PingCentral

Contents

Release Notes

PingCentral 1.5.0

For the best possible experience, review the following information about new features, resolved issues, and known issues prior to using PingCentral.

New features

Ticket ID	Description
PASS-1396	Administrators can create templates from PingAccess applications. For more information, see *Creating PingAccess application templates*.
PASS-1397	Application owners can apply PingAccess templates to their applications and promote them to PingAccess environments. For more information, see *Using PingAccess templates* and *Promoting PingAccess applications*.

Resolved issues

Ticket ID	Description
PASS-1552	When updating a user's role, the **Discard Changes** button works as expected.
PASS-2090	Previously, when PingCentral was configured to authenticate users through single sign-on (SSO) and it was not able to connect to PingFederate, the token provider, PingCentral would fail to start. This issue has been resolved. Now, if PingCentral cannot connect to PingFederate, PingCentral starts and users receive an error message indicating that a connectivity issue is preventing them from signing in.
PASS-2528	If you attempt to create applications without a signing key pair, you will receive the following message.`Application signing settings not found. PingCentral currently only supports connections with signing settings.`
PASS-3259	If administrators add PingFederate environments to PingCentral that are missing dependencies, such as an authentication policy or access token management (ATM) information, they receive an error message that more accurately describes the issue.
PASS-3476	Previously, when adding SAML metadata files or URLs to applications on the edit page, you could inadvertently save applications without any attribute mappings, including the SAML_SUBJECT attribute that is required for promotion. This issue was resolved, and you cannot promote applications until the SAML_SUBJECT attribute is assigned a value.
PASS-3610	If the only environment in PingCentral is deleted, users can see the applications created from and promoted to that environment on the **Applications** page.

Ticket ID	Description
PASS-3615	Previously, attribute scopes within an OpenID Connect policy must already have been defined within the target environment, or the policy could not be promoted.
PASS-4293	Previously, you could not promote a PingAccess application to an environment where an application with the same name, but different destination type (site or agent), already existed. This issue is resolved.
PASS-4307	If a PingFederate application was created from a template in a PingFederate version later than the version to which it is being promoted, the promotion fails. For example, if the template was created from a PingFederate 10.1 application, and you promote it to a PingFederate 9.3 environment, the promotion fails. Previously, when this occurred, users received an unclear error message. Now, users receive an error message stating that promotions to previous versions of Ping Identity products not currently supported.
PASS-4334	PingCentral token provider validation succeeds if the PingFederate base URL matches the PingAccess issuer URL. The default HTTPS port number 443 is no longer required to be explicitly indicated.
PASS-4451	Previously, if you promoted a PingAccess application and renamed it in PingCentral, you could not promote it again without reverting the name change. This issue is resolved.

Known issues

Ticket ID	Description
PASS-2093	When SSO is enabled, custom session settings are modifiable, but are not honored.
PASS-2097	When SSO is enabled, administrators can add and update users in PingCentral through the User Management page, even though it has no effect.
PASS-2122	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 **IDP Certificate Password** field each time a key is pressed.
PASS-2468	Administrators cannot update information for users not associated with a PingCentral environment, template, or application.
PASS-2526	If PostgreSQL is set up without a database, PingCentral will fail to start. To prevent this from happening, add the database to the server prior to starting PingCentral.
PASS-2819	If an OAuth application is added from an environment that does not use a client secret to authenticate, the **Client Secret** field displays, but is ignored. This display could cause confusion, as users can add and generate client secrets for their applications, but the secrets are not saved as expected.
PASS-2824	If you enter an invalid application name when updating a SAML application, you will not receive an error message.

Ticket ID	Description
PASS-3543	If a certificate is added to a SAML application and a SAML metadata file is subsequently provided that contains a certificate, additional changes to the application cannot be saved. If this occurs, exit the edit page and then access it again.
PASS-3613	PingCentral promotes access token mappings and APCs (Authentication Policy Contracts) with OIDC applications, but the APC mappings that link the APCs to the access token managers are not currently promoted with them. If the APC mappings do not already exist in the target PF environments, applications will not function as expected. When new APCs are promoted in PingCentral, access token mapping referencing the APC is created, but persistent grant mapping is not established so the configurations are invalid. To resolve these issues, configure the APC mappings within PingFederate.
PASS-3617	If you promote a SAML applications with an assertion encryption certificate and then attempt to edit the application, the **Save** and **Discard Changes** buttons display on the edit page before you make any changes, which could be misleading. Ignore this irregularity and click the **Save** button, or click the **Discard Changes** button to exit the edit page.
PASS-3618	If applications and environments have long names, you might not be able to see the entire list of available environments when you attempt to promote applications. To select an environment not immediately visible from the list, continue scrolling. The entire list will eventually display, but environment names toward the bottom of the list might appear distorted.
PASS-3634	When application owners use SSO to access PingCentral, administrators cannot assign applications to them prior to the application owners ever accessing PingCentral. However, after they sign on to PingCentral, administrators can access their account information and assign applications to them.
PASS-3643	If the **Promote** button is clicked more than once when a SAML application is promoted, the application could be unintentionally promoted to an environment multiple times. To prevent this from happening, press the Enter key during the promotion process.
PASS-3645	When adding and updating SAML applications, you receive an error message if you provide a service provider metadata file that does not contain certificate information. If this occurs, ignore the message and continue to add or update the application.
PASS-3830	If you update SAML attributes while updating other application information, the attribute information will not be saved. To prevent this from happening, update the attributes and save your changes. Then, you can update additional application information.

Ticket ID	Description
PASS-4174	If owner or promotion configuration information is updated for a PingAccess application, or a PingAccess application is promoted, the modified timestamp does not update as it should, which could be deceiving if the list of applications is sorted by modified date. However, if you update the name, description, context root, resources, or policy, the timestamp is also updated.
PASS-4249	If you add an application to PingCentral from the **Applications** page, unmanaged applications might display that you cannot manage.
PASS-4280	If you filter for PingAccess applications, add a PingAccess application by using the **Add to PingCentral** button, and return to the **Applications** page, the filter might appear to be on and you might not be able to view the details for another unmanaged PingAccess application. If this occurs, refresh your browser window.
PASS-4300	If PingCentral is installed as a service, installation files are stored in a local directory, such as `/usr/local/pingcentral-1-1.4.0/`. When using the command line to upgrade to 1.5.0, ensure that the existing parameter points to the direct path of the previous installation, and not to the softlink path, which appears first. Selecting the softlink path results in the installation failing even though a success message displays.
PASS-4304	Administrators can change environment short codes to codes that already exist. If this occurs, and users promote an application to two different environments with the same short code, only one environment status icon displays, which could be misleading. To prevent this from happening, ensure each environment short code is unique.

PASS-4305	If PingCentral was installed as a Linux service by one user, and the upgrade is performed by another, the service might no longer start. To resolve this issue, run the following command to update the installation files to match the existing ownership:
	`chown -R [user]:[group] [INSTALL_DIR]`
	Where the user and group match the existing installation. For example:
	`chown -R pingcentral:pingcentral /usr/local/pingcentral-1`

PASS-4376	When you start PingCentral 1.5, you might see warning messages related to illegal reflective access by `org.springframework.util.ReflectionUtils`. These messages can be safely ignored.
PASS-4460	If a password is entered for a PKCS12 (P12) file when updating the TLS key pair, you might receive a misleading error indicating that the alias is not found. To prevent this from happening, leave the key password blank for PKCS12 key pair files.
PASS-4579	When editing PingAccess applications, pressing the Enter key after making changes to the context root does not always save the changes to the context root. When these applications are promoted, they contain an incorrect context root. To prevent this from happening, click **Save** rather than pressing **Enter**.

Ticket ID	Description
PASS-4583	If you change a template associated with a PingAccess application and click **Cancel**, the newly selected template displays on the edit page. If this occurs, refresh the page to see that the original template is still associated with the application.
PASS-4615	If unsupported PingCentral APIs are used to update a PingAccess application and the JSON is saved incorrectly, the **Application** page might become unresponsive. If this occurs, ensure the application JSON is valid and reload the page.
PASS-4619	When an assertion encryption certificate has been used to promote an application, or when a certificate is added to an application, the certificate does not display when the application is promoted or when subsequent updates are made. To ensure that the correct certificate is applied, reselect the certificate when you promote the application.
PASS-4633	When using templates to add Web + API applications to PingCentral, you can drag rules between Web and API policies, which might cause the page to go blank. If this occurs, refresh the browser window.
PASS-4660	Entering a context root that begins with the reserved context root in PingAccess (typically `/pa`) displays generic "Save Failed" error message, instead of a more descriptive one. For example, if `/pa` is a reserved context root in PingAccess and you enter `/papapizza` as a context root, you receive this message.
PASS-4668	If a template was created from a PingAccess application, and that application is deleted from PingAccess, you can no longer add applications to PingCentral using that template.
PASS-4685	If administrators attempt to add a PingAccess application to PingCentral while PingAccess is unavailable and they click the **Refresh Now** link, the **Application** page might not display any applications. To prevent this from happening, they should select the `Skip Verification` option for the PingAccess environment to skip the validation process until it becomes available.
PASS-4688	If you are using a Postgres database with PingCentral and you attempt to sort applications by name when filters are applied, you might receive a server error message. To work around this issue, either remove the filters to sort all applications by name, or retain the filters with applications sorted by modification date.

PingCentral 1.4.0

New features, resolved issues, and known issues are listed and described here. For the best possible experience, review this information prior to using PingCentral.

New features

Ticket ID	Description
PASS-2429	During the PingCentral upgrade process, the upgrade utility merges the new version of the `application.properties` file with the older version, preserving property values previously customized.
PASS-2827	You can upgrade to PingCentral version 1.4.0 directly from either version 1.2.0 or 1.3.0. Files that were not modified since they were initially installed are overwritten with new versions during the upgrade process. Note the following: ▪ If the `application.properties` file was modified, the new version of the file will be merged with the latest version, preserving customizations. ▪ If the `conf/log4j2.xml`, `bin/run.sh`, and `bin.run.bat` files were modified, the new versions are installed and the old versions are renamed. Manually update the new files with customizations, as necessary.
PASS-3189	Administrators can add existing PingAccess applications to PingCentral. For more information, see *Adding PingAccess applications*.
PASS-3191	Application owners can promote PingAccess applications to other PingAccess environment tiers and apply environment configuration dependencies, such as web sessions, identity mapping, virtual hosts, sites, and agents.
PASS-3563	Administrators can add PingAccess environment instances to PingCentral. For more information, see *Environment Management*.

Resolved issues

Ticket ID	Description
PASS-2119	Protected environment text on the **Environments** page no longer incorrectly refers to "production" if the protected environment is not a production environment.
PASS-3556	The **Restore** button is now hidden for applications promoted in version 1.2.0.
PASS-3586	Previously, if the combination of an application's Redirect URIs exceeded 255 characters, users could not add the application to PingCentral. This character limitation was removed for this release, which resolved the issue.
PASS-3644	If a PingFederate environment is added to PingCentral and becomes unavailable for any reason, the **Applications** page is no longer empty.
PASS-3646	Scope names cannot contain spaces, so users are now prevented from adding scopes with spaces in the name to their applications.
PASS-3648	When updating SAML applications, users can provide a new metadata file to replace an older version. If the new file contains a certificate, the correct certificate now displays.
PASS-3659	When promoting SAML applications with multiple authentication policy contracts that were directly imported into PingCentral, the first contract on the list is used, as intended, and promotion failures no longer occur.

Ticket ID	Description
PASS-3663	When creating templates or adding existing OAuth or OIDC applications to PingCentral and scopes are not restricted, the **Scopes** field correctly displays the following message: `This application uses all common scopes provided by the target environment.`
PASS-3714	When searching for a scope that does not exist, the **Add** button no longer incorrectly displays.
PASS-3809	Users can no longer add a partial scope name to the**Scopes** field.
PASS-3825	When searching for or adding scopes, users will now receive an appropriate error message when they enter invalid characters.

Known issues

Ticket ID	Description
PASS-1552	When updating a user's role, the **Discard Changes** button does not currently work.
PASS-2090	If SSO is configured for PingCentral and PingFederate is unavailable, PingCentral will fail to start. If this occurs, determine why PingFederate is unavailable, resolve the issue, and restart PingCentral.
PASS-2093	When SSO is enabled, custom session settings are modifiable, but are not honored.
PASS-2097	When SSO is enabled, an administrator is able to update and add users to PingCentral via the User Management page, even though it has no effect.
PASS-2122	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 **IDP Certificate Password** field each time a key is pressed.
PASS-2468	Administrators cannot update information for users not associated with a PingCentral environment, template, or application.
PASS-2526	If PostgreSQL is set up without a database, PingCentral will fail to start. To prevent this from happening, add the database to the server prior to starting PingCentral.
PASS-2528	Users who attempt to create a SAML application without a signing key pair might receive a server error.
PASS-2819	If an OAuth application is added from an environment that does not use a client secret to authenticate, the **Client Secret** field displays, but is ignored. This display could cause confusion, as users can add and generate client secrets for their applications, but the secrets are not saved as expected.
PASS-2824	Users who enter invalid application names when updating their SAML applications do not receive an error message.

Ticket ID	Description
PASS-3259	If an administrator adds a PingFederate environment to PingCentral that is missing a dependency, such as authentication policy or access token management (ATM) information, they will receive the following error message: `Environment <pf_environment> Resource not found <missing_dependency>` To resolve this issue, either add the missing dependency to the environment in PingFederate, or remove the environment from PingCentral. Otherwise, PingCentral might become unusable.
PASS-3476	When adding SAML metadata files or URLs to applications in the edit screen, you can inadvertently save applications without any attribute mappings, including the SAML_SUBJECT attribute that is required for promotion. If you attempt to promote those applications, you will receive an error message informing you that the SAML_SUBJECT attribute is missing from the attribute contract fulfillment. To resolve this issue, access the edit screen for the application, assign the SAML_SUBJECT attribute a value, and attempt to promote the application again.
PASS-3543	If an SP certificate is added to a SAML application and a SAML metadata file is subsequently provided that contains a certificate, additional changes to the application cannot be saved. If this occurs, exit the edit screen and then access it again.
PASS-3610	If only one environment exists when you create a SAML application, and that environment is deleted, the **Applications** page will crash. If this occurs, add an environment directly to /pass/main/environments.
PASS-3613	PingCentral promotes access token mappings and APCs (Authentication Policy Contracts) with OIDC applications, but the APC mappings that link the APCs to the access token managers are not currently promoted with them. If the APC mappings do not already exist in the target PF environments, applications will not function as expected. When new APCs are promoted in PingCentral, access token mapping referencing the APC is created, but persistent grant mapping is not established so the configurations are invalid. To resolve these issues, configure the APC mappings within PingFederate.
PASS-3615	The attribute scopes within an OIDC policy must already be defined within the target environment, or the policy cannot be promoted.
PASS-3617	If you promote a SAML application with an assertion encryption certificate and then attempt to edit the application, the **Save** and **Discard Changes** buttons display on the edit screen before you make any changes, which could be misleading. Ignore this irregularity and click the **Save** button, or click the **Discard Changes** button to exit the edit screen.

Ticket ID	Description
PASS-3618	If applications and environments have long names, you might not be able to see the entire list of available environments when you attempt to promote applications. To select an environment not immediately visible from the list, continue scrolling. The entire list will eventually display, but environment names toward the bottom of the list might appear distorted.
PASS-3634	When application owners use SSO to access PingCentral, administrators cannot assign applications to them prior to the application owners ever accessing PingCentral. However, after they sign on to PingCentral, administrators can access their account information and assign applications to them.
PASS-3643	If the **Promote** button is clicked more than once when a SAML application is promoted, the application could be unintentionally promoted to an environment multiple times. To prevent this from happening, press the Enter key during the promotion process.
PASS-3645	When adding and updating SAML applications, users receive error messages if they provide a service provider metadata file that does not contain certificate information. If this occurs, ignore the message and continue to add or update the application.
PASS-3830	If you update SAML attributes while updating other application information, the attribute information will not be saved. To prevent this from happening, update the attributes and save your changes. Then you can update additional application information.
PASS-4174	If owner or promotion configuration information is updated for a PingAccess application, or a PingAccess application is promoted, the modified timestamp does not update as it should, which could be deceiving if the list of applications is sorted by modified date. However, if a PingAccess application name or description is updated, the modified timestamp behaves as expected.
PASS-4249	If you add an application to PingCentral from the **Applications** page, unmanaged applications might display that you cannot manage.
PASS-4259	When adding PingFederate and PingAccess environments, you might receive an inaccurate messages stating that you successfully connected to PingFederate when you opted to skip the verification. Likewise, you might not receive a message stating that you have successfully connected to PingAccess when you have. To determine the status of the environments, access the Environments page and review the status of the environments to determine which are connected.
PASS-4280	If you filter for PingAccess applications, add a PingAccess application by using the **Add to PingCentral** button, and return to the Applications page, the filter might appear to be on and you might not be able to view the details for another unmanaged PingAccess application. If this occurs, refresh your browser window.

Ticket ID	Description
PASS-4293	Users cannot promote a PingAccess application to an environment where an application with the same name is already present, but has a different destination type (agent or site). The promotion will fail and an error message displays stating that an ID for the existing destination type is required. If this occurs, administrators can manually update the destination within PingAccess to match the application defined in PingCentral.
PASS-4300	If PingCentral is installed as a service, installation files are stored in a local directory, such as `/usr/local/pingcentral-1-1.3.0/`. When using the command line to upgrade to version 1.4.0, ensure that the *existing* parameter points to the direct path of the previous installation, and not to the softlink path, which appears first. Selecting the softlink path results in the installation failing even though a success message displays.
PASS-4305	If PingCentral was installed as a Linux service by one user, and the upgrade is performed by another, the service might no longer start. To resolve this issue, run the following command to update the installation files to match the existing ownership: `chown -R [user]:[group] [INSTALL_DIR]` Where the user and group match the existing installation. For example: `chown -R pingcentral:pingcentral /usr/local/pingcentral-1`
PASS-4307	If a PingFederate application was created from a template in a PingFederate version higher than the version to which it is being promoted, the promotion will fail. For example, if the template was created from a PingFederate version 10.1 application, and you promote it to a PingFederate 9.2.3 environment, the promotion will fail.

PingCentral 1.3.0

New features, resolved issues, and new known issues are listed and described here. For the best possible experience, review this information prior to using PingCentral.

New features

Ticket ID	Description
PASS-933	Access token mapping information is now stored when applications are added to PingCentral and transferred into the target PingFederate instances when applications are promoted.
PASS-1128	Application owners can now revert applications 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.
PASS-1528	PingCentral now supports the PostgreSQL open source relational database system.

Ticket ID	Description
PASS-2015	When using SAML templates, application owners can now provide an `.xml` file that could contain an Entity ID, ACS URL, certificates, attribute information, or all of this information, from a similar SAML application. Or, they can continue providing the Entity ID, ACS URL and certificates during the promotion process.
PASS-2202	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 now available to download as an `.xml` file, which you can use to promote other SAML applications.
PASS-2414	You can now use Docker to deploy PingCentral. Preconfigured Docker images are available in Docker containers, which provide complete working instances of applications that are immediately available to use after they are deployed.
PASS-2839	PingCentral now promotes the first Authentication Policy Contract (APC) configured for service provider connections. In prior releases, the APC, with the same ID, was expected to already exist in the target environment for the connection promotion to succeed.
PASS-3177	Application owners can now encrypt a SAML assertion if encryption is enabled for the connection.
PASS-3262	Application owners can now customize the scopes they apply to their OAuth and OIDC applications.

Resolved issues

Ticket ID	Description
PASS-2119	Protected environment text on the Environments page no longer incorrectly refers to "production" if the protected environment is not a production environment.
PASS-2740	Unverified environments no longer display when templates and applications are added to PingCentral, and when applications are promoted.
PASS-2766	Using special characters when searching on the **Environments**, **Templates**, and **Users** pages no longer results in a server error.
PASS-2783	The sorting feature is no longer case sensitive for applications managed within PingCentral.
PASS-2872	When updating SAML applications, PingCentral now correctly indicates whether certificates are optional.
PASS-2879	Administrators who have been deleted or demoted to an Application Owner role can no longer perform administrative tasks during an open session.
PASS-2888	After creating an environment, the user wizard can now be accessed without errors.
PASS-2925	When adding environments, users who select the **Skip Verification** option and enter passwords with more than 32 characters no longer receive data integrity violation errors.

Known issues

Ticket ID	Description
PASS-1552	When updating a user's role, the **Discard Changes** button does not currently work.
PASS-2090	If SSO is configured for PingCentral and PingFederate is unavailable, PingCentral will fail to start. If this occurs, determine why PingFederate is unavailable, resolve the issue, and restart PingCentral.
PASS-2093	When SSO is enabled, custom session settings are modifiable, but are not honored.
PASS-2097	When SSO is enabled, an administrator is able to update and add users to PingCentral via the User Management page, even though it has no effect.
PASS-2122	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 **IDP Certificate Password** field each time a key is pressed.
PASS-2468	Administrators cannot update information for users not associated with a PingCentral environment, template, or application.
PASS-2526	If PostgreSQL is set up without a database, PingCentral will fail to start. To prevent this from happening, add the database to the server prior to starting PingCentral.
PASS-2528	Users who attempt to create a SAML application without a signing key pair might receive a server error.
PASS-2819	If an OAuth application is added from an environment that does not use a client secret to authenticate, the **Client Secret** field displays, but is ignored. This display could cause confusion, as users can add and generate client secrets for their applications, but the secrets are not saved as expected.
PASS-2824	Users who enter invalid application names when updating their SAML applications do not receive an error message.
PASS-3259	If an administrator adds a PingFederate environment to PingCentral that is missing a dependency, such as authentication policy or access token management (ATM) information, they will receive the following error message: `Environment <pf_environment> Resource not found <missing_dependency>` To resolve this issue, either add the missing dependency to the environment in PingFederate, or remove the environment from PingCentral. Otherwise, PingCentral might become unusable.
PASS-3476	When adding SAML metadata files or URLs to applications in the edit screen, you can inadvertently save applications without any attribute mappings, including the SAML_SUBJECT attribute that is required for promotion. If you attempt to promote those applications, you will receive an error message informing you that the SAML_SUBJECT attribute is missing from the attribute contract fulfillment. To resolve this issue, access the edit screen for the application, assign the SAML_SUBJECT attribute a value, and attempt to promote the application again.

Ticket ID	Description
PASS-3543	If an SP certificate is added to a SAML application and a SAML metadata file is subsequently provided that contains a certificate, additional changes to the application cannot be saved. If this occurs, exit the edit screen and then access it again.
PASS-3556	The **Restore** button incorrectly displays for applcations promoted in version 1.2.0, as these applications cannot be restored to previous versions.
PASS-3586	If the combination of an application's Redirect URIs exceeds 255 characters, users cannot add the application to PingCentral.
PASS-3613	PingCentral now promotes access token mappings and APCs (Authentication Policy Contracts) with OIDC applications, but the APC mappings that link the APCs to the access token managers are not currently promoted with them. If the APC mappings do not already exist in the target PF environments, applications will not function as expected. When new APCs are promoted in PingCentral, access token mapping referencing the APC is created, but persistent grant mapping is not established so the configurations are invalid. To resolve these issues, configure the APC mappings within PingFederate.
PASS-3615	The attribute scopes within an OIDC policy must already be defined within the target environment, or the policy cannot be promoted.
PASS-3617	If you promote a SAML application with an assertion encryption certificate and then attempt to edit the application, the **Save** and **Discard Changes** buttons display on the edit screen before you make any changes, which could be misleading. Ignore this irregularity and click the **Save** button, or click the **Discard Changes** button to exit the edit screen.
PASS-3618	If applications and environments have long names, you might not be able to see the entire list of available environments when you attempt to promote applications. To select an environment not immediately visible from the list, continue scrolling. The entire list will eventually display, but environment names toward the bottom of the list might appear distorted.
PASS-3634	When application owners use SSO to access PingCentral, administrators cannot assign applications to them prior to the application owners ever accessing PingCentral. However, after they sign on to PingCentral, administrators can access their account information and assign applications to them.
PASS-3643	If the **Promote** button is clicked more than once when a SAML application is promoted, the application could be unintentionally promoted to an environment multiple times. To prevent this from happening, press the **Enter** key during the promotion process.

Ticket ID	Description
PASS-3644	If a PingFederate environment is added to PingCentral and becomes unavailable for any reason, no applications will display on the Applications page. To resolve this issue, an administrator can remove the environment from PingCentral, set PingCentral to skip verification on the environment, or resolve the issues making the environment unavailable.
PASS-3645	When adding and updating SAML applications, users receive error messages if they provide a service provider metadata file that does not contain certificate information. If this occurs, ignore the message and continue to add or update the application.
PASS-3646	The names of scopes added to applications cannot contain spaces, nor can the **Scopes** field contain spaces before or after the scope name. If spaces exist, applications cannot be successfully promoted.
PASS-3648	When updating SAML applications, users can provide a new metadata file to replace an older version. If the new file does not contain a certificate, the certificate associated with the older version might still display. If this occurs, click **Cancel** and select the `.xml` file again. The page will reflect the absence of a certificate after it is refreshed.
PASS-3659	When promoting SAML applications with multiple authentication policy contracts that were directly imported into PingCentral, the first contract on the list should be used. However, all contracts in the list are currently being used, which results in promotions failing if the destination environments do not contain authentication policy contracts with matching IDs.
PASS-3663	When creating templates or adding existing OAuth or OIDC applications to PingCentral, information regarding the client displays. When scopes are not restricted, the **Scopes** field displays `None`, when it should display the following message: `This application uses all common scopes provided by the target environment.`
PASS-3714	When searching for a scope that does not exist, the **Add** button incorrectly displays.
PASS-3809	Users can currently add partial scope names to the **Scopes** field.
PASS-3825	When searching for or adding scopes, users who enter invalid characters receive invalid scope error message instead of a message that describes the issue.

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 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 systemv service, a Linux systemd 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 `Skip Verification` 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 `log4j2.xml` file instead of accessing the `application.properties` file.

Known issues

Ticket ID	Description
PASS-1552	When updating a user's role, the **Discard Changes** button does not currently work.
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.
PASS-2090	If SSO is configured for PingCentral and PingFederate is unavailable, PingCentral will fail to start. If this occurs, determine why PingFederate is unavailable, resolve the issue, and restart PingCentral.
PASS-2093	When SSO is enabled, custom session settings are modifiable, but are not honored.
PASS-2097	When SSO is enabled, an administrator is able to update and add users to PingCentral via the User Management page, even though it has no effect.
PASS-2119	Protected environment text on the Environments page refers to “production,” even if the protected environment is not a production environment.
PASS-2122	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 **IDP Certificate Password** field each time a key is pressed.
PASS-2468	Administrators cannot update information for users not associated with a PingCentral environment, template, or application.
PASS-2526	If PostgreSQL is set up without a database, PingCentral will fail to start. To prevent this from happening, add the database to the server prior to starting PingCentral.
PASS-2528	Users who attempt to create a SAML application without a signing key pair might receive a server error.
PASS-2740	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-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.

Ticket ID	Description
PASS-2819	If an OAuth application is added from an environment that does not use a client secret to authenticate, the **Client Secret**field displays, but is ignored. This display could cause confusion, as users can add and generate client secrets for their applications, but the secrets are not saved as expected.
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 **Skip Verification** 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 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	Previously, a blank white screen would occasionally display instead of the intended details when the **View Client Details** link in the Promotion History section of the page was clicked. This issue has been resolved.
PASS-2296	The PingCentral download location in the Red Hat Enterprise Linux installer is now correct.
PASS-2276 PASS-2131	Having the **Username** field empty during the login process no longer results in a server error.

Known issues

Ticket ID	Description
PASS-1552	When updating a user's role, the **Discard Changes** button does not currently work.

Ticket ID	Description
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.
PASS-2090	If SSO is configured for PingCentral and PingFederate is unavailable, PingCentral will fail to start. If this occurs, determine why PingFederate is unavailable, resolve the issue, and restart PingCentral.
PASS-2097	When SSO is enabled, an administrator is able to update and add users to PingCentral via the User Management page, even though it has no effect.
PASS-2122	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 **IDP Certificate Password** field each time a key is pressed.
PASS-2496	Updating the `log4j2.xml` file has no effect. As a workaround, update logging levels through the `application.properties` file.

PingCentral 1.0.0 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 **Discard Changes** button does not currently work.
PASS-1620	Clicking on the **View Client Details** 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 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.
PASS-2090	If SSO is configured for PingCentral and PingFederate is unavailable, PingCentral will fail to start. If this occurs, determine why PingFederate is unavailable, resolve the issue, and restart PingCentral.
PASS-2097	When SSO is enabled, an administrator is able to update and add users to PingCentral via the User Management page, even though it has no effect.

Ticket ID	Description
PASS-2122	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 **IDP Certificate Password** field each time a key is pressed.
PASS-2276 PASS-2131	Having the **Username** field empty during the login process results in a server error.
PASS-2296	The PingCentral download location in the Red Hat Enterprise Linux installer is incorrect.

Known limitations

Limitation	Workaround
There is no PingCentral installer for Microsoft Windows.	Install PingCentral by unzipping the `ping-central-1.0.0.zip` file. Then, `run.bat` script, which is located in the `bin` folder. Or, run PingCentral as a service using the provided method, which is located in the `sbin` 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 `PINGCENTRAL_SESSION_ID` 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, `PINGCENTRAL_SESSION_ID`, 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.	
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.

OAuth/OIDC limitation	Workaround
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 IAM Administrators

Introduction to PingCentral

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

PingCentral:

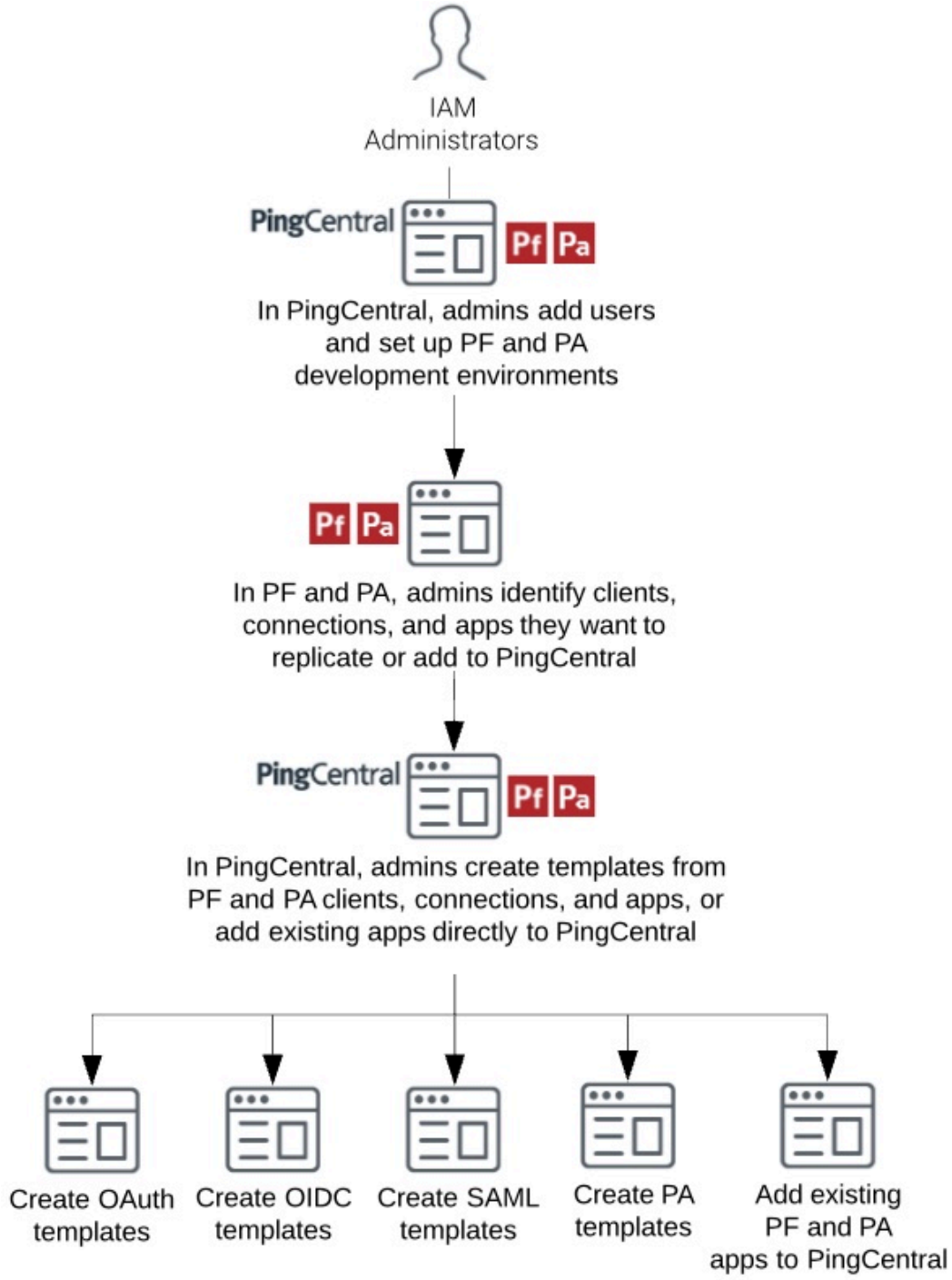
- Removes many tasks from your long list of responsibilities, which lowers operational costs, reduces bottlenecks, and allows you to focus on the more complex elements of your job
- Provides a central monitoring location for greater visibility into applications across deployment life cycles
- Minimizes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

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

How PingCentral works

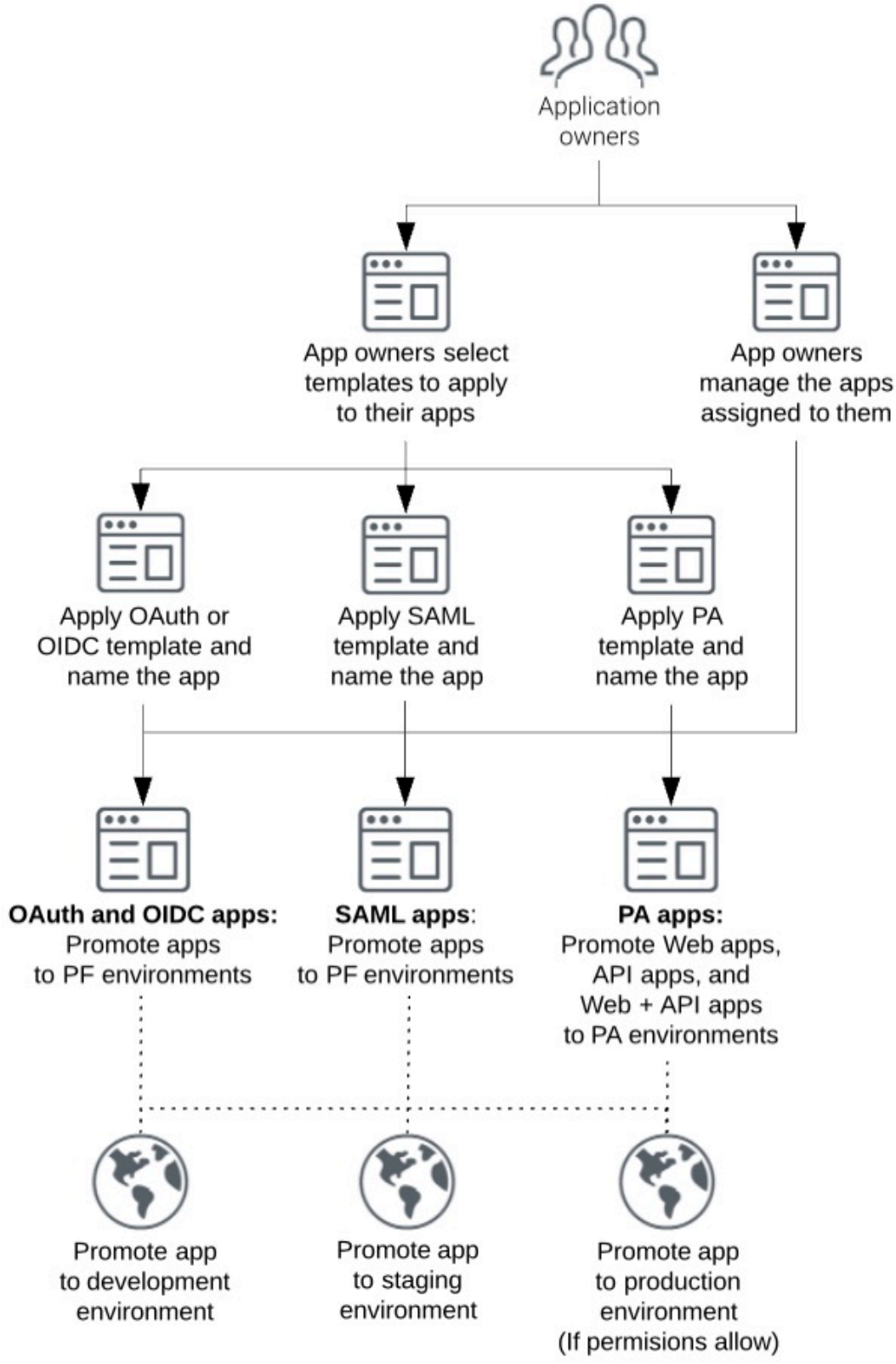
- In PingCentral, you set up users and define PingFederate and PingAccess development, test, and production environments.
- In PingFederate and PingAccess, you locate clients, connections, and application security configurations worthy of replicating.

- In PingCentral, you create PingFederate OAuth, OpenID Connect (OIDC), SAML, and PingAccess application templates based on these clients, connections, and applications by using the template wizard, by saving them as templates, or by adding them directly to PingCentral.



- In PingCentral, application owners manage the applications assigned to them and use your templates to apply OAuth, OIDC, SAML SP, and PingAccess security configurations to them. A wizard guides them through the process of providing a name and description for each application they create, as

well as environment-specific information that makes it possible to run the application on the target environment.



To see which PingFederate components are used to authenticate clients and connections in PingCentral, see *OIDC connection orchestration* and *SAML connection orchestration*.

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

System requirements and supported configurations

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

PingFederate:

- PingFederate 10.1.1
- PingFederate 10.1
- PingFederate 10.0
- PingFederate 9.3
- PingFederate 9.2

PingAccess:

- PingAccess 6.1.1
- PingAccess 6.1
- PingAccess 5.3.2

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

Docker:

- Version: Docker 18.09.0
- Host operating system: Ubuntu 18.04 LTS
- Kernel: 4.4.0-1052-aws 7.3

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

Supported configurations

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

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

- *General configurations*

- *OAuth and OIDC configurations*
- *SAML configurations*
- *PingAccess configurations*

General configurations

Configuration	Supported	Unsupported
Single sign-on and user management	▪ Directly managing users, which are stored in PingCentral embedded database. ▪ Signing on with SSO using an OIDC token. ▪ Beta feature: Provisioning users from an external store using API calls.	
Entitlements	▪ Assigning one or more application owners that have already been provisioned. ▪ Editing and promoting entitlements for an application.	Assigning groups of users entitlements based on an external attribute, such as LDAP group membership.
Backup and restoration	Saving the database and configuration files by copying the directories `h2-data/` and `config/` to a new instance. **Note:** To ensure these files contain the most up-to-date information, do not copy them while PingCentral is running.	Using an API to export PingCentral configuration information.

OAuth and OIDC configurations

Configuration	Supported	Unsupported
Client authentication	Using the client secret method or nothing at all. 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.	

Configuration	Supported	Unsupported
ATMs and OIDC policies	Saving ATMs or OIDC policies into templates created from client applications that have them. ⓘ **Note:** If ATMs or OIDC policies do not exist in an environment, PingCentral will create them during the promotion process. If an ATM or OIDC policy of the same name already exists in a target environment, it will not be modified.	Saving or promoting access token mapping, persistent grants, policy contracts, or authentication policies.
Selectors		Connection set selectors. Clients can only be automatically connected to authentication policies 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	▪ IdP-initiated SSO ▪ SP-initiated SSO ▪ IdP-initiated SLO ▪ SP-initiated SLO	
Attribute mapping	Mapping attributes, provided by a single authentication policy contract, in an unspecified format. You can also map attributes to static text.	▪ Mapping attributes from data sources, such as basic or URI. ▪ Using OGNL expressions as part of attribute mapping.

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

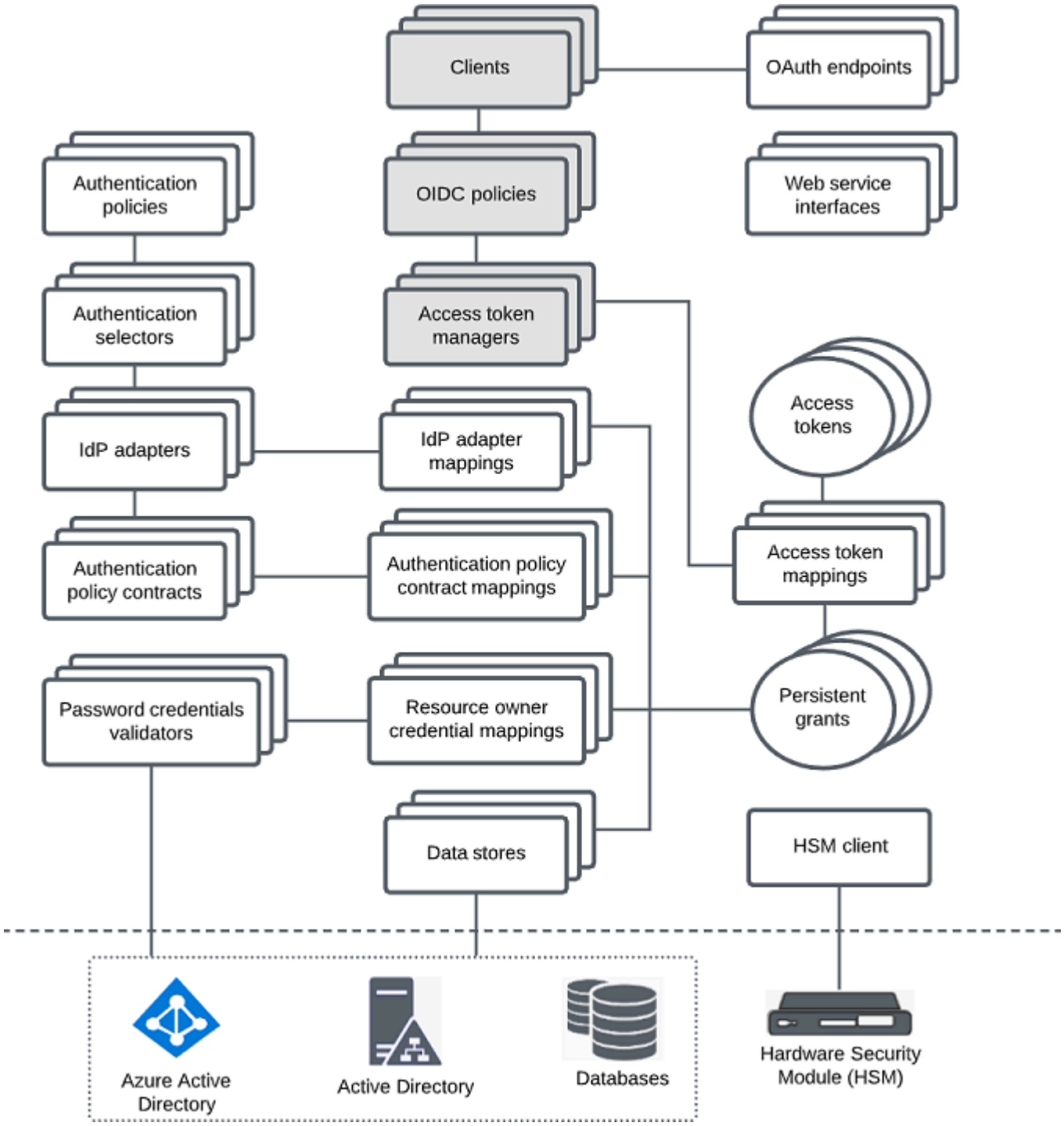
PingAccess configurations

Configuration	Supported	Unsupported
Destination	Both Agent and Site are supported.	The destination is not promoted with the application but selected per environment.
PingAccess application types	All application types (Web, API and Web+API) are supported.	The application type cannot be changed in PingCentral.
Token provider	PingFederate must be the token provider.	Third-party token providers for PingAccess are not supported.
Application resources	Resources can be added and updated for each application.	
Resource ordering	Automated and manual resource ordering are both supported.	
Identity mappings	Identity mappings for all application types (Web, API and Web+API) are supported.	Identity mappings are not promoted with the application but selected per environment.

Configuration	Supported	Unsupported
Virtual hosts	Virtual hosts are supported.	Virtual hosts are not promoted with the application bu selected per environment.
Policy	Application and resource policies can be updated per application.	New rules and rule sets cannot be created in PingCental.

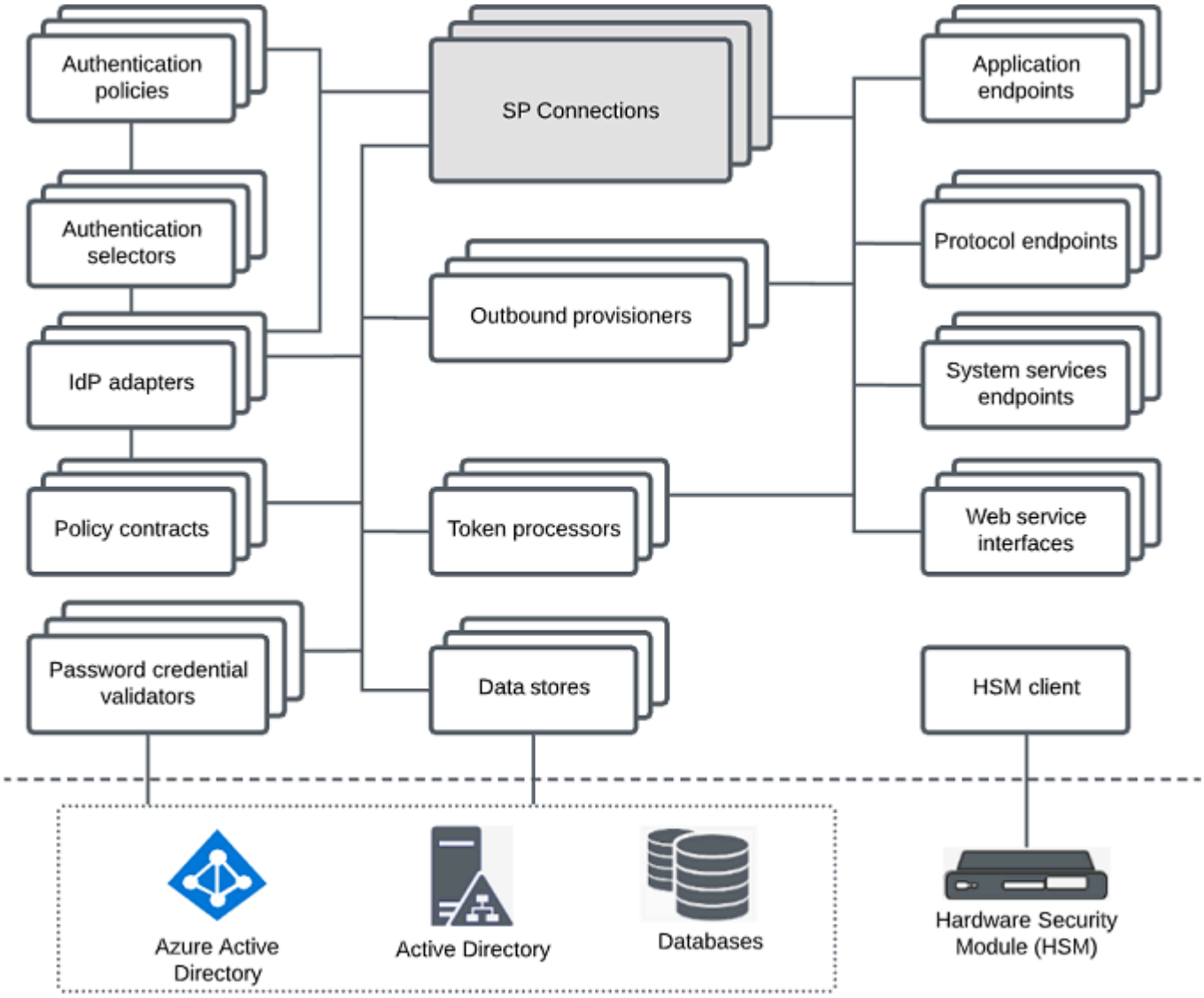
OIDC connection orchestration
This diagram shows which PingFederate components are used to authenticate an OIDC client. PingCentral currently only orchestrates clients, OIDC policies, and access token managers, which are shaded in the diagram.

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.

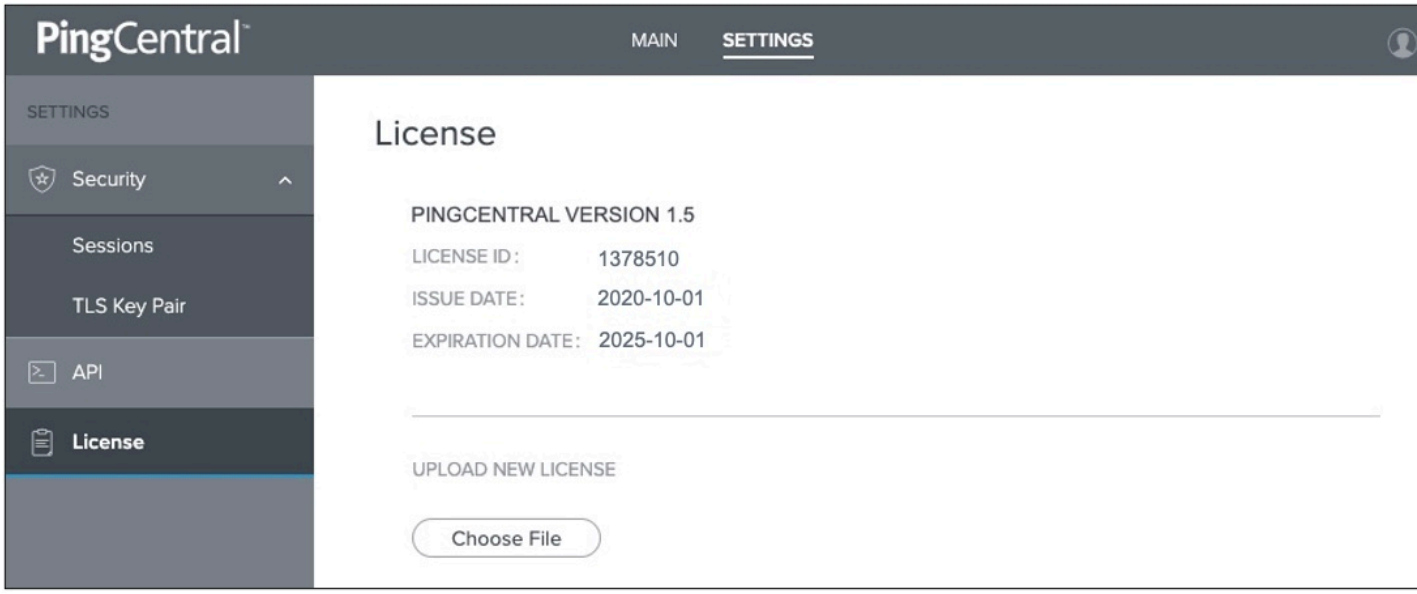


PingCentral licensing

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.

Using Docker to deploy PingCentral

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

Before you begin

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

- *Docker CE for Windows* or *Docker for macOS*
- *Docker Compose*
- *Git*

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

Steps

1. When you are ready, deploy PingCentral:
   - *Register for the DevOps program* to obtain a DevOps user name and key. Then, use the user name and key to start a container. For instructions, see *Using your DevOps user and key*.
   - Use an existing product license. For instructions, see *Using an existing product license*.
2. Set up your DevOps environment.

   For instructions, see *Getting started* on the PingIdentity devops site.
3. Deploy the stack and configure trust and SSO for PingCentral.

   For instructions, see *Deploy PingCentral*.

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 Linux systems*
- *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 Linux systems

To install PingCentral, download the latest version of the software 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 or OpenJDK Java 11 LTS runtime environment is installed.
- The `JAVA_HOME` path points to the JDK software on your system. For example, `/usr/lib/jvm/java-11-openjdk-11.0.5.10-0.e17_7.x86_64`. To verify this information, run the **`echo $JAVA_HOME`** command.
- The `$JAVA_HOME/bin` directory path is added to the *PATH* variable. To verify this information, run the **`echo $PATH`** command.

Steps

1. Download the latest version of PingCentral from the Ping Identity *website*.
2. Extract the file into the appropriate target installation directory.
3. Start PingCentral by running `/<pingcentral_install>/bin/run.sh`.
4. When the installation is complete, open a browser window and enter the machine and PingCentral admin port in the URL field. For example, `https://yourhost:9022`.
5. Log in to the application using the following credentials:
   - **Username**: Administrator
   - **Password**: 2Federate
6. Configure PingCentral to run as a Linux systemv service or a Linux systemd service, as appropriate. Refer to *Configuring PingCentral to run as a Linux systemv service* or *Configuring PingCentral to run as a Linux systemd service*.

> ⓘ **Note:** 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.

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 intallation 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 systemv service

Run PingCentral as a Linux systemv 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 systemv service

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

You can upgrade from PingCentral 1.2, 1.3, or 1.4 directly to 1.5. To begin the upgrade, download and extract the contents of the 1.5.0 distribution 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, see *Upgrading to PingCentral 1.5.0*.

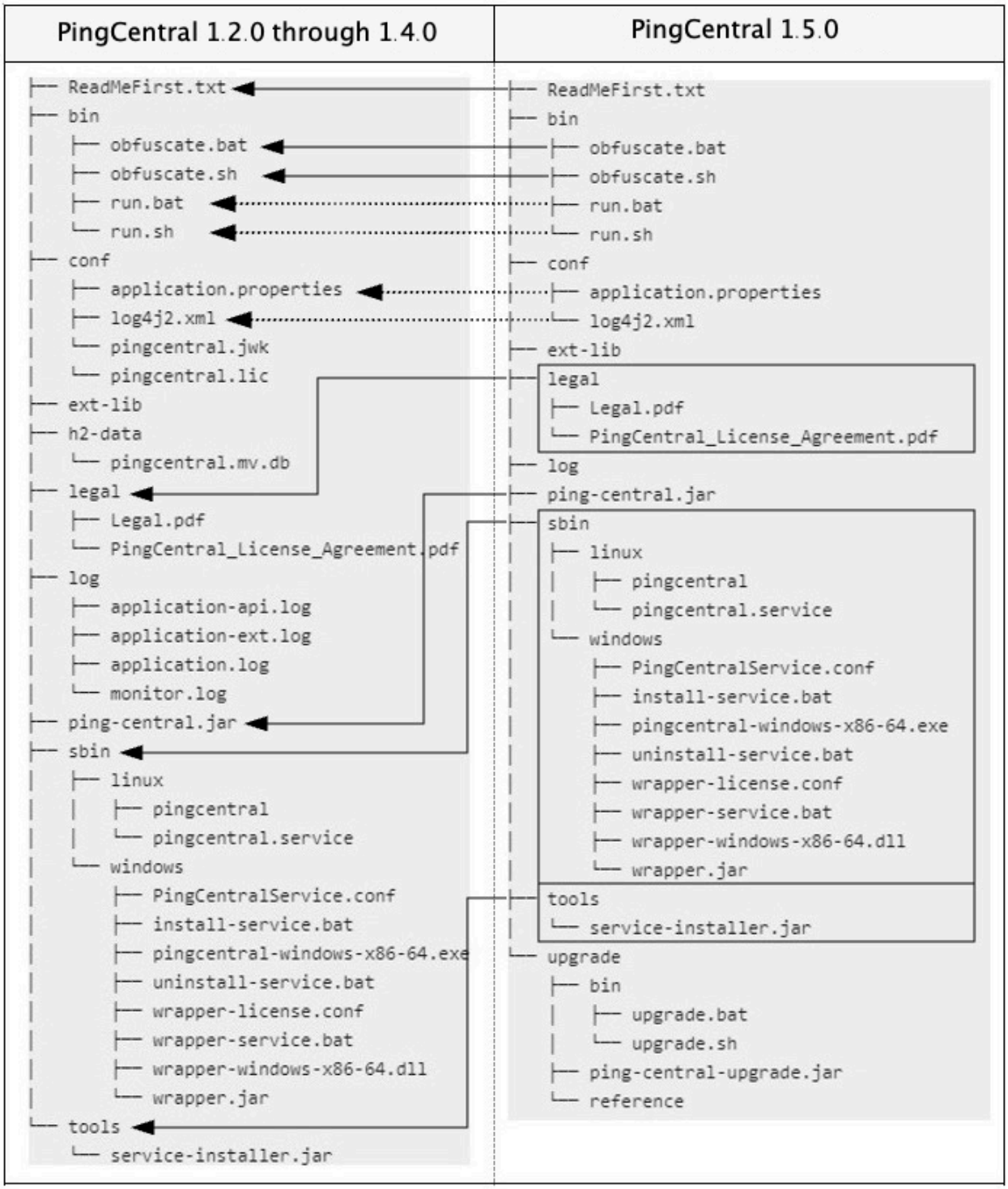
How the upgrade works

The upgrade utility uses the extracted contents of the `ping-central-1.5.0.zip` file to copy and replace the appropriate information in the existing version installation location.

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

- The database files (`h2-data` directory), the log files (`log` directory), the external library files (`ext-lib` directory), and the host key file (`conf/pingcentral.jwk`) remain intact during the upgrade process to preserve user data.
- If the `application.properties` file was modified, the current version of the file will be merged with the latest version, preserving customizations.
- If the `conf/log4j2.xml`, `bin/run.sh`, and `bin.run.bat` files were modified, the new versions are installed and the old versions are renamed. Manually update the new files with customizations, as necessary.

The following image shows PingCentral 1.5.0 after it has been run and the database files that have been generated. It also shows which files are replaced with new files during the upgrade process.



Upgrading to PingCentral 1.5.0

To upgrade PingCentral from 1.2.0, 1.3.0, or 1.4.0 to 1.5.0 on either Windows or Linux, download the 1.5.0 installation file, run the PingCentral upgrade utility, and plan for a short period of downtime.

Before you begin

Ensure that:

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

Steps

1. Download the `ping-central-1.5.0.zip` file and extract its contents.

   You can delete this file after the upgrade is complete.
2. If PingCentral is running, shut it down.

   This maintains the integrity of the H2 database file and ensures that you are running 1.5.0 as you complete the installation.
3. Make a copy of the existing PingCentral version product directory so that the older version can be restored if the upgrade process fails.

   If PingCentral has been configured to use an external database, such as MySQL, or PostgreSQL, make a copy of that database so that it can be restored if the upgrade process fails.
4. Go to the *<pingcentral_1.5.0_install>*`/upgrade` directory and run the appropriate file:

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

   The upgrade process begins. The upgrade utility uses the extracted contents of the `ping-central-1.5.0.zip` file to copy and replace the appropriate information in the existing version location.

> ⓘ **Note:**
>
> When the upgrade is complete for this release, PingCentral 1.5.0 will run from the directory in which PingCentral was initially installed. For example, if PingCentral 1.2.0 was initially installed and you upgraded to 1.3.0, and now to 1.5.0, PingCentral 1.5.0 will run from the original 1.2.0 directory. The same is true if you upgraded directly from 1.2.0 to 1.5.0.

5. Optional: To update the license file (`conf/pingcentral.lic`), add `--license=<file>` at the end of the upgrade command and specify the path to the new license.
   As the upgrade continues, a message displays that reminds you to shut down PingCentral if you have not already done so.
6. To continue, type `yes`.
   A message displays that reminds you to back up your PingCentral program files.

7. To continue, type `yes`.
   The upgrade continues and the system displays a message when the upgrade is complete.

   ⓘ **Note:**

   If PingCentral was installed as a service by one user, and the upgrade is performed by another user, the service will no longer start. To resolve this issue, run the following command to update the installation files to match the existing ownership:

   ```
   chown -R [user]:[group] [INSTALL_DIR]
   ```

   Where the user and group match the existing installation:

   ```
   chown -R pingcentral:pingcentral /usr/local/pingcentral-1-1.3.0/
   ```

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

   ⓘ **Note:**

   Other than the `application.properties` file, which is merged automatically, you must manually merge customizations you consider important. These customizations might include changes you made to the `conf/log4j2.xml` file, or changes you made to a file in the `/bin` directory.

9. Start PingCentral 1.5.0.

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

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

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

11. Upon successful upgrade, delete the 1.5.0 distribution `.zip` file and the directory into which it was extracted.

Configuring logging

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

Steps

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

   The level of detail that the log file contains depends on how the logging level is set. Logging levels are a means of categorizing the entries in your log file by severity, and are described in the following table.

Detailed log files require more system resources, so PingCentral only records errors, warnings, and some information events by default.

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

2. Changing the logging level to have the system record additional details can help with troubleshooting. To change the logging level:
   a. Open the configuration file at `/<pingcentral_install>/conf/log4j2.xml`.
   b. Scroll down, locate the Logger line item shown below, and change the logging level within the quotations. The `DEBUG` logging level provides enough information to troubleshoot most issues.

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

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

Replacing the Admin Console SSL Certificate

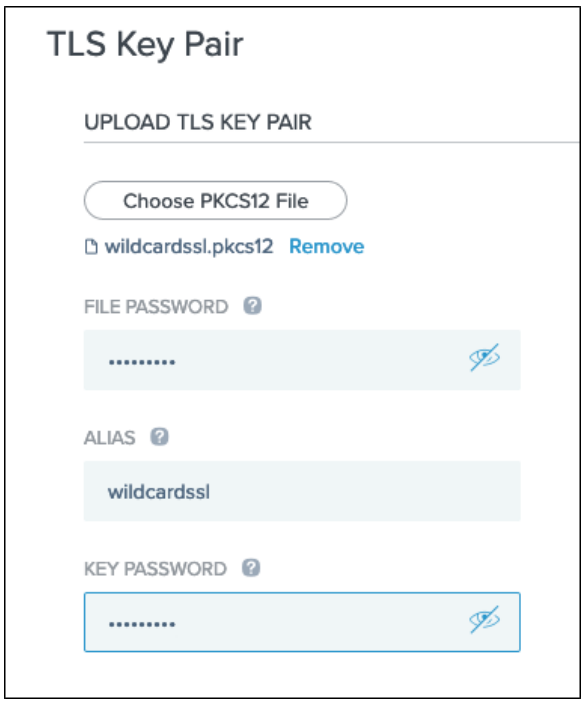
To avoid seeing a certificate warning when you access PingCentral, replace the user-facing SSL certificate so it will no longer use the self-signed certificate.

About this task
Import your proprietary certificate into PingCentral by uploading the PKCS12 file that contains it.

Steps

1. Select the **Setting** tab..
2. Expand the **Security** menu and select **TLS Key Pair**.
3. Click **Choose PKCS12 File** and select the `.p12` file to upload it.
4. In the **File Password** field, enter the password to the keystore file.

5. In the **Alias** field, specify the alias of the certificate in the keystore file that you want to use for the Admin Console SSL Certificate, if required.
   - If the `.p12` file being imported for TLS key pair contains a single alias, PingCentral accepts the file without requiring an alias.
   - If the `.p12` file being imported for TLS key pair contains multiple aliases, PingCentral requires the alias.
6. In the **Key Password** field, enter the password for the selected certificate if the PKCS12 file requires a separate password for the key.



7. Click **Save**.
8. Restart PingCentral.
   After PingCentral restarts, you will be able to access PingCentral without receiving a certificate warning.

Environment management

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

For more information, see the following:

- *Adding environments*
- *Configuring PingFederate as a PingAccess token provider*
- *Updating environments*
- *Deleting environments*

Adding environments

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

Steps

1. On the **Environments** page, click **Add Environment**.

2. On the **Connect to Instances** page, connect to a PingFederate environment:

   a. Complete the **PingFederate Admin**, **PingFederate Admin Username**, and **PingFederate Admin Password** fields with your authentication information.

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

   b. 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** check box.

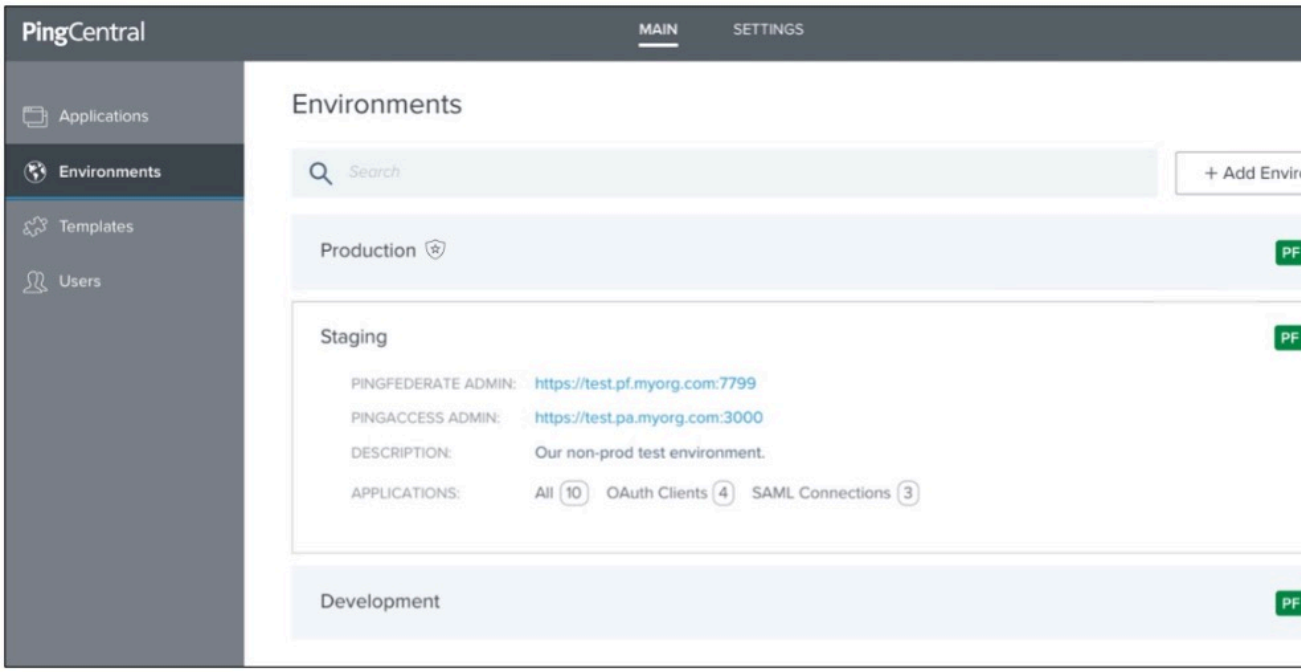
   e. Click **Save and Continue**.

   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. A **PF** icon also displays. The color of this icon represents the status of the environment. A green **PF** icon indicates that the environment is verified, while a red **PF** icon indicates that the environment is not verified.

   g. 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.

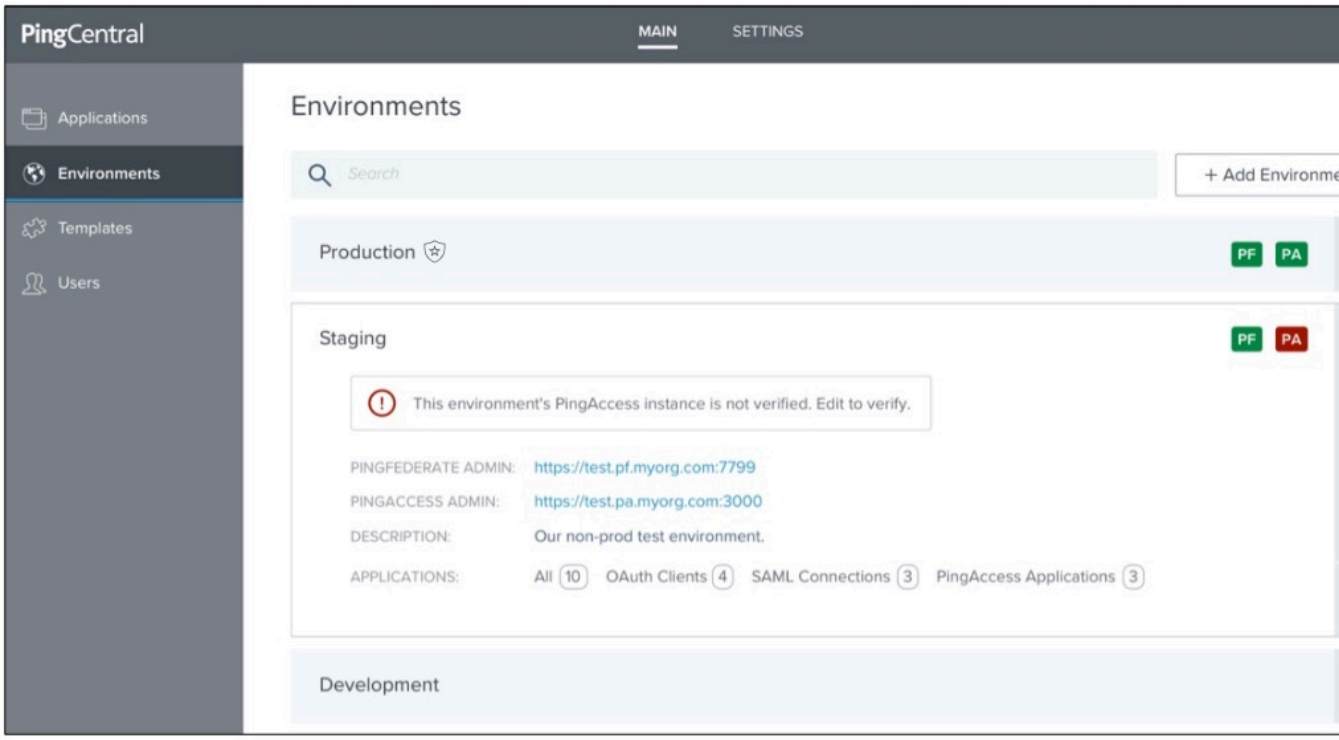


3. To add a PingAccess environment instance to PingCentral, access the **Connect to Instances** page by either clicking on **Add Environment**, or by clicking the **Pencil** icon for an existing PingFederate application.

   a. Complete the **PingAccess Admin**, **PingAccess Admin Username**, and **PingAccess Admin Password** fields with your authentication information.

      If this is the first time you have set up this PingAccess environment, and you set it up correctly, you will not see a **Skip Verification** option. However, if the initial validation fails, this option displays. If selected, it allows you to skip the validation process.
   b. 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** check box.
   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. A **PA** icon also displays. The color of this icon represents the

status of the environment. A green **PA** icon indicates that the environment is verified, while a red **PA** icon indicates that the environment is not verified, as shown in the following example.



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

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

> ⓘ **Note:** If an environment is unavailable, applications in that environment do not display on the **Applications** page.

h. If the environment is not verified, you will receive an error message. Ensure that PingFederate is configured as a token provider for PingAcess. For more information, see *Configuring PingFederate as a PingAccess token provider*.

Configuring PingFederate as a PingAccess token provider

To add PingAccess environments to PingCentral, PingFederate must be configured as the token provider. If you have PingFederate and PingAccess environments established, this configuration is likely in place. So if you set up a new environment or change the token provider settings, be aware of this requirement and ensure PingFederate and PingAccess are configured correctly.

About this task

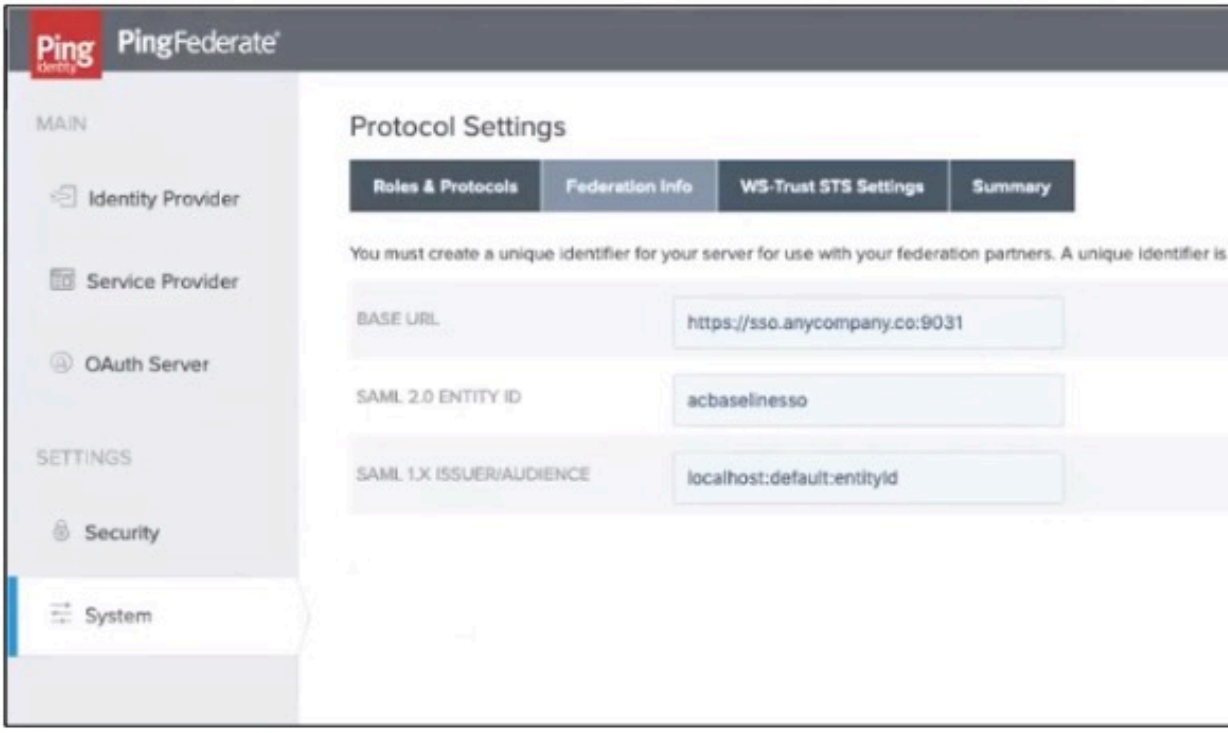
To configure PingFederate as the token provider for PingAccess, the Issuer URL in PingAccess must either match the Base URL in PingFederate, or one of the virtual hosts defined in PingFederate.

Steps

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

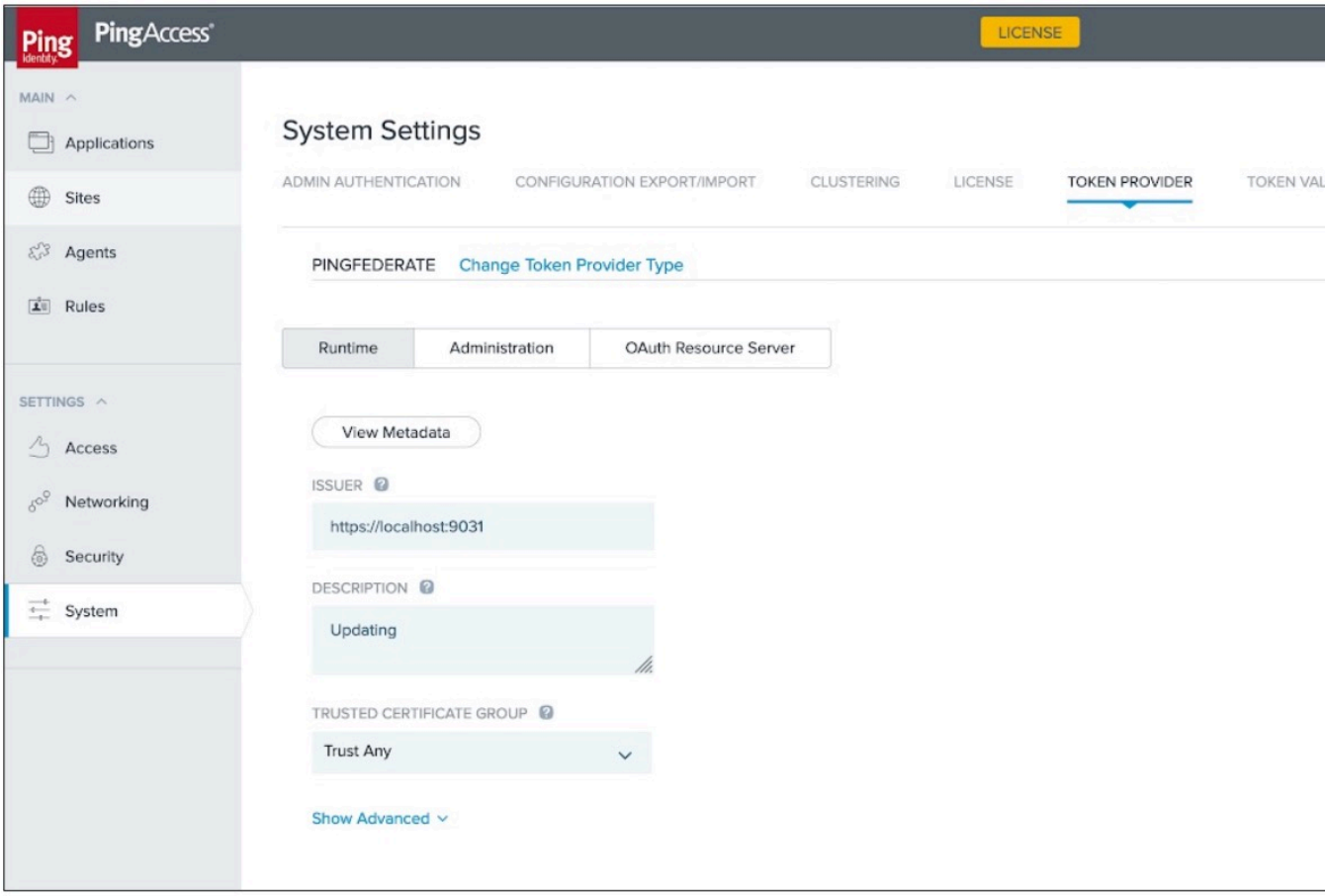
   If a virtual host is defined in PingFederate, continue to step 3.

2. To locate this information:
   - In PingFederate, to locate the **Base URL** field, go to **System**# **Protocol Settings**# **Federation Info**, as shown in the following example.

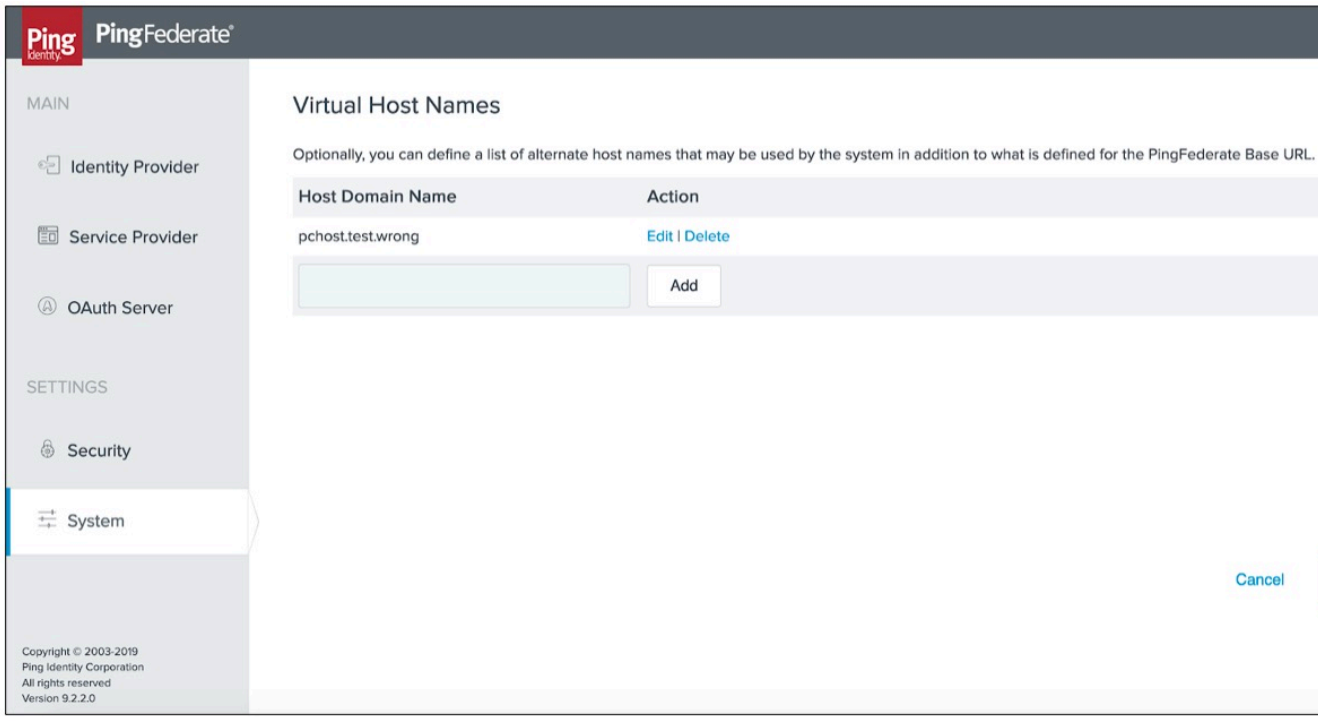


   - In PingAccess, to locate the **Issuer URL**field, go to **System**# **Token Provider**.

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



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



Updating environments

Update PingFederate and PingAccess environment information at any time.

Steps

1. To edit environment information, click the expandable icon associated with it, and then click the **Pencil** icon.
   All of the editable information displays on one page.
2. On the edit page:
   - To update the name and description, change the information in the **Name**, **Short Code**, and **Description** fields and click **Save**.
   - To update the connection information for either a PingFederate or PingAccess environment, change the information in the **Username** and **Password** fields and click **Save**.

     ⓘ **Note:**

     If a PingAccess environment is added to PingCentral and removed through the edit page, the connection information is saved and restored if the PingAccess environment is selected again.
   - To add or remove the protected status of an environment, which prevents non-administrators from promoting applications to the environment, select or clear the **Only Administrators Can Promote Applications** check box and click **Save**.
   - To update the identity provider certificate used to promote SAML applications, click **Choose** to upload a new certificate and enter the certificate password in the appropriate field. Click **Save**.

Deleting environments

Delete environments from PingCentral when they are no longer needed.

Steps

1. Click the expandable icon associated with the environment to view environment details.
2. To delete the environment from PingCentral, click its associated **Delete** icon.
   A message displays asking you if you want to delete the environment.
3. Click **Delete**.
   A message displays saying that the environment was deleted.

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 for PingCentral*
- *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 OIDC 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 signed JWT tokens are supported in this release, so a JWKS endpoint is required to obtain the public keys for signature validation.

If you are using PingFederate 10.1 or later, you can enable the centralized signing key functionality. Additional configuration is not required in PingCentral to access the centralized JWKS endpoint. However, if the access token manager has been configured with an explicit JWKS endpoint path, this must also be specified to PingCentral.

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

To provide this endpoint to PingCentral, access the `application.properties` file, which resides in the `conf` folder in the PingCentral installation directory. Uncomment the 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
```

PingCentral can be configured to validate the access token issuer and audience claim values defined in the access token manager. By default, these claims will not be validated. Validation for either or both is enabled by setting the following properties:

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

Ensure that the values specified match those defined in the access token manager. If they do not match, the validation will fail.

ⓘ **Note:** If a blank value is defined in PingFederate, the claim will not be present in the token, so the validation of that claim must not be enabled in PingCentral.

Configuring the OpenID provider

PingCentral has been tested with PingFederate 9.2.x, 9.3.x, 10.0.x and 10.1.x, serving as both the OpenID provider and OAuth 2 authorization server. PingCentral is an OpenID relying party for browser based SSO, as well as an OAuth 2 resource server when directly accessing the admin API.

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 all of the details of setting up access token managers, OIDC policies, or attribute contracts as these topics are complex and often specific to a customer 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 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.

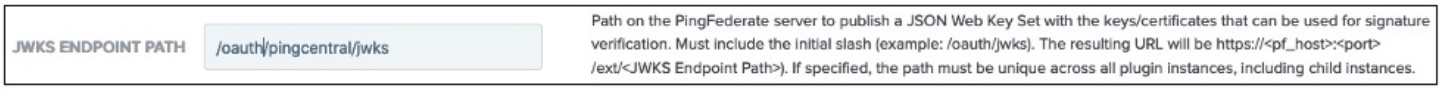
If the default PingCentral role claim name and values need to be altered to match the OIDC policy, update the `application.properties` file. Refer to *Configuring SSO* for details.

Configuring the Access Token Manager

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

If you are using PingFederate 10.1 or later, you can enable the centralized signing key functionality. Additional configuration is not required in PingCentral to access the centralized JWKS endpoint. Select the **Use Centralized Signing Key** check box, as shown in the following example.

Alternatively, or if you are using an older version of PingFederate, you must define an explicit JWKS endpoint path. Select **Show Advanced Fields** and specify the path in the **JWKS Endpoint Path** field, as shown in the following example:



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

If you define either or both of the issuer or audience claim values within the access token manager, you can configure PingCentral to validate them. These claim values are also defined within the advanced fields, as shown in the following example.

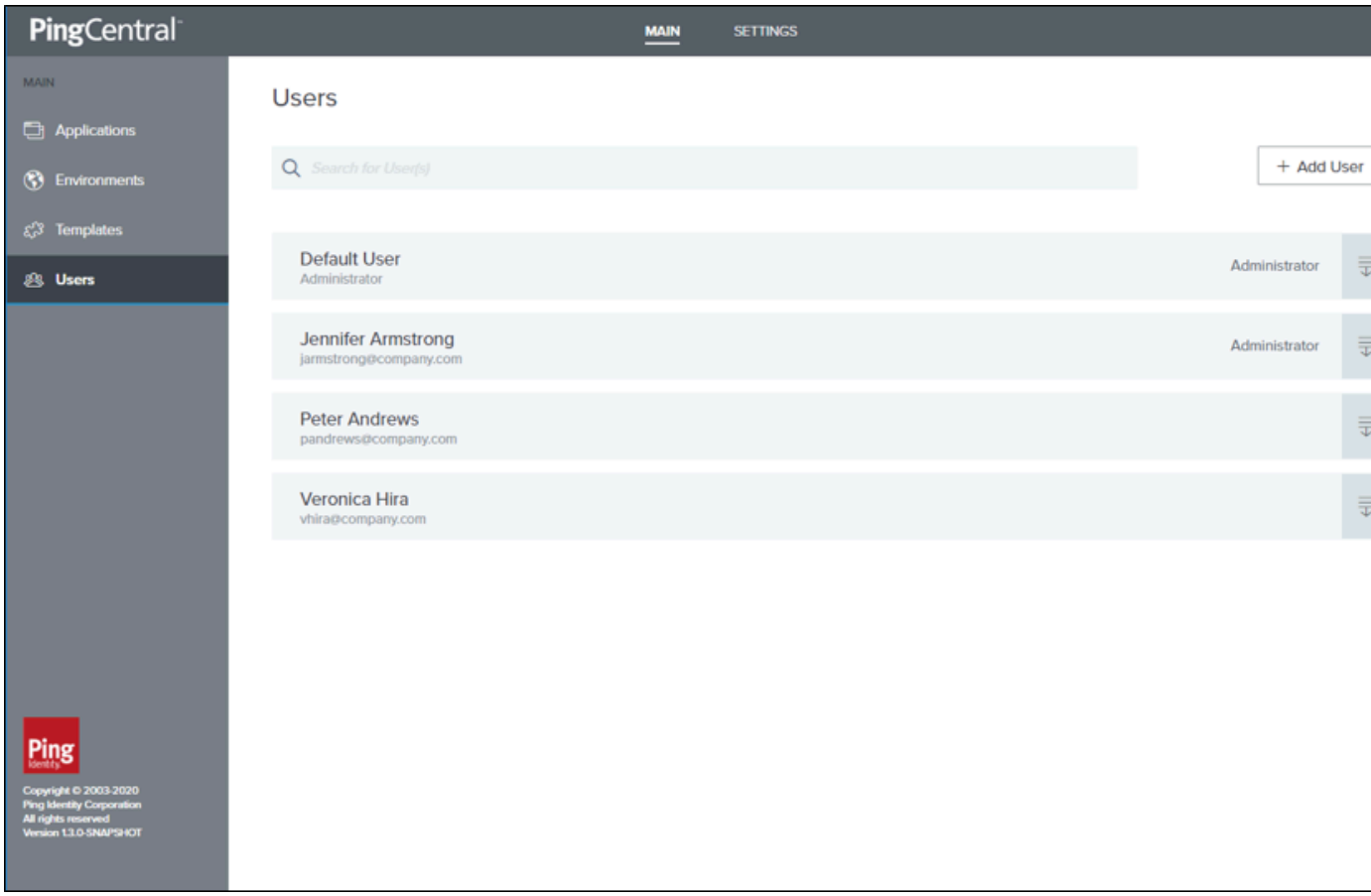
Managing users through PingCentral

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.

Application management

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

For more information, see the following topics:

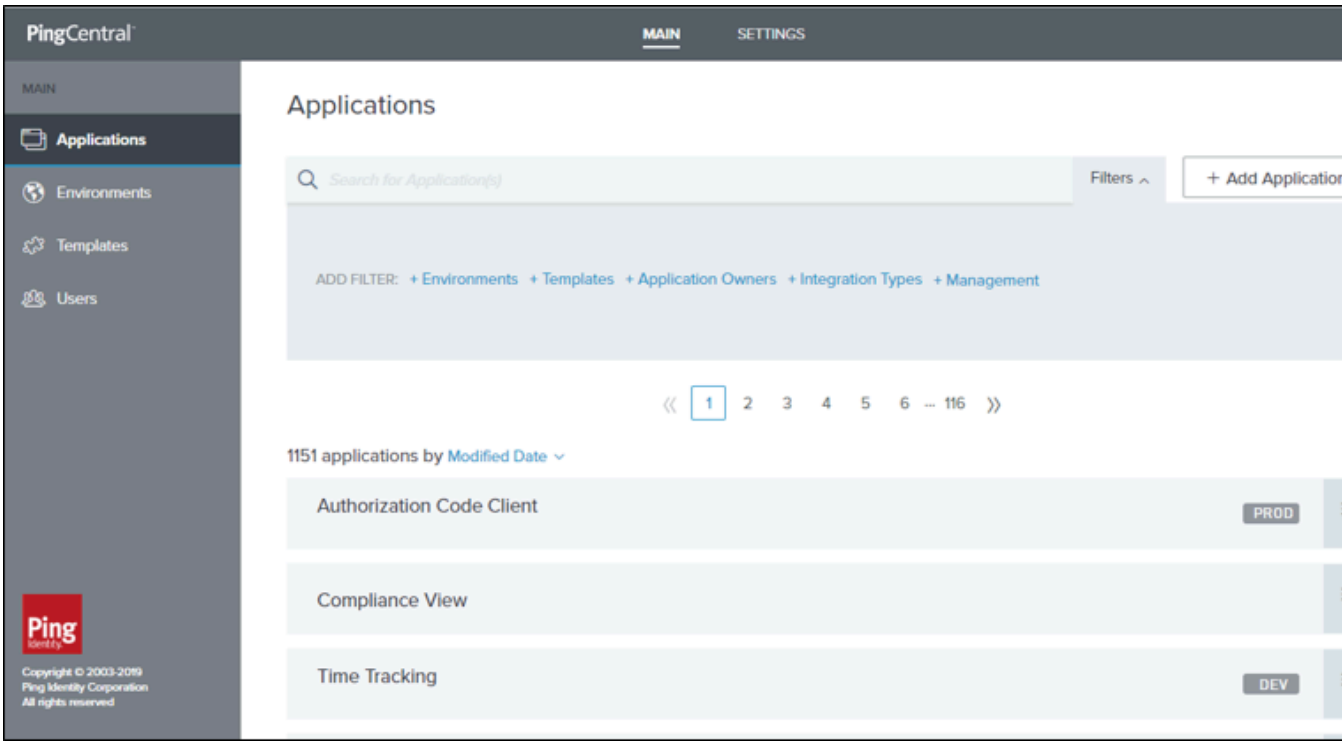
- *Filtering applications*
- *Adding applications to PingCentral*
- *Updating applications*
- *Deleting applications*

Filtering applications

Use the filters at the top of the page to filter your list of applications and the search box to locate specific applications.

Steps

1. Select your filters. 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 verified PingAccess or PingFederate environments.)



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

Adding applications to PingCentral

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

Steps

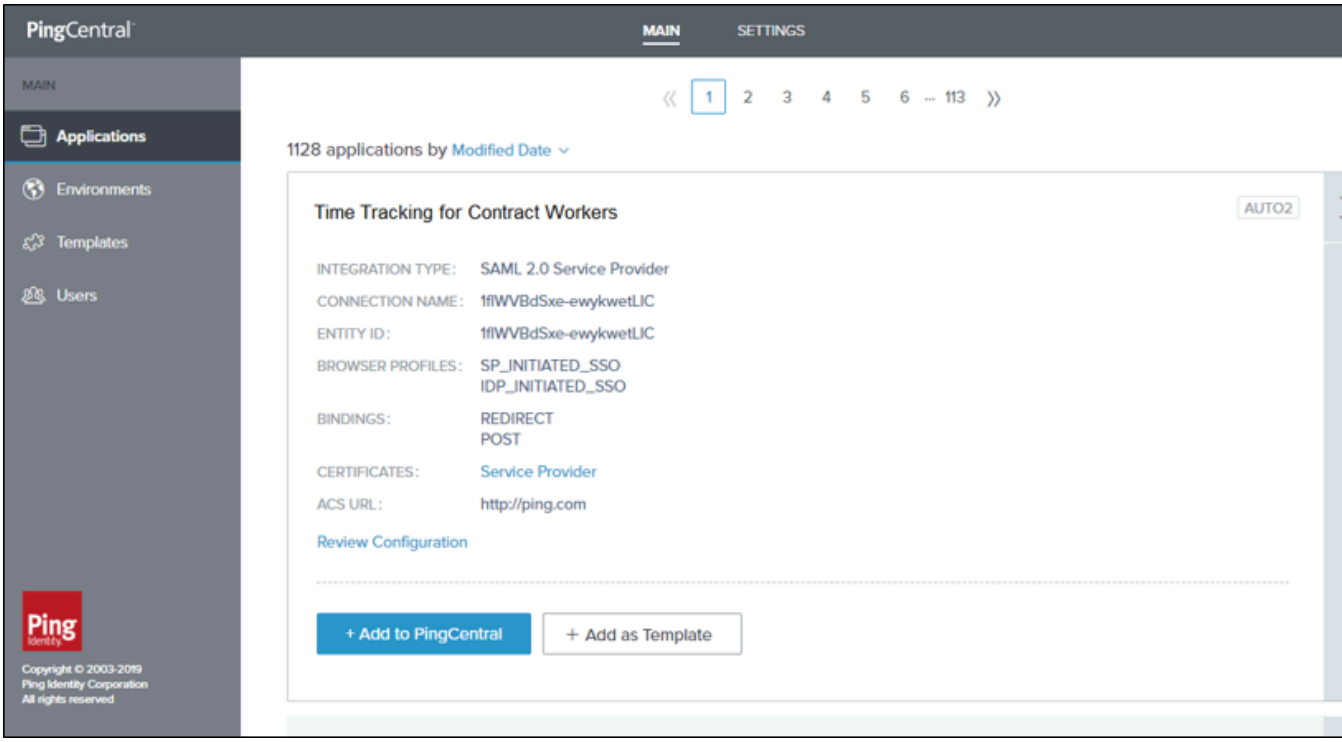
1. To apply an OAuth, OIDC, SAML, or PingAccess template to an application:
   a. Click **Add Application**.
   b. On the **Select Template** page, select the appropriate template and follow the wizard prompts.

      See *Selecting a template* in the*PingCentral for Application Owners* guide for additional information.

2. To create a template from an unmanaged application:
   a. Select the expandable icon associated with the application.
   b. Click **Add as Template** and follow the wizard prompts.

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

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



Updating applications

Update applications at any time.

About this task

To keep your applications secure, rotate certificates and client secrets on a regular basis and apply updated security configurations to applications built from templates if new configuration templates become available. There is no need to recreate your applications in PingCentral to apply new templates. Replace the templates associated with your applications and promote them again.

Steps

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

   All of the editable information displays on one page.
2. To update the name, description, and owners, change the information in the **Name**, **Description**, and **Owners** fields. Click **Save**.

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

> ⓘ **Note:**
>
> You cannot apply a SAML template to an OAuth or OIDC application, nor apply an OAuth or OIDC template to a SAML application.

4. To update application information:

Application type	Update instructions
OAuth or OIDC	▪ In the **Client** section, change the scopes associated with OAuth or OIDC applications. Select or clear the appropriate check boxes and click **Save**. ⓘ **Note:** You cannot edit scopes for applications created in 1.2.0. However, you can update the template associated with an application to a template created in a later version, which will allow you to update scope information. ▪ In the **Promote** section, change the information in the **Redirect URI** fields for the appropriate environments and click **Save**. ▪ To change client secrets, return to the **Applications** page, promote the application again and generate a new secret.
SAML	▪ In the **Attribute Mappings** section, add or remove attributes or update attribute values and click **Save**. ▪ In the **Promotions** section, upload a new `.xml` file that contains service provider metadata, such as the Entity ID, ACS URL, certificates, and attribute information, from another SAML application. Click **Choose File** or **Or Use URL** to provide the metadata file. ⓘ **Note:** If metadata is used, the attribute mapping section might also need to be updated to include new attributes from the metadata file. ▪ Change the information in the **Entity ID** or **ACS URL** fields and click **Save**. ▪ Change the certificate. Click **SP Certificate** to upload a new certificate, or click **Remove** to remove it. Click **Save**.
PingAccess	▪ On the **Properties** tab, in the **Promote** section, update **Virtual Hosts**, **Access**

Application type	Update instructions
	Validation, **Identity Mapping**, and **Site** or **Agent** names, as appropriate. Click **Save**. ▪ On the **Resources** tab, update resource information and click **Save**. ▪ On the **Policy** tab, click the **Pencil** icon associated with the policy you want to update. Make changes and click **Save**.

Deleting applications

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

About this task

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

Steps

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

Template management

When you create a PingCentral template based on an existing PingFederate or PingAcess application, or add an existing PingFederate or PingCentral 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.

OAuth and OIDC templates

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.

SAML templates

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.

PingAccess templates

For PingAccess applications, the following items are saved:

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

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

- *Creating OAuth and OIDC application templates*
- *Creating SAML SP application templates*
- *Creating PingAccess 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 building block for future applications.

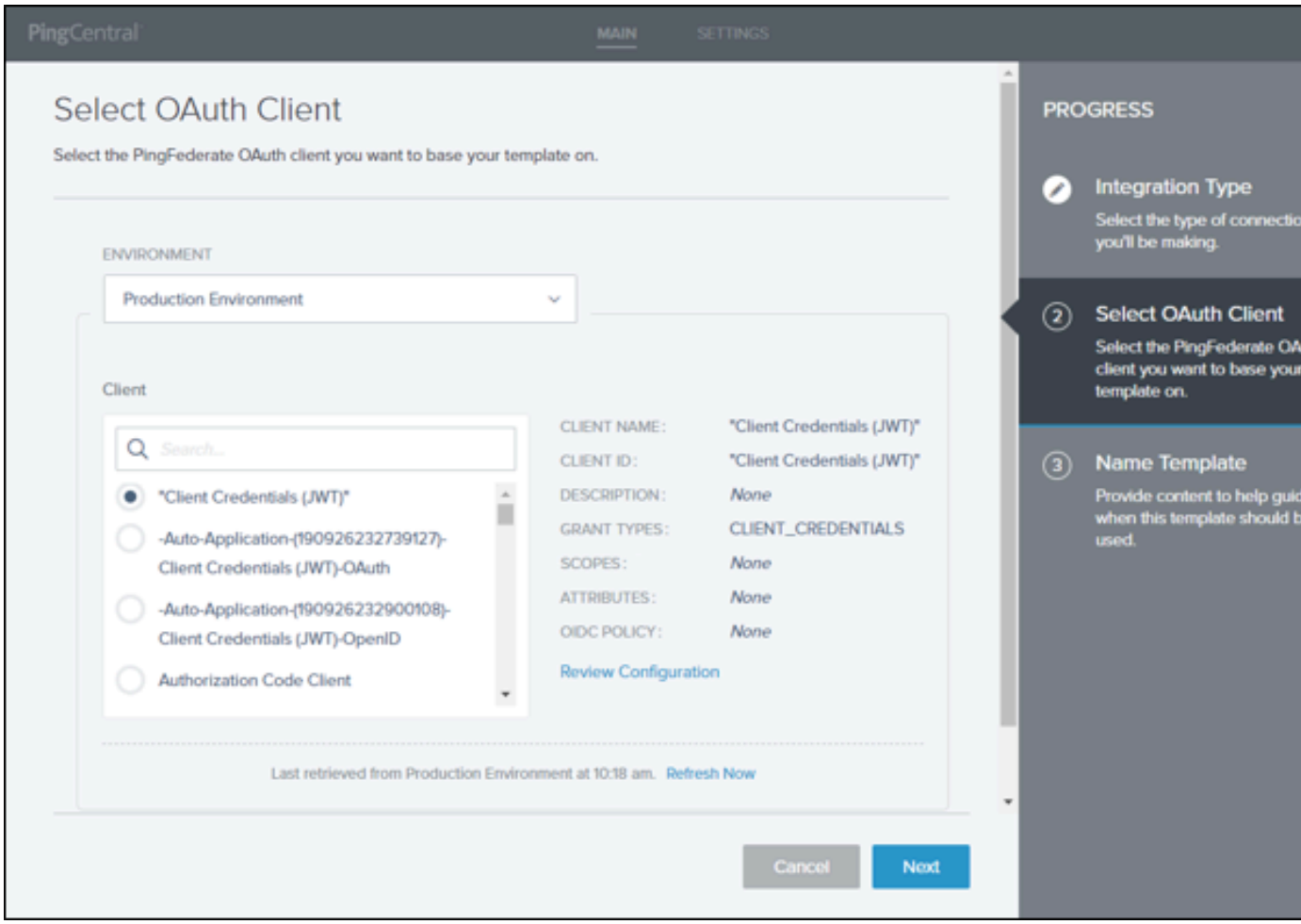
About this task
A good template configuration should include meaningful defaults that will make sense for many different OAuth and OIDC applications.

Steps

1. Select **Templates** to see a list of available templates.
2. Click **Add Template**, select either an OAuth or OpenID Connect template from the Integration Type page and click **Next**.

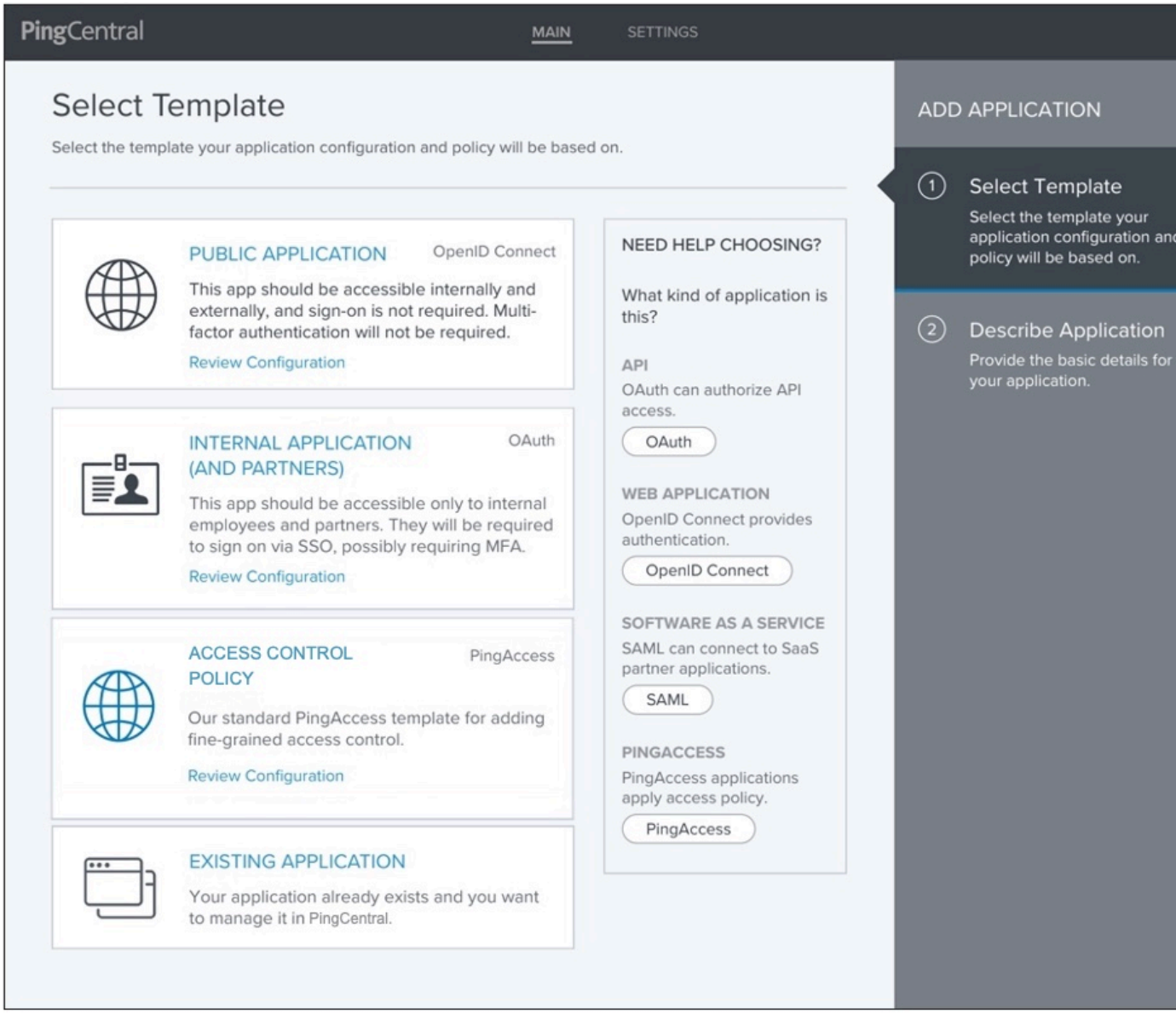
3. On the Select OAuth Client or OIDC Client page, select the PingFederate environment that hosts the client application you want to use as a template, and then select the application itself from the **Client** list.

   Details regarding the selected client display.



4. To see the JSON for the application, click **Review Configuration**.
5. On the **Name Template** page, add a name and description for your template. This information will help application owners select the appropriate template.
6. Select an icon to represent your template. The icon you choose 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.



Creating SAML SP application templates

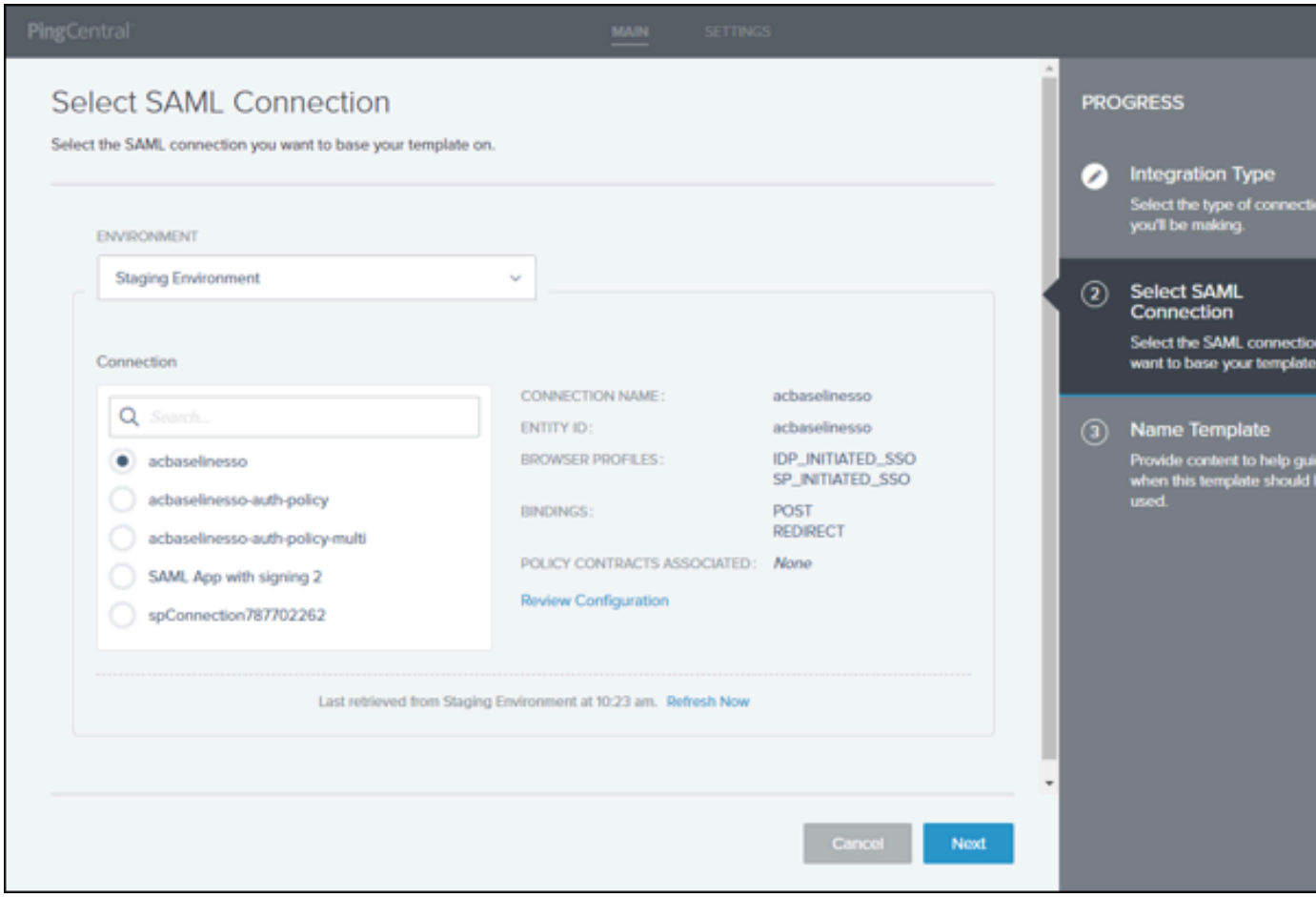
To create a template, select a connection configuration that exists in a PingFederate environment to replicate. PingCentral retrieves this configuration from PingFederate and saves it as a building block for future applications.

About this task
A good template configuration should include meaningful defaults that will make sense for many different SAML applications.

Steps

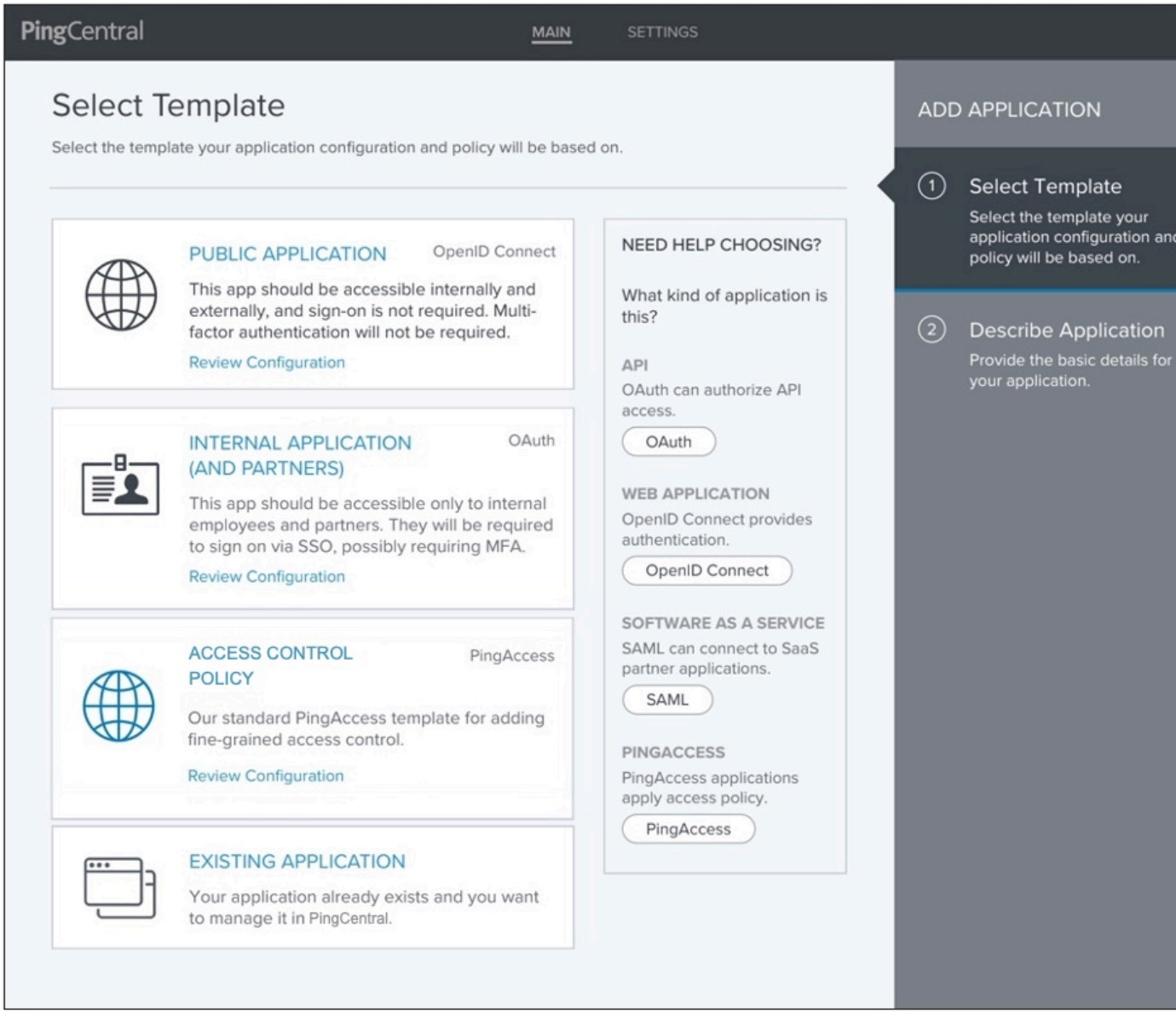
1. Select **Templates** to see a list of available templates.
2. Click **Add Template** and select **SAML** from the Integration Type page. Click **Next**.

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



4. To see the JSON for the SAML connection, click **Review Configuration**.
5. On the Name Template page, add a name and description for your template. This information will help application owners select the appropriate template.
6. Select an icon to represent your template. The icon you choose 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.



Creating PingAccess application templates

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

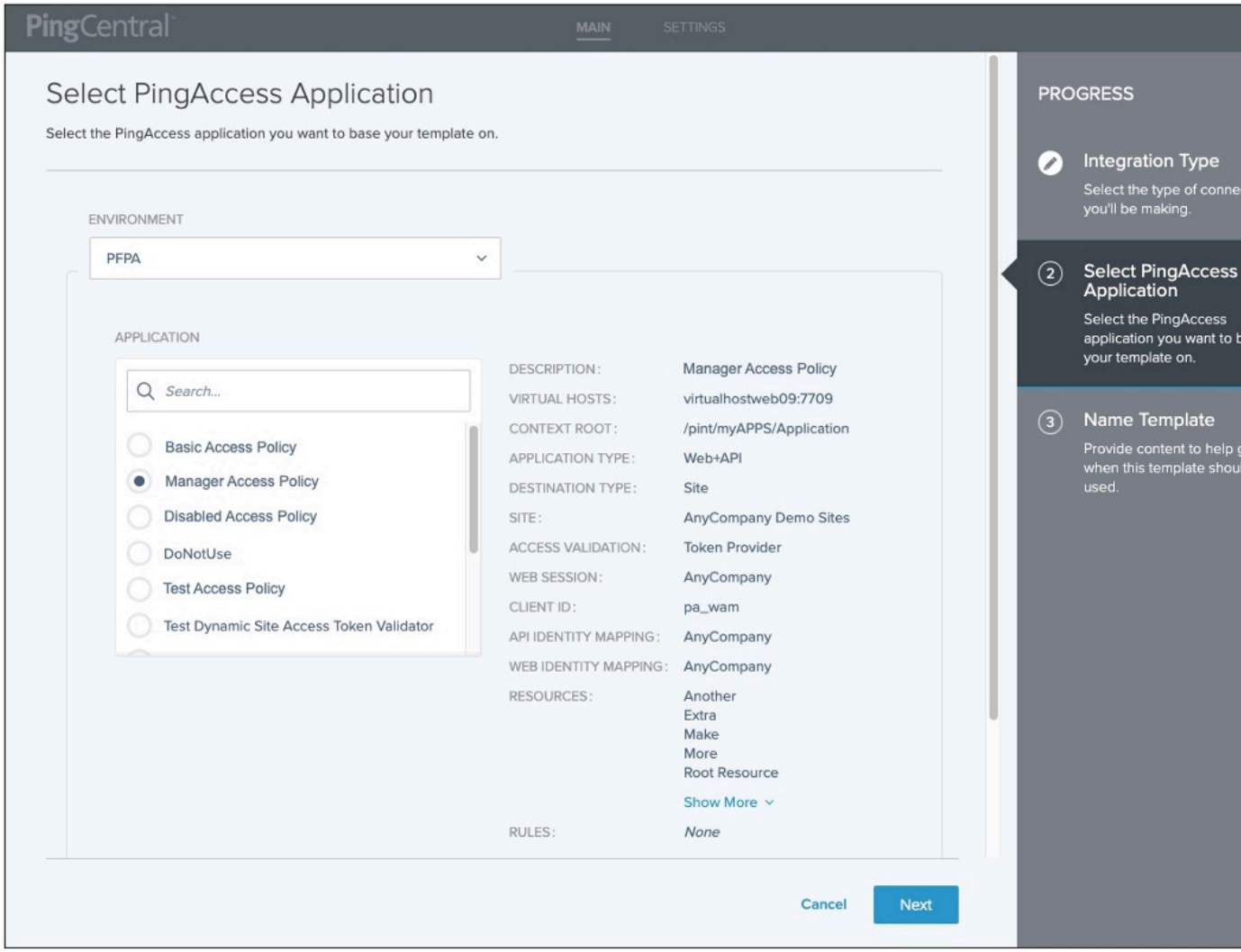
About this task

A good template configuration includes meaningful defaults that make sense for many different PingAccess applications.

Steps

1. To see a list of available templates, select **Templates** .
2. Click **Add Template**.

3. From the **Integration Type** page, select **PingAccess**. Click **Next**.
4. On the **Select PingAccess Application** page, from the **Environment** list, select the PingAccess environment that hosts the application you want to use as a template, and then from the **Application** list, select the application.
   The application details display next to the Application list.

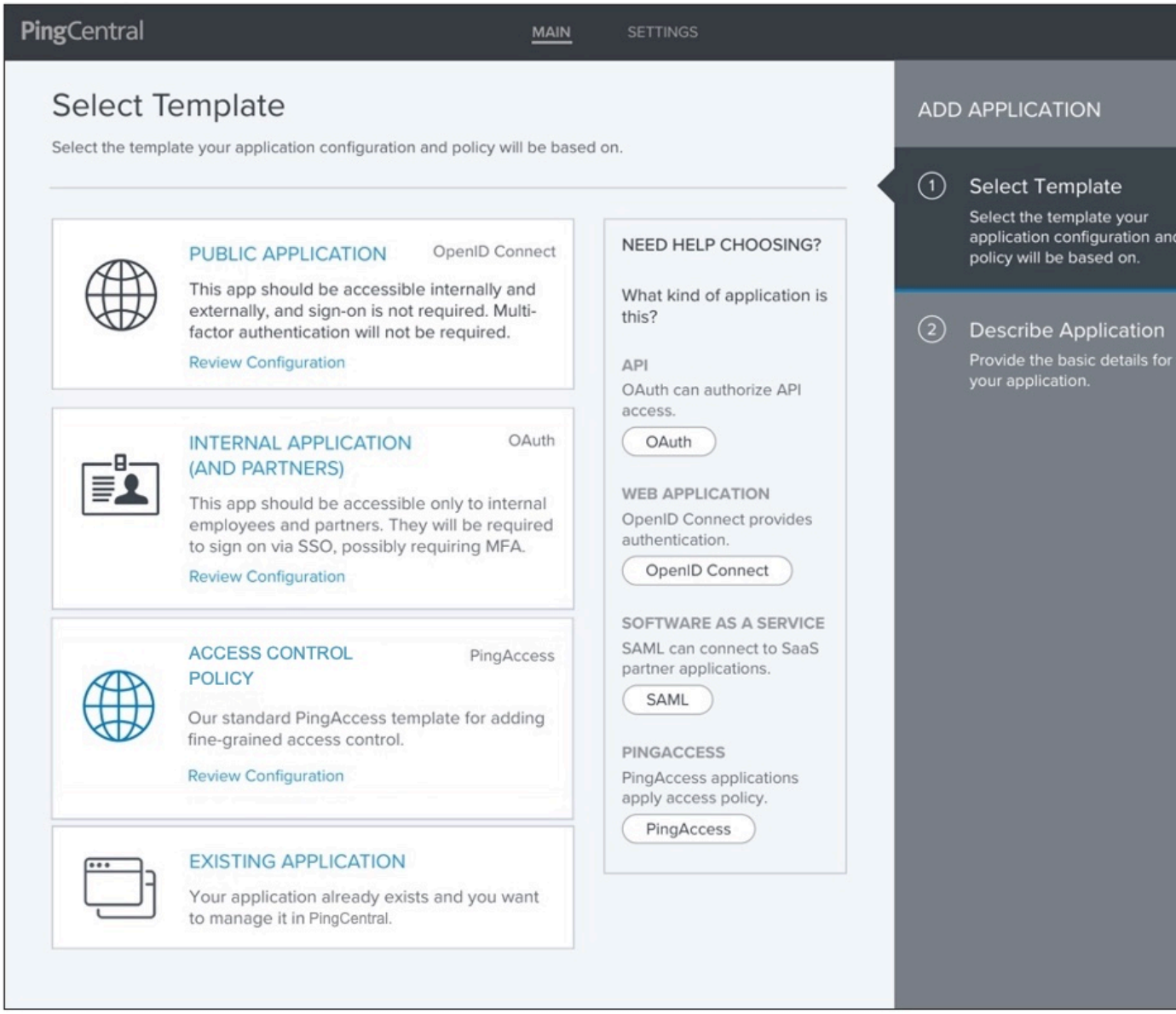


5. To see the JSON for the PingAccess application, click **Review Configuration**.
6. On the **Name Template** page, add a name and description for your template.

   This information helps application owners select the appropriate template.
7. Select an icon to represent your template.

   The icon you choose displays with the template name and description.

8. Click **Save and Close**.
   The new template appears in the list of available application templates. Application owners can see the new template on the **Select Template** page.



Promotion processes

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

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

The templates contain the raw JSON from the model applications on which the templates were based. Although PingCentral saves this information, it 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 or PingAccess. For details, see *Reverting applications to previously promoted versions*.

OAuth and OIDC application promotions

When promoting OAuth and OIDC 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.

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

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

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

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

SAML SP application promotions

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

- **Entity ID**: Uniquely identifies the application.
- **ACS URL**: The application's URL to which SAML assertions from the identity provider is sent after user authentication occur
- **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
- **Assertion encryption certificates**: Used to prove that the SAML assertion is encrypted

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

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

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

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.

PingAccess application promotions

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

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

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

PingCentral for Application Owners

Introduction to PingCentral

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

PingCentral:

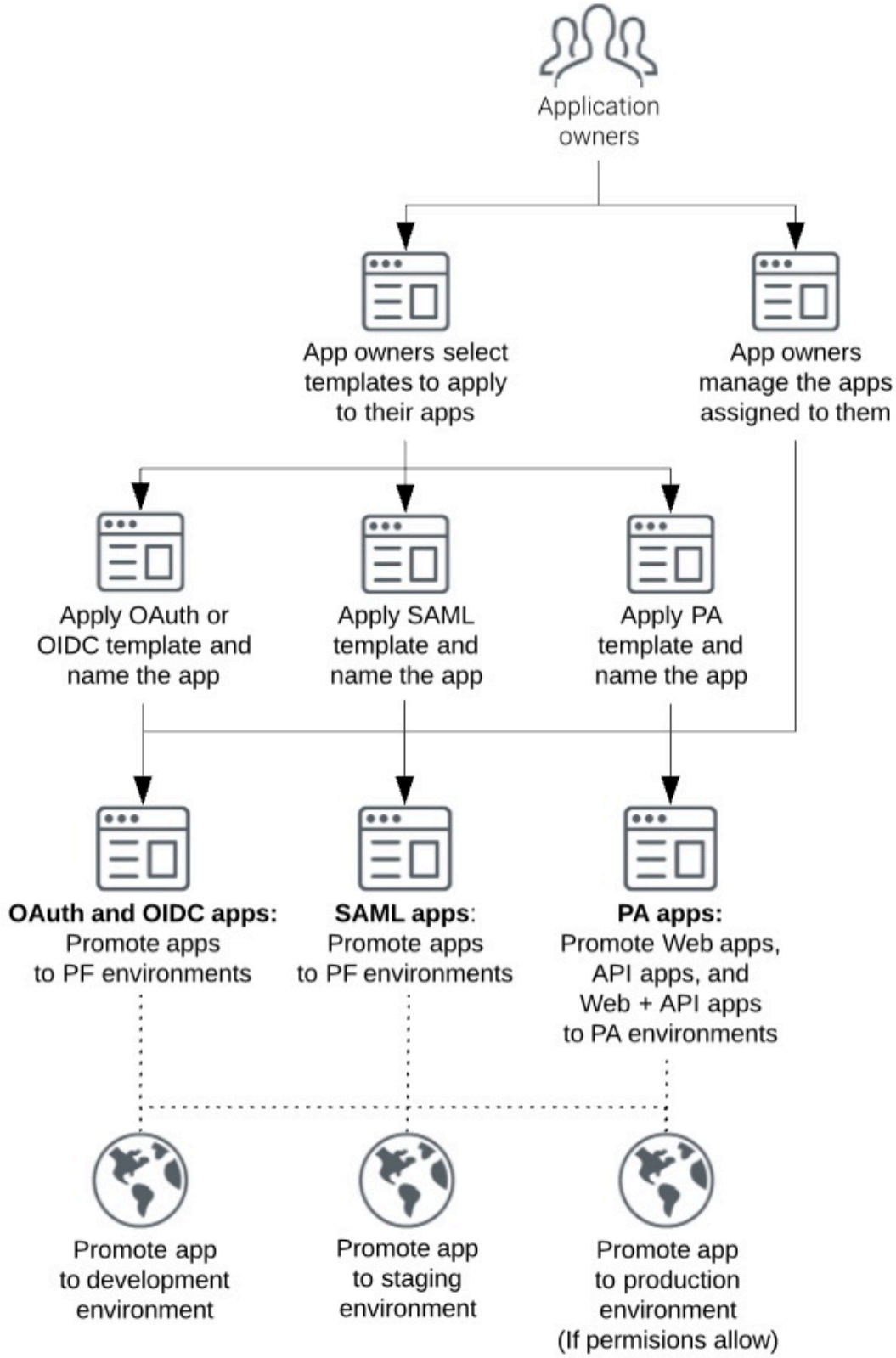
- Makes it possible for you to apply security configurations to your applications yourself without assistance from an administrator
- Allows you to promote these applications yourself, when you are ready, rather than submitting a request and waiting for someone else to promote them for you
- Provides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

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

How PingCentral works

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

4. When you're ready, promote applications to the appropriate development environments to test them and promote them directly to production environments if your permissions allow.



Accessing PingCentral

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

Steps

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

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

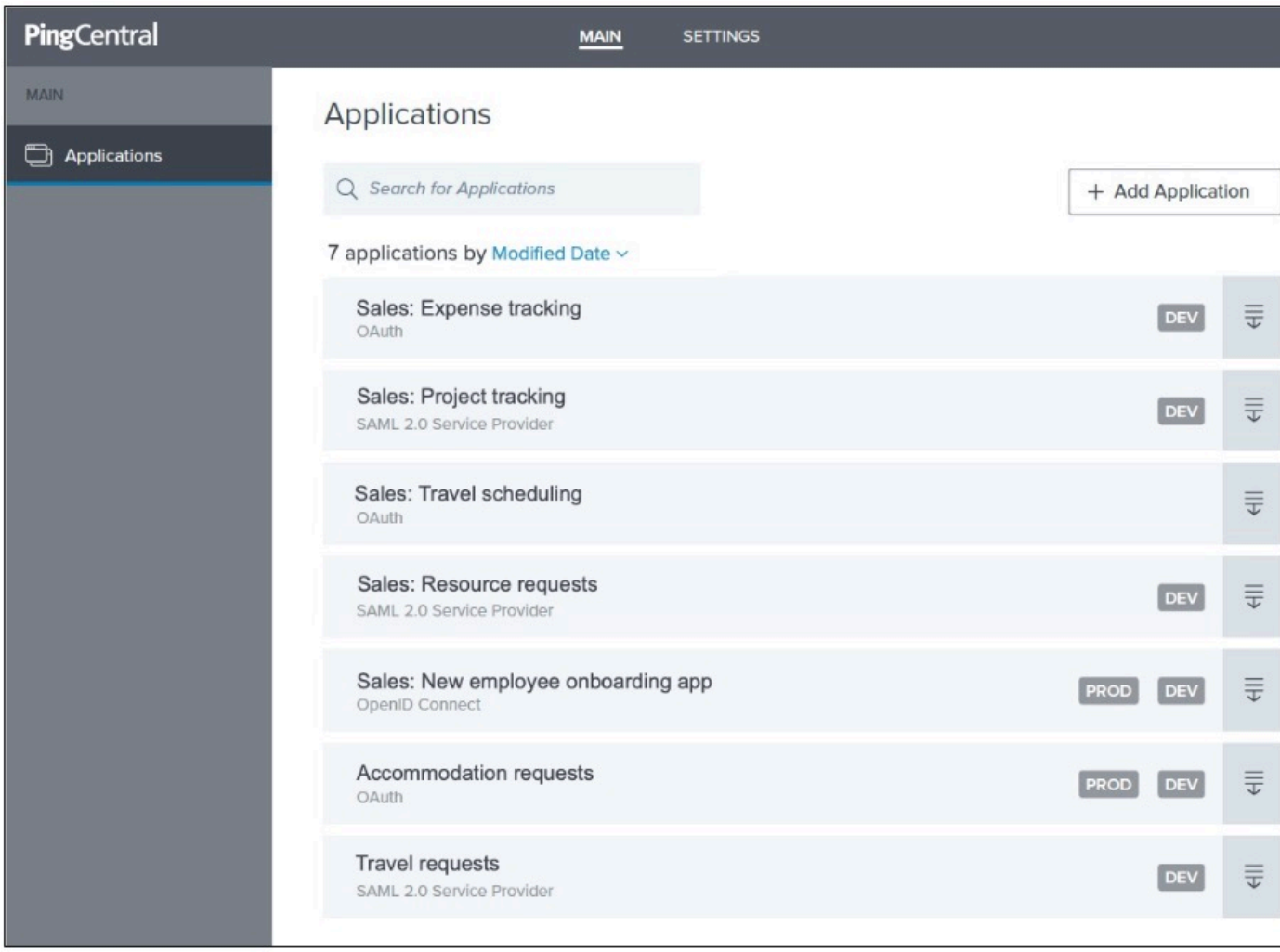
Managing applications

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

Steps

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

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



2. On the **Applications** page, you can:
   - View information about an application. Click the expandable icon associated with it.

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

     For more information, see *Adding applications*.

     ⓘ **Note:** Administrators can also assign you as the owner of an application, in which case the application will display on your **Applications** page.
   - Promote applications to development or production environments. Click the expandable icon associated with the application you want to promote and click the **Promote** tab.

     For more information, see *Promote applications*.
   - To update applications, 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.

     For more information, see *Updating applications*.
   - Delete an application from PingCentral, click its associated **Delete** icon.

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

Viewing application information

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

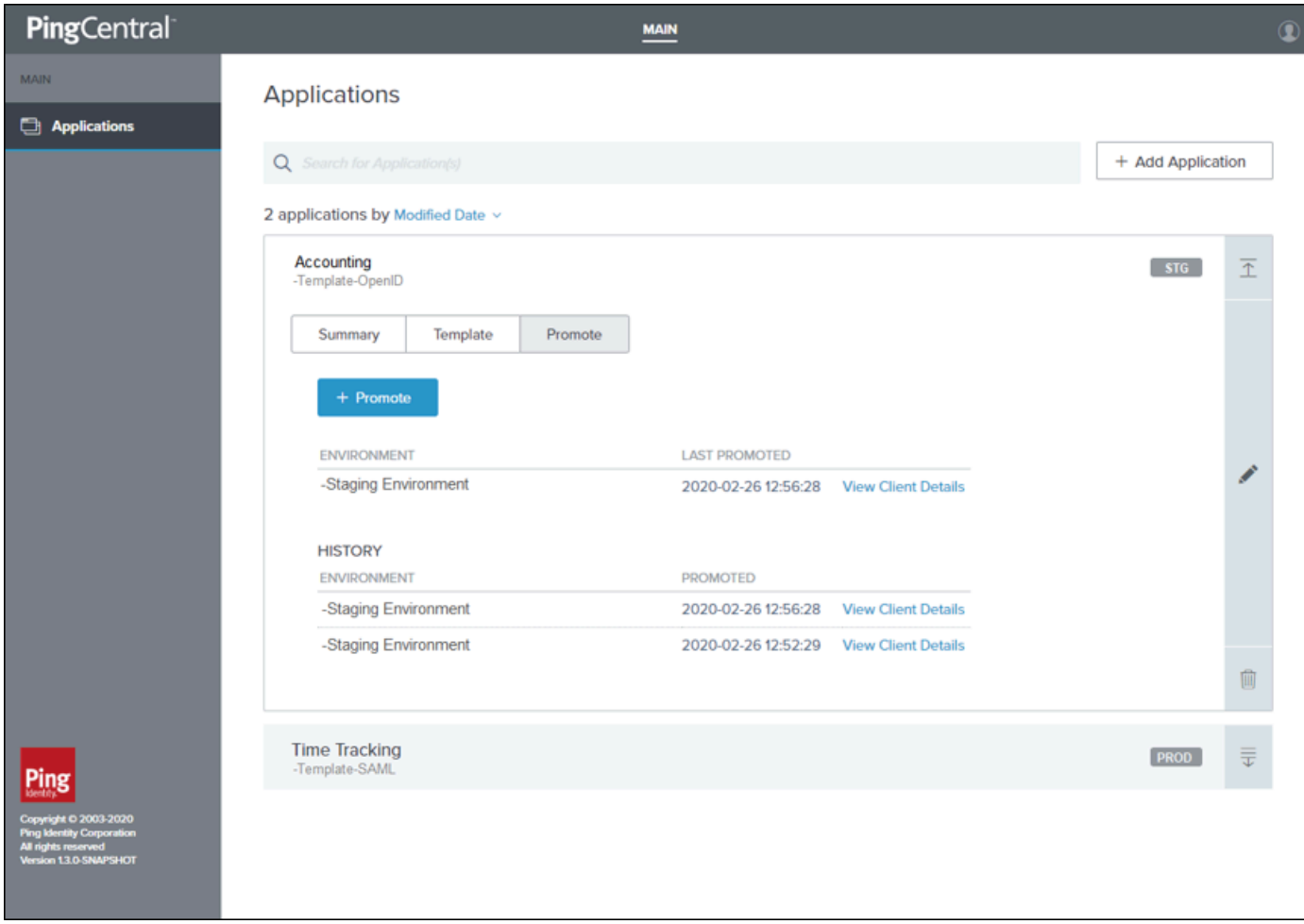
Steps

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

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

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

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



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

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

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

Adding applications

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

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

See the following topics:

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

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

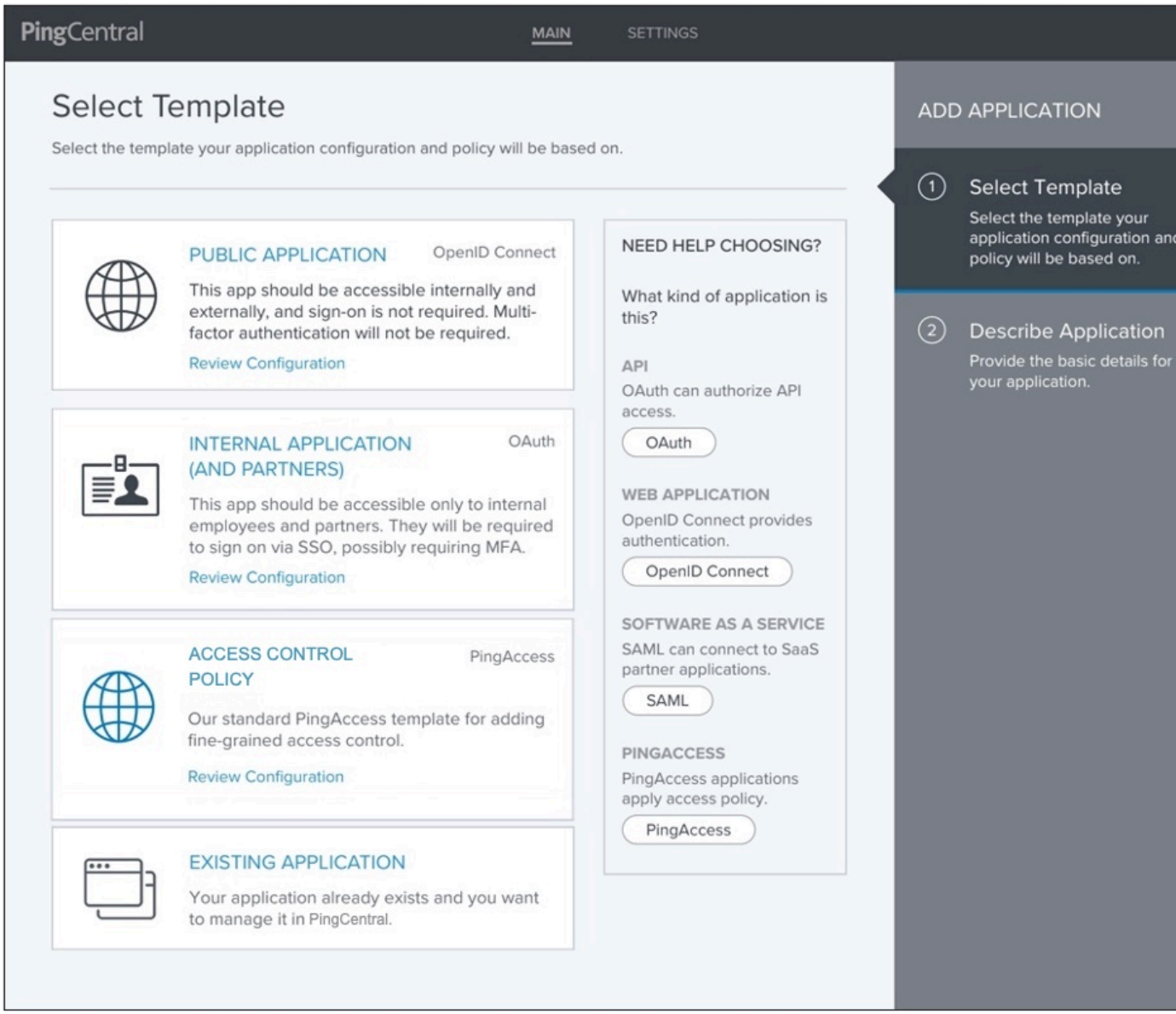
Selecting a template

IAM Administrators can create OAuth, OIDC, SAML, and PingAccess templates and make them available for you to use to apply security configurations to your application.

Steps

1. Click **Add Application**.

2. Review the template descriptions to determine which template you should use.



On this page, you can:

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

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

- OAuth and OIDC are most commonly used by consumer applications and services so users do not need to sign up for a new username and password. "Sign in with Google," or "Log in with Facebook" are examples of OAuth protocols you are likely familiar with. You might also use OAuth if your application is consumed on a mobile device.
- SAML is most commonly used by businesses to allow their users to access services they pay for. Salesforce and Gmail are examples of service providers an employee could gain access to after completing a SAML login. SAML templates can also be used for web applications created and used within your organization.
- PingAccess templates can be used to apply access policy to Web and API applications.

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

   To proceed, see the appropriate topic:

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

Using OAuth and OIDC templates

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

Before you begin

Prepare to provide the following:

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

Steps

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

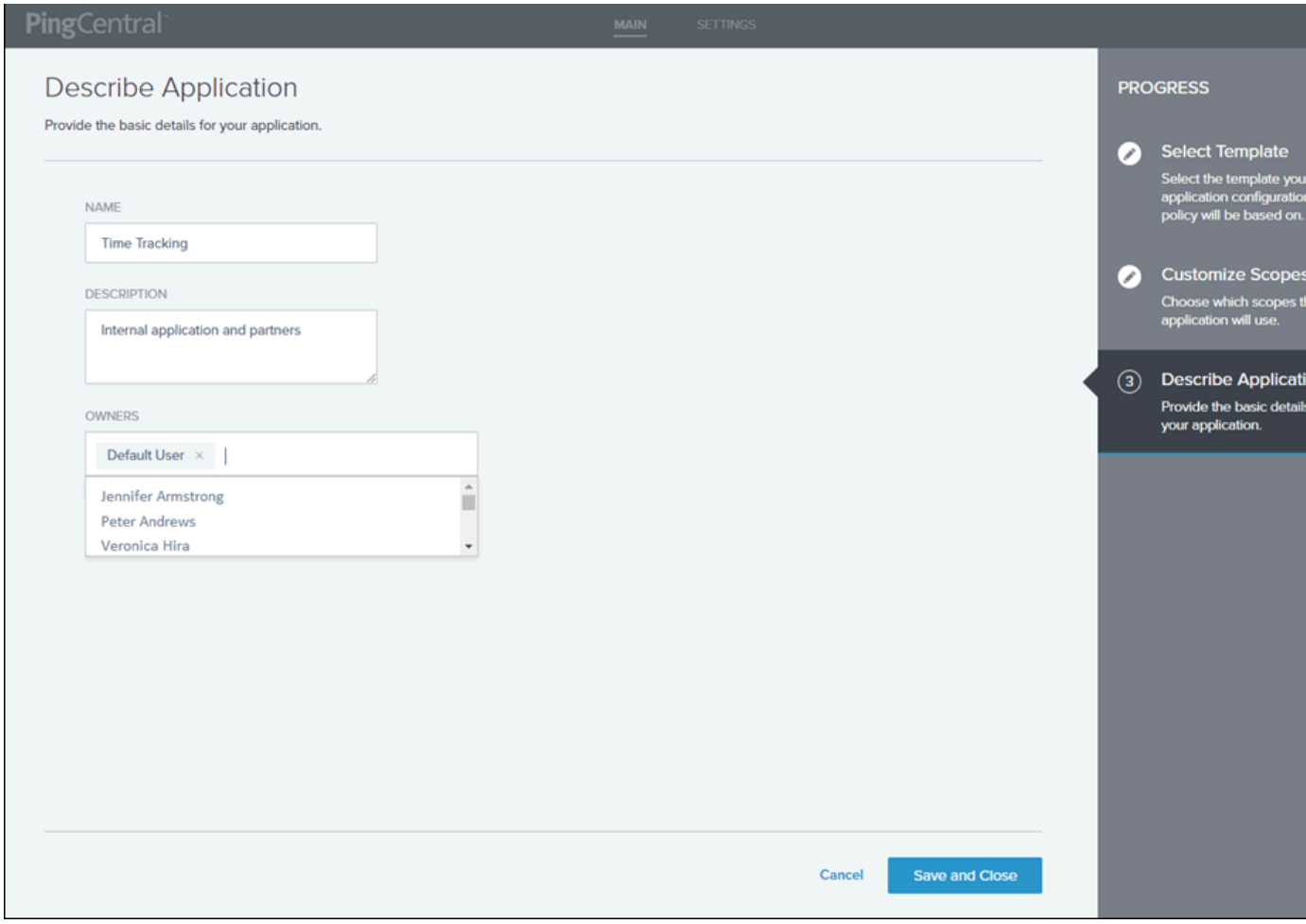
   > ⓘ **Note:**
   >
   > The names of scopes added to applications cannot contain spaces, nor can the **Scopes** field contain spaces before or after the scope name. If spaces exist, applications cannot be successfully promoted.

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

   If the named scope does not exist in the target environment, the scope is created as an exclusive scope. In that case, or if the scope already exists as an exclusive scope, then the scope is associated with the client as an exclusive scope.
2. Click **Next**.
3. On the **Describe Application** page, enter the name of your application and a description of the application in the **Name** and **Description** fields.

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

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



5. Click **Save and Close**.

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

Using SAML templates

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

Before you begin

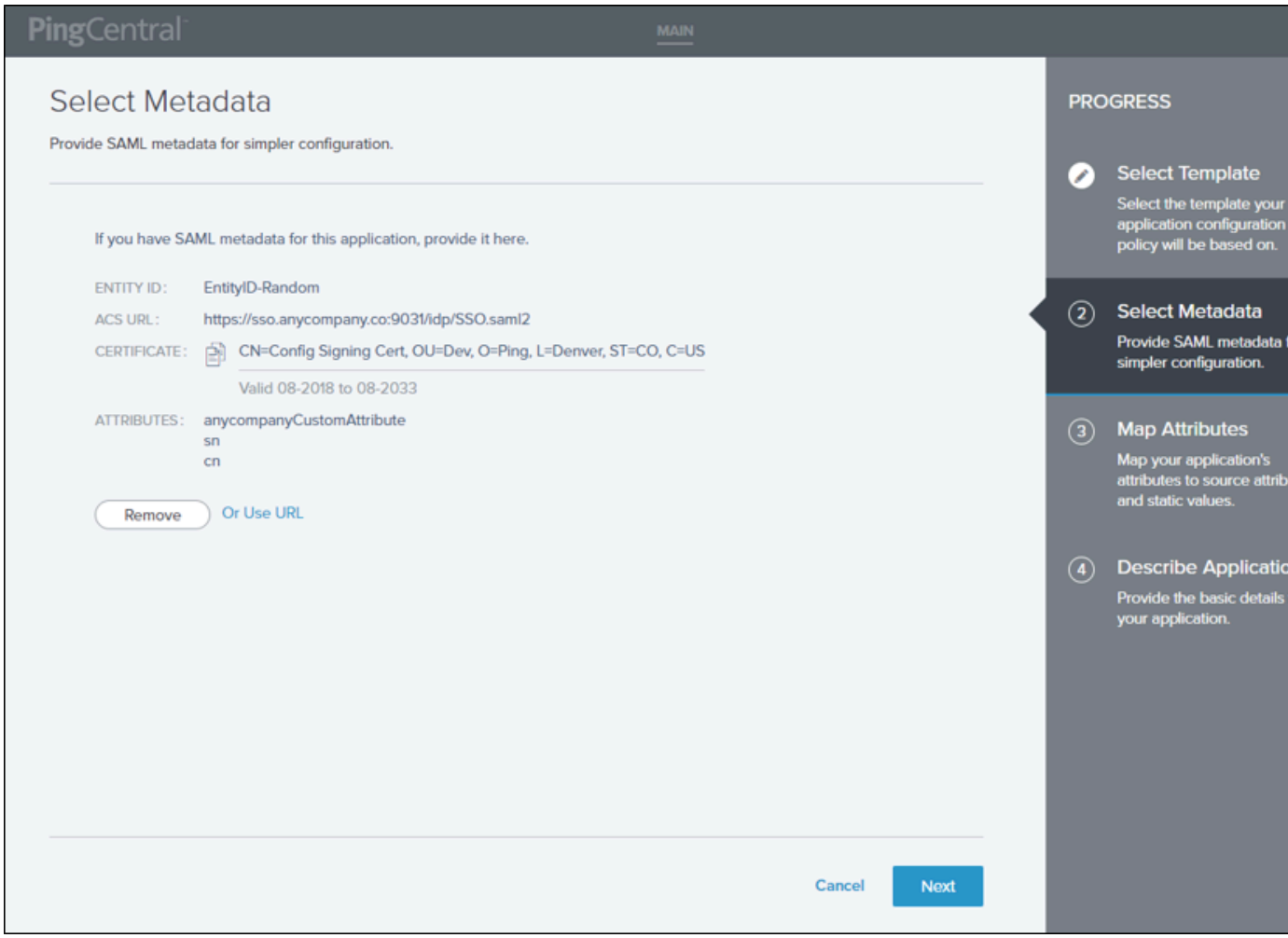
Prepare to provide the following:

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

Steps

1. On the the **Select Metadata** window, you can:
   - Provide a metadata file. Click **Choose file** to provide the file.
   - Provide a URLto the metadata file. Click **Or Use URL** to provide the URL.
   - Skip this step and provide the Entity ID, ACS URL, and certificates, or all of this information, during the promotion process.

   If you choose to provide a metadata file, the information in the file will display, as shown in this example.



2. Click **Next**.
3. 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 click to add static values in the **Static Value** field. Click **Next**.
4. 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.
5. Optional: To add owners, click the **Owners** field 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**.
6. Click **Save and Close**.
   The application displays at the top of the list of applications on the **Applications** page.

Using PingAccess templates

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

Before you begin

Prepare to define the following, as appropriate:

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

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

Steps

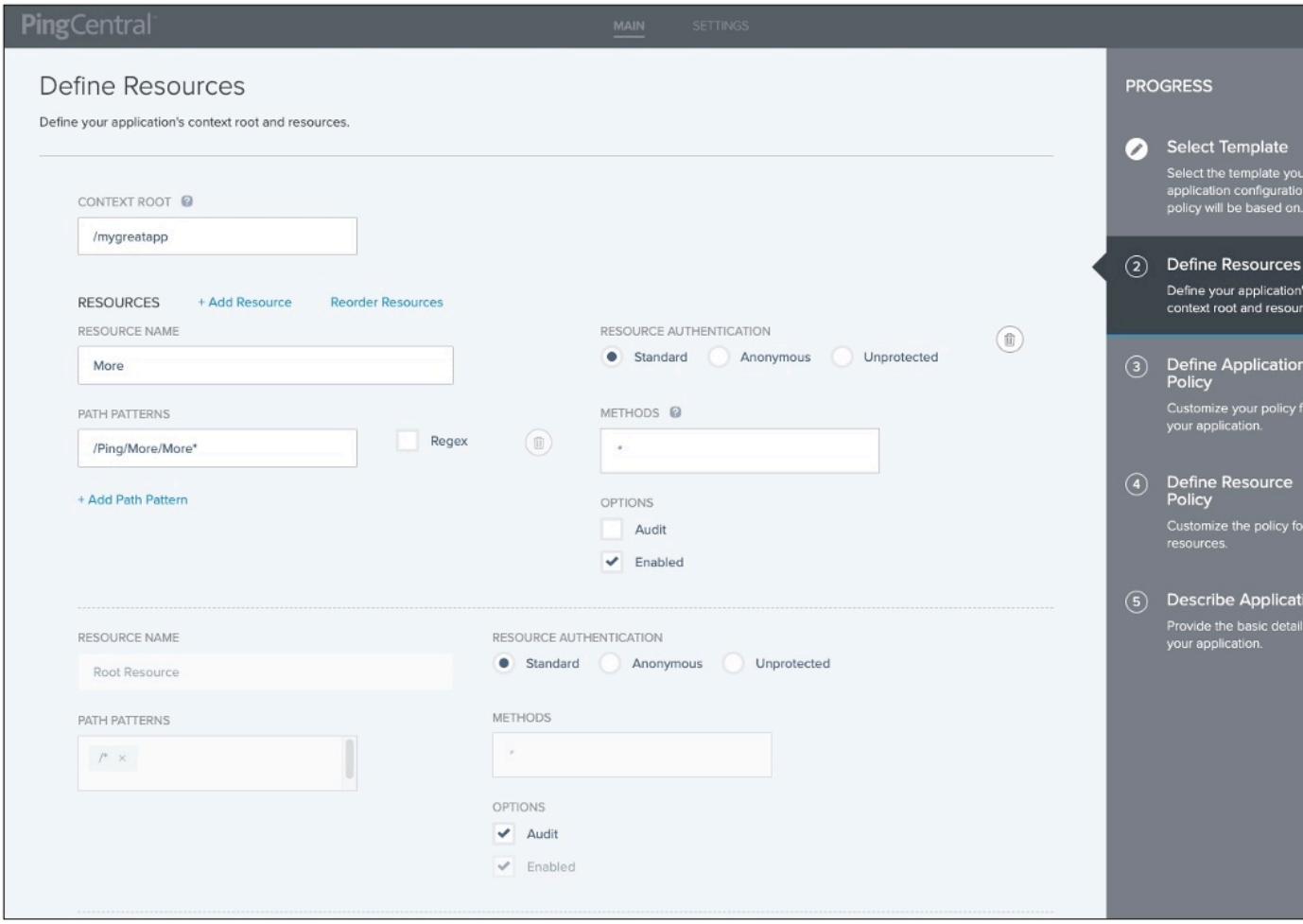
1. On the **Define Resources** page, enter the context root for the application.

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

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

   Every application has at least one root resource.

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



   To add a new resource:

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

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

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

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

   To apply rules or rule sets, drag them from the **Available Rules** list to the **Policy** list. Click **Next**.
4. **Optional**: On the **Define Resource Policy** page, customize the policy for each of your resources.

   To apply rules or rule sets to each resource, drag them from the **Available Rules** list to the **Policy** list. Click **Next**.
5. On the **Describe Application** page, enter the name of the application and a description in the appropriate fields.

   By adding this application to PingCentral, your name automatically populates the **Owners** field.
6. Optional: To add owners, click the **Owners** field and select additional owners from the list. Click **Next**.

   If the name you are looking for does not display in the list, contact your PingCentral administrator and request that the person be provisioned.
7. Click **Save and Close**.
   The application displays at the top of the list of applications on the **Applications** page.

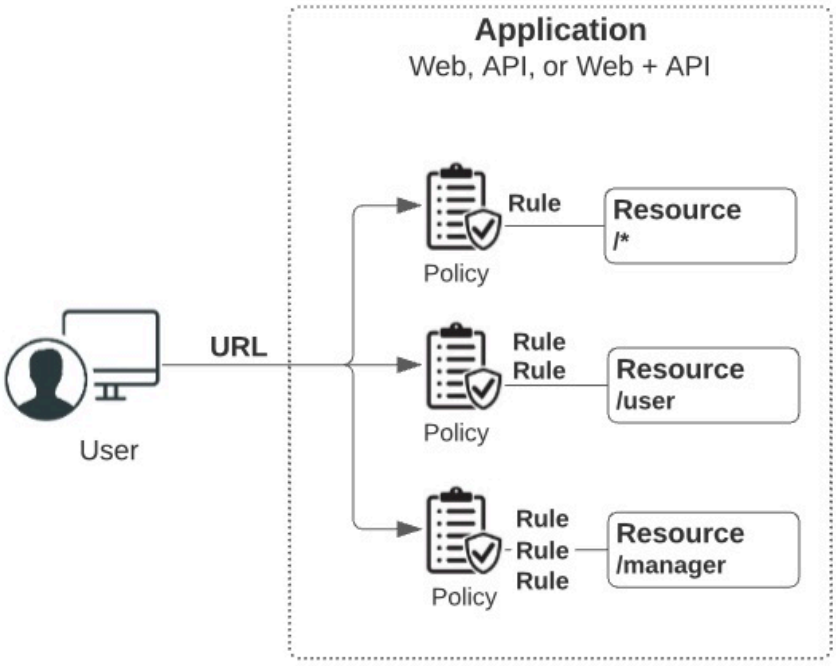
Information needed to add PingAccess applications

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

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

Resources

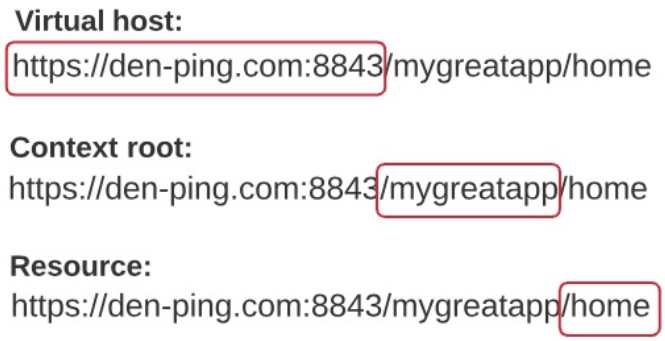
Each application consists of one or more resources, which you define in PingCentral. Resources are components of an application that require different levels of security. When you define resources within an application, you also define security regarding those resources.



Resources are protected by rules, which let you specify who can access your applications and resources, how and when they can do so, and what modifications can be made to the requested content. When rules,

or sets of rules, are applied to applications and resources, they are called policies. Policies are applied to requests, which determine whether users are granted or denied access to the requested resource.

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



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

Path patterns

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

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

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

  matches any of these request paths:

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

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

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

  matches any of these request paths:

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

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

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

```
/index.html
```

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

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

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

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

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

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

Rules and policies

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

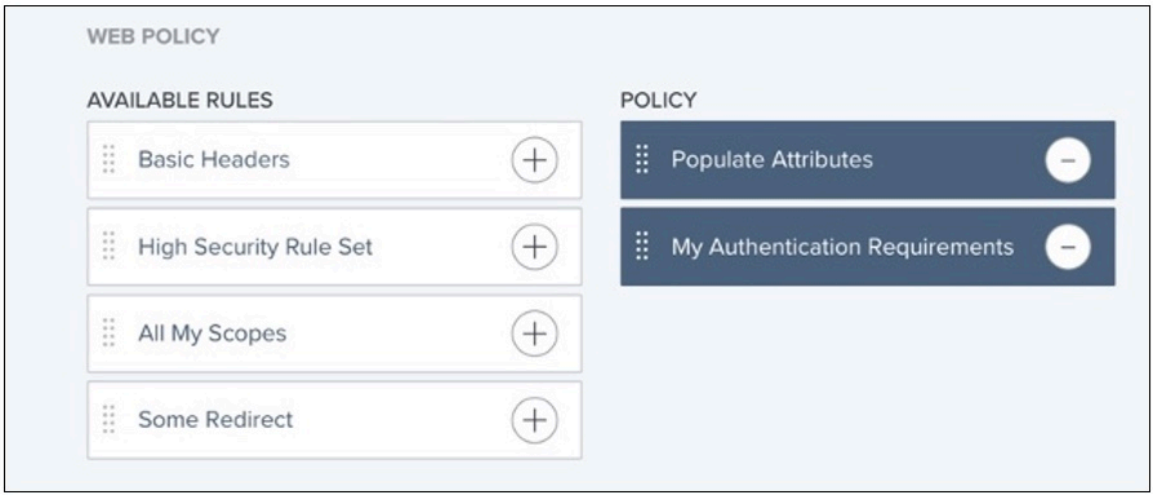
When you put rules together, they are called policies.

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

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

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

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



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

Updating applications

Update applications at any time.

About this task

To keep your applications secure, rotate certificates and client secrets on a regular basis and apply updated security configurations to applications built from templates if new configuration templates become available. There is no need to recreate your applications in PingCentral to apply new templates. Replace the templates associated with your applications and promote them again.

Steps

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

   All of the editable information displays on one page.
2. To update the name, description, and owners, change the information in the **Name**, **Description**, and **Owners** fields. Click **Save**.
3. To change the template used to create the application, click **Change Template** and select a new template from the **Select Template** page. Click **Save and Close**.

> ⓘ **Note:**
>
> You cannot apply a SAML template to an OAuth or OIDC application, nor apply an OAuth or OIDC template to a SAML application.

4. To update application information:

Application type	Update instructions
OAuth or OIDC	▪ In the **Client** section, change the scopes associated with OAuth or OIDC applications.

Application type	Update instructions
	Select or clear the appropriate check boxes and click **Save**. **Note:** You cannot edit scopes for applications created in version 1.2.0. However, you can update the template associated with an application to a template created in a later version, which will allow you to update scope information. ▪ In the **Promote** section, change the information in the **Redirect URI** fields for the appropriate environments and click **Save**. ▪ To change client secrets, return to the **Applications** page, promote the application again, and generate a new secret.
SAML	▪ In the **Attribute Mappings** section, add or remove attributes or update attribute values and click **Save**. ▪ In the **Promotions** section, upload a new `.xml` file that contains service provider metadata, such as the Entity ID, ACS URL, certificates, and attribute information, from another SAML application. Click **Choose File** or **Or Use URL** to provide the metadata file. **Note:** If metadata is used, the attribute mapping section might also need to be updated to include new attributes from the metadata file. ▪ Change the information in the **Entity ID** or **ACS URL** fields and click **Save**. ▪ To change the certificate, click **SP Certificate** to upload a new certificate, or click **Remove** to remove it. Click **Save**.
PingAccess	▪ On the **Properties** tab, in the **Promote** section, update the **Virtual Hosts**, **Access Validation**, **Identity Mapping**, and **Site** or **Agent** names, as appropriate. Click **Save**. ▪ On the **Resources** tab, update information regarding each resource and click **Save**. ▪ On the **Policy** tab, click the **Pencil** icon associated with the policy you want to update. Make changes and click **Save**.

Promote applications

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

See the following topics:

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

Promoting OAuth and OIDC applications

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

Before you begin

Prepare to provide the following:

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

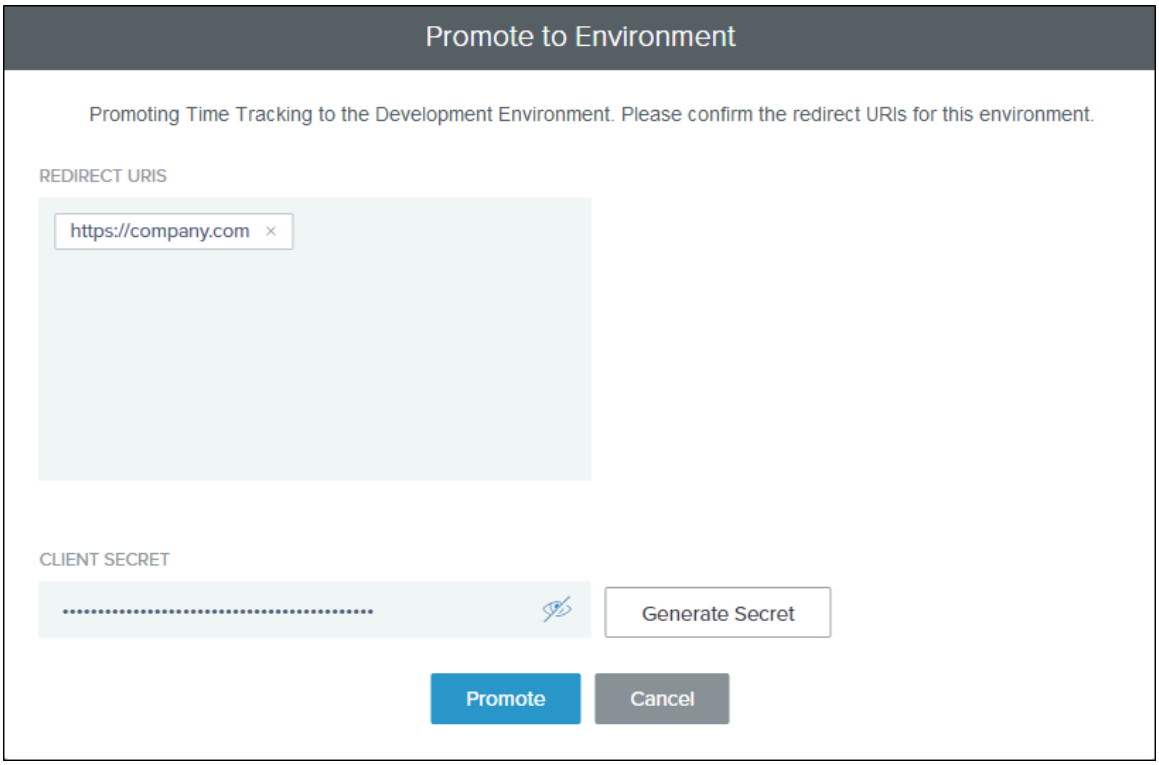
  Redirect URIs are not limited to the number of characters they can contain, but cannot include wildcards or some special characters.
- If a client secret is required to authenticate your application, you can create a custom secret, generate a secret, or leave the field empty and PingCentral will generate a client secret for you.

Steps

1. To promote the application to an environment, click the expandable icon associated with the application, select the **Promote** tab, and click **Promote**.
2. From the **Available Environments** list, select the environment to which you want to promote the application.

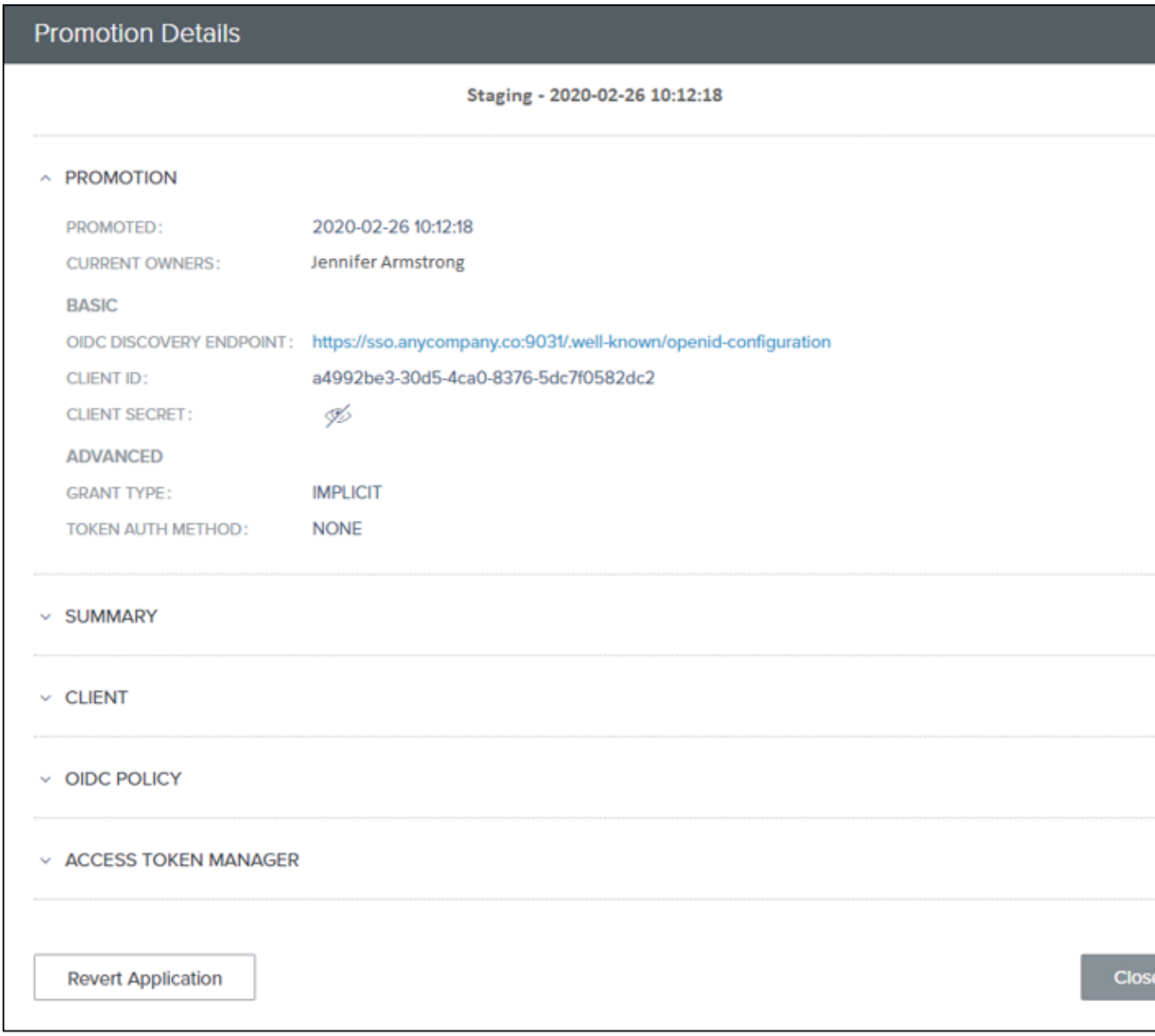
   ⓘ **Note:** If you have the Application Owner role, you cannot promote applications to protected environments, which have shield icons associated with them.
3. If redirect URIs are required to promote the application, enter them in the **Redirect URIs** field.

4. If a client secret is required to authenticate your application, you can:
   - Create a custom secret and enter it in the **Client Secret** text box.
   - Generate a client secret by clicking the **Generate Secret** button.
   - Leave the **Client Secret** text box empty and PingCentral will automatically generate a client secret for you.



5. 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.

6. To configure the SSO connection, provide the following information to your service provider:
   - The client ID. Click **View Client Details** to access the **Promotion Details** window, which displays the client ID.
   - The client secret and OIDC discovery endpoint available in this window.



Promoting SAML applications

You can promote the SAML applications assigned to you.

Before you begin

Prepare to provide the following:

- Entity ID, used to uniquely identify the application and obtained from the service provider ACS URL, the application's URL to which SAML assertions from the identity provider will be sent after user authentication occurs
- ACS URL, the application's URL to which SAML assertions from the identity provider will be sent after user authentication occurs

- SP certificates, if the template you select is based on a PingFederate connection that requires a certificate
- An assertion encryption certificate, which is required if encryption is enabled for the connection

Steps

1. To promote the application to an environment, click the expandable icon associated with the application, select the **Promote** tab, and click **Promote**.
2. From the **Available Environments** list, select the environment to which you want to promote the application.

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

3. In the **Entity ID** and **ACS URL** fields, enter the appropriate information.

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

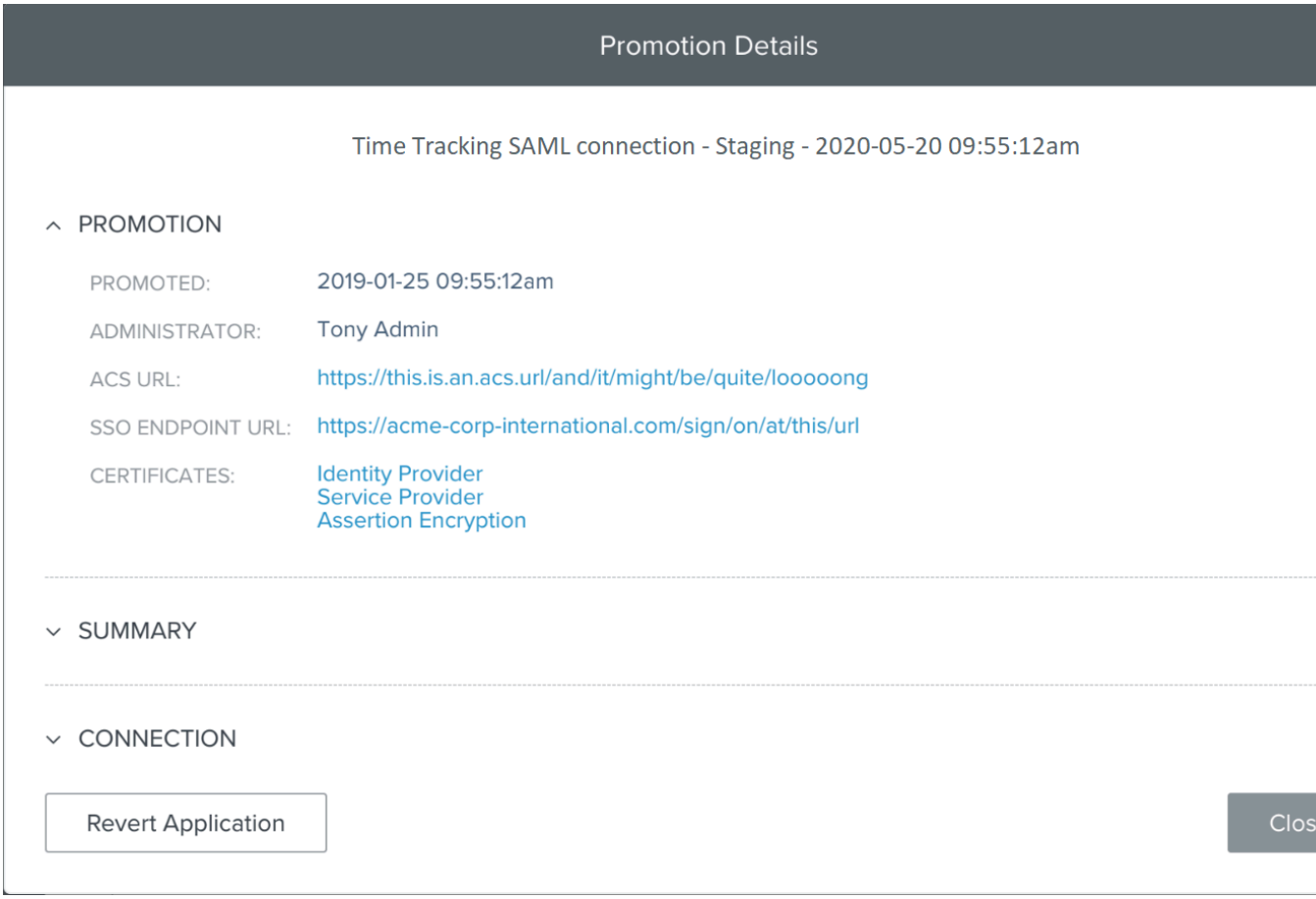
   Certificates are required for PingFederate SP connections when:

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

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

6. 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.

7. Configure the SSO connection.
   a. Enter the application Entity ID.
   b. To specify the SSO endpoint URL, click **View Connection Details** to access the **Promotion Details** window, which displays the SSO endpoint URL.
   c. To add certificates, if applicable, in the **Promotion Details** window, click **Identity Provider** to download the certificate that the identity provider is using to sign the SAML assertion, and the assertion encryption certificate associated with the connection.



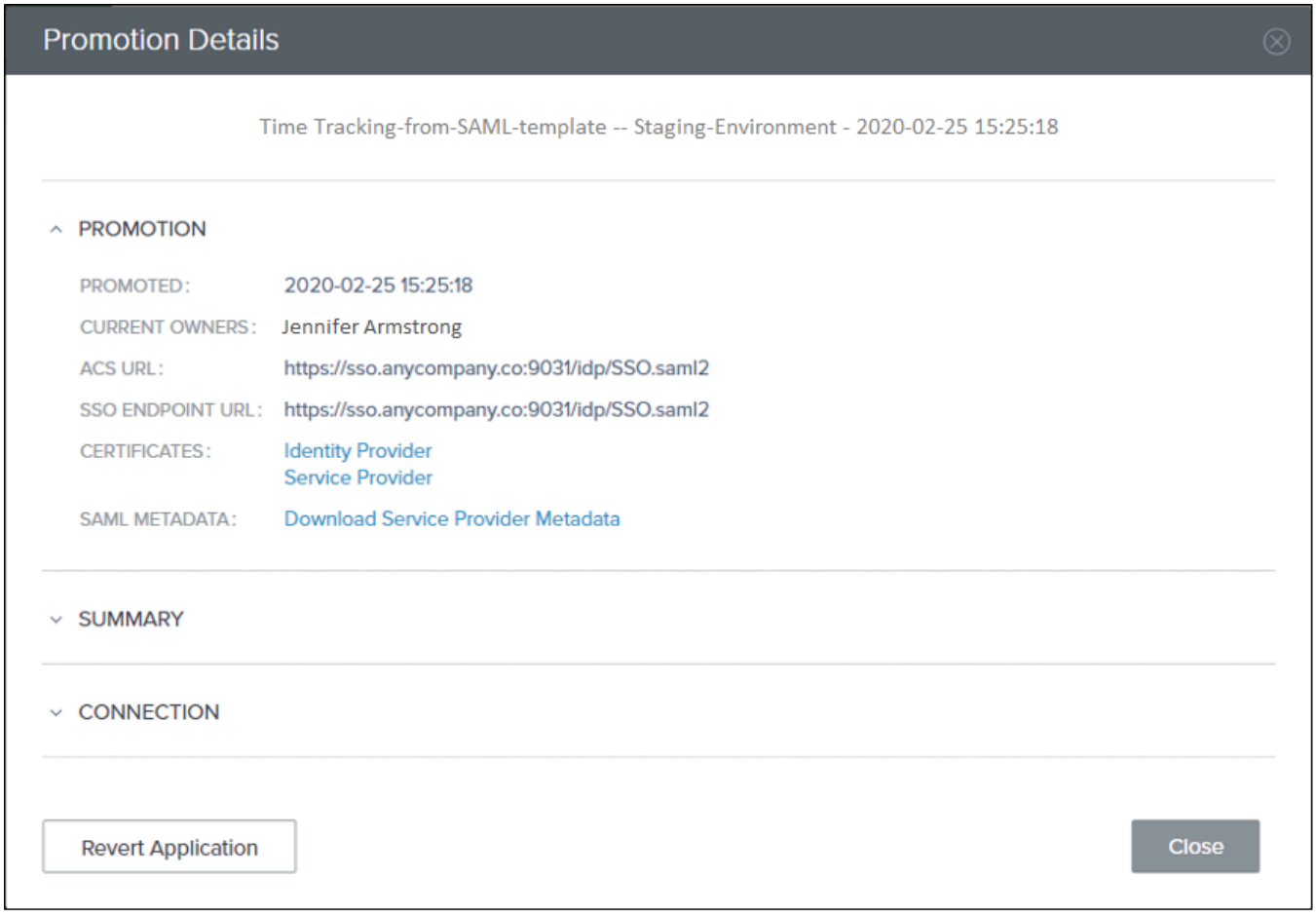
Using metadata to promote SAML applications
When SAML applications are promoted, the connection metadata is exported and stored as part of that application. This metadata is available to download as a `.xml` file, which you can use to promote similar SAML applications.

Steps

1. On the **Applications** page, locate an application that has a configuration you want to replicate in a new SAML application and click the expandable icon associated with that application.

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

   The promotion information displays.



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

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

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

   For more information, see *Updating applications*.

Promoting PingAccess applications

Promote the PingAccess applications assigned to you.

Before you begin

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

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

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

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

Steps

1. To promote the application to an environment, click the Expand icon associated with the application, select the **Promote** tab, and click **Promote**.
2. From the **Available Environments** list, select the environment to which you want to promote the application.

   ⓘ **Note:**

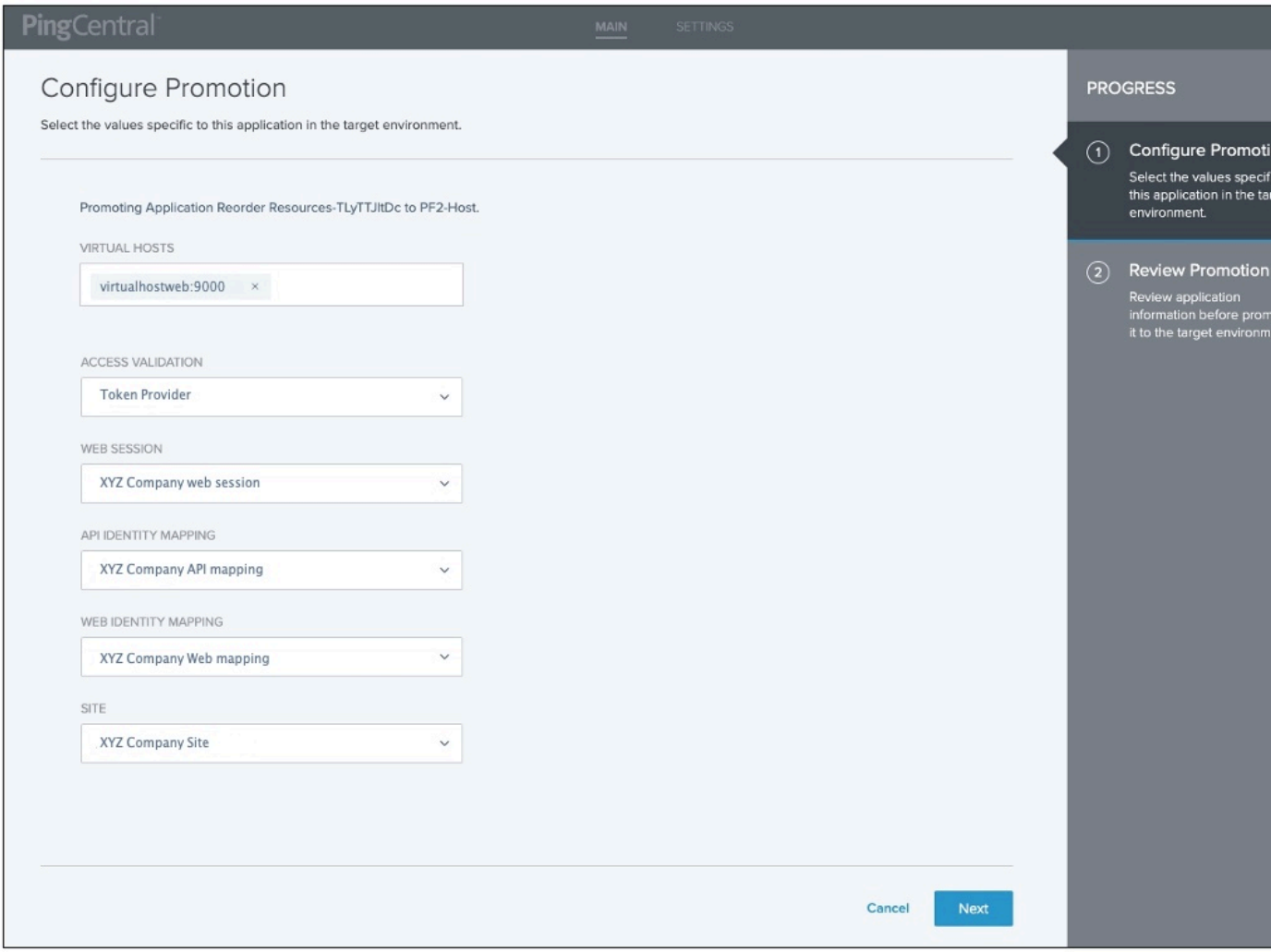
   If you have the Application Owner role, you cannot promote applications to protected environments, which have shield icons associated with them.

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

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

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

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



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

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

Information needed to promote PingAccess applications

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

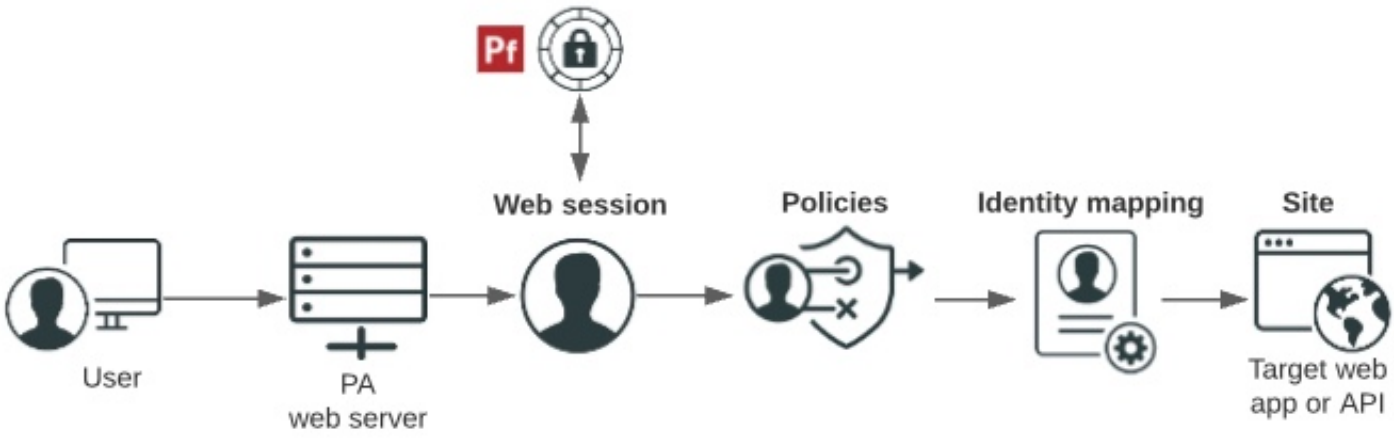
PingAccess can be deployed in one of two ways:

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

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

Gateway deployment

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



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

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

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

   ⓘ **Note:** If you promote Web + API applications in PingCentral, you are required to select a Web session from a drop-down list. This information is not required to promote Web or API applications.
3. You can configure API and Web + API applications to use access token validators to locally verify signed and encrypted access tokens. If you are promoting an API or Web + API application in PingCentral, you can specify the access validation method, whether it be a token provider or a token validator, if appropriate.
4. Users are authenticated through the web session.
5. Policies are applied to the request. Policies are rules, or sets of rules, that are applied to application resources. PingAccess makes policy-based decisions to grant or deny access to the requested resource.

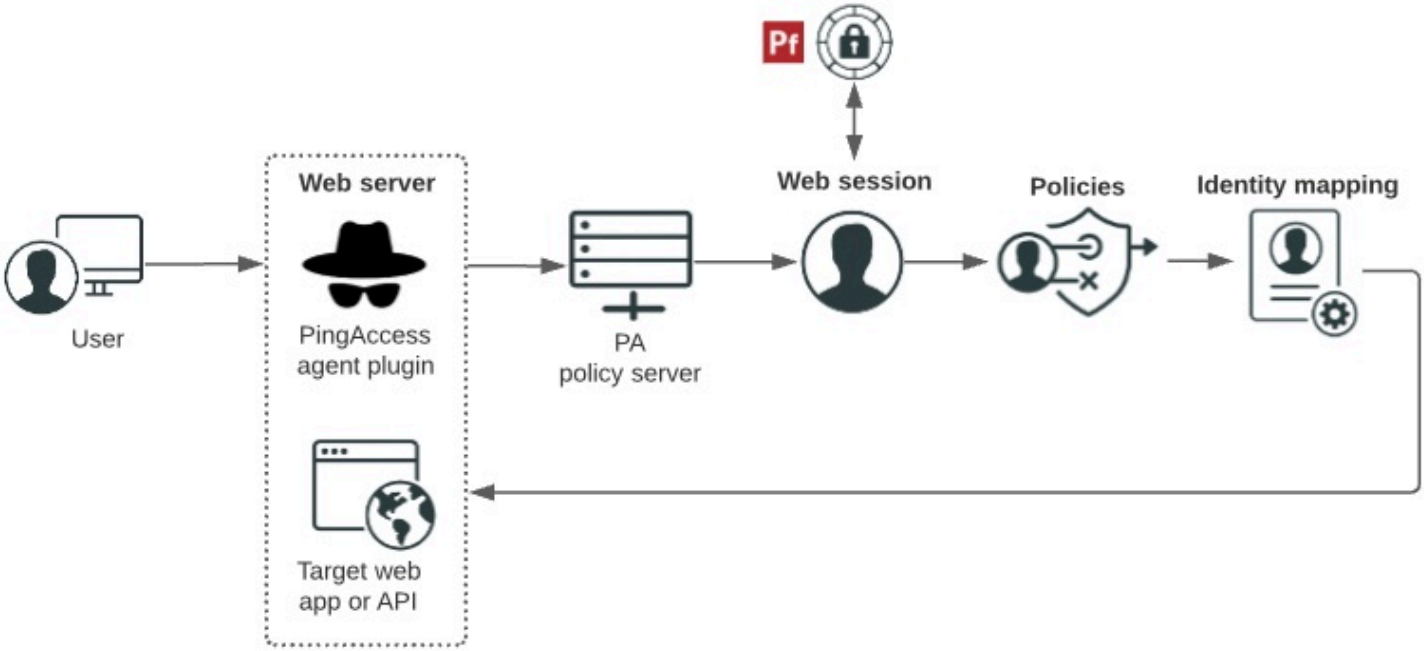
   You can customize application and resource policies when you use templates to add applications to PingCentral.

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

   PingCentral prompts you for the name of the Web and/or API Identity mapping, as appropriate, when you promote it.
7. The user accesses the target web application or API.

Agent deployment

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



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

Reverting applications to previously promoted versions

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

About this task
You cannot revert applications created in previous versions of PingCentral.

Steps

1. On the **Applications** page, locate the application you want to revert to a previously promoted version.
2. Click the expandable icon associated with the application, select the **Promote** tab, and then click **View Details**.
3. In the **Promotion Details** window, click **Revert Application**.
   A message displays asking you if you are sure you want to revert this application.
4. Click **Revert**.
   The reverted version of the application displays in your applications list.

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