PingFederate®

Twitter Cloud Identity Connector

Version 1.2

User Guide

Ping Identity®

PingFederate Twitter Cloud Identity Connector *User Guide*
Version 1.2
January, 2014

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

Phone: 877.898.2905 (+1 303.468.2882 outside North America)
Fax: 303.468.2909
Web Site: www.pingidentity.com

Trademarks

Disclaimer

Document Lifetime

Ping Identity may occasionally update online documentation between releases of the related software. Consequently, if this PDF was not downloaded recently, it may not contain the most up-to-date information. Please refer to the online documentation at documentation.pingidentity.com for the most current information.

From the Web site, you may also download and refresh this PDF if it has been updated, as indicated by a change in this date: **January 6, 2014**.

Contents

Introduction

This PingFederate Cloud Identity Connector allows a Service Provider (SP) to leverage Twitter as an Identity Provider (IdP) for access to Internet applications in the SP domain. The included PingFederate Twitter IdP Adapter works with the Twitter authentication Web service and its application programming interface (API) to allow PingFederate to perform single sign-on (SSO) to service applications.

Using the Connector, a Software-as-a-Service (SaaS) provider, for example, can provide customers direct SSO access to its applications. In addition, a service provider may leverage Twitter credentials for secure, standards-based SSO to services in other local domains or at partner sites, by using the Adapter in an SP partner connection. (For more information about identity-federation standards and partner connections, see "Key Concepts" in the PingFederate *Administrator's Guide*.)

Intended Audience

This document is intended for system administrators with experience in the configuration and maintenance of IT infrastructure. Knowledge of networking and user-management configuration is assumed. Some exposure to the PingFederate administrative console may be helpful.

Additional Resources

Administrators may want to review "SSO Integration Kits and Adapters" in the "Key Concepts" chapter of the PingFederate *Administrator's Guide*.

Tip: If you encounter any difficulties with configuration or deployment, please try searching the Ping Identity Support Center (`www.pingidentity.com/support`).

ZIP Manifest

The distribution ZIP file for the Twitter Cloud Identity Connector contains the following:

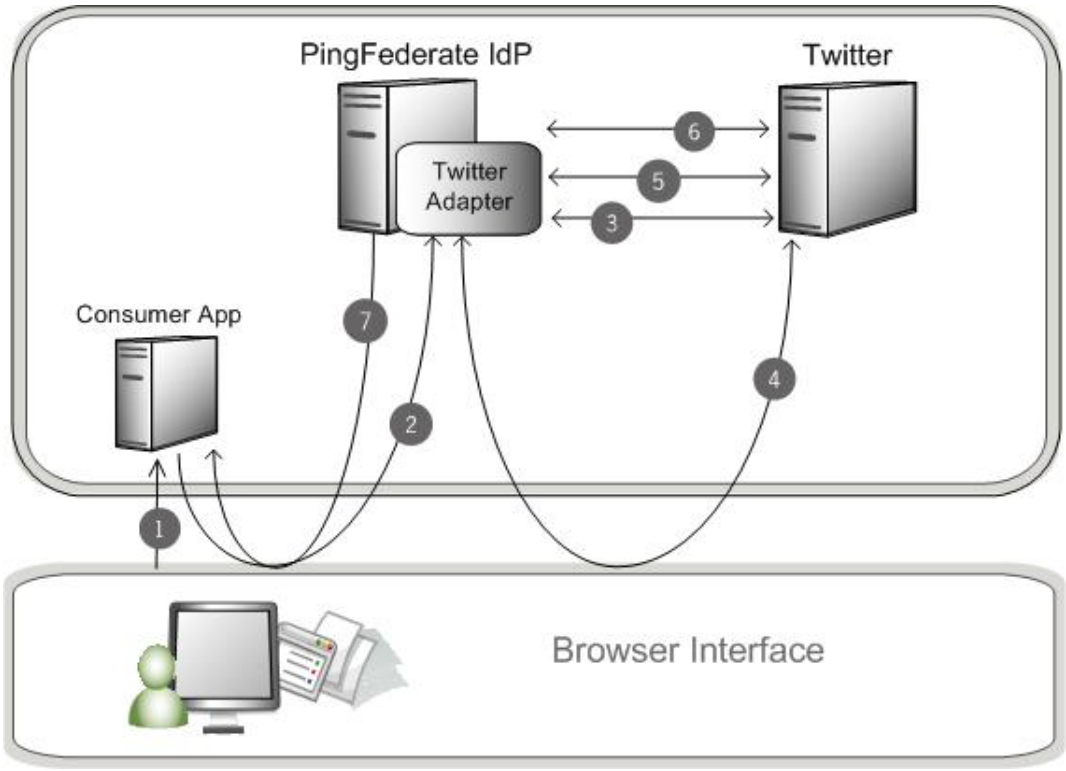
- `ReadMeFirst.pdf` – contains links to this online documentation.
- `/legal` - contains this document:
  - `Legal.pdf` - copyright and license information
- `/dist` – contains libraries needed for the Adapter
  - `pf-twitter-adapter-1.2.jar` – Twitter Adapter JAR file
  - `json-simple-1.1.jar` – JavaScript Object Notation (JSON) JAR file
  - `scribe-1.3.3.jar` – OAuth library for Java

System Requirements

The Twitter Adapter requires installation of PingFederate 6.2 or higher.

Processing Overview

The following figure illustrates an example SSO process flow using the Twitter Adapter:



Processing Steps

1. User navigates to a Web application and chooses to log on using his or her Twitter account.
2. The browser is redirected to the Twitter Adapter.
3. The Twitter Adapter requests a request token from Twitter. The Twitter Adapter callback URL is passed as a parameter with this request. Twitter returns the request token.
4. The PingFederate server redirects the user to Twitter for authentication, including the request token as a parameter. A list of requested permissions is provided in this call.

   If the user is not already logged on, Twitter challenges the user to authenticate. Twitter authenticates the user and provides a consent page for the user to authorize the sharing of information. Once the user authorizes, Twitter redirects the browser to the Twitter Adapter callback URL with a verification code.

   If the user does not authenticate, an error is returned rather than the verification code.
5. The Adapter makes an HTTP request to Twitter to obtain an access token, sending the request token and verification code as parameters. Twitter validates these components and returns an access token.
6. The Adapter uses the access token to retrieve user information from Twitter, and Twitter returns the user information.

Note: For optional, additional Twitter interaction using the access token, see the Twitter API documentation.

7. The Adapter redirects the user to the Web application with the user attributes.

Note: There are two ways for a PingFederate administrator to set up this process, depending on whether the service is part of the enterprise domain or outside that domain (see "Complete the Configuration" on page 10).

Installation and Configuration

The following sections describe how to set up and integrate the Twitter Cloud Identity Connector with your application:

- Install the Twitter Adapter
- Register the Twitter application
- Configure PingFederate
- Integrate Applications

Step 1 -- Install the Twitter Adapter

To install the Twitter Adapter:

1. Stop the PingFederate server if it is running.
2. If you are upgrading the Twitter Adapter, remove any previous release of the Twitter Adapter (`pf-twitter-adapter-1.x.jar`) from the directory:

   `<PF-install>/server/default/deploy`
3. Unzip the distribution ZIP file.
4. From the Twitter Connector `dist/` directory, copy:
   - `pf-twitter-adapter-1.2.jar`
   - `json-simple-1.1.jar`
   - `scribe-1.3.3.jar`

   into the same directory:

   `<PF-install>/server/default/deploy`
5. Start or restart PingFederate.

   (For more information, see "Starting and Stopping PingFederate" in the "System Administration" chapter of the PingFederate *Administrator's Guide*.)

Step 2 -- Register the Twitter Application

You must use a Twitter developer account to register PingFederate as a Twitter application.

Tip: Twitter navigational details and identification of screens and selections in these steps are subject to change. Only configuration options directly relevant to the Twitter Connector are described. Some configuration steps are summarized, and different configurations may be possible. Please consult Twitter documentation for more information.

To register a Twitter application:

1. Go to https://dev.twitter.com/apps and log on to your Twitter developer account.
2. Go to the My Applications Dashboard and create a new Twitter application.
3. Enter the name of the application in the Name field.
4. For the Website field, enter the domain for your Web site (for example, http://yourwebsite.com).
5. For the Callback URL, enter the fully qualified host name, port, and path on which the PingFederate server runs: `https://<pf_host>:<pf_port>`

Note: If you plan to allow the SP Web application to use the access token for subsequent Twitter API calls requiring both read and write access, select **Read & Write** for the Default Access type.

6. When finished, click **Create your Twitter application**.
7. Copy the Consumer Key and the Consumer secret from the application details page that follows.

Note: These credentials are needed in the Twitter Adapter setup (see next sections). You may want to keep the page open to copy the keys directly during the adapter configuration.

Step 3 -- Configure PingFederate

To configure PingFederate, follow the instructions in each of the following sections, in order.

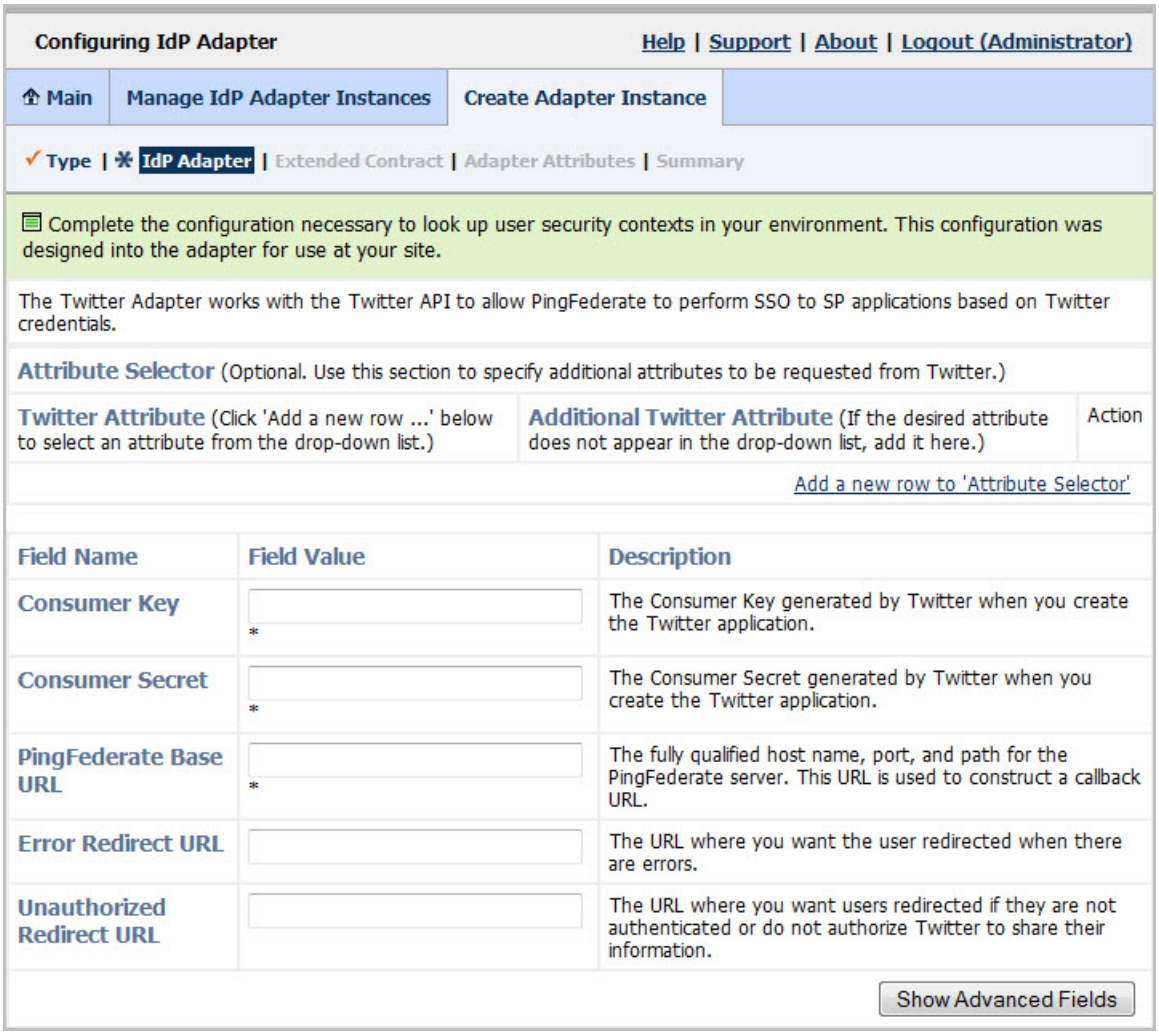
Configure the IdP Adapter

To configure the IdP Adapter, do the following:

To configure the IdP Adapter:

1. Log on to the PingFederate administrative console and click **Adapters** under My IdP Configuration on the Main Menu.
2. On the Manage IdP Adapter Instances screen, click **Create New Instance**.
3. On the Type screen, enter an Instance Name and Instance ID.

   The Name is any you choose for identifying this Adapter Instance. The ID is used internally and may not contain spaces or non-alphanumeric characters.
4. Select Twitter Adapter 1.2 from the Type list and click **Next**.



5. On the IdP Adapter screen provide entries for each of the fields shown, as indicated in the table below.

Field Name	Description
Consumer Key	Enter the key generated when you created the Twitter application.
Consumer Secret	Enter the secret generated when you created the Twitter application.
PingFederate Base URL	Enter the fully-qualified host name, port, and path on which the PingFederate server runs: `http[s]://<pf_host>:<pf_port>` The Adapter uses this URL to construct a callback URL at runtime, sent with the initial request. **Note**: If PingFederate is running behind a reverse proxy, enter the fully qualified host name, port, and path (if applicable) of the proxy server.

Field Name	Description
Error Redirect URL	Optional. Enter a URL for redirecting the user if there are errors. This URL may contain query parameters. The URL has an `errorMessage` query parameter appended to it, which contains a brief description of the error that occurred. The error page can optionally display this message on the screen to provide guidance on remedying the problem. **Note**: When employing the `errorMessage` query parameter in a custom error page, adhere to Web-application security best practices to guard against common content injection vulnerabilities. If no URL is specified, the appropriate default error landing page appears. (For more information, see "Customizing User-Facing Screens" in the "System Administration" chapter of the PingFederate *Administrator's Guide*.)
Unauthorized Redirect URL	Optional. Enter an endpoint URL for redirecting the user if the user declines authorizing Twitter to share information. This URL may contain query parameters. If no URL is specified, the appropriate default error landing page appears. (For more information, see "Customizing User-Facing Screens" in the "System Administration" chapter of the PingFederate *Administrator's Guide*.)

6. (Optional) To add attributes beyond the defaults that Twitter provides, use the Attribute Selector section of the IdP Adapter screen.

Note: A list of the default attributes is shown on the Extended Contract screen. Be sure to extend the contract with the same attributes you add here.

   a. Click **Add a new row to 'Attribute Selector'**.

   b. Select an attribute from the drop-down list on the left.

      If the desired attribute does not appear in the list, type it into the Additional Twitter Attributes box.

      You must use the correct syntax for manual entries.
      For a raw data example of what Twitter returns, see the following wiki page on Twitter: https://dev.twitter.com/docs/api/1.1/get/account/verify_credentials

Note: The Twitter API is subject to change without notice, including renaming of user attributes requested by the Twitter Adapter in this setup.

   c. Click **Update**.

7. (Optional) Click **Show Advanced Fields** to view additional configuration settings.

   The default values for these fields may be modified if necessary:

Field Name	Description
Twitter Authentication URL	Displays the Twitter endpoint used for authentication. If Twitter has altered this endpoint, modify it accordingly.

Field Name	Description
Twiiter User Data URL	Displays the Twiiter endpoint used when retrieving user data. If LinkedIn altered this endpoint, modify it accordingly.

8. Click **Next**.

Tip: PingFederate verifies the Twiiter credentials before going to the next screen.

9. On the Extended Contract screen, *if* you added additional attributes on the previous screen, then you *must* add the corresponding attribute to the contract in order for those values to be passed to the Web application.

   (For information on using the Extended Contract screen, see "Extending an Adapter Contract" in the "Identity Provider SSO Configuration" chapter of the PingFederate *Administrator's Guide* or click **Help** on the screen.)

10. Click **Next**.

11. On the Adapter Attributes screen under Pseudonym, select a checkbox for an attribute that may be considered a unique user identifier.

    Pseudonyms are opaque subject identifiers used for SAML account linking and are not generally applicable in the context of cloud-identity deployments. To ensure correct PingFederate performance under all circumstances, however, a selection is required. (For information about account linking, refer to "Account Linking" in the "Key Concepts" chapter of the PingFederate *Administrator's Guide* or use the context-sensitive **Help** for this screen.)

12. On the Summary screen, verify that the information is correct and click **Done**.

13. On the Manage IdP Adapter Instances screen, click **Save**.

Complete the Configuration

To complete the SSO setup in PingFederate:

- For SSO to an application at your site in the domain covered by PingFederate, a standard SAML connection is not necessary; instead you can use direct IdP-to-SP adapter mapping (see instructions under "For SSO to an Enterprise Service Application" next).
- For an external SP partner (or any service outside the domain covered by PingFederate), configure an SP connection (see instructions under "For SSO to an SP Partner").

For SSO to an Enterprise Service Application

1. On the Main Menu, click **Server Settings**.
2. On the Roles and Protocols screen in the Server Settings configuration, ensure that both the IdP and SP roles are enabled.

Note: The choice of protocol is not relevant for either role to implement the Twitter Cloud Identity Connector for in-domain SSO, but a selection is required to enable a role. If updates are needed on the screen, be sure to click **Save**.

3. Configure an SP Adapter Instance, if one is not already configured or you want to use a new one.

   Click **Adapters** under SP Configuration on the Main Menu.

   Use any adapter type, such as the ReferenceID Adapter (available separately in the PingFederate Agentless Integration Kit) or the OpenToken Adapter (bundled with PingFederate).

   For a list of other available Ping Identity integration kits, see the Ping Identity Web site (www.pingidentity.com/support-and-downloads).

4. On the Main Menu under System Settings, click **IdP-to-SP Adapter Mapping** and follow the screen flow to complete this configuration.

   Select the IdP Adapter Instance configured earlier as the Source instance and any SP Adapter Instance as the Target.

   For more information, see "IdP-to-SP Adapter Mapping" in the "System Settings" chapter of the PingFederate *Administrator's Guide* (or use the context-sensitive **Help**).

For SSO to an SP Partner

- Use the IdP Adapter Instance (configured earlier) in an SP Connection.

  You select the Adapter Instance for the IdP Adapter Mapping setup under Assertion Creation.

  For more information, see "Managing SP Connections" in the "Identity Provider SSO Configuration" chapter of the PingFederate *Administrator's Guide* and refer to the context-sensitive **Help** for IdP Adapter Mapping screens.

Step 4 -- Application Integration

For users to authenticate via the Twitter Cloud Identity Connector, administrators must provide a specific PingFederate URL:

For IdP-to-SP adapter mapping configuration:

- Use the following URL in a hypertext link on your Web-application logon page to start SSO:

  ```
  https://<pf_host>:<pf_port>/pf/
  adapter2adapter.ping?IdpAdapterId=<adapterId>
  ```

  where:

  - `<pf_host>` is the host name or IP address where PingFederate is running.
  - `<pf_port>` is the port number for PingFederate.
  - `<adapterId>` is the Instance ID defined in the Twitter IdP Adapter set up earlier.

For an SP-connection configuration:

- Use the following URL in your Web-application for SSO to the target application:

  ```
  https://<pf_host>:<pf_port>/idp/
  startSSO.ping?PartnerSpId=<ConnectionId>&
  IdpAdapterId=<IdPAdapterId>
  ```

  where:

  - `<pf_host>` is the host name or IP address where PingFederate is running.
  - `<pf_port>` is the port number for PingFederate.

- <ConnectionId> is the SP-connection identifier (e.g.: SAML 2.0 Entity ID) for the connection using the Twitter Adapter instance.
- <IdPAdapterId> is the applicable Instance ID for the Twitter Adapter used in the SP-connection.

Troubleshooting

The following table lists potential problems administrators might encounter during the setup or deployment of the Twitter Adapter, along with possible solutions.

Problem	Possible Cause/Solution
The launch URL fails to reach the PingFederate endpoint, and you are running the PingFederate server behind a reverse proxy.	You may need to extend the existing proxy rules within your network to allow network traffic to the endpoint (http[s]:<pf_host>:<pf_port>).
User is presented with an unauthorized page by Twitter containing a link to the Adapter. User clicks the link and is redirected to the configured Unauthorized Redirect URL (in the Adapter setup) or the standard Adapter error page if an Unauthorized Redirect URL is not specified.	During authentication, the user did not authorize transfer of his or her attributes.
The HTTP Error 400 - Bad Request error message displays.	The user attempted to access the PingFederate endpoint (<pf_host>:<pf_port>) directly from the browser.