IDaaS Directory Provisioner

Contents

IDaaS Directory Provisioner

The PingFederate IDaaS Directory Provisioner enables an enterprise to provision its users to the PingOne for Enterprise IDaaS Directory. This connector includes a quick connection template to easily set up SCIM provisioning.

Features

- Outbound user provisioning

Intended audience

This document is intended for PingFederate administrators.

If you need help during the setup process, see the following resources:

- *PingOne for Enterprise IDaaS Directory*
- *How PingOne for Enterprise Works*
- *How to Manage PingOne for Enterprise Directory Users*
- *Selecting a PingOne for Enterprise Directory*

System requirements

- PingFederate 7.3 or later with Java 8
- To allow PingFederate to make outbound connections to IDaaS Directory, you might need to allow the following endpoint in your firewall:
  - North America: https://directory-api.pingone.com/api
  - Europe: https://directory-api.pingone.eu/api
  - Australia: https://directory-api.pingone.com.au/api

User management

The IDaaS Directory Provisioner synchronizes users from your datastore to IDaaS Directory. The following describes the behavior of each provisioning capability.

> ⓘ **Tip:**
>
> You can configure the following capabilities and specify which users to provision when you get to the *Configure provisioning* on page 6 part of the setup process.

Synchronizing existing users

PingFederate synchronizes users based on the `Username` attribute in IDaaS Directory. If a user already exists in your datastore and IDaaS Directory, mapping this attribute correctly links the two records together.

For example:

- In IDaaS Directory, Janet's `Username` is `jsmith@domain.com`.
- In your datastore, Janet's `mail` is `jsmith@domain.com`.
- On the **Attribute Mapping** tab of your provisioning connection configuration, map the `Username` attribute to `mail`.

- When the provisioning connector runs, the datastore user is provisioned with a `Username` of `jsmith@domain.com`. That matches Janet's existing `Username` in IDaaS Directory, so her information in the datastore is synchronized to her IDaaS Directory account.

User provisioning

PingFederate provisions users when any of the following happens:

- A user is added to the datastore group or filter that is targeted by the provisioning connector.
- A user with `disabled` status is added to the datastore group or filter that is targeted by the provisioning connector, and the **Provision disabled users** provisioning option is enabled. This feature is not available in all provisioning connectors.

ⓘ **Tip**:

You can define which users PingFederate targets for provisioning on the **Source Location** tab of your provisioning connection configuration.

User updates

PingFederate updates users when a user attribute changes in your datastore.

ⓘ **Tip**:

You can define which attributes PingFederate monitors for changes on the **Attribute Mapping** tab of your provisioning connection configuration.

User deprovisioning

PingFederate deprovisions users when any of the following happens:

- A user is deleted from the user store.
- A user is disabled in the user store.
- A user is removed from the datastore group or filter that is targeted by the provisioning connector.

Setup

Getting started

About this task

Before configuring this connector, you will need to complete the following steps.

ⓘ **Tip**: For additional information, see *View or renew directory API credentials* in the PingOne for Enterprise documentation.

Obtain your Client ID & API key

Steps

1. Log into PingOne as an administrative user.
2. Select **Setup**, followed by **Directory**

3. Select **API Credentials**.
4. Copy the **Client ID** and **API Key** values to use in the next section.

Install the connector

About this task

This section describes the common steps required to install the PingFederate IDaaS Directory Connector.

Steps

1. Stop the PingFederate server if it is running.
2. Unzip the PingFederate IDaaS Directory Connector distribution `.zip` archive.
3. Copy the contents of the `dist` directory into the directory:

   ```
   <pf_install>/pingfederate/server/default/deploy
   ```
4. Optional: If you plan to use the connector for Outbound Provisioning, edit the `run.properties` file located in `<pf_install>/pingfederate/bin`, changing the property `pf.provisioner.mode` to `STANDALONE.`For example:

   ```
   pf.provisioner.mode=STANDALONE
   ```

   ⓘ **Note:** For information about using the FAILOVER setting for runtime deployment, see *Deploying provisioning failover* in the PingFederate documentation.
5. Start the PingFederate server.

Enable outbound provisioning

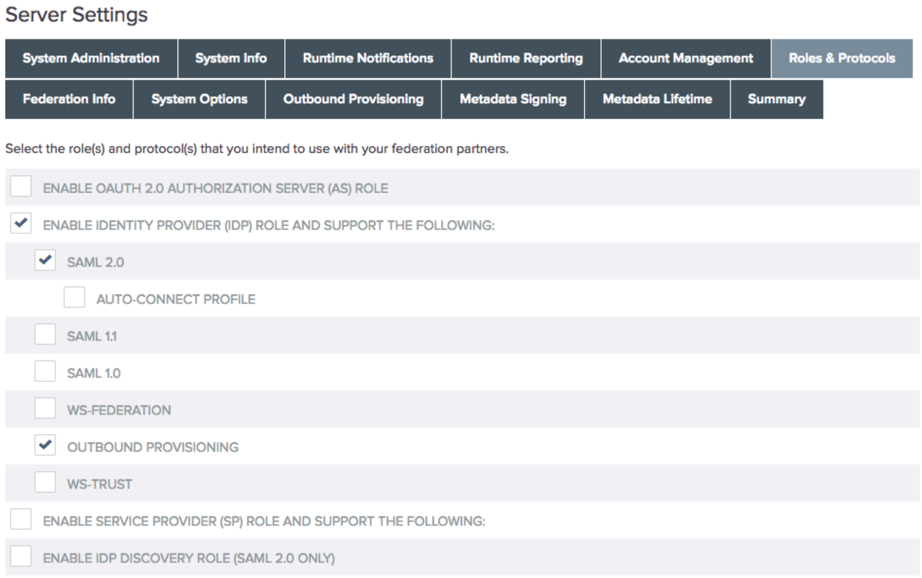
About this task

After enabling outbound provisioning in the `<pf_install>/pingfederate/bin/run.properties` file, you must also activate the outbound provisioning role in the administrative console.

Steps

1. Go to the **Server Configuration** # **Server Settings** # **Roles & Protocol** screen.

2. Select the **Outbound Provisioning** check box.



Server Settings

Select the role(s) and protocol(s) that you intend to use with your federation partners.

- □ ENABLE OAUTH 2.0 AUTHORIZATION SERVER (AS) ROLE
- ☑ ENABLE IDENTITY PROVIDER (IDP) ROLE AND SUPPORT THE FOLLOWING:
  - ☑ SAML 2.0
    - □ AUTO-CONNECT PROFILE
  - □ SAML 1.1
  - □ SAML 1.0
  - □ WS-FEDERATION
  - ☑ OUTBOUND PROVISIONING
  - □ WS-TRUST
- □ ENABLE SERVICE PROVIDER (SP) ROLE AND SUPPORT THE FOLLOWING:
- □ ENABLE IDP DISCOVERY ROLE (SAML 2.0 ONLY)

> **Note:** Enabling outbound provisioning adds the outbound provisioning screen, requiring the selection of a database to facilitate provisioning. For more information, see *Configuring outbound provisioning* in the PingFederate documentation.

Configure provisioning

About this task

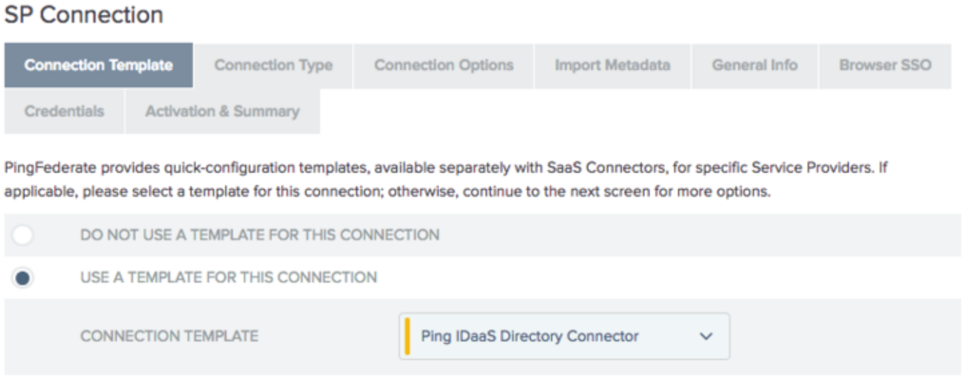
This procedure provides instructions for configuring provisioning for the PingFederate IDaaS Directory Connector.

Outbound provisioning details are managed within an SP connection. You can configure outbound provisioning with or without Browser SSO, WS-Trust STS, or both when you create a new SP connection. You also the option to add outbound provisioning to an existing SP connection.

Steps

1. In the PingFederate administrator console, configure the data store that PingFederate will use as the source of user data. For instructions, see *Datastores* in the PingFederate documentation.
   - When targeting users and groups for provisioning, exclude the user account that you will use to administer users in your connection to IDaaS Directory. This prevents the PingFederate provisioning engine from interfering with the account that provisions users and groups.
2. Create a new SP connection or select an existing SP connection from the **SP Configuration** menu.

3. On the Connection Template screen, select the **Use a template for this connection** option and choose **Ping IDaaS Directory Connector** from the Connection Template drop-down list.



PingFederate provides quick-configuration templates, available separately with SaaS Connectors, for specific Service Providers. If applicable, please select a template for this connection; otherwise, continue to the next screen for more options.

○ DO NOT USE A TEMPLATE FOR THIS CONNECTION

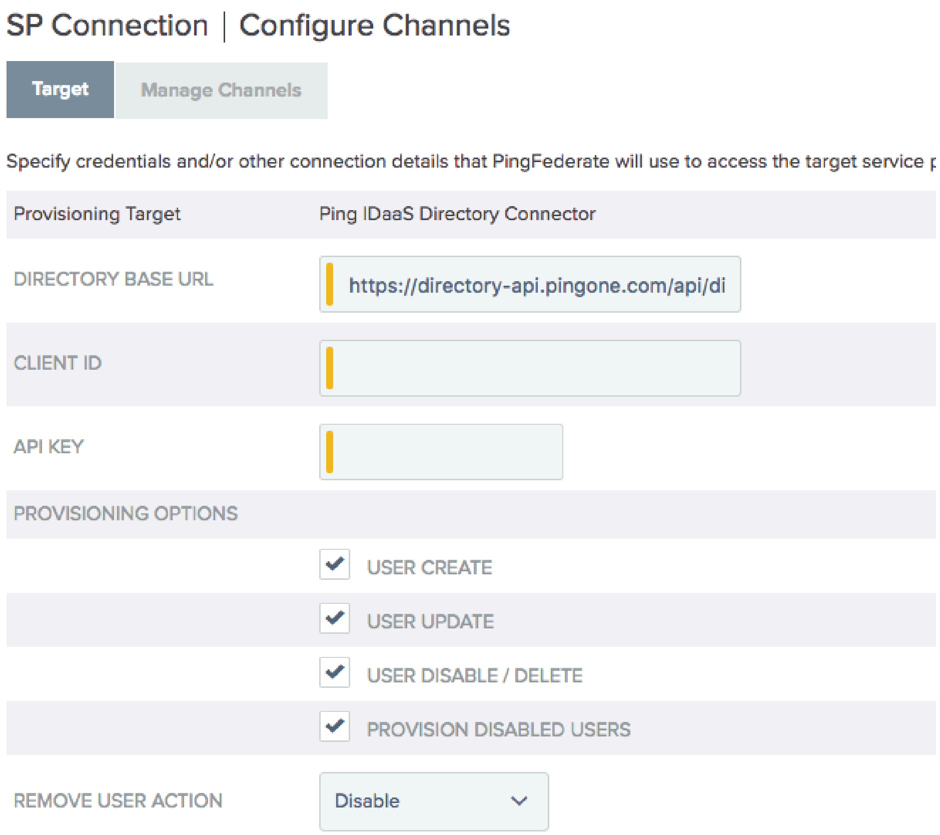
● USE A TEMPLATE FOR THIS CONNECTION

CONNECTION TEMPLATE: Ping IDaaS Directory Connector

Tip: If this selection is not available, verify the Connector installation and restart PingFederate.

4. On the **Connection Type** screen, ensure the **Outbound Provisioning** checkbox is selected, and the **Browser SSO Profiles** checkbox is unselected (if appropriate).
5. Follow the connection wizard to configure the connection.
6. On the **Outbound Provisioning** screen, click **Configure Provisioning**.

7. On the **Target** screen, enter the values for each field as required by the PingFederate IDaaS Directory Connector.



Specify credentials and/or other connection details that PingFederate will use to access the target service p

Provisioning Target	Ping IDaaS Directory Connector
DIRECTORY BASE URL	https://directory-api.pingone.com/api/di
CLIENT ID	
API KEY	
PROVISIONING OPTIONS	
	☑ USER CREATE
	☑ USER UPDATE
	☑ USER DISABLE / DELETE
	☑ PROVISION DISABLED USERS
REMOVE USER ACTION	Disable

Target screen options

Field Name	Description
Directory Base URL	The Directory Base URL for the Ping IDaaS Directory. The URL depends on the geographic setup of your IDaaS Directory tenant: ▪ North America (default): `https://directory-api.pingone.com/api` ▪ Europe: `https://directory-api.pingone.eu/api` ▪ Australia: `https://directory-api.pingone.com.au/api`
Client ID	The Client ID for your PingFederate IDaaS Directory account. For more information on obtaining a Client ID and API Key, see *Getting started* on page 4.
API Key	The API Key for your PingFederate IDaaS Directory account.For more information on obtaining a Client ID and API Key, see *Getting started* on page 4

Field Name	**Description**
Provisioning Options	
User Create	**True** (default) – Users will be created in the target application. **False** – Users will not be created in the target application. ⓘ **Note:** The provisioner.log will display a warning within the create user workflow that the user was not created in the target application.
User Update	**True** (default) – Users will be updated in the target application. PingFederate can also re-enable disabled users. **False** – Users will not be updated in the target application. ⓘ **Note:** The provisioner.log will display a warning within the update user workflow that the user was not updated in the target application.
User Delete / Disable	**True** (default) – Users will be disabled or deleted in the target application. ⓘ **Note:** A disabled user can only be re-enabled if **User Update** is true. **False** – Users will not be disabled or deleted in the target application. ⓘ **Note:** The provisioner.log will display a warning within the disable user workflow that the user was not disabled in the target application.
Provision Disabled Users	This option is only applicable if User Create is set to True. **True** (default) – If a disabled user in the user store is targeted for provisioning, it will be created in a disabled state in the target application. **False** – If a disabled user in the user store is targeted for provisioning, it will be not be created in the target application. ⓘ **Note:** The provisioner.log will display a warning within the create user workflow indicating that the user was not created in target application.

Field Name	Description
Remove User Action	Select a deprovision method (Disable or Delete). Deprovisioning is triggered when previously provisioned users no longer meet the condition set in the Source Location screen, or when a user has been disabled or deleted from the data store. This option is only applicable if User Disable is set to True. **Disable** (default) – Deactivates the user account in the target application (also known as a Soft-Delete). **Delete** – Removes the user account in the target application (also known as a Hard-Delete) ⓘ **Note:** Some target applications do not support hard deleting users through external interfaces. For those applications we only support disabling the user.

8. Click **Next** to continue the provisioning configuration. For more information, see the following sections under *Outbound provisioning for IdPs* in the PingFederate documentation:

   - *Managing channels*
   - *Specifying channel information*
   - *Identifying the source datastore*
   - *Modifying source settings*
   - *Specifying a source location*
   - *Mapping attributes*
   - *Reviewing channel settings*

ⓘ **Note:** Credentials will be verified when the channel and SP connection is set to Active and provisioning is initiated.

ⓘ **Tip:** If you are not ready to complete the provisioning configuration, you can click **Save** and return to the configuration page later (from the Manage Connections page – select **Manage All SP** on the Main Menu).

Supported attributes reference

The following table consists of the attributes that can be mapped for user provisioning. For more information on IDaaS Directory SCIM attributes, see the SCIM Schema section of the *SCIM 1.1 Developer Guide* on the Ping Identity site.

Attribute	Description
userName	The name to assign to the account user. The name must be unique within the account. **This attribute is required.**
givenName	The given name of the User, or first name in most Western languages (e.g., "Barbara" given the full name "Ms. Barbara Jane Jensen, III").
familyName	The family name of the User, or last name in most Western languages (e.g., "Jensen" given the full name "Ms. Barbara Jane Jensen, III").

Attribute	Description
middleName	The middle name(s) of the User (e.g., "Jane" given the full name "Ms. Barbara Jane Jensen, III").
honorificPrefix	The honorific prefix(es) of the User, or title in most Western languages (e.g., "Ms." given the full name "Ms. Barbara Jane Jensen, III").
honorificSuffix	The honorific suffix(es) of the User, or suffix in most Western languages (e.g., "III" given the full name "Ms. Barbara Jane Jensen, III").
formattedName	The full name, including all middle names, titles, and suffixes as appropriate, formatted for display (e.g., "Ms. Barbara Jane Jensen, III").
workEmail	Work email for the User (e.g., "bjensen@example.com").
displayName	The name of the User, suitable for display to end-users. Each User returned MAY include a non-empty displayName value. The name should be the full name of the User being described (e.g., "Babs Jensen" or "Ms. Barbara J Jensen, III") but MAY be a username or handle. The value provided should be the primary textual label by which this User is normally displayed by the service provider when presenting it to end-users.
title	The User's title, such as "Vice President".
externalId	A String that is an identifier for the resource as defined by the provisioning client.
password	This attribute is intended to be used as a means to set, replace, or compare (i.e., filter for equality) a password.
preferredLanguage	Indicates the User's preferred written or spoken languages and is generally used for selecting a localized User interface.
userType	Used to identify the relationship between the organization and the User. Typical values used might be "Contractor", "Employee", "Intern", "Temp", "External", and "Unknown", but any value may be used.
locale	Used to indicate the User's default location for purposes of localizing such items as currency, date time format, or numerical representations.
nickName	The casual way to address the User in real life, e.g., "Bob" or "Bobby" instead of "Robert".
profileUrl	A URI that is a uniform resource locator that points to a location representing the User's online profile (e.g., a web page).
profilePhotoUrl	**(API use only)** A URI that is a uniform resource locator that points to the User's profile photo. The resource MUST be a file (e.g., a GIF, JPEG, or PNG image file) rather than a web page containing an image.
profileThumbnailUrl	**(API use only)** A URI that is a uniform resource locator that points to the User's profile thumbnail. The resource MUST be a file (e.g., a GIF, JPEG, or PNG image file) rather than a web page containing an image.
timezone	The User's time zone, in IANA Time Zone database format (e.g., "America/ Los_Angeles").
workPhone	The work phone number for the User (e.g., "+1-201-555-0123").
mobilePhone	The mobile phone number for the User (e.g., "+1-201-555-0123")
pagerPhone	The pager number for the User (e.g., "+1-201-555-0123")
faxPhone	The fax number for the User (e.g., "+1-201-555-0123")
homePhone	The home phone number for the User (e.g., "+1-201-555-0123")

Attribute	**Description**
otherPhone	Another phone number that can be used to reach the User (e.g., "+1-201-555-0123")
workStreetAddress	The work street address for the User, which may include house number, street name, P.O. box, and multi-line extended street address information.
workCity	The work city or locality component for the User's mailing address.
workState	The work state or region component for the User's mailing address.
workPostalCode	The work ZIP or postal code component for the User's mailing address.
workCountry	The work country component for the User's mailing address. When specified, the value MUST be in ISO 3166-1 "alpha-2" code format [*ISO3166*]; e.g., the United States and Sweden are "US" and "SE", respectively.
workFormattedAddress	The User's full work address, formatted for display.
homeStreetAddress	The home street address for the User, which may include house number, street name, P.O. box, and multi-line extended street address information.
homeCity	The home city or locality component for the User's mailing address.
homeState	The home state or region component for the User's mailing address.
homePostalCode	The home ZIP or postal code component for the User's mailing address.
homeCountry	The home country component for the User's mailing address. When specified, the value MUST be in ISO 3166-1 "alpha-2" code format [*ISO3166*]; e.g., the United States and Sweden are "US" and "SE", respectively.
homeFormattedAddress	The User's full home address, formatted for display.
otherStreetAddress	An alternate street address for the User, which may include house number, street name, P.O. box, and multi-line extended street address information.
otherCity	The alternate city or locality component for the User's mailing address.
otherState	The alternate state or region component for the User's mailing address.
otherPostalCode	The alternate ZIP or postal code component for the User's mailing address.
otherCountry	The alternate country component for the User's mailing address. When specified, the value MUST be in ISO 3166-1 "alpha-2" code format [*ISO3166*]; e.g., the United States and Sweden are "US" and "SE", respectively.
otherFormattedAddress	The alternate address for the User, formatted for display.
qqIm	The QQ instant messaging address for the User.
skypeIm	The Skype instant messaging address for the User.
gtalkIm	The Google Talk instant messaging address for the User.
aimIm	The AOL Instant Messenger instant messaging address for the User.
icqIm	The ICQ instant messaging address for the User.
yahooIm	The Yahoo Messenger instant messaging address for the User.
msnIm	The MSN Messenger instant messaging address for the User.
xmppIm	The XMPP instant messaging address for the User.
entitlements	A list of entitlements for the User that represent a thing the User has. An entitlement may be an additional right to a thing, object, or service.

Attribute	Description
roles	A list of roles for the User that collectively represent who the User is, e.g., "Student", "Faculty".
certificates	**(API use only)** A list of certificates associated with the resource (e.g., a User). Each value contains exactly one DER-encoded X.509 certificate (see *Section 4 of [RFC5280]*), which MUST be base64 encoded per *Section 4 of [RFC4648]*.

Release notes

Changelog

PingFederate IDaaS Directory Connector 1.0 – October 2017 (current release)

- Initial Release
- Added Support for User Provisioning
- Added configuration options for CRUD capabilities
- Added configuration options for provisioning disabled users
- Added configuration options for deprovisioning actions

Known issues and limitations

- Due to a limitation with PingFederate 8.1 and earlier versions, when configuring two SP connections with the same provisioner, the second connection built may be pre-populated with the channel from the first connection. To avoid conflicts, delete this pre-populated channel and create a unique channel for each connection.
- User attributes cannot be cleared once set.
- When an LDAP user is deleted in a targeted group distinguished name (DN), the provisioning connector does not propagate the deletion until a new user is added to the group. This limitation is compounded when the **User Create** provisioning option is disabled. For solutions, see *SaaS provisioner does not remove the user* in the Knowledge Base.
- Outbound Group Provisioning and Memberships is not supported.

Download manifest

The distribution `.zip` archive for the connector contains the following:

- `ReadMeFirst.pdf` – contains links to this online documentation.
- `/legal`:
  - `Legal.pdf` – copyright and license information.
- `/dist` – contains libraries needed for the Connector:
  - `pf-pingdirectory-quickconnection-1.0.jar` – PingFederate Ping IDaaS Directory Connector