNow must be made to sync user role. This may impact provisioning performance.

- For departments that contain the `^` character in the name, the ServiceNow API causes the creation of multiple departments with the same name.

- For the `department` and `location` parameters, the ServiceNow API ignores capitalization. When provisioning a user that matches multiple departments or locations in ServiceNow (such as Accounting and accounting), PingFederate provisions the user with an empty department or location attribute and logs an error in `provisioner.log`.

March 2023

Email communications

Info PingOne for Enterprise, PingOne SSO for SaaS Apps

Updated our email communications to change the product name from "PingOne" to "PingOne for Enterprise".

This change affects both PingOne for Enterprise and PingOne SSO for SaaS Apps licenses, and will include all emails from Ping, including certificate expiration and password expiration messages.

Email templates that you have customized for your customer accounts are not affected by this change.

If you have any email filters in place, update them to reflect this change.

February 2023

PingID license management for customer accounts

New PingOne for Enterprise

Added the ability to manage PingID licensing for your PingOne for Enterprise for Managed Service Providers customer accounts.

> **Note**
>
> This feature is in limited release. To request access to this feature, open a support case.

For more information, see Administer customer accounts.

Google Workspace Connector 3.2.1

Improved PingOne for Enterprise

- Added support for the `addressFormatted` user attribute.

Copyright © 2025 Ping Identity Corporation

`addressFormatted` is a full and unstructured postal address. This single-string attribute can include any values like: PO Box, city, state/province, ZIP/postal code, or country/region.

- Fixed an issue that caused new users not to be provisioned with group membership.
- Fixed an issue that caused users not to be disabled by a disable deprovision action.

Learn more in Google Workspace Provisioner.

December 2022

Improved messaging for expired user invitations

Improved PingOne for Enterprise

Updated the messaging for the following PingOne for Enterprise Directory invited user scenarios:

If an invited user clicks on an expired invitation link, they are redirected to the PingOne for Enterprise sign-on page with an error message directing them to request a new invitation from an administrator. For more information, see Add directory users.

If an invited user has not yet been approved, and they try to use the **Forgot Password** link, they will see an error message that their account is still awaiting approval.

SCIM SaaS Provisioner 1.5

Improved PingOne for Enterprise

Added the `homeEmail` and `otherEmail` attributes.

The following known limitations apply:

- Clearing fields on updates is not supported.
- Outbound Group Provisioning and Memberships are not supported.
- Patch updates to SCIM-enabled target applications are not supported.
- There is a limit of one value per type (such as home, work, or other) for multivalue attributes such as `email`, `phone`, and `address`.
- Unexpected behavior may occur if the SaaS does not specify either type and primary information, or both type and primary information for multivalue attribute such as such as `email`, `phone`, and `address`. Also, existing SaaS attributes might not be removed during an Update, and the desired value might not be correctly set as primary.
- SCIM-compliant service providers can implement or interpret SCIM standards differently, which can result in behavior that is not consistent with the intended use of the SCIM SaaS Provsioner.

Learn more in SCIM Provisioner.

Zoom Connector 1.2

Improved PingOne for Enterprise

Copyright © 2025 Ping Identity Corporation

We added a feature to restore the user's Zoom license when the user is re-enabled.

The following known issues apply:

- The Zoom Provisioner does not support group provisioning.
- User attributes cannot be cleared once set. They can only be updated.
- Zoom only allows a single value for the `Roles` attribute.
- Deleting the administrative user that is set up for provisioning may lead to undesired consequences. The provisioner makes the administrative user the owner and member of each group that is created by the provisioner. We recommend not deleting the administrative user and not managing this user through the provisioner.
- Zoom does note allow attribute updates for users with a "disabled" status. To update attributes, re-enable the user first.
- Zoom does not allow users with the admin role to be disabled or deleted. Change the user's role first.

Learn more in Zoom Provisioner.

November 2022

Export a report of applications by group access

Improved PingOne for Enterprise

You can now export a `.csv` report of configured applications and the user groups assigned to access them. This can be useful for filtering purposes if you have a large number of active applications.

For more information, see Exporting a report of applications by group.

September 2022

Managed accounts certificate notifications

Improved PingOne for Enterprise, PingOne SSO for SaaS Apps

If you have a PingOne for Enterprise for Managed Service Providers or PingOne SSO for SaaS Apps with Managed Accounts license, you can now enable your administrators to receive email notifications when your customer accounts have certificates that are about to expire or have expired.

For more information, see Editing administrative roles, permissions, and notifications.

August 2022

Custom application and customer connection secrets

New PingOne SSO for SaaS Apps

Copyright © 2025 Ping Identity Corporation

You can now generate client secret values for each application and customer connection API connection.

This ability improves security over using a single set of client credentials for all connections.

> **Note**
>
> This feature is currently in limited release. To request access to this feature, open a support case.

For more information, see Creating or editing application-specific credentials and Creating or editing additional Connection API credentials.

PingOne for Enterprise Directory self-registration

Improved PingOne for Enterprise

You can now configure how long the email invitation remains valid for new self-registering PingOne for Enterprise Directory users.

You can set the duration between 1 hour and 168 hours. The default duration is 24 hours.

For more information, see Allow self registration for new directory users.

Custom Entity ID

Info PingOne SSO for SaaS Apps

The ability to define a custom entity ID for applications that are enabled through PingOne SSO for SaaS Apps is now available to all customers.

If a custom entity ID is in use by a non-multiplexed connection, it cannot be changed.

For more information, see Add or update other applications.

July 2022

ServiceNow Connector 2.3

Improved PingOne for Enterprise

Added support for the Rome and San Diego versions of ServiceNow.

The following known issues apply:

- Outbound Group Provisioning and Memberships are not supported.
- User attributes cannot be cleared once set. They can only be updated.

Copyright © 2025 Ping Identity Corporation

- When provisioning to ServiceNow, all user accounts in ServiceNow must have a `username` (User ID). This is not a required field in ServiceNow, but it is required for provisioning to work due to the provisioner using this field to sync with pre-existing users in ServiceNow. If a user in ServiceNow resolves to `sAMAccountName` (the "standard" mapping in the provisioning channel), then the accounts will be linked. Currently, if users exist in ServiceNow without a `username` that will cause errors in provisioning. You can resolve this by ensuring every user has the `username` field populated even if they are not intended to be managed by the provisioner.
- When provisioning users, the `username` attribute must only contain URL-safe characters.
- When synchronizing roles with users, the role attribute must contain only URL-safe charcters.
- If a new user is created with the same `username` as an existing user, a duplicate user will not be created. Instead, the existing user will be updated with any information in the create.
- Due to limitations with the ServiceNow API, a role can be added to a user, but not removed, which may cause a user's role in the source datastore to become out-of-sync with the user's role in ServiceNow. Learn more in ServiceNow Provisioner.
- When mapping the roles attribute multiple additional calls to ServiceNow must be made to sync user role. This may impact provisioning performance.
- For departments that contain the `^` character in the name, the ServiceNow API causes the creation of multiple departments with the same name.
- For the department and location objects, the ServiceNow API ignores capitalization. When provisioning a user that matches multiple departments or locations in ServiceNow (such as `Accounting` and `accounting`), PingFederate provisions the user with an empty department or location attribute and logs an error in `provisioner.log`.

March 2022

PingID admins multi-factor authentication (MFA) bypass

New PingOne for Enterprise

Added an optional permission to allow PingID Device Administrators to grant temporary MFA bypass to users.

To enable this permission, go to **Account > Administrators > Permissions** and select **Allow Bypass**.

For more information, see Administrative roles.

Google Workspace Provisioner improvements

Improved PingOne for Enterprise

Added the following improvements to the Google Workspace Provisioner:

- Added the ability to disable and delete users
- Added the ability to provision disabled users
- Added the ability to remove user actions

Copyright © 2025 Ping Identity Corporation

- Added support for Google Admin SDK 1.32.1

The following known issues apply:

- User attributes cannot be cleared once set.
- Google does not properly handle creating users with an invalid `addressCountry` value.
- The Provisioner sends the value of `work` for the `Organization` type. However Google does not retain this value. and as a result the *Organization* type has no value.
- Google treats certain user attributes as complex data sets:
  - Address (address* attributes)
  - Organization (org* attributes)
  - Phone (work* attributes)

  Any unmapped or empty fields within a complex data set will be cleared in the corresponding Google account.

New report type

New PingOne for Enterprise

Added a new report type for PingOne for Enterprise for Managed Service Providers accounts.

The **SSO Summary by Customer** report displays unique users and SSO transactions for each of your customer accounts.

For more information, see PingOne for Enterprise report types.

New report type

New PingOne for Enterprise

The **SSO User Summary** report displays a list of all unique users who have used SSO during the defined period.

> **Note**
>
> This feature is currently in limited release. To request access to this feature, open a support case.

For more information, see PingOne for Enterprise report types.

Application integration testing change

Info PingOne SSO for SaaS Apps

Changed the tenant used to generate test users from PingFederate to PingOne for Enterprise Directory.

Test user IDs and passwords will no longer automatically populate on the test IdP login site. You can find a complete list of test user IDs and their passwords in the documentation.

For more information, see Testing your application using the built-in IdP.

Copyright © 2025 Ping Identity Corporation

REST application customization

New PingOne SSO for SaaS Apps

Added an option to allow your customers to customize the **Default Application URL** and **Error URL** when they configure your REST application from the application catalog.

For more information, see Add or update other applications.

Previous PingOne for Enterprises releases

February 2022

Enhancements

Feature	Description
PingFederate Connection	The latest version of PingFederate available for download through PingOne for Enterprise is 10.3. You can download later versions of PingFederate from the Ping Identity main download site.
PingOne Connector	• Fixed an issue that caused an error when trying update the population ID attribute. See **Known Issues and Limitations** below for important information.
PingOne for Enterprise Directory	Notification emails sent to administrators when new users self-register now include a link to the **Users > User Directory > Users** menu where you can approve the new user. For more information, see Approve new directory users.

December 2021

Enhancements

Feature	Description
Azure Conditional Access	Added the `MFA_SUBJECT` attribute to the Microsoft Azure AD identity repository configuration. If you're using PingID for Azure Conditional Access, the `MFA_SUBJECT` attribute in PingOne for Enterprise can be mapped the same as the `username` attribute in PingID. For more information, see Connect to Azure and Configuring PingID MFA for Microsoft Azure AD Conditional Access in the PingID documentation.

Copyright © 2025 Ping Identity Corporation

Feature	Description
Office 365 Connector	Migrated the Office 365 Connector from the Azure AD Graph API 1.6 to the Microsoft Graph API 1.0 See **Known Issues and Limitations** below. Learn more in the Office 365 Connector documentation.
SSO Admins	Updated the **Account > Administrators** page to display all single sign-on (SSO) administrative users. Previously, SSO admins who were also registered in other PingOne for Enterprise accounts did not display. For more information, see Assign administrative roles.

Known issues and limitations

Subject	Issue/Limitation
Office 365 Connector	• Opting out of license management for users is not supported. The connector will clear existing licenses even when the attribute is unmapped. • Updating mobile attribute requires that the service principal representing the connector be assigned a role with Company Administrator privileges using Powershell. See this KB article for more information. • Updating the `Password` attribute is not supported. • User updates containing a manager that has not yet been provisioned or updated by the new version will fail. Older version updates will not have the new extended attribute with their distinguished name (DN) from Active Directory. • If the **DoBase64Conversion** field is switched to `false`, conflicts or failures will likely result on federated domains containing pre-existing users provisioned by dirsync/V1.0. • Only outbound provisioning is supported. • Group provisioning is not supported. • Automatic licensing of users is not supported.

Copyright © 2025 Ping Identity Corporation

October 2021

Enhancements

Feature	Description
PingOne Connector	• Changed the **North America** region to **North America (US)** • Added the **North America (Canada)** region See **Known Issues and Limitations** below for important information.
SSO/SLO	Increased the `max-age` parameter of the `strict-transport-security` header for the `https://sso.connect.pingidentity.com/sso/` endpoint. The previous `max-age` was 1 year. The new `max-age` is 2 years.

Known issues and limitations

Subject	Issue/Limitation
PingOne Connector	• Clearing fields on updates is not supported. • Multivalued attributes such as email or address are not supported. Multiple values appear as a single array on PingOne. • Custom attributes are set when the user is initially created, and cannot be updated afterward.

September 2021

Enhancements

Feature	Description
Custom Application Categories	Added the ability to create custom application categories. Custom application categories let you organize applications in ways that work best for your organization. For more information, see Creating a custom application category.

Copyright © 2025 Ping Identity Corporation

Feature	Description
PingOne Connector	• Added support for group provisioning • Added the ability to select a default MFA device during user creation • Added voice as an option for offline device pairing • Fixed an issue that prevented all of a user's authentication methods from being provisioned if any of them were invalid. • Fixed an issue that allowed duplicate local attributes to be defined when configuring an adapter. • Fixed an issue that could cause an attribute containing an array of objects to be returned in the incorrect format. • Fixed an issue that caused password validation to fail intermittently when the user's access token had expired. See **Known Issues and Limitations** below for important information.
Single Logout	Added support for the optional `idpid` parameter to all single logout (SLO) endpoints. If you specify the `idpid` value, the SLO operation is restricted only to sessions with the specified `idpid` value. For more information, see PingOne for Enterprise and SLO.
SSO Admins	Updated the **Account > Administrators** page to display all single sign-on (SSO) administrative users. Previously, SSO admins who were also registered in other PingOne for Enterprise accounts did not display. For more information, see Assign administrative roles.

Known issues and limitations

Subject	Issue/Limitation
PingOne Provisioner	Clearing fields on updates is not supported. Multivalued attributes, such as emails and addresses, are not supported. Multiple values appear as a single-array value in PingOne. Custom attributes are set when the user is initially created. They cannot be updated after they are set.

August 2021

Enhancements

Feature	Description
PingOne Provisioner	Added support for custom string attributes. See Known Issues and Limitations below for important information.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
PingOne Provisioner	Clearing fields on updates is not supported. Multivalued attributes, such as emails and addresses, are not supported. Multiple values appear as a single-array value in PingOne. Custom attributes are set when the user is initially created. They cannot be updated after they are set.

July 2021

Enhancements

Feature	Description
Admin Portal Banner	Added a feature allowing you to display a banner message in the administrative portal. For more information, see Adding a logo and banner message.

June 2021

Enhancements

Feature	Description
Single Logout Flow	Added a feature allowing administrators to choose how PingOne for Enterprise handles single logout (SLO) requests. For more information, see Configure the dock when using PingOne for Enterprise Directory and Configuring the dock when using an identity bridge.
PingID Device Administrator Role	Added a new administrative role to manage user PingID Device settings. For more information, see Assign administrative roles.
Read-Only Administrative Roles	Added a feature allowing you to assign user groups to read-only versions of administrative roles. Read-only roles allow administrators to access the areas of the admin portal normally allowed by that role, but not to change settings. For more information, see Configuring SSO to the PingOne for Enterprise admin portal.
Password Policy	Changed the default password requirements for new accounts. Previous default settings required a minimum password length of 6 characters, with no requirement for special characters. New default settings require a minimum password length of 8 characters, and a minimum of one special character. This change only applies to new accounts.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
Single Logout Flow	Single logout from the admin portal does not currently support redirect SLO flow. If you select **Redirect** SLO flow for your users, your SSO admins should use the **Sign Off** button at the top right of the admin portal rather than signing off through the PingOne Dock.

May 2021

Enhancements

Feature	Description
Admin-API Client	Removed the ability to use special characters in the **Client Name** and **Description** fields when creating API clients. Special characters in these fields can present a security risk. If you have existing API clients that include special characters, you will be forced to remove the characters the next time you edit the client. For more information, see Creating an Admin-API client.
Password Policy Customization	Added a feature giving PingOne for Enterprise for Managed Service Providers administrators the ability to permit their customer accounts to customize password policies. For more information, see Configuring customer account service settings.

April 2021

Enhancements

Feature	Description
Admin-API Client	Removed the ability to use special characters in the **Client Name** and **Description** fields when creating API clients. Special characters in these fields can present a security risk. If you have existing API clients that include special characters, you will be forced to remove the characters the next time you edit the client. For more information, see Creating an Admin-API client.
Password Policy Customization	Added a feature giving PingOne for Enterprise for Managed Service Providers administrators the ability to permit their customer accounts to customize password policies. For more information, see Configuring customer account service settings.

Copyright © 2025 Ping Identity Corporation

March 2021

Enhancements

Feature	Description
OAuth Access Token	Increased the allowed number of trusted origins for OAuth access token Cross-Origin Resource Sharing. The previous limit was 10. The current limit is 100. For more information, see Configuring your OAuth settings.
PingOne for Customers Provisioner	Added a new provisioner for PingOne for Customers. This provisioner includes: • Authoritative IdP attribute • Default nicknames for email and SMS Learn more in PingOne Integration Kit.
Self-Service Password Reset	Reduced the lifetime of self-service user password reset from the sign on screen. Previously the password reset link was valid for 3 days. Currently the password reset link is valid for 24 hours.

Known issues and limitations

Subject	Issue/Limitation
PingOne for Customers Provisioner	• Clearing fields on updates is not supported.

December 2020

Enhancements

Feature	Description
Aquera Provisioner	Added a new provisioner for Aquera Connector. This is the initial release for this provisioner. This provisioner includes: • Support for user provisioning • Support for SCIM core and enterprise attributes • Support for bearer token and HTTP basic authentication • configuration options for deprovisioning actions Learn more in Aquera Provisioner
SCIM SaaS Provisioner	Fixed application/JSON headers for SCIM 1.1 requests. Added logic to avoid sending an empty `FormattedName` attribute. Learn more in SCIM Provisioner.

Copyright © 2025 Ping Identity Corporation

Feature	Description
ServiceNow Provisioner	Added support for the Orlando and Paris versions of Service Now. Learn more in ServiceNow Provisioner.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
ServiceNow Provisioner	• Outbound Group Provisioning and Memberships is not supported. • Once set, user attributes cannot be cleared, only updated • When provisioning to ServiceNow, all user accounts in ServiceNow must have a `UserName` (User ID). This is not a required field in ServiceNow, but it is required for provisioning to work due to the provisioner using this field to sync with pre-existing users in ServiceNow. If a user in ServiceNow resolves to `sAMAccountName` (the "standard" mapping in the provisioning channel), then the accounts will be linked.Users in ServiceNow without a `UserName` will cause errors in provisioning. Resolve this by ensuring every user has this field populated, even if they are not intended to be managed by the provisioner. • When provisioning users, the `UserName` attribute must only contain URL-safe characters. • When synchronizing roles with users, the role attribute must contain only URL-safe characters. • If a new user is created with the same `UserName` as an existing user, a duplicate user will not be created. Instead, the existing user will be updated with any information in the creation. • Due to limitations with the ServiceNow API, a role can be added to a user but not removed. This may cause a user's role in the source datastore to become out-of-sync with the user's role in ServiceNow. Learn more in ServiceNow Provisioner. • When mapping the `roles` attribute, multiple additional calls to ServiceNow must be made to sync user role. This may impact provisioning performance. • For department names that contain the ^ character, the ServiceNow API causes the creation of multiple departments with the same name. • For the `department` object, the ServiceNow API ignores capitalization. When provisioning a user that matches multiple departments in ServiceNow (such as Accounting and accounting), PingFederate provisions the user with an empty department attribute and logs an error in `provisioner.log`.

Copyright © 2025 Ping Identity Corporation

Subject	Issue/Limitation
SCIM SaaS Provisioner	• Clearing fields on updates is not supported. • Outbound Group Provisioning and Memberships is not supported. • Patch updates to SCIM-enabled target applications are not supported. • Multivalue attributes such as email, phone, and address have a limit of one value per type, such as home, work, or other. • For multivalue attributes such as email, phone, and address, if the SaaS does not specify either type and primary information, or both type and primary information, the provisioner may behave in unexpected ways. Also, existing attributes on the SaaS might night be removed during an updated, and the desired value might not be correctly set as primary. * SCIM-compliant service providers may implement or interpret the SCIM standards differently. This can result in behavior that is not consistent with the intended use of the SCIM SaaS Provisioner. * The SCIM provisioner will not provision users until the users are updated.

November 2020

Enhancements

Feature	Description
Authentication Policy	Added a feature that allows you to choose whether to authenticate SSO admins using their email or their SSO username. For more information, see Create or update an authentication policy.
Administrator Settings	Added a feature that allows you to change the certificate expiration notification settings for Global and SaaS administrators. For more information, see Editing administrative roles, permissions, and notifications and Manage your user profile.
Subscription API	Added a new result status to PingID audit events. `UNSUCCESSFUL_ATTEMPT` represents an invalid one-time passcode (OTP) attempt that did not result in failed authentication. For more information about audit events, see Get the audit events for a Poll subscription.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
Single Logout	PingOne for Enterprise's single logout (SLO) implementation relies on the ability to send cookies within an iframe. Safari now blocks this function by default, which causes SLO to fail in most scenarios. We are working to accommodate this new behavior. This issue impacts SLO on the following browsers: • Safari 13.1+ on MacOS • Safari on iOS and iPadOS 13.4+ • Any browser where the user has disabled third party cookies You can solve this problem by enabling third-party cookies in the browser settings.

October 2020

Enhancements

Feature	Description
Admin-API Clients	Added a feature that allows you to create Admin-API clients to access subscription endpoints without the need for additional administrator accounts. For more information, see Creating an Admin-API client
AWS Single Sign-On Provisioner	Added a new provisioner for AWS Single Sign-On. This is the initial release for this provisioner. This provisioner includes: • Included support for user provisioning • Included configuration for deprovisioning actions See Known Issues and Limitations below for important information. For more information, see Overview of the AWS Single Sign-On Connector.
PingOne Directory	Added a feature that directs a user to the specified redirect URL if they click on the registration URL after completing the registration process. For more information about self-registration, see Allow self registration for new directory users.
Signing Certificates	Added a feature that allows administrators to designate a signing certificate as the default certificate for newly added application connections. For more information, see Create a signing certificate and View certificate details.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
AWS Single Sign-On Provisioner	• This integration does not support group provisioning • Once set, user attributes cannot be cleared, only updated

July 2020

Enhancements

Feature	Description
PingOne Directory	Added a feature that allows administrators to enable additional directory attributes for use in attribute mapping for IdP, dock, and application configuration. For more information, see Manage directory attributes.
PingOne Provisioner	• Changed name from PingOne for Customers Provisioner to PingOne Provisioner • Added the ability to manage PingOne MFA Email and SMS devices

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
PingOne Provisioner	• Clearing fields on updates is not supported. • Outbound Group Provisioning and Memberships is not supported. • Patch updates to SCIM-enabled target applications are not supported. • There is a limit of one value per type (such as, home, work, other) for multivalue attributes (email, phone, address). • Unexpected behavior may occur if the SaaS application does not specify either type and primary information, or both type and primary information for multivalue attributes (email, phone, address). Also, existing attributes on the application may not be removed during an update, and the desired value may not be correctly set as primary. • SCIM-compliant service providers may implement or interpret the SCIM standards differently. This can result in behavior that is not consistent with the intended use of the SCIM SaaS provisioner.

July 2020

Enhancements

Feature	Description
Concur 1.0.1	• Fixed an issue that prevented users from being updated in Concur. Learn more in Concur Provisioner.

Copyright © 2025 Ping Identity Corporation

June 2020

Enhancements

Feature	Description
Atlassian Cloud Provisioner	• Initial release • Includes SAML 2.0 support for IdP- and SP-initiated SSO • Included support for user provisioning • Included configuration for deprovisioning actions • Learn more in Atlassian Cloud Provisioner.
ServiceNow Connector 2.2	• Added the ServiceNow URL field and removed the ServiceNow Instance Name field • Fixed an issue that caused an error when assigning a role that was not also assigned to the provisioning user account • Added support for the Orlando version of ServiceNow • Learn more in ServiceNow Provisioner.

Known issues and limitations

Subject	Issue/Limitation
Atlassian Cloud Provisioner	• Clearing fields on updates is not supported • This integration does not support group provisioning • Once set, user attributes can only be updated, not cleared

May 2020

Enhancements

Feature	Description
Code42 Provisioner	• Initial release. • Included support for user provisioning. • Learn more in Code42 Integration Guide for PingFederate.

Copyright © 2025 Ping Identity Corporation

Feature	Description
ZScaler Private Access Provisioner	• Initial release. • Included support for user provisioning. • Included configuration for deprovisioning actions. • Learn more in Zscaler Private Access Provisioner.

Known issues and limitations

Subject	Issue/Limitation
Code42 Provisioner	• User attributes cannot be cleared once set. They can only be updated. • This integration does not support group provisioning. • Deleting the administrative user that is set up for provisioning may lead to undesired consequences. The provisioner makes the administrative user the owner and member of each group that is created by the provisioner. We recommend not deleting the administrative user and not managing this user through the provisioner.
Zscaler Private Access Provisioner	• This integration does not support group provisioning. • Once set, user attributes can only be updated, not cleared. • Deleting the administrative user that is set up for provisioning may lead to undesired consequences. The provisioner makes the administrative user the owner and member of each group that is created by the provisioner. We recommend not deleting the administrative user and not managing this user through the provisioner.

April 2020

Enhancements

Feature	Description
AD Connect agent management	• Added a feature allowing administrators to view and manage AD Connect nodes from PingOne portal. See View and manage AD Connect agent nodes for more information.

Copyright © 2025 Ping Identity Corporation

Feature	Description
Metadata Download URL	• Added a feature to generate a shareable metadata URL for applications and the configured SAML IdP. See Adding or updating a SAML application and Connecting to a custom SAML provider for more information.
Session Idle Timeout	• Added a setting to the **Setup > Dock** menu allowing administrators to set the time that a user session can be idle before the session is automatically signed out.
Slack Connecter	• Added Support for handling rate-limiting responses from Slack.
Zoom Connector 1.0	• Initial release. • Included support for user provisioning. • Included support for Zoom attributes. • Included support for API key and secret authentication. • Included configuration options for deprovisioning actions. • Learn more in Zoom Provisioner.

Known issues and limitations

Subject	Issue/Limitation
Zoom Connector 1.0	• This integration does not support group provisioning. • Once set, user attributes can only be updated, not cleared. • Zoom only allows a single value for the `Roles` attribute. • Deleting the administrative user that is set up for provisioning may lead to undesired consequences. The provisioner makes the administrative user the owner and member of each group created by the provisioner. We recommend not deleting the administrative user and not managing the user through the provisioner. • Due to a limitation in Zoom, if a user's attributes change at the same they are enabled or disabled, only the `disabled` status is updated in Zoom. The attributes are updated the next time a change is made to that user. • Zoom does not allow users with the admin role to be disabled or deleted. Change the user's role first.

Copyright © 2025 Ping Identity Corporation

March, 2020

Enhancements

Feature	Description
SCIM Provisioner	• Added support for the application/scim+json HTTP header type • Improved the SCIM URL field in the connection configuration to work either with or without a trailing slash (/) in the URL
Zscaler ZIA Provisioner 1.1	• Renamed the integration to "Zscaler Internet Access" to match official branding • Added the ability to update the username attribute in Zscaler • Improved error handling and reporting when encountering a user that does not have an ID

Known issues and limitations

Subject	Issue/Limitation
Zscaler ZIA Provisioner 1.1	The following limitations apply: • Clearing fields on updates is not supported. • Deleting the administrative user that is set up for provisioning may lead to undesired consequences. The provisioner makes the administrative user the owner and member of each group that is created by the provisioner. We recommend not deleting the adminstrative user and not managing this user through the provisioner.

January, 2020

Enhancements

Feature	Description
Branding	We've expanded the branding options for the PingOne dock as well as the AD Connect and PingOne Directory login screens. We have also added new branding options for intermediate SSO screens including error, SLO, and IdP Discovery screens. Finally we have reorganized the branding screens in the PingOne admin portal. See Assign branding and design for more information.

Copyright © 2025 Ping Identity Corporation

Resolved issues

Ticket ID	Issue
SSD-12791	Fixed an issue to allow non-HTTPS URI redirects in OIDC mobile applications.

November, 2019

Enhancements

Feature	Description
OAuth refresh tokens	We've added support for OAuth refresh tokens with OpenID Connect applications. See Configuring your OAuth settings and Adding or updating an OIDC application for more information.
Updated provisioner for ServiceNow	We've updated the provisioner for Salesforce. The update to this provisioner includes support for: • Added support for the London, Madrid, and New York versions of ServiceNow. • Added support for mapping users to departments in ServiceNow. • Improved user ID validation when updating and deleting users. • Removed support for the Jakarta and Istanbul versions of ServiceNow. **Note** This is an update to the existing ServiceNow provisioner (Kingston, Jakarta, Istanbul). It has also been rebranded from "ServiceNow (Kingston, Jakarta, Istanbul)" to "ServiceNow". See **Known Issues and Limitations** for important information.
Delegated administration of applications	We've added an Application Administrator role and the ability for you to delegate administration of applications to an Application Administrator. See Assign Application Administrator applications for more information.
SLO for OpenID Connect applications	We've added single logout (SLO) support for OpenID Connect (OIDC) applications. See the **Logout URI** when adding an OIDC application, or Adding or updating an OIDC application for more information.
Disable inactive users in PingOne directory	We've added the ability for you to disable users who've been inactive for an extended period of time. See Disable directory users for more information.

Resolved issues

Ticket ID	Issue
IO-5615	(Slack provisioner) Fixed an issue that caused the connector to update the wrong phone number attribute as a result of a change in the Slack API.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
SSD-12509	Fixed an issue in Google Chrome where a SameSite=none setting in cookies was affecting SSO.
SSD-12579	Fixed an issue where PingOne directory error messages weren’t displaying single quotes.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Copyright © 2025 Ping Identity Corporation

Subject	Issue/Limitation
ServiceNow provisioner	The following limitations apply: • For departments that contain the "^" (caret) character in the name, the ServiceNow API causes the creation of multiple departments with the same name. • For the department object, the ServiceNow API ignores capitalization. When provisioning a user that matches multiple departments in ServiceNow (such as, Accounting and accounting), PingOne provisions the user with an empty department attribute and logs an error in the Dashboard Report. • `Outbound Group Provisioning` and `Memberships` are not supported. • User attributes cannot be cleared once set. They can only be updated. • When provisioning to ServiceNow, all user accounts in ServiceNow must have an assigned `username` (User ID) value. This is not a required field in ServiceNow. However, because the provisioner must use this field to sync with pre-existing users in ServiceNow, it is required for provisioning to function. If a user in ServiceNow resolves to sAMAccountName (the "standard" mapping in the provisioning channel), the accounts will be linked. Currently, if users exist in ServiceNow without an assigned UserName value, this will cause errors in provisioning. In this case, you can resolve the issue by ensuring every user has an assigned UserName, even if they are not intended to be managed by the provisioner. • When provisioning users, the `username` attribute must contain only URL-safe characters. • When synchronizing roles with users, the `role` attribute must contain only URL-safe characters. • If a new user is created with the same `username` as an existing user, a duplicate user will not be created. Instead, the existing user will be updated with any information assigned. • Due to limitations with the ServiceNow API, a role can be added to a user but not removed, which may cause a user's role in the source data store to become out of sync with the user's role in ServiceNow. For more information, see Adding the Ping Identity provisioning role in ServiceNow. • When mapping the `roles` attribute, multiple calls to ServiceNow must be made to sync the user role information. This may impact provisioning performance.

Copyright © 2025 Ping Identity Corporation

September, 2019

Enhancements

Feature	Description
Adding OIDC applications	We've updated the selection and configuration of OIDC applications, streamlining this process based on the type of OIDC application connection you want to add. See Adding or updating an OIDC application for more information.
Encryption certificates	We've added management of encryption certificates to the certificate management page (**Setup > Certificates**). You can choose the encryption certificate used for an application. See Update an encryption certificate for more information.
Administrators and SSO	We've updated the Administrators page so that when an assigned administrator first signs on (SSO) to the admin portal, they're automatically added to the list of administrators displayed on the **Account > Administrators** page. See Assign administrative roles for more information.
Browser extension updated	The browser extension (used for Basic SSO password vaulting) has been updated to version 2.54.9. This update included a fix for an unexpected prompt to restart the browser extension.
Updated provisioner for Salesforce	We've updated the provisioner for Salesforce. The update to this provisioner includes support for: • Provisioning to Salesforce Community Cloud (customer, partner, and custom communities). • Provisioning to custom Salesforce domains. • Version 46.0 of the Salesforce REST API. • Configuring options to manage permission sets by merging or overwriting. • Additional salesforce attributes. • Improved error handling and reporting for cases where users in the target application do not have an ID. • Improved error handling and reporting for cases where groups are updated or deleted but do not exist in the target application.See **Known Issues and Limitations** for important information.

Resolved issues

Ticket ID	Issue
(Browser extension) Staging-8549	Fixed an issue where users were unexpectedly prompted to restart the browser extension.
IO-5467	Fixed an issue that prevented users with certain special characters from being provisioned to Salesforce.
SSD-12043	Fixed an issue where the SAML_SUBJECT attribute was not appearing in the attributes dropdown list in Advanced Attribute Mapping mode.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
Salesforce provisioner	The following limitations apply: • The provisioner cannot clear user attributes once they have been set. • This provisioner does not support custom attributes. • The Salesforce provisioner does not support hard deleting users in Salesforce. When users are enabled/disabled or deleted in your user store, the user will only be soft deleted (enabled/disabled) accordingly in Salesforce. • The `username` attribute must be in an email format. • The `alias` attribute can be no more than 8 characters. • Group provisioning is not supported. • 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 will cause the provisioner 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. • Salesforce Communities: ◦ The provisioner can link users to "customer" and "partner" business accounts, but not to "person" accounts. See *Accounts* in the Salesforce documentation.

July, 2019

Enhancements

Feature	Description
PingOne directory user passwords	We've updated the PingOne directory user password process for new users. Now after you create a new user, the user must change their assigned password when they first sign on. See Add directory users for more information.

Copyright © 2025 Ping Identity Corporation

Feature	Description
Updated provisioner for WebEx®	We've updated the provisioner for WebEx. The update to this provisioner includes: • Fixed an issue that prevented users with special characters from being provisioned to WebEx. • Improved error handling and reporting for cases where users in the target application do not have an ID. • Improved error logging security. • Fixed an issue that caused a user to be recreated when the provisioning engine tried to delete or disable a user that was already deleted in WebEx.See **Known Issues and Limitations** for important information.
Updated provisioner for Amazon Web Services	We've updated the provisioner for Amazon Web Services (AWS). The update to this provisioner includes: • Support for the AWS 2.0 API. • Support for the Password and PasswordResetRequired attributes. • Support for updating the UserName attribute. • Improved error-handling and reporting behavior.See **Known Issues and Limitations** for important information.
PingFederate Bridge	PingFederate Bridge is now the default PingFederate identity bridge for PingOne. It's a light-weight version of PingFederate designed for quick and easy configuration with PingOne. See .pingidentity.com/pingfederatebridge/pf93///[Introduction to PingFederate Bridge] and Connect to PingFederate for more information.
Admin portal SSO for multiple groups	You can now assign multiple groups to administrative roles for the purpose of SSO to the PingOne admin portal from the PingOne dock. We've also created a new page for this assignment: **Setup > Dock > Admin Portal SSO**. See Configure SSO from the dock to the admin portal for more information.
Ping directory branding	We've added the ability for you to brand PingOne directory pages for your organization. See Assign directory branding and designs for more information.
SSO reports	You can now apply filtering to SSO reports based on specific applications. See Run a predefined report or Run a custom report for more information.
Supported languages	PingOne UI components now support the use of more languages. See PingOne for Enterprise language support for more information.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
WebEx provisioner	The following limitations apply: • The provisioner cannot re-enable user meeting types that have been disabled through the Webex administration console. If the provisioner tries to update the user's meeting types in this scenario, it can cause all meeting types for that user to be disabled. • The WebEx ID attribute is not updateable in PingOne. • The MeetingType attribute is limited to one value in PingOne (not a multivalued attribute). • Due to API Limitations, WebEx doesn't allow a user to be created in a suspended state. WebEx will automatically activate the user after it is created.
Amazon Web Services provisioner	The following limitations apply: • Group Provisioning is not supported. • Deprovisioning: ◦ AWS does not support disabled users. These users are deleted instead. • Attributes: ◦ When a user is created with a passwordResetRequired value other than "true" or "TRUE", the provisioning connector sets the value to "false" in AWS. ◦ Clearing fields on updates is not supported.

June, 2019

Enhancements

Feature	Description
PingFederate Bridge	PingFederate Bridge is now the default PingFederate identity bridge for PingOne. It's a light-weight version of PingFederate designed for quick and easy configuration with PingOne. See .pingidentity.com/pingfederatebridge/pf93///[Introduction to PingFederate Bridge] and Connect to PingFederate for more information.
Admin portal SSO for multiple groups	You can now assign multiple groups to administrative roles for the purpose of SSO to the PingOne admin portal from the PingOne dock. We've also created a new page for this assignment: **Setup > Dock > Admin Portal SSO**. See Configure SSO from the dock to the admin portal for more information.

Copyright © 2025 Ping Identity Corporation

Feature	Description
Ping directory branding	We've added the ability for you to brand PingOne directory pages for your organization. See Assign directory branding and designs for more information.
SSO reports	You can now apply filtering to SSO reports based on specific applications. See Run a predefined report or Run a custom report for more information.
Supported languages	PingOne UI components now support the use of more languages. See PingOne for Enterprise language support for more information.
Basic SSO option	We've added an option for you to enable Basic SSO on the **Setup > Dock > Configurations** page in the admin portal. When enabled, you'll use the browser extension to add apps for Basic SSO. See Basic SSO (password vaulting) for more information.
Basic SSO browser extension new field available	We've updated the browser extension used for Basic SSO apps to support an additional field for use when training the browser extension to sign on to a Basic SSO app. The additional (third) field is optional and is supplied for those apps that require sign-on information in addition to the user name and password fields.

Resolved issues

Ticket ID	Issue
IO-5262	(Provisioning) Fixed an issue where disabling users in the user source without a synchronized user in a target SaaS could result in a new user being created in the SaaS. The affected PingOne apps are: • Amazon Web Services • Box • Concur • Dropbox • Egnyte • Github • Google • Lucidchart • Office 365 • Ping IDaaS Directory Provisioner • PingOne for Customers Provisioner • Ping IDaaS Generic Scim Provisioner • Salesforce • ServiceNow Jakarta • Slack • WebEx • Workplace by Facebook • Zendesk • Zscaler

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
SSD-11699	Fixed an issue in PingOne directory where a user having the same email address could not be recreated being deleted.

May, 2019

Enhancements

Feature	Description
Basic SSO option	We've added an option for you to enable Basic SSO on the **Setup > Dock > Configurations** page in the admin portal. When enabled, you'll use the browser extension to add apps for Basic SSO. See Basic SSO (password vaulting) for more information.
Basic SSO browser extension new field available	We've updated the browser extension used for Basic SSO apps to support an additional field for use when training the browser extension to sign on to a Basic SSO app. The additional (third) field is optional and is supplied for those apps that require sign-on information in addition to the user name and password fields.
Updated provisioner for PingOne for Customers	We've updated the provisioner for PingOne for Customers. This provisioner is intended for existing PingOne for Enterprise accounts using either PingOne directory or AD Connect who want to migrate their users to PingOne for Customers. The update to this provisioner includes: • Fixed an issue that prevented users with empty attributes from being provisioned to PingOne for Customers. • Removed support for obsolete scopes from the provisioner.See **Known Issues and Limitations** for important information.

Resolved issues

Ticket ID	Issue
BE-2752	(Browser extension) Fixed an issue where the browser extension wasn't properly replaying an app in Chrome resulting in the Login button not functioning.
SSD-11636	Fixed an issue where a CSR response could not be uploaded to PingOne.
SSD-11595	Fixed an issue where the PingOne attribute mapping for PingFederate defaulted to `sub` instead of `SAML_SUBJECT` as expected.
SSD-11570	Fixed an issue where the activation key for a PingOne 30 day trial account was not accepted by PingFederate.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
SSD-11351	Fixed an issue where a routing for a PingFederate connection was being retained to a Ping data center that was no longer being used.

Known issues and limitations

Subject	Issue/Limitation
PingOne for Customers provisioner	The following limitations apply: * Clearing fields on updates is not supported. * Outbound Group Provisioning and Memberships is not supported. * Patch updates to SCIM-enabled target applications are not supported. * There is a limit of one value per type (such as, home, work, other) for multivalue attributes (email, phone, address). * Unexpected behavior may occur if the SaaS application does not specify either type and primary information, or both type and primary information for multivalue attributes (email, phone, address). Also, existing attributes on the application may not be removed during an update, and the desired value may not be correctly set as primary. * SCIM-compliant service providers may implement or interpret the SCIM standards differently. This can result in behaviour that is not consistent with the intended use of the SCIM SaaS provisioner.

April, 2019

Enhancements

Feature	Description
PingOne registration page	We've updated the UI for the registration page, administrator login, and password recovery. Most importantly, we've added the selection of the PingOne data center to use for the new account. See Registering a PingOne for Enterprise account for more information.

Copyright © 2025 Ping Identity Corporation

Feature	Description
Identity repository setup	We've updated the UI for identity repository setup and added an attribute mapping option enabling you to configure the attribute mapping from the identity provider to the standard set of PingOne SSO attributes.
Microsoft include::pingone_for_enterprise:partial$p14e_p1refs_azure.adoc[tags=Azure]identity bridge	We've added an identity bridge for Azure, with the option to synchronize groups from your Azure tenant to PingOne for Enterprise. See Connect to Azure for more information.
Microsoft ADFS identity bridge	We've added an identity bridge for Active Directory Federation Services (ADFS). See Connect to ADFS for more information.
Group assignment	You can now authorize groups for application access as part of the application setup for SAML, OIDC, or Application Catalog applications.
Pingone directory self-registration	If you're using PingOne directory as your identity repository, you can now assign the email domains that can be used for self-registration. If you choose not to assign the email domains, then all domains can be used for self-registration. See Allow self registration for new directory users for more information.
Cross-origin resource sharing (CORS) for OpenID Connect	If you're integrating OpenID Connect (OIDC) applications with PingOne, you can now configure one or more trusted origins to enable cross-origin resource sharing (CORS). See Configuring your OAuth settings for more information.

Copyright © 2025 Ping Identity Corporation

Feature	Description
SAML response signing	If you're integrating SAML applications with PingOne, you can now configure whether PingOne for Enterprise signs the SAML assertion or the SAML response that is sent to the application during SSO. See Adding or updating a SAML application for more information.

Resolved issues

Ticket ID	Issue
SSD-10739	(Ping directory) Fixed an issue where a user was invited and confirmed the email activation, but the user wasn't provisioned to Ping directory until another user was created or invited.
SSD-11230	Fixed an issue where the SAML response signing selection for existing connections defaults to signing the assertion.

March, 2019

Enhancements

Feature	Description
SCIM SaaS provisioner	We've updated the provisioner for SCIM SaaS applications. This provisioner includes: • Configuration options for the Unique User Identifier (userName or workEmail) which is used to search for users in the target application.See **Known Issues and Limitations** for important information.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
PingOne for Customers provisioner	The following limitations apply: • Clearing fields on updates is not supported. • Outbound Group Provisioning and Memberships is not supported. • Patch updates to SCIM-enabled target applications are not supported. • There is a limit of one value per type (such as, home, work, other) for multivalue attributes (email, phone, address). • Unexpected behavior may occur if the SaaS application does not specify either type and primary information, or both type and primary information for multivalue attributes (email, phone, address). Also, existing attributes on the application may not be removed during an update, and the desired value may not be correctly set as primary. • SCIM-compliant service providers may implement or interpret the SCIM standards differently. This can result in behaviour that is not consistent with the intended use of the SCIM SaaS provisioner.

February, 2019

Enhancements

Feature	Description
New provisioner for PingOne for Customers	We've added a new provisioner for PingOne for Customers. This provisioner is intended for existing PingOne for Enterprise accounts using either PingOne directory or AD Connect who want to migrate their users to PingOne for Customers. This provisioner includes: * Support for user provisioning. * Support for user attributes: Username, Email, Population ID, Account ID, City, Country, External ID, First Name, Force Change Password, Full Name, Honorific Prefix, Honorific Suffix, Job Title, Last Name, Locale, Middle Name, Mobile Phone, Nickname, Password, Preferred Language, Primary Phone, Profile Image, State/Region, Street Address, Timezone, User Type and ZIP Code.See **Known Issues and Limitations** for important information.

Copyright © 2025 Ping Identity Corporation

Resolved issues

Ticket ID	Issue
SSD-10517	Fixed an issue where user provisioning to PingOne directory failed when switching to the PingOne directory from either a PingFederate or AD Connect identity bridge.

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

Known issues and limitations

Subject	Issue/Limitation
PingOne for Customers provisioner	The following limitations apply: • Clearing fields on updates is not supported.

January, 2018

Enhancements

Feature	Description
OpenID Connect custom scopes	We've added OAuth configuration settings for OpenID Connect applications to enable you to define custom scopes or to modify existing scopes with custom or standard claims. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Configure the access token].
PingOne redirect URI	We've updated the PingOne redirect URI to include a verification code unique to your account. The redirect URI used by your OpenID Connect provider for PingOne must include the verification code for SSO to be successful. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Connect to OpenID Connect].

Copyright © 2025 Ping Identity Corporation

Feature	Description
Audit & Report administrator	We've added a dedicated administrator role for working with the audit event streaming and polling capabilities. The Audit & Report administrator is restricted to accessing the PingOne Dashboard and the Reporting and Subscriptions pages. The Audit & Report administrator can also access the API for polling audit events when audit subscriptions are configured as polling subscriptions. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Assign administrative roles] and .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Managing reports and subscriptions].
SSO reporting	We've added new report types and predefined reports for SSO transactions. For more information, see .pingidentity.com/pingone/saasSsoAdminGuide/index.shtml//[Report types] and .pingidentity.com/pingone/saasSsoAdminGuide/index.shtml//[Report event information].

Resolved issues

Ticket ID	Issue
SSD-10353	Fixed an issue where access to the PingOne admin portal generated an error when the PingOne authentication policy applied multi-factor authentication for SSO to the admin portal.
SSD-10402	Fixed an issue that occurred while adding a new SAML application. The signing certificate selected during the configuration process was not being used for the signing certificate download link displayed on the summary page at the end of the configuration process. Instead, the download link used the default signing certificate.

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

Copyright © 2025 Ping Identity Corporation

December, 2018

Enhancements

Feature	Description
OpenID Connect custom scopes	We've added OAuth configuration settings for OpenID Connect applications to enable you to define custom scopes or to modify existing scopes with custom or standard claims. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Configure the access token].
PingOne redirect URI	We've updated the PingOne redirect URI to include a verification code unique to your account. The redirect URI used by your OpenID Connect provider for PingOne must include the verification code for SSO to be successful. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Connect to OpenID Connect].

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

November, 2018

Enhancements

Feature	Description
OpenID Connect query parameters	We've updated the OpenID Connect repository configuration to enable you to specify additional query parameters for the authentication request PingOne sends to the OpenID Connect provider. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Connect to OpenID Connect].
PingOne dock and SSO session lifetimes	We've updated the PingOne dock to use the same session lifetime as the SSO session. The PingOne dock and SSO session can now be set to as low as 15 minutes. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Configure the dock when using an identity bridge].
Turkish language support	We've updated the PingOne user interface to include support for Turkish. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[PingOne language support].

Copyright © 2025 Ping Identity Corporation

Resolved issues

Ticket ID	Issue
SSD-9795	Fixed an issue where users who are members of a large number of groups were unable to use SafeNet for multi-factor authentication.

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

October, 2018

Enhancements

Feature	Description
include::partial$p14e_p1refs_github.adoc[tags=Github]provisioner	We've a new provisioner for Github applications. This provisioner includes: • Added support for user provisioning. • Added support for user attributes: Username, Email, First Name, Last Name and External ID.See **Known Issues and Limitations** for important information.
Administrative auditing (reports and subscriptions)	Administrative auditing is now available PingOne for Enterprise, PingID and PingOne SSO for SaaS Apps. You can utilize the administrative audit events through both the Reports and the Subscriptions facilities .

Copyright © 2025 Ping Identity Corporation

Feature	Description
PKCE support for OpenID Connect (OIDC)	We've added support for Proof Key for Code Exchange (PKCE) to secure OIDC clients that cannot or choose not to use a client secret. We have therefore relaxed the requirement that a client secret must be specified when configuring an OIDC application with the authorization code flow. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Integrate an OIDC application, PKCE parameters] For more information, see .pingidentity.com/pingone/saasSsoAdminGuide/index.shtml//[Integrate an OIDC application, PKCE parameters].
SLO for OIDC identity providers	We've added single logout (SLO) support for PingOne for Enterprise OIDC identity providers (IdPs). You can specify the end-session URL through the well-known metadata of the OpenID Connect provider (end_session_endpoint), or when you configure the PingOne connection for the OIDC IdP. When SLO is triggered, PingOne redirects the user logout process to the end-session URL for the OIDC IdP.
Automatic IdP Discovery	We've added automatic IdP discovery for all PingOne for Enterprise managed applications (applications managed by your account, rather than a service provider). For these applications, we no longer require that you specify the idpid for SP-initiated (SAML) requests or OIDC authorization requests.
SAML assertion available in reports	For SAML applications, we've added an enhancement to reports for you to display the SAML assertion for a failed SSO audit event included in a report. You can click on the failure code to display a popup containing the SAML assertion.

Copyright © 2025 Ping Identity Corporation

Feature	Description
PingOne directory enhancements	We've added features to PingOne directory allowing you to: • Configure the reply-to email address used for PingOne Directory user invitations. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Allow self registration for new directory users]. • Enable or disable the password expiry and password lockout notification emails sent to PingOne Directory users. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Allow self registration for new directory users].
include::partial$p14e_p1refs_faw.adoc[tags=faw]provisioner	We've updated the provisioner for Workplace by Facebook applications. This provisioner includes: • Improved error handling and reporting when Workplace by Facebook users contain no ID. • Improved check connection call by not retrieving a list of users.See **Known Issues and Limitations** for important information.

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
Github provisioner	The following limitations apply: • Clearing fields on updates is not supported. • Enabling a previously deleted user in GitHub will trigger a create operation. • When a user is deleted from GitHub they are removed from the organization. The user will still have a GitHub account but no access to the organization's resources. • Due to GitHub API limitations, provisioning with multiple threads or making more than 5000 requests per hour may trigger GitHub's abuse detection mechanism, rate-limiting, or both. This will prevent requests from being completed. For more information, see .github.com/v3///[Github rate-limiting].
Workplace by Facebook provisioner	The following limitations apply: • Clearing fields on updates is not supported. • Due to API limitations with matching a user's manager using the display name, if multiple matches occur the first match will be used. This could be an issue if multiple employees in the Workplace by Facebook account have the same first and last names. To avoid conflicts, you can use a custom attribute mapping to link the manager attribute to a manager's email. • Due to LDAP limitations, when you update a manager's name it does not update their Distinguished Name (DN). The provisioner uses the distinguished name to match a manager in Workplace by Facebook and may not find the correct match. To avoid this, you can use a custom attribute mapping to link the manager attribute to a manager's email. • Due to SaaS API limitations, adding a manger may require a search of all Workplace by Facebook users. This will impact provisioning performance. To avoid this, you can use a custom attribute mapping to link the manager attribute to a manager's email.

Copyright © 2025 Ping Identity Corporation

September, 2018

Enhancements

Feature	Description
PKCE support for OpenID Connect (OIDC)	We've added support for Proof Key for Code Exchange (PKCE) to secure OIDC clients that cannot or choose not to use a client secret. We have therefore relaxed the requirement that a client secret must be specified when configuring an OIDC application with the authorization code flow. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Integrate an OIDC application, PKCE parameters] For more information, see .pingidentity.com/pingone/saasSsoAdminGuide/index.shtml//[Integrate an OIDC application, PKCE parameters].
SLO for OIDC identity providers	We've added single logout (SLO) support for PingOne for Enterprise OIDC identity providers (IdPs). You can specify the end-session URL through the well-known metadata of the OpenID Connect provider (end_session_endpoint), or when you configure the PingOne connection for the OIDC IdP. When SLO is triggered, PingOne redirects the user logout process to the end-session URL for the OIDC IdP.
Automatic IdP Discovery	We've added automatic IdP discovery for all PingOne for Enterprise managed applications (applications managed by your account, rather than a service provider). For these applications, we no longer require that you specify the idpid for SP-initiated (SAML) requests or OIDC authorization requests.
PingOne directory enhancements	We've added features to PingOne directory allowing you to: • Configure the reply-to email address used for PingOne Directory user invitations. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Allow self registration for new directory users]. • Enable or disable the password expiry and password lockout notification emails sent to PingOne Directory users. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Allow self registration for new directory users].

Copyright © 2025 Ping Identity Corporation

Feature	Description
include::partial$p14e_p1refs_faw.adoc[tags=faw]provisioner	We've updated the provisioner for Workplace by Facebook applications. This provisioner includes: • Improved error handling and reporting when Workplace by Facebook users contain no ID. • Improved check connection call by not retrieving a list of users.See **Known Issues and Limitations** for important information.

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
Workplace by Facebook provisioner	The following limitations apply: • Clearing fields on updates is not supported. • Due to API limitations with matching a user's manager using the display name, if multiple matches occur the first match will be used. This could be an issue if multiple employees in the Workplace by Facebook account have the same first and last names. To avoid conflicts, you can use a custom attribute mapping to link the manager attribute to a manager's email. • Due to LDAP limitations, when you update a manager's name it does not update their Distinguished Name (DN). The provisioner uses the distinguished name to match a manager in Workplace by Facebook and may not find the correct match. To avoid this, you can use a custom attribute mapping to link the manager attribute to a manager's email. • Due to SaaS API limitations, adding a manger may require a search of all Workplace by Facebook users. This will impact provisioning performance. To avoid this, you can use a custom attribute mapping to link the manager attribute to a manager's email.

August, 2018

Enhancements

Feature	Description
Users by Service	We've added support for first and last name values for provisioned users on the **Users > Users By Service** page.
PingOne directory user registrations	We've added the ability for you to specify a reply-to email address for user registrations on the **Setup > Directory > Registration** page.

Copyright © 2025 Ping Identity Corporation

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

July, 2018

Enhancements

Feature	Description
OpenID Connect applications	PingOne for Enterprise and PingOne SSO for SaaS Apps now support the OpenID Connect (OIDC) protocol for application integration using code, implicit or hybrid flows. You can customize access tokens for your account or per application. Client authentication is done using client secrets. For PingOne for Enterprise, you can make PingOne OIDC applications available on the PingOne dock. The applications are also selectable in access and authentication policies.
Updated provisioner for Evernote®	We have updated the provisioner for Evernote applications. The update includes: * Support for user attributes: Display Name and External ID. * Support for the Evernote SCIM 2.0 API. * Removed support for hard delete (feature deprecated by Evernote). * Removed support for reactivating a disabled user (feature deprecated by Evernote). See **Known Issues and Limitations** for important information.

Copyright © 2025 Ping Identity Corporation

Feature	Description
Updated SCIM SaaS provisioner	We have updated the provisioner for SCIM SaaS applications. The updates include: * Fixed issue where SCIM v2 requests included SCIM v1.1 schema URN's. * Fixed issue where the NO_CONTENT HTTP response code was not being handled. * Fixed issue where the SERVER_ERROR HTTP response code was not being handled. * Fixed issue where the user's active status was not updated correctly on update requests. * Fixed issue where SCIM v2 error descriptions were not logged correctly. * Fixed issue where an empty return body on a user PUT operation caused a JSON parsing exception. See **Known Issues and Limitations** for important information.
New provisioner for Lucidchart®	We have added a new provisioner for the Lucidchart applications. This provisioner includes: * Support for user provisioning. * Support for these user attributes: Username, Display Name, Email, External ID, First Name, Last Name and Roles. See **Known Issues and Limitations** for important information.
Updated provisioner for Office 365™	We have updated the provisioner for Office 365 applications. The update includes: * Support for hard-deleting users. See **Known Issues and Limitations** for important information.

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
Evernote provisioner	The following limitations apply: * Clearing fields on updates is not supported. * Provisioning disabled users from an LDAP user repository to Evernote is not supported. * Due to Evernote API limitations, a deactivated user cannot be reactivated using SCIM. * Due to Evernote API limitations, new users cannot be created with the same username as a previously deactivated user.
SCIM SaaS provisioner	The following limitations apply: * Clearing fields on updates is not supported. * Outbound Group Provisioning and Memberships is not supported. * Patch updates to SCIM-enabled target applications are not supported. * There is a limit of one value per type (such as, home, work, other) for multivalue attributes (email, phone, address). * Unexpected behavior may occur if the SaaS application does not specify either type and primary information, or both type and primary information for multivalue attributes (email, phone, address). Also, existing attributes on the application may not be removed during an update, and the desired value may not be correctly set as primary. * SCIM-compliant service providers may implement or interpret the SCIM standards differently. This can result in behaviour that is not consistent with the intended use of the SCIM SaaS provisioner.
Lucidchart provisioner	The following limitations apply: * Clearing fields on updates is not supported. * Due to Lucidchart API limitations, there will be a performance impact to creating users when mapping External ID or Roles. Both External ID and Role may fail to be added to a user on the initial create. If this happens, an error will be logged and the update to External ID and Roles will be retried up to three times. * Due to Lucidchart API limitations, attempting to update a user immediately after creating them may result in user not found exceptions. This is due to a delay in Lucidchart between creating a user and being able to modify the user. Failed attempts to update the user will be re-attempted up to three times.

Copyright © 2025 Ping Identity Corporation

Subject	Issue/Limitation
Office 365 provisioner	The following limitations apply: * Opting out of license management for users is not supported. The provisioner will clear existing licenses even when the attribute is unmapped. * Updating the mobile attribute requires that the service principal representing the provisioner (where the user gets the client key and secret) be assigned a role with Company Administrator privileges (using Powershell). See this KB article for more information. * Updating the Password attribute is not supported. * User updates containing a manager that has not yet been provisioned or updated by the new version will fail, because the manager will not have the new extended attribute holding their distinguished name from Active Directory. * If the DoBase64Conversion field is switched to “false”, expect conflicts or failures on federated domains containing pre-existing users provisioned by dirsync or V1.0. * Only outbound provisioning is supported. * Group provisioning is not supported. * Automatic licensing of users is not supported.

June, 2018

Enhancements

Feature	Description
New provisioner for Zscaler®	We have added a new provisioner for the Zscaler applications. This provisioner includes: * Support for user provisioning. * Support for these user attributes: Username, Display Name, Department, Email, External ID, First Name and Last Name. See **Known Issues and Limitations** for important information.
Audit subscriptions	We have added UI for you to configure subscriptions to audit events. You can now display a list of your audit subscriptions, create new Push or Poll subscriptions, and edit or delete existing subscriptions. Learn more in Monitoring PingOne for Enterprise use.

Copyright © 2025 Ping Identity Corporation

Feature	Description
Service provider SAML encryption	We have added an option for you to configure encryption of the assertion in the outbound SAML response sent from PingOne to the service provider (SP). This functionality is available only for non-multiplexed SAML applications. You can assign the encryption algorithm to use. You can also upload your own certificate to use for encryption. NOTE: For enhanced security we will sign the SAML response rather than the assertion in the SAML response when encryption is enabled. Learn more in Adding or updating a SAML application
Service provider SAML encryption	We have added an option for you to configure encryption of the assertion in the outbound SAML response sent from PingOne for an application. You can assign the encryption algorithm to use. You can also upload your own certificate to use for encryption. NOTE: For enhanced security we will sign the SAML response rather than the assertion in the SAML response when encryption is enabled. See Adding or updating a SAML-enabled application for more information.
Updated navigation design	We have updated the design of the top-level navigation for the PingOne admin portal. There is no functional or behavioral impact. This is solely a style change.

Resolved issues

Ticket ID	Issue
SSD-8111	Fixed an issue where the Target Resource URL was limited to 128 characters.
SSD-8413	Fixed an issue where changing the PingOne for Enterprise Target Resource URL for an application supplied by a service provider (SP) to the same Target Resource value as set by the SP resulted in the setting change failing.

Copyright © 2025 Ping Identity Corporation

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

Known issues and limitations

Subject	Issue/Limitation
Zscaler provisioner	The following limitations apply: * Clearing fields on updates is not supported. * Due to a Zscaler limitation, a user's username cannot be updated. * Deleting the administrative user that is set up for provisioning may lead to undesired consequences. The provisioner makes the administrative user the owner and member of each group that is created by the provisioner. We recommend that this administrative user is not managed through the provisioner and is not deleted.

May, 2018

Enhancements

Feature	Description
ServiceNow provisioner (Kingston, Jakarta, Istanbul)	We've added new capabilities for the ServiceNow applications: • Configuration options for the create/read/update/delete (CRUD) capabilities. • Configuration options for provisioning disabled users. • Support for Istanbul, Jakarta, and Kingston. See **Known Issues and Limitations** for important information. This is a new ServiceNow provisioner. We've rebranded the existing provisioner from ServiceNow to "ServiceNow (Fuji)".

Copyright © 2025 Ping Identity Corporation

Feature	Description
Box provisioner	We've added new capabilities for the Box applications: • An option to create personal folders on user creates. • An option to force delete users with managed content. See **Known Issues and Limitations** for important information. **Note** If you have an existing Box application, to take advantage of the new features you will need to click through to the last page and save the application.

Resolved issues

Ticket ID	Issue
SSD-7486	Fixed an issue when adding a new SAML application where changes to the signing algorithm were not being retained after saving the changes.

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
ServiceNow provisioner (Kingston, Jakarta, Istanbul)	The following limitations apply: • `Outbound Group Provisioning` and `Memberships` are not supported. • User attributes cannot be cleared once set. They can only be updated. • When provisioning to ServiceNow, all user accounts in ServiceNow must have an assigned `username` (User ID) value. This is not a required field in ServiceNow. However, because the provisioner must use this field to sync with pre-existing users in ServiceNow, it is required for provisioning to function. If a user in ServiceNow resolves to sAMAccountName (the "standard" mapping in the provisioning channel), the accounts will be linked. Currently, if users exist in ServiceNow without an assigned UserName value, this will cause errors in provisioning. In this case, you can resolve the issue by ensuring every user has an assigned UserName, even if they are not intended to be managed by the provisioner. • When provisioning users, the `username` attribute must contain only URL-safe characters. • When synchronizing roles with users, the `role` attribute must contain only URL-safe characters. • If a new user is created with the same `username` as an existing user, a duplicate user will not be created. Instead, the existing user will be updated with any information assigned. • Due to limitations with the ServiceNow API, a role can be added to a user but not removed, which may cause a user's role in the source data store to become out of sync with the user's role in ServiceNow. Learn more in ServiceNow Provisioner. • When mapping the `roles` attribute, multiple calls to ServiceNow must be made to sync the user role information. This may impact provisioning performance.

Copyright © 2025 Ping Identity Corporation

Subject	Issue/Limitation
Box provisioner	The following limitations apply: • Clearing fields on updates is not supported. • The login attribute cannot be updated through provisioning. • The `Inactive Status Default` user attribute has no effect if the Box connector is configured to delete (hard-delete) users instead of disable (soft-delete) users when de-provisioning. Additionally, deleting a user in an LDAP repository will always set the status for the user as "inactive" in the Box application. • `Outbound Group Provisioning` and `Memberships` are not supported. • A Box API limitation prevents login credentials from being updated by the provisioner when the character case differs. For example, "USER@TEST.COM", cannot be updated to "user@test.com". When the case differs, the Box API omits the login from the API operation. So, in an update operation, when the case differs, the login is omitted, but any other attributes that may have changed are provisioned and updated. • Due to Box API requirements, only primary, validated email addresses can be used to sync users. • Enabling Personal Folder functionality will diminish initial synchronization provisioning performance.

April, 2018

Enhancements

Feature	Description
OpenID Connect identity repository	We've added support for OpenID Connect identity repositories. You can now authenticate users through any OpenID provider. See Connect to OpenID Connect for more information.
Force MFA option	If you have an authentication policy in place for your PingOne account, when you add an application to PingOne, you now have the option to require that each time a user accesses the application, they must use multi-factor authentication (MFA).
New attribute mapping settings	When you add an application to PingOne and use advanced attribute mapping to map your identity provider attributes to service provider attributes, you will now find settings for `random` and `hash` functions. The hash function takes a literal string or attribute value. The random function generates a random string of a specified length. Both functions optionally hash the string using the selected algorithm (MD5, SHA-1, SHA-256) and encode the string using the selected encoder (hex, base64).

Copyright © 2025 Ping Identity Corporation

Resolved issues

Ticket ID	Issue
SSD-6937	Fixed an issue where the signing algorithm for a non-multiplexed application wasn't updating the signing algorithm for the connection.
SSD-6763	Fixed an issue where administrative SSO to the PingOne admin portal for newly assigned administrators was failing when multi-factor authentication (MFA) for the admin portal was required in the authentication policy.

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

March, 2018

Resolved issues

Ticket ID	Issue
SSD-6751	Fixed an issue where the `restAuthUsername` value wasn't always set when the integration page was loaded.
SSD-6627	Fixed an issue where Basic SSO apps were being counted towards the application limit even though the setting to allow Basic SSO was disabled (the default).

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

Copyright © 2025 Ping Identity Corporation

January - February, 2018

Enhancements

Feature	Description
include::partial$p14e_p1refs_faw.adoc[tags=faw]provisioner	We've updated the Workplace by Facebook provisioner to add support for additional user attributes. See **Known Issues and Limitations** for important information. NOTE: If you've been using the Workplace by Facebook application (formerly known as Facebook at Work), you will need to edit the application by clicking through to the last page and saving the application. You will then be able to take advantage of the new provisioner features.

Resolved issues

Ticket ID	Issue
SSD-6604	Fixed an issue where you were unable to edit or delete duplicate groups.
SSD-6599	Fixed an issue where the PingOne was using the NA region authenticator for multi-factor authentication, rather than the proper regional authenticator for the PingOne account.

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
Workplace by Facebook provisioner	The following limitations apply: • Clearing fields on updates is not supported. • Due to API limitations with matching a user's manager using the display name, if multiple matches occur, the first match will be used. This may be an issue if multiple employees in the Workplace by Facebook account have the same first and last names. To avoid conflicts, you can use a custom attribute mapping to link the Manager attribute to a manager's email address. • Due to LDAP limitations, when you update a manager's name it does not update their Distinguished Name (DN). The provisioner uses the DN to match a manager name in Workplace by Facebook, so may not find the correct match. To avoid this, you can use a custom attribute mapping to link the Manager attribute to a manager's email address. • Due to SaaS API limitations, adding a manger may require a search of all Workplace by Facebook users. This will impact provisioning performance. To avoid this, you can use a custom attribute mapping to link the Manager attribute to a manager's email address.

December, 2017

Enhancements

Feature	Description
Multi-factor authentication for the PingOne admin portal	We've added a feature on the Authentication Policy page in the admin portal to enable and require PingID multi-factor authentication (MFA) for PingOne administrators who access the PingOne admin portal. Included is an option to specify an administrator who can access the admin portal without requiring MFA. See SSO to the PingOne for Enterprise admin portal with multi-factor authentication for more information.

Copyright © 2025 Ping Identity Corporation

Feature	Description
SAML signature signing algorithm for SSO	We've added the ability for you to configure the signature signing algorithm for all authentication requests, assertion signing and single logout (SLO) between PingOne and SAML identity providers and between PingOne and SAML service providers. PingOne will continue to support the SHA-1 algorithm, but now allows you to select SHA-256, SHA-384 and SHA-512. New SAML connections default to SHA-256. See Connect to PingFederate for more information. **Note** If you're using PingFederate version 8.0 or greater, you will be automatically updated to use SHA-256 for authentication requests at a future date, with no interruption to SSO.
SAML signature signing algorithm	We've added the ability for you to configure the signature signing algorithm for all assertion signing to PingOne. PingOne will continue to support the SHA-1 algorithm, but now allows you to select SHA-256, SHA-384 and SHA-512. New SAML connections default to SHA-256. See Adding or updating a SAML-enabled application for more information.
Session revocation for PingOne directory	We've implemented a session revocation service for the PingOne directory workflows: user deletion, user disablement and password reset. When you perform these workflows for a PingOne Directory user, the session revocation service will now terminate the PingOne session associated with that user and prevent them from performing new SSO requests through PingOne. See Delete directory users for a description. NOTE: The session revocation service does not perform SLO to SaaS applications that the user may have in an active session.
PingFederate summary information	We've added configuration summary information on the **Identity Repository Settings** page for identity repositories using PingFederate 8.0 or greater.
New provisioner for Jive®	We've added a new provisioner for Jive applications. This provisioner includes: • Added support for user provisioning. • Added support for the user attributes: userName, givenName, familyName, workEmail, password, locale, timeZone, workPhone, externalContributor, federated and location. See **Known Issues and Limitations** for important information.

Deprecated features

Feature	Description
Basic SSO and the browser extension	Basic SSO and the PingOne browser extension are no longer offered for new PingOne accounts. Accounts that are currently utilizing Basic SSO or the browser extension can continue using these facilities without interruption. For accounts not currently using Basic SSO or the browser extension, availability of these facilities is no longer displayed.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
Jive provisioner	The following limitations apply: • Clearing fields on updates is not supported. • Outbound Group Provisioning and Memberships is not supported. • Due to a Jive limitation, a user's `username` cannot be updated. • Due to a Jive limitation, the `externalContributor` attribute cannot be updated. • Due to a Jive limitation, when a user is created their email address must be unique. However, after creation their email address can be updated to match that of an existing user. • Deleting the administrative user that is set up for provisioning can lead to undesired consequences, because the provisioner makes the admin user the owner and member of each group that is created by the provisioner. We recommend that this admin user is not managed through the provisioner and is not deleted.

November, 2017

October, 2017

Enhancements

Feature	Description
include::partial$p14e_p1refs_slack.adoc[tags=Slack]provisioner	We've have added support for additional user attributes. See **Known issues and limitations** for important information. NOTE: Existing customers must edit their existing Slack application, click through to the end page and save to take advantage of the new features

Copyright © 2025 Ping Identity Corporation

Feature	Description
SCIM SaaS provisioner	We've added a new provisioner for SCIM SaaS applications. This provisioner includes: • Support for SCIM 1.1 and 2.0 • Support for user provisioning • SCIM core and enterprise attributes • Support for Basic Authentication, OAuth 2 Bearer Token and OAuth 2 Client Credentials Authentication • SCIM Overrides (Filter Expression, Authorization Header Type, Users API Path) See **Known issues and limitations** for important information.
Ping IDaaS Directory provisioner	We've added a new provisioner for Ping IDaaS Directory. See **Known issues and limitations** for important information.

Resolved issues

Ticket ID	Issue
SSD-6063	Fixed an issue where you were unable to preview the PingOne dock.
SSD-5879	Fixed an issue where the number of connections displayed on the My Applications page for applications was incorrect when an application was disabled.
SSD-3780	Fixed an issue where no warning or confirmation prompt was displayed when saving an Attribute Policy that had no associated connection.
SSD-3838	Fixed an issue where the dropdown list on the search bar automatically displayed when opening the PingOne dock using include::pingone_for_enterprise:partial$p14e_p1refs_ie.adoc[tags=IE]10.
SSD-3838	Fixed an issue when using include::pingone_for_enterprise:partial$p14e_p1refs_ie.adoc[tags=IE]and clicking the search bar, where an application description wasn't being displayed after clicking the down arrow.

. Known issues and limitations

Copyright © 2025 Ping Identity Corporation

Subject	Issue/Limitation
Slack provisioner	• Clearing fields on updates is not supported. • Outbound Group Provisioning and Memberships is not supported. • Due to an API limitation, a user name cannot be updated. • Due to an API limitation, users cannot be created in a deactivated state. For example, if a user is disabled in your user store it will not be created in Slack by the provisioner. • For more information on Slack provisioning limitations, see the .slack.com/scim//[Slack API documentation].
SCIM SaaS provisioner	• Clearing fields on updates is not supported. • Outbound Group Provisioning and Memberships is not supported. • Patch updates to SCIM enabled target applications are not supported. • There is a limit of one value per type (such as, home, work, other) for multivalue attributes (email, phone, address). • Unexpected behavior may occur if the SaaS does not specify either type and primary information, or both type and primary information for multivalue attributes (email, phone, address). Also, existing attributes on the SaaS may not be removed during an Update, and the desired value may not be correctly set as primary. • SCIM-compliant service providers may implement or interpret the SCIM standards differently which can result in behaviour that is not consistent with the intended use of the SCIM SaaS Provisioner.
Ping IDaaS Directory provisioner	• Clearing fields on updates is not supported. • Outbound Group Provisioning and Memberships is not supported. • The password, external id, profilePhotoUrl, profileThumbnailUrl, role, certificates and entitlements attributes cannot be mapped from the source. A default literal value can be used for setting values in the target PingOne tenant.

Copyright © 2025 Ping Identity Corporation

Subject	Issue/Limitation
Multiplexing and manual connections	When configuring a manual connection to an application, currently it is possible to select for multiplexing not to be used for non-SAML applications. Multiplexing is used for all non-SAML applications.

September, 2017

Enhancements

Feature	Description
Deleting a customer account	We've added a confirmation dialog box when you choose to delete a customer account. (SSD-5867)

Resolved issues

Ticket ID	Issue
SSD-5735	Fixed an issue where changing the application category for a PingOne for Enterprise managed application did not update the application category on the PingOne dock.
SSD-5603, 5604	Updated Ping logo, icon and favicon.

August, 2017

Enhancements

Feature	Description
include::partial$p14e_p1refs_msedge.adoc[tags=MsEdge]support	You can now use the Microsoft Edge browser (minimum EdgeHTML version: 15.15063) with the PingOne dock and the PingOne browser extension.
PingOne directory `phoneNumbers` attribute	We've expanded the `phoneNumbers` multivalued attribute to include more subattributes. See PingOne for Enterprise Directory attributes for the list of subattributes you can use.
PingID Standalone upgrade supported	Customers with an existing PingID Standalone account can now upgrade to a PingOne for Enterprise account (SSD-5464).

Copyright © 2025 Ping Identity Corporation

Resolved issues

Ticket ID	Issue
SSD-5536	Fixed an issue where the legacy UI was being displayed for Service User administrators.
SSD-5297, SSD-3839	(PingOne directory) Fixed an issue where the UI wasn't operating as expected when entering email addresses to share a certificate (**Setup > Certificates**, expand the details for a certificate and click **Share**).
SSD-5345	Fixed an issue where the dropdown lists for setting attribute mappings in the **Dock > Configuration** page wasn't being displayed.
SSD-5633	Fixed an issue when configuring a new custom SAML application where the list of attributes available for attribute mapping wasn't loading properly until you saved and refreshed the page.

July, 2017

Enhancements

Feature	Description
Administrators page	We've redesigned the **Account > Administrators** page for clarity and ease of use.
Users By Service Bypass option	We've removed the Unlimited Time setting for the **Bypass** option for Users By Service for all administrators except Global Administrators. You must now be a Global Administrator to enable the **Bypass** option for a user for an unlimited time. (SSD-4983)
include::partial$p14e_p1refs_msedge.adoc[tags=MsEdge]support	You can now use the Microsoft Edge browser (version 40) to access the PingOne admin portal.

Resolved issues

Ticket ID	Issue
SSD-5358	Fixed an issue on the My Applications page in the admin portal where the **Request Ping Identity add a new application to the application catalog** selection did not reference the proper URL.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
SSD-5307	Fixed an issue when adding a new private SAML application where the setting for the **Force Re-authentication** option wasn't being saved correctly.
BE-2344	(Browser extension) Fixed an issue where the locale setting for the browser extension didn't match the locale setting for the PingOne dock.

June, 2017

Enhancements

Feature	Description
PingOne universal certificate	A new PingOne universal certificate is now available. You need to update to the new PingOne universal certificate if you're using either PingFederate or a Third-Party SAML provider as your identity bridge and your configuration requires either: • Signed AuthN requests. • SAML single logout (SLO), either IdP-initiated or SP-initiated. **Note** You do not need to update the PingOne universal certificate if you're using an identity repository other than PingFederate or Third-Party SAML. See Check whether you need to update the PingOne for Enterprise universal certificate for more instructions.

Copyright © 2025 Ping Identity Corporation

Feature	Description
PingOne encryption certificate	We now include the PingOne encryption certificate in the PingOne metadata available when you're configuring a PingFederate or Third-Party SAML identity bridge. We've also added the option to separately download the PingOne encryption certificate if you intend to manually configure the IdP settings (rather than using the PingOne metadata).
Custom entity IDs	When configuring a PingFederate or Third-Party SAML identity bridge, you can now select to enable account-specific entity IDs and specify a custom entity ID for your account. We will validate the ID to ensure that it is unique across all PingOne accounts.
include::pingone_for_enterprise:partial$p14e_p1refs_gapps.adoc[tags=GApps]provisioner	We've updated the Google Apps for Work provisioner as follows: • Improved exception handling and reporting • Added support for Google Admin SDK v1.22.0 • Updates to the password and includeInGlobalAddressList attributes
include::partial$p14e_p1refs_zendesk.adoc[tags=Zendesk]provisioner	We've updated the Zendesk provisioner as follows: • Added Support for updating user emails

Copyright © 2025 Ping Identity Corporation

Feature	Description
PingOne universal certificate	A new PingOne universal certificate is now available. If you're using multiplexing, or using manually configured customer connections, you're using the PingOne universal certificate. In this case, it is imperative that you edit the application configuration to update the PingOne universal certificate. See Update the PingOne SSO for SaaS Apps universal certificate for instructions.
PingOne encryption certificate	When you're adding a customer connection manually, we've added the option to separately download the PingOne encryption certificate.
IdP discovery	When you edit a customer connection, you need only specify the domain or domains used for customer email addresses and we will use this information to discover the IdP for the connection. We've added the option to set the current connection as the default IdP connection used for all of your applications. We've also updated the IdP Discovery popup window to display the application logo and your corporate logo (if you've configured this).
Testing application integration	For security reasons, we've disabled connections to the PingOne Test IdP by default. This connection is enabled only when you select to test your application. We also ensure that you can disable the connection when you're done testing.

Copyright © 2025 Ping Identity Corporation

Resolved issues

Ticket ID	Issue
SSD-4485	Fixed an issue where selecting to use the PingOne universal certificate for a Third-Party SAML identity bridge configuration, then changing to use the PingOne directory as the identity repository, caused the Renewal Certificate to be selected for use rather than the PingOne universal certificate.
SSD-4450	Fixed an issue that resulted in configuration updates not being used during SSO.
SSD-4298	Fixed an issue where the Upload link was being displayed on top of the company logo icon when registering for a new account.
SSD-3777	Fixed an issue where the Signoff button was being displayed after closing the browser tab for an impersonated session, then going to the PingOne admin portal (the impersonated session) from the PingOne dock.
SSD-3721	Fixed an issue on the My Devices page where pressing the Enter key did not correspond to clicking the Save button.

April-May, 2017

Enhancements

Feature	Description
include::partial$p14e_p1refs_box.adoc[tags=Box]and include::partial$p14e_p1refs_webex.adoc[tags=WebEx]provisioners	We've improved handling of look-up by Secondary ID, for instances when look-up by Primary ID fails to return a user.
Corporate branding	We've added an **Account > Branding** page for you to assign branding to be used for your organization's account.
Corporate branding	We've removed the **Setup > General** page and moved the account branding setting to a new **Account > Branding** page. On this page, you can assign branding to be used for your organization's account.
User support message	The user support message setting that appeared on the (now removed) **Setup > General** page is displayed as one of the settings on the **Setup > Dock** page. The user support message is displayed to your users when they click the **Need Help?** link in the dock.

Copyright © 2025 Ping Identity Corporation

Resolved issues

Ticket ID	Issue
SSD-4300	Fixed an error message that was displaying repeatedly.
SSD-4659	Fixed an error message displayed when attempting to SSO to an application without the appropriate permissions.
SSD-4671	Fixed an issue where Application Catalog icons weren't being displayed consistently.
SSD-3167	Fixed an issue where Support Admins (Read-Only) were unable to view the Users tab when impersonating an account using PingOne directory as the identity repository.
SSD-4661	Fixed an issue where the QR code wasn't being displayed when selecting to add a new device in the PingOne dock.
SSD-4511	Removed the (non-editable) corporate logo field from the **Account > Company** page. The corporate logo assignment is on the **Account > Branding** page.
SSD-4687	Fixed an issue where selecting "Other" as the country on the Company page resulted in an error.
SSD-4806	Fixed an issue where an error was thrown when mapping an advanced attribute using "As Literal", entering data, then clicking Save before the preview field updated.
SSD-4844	Fixed an issue where the expiry date for the PingOne universal certificate shown after setting up an identity repository was different (by one day) from the expiry date shown in for the certificate in the list on the **Setup > Certificates** page.
SSD-4915	Fixed an issue on the Company page when the country is France. The dropdown list for State/Province/Region displayed a second entry for "Limousin", rather than an entry for "Lorraine".
SSD-4425	Fixed an issue where the Company ID value was no longer displayed in the PingOne dock. The **Company ID** value is now displayed on the bottom of the navigation pane in the dock.
SSD-5064, 5065	Fixed an issue where attempting to SSO to the admin portal from the PingOne dock fails when the prior SSO request was from the dock to PingFederate.
SSD-3773	Fixed an issue where a customer password reset was not also triggering the display of the license agreement if the license agreement had been updated.
BE-2192	Fixed an issue where an error wasn't being displayed when attempting to launch a Basic SSO application in the PingOne dock (without refreshing the page) after the application had been removed from the My Applications list.
BE-2228	Fixed an issue where the PingOne browser extension training wizard wasn't able to complete for the Cloudpay Community application.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
BE-2228	Fixed issues where the PingOne browser extension training wizard wasn't able to complete for a number of applications.
BE-2268	Fixed an issue where the PingOne browser extension for include::pingone_for_enterprise:partial$p14e_p1refs_ie.adoc[tags=IE]was affecting the ability to load intranet sites.

March, 2017

Enhancements

Feature	Description
Directory settings permissions	We've expanded Identity Repository administrators permissions to include access to view and modify the directory settings when the identity repository is PingOne directory.
API Provisioning	From March 4th 2017 Salesforce is no longer supporting TLS 1.0 protocol. PingOne has been updated to support OAuth for Provisioning communication to accommodate this change. See How to Migrate the Salesforce Provisioner for instructions. JIT Provisioning (just-in-time) is not impacted by this change.

Resolved issues

Ticket ID	Issue
SSD-3822	Fixed an error message displayed when uploading an IdP metadata file that is missing necessary information for SP-initiated SSO.
SSD-3695	Fixed an issue where the phone number wasn't being passed to the authentication provider (PingID).

February, 2017

Enhancements

Feature	Description
PingOne reporting	We've added a new SSO summary report to the list of predefined reports included in the PingOne admin portal reporting. This report shows the number of unique users that are actively using PingOne, and which applications they are logging in to. It also shows the total number of SSO events for each application.

Copyright © 2025 Ping Identity Corporation

Feature	Description
Password change	We've enhanced security to ensure that if a user fails to enter the correct password three times when changing their password on the User Profile page, they are automatically logged out.
Salesforce provisioner	We've updated the Salesforce provisioner with the following changes and enhancements: • Support for approximately 150 additional user attributes. • Support for Salesforce REST v37.0 API. • Support for OAuth Authentication with the OAuth Configuration Service (OCS). • Support for custom subdomains. • You now have the option to freeze user accounts, rather than deactivating them. • Improved exception handling and reporting. • Support for Salesforce disabling TLS 1.0.

Resolved issues

Ticket ID	Issue
SSD-4473	Fixed an issue that was preventing an MSP administrator from impersonating an account to which only disabled administrators has access.
BE-2130	Fixed an issue that was preventing the browser extension welcome message from displaying correctly in some browsers.
SSD-4316	Fixed an issue that was prompting a user to activate OAuth when creating a connection for which provisioning was not selected.
SSD-4289	Fixed a security issue with an MSP administrator's ability to impersonate customer accounts.
SSD-4282	Fixed an issue that was preventing error message popups from closing correctly in the PingOne admin portal.
BE-2080/BE-1940	Fixed an issue that was preventing characters from displaying correctly when training an app, if the language is not English.
IO-2027	We've improved the handling of different letter case logins and aliases for the Box provisioner.
IO-2243	Fixed an issue with the Microsoft Office 365 provisioner that was causing an error when trying to retrieve a user during provisioning.
IO-2242	Fixed an issue with the WebEx provisioner's handling of the timezones not listed in WebEx's timezone encoding list.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
Salesforce provisioner	• User attributes cannot be cleared once they have been set. • You cannot delete permission set assignments. • Custom attributes are not supported. • If you enable/disable or delete a user in your user store, the Salesforce provisioner can only disable the corresponding user in Salesforce as it cannot perform a hard delete of the user entry in Salesforce. • Username attribute must be entered in email format only. • Alias attribute entries can be a maximum of 8 characters in length.

January, 2017

Enhancements

Feature	Description
Certificate Management	PingOne will now inform you if a verification certificate that has been configured on a connection is invalid when the connection is being edited.
Reporting	We've added the ability to navigate back to the Users by Service page if you clicked on the Latest Activity link for a user on the Users by Service page.

Resolved issues

Ticket ID	Issue
SSD-4040	Fixed an issue when filtering dashboard metrics, where filtering by "today" would return 0 results. Also fixed an issue with the mouse over popup on chart data that spanned a DST boundary where the time reported was offset by +1/-1 hour.
SSD-4064	Fixed an issue where viewing latest activity for a user on the Users by Service page was redirecting to the old report logging UI.
SSD-4144	Fixed an issue that was preventing the first and last name from being displayed in the PingOne dock when using PingOne directory.
SSD-4116	Fixed an issue that was preventing an administrator from accessing report entries if they occurred in a timezone and at a time that was considered the next day for the local timezone. Administrators can now select up to one day in the future for the end date of a report filter.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
SSD-4071	Fixed an issue that was preventing the propagation of SLO settings changed on an application in a PingOne for SaaS Apps account from being applied to all connections to that application.
SSD-4078	Fixed an issue that was limiting the value that can be entered in each field on the Password Policy page to three digit numbers (i.e. a maximum value of 999). This limit is now removed.
SSD-4037	Fixed an issue that was not clearing the filter criteria from the previous report, when running a predefined report in the **Reporting** tab.
SSD-3718	The dropdown box used to select fields when running a report has been fixed so that it now displays field names alphabetically.
SSD-3794/SSD-3784	Fixed an issue when impersonating an account via the PingOne dock that was causing the navigation window to resize incorrectly.
ID-5209	Fixed an issue that was marking the SAML_SUBJECT as an optional field when creating an application connection, rather than mandatory.
BE-2050	The browser extension can now handle language-based variations of the Eventzilla URL.
BE-1943	Fixed an issue that was preventing the browser extension from detecting the **Password** and **Sign In** button for the Office 365 app.
BE-1883	Fixed an issue displaying French language text when signing on to the browser extension.
BE-2003/BE-2005/BE-1995	Fixed an issue that was preventing the browser extension from loading correctly after changing the privacy key on a different browser or machine.

December, 2016: Minor Release

Enhancements

Feature	Description
PingOne admin portal	We've made the following enhancements to the PingOne admin portal: • You can now use any Top Level Domain (TLD) URL as a connection configuration URL, in addition to those that are defined by Internet Assigned Numbers Authority (IANA). • We've increased the number of records you can download from the report log, and added a progress bar to the **Reports** tab. You can now download up to 500,000 records to a .csv file.
Application catalog	We've added support for the StartMeeting cloud application.

Copyright © 2025 Ping Identity Corporation

Feature	Description
Reporting	The report log has been updated and enhanced. • You can now run detailed reports from the PingOne admin portal. PingOne provides a number of predefined reports, and also gives you the ability to run your own custom ad hoc report. You can view the results directly in the PingOne admin portal, or export the results in .csv format. • We've also added the ability to view SSO activity per application, via the API.

Resolved issues

Ticket ID	Issue
BE-2003/BE-1995	Fixed an issue that was preventing the browser extension from loading correctly after changing the privacy key on a different browser or machine.
BE-1994	Fixed an issue that was preventing the sign in popup from being displayed in the PingOne dock following a browser refresh.
SSD-3630	Fixed an issue that was preventing the system from saving the correct value for the **Account Specific Entity ID** field and the **Sign AuthRequest** field when uploading metadata for a third party SAML identity repository configuration.
ID-5966	Fixed an issue when checking whether the Entity ID is unique during identity repository configuration.
ID-6344	Fixed an issue that was categorizing identity provider connections associated with a signing certificate incorrectly.
SSD-3572	Fixed an issue that was preventing the removal of the **Identity Bridge Logout URL** value assigned in PingOne.
SSD-3543	Fixed an issue where during configuration of an Invited PingOne SSO account, attempting to download a metadata file or a signing certificate generated an error.

November, 2016: Minor Release

Enhancements

Feature	Description
Administrator capabilities	A global or support administrator impersonating a customer account can now delete the last administrator on the account.
PingOne admin portal	We've added the ability for a Managed Service Provider (MSP) to delete a custom email template in the PingOne admin portal.

Copyright © 2025 Ping Identity Corporation

Feature	Description
PingOne admin portal	We've reduced the idle timeout for an admin session to 15 minutes. We've added the ability for a Managed Service Provider (MSP) to delete a custom email template in the PingOne admin portal.
Certificate Management	We've made the following enhancements: • We've provided admins the ability to remove a verification certificate from a PingOne application connection. • We've added the ability to promote a secondary verification certificate to a primary verification certificate when editing an application connection or a third party SAML identity repository. • Primary and secondary certificates now display the common name and expiry date for the certificate.
Workplace by Facebook™	We've renamed this feature (formerly known as Facebook at Work), and removed the suppressEmail attribute.
Box Provisioner	We've added support for updating user emails in Box Provisioner. NOTE: Existing customers must remove their existing Box applications and then add the application connection to take advantage of the new feature.

Resolved issues

Ticket ID	Issue
SSD-3501	Fixed an issue that was preventing a customer from creating an account when receiving an email invitation from a Managed Service Provider (MSP) administrator in PingOne.
SSD-3497/SSD-3394	Fixed an issue that was preventing the use of "?" and "/" characters in advanced attribute mapping.
SSD-3480	Fixed an issue that was preventing the validation error message from appearing when importing invalid metadata into the PingOne.
SSD-3464	Fixed an issue that was causing an exception error when trying to save an application with an invalid ACS URL in PingOne.
SSD-3441	Fixed an issue that was displaying the administrator role incorrectly when sending an invitation to a new administrator to become the administrator of an existing PingOne account.
ID-5882	Fixed an issue that was causing PingOne to automatically insert default values into optional attribute mapping fields that were purposefully left blank.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
BE-1892	Fixed issues with the following apps, and enabled them in the Application Catalog: • Glassdoor • Wells Fargo CEO portal • 8x8 Virtual Office • 8x8 Account Manager
ID-6039	We've hidden the ability to add primary and secondary verification certificates when creating an SAML 1.1 application connection, as verification certificates are not supported in SAML v1.1.
ID-6266	Fixed an issue that was preventing a newly created certificate from appearing in the Certificate List when using Internet Explorer v10 and v11.
ID-5714	The **Single Logout Endpoint**, **Single Logout Response Endpoint**, and **Single Logout Binding Type** fields have been removed from SAML v1.1 managed applications. SAML v1.1 does not support Single Logout Endpoints.
SSD-3421	Fixed an issue that was causing the admin account to be locked, if resetting a password in the PingOne admin portal using a password that does not meet the PingOne directory policy.
SSD-3418	Fixed an issue when resetting a password from the PingOne admin portal.
SSD-3294	Fixed an issue when loading content from PingOne admin portal using Internet Explorer 10.

October, 2016: Minor Release

Enhancements

Feature	Description
Certificate management	We've now added email notifications to inform you when the primary verification certificate or secondary verification certificate associated with a conniction or identity bridge is expiring. Email notifications are sent two months before expiry, a week before expiry, and at the time of expiry.
Admin roles	We've renamed the Directory Administrator role to Identity Repository Administrator, for clarity. The Identity Repository Administrator refers to an administrator who is responsible for the identity repository, regardless of whether it is PingFederate, AD Connect, a Third Party repository, or PingOne Directory.
Dashboard	We've enhanced the layout of data in the graphs displayed on the dashboard.

Copyright © 2025 Ping Identity Corporation

Feature	Description
MSP administrator	We've enhanced the Managed Service Provider (MSP) admin account capabilities. Now if an MSP account owns a PingOne SSO for SaaS Apps account and invites a customer or partner to create a connection to an application under that PingOne SSO for SaaS Apps account by registering an "Invited PingOne SSO" account, the Invited PingOne SSO account is now listed in the MSP's customer list page.
PingOne user accounts	For any new identity provider that you set up, the lifetime of any user session is now set to 2 hours by default. You can change the duration from PingOne, if you need to do so.
Attribute mapping	We've added the phone number attribute to the list of dock attribute mapping options for PingFederate, AD Connect, and third party SAML identity repositories.

Resolved issues

Ticket ID	Issue
SSD-3356	Restored the setting application logos on applications created in PingOne SSO for SaaS Apps accounts, as they were being removed incorrectly. The logos were removed when this capability was removed for PingOne for Enterprise when using the new PingOne for Enterprisedock.
BE-1812	Fixed an issue that was preventing the **Go to PingOne**and **Sign Off**buttons from showing in the browser extension.
ID-5976	Fixed an error handling issue on the PingOne for Enterprise password reset page.
ID-5993	Fixed an issue that was preventing users changing the default signing certificate assigned to their managed application.
ID-6171	Fixed an issue with the delete certificate feature.
SSD-3288	Fixed an issue that was preventing a user from entering an email address that includes the '+' character, when inviting a customer from a Managed Service Provider (MSP) account in PingOne for Enterprise.
SSD-3331	Fixed an error displayed when adding Google Drive as a Basic SSO application in PingOne for Enterprise.
SSD-3259	Implemented a fix to make transaction processing more resilient to service configuration problems.
SSD-3169	Fixed a security issue with MSP Support Admin (read-only) roles.
SSD-3108	Fixed an issue updating login failures on the dashboard.

Copyright © 2025 Ping Identity Corporation

September, 2016: Minor Release

Enhancements

Feature	Description
Admin log reporting	We've added a new Administrator Login category to the reports log. The new report shows all login attempts by a PingOne administrator, the method of login used (username and password, or SSO) and whether the login attempt was successful.
SSO to PingOne Admin portal	We've added the ability for administrators having Identity Repository administrator or SaaS administrator roles to SSO directly to the PingOne admin portal. In previous versions this was only available for the Global administrator and the Service User administrator roles. This option is only available when using PingFederate, AD Connect, or Third Party SAML as your identity repository.
PingOne API	We've added support for PKCS7 formatted certificates.
Certificate Management	We've reorganized the layout of the connections that are listed in the certificate Connections tab. Connections are now listed by category (identity bridge or application). Identity bridge connections are listed by type (such as PingFederate, or Third Party SAML). The applications header shows the number of application connections associated with the certificate. .

Resolved issues

Ticket ID	Issue
SSD-3020	Verification certificate tool tip text updated.
SSD-3129	Fixed an issue that was permitting users to upload expired or invalid certificates for third party SAML Identity Providers.
SSD-3112	Fixed an issue when accessing the attribute mapping page for a SAML 2.0 connection. When exiting the page and then uploading metadata with a different attribute set, the attributes were not being updated correctly.
SSD-3161	Fixed an issue with caching when trying to SSO with an account that was suspended and then re-enabled.
SSD-3168	Fixed a security issue with Managed Service Provider (MSP) admin capabilities in PingOne.

Copyright © 2025 Ping Identity Corporation

August 30, 2016: Minor Release

Enhancements

Feature	Description
Certificate management	Certificates that do not have a CN defined, now show the first 20 characters of the Subject DN as the certificate name. Performance enhancements were applied to the Certificate Management page. Certificate expiry dates are now displayed in a 4 digit format.

Resolved issues

Ticket ID	Issue
ID-5718	Fixed an issue when adding SAML v1.1 applications from the application catalog, where certificate management was not being supported.
ID-5717	Fixed an issue that was preventing a user from being able to add a multiplexed SAML app from the Application Catalog.
ID-5679	Fixed an issue with the appearance of the **Select Image**button for the Application logo and icon. The appearance is now sized correctly and consistently in the UI.
ID-5671	Fixed a issue when clicking the **Active Download**link in Safari, that was causing it to be displayed, rather than downloaded.
ID-5846	Fixed a bug that was causing an infinite loop when attempting to access the Devices page before completing first factor authentication using PingOne.
SSD-3136	The option to define an application logo has been removed when creating or editing an application connection for users that have upgraded to the new dock. The option remains for users that are using legacy dock.
SSD-2993 SSD-3121	Fixed a bug when uploading metadata that included mappings that were already in the connection, and was causing these mappings to be lost.
SSD-3036	Fixed an issue that was causing an exception when loading the Certificate Management page if invalid certificates were present.
SSD-3017	Fixed a bug where binary certificates that were uploaded were not saved correctly.

Copyright © 2025 Ping Identity Corporation

August 9, 2016: Minor Release

Enhancements

Feature	Description
My Applications search	We've enhanced the ability to search the My Applications list. You can now search by the: • Entity ID. • Application description or part of the description. • Application name. In previous versions it was only possible to search by the application name.
PingOne certificate management	We've added the ability to view the SHA1 and SHA256 fingerprint in the certificate Properties tab.
PingOne passwords	When changing the administrator password in the PingOne admin portal, the administrator is now required to enter their current password, as well as their new password. If the administrator enters the wrong password three times, the account is temporarily locked.

Resolved issues

Ticket ID	Issue
ID-5685	Fixed a broken link in the Invite IdP page.
ID-5549	Properties and connections associated with a verification certificate are now displayed in separate tabs. This matches the way this information is presented for signing certificates.
ID-4585	Fixed an issue that was preventing the secondary instance of a certificate from being deleted when replacing a primary certificate with a secondary certificate.
ID-5428	When configuring a managed connection, the text for the Application Icon has been changed to 'For use on the dock'. As the Application Logo is not used on the new PingOne dock, the text for this field has been changed to 'For use on the previous version of the dock'.
BE-1642	Fixed an issue that was making the browser extension unresponsive when clicking the username and then clicking **Learn** when training an app.
BE-1601	Fixed an issue when training an app that was causing a loop when clicking the **Login** button.
ID-5712	Fixed an issue when editing an application that was preventing changes to the SLO or SLO Response Endpoint from being saved.
ID-5689	Fixed an issue in the Certificate Management page that was preventing the **Download** and **Export** buttons from working in some browsers.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
ID-5691	Fixed an issue on the Certificate Management page where applications sharing a connection (a multiplexed connection) were being displayed as disabled.

July 19, 2016: Minor Release

Enhancements

Feature	Description
Certificate management	We've added a new centralized certificate management UI. The new UI enables you to: • Create new signing certificates. • Migrate individual connections to different signing certificates. • Add certificate expiration notifications. • Verify certification for failover and migration. • Share certificates. See Overview of signing and verification certificates for more information.
Additional language support for end user components	The following languages are now supported for all PingOne user subsystems (PingOne dock, transaction processing, browser extension, and authentication): Chinese, Dutch, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, Spanish, and Thai.

Resolved issues

Ticket ID	Issue
ID-5544	Fixed an issue where the PingOne signing certificate wasn't showing up in the list of results when typing "Ping" in the certificate search field.
ID-5502	Fixed an issue when setting up a connection to an application, that meant the PingOne default certificate was always selected even when a different signing certificate was chosen.
ID-5481	Fixed an issue that caused the PingOne provided signing certificate to be downloaded for an application connection, even if a different singing certificate was selected for the connection.
ID-5486	Renamed the Connection Summary "Certificate" label to "Signing Certificate".
ID-5485	Fixed an issue when promoting a secondary verification certificate to the primary verification certificate. The instance of the secondary verification certificate wasn't being automatically deleted.
ID-5482	Fixed an issue that the certificate properties Issuer DN and Expiration Date fields were not updating accordingly when uploading a response to a certificate signing request (CSR).

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
ID-5343	Fixed an issue importing the PingOne metadata file via a URL when setting up a Third-Party SAML identity bridge.
ID-5329	Fixed an issue that was affecting the proper display of text when verifying AD Connect as an identity bridge.
BE-1569	Fixed an issue for trained apps in PingOne browser extension v2.22.0 that was preventing the browser extension from signing in users automatically.
ID-5585	Fixed a bug that was causing formatting issues in the PingOne dock search.
ID-5543	Change the name of the link used to change an identity repository from "Change User Store Type" to "Change Identity Repository".
ID-5508	Fixed an issue that was preventing some users from editing an application.

June 28, 2016: Minor Release

Enhancements

Feature	Description
New Application Catalog categories	We've added the following categories to the application catalog: benefits, training, and travel.

Resolved issues

Ticket ID	Issue
ID-5444	Fixed an issue when attempting to erase the identity bridge URL, the field was not updating correctly.
ID-5385	Fixed formatting of the applications listed in the application catalog.
ID-5342	Fixed an issue with editing an application, where Chrome and Firefox browsers were auto-populating the first two application configuration fields with autosaved username and password data.
ID-4503	Fixed missing link that enables a user to log back into the admin web portal after they successfully logged out.
BE-1493	Fixed an issue when training a basic SSO app, that caused training to pause when clicking on the Login field.
ID-5462	Fixed an error when setting up a Third Party SAML identity bridge that prevented the list of connection information from being displayed.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
ID-5363	Fixed an issue that custom app icons were not being displayed in the My Applications page, unless the entry was expanded. Custom app icons now app in the My Applications page, and when deleting an application.
ID-5356	The browser extension install option now only appears if there is at least one Basic SSO application installed.
ID-5361	Fixed a security vulnerability associated with the application name on the legacy dock.
ID-5415	Fixed a security vulnerability associated with the browser extension.
SSD-2817	Fixed an issue that was causing a mismatch between the total number of logins displayed in the Dashboard maps and the number of logins recorded in the Logins field.

June 15, 2016: Minor Release

Resolved issues

Ticket ID	Issue
ID-5268	Performance enhancements, to address customer issues when performing a search of Users by Service.
ID-4656	Fixed a potential security vulnerability.
ID-5342	Fixed an issue with editing an application, where Chrome and Firefox browsers were auto-populating the first two application configuration fields with autosaved username and password data.
ID-5334	Fixed an issue that was causing an error when adding an application.
ID-5274	Fixed an issue when clicking a Configuration page link it was landing on the Dashboard.
ID-1671	Fixed an issue on the Company Settings page when viewing company description the characters were not displaying correctly.
ID-5332	Fixed and issue that an application which had been updated to show a new icon displayed the old icon when trying to delete the application.

Copyright © 2025 Ping Identity Corporation

June 1, 2016: Major Release

Enhancements

Feature	Description
New PingOne dock	We've totally redesigned the PingOne dock: • There's a new user interface, with application categories, frequently used applications and quick access to account information. • A new search bar to help you find applications and install new ones. • More options for you to customize and brand the interface. This includes use of company logos, custom background images, definitions of application categories, and colors of navigation panes, fonts and the search bar. • And improved display quality of application icons. See Introducing the PingOne for Enterprise dock for more information.
include::partial$p14e_p1refs_faw.adoc[tags=faw]provisioning	We've updated Facebook at Work provisioning to support provisioning user manager details. See Known Limitations for more information.

Known issues and limitations

Copyright © 2025 Ping Identity Corporation

Subject	Issue/Limitation
Facebook at Work provisioning	• Clearing fields on updates is not supported. • Due to API limitations with matching a user's manager using the display name, if multiple matches occur the first match will be used. This could be an issue if multiple employees in the Facebook at Work account have the same first and last names. To avoid conflicts, you can use a custom attribute mapping to link the manager attribute to a manager's email. • Due to LDAP limitations, when you update a manager's name it does not update their Distinguished Name (DN). The provisioner uses the distingushed name to match a manager in Facebook At Work and may not find the correct match. To avoid this, you can use a custom attribute mapping to link the manager attribute to a manager's email. • Due to SaaS API limitations, adding a manger may require a search of all Facebook At Work users. This will impact provisioning performance. To avoid this, you can use a custom attribute mapping to link the manager attribute to a manager's email.

May 17, 2016: Minor Release

Enhancements

Feature	Description
include::partial$p14e_p1refs_webex.adoc[tags=WebEx]Provisioning	We've updated WebEx provisioning to support: * Additional user attributes. * WebEx API v10.0 SP3. * Improvements to error handling and logging. See Known Limitations for more information.

Resolved issues

Ticket ID	Issue
ID-4842	Fixed an issue on the PingID Configuration page where choosing to discard changes when attempting to exit this page didn't exit the page.
ID-5135	Fixed an issue where a new token wasn't being generated when a PingOne for Enterprise administrator clicked the Invite SaaS Admin link to send an email to the PingOne for SaaS Apps application administrator.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
ID-5128	Fixed an issue where some users were not being removed from the PingID service when selecting Remove on the Users by Service page.
ID-5020	Fixed an issue with removing customers from the customers listing. The last customer displayed in the listing wasn't being removed.
BE-1300	(Browser extension) Fixed an issue causing an include::pingone_for_enterprise:partial$p14e_p1refs_ie.adoc[tags=IE]installation error (1603) when attempting to install the browser extension.

Deprecated features

Feature	Description
PingID Standalone account	The registration option for a PingID Standalone account has been removed. All of the functionality offered by this account is now included in a PingOne for Enterprise account.

Known issues and limitations

Subject	Issue/Limitation
WebEx provisioning	* The WebEx ID attribute is not updateable in PingOne. * The MeetingType attribute is limited to one value in PingOne (not a multivalued attribute). * Due to API Limitations, WebEx doesn't allow a user to be created in a suspended state. WebEx will automatically activate the user after it is created.

April 26, 2016: Minor Release

Resolved issues

Ticket ID	Issue
ID-4842	Fixed an issue where a Managed Service Provider (MSP) was unable to log in to an Invited PingOne SSO account as a Directory Admin.
ID-3881	Fixed an issue where downloading the PingOne metadata file for a Third-Party SAML identity bridge wasn't working properly in Safari.
ID-5134	Fixed an issue where user were unable to add applications to their personal dock.
SSD-2627	Fixed a security issue with an error message.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
BE-1084	(Browser extension) Fixed an issue when using include::pingone_for_enterprise:partial$p14e_p1refs_ie.adoc[tags=IE]version 11 where the browser extension wasn't capturing and supplying user credentials properly.
BE-1222	(Browser extension) Fixed an issue where Basic SSO wasn't working properly when using Internet Explorer for some applications not in the Application Catalog.
BE-1279	(Browser extension) Fixed an in Internet Explorer 11 when signing on to a Basic SSO application from the PingOne dock.

Deprecated features

Feature	Description
PingID Standalone account	The registration option for a PingID Standalone account has been removed. All of the functionality offered by this account is now included in a PingOne for Enterprise account.

April 19, 2016: Minor Release

Enhancements

Feature	Description
include::partial$p14e_p1refs_box.adoc[tags=Box]Provisioning	We've updated Box provisioning to support: • Additional user attributes. • Improvements to error handling and logging. See Known Limitations for more information.

Resolved issues

Ticket ID	Issue
None	(None to report for this release.)

Known issues and limitations

Copyright © 2025 Ping Identity Corporation

Subject	Issue/Limitation
Box provisioning	• Once set, you cannot clear user attributes. • The login attribute cannot be updated through provisioning. • The `Inactive Status Default` user attribute has no effect if the Box connector is configured to delete (hard-delete) users instead of disable (soft-delete) users when de-provisioning. Additionally, deleting a user in an LDAP repository will always set the status for the user as "inactive" in Box.

April 5, 2016: Minor Release

Enhancements

Feature	Description
None	(None to report for this release.)

Resolved issues

Ticket ID	Issue
None	(None to report for this release.)
SSD-2572	Added new application categories for Benefits, Training and Travel.
ID-4819	Fixed an issue where an error occurred when you attempted to change your password using AD Connect with the Password Change option enabled and the IWA option disabled.
ID-4839	Fixed an issue where Basic SSO transactions weren't being logged.

Known issues and limitations

Subject	Issue/Limitation
Browser extension installation in Mozilla Firefox®	After installing the PingOne browser extension in Firefox, you need to refresh the page. Otherwise, the browser extension installation will begin again. Ticket ID: ID-4248.

Copyright © 2025 Ping Identity Corporation

March 15, 2016: Minor Release

Enhancements

Feature	Description
None	(None to report for this release.)

Resolved issues

Ticket ID	Issue
None	(None to report for this release.)
ID-4658	Fixed an issue where the number of applications displayed in the Dashboard page didn't match the number of applications displayed in the My Applications page.
ID-4650	Fixed an issue where provisioning for AD Connect was failing.
ID-4422	Fixed an issue where the PingID settings file had an extraneous escape character.
BE-1142	(Browser extension) Fixed an issue where the PingOne browser extension was interfering with display rendering in include::pingone_for_enterprise:partial$p14e_p1refs_ie.adoc[tags=IE]version 10 or 11 when using include::partial$p14e_p1refs_oracle.adoc[tags=Oracle]Business Intelligence Enterprise Edition.

Known issues and limitations

Subject	Issue/Limitation
Dropbox provisioning	• Clearing fields on updates is not supported. • Due to API limitations, a user's email cannot be updated until the user has activated their account. • Due to API limitations, a user cannot be suspended or unsuspended until the user has activated their account. • Due to API limitations, if a user's given name or surname fails to update due to the new value containing unsupported characters (* | : " < > ?), an error may not be reported in the provisioning logs.

Copyright © 2025 Ping Identity Corporation

Subject	Issue/Limitation
Browser extension installation in Mozilla Firefox®	After installing the PingOne browser extension in Firefox, you need to refresh the page. Otherwise, the browser extension installation will begin again. Ticket ID: ID-4248.

February 23, 2016: Minor Release

Enhancements

Feature	Description
include::partial$p14e_p1refs_dropbox.adoc[tags=Dropbox]Provisioning	We've updated Dropbox provisioning to support additional user attributes. See Known Limitations for more information.
Invited PingOne SSO Accounts	We've add an Administrators page to the PingOne admin portal for Invited PingOne SSO accounts. You can now assign multiple administrators for your account.

Resolved issues

Ticket ID	Issue
None	(None to report for this release.)
SSD-2267	Fixed an issue for multi-factor authentication with include::partial$p14e_p1refs_safenet.adoc[tags=SafeNet]where users needed to authenticate a second time when logging in to Safenet.
ID-4278	Fixed an issue in the Reports page display where the Category values was removed whenever the report results were expanded.
ID-1682	Fixed an issue on the User Groups page where the Deprovision all users checkbox wasn't displayed when you cleared a selected checkbox next to the application name.
BE-976	(Browser extension) Fixed an issue where the Save Learning popup wasn't displaying properly for include::pingone_for_enterprise:partial$p14e_p1refs_ie.adoc[tags=IE]version 9.

Known issues and limitations

Copyright © 2025 Ping Identity Corporation

Subject	Issue/Limitation
Dropbox provisioning	• Clearing fields on updates is not supported. • Due to API limitations, a user's email cannot be updated until the user has activated their account. • Due to API limitations, a user cannot be suspended or unsuspended until the user has activated their account. • Due to API limitations, if a user's given name or surname fails to update due to the new value containing unsupported characters (* | : " < > ?), an error may not be reported in the provisioning logs.
Browser extension installation in Mozilla Firefox®	After installing the PingOne browser extension in Firefox, you need to refresh the page. Otherwise, the browser extension installation will begin again. Ticket ID: ID-4248.

February 2, 2016: Minor Release

Resolved issues

Ticket ID	Issue
ID-4216	Fixed an issue where the Save button wasn't working in the application credentials dialog box for Basic SSO applications.
ID-4213	Fixed an issue where the step to configure provisioning for a PingFederate identity bridge displayed in the existing tab/window rather than a new tab/window.
ID-4145	Fixed an issue where the browser extension wasn't automatically signing in after you install your first Basic SSO application.
ID-3883	Fixed an issue where errors weren't being displayed properly when installing an identity bridge.
ID-3398	Fixed an issue for PingID Standalone accounts, where an extraneous warning was being displayed when clicking the Setup tab.
ID-3031	Fixed an issue where you were unable to upload a JPG image file for your profile picture.
ID-3030	Fixed an issue where invited PingOne directory users were unable to upload a JPG image file for their profile picture during the registration process.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
BE-12	(Browser extension) Fixed an issue where the browser extension wasn't working properly when login fields displayed in an iFrame.
BE-747	(Browser extension) Fixed an issue where sign on for Basic SSO applications wasn't working properly when the application login required text input.
BE-623	(Browser extension) Fixed an issue where browser extension wasn't working properly when the PingOne dock tab wasn't the current tab.
ID-1656	Fixed an issue where the instruction steps for creating or editing an application displayed HTML tags and encoded characters.
ID-4214	Fixed an issue where the SSO endpoint was being truncated. Now extended to 2048 characters.

Known issues and limitations

Subject	Issue/Limitation
Browser extension installation in Mozilla Firefox®	After installing the PingOne browser extension in Firefox, you need to refresh the page. Otherwise, the browser extension installation will begin again. Ticket ID: ID-4248.

January 26, 2016:

include::partial$p14e_p1refs_faw.adoc[tags=faw]Provisioning

Enhancements

Feature	Description
Facebook at Work Provisioning	We've updated Facebook at Work provisioning to support additional user attributes.

Known issues and limitations

Copyright © 2025 Ping Identity Corporation

Subject	Issue/Limitation
Known limitations for this release:	• Making attributes create-only isn't supported. • Clearing fields on updates isn't supported. • The `roles` field supports only a single value.

January 19, 2016:

include::pingone_for_enterprise:partial$p14e_p1refs_365.adoc[tags=365]Provisioning

Enhancements

Feature	Description
Office 365 Provisioning	We've updated Office 365 provisioning to support: • Provisioning additional user attributes. • Azure Active Directory Graph API v1.6 (updated from version v1.5). • Clearing of licenses on updates. • Improved exception handling and reporting.

Known issues and limitations

Copyright © 2025 Ping Identity Corporation

Subject	Issue/Limitation
Known limitations for this release:	• Opting out of license management for users is not supported. The provisioner will clear existing licenses even when the attribute is unmapped. • User delete is not supported. However, you can disable users. • Users cannot be created in a disabled state. They must first be created in an active state and then disabled. • Updating the mobile attribute requires that the service principal representing the provisioner (the place the user gets the Client ID and Secret) be assigned a role with Company Administrator privileges (using PowerShell). • Updating the ImmutableID and Password attributes is not supported. • User updates containing a manager that has not yet been provisioned or updated by the new version will fail because the manager will not have the new extended attribute holding their Active Directory distinguished name. • If the DoBase64Conversion field is set to “false”, expect conflicts or failures on federated domains containing pre-existing users provisioned by Dirsync or a Ping product. • Only outbound provisioning is supported. • Automatic licensing of users is not supported.

January 12, 2016: Minor Release

Resolved issues

Ticket ID	Issue
ID-3828	Fixed a misleading error message.
ID-3758	Fixed an issue regarding lapse of synchronization between PingOne directory administrators and directory users.
SSD-1956	Fixed an issue where meaningful information wasn’t being displayed in the Logout Confirmation screen.
ID-3904	Fixed an issue where some pages were displaying an error saying the domains wasn’t set, when the domain had already been set for the PingOne session.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
ID-3504	Fixed an issue where you were unable to remove validation certificates assigned to Third-Party SAML identity bridges.
ID-1656	Fixed an issue where the instruction steps for creating or editing an application displayed HTML tags and encoded characters.
BE-656	(Browser extension) Fixed an issue during adding an application where the prompt to sign in normally for the application site was being displayed a second time after you'd already successfully signed in.
BE-623	(Browser extension) Fixed an issue where the Save popup wasn't being displayed when adding the include::partial$p14e_p1refs_netflix.adoc[tags=netflix]application in include::pingone_for_enterprise:partial$p14e_p1refs_ie.adoc[tags=IE]10.

Previous PingOne SSO for SaaS Apps releases

February 2022

Enhancements

Feature	Description
Manual Connection IdPID	Removed the ability to change the *idpid* value for an existing manual customer connection. The *idpid* value acts as the identifier for an IdP connection, and changing it can cause unexpected behavior. If you need to change the *idpid* value, you can create a new manual connection. For more information, see What is an idpId?.

October 2021

Enhancements

Feature	Description
SSO/SLO	Increased the `max-age` parameter of the `strict-transport-security` header for the `https://sso.connect.pingidentity.com/sso/` endpoint. The previous `max-age` was 1 year. The new `max-age` is 2 years.

Copyright © 2025 Ping Identity Corporation

September 2021

Enhancements

Feature	Description
Custom Entity ID	Added the ability to define a custom entity ID for applications that are enabled through PingOne. If a custom entity ID is in use by a non-multiplexed connection, it cannot be changed. For more information, see Add or update other applications.
SSO Summary Report	Added a new **SSO User Count** report type. The **SSO User Count** report counts the total number of unique users for a customer during the specified period. You can run the report either by customer name or `IdP ID`. For more information, see PingOne for Enterprise report types.

Resolved issues

Ticket ID	Issue
SSD-16877	Fixed an issue that reassigned the signing certificate to the default signing certificate when the `signingCertFingerprint` parameter was not specified when updating a customer connection.

July 2021

Enhancements

Feature	Description
Customer Connection API	Added a feature allowing you to delete customer connections and application connections using the customer connection API. For more information, see PingOne SSO for SaaS Apps Customer Connection API.
Admin Portal Banner	Added a feature allowing you to display a banner message in the administrative portal. For more information, see Assign branding and design.

Copyright © 2025 Ping Identity Corporation

June 2021

Enhancements

Feature	Description
Read-Only Administrative Roles	Added a feature allowing you to assign user groups to read-only versions of administrative roles. Read-only roles allow administrators to access the areas of the admin portal normally allowed by that role, but not to change settings. For more information, see Configure SSO to the admin portal.
Verbose Reporting	Added a feature allowing more detailed reports and subscriptions for partner accounts with OIDC identity providers. For more information, see Creating and administering a partner account.

May 2021

Enhancements

Feature	Description
Account ID	Added a feature allowing administrative users to look up their unique account ID. To find your account ID, go to **Account > Properties**.

April 2021

Enhancements

Feature	Description
Invited Connection Contact Email	Added a feature allowing administrators to change the contact email for invited accounts. For more information, see Edit an invited customer connection.

March 2021

Enhancements

Feature	Description
Customer Connections REST API	Added request parameters to the Customer Connection Rest API. These optional parameters give you the same control over application connections using the API that you would have using the admin console. For more information, see PingOne SSO for SaaS Apps Customer Connection API

Copyright © 2025 Ping Identity Corporation

Feature	Description
OAuth Access Token	Increased the allowed number of trusted origins for OAuth access token Cross-Origin Resource Sharing. The previous limit was 10. The current limit is 100. For more information, see Configuring your OAuth settings.

January 2021

Enhancements

Feature	Description
Admin Console SSO	Added the ability to configure your IdP connection to allow administrative users to SSO into the admin console. See **Known issues and limitations** below for important limitations to this feature. For more information, see Configure SSO to the admin portal
PingOne Token Lifetime	Reduced the lifetime of the PingOne user token from ten minutes to five minutes. For more information, see Process the PingOne SSO for SaaS Apps token exchange.

Known issues and limitations

Subject	Issue/Limitation
Single Logout	PingOne's single logout (SLO) implementation relies on the ability to send cookies within an iframe. Some browsers now block this ability by default, which causes problems with SLO. SLO does not function on browsers where third-party cookies are disabled. This issue impacts SLO on the following browsers: • Safari 13.1+ on MacOS • Safari on iOS and iPadOS 13.4+ • Any browser where the user has disabled third party cookies IdP-initiated SLO does not terminate the admin portal session in browsers that enforce SameSite. We are working to accommodate this new behavior.

Copyright © 2025 Ping Identity Corporation

November 2020

Enhancements

Feature	Description
Administrator Settings	Added a feature that allows you to change the certificate expiration notification settings for Global and SaaS administrators. For more information, see Editing administrative roles, permissions, and notifications and Manage your user profile.

October 2020

Enhancements

Feature	Description
Customer Connections	Added a feature that allows you to filter the list of existing customer connections by status or type. For more information, see Edit an invited customer connection and Edit a managed customer connection.

April 2020

Enhancements

Feature	Description
Certificate management	We've added a new certificate management UI. The new UI enables you to: • Create new signing certificates • View usage of configured certificates • Migrate individual applications and identity providers to different signing certificates, or change the configured verification certificate • Automatically receives email notifications when certificates are expiring or have expired See Certificate management for more information.

Copyright © 2025 Ping Identity Corporation

September-November 2019

Enhancements

Feature	Description
Adding OIDC applications	We've updated the selection and configuration of OIDC applications, streamlining this process based on the type of OIDC application connection you want to add. See Adding or updating an OIDC application for more information.
OpenID Connect login_hint parameter	We've added the ability for you to pass the `idpid` or email domain in the OpenID Connect (OIDC) login_hint parameter when adding an OIDC application. See the Default User Profile Attribute Contract settings in Adding or updating an OIDC application for more information.

June, 2019

Enhancements

Feature	Description
Customer connection email invitation	You can now select the PingOne data center region for invited customers. See Creating an invited SSO connection for more information.

April, 2019

Enhancements

Feature	Description
Cross-origin resource sharing (CORS) for OpenID Connect	If you're integrating OpenID Connect (OIDC) applications with PingOne, you can now configure one or more trusted origins to enable cross-origin resource sharing (CORS). See Configuring your OAuth settings for more information.

January, 2019

Enhancements

Feature	Description
SSO reporting	We've added new report types and predefined reports for SSO transactions. For more information, see .pingidentity.com/pingone/saasSsoAdminGuide/index.shtml//[Report types] and .pingidentity.com/pingone/saasSsoAdminGuide/index.shtml//[Report event information].

Copyright © 2025 Ping Identity Corporation

November, 2018

Enhancements

Feature	Description
Turkish language support	We've updated the PingOne user interface to include support for Turkish. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[PingOne language support].

October, 2018

Enhancements

Feature	Description
Administrative auditing (reports and subscriptions)	Administrative auditing is now available PingOne for Enterprise, PingID and PingOne SSO for SaaS Apps. You can utilize the administrative audit events through both the Reports and the Subscriptions facilities.
PKCE support for OpenID Connect (OIDC)	We've added support for Proof Key for Code Exchange (PKCE) to secure OIDC clients that cannot or choose not to use a client secret. We have therefore relaxed the requirement that a client secret must be specified when configuring an OIDC application with the authorization code flow.

September, 2018

Enhancements

Feature	Description
PKCE support for OpenID Connect (OIDC)	We've added support for Proof Key for Code Exchange (PKCE) to secure OIDC clients that cannot or choose not to use a client secret. We have therefore relaxed the requirement that a client secret must be specified when configuring an OIDC application with the authorization code flow. For more information, see .pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml//[Integrate an OIDC application, PKCE parameters] For more information, see .pingidentity.com/pingone/saasSsoAdminGuide/index.shtml//[Integrate an OIDC application, PKCE parameters].

Copyright © 2025 Ping Identity Corporation

July, 2018

Enhancements

Feature	Description
OpenID Connect applications	PingOne for Enterprise and PingOne SSO for SaaS Apps now support the OpenID Connect (OIDC) protocol for application integration using code, implicit or hybrid flows. You can customize access tokens for your account or per application. Client authentication is done using client secrets. For PingOne for Enterprise, you can make PingOne OIDC applications available on the PingOne dock. The applications are also selectable in access and authentication policies.

June, 2018

Enhancements

Feature	Description
Service provider SAML encryption	We have added an option for you to configure encryption of the assertion in the outbound SAML response sent from PingOne for an application. You can assign the encryption algorithm to use. You can also upload your own certificate to use for encryption. NOTE: For enhanced security we will sign the SAML response rather than the assertion in the SAML response when encryption is enabled. See Adding or updating a SAML-enabled application for more information.
Updated navigation design	We have updated the design of the top-level navigation for the PingOne admin portal. There is no functional or behavioural impact. This is solely a style change.

March, 2018

Resolved issues

Ticket ID	Issue
SSD-6751	Fixed an issue where the `restAuthUsername` value wasn't always set when the integration page was loaded.

Copyright © 2025 Ping Identity Corporation

December, 2017

Enhancements

Feature	Description
SAML signature signing algorithm	We've added the ability for you to configure the signature signing algorithm for all assertion signing to PingOne. PingOne will continue to support the SHA-1 algorithm, but now allows you to select SHA-256, SHA-384 and SHA-512. New SAML connections default to SHA-256. See Adding or updating a SAML-enabled application for more information.

November, 2017

Known issues and limitations

Subject	Issue/Limitation
Multiplexing and manual connections	When configuring a manual connection to an application, currently it is possible to select for multiplexing not to be used for non-SAML applications. Multiplexing is used for all non-SAML applications.

October, 2017

Resolved issues

Ticket ID	Issue
SSD-5879	Fixed an issue where the number of connections displayed on the My Applications page for applications was incorrect when an application was disabled.
SSD-3780	Fixed an issue where no warning or confirmation prompt was displayed when saving an Attribute Policy that had no associated connection.

. Known issues and limitations

Subject	Issue/Limitation
Multiplexing and manual connections	When configuring a manual connection to an application, currently it is possible to select for multiplexing not to be used for non-SAML applications. Multiplexing is used for all non-SAML applications.

Copyright © 2025 Ping Identity Corporation

June, 2017

Enhancements

Feature	Description
PingOne universal certificate	A new PingOne universal certificate is now available. If you're using multiplexing, or using manually configured customer connections, you're using the PingOne universal certificate. In this case, it is imperative that you edit the application configuration to update the PingOne universal certificate. See Update the PingOne SSO for SaaS Apps universal certificate for instructions.
PingOne encryption certificate	When you're adding a customer connection manually, we've added the option to separately download the PingOne encryption certificate.
IdP discovery	When you edit a customer connection, you need only specify the domain or domains used for customer email addresses and we will use this information to discover the IdP for the connection. We've added the option to set the current connection as the default IdP connection used for all of your applications. We've also updated the IdP Discovery popup window to display the application logo and your corporate logo (if you've configured this).
Testing application integration	For security reasons, we've disabled connections to the PingOne Test IdP by default. This connection is enabled only when you select to test your application. We also ensure that you can disable the connection when you're done testing.

April-May, 2017

Enhancements

Feature	Description
Corporate branding	We've added an **Account > Branding** page for you to assign branding to be used for your organization's account.

Copyright © 2025 Ping Identity Corporation

February, 2017

Enhancements

Feature	Description
Salesforce provisioner	We've updated the Salesforce provisioner with the following changes and enhancements: • Support for approximately 150 additional user attributes. • Support for Salesforce REST v37.0 API. • Support for OAuth Authentication with the OAuth Configuration Service (OCS). • Support for custom subdomains. • You now have the option to freeze user accounts, rather than deactivating them. • Improved exception handling and reporting. • Support for Salesforce disabling TLS 1.0.

Resolved issues

Ticket ID	Issue
SSD-4316	Fixed an issue that was prompting a user to activate OAuth when creating a connection for which provisioning was not selected.
IO-2027	We've improved the handling of different letter case logins and aliases for the Box provisioner.
IO-2243	Fixed an issue with the Microsoft Office 365 provisioner that was causing an error when trying to retrieve a user during provisioning.
IO-2242	Fixed an issue with the WebEx provisioner's handling of the timezones not listed in WebEx's timezone encoding list.

January, 2017

Resolved issues

Ticket ID	Issue
SSD-4040	Fixed an issue when filtering dashboard metrics, where filtering by "today" would return 0 results. Also fixed an issue with the mouse over popup on chart data that spanned a DST boundary where the time reported was offset by +1/-1 hour.
SSD-4071	Fixed an issue that was preventing the propagation of SLO settings changed on an application in a PingOne for SaaS Apps account from being applied to all connections to that application.

Copyright © 2025 Ping Identity Corporation

Previous AD Connect Releases

April 2020 Release: Version 5.0.3

Resolved issues

Ticket ID	Issue
SSD-15239	(AD Connect) Fixed an issue where AD Connect could not be installed on a non-Domain Controller sever.

February 2020: Version 5.0.1

Enhancements

Feature	Description
TLS Support	AD Connect 5.0.1 supports TLS 1.2 as we prepare to End of Life TLS 1.0. and 1.1.
	New installations and upgrades to AD Connect 5.0.1 require the installation of Microsoft .NET Framework 4.7.2. See Installing AD Connect for more information.

Fall 2019: Version 4.0.10

Enhancements

Feature	Description
Active Directory Global Catalog	(AD Connect only) You can now elect to use the Active Directory Global Catalog for lookups. The option to enable the Global Catalog is in the AD Connect Configuration section of the AD Connect setup (**Setup > Identity Repository > Connect to an Identity Repository > AD Connect**). See AD Connect final setup for more information.

Summer 2019 Release: Version 4.0.65

Enhancements

Feature	Description
Branding	(AD Connect) You can now assign branding for the login and password reset pages. See Assign AD Connect branding and designs for more information.

Copyright © 2025 Ping Identity Corporation

Fall 2018 Release: Version 4.0.5

Resolved issues

Ticket ID	Issue
SSD-10054	(AD Connect) Fixed an issue where AD Connect did not allow duplicate values in an Octet String attribute.

August, 2018: Version 4.0.3

Enhancements

Feature	Description
TLS 1.1 and 1.2 now supported	We've added support for TLS 1.1 and 1.2. (SSD-8913).

March, 2018: Version 4.0.1

Resolved issues

Ticket ID	Issue
SSD-6889	(AD Connect) Fixed an issue where AD Connect was prevented from reconnecting to PingOne if an error was encountered while attempting to connect.

October, 2017: Version 3.0.60

Enhancements

Feature	Description
(AD Connect) Added logging of authentication method	We updated AD Connect logging to distinguish the method a user employs to authenticate (such as, IWA or Forms-based). (SSD-6103).

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
ID-1289	If you import more than one signing certificate with the same subject name into the IIS host for AD Connect, you must first remove expired certificates with the same subject name directly through IIS Manager. If this is not done you may experience problems when removing an expired certificate and updating it with a new one.

July, 2017: Version 3.0.50

Enhancements

Feature	Description
Invalid credential errors	Invalid credential errors are now logged at the Debug level, rather than the Error level as previously. (SSD-5372, SSD-5501).

Resolved issues

Ticket ID	Issue
PINGONESTG-2489, SSD-5501	(AD Connect with IIS only) Fixed an issue where communication issues with the DC were being masked by other error messages.

Known issues and limitations

Subject	Issue/Limitation
ID-1289	If you import more than one signing certificate with the same subject name into the IIS host for AD Connect, you must first remove expired certificates with the same subject name directly through IIS Manager. If this is not done you may experience problems when removing an expired certificate and updating it with a new one.

Copyright © 2025 Ping Identity Corporation

June, 2017: Version 3.0.49

Enhancements

Feature	Description
Invalid credential errors	(AD Connect with IIS only) Invalid credential errors are now logged at the Debug level, rather than the Error level as previously. (SSD-5372).

Resolved issues

Ticket ID	Issue
PINGONESTG-2447, SSD-5372	(AD Connect with IIS only) Fixed an issue in AD Connect with IIS where look ups for additional user information were sometimes incorrectly based on the user's email domain instead of the Windows domain, as expected.
PINGONESTG-2455, SSD-5372	Fixed an issue where AD Connect could unintentionally be configured to strip the email domain from the username before trying to look up the user information based on their email (which would always fail). The Strip Email setting is now disabled for email-based lookup.

Known issues and limitations

Subject	Issue/Limitation
ID-1289	If you import more than one signing certificate with the same subject name into the IIS host for AD Connect, you must first remove expired certificates with the same subject name directly through IIS Manager. If this is not done you may experience problems when removing an expired certificate and updating it with a new one.

June, 2017: Version 3.0.47

Enhancements

Feature	Description
Debug logging	We've improved debug logging (PINGONESTG-2292).

Copyright © 2025 Ping Identity Corporation

Resolved issues

Ticket ID	Issue
PINGONESTG-2413	Fixed an issue where a user's thumbnail photo attribute wasn't encoded properly.

Known issues and limitations

Subject	Issue/Limitation
ID-1289	If you import more than one signing certificate with the same subject name into the IIS host for AD Connect, you must first remove expired certificates with the same subject name directly through IIS Manager. If this is not done you may experience problems when removing an expired certificate and updating it with a new one.

June, 2017: Version 3.0.44

Resolved issues

Ticket ID	Issue
PINGONESTG-2377	Fixed an issue where the photo attribute wasn't encoded properly.

Known issues and limitations

Subject	Issue/Limitation
ID-1289	If you import more than one signing certificate with the same subject name into the IIS host for AD Connect, you must first remove expired certificates with the same subject name directly through IIS Manager. If this is not done you may experience problems when removing an expired certificate and updating it with a new one.

Copyright © 2025 Ping Identity Corporation

May, 2017: Version 3.0.43

Resolved issues

Ticket ID	Issue
SSD-4726	Fixed an issue when using Filter as the lookup method with "Strip mail" disabled. AD Connect was appending the domain name if the user didn't include it.
SSD-5013	Fixed an issue where, under certain conditions, errors were being displayed without the proper styling.
PINGONESTG-2341	Fixed issue where static resources weren't loaded correctly on some pages.

Known issues and limitations

Subject	Issue/Limitation
ID-1289	If you import more than one signing certificate with the same subject name into the IIS host for AD Connect, you must first remove expired certificates with the same subject name directly through IIS Manager. If this is not done you may experience problems when removing an expired certificate and updating it with a new one.

April, 2017: Version 3.0.42

Resolved issues

Ticket ID	Issue
PINGONESTG-2251	Fixed an issue with filter-based authentication where disabling the **Strip Email** resulted in appending the Windows domain to usernames during the lookup.

Copyright © 2025 Ping Identity Corporation

Known issues and limitations

Subject	Issue/Limitation
ID-1289	If you import more than one signing certificate with the same subject name into the IIS host for AD Connect, you must first remove expired certificates with the same subject name directly through IIS Manager. If this is not done you may experience problems when removing an expired certificate and updating it with a new one.

March, 2017: Version 3.0.38

Enhancements

Support for TLS v1.1 & v1.0 following Salesforce removal of TLS v1.0 support

From March 4, 2017, Salesforce is no longer supporting TLS v1.0. To minimize impact for PingOne customers that use PingOne to connect to Salesforce via delegated authentication for AD Connect with IIS, we've put together information and instructions. These show you how to ensure your IIS deployment running AD Connect for IIS supports the updated version of TLS (TLS v1.1 or v1.2).

Resolved issues

Ticket ID	Issue
SSD-4121	(AD Connect) Fixed an issue where concurrent SSO requests using IWA were resulting in network collisions.
ID-1357	Fixed an issue that was causing some users to get an HTTP Error 400 when attempting to SSO to ZScalar from AD Connect.

Known issues and limitations

Subject	Issue/Limitation
ID-1289	If you import more than one signing certificate with the same subject name into the IIS host for AD Connect, you must first remove expired certificates with the same subject name directly through IIS Manager. If this is not done you may experience problems when removing an expired certificate and updating it with a new one.

Copyright © 2025 Ping Identity Corporation

January 2017: Version 3.0.37

Known issues and limitations

Subject	Issue/Limitation
SSD-3870	If you import more than one signing certificate with the same subject name into the IIS host for AD Connect, you must first remove expired certificates with the same subject name directly through IIS Manager. If this is not done you may experience problems when removing an expired certificate and updating it with a new one.
SSD-4139	Fixed an issue where a user's middle name attribute could not be used in a SAML assertion.

August 16, 2016: Version 3.0.31

Resolved issues

Ticket ID	Issue
ID-5623	Fixed an issue where AD Connect was providing PingOne with the computer name, rather than the fully qualified domain name (FQDN).

August 30, 2016: Version 3.0.32

Resolved issues

Ticket ID	Issue
ID-5826	Fixed an issue where the connection to PingOne can intermittently be lost under certain conditions.
ID-5838	When you use a custom theme.zip with AD Connect with IIS, the favicon is placed in the root directory. This prevents the custom theming from handling the state properly.

August 9, 2016: Version 3.0.22-→

Enhancements

Copyright © 2025 Ping Identity Corporation

AD Connect installer

We've added the ability to define a verification certificate as part of the AD Connect installation process. During installation, you have the option to:

- Create a new self-signed certificate.
- Select an existing certificate.
- Upload a certificate file.The options available vary depending on whether you are performing a new installation or an upgrade.

May 17, 2016: Version 3.0.22

Enhancements

New configuration parameter for AD Connect

We've add the Subject Attribute parameter to the AD Connect Configuration section when installing or reconfiguring AD Connect. Use this parameter to choose the value to use for SAML_SUBJECT. The possible values are sAMAccountName and userPrincipalName.

Resolved issues

Ticket ID	Issue
ID-361	Fixed an issue where AD Connect wasn't sending the address attributes in the SCIM User object if the StreetAddress attribute wasn't set.

Known issues and limitations

Subject	Issue/Limitation
Provisioning	For a single PingOne account, if you have two AD domains with two provisioners, do not modify groups on one domain while the other domain's provisioner is restarting. This can cause unpredictable behaviour to occur. Ticket ID: IX-315.

April 26, 2016: Version 3.0.20

Enhancements

New configuration parameter for AD Connect

We've add the Subject Attribute parameter to the AD Connect Configuration section when installing or reconfiguring AD Connect. Use this parameter to choose the value to use for SAML_SUBJECT. The possible values are sAMAccountName and userPrincipalName.

Copyright © 2025 Ping Identity Corporation

Resolved issues

Ticket ID	Issue
ID-5012	Fixed an issue where users had no access to applications until the AD Connect Configuration service was restarted.
ID-4705	Fixed an issue where PingID needed to be re-enabled after upgrading AD Connect.

Known issues and limitations

Subject	Issue/Limitation
Provisioning	For a single PingOne account, if you have two AD domains with two provisioners, do not modify groups on one domain while the other domain's provisioner is restarting. This can cause unpredictable behaviour to occur. Ticket ID: IX-315.

March 15, 2016: Version 3.0.14

Enhancements

None

(None to report for this release.)

Resolved issues

Ticket ID	Issue
ID-4668	Fixed an issue where the AD Connect for IIS installation wasn't finding the required .NET version, although it was installed.
ID-4650	Fixed an issue where provisioning for AD Connect was failing.

Known issues and limitations

Subject	Issue/Limitation
Provisioning	For a single PingOne account, if you have two AD domains with two provisioners, do not modify groups on one domain while the other domain's provisioner is restarting. This can cause unpredictable behaviour to occur. Ticket ID: IX-315.

Copyright © 2025 Ping Identity Corporation

January 22, 2016: Version 3.0.12

Enhancements

None

(None to report for this release.)

Resolved issues

Ticket ID	Issue
ID-4010	Fixed an issue where SSO wasn't working unless you restarted the AD Connect Configuration Service.

Known issues and limitations

Subject	Issue/Limitation
Provisioning	For a single PingOne account, if you have two AD domains with two provisioners, do not modify groups on one domain while the other domain's provisioner is restarting. This can cause unpredictable behaviour to occur. Ticket ID: IX-315.

January 12, 2016: Version 3.0.10

Enhancements

None

(None to report for this release.)

Resolved issues

Ticket ID	Issue
ID-3995	Fixed an issue where you weren't able to select the Provisioner Only option using a mouse or trackpad.

Known issues and limitations

Subject	Issue/Limitation
Provisioning	For a single PingOne account, if you have two AD domains with two provisioners, do not modify groups on one domain while the other domain's provisioner is restarting. This can cause unpredictable behaviour to occur. Ticket ID: IX-315.

Copyright © 2025 Ping Identity Corporation

October 15, 2015: Version 3.0.8

Enhancements

None

(None to report for this release.)

Resolved issues

Ticket ID	Issue
ID-3613	Fixed an issue where the installation instructions in the header of the screen to select the installation type weren't being displayed properly.
ID-3501	Fixed the naming of the AD Connect with IIS selection on the installation type screen.

September 16, 2015: Version 3.0

Enhancements

Group Hierarchy Support

We've added a configuration option to enable support for nested Active Directory groups. When this option is enabled, the nested groups will inherit the SSO permissions of their parent group or groups. See Installing AD Connect for instructions.

Auto-Update Changes

You can now use auto-update if your current installation is version 3.0 or higher. All prior versions of AD Connect require a manual update. See Updating AD Connect for instructions.

.NET Requirements

Microsoft Net 4.5.2 Framework is now required. The framework installation file is packaged with the AD Connect and AD Connect with IIS distributions.

Resolved issues

Ticket ID	Issue
ID-2277	Fixed issue where the option to require a password on an initial login wasn't enabled by default.
ID-2222	Fixed display of popup window to authorize an AD Connect update.
ID-2117	Fixed error when configuring IdP using a new account.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
ID-2074	Fixed error when switching to edit mode from the settings summary page after previously exiting edit mode without making any changes.

Known issues and limitations

Subject	Issue/Limitation
AD Connect application requests redirected to the PingOne dock (ID-1441)	If you are using AD Connect and experiencing an issue where your application requests are being redirected to the PingOne dock when you aren't using the dock, enable the stateless option for AD Connect: 1. Ensure that you're using AD Connect version 2.1.14 or higher. See Updating AD Connect for upgrade instructions. 2. Open the *installation_path*Ping Identity\AdConnect\SSO\web.config file in a text editor. 3. Under the <appSettings> section, add the following entry: `<add key="stateless" value="true" />` 4. Save the web.config file. Your changes will take affect immediately.

August 21, 2015: Version 2.1.17

Enhancements

None

(None to report for this release).

Resolved issues

Ticket ID	Issue
ID-2277	Fixed issue where the option to require a password on an initial login wasn't enabled by default.
ID-2222	Fixed display of popup window to authorize an AD Connect update.
ID-2117	Fixed error when configuring IdP using a new account.

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
ID-2074	Fixed error when switching to edit mode from the settings summary page after previously exiting edit mode without making any changes.

Known issues and limitations

Subject	Issue/Limitation
AD Connect application requests redirected to the PingOne dock (ID-1441)	If you are using AD Connect and experiencing an issue where your application requests are being redirected to the PingOne dock when you aren't using the dock, enable the stateless option for AD Connect: 1. Ensure that you're using AD Connect version 2.1.14 or higher. See Updating AD Connect for upgrade instructions. 2. Open the *installation_path*Ping Identity\AdConnect\SSO\web.config file in a text editor. 3. Under the <appSettings> section, add the following entry: `<add key="stateless" value="true" />` 4. Save the web.config file. Your changes will take affect immediately.

July 21, 2015: Version 2.1.15

Enhancements

None

(None to report for this release).

Resolved issues

Ticket ID	Issue
ID-1306	Fixed a misleading error message when attempting to communicate with PingOne.

Known issues and limitations

Copyright © 2025 Ping Identity Corporation

Subject	Issue/Limitation
AD Connect application requests redirected to the PingOne dock (ID-1441)	If you are using AD Connect and experiencing an issue where your application requests are being redirected to the PingOne dock when you aren't using the dock, enable the stateless option for AD Connect: 1. Ensure that you're using AD Connect version 2.1.14 or higher. See Updating AD Connect for upgrade instructions. 2. Open the *installation_path*Ping Identity\AdConnect\SSO\web.config file in a text editor. 3. Under the <appSettings> section, add the following entry: `<add key="stateless" value="true" />` 4. Save the web.config file. Your changes will take affect immediately.

March 16, 2015: Version 2.1.10

Enhancements

None

(None to report for this release).

Resolved issues

Ticket ID	Issue
ID-246	Fixed an issue where the `distinguishedName` include::pingone_for_enterprise:partial$p14e_p1refs_ad.adoc[tags=AD]attribute wasn't being sent for provisioning.
ID-242	Fixed an issue where the attribute were being converted to all lowercase.

February 25, 2015: Version 2.1.9

Enhancements

ID-53

We've added `immutableId` to the SCIM user object map in AD Connect outbound provisioning.

Resolved issues

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
None	(None to report for this release.)

January 10, 2015: Version 2.1.4

Enhancements

include::pingone_for_enterprise:partial$p14e_p1refs_365.adoc[tags=365]Active Profiles

We've added support for Office 365 active profiles.

Password Functionality

We've added the ability to reset passwords for AD Connect.

Resolved issues

Ticket ID	Issue
None	(None to report for this release.)

October 28, 2014: Version 2.0.45

Enhancements

None

(None to report for this release.)

Resolved issues

Ticket ID	Issue
PINT-524	Fixed exception when selecting CA signed certificate during installation.

October 7, 2014: Version 2.0.44

Enhancements

None

(None to report for this release.)

Resolved issues

Copyright © 2025 Ping Identity Corporation

Ticket ID	Issue
Various	Minor fixes.

August 26, 2014: Version 2.0.42

Enhancements

Resolved issues

Ticket ID	Issue
PINT-277	Fix an issue where the subject is missing when the user principal name (UPN) isn't specified for the user.

July 17, 2014: Version 2.0.39

Enhancements

Authentication Lookup Parameters

We've added support for configuration of authentication lookup parameters (such as attribute name and filter).

June 24, 2014: Version 2.0.34

Enhancements

New AD Connect

AD Connect is now available without an IIS dependency. You now have the option to install "AD Connect" or "AD Connect with IIS".

IWA Support

We've added the option to use Integrated Windows Authentication (IWA) with AD Connect.

SAML_SUBJECT Value Changed

The SAML_SUBJECT value is changed to `userPrincipalName` rather than `sAMAccountName` as in previous AD Connect versions. You need to update your application attribute mappings if SAML_SUBJECT is a source value for any of your application connections.

SCIM Events

We've added support for resending of user SCIM events on group monitoring changes.

SCIM Attributes

We now send only required SCIM attributes during provisioning.

Copyright © 2025 Ping Identity Corporation

PingOne URL

The new PingOne configuration URLs are now used.

Certificate DN Parsing

We've improved certificate DN parsing for AD Connect with IIS.

Auto-Update

We've improved the workflows for auto-update.

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise

PingOne for Enterprise is a cloud-based identity as a service (IDaaS) framework for secure identity access management. You will use PingOne for Enterprise to give members of your organization secure single sign-on (SSO) to cloud applications.

Log in to the PingOne admin portal to set up, configure and maintain your PingOne for Enterprise account.

> **Note**
>
> If you forget your password, click **Change My Password** on the login page to reset your password. After 3 attempts to log in with the wrong credentials, you're locked out for 15 minutes. Further login attempts during the 15 minute lockout period do not reset or change the lockout duration.

Getting started

About this task

Use this workflow to guide you in setting up PingOne for Enterprise:

Steps

1. Get familiar with how PingOne for Enterprise works.

   See PingOne for Enterprise and its subtopics for information.

   You can also download the PingOne Security Hardening Guide for security-related best practices.

2. Register your PingOne for Enterprise account.

   See Registering a PingOne for Enterprise account for registration instructions.

3. Connect to an identity repository.

Copyright © 2025 Ping Identity Corporation

You can configure a PingOne for Enterprise identity bridge to connect to external identity repositories, or use the PingOne for Enterprise Directory as your identity repository. See Connecting to an identity repository for instructions.

4. Assign the administrative users for your account.

   Administration of your PingOne for Enterprise account is role-based. See Assign administrative roles for more information.

5. Add groups for your users.

   User access to applications in PingOne for Enterprise is controlled through group membership. See Managing users by group for information and Adding user groups for instructions.

6. Add applications for your users.

   See Managing applications for information and refer to the relevant subtopic to add the applications.

7. Add an authentication policy.

   The authentication policy can be applied when users or administrators single sign-on (SSO), and for applications using SAML connections. You have the option of using PingID to apply a secondary level of authentication (multi-factor authentication). See Authenticating users for information and its subtopics for instructions.

8. Manage the certificates to use for your account.

   See Certificate management for information and its subtopics for instructions.

9. To assign your corporate logo, go to **Account > Branding**.

The corporate logo is displayed when users sign on to PingOne for Enterprise. See Assign branding and design for logon and SSO for more information.

1. Configure the PingOne for Enterprise Directory dock.

   For more information, see Configuring the dock when using an identity bridge or Configure the dock when using PingOne for Enterprise Directory.

   Go to **Setup > Branding** to configure branding and design settings for the dock. See Assign branding and design for more information.

2. If you're using PingOne for Enterprise Directory, go to **Setup > Directory > Branding** to configure branding for additional user-facing pages.

   For more information, see Assign directory branding and designs.

Next steps

As you refine your PingOne for Enterprise configuration, if you don't find what you're looking for in this guide, go to the Support and Community portal for additional information.

Registering a PingOne for Enterprise account

Registering a new PingOne for Enterprise account takes only a few minutes.

About this task

Copyright © 2025 Ping Identity Corporation

When registering for your new PingOne for Enterprise account, you'll need to know:

- Whether you're registering for a PingOne for Enterprise or PingOne SSO for SaaS Apps account.
- Which data center region—North America, Europe, or Australia—will contain all of your account data.
- Your registration key. To obtain a registration key, sign on to the Ping Identity Support Portal and open a case.

> **Note**
>
> To open a support case you must have a Ping Identity account. If you don't have an account you can register an account for free.

To register for your PingOne for Enterprise or PingOne SSO for SaaS Apps account:

Steps

1. Go to https://admin.pingone.com/web-portal/register.
2. On the **Select One** list, select either **PingOne for Enterprise** or **PingOne SSO for SaaS Apps** and click **Next**.
3. Enter your **First Name**, **Last Name**, and **Company Name**.
4. On the **Data Center Region** list, select the data center region for this account.

   > **Caution**
   >
   > Data cannot be moved across data center regions, so if you decide later you need to use a different data center region, you'll need to start over.

5. Enter your **Corporate Email** address.

   For PingOne for Enterprise accounts, you'll be assigned as a Global Administrator for the account (based on your email address). You can change this later, if needed.
6. In the **Registration Key** field, enter the registration key supplied to you by your Ping Identity support representative.
7. Click **Next**.
8. In the **Set Password** and **Verify Password** fields, enter a valid password and click **Register**.
9. Select the **I agree to the terms of service** box and click **Agree & Proceed**.

   Result:

   The PingOne for Enterprise admin portal opens, and a confirmation email is sent to your email address for this account.
10. Open the confirmation email and activate your account.

    > **Note**
    >
    > You must activate the account to begin using it.

Result

Your new account is registered and activated. Welcome to PingOne for Enterprise.

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise language support

This table shows the languages supported per component for PingOne for Enterprise user pages.

PingOne for Enterprise language support

Language	ISO language code	User pages				
		Dock	MFA authenticator	PingID mobile	AD Connect	Directory
Chinese-simplified	zh-Hans	Y	Y	Y	Y	Y
Dutch	nl	Y	Y	Y	Y	Y
English	en	Y	Y	Y	Y	Y
French-CA	fr-ca	Y	Y	Y	Y	Y
French-EU	fr	Y	Y	Y	Y	Y
German	de	Y	Y	Y	Y	Y
Italian	it	Y	Y	Y	Y	Y
Japanese	ja	Y	Y	Y	Y	Y
Korean	ko	Y	Y	Y	Y	Y
Portugese-EU	pt	Y	Y	Y	Y	Y
Russian	ru	Y	Y	Y	Y	Y
Spanish-EU	es	Y	Y	Y	Y	Y
Thai	th	Y	Y	Y	Y	Y
Turkish	tr	Y	Y	Y	Y	Y

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise identity repositories

An identity repository stores the user credentials necessary to validate a user's local or network access to your organization. You can use PingOne for Enterprise Directory as your identity repository, or use an identity bridge to establish a connection to an identity repository. An identity bridge establishes a standards-based, high security relationship with an identity repository to authenticate and provision your users for single sign-on (SSO).

Provisioning dynamically creates and updates SSO user information in your PingOne for Enterprise user groups based on attributes in incoming SAML assertions from a cloud application provider. Only SAML-enabled applications can support provisioning.

> **Note**
>
> User provisioning is supported by the following identity repositories:
>
> - PingOne for Enterprise Directory
> - PingFederate Bridge
> - AD Connect

PingOne for Enterprise Directory

The PingOne for Enterprise Directory is a cloud-based user directory as a service, providing user and group management, user provisioning, directory access entitlements, easy user registration, and API support for custom applications.

Identity bridges

The identity bridges use Federated SSO. Federated SSO uses the industry-standard protocols SAML or OpenID Connect to establish a secure connection, an identity bridge, to your user repositories. User credentials are authenticated through the identity bridge using either SAML or OAuth. You can also choose to apply a secondary level of authentication using PingID through the use of an authentication policy.

AD Connect

AD Connect is a free PingOne for Enterprise plugin that provides an identity bridge to AD Connect, and supports user provisioning. AD Connect comes in two versions:

- Standard AD Connect uses a secure backchannel protocol to communicate with PingOne. This eliminates the requirement for IIS, open ports, or signing certificates.
- The AD Connect with IIS version uses IIS with open ports for HTTPS to communicate with PingOne for Enterprise, and verifies the communication with signing certificates.You need to install either version of AD Connect on a Windows Server host in an Active Directory domain.

PingFederate Bridge

PingFederate Bridge is a lightweight version of PingFederate, designed for use with PingOne for Enterprise. PingFederate Bridge can connect to a large variety of user repositories, and supports user provisioning. A PingFederate license can be either a "Bridge" license or a "Full" license. You can use either type of license with PingOne. This documentation references PingFederate Bridgee. If your organization has a full PingFederate license, all instructions are the same unless otherwise noted. See .pingidentity.com/pingfederatebridge/pf93///[Introduction to PingFederate Bridge] for more information.

Copyright © 2025 Ping Identity Corporation

OpenID Connect

If you have an identity provider that supports OpenID Connect, you can set up PingOne to use OpenID Connect as your identity bridge.

Microsoft ADFS

If you have a Microsoft Active Directory Federation Services (ADFS) identity provider, you can set up PingOne for Enterprise to use ADFS as your identity bridge.

Google

If you are already using Google Apps for mail and calendar, there are just a few extra steps to set up PingOne for Enterprise to use Google as your identity bridge.

Third Party SAML

There are many federation tools that support the SAML protocol. Examples of third party SAML products that can operate as identity bridges are Shibboleth, CA Siteminder, Oracle Identity Federation, and others. PingOne for Enterprise can interoperate with all identity providers supporting SAML 2.0.

Connections to multiple PingOne for Enterprise accounts

In some cases, your organization may want to configure the identity bridge to support connections to multiple PingOne for Enterprise accounts. A typical scenario is organizations needing distinct connections from a number of divisions or subsidiaries.

PingOne for Enterprise supports these types of multiple connections through the identity bridge setup option `Enable account-specific Entity IDs`. Choosing this option creates a unique Entity ID based on your PingOne for Enterprise account (Company ID). This custom entity ID is written to the PingOne for Enterprise metadata file that you download for import to your identity bridge.

> **Note**
>
> When changing an existing entity ID for a PingOne for Enterprise identity repository, you also need to see that this value is changed on the Identity Provider (IdP). Otherwise, SSO can be disrupted.

To make use of PingOne for Enterprise's account-specific IDs for multiple connections to a single identity bridge instance, your identity bridge needs to support the PingFederate concept of "virtual server IDs". This is an identity bridge feature for aliasing entity IDs (connection IDs) for use by multiple service providers (SPs). Using account-specific IDs, PingOne for Enterprise effectively impersonates multiple SPs.

The Google identity bridge doesn't support a "virtual server IDs" facility, so you cannot use account-specific entity IDs in this case.

SSO with PingOne for Enterprise

Single sign-on (SSO) using PingOne for Enterprise means setting up a connection to a user repository using either:

Copyright © 2025 Ping Identity Corporation

Federated SSO

Federated SSO uses the industry-standard protocols SAML or OpenID Connect to establish a secure connection, an identity bridge, to your user repositories. User credentials are authenticated through the identity bridge using either SAML or OAuth. You can also choose to apply a secondary level of authentication using PingID through the use of an authentication policy.

Basic SSO

Basic SSO (password vaulting) uses the PingOne for Enterprise browser extension to relay credentials to the target cloud application. User credentials are encrypted (128 bit AES) with a user-specified privacy key and are stored in PingOne for Enterprise. The privacy key is stored in the local file system and is never sent to PingOne for Enterprise. PingOne for Enterprise uses stored encrypted credentials for single sign-on (SSO) to your cloud applications. The browser extension can access the encrypted credentials only after a user is authenticated to the identity repository.

See Ping Identity services for operational status of all Ping Identity services, including PingOne. You can also choose to subscribe to alert notifications.

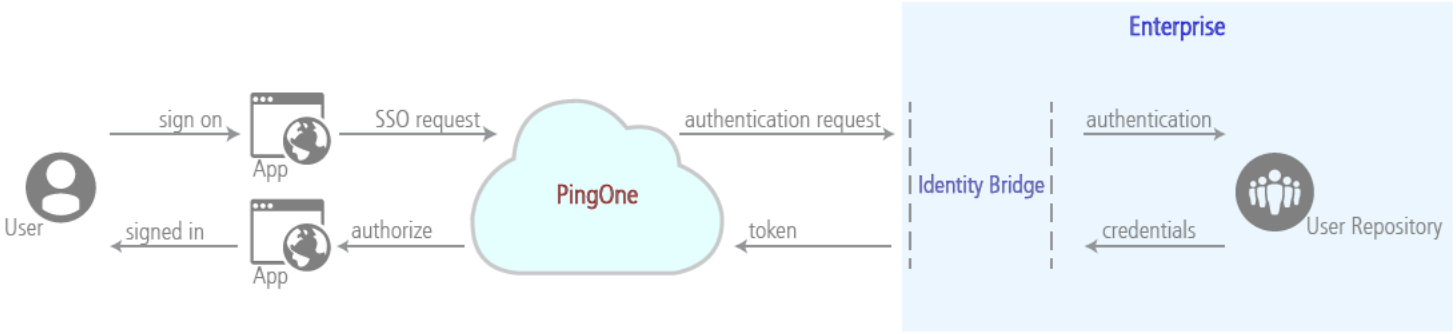
As a corollary to SSO, the SAML protocol also supports a single logout (SLO) process. For more information, see PingOne for Enterprise and SLO.

For Federated SSO, the SSO process can be initiated from either the identity provider (IdP) through a PingOne for Enterprise identity bridge, or from a Service Provider (SP) through a PingOne SSO for SaaS Apps connection to an application. For more information, see Configuring IdP-initiated SSO and Configuring SP-initiated SSO.

Federated SSO with PingOne for Enterprise

Federated SSO uses an identity bridge to establish secure user authentication. You will choose an identity bridge to establish a connection to your user repository. The identity bridge ensures secure user authentication and (when used) provisioning from the user repository. When your identity bridge connection is set up, you're automatically provided with a PingOne dock URL for your organization. You will then customize your dock to reflect your organization, and add selected applications to PingOne for Enterprise for single sign-on (SSO) by your users. After you add and authorize your groups for access to the applications you've added, you're all set.

How It Works



What PingOne for Enterprise Logs for Every Federated SSO Transaction

Whenever a user signs on (SSO) to PingOne for Enterprise, we log the information in the following table. You can see the logging details displayed on your Reports page.

Copyright © 2025 Ping Identity Corporation

Parameter	Description
(date)	The date and time of the SSO transaction.
TOKEN SUBJECT	The user ID we send to the Service Provider (SP).
SUBJECT_FROM_IDP	The user ID returned by the identity bridge.
TOKEN	A generated ID used to retrieve SSO attributes from PingOne. Limited to one-time use.
ASSERTIONID	The ID for the SAML assertion from the identity bridge.
IP	The user's IP address for this SSO transaction.
AGENT_ID	The ID assigned to the user's client or agent (generally a browser) used for SSO.
AGENT	Information about the client or agent used for SSO.
APP_NAME	The name of the application used for SSO.
SAAS_DOMAIN	If specified, the host name or domain name for the user application.
SAAS_ID	The ID assigned to the user application.
SP_ACCOUNT_ID	The PingOne account ID for the SP.
SP_ACCOUNT_NAME	The name assigned to the SP account in PingOne.
IDP_ID	The identity bridge ID used by the SP to identify the identity bridge.
IDP_ACCOUNT_ID	The unique account ID for the identity bridge in PingOne.
IDP_ACCOUNT_NAME	The name of the identity bridge in PingOne.
ACCOUNT_REGION	The region of the identity bridge.
FIRST_NAME_FROM_IDP	The user's first name as assigned by the IdP.
LAST_NAME_FROM_IDP	The user's last name as assigned by the IdP.
EMAIL_FROM_IDP	The user's email address as assigned by the IdP.
STATUS	The status of the SSO transaction.
ERROR_CODE	Contains the error information if an error occurs.

Copyright © 2025 Ping Identity Corporation

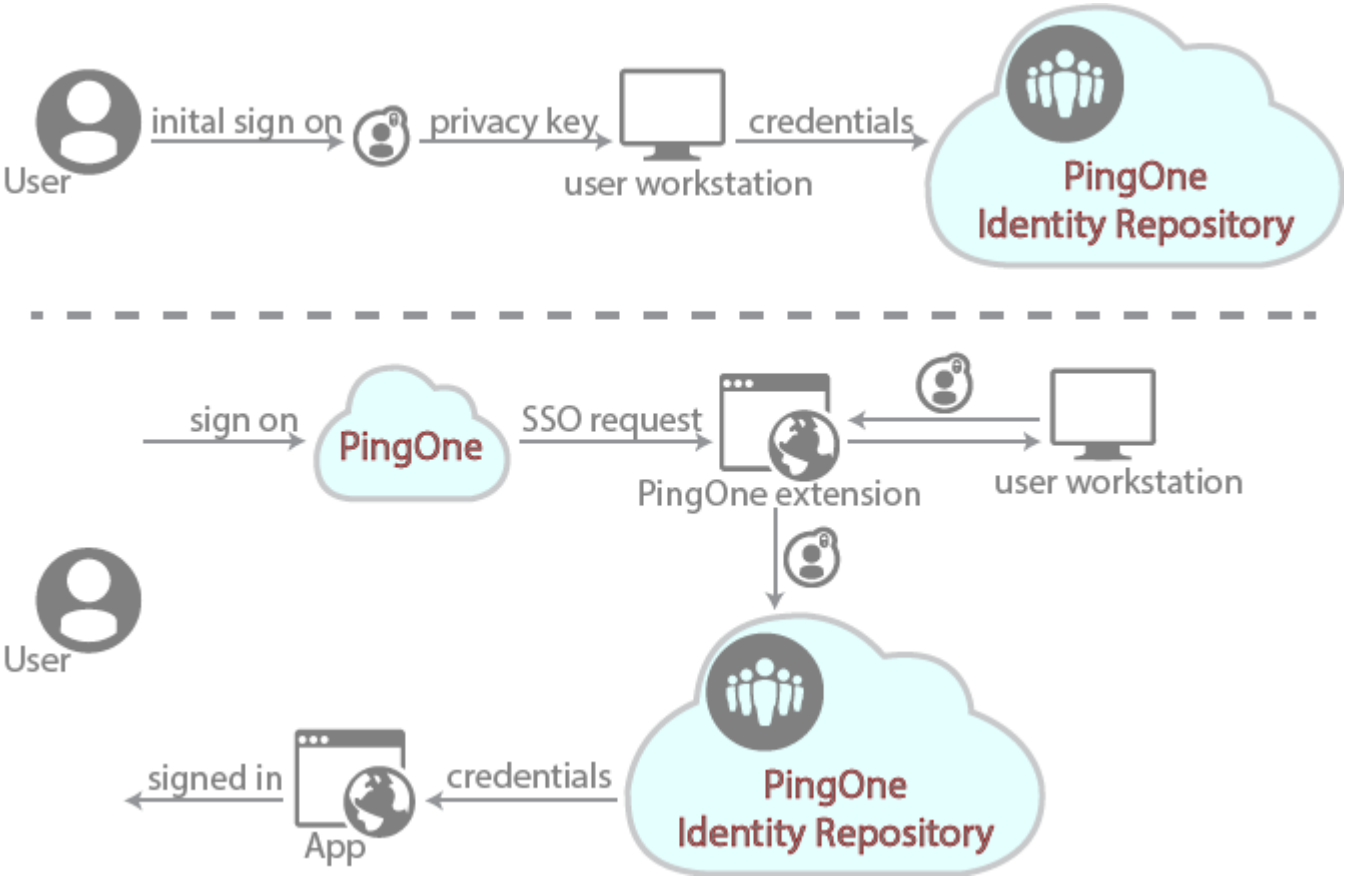
Basic SSO (password vaulting)

Basic SSO (password vaulting) uses the PingOne for Enterprise browser extension to relay credentials to the target cloud application. User credentials are encrypted (128 bit AES) with a user-specified privacy key and are stored in PingOne for Enterprise. The privacy key is stored in the local file system and is never sent to PingOne for Enterprise. PingOne for Enterprise uses stored encrypted credentials for single sign-on (SSO) to your cloud applications. The browser extension can access the encrypted credentials only after a user is authenticated to the identity repository.

To use Basic SSO, you must first enable it on the **Setup > Dock > Configurations** page. For more information, see Configuring the dock when using an identity bridge or Configure the dock when using PingOne for Enterprise Directory.

> **Note**
>
> If you're using Basic SSO applications, there might be circumstances where you want to remove a prior version of the browser extension. You can remove the browser extension using the browser's standard extension or add-on removal process.

How Basic SSO works



What we log for every Basic SSO transaction

Whenever a Basic SSO user signs on with SSO to PingOne for Enterprise, we log the information in the following table. You can see the logging details displayed on your **Reports** page.

Copyright © 2025 Ping Identity Corporation

Parameter	Description
`(date)`	The date and time of the SSO transaction.
`CDP SUBJECT`	The user ID we send to the service provider (SP).
`SUBJECT_FROM_IDP`	The user ID returned by the identity bridge.
`IP`	The user's IP address for this SSO transaction.
`CONNECTION_ID`	A unique ID for the connection we establish between the identity bridge and the application.
`SAAS_ID`	The ID assigned to the user application.
`SP_ACCOUNT_ID`	The PingOne for Enterprise account ID for the SP.
`SP_ACCOUNT_NAME`	The name assigned to the SP account in PingOne for Enterprise.
`TARGET_RESOURCE`	The URL used for the SSO transaction.
`AGENT`	Information about the client or agent used for SSO.
`APP_NAME`	The name of the application used for SSO.
`IDP_ID`	The identity bridge ID used by the SP to identify the identity bridge.
`IDP_ACCOUNT_ID`	The unique account ID for the identity bridge in PingOne for Enterprise.
`IDP_ACCOUNT_NAME`	The name of the identity bridge in PingOne for Enterprise.
`FIRST_NAME_FROM_IDP`	The user's first name as assigned by the identity provider (IdP).
`LAST_NAME_FROM_IDP`	The user's last name as assigned by the IdP.
`EMAIL_FROM_IDP`	The user's email address as assigned by the IdP.
`STATUS`	The status of the SSO transaction.
`ERROR_CODE`	Contains the error information if an error occurs.

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise and SLO

PingOne for Enterprise uses a single logout (SLO) process to log out all participants of a PingOne for Enterprise session. In the PingOne for Enterprise context, the session participants are the identity repository, PingOne for Enterprise, and any applications to which a user has signed on (SSO) for the session.

Any one of the session participants can initiate SLO. PingOne for Enterprise acts as the session authority, mediating the SLO request and response messages so that all participants are notified. In this way, when a user logs off, the PingOne for Enterprise session is ended for all participants.

PingOne for Enterprise supplies three SLO endpoints, each for a particular purpose:

`https://sso.connect.pingidentity.com/sso/SLO.saml2/`

This is the normal SAML endpoint to receive SLO requests and responses. It can be used only by SAML applications or SAML IdPs. Here's an illustration of standard SAML SLO:

1. The user logs out of the SAML application, which results in an SLO request to PingOne.
2. PingOne for Enterprise redirects the request to `https://sso.connect.pingidentity.com/sso/SLO.saml2`.
3. PingOne for Enterprise sends SLO requests to the IdP and the other SAML application.
4. PingOne for Enterprise ends the user session.
5. PingOne for Enterprise sends the SLO response (session ended) to the SAML application.You can append the optional `idpid` parameter to limit SLO only to sessions with the specified `idpid` value.The format for the `idpid` parameter is:

```
https://sso.connect.pingidentity.com/sso/SLO.saml2/?idpid=<idpid value>
```

Copyright © 2025 Ping Identity Corporation

`https://sso.connect.pingidentity.com/sso/initslo/`

This is the PingOne for Enterprise endpoint to which non-SAML applications are redirected in response to their logout request. Here's an illustration initiated by a non-SAML application:

1. The user logs out of the non-SAML application, which results in an logout request to PingOne for Enterprise.
2. If specified, PingOne for Enterprise redirects the request to `https://sso.connect.pingidentity.com/sso/initslo/?page=<landing page URL>`.
3. PingOne for Enterprise sends SLO requests to the IdP and the other SAML application.
4. PingOne for Enterprise ends the user session. You can append the optional `page` parameter to specify a URL to direct logged out users to. The format for the `page` parameter is:

```
https://sso.connect.pingidentity.com/sso/initslo/?page=<landing page URL>
```

If you specify the `page` parameter, PingOne for Enterprise will validate it. To be valid, an SLO `page` parameter value must meet one of the following criteria:

- The URL has the same hostname as the identity provider's (IdP's) SSO URL.
- The URL has the same hostname as the URL of one of the applications in the current session.
- The URL has the same hostname as the `Assertion Consumer Service URL` of one of the applications in the current SSO session.
- The domain of the URL is in the domain list of one of the applications in the current SSO session.
- The URL is https://desktop.pingone.com/*.
- The URL is https://sso.connect.pingidentity.com/*.

If we're unable to validate the SLO page parameter value, the logout process continues and the page parameter is ignored. The PingOne default logout landing page then will be displayed. You can append the optional `idpid` parameter to limit SLO only to sessions with the specified `idpid` value. The format for the `idpid` parameter is:

```
https://sso.connect.pingidentity.com/sso/initslo/?idpid=<idpid value>
```


Copyright © 2025 Ping Identity Corporation

`https://sso.connect.pingidentity.com/sso/terminatesession?page=logoutPageUrl`

This is the PingOne for Enterprise endpoint to which other participants are redirected when SLO isn't supported or isn't configured. The logout requests can be from non-SAML applications, non-SAML IdPs, or from a SAML IdP that doesn't have SLO configured. Here's an illustration of a session termination initiated by a non-SAML application and using Google as the IdP. In this case *logoutPageUrl* is https://accounts.google.com/Logout:

1. The user logs out of the non-SAML application, which results in a logout request to PingOne for Enterprise.
2. PingOne for Enterprise redirects the request to `https://sso.connect.pingidentity.com/sso/terminatesession?page=https://accounts.google.com/Logout`.
3. PingOne for Enterprise ends the user session.

> **Note**
>
> `{google} uses OpenID Connect as the authentication protocol, which does not support SLO.`

You can append the optional `page` parameter to specify a URL to direct logged out users to. The format for the `page` parameter is:

```
https://sso.connect.pingidentity.com/sso/terminatesession?page=logoutPageUrl
```

If you specify the `page` parameter, PingOne for Enterprise will validate it. To be valid, an SLO `page` parameter value must meet one of the following criteria:

- The URL has the same hostname as the identity provider's (IdP's) SSO URL.
- The URL has the same hostname as the URL of one of the applications in the current session.
- The URL has the same hostname as the `Assertion Consumer Service URL` of one of the applications in the current SSO session.
- The domain of the URL is in the domain list of one of the applications in the current SSO session.
- The URL is https://desktop.pingone.com/*.
- The URL is https://sso.connect.pingidentity.com/*.

If we're unable to validate the SLO page parameter value, the logout process continues and the page parameter is ignored. The PingOne for Enterprise default logout landing page then will be displayed. You can append the optional `idpid` parameter to limit SLO only to sessions with the specified `idpid` value. The format for the `idpid` parameter is:

Copyright © 2025 Ping Identity Corporation

```
https://sso.connect.pingidentity.com/sso/terminatesession?idpid=<idpid value>
```

Initiating SSO in PingOne for Enterprise

PingOne for Enterprise supports three methods of initiating single sign-on (SSO).

When a user opens a cloud application through PingOne for Enterprise, there are three participating entities involved in the SSO process: PingOne for Enterprise itself, the identity provider (IdP) storing the user information for your organization, and the service provider (SP) who makes their application available.

By default, when you add an application for SSO by your users, PingOne for Enterprise will initiate the SSO process. If your organization has a policy requiring that SSO is initiated by your IdP or the SP, you can configure either your IdP or the SP for the application as the entity that initiates the SSO process.

The topics in this section will help guide you in selecting and configuring how you want SSO to be initiated for your users.

Why use PingOne for Enterprise-initiated SSO?

- It's easy and works well.
- You don't want users to initiate SSO at the SP.
- You want users to sign on to applications using either the PingOne for Enterprise dock or a custom sign-on page or portal, and you have no need to use IdP-initiated SSO.

Why use IdP-initiated SSO?

- You don't want users to initiate SSO at the SP.
- You want users to sign on to applications using a custom sign-on page or portal, rather than the PingOne for Enterprise dock. You can configure a custom sign-on page or portal using either IdP-initiated SSO or PingOne for Enterprise-Initiated SSO.
- Your organization uses PingFederate and you want to add an application to the PingOne for Enterprise dock using an IdP-initiated SSO URL used by PingFederate.
- Your organization has a policy permitting only IdP-initiated SSO.

Why use SP-initiated SSO?

- You want users to initiate SSO at the SP.
- Users need to sign on to applications that have integrations that aren't browser-based, such as applications that use email integration or applications that use desktop plugins.
- The SP has a policy permitting only SP-initiated SSO.

Configuring PingOne for Enterprise-initiated SSO

SSO that's initiated by PingOne for Enterprise is the default SSO method used for all applications that you add to your account.

Copyright © 2025 Ping Identity Corporation

Steps

- Configure SSO in PingOne for Enterprise.

  Choose from:

  - Use PingOne for Enterprise-initiated SSO with the PingOne for Enterprise dock.

    1. In PingOne for Enterprise, configure a new SAML application.

    For instructions, see Adding or updating a SAML application.

    1. Make the application available to your users on the **Users > User Groups** page. The application is then automatically added to the PingOne for Enterprise dock.

  - Use PingOne for Enterprise-initiated SSO from a custom sign-on page or portal:

    1. In PingOne for Enterprise, configure a new SAML application.

    See Adding or updating a SAML application for instructions.

    1. Add the resulting assigned SSO URL to your custom sign-on page or portal.

Configuring IdP-initiated SSO

About this task

SSO is initiated by the IdP itself, rather than by PingOne for Enterprise. In this case, the IdP needs to reference the particular application for SSO. PingOne for Enterprise assigns a unique ID, the `saasid`, to the connection for each application a SP publishes through PingOne for Enterprise. The IdP uses the `saasid` to reference the application connection for SSO.

If you're using a custom sign-on page or portal instead of the PingOne for Enterprise dock:

Steps

1. In PingOne for Enterprise, configure a new SAML application.

   > **Tip**
   >
   > After you save and publish the application, remain on the **Review Setup** page. You'll need the application configuration information to configure SSO settings.

   See Adding or updating a SAML application for instructions.

2. Use the application's `saasid` value to configure SSO settings in your IdP in one of the following ways:

   Choose from:

   - Add the `saasid` as a query parameter to the connection's ACS URL. For example `https://sso.connect.pingidentity.com/sso/sp/ACS.saml2?saasid=<saasid>`.
   - Configure your IdP to include a `RelayState` parameter along with the SAML request in the format `RelayState=https://pingone.com/1.0/<saasid>`.

3. Get the full IdP-initiated SSO URL from the IdP and add it to your custom sign-on page or portal.

   If PingFederate is your IdP, the IdP-initiated settings used are the `startSSO` and `TargetResource` parameters.

Copyright © 2025 Ping Identity Corporation

Learn more in IdP endpoints.

> **Note**
>
> If you don't specify the `saasid` in your SSO URL, the URL will default to the PingOne for Enterprise dock. If your tenant doesn't include the dock (for example, if you're using PingOne SSO for SaaS Apps or an Invited SSO account), this will result in an error.

Configuring SP-initiated SSO

About this task

SSO is initiated at the SP itself, rather than through PingOne for Enterprise or the IdP. The SP uses the PingOne for Enterprise SSO URL assigned to the IdP to redirect user authentication requests.

Steps

- Configure the SP to initiate SSO.

  Choose from:

  - If you're using PingFederate as the SP:
  - Specify the `AuthenticatingIdpId` query parameter for the PingFederate `/sp/startSSO.ping` endpoint.

    For example:

    ```
    /sp/startSSO.ping?AuthenticatingIdpId=customer001.com
    ```

    For more information, see .pingidentity.com/pingfederate/pf83/index.shtml//[SP services].
  - If you're not using PingFederate as the SP:

    1. Get the application SSO URL from the SP.
    2. Add the application to the PingOne for Enterprise dock using this URL.

For instructions, see Add or update an application using its SSO URL.

Connecting to an identity repository

An identity repository stores identity data for your PingOne for Enterprise users.

About this task

To learn more, see PingOne for Enterprise identity repositories.

You can connect to an identity repository by either:

- Configuring an identity bridge to your identity provider (IdP).
- Using PingOne for Enterprise Directory as your identity repository.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> You can always view the configuration of your identity repository, but if you've established a connection, we recommend that you do not change to a different identity repository. Doing so can invalidate your PingOne for Enterprise dock, applications' attribute mappings, user group assignments, signing certificates, and authentication policy.

If you've not yet established a working connection to an identity repository, you can safely change it.

Steps

1. In the PingOne for Enterprise admin portal, go to **Setup > Identity Repository** and click **Connect to an Identity Repository**.
2. Do one of the following:

   Choose from:

   - Select **PingOne for Enterprise Directory**.
   - Select the identity bridge that's right for your organization. For configuration instructions, choose the link for your identity bridge:
     - Connect to Active Directory
     - Connect to PingFederate
     - Connect to Azure
     - Connect to Google
     - Connect to OpenID Connect
     - Connecting to a custom SAML provider

Select PingOne for Enterprise Directory

About this task

The PingOne for Enterprise Directory supports user provisioning using the current SCIM (System for Cross-Domain Identity Management) protocol. PingOne for Enterprise Directory attributes are SCIM attributes.

> **Note**
>
> For Invited PingOne SSO accounts, you're limited to 5 directory users.

Steps

1. Go to **Setup > Identity Repository**, click **Connect to an Identity Repository**, and select `PingOne for Enterprise Directory`.
2. Click **Next** to assign attribute mapping.

   Currently, only the Phone Number field can be edited here. All other attributes are mapped to their default values. You can assign additional attributes after you complete the setup. See PingOne for Enterprise Directory attributes for more information.

Copyright © 2025 Ping Identity Corporation

3. **Optional:** Click **Add/Invite Users** to add or invite new users. The Users page is displayed. See Add directory users for instructions.

   In most cases, we recommend you create the user groups before adding new users. Refer to Add directory groups and entitlements for more information.

4. Click **Finish**.

When you return to the **Setup > Identity Repository** page, a summary of the settings for your directory is displayed.

Result

The new PingOne for Enterprise Directory is created and ready for you to add groups and add or invite your users. For more information, see Managing PingOne for Enterprise Directory users.

Manage directory settings

These settings apply to all PingOne for Enterprise Directory users.

Configure the directory password policy

About this task

You need to be either a Global Administrator or Identity Repository Administrator to configure the password policy for your directory users. You will edit the default password policy to assign password requirements, expiration settings and lockout settings.

> **Note**
>
> The PingOne for Enterprise Directory uses HMAC SHA-256 with salt for hashing passwords.

Steps

1. Go to **Setup > Directory Settings > Password Requirements**.
2. Change any of the minimum requirement settings as needed:

Setting	Description
Minimum Length	The minimum number of characters required.
Minimum Uppercase Characters	The minimum number of uppercase characters required.
Minimum Numbers	The minimum number of numbers required.
Minimum Special Characters	The minimum number of special characters required (such as, @ # ! % &).
Block Dictionary Words	If enabled, common dictionary words aren't allowed as passwords.

Copyright © 2025 Ping Identity Corporation

Setting	Description
Block Prior Passwords	If enabled, previously used passwords aren't allowed.

3. Assign any of the password expiration settings as needed:

Setting	Description
Password Duration	The number of days a password remains valid. When set to 0 (zero), passwords will never expire.
First Notification	The user will receive their first notice of an expiring password this number of days before expiration.
Second Notification	The user will receive their second notice of an expiring password this number of days before expiration.
Password Expiry Notifications	When enabled, an email notification is sent to users prior to their password expiring.

4. Change any of the account lockout settings as needed:

Setting	Description
Consecutive Failures to Trigger Lockout	The number of consecutive, failed attempts to sign on needed to trigger an account lockout.
Consecutive Failure Timeframe	The length of time a user remains locked out (in minutes).
Lockout Duration	The length of time without user activity (in minutes) that's needed before the count of failed sign on attempts is reset to zero.
Password Lockout Notifications	When enabled, an email notification is sent to users when their password has expired and they are locked out.

Allow self registration for new directory users

About this task

You need to be either a Global Administrator or Identity Repository Administrator to enable self registration for your directory users. You will edit the default registration settings for new directory users to allow self registration.

Steps

1. Go to **Setup > Directory > Registration**.
2. Click **Edit**.

Copyright © 2025 Ping Identity Corporation

3. Set the registration options:

Setting	Description
User Invite Duration	Click the arrow buttons to increase or decrease the number of hours a user invitation remains valid. The duration range is 1 hour to 168 hours.
Allow Self Registration	If enabled, as an additional method of new user registration, you can direct new users to the PingOne for Enterprise `Registration URL` that's automatically assigned when you enable this setting. You're still able to create or invite new users using the process described in Add directory users. **Note** All of the remaining settings on this page apply only to self registration. If you do not select the checkbox to allow self registration, the other settings are not applied or saved.
Approval Required	If enabled, this setting indicates that an administrator needs to approve all new user registrations that occur through the self registration site. The users will not be able to access PingOne for Enterprise until the administrator has approved their registration.
Self Registration Email Domains	Use this field to restrict the email domains that can be used for self registration. Enter the allowed email domain or domains (comma-delimited). **Note** If you do not enter any email domains, all domains are allowed for self registration.
Email Address for Notifications	When a new user registers at the self registration site, an email notifying you of the new registration is automatically sent to this address. Leave this blank if you do not want to receive notification emails.
Email Address for Summaries	A daily summary of user registrations at the self registration site is sent to the email address you enter here. Leave this blank if you do not want to receive daily registration summaries.
Registration URL	If you've enabled `Self Registration`, this URL is automatically assigned when you save your changes on this page. This is the URL to which you need to direct any new users that you want to be able to self-register.

Copyright © 2025 Ping Identity Corporation

Setting	Description
Reply-to Email Address	You can choose to assign a custom email address to use as the reply-to email address displayed in the registration invitation email that is sent to the user. The default is no-reply@pingidentity.com (an unattended email address).

4. Click **Save Changes** when you're done.

Manage directory attributes

About this task

You need to be either a Global Administrator or Identity Repository Administrator to add an attribute to the directory. For more information about changing administrative roles, see Editing administrative roles, permissions, and notifications.

The predefined attributes for the directory are SCIM version 1.1 core schema attributes. See System for Cross-Domain Identity Management: Protocol 1.1 for more information.

For more information, see PingOne for Enterprise Directory attributes.

Steps

- Go to **Setup > Directory Settings > Attributes**.

  Result:

  The attributes that are currently applied to the directory are displayed. A check in the Registration column indicates the attribute is displayed on the new user registration page. A check in the Required column indicates the attribute must be assigned a value.

- Click **Details** for an attribute to display the attribute information.

  Attributes that are Complex data types are multivalued attributes. For example, if you display the details for the `Name` attribute, you will see the multiple values listed in the Elements panel.

  1. For multivalued attributes, click the **Details** button in the Elements panel to display the properties of the attribute element.

- To reorder the listing of attributes, click **Reorder Attributes**.

The reordering will be applied to the attributes on the **User details** page as well as the listing displayed here.

1. Select and drag attributes into different positions within the listing.
2. Click **Save** when you're done.
   - To add an attribute,
3. Click **Add Attribute**.
4. Select an attribute from the **Add Attribute** window.
5. Click **Add**.

Copyright © 2025 Ping Identity Corporation

Result:

The attribute is available when configuring the dock or applications.

- To remove an attribute, click the **down arrow** on the attribute line and click **Remove**.

Add directory attributes

About this task

You need to be either a Global Administrator or Identity Repository Administrator to add an attribute to the directory. For more information about changing administrative roles, see Editing administrative roles, permissions, and notifications.

The predefined attributes for the directory are SCIM version 1.1 core schema attributes. For more information, see System for Cross-Domain Identity Management: Protocol 1.1.

Steps

1. Go to **Setup > Directory > Attributes**.

The attributes that are currently applied to the directory are displayed.

1. Click **Add Attribute** to add more predefined attributes.

   Result:

   The listing of available attributes from the SCIM core schema is displayed.

2. Select the attribute to add and click **Add**.

   Result:

   The attribute is added to the listing.

3. Click **Save Attribute** when you're finished.

Remove directory attributes

About this task

You need to be either a Global Administrator or Identity Repository Administrator to remove an attribute from the directory. You cannot remove an attribute that is listed as Required or used for Registration.

Steps

1. Go to **Setup > Directory Settings > Attributes**.
2. For the attribute to remove, click the down-arrow next to the Details button and click **Remove**.

   Result:

   The selected attribute is removed from the directory attributes used.

3. Repeat these steps for any additional attributes to remove.

Copyright © 2025 Ping Identity Corporation

View or renew directory API credentials

Find or update your PingOne for Enterprise Directory API Client ID and API key.

About this task

Any client applications that are to access the PingOne for Enterprise Directory for your account must use the directory API credentials assigned to your account. These credentials are displayed on the Credentials page, and consist of the Client ID and API Key for your account. The Client ID setting is tied to your account and cannot be changed. You need to be either a Global Administrator or Identity Repository Administrator to renew the API key. If necessary, you can also generate a new API key.

The API Credentials page isn't accessible for PingOne for Enterprise trial accounts.

The locations of the Directory API are:

- (North America) https://directory-api.pingone.com/api
- (Europe) https://directory-api.pingone.eu/api
- (Australia) https://directory-api.pingone.com.au/api

> **Note**
>
> We implement rate limiting on PingOne for Enterprise Directory APIs to maintain a high quality of service for all our customers. Rate limiting restricts any one API client from flooding PingOne for Enterprise Directory APIs with an unusually high amount of traffic, which could affect usage of PingOne for Enterprise Directory by other customers. If a customer reaches the defined rate limit, the PingOne for Enterprise Directory API responds with a 429 HTTP status code (Too Many Requests).
> If your integration hits the rate limit, you will need to reduce the rate at which your API client is making requests in order to complete any further API calls successfully. The enforcement of an API rate limit is standard practice for SaaS services. If rate limits are negatively affecting your usage of the PingOne for Enterprise Directory API, please contact our support team, so we can review your integration.

Steps

1. Go to **Setup > Directory Settings > API Credentials**.
2. To generate a new API key:
    1. Click **Edit** to switch to Edit mode.
    2. Click **Renew** to generate a new API key, then click **Save**.

Next steps

For more information about creating API requests, see the PingOne for Enterprise Directory API documentation.

Assign directory branding and designs

About this task

The branding and design settings apply to the following user-facing pages for PingOne for Enterprise Directory:

- Login page

Copyright © 2025 Ping Identity Corporation

- Self-service registration page
- Password reset page

These settings are all optional. At any point after assigning settings, you can click the **Restore Defaults** button at the top of the page to use the PingOne for Enterprise Directory default branding and design settings.

You can also assign branding and design settings for the PingOne dock. See Assign branding and design for more information.

You need to be either a Global Administrator or Identity Repository Administrator to assign these settings.

Steps

1. Go to **Setup > Directory > Branding**.
2. For **Logo**, choose to use either your corporate logo (set on the **Account > Branding** page), or a custom logo that you assign here.

   The standard maximum display dimensions are 72px high by 350px wide. The image dimension ratio is preserved. For the logo to render optimally on high-definition displays (such as Apple Retina displays), double the dimensions to 144px high by 700px wide.

   The maximum file size for the image is 10 Mb.
3. For **Backgrounds**, you can set the following:

   1. For **Main Background**, choose either an image or a color setting to use as the background for pages.

   The maximum file size for the image is 10 Mb.

   1. For **Form Background Color**, choose a color setting to use as the background for forms.
4. For **Buttons**, you can set the following:

   1. For **Button Color**, choose a color setting to use for buttons.
   2. For **Button Font Color**, choose a color setting to use for button text.
5. For **Text**, you can set the following:

   1. For **Form Fill Color**, choose a color setting to use as the fill for entry boxes on forms.
   2. For **Form Font Color**, choose a color setting to use for text in forms.
   3. For **Link Color**, choose a color setting to use for links.
   4. For **Header and Custom Text Color**, choose a color setting to use for the header and any text in the page header.
6. For **Content**, you can set the following:

   1. For **Registration Page Header**, enter up to 100 characters to use as the Registration page header.
   2. For **Registration Page Text**, enter up to 300 characters to use as custom text at the top of the Registration page.
   3. For **Login Page Header**, enter up to 100 characters to use as the Login page header.
   4. For **Login Page Text**, enter up to 300 characters to use as custom text at the top of the Login page.
   5. For **Reset Password Header**, enter up to 100 characters to use as the Reset Password page header.

Copyright © 2025 Ping Identity Corporation

6. For **Reset Password Custom Text**, enter up to 300 characters to use as custom text at the top of the Reset Password page.

7. Click **Save** to save your new settings.

PingOne for Enterprise Directory attributes

You can find the PingOne for Enterprise Directory attributes on the **Setup > Directory > Attributes** page in the PingOne for Enterprise admin portal. The list of commonly used attributes is displayed on this page. You can display the additional attributes available by clicking **Add Attribute**. The attributes we make available are:

Attributes available by default

Attribute	Description
userName	The name to assign to the account user. The name must be unique within the account.
externalId	The UUID for the user (assigned by PingOne).
name	A multivalued attribute fully identifying the user. The subattributes are: • givenName • middleName • familyName • honorificPrefix • honorificSuffix
emails	A multivalued attribute for the email addresses associated with the user. The subattributes are: • type • primary • secondary
id	The UUID for the account user.
active	A boolean value indicating whether the account user is currently active.
userType	The type of account user (such as, administrator).

Copyright © 2025 Ping Identity Corporation

Additional attributes available

Attribute	Description
preferredLanguage	The user's preferred written or spoken language (for selecting a localized user interface).
displayName	The user's name to be displayed.
locale	The user's default location (for localized display of data, such as currency).
timezone	The default timezone for the user.
nickName	A nickname to assign to the user.
title	The user's title within the organization.
profileUrl	A fully qualified URL for the page representing the user's online profile.
entitlements	A multivalued attribute for the entitlements assigned to the user. The subattributes are one or more entitlement entries: • value
x509Certificates	(API use only) A multivalued attribute for the x509 certificates assigned to the user. The subattributes are one or more certificate entries: • value
phoneNumbers	A multivalued attribute listing the phone numbers associated with the user. The subattributes are: • fax • home • mobile • other • pager • work

Copyright © 2025 Ping Identity Corporation

Attribute	Description
addresses	A multivalued attribute listing the physical addresses associated with the user. The subattributes are: • type • streetAddress • locality • region • postalCode • country • formatted • primary
ims	A multivalued attribute listing the instant messaging service or services associated with the user. The subattributes are one or more pairs of type/value entries: • type • value
roles	A multivalued attribute listing of the role or roles associated with the user within the account. The subattributes are one or more role entries: • value

Connect to Active Directory

The identity bridge for Active Directory® is PingOne® AD Connect. You can choose to install standard AD Connect or AD Connect with IIS.

Standard AD Connect

AD Connect uses a secure back channel protocol to communicate with PingOne. This is an inbound/outbound connection on port 443. No other external access to the AD Connect host is necessary. AD Connect doesn't need you to open ports in a firewall, install IIS, or employ signing certificates. You can optionally use Integrated Windows Authentication (IWA) as the authentication protocol on your network. High availability (automatic failover and load balancing) is handled by the PingOne datacenters, and requires no configuration or management on your part. User provisioning is an optional feature.

> **Note**
>
> You cannot use a proxy for AD Connect back channel transactions. However, you can use a proxy for REST calls to AD Connect (https://connect.pingidentity.com).

If you have an existing AD Connect with IIS installation, you can stop or uninstall IIS. You can then install AD Connect instead. The open ports for AD Connect with IIS are no longer required.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> You will want to install AD Connect with IIS rather than standard AD Connect if you prefer to use your own solution for high availability.

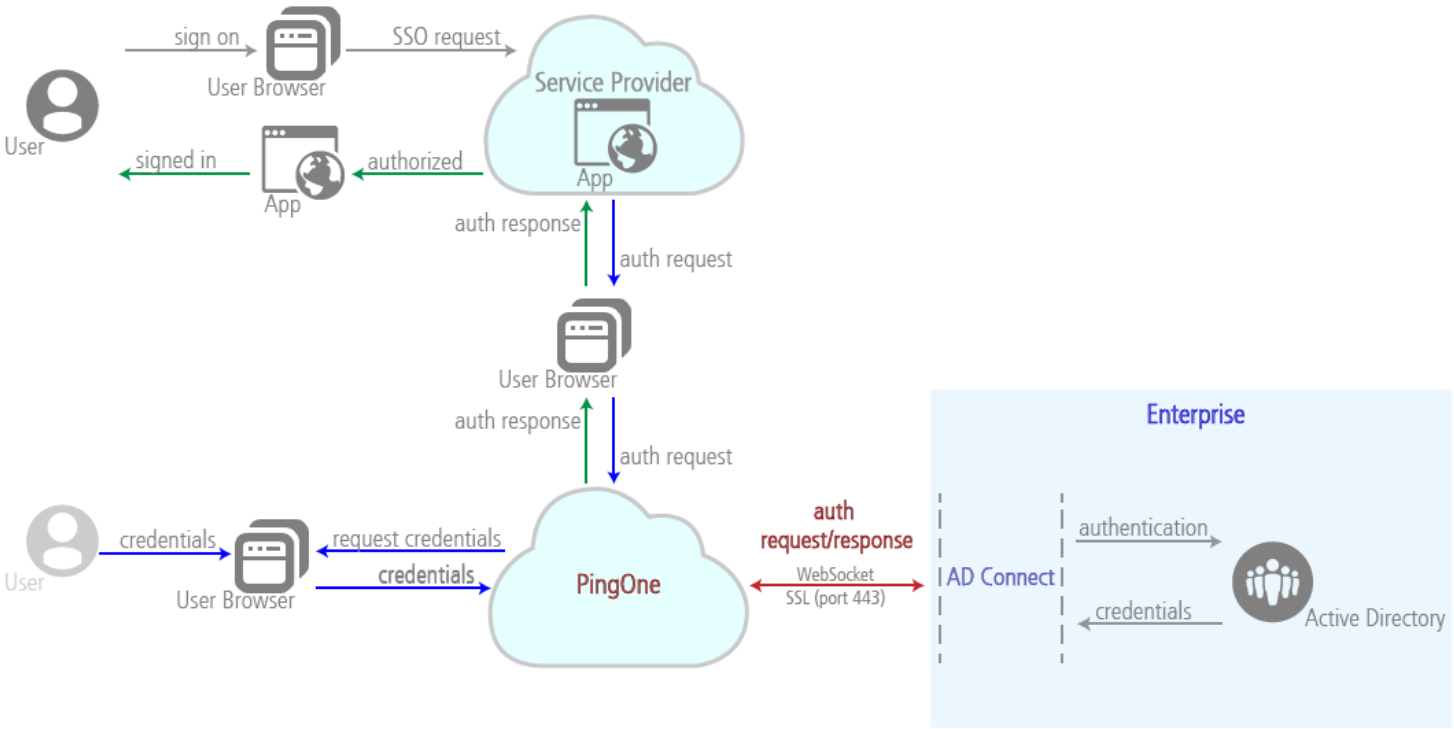
AD Connect with IIS

AD Connect with IIS uses the SAML 2.0 protocol to communicate with PingOne. It is necessary that you ensure the security of your IIS host, and high availability is an option you may want to consider. User provisioning is an optional feature.

> **Note**
>
> You will want to install AD Connect with IIS rather than standard AD Connect if you prefer to use your own solution for high availability.

How AD Connect works

AD Connect is a Ping product that enables connections between Microsoft Active Directory (AD) and PingOne for Enterprise.



1. AD Connect connects to PingOne for Enterprise through a WebSocket secure connection on port 443 and authenticates PingOne for Enterprise using SSL.
2. PingOne for Enterprise authenticates the requesting AD Connect instance using the digital signature.

> **Note**
>
> AD Connect doesn't need an SSL certificate. This connection is used for full-duplex communications between PingOne for Enterprise and AD Connect services.

Copyright © 2025 Ping Identity Corporation

3. PingOne for Enterprise sends the authentication request to AD Connect using a WebSocket backchannel.

   The PingOne for Enterprise authentication request sent to AD Connect is a token that contains the username and password encrypted with the public key of the selected AD Connect instance.

   > **Note**
   >
   > Only the intended AD Connect instance can decrypt the request token.

4. AD Connect validates the username and password with Active Directory and sends a response token back to PingOne for Enterprise.

   > **Note**
   >
   > The response tokens are only valid for a single use.

High availability and failover

For high availability and failover, you can install multiple instances of AD Connect. The status of the connection for each AD Connect instance is stored in and managed by PingOne for Enterprise. PingOne for Enterprise selects an AD Connect instance to use from the active list of instances and begins sending authentication requests to that instance. The load is balanced among all instances of AD Connect. New instances of AD Connect are added to PingOne for Enterprise's active list of instances.

AD Connect with IWA

When you install AD Connect, the PingOne for Enterprise admin portal gives you the option to enable integrated Windows authentication (IWA). You specify the IP address or IP range, in IP blocks, for PingOne for Enterprise to use in identifying whether or not a user request is from your organization's network.

The IP address needs to be (or the IP range needs to include) the IP address of the AD Connect host as identified by PingOne for Enterprise.

> **Tip**
>
> You can find the IP address by opening a web browser and searching for `my ip`.

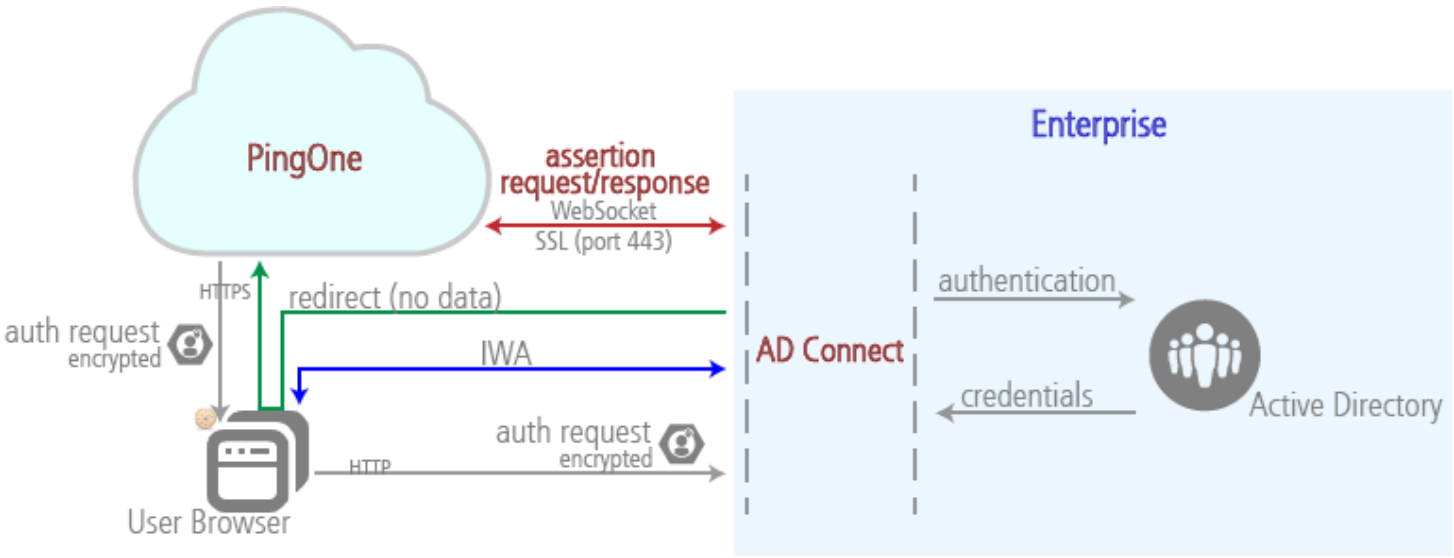
When IWA is enabled, AD Connect listens on port 80, which doesn't need to be externally exposed, and PingOne for Enterprise tries to use IWA to authenticate user requests coming from your organization's network. When PingOne for Enterprise doesn't use IWA, PingOne for Enterprise prompts the user for their credentials, and validates the credentials using the WebSocket backchannel.

> **Note**
>
> Each user's initial single sign-on (SSO) to PingOne for Enterprise always uses the WebSocket backchannel, regardless of whether or not the user is located in your organization's network.

Optional IWA support for AD Connect works like this:

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise



1. If a user within the defined IP range makes an authentication request, PingOne for Enterprise redirects the user to AD Connect's IWA page with a token on port 80. If the user is outside of the IP range, they are directed to the PingOne for Enterprise sign on page.
2. The user authenticates through IWA. AD Connect stores the authentication assertion and any user attributes locally, and redirects the user to PingOne for Enterprise with no data.
3. PingOne for Enterprise retrieves the authentication assertion from IWA. It does so through the Websocket so it can retrieve the assertion securely even though AD Connect doesn't use SSL on the IWA page.
4. PingOne for Enterprise validates the assertion and authenticates the user. If an error occurs, the user is directed to the PingOne for Enterprise sign on page.

AD Connect with IIS

When you use AD Connect with IIS, PingOne for Enterprise directs users to the sign-on page hosted by IIS. The user enters their credentials and AD Connect submits them to Active Directory for authentication.

Because PingOne for Enterprise directs the user to the AD Connect sign-on page in the browser, the identity bridge configuration includes the URL for AD Connect with IIS.

AD Connect with IIS doesn't use a Websocket backchannel to communicate with PingOne for Enterprise. User authentication takes place in the IIS application, which then generates a SAML assertion that is sent to PingOne for Enterprise through the browser using the redirect or POST protocols. Unlike standalone AD Connect, AD Connect with IIS requires an SSL certificate to authenticate users.

> **Note**
>
> If you use multiple instances of AD Connect with IIS, you must deploy them behind a load balancer. PingOne for Enterprise directs users to the URL of the load balancer for authentication rather than the URL of a specific AD Connect with IIS instance.

Copyright © 2025 Ping Identity Corporation

AD Connect in a DMZ

When installing AD Connect on a host in a DMZ, you will need to open the following ports between the DMZ and your internal network:

> **Note**
>
> TCP and UDP are shown together below. Depending on the firewall network device, you may need to add the TCP and UDP rules separately.

TCP/UDP 389, 636, 3268, 3269

These are the Lightweight Directory Access Protocol (LDAP) ports. AD Connect uses LDAP to access the Active Directory DC (when in-network or Windows Authentication is used). Also used for mobile authentication.

UDP 138

NetBIOS name resolution.

TCP/UDP 445

SAM/LSA.

UDP 123

NTP W32 Time.

TCP/UDP 135, 49152-65535

RPC Endpoint Mapper.

UDP 137

NetBios datagram.

TCP/UDP 88

This port belongs exclusively to Kerberos. AD Connect uses this port for off-network access when executing a single sign-on (SSO) event outside of the corporate network.

TCP/UDP 464

This server port is also used by Kerberos (to set or change the password).

TCP/UDP 53

The DNS service runs on this port. It's used to convert between URLs and IP Addresses.

Installing AD Connect

To designate AD Connect as your identity repository, install AD Connect to your server and configure PingOne for Enterprise to connect to it.

Copyright © 2025 Ping Identity Corporation

Before you begin AD Connect requirements:

- One of the following platforms:
  - Microsoft Windows Server 2019 Desktop (not Core)
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2012
- TLS 1.2
- Microsoft .NET Framework 4.7.2 installed. The framework installation file is packaged with the AD Connect distribution.
- Port requirements:
  - TCP 443 inbound/outbound (Websocket connections to PingOne for Enterprise)
  - (If IWA is enabled) TCP 80 internal, inbound/outbound (IWA connections)
- Ensure that the AD Connect account lockout option is enabled for all PingOne for Enterprise users. This is necessary to protect user information in PingOne for Enterprise.
- AD Connect does not support authentication using IWA with Microsoft 365 or mobile devices. IWA does not work with iOS.

About this task

You must install AD Connect on a Windows Server host that resides in an Active Directory domain.

If you're installing AD Connect on a host in a DMZ, you must ensure some ports are open. For more information, see AD Connect in a DMZ.

Steps

1. Go to **Setup > Identity Repository**, and then click **Connect to an Identity Repository**.

   If you are changing to AD Connect from another identity repository, click **Change Identity Repository**.
2. Select **Active Directory**. Click **Next**.
3. Download AD Connect:
   1. Click **Download AD Connect** and save the `adconnect-installer.zip` file to your directory.
   2. Extract the `.zip` file and open the `ADConnectSetup.msi` file to start the installer.
   3. When the installer starts, click **Next**.
   4. On the **Installation Type** window, select **AD Connect**. Click **Next**.
   5. **Optional:** To enable users and groups to be automatically provisioned into PingOne for Enterprise, select **Enable user provisioning**.
4. Set up the product key:
   1. In **PingOne for Enterprise**, on the **Set Up Product Key** tab, in the **Product Key** text field, enter a key.

Copyright © 2025 Ping Identity Corporation

2. In the **AD Connect Installer**, on the **Enter Product Key** field, enter the same key you entered in the previous step.

5. Install AD Connect:

    1. From the **Install AD Connect** tab in **PingOne for Enterprise**, copy the **Organization ID** value.
    2. In the **AD Connect installer**, paste the value in the **Enter Organization ID** field and click **Activate**.

        Result:

        If the product key and organization ID match in both PingOne for Enterprise and the AD Connect installer, the AD Connect installer displays a confirmation message.

    3. Click **Next**.
    4. In the **Destination Folder** window, enter the destination folder where you will install AD Connect. Click **Next**.
    5. Click **Install**.
    6. When the installation finishes, click **Finish**.
    7. In **PingOne for Enterprise**, click **Verify Installation**.

        Result:

        PingOne for Enterprise displays a message confirming the installation.

    8. Click **Next**.

6. In **PingOne for Enterprise**, from the **Authentication - Account Lookup Method** list, select the Active Directory attribute to verify the user account:

    Choose from:

    - **Mail**: the email address assigned to the user.
    - **sAMAccountName**: The legacy Windows login name for the user
    - **Filter**: An LDAP filter to use when looking up the account information for the user
    - **userPrincipalName**: Typically the user's email address without the divider or the domain

7. From the **Subject Attribute** list, choose a value to return to your applications as the SAML subject.

    Possible values are **sAMAccountName** or **userPrincipalName**. **userPrincipalName** is appropriate for most organizations.

8. **Optional:** To pass Windows credentials through your web browsers for automated authentication, click **Enable Integrated Windows Authentication**.

    > **Note**
    >
    > This requires further configuration for your web browsers. For more information, see Using IWA with browser clients.

9. **Optional:** To allow users to reset their Active Directory password from the PingOne for Enterprise sign-on page, click **Enable Password Change**.

10. **Optional:** To return all of the nested group memberships for your users, click **Enable Group Hierarchy**.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Enabling this option can cause sign-ons to take longer.

11. Click **Next**.
12. On the **Map Attributes** tab, map attributes from Active Directory to the SAML assertions for your applications.
    1. For the **SAML_SUBJECT** list, select the same value that you chose for the **Subject Attribute** list in the previous tab.
    2. For the **memberOf** attribute, select **memberOf**.
    3. For the **fname** attribute, select **givenName**.
    4. For the **lname** attribute, select **sn**.
    5. For the **email** attribute, select **mail**.
    6. For the **phoneNumber** attribute, select **telephoneNumber**.
13. Click **Save**.

Next steps

To assign branding for your AD Connect connection, see Assign AD Connect branding and designs.

Assign AD Connect branding and designs

About this task

The branding and design settings apply to the following user-facing pages for AD Connect:

- Login page
- Password reset page

These settings are all optional. At any point after assigning settings, you can click the **Restore Defaults** button at the top of the page to use the AD Connect default branding and design settings.

You can also assign branding and design settings for the PingOne dock. See Assign branding and design for more information.

You need to be either a Global Administrator or Identity Repository Administrator to assign these settings.

Steps

1. Go to **Setup > Branding > Logon & SSO**.
2. For **Logo**, choose to use either your corporate logo (set on the **Account > Branding** page), or a custom logo that you assign here.

   The standard maximum display dimensions are 72px high by 350px wide. The image dimension ratio is preserved. For the logo to render optimally on high-definition displays (such as Apple Retina displays), double the dimensions to 144px high by 700px wide.

   The maximum file size for the image is 10 Mb.

Copyright © 2025 Ping Identity Corporation

3. For **Backgrounds**, you can set the following:
    1. For **Main Background**, choose either an image or a color setting to use as the background for pages.

    The maximum file size for the image is 10 Mb.

    1. For **Form Background Color**, choose a color setting to use as the background for forms.
4. For **Buttons**, you can set the following:
    1. For **Button Color**, choose a color setting to use for buttons.
    2. For **Button Font Color**, choose a color setting to use for button text.
5. For **Text**, you can set the following:
    1. For **Form Fill Color**, choose a color setting to use as the fill for entry boxes on forms.
    2. For **Form Font Color**, choose a color setting to use for text in forms.
    3. For **Link Color**, choose a color setting to use for links.
    4. For **Header and Custom Text Color**, choose a color setting to use for the header and any text in the page header.
6. For **Content**, you can set the following:
    1. For **Login Page Header**, enter up to 100 characters to use as the Login page header.
    2. For **Login Page Text**, enter up to 300 characters to use as custom text at the top of the Login page.
    3. For **Reset Password Header**, enter up to 100 characters to use as the Reset Password page header.
    4. For **Reset Password Custom Text**, enter up to 300 characters to use as custom text at the top of the Reset Password page.
7. Click **Save** to save your new settings.

Using IWA with browser clients

You can enable your users' browser clients for seamless SSO with AD Connect using Integrated Windows authentication (IWA).

Before you begin

Ensure that:

1. Your AD Connect configuration in PingOne for Enterprise has an `Authentication Type` value of `Integrated`. This authentication type uses Integrated Windows Authentication (IWA).
2. Port 80 is open for use by AD Connect.
3. The browser clients for your users have the AD Connect host listed as a trusted site.

Click the corresponding tabs for instructions on adding trusted sites to Google Chrome, Microsoft Edge, and Mozilla Firefox.

Copyright © 2025 Ping Identity Corporation

Chrome

Adding trusted sites to Chrome
Steps

1. In Chrome, go to **Settings** > **Privacy and Security**.
2. Click **Third-party Cookies**.
3. Click **Add**.
4. In the **Site** field, enter the host name of the AD Connect host.
5. Click **Add**.

Edge

Adding trusted sites to Edge
Steps

1. In Windows, open the **Control Panel**.
2. Go to **Network and Internet** > **Internet Options**.
3. In the **Internet Properties** window, go to **Security** > **Trusted Sites** > **Sites**.
4. In the **Add this website to the zone** field, enter the host name of the AD Connect host.
5. Click **Add**, then click **Close**.

Firefox

Adding trusted sites for Firefox
Steps

1. In Firefox, enter `about:config` in the URL address bar.
2. Click **Accept the Risk and Continue**.
3. In the **Search** bar, enter `network.negotiate`.
4. Click the **Pencil** icon for **network.negotiate-auth.trusted-uris**.
5. In the field that opens, enter the host name of the AD Connect host.
6. Click the **Save** icon.

Result

The name of the AD Connect host is displayed as the value of **network.negotiate-auth.trusted-uris**.

Copyright © 2025 Ping Identity Corporation

AD Connect final setup

Complete the setup or manual update of AD Connect, verify the AD Connect installation, and configure additional settings in PingOne for Enterprise.

About this task
Steps

1. On the PingOne for Enterprise admin portal page for AD Connect, click **Verify Installation**.

> **Note**
>
> If you're using AD Connect in a clustered, high availability configuration, you will verify the installation in the PingOne admin portal only for the initial AD Connect installation.

2. **Optional:** Choose whether to enable Integrated Windows Authentication (IWA).

   When enabled, IWA is applied when the user is on your organization's network. When the user comes from outside your network, NTLM is used. A user is prompted for their credentials only once per browser session.

   1. If you enable IWA, the **Intranet IP Ranges** entry box is displayed. Your entries here apply IWA to all users whose IP addresses are specified or contained within a block of IP addresses. The addresses need to be IPv4 addresses in dot-decimal format (123.123.123.123), or an IPv4 address block in CIDR format (123.123.123.0/24).

3. In **AD Connect Configuration**, the following settings are available:

Authentication Account Lookup Method

Assigns the Active Directory attribute to use when looking up the account information for the user during delegated authentication. This can be:

- **Mail**. The email address assigned to the user.
- **sAMAccountName**. The legacy Windows logon name for the user.
- **Filter**. An LDAP filter to use when looking up the account information for the user.
- **userPrincipalName**. We recommend you use `userPrincipalName` if you select the **Enable Global Catalog** option.

Subject Attribute

Choose the value to use for `SAML_SUBJECT`. The possible values are `sAMAccountName` or `userPrincipalName`.

> **Tip**
>
> If your user population comes from multiple domains, choose `userPrincipalName` as the subject attribute to avoid the potential of different users in different domains signing in using the same username.

Copyright © 2025 Ping Identity Corporation

Enable Delegated Windows Authentication

Select to enable a URL automatically created by PingOne that is unique to your account. We use this URL to verify the credentials used for sign-on requests received when a Salesforce user attempts to sign on using either the Salesforce UI or API.

To ensure security, PingOne also generates a random key that is associated with this URL. If the existing key is compromised, click **Renew** to generate a new random key for the URL.

Enable Password Change

Select to enable users to change their corporate passwords through AD Connect. When enabled, a Change My Password option is displayed on the AD Connect sign on screen. Users selecting this option are prompted for their existing password and the new password to use. Their password is then changed in Active Directory.

Enable Group Hierarchy

Select to enable support for group hierarchies in Active Directory. When enabled, Active Directory groups that are nested will inherit the SSO permissions of their parent group or groups. When disabled (the default), an Active Directory group uses only the SSO permissions that are assigned to it, with no inheritance.

Enable Global Catalog

Select to use the Active Directory Global Catalog for user lookup. When enabled, we recommend you use `userPrincipalName` as the **Authentication Account Lookup Method**.

4. Assign the Active Directory-to-PingOne attribute mapping.

   This assignment maps Active Directory attributes to the default PingOne attributes. This attribute mapping is not used by applications that you add to PingOne. You will configure those attribute mappings for each application.

   1. For any of the attribute mappings, you can choose to configure an advanced mapping. See Creating advanced attribute mappings for instructions.

5. Click **Finish**.

   When you return to the **Setup > Identity Repository**, a summary of the settings for your identity bridge is displayed.

Next steps

If you're using AD Connect in a clustered, high availability configuration, repeat these steps on each AD Connect host.

AD Connect security best practices

Keep your AD Connect configuration and data secure with the following tips and tools.

Copyright © 2025 Ping Identity Corporation

Encrypt configuration files

AD Connect stores configuration data in the following files:

- `AuthenticationAgent.exe.config`
- `Provisioner.exe.config`
- `Softwareupdater.exe.config`

> **Note**
>
> These files contain sensitive data, such as the product key.

You can encrypt these files using the Windows `Aspnet_config.exe` utility.

> **Important**
>
> Because of a limitation of `Aspnet_config.exe`, you must:
>
> 1. Rename the configuration files to `web.config`.
> 2. Run `Aspnet_config.exe` to encrypt the files.
> 3. Rename the files back to their original filenames.

For more information, see Encrypting and Decrypting Configuration Sections in the Microsoft documentation.

> **Warning**
>
> Ping Identity does not test AD Connect with encrypted configuration files. Encrypting these files could cause unforeseen complications, and you do so at your own risk.
> If encrypted configuration files do cause trouble, you can reinstall AD Connect.

Enable IWA

If you enable Integrated Windows Authentication (IWA), users within your organization's network will be authenticated through IWA. This improves security by reducing the need for user credentials to be communicated over the internet.

However, IWA has other limitations to consider. For example, your users will be unable to sign off of PingOne for Enterprise because IWA will automatically sign them back on.

For more information, see Using IWA with browser clients.

Copyright © 2025 Ping Identity Corporation

Use `userPrincipalName` as the subject attribute

AD Connect has two options for which attribute to use as the subject attribute. While `sAMAccountName` is unique only within an Active Directory (AD) domain, `userPrincipalName` is unique across all AD domains.

If your user population contains multiple AD domains, select `userPrincipalName` as the subject attribute to avoid the potential of different users in different domains signing in using the same username.

For more information, see AD Connect final setup.

Installing AD Connect with IIS

To designate AD Connect with IIS as your identity repository, install AD Connect to your server and configure PingOne for Enterprise to connect to it.

Before you begin

AD Connect with IIS requirements:

- One of the following platforms:
  - Microsoft Windows Server 2019 Desktop with IIS 10.0

    > **Note**
    >
    > Microsoft Windows Server 2019 Core is not supported.

  - Microsoft Windows Server 2016 with IIS 10.0
  - Microsoft Windows Server 2012 R2 with IIS 8.0 (32-bit/64-bit)
  - Microsoft Windows Server 2012 with IIS 8.0 (32-bit/64-bit)
- TLS 1.2
- Administrator privileges on the Windows Server IIS host.
- The Windows Server IIS host must reside in an Active Directory domain, but for security reasons, must not be a domain controller (DC). We highly recommend that AD Connect is installed on its own IIS host to avoid potential conflicting IIS version requirements for other applications (such as SharePoint).
- Port 443 (HTTPS) must be open to your organization.
- Time synchronization must be set up on the Windows Server IIS host.
- Microsoft .NET 4.7.2 Framework installed. The framework installation file is packaged with the AD Connect distribution.
- IIS Server role service installed.
- Windows Authentication role service installed for IIS.

Copyright © 2025 Ping Identity Corporation

- Port requirements (internal):
  - TCP/UDP 389/636 or 3268 or 3269 inbound/outbound (LDAP connections)
  - TCP/UDP 88 inbound/outbound (Kerberos connections)
  - TCP/UDP 464 (Kerberos, set/change passwords)

  There may be additional port requirements depending on your security policies and deployment.
- Ensure that the Active Directory account lockout option is enabled for all PingOne users. This is necessary to protect user information in PingOne.
- Authentication using Kerberos with Office 365™ for Windows Applications and Mobile devices is supported. Mac Clients for Office 365 require forms-based authentication.

> **Note**
>
> Before you install AD Connect with IIS, ensure that your deployment platform is secure. See Secure your AD Connect with IIS deployment.

About this task

You'll download AD Connect from the PingOne for Enterprise admin portal and install it on a Windows Server IIS host that resides in an Active Directory domain. During installation, AD Connect with IIS deploys as a Web application in IIS. If you're not downloading to the IIS host, you'll need to copy the AD Connect distribution to the host.

Steps

1. In PingOne for Enterprise, go to **Setup > Identity Repository**, click **Connect to an Identity Repository**, select **AD Connect** and follow the prompts to download and install AD Connect.

   You'll be returning to this PingOne for Enterprise page as part of the AD Connect installation.

   > **Note**
   >
   > We recommend you copy and save the product key. If you find the need to reinstall AD Connect, you can reuse this key.

2. On the Windows host, if you're installing AD Connect in a DMZ, see AD Connect in a DMZ for the ports to open, then join the host to the Windows network.
3. Extract the zipped file, and launch the installation package. The Welcome page is displayed.
4. Click **Next**.The installation options are displayed:

   Choose from:

   - AD Connect (with the option to enable user provisioning between Active Directory and PingOne for Enterprise).
   - AD Connect with IIS (with the option to enable user provisioning between Active Directory and PingOne for Enterprise).
   - Provisioner only. Select this option if you already have an AD Connect or AD Connect with IIS installation and want to add user provisioning support for another Active Directory domain.

Copyright © 2025 Ping Identity Corporation

5. Select **AD Connect with IIS** and optionally, click **Enable user provisioning**, then click **Next**. TheAD Connect installer checks that the prerequisites are in place. If all prerequisites are in place, the installation proceeds to the activation tab.

   The installer checks whether the following services are installed:

   - .NET framework. If this isn't installed, you can install it using the .NET distribution located in the AD Connectinstallation directory.
   - IIS Server role. If this isn't installed, install this role service using Windows Server Manager.
   - Windows Authentication role. If this isn't installed for IIS, install this role service using Windows Server Manager.

   If you need to install any of these services, return to the AD Connect screen when the service installations are complete and click **Verify Install**.

6. At the AD Connect activation screen, paste the `Organization ID` value displayed in the PingOne for Enterprise admin portal.

   If you've closed the browser window, log in to admin.pingone.com again, and on the **Setup > Identity Repository** page, select to **Review/Change** the AD Connect configuration.

7. In the `Product Key` field, enter the product key you assigned in the PingOne for Enterprise admin portal, then click **Activate**. The activation message is displayed.

8. Click **Next**. The web site selection screen is displayed.

9. Select the IIS HTTPS-enabled site that AD Connect is to use. AD Connect is deployed to this site as a web application. Click **Next**. The installation screen is displayed.

10. You're prompted for the installation path to use, and are then prompted to install AD Connect.

    When the installation is complete, we'll send you a notification email.

11. When you click **Finish**, the PingOne for Enterprise admin portal login page is automatically displayed in a new tab or window.

    Whenever you log in to PingOne for Enterprise, your prior session state is retained.

12. See AD Connect for IIS final setup to complete the setup for AD Connect with IIS.

Customize the login, error, and password change windows in AD Connect for IIs

Add custom branding, styles, and destinations to PingOne windows using a custom theme file.

> **Note**
>
> These specifications apply only to installations of AD Connect with IIs. To customize branding and styles for standard AD Connect installations, see Assign AD Connect branding and designs.

`C:\Program Files (x86)\Ping Identity\ADconnect\Examples\Default\theme.zip` contains the HTML and related media files for PingOne login and error windows. The archive folder structure is unrestricted. The only required files for `theme.zip` are:

- `login.html`
- `error.html`

Copyright © 2025 Ping Identity Corporation

- `changepassword.html`
- `passwordchanged.html`

These files must all be present in the `Theme.zip` root.

Templates can include any javascript, graphics, CSS or other scripts included in `theme.zip`, using relative links, as in the following example.

```
<link rel="stylesheet" media="all" type="text/css" href="css/screen.css ">
```

```
<script src=" assets/js/script.js "></script>
```

> **Note**
>
> All image name references must be in lower case.

Templates must use substitution symbols to render dynamic content generated by AD Connect.

The `login.html` template must use the following names for authentication form fields:

- `ad.username` for username
- `ad.password` for password

The `changepassword.html` template must use the following names for form fields:

- `ad.username` for username
- `ad.password` for current password
- `ad.newpassword` for new password
- `ad.confirmpasswaord` for new password confirmation

The substitution symbols and syntax for each required template file are listed in the following tables.

`login.html`

Substitution symbol	Description	Syntax
`$action$`	Replaced with the actual AD Connect URL where form data is posted for authentication.	`<form method="POST" action="$action$"> </form>`
`$error$`	Replaced by error message text.	

Copyright © 2025 Ping Identity Corporation

Substitution symbol	Description	Syntax
`$if(error)$ $endif$`	Renders a conditional block of markup if an error occurs.	`$if(error)$ <div>$error$</div> $endif$`
`$username$`	Attach to the `username` input field to retain the `username` value if an error occurs.	`<input id="username" type="text" size="36" name="ad.username" value="$username$"/>`
`$username$_url`	Replaced by the URL for the change password page.	`<a href="$changepassword_url$">Change my password</a>`

error.html

Substitution symbol	Description	Syntax
`$errormessage$`	Replaced with error description.	`<font face="Arial">$errormessage$</font>`

changepassword.html

Substitution symbol	Description	Syntax
`$action$`	Replaced with the AD Connect URL where form data is posted for authentication.	`<form method="POST" action="$action$"> </form>`
`$username$`	Attach to the `username` input field to retain the `username` value if an error occurs.	
`$error$`	Replaced by error message text.	

Copyright © 2025 Ping Identity Corporation

Substitution symbol	Description	Syntax

`$if(error)$ $endif$`	Renders a conditional block of markup if an error occurs.	`$if(error)$`
		`<div>$error$</div>`
		`$endif$`

`$msg$`	Replaced by success message text.	

`$if(msg)$ $endif$`	Renders a conditional block of markup after a successful operation.	`$if(msg)$`
		`<div>$msg$</div>`
		`$endif$`

`$cancel_url$`	Replaced by a URL that the user is directed to when they click **Cancel**.	

`$if(cancel_url)$ $endif$`	Renders a conditional block of markupif cancellation is possible.	`$if(cancel_url)$`
		`<a href="$cancel_url$"`
		`title="Cancel">Cancel</a>`
		`$endif$`

`passwordchanged.html`

Substitution symbol	Description	Syntax

`$resume_url$`	Replaced by a URL that the user is directed to when they click **Continue**.	`<a href="$resume_url$"`
		`class="button normal allow"`
		`title="Continue">Continue</a>`

To install the customization archive, copy the updated `theme.zip` file into the single sign-on (SSO) application folder.

The default folder location is `C:\Program Files (X86)\Ping Identity\ADConnect\SSO`.

Configure IWA for AD Connect with IIS

Add Integrated Windows authentication (IWA) authentication to AD Connect with IIS.

Copyright © 2025 Ping Identity Corporation

Steps

1. Create a service account in AD Connect to use for the IIS application pools on the PingOne for Enterprise AD ConnectAD Connect hosts.
2. Create an SPN (Service Principal Name) in Active Directory for the HTTP service that's bound to the service account. For example:

   Example:

   ```
   setspn –U –S HTTP/pingone.example.com example\svc.adciis
   ```

3. On each AD Connect host, set the AD Connect application pool that you want to run under the service account credentials.

   In IIS Manager, **expand the node for AD Connect host > Application Pools > ADconnectAppPool**
4. Click **Advanced Settings** in the **Actions** bar on the right, scroll down to **Identity** and click the **edit** button.
5. Select **Custom Account**, click **Set** and enter the SPN credentials.
6. In the **Actions** bar on the right, click **Recycle** to recycle the application pool.
7. If you're using a high availability configuration, check the SNAT (Secure Network Address Translation) requirements for your network load balancing. Also verify that the IP address of the originating client is preserved by the SNAT configuration.

Secure your AD Connect with IIS deployment

About this task

Before installing AD Connect with IIS, ensure the deployment platform, the Windows Server® Internet Information Server (IIS) host for AD Connect, is secure.

You will want to consider:

- Deploying the Windows Server IIS host to a secured network location (such as, a combination of firewall with NAT and reverse proxy, or a DMZ). If the IIS host is to be directly connected to the Internet, this is critical.
- Assigning client browser trusted sites. You will need to add the IIS host as a trusted site to your users' browser clients. We tell you how to do this using Internet Explorer and Mozilla Firefox settings or using Group Policy for IE.
- Using load-balancing and clustering. If you expect to have large numbers of single sign-on (SSO) users, for high-availability you may want to consider using Microsoft Network Load Balancing (NLB) or another load-balancing and clustering solution.

Steps

1. Follow these deployment requirements:
    1. The Windows Server IIS host must reside in an Active Directory domain, but for security reasons, must not be a domain controller (DC).
    2. Port 443 (HTTPS) must be the only opened port. You need to verify that this is the case.
    3. Time synchronization must be set up on the Windows Server IIS host.

Copyright © 2025 Ping Identity Corporation

4. The Windows Server IIS host should use a trusted Certificate Authority (CA), rather than self-signed certificates.
5. The Windows Server IIS host must not have a direct Internet connection unless it is deployed in a properly configured DMZ.

2. Follow Microsoft's Security Best Practices for IIS 8, or the corresponding best practices for your version of IIS, to configure the Windows Server IIS host.
3. **Optional:** If the IIS host is to be directly connected to the Internet, deploy the host in a DMZ. AD Connect needs the following ports open between the DMZ and your internal network (firewall):

> **Note**
>
> TCP and UDP are shown together below. Depending on the firewall network device, you may want to add the TCP and UDP rules separately.

TCP/UDP 389/636 or 3268 or 3269

These are the Lightweight Directory Access Protocol (LDAP) ports. Ensure that one of these ports is open for AD Connect with IIS. AD Connect with IIS uses LDAP to access the Active Directory DC (when in-network or Windows Authentication is used). Also used for mobile authentication.

TCP/UDP 88

This port belongs exclusively to Kerberos. AD Connect with IIS uses this port for off-network access when executing a single sign-on (SSO) event outside of the corporate network.

TCP/UDP 464

This server port is also used by Kerberos (to set or change the password). Evidently it is also used to join the IIS (and AD Connect) host to the domain.

Additionally, we assume the following ports are also open. These ports are generally needed by any server operating in a DMZ:

UDP 138

NetBIOS name resolution.

TCP/UDP 445

SAM/LSA.

UDP 123

NTP W32 Time.

TCP/UDP 135, 49152-65535

RPC Endpoint Mapper.

UDP 137

NetBios datagram.

Copyright © 2025 Ping Identity Corporation

TCP/UDP 53

The DNS service runs on this port. It's used to convert between URLs and IP Addresses, and is also needed to join the IIS (and AD Connect) host to the domain.

4. **Optional:** Configure NLB clustering for AD Connect.

   See High Availability for AD Connect for instructions.

5. Add the URLs for the Windows Server IIS hosts to the trusted sites list for your users.

   You can use either of these methods to add the URLs as trusted sites:

   - Group Policy settings (Internet Explorer only). See Add trusted sites using Group Policy for instructions.
   - Browser site security settings (Internet Explorer and Firefox). See Add trusted sites using Internet Explorer settings or Add trusted sites using Firefox settings for instructions.

6. You can now install and configure your AD Connect identity bridge. See Installing AD Connect with IIS for instructions.

Add trusted sites using Firefox settings

Before you begin

Requirements

- Your AD Connect configuration in PingOne must have an `Authentication Type` value of either "Hybrid" or "Integrated".

About this task

For seamless SSO with AD Connect, use these instructions to assign the Windows Server IIS host to the Mozilla Firefox client's list of trusted sites.

Steps

1. In Firefox, enter "about:config"" in the URL address bar.
2. In the Search bar, enter "network.negotiate".
3. Double-click the entry **network.negotiate-auth.trusted-uris**, and enter the URL of the IIS host for AD Connect (for example, https://www.my-adconnect-host.com).

   > **Note**
   >
   > If you're using NLB, or another clustering solution, you will add the virtual cluster IP rather than an individual IIS host IP.

4. Click **OK**. The URL for the IIS host is displayed as the value of `network.negotiate-auth.trusted-uris`.

Result

The IIS host(s) for AD Connect should now be accessible from your Firefox clients.

Copyright © 2025 Ping Identity Corporation

High availability for AD Connect

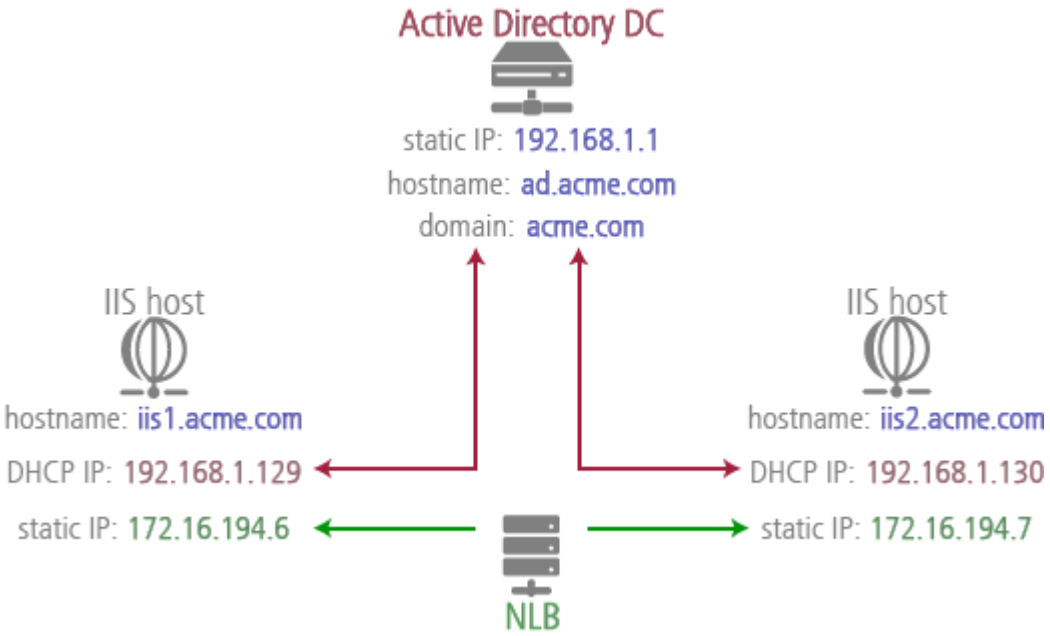
About this task

Use these instructions when expect to have large numbers of single sign-on (SSO) users for AD Connect, and you want to use Microsoft Network Load Balancing (NLB) as the load-balancing and clustering solution. NLB is an optional Windows Server feature.

> **Note**
>
> If you're using a load-balancing and clustering solution other than NLB, you can also apply these settings to your configuration by replacing the NLB-specific steps for those that match your solution.

You will configure NLB clustering for AD Connect, using the example configuration shown in the illustration as a guideline.

Although you can use this process for other configurations, these instructions are for a minimal configuration, one Active Directory domain controller (DC) and two Windows Server IIS hosts.



> **Note**
>
> The IIS hosts need two NICs, one for the static IP used by NLB (NLB requires static IPs), the other for the dynamic IP used by the DC. The NLB-dedicated NICs for all IIS hosts should be in the same subnet.

Steps

1. Install AD Connect on the IIS hosts (iis1.acme.com and ii2.acme.com).

   One of the IIS hosts will supply the signing certificate to be used on all other IIS hosts. We will call this the master IIS host.

2. On one of the IIS hosts (here we will use iis1.acme.com), use the Services MMC to disable **ADConnect Provisioner Service**. This will be the master IIS host.

Copyright © 2025 Ping Identity Corporation

3. On the master IIS host (iis1.acme.com), export the signing certificate.
    1. Open MMC, and from the File menu, select **Add/Remove Snap-in**. The Add or Remove Snap-ins dialog box is displayed.
    2. Select **Certificates** and click **Add**. The Certificates Snap-in dialog box is displayed.
    3. Select **Computer Account** and click **Next**. The Select Computer dialog box is displayed.
    4. Select **Local computer** and click **Finish**, and **OK**. The Certificates snap-in is displayed in MMC.
    5. Expand **Certificates (Local Computer) > Personal** and select Certificates. The certificates for the Local Computer account are displayed.
    6. Right-click the signing certificate (the certificate name includes the full domain name of the host) and select **All tasks > Export**. The Certificate Export Wizard is displayed.
    7. Follow the Certificate Export Wizard to export the private key.

        Result:

        The master IIS host signing certificate has been exported to the current user directory.
4. On the other IIS hosts (iis2.acme.com), import this signing certificate.
    1. Follow the steps above to add the Certificates snap-in to MMC.
    2. Expand **Certificates (Local Computer) > Trusted People**. Right-click **Certificates** and select **All tasks > Import**. The Certificate Import Wizard is displayed.
    3. Follow the Certificate Import Wizard and select the signing certificate you exported from the master IIS host.

        Result:

        The master IIS host signing certificate is now imported to the other IIS host.
5. On the other IIS hosts (iis2.acme.com), grant the IIS process access to the signing keys.
    1. Open MMC and go to **Certificates (Local Computer) > Personal > Certificates**. Right-click the master IIS host certificate that you imported and select **All tasks > Manage private private keys**. The permissions dialog box is displayed.
    2. Click **Add**, and in the entry box, enter the object name "IIS_IUSRS". Click **OK**.
    3. Grant Full Control and Read permissions to IIS_IUSRS.

        Result:

        The IIS host now has the necessary permissions to use the imported signing certificate.
6. On the other IIS hosts (iis2.acme.com), update the AD Connect `Web.config` file to use the imported signing certificate.
    1. Edit the AD Connect file `<installPath>\Ping Identity\ADConnect\SSO\Web.config`.
    2. Change the `saml.signing.cert` value to the name of the imported signing certificate, and save the file.

        Result:

Copyright © 2025 Ping Identity Corporation

AD Connect will now use the imported signing certificate.

7. On each IIS host (iis1.acme.com and iis2.acme.com), install the Network Load Balancing feature. This is an optional feature for Windows Server.
8. On each IIS host, configure network load balancing.
    1. Open Network Load Balancing Manager (in Administrative Tools) and choose to create a new cluster.
    2. Enter the static IP address (the NLB-dedicated NIC) of one of the IIS hosts.
    3. Select this interface, click **Next**, and assign a unique host ID.
    4. Click **Add** to create a virtual cluster IP address for this interface. Specify an address in the same subnet as the NLB-dedicated NICs of your IIS hosts.

        > **Note**
        >
        > The virtual cluster IP is the address you will use to access AD Connect. Do not use the IP addresses (static or dynamic) assigned to the IIS hosts.

    5. If you're deploying the IIS hosts in a VM (virtual machine), set the cluster operation mode to Multicast. Otherwise, set this mode to Unicast.

    Microsoft recommends using Unicast as the cluster operation mode. Unicast is compatible with all routers, switches and network devices. include::partial$p14e_p1refs_vm.adoc[tags=VM]recommends using Multicast if you're configuring NLB clusters on VMs.

    1. **Optional:** Set any port rules you consider necessary.
    2. When the information for the new cluster node (the IIS host) indicates the node is in a **Converged** state, right-click the node and select **Add Host to Cluster**.

        Result:

        The IIS host is now configured for NLB.
9. Repeat the above steps for each remaining IIS host (iis2.acme.com).

Result

You should now be able to power cycle a clustered IIS host, with automatic failover to another IIS host in the cluster. You also can add additional IIS hosts to the cluster as needed.

AD Connect for IIS final setup

About this task

You're completing the setup or manual update of AD Connect for IIS and are ready to verify the AD Connect for IIS installation and configure additional settings in PingOne for Enterprise.

Steps

1. On the PingOne for Enterprise admin portal page for AD Connect, click **Verify Installation**. PingOne for Enterprise checks the connection to the AD Connect identity bridge.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If you're using AD Connect in a clustered, high availability configuration, you will verify the installation in the PingOne admin portal only for the initial AD Connect installation.

2. For Authentication, the setting for `Account Lookup Method` is displayed.

   This setting assigns the Active Directory user attribute to use when looking up the account information for the user during authentication. This can be:

   - **Mail**. The email address assigned to the user.
   - **sAMAccountName**. The legacy Windows logon name for the user.
   - **Filter**. An LDAP filter to use when looking up the account information for the user.

3. For Delegated Authentication, the setting for `Account Lookup Method` is displayed.

   This setting assigns the Active Directory user attribute to use when looking up the account information for the user during delegated authentication. This can be:

   - **Mail**. The email address assigned to the user.
   - **sAMAccountName**. The legacy Windows logon name for the user.
   - **Filter**. An LDAP filter to use when looking up the account information for the user.

4. In the Identity Provider SSO URL section, check that a valid URL to your IIS host is displayed, and that the connection string for the SSO URL is correct. If needed, change either of these URLs.

5. The settings for `Entity ID`, `Assertion Lifetime` and `Authentication Type` are displayed.

   > **Note**
   >
   > The `Entity ID` setting for your deployment is also displayed. This uniquely identifies the identity bridge to PingOne. This identifier is used in the Issuer element of the SAML assertion sent to us by the identity bridge. Do not change this setting unless we advise you to do so.

   1. Check that the `Assertion Lifetime` setting is acceptable. Generally, you needn't change the default setting.

      This setting indicates how long the SAML assertion remains valid (in minutes).

   2. For Authentication, check that the `Authentication Type` setting is acceptable.

      This setting assigns the type of authentication the AD Connect identity bridge is to use. This can be:

      - **Integrated**. Integrated Windows Authentication (IWA) is used when the user is on your organization's network. A user is prompted for their credentials only once during the same browser session.
      - **Forms**. A Web-based authentication form is used. A user is prompted for their credentials at every authentication point during the same browser session.
      - **Hybrid**. A combination of Integrated Windows Authentication (IWA) and Form-based authentication is used. IWA is limited to intranet users who fall within a certain IP block range (specified in the `Intranet IP Block` attribute. Form-based authentication is used in all other cases (intended for those users authenticating from outside your organization's intranet).

Copyright © 2025 Ping Identity Corporation

If you're using Integrated or Hybrid types, see Configure IWA for AD Connect with IIS.

6. Click **Finish**.

   When you return to the **Setup > Identity Repository** page, a summary of the settings for your identity bridge is displayed. You can click the Edit icon to modify the settings.

Next steps

When you've completed your configuration:

- If you've upgraded:
  - You need to set the proper verification certificate. While logged in as an Administrator, browse to `https://localhost/adconnect/config.aspx`.

    In the bottom left of this page you will find the digital signature portion. Select the certificate that you'd assigned for the previous AD Connect installation, or want to assign for this installation. You can also choose to use the self-signed certificate.

    > **Note**
    >
    > If an error displays after you've selected the verification certificate stating that the certificate does not have the proper permissions, see the PingOne Knowledge Base article Manually updating the AD Connect signing certificate.

  - If you upgraded from version 1.x, in the PingOne admin portal, you will see that the group short names have been converted to their full DN. If you have multiple domains or child domains, check your application group mappings to ensure all of the correct groups have been selected for your application.
- If you're using AD Connect with IIS in a clustered, high availability configuration, repeat these steps on each AD Connect host.

Updating AD Connect

For AD Connect versions 3.0 or higher, you can choose to use the auto-update method. You will need to use the manual update process for all versions prior to 3.0. If an update is available for your currently installed version of AD Connect, you will find a notification displayed on the setup details page for AD Connect (**Setup > Identity Repository: PingOne AD Connect > Setup**).

> **Note**
>
> You can also choose to use the manual update process for any version of AD Connect, if you want to have full control over down-time.

Auto-update AD Connect

Before you begin

Make sure that you have Microsoft .NET Framework 4.7.2 installed before upgrading to AD Connect 5.0.1 or later.

About this task

Copyright © 2025 Ping Identity Corporation

Auto-update is supported only for AD Connect version 3.0 or higher.

Follow the instructions to authorize the AD Connect update from the PingOne admin portal. You do not need to uninstall the previous version of AD Connect.

> **Note**
>
> (AD Connect with IIS only) Back up the AD Connect web.config file. During the installation process, your AD Connect Organization ID and Product Key will be restored from the AD Connect web.config file, then the installation process overwrites the web.config file (retaining the Organization ID and Product Key unless this is changed).

For high availability clustered environments, each AD Connect node will receive the notification to auto-upgrade, and will download and install the latest version independent of other nodes in the cluster.

When the new installer runs, the AD Connect SSO and Provisioner services will be stopped. The AD Connect SSO and Provisioner services will be restarted when the installation is complete.

Any proxy settings are preserved during the auto-upgrade process.

Service interruption to both SSO and Provisioning while performing the auto-upgrade to AD Connect generally takes less than 5 minutes.

Steps

1. Select **Setup > Identity Repository**, then choose to edit the AD Connect identity bridge settings.
2. Click **Authorize AD Connect Update** to initiate the upgrade request. You're prompted to authorize the update. The installation update process on the host begins within 15 minutes. When the update completes, AD Connect restarts automatically, retaining the existing configuration.

   What's happening while you wait: The AD Connect configuration for your account indicates to the AD Connect SSO service that you've chosen to upgrade AD Connect (the AD Connect SSO service regularly polls your PingOne account). When AD Connect receives the authorization, it downloads the latest version of AD Connect and begins the installation process. The installer stops the existing SSO and Provisioner services and then installs the new version of AD Connect, reading the Organization Id and Product Key from the AD Connect web.config file and connecting to PingOne to retrieve the current configuration.

Manually Update AD Connect

If you are unable to run the automatic updater for AD Connect, download and run the install wizard to manually upgrade to the latest version.

Before you begin

Changes introduced by an upgrade

When upgrading AD Connect with IIS:

Updating from 1.x

The update converts all group names to the full distinguished names (DNs). The conversion completes after the new version of AD Connect registers with PingOne. Thereafter, group names sent during single sign-on (SSO) use the full DN instead of the short name.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If any connections require short group names to be passed during SSO, you will need to update the attribute mapping for these connections to convert from full DNs to short names.

You must update your application attribute mappings if `SAML_SUBJECT` is a source value for any of your application connections. When you update AD Connect, the `SAML_SUBJECT` value is changed to `userPrincipalName` rather than `sAMAccountName` as in your existing AD Connect 1.x.

This `SAML_SUBJECT` change will affect SSO for any applications configured to pass `SAML_SUBJECT` to the application. If you have any application attributes mapped to `SAML_SUBJECT`, update it to `sAMAccountName`.

> **Note**
>
> To ensure the correct attribute value will be passed to the application after completing the upgrade, also check your application attribute configuration for each of your applications.

The **Subject** displayed on the **Reports** page in the PingOne admin portal will show `userPrincipalName` rather than `sAMAccountName`. The dashboard counts of unique users will count the same user twice if the selected data range is before and after the upgrade. This is true only for users who SSO both prior to and after the upgrade.

When configuring the new AD Connect installation, you can enable support for Active Directory group hierarchy. When enabled, Active Directory groups that are nested will inherit the SSO permissions of their parent group or groups. When disabled, an Active Directory group uses only the SSO permissions that are assigned to it, with no inheritance.

If AD Connect is configured for high availability, schedule a maintenance window for this upgrade because SSO might be interrupted during the upgrade process. Perform any necessary server upgrades at this time because earlier versions of AD Connect might not continue to work after one of the servers has been upgraded.

Are other applications running on the IIS host? The current version of AD Connect requires .NET 4.7.2. Other applications running on IIS might require earlier versions of .NET.

Updating from 2.x

If AD Connect is configured for high availability, schedule a maintenance window for this upgrade because SSO might be interrupted during the upgrade process. Perform any necessary server upgrades at this time because earlier versions of AD Connect might not continue to work after one of the servers has been upgraded.

Are other applications running on the IIS host? The current version of AD Connect requires .NET 4.7.2. Other applications running on IIS might require earlier versions of .NET.

Upgrading to 5.x

Upgrading to 5.0.1 or later requires .NET Framework 4.7.2.

About this task

If you're uncertain whether you're running AD Connect or AD Connect with IIS, see the Knowledge Base article Differentiating between AD Connect and AD Connect with IIS.

When the new installer runs, the AD Connect SSO and Provisioner services will be stopped and the installer will guide you through the installation process. The AD Connect SSO and Provisioner services will restart when the installation is complete.

Copyright © 2025 Ping Identity Corporation

Steps

1. Back up the AD Connect `Program Files (x86)\Ping Identity\Ad Connect\SSO\web.config` file.

   You will use the Organization ID and Product Key when prompted for the new installation.

2. (AD Connect with IIS only) Copy the AD Connect `web.config` file you backed up into a new directory.

   In this topic, this is called the *update directory*. For a clustered, high-availability configuration, this is the directory you will use to update AD Connect on each host.

3. To ensure you can return to your existing version of AD Connect if needed, rename the `adconnect-installer.zip` file for your existing version of AD Connect and copy this file to your update directory.

4. If you customized the AD Connect authentication form, copy the AD Connect `Program Files (x86)\Ping Identity\Ad Connect\SSO\theme.zip` file to your update directory to ensure a backup is available.

5. Go to **Setup > Identity Repository > Change Identity Repository**.

6. Select **Active Directory** and click **Next**. Follow the prompts to download the AD Connect installer.

7. Copy the new AD Connect installer version to your update directory.

8. If AD Connect is installed in a clustered, high availability configuration, copy your update directory to each AD Connect host.

9. On the AD Connect host:

   1. Make a note of the account that is running the AD Connect services, as you will need to switch back to it later.

   2. Stop the Windows Services for AD Connect.

   The AD Connect services can have different names depending on the version that you have installed as well as which services are installed on the host. These can include "AD Connect Configuration Service", "AD Connect Provisioner Service", "AD Connect Software Update Service", and "AD Connect Watchdog Service".

10. Uninstall the existing version of AD Connect.

11. From the update directory you created, install the new version of AD Connect or AD Connect with IIS, depending on your previous installation type.

    For more information on the installation process, see Installing AD Connect or Installing AD Connect with IIS.

    > **Note**
    >
    > Be careful to choose the installation type (AD Connect or AD Connect with IIS) that corresponds to your previous installation. Installing the wrong type will result in an outage to existing SSO connections and might require reconfiguration. See Troubleshoot an AD Connect update if this occurs.

12. (AD Connect with IIS only) When prompted for the Organization ID and Product Key, use the values from the AD Connect `web.config` in your update directory.

13. Follow the remaining prompts to finish the AD Connect installation on the host, then verify the installation in the PingOne admin portal.

    - If you're updating standard AD Connect, see AD Connect final setup for instructions on how to verify the AD Connect installation and configure additional settings.

Copyright © 2025 Ping Identity Corporation

- If you're updating AD Connect for IIS, see AD Connect for IIS final setup for instructions on how to verify the AD Connect for IIS installation and configure additional settings.

> **Note**
>
> If you're using AD Connect in a clustered, high availability configuration, you only need to verify the installation in the PingOne admin portal for the initial AD Connect installation.

14. Switch back to the account that was originally running the AD Connect services.

Troubleshoot an AD Connect update

You updated an AD Connect with IIS installation to AD Connect and SSO is broken.

See this Ping Knowledge Base article for instructions to correct the issue.

AD Connect installer did not download.

If for some reason the AD Connect installer is not automatically downloaded to the AD Connect host during an auto-update, you will need to manually install the new version of AD Connect.

Rolling back to a previous version.

If necessary, you can roll back to a previous version of AD Connect. Just uninstall the existing AD Connect version and install the desired version. If you decide you want to upgrade at some point, you will need to authorize the auto-update.

View and manage AD Connect agent nodes

The Identity Repository window allows you to view and manage AD Connect agent nodes.

About this task

The **Identity Repository** window allows you to view and edit your AD Connect configuration. You can also use this menu to view and manage the AD Connect agent nodes installed within your infrastructure and connected to your PingOne account.

Steps

- Go to **Setup > Identity Repository** to view your AD Connect agent nodes.
- Expand the AD Connect identity repository and click **Nodes**.
- Click the agent name to expand the entry and display the following agent node information:
  - **Agent name**
  - **Connection status**: Green indicates the agent is up. Red indicates the agent is down.
  - **Last seen**: The date and time when the agent connection was lost. Only displays if the node is offline.
  - **Agent ID**: A GUID ID.
  - **Datacenters**: The data centers connected to the agent.

Copyright © 2025 Ping Identity Corporation

- **Connected on**: The date the agent connection was created.

- You can also manage each connection in the following ways:
  - **Connection**: Toggle the agent connection on and off. Disabled agents are still connected, but not used for SSO. Disabling the connection reroutes SSO traffic to other agents. If you disable all node agents then SSO will not function.
  - **Delete**: Click to delete a disconnected agent.

> **Note**
>
> You must first disconnect an agent in order to delete it.

Configure logging in AD Connect

Configure logging in your AD Connect environment to help troubleshoot connection issues.

By default, AD Connect logs activity to the Windows Event Viewer with the following source names:

Agent	Source Name
AD Connect Agent	`AuthenticationAgent.exe`
AD Connect with IIS	SSO
Provisioning agent	`Provisioner.exe`
Update monitoring agent	`SoftwareUpdates.exe`
Configuration monitoring agent (IIS only)	`ConfigurationService.exe`

To view these logs, go to **Logs > Application** in the Windows Event Viewer.

You can configure both the IIS and non-IIS versions of AD Connect to log events to a log file in addition to the Event Viewer.

Copyright © 2025 Ping Identity Corporation

With IIS

Configure logging in AD Connect with IIS
Steps

1. In a text editor, open the `<install directory>\ADconnect\SSO\web.config` file.
2. In the `<log4net>` section, add the following code:

```
<appender name="file" type="log4net.Appender.FileAppender">
  <file value="c:\tmp\watchdog.log" />
  <appendToFile value="true" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%date %-5level %logger - %message%newline" />
  </layout>
</appender>
```

3. In the `<root>` section, under `<log4net>`, add the file logger:

```
<appender-ref ref="file" />
```

Example:

The following is an example of how the `<log4net>` section of the `web.config` file will appear after making the changes in steps 2 and 3.

```
<log4net>
  <appender name="eventlog" type="com.pingidentity.adconnect.logger.CustomEventLogAppender">
    <applicationName value="Sso"/>
    <EventID value="1"/>
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%date %-5level %logger - %message%newline"/>
    </layout>
  </appender>
  <appender name="file" type="log4net.Appender.FileAppender">
    <file value="c:\tmp\watchdog.log"/>
    <appendToFile value="true"/>
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%date %-5level %logger - %message%newline"/>
    </layout>
  </appender>
  <root>
    <level value="INFO"/>
    <appender-ref ref="eventlog"/>
    <appender-ref ref="file"/>
  </root>
</log4net>
```

Copyright © 2025 Ping Identity Corporation

4. **Optional:** To configure the log file parameters, add the following code to the `<appender>` file section.

```
<rollingStyle value="Size" />
<maxSizeRollBackups value="0" />
<maximumFileSize value="100MB" />
<staticLogFileName value="true" />
```

> **Note**
>
> If you're using a log file temporarily to gather data, you can ignore this step. If you plan to use log files on a long-term basis, this step limits the size of the log file to prevent overusing resources.

Example:

Below is an example of how the `<appender>` file section will appear after you add the code in step 4.

```
<appender name="file" type="log4net.Appender.FileAppender">
  <file value="c:\tmp\watchdog.log"/>
  <appendToFile value="true"/>
  <rollingStyle value="Size" />
  <maxSizeRollBackups value="0" />
  <maximumFileSize value="100MB" />
  <staticLogFileName value="true" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%date %-5level %logger [%property{NDC}] - %message%newline"/>
  </layout>
</appender>
```

5. **Optional:** To enable verbose logging, in the `<root>` section, change the `<level value>` value from `INFO` to `DEBUG`.

Example:

```
<root>
    <level value="DEBUG"/>
    <appender-ref ref="eventlog"/>
  </root>
```

Verbose logging can help troubleshoot authentication issues, such as user authentication failures. Verbose logging adds logs showing which domain controller is being used for the lookup, what LDAP filters are being used to find users, and whether a user was found or their password didn't match.

6. Save and close the file.

Copyright © 2025 Ping Identity Corporation

Without IIS

Configure logging in AD Connect without IIS
Steps

1. In a text editor, open the `<install directory>\AuthenticationAgent\log4net.config` file.
2. In the `<root>` section, add the following file appender:

```
<root>
  <level value="INFO"/>
  <appender-ref ref="eventlog"/>
  <appender-ref ref="file"/>
</root>
```

3. **Optional:** To configure the log file parameters, add the following code to the `<appender>` file section.

```
<rollingStyle value="Size" />
<maxSizeRollBackups value="0" />
<maximumFileSize value="100MB" />
<staticLogFileName value="true" />
```

> **Note**
>
> If you're using a log file temporarily to gather data, you can ignore this step. If you plan to use log files on a long-term basis, this step limits the size of the log file to prevent overusing resources.

Example:

Below is an example of how the `<appender>` file section will appear after you add the code in step 3.

```
<appender name="file" type="log4net.Appender.FileAppender">
  <file value="c:\tmp\watchdog.log"/>
  <appendToFile value="true"/>
  <rollingStyle value="Size" />
  <maxSizeRollBackups value="0" />
  <maximumFileSize value="100MB" />
  <staticLogFileName value="true" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%date %-5level %logger [%property{NDC}] - %message%newline"/>
  </layout>
</appender>
```

4. **Optional:** To enable verbose logging, in the `<root>` section, change the `<level value>` value from `INFO` to `DEBUG`.

Copyright © 2025 Ping Identity Corporation

Example:

```
<root>
    <level value="DEBUG"/>
    <appender-ref ref="eventlog"/>
  </root>
```

Verbose logging can help troubleshoot authentication issues, such as user authentication failures. Verbose logging adds logs showing which domain controller is being used for the lookup, what LDAP filters are being used to find users, and whether a user was found or their password didn't match.

5. Save and close the file.

Connect to PingFederate

Connect to a new or existing PingFederate account as your PingOne for Enterprise identity repository.

Before you begin

PingFederate requirements

- Network access to a PingFederate installation.
- Administrator permissions on PingFederate.
- PingFederate access to the appropriate identity repository.

Note

Before connecting to PingOne for Enterprise, you must allow access to the following domains on the server running PingFederate.

- `admin-api.pingone.com` for administration
- `ore-routingsvc.pingone.com` for monitoring PingFederate from PingOne for Enterprise
- `ohi-routingsvc.pingone.com` for monitoring PingFederate from PingOne for Enterprise
- `scim.connect.pingidentity.com` for provisioning

About this task

You'll be working on both the PingOne side and the PingFederate side.

Note

A PingFederate license can be either a "Bridge" license or a "Full" license. You can use either type of license with PingOne. This documentation references PingFederate Bridge. If your organization has a full PingFederate license, all instructions are the same unless otherwise noted. For more information, see Connections to PingOne for Enterprise in the PingFederate documentation.
Bridge licenses are available for PingFederateversions 10.3 and earlier. You can download later versions of PingFederate from the Ping Identity download site, but those versions require a full PingFederate license.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Setup > Identity Repository**, click **Connect to an Identity Repository**, select **PingFederate**, and click **Next**.

   The steps to complete your PingFederate Bridge setup depend on whether you have an existing PingFederate installation, and if so, whether you've installed PingFederate version 8.0 or higher.

2. Select whether or not you have an existing PingFederate installation.

3. If you selected that you don't have an existing PingFederate installation, click **Next**.

    1. Select the server platform you'll use for the PingFederate Bridge installation.

       The installation instructions to depend on the platform you've chosen:

Windows installations

1. Click **Download PingFederate** and click **Next**.

2. Run the PingFederate Bridge installer and follow the installation steps.

   When the installation is complete, the URL for your PingFederate Bridge admin console will be displayed. Open the PingFederate admin console URL in a browser and follow the initial setup tutorial.

3. Copy into PingFederate Bridge the single-use **Activation Key** displayed in PingOne.

4. In PingOne, click **Next**.

5. Assign the PingFederate-to-PingOne attribute mapping.

   This assignment maps PingFederate attributes to the default PingOne attributes (used by PingOne for Enterprise dock). This attribute mapping is not used by applications that you add to PingOne for Enterprise. You will configure those attribute mappings for each application.

For any of the attribute mappings, you can choose to configure an advanced mapping. See Creating advanced attribute mappings for instructions.

Linux installations

1. Open a command line console on your selected server for the PingFederate Bridge installation and enter the displayed command to download PingFederate.

2. In PingOne, click **Next** to display the Install and Configure PingFederate panel.

3. In the command line console on your selected server, enter the displayed PingFederate Bridge installation script.

   When the installation is complete, the URL for your PingFederate Bridge admin console will be displayed. Open the PingFederate Bridge admin console URL in a browser and follow the initial setup tutorial.

4. Copy into PingFederate Bridge the single-use **Activation Key** displayed in PingOne.

5. In PingOne, click **Next**.

6. Assign the PingFederate-to-PingOne attribute mapping.

Copyright © 2025 Ping Identity Corporation

This assignment maps PingFederate attributes to the default PingOne attributes (used by PingOne dock). This attribute mapping is not used by applications that you add to PingOne. You will configure those attribute mappings for each application.

For any of the attribute mappings, you can choose to configure an advanced mapping. See Creating advanced attribute mappings for instructions.

4. If you have selected that you have an existing PingFederate installation, click **Next**.

   The UI skips ahead to **Install and Configure PingFederate Bridge**.

   1. Copy the PingFederate Bridge activation key that's displayed and click **Next**.
   2. Log in to your PingFederate installation to enter the activation key.

      If you have a new, unconfigured PingFederate installation, the section for the PingOne for Enterprise activation key is displayed on the first page.

      If you are using an already configured PingFederate installation, go to **System > External Systems** and click **Connect to PingOne for Enterprise**.
   3. Copy into PingFederate the single-use **Activation Key** displayed in PingOne and click **Next**.

      Follow the instructions to configure your PingOne for Enterprise connection. Refer to your PingFederate documentation for more information.
   4. In PingOne, when the PingFederate configuration is verified, click **Next**.

      The PingFederate connection can't be verified until you've saved the PingOne connection configuration in PingFederate.
   5. Assign the PingFederate-to-PingOne attribute mapping.

      This assignment maps PingFederate attributes to the default PingOne attributes (used by PingOne dock). This attribute mapping is not used by applications that you add to PingOne. You'll configure those attribute mappings for each application.

      For any of the attribute mappings, you can choose to configure an advanced mapping. See Creating advanced attribute mappings for instructions.

5. When you've completed the PingFederate configuration, your new PingFederate Bridge or PingFederate connection (node) is displayed.

   > **Important**
   >
   > For PingFederate nodes to appear in PingOne for Enterprise, the **Enable Monitoring of PingFederate from PingOne** option must be enabled. This option is enabled by default.
   > This option can be found in PingFederate at **System > External Systems > PingOne for Enterprise Settings**.

   1. Click the node name to display information about the PingFederate node.

      You can optionally assign:

      - A different URL for the link to the PingFederate admin page.
      - A different name for the PingFederate node.

Copyright © 2025 Ping Identity Corporation

2. Click **Settings** to display a summary of the PingOne and PingFederate configuration details for the identity repository. From here you can click to download the **Active Signing Certificate** and the **Encryption Certificate**. You can also copy and share the **PingOne Metadata URL**.

6. **Optional:** Click to download the displayed PingOne signing and encryption certificates.

7. **Optional:** If you've deployed PingFederate in clustered mode, you can choose to add other PingFederate nodes in the cluster to the PingOne admin portal for monitoring.

Result

Your PingFederate Bridge or PingFederate setup for PingOne is complete.

Configuring Provisioning for PingFederate

Provision user data between PingFederate Bridge and PingOne for Enterprise.

Steps

1. From the PingFederate Bridge admin portal, go to **Applications > Integration > SP Connections**.
2. Click the **PingOne** connection and then click the **Connection Type** tab.
3. Select the **Outbound Provisioning** checkbox.
4. Click **Next** until you reach the **Outbound Provisioning** tab.
5. Click **Configure Provisioning**.
6. Click **Create**.
7. On the **Channel Info** tab, in the **Channel Name** field, enter a name for the provisioning channel. Click **Next**.
8. On the **Source** tab, in the **Active Data Store** list, select a data store.

   If you haven't configured a data store, click **Manage Data Stores** to create one. For more information, see Adding a new datastore.
9. Click **Next** until you reach the **Source Location** tab.
10. On the **Source Location** tab, enter the source record names for the user repository you've selected.

    These entries must be in the proper format for the repository. An LDAP repository requires Base DN and Users Group DN entries, for example: `DC=pingone,` , `CN=Users` , `CN=Builtin` , `DC=pingone` , `DC=com` .

    > **Tip**
    >
    > Microsoft Active Directory administrators can use the `dsquery` command on the Active Directory host to find the Base DN and Users Group DN values.

11. On the **Attribute Mapping** tab, change any attribute settings as needed. PingFederate Bridge will automatically populate a valid configuration, but you can use this menu to add or modify attributes depending on your organization's needs. For more information, see Mapping Attributes.
12. Click **Next**.

Copyright © 2025 Ping Identity Corporation

13. On the **Activation & Summary** tab, click **Active**, then click **Done**.
14. On the **Manage Channels** tab, click **Save**.

Result

After completing your PingFederate Bridge SP outbound provisioning, you're returned to the **SP Connections** window.

Connect to OpenID Connect

About this task

The OpenID Connect identity bridge uses OpenID Connect and OAuth to connect to your OpenID Connect provider (OP) to authenticate your users and access user information. In OpenID terms, PingOne is the Relying Party (RP) that sends authentication and information requests to the OpenID Connect provider.

You will need to supply the OAuth `Client ID` and `Client Secret` values registered for your OpenID Connect provider.

OpenID Connect supports a discovery mechanism whereby an OpenID Connect host publishes metadata using a well-known URL, by convention of the form: `https://host.com/.well-known/openid-configuration`. The URL returns OpenID Connect and OAuth endpoints, supported scopes and claims, public keys used to sign tokens, and other metadata. We use this metadata to complete your authentication requests and requests for user information.

If your OpenID Connect provider doesn't have a discovery endpoint (URL) that we can use to query your IdP for the metadata, we will display the information we need and you will supply these values. See the configuration or documentation for your OpenID Connect provider to find the necessary values.

Steps

1. Go to **Setup > Identity Repository**, click **Connect to an Identity Repository**, and select OpenID Connect. Click **Next**.
2. Enter the OAuth **Client ID** and **Client Secret** values registered with your OpenID Connect provider.
3. We need to be able to query your OpenID provider for the necessary metadata. Choose:

   Choose from:

   - **Discovery Endpoint** if your OpenID Connect provider supplies an endpoint set up for this purpose, then enter the URL.
   - **All Endpoints** if your OpenID Connect provider doesn't have an endpoint set up for such queries. In this case, you will need to enter the necessary metadata:

     ### *Issuer*

     The URL referencing the location of your OpenID Connect provider.

     ### *Authorization Endpoint*

     The URL for your OpenID Connect provider's OAuth authorization endpoint.

     ### *Token Endpoint*

     The URL for your OpenID Connect provider's OAuth token endpoint.

Copyright © 2025 Ping Identity Corporation

Userinfo Endpoint

The URL for your OpenID Connect provider's userinfo endpoint.

JWKS URI

The URI for your OpenID Connect provider's JSON Web Key Set (JWKS) document. This contains the signing key or keys we will use to validate signatures from your OpenID provider.

End Session Endpoint

The URL to which the OpenID Connect provider is redirected for single logout (SLO) of a PingOne session.

PingOne uses a single logout (SLO) process to log out all participants of a PingOne session. In the PingOne context, the session participants are the identity repository, PingOne, and any applications to which a user has signed on (SSO) for the session. Any one of the session participants can initiate SLO. PingOne acts as the session authority, mediating the SLO request and response messages so that all participants are notified. In this way, when a user logs off, the PingOne session is ended for all participants.

When **Discovery Endpoint** is used, if `end_session_endpoint` is defined in the discovery document returned, PingOne will use the `end_session_endpoint` value.

4. Click **Verify**.

PingOne will verify that it can query the endpoint or endpoints you've specified. If verification isn't successful, check that the endpoint or endpoints appear exactly as they do on your OpenID Connect provider.

1. For **Scope**, either select or specify the OAuth scopes that you'd like us to include in authentication requests.

   The available scopes of authorization for your OpenID Connect provider are displayed based on the response from your supplied **Discovery Endpoint**. The scopes indicate the access privileges you're requesting for the access token returned by the OpenID Connect provider. We use the access token to request additional claims from the userinfo endpoint.

   1. You can use the **Additional Scopes** entry box to specify other scopes you'd like us to include in the authentication requests.

2. **Optional:** If your OpenID Connect provider requires additional parameters for the authorization request, you can supply these by adding **Query Parameters**.

The query parameters are name/value pairs specifying the necessary parameter name and value.

1. Click **Add Query Parameter** and enter the parameter name and value for each parameter needed.
2. Click **Next** to continue to the next section.

   1. The **PingOne Redirect URI** is the URI assigned by PingOne to which the OpenID Connect provider sends OAuth authorization codes indicating whether or not a user was authenticated.

   To ensure security, the PingOne redirect URI includes a verification code unique to your account. The redirect URI used by your OpenID Connect provider for PingOne must include the verification code for SSO to be successful.

3. Copy the entire URI and see that it is entered at your OpenID Connect provider as the redirect URI for PingOne.
4. Click **Next** to continue to the next section.

   1. Assign the OpenID Connect provider-to-PingOne attribute mapping.

Copyright © 2025 Ping Identity Corporation

This assignment maps identity provider attributes to the default PingOne attributes (used by PingOne dock). This attribute mapping is not used by applications that you add to PingOne. You will configure those identity provider-to-service provider attribute mappings for each application.

5. For any of the attribute mappings, you can choose to configure an advanced mapping. See Creating advanced attribute mappings for instructions.
6. Click **Done** when you're finished.

Result

Your OpenID Connect identity bridge is now set up.

Connect to Azure

About this task

The Microsoft Azure identity bridge uses OpenID Connect and OAuth to connect to your Azure provider (OP) to authenticate your users and access user information. In OpenID terms, PingOne for Enterprise is the Relying Party (RP) that sends authentication and information requests to the Azure provider.

To configure the identity bridge, you'll be working on both the Azure and PingOne for Enterprise sides and copying information from your Azure tenant to the PingOne for Enterprise identity bridge setup.

OpenID Connect supports a discovery mechanism whereby an OpenID Connect host publishes metadata using a well-known URL, by convention of the form: `https://host.com/.well-known/openid-configuration`. The URL returns OpenID Connect and OAuth endpoints, supported scopes and claims, public keys used to sign tokens, and other metadata. We use this metadata to complete your authentication requests and requests for user information.

Steps

1. In PingOne for Enterprise, go to **Setup > Identity Repository**, click **Connect to an Identity Repository**, and select **Microsoft Azure AD**. Click **Next**.
2. Sign on to your Azure tenant and go to **Azure Active Directory > Add > App registration**.
    1. On the **Register an application** page, enter a name for the PingOne for Enterprise client (such as, "PingOne").
    2. Under **Supported Account Types**, click to select which Microsoft account types you will allow access.
    3. **Optional:** Under **Redirect URI**, select an authentication method from the list, and in the text field enter a URL.
    4. Click **Register** to save the PingOne for Enterprise client.

        Result:

        The application overview page is displayed.
3. Copy the **Application (client) ID** value.
4. PingOne for Enterprise, on the **Configure Your Microsoft Azure Connection** tab, paste the **Application (client) ID** value into the **Client ID** field.

Copyright © 2025 Ping Identity Corporation

5. In Azure, click **Add a certificate or secret** and click **New client secret**.
    1. Enter a description and expiration for the client secret.

    You'll need to update the client secret when it expires.

    1. Click **Add** to add the new client secret.
    2. Copy the **Value** value.
6. In PingOne for Enterprise, paste the Client ID value into the **Client Secret** field.
7. In Azure, return to the overview page.
    1. Click **Endpoints** to display the OAuth endpoints for your Azure tenant.
    2. Copy the URL for the **OpenID Connect metadata document** endpoint.
8. In PingOne for Enterprise, while still on the **Configure Your Microsoft Azure Connection** panel, for **Discovery Endpoint**, enter the URL for the OpenID Connect metadata document endpoint you copied from your Azure tenant.
9. Click **Verify**.

    PingOne for Enterprise will verify that it can query the endpoint or endpoints you've specified. If verification isn't successful, check that the endpoint or endpoints appear exactly as they do on your OpenID Connect provider.
10. For **Scope**, select the OAuth scopes that you'd like us to include in authentication requests, then click **Next**.

    The available scopes of authorization for your Azure tenant are displayed based on the response from your supplied **Discovery Endpoint**. The scopes indicate the access privileges you're requesting for the access token returned by Azure. We use the access token to request additional claims from the userinfo endpoint.
11. In Azure, close the **Endpoints** panel and from the *clientName* IdP (Test) page, click **API permissions** for your PingOne for Enterprise client.
    1. Check whether **User.Read** is already added by default.

    If it isn't already added, you'll add it in a subsequent step.

    1. Click **Add a permission**.
    2. The Request API permissions page is displayed. Select **Microsoft APIs > Microsoft Graph**.
    3. For **What type of permissions does your application require?**, select **Application permissions**.
    4. The list of APIs is displayed. Expand **Group** and select **Group.Read.All**.
    5. If the **User.Read** permission wasn't added by default, expand **User** and select **User.Read**.
    6. On the API permissions page, click **Add permissions**.
    7. Click **Grant admin consent for...**.

        Doing this ensures your users don't need to grant consent during SSO.
12. On the *clientName* IdP (Test) page, click **Manifest**.
13. Find the **groupMembershipClaims** element and change it from "null" to either "SecurityGroup" or "All".

Copyright © 2025 Ping Identity Corporation

This will ensure that the group membership claim is sent in the access token to PingOne for Enterprise during SSO.

14. In PingOne for Enterprise, on the **Microsoft Azure Provider** panel, copy the displayed **PingOne Redirect URI**.

    The PingOne Redirect URI is the URI assigned by PingOne to which your Azure tenant sends OAuth authorization codes indicating whether or not a user was authenticated.

    To ensure security, the PingOne for Enterprise redirect URI includes a verification code unique to your account. The redirect URI used by your Azure tenant for the PingOne client must include the verification code for SSO to be successful.

15. In Azure, go to the **Overview** page for your registered PingOne for Enterprise client and click the link for **Redirect URIs**.

    1. Add a new Redirect URI of type **Web**.
    2. Enter the URI you copied from the **Microsoft Azure Provider** panel in PingOne for Enterprise.
    3. Click **Save**.

16. In PingOne for Enterprise, assign the Azure provider-to-PingOne for Enterprise attribute mapping.

    This assignment maps your selected Azure provider attributes to the default PingOne for Enterprise attributes (used by PingOne for Enterprise dock). This attribute mapping is not used by applications that you add to PingOne for Enterprise. You will configure those identity provider-to-service provider attribute mappings for each application.

    > **Note**
    >
    > If you're also using PingID for Azure Conditional Access, make sure the `MFA_SUBJECT` mapping for PingOne for Enterprise matches the `username` mapping for PingID.
    > Learn more in Configuring PingID MFA for Microsoft Azure AD Conditional Access in the PingID documentation.

    1. For any of the attribute mappings, you can choose to configure an advanced mapping. Find instructions in Creating advanced attribute mappings.
    2. Click **Next** when you're finished.

17. Choose whether or not to synchronize the user groups on your Azure provider with your PingOne user groups.

    Group synchronization relies on the Microsoft Graph API permissions you specified for the PingOne client you registered in Azure. The permissions `User.Read` and `Group.Read.All` are required for synchronization to be successful.

    Any PingOne for Enterprise user groups that do not exist in your Azure provider will be replaced by the Azure groups.

    Each of your Azure group members are automatically added to the corresponding PingOne for Enterprise groups when the user initially signs on (SSO) to PingOne for Enterprise This is PingOne for Enterprises just-in-time user provisioning.

    1. When you elect to synchronize your Azure groups with PingOne for Enterprise, a banner is displayed notifying you that synchronization is under way. In the banner is a **User Groups** link. Clicking this link will take you to the User Groups page where you can see the groups being added to PingOne for Enterprise

       The Azure groups are added using their Azure group IDs. After this initial synchronization, when additions or changes to your Azure groups occur, you'll need to choose to resynchronize the groups using the **Synchronize Groups** button on the User Groups page. See Adding user groups for more information.

    2. Click **Done**.

Copyright © 2025 Ping Identity Corporation

Result

Your Azure identity bridge is now set up.

Connect to ADFS

PingOne uses the SAML protocol to connect to Microsoft Active Directory Federation Services (ADFS).

About this task

To configure the identity repository side of the connection, you will need to supply the PingOne SAML connection settings to your ADFS administrator. To configure the PingOne side of the connection, the ADFS administrator will need to supply you with the ADFS SAML connection settings. We recommend using metadata files to update these settings, although you can configure the settings manually.

Steps

1. Go to **Setup > Identity Repository**, click **Connect to an Identity Repository**, and select **Microsoft ADFS**.
2. Click **Next**.
3. From the **Choose Signing Certificate** list, select the signing certificate for PingOne to use to sign SAML assertions sent to ADFS.
4. Click **Download PingOne Metadata**.

   The PingOne metadata includes all of the necessary PingOne connection information, including the encryption certificate and the primary and renewal certificates.
5. Click **Next**.
6. Assign the ADFS SAML connection settings in PingOne:

   Choose from:

   - Click the **Import Your ADFS SAML Connection Metadata** button. Click either **Select File** or **Use URL**.

     The SAML parameters required for the PingOne side of the connection will be automatically assigned based on the settings in the metadata.

     > **Note**
     >
     > The SAML connection metadata must be in UTF-8 format without a byte order mark (BOM).

   - Manually enter the values for these SAML connection settings used by ADFS:

     Entity ID

     Uniquely identifies the identity bridge to PingOne. This identifier is used in the Issuer element of the SAML assertion sent to us by the identity bridge.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> To ensure against possible identifier conflicts with the `idpid`, the Entity ID must be unique, unless you're assigning the Entity ID value for a private, managed application (an application that is supplied and configured by a PingOne for Enterprise administrator, rather than by an SP).

SSO Endpoint

The endpoint at your identity bridge to which PingOne sends AuthnRequests (using the Redirect method you assigned to the `Request Binding` attribute for your identity bridge).

Verification Certificate

The public verification certificate for your identity bridge. PingOne will use this certificate on your behalf to sign SAML assertions. Ensure that your IdP imports and recognizes this verification certificate.

Secondary Verification Certificate

A second certificate for us to use to sign SAML assertions on your behalf if verification fails when using your primary certificate. Ensure that your IdP imports and recognizes this verification certificate.

Single Logout Endpoint

(Optional) The endpoint (URL) configured for the identity bridge to which PingOne sends SAML single logout (SLO) requests. The SLO process uses the binding you choose for the `Single Logout Binding Type` attribute.

Single Logout Response Endpoint (IdP)

(Optional) The endpoint (URL) configured for the identity bridge to which PingOne sends single logout (SLO) responses. If you do not assign a value here, `Single Logout Endpoint` is also used as the response endpoint. The SLO process uses the binding you choose for the `Single Logout Binding Type` attribute.

Single Logout Binding Type

The binding type determines how the SAML protocol uses another protocol (in this case, HTTP) to transport messages. The SAML single logout (SLO) process can use either the POST or Redirect methods.

7. Click **Next**.
8. For each PingOne attribute, enter or select an ADFS attribute to map it to.

> **Note**
>
> For any of the attribute mappings, you can choose to configure an advanced mapping. See Creating advanced attribute mappings for instructions.

This assignment maps identity provider attributes to the default attributes used by the PingOne dock. This attribute mapping is not used by applications that you add to PingOne. Application attributes are mapped in each application.

Troubleshooting:

Mapping the PingOne `email` attribute to a custom ADFS attribute called `Email` can cause ADFS to send improperly formatted SAML assertions. When mapping the ADFS claim attribute `E-mail Addresses`, use the default ADFS claim attribute `E-mail Address` instead.

9. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Result

When you return to **Setup > Identity Repository**, a summary of the settings for your ADFS identity bridge is displayed. You can click **Edit** to modify the settings. You can also copy the **PingOne Metadata URL** and use it to keep your IdP configuration updated with PingOne metadata.

Connect to Google

About this task

The Google identity bridge uses the OpenID Connect protocol to connect to your Google domain.

You will need to log in to your Google account and enable settings to use Google as your identity bridge, with support for user provisioning. Then you will configure PingOne to use one of your Google groups and create PingOne groups of the same names as your Google groups.

> **Note**
>
> Every user who will SSO using PingOne dock needs to belong to a Google group.

Steps
In Google

1. Enable Domain Admin API access for your Google account:
    1. Sign on to your Google Admin console.
    2. On the menu bar, select **More controls**.
    3. Select **Security > API Reference**.
    4. Ensure the **Enable API Access** checkbox is selected.
    5. Save any changes.
2. Create a Google group, if you do not have one already.

    We require that you have at least one Google group. Each user signing on (SSO) through PingOne dock must be assigned to one or more Google groups.

    1. On the Admin console, select **Groups**.
    2. Click the **Create Group** link and assign a group name.
    3. On the Members tab, enter the user names to assign to the group, or select **Add all users**.

Note the names of the groups you create. You will use these in PingOne group management.

In PingOne

1. Configure the PingOne connection to your Google domain.
    1. Go to **Setup > Identity Repository**, click **Connect to an Identity Repository**, and select to set up the Google identity bridge.
    2. In the entry box for **Google Domain Name**, enter the domain name for your Google account.

Copyright © 2025 Ping Identity Corporation

3. Make sure you have popups enabled for your browser, the click **Configure OAuth**. This establishes a secure connection to your Google account using the OAuth protocol.
4. Assign the Google-to-PingOne attribute mapping.

   This assignment maps Google OpenID Connect attributes to the default PingOne attributes (used by PingOne dock). This attribute mapping is not used by applications that you add to PingOne. You will configure those attribute mappings for each application.

   For any of the attribute mappings, you can choose to configure an advanced mapping. See Creating advanced attribute mappings for instructions.
5. Click **Finish**.

   When you return to the Setup > Identity Repository page, a summary of the settings for your identity bridge is displayed. You can click the edit icon to modify the settings.

2. Add your Google groups to PingOne.
   1. See Adding user groups to add your groups to PingOne.

Result

Your Google identity bridge is now set up, with provisioning support for all users in your Google groups.

Connecting to a custom SAML provider

Any federated identity management service that supports SAML 2.0 can operate as a PingOne for Enterprise identity bridge.

About this task

You supply the PingOne for Enterprise connection details to the identity provider (IdP) administrator to configure the identity repository side of the connection, and you use the SAML connection settings supplied by the identity repository administrator to configure the PingOne for Enterprise side of the connection.

You can make the configuration entries manually or use metadata files to upload the information on both the identity repository side and the PingOne for Enterprise side.

Steps

1. In PingOne for Enterprise, select the public signing certificate for your identity bridge. You can choose either:

   Choose from:

   - Primary Certificate: When you select the primary certificate, the PingOne for Enterprise metadata for download contains both the primary and the renewal certificates.
   - Renewal Certificate: When you select the renewal certificate, the PingOne for Enterprise metadata for download contains only the renewal certificate. A renewal certificate is available only thirty days before the expiration of the primary certificate.

     PingOne for Enterprise uses this certificate on your behalf to sign SAML assertions sent to your IdP.
2. If you're configuring the identity bridge to support connections to multiple PingOne for Enterprise accounts, select **Enable Account-Specific Entity ID**.

Copyright © 2025 Ping Identity Corporation

In some cases, your organization may want to configure the identity bridge to support connections to multiple PingOne for Enterprise accounts. A typical scenario is organizations needing distinct connections from a number of divisions or subsidiaries.

PingOne for Enterprise supports these types of multiple connections through the identity bridge setup option `Enable account-specific Entity IDs`. Choosing this option creates a unique Entity ID based on your PingOne for Enterprise account (Company ID). This custom Entity ID is written to the PingOne for Enterprise metadata file that you download for import to your identity bridge.

> **Note**
>
> When changing an existing Entity ID for a PingOne for Enterprise identity repository, you also need to see that this value is changed on the IdP. Otherwise, SSO can be disrupted.

To make use of PingOne for Enterprise's account-specific IDs for multiple connections to a single identity bridge instance, your identity bridge needs to support the PingFederate concept of "virtual server IDs". This is an identity bridge feature for aliasing Entity IDs (connection IDs) for use by multiple service provider (SP)s. Using account-specific IDs, PingOne for Enterprise effectively impersonates multiple SPs.

1. A default Entity ID is displayed. You can accept the default value, which is uniquely-generated PingOne for Enterprise, or click the edit icon to enter your own Entity ID value.

   The Entity ID you enter is validated to ensure that it is unique in PingOne for Enterprise.

3. **Optional:** Select **Sign the AuthnRequest from PingOne** to have PingOne for Enterprise sign connection requests on your behalf.

   PingOne for Enterprise uses the public verification certificate you assign to your IdP.

   When checked, `AuthnRequestsSigned="true"` is added to the PingOne for Enterprisemetadata for download. When unchecked, `AuthnRequestsSigned="false"` is added.

4. In the **Signing Algorithm**list, select the algorithm used to sign both authentication and single logout (SLO) requests.

   If you're setting up a new identity bridge, the signing algorithm defaults to the recommended SHA-256.

   If you have an existing identity bridge configuration, SHA-1 may be displayed as the default signing algorithm. We recommend you change it to SHA-256.

5. Assign the PingOne for Enterprise connection settings in your IdP:

   Choose from:

   - **Download the PingOne metadata for import to your IdP**: All of the necessary PingOne for Enterprise connection information is contained in the metadata.

     The PingOne for Enterprise metadata includes the encryption certificate and the primary and renewal certificates or only the renewal certificate if you selected **Renewal certificate** for the public signing certificate.

   - Enter the PingOne for Enterprise connection information manually in your IdP. The following SAML parameters are required for assignment at your identity bridge:

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> You might want to download the PingOne for Enterprise metadata and reference the settings in the metadata file when assigning the parameter settings.

PingOne Entity ID

A globally unique name identifying PingOne for Enterprise as a SAML entity.

Assertion Consumer Service URL

The Assertion Consumer Service (ACS) URL used by PingOne for Enterprise to receive the AuthnResponse from your identity bridge indicating whether a user has been successfully authenticated for single sign-on (SSO).

SSO

Indicates whether SSO is initiated by the SP or by the IdP.

RelayState

The target resource used by PingOne for Enterprise to continue SSO to a particular application when initiating SSO from the IdP. If you're using IdP-initiated SSO, you need to include the SaaS ID either in this target resource or in the `ACS URL Parameter`.

ACS URL Parameter

A query parameter added to the `Assertion Consumer Service URL` to direct PingOne for Enterprise to continue SSO to a particular application when initiating SSO from the identity bridge. If you're using IdP-initiated SSO, you need to include the SaaS ID either here or in the `RelayState` value.

Outbound

The binding for outbound exchanges. Use POST.

Inbound

The binding for inbound exchanges. Use Redirect.

Protocol

The protocol to use for authentication assertions. Use SAML 2.0.

Profile

The method the identity bridge uses to send an assertion to PingOne for Enterprise. POST is the default.

Request Binding

The method PingOne for Enterprise uses to request an assertion. Redirect is the default.

6. Click to download the **Signing Certificate** and **Encryption Certificate**.

7. In your IdP, do one of the following:

Copyright © 2025 Ping Identity Corporation

Choose from:

- Upload or import the PingOne for Enterprise metadata file. The required SAML parameters will be assigned based on the settings in the metadata file.
- Manually assign the SAML parameter settings required for the PingOne for Enterprise connection. Reference the PingOne for Enterprise metadata file, if necessary.

8. In your IdP, select a method to assign the IdP connection settings in PingOne for Enterprise in the next step:

Choose from:

- Export your IdP metadata file for import into PingOne for Enterprise. The metadata must be in UTF-8 format without a byte order mark (BOM).
- Enter the following IdP connection information manually into PingOne for Enterprise. Reference the IdP metadata file, if necessary.:

Entity ID

Uniquely identifies the identity bridge to PingOne for Enterprise. This identifier is used in the `Issuer` element of the SAML assertion sent to us by the identity bridge.

> **Note**
>
> To ensure against possible identifier conflicts with the `idpid`, the Entity ID must be unique, unless you're assigning the Entity ID value for a private, managed application (an application that is supplied and configured by a PingOne for Enterprise administrator, rather than by an SP).

SSO Endpoint

The endpoint at your identity bridge to which PingOne for Enterprise sends AuthnRequests, using the Redirect method you assigned to the `Request Binding` attribute for your identity bridge.

Verification Certificate

The public verification certificate for your identity bridge. PingOne for Enterprise will use this certificate on your behalf to sign SAML assertions. Ensure that your IdP imports and recognizes this verification certificate.

Secondary Verification Certificate

A second certificate that PingOne for Enterprise can use to sign SAML assertions on your behalf if verification fails when using your primary certificate. Ensure that your IdP imports and recognizes this verification certificate.

Single Logout Endpoint

(Optional) The endpoint URL configured for the identity bridge to which PingOne for Enterprise sends SAML single logout (SLO) requests. The SLO process uses the binding you choose for the `Single Logout Binding Type` attribute.

Copyright © 2025 Ping Identity Corporation

Single Logout Response Endpoint (IdP)

(Optional) The endpoint (URL) configured for the identity bridge to which PingOne for Enterprise sends SLO responses. If you do not assign a value here, `Single Logout Endpoint` is also used as the response endpoint. The SLO process uses the binding you choose for the `Single Logout Binding Type` attribute.

Single Logout Binding Type

The binding type determines how the SAML protocol uses another protocol (in this case, HTTP) to transport messages. The SAML SLO process can use either the POST or Redirect methods.

9. In PingOne for Enterprise, assign the IdP connection settings in PingOne for Enterprise:

   Choose from:

   - Select to import your IdP connection metadata. The SAML parameters required for the IdP connection will be assigned based on the settings in the metadata file.
   - Use the list of connection settings you copied from your identity bridge to enter settings for the PingOne for Enterprise attributes displayed.

10. Ensure that the connection settings are correct.
11. Assign the IdP-to-PingOne for Enterprise attribute mapping.

    This assignment maps identity provider attributes to the default attributes used by PingOne for Enterprise dock. This attribute mapping is not used by applications that you add to PingOne for Enterprise. Configure those attribute mappings for each application.

    1. **Optional:** For any of the attribute mappings, configure an advanced mapping.

    For instructions, see Creating advanced attribute mappings.

    1. Click **Done**.

12. Click **Finish**.

Result

When you return to **Setup > Identity Repository**, you see a summary of the settings for your identity bridge.

Next steps

You can click **Edit** to modify the settings. You can also copy the **PingOne Metadata URL** and use it to keep your IdP configuration updated with PingOne for Enterprise metadata.

Creating advanced attribute mappings

Advanced attribute mappings allow you to customize attributes for specific applications or identity providers (IdPs).

About this task

> **Note**
>
> Advanced attribute mapping is not available for PingOne for Enterprise Directory.

Copyright © 2025 Ping Identity Corporation

Advanced attribute mapping mode enables you to modify the mapping of an identity repository attribute to a service provider's (SP) application attribute or to assign more than one identity repository attribute to an application attribute so that the needed attribute can be used without altering the existing mapping.

Use advanced attribute mapping when you:

- Customize PingOne dock settings, and you want to change one or more of the default attributes used by the identity bridge.
- Add a cloud application for your single sign-on (SSO) users, and one or more of the attributes for the application are different than the attributes used by the identity bridge.

In both cases, if the standard available attributes don't meet your needs, use advanced mode to customize an attribute.

Steps

1. On the **Attribute Mapping** tab for any application you are editing, click **Advanced** on the line of the attribute you want to map.
2. **Optional:** For **SAML_SUBJECT**, configure the **Name ID Format**.

Setting	Available Values
Name ID Format to request from IdP	◦ **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** ◦ **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress** ◦ **urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName** ◦ **urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName** ◦ **urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified** ◦ **urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos** ◦ **urn:oasis:names:tc:SAML:2.0:nameid-format:entity** ◦ **urn:oasis:names:tc:SAML:2.0:nameid-format:persistent** ◦ **urn:oasis:names:tc:SAML:2.0:nameid-format:transient**
Name ID Format to send to SP	

3. **Optional:** For all other attributes, configure the **NameFormat**.

Copyright © 2025 Ping Identity Corporation

Setting	Available Values
NameFormat	◦ **urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified** ◦ **urn:oasis:names:tc:SAML:2.0:attrname-format:uri** ◦ **urn:oasis:names:tc:SAML:2.0:attrname-format:basic**

4. **Optional:** For all attributes, apply advanced attribute mappings.

   Choose from:

   - In the **IDP Attribute Name or Literal Value** list, enter or select an attribute value.
   - Select the **As Literal** checkbox and enter a literal value to assign as an attribute.
   - For attributes that aren't literal values, select a transformation to apply to an attribute in the **Function** drop-down list. The following transformation functions are available.

Function	Description
Base64Decode	Decode the source value. Returns a null result if the source value isn't a valid Base64 encoding.
Base64Encode	Encode the source value.
ExtractByRegularExpression	Apply a regular expression to the attribute values. Any portion of a value that matches the regular expression is assigned to the attribute. For example, an incoming assertion uses `memberOf`, and you want only groups that match a specified list sent in the outgoing assertion. Assume the groups you want are A, B, C and D, and the incoming assertion contains the groups A, B, E, F in the `memberOf` attribute. In this case, your regular expression extracts only the group A and B values.
FilterByRegularExpression	Apply a regular expression to the attribute values. Only values that match the regular expression are assigned to the attribute. For example, if you want the resulting values to start with 'A' or 'b', use the regular expression `[Ab].*`.
GetDomainPartFromEmail	Get the domain part from an email string. For example, get *foo.com* from `bob.smith@foo.com`.

Copyright © 2025 Ping Identity Corporation

Function	Description
GetFirstRelativeDN	Get the first relative distinguished name (DN) from a DN string. For example, get *Bob Smith* from `CN=Bob Smith`, `OU=Sales`, `DC=Fabrikam`, `DC=com`.
GetLocalPartFromEmail	Get the local part from an email string. For example, get *bob.smith* from `bob.smith@foo.com`
Hash	Apply a hashing algorithm to the attribute value. You select the algorithm and the encoding format in the **Hashing Algorithm** and **Encoding Format** lists. **Hashing Algorithm** options: ■ **MD5** ■ **SHA-1** ■ **SHA-256** **Encoding Format** options: ■ **hex** ■ **Base64**
PickByFieldsFrom JsonList	Pick the field values from a multivalued attribute that match the condition you specify. Each field value is a JSON object.
PickPrimaryObjectByTypeFromJsonList	Pick the JSON objects in the list that have a `primary` value of true, and a `type` value equal to the condition value. If you don't specify a condition, the `type` value is ignored and all matching `primary` value objects are returned.
PickPrimaryValueByTypeFromJsonList	Pick the JSON objects' `value` field values in the list, where the objects' `primary` value is true and the `type` value matches the condition value. If you don't specify a condition, the `type` value is ignored and all matching `primary` value objects are returned.

Copyright © 2025 Ping Identity Corporation

Function	Description
Random	Assign a random value to the attribute. You must supply the character length to use. You can also apply a hashing algorithm and encoding format to the random value. **Hashing Algorithm** options: ■ **None** ■ **MD5** ■ **SHA-1** ■ **SHA-256** **Encoding Format** options: ■ **None** ■ **hex** ■ **Base64**
ToLowerCase	Change all characters to lower case.
ToUpperCase	Change all characters to upper case.

1. To add an additional value to map to the attribute, click **Add Attribute**.
2. Click **Save**.

Managing applications

PingOne for Enterprise allows you to connect your workforce users to hundreds of applications with a single sign-on (SSO).

You can make applications available to your users in the following ways:

- Add an application using its SAML connection information
- Add an application using its OIDC connection information
- Add an application using its SSO URL
- Add an application from the Application Catalog
- Create a Basic SSO (password vaulting) application

When you add an application to your PingOne for Enterprise account, you establish a connection through which your users access the application. The applications you add are then available in the PingOne for Enterprise dock.

If you are not using the PingOne for Enterprise dock, you can make applications directly available to your users through an SSO URL. See Add or update an application using its SSO URL for instructions.

You don't need to make all applications available to all users. You have the option to limit users' access to applications based on their group membership. For more information, see Managing users by group.

Applications are assigned to a default category when you configure them, but you can also create custom application categories that fit the needs of your organization. For more information, see Creating a custom application category.

Copyright © 2025 Ping Identity Corporation

Applications that you add to PingOne for Enterprise are listed at **Applications > My Applications** in the admin portal.

You can edit an existing application's configuration by expanding its entry on the **My Applications** page and clicking **Edit**. When you edit an application, refer to the corresponding documentation for adding and updating an application.

Adding or updating a SAML application

If you don't have the service provider's (SP) single sign-on (SSO) URL for the application (generally a SAML application that already exists in your organization), you will need to configure the necessary SAML settings to add the application.

About this task

> **Note**
>
> If you are using the Google identity bridge, you cannot add Google applications using this method. See Add or update an application using its SSO URL to add these applications.

Steps

1. Go to **Applications > My Applications > SAML**.
2. Click **Add Application > New SAML Application**.
3. On the **Application Details** tab, enter the application details. **Application Name**, **Application Description** and **Category** are required fields.

   You can optionally assign an application icon. The icon file can be up to 5 Mb in size. The supported graphics formats are JPEG/JPG and PNG.
4. Click **Continue to Next Step**.
5. On the **Application Configuration** page, provide the SAML configuration details for the application.
    1. **Signing Certificate**. In the list, select the signing certificate you want to use.
    2. **SAML Metadata**. Click **Download** to retrieve the SAML metadata for PingOne for Enterprise. This supplies the PingOne for Enterprise connection information to the application.
    3. **Protocol Version**. Select the SAML protocol version appropriate for your application.
    4. **Upload Metadata**. Click **Select File** to upload the application's metadata file, or click **Or use URL** to enter the URL of the metadata file. The **ACS URL** and **Entity ID** will then be supplied for you. If you don't upload the application metadata, you'll need to enter this information manually with values provided by the application.

       > **Note**
       >
       > The application's **Entity ID** must be unique within your account. You can't configure more than one application in PingOne for Enterprise using the same SP entity ID.
    5. **Application URL**. This is required by some applications as the target URL. It's used in identity provider (IdP)-initiated SSO for a deep-linking purpose. The application URL is passed in the `RelayState` parameter by the IdP.
    6. **Single Logout Endpoint**. The URL to which our service will send the SAML Single Logout (SLO) request using the **Single Logout Binding Type** that you select).

Copyright © 2025 Ping Identity Corporation

7. **Single Logout Response Endpoint**. The URL to which your service will send the SLO Response.
8. **Single Logout Binding Type**. Select the binding type (**Redirect** or **POST**) to use for SLO.
9. **Primary Verification Certificate**. Click **Choose File** to upload the primary public verification certificate to use for verifying the SP signatures on SLO requests and responses.
10. **Secondary Verification Certificate**. Click **Choose File** and upload the secondary verification certificate if available. The secondary verification certificate is used if the primary verification certificate fails to validate a signature.
11. **Optional: Encrypt Assertion**. If selected, the assertions PingOne sends to the SP for a multiplexed application will be encrypted. You can also use this option for your managed applications. Available for SAML 2.0 applications only.

    > **Note**
    >
    > If an encryption certificate is included in the metadata you upload, this option is automatically enabled. The entry for **Encryption Certificate** will show the name of the certificate and the entry for **Encryption Algorithm** will be set to AES_256.

    Selecting this option displays the information needed to encrypt the assertion:

    ### *Encryption Certificate*

    Upload the certificate to use to encrypt the assertions.

    ### *Encryption Algorithm*

    Choose the algorithm to use for encrypting the assertions. We recommend **AES_256** (the default), but you can select **AES_128** instead.

    ### *Transport Algorithm*

    The algorithm used for securely transporting the encryption key. Currently, **RSA-OAEP** is the only transport algorithm supported.

12. **Signing**. Select either to sign the SAML assertion or to sign the SAML response.

    When you have selected **Encrypt Assertion**, we highly recommend that you choose to sign the response. This provides a significant increase in security.

13. **Signing Algorithm**. Select an algorithm from the list.

We strongly recommend using the default **RSA_SHA256** algorithm or higher.

1. **Force Re-authentication**. If selected, users having a current, active SSO session will be re-authenticated by the identity bridge to establish a connection to this application.
2. **Force MFA**. If selected, users are required to use multi-factor authentication (MFA), as defined by the applied application policy, each time they access the application.

   You'll need to have an authentication policy in place to use this setting. See Create or update an authentication policy for more information.
3. **Use Custom URL**. Select and enter a custom URL in the text box to customize the URL to launch the application from the dock. This can be an SSO URL assigned by the SP or IdP. The default URL is generated by PingOne for Enterprise.

Copyright © 2025 Ping Identity Corporation

The remaining entries are optional, depending on your requirements. Click **Continue to Next Step**. The SSO Attribute Mapping page is displayed.

6. Modify or add any attribute mappings as necessary for the application.

   In most cases, the default attribute mappings are sufficient. These mappings assign your identity repository attributes to the attributes provided by the SP for the application.

   > **Note**
   >
   > If you're adding SAML subject as an attribute, make sure to use the value `SAML_SUBJECT` for the **Application Attribute** field. If not defined, `SAML_SUBJECT` will be mapped to the subject sent by the IdP.

   For each application attribute, you can:

   Choose from:

   - Click the **Required** checkbox to designate an attribute or attributes as required by the application.
   - Click in an entry box and select an identity repository attribute from a drop-down list.
   - Click in an entry box and enter an identity repository attribute.
   - Click the **As Literal** checkbox and in the entry box, enter a literal value to assign.
   - Click **Advanced** and enter Advanced Attribute Mapping mode. See Creating advanced attribute mappings for instructions.
   - Click **Add new attribute** to enter any additional attributes required by the application. You can then enter custom text in the **Application Attribute** text box, in addition to all of the choices above when configuring the new attribute.

7. When you have finished modifying or adding any additional attributes, click **Continue to Next Step**.

   The **Add Groups** page is displayed.

8. Make the new application available to your users by assigning the groups authorized to use the application.

   All members of the selected group or groups will be able to use the application. When the application supports user provisioning, user provisioning to this application is also enabled for members of the assigned groups.

   1. Click **Add** for each group you want to authorize to use the application.
   2. Click **Continue to Next Step**

      Result:

      The summary information for the application configuration is then displayed on a new page.

9. Review the application connection information.

   Some of this information might be needed by the SP to complete the SSO configuration for the application. In particular, you can download the PingOne for Enterprise signing certificate or the PingOne for Enterprise **SAML metadata**, which has the certificate embedded. You can also copy the **SAML Metadata URL** and use it to keep your IdP configuration updated with PingOne for Enterprise metadata.

Copyright © 2025 Ping Identity Corporation

The SSO URL for the application is displayed as the value of **Initiate Single Sign-On (SSO) URL**. You can use this to test SSO directly to the application without going through the PingOne for Enterprise dock.

10. Click **Edit** to change any of the configuration settings, or **Finish** to complete the application setup.

Result

The new SAML application is added to your My Applications list.

You can go to **Users > User Groups** to see that the application you have added is now authorized for use by the selected group or groups.

Configuring your OAuth settings

The OAuth settings enable you to configure the access token and any refresh tokens issued for your OpenID Connect (OIDC) applications when requesting user authorization.

About this task

PingOne for Enterprise supports OAuth authorization code, refresh token, implicit and hybrid (both code and implicit) grant types. PingOne for Enterprise issues an OAuth access token for an application only when `token` is one of the `response_type` values specified in the application's authorization request.

When PingOne for Enterprise issues an access token, it contains attributes required by the OIDC specification and any other attributes you assign for the OAuth attributes contract.

As part of the authorization request, PingOne for Enterprise requires the scopes (permissable user resources) you assign when authorizing users.

You can also specify attribute mappings (OAuth claims to identity repository attributes) both at the account level and at the application level. The account-level settings can be overridden when you configure the attribute mapping at the application level (when you are adding the OIDC application).

For implicit grant types, PingOne for Enterprise issues an OAuth access token specifying the attribute contracts that your OIDC applications use to request user authorization. The OAuth access token settings govern how the access token is issued, such as whether it's signed or encrypted. The issued access token is used in your application's authorization requests to PingOne for Enterprise.

Additionally, all authorization request include the user scopes (permissable user resources) you assign here. The scopes are granted after the user is authenticated. You can also specify any attribute mappings that you want to be inherited by OIDC applications. Optionally, you can assign trusted origins for Cross-Origin Resource Sharing (CORS).

> **Note**
>
> For managed accounts, the OAuth settings apply only to your managed applications, not to applications supplied by a service provider (SP).

Steps

1. Go to **Applications > OAuth Settings > Access Token**.

Copyright © 2025 Ping Identity Corporation

2. On the **Access Token** page:

    1. Select the **Format** to use for the access token:

        - **Signed**: The access token is signed using the PingOne for Enterprise OIDC signing key. The PingOne for Enterprisesigning key is available at the PingOne for Enterprise OAuth endpoint `https://sso.connect.pingidentity.com/sso/as/jwks`.
        - **Encrypted**: The content of the access token is hidden from both the application and from any API.

    2. Enter the number of minutes for the access token's **Lifetime**.

    This is the duration an access token is valid before expiring. The valid range is 1 - 60 minutes.

    1. Enter any additional **Attribute Contracts** that are to be included in the access token:

        - The `sub` (Subject) attribute is always required for the access token.
        - The `idpid` attribute can be removed, but is assigned by default. This is a PingOne for Enterprise attribute used to identify the identity repository used. When included, the `idpid` attribute is automatically mapped to the `idpid` of the identity repository when you configure an application that uses this access token.

          These attributes and any others you specify here are available in the attribute mapping used for the connection to an application that uses this access token.

          > **Note**
          >
          > Only attributes that are marked as required must be mapped to a valid attribute for your identity repository for applications using this access token.

    2. Click **Save**.

3. Click the **Refresh Token** tab.

    Refresh tokens are available only when you're using the Authorization Code grant type. In this case, a refresh token is automatically exchanged for an access token if the access token expires.

    The refresh token settings control the duration for which a refresh token is valid. Together, these settings help ensure the security of your refresh tokens.

    1. Select a value for **Idle Lifetime**.

        This is the maximum number of minutes that a refresh token can be idle (unused) before being used again. The default value is 10 minutes.

    2. Select a value for **Max Lifetime**.

        This is the maximum number of minutes that a refresh token can be valid. The default value is 10 minutes.

4. Click the **Scopes** tab.

    The scopes identify the permissible user resources that are to be included in the OAuth authorization request. You can do any of the following actions with the scopes.

Copyright © 2025 Ping Identity Corporation

Option	Description
Add a scope	1. Click **Add New Scope**. 2. Enter a **Scope** supported by your OIDC provider. 3. Enter a **Name** to use for the scope. 4. Enter a claim for the scope. The claims are attributes of the scope that you want to be included in the authorization request. 5. Click **Add Claim** for each additional claim to include. 6. Click **Save**.
Edit existing scopes	1. Expand the details for the scope to modify and click the **Pencil** icon. 2. Click **Add Claim** for each additional claim to include. 3. Click the **Delete** icon for each claim you want to delete. 4. Click **Save** when you're finished.
Delete a custom scope	1. Expand the details of a custom scope. 2. Click the **Delete** icon. **Note** The default scopes can't be deleted.

5. To configure the mapping of identity repository attributes to OIDC scope claims click the **Attribute Mapping** tab.

   The **Attribute Mapping** page is an account-level mapping of identity repository attributes to OIDC scope claims. When you are configuring an application that uses this access token, the mappings you specify here are inherited at the application configuration level (where you can override the settings as needed). Doing this mapping at the account level streamlines the attribute to claims mapping you might need to do when configuring applications.

   The listing of claims applies to all scopes. Claims that exist in more than one scope use the same attribute mapping that you specify here.

   1. For the desired OAuth claim, in the **Mapping** list, select the identity repository attribute to use for the mapping.
   2. If you want to further customize the mapping, click **Advanced** to display the advanced attribute mapping mode.

   For detailed instructions, see Assign advanced attribute mappings.

   1. To exit advanced attribute mapping mode, click **Close Advanced**.
   2. Continue mapping any further OAuth claims to identity repository attributes.
   3. Click **Save**.

6. To configure Cross-Origin Resource Sharing (CORS), click **Additional Settings**.

Copyright © 2025 Ping Identity Corporation

When configured, applications from the trusted origins are allowed to make requests to the supported PingOne for Enterprise authorization server endpoints.

1. In the **Allowed Origin** field, enter a valid URI for one or more of the trusted origins.

   > **Note**
   >
   > The maximum number of trusted origins is 100.

   Example:

   For example:

   `https://www.example.com`

   CORS requests originating from this URI are allowed.

   `https://www.example.com:8080`

   CORS requests originating from port 8080 of this URI are allowed.

   `https://www.example.com:*`

   CORS requests originating from any port for this URI are allowed.

   The specified origin or origins must be available at SSO runtime to all of your managed OIDC applications. OIDC applications originating at a service provider or (for PingOne for Managed Service Providers) customer accounts are not supported as trusted origins.

Requests from the trusted origins apply to the following PingOne for Enterprise OAuth endpoints:

- `/sso/as/token.oauth2`
- `/sso/as/introspect.oauth2`
- `/sso/idp/userinfo.openid`
- `/sso/as/jwks`
- `/.well-known/openid-configuration`
- `/{client_id}/.well-known/openid-configuration`

Adding or updating an OIDC application

Create a new OpenID Connect (OIDC) application or modify an existing application in PingOne for Enterprise.

Before you begin

Before you add an OIDC application, you must configure the access token that your account will use for OIDC applications. These account-level settings are inherited at the application level when you add or update an application.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Account-level OAuth settings apply only to your managed applications, not to applications supplied by a service provider (SP).

PingOne for Enterprise returns OIDC user attributes in different ways depending on the `response_type` parameter.

The contents of the ID token depend on whether or not the application also returns an access token:

- For flows that return both an access token and an ID token (such as authorization code flow, or implicit flows where the `response_type` includes `token`) the ID token contains the `sub` and, if requested, `email` scopes. The `userinfo` endpoint contains all of the attributes for the requested scopes and attributes configured on the **User Info** tab for the application, if the `openid` scope was requested.
- For flows that don't return an access token, the ID token contains all of the attributes for the requested scopes and any attributes configured on the **User Info** tab for the application, if the `openid` scope was requested. The `userinfo` endpoint is inaccessible in this case because no access token is issued.

The access token contains attributes configured at **Applications > OAuth Settings > Access Token**.

For more information, see Configuring your OAuth settings.

> **Note**
>
> When you add an OIDC application, you must have access to the necessary configuration information for the application. For applications supplied by an SP, the SP will direct you to this information.

Steps

1. Go to **Applications > My Applications > OIDC**.
2. Add a new application or edit an existing application.

   Choose from:

   - To create a new application, click **Add Application**. See Step 3 for new application types.
   - To update an existing application, expand the application and click the **Pencil** icon. Skip to step 4.
3. Select the type of application that you want to add and click **Next**:

   Choose from:

   - To create an application that is accessed and used within a browser, click**Web App**.
   - To create an application that is stored locally and run on a desktop or device, click **Native App**.
   - To create an API-driven front-end application, such as applications using Node.js or Angular, click **Single Page App**.
   - If you want full control of all available configuration parameters, click **Advanced Configuration**.
4. In the **Application Name** field, enter an application name.
5. In the **Short Description** field, enter an application description.
6. In the **Category** list, select a category to assign the application to.

Copyright © 2025 Ping Identity Corporation

7. **Optional:** To add an icon for the application, click the **Image** icon and upload an icon image.

   The icon file can be up to 1 Mb in size. The supported graphics formats are JPEG/JPG, PNG and GIF.

8. Click **Next**.

9. **Optional:** To enable or disable a custom valid duration for the application access token, click the **Override Access Token Lifetime** toggle.

10. **Optional:** If you enabled the override, enter the number of minutes access token lifetime in the **Minutes** field.

    The valid range is 1 - 60 minutes. The default value is inherited from your account-level OAuth settings. For more information, see Configuring your OAuth settings.

11. Select the allowed grant types for the application.

    Available grant types are determined by the application type. For more information, see OIDC application grant types.

12. **Optional:** If you selected **Refresh Token**, configure the token settings:

    1. Click the **Override Refresh Idle Lifetime** toggle to override the global OAuth setting for the application.
    2. In the **Refresh Token Idle Lifetime** field, enter the number of minutes that a refresh token can be idle before being used again.
    3. Click the **Override Refresh Token Max Lifetime** toggle to override the global OAuth setting for this application.
    4. In the **Refresh Token Max Lifetime** field, enter the maximum number of minutes that a refresh token can be valid.

13. **Optional:** For Web Apps and Advanced Configuration applications, click **Add Secret** to add a secret to pair with the application **Client ID**.

    If you want to change a client secret, you must generate a second secret before deleting the first.

    > **Tip**
    >
    > For greater security with Web App applications, you can use PKCE in your authorization and token request. In this case, a client secret is not used. For more information, see OAuth 2.0 RFC 7636.

14. Copy the **Discovery URL**, **Issuer**, and **IDPID** values to use later in integrating the application with PingOne for Enterprise.

    This information also displays on the summary page for the application after you've added the application to PingOne for Enterprise.

    For more information, see Integrating an OIDC application.

15. Click **Next**.

16. In the **Start SSO URL** field, enter the URL to use for SSO to the application.

    This is the URL to which application users will redirect to initiate SSO to PingOne for Enterprise using OIDC.

17. In the **Redirect URIs** field, enter URIs forPingOne for Enterprise to send responses to for the application's authorization requests.

Copyright © 2025 Ping Identity Corporation

> **Tip**
>
> Click **Add URL** to define multiple redirect URIs.

18. **Optional:** In the **Logout URI** field, enter the URI to which PingOne for Enterprise sends a user for single logout (SLO).
19. **Optional:** Select the authentication requirements.

Authentication Method	Description
Force authentication	If selected, to establish a connection to this application, users having a current, active SSO session will be re-authenticated by the identity repository.
Force multi-factor authentication	If selected, users are required to use multi-factor authentication (MFA) as defined by your authentication policy each time they access the application. You'll need to have an authentication policy in place to use this setting. See Create or update an authentication policy for more information.

20. Click **Next**.
21. To add attributes to the **Default User Profile Attribute Contract**, click **Add Attribute** and enter an attribute in the **Attribute Name** field.

    Select the **Required** checkbox to make the attribute required.

    The default user profile attribute contract is the user profile returned by the `userinfo` endpoint for this application when the `openid` scope is included in the authentication request.

    The (subject) `sub` attribute is required for all UserInfo requests.

    PingOne for Enterprise uses the `idpid` attribute to identify the identity provider (IdP) and is included in the attribute contract by default.

    If the application you're adding is a managed application, you can remove the `idpid` attribute from the contract. For managed applications,PingOne for Enterprise already has the `idpid` value for your account.
22. Click **Next**.
23. Click the [.uicontrol]***+***icon to add scopes to the allowed list, or click the **-** icon to remove them.

    These OAuth user scopes are the user resources to which the application will request access. The `openid` scope is expected to always be included in the authorization request.
24. Click **Next**.

1. Map identity repository attributes to claims made by the application.

   For each IdP attribute, enter or select the target attribute from the list.

   Click **Advanced** to display the advanced attribute mapping mode. For more information, see Assign advanced attribute mappings.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> This is a mapping of your identity repository attributes to the OIDC scope claims available to the application. By default, the attribute mapping inherits the account-level attribute mapping that you specify when you configure your OAuth settings.
> You can override the account-level attribute mappings for the application. If you update the attribute mappings, the inherited account-level mappings remain available as selections in the list.
> The OIDC claims listed here include all claims from the access token attribute contract, the `UserInfo` attribute contract for this application, and the claims for any scopes to which this application is permitted.
> The attributes listed are determined by the scopes that you added previously. The `sub` attribute is required for all applications.

1. Click **Next**.
2. Make the new application available to your users by assigning the groups authorized to use the application.

   Click the + icon for each group that you want to authorize.

   > **Note**
   >
   > All members of the selected groups can use the application.

3. Click **Done**.

Result

The new OIDC application is added to your **My Applications** list for OIDC. You can edit the application configuration by clicking the **Edit** icon.

Next steps

Integrate your OIDC applicationwith PingOne for Enterprise.

Integrating an OIDC application

After you add or update an OIDC application, you need to integrate it with PingOne for Enterprise.

About this task

After adding an OpenID Connect (OIDC) application, you need to integrate the application with PingOne for Enterprise, which will act as the OAuth provider (OP) for your application. Your application then needs to request authorization from the PingOne for Enterprise OAuth authorization endpoint when users attempt to single sign-on (SSO) to the application.

See the OpenID Connect Core 1.0 specification for reference when integrating the application.

PingOne for Enterprise returns OIDC user attributes in different ways depending on the `response_type` parameter.

The contents of the ID token depend on whether or not the application also returns an access token (If the `response_type` includes `token`).

If an access token is returned, the application returns an ID token containing the `sub` and, if requested, `email` scopes. The userinfo endpoint contains all of the attributes for the requested scopes, as well as an attributes configured on the **User Info** tab for the application, if the `openid` scope was requested.

Copyright © 2025 Ping Identity Corporation

If an access token is not returned, the ID token contains all of the attributes for the requested scopes, as well as any attributes configured on the **User Info** tab for the application, if the `openid` scope was requested. The userinfo endpoint is inaccessible in this case because no access token is issued.

The access token contains attributes configured at **Applications > OAuth Settings > Access Token**.

For more information, see Configuring your OAuth settings.

The authorization request flow depends on the grant type you have selected for the application. The grant type can be **Authorization code**, **Implicit**, or a hybrid (both code and implicit).

For more information, see OIDC application grant types.

Steps

1. Go to **Applications > My Applications > OIDC**.
2. Click **Expand** to display the summary page for the OIDC application to integrate.

   Result:

   The PingOne for Enterprise **Discovery URL** for the application is displayed in the **Details** section. The application's client ID value is part of the URL.
3. In a new browser tab, enter the **Discovery URL**.

   Result:
   `{p14e} returns OIDC configuration information, including the endpoints you will use to integrate the application.`

Copyright © 2025 Ping Identity Corporation

Code

Code grant type

For any grant type, the application needs to send the authorization request to the PingOne for Enterprise authorization endpoint returned by the **Discovery URL**(`https://sso.connect.pingidentity.com/sso/as/authorization.oauth2`).

PingOne for Enterprise validates the `redirect_uri` parameter against the list of redirect URIs specified in the application's configuration. You can find these URIs in the **Authentication Flow** section on the application summary page. If the `redirect_uri` is valid, PingOne for Enterprise sends the response to the specified redirect URI.

If your application uses an authorization code grant type, PingOne for Enterprise uses the following process to complete the authorization request:

1. The application sends an authorization request for a code grant type.

   Here is an example of an authorization request URI:

   ```
   https://sso.connect.pingidentity.com/sso/as/authorization.oauth2?client_id=5f65fdde-44e2-4d1c-be2b-41d5e0d6b903&response_type=code&redirect_uri=https://localhost&scope=openid
   ```

   The following table describes the parameters that make up the authorization request URI.

Parameter	Description
`client_id`	Your client ID, assigned by PingOne for Enterprise. You can find this value on the **Details** tab.
`scope`	The user resources that can be accessed by the application. The `openid` scope is expected to be specified, either as the sole scope value or one of the scope values.
`response_type`	This must be `code`. An authorization code is then returned in the response.
`code_challenge`	This PKCE parameter is either plain text or a cryptographic hash of a random string. The random string or plain text must be a `code_verifier` value that you will include in the subsequent token request. **Note** Use PKCE only when you aren't using a client secret, including `client_secret` in the token request. For more information, see OAuth 2.0 RFC 7636.

Copyright © 2025 Ping Identity Corporation

Parameter	Description
`code_challenge_method`	This PKCE parameter is required only when `code_challenge` is specified. This can be either: ◦ `plain` When the `code_challenge_method` value is plain text ◦ `S256` When the `code_challenge_method` value is an SHA-256 cryptographic hash **Note** When you subsequently include the `code_verifier` value in the token request, the `code_challenge` value and the `code_verifier` value must match. For more information, see OAuth 2.0 RFC 7636.

2. The PingOne for Enterprise authorization endpoint returns the authorization code to the application.

   The HTTPS response will be similar to this:

   ```
   https://localhost/?code=I0YAW2EWll_V8xH4m6b7IJ3WWD1wNZ5BnvkCQw7gknp4z2gQkHCM66AHsbCLA7
   ```

3. The application uses the authorization code returned in the response to request an access token and ID token from the PingOne for Enterprise token endpoint, https://sso.connect.pingidentity.com/sso/as/token.oauth2.

   Here is an example request using cURL:

   ```
   curl -k -X POST -H "Accept: application/json" -d 'client_id=cdd237bb-3404-4ad4-90eb-
   d2e2528xxxxx&client_secret=CpquMknCg9An9Up1Ys2mnVEdKkCDaxtJcJG4adFPBDnPU6SBp7VNGUhyTmaJXXmpR&grant_typ
   e=authorization_code&code=ID5d7d1770409374639980ce161952fda57b21db562ff8320b020000016543fxxxxx&redirec
   t_uri=https://example.com\' https://sso.connect.pingidentity.com/sso/as/token.oauth2
   ```

   Because the authorization request did not include PKCE parameters, the token request must use the client secret value assigned when the application was added to PingOne for Enterprise. You can find the assigned client secret in the **Details** tab.

4. The application validates the `id_token` returned. For more information see the OpendID Connect Core 1.0 specifications.

5. The application can also optionally validate the token or access token returned.

   Use the PingOne for Enterprise introspection endpoint returned by the **Discovery URL** `https://sso.connect.pingidentity.com/sso/as/introspect.oauth2` to validate the access token.

   For access tokens that are signed rather than encrypted, you can also use the JWKS URI returned by the **Discovery URL** `https://sso.connect.pingidentity.com/sso/as/jwks`.

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise

> **Note**
>
> You can see your access token settings at **Applications > My Applications > OAuth Settings**.
> For more information, see Configuring your OAuth settings.

Copyright © 2025 Ping Identity Corporation

Implicit

Implicit grant type

For any grant type, the application needs to send the authorization request to the PingOne for Enterprise authorization endpoint returned by the **Discovery URL**(`https://sso.connect.pingidentity.com/sso/as/authorization.oauth2`).

PingOne for Enterprise validates the `redirect_uri` parameter against the list of redirect URIs specified in the application's configuration. You can find these URIs in the **Authentication Flow** section on the application summary page. If the `redirect_uri` is valid, PingOne for Enterprise sends the response to the specified redirect URI.

If your application uses an authorization implicit grant type, PingOne for Enterprise uses the following process to complete the authorization request:

1. The application sends an authorization request for an implicit grant type.

   Here is an example of an authorization request URI:

   ```
   https://sso.connect.pingidentity.com/sso/as/authorization.oauth2?client_id=5f65fdde-44e2-4d1c-be2b-41d5e0d6b903&response_type=token id_token&redirect_uri=https://localhost&scope=openid&nonce=123
   ```

   The following table describes the parameters that make up the authorization request URI.

Parameter	Description
`client_id`	Your client ID, assigned by PingOne for Enterprise. You can find this value on the **Details** tab.
`scope`	The user resources that can be accessed by the application. The `openid` scope is expected to be specified, either as the sole scope value or one of the scope values. **Note** When `openid` is not specified and the `response_type` value indicates `id_token`, an `id_token` is not returned.
`response_type`	This can either be `id_token`, `token` (access token), or both. The token or tokens specified are returned in the response.
`nonce`	This is used to securely associate `client_id` with `id_token`. For more information, see OpenID Connect Core 1.0 Nonce Implementation Notes.

2. The PingOne for Enterprise authorization endpoint returns the `response_type` value to the application.

Copyright © 2025 Ping Identity Corporation

If you included `id_token` and `token` in the authorization request, as in the example, an access token is returned with the `id_token` value in the response.

The HTTPS response will be similar to this:

```
https://localhost/
#access_token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjdBOUMxMDA4REEzMzAwQTExMTYwQkQ1NUFEMUExOEFGQTQ3C
w7reDCUoF-7XjhQGYp4ttUiOFFHRjmAsVtFsLdcLSP3uCtsIU7-Hk45hZdNXkbdFg44GSRNQNegtJYI-YB0qv4_5rr-
zVEJV_MR6ZRbUYre2lFiIMtj44CRCkeGA9_kajJY0rcumT9SlbFkNcz8axUSoYKK_D-Eh_pWY4-y54P1FLB0xQ-
mwPl28K-DNcO3vxinlnh54X-Xt2Vn3qPBPHSf0wtvb-ko8lzw_dcZmWOjt-
ZX8KOBbz3OgBMg2kbP6re0o2aB73gGxHyzwVsuUPhjUg&token_type=Bearer&id_token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCI
```

3. If an `id_token` was included in the authorization request, the application validates the `id_token` returned.

   For more information, see the OpendID Connect Core 1.0 specifications.

4. The application can also optionally validate the token (access token) returned.

   Use the PingOne for Enterprise introspection endpoint returned by the **Discovery URL** `https://sso.connect.pingidentity.com/sso/as/introspect.oauth2` to validate the access token.

   For access tokens that are signed rather than encrypted, you can also use the JWKS URI returned by the **Discovery URL** `https://sso.connect.pingidentity.com/sso/as/jwks`.

   > **Note**
   >
   > You can see your access token settings at **Applications > My Applications > OAuth Settings**. For more information, see Configuring your OAuth settings.

Copyright © 2025 Ping Identity Corporation

Hybrid

Hybrid grant type

For any grant type, the application needs to send the authorization request to the PingOne for Enterprise authorization endpoint returned by the **Discovery URL**(`https://sso.connect.pingidentity.com/sso/as/authorization.oauth2`).

PingOne for Enterprise validates the `redirect_uri` parameter against the list of redirect URIs specified in the application's configuration. You can find these URIs in the **Authentication Flow** section on the application summary page. If the `redirect_uri` is valid, PingOne for Enterprise sends the response to the specified redirect URI.

If your application uses both code and implicit grant types, PingOne for Enterprise uses the following process to complete the authorization request:

1. Your applications sends an authorization request for a hybrid grant type.

   Here's an example of an authorization request URI:

   ```
   https://sso.connect.pingidentity.com/sso/as/authorization.oauth2?client_id=5f65fdde-44e2-4d1c-be2b-41d5e0d6b903&response_type=code token id_token&redirect_uri=https://localhost&scope=openid&nonce=123
   ```

   The following table describes the parameters contained in the authorization request URI.

Parameter	Description
`client_id`	Your client ID, assigned by PingOne for Enterprise. You can find this value on the **Details** tab.
`scope`	The user resources that can be accessed by the application. The `openid` scope is expected to be specified, either as the sole scope value or one of the scope values. **Note** When `openid` is not specified and the `response_type` value indicates `id_token` , an `id_token` is not returned.
`response_type`	This can be any or all of the following: ◦ `code` ◦ `id_token` (as in the above example) ◦ `token` (access token) The specified tokens are returned in the response along with the authorization code.
`nonce`	Required when `id_token` is included in `response_type` . It is used to securely associate `client_id` with `id_token` . For more information, see OpenID Connect Core 1.0 Nonce Implementation Notes.

Copyright © 2025 Ping Identity Corporation

Parameter	Description
`code_challenge`	This PKCE parameter is either plain text or a cryptographic hash of a random string. The random string or the plain text must be the `code_verifier` value that you will include in the subsequent token request. **Note** Use PKCE only when you aren't using a client secret, including `client_secret` in the token request.
`code_challenge_method`	This PKCE parameter is required only when `code_challenge` is specified. This can be either: ◦ `plain` When the `code_challenge` value is plain text. ◦ `S256` When the `code_challenge` value is an SHA-256 cryptographic hash. **Note** When you subsequently include the `code_verifier` value in the token request, the `code_challenge` value and the `code_verifier` value must match.

2. The PingOne for Enterprise authorization endpoint returns the `response_type` value or values to the application. If you included `code`, `id_token`, and `token` in the authorization request, as in the example, an authorization code, `access_token`, and `id_token` are all returned in the response.

   The HTTPS response will be similar to this (using the fragment response method):

   ```
   https://localhost/#code=I09HefT4OVGqJl1r-HrycCWsIG-
   rTNBN4BC_P_AyGsw0bEeTdintMtGjWMBfxL&access_token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjdBOUMxMDA4RE
   yeJ5_BeFvFzlxvriCvJNx6TsEuDK8kw-GVlcTcTWd3MN0cdVYY2XkmihNJzuZbJfzgG3-
   Ec22npOuyGbYkQQKGsUWJC9oHntAhl2VMPi4YwS7-as4pTRIsdk7-GZ6KgQ5ZXL9Rk9vJmsLpfghEtsYh6SX41-
   E_PA5LP9fG7BmfK7vnvtIfyVC28C6NAaWT5i-
   WSJImEcdCL79T9LMlfixUJrY7jfi1cJ7jlr9pPITFOd7eny9g0Q_W2jG2f5Jg8cmK8Pmpd6W1O2xuIKlcamwEP7hF3OkD16kR0v84BT0L2e
   M8BhMNSF4fP5uZyhJRhHduEog-Fc7NMHySzhnhlEsRlC94isjteSJeu2Co_geDjlWt_7xJ-ir0XzExnWh-
   quCicsuh_uJvpVWr1jKtEt7e0OCnfudnUL6ZEW6_grw9oCrkRb-
   JU6mktdWWJ4XtMmKYgedqNJP5LJ5t8U4NMyIyj_WPxk20rMGHW1_15LVZ_3ZsYFFj9PH0Jl7hX-0NqYYi6RB0YAeVnJsPdsRvznVzFQ_yP3
   ```

3. If an `id_token` was included in the authorization request, the application validates the `id_token` returned.

   For more information, see the OpendID Connect Core 1.0 specifications.

4. If a `token` (access token) was included in the authorization request, the application can also optionally validate the access token returned.

Copyright © 2025 Ping Identity Corporation

Use the PingOne for Enterprise introspection endpoint returned by the **Discovery URL**, `https://sso.connect.pingidentity.com/sso/as/introspect.oauth2`, to validate the access token.

For access tokens that are signed rather than encrypted, you can also use the JKWS URI returned by the **Discovery URL**, `https://sso.connect.pingidentity.com/sso/as/jwks`.

> **Note**
>
> You can see your access token settings at **Applications > My Applications > OAuth Settings**. For more information, see Configuring your OAuth settings.

OIDC application grant types

PingOne for Enterprise supports the following authorization grant types for OpenID Connect (OIDC) applications.

Grant Type	Application Availability	Description
Authorization Code	• Web App • Advanced Configuration	PingOne for Enterprise issues the application an authorization code in the response to the application's authorization request. The application then exchanges the authorization code with the PingOne for Enterprise token endpoint for an access token and ID token for the application.
Refresh Token	• Web App	Refresh tokens are available only when you're using the Authorization Code grant type. In this case, PingOne for Enterprise automatically exchanges a refresh token for a new access token if the access token expires. When you enable this grant type, the **Refresh Token** settings section displays.

Copyright © 2025 Ping Identity Corporation

Grant Type	Application Availability	Description
Authorization Code with PKCE	• Native App	Instead of using a client secret, Proof Key for Code Exchange (PKCE) embeds a code verifier that's transformed by the application and returned to PingOne for Enterprise in the authorization request. PingOne for Enterprise then issues the application an authorization code in the response. The application then exchanges the authorization code with the PingOne for Enterprise token endpoint for an access token and ID token for the application. For more information, see OAuth 2.0 RFC 7636.
Implicit	• Single Page App • Advanced Configuration	PingOne for Enterprise issues the application an access token, ID token or both in the response to the application's authorization request, depending on the `response_type` parameter values.
Authorization Code and Implicit	• Advanced Configuration	This is a hybrid grant type. Depending on the `response_type` parameter values.PingOne for Enterprise issues the application any or all of these in the response to the application's authorization request: • Authorization code • Access token • ID token

Assign advanced attribute mappings

About this task

You will want to use advanced attribute mapping when:

- Adding an application for your single sign-on (SSO) users, and one or more of the attributes for the application are different than the attributes used by the identity repository.
- Customizing PingOne dock settings and you want to change one or more of the default attributes used by the identity repository.

In both cases, use advanced attribute mapping if the standard attributes available in the dropdown listing for an attribute assignment do not meet your needs, and you want to use advanced mode to customize an attribute.

Copyright © 2025 Ping Identity Corporation

Advanced attribute mapping mode enables you to modify the mapping of an identity repository attribute to an application attribute, or to assign more than one identity repository attribute to an application attribute (so the needed attribute can be used without altering the existing mapping).

Steps

1. In advanced attribute mapping mode, you map additional identity repository attributes to the single application attribute. You can:

   Choose from:

   - Select an identity repository attribute from a drop-down list.
   - Enter an identity repository attribute.
   - Click the **As Literal** checkbox and enter a literal value to assign.

   For attributes that aren't literal values, you can select a transformation **Function** to apply to an attribute from the drop-down list. The following transformation functions are available:

   ### *FilterByRegularExpression*

   Apply a regular expression (regex) to the attribute value(s). Only values that match the regular expression are assigned to the attribute. For example, if you want the resulting value(s) to start with 'A' or 'b', use the regular expression '[Ab].*'.

   ### *ExtractByRegularExpression*

   Apply a regular expression (regex) to the attribute value(s). Any portion of a value that matches the regular expression is assigned to the attribute. For example, an incoming assertion uses `memberOf`, and you want only groups that match a specified list sent in the outgoing assertion. Assume the groups you want are A, B, C and D, and the incoming assertion contains the groups A, B, E, F in the memberOf attribute. In this case, your regular expression extracts only the group A and B values.

   ### *GetDomainPartFromEmail*

   Get the domain part from an email string. For example, get *foo.com* from "bob.smith@foo.com".

   ### *GetFirstRelativeDN*

   Get the first relative distinguished name (DN) from a DN string. For example, get *Bob Smith* from "CN=Bob Smith,OU=Sales,DC=Fabrikam,DC=com".

   ### *GetLocalPartFromEmail*

   Get the local part from an email string. For example, get *bob.smith* from "bob.smith@foo.com"

   ### *Hash*

   Apply a hashing algorithm to the attribute value. You will select the algorithm and the encoding format, choosing the settings from a dropdown list.

   For **Hashing Algorithm**, the options are:

   - MD5

Copyright © 2025 Ping Identity Corporation

- SHA-1
- SHA-256

For **Encoding Format**, the options are:

- hex
- base64

This setting is not available in the Attribute Mapping section on the **Dock > Configuration** page.

PickByFieldsFromJsonList

Pick the field values from a multivalued attribute that match the condition you specify. Each field value is a JSON object.

PickPrimaryObjectsByTypeFromJsonList

Pick the JSON object(s) from the list that have a `primary` field value of true, and a `type` field value equal to the condition value. If you do not specify a condition, the `type` value is ignored and all matching `primary` value objects are returned.

PickPrimaryValueByTypeFromJsonList

Pick the JSON object(s) `value` field values from the list, where the object's `primary` field value is true and the `type` field value matches the condition value. If you do not specify a condition, the `type` value is ignored and all matching `primary` value objects are returned.

Random

Assign a random value to the attribute. You will need to supply the character length to use. You can also select to apply a hashing algorithm and encoding format to the random value, choosing the settings from a dropdown list.

For **Hashing Algorithm**, the options are:

- None (default)
- MD5
- SHA-1
- SHA-256

For **Encoding Format**, the options are:

- None (default)
- hex
- base64

This setting is not available in the Attribute Mapping section on the **Dock > Configuration** page.

ToLowerCase

Change all characters to lowercase.

Copyright © 2025 Ping Identity Corporation

ToUpperCase

Change all characters to uppercase.

2. Click **Close Advanced** to save the attribute assignment.

Add or update an application using its SSO URL

Before you begin

If you have the SSO URL for an application that is not in the Application Catalog, you can connect to the application without using SAML. Typically, the application already exists in your organization, but it may be an application from a service provider (SP) if the SP supplies you the URL for the application.

About this task

You can then make the application available to your single sign-on (SSO) users.

> **Note**
>
> Applications you've made available using the SSO URL cannot be added to the authentication context in the PingOne authentication policy. However, if the SSO URL references an application configured for SSO in PingFederate, you can apply multi-factor authentication in PingFederate using a PingID advanced policy.

Steps

1. Go to **Applications > My Applications > SAML**.
2. Click **Add Application**.
3. On the Application Details page, enter the application details. **Application Name**, **Application Description** and **Category**are required fields. You can optionally assign an application icon. The icon file can be up to 5 Mb in size. The supported graphics formats are JPEG/JPG and PNG.
4. Click **Continue to Next Step**. The Application Configuration page is displayed.
5. On the Application Configuration page, click **I have the SSO URL** and enter the URL to use for SSO to the application.

   If the application is being supplied by an SP, the SP will need to supply the URL to you. We encode this URL, so do not encode it yourself (for example, by using `&` rather than `&`).

   If you are using Google as your identity bridge and adding a Google application, enter the URL for the application using this format:

   ```
   https://<application>.google.com/a/<GoogleAppsDomainName>
   ```

   Where *application* is the name of one of the Google applications, and *GoogleAppsDomainName* is the domain name assigned to your Google account.
6. Confirm that the SSO URL is correct. You can use the Single Sign-On link to test the URL. The application connection is established, and available on your PingOne dock.
7. Click **Finish** to complete the application setup.

Copyright © 2025 Ping Identity Corporation

The new application is added to your My Applications list for SAML. You can edit the application configuration as needed by clicking the right arrow icon then clicking **Edit**. Refer to this documentation when changing configuration values.

8. Make the new application available to your users.

   See Authorize group access to applications for instructions.

Add an application from the Application Catalog

The Application Catalog contains applications that service providers have made available through PingOne. You can configure these applications to make them available to your users.

About this task

For more detailed directions to configure the most popular catalog applications, see PingOne for Enterprise Application Catalog.

Steps

1. Go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for your application by typing the name, entity ID, or description of the application you want to add.
3. When you find the application you want, click the line of the application to expand the description.
4. Click **Setup** to begin. The SSO Instructions page for the application is displayed.
5. Follow the instructions to configure SSO for the application. Click **Continue to Next Step**.
6. Configure your connection to the application per the application instructions. Click **Continue to Next Step**.
7. To add a new attribute, click **Add New Attribute**.

   In most cases, the default attribute mappings are sufficient. These mappings assign your identity repository attributes to the attributes provided by the Service Provider for the application.

   For each application attribute, you can:

   1. Enter a value in the **Application Attribute** field
   2. Click the **Required** checkbox to designate an attribute or attributes as required by the application.
   3. In the **Identity Bridge Attribute or Literal Value** field, choose between:
      - Select an attribute from the drop down list.
      - Select **As Literal** and enter a literal value to assign.

      1. Click **Advanced** and enter Advanced Attribute Mapping mode.

         For more information, see Creating advanced attribute mappings

      2. Select the **Provisioning** checkbox to make this a provisioning attribute rather than an SSO attribute.

Copyright © 2025 Ping Identity Corporation

Custom provisioning attributes are currently only available for Aquera and Salesforce applications.

8. When you've finished modifying or adding any additional attributes, click **Continue to Next Step**.
9. **Optional:** Customize how the application appears in your dock.
    - Click **Select Image** to upload a new application icon image.
    - In the **Name** field, enter a new name for the application.
    - In the **Description** field, enter a new description for the application.
    - From the **Category** list, select the category to assign the application to.
    - Click **Continue to Next Step**.
10. Make the new application available to your users by assigning the groups authorized to use the application.

    All members of the selected group or groups will be able to use the application. When the application supports user provisioning, user provisioning to this application is also enabled for members of the assigned groups.

    For more information about group access, see Authorize group access to applications.

    1. For each group you want to grant access to the application, click **Add**.
    2. Click **Continue to Next Step**

       Result:

       The summary information for the application configuration is then displayed on a new page.
11. Review your configuration and click **Finish** to add the application to the PingOne Dock.

PingOne for Enterprise Application Catalog

The Application Catalog contains applications that service providers have made available through PingOne for Enterprise.

After selecting an application from the catalog, follow the configuration instructions to add the application and make it available to your users.

To begin, choose an application:

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise

A - D

- Achievers
- ADP Workforce
- Amazon Web Services
- Aquera
- Arena BOMControl
- Ariba
- Atlassian Cloud
- Bomgar
- Box
- Concur
- Cornerstone
- Coupa
- CylancePROTECT
- DocuSign
- Dropbox

E - P

- Egnyte
- Evernote
- Github.com
- Kronos
- Lucidchart
- Microsoft 365
- NetSuite
- New Relic
- PagerDuty

Copyright © 2025 Ping Identity Corporation

S - Z

- Salesforce
- ServiceNow
- ShareFile
- Slack
- Smartsheet
- SuccessFactors
- Ultimate Software
- WebEx
- Workday
- Workplace by Facebook
- Zendesk
- Zoom

Adding Achievers to Your PingOne for Enterprise Dock

Add the Achievers application your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Achievers** application line to expand it and click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. Send an email to your Achievers client success manager with the following information:
    - The signing certificate file you downloaded in step 2, attached to the email.
    - The entity ID, which is the **Issuer** URL.
    - The sign-on page URL, which is https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=*<your IdP ID>*, where *<your Idp ID>* is your **IdP ID** number.

Next steps

After your client success manager responds with the necessary information, click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Achievers Connection Configuration

Steps

1. Import the metadata for Achievers:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** and **Entity ID** fields, replace the *${programName}* and *${serverName}* variables with the information provided by your client success manager.
3. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
4. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
5. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
6. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Achiever.
7. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
8. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an activeSSO session.
9. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
10. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

11. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
12. Select the **Use Custom URL** checkbox to enter a customer URL to launch Achievers from the dock.

Next steps

Click **Continue to Next Step**.

Achievers Attribute Mapping

About this task

Copyright © 2025 Ping Identity Corporation

PingOne will automatically populate required SAML attributes.

For Achievers, the required attribute is `SAML_SUBJECT`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Achievers Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Achievers Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding ADP Workforce Now to Your PingOne for Enterprise Dock

Add the ADP Workforce Now application your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click on the **ADP Workforce Now** application line to expand it and click **Setup**.

Next steps

On the **SSO Instructions** tab, click **Continue to Next Step**.

ADP Workforce Now Connection Configuration

Steps

1. In the **ACS URL** field, enter the assertion consumer service (ACS) URL.

   > **Note**
   >
   > The default ACS URL is pre-populated, and should work for most ADP Workforce Now connections.

2. In the **Entity ID** field, enter the Entity ID.

   The default Entity ID is pre-populated, and should work for most ADP Workforce Now connections.

3. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).

Copyright © 2025 Ping Identity Corporation

The default URL is pre-populated, and should work for most ADP Workforce Now connections.

4. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
5. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
6. On the **Primary Verification Certificate** line, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses.
7. On the **Secondary Verification Certificate** line, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
8. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
9. Select the **Encrypt Assertion** box to encrypt outgoing SAML assertions.
10. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.
11. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
12. Select the **Use Custom URL**checkbox to enter a customer URL to launch ADP Workforce Now from the dock.

Next steps

Click **Continue to Next Step**.

ADP Workforce Now Attribute Mapping

About this task

PingOne will automatically add required SAML attributes.

For ADP Workforce Now, the required attributes are:

- `SAML_SUBJECT`. The identity bridge attribute is mapped by default.
- `PersonImmutableID`. Map the identity bridge attribute representing your employee ID.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

Copyright © 2025 Ping Identity Corporation

Choose from:

- To map to the application attribute: Enter or select a directory attribute.
- To assign to the application attribute: Select **As Literal**, then enter a literal value.

4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

ADP Workforce Now Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

ADP Workforce Now Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Copyright © 2025 Ping Identity Corporation

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

ADP Workforce Now SAML Connection

Steps

1. On the **Review Setup** tab, go to the **SAML Metadata** line and click **Download** to download the PingOne metadata.
2. Click **Finish** to complete your configuration and add ADP Workforce Now to your PingOne Dock.
3. Go to https://adpfedsso.adp.com and sign on using your ADP account credentials.
4. Follow the steps on the ADP site to upload the metadata file.
5. After your metadata has been uploaded, your ADP account representative will confirm that the setup is complete in the live environment and to advise on next steps.

Adding Amazon Web Services to Your PingOne for Enterprise Dock

Add the Amazon Web Services (AWS) application to your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the Amazon Web Services application line to expand it and then click **Setup**.
4. Sign on to your AWS administration account and go to the **Management Console**.
5. Click your user name, click**My Security Credentials**, and click to expand **Access Keys**.
6. Copy the **Access Key ID** and the **Access Key Secret** values.

   For more information about your access key ID and access key secret, see the related AWS documentation.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Amazon Web Services Connection Configuration

About this task

The **ACS URL** and **Entity ID** fields are populated with the correct values for Amazon Web Services (AWS).

All other fields are optional.

Steps

1. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
2. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
3. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
4. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Achiever.
5. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses in case the primary certificate fails.
6. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
7. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
8. On the **Signing** line:

   Choose from:

   - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
   - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.
9. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
10. Select the **Use Custom URL**checkbox to enter a customer URL to launch AWS from the dock.
11. Select the **Set Up Provisioning** checkbox to configure user provisioning to AWS.

Next steps

Click **Continue to Next Step**.

Amazon Web Services Provisioning

About this task

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If you don't need to set up user provisioning, proceed to Amazon Web Services Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Steps

1. In the AWS Management Console, go to **My Security Credentials**.
2. Expand the **Access keys** tab and click **Create New Access Key**.
3. When prompted, click **Show Access Key**.
4. Copy the **Access Key ID** and **Access Key Secret**.
5. In PingOne, click **Continue to Next Step** to open the **Application Configuration** tab.
6. On the **Application Configuration** tab, enter the credentials you copied in step 4 in the **accessKey** and **accessKeySecret** fields.

Next steps

Click **Continue to Next Step**.

Amazon Web Services Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

For Amazon Web Services, the required attributes are:

- `SAML_SUBJECT`
- `https://aws.amazon.com/SAML/Attributes/Role`
- If you selected **Set Up Provisioning**, `UserName(provisioning)`

Steps

1. For `SAML_SUBJECT`:
    1. In the **Identity Bridge Attribute or Literal Value** field, enter or select **Username**.
    2. Click **Advanced**.
    3. In the **Name ID Format to send to SP** field, enter or select **urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**.
    4. Click **Save**

Copyright © 2025 Ping Identity Corporation

2. For `https://aws.amazon.com/SAML/Attributes/Role`
    1. In the **Identity Bridge Attribute or Literal Value** field, select the attribute that matches `Role`.
    2. Click **Advanced**.
    3. In the **NameFormat** field, select **urn:oasis:names:tc:SAML:2.0:attrname-format:uri**.
    4. Click **Save**

    The expected format for this attribute is

    +

    ```
    arn:aws:iam::<account-number>:role/<role-name>,arn:aws:iam::<account-number>:saml-provider/
    <provider-name>
    ```

3. To add an additional optional attribute, click **Add new attribute**.
4. In the **Application Attribute** field, enter the attribute name as it appears in the application.
5. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

    Choose from:

    - Enter or select a directory attribute to map to the application attribute.
    - Select **As Literal**, then enter a literal value to assign to the application attribute.
6. To create advanced attribute mappings, click **Advanced**.

Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Amazon Web Services Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Amazon Web Services Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

Click **Continue to Next Step**.

Amazon Web Services SAML connection

About this task

After completing the Amazon Web Services configuration in the PingOne for Enterprise admin portal, you must authorize PingOne for Enterprise as a SAML provider in the AWS console.

Steps

1. In the PingOne for Enterprise admin console, on the **Review Setup** tab, click **Download** to download the **SAML Metadata** file.
2. Click **Finish** to add Amazon Web Services to your PingOne for Enterprise Dock.

Copyright © 2025 Ping Identity Corporation

3. In the AWS console, create a SAML provider.

   For information about creating a SAML provider in AWS, see Create a SAML identity provider in IAM in the AWS documentation.

4. In the AWS console, create a SAML role.

   For more information about creating a SAML role in AWS, see Create a role for a third-party identity provider in the AWS documentation.

Next steps

To configure AWS for multiple roles and accounts, see Configure Amazon Web Services SSO for multiple roles and accounts in the Ping Identity Knowledge Base.

Adding Aquera to Your PingOne for Enterprise Dock

Add the Aquera application your PingOne for Enterprise dock from the application catalog.

About this task

This application enables outbound provisioning to various services through Aquera. It can also be used to configure SSO to the target service. See the configuration documentation for the target service for more information.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Aquera** application line to expand it and then click **Setup**.

Next steps

Click **Continue to Next Step**.

Aquera Connection Configuration

Steps

1. On the **Connection Configuration** form, select the **Set Up Provisioning** checkbox.

Next steps

Click **Continue to Next Step**.

Aquera Application Configuration

Before you begin

Copyright © 2025 Ping Identity Corporation

Before configuring the **Application Configuration** form, sign on to the Aquera admin console in a separate browser window.

Steps

1. In the Aquera admin console, go to **Applications**.
2. Click the application that you want to provision.
3. Copy the URL in the **Copy this URL** field.
4. In PingOne for Enterprise, paste the URL into the **SCIM_URL** field.
5. In Aquera, from the **Authorization** field, copy the bearer token.
6. In PingOne for Enterprise, paste the bearer token into the **ACCESS_TOKEN** field.
7. **Optional:** In the **BASIC_AUTH_USER** and **BASIC_AUTH_PASSWORD** fields, enter the credentials for the administrator account of the service you're provisioning.

   > **Note**
   >
   > If you enter and save both the access token and the basic authorization credentials, only the access token is saved and used to authenticate.

8. From the **REMOVE_ACTION** list, select the action you want Aquera to take when you delete or disable a user in PingOne for Enterprise.

   Choose from:

   - Select **Disable** to have Aquera disable a user that you've disabled or deleted in PingOne for Enterprise.
   - Select **Delete** to have Aquera delete a user that you've disabled deleted in PingOne for Enterprise.

Next steps

Click **Continue to Next Step**.

Aquera Attribute Mapping

About this task

For Aquera, the required attributes are `SAML_SUBJECT` and `userName`.

If you want to add additional attributes, Aquera supports provisioning for standard System for Cross-domain Identity Management (SCIM) attributes. For a list of SCIM attributes, see Supported attributes reference.

Aquera also supports custom provisioning attributes. When creating a custom attribute, use the `IANUser` prefix. For example, if you want to create a custom attribute for office location, call it `IANUser:officeLocation` and map it to `IANUser:officeLocation`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.

Copyright © 2025 Ping Identity Corporation

2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. For custom attributes, select the **Provisioning** checkbox.
4. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - Enter or select a directory attribute to map to the application attribute.
   - Select **As Literal**, then enter a literal value to assign to the application attribute.
5. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Aquera Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Aquera Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne for Enterprise Dock.

Adding Arena BOMControl to Your PingOne for Enterprise Dock

Add the Arena BOMControl application your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Arena BOMControl** application line to expand it and then click **Setup**.
4. To enable cloud single sign-on (SSO), email Arena Sales.

> **Note**
> You can continue configuring this application for PingOne before your sales representative activates SSO.

Next steps

Click **Continue to Next Step**.

Arena BOMControl Connection Configuration

About this task

Your Arena representative will configure your application connection based on your specific requirements.

Copyright © 2025 Ping Identity Corporation

Steps

- Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active single sign-on (SSO) session when they start this application.

Next steps

Click **Continue to Next Step**.

Arena BOMControl Attribute Mapping

About this task

For Arena BOMControl, the required attribute is `subject`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Arena BOMControl Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Arena BOMControl Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding Ariba to Your PingOne for Enterprise Dock

Add the Ariba application your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Ariba** application line to expand it and then click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. Send an email to your Ariba representative with the following information:
   - The signing certificate file you downloaded in step 3, attached to the email

Copyright © 2025 Ping Identity Corporation

- The **Issuer** URL
- The sign-on page URL, which is https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=*<your IdP ID>*, where *<your Idp ID>* is your **IdP ID** number.
- The logout URL where you would like to redirect users after they sign off of Ariba.

Next steps

After your client success manager responds with the necessary information, click **Continue to Next Step**.

Ariba Connection Configuration

About this task

Your Ariba representative will provide you with connection parameters for the **ACS URL** and **Entity ID** fields.

All other fields are optional.

Steps

1. Import the metadata for Ariba:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** and **Entity ID** fields, replace the *${parameter}* variables with the information provided by your Ariba representative.
3. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
4. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
5. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
6. On the **Primary Verification Certificate** line, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses.
7. On the **Secondary Verification Certificate** line, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
8. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
9. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
10. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.

Copyright © 2025 Ping Identity Corporation

- Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

11. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
12. Select the **Use Custom URL** checkbox to enter a customer URL to launch Ariba from the dock.

Next steps

Click **Continue to Next Step**.

Ariba Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

For Ariba, the required attribute is `SAML_SUBJECT`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Ariba Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum

Copyright © 2025 Ping Identity Corporation

- 2 MB maximum file size

> **Note**
>
> Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Ariba Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding Atlassian Cloud to Your PingOne for Enterprise Dock

Add the Atlassian Cloud application to your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Atlassian Cloud** application line to expand it and click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. Sign on to Atlassian Cloud as an administrator

Copyright © 2025 Ping Identity Corporation

6. Go to **Security > SAML Single Sign-On**
7. Copy the **ACS URL** and **Entity ID** values.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Atlassian Cloud Connection Configuration

Steps

1. Import the metadata for Atlassian Cloud,

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.
2. In the **ACS URL** field, enter the assertion consumer service (ACS) URL.
3. In the **Entity ID** field, enter the Entity ID.
4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).

   The default URL is pre-populated, and should work for most Atlassian Cloud connections.
5. In the **Single Logout Endpoint** field, enter a URL for PingOne for Enterprise to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne for Enterprise to send SLO responses to.
7. On the **Primary Verification Certificate** line, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses.
8. On the **Secondary Verification Certificate** line, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** box to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne for Enterprise sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne for Enterprise sign responses to incoming SAML assertions.
12. In the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL**checkbox to enter a customer URL to launch Atlassian Cloud from the dock.

Copyright © 2025 Ping Identity Corporation

14. Select the **Set Up Provisioning** checkbox to configure provisioning to Atlassian Cloud.

Next steps

Click **Continue to Next Step**.

Atlassian Cloud Provisioning

About this task

> **Note**
>
> If you don't need to set up user provisioning, proceed to Atlassian Cloud Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Steps

{In Atlassian Cloud}

1. In Atlassian Cloud, go to **Directory > User Provisioning**.
2. Click **Create a Directory**.
3. In the **Directory** field, enter a name for your directory.
4. Copy your **Directory Base URL** and **API Key**.

{In PingOne for Enterprise}

1. Click **Continue to Next Step**.
2. In the **DIRECTORY_BASE_URL** field, enter the directory base URL.
3. In the **API_KEY** field, enter your API key.
4. In the **REMOVE_ACTION** list, select one of the following options:

   Choose from:

   - If you select **Disable**, a user you disable or delete in PingOne for Enterprise will be disabled in Atlassian Cloud.
   - If you select **Delete**, a user you disable or delete in PingOne for Enterprise will be deleted in Atlassian Cloud.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Atlassian Cloud Attribute Mapping

About this task

For Atlassian Cloud, the required attribute is `SAML_SUBJECT`.

If you want to add additional attributes, Atlassian Cloud supports provisioning for standard System for Cross-domain Identity Management (SCIM) attributes. For a list of SCIM attributes, see Supported attributes reference.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. For custom attributes, select the **Provisioning** checkbox.
4. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - Enter or select a directory attribute to map to the application attribute.
   - Select **As Literal**, then enter a literal value to assign to the application attribute.
5. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Atlassian Cloud Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.

Copyright © 2025 Ping Identity Corporation

- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Atlassian Cloud Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Atlassian Cloud SAML connection

Steps

1. In PingOne for Enterprise, on the **Review Setup** tab, click **Download** to download the signing certificate.
2. Copy the **Issuer** and **idpid** values.
3. Click **Finish** to add Atlassian Cloud to your PingOne for Enterprise Dock.
4. In Atlassian Cloud, go to **Security > Identity providers** and select your PingOne for Enterprise **Directory**.
5. Click **Set up SAML single sign-on**.
6. Enter your configuration information.
    1. In the **Identity provider Entity ID** field, enter the **Issuer** value.
    2. In the **Identity provider SSO URL** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<your idpid>`, where *<your idpid>* is the **idpid** value.
    3. In the **Public x509 Certificate** field, paste the text of the signing certificate you downloaded, including the `----BEGIN CERTIFICATE----` line.

Copyright © 2025 Ping Identity Corporation

7. Click **Save SAML configuration** to activate the connection to PingOne for Enterprise.

Adding Bomgar to Your PingOne for Enterprise Dock

Add the Bomgar application your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Bomgar** application line to expand it and then click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. In the Bomgar admin interface, go to **Users & Security > Security Providers > Add a SAML Provider**.
6. In the **Bomgar admin interface**:
    1. In the **Name** field, enter a name for the connection.
    2. Select the **Enabled** checkbox to activate the connection.
    3. In the **Entity ID** field, enter the **Issuer** value from the **SSO Instructions** tab in PingOne.
    4. In the **Single Sign-On Service URL** field, enter the **Initiate Single Sign-On URL** value from the **SSO Instructions** tab in PingOne.
    5. In the **Certificate** section, click **Choose File** and upload the signing certificate you downloaded previously.
7. In the Bomgar admin interface, click **Download Service Provider Metadata**.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Bomgar Connection Configuration

Steps

1. In PingOne for Enterprise, import the metadata for Bomgar:

    Choose from:

    - Click **Select File** to upload the metadata file.
    - Click **Or use URL** to enter the URL of the metadata.
2. In the **ACS URL** field, enter the value from the **Assertion Consumer Service URL** field in the Bomgar admin interface.
3. In the **Entity ID** field, enter the value from the **Entity ID** field in the Bomgar admin interface.
4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).

Copyright © 2025 Ping Identity Corporation

5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. On the **Primary Verification Certificate** line, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses.
8. On the **Secondary Verification Certificate** line, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an activeSSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.
12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Bomgar from the dock.

Next steps

Click **Continue to Next Step**.

Bomgar Attribute Mapping

About this task

PingOne for Enterprise will automatically populate requested SAML attributes.

For Bomgar, the populated attributes are:

- `SAML_SUBJECT`. Maps to a unique value.
    1. Click **Advanced**.
    2. From the **Name ID Format to send to SP** list, select **urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**.
    3. Click **Save** to apply this format.
- `Username`. Map to `Email`.
- `Email`. Map to `Email`.
- `FirstName`. Map to `FirstName`.
- `LastName`. Map to `Last Name`.

Copyright © 2025 Ping Identity Corporation

- `Groups`. Map to `memberOf`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Bomgar Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Bomgar Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Bomgar SAML connection

Steps

1. In PingOne for Enterprise, on the **Review Setup** tab, click **Download** to download the SAML metadata file.
2. Click **Finish** to add Bomgar to your PingOne Dock.
3. In the **Bomgar admin interface**, on the **Identity Provider Settings** tab, click **Choose File** and upload the PingOne metadata file.
4. Click **Save Changes** to activate the connection to PingOne.

Adding Box to Your PingOne for Enterprise Dock

Add the Box application your PingOne for Enterprise dock from the application catalog.

About this task

After you configure the Box application for the PingOne for Enterprise dock, you must email your Box representative with configuration and connection information.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Box** application line to expand it and click **Setup**.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Box Connection Configuration

About this task

PingOne for Enterprise automatically populates the values for the **ACS URL** and **Entity ID** fields. All other fields are optional.

For most configurations, the values on this tab should not change.

Steps

1. Import the metadata for Box:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, the value should be `https://sso.services.box.net/sp/ACS.saml2`.
3. In the **Entity ID** field, the value should be `box.net`.
4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
5. In the **Single Logout Endpoint** field, enter a URL for PingOne for Enterprise to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne for Enterprise to send SLO responses to.
7. On the **Primary Verification Certificate** line, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses.
8. On the **Secondary Verification Certificate** line, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne for Enterprise sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne for Enterprise sign responses to incoming SAML assertions.

12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Achievers from the dock.
14. Select the **Set Up Provisioning** checkbox to configure user provisioning to Box.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Box Provisioning

Before you begin

Ensure that popups are permitted in your browser.

About this task

> **Note**
>
> If you don't need to set up user provisioning, proceed to Box Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Steps

1. On the **Provisioning Instructions** tab, click **Continue to Next Step**.
2. **Optional:** On the **Application Configuration** tab, complete the following steps.
    1. Select the **CREATE_PERSONAL_FOLDERS** checkbox to create a new Box folder when a new user is created.
    2. In the **PARENT_FOLDER_ID** field, enter the ID of the folder where the new user folders will be created.

    > **Note**
    >
    > Find the ID of the desired parent folder by navigating to the Box web portal and copying the string at the end of the URL. For the folder located at https://myconnector.app.box.com/folder/1234567890, the folder ID would be 123456789.

The administrator account used to obtain the **Client ID** and **Client Secret** must be the owner of this folder.

1. From the **PERSONAL_FOLDER_PERMISSION_LEVELS** list, select the ownership and access permissions to apply to new user folders.
2. From the **REMOVE_ACTION** list, select the action to take when you disable or delete a user account in PingOne.
    - Select **Suspend** to suspend a deleted user's Box account.
    - Select **Delete** to delete a deleted user's Box account.
3. In the **DELETED_CONTENT_ACCOUNT** field, enter the email address to which the content of a deleted user's account will be transferred.
4. From the **FORCE_DELETE** list, select whether to delete users who own content.
    - **False** is the default option. Attempts to delete users who own content will fail.
    - **True** allows users who own content to be deleted.
        1. Click **Continue to Next Step**.
        2. Click **Activate**.

        Result:

Copyright © 2025 Ping Identity Corporation

The **Customer Log In** page appears in a pop-up window.

3. Enter your Box credentials and click **Authorize**.
4. Click **Grant Access to Box**.

   Result:

   You will be redirected to PingOne. The **Activate** button should now read **Activated**.

Next steps

Click **Continue to Next Step**.

Box Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

For Box, the required attribute is `SAML_SUBJECT`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Box Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

Copyright © 2025 Ping Identity Corporation

The image file must be:

- PNG, GIF, or JPG format
- 312 x 52 pixels maximum
- 2 MB maximum file size

> **Note**
>
> Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Box Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Box SAML connection

About this task
Steps

1. In PingOne, on the **Review Setup** tab, click **Download** to download the SAML metadata file.
2. Click **Finish** to add Box to your PingOne Dock.

Copyright © 2025 Ping Identity Corporation

3. Send an email to inform your Box representative that you want to enable SSO. Include the following information.
    - The SAML metadata file you downloaded, attached to the email.
    - Which SSO mode you want.
        - SSO Enabled allows users to sign on to Box using either their Box credentials or SAML SSO.
        - SSO Required requires users to sign on to Box using SSO.

Adding Concur to Your PingOne for Enterprise Dock

Add the Concur application your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Concur** application line to expand it and then click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the PingOne signing certificate.
5. Email Ping Identity at concursso@pingidentity.com. Include the following information in the email.
    - The signing certificate you downloaded, attached to the email.
    - The **Issuer** value.
    - The email address of your employee who is the primary point of contact for the Concur configuration.
    - A logout URL to direct users to when they log out of Concur.

Next steps

Click **Continue to Next Step**.

Concur Connection Configuration

Steps

1. Import the metadata for Concur:

   Choose from:

    - Click **Select File** to upload the metadata file.
    - Click **Or use URL** to enter the URL of the metadata.
2. In the **ACS URL** field, replace *$\{www or implementation}* with the information supplied by Ping.

   The **Entity ID** field is automatically populated. You should not need to change it. All other fields are optional.

Copyright © 2025 Ping Identity Corporation

3. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
4. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
5. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
6. On the **Primary Verification Certificate** line, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses.
7. On the **Secondary Verification Certificate** line, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
8. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an activeSSO session.
9. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
10. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.
11. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
12. Select the **Use Custom URL** checkbox to enter a customer URL to launch Concur from the dock.
13. Select the **Set Up Provisioning** checkbox to configure user provisioning to Concur.

Next steps

Click **Continue to Next Step**.

Concur Provisioning

Before you begin

Ensure that popups are permitted in your browser.

About this task

> **Note**
>
> If you don't need to set up user provisioning, proceed to Concur Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Steps

1. Sign on to Concur as a Web Services Administrator.
2. Go to **Administration > Web Services**.

Copyright © 2025 Ping Identity Corporation

3. Click **Enable Partner Application**.
4. Select **PingOne Provisioning** and click **Enable**.
5. In PingOne, click**Continue to Next Step**.
6. Click **Activate**.

   Result:

   The **Customer Log In** page appears in a pop-up window.
7. Enter your Concur credentials and click **Authorize**.
8. Click **Grant Access to Concur**.

   Result:

   You will be redirected to PingOne. The **Activate** button should now read **Activated**.

Next steps

Click **Continue to Next Step**.

Concur Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

For Concur, the required attribute is `SAML_SUBJECT`.

Enabling user provisioning creates additional required attributes, which are designated with asterisks (`\*`). We recommend literal mapping for these attributes.

> **Note**
>
> The `EmpID` attribute is unique to Concur and is required to complete user provisioning for this application. It is mapped to `Email` by default, but we recommend changing it.
> Click **Advanced**, and from the **Function** list, select **PickByFieldsFromJsonList**. In the **Expression** field, enter `\{"primary":true,"type":"work","targetField":"employeeID"}`

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.

Copyright © 2025 Ping Identity Corporation

- To assign to the application attribute: Select **As Literal**, then enter a literal value.

4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Concur Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Concur Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Copyright © 2025 Ping Identity Corporation

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding Cornerstone to Your PingOne for Enterprise Dock

Add the Cornerstone application your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Cornerstone** application line to expand it and then click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. Send an email to your Cornerstone representative with the following information:
    - The signing certificate file you downloaded in step 2, attached to the email.
    - The entity ID, which is the **Issuer** URL.

Next steps

After your client success manager responds with the necessary information, click **Continue to Next Step**.

Cornerstone Connection Configuration

About this task

Your Cornerstone representative will respond with your host name, which you will enter into the **ACS URL** and **Entity ID** fields. All other fields on this tab are optional.

Steps

1. Import the metadata for Cornerstone.

    Choose from:

    - Click **Select File** to upload the metadata file.
    - Click **Or use URL** to enter the URL of the metadata.

Copyright © 2025 Ping Identity Corporation

2. In the **ACS URL** and **Entity ID** fields, replace the *${host}* variables with the host name provided by your Cornerstone representative.
3. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
4. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
5. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
6. On the **Primary Verification Certificate** line, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses.
7. On the **Secondary Verification Certificate** line, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
8. Select the **Force Re-authentication**checkbox to require your identity bridge to re-authenticate users with an active SSO session.
9. Select the **Encrypt Assertion** box to encrypt outgoing SAML assertions.
10. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.
11. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
12. Select the **Use Custom URL** box to enter a customer URL to launch Achievers from the dock.

Next steps

Click **Continue to Next Step**.

Cornerstone Attribute Mapping

About this task

PingOne for Enterprise will automatically populate required SAML attributes.

For Cornerstone, the required attribute is `SAML_SUBJECT`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

Copyright © 2025 Ping Identity Corporation

Choose from:

- To map to the application attribute: Enter or select a directory attribute.
- To assign to the application attribute: Select **As Literal**, then enter a literal value.

4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Cornerstone Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Cornerstone Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Copyright © 2025 Ping Identity Corporation

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding Coupa to Your PingOne for Enterprise Dock

Add the Coupa application your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Coupa** application line to expand it and click **Setup**.
4. On the **SSO Instructions** page, click the **Download** link to download the PingOne for Enterprise signing certificate.

Next steps

Click **Continue to Next Step**.

Coupa Connection Configuration

About this task

PingOne for Enterprise automatically populates the values for the **ACS URL** and **Entity ID** fields. All other fields are optional.

Steps

1. Import the metadata for Coupa:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, make sure the value is `https://prdsso40.coupahost.com/sp/ACS.saml2`.
3. In the **Entity ID** field, make sure the value is `prdsso40.coupahost.com`.
4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).

Copyright © 2025 Ping Identity Corporation

5. In the **Single Logout Endpoint** field, enter a URL for PingOne for Enterprise to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne for Enterprise to send SLO responses to.
7. On the **Primary Verification Certificate** line, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses.
8. On the **Secondary Verification Certificate** line, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne for Enterprise sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne for Enterprise sign responses to incoming SAML assertions.
12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Coupa from the dock.
14. Select the **Set Up Provisioning** checkbox to configure user provisioning to Coupa.

Next steps

Click **Continue to Next Step**.

Coupa Provisioning

About this task

> **Note**
>
> If you don't need to set up user provisioning, proceed to Coupa Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection Configuration** tab:

Steps

1. On the **Provisioning Instructions** tab, click **Continue to Next Step** to proceed to the **Application Configuration** tab.
2. In the **COUPA_SUBDOMAIN** field, enter your Coupa subdomain.

   Your Coupa subdomain is the subdomain in the URL for your Coupa login.

   Example:

   https://<*subdomain*>.coupacloud.com

Copyright © 2025 Ping Identity Corporation

3. In the **API_KEY** field, enter the API key used to authenticate provisioning requests.

   To obtain your API key:

   1. Sign on to your Coupa account as an administrative user.
   2. Go to **Setup > API Keys**.
   3. Click **Create**.
   4. Complete the creation form and click **Create**.
   5. Copy the API key value and paste into the **API_KEY** field.

Next steps

Click **Continue to Next Step**.

Coupa Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

For Coupa, the required attribute is `SAML_SUBJECT`.

If you enabled provisioning, the required provisioning attributes are:

- `login`
- `email`
- `firstname`
- `lastname`

Provisioning creates and populates a number of optional attributes. Clear the **Identity Bridge Attribute** field for any attribute you don't intend to use.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.

4. To create advanced attribute mappings, click **Advanced**.

Copyright © 2025 Ping Identity Corporation

Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Coupa Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Coupa Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.

Copyright © 2025 Ping Identity Corporation

- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

Click **Continue to Next Step**.

Coupa SAML Connection

Steps

1. On the **Review Setup** tab, on the **SAML Metadata** line, click **Download** to download the metadata file.
2. Click **Finish** to add Coupa to your PingOne Dock.
3. Send an email to inform your Coupa representative that you want to enable SSO. Include the following information.
    - The SAML metadata file you downloaded, attached to the email.
    - A login URL. The login URL should be in the following format.

      ```
      https://prdsso40.coupahost.com/sp/startSSO.ping?PartnerIdpId=<Issuer>&TARGET=https://
      <your_site>.coupahost.com/sessions/saml_post
      ```

        - Replace <*Issuer*> with the **Issuer** value on the **Review Setup** tab.
        - Replace <*your_site*> with the complete URL of your site as registered at Coupa.
    - A logout page URL. Consider using the PingOne dashboard URL, which you can find in the **Configure Single Sign-on** box on your PingOne Dashboard.
    - Test user. Coupa needs a test user name and password to test SSO functionality.
4. Sign on to Coupa.
5. Go to **Setup > Company Setup > Security Controls**.
    1. Check the **Log in using SAML** checkbox.
    2. In the **Login Page URL** field, enter the login URL that you emailed to your Coupa representative.
    3. In the **Logout Page URL** field, enter the logout page URL that you emailed to your Coupa representative.
    4. In the **Timeout URL**, enter the same URL as the **Logout Page URL**.
    5. In the **Certificate** field, upload the signing certificate that you downloaded in Adding Coupa to Your PingOne for Enterprise Dock.
6. Save your configuration in Coupa.

Adding CylancePROTECT to Your PingOne for Enterprise Dock

Add the CylancePROTECT application your PingOne for Enterprise dock from the application catalog.

Copyright © 2025 Ping Identity Corporation

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **CylancePROTECT** application line for your region to expand it and then click **Setup**.
4. On the **Signing Certificate** line, click **Download**.
5. In a separate tab or window, sign on to the CylancePROTECT console.
6. In CylancePROTECT, Go to **Settings > Application**.
7. From the **Provider** list, select **PingOne**.
8. Open the signing certificate file you downloaded in step 4 in a plain text editor.
9. Copy the contents of the signing certificate and, in CylancePROTECT, paste the contents into the **X.509 Certificate** field.
10. In the **Login URL** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<IdP ID>`, where *<IdP ID>* is the value of the **IdP ID** line on the PingOne **SSO Instructions** tab.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

CylancePROTECT Connection Configuration

About this task

The pre-populated values for the **ACS URL**, **Entity ID**, and **Target Resource** fields will work for most configurations.

All other fields are optional.

Steps

1. Import the metadata for CylancePROTECT:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** and **Entity ID** fields, replace the *${programName}* and *${serverName}* variables with the information provided by your client success manager.
3. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
4. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
5. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.

Copyright © 2025 Ping Identity Corporation

6. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from CylancePROTECT.
7. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
8. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
9. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
10. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.
11. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
12. Select the **Use Custom URL** checkbox to enter a customer URL to launch CylancePROTECT from the dock.

Next steps

Click **Continue to Next Step**.

CylancePROTECT Attribute Mapping

About this task

PingOne will automatically populate the required SAML attributes.

For CylancePROTECT, the required attribute is `SAML_SUBJECT`, which you should map to `Email (Work)`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

    Choose from:

    - To map to the application attribute: Enter or select a directory attribute.
    - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

    Learn more in Creating advanced attribute mappings.

Next steps

Copyright © 2025 Ping Identity Corporation

Click **Continue to Next Step**.

CylancePROTECT Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

CylancePROTECT Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

Copyright © 2025 Ping Identity Corporation

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding DocuSign to Your PingOne for Enterprise Dock

Add the DocuSign application your PingOne for Enterprise dock from the application catalog.

About this task

For more information about configuring an identity provider for DocuSign, see Set Up an Identity Provider in the DocuSign documentation.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **DocuSign 2.0 - Production** application line to expand it and then click **Setup**.

Next steps

Click **Continue to Next Step**.

Docusign Connection Configuration

Steps

1. Import the metadata for DocuSign:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. **Required:** In the **ACS URL** and **Entity ID** fields, replace the *${customer-organization-ID-goes-here}* variable with the value in your DocuSign account.
3. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
4. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
5. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
6. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from DocuSign.
7. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
8. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.

Copyright © 2025 Ping Identity Corporation

9. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
10. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.
11. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
12. Select the **Use Custom URL** checkbox to enter a customer URL to launch DocuSign from the dock.

Next steps

Click **Continue to Next Step**.

DocuSign Attribute Mapping

About this task

For DocuSign, the required attributes are:

- `SAML_SUBJECT` : Map to your username attribute.

  > **Note**
  >
  > On the **SAML_SUBJECT** line, click **Advanced**.
  > In the **Name ID Format to send to SP** list, select **urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**.
  > Click **Save**.

- `emailaddress` : Map to your email attribute. This can be the same as your username attribute.
- `givenname` : Map to your first name attribute.
- `surname` : Map to your last name attribute.

DocuSign also creates two optional attributes.

- `accountid` : Map to your account ID attribute.
- `permissionprofileid` : Map to your permission profile id, for example `memberof` .

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

Copyright © 2025 Ping Identity Corporation

Choose from:

- To map to the application attribute: Enter or select a directory attribute.
- To assign to the application attribute: Select **As Literal**, then enter a literal value.

4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

DocuSign Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

DocuSign Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Copyright © 2025 Ping Identity Corporation

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

DocuSign SAML connection

About this task

Keep the PingOne for Enterprise **Review Setup** tab open. You will need values from the **Review Setup** tab to complete your configuration in DocuSign.

Steps

1. In a separate tab or window, sign on to the DocuSign administrative console.
2. From the DocuSign dashboard, click **Identity Providers**, then click **Add Identity Provider**.
3. In the **Identity Provider Settings** form, enter the following information:

Field	Value
Name	Enter a name for this connection.
Identity Provider Issuer	**Issuer**
Identity Provider Login URL	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<idpid>` Replace <*idpid*> with the **idpid** value.
Optional: **Identity Provider Logout URL**	**Single Logout Endpoint**
Optional: **Identity Provider Metadata URL**	**SAML Metadata URL**

4. In PingOne for Enterprise, click **Download** to download the **Signing Certificate**.
5. In DocuSign, click **Add Certificate** and upload the PingOne for Enterprise signing certificate you downloaded.
6. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Adding Dropbox to Your PingOne for Enterprise Dock

Add the Dropbox application to your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Dropbox** application line to expand it and then click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the PingOne for Enterprise signing certificate.
5. In a new tab or window, sign on to the Dropbox admin console.
6. Go to **Settings > Single Sign-On** and select the **Enable single sign-on** checkbox.
7. From the **Single sign-on** list, select one of the following:

   Choose from:

   - **Optional** allows users to authenticate using either their single sign-on (SSO) credentials or their Dropbox account.
   - **Required** forces users to authenticate using SSO.
8. On the **Identity provider sign-in URL** line, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<IdP ID>`, where *<IdP ID>* is the **IdP ID** value on the **SSO Instructions** in PingOne.
9. **Optional:** On the **Identity provider sign-out URL** line, enter `https://sso.connect.pingidentity.com/sso/SLO.saml2`.
10. On the **X.509 certificate** line, upload the PingOne for Enterprise signing certificate that you downloaded in step 4.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Dropbox Connection Configuration

About this task

PingOne automatically populates the values for the required **ACS URL** and **Entity ID** fields.

All other fields are optional.

Steps

1. Import the metadata for Dropbox:

   Choose from:

   - Click **Select File** to upload the metadata file.

Copyright © 2025 Ping Identity Corporation

- Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, enter the ACS URL.

   The pre-populated value for this field should work for most configurations.

3. In the **Entity ID** field, enter an entity ID.

   The pre-populated value for this field should work for most configurations.

4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Dropbox.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Dropbox from the dock.
14. Select the **Set Up Provisioning** checkbox to configure user provisioning to Dropbox.

Next steps

Click **Continue to Next Step**.

Dropbox Provisioning

Before you begin

Ensure that popups are permitted in your browser.

About this task

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If you don't need to set up user provisioning, proceed to Dropbox Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Steps

1. In PingOne, click**Continue to Next Step**.
2. Click **Activate**.

   Result:

   The **Customer Log In** page appears in a pop-up window.
3. Sign on to the Dropbox admin console.
4. Click **Allow**.

Next steps

Click **Continue to Next Step**.

Dropbox Attribute Mapping

About this task

PingOne will automatically populate the required SAML attributes.

For Dropbox, the required attribute is `SAML_SUBJECT`. Map it to an attribute that matches the Dropbox username. Click **Advanced** and from the **Name ID Format to send to SP** list, select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Dropbox Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Dropbox Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne dock.

Copyright © 2025 Ping Identity Corporation

Adding Egnyte to Your PingOne for Enterprise Dock

Add the Egnyte application your PingOne for Enterprise Dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Egnyte** application line to expand it and click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. In a separate tab or window, sign on to your Egnyte domain.
6. In Egnyte, go to **Settings > External Authentication > SAML (SSO)**.
7. Select the **Enable SAML (SSO)** checkbox.

   Result:

   Egnyte presents a SAML connection form.
8. From the **IdP Name** list, select **PingIdentity**.
9. In the **IdP Account Name** field, enter your Egnyte account name.

   Do not include the ".egnyte.com" part of your account name.
10. In the **IdP Target URL** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<IdP ID>`, where *<IdP ID>* is the **IdP ID** value from the **SSO Instructions** tab in PingOne.
11. In the **IdP Issuer URL** field, enter the **Issuer** value from the **SSO Instructions** tab in PingOne.
12. In the **SAML Certificate** field, enter the signing certificate information.

    1. In a plain text editor, open the signing certificate you downloaded in step 4.
    2. Copy the text of the certificate.

    Do not copy theBegin CertificateorEnd Certificatelines.

    1. Paste the text into the **SAML Certificate** field.
13. From the **Default User Mapping** list, select **Email address**.
14. Click **Save**.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Egnyte Connection Configuration

Steps

1. Import the metadata for Egnyte:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, replace *$\{your Egnyte domain}* with your Egnyte subdomain.
3. In the **Entity ID** field, enter the Egnyte entity ID.

   The pre-populated value for this field should work for most configurations.

4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Achiever.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Egnyte from the dock.
14. Select the **Set Up Provisioning** checkbox to configure user provisioning to Egnyte.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Egnyte Provisioning

Before you begin

Ensure that popups are permitted in your browser.

About this task

> **Note**
>
> If you don't need to set up user provisioning, proceed to Egnyte Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Steps

1. In PingOne, click **Continue to Next Step**.
2. In the **Subdomain** field, enter your Egnyte subdomain.
3. Click **Continue to Next Step**.
4. Click **Activate**.

   Result:

   The **Customer Log In** page appears in a pop-up window.
5. Sign on to the Egnyte admin console.
6. Click **Authorize**.

Next steps

Click **Continue to Next Step**.

Egnyte Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

For Egnyte, the required attribute is `SAML_SUBJECT`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

Copyright © 2025 Ping Identity Corporation

Choose from:

- To map to the application attribute: Enter or select a directory attribute.
- To assign to the application attribute: Select **As Literal**, then enter a literal value.

4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Egnyte Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Egnyte Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Copyright © 2025 Ping Identity Corporation

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding Evernote to Your PingOne for Enterprise Dock

Add the Evernote application your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Evernote** application line to expand it and click **Setup**.
4. On the **SSO Instructions** tab, click the **Download** link to download the PingOne for Enterprise signing certificate.
5. In a separate tab or window, sign on to the Evernote admin console.
6. In Evernote, go to **Authentication**.
7. In the **HTTP Endpoint**, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<IdP ID>`, where *<IdP ID>* is the**IdP ID** value from the **SSO Instructions** tab in PingOne for Enterprise.
8. Using a text editor, open the PingOne for Enterprise signing certificate you downloaded in step 4.
9. Copy the contents of the certificate and paste them into the **X.509 Certificate** field in Evernote.
10. Click **Save and Enable**.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Evernote Connection Configuration

Steps

1. Import the metadata for Evernote:

   Choose from:

   - Click **Select File** to upload the metadata file.

Copyright © 2025 Ping Identity Corporation

- Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, enter the ACS URL.

   The pre-populated value for this field should work for most configurations.

3. In the **Entity ID** field, enter an entity ID.

   The pre-populated value for this field should work for most configurations.

4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Achiever.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Evernote from the dock.
14. Select the **Set Up Provisioning** checkbox to configure user provisioning to Evernote.

Next steps

Click **Continue to Next Step**.

Evernote Provisioning

About this task

> **Note**
>
> If you don't need to set up user provisioning, proceed to Dropbox Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Copyright © 2025 Ping Identity Corporation

Steps

1. In PingOne for Enterprise, click **Continue to Next Step** to proceed to the **Application Configuration** tab.
2. In the **BASE_URL** field, enter your Evernote base URL.

   The default value of `https://m1.svc.evernote.com/scim/v2/` should work for most configurations. If you use the SCIM 1.1 protocol, replace the *v2* in the base URL with *v1*.
3. Enter your Evernote bearer token.
    1. In Evernote, go to **Integrations** > **SCIM**.
    2. Click **Generate token**.
    3. Copy the bearer token value and paste it into the **BEARER_TOKEN** field in PingOne for Enterprise.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Evernote Attribute Mapping

About this task

PingOne will automatically populate the required SAML attributes.

For Evernote, the required attribute is `SAML_SUBJECT`. Map it to an attribute that matches the Evernote business email address. Click **Advanced** and from the **Name ID Format to send to SP** list, select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.

If you enabled provisioning, the required provisioning attributes are:

- `userName`: Evernote's unique identifier for the user. The expected format is `user@domain.com`. This attribute is mapped to `Email` by default.
- `displayName`: The user's name as it will be displayed. This attribute is mapped to `Display Name` by default.
- `externalID`: A string that identifies the resource in the provisioning client. This attribute is mapped to `externalID` by default.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

    - To map to the application attribute: Enter or select a directory attribute.
    - To assign to the application attribute: Select **As Literal**, then enter a literal value.

Copyright © 2025 Ping Identity Corporation

4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Evernote Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Evernote Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.

Copyright © 2025 Ping Identity Corporation

- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding Workplace by Facebook to Your PingOne for Enterprise Dock

Add the Workplace by Facebook application your PingOne for Enterprise Dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Workplace by Facebook** application line to expand it and click **Setup**.
4. On the **Signing Certificate** line, click **Download**.
5. In a separate tab or window, sign on to Workplace by Facebook as an administrator.
6. From the dashboard, go to **Settings > SSO Settings**.
7. From the **Allow users to login via** list, select **SSO only**.
8. In the **SAML URL** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<IdP ID>`, where *<IdP ID>* is the value of the **IdP ID** line on the PingOne for Enterprise **SSO Instructions** tab.
9. In the **SAML Issuer URI** field, enter the **Issuer** value from the PingOne for Enterprise **SSO Instructions** tab.
10. Using a text editor, open the PingOne for Enterprise signing certificate you downloaded in step 4.
11. Copy the contents of the certificate and paste them into the **SAML Certificate** field in Workplace by Facebook.
12. Click **Test SSO** to confirm that the SSO connection is successful.
13. Click **Save**.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Workplace by Facebook Connection Configuration

Steps

1. Import the metadata for Workplace by Facebook:

   Choose from:

   - Click **Select File** to upload the metadata file.

Copyright © 2025 Ping Identity Corporation

- Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, replace *${company_subdomain}* with your company subdomain.
3. In the **Entity ID** field, replace *${companyid}* with your company ID.
4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Achiever.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Workplace by Facebook from the dock.

Next steps

Click **Continue to Next Step**.

Workplace by Facebook Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

For Workplace by Facebook, the required attribute is `SAML_SUBJECT`. Map it to an attribute that matches the `userName` attribute. Click **Advanced** and from the **Name ID Format to send to SP** list, select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.

Copyright © 2025 Ping Identity Corporation

3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.

4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Workplace by Facebook Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Workplace by Facebook Group Access

About this task

Copyright © 2025 Ping Identity Corporation

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding Github.com to Your PingOne for Enterprise Dock

Add the Github.com application your PingOne for Enterprise Dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Github.com** application line to expand it and then click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. In a separate tab or window, sign on to the Github.com admin portal.
6. In the Github admin portal, click your profile photo, then go to **Enterprise Settings > Settings > Security**.
7. Under **SAML single sign-on**, select the **Enable SAML authentication** checkbox.
8. In Github, enter the following information.
    1. In the **Sign on URL** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<idpid>`, replacing *<idpid>* with the **IdP ID** value from PingOne for Enterprise.
    2. In the **Issuer** field, enter the **Issuer** value from PingOne for Enterprise.
    3. In a plain text editor, open the PingOne for Enterprise signing certificate you downloaded in Step 4.
    4. Copy the contents of the certificate (including the "Begin Certificate" and "End Certificate" lines) and paste it into the **Public certificate** field.
9. Click **Test SAML configuration**.
10. Click **Save**.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Github.com Connection Configuration

Steps

1. Import the metadata for Github:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, enter the **ACS URL** value from Github.

   The ACS URL will be in the format `https://<github hostname>/saml/consume`.

3. In the **Entity ID** field, enter the **SP Entity ID** value from Github.

   The entity ID will be in the format `https://<github hostname>`.

4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Github.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Github from the dock.
14. Select the **Set Up Provisioning** checkbox to configure user provisioning to Github.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Github.com Provisioning

Before you begin

Ensure that popups are permitted in your browser.

About this task

> **Note**
>
> If you don't need to set up user provisioning, proceed to Github.com Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Steps

1. In PingOne for Enterprise, click**Continue to Next Step**.
2. In the **BASE_URL** field, enter you base URL.

   The base URL format is `https://api.github.com/scim/v2/organizations/<organization name>`.

   For information on finding your organization name, see Accessing an organization in the Github documentation.
3. Generate and enter your OAuth access token.
   1. Obtain your Github client ID and client secret.

      For more information, see Obtain client ID and secret from GitHub.
   2. Go to the Ping OAuth Configuration Service and generate your access token.

   For more information about generating tokens, see Generate OAuth access tokens in the Ping documentation.
   1. In PingOne for Enterprise, in the **OAUTH_ACCESS_TOKEN** field, enter your access token.

Next steps

Click **Continue to Next Step**.

Github.com Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

For Github.com, the required attribute is `SAML_SUBJECT`. Map this to the email address attribute.

If you enabled provisioning, the required provisioning attributes are:

- `userName`: Github's unique identifier for the user. This attribute is mapped to `Email` by default.

Copyright © 2025 Ping Identity Corporation

- `workEmail`: This attribute is mapped to `Email` by default.
- `firstName`: This attribute is mapped to `First Name` by default.
- `lastName`: This attribute is mapped to `Last Name` by default.
- `externalID`: A string that identifies the resource in the provisioning client. This attribute is mapped to `externalID` by default.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Github.com Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

Copyright © 2025 Ping Identity Corporation

Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Github.com Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding Kronos Workforce to Your PingOne for Enterprise Dock

Add the Kronos Workforce application your PingOne for Enterprise Dock from the application catalog.

About this task

The PingOne for Enterprise Dock supports both Kronos Workforce Central and Kronos Workforce Ready. The configuration instructions are the same for both applications.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the appropriate Kronos Workforce application line to expand it and click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. In a separate tabs or window, sign on to your Kronos account.
6. In Kronos, go to **Company Settings > Global Setup > Company Setup > Login Config**.
7. Select the **Enable SSO** checkbox.

Copyright © 2025 Ping Identity Corporation

8. In Kronos, enter the following information.
    1. In the **Redirect URL** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<IdP ID>`, replacing *<IdP ID>* with the **IdP ID** value in PingOne for Enterprise.
    2. In the **Entity ID of the Identity Provider** field, enter the **Issuer** value from PingOne for Enterprise.
    3. On the **Signing Certificate** line, upload the PingOne for Enterprise signing certificate you downloaded in step 4.
    4. Click **Save**.

Next steps

In PingOne for Enterprise, click**Continue to Next Step**.

Kronos Workforce Connection Configuration

Steps

1. Import the metadata for Kronos Workforce:

   Choose from:

    - Click **Select File** to upload the metadata file.
    - Click **Or use URL** to enter the URL of the metadata.
2. In the **ACS URL** field, replace the *${client-id}* variable with your client ID.
3. In the **Entity ID** field, enter your entity ID.

   The pre-populated value for this field should work for most configurations.
4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Achiever.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

Copyright © 2025 Ping Identity Corporation

Choose from:

- Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
- Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Kronos Workforce from the dock.

Next steps

Click **Continue to Next Step**.

Kronos Workforce Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

For Kronos Workforce, the required attribute is `SAML_SUBJECT`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Kronos Workforce Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

Copyright © 2025 Ping Identity Corporation

The image file must be:

- PNG, GIF, or JPG format
- 312 x 52 pixels maximum
- 2 MB maximum file size

> **Note**
> Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Kronos Workforce Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding Lucidchart to Your PingOne for Enterprise Dock

Add the Lucidchart application your PingOne for Enterprise Dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.

Copyright © 2025 Ping Identity Corporation

3. Click the **Lucidchart** application line to expand it and click **Setup**.

Next steps

Click **Continue to Next Step**.

Lucidchart Connection Configuration

Steps

1. Import the metadata for Lucidchart:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, replace the *${domain.name}* with your Lucidchart domain.
3. In the **Entity ID** field, enter your entity ID.

   The pre-populated value for this field should work for most configurations.

4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Lucidchart.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Lucidchart from the dock.
14. Select the **Set Up Provisioning** checkbox to configure user provisioning to Lucidchart.

Copyright © 2025 Ping Identity Corporation

Next steps

Click **Continue to Next Step**.

Lucidchart Provisioning

About this task

> **Note**
>
> If you don't need to set up user provisioning, proceed to Lucidchart Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Steps

1. Click **Continue to Next Step**.
2. Obtain your Lucidchart base URL and bearer token.
    1. In a separate tab or window, sign on to your Lucidchart account as an administrative user.
    2. In Lucidchart, go to **Team > App Integration > SCIM**.
    3. Click **Generate Token**.

       Result:

       Lucidchart will display your **Base URL** and **Bearer Token** values.
3. In PingOne, in the **BASE_URL** field, enter your Lucidchart base URL.
4. In the **BEARER_TOKEN** field, enter your bearer token value.
5. From the **REMOVE_ACTION** list, select the action Lucidchart will take when you delete or disable a user in PingOne.

   Choose from:

    - Select **Disable** to have Lucidchart disable a user that you have disabled or deleted in PingOne.
    - Select **Delete** to have Lucidchart delete a user that you have disabled deleted in PingOne.

Next steps

Click **Continue to Next Step**.

Lucidchart Attribute Mapping

About this task

Copyright © 2025 Ping Identity Corporation

PingOne will automatically populate required SAML attributes.

For Lucidchart, the following attributes are required for SSO:

- `SAML_SUBJECT`
- `User.FirstName`
- `User.Lastname`

If you enabled provisioning, the following attributes are required for provisioning:

- `userName`. This attribute cannot be changed once set.
- `workEmail`.
- `givenName`.
- `familyName`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Lucidchart Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Lucidchart Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

Click **Continue to Next Step**.

Lucidchart SAML Connection

About this task

For more information about establishing a SAML connection to Lucidchart, see SAML Overview in the Lucid Help Center documentation.

Steps

1. On the **Review Setup** tab, go to the **SAML Metadata** line and click **Download** to download the PingOne for Enterprise metadata.
2. Sign on to Lucidchart as an administrative user.

Copyright © 2025 Ping Identity Corporation

3. Go to **Team > Admin > App Integration > SAML**.
4. Select the **Enable SAML** checkbox.
5. Under **Lucidchart Sign In URL**, in the **Domain** field, enter your Lucidchart account domain.
6. Under **Identity Providers**, click **Add Identity Provider**.
7. In a plain text editor, open the PingOne for Enterprise metadata file you downloaded in step 1.
8. Copy the contents of the metadata file, and paste it into the **Identity Provider Metadata** field.
9. In the **Identity Provider Name**, enter a name for the connection.
10. From the **Product** list, select **Lucidchart**.
11. Click **Add Provider**.
12. Under **Download Service Provider Metadata**, click **Save Changes**.
13. In PingOne for Enterprise, click **Finish** to complete your configuration and add Lucidchart to your PingOne for Enterprise Dock.

Adding Microsoft 365 to your PingOne for Enterprise Dock

Add Microsoft 365 to your PingOne for Enterprise Dock from the application catalog.

> **Important**
>
> If you use Azure Active Directory as your identity repository, you cannot integrate with Microsoft 365 through PingOne for Enterprise. This configuration creates a redirect loop where Azure and PingOne for Enterprise try to authenticate through one another.

PingOne for Enterprise support for Microsoft 365 depends on factors such as:

- The type of Microsoft 365 client you want to use
- The identity repository you've configured for PingOne for Enterprise

PingOne for Enterprise Support for Microsoft 365

Client	Support Level	Exceptions
Passive profile or browser-based logins. These logins use portal.office.com or login.microsoft.com.	Supported	None

Copyright © 2025 Ping Identity Corporation

Client	Support Level	Exceptions
Active Profile or thick clients. These logins use thick clients installed on servers, desktops, or mobile devices. Includes: • Word • Excel • Powerpoint • Outlook • SharePoint	Supported only when AD Connect is your identity repository. **Note** You must disable Integrated Windows Authentication (IWA) if you're using AD Connect without IIS. AD Connect without IIS does not support IWA with the Active Profile, and Office clients don't support forms-based authentication.	Not supported whenPingFederate or ADFS is your identity repository. If you use any identity provider (IdP) other than AD Connect, thick client logins are not supported.

Learn more in Connecting to an identity repository.

Microsoft 365 prerequisites

- Active Directory must be deployed and running with a functional level of mixed or native mode on:
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019 (Desktop only, not Core)
- You must configure Microsoft Azure Active Directory Module for Windows PowerShell to establish a federated trust between your IdP and Azure AD.

> **Note**
>
> For more information, see Connect to Microsoft 365 with PowerShell in the Microsoft documentation.

- You must install the required Microsoft cloud service subscription updates to make sure your users are running the latest version of Windows.

Preparing Active Directory for SSO

Steps

1. Run the Microsoft Readiness Toolkit.

Copyright © 2025 Ping Identity Corporation

This application inspects your Active Directory environment and reports whether you are ready to set up single sign-on (SSO). If not, it lists the changes that you need to make.

Learn more in Microsoft 365 Apps readiness dashboard in the Microsoft documentation.

2. Make sure that your user principal names (UPN) are assigned and properly formatted:
    - The UPN domain suffix must be under the domain you're going to use for SSO.
    - The domain that you want to federate must be registered as a public domain with a domain registrar or within your own public DNS servers.

      If your Active Directory domain name is not a public internet domain (for example, if it ends with the .local suffix), you must set UPNs with an internet domain suffix that can be registered publicly. This should be a domain that is familiar to your users, such as their email domain.

    For more information about creating UPNs, see Add UPN suffixes and update your users to them in the Microsoft documentation.

    - If you have already set up Active Directory synchronization, the users' UPN might not match their on-premises UPN defined in Active Directory.

      You can rename users' UPN using the Set-MsolUserPrincipleName cmdlet in the Microsoft Azure Active Directory Module for Windows PowerShell.

Configuring Microsoft 365 in PingOne for Enterprise

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Office 365** application line to expand it and click **Setup**.
4. On the **SSO Instructions** tab, click **Continue to Next Step**.
5. On the **Basic Information** tab:
    1. Copy the values for the following settings:
        - **Issuer URI**
        - **Passive Log On URI**
        - **Active Log On URI**
        - **Log Off URI**
        - **Metadata Exchange URI**
    2. Click **Download** to download the signing certificate.
    3. Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

6. On the **Connection Configuration** tab, select the **Force Re-authentication** checkbox to force users with an active single sign-on (SSO) session to reauthenticate before using Microsoft 365.

   Reauthentication ensures that active sessions don't cause problems with Microsoft 365 SSO.

Next steps

Click **Continue to Next Step**.

Microsoft 365 Connection Configuration

Before you begin

You must have an .onmicrosoft.com admin account to add a domain and configure DNS for Microsoft 365.

About this task

To add a domain to Microsoft 365 and configure domain federation:

Steps

1. In the Microsoft 365 Admin Center, go to **Settings** > **Domains**
2. Click **Add Domain**.
3. In the **Enter a domain you own** field, enter the name of your domain.
4. Click **Next**.
5. Choose a method to verify your ownership of the domain:

   Choose from:

   - Use Domain Connect to let Microsoft verify the domain.
   - Add a TXT record to your domain's website using the values supplied by Microsoft.
   - Upload a text file to your website's top-level folder.
6. Click **Verify**.
7. Configure the DNS records on the domain registrar for other services.

   > **Important**
   >
   > Do not make the new domain the primary domain for your Microsoft 365 account. Setting the new domain as the default domain causes an error when you use `Set-MsolDomainAuthentication` to set the domain as a federated domain.

   Learn more in Add a domain to Microsoft 365 in the Microsoft documentation.

   Result:

   You've added your domain. Now you're ready to configure federation.

Copyright © 2025 Ping Identity Corporation

8. At the PowerShell command line, enter `Connect-MsolService`.

   Result:

   PowerShell initiates a connection to Azure and opens an embedded browser window.

9. In the browser window, sign on to the Azure tenant with a Global Administrator account.

10. Run the following commands in the Azure AD PowerShell.

    > **Note**
    >
    > You can find the bolded values in the Microsoft 365 application configuration tab in PingOne for Enterprise.

    ```
    $dom = "<your domain name, such as example.com>"
    $BrandName = "<The name of your organization, such as Example Inc.>"
    $ActiveLogOn = "<The Active Log On URI value from PingOne for Enterprise>"
    $LogOnURl = "<The Passive Log On URI value from PingOne for Enterprise>"
    $LogOffUrl = "<The Log Off URI value from PingOne for Enterprise>"
    $MyURI = "<The Issuer URI value from PingOne for Enterprise>"
    $Metadata = "<The Metadata Exchange URI value from PingOne for Enterprise>"
    $MySigningCert = "<The Signing Certificate text from PingOne for Enterprise in base64 format>"
    Set-MsolDomainAuthentication `
    -DomainName $dom `
    -FederationBrandName $BrandName `
    -Authentication Federated `
    -PassiveLogOnUri $LogonUrl `
    -SigningCertificate $MySigningCert `
    -IssuerUri $MyURI `
    -LogOffUri $LogOffUrl `
    -MetadataExchangeUri $Metadata `
    -ActiveLofOnUri $ActiveLogOn `
    ```

    > **Important**
    >
    > When copying the base64-encoded signing certificate to enter into the MSOL cmdlet, make sure to remove any line breaks in the certificate text. Line breaks will cause errors when attempting to execute the commands.

11. Use the following commands to confirm domain federation settings:

    - **`Get-MsolDomain`**: check the status of domain federation.
    - **`Set-MsolDomainAuthentication`**: change the authentication type for a given domain.

      > **Note**
      >
      > For a complete list of commands, see MSOnline in the Microsoft documentation.

Microsoft 365 Attribute Mapping

About this task

Copyright © 2025 Ping Identity Corporation

PingOne automatically populates required SAML attributes.

For Microsoft 365, the required attributes are:

- `subject` : maps to the `userPrincipalName` Active Directory attribute.
- `guid` : maps to the `objectGUID` Active Directory attribute.

> **Note**
>
> Microsoft has updated the default `sourceAnchor` attribute to use `ms-DS-consistencyGUID` by default. To determine which option is best for your organization, see Azure AD Connect: Design concepts in the Microsoft documentation.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Microsoft 365 App Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

Copyright © 2025 Ping Identity Corporation

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Troubleshooting

If you did not download the signing certificate on the **Basic Information** tab, an error message will prevent you from proceeding.

Next steps

Click **Continue to Next Step**.

Microsoft 365 Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration. Click **Finish** to add the application to your PingOne Dock.

Adding NetSuite to Your PingOne for Enterprise Dock

Add the NetSuite application to your PingOne for Enterprise Dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **NetSuite** application line to expand it and click **Setup**.
4. In a new tab or window, sign on to NetSuite as an administrative user.
5. In NetSuite, go to **Setup > Company > Enable Features**.
6. On the **Enable Features** page, click **SuiteCloud**.

Copyright © 2025 Ping Identity Corporation

7. Under the **Manage Authentication** heading, select the **SAML Single Sign-on** checkbox.
8. On the **Netsuite Service Provider Metadata** line, click **Download**.

The file will provide you the values for the **ACS URL** and **Entity ID** fields in following steps.

1. In the **Logout Landing Page** field, enter `https://sso.connect.pingidentity.com/sso/terminatesession?page=<logout_url>`, replacing *<logout_url>* with the URL to redirect users to when they sign off from Netsuite.
2. On the **SAML v2 Identity Provider Metadata** line, click **Browse** to upload the PingOne for Enterprise metadata file.

   Download the PingOne for Enterprise metadata file from the **Review Setup** tab at the end of the application configuration process.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

NetSuite Connection Configuration

Steps

1. Import the metadata for NetSuite:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.
2. In the **ACS URL** field, enter the ACS URL value from the NetSuite service provider metadata file.
3. In the **Entity ID** field, enter the entity ID value from the NetSuite service provider metadata file.
4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from NetSuite.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

Copyright © 2025 Ping Identity Corporation

Choose from:

- Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
- Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch NetSuite from the dock.

Next steps

Click **Continue to Next Step**.

NetSuite Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

For NetSuite, the following attributes are required.

- `SAML_SUBJECT` : Map to the attribute that matches the username in NetSuite.
- `account` : Enter the NetSuite Account ID for your organization. Because this is a static value for your organizations, select the **As Literal** checkbox.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

NetSuite Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

NetSuite Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Copyright © 2025 Ping Identity Corporation

NetSuite SAML Connection

Steps

1. On the **Review Setup** tab, go to the **SAML Metadata** line and click **Download** to download the PingOne metadata.
2. Click **Finish** to complete your configuration and add NetSuite to your PingOne Dock.
3. In NetSuite, on the **SAML v2 Identity Provider Metadata** line, click **Browse** to upload the PingOne metadata file.
4. Click **Submit** to apply your configuration.

Adding New Relic to Your PingOne for Enterprise Dock

Add the New Relic application your PingOne for Enterprise Dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **New Relic** application line to expand it and click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. In a separate tab or window, sign on to your New Relic account as an administrative user.
6. In New Relic, go to **Account Settings > Integrations > Single Sign On > Configure**.
7. On the **Your SAML Identity Provider Certificate** line, click **Upload** to upload the signing certificate you downloaded in step 4.
8. In the **Your SAML Identity Provider Details** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<IdP ID>`, replacing *<IdP ID>* with your **IdP ID** value from PingOne.
9. On the **New Relic SAML Service Provider Details** line, copy the **Assertion Consumer Service URL** for use in a future step.
10. Click **Save My Changes**.
11. Click **Login With SAML** to test your settings.
12. After a successful test, click **Enable SSO**.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

New Relic Connection Configuration

Steps

1. Import the metadata for New Relic:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, enter the **Assertion Consumer Service URL** value that you copied previously.
3. In the **Entity ID** field, enter the entity ID value.

   The pre-populated value for this field should work for most configurations.

4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from New Relic.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch New Relic from the dock.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

New Relic Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

For New Relic, the required attribute is `SAML_SUBJECT`. Map it to an attribute that matches the user email address. Click **Advanced** and from the **Name ID Format to send to SP** list, select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

New Relic Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.

Copyright © 2025 Ping Identity Corporation

- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

New Relic Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding PagerDuty to Your PingOne for Enterprise Dock

Add the PagerDuty application your PingOne for Enterprise Dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **PagerDuty** application line to expand it and click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. In a separate tab or window, sign on to PagerDuty as the account owner.
6. In PagerDuty, go to **Account Settings > Single Sign-on**.
7. Enter the signing certificate:
    1. In a plain text editor, open the signing certificate you downloaded in step 4.
    2. Copy the contents of the certificate.
    3. In PagerDuty, in the **X.509 Certificate** field, paste the certificate contents, including the `Begin Certificate` and `End Certificate` lines.

Copyright © 2025 Ping Identity Corporation

8. In the **Login URL** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<IdP ID>`, replacing *<IdP ID>* with the **IdP ID** value from PingOne for Enterprise.
9. Select the **Turn on single sign-on** checkbox.
10. Select the **Allow username/password login** checkbox.

    Enable this option while testing your single sign-on (SSO) connection. After a successful test, you can disable it.
11. Click **Save Changes**.
12. Sign out of PagerDuty.
13. On the PagerDuty sign on page, click **Sign in with your Identity Provider**.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

PagerDuty Connection Configuration

Steps

1. Import the metadata for PagerDuty:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.
2. In the **ACS URL** and **Entity ID** fields, replace *${accountid}* with your PagerDuty account ID.
3. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated SSO.
4. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
5. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
6. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from PagerDuty.
7. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
8. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
9. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
10. On the **Signing** line:

Copyright © 2025 Ping Identity Corporation

Choose from:

- Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
- Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

11. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
12. Select the **Use Custom URL** checkbox to enter a customer URL to launch PagerDuty from the dock.

Next steps

Click **Continue to Next Step**.

PagerDuty Attribute Mapping

About this task

PingOne for Enterprise will automatically populate required SAML attributes.

For PagerDuty, the required attribute is `SAML_SUBJECT`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

PagerDuty Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

Copyright © 2025 Ping Identity Corporation

The image file must be:

- PNG, GIF, or JPG format
- 312 x 52 pixels maximum
- 2 MB maximum file size

> **Note**
> Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

PagerDuty Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding Salesforce to Your PingOne for Enterprise Dock

Add the Salesforce application your PingOne for Enterprise Dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.

Copyright © 2025 Ping Identity Corporation

3. Click the **Salesforce** application line to expand it, and then and click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. In a separate tab or window, sign on to the Salesforce admin portal.
6. In Salesforce, go to **Setup > Administer > Security Controls > Single Sign-On Settings**.
7. Select the **SAML Enabled** checkbox.
8. In the **Name** field, enter a name for the connection to PingOne.
9. In the **Issuer** field, enter the **Issuer** value from PingOne.
10. On the **Identity Provider Certificate** line, click **Browse** to upload the signing certificate you downloaded in step 4.
11. From the **SAML Identity Type** list, select **Assertion contains User's salesforce.com username**.
12. From the **SAML Identity Location** list, select **Identity is in the NameIdentifier element of the Subject Statement**.
13. In the **API Name** field, enter a unique name for the API.
14. In the **Entity ID** field, enter `https://saml.salesforce.com`

    If you have a Salesforce.com My Domain URL, you can enter it into this field instead.
15. **Optional:** In the **Identity Provier Login URL**, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<IdP ID>`, replacing *<IdP ID>* with the **IdP ID** value from PingOne.
16. **Optional:** In the **Identity provider Logout URL** field, enter `https://sso.connect.pingidentity.com/sso/terminatesession.aspx?page=https://www.salesforce.com`.
17. **Optional:** In the **Custom Error URL**, enter a URL to redirect users to when an error occurs.

    If your identity bridge is AD Connect with IIS, you can enter `https://<AD Connect IIS Server URL>/ADconnect/error.aspx`.
18. Click **Save**.

> **Note**
>
> Keep the Salesforce tab open, as you will need values from it for the next steps.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Salesforce Connection Configuration

Steps

1. Import the metadata for Salesforce:

Copyright © 2025 Ping Identity Corporation

Choose from:

- Click **Select File** to upload the metadata file.
- Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, enter the **Salesforce Login URL** value from Salesforce.
3. In the **Entity ID** field, enter the **Entity ID** value from Salesforce.
4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Salesforce.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.
12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Salesforce from the dock.
14. Select the **Set Up Provisioning** checkbox to configure user provisioning to Salesforce.

Next steps

Click **Continue to Next Step**.

Salesforce Provisioning

Before you begin

Ensure that popups are permitted in your browser.

About this task

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If you don't need to set up user provisioning, proceed to Salesforce Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Steps

1. In PingOne, click **Continue to Next Step** to proceed to the **Application Configuration** tab.
2. Chose how Salesforce will deprovision:

   Choose from:

   - Select the **FREEZE_USER_FLAG** checkbox to freeze a deprovisioned user account.
   - Leave the checkbox clear to deactivate a deprovisioned user account.
3. In the **SUBDOMAIN** field, your Salesforce subdomain

   Example:

   If your Salesforce URL is `example.my.salesforce.com`, your subdomain is `example.my`.
4. From the **PERMISSION_SET_MANAGEMENT** list, select how to handle permission sets provisioned from PingOne to Salesforce:

   Choose from:

   - Select **Merge with permission sets in Salesforce** to add provisioned PingOne user permissions to existing permission sets in Salesforce.
   - Select **Overwrite permission sets in Salesforce** to overwrite permissions in Salesforce with the provisioned permissions from PingOne.
5. Click **Continue to Next Step**.
6. On the **Connection Configuration** tab, click **Activate**.

   Result:

   PingOne opens the Salesforce sign-on page in a pop-up window.
7. Sign on to Salesforce as an administrative user.
8. Click **Allow**.

Next steps

In PingOne, click **Continue to Next Step**.

Salesforce Attribute Mapping

About this task

Copyright © 2025 Ping Identity Corporation

PingOne will automatically populate required SAML attributes.

For Salesforce, the required attribute is `SAML_SUBJECT`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Salesforce Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Salesforce Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding ServiceNow to Your PingOne for Enterprise Dock

Add the ServiceNow application to your PingOne for Enterprise Dock from the application catalog.

Before you begin

To configure single sign-on (SSO) for ServiceNow, you must have the SAML 2.0 Single Sign-On plugin installed in your ServiceNow account. If this plugin is not yet installed, contact ServiceNow customer support.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **ServiceNow** application line to expand it and click **Setup**.
4. In a separate tab or window, sign on to your ServiceNow account as an administrative user.
5. In ServiceNow, go to **SAML 2.0 Single Sign-On > Properties**.
6. On the **Enable External Authentication** line, click **Yes**.
7. In the **Identity Provider URL which will issue the SAML2 Security token with user info** field, enter the **Issuer** value from PingOne for Enterprise.
8. In the **The base URL to the Identity Provider's AuthnRequest service. The AuthnRequest will be posted to this URL as the SAMLRequest parameter** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<IdP ID>`, replacing *<IdP ID>* with the **IdP ID** value from PingOne.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

ServiceNow Connection Configuration

Steps

1. Import the metadata for ServiceNow:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, enter the **The URL to the ServiceNow instance homepage** value from ServiceNow.
3. In the **Entity ID** field, enter the **The entity identification, or the issuer** value from ServiceNow.
4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single SSO.
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from ServiceNow.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch ServiceNow from the dock.
14. Select the **Set Up Provisioning** checkbox to configure user provisioning to ServiceNow.

Next steps

In PingOne, click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

ServiceNow Provisioning

Before you begin

Ensure that popups are permitted in your browser.

About this task

> **Note**
>
> If you don't need to set up user provisioning, proceed to ServiceNow Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Steps

1. In PingOne, click**Continue to Next Step** to proceed to the **Application Configuration** tab.
2. Install the Ping Identity Provisioning Solution application.

   For more information, see Adding the Ping Identity provisioning role in ServiceNow.
3. Create a provisioning user.

   Learn more in Creating a provisioning user in ServiceNow.
4. In PingOne, in the **Administrator_Username** field, enter the username for the provisioning user.
5. In the **Administrator_Password** field, enter the password for the provisioning user.
6. In the **ServiceNow_URL** field, enter the full URL of your ServiceNow instance.

   Example:`https://<yourinstance>.servicenow.com`

Next steps

Click **Continue to Next Step**.

ServiceNow Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

For ServiceNow, the required attribute is `SAML_SUBJECT`.

If you enabled provisioning, the required provisioning attribute is `Username`. All other provisioning attributes are optional.

Steps

1. To add an additional optional attribute, click **Add new attribute**.

Copyright © 2025 Ping Identity Corporation

2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

ServiceNow Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

ServiceNow Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

ServiceNow SAML Connection

Steps

1. On the **Review Setup** tab, go to the **SAML Metadata** line and click **Download** to download the PingOne metadata.
2. Click **Finish** to complete your configuration and add ServiceNow to your PingOne Dock.
3. In ServiceNow, go to **SAML 2.0 Single Sign-On > Certificate**.
4. In the **Name** field, enter or select **SAML 2.0**.
5. From the **Format** list, select **PEM**.
6. In a plain text editor, open the PingOne metadata file.
7. Copy the contents of the metadata file and paste them into the **PEM Certificate** field.
8. Click **Save**.

Adding ShareFile to Your PingOne for Enterprise Dock

Add the ShareFile application to your PingOne for Enterprise Dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **ShareFile** application line to expand it and click **Setup**.

Copyright © 2025 Ping Identity Corporation

4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. In a separate tab or window, sign on to ShareFile as an administrative user.
6. In ShareFile, go to **Admin > Configure Single Sign-On**.
7. Select the **Enable SAML** checkbox.
8. In the **Your Issuer/Entity ID** field, enter the **Issuer** value from PingOne for Enterprise.
9. In the **Sharefile Issuer/Entity ID** field, enter `https//<subdomain>.sharefile.com/saml/info`, replacing *<subdomain>* with your Sharefile subdomain.
10. In a plain text editor, open the signing certificate you downloaded in step 4.
11. Copy the contents of the certificate, and paste them into the **X.509 Certificate** field.
12. In the **Login URL** field, enter the **Initiate Single Sign-On URL** value from PingOne for Enterprise.
13. In the **Logout URL** field, enter a URL to redirect users to when they sign off from ShareFile.

    Consider the **PingOne Dock URL**, which you can find at **Setup > Dock**.
14. Click **Save**.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

ShareFile Connection Configuration

Steps

1. Import the metadata for ShareFile:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.
2. In the **ACS URL** and **Entity ID** fields, replace *${mydomain}* with your ShareFile subdomain.
3. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
4. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
5. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
6. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from ShareFile.
7. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.

Copyright © 2025 Ping Identity Corporation

8. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
9. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
10. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.
11. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
12. Select the **Use Custom URL** checkbox to enter a customer URL to launch ShareFile from the dock.

Next steps

Click **Continue to Next Step**.

ShareFile Attribute Mapping

About this task

PingOne for Enterprise will automatically populate required SAML attributes.

For ShareFile, the required attribute is `SAML_SUBJECT`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

    Choose from:

    - To map to the application attribute: Enter or select a directory attribute.
    - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

    Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

ShareFile Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

ShareFile Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Copyright © 2025 Ping Identity Corporation

Adding Slack to Your PingOne for Enterprise Dock

Add the Slack application to your PingOne for Enterprise Dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Slack** application line to expand it, and then click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. In a separate tab or window, go to slack.com/admin and sign on to your Slack account as a team owner.
6. In Slack, go to **Menu > Authentication > SAML authentication > Configure**.
7. From the **SAML provider** list, select **Custom SAML 2.0**.
8. In the **SAML SSO URL** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<IdP ID>`, replacing *<IdP ID>* with the **IdP ID** field from PingOne.
9. Enter the PingOne for Enterprise signing certificate:
    1. In a plain text editor, open the PingOne for Enterprise signing certificate you downloaded in step 4.
    2. Copy the contents of the certificate.
    3. In Slack, paste the copied certificate contents into the **X.509 Certificate** field.
10. On the **Settings** line, click the button to set single sign-on (SSO) requirements.

    Choose from:

    - **Required**
    - **Partially Required**
    - **Optional**

    If your users include restricted or single-channel guest accounts, select **Partially Required**.
11. Click **Save Configuration**.

Result

Slack will send a confirmation email to all users, prompting them to connect their Slack accounts to their single sign-on (SSO) accounts. After they confirm, they will be able to SSO into Slack.

Next steps

In PingOne, click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Slack Connection Configuration

Steps

1. Import the metadata for Slack:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, replace the *${teamname}* variable with your Slack subdomain.
3. In the **Entity ID** field, enter the entity ID.

   The default value of `https://slack.com` should work for most configurations.

4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated SSO.
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Slack.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Slack from the dock.
14. Select the **Set Up Provisioning** checkbox to configure user provisioning to Slack.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Slack Provisioning

Before you begin

Ensure that popups are permitted in your browser.

About this task

> **Note**
>
> If you don't need to set up user provisioning, proceed to Slack Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Steps

1. In PingOne, click**Continue to Next Step**.
2. Click **Activate**.

   Result:

   The **Customer Log In** page appears in a pop-up window.
3. On the **Customer Log In**, page, enter your team name and sign on to the Slack admin console.
4. Click **Authorize**.

Next steps

In PingOne, click **Continue to Next Step**.

Slack Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

For Slack, the required attribute is `SAML_SUBJECT`. Map it to your email attribute. Click **Advanced** and from the **Name ID Format to send to SP** list, select **urn:oasis:names:tc:SAML:1.1:nameid-format:persistent**.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.

Copyright © 2025 Ping Identity Corporation

- To assign to the application attribute: Select **As Literal**, then enter a literal value.

4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Slack Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Slack Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Copyright © 2025 Ping Identity Corporation

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding Smartsheet to Your PingOne for Enterprise Dock

Add the Smartsheet application your PingOne for Enterprise Dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Smartsheet** application line to expand it, and then click **Setup**.

Next steps

On the **SSO Instruction** tab, click **Continue to Next Step**.

Smartsheet Connection Configuration

Steps

1. Import the metadata for Smartsheet:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

   Find your Smartsheet metadata URL at What You Need to Set Up Smartsheet with Your Identity Provider in the Smartsheet documentation.

2. In the **ACS URL** field, enter the Smartsheet ACS URL.

   The pre-populated value for this field should work for most configurations.

3. In the **Entity ID** field, enter the Smartsheet entity ID.

   The pre-populated value for this field should work for most configurations.

4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.

Copyright © 2025 Ping Identity Corporation

6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Smartsheet.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.
12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Smartsheet from the dock.

Next steps

Click **Continue to Next Step**.

Smartsheet Attribute Mapping

About this task

PingOne will automatically populate required SAML attributes.

Smartsheet requires two attributes:

- `SAML_SUBJECT`. Map to an attribute that matches user email address. Click **Advanced** and from the **Name ID Format to send to SP** list, select **urn:oasis:names:tc:SAML:1.1:nameid-format:persistent**.
- `emailaddress`. Map to email. Click **Advanced** and in the **NameFormat** field, enter `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.

Copyright © 2025 Ping Identity Corporation

- To assign to the application attribute: Select **As Literal**, then enter a literal value.

4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Smartsheet Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Smartsheet Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Copyright © 2025 Ping Identity Corporation

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

Click **Continue to Next Step**.

Smartsheet SAML Connection

Before you begin

Ensure that your Smartsheet account is an enterprise account.

Steps

1. On the **Review Setup** tab, go to the **SAML Metadata** line and click **Download** to download the PingOne metadata.
2. Click **Finish** to complete your configuration and add Smartsheet to your PingOne Dock.
3. In a separate tab or window, sign on to your Smartsheet account as an administrative user.
4. In Smartsheet, go to **Account > Account Admin > Security Controls**.
5. Under the **Authentication** heading, click **Edit**.
6. Click **Not Configured**.

   Result:

   Smartsheet opens the **SAML Administration** form.
7. Click **Add IdP**.
8. In the **IdP Nickname** field, enter a name for the connection.
9. Enter the PingOne metadata.
    1. In a plain text editor, open the PingOne metadata file you downloaded in step 1.
    2. Copy the contents of the file.
    3. In Smartsheet, paste the file contents into the **IdP Metadata** field.
10. Click **Save**.
11. Click **Activate**.

    Result:

    The **IdP Status** will change from **Inactive** to **Active, Default**

Copyright © 2025 Ping Identity Corporation

12. In the **Authentication** form, select the **SAML** checkbox to enable the SAML connection.
13. Click **Save**.

Adding SuccessFactors to Your PingOne for Enterprise Dock

Add the SuccessFactors application your PingOne for Enterprise Dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **SuccessFactors** application line to expand it, and then click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. Email your SuccessFactors representative requesting a single sign-on (SSO) connection. Include the following information in the email:
    - The **Issuer** value.
    - The SAML version you want to use. In most cases this is SAML 2.0.
    - The PingOne signing certificate you downloaded in step 4, attached to the email.

    In the email, request the following information from your SuccessFactors representative:
    - The assertion consumer service (ACS) URL
    - The target resource value

Next steps

After your SuccessFactors representative replies with the requested information, click **Continue to Next Step**.

SuccessFactors Connection Configuration

Steps

1. Import the metadata for SuccessFactors:

    Choose from:
    - Click **Select File** to upload the metadata file.
    - Click **Or use URL** to enter the URL of the metadata.
2. In the **ACS URL** field, enter ACS URL value supplied by your SuccessFactors representative.
3. In the **Entity ID** field, enter the entity ID.

    The pre-populated value for this field should work for most configurations.

Copyright © 2025 Ping Identity Corporation

4. In the **Target Resource** field, enter the target resource value supplied by your SuccessFactors representative.
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Achiever.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.
12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch SuccessFactors from the dock.

Next steps

Click **Continue to Next Step**.

SuccessFactors Attribute Mapping

About this task

PingOne for Enterprise will automatically populate required SAML attributes.

For SuccessFactors, the required attribute is `SAML_SUBJECT`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.

Copyright © 2025 Ping Identity Corporation

4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

SuccessFactors Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

SuccessFactors Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.

Copyright © 2025 Ping Identity Corporation

- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding Ultimate Software to Your PingOne for Enterprise Dock

Add UltiPro your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Ultimate Software** application line to expand it , and then click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the PingOne for Enterprise signing certificate.
5. Email Setupmanagement@ultimatesoftware.com with your company name to request a single sign-on (SSO) connection.

   Result:

   Ultimate Software will respond with the **ACS URL** and **Entity ID** values you will need in following steps.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**

Ultimate Software Connection Configuration

Steps

1. Import the metadata for Ultimate Software:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.
2. In the **ACS URL** and **Entity ID** fields, replace *${ultipro provided host}* with the values supplied by your Ultimate Software representative.
3. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated SSO.
4. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
5. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.

Copyright © 2025 Ping Identity Corporation

6. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Ultimate Software.
7. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
8. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
9. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
10. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.
11. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
12. Select the **Use Custom URL** checkbox to enter a customer URL to launch Achievers from the dock.
13. Select the **Set Up Provisioning** checkbox to configure user provisioning to Ultimate Software.

Next steps

Click **Continue to Next Step**.

Ultimate Software Provisioning

About this task

> **Note**
>
> If you don't need to set up user provisioning, proceed to Ultimate Software Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Steps

1. Email your Ultimate Software representative and ask them to configure provisioning for your account.
2. After your representative confirms the provisioning configuration, click**Continue to Next Step**.
3. In a separate tab or window, sign on to your Ultimate Software account.
4. In Ultimate Software, go to **System Admin > Web Services**.
5. In PingOne, enter the following information:
    1. In the **Username** field, enter the username for your Ultimate Software account.
    2. In the **Password** and **Repeat Password** fields, enter your Ultimate Software account password.

Copyright © 2025 Ping Identity Corporation

3. In the **User API Key**, **Client API Key**, and **Login Service Endpoint**, enter the corresponding values from the Ultimate Software **Web Services** page.

Next steps

Click **Continue to Next Step**.

Ultimate Software Attribute Mapping

About this task

PingOne for Enterprise will automatically populate required SAML attributes.

For Ultimate Software, the required attribute is `SAML_SUBJECT`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Ultimate Software Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Ultimate Software Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

Click **Continue to Next Step**.

Ultimate Software SAML Connection

Steps

1. On the **Review Setup** tab, click **Download** to download the PingOne SAML metadata file.
2. Email your Ultimate Software representative with the following information:
   - The **IdP ID** value.
   - The PingOne SAML metadata file you downloaded in step 1, attached to the email.

   Result:

Copyright © 2025 Ping Identity Corporation

Your Ultimate Software representative will respond with your SSO URL.

3. In PingOne, click **Finish** to add Ultimate Software to your PingOne Dock.

Adding WebEx to Your PingOne for Enterprise Dock

Add the WebEx application your PingOne for Enterprise Dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **WebEx** application line to expand it, and then click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the signing certificate.
5. In a separate tab or window, sign on to your WebEx account as an administrative user.
6. In WebEx, go to **Site Administration > SSO Configuration**.
7. Click **Organization Certificate Management** and upload the PingOne for Enterprise signing certificate you downloaded in step 4.
8. In the single sign-on (SSO) configuration form, enter the following information.

Field	Action
Federation Protocol	**SAML 2.0**
WebEx SAML Issuer (SP ID)	`https://webex.com`
Issuer for SAML (IdP ID)	Enter the **IdP ID** from PingOne
Customer SSO Service Login URL	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<IdP ID>`, replacing *<IdP ID>* with the **IdP ID** value from PingOne for Enterprise.
Default WebEx Target Page URL	Leave blank
Customer SSO Error URL	Leave blank
NameID Format	`Unspecified`
AuthnContextClassRef	`urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified`
SSO Profile	`SP Initiated`
Single Logout	Leave checkbox clear
AuthnRequest Signed	Leave checkbox clear

Copyright © 2025 Ping Identity Corporation

Field	Action
Auto Account Update	Leave checkbox clear
Remove uid Domain Suffix for Active Directory UPN	Leave checkbox clear

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

WebEx Connection Configuration

Steps

1. Import the metadata for WebEx:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, replace *${parameter}* with your WebEx subdomain.
3. In the **Entity ID** field, enter your entity ID.

   The pre-populated value for this field should work for most configurations.

4. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated SSO.
5. In the **Single Logout Endpoint** field, enter a URL for PingOne to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from WebEx.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne sign responses to incoming SAML assertions.

Copyright © 2025 Ping Identity Corporation

12. From the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch WebEx from the dock.
14. Select the **Set Up Provisioning** checkbox to configure user provisioning to WebEx.

Next steps

Click **Continue to Next Step**.

WebEx Provisioning

About this task

> **Note**
>
> If you don't need to set up user provisioning, proceed to WebEx Attribute Mapping.

If you selected **Set Up Provisioning** on the **Connection configuration** tab:

Steps

1. In PingOne, click**Continue to Next Step**.
2. On the **Application Configuration** tab, enter the following information.
    1. In the **webexid** field, enter your WebEx administrator user name
    2. In the **password** field, enter the WebEx administrator user password.
    3. In the **siteName** field, enter your WebEx subdomain.
    4. **Optional:** In the **siteid** field, enter your WebEx **Account Site ID** value.

       You can find this value on the WebEx Administration Tool page.
    5. In the **partnerId** field, enter your WebEx **Account Partner ID** value.

    You can find this value on the WebEx Administration Tool page.

Next steps

In PingOne, click **Continue to Next Step**.

WebEx Attribute Mapping

About this task

PingOne for Enterprise will automatically populate required SAML attributes.

Copyright © 2025 Ping Identity Corporation

For WebEx, the following attributes are required for SSO:

- `SAML_SUBJECT`. Map to the username attribute. Email address is preferred.
- `SAML_AUTHN_CTX`. Select the **As Literal** checkbox. Enter a value of `urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified`.

If you enabled provisioning, the following provisioning attributes are required:

- `firstname`
- `lastname`
- `password`
- `email`

All other provisioning attributes are optional.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

WebEx Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

WebEx Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne Dock.

Adding Workday to Your PingOne for Enterprise Dock

Add the Workday application to your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Workday** application line to expand it, and then click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the PingOne for Enterprise signing certificate.
5. Copy the **IdP ID** value.
6. Send an email to your Workday partner representative with the following information.

Copyright © 2025 Ping Identity Corporation

Property	Description
Certificate	Attach the signing certificate you downloaded in step 4.
Certificate validity range	The issued date and the expiration date of the certificate.
Redirect URL	Include the following URL with your PingOne for Enterprise account information filled in. `https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=e003a904-a9d8-4d2e-a3e8-74dac7879938&idpid=<Enter idpid here>&apurl=https%3A%2F%2Fwww.myworkday.com%2<Enter Workday tenant here>%2Flogin.flex` **Note** The Redirect URL is not required if you plan to use the Target Resource URL.
Logout URL	Specify where to redirect users when they sign out of Workday.
Identity Provider ID	The **IdP ID** value from above.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Workday Connection Configuration

Steps

1. Import the metadata for Workday:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** field, replace the *${tenant}* variable with the your Workday account name.
3. Leave the default **Entity ID** value.
4. **Optional:** In the **Target Resource** field, replace the *${tenant}* variable with the your Workday account name.

> **Note**
> Enter this information only if you're using a target resource URL instead of a redirect URL.

Copyright © 2025 Ping Identity Corporation

5. In the **Single Logout Endpoint** field, enter a URL for PingOne for Enterprise to send single logout (SLO) requests to.
6. In the **Single Logout Response Endpoint** field, enter a URL for PingOne for Enterprise to send SLO responses to.
7. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Zendesk.
8. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
9. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
10. Select **Pass-Thru RequestedAuthnContext to IdP** if you want PingOne for Enterprise to pass the `RequestedAuthnContext` request to the IdP for your account.

    This option is available only if you upload a primary verification certificate.
11. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
12. On the **Signing** line:

    Choose from:

    - Click **Sign Assertion** to have PingOne for Enterprise sign outgoing SAML assertions. This is the default option.
    - Click **Sign Response** to have PingOne for Enterprise sign responses to incoming SAML assertions.
13. In the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
14. Select the **Use Custom URL** checkbox to enter a customer URL to launch Workday from the dock.

Next steps

Click **Continue to Next Step**.

Workday Attribute Mapping

About this task

PingOne for Enterprise will automatically populate required SAML attributes.

For Workday, the required attribute is `SAML_SUBJECT`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

Copyright © 2025 Ping Identity Corporation

Choose from:

- To map to the application attribute: Enter or select a directory attribute.
- To assign to the application attribute: Select **As Literal**, then enter a literal value.

4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Workday Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Workday Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Copyright © 2025 Ping Identity Corporation

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne for Enterprise dock.

Adding Zendesk to Your PingOne for Enterprise Dock

Add the Zendesk application to your PingOne for Enterprise dock from the application catalog.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Zendesk** application line to expand it, and then click **Setup**.
4. On the **SSO Instructions** tab, click **Download** to download the PingOne for Enterprise signing certificate.
5. In the Zendesk admin console, click the **Zendesk Products** icon, then click **Admin Center**.
6. Click the **Security** icon, then click the **Single sign-on** tab.
7. Click **Configure**.
8. In the single sign-on (SSO) configuration form, enter the following information.

Field	Action
SAML SSO URL (Required)	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<your IdP ID value>`
Certificate fingerprint (Required)	Enter the certificate fingerprint for your signing certificate. **Tip** To obtain the certificate fingerprint, in PingOne for Enterprise, go to **Setup > Certificates**, and expand the line for your signing certificate. PingOne for Enterprise displays both the **SHA1 Fingerprint** and **SHA256 Fingerprint** values.
Remote logout URL (Optional)	`https://sso.connect.pingidentity.com/sso/terminatesession?page=https://<URL to redirect users to>`

Copyright © 2025 Ping Identity Corporation

Field	Action
IP Ranges (Optional)	Enter a range of IP addresses to restrict SSO to those locations. Users requesting sign on from outside those locations will be redirected to the Zendesk sign-on page. Leave this field blank to allow SSO from any location.

9. Click **Enabled**
10. Click **Save**.

Next steps

In PingOne for Enterprise, click **Continue to Next Step**.

Zendesk Connection Configuration

Steps

1. Import the metadata for Zendesk:

   Choose from:

   - Click **Select File** to upload the metadata file.
   - Click **Or use URL** to enter the URL of the metadata.

2. In the **ACS URL** and **Entity ID** fields, replace the *${accountname}* variables with the your Zendesk account name.
3. In the **Target Resource** field, enter a URL to redirect the user to after IdP-initiated single sign-on (SSO).
4. In the **Single Logout Endpoint** field, enter a URL for PingOne for Enterprise to send single logout (SLO) requests to.
5. In the **Single Logout Response Endpoint** field, enter a URL for PingOne for Enterprise to send SLO responses to.
6. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Zendesk.
7. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
8. Select the **Force Re-authentication** checkbox to require your identity bridge to re-authenticate users with an active SSO session.
9. Select **Pass-Thru RequestedAuthnContext to IdP** if you want PingOne for Enterprise to pass the `RequestedAuthnContext` request to the IdP for your account.

   This option is available only if you upload a primary verification certificate.

10. Select the **Encrypt Assertion** checkbox to encrypt outgoing SAML assertions.
11. On the **Signing** line:

Copyright © 2025 Ping Identity Corporation

Choose from:

- Click **Sign Assertion** to have PingOne for Enterprise sign outgoing SAML assertions. This is the default option.
- Click **Sign Response** to have PingOne for Enterprise sign responses to incoming SAML assertions.

12. In the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. Select the **Use Custom URL** checkbox to enter a customer URL to launch Zendesk from the dock.

Next steps

Click **Continue to Next Step**.

Zendesk Attribute Mapping

About this task

PingOne for Enterprise will automatically populate required SAML attributes.

For Zendesk, the required attribute is `SAML_SUBJECT`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.
2. In the **Application Attribute** field, enter the attribute name as it appears in the application.
3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

   Choose from:

   - To map to the application attribute: Enter or select a directory attribute.
   - To assign to the application attribute: Select **As Literal**, then enter a literal value.
4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Zendesk Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

Copyright © 2025 Ping Identity Corporation

The image file must be:

- PNG, GIF, or JPG format
- 312 x 52 pixels maximum
- 2 MB maximum file size

> **Note**
>
> Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Zendesk Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne for Enterprise dock.

Adding Zoom to Your PingOne for Enterprise Dock

Add the Zoom application to your PingOne for Enterprise dock from the application catalog.

About this task

> **Note**
>
> Single sign-on (SSO) is only available to paid business and educational Zoom accounts.

Copyright © 2025 Ping Identity Corporation

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > Application Catalog**.
2. **Optional:** In the **Search** field, search for the application.
3. Click the **Zoom** application line to expand it and click **Setup**.

> **Important**
>
> As of June 2023, Zoom no longer allows the creation of new JSON Web Token (JWT) applications.
> If you want to enable user provisioning for Zoom, select the **Zoom - OAuth** application in the PingOne for Enterprise Application Catalog.
> For more information, see JWT App Type Deprecation FAQ in the Zoom documentation.

4. In a separate tab, go to https://www.zoom.us/signin and sign on to your account as an administrative user.
5. In the Zoom admin console, click **Single Sign-On**.
6. On the **Vanity URL** line, click **Apply**.
7. In the **Vanity URL** field, enter a vanity URL for your organization and click **Apply**.

   For more information, see Guidelines for Vanity URL requests in the Zoom documentation.

> **Note**
>
> Zoom takes 1-2 business days to process vanity URL requests.

Next steps

After Zoom approves your vanity URL request, return to the Zoom app catalog application and click **Continue to Next Step**.

Zoom Connection Configuration

Steps

1. Import the metadata for Zoom:

   Choose from:

   - To upload the metadata file: Click **Select File**.
   - To enter the URL of the metadata: Click **Or use URL**.

> **Important**
>
> If you upload a metadata file, the **Entity ID** field is automatically populated to include the `https` prefix. Leaving this prefix intact can cause configuration errors.
> After you upload the metadata file, you should verify that the **Entity ID** value is in the format `<vanity name>.zoom.us` .

Copyright © 2025 Ping Identity Corporation

2. **Required:** In the **ACS URL** and **Entity ID** fields, replace the *${vanity}* variables with your Zoom vanity URL.
3. In the **Target Resource** field, enter a URL to redirect the user to after identity provider (IdP)-initiated SSO.
4. In the **Single Logout Endpoint** field, enter a URL for PingOne for Enterprise to send single logout (SLO) requests to.

> **Note**
>
> If you enter a value in the **Single Logout Endpoint** field, it should be in the format `https://<vanity name>.zoom.us/saml/SingleLogout`.

5. In the **Single Logout Response Endpoint** field, enter a URL for PingOne for Enterprise to send SLO responses to.

> **Tip**
>
> Using the https://*<your vanity URL>*.zoom.us/saml/singlelogout SLO endpoint for both **Single Logout Endpoint** and **Single Logout Response Endpoint** improves your security by ending the user session in the application when the user's SSO session ends.

6. To add a **Primary Verification Certificate**, click **Browse** to locate and upload a local certificate file used to verify SLO requests and responses coming from Zoom.
7. To add a **Secondary Verification Certificate**, click **Browse** to locate and upload a local certificate used to verify SLO requests and responses if the primary certificate fails.
8. To require your identity bridge to re-authenticate users with an active SSO session, select the **Force Re-authentication** checkbox .
9. If you want PingOne for Enterprise to pass the `RequestedAuthnContext` request to the IdP for your account, select **Pass-Thru RequestedAuthnContext to IdP**.

> **Note**
>
> This option is available only if you upload a primary verification certificate.

10. To encrypt outgoing SAML assertions, select the **Encrypt Assertion** checkbox.
11. On the **Signing** line:

    Choose from:

    - To have PingOne for Enterprise sign outgoing SAML assertions: Click **Sign Assertion**. This is the default option.
    - To have PingOne for Enterprise sign responses to incoming SAML assertions: Click **Sign Response**.

12. In the **Signing Algorithm** list, select an algorithm with which to sign SAML assertions.
13. To enter a custom URL to launch Zoom from the dock, select the **Use Custom URL** checkbox.
14. To enable user provisioning, select the **Set Up Provisioning** checkbox.

Next steps

Click **Continue to Next Step**.

Copyright © 2025 Ping Identity Corporation

Zoom Provisioning

About this task

> **Note**
>
> If you don't need to set up user provisioning, proceed to Zoom Attribute Mapping.

Steps

1. Sign on to the Zoom App Marketplace as an administrator.
2. Click **Develop > Build App**.
3. On the **Choose your app type** page, in the **Server-to-Server OAuth** tile, click **Create**.
4. In the **App Name** field, enter a name for your application and click **Create**.
5. On the **App credentials** tab, copy the **Account ID**, **Client ID**, and **Client Secret** values, then click **Continue**.

You will enter these values into PingOne for Enterprise later.

1. On the **Information** tab, complete the following information:
    1. In the **Short description** field, enter a description for the application.
    2. In the **Company Name** field, enter the name of your organization.
    3. In the **Name**, enter the name of the contact for your Zoom account administrator.
    4. In the **Email address** field, enter to company email address of your Zoom account administrator.

    > **Note**
    >
    > The information on this tab is required for you to activate your application.

2. On the **Features** tab, click **Continue**.
3. On the **Scopes** tab:
    1. Click **Add Scopes**.
    2. On the **Add Scopes** dialog, select the checkboxes to add the following scopes:
        - **User**
            - **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**
            - **View and manage sub accounts** (account:master)

Copyright © 2025 Ping Identity Corporation

- **View account info** (account:read:admin)
- **View and manage account info** (account:write:admin)

- **SCIM2**
  - **Call Zoom SCIM2 API** (scim2)

3. Click **Done** to add the selected scopes.

4. On the **Activation** tab, click **Activate**.

5. In PingOne for Enterprise, click **Continue to Next Step** until you see the **Application Configuration** tab.

6. On the **Application Configuration** tab, configure your Zoom connection.

   1. Review the values for the **SCIM_URL** and **OAUTH_TOKEN_URL** fields, and change if necessary.

      > **Tip**
      >
      > The default values will work for most customers.

   2. In the **OAUTH_ACCOUNT_ID** field, enter your Zoom account ID.

   3. In the **OAUTH_CLIENT_ID** field, enter your Zoom client ID

   4. In the **OAUTH_CLIENT_SECRET** field, enter your Zoom client secret.

   5. From the **REMOVE_ACTION** list, select one of the following options:

      - If you select **Disable**, a user you disable or delete in PingOne for Enterprise will be disabled in Zoom.
      - If you select **Delete**, a user you disable or delete in PingOne for Enterprise will be deleted in Zoom.

   6. Click **Continue to Next Step**.

Zoom Attribute Mapping

About this task

PingOne for Enterprise automatically populates required SAML attributes.

For Zoom, the required attribute is `SAML_SUBJECT`. Map this to the attribute of the user's email address, usually `SAML_SUBJECT` or `email`.

Steps

1. To add an additional optional attribute, click **Add new attribute**.

2. In the **Application Attribute** field, enter the attribute name as it appears in the application.

3. In the **Identity Bridge Attribute or Literal Value** field, choose one of the following:

Copyright © 2025 Ping Identity Corporation

Choose from:

- To map to the application attribute: Enter or select a directory attribute.
- To assign to the application attribute: Select **As Literal**, then enter a literal value.

4. To create advanced attribute mappings, click **Advanced**.

   Learn more in Creating advanced attribute mappings.

Next steps

Click **Continue to Next Step**.

Zoom Customization

Steps

- To change the application icon, click **Select image** and upload a local image file.

  The image file must be:

  - PNG, GIF, or JPG format
  - 312 x 52 pixels maximum
  - 2 MB maximum file size

  > **Note**
  >
  > Images are scaled to 64 x 64 pixels for display.

- To change the name of the application displayed on the dock, in the **Name** field, enter a new name.
- To change the description of the application, in the **Description** field, enter the new description text.
- To change the category to which the application is assigned on the dock, in the **Category** list, select a category.

  Learn more in Creating a custom application category.

Next steps

Click **Continue to Next Step**.

Zoom Group Access

About this task

The **Group Access** tab shows every user group that you have created.

Copyright © 2025 Ping Identity Corporation

Learn more in Adding user groups.

Steps

- To add a group's access to the application, on the line for that group, click **Add**.
- To remove a group's access, on the line for that group, click **Remove**.
- When you're finished assigning groups, click **Continue to Next Step**.

Next steps

On the **Review Setup** tab, review your configuration, and click **Finish** to add the application to your PingOne for Enterprise Dock.

Zoom SAML Connection

Steps

1. On the **Review Setup** tab:
    1. On the **Signing Certificate** line, click **Download** to download the signing certificate.
    2. On the **SAML Metadata** line, click **Download** to download the metadata file.
2. In a separate tab, sign on to the Zoom admin console and go to the **Single Sign-On** tab.
3. In Zoom, set the **Sign-in Page URL** value:
    1. Open the metadata file in a text editor.
    2. Copy the `SingleSignOnService` `Location` value.

       Example: `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<idpid value>`
    3. In the Zoom admin console, paste the `Location` value into the **Sign-in Page URL** field.
4. **Optional:** In the **Sign-Out page URL** field, enter `https://<vanity name>.zoom.us/saml/SingleLogout`.

> **Tip**
>
> An SLO URL improves security by ending a user session in Zoom when the user's SSO session ends.

5. In the **Service Provider (SP) Entity ID** list, select the non-HTTPS option.
6. In the **Enter Issuer** field, paste the *entityID* value from the metadata file.
7. Enter the **Identity provider certificate** value:
    1. Open the signing certificate file in a text editor.
    2. Copy the contents of the signing certificate file, excluding the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines.
    3. In the Zoom admin console, paste the certificate contents into the **Identity provider certificate** field.

Copyright © 2025 Ping Identity Corporation

8. On the **Binding** line, click either **HTTP-POST** or **HTTP-Redirect**.

> **Tip**
>
> **HTTP-POST** is the more secure option, because it doesn't expose the SAML token as a query parameter in the URL.

9. On the **Signature Hash Algorithm** line, click **SHA-256**.
10. On the **Security** line, select the checkboxes of the security policies to implement.

> **Tip**
>
> Improve your security by selecting **Sign SAML request** and **Save SAML response logs on user sign-in**.

11. Click **Save Changes**.

Add a Basic SSO (password vaulting) application

About this task

To use Basic SSO, you first need to enable it on the **Setup > Dock > Configurations** page. See Configuring the dock when using an identity bridge or (if you're using PingOne directory as your identity repository) Configure the dock when using PingOne for Enterprise Directory for more information.

You'll need to install the PingOne browser extension to add Basic SSO applications. If you've not already installed the browser extension, you will be prompted to do so when adding the app.

Basic SSO (password vaulting) uses the PingOne for Enterprise browser extension to relay credentials to the target cloud application. User credentials are encrypted (128 bit AES) with a user-specified privacy key and are stored in PingOne for Enterprise. The privacy key is stored in the local file system and is never sent to PingOne for Enterprise. PingOne for Enterprise uses stored encrypted credentials for single sign-on (SSO) to your cloud applications. The browser extension can access the encrypted credentials only after a user is authenticated to the identity repository.

Steps

1. Click the **Applications** tab. The My Applications page is displayed.
2. Click **Add Application** and select **New Basic SSO Application**.
3. If you've not installed the PingOne browser extension for the current browser, you're prompted to install it. When the browser extension is installed, click **Begin** to launch the wizard for adding new Basic SSO applications. The wizard will guide you through training the browser extension for password vaulting into the application.

   When you're finished, the new Basic SSO application is added to your My Applications list.
4. Make the new application available to your users.

   See Authorize group access to applications for instructions.

Copyright © 2025 Ping Identity Corporation

Creating a custom application category

Custom application categories let you organize your applications in ways that work best for your organization.

About this task

You can create categories such as applications that are accessible only by VPN, applications specifically geared toward onboarding new hires, or applications that are intended for specific departments.

Categories don't change the behavior or access privileges of an application, but you can use categories to organize applications for easier administration.

Steps

1. In the PingOne for Enterprise admin console, go to **Applications > My Applications > Custom Categories**.
2. Click **Add Category**.
3. In the **Name** field, enter a category name.
4. Click **Next**.
5. **Optional:** For each language field, enter the localized category name for the corresponding localization region.

   Entries in these fields replace the original category name for administrators in the corresponding localization regions.
6. Click **Done**.

   Result:

   The new category appears in the custom category list.
7. To view the applications assigned to a custom category, click the **Expand** icon for the category, and click **Applications**.

> **Tip**
>
> You can assign an application to a category on the **PingOne App Customization** tab of the application adding or editing process.
> For more information about adding or editing an application, see Adding or updating a SAML application and Adding or updating an OIDC application.

Result

The custom category appears in the list of available application categories.

Managing users

You can manage users in three different ways.

You can use the following operations to manage your PingOne for Enterprise service users:

If you are using PingOne for Enterprise Directory as your identity provider (IdP), you can manage users by their listing in the PingOne for Enterprise Directory. For more information, see Managing PingOne for Enterprise Directory users.

Copyright © 2025 Ping Identity Corporation

Regardless of which IdP you are using, you can manage users by their group membership. For more information, see Managing users by group.

> **Note**
>
> Applications and authentication policies assigned to users are managed by group membership. For PingOne for Enterprise Directory, this is done through the permissions assigned to a group.

User access to PingOne services and their usage of each service is managed on a services basis. For more information, see Managing service users.

Managing PingOne for Enterprise Directory users

If you're using PingOne for Enterprise Directory as an identity repository, you can directly manage users in your directory.

Directory Entitlements

We recommend you add groups before adding any users. Your users' ability to view and change any user or group information in the directory is controlled through your assignment of directory roles to groups. Each role has associated entitlements to directory information. Users inherit the entitlements assigned to a role through their group memberships. The roles have ascending levels of entitlement: each role includes the entitlements assigned to a lower level role. A group can be assigned only one role. When a user is a member of more than one group, the highest level role assigned to any one of the user's groups is applied. The directory available roles are:

User Reader

Groups assigned this role are entitled only to view user and group directory information.

User Manager

Groups assigned this role have User Reader entitlements plus the ability to invite and create directory users and modify user attributes, though not group memberships.

Group and Entitlement Manager

Groups assigned this role have User Manager entitlements plus the ability to create directory groups, assign entitlements to groups and change group membership.

You need to be either a Global Administrator or Identity Repository Administrator to view and change directory settings.

Provisioning

The PingOne for Enterprise Directory supports user provisioning using the current SCIM protocol (System for Cross-Domain Identity Management: Protocol 1.1).

PingOne for Enterprise Directory attributes are SCIM attributes, and apply to all users. The predefined attributes for the directory are SCIM version 1.1 core schema attributes.

Reporting

You will find user transactions logged for the PingOne for Enterprise Directory on the Reports page. These transactions are designated by the subsystem **Directory**. See Managing reports and subscriptions for more information.

Copyright © 2025 Ping Identity Corporation

Directory API

You can use the PingOne for Enterprise Directory REST API to validate credentials and authorize user access to perform user or group operations:

- (North America) https://directory-api.pingone.com/api
- (Europe) https://directory-api.pingone.eu/api
- (Australia) https://directory-api.pingone.com.au/api

Access to the directory API requires that you have the client ID and API key for your account. See View or renew directory API credentials for instructions.

Add directory groups and entitlements

Before you begin

You need to be either either a Global Administrator, an Identity Repository Administrator or Group and Entitlement Manager to add directory groups.

About this task

By default, all new users are automatically assigned to the group `Users`, which has no directory entitlements (users aren't able to view directory information).

You can add a new group to the PingOne for Enterprise Directory, give the group a meaningful name, and (optionally) assign a directory role to the group. A user's directory entitlements are inherited from the entitlements from their group memberships. A group's entitlements derive from the role assigned to the group.

By default all members of all groups have access to all of the applications you add. The applications available to a user are displayed in the PingOne dock. If you've added applications to PingOne, when you're finished adding directory groups, see Authorize group access to applications to control a group's access to applications.

By default, all PingOne for Enterprise administrative users are assigned to a group called `Domain Administrators`. This group is read-only and can't be directly modified. Learn how to change your administrators' permissions in Assign administrative roles.

> **Tip**
>
> Regular reviews of group access privileges and memberships helps prevent unauthorized access to critical applications and sensitive data.

Steps

1. Go to **Users > User Directory > Groups**.
2. Click **Add Group**. The New Group page is displayed.
3. Enter a name to use for the new group and select the directory role to assign to the group.

   A group can be assigned only one role.

   User Reader

   Groups assigned this role are entitled only to view user and group directory information.

Copyright © 2025 Ping Identity Corporation

User Manager

Groups assigned this role have User Reader entitlements plus the ability to invite and create directory users and modify user attributes, though not group memberships.

Group and Entitlement Manager

Groups assigned this role have User Manager entitlements plus the ability to create directory groups, assign entitlements to groups and change group membership.

Result:

For all of the roles, the PingOne admin portal application is added to the PingOne dock for each group member. In this case (for all roles), the PingOne admin portal displays only the **Users** and **Groups** tabs.

4. Click **Save** when you're finished.
5. Repeat these steps for any additional groups to add to the directory.
6. If you've added applications to PingOne, see Authorize group access to applications to control a group's access to applications.

Add directory users

Add new users to the PingOne for Enterprise Directory.

Before you begin

You need to be either a Global Administrator, Identity Repository Administrator, or have at least User Manager entitlements to add a directory user.

About this task

When you add new users to the PingOne for Enterprise Directory, you can pre-fill some or all of the user attribute values, or you can allow the new user to enter all of the necessary information.

By default, all new users are automatically assigned to the group `Users`, which has no directory entitlements (users aren't able to view directory information).

By default, all PingOne for Enterprise administrative users are assigned to a group called `Domain Administrators`. This group is read-only and can't be directly modified. Learn how to change your administrators' permissions in Assign administrative roles.

Steps

1. Go to **Users > User Directory > Users**.
2. Do one of the following:

   Choose from:

   - To create the user using attribute values you assign:
     1. Click **Add Users** to display the list of methods to add a user, and select **Create New User**.
     2. In the **Password** section, enter the initial password to assign to the user.

        The user will be required to reset their password the first time they sign on.

Copyright © 2025 Ping Identity Corporation

3. Enter the attribute values you want to assign to the user.

   The **Username**, and **Email** values are required. All new users are automatically assigned to the `Users` group, so specifying group membership isn't required, though we recommend it.

4. Click **Save** when you're done.

5. Send the user's single sign-on (SSO) credentials to them. The new user can then SSO to PingOne for Enterprise.

- To invite the user, having them enter all of the necessary user attributes:

  1. Click **Add Users** to display the list of methods to add a user, and select **Invite New User**. You're prompted for the email address to use.

     Use this method when you need to contact the user via an alternate email address (one not associated with an application dependent on their single sign-on to PingOne for Enterprise).

  2. If the user currently has access to the email address assigned to their PingOne for Enterprise account, use **Email Address** to send the invitation. The new user is added to the directory and an email invitation is sent to the email address you've entered.

     Optionally, if the user currently doesn't have access to the email address assigned to their PingOne for Enterprise account, you can use **Alternate Email** to send the invitation.

3. If you've chosen to invite the user, note the user's Invited status on the **Users** page. This status will change to Enabled when the new user activates their PingOne for Enterprise account.

> **Note**
>
> The user invitation has a lifetime of 24 hours. If the user hasn't responded within that time you will need to resend the invitation.
> If a user clicks on an expired invitation link, they're redirected to the PingOne for Enterprise sign-on page, which displays an error message to request a new invitation from the administrator.
> You can change the destination of the redirect by using the `redirectLink` attribute in the PingOne for Enterprise Directory API. For more information, see .pingidentity.com/pingone/enterprise/v1/api///[User Registration Notifications].

While the user status is Invited, you can choose to do any of the following (from the list next to the **Details** button):

- **Resend email** to resend an email invitation using the user's account email address.
- **Resend email to alternate email address** to resend an email invitation to an email address for the user that's not used for the account email.
- **Delete** to remove the user from the directory.

4. Repeat these steps for each new user to add to PingOne for Enterprise.

5. To add a user to an administrative role (including adding a user to the Domain Administrators group), see Assign administrative roles.

Approve new directory users

Before you begin

Copyright © 2025 Ping Identity Corporation

See Allow self registration for new directory users for instructions to enable self registration.

You need to be either a Global Administrator, Identity Repository Administrator, or have at least User Manager entitlements to approve a new directory user.

About this task

If you've configured self-registration to require approval, after a new directory user registers, you will need to approve their access to PingOne.

Steps

1. Go to **Users > User Directory > Users**.

Users who have self-registered and haven't yet been approved have a Status value of `Pending Approval`.

1. For the user to approve, click the down-arrow next to the Details button and click **Approve**.

   Result:

   The user status changes to `Enabled` and the user can now access PingOne.

2. Repeat these steps for any additional new users to approve.

Display directory user details

About this task

Any user with User Reader entitlements can view user details.

Steps

1. Go to **Users > User Directory**.

   The Status column displays the current state of each user. This can be:

   - Enabled. The user can access PingOne.
   - Disabled. The user has been disabled and cannot access PingOne.
   - Pending Approval. The user needs to be approved before they can access PingOne.
   - Locked. The user has exceeded the maximum number of sign on attempts. See Configure the directory password policy for more information.

2. Do one of the following:

   Choose from:

   - Click a user ID to display the user details. Alternatively, you can click **Details**.
   - Search for a user. The search begins matching users as you enter the characters. You can search in either of these ways:

Copyright © 2025 Ping Identity Corporation

Simple search

You can search on:

- `Username`
- `First Name`
- `Last Name`
- `Emails`

Use the dropdown list of search categories to constrain the search domain. You can search all users (the default), or only those users having a `Status` of: Enabled, Disabled, Invited, Locked, or Pending Approval.

Advanced search

Enable advanced search. The suggested text in the search box changes to a SCIM example. The search begins matching SCIM criteria as you enter the characters.

Your search criteria needs to conform to the .simplecloud.info/specs/draft-scim-api-01.html//[SCIM filtering specification]. You can find the SCIM attributes for your searches on the Attributes page. See Manage directory attributes.

Operator	Description	Behaviour
( )	Precedence grouping	Enclose boolean expressions in parentheses to have the expression(s) evaluated first in the order of operations.
and	Logical AND	Matches if both expressions are true.
or	Logical OR	Matches if either expression is true.
eq	Equals	The value of the specified attribute equals the specified value.
co	Contains	The value of the specified value is a substring of the specified attribute.
sw	Starts With	The value of the specified value is a substring of the specified attribute when starting at the beginning of the attribute value string.

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise

Operator	Description	Behaviour
pr	Present	The value of the specified attribute has a value (not a null string), or (for complex attributes) contains a non-empty node.
gt	Greater Than	The value of the specified attribute is greater than the specified value. The comparison used depends on the data type. For strings, the comparison is lexicographic; for DateTime, it is chronological.
ge	Greater Than or Equal	The value of the specified attribute is greater than or equal to the specified value. The comparison used depends on the data type. For strings, the comparison is lexicographic; for DateTime, it is chronological.
lt	Less Than	The value of the specified attribute is less than the specified value. The comparison used depends on the data type. For strings, the comparison is lexicographic; for DateTime, it is chronological.
le	Less Than or Equal	The value of the specified attribute is less than or equal to the specified value. The comparison used depends on the data type. For strings, the comparison is lexicographic; for DateTime, it is chronological.

Some examples:

```
username eq "charlie"
```

```
name.familyName co "jones"
```

```
emails.value co "jones"
```


Copyright © 2025 Ping Identity Corporation

```
name.givenName sw "char"
```

Update directory user details

About this task

You need to be either a Global Administrator, Identity Repository Administrator, or have at least User Manager entitlements to update directory user information.

Steps

1. Go to **Users > User Directory > Users**.
2. Click a user ID to display the user details. Alternatively, you can click **Details**.
3. Click **Edit** to switch to Edit mode.
4. Update the user details as needed.

   The user attributes you can change are determined by the settings on the Attributes page (see Manage directory attributes).
5. Click **Save** when you're finished.
6. Repeat these steps to update information for any additional users.

Reset a user's password

Before you begin

You need to be either a Global Administrator, Identity Repository Administrator, or have at least User Manager entitlements to reset a directory user's password.

About this task

You will need to edit a user profile to reset their password. As a consequence of resetting the password, the current user session will be revoked.

Steps

1. Go to **Users > User Directory > Users**.
2. Click **Edit** to display the user details in Edit mode.
3. Enter a new password in the **Password** field and confirm the new password.
4. Click **Save**.

Disable directory users

Before you begin

You need to be either a Global Administrator, Identity Repository Administrator, or have at least User Manager entitlements to disable a directory user.

Copyright © 2025 Ping Identity Corporation

About this task

Disabling a directory user revokes the current user session and removes user access to any of the PingOne services or applications for your account. You can subsequently re-enable the user.

Steps

1. Go to **Users > User Directory > Users**.
2. For the user to disable, click the down-arrow next to **Details** and click **Disable**.

   Result:

   PingOne access for the selected user is disabled. You can choose to re-enable the user using this same process whenever you like.
3. Repeat these steps for any additional users to disable.

Delete directory users

Before you begin

You need to be either a Global Administrator. Identity Repository Administrator, or have at least User Manager entitlements to delete a directory user.

About this task

Deleting a user revokes the current user session and permanently removes them from the directory.

Steps

1. Go to **Users > User Directory > Users**.
2. Click the down-arrow next to **Details** and click **Delete**.

   Result:

   The selected user is permanently removed from the directory.
3. Repeat these steps for any additional users to delete.

Validating user credentials with PingFederate

About this task

If you're using PingOne for Enterprise Directory as an identity repository, and your organization uses PingFederate, you should have PingFederate verify user credentials stored in the PingOne for Enterprise Directory. You don't need to make any configuration changes in PingOne for Enterprise when you configure the PingOne for Enterprise Directory Password Credential Validator in PingFederate.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> We implement rate limiting on PingOne for Enterprise Directory APIs to maintain a high quality of service for all our customers. Rate limiting restricts any one API client from flooding PingOne for Enterprise Directory APIs with an unusually high amount of traffic, which could affect usage of PingOne for Enterprise Directory by other customers. If a customer reaches the defined rate limit, the PingOne for Enterprise Directory API responds with a 429 HTTP status code `Too Many Requests`.
> If your integration hits the rate limit, you must reduce the rate at which your API client is making requests to complete any further API calls successfully. The enforcement of an API rate limit is standard practice for software as a service (SaaS) services. If rate limits are negatively affecting your usage of the PingOne for Enterprise Directory API, contact our support team to review your integration.

Steps

1. To get the API credentials for your account, go to **Setup > Directory Settings > Credentials**.

   Learn more about API credentials in View or renew directory API credentials.

2. Configure thePingOne for Enterprise Directory Password Credentials Validator.

   For more information, see Configuring the PingOne for Enterprise Directory Password Credential Validator in the PingFederate documentation.

   Result:

   The credentials for PingOne for Enterprise Directory users are then verified through PingFederate as well as PingOne for Enterprise. SSL is used to send the credentials to PingOne for Enterprise from PingFederate.

Next steps

To enable users to change or reset their passwords, see Changing user passwords for PingFederate.

Changing user passwords for PingFederate

About this task

If you're using the PingOne for Enterprise Directory Password Credential Validator for PingFederate, you can allow your users to change or reset their passwords.

Ensure your PingFederate adapter is set to allow password changes, then have your users choose to change their passwords when they sign on.

Steps

1. Set your PingFederate adapter configuration to allow password changes.

   For instructions on setting this adapter, see Configuring an HTML Form IdP Adapter instance.

   Enabling password changes or resets adds a selection to change the password to your users' sign-on (SSO) prompt.

2. Notify your users that they can elect to change their changes their passwords when they sign on.

Copyright © 2025 Ping Identity Corporation

Managing users by group

PingOne groups correspond to groups in the user repository associated with your identity bridge. When a user signs on (SSO), their group information from the identity bridge is matched to a corresponding PingOne group. This enables you to authorize user access to cloud applications based on their group membership.

When you authorize applications for a group, those applications displayed in the PingOne dock for all members of the group and are available only to the group members. Any applications that you do not assign to a group are available to all users, but aren't displayed in the PingOne dock. Instead, users can SSO to these applications using the SSO URL assigned to the application.

> **Note**
>
> You cannot use the Active Directory group Domain Users for provisioning users.

Adding user groups

PingOne for Enterprise user groups authorize user access to applications based on a user's group membership.

About this task

You'll need to add the relevant groups to PingOne for Enterprise from the identity repository associated with your identity bridge

You can create user groups in the following ways:

- PingOne for Enterprise creates groups automatically based on a user's group membership during single sign-on (SSO). For example, PingOne for Enterprise will create a group based on the user's `memberOf` attribute in the Security Assertion Markup Language (SAML) response.
- If you're using an identity provider (IdP) that supports provisioning, you can also create groups through provisioning. AD Connect and PingOne for Enterprise Directory do this automatically. Learn more in PingOne for Enterprise identity repositories.

  PingFederate requires you to configure group provisioning on the PingFederate side. Learn more in Creating a provisioning connection in the PingFederate SCIM Provisioner documentation.
- Follow the steps below to create groups manually.

Provisioned groups appear automatically at **Users > User Groups**. Groups are removed when they're deprovisioned.

If you don't use provisioning, groups will appear when you create groups manually or after a user SSOs into the group.

You can remove old groups manually. Learn more in Delete groups.

If you're using Microsoft Entra ID (formerly known as Azure AD) as your IdP, PingOne for Enterprise has a **Sync Groups** button on the **User Groups** page that fetches groups from Azure. This adds new groups to PingOne for Enterprise and removes old groups that no longer exist in Azure. You can also create groups manually or have a user SSO to create a group. Learn more in Connect to Azure.

If you haven't added any applications for SSO, no applications will be listed when you add a group, but you can assign the groups to applications when you add SAML, OpenID Connect (OIDC), or Application Catalog apps.

For all other applications and general use, follow the steps in Authorize group access to applications. The applications you've added then will be displayed.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Unless you specify group authorization for an application when you add the application, all members of all groups are given access to the application by default.

Steps

1. Go to **Users > User Groups**.
2. Do one of the following, depending on whether or not you're using an Azure identity bridge with group synchronization:

   Choose from:

   - For an Azure identity bridge configured for group synchronization, the initial group synchronization has already occurred as part of the Azure identity bridge setup. To resynchronize the PingOne for Enterprise groups when additions or changes have occurred on your Azure provider, click **Synchronize Groups**.
   - For all other identity bridges as well as for Azure identity bridges without group synchronization, click **Add New Groups** and enter the name of one of your groups in the entry field.
3. Click **Save**. The new group is added to PingOne for Enterprise and will appear in the groups listing on the **User Groups** page.
4. Repeat these steps for each of the groups to add to PingOne for Enterprise.

Authorize group access to applications

Before you begin

Before you start authorizing group access to applications, you will need to set up your identity bridge, and add the relevant applications for your single sign-on (SSO) users.

About this task

You can use PingOne groups to authorize user access to applications based on a user's group membership. To do this, you will assign applications to groups. This authorizes the group members to access the applications and displays the applications on each member's PingOne dock. Only members of the group will then have access to the application.

By default, all users in your PingOne groups are given access to the applications you have added. Applications that you do not assign to a group are available to all users (they can SSO to the application URL), but the applications will not be displayed in their PingOne dock.

Steps

1. Go to **Users > User Groups**.
2. Select the group whose application access you want to limit and click **Edit**. The Edit Group/Application Associations page is displayed.
3. Click the checkbox next to each application that you want this group to be able to access.

   Use the Default Application checkbox to assign the selected applications as the default applications for this group.
4. Click **Save**. The group is authorized to use the selected applications. The application names are displayed in the group listing on the User Groups page.

Copyright © 2025 Ping Identity Corporation

5. Repeat these steps for each group whose access to applications you want to limit.

Exporting a report of applications by group

You can get a list of your applications and the groups assigned to access them by exporting a report file in `.csv` format.

About this task

If you have a large number of applications, it might be easier to sort and filter them using a spreadsheet before managing them in PingOne for Enterprise. Use the **Export Summary** button to export this list.

In the exported `.csv` file, the first column lists the application name. The second column lists all of the groups assigned to the application, separated by a semicolon.

Steps

1. Go to **Users** > **User Groups**.
2. Click **Export Summary**.

Result

Your browser downloads a `.csv` file to your default downloads directory.

Delete groups

About this task

Deleting a group is useful if, for example, you've either added a group by mistake, or the group no longer exists in your user repository and you need to remove it from PingOne for Enterprise.

Deleting a group removes the group and any of its associations to applications.

If your identity bridge supports provisioning, your PingOne for Enterprise groups are automatically updated to reflect any changes in the associated user repository. Provisioning dynamically creates and updates SSO user information in your PingOne for Enterprise user groups based on attributes in incoming SAML assertions from a cloud application provider. Only SAML-enabled applications can support provisioning.

> **Note**
>
> If a user who is a member of a deleted group signs on to PingOne for Enterprise, the group is recreated, and is again listed on the **User Groups** page.

Steps

1. On the **Users** tab, click the **User Groups** tab. The **User Groups** page is displayed.
2. In the groups listing, click **Edit** for the group you want to delete. The **Edit Group/Application Associations** page is displayed.
3. Verify that the group members belong only to this group, then click **I understand - delete the group**.
4. Click **Save**.The group and its application associations are deleted.

Copyright © 2025 Ping Identity Corporation

Managing service users

You can:

- Monitor a particular service activity for your users.
- Manage users' access to the service.
- Generate reports of service activity for a selected user.

Temporarily hiding a user's service

Temporarily hide a user's service if you want to remove them from activity reports.

About this task

You might want to temporarily hide a user's service because of security issues or if a user will be absent for an extended period.

Learn more about disabling a user's PingID access in Disabling a user's service.

Steps

1. Go to **Users > Users by Service**.
2. (Optional) Filter or search the user list.
    - Click a service name to filter by users of that service.
    - In the **Search** field, enter a string to search for.
        - In the **Search by** list, select a user attribute to search by.

        > **Note**
        >
        > To use the search filter, your account must not have the `SERVICE_USER_LEGACY` feature flag, which preserves legacy search behavior from before a PingOne for Enterprise update in April 2023.
        > Your account only has this feature flag enabled if you requested it. If you're not sure whether you have this feature flag, or if you want it removed so you can access this new behavior, open a support case.
        > The email and name filters can only filter user data that was newly created or updated after this feature was deployed (February 2025).
        > To search by `Name` , the input string must be in the format "last name, first name".
3. Click to expand the user and display a list of services the user is subscribed to.
4. Click to expand the service you want to change.
5. Click the **Pencil** icon followed by the **Temporarily Hide Activity** dialog to open the **Temporarily Hide Activity** popup.
6. Click **Confirm** to remove the user from the selected service.

   For single sign-on (SSO) and provisioning, users are shown in the list the next time they sign on. For other services, such as PingID, users must reregister after being disabled.

Copyright © 2025 Ping Identity Corporation

Bypassing a user's service

You can bypass the need for a user to authenticate using their secondary authentication method.

About this task

Bypassing a user's service can be necessary, for example, if a user of the PingID service doesn't have access to the mobile device that is paired with PingID. Generally, you will bypass a user's secondary authentication for a selected duration. At the end of a limited duration, secondary authentication for the user resumes automatically.

Global Administrators can set the bypass for an unlimited duration if you want to bypass the user's service permanently. All other administrators are limited to a maximum bypass period of 3 days.

Steps

1. Go to **Users > Users by Service**.
2. (Optional) Filter or search the user list.
    - Click a service name to filter by users of that service.
    - In the **Search** field, enter a string to search for.
        - In the **Search by** list, select a user attribute to search by.

> **Note**
>
> To use the search filter, your account must not have the `SERVICE_USER_LEGACY` feature flag, which preserves legacy search behavior from before a PingOne for Enterprise update in April 2023.
> Your account only has this feature flag enabled if you requested it. If you're not sure whether you have this feature flag, or if you want it removed so you can access this new behavior, open a support case.
> The email and name filters can only filter user data that was newly created or updated after this feature was deployed (February 2025).
> To search by `Name`, the input string must be in the format "last name, first name".

3. For a selected user, click the **Expand** icon to expand the user information for the service.
4. Click the edit icon, then click the **Bypass** toggle.

    Result:

    You are prompted to select the duration for bypassing the specific service from a list.
5. Select the duration to bypass the service.

    If you're a Global Administrator, you can select **Unlimited Time** to bypass the service indefinitely. All other administrators are restricted to a maximum period of 3 days.
6. Click the **Bypass** toggle again to enable your bypass setting.

    When the selected length of time has passed, authentication automatically resumes for the user.

    If you select **Unlimited Time**, the user is never authenticated using this authentication provider.

Copyright © 2025 Ping Identity Corporation

Result:

The bypass is implemented and effective immediately.

Removing service users

When you view the users by service listing, you can choose to remove a user from a particular service.

About this task

You can filter the user list by a specific service, or search for a specific user.

Steps

1. Go to **Users > Users by Service**.
2. (Optional) Filter or search the user list.
    - Click a service name to filter by users of that service.
    - In the **Search** field, enter a string to search for.
        - In the **Search by** list, select a user attribute to search by.

> **Note**
>
> To use the search filter, your account must not have the `SERVICE_USER_LEGACY` feature flag, which preserves legacy search behavior from before a PingOne for Enterprise update in April 2023.
> Your account only has this feature flag enabled if you requested it. If you're not sure whether you have this feature flag, or if you want it removed so you can access this new behavior, open a support case.
> The email and name filters can only filter user data that was newly created or updated after this feature was deployed (February 2025).
> To search by `Name`, the input string must be in the format "last name, first name".

3. Click the **Expand** icon to display the service details for the selected user.

    Result:

    The expanded entry displays the last activity for that user per service and, for single sign-on (SSO), the last sign-on. If more than one service is shown for the user, expand the details for the target service.

4. Click the edit icon and choose the option to remove the user from the selected service.

    Result:

    You're prompted to confirm the action.

User provisioning in PingOne for Enterprise

PingOne for Enterprise supports user provisioning for certain identity providers (IdPs) and applications.

Copyright © 2025 Ping Identity Corporation

User provisioning allows you to manage your users' status and permissions in your IdP and your applications from the PingOne for Enterprise admin console. Provisioning saves your admins time and improves security by ensuring consistency across your user experience.

How provisioning works

Your IdP must be configured to provision both users and groups to PingOne for Enterprise. PingOne for Enterprise Directory and AD Connect are automatically configured to do this. You must manually configure PingFederate.

Learn more in Configuring outbound provisioning in the PingFederate documentation.

PingOne for Enterprise will provision users to a target application when:

- The IdP sends a group update with a membership change that references a user that already exists in PingOne for Enterprise.
- The IdP sends a user update for a user that already exists in PingOne for Enterprise and is already a member of a tracked group.

Creating a new user and adding them to a provisioning group will result in outbound provisioning. The IdP provisions the user and PingOne for Enterprise takes no action. Then the IdP updates the group to include the new user and PingOne for Enterprise creates the user in the target application.

Editing a user that already exists in a provisioning group will result in outbound provisioning. The IdP provisions the user update and PingOne for Enterprise updates the user in the target application.

Group provisioning

PingOne for Enterprise doesn't support outbound group provisioning. To provision groups, you must configure provisioning in PingFederate.

Learn more in User provisioning in the PingFederate documentation.

Identity providers

PingOne for Enterprise supports user provisioning using the following IdPs:

- PingOne for Enterprise Directory
- PingFederate.

  For more information, see Configuring Provisioning for PingFederate.
- AD Connect

Provisioning applications

The following PingOne for Enterprise Application Catalog applications support provisioning:

- Amazon Web Services
- AWS Single Sign-On
- Aquera
- Atlassian Cloud

Copyright © 2025 Ping Identity Corporation

- Box
- Code42
- Concur
- Contentful SCIM
- Coupa
- Dropbox
- Egnyte
- Evernote
- Github.com
- Google Gmail
- Jive - Production
- Jive - UAT
- Lucidchart
- Microsoft 365
- Ping IDaaS Directory Provisioner
- PingOne Provisioner
- Ping SCIM SaaS Provisioner
- Ping SCIM SaaS Provisioner 2
- Ping SCIM SaaS Provisioner 3
- Salesforce
- Salesforce Sandbox
- Salesforce Communities
- Salesforce Communities Sandbox
- ServiceNow
- ServiceNow (Fuji)
- Slack
- Ultimate Software
- WebEx
- Zendesk
- Zoom

Copyright © 2025 Ping Identity Corporation

- Zscaler Internet Access
- Zscaler Private Access 2.0

Provisioning setup

For general directions about configuring an Application Catalog application, see Add an application from the Application Catalog. For application-specific instructions, find the application in the PingOne for Enterprise Application Catalog documentation.

> **Note**
>
> While configuring your application, keep the following in mind:
>
> - On the **Connection Configuration** tab, select the **Set Up Provisioning** checkbox.
> - On the **Attribute Mapping** tab, attributes marked as **(provisioning)** are used only for provisioning. Attributes marked as **(sso)** are used only for single sign-on (SSO).

After you finish configuring the application, ensure that your user groups have provisioning enabled. Go to **Users > User Groups**. Click **Edit**, and select the **SSO** and **Provisioning** checkboxes for each application you want to enable for that group.

Provisioning troubleshooting

If you encounter provisioning problems, go to **Dashboard > Reporting > Run New Report > Provisioning** and run a provisioning activity report.

- If you don't see any outbound requests for an application, check that the group mapped to that application is actually being updated by the IdP.
- If you do see requests, but they result in errors, the error messages will usually indicate whether the issue is with the target application, the attribute mapping, or something else.
- If you see group updates but no user updates, or user updates but no group updates, check the IdP configuration to ensure that the IdP is configured to provision both users and groups.

Authenticating users

Your users are initially authenticated through the identity bridge, and for most purposes this single, secure authentication is sufficient. However, you can choose a secondary level of authentication as well. Together, the primary and secondary levels of authentication are known as multi-factor authentication.

> **Note**
>
> Creating a PingOne for Enterprise account also automatically creates a PingID account. If your organization doesn't use PingID, go to **Setup > PingID > Configuration** and clear the **Allow users to manage their devices on the web** box. This will prevent users from accessing the PingID **Devices** page from the web or PingOne Dock.

You can apply the authentication policy to all users, or a subset of your users based on group membership or IP address. The policy applies to:

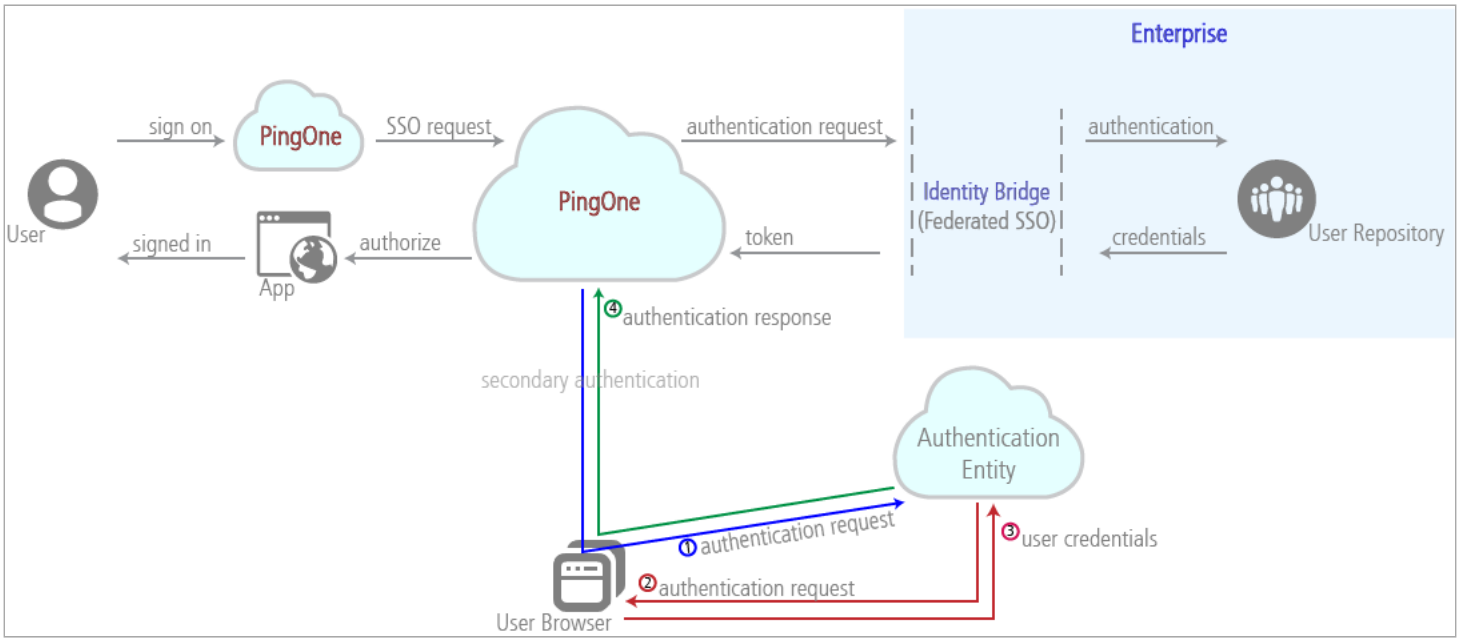
- SSO to PingOne.
- All SAML-enabled applications.

Copyright © 2025 Ping Identity Corporation

- Selected SAML-enabled applications.

You can also apply secondary authentication to the PingOne admin portal.

How It Works



> **Note**
>
> For Basic SSO applications, an identity bridge isn't used and user credentials are sent to PingOne Directory. See Basic SSO (password vaulting) and Federated SSO with PingOne for Enterprise for descriptions.

Create or update an authentication policy

An authentication policy enables you to use PingID to provide a secondary level of authentication (multi-factor authentication) to the single sign-on (SSO) process for your users, or for some subset of your users.

About this task

By default the policy is applied to all users and all applications, but you can filter the policy by user group, IP, and application.

The authentication policy is applied to any new SSO sessions for SAML or OpenID Connect applications. Applications that have been added to PingOne that use Basic SSO or an SSO URL cannot be included in the authentication context for the policy.

Once enabled, your PingOne authentication policy works in conjunction with any PingID policies you have configured. For more information, see PingID policy overview.

> **Note**
>
> Changing to a different identity bridge can break any group filtering you include in your authentication policy. In this case, you will need to update your group assignments at **Users > User Groups** and change the group filtering for your policy. For more information, see Managing users by group.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Setup > Authentication Policy**.
2. Select **Enable Authentication Policy**.
3. Select PingID as the authentication provider to use for the policy.

   If you don't select PingID here, no PingID policies will be applied for PingOne SSO.

Authentication Filter

1. For **Apply policy to**, select a filter to define how the policy is to be applied:

   Choose from:

   - **Selected groups**. Applies the authentication policy only to users who are members of the selected groups.
   - **All IPs except**. Applies the authentication policy to all users except those whose IP address is specified or contained within a block of IP addresses. The addresses need to be IPv4 addresses in dot-decimal format (123.123.123.123), or an IPv4 address block in CIDR format (123.123.123.0/24).
   - **All cases**. Applies the policy to all users. This is the default option.

PingOne Admin Portal Configuration

1. Select **Apply authentication policy to PingOne Admin Portal** to apply this policy to administrators who sign on through the PingOne admin portal.

   > **Note**
   >
   > This option is displayed only if you've upgraded to the new PingOne dock. Go to **Dock > Configuration** to upgrade the dock.

2. **Optional:** If you don't want to apply the policy to a specific user, such as a global administrator, select the user from the **Do not apply authentication to** dropdown list.
3. Select how you want SSO administrators to authenticate.

   Choose from:

   - Select **SSO username** to prompt SSO administrators to authenticate using the PingID factors required for SSO users.
   - Select **Email** to prompt SSO administrators to authenticate using the factors required for them to sign on to the admin portal.

Authentication Policy Context

1. Select the **Apply to all sign-on attempts** box to apply the policy to all attempts to SSO to SAML applications. Clear the box to apply the policy only to select applications.

   When you select this option, you do not need to select applications for the **Apply on application launch** option.

   For more information, see Configure an app or group-specific authentication policy in PingID documentation.

2. **Optional:** Enter a search term in the text box to filter application by name.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Do not use the underscore (_) or percent (%) characters in your search filter entry.

3. Select the checkboxes for the applications you want to apply the policy to at launch.

   You must select at least one application if you did not select **Apply to all sign-on attempts**.

4. Click **Save**.

   Result:

   The authentication policy is applied to all new user SSO sessions.

Next steps

You can now configure PingID policies to further refine your secondary level of authentication. For more information, see Configure web authentication policy.

If want to apply the authentication policy to the admin portal, see SSO to the PingOne for Enterprise admin portal with multi-factor authentication.

If you're using the PingFederate identity bridge, refer to SSO to the PingOne for Enterprise admin portal from PingFederate.

Disable an authentication policy

About this task

To disable an authentication policy:

Steps

1. Select **Setup > Authentication Policy**.
2. Deselect **Enable Authentication Policy**.
3. Click **Save**. The policy is disabled, and the authentication policy change is applied to all new user SSO sessions.

Certificate management

PingOne for Enterprise uses signing certificates to sign single sign-on (SSO) messages sent from PingOne for Enterprise.

Signing certificates created in PingOne for Enterprise are self-signed by default. You can also create a certificate signing request (CSR) in PingOne for Enterprise and send the certificate for signing by a certificate authority (CA).

PingOne for Enterprise uses verification certificates to verify the signature on SSO messages received by PingOne for Enterprise. Your SSO partner provides you with a primary and (optionally) a secondary verification certificate. The secondary verification certificate allows for seamless rollover of signature verification in the event that your SSO partner switches certificates. PingOne for Enterprise first attempts to validate a signature using the primary verification certificate. If verification fails, PingOne for Enterprise will then attempt to use the secondary verification certificate, where defined.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Verification certificates are not supported for applications using SAML v1.1

When you sign on to the PingOne for Enterprise admin portal, the **Dashboard** notification area displays an alert for certificates that are about to expire or have expired.

A yellow alert indicates:

- One or more signing certificates are due to expire in the next three months
- A primary verification certificate is about to expire (and will be replaced by a secondary verification certificate, if available)
- A secondary verification certificate is about to expire
- An encryption certificate is about to expire

A yellow alert for expiring certificates creates a link to the **Certificate Management** page.

A red alert indicates a certificate has expired. The alert contains a link to the **Certificate Management** page.

In addition to **Dashboard** messages, PingOne for Enterprise notifies Global Administrators and SaaS Administrators about expiring certificates by email. Notification emails are sent 60 days, 7 days, and 1 day before a certificate expires, and again after the certificate expires.

For more information about email notification preferences, see Editing administrative roles, permissions, and notifications.

View certificate details

You can use the **Certificates** tab to view certificate properties and the application connections or identity bridge associated with a specific signing certificate, verification certificate, or encryption certificate.

About this task

The certificate expiry date is displayed in the right hand column of the entry. For signing certificates, you can also generate a signing certificate request (CSR).

Steps

1. In the PingOne admin portal, click **Setup > Certificates**.
2. Select the type of certificates that you want to view. By default, all certificates are displayed.
3. Click to expand and display the certificate details for a selected certificate.
4. You have these options:

   Choose from:

   - **Properties**. View certificate properties, including type, issue date, serial number, Issuer and Subject DN, and the SHA1 and SHA256 fingerprints.

Copyright © 2025 Ping Identity Corporation

Click **Make Default** to make this the default signing certificate for new application connections.

- **Usage**. View the application connections or identity bridge associated with the certificate. Click a connection or identity bridge to switch to another certificate (signing certificates), upload a new certificate (verification certificate) or upload a new encryption certificate.
- **CSR**. (Signing certificates only). Generate a certificate signing request, and import the CSR response.
- **Share**. Share the certificate via email. You're prompted for the user's email address and the user is sent a download link for the certificate.
- **Download**. Download the certificate to the default download location used by the browser.

Download or share a certificate

You can download a public verification, signing, or encryption certificate; or share it with others via email.

About this task

> **Note**
>
> For security reasons, PingOne doesn't allow exporting the private key of signing certificates.

Steps

1. Go to **Setup > Certificates**.
2. **Optional:** Click the **All Certificates** drop-down to filter certificates by type.
3. Expand the certificate and click either:

   Choose from:

   - **Download** to download the certificate.
   - **Share** to email the certificate to one or more email addresses.

Create a signing certificate

To create a new signing certificate, you specify the certificate settings and the certificate key settings.

About this task

You can also use the signing certificate to create a CSR.

> **Note**
>
> Security is a function of the combination of algorithm and key size. A larger key size provides higher security but may take longer to sign messages.

Steps

1. In the PingOne admin portal, go to **Setup > Certificates**.

Copyright © 2025 Ping Identity Corporation

2. Click **+Add** > **Create Certificate**.
3. Under the **Certificate Settings** tab, enter the certificate information:
    - **Common name**. The common name (CN) identifying the certificate.
    - **Organization**. The organization (O) or company name creating the certificate.
    - **Organizational Unit**. The specific unit within the organization (OU).
    - **City**. The city or other primary location (L) where your organization operates.
    - **State**. The state (ST) or other political unit encompassing the location.
    - **Country**. The two-letter ISO code for the country where your organization is located (such as US, GB, CA).
    - Select **Make certificate default** to make this the default certificate for new application connections.
4. Specify the certificate key settings:
    - **Validity (Days)**. The number of days until the certificate expires (defaults to 365).
    - **Key Algorithm**. The algorithm used to generate a key (RSA or ECC). Defaults to RSA.
    - **Key Size (Bits)**. The number of bits used in the key. Defaults to 2048.
    - **Signature Algorithm**. The algorithm used to generate a signature. Defaults to RSA SHA256.
5. Click **Save**.

    Result:

    The certificate appears in the certificate list.

Importing a certificate and key pair

Add an imported key pair and certificate to use as a signing certificate for PingOne for Enterprise.

About this task

The imported certificate file must meet the following criteria:

- The certificate file must be a PKCS12 file in `.p12` or `.pfx` format
- The certificate must have a key length of 2048 bits or greater
- The certificate must be encrypted using SHA-256 or better
- The certificate must not be expired

> **Important**
>
> PingOne for Enterprise can't accept certificate files created with OpenSSL 3.0.1. Use OpenSSL 1.1.1 or LibreSSL 2.8.3 instead.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Setup > Certificates**.
2. Click **Add > Import KeyPair/Cert**.
3. In the **Password** field, enter the password used to protect the PKCS12 file.
4. **Optional:** Select the **Make certificate default** checkbox to make this the default signing certificate.
5. Click **Select a file** and choose a key store file to import.
6. Click **Upload**.

View and change certificate usage

You can view a list of the application connections and the identity repository associated with a signing, verification, or encryption certificate in the **Certificates** menu.

About this task

> **Note**
>
> Signing certificates can be associated with multiple application connections.

Steps

1. Click **Setup > Certificates**.
2. In the row for the certificate that you want to view, click to expand the details.
3. Click **Usage**.

   Result:

   A list of application connections or the identity repository associated with the certificate is displayed.
4. Click an application connection to open an Update Certificate window.
5. Change an application connection or identity repository.
    1. For signing certificates, you have the option to select a different signing certificate, if available. For more information, see Updating a signing certificate
    2. For verification or encryption certificates, you have the option to replace the certificate by uploading a new verification or encryption certificate. For more information, see Updating a verification certificate or Update an encryption certificate.

Updating a signing certificate

In the event that a signing certificate expires or is about to expire, you must update the certificate. You must update the certificate for both application connections and your identity bridge.

Copyright © 2025 Ping Identity Corporation

You can:

- Update an individual connection. Access the connection in the My Applications list and update its signing certificate.
- Update multiple connections. Access the certificate and update each connection associated with it via certificate management.
- Update a signing certificate for a SAML-based identity bridge.
- Update a signing certificate by issuing a certificate signing request and sending it for signing by a Certificate Authority.

> **Caution**
>
> You should coordinate the update of a signing certificate with your Service Providers to ensure that the update does not trigger an outage. We recommend that you contact the SPs before scheduling the update. While it is easy for SPs with self-service capabilities to update their signing certificate, you may need to supply other SPs with the new certificate using other means and coordinate the timing with them, before performing the update.

Update a signing certificate for application connections

You can view and update a signing certificate either for an individual application or in bulk.

About this task

> **Caution**
>
> Before you update the signing certificate with a connection, you must coordinate with your SP to make sure they have the latest signing certificate. If the SP does not have the updated signing certificate in their system, users will not be able to SSO into the application.

Steps

1. Go to **Setup > Certificates**.
2. In the certificates list, expand the certificate you want to change and click **Usage** to display a list of application connections associated with the certificate.
3. Update a signing certificate.

   Choose from:

   - To update the certificate for an individual application:
     1. Click the name of the application to open the **Update Certificate** window.
     2. Select a new certificate from the **Select a Signing Certificate** list.
     3. Click **Save**.
   - To update the certificate for multiple applications:
     1. Select the box for each application you want to update.
     2. Click **Update Selected** to open the **Update Certificate** window.
     3. Select a new certificate from the **Select a Signing Certificate** window.

Copyright © 2025 Ping Identity Corporation

4. Click **Save**.

   Result:

   A message is displayed to indicate the certificate has been successfully assigned to the application connection. The applications no longer appear in the list of applications to update.

4. When you've updated all application connections, you can delete the expired (or expiring) certificate by clicking the **Delete** icon.

   Result:

   The signing certificate is removed from the certificates list.

Updating a signing certificate for an identity repository

If the current signing certificate for your identity provider (IdP) is nearing expiration, you can replace it with a new certificate.

Before you begin

If you want to create a new signing certificate to use for your IdP, see Create a signing certificate.

About this task

You can update a signing certificate for the following IdPs:

- PingFederate
- Microsoft AD FS
- a custom SAML provider

If the certificate in question is the PingOne for Enterprise universal certificate, you do not need to update this certificate if you're using any other identity repository.

> **Note**
>
> If your connection from PingFederate to PingOne for Enterprise is a managed connection, you must manually upload the new signing certificate to PingFederate Bridge. This is only needed if PingOne for Enterprise is signing the AuthnRequest to PingFederate. For more information, see Importing a certificate and its private key in the PingFederate documentation.

Steps

1. In the PingOne for Enterprise admin console, go to **Setup > Certificates**.
2. In the list of certificates, expand the certificate you want to expand.
3. Click **Usage**, and then click the name of the IdP.

   Result:

   The **Certificate Update** dialog appears.

4. In the **Select a Signing Certificate** list, select a new certificate to use for the IdP connection.
5. Click **Save**.

Copyright © 2025 Ping Identity Corporation

Result:

The **Certificates Successfully Updated** dialog confirms that the certificate renewal was successful.

6. Click **Okay**.

Check whether you need to update the PingOne for Enterprise universal certificate

You may need to update the PingOne for Enterprise universal certificate if you're using PingFederate, Microsoft Active Directory Federation Service (AD FS), or a custom SAML provider as your identity bridge

About this task

In this case, it is imperative that you update the certificate if your configuration requires either:

- Signed AuthN requests.
- SAML single logout (SLO; either IdP-initiated or SP-initiated.

> **Note**
>
> You do not need to update the PingOne universal certificate if you're using an identity repository other than PingFederate, Microsoft AD FS, or a custom SAML provider.

Check the **Dashboard** in the PingOne for Enterprise admin portal to see whether a certificate is due to expire. For more information, see Certificate alerts.

PingOne for Enterprise will also send you an email notifying you when the universal certificate is nearing expiration.

If you use Microsoft AD FS or a custom SAML provider as your identity repository, you will need to check your configuration.

If the identity repository is configured to use either SLO (IdP-initiated or SP-initiated) or signed AuthN requests, you will need to update the PingOne universal certificate.

Steps

1. If PingFederate Bridge is your identity repository, check whether PingFederate Bridge is configured to sign AuthN requests or use SLO:
    1. Log in to the PingFederate Bridge console.
    2. On the left navigation menu, click **Identity Provider**.
    3. Click **Connections > PingOne** to show the connection summary.
    4. In the summary under Browser SSO, check the **IdP-Initiated SLO** and **SP-Initiated SLO** settings.

       If either setting is `True`, you will need to update the PingOne universal certificate.
    5. Scroll down toward the bottom of the summary to **Protocol Settings**. Check the setting for **Require digitally signed AuthN requests**.

       If this setting is `True`, you will need to update the PingOne universal certificate.

       Result:

Copyright © 2025 Ping Identity Corporation

If the configuration doesn't use SLO and doesn't require signed AuthN requests, you do not need to update the PingOne universal certificate.

Result

To update the PingOne universal certificate, follow these instructions: Updating a signing certificate for an identity repository.

Sign a certificate using a CSR

About this task

You can generate a Certificate Signing Request (CSR) using a signing certificate that you created. In the PingOne for Enterprise certificate management page, download the CSR for the relevant certificate, and then send it to your Certificate Authority (CA). The CA will send back a CSR response which you can upload to PingOne for Enterprise. Once it is uploaded, your certificate is updated to the version signed by the CA.

Steps

1. Click **Setup > Certificates**.
2. In the certificate list, expand the relevant entry and click **CSR**.
3. Click **Export** and navigate to the location at which you want to save the CSR response.
4. Upload the CSR to the relevant CA for signing.

   Result:

   The CA signs the certificate and sends you a CSR response.
5. Click **Import**, navigate to the CSR response and click **OK**.

   Result:

   The CSR response is imported and saved. When PingOne for Enterprise uses the certificate to sign SSO messages (SAML assertions) it uses the updated certificate signed by the CA.

Updating a verification certificate

In the event that a verification certificate expires or is about to expire, you must update it.

You can update:

- An application verification certificate using SAML 2.0 or later
- A verification certificate associated with an identity provider (IdP)

Copyright © 2025 Ping Identity Corporation

Application Certificate

Updating an application verification certificate
About this task

When a verification certificate expires or is about to expire, generally you must upload a new verification certificate.

Steps

1. In the PingOne for Enterprise admin portal, go to **Setup > Certificates**.
2. Expand the relevant certificate and click the **Usage** tab.
3. Click the application for which you need to update the verification certificate.

   Result:

   The **Replace Primary Certificate** popup window opens, prompting you to upload the new verification certificate.

   > **Note**
   >
   > If the certificate is used as a secondary verification certificate, the popup window is called **Replace Secondary Certificate**.

4. Click **Choose File** and browse to the location of the new verification certificate.

   Result:

   A message is displayed to indicate the certificate has been successfully updated for the application.

Copyright © 2025 Ping Identity Corporation

IdP Certificate

Updating an identity repository verification certificate
About this task

You can update a verification certificate for a PingFederate Bridge manual connection, Microsoft Active Directory Federation Services (AD FS), or a custom SAML identity repository. If a verification certificate expires or is about to expire, you must obtain an updated certificate from the identity repository.

If a secondary certificate is defined and you have not yet received an updated primary verification certificate, PingOne for Enterprise can validate a signature using the secondary certificate.

In most cases, you must replace the primary verification certificate with the secondary verification certificate. Do this when your single sign-on (SSO) partner confirms they are no longer signing messages with the certificate previously assigned as the primary verification certificate.

Steps

1. In the PingOne for Enterprise admin portal, go to **Setup > Certificates**.
2. Expand the relevant certificate and click the **Usage** tab.
3. Click the identity repository for which you need to update the verification certificate.

   Result:

   The **Replace Primary Certificate** popup window opens, prompting you to upload the new verification certificate.

   > **Note**
   >
   > If the certificate is used as a secondary verification certificate, the popup window is called **Replace Secondary Certificate**.

4. Click **Choose File** and go to the location of the new verification certificate.

   Result:

   A message opens to indicate the certificate has been successfully updated for the identity repository.

Result

The identity repository is updated with the new verification certificates.

Update an encryption certificate

About this task

You can update the encryption certificate used for an application connection. You'll need to be able to browse to the new certificate file to use.

Steps

1. In the PingOne admin portal, click **Setup > Certificates**.

Copyright © 2025 Ping Identity Corporation

2. In the certificate list, filter the list to display only encryption certificates.
3. Expand the entry for the encryption certificate to update and click **Usage**.

The application connections using the encryption certificate are displayed.

1. For each application or application connection displayed, click the application and browse to select the new encryption certificate to be used for the application or application connection.
2. Click **Save**.

Result

The new encryption certificate will now be used for the application or application connections.

Delete a certificate

About this task

You must ensure there are no dependent connections before deleting a signing certificate. If there are active applications, application connections, or an identity bridge, the signing certificate cannot be deleted.

> **Note**
>
> If no connection is associated with a verification or encryption certificate, the certificate is automatically deleted.

Steps

1. In the PingOne admin portal, click **Setup** > **Certificates**.
2. In the certificate list, expand the relevant entry and click the Delete icon.

Monitoring PingOne for Enterprise use

Use the reports and subscription tools to monitor PingOne for Enterprise user activity.

Reports return a one-time report of data using either predefined or custom reports. PingOne for Enterprise logs events per report type and retains the logs for 1 year. For a list of the available event data, see PingOne for Enterprise report types.

Subscriptions generate recurring reports of audit events for a report type. For example, you might create a subscription to the Administrator Login report type to receive the event data for each time a PingOne for Enterprise administrator signs on. A subscription can be either a Push or Poll type. See Subscriptions for more information.

You can view a list of users filtered by services such as single sign-on (SSO) and multi-factor authentication (MFA). For more information, see Monitoring service activity.

Your PingOne for Enterprise billing is partially determined by the number of SSO transactions in your environments. For more information about monitoring SSO activity, see PingOne for Enterprise usage monitoring.

Copyright © 2025 Ping Identity Corporation

Monitoring service activity

You can view a list of users by service, filter the list by a specific service, or search for a specific user.

Steps

1. Go to **Users > Users by Service**.

   Result:

   The **Users by Service** page displays users for all services. By default, each user entry lists all services associated with that user. Hover over a service to view its full name.

2. Filter the user list by one of the following methods:

Option	Description
Click the service name.	Displays a list of all users associated with the selected service.
Enter the username in the **Search** bar.	Displays the user associated with that username. **Note** If you filter the list by a specific service, the search returns results only for users of that service.

3. Click the **Expand** icon for any user.

   Result:

   Expanding the service entry displays the last activity for that user and, for single sign-on (SSO), the last sign-on.

   If more than one service is shown for the user, you can expand each service to see the last activity details.

4. Click the **View all activity** link to generate a report of all activity by this service for this user.

Reports

You can choose to run a predefined report or run a custom report by modifying predefined report parameters.

Create an 'on the fly' report to view event data information per report type, for a specific time period, or run one of the predefined reports provided. We provide a number of predefined reports for your convenience. The predefined report is based on a specific report type.

You can specify that the results are displayed relative to a particular time zone. You're also able to filter results based on the event data for the report type (such as, `Action` or `Admin Id`).

You can select which of the available event data you want to include in the report, and export a copy of the report in `.csv` format.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> The amount of data that can be exported for a report is determined either by duration or quantity. The exported data is limited to either one week's data or 500,000 lines of data. We will use the smaller of the two values.

PingOne for Enterprise report types

The `Report Type` parameter controls the type of report to produce or the audit event type to use for a subscription.

> **Note**
>
> Some of the types are for reports only and are not used for subscriptions, as indicated.

The following report types are available for PingOne for Enterprise and PingOne for Enterprise for Managed Service Providers.

For report types available on PingOne SSO for SaaS Apps, see PingOne SSO for SaaS Apps report types.

PingOne for Enterprise report types

Report Name	Description
AD Connect	AD Connect connection and disconnection events from the PingOne for Enterprise hosts during a specific period.
Administrative Activity	Transactions initiated by a PingOne for Enterprise administrator during a specific period. If a Ping Support administrator accesses your account and makes a requested change, an audit event is triggered for that change. Both the **Admin** and **Admin Type** will be `Ping Identity Support`. For PingOne for Enterprise for Managed Service Providers accounts, if an administrator accesses a customer account and makes a change, an audit event is triggered for that change. The actor associated with the audit event will be the name of the administrator and the type will be `msp admin`.
Administrative API (Reports only)	Transactions initiated through the PingOne for Enterprise Admin API during a specific period.
Administrator Login	Sign on attempts by administrators and their success or failure during a specific period.
Directory	Audit events related to any user change within the PingOne for Enterprise Directory during a specific period.
Log Subscription (Reports only)	Audit events related to the creation, update, and deletion of audit log subscriptions during a specific period.
PingID	PingID authentication provider transactions during a specific period.
PingID Administrative Activity	PingID transactions initiated by a PingID administrator during a specific period.

Copyright © 2025 Ping Identity Corporation

Report Name	Description
PingID User Detailed Status Report(For export only)	Detailed information regarding the status of the PingID transaction, including PingID registration, pairing, and authentication. For successful authentication, the method used to authenticate (such as swipe, or fingerprint) is included.
Provisioning	User provisioning transactions during a specific period.
SafeNet (Reports only)	SafeNet authentication provider transactions during a specific period.
SSO	Transactions for Federated SSO during a specific period. **Note** For SAML applications, if an SSO failure is included in a report, you can click on the failure code to display a popup containing the SAML assertion.
SSO Summary (Reports only)	The count of unique users and the total number of SSO transaction events during a specific period for each application configured for your organization.
SSO User Summary	A list of all unique users who used SSO during the specified period. **Note** This report is based on **Users by Service** data. If you remove SSO users from **Users by Service**, they will not appear in this report until the next time they use SSO.

PingOne for Enterprise for Managed Service Provider report types

In addition to the above reports, the following report types are available on PingOne for Enterprise for Managed Service Providers:

Report Name	Description
PingID SDK	PingID device user transactions during a specific period.
PingID SDK Administrative Activity	PingID device user transactions initiated by a PingID administrator during a specific period.
SSO Summary by Customer	The count of unique users and the total number of SSO transaction events during a specific period for each of your customer accounts.

PingOne for Enterprise report event reference

The following table describes the event data types found in PingOne for Enterprise reports.

For more information about report types, see PingOne for Enterprise report types.

Copyright © 2025 Ping Identity Corporation

Event Data	Report Type	Event Data Description
Account ID	**PingID Consumer**	The applications used for single sign-on (SSO).
Action	• **Administrative Activity** • **Directory** • **Log Subscription** • **PingID Administrative Activity** • **PingID SDK Administrative Activity**	The action performed by the audited user.
Admin	• **Administrative Activity** • **PingID Administrative Activity** • **PingID SDK Administrative Activity**	The email address or LDAP name assigned to the administrator.
Admin Id	**Administrative Activity**	The unique identifier assigned by PingOne for Enterprise to the administrator.
Admin Type	• **Administrative Activity** • **Directory** • **PingID Administrative Activity** • **PingID SDK Administrative Activity**	The type of administrator. **Note** The type of administrator is `user` unless the action was performed by a Ping Identity employee.
Application	**SSO Summary**	The applications used for SSO.
Application ID	• **SSO** • **Basic SSO** • **PingID Consumer**	The identifier assigned to the application used for SSO.
Application Name	• **SSO** • **Basic SSO** • **PingID Consumer**	The name of the application used for SSO.
Application Subject	• **Provisioning** • **PingID Consumer**	The contact email address for the application's service provider (SP).

Copyright © 2025 Ping Identity Corporation

Event Data	Report Type	Event Data Description
Browser Agent	• **Administrator Login** • **Administrative Activity** • **SSO** • **Basic SSO** • **PingID Consumer**	The browser name and version used for SSO.
Connection ID	• **SSO** • **Basic SSO** • **PingID Consumer**	The unique identifier assigned to the PingOne for Enterprise connection used for SSO.
Country	**SSO**	The country where the SSO event originated.
Identity Repository Subject	• **Provisioning** • **PingID Consumer**	The contact email address for the application's identity provider (IdP).
IdP ID	• **SSO** • **Basic SSO** • **PingID Consumer**	The unique identifier assigned to the identity repository used for user authentication.
IP Address	• **Administrator Login** • **Administrative Activity** • **SSO** • **Basic SSO** • **PingID Consumer** • **Safenet** • **Administrative API**	The IP address of the host used to initiate the transaction.
Message	All report types	A PingOne for Enterprise message providing information related to the transaction.
Resource Id	**Administrative Activity**	The unique identifier assigned by PingOne for Enterprise to the PingOne for Enterprise resource.

Copyright © 2025 Ping Identity Corporation

Event Data	Report Type	Event Data Description
Resource Name	• **Administrative Activity** • **Directory** • **Log Subscription** • **PingID Administrative Activity** • **PingID SDK Administrative Activity**	The display name for the PingOne for Enterprise resource upon which an action was performed.
Resource Name 2	• **Administrative Activity** • **Directory** • **Log Subscription** • **PingID Administrative Activity** • **PingID SDK Administrative Activity**	The display name for an additional PingOne for Enterprise resource upon which an action was performed.
Resource Name 3	• **Administrative Activity** • **Directory** • **Log Subscription** • **PingID Administrative Activity** • **PingID SDK Administrative Activity**	The display name for an additional PingOne for Enterprise resource upon which an action was performed.
Resource Type	• **Administrative Activity** • **Directory** • **Log Subscription** • **PingID Administrative Activity** • **PingID SDK Administrative Activity**	The type of PingOne for Enterprise resource upon which an action was performed.
Resource Type 2	• **Administrative Activity** • **Directory** • **Log Subscription** • **PingID Administrative Activity** • **PingID SDK Administrative Activity**	The type of PingOne for Enterprise resource for **Resource Name 2** upon which an action was performed.

Copyright © 2025 Ping Identity Corporation

Event Data	Report Type	Event Data Description
Resource Type 3	• **Administrative Activity** • **Directory** • **Log Subscription** • **PingID Administrative Activity** • **PingID SDK Administrative Activity**	The type of PingOne for Enterprise resource for **Resource Name 3** upon which an action was performed.
SP Account ID	• **SSO** • **Basic SSO** • **PingID Consumer**	The unique identifier for the SP's PingOne for Enterprise or PingOne SSO for SaaS Apps account.
Status	All report types	The current status of the transaction. Possible status values are: ***IDP_DONE*** The user was authenticated by the configured IdP and PingOne for Enterprise has received an assertion from the IdP. ***SUCCESS*** The user was successfully redirected to the target application. ***FAILURE*** SSO was not successful. ***OIDC_TOKEN*** The OpenID Connect (OIDC) token request was processed. ***OIDC_USERINFO*** The OIDC UserInfo request was processed. ***OIDC_INTROSPECT*** The OIDC token introspection request was processed.

Copyright © 2025 Ping Identity Corporation

Event Data	Report Type	Event Data Description
Subject	• **Administrator Login** • **SSO** • **Provisioning** • **Basic SSO** • **PingID** • **Directory** • **Administrative API**	The email address for the user initiating the transaction. For SSO and Provisioning, this is equivalent to the **Identity Repository Subject**.
Timestamp	All report types	The date and time for the current reporting data.
Total SSO Transactions	**SSO Summary**	The total number of SSO transactions attempted for the reporting period.
Tracking ID	• **SSO** • **Administrative API**	A unique identifier for the transaction. The **Tracking ID** can be used by PingOne for Enterprise to troubleshoot issues if necessary.
Unique Users	**SSO Summary**	The total number of unique users attempting SSO for the reporting period. Subsequent attempts by the same user aren't included in the total.

Run a predefined report

About this task

We provide a number of predefined reports for commonly used data. You can run any of these reports without alteration, or modify the report parameters to customize the report as needed.

Steps

1. From the Dashboard, click **Reporting > Reports**.

   Result:

   A list of predefined reports is displayed.

2. Select the predefined report you want to run. You can click the edit icon to expand and show the report parameters. Click **Run**.

   Result:

   The report parameters and results are displayed.

Copyright © 2025 Ping Identity Corporation

3. You also can modify the report parameters and run the report again for a different set of results:
    1. To filter results, in the **Filter** entry for the selected report type, enter the name of a logged Subject value and click **Run**.

       If the report includes more than one subject value, the report filter is applied to the **SUBJECT_BY_IDP** field only.
    2. To change the fields displayed in the report results, click **Show Options** and in the **Select Fields** dropdown list select each field you want to show in the results. Click **Run** to update the displayed results.
    3. To change the reporting time zone used for the report, click **Show Options**, select the appropriate time zone from the dropdown list, and click **Run** to update the displayed results.
    4. For SSO reports, you can also use the **Application Name** dropdown list to select an application as the target of the report.
4. To export the report in `.csv` format, click **Export**. The report is saved in your browser's default downloads folder.

   Exporting the report to `.csv` may take several minutes to complete, depending on the size of the report.

   > **Note**
   >
   > The amount of data that can be exported for a report is determined either by duration or quantity. The exported data is limited to either one week's data or 500,000 lines of data. We will use the smaller of the two values.

   Next steps

   If needed, modify the report parameters and run the report again.

Run a custom report

About this task

You can define and run a custom report, defining the report type, and other parameters as required. This gives you greater flexibility than the predefined report. However, unlike a predefined report, you need to reset the specific parameters each time you run the custom report.

Steps

1. From the Dashboard, click **Reporting > Reports**.
2. Click **Run New Report**.

   Result:

   The available report parameters are displayed.
3. In the **Report Type** dropdown, select the type of report you want to run.
4. In the **Time Range**field, select either:

   Choose from:

   - **Specific Date** and then select the dates you want the report to start and end respectively.

Copyright © 2025 Ping Identity Corporation

- **Relative**: enter a value and units (for example, Days, Weeks, or Minutes) representing a relative time frame from the current date and time.

5. (Optional) Select a time zone from the dropdown list to change the default time zone.
6. To filter the **Subject** field for the selected report type, enter the subject in full and click **Run**.

If the report includes more than one subject field, the report filter is applied to the **IdP Subject** field only.

1. To change the fields displayed, in the **Report Parameters** area, click **Show Options**, and then in the **Select Fields** dropdown list select the checkbox for the event data you want to show in the results (all fields are selected by default). Click **Run** to update the results table.
2. To change the reporting time zone in the **Report Parameters** area, click **Show Options**, select the time zone you require from the dropdown list, and click **Run** to update the results table.

   The default time zone is defined in the **User Settings**.
3. To limit the event data displayed in the results, click **Show Options**and in the **Select Fields** section click the **Selected** dropdown. Select from the event data available for the report.
4. To change the reporting time zone used for the report, click **Show Options**, select the appropriate time zone from the dropdown list, and click **Run** to update the displayed results.
5. For SSO reports, you can also use the **Application Name** dropdown list to select an application as the target of the report.
6. Click **Run**. The report is run and the results displayed.
7. To modify the report, in the **Report Parameters** area, change the parameters as required and click **Run** to refresh the results.
8. To export the report in `.csv` format, click **Export**. The report is saved in your default download folder.

> **Note**
>
> The amount of data that can be exported for a report is determined either by duration or quantity. The exported data is limited to either one week's data or 500,000 lines of data. We will use the smaller of the two values.

Subscriptions

PingOne audit events are available through a subscription facility.

The subscriptions can be either:

- A Push type, where PingOne for Enterprise streams audit events to an external service in real time.
- A Poll type, where your client retrieves audit events as needed in configurable blocks of records, until all retrievable records are consumed.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Audit events that occurred prior to a subscription being created are not delivered. Only audit events occurring after the subscription is created are delivered.
> However, if you create another subscription of the same type, you will have access to events that occurred prior to that subscription, because those events were already being tracked.

Each audit event for a subscription is retained for seven days. After that time, if you haven't already received or retrieved the audit event record, it will not be available.

PingOne attempts to deliver an audit event message for both types of subscriptions. You might receive duplicate messages because of streaming retries or very frequent polling. Each audit event message includes a unique `id`, so you can easily identify duplicate messages.

Push subscriptions

Push subscriptions push events to the target server in real time.

The audit events matching the subscription are streamed to the HTTPS endpoint configured for the subscription.

The uploaded certificate must match what an external client would see when accessing the configured URL. Be aware of load balancers or other network devices that might present a different certificate.

The audit event information can be returned in either the PingOne audit format or a include::ROOT:partial$p14e_p1refs_splunk.adoc[tags=Splunk]-compatible format. Both formats are JSON.

If the delivery of a Push audit event fails, PingOne will continue to retry delivery. The interval period between retries will increase to a maximum of 15 minutes. PingOne for Enterprise will retry to deliver for 7 days and then discard the event.

If events aren't arriving as expected, check the reports at **Dashboard > Reporting > Run New Report**. Choose **Log Subscription** as the type and check for errors. For example, certificate-related exceptions indicate that the certificate being presented does not match the certificate on file in PingOne for Enterprise.

Poll subscriptions

Poll subscription audit events are accumulated and made available to you. You must use a script or client to retrieve the audit events. The client can retrieve the events, up to the configured batch size specified for the subscription.

Poll subscription audit events are collected and returned once per subscription. This means that each poll retrieval will have a different result set.

The audit event information is returned in the PingOne audit format.

An easy way to retrieve the audit events for a poll subscription is to use `cURL`. For instructions on how to create a cURL command, see Get the audit events for a Poll subscription.

Estimate how much traffic you expect to generate and set your poll rate and batch size accordingly. Leave some extra room in your batch size, because some transactions can generate multiple events. For example, if you have 1000 users authenticating per hour, it will generate from 1000 to 3000 events. For this traffic level, you can set a batch size of 1000 and poll every 20 minutes, or a batch of 200 and poll every four minutes. You should poll at least hourly, even with lower usage.

The number of audit events accumulated may be less than the batch size. The configured batch size is an upper limit, not a consistent number of returned events.

Copyright © 2025 Ping Identity Corporation

A poll request with zero results means that you are caught up to the present and there are no new events. Your poll rate should be set so that this happens regularly.

Polling events are returned in roughly chronological order from oldest to newest. To ensure strict chronological order, set your client to sort events by timestamp.

Events are stored for 7 days and then discarded. You must ensure that your client doesn't fall more than 7 days behind, or you will lose data.

If you do fall behind and events begin to backlog, batch size and sorting can become less consistent. For example, if your batch size is 1000 and you fall a week behind in polling, you might get responses with 600-700 events, with older events grouped in with new ones. This doesn't mean that events are missing. All events are available and will be returned as your collector catches up. But they won't be in consistent order.

Choosing Push or Poll

Poll subscriptions give the client control over the rate at which events are collected and saved to your storage system, but the client is responsible for ensuring it doesn't fall behind.

Push subscriptions are not batched, and therefore generate more traffic because they generate one request per event. Your target system must be able to handle the traffic load.

We generally recommend Push subscriptions because they are simpler, especially if you have large amounts of traffic (in the tens of thousands of events per hour), which can make it difficult to determine the right poll frequency.

Adding a Push subscription

Push subscriptions stream audit events of the selected type to the HTTPS URL you specify.

Steps

1. Go to **Dashboard > Reporting > Subscriptions > Add Subscription**.
2. In the **Name** field, enter a name for this subscription.
3. In the **Type** list, select the type of audit event that will be pushed for this subscription.

   For more information, see PingOne for Enterprise report types.
4. Select **Push** to create a Push subscription.
5. In the **Format** list, select the format for the audit events.

   For Push subscriptions, this can be either:

   - `Audit` (the PingOne for Enterprise default format).
   - `Splunk` (a format compatible with Splunk processing).

   Both formats are JSON.
6. In the **URL** field, enter the URL to stream audit events to.

> **Note**
>
> The URL must be HTTPS.

Copyright © 2025 Ping Identity Corporation

7. In the **Authorization Header** field, enter a request header that will be posted to the **URL** you specified.

   For example, `"Authorization: Basic 80F4FC1D78C0F15627C9B95C"`.

8. Click **Upload** to upload the public certificate registered to the **URL** you specified.

   > **Note**
   >
   > For Splunk subscriptions, you need to upload the endpoint certificate, not the entire certificate chain. You can get your endpoint certificate by going to your Splunk endpoint in a browser and downloading it.

9. Click **Done**.

   Result:

   You will find the new subscription listed on the **Subscriptions** page.

Result

The audit events pushed to the URL you specified will look similar to these samples:

`Audit` format

```
{
  "source": "ADMINISTRATOR_LOGIN",
  "id": "8fd3d92f-7af2-11e8-b80d-0ec0fbebxxxx",
  "recorded": "2018-28-06T16:44:44.849Z",
  "action": {
    "type": "Password"
  },
  "actors": [
    {
      "type": "user",
      "name": "pcasso@pingidentity.com"
    }
  ],
  "resources": [],
  "client": {
    "id": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99
Safari/537.36",
    "ipAddress": "192.168.10.1, 172.138.206.50"
  },
  "result": {
    "status": "SUCCESS",
    "message": "Password"
  }
}
```

`Splunk` format

Copyright © 2025 Ping Identity Corporation

```
{
  "event": {
    "source": "ADMINISTRATOR_LOGIN",
    "id": "44990ce5-7af4-11e8-b80d-0ec0fbebxxxx",
    "recorded": "2018-28-06T16:56:57.627Z",
    "action": {
      "type": "Password"
    },
    "actors": [
      {
        "type": "user",
        "name": "pcasso@pingidentity.com"
      }
    ],
    "resources": [],
    "client": {
      "id": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
67.0.3396.99 Safari/537.36",
      "ipAddress": "24.222.35.218, 172.18.26.54"
    },
    "result": {
      "status": "SUCCESS",
      "message": "Password"
    }
  },
  "host": "pingidentity.com",
  "time": 1530205017627,
  "source": "ADMINISTRATOR_LOGIN"
}
```


Add a Poll subscription

About this task

For Poll subscriptions, the audit events of the selected type are accumulated and made available to a client pulling those events. Accumulated audit events are kept for seven days and then discarded.

You can assign an Audit & Report Administrator to manage subscriptions for audit events. For more information, see Assign administrative roles or Assign administrators.

Steps

1. From the Dashboard, click **Reporting > Subscriptions > Add Subscription**.
2. Enter the **Name** to assign to the subscription.
3. Enter the **Type** of audit event that will be polled for this subscription.

   See PingOne for Enterprise report types for the available types.
4. Select **Poll** to create a Poll subscription.
5. Select a **Batch Size** to indicate the maximum number of audit events to get for each call when polling for new audit events.

   The Poll subscription will retrieve the accumulated audit events, up to this batch size.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> The number of audit events accumulated and returned by the subscription can also be less or more than the batch size specified. If the number of audit events exceeds the batch size, the remaining audit events are retrieved by your next call to retrieve the audit events for this subscription.

6. Click **Done**.

You will find the new subscription listed on the Subscriptions page.

Get the audit events for a Poll subscription

Using a script or a client, you can configure a scheduled retrieval of the audit events accumulated for a poll subscription.

About this task

The audit events are kept for seven days and then discarded.

You can assign an Audit & Report Administrator to manage subscriptions for audit events. For more information, see Assign administrative roles or Assign administrators.

These instructions use `cURL` to illustrate audit event retrieval.

Steps

1. From the Dashboard, click **Reporting > Subscriptions**.
2. Select the poll subscription you want and click the expand icon on the right to display the details.
3. Copy the **Poll URL** by clicking the displayed URL.

   This URL contains both your account ID and the poll subscription ID. For example, in this URL:

   ```
   https://admin-api.pingone.com/v3/reports/5733a0b1-ff99-4e59-95e6-58c14831xxxx/poll-subscriptions/
   8ae7c229-5198-40ae-bb68-b67bb46exxxx/events
   ```

   The value that follows "reports/" (in this case, "5733a0b1-ff99-4e59-95e6-58c14831xxxx") is the account ID. The value that follows "poll-subscriptions" is the poll subscription ID (in this case, "8ae7c229-5198-40ae-bb68-b67bb46exxxx").

   You will use the account ID and poll-subscription ID displayed to retrieve the audit events.

4. Create the `cURL` command to retrieve the audit events.
   1. Generate an OAuth token using your API client ID and secret:

      ```
      curl -X POST -d "grant_type=client_credentials&client_id=<clientid>&client_secret=<secret>" https://
      admin-api.pingone.com/latest/as/token.oauth2
      ```

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> To obtain your API client ID and secret, go to **Dashboard > Reporting > API Clients** and expand any existing client to see the **Client ID** and **Client Secret** values.
> If you don't have an existing client, you can generate a new one in order to obtain the client ID and secret. For more information, see Creating an Admin-API client.

2. Use the generated token to retrieve events:

```
curl -H "Authorization: Bearer  <OAuth token>" https://admin-api.pingone.com/v3/reports/<accountId>/
poll-subscriptions/<id>/events
```

The `accountID` is the account ID for your PingOne for Enterprise account. The `id` is the `id` for the Poll subscription. You can find both in the **Poll URL**.

> **Note**
>
> If you are using an admin user to retrieve events, use HTTP Basic authentication with the admin's username and password as shown below. However, we recommend using the OAuth client method.
>
> ```
> curl -X GET --user  <username>:<password>  "https://admin-api.pingone.com/v3/reports/
> <accountId>/poll-subscriptions/<id>/events"
> ```
>
> The `username` and `password` are the credentials for the admin user.

5. Run the `cURL` request from the command line.

The audit events returned in the response will be similar to the following:

Example:

Copyright © 2025 Ping Identity Corporation

```
[
  {
    "source": "ADMINISTRATOR_LOGIN",
    "id": "06cb28fa-3d9c-11e8-9341-0e6804xxxxxx",
    "recorded": "2018-11-04T15:21:37.295Z",
    "action": {
      "type": "Password"
    },
    "actors": [
      {
        "type": "user",
        "name": "jdoenut@pingidentity.com",
        "id": null
      }
    ],
    "resources": [ ],
    "client": {
      "id": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/65.0.3325.181 Safari/537.36",
      "ipAddress": "192.168.10.1"
    },
    "result": {
      "status": "SUCCESS",
      "message": "Password"
    }
  },
  {
    "source": "ADMINISTRATOR_LOGIN",
    "id": "c25191cd-3f27-11e8-be81-0e3810xxxxxx",
    "recorded": "2018-13-04T14:34:23.119Z",
    "action": {
      "type": "Password"
    },
    "actors": [
      {
        "type": "user",
        "name": "jdoenut@pingidentity.com",
        "id": null
      }
    ],
    "resources": [ ],
    "client": {
      "id": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/65.0.3325.181 Safari/537.36",
      "ipAddress": "192.168.10.1"
    },
    "result": {
      "status": "SUCCESS",
      "message": "Password"
    }
  }
]
```


Copyright © 2025 Ping Identity Corporation

Parameter	Description
`source`	The report type that is the source of this audit event. See PingOne for Enterprise report types for descriptions of the report types.
`id`	The UUID of the audit event.
`recorded`	The date that the audit event was recorded. The date format for audit events is: YYYY-DD-MM'T'HH:mm:ss.SSS'Z.
`action`	The action associated with the audit event. The action is described by: ***type*** The type of action performed or submitted.
`actors`	Identifies the actor associated with the audit event. The actor is described by: ***type*** The type of actor. ***name*** The identifier used to uniquely name the actor. ***id*** The ID associated with the actor. This may be null.
`resources`	The resources (if any) accessed by the actor for the audit event.
`client`	Identifies the client used by the actor during the audit event. The client is described by: ***id*** The information used to identify the client. ***ipAddress*** The IP address assigned to the client.
`result`	Identifies the result of the action associated with the audit event. The result is described by: ***status*** The resulting status of the action associated with the audit event. ***message*** A message associated with the result status for the audit event.

Copyright © 2025 Ping Identity Corporation

Creating an Admin-API client

Create an API client to grant dedicated access to subscription endpoints.

About this task

Admin-API clients allow you to grant access to subscription endpoints without creating additional administrator accounts.

> **Important**
>
> The use of the following special characters is forbidden in the **Client Name** and **Description** fields.
>
> ```
> & % \ ' " ; < > + ( ) { } |
> ```

Steps

1. Go to **Dashboard > Reporting > API Clients**.
2. Click **+ Add API Client**.
3. In the **Client Name** field, enter a name.
4. **Optional:** In the **Short Description** field, enter a description .
5. Click **Next**.
6. **Optional:** To generate a new shared secret for this client, click **New Secret**.
7. Click **Done**.

Result

The new client appears on the **API Clients** tab.

Managing your administrators and account

Members of your organization who are assigned the Global Administrator role can manage the PingOne account. If you created the account, you are automatically assigned Global Administrator permissions.

For PingOne for Managed Service Providers, only a Global Administrator can access the **Dashboard** and **Service Settings** pages.

The account management features available to your administrators are determined by the type of account and the administrator roles you assign.

When an assigned administrator first signs on (SSO) to the admin portal, they're added to the list of administrators displayed on the **Account > Administrators** page.

> **Note**
>
> Administrators that SSO into the admin console must have a username that is unique within that PingOne for Enterprise account.
> Administrators who do not SSO into the admin console must use an email address that is unique across all PingOne for Enterprise accounts.

Copyright © 2025 Ping Identity Corporation

Assign administrative roles

PingOne for Enterprise has several levels of administrative access that you can assign.

About this task

The administrators of your PingOne for Enterprise account will have access to the admin portal. The people you invite as administrators do not need to be current users of your account. They'll be added as new users when they accept your email invitation.

You must be a Global Administrator to assign other administrative roles, to disable or delete other administrators, and to access the **Dashboard** page.

> **Note**
>
> You can enable single sign-on (SSO) for admin authentication to the admin portal. The admin portal is then displayed as one of the applications on the PingOne for Enterprise dock for these administrative users. For instructions, see Configuring SSO to the PingOne for Enterprise admin portal.

Steps

1. In PingOne for Enterprise, go to **Account > Administrators** and click **Add Administrator**.
2. In the **First Name** and **Last Name** fields, enter the new admin's name.
3. In the **Email** field, enter the email address to which to send the invitation email.
4. In the **Role** list, choose an administrative role.

   Learn more about administrative roles and permissions in Administrative roles.
5. (Optional) Select **Read Only** to give the administrator the ability to view data and configurations allowed by their role, but not the ability to make system changes.
6. (Optional) Select **SSO Admin** to create an administrator who can access the admin portal only through single sign-on (SSO).

   Selecting this option changes the **Email** field to **Username**. Administrators created with this option won't receive an email invitation, and must access the admin portal by SSO into the PingOne for Enterprise dock.

   > **Note**
   >
   > SSO administrators can't reset their own passwords in PingOne for Enterprise because they don't have passwords. Instead, their passwords are managed at the identity provider (IdP) where they authenticate. SSO administrators won't receive an email when they attempt the password reset flow.

   > **Tip**
   >
   > An email-invited administrator email address must be unique across all PingOne for Enterprise accounts. If an admin's email address is already in use in another account, you can still add them as an admin using the **SSO Admin** checkbox. SSO admin usernames must be unique only within your account.
7. Click **Save**.

Result

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise sends an email invitation to the user you're inviting. The email invite is valid for 3 days, or until a new invitation is sent.

When the user clicks the link in the email to accept the invitation, they're prompted to assign a password for their account. If their account doesn't already exist, the new account is created.

When the new administrator first signs on (SSO) to the admin portal, they are added to the list of administrators located at **Account > Administrators**.

> **Note**
>
> The administrator is added to the administrators list only if the PingOne for Enterprise connection to your identity repository maps either the PingOne for Enterprise `email` or `SAML_SUBJECT` attribute to the `email` attribute for your identity repository. This is generally the case.

Assign Application Administrator applications

After saving an Application Administrator role assignment, you can assign the specific applications and management permissions for each application.

About this task

An Application Administrator can access only those PingOne admin portal pages associated with their assigned management permissions.

Steps

1. Go to **Account > Administrators**.
2. Expand the entry for the relevant Application Administrator and click the **Edit** icon.
3. Click the **Delegated Administration** tab to add or edit an application.
4. Click the **Add Application** button.

   Result:

   The list of applications is displayed. You can assign more than one Application Administrator to an application.
5. Click the add icon for each application you want the Application Administrator to manage. When you're finished click **Save**.

   Result:

   The applications now assigned to the Application Administrator are displayed with the currently unassigned management permissions.
6. For each application on the list, select or clear the checkboxes for the management permissions you want to assign to the Application Administrator. The available management permissions are:

   Choose from:

   - **Full Control**. Assigns all of the displayed management permissions to the administrator. The admin portal pages My Applications, Users, Certificates, and Reporting will be available to the administrator.
   - **Edit**. Assigns the ability to edit the application configuration, including updating the application certificates. The admin portal pages My Applications and Certificates will be available to the administrator.

Copyright © 2025 Ping Identity Corporation

- **Policy**. Assigns the ability to define policy for the selected application, including assigning the application to groups for access control. The administrator can also enable or disable the application (removing group access to the application). The admin portal pages My Applications, Users, and Certificates will be available to the administrator.
- **Report**. Assigns the ability to run and view reports for the application. The admin portal Reporting page will be available to the administrator.
- **View**. Assigns the administrator read-only permissions for the application configuration. The admin portal page My Applications will be available to the administrator.

> **Note**
>
> You can assign multiple Application Administrators to an application, assigning different management permissions to each administrator. You can also choose to assign multiple administrators the same management permissions.

> **Note**
>
> You can select **Default Permissions** that will apply to every new application assigned to this administrator. You can change these permissions for individual applications after you add them.

7. Click **Save** when you're finished.

Result:

The applications will be displayed on the My Applications page for the Application Administrator.

Manage your user profile

View and edit your user profile on the **User Settings** page.

Steps

- In the top right corner of the admin portal, click your name to open the **User Settings** page.
- Click **Edit** to change your profile information.

  Your administrative role is displayed, but cannot be changed, on this page. For information on changing your administrative role, see Editing administrative roles, permissions, and notifications.
- To change your name, enter new names in the **First Name** and **Last Name** fields.
- To change your email, enter a new email address in the **Email** field.

  If you change your email address, you will receive a confirmation email that you must respond to before the change is applied.
- To change your password, enter your current password in the **Current Password** field, and your new password in the **New Password** and **Confirm New Password** fields.
- To change your default time zone, select a location from the **Time Zone** list.

> **Note**
>
> If you choose a different time zone when creating a report, that time zone overrides your default time zone.

Copyright © 2025 Ping Identity Corporation

- To change your certificate notification settings,
    1. Select **Expiring Certificate Warnings** to enable emails when certificates will be expiring soon.
    2. Select **Expired Certificate Alerts** to enable emails when certificates have expired.

    > **Note**
    >
    > These options are only available for Global and SaaS administrators.

- To apply changes, click **Save**.

Editing administrative roles, permissions, and notifications

Global administrators can edit the permissions for other administrators.

About this task

You cannot change the administrative role for the administrator currently signed on to the admin portal. In this case, you must sign on as a different global administrator.

> **Note**
>
> In PingOne for Enterprise for Managed Service Providers, you can change the administrative role for the currently signed-on administrator on the customer account. You can also disable or delete this administrator on the customer account.

Steps

1. Go to **Account > Administrators**.
2. Expand the line for the administrator whose profile you want to edit.
3. Click the **Pencil icon**.
4. To change the administrator's name, enter new names in the **First Name** and **Last Name** fields.
5. In the **Role** list, select the new administrative role to assign.

   For more information about administrative roles and permissions, see Administrative roles.
6. Select the **Read Only** box to allow the administrator to read data for their role but prohibit them from making system changes.
7. If the administrator is a global or software as a service (SaaS) administrator, click **Notifications** to edit the alerts they receive regarding certificate management.
    1. Select the **Expiring Certificate Warnings** checkbox to enable emails alerting this administrator when certificates will be expiring soon.
    2. Select the **Expired Certificate Alerts** checkbox to enable emails alerting this administrator when certificates have expired.
    3. Select the **Expiring Certificate Warnings (Customer Accounts)** checkbox to enable email alerts alerting this administrator when your customer accounts have a certificate will be expiring soon.

Copyright © 2025 Ping Identity Corporation

4. Select the **Expired Certificate Alerts (Customer Accounts)** checkbox to enable email alerts when your customer accounts have expired certificates.

   Clearing these options only affects email notifications. Dashboard certificate warnings still appear.

   > **Note**
   >
   > The **Customer Accounts** notification options are only available to global or support admins on PingOne for Enterprise for Managed Service Providers or global admins on PingOne SSO for SaaS Apps with Managed Accounts licenses.

8. If the administrator is an application administrator, click **Delegated Administration** to edit their application delegations.

   For more information, see Assign Application Administrator applications.

9. Click **Save**.

Assign admin portal groups

Add user groups to administrative roles, allowing them to single sign-on (SSO) into those administrative roles.

Steps

1. Go to **Setup > Dock > Admin Portal SSO**.
2. Assign user groups to administrative roles. After authenticating to PingOne, members of these groups can access the admin portal.

   For more information about administrative roles and permissions, see Administrative roles.

   If you're using LDAP groups, this needs to be the full distinguished name (FDN) for the administrator group ("CN=admins,OU=example,...").

   Active Directory administrators can use the `dsquery` command on the Active Directory host to find the DN.

3. When you finish assigning groups, click **Save**.

Configuring SSO to the PingOne for Enterprise admin portal

Your administrative users can access the admin portal using single sign-on (SSO) rather than logging in separately with username and password.

About this task

You can enable SSO to the PingOne for Enterprise admin portal for administrators using:

- PingOne for Enterprise dock: For admins or members of the specified LDAP groups for your user repository
- Any supported browser: For members of the specified LDAP groups for your user repository

If you're using PingOne for Enterprise Directory as your identity provider (IdP), all PingOne for Enterprise Directory admins have access to the admin portal from the dock.

Copyright © 2025 Ping Identity Corporation

If you're using PingFederate as your IdP , you can choose to configure SSO to the PingOne for Enterprise admin portal from PingFederate. For more information, see SSO to the PingOne for Enterprise admin portal from PingFederate.

If you've enabled an authentication policy and selected PingID as the authentication provider, you can use multi-factor authentication for SSO to the PingOne for Enterprise admin portal. For more information, see SSO to the PingOne for Enterprise admin portal with multi-factor authentication.

For more information about administrative roles and permissions, see Administrative roles.

Steps

1. In the PingOne for Enterprise admin portal, go to **Setup > Dock > Admin Portal SSO**.
2. For each administrative role, click **Add Group** and enter the name of a user group to add to that administrative role.

   If you're using LDAP groups, this needs to be the full distinguished name (FDN) for the administrator group ("CN=admins,OU=example,...").

   Active Directory administrators can use the `dsquery` command on the Active Directory host to find the DN.

   > **Note**
   >
   > You can assign groups to a read-only administrative role, which grants the administrator access to the areas of the admin portal normally allowed by that role, but not the ability to change settings.

   Users who are members of the group will be able to SSO to the admin portal from any supported browser, as well as from the PingOne for Enterprise dock.
3. Click **Save**.

Result

After you've configured SSO to the admin portal, your admin users can access the admin portal by clicking their avatar in the upper-right of the PingOne for Enterprise dock and then clicking **Admin**.

Next steps

After you've enabled SSO to the PingOne for Enterprise admin portal, you also can choose to apply a secondary level of authentication using PingID. For more information, see SSO to the PingOne for Enterprise admin portal with multi-factor authentication.

SSO to the PingOne for Enterprise admin portal with multi-factor authentication

If you have configured single sign-on (SSO) to the admin portal, you can improve security by requiring multi-factor authentication (MFA) using PingID.

Before you begin

You must complete the following:

- Configuring SSO to the PingOne for Enterprise admin portal
- Configure PingID authentication

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> MFA to the PingOne for Enterprise admin portal is enforced through PingOne for Enterprise, so even if you've configured PingFederate for PingID authentication, you still need to enable a PingOne for Enterprise authentication policy for PingID.
> Learn more in Create or update an authentication policy.

About this task

> **Note**
>
> If the username your administrator uses for SSO to the admin console differs from the email address they use for PingOne for Enterprise, PingID treats that username as a separate identity.
> You can streamline the admin SSO experience with the following recommended configuration:
>
> 1. Configure SSO for administrators. For more information, see Configuring SSO to the PingOne for Enterprise admin portal.
> 2. Remove administrative users who use an email rather than a username for sign on. If necessary, create new administrative users and select the **SSO Admin** checkbox. For more information, see Assign administrative roles.
> 3. When enabling MFA (see step 7 below), select **SSO Username**as the SSO method for admin users.
>
> If your admin users' usernames are the same as the email address that they use to sign on to the admin portal, you can ignore this configuration because usernames will be the same for PingID.

Steps

1. In the PingOne for Enterprise admin portal, go to **Setup > Authentication Policy**.
2. Click **Edit**.
3. Select **Enable authentication policy**.
4. On the **Apply policy to** line, click **Selected groups** and select the checkboxes of the groups assigned as administrative groups.

   > **Tip**
   >
   > To improve security, click **All cases** to require all users to authenticate using MFA.

5. Select the **Apply authentication policy to PingOne Admin Portal** checkbox.
6. **Optional:** In the **Do not apply authentication policy to** list, select an administrator.

   > **Tip**
   >
   > Exempting a designated administrator from the authentication policy allows that administrator to sign on to the admin portal in case of problems with PingID.

7. In the **PingID username attribute for SSO admins** line, select an SSO method for administrators:

   Choose from:

   - **SSO Username**: Administrators sign on using their username and PingID devices as they would to sign on to the PingOne Dock.

Copyright © 2025 Ping Identity Corporation

- **Email**: Administrators sign on using their email address and PingID devices as they would to sign on to the admin portal.

> **Important**
>
> Selecting **Email** is not recommended unless you intend for admins to sign on through SSO as well as directly using their email and password. This will usually require admins to maintain a second set of PingID devices specifically for admin access.

8. Select the **Apply to all sign-on attempts** checkbox.
9. Click **Save**.

Next steps

If you want to configure an advanced PingID authentication policy for your administrative users, see Configuring an app or group-specific authentication policy in the PingID documentation.

SSO to the PingOne for Enterprise admin portal from PingFederate

If you use PingFederate as your identity bridge, there are a couple of ways you can configure single sign-on (SSO) directly to the PingOne for Enterprise admin portal from PingFederate.

Steps

1. Use one of the following methods to SSO to the PingOne for Enterprise admin portal:

   Choose from:

   - For all PingFederate versions:

     1. Log in to PingFederate and go to **IdP Configuration > SP Connections - PingOne**.
     2. Copy the **SSO Application Endpoint** entry to a text file and add this specific `TargetResource` value to the `/idp/startSSO.ping` endpoint:

        ```
        https://pingone.com/1.0/8bfe0aeb-79ca-4fd4-a116-c3f7c7dbe6ca
        ```

        Entering the resulting URL in a browser displays the credentials prompt for SSO to the PingOne for Enterprise admin portal. For example:

        ```
        /idp/startSSO.ping?PartnerSpId=http://pingone.com/yourAccount&TargetResource=https://
        pingone.com/1.0/8bfe0aeb-79ca-4fd4-a116-c3f7c7dbe6ca
        ```

        Learn more about the start SSO endpoint in /idp/startSSO.ping in the PingFederate documentation.

   - PingFederate 8.0 or later

     1. Go to **Server Configuration > Server Settings > PingOne Settings**.
     2. Click **Launch PingOne Admin Portal**.

Copyright © 2025 Ping Identity Corporation

PingFederate uses the credentials you used to log in to PingFederate for SSO to the PingOne for Enterprise admin portal.

Next steps

After you've configured SSO to the PingOne for Enterprise admin portal from PingFederate, you also can choose to apply a secondary level of authentication using PingID. See Create or update an authentication policy for more information.

Assign branding and design

You can assign custom branding on PingOne for Enterprise pages for your organization.

Custom branding is available in the following areas:

- Your corporate logo for use on login, single sign-on (SSO), and in the PingOne for Enterprise dock. See Adding a logo and banner message.
- Users' login and SSO pages. See Assign branding and design for logon and SSO.
- The PingOne for Enterprise dock. See Assign branding and design.

Adding a logo and banner message

About this task

The logo you assign can be used for display on users' login and SSO pages as well as in the PingOne for Enterprise dock.

Steps

1. Go to **Account > Branding**.
2. In the **Corporate Logo** section, click the **Add** icon and browse for the logo that you want to assign.

   The standard maximum display dimensions on the PingOne for Enterprise dock are 72px high by 350px wide. The image dimension ratio is preserved. For the logo to render optimally on high-definition displays (such as Apple Retina displays), double the dimensions to 144px high by 700px wide.
3. To create a banner message, enter you message text into the **Banner Message** field.

   The banner is displayed at the top of the admin portal and is only visible to your administrative users.
4. Click **Save**.

Assign branding and design for logon and SSO

About this task

To assign branding and design elements for the PingOne for Enterprise logon and SSO pages:

Steps

1. Go to the **Setup > Branding > Logon & SSO** page.
2. In the **Corporate Logo** section, accept the default **Use Corporate Logo**, or click **Custom** and browse for the logo that you want to assign.

Copyright © 2025 Ping Identity Corporation

The standard maximum display dimensions are 72px high by 350px wide. The image dimension ratio is preserved. For the logo to render optimally on high-definition displays (such as Apple Retina displays), double the dimensions to 144px high by 700px wide.

The maximum file size for the image is 10 Mb.

3. In the **Backgrounds** section, select from the following:

   Choose from:

   - **Main Background**: Select one of the following:
   - **None**: No background color or image. The background is white by default.
   - **Image**: Click **Choose Background**and browse for the image that you want to use as the dock background.

     > **Note**
     >
     > Images larger than 3000 x 1500 are automatically resized, resulting in possible loss of quality.

   - **Color**: Select a background color from the color picker, or enter the Hex color code you require.
   - **Form Background Color**: Select a background color from the color picker, or enter the Hex color code you require.

4. In the **Buttons** section, select from the following:

   Choose from:

   - **Button Color**: Select a button color from the color picker, or enter the Hex color code you require.
   - **Button Font Color**: Select a font color for button labels from the color picker, or enter the Hex color code you require.

5. In the **Text** section, select from the following:

   Choose from:

   - **Form Fill Color**: Select a fill color to use for the form from the color picker, or enter the Hex color code you require.
   - **Form Font Color**: Select a font color to use for text from the color picker, or enter the Hex color code you require.
   - **Link color**: Select a color to use for links from the color picker, or enter the Hex color code you require.
   - **Header and Custom Text Color**: Select the color to use for the header and custom text from the color picker, or enter the Hex color code you require.

6. In the **Content** section, select from the following:

   Choose from:

   - **Registration Page Header**: Enter any custom text to display in the header for the PingOne for Enterprise registration page (100 characters maximum).
   - **Registration Page Text**: Enter any custom text to display on the PingOne registration page (300 characters maximum).
   - **Login Page Header**: Enter any custom text to display in the header for the login page (100 characters maximum).

Copyright © 2025 Ping Identity Corporation

- **Login Page Text**: Enter any custom text to display on the login page (300 characters maximum).
- **Reset Password Page Header**: Enter any custom text to display in the header for the password reset page (100 characters maximum).
- **Reset Password Custom Text**: Enter any custom text to display on the password reset page (300 characters maximum).
- **Error Page Header**: Enter any custom text to display in the header for the error page (100 characters maximum).
- **Error Page Text**: Enter any custom text to display on the error page (300 characters maximum).

7. Click **Save**.

Result

The settings are applied and are immediately visible on the associated pages.

Upgrade a PingOne for Groups account

About this task

If your organization has a PingOne for Groups account and you want to upgrade to a PingOne for Enterprise account, you can select to contact us, so we can have a representative help you with the upgrade.

Steps

1. Select the **Account** tab, then choose **Account Plan**. The Account Plan page is displayed.
2. Under PingOne for Enterprise, click **Contact Us**. An automatically-generated message is sent to us at Ping Identity.

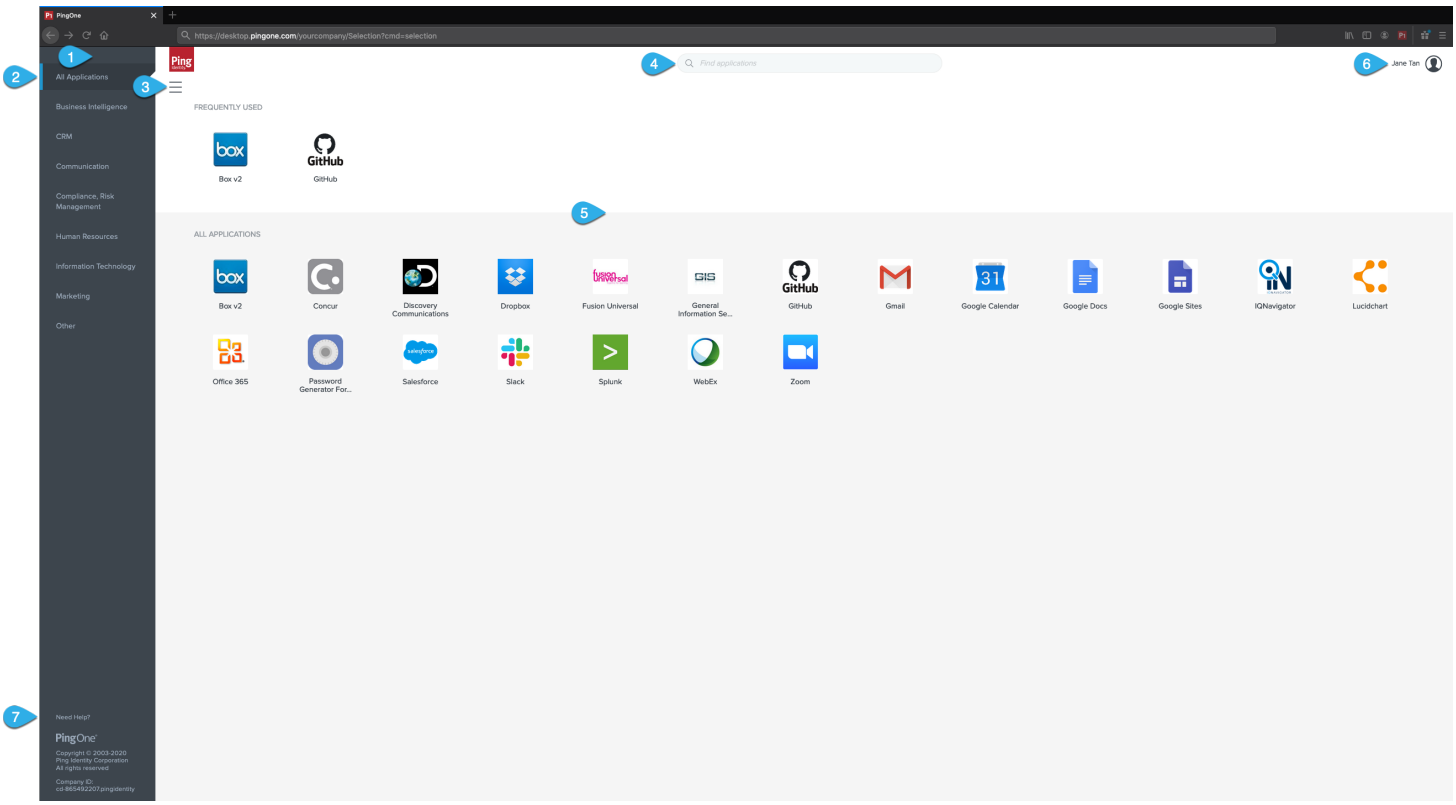
   One of our representatives will contact you within a day or two to help you.

Using the PingOne for Enterprise dock

Introducing the PingOne for Enterprise dock

The PingOne for Enterprise dock gives you a single, unified interface for single sign-on (SSO) to the applications you've added for your organization.

Copyright © 2025 Ping Identity Corporation



Key	Description
1	Left navigation pane
2	Left navigation pane: Category selector
3	Main area: Left navigation toggle button
4	Main area: Search bar
5	Main area: Applications
6	Main area: Avatar menu
7	Main area: Access help

- **Main area** (5). The main area lists all applications that you currently have installed.
  - Double-click an app to launch it in a new browser window.
  - If you have more than 15 applications installed, the **Frequently Used** area displays the apps you use most frequently at the top of the dock.
  - Click a category in the **Left Navigation pane** (1) to filter the apps list and view only the apps of that category. The**Category Selector** (2) indicates which category is currently displayed.
  - Click the menu icon (3) to show or hide the navigation pane.

Copyright © 2025 Ping Identity Corporation

- **Search bar** (4). Search for the app that you want to launch. Enter the name or part of the name for an app. A dropdown list shows the closest matches.
    - Click **Open**: to launch an existing app.
    - Click **Install**: to install new app (only available if your personal dock is enabled).
- **Avatar menu** (6). A quick access menu from which you can select:
    - **Devices** (For organizations using PingID multi-factor authentication): Manage the devices you use for authentication.
    - **Manage Passwords**: Edit passwords for basic SSO apps.
    - **Admin**: Access the admin console (administrators only).
    - **Show help**: take a guided tour around the main features of your PingOne dock.
    - **Logout**: Logout of the PingOne dock.
- **Access help** (7). Click the link to get details of where to go for help in your organization.

Launch an application

About this task

Click an application in the PingOne dock, or search for an app and launch it from the search bar.

> **Note**
>
> Some Basic SSO applications require you to enter your username and password the first time you log on to the application. Your details are saved by the PingOne browser extension, so you will not have to enter them when you access the application again. If the PingOne browser isn't installed, you will be prompted to install it when you try to access an application.

Steps

1. In the PingOne dock search bar, type the name, or part of the name of the application, and then click **Open**. The app opens in a new browser window or tab.

Manage your devices

About this task

You can use more than one device to authenticate access to the PingOne dock. If your primary device is temporarily unavailable for any reason, you can switch to a secondary authentication device to access the dock.

You can add devices, decide which is the primary (default) device, update device details, or delete a device.

> **Note**
>
> This feature is only available if your organization is using PingID multi-factor authentication (MFA). The ability to add and manage devices is enabled by your administrator.

Copyright © 2025 Ping Identity Corporation

Steps

1. In your PingOne dock, click the avatar menu icon and select **Devices**. The **My Devices** page displays, listing your current devices.

   If you have more than one device listed, the primary device is indicated in green in the **PRIMARY** column.

   You can also access the **My Devices** page during authentication. When authenticating, click **Settings**, or **Change Authentication Device**.

2. To change the primary device, in the **PRIMARY** column on the row listing the entry for that device, move the slider to "ON". All other devices are automatically switched to unmarked.

3. To edit the device details, click the edit icon to expand and display the details:

   Choose from:

   - **Device nickname**. Enter the name or description for the authenticating device, as you want it to appear during authentication. The default value is the name of the authentication method, or the marketing name of the phone.
   - **Device details**. Enter the details that identify the authentication device (such as, phone number, email address, YubiKey, or PingID App details). Basic validation is applied to ensure the entry is valid and in the correct format. Changing this entry changes the authentication device. The default value is the value captured when authenticating the device for the first time.

4. To add a device, click **Add**. The **Add New Device** dialog box displays.

   1. Select the new authentication method or device that you want to add. The steps for each method vary. Follow the instructions and complete the registration and pairing of your new authentication device.

   The available authentication methods are determined by your organization's authentication policy.

Result

When the process is complete and the device is paired, the My Devices page displays. Your new device is listed in the last row of the table, with its default nickname.

Install the PingOne for Enterprise browser extension

The PingOne for Enterprise browser extension manages your credentials for basic dingle sign-on (SSO) applications.

About this task

When you first launch a basic SSO application you may be prompted to enter your credentials. The browser extension saves the credentials for the basic SSO app and ensures that thereafter you can SSO to the application using the browser. If the browser extension isn't installed when you try to access a basic SSO application, you're prompted to install it and create a privacy key.

The browser extension uses your privacy key to encrypt the credentials you use to access basic SSO applications. privacy key to access and manage passwords for your SSO applications, and enable the browser extension to access password information from different browsers and devices.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> The privacy key you define is known only to you. It enables you to access and modify the passwords for all of your basic SSO apps. If you forget your privacy key, it cannot be recovered.

Steps

1. In the PingOne for Enterprise dock, double-click a basic SSO application.

   Result:

   If the PingOne for Enterprise browser extension is not installed, a message appears prompting you to install it.

2. Click **Install**.

   Result:

   A confirmation message is displayed.

3. Click **Add extension**.

   Result:

   The browser extension is installed, and an associated icon is added to your browser bar. When you try to access an application on the dock, you are prompted to create a privacy key.

4. Enter a privacy key and click **Continue**.

   > **Note**
   >
   > The privacy key must be a minimum of 8 characters.

   Result:

   The privacy key is saved. When you log on to a basic SSO application for the first time, you will need to enter your username and password.

5. To manage your passwords or change your privacy key, in the avatar menu, click **Manage Passwords**.

Change your privacy key

About this task

The PingOne browser extension saves your passwords for reuse. To access or change your passwords, you need to enter your privacy key.

> **Note**
>
> The privacy key you define is known only to you. It enables you to access and modify the passwords for all of your Basic SSO apps. If you forget your privacy key, it cannot be recovered.

Steps

1. To modify your privacy key, in the PingOne dock, click the avatar menu icon and select **Manage Passwords**.

2. Click **Sign On** and enter your old privacy key.

Copyright © 2025 Ping Identity Corporation

3. In the **Manage Passwords** window, click the **Privacy Key** tab.
4. In the**Privacy Key** area, enter and confirm your new privacy key, then click **Change**.

Result

Your privacy key is updated.

Manage your Basic SSO passwords

About this task

The PingOne for Enterprise browser extension saves passwords for all Basic SSO apps. If you need to change or delete a password, you can access them from the avatar menu in the PingOne for Enterprise dock.

Steps

1. In the PingOne for Enterprise dock, click the avatar menu icon and select **Manage Passwords**.
2. If you are prompted to authenticate your account, enter your username and password to proceed.
3. In the **Manage Passwords** frame, click the tab for the app that you want to modify.
4. Edit the username or password as required, and click **Save**. The changes are applied automatically.
5. To remove username and password details for an application, in the relevant tab, click **Remove Application** (located below the **Save** button).

Configuring the dock when using an identity bridge

For most identity repositories, you can configure the following dock options.

About this task

- Configure the format of the URL used to access the dock.
- Give your users the option to add personal apps to the dock.

> **Note**
>
> If you're using PingOne for Enterprise Directory, the configuration options differ slightly. See Configure the dock when using PingOne for Enterprise Directory.

If you're currently using the legacy PingOne for Enterprise dock, you can configure and customize the new dock and then preview your changes using the displayed **Upgraded Ping Dock URL** before upgrading to the new dock. Your users can continue to work in the legacy dock until you upgrade.

Steps

1. Go to **Setup > Dock > Configuration**.
2. Edit one or more of the following settings.

Copyright © 2025 Ping Identity Corporation

Option	Description
Company ID	The unique identifier for your company. This string becomes part of your dock URL.
Identity Bridge Logout URL	The location to which you will send users then they sign out of PingOne for Enterprise. Specify this URL if you don't want to use the default SAML single logout (SLO) protocol.
Maximum Session Lifetime	In the**Maximum Session Lifetime** list, select the maximum duration of a user session before the user is automatically signed out. The minimum duration is 15 minutes. The default is 2 hours. The maximum is 12 hours.
SLO Flow	If you click **Redirect**, PingOne for Enterprise responds to SLO requests by visiting each application's SLO endpoint and then returning to the sign-on page. If you click **Single page**, PingOne for Enterprise responds to SLO requests by sending requests from its own page using an iframe. **Note** **Single page** SLO flow requires third-party cookies to be enabled in the user's browser, and session cookies in Chrome must use `SameSite=None`. **Redirect** flow works regardless of cookie settings. **Redirect** flow halts if an application fails to return control to PingOne for Enterprise. **Single page** flow continues even if errors occur at the application. OpenID Connect (OIDC) applications always follow single page flow even if **Redirect** is enabled. To support SLO for OIDC applications, user browsers must allow third party cookies, and Chrome cookies must use `SameSite=None`.
Session Idle Timeout	In the **Session Idle Timeout** list, select the maximum duration of a user's idle time before the user is automatically signed out. The maximum duration is 12 hours. The idle timeout duration cannot exceed the maximum session lifetime.
Enable Basic SSO	Enable this option if you want to use basic single sign-on (SSO), a password vaulting capability for PingOne for Enterprise. See Basic SSO (password vaulting) for more information.

Copyright © 2025 Ping Identity Corporation

Option	Description
Add Basic SSO Applications	Select this to enable users to add basic SSO applications to their dock. Applications that users install appear on the dock in the personal category.
User Support Message	Enter text that shows when a user clicks the **Need Help?** link in the PingOne for Enterprise dock.
Upgrade Dock	If you are currently using the legacy dock, you can preview your changes in the dock preview until you upgrade. To upgrade to the new dock, click **Upgrade Dock**. When upgraded, this option and the dock preview are no longer available.

3. In the **Attribute Mapping** section, map the identity bridge attributes to the supported dock attributes.

   Generally, the default attribute mapping is sufficient. However, you can change the mapping as needed for the following attributes.

Option	Description
SAML_Subject	Maps to the attribute representing the unique identifier, username, or user subject in the identity repository.
memberOf	Maps to the attribute that represents the group membership information for users in the identity repository. **Note** This is a special attribute representing the group membership information for users using SSO through the PingOne for Enterprise dock. Group membership information is applied on the **User Groups** page to authorize user access to software as a service (SaaS) applications.
fname	Maps to the attribute representing the first name of users in the identity repository.
lname	Maps to the attribute representing the last name of the users in the identity repository.
email	Maps to the attribute representing the email address for users in the identity repository.

Copyright © 2025 Ping Identity Corporation

Option	Description
phoneNumber	Maps to the attribute representing the phone number for users in the identity repository.
secondaryEmail	Maps to the attribute representing the user's secondary email in the identity repository.
voiceNumber	Optional attribute allowing you to specify a second number specifically for PingID voice one-time passcodes (OTPs). For more information, see SMS and voice authorization.

1. **Optional:** For each attribute, click **Advanced** to customize the selected attribute.

   Customizing is useful if the attribute used by your identity bridge doesn't match the corresponding attribute used by an application. Advanced attribute mapping lets you:

   - Apply a transformation function to alter the identity bridge attribute to match the application attribute.
   - Assign multiple identity bridge attributes to a single application attribute.

See Creating advanced attribute mappings for more information.

4. Click **Save**.

Next steps

To view the changes, refresh the dock page.

Configure the dock when using PingOne for Enterprise Directory

About this task

When using the PingOne for Enterprise Directory, you can configure the following options for the dock:

- Change the format of the URL used to access the dock.
- Give your users the option to add personal apps to the dock.

> **Note**
>
> If you are not using PingOne for Enterprise Directory as your identity repository, the configuration options differ slightly. See Configuring the dock when using an identity bridge

If you're currently using the legacy PingOne dock, you can configure and customize the new dock, then preview your changes using the displayed **Upgraded Ping Dock URL** before upgrading to the new dock. Your users can continue to work in the legacy dock until you upgrade.

Steps

1. Click **Setup > Dock**.

Copyright © 2025 Ping Identity Corporation

2. **Optional:** In **Configuration**, edit one or more of the following configuration settings:

Option	Description
Company ID	The unique identifier for your company. This string becomes part of your dock URL.
Maximum Session Lifetime	In the**Maximum Session Lifetime** list, select the maximum duration of a user session before the user is automatically signed out. The minimum duration is 15 minutes. The default is 2 hours. The maximum is 12 hours.
SLO Flow	If you click **Redirect**, PingOne for Enterprise responds to SLO requests by visiting each application's SLO endpoint and then returning to the sign-on page. If you click **Single page**, PingOne for Enterprise responds to SLO requests by sending requests from its own page using an iframe. **Note** **Single page** SLO flow requires third-party cookies to be enabled in the user's browser, and session cookies in Chrome must use `SameSite=None`. **Redirect** flow works regardless of cookie settings. **Redirect** flow halts if an application fails to return control to PingOne for Enterprise. **Single page** flow continues even if errors occur at the application. OpenID Connect (OIDC) applications always follow single page flow even if **Redirect** is enabled. To support SLO for OIDC applications, user browsers must allow third party cookies, and Chrome cookies must use `SameSite=None`.
Session Idle Timeout	In the **Session Idle Timeout** list, select the maximum duration of a user's idle time before the user is automatically signed out. The maximum duration is 12 hours. The idle timeout duration cannot exceed the maximum session lifetime.
Enable Basic SSO	Enable this option if you want to use basic single sign-on (SSO), a password vaulting capability for PingOne for Enterprise. See Basic SSO (password vaulting) for more information.
Add Basic SSO Applications	Select this to enable users to add basic SSO applications to their dock. Applications that users install appear on the dock in the personal category.

Copyright © 2025 Ping Identity Corporation

Option	Description
User Support Message	Enter text that shows when a user clicks the **Need Help?** link in the PingOne for Enterprise dock.
Upgrade Dock	If you are currently using the legacy dock, you can preview your changes in the dock preview until you upgrade. To upgrade to the new dock, click **Upgrade Dock**. When upgraded, this option and the dock preview are no longer available.

3. Click **Save**. The changes are applied to the dock.

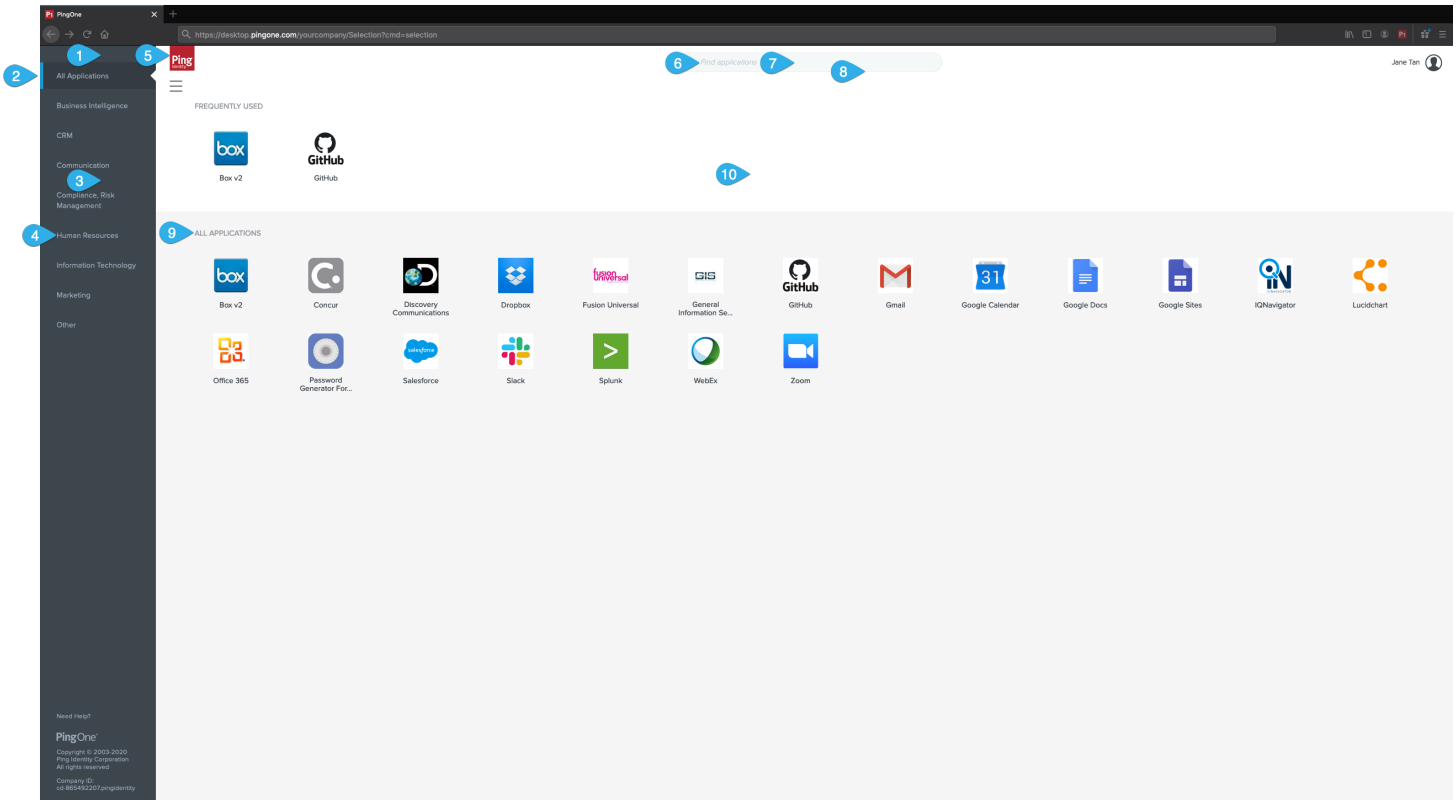
   To view the changes, refresh the page.

Assign branding and design

The PingOne dock features a variety of branding and design options to customize for your organization.

About this task

If you're currently using the legacy PingOne dock, you can customize the new dock, then preview your changes using the displayed **Upgraded Ping Dock URL** before upgrading to the new dock. Your users can continue to work in the legacy dock until you upgrade.



Copyright © 2025 Ping Identity Corporation

Dock branding attributes

Key	Element	Key	Element
1	Left navigation pane	6	Search: font color
2	Left navigation pane: selected color	7	Search: fill color
3	Left navigation pane: background color	8	Search: border color
4	Left navigation pane: font color	9	Main area: fonts
5	Dock logo	10	Main area: background

> **Note**
>
> All branding fields are optional. If you do not specify your preference, the default values are applied.

Steps

1. Go to the **Setup > Branding > Dock** page.
2. **Optional:** In the Logo For Dock section (5), select either:

   Choose from:

   - **Use Corporate Logo**. Automatically add to the dock the corporate logo you have assigned for PingOne. See Assign branding and design for logon and SSO to assign the logo to use for your organization.
   - **Custom**. Click **Choose Logo**, select the logo that you want to add to the dock and click **Open**.
3. Define the appearance of the main area background (10), in the **Main Area**, **Background** field.

   Select one of the following:

   Choose from:

   - **None**: No background color or image. The background is white by default.
   - **Image**: Click **Choose Background**and navigate to the image that you want to use as the dock background.

     > **Note**
     >
     > Images larger than 3000 x 1500 are automatically resized, resulting in possible loss of quality.

   - **Color**: Select a background color from the dropdown color palette, or enter the Hex color code you require.
4. Define the font color and appearance (9) in the main section:

Copyright © 2025 Ping Identity Corporation

Choose from:

- In the **Font Color** dropdown color palette, select a color for the main area fonts, or enter the Hex color code you require.
- In the **Drop Shadow** field, click **Yes** if you want to add a drop shadow.

> **Tip**
>
> The addition of a drop shadow can make text easier to read.

5. In the **Left Navigation Colors** section, define the appearance of the left navigation pane (1) attributes:

   Choose from:

   - **Background Color** (3): In the dropdown color palette, select the color of the navigation pane background, or enter the Hex color code you require.
   - **Selected Color** (2): In the dropdown color palette, select the color you want to use to indicate which category is currently selected in the navigation pane, or enter the Hex color code you require.
   - **Font Color** (4): In the dropdown color palette, select the color you want to apply to text in the navigation pane, or enter the Hex color code you require.

6. In the **Search Colors** section, define the appearance of the following search bar attributes:

   Choose from:

   - **Fill color** (7): In the dropdown color palette, select the fill color of the search bar, or enter the Hex color code you require.
   - **Border color** (8): In the dropdown color palette, select the color of the border of the search bar, or enter the Hex color code you require.
   - **Font color** (6): In the dropdown color palette, select the color of text entered in the search bar, or enter the Hex color code you require.

7. In the **Sign Off** section, select any branding to use for the dock sign off page:

   Select one of the following for the main background:

   Choose from:

   - **None**: No background color or image. The background is white by default.
   - **Image**: Click **Choose Background**and navigate to the image that you want to use as the dock background.

     > **Note**
     >
     > Images larger than 3000 x 1500 are automatically resized, resulting in possible loss of quality.

   - **Color**: Select a background color from the dropdown color palette, or enter the Hex color code you require.

   Select the sign off page colors:

   +

Copyright © 2025 Ping Identity Corporation

Choose from:

- **Form color**: In the dropdown color palette, select the color to use for the sign off form, or enter the Hex color code you require.
- **Font color**: In the dropdown color palette, select the color of text used in the sign off page, or enter the Hex color code you require.
- **Link color**: In the dropdown color palette, select the color to use for links in the sign off page, or enter the Hex color code you require.
- **Sign Off Page Text**: Enter the text to display to a user when they sign off of the dock (300 characters maximum).

8. Click **Save**. The changes are applied and visible on the new dock.

> **Note**
>
> If you do not see the changes immediately, refresh the page.

9. To restore the default settings, click **Restore Defaults**.

Add an app to a category

About this task

The PingOne dock can contain many apps. Categorizing them can organize the dock and ease search and navigation for your users.

When you add an app to the applications list, select the appropriate category from the list provided. If the app is available to a user in their dock, the category is listed in their navigation pane, and the app appears under the selected category, as well as in the **All Applications** category.

> **Note**
>
> The PingOne dock navigation pane lists only the categories having at least one associated app.

Steps

1. Click **Applications > My Applications**.
2. Select an application from the list and click **Edit**.
3. Continue through the app wizard until you reach the page containing the **PingOne App Customization** section. Here you can select the logo, icon, name and description for the app.
4. In the **Category** dropdown menu, select the category that you want to apply to this app and click **Save & Publish**.

   Result:

   The app is added to the selected category. When a user with access to the app signs on to PingOne dock, the app appears on the dock in the category that you selected and in the **All Applications** category.

Copyright © 2025 Ping Identity Corporation

Upgrade the PingOne for Enterprise dock

Configure the settings and branding that you want to appear on the new dock. Once you are finished, upgrade the dock. After the upgrade, all users are directed to the new dock.

About this task

You can customize the look and feel of your new dock, and then preview the changes before you upgrade. Your users can continue to work in the legacy dock until you are ready to upgrade. You can preview the changes as many times as you need using the new dock URL provided in the admin portal.

Steps

1. In the PingOne for Enterprise admin portal, go to **Setup > Dock > Configuration**.
2. Configure Dock settings.

   Choose from:

   - If you use the PingOne for Enterprise Directory as your identity provider, see Configure the dock when using PingOne for Enterprise Directory.
   - If you use another identity provider, see Configuring the dock when using an identity bridge.
3. Customize the branding and design of the Dock.
4. To preview your new Dock settings, click the **Upgraded Ping Dock URL**.
5. When you are finished configuring your Dock, click **Upgrade Dock** and then click **Save**.

Result

The dock is upgraded to the new dock, and in the **Configuration** tab, the preview URL is removed and only the live PingOne dock URL field is shown.

Next steps

If you have not already done so, assign your applications to categories. for more information, see Add an app to a category

Monitoring and modifying customer accounts

As a Managed Service Provider (MSP), you can monitor and modify your customer accounts, as well as suspend an account when necessary. When you administer a customer account, you access the account's admin portal as a Support Administrator (the default) or Global Administrator. Depending on the permissions assigned to you by your Global Administrator, you'll have Read-Only, Read-Write, or full rights (Global Administrators only) to the customer account.

Only Global Administrators have access to the Dashboard and Service Settings pages for an MSP account.

Display and search customer accounts

Before you begin

If you have a PingOne for Managed Service Providers account, you can view and manage your customer accounts.

Copyright © 2025 Ping Identity Corporation

About this task

You'll use the search facility to find a specific account to display. You can also sort the account listing.

Steps

1. Select the **Customers** tab.
2. Select the customer account to display, or in the search entry box, enter the search criteria for the account.

   You can search by account name, email address or account ID. Use the wildcard characters percent sign (%) and underscore (_) in your account name and email address searches (not in ID searches). The % character matches any sequence of characters (including no characters). The _ character matches any single character.

Administer customer accounts

Before you begin

If you have a PingOne for Enterprise for Managed Service Providers account, you can access the PingOne for Enterprise admin portal of one of your customer accounts.

About this task

Choose a customer account to administer. You need to be either a Support Administrator (Read/Write or Read-Only permissions), or a Global Administrator to access the admin portal for the account.

Steps

1. Click **Customers**.
2. Click the **Expand** icon for the account you want to administer.

   If you have read/write or full permissions, you can modify the PingOne for Enterprise configuration for the customer account.
3. To manage PingID licensing for your customer accounts, click **Licensing**.
    1. Click the **Full License** toggle to switch between aPingID trial or full license for this customer account.

   For more information about the differences between PingID trial and licensed accounts, see SMS and voice usage limits in the PingID documentation.
    1. Click the **Enable SMS/Voice** toggle to enable or disable this customer account's ability to send SMS or voice one-time passcodes.

       > **Note**
       >
       > This feature is in limited release. To request access to this feature, open a support case.
4. Click **Enter Account**. You're prompted to verify the account access, then the admin portal for the customer account is displayed. In the header at the top of each page is a Support Admin banner identifying you as administering this account.
5. When you're finished, click the **Exit** button in the Support Admin banner to quit administering the customer account and return to the Customers administration page.

Copyright © 2025 Ping Identity Corporation

Configuring customer account service settings

As a Global Administrator, you can configure customer settings for your managed service.

About this task

All of the service settings are optional. Any settings that you don't assign will use the default values.

> **Note**
>
> The **Service Settings** page is not available for Support Administrators.

Steps

1. Go to **Customers > Service Settings**.
2. Click **Edit**.
3. To allow your customers to change the corporate logo displayed on their dock, make sure the **Allow Logo Customization** checkbox is selected.

   Your customers can customize their corporate logo on one of three menus in their PingOne for Enterprise admin portal:

   - **Setup > Branding > Dock**
   - **Setup > Branding > Logon & SSO**
   - **Account > Branding**
4. To choose the branding logos for your customer's **User Dock** and **Admin Portal**, click **Select Image**.
5. Select the **Enable 'Add Basic SSO Applications' Option** checkbox to give your customers the option of allowing end users to add basic single sign-on (SSO) applications to their PingOne for Enterprise Dock.

   Result:

   The **Add Basic SSO Applications** option will be displayed on the **PingOne Dock Configuration** page in your customer's PingOne for Enterprise admin portal.

   > **Note**
   >
   > If you clear the **Enable 'Add Basic SSO Applications' Option** checkbox, the option won't show in your customer's **Dock Configuration** window.

   When your customers choose the **Add Basic SSO Applications** option, your customer's end users can add and remove basic SSO applications in their personal dock from the PingOne for Enterprise Application Catalog.
6. To limit the identity repositories available to your customers, clear the **Allow All Identity Repositories** checkbox, and select the allowed identity repositories.

   > **Note**
   >
   > By default, all PingOne for Enterprise identity repositories are available for your customers to configure.

Copyright © 2025 Ping Identity Corporation

7. To allow your customers to configure their multi-factor authentication (MFA) settings, make sure the **Allow MFA Customization** checkbox is selected.

   When this option is enabled, your customers can:

   - Configure their MFA settings at **Setup > Authentication Policy**.
   - Configure their PingID MFA settings at **Setup > PingID**.

   > **Note**
   >
   > When **Allow MFA Customization** is disabled, your customers see MFA settings as read-only.

8. To allow your customers using the PingOne for Enterprise Directory to configure password policies for their users, make sure the **Allow Password Policy Customization** checkbox is selected.

   When this option is enabled, your customers using the PingOne for Enterprise Directory can customize Directory password policies at **Setup > Directory**.

   > **Note**
   >
   > When **Allow Password Policy Customization** is disabled, your customers see the PingOne for Enterprise Directory password policy as read-only.

9. Configure the templates for emails automatically sent to customers.

Option	Description
Sender	The sender address used in emails sent to your customers. The ability to customize this field is disabled by default. To enable it, log on to your account and submit a support case.
Account Activation	In the **Subject Line** field, enter a subject line for account activation emails. To customize the account activation email template click **Download Template**.
Admin Invite	In the **Subject Line** field, enter a subject line for admin invite emails. To customize the admin invite email template click **Download Template**.
Password Reset	In the **Subject Line** field, enter a subject line for password reset emails. To customize the password reset email template click **Download Template**.

Copyright © 2025 Ping Identity Corporation

Option	Description
Account Upgrade	In the **Email** field, enter an email address to send account upgrade emails from. In the **Subject Line** box, enter a subject line for account upgrade emails. To customize the password reset email template click **Download Template**.

1. To view or modify the default HTML email template that's sent to customers, click **Download Current Template**.

You can modify this template for your use or create a new HTML template. Any new templates you create need to be valid HTML and use the same variables as in the default template (do not add any new variables).

1. To replace the current (default) template, click **Replace Template** and select the HTML file to use.
2. To delete an email template, in the Email Templates area, next to the relevant template, click **Remove Saved Template**, and then click **Save**. The custom template is removed and the default PingOne for Enterprise email template is applied.

10. To add a support email address and support URL to the **Help** menu of the customer's PingOne for Enterprise admin portal, in the **Support & Policies** section:
    1. For **Support Email**, enter your support team email address.
    2. For **Support URL**, enter the URL for your customer support page.

Invite a new customer

Before you begin

If you have a PingOne for Managed Service Providers account, you can invite a new customer to use your service.

About this task

You'll enter the profile information for the new customer. An email invitation is then sent to the customer. You can configure the email that is sent. See Configuring customer account service settings. You need either to be a Global Admnistrator or Support Administrator (Read/Write or Read-Only) to invite a new customer.

After sending the invitation, if necessary, you can choose to resend or cancel the customer invitation.

Steps

1. Select the **Customers** tab.
2. Click **Invite Customer**.
3. Enter the profile information for the new customer.

   The **Managed Service Provider ID** entry is optional. This is a unique identifier you can use for this customer within the context of your service (as Managed Service Provider).

Copyright © 2025 Ping Identity Corporation

4. Click **Invite Customer**. An email invitation is automatically sent to the customer email address you specified, and the new customer is added to your customer listing.

   If you've customized an email template for your service, this is the template used. Otherwise, the PingOne default email template is used.

Creating a customer account

Creating an account for a customer allows you to configure and manage the account without the need for customer-side administrators.

About this task

You can add administrators after you create the account. See Assign administrative roles for more information.

When creating a customer account, enter profile information for the new customer. You can also connect the account to an identity repository.

Unlike Inviting a new customer, no email invitation is sent to the customer when creating an account in this way. This gives you the option to coordinate with the customer when and how you choose.

Steps

1. Go to **Customers > Customers**.
2. Click **+ Create Account**.
3. Enter an **Account Name**.
4. **Optional:** Add an **MSP ID**.

   This is a unique identifier you can use for this customer within the context of your service as the managed service provider.
5. Select a region from the **Data Center Region** list.
6. Click **Done**.
7. **Optional:** If you want to select an identity repository for this customer, click **Yes, Enter Account**.

   You have Support Admin access to this account. For more information on administrative roles, see Assign administrative roles. For more information on connecting to an identity repository, see Connecting to an identity repository.
8. After you configure the account, click **Exit** in the blue band at the top of any window to return to the **Customers** window.

Upgrade a customer account

Before you begin

If you have a PingOne for Managed Service Providers account, you can upgrade one of your customer accounts.

About this task

Copyright © 2025 Ping Identity Corporation

You'll choose a customer account to upgrade. You need either to be a Global Admnistrator or Support Administrator (Read/Write) to suspend an account.

Steps

1. Select the **Customers** tab.
2. Expand the account details for the selected customer and click the edit icon.
3. Under the Account Type, click **Upgrade**.

   Result:

   You're prompted to confirm the account upgrade. The upgrade takes effect the next time the customer signs on (either SSO or to the admin portal).
4. Click **Save**.

Suspend a customer account

Before you begin

If you have a PingOne for Managed Service Providers account, you can suspend one of your customer accounts. This doesn't remove the account, but does remove the customer's ability to single sign-on (SSO) to PingOne or to access the admin portal. You can subsequently reactivate an account when the account status changes.

About this task

You'll choose a customer account to suspend. You need either to be a Global Admnistrator or Support Administrator (Read/Write) to suspend an account.

Steps

1. Select the **Customers** tab.
2. For the customer account, click in the green area (left) of the toggle button to suspend the account.

   Result:

   The customer will be unable to SSO or to access the admin portal.
3. To reactivate the account, click the grey area (right) of the toggle button.

Change a customer ID or account name

Before you begin

If you have a PingOne for Managed Service Providers account, you can change either the `MSP ID` value, the `Account Name` value, or both, for one of your customer accounts.

About this task

You'll choose a customer account to modify. You need either to be a Global Admnistrator to change the assigned MSP ID or the Account Name.

Copyright © 2025 Ping Identity Corporation

Steps

1. Select the **Customers** tab.
2. Expand the account details for the selected customer and click the edit icon.

   Result:

   The `MSP ID` and `Account Name` fields are now editable.
3. Enter a new value for either `MSP ID`, the `Account Name`, or both and click **Save**.

Reference

Administrative roles

The following table describes the administrative roles available in PingOne for Enterprise accounts.

You can assign administrators to a read-only role, which grants access to the areas of the admin portal normally allowed by that administrative role, but not the ability to change settings.

> **Note**
>
> Administrators can only be assigned one administrative role at a time.

In PingOne SSO for SaaS Apps accounts, the only administrative roles are **Audit & Report Administrator** and **Global Administrator**.

For PingOne SSO for SaaS Apps with Managed Accounts, managed accounts have the PingOne for Enterprise administrative roles.

Administrative Role	Description
Application Administrator	Can manage only the specific applications that you assign. After saving the role assignment, you can choose to limit the management permissions. An application administrator has access only to the admin portal pages associated with their assigned management permissions. For more information, see Assign Application Administrator applications.
Audit & Report Administrator	Can manage subscriptions for audit events and run reports. Can only access the following pages: • **SSO Dashboard** • **PingID Dashboard** • **Reporting**

Copyright © 2025 Ping Identity Corporation

Administrative Role	Description
Global Administrator	Has full permissions to manage and configure all aspects of the account and the admin portal, including the ability to manage all group and role assignments. Receives email notifications before and after certificate expiration. For more information, see Certificate management. For the PingOne for Enterprise Directory, assigning a user the global administrator role also assigns the user to the domain administrators group. If you set up the PingOne for Enterprise account, you are automatically assigned the role of global administrator.
Identity Repository Administrator	Manages the configuration of identity repositories. Can only access the following pages: • **Identity Repository** • **Dock** • **Authentication Policy** • **PingID** • **Certificates** • **Branding** • **User Directory** • **Users by Services** • **Reporting** • **SSO Dashboard** • **PingID Dashboard** The identity repository administrator can also view and modify the directory settings when using the PingOne for Enterprise Directory.
PingID Device Administrator	This role can only access **Users > Users by Service > PingID**. This role can unpair one or more user devices, or assign a device as the user's primary device. **Note** PingID Device Administrators have the optional ability to grant temporary MFA bypasses to users. To enable this permission, go to **Account > Administrators > Permissions** and select **Allow Bypass**. For more information about managing PingID device settings, see PingID User Life Cycle Management in the PingID documentation.

Copyright © 2025 Ping Identity Corporation

Administrative Role	Description
SaaS Administrator	Manages the Application Catalog and application connections. Receives email notifications before and after certificate expiration. For more information, see Certificate management. Can only access the following pages: • **My Applications** • **Application Catalog** • **PingID SDK Applications** • **OAuth Settings** • **User Groups** • **Users by Service** • **Authentication Policy** • **PingID** • **Certificates** • **Reporting** • **SSO Dashboard** • **PingID Dashboard**
Service User Administrator	Manages the PingOne for Enterprise services a user can use. This role includes the capabilities of the PingID Device Administrator. Can only access the following pages: • **Users by Service** • **Reporting**
Support Administrator	Has Read/Write permissions to the admin portal. Can impersonate and manage subtenants, but cannot make changes in parent account. Available only on PingOne for Enterprise for Managed Service Providers.

Error code reference

The following table describes common error messages in PingOne for Enterprise and PingOne SSO for SaaS Apps.

> **Note**
>
> **Error message 1** is the text of the error message that displays to users. **Error message 2** is the message that PingOne for Enterprise logs for internal review.

Copyright © 2025 Ping Identity Corporation

Error Code	Description	Error message 1	Error message 2
`AUTHN_005`	Invalid session.	`It looks like your session has expired or is invalid. Please sign in (SSO) again.`	`It looks like your session has expired or is invalid. Please sign in (SSO) again.`
`AUTHN_209`	OpenToken decoding error.	`We received an error while decoding the authentication response. Check your configuration or contact Ping Identity Customer Support.`	`Error in decoding authentication response. Please verify your configuration.`
`AUTHZ_001`	User is not in an authorized group for this application.	`Sorry, you're not authorized to access the requested resource. Check that you belong to one of the authorized groups.`	`You are not authorized to access the target resource. Please verify that you belong to one of the authorized group(s).`
`MFA_001`	Multi-factor authentication (MFA) failure.	`The multi-factor authentication was not successful. Please try again.`	`The multi-factor authentication was not successful.`
`MFA_003`	Missing PPM response.	`Missing PPMResponse`	`Missing PPMResponse`
`MFA_005`	Unsigned PPM response.	`The PPMResponse that we received is not signed.`	`The PPMResponse that we received is not signed.`
`MFA_006`	Invalid signature for PPM response.	`The signature of PPMResponse that we received is not valid. Please make sure that the key imported to PingOne matches the signing key configured in the authentication module.`	`The signature of PPMResponse that we received is not valid. Please make sure that the key imported to PingOne matches thesigning key configured in the authentication module.`
`MFA_008`	Expired MFA response.	`The assertion from 2nd factor authentication module has expired.`	`The assertion from 2nd factor authentication module has expired.`
`MFA_009`	Invalid nonce in PPM Response.	`The nonce in PPMResponse must be the same as the one in PPMRequest.`	`The nonce in PPMResponse must be the same as the one in PPMRequest.`

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise

Error Code	Description	Error message 1	Error message 2
`MFA_010`	Username in PPM response doesn't match PPM request.	`The user in PPMResponse must be the same as the one in PPMRequest.`	`The user in PPMResponse must be the same as the one in PPMRequest.`
`OIDC_001`	Invalid ID token from IdP.	`The id token from authorization service is invalid.`	`The id token from authorization service is invalid.`
`OIDC_002`	Failed to get tokens from IdP.	`Unable to retrieve tokens from authorization service. Please try again later.`	`Unable to retrieve tokens from authorization service. Please try again later.`
`OIDC_003`	Invalid `userinfo` response from IdP.	`The userinfo response from authorization service is invalid.`	`The userinfo response from authorization service is invalid.`
`OIDC_004`	Invalid Google API credentials (Google IdP only).	`A call to the Google Directory API service was rejected due to invalid credentials.`	`A call to the Google Directory API service was rejected due to invalid credentials.`
`REQ_001`	Connection for this `idpid` and `saasid` combination is disabled or doesn't exist.	`We're unable to process the SSO request. The request contains an invalid saasid or idpid value. Check that your registration is complete and the connection configured in PingOne is not disabled.`	`SSO request contained an invalid saasid or idpid. Please make sure the registration is complete and the connection is not disabled.`
`REQ_002`	Missing `saasid` or `idpid`.	`We are unable to determine which IdP to use for your SSO request. Check that you are using the idpid parameter in your SSO request (for example, https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<idpid>), and perform an IdP-initiated SSO or PingOne-initiated SSO first.`	`SSO request was missing a required parameter: saasid or idpid. An SSO request has following form https://sso.connect.pingidentity.com/sso/sp/initsso/?saasid=<saasid>&idpid=<idpid>`

Copyright © 2025 Ping Identity Corporation

Error Code	Description	Error message 1	Error message 2
`REQ_004a`	`appurl` or `errorurl` is not HTTPS.	`We're unable to process the SSO request. The request contains an invalid appurl or errorurl value. Check that the appurl and errorurl values you have specified use HTTPS.`	`Invalid appurl or errorurl: https is required.`
`REQ_004b`	Invalid `appurl` or `errorurl`.	`We're unable to process the SSO request. The appurl or errorurl value contains a line feed. Line feeds are not allowed.`	`Invalid appurl or errorurl: line feed is not allowed.`
`REQ_008`	AuthnRequest sent to wrong endpoint.	`We're unable to process the SSO request. Update your SP configuration to send the AuthnRequest to /sso/idp/SSO.saml2?idpid=<idpid>, where idpid is an optional parameter. If idpid is not specified, a user needs to perform an IdP-initiated SSO or PingOne-initiated SSO first.`	`Please update your SP configuration to send AuthnRequest to /sso/idp/SSO.saml2?idpid=<idpid>, where idpid is an optional parameter. If idpid is not specified, a user needs to perform an IdP-initiated SSO or PingOne-initiated SSO once first.`
`REQ_009`	Connection for this service provider (SP) `entityid` and `idpid` combination is disabled or doesn't exist.	`We're unable to process the SSO request. The request contains an invalid SP entityid or idpid. Check that your registration is complete and the connection to PingOne is not disabled.`	`SSO request contained an invalid sp entityid or idpid. Please make sure the registration is complete and the connection is not disabled.`
`REQ_011`	Cross-site request forgery (CSRF) failure during IdP discovery.	`CSRF validation failed.`	`CSRF validation failed.`
`SAML_001`	Missing AuthnStatement in response from IdP.	`We're unable to process the SAML response. The response is missing an AuthnStatement.`	`Invalid SAML response. Missing AuthnStatement.`

Copyright © 2025 Ping Identity Corporation

Error Code	Description	Error message 1	Error message 2
SAML_002	Invalid SAML response from IdP.	We're unable to process the SAML response. The response is invalid. Contact your system administrator or Ping Identity Customer Support for more information.	Invalid SAML response
SAML_003	IdP returned failure.	We received an unsuccessful response from your IdP. Contact your administrator or an IdP administrator for more information.	Unsuccessful SAML response
SAML_003.1	No status in response from IdP.	We received a response with no status from your IdP. Contact your administrator or an IdP administrator for more information.	PingOne received a response with no status from your IdP. Please contact your administrator or authenticating authority for more information.
SAML_005	No application specified in response from IdP.	We're unable to find a SaaS for the SAML response received. Send the saasid either as a relaystate value (https://pingone.com/1.0/<saasid>) or as an ACS URL parameter (saasid=<saasid>). To find the saasid of the application, log into your APS account and view the application details.	Unable to find a SaaS for the SAML response received. Please send saasid either as a relaystate (https://pingone.com/1.0/<saasid>) or as an ACS URL parameter (saasid=<saasid>). To find the saasid of the application, log into your APS account and view the application details.

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise

Error Code	Description	Error message 1	Error message 2
SAML_006	Unable to find target for specified SP entity ID.	We're unable to find the correct settings for the SAML response received. Verify that the Entity ID setting in your PingOne configuration matches the Entity ID of your identity bridge (IdP), and that the correct saasid parameter value is being sent with your SAML messages.	We're unable to find the correct settings for the SAML response received. Verify that the Entity ID setting in your PingOne configuration matches the Entity ID of your identity bridge (IdP), and that the correct saasid parameter value is being sent with your SAML messages.
SAML_100	Invalid assertion from IdP.	We received an invalid assertion. Contact your administrator or Ping Identity Customer Support for more information.	Invalid assertion.
SAML_200	Invalid signature from IdP.	The Signature is invalid. Check that your signing certificate is the same certificate uploaded to PingOne.	Invalid Signature. Please make sure that your signing certificate matches the certificate uploaded to PingOne.
SAML_201	Invalid certificate for this connection.	The certificate is invalid. Check that your signing certificate has not expired.	Invalid Certificate. Please verify that the signing certificate is valid and that the certificate has not expired.
SAML_202	Invalid issuer from IdP.	The issuer is invalid. Check that the IdP entityid value matches the entityid value configured for the IdP in PingOne.	Invalid Issuer. Please verify that the IdP entityid matches the entityid that is configured for the IdP in PingOne.
SAML_202.1	Missing issuer in assertion from IdP.	There's no issuer in the assertion we received.	No Issuer in the assertion.
SAML_202.2	Missing issuer in SAML response from IdP.	There's no issuer specified in the SAML response we received.	No Issuer in the SAML response.

Copyright © 2025 Ping Identity Corporation

Error Code	Description	Error message 1	Error message 2
`SAML_203`	Invalid `RelayState` from IdP.	`The RelayState value is not a valid URL. Check that the RelayState URL uses HTTPS and that the domain specified matches the configured domain for the application.`	`Invalid URL in RelayState. Please verify that the RelayState URL uses HTTPS and that the domain matches the configured domain for the application.`
`SAML_209`	Missing signature in assertion from IdP.	`It looks like the Signature is missing.`	`Missing Signature.`
`SAML_210`	Missing `nameid` in assertion from IdP.	`It looks like the NameID is missing.`	`Missing NameID.`
`SAML_211`	Invalid XML from IdP.	`We're unable to parse the XML message.`	`Unable to parse the XML message.`
`SAML_212`	Unable to decrypt assertion from IdP.	`We're unable to decrypt the assertion. Check that the PingOne certificate is used to encrypt the assertion from your IdP.`	`Unable to decrypt the assertion. Please make sure that the PingOne certificate is used to encrypt the assertion from your IdP.`
`SAML_213`	Invalid `RelayState` from IdP.	`The RelayState value is not valid. Check that the format for the RelayState value is: https://pingone.com/1.0/<saasid>?appurl=<appurl>. Notice the delimiter between the saasid value and the appurl parameter. The RelayState value we received was:`	`Invalid RelayState. Please verify the format of the RelayState: https://pingone.com/1.0/<saasid>?appurl=<appurl>. Pay close attention to the delimiter between the saasid and the appurl. The received RelayState was:`
`SAML_214`	Certificate in assertion doesn't match configuration.	`There is a certificate mismatch. Your signing certificate does not match the certificate uploaded to PingOne.`	`Certificate mismatch. Your signing certificate does not match the certificate uploaded to PingOne.`

Copyright © 2025 Ping Identity Corporation

PingOne for Enterprise

Error Code	Description	Error message 1	Error message 2
`SAML_218`	Invalid single logout (SLO) request.	`We're unable to process the message received at the SLO endpoint. The request is missing either SAMLRequest or SAMLResponse.`	`Unknown message was received at SLO endpoint. Missing SAMLRequest or SAMLResponse.`
`SAML_219`	Unable to verify SLO signature, no certificate configured.	`It looks like the signing certificate has not been configured.`	`Missing certificate. Please check your configuration.`
`SAML_220`	Invalid signature for SLO request.	`The Signature for the SLO Request or Response is invalid. Check that your signing certificate matches the certificate uploaded to PingOne.`	`Invalid Signature for Logout Request/Response. Please make sure that your signing certificate matches the certificate uploaded to PingOne.`
`SAML_223`	Expired request.	`The request you sent is outdated. This can be due to an old entry in the browser cache or a bookmark to a transient login page. Try restarting your browser and using the application URL again.`	`The request you sent is outdated. This can be due to an old entry in the browser cache or a bookmark to a transient login page. Try restarting your browser and using the application URL again.`
`SAML_224`	Invalid request to assertion consumer service (ACS) URL.	`We received a request without a SAML Response. A request was made to the PingOne Assertion Consumer service, but we found no SAML Response message in the request.`	`Missing SAML Response. A request was made to PingOne Assertion Consumer service. However, SAML Response message was not found.`
`SSO_001`	Unknown error occurred.	`We're unable to complete the authentication process with the Identity Provider (IdP). You can try to connect to the application again later or contact an administrator.`	`Generic exception`

Copyright © 2025 Ping Identity Corporation

Error Code	Description	Error message 1	Error message 2
`SSO_002`	Invalid request.	`Due to an invalid request, we're unable to complete the authentication process with the Identity Provider (IdP). You can try to connect to the application again later or contact an administrator.`	`Invalid request exception`
`SSO_206`	Missing required attribute from IdP.	`The response from your IdP is missing a required attribute(s). Check that all necessary attributes are being sent by your IdP.`	`The response from your IdP was missing the required attribute(s). Please review the attributes sent by your IdP.`
`SSO_206c`	Missing required attribute from IdP.	`The response from your IdP or a secondary module is missing a required attribute(s). Check that all necessary attributes are being returned.`	`The response from your IdP or a secondary module was missing the required attribute(s). Please review the attributes returned.`
`SSO_208.1`	Invalid advanced attribute mapping configuration.	`We've had a system error: An unknown transformation function is being used in attribute mapping. Please update your attribute mapping configuration in PingOne.`	`System Error: An unknown transformation function is used in attribute mapping.`
`SSO_208.2`	Invalid advanced attribute mapping configuration.	`We've had a system error: An unknown builder function is being used in attribute mapping. Please update your attribute mapping configuration in PingOne.`	`System Error: An unknown builder function is used in attribute mapping.`

Copyright © 2025 Ping Identity Corporation

Error Code	Description	Error message 1	Error message 2
`SYS_001`	Internal error.	`We're unable to complete Single Sign-On (SSO) at this time. Contact your system administrator or Ping Identity Customer Support for more information.`	`Internal server error`
`SYS_004`	Unknown configuration error.	`It looks like there's a configuration error. Contact your administrator or Ping Identity Customer Support for help.`	`There is a configuration error.`
`SYS_404`	Requested page doesn't exist.	`The resource you requested does not exist on this server.`	`The resource you requested does not exist on this server.`

If you encounter an error not listed here, sign on to the Ping Identity Support Portal and open a case.

PingOne for Enterprise security best practices

Keep your applications and data secure with the following tips and tools.

Multi-factor authentication

Multi-factor authentication (MFA) improves security by requiring your users to verify their identity in at least two ways to access PingOne for Enterprise. Usually, this is a combination of their username and password credentials combined with a biometric validation or one-time passcode (OTP) from email, a YubiKey, or the PingID mobile app.

You can configure MFA settings in the **Setup > PingID** menu. Learn more in Configure PingID authentication in the PingID documentation.

You can also separately configure MFA for administrative users at **Setup > Authentication Policy**. For more information, see Create or update an authentication policy.

Administrative role assignment

PingOne for Enterprise supports a number of different Administrative roles. When assigning administrative roles, you should follow the principle of least privilege, meaning that administrators have only as much access as they need to complete their job functions.

This practice reduces the impact of compromised accounts and reduces the likelihood of insider privilege abuse.

You should also conduct regular reviews of administrative access to determine whether they require and use the privileges they have, and whether they need greater or lesser levels of access. This also helps prevent privilege creep, or gradual accumulation of access rights beyond what an administrator needs to do their job.

Copyright © 2025 Ping Identity Corporation

For instructions on assigning administrative roles, see Assign administrative roles.

Signing algorithm selection

Every SAML assertion includes a signature to verify the authenticity of the sender. More complex algorithms used to generate these signatures make SAML assertions more secure.

You should use at least 256-bit encryption. In most cases, PingOne for Enterprise uses 256-bit signing algorithms by default, but you can improve security further by increasing the complexity of the algorithms.

For more information, see the following:

- Connecting to a custom SAML provider
- Create a signing certificate
- Adding or updating a SAML application

Application management

Not all applications have the same risk profile. Some applications might contain more sensitive data or perform critical operations.

The following settings allow you to strengthen security for your more sensitive applications:

- Assign applications to a group. Any application that isn't assigned to a group is available to all of your users.
- Configure an authentication policy. An authentication policy lets you require additional MFA for certain applications, certain user groups, or both.
- Configure SLO endpoints. You can set single logout (SLO) endpoints for each SAML application to make sure that user sessions in the application end promptly.

Session lifetime

Session lifetime is the length of time that PingOne for Enterprise caches a user's authenticated status and allows a user to access an application without contacting the identity provider (IdP) to re-validate the user.

The session idle timeout is the duration that an authenticated user's session can be idle before being signed out.

The value of these settings should depend on the sensitivity of the applications on the dock and user activity patterns. If you have more sensitive applications, you should set a shorter session lifetime. If your users share computers or often leave computers unattended, you should set shorter session lifetime and idle time.

To configure the **Maximum Session Lifetime** and **Session Idle Timeout**, go to **Setup > Dock > Configuration**.

Reporting

Data breaches are commonly made worse by being undiscovered for weeks or even months. Some organizations don't discover breaches until they're alerted by third parties. That's why it's important to review security logs regularly.

PingOne for Enterprise audit logs are available at **Dashboard > Reporting**. In addition to the predefined reports, you can run custom reports that can help you detect unusual access activity

Copyright © 2025 Ping Identity Corporation

Most report types are also available as Push or Poll subscriptions to a third-party service. You can then configure that service to alert you to suspicious event types. Subscriptions allow you to monitor PingOne for Enterprise activity on a regular basis without having to run manual reports. For more information, see Subscriptions.

The following are a few examples of how you can use custom report types:

- Use the **Administrator Login** report to detect suspicious administrator access from unusual times, IP addresses, or browser agents.
- Use the **SSO** report to detect unauthorized access to specific applications.
- Use the **Directory** report to detect unexpected account creation in the PingOne for Enterprise Directory.

PingOne for Enterprise use cases

The following use case links can help you with common PingOne for Enterprise configurations.

- Configuring SP-Initiated SSO in PingOne for Enterprise
- Setting up an authentication flow that includes MFA (PingOne for Enterprise and PingID)
- Integrating CyberArk with PingOne for Enterprise
- Configuring authentication request signing in PingOne for Enterprise
- Configuring SSO for GlobalProtect VPN with PingOne for Enterprise
- Configuring OIDC authentication for AWS EKS clusters

Copyright © 2025 Ping Identity Corporation

PingOne SSO for SaaS Apps

PingOne SSO for SaaS Apps is a cloud solution that connects your customers securely to your applications.

> **Note**
>
> If you have a PingOne for Enterprise license, see PingOne for Enterprise. If you're not sure which license you have, see Which PingOne am I using?.

PingOne SSO for SaaS Apps operational status

See Ping Identity Services for the operational status of all Ping Identity services, including PingOne SSO for SaaS Apps, which runs on the PingOne for Enterprise platform. You can also choose to subscribe to alert notifications.

You can also connect to the following heartbeat endpoints to monitor PingOne SSO for SaaS Apps operational status:

- SSO: https://sso.connect.pingidentity.com/sso/heartbeat
- Admin Portal: https://admin.pingone.com/web-portal/heartbeat

Get started with PingOne SSO for SaaS Apps

- Assign administrators
- Assign branding and design
- Configure your user profile
- Configure SSO to the admin portal

Copyright © 2025 Ping Identity Corporation

Administering your PingOne SSO for SaaS Apps account

- Edit administrative roles, permissions, and notifications
- Manage certificates
- Monitor usage with reports and subscriptions

Manage applications in PingOne SSO for SaaS Apps

- Add a SaaS application
- Integrate an application
- Connect customers to your application
- PingOne SSO for SaaS Apps and SLO
- Finding the `idpId` value

PingOne SSO for SaaS Apps with Managed Accounts

PingOne SSO for SaaS Apps with Managed Accounts includes all of the features of a PingOne SSO for SaaS Apps license, as well as additional functionality to manage your partner accounts.

- Manage partner accounts

Copyright © 2025 Ping Identity Corporation

PingOne SSO for SaaS Apps reference

- PingOne SSO for SaaS Apps Customer Connection API
- About multiplexing
- What is an idpId?
- Error code reference
- PingOne SSO for SaaS Apps security best practices

PingOne SSO for SaaS Apps overview

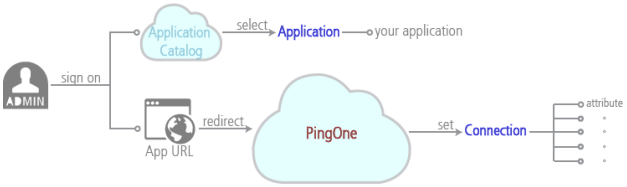
PingOne SSO for SaaS Apps PingOne SSO for SaaS Apps is for Service Providers (SPs) who want to provide customers secure, single sign-on (SSO) to cloud applications. Your applications are published to our Application Catalog for either private or public availability.

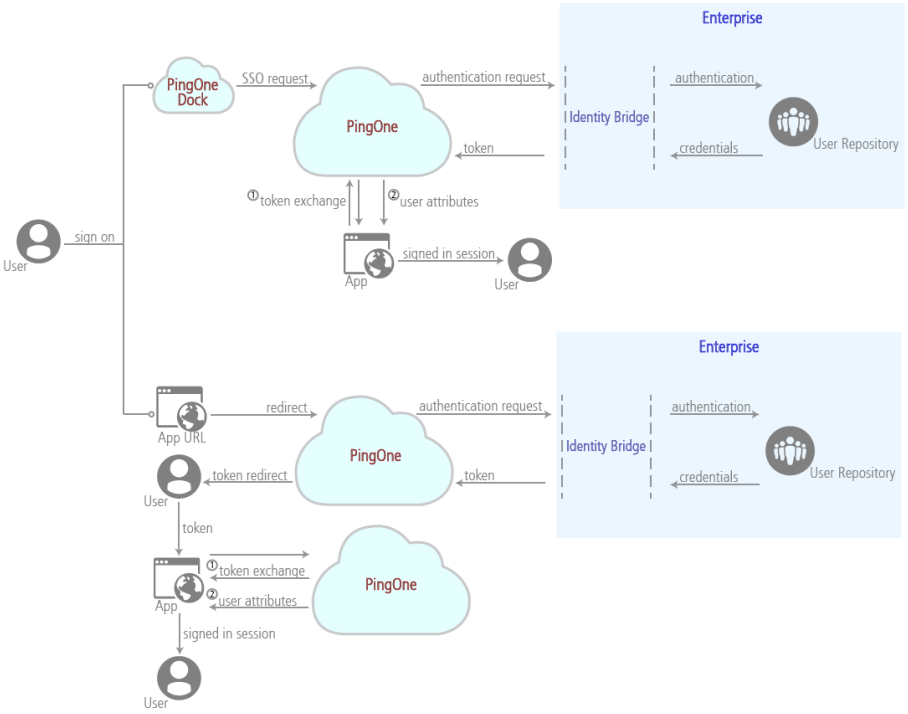
Log in to the PingOne admin portal to set up, configure and maintain your PingOne account.

> **Note**
>
> If you forget your password, click **Change My Password** on the login page to reset your password. After 3 attempts to log in with the wrong credentials, you're locked out for 15 minutes. Further login attempts during the 15 minute lockout period do not reset or change the lockout duration.

Copyright © 2025 Ping Identity Corporation

How It Works





Update the PingOne SSO for SaaS Apps universal certificate

If your universal certificate is about to expire or has expired, you must update it.

About this task

For application connections that are multiplexed, or are manually configured customer connections, the PingOne SSO for SaaS Apps universal certificate is the primary and renewal certificate, used for both verification and encryption. In these cases, when notified, you need to update the PingOne universal certificate.

Check the **Dashboard** in the PingOne SSO for SaaS Apps admin portal to see whether a certificate is due to expire. PingOne SSO for SaaS Apps will also send you an email notifying you when the universal certificate is nearing expiration.

Steps

1. For manually configured customer connections, to update the PingOne SSO for SaaS Apps universal certificate:
    1. In the PingOne SSO for SaaS Apps admin portal, go to the **Customer Connections**, select the application and click **Details > Edit**.

Copyright © 2025 Ping Identity Corporation

2. For **Verification Certificate**, click the dropdown list and select the **Renewal Certificate**.
3. **Optional:** If you choose to download the PingOne SSO for SaaS Apps metadata, the updated PingOne SSO for SaaS Apps (Renewal) certificate and Encryption certificate is included in the metadata file.
4. **Optional:** You can also choose to separately download any of the certificates:
    - Existing (expiring) Verification certificate
    - New Renewal certificate
    - New Encryption certificate
5. Click to **Save** your changes.

2. For all other multiplexed applications, select to update each application that uses multiplexing and update the certificate. See Adding or updating a SAML-enabled application for instructions.

Getting started

About this task

Use this workflow to guide you in making your applications available to your customers:

Steps

1. Configure your account.

   If you have not already added administrators and branding for your PingOne SSO for SaaS Apps account, start here.

2. Add a SaaS application.

   When you add an application, you can choose whether the application is to be publicly available or private (available only to selected customers).

3. Integrate an application.

   How you will integrate your application with PingOne is determined by whether customer SSO to your application is initiated through the identity provider (IdP), or through your service.

4. Manage partner accounts.

   For managed accounts, you'll set up and administer the PingOne for Enterprise accounts your partners will use to connect to your applications.

5. Connect customers to your application. You can choose how you want to create the connection, based on your customer use case:

   Choose from:

    - Partner account applications
    - Invited SSO
    - Application Catalog app connection

Copyright © 2025 Ping Identity Corporation

- Direct SAML connection

6. Use auditing event reports and subscriptions to monitor customer use of your applications.

   See Managing reports and subscriptions for more information.

Configure your account

Assign administrators

About this task

Members of your organization who are assigned the Global Administrator role can manage the PingOne for SaaS Apps account. If you created the account, you are automatically assigned Global Administrator permissions.

You can also choose to assign an Audit & Report Administrator. Administrators having this role can manage subscriptions for audit events and run reports. They have access only to the Reporting and Dashboard pages.

Steps

1. Select the **Account > Administrators**.
2. Click **Add Administrator**.
3. Enter the **First Name**, **Last Name**, and **Email** for the administrator you want to add.
4. From the **Role** list, select the administrator role to assign.

   For more information about administrative roles and permissions, see Administrative roles.
5. If you want to assign read-only permissions to the administrator role, click the **Read Only** checkbox.
6. Click **Save**. An email invitation is sent to the person you're inviting. The email invitation is valid for 3 days, or until a new invitation is sent.

   When the person clicks the PingOne link in the email to accept the invitation, they're prompted to assign a password.
7. Repeat these steps for each of the administrators you want to add.

Assign branding and design

About this task

Assign your organization's branding for the IdP Discovery page and the associated error page. Both of these pages are displayed to users.

Steps

1. Go to the **Account > Branding** page.
2. In the **Corporate Logo** section, click the **Add** and browse for the logo that you want to assign.
3. To create a banner message, enter text into the **Banner Message** field.

Copyright © 2025 Ping Identity Corporation

The banner will display at the top of the admin portal, and will only be visible to your administrative users.

4. In the **Backgrounds** section, select from the following:

   Choose from:

   - **Main Background**. Select one of the following:
   - **None**: No background color or image. The background is white by default.
   - **Image**: Click **Choose Background** and navigate to the image that you want to use as the dock background.

     > **Note**
     >
     > Images larger than 3000 x 1500 are automatically resized, resulting in possible loss of quality.

   - **Color**: Select a background color from the dropdown color palette, or enter the Hex color code you require.
   - **Form Background Color**: Select a background color from the dropdown color palette, or enter the Hex color code you require.

5. In the **Buttons** section, select from the following:

   Choose from:

   - **Button Color**: Select a button color from the dropdown color palette, or enter the Hex color code you require.
   - **Font Color**: Select a font color for button labels from the dropdown color palette, or enter the Hex color code you require.

6. In the **Text** section, select from the following:

   Choose from:

   - **Form Fill Color**: Select a fill color to use for the form from the dropdown color palette, or enter the Hex color code you require.
   - **Form Font Color**: Select a font color to use for text from the dropdown color palette, or enter the Hex color code you require.
   - **Link color**: Select a color to use for links from the dropdown color palette, or enter the Hex color code you require.
   - **Header and Custom Text Color**: Select the color to use for the header and custom text from the dropdown color palette, or enter the Hex color code you require.

7. In the **Content** section, select from the following:

   Choose from:

   - Select whether to display application icons on the IdP Discovery page.
   - **IdP Discovery Page Text**: Enter any custom text to display in the IdP Discovery form (300 characters maximum).
   - **Error Page Header**: Enter any custom text to display in the header for the error page (100 characters maximum).
   - **Error Page Text**: Enter any custom text to display on the the error page (300 characters maximum).

Copyright © 2025 Ping Identity Corporation

8. Click **Save**. The changes are applied and will be immediately visible on the IdP Discovery page and the associated error page.

Manage your user profile

View and edit your user profile on the **User Settings** page.

Steps

- In the top right corner of the admin portal, click your name to open the **User Settings** page.
- Click **Edit** to change your profile information.

  Your administrative role is displayed, but cannot be changed, on this page. For information on changing your administrative role, see Editing administrative roles, permissions, and notifications.
- To change your name, enter new names in the **First Name** and **Last Name** fields.
- To change your email, enter a new email address in the **Email** field.

  If you change your email address, you will receive a confirmation email that you must respond to before the change is applied.
- To change your password, enter your current password in the **Current Password** field, and your new password in the **New Password** and **Confirm New Password** fields.
- To change your default time zone, select a location from the **Time Zone** list.

  > **Note**
  >
  > If you choose a different time zone when creating a report, that time zone overrides your default time zone.

- To change your certificate notification settings,

  1. Select **Expiring Certificate Warnings** to enable emails when certificates will be expiring soon.
  2. Select **Expired Certificate Alerts** to enable emails when certificates have expired.

  > **Note**
  >
  > These options are only available for Global and SaaS administrators.

- To apply changes, click **Save**.

Editing administrative roles, permissions, and notifications

Global administrators can edit the permissions for other administrators.

About this task

You cannot change the administrative role for the administrator currently signed on to the admin portal. In this case, you must sign on as a different global administrator.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> In PingOne for Enterprise for Managed Service Providers, you can change the administrative role for the currently signed-on administrator on the customer account. You can also disable or delete this administrator on the customer account.

Steps

1. Go to **Account > Administrators**.
2. Expand the line for the administrator whose profile you want to edit.
3. Click the **Pencil icon**.
4. To change the administrator's name, enter new names in the **First Name** and **Last Name** fields.
5. In the **Role** list, select the new administrative role to assign.

   For more information about administrative roles and permissions, see Administrative roles.
6. Select the **Read Only** box to allow the administrator to read data for their role but prohibit them from making system changes.
7. If the administrator is a global or software as a service (SaaS) administrator, click **Notifications** to edit the alerts they receive regarding certificate management.
   1. Select the **Expiring Certificate Warnings** checkbox to enable emails alerting this administrator when certificates will be expiring soon.
   2. Select the **Expired Certificate Alerts** checkbox to enable emails alerting this administrator when certificates have expired.
   3. Select the **Expiring Certificate Warnings (Customer Accounts)** checkbox to enable email alerts alerting this administrator when your customer accounts have a certificate will be expiring soon.
   4. Select the **Expired Certificate Alerts (Customer Accounts)** checkbox to enable email alerts when your customer accounts have expired certificates.

      Clearing these options only affects email notifications. Dashboard certificate warnings still appear.

      > **Note**
      >
      > The **Customer Accounts** notification options are only available to global or support admins on PingOne for Enterprise for Managed Service Providers or global admins on PingOne SSO for SaaS Apps with Managed Accounts licenses.
8. If the administrator is an application administrator, click **Delegated Administration** to edit their application delegations.

   For more information, see Assign Application Administrator applications.
9. Click **Save**.

Configure SSO to the admin portal

Grant administrative users single sign-on (SSO) access to the PingOne SSO for SaaS Apps admin portal.

Copyright © 2025 Ping Identity Corporation

About this task

To permit service-provider (SP)-initiated SSO to the admin portal, you must configure the connection between the portal and your identity provider (IdP).

Steps

1. In the admin portal, go to **Setup > Admin Portal SSO > IdP Configuration**.
2. **Optional:** Import the IdP metadata.

   Choose from:

   - To upload the metadata file, click **Select File**.
   - To enter the metadata URL, click **Or use URL**.
3. In the **Entity ID** field, enter the entity ID provided by the IdP.
4. In the **SSO Endpoint** field, enter the endpoint at the IdP to which PingOne sends AuthnRequests.
5. On the **Verification Certificate** line, click **Select File** to browse and upload the IdP's public signing certificate that PingOne will use to sign SAML assertions.
6. In the **Single Logout Endpoint** field, enter the IdP endpoint to which PingOne will send single logout (SLO) requests.
7. In the **Single Logout Response Endpoint** field, enter the IdP endpoint to which PingOne will send SLO responses.
8. On the **Single Logout Binding Type** line, click either the **Redirect** or **Post** button to determine which binding type PingOne will use to send SLO requests.
9. Select the **Sign the AuthnRequest** box to make PingOne sign AuthnRequests to the IdP.
10. To download the PingOne signing certificate for upload to your IdP, click **Download**.
11. From the **Signing Algorithm** list, select the algorithm PingOne will use to sign AuthnRequests to the IdP.
12. To download the PingOne metadata for upload to your IdP, click **Download PingOne Metadata**.
13. Click **Save Settings**.
14. Go to **Setup > Admin Portal SSO > Group Permissions**.
15. For each admin group you want to authorize to SSO, click **Add Group**.

    If you're using LDAP groups, this needs to be the full distinguished name (FDN) for the administrator group (`CN=admins,OU=example,…`).

    > **Note**
    >
    > You can assign groups to a read-only administrative role, which grants the administrator access to the areas of the admin portal normally allowed by that role, but not the ability to change settings.
16. Click **Save**.

Result

Copyright © 2025 Ping Identity Corporation

Your administrative users can sign on from the **Initiate Single Sign-On (SSO) URL** displayed at **Setup > Admin Portal SSO > IdP Configuration** after you complete the form.

Next steps

If you also intend to initiate SSO from your IdP, you must configure your IdP to append one of the following parameters to PingOne's ACS URL:

- `RelayState=https://pingone.com/1.0/8bfe0aeb-79ca-4fd4-a116-c3f7c7dbe6ca`
- `saasid=8bfe0aeb-79ca-4fd4-a116-c3f7c7dbe6ca`

Add a SaaS application

As a service provider (SP), you'll make your cloud application available to your customers through PingOne SSO for SaaS Apps.

Steps

1. Go to **Applications > My Applications**.
2. Select the type of application you're adding:.

   Choose from:

   - For instructions to add a SAML application, see Adding or updating a SAML-enabled application.
   - For instructions to add an OpenID Connect (OIDC) application, see Manage OAuth settings, Configuring your OAuth settings and Adding or updating an OIDC application.

Adding or updating a SAML-enabled application

Create a SAML application for your customers to connect to.

About this task

When you're adding or updating a SAML-enabled application, you'll need to specify the proper SAML configuration to establish a connection for your application.

Steps

1. Go to **Applications > My Applications > SAML**.
2. Click **Add New Application**.
3. On **Basic information** tab, select the category that applies to your application.
4. Enter the application name and a description that will identify your application to users.
5. Select whether your application is to be made publicly available (listed in the Application Catalog), or privately available (not listed in the Application Catalog, and available to organizations only at your invitation).
6. **Optional:** Upload a logo and icon to use for your application. The logo is used for workstation users. The icon is displayed for mobile users.

Copyright © 2025 Ping Identity Corporation

PNG is the only supported graphics format.

7. Click **Continue to Next Step** and choose **Yes, it is SAML-enabled**.
8. **Optional:** On the Create Connections page, select the SAML version supported by your application. If you're uncertain, the default version (SAML 2.0) is generally correct.
9. **Upload Metadata**. Click **Select File** to upload the application's metadata file, or click **Or use URL** to enter the URL of the metadata file. The **ACS URL** and **Entity ID** will then be supplied for you. If you don't upload the application metadata, you'll need to enter this information manually with values provided by the application.

   > **Note**
   >
   > The application's **Entity ID** must be unique within your account. You can't configure more than one application in PingOne SSO for SaaS Apps using the same SP entity ID.

10. **Optional:** Choose whether or not to enable SAML multiplexing (the default).

    For more information about application multiplexing, see About multiplexing.

11. Select the public signing certificate to use. PingOne SSO for SaaS Apps will use this certificate on your behalf to sign SAML assertions. You can choose either:

    Choose from:

    - Primary Certificate

      When you select the primary certificate, the PingOne SSO for SaaS Apps metadata for download contains both the primary and the renewal certificates.

    - Renewal Certificate

      When you select the renewal certificate, the PingOne SSO for SaaS Apps metadata for download contains only the renewal certificate. A renewal certificate is available only thirty days before the expiration of the primary certificate.

      > **Note**
      >
      > If you are using multiplexing, the primary and renewal certificates are PingOne SSO for SaaS Apps universal certificates. In this case, when you're notified to update the certificate, it's imperative that you do so.

      1. You can also choose to download the certificates independently (not as part of the PingOne SSO for SaaS Apps metadata). To do this, scroll down to the certificate **Download** links and click the appropriate link.

         The Signing Certificate download link is for the certificate you selected in the **Signing Certificate** dropdown list. The other certificate is the certificate you didn't select in the **Signing Certificate** dropdown list. Note the expiration dates for the certificates.

         If a certificate is identified as Expired, currently, we'll still accept it. At some point, we may no longer accept the certificate, so we recommend you install a valid certificate soon. Note that your IdP or an application may not accept an expired certificate.

Copyright © 2025 Ping Identity Corporation

12. You need to supply the PingOne SSO for SaaS Apps connection information to each customer connecting to your application. You can either:
    - Click **Download** to retrieve all of SAML metadata for the PingOne SSO for SaaS Apps connection.
    - Copy the displayed connection information (for **SSO Service URL** and **Entity ID**) and download the PingOne SSO for SaaS Apps signing certificate.
13. **Optional:** Enter the URL for the SAML **Single Logout Endpoint**. We send the single logout (SLO) request to this URL using the binding type you select for **Single Logout Binding Type**.

    The attributes for **Single Logout Endpoint**, **Single Logout Binding Type** and **Verification Certificate** are interdependent. To support SLO, you'll need to specify all of these attribute values, and optionally, **Single Logout Response Endpoint**. See PingOne for Enterprise and SLO for more information.

    > **Note**
    >
    > If you choose not to support SLO for an application, when the user session ends the application will not be notified.

14. **Optional:** Enter the URL for the SAML **Single Logout Response Endpoint**. If you don't assign a value here, **Single Logout Endpoint** is also used as the response endpoint. You send the application SLO response to this URL.
15. **Optional:** Select the binding type to use for SLO. This can be **POST** or **Redirect** (defaults to **POST**).
16. **Optional:** Upload the signing certificate you'll use to sign SLO requests. This can be the same certificate you use for SAML assertions.
17. Click **Signing Algorithm** to choose the algorithm used to sign both SAML assertions and SLO requests.

    If you are setting up a new application, the signing algorithm defaults to the recommended SHA-256.

    If you have an existing application configuration, SHA-1 may be displayed as the default signing algorithm. We recommend you change it to SHA-256 at your convenience.
18. **Optional: Encrypt Assertion**. If selected, the assertions sent from PingOne SSO for SaaS Apps for the application will be encrypted. Available for SAML 2.0 multiplexed applications only.

    Selecting this option will prompt you for the information necessary to encrypt the assertion:

    ### *Encryption Certificate*

    Upload the certificate to use to encrypt the assertions.

    ### *Encryption Algorithm*

    Choose the algorithm to use for encrypting the assertions. We recommend **AES_256** (the default), but you can select **AES_128** instead.

    ### *Transport Algorithm*

    The algorithm used for securely transporting the encryption key. Currently, **RSA-OAEP** is the only transport algorithm supported.
19. Verify that all entries are correct, then click **Continue to Next Step**. The SSO Attribute Requirements page is displayed.

Copyright © 2025 Ping Identity Corporation

On the SSO Attribute Requirements page, click **Add Attribute** to add any attributes necessary for SSO to your application.

20. **Optional:** Click on the **Name** or **Description** of any existing attribute to edit the value. Press Enter to save your changes or Esc to cancel.

    Click the **Required** checkbox for any attributes that require a value for SSO to your application.

    Click **Continue to Next Step**.

    On the Create Instructions page, for **Introduction Text**, enter text introducing your application and supplying any necessary instructions to users.

    For **SSO Configuration Path**, enter user guidance for the location of any SSO settings for your application.

    For **SSO Configuration Page URL**, enter the URL for any SSO settings for your application.

    For **Configuration Steps**, click **Add Step** to add stepped instructions for configuring SSO for your application.

    For **SSO Configuration Page Screenshot**, click **Select Image** to upload a screenshot of the SSO configuration page for your application.

    On the Publish page, click **Add Parameter** to assign any connection parameters customers can use for your application. You can elect to make the parameters required.

    On the Publish page, verify that the information is correct, then click **Save & Publish**.If you have selected to publish your application publicly, it is submitted to us for registration. When we have processed the registration for your application, your application information is published in the Application Catalog.

    Your application is displayed in the listing on your My Applications page, where you can view or edit all of the your application settings as needed.

    If you have selected to publish your application privately, the application will not be listed in the Application Catalog. Instead, you will invite customers to connect to your application. See Customer connection methods for instructions.

Result

After you have published an application, you will not be able to change the SSO connection type(s). You will need to remove the application, then add it again in this case. However, you can change configuration settings for the SSO connections.

Next steps

To test your application before connecting to a customer, see Testing your application using the built-in IdP or Testing your application using PingOne for Enterprise.

Adding or updating an OIDC application

Create a new OpenID Connect (OIDC) application, or modify an existing application in PingOne SSO for SaaS Apps.

Before you begin

Before you initially add an OICD application, you need to configure the access token your account will use for OIDC applications. These are account-level settings that will be inherited at the application level when you add or update and application, as you are doing here.

PingOne SSO for SaaS Apps returns OIDC user attributes in different ways depending on the `response_type` parameter.

Copyright © 2025 Ping Identity Corporation

The contents of the ID token depend on whether or not the application also returns an access token:

- For flows that return both an access token and an ID token (such as authorization code flow, or implicit flows where the `response_type` includes `token`) the ID token contains the `sub` and, if requested, `email` scopes. The `userinfo` endpoint contains all of the attributes for the requested scopes and attributes configured on the **User Info** tab for the application, if the `openid` scope was requested.
- For flows that don't return an access token, the ID token contains all of the attributes for the requested scopes and any attributes configured on the **User Info** tab for the application, if the `openid` scope was requested. The `userinfo` endpoint is inaccessible in this case because no access token is issued.

The access token contains attributes configured at **Applications > OAuth Settings > Access Token**.

See Manage OAuth settings and Configuring your OAuth settings.

About this task

When updating an application, any changes you make to the existing configuration parameters will be reflected in your customer's or partner's connection to the application.

However, if your customer or partner has changed the parameter settings in their PingOne for Enterpriseaccount, their local settings will override your updated configuration.

In other words, configuration updates made by a service provider at the application level will not override configuration updates made at the connection level.

Steps

1. Go to **Applications > My Applications > OIDC**.
2. Add a new application or edit an existing application.

   Choose from:

   - To create a new application, click **Add Application**. See Step 3 for new application types.
   - To update an existing application, expand the application and click the **Pencil** icon. Skip to Step 4.
3. Select the type of application you want to add and click **Next**:

   Choose from:

   - To create an application that is accessed and used within a browser, click **Web App**.
   - To create an application that is stored locally and run on a desktop or device, click **Native App**.
   - To create an API-driven front-end application, such as applications using Node.js or Angular, click **Single Page App**.
   - If you want full control of all available configuration parameters, click **Advanced Configuration**.
4. In the **Application Name** field, enter a name for the application.
5. In the **Short Description** field, enter a description of the application.

   Customers will be able to see your description.
6. In the **Category** list, select a category for the application.

Copyright © 2025 Ping Identity Corporation

7. **Optional:** Click **Icon** to add an icon for this application.

   The icon file can be up to 1 Mb in size. The supported graphics formats are JPG, PNG and GIF.

8. Click **Next**.

9. **Optional:** To enable or disable a custom valid duration for the application access token, click the **Override Access Token Lifetime** toggle.

   When this control is enabled, a **Minutes** selector is displayed. The valid range is 1 - 60 minutes. The default value is inherited from your account-level OAuth settings.

10. If you enabled the override, enter the number of minutes access token lifetime in the **Minutes** field.

    The valid range is 1 - 60 minutes. The default value is inherited from your account-level OAuth settings. For more information, see Configuring your OAuth settings.

11. Select the grant types allowed for the application.

    Available grant types are determined by the application type. For more information, see OIDC application grant types.

12. If you selected **Refresh Token**, configure the token settings:

    1. Click the **Override Refresh Idle Lifetime** toggle to override the global OAuth setting for the application.
    2. In the **Refresh Token Idle Lifetime** field, enter the number of minutes that a refresh token can be idle before being used again.
    3. Click the **Override Refresh Token Max Lifetime** toggle to override the global OAuth setting for this application.
    4. In the **Refresh Token Max Lifetime** field, enter the maximum number of minutes that a refresh token can be valid.

13. Copy the **Client ID**, **Discovery URL**, and **Issuer** values to use later in integrating the application with PingOne SSO for SaaS Apps.

14. **Optional:** For applications that use the Authorization Code grant type, you can click **Add Secret** to generate up to two client secrets to pair with the client ID.

15. Click **Next**

16. **Optional:** In the **Start SSO URL** field, enter the URL to use for SSO to the application.

    This is the URL to which application users will redirect to initiate SSO to PingOne for Enterprise using OIDC.

17. In the **Redirect URI** field, enter URIs for PingOne SSO for SaaS Apps to send responses to for the application's authorization requests.

    > **Tip**
    >
    > Click **Add URL** to define multiple redirect URIs.

18. **Optional:** In the **Logout URI** field, enter the URI to which PingOne for Enterprise sends a user for single logout (SLO).

19. Click **Next**

Copyright © 2025 Ping Identity Corporation

20. Click **Add Attribute** to configure attributes returned by the `UserInfo` endpoint for this application when the `openid` scope is included in the authorization request.

    1. In the **Attribute Name** field, enter a name for the attribute.
    2. Select the **Required** checkbox to require the attribute mapping when a UserInfo request is made for this application.

       The `sub` (Subject) attribute is required for all UserInfo requests.

    The `idpid` attribute is used by PingOne for Enterprise to identify the identity provider (IdP), and is included in the attribute contract by default.

21. Click **Next**.
22. Click the **+** icon to add scopes to the allowed list, or click the **-** icon to remove them.

    These OAuth user scopes are the user resources to which the application will request access. The `openid` scope is expected to always be included in the authorization request.

23. Click **Save**.

Result

The new OIDC application is added to your **My Applications** list for OIDC. You can edit the application configuration as needed by expanding the application and clicking the **Pencil** icon. Refer to this documentation when updating configuration values.

Next steps

Integrate the application with PingOne SSO for SaaS Apps. See Integrating an OIDC application for instructions.

Add or update other applications

You can add applications to PingOne SSO for SaaS Apps that are neither SAML nor OpenID Connect (OIDC). These are software as a service (SaaS) applications that you make available directly to customers or partners.

About this task

PingOne SSO for SaaS Apps handles most of the connection details for these applications and will send single sign-on (SSO) users to the URL that you specify for an application.

However, you will need to set up the referenced page to process the security token sent from PingOne and create a user session for the authenticated user. See Process the PingOne SSO for SaaS Apps token exchange for more information.

Each application connection is multiplexed, meaning PingOne SSO for SaaS Apps will use the same connection to the application for all customers or partners.

Steps

1. Go to **Applications > My Applications > SAML** and click **Add New Application**.
2. In the **Category** list, select the category that applies to your application.
3. In the **Name** field, enter a name for your application.
4. In the **Description** field, enter a description for your application.

Copyright © 2025 Ping Identity Corporation

5. Select a visibility option for your application:

   Choose from:

   - Click **Public** to add your application to the Application Catalog.
   - Click **Private** to make your application available only to the organizations you invite.

6. **Optional:** Upload an icon and logo for your application.

   > **Note**
   >
   > If you're using the current version of the dock, you don't need to add a logo.

7. Click **Continue to Next Step**.
8. On the **Create Connections** page, click **No, I want to enable through PingOne**.
9. **Optional:** In the **Hostname or Domain** field, enter the host or domain name associated with your application.

   > **Tip**
   >
   > If your application has only one entry point, make your application more secure by leaving the **Hostname or Domain** field empty to disable the `appurl` parameter.
   > If you must use `appurl`, a domain such as `app.example.com` can provide stricter validation than `example.com`.

10. On the **Binding Type** line, select the binding type to use for sending tokens to this application.

    > **Tip**
    >
    > The default binding type of **Post** is more secure, because it doesn't expose the token as a query parameter in the URL.

11. In the **Default Application URL** field, enter an application URL to send authenticated users to.

    > **Tip**
    >
    > Although both HTTP and HTTPS URLs are accepted in this field, HTTPS is more secure for production applications.

    The page for this URL will need to process the security token sent from PingOne SSO for SaaS Apps and create a user session. For more information, see Process the PingOne SSO for SaaS Apps token exchange.

12. **Optional:** In the **Error URL** field, enter a URL to direct users to in case of an error.

    If you don't specify an error URL, PingOne SSO for SaaS Apps will display a generic error page.

13. **Optional:** Select the **Allow Customization** to allow PingOne for Enterprise accounts to override the **Default Application URL** and **Error URL** when they configure this application from the application catalog.

    > **Note**
    >
    > This option is available only if you make your application visibility **Public**.

Copyright © 2025 Ping Identity Corporation

14. In the **Entity ID** field, enter a unique identifier for SAML connections to this application.

    If you don't specify an entity ID, PingOne SSO for SaaS Apps uses either PingConnect or the application's `saasid`, depending on what connection type you select during connection configuration.

    If a custom entity ID is in use by a non-multiplexed connection, it cannot be changed.

    For more information, see Creating a manual SAML connection.

15. Click **Continue to Next Step**.

16. **Optional:** To add SSO attributes, click **Add Attribute**.

Field	Action
Name	Enter a name for the attribute.
Description	Enter a description for the attribute.
Required	Select the checkbox to make the attribute required for SSO.
Advanced	Click to configure advanced attribute options. For more information, see Creating advanced attribute mappings.

17. Click **Continue to Next Step**.

18. On the **Create Instructions** tab, enter instructions to guide a user in enabling SSO for this application.

> **Note**
>
> This tab only appears if you made your application public in step 5.

    1. In the **Introduction Text** field, enter text introducing your application and supplying any necessary instructions to users.
    2. **Optional:** In the **SSO Configuration Path** field, enter navigation instructions to guide users to your application's SSO configuration page.
    3. **Optional:** In the **SSO Configuration Page URL** field, enter the URL for your application's SSO configuration page.
    4. **Optional:** For each configuration step that you want to add, click **Add Step**, and fill in the **Label** and **Instruction** fields.
    5. **Optional:** To add an image, click **Select Image** and browse to the image you want to upload.

19. Click **Continue to Next Step**.

20. On the **Publish** tab, verify that the information is correct, then click **Save & Publish**.

    If you made your application public, it's submitted to us for registration. After we have processed the registration for your application, your application information is published in the Application Catalog.

Copyright © 2025 Ping Identity Corporation

Your application displays in the listing on your **My Applications** page, where you can view or edit all of the your application settings.

If you made your application private, you must invite customers to connect to your application. For instructions, see Customer connection methods.

> **Note**
>
> After you publish an application, you cannot change the SSO connection types. You must remove the application and add it again. However, you can change the configuration settings for the SSO connections.

Next steps

To test your application before connecting to a customer, see Testing your application using the built-in IdP or Testing your application using PingOne for Enterprise.

PingOne for Enterprise and SLO

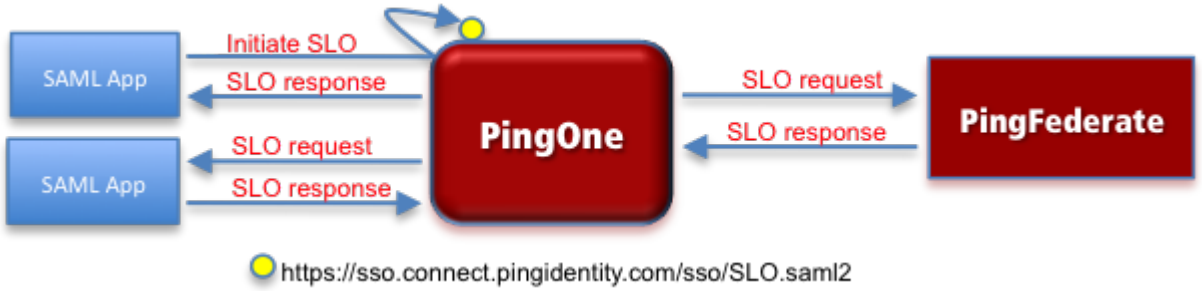
PingOne for Enterprise uses a single logout (SLO) process to log out all participants of a PingOne for Enterprise session. In the PingOne for Enterprise context, the session participants are the identity repository, PingOne for Enterprise, and any applications to which a user has signed on (SSO) for the session.

Any one of the session participants can initiate SLO. PingOne for Enterprise acts as the session authority, mediating the SLO request and response messages so that all participants are notified. In this way, when a user logs off, the PingOne for Enterprise session is ended for all participants.

PingOne for Enterprise supplies three SLO endpoints, each for a particular purpose:

`https://sso.connect.pingidentity.com/sso/SLO.saml2/`

This is the normal SAML endpoint to receive SLO requests and responses. It can be used only by SAML applications or SAML IdPs. Here's an illustration of standard SAML SLO:



1. The user logs out of the SAML application, which results in an SLO request to PingOne.
2. PingOne for Enterprise redirects the request to `https://sso.connect.pingidentity.com/sso/SLO.saml2`.
3. PingOne for Enterprise sends SLO requests to the IdP and the other SAML application.
4. PingOne for Enterprise ends the user session.
5. PingOne for Enterprise sends the SLO response (session ended) to the SAML application.

You can append the optional `idpid` parameter to limit SLO only to sessions with the specified `idpid` value.

Copyright © 2025 Ping Identity Corporation

The format for the `idpid` parameter is:

```
https://sso.connect.pingidentity.com/sso/SLO.saml2/?idpid=<idpid value>
```

https://sso.connect.pingidentity.com/sso/initslo/

This is the PingOne for Enterprise endpoint to which non-SAML applications are redirected in response to their logout request. Here's an illustration initiated by a non-SAML application:

1. The user logs out of the non-SAML application, which results in an logout request to PingOne for Enterprise.
2. If specified, PingOne for Enterprise redirects the request to `https://sso.connect.pingidentity.com/sso/initslo/?page=<landing page URL>`.
3. PingOne for Enterprise sends SLO requests to the IdP and the other SAML application.
4. PingOne for Enterprise ends the user session.

You can append the optional `page` parameter to specify a URL to direct logged out users to.

The format for the `page` parameter is:

```
https://sso.connect.pingidentity.com/sso/initslo/?page=<landing page URL>
```

If you specify the `page` parameter, PingOne for Enterprise will validate it. To be valid, an SLO `page` parameter value must meet one of the following criteria:

- The URL has the same hostname as the identity provider's (IdP's) SSO URL.
- The URL has the same hostname as the URL of one of the applications in the current session.
- The URL has the same hostname as the `Assertion Consumer Service URL` of one of the applications in the current SSO session.
- The domain of the URL is in the domain list of one of the applications in the current SSO session.
- The URL is https://desktop.pingone.com/*.
- The URL is https://sso.connect.pingidentity.com/*.

If we're unable to validate the SLO page parameter value, the logout process continues and the page parameter is ignored. The PingOne default logout landing page then will be displayed.

Copyright © 2025 Ping Identity Corporation

You can append the optional `idpid` parameter to limit SLO only to sessions with the specified `idpid` value.

The format for the `idpid` parameter is:

```
https://sso.connect.pingidentity.com/sso/initslo/?idpid=<idpid value>
```

`https://sso.connect.pingidentity.com/sso/terminatesession?page=logoutPageUrl`

This is the PingOne for Enterprise endpoint to which other participants are redirected when SLO isn't supported or isn't configured. The logout requests can be from non-SAML applications, non-SAML IdPs, or from a SAML IdP that doesn't have SLO configured. Here's an illustration of a session termination initiated by a non-SAML application and using Google as the IdP. In this case *logoutPageUrl* is `https://accounts.google.com/Logout`:

1. The user logs out of the non-SAML application, which results in a logout request to PingOne for Enterprise.
2. PingOne for Enterprise redirects the request to https://sso.connect.pingidentity.com/sso/terminatesession?page=https://accounts.google.com/Logout.
3. PingOne for Enterprise ends the user session.

> **Note**
>
> `{google} uses OpenID Connect as the authentication protocol, which does not support SLO.`

You can append the optional `page` parameter to specify a URL to direct logged out users to. The format for the `page` parameter is:

```
https://sso.connect.pingidentity.com/sso/terminatesession?page=logoutPageUrl
```

If you specify the `page` parameter, PingOne for Enterprise will validate it. To be valid, an SLO `page` parameter value must meet one of the following criteria:

- The URL has the same hostname as the identity provider's (IdP's) SSO URL.
- The URL has the same hostname as the URL of one of the applications in the current session.
- The URL has the same hostname as the `Assertion Consumer Service URL` of one of the applications in the current SSO session.
- The domain of the URL is in the domain list of one of the applications in the current SSO session.
- The URL is https://desktop.pingone.com/*.

Copyright © 2025 Ping Identity Corporation

- The URL is https://sso.connect.pingidentity.com/*.

If we're unable to validate the SLO page parameter value, the logout process continues and the page parameter is ignored. The PingOne for Enterprise default logout landing page then will be displayed.

You can append the optional `idpid` parameter to limit SLO only to sessions with the specified `idpid` value.

The format for the `idpid` parameter is:

```
https://sso.connect.pingidentity.com/sso/terminatesession?idpid=<idpid value>
```

Integrate an application

Connect your existing application to PingOne SSO for SaaS Apps.

OIDC applications

The PingOne SSO for SaaS Apps OAuth endpoints for OpenID Connect (OIDC) applications are available at `https://sso.connect.pingidentity.com/client_id/.well-known/openid-configuration`, where *client_id* is the **Client ID** entry in the **Details** section of the summary page for the application.

For more information, see Integrating an OIDC application.

PingOne SSO for SaaS Apps REST Authentication

The PingOne SSO for SaaS Apps REST service uses HTTP Basic authentication. When calling the REST API you need to authenticate to PingOne SSO for SaaS Apps using these credentials (Base64-encoded) in the Basic authentication header:

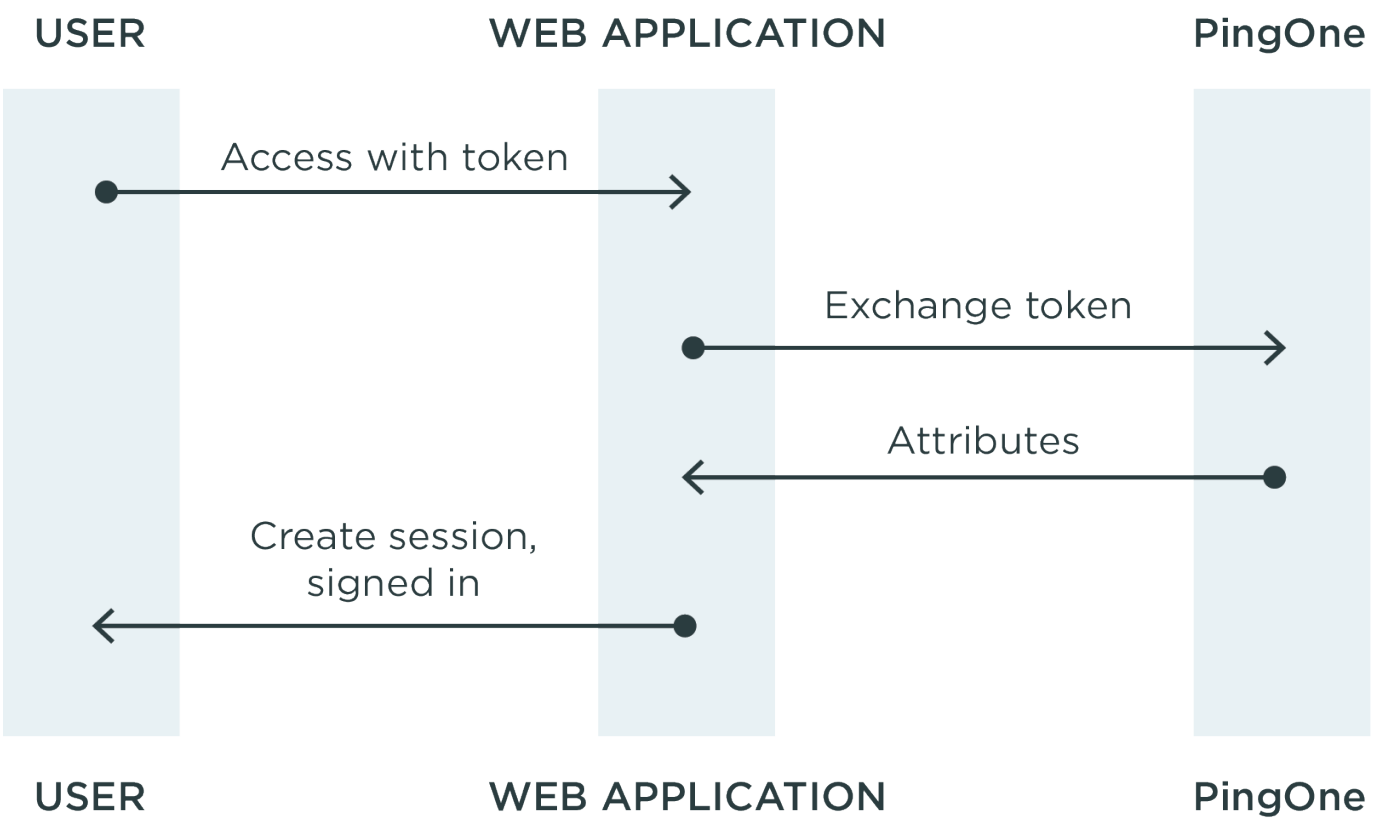
- `username`: Your REST username is the REST API Client ID value automatically assigned in the PingOne SSO for SaaS Apps admin portal on the **Account > Integration** page.
- `password`: Your password is also specified on this page as the **REST API Client Secret** value. You need to assign a REST API Client Secret value before using your credentials. For more information, see Using the global REST API client credentials.

IdP-initiated SSO

When the single sign-on (SSO) process begins from the identity bridge side, the user authentication to the identity bridge is already done. You just need to create a session for the user when they return to your application with a secure token from PingOne SSO for SaaS Apps. Your application makes a REST call to the PingOne SSO for SaaS Apps REST service using this token. This completes the PingOne SSO for SaaS Apps token exchange that authenticates the user and returns the user attributes. The SSO session for the user is then initiated.

Here's a sequence diagram illustrating these steps:

Copyright © 2025 Ping Identity Corporation



For IdP-initiated SSO, start with Process the PingOne SSO for SaaS Apps token exchange.

SP-initiated SSO

When you begin the SSO process from your side, as a Service Provider (SP), you need to:

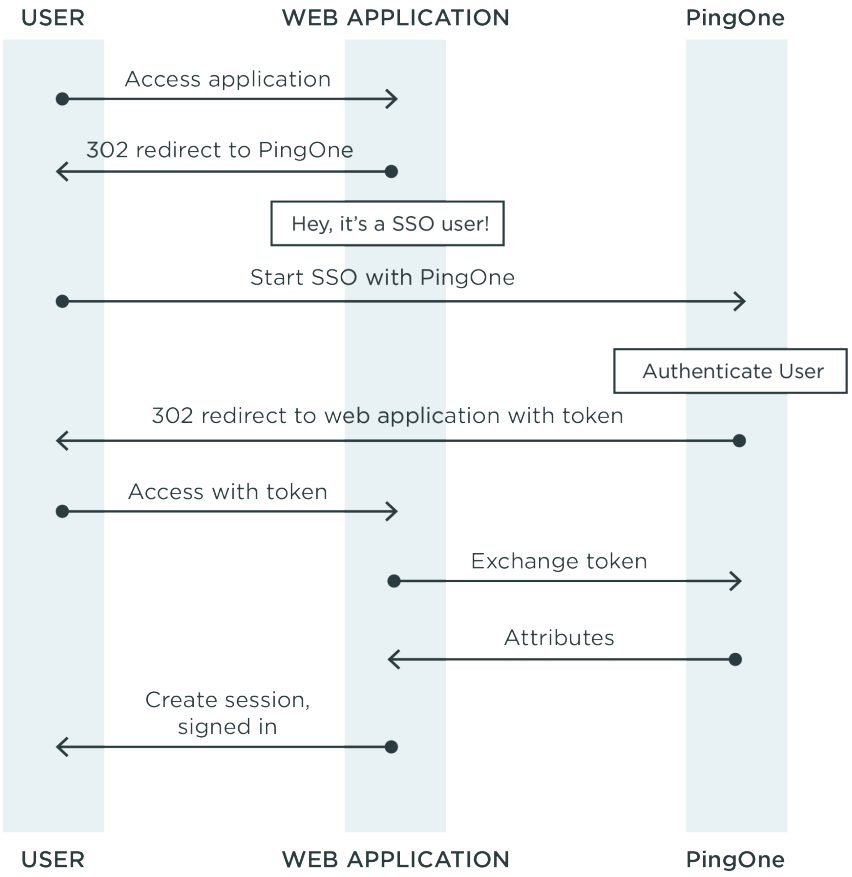
1. Redirect a user's browser to PingOne SSO for SaaS Apps to start SSO. PingOne SSO for SaaS Apps will then authenticate the user at the IdP.
2. Create a session for the user when they return to your application with a secure token from PingOne SSO for SaaS Apps.

So, what you need to know about are HTTP redirects and how to create user sessions within your application.

After a user is authenticated through PingOne SSO for SaaS Apps, the user arrives at your application via an HTTP redirect with a security token. Your application makes a REST call to the PingOne SSO for SaaS Apps REST service using this token. This completes the PingOne SSO for SaaS Apps token exchange that authenticates the user and returns the user attributes.

Here's a sequence diagram illustrating these steps:

Copyright © 2025 Ping Identity Corporation



After you've determined that a user accessing your application is trying to perform SSO, you redirect that user's browser to PingOne SSO for SaaS Apps using an HTTP 302 redirect. PingOne SSO for SaaS Apps needs to know a few things to successfully process an SSO request:

1. Who is the user?
2. Where should I send this user to authenticate?
3. (Optional) Where should I send this user after they've authenticated?
4. (Optional) Where should I send this user if something goes wrong?

For SP-initiated SSO, start with Redirect users to PingOne SSO for SaaS Apps (SP-initiated SSO).

PingOne SSO for SaaS Apps token exchange

After authenticating, the user returns to your application with a token. We create this token as a one-time secret between you, the user, and PingOne SSO for SaaS Apps.

The token exchange is a one-time only REST call. After the first call, the token expires. Subsequent calls using this token will return HTTP 404.

You use the PingOne SSO for SaaS Apps REST API to make a REST call and initiate the token exchange. Our Token Resolution Service will process the exchange and we will return the set of attributes for the user.

Copyright © 2025 Ping Identity Corporation

The PingOne SSO for SaaS Apps token exchange process is secured at each stage:

- The REST call uses TLS.
- The REST call is authenticated.
- The token can only be exchanged by you.
- The token can only be exchanged once, then it expires.

Your REST call needs to:

1. Identify the token you're exchanging.
2. Specify the return format for the user attributes.

For more information, see Process the PingOne SSO for SaaS Apps token exchange.

HTTP status codes

HTTP status codes are likely familiar to you. Status codes that can be returned to you include:

Code	Description
`200 OK`	Success. The requested token is returned.
`400 Bad Request`	The request format isn't supported.
`401 Unauthorized`	The HTTP Basic authentication failed.
`404 Not Found`	The requested resource or token doesn't exist. For tokens, this can mean the `saasid` value used in the request doesn't match the `saasid` value in the token.

Integrating an OIDC application

After you Add or update an OIDC application, you need to integrate it with PingOne SSO for SaaS Apps.

Before you begin

See Adding or updating an OIDC application to add an application to PingOne SSO for SaaS Apps.

About this task

When you integrate an OpenID Connect (OIDC) application, PingOne SSO for SaaS Apps will act as the OAuth provider for your application. Your application then needs to request authorization from the PingOne SSO for SaaS Apps OAuth authorization endpoint when users attempt to single sign-on (SSO) to the application.

See the OpenID Connect Core 1.0 specification for reference when integrating the application.

The authorization request flow depends on the grant type you have selected for the application. The grant type can be **Authorization code**, **Implicit**, or a hybrid (both code and implicit).

Copyright © 2025 Ping Identity Corporation

For more information, see OIDC application grant types.

Steps

1. Go to **Applications > My Applications > OIDC**.
2. Expand the details to display the summary page for the OIDC application to integrate.

   Result:

   The unique **Client ID** and **Discovery URL** for the application is displayed in the **Details** section.
3. Copy the **Discovery URL** and enter it in a new browser tab.

   Result:

   PingOne SSO for SaaS Apps returns OIDC configuration information, including the endpoints you will use to integrate the application.

Copyright © 2025 Ping Identity Corporation

Code

Code grant type

For any grant type, the application needs to send the authorization request to the PingOne SSO for SaaS Apps authorization endpoint returned by the **Discovery URL**(`https://sso.connect.pingidentity.com/sso/as/authorization.oauth2`).

PingOne SSO for SaaS Apps sends the response to the authorization request to the URL you assigned to the **Redirect (Callback) URI** setting when you created the application. You can find this URL in the **Authentication Flow** section on the application summary page.

PingOne SSO for SaaS Apps validates the `redirect_uri` parameter against the list of redirect URIs specified in the application's configuration. You can find these URIs in the **Authentication Flow** section on the application summary page. If the `redirect_uri` is valid, PingOne SSO for SaaS Apps sends the response to the specified redirect URI.

If your application uses an authorization code grant type, PingOne SSO for SaaS Apps uses the following process to complete the authorization request:

1. The application sends an authorization request for a code grant type.

   Here is an example of an authorization request URI:

   ```
   https://sso.connect.pingidentity.com/sso/as/authorization.oauth2?
   client_id=cdd237bb-3404-4ad4-90eb-d2e2528xxxxx&scope=openid&response_type=code
   ```

   The following table describes the parameters that make up the authorization request URI.

Parameter	Description
`client_id`	Your client ID, assigned by PingOne for Enterprise. You can find this value on the **Details** tab.
`scope`	The user resources that can be accessed by the application. The `openid` scope is expected to be specified, either as the sole scope value or one of the scope values.
`response_type`	This must be `code`. An authorization code is then returned in the response.

Copyright © 2025 Ping Identity Corporation

Parameter	Description
`code_challenge`	This PKCE parameter is either plain text or a cryptographic hash of a random string. The random string or plain text must be a `code_verifier` value that you will include in the subsequent token request. **Note** Use PKCE only when you aren't using a client secret, including `client_secret` in the token request. For more information, see OAuth 2.0 RFC 7636.
`code_challenge_method`	This PKCE parameter is required only when `code_challenge` is specified. This can be either: ◦ `plain` When the `code_challenge_method` value is plain text ◦ `S256` When the `code_challenge_method` value is an SHA-256 cryptographic hash **Note** When you subsequently include the `code_verifier` value in the token request, the `code_challenge` value and the `code_verifier` value must match. For more information, see OAuth 2.0 RFC 7636.
`login_hint`	Used to specify either the idpid or an email domain. If you specify the idpid, the user is redirected to the IdP associated with the idpid value for the current application, identified in PingOne SSO for SaaS Apps by the `saasid` parameter. If you specify an email domain as the `login_hint` value, the domain must be included in the IdP Discovery configuration for the application and tenant. For more information about IdP Discovery for your connection type, see: ◦ Edit an invited customer connection ◦ Edit a managed customer connection ◦ Enable IdP discovery for partner accounts

2. The PingOne for Enterprise authorization endpoint returns the authorization code to the application.

Copyright © 2025 Ping Identity Corporation

The HTTPS response will be similar to this:

```
https://example.com/#code=IDa4e54a98b90b234476819295a791e4a95bbb9a6e1a3095b50200000164fbeb8b43
```

3. The application uses the authorization code returned in the response to request an access token and ID token from the PingOne for Enterprise token endpoint, https://sso.connect.pingidentity.com/sso/as/token.oauth2 .

   Here is an example request using cURL:

   ```
   curl -k -X POST -H "Accept: application/json" -d 'client_id=cdd237bb-3404-4ad4-90eb-
   d2e2528xxxxx&client_secret=CpquMknCg9An9Up1Ys2mnVEdKkCDaxtJcJG4adFPBDnPU6SBp7VNGUhyTmaJXXmpR&grant_typ
   e=authorization_code&code=ID5d7d1770409374639980ce161952fda57b21db562ff8320b020000016543fxxxxx&redirec
   t_uri=https://example.com\' \https://sso.connect.pingidentity.com/sso/as/token.oauth2
   ```

   Because the authorization request did not include PKCE parameters, the token request must use the client secret value assigned when the application was added to PingOne SSO for SaaS Apps. You can find the assigned client secret in the **Details** tab.

4. The application validates the `id_token` returned. For more information see the OpendID Connect Core 1.0 specifications.

5. The application can also optionally validate the token or access token returned.

   Use the PingOne for Enterprise introspection endpoint returned by the **Discovery URL** `https://sso.connect.pingidentity.com/sso/as/introspect.oauth2` to validate the access token.

   For access tokens that are signed rather than encrypted, you can also use the JWKS URI returned by the **Discovery URL** `https://sso.connect.pingidentity.com/sso/as/jwks`.

   > **Note**
   >
   > You can see your access token settings at **Applications > My Applications > OAuth Settings**. For more information, see Configuring your OAuth settings.

Copyright © 2025 Ping Identity Corporation

Implicit

Implicit grant type

For any grant type, the application needs to send the authorization request to the PingOne SSO for SaaS Apps authorization endpoint returned by the **Discovery URL**(`https://sso.connect.pingidentity.com/sso/as/authorization.oauth2`).

PingOne SSO for SaaS Apps sends the response to the authorization request to the URL you assigned to the **Redirect (Callback) URI** setting when you created the application. You can find this URL in the **Authentication Flow** section on the application summary page.

PingOne SSO for SaaS Apps validates the `redirect_uri` parameter against the list of redirect URIs specified in the application's configuration. You can find these URIs in the **Authentication Flow** section on the application summary page. If the `redirect_uri` is valid, PingOne SSO for SaaS Apps sends the response to the specified redirect URI.

If your application uses an authorization implicit grant type, PingOne SSO for SaaS Apps uses the following process to complete the authorization request:

1. The application sends an authorization request for an implicit grant type.

   Here is an example of an authorization request URI:

   ```
   https://sso.connect.pingidentity.com/sso/as/authorization.oauth2?
   client_id=930bc6bc-4bee-4ad4-90eb-
   d2e2528xxxxx&scope=openid&response_type=id_token%20token&nonce=Q4CLVJYiQbfLKoEovYyg
   ```

   The following table describes the parameters that make up the authorization request URI.

Parameter	Description
`client_id`	Your client ID, assigned by PingOne SSO for SaaS Apps. You can find this value on the **Details** tab.
`scope`	The user resources that can be accessed by the application. The `openid` scope is expected to be specified, either as the sole scope value or one of the scope values. **Note** When `openid` is not specified and the `response_type` value indicates `id_token`, an `id_token` is not returned.
`response_type`	This can either be `id_token`, `token` (access token), or both. The token or tokens specified are returned in the response.

Copyright © 2025 Ping Identity Corporation

Parameter	Description
`nonce`	This is used to securely associate `client_id` with `id_token`. For more information, see OpenID Connect Core 1.0 Nonce Implementation Notes.
`login_hint`	Used to specify either the idpid or an email domain. If you specify the idpid, the user is redirected to the IdP associated with the idpid value for the current application, identified in PingOne SSO for SaaS Apps by the `saasid` parameter. If you specify an email domain as the `login_hint` value, the domain must be included in the IdP Discovery configuration for the application and tenant. For more information about IdP Discovery for your connection type, see: ◦ Edit an invited customer connection ◦ Edit a managed customer connection ◦ Enable IdP discovery for partner accounts

2. The PingOne SSO for SaaS Apps authorization endpoint returns the `response_type` value to the application.

   If you included `id_token` and `token` in the authorization request, as in the example, an access token is returned with the `id_token` value in the response.

   The HTTPS response will be similar to this:

   ```
   https://example.com/
   #access_token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjQ4RUU0RjNGRDEyQTcwMUFERjYzMzEwMTRENzIzMzUyRDE3(
   653sxLCeTx8u_QD84fTPv8guFjir2iDylqi9vV2t-
   O6F_HfPJCank7IqWv50V7Apum3BnDpD1OBJtwlHNFmb2NGDgydDEegCCrlaEfHNjTogiqGISdoDsPAbUGWelRoGRrYmNt-
   aJGACwqqfiVVVRux7DARB8rF4opMwXRJM3FmjuA3_hVDbldl48NoA3TGJukmWg-2risFxUTuFnQmHgv1JZQhSiCH30YJtIleih9J1XnvrtH
   te2W-
   sc3RcelpRAIUi6lbBmmDrj2cvaTThSVzin-8Ho9PAZTJcUHHLnyPyOxFgaN7OO8T1WRCsEc_loCuTNdyYThxbepkd1m8Q9BwcK3w-
   VG0GEomQI4yKDp7FvqDjt4pbupMWjSujBYwDjARdL05nUAvvWFnXrNMaYY0aWxm793qG-VlXhm1WYmLgA
   ```

3. If an `id_token` was included in the authorization request, the application validates the `id_token` returned.

   For more information, see the OpenID Connect Core 1.0 specifications.

4. The application can also optionally validate the token (access token) returned.

   Use the PingOne SSO for SaaS Apps introspection endpoint returned by the **Discovery URL** `https://sso.connect.pingidentity.com/sso/as/introspect.oauth2` to validate the access token.

   For access tokens that are signed rather than encrypted, you can also use the JWKS URI returned by the **Discovery URL** `https://sso.connect.pingidentity.com/sso/as/jwks`.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> You can see your access token settings at **Applications > My Applications > OAuth Settings**. For more information, see Configuring your OAuth settings.

Copyright © 2025 Ping Identity Corporation

Hybrid

Hybrid grant type

For any grant type, the application needs to send the authorization request to the PingOne SSO for SaaS Apps authorization endpoint returned by the **Discovery URL**(`https://sso.connect.pingidentity.com/sso/as/authorization.oauth2`).

PingOne SSO for SaaS Apps validates the `redirect_uri` parameter against the list of redirect URIs specified in the application's configuration. You can find these URIs in the **Authentication Flow** section on the application summary page. If the `redirect_uri` is valid, PingOne SSO for SaaS Apps sends the response to the specified redirect URI.

PingOne SSO for SaaS Apps validates the `redirect_uri` parameter against the list of redirect URIs specified in the application's configuration. You can find these URIs in the **Authentication Flow** section on the application summary page. If the `redirect_uri` is valid, PingOne SSO for SaaS Apps sends the response to the specified redirect URI.

If your application uses both code and implicit grant types, PingOne SSO for SaaS Apps uses the following process to complete the authorization request:

1. Your applications sends an authorization request for a hybrid grant type.

   Here's an example of an authorization request URI:

   ```
   https://sso.connect.pingidentity.com/sso/as/authorization.oauth2?
   client_id=cdd237bb-3404-4ad4-90eb-
   d2e2528xxxxx&scope=openid&response_type=code%20id_token%20token&nonce=Q4CLVJYiQbfLKoEovYyg
   ```

   The following table describes the parameters contained in the authorization request URI.

Parameter	Description
`client_id`	Your client ID, assigned by PingOne SSO for SaaS Apps. You can find this value on the **Details** tab.
`scope`	The user resources that can be accessed by the application. The `openid` scope is expected to be specified, either as the sole scope value or one of the scope values. **Note** When `openid` is not specified and the `response_type` value indicates `id_token`, an `id_token` is not returned.
`response_type`	This can be any or all of the following: ◦ `code` ◦ `id_token` (as in the above example) ◦ `token` (access token) The specified tokens are returned in the response along with the authorization code.

Copyright © 2025 Ping Identity Corporation

Parameter	Description
`nonce`	Required when `id_token` is included in `response_type`. It is used to securely associate `client_id` with `id_token`. For more information, see OpenID Connect Core 1.0 Nonce Implementation Notes.
`code_challenge`	This PKCE parameter is either plain text or a cryptographic hash of a random string. The random string or the plain text must be the `code_verifier` value that you will include in the subsequent token request. **Note** Use PKCE only when you aren't using a client secret, including `client_secret` in the token request.
`code_challenge_method`	This PKCE parameter is required only when `code_challenge` is specified. This can be either: ◦ `plain` When the `code_challenge` value is plain text. ◦ `S256` When the `code_challenge` value is an SHA-256 cryptographic hash. **Note** When you subsequently include the `code_verifier` value in the token request, the `code_challenge` value and the `code_verifier` value must match.
`login_hint`	Used to specify either the idpid or an email domain. If you specify the idpid, the user is redirected to the IdP associated with the idpid value for the current application, identified in PingOne SSO for SaaS Apps by the `saasid` parameter. If you specify an email domain as the `login_hint` value, the domain must be included in the IdP Discovery configuration for the application and tenant. For more information about IdP Discovery for your connection type, see: ◦ Edit an invited customer connection ◦ Edit a managed customer connection ◦ Enable IdP discovery for partner accounts

Copyright © 2025 Ping Identity Corporation

2. The PingOne SSO for SaaS Apps authorization endpoint returns the `response_type` value or values to the application. If you included `code`, `id_token`, and `token` in the authorization request, as in the example, an authorization code, `access_token`, and `id_token` are all returned in the response.

   The HTTPS response will be similar to this (using the fragment response method):

   ```
   https://example.com/
   #code=ID453b3dfe58d55eed052373d0dc8dcfe2b0f03c234f569fc50200000165483652ee&access_token=eyJhbGciOiJSUzI1Ni
   hgmJb_ZVXFEbFred-L-LBIagLCdqppUUSYLrdXPM7W-XIhiR0rlLiWYtlk9S2g2wAzVyFv-JG1J-
   OUp555Vh3QJvedXll0l3MM42UTrSn3D0QuZQDWLYFiMB730FVhXWWyTaDpaYOCX0JnMWv_TYaJhxGj5tngWr7pBNYWqINpk4PrNlDfp65a
   BYoepgBawThLIy948h7Z3LTtPmfYzGsmVkBAfNCg8DXKvJXlRvEnVn3XZ5_D4uNHBwT6yfZf4GYQylq-
   hwITvN_c_OTCaPOP97bnRt6yGwWul40DBrR5xBGhphbh5qA&token_type=Bearer&id_token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpX
   AfiwYeEuQpH6Lm7bhLPP-hMCplWw9UG01pTcHNsujq07ybUNOTGBFjF8FgXuKU3GUkp1-
   MY1fWf8bPNf0OOWwKS7nb6ISqUN-gGWMaQrjrBs0JCLPwaHabqhdjGGc_GtJaUFY4W-B-mol-2_SoVhxU-
   eDSNlbWF21jNYlJUkPyOTXJIkj3hjPXNUyUspDA
   ```

3. If an `id_token` was included in the authorization request, the application validates the `id_token` returned.

   For more information, see the OpendID Connect Core 1.0 specifications.

4. If a `token` (access token) was included in the authorization request, the application can also optionally validate the access token returned.

   Use the PingOne SSO for SaaS Apps introspection endpoint returned by the **Discovery URL**, `https://sso.connect.pingidentity.com/sso/as/introspect.oauth2`, to validate the access token.

   For access tokens that are signed rather than encrypted, you can also use the JKWS URI returned by the **Discovery URL**, `https://sso.connect.pingidentity.com/sso/as/jwks`.

   > **Note**
   >
   > You can see your access token settings at **Applications > My Applications > OAuth Settings**. For more information, see Configuring your OAuth settings.

Using the global REST API client credentials

View and update the global **REST API Client ID** and **REST API Client Secret** values.

About this task

As a Service Provider (SP), to integrate your cloud application with PingOne SSO for SaaS Apps, you must assign a **REST API Client Secret** value. This value with the associated **REST API Client ID** are the credentials required for basic HTTP authentication between your client and PingOne SSO for SaaS Apps, which creates a secure connection over which your application can receive user attributes.

You can use the **REST API Client ID** and **REST API Client Secret** on the **Global Credentials** tab for all of your application connections and the Customer Connections API. For improved security, you should create separate credentials for each application.

Copyright © 2025 Ping Identity Corporation

For more information on creating additional credentials, see Creating or editing application-specific credentials and Creating or editing additional Connection API credentials.

> **Note**
>
> Include these credentials in the Basic authorization header as `REST_API_Client_ID:REST_API_Client_Secret` using Base64-encoding.
> When using cURL, the `--user` parameter is a wrapper for Basic authentication.

Steps

1. Go to **Account > Integration > Global Credentials**.

   > **Note**
   >
   > If you have not set a global **REST API Client Secret**, this tab is being deprecated in favor of the new application credential and connection credential tabs.
   > If you have set the global **REST API Client Secret**, you can disable it in favor of the more secure application and connection credentials.

2. To change the global credentials, click **Edit**:

   1. Enter a **REST API Client Secret** value.
   2. Select or clear the **Enabled** checkbox.

   When disabled, these credentials are no longer valid for the PingOne SSO for SaaS Apps Customer Connection API or Token Exchange API.

   1. Click **Save**.

      > **Important**
      >
      > Your **REST API Client ID** value is assigned when you activate your PingOne SSO for SaaS Apps account. This value cannot be changed.

Result

Any of your clients that use the PingOne SSO for SaaS Apps Customer Connection API will use these credentials.

Next steps

Next, Redirect users to PingOne SSO for SaaS Apps (SP-initiated SSO).

Creating or editing application-specific credentials

Create **Client ID** and **Client Secret** values for your applications.

About this task

> **Note**
>
> The application credentials feature is currently in limited release. To request access to this feature, open a support ticket.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to **Account > Integration > Application Credentials**.
2. To add a new set of credentials, click **Add Secret**.

> **Note**
>
> An application can be associated with multiple credentials. You can create a maximum of 30 application credentials.

3. **Optional:** In the **Short Description** field, enter a description for the application connection.
4. In the **Application** list, select the application for which you want to create credentials.
5. Click **Done**.

   Result:

   The new application credentials are displayed.
6. To edit existing credentials, expand the credentials and click the **Pencil** icon.

   Editing an existing credential allows you to change the **Description**.

> **Important**
>
> The **Application SaaSID**, **Client ID**, and **Client Secret** values cannot be changed.
> If you need a new **Client Secret**, you must create a new credential.

Creating or editing additional Connection API credentials

Create **Client ID** and **Client Secret** values for specific customer connections.

About this task

> **Note**
>
> The connection API credentials feature is currently in limited release. To request access to this feature, open a support ticket.

Steps

1. Go to **Account > Integration > Connection API Credentials**.
2. To add a new set of credentials, click **Add Secret**.

> **Note**
>
> You can create a maximum of three connection client credentials.

3. **Optional:** In the **Short Description** field, enter a description for the application connection.
4. Click **Next**.

Copyright © 2025 Ping Identity Corporation

5. **Optional:** In the **Client Secret** box, enter a client secret to replace the automatically-generated secret value.
6. Click **Done**.

   Result:

   The new application credentials are displayed.
7. To edit existing credentials, expand the credentials and click the **Pencil** icon.

   Editing an existed credential allows you to change the **Short Description** and **Client Secret**. The **Client ID** value cannot be changed.

Result

Any of your clients that will use the PingOne SSO for SaaS Apps Customer Connection API will use these credentials

Next steps

Next, Redirect users to PingOne SSO for SaaS Apps (SP-initiated SSO).

Redirect users to PingOne SSO for SaaS Apps (SP-initiated SSO)

Redirect users from your application to PingOne SSO for SaaS Apps.

About this task

You will redirect your users to PingOne SSO for SaaS Apps using the PingOne SSO for SaaS Apps URL format and attributes.

Steps

1. Format the PingOne SSO for SaaS Apps URL.

   The HTTP redirect has to go to this PingOne URL: `https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=<parmname>&idpid=<idpid>&appurl=<url>&errorurl=<errorUrl>`
2. Assign the query parameters.

   The following parameters are supported:

   saasid

   Identifies the application your user wants to access. You will find a listing of your applications and the associated SaaS ID (in parentheses below the application name) on the My Applications tab.

   idpid

   Identifies the identity repository for user authentication. This ID must be unique. The `idpid` value is used during HTTP redirect and token exchange. We recommended that you use a domain name here, if possible. **Note**: IdP IDs containing the forward-slash character (/) aren't allowed.For methods you can use to discover the `idpid` for a particular IdP, see Finding the `idpId` value.

   appurl

Copyright © 2025 Ping Identity Corporation

A URL in your domain to which the user is redirected after authenticating. Use this to override the Default Application URL value set on the Create connections page. Unlike a Default Application URL value, for `appurl` you cannot use a non-SSL URL for a test or development environment. Instead, you can use only SSL. If you specify a value here, you must have a matching value for the `Hostname or Domainname` entry on the Create connections page.

errorurl

An error-handling URL for your domain to redirect to in case of an error. This is used to override the `Error URL` value set on the Create connections page.

forceauthn

If true, ensures the IdP forces the user to re-authenticate, even if the user possess a valid SSO session.

For multiplexed SAML applications, multiple IdPs use a single connection to an application. In this case, PingOne needs to determine which IdP to use to authenticate a user. If we cannot determine this from the `idpid` parameter, we prompt the user for their email address and look up the IdP based on the email domain. However, when you're doing SP-initiated SSO from a PingFederate SP server, you can specify the IdP using the SP Services query parameter `AuthenticatingIdpId`. Learn more in the `AuthenticatingIdpId` entry in SP services.

Example:

Here's an example of a redirect to PingOne SSO for SaaS Apps: `https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=mysaas.com&idpid=exampleIdp.com`

> **Note**
>
> This URL is different for every IdP.

3. Write the supporting code to implement the HTTP redirect. You can use these samples as a basis:

   Choose from:

   - Java
   - C#
   - PHP
   - Ruby
   - Python
   - Perl

4. Next, you will need to process the PingOne token exchange.

Copyright © 2025 Ping Identity Corporation

Java Redirect Sample

```
package com.example.servlet;

import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

import java.io.IOException;
import java.net.URLEncoder;

/
 * The saasid value is the GUID associated with the application. This is displayed in parentheses below the
 * application name on the My Applications page.
 * You will need to replace the saasid value in "${saasId}" in the sample below with the GUID for your
application.
 * For example: final String saasId = URLEncoder.encode("18a6ada7-8f37-4d77-86f4-173046796193", "UTF-8");
 */

public class SaasExampleRedirectServlet
    extends HttpServlet
{
    @Override
    protected void doGet(HttpServletRequest req, HttpServletResponse resp)
        throws ServletException, IOException
    {

        final String saasId = URLEncoder.encode("${saasId}", "UTF-8");
        String idpId = URLEncoder.encode(getIdpIdFromRequest(req), "UTF-8");
        String location = String.format("https://sso.connect.pingidentity.com/sso/sp/initsso?
saasid=%s&idpid=%s",
                                        saasId,
                                        idpId);
        resp.sendRedirect(location);
    }

    /
     * Implement me!
     */
    public String getIdpIdFromRequest(HttpServletRequest req)
    {
        return "testidp.admin.pingidentity.com";
    }
}
```


Copyright © 2025 Ping Identity Corporation

.NET Redirect Sample

```
<%@ Page Language="C#" %>
<script runat="server">

  protected String GetIdpId()
  {
      //Implement me!
      return "testidp.admin.pingidentity.com";
  }

/**
 * The saasid value is the GUID associated with the application. This is displayed in parentheses below the
 * application name on the My Applications page.
 * You will need to replace the saasid value in "${saasId}" in the sample below with the GUID for your
application.
 * For example: String saasId = "18a6ada7-8f37-4d77-86f4-173046796193";
 */

  protected override void OnLoad(EventArgs e)
  {
      String saasId = "${saasId}";
      String idpId = GetIdpId();
      String baseUrl = "${tokenServiceBaseUrl}/sso/sp/initsso";
      String initSsoUrl = String.Format("{0}?saasid={1}&idpid={2}", baseUrl,
                                        saasId, idpId);
      Response.Redirect(initSsoUrl);
      base.OnLoad(e);
  }
</script>
```

Copyright © 2025 Ping Identity Corporation

PHP Redirect Sample

```
<?php

/
 * The saasid value is the GUID associated with the application. This is displayed in parentheses below the
 * application name on the My Applications page.
 * You will need to replace the saasid value in "${saasId}" in the sample below with the GUID for your
application.
 * For example: define("SAASID","18a6ada7-8f37-4d77-86f4-173046796193");
 */
define("SAASID","${saasId}");

/
 * Look up idpId for SSO - implement me!
 */
function getIdpId()
{
    return "testidp.admin.pingidentity.com";
}

$idpId = urlencode(getIdpId());
$saasId = urlencode(SAASID);

header("Location: https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=$saasId&idpid=$idpId");

?>
```


Copyright © 2025 Ping Identity Corporation

Ruby Redirect Sample

```
#Example rails controller

class SampleIntegrationController < ApplicationController

  def redirect
    @initSsoUrl = getInitSsoUrl()
    redirect_to @initSsoUrl
  end

  #
  # Implement me! This logic would not ordinarily be in your
  # controller, it is included for convenience sake
  #
  # The saasid value is the GUID associated with the application. This is displayed in parentheses below
  # the application name on the My Applications page.
  # You will need to replace the saasid value in "${saasId}" in the sample below with the GUID for your
application.
  # For example: @saasid = "18a6ada7-8f37-4d77-86f4-173046796193";
  #
  def getInitSsoUrl
    @saasId = "${saasId}"
    @idpId = "testidp.admin.pingidentity.com"
    @baseUrl = "${tokenServiceBaseUrl}"
    return "%{baseUrl}/sso/sp/initsso?saasid=%{saasId}&idpid=%{idpId}"  % { :baseUrl => @baseUrl, :saasId
=> @saasId, :idpId => @idpId }
  end

end
```

Copyright © 2025 Ping Identity Corporation

Python Redirect Sample

```
from django.http import HttpResponseRedirect

# This example uses the django web framework, but you can adapt it for your
# own framework if needed. Simply take the ssoUrl set in startSso() and
# send an HTTP 302 response to that location.

# The saasid value is the GUID associated with the application. This is displayed in parentheses below
# the application name on the My Applications page.
# You will need to replace the saasid value in "${saasId}" in the sample below with the GUID for your
application.
# For example: saasid = "18a6ada7-8f37-4d77-86f4-173046796193";
#
def startSso(request):
    idpid = getIdpId()
    saasid = "${saasId}"
    ssoUrl = "${tokenServiceBaseUrl}/sso/sp/initsso?saasid={0}&idpid={1}".format(saasid, idpid)
    return HttpResponseRedirect(ssoUrl)

# Implement me!
def getIdpId():
    return "testidp.admin.pingidentity.com"
```


Copyright © 2025 Ping Identity Corporation

Perl Redirect Sample

```
#!/usr/bin/perl -T

#
# Perl CGI example
#

use 5.010;
use strict;
use warnings;

#
# Replace this with the Idp you want to redirect to for SSO
#
my $idp_id = "testidp.admin.pingidentity.com";

my $base_url = "${tokenServiceBaseUrl}";

#
# The saasid value is the GUID associated with the application. This is displayed in parentheses below the
# application name on the My Applications page.
# You will need to replace the saasid value in "${saasId}" in the sample below with the GUID for your
application.
# For example: my $saas_id = "18a6ada7-8f37-4d77-86f4-173046796193";
#
my $saas_id = "${saasId}";
my $init_sso_url = "$base_url/sso/sp/initsso?saasid=$saas_id&idpid=$idp_id";

print "Status: 302 Moved\\n";
print "Location: ".$init_sso_url."\\n\\n";
```

Process the PingOne SSO for SaaS Apps token exchange

To process the token exchange, you will get the user's security token and make a REST call to PingOne SSO for SaaS Apps to initiate the token exchange.

About this task

It is important that you always get and exchange the user token, even if the user already has an active session. This ensures that the proper token exchange occurs. A token will be valid for five minutes or until it is exchanged. The token exchange is a one-time only REST call. After the exchange, the token expires and any subsequent calls using this token return HTTP 404.

> **Note**
>
> Ping Identity periodically deprecates obsolete TLS protocols and cipher suites. To stay compatible with these changes, you should ensure that your platform stays within its support life cycle. For example, a Java application should use a Java version that is currently supported by the Java vendor.

Steps

1. Get the user's token.

Copyright © 2025 Ping Identity Corporation

After PingOne SSO for SaaS Apps authenticate the user, they will return to one of these URLs:

- For SP-initiated SSO, the `appurl` value specified during the HTTP redirect.
- For IdP-initiated or SP-initiated SSO, the `Default Application URL` value you assigned on the Create connections page (for SP-initiated SSO the `appurl` value takes precedence, if specified).

  The user's token is passed as a `tokenid` POST parameter in the HTTP request.

  > **Note**
  >
  > POST is the default parameter type, but you can change the token to a query parameter, depending on your binding configuration.

  Example:

  For example: `https://www.mysaas.com/testapp?tokenid=158affc71d6bc65fe2a92ffac7760dce&agentid=0055f3da`

2. Make a REST call using the PingOne SSO for SaaS Apps REST API.

   The REST call identifies the token and specifies the return format for the user attributes.

   Example:

   This will be an HTTP GET call structured like this: `https://sso.connect.pingidentity.com/sso/TXS/2.0/<formatNumber>/<tokenid>`

   Accepted `formatNumber` parameters are indicated by:

   - **1** (JSON format)
   - **2** (Properties format)

3. Process the user attributes returned. PingOne SSO for SaaS Apps will return the following attributes, formatted according to your choice (JSON or Properties):

   pingone.subject

   The user name of the authenticated user. This is the subject for the target resource of the SSO transaction. It is important that you validate this. The user identified by pingone.subject must belong to the organization identified by pingone.idp.id.

   This value can be the same as the `pingone.subject.from.idp` value. However, it will be a different value if an attribute mapping transformation or a different attribute is used for the target resource.

   pingone.subject.from.idp

   The value used to authenticate against the IdP. For SAML transactions, this is the value in the `Subject` attribute of the assertion returned from the IdP.

   pingone.saas.id

   The cloud application to which the token is issued. This will be your SaaS ID.

Copyright © 2025 Ping Identity Corporation

> **Tip**
>
> Make sure your application's SaaS ID value matches the `pingone.saas.id` value. This prevents tokens issued for other applications from accessing your application.

pingone.idp.id, pingone.idpid

The id of the PingOne SSO for SaaS Apps customer connection associated with the currently authenticating user.

- If your application is using the REST API, this value is returned in JSON/XML, and has the format "pingone.idp.id" (note the two periods).
- If your application is using SAML, this value is always returned in the attribute statement as "pingone.idpid" (note the single period). This value is always returned by PingOne, so you do not need to configure an attribute mapping.

> **Tip**
>
> Identifying users with a combination of the `pingone.idp.id` and `pingone.subject` parameters prevents other identity providers (IdP) from using identifiers that resemble credentials from your intended IdP.

pingone.authn.context

The authentication context for which the user is authenticated by the identity bridge.

4. Write the supporting code to implement the token exchange. You can use these samples as a basis:

   Choose from:

   - Java
   - C#
   - PHP
   - Ruby
   - Python
   - Perl

   As a best practice, always have your client do an HTTP redirect after exchanging the token.

5. Next, you will need to Testing your application using the built-in IdP.

Copyright © 2025 Ping Identity Corporation

Java Token Exchange Sample

Copyright © 2025 Ping Identity Corporation

```
/
 * Requires commons codec library for Base-64 encoding the HTTP
 * basic authentication header:
 * http://commons.apache.org/codec/
 *
 * Alternatively, you can use the javax.mail library:
 * javax.mail.internet.MimeUtility;
 /
package com.example;

import java.io.IOException;
import java.io.InputStream;
import java.net.HttpURLConnection;
import java.net.URL;
import java.util.Properties;

import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

import org.apache.commons.codec.binary.Base64;

 /
 * The restAuthUsername value is the REST API Client ID (a GUID) automatically assigned to your account in
the PingOne admin portal
 * on the Account > Integration page.
 * You will need to replace the restAuthUsername value in "${restAuthUsername}" in the sample below with
your REST API Client ID.
 * For example: private static final String REST_USERNAME = "5f6ce45e-1a00-488e-8519-7c9946cb6379";
 *
 * The restApiKey value is the REST API Client Secret (the password/secret associated with your REST API
Client ID). You will need
 * to uncomment the private static final String REST_API_KEY statement and replace the empty string in the
sample below with
 * your REST API Client Secret.
 * For example:  private static final String REST_API_KEY = "mySecretApiPassword";
 */

public class SaasTokenExchangeExampleServlet
    extends HttpServlet
{
    private static final String REST_USERNAME = "${restAuthUsername}";

    // Specified at http://admin.pingidentity.com
    //private static final String REST_API_KEY = "";

    @Override
    protected void doGet(HttpServletRequest req, HttpServletResponse resp)
        throws ServletException, IOException
    {
        String token = req.getParameter("tokenid");
        String agentId = req.getParameter("agentid");
        String tokenResolutionUrl = String.format("https://sso.connect.pingidentity.com/sso/TXS/2.0/2/%s",
```

Copyright © 2025 Ping Identity Corporation

```
token);
        URL url = new URL(tokenResolutionUrl);
        HttpURLConnection urlConnection = (HttpURLConnection)url.openConnection();
        String authValue = REST_USERNAME + ":" +  REST_API_KEY;
        String basicAuthHeader = "Basic " + new String(Base64.encodeBase64((authValue).getBytes()));
        urlConnection.setRequestProperty("Authorization", basicAuthHeader);
        String agentidCookie = "agentid=" + agentId;
        urlConnection.setRequestProperty("Cookie", agentidCookie);
        InputStream is = urlConnection.getInputStream();
        Properties properties = new Properties();
        properties.load(is);
        String username = properties.getProperty("pingone.subject");
        String idpId = properties.getProperty("pingone.idp.id");
        createUserSession(resp, username, idpId);
    }

    /*
     * Implement me! Must validate that subject belongs to this idpId
     * @param resp - The response to create the user session with
     * @param user - The userid of the user doing SSO authentication into your application
     * @param idpid - The idpid of the user's organization where they have authenticated
     */
    private void createUserSession(HttpServletResponse resp, String user, String idpid) throws IOException
    {
        resp.setContentType("text/html");
        user = user.replace("<", "&lt;");
        user = user.replace(">", "&gt;");
        resp.getOutputStream().println("<p>Welcome, " + user + "</p>");
    }
}
```


Copyright © 2025 Ping Identity Corporation

.NET Token Exchange Sample

Copyright © 2025 Ping Identity Corporation

```
using System;
using System.Data;
using System.IO;
using System.Text;
using System.Net;
using System.Configuration;
using System.Collections.Generic;

public partial class ssoLogin : System.Web.UI.Page
{

    private static void SetBasicAuthHeader(HttpWebRequest req, String userName,
        String userPassword)
    {
        string authInfo = userName + ":" + userPassword;
        authInfo = Convert.ToBase64String(Encoding.Default.GetBytes(authInfo));
        req.Headers["Authorization"] = "Basic " + authInfo;
    }

    private static void SetAgentIdCookie(HttpWebRequest req, String agentid)
    {
        if (agentid != null)
        {
            req.Headers["Cookie"] = "agentid=" + agentid;
        }
    }

    private static string GetTokenServiceUrl(string pingConnectToken)
    {
        return "${tokenServiceBaseUrl}/sso/TXS/2.0/2/"+ pingConnectToken;
    }

 /**
 * The restApiKey value is the REST API Client Secret (the password/secret associated with your REST API
Client ID). You will need
 * to uncomment the String restApiKey statement and replace the empty string in the sample below with your
REST API Client Secret.
 * For example:  String restApiKey = "mySecretApiPassword";
 *
 * The restAuthUsername value is the REST API Client ID (a GUID) automatically assigned to your account in
the PingOne admin portal
 * on the Account > Integration page.
 * You will need to replace the restAuthUsername value in "${restAuthUsername}" in the sample below with
your REST API Client ID.
 * For example: SetBasicAuthHeader(request, "5f6ce45e-1a00-488e-8519-7c9946cb6379", restApiKey);
 */

protected void Page_Load(object sender, EventArgs e)
    {
        String tokenId = Request.QueryString["tokenid"];
        String agentId = Request.QueryString["agentid"];

        HttpWebRequest request = WebRequest.Create(GetTokenServiceUrl(tokenId))
                            as HttpWebRequest;
```


Copyright © 2025 Ping Identity Corporation

```
        // Specify this value at http://admin.pingidentity.com
        //String restApiKey = "";
        SetBasicAuthHeader(request, "${restAuthUsername}", restApiKey);
        SetAgentIdCookie(request, agentId);
        request.Method = "GET";
        request.ContentType = "text/plain;charset=utf-8";
        HttpWebResponse response = (HttpWebResponse)request.GetResponse();
        StreamReader reader = new StreamReader(response.GetResponseStream());
        String content = reader.ReadToEnd();
        String [] lines = content.Split('\\n');
        Dictionary<string, string> properties = new Dictionary<string, string>();
        foreach (string line in lines )
        {
            if (line.Contains("="))
            {
                properties.Add(line.Split('=')[0], line.Split('=')[1]);
            }
        }
        String subject = properties["pingone.subject"];
        String idpId = properties["pingone.idp.id"];
        CreateUserSession(subject, idpId);
    }

    protected void CreateUserSession(string subject, string idpId)
    {
        // Implement Me! Must validate that subject belongs to this idpId
        Response.Write("<p>Welcome, " + subject + "</p>");
    }
}
```

Copyright © 2025 Ping Identity Corporation

PHP Token Exchange Sample

Copyright © 2025 Ping Identity Corporation

```
<?php

/
 * Requires libcurl to be installed. For more info, see:
 * http://us.php.net/manual/en/book.curl.php
 /

/
 * Create a new user session for this user, identified by "$username",
 * by the identity provider identified by "$idpId"
 *
 * Implement me!! Must validate that subject belongs to this idpId
 */

 /*
 * The restAuthUsername value is the REST API Client ID (a GUID) automatically assigned to your account in
the PingOne admin portal
 * on the Account > Integration page.
 * You will need to replace the restAuthUsername value in "${restAuthUsername}" in the sample below with
your REST API Client ID.
 * For example: $restAuthUsername = '5f6ce45e-1a00-488e-8519-7c9946cb6379';
 *
 * The restApiKey value is the REST API Client Secret (the password/secret associated with your REST API
Client ID). You will need
 * to uncomment the $restApiKey statement and replace 'Specify me at https://admin.pingidentity.com/' in
the sample below with
 * your REST API Client Secret.
 * For example:  $restApiKey = 'mySecretApiPassword';
 */

function createUserSession($username, $idpid)
{
   echo "<p>Welcome, ".strip_tags($username)."</p>";
}

$tokenid = $_GET['tokenid'];
$agentid = $_GET['agentid'];

$restAuthUsername = '${restAuthUsername}';
//$restApiKey = 'Specify me at https://admin.pingidentity.com/';

$sso_service = "https://sso.connect.pingidentity.com/sso/TXS/2.0/1/$tokenid";
$c = curl_init($sso_service);
curl_setopt($c, CURLOPT_RETURNTRANSFER, true);
curl_setopt($c, CURLOPT_HTTPAUTH, CURLAUTH_BASIC);
curl_setopt($c, CURLOPT_COOKIE, "agentid=$agentid;");
curl_setopt($c, CURLOPT_USERPWD, "$restAuthUsername:$restApiKey");
$response = curl_exec($c);
curl_close($c);
$responseData = json_decode($response, true);

createUserSession($responseData['pingone.subject'],
        $responseData['pingone.idp.id']);
?>
```

Copyright © 2025 Ping Identity Corporation

Ruby Token Exchange Sample

```
#Sample rails controller

class TestIntegrationController < ApplicationController

  #
  # The restApiKey value is the REST API Client Secret (the password/secret associated with your REST API
Client ID). You will need
  # to uncomment the @restApiKey statement and replace the empty string in the sample below with your REST
API Client Secret.
  # For example:  @restApiKey = "mySecretApiPassword"
  #
  # The restAuthUsername value is the REST API Client ID (a GUID) automatically assigned to your account in
the PingOne admin portal
  # on the Account > Integration page.
  # You will need to replace the restAuthUsername value in "${restAuthUsername}" in the sample below with
your REST API Client ID.
  # For example: @request.basic_auth "5f6ce45e-1a00-488e-8519-7c9946cb6379", restApiKey
  #
  def sso
    @tokenid = params[:tokenid]
    @url = URI.parse "${tokenServiceBaseUrl}/sso/TXS/2.0/1/%s" % @tokenid
    @http = Net::HTTP.new(@url.host, @url.port)
    @http.use_ssl = true
    @request = Net::HTTP::Get.new(@url.path)
    @restApiKey = ""
    @request.basic_auth "${restAuthUsername}", @restApiKey
    @response = @http.request(@request)
    @data = JSON.parse @response.body
    @subject = @data['pingone.subject']
    @idpid = @data['pingone.idp.id']
    # TODO: Verify that @subject belongs to @idpid, and
    # Create a user session
    respond_to do |format|
      format.html # sso.html.erb
    end
  end

end

# sso.html.erb

<p>Welcome, <%= @subject %> </p>
```


Copyright © 2025 Ping Identity Corporation

Python Token Exchange Sample

Copyright © 2025 Ping Identity Corporation

```
# This example uses Django 1.3, but can be converted for use in any
# web framework.
# Requires:
#     * Python 2.6.x or 2.7.x
#         * (If using Python 2.4.x or 2.5.x, replace json with simplejson)
#     * Python's socket module must be built with SSL support.
#         * For more info: http://www.python.org/doc//current/library/httplib.html
#

from django.http import HttpResponse
import httplib
import base64
import json # new in python 2.6 -- use simplejson if python < 2.6
import ssl
import socket
import os

# Download from http://curl.haxx.se/ca/cacert.pem, place in folder
CERT_FILE = os.path.join(os.path.dirname(file), 'cacert.pem')

# HTTPSConnection with SSL certificate validation
class ValidHTTPSConnection(httplib.HTTPSConnection):
    default_port = httplib.HTTPS_PORT

    def init(self, *args, * *kwargs):
        httplib.HTTPConnection.init(self, *args, * *kwargs)

    def connect(self):
        sock = socket.create_connection((self.host, self.port),
                                        self.timeout, self.source_address)
        if (self._tunnel_host):
            self.sock = sock
            self._tunnel()
        self.sock = ssl.wrap_socket(sock, ca_certs=CERT_FILE,
                                    cert_reqs=ssl.CERT_REQUIRED)

# Implement me!

def getIdpId():
    return "testidp.admin.pingidentity.com"

#
# The restApiKey value is the REST API Client Secret (the password/secret associated with your REST API
Client ID). You will need
# to uncomment the @restApiKey statement and replace the empty string in the sample below with your REST
API Client Secret.
# For example:  restApiKey = "mySecretApiPassword"
#
# The restAuthUsername value is the REST API Client ID (a GUID) automatically assigned to your account in
the PingOne admin portal
# on the Account > Integration page.
# You will need to replace the restAuthUsername value in "${restAuthUsername}" in the sample below with
your REST API Client ID.
# For example: credential = base64.b64encode("5f6ce45e-1a00-488e-8519-7c9946cb6379" + restApiKey)
```


Copyright © 2025 Ping Identity Corporation

```
#

def handleSso(request):
    tokenid = request.GET.getitem('tokenid')
    agentid = request.GET.getitem('agentid')

    restApiKey = ""
    credential = base64.b64encode("${restAuthUsername}:" + restApiKey)
    print(credential)
    headers = {
        "Accept": "application/json",
        "Authorization": "Basic " + credential,
        "Cookie": "agentid=" + agentid,
    }

    conn = ValidHTTPSConnection("sso.connect.pingidentity.com", 443)
    conn.request("GET", "/sso/TXS/2.0/1/" + tokenid, headers = headers)
    response = conn.getresponse()
    if (response.status != 200):
        raise Exception("Bad resonse: {0} {1} {2} {3}".format(response.status, response.reason,
response.read(), response.msg))
    attributes = json.loads(response.read())
    subject=attributes['pingone.subject']
    idpid=attributes['pingone.idp.id']
    #
    # Implement me! You will need to use subject and idpid to create a user
    # session on your application. In this example, we just write the subject
    # directly to the response stream.
    #
    return HttpResponse("Welcome, {0}!".format(subject))
```

Copyright © 2025 Ping Identity Corporation

Perl Token Exchange Sample

Copyright © 2025 Ping Identity Corporation

```
#!/usr/bin/perl -T

#
# Perl CGI example
#

use 5.010;

use strict;
use warnings;
use CGI;
use JSON;
use MIME::Base64;

#
# This sample requires installing REST::Client from
# cpan -- installing this will depend on your environment.
#
use REST::Client;

#
# The restApiKey value is the REST API Client Secret (the password/secret associated with your REST API
Client ID). You will need
# to uncomment the @restApiKey statement and replace the empty string in the sample below with your REST
API Client Secret.
# For example:  my restApiKey = "mySecretApiPassword"
#
# The restAuthUsername value is the REST API Client ID (a GUID) automatically assigned to your account in
the PingOne admin portal
# on the Account > Integration page.
# You will need to replace the restAuthUsername value in "${restAuthUsername}" in the sample below with
your REST API Client ID.
# For example: my restAuthUsername = "5f6ce45e-1a00-488e-8519-7c9946cb6379";
#

my $q = CGI->new();
my $client = REST::Client->new();
my $token = $q->param('tokenid');
my $agent = $q->param('agentid');
my $token_endpoint = "${tokenServiceBaseUrl}/sso/TXS/2.0/1/".$token;
my restAuthUsername = "${restAuthUsername}";
my restApiKey = "";

my $auth_header = "Basic ".encode_base64(sprintf("%s:%s", $rest_username,
                                                 $rest_api_key));
$client->addHeader("Authorization", $auth_header);
$client->addHeader("Cookie", "agentid=".$agent);
$client->GET($token_endpoint);
my $response = from_json($client->responseContent());
my $subject = $response->{'pingone.subject'};
```

Copyright © 2025 Ping Identity Corporation

```
my $idp_id = $response->{'pingone.idp.id'};

#
# Create a user session for $subject authenticated at $idp_id
#
```

Integrate an application hosted on multiple URLs

About this task

If your application is hosted on multiple URLs, you can send users to any one of these URLs after they authenticate.

Use the `appurl` parameter to redirect users to your application. The `appurl` parameter is a URL in your domain to which the user is redirected after authenticating. Use this to override the Default Application URL value set on the Create connections page. Unlike a Default Application URL value, for `appurl` you cannot use a non-SSL URL for a test or development environment. Instead, you can use only SSL. If you specify a value here, you must have a matching value for the `Hostname or Domainname` entry on the Create connections page.

You can use either of the following approaches to integrate an application hosted on multiple URLs:

Steps

- Do the PingOne token exchange processing for each URL. This is necessary if you cannot create a user session until you are at that URL. See Process the PingOne SSO for SaaS Apps token exchange for instructions.

    1. When you start SSO, each URL is then the value of the `appurl` parameter.

        Example:

        For example, if one of the URLs is `https://acme.example.com/sso`, starting SSO might look like this (URL-encoded):

        ```
        https://sso.connect.pingidentity.com/sso/sp/initsso?
        saasid=saasId&idpid=idpId&appurl=https%3A%2F%2Facme.example.com%2Fsso
        ```

- Do the PingOne token exchange processing at a single place in your application, and then redirect to a different URL after creating the user session. This is only possible if you can create a valid user session outside of that URL (such as, when there's no subdomain restriction).

    1. Create a location to process the token exchange. For example, assuming all of the URLs are in an **`example.com`** subdomain (such as, example.com/acme/home), you might implement token exchange processing at `https://example.com/finish-sso`.

    2. Use the `redirect_to` parameter to form a URL-encoded value as the redirect.

        Example:

        For example, the redirect might look like this:

        ```
        https://example.com/finish-sso?redirect_to=https%3A%2F%2Facme.example.com%2Fsso
        ```


Copyright © 2025 Ping Identity Corporation

3. To start SSO, use this redirect as the value of the `appurl` parameter.

> **Note**
>
> Use "%3F" before the redirect_to parameter.

Example:

For example:

```
   https://sso.connect.pingidentity.com/sso/sp/initsso?
saasid=saasId&idpid=idpId&appurl=https%3A%2F%2Fexample.com%2Ffinish-
sso%3Fredirect_to%3Dhttps%253A%252F%252Facme.example.com%252Fsso
```

Test your application

Testing your application using the built-in IdP

PingOne SSO for SaaS Apps automatically creates connections to the internal Test identity provider (IdP) which you can use to test your multiplexed SAML applications and applications enabled through PingOne SSO for SaaS Apps.

Before you begin

Your application must be enabled before you can test the integration.

About this task

Use the PingOne SSO for SaaS Apps Test IdP to test your application integration. For security reasons, connections to the PingOne SSO for SaaS Apps Test IdP are disabled by default and are enabled only when you select to test your application.

Steps

1. In the PingOne SSO for SaaS Apps administrator portal, go to **Applications > My Applications**.
2. Click the **Test** button associated with your application.

   Result:

   The **Test Integration** pop-up window opens.
3. Click the **Start Single Sign-On** link.

   Result:

   The sign-on page for the PingOne SSO for SaaS Apps Test IdP opens.
4. Enter the **User Id** and **Password** for a test user and click **Login**.

   Use the following automatically-generated test user names:

   - `test@testidp.connect.pingidentity.com`
   - `testuser1@testidp.connect.pingidentity.com`

Copyright © 2025 Ping Identity Corporation

- `testuser2@testidp.connect.pingidentity.com`
- `testuser3@testidp.connect.pingidentity.com`
- `testuser4@testidp.connect.pingidentity.com`
- `testuser5@testidp.connect.pingidentity.com`
- `testuser6@testidp.connect.pingidentity.com`
- `testuser7@testidp.connect.pingidentity.com`

The password for each of these user IDs is `test`.

> **Note**
>
> For more information about enabling testing applications enabled through PingOne SSO for SaaS Apps see Process the PingOne SSO for SaaS Apps token exchange.

> **Tip**
>
> If your application is SAML, you can use a SAML tracer browser add-on or application to view SAML exchanges between your application and PingOne SSO for SaaS Apps.

5. When you're finished testing, close the **Test Integration** pop-up window to disable the Test IdP connection.

Testing your application using PingOne for Enterprise

Create test users in an invited or managed PingOne for Enterprise account.

Your PingOne SSO for SaaS Apps account comes with a built-in identity provider (IdP) populated with test users that you can use to test your applications.

You can also create test users in a PingOne for Enterprise account with a connection to your application, populated with test users that you control. The method for creating test users depends on whether you have a PingOne SSO for SaaS Apps with Managed Accounts license.

Copyright © 2025 Ping Identity Corporation

Without Managed Accounts

Creating test users with PingOne SSO for SaaS Apps

Steps

1. Create an invited connection for your application.

   > **Note**
   >
   > Send the invite email to an email address that you control. It must be unique and cannot be the email address you use to manage your PingOne SSO for SaaS Apps account.

   For more information, see Creating an invited SSO connection.

2. When you receive the invite, set up a new PingOne for Enterprise account.

3. Choose the PingOne for Enterprise Directory.

   For more information, see Select PingOne for Enterprise Directory.

4. Add some test users.

   For more information, see Add directory users.

5. On the invited PingOne for Enterprise account **Applications** tab, finish configuring the application.

   For more information, see Managing applications.

6. To test single sign-on (SSO), redirect to PingOne for Enterprise using the redirect URL, as documented in step 1 of Redirect users to PingOne SSO for SaaS Apps (SP-initiated SSO).

Copyright © 2025 Ping Identity Corporation

With Managed Accounts

Creating test users with PingOne SSO for SaaS Apps with Managed Accounts
Steps

1. Create a managed PingOne for Enterprise account.

   For more information, see Creating and administering a partner account.

2. In the managed account, select the PingOne for Enterprise Directory as the identity provider (IdP).

   For more information, see Select PingOne for Enterprise Directory.

3. Add some test users.

   For more information, see Add directory users.

4. Go to **Applications > Private App Catalog** and add the application that you're testing.

   > **Note**
   >
   > Be sure to note the **idpid** value on the **Summary** tab of the application configuration wizard.

For more information, see Managing applications.

1. To test single sign-on (SSO), redirect to PingOne for Enterprise using the `idpid`, as documented in step 3 of Redirect users to PingOne SSO for SaaS Apps (SP-initiated SSO).

Connect customers to your application

PingOne SSO for SaaS Apps has several ways to connect customers to your application.

To connect a customer to your application, you first choose a connection method. When the customer has accepted the connection, you edit the connection to assign additional settings and verify or reconfigure the existing settings.

Choose the appropriate connection method for your application:

SSO Self-Service widget

Adding the single sign-on (SSO) Self-Service widget is the easiest way to add customer connections to your Application Catalog app. For more information, see Application Catalog app connection.

Email Invitation

You can send you customer an invitation email containing a link to PingOne for Enterprise to provide their SSO information. This is the best option if you can't use the Self-Service widget. For more information, see Creating an invited SSO connection.

Copyright © 2025 Ping Identity Corporation

Customer Connection REST API

If you want your customers to provide their information directly to your application without ever visiting PingOne for Enterprise, you can add connections using the Customer Connection REST API. You should only use the Customer Connection API in cases where sending the customer's administrative user to the PingOne for Enterprise portal isn't a viable option. For more information, see Application Catalog app connection.

Manual SAML connection

You can add customer connections manually. You should only choose this method in circumstances, such as:

- Your customer prefers that you manage their connection to your application.
- A direct SAML connection to your application is all that your customer needs.
- You anticipate connecting to a limited number of customers.
- Your customer is not using PingOne for Enterprise.

See Direct SAML connection for more information.

Configure a private application for a managed partner account

If you have a PingOne SSO for SaaS Apps with Managed Accounts license, you can create a private connection for your partner accounts. After entering a partner account and adding an application, you'll configure the application connection from within the partner's account, rather than from your PingOne SSO for SaaS Apps account. For more information, see Connect an application for a partner account.

PingOne Invited SSO

Invited SSO accounts are PingOne for Enterprise accounts designed specifically for your customers who already have an identity provider (IdP) set up and want to handle the application connection themselves. They can then use their Invited SSO account to add the connection to your application and configure an identity bridge to their IdP. For more information, see Invited SSO.

Partner account applications

When you create a partner account, an **Applications > Private App Catalog** page is added in the partner's PingOne for Enterprise admin portal. This page exists only in managed partner accounts. When you add an application from your PingOne SSO for SaaS Apps account, then enter the partner account, you will find the application you have added displayed on this page.

For partner accounts, you will configure the application connections from the **Private App Catalog** page in the partner's PingOne for Enterprise account.

> **Note**
>
> When you add and configure applications for a partner account, the application connections are displayed only in the PingOne for Enterprise admin portal for the partner account, and are not displayed on the **Customer Connections** page in your PingOne SSO for SaaS Apps account.

Connect an application for a partner account

About this task

Copyright © 2025 Ping Identity Corporation

For partner accounts, you will need to set up the connection to an application that you have added from your PingOne SSO for SaaS Apps account by entering the partner PingOne for Enterprise account and selecting the application from the list on the the Private App Catalog page.

Steps

In your PingOne SSO for SaaS Apps account

1. On the **Managed Accounts** page, expand the details for the partner account for which you want to connect an application and click **Enter Account** to administer the partner account.

In the partner PingOne for Enterprise account

1. Go to **Applications > Private App Catalog**.
2. **Optional:** In the Search field, search for your app by typing the name, entity ID, or description of the application you want to add.

   The application listing will display the type of the application.
3. When you find the application you want to configure, click the right-arrow icon. The application description is displayed.
4. Click **Setup** to begin.
5. **Optional:** If the application connection is multiplexed or uses IdP-initiated SSO (the PingOne SSO for SaaS Apps Customer Connection API), the option to enter the URL to use as the **Target Resource** is displayed.

   This is the URL to which the user is directed after IdP-initiated SSO.
6. **Optional:** Select whether or not to enable **Force Re-authentication**. Click **Continue to Next Step**.

   When enabled, to establish a connection to the application, users having a current, active SSO session are re-authenticated by the identity provider.
7. To add a new attribute, click **Add New Attribute**.

   In most cases, the default attribute mappings are sufficient. These mappings assign your identity repository attributes to the attributes provided by the Service Provider for the application.

   For each application attribute, you can:

   1. Enter a value in the **Application Attribute** field
   2. Click the **Required** checkbox to designate an attribute or attributes as required by the application.
   3. In the **Identity Bridge Attribute or Literal Value** field, choose between:

      - Select an attribute from the drop down list.
      - Select **As Literal** and enter a literal value to assign.

        1. Click **Advanced** and enter Advanced Attribute Mapping mode.

           For more information, see Creating advanced attribute mappings
        2. Select the **Provisioning** checkbox to make this a provisioning attribute rather than an SSO attribute.

Copyright © 2025 Ping Identity Corporation

Custom provisioning attributes are currently only available for Aquera and Salesforce applications.

8. When you've finished modifying or adding any additional attributes, click **Continue to Next Step**.
9. Make the new application available to your partner's users.

   See Authorize group access to applications for instructions.

Creating an invited SSO connection

Invited single sign-on (SSO) connects your customer to your application using an email invitation.

About this task

Invited SSO is for your customers who already have an identity provider (IdP) set up. You send them an email invitation containing the connection information for your application. Included in your email is a link for the customer to either register a new PingOne for Enterprise Invited SSO account or sign on to their existing account. They then add the connection to your application.

Steps

1. In the PingOne SSO for SaaS Apps admin portal, go to **Customer Connections** > **Adding Connections** > **Customer Email Invitation**.
2. Select the checkboxes of the applications you want to invite the customer to connect with.
3. In the **Customer Email** field, enter the administrator email address of the IdP to connect your application to.

   The email message is specific to your application and the PingOne SSO for SaaS Apps connection established.
4. In the **Customer ID** field, enter a value for the customer's `idpid`.

   The `idpid` value is a unique identifier for the IdP. You can reference the `idpid` later by going to **Customer Connections** and clicking on **Details** for that customer connection.
5. Click **Create Connection**.

   Result:

   PingOne SSO for SaaS Apps creates the SSO connection using the email address and `idpid` you provided.
6. Send the invitation email:

   Choose from:

   - Click **Send E-Mail** to have PingOne SSO for SaaS Apps send the email.
   - Copy the email text and customize it in your email platform before sending it yourself. Click **Close** to return to the **Customer Connections** list.

Result

When the customer receives the email and clicks the link in the message, they're directed to the PingOne SSO for SaaS Apps portal to either register a new SSO account or add the connection to your application to an existing account.

Copyright © 2025 Ping Identity Corporation

Application Catalog app connection

Use either of these ways to connect customers to your Application Catalog app:

The SSO Self-Service widget

You will need to paste some JavaScript and a minimal amount of code into a page or section of your application that's accessible only to your customer's administrative users. You then ask one of your customer's administrators to visit your page and run our widget. The administrator is redirected to a page on the PingOne portal where they enter their customer configuration information. This makes it easy for you to capture customer configurations without having to be concerned with customer-specific protocol settings.

Customer Connection API

To use the Customer Connection API, you will authenticate using your PingOne credentials. See Using the global REST API client credentials. Your application needs to include an administrator-only page or section for the customer. You also need to elicit the necessary SAML connection information from your customer.

Create a connection using the SSO self-service widget

About this task

To integrate the SSO Self-Service widget into your application you will need to add:

1. Client-side code in a new HTML page.
2. The SSO Self-Service widget's JavaScript in the new HTML page.
3. Server-side code to ensure the widget runs securely.

The SSO Self-Service widget displays a link to your application page similar to the following (by default):

> **Note**
>
> You can customize the appearance of this widget by choosing non-default CSS settings.

When your customer clicks the link, they will be securely redirected to the PingOne SaaS SSO portal where they will enter their configuration information.

Steps
Add the Client-Side Code

1. Create a new HTML page or section in your application. This is the location you will ask your customer's administrator to visit.
2. Add a blank tag with a unique `id` attribute value. For example:

Copyright © 2025 Ping Identity Corporation

```
<div id="pingWidget">Loading...</div>
```

Any tag contents will be replaced by the SSO Self-Service widget.

3. Get the SSO Self-Service widget from the PingOne site.
    1. Sign in to the PingOne admin portal and go to the SSO Self-Service page.
    2. Click the link to download the SSO Self-Service widget.
4. Open the downloaded widget JS file and copy and paste the JavaScript within the tags you added to your HTML page.
5. Edit the JavaScript for the widget to add the `pingOneParams` parameter values:

pingOneParams.ssoDivId

The element id of the HTML tag that contains the SSO Self-Service widget JavaScript.

pingOneParams.openToken

The OpenToken from your server code. See the following *Add the Server-Side Code* section for more information.

pingOneParams.saasId (Optional)

The `saasID` value for your application that you want to enable for SSO. This allows you to confine SSO to a specific application. If you do not specify a value here, all of your applications will be enabled for SSO. Refer to the SSO Self-Service page for the SaaS ID values for your applications.

pingOneParams.accountId

The Company ID for your account.

pingOneParams.useDefaultCss (Optional)

A boolean value indicating whether to include the default CSS for the SSO Self-Service widget (defaults to true). Set this to false if you want to use your own CSS (to customize the widget display, for example).

pingOneParams.useDefaultHtml (Optional)

A boolean value indicating whether to include the default HTML for the SSO Self-Service widget (defaults to true). Set this to false if you want to use your own HTML.

Add the Server-Side Code

1. Go to the SSO Self-Service page.
2. Select the appropriate language link to download sample server-side code for one of the available languages.
3. Using your downloaded sample as the basis, write the supporting code to implement the server-side functionality.

    Your server-side code constructs two name/value pairs (the `idpId` name/value pair and the `email` name/value pair) and uses the OpenToken library to generate an OpenToken. OpenToken is a secure, open standard for encrypting and sending name/value pairs.

Copyright © 2025 Ping Identity Corporation

The OpenToken standard requires that a subject attribute be passed. To comply with the standard, we pass the `idpId` parameter as subject. This is reflected in all of our sample code.

4. Follow the instructions in the readme file included in the download to generate an OpenToken for your specified `idpId` and `email` values.
5. In the client-side JavaScript for the SSO Self-Service widget on your HTML page, assign the generated token as the value of the `openToken` parameter.

Create a connection using the Customer Connection API

About this task

Create a page or section in your application for the customer's administrator. Then use the Customer Connection REST API to elicit the necessary SAML connection information (SAML attribute values) from the customer.

All PingOne resource requests require authentication. You need to include your REST API Client ID and REST API Client Secret credentials in the request, otherwise the resource returns a 401 (Unauthorized) status code. Currently, we support HTTP basic authentication, which includes encrypted credentials in the request header. See Using the global REST API client credentials for more information.

Steps

1. Create a page or section in your application that can be accessed only by the customer's administrator.
2. Use the Customer Connection API to:
    1. Get the SAML attributes containing the customer's information.
    2. Create a customer connection using the customer information retrieved and the customer's signing certificate.

    See the PingOne SSO for SaaS Apps Customer Connection API for more information.

Creating a manual SAML connection

After integrating your application with PingOne SSO for SaaS Apps, you can use your customer's SAML connection information to manually configure the connection to your application.

About this task

For direct connections, you manually configure and establish a SAML connection to your application for the customer. You must collect from the customer all necessary SAML information for the customer side of the connection using your own (out-of-band) methods.

> **Important**
>
> For manual connections, your IdP partner must send attributes exactly as your application requires. If you need to transform or remap your attributes in PingOne SSO for SaaS Apps before sending them to your application, use an invited connection or managed account.
> Don't use a manual connection if your customer is using PingOne for Enterprise. Use an invited connection instead.

Steps

1. Go to **Customer Connections > Adding Connections > Manual Connection**.

Copyright © 2025 Ping Identity Corporation

2. Select the checkboxes of the applications you want to make available to this customer connection.
3. Click **Yes** to make this a multiplexed connection, or **No** to make it non-multiplexed.

   For more information about connection multiplexing, see About multiplexing.
4. Enter the customer information for the **Customer Email** and **Customer ID**(`idpid`) fields.
5. For **Upload Metadata**:

   Choose from:

   - To upload your customer's connection metadata file, click **Choose File**.
   - To enter your customer's metadata URL, click **Or use URL**, and enter the metadata URL in the **URL of the file** field.

     The entries for **Entity ID** and **SSO Endpoint** are populated for you.

     +

     > **Note**
     >
     > If you don't upload the customer's connection metadata, you must enter the **Entity ID** and **SSO Endpoint** values.
6. For **Verification Certificate**, click **Choose File** to upload the customer's public certificate.

   PingOne SSO for SaaS Apps uses this certificate to sign SAML assertions.
7. **Optional:** In the **Single Logout Endpoint** field, enter the URL for the SAML single logout (SLO) endpoint.

   PingOne SSO for SaaS Apps sends SLO requests to this URL using the binding type you select for `Single Logout Binding Type` .

   The attributes for `Single Logout Endpoint` , `Single Logout Binding Type` , and `Verification Certificate` are interdependent. To support SLO, you will need to specify all of these attribute values, and optionally, `Single Logout Response Endpoint` . For more information, see PingOne for Enterprise and SLO.

   > **Note**
   >
   > If you choose not to support SLO for an application, the application is not notified when the user session ends.
8. **Optional:** In the **Single Logout Response Endpoint** field, enter the URL for the SAML SLO endpoint.

   > **Note**
   >
   > If you don't assign a value here, **Single Logout Endpoint** is also used as the response endpoint. Your application sends the SLO response to this URL.
9. **Optional:** Click either **POST** or **Redirect** for the SLO binding type.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If the IdP metadata you uploaded in Step 5 contains both Redirect and POST SSO bindings, PingOne SSO for SaaS Apps will use the Redirect binding to send AuthnRequests for this connection.
> If the metadata only contains a POST binding, PingOne SSO for SaaS Apps will use POST for this connection.
> If you configure the fields manually without importing metadata, PingOne SSO for SaaS Apps will use the Redirect binding.

10. Select the **Sign the AuthnRequest** checkbox to make PingOne SSO for SaaS Apps sign AuthnRequests to the customer.
11. **Optional:** Upload the signing certificate you will use to sign SLO requests. This can be the same certificate you use for SAML assertions.

    In the **Signing Algorithm** list, select the algorithm used to sign both SAML assertions and SLO requests.

If you are setting up a new application, the signing algorithm defaults to the recommended SHA-256.

If you have an existing application configuration, SHA-1 might be displayed as the default signing algorithm. We recommend you change it to SHA-256 at your convenience.

1. Download the files and data from the **PingOne Connection Information** section to supply to your customer.

   If this connection is not multiplexed, and enabled through PingOne SSO for SaaS Apps rather than SAML or OIDC, you can select **Use Custom Entity ID** to use the application's custom entity ID rather than the default `saasid`.

   For more information about configuring a custom entity ID, see Add or update other applications.
2. Click **Save settings**.

Edit an invited customer connection

Change the identity provider (IdP) discovery settings for existing invited customer connections.

About this task

Only certain settings are available for editing on invited connections. Managed connections have more settings that you can edit.

For information about editing an existing managed customer connection, see Edit a managed customer connection.

> **Note**
>
> The following steps are optional. You only need to change the settings that apply to your customer connection.

Steps

- To display the list of customer connections for your applications, click the **Customer Connections** tab.
- **Optional:** To display the customer connection filtering options, click **Narrow by**.
    1. To filter the list of customer connections, select or clear the **Enabled** or **Type** boxes.
- For the connection you want to edit, click the **down arrow** to display the drop-down list, and click **Edit**.
- To edit the contact email for this connection, enter a new email address in the **Contact Email** field.

Copyright © 2025 Ping Identity Corporation

- Enter the **Email Domain** to use for IdP discovery.

  PingOne uses the email domain you specify to discover the IdP and assign it to the customer account.

- Enable the **Set as default IdP** box to redirect users who enter an email address that cannot be matched to an IdP during service provider (SP)-initiated single sign-on (SSO).

  > **Note**
  >
  > The **Set as default IdP** setting is not displayed if you have already enabled this setting for the customer account.

  You can enable IdP discovery to associate each connection with an IdP. When you initiate an SSO request (SP-initiated SSO), there is no need to specify the identifier for the IdP. Instead, PingOne resolves the correct IdP by associating email domains with specific managed accounts and their IdP. Then, during a user's initial SSO, the user enters a matching email domain. PingOne prompts the user for their email domain only during their initial SSO.

  When a user initially attempts to SSO to the application, the user is prompted for their email address. If the domain of the email address matches one of the IdP discovery domains you assigned, PingOne redirects the user to the corresponding IdP for authentication. If the domains do not match and you have not enabled **Set as default IdP**, an error is displayed and the user is prompted again for their email address. When **Set as default IdP** is enabled, the user is redirected to the default IdP to authenticate.

- When you are finished making changes, click **Save changes**.

Edit a managed customer connection

Change the basic information, SAML details, and identity provider (IdP) discovery settings of your existing managed customer connections.

About this task

For information on editing existing invited customer connections, see Edit an invited customer connection.

Only certain settings are available for editing. These settings depend on whether your application is SAML-enabled, whether the application connection is manually configured, and whether or not the connection is multiplexed.

> **Note**
>
> The following steps are optional. You only need to change the settings that apply to your customer connection.

Steps

- To display the list of customer connections for your applications, click the **Customer Connections** tab.
- **Optional:** To display the customer connection filtering options, click **Narrow by**.
    1. To filter the list of customer connections, select or clear the **Enabled** or **Type** boxes.
- For the connection you want to edit, click the **down arrow** to display the drop-down list, and click **Edit**.
- To indicate whether this connection is multiplexed, click **Yes** or **No**.
- In the **Contact Email** field, enter the email address of the person assigned as the contact for this connection.

Copyright © 2025 Ping Identity Corporation

- In the **IdpId** field, enter the idpid.

  For more information, see Finding the `idpId` value.

- In the **Entity ID** field, enter a unique name for the identity bridge.
- Upload metadata.

  Choose from:

  - Click **Select File** to upload a local metadata file.
  - Click **Or use URL** to enter a metadata URL.

- In the **SSO Endpoint** field, enter an identity bridge endpoint URL to which PingOne will send AuthNRequests.
- To upload a verification certificate, click **Browse...**, and select a local signing certificate file to upload.

  Result:

  If you upload a verification certificate, the details for that certificate display in the **Certificate File Name**, **Certificate Subject DN**, and **Expiration Date** fields.

- In the **Single Logout Endpoint** field, enter the endpoint URL to redirect users to when they sign out of an application.
- In the **Single Logout Response Endpoint** field, enter a URL for applications to send logout responses to.
- For **Single Logout Binding Type**, click either **Redirect** or **Post** to determine how SAML uses HTTP to transport messages.
- To enable PingOne to sign outgoing connection requests, select the **Sign the AuthNRequest** box.
- From the **Signing Algorithm** list, select the algorithm for PingOne to use when signing outgoing connection requests.
- From the **Connection Data** section, you can download the **Signing Certificate**, **PingOne Metadata**, and **Encryption Certificate**. You can also copy and share the **ACS URL** with the customer's IdP.

  If this connection is not multiplexed, and enabled through PingOne rather than SAML or OIDC, you can select **Use Custom Entity ID** to use the application's custom entity ID rather than the default `saasid`.

  For more information about configuring a custom entity ID, see Add or update other applications.

- In the **IdP Discovery** section, enter the **Email Domain** to use for IdP discovery.

  PingOne uses the email domain you specify to discover the IdP and assign it to the customer account.

- Enable the **Set as default IdP** box to redirect users who enter an email address that cannot be matched to an IdP during service provider (SP)-initiated single sign-on (SSO).

> **Note**
>
> The **Set as default IdP** setting will not be displayed if you have already enabled this setting for the customer account.

You can enable IdP discovery to associate each connection with an IdP. When you initiate an SSO request (SP-initiated SSO), there is no need to specify the identifier for the IdP. Instead, PingOne resolves the correct IdP by associating email domains with specific managed accounts and their IdP. Then, during a user's initial SSO, the user enters a matching email domain. PingOne prompts the user for their email domain only during their initial SSO.

Copyright © 2025 Ping Identity Corporation

When a user initially attempts to SSO to the application, the user is prompted for their email address. If the domain of the email address matches one of the IdP discovery domains you assigned, PingOne redirects the user to the corresponding IdP for authentication. If the domains do not match and you have not enabled **Set as default IdP**, an error is displayed and the user is prompted again for their email address. When **Set as default IdP** is enabled, the user is redirected to the default IdP to authenticate.

- When you are finished making changes, click **Save changes**.

Adding a new connection to an existing customer

Connect an existing customer to a new application by creating a new application connection using the same customer details.

Steps

1. Create a new connection:

   Choose from:

   - Add the SSO self-service widget to your new application.
   - Use the customer connection API to add a new connection to your new application.
   - Send a new SSO connection invitation.
   - Create a new manual SSO connection.

2. When choosing which applications to add to the connection, select only the new applications you want to add.

   > **Important**
   >
   > If you select applications that are part of an existing customer connection, PingOne SSO for SaaS Apps attempts to create a duplicate application connection, which results in an error.

3. When entering the **Customer Email** and **Customer ID (idpid)**, use the same values as the existing connection for this customer.

   > **Tip**
   >
   > To find the email and `idpid` values for an existing customer connection, go to **Customer Connections** and click **Details** for the appropriate customer connection.

4. Complete the rest of the connection creation process as normal.

Result

PingOne SSO for SaaS Apps adds your new application to the existing customer connection.

Finding the `idpId` value

When you are uncertain of a customer's `idpId` value, you can use IdP Discovery to specify the email domains associated with the customer (see Edit an invited customer connection). Alternatively, you can find the `idpId` in one of these ways:

Copyright © 2025 Ping Identity Corporation

Applications having multiple login URLs

Some cloud applications use a different login URL for each customer organization. If your application works this way, use URL-based IdP discovery, looking at the URL itself to find the `idpid`.

For example, if the customer is "Acme" and your application domain is "example.com", the login URL is similar to this:

```
https://acme.example.com/login
```

In this case, use "acme" as the `idpid` value.

Applications having a single login URL

Some cloud applications use a single login URL for all of their users, and associate the users with an organization after they are logged in.

If your application needs to work this way, you can specify the corporate identifier as the `idpid` parameter value in the request. For example:

```
https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=customer001.com
```

You can also use cookie-based IdP discovery (see below) in conjunction with this method.

Cookie-based IdP discovery

You can also store the user information in a cookie. However, you can only use this method when the user has signed on (SSO) previously using the same browser. Because this cannot be the only method used to find the IdP, you will need to use it with another discovery mechanism.

To use this method, when a user signs on (SSO), your application does a token exchange with PingOne to identify the user and create a session. When creating the user session, you will also have access to the `idpid` value, since it is one of the attributes supplied during the token exchange. You can then store this `idpid` value in a persistent cookie (named "idpid", for example). For subsequent user sign-ons, you then read the value from the request.

Certificate management

PingOne SSO for SaaS Apps tracks the status of active certificates and allows you to manage them from the **Certificate Management** page.

For multiplexed SAML applications and connected customer identity providers, you use signing certificates to sign single sign-on (SSO) and single logout (SLO) messages sent from PingOne SSO for SaaS Apps. Signing certificates created in PingOne SSO for SaaS Apps are self-signed by default. You can also create a certificate signing request (CSR) in PingOne SSO for SaaS Apps and send the certificate for signing by a certificate authority (CA).

PingOne SSO for SaaS Apps uses verification certificates to verify the signature on SSO and SLO messages received by PingOne SSO for SaaS Apps from service providers and identity providers. PingOne SSO for SaaS Apps first attempts to validate a signature using the primary verification certificate. If verification fails, PingOne SSO for SaaS Apps will then attempt to use the secondary verification certificate, where defined.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Verification and encryption certificates are not supported for applications using SAML v1.1

The **Dashboard** notification area in the admin portal displays an alert for certificates that are about to expire or have expired.

A yellow alert indicates:

- One or more signing certificates are due to expire in the next three months
- A primary verification certificate is about to expire (and will be replaced by a secondary verification certificate, if available)
- A secondary verification certificate is about to expire
- An encryption certificate is about to expire

A yellow alert for expiring certificates creates a link to the **Certificate Management** page.

A red alert indicates a certificate has expired. The alert contains a link to the **Certificate Management** page.

In addition to **Dashboard** messages, PingOne SSO for SaaS Apps notifies Global Administrators about expiring certificates by email. Notification emails are sent 60 days, seven days, and one day before a certificate expires, and again after the certificate expires.

For more information about email notification preferences, see Editing administrative roles, permissions, and notifications.

> **Note**
>
> You will be able to see certificates (signing or verification) that you cannot manage, and that originate outside of your account in the following circumstances:
>
> - A PingOne for Enterprise or Invited SSO account has a connection to your account's non-multiplexed SAML application. In this case, the connection's signing certificates will be visible to you.
> - A PingOne for Enterprise account uses an identity repository that employs certificates, such as PingFederate, a custom SAML, or ADFS identity repository, and also has a connection to one of your account's SAML applications. In this case both the signing and verification certificates for the identity repository, as well as the connection's signing certificate, will be visible to you.
>
> Although these certificates are visible to you, they are owned by a separate account and must be managed by an administrator in that account.
> Such certificates will also appear in your **Dashboard** notification area, if the certificates are expired or due to expire. This gives you visibility into certificates that are expiring or expired that your connected customers need to take action on.

View certificate details

You can use the **Certificates** menu to view detail about certificates ad the connections associated with them.

About this task

You can view certificate properties and the applications, connections, and identity bridges associated with a specific signing certificate, verification certificate, or encryption certificate. The certificate expiry date is displayed at the top right of the certificate entry. For signing certificates that you manage, you can also generate a signing certificate request (CSR).

Copyright © 2025 Ping Identity Corporation

Steps

1. In the PingOne admin portal, click **Setup** > **Certificates** > **Filters** and select the type of certificate you want to view.
2. Click to expand and display the certificate details for a selected certificate.
3. You have these options:

   Choose from:

   - **Properties**. View certificate properties, including type, issue date, serial number, Issuer and Subject DN, and the SHA1 and SHA256 fingerprints.

   Click **Make Default** to make this the default signing certificate for new application connections.

   - **Usage**. View the application connections or identity bridge associated with the certificate. Click a connection or identity bridge to switch to another certificate (signing certificates), upload a new certificate (verification certificate) or upload a new encryption certificate.
   - **CSR**. (Signing certificates only). Generate a certificate signing request, and import the CSR response.
   - **Share**. Share the certificate via email. You're prompted for the user's email address and the user is sent a download link for the certificate.
   - **Download**. Download the certificate to the default download location used by the browser.

Download or share a certificate

About this task

You can download a public certificate, or share it with others via email.

> **Note**
>
> For security reasons, PingOne doesn't allow exporting the private key of signing certificates.

Steps

1. Click **Setup** > **Certificates**.
2. Select the certificate and click either:

   Choose from:

   - **Download** to download the certificate.
   - **Share** to email the certificate to one or more email addresses.

Create a signing certificate

You can create signing certificates for use with multiplexed SAML applications or with manually configured customer IdP connections.

About this task

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> You cannot use signing certificates with non-multiplexed SAML applications because the signing certificate is specified when the connection to the application is created.

To create a new signing certificate, specify the certificate settings and the certificate key settings. You can also use the signing certificate to create a certificate signing request (CSR).

> **Note**
>
> Security is a function of the combination of algorithm and key size. A larger key size provides higher security but may take longer to sign messages.

Steps

1. In the PingOne admin portal, click **Setup** > **Certificates**.
2. Click **+Certificate** to add a new signing certificate.

   Result:

   Required fields are highlighted.
3. In the Certificate Settings section, enter the certificate information:
   - **Common name**. The common name (CN) identifying the certificate.
   - **Organization**. The organization (O) or company name creating the certificate.
   - **Organizational Unit**. The specific unit within the organization (OU).
   - **City**. The city or other primary location (L) where your organization operates.
   - **State**. The state (ST) or other political unit encompassing the location.
   - **Country**. The two letter ISO code for the country where your organization is located (such as, US, GB).
   - Select **Make certificate default** to make this the default certificate for new application connections.
4. Specify the certificate key settings:
   - **Validity** (days). The number of days until the certificate expires (defaults to 365).
   - **Key Algorithm**. The algorithm used to generate a key (RSA or ECC). Defaults to RSA.
   - **Key Size** (bits). The number of bits used in the key (defaults to 2048).
   - **Signature Algorithm**. The algorithm used to generate a signature (defaults to RSA SHA256).
5. Click **Save**.

   Result:

   The certificate appears in the certificates list.

Copyright © 2025 Ping Identity Corporation

Importing a certificate and key pair

Add an imported key pair and certificate to use as a signing certificate for PingOne SSO for SaaS Apps.

About this task

The imported certificate file must meet the following criteria:

- The certificate file must be a PKCS12 file in `.p12` or `.pfx` format
- The certificate must have a key length of 2048 bits or greater
- The certificate must be encrypted using SHA-256 or better
- The certificate must not be expired

> **Important**
>
> PingOne SSO for SaaS Apps can't accept certificate files created with OpenSSL 3.0.1. Use OpenSSL 1.1.1 or LibreSSL 2.8.3 instead.

Steps

1. Go to **Setup > Certificates**.
2. Click **Add > Import KeyPair/Cert**.
3. In the **Password** field, enter the password used to protect the PKCS12 file.
4. **Optional:** Select the **Make certificate default** checkbox to make this the default signing certificate.
5. Drag and drop, or click **Select a file** and choose a key store file to import.
6. Click **Upload**.

Associate certificates with a SAML application or customer IdP connection

When you manage the customer's identity provider (IdP) configuration and connection to a SAML application, or when the application is multiplexed, you can select the signing and verification certificates to associate with the application or direct customer IdP connection.

About this task

> **Note**
>
> Signing certificates can be associated with multiple applications and identity repositories.

Steps

1. Go to **Setup > Certificates**.
2. Click to expand the certificate currently associated with the application or direct customer IdP connection you want to change.
3. Click **Usage** to display a list of applications and direct customer IdP connections associated with that certificate.

Copyright © 2025 Ping Identity Corporation

4. Click to select the application or direct customer IdP connection you want to change. The **Update Certificate** window will appear.
5. Select a new signing certificate or verification certificate from the drop-down list and click **Save**.

View certificate usage

You can view a list of the applications, connections, and customer IdP connections associated with a signing, verification, or encryption certificate.

Steps

1. Click **Setup > Certificates**.
2. In the row for the certificate that you want to view, click to expand the details.
3. Click **Usage**.

   Result:

   A list of applications, connections, and/or customer IdP connections associated with the certificate is displayed.
4. Click an application or identity repository to update it.

   Result:

   A popup window opens showing the options for the multiplexed SAML application or customer IdP connection. You can only update the usage for multiplexed SAML applications and customer IdP connections that you manage.

Updating a signing certificate

You can update a signing certificate for a SAML application or customer IdP connection if:

- You are managing the customer IdP configuration and connection to the application.
- The application is multiplexed.

You can update the certificate for a single application, for multiple applications, for customer IdP connections, or by generating a certificate signing request (CSR) for signing by a certificate authority (CA).

Update a signing certificate for applications

You can view and update a signing certificate for applications from the certificate list.

About this task

> **Caution**
>
> Before you update a signing certificate with an application, you must ensure that your service provider (SP) has the latest signing certificate. If the SP does not have the updated signing certificate in their system, users will not be able to SSO into the application.

Copyright © 2025 Ping Identity Corporation

Steps

1. Go to the **Setup > Certificates** page.
2. In the certificates list, expand the relevant entry and click **Usage** to display a list of applications associated with the certificate.
3. For each application:
    1. Click the application link. The **Update Certificate** popup window opens.
    2. Select a signing certificate from the dropdown list and then click **Save**.

       Result:

       A message is displayed to indicate the certificate has been successfully assigned to the application. The application no longer appears in the list of applications to update.
4. When you've updated all applications, you can delete the expired (or expiring) certificate by clicking the **Delete** icon.

   Result:

   The signing certificate is removed from the certificates list.

Update a signing certificate for a customer IdP

You can edit a customer identity provider (IdP) connection either individually or in bulk.

About this task

> **Caution**
>
> Before you update a signing certificate with an IdP, you must ensure that your IdP has the latest signing certificate. If the IdP does not have the updated signing certificate in their system, users will not be able to SSO into the application.

Steps

1. Go to **Setup > Certificates**.
2. In the certificates list, expand the certificate you want to change and click **Usage** to display a list of customer IdP connections associated with the signing certificate.
3. Update a signing certificate.

   Choose from:

    - To update the certificate for an individual application:
        1. Click the name of the application to open the **Update Certificate** window.
        2. Select a new certificate from the **Select a Signing Certificate** list.
        3. Click **Save**.
    - To update the certificate for multiple applications:
        1. Select the box for each application you want to update.

Copyright © 2025 Ping Identity Corporation

2. Click **Update Selected** to open the **Update Certificate** window.
3. Select a new certificate from the **Select a Signing Certificate** window.
4. Click **Save**.

   Result:

   A message is displayed to indicate the certificate has been successfully assigned to the application connection. The applications no longer appear in the list of applications to update.

Sign a certificate using a CSR

You can generate a Certificate Signing Request (CSR) using a signing certificate that you created by downloading the CSR for the relevant certificate and sending the CSR to a Certificate Authority (CA). The CA will send back a CSR response that you can upload to PingOne.

Steps

1. Click **Setup > Certificates**.
2. In the certificate list, expand the details for a signing certificate and click **CSR**.
3. Click **Export** and browse to the location to save the CSR response.
4. Upload the CSR to a CA for signing.

   Result:

   The CA signs the certificate and sends you a CSR response.

5. Click **Import**, browse to the CSR response and click **OK**.

   Result:

   The CSR response is imported and saved. Your multiplexed SAML applications and identity repositories. will be associated with this CA-signed certificate for SAML assertions.

Updating a verification certificate for an application or customer IdP connection

When an application or customer identity provider (IdP) connection verification certificate expires or is about to expire, generally you must upload a new verification certificate.

About this task

You can update a verification certificate for a SAML 2.0 application if:

- You are managing the customer IdP configuration and connection to the application.
- The application is multiplexed.

Steps

1. Go to **Setup > Certificates**.
2. Expand the relevant entry and click the **Usage** tab.

Copyright © 2025 Ping Identity Corporation

3. Click the application or customer IdP connection for which you need to update the verification certificate.

   Result:

   The **Replace Primary Certificate** popup window opens, prompting you to upload the new verification certificate.

4. Click **Choose File** and browse to the location of the new verification certificate.

   Result:

   A message is displayed to indicate the certificate has been successfully updated for the application.

Update an encryption certificate

You can update the encryption certificate used for an application. You will need to upload the new encryption certificate.

Steps

1. In the PingOne admin portal, click **Setup** > **Certificates**.
2. Expand the entry for the encryption certificate to update and click **Usage**.

The applications using the encryption certificate are displayed.

1. For each application displayed, click the application and click **Choose File**, then browse to the location of the new encryption certificate.
2. Click **Save**.

Result

The new encryption certificate will now be used for the application.

Delete a certificate

About this task

You must ensure there are no dependent applications or customer connections before deleting a signing certificate. If there are applications associated with the signing certificate, it cannot be deleted.

> **Note**
>
> If there are no dependencies for a verification or encryption certificate, the certificate is automatically deleted.

Steps

1. Go to **Setup** > **Certificates**.
2. In the certificates list, expand the relevant entry and click the Delete icon.

Copyright © 2025 Ping Identity Corporation

Managing reports and subscriptions

Use the reports and subscription tools to monitor PingOne SSO for SaaS Apps activity.

Reports return a one-time report of data using either predefined or custom reports. PingOne SSO for SaaS Apps logs events per report type and retains the logs for 1 year. For a list of the available event data, see PingOne SSO for SaaS Apps report types.

Subscriptions generate recurring reports of audit events for a report type. For example, you might create a subscription to the Administrator Login report type to receive the event data for each time a PingOne SSO for SaaS Apps administrator signs on. A subscription can be either a Push or Poll type. See Subscriptions for more information.

Reports

You can choose to run a predefined report or run a custom report by modifying predefined report parameters.

Create an 'on the fly' report to view event data information per report type, for a specific time period, or run one of the predefined reports provided. We provide a number of predefined reports for your convenience. The predefined report is based on a specific report type.

You can specify that the results are displayed relative to a particular time zone. You're also able to filter results based on the event data for the report type (such as, `Action` or `Admin Id`).

You can select which of the available event data you want to include in the report, and export a copy of the report in `.csv` format.

> **Note**
>
> The amount of data that can be exported for a report is determined either by duration or quantity. The exported data is limited to either one week's data or 500,000 lines of data. We will use the smaller of the two values.

For more information about running reports, see Run a predefined report and Run a custom report.

PingOne SSO for SaaS Apps report types

The `Report Type` parameter controls the type of report to produce or the audit event type to use for a subscription.

For more information about running reports, see Run a predefined report and Run a custom report.

> **Note**
>
> Some of the types are for reports only and are not used for subscriptions, as indicated.

The following report types are available for PingOne SSO for SaaS Apps and PingOne SSO for SaaS Apps for Managed Accounts.

For report types available on PingOne for Enterprise, see PingOne for Enterprise report types.

Copyright © 2025 Ping Identity Corporation

PingOne SSO for SaaS Apps report types

Report Name	Description
Administrative Activity	Transactions initiated by a PingOne SSO for SaaS Apps administrator during a specific period. If a Support administrator accesses your account and makes a change, an audit event is triggered for that change. The actor associated with the audit event will be the name of the Ping Support administrator and the type will be `ping admin`. If a PingOne SSO for SaaS Appss administrator disables or deletes a connection to one of their applications, an audit event is triggered for that change in the connecting customer account. The actor associated with the audit event will be the name of the PingOne SSO for SaaS Apps administrator and the type will be `application admin`. For PingOne SSO for SaaS Apps With Managed Accounts, if an administrator accesses a managed account and makes a change, an audit event is triggered for that change. The actor associated with the audit event will be the name of the administrator and the type will be `msp admin`.
Administrator Login	Sign on attempts by administrators and their success or failure during a specific period.
Log Subscription (Reports only)	Audit events related to the creation, update, and deletion of audit log subscriptions during a specific period
SSO By Customer	The count of unique users and the total number of SSO transaction events during a specific period for each application configured for your account. You can choose to filter the results based on `Application Name` or `Customer Name` event data.
SSO By Customer (IDPID)	The count of unique users and the total number of SSO transaction events during a specific period for each application configured for your account, based on the customer's `idpid`. You can choose to filter the results based on `Application Name` or `IdP ID` event data.
SSO Summary By Customer	The count of unique users and the total number of SSO transaction events during a specific period for each application configured for your account. You can choose to filter the results based on `Application Name` or `Customer Name` event data.
SSO Summary By Customer (IDPID)	The count of unique users and the total number of SSO transaction events during a specific period for each application configured for your account, based on the customer's `idpid`. You can choose to filter the results based on `Application Name` or `IdP ID` event data.
SSO User Count	The count of total unique users and total SSO transactions for each customer during a specific period.

Copyright © 2025 Ping Identity Corporation

Report Name	Description
SSO User Count (IDPID)	The count of total unique users and total SSO transactions for each customer during a specific period, by customer `IdP ID`.

PingOne SSO for SaaS Apps report event reference

The following table describes the event data types found in PingOne SSO for SaaS Apps reports.

For more information about running reports, see Run a predefined report and Run a custom report.

For more information about report types, see PingOne SSO for SaaS Apps report types.

Event Data	Report Type	Event Data Description
Action	• **Administrative Activity** • **Directory** • **Log Subscription**	The action performed by the audited user.
Admin	**Administrative Activity**	The email address or LDAP name assigned to the administrator.
Admin Id	**Administrative Activity**	The unique identifier assigned by PingOne SSO for SaaS Apps to the administrator.
Admin Type	**Administrative Activity**	The type of administrator. **Note** The administrator type is `user` unless the action was performed by a Ping Identity employee.
Application	• **SSO Summary By Customer** • **SSO Summary By Customer (IDPID)**	The applications used for single sign-on (SSO).
Application Name	• **SSO Summary By Customer** • **SSO Summary By Customer (IDPID)**	The name of the application used for SSO.

Copyright © 2025 Ping Identity Corporation

Event Data	Report Type	Event Data Description
Application Subject	• **SSO Summary By Customer** • **SSO Summary By Customer (IDPID)**	The contact email address for the application's service provider (SP).
Browser Agent	• **Administrator Login** • **Administrative Activity** • **SSO By Customer** • **SSO By Customer (IDPID)**	The browser name and version used for SSO.
Connection ID	• **SSO By Customer** • **SSO By Customer (IDPID)**	The unique identifier assigned to the PingOne SSO for SaaS Apps connection used for SSO.
Customer Account ID	• **SSO By Customer** • **SSO By Customer (IDPID)**	The unique identifier for the customer.
Customer Name	• **SSO By Customer** • **SSO By Customer (IDPID)**	The name of the customer.
Identity Repository Subject	• **SSO By Customer** • **SSO By Customer (IDPID)**	The contact email address for the application's identity provider (IdP).
IdP ID	• **SSO By Customer** • **SSO By Customer (IDPID)**	The unique identifier assigned to the identity repository used for user authentication.
IP Address	• **Administrator Login** • **Administrative Activity** • **SSO By Customer** • **SSO By Customer (IDPID)**	The IP address of the host used to initiate the transaction.
Message	All report types	A PingOne SSO for SaaS Apps message providing information related to the transaction.
Resource Id	**Administrative Activity**	The unique identifier assigned by PingOne SSO for SaaS Apps to the PingOne SSO for SaaS Apps resource.

Copyright © 2025 Ping Identity Corporation

Event Data	Report Type	Event Data Description
Resource Name	• **Administrative Activity** • **Directory** • **Log Subscription**	The display name for the PingOne SSO for SaaS Apps resource upon which an action was performed.
Resource Name 2	• **Administrative Activity** • **Directory** • **Log Subscription**	The display name for an additional PingOne SSO for SaaS Apps resource upon which an action was performed.
Resource Name 3	• **Administrative Activity** • **Directory** • **Log Subscription**	The display name for an additional PingOne SSO for SaaS Apps resource upon which an action was performed.
Resource Type	• **Administrative Activity** • **Directory** • **Log Subscription**	The type of PingOne SSO for SaaS Apps resource upon which an action was performed.
Resource Type 2	• **Administrative Activity** • **Directory** • **Log Subscription**	The type of PingOne SSO for SaaS Apps resource for**Resource Name 2** upon which an action was performed.
Resource Type 3	• **Administrative Activity** • **Directory** • **Log Subscription**	The type of PingOne SSO for SaaS Apps resource for **Resource Name 3** upon which an action was performed.
SP Account ID	• **SSO By Customer** • **SSO By Customer (IDPID)**	The unique identifier for the SP's PingOne SSO for SaaS Apps account.

Copyright © 2025 Ping Identity Corporation

Event Data	Report Type	Event Data Description
Status	All report types	The current status of the transaction. Possible status values are: ***IDP_DONE*** The user was authenticated by the configured IdP and PingOne SSO for SaaS Apps has received an assertion from the IdP. ***SUCCESS*** The user was successfully redirected to the target application. ***FAILURE*** SSO was not successful. ***OIDC_TOKEN*** The OpenID Connect (OIDC) token request was processed. ***OIDC_USERINFO*** The OIDC UserInfo request was processed. ***OIDC_INTROSPECT*** The OIDC token introspection request was processed.
Subject	**Administrator Login**	The email address for the person initiating the transaction. For SSO, this is equivalent to the **Identity Repository Subject**.
Timestamp	All report types	The date and time for the current reporting data.
Total SSO Transactions	• **SSO Summary By Customer** • **SSO Summary By Customer (IDPID)**	The total number of SSO transactions attempted for the reporting period.
Tracking ID	• **SSO By Customer** • **SSO By Customer (IDPID)**	A unique identifier for the transaction. The **Tracking ID** can be used by PingOne SSO for SaaS Apps to troubleshoot issues if necessary.

Copyright © 2025 Ping Identity Corporation

Event Data	Report Type	Event Data Description
Unique Users	• **SSO Summary By Customer** • **SSO Summary By Customer (IDPID)**	The total number of unique users attempting SSO for the reporting period. Subsequent attempts by the same user aren't included in the total.

Subscriptions

PingOne SSO for SaaS Apps audit events are available through a subscription facility.

The subscriptions can be either:

- A Push type, where PingOne for Enterprise streams audit events to an external service in real time.
- A Poll type, where your client retrieves audit events as needed in configurable blocks of records, until all retrievable records are consumed.

> **Note**
>
> Audit events that occurred prior to a subscription being created are not delivered. Only audit events occurring after the subscription is created are delivered.
> However, if you create another subscription of the same type, you will have access to events that occurred prior to that subscription, because those events were already being tracked.

Each audit event for a subscription is retained for seven days. After that time, if you haven't already received or retrieved the audit event record, it will not be available.

PingOne attempts to deliver an audit event message for both types of subscriptions. You might receive duplicate messages because of streaming retries or very frequent polling. Each audit event message includes a unique `id`, so you can easily identify duplicate messages.

Push subscriptions

Push subscriptions push events to the target server in real time.

The audit events matching the subscription are streamed to the HTTPS endpoint configured for the subscription.

The uploaded certificate must match what an external client would see when accessing the configured URL. Be aware of load balancers or other network devices that might present a different certificate.

The audit event information can be returned in either the PingOne audit format or a include::ROOT:partial$p14e_p1refs_splunk.adoc[tags=Splunk]-compatible format. Both formats are JSON.

If the delivery of a Push audit event fails, PingOne will continue to retry delivery. The interval period between retries will increase to a maximum of 15 minutes. PingOne for Enterprise will retry to deliver for 7 days and then discard the event.

If events aren't arriving as expected, check the reports at **Dashboard > Reporting > Run New Report**. Choose **Log Subscription** as the type and check for errors. For example, certificate-related exceptions indicate that the certificate being presented does not match the certificate on file in PingOne for Enterprise.

Copyright © 2025 Ping Identity Corporation

For more information, see Adding a Push subscription

Poll subscriptions

Poll subscription audit events are accumulated and made available to you. You must use a script or client to retrieve the audit events. The client can retrieve the events, up to the configured batch size specified for the subscription.

Poll subscription audit events are collected and returned once per subscription. This means that each poll retrieval will have a different result set.

The audit event information is returned in the PingOne audit format.

An easy way to retrieve the audit events for a poll subscription is to use `cURL`. For instructions on how to create a cURL command, see Get the audit events for a Poll subscription.

Estimate how much traffic you expect to generate and set your poll rate and batch size accordingly. Leave some extra room in your batch size, because some transactions can generate multiple events. For example, if you have 1000 users authenticating per hour, it will generate from 1000 to 3000 events. For this traffic level, you can set a batch size of 1000 and poll every 20 minutes, or a batch of 200 and poll every four minutes. You should poll at least hourly, even with lower usage.

The number of audit events accumulated may be less than the batch size. The configured batch size is an upper limit, not a consistent number of returned events.

A poll request with zero results means that you are caught up to the present and there are no new events. Your poll rate should be set so that this happens regularly.

Polling events are returned in roughly chronological order from oldest to newest. To ensure strict chronological order, set your client to sort events by timestamp.

Events are stored for 7 days and then discarded. You must ensure that your client doesn't fall more than 7 days behind, or you will lose data.

If you do fall behind and events begin to backlog, batch size and sorting can become less consistent. For example, if your batch size is 1000 and you fall a week behind in polling, you might get responses with 600-700 events, with older events grouped in with new ones. This doesn't mean that events are missing. All events are available and will be returned as your collector catches up. But they won't be in consistent order.

For more information, see Add a Poll subscription.

Choosing Push or Poll

Poll subscriptions give the client control over the rate at which events are collected and saved to your storage system, but the client is responsible for ensuring it doesn't fall behind.

Push subscriptions are not batched, and therefore generate more traffic because they generate one request per event. Your target system must be able to handle the traffic load.

We generally recommend Push subscriptions because they are simpler, especially if you have large amounts of traffic (in the tens of thousands of events per hour), which can make it difficult to determine the right poll frequency.

Copyright © 2025 Ping Identity Corporation

Manage partner accounts

Using PingOne SSO for SaaS Apps with Managed Accounts, you can create and configure PingOne for Enterprise accounts for your partners.

You can also suspend a partner account when necessary. When you administer a partner account, you access the account's PingOne for Enterprise admin portal as a Global Administrator, with full rights to the partner account.

In the instructions to create or edit a partner account, you're linked to the PingOne for Enterprise instructions needed to complete the workflows. There's also much more you can do to configure and administer the partner account.

For more information, see the PingOne for Enterprise documentation.

> **Important**
>
> PingOne SSO for SaaS Apps with Managed Accounts is a limited-release function. To request access, open a support case.

Configure partner account service settings

As a Global Administrator, configure partner settings for your managed service.

About this task

> **Note**
>
> All of the settings on this page are optional. Any settings that you do not assign will use the default values. Default values are noted where possible.

Steps

1. Go to **Managed Accounts** > **Service Settings**.

   Service Settings is not displayed for Audit & Report Administrators.

2. To enable Edit mode, click **Edit**.

3. To allow your partners to change the corporate logo displayed on their dock, select **Allow Logo Customization**.

   > **Note**
   >
   > When this option is enabled, your partners can change this logo on one of three menus in their PingOne SSO for SaaS Apps admin portal:
   > - **Setup** > **Branding** > **Dock**
   > - **Setup** > **Branding** > **Logon & SSO**
   > - **Account** > **Branding**

4. To assign the corporate branding logos for your service, click the appropriate **Select Image** button, and then select the local image you want to use.

   Once saved, the logo will appear on your partners' **User Dock** and in their **Admin Portal**

Copyright © 2025 Ping Identity Corporation

5. To make only certain identity repositories available for selection, click to clear the **Allow All Identity Repositories** checkbox.

   By default, all PingOne SSO for SaaS Apps identity repositories (current or future) are available for your customers to select. After you disable the **Allow All Identity Repositories** checkbox, the identity repository options display.

   1. Select the identity repositories to allow your customers to use.

6. To allow your partners to set up, customize, or disable the multi-factor authentication (MFA) policy, enable the **Allow MFA Customization** setting.

   When this setting is enabled (the default), your customers can change their account settings for MFA.

   When disabled, the configuration for MFA appears as read-only information to your customers and they're unable to change the settings.

7. Configure the templates for emails automatically sent to partners.

Option	Description
Sender	The sender address used in emails sent to your customers. The ability to customize this field is disabled by default. To enable it, log on to your account and submit a support case.
Admin Invite	In the **Subject Line** field, enter a subject line for admin invite emails. To customize the admin invite email template click **Download Template**.
Password Reset	In the **Subject Line** field, enter a subject line for password reset emails. To customize the password reset email template click **Download Template**.

   1. To view or modify the default HTML email template sent to customers, click **Download Current Template**.

   You can modify this template for your use or create a new HTML template. Any new templates you create need to be valid HTML and use the same variables as in the default template. Do not add any new variables.

   1. To replace the current default template, click **Replace Template** and then select the HTML file to use.
   2. To delete an email template, click **Remove Saved Template**, and then click **Save**.

      Result:

      The custom template is removed and the default PingOne SSO for SaaS Apps email template is restored.

      > **Note**
      >
      > The ability to customize this field is disabled by default. To enable it, log on to your account and submit a support case.

Copyright © 2025 Ping Identity Corporation

8. To change the support link that appears in the header of each page, enter a new URL in the **Support Link** field.
9. Click **Save**.

Creating and administering a partner account

About this task

You will create PingOne for Enterprise accounts for your partners. You have the option to enter the partner account immediately to configure the identity repository and any other initial settings. You can also choose to create your partner accounts and configure the accounts later.

When you create a partner account, an **Applications > Private App Catalog** page is added to the partner's PingOne for Enterprise admin portal. This page exists only in PingOne for Enterprise managed partner accounts. When you add an application in the partner account, the application is displayed on this page as well as on the **My Applications** page.

The application listing in the Private App Catalog is the same for all partner accounts. Any applications that you add for a partner account are displayed in the Private App Catalog for all partner accounts.

> **Note**
>
> When you add applications to a partner account, the application connections are not displayed on the **Customer Connections** page in your PingOne SSO for SaaS Apps account.

Steps

1. Sign on to your account in the PingOne SSO for SaaS Apps admin portal and go to **Managed Accounts**.
2. Click the **Create Account** button (upper right).
3. Enter the account name to assign to the partner account.
4. Enter the ID you want to use internally to refer to the partner account. This is a unique identifier you can use for this customer within the context of your service. Click **Done**.

   You are then prompted whether to enter the new partner account.

   Choose from:

   - If you choose to enter the partner account immediately, we assume your intent is to configure the account and the identity repository setup is displayed.

     Learn more about PingOne for Enterprise identity repositories in PingOne for Enterprise identity repositories. Fin instructions for setting up an identity repository in Connecting to an identity repository

   - If you choose not to enter the partner account immediately, the new partner account is added to your Managed Accounts page. You can then edit the account later and click **Enter Account** to do the configuration.

     When you do enter the account for configuration, see PingOne for Enterprise identity repositories for information about PingOne identity repositories. For instructions when setting up an identity repository, see Connecting to an identity repository

Copyright © 2025 Ping Identity Corporation

5. **Optional:** Click **Enter Account**. You are prompted to verify the account access, then the admin portal for the partner PingOne for Enterprise account is displayed. In the header at the top of each page is a banner identifying you as administering this account.

> **Tip**
>
> If your partner account uses Azure AD, Google, or a custom OIDC identity provider (IdP), you can enable more detailed event reporting by going to **Dashboard > Reporting > Settings** and clicking **Verbose**.
> Normal reports and subscriptions display events. Verbose reports and subscriptions display events and the claims sent by the IdP, though not the values of those claims.
> Verbose reporting helps accounts with OIDC IdPs troubleshoot missing or misspelled claims.
> The verbose reporting feature is currently in limited release. To request access to this feature, open a support case.

See the PingOne for Enterprise documentation for complete information when administering a partner account.

1. When you are finished, click the **Exit** button in the banner to quit administering the customer account and return to the **Managed Accounts** page.

Inviting a new customer

Create a new customer connection by inviting them to connect with your application.

About this task

When you invite a customer to use your applications, you enter the profile information for the new customer. PingOne SSO for SaaS Apps sends an email invitation to the customer.

> **Note**
>
> To invite a new customer, you must be either a Global Administrator or Support Administrator (either Read and Write or Read-Only)

After sending the invitation, you can choose to resend or cancel the customer invitation, if necessary.

Steps

1. Go to **Managed Accounts**.
2. Click **+ Invite Customer**.
3. Enter the profile information for the new customer.

   The **Customer ID** entry is optional. This is a unique identifier you can use for this customer within the context of your service as account manager.
4. Click **Done**.

   Result:

   An email invitation is automatically sent to the customer email address you specified, and the new customer is added to your customer listing.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> If you have customized an email template for your service, the customized template will be used. Otherwise, the PingOne SSO for SaaS Apps default email template is used.
> For more information about customizing email templates, see Configuring customer account service settings.

Enable IdP discovery

About this task

You can use IdP discovery to associate the partner account with an identity provider (IdP). When you're initiating an SSO request (SP-initiated SSO), there's then no need to specify the identifier for the identity provider (IdP). Instead, we will resolve the correct IdP by associating an email domain with the partner's IdP. During a user's initial SSO, we will prompt the user to enter a matching email domain. (The user is prompted for the email domain only during their initial SSO.)

Steps

1. Select the **Managed Accounts** tab to display the list of managed customer accounts.
2. Click the Details icon to display the account details, and click the edit icon.
3. **Optional:** Edit the available account settings.
4. In the **IdP Discovery** section, enter the **Email Domain** to use for IdP discovery. We'll use the email domain you specify to discover the IdP and assign it to the partner account.
    1. Enable **Set as default IdP** if you want us to redirect users to the IdP for the specified email domain. We will redirect users to this IdP in the event that, during SP-initiated SSO, users enter an email address that we are unable to match to an IdP.

       The **Set as default IdP** setting will not be displayed if you have already enabled this setting for the partner account.

    When a user initially attempts to sign on (SSO) to the application, the user is prompted for their email address. If the domain of the email address matches one of the IdP discovery domains you've assigned, we will redirect the user to the corresponding IdP for authentication. If the domains do not match and you have not enabled **Set as default IdP**, an error is displayed and the user is prompted again for their email address. When **Set as default IdP** is enabled, the user is redirected to the default IdP to authenticate.

Reference

- If you don't find what you need in this guide, try the Support and Community portal.
- The Ping Developer portal is your information center for integration with Ping Identity products.

PingOne SSO for SaaS Apps Customer Connection API

You can use the PingOne SSO for SaaS Apps Customer Connection API to create or update application connections without using the admin console.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Ping Identity periodically deprecates obsolete TLS protocols and cipher suites. To stay compatible with these changes, you should ensure that your platform stays within its support life cycle. For example, a Java application should use a Java version that is currently supported by the Java vendor.

The PingOne SSO for SaaS Apps Apps Customer Connection API conforms to the design principles of Representational State Transfer (REST), providing a set of resources you can use, and supporting the JSON data format. The API returns HTTP status codes with each resource response. If an error occurs, an error message is returned in the response. Resource request parameter values are required unless otherwise indicated. These parameter values need to be converted to UTF-8 and URL-encoded.

PingOne considers connections with the same `idpId` value as belonging to the same identity provider (IdP), so most parameter settings are shared across all connections using the same idpId. Updating the parameter settings on one connection applies the same changes to all connections with the same idpId.

The exception to this is the `multiplexed` parameter, which determines whether the IdP uses a single connection to PingOne or distinct connections to each of your applications. The `multiplexed` setting is specific to each application connection.

To use the Customer Connection API, you need the API credentials for your account. For information on retrieving these credentials, see Using the global REST API client credentials.

> **Note**
>
> The `saasid` is a UUID that uniquely identifies an application connection.
> To find the `saasid`, go to **Applications > My Applications**. The `saasid` for each application connection is in parentheses under the connection name.

Create a customer connection

Creates a connection between your service and a customer.

```
PUT https://admin.pingone.com/web-portal/rest/saas/idp/2.0/spManaged/<idpId>
```


Copyright © 2025 Ping Identity Corporation

Request parameters

Parameter	Description
`applications` (optional)	An array of one or more unique application saasids. For example: `["6964005a-6270-4a88-9ddc-0e6a4e05e51d", "338821d7-dd17-469f-a3c1-8025a0112ebe"]` If you include specific application values: • If the application is multiplexed SAML or OIDC, creates a connection to specified applications • If the application is non-multiplexed SAML, returns an error message • If the application is multiplexed or OIDC but disabled, returns an error message If you don't include application values, creates a connection to all enabled applications with the specified idpId, as long as they are enabled and either multiplexed SAML or OIDC.
`multiplexed` (optional)	If `true` or not specified, creates multiplexed connections. If `false`, creates non-multiplexed connections.
`email`	The email address for the customer administrator.
`idpId`	A unique identifier for the customer. See The `idpId` Parameter for more information.
`entityId`	A unique string used to identify the customer to us.
`ssoEndpoint`	The endpoint at the customer to which we will send SAML AuthnRequests. **Note** The SSO binding is not configurable using the Customer Connection API. PingOne SSO for SaaS Apps will always send the AuthnRequest using the Redirect binding for connections created through the API.
`sloEndpoint` (optional)	The URL at the identity provider (IdP) to which PingOne sends SAML single logout (SLO) requests.
`sloResponseEndpoint` (optional)	The URL at the IdP to which PingOne sends SAML SLO responses.

Copyright © 2025 Ping Identity Corporation

Parameter	Description
`sloBinding` (optional)	Determines which binding type PingOne uses to send SAML SLO requests. Valid values are `Redirect` or `POST`. If not specified, defaults to `POST`.
`signAuthnRequest` (optional)	If `true`, enables AuthnRequest signing. If `false` or not specified, defaults to disabled.
`signingCertificateData`	The public certificate for the customer's signing certificate. The customer IdP uses this certificate to sign SAML assertions to PingOne. PingOne sees this as the verification certificate.
`signingCertFingerprint` (optional)	The signing certificate fingerprint that PingOne uses to sign the AuthnRequest or SLO request to the customer IdP. You can find the fingerprint value by expanding the certificate details in the **Setup > Certificates** menu. For more information, see View certificate details. If not specified, designates the default signing certificate.
`signingAlgorithm` (optional)	If specified, sets signing algorithm to specified value. Valid values are: • `RSA_SHA1` • `RSA_SHA256` (default) • `RSA_SHA384` • `RSA_SHA512` If not specified, defaults to `RSA_SHA256`.

Response Parameters

None.

Status Codes Returned

Status Code	Description
`201 Created`	The resource has been created.
`400 Bad Request`	The request was invalid. An accompanying error message explains why.
`403 Forbidden`	The request was understood, but has been refused. An accompanying error message explains why.
`404 Not Found`	No available application found with given parameters.
`409 Conflict`	The resource requested to be created already exists.

Copyright © 2025 Ping Identity Corporation

Example

```
   PUT https://admin.pingone.com/web-portal/rest/saas/idp/2.0/spManaged/exampleIdp.com
{
        "email": "admin@exampleIdp.com",
        "entityId": "example Identity Provider",
        "ssoEndpoint": "http://www.exampleIdp.com",
        "signingCertificateData": "MIIDkDCCAvmgAwIBAgIJAONZ/
Sh8jJVaMA0GCSqGSIb3DQEBBQUAMIGNMQswCQYDVQQGEwJVUzER\
                nMA8GA1UECBMIQ29sb3JhZG8xDzANBgNVBAcTBkRlbnZlcjEiMCAGA1UEChMZRXhhbXBsZSBJZGVu\
                ndGl0eSBQcm92aWRlcjERMA8GA1UEAxMISm9obiBEb2UxIzAhBgkqhkiG9w0BCQEWFGFkbWluQGV4\
                nYW1wbGVJZHAuY29tMB4XDTExMTAyNjIyNDA1MFoXDTIxMTAyMzIyNDA1MFowgY0xCzAJBgNVBAYT\
                nAlVTMREwDwYDVQQIEwhDb2xvcmFkbzEPMA0GA1UEBxMGRGVudmVyMSIwIAYDVQQKExlFeGFtcGxl\
                nIElkZW50aXR5IFByb3ZpZGVyMREwDwYDVQQDEwhKb2huIERvZTEjMCEGCSqGSIb3DQEJARYUYWRt\
                naW5AZXhhbXBsZUlkcC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMx6WsTrzwhi10De\
                nPvvTa/Ndle2+3ZLePGXE/0v1qmm8Pji8l0czcg8ner56KBgnt2gnJ5xGrN51zBjZi7Qg2cL3A5cQ\
                nErJdYNsc7Oedulmp6RnDInMX1sfn/kGc3L/zBdwrngQWv86vN3bawvtj5wYsc9OAG1+X1kQeDuyR\
                ne/NlAgMBAAGjgfUwgfIwHQYDVR0OBBYEFMDDtN8tPSFrVtUWcpc0mbtsge9UMIHCBgNVHSMEgbow\
                ngbeAFMDDtN8tPSFrVtUWcpc0mbtsge9UoYGTpIGQMIGNMQswCQYDVQQGEwJVUzERMA8GA1UECBMI\
                nQ29sb3JhZG8xDzANBgNVBAcTBkRlbnZlcjEiMCAGA1UEChMZRXhhbXBsZSBJZGVudGl0eSBQcm92\
                naWRlcjERMA8GA1UEAxMISm9obiBEb2UxIzAhBgkqhkiG9w0BCQEWFGFkbWluQGV4YW1wbGVJZHAu\
                nY29tggkA41n9KHyMlVowDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQBqagX/ZasSD0NP\
                nQnR3zDXAYJK87VO59mn21TLEYaKG9vcm+odQhc0XkwLR/PLMTv3GSV9dfC0F6QHogLpZe1W+oa7Q\
                n+7Utasnsgs4Kfp0s2jQaPnUJRpGKXFPyOJ17RkjJgubKcYnX+vYV13tBDq4cIIm68dqZZqzaXDau\n0Z3h2Q==",
}
```

Get a Customer Connection

Returns all available information about a customer connection.

```
   GET https://admin.pingone.com/web-portal/rest/saas/idp/2.0/spManaged/<idpId>
```

Request Parameters

Parameter	Description
`application` (optional)	If the application connection exists, returns only that connection's information. If no application matches the saasid, returns all connections with the same idpId.
`idpId`	A unique identifier for the customer. See The `idpId` Parameter for more information.

Response Parameters

Parameter	Description
`email`	The email address for the customer administrator.

Copyright © 2025 Ping Identity Corporation

Parameter	Description
`idpId`	A unique identifier for the customer. For more information, see The `idpId` Parameter.
`entityId`	A unique string used to identify the customer to us.
`ssoEndpoint`	The endpoint at the customer to which we will send SAML AuthnRequests. **Note** The SSO binding is not configurable using the Customer Connection API. PingOne SSO for SaaS Apps will always send the AuthnRequest using the Redirect binding for connections created through the API.
`signingCertificate`	The customer's public certificate for the customer's signing certificate (encoded in MIME Base64). PingOne uses this to sign SAML assertions.
`multiplexed`	Whether the connection is multiplexed.
`sloEndpoint`	The URL to which the connection sends SLO requests.
`sloResponseEndpoint`	The URL at the IdP to which PingOne sends SAML SLO responses.
`sloBinding`	The binding type the connection uses to send SLO requests.
`signAuthnRequest`	Whether the connection signs outgoing AuthnRequests.
`signingAlgorithm`	Which signing algorithm the connection uses to sign outgoing AuthnRequests.
`signingCertFingerprint`	Not provided in the GET response.
`connectionsStatus`	The customer connection status. Possible values are: • Active • Complete • Disabled • Disabled by Customer • Account Suspended

Copyright © 2025 Ping Identity Corporation

Status Codes Returned

Status Code	Description
`201 Created`	The resource has been created.
`400 Bad Request`	The request was invalid. An accompanying error message explains why.
`403 Forbidden`	The request was understood, but has been refused. An accompanying error message explains why.
`404 Not Found`	No available application found with given parameters.
`409 Conflict`	The resource requested to be created already exists.

Example

```
   GET https://admin.pingone.com/web-portal/rest/saas/idp/2.0/spManaged/exampleIdp.com
[
        {
                "email": "admin@exampleIdp.com",
                "idpId": "exampleIdp.com",
                "entityId": "example Identity Provider",
                "ssoEndpoint": "http://www.exampleIdp.com",
                "signingCertificate": "MIIDkDCCAvmgAwIBAgIJAONZ/
Sh8jJVaMA0GCSqGSIb3DQEBBQUAMIGNMQswCQYDVQQGEwJVUzER\
                nMA8GA1UECBMIQ29sb3JhZG8xDzANBgNVBAcTBkRlbnZlcjEiMCAGA1UEChMZRXhhbXBsZSBJZGVu\
                ndGl0eSBQcm92aWRlcjERMA8GA1UEAxMISm9obiBEb2UxIzAhBgkqhkiG9w0BCQEWFGFkbWluQGV4\
                nYW1wbGVJZHAuY29tMB4XDTExMTAyNjIyNDA1MFoXDTIxMTAyMzIyNDA1MFowgY0xCzAJBgNVBAYT\
                nAlVTMREwDwYDVQQIEwhDb2xvcmFkbzEPMA0GA1UEBxMGRGVudmVyMSIwIAYDVQQKExlFeGFtcGxl\
                nIElkZW50aXR5IFByb3ZpZGVyMREwDwYDVQQDEwhKb2huIERvZTEjMCEGCSqGSIb3DQEJARYUYWRt\
                naW5AZXhhbXBsZUlkcC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMx6WsTrzwhi10De\
                nPvvTa/Ndle2+3ZLePGXE/0v1qmm8Pji8l0czcg8ner56KBgnt2gnJ5xGrN51zBjZi7Qg2cL3A5cQ\
                nErJdYNsc7Oedulmp6RnDInMX1sfn/kGc3L/zBdwrngQWv86vN3bawvtj5wYsc9OAG1+X1kQeDuyR\
                ne/NlAgMBAAGjgfUwgfIwHQYDVR0OBBYEFMDDtN8tPSFrVtUWcpc0mbtsge9UMIHCBgNVHSMEgbow\
                ngbeAFMDDtN8tPSFrVtUWcpc0mbtsge9UoYGTpIGQMIGNMQswCQYDVQQGEwJVUzERMA8GA1UECBMI\
                nQ29sb3JhZG8xDzANBgNVBAcTBkRlbnZlcjEiMCAGA1UEChMZRXhhbXBsZSBJZGVudGl0eSBQcm92\
                naWRlcjERMA8GA1UEAxMISm9obiBEb2UxIzAhBgkqhkiG9w0BCQEWFGFkbWluQGV4YW1wbGVJZHAu\
                nY29tggkA41n9KHyMlVowDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQBqagX/ZasSD0NP\
                nQnR3zDXAYJK87VO59mn21TLEYaKG9vcm+odQhc0XkwLR/PLMTv3GSV9dfC0F6QHogLpZe1W+oa7Q\
                n+7Utasnsgs4Kfp0s2jQaPnUJRpGKXFPyOJ17RkjJgubKcYnX+vYV13tBDq4cIIm68dqZZqzaXDau\n0Z3h2Q==",
                "status":"Active"
        }
]
```

Update a Customer Connection

Updates a connection between your service and a customer. Optional parameters will be updated only if they are included in the request.

Copyright © 2025 Ping Identity Corporation

```
POST https://admin.pingone.com/web-portal/rest/saas/idp/2.0/spManaged/<idpId>
```

Request Parameters

Parameter	Description
`applications` (optional)	An array of one or more unique application saasids. For example: `["6964005a-6270-4a88-9ddc-0e6a4e05e51d", "338821d7-dd17-469f-a3c1-8025a0112ebe"]` Updates connections to specified applications. If you don't include application values, updates connections to all applications with the specified `idpId`. If no connection with the specified `idpId` exists, returns an error message.
`multiplexed` (optional)	If `true`, changes the connection to multiplexed. If `false`, changes the connection to non-multiplexed.
`email`	The email address for the customer administrator.
`idpId`	A unique identifier for the customer. Will not return an error message, but will not update the idpId.
`entityId`	A unique string used to identify the customer to us.
`ssoEndpoint`	The endpoint at the customer to which we will send SAML AuthnRequests. **Note** The SSO binding is not configurable using the Customer Connection API. PingOne SSO for SaaS Apps will always send the AuthnRequest using the Redirect binding for connections created through the API.
`sloEndpoint` (optional)	The URL at the identity provider (IdP) to which PingOne sends SAML single logout (SLO) requests. If included and left blank (`"sloEndpoint":""`), clears the setting.
`sloResponseEndpoint` (optional)	The URL at the IdP to which PingOne sends SAML SLO responses. If included and left blank (`"sloResponseEndpoint":""`), clears the setting.
`sloBinding` (optional)	Determines which binding type PingOne uses to send SAML SLO requests. Valid values are `Redirect` or `POST`.

Copyright © 2025 Ping Identity Corporation

Parameter	Description
`signAuthnRequest` (optional)	If `true`, enables AuthnRequest signing. If `false`, defaults to disabled.
`signingCertificateData`	The public certificate for the customer's signing certificate. The customer IdP uses this certificate to sign SAML assertions to PingOne. PingOne sees this as the verification certificate.
`signingCertFingerprint` (optional)	The signing certificate fingerprint that PingOne uses to sign the AuthnRequest or SLO request to the customer IdP. You can find the fingerprint value by expanding the certificate details at **Setup > Certificates** For more information, see View certificate details.
`signingAlgorithm` (optional)	If specified, sets signing algorithm to specified value. Valid values are: • `RSA_SHA1` • `RSA_SHA256` • `RSA_SHA384` • `RSA_SHA512`

Response Parameters

None.

Status Codes Returned

Status Code	Description
`200 OK`	Success.
`400 Bad Request`	The request was invalid. An accompanying error message explains why.
`403 Forbidden`	The request was understood, but has been refused. An accompanying error message explains why.
`404 Not Found`	The requested URI is either invalid or the resource doesn't exist.

Copyright © 2025 Ping Identity Corporation

Example

```
   PUT https://admin.pingone.com/web-portal/rest/saas/idp/2.0/spManaged/exampleIdp.com
{
        "email": "admin@exampleIdp.com",
        "entityId": "example Identity Provider",
        "ssoEndpoint": "http://www.exampleIdp.com",
        "signingCertificateData": "MIIDkDCCAvmgAwIBAgIJAONZ/
Sh8jJVaMA0GCSqGSIb3DQEBBQUAMIGNMQswCQYDVQQGEwJVUzER\
                nMA8GA1UECBMIQ29sb3JhZG8xDzANBgNVBAcTBkRlbnZlcjEiMCAGA1UEChMZRXhhbXBsZSBJZGVu\
                ndGl0eSBQcm92aWRlcjERMA8GA1UEAxMISm9obiBEb2UxIzAhBgkqhkiG9w0BCQEWFGFkbWluQGV4\
                nYW1wbGVJZHAuY29tMB4XDTExMTAyNjIyNDA1MFoXDTIxMTAyMzIyNDA1MFowgY0xCzAJBgNVBAYT\
                nAlVTMREwDwYDVQQIEwhDb2xvcmFkbzEPMA0GA1UEBxMGRGVudmVyMSIwIAYDVQQKExlFeGFtcGxl\
                nIElkZW50aXR5IFByb3ZpZGVyMREwDwYDVQQDEwhKb2huIERvZTEjMCEGCSqGSIb3DQEJARYUYWRt\
                naW5AZXhhbXBsZUlkcC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMx6WsTrzwhi10De\
                nPvvTa/Ndle2+3ZLePGXE/0v1qmm8Pji8l0czcg8ner56KBgnt2gnJ5xGrN51zBjZi7Qg2cL3A5cQ\
                nErJdYNsc7Oedulmp6RnDInMX1sfn/kGc3L/zBdwrngQWv86vN3bawvtj5wYsc9OAG1+X1kQeDuyR\
                ne/NlAgMBAAGjgfUwgfIwHQYDVR0OBBYEFMDDtN8tPSFrVtUWcpc0mbtsge9UMIHCBgNVHSMEgbow\
                ngbeAFMDDtN8tPSFrVtUWcpc0mbtsge9UoYGTpIGQMIGNMQswCQYDVQQGEwJVUzERMA8GA1UECBMI\
                nQ29sb3JhZG8xDzANBgNVBAcTBkRlbnZlcjEiMCAGA1UEChMZRXhhbXBsZSBJZGVudGl0eSBQcm92\
                naWRlcjERMA8GA1UEAxMISm9obiBEb2UxIzAhBgkqhkiG9w0BCQEWFGFkbWluQGV4YW1wbGVJZHAu\
                nY29tggkA41n9KHyMlVowDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQBqagX/ZasSD0NP\
                nQnR3zDXAYJK87VO59mn21TLEYaKG9vcm+odQhc0XkwLR/PLMTv3GSV9dfC0F6QHogLpZe1W+oa7Q\
                n+7Utasnsgs4Kfp0s2jQaPnUJRpGKXFPyOJ17RkjJgubKcYnX+vYV13tBDq4cIIm68dqZZqzaXDau\n0Z3h2Q==",
}
```

Disable a Customer Connection

Disables the customer connection and single sign-on (SSO) access.

```
   POST https://admin.pingone.com/web-portal/rest/saas/idp/2.0/spManaged/disable/<idpId>
```

Request Parameters

Parameter	Description
`application` (optional)	If you include specific saasid, changes only that connection. If you don't include application values, changes connections to all applications with the specified idpId.

Response Parameters

None.

Status Codes Returned

Status Code	Description
`200 OK`	Success.

Copyright © 2025 Ping Identity Corporation

Status Code	Description
`304 Not Modified`	The resource hasn't been modified. There was no new data to return.
`403 Forbidden`	The request was understood, but has been refused. An accompanying error message explains why.
`404 Not Found`	The requested URI is either invalid or the resource doesn't exist.

Example

```
POST https://admin.pingone.com/web-portal/rest/saas/idp/2.0/spManaged/disable/exampleIdp.com
```

Enable a Customer Connection

Enables the customer connection and SSO access.

```
POST https://admin.pingone.com/web-portal/rest/saas/idp/2.0/spManaged/enable/<idpId>
```

Request Parameters

Parameter	Description
`application` (optional)	If you include specific saasid, changes only that connection. If you don't include application values, changes connections to all enabled applications with the specified idpId.

Response Parameters

None.

Status Codes Returned

Status Code	Description
`200 OK`	Success.
`304 Not Modified`	The resource hasn't been modified. There was no new data to return.
`403 Forbidden`	The request was understood, but has been refused. An accompanying error message explains why.
`404 Not Found`	The requested URI is either invalid or the resource doesn't exist.

Copyright © 2025 Ping Identity Corporation

Example

```
POST https://admin.pingone.com/web-portal/rest/saas/idp/2.0/spManaged/enable/exampleIdp.com
```

Delete a Customer Connection

Deletes all connections for an idpId.

```
DELETE https://admin.pingone.com/web-portal/rest/saas/idp/2.0/spManaged/<idpid>
```

Request Parameters

Parameter	Description
`application` (optional)	If you include specific saasid, deletes only that connection. If you don't include application values, deletes all connections with the specified idpId.

Response Parameters

None.

Status Codes Returned

Status Code	Description
`200 OK`	Connections have been deleted.
`404 Not Found`	Connections not found for the specified idpid and saasid.

Example

```
DELETE https://admin.pingone.com/web-portal/rest/saas/idp/2.0/spManaged/exampleIdp.com
```

About multiplexing

PingOne SSO for SaaS Apps supports two kinds of multiplexing: application multiplexing and connection multiplexing.

Application multiplexing

A multiplexed application has a single connection to PingOne SSO for SaaS Apps. This allows you to share an application configuration across all identity providers (IdPs) connected to the application. For example, if you have one customer using PingFederate as an IdP, and another customer using Active Directory, they can both connect to a multiplexed application without any additional configuration.

Copyright © 2025 Ping Identity Corporation

PingOne SSO for SaaS Apps uses the entity ID value `PingConnect` to send SAML assertions to multiplexed applications. For non-multiplexed applications, PingOne uses the entity ID of the IdP.

With a non-multiplexed application, you configure a connection for each individual customer, often with different ACS URLS and entity IDs for each individual IdP.

> **Note**
>
> Only SAML applications can be non-multiplexed. OIDC and REST applications are always multiplexed.

Application multiplexing simplifies administration by allowing you to apply an application configuration to all customers and IdPs instead of administering each instance of the application separately. For example, exchanging metadata or updating certificates applies the change to all IdPs connected to the multiplexed application.

> **Note**
>
> Manual connections to non-multiplexed applications are not supported. You can only create connections to non-multiplexed applications through invited or managed PingOne for Enterprise accounts.

Connection multiplexing

A multiplexed connection is a single connection from an IdP to PingOne SSO for SaaS Apps. Multiplexing allows the IdP to access all of your customer's applications using a shared attribute contract, the same certificates, and a single entity ID, `PingConnect`.

A non-multiplexed connection is application-specific. The IdP configures a connection for each application using different attribute contracts and application-specific entity ID values.

> **Note**
>
> IdP connections through a PingOne for Enterprise account are always multiplexed.

Without multiplexing, PingOne SSO for SaaS Apps connections to your applications are separate, one-to-one connections to an IdP. Each application is assigned a separate entity ID value for its connection. If your account has an existing multiplexed connection for some IdPs, you can still create non-multiplexed connections for other IdPs.

Because the IdP only needs to maintain a single connection to PingOne SSO for SaaS Apps rather than maintaining a separate connection for each application, connection multiplexing simplifies administration.

> **Note**
>
> Manual connections can be either multiplexed or non-multiplexed.

Combining application and connection multiplexing

Multiplexing combination support

Connection type	Multiplexed application	Non-multiplexed application
Multiplexed connection	Supported	Supported

Copyright © 2025 Ping Identity Corporation

Connection type	Multiplexed application	Non-multiplexed application
Non-Multiplexed connection	Supported	Not supported **Note** Because non-multiplexed connections must be established manually, and it's not possible to create a manual connection to a non-multiplexed application, non-multiplexed connections to non-multiplexed applications are not supported.

PingOne SSO for SaaS Apps security best practices

Keep your applications and customer connections secure with the following tips and tools.

SAML applications

Configure the single logout (SLO) endpoints for your SAML-enabled applications so that user sessions can be closed and cleaned up in a timely manner. If your application doesn't support SLO, PingOne SSO for SaaS Apps won't notify the application when a user session ends.

For instructions on configuring SLO endpoints, see PingOne for Enterprise and SLO.

Non-SAML applications

`appurl` *parameter*

Disable the `appurl` parameter or tighten its validation. The purpose of the `appurl` parameter is to provide a way to override the default application URL.

If your application has only one entry point, leave the **Hostname or Domain** field empty, which will disable the `appurl` parameter.

If you must use `appurl`, a hostname such as `app.example.com` can provide stricter validation than `example.com`.

Binding type

When you create a new application, you must choose between **Post** or **Redirect** bindings for sending tokens to the application. Post is the default and more secure option because it doesn't expose the token as a query parameter in the URL.

HTTPS

Use HTTPS for the **Default Application URL** and **Error URL**. Although HTTP is permitted, HTTPS improves data security in transit.

For more information about configuring non-SAML applications, see Add or update other applications.

Copyright © 2025 Ping Identity Corporation

Application integration

Processing the PingOne token exchange is the key step in integrating your application with PingOne SSO for SaaS Apps. Based on the user attributes returned from the token exchange, applications need to perform two important validations before accepting a token:

1. Does the `pingone.saas.id` value match the application's SaaS ID value?

   Matching the `pingone.saas.id` to the application's SaaS ID value prevents attackers from using tokens issued for other applications to access your application.

2. Is the `pingone.idp.id` value used to qualify the `pingone.subject` parameter?

   Identifying a user with a combination of the `pingone.idp.id` and `pingone.subject` parameters prevents other identity providers (IdPs) from using identifiers that resemble credentials from your intended IdP.

For more information, see Process the PingOne SSO for SaaS Apps token exchange.

What is an idpId?

Learn about the `idpId` parameter and how it's used in PingOne SSO for SaaS Apps.

The `idpId` parameter is a unique value that identifies a customer organization to your software as a service (SaaS) application.

The `idpId` represents a unique identity provider (IdP) configuration for a given customer. The same IdP configuration is applied across all connections that share an `idpId` within your PingOne SSO for SaaS Apps account.

Once set, the `idpId` value can't be changed. You can change the configuration that is used by the `idpId`, which will update all connections using that `idpId`.

> **Tip**
>
> If your IdP partner has separate environments for testing and production, create a different `idpId` configuration for each.
> If your IdP partner has only one environment, but you want separate application connections for test and production, create test and production versions of your application, and use the same `idpId` configuration for both.

The `idpId` parameter is used in three application workflows:

- When you add a connection, you are required to provide an `idpId`.

  For more information, see:

  - Create a connection using the SSO self-service widget
  - Creating an invited SSO connection
  - PingOne SSO for SaaS Apps Customer Connection API
  - Creating a manual SAML connection

- When you redirect users from your application to PingOne for Enterprise to initiate single sign-on (SSO), you must tell PingOne for Enterprise which `idpId` to use.

  For more information, see Redirect users to PingOne SSO for SaaS Apps (SP-initiated SSO).

Copyright © 2025 Ping Identity Corporation

- When the user returns to your application with either a token or a SAML assertion, PingOne SSO for SaaS Apps includes the `idpId` in the user data for you to use in creating a user session.

  For more information, see Process the PingOne SSO for SaaS Apps token exchange.

Most applications should use the domain name as an `idpId` value because it's a common way of uniquely identifying a domain of users.

However, if your application doesn't include a domain name, can't guarantee the domain name's uniqueness, or if you already have a scheme for identifying an organization in your application (for example, by company name or UUID), you can assign any value. The `idpId` is ultimately for your application to consume.

`idpId` is used during single sign-on (SSO) to identify which IdP connection/configuration to use. If the `idpId` is not specified, the user will be prompted to perform IdP discovery based on their email domain. For more information on configuring email domains for `idpId` discovery, see Edit an invited customer connection and Edit a managed customer connection.

For more information about finding an existing `idpId` value, see Finding the `idpId` value.

> **Note**
>
> The PingOne for Enterprise test identity provider will automatically be added to your application with a random GUID as the `idpId` . To find the test provider, go to **Customer Connections**, click **Narrow by**, and select **Test IdP**.

Copyright © 2025 Ping Identity Corporation

Invited PingOne for Enterprise SSO

Invited SSO allows PingOne SSO for SaaS Apps customers to delegate SSO configurations to their partners.

Partners can manage both IdP and SP sides of the connection themselves. Invited SSO also allows partners to connect to non-SAML IdPs using PingOne for Enterprise as a bridge.

> **Note**
>
> Invited SSO is a legacy function that has been improved on by PingOne SSO for SaaS Apps Managed Accounts. Managed Accounts lets you directly manage and monitor partner accounts, and also allows you to delegate management by assigning appropriate administrative roles. This gives your partners the ability to manage their own accounts, but also allows you to access a partner account for onboarding or troubleshooting.
> To learn more, see Manage partner accounts.

Getting started with Invited PingOne for Enterprise SSO

Follow this workflow to set up Invited PingOne single sign-on (SSO).

Steps

1. Familiarize yourself with how PingOne for Enterprise works.

   See PingOne for Enterprise and Federated SSO with PingOne for Enterprise for information.

2. Connect to an identity repository.

   You can configure an identity bridge to connect to an external identity repository or use the PingOne for Enterprise Directory as your identity repository. See Connecting to an identity repository for information.

3. Assign administrators.

   See Assign administrative roles for information.

4. Add user groups.

   See Managing users by group for information.

5. **Optional:** Manage your PingOne for Enterprise Directory users.

   If you're using PingOne for Enterprise Directory as your identity repository, see Managing PingOne for Enterprise Directory users for information and instructions.

6. Manage certificates for your account.

   See Certificate management for information.

Next steps

If you encounter problems as you configure PingOne for Enterprise, visit the Ping support portal to look for answers, or sign on to your account to file a support case.

Copyright © 2025 Ping Identity Corporation