PingFederate®

Facebook Cloud Identity Connector

Version 1.3

User Guide

PingFederate Facebook Cloud Identity Connector *User Guide*
Version 1.3
March, 2015

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 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: **March 11, 2015**

Contents

Introduction

This PingFederate Cloud Identity Connector allows a Service Provider (SP) to leverage Facebook as an Identity Provider (IdP) for access to Internet applications in the SP domain. The included PingFederate Facebook IdP Adapter works with the Facebook 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 Facebook 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 Manual*.)

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.

> **Note:** If you encounter any difficulties with configuration or use of the Facebook CIC, please try reaching the Ping Identity Support Center (`ping.force.com/Support`).

Additional Resources

Administrators should review SSO Integration Kits and Adapters in the PingFederate *Administrator's Manual*.

ZIP Manifest

The distribution ZIP file for the Facebook CIC contains the following:

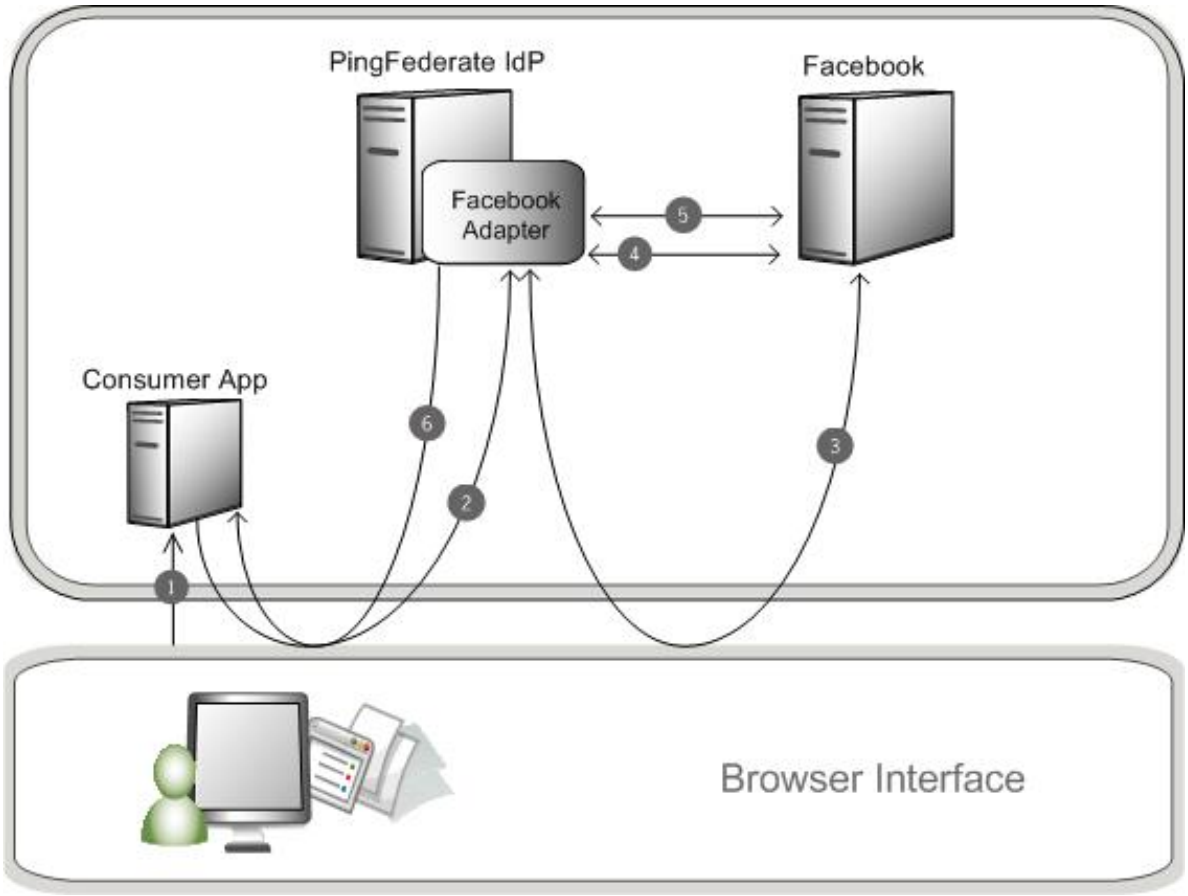
- `ReadMeFirst.pdf` – contains links to this online documentation
- `/legal` – contains the legal information:
  - `Legal.pdf` – copyright and license information
- `/dist` – contains libraries needed to run the Facebook CIC:
  - `pf-facebook-adapter-1.3.jar` – Facebook CIC adapter
  - `json-simple-1.1.jar` - JavaScript Object Notation (JSON) library

System Requirements

The Facebook CIC requires installation of PingFederate 7.0.1 or higher.

Processing Overview

The following figure illustrates an example SSO process flow using the Facebook CIC:



Processing Steps

1. User navigates to a Web application and chooses to log on using Facebook.
2. The browser is redirected to the Facebook CIC.
3. The PingFederate server redirects the user to Facebook for authentication. A list of requested permissions is provided in this call.

   If the user is not already logged on, Facebook challenges the user to authenticate. Facebook authenticates the user and provides a consent page for the user to authorize the sharing of information. Once the user authorizes, Facebook redirects the browser to the /ext/facebook-authn/ endpoint with an authorization code.

   If the user does not authenticate, an error is returned rather than the authorization code.
4. The Adapter makes an HTTP request to Facebook to obtain an access token, sending the Application ID, Application Secret, and authorization code as parameters. Facebook validates these components and returns an access token.
5. The Adapter uses the access token to request user information from Facebook, and Facebook returns the user information.

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

---

6. The Adapter uses the access token to request user information from Facebook, and Facebook returns the user information.

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 Completing the Configuration).

Installation and Configuration

The following section describes how to install and configure the Facebook CIC with your application.

Install the Facebook Cloud Identity Connector

To Install the Facebook Cloud Identity Connector:

1. Stop the PingFederate server if it is running.
2. Remove any existing Facebook CIC files (`pf-facebook-adapter-1.x.jar`) from the directory:

   `<PF_install>\pingfederate\server\default\deploy`
3. Unzip the distribution file and copy the contents of the `/dist` directory to the PingFederate directory:

   `<PF_install>\pingfederate\server\default\deploy`
4. Start the PingFederate server.

Register the Facebook Application

You must use a Facebook account to register PingFederate as a Facebook application.

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

To register a Facebook application:

1. Go to https://developers.facebook.com/apps and log on to your Facebook account.
2. Click **Add a New App**, enter the name of the application, agree to the Facebook Terms, and click **Create App**.
3. On the application page that follows, choose the **WWW** option.
4. Enter the name of your app, then click **Create New Facebook App ID**
5. Choose a **Category** then click **Create App ID**
6. Click **App Configuration**
7. For the **Site URL**, enter the fully qualified host name, port, and path for the PingFederate endpoint: `https://<pf_host>:<pf_port>/ext/facebook-authn`

8. Click **Next**. At this point the Facebook application is set up.
9. Copy the Application ID and the Application Secret. You can obtain these values from the Dashboard of your new Facebook application (Click **My Apps** in the top menu and select your new app to go to the dashboard).

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

Configure PingFederate

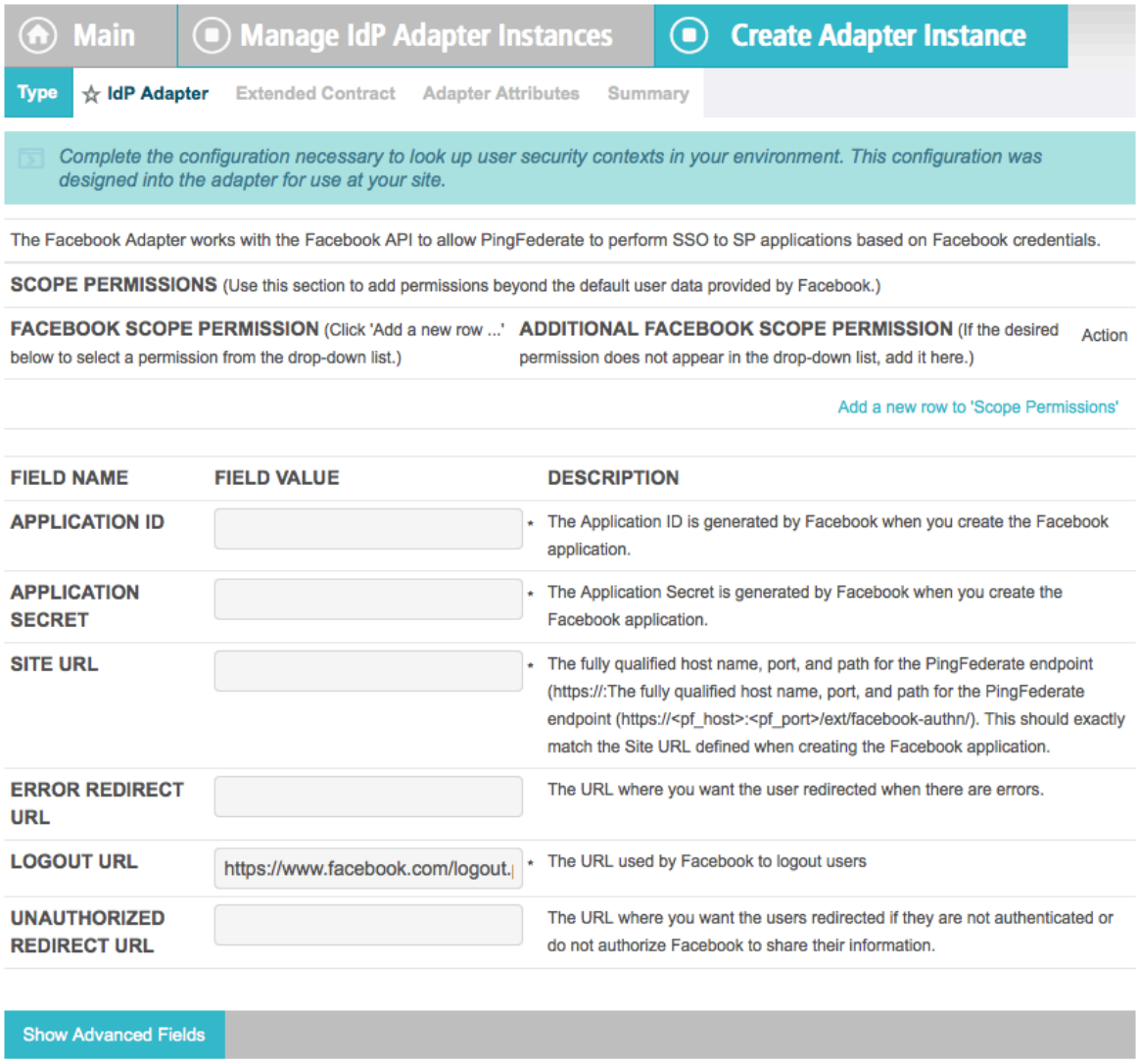
To configure PingFederate, follow the instructions in each of the following sections, in order.

Configuring the IdP Adapter

1. Log on to the PingFederate administrative console and click **Adapters** under My IdP Configuration on the Main Menu.

   (For more information about IdP Adapters, see Configuring IdP Adapters in the PingFederate *Administrator's Manual*.)
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 Facebook Adapter 1.3 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	Description
Application ID	Enter the ID generated when you created the Facebook application.
Application Secret	Enter the secret generated when you created the Facebook application.
Site URL	Enter the Site URL for the PingFederate endpoint: `https://<pf_host>:<pf_port>/ext/facebook-authn.` This also needs to be input into the configuration settings of your Facebook application.

Field	Description
Error Redirect URL	Optional. Enter a URL for redirecting the user if there are errors: for example, incorrect parameters in the link. This URL may contain query parameters. The URL will have 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 PingFederate *Administrator's Manual*.)
Logout URL	The URL used by Facebook to logout users.
Unauthorized Redirect URL	Optional. Enter an endpoint URL for redirecting the user if the user declines authorizing Facebook 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 PingFederate *Administrator's Manual*.)

6. (Optional) To add attributes beyond the defaults that Facebook provides, use the Scope Permissions 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 'Scope Permissions'.

   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 Facebook Scope Permission box.

      You must use the correct syntax for manual entries. For a list of available permissions, see the following page on Facebook: http://developers.facebook.com/docs/reference/api/permissions

Note: The Facebook API is subject to change without notice, including renaming of user attributes requested by the 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	Description
Facebook Authentication URL	Displays the Facebook endpoint used for authentication. If Facebook has altered this endpoint, modify it accordingly.

Field	Description
Facebook Access Token URL	Displays the Facebook endpoint used to retrieve an OAuth Access Token. If Facebook has altered this endpoint, modify it accordingly.
Facebook User Data URL	Displays the Facebook endpoint used when retrieving user data. If Facebook has altered this endpoint, modify it accordingly.

8. Click **Next**.
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.

   Although some permissions do not have a corresponding attribute, most permissions do. For example, the current version of Facebook includes an extended permission called user_religion_politics. Once the user authorizes Facebook to share that information, Facebook sends back the attributes: religion and/or political (if the information exists in the profile). In order for the religion and/or political attriutes to be passed to the Web application, you must add those attributes on this page.

   Note: For a list of the properties associated with extended permissions in Facebook, see http://developers.facebook.com/docs/reference/api/permissions.

   (For information on using the Extended Contract screen, see Extending an Adapter Contract in the PingFederate *Administrator's Manual*, 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 PingFederate *Administrator's Manual*, 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 below).

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 Facebook 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 website (www.pingidentity.com/en/products/downloads.html).

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 Facebook 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 PingFederate *Administrator's Manual* (or use the context-sensitive Help).

For SSO to an SP Partner:

Use the Facebook 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 PingFederate *Administrator's Manual* and refer to the context-sensitive Help for IdP Adapter Mapping screens.

Application Integration

For users to authenticate via the Facebook 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 Facebook 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 Facebook Adapter instance.
- `<IdPAdapterId>` is the applicable Instance ID for the Facebook Adapter used in the SP-connection.

Upgrade Notes

In the adapter configuration, the `Facebook User Data URL` must be updated to the value listed below (see Step 7 of Configuring the IdP Adapter):

```
https://graph.facebook.com/v2.2/me
```

Extended Development

By default, the Web application can access all public data in a user's profile, including name, profile picture, gender, and friends. If your Web application needs to access other parts of the user's profile that may be private, you must request extended permissions. For example, if you want to incorporate a user's photos into your Web application, you would request the user_photos extended permission. During authentication, users are asked whether they want to authorize your application to access their photos. However, no actual photos are sent. The Facebook Adapter sends back an access token and the user attributes to your application. Incorporate this access token into an HTTP request from the Web application to the Facebook API to get the actual photos from Facebook.

For information on using the access token to fetch information that requires additional calls, see the Facebook developer documentation: http://developers.facebook.com/docs/authentication/permissions.

Note: The Facebook Adapter provides no check to determine whether a requested field is available for the User API call. It is up to the SP to make this determination.

Note: Even though additional fields (extended attributes) are specified in the Facebook IdP configuration, there is no guarantee that Facebook will return those fields back to the Facebook adapter. In such cases, extended scopes permissions may be required if the attributes are not part of the core scopes"basic permissions".

Troubleshooting

The following table lists potential problems administrators might encounter during the setup or deployment of the Facebook 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>/ext/facebook-authn/`).
User is redirected to the configured Unauthorized URL (in the Adapter UI) with an error_msg parameter appended to the URL.	- During authentication, the user did not authorize transfer of his or her attributes. - An administrator entered an invalid permission in the Adapter setup.
The HTTP Error 400 - Bad Request error message displays.	The user attempted to access the Site URL endpoint directly from the browser.