

# PingCentral



# Contents

<b>Release Notes.....</b>	<b>3</b>
PingCentral 1.2.0.....	3
PingCentral 1.0.1.....	4
PingCentral 1.0 known issues and limitations.....	5
<b>PingCentral for Application Owners.....</b>	<b>7</b>
Introduction to PingCentral.....	7
Accessing PingCentral.....	9
Viewing application information.....	10
Adding and promoting applications.....	11
Selecting a template.....	11
Using OAuth and OIDC templates.....	13
Using SAML SP templates.....	15
Updating applications.....	19
Reverting applications to previously promoted versions.....	21
<b>PingCentral for IAM Administrators.....</b>	<b>22</b>
Introduction to PingCentral.....	22
System requirements and supported configurations.....	23
PingCentral licensing.....	28
Use Docker to deploy PingCentral.....	29
Install and configure PingCentral.....	29
Installing PingCentral on Microsoft Windows.....	30
Installing PingCentral on Red Hat Enterprise Linux.....	30
Creating and configuring trust.....	31
Configuring PingCentral to run as a Linux systemd service.....	33
Configuring PingCentral to run as a Linux systemv service.....	34
Configuring PingCentral to run as a Windows service.....	35
Setting up MySQL.....	35
Upgrade PingCentral.....	36
Upgrading to PingCentral version 1.2.0.....	38
Configuring logging.....	39
Replacing the Admin Console SSL Certificate.....	40
Managing environments.....	41
Managing applications.....	43
User management.....	44
Setting up SSO for PingCentral.....	45
Managing users through PingCentral.....	47
Template management.....	48
Creating OAuth and OIDC application templates.....	49
Creating SAML SP application templates.....	50
Promotion processes.....	52

# Release Notes

---

## PingCentral 1.2.0

---

New features, resolved issues, and new known issues are listed and described here. For the best possible experience, review this information, and the information outlined in [PingCentral 1.0 known issues and limitations](#), prior to using PingCentral.

### New features

Ticket ID	Description
PASS-939	In addition to seeing the list of applications managed within PingCentral, administrators can see all of the applications that exist in connected PingFederate environments. This enhanced view makes it easy for administrators to review application configurations, and quickly save the configurations as templates or add them directly to PingCentral without going through the Add Application wizard.
PASS-1115	Administrators can filter their application lists by environment, template, application owner, integration type (OAuth and OIDC or SAML), management type (managed or unmanaged), or by using any combination of these filters.
PASS-1318	Administrators can restrict application owners from promoting their applications to specific environments. Protected environments display shield icons next to their names within PingCentral.
PASS-1469	Administrators and application owners can change the templates associated with SAML applications, rather than creating new applications using different SAML templates. Attribute mappings will likely need to be recreated before the application is promoted.
PASS-1525	Administrators can run PingCentral as a Linux systemd service, a Linux systemv service, or a Windows service.
PASS-1826	Administrators can configure PingCentral to use the MySQL relational database management system instead of using the default H2 database.
PASS-1832	The ACS URL is used to promote SAML applications instead of the base URL.
PASS-2016	Certificates are no longer required to promote SAML applications that do not require SP certificates.
PASS-2158	Administrators and application owners can sort their application lists by modified date or application name.
PASS-2203	After application owners promote their SAML applications, the SSO endpoint URL displays on the Promotion Details window and is available for them to give to their service providers.
PASS-2424 PASS-2425	Administrators can use the Linux or Windows upgrade utility to upgrade from PingCentral version 1.0.1 to version 1.2.0. PingCentral cannot be upgraded directly from version 1.0.0 to 1.2.0.
PASS-2925	When adding environments, users who select the <code>Skip Verification</code> option and enter passwords with more than 32 characters receive data integrity violation errors.

## Resolved issues

Ticket ID	Description
PASS-2496	Administrators can now update logging files directly through the <code>log4j2.xml</code> file instead of accessing the <code>application.properties</code> file.

## New known issues

Ticket ID	Description
PASS-2093	When SSO is enabled, custom session settings are modifiable but are not honored.
PASS-2119	Protected environment text on the Environments page refers to “production,” even if the protected environment is not a production environment.
PASS-2468	Administrators cannot update information for users not associated with a PingCentral environment, template, or application.
PASS-2470	Unverified environments should not display when templates and applications are added to PingCentral, and when applications are promoted. If selected, users receive an error message.
PASS-2585	Applications that include spaces at the end of the application name can only be promoted once.
PASS-2766	Using special characters when searching on the Environments, Templates, and Users pages results in a server error.
PASS-2783	The sorting feature is case sensitive for applications managed within PingCentral.
PASS-2819	The <b>Client Secret</b> field displays in the Promotion History page, even if it is not relevant to the application.
PASS-2824	Users who enter invalid application names when updating their SAML applications do not receive an error message.
PASS-2872	Administrators who are deleted or demoted to an Application Owner role can still perform administrative tasks during an open session.
PASS-2879	When updating SAML applications, PingCentral does not indicate whether certificates are optional.
PASS-2888	After an environment is created in PingCentral, the administrator must refresh the page before they can add a user.
PASS-2925	When adding environments, users who select the <b>Skip Verification</b> option and enter passwords with more than 32 characters receive data integrity violation errors.

## PingCentral 1.0.1

---

PingCentral 1.0.1 is a maintenance release for PingCentral 1.0. For the best possible experience, review this information and the information outlined in [PingCentral 1.0 known issues and limitations](#) on page 5 prior to using PingCentral.

## Resolved issues

Ticket ID	Description
PASS-909	If you have only one person with an Administrator role, you can no longer change that person's role to Application Owner.
PASS-1620	Fixed an issue that caused a blank white screen to occasionally display instead of the intended details when the <b>View Client Details</b> link in the Promotion History section of the page was clicked.
PASS-2296	Corrected the PingCentral download location in the Red Hat Enterprise Linux installer.
PASS-2276 PASS-2131	Having the <b>Username</b> field empty during the login process no longer results in a server error.

## New known issue

Ticket ID	Description	Workaround
PASS-2496	Updating the <code>log4j2.xml</code> file has no effect.	Update logging levels through the <code>application.properties</code> file.

## PingCentral 1.0 known issues and limitations

---

Known issues and limitations for this release are listed and described here. For the best possible experience, review this information prior to using PingCentral.

## Known issues

Ticket ID	Description
PASS-909	If you have only one person with an Administrator role and change that person's role to Application Owner, PingCentral will become impossible to administer.
PASS-1552	When updating a user's role, the <b>Discard Changes</b> button does not currently work.
PASS-1620	Clicking on the <b>View Client Details</b> link that displays in the Promotion History section of the page occasionally causes a blank white screen to display instead of the intended details. If this occurs, select another page within PingCentral and then return to the Applications page.
PASS-1998	When an OAuth/OIDC application is promoted from PingCentral to PingFederate, the secret is captured and saved. If this application is removed from PingCentral and a new application is created with the same name, promotions to PingFederate will use the client secret provided for the original application instead of the new secret that was provided in the new application. There is currently no way to retrieve the secret that was provided for the original promotion.

Ticket ID	Description
PASS-2090	<p>If SSO is enabled and PingCentral cannot contact the OpenID provider on startup, PingCentral will fail to start. Either ensure your configuration is correct and the provider is up and running, or disable SSO. Review the <code>application.log</code> file to identify the issue.</p> <p>PingCentral only accesses the OpenID Provider configuration at startup time. If relevant changes have been made on the provider which affect the configuration, PingCentral must be restarted to recognize them.</p>
PASS-2097	<p>When a user logs into PingCentral for the first time using SSO, a local user is provisioned to associate applications with the user. PingCentral Administrators can update local user information. However, if Administrators update the user name or delete a user name for an SSO user, that user will need to be reprovisioned the next time the user logs in using SSO, which can result in them losing ownership of their applications.</p>
PASS-2122	<p>When modifying an environment, if an identity provider certificate is added or updated, and then the PingFederate admin password is updated, the cursor will jump down to the <b>IDP Certificate Password</b> field each time a key is pressed.</p>

#### Known limitations

Limitation	Workaround
There is no PingCentral installer for Microsoft Windows.	Install PingCentral by unzipping the <code>ping-central-1.0.0.zip</code> file. Then, run <code>run.bat</code> script, which is located in the <code>bin</code> folder. Or, run PingCentral as a service using the provided method, which is located in the <code>sbin</code> folder.
You cannot promote applications created in more recent versions of PingFederate to older versions of PingFederate. For example, you cannot promote an application created in PingFederate v9.3 to PingFederate v9.2.	
SSO limitation	Workaround
Rather than maintain a JWT within a cookie, the authentication state is maintained on the server side within PingCentral. The HTTP session is identified via the <code>PINGCENTRAL_SESSION_ID</code> cookie. Restarting PingCentral will reset this state, as it is not persistent.	
PingCentral session settings are ignored when SSO is enabled. The HTTP session cookie, <code>PINGCENTRAL_SESSION_ID</code> , is fixed at this time. The token obtained from the provider is only subject to the expiration defined by the provider. Likewise, key rolling is defined by the provider and it is responsible for maintaining the appropriate keys within its JWKS endpoint.	

SSO limitation	Workaround
When SSO is enabled, local PingCentral user access is not possible. This includes the default Administrator user. HTTP basic authentication is not available for PingCentral API access. OAuth 2 bearer tokens must be used.	
OAuth/OIDC limitation	Workaround
When using OAuth and OIDC, access token mappings are not automatically promoted with the application.	Ensure access token mapping are available on the target instance of PingFederate.
When using OAuth and OIDC, authentication policy contracts and the associated mappings are not automatically promoted with the application.	Ensure authentication policy contracts and the associated mappings are available on the PingFederate target instance.
SAML limitation	Workaround
SP connections require authentication policy contract mappings. Adapter mappings are not supported.	
Artifact and SOAP bindings are not supported for SP connections.	
Dependent entities, including authentication policy contracts, data stores, etc., are not automatically promoted with the application.	Ensure dependent entities are available on the PingFederate target instance.
All connections must specify a primary certificate for signature validation. Multiple connections are not supported.	
Assertion encryption is not supported.	

## PingCentral for Application Owners

---

### Introduction to PingCentral

---

PingCentral makes it easy to apply security configurations to your applications, promote them to the appropriate development environments, and monitor them throughout their life cycles.

As an application owner, you focus on creating applications. You do not often have time to learn how to integrate SSO and access management to protect your applications, and would prefer that your IAM Administrator handle it for you.

You also need to test your application with authentication and authorization policies in a variety of different environments before deploying it to your users. Promoting, testing, and tweaking can be time-consuming, especially if you have to rely on others to promote your applications for you.

PingCentral:

- Makes it possible for you to add user authentication and authorization support to your applications in a few simple steps.

- Allows you to promote your 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.

Extensive training is not required to use PingCentral. However, for the best possible experience, become familiar with how the platform works before getting started.

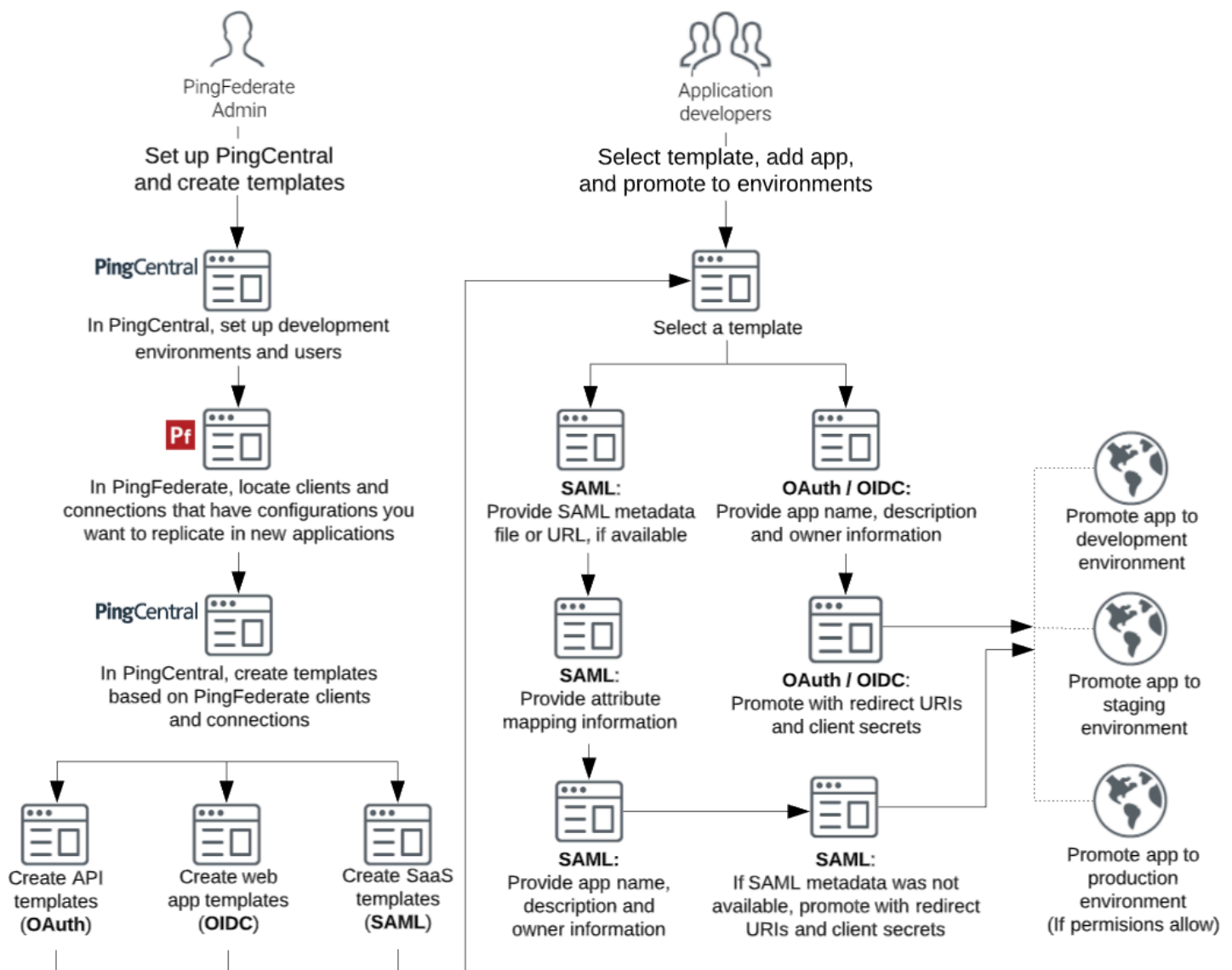
#### How PingCentral works

In PingCentral, IAM Administrators build best-practice security configuration OAuth (Open Authorization), OIDC (OpenID Connect), and SAML SP templates, which you apply to your application. Then, you promote your application to the appropriate development environment.

Here's how it works:

- IAM Administrators create standardized OAuth, OIDC, and SAML SP templates based on best-practice configurations.
- You select the appropriate OAuth, OIDC, or SAML SP template for your application, and a wizard guides you through the process of applying security configurations to it.
- When you're ready, you can promote your application to the appropriate development environment to test it and ensure it's working correctly. You can also promote it directly to the production environment 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 login 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.

## Viewing application information

When you are assigned as an owner of an application, the application displays on the Applications page.

### Steps

1. Applications are listed in the order in which they were created, by default. Use the sort menu at the top of the page to sort the list of applications by modified date or by application name.
2. To view details regarding an application, click the expandable icon associated with it.

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

The screenshot shows the PingCentral interface for the Applications page. The page title is "Applications" and it includes a search bar and an "Add Application" button. Two applications are listed, sorted by Modified Date:

- Accounting** (-Template-OpenID) with a "STG" environment icon. It has tabs for "Summary", "Template", and "Promote", and a "+ Promote" button. Below the tabs is a table with two sections:
 

ENVIRONMENT	LAST PROMOTED
-Staging Environment	2020-02-26 12:56:28 <a href="#">View Client Details</a>

ENVIRONMENT	PROMOTED
-Staging Environment	2020-02-26 12:56:28 <a href="#">View Client Details</a>
-Staging Environment	2020-02-26 12:52:29 <a href="#">View Client Details</a>
- Time Tracking** (-Template-SAML) with a "PROD" environment icon.

The footer of the page includes the Ping Identity logo and copyright information: Copyright © 2003-2020 Ping Identity Corporation. All rights reserved. Version 13.0.0 SNAPSHOT.

3. Click each tab to review additional information about the application:

- **Summary tab:** This tab displays the application or connection name, application description, application owners, and the date on which the application was last modified.
- **Template tab:** This tab displays the name of the template applied to the application, and details regarding the client or connection on which the template was based.
- **Promote tab:** This tab displays the promotion history of this application, which includes the date and time each promotion occurred. Click the **View Client Details** link to access additional information regarding the application and its promotion.

## Adding and promoting applications

---

To add an application to PingCentral, select the appropriate security configuration template, use that template to apply user authentication and authorization support to the application, and promote the application to the appropriate development environment.

Refer to the following:

- [Selecting a template](#)
- [Using OAuth and OIDC templates](#)
- [Using SAML SP templates](#)

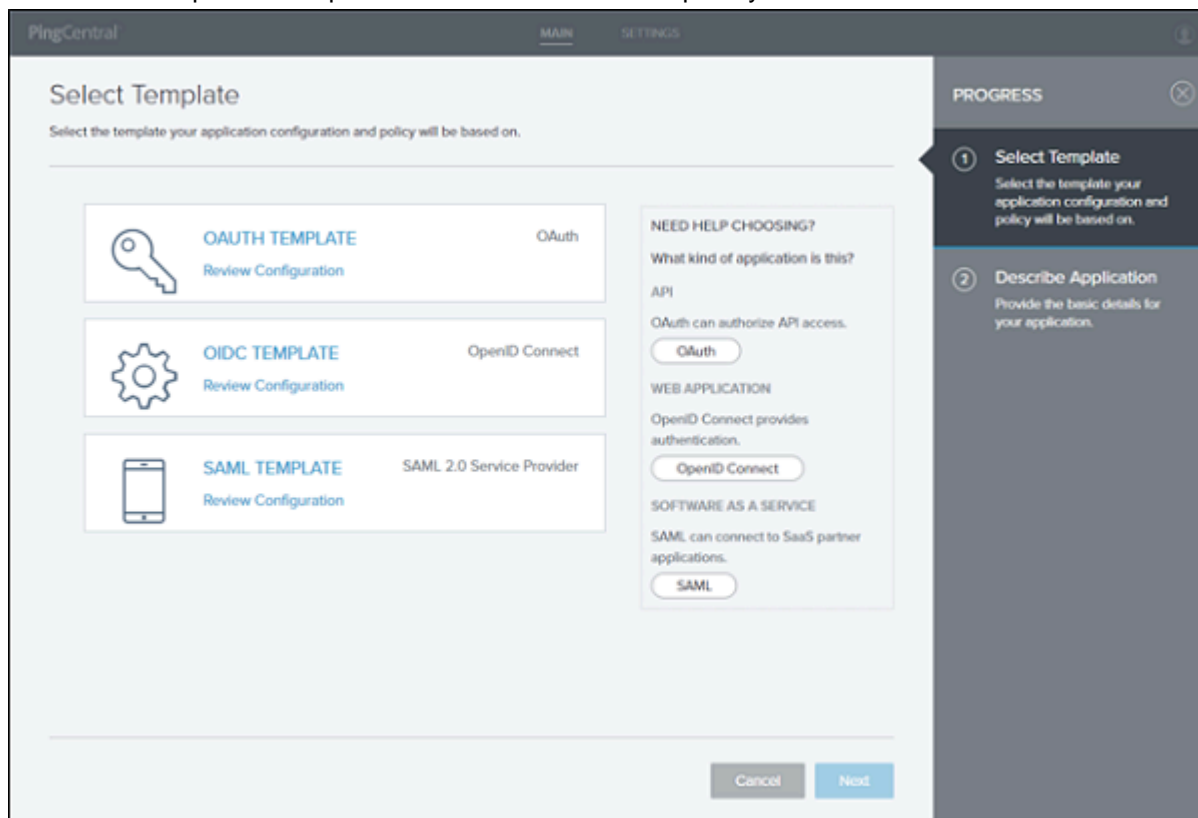
### Selecting a template

The first step is to select a template appropriate for your application. IAM Administrators can create OAuth, OIDC, and SAML SP 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.



On this page, you can:

- Use the filtering options on the right side of the screen to filter OAuth, OIDC, and SAML SP templates.
- Click the **Review Configuration** link within the template description to view the details associated with the template.

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

- OAuth and OIDC are most commonly used by consumer applications and services so users do not need to sign up for a new user name and password. "Sign in with Google," or "Log in with Facebook" are examples of OAuth protocols you are likely familiar with. You might also use OAuth if your application will be 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.

3. Select the template you want to use and click **Next**.

4. Use the template to apply security configurations to the application. Refer to the appropriate topic for instructions:

- [Using OAuth and OIDC templates](#)
- [Using SAML SP templates](#)

## Using OAuth and OIDC templates

After selecting an OAuth or OIDC template, you can apply the template to the application and then promote the application to the appropriate environment for testing.

Before you begin

Prepare to provide the following:

- Name of the application.
- A brief, accurate description of your application.
- Redirect URI, if required. This is the URI 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.

Steps

1. 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.
2. **Optional:** To add owners, click the box and select additional owners from the 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.

The screenshot displays the 'Describe Application' interface in PingCentral. The main content area is titled 'Describe Application' and includes the instruction 'Provide the basic details for your application.' Below this, there are three input sections: 'NAME' with the text 'Time Tracking', 'DESCRIPTION' with the text 'Internal application (and partners)', and 'OWNERS' which shows 'Jennifer Armstrong' as the selected owner and a list of other potential owners: 'Default User', 'Peter Andrews', and 'Veronica Hira'. On the right side, a 'PROGRESS' sidebar indicates the current step is '2 Describe Application' (Provide the basic details for your application.) following '1 Select Template'. At the bottom right of the form, there are 'Cancel' and 'Save and Close' buttons.

3. Click **Save and Close**.  
The application appears at the top of the list of applications on the **Applications** page.
4. Promote the application to the appropriate environment. Click **Promote**.

5. Select the environment to which you want to promote the application from the **Available Environments** list.

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

6. If redirect URIs are required to promote the application, enter them in the **Redirect URIs** field.
7. 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.
  - Leave the **Client Secret** text box empty and PingCentral will automatically generate a client secret for you, if it is required.


### Promote to Environment

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

REDIRECT URIS

×

CLIENT SECRET



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

9. 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, which 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: [redacted]

ADVANCED

GRANT TYPE: IMPLICIT

TOKEN AUTH METHOD: NONE

^ SUMMARY

^ CLIENT

^ OIDC POLICY

^ ACCESS TOKEN MANAGER

Revert Application Close

## Using SAML SP templates

After selecting a SAML template, you can apply the template to the application and then promote the application to the appropriate environment for testing.

Before you begin

Prepare to provide the following:

- 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.
- 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 IdP will be sent after user authentication occurs.
- Certificates, if the template you select is based on a PingFederate connection that requires a certificate.

When you add an application to PingCentral, you can provide an `.xml` file that contains service provider metadata from a similar SAML application. This file could contain an Entity ID, ACS URL, certificates, attribute information, or all of this information.

Or, you can provide the Entity ID, ACS URL and certificates during the promotion process.

To create an .xml file from a similar application, see [Downloading service provider metadata](#).

### Steps

1. After selecting a SAML template, the Select Metadata page displays. Complete one of the following tasks and click **Next**.
  - Click **Choose file** to provide a metadata file.
  - Click the **Or Use URL** link to provide a link to the metadata file.
  - Opt to skip this step and provide the Entity ID, ACS URL, and certificates during the promotion process.

After providing a metadata file, the Entity ID, ACS URL, certificate, and attributes display on the screen, as shown in the following example.

2. On the Map Attributes page, map the application attributes to the identity attributes required to fulfill the authentication policy contract in PingFederate. Select identity attributes from the **Identity Attribute** list or add static values in the **Static Value** field. Click **Next**.
3. On the **Describe Application** page, enter the name of the application and a description in the appropriate fields.  
You are adding this application to PingCentral, so your name will automatically populate the **Owners** field.
4. Optional: To add owners, click the box and select additional owners from the 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. Click **Next**.



5. Click **Save and Close**.

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

6. Promote the application to the appropriate environment. Click **Promote**.

7. Select the environment to which you want to promote the application from the **Available Environments** list.

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

8. If you provided a metadata file when you added your application to PingCentral, you will see that the page is pre-populated with the information from the other SAML application. Modify this information, as necessary.

If you did not upload a metadata file, enter the appropriate information in the **Entity ID** and **ACS URL** fields, and upload certificates, if required.

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 **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](#)
- [Configure signature verification settings \(SAML 2.0\)](#)

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

PingCentral promotes your application to the designated environment in PingFederate. You will see the new promotion 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.

10. To configure the SSO connection, provide the following information to your service provider:

- The application Entity ID.
- The SSO endpoint URL. Click **View Connection Details** to access the **Promotion Details** window, which displays the SSO endpoint URL.
- Certificates, if applicable. On the **Promotion Details** window, click **Identity Provider** to download the certificate that the identity provider is using to sign the SAML assertion, as shown in the following example.

The screenshot shows a window titled "Promotion Details" with a close button in the top right corner. The window content is as follows:

Time Tracking-from-SAML-template -- Staging-Environment - 2020-02-25 15:25:18

---

^ PROMOTION

PROMOTED: 2020-02-25 15:25:18

CURRENT OWNERS: Jennifer Armstrong

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

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

CERTIFICATES: [Identity Provider](#)  
[Service Provider](#)

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

---

∨ SUMMARY

---

∨ CONNECTION

---

Revert Application Close

### Downloading service provider metadata

After a SAML application has been promoted to an environment, the connection metadata is exported and stored as part of that application. This metadata is available to download as an `.xml` file, which you can use to promote other similar SAML applications.

### Steps

1. On the Applications page, locate an application that has a configuration you want to replicate in a new SAML application.

2. Select the **Promote** tab and click the **View Connection Details** link.

The Promotion Details window opens and displays promotion information for the application.

The screenshot shows a window titled "Promotion Details" with a close button in the top right corner. The window content is as follows:

Time Tracking-from-SAML-template -- Staging-Environment - 2020-02-25 15:25:18

---

^ PROMOTION

PROMOTED: 2020-02-25 15:25:18

CURRENT OWNERS: Jennifer Armstrong

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

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

CERTIFICATES: [Identity Provider](#)  
[Service Provider](#)

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

---

∨ SUMMARY

---

∨ CONNECTION

---

Revert Application Close

3. Click the **Download Service Provider Metadata** link to download the metadata as an `.xml` file.

Note the location of this file, as you can use it to promote other similar SAML applications.

## Updating applications

Update your applications, either before or after promoting them, with new names, descriptions, owners, templates, entity IDs, URIs, URLs, certificates, and attribute mappings associated with the application. To update client secrets, repromote the application and generate a new secret during the promotion process.

### 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. There is no need to recreate your applications in PingCentral to apply new templates. You can just replace the templates associated with your applications and promote them again.

## Steps

1. Click the expandable icon associated with the application you want to update. Then, click the pencil icon.

All of the editable information displays on one page.

The screenshot shows the PingCentral interface for editing an application. The page title is 'Time tracking for Accounting'. The interface is divided into several sections:

- SUMMARY:** Contains fields for NAME (Time tracking for Accounting), DESCRIPTION (Internal time-tracking system), and OWNERS (Veronica Hira).
- TEMPLATE:** Shows the current template as '-Auto-Template-(2002261654141000005)-SAML-Optional' with a 'Change Template' button and a 'Review Configuration' link.
- ATTRIBUTE MAPPINGS:** A table with columns for APPLICATION ATTRIBUTE and IDENTITY ATTRIBUTE. One mapping is shown: SAML\_SUBJECT = SAML\_SUBJECT.

The left sidebar shows the 'Applications' menu. The bottom left corner contains the Ping Identity logo and copyright information: Copyright © 2003-2020 Ping Identity Corporation. All rights reserved. Version 13.0-SNAPSHOT.

2. To update application names, descriptions, and owners:
  - Enter the new information in the **Name**, **Description**, and **Owners** fields.
  - Click **Save**.
3. To update the template associated with the application, complete the following steps. You cannot apply a SAML template to an OAuth or OIDC application, or apply an OAuth or OIDC template to a SAML application.

For OAuth or OIDC applications:

- Click **Change Template**.
- On the **Select Template** page, select the new template and click **Save and Close**.

For SAML applications:

- Click **Change Template**.
- On the **Select Template** page, select the new template and click **Next**.
- On the **Map Attributes** page, map the application attributes to the identity attributes required to fulfill the authentication policy contract in PingFederate.
- Click **Save and Close**.

- To update information you provided to promote your application, complete the following steps:

For OAuth or OIDC applications:

- Enter the new information in the **Redirect URIs** fields.
- Click **Save**.

For SAML applications:

- Click the expandable icon next to the application you want to update and enter the new information in the **Entity ID** or **ACS URL** fields, or click the **Certificate** button to upload a new certificate.

Or, upload an `.xml` file that contains service provider metadata, such as the Entity ID, ACS URL, certificates, and attribute information, from a similar SAML application. Click **Choose** and upload the metadata file.

(For instructions on creating an `.xml` file from a similar application, see [Downloading service provider metadata](#).)

Or, click the **Or Use URL** link to provide a link to the metadata file.

- Click **Save**.

- To update attribute mappings for a SAML application, update the information in the **Attribute Mappings** page and click **Save**.
- To update the client secret associated with an OAuth or OIDC application, return to the **Applications** page, repromote the application, and generate a new secret.

## Reverting applications to previously promoted versions

---

After an application is promoted, you can quickly revert it to a previously promoted version. The reverted version of the application will not exist outside of PingCentral until you promote it again, at which point it will also be available in PingFederate.

About this task

This functionality is not available for applications created with version 1.2 templates, and only applies to applications created with version 1.3 templates.

To upgrade a version 1.2 application to a version 1.3 application, edit the application and apply a template created in version 1.3 to it.

Steps

- On the Applications page, locate the application you want to revert to a previously promoted version.
- Click the expandable icon associated with the application, select the **Promote** tab and then the **View Details** link associated with the promotion.
- On the Promotion Details window, click the **Revert Application** button.  
A message displays asking you if you are sure you want to revert this application.
- Click the **Revert** button.  
The reverted version of the application displays at the top of your applications list open to the **Promote** tab.

When OAuth and OIDC applications are reverted to previously promoted versions client secrets are overridden, so you will need to create or generate new secrets before you promote them again.

When SAML applications are reverted to previously promoted versions, Entity IDs, ACS URLs, and certificates are also overridden, so you might need to update this information before you promote them again.

# PingCentral for IAM Administrators

---

## Introduction to PingCentral

---

PingCentral is an orchestrator for a variety of Ping products that makes it possible for you to delegate common configuration and deployment tasks to others. In this version, PingCentral serves as an orchestrator for PingFederate and makes it possible for application owners to apply your security configurations templates to their applications and promote them to development environments themselves.

As an IAM Administrator and security professional, your time and expertise are in high demand. You maintain complex configurations in a variety of different tools and interfaces and serve as the central point-of-contact for many groups within your organization. With a growing list of demands from business and system administrators, application developers, and compliance representatives, and the inability to delegate to those who lack your expertise, it can be difficult to keep up.

PingCentral:

- Allows application owners to add user authentication and authorization support to their applications and promote them to development environments themselves.
- Removes many common application configuration and deployment tasks from your long list of responsibilities, which will lower operational costs, reduce bottlenecks, and allow you to focus on the more complex elements of your job.
- 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 make it easier to standardize policies across the applications within your organization.

Extensive training is not required to use PingCentral. However, for the best possible experience, become familiar with how the platform works, and the mechanics behind the template creation and environment promotion processes, before getting started.

How PingCentral works

Being a PingFederate expert, you enjoy building complex configurations and look forward to learning about the latest and greatest security technology available. However, most application owners do not feel the same way.

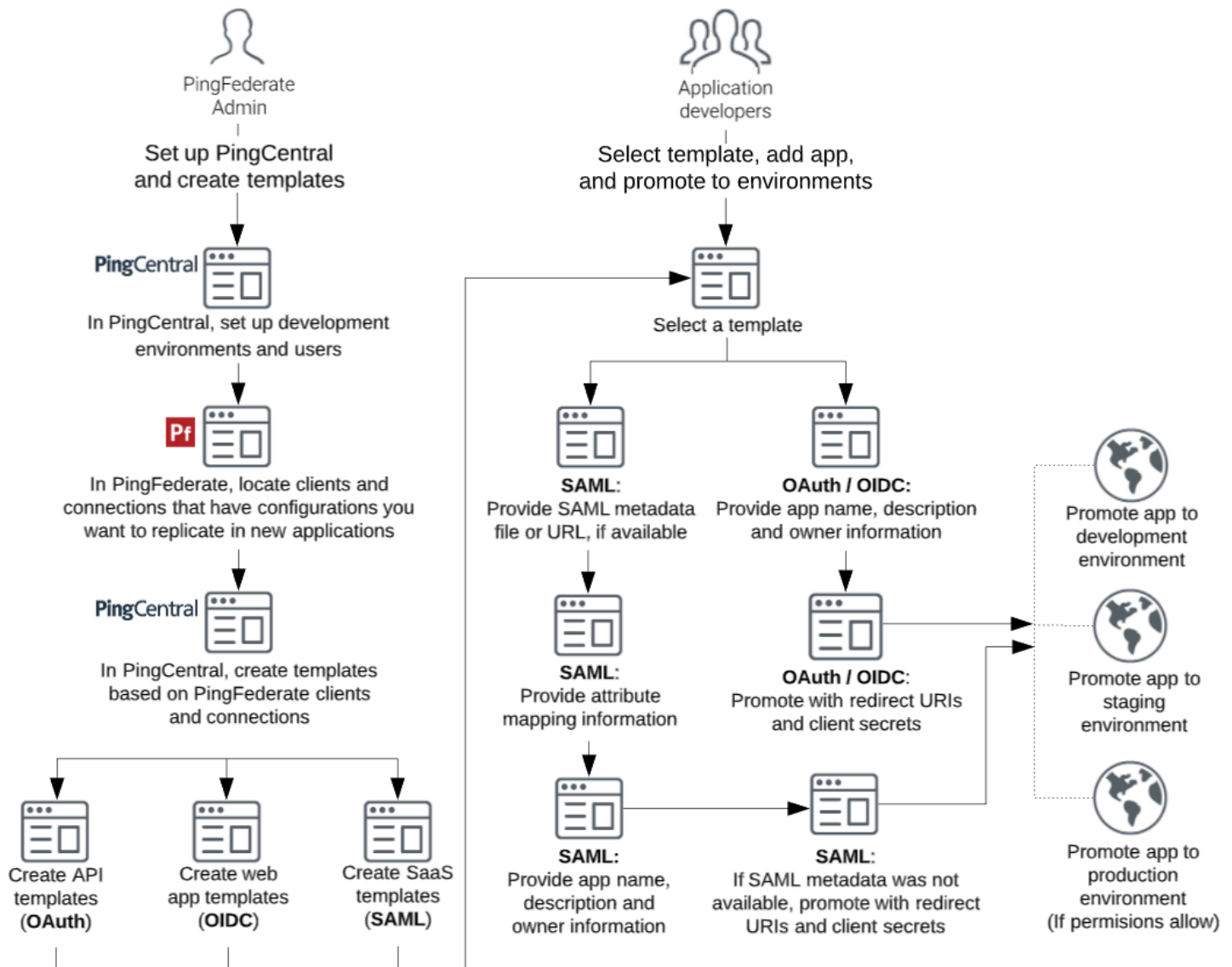
The vast majority of application owners do not know (or want to know) anything about OAuth, OIDC, or SAML. All they want to do is find the simplest and most straightforward way to support user authentication and authorization within their applications. They would prefer that someone like you handle all of that for them.

Application owners also need to test their applications in a variety of different environments before they are promoted to production. Promoting, testing, and tweaking can be time-consuming, and even more so if they have to rely on someone else to promote their applications for them.

Here's how it works:

- In PingCentral, you set up development environments and users.
- In PingFederate, you locate clients and connections that have best-practice security configurations worthy of replicating in new applications.
- In PingCentral, you create standardized OAuth, OIDC, and SAML SP templates based on best-practice configurations.
- In PingCentral, application owners use your templates to create new OAuth, OIDC, and SAML SP applications. A wizard guides them through the process of providing a name and description for

each application they create, and environment-specific information that makes it possible to run the application on the target environment.



OIDC client and SAML connection authentication can only occur if PingFederate is correctly configured. Refer to [OIDC connection orchestration](#) and [SAML connection orchestration](#) to see which PingFederate components are used to authenticate clients and connections in PingCentral.

## 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.

### System requirements

#### PingFederate:

- PingFederate v9.2. See [PingFederate v9.2 system requirements](#).
- PingFederate v9.3. See [PingFederate v9.3 system requirements](#).

#### Platforms:

- Microsoft Windows Server 2016

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

Browsers:

- Chrome
- Firefox

Java runtime environments:

- Oracle Java 11 LTS
- OpenJDK 11

External databases:

- MySQL 5.7+
- PostgreSQL 11.5+

### 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](#)

### General configurations

Configuration	Supported	Unsupported
Single sign-on and user management	<ul style="list-style-type: none"> <li>▪ Directly managing users, which are stored in PingCentral embedded database.</li> <li>▪ Signing on with SSO using an OIDC token.</li> <li>▪ Beta feature: Provisioning users from an external store using API calls.</li> </ul>	
Entitlements	<ul style="list-style-type: none"> <li>▪ Assigning one or more application owners that have already been provisioned.</li> <li>▪ Editing and promoting entitlements for an application.</li> </ul>	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> <p><b>Note:</b> To ensure these files contain the most up-to-date information, do not copy them while PingCentral is running.</p>	Using an API to export PingCentral configuration information.



**OAuth and OIDC configurations**

Configuration	Supported	Unsupported
Client authentication	Using None or the client secret method. Client secrets can be provided by the user or generated.	Using a client TLS certificate, private key JWT, or symmetric keys.
Grant types	Using all OAuth and OIDC grant types.	
Scopes	All scopes and exclusive scopes referenced in the PingFederate client JSON file, which is obtained during the template creation process.	Scopes cannot be customized when creating an application in PingCentral.
ATMs and OIDC policies	<p>Saving ATMs or OIDC policies into templates created from client applications that have them.</p> <p><b>Note:</b> 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 SP configurations**

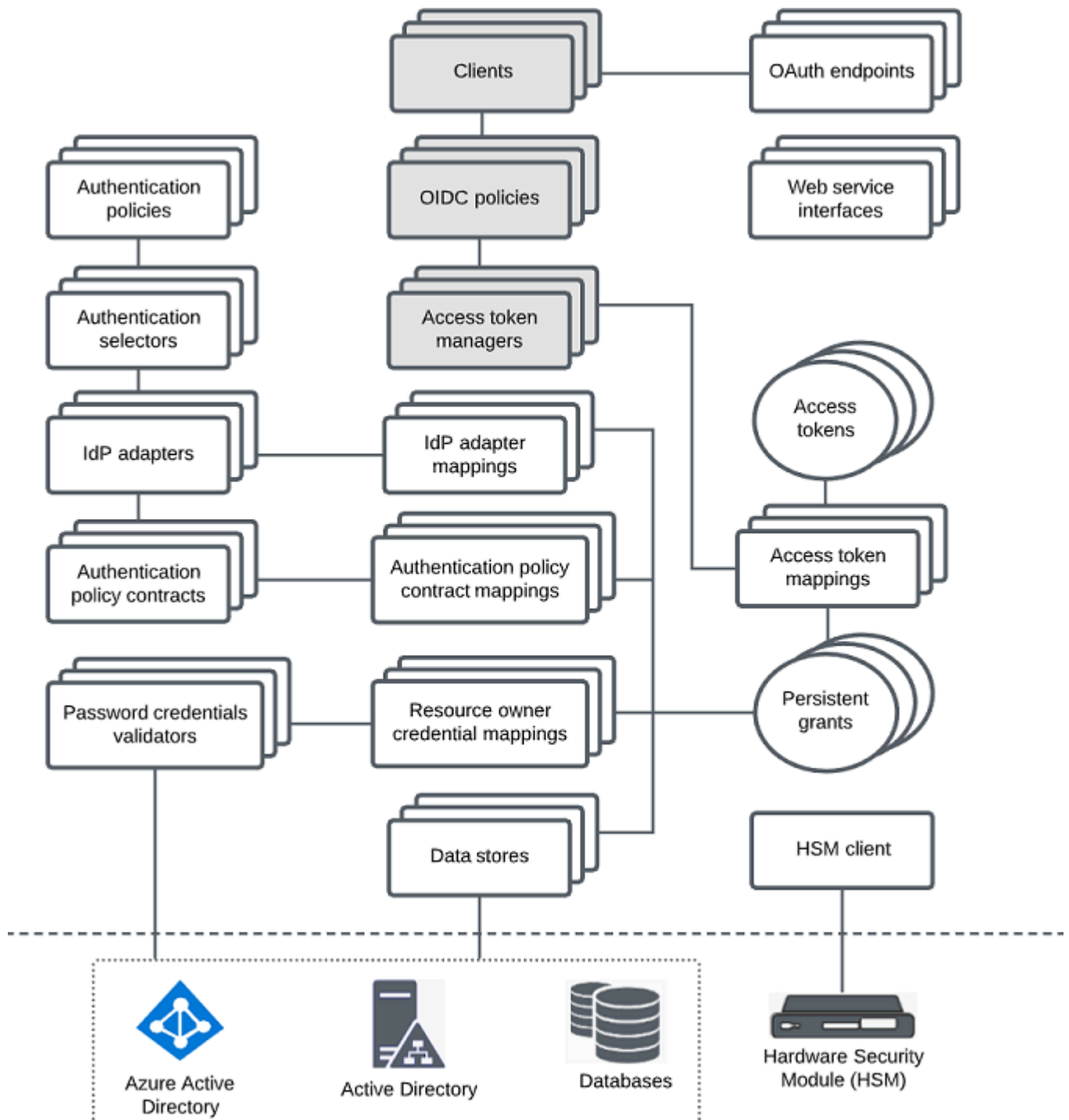
Configuration	Supported	Unsupported
Bindings	Using POST bindings.	Using artifact, redirect, or SOAP bindings.
Profiles	<ul style="list-style-type: none"> <li>▪ IdP-initiated SSO</li> <li>▪ SP-initiated SSO</li> <li>▪ IdP-initiated SLO</li> <li>▪ SP-initiated SLO</li> </ul>	
Attribute mapping	Mapping attributes, provided by a single authentication policy contract, in an “unspecified” format. You can also map attributes to static text.	<ul style="list-style-type: none"> <li>▪ Mapping attributes from data sources, such as “basic” or “URI.”</li> <li>▪ Using OGNL expressions as part of attribute mapping.</li> </ul>

Configuration	Supported	Unsupported
Policy contracts	Referencing one policy contract per template.	Referencing more than one policy contract per template. 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		Authentication policies must be specified through a policy contract consistent with PingFederate best practices.
Certificate management	<ul style="list-style-type: none"> <li>▪ Providing a public certificate for an SP connection. PingCentral creates a self-signed certificate with an expiration date of one year from today and configures it as the PingFederate IDP certificate.</li> <li>▪ Uploading a key pair to use as the IdP certificate for all SAML connections promoted to an environment.</li> </ul>	An SP certificate is required to promote a SAML connection, but might be optional in future releases.

### OIDC connection orchestration

This diagram shows which PingFederate components are used to authenticate an OIDC client. PingCentral currently only orchestrates clients, OIDC policies, and access token managers, which are shaded in the diagram.

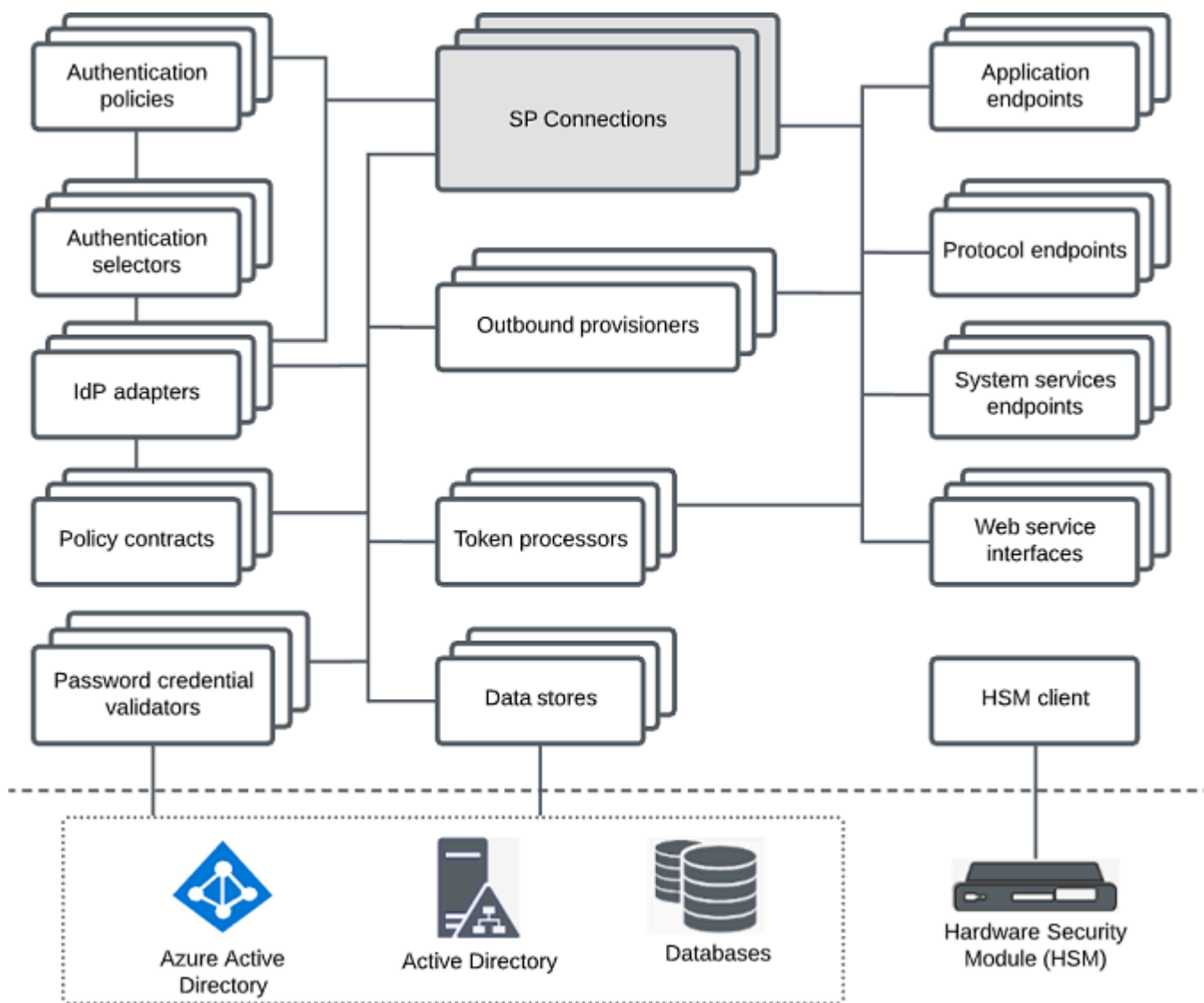
With PingCentral, OIDC client authentication can only occur if PingFederate is correctly configured with the appropriate data sources, password credential validators, authentication policies, policy contracts, policy contract mappings, persistent grants, and access token mappings. In this version, you cannot create clients with direct adapter mappings to an IdP adapter.



### SAML connection orchestration

This diagram shows which PingFederate components are used to authenticate a SAML connection. PingCentral currently only orchestrates the PingFederate IdP connection, which is shaded in the diagram.

With PingCentral, SAML connection authentication can only occur if PingFederate is correctly configured with the appropriate data sources, password credential validators, authentication policies, and policy contracts. In this version, you cannot create connections to an IdP adapter with direct adapter mappings.

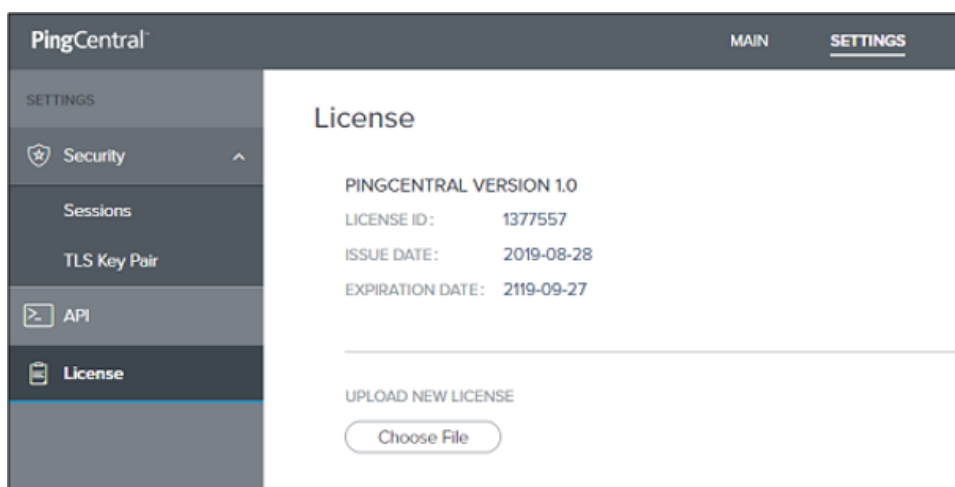


## PingCentral licensing

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.

## Use Docker to deploy PingCentral

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

Detailed instructions for using Docker to deploy PingCentral are available on the [PingIdentity DevOps site](#), but are also summarized here, for your convenience.

Before you begin, ensure that you have the appropriate tools and applications installed:

- [Docker CE for Windows](#) or [Docker for macOS](#)
- [Docker Compose](#)
- [Git](#)

When you are ready, deploy PingCentral:

- Create a Ping Identity account and register for the DevOps program, or sign on to your existing account. See [DevOps registration](#) for instructions.
- Set up your DevOps environment. See [Get started](#) for instructions.
- Deploy the stack and configure trust and SSO for PingCentral. See [Deploy PingCentral](#) for instructions.

## Install and configure PingCentral

Install and upgrade PingCentral on Microsoft Windows Server 2016 or 2019, or on Red Hat Enterprise Linux ES 7.6 or 8.0. After installation, configure PingCentral to run as a Linux systemv service, a systemd service, or a Windows service, as appropriate.

Refer to the following:

- [Installing PingCentral on Microsoft Windows](#)
- [Installing PingCentral on Red Hat Enterprise Linux](#)
- [Configuring PingCentral to run as a Linux systemv service](#)
- [Removing the PingCentral systemv service](#)
- [Configuring PingCentral to run as a Linux systemd service](#)
- [Removing the PingCentral systemd service](#)
- [Configuring PingCentral to run as a Windows service](#)

- [Removing the PingCentral Windows service](#)

## 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 logged 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` file and extract its contents in a place where you want the service run.
2. Navigate 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:** As you are running PingCentral locally, your browser might warn you that the application you are accessing does not have a signed certificate.

4. Log in to PingCentral using the following credentials:

- **Username:** Administrator
- **Password:** 2Federate

Without modification, PingCentral is secure by default. However, if you want to use self-signed server certificates, root certificates, intermediate certificates, and certificates from a private certificate authorities, create a PingCentral-specific truststore and configure PingCentral to access it. Refer to [Creating and configuring trust](#) for instructions.

5. Configure PingCentral to run as a Windows service, if appropriate. Refer to [Configuring PingCentral to run as a Windows service](#).

## Installing PingCentral on Red Hat Enterprise Linux

PingCentral can be installed on Red Hat Enterprise Linux ES 7.6 or 8.0. Download the installation script and the distribution file, run the script, and respond to the prompts as they display on your screen.

Before you begin

Ensure that:

- You are logged 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 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 installation script into your installation directory.
2. Download the distribution `.zip` file into your installation directory.
3. Run the following installation scripts:

- ```
chmod +x ./<pingcentral_install>/pingcentral-install.sh
```
- ```
sudo -E ./<pingcentral_install>/pingcentral-install.sh
```

4. Follow the installation prompts and accept the default values or specify your preferences. You can change the port and add or replace PingCentral services.
5. When the installation is complete, open a browser window and enter the machine and PingCentral admin port in the URL field. For example, `https://yourhost:9022`. PingCentral is installed as a systemd service from the `PINGCENTRAL_HOME` directory.
6. Start PingCentral by running `/<pingcentral_install>/bin/run.sh`, or by running the systemd service command, `systemctl pingcentral-# start`.

 **Note:** The `pingcentral-#` is specified during the installation.

7. Log in to the application using the following credentials:

- **Username:** Administrator
- **Password:** 2Federate

Without modification, PingCentral is secure by default. However, if you want to use self-signed server certificates, root certificates, intermediate certificates, and certificates from a private certificate authorities, create a PingCentral-specific truststore and configure PingCentral to access it. Refer to [Creating and configuring trust](#) for instructions.

8. Configure PingCentral to run as a Linux systemd service or a Linux systemv service, as appropriate. Refer to [Configuring PingCentral to run as a Linux systemv service](#) or [Configuring PingCentral to run as a Linux systemd service](#).

## Creating and configuring trust

The standard Java Development Kit (JDK) includes a default truststore, which is pre-provisioned with the root certificates of a number of well-known certificate authorities. If you need to store and maintain certificates that are not in the default truststore, you need to create a PingCentral-specific truststore.

### About this task

Without modification, PingCentral is secure by default:

- The server certificate chain must be ultimately signed by one of the public certificate authority root certificates present in the JVM default trust store.
- Hostname verification is performed. The hostname or IP address specified in the URL must match a name defined in the server certificate presented, which encompasses the distinguished name, subject alternative names, and wildcard matching.

If you want to use self-signed server certificates, root certificates, intermediate certificates, and certificates from a private certificate authorities, create a PingCentral-specific truststore and configure PingCentral to access it.

Each time a connection is made, PingCentral checks the remote server's certificate against the PingCentral-specific truststore. If certificate validation fails, PingCentral delegates validation to the default

system truststore. If you disable delegation to the default truststore, the only trusted certificates are those in the PingCentral-specific truststore.

In PingCentral, two types of outbound connections perform server certificate validation using the PingCentral-specific truststore. You cannot configure these connections independently.

- Admin API access to PingFederate to manage environments and deploy applications.
- Back-channel access to the configured OIDC provider when SSO is enabled.

You can configure PingCentral so that hostname verification and certificate validation is disabled. However, it is highly recommended that these options only be disabled for demonstration or testing purposes.

PingCentral only reads truststore configurations at startup, so restart PingCentral after creating or configuring truststore information.

## Steps

### 1. To create a PingCentral-specific truststore:

- a. Run the following Java built-in `keytool` command.

```
<JAVA_HOME>/bin/keytool -import -trustcacerts -  
alias <ALIAS> -file <PATH_TO_TRUSTED_AUTHORITY_CERT> -  
keystore <TRUST_STORE_FILE_NAME>.jks
```

#### **Note:**

It is highly recommended that you store the new truststore in a secure location on the local file system of the PingCentral user, and limit access permissions to that user.

- b. Run this command for each certificate you need to import. Specify a unique alias for each certificate and ensure you refer to the same truststore file name each time you run this command.
- c. During this process, the system will prompt you to create a password to secure the truststore. You will need to provide this password when you configure PingCentral to access the truststore.
- d. To view a list of the certificates included in the truststore, run the following command:

```
<JAVA_HOME>/bin/keytool -list -v -keystore <TRUST_STORE_FILE_NAME>.jks
```

#### **Note:**

Java trusts certificates in the configured truststore even if they are expired.



## 2. To configure PingCentral to access the PingCentral-specific truststore:

- a. Open `<PingCentral installation directory>/conf/application.properties` in a text editor and configure PingCentral to access the PingCentral-specific truststore.
- b. Locate the following properties, uncomment them by removing the `#` from the line, and define each property with your system-specific information:

- `server.ssl.trust-store=<ABSOLUTE_PATH_TO_TRUSTSTORE_JKS_FILE>`

**Note:**

If the `.jks` file is in the PingCentral `home/install` directory, you can use a relative link instead:  
`${pingcentral.home}/<PATH_TO_TRUSTSTORE_JKS_FILE>`

- `server.ssl.trust-store-password=<TRUSTSTORE_PASSWORD>`

On startup, PingCentral will attempt to access the truststore with the password specified here, which must be the password used when the truststore was created.

**Note:**

It is highly recommended that you secure the password using the obfuscation script available in `bin/obfuscate`, and by using output ciphertext rather than the cleartext secret.

## 3. Configure the following PingCentral properties, as appropriate:

- To force PingCentral to use the PingCentral-specific truststore as the certificate validation authority and not delegate validation to the default system truststore, uncomment the following property and set the value to `false`: `server.ssl.delegate-to-system=false`
- To configure PingCentral so that it will accept a valid certificate even if the URL hostname does not match the one defined in the certificate, uncomment the following property and set the value to `false`: `server.ssl.https.verify-hostname=false`
- To configure PingCentral so that certificate validation is completely disabled (any certificate presented by a server is trusted), uncomment the following property and set the value to `true`: `server.ssl.trust-any=true`

## 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 logged on to your system as a root user.
- 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 `PINGCENTRAL_HOME` path points to the folder extracted from the `.zip` file in your installation directory. Ensure that this path does not reside within a user's home folder.

Steps

1. Copy the `pingcentral` file from `PINGCENTRAL_HOME/sbin/linux/pingcentral` to `/etc/init.d`.
2. **Optional:** 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 the following location: `/var/run/pingcentral`. 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. Log on to the system as a root user.
2. To stop the service, run the `/etc/init.d/pingcentral stop` command.
3. To delete the service, run the `chkconfig --del pingcentral` command.
4. Optional: Delete the `/etc/init.d/pingcentral` 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 logged on to your system as a root user.
- The `JAVA_HOME` path points to the JDK software on your system. For example, `usr/java/jdk11.0_4`.
- The `PINGCENTRAL_HOME` path points to the folder extracted from the `.zip` file 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 `/etc/systemd/system/pingcentral.service`.
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 /etc/systemd/system/pingcentral.service` command.

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. Log on to the system as a root user.
2. To stop the service, run the `systemctl stop pingcentral` command.
3. To disable the service, run the `systemctl disable pingcentral` command.
4. Optional: Delete the `/etc/systemd/system/pingcentral.service` script if it is no longer needed.

## Configuring PingCentral to run as a Windows service

Run PingCentral as a Windows service that automatically starts when Windows starts. You must have administrator privileges to configure PingCentral as a Windows service.

#### Before you begin

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

#### Steps

1. In **Search**, type `cmd` to access the command prompt.
2. Right-click **Command Prompt** and select **Run as administrator** from 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 and search for `view local services`.
5. Locate **PingCentral Service** from the list of available services, right-click it, and select **Start**. 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 Search, type `cmd` to access the Command Prompt.
2. Right-click **Command Prompt** and select **Run as administrator** from 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 has run, remove the `PINGCENTRAL_HOME` environment variable from the system.

## Setting up MySQL

PingCentral uses the Java-based H2 relational database management system by default, but you can also use MySQL. This section contains instructions on installing the MySQL connector and configuring it to communicate with PingCentral. It does not provide instructions on setting up or maintaining the MySQL database.

#### About this task

To set up MySQL, you must have the privileges required to access the `pingcentral` schema and configure the database.

**Note:** 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. However, 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/](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:

- Update the datasource URL to your location. For example:

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

- Update the user name and password, if necessary. For example:

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

- Update the driver class name, if necessary. For example:

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

4. Restart PingCentral so the changes take effect.

## Upgrade PingCentral

---

To upgrade to PingCentral version 1.2.0, you must first have version 1.0.1 installed. You cannot upgrade directly from version 1.0.0 to 1.2.0. To begin the upgrade, download and extract the contents of the version 1.2.0 build and run the upgrade utility for Windows or Linux, as appropriate.

This section explains how the upgrade works and shows you which files are added and replaced during the process. For instructions on running the upgrade itself, refer to [Upgrading to PingCentral version 1.2.0](#).

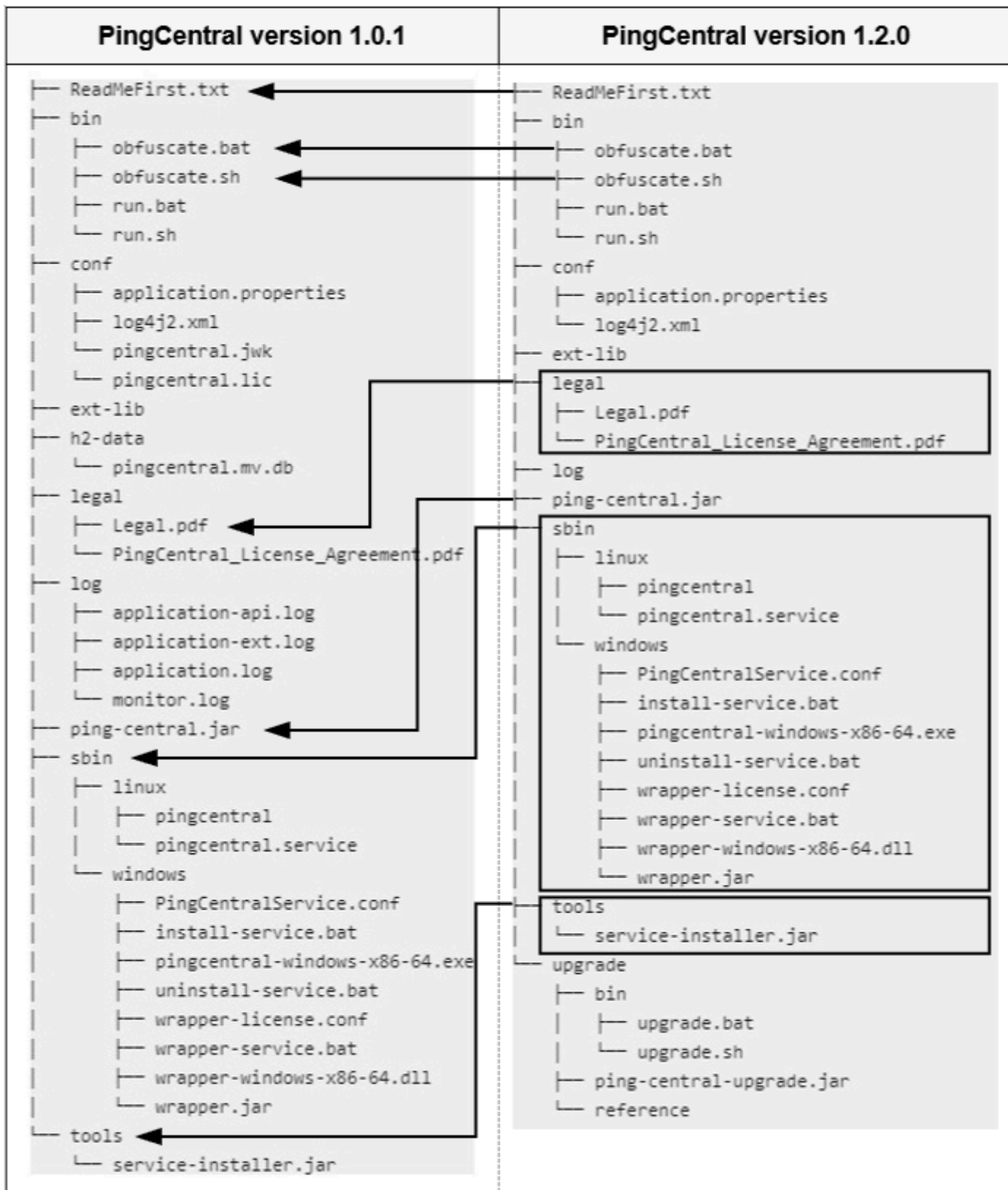
### How the upgrade works

The upgrade utility uses the extracted contents of the `ping-central-1.2.0.zip` file to copy and replace the appropriate information in the existing version 1.0.1 location.

This upgrade utility does not yet support file merging. Consequently, several files remain intact during the upgrade process to preserve customizations. These files include:

- Database files (`h2-data` directory)
- Log files (`log` directory)
- Configuration files (`conf/application.properties` and `conf/log4j2.xml`)
- Script files (`bin/run.bat` and `bin/run.sh`)

The following image shows PingCentral version 1.0.1 after it has been run and the database files have been generated. It also shows which files are replaced with new files from version 1.2.0 during the upgrade process.



## Upgrading to PingCentral version 1.2.0

To upgrade PingCentral from version 1.0.1 to version 1.2.0 on either Windows or Linux, download the installation file, run the PingCentral upgrade utility, and plan for a short period of downtime.

Before you begin

Ensure that:

- You are logged 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. Make a copy of the PingCentral version 1.0.1 product directory so that version 1.0.1 can be restored if the upgrade process fails.
2. If PingCentral is running, shut it down to maintain the integrity of the H2 database file during the upgrade.
3. Download the `ping-central-1.2.0.zip` file and extract its contents to a suitable location.
4. Go to the `<pingcentral_1.2.0_install>/upgrade` directory and run the appropriate file:
  - For Windows, run `bin\upgrade.bat "--existing=PINGCENTRAL_HOME"`
  - For Linux, run `bin/upgrade.sh --existing=PINGCENTRAL_HOME`

The upgrade process begins. The upgrade utility uses the extracted contents of the `ping-central-1.2.0.zip` file to copy and replace the appropriate information in the existing version 1.0.1 location.

**Note:** When the upgrade is complete for this release, PingCentral version 1.2.0 will run from the `ping-central-1.0.1` directory.

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.  
As the upgrade continues, a message displays that reminds you to shut down PingCentral if you have not already done so.
6. Type `yes` to continue.  
A message displays that reminds you to back up your PingCentral program files.
7. Type `yes` to continue.  
The upgrade continues and the system displays a message when the upgrade is complete.
8. Start PingCentral version 1.2.0.
  - For Windows, run `/<PINGCENTRAL_HOME>/bin/run.bat`.
  - For Linux, run `/<PINGCENTRAL_HOME>/bin/run.sh`, or by running the systemd service command, `systemctl pingcentral-# start`.
9. Log in to the application using the following credentials:
  - **Username:** Administrator
  - **Password:** 2Federate

Without modification, PingCentral is secure by default. However, if you want to use self-signed server certificates, root certificates, intermediate certificates, and certificates from a private certificate

authorities, create a PingCentral-specific truststore and configure PingCentral to access it. Refer to [Creating and configuring trust](#) for instructions.

10. Configure PingCentral to run as a Windows service, Linux systemd service, or Linux systemd service, if appropriate.

## 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.

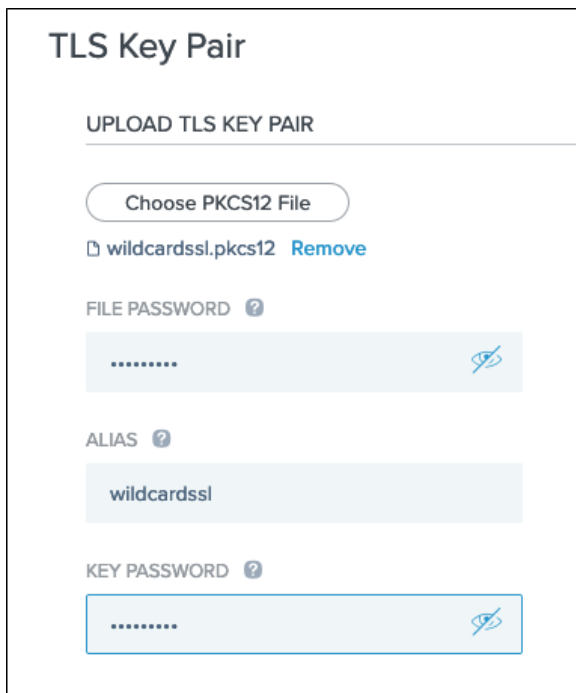
## Replacing the Admin Console SSL Certificate

---

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.

### Steps

1. Select the **Setting** tab at the top of the page.
2. Expand the **Security** menu on the left side of the page and select TLS Key Pair.
3. Click the **Choose PKCS12 File** button and upload the new file.
4. Enter the alias and passwords in the appropriate fields and click **Save**.



The screenshot shows the 'TLS Key Pair' configuration page. At the top, there is a section titled 'UPLOAD TLS KEY PAIR'. Below this, there is a button labeled 'Choose PKCS12 File'. Underneath the button, a file named 'wildcardssl.pkcs12' is listed with a 'Remove' link next to it. Below the file list, there are three input fields: 'FILE PASSWORD' with a question mark icon, 'ALIAS' with a question mark icon, and 'KEY PASSWORD' with a question mark icon. Each password field contains a series of dots and has an eye icon to toggle visibility. The 'ALIAS' field contains the text 'wildcardssl'.

5. Restart PingCentral.

After PingCentral is restarted, you will be able to access PingCentral without receiving a certificate warning.



## Managing environments

---

All environments managed within PingCentral and connected PingFederate environments display on the Environments page, where you can view and update information about each environment, update identity provider certificates, and delete environments from PingCentral when you no longer need them.

### Steps

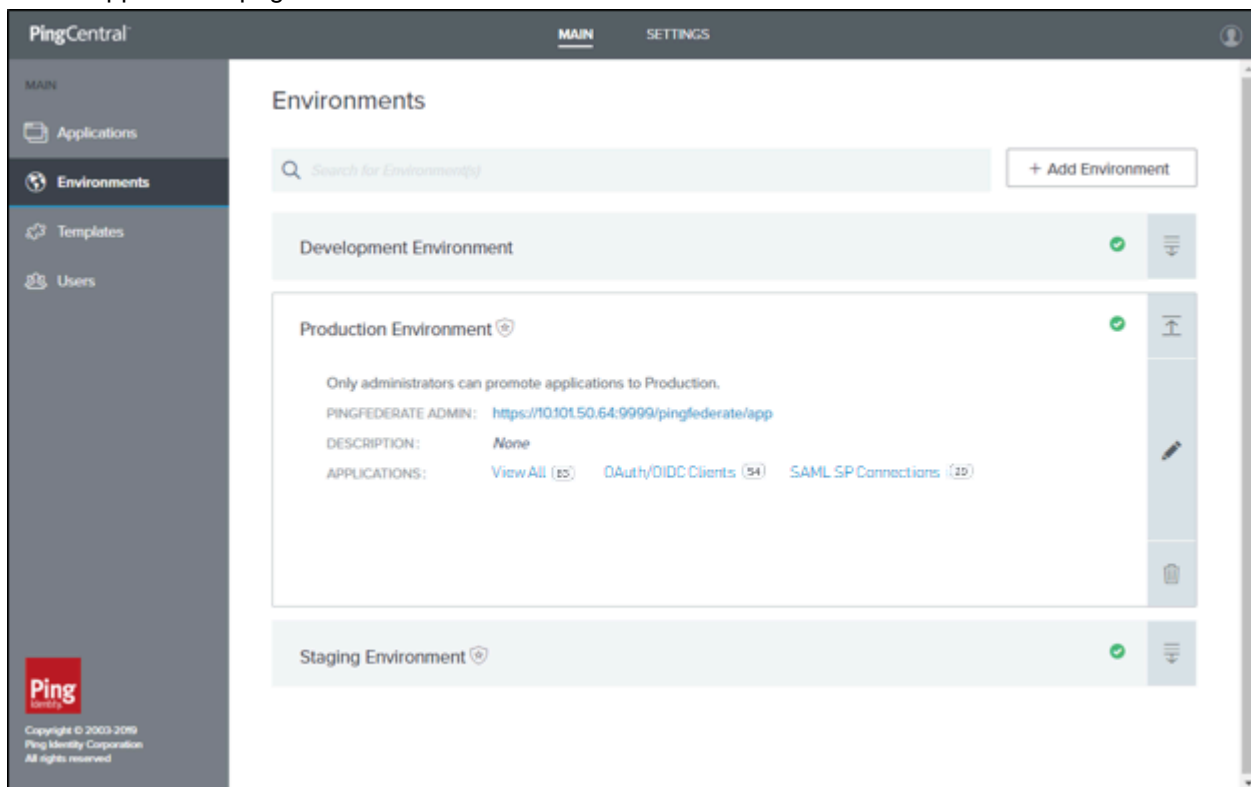
#### 1. To add an environment:

- a. Click **Add Environment** on the Environments page.
- b. Connect to PingFederate using your PingFederate Admin credentials. Click **Next**.
- c. On the Name Environment page, complete the **Name**, **Short Code**, and **Description** fields.
- d. Optional: To prevent non-administrators from promoting applications to the environment, select the **Protect** checkbox.
- e. Click **Save and Continue**.
- f. To upload an identity provider certificate for SAML applications, click **Choose** and enter the certificate password in the appropriate field. Click **Save and Close**.  
The environment displays on the Environments page. If you chose to protect the environment, a shield icon displays next to its name.

2. To view and edit environment information:

a. Click the expandable icon associated with the environment to view environment details. You will see:

- 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 SP connections. Click these links to access filtered lists of these applications on the Applications page.



b. To edit the environment information, click the pencil icon.

All of the editable information displays on one page. Update it as necessary.

c. To update the identity provider certificate used to promote SAML applications, click **Choose** to upload a new certificate, and then enter the certificate password in the appropriate field.

d. Click **Save**.

3. To delete an environment from PingCentral, click its associated trash can icon.

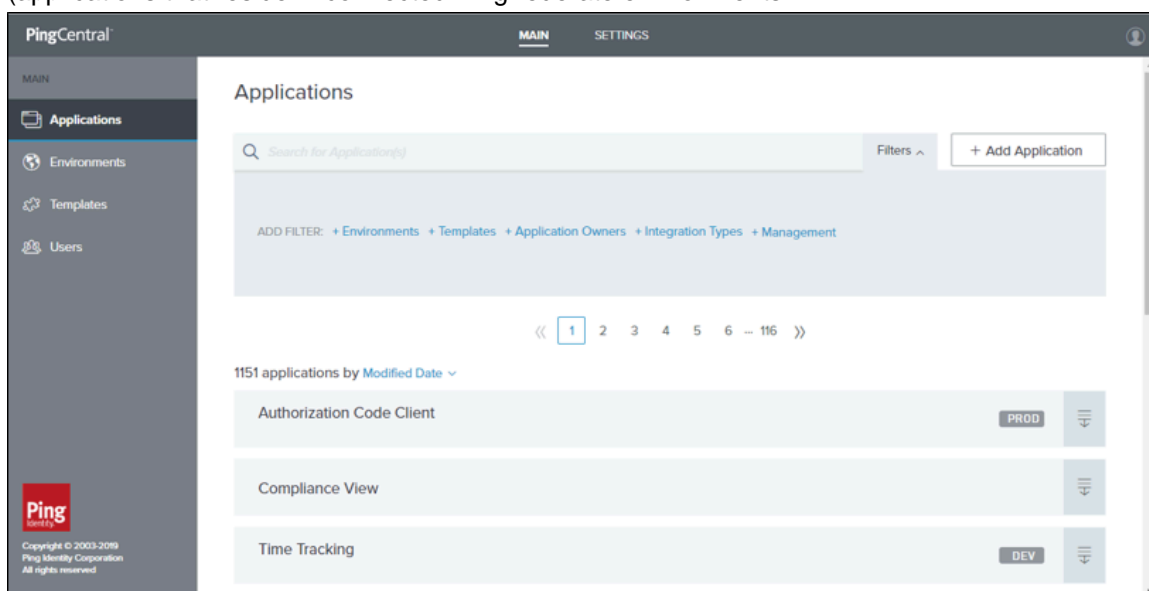
## Managing applications

All PingCentral applications and applications in connected PingFederate environments display on the Applications page, where 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 filters at the top of the page to filter your list of applications. You can filter by:

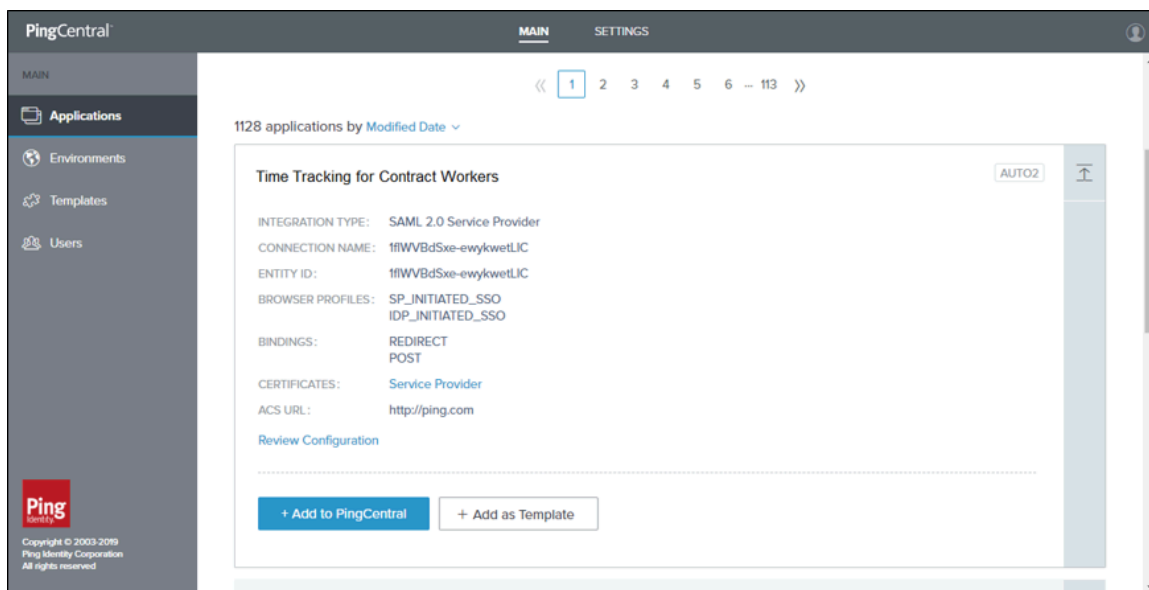
- Environment
- Template
- Application owner
- Integration type (OAuth and OIDC or SAML)
- Managed (applications created from or promoted to PingCentral environments), and Unmanaged (applications that reside in connected PingFederate environments).



The screenshot displays the PingCentral interface for managing applications. The top navigation bar includes 'MAIN' and 'SETTINGS'. The left sidebar shows 'MAIN' with sub-items: 'Applications', 'Environments', 'Templates', and 'Users'. The main content area is titled 'Applications' and features a search bar with the placeholder 'Search for Application(s)', a 'Filters' dropdown, and a '+ Add Application' button. Below the search bar, there is a filter bar with the text 'ADD FILTER: + Environments + Templates + Application Owners + Integration Types + Management'. A pagination control shows '1' selected, with other numbers 2, 3, 4, 5, 6, and a range '... 116'. The application list is sorted by 'Modified Date' and contains three entries: 'Authorization Code Client' (status: PROD), 'Compliance View', and 'Time Tracking' (status: DEV). Each entry has a three-line menu icon on the right. The bottom left corner of the interface shows the Ping logo and copyright information: 'Copyright © 2003-2019 Ping Identity Corporation All rights reserved'.

2. To add an application to PingCentral, you can:

- Click **Add Application** and follow the wizard prompts to apply a template to your application.
- Create a template from an unmanaged application. Select the expandable icon associated with it, click **Add as Template** as shown below, and follow the wizard prompts. Then, apply the new template to an application.
- Add an unmanaged application directly to PingCentral without using a template. Select the expandable icon associated with it, click **Add to PingCentral** as shown below, name the application, and save it.



3. To edit applications managed in PingCentral, click the expandable icon associated with the application you want to update and click the pencil icon. All of the editable information displays on one page. Update it as necessary.
4. To delete an application from PingCentral, click its associated trash can icon.

**Note:** Although the application will no longer be available in PingCentral, it will still exist in PingFederate. Delete it from PingFederate, as necessary.

## User management

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 login screen.

Refer to the following:

- [Setting up SSO](#)
- [Managing users through 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.

## Setting up SSO for PingCentral

The SSO login method is significantly more secure than the password authentication method. However, there are a variety of items to configure for it to work. At this time, OpenID Connect (OIDC) is used for SSO.

Refer to the following:

- [Auto-provisioning users](#)
- [Configuring SSO](#)
- [Configuring resource server functionality](#)
- [Configuring the OpenID provider](#)

### Auto-provisioning users

For each SSO user, a local PingCentral user is automatically created the first time they log in. This information is obtained from the subject (sub) claim provided by the OpenID provider.

The user's first name, last name, and role are also recorded. The user's name is derived from the given\_name and family\_name claims defined by the profile scope.

If first-time access to PingCentral is by way of API access using a bearer token, auto-provisioning also occurs if the user name and role are available. For performance reasons, subsequent bearer token access does not update the local user information, such as first name and last name.

At each SSO login, the role, first name, and last name might be updated based on token claims, which will overwrite any administrative updates made within PingCentral.

Although it is possible for PingCentral administrators to modify or delete auto-provisioned users, doing so will result in the SSO user being auto-provisioned again. Since the provisioning process generates a new PingCentral user ID, any application associations with the previous user ID will be lost.

### Configuring SSO

With PingCentral, SSO is disabled by default. To configure PingCentral for SSO, you need to enable it, configure OIDC properties to access OIDC configuration information, define an OAuth client at the OpenID provider, and configure PingCentral role mapping.

#### Enabling SSO

To enable SSO, access the `application.properties` file, which resides in the `conf` folder in the PingCentral installation directory.

Uncomment the following property and set the value to **true**:

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

#### Configuring OIDC

To configure OIDC, locate the following property, uncomment it, and define the Issuer URI:

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

In this example, PingCentral will attempt to access OIDC configuration information at:

```
https://sso.mycompany.com:9031/.well-known/openid-configuration
```

PingCentral will fail to start if it cannot access this information. Ensure 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, PingCentral must be restarted to incorporate it.

#### Defining the OAuth client

An OAuth client must be defined for PingCentral at the OpenID provider. Locate the following property, uncomment it, and provide the client ID and client secret for the OAuth client:

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

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

It is highly recommended that you 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

In PingCentral version 1.0, two user roles are defined: the IAM Administrator, and the Application Owner. An initial IAM Administrator is created by default. That user 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 via a claim defined in the ID token or UserInfo endpoint. If this claim is not found, or its value is nonsensical, the user is denied access to PingCentral, and auto-provisioning does not occur.

With PingFederate, an attribute can be mapped into the appropriate claim. The claim name and values are configurable, as shown in this example:

```
# 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
```

If these defaults can be used with the OpenID Provider, no further configuration is required. Otherwise, the claim name and/or values can be set to synchronize PingCentral to the OpenID Provider configuration, as shown in this example:

```
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 resource server functionality

PingCentral supports OAuth resource server functionality by validating provided bearer tokens when accessing the Admin API. Only JWT tokens are supported in this release, so a JWKS endpoint is required for signature validation.

To define this endpoint, access the `application.properties` file, which resides in the `conf` folder in the PingCentral installation directory. Uncomment the following property and define the JWKS endpoint URI, as shown in this example:

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

While the subject (sub) claim is mandatory with OpenID Connect, it is not required when using OAuth 2.

With bearer tokens, PingCentral looks for the **Username** claim by default, but this also can be configured, as shown in this example:

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

## Configuring the OpenID provider

PingCentral version 1.0 has been tested with PingFederate 9.2.x and 9.3.x, serving as both the OpenID provider and OAuth 2 authorization server. PingCentral is an OpenID relying party, as well as an OAuth 2 resource server.

This section provides tips for integrating PingCentral into an existing OIDC 1.0 SSO infrastructure using PingFederate as the Open ID provider. However, 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, such as PingOne for Customers, can also be used.

This section does not provide details on setting up ATMs, OIDC policies, or attribute contracts as these topics are complex and often specific to a development environment.

### Configuring the OAuth client

Defining a PingCentral-specific OAuth client is recommended. Configure the following:

- **Client authentication:** Choose client secret and assign a secret. This secret also needs to be defined in PingCentral when you configure SSO. Refer to [Configuring SSO](#) for details.
- **Redirect URI:** Provide the redirect URI. For example, `https://<pc-host>:<pc-port>/login/oauth2/code/pingcentral`.
- **Allowed grant types:** Ensure **Authorization Code** is selected. If you want API access via bearer tokens, select the **Resource Owner Password Credentials** option as well.
- **OpenID connect:** For ID Token Signing Algorithm, select **RSA using SHA-256**. PingCentral 1.0 does not support ID token encryption.

### Configuring the OIDC policy

The OAuth client will be associated with an OIDC Policy, perhaps 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 `application.properties` file. Refer to [Configuring SSO](#) for details.

### Configuring the ATM

The ATM associated with the OIDC Policy must support JWT tokens. To validate the token signature, PingCentral must be provided a JWKS endpoint URL. Signing certificates and JWE encryption (symmetric or asymmetric) are not supported in this release.

In the ATM Instance Configuration, under **Show Advanced Fields**, define a JWKS endpoint path.

For example, given the endpoint path `/oauth/pingcentral/jwks`, configure PingCentral with:

```
pingcentral.sso.oidc.oauth-jwk-set-uri=https://<pf-host>:<pf-port>/ext/oauth/pingcentral/jwks
```

## Managing users through PingCentral

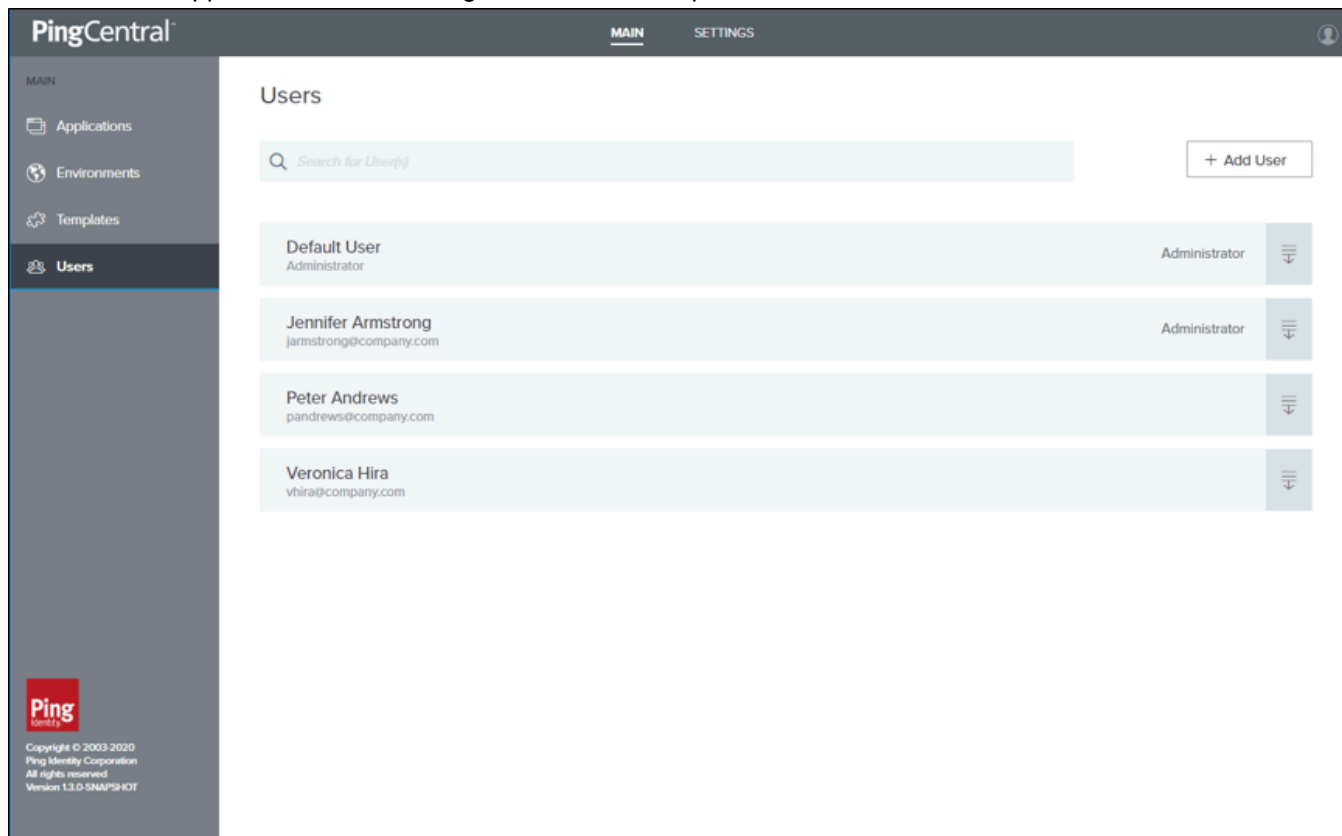
If you have a small number of users, you might want to manually add them to PingCentral and manage their access directly through the application. You need their first and last names, user names, and the roles they will assume.

### 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.

## Template management

When you create a PingCentral template based on an existing PingFederate application, or add an existing PingFederate application to PingCentral, the raw JSON is saved to PingCentral.

PingCentral does not display the entire JSON file when you select an application, but the most relevant information is provided to help you distinguish between applications.

For OAuth or OIDC, 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.
- Definitions of exclusive scopes referenced by the client.

Refer to [OIDC connection orchestration](#) to see a diagram of the PingFederate items orchestrated by PingCentral.

For SAML SP connections, the following items are saved:

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



Refer to [SAML connection orchestration](#) to see a diagram of the PingFederate items orchestrated by PingCentral.

Refer to the following for instructions on creating and updating OAuth and SAML SP templates:

- [Creating OAuth and OIDC application templates](#)
- [Creating SAML SP application templates](#)

## Creating OAuth and OIDC application templates

To create a template, select a client configuration that exists in a PingFederate environment to replicate. PingCentral retrieves this configuration from PingFederate and saves it as a generic building block for future applications.

About this task

A good template configuration should include meaningful defaults that will make sense across specific types of applications and if possible, reference authentication policies via policy contracts.

Steps

1. Select **Templates** to see a list of available templates.
2. Click **Add Template**, select the type of template you want to create from the initial screen (OAuth or OIDC), and click **Next**.
3. 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.

Details regarding the selected client

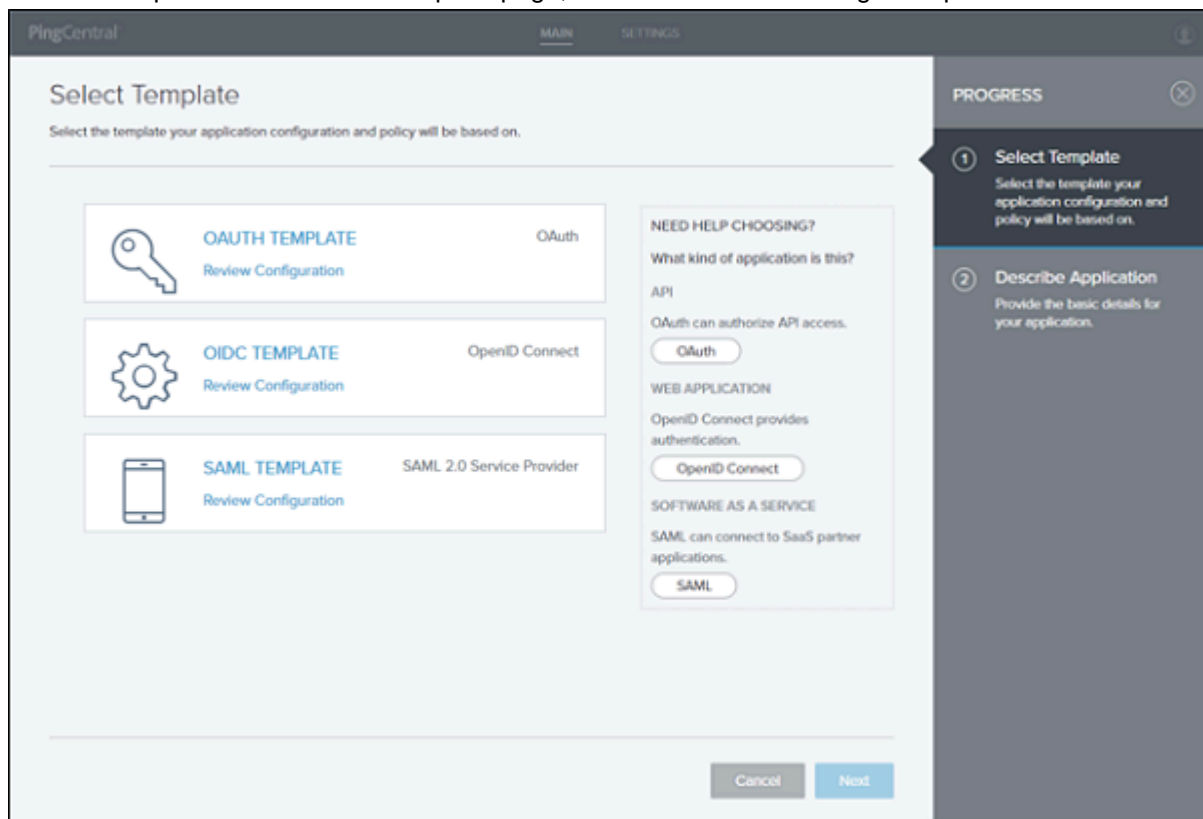
The screenshot displays the 'Select OAuth Client' wizard in PingCentral. The main content area is titled 'Select OAuth Client' and includes the instruction 'Select the PingFederate OAuth client you want to base your template on.' Below this, there is an 'ENVIRONMENT' dropdown menu set to 'Production Environment'. Underneath, 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, the details for the selected client are displayed: CLIENT NAME: '\*Client Credentials (JWT)\*', CLIENT ID: '\*Client Credentials (JWT)\*', DESCRIPTION: 'None', GRANT TYPES: 'CLIENT\_CREDENTIALS', EXCLUSIVE SCOPES: 'None', ATTRIBUTES: 'None', and OIDC POLICY: 'None'. A 'Review Configuration' link is located below these details. At the bottom of the main area, there are 'Cancel' and 'Next' buttons. On the right side, a 'PROGRESS' sidebar shows three steps: 1. Integration Type, 2. Select OAuth Client (current step), and 3. Name Template.

display.

4. To see the JSON for the application, click **Review Configuration**.
5. On the last page of the wizard, 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 will display with the template name and description.
7. Click **Save and Close**.

You will see the new template in the list of available application templates. Application owners will see the new template on the Select Template page, as shown in the following example.



## Creating SAML SP application templates

To create a template, select a connection configuration that exists in a PingFederate environment to replicate. PingCentral retrieves this configuration from PingFederate and saves it as a generic building block for future applications.

About this task

A good template configuration should include meaningful defaults that will make sense across specific types of applications and if possible, reference authentication policies via policy contracts.

Steps

1. Select **Templates** to see a list of available templates.
2. Click **Add Template** and select **SAML** from the initial screen. Click **Next**.

3. Select the PingFederate environment that hosts the connection you want to use as a template, and then select the connection from the **Connection** list.

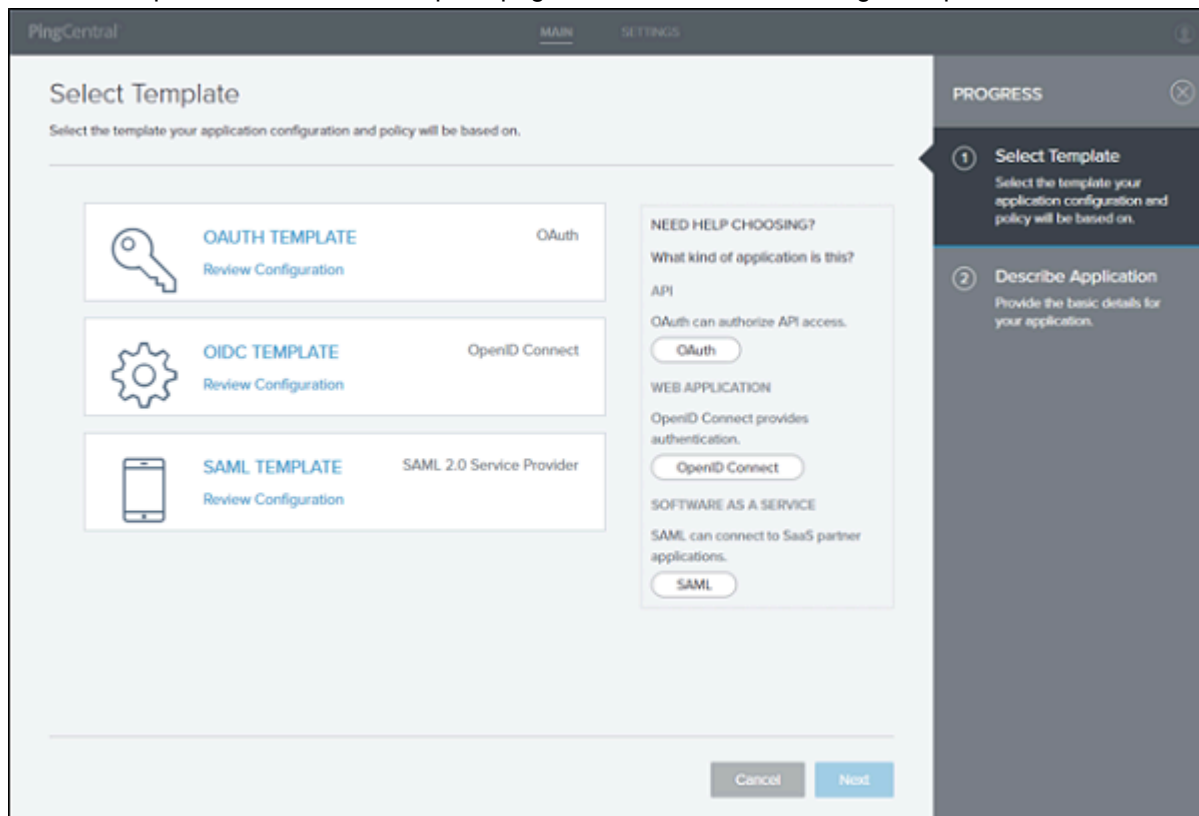
Details regarding the connection display.

The screenshot displays the 'Select SAML Connection' interface in PingCentral. The main area is titled 'Select SAML Connection' and includes the instruction 'Select the SAML connection you want to base your template on.' Below this, there is an 'ENVIRONMENT' dropdown menu currently set to 'Staging Environment'. A 'Connection' list is shown with a search bar and several radio button options: 'acbaselnesso' (selected), 'acbaselnesso-auth-policy', 'acbaselnesso-auth-policy-multi', 'SAML App with signing 2', and 'spConnection787702262'. To the right of the list, configuration details are displayed: CONNECTION NAME: acbaselnesso, ENTITY ID: acbaselnesso, BROWSER PROFILES: IDP\_INITIATED\_SSO, SP\_INITIATED\_SSO, BINDINGS: POST, REDIRECT, and POLICY CONTRACTS ASSOCIATED: None. A 'Review Configuration' link is provided below these details. At the bottom of the list area, it states 'Last retrieved from Staging Environment at 10:23 am. Refresh Now'. At the bottom right of the main panel are 'Cancel' and 'Next' buttons. On the far right, a 'PROGRESS' sidebar indicates the current step: '2 Select SAML Connection', with previous steps '1 Integration Type' and '3 Name Template' also visible.

4. To see the JSON for the SAML connection, click **Review Configuration**.
5. 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 will display with the template name and description.

## 7. Click **Save and Close**.

You will see the new template in the list of available application templates. Application owners will see the new template on the Select Template page, as shown in the following example.



## Promotion processes

PingCentral makes it possible for application owners to promote their OAuth, OIDC, and SAML SP applications to development environments themselves. This section explains how these promotion processes work.

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 does not 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, application owners can revert them to previously promoted versions. The reverted version of the application will not exist outside of PingCentral until it is promoted again, at which point it will also be available in PingFederate. See [Reverting applications to previously promoted versions](#) for details.

### OAuth and OIDC application promotions

When promoting OAuth and OpenID Connect applications, application owners provide the following information:

- **Redirect URIs:** The trusted location that the application will be 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.

Refer to [Using OAuth and OIDC templates](#) on page 13 in the *PingCentral for Application Owners guide* to learn more about this process.

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, will overwrite the PingFederate OAuth client within the target environment. If the client does not already exist, PingCentral will create 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 exclusive scopes that conflict with the target environment during the promotion process, PingCentral will not change them because they could be shared across clients. Otherwise, PingCentral will add the ATMs, OIDC policies, and exclusive scopes specified in the original JSON file.

PingCentral does not support saving or promoting access token mapping, persistent grants, policy contracts, or authentication policies.

### SAML SP application promotions

When promoting SAML SP applications, application owners can provide the following information:

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 could contains any or all of the following items:

- **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 IdP will be sent after user authentication occurs.
- **Attribute mapping information:** The application attributes 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.

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

Refer to [Using SAML SP templates](#) on page 15 in the *PingCentral for Application Owners guide* to learn more about this process.

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, will overwrite the PingFederate connection within the target environment. If the connection does not already exist, PingCentral will create all of the items defined in the application JSON, along with the information that the application owner provided.

PingCentral generates a self-signed IdP certificate with a 1-year expiration for each application and environment. This certificate cannot be uploaded, selected, or rotated in this release. If a connection is re-promoted, the same certificate is used and orchestrated to PingFederate.