PingCentral

June 3, 2025

PINGCENTRAL
Version: 2.3;latest

Table of Contents

PingCentral for Application Owners

PingCentral

PingCentral makes it possible for identity and access management (IAM) administrators to delegate common application configuration and deployment tasks to application owners, which saves time and streamlines processes.

1. Administrators set up users and define PingFederate and PingAccess development, test, and production environments.
2. Administrators create OAuth, OpenID Connect (OIDC), Security Assertion Markup Language (SAML), and PingAccess templates based on clients, connections, and application security configurations they think are worth replicating.
3. Application owners use these templates to apply security configurations to their applications and then promote them to the appropriate development environments to test them.

Using PingCentral does not require extensive training. However, for the best possible experience, learn how the platform works before getting started.

PingCentral for IAM Administrators

PingCentral for Application Owners

Release Notes

These release notes summarize the changes in current and previous PingCentral product updates. Updated December 20, 2024.

PingCentral 2.3 (April 2025)

FIPS-compliant mode now available

New PASS-7036

Administrators can now enable PingCentral to run in FIPS-compliant mode, which guarantees that all cryptographic algorithms and protocols meet the U.S. federal standard for security compliance.

To enable this option, access the `<PingCentral_install> /conf/application.properties` file and set the `pingcentral.fips.enabled` property value to `true`. Learn more in Configuring PingCentral to run in FIPS-compliant mode.

PingCentral is currently running FIPS 140-3. Learn more about this version in FIPS 140-3.

Spring Security upgrade

Improved PASS-7022

Spring Security has been upgraded from version 5.3.31 to 5.3.39 to prevent future false-positive scan alerts. You can find more information in CVE-2024-38816: Path traversal vulnerability in functional web frameworks in the Spring documentation.

d3-color upgrade

Improved PASS-7031

The d3-color package has been upgraded from version 1.4.1 to 3.1.0, where the security vulnerability was fixed.

Promotion approval requests enhanced

Improved PASS-7033

Those who approve promotions can now determine if a promotion approval request is for a new or existing application by viewing the newly added detail on the **Promotion Approvals** page. **Last Promoted** or **Last Updated** now displays next to the date and timestamp that indicates when the application was last promoted or updated.

Updated scripts

Improved PASS-7037

All PingCentral scripts have been updated to be DevOps-friendly.

JDK 21 support added

New PASS-7038

Support was added for Java Development Kit (JDK) 21.

PingCentral 2.2 (December 2024)

Trusted OGNL expression usability improvement

Improved PASS-7028

Previously, trusted OGNL expressions could only be assigned to applications one at a time. Now, a **Select All** checkbox is available to select all applications and assign the selected trusted OGNL expression to them.

Signing and encryption certificates can now be the same

Improved PASS-7029

Previously, PingCentral did not allow the signing and encryption certificate the same, which is allowed in PingFederate. When application owners tried to promote and upload the same certificate and use it for both the signing and encryption certificate, users received validation errors. Now, the same certificates can be used in PingCentral.

Spring Security upgrade

Improved PASS-7019

Spring Security has been upgraded from version 5.7.11 to prevent future false-positive scan alerts. Learn more about this upgrade in CVE-2024-22257: Possible Broken Access Control in Spring Security With Direct Use of AuthenticatedVoter in the Spring documentation.

CVE issues fixed

Fixed PASS-7020

A number of third-party libraries have been updated to address Common Vulnerabilities and Exposures (CVEs) reported in these libraries. These CVEs were not exploitable, but they were updated to avoid unnecessary concerns.

Upgrade issues fixed

Fixed PASS-7023

Previously, when upgrading from PingCentral 2.0.2 to 2.1.0, users received a warning message regarding their APIs. This issue has been resolved, and this message no longer displays when the upgrade is performed.

SAML application deletion issue resolved

Fixed PASS-7026

Previously, when users tried to delete SAML applications, either through the PingCentral UI or API, and they selected the **Delete from PingFederate in all environments** option, the application was not deleted in PingFederate. This issue has been resolved and now works as expected.

PingCentral and PingFederate application sync issue resolved

Fixed PASS-7027

Previously, when syncing a PingCentral application with a server-side PingFederate application, data within the **advancedEditPromotionJson** field was being deleted. This issue has been resolved, and the data within that field is now preserved.

PingCentral 2.1 (June 2024)

More control over client secrets

New PASS-6911

Application owners now have more control over which client secrets are used when promoting OAuth and OIDC applications from PingCentral to PingFederate. If the application is configured to use a client secret for authentication, and the environment to which the application is being promoted requires that a random secret be used, users can choose to either generate a new client secret or retain the existing client secret. See Promoting OAuth and OIDC applications for details.

mTLS is now supported

New PASS-6915

Mutual TLS (mTLS) can now be used for admin API authentication from PingCentral to PingFederate. To set up this connection, access the new **Client TLS Key Pair** page, import the key pair that you want to use for authentication, and configure the environment to use the client certificate you specify. The **TLS Key Pair** page has also been renamed to **Server TLS Key Pair** to clearly differentiate between them. See Configuring MTLS for details.

Rocky Linux is now supported

New PASS-6918

Rocky Linux version 9.3 and later is now a supported enterprise operating system.

New email parameter added to all user accounts

New PASS-6967

The email parameter has been added to all PingCentral user accounts, which will let you extract users' email addresses and notify them about important events, such as upgrades, and maintenance windows. The **Email Address** field now displays on the **Add** and **Edit User** pages, an email property has been added to the API, and for SSO configurations, PingCentral will derive the user's email from the email claim defined by the email scope.

Performance improvements

Improved PASS-6904 and PASS-6910

If you have many different applications in many different environments, or if you have many groups using SSO to access PingCentral, you will notice that PingCentral's performance has been greatly improved with this release. Now, when you filter your applications, you will only see managed applications (created from or promoted to PingCentral environments) by default, which improves page loading speeds. The application owner search functionality has also been improved, which makes it faster and easier to configure owners for applications.

Application owners limited to whom they can assign as owners

Improved PASS-6913

Previously, when application owners used SSO to sign on to PingCentral and group memberships were also supplied, application owners could select any group as an owner of their application, which gave all group members the ability to manage it. Now, application owners can only select a group as an owner if the application owner is a member of the group.

Certificates management usability improvement

Improved PASS-6917

When promoting SAML applications, the names of the signing certificates available now include the valid date range, which makes it easier to discern between certificates.

Application owners list is now easier to navigate

Fixed PASS-2114

Previously, all application owners were listed on the application **Summary** tab, regardless of the number of owners. If an application had a large number of owners, the list would be long and difficult to read. Now, if the list is large, **Show More** and **Show Less** buttons are available to help you navigate the list.

Change Template button fixed

Fixed PASS-6941

Previously, when importing metadata for a SAML application, the **Change Template** button would disappear. This issue has been fixed, and the **Change Template** button continually displays as expected.

JSON editor promotion issues resolved

Fixed PASS-6966

Previously, under certain circumstances, server errors were encountered when JSON-based promotions occurred. This issue has been resolved.

Keystore password issues resolved

Fixed PASS-6970

Previously, when configuring an environment and uploading a signing certificate, if an existing keystore file (*.p12) was selected, the matching password provided could be too long for PingCentral to accept. This password limit has been increased.

Assertion encryption certificate issues resolved

Fixed PASS-6985

Previously, if an application was configured with an assertion encryption certificate, the certificate would disappear from the **Promote to Environment** modal when the application was being promoted, and users had to upload the certificate again. This issue has been resolved.

PingCentral 2.0.2 (April 2024)

Upgrade processes now work as expected

Fixed PASS-6905

Previously, if PingCentral had at least one (service provider) SP connection or one PingAccess template, upgrades from version 1.14 to 2.0 would fail. This issue has been resolved and upgrades now work as expected.

Expressions can now be added or updated in SAML applications

Fixed PASS-6906

Previously, if applications were created from SAML templates that contained at least 1 OGNL expression, the expressions could not be updated, nor could new expressions be added for attribute mapping. This issue has been resolved, and expressions can now be added and updated as needed.

SAML application templates can now be updated

Fixed PASS-6907

Previously, when administrators tried to change the templates associated with SAML applications, the change would not be saved. This issue has been resolved and SAML applications can now be updated with new templates.

Database errors no longer occur during upgrade

Fixed PASS-6940

Previously, if PingCentral had a SAML template with expressions or PingAccess templates, database errors would occur when upgrading from version 1.14 to 2.0. The issue has been resolved and upgrade processes now work as expected.

PingCentral 2.0.1 (January 2024)

Approval window now displays most recently promoted version

Fixed PASS-6865

Previously, when administrators reviewed application promotion requests and compared the submitted JSON to the most recently promoted version, the original version was displayed instead of the most recently promoted version. This issue has been resolved and the most recently promoted version now displays in the approval window.

Updated JSON for OIDC applications now displays in PingFederate after promotion

Fixed PASS-6900

Previously, if application owners updated the underlying application JSON in their OIDC applications, and administrator approval was required to promote them, the updated JSON was not reflected in PingFederate. This issue has been resolved and the updated JSON now displays in PingFederate as expected.

Application synchronization now works as expected for OIDC applications

Fixed PASS-6901

Previously, when OIDC applications were synchronized to the most up-to-date configurations available, they were saved as OAuth applications. This issue has been resolved, and the synchronization process now works as expected.

PingCentral 2.0 (December 2023)

New features and improvements in PingCentral 2.0.

Template synchronization now available for SAML and PingAccess applications

New PASS-6730

Administrators can now synchronize OAuth, OIDC, SAML, and PingAccess templates to ensure that their templates are based on the most up-to-date configurations available. Applications based on out-of-date templates have **Outdated Template** icons displayed next to them, which inform application owners that newer versions of the templates are available.

Administrators can also now revert SAML SP connections and PingAccess application templates to previous versions. See the **Reverting templates to previous versions** tab on the SAML 2.0 and PingAccess templates page for details.

Note that when you upgrade to PingCentral 2.0, SAML and PingAccess application templates will have base revisions created for them. OAuth and OIDC templates created prior to version 2.0 cannot be synced with the most recent configurations available. Recreate the template in version 2.0 to use the sync feature going forward.

Application owners can now edit application JSON themselves

New PASS-6670

To accommodate a wide variety of promotion needs, application owners can now edit the application JSON for their applications when they promote them.

Note that providing application owners with this ability can be risky, so it's highly recommended that approvals are enabled for the environment. Administrators can review the submitted application JSON and compare it to the original application JSON before approving the promotion request.

Also note that:

- This functionality is not yet available for PingAccess applications.
- Applications cannot be reverted to a promotion that uses JSON editing.
- Be aware that the JSON review window compares against the original application JSON and not the most recently promoted JSON.

Prevent application owners from deleting applications

New PASS-6731

To prevent application owners from accidentally deleting applications from PingFederate (and PingAccess, when applicable) environments, you can enable a new option that allows only administrators to delete applications from the environment.

Hide inactive promotion approvals

Improved PASS-6733

To help manage promotion approvals, both administrators and application owners can now hide promotion approvals that are in a **canceled**, **promoted**, or **rejected** status that display on the **Promotion Approvals** page. The **Visible** filter is is enabled by default.

Approval expressions drag and drop enhancement

Improved PASS-6732

Administrators can add multiple approval expressions for an environment, which are evaluated sequentially from top to bottom in an IF/ELSE chain. Now, administrators can change the order in which these expressions display in the list by dragging and dropping them into different locations within the list instead of copying and pasting them between fields.

Multi-APC connection synchronization

Issue PASS-6705

Previously, PingCentral was unable to handle a service provider (SP) connection with multiple Authentication Policy Contracts (APC) mapped within it. The PingCentral 1.14 release enables users to select from multiple mapped contracts when adding an application as a managed application or a template.

However, due to a known synchronization limitation, if you update an existing single APC SP connection already managed by PingCentral to include a second APC and subsequently synchronize the application, you won't find an option to specify your preferred APC.

To simplify your workflow and mitigate potential challenges, we recommend refraining from using synchronization to modify multi-APC connections. Instead, consider creating a new SP connection that aligns with your desired APC configuration. This approach grants you control over APC selection, ensuring a smoother and more efficient process.

Configure APC mappings for OIDC applications in PingFederate

Issue PASS-3613 PingFederate

PingCentral promotes access token mappings and authentication policy contracts (APCs) with OIDC applications, but the APC mappings that link the APCs to the access token managers are not currently promoted with them. If the APC mappings do not already exist in the target PingFederate environments, applications do not function as expected.

When new APCs are promoted in PingCentral, access token mapping referencing the APC is created, but persistent grant mapping is not established, so the configurations are invalid.

To resolve these issues, configure the APC mappings within PingFederate.

Promoting applications with authentication challenge policies

Issue PASS-4948 PingAccess

Customized authentication challenge responses, which support single-page applications, are available in PingAccess 6.2 or later. Applications with this type of policy can be added to PingCentral but cannot be promoted to another environment unless the authentication challenge policy, with the same UUID, also exists in the target environment.

SP certificates and assertion encryption certificates must be different

Issue PASS-5663 PingAccess

When promoting SAML applications, PingFederate does not allow you to use the same certificate as both a service provider (SP) certificate and an assertion encryption certificate. Instead of preventing the promotion to continue, you receive a message similar to the following:

```
Environment'staging':  {pingfed}. This certificate either has the same ID or the same content as the
certificate with index 0.
```

To continue the promotion, ensure that the SP certificate and the assertion encryption certificate are different.

Update truststore path if PingCentral fails to start

Issue PASS-5977

After upgrading to 1.8, 1.9, 1.10, or 1.11, PingCentral fails to start if `$\{pingcentral.home}` is used in the trust store path. To prevent this from happening, change the home path to be the absolute trust store path and delete the **Certificates** table in the database.

Cannot update or revert templates created in 1.2 or earlier

Issue PASS-6466

Templates created in 1.2 or earlier do not store the environment ID, so you cannot update their grant types, scopes, or policy contracts, nor can you revert them to previous versions.

PingCentral 1.14.1 (November 2023)

Enhancements and resolved issues in PingCentral 1.14.1.

Forbidden error when loading API documentation

Fixed PASS-6820

We fixed an error that prevented API documentation from loading when using OIDC single sign-on (SSO) with PingCentral.

PingCentral 1.14 (September 2023)

New features and improvements in PingCentral 1.14.

Disable environments when down for maintenance or offline

New PASS-6666 and PASS-6683

PingCentral administrators can now disable referenced PingFederate environments for any reason, such as PingFederate being unavailable due to maintenance tasks. Additionally, we added a new environment status bar that indicates if an environment is offline. In such cases, application owners will receive a notification indicating that the environment is disabled or offline rather than encountering a UI error. For more information, see step 1 of the Updating environments tab in Managing environments.

Import SAML Connection to PingCentral from PingFederate with attributes mapped to data source

New PASS-6667

All attributes defined in a SAML SP connection are now integrated into the PingCentral application. This enhancement eliminates a limitation and is expected to enhance usability significantly. For more information, see step 3 in Using SAML 2.0 templates.

Additional synchronization capabilities

New PASS-6696

We added the ability to effortlessly initiate an application synchronization in PingCentral. Now, when you make external modifications to an application configuration, you can seamlessly update the application information within PingCentral. This removes the need to manually update application information and introduces a more streamlined and efficient process. For more information, see step 2 in Updating applications.

Other improvements

New

- We also updated the following bundled components and third-party dependencies:
  - Apache Commons Text 1.10

H2 database migration when the installation path has any spaces

Fixed PASS-6591

We resolved an issue where H2 database migration fails during an upgrade if there are spaces in the installation path for the existing or new instance.

SSO inactivity sign off

Fixed PASS-6690

We fixed an issue where utilizing single sign-on (SSO) to access the PingCentral console incorrectly triggered a timeout based on an ID token's lifetime.

Multi-APC connection synchronization

Issue PASS-6705

Previously, PingCentral was unable to handle a service provider (SP) connection with multiple Authentication Policy Contracts (APC) mapped within it. The PingCentral 1.14 release enables users to select from multiple mapped contracts when adding an application as a managed application or a template.

However, due to a known synchronization limitation, if you update an existing single APC SP connection already managed by PingCentral to include a second APC and subsequently synchronize the application, you won't find an option to specify your preferred APC.

To simplify your workflow and mitigate potential challenges, we recommend refraining from using synchronization to modify multi-APC connections. Instead, consider creating a new SP connection that aligns with your desired APC configuration. This approach grants you control over APC selection, ensuring a smoother and more efficient process.

Configure APC mappings for OIDC applications in PingFederate

Issue PASS-3613 PingFederate

PingCentral promotes access token mappings and authentication policy contracts (APCs) with OIDC applications, but the APC mappings that link the APCs to the access token managers are not currently promoted with them. If the APC mappings do not already exist in the target PingFederate environments, applications do not function as expected.

When new APCs are promoted in PingCentral, access token mapping referencing the APC is created, but persistent grant mapping is not established, so the configurations are invalid.

To resolve these issues, configure the APC mappings within PingFederate.

Promoting applications with authentication challenge policies

Issue PASS-4948 PingAccess

Customized authentication challenge responses, which support single-page applications, are available in PingAccess 6.2 or later. Applications with this type of policy can be added to PingCentral but cannot be promoted to another environment unless the authentication challenge policy, with the same UUID, also exists in the target environment.

SP certificates and assertion encryption certificates must be different

Issue PASS-5663 PingAccess

When promoting SAML applications, PingFederate does not allow you to use the same certificate as both a service provider (SP) certificate and an assertion encryption certificate. Instead of preventing the promotion to continue, you receive a message similar to the following:

```
Environment'staging':  {pingfed}. This certificate either has the same ID or the same content as the
certificate with index 0.
```

To continue the promotion, ensure that the SP certificate and the assertion encryption certificate are different.

Update truststore path if PingCentral fails to start

Issue PASS-5977

After upgrading to 1.8, 1.9, 1.10, or 1.11, PingCentral fails to start if `$\{pingcentral.home}` is used in the trust store path. To prevent this from happening, change the home path to be the absolute trust store path and delete the **Certificates** table in the database.

Cannot update or revert templates created in 1.2 or earlier

Issue PASS-6466

Templates created in 1.2 or earlier do not store the environment ID, so you cannot update their grant types, scopes, or policy contracts, nor can you revert them to previous versions.

PingCentral 1.13

PingCentral 1.13 was skipped.

PingCentral 1.12 (June 2023)

New features and improvements in PingCentral 1.12.

Approval workflow

New PASS-6479

Previously, PingCentral did not allow an administrator to require approval for a non-administrator to promote an application to an environment. As of now, administrators can use Spring Expression Language (SpEL) based rules to trigger an approval requirement if an expression is or isn't met. Administrators will find a bell icon indicating active approval requests, and developers are informed when their requests are approved. For more information, see Managing approvals (administrators).

Client secret management enhancements

Improved PASS-6500

Administrators can now enforce a strong client secret for applications by requiring that PingCentral generate the client secret. With this feature enabled, when developers promote an application, they won't be able to create a client secret manually. This avoids the usage of weak client secrets. For more information, see Managing environments.

Multiple SLO Service URLs

New PASS-6609

When promoting SAML applications, developers can adjust and configure single logout (SLO) URLs. This adds flexibility and removes the need to manage multiple SAML applications only because different SLO URLs are required. For more information, see Promoting SAML applications.

JDK 17 support

New

We added support for Java Development Kit (JDK) 17.

SAML metadata export

Fixed PASS-5630

To set up a service provider (SP) connection, PingCentral now accepts SAML metadata files exported from other SP connections. These files are used to extract the following information: entity IDs, ACS URLs, SLO service URLs, certificates, and attributes.

Configure APC mappings for OIDC applications in PingFederate

Issue PASS-3613 PingFederate

PingCentral promotes access token mappings and authentication policy contracts (APCs) with OIDC applications, but the APC mappings that link the APCs to the access token managers are not currently promoted with them. If the APC mappings do not already exist in the target PingFederate environments, applications do not function as expected.

When new APCs are promoted in PingCentral, access token mapping referencing the APC is created, but persistent grant mapping is not established, so the configurations are invalid.

To resolve these issues, configure the APC mappings within PingFederate.

Promoting applications with authentication challenge policies

Issue PASS-4948 PingAccess

Customized authentication challenge responses, which support single-page applications, are available in PingAccess 6.2 or later. Applications with this type of policy can be added to PingCentral but cannot be promoted to another environment unless the authentication challenge policy, with the same UUID, also exists in the target environment.

SP certificates and assertion encryption certificates must be different

Issue PASS-5663 PingAccess

When promoting SAML applications, PingFederate does not allow you to use the same certificate as both a service provider (SP) certificate and an assertion encryption certificate. Instead of preventing the promotion to continue, you receive a message similar to the following:

```
Environment'staging':  {pingfed}. This certificate either has the same ID or the same content as the
certificate with index 0.
```

To continue the promotion, ensure that the SP certificate and the assertion encryption certificate are different.

Update truststore path if PingCentral fails to start

Issue PASS-5977

After upgrading to 1.8, 1.9, 1.10, or 1.11, PingCentral fails to start if `$\{pingcentral.home}` is used in the trust store path. To prevent this from happening, change the home path to be the absolute trust store path and delete the **Certificates** table in the database.

Cannot update or revert templates created in 1.2 or earlier

Issue PASS-6466

Templates created in 1.2 or earlier do not store the environment ID, so you cannot update their grant types, scopes, or policy contracts, nor can you revert them to previous versions.

PingCentral 1.11 (March 2023)

For the best possible experience, review these notes before using PingCentral 1.11.

Updated client secret generation to produce client secrets compatible with PingFederate

New

When creating a new client, PingCentral now generates OAuth client secrets compatible with PingFederate. For more information, see Promoting OAuth and OIDC applications.

Multiple ACS URLs

New

You can now configure multiple Assertion Consumer Service (ACS) URLs during SAML application creation. This new feature simplifies application development since the same application can use different URLs simultaneously. For more information, see Using SAML 2.0 templates.

Set application name

New

When promoting an application between environments, you can now configure an application name for OAuth and OpenID Connect (OIDC) clients, SAML connections, and PingAccess applications. For more information, see Promoting applications.

Deleting an application in PingCentral also deletes it in other environments

Improved

You can now choose to delete applications from PingFederate or PingAccess in addition to PingCentral. This feature is flexible because you can select which environments to delete the application from. For more information, see Managing applications.

Configure OAuth credentials for use instead of username and password to connect to PingFederate or PingAccess

Improved

Instead of using administrator credentials for basic authentication, you can now configure PingCentral to use OAuth client credentials to connect to PingFederate or PingAccess. PingCentral will request an `access_token` to use whenever it connects to PingFederate or PingAccess. For more information, see Configuring PingFederate and PingAccess for SSO.

Upgraded from v1 H2 database to v2

Security

Along with other dependencies (libraries), we've upgraded the H2 database from v1 to v2. For more information, see Upgrading PingCentral.

Configure APC mappings for OIDC applications in PingFederate

Issue | PASS-3613 | PingFederate

PingCentral promotes access token mappings and authentication policy contracts (APCs) with OIDC applications, but the APC mappings that link the APCs to the access token managers are not currently promoted with them. If the APC mappings do not already exist in the target PingFederate environments, applications do not function as expected.

When new APCs are promoted in PingCentral, access token mapping referencing the APC is created, but persistent grant mapping is not established, so the configurations are invalid.

To resolve these issues, configure the APC mappings within PingFederate.

Promoting applications with authentication challenge policies

Issue | PASS-4948 | PingAccess

Customized authentication challenge responses, which support single-page applications, are available in PingAccess 6.2 or later. Applications with this type of policy can be added to PingCentral but cannot be promoted to another environment unless the authentication challenge policy, with the same UUID, also exists in the target environment.

SP certificates and assertion encryption certificates must be different

Issue | PASS-5663 | PingAccess

When promoting SAML applications, PingFederate does not allow you to use the same certificate as both a service provider (SP) certificate and an assertion encryption certificate. Instead of preventing the promotion to continue, you receive a message similar to the following:

```
Environment'staging': PingFederate. This certificate either has the same ID or the same content as the certificate with index 0.
```

To continue the promotion, ensure that the SP certificate and the assertion encryption certificate are different.

Update truststore path if PingCentral fails to start

Issue | PASS-5977

After upgrading to 1.8, 1.9, 1.10, or 1.11, PingCentral fails to start if `$\{pingcentral.home}` is used in the trust store path. To prevent this from happening, change the home path to be the absolute trust store path and delete the **Certificates** table in the database.

Cannot update or revert templates created in 1.2 or earlier

Issue | PASS-6466

Templates created in 1.2 or earlier do not store the environment ID, so you cannot update their grant types, scopes, or policy contracts, nor can you revert them to previous versions.

Cannot migrate the H2 database if the installation path has any spaces

Issue PASS-6591

If the installation path has any spaces in the existing or new instance, the H2 database is not migrated during upgrade. Upon removing the spaces from the file path, the migration is successful.

PingCentral 1.10 (June 2022)

For the best possible experience, review these notes before using PingCentral 1.10.

Update OAuth and OIDC template grant types, scopes, and policy contracts and revert to previous versions

New PASS-2017

If you are an administrator, you can now update the grant types, scopes, and policy contracts in OAuth and OpenID Connect (OIDC) templates to further customize them to meet your needs.The history of these templates is also available to review and compare with previous versions. You can see which administrator modified the template configuration or policy contract, when it was modified, and details regarding these modifications. You can also revert templates to previous versions, if necessary. See OAuth and OIDC templates for details.

Update applications with the latest template version available

New PASS-6007

If an application is based on an outdated template, an **Outdated Template** icon now displays next to its name in the applications list. Edit the template and click the **Update Template** button. See Updating applications for details.

Use SSO to access PingFederate and PingAccess from PingCentral

New PASS-5202 and PASS-6018

You can now use SSO to access PingFederate and PingAccess from PingCentral. For details, see Configuring PingFederate and PingAccess for SSO.

Account lockout mechanisms added to mitigate password guessing

Improved PASS-6388

Account lockout mechanisms that prevent users from accessing the application or API after a specified number of failed sign-on attempts were added to this release. Specify the number of failed attempts that are allowed before users are locked out and the lockout period in the `application.yaml` file.

Cannot update or revert templates created in version 1.2 or earlier

Issue PASS-6466

Templates created in version 1.2 or earlier do not store the environment ID, so you cannot update their grant types, scopes, or policy contracts, nor can you revert them to previous versions.

Resolved a potential security vulnerability

Security PASS-6387 and PASS-6378

Resolved a potential security vulnerability that is described in security bulletin SECBL022 (requires sign-on).

Configure APC mappings for OIDC applications in PingFederate

Issue PASS-6316 PingFederate

PingCentralpromotes access token mappings and authentication policy contracts (APCs) with OIDC applications, but the APC mappings that link the APCs to the access token managers are not currently promoted with them. If the APC mappings do not already exist in the target PingFederate environments, applications do not function as expected.When new APCs are promoted in PingCentral, access token mapping referencing the APC is created, but persistent grant mapping is not established, so the configurations are invalid.To resolve these issues, configure the APC mappings within PingFederate.

SP certificates and assertion encryption certificates must be different

Issue PASS-5663 PingFederate

When promoting SAML applications, PingFederate does not allow you to use the same certificate as both a service provider (SP) certificate and an assertion encryption certificate. Instead of preventing the promotion to continue, you receive a message similar to the following: `Environment'staging': PingFederate. This certificate either has the same ID or the same content as the certificate with index 0.` To continue the promotion, ensure that the SP certificate and the assertion encryption certificate are different.

Promoting applications with authentication challenge policies

Issue PASS-4948 PingAccess

Customized authentication challenge responses, which support single-page applications, are available in PingAccess 6.2 or later. Applications with this type of policy can be added to PingCentral, but cannot be promoted to another environment unless the authentication challenge policy, with the same UUID, also exists in the target environment.

Update truststore path if PingCentral fails to start

Issue PASS-5977

After upgrading to 1.8, 1.9, or 1.10, PingCentral fails to start if `$\{pingcentral.home}` is used in the trust store path. To prevent this from happening, change the home path to be the absolute trust store path and delete the **Certificates** table in the database.

Adding SAML applications through the API

Issue | PASS-5009

If you attempt to add a SAML application to PingCentral from an existing application through the API, and the connection JSON contains identity attribute names and placeholders, you receive an error message advising you to nullify the **Names** field. However, even if you nullify this field, you still receive an error message because the JSON contains placeholders. Remove these placeholders before you proceed.

Managing environments through the API

Issue | PASS-5001 and PASS-5002

When creating, updating, or validating an environment through the API, you receive a server error message if the environment **Name** or **Password** fields are null or missing. API requests cannot be processed without this information, so ensure that these fields contain valid values.You will also receive a misleading error message if the **PingAccess Password** field is null. Rather than informing you that the information in this field is invalid, it informs you that you cannot connect to the PingFederateadministrative console, which is misleading.Requests to connect PingAccess to a PingCentral environment cannot be processed without this information, so ensure that this field contains a valid value.

Previous Releases

Release notes for previous releases are available here.

2022

- PingCentral 1.10 (June 2022)
- PingCentral 1.9.3 (Februrary 2022)

2021

- PingCentral 1.9.2 (December 2021)
- PingCentral 1.9.1 (December 2021)
- PingCentral 1.9 (October 2021)
- PingCentral 1.8.2 (December 2021)
- PingCentral 1.8.1 (December 2021)
- PingCentral 1.8 (June 2021)
- PingCentral 1.7 (March 2021)

2020

- PingCentral 1.6 (December 2020)

- PingCentral 1.5 (September 2020)
- PingCentral 1.4 (July 2020)
- PingCentral 1.3 (March 2020)

2019

- PingCentral 1.2 (November 2019)
- PingCentral 1.01 (October 2019)
- PingCentral 1.0 (August 2019)

PingCentral for IAM Administrators

Introduction to PingCentral

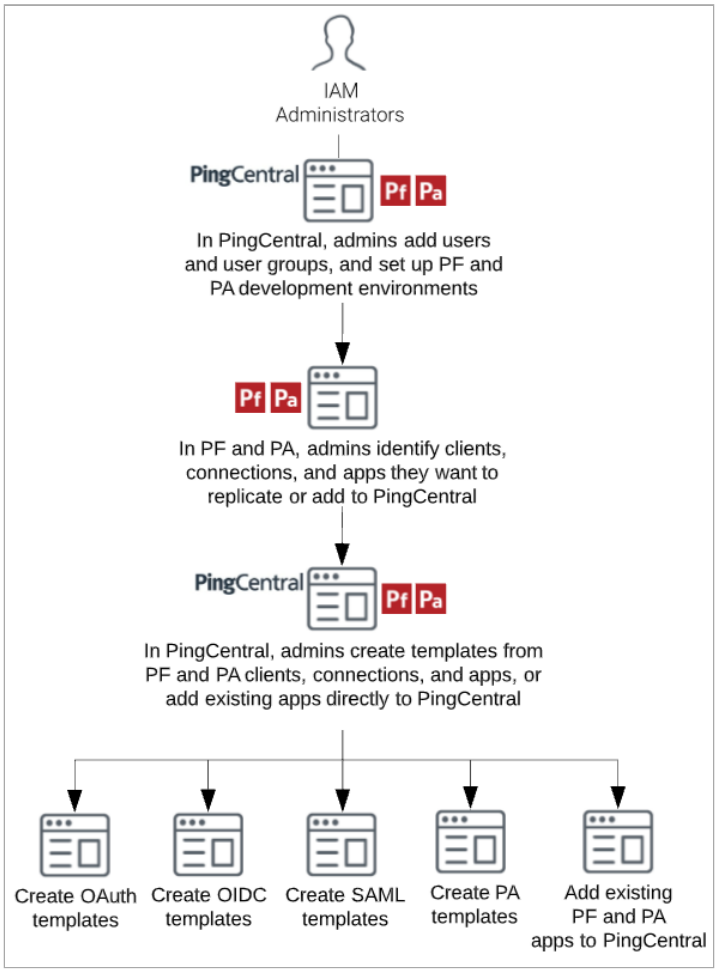
PingCentral allows you to delegate common application configuration and deployment tasks to application owners, streamlining processes and saving time.

PingCentral:

- Removes many tasks from your list of responsibilities, which lowers operational costs and reduces bottlenecks.
- Provides a central monitoring location for greater visibility into applications across deployment life cycles.
- Minimizes the risk of promoting applications with vulnerable security policies and makes it easier to standardize policies across the applications within your organization.

Using PingCentral does not require extensive training. However, for the best possible experience, review how the platform works before getting started.

- In PingCentral, you set up users and define PingFederate and PingAccess development, test, and production environments.
- In PingFederate and PingAccess, you locate clients, connections, and application security configurations worthy of replicating.
- In PingCentral, you create PingFederate OAuth, OpenID Connect (OIDC), Security Assertion Markup Language (SAML), and PingAccess application templates based on these clients, connections, and applications by using the template wizard, by saving them as templates, or by adding them directly to PingCentral.

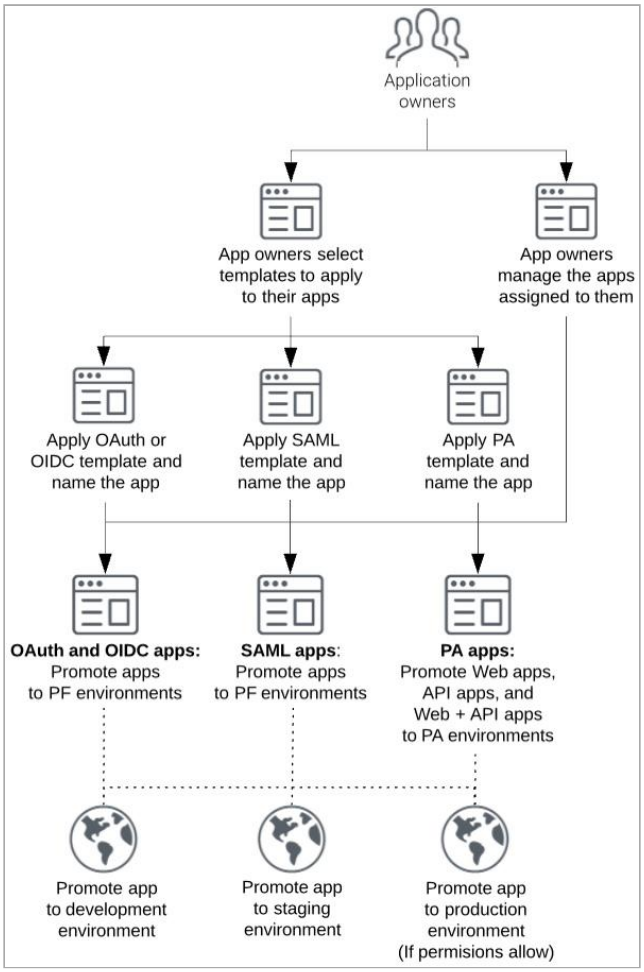


How PingCentral works

This flowchart illustrates the tasks that IAM Administrators perform when using PingCentral.

This flowchart illusrates the tasks that application owners perform when using PingCentral.

In PingCentral, application owners manage the applications assigned to them and use your templates to apply OAuth, OIDC, SAML SP, and PingAccess security configurations to them. A wizard guides them through the process of providing a name and description for each application they create as well as environment-specific information that makes it possible to run the application on the target environment.



For a deeper understanding of how PingAccess applications work, see PingAccess application deployments and configurations.

System requirements and supported configurations

For the best possible experience, ensure your computer meets or exceeds the minimum system requirements and become familiar with the configurations supported for this release.

PingFederate 10.3 and later.

PingAccess 5.3.2 and later.

Platforms:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Red Hat Enterprise Linux ES 8.0
- Red Hat Enterprise Linux ES 7.6
- Red Hat Enterprise Linux ES 9.0
- Rocky Linux 9.3

Browsers:

- Chrome
- Firefox

Databases:

- MySQL 5.7+
- PostgreSQL 11.5+
- RDS (MySQL)

> **Note**
>
> A demonstration-only, embedded H2 database is installed by default. Use the H2 database only for trial or training environments. It's not recommended to use the default H2 database in production. For testing and production environments, always use a secured external storage solution for proper functioning in a clustered environment.

Java runtime environments:

- JDK 21
- Oracle Java 11 LTS
- OpenJDK 11
- OpenJDK 17

Docker:

- Docker 23.0.1
- Docker 19.03.13. Base image operating system: Alpine Linux 3.11.
- Docker 18.09.0. Host operating system: Ubuntu 18.04 LTS, Kernal: 4.4.0-1052-aws 7.3.

> **Note**
>
> Ping Identity accepts no responsibility for the performance of any specific virtualization software and in no way guarantees the performance or interoperability of any virtualization software with its products.

Supported configurations

PingCentral is an orchestrator for PingFederate. Configurations are sourced from PingFederate to define PingCentral applications and templates. Configure each environment in advance and ensure you have authentication policies with persistent grants, access token mappings, and access token managers (ATMs) in place before using PingCentral to promote new applications.

Review additional information regarding supported features, protocols, and frameworks before you get started:

- General configurations
- OAuth and OIDC configurations
- SAML 2.0 SP configurations

- PingAccess configurations

General configurations

Configuration	Supported	Unsupported
Single sign-on and user management	• Directly managing users, which are stored in a PingCentral embedded database. • Signing on with SSO using an OpenID Connect token. • Optional feature: Group management, which allows the OIDC token used for SSO to include the group's claim. • Beta feature: Provisioning users and groups from an external store using API calls. **Note** If you want to provision users and groups of users through the API, you must disable the groups claim functionality by setting the `pingcentral.sso.oidc.groups-claim-enabled` property to `false` in the `application.properties` file.	
Entitlements	• Assigning one or more application owners that have already been provisioned. • Editing and promoting entitlements for an application. • After signing into PingCentral using SSO, administrators can assign groups of users as application owners, in addition to adding users one at a time. Group membership is based on the group's claim included in the OIDC token used for SSO.	Assigning groups of users entitlements based on an external attribute, such as LDAP group membership.

Configuration	Supported	Unsupported
Backup and restoration	Saving the database and configuration files by copying the directories `h2-data/` and `config/` to a new instance. **Caution** Use the H2 database only for trial or training environments. It is not recommended to use the default H2 database in production. For testing and production environments, always use a secured external storage solution for proper functioning in a clustered environment. Learn more about setting up an external database in Setting up MySQL. Testing involving H2 is not a valid test. In both testing and production, it might cause various problems due to its limitations, and PingCentral does not support H2-involved cases. **Note** To ensure these files contain the most up-to-date information, do not copy them while PingCentral is running.	Using an API to export PingCentral configuration information.

OAuth and OIDC configurations

Configuration	Supported	Unsupported
Client authentication		Using a client TLS certificate, private key JWT, or symmetric keys.
Grant types	Using all OAuth and OIDC grant types.	
Scopes	All scopes and exclusive scopes referenced in the PingFederate client JSON file, which is obtained during the template creation process.	

Configuration	Supported	Unsupported
ATMs and OIDC policies	Saving ATMs or OIDC policies into templates created from client applications that have them. **Note** If ATMs or OIDC policies do not exist in an environment, PingCentral will create them during the promotion process. If an ATM or OIDC policy of the same name already exists in a target environment, it will not be modified.	Saving or promoting access token mapping, persistent grants, policy contracts, or authentication policies.
Selectors		Connection set selectors. Clients can only be automatically connected to authentication policies through policy contracts. If your authentication logic requires use of a selector, add it in PingFederate.

SAML 2.0 SP configurations

Configuration	Supported	Unsupported
Bindings	Using POST bindings.	Using artifact, redirect, or SOAP bindings.
Profiles	• IdP-initiated SSO • SP-initiated SSO • IdP-initiated SLO • SP-initiated SLO	
Attribute mapping	• Mapping attributes, provided by a single authentication policy contract, in an unspecified format. You can also map attributes to static text. • Mapping attributes from data sources. • Using OGNL expressions as part of attribute mapping.	Any SAML SP connections with adapter mappings.

Configuration	Supported	Unsupported
Policy contracts	Referencing one policy contract per template.	Referencing more than one policy per template. **Note** If multiple policy contracts are referenced in a template when it is promoted, newly created applications will only map attributes from the first policy contract referenced. If PingFederate applications are directly added to PingCentral, the mappings from each policy contract are preserved.
Adapter mappings		Use authentication policy contract mappings instead of adapter mappings.
Certificate management	• Providing a public certificate for an SP connection. PingCentral creates a self-signed certificate with an expiration date of 1 year from today and configures it as the PingFederate IdP certificate. • Uploading a key pair to use as the IdP certificate for all SAML 2.0 connections promoted to an environment.	An SP certificate is required to promote a SAML 2.0 connection, but might be optional in future releases.

PingAccess configurations

Configuration	Supported	Unsupported
Destination	Both Agent and Site are supported.	The destination is not promoted with the application but selected per environment.
PingAccess application types	All application types (Web, API and Web+API) are supported.	The application type cannot be changed in PingCentral.
Token provider	PingFederate must be the token provider.	Third-party token providers for PingAccess are not supported.

Configuration	Supported	Unsupported
Application resources	Resources can be added and updated for each application.	You can configure resources in Web applications with specific HTTP methods in PingAccess version 6.2 or later, but this feature is not yet supported in PingCentral.
Resource ordering	Automated and manual resource ordering are both supported.	
Identity mappings	Identity mappings for all application types (Web, API and Web+API) are supported.	Identity mappings are not promoted with the application but selected per environment.
Virtual hosts	Virtual hosts are supported.	Virtual hosts are not promoted with the application but selected per environment.
Policy	Application and resource policies can be updated per application.	New rules and rule sets cannot be created in PingCentral. Virtual resources are available in PingAccess version 6.2 or later, but are not yet supported in PingCentral. Customized authentication challenge responses, which support single-page applications, are also available in PingAccess version 6.2 or later. Applications with this type of policy can be added to PingCentral, but cannot be promoted to another environment unless the authentication challenge policy also exists in the target environment.

Installing and configuring PingCentral

Installation, upgrade, and configuration instructions are accessible from the links on this page.

Installing PingCentral

- Using Docker to deploy PingCentral
- Installing PingCentral on Microsoft Windows
- Installing PingCentral on Linux systems
- PingCentral licensing
- Setting up MySQL
- Upgrading PingCentral

Configuring PingCentral

- Configuring PingCentral to run as a Windows service
- Configuring PingCentral to run as a Linux systemv service
- Configuring PingCentral to run as a Linux systemd service
- Configuring PingCentral to run in FIPS-compliant mode
- Configuring logging
- Removing the PingCentral Windows service
- Removing the PingCentral systemv service
- Removing the PingCentral systemd service
- Configuring PingFederate and PingAccess for SSO

To avoid seeing a certificate warning when you access PingCentral, replace the user-facing SSL certificate so it will no longer use the self-signed certificate. See Replacing the Admin Console SSL Certificate.

The Spring Boot Actuator, enabled by default, collects a wide variety of information to help you monitor and manage PingCentral in production environments. Spring Metrics collects a large amount of data, but it does not present the data in ways that are easy to understand, so you might want to move this data to either a Prometheus or Graphite time series database and use Grafana to view it through interactive dashboards with charts and graphs. See Monitoring PingCentral for details.

Using Docker to deploy PingCentral

Preconfigured Docker images of PingCentral are available in Docker containers on Docker Hub. Each container provides a complete working instance of an application that is available to use immediately after it is deployed.

Before you begin

Ensure that you have up-to-date tools and applications installed:

- Docker CE for Windows or Docker for macOS
- .docker.com/compose/install///[Docker Compose]
- Git

To ensure you are using appropriate versions of Docker, see System requirements and supported configurations.

Steps

1. When you are ready, deploy PingCentral by completing one of these tasks:
    - Register for the DevOps program to obtain a DevOps user name and key.
    - Use an existing product license. For instructions, see Use existing licenses.
2. Set up your server profile.

    For instructions, see the Deployment instructions on the PingIdentity DevOps site. The PingCentral Docker image is also available on this site.

Installing PingCentral on Microsoft Windows

PingCentral can be installed on Microsoft Windows Server 2016 or 2019. An installation script is not yet available, so download and extract the contents of the installation file to a suitable location within the host file system.

Before you begin

Ensure that:

- You are signed on to your system and have privileges that allow you to install applications.
- All System requirements and supported configurations are met, and the Oracle Java 11 LTS runtime environment is installed.
- The *<JAVA_HOME>* path points to the JDK software on your system. For example, `/usr/lib/jvm/java-11-openjdk-11.0.5.10-0.e17_7.x86_64`. To verify this information, run the **`echo $JAVA_HOME`** command.
- The JAVA `/bin` directory path is added to the *<PATH>* variable. To verify this information, run the **`$echo $PATH`** command.

Steps

1. Download the distribution `.zip` archive and extract its contents where you want the service run.
2. Go to `/<pingcentral_install>/bin/run.bat` and run **`run.bat`** from a command-line interface.

3. Open a web browser and go to `https://localhost:9022`.

> **Note**
>
> While you are running PingCentral locally, your browser might warn you that the application you're accessing doesn't have a signed certificate.

4. Sign on to PingCentral using the following credentials:
   - **Username**: Administrator
   - **Password**: 2FederateM0re!

   Without modification, PingCentral is secure by default.

   > **Note**
   >
   > If you're running PingCentral in FIPS-compliant mode, your password must contain at least 14 characters.

   Items worth mentioning:
   - If you add PingAccess environments to PingCentral, ensure that PingFederate is configured as the PingAccess token provider. See Configuring PingFederate as a PingAccess token for details.
   - If your application owners promote SAML applications to PingFederate or PingAccess environments, ensure that the appropriate trusted certificate authority (CA) certificates are available in PingCentral. You can find details in Adding trusted CA certificates to PingCentral for details.

5. Configure PingCentral to run as a Windows service, if appropriate.

   Learn more in Configuring PingCentral to run as a Windows service.

Installing PingCentral on Linux systems

To install PingCentral, download the latest version of the software and follow the on-screen instructions.

Before you begin

Ensure that:

- You are signed on to your system and have privileges that allow you to install applications. Run PingCentral as a non-root user.
- All System requirements and supported configurations are met, and the Oracle or OpenJDK Java 11 LTS runtime environment is installed.
- The *<JAVA_HOME>* path points to the JDK software on your system. For example, `/usr/lib/jvm/java-11-openjdk-11.0.5.10-0.e17_7.x86_64`. To verify this information, run the `echo $JAVA_HOME` command.
- The JAVA `/bin` directory path is added to the *<PATH>* variable. To verify this information, run the `echo $PATH` command.

Steps

1. Download the latest version of PingCentral from the Ping Identity website.

2. Extract the file into the appropriate target installation directory.
3. Start PingCentral by running `/<pingcentral_install>/bin/run.sh`.
4. When the installation is complete, open a browser window and enter the machine and PingCentral admin port in the URL field.

   Example:

   https://*<yourhost>*:9022.
5. Sign on to the application using the following credentials:
   - **Username**: Administrator
   - **Password**: 2FederateM0re!

   > **Note**
   >
   > If you're running PingCentral in FIPS-compliant mode, your password must contain at least 14 characters.
6. Configure PingCentral to run as a Linux systemv service or a Linux systemd service, as appropriate.

   Learn more in Configuring PingCentral to run as a Linux systemv service or Configuring PingCentral to run as a Linux systemd service.

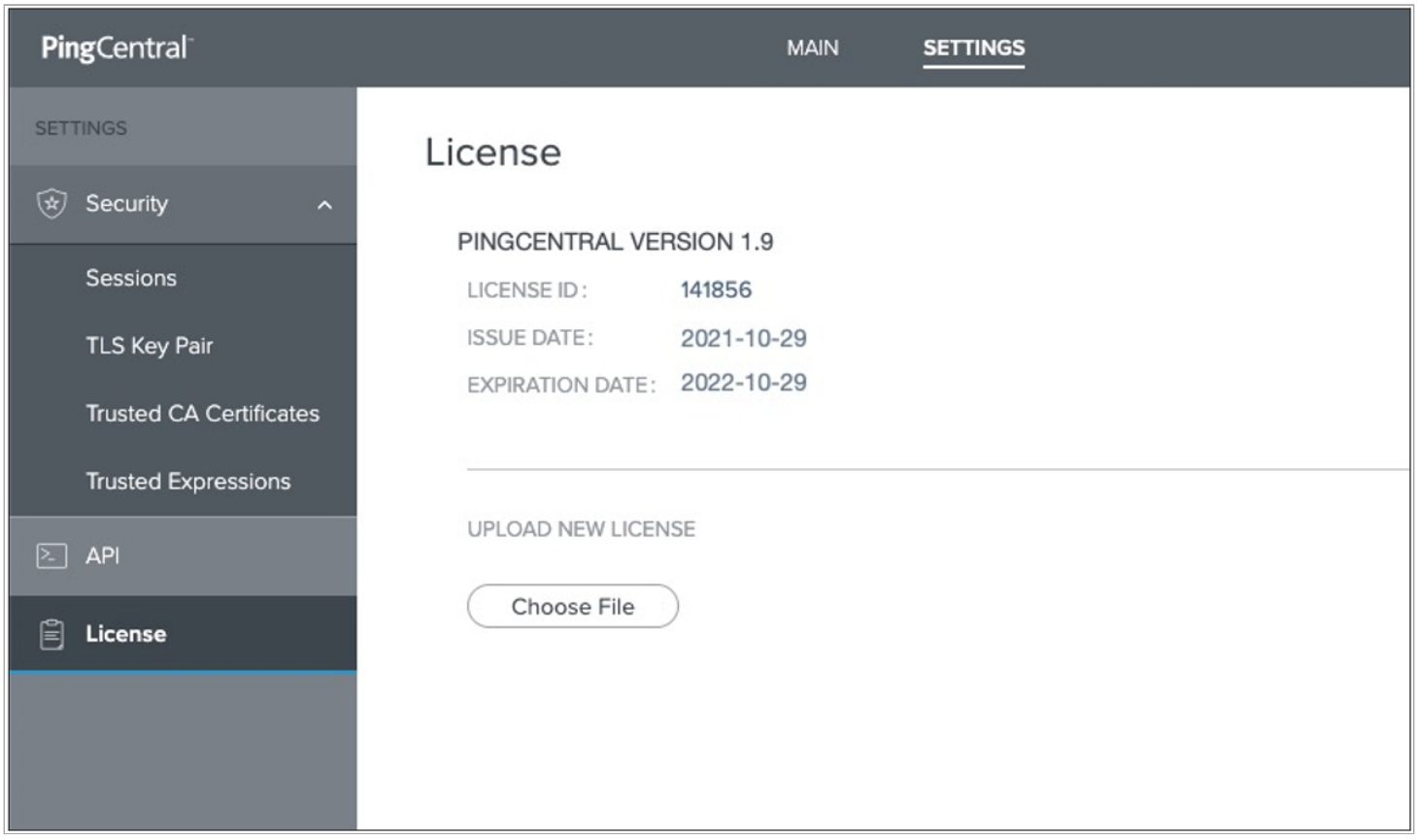
   Without modification, PingCentral is secure by default.

PingCentral licensing

Licensing ensures that you are authorized to use the application and provides information about your contract terms.

You need a valid PingCentral license to access the application. After installing PingCentral, you are prompted to log in, accept the license agreement, and upload your license.

To view license information, click **Settings** at the top of the page and then **License**. The product version number, license ID, issue date, and expiration date display on the License page, as shown in this example:



If you are an IAM Administrator and your license expires, you will be prompted to upload a new license.

Setting up MySQL

Install the MySQL connector and configure it to communicate with PingCentral.

About this task

PingCentral uses the Java-based H2 relational database management system by default, but you can also use MySQL. To set up MySQL, you must have the privileges required to access the `pingcentral` schema and configure the database.

> **Note**
>
> This topic doesn't provide instructions on setting up or maintaining the MySQL database.

> **Important**
>
> if you choose to migrate from the PingCentral H2 database to a MySQL database, you will lose all of your PingCentral data, including your environments, templates, environments, and promotion history information. Data residing in PingFederate, PingAccess, and other Ping products will not be affected.

Steps

1. Locate and download the appropriate MySQL connector.

For example, you can download the platform independent Java connector from https://www.mysql.com/downloads/connector/j/.

2. Place the MySQL connector in the following location: `/<pingcentral_install>/ext-lib/`.
3. Update the `/<pingcentral_install>/conf/application.properties` file to point to the new MySQL database:
    1. Update the datasource URL to your location.

        Example:

        ```
        spring.datasource.url=jdbc:mysql://${MYSQL_HOST:localhost}:3306/pingcentral?
        createDatabaseIfNotExist=true&useUnicode=true&useJDBCCompliantTimezoneShift=true&useLegacyDatetimeCode=f
        ```

    2. Update the user name and password, if necessary.

        Example:

        ```
        spring.datasource.username=DataSourceUsername
        spring.datasource.password=DataSourcePassword
        ```

    3. Update the driver class name, if necessary.

        Example:

        ```
        spring.datasource.driver-class-name=com.mysql.cj.jdbc.Driver
        ```

4. Restart PingCentral for the changes to take effect.

Upgrading PingCentral

You can upgrade from PingCentral 1.2 through 1.7 directly to 2.0. To begin the upgrade, download and extract the contents of the 2.0 distribution file and run the upgrade utility for Windows or Linux, as appropriate.

To learn how the upgrade works and which files are added and replaced during the process, see How the upgrade works.

For instructions on running the upgrade itself, see Upgrading to PingCentral 2.0.

> **Note**
>
> Starting with PingCentral 1.8, signing certificates are stored in the PingCentral database instead of a PingCentral-specific trust store. Certificates that exist in this trust store are imported to the PingCentral database during the upgrade process.

How the upgrade works

The upgrade utility uses the extracted contents of the `ping-central-2.0.0.zip` file to copy and replace the appropriate information in the existing version installation location.

Files that were not modified since they were initially installed are overwritten with new versions during the upgrade process.

Note the following:

- The database files (`h2-data` directory), the log files (`log` directory), the external library files (`ext-lib` directory), and the host key file (`conf/pingcentral.jwk`) remain intact during the upgrade process to preserve user data.

  > **Note**
  >
  > If you are using the H2 database, when upgrading from any version prior to PingCentral to 1.11, the upgrade script will generate a directory that contains the old H2 v1 database (`h2v1-data`). This file may be deleted after checking that the upgrade was successful in PingCentral.

  > **Caution**
  >
  > Use the H2 database only for trial or training environments. It is not recommended to use the default H2 database in production. For testing and production environments, always use a secured external storage solution for proper functioning in a clustered environment. For more information on setting up an external database, see Setting up MySQL.
  > Testing involving H2 is not a valid test. In both testing and production, it might cause various problems due to its limitations, and PingCentral does not support H2-involved cases.

- If the `application.properties` file was modified, the current version of the file is merged with the latest version, preserving customizations.

  > **Note**
  >
  > If you upgrade from any version prior to 1.10, use an H2 database, and still use the default password from your last installation, a new password will override it during this upgrade. However, if you updated the password from the original default, it is preserved in the `application.properties` file.

- If the `conf/log4j2.xml` , `bin/run.sh` , and `bin.run.bat` files were modified, the new versions are installed and the old versions are renamed. Manually update the new files with customizations as necessary.

The following list indicates which directories and files are replaced with new files during the upgrade process of PingCentral 2.0, provided that they were not modified since the initial installation.

- `ReadMeFirst.txt`
- `bin/obfuscate.bat`
- `bin/obfuscate.sh`
- `bin/run.bat`
- `bin/run.sh`
- `conf/application.properties`
- `conf/log4j2.xml`
- `bin/obfuscate.bat`
- `legal`
- `ping-central.jar`

- `sbin`
- `tools`

Upgrading to PingCentral 2.0

To upgrade PingCentral to 2.0, on either Windows or Linux, download the 2.0 installation file, run the PingCentral upgrade utility, and plan for a short period of downtime.

Before you begin

Ensure that:

- You are signed on to your system and have privileges that allow you to install applications.
- All System requirements and supported configurations are met, and the Oracle Java 11 LTS runtime environment is installed.
- The *<JAVA_HOME>* path points to the Java Development Kit software on your system. For example, `/usr/lib/jvm/java-11-openjdk-11.0.5.10-0.e17_7.x86_64`. To verify this information, run the **`echo $JAVA_HOME`** command.
- The JAVA `/bin` directory path is added to the *<PATH>* variable. To verify this information, run the **`echo $PATH`** command.

Steps

1. Download the `ping-central-2.0.0.zip` file and extract its contents.

   You can delete this file after the upgrade is complete.

2. If PingCentral is running, shut it down.

   This maintains the integrity of the H2 database file and ensures that you are running 2.0 as you complete the installation.

3. Make a copy of the existing PingCentral version product directory so that the older version can be restored if the upgrade process fails.

   If PingCentral has been configured to use an external database, such as MySQL, or PostgreSQL, make a copy of that database so that it can be restored if the upgrade process fails.

4. Go to the `<pingcentral_2.0.0_install>/upgrade` directory and run the appropriate file:

Option	Description
Windows	Run `bin\upgrade.bat "--existing=<PINGCENTRAL_HOME>"`
Linux	Run `bin/upgrade.sh --existing=<PINGCENTRAL_HOME>`

   Result:

   The upgrade process begins. The upgrade utility uses the extracted contents of the `ping-central-2.0.0.zip` file to copy and replace the appropriate information in the existing version location.

> **Note**
>
> When the upgrade is complete for this release, PingCentral 2.0 will run from the directory in which PingCentral was initially installed. For example, if PingCentral 1.4 was initially installed and you upgraded to 1.6, and now to 2.0, PingCentral 2.0 will run from the original 1.4 directory. The same is true if you upgraded directly from 1.4 to 2.0.

5. **Optional:** To update the license file (`conf/pingcentral.lic`), add `--license=<file>` at the end of the upgrade command and specify the path to the new license.

   Result:

   As the upgrade continues, a message displays that reminds you to shut down PingCentral if you have not already done so.

6. To continue, type `yes`.

   Result:

   A message displays that reminds you to back up your PingCentral program files.

7. To continue, type `yes`.

   Result:

   The upgrade continues and the system displays a message when the upgrade is complete.

> **Note**
>
> If PingCentral was installed as a service by one user, and the upgrade is performed by another user, the service will no longer start. To resolve this issue, run the following command to update the installation files to match the existing ownership:
>
> ```
> chown -R [user]:[group] [INSTALL_DIR]
> ```
>
> Where the user and group match the existing installation:
>
> ```
> chown -R pingcentral:pingcentral /usr/local/pingcentral-1-2.0.0/
> ```

8. Inspect the upgrade utility output for warnings regarding required manual merges.

> **Note**
>
> Other than the `application.properties` file, which is merged automatically, you must manually merge customizations you consider important. These customizations might include changes you made to the `conf/log4j2.xml` file, or changes you made to a file in the `/bin` directory.
> If you are upgrading from any version prior to 1.10, using an H2 database and were still using the default password from your last upgrade, you need to update the password in the `application.properties` file.

9. Start PingCentral 2.0.

Option	Description
Windows	Run `/<PINGCENTRAL_HOME>/bin/run.bat`.
Linux	Run `/<PINGCENTRAL_HOME>/bin/run.sh`, or by running the systemd service command, `systemctl pingcentral-# start`.

10. Sign on to PingCentral using the credentials you used to sign on to the previous version.

    There is no need to reconfigure PingCentral to run as a Windows or Linux systemv or systemd service after the upgrade.

11. Upon successful upgrade, delete the 2.0 distribution `.zip` file and the directory into which it was extracted.

> **Tip**
>
> After the upgrade, advise your users to refresh their browsers if they experience issues.

Configuring PingCentral to run as a Windows service

Run PingCentral as a Windows service that automatically starts when Windows starts.

Before you begin

Manually start the server to ensure that PingCentral is running as expected.

About this task

> **Note**
>
> You must have administrator privileges to configure PingCentral as a Windows service.

Steps

1. In the Windows **Search** field, enter `cmd` to access the command prompt.
2. Right-click **Command Prompt** and select **Run as administrator** in the menu.
3. In the command prompt, change directories to the `$PINGCENTRAL_HOME\sbin\windows` directory and run the `install-service.bat` script.
4. Open the Windows Control Panel. In the search field, enter `view local services`.
5. In the list of available services, right-click **PingCentral Service** , and select **Start**.

Result

The service starts immediately and restarts automatically when rebooted, by default.

Removing the PingCentral Windows service

If you have administrator privileges, you can remove the PingCentral Windows service.

Steps

1. In the Windows **Search** field, enter `cmd` to access the command prompt.
2. Right-click **Command Prompt** and select **Run as administrator** in the menu.
3. In the command prompt, change to the `<PINGCENTRAL_HOME>\sbin\windows` directory and run the `uninstall-service.bat` script.
4. After the script is finished running, remove the *<PINGCENTRAL_HOME>* environment variable from the system.

Configuring PingCentral to run as a Linux systemv service

Run PingCentral as a Linux systemv service that automatically starts when Linux starts.

Before you begin

Ensure that:

- You are signed on to your system as a root user.
- The *<JAVA_HOME>* `JAVA_HOME` path points to the Java Development Kit (JDK) software on your system. For example, `/usr/lib/jvm/java-11-openjdk-11.0.5.10-0.e17_7.x86_64`. To verify this information, run the **`echo $JAVA_HOME`** command.
- The `PINGCENTRAL_HOME` path points to the folder extracted from the `.zip` archive in your installation directory. Ensure that this path doesn't reside within a user's home folder.

Steps

1. Copy the `pingcentral` file from `<PINGCENTRAL_HOME>/sbin/linux/pingcentral` to `/etc/init.d`.
2. Create a new user to run PingCentral. You might want to create a new user account for each service you run as a way of keeping your services separate, or associate the account with a running process.
3. Create a new `pingcentral` folder in `/var/run/pingcentral` and ensure that the user who will run the service has read and write permissions to the folder.
4. Access the `pingcentral` file in the `/etc/init.d` folder and set values for the following variables at the beginning of the script:
    - `export <JAVA-HOME>`: Specify the name and location of the Java installation folder.
    - `export <PINGCENTRAL_HOME>`: Specify the name and location of the PingCentral installation folder.
    - (Optional): `export USER`: Specify the name of the user who will run the service, if applicable.
5. Register the service by running the **`chkconfig --add pingcentral`** command from the `/etc/init.d` folder.
6. Make the service script executable by running the **`chmod +x pingcentral`** command.

   After registering the service, you can control it by running the **`pingcentral`** command from the `/etc/init.d` folder with the following options:
    - **`start`**: Starts the PingCentral service.
    - **`stop`**: Stops the PingCentral service.

- `restart`: Restarts the PingCentral service.
- `status`: Displays the status of the PingCentral service and the service process ID.

Removing the PingCentral systemv service

If you have privileges that allow you to install applications, you can remove the PingCentral systemd service.

Steps

1. Sign on to the system as a root user.

Option	Description
Stop the service	Run the `systemctl stop pingcentral` command.
Disable the service	Run the `systemctl disable pingcentral` command.

2. Delete the `/etc/systemd/system/pingcentral.service` script if it is no longer needed.

Configuring PingCentral to run as a Linux systemd service

Run PingCentral as a Linux systemd service that automatically starts when Linux starts.

Before you begin

Ensure that:

- You are signed on to your system as a root user.
- The *<JAVA-HOME>* path points to the Java Development Kit (JDK) software on your system. For example, `usr/java/jdk11.0_4`.
- The *<PINGCENTRAL_HOME>* path points to the folder extracted from the `.zip` archive in your installation directory. Ensure that this path does not reside within a user's home folder.

Steps

1. Copy the `pingcentral.service` configuration file from `$PINGCENTRAL_HOME/sbin/linux/pingcentral.service` to `/lib/systemd/system/pingcentral.service`.

> **Note**
>
> You can also copy this file to the `/etc/systemd/system` location, if appropriate

2. Open the `pingcentral.service` file and assign appropriate values to the following variables:
   - *<PINGCENTRAL_HOME>*: Labeled "WorkingDirectory."
   - *<PINGCENTRAL_USER>*: Labeled "User."
   - *<JAVA_HOME>*: Labeled "Environment."

3. Enable read and write activity for the service using the `chmod 644 /lib/systemd/system/pingcentral.service` command.

   If you copied this file to the /etc/systemd/system location in step 1, use this command instead: `chmod 644 /etc/systemd/system/pingcentral.service`.

4. Load the systemd service using the `systemctl daemon-reload` command.
5. Enable the service using the `systemctl enable pingcentral.service` command.
6. Start the service using the `systemctl start pingcentral.service` command.

Removing the PingCentral systemd service

If you have privileges that allow you to install applications, you can remove the PingCentral systemv service.

Steps

1. Sign on to the system as a root user.

Option	Description
Stop the service	Run the `/etc/init.d/pingcentral stop` command.
Delete the service	Run the `chkconfig --del pingcentral` command.

2. Delete the `/etc/init.d/pingcentral` script if it is no longer needed.

Configuring PingFederate and PingAccess for SSO

To access PingFederate or PingAccess from PingCentral using single sign-on (SSO), each application must be correctly configured.

> **Note**
>
> You can configure PingFederate to use OAuth2 or a native sign-on to connect to PingCentral, but not both. You can configure PingAccess to use either native sign-on, OAuth2, or both.

Configuring PingFederate for SSO

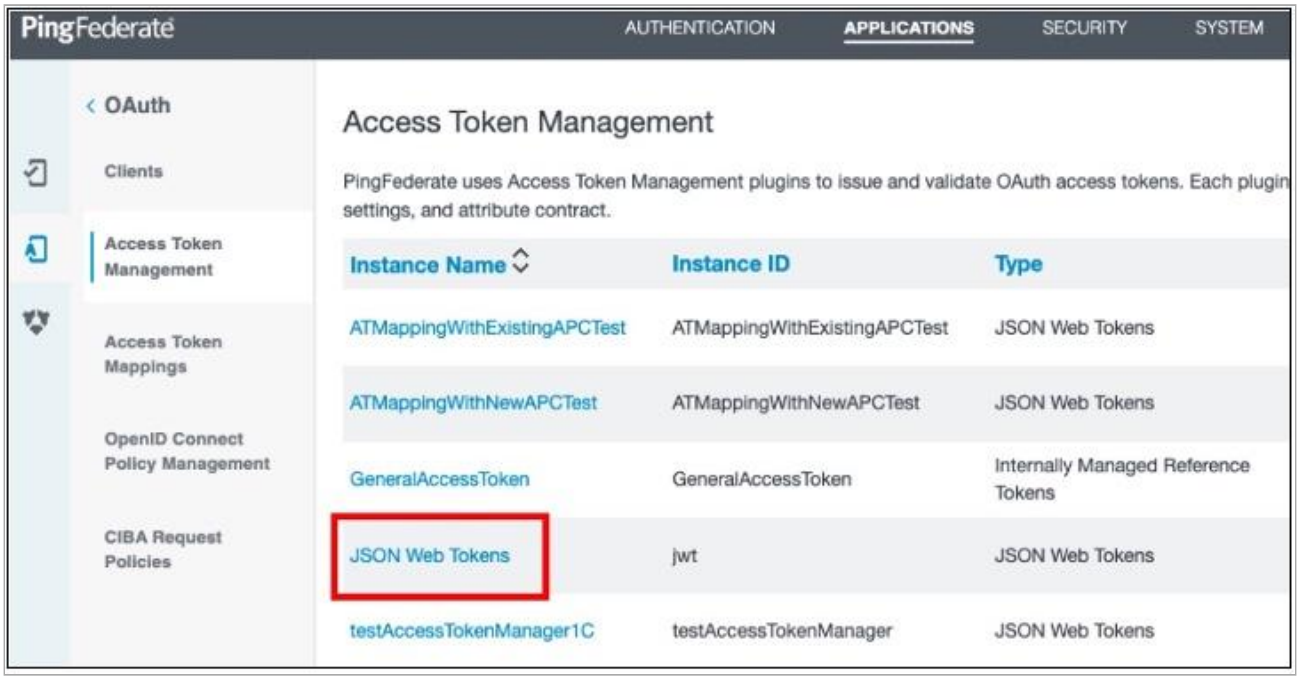
About this task

To access PingFederate from PingCentral using SSO:

Steps

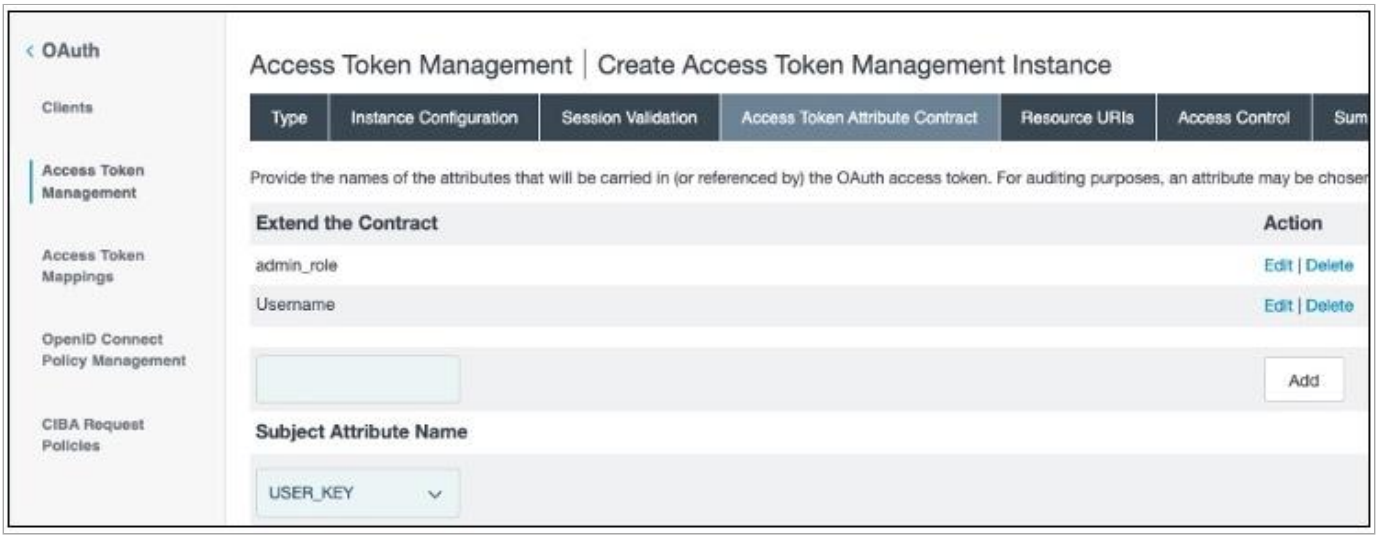
1. Review the PingFederate configurations:
   1. In PingFederate, go to **Applications → OAuth → Access Token Management** and ensure that JSON web tokens are configured, as shown in this example.

      See Configuring JSON-token management in the *PingFederate Server* guide for details.

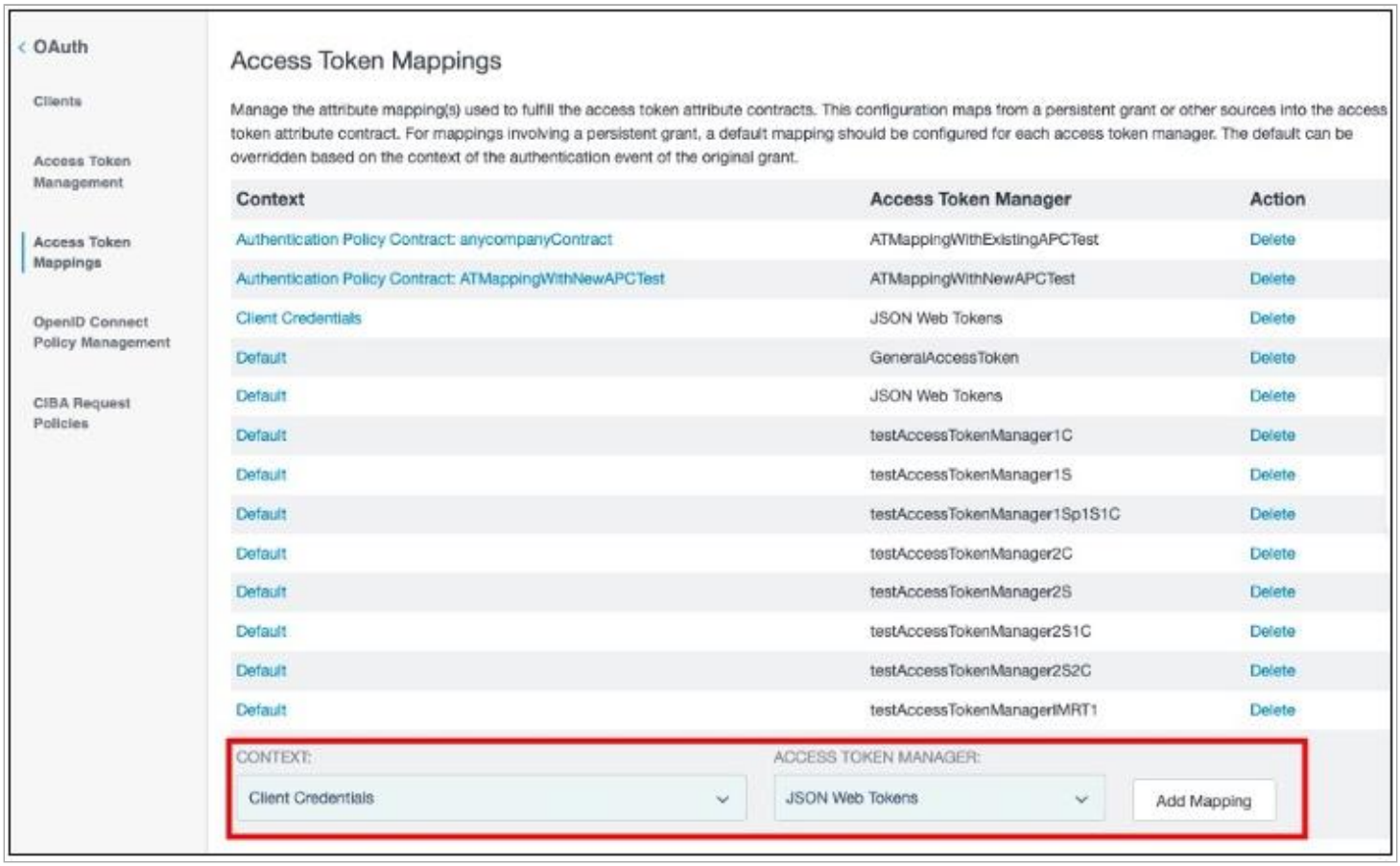


2. On the **Access Token Attribute Contract** tab, ensure that the access token attribute contract includes the following attributes, as listed here and shown in this example.
    - `admin_role`
    - `Username`

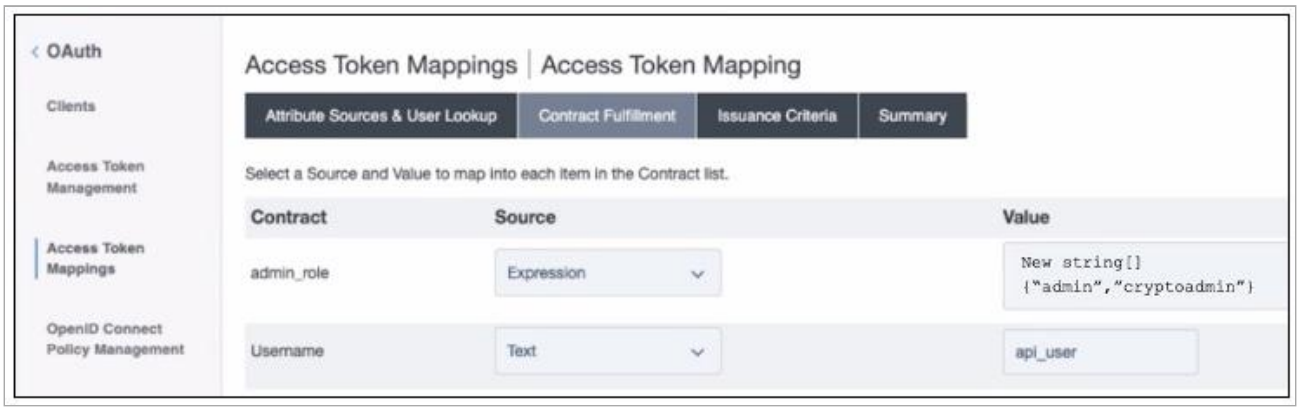
See Defining the access token attribute contract in the *PingFederate Server* guide for details.



1. Go to **Applications → OAuth → Access Token Mappings** and ensure that **Client Credentials** are mapped to use**JSON Web Tokens** as the access token manager, as shown in this example. Click **Add Mapping**.



1. On the **Contract Fulfillment** tab, ensure that the access token attributes in the contract are correctly mapped and the following attributes are included in the contract:
    - `Username` : The username of the administrator used to access APIs.
    - `admin_role` : This multi-valued attribute must include the `admin` and `cryptoadmin` roles. In this example, an OGNL expression is used to include these values.

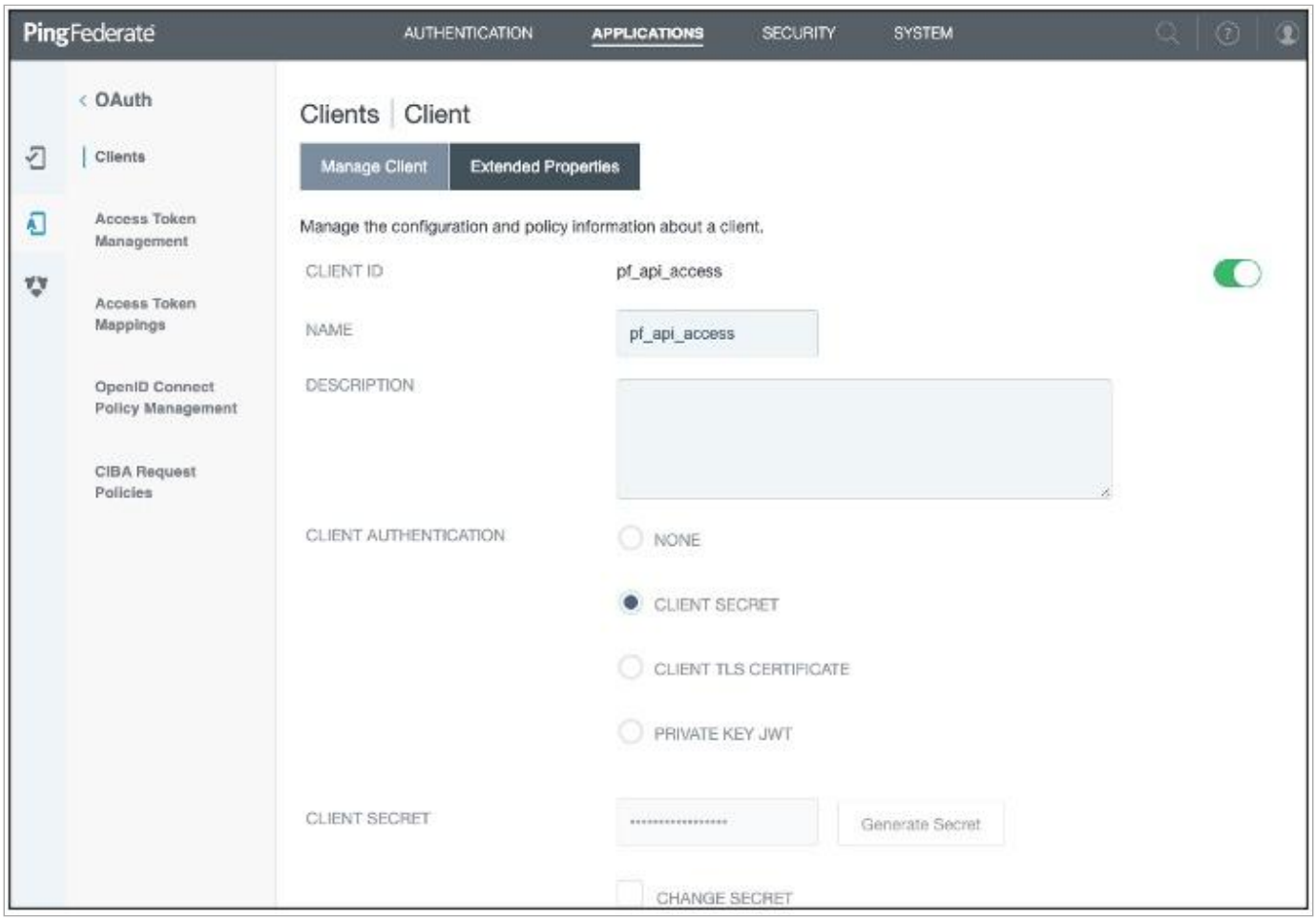


    1. Configure a new PingFederate client:

2. In PingFederate, go to **Applications → OAuth → Clients**.

3. On the **Manage Client** tab, complete these fields:
    - **Client ID**: Enter a unique identifier for the client.
    - **Name**: Enter a name for the client.
    - **Description**: Enter a description of the client.

    See Configuring OAuth clients in the *PingFederate Server* guide for details.



4. In the **Client Authentication** field, select **Client Secret**.
5. In the **Client Secret** field, you can:

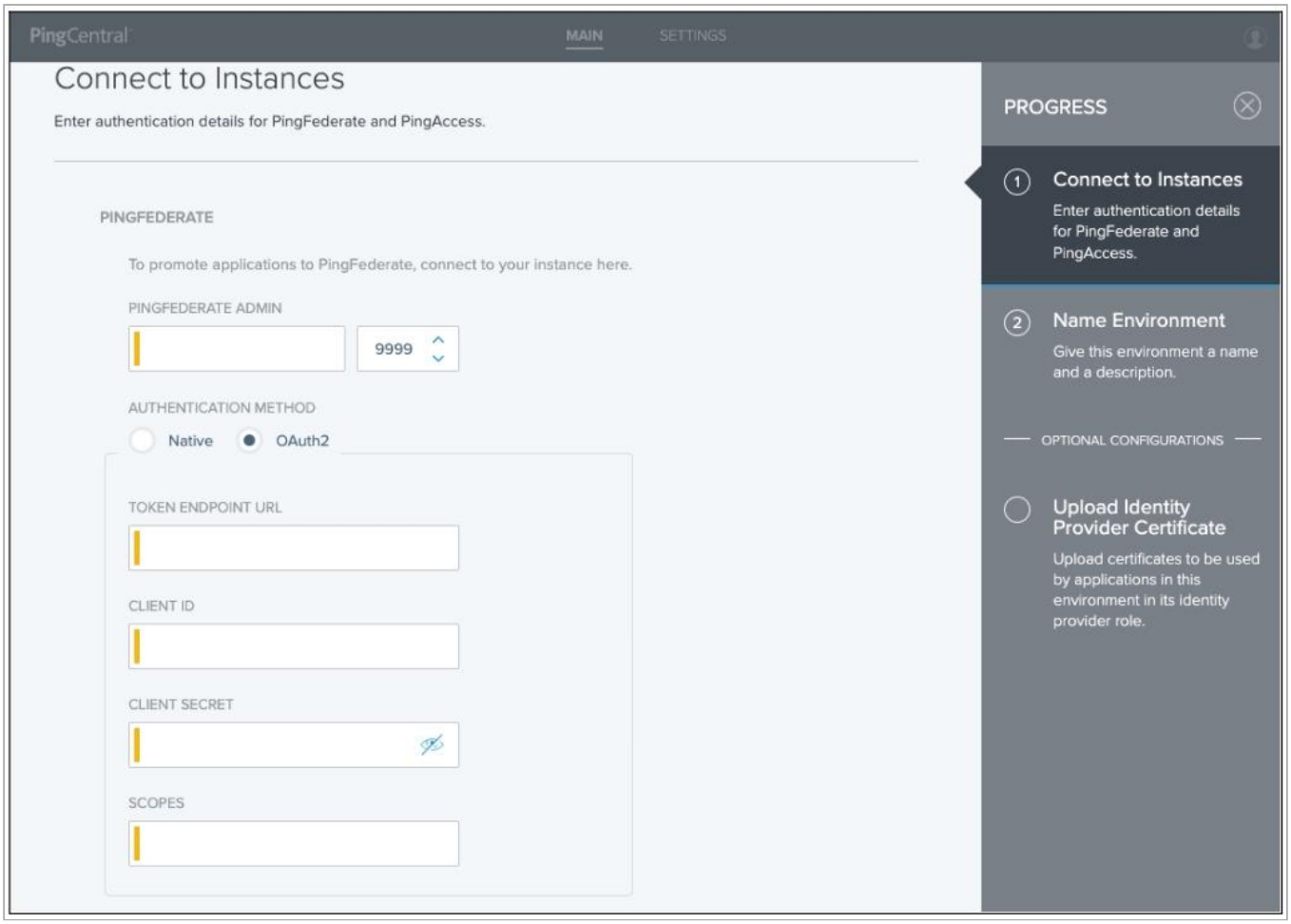
Option	Description
Create or generate a secret.	Choose from: ◦ To create a strong, random alphanumeric string, click **Generate Secret**. ◦ Manually enter a secret.
Modify an existing secret.	1. Select the **Change Secret** check box. 2. Click **Generate Secret** to create a strong random alphanumeric string or manually enter a secret.

6. In the **Grant Types** field, select the **Client Credentials** and **Access Token Validation (Client is a Resource Server)** options.
7. In the **Default Access Token Manager** field, select **JSON Web Tokens** . Click **Save**.
8. Access the PingFederate `<pf_install>/pingfederate/bin/run.properties` file, and ensure that this property is set: `pf.admin.api.authentication=OAuth2` .
9. Access the PingFederate `<pf_install>/pingfederate/bin/oauth2.properties` file, and ensure that the following properties are set.

Property	Description
`client.id`	The unique client identifier defined in step 2.
`client.secret`	The client secret defined in step 4.
`introspection.endpoint`	This URL specifies where PingFederate validates the authentication token. For example, `https://<PF_RUNTIME_HOST>:<PF_RUNTIME_PORT>/as/introspect.oauth2`
`required.scopes`	Use any of the scopes defined in PingFederate. Go to **System → OAuth Settings → Scope Management** to see a list of available scopes. For details, see Scopes in the *PingFederate Server* guide.
`username.attribute.name`	The value mapped to the **Username** attribute defined on the **Contract Fulfillment** tab.
`role.attribute.name`	The value mapped to the **admin_role** attribute defined on the **Contract Fulfillment** tab.

    1. Configure PingCentral:

10. In PingCentral, to connect to the new PingFederate client, go to **Environments → Add Environments**.
11. On the **Connect to Instances** page, complete the following fields using the properties you just set in the PingFederate `oauth2.properties` file.



- **PingFederate Admin**: Enter the URL defined in the `pf.admin.baseurl` property for the new client. For details, see Configuring PingFederate properties in the *PingFederate Server* guide.
- **Authentication Method**: Select **OAuth2**.
- **Token Endpoint URL**: Enter the token endpoint URL, which is PingFederate: `https://<PF_RUNTIME_HOST>:<PF_RUNTIME_PORT>/as/token.oauth2`.
- **Client ID**: Enter the unique client identifier set as the `client.id` property.
- **Client Secret**: Enter the client secret set as the `client.secret` property.
- **Scopes**: Enter the scopes set as the `required.scopes` property.

12. Click **Next**.

Configuring PingAccess for SSO

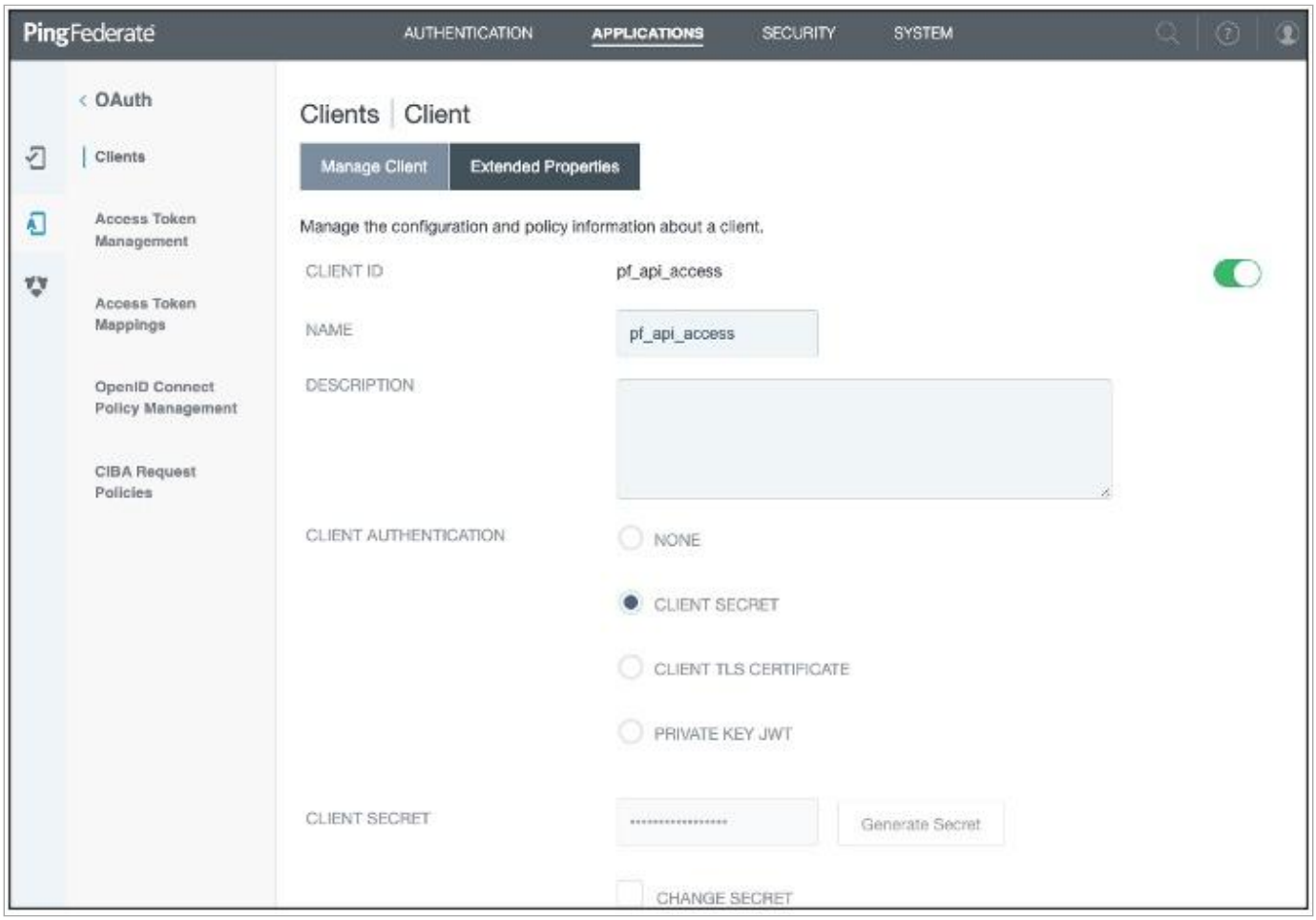
About this task

To use SSO to access PingAccess from PingCentral:

Steps

1. Configure a new PingFederate client:
    1. In PingFederate, go to **Applications → OAuth → Clients**.
    2. On the **Manage Client** tab, complete these fields:
        - **Client ID**: Enter a unique identifier for the client.
        - **Name**: Enter a name for the client.
        - **Description**: Enter a description of the client.

See Configuring OAuth clients in the *PingFederate Server* guide for details.



    1. In the **Client Authentication** field, select **Client Secret**.
    2. In the **Client Secret** field, you can:

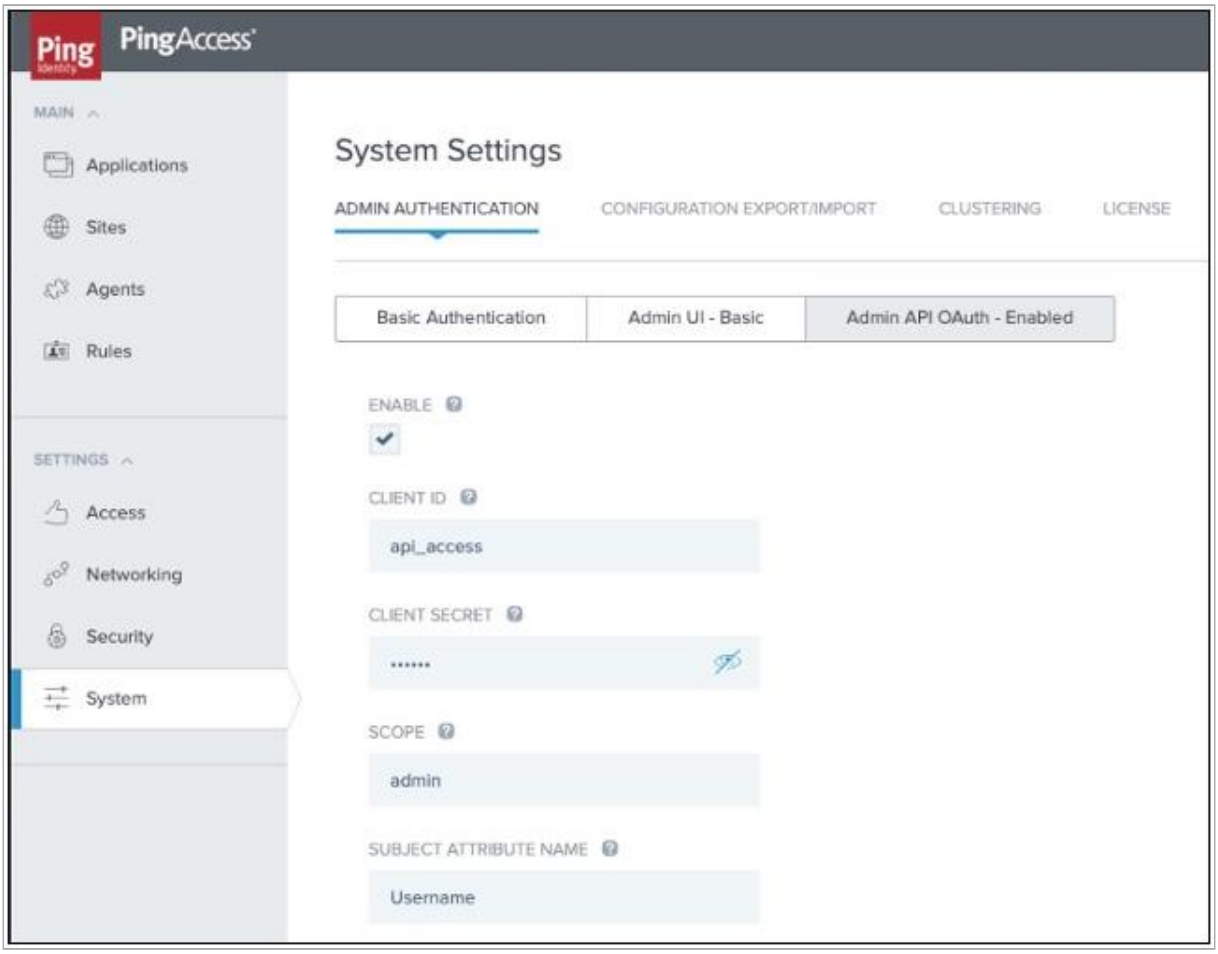
Option	Description
Create or generate a secret.	Choose from: ■ To create a strong, random alphanumeric string, click **Generate Secret**. ■ Manually enter a secret.
Modify an existing secret.	1. Select the **Change Secret** check box. 2. Click **Generate Secret** to create a strong random alphanumeric string or manually enter a secret.

3. In the **Grant Types** field, select the **Client Credentials** and **Access Token Validation (Client is a Resource Server)** options.
4. In the **Default Access Token Manager** field, select **JSON Web Tokens** . Click **Save**.
5. Access the PingFederate `<pf_install>/pingfederate/bin/run.properties` file, and ensure that this property is set: `pf.admin.api.authentication=OAuth2` .
6. Access the PingFederate `<pf_install>/pingfederate/bin/oauth2.properties` file, and ensure that the following properties are set.

Property	Description
`client.id`	The unique client identifier defined in step 2.
`client.secret`	The client secret defined in step 4.
`introspection.endpoint`	This URL specifies where PingFederate validates the authentication token. For example, `https://<PF_RUNTIME_HOST>:<PF_RUNTIME_PORT>/as/introspect.oauth2`
`required.scopes`	Use any of the scopes defined in PingFederate. Go to **System → OAuth Settings → Scope Management** to see a list of available scopes. For details, see Scopes in the *PingFederate Server* guide.
`username.attribute.name`	The value mapped to the **Username** attribute defined on the **Contract Fulfillment** tab.
`role.attribute.name`	The value mapped to the **admin_role** attribute defined on the **Contract Fulfillment** tab.

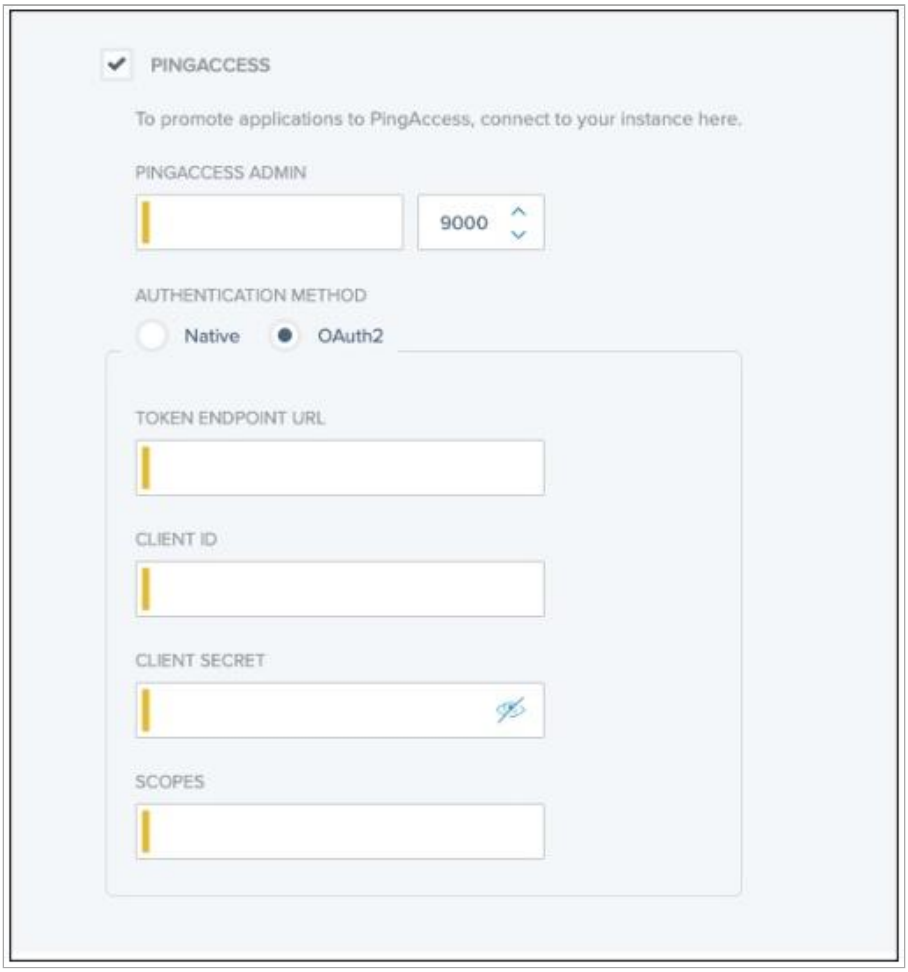
2. Configure PingAccess:
    1. In PingAccess, go to **System → System Settings → Admin Authentication**.

2. On the **Admin API OAuth** tab, select **Enable** and complete these fields as shown in the example:
    - **Client ID**: Enter the unique client identifier for the new client.
    - **Client Secret**: Enter the client secret defined for the new client.
    - **Scope**: Enter the scopes set as required scopes for the new client.
    - **Subject Attribute Name**: Enter the name of an access token attribute that you want to use as the **Subject** field in audit log entries for the admin API.



3. Click **Save**.

3. Configure PingCentral:
    1. In PingCentral, to connect to the new PingFederate client, go to **Environments → Add Environments**.
    2. On the **Connect to Instances** page, scroll down and select **PingAccess**.
    3. Complete the following fields using the properties you just set in PingAccess.



- **PingAccess Admin**: Enter the link to access PingAccess.
- **Authentication Method**: Select **Native** or**OAuth2**.
- **Token Endpoint URL**: Enter the token endpoint URL, which is available here in PingFederate: `https://<PF_RUNTIME_HOST>:<PF_RUNTIME_PORT>/.well-known/openid-configuration`.
- **Client ID**: Enter the unique identifier for the new client.
- **Client Secret**: Enter the client secret defined for the new client.
- **Scopes**: Enter the scopes set as required scopes for the new client.

4. Click **Next**.

Configuring PingCentral to run in FIPS-compliant mode

Running PingCentral in FIPS-compliant mode guarantees that all cryptographic algorithms and protocols meet the U.S. federal standard for security compliance. When you're connecting PingCentral to an external database, you must use a FIPS-compliant authentication method.

PingCentral is currently running FIPS 140-3. Learn more about this version in FIPS 140-3.

To enable this option, access the `<PingCentral_install> /conf/application.properties` file and set the `pingcentral.fips.enabled` property value to `true`.

> **Note**
>
> If on Linux systems, the Bouncy Castle FIPS-approved secure random number generator might drain a large amount of entropy during initial seeding. If available entropy becomes too low, the PingCentral server or bundled command-line tools could stall on startup for an extended period of time. If this occurs, then you will likely need to integrate with a hardware random number generator or install an entropy-supplementing daemon like `rngd`.

Configuring logging

The log file serves as a record of events that occurred within the system and is often used for troubleshooting purposes. This section explains how to access the log file, interpret the entries within it, and change the level of detail the log file captures.

Steps

1. Access the PingCentral log file from the following location: `/<pingcentral_install>/log/application.log`.

   The level of detail that the log file contains depends on how the logging level is set. Logging levels are a means of categorizing the entries in your log file by severity, and are described in the following table. Detailed log files require more system resources, so PingCentral only records errors, warnings, and some information events by default.

Logging level	Description
ERROR	Indicates a failure within the application occurred.
WARNING	Indicates the system detected an unusual situation and errors might occur.
INFO	Provide basic information about activities that occurred. For example, a service was started and stopped, or a new user was added to the application.
DEBUG	Provides additional detail regarding the events that occurred, and is often used to diagnose and troubleshoot reported issues.
TRACE	Provides even more detailed information than the Debug level regarding the application's behavior. This logging level is not used often and can affect system performance.

2. Changing the logging level to have the system record additional details can help with troubleshooting. To change the logging level:

   1. Open the configuration file at `/<pingcentral_install>/conf/log4j2.xml`.
   2. Scroll down, locate the Logger line item shown below, and change the logging level within the quotations. The `DEBUG` logging level provides enough information to troubleshoot most issues.

```
<Logger name="com.pingidentity" level="INFO" additivity="false" includeLocation="false">
        <!--<AppenderRef ref="console"/>-->
        <AppenderRef ref="file"/>
</Logger>
```

3. Save and close the file and repeat the task you performed when the error occurred.
4. For optimal system performance, open the `log4j2.xml` file again and change the logging level back to `INFO`.
5. Access the `application.log` file again and review the information that was recorded in `DEBUG` mode. If you are working with a technical support team to troubleshoot an issue, you can send them the log file that recorded your activities.

Replacing the Admin Console SSL Certificate

To avoid seeing a certificate warning when you access PingCentral, replace the user-facing SSL certificate so it will no longer use the self-signed certificate.

About this task

Import your proprietary certificate into PingCentral by uploading the `.p12` or `.pem` file that contains it. If you're running PingCentral in FIPS-compliant mode, you'll import a `.pem` file, as `.p12` files are not allowed.

Steps

1. Select the **Security** tab, expand the menu, and select **Server TLS Key Pair**.

   Result:

   The **Server TLS Key Pair** page displays information about the key pair, including its status and expiration date.
2. To import a new key pair, click **Import Key Pair**.
3. On the **Import Key Pair** page, click **Choose PKCS12 or PEM File** and select the `.p12` or `.pem` file to upload.
4. In the **File Password** field, enter the password to the key store file.

   > **Note**
   >
   > If you're running PingCentral in FIPS-compliant mode, your password must be at least 14 characters long, and the RSA key must be at least 2048 bits.
5. In the **Alias** field, specify the alias of the certificate in the key store file that you want to use for the Admin Console SSL Certificate, if required.
   - If the `.p12` file being imported for the TLS key pair contains a single alias, PingCentral accepts the file without requiring an alias.
   - If the `.p12` file being imported for TLS key pair contains multiple aliases, PingCentral requires the alias.
6. In the **Key Password** field, enter the password for the selected certificate if the PKCS12 file requires a separate password for the key.

7. Click **Import**.
8. Restart PingCentral.

   Result:

   After PingCentral restarts, you can access PingCentral without receiving a certificate warning.

Configuring MTLS

To use mutual TLS (MTLS) for Admin API authentication, import a client TLS key pair. If you're running PingCentral in FIPS-compliant mode, you'll import a `.pem` file, as `.p12` files are not allowed.

Steps

1. Select the **Security** tab, expand the menu, and select **Client TLS Key Pair**.
2. Click **Import Key Pair**.
3. On the **Import Key Pair** page, click **Choose PKCS12 or PEM File** and select the `.p12` or `.pem` file to upload it.
4. In the **File Password** field, enter the password to the key store file.

   > **Note**
   >
   > If you're running PingCentral in FIPS-compliant mode, your password must be at least 14 characters long, and the RSA key must be at least 2048 bits.

5. In the **Alias** field, specify the alias of the certificate in the key store file that you want to use, if required.
6. In the **Key Password** field, enter the password for the selected certificate if the PKCS12 file requires a separate password for the key.
7. Click **Import**.

Managing environments

All environments managed within PingCentral, as well as connected PingFederate and PingAccess environments, display on the **Environments** page, where you can view and update information about each environment and delete them from PingCentral when they are no longer needed.

Items worth mentioning:

- If you add PingAccess environments to PingCentral, ensure that PingFederate is configured as the PingAccess token provider. See Configuring PingFederate as a PingAccess token provider for details.
- To enforce random secret generation and restrict non-administrators from creating their own, select the **Generate Client Secret on Promotion** check box when managing your environments. PingCentral will generate random client secrets.
- If your application owners promote Security Assertion Markup Language (SAML) applications to PingFederate or PingAccess environments, ensure that the appropriate trusted certificate authority (CA) certificates are available in PingCentral. See Adding trusted CA certificates to PingCentral for details.

- Starting with version 1.14, PingCentral performs regular health checks on its environments. These checks involve calling either the heartbeat endpoint or the admin API version endpoint, depending on the version of PingFederate being used. To configure this process, modify the `orchestrator.heartbeat.polling-interval-ms` and `orchestrator.heartbeat.offset-ms` parameters in the `conf/application.properties` file. These settings determine both the frequency of polling and the initial delay before the health check begins.
- Starting with PingCentral 1.8, trusted CA certificates are stored in the PingCentral database instead of an external trust store. Certificates that exist in this trust store in previous versions are imported to the PingCentral database during the upgrade process.

Adding environments

Use the wizard to add PingFederate and PingAccess environments to PingCentral.

Before you begin

Ensure that PingFederate is configured as a token provider for PingAccess.

For more information, see Configuring PingFederate as a PingAccess token provider.

Steps

1. On the **Environments** page, click **Add Environment**.
2. On the **Connect to Instances** page, connect to a PingFederate or PingAccess environment:

   Choose from:

   - **Native**: Complete the **Username** and **Password** fields for your PingFederate or PingAccess environments.
   - **OAuth2**: Complete the **Token Endpoint URL**, **Client ID**, **Client Secret**, and **Scopes** fields.
   - **Client Certificate**: Select the certificate you want to use for mTLS. See Configuring MTLS for details on uploading these certificates.

     > **Note**
     >
     > If an environment is disabled or offline, you will be unable to add the environment to PingCentral.

     If this is the first time that you have set up this environment, and the initial validation fails, you see a **Skip Verification** option. If you select this option, it allows you to skip the validation process. However, if you set it up correctly, you won't see this option.

   If the environment is disabled or offline, and you edit the connection configuration, the **Skip Verification** check box is automatically marked.
3. Click **Next**.
4. On the **Name Environment** page, complete the **Name**, **Short Code**, and **Description** fields.
5. **Optional:** To configure whether non-administrators need approval for promoting an application to an environment, select an option from the **Approval Type** list:

   Choose from:

   - Select **No Approval** to allow non-administrators to promote applications to the environment freely.

- Select **Approval Required** to indicate that application promotion requires approval.
- Select **Require Approval If Any Expression Fails** and proceed to the next step to configure an **Approval Expression**.
- Select **Require Approval If Any Expression Succeeds** and proceed to the next step to configure an **Approval Expression**.

6. **Optional:** If you selected **Require Approval If Any Expression Fails** or **Require Approval If Any Expression Succeeds**, you must configure a Spring Expression Language (SpEL) expression in the **Approval Expression** field.

   You can use SpEL expressions to determine whether an application requires approval or not. For more information, see Creating and testing approval expressions at the bottom of this page for details.

   > **Tip**
   >
   > For more information on SpEL, see Spring Expression Language (SpEL) in the Spring Framework documentation.

7. **Optional:** If you want application owners to be able to edit the underlying application JSON when they promote their OAuth and SAML applications, select **Allow JSON editing for application promotions**.

   > **Warning**
   >
   > Providing application owners with this ability can be risky, so it's highly recommended that you require promotion requests to be approved. That way, you'll be able to compare the submitted application JSON to the original application JSON before you approve the promotion.

8. **Optional:** To enforce random secret generation and restrict non-administrators from creating their own, select the **Enforce Random Client Secrets** check box.

   PingCentral will generate random client secrets.

9. **Optional:** Select the **Allow only administrators to delete applications from PingFederate** (and PingAccess, when applicable), option to restrict application owners from deleting applications from environments.

10. **Optional:** To add an identity provider (IdP) certificate, select the appropriate certificate in the **Signing Certificate** list or to upload your own certificate, click **Choose** and enter the certificate password in the appropriate field. Click **Save and Close**.

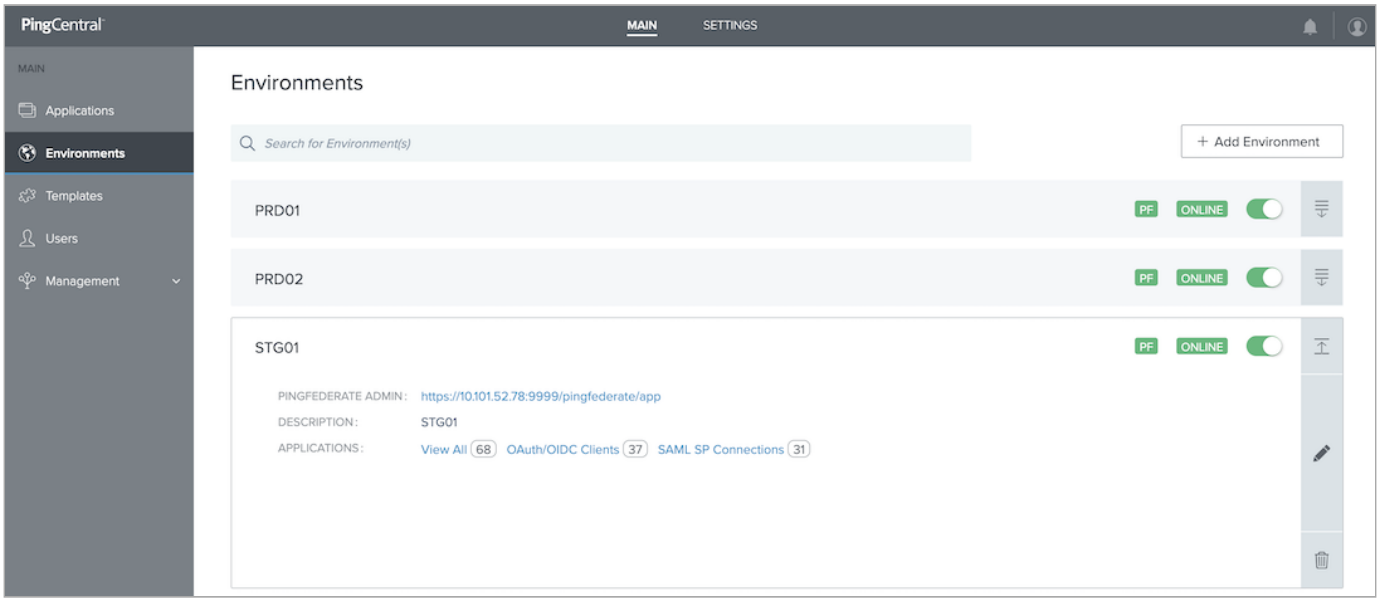
    Result:

    The environment is displayed on the **Environments** page. If you chose to protect the environment, you see a shield icon next to its name. Depending on the type of environment, you also see a **PF** or **PA** icon. The color of this icon represents the status of the environment. A green icon indicates that the environment is verified while a red icon indicates that the environment isn't verified.

    Depending on if an environment is online, offline, or disabled, you see the environment status in a display bar. You also see the toggle switch that you can click to disable the environment and indicate that it is undergoing maintenance.

11. Click **Save and Continue**.

12. Click the expandable icon associated with the environment to view environment details.



Environment details include:

- A link to PingFederate.
- A link to PingAccess.
- A description of the environment.
- The total number of applications hosted on this environment and a breakdown of or clients, connections, and applications. Click these links to access filtered lists of these applications on the **Applications** page.

> **Note**
>
> If an environment is unavailable, applications in that environment don't display on the **Applications** page.

Updating environments

Update PingFederate and PingAccess environment information at any time.

Steps

1. To manage the environment maintenance status, see the following choices:

   Choose from:

   - To indicate that an environment is down for maintenance, toggle the switch on the applicable environment status bar from left (green) to right (gray). This action signals to application owners that the environment is undergoing maintenance and is now **Disabled**. This prevents PingCentral from connecting to the environment, avoiding UI errors.
   - To revert maintenance status, toggle the switch on the applicable environment status bar from right (gray) to left (green). This action removes the maintenance **Disabled** status, allowing application owners to resume interactions with the environment. This is the default status.

> **Note**
>
> If an environment is offline or **Disabled**, the environment information displays a gray **OFFLINE** status bar. If an environment status is unknown, the status bar is unavailable.

2. To edit environment information, click the expandable icon associated with it, and then click the **Pencil** icon.

   All of the editable information displays on one page.

Option	Description
Update the name and description	To update the name and description, change the information in the **Name**, **Short Code**, and **Description** fields.
Update the assertion encryption certificate	To update the assertion encryption certificate, click **Choose** to upload a new certificate and enter the certificate password in the appropriate field.
Update connection information	To update the connection, ensure that the authentication method you want to use is selected: ◦ **Native**: Update the **Username** and **Password** fields for your PingFederate or PingAccess environments. ◦ **OAuth2**: Update the information in the **Token Endpoint URL**, **Client ID**, **Client Secret**, and **Scopes** fields. ◦ **Client Certificate**: Update the certificate used for mTLS. **Note** If a PingAccess environment is added to PingCentral and removed through the edit page, the connection information is saved and restored if the PingAccess environment is selected again.

Option	Description
Configure promotion approval requirements	To configure if non-administrators need approval for promoting an application to an environment, select an option from the **Approval Type**. Choose from: ◦ Select **No Approval** to allow non-administrators to promote applications to the environment freely. ◦ Select **Approval Required** to indicate that application promotion requires approval. ◦ Select **Require Approval If Any Expression Fails** and see Creating and testing approval expressions at the bottom of this page for details. ◦ Select **Require Approval If Any Expression Succeeds** and go to Creating and testing approval expressions on this page.
Update the JSON editing option	If you want application owners to be able to edit the underlying application JSON when they promote their OAuth and SAML applications, select **Allow JSON editing for application promotions**. ⚠ **Warning** Providing application owners with this ability can be risky, so it's highly recommended that you require promotion requests to be approved. That way, you'll be able to compare the submitted application JSON to the original application JSON before you approve the promotion.
Add or remove the enforcement of random client secret generation	To enforce random secret generation and restrict non-administrators from creating their own, select the **Enforce Random Client Secrets** check box. PingCentral will generate random client secrets. To allow non-administrators to generate their own secret, clear the check box.
Configure application owner deletion access	To restrict application owners from deleting applications from environments, select the **Allow only administrators to delete applications from PingFederate** (and PingAccess, when applicable), option.
Update the signing certificate	To update the signing certificate used to promote SAML applications, select the appropriate certificate in the **Signing Certificate** list or upload your own.
Update the SP certificate	To update the service provider (SP) certificate, click **Choose** to upload a new certificate and enter the certificate password in the appropriate field.

Option	Description
Update the assertion encryption certificate	To update the assertion encryption certificate, click **Choose** to upload a new certificate and enter the certificate password in the appropriate field.

3. Click **Save**.

Deleting environments

Delete environments from PingCentral when they are no longer needed.

Steps

1. Click the expandable icon associated with the environment to view environment details.
2. To delete the environment from PingCentral, click its associated **Delete** icon.

   Result:

   A message displays asking you if you want to delete the environment.
3. Click **Delete**.

   Result:

   A message displays saying that the environment was deleted.

> **Note**
>
> When an environment is deleted, applications that were promoted to that environment retain the promotion details from the deleted environment.

Configuring PingFederate as a PingAccess token provider

To add PingAccess environments to PingCentral, PingFederate must be configured as the token provider. If you have PingFederate and PingAccess environments established, this configuration is likely in place.

About this task

To configure PingFederate as the token provider for PingAccess, the Issuer URL in PingAccess must either match the Base URL in PingFederate, or one of the virtual hosts defined in PingFederate.

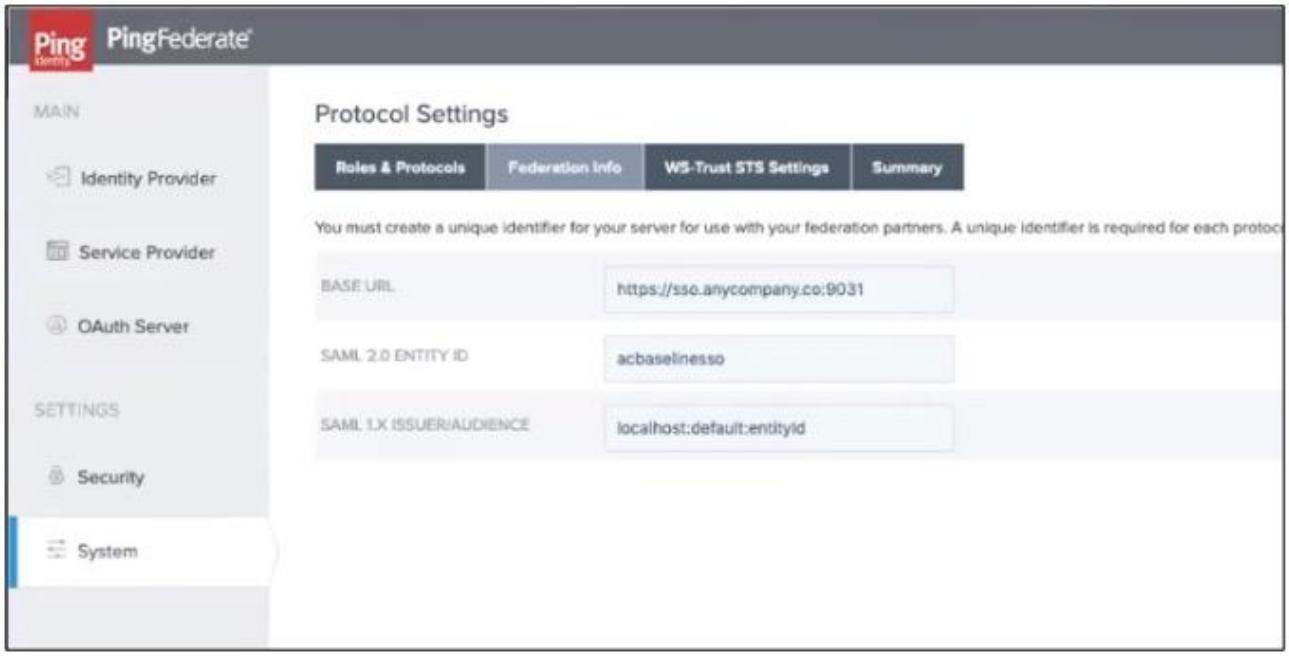
Steps

1. To configure PingFederate as a PingAccess token provider, ensure the PingAccess **Issuer URL** and the PingFederate **Base URL** match.

   If a virtual host is defined in PingFederate, continue to step 3.

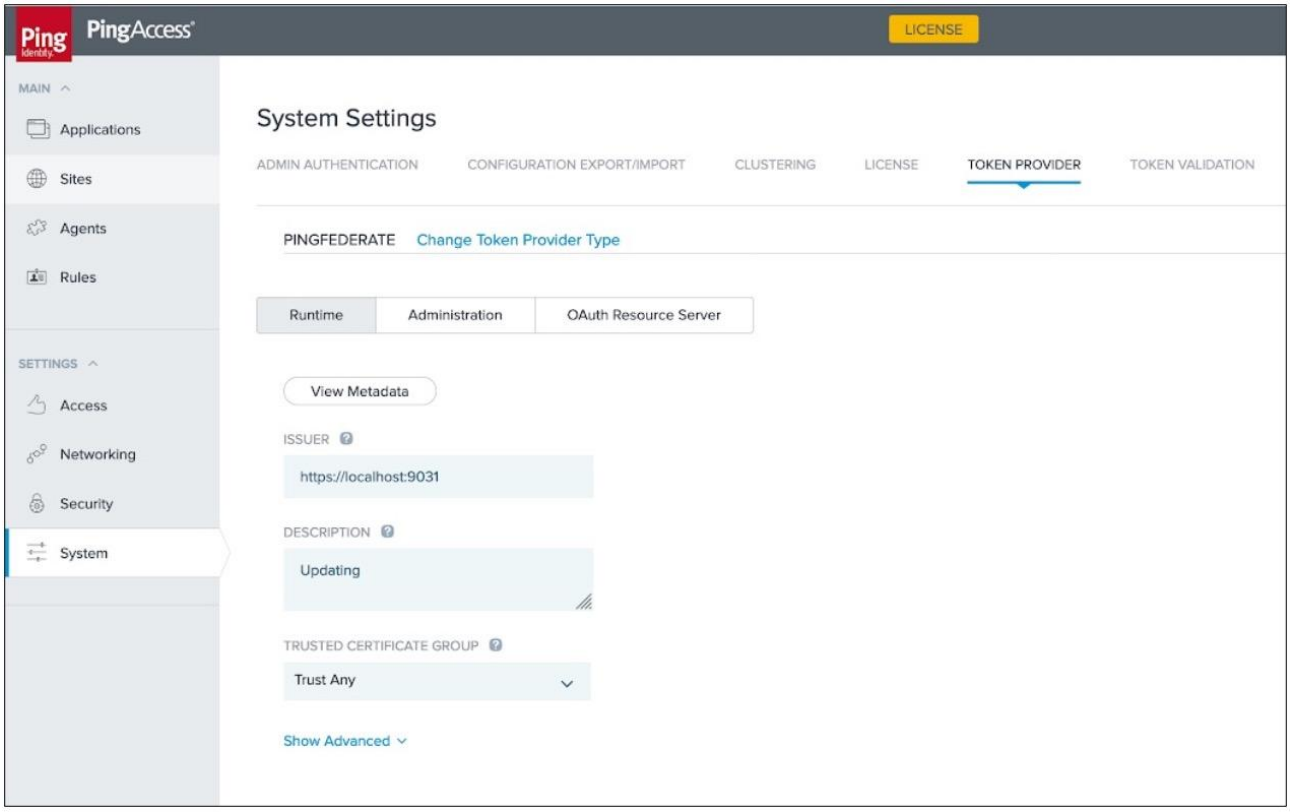
2. To locate this information:

   - In PingFederate, to locate the **Base URL** field, go to **System → Protocol Settings → Federation Info**, as shown in the following example.

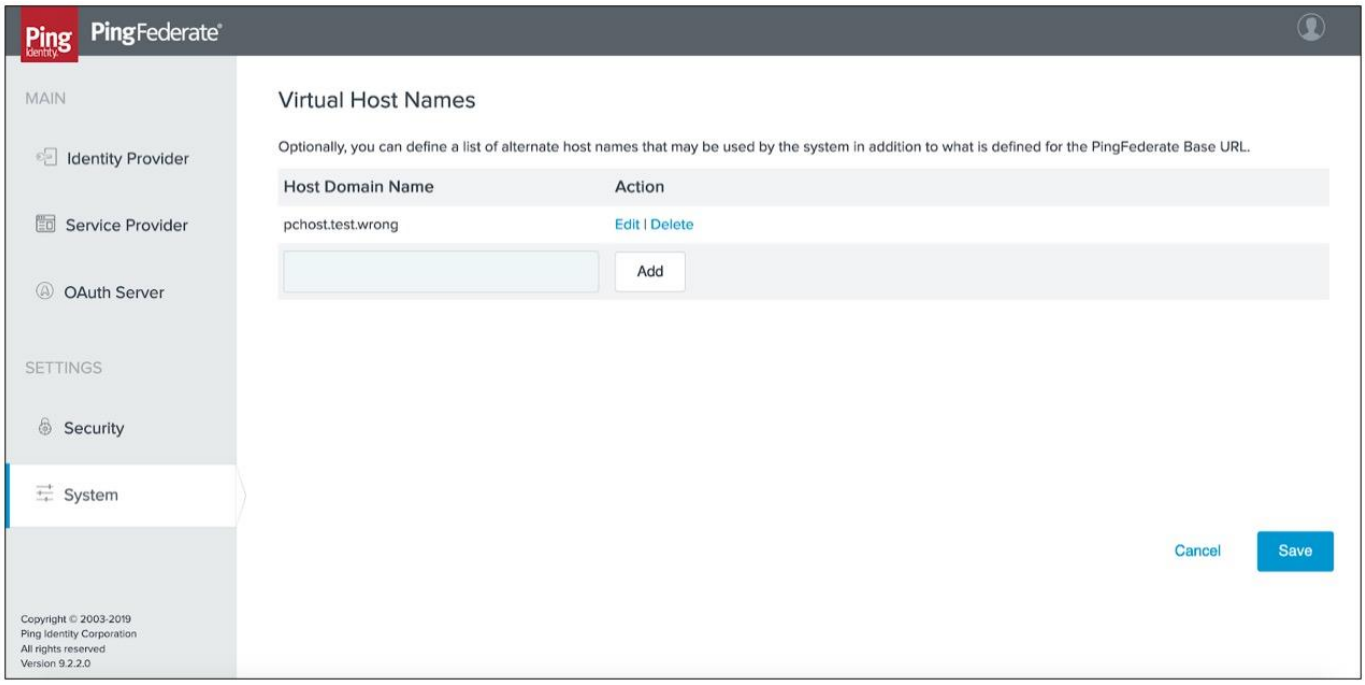


   - In PingAccess, to locate the **Issuer URL**field, go to **System → Token Provider**.

> **Note**
>
> In some versions of PingAccess, the Issuer URL might exist as separate **Host** and **Port** fields.



3. If a virtual host is defined in PingFederate, the PingAccess Issuer URL can reference that instead of Base URL. In PingFederate, to locate the virtual host, go the **System → Virtual Host Names** page and review the information in the **Host Domain Name** field.



Adding trusted CA certificates to PingCentral

For application owners to securely promote Security Assertion Markup Language (SAML) applications to PingFederate and PingAccess environments, trusted certificate authority (CA) certificates must be available in PingCentral.

Steps

1. To add a trusted certificate to PingCentral, select the **Settings** tab.
2. Expand the **Security** menu and select **Trusted CA Certificates**.

   Result:

   The **Trusted CA Certificates** page displays a list of the certificates currently available in PingCentral.
3. Click **Add Certificate**.
4. In the **Add Certificate** window, in the **Alias** field, enter a unique name for the certificate.
5. Click **Choose File**, select the certificate, and click **Add** to upload it.

   Result:

   The certificate displays in the list of trusted CA certificates.
6. Click the **Expand** icon for the certificate to view details.

   + image::dwn1624648315152.png[alt="An screen capture of the Trusted CA Certificate page containing several certificates. The Test signing cert certificate is expanded.",role="border-no-padding"]

Creating and testing approval expressions

Configure a Spring Expression Language (SpEL) expression to manage promotion approval requirements for your environment.

Before you begin

When you configure an environment, on the **Connection** page, select **Require Approval If Any Expression Fails** or **Require Approval If Any Expression Succeeds** from the **Approval Expression** list. For more information, see Adding environments.

About this task

You can manage promotion approval requirements for your PingCentral environment by creating custom approval expressions with Spring Expression Language (SpEL). These expressions will evaluate the application based on its JSON payload to determine whether an administrator will be required to approve promotions.

Steps

1. On the **Connection** page, in the **Approval Expression** field, click **Test** to expand the **Test Spring Expression** window.

   Result:

   The **Test Spring Expression** window displays.
2. In the **Application Configuration** field, enter the application configuration information as a JSON payload.

If you have promotion configuration information, enter it as a JSON payload in the **Promotion Configuration** field.

3. In the **Spring Expression** field, use the following function to extract values from the JSON payload using a specified JSON path: `#jsonPath(\{JSON payload}, \{JSON path})`.

   Build your own expressions using the following variables:

   - *#application*: Represents the type of application (OAuth, OIDC, SAML Service Provider (SP), or PingAccess) and its corresponding API model (**ClientApplicationView**, **ConnectionApplicationView**, or **PingAccessApplicationView**).
   - *#oAuthApplicationPromotion*: Provides access to the **OAuthApplicationPromotionView** API model and promotion configuration information for OAuth and OIDC applications.
   - *#samlSpApplicationPromotion*: Provides access to the **SamlApplicationPromotionView** API model and promotion configuration information for SAML SP applications.
   - *#pingAccessApplicationPromotion*: Provides access to the **PingAccessApplicationPromotionView** API model and promotion configuration information for PingAccess applications.

   For help building expressions, see SpEL approval expression examples or Spring Expression Language (SpEL) in the *Spring Framework* documentation.

4. Under the **Spring Expression** field, click **Test Expression** to test your expression.

   Result:

   The **Spring Expression** result displays.

   For information about approval expression handling, see the following:

   - If you selected **Require Approval If Any Expression Fails** from the **Approval Type** list: If any expression results in `false` then approval is required. If all expressions are `true` then approval is not required.
   - If you selected **Require Approval If Any Expression Succeeds** from the **Approval Type** list: If any expression results in `true` then approval is required. If all expressions are `false` then approval is not required.
   - If any of the expressions do not return a Boolean value or if there are any errors in the expressions, the promotions will require approval.
   - Multiple expressions can be added, and are evaluated sequentially from top to bottom in an IF/ELSE chain. You can change the order in which these expressions display in the list by dragging and dropping them into different locations within the list.

5. Click the **Update** button to save your configuration or click the **Cancel** button to discard it.

SpEL approval expression examples

This section contains SpEL approval expression examples for OAuth and SAML applications.

OAuth approval example

In this example, if the **Require Approval If Any Expression Succeeds** option is selected and the application is an OAuth application with the **Client Credentials** grant type, PingCentral requires that an administrator approve the promotion before the application owner can promote it to the target environment.

```
#jsonPath(#application, 'type').equals('OAuth')
&& #jsonPath(#application,
'grantTypes').contains('CLIENT_CREDENTIALS')
```

SAML SP approval example

In this example, if the **Require Approval If Any Expression Succeeds** option is selected, the application is a SAML SP application, and one or more of the attribute mappings are OGNL expressions, PingCentral requires that an administrator approve the promotion before the application owner can promote it to the target environment.

```
#jsonPath(#application, 'type').equals('SAML_20_SP')
&& !#jsonPath(#application,
"attributeMappings[?(@.type == 'EXPRESSION')]").isEmpty()
```

Monitoring PingCentral

The Spring Boot Actuator, enabled by default, collects a wide variety of information to help you monitor and manage PingCentral in production environments and can be connected to your time series database in a few simple steps.

Spring Actuator data and Spring Metrics can be accessed at their respective endpoints:

- `https://localhost:9022/actuator/`
- `https://localhost:9022/actuator/metrics`

Actuator data includes:

Endpoint	Usage
`/beans`	Displays a list of the Spring beans in PingCentral.
`/caches`	Displays a list of available caches.
`/conditions`	Displays the conditions that were evaluated on configuration and auto-configuration.
`/configprops`	Displays a list of configuration properties.
`/env`	Displays a list of environment properties.
`/environmentConnectivity`	Returns a list of environments in PingCentral and their connectivity statuses.
`/environmentConnectivity/ <environmentName>`	Returns connectivity status of the specified environment.
`/health`	Displays health check information regarding PingCentral.
`/heapdump`	Used to perform a heap dump.

Endpoint	Usage
`/info`	Displays general information about PingCentral, such as the vendor and version number.
`/liquidbase`	Displays information regarding database migrations that have been applied.
`/loggers`	Displays the logger configuration for PingCentral.
`/mappings`	Displays a collated list of all @RequestMapping paths.
`/scheduledtasks`	Displays the scheduled tasks within PingCentral.
`/threaddump`	Used to perform a thread dump.

Metrics data includes a wide variety of information, such as the amount of JVM (Java Virtual Machine) memory used, the number of Jetty threads used, and the amount of time it takes to complete processes. Counters and timers are also available for most API endpoints. Counters count the number of times an endpoint is hit, and timers measure the amount of time it takes for events to occur.

Spring Metrics collects a large amount of data, but it does not present the data in ways that are easy to understand. Consequently, many choose to move this data to either a Prometheus or Graphite time series database and use Grafana to view it through interactive dashboards with charts and graphs.

Because Graphite supports only counters, but Prometheus supports both counters and timers, Prometheus is the preferred choice. See the following topics for instructions on setting up one of these time series databases to communicate with PingCentral.

- Setting up Prometheus using basic authorization
- xref:
- Setting up Graphite
- Setting up Grafana
- Accessing Prometheus and Grafana

Managing users

You can set up PingCentral so users access the application through single sign-on (SSO), or you can set it up so users access the application directly through a sign on page.

See the following:

- Managing users through PingCentral
- Setting up SSO for PingCentral

> **Note**
>
> When SSO is enabled, local users defined within PingCentral and the default Administrator will not be able to access the application or access the Admin API using HTTP basic authentication.

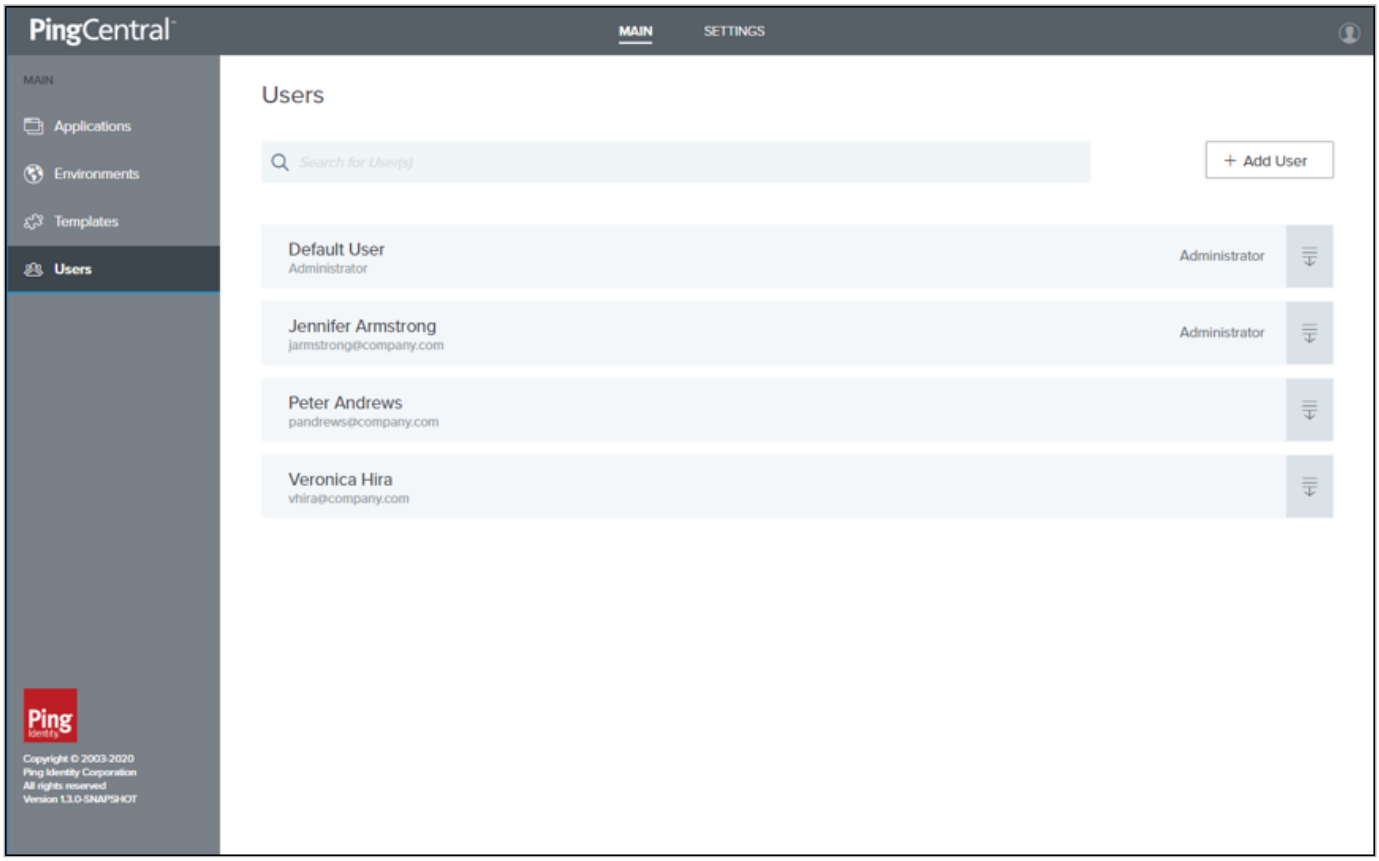
Managing users through PingCentral

If you have a small number of users, you might want to manually add them to PingCentral and manage their access directly through the application. You need their first and last names, user names, and the roles they will assume.

Steps

1. On the **Users** tab, click **Add User**.
2. Enter the user name, first name, last name, and email address in the appropriate fields.
3. Select the user's role (either Application Owner or Administrator). Click **Next**.
4. Enter an initial password for the new user in the **Password** field. Passwords must be at least 8 characters long, contain one upper-case letter, one lower-case letter, and one number.
5. Enter it again in the **Confirm Password** field. Click **Save and Close**.

   The new user appears in the list of PingCentral users in alphabetical order.



6. Update user information or delete a user by selecting the expandable icon associated with the user and clicking the pencil or delete icon.

Setting up SSO for PingCentral

The single sign-on (SSO) method is significantly more secure than the password authentication method. At this time, OpenID Connect (OIDC) is used for SSO.

To set up SSO:

1. Configure SSO for PingCentral
2. Configure the resource server
3. Configure the OpenID provider

> **Note**
>
> When SSO access to PingCentral is configured, administrators cannot assign applications to application owners before they access PingCentral. After application owners sign on to PingCentral, administrators can access their account information and assign applications to them.

Auto-provisioned users

For each SSO user, a local PingCentral user is auto-provisioned the first time they sign on with information obtained from the subject (sub) claim provided by the OpenID provider.

The user's first name, last name, and role are also recorded. PingCentral derives the user's name from the `given_name` and `family_name` claims defined by the profile scope.

If first-time access to PingCentral is with API access using a bearer token, auto-provisioning occurs if the user's name and role are available. For performance reasons, subsequent bearer token access doesn't update the local user information, such as first name and last name.

Although PingCentral administrators can modify or delete auto-provisioned users, doing so results in the SSO user being auto-provisioned again. Because the provisioning process generates a new PingCentral user ID, any application associations with the previous user ID will be lost.

Configuring SSO for PingCentral

With PingCentral, single single sign-on (SSO) is disabled by default.

To configure PingCentral for SSO:

1. Enable SSO.
2. Configure OpenID Connect (OIDC) properties to access OIDC configuration information.
3. Define an OAuth client at the OpenID provider.
4. Configure PingCentral role mapping.

After completing these steps, configure the resource server.

Enabling SSO for PingCentral

Steps

1. Open the `<PingCentral_install>/conf/application.properties` file.
2. Uncomment the following property and set the value to **true**.

   Example:

   ```
   pingcentral.sso.oidc.enabled=true
   ```

Configuring OIDC for PingCentral

Steps

- In the `<PingCentral_install>/conf/application.properties` file, locate the `pingcentral.sso.oidc.issuer-uri` property, uncomment it, and define the Issuer URI.

  Example:

  In this example, PingCentral attempts to access OIDC configuration information at `https://sso.mycompany.com:9031/.well-known/openid-configuration`.

  ```
  pingcentral.sso.oidc.issuer-uri=https://sso.<mycompany>.com:9031
  ```

  If PingCentral can't access the OIDC configuration information, it fails to start. Make sure the OpenID provider is running and accessible before starting PingCentral.

  In the future, if changes are made on the OpenID Provider that affect the OIDC configuration information used for SSO, you must restart PingCentral to incorporate them.

Defining the OAuth client for PingCentral

Define an OAuth client for PingCentral at the OpenID provider.

Steps

- In the `<PingCentral_install>/conf/application.properties` file, locate the following property, uncomment it, and provide the client ID and client secret for the OAuth client.

  Example:

  ```
  pingcentral.sso.oidc.client-id=<CLIENT_ID>
  pingcentral.sso.oidc.client-secret=<CLIENT_SECRET>
  ```

  > **Important**
  >
  > Secure the secret using the obfuscation script available in `bin/obfuscate`, and by using output ciphertext rather than the cleartext secret.

Configuring PingCentral role mapping

About this task

In PingCentral, two user roles are defined: the IAM Administrator, and the Application Owner. An initial IAM Administrator is created by default and can add other users to PingCentral and assign them to the appropriate role.

When SSO is enabled, the OpenID Provider must indicate the PingCentral role with a claim defined in the ID token or UserInfo endpoint. If this claim isn't found, or its value is nonsensical, the user is denied access to PingCentral, and auto-provisioning doesn't occur.

With PingFederate, an attribute can be mapped into the appropriate claim. To configure role mapping:

Steps

- In the `<PingCentral_install>/conf/application.properties` file, locate the following attributes and configure them for mapping into the appropriate claim.

```
# The name of the claim which identifies the PingCentral role associated with the user.
#pingcentral.sso.oidc.role-claim-name=PingCentral-Role
```

```
# The expected value of the role claim which indicates the user is a PingCentral administrator.
#pingcentral.sso.oidc.role-claim-value-admin=IAM-Admin
```

```
# The expected value of the role claim which indicates the user is a PingCentral application owner
(non-administrator).
#pingcentral.sso.oidc.role-claim-value-app-owner=Application-Owner
```

Result

If these default values can be used with the OpenID Provider, no further configuration is required.

Next steps

If the defaults can't be used with the OpenID Provider, set the claim name or values to synchronize PingCentral to the OpenID Provider configuration as shown.

```
pingcentral.sso.oidc.role-claim-name=UserRole
pingcentral.sso.oidc.role-claim-value-admin=Admin
pingcentral.sso.oidc.role-claim-value-app-owner=Developer
```

Configuring the resource server

PingCentral supports OAuth resource server functionality by validating provided bearer tokens when accessing the Admin API. Only signed JSON Web Token (JWT) tokens are supported in this release, so a JSON Web Key Set (JWKS) endpoint is required to obtain the public keys for signature validation.

About this task

If you are using PingFederate 10.1 or later, you can enable the centralized signing key functionality. Additional configuration isn't required in PingCentral to access the centralized JWKS endpoint.

If the access token manager has been configured with an explicit JWKS endpoint path, you must also specify this path in PingCentral.

> **Note**
>
> In PingFederate, this endpoint is exposed as https://*<pf_host>*:*<port>*/ext/*<JWKS Endpoint Path>*.

Steps

1. To provide the JWKS endpoint to PingCentral, open the `<PingCentral_install>/conf/application.properties` file, uncomment the `pingcentral.sso.oidc.oauth-jwk-set-uri` property, and define the JWKS endpoint URI, as in this example.

   Example:

   ```
   pingcentral.sso.oidc.oauth-jwk-set-uri=https://sso.<mycompany.com>:9031/ext/oauth/pingcentral/jwks
   ```

2. Configure the `username-claim` that PingCentral will use with bearer tokens.

   ```
   pingcentral.sso.oidc.oauth-username-claim-name=UserId
   ```

   With bearer tokens, PingCentral looks for the Username claim by default.

   > **Note**
   >
   > While the subject (sub) claim is mandatory with OpenID Connect (OIDC), it's not required when using OAuth 2.

3. Configure PingCentral to validate the access token issuer and audience claim values defined in the access token manager.

   By default, these claims aren't validated. Validation for either or both is enabled by setting the following properties:

   - `pingcentral.sso.oidc.oauth-iss-claim-value=<myissuer>`
   - `pingcentral.sso.oidc.oauth-aud-claim-value=<myaudience>`

4. Make sure that the values specified match those defined in the access token manager.

   > **Note**
   >
   > If the values don't match, the validation fails.

   > **Tip**
   >
   > If a blank value is defined in PingFederate, the claim won't be present in the token, so do not enable the validation of that claim in PingCentral.

5. Now that the resource server is configured, configure the OpenID provider.

Configuring the OpenID provider

PingCentral is an OpenID relying party for browser-based single sign-on (SSO), as well as an OAuth 2 resource server when directly accessing the admin API.

PingCentral has been tested with PingFederate 9.2.x, 9.3.x, 10.0.x and 10.1.x, serving as both the OpenID provider and OAuth 2 authorization server. This section provides tips for integrating PingCentral into an existing OpenID Connect (OIDC) 1.0 SSO infrastructure using PingFederate as the OpenID provider.

> **Note**
>
> As long as an OpenID provider is able to provide the endpoints and claims required by PingCentral (most notably the user name and role), other OpenID Connect 1.0 providers, can also be used.

To configure the OpenID provider:

1. Configure the Access Token Manager (ATM) for PingCentral.
2. Configure the OIDC policy for PingCentral.
3. Configure the OAuth client for PingCentral.

This section doesn't provide all of the details of setting up access token managers, OIDC policies, or attribute contracts because these topics are complex and often specific to a customer environment.

Step 1. Configuring the Acesss Token Manager

Configuring the Access Token Manager for PingCentral
About this task

The access token manager associated with the OIDC Policy must support signed JSON Web Token (JWT) tokens. To validate the token signature, PingCentral must be able to access a JSON Web Key Set (JWKS) endpoint URL in PingFederate. See Configuring JSON-token management in the *PingFederate Server* guide for additional information.

> **Note**
>
> Signing certificates and JSON Web Encryption (JWE) encryption (symmetric or asymmetric) are not currently supported.

Steps

1. In PingFederate, go to **Applications → OAuth → Access Token Management** and click **Create New Instance**.
2. On the **Instance Configuration** tab, add one or more symmetric keys, signing certificates, or both.
    1. Click **Add a new row to...** or click **Update** to modify an existing entry.

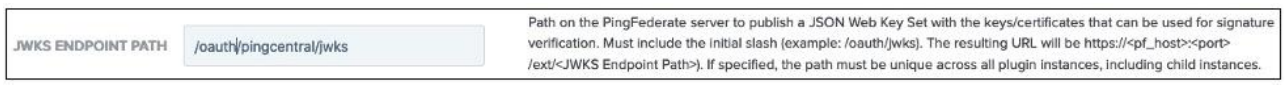
        > **Important**
        >
        > The **Key ID** field values must be unique across all JSON-token management instances, including child instances.

    2. If you have not yet created or imported your certificate into PingFederate, click **Manage Signing Certificates** and complete the task.

        > **Note**
        >
        > To use an RSA-based algorithm for JSON Web Signature (JWS), the key size of the signing certificate must be at least 2,048 bits. For an EC-based JWS algorithm, the key size depends on the chosen algorithm.

3. On the **Instance Configuration** tab, select the **Use Centralized Signing Key** option.

4. Select **Show Advanced Fields** and specify the path in the **JWKS Endpoint Path** field. This setp is optional when an algorithm is selected in the JWE Algorithm list.



> **Note**
>
> This path must be explicitly configured in PingCentral. See Configuring resource server functionality.

5. If you define either or both of the issuer or audience claim values within the access token manager, you can configure PingCentral to validate them.

    These claim values are also defined in the **Issuer Claim Value** and**Audience Claim Value** fields.

Step 2. Configuring the OIDC policy

Configuring the OIDC policy for PingCentral
About this task

The OAuth client will be associated with an OIDC Policy, which could be the default policy. This policy must map an attribute into the expected claim to signify the user's PingCentral role, which is defined in the **Attribute Contract**, **Attribute Sources & User Lookup**, and **Contract Fulfillment** in PingFederate.

In addition to the `sub` claim, the important claim is the `PingCentral-Role` claim. Optionally, you can also include the `given_name` and `family_name` claims with the profile scope.

You can fulfill the `sub` claim from the access token, and you need to fulfill the `PingCentral-Role` claim using an OGNL expression based on group memberships in your directory. The following is an example of an OGNL expression used in **Contract Fulfillment** to map roles.

```
// Reads the memberOf attribute values from the access token.
#pcrole = #this.get("memberOf"),
// If the values in memberOf contain the IAM administrator's group name, send 'IAM-ADMIN' in the
claim value.
#pcrole ==null?"False":#this.get("memberOf").toString().contains("pingcentral-iamadmins")? "IAM-
Admin":
// If the values in memberOf contain the application owner's group name, send 'Application-Owner' in
the claim value or send 'NoAccess'.
#pcrole ==null?"False":#this.get("memberOf").toString().contains("pingcentral-appowners")?
"Application-Owner" :"NoAccess"
```

> **Note**
>
> `memberOf` must be in your access token contract or retrieved through a lookup for the expression to work.

If the default PingCentral role claim name and values need to be altered to match the OIDC policy, update the `<PingCentral_install>/conf/application.properties` file.

Step 3. Configuring the OAuth client

Configuring the OAuth client for PingCentral
Before you begin

Define a PingCentral-specific OAuth client. These steps explain how to configure PingFederate as the OpenID provider. See Configuring OAuth clients in the *PingFederate Server* guide for additional information.

Steps

1. In PingFederate, go to **Applications → OAuth → Clients**.
2. In the **Client ID** field, enter a unique identifier the client provides to the resource server (RS) to identify itself. This identifier is included with every request the client makes.
3. In the **Name** field, enter a descriptive name for the client instance. This name appears when the user is prompted for authorization.
4. In the **Client Authentication** field, select **Client Secret**, and manually enter a secret or click **Generate Secret** to have one created for you.

   You will also use this secret when you configure SSO for PingCentral. See Configuring SSO for details.
5. In the **Redirection URIs** field, enter this URI: `https://<pc-host>:<pc-port>/login/oauth2/code/pingcentral`.
6. Locate the **Allowed Grant Types** field and select **Authorization Code**.
7. **Optional**: If you want API access with bearer tokens, locate the field and select the **Resource Owner Password Credentials** option.

   > **Note**
   >
   > PingCentral doesn't support ID token encryption.
8. From the **Default Access Token Manager** list, select your access token manager.
9. In the **OpenID Connect** section, from the **ID Token Signing Algorithm** list, select **RSA using SHA-256**. From the **Policy** list, select your OIDC policy.
10. Click **Save**.

Accessing the PingCentral API with SSO enabled

Access PingCentral's API with single sign-on (SSO) enabled using the OpenID Connect (OIDC) protocol.

Before you begin

Ensure you have an authorization server configured to authenticate users and issue access tokens. For more information, see Configuring the OpenID provider.

About this task

To access the PingCentral API with SSO enabled:

Steps

1. Obtain an access token from the authorization server's response. This token will authorize your API requests.

   > **Tip**
   >
   > The access token is a long string of characters and acts as your proof of authorization to access the requested resources.

2. Include the access token in the API request's authorization header. The PingCentral API server will verify the token's validity, authenticity, and scopes to ensure the necessary permissions.

   Example:

   ```
   GET /api/resource HTTP/1.1
   Host: pingcentral.example.com
   Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyL
   ```

Testing SSO configuration for PingCentral

Verify the security and functionality of your PingCentral single sign-on (SSO) configuration through testing.

Before you begin

Before testing your SSO configuration for PingCentral:

- Configure SSO within PingCentral
- Set up the resource server
- Establish the required settings for the OpenID provider

For more information, see Setting up SSO for PingCentral.

Steps

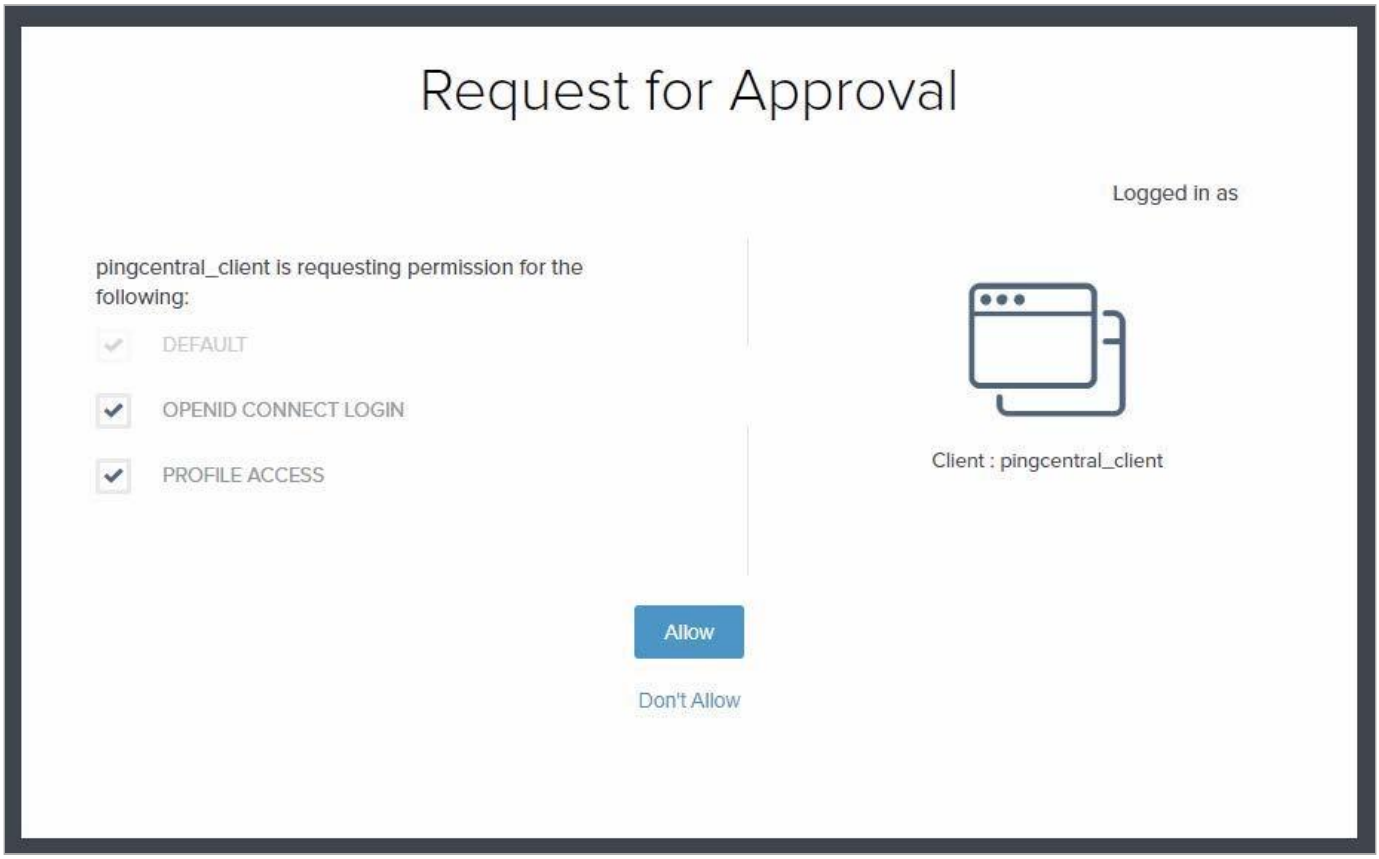
1. Go to your PingCentral console URL (for example: `https://pingcentral.ad.jibboo.org:9022/pass/login`), and after redirection to PingFederate, sign on with your credentials.

   Result:

   A **Request for Approval** window opens. The scopes listed in the window represent the permissions that PingCentral is requesting. These scopes determine what information PingCentral can access and use.

2. Select each check box to approve the scopes for the PingCentral client and click **Allow**.

   > **Tip**
   >
   > After testing is successful, you can set the approval window to **Bypass** in the OAuth client settings.



Result

- If you test as an IAM administrator group member in PingCentral, you can access **Applications**, **Environments**, **Templates**, **Users**, and **Management**.
- As an application owner group member, you can access **Applications** and **Management**.
- If you tested as a user in neither group, an error message displays.

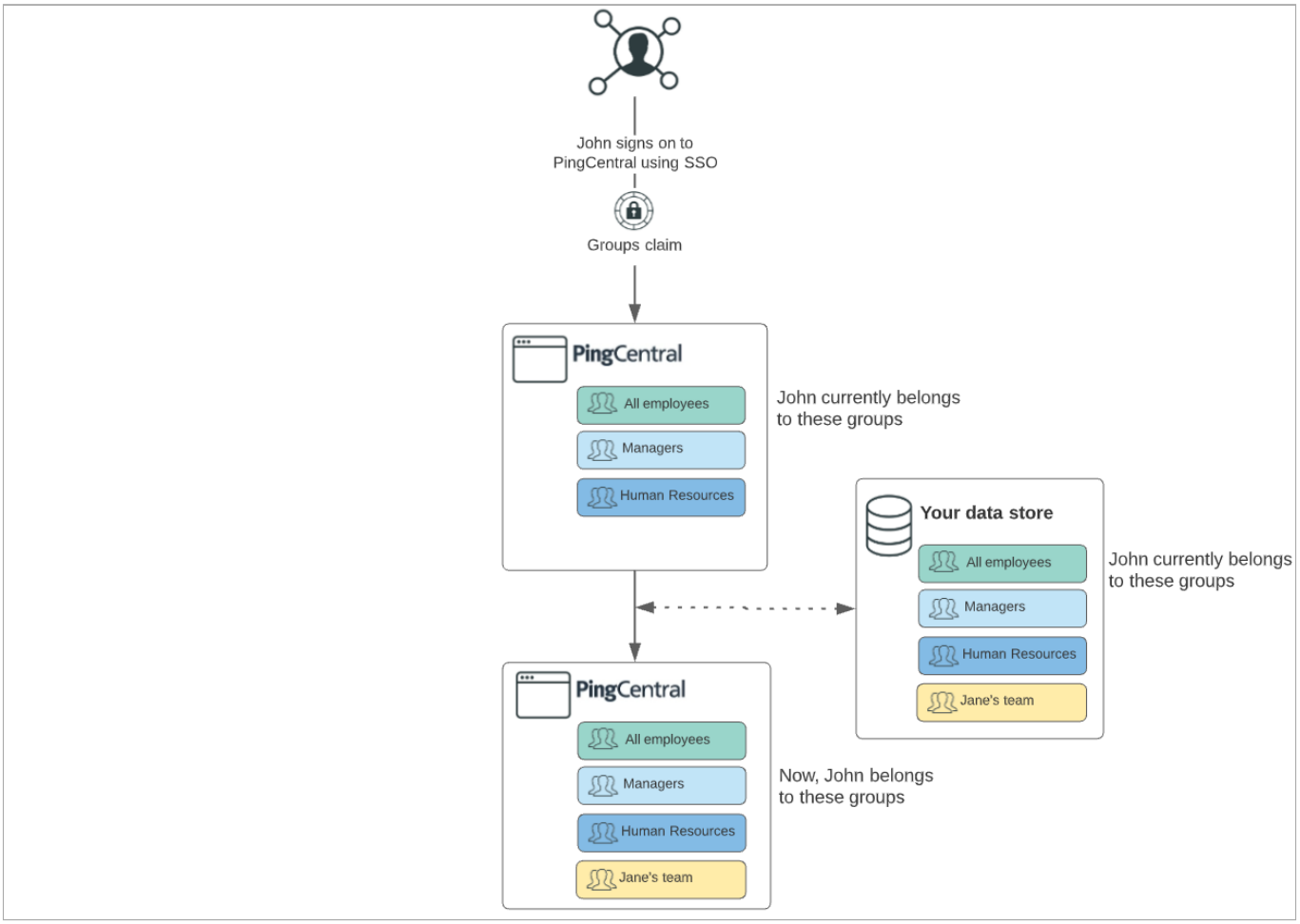
Managing user groups

Adding individual users to PingCentral applications can be a time-consuming process. If you have user groups defined in your data store, you can add the groups to PingCentral so that application owners can associate them with PingCentral applications and provide application access to multiple users at once.

Start by signing on PingCentral using single sign-on (SSO). Next, add information about each group, such as the group name, display name, and description to PingCentral. Group names should match the group names in your data store and aren't case sensitive.

If you have a large number of groups to add, you can upload the information into PingCentral in a `.csv` file. Then, you can add these groups of users to PingCentral applications, which provides application access to each user in the group.

Identities, user groups, and group membership information are managed in your data store. When a user signs on to PingCentral, the groups to which the user belongs are sent as part of the groups claim. PingCentral not only updates its existing group information with information from the data store, but if the claim contains new groups, it adds those groups to PingCentral, as shown in this diagram. It also updates the user profile to reflect current group memberships.



Adding user groups

After adding groups to PingCentral, associate them with PingCentral applications and provide application access to many users at once. Add groups one by one or import group information in a `.csv` file.

Steps

1. Sign on to PingCentral using SSO.

> **Note**
>
> Group functionality is only available if you sign on using SSO.

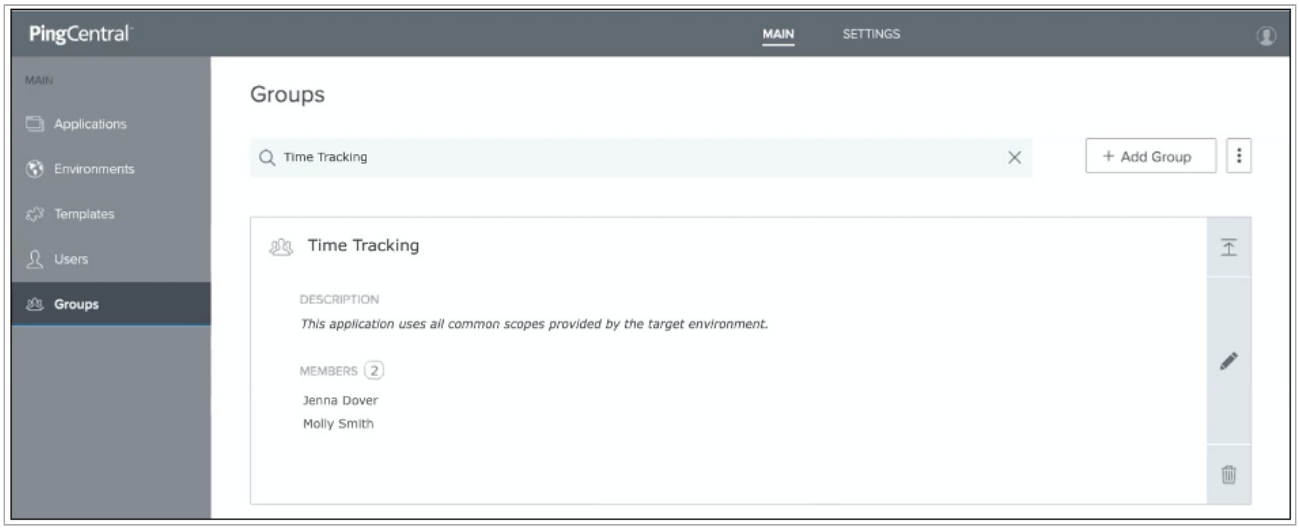
2. To add groups of users one by one:
    1. On the **Groups** tab, click **Add Group**.
    2. On the **Add Group** page, complete these fields:
        - **Group Name**: Enter the group name. Group names should match the group names in your data store and are not case sensitive.
        - **Display Name (Optional)**: Enter the name to display in PingCentral.

- **Description (Optional)**: Enter a description of the user group to display in PingCentral.

3. Click **Save and Close**.

   Result:

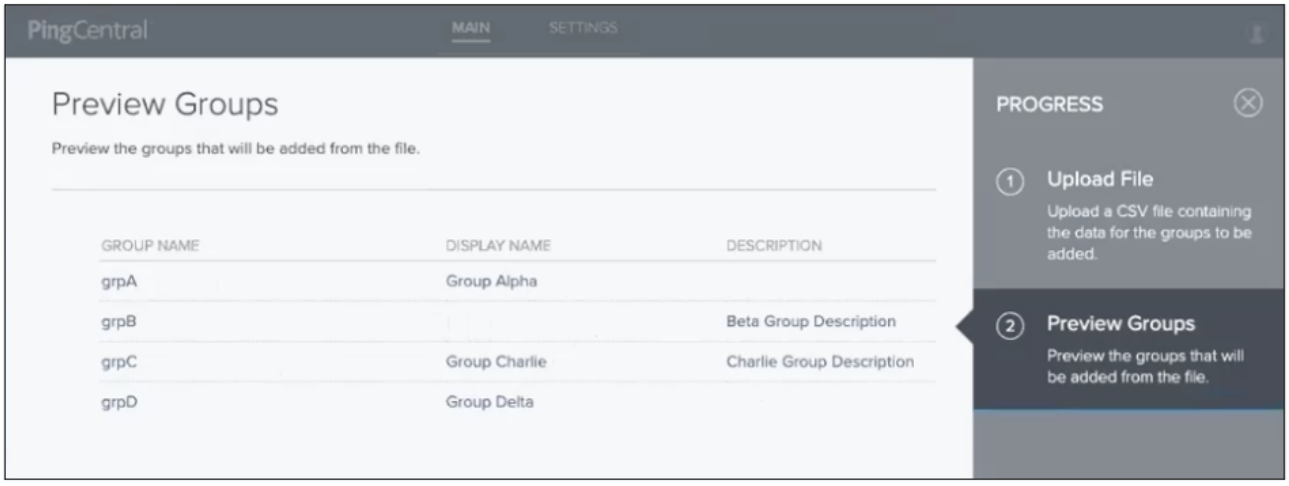
   The new group displays at the top of the **Groups** list. Click the **Expand** icon to see information about the groups and its members. Use the filter to locate specific groups.



3. To import information about a group of users:

   1. On the **Groups** tab, click **Import Groups**.
   2. On the **Upload File** page, click **Choose**.
   3. Select the `.csv` files that you want to import and click **Open** and click **Next**.
   4. On the **Preview Groups** page, review the group names, display names, and descriptions, and ensure they are accurate. If not, correct the `.csv` file and import it again.

      The **Name** field is required, but the **Display Name** and **Description** fields are optional.

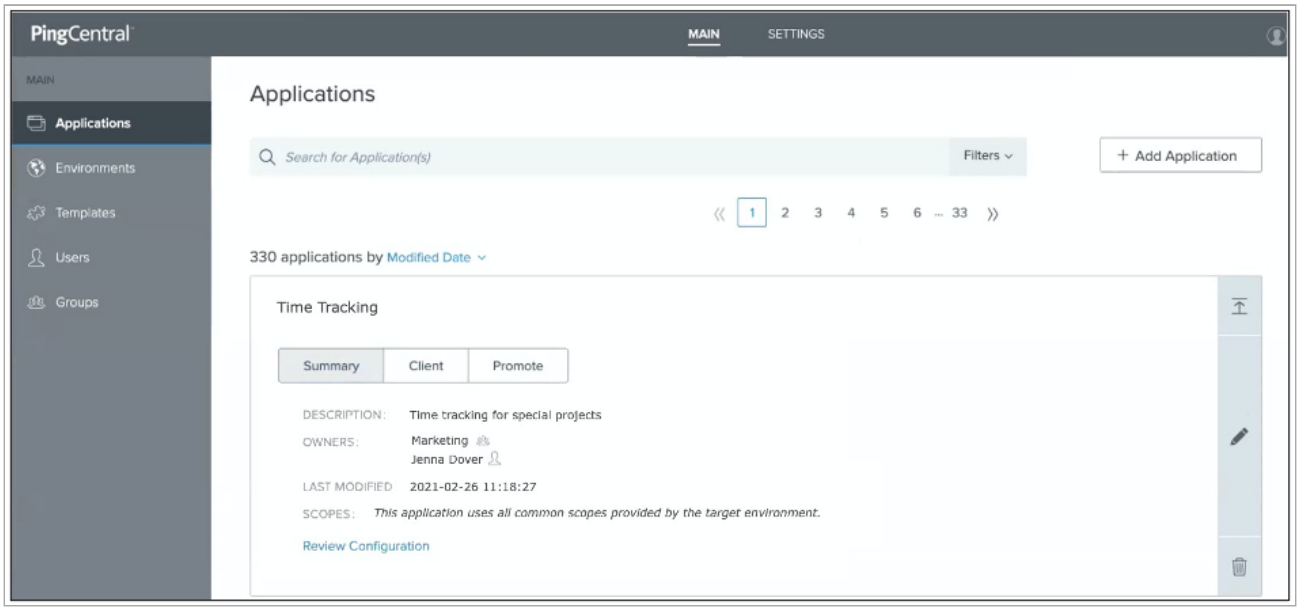


5. Click **Save and Close**.

Result:

The new group displays at the top of the **Groups** list. Click the **Expand** icon to see information about the groups and its members. Use the filter to locate specific members or groups.

After application owners associate users or groups of users with their applications, the ownership information also displays when you select the application.



Updating user groups

You can update the name, display name, and description for a user group.

Steps

1. To update user group information, click the **Expand** icon associated with the group that you want to update and then click the **Pencil** icon.

   Result:

   All of the editable information displays on the page.

2. Update the information in the **Name**, **Display Name**, and **Description** fields as needed, and click **Save and Close**.

> **Note**
>
> If the group name is updated in PingCentral but not in your data store, the groups will be out of sync, which might cause users to lose access to their applications.

Deleting user groups

Delete user groups when they are no longer needed.

Steps

1. On the **Groups** tab, select the group you want to delete and click the associated **Delete** icon.

Result:

A message displays asking you if you want to delete the group.

2. Click **Delete**.

Managing applications

All PingCentral applications and applications in verified PingAccess and PingFederate environments display on the **Applications** page, where you can filter the list of applications, add new applications, update existing applications, and delete them from PingCentral when they are no longer needed.

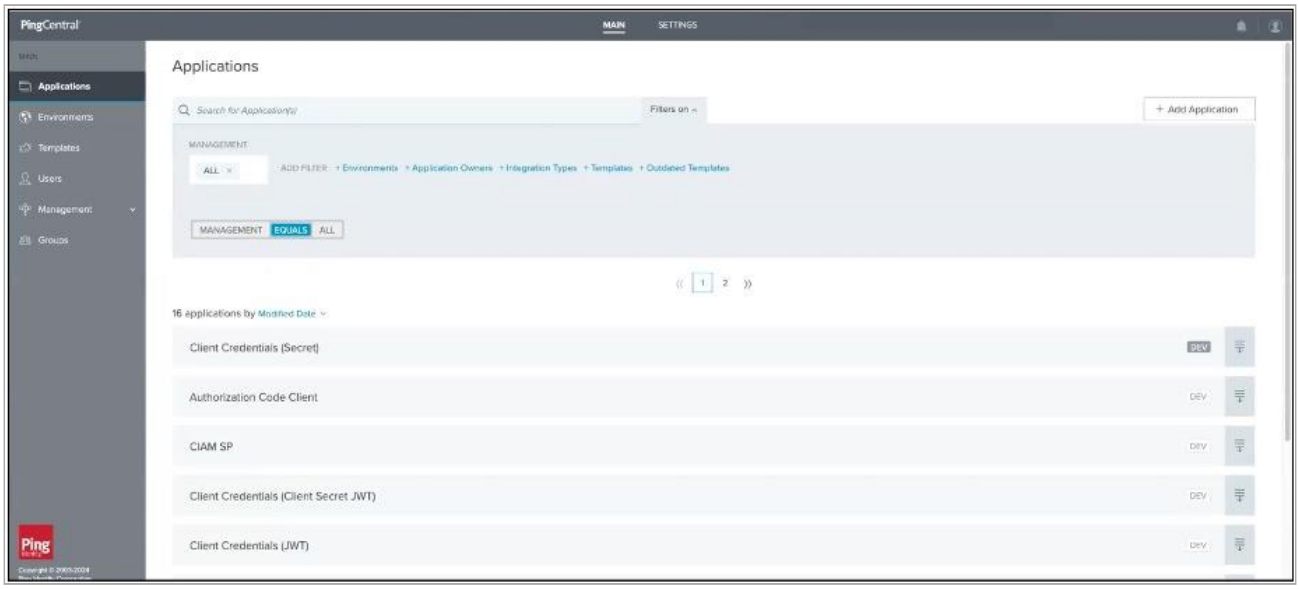
> **Note**
>
> If an environment is offline or if a PingCentral administrator has set the environment status to **Disabled**, application owners will be unable to update or delete applications for a disabled or offline environment.

Filtering applications

Use the filters at the top of the page to filter your list of applications, or use the search feature to locate specific applications.

Steps

1. Select your filters. You can filter by:
    - Environment
    - Application owner, or groups of application owners
    - Integration type (OAuth and OIDC or SAML)
    - Templates
    - Outdated templates
    - Type. Applications can be managed (applications created from or promoted to PingCentral environments), unmanaged (applications that reside in verified PingAccess or PingFederate environments), or you can select **All** to view all applications at once. Managed applications initially display by default.



2. Click the filters to remove them.
3. If you know the name of an application, further refine your search by entering the first few letters of application's name.

Adding applications

There are a variety of ways you can add applications to PingCentral. You can apply templates to them, you can create templates from them, or you can add them directly to PingCentral.

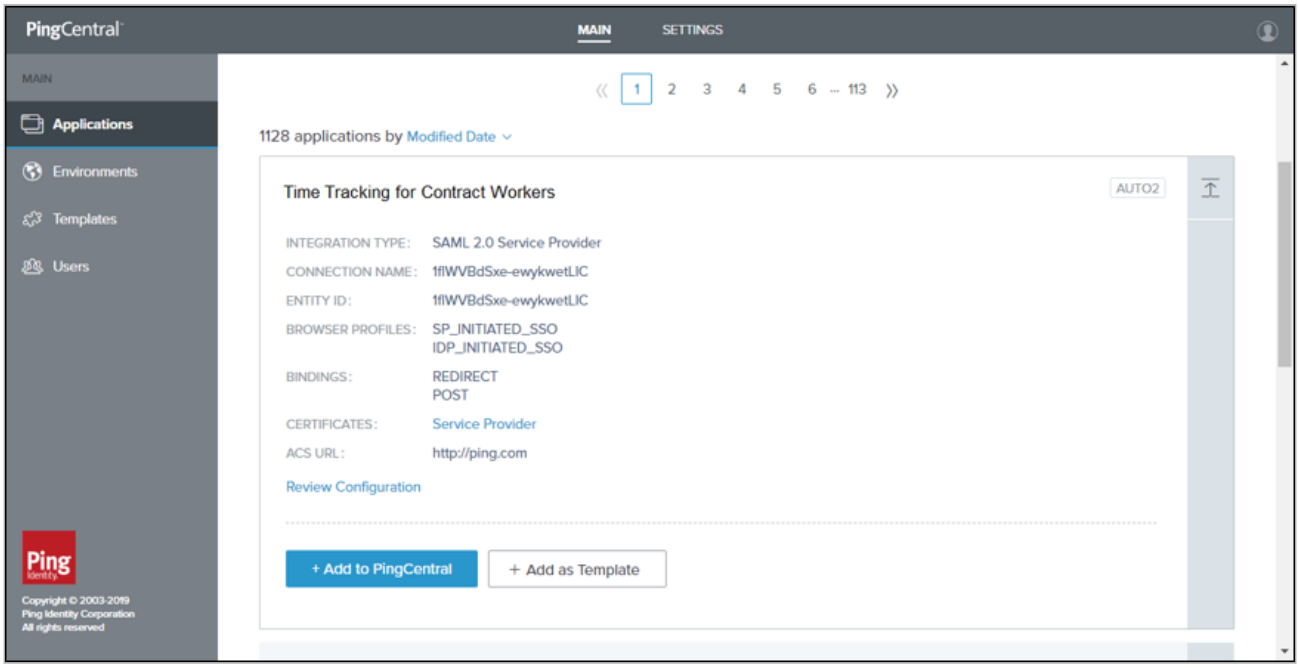
Steps

1. To apply an OAuth, OIDC, SAML, or PingAccess template to an application:
    1. Click **Add Application**.
    2. On the **Select Template** page, select the appropriate template and follow the wizard prompts.

   See Selecting a template in the *PingCentral for Application Owners* guide for additional information.
2. To create a template from an unmanaged application:
    1. Select the expandable icon associated with the application.
    2. Click **Add as Template** and follow the wizard prompts.

   The template displays in the list of available templates.
3. To add a PingFederate or PingAccess application directly to PingCentral:
    1. Use the search and filtering features to locate applications.

   For more information, see Filtering applications
    1. Select the expandable icon associated with the application.
    2. Click **Add to PingCentral** as shown in the following example, name the application, assign owners, and save it.



Updating applications

Update your applications at any time.

About this task

To keep your applications secure, rotate certificates and client secrets on a regular basis and apply updated security configurations to applications built from templates when new configuration templates become available.

You don't need to recreate your applications in PingCentral to apply new templates. Replace the templates associated with your applications and promote them again.

Steps

1. On the **Applications** page, click the **Expand** icon associated with the application you want to update.
2. **Optional:** On the **Connection** tab, if you modified the application configuration externally, click the **Sync** button to initiate an application synchronization.

> **Note**
>
> Depending on your application type, the **Connection** tab might be labeled **Client** or **Application**.

> **Important**
>
> If you created the application from a template, it cannot be synchronized with PingCentral. Only applications added directly to PingCentral can undergo synchronization.

Result:

PingCentral retrieves the latest JSON data from the original environment and updates the application.

> **Important**
> Syncing an application cancels all pending approvals for that application.

3. Click the **Pencil** icon.

   All of the editable information is on one page.

Option	Steps
Update the name, description, or owner information.	To update the application name, description, and owner, change the information in the **Name**, **Description**, or **Owners** fields.
Update or change the template.	If an application is based on an outdated template, an **Outdated Template** icon displays next to it. To update the application to the latest version of the template, click the **pencil** icon, click **Update Template**. Configurations in the new template will override those specified in the previous template. To update or change the template used to create the application, click the **pencil** icon, click **Change Template**, and select a new template from the **Select Template** page. **Note** You cannot apply different template types to applications. For example, you cannot apply SAML template to an OAuth or OIDC application or apply an OAuth or OIDC template to a PingAccess application.
Update OAuth or OIDC application information.	To update the application: ◦ In the **Client** section, change the scopes associated with OAuth or OIDC applications. Select or clear the appropriate check boxes. **Note** You cannot edit scopes for applications created in PingCentral 1.2.0. However, you can change the template associated with an application to a template created in a later version, which allows you to update scope information. ◦ In the **Promote** section, change the information in the **Redirect URI** fields for the appropriate environments. ◦ To change client secrets, return to the **Applications** page, promote the application again, and generate a new secret.

Option	Steps
Update SAML SP application information.	To update the application: ◦ In the **Attribute Mappings** section, add or remove attributes and expressions or update attribute and expression values. ◦ If attribute sources are defined in the underlying connection, select the **- Data Store -** identity attribute option and the applicable data store values. ◦ In the **Promotions** section, upload a new `.xml` file that contains service provider (SP) metadata, such as the entity ID, ACS URL, certificates, and attribute information, from another SAML application. Click **Choose File** or **Or Use URL** to provide the metadata file. **Note** If you're providing a new metadata file, you might also need to update the attribute mapping section to include new attributes from the metadata file. ◦ Change the information in the **Entity ID** or **ACS URL** fields. ◦ To change the signing certificate, select the appropriate certificate in the **Signing Certificate** list. ◦ To change the SP certificate, click **SP Certificate** to upload a new certificate, or click **Remove** to remove it. **Note** If a certificate is added to a SAML application and a SAML metadata file is subsequently provided that contains a certificate, additional changes to the application cannot be saved. If this occurs, exit the edit page and reopen it.
Update PingAccess application information.	To update the application: ◦ On the **Properties** tab, in the **Promote** section, update the **Virtual Hosts**, **Access Validation**, **Identity Mapping**, and **Site** or **Agent** names, as appropriate. ◦ On the **Resources** tab, update information regarding each resource. ◦ On the **Policy** tab, click the **Pencil** icon associated with the policy you want to update.

4. Click **Save**.

Deleting applications

About this task

You can delete applications within PingCentral, or choose to delete the application from all environments.

Steps

1. To delete an application, click the associated **Delete** icon.

   Result:

   A message displays asking you if you want to delete the application from PingCentral only or from all environments.

2. Select which environments to delete the application from.

   Choose from:

   - To delete an application from PingCentral only, click the **Delete** button.
   - To delete an application from all environments, depending on the application type, select the **Delete from PingFederate in all environments** or **Delete from PingAccess in all environments** check box and click the **Delete** button.

Managing templates

Templates created in PingCentral are snapshots of the configurations for existing OAuth, OIDC, SAML, and PingAccess applications. If changes are made to those applications, the configurations on which the templates are based become outdated.

Add, update, and delete templates to meet your needs, or revert them to previous versions, as necessary.

You can create PingCentral templates from existing PingFederate or PingAccess applications or build your own.

See the following for details:

- OAuth and OIDC templates
- SAML 2.0 and PingAccess templates

OAuth and OIDC templates

Add, update, or delete OAuth and OpenID Connect (OIDC) templates to meet your needs, or revert them to previous versions, as necessary.

To add an OAuth or OIDC template, select a client configuration to replicate. PingCentral retrieves this configuration and saves it as a template, which serves as a building block for future applications.

Adding OAuth and OIDC templates

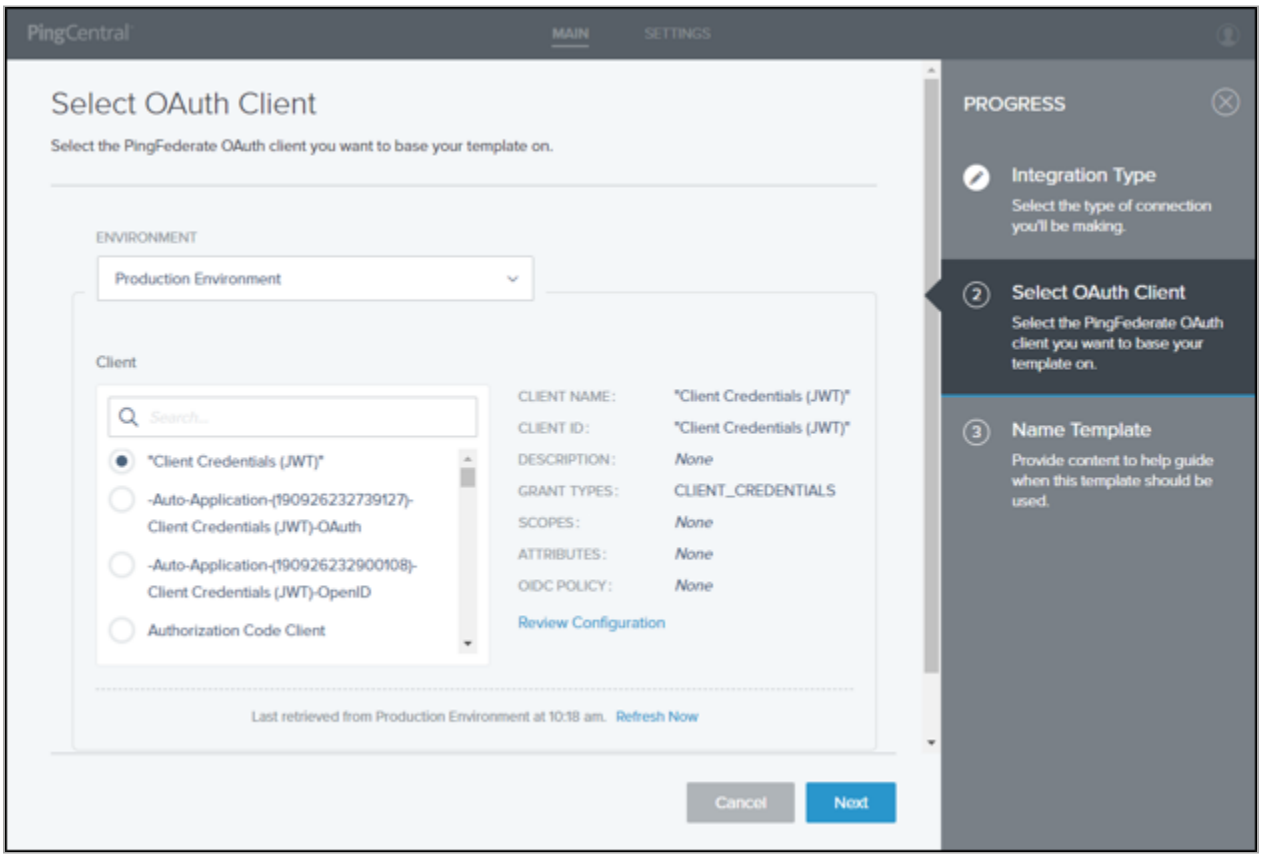
Steps

1. All templates are listed on the **Templates** page. To add a new template, click **Add Template**.
2. On the **Integration Type** page, select either an OAuth or OpenID Connect template. Click **Next**.
3. On the **Select OAuth Client** or **OIDC Client** page, select the PingFederate environment that hosts the client application you want to use as a template, and then select the application itself from the **Client** list.

> **Note**
>
> If an environment is offline or if a PingCentral administrator has set the environment status to **Disabled**, you will be unable to select a disabled environment for template creation.

Result:

You see details regarding the selected client.



4. To see the JSON for the application, click **Review Configuration**.
5. On the **Name Template** page, add a name and description for your template.

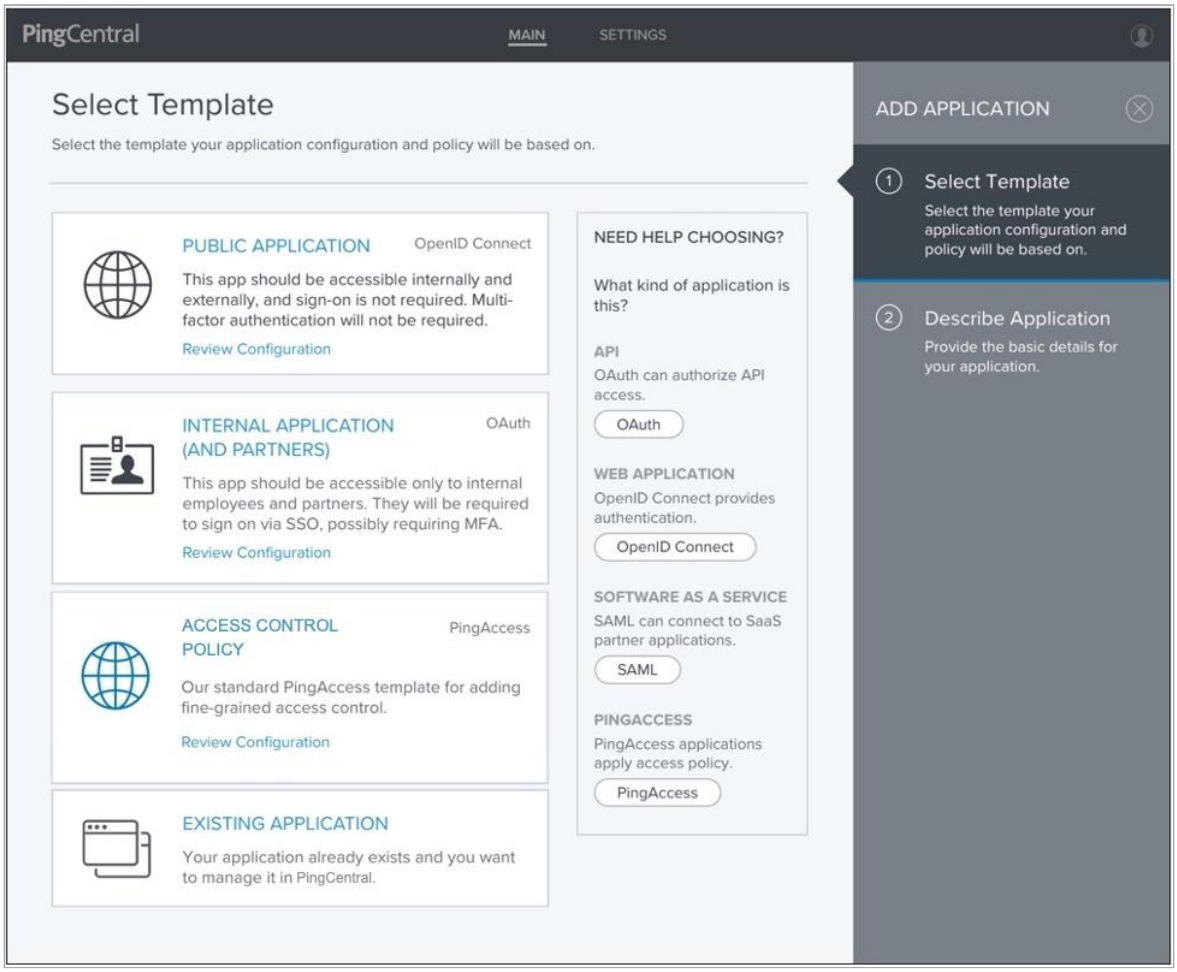
   This information will help application owners select the appropriate template.
6. Select an icon to represent your template.

   The icon you choose is shown with the template name and description.

7. Click **Save and Close**.

   Result:

   You see the new template in the list of available application templates. Application owners will see the new template on the **Select Template** page.



   For OAuth or OIDC application templates, the following items are saved:

   - The client application
   - The ATM, if one exists
   - The parent ATM, if one exists
   - The OIDC policy, if one exists
   - Grant types
   - Definitions of exclusive scopes referenced by the client

Updating OAuth and OIDC templates

Steps

1. To update an OAuth or OIDC template, click the **Expand** icon associated with the template.

2. If the template is based on an outdated configuration, you can click the **Sync** button to sync the template with the latest configuration available.

> **Note**
>
> When you upgrade to PingCentral 2.0, OAuth and OIDC templates created prior to version 2.0 cannot be synced with the most recent configuration available. Recreate the template in version 2.0 to use the sync feature going forward.

3. Click the **Pencil** icon to make additional changes.

   All of the editable information is on one page.

Option	Description
To update the name, description, or icon:	Update the information in the **Name** and **Description** fields or select a new icon to represent the template.
To update grant types:	To update the grant types used for authorization, select or deselect the grant types that you want to use for this template. For details, see Grant Types in the *PingFederate Server* guide. **Note** Some grant types might not be available with your version of PingFederate.
To update scopes:	To add or update scopes, search for them and select or deselect the scopes that you want to use for this template. For details, see Scopes in the *PingFederate Server* guide.
To update policy contracts:	Add, delete, or update the current attribute mappings in the PingFederate policy contract associated with this template. For details, see Attribute contracts in the *PingFederate Server* guide. **Important** If you update a policy contract, a new contract is created in PingFederate, and you will be prompted to name it. **Note** If a template is associated with an environment that is deleted, you will not be able to update OIDC policy information for the template.

4. Click **Save**.

   If you updated the grant types, scopes, or policy contract information, the **Save Template** window displays and reminds you that you are creating a new version of this template. Applications created from the previous template will not change until you update the application to the latest template version. Briefly describe the updates you made to the template in the **Comments** field for tracking purposes and click **Save**.

Reverting templates to previous versions

The history of each template is available to review and compare with previous versions. You can see which administrator modified the template configuration or policy contract, when it was modified, and details regarding these modifications. You can revert templates to previous versions if necessary.

Steps

1. To review the template history, click the **Expand** icon associated with the template, and then click the **History** tab.
2. Click the **Details** link associated with each template version to see its configuration.
3. Click the **Diff with Current Version** toggle to see the differences between this version and the most recent version.
4. To restore this version as the current version, click **Restore This Version**.

   Result:

   A new version of the template is created that matches the configuration of the version that you want to restore.

   > **Note**
   >
   > The template revision numbers increment on a system-wide level, not on a per-template basis. So the first time any template in PingCentral is changed, it will have a revision of 1. A change made to a completely different template results in a revision of 6, and so forth. Reverting a template generates another revision, which again increments on a system-wide basis.

SAML 2.0 and PingAccess templates

Add, update, or delete SAML and PingAccess templates to meet your needs, or revert them to previous versions, as necessary.

To add a SAML or PingAccess template, select a configuration to replicate. PingCentral retrieves this configuration and saves it as a template, which serves as a building block for future applications.

Adding SAML application templates

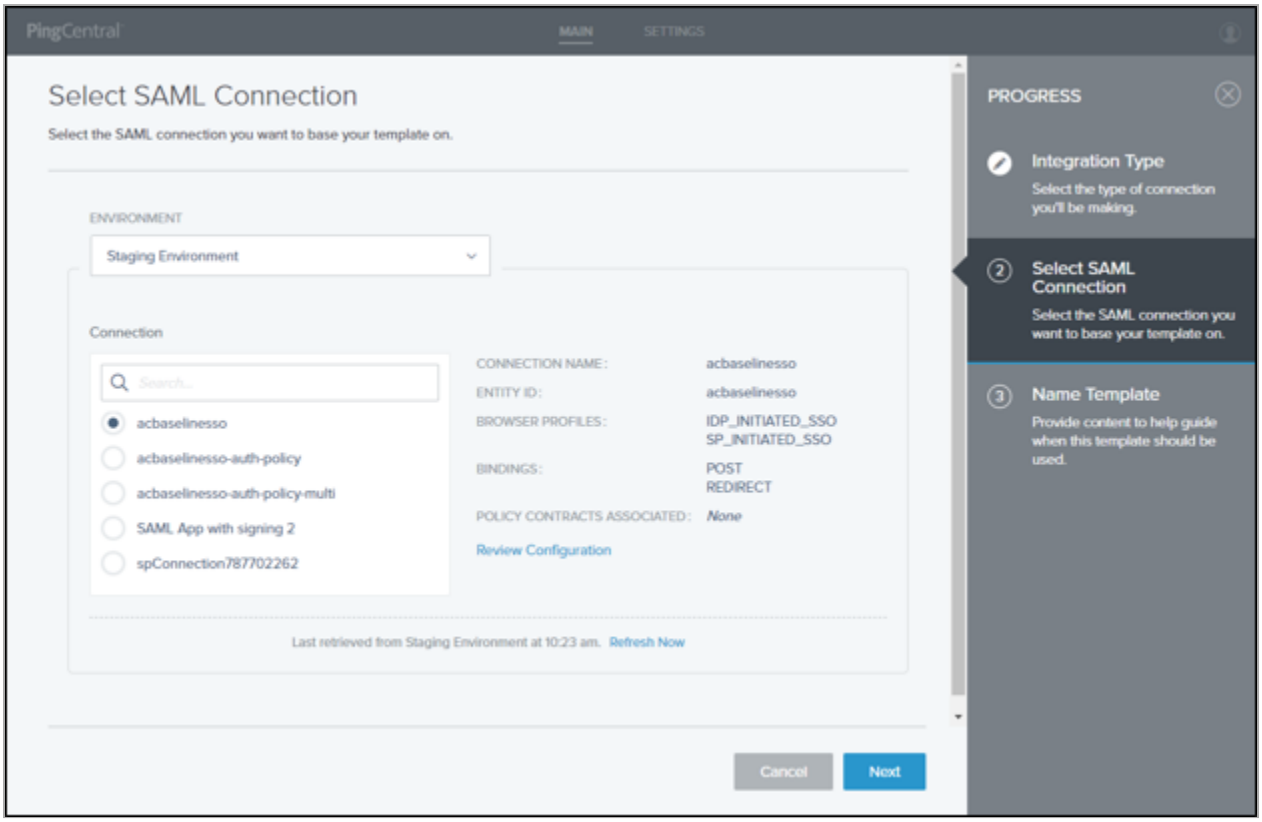
Steps

1. All templates are listed on the **Templates** page. To add a new template, click **Add Template**.
2. On the **Integration Type** page, select **SAML**. Click **Next**.
3. On the **Select SAML Connection** page, select the PingFederate environment that hosts the connection you want to use as a template, and then select the connection from the **Connection** list.

> **Note**
>
> If an environment is offline or if a PingCentral administrator has set the environment status to **Disabled**, you will be unable to select a disabled environment for template creation.

Result:

Details regarding the connection display.



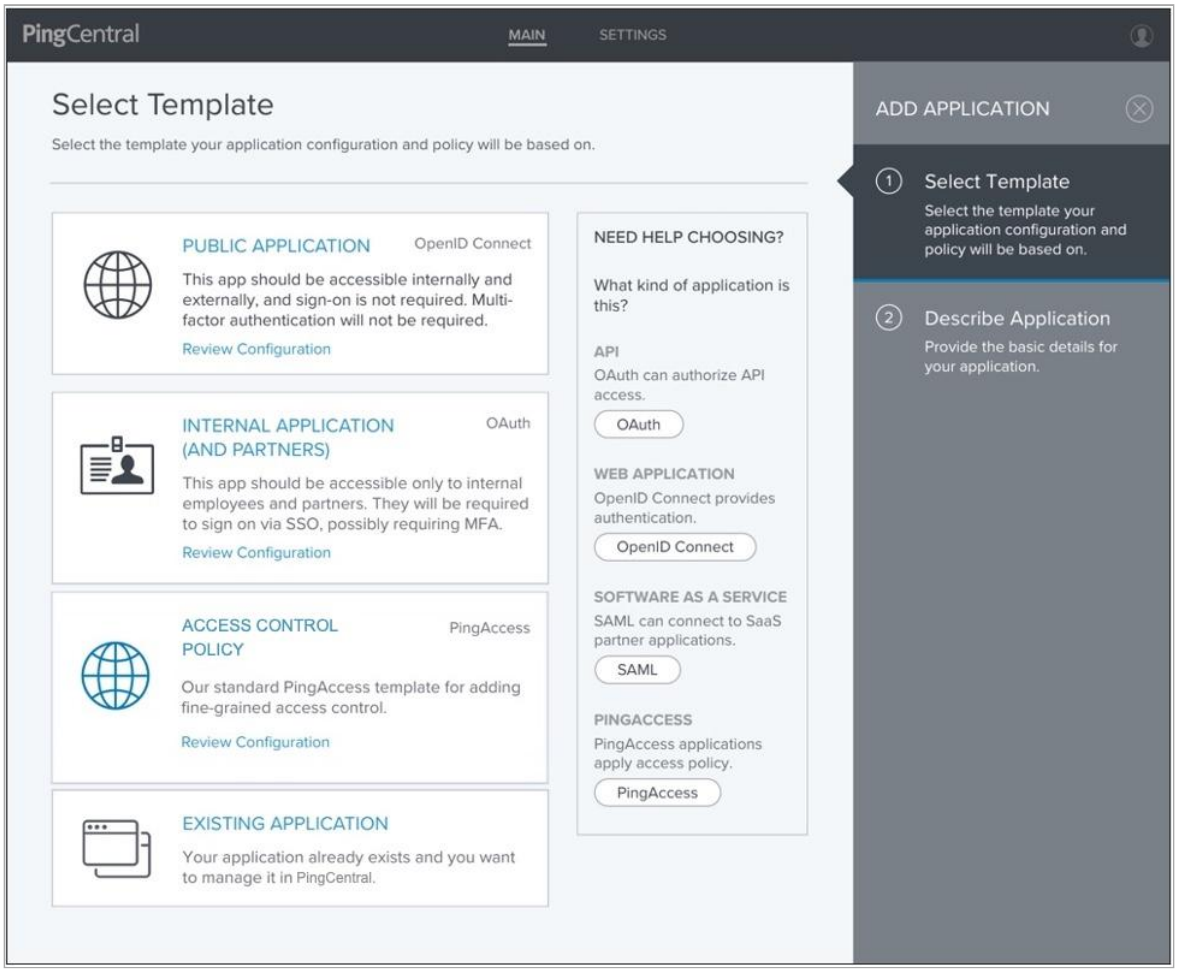
4. To see the JSON for the SAML connection, click **Review Configuration**.
5. On the **Name Template** page, add a name and description for your template.

   This information will help application owners select the appropriate template.
6. Select an icon to represent your template.

   The icon you choose is shown with the template name and description.
7. **Optional:** If multiple authentication policy contracts exist in the underlying connection, choose the desired contract from the **Authentication Policy Contracts** list.
8. Click **Save and Close**.

   Result:

   You see the new template in the list of available application templates. Application owners see the new template on the**Select Template** page.



For SAML SP connection templates, the following items are saved:

- Connection information
- Attribute names and, if applicable, attribute sources defined in the associated authentication policy contract

Updating SAML and PingAccess templates

Applications based on outdated templates have **Outdated Template** icons associated with them, which inform application owners of changes.

Steps

1. To update a SAML or PingAccess template, click the **Expand** icon associated with the template.
2. If the template is based on an outdated configuration, you can click the **Sync** button to sync the template with the latest configuration available.
3. Click the **Pencil** icon.

   All of the editable information is on one page.
4. Update the information in the **Name** and **Description** fields or select a new icon to represent the template.
5. Click **Save**.

Reverting templates to previous versions

The history of each template is available to review and compare with previous versions. You can see which administrator modified the template configuration or policy contract, when it was modified, and details regarding these modifications. You can revert templates to previous versions if necessary.

Steps

1. To review the template history, click the **Expand** icon associated with the template, and then click the **History** tab.
2. Click the **Details** link associated with each template version to see its configuration.
3. To restore this version as the current version, click **Restore This Version**.

   Result:

   A new version of the template is created that matches the configuration of the version that you want to restore.

   > **Note**
   >
   > The template revision numbers increment on a system-wide level, not on a per-template basis. So the first time any template in PingCentral is changed, it will have a revision of 1. A change made to a completely different template results in a revision of 6, and so forth. Reverting a template generates another revision, which again increments on a system-wide basis.

Deleting templates

Steps

1. Click the expandable icon associated with the template to view template details.
2. To delete the template from PingCentral, click its associated **Delete** icon.

   > **Note**
   >
   > You cannot delete templates that are still associated with applications.

   Result:

   A message opens, asking you if you want to delete the template.

3. Click **Delete**.

   Result:

   A message opens, saying that the template was deleted.

Promotion processes

PingCentral makes it possible for application owners to promote their OAuth, OpenID Connect (OIDC), SAML, and PingAccess applications to development environments themselves.

After applying the templates to their applications, application owners enter information about their target environments into PingCentral and promote their applications to the designated environment.

The templates contain the raw JSON from the model applications on which the templates were based. Although PingCentral saves this information, it doesn't modify it. Instead, the saved JSON is used as a starting point for creating new applications and is modified only in memory with the environment-specific information during the promotion process.

After an application is promoted, you can revert them to previously promoted versions. The reverted version of the application won't exist outside of PingCentral until it's promoted again, at which point it's also available in PingFederate or PingAccess. For details, see Reverting applications to previously promoted versions.

> **Note**
>
> If an environment is offline or if a PingCentral administrator has set the environment status to **Disabled**, application owners will be unable to promote the application to a disabled or offline environment.

OAuth and OIDC application promotions

When promoting OAuth and OpenID Connect (OIDC) applications, application owners provide this information:

- **Redirect URIs**: The trusted location that the application is redirected to with the authorization code or access token after the OAuth flow is complete. Redirect URIs are only required when promoting applications that use an authorization code and implicit grant types.
- **Client secret**: Used if a client secret is required to authenticate the application. Application owners can generate a client secret or create one of their own.

To learn more about this process, see Promoting OAuth and OIDC applications in the *PingCentral for Application Owners guide*.

During the promotion process, the application name and description remains the same. If PingCentral identifies an identical client in PingFederate, the application JSON, along with the information that the application owner provides, overwrites the PingFederate OAuth client within the target environment. If the client doesn't already exist, PingCentral creates all of the items defined in the application JSON, along with the information that the application owner provided.

If the **Allow JSON editing for application promotions** option is enabled for the environment, application owners are able to edit the underlying application JSON when they promote their OAuth client applications.

If OAuth clients have ATMs, OIDC policies, or scopes that conflict with the target environment during the promotion process, PingCentral does not change them because they could be shared across clients. Otherwise, PingCentral adds the ATMs, OIDC policies, and scopes specified in the original JSON file. If scopes are added, they're defined as exclusive scopes and are associated with the client upon promotion.

While PingCentral does not promote the policy contract to persistent grant mappings, it promotes all access token mappings associated with the client, which are determined by the access token managers associated with the client. Only access token mappings that use the default, client credentials, or authentication policy contract contexts will be promoted.

SAML SP application promotions

When application owners add an application to PingCentral, they can provide an `.xml` file that contains service provider metadata from a similar SAML application. This file might contain any or all of these items:

- **Entity ID**: Uniquely identifies the application.

- **ACS URL**(s): The application's URL to which SAML assertions from the identity provider are sent after user authentication occurs.
- **SLO Service URL**(s): the application's URL utilized for single logout (SLO) functionality.
- **Attribute mapping information**: The application attributes are mapped to the identity attributes required to fulfill the authentication policy contract in PingFederate.
- **SP public certificate**: Used to prove ownership of a public key and obtained from the service provider.
- **Assertion encryption certificates**: Used to prove that the SAML assertion is encrypted.

Alternatively, they can provide the Entity ID, ACS URL, and certificates during the promotion process.

If the **Allow JSON editing for application promotions** option is enabled for the environment, application owners are able to edit the underlying application JSON when they promote their SAML SP applications.

Application owners are also asked to provide a signing certificate during the promotion process. They can select an existing PingFederate signing certificate, or the environment default certificate, if one exists. The default certificate is the certificate added to the environment when it was created or last updated. If signing certificates are not available in the PingFederate environment and an environment default certificate is not available, or if an environment default certificate is available but expired, they can choose to automatically generate a certificate.

To learn more about this process, see Promoting SAML applications in the *PingCentral for Application Owner's guide*.

During the promotion process, the application name and description remains the same. If PingCentral identifies an identical connection in PingFederate, the application JSON, along with the information that the application owner provides, overwrites the PingFederate connection within the target environment. If the connection does not already exist, PingCentral creates items defined in the application JSON, along with the information that the application owner provided.

PingAccess application promotions

The information required to promote PingAccess web applications, API applications, and Web + API applications to PingAccess environments varies by type and includes:

- **Virtual host**: The public-facing host name and host port required to promote all applications. For example, den.ping.com:8443.
- **Access validation method**: If the application is an API or Web + API application, owners can specify the access validation method, whether it be a token provider or a token validator, if appropriate.
- **Web session**: If the application is a Web + API application, owners are required to select a web session from a drop-down list. This information isn't required to promote web or API applications.
- **Identity mapping**: Owners can select identity mappings from drop-down lists for web, API, and Web + API applications.
- **Site** or **Agent** name: Owners specify the name of the site for gateway deployments and the name of the agent in an agent deployment.

To learn more about this process, see Promoting PingAccess applications in the *PingCentral for Application Owners guide*.

Reverting applications to previously promoted versions

When you revert applications to previously promoted versions, the reverted versions of the application will not exist outside of PingCentral until you promote them again, at which point they will also be available in PingFederate or PingAccess.

Steps

1. On the **Applications** page, locate the application you want to revert to a previously promoted version.

   > **Note**
   >
   > You cannot revert applications created in previous versions of PingCentral.

2. Click the expandable icon associated with the application, select the **Promote** tab, and then click **View Details**.
3. In the **Promotion Details** window, click **Revert Application**.

   Result:

   A message displays asking you if you are sure you want to revert this application.

4. Click **Revert**.

   Result:

   The reverted version of the application displays in your applications list.

   > **Note**
   >
   > Reverting OAuth and OIDC applications to previously promoted versions overrides client secrets, so you will need to create or generate new secrets before you promote them again. Reverting SAML applications to previously promoted versions overrides the Entity IDs, ACS URLs, and certificates, so you might need to update this information before you promote them again.

Managing approvals (administrators)

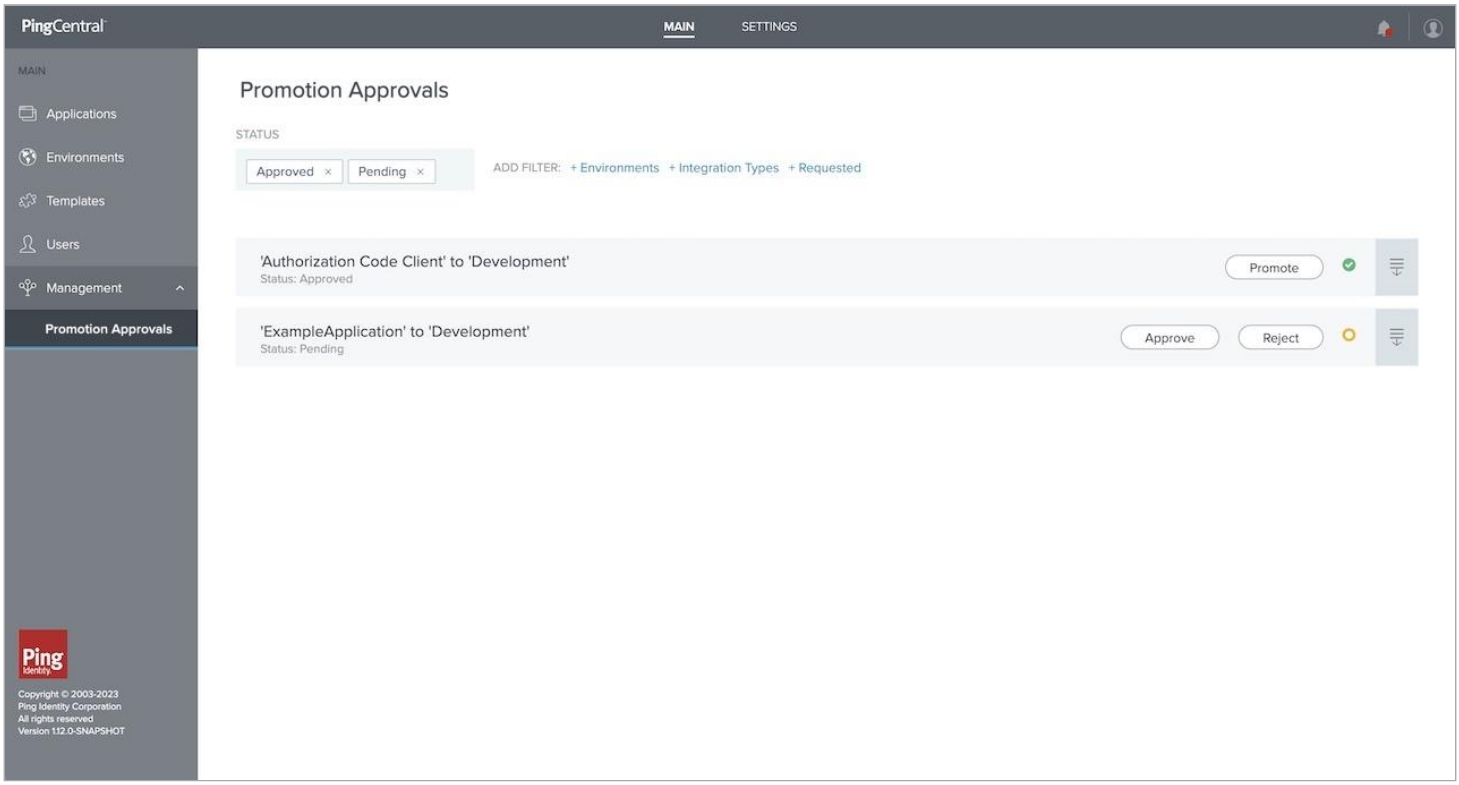
When an application owner submits an application for promotion approval, administrators can view the application and its approval status on the **Promotion Approvals** page, located under the **Management** tab.

About this task

From this page, you can:

- Filter for approved, promoted, pending, rejected, or canceled approvals, or by environments or integration type. Use the **Visible** filter, which is enabled by default, to hide approvals that are in a canceled, promoted, or rejected status.
- **Approve**, **Approve and Promote**, or **Reject** an approval.

> **Note**
>
> You see a bell icon in the top navigation bar when there are pending approval requests.



Steps

1. Select your filters.

   You can filter by:

   - **Status**: **Approved** or **Pending**. The page automatically filters for any approved and pending approvals.
   - Environments.
   - Integration types (OAuth and OIDC or SAML).
   - Requested (the user that made the request).

   Click the filters to add or remove them.

2. To approve promotion requests from application owners, click **Approve** in the row for the promotion request that you want to approve.

   > **Note**
   >
   > If the **Allow JSON editing for application promotions** is enabled for the targeted environment and the promotion request requires approval, you'll be able to compare the submitted application JSON to the original application JSON.

   1. **Optional:** To approve the request and promote the application to an environment, after you click **Approve**, select the **Promote Application to Environment** check box in the dialog that opens, and click **Approve** to approve the request and promote the application.

      For more information, see Promotion processes

> **Note**
>
> If an environment is offline or if a PingCentral administrator has set the environment status to **Disabled**, you will see a note indicating that the environment is inaccessible, and you will be unable to promote the application while the environment is disabled or offline.

3. To reject an approval request, click **Reject** in the row for the request that you want to decline.
    1. **Optional:** Supply a rejection explanation in the dialogue box that displays.

PingCentral for Application Owners

Introduction to PingCentral

Use PingCentral to add user authentication and authorization support to your applications, promote them to the appropriate development environments for testing, and monitor them throughout their life cycles.

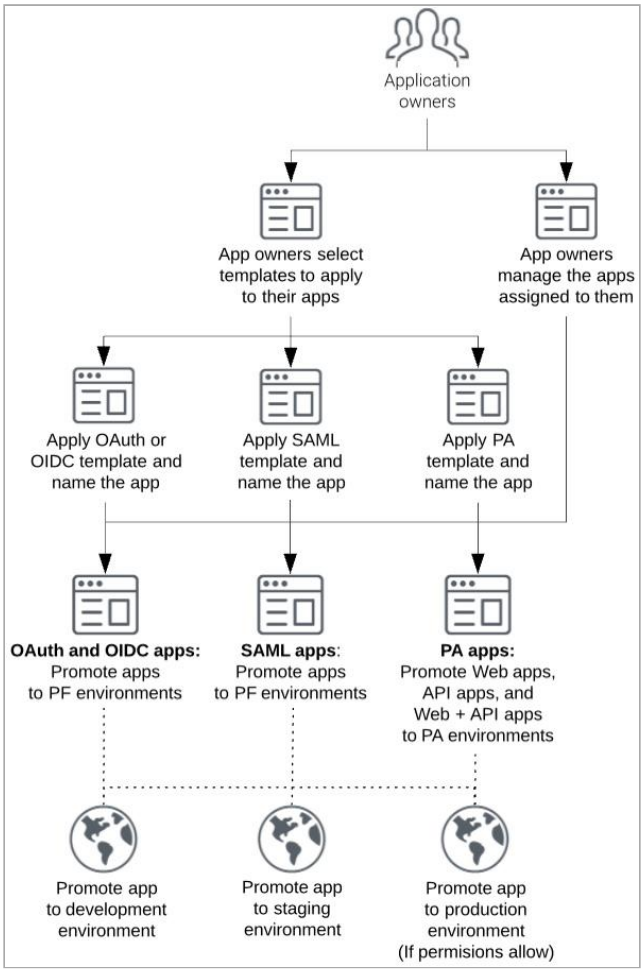
PingCentral:

- Makes it possible for you to apply security configurations to your applications without assistance from an administrator.
- Allows you to promote these applications yourself, when you are ready, rather than submitting a request and waiting for someone else to promote them for you.
- Provides a central monitoring location for greater visibility into applications across deployment life cycles.
- Minimizes the risk of promoting applications with vulnerable security policies within your organization.

Using PingCentral does not require extensive training. However, for the best possible experience, become familiar with how the platform works before getting started.

How PingCentral works

1. IAM Administrators create OAuth, OpenID Connect (OIDC), SAML, and PingAccess templates based on clients, connections, and application security configurations they think are worth replicating.
2. Administrators can also add clients, connections, and applications directly to PingCentral and assign owners to them.
3. You use SAML, OAuth, OIDC, and PingAccess templates to apply security configurations to your applications. A wizard guides you through the process of providing a name and description for each application you add to PingCentral. Another wizard guides you through the process of promoting your application to the target environment.
4. When you're ready, promote applications to the appropriate development environments to test them and promote them directly to production environments if your permissions allow.



Accessing PingCentral

PingCentral is a web-based application that you access from a URL. For the best possible experience, use Chrome or Firefox as your browser.

Steps

1. Contact your IAM Administrator for the PingCentral URL and your sign-on credentials.
2. Enter your credentials.

> **Caution**
>
> If you have multiple failed login attempts, you wil be locked out of PingCentral for a short period of time.

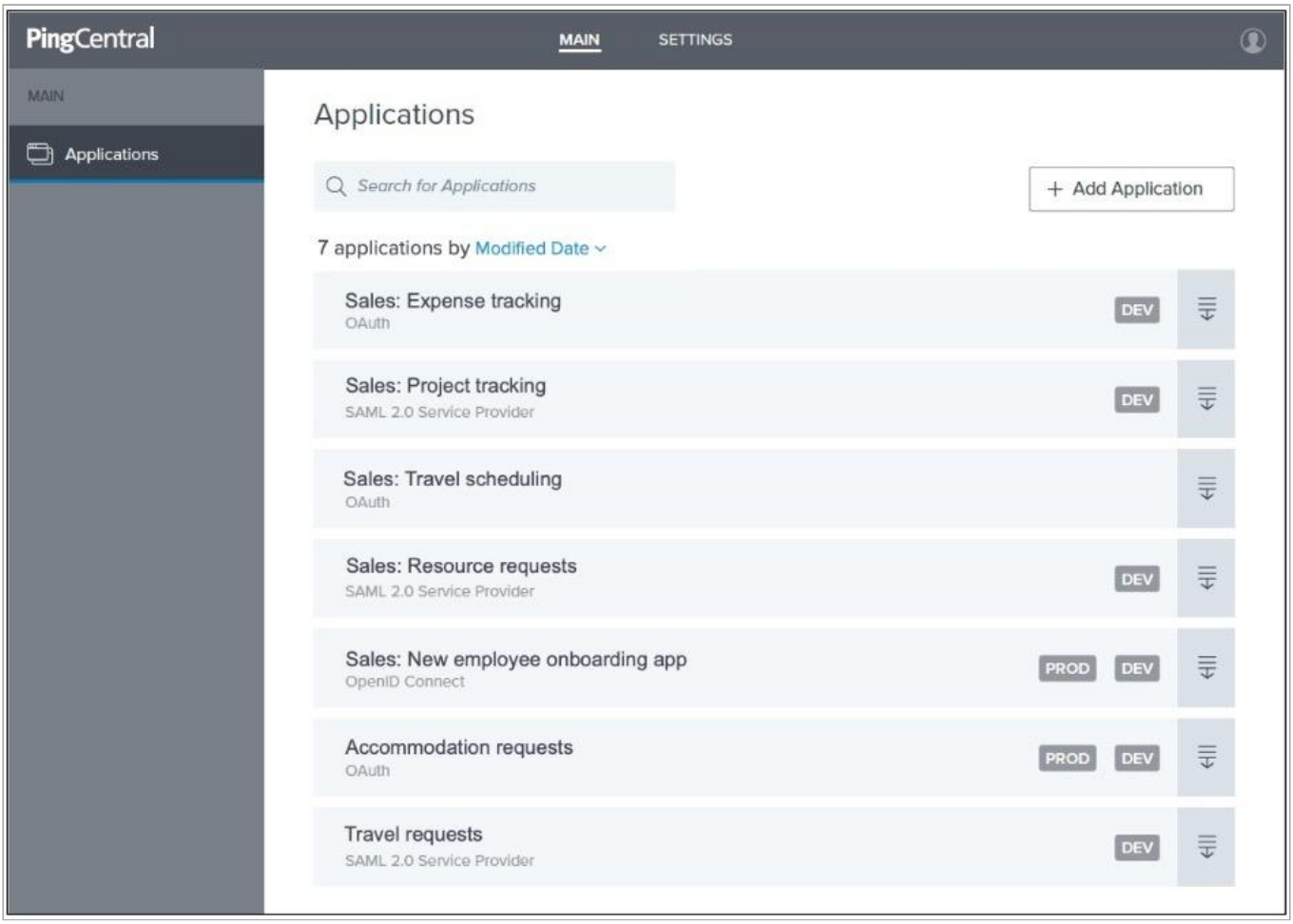
Managing applications

If you are an owner of an application, the application displays on the **Applications** page. From this page, you can add new applications, view and update existing applications, and delete them from PingCentral when they are no longer needed.

Steps

1. Use the menu at the top of the page to sort the list of applications by modified date or by application name, or use the search feature to locate an application by name.

   OAuth, OIDC, SAML, and PingAccess applications are listed in the order in which they were last modified, by default, with the most recently modified at the top of the list.



2. On the **Applications** page, you can:

   - View information about an application. Click the expandable icon associated with it.

     For more information, see Viewing application information.

   - Add a new SAML, OAuth, or OIDC application to PingCentral. Click **Add Application**, select a template, and follow the wizard prompts.

     For more information, see Adding applications.

     > **Note**
     >
     > Administrators can also assign you as the owner of an application, in which case the application will display on your **Applications** page.

- Promote applications to development or production environments. Click the expandable icon associated with the application you want to promote and click the **Promote** tab. For more information, see Promoting applications.
- Delete an application from PingCentral. Click its associated **Delete** icon.

  Choose from:

  - To delete an application from PingCentral only, click the **Delete** button.
  - To delete an application from all environments, depending on the application type, select the **Delete from PingFederate in all environments** or **Delete from PingAccess in all environments** check box and click the **Delete** button.

> **Note**
>
> If a PingCentral administrator restricts access to application deletion, you cannot delete applications from PingFederate or PingAccess.

Viewing application information

If you are an owner of an application, the application displays on the **Applications** page.

Steps

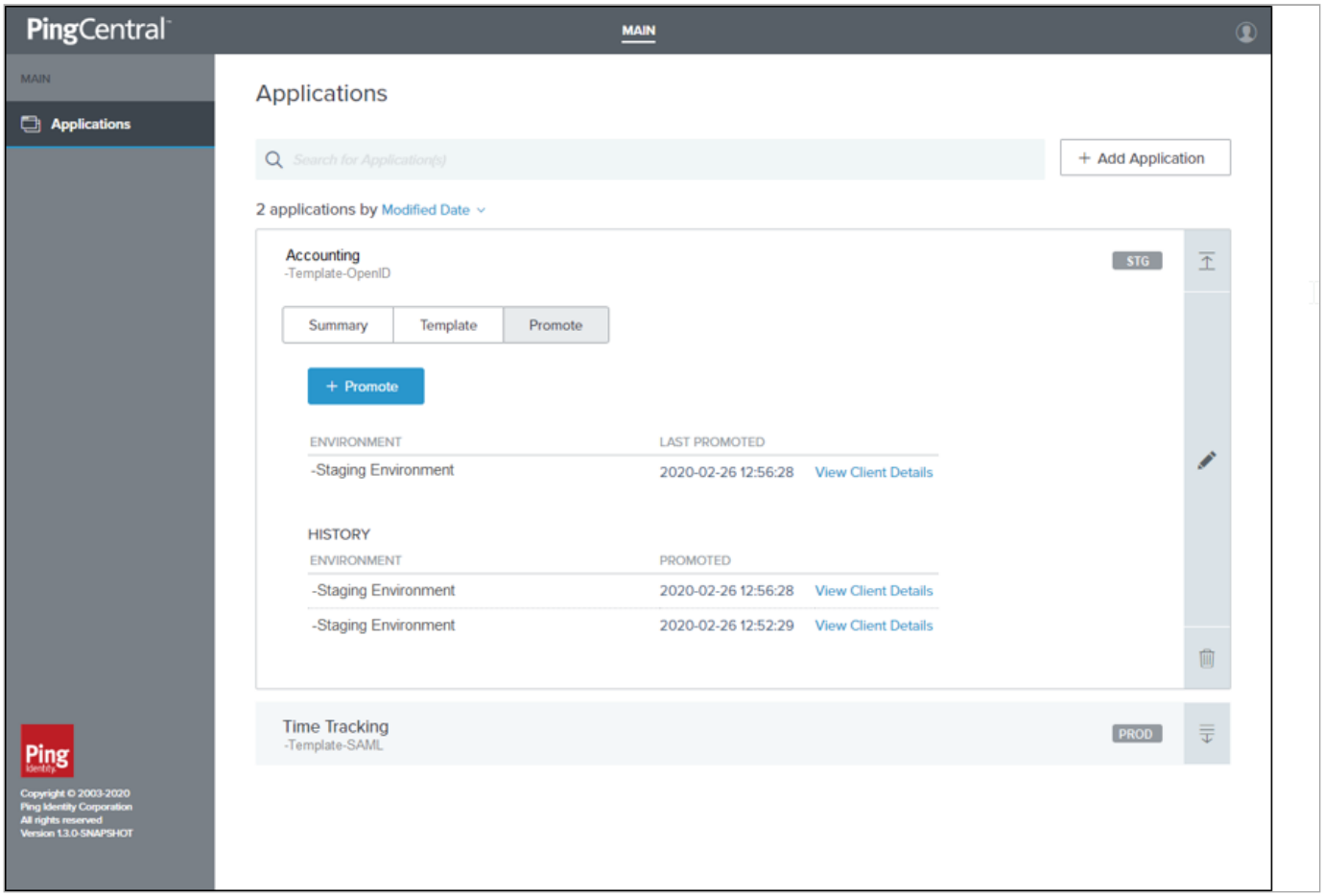
1. Use the menu at the top of the page to sort the list of applications by modified date or by application name, or use the search feature to locate an application by name.

   Result:

   Security Assertion Markup Language (SAML), OAuth, OpenID Connect (OIDC), and PingAccess applications are listed in the order in which they were last modified, by default, with the most recently modified at the top of the list.

2. To view details regarding an application, click the expandable icon associated with it.

   Applications promoted to development environments (such as development, staging, or production) display icons associated with each environment. If an application has not yet been promoted to a specific environment, you will not see an icon representing that environment.



3. To review additional information about the application, click each tab.

    - **Summary tab**: This tab displays the application or connection name, description, owners, the date on which the application was last modified, and additional information specific to the application, client, or connection.
    - **Template tab**: This tab displays if the application was created from a template. It includes the name of the template applied to the application, and details regarding the application, client or connection on which the template was based.
    - **Client tab**: This tab displays if the application was created from an OAuth or OIDC application that was directly added to PingCentral from PingFederate. It includes the client name, ID, grant types, attributes, and applicable policies.
    - **Connection tab**: This tab displays if the application was created from a SAML application that was directly added to PingCentral from PingFederate. It includes the name of the connection, browser profiles, and binding information.
    - **Application tab**: This tab displays if the application was directly added to PingCentral from PingAccess. It includes the application name, description, and details regarding the application.
    - **Promote tab**: This tab displays the promotion history of this application, which includes the date and time each promotion occurred.

> **Note**
>
> If an environment is offline or if a PingCentral administrator has set the environment status to **Disabled**, you may still view the application details, however, you will be unable to edit the application in a disabled or offline environment.

4. To access additional information regarding the application and its promotion history, click **View Client Details**.

Adding applications

Before you can promote applications to development environments for testing, you must add them to PingCentral.

To add applications to PingCentral, you can use OAuth, OIDC, SAML, and PingCentral templates to apply security configurations to your applications. Wizards guide you through these processes.

See the following:

- Selecting a template
- Using OAuth and OIDC templates
- Using SAML templates
- Using PingAccess templates

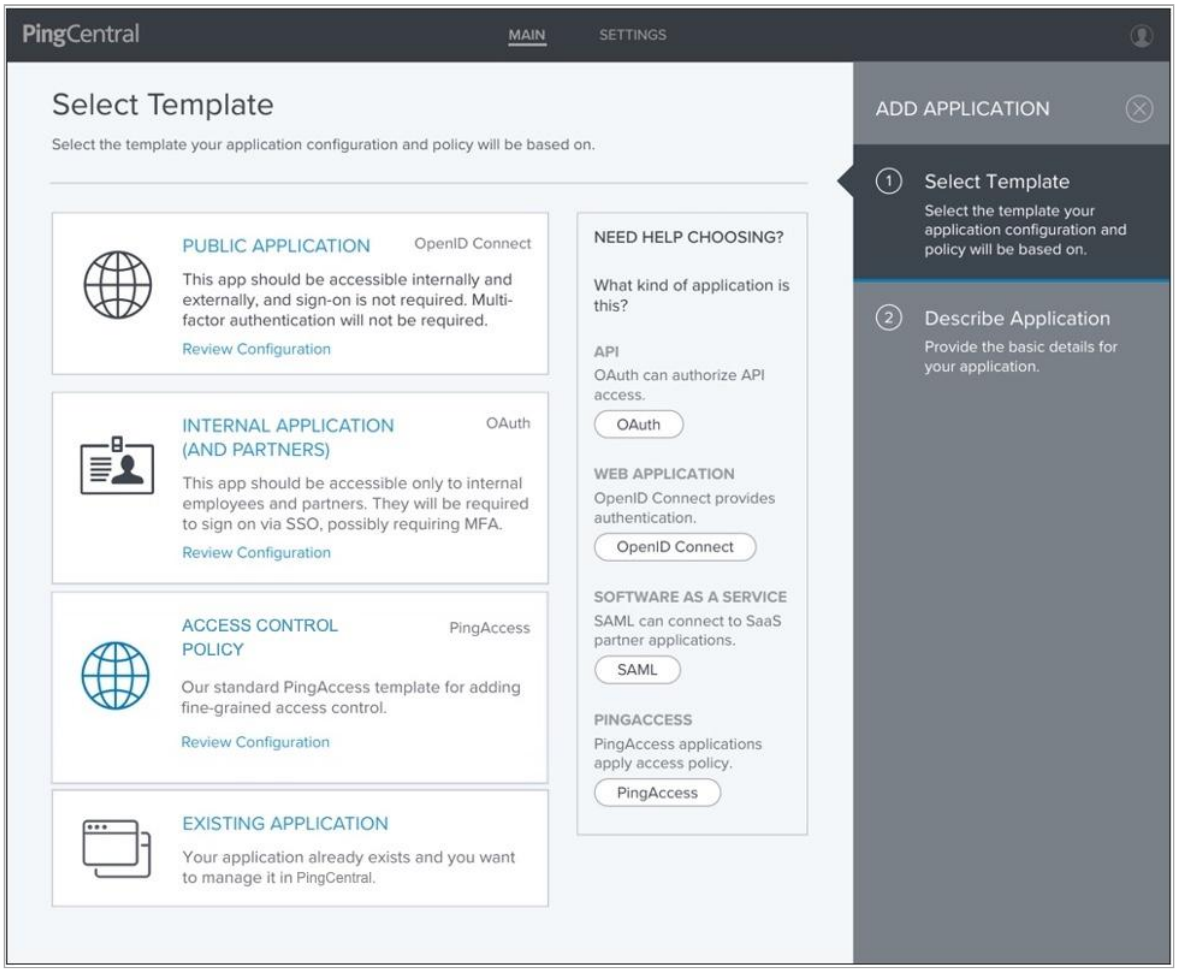
Administrators can also assign applications directly to you. These applications display on your **Applications** page, where you can promote them, test them on development environments, modify them, and manage them throughout their life cycles.

Selecting a template

IAM Administrators can create OAuth, OpenID Connect (OIDC), Security Assertion Markup Language (SAML), and PingAccess templates and make them available for you to use to apply security configurations to your application.

Steps

1. Click **Add Application**.
2. Review the template descriptions to determine which template you should use.



Result:

On this page, you can:

- Select the filtering options to filter OAuth, OpenID Connect, SAML, and PingAccess templates.
- Click the **Review Configuration** link within the template description to view the details associated with each template.

If you are unclear about what type of template to select, keep the following in mind:

- OAuth and OIDC are most commonly used by consumer applications and services so users do not need to sign up for a new user name and password. "Sign in with Google," or "Log in with Facebook" are examples of OAuth protocols you are likely familiar with. You might also use OAuth if your application is consumed on a mobile device.
- SAML is most commonly used by businesses to allow their users to access services they pay for. Salesforce and Gmail are examples of service providers an employee could gain access to after completing a SAML sign on. SAML templates can also be used for web applications created and used within your organization.
- PingAccess templates can be used to apply access policy to Web and API applications.
- If an environment is offline or if a PingCentral administrator has set the environment status to **Disabled**, you will be unable to select a disabled or offline environment for template creation.

3. Select the template you want to use, or the existing application you want to add to PingCentral and click **Next**.

4. To proceed, see the appropriate topic:

   Result:

   - Using OAuth and OIDC templates
   - Using SAML templates
   - Using PingAccess templates

Using OAuth and OIDC templates

After selecting an OAuth or OIDC template, use that template to apply user authentication and authorization support to an application.

Before you begin

Prepare to provide the following:

- Name of the application.
- A brief, accurate description of your application.
- Scopes, which are optional and can be customized to meet your needs. See Scopes and scope management in the PingFederate documentation for additional information.

Steps

1. If you want to add scopes to the applications, begin typing the name of the scope you want to add and select it from the list when it displays.

   > **Note**
   >
   > The names of scopes added to applications cannot contain spaces, nor can the **Scopes** field contain spaces before or after the scope name. If spaces exist, applications cannot be successfully promoted.

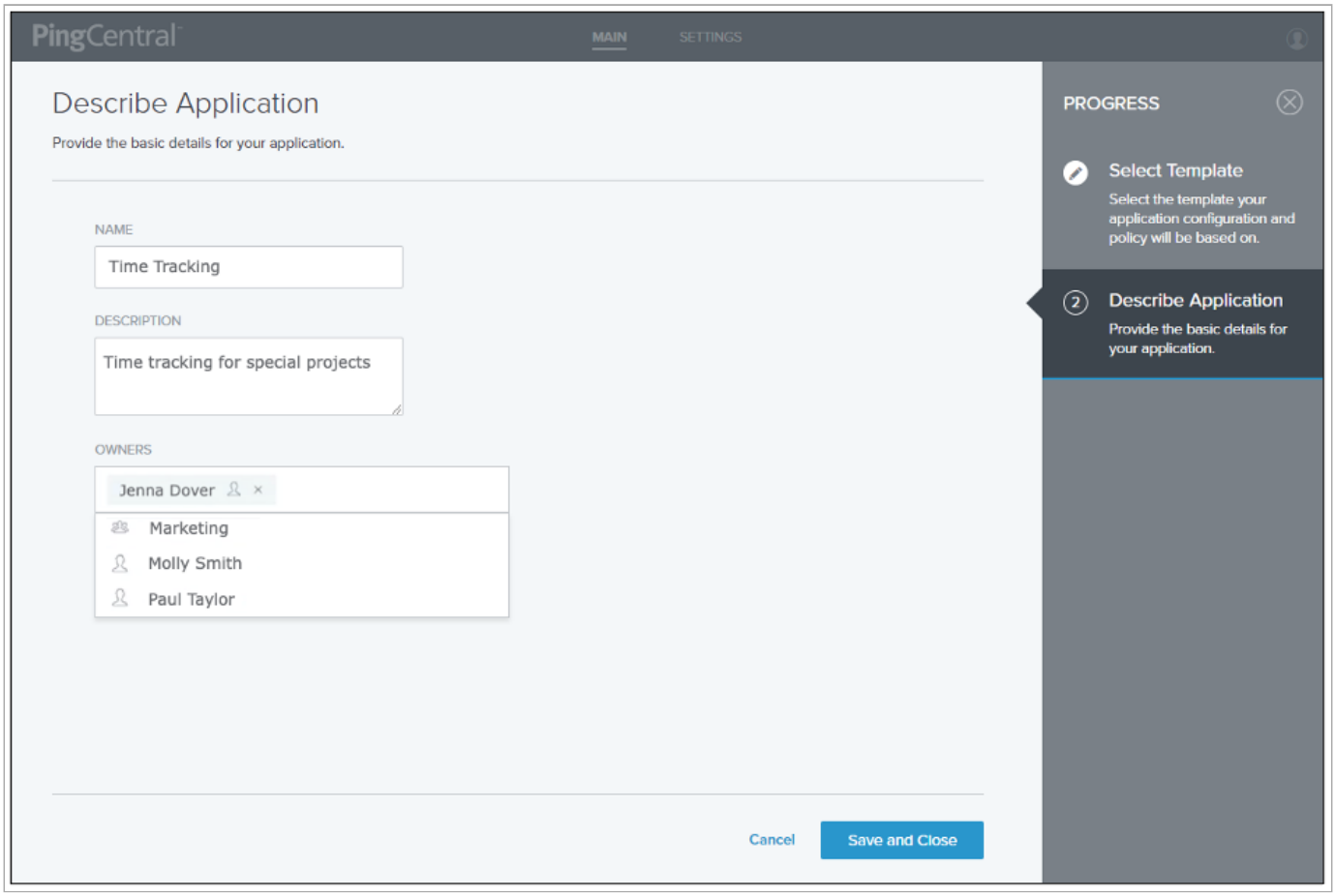
   When this application is later promoted, the target PingFederate scope management configuration is referenced to satisfy the scope requirements of the client. Any named scope identified as a common scope in the target environment is configured within the client as a restricted scope.

   If the named scope does not exist in the target environment, the scope is created as an exclusive scope. In that case, or if the scope already exists as an exclusive scope, then the scope is associated with the client as an exclusive scope.

2. Click **Next**.
3. On the**Describe Application** page, enter the name of your application and a description of the application in the **Name** and **Description** fields.

   You are adding this application to PingCentral, so your name will automatically populate the **Owners** field.

4. **Optional:** To add owners, or groups of owners, select additional owners from the **Owners** list. If the name you are looking for does not display in the list, contact your PingCentral administrator and request that the person be provisioned.



5. Click **Save and Close**.

The application appears at the top of the list of applications on the **Applications** page.

Using SAML 2.0 templates

After selecting a SAML template, use that template to apply user authentication and authorization support to an application.

Before you begin

You must provide:

- The name of the application.
- A brief, accurate description of your application.
- Attribute mapping information, used to map your application attributes to the identity attributes required from the identity provider to verify users' identities.

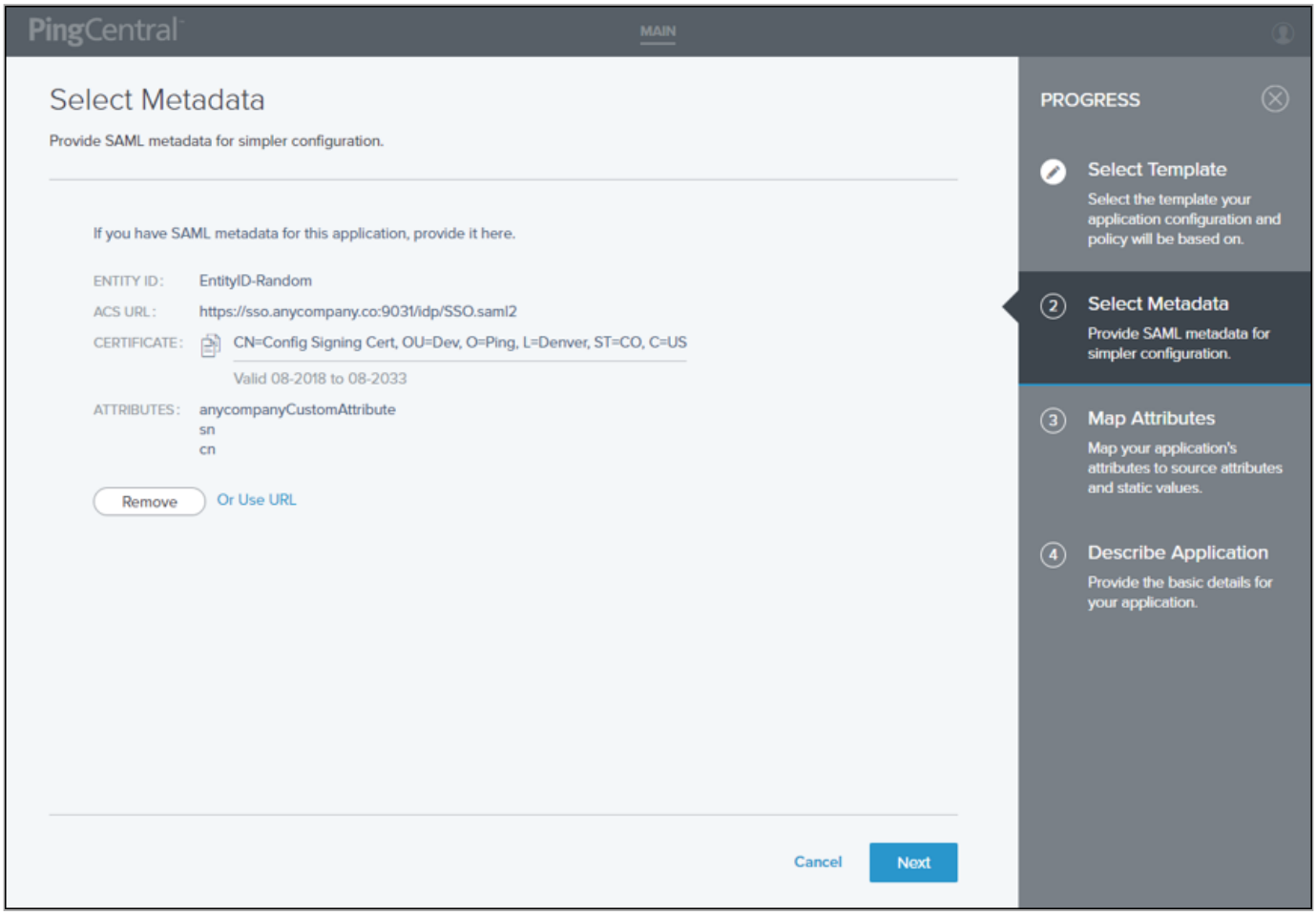
Steps

1. In PingCentral, on the **Select Metadata** page, complete one of the following tasks:

Result:

- Provide a metadata file from service provider (SP) connections, which might include entity IDs, ACS URLs, and certificates. Click **Choose file** to provide the file.
- Provide a URL to the metadata file. Click **Or Use URL** to provide the URL.
- Skip this step and provide the Entity ID, ACS URL, certificate, and attributes, or all of this information, during the promotion process.

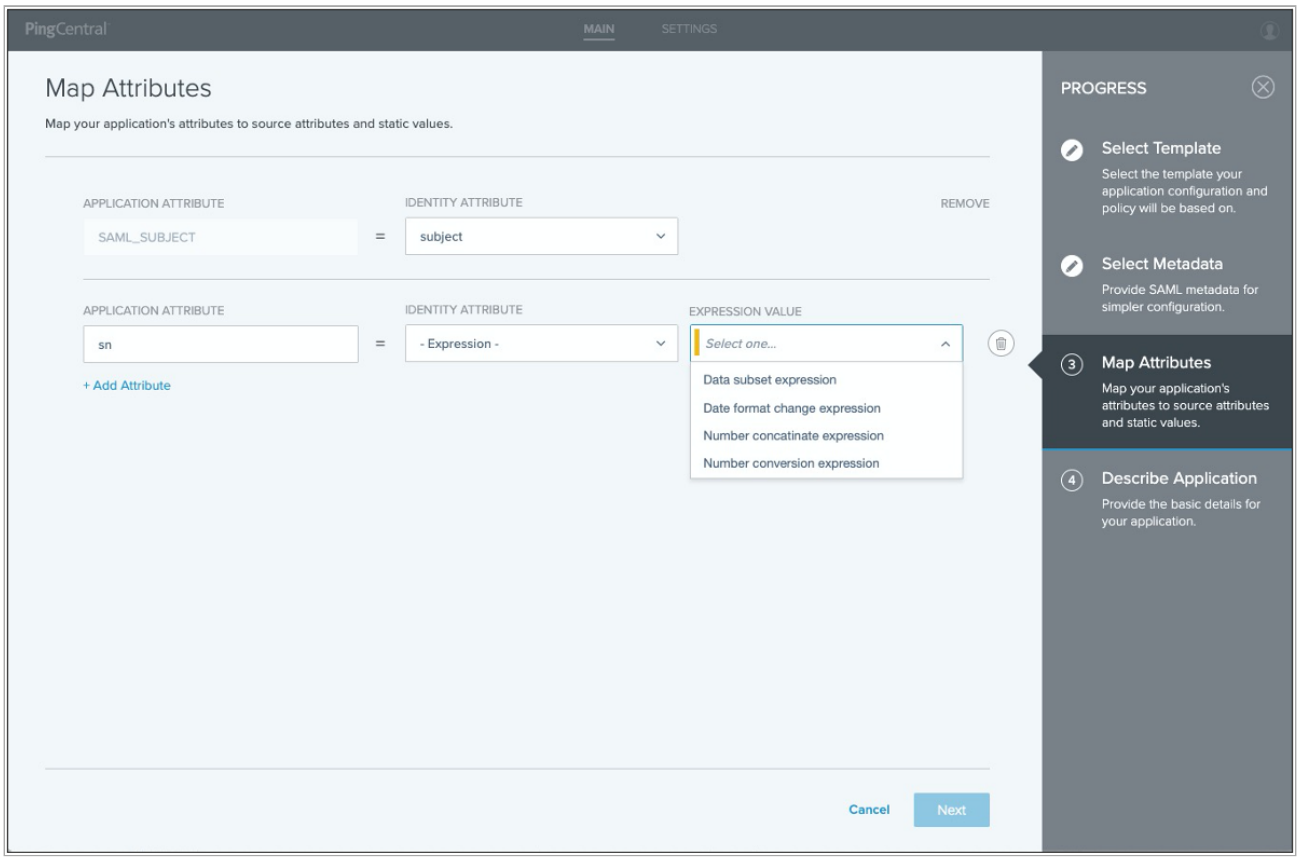
If you choose to provide a metadata file, the information in the file shows on the page.



2. Click **Next**.
3. On the **Map Attributes** page, to map the application attributes to the identity attributes required to fulfill the authentication policy contract in PingFederate, select identity attributes in the **Identity Attribute** list or click to add static values in the **Static Value** field.
    1. **Optional:** If attribute sources are defined in the underlying connection, select the **- Data Store -** identity attribute option and the applicable data store values.

        > **Note**
        >
        > To ensure successful promotion, the target PingFederate must have the necessary Data Stores with identical names as required for authentication policy contract mapping.

2. **Optional:** To define an OGNL expression and fine-tune attribute values to meet your needs, select the **- Expression -** identity attribute option and enter an **Expression Value** in the appropriate field.



4. When you're finished, click **Next**.
5. On the **Describe Application** page, enter the name of the application and a description in the appropriate fields.

   Result:

   You are adding this application to PingCentral, so your name will automatically populate the **Owners** field.
6. **Optional:** To add owners or groups of owners, click the **Owners** field and select additional owners in the list. Click **Next**.

> **Note**
>
> If the name you are looking for isn't showing in the list, contact your PingCentral administrator and request that the person be provisioned.

7. Click **Save and Close**.

   Result:

   The application is added at the top of the list of applications on the **Applications** page.

Using PingAccess templates

After selecting a PingAccess template, use that template to apply user authentication and authorization support to an application.

Before you begin

Prepare to define the following, as appropriate:

- The application context root and resources
- The application policy
- The resource policy
- The application name and description

For details regarding each of these items, see Information needed to add PingAccess applications.

Steps

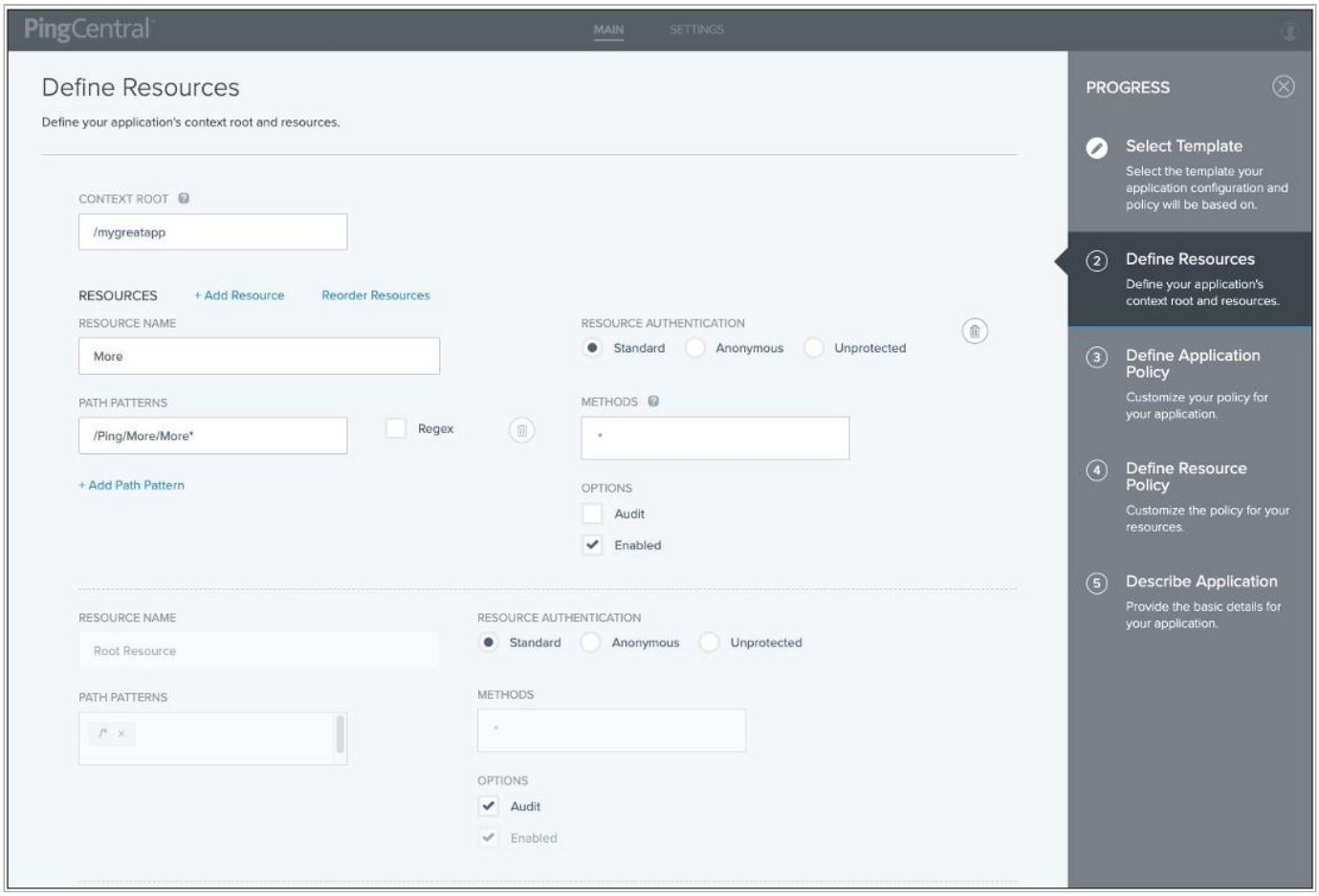
1. On the **Define Resources** page, enter the context root for the application.

   The context root is the common root of all application resources, specifies where in the URL path the application begins, and starts with a slash. In the example URL, `den-ping.com:8443/mygreatapp/home`, the `/mygreatapp` is the context root.

2. Add, delete, or reorder application resources for your application.

   Every application has at least one root resource.

   If resource reordering is available, a **Reorder Resources** link displays on the page, as shown in the following example. If resource ordering was not enabled in the PingAccess application that was used to create this template, it is not enabled in PingCentral.



> **Note**
>
> Virtual resources are available in PingAccess version 6.2 or later, but are not yet supported in PingCentral.

To add a new resource:

1. Click **Add Resource** and in the **Resource Name** field, enter the name of the resource.
2. In the **Path Patterns** field, enter a list of URL path patterns that identify this resource. Path patterns start with a forward slash (/), begin after the context root, and extend to the end of the URL. There are two different types of path patterns: Basic and Regex. Select the **Regex** option, when appropriate.
3. In the **Resource Authentication** section, select the type of authentication the resource requires.

   If the resource requires the same authentication as the root application, select **Standard**. If authentication is not required to access the resource, select **Anonymous** or **Unprotected**.
4. If the application is an API or Web + API application, in the **Methods** field, select the HTTP methods supported by the resource. Leave this field empty if the resource supports all methods.
5. To log information regarding requests to this resource, select the **Audit** check box.
6. Resources are enabled when they are added, by default. To disable a resource, clear the **Enable** check box.
7. If resource reordering is available, a **Reorder Resources** link displays on the page. To change the order of these resources, click the link, rearrange the resources, and click **Done**.

To delete the resource, click the associated **Delete** icon.

3. On the **Define Application Policy** page, customize the policy for the application, if needed.

   To apply rules or rule sets, drag them from the **Available Rules** list to the **Policy** list. Click **Next**.

4. **Optional**: On the **Define Resource Policy** page, customize the policy for each of your resources.

   To apply rules or rule sets to each resource, drag them from the **Available Rules** list to the **Policy** list. Click **Next**.

5. On the **Describe Application** page, enter the name of the application and a description in the appropriate fields.

   By adding this application to PingCentral, your name automatically populates the **Owners** field.

6. **Optional:** To add owners, or groups of owners, click the **Owners** field and select additional owners from the list. Click **Next**.

   If the name you are looking for does not display in the list, contact your PingCentral administrator and request that the person be provisioned.

7. Click **Save and Close**.

   Result:

   The application displays at the top of the list of applications on the **Applications** page.

Information needed to add PingAccess applications

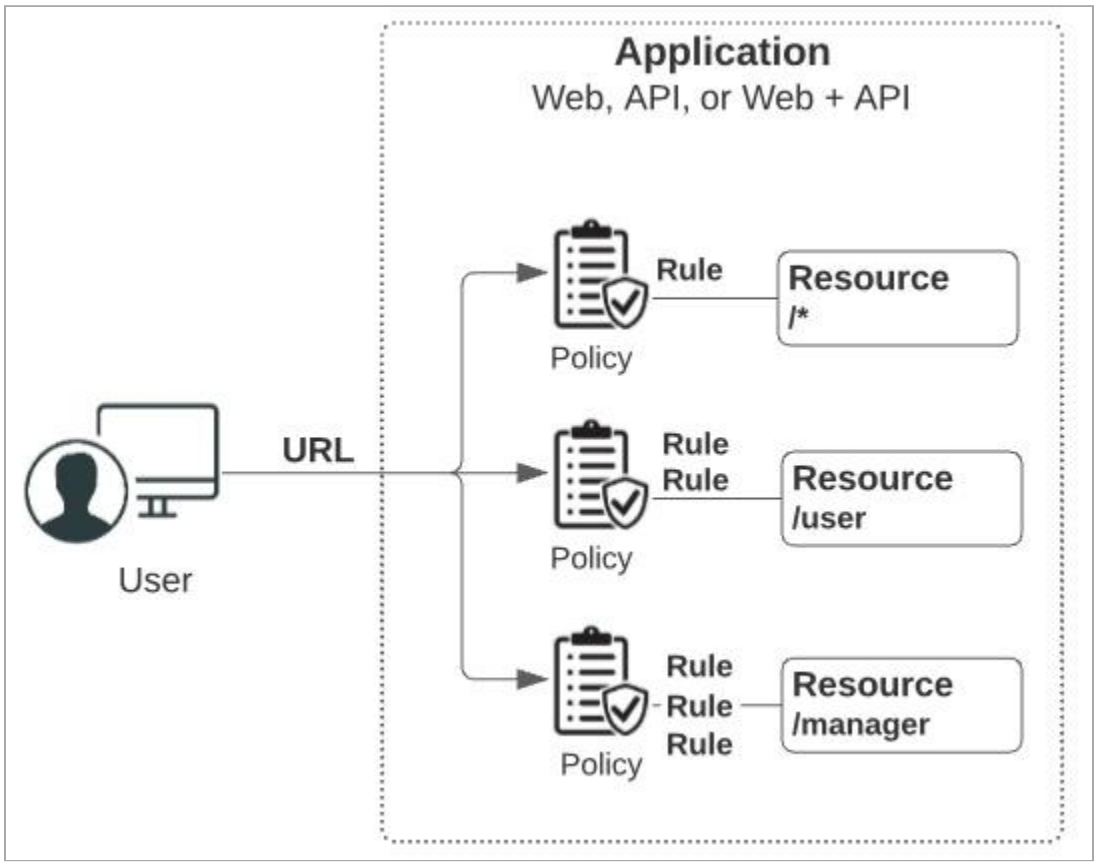
When you use templates to PingAccess applications to PingCentral, you provide the application context root and then define its resources, application policy, and resource policies. This section describes these items in detail and explains why you are prompted to provide this information.

There are three different types of PingAccess applications: Web, API, and Web + API. With Web + API applications, administrators can configure both Web and API settings for an application. These applications can switch between web and API processing behaviors on the fly based on whether the inbound request contains a web session cookie (Web) or an OAuth token (API).

Resources

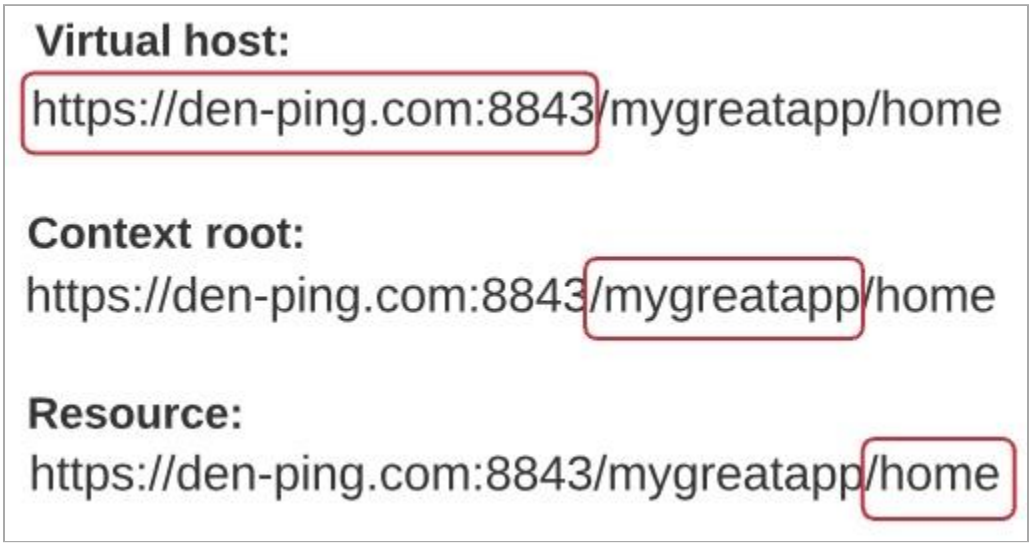
Resources

Each application consists of one or more resources, which you define in PingCentral. Resources are components of an application that require different levels of security. When you define resources within an application, you also define security regarding those resources.



Resources are protected by rules, which let you specify who can access your applications and resources, how and when they can do so, and what modifications can be made to the requested content. When rules, or sets of rules, are applied to applications and resources, they are called policies. Policies are applied to requests, which determine whether users are granted or denied access to the requested resource.

To access an application, users enter a URL. This URL consists of a virtual host, a context root, and the name of the resource they want to access.



When you use a template to add a PingAccess application to PingCentral, you are prompted to provide the context root and define the resources within it. For more information, see Application resources in the *PingAccess User Interface Reference Guide*.

Path patterns

Path patterns

When handling requests, PingAccess uses resource path patterns to match resources. There are two different types of path patterns: Basic and Regex.

- **Basic patterns**: The default path pattern type, which defines a path to a specific resource or a pattern that matches multiple paths. Basic patterns can contain any number of "*" wildcards. For example:

  ```
  /path/x/*
  ```

  matches any of these request paths:

  ```
  /path/x/
  /path/x/index.html
  /path/x/y/z/index.html
  ```

- **Regex patterns**: Regex patterns contain regular expressions and allow for more flexibility in resource matching as they support resource ordering. For example:

  ```
  /[^/]+/[a-z]+\.html
  ```

  matches any of these request paths:

  ```
  /images/gallery.html
  /search/index.html
  ```

  However, it would not match any of these request paths:

  ```
  /images/gallery2.html
  /search/pages/index.html
  /index.html
  ```

  > **Note**
  >
  > Although Regex path patterns function in an agent deployment, system performance might decrease if they are used. Agents are unable to interpret Regex path patterns, so they must consult PingAccess for policy decisions for each resource with a Regex path pattern.

When one or more path patterns match a request, PingAccess uses the first matching pattern it identifies, so the order in which path patterns are evaluated is important. By default, PingAccess orders path patterns automatically so that the most specific patterns are matched first. However, if more explicit control is needed, or if you are using regular expressions, enable resource ordering to manually specify the order in which path patterns are evaluated.

For example, an application might have three resources, such as:

- `/images/logo.png` (Basic)

- `/images/*` (Basic)
- `/.+/[a-z]\.png` (Regex)

A request to resource `/images/logo.png` is matched by all 3 path patterns, yet each resource can have different policy requirements. Resource ordering allows you to specify which of these path patterns is parsed first, further allowing you to control the policy that is applied to a particular request.

When you define the application resources in PingCentral, you are prompted to provide path pattern information. For more information, see Path patterns reference in the *PingAccess User Interface Reference Guide*.

Rules and policies

Rules and policies

Rules let you specify who can access your applications and resources, how and when they can do so, and what modifications can be made to the requested content. There are two different types of rules: access control rules and processing rules. Access control rules determine whether users can access a resource, and processing rules determine how requests are processed.

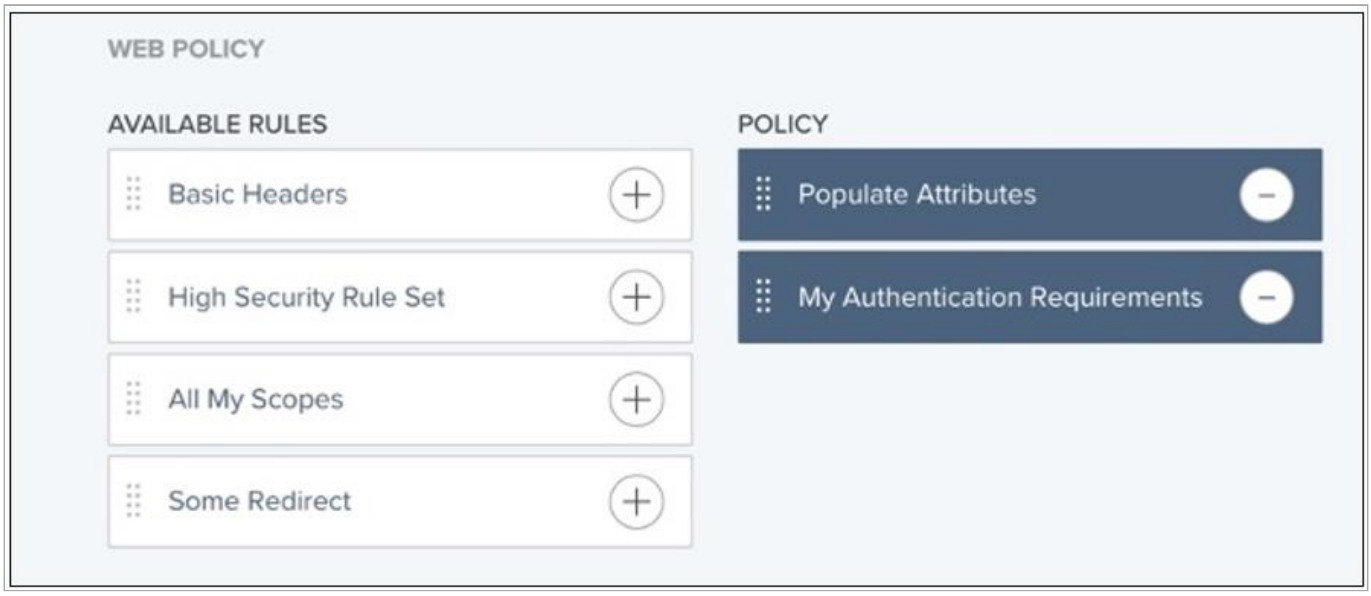
When you put rules together, they are called policies.

- **Application policies**: Rules applied to the application as a whole. You can define Web rules and API rules for Web + API applications.
- **Resource policies**: Rules applied to specific resources. Every application has at least one resource.

Rules can limit access based on information such as user attributes, client network range, time of day. You can combine rules to create rule sets, which are reusable and can be applied to many different resources and applications. Rule sets grant requests if any or all of the constituent rules are successful:

- **Any**: An any rule set is evaluated from top to bottom and stops at the first rule that has its criteria met. If all rules fail, the request is denied.
- **All**: An all rule set is evaluated from top to bottom and stops when it gets to the first rule that does not have its criteria met. If one rule fails, the request is denied.

Since rules within a rule set are evaluated from top to bottom, the order in which rules display in rule sets is important. In PingCentral, you can customize policies by dragging rules from the **Available Rules** list to the **Policy** list and changing the order to meet your needs.



For more information, see Rules in the *PingAccess User Interface Reference Guide*.

Updating applications

Update applications at any time.

About this task

To keep your applications secure, rotate certificates and client secrets on a regular basis and apply updated security configurations to applications built from templates if new configuration templates become available. You don't need to recreate your applications in PingCentral to apply new templates. Replace the templates associated with your applications and promote them again.

Steps

1. Click the **Expand** icon associated with the application you want to update and click the **Pencil** icon.

   All of the editable information is shown on one page.

2. To update the name, description, and owners, change the information in the **Name**, **Description**, and **Owners** fields. Click **Save**.

3. To change the template used to create the application, click **Change Template** and select a new template from the **Select Template** page. Click **Save and Close**.

   > **Note**
   >
   > You cannot apply a SAML template to an OAuth or OpenID Connect (OIDC) application nor apply an OAuth or OIDC template to a SAML application.

4. **Optional:** To update OAuth or OIDC application information:

   - In the **Client** section, change the scopes associated with OAuth or OIDC applications. Select or clear the appropriate check boxes and click **Save**.

     > **Note**
     >
     > You cannot edit scopes for applications created in PingCentral 1.2.0. However, you can update the template associated with an application to a template created in a later version, which allows you to update scope information.

   - In the **Promote** section, change the information in the **Redirect URI** fields for the appropriate environments and click **Save**.

   - To change client secrets, return to the **Applications** page, promote the application again, and generate a new secret.

5. **Optional:** To update SAML application information:

   - In the **Attribute Mappings** section, add or remove attributes and expressions, or update attribute and expression values, and click **Save**.

   - In the **Promotions** section, upload a new `.xml` file that contains service provider metadata, such as the Entity ID, ACS URL, certificates, and attribute information, from another SAML application. Click **Choose File** or **Or Use URL** to provide the metadata file.

> **Note**
>
> If metadata is used, the attribute mapping section might also need to be updated to include new attributes from the metadata file.

- Change the information in the **Entity ID** or **ACS URL** fields and click **Save**.
- To change the signing certificate, select the appropriate certificate in the **Signing Certificate** list and click **Save**.
- To change the service provider (SP) certificate, click **SP Certificate** to upload a new certificate, or click **Remove** to remove it. Click **Save**.

6. **Optional:** To update PingAccess application information:
   - On the **Properties** tab, in the **Promote** section, update the **Virtual Hosts**, **Access Validation**, **Identity Mapping**, and **Site** or **Agent** names, as appropriate. Click **Save**.
   - On the **Resources** tab, update information regarding each resource and click **Save**.
   - On the **Policy** tab, click the **Pencil** icon associated with the policy you want to update. Make changes and click **Save**.

Promoting applications

You can promote all applications assigned to you to development environments for testing, and to production environments if your permissions allow.

See the following:

- Promoting OAuth and OIDC applications
- Promoting SAML applications
- Using metadata to promote SAML applications
- Promoting PingAccess applications

> **Note**
>
> If an environment is offline or if a PingCentral administrator has set the environment status to **Disabled**, you will be unable to promote the application to a disabled or offline environment.

Promoting OAuth and OIDC applications

You can promote the OAuth and OIDC applications assigned to you.

Before you begin

Prepare to provide the following:

- Redirect URIs, if required. These are the URIs your users will be directed to after they receive authorization to access your application. Redirect URIs are only required when promoting applications that use an authorization code and implicit grant types.

Redirect URIs are not limited to the number of characters they can contain, but cannot include wildcards or some special characters.

- If a client secret is required to authenticate your application, you can create a custom secret, generate a secret, or leave the field empty and PingCentral will generate a client secret for you.

Steps

1. To promote the application to an environment, click the expandable icon associated with the application, select the **Promote** tab, and click **Promote**.

   > **Note**
   >
   > If an environment is offline or if a PingCentral administrator has set the environment status to **Disabled**, you will be unable to promote the application to a disabled or offline environment.

2. From the **Available Environments** list, select the environment to which you want to promote the application.

   > **Note**
   >
   > If you have the Application Owner role, you cannot promote applications to protected environments, which have shield icons associated with them.

3. If curly brackets display in the upper right corner of the window, you have the ability to edit the underlying application JSON yourself. Or, you can complete the fields on this window.

   If you choose to complete the fields on this window, refer to the following:

   1. If redirect URIs are required to promote the application, enter them in the **Redirect URIs** field.
   2. If a client secret is required to authenticate your application, you can either:
      - Generate a new secret by selecting the option at the bottom of the modal.
      - Continue using the existing secret. Bypass the **Generate New Secret** button and promote the application.

   To edit the JSON yourself:

   1. Click the curly brackets.

      Result:

      The application JSON displays in the window.

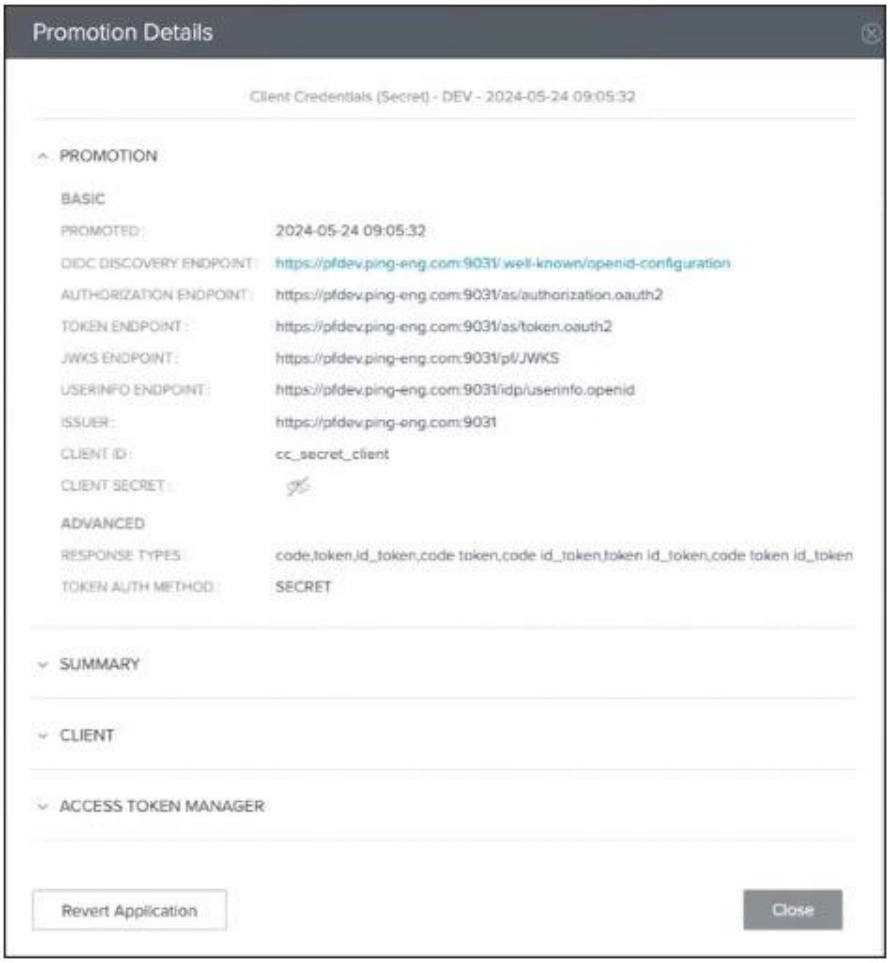
   2. Update the JSON to meet your needs. Built-in JSON syntax validation occurs as you make updates to help prevent mistakes.
   3. When you're finished, promote the application.

      Result:

      PingCentral promotes your application to the designated environment in PingFederate. You will see the new promotion in the **History** section of the page.

4. To configure the SSO connection, provide the following information to your service provider:
   - The Client ID. Click **View Client Details** to access the **Promotion Details** window, which displays the client ID.

- The OIDC discovery endpoint and client secret are also available in this window.



Promoting SAML applications

You can promote the SAML applications assigned to you.

Before you begin

Prepare to provide the following:

- **Entity ID**: used to uniquely identify the application and obtained from the service provider ACS URL, the application's URL to which SAML assertions from the identity provider will be sent after user authentication occurs.
- **ACS URL**(s): the application's URL to which SAML assertions from the identity provider will be sent after user authentication occurs.
- **SLO Service URL**(s): the application's URL utilized for single logout (SLO) functionality.
- **SP certificates**: if the template you select is based on a PingFederate connection that requires a certificate.
- **An assertion encryption certificate**: required if encryption is enabled for the connection.

Steps

1. To promote the application to an environment, click the **Expand** icon associated with the application, select the **Promote** tab, and click **Promote**.

   > **Note**
   >
   > If an environment is offline or if a PingCentral administrator has set the environment status to **Disabled**, you will be unable to promote the application to a disabled or offline environment.

2. In the **Available Environments** list, select the environment to which you want to promote the application.

   > **Note**
   >
   > If you have the Application Owner role, you cannot promote applications to protected environments, which have shield icons associated with them.

3. If curly brackets display in the upper right corner of the window, you have the ability to edit the underlying application JSON yourself. Or, you can complete the fields on this window.

   If you choose to complete the fields on this window, refer to the following:

   1. In the **Entity ID**, **ACS URL**, and **SLO Service URL** fields, enter the appropriate information.

      If you provided a metadata file when you added your application to PingCentral, the **Promote to Environment** window is prepopulated with the information from the other SAML application. You can modify this information as necessary.

   2. In the **Signing Certificate** list, select the appropriate certificate:

      - If the PingFederate environment contains signing certificates, those certificates display in the list.
      - The signing certificate added to the environment when it was created or last updated displays as the **Environment Default** certificate.
      - If signing certificates are not available in the PingFederate environment and an environment default certificate isn't available, or if an environment default certificate is available but expired, the **Automatically generate certificate** option displays in the list.

        > **Note**
        >
        > If you used signing certificates that were automatically generated to promote applications in PingCentral 1.7 or earlier, and you want to promote those applications to the same environments, you need to locate the signing certificates. Search for a signing certificate with a subject DN that matches the name of the application and select it as the signing certificate.

   3. Upload SP certificates, if required. SP certificates are required for PingFederate SP connections when:

      - Either of the single logout (SLO) options, **IdP-Initiated-SLO** or **SP-Initiated-SLO**, are selected as the SAML profile.
      - Digital signatures are required, and the Signature Policy is set to the **Require authn requests to be signed when received via the POST or redirect bindings** option.

- Inbound backchannel authentication is configured. For more information, see the following topics in the *PingFederate Server Guide*:
  - Configure digital signature settings
  - Configuring signature verification settings (SAML 2.0)

4. If encryption is enabled for the connection, click in the **Assertion Encryption Certificate** field. Select an assertion encryption certificate used for a previous promotion in the list or provide a new one.

> **Note**
>
> Only whole encryption is currently supported, so if a connection has attributes specified for encryption, the promotion will fail.

To edit the JSON yourself:

1. Click the curly brackets.

   Result:

   The application JSON displays in the window.

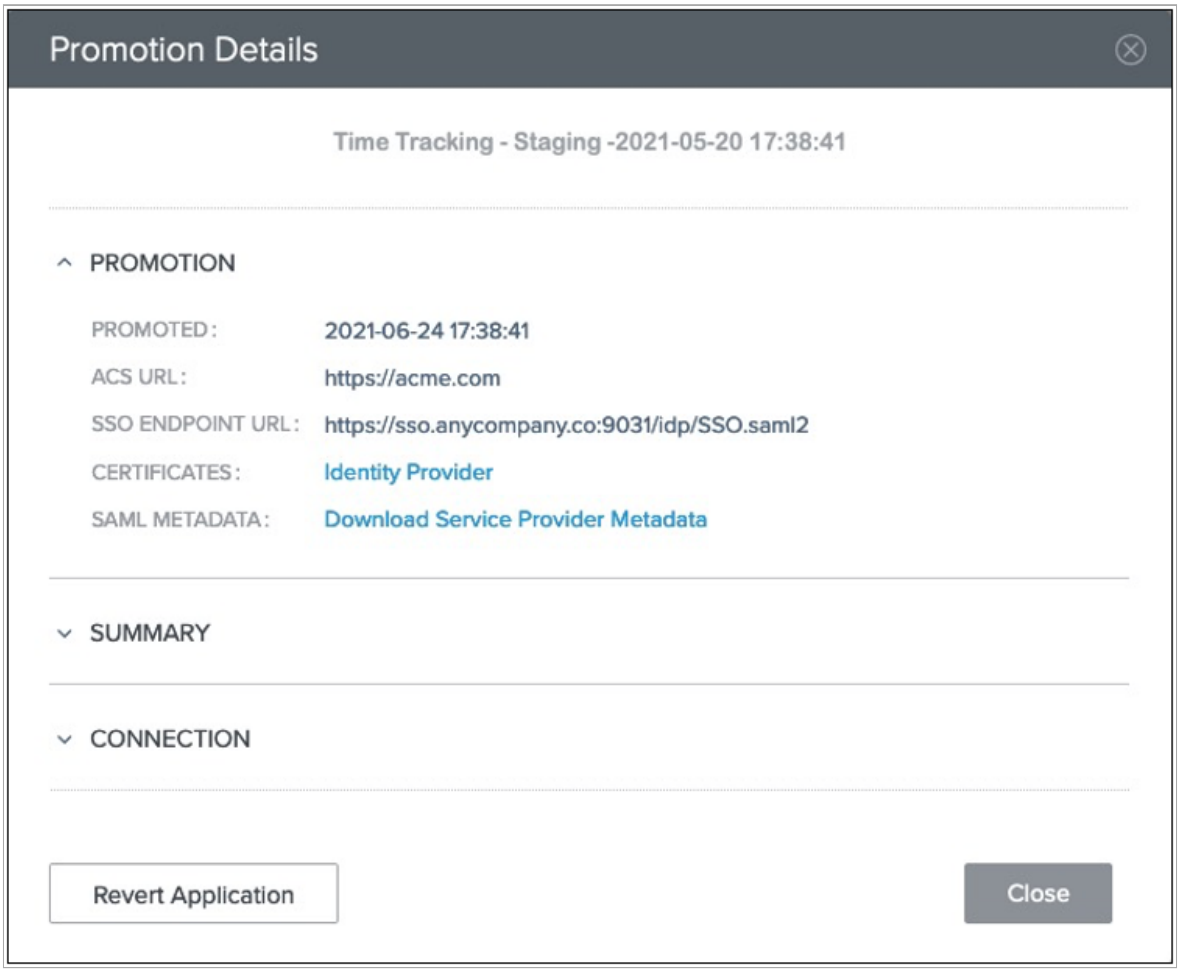
2. Update the JSON to meet your needs. Built-in JSON syntax validation occurs as you make updates to help prevent mistakes.

4. Verify that the information displayed in the **Promote to Environment** window is correct and click **Promote**.

   Result:PingCentral promotes your application to the designated environment in PingFederate. The new promotion shows in the History section of the page. If the signature verification certificate used during promotion is available in the PingFederate environment, that certificate is used. If not, a new certificate is created.

5. To configure a single sign-on (SSO) connection, provide the application Entity ID and the SSO endpoint URL to your service provider.

   To locate the SSO endpoint URL, click the **View Connections Detail** link associated with the promotion. The URL displays on the **Promotion Details** window.



Using metadata to promote SAML applications

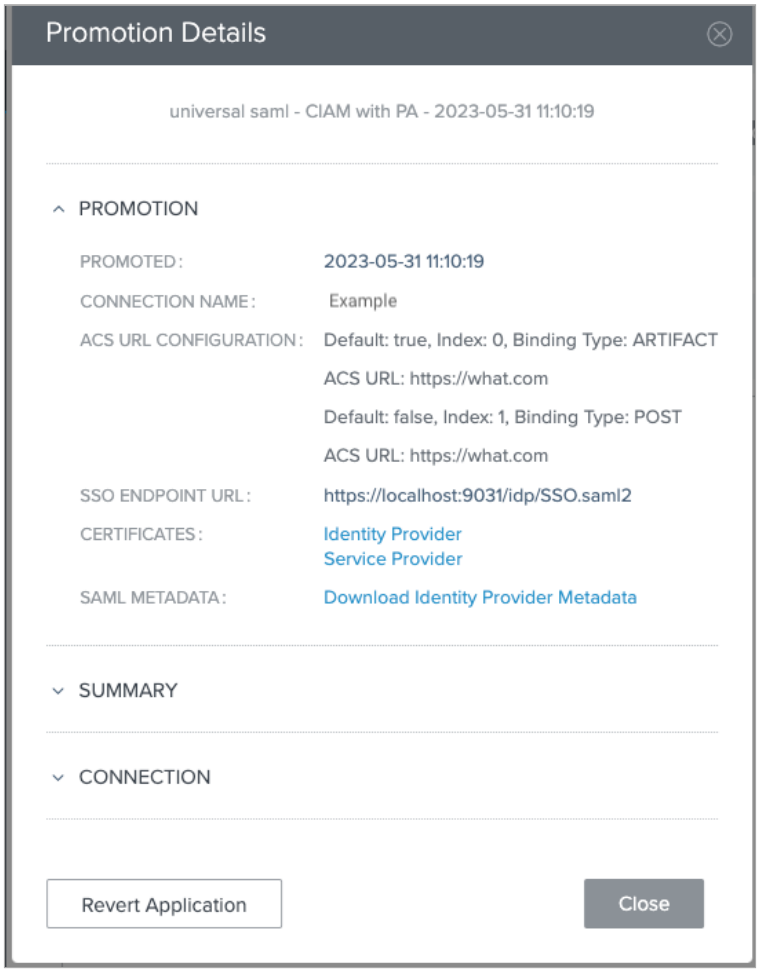
When SAML applications are promoted, the connection metadata is exported and stored as part of that application. This metadata is available to download as a `.xml` file, which you can use to promote similar SAML applications.

Steps

1. On the **Applications** page, locate an application that has a configuration you want to replicate in a new SAML application and click the expandable icon associated with that application.
2. Go to the **Promote** tab and click the **View Connection Details** link.

   Result:

   The promotion information displays.



3. Click **Download Identity Provider Metadata** to download the metadata as a `.xml` file and click **Close**.
4. Use the metadata on the service provider (SP) side to update the connection to the identity provider (IdP), as appropriate.

Promoting PingAccess applications

Promote the PingAccess applications assigned to you.

Before you begin

The information required to promote PingAccess Web applications, API applications, and Web + API applications varies by type. Prepare to provide the following information:

Web applications	API applications	Web + API applications
Virtual host (required)	Virtual host (required)	Virtual host (required)
	Access validation method (required if an identity mapping is specified)	Access validation method (required)
Web session (optional)	Web session (optional)	Web session (required)

Web applications	API applications	Web + API applications
Identity mapping (optional)	Identity mapping (optional)	Identity mapping (optional)
Site or agent (required)	Site or agent (required)	Site or agent (required)

For details regarding each of these items, see Information needed to promote PingAccess applications.

> **Note**
>
> Customized authentication challenge responses, which support single-page applications, are available in PingAccess version 6.2 or later. Applications with this type of policy can be added to PingCentral, but cannot be promoted to another environment unless the authentication challenge policy also exists in the target environment.

Steps

1. To promote the application to an environment, click the Expand icon associated with the application, select the **Promote** tab, and click **Promote**.

   > **Note**
   >
   > If an environment is offline or if a PingCentral administrator has set the environment status to **Disabled**, you will be unable to promote the application to a disabled or offline environment.

2. From the **Available Environments** list, select the environment to which you want to promote the application.

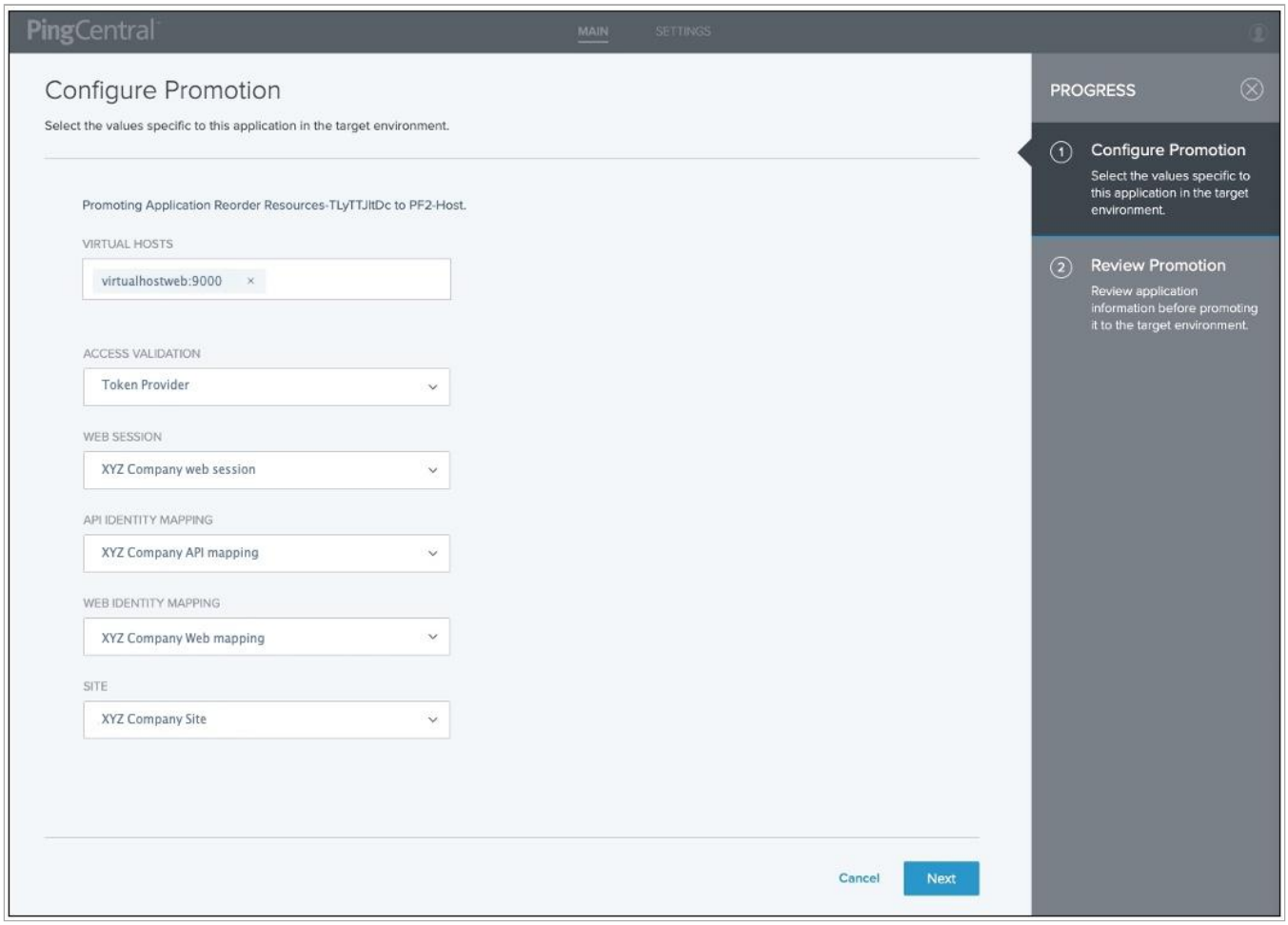
   > **Note**
   >
   > If you have the Application Owner role, you cannot promote applications to protected environments, which have shield icons associated with them.

3. On the **Configure Promotion** page, click in the **Virtual Hosts** field, and select the virtual hosts you want to add.

   To remove a virtual host, click the **X** icon next to the virtual host name.

4. Complete the remaining fields, which vary, depending on the type of application you are promoting.

   The following example shows the fields available to provide information for a Web + API application.



5. Click **Next**.
6. On the **Review Promotion** page, review promotion information you added.

   Additional detail is available in the **Summary** and **Application** sections of the page.
7. Click **Promote and Close**.
8. To review details regarding the promotion, click the **View History Details** link associated with the promotion.

Information needed to promote PingAccess applications

When you promote PingAccess applications to PingAccess environments, you provide virtual host, access validation, web session, and identity mapping information, as appropriate.

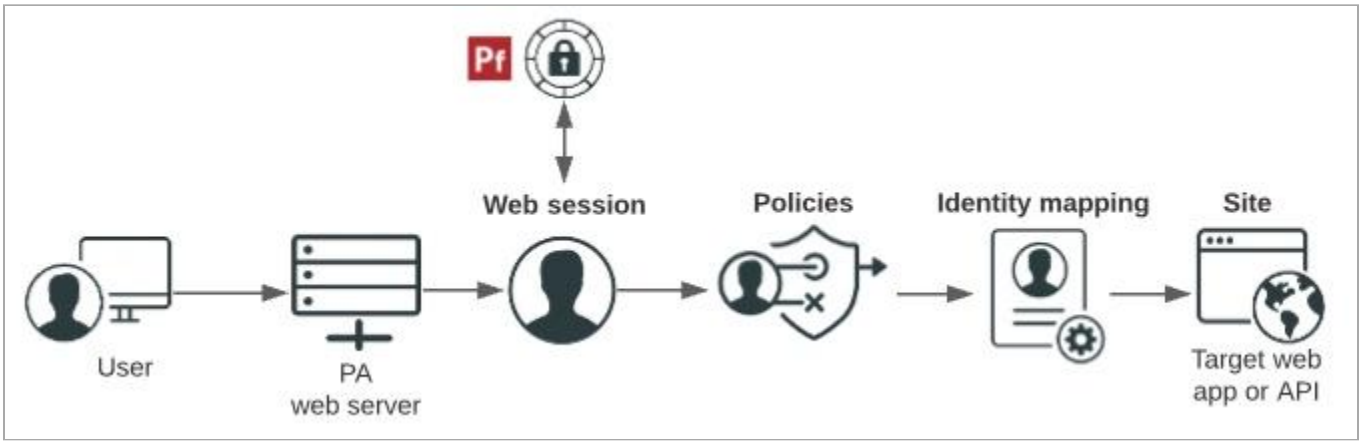
PingAccess can be deployed in one of two ways:

- **Gateway deployment**: In a gateway deployment, the destination is a site. Requests are routed to a PingAccess web server, which then forwards authorized requests to the target application or API on the site.
- **Agent deployment**: In an agent deployment, the destination is an agent. Requests are intercepted at the web server hosting the target application or API by the PingAccess agent plugin. The agent communicates with the PingAccess policy server to validate access before allowing the request to proceed to the target application or API.

The key difference between these deployments is where the initial request is directed. In a gateway deployment, the initial request is routed to a PingAccess web server, so the destination is a site. In an agent deployment, the initial request is routed to the web server that hosts the target application or API, so the destination is an agent. When you promote PingAccess applications, you are prompted to provide the name of the site or agent.

Gateway deployment

This diagram shows how users are authenticated, and how access policies and identity mappings are applied to requests to access applications or APIs with a gateway deployment.



1. Users enter a URL that consists of a unique virtual host and context root.
    - **Virtual host**: The public-facing host name and host port. For example, `den.ping.com:8443`.

      A wildcard (`*`) can be used either to define either any host (`*:8443`, for example) or any host within a domain (`*.ping.com`, for example). If a request matches more than one virtual host, the most specific match is used.
    - **Context root**: The common root of all resources, specifies where in the URL path the application begins, and starts with a slash. In the example URL, `den-ping.com:8443/mygreatapp/home`, `/mygreatapp/` is the context root.

      PingCentral prompts you for the context root when you add the application, and for the virtual hosts when you promote it.
2. The PingAccess web server determines whether a PingAccess session cookie (Web) or an OAuth token (API) exists for the user. If it does not, a web session starts. Web sessions define the policy for web application session creation, lifetime, timeouts, and their scope.

    > **Note**
    >
    > If you promote Web + API applications in PingCentral, you are required to select a Web session from a drop-down list. This information is not required to promote Web or API applications.

3. You can configure API and Web + API applications to use access token validators to locally verify signed and encrypted access tokens. If you are promoting an API or Web + API application in PingCentral, you can specify the access validation method, whether it be a token provider or a token validator, if appropriate.
4. Users are authenticated through the web session.
5. Policies are applied to the request. Policies are rules, or sets of rules, that are applied to application resources. PingAccess makes policy-based decisions to grant or deny access to the requested resource.

You can customize application and resource policies when you use templates to add applications to PingCentral.

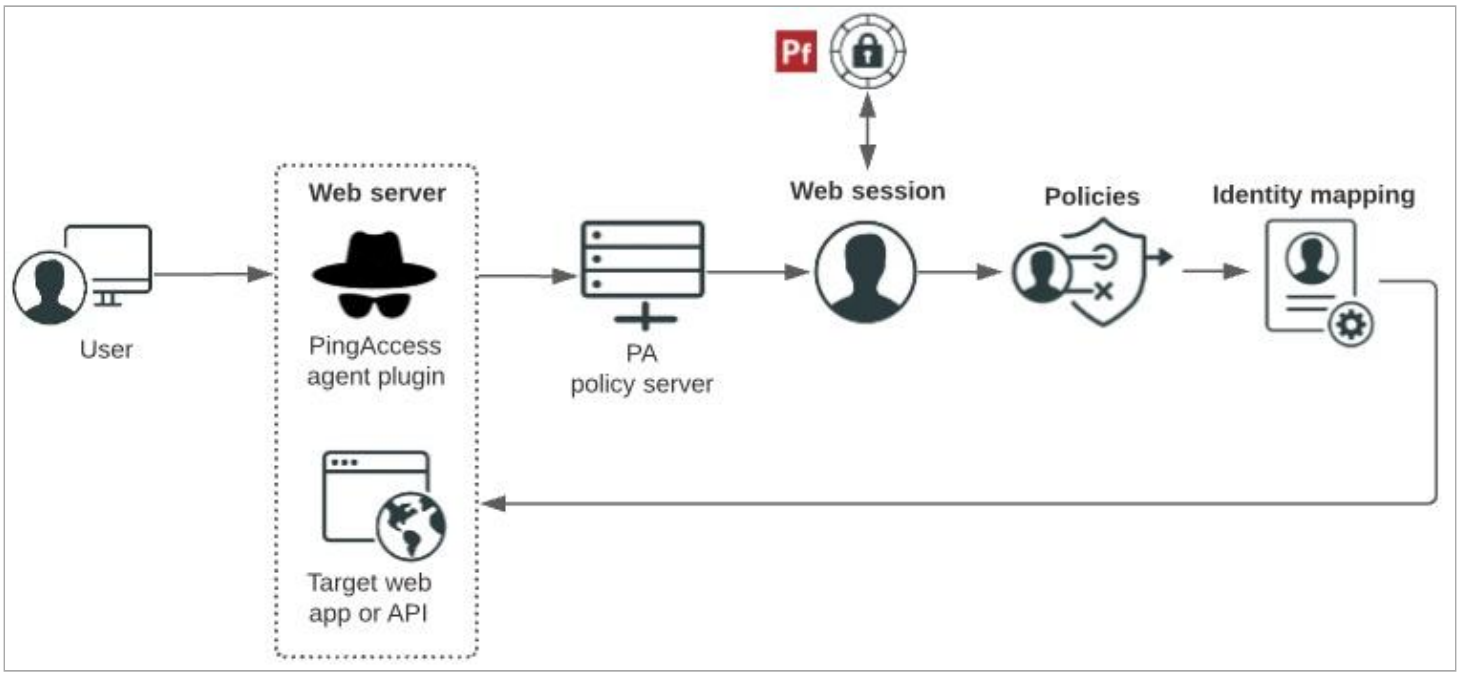
6. Identity mapping is applied to the request if the target application expects user information to be included to further authenticate the user.

   PingCentral prompts you for the name of the Web and/or API Identity mapping, as appropriate, when you promote it.

7. The user accesses the target web application or API.

Agent deployment

The following diagram shows hows users are authenticated, and how access policies and identity mappings are applied to requests to access applications or APIs with an agent deployment.



1. Users enter a URL to request access to a resource and their requests.
2. The PingAccess agent plugin intercepts the request. Agents use names and shared secrets to authenticate with the policy server. These names and secrets do not need to be unique. Any number of agents can have the same name and secret, and they are all treated equally by the policy server.
3. If the agent does not have previously cached policies for the resource, it contacts the PingAccess policy server for instructions.
4. The PingAccess policy server receives claims from the token provider, which provides instructions for handling the request.
5. Policies are applied to the request and PingAccess makes policy-based decisions to grant or deny access to the requested resource.
6. Identity mapping is applied to the request if the target application expects user information to be included to further authenticate the user.
7. The user accesses the target web application or API.

Reverting applications to previously promoted versions

When you revert applications to previously promoted versions, the reverted versions of the application will not exist outside of PingCentral until you promote them again, at which point they will also be available in PingFederate or PingAccess.

Steps

1. On the **Applications** page, locate the application you want to revert to a previously promoted version.

   > **Note**
   >
   > You cannot revert applications created in previous versions of PingCentral.

2. Click the expandable icon associated with the application, select the **Promote** tab, and then click **View Details**.
3. In the **Promotion Details** window, click **Revert Application**.

   Result:

   A message displays asking you if you are sure you want to revert this application.

4. Click **Revert**.

   Result:

   The reverted version of the application displays in your applications list.

   > **Note**
   >
   > Reverting OAuth and OIDC applications to previously promoted versions overrides client secrets, so you will need to create or generate new secrets before you promote them again. Reverting SAML applications to previously promoted versions overrides the Entity IDs, ACS URLs, and certificates, so you might need to update this information before you promote them again.

Managing approvals (application owners)

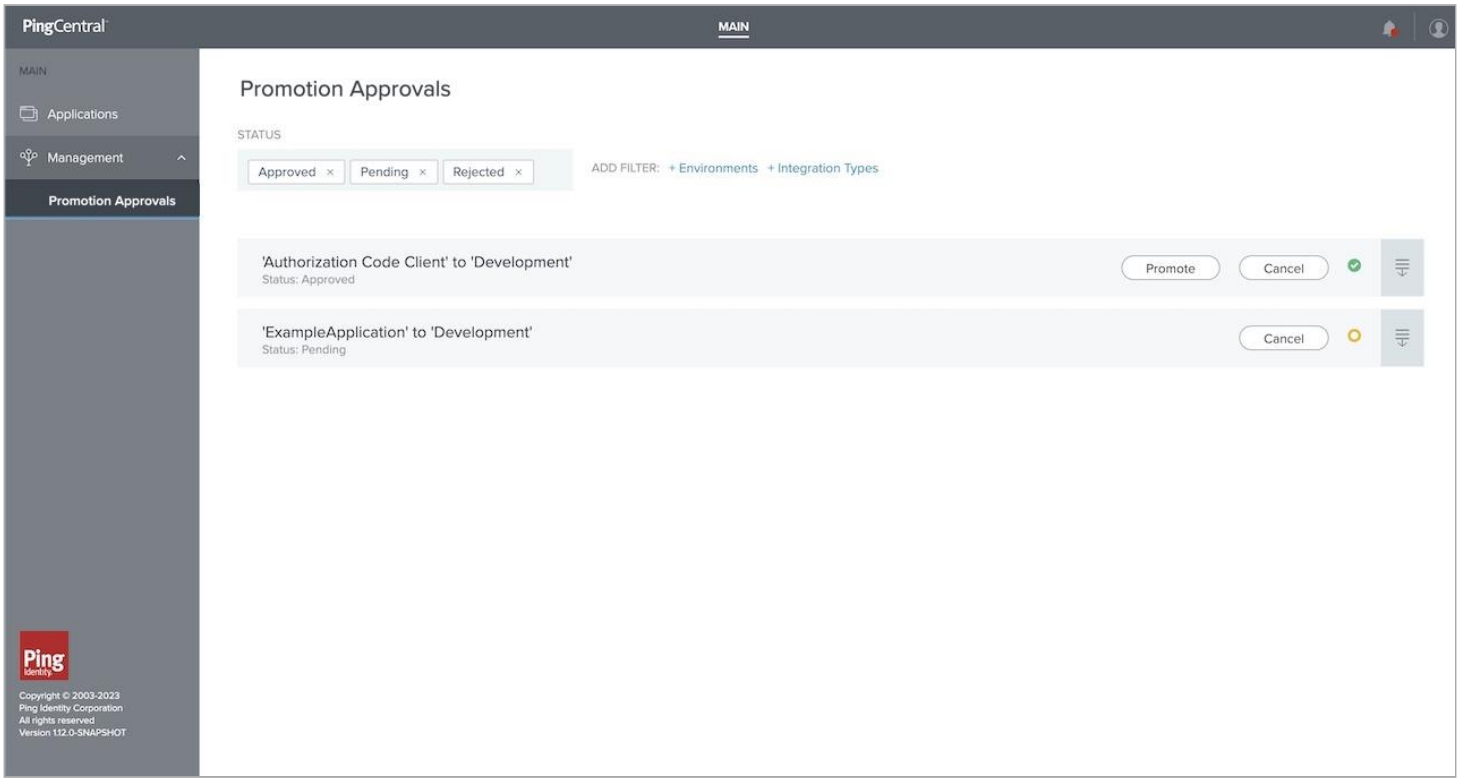
If you submit a request for application promotion to your administrator, you can track the application's approval status by accessing the **Promotion Approvals** page, located under the **Management** tab.

About this task

From this page, you can:

- Filter for approved, promoted, pending, rejected, or canceled approvals, or by environments or integration type. Use the **Visible** filter, which is enabled by default, to hide approvals that are in a canceled, promoted, or rejected status.
- **Promote** an approved application, or **Cancel** an approval request.

> **Note**
>
> You see a bell icon in the top navigation bar when an administrator approves your promotion request.



Steps

1. Select your filters.

   You can filter by:

   - **Status**: **Approved**, **Pending**, or **Rejected**. The page automatically filters for any approved, pending, or rejected approval requests.
   - Environments.
   - Integration types (OAuth and OIDC or SAML).

   Click the filters to add or remove them.

2. To promote approved applications to an environment, click **Promote** in the row for the application that you want to promote.

   For more information, see Promoting applications.

   > **Note**
   >
   > There can only be one outstanding promotion approval request per application to an environment.

   > **Note**
   >
   > If an environment is offline or if a PingCentral administrator has set the environment status to **Disabled**, the environment is undergoing maintenance. During this time, the **Promote** button is inaccessible. You will be unable to promote the application while the environment is offline or disabled and undergoing maintenance.

3. To cancel an approval request, click **Cancel** in the row for the application that you no longer want to request promotion approval.