

PingCentral



Contents

PingCentral.....	4
Release Notes.....	4
PingCentral 1.10 (June 2022).....	4
Previous Releases.....	6
PingCentral for IAM Administrators.....	6
Introduction to PingCentral.....	6
System requirements and supported configurations.....	9
Installing and configuring PingCentral.....	14
Using Docker to deploy PingCentral.....	15
Installing PingCentral on Microsoft Windows.....	15
Installing PingCentral on Linux systems.....	16
PingCentral licensing.....	17
Setting up MySQL.....	17
Upgrading PingCentral.....	18
Configuring PingCentral to run as a Windows service.....	22
Configuring PingCentral to run as a Linux systemd service.....	23
Configuring PingCentral to run as a Linux systemv service.....	24
Configuring PingFederate and PingAccess for SSO.....	25
Configuring logging.....	34
Replacing the Admin Console SSL Certificate.....	35
Managing environments.....	36
Adding a PingFederate environment.....	37
Updating environments.....	38
Deleting environments.....	39
Configuring PingFederate as a PingAccess token provider.....	39
Adding trusted CA certificates to PingCentral.....	42
Managing users.....	43
Managing users through PingCentral.....	43
Setting up SSO for PingCentral.....	44
Monitoring PingCentral.....	51
Setting up Prometheus using OAuth.....	53
Setting up Prometheus using basic authorization.....	53
Setting up Graphite.....	54
Accessing Prometheus and Grafana.....	55
Setting up Grafana.....	56
Managing user groups.....	57
Adding user groups.....	58
Updating user groups.....	60
Deleting user groups.....	60
Managing applications.....	60
Filtering applications.....	61
Adding applications.....	61
Updating applications.....	62
Deleting applications.....	64
Managing templates.....	64

OAuth and OIDC templates.....	65
SAML 2.0 and PingAccess templates.....	69
Deleting templates.....	74
Promotion processes.....	74
OAuth and OIDC application promotions.....	74
SAML SP application promotions.....	75
PingAccess application promotions.....	75
Reverting applications to previously promoted versions.....	76
PingCentral for Application Owners.....	76
Introduction to PingCentral.....	76
Accessing PingCentral.....	79
Managing applications.....	80
Viewing application information.....	81
Adding applications.....	83
Selecting a template.....	83
Using OAuth and OIDC templates.....	85
Using SAML 2.0 templates.....	86
Using PingAccess templates.....	89
Updating applications.....	94
Promoting applications.....	95
Promoting OAuth and OIDC applications.....	96
Promoting SAML applications.....	97
Promoting PingAccess applications.....	100
Reverting applications to previously promoted versions.....	105

PingCentral

PingCentral makes it possible for 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), 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

- [Introduction to PingCentral](#)
- [Release Notes](#)
- [System requirements and supported configurations](#)
- [Installing and configuring PingCentral](#)
- [Monitoring PingCentral](#)
- [Managing environments](#)
- [Managing users](#)
- [Managing user groups](#)
- [Managing applications](#)
- [Managing templates](#)
- [Promotion processes](#)



PingCentral for Application Owners

- [Introduction to PingCentral](#)
- [Accessing PingCentral](#)
- [Managing applications](#)
- [Viewing application information](#)
- [Adding applications](#)
- [Updating applications](#)
- [Promoting applications](#)
- [Reverting applications to previously promoted versions](#)

Release Notes

New features and improvements in PingCentral. Updated January 22, 2024.

PingCentral 1.10 (June 2022)

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

Update OAuth and OIDC templates, grant types, scopes, and policy contracts in PingCentral

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](#) on page 65 for details.

Update applications with the latest template version available

PASS-6007 New

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](#) on page 62 for details.

Use SSO to access PingFederate and PingAccess from PingCentral PASS-5202 and PASS-6018 **New**

You can now use SSO to access PingFederate and PingAccess from PingCentral. For details, see [Configuring PingFederate and PingAccess for SSO](#) on page 25.

Account lockout mechanisms added to mitigate password guessing PASS-6388 **Improved**

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 PASS-6466 **Issue**

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 PASS-6387 and PASS-6378 **Security**

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

Configure APC mappings for OIDC applications in PingFederate PingFederate PASS-3613 **Issue**

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.

SP certificates and assertion encryption certificates must be different PingFederate PASS-5663 **Issue**

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 PingAccess PASS-4948 **Issue**

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 PASS-5977 **Issue**

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 PASS-5009 **Issue**

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 PASS-5001 and PASS-5002 **Issue**

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 PingFederate administrative 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](#).

- [PingCentral 1.9.3 \(February 2022\)](#)
- [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 \(March 2021\)](#)
- [PingCentral 1.6 \(December 2020\)](#)
- [PingCentral 1.5 \(September 2020\)](#)
- [PingCentral 1.4 \(July 2020\)](#)
- [PingCentral 1.3 \(March 2020\)](#)
- [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.

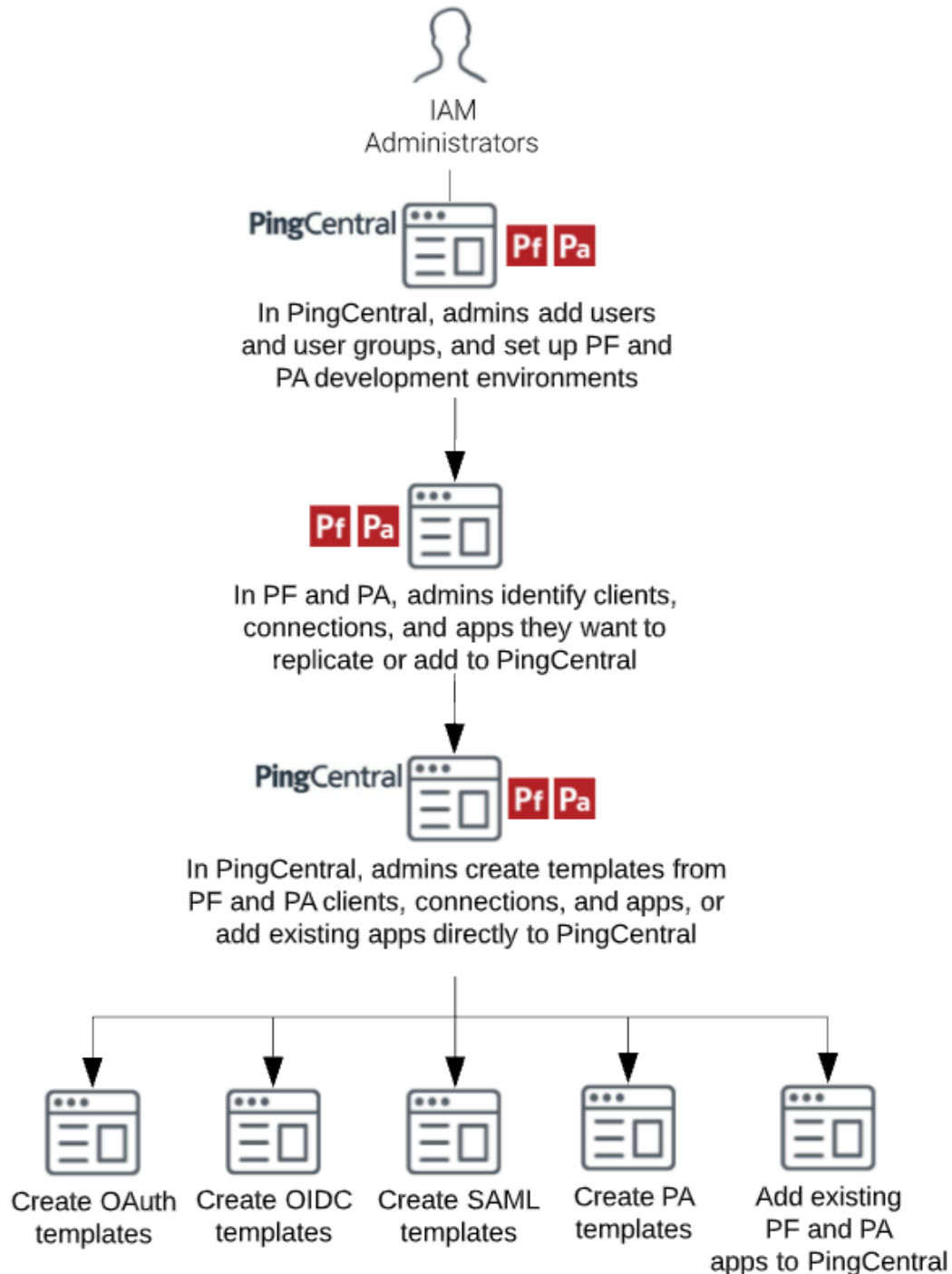
PingCentral:

- 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), 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.



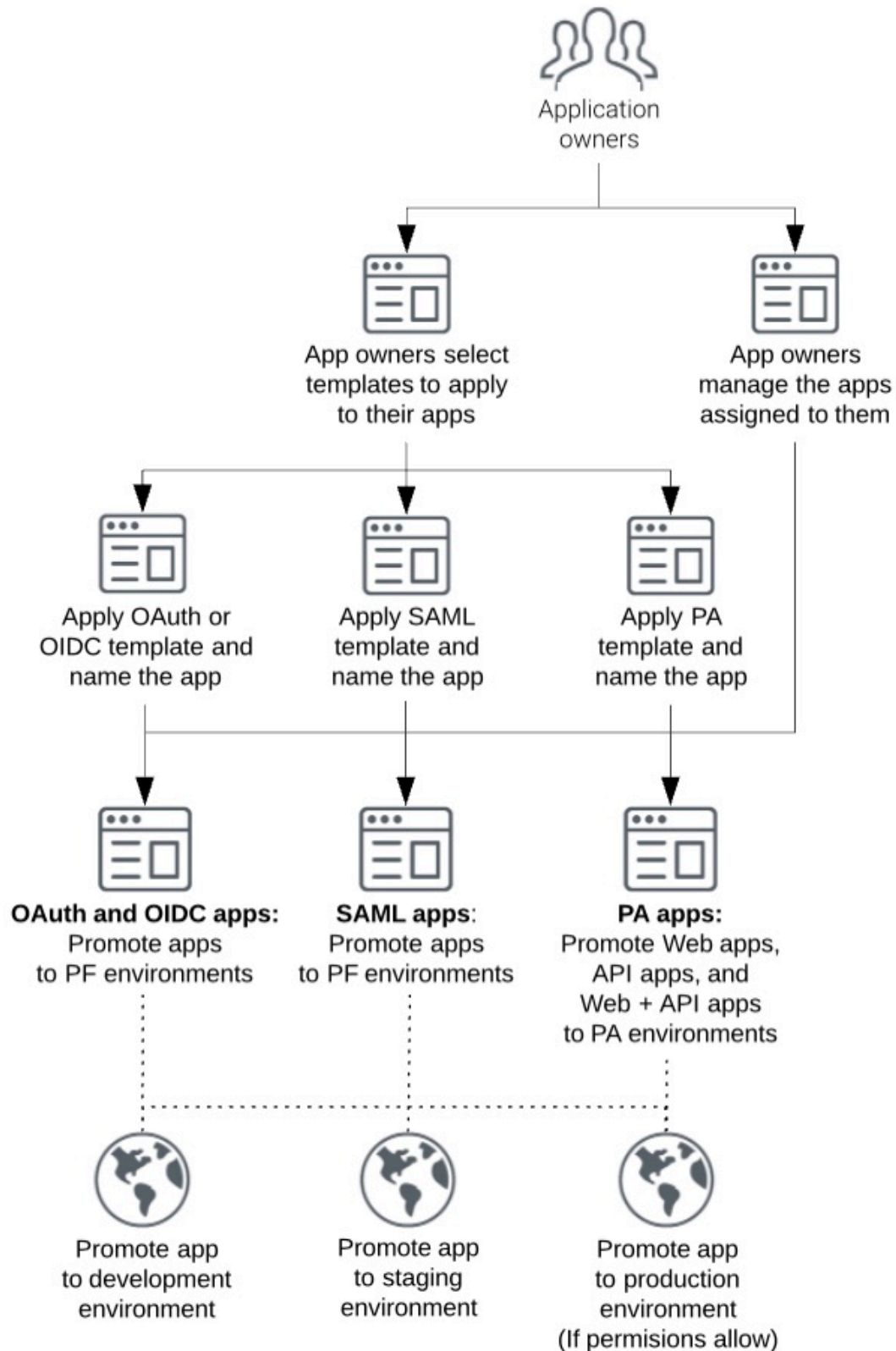
How PingCentral works

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

This flowchart illustrates 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:

- PingFederate 11.2
- PingFederate 11.1
- PingFederate 11.0
- PingFederate 10.3
- PingFederate 10.2
- PingFederate 10.1
- PingFederate 10.0
- PingFederate 9.3
- PingFederate 9.2

PingAccess:

- PingAccess 7.2
- PingAccess 7.1
- PingAccess 7.0
- PingAccess 6.3
- PingAccess 6.2
- PingAccess 6.1
- PingAccess 6.0
- PingAccess 5.3.2

Platforms:

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

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 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.

Java runtime environments:

- Oracle Java 11 LTS
- OpenJDK 11

Docker:

- 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 working 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 configurations](#)
- [PingAccess configurations](#)


General configurations

Configuration	Supported	Unsupported
Single sign-on and user management	<ul style="list-style-type: none"> ▪ Directly managing users, which are stored in PingCentral embedded database. ▪ Signing on with single sign-on (SSO) using an OpenID Connect (OIDC) token. ▪ Optional feature: Group management, which allows the OIDC token used for SSO to include the groups claim. ▪ Beta feature: Provisioning users and groups from an external store using API calls. <div data-bbox="613 1528 659 1570" data-label="Image"></div> <div data-bbox="662 1541 738 1572" data-label="Section-Header">Note:</div> <div data-bbox="609 1587 1099 1841" data-label="Text"> <p>If you want to provision users and groups of users through the API, you must disable the groups claim functionality by setting the <code>pingcentral.sso.oidc.groups-claim-enabled</code> property to <code>false</code> in the <code>application.properties</code> file.</p> </div>	

Configuration	Supported	Unsupported
Entitlements	<ul style="list-style-type: none"> 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 groups claim included in the OIDC token used for SSO. 	Assigning groups of users entitlements based on an external attribute, such as LDAP group membership.
Backup and restoration	<p>Saving the database and configuration files by copying the directories <code>h2-data/</code> and <code>config/</code> to a new instance.</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p> CAUTION:</p> <p>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 on page 17.</p> <p>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.</p> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p> Note:</p> <p>To ensure these files contain the most up-to-date information, do not copy them while PingCentral is running.</p> </div>	Using an API to export PingCentral configuration information.


OAuth and OIDC configurations

Configuration	Supported	Unsupported
Client authentication		Using a client TLS certificate, private key JSON web token (JWT), or symmetric keys.

Configuration	Supported	Unsupported
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.	
ATMs and OIDC policies	<p>Saving ATMs or OIDC policies into templates created from client applications that have them.</p> <p> 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.</p>	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 via 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	<ul style="list-style-type: none"> ▪ IdP-initiated SSO ▪ SP-initiated SSO ▪ IdP-initiated SLO ▪ SP-initiated SLO 	
Attribute mapping	<ul style="list-style-type: none"> ▪ Mapping attributes, provided by a single authentication policy contract, in an unspecified format. You can also map attributes to static text. ▪ Using OGNL expressions as part of attribute mapping. 	Mapping attributes from data sources, such as basic or URI.

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	<ul style="list-style-type: none"> Providing a public certificate for a service provider (SP) connection. PingCentral creates a self-signed certificate with an expiration date of one year from today and configures it as the PingFederate identity provider (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.	<p>New rules and rule sets cannot be created in PingCentral.</p> <p>Virtual resources are available in PingAccess version 6.2 or later, but are not yet supported in PingCentral.</p> <p>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.</p>

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 systemd service](#)
- [Configuring PingCentral to run as a Linux systemv service](#)
- [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 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 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:** 2Federate

Without modification, PingCentral is secure by default.

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. See [Adding trusted CA certificates to PingCentral](#) for details.
5. Configure PingCentral to run as a Windows service, if appropriate.
For more information, see [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 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`.

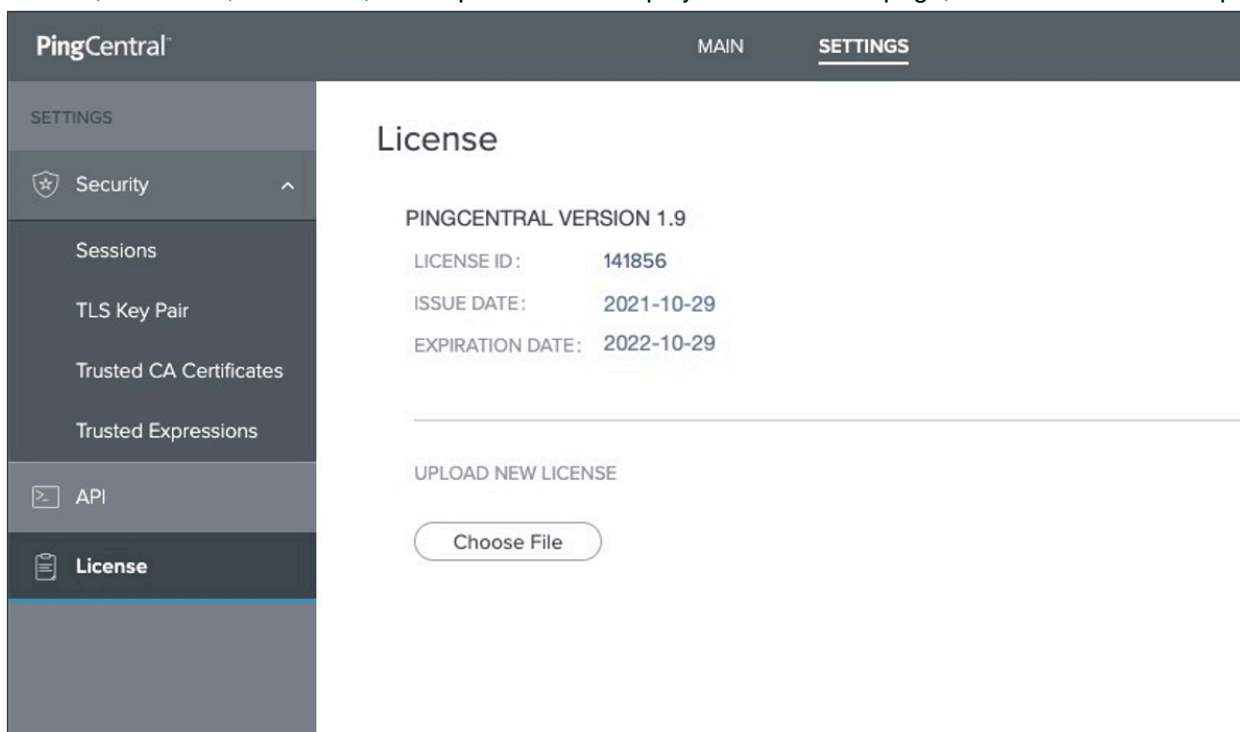
4. When the installation is complete, open a browser window and enter the machine and PingCentral admin port in the URL field.
Example: `https://<yourhost>:9022`.
5. Sign on to the application using the following credentials:
 - **Username:** Administrator
 - **Password:** 2Federate
6. Configure PingCentral to run as a Linux systemv service or a Linux systemd service, as appropriate.
For more information, see [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:
 - a. Update the datasource URL to your location.

Example:

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

- b. Update the user name and password, if necessary.

Example:

```
spring.datasource.username=PingCentralUsername
spring.datasource.password=PingCentralPassword
```

- c. 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 1.10. To begin the upgrade, download and extract the contents of the 1.10 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 1.10](#).

**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-1.10.0.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.
- If the `application.properties` file was modified, the current version of the file is merged with the latest version, preserving customizations.
- 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.



Note:

If you are using an H2 database and are still using 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.

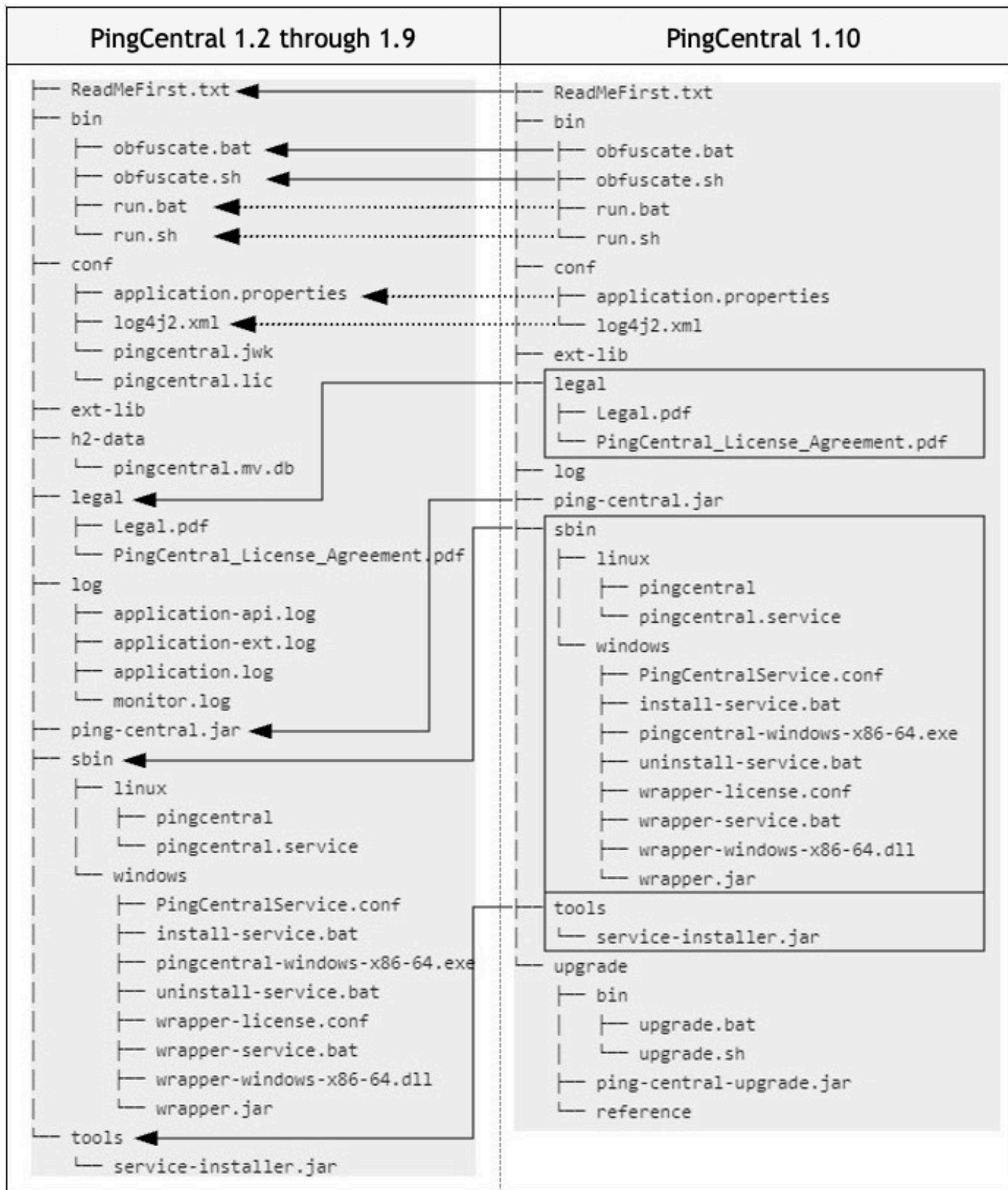


CAUTION:

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](#) on page 17.

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.

The following image shows PingCentral 1.10 after it has been run and the database files that have been generated. It also shows which files are replaced with new files during the upgrade process.



Upgrading to PingCentral 1.10

To upgrade PingCentral to 1.10, on either Windows or Linux, download the 1.10 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 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-1.10.0.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 1.10 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 1.10.0 install>/upgrade` directory and run the appropriate file:

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

Result: The upgrade process begins. The upgrade utility uses the extracted contents of the `ping-central-1.10.0.zip` file to copy and replace the appropriate information in the existing version location.



Note:

When the upgrade is complete for this release, PingCentral 1.10 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 1.10, PingCentral 1.10 will run from the original 1.4 directory. The same is true if you upgraded directly from 1.4 to 1.10.

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-1-1.10.0/
```

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 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 1.10.

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

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 1.10 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 systemd 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 <code>systemctl stop pingcentral</code> command.
Disable the service	Run the <code>systemctl disable pingcentral</code> 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 systemd service.

Steps

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

Option	Description
Stop the service	Run the <code>/etc/init.d/pingcentral stop</code> command.
Delete the service	Run the <code>chkconfig --del pingcentral</code> 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:
 - a. 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.

The screenshot shows the PingFederate Admin Console interface. The top navigation bar includes 'AUTHENTICATION', 'APPLICATIONS', and 'SECURITY'. The left sidebar shows the navigation menu with 'OAuth' selected. Under 'OAuth', the 'Access Token Management' option is highlighted. The main content area is titled 'Access Token Management' and contains a table of instances. The 'JSON Web Tokens' instance is highlighted with a red box.

Instance Name	Instance ID	Type
ATMappingWithExistingAPCTest	ATMappingWithExistingAPCTest	JSON Web Tokens
ATMappingWithNewAPCTest	ATMappingWithNewAPCTest	JSON Web Tokens
GeneralAccessToken	GeneralAccessToken	Internally Managed R Tokens
JSON Web Tokens	jwt	JSON Web Tokens
testAccessTokenManager1C	testAccessTokenManager	JSON Web Tokens

- b. 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.

The screenshot shows the 'Create Access Token Management Instance' configuration page in the PingFederate Admin Console. The 'Access Token Attribute Contract' tab is selected. The page displays a form for extending the contract with the following attributes:

- admin_role
- Username

The 'Subject Attribute Name' is set to USER_KEY.

- c. 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**.

Access Token Mappings

Manage the attribute mapping(s) used to fulfill the access token attribute contracts. This configuration maps from a persistent grant or other source token attribute contract. For mappings involving a persistent grant, a default mapping should be configured for each access token manager. The default mapping is overridden based on the context of the authentication event of the original grant.

Context	Access Token Manager	Action
Authentication Policy Contract: anycompanyContract	ATMappingWithExistingAPCTest	Del
Authentication Policy Contract: ATMappingWithNewAPCTest	ATMappingWithNewAPCTest	Del
Client Credentials	JSON Web Tokens	Del
Default	GeneralAccessToken	Del
Default	JSON Web Tokens	Del
Default	testAccessTokenManager1C	Del
Default	testAccessTokenManager1S	Del
Default	testAccessTokenManager1Sp1S1C	Del
Default	testAccessTokenManager2C	Del
Default	testAccessTokenManager2S	Del
Default	testAccessTokenManager2S1C	Del
Default	testAccessTokenManager2S2C	Del
Default	testAccessTokenManagerMRT1	Del

CONTEXT: Client Credentials | ACCESS TOKEN MANAGER: JSON Web Tokens | Add Mapping

- d. 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.

Access Token Mappings | Access Token Mapping

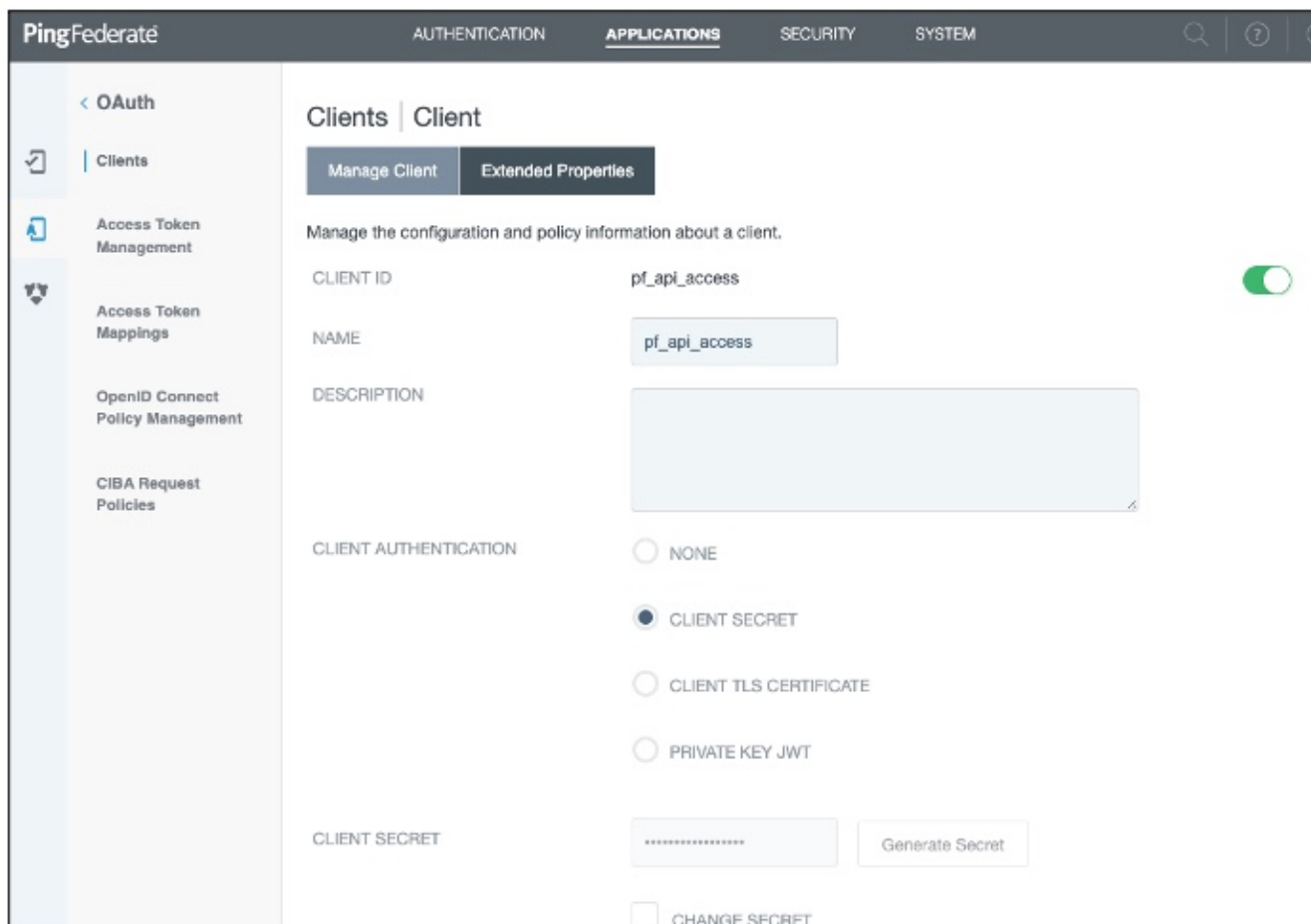
Attribute Sources & User Lookup | **Contract Fulfillment** | Issuance Criteria | Summary

Select a Source and Value to map into each item in the Contract list.

Contract	Source	Value
admin_role	Expression	New string [{"admin", "c
Username	Text	api_user

2. Configure a new PingFederate client:
 - a. In PingFederate, go to **Applications # OAuth # Clients**.
 - b. 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.



- c. In the **Client Authentication** field, select **Client Secret**.
- d. In the **Client Secret** field, you can:

Option	Description
Create or generate a secret.	Choose from: <ul style="list-style-type: none"> ▪ To create a strong, random alphanumeric string, click Generate Secret. ▪ Manually enter a secret.

Option	Description
Modify an existing secret.	<ol style="list-style-type: none"> 1. Select the Change Secret check box. 2. Click Generate Secret to create a strong random alphanumeric string or manually enter a secret.

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

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

3. Configure PingCentral:
 - a. In PingCentral, to connect to the new PingFederate client, go to **Environments # Add Environments**.
 - b. 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.
- c. Click **Next**.

Configuring PingAccess for SSO

About this task

To use SSO to access PingAccess from PingCentral:

Steps

1. Configure a new PingFederate client:
 - a. In PingFederate, go to **Applications # OAuth # Clients**.
 - b. 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.

The screenshot displays the PingFederate web interface for managing an OAuth client. The navigation menu on the left includes 'Clients', 'Access Token Management', 'Access Token Mappings', 'OpenID Connect Policy Management', and 'CIBA Request Policies'. The main content area is titled 'Clients | Client' and has two tabs: 'Manage Client' (selected) and 'Extended Properties'. Below the tabs, there is a heading 'Manage the configuration and policy information about a client.' followed by several configuration fields:

- CLIENT ID:** A text field containing 'pf_api_access'.
- NAME:** A text field containing 'pf_api_access'.
- DESCRIPTION:** A large, empty text area.
- CLIENT AUTHENTICATION:** A group of radio buttons with options: 'NONE', 'CLIENT SECRET' (which is selected), 'CLIENT TLS CERTIFICATE', and 'PRIVATE KEY JWT'.
- CLIENT SECRET:** A text field with masked characters (dots) and a 'Generate Secret' button to its right.
- At the bottom, there is a 'CHANGE SECRET' checkbox.

 A green toggle switch is visible on the right side of the page.

- c. In the **Client Authentication** field, select **Client Secret**.
- d. In the **Client Secret** field, you can:

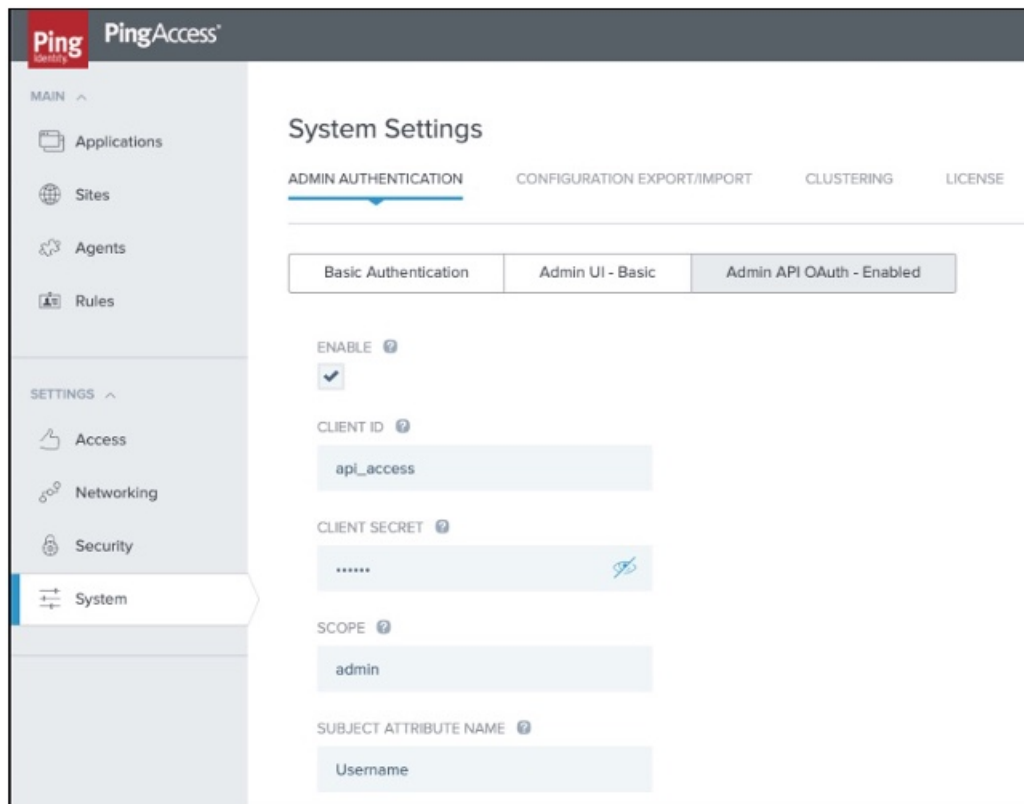
Option	Description
Create or generate a secret.	Choose from: <ul style="list-style-type: none"> ▪ To create a strong, random alphanumeric string, click Generate Secret. ▪ Manually enter a secret.

Option	Description
Modify an existing secret.	<ol style="list-style-type: none"> 1. Select the Change Secret check box. 2. Click Generate Secret to create a strong random alphanumeric string or manually enter a secret.

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

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

2. Configure PingAccess:
 - a. In PingAccess, go to **System # System Settings # Admin Authentication**.
 - b. 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.



The screenshot shows the PingAccess System Settings interface. The left sidebar contains navigation options: MAIN (Applications, Sites, Agents, Rules) and SETTINGS (Access, Networking, Security, System). The main content area is titled "System Settings" and has tabs for ADMIN AUTHENTICATION, CONFIGURATION EXPORT/IMPORT, CLUSTERING, and LICENSE. Under ADMIN AUTHENTICATION, there are three tabs: Basic Authentication, Admin UI - Basic, and Admin API OAuth - Enabled. The Admin API OAuth - Enabled tab is active, showing the following configuration:

- ENABLE:
- CLIENT ID:
- CLIENT SECRET: (with a copy icon)
- SCOPE:
- SUBJECT ATTRIBUTE NAME:

- c. Click **Save**.

3. Configure PingCentral:
 - a. In PingCentral, to connect to the new PingFederate client, go to **Environments # Add Environments**.
 - b. On the **Connect to Instances** page, scroll down and select **PingAccess**.
 - c. 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.
- d. Click **Next**.

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:
 - a. Open the configuration file at `<pingcentral_install>/conf/log4j2.xml`.
 - b. 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>
```

- c. Save and close the file and repeat the task you performed when the error occurred.
- d. For optimal system performance, open the `log4j2.xml` file again and change the logging level back to `INFO`.
- e. 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 PKCS12 file that contains it.

Steps

1. Select the **Setting** tab..

- Expand the **Security** menu and select **TLS Key Pair**.

Result: The TSK Key Pair page displays information about the key pair, including its status and expiration date.

The screenshot shows the PingCentral interface. On the left is a sidebar with a 'SETTINGS' menu. Under 'Security', 'TLS Key Pair' is selected. The main content area is titled 'TLS Key Pair' and contains the following information:

SERIAL NUMBER:	1562079646
SUBJECT DN:	CN=localhost, C=US
ISSUER DN:	CN=localhost, C=US
EXPIRES:	2028-10-27T23:40:40Z
STATUS:	Valid
SUBJECT ALTERNATIVE NAMES:	None
SIGNATURE ALGORITHM:	SHA256withRSA

At the bottom of the main content area, there is a button labeled 'Import Key Pair'.

- To import a new key pair, click **Import Key Pair**.

Result:

- On the **Import Key Pair** window, click **Choose PKCS12 File** and select the .p12 file to upload it.
- In the **File Password** field, enter the password to the keystore file.
- In the **Alias** field, specify the alias of the certificate in the keystore file that you want to use for the Admin Console SSL Certificate, if required.
 - If the .p12 file being imported for 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.
- In the **Key Password** field, enter the password for the selected certificate if the PKCS12 file requires a separate password for the key.
- Click **Import**.
- Restart PingCentral.

Result: After PingCentral restarts, you will be able to access PingCentral without receiving a certificate warning.

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.

- 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. See [Adding trusted CA certificates to PingCentral](#) for details.



Note:

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 a PingFederate environment

Use the wizard to add PingFederate environment to PingCentral.

Steps

1. On the **Environments** page, click **Add Environment**.
2. On the **Connect to Instances** page, Complete the **PingFederate Admin**, **PingFederate Admin Username**, and **PingFederate Admin Password** fields with your authentication information.

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

3. Click **Next**.
4. On the **Name Environment** page, complete the **Name**, **Short Code**, and **Description** fields.
5. **Optional:** 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 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.

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. SpEL expressions are used to determine whether an application requires approval or not. See [Create and test expressions](#).

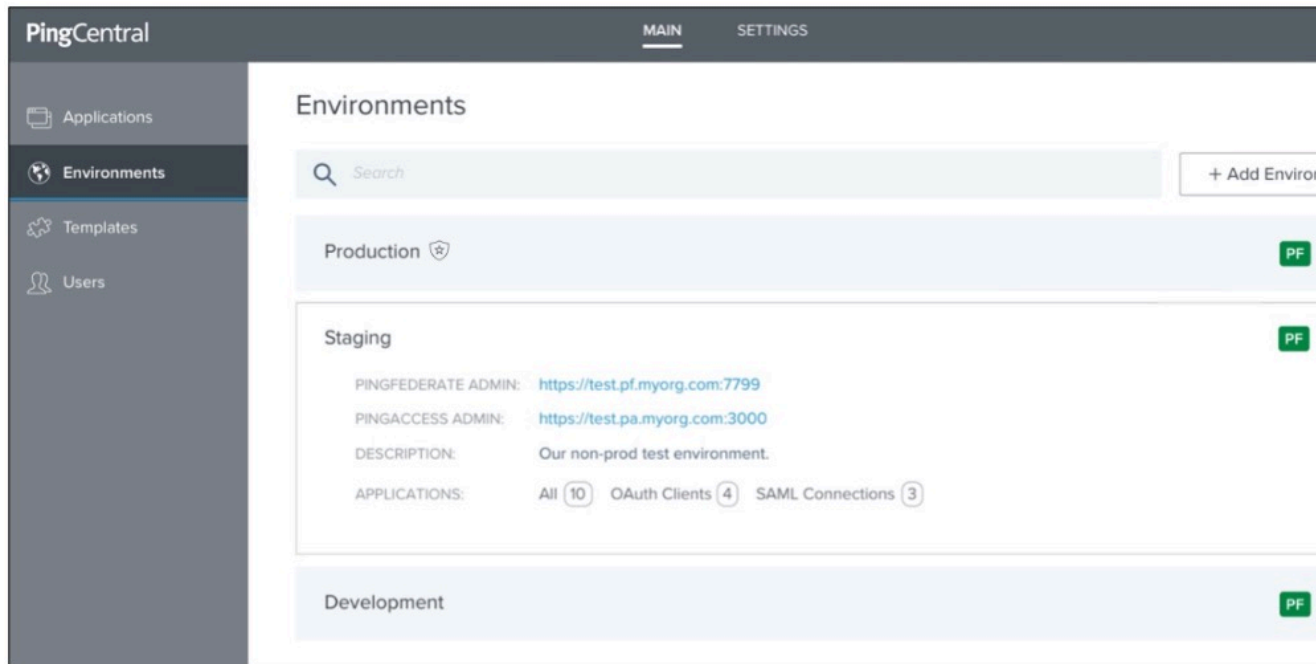
For more information on SpEL, see Spring Expression Language (SpEL) in the Spring Framework documentation.

6. **Optional:** To prevent non-administrators from promoting applications to the environment, select the **Protect** check box.
7. **Optional:** To enforce random secret generation and restrict non-administrators from creating their own, select the **Generate Client Secret on Promotion** check box. PingCentral will generate random client secrets.
8. **Optional:** To add an identity provider 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, a shield icon displays next to its name. A **PF** icon also displays. The color of this icon represents the status of the environment. A green **PF** icon indicates that the environment is verified while a red **PF** icon indicates that the environment isn't verified.

9. Click **Save and Continue**.

10. Click the expandable icon associated with the environment to view environment details. Environment details include:
 - A link to PingFederate.
 - A description of the environment.
 - The total number of applications hosted on this environment and a breakdown of OAuth/OIDC clients and SAML service provider (SP) connections. Click these links to access filtered lists of these applications on the **Applications** page.




Updating environments

Update PingFederate and PingAccess environment information at any time.

Steps

1. 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
To update the name and description:	To update the name and description, change the information in the Name , Short Code , and Description fields.
To 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.
To update connection information:	To update the connection information for either a PingFederate or PingAccess environment, change the information in the Username and Password fields.
	 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
To add or remove protection status:	To add or remove the protected status of an environment, which prevents non-administrators from promoting applications to the environment, select or clear the Only Administrators Can Promote Applications check box.
To 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.
To update the SP certificate:	To update the SP certificate, click Choose to upload a new certificate and enter the certificate password in the appropriate field.
To 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.

2. 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

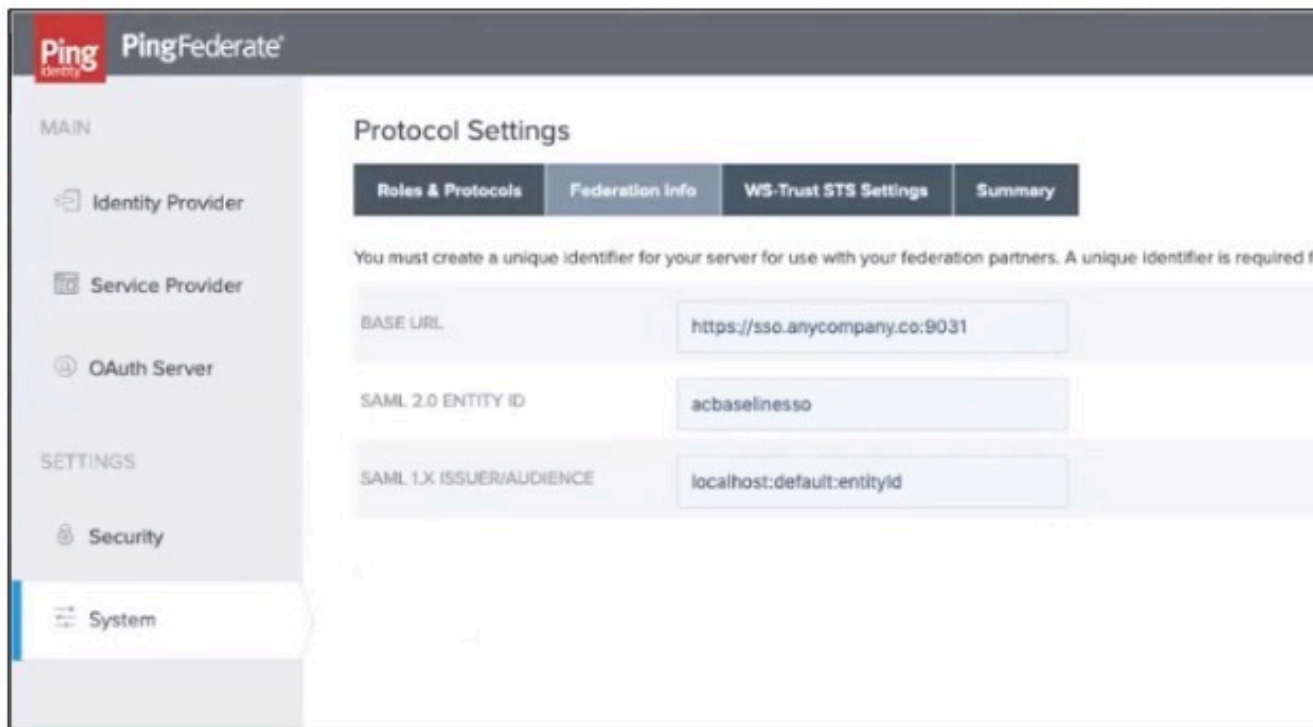
To configure PingFederate as the token provider for PingAccess, the Issuer URL in PingAccess must either match the Base URL in PingFederate, or one of the virtual hosts defined in PingFederate.

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.

The screenshot shows the PingAccess System Settings page. The left sidebar is expanded to 'System'. The main content area is titled 'System Settings' and has tabs for 'ADMIN AUTHENTICATION', 'CONFIGURATION EXPORT/IMPORT', 'CLUSTERING', 'LICENSE', 'TOKEN PROVIDER', and 'TOKEN'. The 'TOKEN PROVIDER' tab is active, showing 'PINGFEDERATE' with a link to 'Change Token Provider Type'. Below this are three tabs: 'Runtime', 'Administration', and 'OAuth Resource Server'. A 'View Metadata' button is present. The configuration fields are:

- ISSUER: `https://localhost:9031`
- DESCRIPTION: `Updating`
- TRUSTED CERTIFICATE GROUP: `Trust Any`

 A 'Show Advanced' link is at the bottom.

- 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.

The screenshot shows the PingFederate Virtual Host Names configuration page. The left sidebar is expanded to 'System'. The main content area is titled 'Virtual Host Names' and includes the text: 'Optionally, you can define a list of alternate host names that may be used by the system in addition to what is defined for the PingFederate Base URL.' Below this is a table with two columns: 'Host Domain Name' and 'Action'.

Host Domain Name	Action
pchost.test.wrong	Edit Delete
<input type="text"/>	<input type="button" value="Add"/>

 At the bottom right, there are 'Cancel' and 'Save' buttons. The footer contains copyright information: 'Copyright © 2003-2019 Ping Identity Corporation All rights reserved Version 9.2.2.0'.

Adding trusted CA certificates to PingCentral

For application owners to securely promote 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.

The screenshot shows the PingCentral interface with the 'Trusted CA Certificates' page. The left sidebar contains the 'SETTINGS' menu with 'Security' expanded to show 'Trusted CA Certificates'. The main content area displays a list of certificates with their details.

Trusted CA Certificates

These certificates are used to make outbound TLS connections to PingFederate and PingAccess in PingCentral environments, and to OpenID backchannel authentication endpoints when SSO is configured.

[+ Add Certificate](#)

Alias	Expires
Test signing cert CN=sso.anycompany.co, O=AnyCompany, C=US	Expires 11-27-2120
PingFederate signing cert CN=sso.anycompany.co, O=AnyCompany, C=US	Expires 05-08-2120
PingAccess signing cert CN=sso.anycompany.co, O=AnyCompany, C=US	Expires 03-31-2120

Test signing cert
CN=sso.anycompany.co, O=AnyCompany, C=US

ALIAS:	Test signing cert
SERIAL NUMBER:	1608580120138
SUBJECT DN:	CN=sso.anycompany.co, O=AnyCompany, C=US
ISSUER DN:	CN=sso.anycompany.co, O=AnyCompany, C=US
VALID FROM:	12-21-2020
SIGNATURE ALGORITHM:	SHA256withRSA
STATUS:	Valid
EXPIRES:	11-27-2120
VERSION:	3
SUBJECT ALTERNATIVE NAMES:	None

Managing users

You can set up PingCentral so users access the application through 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.

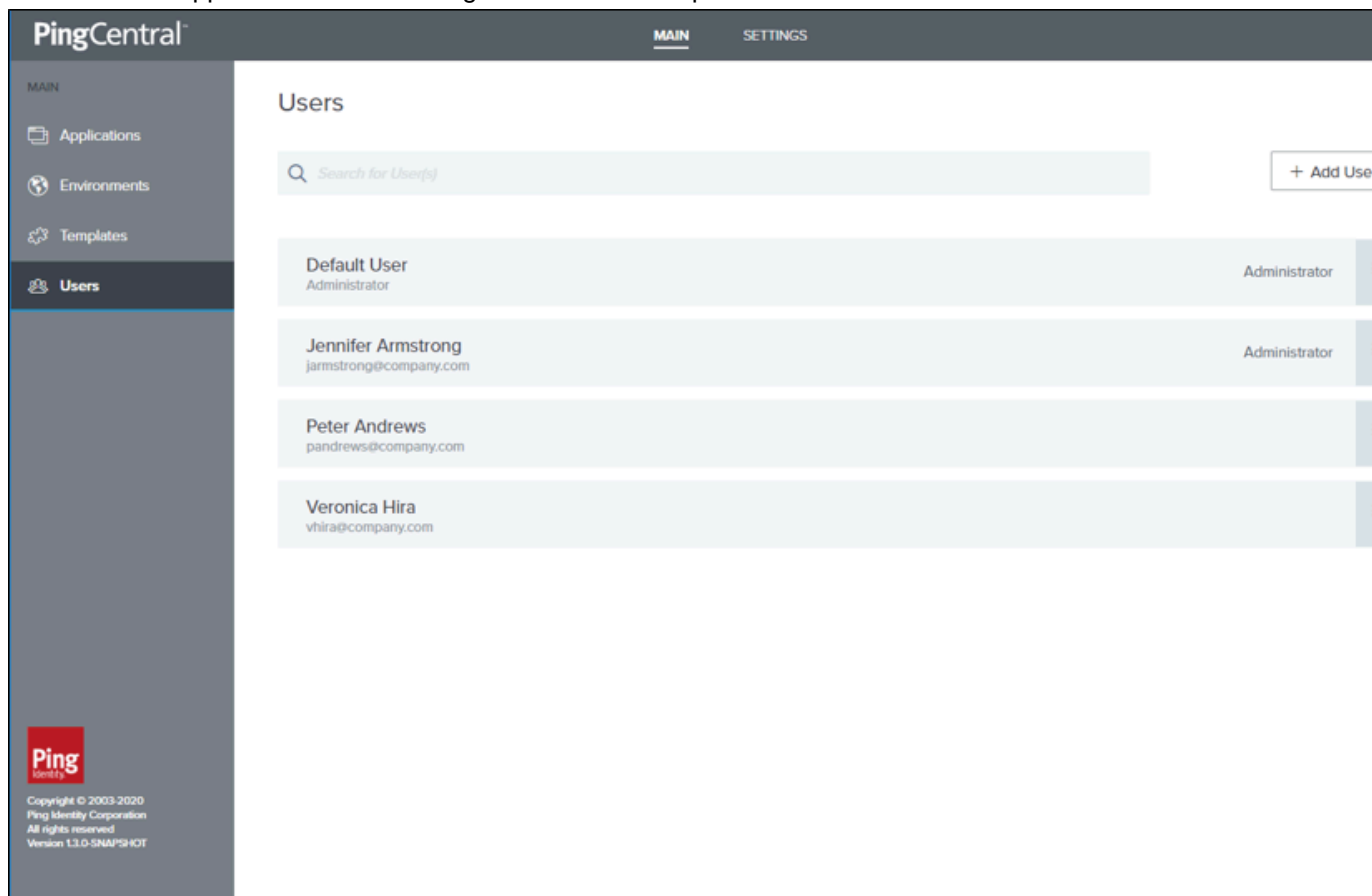
Managing users through PingCentral

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, and last name 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 single sign-on (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 single sign-on (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 sign-on (SSO) is disabled by default.

To configure PingCentral for SSO:

1. Enable SSO.
2. Configure 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, 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 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.

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.
 - a. 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.

- b. 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.

USE CENTRALIZED SIGNING KEY



Select this option to use a centralized key when signing JWTs using an RSA-based or EC-based algorithm.

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.

JWKS ENDPOINT PATH

/oauth/pingcentral/jwks

Path on the PingFederate server to publish a JSON Web Key Set with the keys/certificates that can be used for signature verification. Must include the initial slash (example: /oauth/jwks). The resulting URL will be https://<pf_host>:<port>/ext/<JWKS Endpoint Path>. If specified, the path must be unique across all plugin instances, including child instances.

**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.

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.

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.

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. In the **OpenID Connect** field, select **ID Token Signing Algorithm**, and then **RSA using SHA-256** from the list.
9. 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](#) on page 48.

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.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG
```

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:

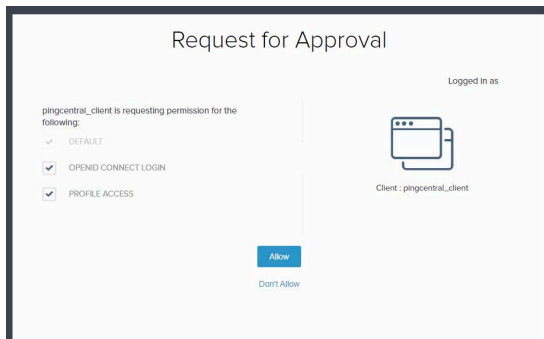
A **Request for Approval** window opens. The scopes listed in the window represent the permissions that PingCentral is requesting. These scopes determine what information PingCentral can access and use.

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.

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.
/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 OAuth

Prometheus pulls information from PingCentral endpoints and stores the data it retrieves.

Steps

1. In PingCentral, in the `conf/application.properties` file, which resides in the PingCentral installation directory, locate and define the following properties.

```
management.metrics.export.prometheus.enabled=true
management.metrics.export.prometheus.step=5s
```

2. Save and close the file.
3. Restart PingCentral.
4. Set up the Prometheus `prometheus.yaml` configuration file and save it in the appropriate location.

Example:

The following example uses the `prometheus.yaml` file locally with `basic_auth`:

```
global:
  scrape_interval: 15s # Set the scrape interval to every 15 seconds.
    Default is every 1 minute.
  # scrape_timeout is set to the global default (10s).

# A scrape configuration containing exactly one endpoint to scrape:
# Here it's Prometheus itself.
scrape_configs:
  # Metrics for PingCentral
  - job_name: 'pingcentral-metrics'
    honor_timestamps: false
    metrics_path: '/actuator/prometheus'
    scrape_interval: 5s
    scheme: https
    static_configs:
      - targets: [ 'xxx.xxx.x.x:9022' ]
    basic_auth:
      username: Administrator
      password: 2Federate
    tls_config:
      insecure_skip_verify: true
```



Important:

Use `insecure_skip_verification: true` exclusively in development or test environments.

5. Access Prometheus.

For more information, see [Get started with Grafana and Prometheus](#) in the Grafana documentation.

Setting up Prometheus using basic authorization

Prometheus pulls information from PingCentral endpoints and stores the data it retrieves.

Steps

1. In PingCentral, in the `conf/application.properties` file, which resides in the PingCentral installation directory, locate and define the following properties.

```
management.metrics.export.prometheus.enabled=true
management.metrics.export.prometheus.step=5s
```

2. Save and close the file.
3. Restart PingCentral.
4. Set up the Prometheus `prometheus.yaml` configuration file and save it in the appropriate location.

Example:

The following example uses the `prometheus.yaml` file locally with `basic_auth`:

```
global:
  scrape_interval: 15s # Set the scrape interval to every 15 seconds.
    Default is every 1 minute.
  # scrape_timeout is set to the global default (10s).

# A scrape configuration containing exactly one endpoint to scrape:
# Here it's Prometheus itself.
scrape_configs:
  # Metrics for PingCentral
  - job_name: 'pingcentral-metrics'
    honor_timestamps: false
    metrics_path: */actuator/prometheus'
    scrape_interval: 5s
    scheme: https
    static_configs:
      - targets: [ 'xxx.xxx.x.x:9022' ]
  basic_auth:
    username: Administrator
    password: 2Federate
  tls_config:
    insecure_skip_verify: true
```



Important:

Use `insecure_skip_verification: true` exclusively in development or test environments.

5. Access Prometheus.

For more information, see [Get started with Grafana and Prometheus](#) in the Grafana documentation.

Setting up Graphite

Use PingCentral to push data to the Graphite time series database.

Steps

1. In PingCentral, in the `conf/application.properties` file, which resides in the PingCentral installation directory, locate and define the following properties.

```
management.metrics.export.graphite.step=5s
management.metrics.export.graphite.enabled=true
management.metrics.export.graphite.host=127.0.0.1
management.metrics.export.graphite.port=2004
```

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

Result: PingCentral automatically starts pushing data to Graphite.

Accessing Prometheus and Grafana

At Ping, we use Prometheus and Grafana to monitor PingCentral in our Docker PingCentral deployment in our CI/CD.

To access Prometheus and Grafana, use URLs that reflect their installation locations using the following format:

Prometheus:

```
http://██.███.██.███:9090/graph
```

To ensure Prometheus is correctly gathering metrics from PingCentral, use

```
http://██.███.██.███:9090/targets
```

Grafana:

```
http://██.███.██.███:3000
```

Setting up Grafana

Use Grafana with either Graphite or Prometheus to view data through interactive dashboards with charts and graphs.

Steps

1. Connect Grafana to either Prometheus or Graphite by adding a data source with the information shown in this example.

The screenshot shows the Grafana 'Data Sources' configuration page for a Prometheus local docker data source. The page is titled 'Data Sources / Prometheus local docker' and has a 'Type: Prometheus' label. It features a 'Settings' tab and a 'Dashboards' tab. The 'Name' field is 'Prometheus local docker' and is marked as 'Default'. The 'HTTP' section includes a 'URL' field set to 'http://172.17.0.1:9090', an 'Access' dropdown set to 'Server (default)', and a 'Whitelisted Cookies' section with an 'Add Name' input and an 'Add' button. The 'Auth' section has several toggle switches: 'Basic auth' (off), 'With Credentials' (off), 'TLS Client Auth' (off), 'With CA Cert' (off), 'Skip TLS Verify' (off), and 'Forward OAuth Identity' (off). The 'Custom HTTP Headers' section has an 'Add header' button. The 'Scrape Interval' is set to '15s', 'Query timeout' is '60s', and 'HTTP Method' is 'Choose'. The 'Misc' section has a 'Disable metrics lookup' toggle (off) and a 'Custom query parameters' field with the example 'max_source_resolution=5m&timeout=10'. At the bottom, there are 'Save & Test', 'Delete', and 'Back' buttons.



Note:

The URL you enter in the **URL** field should reflect the location of your time series database.

2. Click **Save and Test**.
3. Access Grafana.

For more information, see [Accessing Prometheus and Grafana](#).

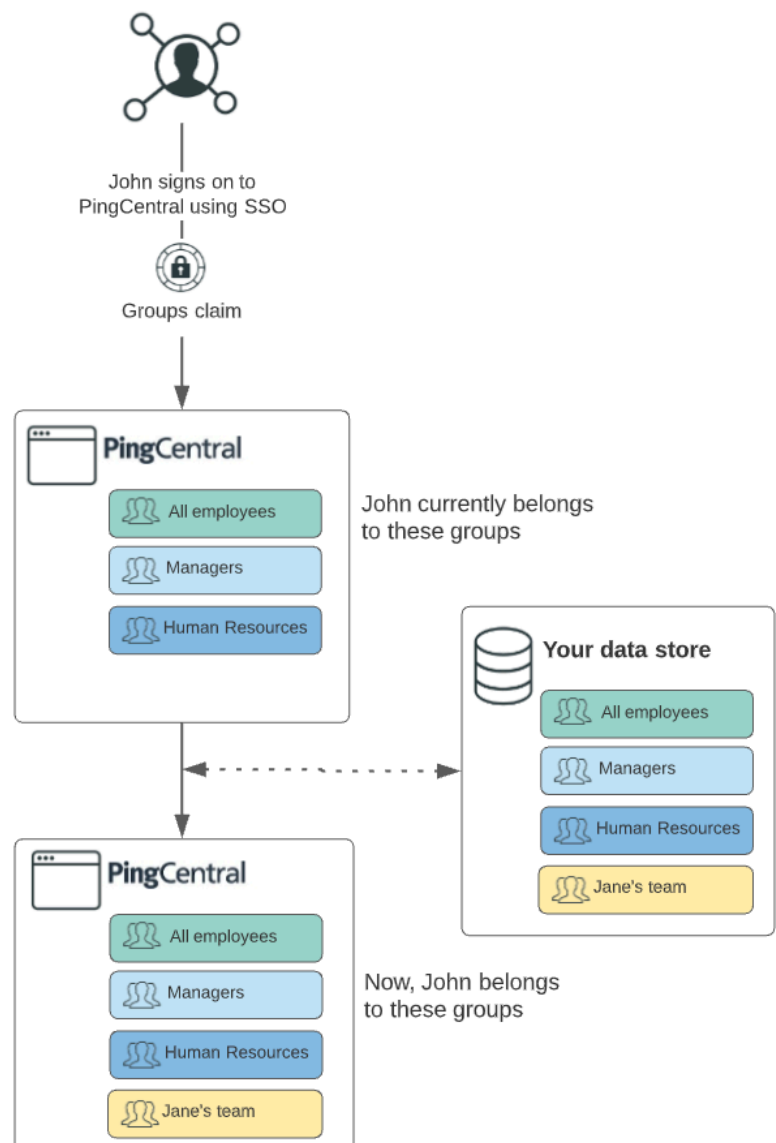
Managing user groups

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.

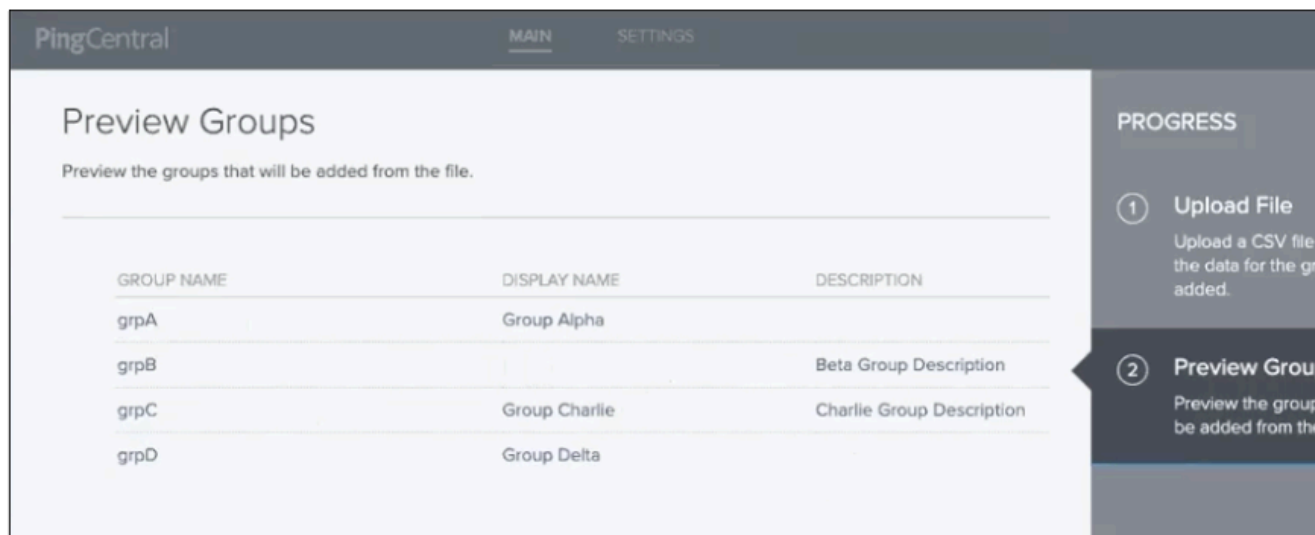
2. To add groups of users one by one:
 - a. On the **Groups** tab, click **Add Group**.
 - b. On the **Add Group** page, complete these fields:
 - **Group Name:** Enter the group name. Group names should match the group names in your data store and are not case sensitive.
 - **Display Name (Optional):**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

The screenshot shows the PingCentral interface. On the left is a navigation sidebar with 'Groups' selected. The main content area is titled 'Groups' and features a search bar containing 'Time Tracking'. Below the search bar, a group card for 'Time Tracking' is displayed. The card includes a description: 'This application uses all common scopes provided by the target environment.' and a 'MEMBERS' section with a count of 2, listing 'Jenna Dover' and 'Molly Smith'. A '+ Add Group' button is visible in the top right corner of the main area.

3. To import information about a group of users:
 - a. On the **Groups** tab, click **Import Groups**.
 - b. On the **Upload File** page, click **Choose**.
 - c. Select the `.csv` files that you want to import and click **Open** and click **Next**.
 - d. 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. .

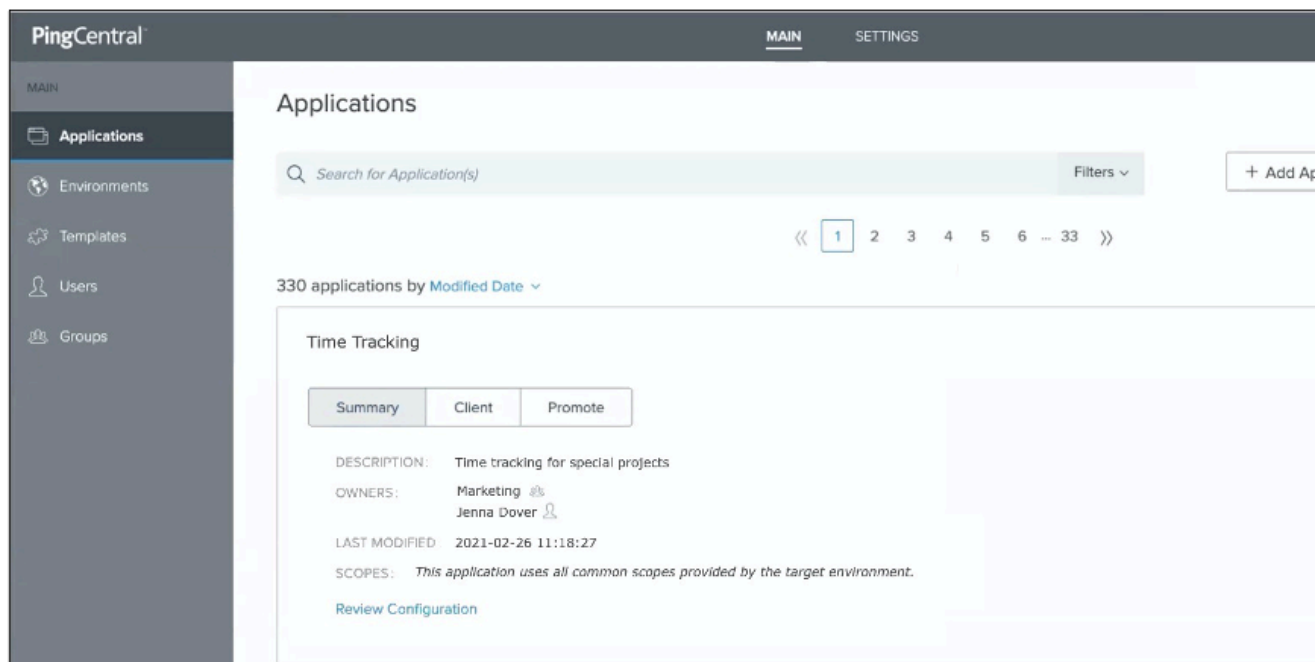
The **Name** field is required, but the **Display Name** and **Description** fields are optional.



- e. 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

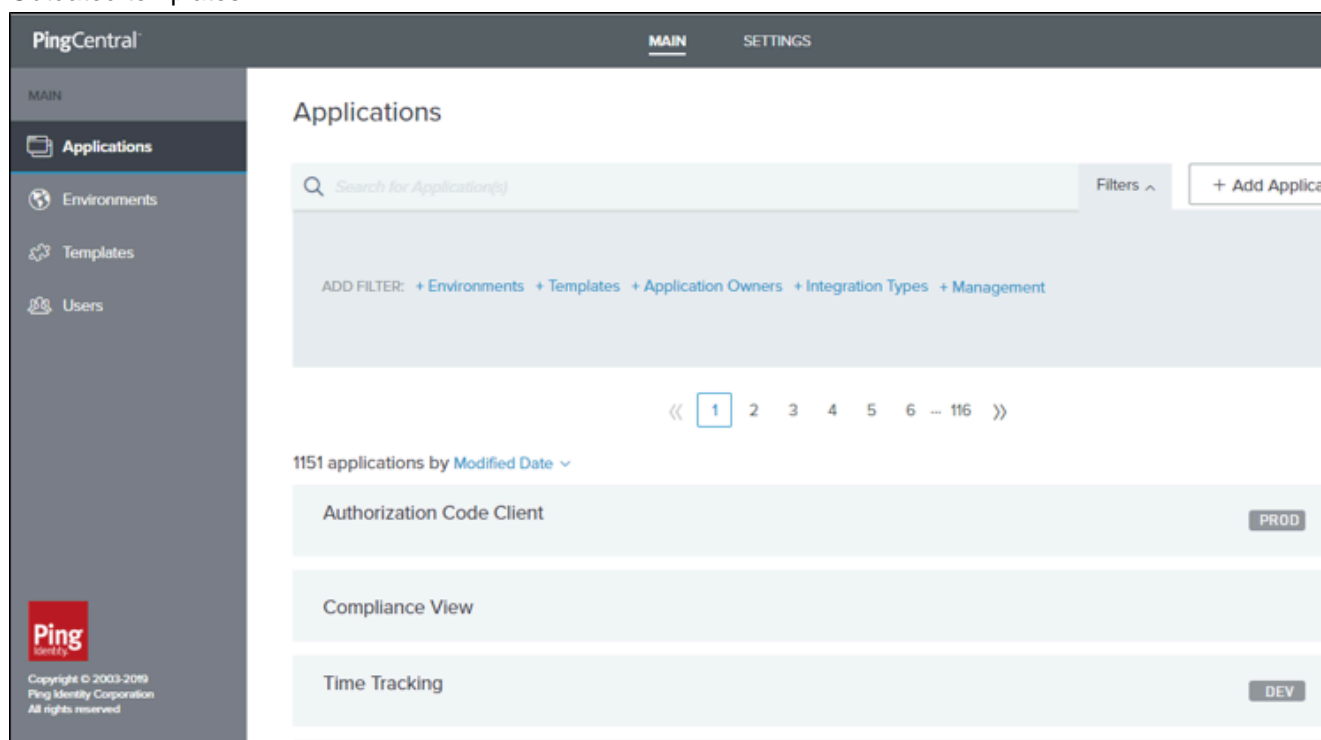
All PingCentral applications and applications in verified PingAccess and PingFederate environments display on the **Applications** page, where you can filter the list of applications, add new applications, update existing applications, and delete them from PingCentral when they are no longer needed.

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
 - Template
 - Application owner, or groups of application owners
 - Integration type (OAuth and OIDC or SAML)
 - Managed (applications created from or promoted to PingCentral environments), and Unmanaged (applications that reside in verified PingAccess or PingFederate environments.)
 - Outdated templates



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

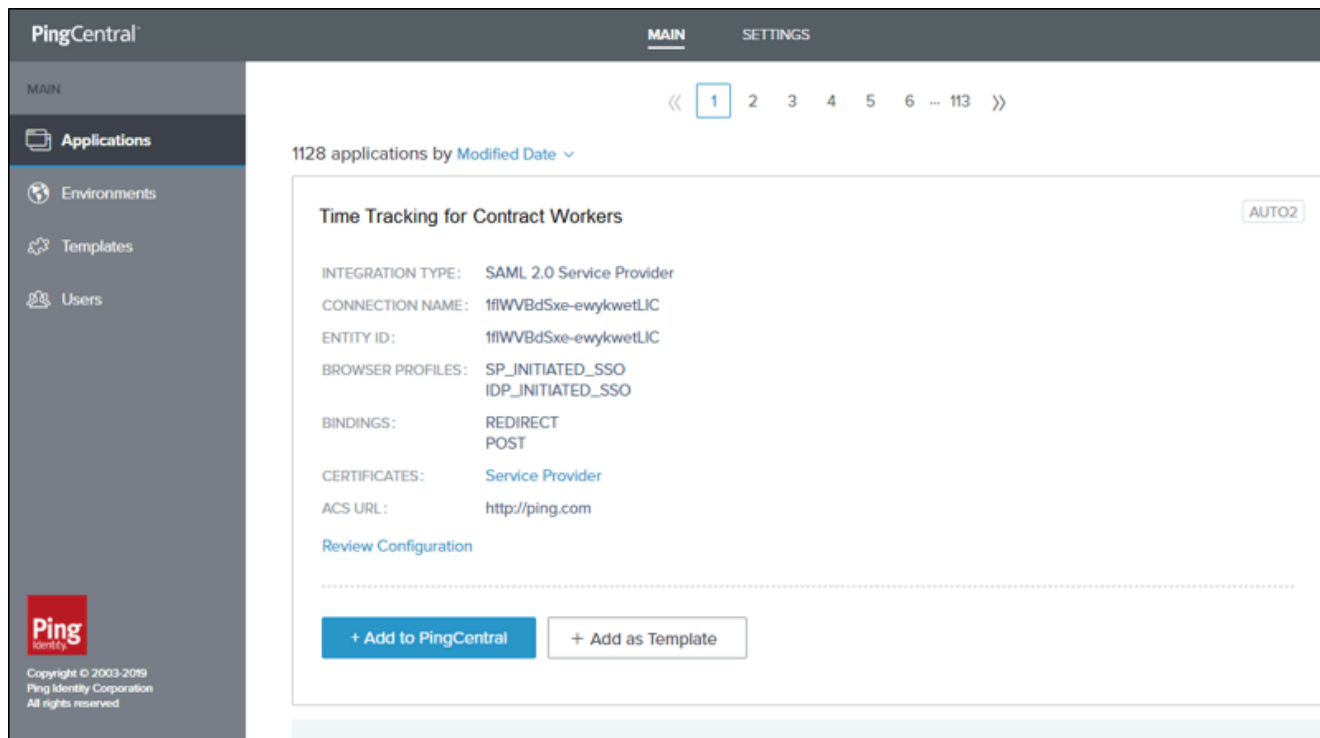
There are a variety of ways you can add applications to PingCentral. You can apply templates to them, you can create templates from them, or you can add them directly to PingCentral.

Steps

1. To apply an OAuth, OIDC, SAML, or PingAccess template to an application:
 - a. Click **Add Application**.
 - b. 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:
 - a. Select the expandable icon associated with the application.
 - b. 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:
 - a. Use the search and filtering features to locate applications.
For more information, see [Filtering applications](#)
 - b. Select the expandable icon associated with the application.
 - c. 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 and then 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.	<ul style="list-style-type: none"> ▪ To change the template used to create the application, click Change Template and select a new template from the Select Template page. ▪ 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 Update Template. Grant types and OpenID Connect (OIDC) policies in the new template will override those specified in the previous template, and scopes from both templates are included in the new version. <div data-bbox="597 793 1468 1003" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note:</p> <p>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.</p> </div>
Update OAuth or OIDC application information.	<ul style="list-style-type: none"> ▪ In the Client section, change the scopes associated with OAuth or OIDC applications. Select or clear the appropriate check boxes. <div data-bbox="597 1115 1468 1352" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note:</p> <p>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.</p> </div> <ul style="list-style-type: none"> ▪ 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.
Update SAML SP application information.	<p>In the Attribute Mappings section, add or remove attributes and expressions or update attribute and expression values.</p> <p>In the Promotions section, upload a new <code>.xml</code> 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.</p> <div data-bbox="548 1745 1468 1913" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note:</p> <p>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.</p> </div>

Option	Steps
	<p>Change the information in the Entity ID or ACS URL fields.</p> <p>To change the signing certificate, select the appropriate certificate in the Signing Certificate list.</p> <p>To change the SP certificate, click SP Certificate to upload a new certificate, or click Remove to remove it.</p> <hr/> <p> Note:</p> <p>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.</p>
<p>Update PingAccess application information.</p>	<ul style="list-style-type: none"> ▪ 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.

2. Click **Save**.

Deleting applications

About this task

You can delete applications within PingCentral, but they will still exist in PingFederate or PingAccess. You need to delete them directly from PingFederate or PingAccess.

Applications owners can also delete applications within PingCentral but might not be able to access PingFederate or PingAccess, so you might receive requests to delete applications from PingFederate or PingAccess for them.

Steps

1. To delete an application from PingCentral, click the associated **Delete** icon.
Result: A message displays asking you if you want to delete the application.
2. Click **Delete**.

Managing templates

Create, update, and delete templates to meet the needs of your organization.

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

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

To create 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.

Update these templates at any time, or revert them to previous versions, as necessary. Applications based on outdated templates have **Outdated Template** icons associated with them, which inform application owners of changes.

Creating 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.

Result:

You see details regarding the selected client.

The screenshot displays the 'Select OAuth Client' page in PingCentral. The interface includes a navigation bar with 'MAIN' and 'SETTINGS' tabs. The main heading is 'Select OAuth Client' with a sub-instruction: 'Select the PingFederate OAuth client you want to base your template on.' Below this, there is an 'ENVIRONMENT' dropdown menu currently set to 'Production Environment'. A 'Client' section features a search bar and a list of client options. The first option, '*Client Credentials (JWT)*', is selected with a radio button. Other options include '-Auto-Application-(190926232739127)-Client Credentials (JWT)-OAuth', '-Auto-Application-(190926232900108)-Client Credentials (JWT)-OpenID', and 'Authorization Code Client'. To the right of the client list, configuration details are shown: CLIENT NAME: '*Client Credentials (JWT)*', CLIENT ID: '*Client Credentials (JWT)*', DESCRIPTION: 'None', GRANT TYPES: 'CLIENT_CREDENTIALS', SCOPES: 'None', ATTRIBUTES: 'None', and OIDC POLICY: 'None'. A 'Review Configuration' link is located below these details. At the bottom of the client list area, it states 'Last retrieved from Production Environment at 10:18 am. Refresh Now'. At the bottom of the page, there are 'Cancel' and 'Next' buttons. On the right side, a 'PROGRESS' sidebar shows three steps: 1. Integration Type, 2. Select OAuth Client (highlighted), and 3. Name Template.

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.

The screenshot displays the 'Select Template' interface in PingCentral. At the top, there are navigation tabs for 'MAIN' and 'SETTINGS'. The main content area is titled 'Select Template' and includes the instruction: 'Select the template your application configuration and policy will be based on.' Below this, four template cards are listed:

- PUBLIC APPLICATION** (OpenID Connect): This app should be accessible internally and externally, and sign-on is not required. Multi-factor authentication will not be required. [Review Configuration](#)
- INTERNAL APPLICATION (AND PARTNERS)** (OAuth): This app should be accessible only to internal employees and partners. They will be required to sign on via SSO, possibly requiring MFA. [Review Configuration](#)
- ACCESS CONTROL POLICY** (PingAccess): Our standard PingAccess template for adding fine-grained access control. [Review Configuration](#)
- EXISTING APPLICATION**: Your application already exists and you want to manage it in PingCentral.

To the right, a 'NEED HELP CHOOSING?' section provides guidance with buttons for:

- OAuth**
- OpenID Connect**
- SAML**
- PingAccess**

On the far right, a vertical sidebar titled 'ADD APPLICATION' shows a progress indicator with two steps:

- 1 Select Template**: Select the template your application configuration and policy will be based on.
- 2 Describe Application**: Provide the basic details for your application.

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 and click the **Pencil** icon.

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

2. Click **Save**.

All applications based on the previous template version display an **Outdated Template** icon next to their names.

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**.

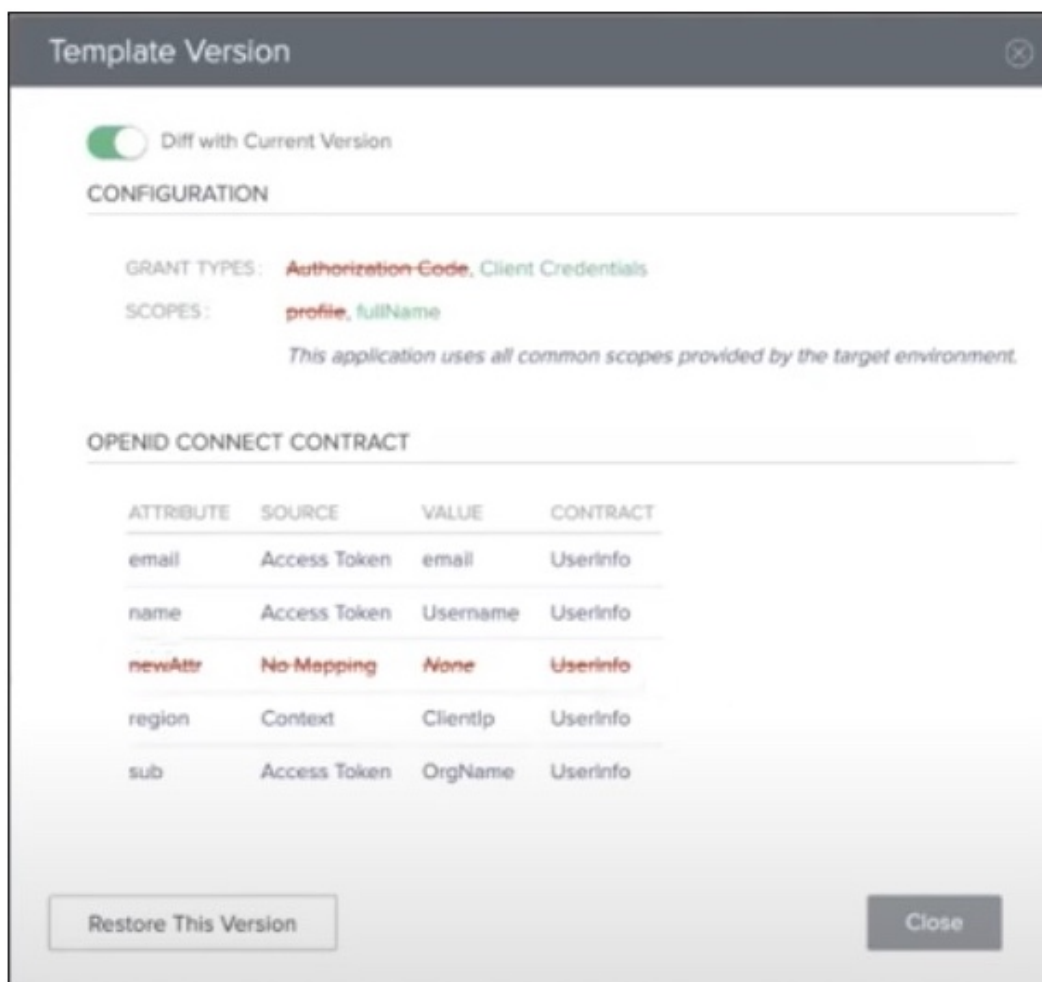
Reverting templates to previous versions

The history of each OAuth and OIDC 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. All applications based on the previous version of this template display an **Outdated Template** icon next to their names.

SAML 2.0 and PingAccess templates

Create, update, or delete SAML and PingAccess templates to meet your needs.

To create 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.

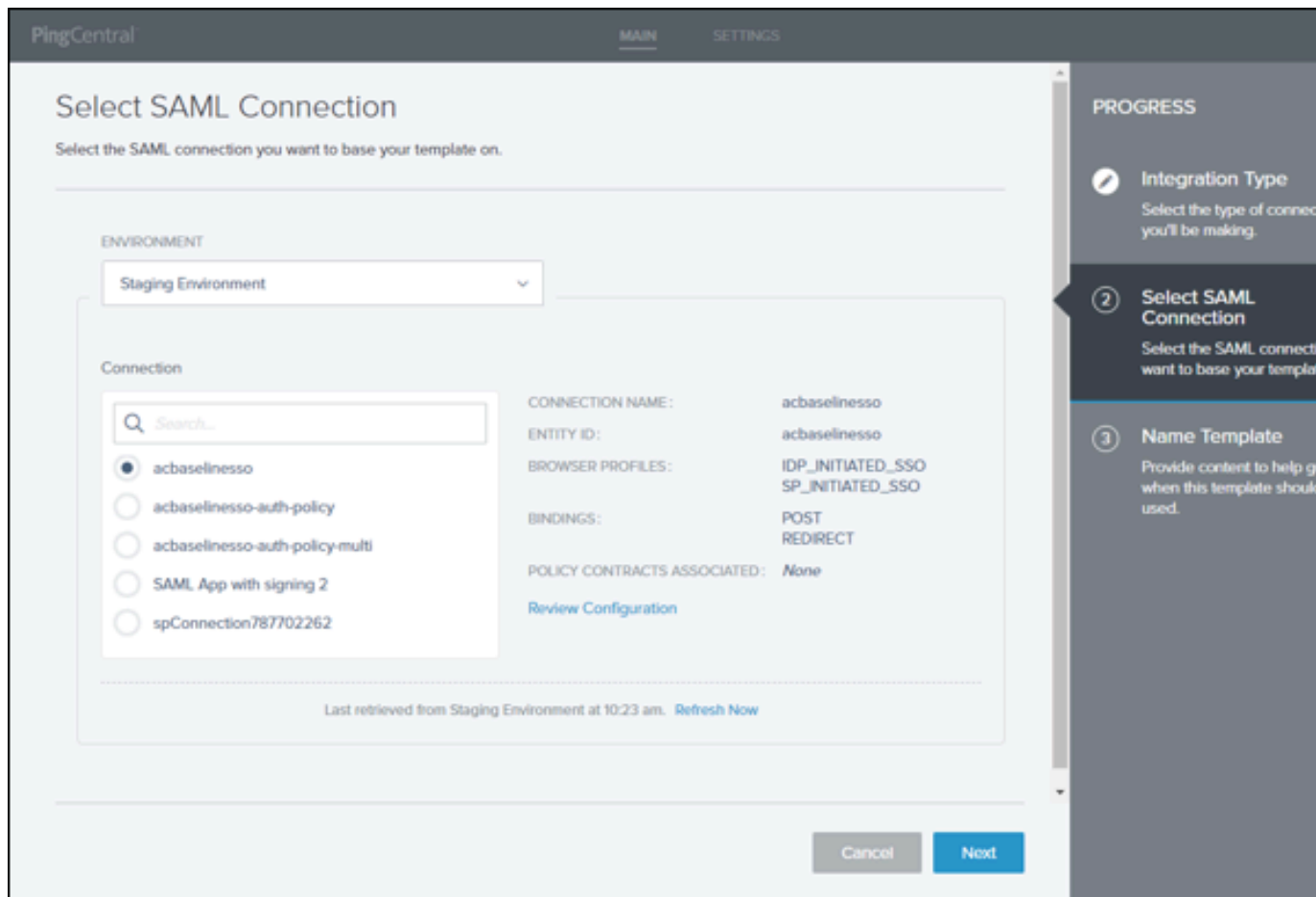
Creating SAML application templates

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.

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. 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.

The screenshot displays the 'Select Template' interface in PingCentral. The main content area lists four templates:

- PUBLIC APPLICATION** (OpenID Connect): This app should be accessible internally and externally, and sign-on is not required. Multi-factor authentication will not be required. [Review Configuration](#)
- INTERNAL APPLICATION (AND PARTNERS)** (OAuth): This app should be accessible only to internal employees and partners. They will be required to sign on via SSO, possibly requiring MFA. [Review Configuration](#)
- ACCESS CONTROL POLICY** (PingAccess): Our standard PingAccess template for adding fine-grained access control. [Review Configuration](#)
- EXISTING APPLICATION**: Your application already exists and you want to manage it in PingCentral.

A sidebar titled 'NEED HELP CHOOSING?' provides additional options:

- API**: OAuth can authorize API access. [OAuth](#)
- WEB APPLICATION**: OpenID Connect provides authentication. [OpenID Connect](#)
- SOFTWARE AS A SERVICE**: SAML can connect to SaaS partner applications. [SAML](#)
- PINGACCESS**: PingAccess applications apply access policy. [PingAccess](#)

On the right, a vertical sidebar shows the 'ADD APPLICATION' process steps:

- 1 Select Template**: Select the template your application configuration and policy will be based on.
- 2 Describe Application**: Provide the basic details for your application.

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

- Connection information
- Attribute names defined in the associated authentication policy contract

Creating PingAccess 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 **PingAccess**. Click **Next**.
3. On the **Select PingAccess Application** page, in the **Environment** list, select the PingAccess environment that hosts the application you want to use as a template.

- In the **Application** list, select the application.

Result:

The application details display next to the **Application** list.

PingCentral MAIN SETTINGS

Select PingAccess Application

Select the PingAccess application you want to base your template on.

ENVIRONMENT
PFPA

APPLICATION

Search...

- Basic Access Policy
- Manager Access Policy
- Disabled Access Policy
- DoNotUse
- Test Access Policy
- Test Dynamic Site Access Token Validator

DESCRIPTION: Manager Access Policy

VIRTUAL HOSTS: virtualhostweb09:7709

CONTEXT ROOT: /pint/myAPPS/Application

APPLICATION TYPE: Web+API

DESTINATION TYPE: Site

SITE: AnyCompany Demo Sites

ACCESS VALIDATION: Token Provider

WEB SESSION: AnyCompany

CLIENT ID: pa_wam

API IDENTITY MAPPING: AnyCompany

WEB IDENTITY MAPPING: AnyCompany

RESOURCES: Another
Extra
Make
More
Root Resource
[Show More](#)

RULES: None

Cancel **Next**

PROGRESS

- Integration Type
Select the type of connection you'll be making.
- Select PingAccess Application**
Select the PingAccess application you want to base your template on.
- Name Template
Provide content to help when this template is used.

- To see the JSON for the PingAccess application, click **Review Configuration**.
- On the **Name Template** page, add a name and description for your template.
This information helps application owners select the appropriate template.
- Select an icon to represent your template.
The icon you choose is shown with the template name and description.

8. Click **Save and Close**.

Result:

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

The screenshot displays the 'Select Template' interface in PingCentral. The main content area lists four templates:

- PUBLIC APPLICATION** (OpenID Connect): This app should be accessible internally and externally, and sign-on is not required. Multi-factor authentication will not be required. [Review Configuration](#)
- INTERNAL APPLICATION (AND PARTNERS)** (OAuth): This app should be accessible only to internal employees and partners. They will be required to sign on via SSO, possibly requiring MFA. [Review Configuration](#)
- ACCESS CONTROL POLICY** (PingAccess): Our standard PingAccess template for adding fine-grained access control. [Review Configuration](#)
- EXISTING APPLICATION**: Your application already exists and you want to manage it in PingCentral.

A sidebar titled 'NEED HELP CHOOSING?' provides additional options:

- API**: OAuth can authorize API access. [OAuth](#)
- WEB APPLICATION**: OpenID Connect provides authentication. [OpenID Connect](#)
- SOFTWARE AS A SERVICE**: SAML can connect to SaaS partner applications. [SAML](#)
- PINGACCESS**: PingAccess applications apply access policy. [PingAccess](#)

On the right, a vertical sidebar shows the 'ADD APPLICATION' process with two steps: 1. Select Template (current step) and 2. Describe Application.

For PingAccess applications, the following items are saved:

- Virtual host information
- The context root
- Application type (Web, API, or Web + API)
- Destination type (site or agent)
- Web session information
- Identity mappings
- Resource definitions
- The rules with the application and resource policies

Updating SAML and PingAccess templates

Steps

1. To update a SAML or PingAccess template, click the **Expand** icon associated with the template and click the **Pencil** icon.

All of the editable information is on one page.

2. Update the information in the **Name** and **Description** fields or select a new icon to represent the template.
3. Click **Save**.

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](#).

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 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 yet 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:** The application's URL to which SAML assertions from the identity provider are sent after user authentication occurs.
- **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.

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.

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.

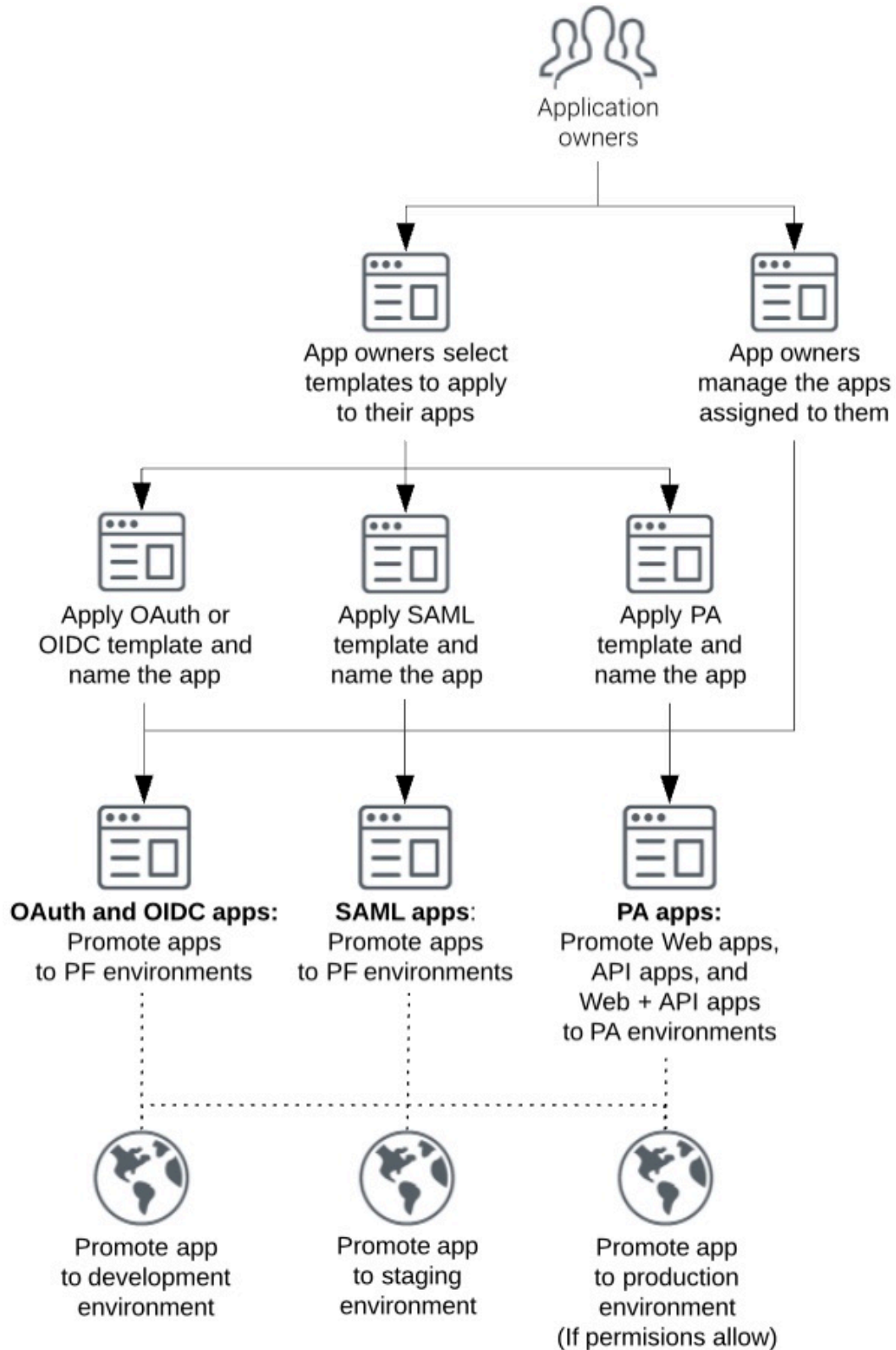
- Provides a central monitoring location for greater visibility into applications across deployment life cycles.
- Minimizes the risk of promoting applications with vulnerable security policies within your organization.

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.

- 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 will 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.

The screenshot displays the PingCentral interface for managing applications. The top navigation bar includes 'PingCentral', 'MAIN', and 'SETTINGS'. A left sidebar shows 'MAIN' and 'Applications'. The main content area is titled 'Applications' and features a search bar with the placeholder 'Search for Applications' and a '+ Add Application' button. Below the search bar, it indicates '7 applications by Modified Date'. The applications are listed in a table-like format with the following details:

Application Name	Protocol	Environment	Actions
Sales: Expense tracking	OAuth	DEV	⋮
Sales: Project tracking	SAML 2.0 Service Provider	DEV	⋮
Sales: Travel scheduling	OAuth		⋮
Sales: Resource requests	SAML 2.0 Service Provider	DEV	⋮
Sales: New employee onboarding app	OpenID Connect	PROD, DEV	⋮
Accommodation requests	OAuth	PROD, DEV	⋮
Travel requests	SAML 2.0 Service Provider	DEV	⋮

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.



Note:

Although the application will no longer be available in PingCentral, it will still exist in PingAccess or PingFederate. Ask your administrator to delete it from PingAccess or PingFederate, as necessary.

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:

SAML, OAuth, 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.

- 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.

The screenshot shows the PingCentral interface for managing applications. The main header is 'Applications' with a search bar and a '+ Add Application' button. Below the header, it indicates '2 applications by Modified Date'. The first application is 'Accounting' with the template '-Template-OpenID' and a 'STG' environment icon. It has three tabs: 'Summary', 'Template', and 'Promote'. A '+ Promote' button is visible. Below the tabs, there are two tables. The first table, 'ENVIRONMENT', shows a row for '-Staging Environment' with a 'LAST PROMOTED' date of '2020-02-26 12:56:28' and a 'View Client Details' link. The second table, 'HISTORY', shows two rows for '-Staging Environment' with 'PROMOTED' dates of '2020-02-26 12:56:28' and '2020-02-26 12:52:29', each with a 'View Client Details' link. The second application, 'Time Tracking' with template '-Template-SAML', is partially visible at the bottom with a 'PROD' environment icon. The footer contains the Ping Identity logo and copyright information: 'Copyright © 2003-2020 Ping Identity Corporation All rights reserved. Version 13.0-SNAPSHOT'.

- 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.
- 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, OIDC, 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.

PingCentral MAIN SETTINGS

Select Template


Select the template your application configuration and policy will be based on.



PUBLIC APPLICATION OpenID Connect

This app should be accessible internally and externally, and sign-on is not required. Multi-factor authentication will not be required.


[Review Configuration](#)



INTERNAL APPLICATION (AND PARTNERS) OAuth

This app should be accessible only to internal employees and partners. They will be required to sign on via SSO, possibly requiring MFA.


[Review Configuration](#)



ACCESS CONTROL POLICY PingAccess

Our standard PingAccess template for adding fine-grained access control.

[Review Configuration](#)



EXISTING APPLICATION

Your application already exists and you want to manage it in PingCentral.

NEED HELP CHOOSING?

What kind of application is this?

API
OAuth can authorize API access.
[OAuth](#)

WEB APPLICATION
OpenID Connect provides authentication.
[OpenID Connect](#)

SOFTWARE AS A SERVICE
SAML can connect to SaaS partner applications.
[SAML](#)

PINGACCESS
PingAccess applications apply access policy.
[PingAccess](#)

ADD APPLICATION

- 1 Select Template**
Select the template your application configuration and policy will be based on.
- 2 Describe Application**
Provide the basic details for your application.

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 username 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 login. 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.

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.

PingCentral MAIN

Select Metadata

Provide SAML metadata for simpler configuration.

If you have SAML metadata for this application, provide it here.

ENTITY ID: EntityID-Random

ACS URL: https://sso.anycompany.co:9031/idp/SSO.saml2

CERTIFICATE: CN=Config Signing Cert, OU=Dev, O=Ping, L=Denver, ST=CO, C=US
Valid 08-2018 to 08-2033

ATTRIBUTES: anycompanyCustomAttribute
sn
cn

[Remove](#) [Or Use URL](#)

[Cancel](#) [Next](#)

PROGRESS

- 1 Select Template
Select the template you want to use. The application configuration policy will be based on this template.
- 2 Select Metadata**
Provide SAML metadata for simpler configuration.
- 3 Map Attributes
Map your application's attributes to source attributes and static values.
- 4 Describe Application
Provide the basic details for your application.

2. Click **Next**.

- 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.

Result:

Add OGNL expressions to fine-tune attribute values to meet your needs.

The screenshot displays the 'Map Attributes' interface in PingCentral. At the top, there are tabs for 'MAIN' and 'SETTINGS'. The main content area is titled 'Map Attributes' and includes the instruction 'Map your application's attributes to source attributes and static values.' Below this, there are two rows for mapping application attributes to identity attributes. The first row shows 'SAML_SUBJECT' mapped to 'subject'. The second row shows 'sn' mapped to '- Expression -', with a dropdown menu open for selecting an expression value. The dropdown menu lists several options: 'Select one...', 'Data subset expression', 'Date format change expression', 'Number concatenate expression', and 'Number conversion expression'. A '+ Add Attribute' link is visible below the second row. At the bottom right, there are 'Cancel' and 'Next' buttons. On the right side, a 'PROGRESS' sidebar shows the current step '3 Map Attributes' highlighted, with other steps '1 Select Template', '2 Select Metadata', and '4 Describe Application' listed below it.

- When you're finished, click **Next**.
- 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.

- 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.

- 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.

PingCentral MAIN SETTINGS

Define Resources

Define your application's context root and resources.

CONTEXT ROOT

/mygreatapp

RESOURCES [+ Add Resource](#) [Reorder Resources](#)

RESOURCE NAME

More

RESOURCE AUTHENTICATION

Standard Anonymous Unprotected

PATH PATTERNS

/Ping/More/More* Regex

[+ Add Path Pattern](#)

METHODS

*

OPTIONS

Audit Enabled

RESOURCE NAME

Root Resource

RESOURCE AUTHENTICATION

Standard Anonymous Unprotected

PATH PATTERNS

/*

METHODS

*

OPTIONS

Audit Enabled

PROGRESS

- 1 Select Template
Select the template your application configuration policy will be based on.
- 2 **Define Resources**
Define your application's context root and resources.
- 3 Define Application Policy
Customize your policy for your application.
- 4 Define Resource Policy
Customize the policy for your resources.
- 5 Describe Application
Provide the basic details for your application.



Note:

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

To add a new resource:

- a. Click **Add Resource** and in the **Resource Name** field, enter the name of the resource.
- b. 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.

- c. 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**.

- d. 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.
- e. To log information regarding requests to this resource, select the **Audit** check box.
- f. Resources are enabled when they are added, by default. To disable a resource, clear the **Enable** check box.
- g. 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.

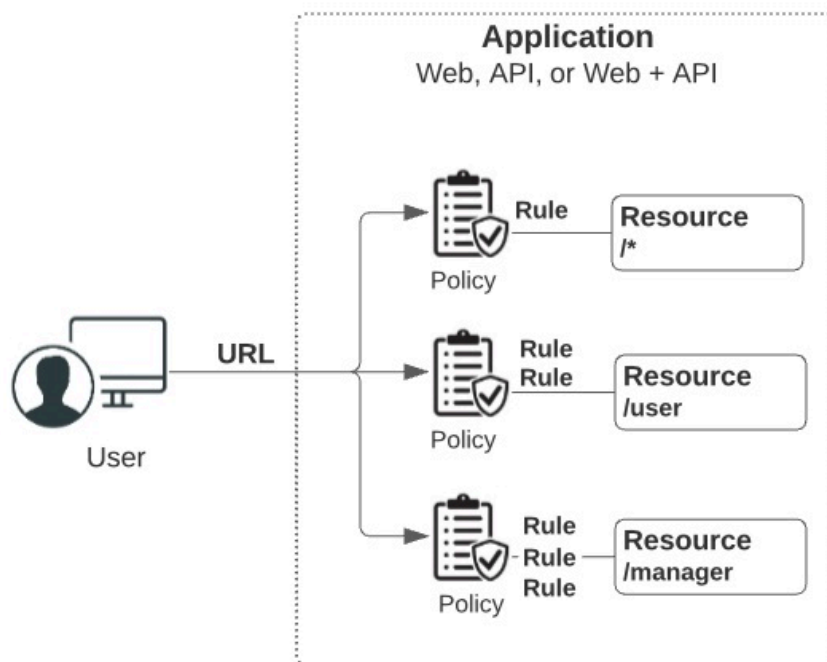
Information needed to add PingAccess applications

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

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.

Virtual host:

`https://den-ping.com:8843/mygreatapp/home`

Context root:

`https://den-ping.com:8843/mygreatapp/home`

Resource:

`https://den-ping.com:8843/mygreatapp/home`

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

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:

```
/[^\s]+/[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 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.

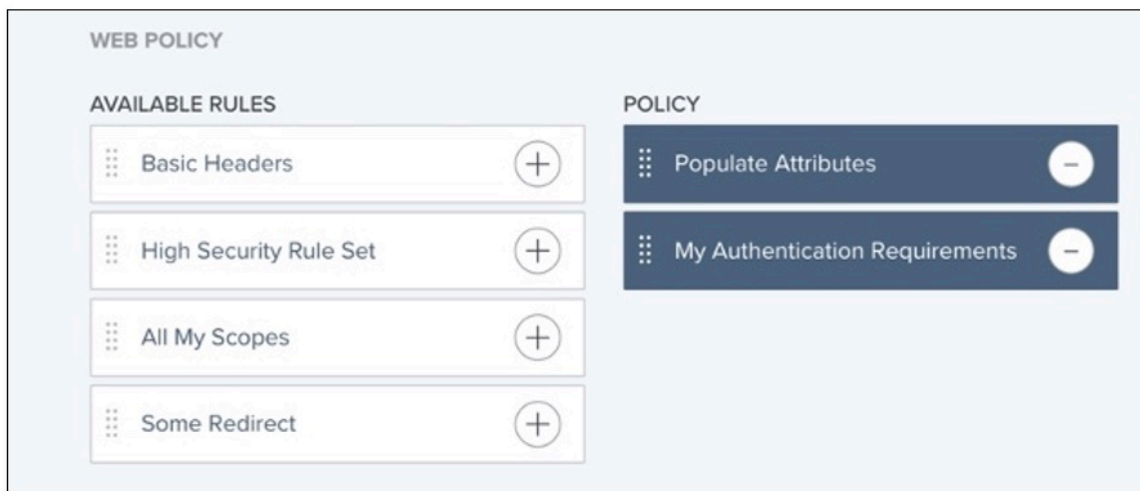
When you put rules together, they are called policies.

- **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](#)

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**.
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 redirect URIs are required to promote the application, enter them in the **Redirect URIs** field.
4. If a client secret is required to authenticate your application, you can:
 - Create a custom secret and enter it in the **Client Secret** text box.
 - Generate a client secret by clicking the **Generate Secret** button.

Promote to Environment

Promoting Time Tracking to the Development Environment. Please confirm the redirect URIs for this environment.

REDIRECT URIS

https://company.com ×

CLIENT SECRET

5. Click **Promote**.

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

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

Promotion Details

Staging - 2020-02-26 10:12:18

^ PROMOTION

PROMOTED: 2020-02-26 10:12:18

CURRENT OWNERS: Jennifer Armstrong

BASIC

OIDC DISCOVERY ENDPOINT: <https://sso.anycompany.co:9031/well-known/openid-configuration>

CLIENT ID: a4992be3-30d5-4ca0-8376-5dc7f0582dc2

CLIENT SECRET:

ADVANCED

GRANT TYPE: IMPLICIT

TOKEN AUTH METHOD: NONE

∨ SUMMARY

∨ CLIENT

∨ OIDC POLICY

∨ ACCESS TOKEN MANAGER

Revert Application

CI

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:** the application's URL to which SAML assertions from the identity provider will be sent after user authentication occurs.
- **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**.
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. In the **Entity ID** and **ACS 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.

4. 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.

5. 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 \(SAML 2.0\)](#)

- 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.

- 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.

- 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.

Promotion Details ✕

Time Tracking - Staging -2021-05-20 17:38:41

^ PROMOTION

PROMOTED: 2021-06-24 17:38:41

ACS URL: <https://acme.com>

SSO ENDPOINT URL: <https://sso.anycompany.co:9031/idp/SSO.saml2>

CERTIFICATES: [Identity Provider](#)

SAML METADATA: [Download Service Provider Metadata](#)

∨ SUMMARY

∨ CONNECTION

Revert Application

Close

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

- 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.

- Go to the **Promote** tab and click the **View Connection Details** link.

Result:

The promotion information displays.

- Click **Download Service Provider Metadata** to download the metadata as a .xml file and click **Close**.

Note the location of this file to promote similar SAML applications.

- Update applications with this service provider information, as appropriate.

For more information, see [Updating applications](#).

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 applications	API applications	Web + API applications
Web session (optional)	Web session (optional)	Web session (required)
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**.
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.

- 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.

The screenshot displays the 'Configure Promotion' interface in PingCentral. At the top, there are navigation tabs for 'MAIN' and 'SETTINGS'. The main heading is 'Configure Promotion', followed by the instruction: 'Select the values specific to this application in the target environment.' Below this, the application being promoted is identified as 'Promoting Application Reorder Resources-TLyTTJItDc to PF2-Host'.

The configuration fields are organized into sections:

- VIRTUAL HOSTS:** A text input field containing 'virtualhostweb:9000' with a close button (x).
- ACCESS VALIDATION:** A dropdown menu set to 'Token Provider'.
- WEB SESSION:** A dropdown menu set to 'XYZ Company web session'.
- API IDENTITY MAPPING:** A dropdown menu set to 'XYZ Company API mapping'.
- WEB IDENTITY MAPPING:** A dropdown menu set to 'XYZ Company Web mapping'.
- SITE:** A dropdown menu set to 'XYZ Company Site'.

At the bottom right of the form, there are two buttons: 'Cancel' and 'Next'. On the right side of the screen, a 'PROGRESS' sidebar shows two steps: '1 Configure Promotion' (the current step) and '2 Review Promotion'. The description for step 1 is 'Select the values specific to this application in the target environment.'

- Click **Next**.
- On the **Review Promotion** page, review promotion information you added. Additional detail is available in the **Summary** and **Application** sections of the page.
- Click **Promote and Close**.
- 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.

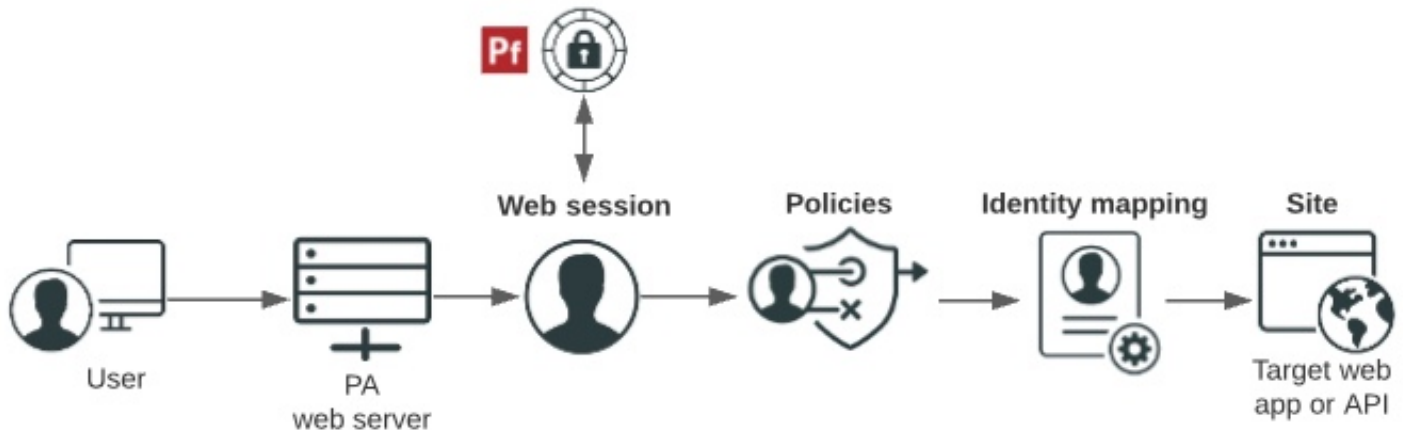
PingAccess can be deployed in one of two ways:

- **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.



- 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.

- 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.

- 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.
- Users are authenticated through the web session.
- 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.

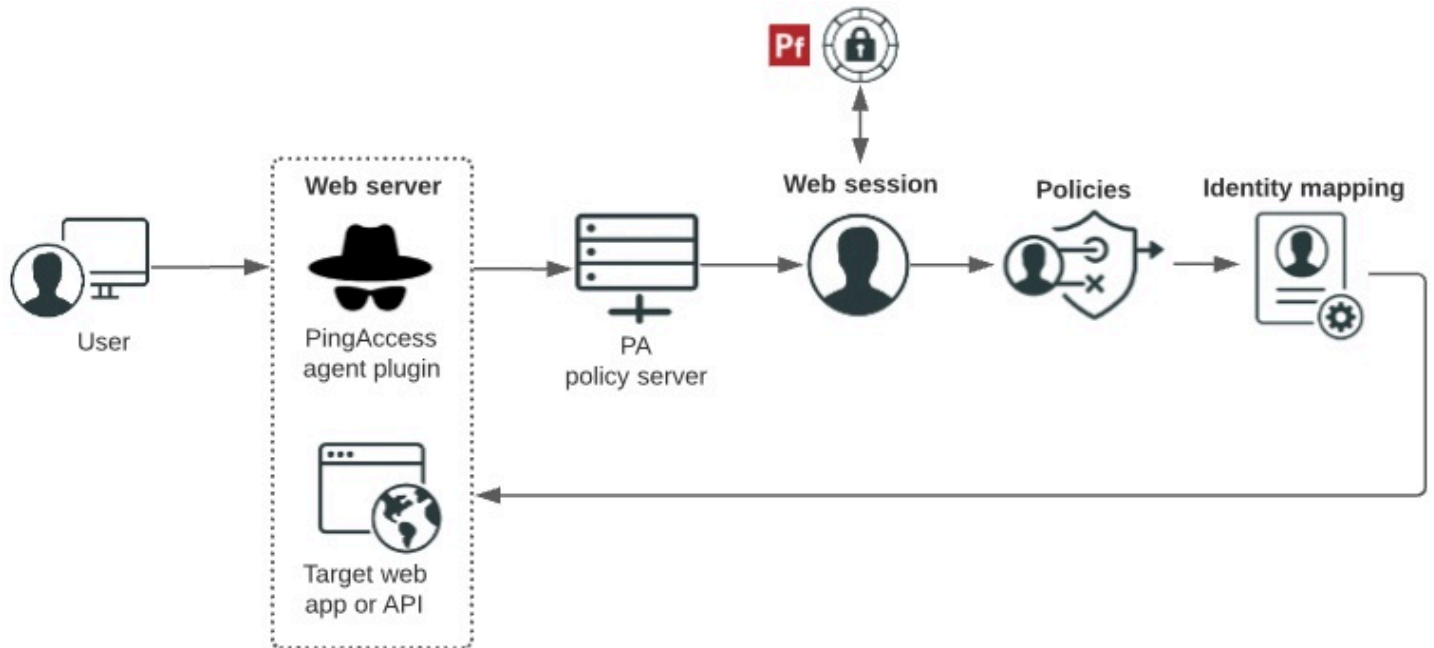
6. Identity mapping is applied to the request if the target application expects user information to be included to further authenticate the user.

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.