PingFederate® Bridge

Contents

Introduction to PingFederate Bridge

PingFederate Bridge is a light-weight version of PingFederate, which is Ping Identity's federated enterprise identity management solution. PingFederate Bridge is for use primarily by new customers who want to quickly and easily configure user authentication from an on-premise directory to PingOne for Enterprise in the cloud.

PingFederate Bridge allows you to enable single sign-on (SSO) for PingOne for Enterprise and to integrate PingID multi-factor authentication (MFA) with VPN using RADIUS. One or both of these options can be configured in a PingFederate Bridge environment.

ⓘ **Important:**

To install and use PingFederate Bridge, you must have a PingOne for Enterprise account. PingOne for Enterprise must be set up with a PingFederate Bridge identity repository.

Installation

Prerequisites

Before you install PingFederate Bridge, make sure that your system meets the requirements and that you have the required ports available. You must also install Java.

System requirements

Ping Identity® has qualified the following configurations and certified that they are compatible with the product. Variations of these platforms (for example, differences in operating system version or service pack) are supported up until the point at which an issue is suspected as being caused by the platform or other required software.

Operating systems and virtualization

ⓘ **Note:** PingFederate has been tested with default configurations of operating-system components. If your organization has customized implementations or has installed third-party plug-ins, deployment of the PingFederate server may be affected.

Operating systems

- Alpine Linux 3.10
- Amazon Linux 2
- Canonical Ubuntu 16.04 LTS
- Canonical Ubuntu 18.04 LTS
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Oracle Enterprise Linux 6.10 (Red Hat compatible kernel)
- Oracle Enterprise Linux 7.6 (Red Hat compatible kernel)
- Oracle Enterprise Linux 8.0 (Red Hat Compatible Kernel)
- Red Hat Enterprise Linux ES 6.10
- Red Hat Enterprise Linux ES 7.6

- Red Hat Enterprise Linux ES 8.0
- SUSE Linux Enterprise 12 SP4
- SUSE Linux Enterprise 15 SP1

ⓘ **Note:**

For Alpine Linux, PingFederate must be deployed with Oracle Server JRE (Java SE Runtime Environment) 8.

Docker support

- Docker version: 19.03.5
- Host operating system: Canonical Ubuntu 18.04 LTS
- Kernel: 4.15.0-1052-aws

Virtualization

Although Ping Identity does not qualify or recommend any specific virtual-machine (VM) or container products other than those listed above, PingFederate has been shown to run well on several, including Hyper-V, VMWare, and Xen.

ⓘ **Note:** The list of products is provided for example purposes only. We view all products in this category equally. Ping Identity accepts no responsibility for the performance of any specific virtualization software and in no way guarantees the performance, interoperability, or both of any VM or container software with its products.

Java environment

- Amazon Corretto 11
- Amazon Corretto 8
- OpenJDK 11
- Oracle Java SE Development Kit 11 LTS
- Oracle Java SE Runtime Environment (Server JRE) 8

ⓘ **Note:**

Ping Identity Java Support Policy applies. Refer to this article for more information.

Browsers

Runtime server

- Apple Safari
- Google Chrome
- Microsoft Edge
- Microsoft Internet Explorer 11 (and higher)
- Mozilla Firefox
- Apple iOS 12 (Safari)
- Google Android 9 (Chrome)

Administrative server

- Google Chrome

- Microsoft Internet Explorer 11 (and higher)
- Mozilla Firefox

TLS protocol

Runtime server and administrative server

- TLS 1.2 and 1.3

> ⓘ **Note:** TLS 1.3 requires Oracle Java SE Development Kit 11 or OpenJDK 11.

Data store integration

User-attribute lookup

- PingDirectory 6.2, 7.0, 7.2, 7.3, 8.0
- Microsoft Active Directory 2016
- Oracle Directory Server Enterprise Edition 11g
- Oracle Unified Directory 12c
- Microsoft SQL Server 2016 SP2 and 2017
- Oracle Database 12c Release 1
- Oracle Database 19c
- Oracle MySQL 8.0
- PostgreSQL 9.6.15 and 11.5
- Custom implementation through the PingFederate SDK

SaaS or SCIM outbound provisioning

Provisioning channel data source

- PingDirectory 6.2, 7.0, 7.2, 7.3, 8.0
- Microsoft Active Directory 2016
- Oracle Directory Server Enterprise Edition 11g
- Oracle Unified Directory 12c

Provisioning internal data store

- Microsoft SQL Server 2016 SP2 and 2017
- Oracle Database 12c Release 1
- Oracle Database 19c
- Oracle MySQL 8.0
- PostgreSQL 9.6.15 and 11.5

SCIM inbound provisioning

- Microsoft Active Directory 2016
- Custom implementation through the PingFederate SDK

Just-in-time (JIT) inbound provisioning

- PingDirectory 6.2, 7.0, 7.2, 7.3, 8.0
- Microsoft Active Directory 2016
- Oracle Directory Server Enterprise Edition 11g
- Oracle Unified Directory 12c

- Microsoft SQL Server 2016 SP2 and 2017

Account linking

- PingDirectory 6.2, 7.0, 7.2, 7.3, 8.0
- Microsoft Active Directory 2016
- Oracle Directory Server Enterprise Edition 11g
- Oracle Unified Directory 12c
- Microsoft SQL Server 2016 SP2 and 2017
- Oracle Database 12c Release 1
- Oracle Database 19c
- Oracle MySQL 8.0
- PostgreSQL 9.6.15 and 11.5

OAuth client configuration and persistent grants

- PingDirectory 6.2, 7.0, 7.2, 7.3, 8.0
- Microsoft Active Directory 2016
- Oracle Directory Server Enterprise Edition 11g
- Oracle Unified Directory 12c
- Microsoft SQL Server 2016 SP2 and 2017
- Oracle Database 12c Release 1
- Oracle Database 19c
- Oracle MySQL 8.0
- PostgreSQL 9.6.15 and 11.5
- Custom implementation through the PingFederate SDK

Registration and profile management of local identities

- PingDirectory 6.2, 7.0, 7.2, 7.3, 8.0

Persistent authentication sessions

- PingDirectory 7.2, 7.3, 8.0
- Microsoft SQL Server 2016 SP2 and 2017
- Oracle Database 12c Release 1
- Oracle Database 19c
- Oracle MySQL 8.0
- PostgreSQL 9.6.15 and 11.5

ⓘ **Note:**

PingFederate has been tested with vendor-specific JDBC 4.2 drivers. For more information, see .

Hardware security module (optional)

AWS CloudHSM

- Client software version: 2.0.4

ⓘ **Note:**

PingFederate must be deployed on one of the Linux operating systems supported by both AWS CloudHSM and PingFederate.

Gemalto SafeNet Luna Network HSM 6

- HSM firmware version: 6.3
- Firmware version: 6.27.0
- Client software version: 6.3

Gemalto SafeNet Luna Network HSM 7

- Appliance software version: 7.2.0
- Firmware version: 7.2.0
- Client software version: 7.2.0

nCipher nShield Connect

- Host and Firmware version: 12.40.0
- Client driver version: 12.40.2
- Hardware Model: Net HSM 6000 appliance

ⓘ **Note:**

When integrating with a hardware security module (HSM), PingFederate must be deployed with Oracle Server JRE (Java SE Runtime Environment) 8.

Hardware requirements

Minimum hardware recommendations

- Multi-core Intel Xeon processor or higher

  4 CPU/Cores recommended
- 4 GB of RAM

  1.5 GB available to PingFederate
- 1 GB of available hard drive space

ⓘ **Note:**

Although it is possible to run PingFederate on less powerful hardware, the following guidelines accommodate disk space for default logging and auditing profiles and CPU resources for a moderate level of concurrent request processing.

Database driver information

PingFederate has been tested with the following vendor-specific JDBC drivers.

Database server	Driver information
Microsoft SQL Server 2016 SP2 and 2017	**Driver version information** sqljdbc version 7.2.1 **Driver class** `com.microsoft.sqlserver.jdbc.SQLServerDriver` **JDBC URL** `jdbc:sqlserver://`*databaseservername*`;databaseName=`*databasename*
Oracle Database 12c Release 1 and 19c	**Driver version information** ojdbc7 version 12.1.0.2.0 **Driver class** `oracle.jdbc.OracleDriver` **JDBC URL** `jdbc:oracle:thin:@`*databaseservername*`:`*databasename*
Oracle MySQL 8.0	**Driver version information** mysql-connector-java version 8.0.15 **Driver class** `com.mysql.cj.jdbc.Driver` **JDBC URL** `jdbc:mysql://`*databaseservername*`/`*databasename*
PostgreSQL 9.6.1 and 11.2	**Driver version information** postgresql version 42.2.5 **Driver class** `org.postgresql.Driver` **JDBC URL** `jdbc:postgresql://`*databaseservername*`/`*databasename*

For additional information about these drivers, please contact the respective vendors.

Port requirements

The following table summarizes the ports and protocols that PingFederate Bridge uses to communicate with external components. This information provides guidance for firewall administrators to ensure the correct ports are available across network segments.

ⓘ **Note:**

Direction refers to the direction of the initial requests relative to PingFederate Bridge. Inbound refers to requests received by PingFederate Bridge from external components. Outbound refers to requests sent by PingFederate Bridge to external components.

Ports and protocols

Service	Protocol, direction, transport, default port	Source	Destination	Description
Administrative console	HTTPS, inbound, TCP, 9999	Browsers accessing the administrative console, REST calls to the administrative API, web service calls to the Connection Management Service. Applicable to the console node in a clustered PingFederate environment.	Administrative node	Used for incoming requests to the administrative console. Configurable in the `run.properties` file.
Administrative console	HTTPS, outbound, TCP, 443	Administrator accessing online help. Applicable to the console node in a clustered PingFederate environment.	docs.pingidentity.com	Used for accessing online help from the administrative console.
Runtime engine	HTTPS, inbound, TCP, 9031 (and 9032 if configured)	Browsers accessing the runtime server for SSO or SLO; web service calls to the SSO Directory Service; REST calls to the OAuth Client Management Service, the OAuth Access Grant Management Service, the Persistent Grant Management API, and the Session Revocation API. Applicable to all runtime engine nodes in a clustered PingFederate environment.	Runtime engine nodes	Used for incoming requests to the runtime engine. Configurable in the `run.properties` file.

Service	Protocol, direction, transport, default port	Source	Destination	Description
PingOne for Enterprise integration (if configured)	HTTPS and secure WebSocket, TCP, 443	PingFederate Applicable to the console node in a clustered PingFederate environment.	pingone.com	Used for communications between PingFederate and PingOne for the purpose of establishing and maintaining a managed SP connection to PingOne for Enterprise, monitoring of PingFederate from the PingOne admin portal, authenticating end users against the PingOne Directory.
Active Directory domains/ Kerberos realms (if configured)	Kerberos, outbound, TCP or UDP, 88	PingFederate	Windows domain controllers	Used for communications between PingFederate and Windows domain controllers for the purpose of Kerberos authentication.

ⓘ **Note:**

For PingID integration, refer to PingID documentation for a list of required URLs and ports.

Furthermore, additional ports may be required depending on the integration kits deployed and the connecting third-party systems; for example, email server or SMS service provider.

Installing Java

About this task

You must install Java on your server before installing PingFederate Bridge. PingFederate has been tested in the following Java environments:

- Amazon Corretto 11
- Amazon Corretto 8
- OpenJDK 11
- Oracle Java SE Development Kit 11 LTS
- Oracle Java SE Runtime Environment (Server JRE) 8

ⓘ **Note:** Ping Identity Java Support Policy applies. Refer to this *article* for more information.

ⓘ **Important:**

Due to the import restrictions of some countries, Oracle Server JRE (Java SE Runtime Environment) 8 has built-in restrictions on available cryptographic strength (key size). To use larger key sizes, the Java Cryptography Extension (JCE) "unlimited strength" jurisdiction policy must be enabled. For more information, see the *Java 8 release notes* from Oracle.

For Oracle Java SE Development Kit 11, the JCE jurisdiction policy defaults to unlimited strength. For more information, see the *Oracle JDK Migration Guide*.

Steps

1. Download and install a Java runtime.
2. Set the JAVA_HOME system environment variable to the Java installation directory.
3. Modify the Path system environment variable to include the path to the Java `bin` directory.

Installing PingFederate Bridge on Windows

Before you begin

Before you install PingFederate Bridge, make sure that you have the following in place:

- You must have a PingOne for Enterprise account and be connected to the PingFederate identity repository. For more information see *Connecting PingOne to a PingFederate repository*.
- You must be logged into a system with appropriate privileges to install and run an application.
- A supported version of the Java runtime environment must be installed as explained in *Installing Java* on page 11.

  The JAVA_HOME system environment variable must be set to the Java installation directory path. Also, the full path to the Java `bin` directory must be added to the Path system environment variable.

About this task

You install PingFederate Bridge by running an installer for Microsoft Windows Server.

ⓘ **Note:**

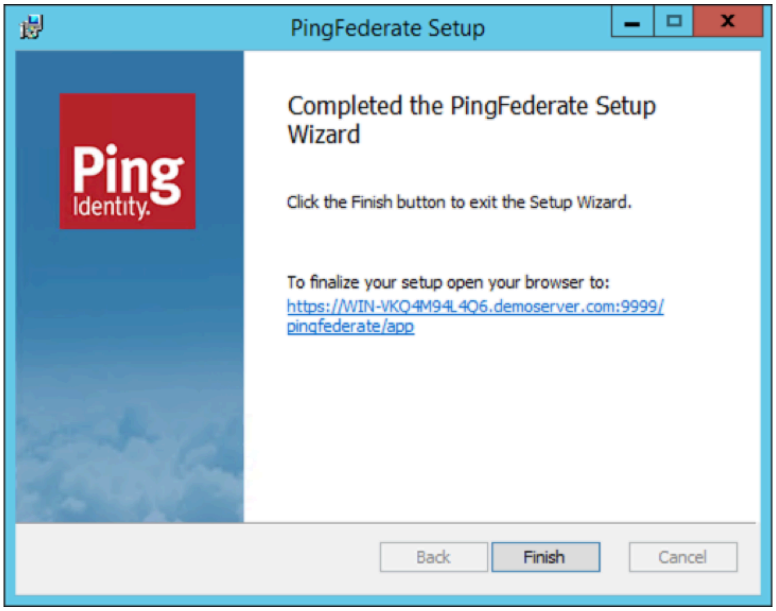
PingFederate Bridge is configured to run as a service; the service is started automatically at the end of the installation process.

Steps

1. Download the PingFederate installer for Windows from PingOne for Enterprise.

2. Run the installer and follow the installation steps.

   When the installation has finished, you see the **Completed the PingFederate Setup Wizard** screen.



Completed the PingFederate Setup Wizard

Click the Finish button to exit the Setup Wizard.

To finalize your setup open your browser to:
https://WIN-VKQ4M94L4Q6.demoserver.com:9999/pingfederate/app

3. Click the link provided on the screen to open the PingFederate administrative console in a browser where you can begin the initial setup.

   ⓘ **Important:** On the PingFederate administrative console, select **Yes, Connect to PingOne for Enterprise** to begin your PingFederate Bridge setup.

Setting up PingFederate Bridge

The first time you open the PingFederate Bridge administrative console, you see the initial setup screen, from which you can begin setting up PingFederate Bridge. Each screen has online help, which you can access by clicking the question mark icon (?) located in the top right corner.

Opening the PingFederate Bridge administrative console

About this task

The PingFederate Bridge administrative console is built around a system of wizard-like control screens, in which you configure various settings and components to support your federation use cases.

Steps

1. Make sure that the PingFederate Bridge service is running.
2. Start a web browser.
3. Browse to the following URL:

   `https://<pf_host>:9999/pingfederate/app`

   where *<pf_host>* is the network address of your PingFederate Bridge server. It can be an IP address, a host name, or a fully qualified domain name. It must be reachable from your computer.

Managing SSL server certificates

Use the **Security # SSL Server Certificates** screen to establish and maintain the certificates presented for access to the PingFederate Bridge administrative console (or the administrative API) and for incoming HTTPS connections at runtime.

The first system-generated certificate is the default certificate for both the administrative console and the runtime server. As multiple certificates are created, they can be activated (or deactivated) for the administrative console, the runtime server, or both. Additionally, any of them may be selected as the new default certificate for the administrative console, the runtime server, or both at a latter time.

When creating a certificate, additional domain names may be added through the use of the **Subject Alternative Names** field. Furthermore, if a user agent includes the host name that it intends to reach as part of the TLS handshake, PingFederate Bridge selects the applicable certificate based on the provided SNI (Server Name Indication) information. The selection looks at the common name and subject alternative names of each activated certificate. If PingFederate Bridge finds no match, it serves the default certificate. If PingFederate Bridge finds multiple matches, it serves the certificate with the better match. Consider the following sample configuration and inbound requests.

SSL Server Certificates configuration

Certificate	Common name	Subject alternative names	Activation status
#1	`www.example.com`	(None)	Administrative console and runtime server
#2	`www.example.org`	`*.example.org` and `test.example.local`	Administrative console and runtime server
#3	`www.example.info`	`*.example.info` and `*.example.com`	Administrative console and runtime server
#4	`admin.example.local`	(None)	Administrative console (Default) and runtime server
#5	`runtime.example.local`	(None)	Administrative console and runtime server (Default)

Runtime behavior

Request type	Host name from SNI	Certificate served
Administrative or runtime	www.example.com	The host name from the SNI is an exact match to the common name of certificate #1 and a partial match to the second subject alternative name (`*.example.org`) of certificate #3. An exact match is a better match; therefore, PingFederate serves certificate #1.

Request type	Host name from SNI	Certificate served
Administrative or runtime	www.example.org	The host name from the SNI is an exact match to the common name of certificate #2. PingFederate serves certificate #2.
Administrative or runtime	sso.example.org	The host name from the SNI is a partial match to the first subject alternative name (`*.example.org`) of certificate #2. There is no other exact or partial match. PingFederate serves certificate #2.
Administrative or runtime	sso.example.info	The host name from the SNI is a partial match to the first subject alternative name (`*.example.info`) of certificate #3. There is no other exact or partial match. PingFederate serves certificate #3.
Administrative or runtime	sso.example.com	The host name from the SNI is a partial match to the second subject alternative names (`*.example.com`) of certificate #3. There is no other exact or partial match. PingFederate serves certificate #3.
Administrative	www.example.local	The host name from the SNI does not match any configured certificate. PingFederate serves certificate #4, the default certificate for the administrative console.
Runtime	localhost	The host name from the SNI does not match any configured certificate. PingFederate serves certificate #5, the default certificate for the runtime server.

ⓘ **Note:**

If PingFederate Bridge finds multiple certificates of the same matching quality, it returns one of them in the TLS handshake. This response should not impact the user agent because either the common name or one of the subject alternative names matches the host name of the request. If PingFederate should always serve a particular certificate for any given host name, ensure that the common name and any configured subject alternative names do not overlap among multiple certificates.

Creating a new certificate

Steps

1. On the **SSL Server Certificates** screen, click **Create new**.

2. On the **Create Certificate** screen, enter the required information.

   For information about each field, refer to the following table:

Field	Description
Common Name	The common name (CN) identifying the certificate.
Subject Alternative Names	The additional DNS names or IP addresses that can be associated with the certificate.
Organization	The organization (O) or company name creating the certificate.
Organizational Unit	The specific unit within the organization (OU).
City	The city or other primary location (L) where the company operates.
State	The state (ST) or other political unit encompassing the location.
Country	The country (C) where the company is based.
Validity (days)	The time during which the certificate is valid.
Cryptographic Provider	The storage facility of the certificate. Applicable and visible only when PingFederate is integrated with an HSM in hybrid mode. ▪ Select **HSM** to store the certificate in the HSM. ▪ Select **Local Trust Store** to store the certificate in the local trust store managed by PingFederate.
Key Algorithm	A cryptographic formula used to generate a key. PingFederate uses either of two algorithms, RSA or EC.
Key Size (bits)	The number of bits used in the key. (RSA-1024, 2048 and 4096; and EC-256, 384 and 521.)
Signature Algorithm	The signing algorithm of the certificate. (RSA-SHA256, SHA384, and SHA512; and ECDSA-SHA256, SHA384, and SHA512.)

> **Note:**
>
> When using PingFederate Bridge with the Thales nShield Connect HSM, it is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.
>
> Select **RSA** and an RSA signing algorithm from the **Key Algorithm** list and the **Signature Algorithm** list, respectively.

3. When finished, click **Next**.
4. On the **Summary** screen, review your configuration, amend as needed, click **Save** to keep your configuration or click **Cancel** to discard it.

Importing a certificate and its private key

Steps

1. On the **SSL Server Certificates** screen, click **Import**.

2. On the **Import Certificate** screen, choose the applicable certificate file and enter its password.

   ⓘ **Note:**

   If PingFederate Bridge is integrated with an HSM from Thales, it is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.

   You must select a certificate that uses the RSA key algorithm.

   If PingFederate Bridge is integrated with an HSM in hybrid mode, select the storage facility of the certificate from the **Cryptographic Provider** list.

   - Select **HSM** to store the certificate in the HSM.
   - Select **Local Trust Store** to store the certificate in the local trust store managed by PingFederate Bridge.
3. On the **Summary** screen, review your configuration, amend as needed, click **Save** to keep your configuration or click **Cancel** to discard it.

Creating a certificate-authority signing request (CSR)

Steps

1. On the **SSL Server Certificates** screen, select **Certificate Signing** under **Action** for the certificate.

   ⓘ **Note:**

   This selection is inactive if you have not yet saved a newly created or imported certificate. Click **Save** and then return to this screen to initiate the process.

   The selection is also inactive if a previously signed certificate has been revoked. Because the revocation may indicate that the private key has been compromised, the best practice is to import or create a replacement certificate for certificate signing.
2. On the **Certificate Signing** screen, select the **Generate CSR** option.
3. On the **Generate CSR** screen, click **Export** to save the CSR file and click **Done**.

   Once saved, you can submit this CSR file to a certificate authority (CA) for a CA-signed certificate.

Importing a certificate-authority response (CSR response)

Steps

1. On the **SSL Server Certificates** screen, select **Certificate Signing** under **Action** for the certificate.
2. On the **Certificate Signing** screen, select the **Import CSR Response** option.
3. On the **Import CSR Response** screen, choose the applicable CSR response file.
4. On the **Summary** screen, review your configuration, click **Save** to keep your configuration or click **Cancel** to discard it.

Exporting a certificate

Steps

1. On the **SSL Server Certificates** screen, select **Export** under **Action** for the certificate.

2. On the **Export Certificate** screen, select the export type.
   - Select **Certificate Only** to export the selected certificate without its private key. This is the default choice.
   - Select **Certificate and Private Key** to export the selected certificate with its private key.

     ⓘ CAUTION:

     This export contains the private key of the certificate. You must also enter an encryption password.

     If the selected certificate is stored in an HSM, the **Certificate and Private Key** option does not apply.
3. On the **Export & Summary** screen, click **Export** to save the certificate file and then click **Done**.

Reviewing a certificate

Steps

1. On the **SSL Server Certificates** screen, select the certificate by its serial number.
2. Review the selected certificate in the pop-up window.

Activating or deactivating a certificate

Steps

1. On the **SSL Server Certificates** screen, select the relevant option under **Action** for the certificate.

   Any certificate can be activated for the administrative console, the runtime server, or both.

   When multiple certificates are activated for the administrative console (or the runtime server), you can deactivate any of them as long as one certificate remains active. Additionally, you can select any of them as the default certificate.
2. Click **Save** to keep your configuration or click **Cancel** to discard it.

Removing a certificate

Steps

1. On the **SSL Server Certificates** screen, select **Delete** under **Action** for the certificate.

   If the selected certificate is activated for the administrative port, the runtime port, or both, the **Delete** option does not apply.

   To cancel the removal request, select **Undelete** under **Action** for the certificate.
2. Click **Save** to confirm your action.

Configuring the Active Directory environment

About this task

To enable Kerberos authentication, you must make several Active Directory configuration changes to grant PingFederate Bridge access to the domain and add the domain to PingFederate Bridge.

ⓘ **Important:**

Do not configure subdomains if the parent domain in the same forest has already been configured.

ⓘ **Note:**

You must have Domain Administrator permissions to make the required changes.

Steps

1. Create a domain user account that PingFederate Bridge can use to contact the Kerberos Key Distribution Center (KDC). The account should belong to the Domain Users group. We recommend that the password be set with no expiration.
2. Use the Windows utility **`setspn`** to register SPN directory properties for the account by executing the following command on the domain controller:

   ```
   setspn -s HTTP/<pf-idp.domain.name> <pf-server-account-name>
   ```

   where:

   <pf-idp.domain.name>

   The canonical name of the PingFederate Bridge server.

   For more information on "canonical name", see *the IETF specifciation*.

   <pf-server-account-name>

   The domain account you want to use for Kerberos authentication.

   ⓘ **Note:**

   When executing the **`setspn`** command, `HTTP` must be capitalized and followed by a forward-slash (`/`).
3. Verify that the registration was successful by executing the following command:

   ```
   setspn -l <pf-server-account-name>
   ```

   This gives you a list of SPNs for the account. Verify that `HTTP/<pf-idp.domain.name>` is one of them.

   ⓘ **Note:**

   After making an SPN change, any end-users already authenticated must re-authenticate (close the browser or log off and back on) before attempting SSO.

Configuring end-user browsers

About this task

You must also configure browsers at your site in order to use the Kerberos Adapter to authenticate users.

ⓘ **Note:** The client-side configuration requires the base URL or an applicable virtual host name of your PingFederate Bridge environment. Base URL is defined on the **System**# **Protocol Settings**# **Federation Info** screen. Virtual host names, if configured, are defined on the **System**# **Virtual Host Names** screen.

ⓘ **Important:** If the browsers are not properly configured, users may be prompted to authenticate manually using their network credentials or fail to SSO to the service providers.

Steps

- Refer to subsequent topics for configuration steps.

Configuring Microsoft Internet Explorer

About this task

To configure Internet Explorer for Kerberos authentication, review the following settings in Internet Options.

Steps

1. Add the base URL to **Local intranet**.

   ⓘ **Note:** This step may be skipped if the base URL (<*pf-idp.domain.name*>) is internal and not fully qualified. For example, if it is `pingfederatebridge`, you can skip this step. However, if <*pf-idp.domain.name*> is `www.example.com`, then you must add the base URL to the **Sites** list, as described in the following sub steps.

   a. Close all Internet Explorer tabs and windows.
   b. Open **Control Panel**# **Internet Options**.
   c. Click the **Security** tab.
   d. Select **Local intranet** and click **Sites**.
   e. Click **Advanced**.
   f. Enter the base URL (for example, `www.example.com`), and then click **Add**.
   g. Click **Close**, and then click **OK** to return to the Security tab.
2. Verify **Automatic logon only in the Intranet zone** is selected.
   a. Under the Security tab, select **Local intranet** and click **Custom level**.
   b. Verify **Automatic logon only in the Intranet zone** is selected in the **Settings** pane.
   c. Click **OK** to return to the Security tab.
3. Verify proxy settings.

   ⓘ **Note:** Skip the following sub steps if a proxy is not used.

   a. Click the **Connections** tab.
   b. Click **LAN settings**.
   c. Verify the **Use a proxy server for your LAN ...** check box is selected, and then click **Advanced**.
   d. Enter the base URL in the **Exceptions** field, and then click **OK**.
   e. Click **OK** to return to the Connections tab.
4. Verify **Enable Integrated Windows Authentication** is selected.
   a. Click the **Advanced** tab.
   b. Verify **Enable Integrated Windows Authentication** is selected in the **Settings** pane.
5. Click **OK** to close Internet Options.

Configuring Mozilla Firefox

About this task

To configure Firefox for Kerberos authentication, configure Firefox as follows:

Steps

1. Start Firefox.
2. Open a new tab, and then enter `about:config` in the address bar.
3. Search for the `network.negotiate-auth.trusted-uris` preference name.
4. Double-click to modify its value to include the base URL of your PingFederate Bridge environment (for example, `www.example.com`).
5. Click **OK** and close the `about:config` tab.
6. Optional: Exit Firefox.

Contextual help topics

PingOne Account

About this task

On the **PingOne Account** tab, you can connect PingFederate Bridge to PingOne for Enterprise to deploy a powerful on-premise and cloud-based hybrid solution.

To connect PingFederate Bridge to PingOne for Enterprise:

Steps

1. Select **Yes, Connect to PingOne for Enterprise**.

   A link and an **Activation Key** field appear.
2. Click **Sign on to PingOne to get your activation key**.

   The Ping Identity **Sign On** screen opens.
3. Enter your PingOne for Enterprise account credentials and click **Sign On**.

   The **Activation Key** screen opens.
4. Copy the activation key, and click **Save**.
5. Return to PingFederate, and paste the key into the **Activation Key** field.
6. Click **Next**.

Identities

About this task

On the **Identities** tab, choose whether to connect PingFederate Bridge to a directory server. If you connect to a directory server, LDAP is used for user lookup and credential validation.

ⓘ **Note:**

You do not need to use a directory server if you are only using PingID VPN or if you are configuring PingFederate Bridge to function as a test identity provider. If this is the case, select **No, Don't Connect a Directory Server** and click **Next**.

To connect to a directory server:

Steps

1. Select **Yes, Connect a Directory Server**.

   Configuration fields appear.
2. Enter information in the fields that is appropriate for your directory server.

   Directory Type

   Select the type of directory server that you are using.

   Data Store Name

   Enter the name of the data store representing the directory server.

   Hostname

   Enter the IP address or the fully qualified domain name of the directory server.

   Service Account DN

   Enter the distinguished name (DN) of the service account that PingFederate Bridge can use to communicate with the directory server.

   Password

   Enter the service account password.

   Search Base

   Enter the DN of the location of the directory where PingFederate Bridge begins its data store queries.

   Search Filter

   Optionally, enter the LDAP query to locate a user record for attribute lookup and potentially credential validation. The default value is `sAMAccountName=${username}` for Active Directory, and `uid={$username}` for PingDirectory and Oracle Directory Server.

   Note:

   If you update this field, make sure to enter a valid LDAP filter. For more information, consult your directory administrators.
3. Click **Next**.

   PingFederate Bridge tries to establish a secure (LDAPS) connection to the directory server.

Identities

About this task

On the **Identities** tab, choose whether to connect PingFederate Bridge to a directory server. If you connect to a directory server, LDAP is used for user lookup and credential validation.

Note:

You do not need to use a directory server if you are only using PingID VPN or if you are configuring PingFederate Bridge to function as a test identity provider. If this is the case, select **No, Don't Connect a Directory Server** and click **Next**.

To connect to a directory server:

Steps

Select **Yes, Connect a Directory Server**.

You can create a new data store or reuse an existing data store in this configuration.

Create a new data store

Provide the required information to connect to a directory server and then click **Next**.

For more information about each field, refer to the following table.

Field	Description
Directory Type	Select the type of the directory server from the list. Refer to *System requirements* on page 4 for a list of supported directory servers.
Data Store Name	Enter the name of the data store.
Hostname	Enter the location of the directory server. It can be the IP address, the host name, or the fully qualified domain name of the directory server. The entry may include a port number.
Service Account DN	Enter the distinguished name (DN) of the service account that PingFederate Bridge can use to communicate with the directory server.
Password	Enter the password associated with the service account.
Search Base	Enter the DN of the location in the directory where PingFederate Bridge begins its data store queries.
Search Filter	Enter the LDAP query to locate a user record for attribute lookup and potentially credential validation. The default value is either `sAMAccountName=${username}` or `uid=${username}`, depending on the selected directory type. If you require a more advanced search filter, ensure the value is a valid LDAP filter. For more information, consult your directory administrators.

When you click **Next**, PingFederate tries to establish a secure (LDAPS) connection to the directory server.

Use an existing data store

Click **Begin** and then follow the on-screen instructions to create an SP connection to PingOne for Enterprise.

Unsecure Connection or Certificate Error

You see the **Unsecure Connection** tab if your directory server does not support LDAPS. If you want to continue without a secure connection, click **Next**. Alternatively, you can click **Previous** to go back to the **Identities** tab and specify a different directory server.

You see the **Certificate Error** tab if the certificate presented by the directory server is not trusted by PingFederate Bridge. You can click **Choose Certificate** to import a certificate used by the directory server to establish a secure connection and then click **Next**. Alternatively, you can click **Previous** to go back to the **Identities** tab and specify a different directory server.

Use Cases

On the **Use Cases** tab, select what you plan to use PingFederate Bridge to do.

PingOne SSO

Select this option and click **Next** if you want to enable single sign-on with PingOne for Enterprise and your configured identity store. For more information about using PingOne SSO, see *SSO with PingOne* in the *PingOne for Enterprise Administration Guide*.

ⓘ **Note:**

If you have not connected to an LDAP directory, the system configures test user accounts.

Optionally, you can enable Kerberos authentication (if you are using Active Directory). You can also enable user provisioning. To do this, select **Additional SSO Features**, and click **Begin**. After you have finished the Kerberos and provisioning configuration, you will be returned to the **Use Cases** tab.

PingID VPN (RADIUS)

Select this option and click **Next** if you want to configure PingFederate Bridge to integrate with a RADIUS server to support PingID multi-factor authentication through your virtual private network. When you select this option, a **Begin** button appears. Click **Begin**.

For more information about using PingID VPN, see *Integrate PingID with your VPN/Remote access system* in the *PingID Administration Guide*.

PingOne SSO

Kerberos Authentication

About this task

If you are using Active Directory, you see the **Kerberos Authentication** tab, on which you can optionally configure Kerberos-based authentication for Windows users.

If you do not want to configure Kerberos authentication, click **Next**.

To configure Kerberos authentication:

Steps

1. Select the **Configure Kerberos Authentication** check box to display the configuration fields.
2. Enter the following information:

   Realm Name

   Enter the Kerberos realm name.

   Realm Username

   Enter the Kerberos username.

Realm Password

Enter the Kerberos password.

Internal IP Ranges (At Least One Required)

Enter one or more internal IP ranges in CIDR notation to indicate the boundaries of your network, and click **Add**.

KDC Hostnames (Optional)

Optionally, enter a Kerberos Key Distribution Center (KDC) hostname and click **Add**. You can add multiple KDC hostnames. If you do not specify a hostname, PingFederate Bridge uses a DNS query to find a list of KDCs.

3. Click **Next**.

Provisioning

About this task

On the **Provisioning** tab, you can configure the provisioning of users from your directory server to PingOne for Enterprise. In this configuration, you specify the group where PingFederate Bridge should look for member users and update PingOne for Enterprise when their email address, first name, or last name has changed. When PingFederate Bridge detects that a user has been removed from the specified group or disabled in the directory server, PingFederate Bridge sends an update to PingOne for Enterprise to disable the PingOne for Enterprise service for that account.

Steps

1. Select **Configure Provisioning**.
2. Under **Group DN**, enter the distinguished name (DN) of the group for which you are configuring user provisioning.

   The specified group must reside under the hierarchy of the previously defined **Search Base** value (as described in *Identities* on page 21).
3. Select **Nested** if you want PingFederate Bridge to monitor changes for users through nested group membership.
4. Click **Next**.

Summary

About this task

The **Summary** tab contains a summary of your single sign-on configuration.

Steps

1. Review your configuration.
2. If a setting is incorrect, click **Previous** and navigate to the information that needs to change. Make your changes and click **Next** until you see the **Summary** tab again.
3. When you are satisfied with your configuration, click **Done**.

PingID VPN (RADIUS)

Basic Settings

About this task

The **Basic Settings** tab contains configuration settings for connecting to your RADIUS server.

ⓘ **Note:** You see the **Validate User Credentials** and **PingID Username Attribute** fields only if you configured LDAP on the **Identities** tab.

Steps

1. Enter information in the following fields:

   Client IP

   Enter the IP address of the VPN RADIUS client.

   Client Shared Secret

   Enter the password shared between PingFederate Bridge and the RADIUS server used to encrypt passwords.

   Server Authentication Port

   Enter the UDP port used to authenticate to the RADIUS server. Port number 1812 is provided by default.

   Validate User Credentials

   Enter the **Validate with LDAP** option if you want to use LDAP to validate credentials. This option is displayed only when an LDAP directory is connected.

   PingID Username Attribute

   Enter the LDAP attribute that represents the user identifier in PingID.
2. Click **Next**.

Provisioning

About this task

On the **Provisioning** tab, you can configure the provisioning of users from your directory server to PingID. In this configuration, you specify the group where PingFederate Bridge should look for member users and update PingID when their email address, first name, or last name has changed. When PingFederate Bridge detects that a user has been removed from the specified group or disabled in the directory server, PingFederate Bridge sends an update to PingID to disable the PingID service for that account.

Steps

1. Select **Configure Provisioning**.
2. Under **PingID Group DN**, enter the distinguished name (DN) of the group for which you are configuring user provisioning.

   The specified group must reside under the hierarchy of the previously defined **Search Base** value (as described in *Identities* on page 21).
3. Select **Nested** if you want PingFederate Bridge to monitor changes for users through nested group membership.

4. Click **Next**.

Summary

About this task

The **Summary** tab contains a summary of your PingID VPN configuration.

Steps

1. Review your configuration.
2. If a setting is incorrect, click **Previous** and navigate to the information that needs to change. Make your changes and click **Next** until you see the **Summary** tab again.
3. When you are satisfied with your configuration, click **Done**.

Basic Information

About this task
The **Basic Information** tab contains your base URL. Users will access this URL when interacting with PingFederate Bridge.

Steps

1. Change the base URL if needed.

   The domain portion of the base URL should match the domain name of your organization because it is part of the address where your applications, users, and partners communicate with your PingFederate Bridge environment. You can update this URL as needed.
2. Click **Next**.

Confirmation

The **Confirmation** tab displays a summary of the configuration that will be applied to PingFederate Bridge. Click **Next** to apply the configuration.

Complete

About this task

The **Complete!** tab congratulates you on successfully setting up PingFederate Bridge.

Steps

1. Make a note of the instructions under **What's Next?** You will need to complete these tasks when you begin configuring PingFederate Bridge.
2. Click **Done**.