PingFederate®

OpenID Cloud Identity Connector

Version 1.3.x

User Guide

PingIdentity®

© 2016 Ping Identity® Corporation. All rights reserved.

PingFederate OpenID Cloud Identity Connector *User Guide*
Version 1.3.x
January, 2016

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

Ping Identity, the Ping Identity logo, PingFederate, PingOne, PingConnect, and PingEnable are registered trademarks of Ping Identity Corporation ("Ping Identity"). All other trademarks or registered trademarks are the property of their respective owners.

Disclaimer

The information provided in this document is provided "as is" without warranty of any kind. Ping Identity disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Ping Identity or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Ping Identity or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

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: **January 27, 2016**.

Contents

Introduction

The PingFederate OpenID Cloud Identity Connector allows a service enterprise to provide consumer access to its Web applications by using OpenID-enabled organizations (for example, Yahoo!) as Identity Providers (IdPs). The included IdP Adapter enables PingFederate to perform single sign-on (SSO) to Service Provider (SP) applications based on the OpenID protocol (without the need to involve identity-federation standards).

Using the Connector, a Software-as-a-Service (SaaS) provider, for example, can provide customers direct SSO access to its applications, using any organization that supports OpenID for authentication. In addition, a service provider may leverage OpenID credentials for SSO to other services in other domains that are protected via identity-federation gateways (including PingFederate) based on the Security Assertion Markup Language (SAML). (For more information about identity federation, 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 information-technology infrastructure. Knowledge of networking and user-management configuration is assumed as well as some familiarity with PingFederate.

System Requirements

The OpenID Adapter requires installation of PingFederate 7.2 or higher.

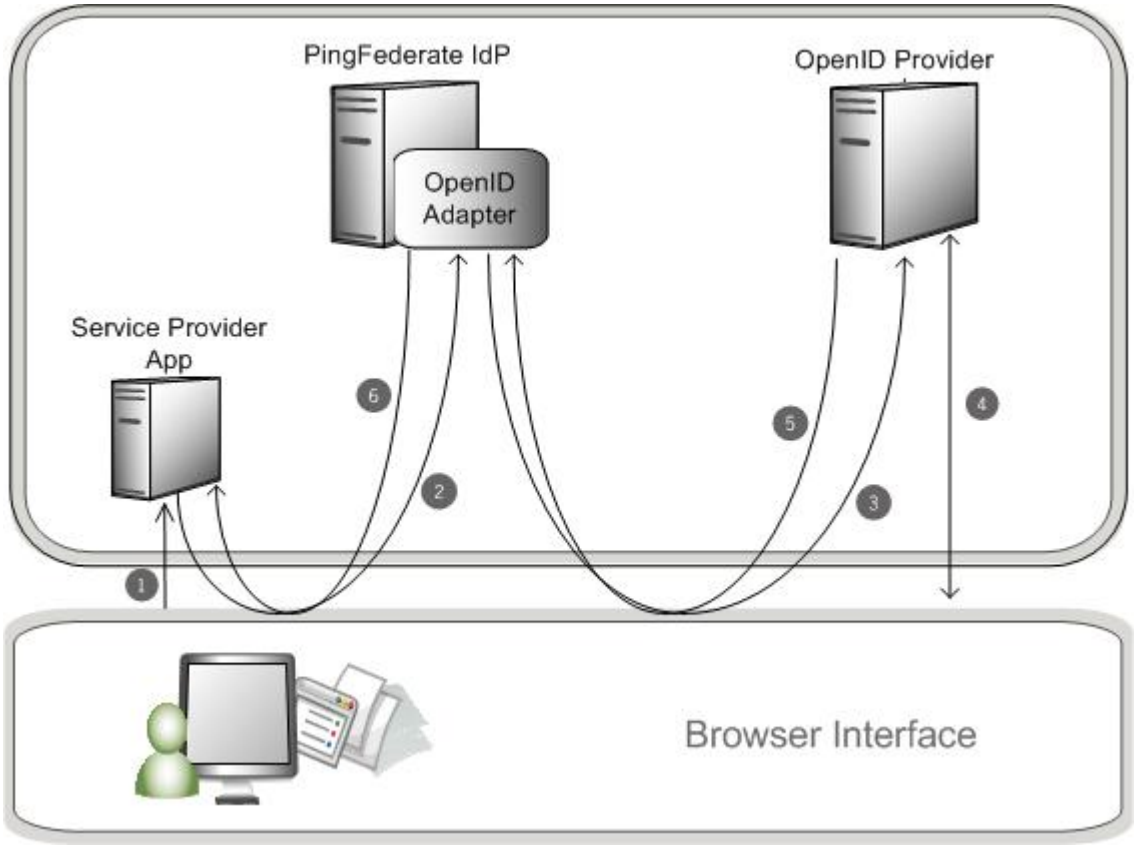
ZIP Manifest

The distribution ZIP file for the OpenID Cloud Identity Connector Kit 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 to run the Adapter
  - `pf-openid-authn-adapter-1.3.1.jar` – The OpenID Adapter JAR file
  - `pf-openid-idp-consumer-app.war` – The OpenID Web Archive

Processing Overview

The following figure illustrates an example SSO process flow between OpenID, PingFederate, and an SP Application using the OpenID Adapter:



Processing Steps

1. User navigates to a Web application and chooses to log on using an OpenID provider (for example, Yahoo!).
2. The browser is directed to the appropriate PingFederate endpoint for the OpenID Adapter instance selected.
3. PingFederate redirects the user to the provider for authentication. A list of requested attributes is provided in this call.
4. The user authenticates.
5. The browser is redirected to the IdP endpoint with a valid session.
6. The browser is redirected to the target 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 11).

Installation and Configuration

This section describes how to:

- Install the OpenID Adapter.
- Configure PingFederate.
- Integrate Applications

Step 1 -- Install the OpenID Adapter

To install the OpenID Adapter:

1. Stop the PingFederate server if it is running.
2. If you are upgrading the OpenID Adapter, remove any existing OpenID Adapter files from the directory:

   `<PF-install>/server/default/deploy`

   The OpenID Adapter JAR file is `pf-openid-authn-adapter-1.x.jar.`

   The OpenID Web Archive file is `pf-openid-idp-consumer-app-1.x.war.`
3. Unzip the distribution ZIP file.
4. From the OpenID Connector distribution `/dist` directory, copy both the `pf-openid-authn-adapter-1.3.1.jar` and `pf-openid-idp-consumer-app.war` into the directory:

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

Step 2 -- Configure PingFederate

Setting up PingFederate involves configuring an instance of the OpenID IdP Adapter and then using it either for IdP-to-SP Adapter Mapping in a single PingFederate instance (to provide SSO for in-domain services) or for IdP adapter mapping in an SP SSO connection.

Configure the IdP Adapter

When configuring the IdP Adapter, you can create an adapter instance based on the following choices:

- Yahoo!
- Any "Generic" OpenID provider (the default)

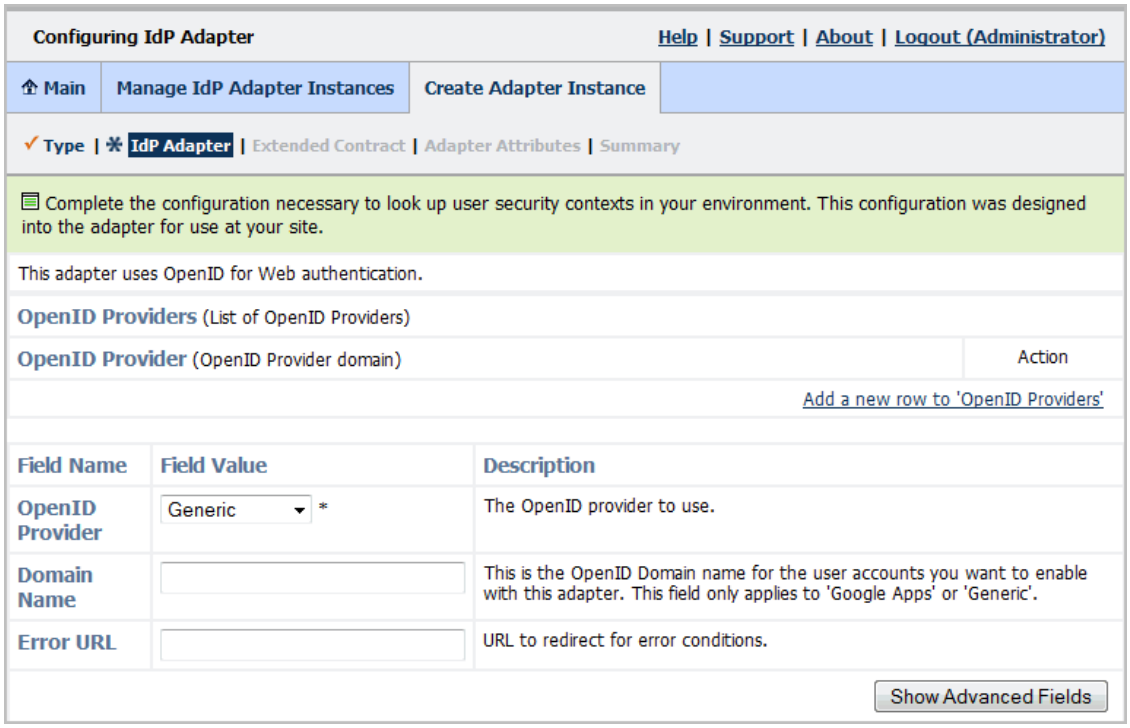
  PingFederate determines the provider to use based on user input.
- Any single "Generic" provider specified with a URL
- Any OpenID provider in a specified list

Note: You can configure multiple adapter instances as needed and then use them in different adapter-to-adapter configurations and/or SP connections and then in different links on your Web site (see Complete the Configuration on page 11 and Step 3 -- Application Integration on page 12).

To configure the IdP Adapter:

1. Log on to the PingFederate administrative console and click **Adapters** from the 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 OpenID IdP Adapter 1.3.1 from the Type list and click **Next**.



5. Provide entries on the IdP Adapter screen, as described on the screen and in the table below.

Field	Description
OpenID Provider	Select a preset OpenID provider or leave the default Generic selection.
Domain Name	Required only if you wish to restrict the Generic default to a single domain. Enter the fully-qualified OpenID Domain name, as needed. Alternatively, for Generic providers you can use the OpenID Providers list (see the next step).
Error 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 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 *PingFederate Administrator's Manual*.)

6. (Optional) For Generic providers, use the OpenID Providers section of the IdP Adapter screen to list providers you support.

Caution: As a best security practice, we recommend either defining supported providers here or entering a single domain in the Domain Name box on this screen. Otherwise, PingFederate uses any provider specified in the logon-link parameter.

Use entries in query parameters when you integrate logon links into your Web application (see Step 3 -- Application Integration).

a. Click **Add a new row to 'OpenID Providers'**.

b. Enter the fully-qualified domain name for Generic OpenID provider.

   For example: `openid.domain.com`

c. Click **Update**.

d. Repeat these steps to add more providers, as needed.

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

   You can change default settings, depending on your network configuration and other requirements at your site.

   Refer to the screen descriptions in the administrative console. The following table provides supplemental information and instructions.

Field	Description
Realm	(Optional) Realm is a parameter used to present information about the domain and is only used by the provider to display information to the user and validate the return URL. The Realm name is sent as part of the HTTP Basic Authentication request and appears in the box that prompts the user for authentication. Enter the URL of the Realm associated with the PingFederate server. For example, if PingFederate is running on 9031, enter `https://my.domain.com:9031`. You can use wildcards at the beginning of the URL, for example, `https://*.domain.com:9031`. PingFederate assumes the Realm to be the return URL if no Realm is specified. **Note**: Some OpenID providers may not support nonstandard ports.
PF Base URL	(Optional) If PingFederate is running behind a reverse proxy, enter the fully-qualified host name, port, and path (if applicable) of the proxy server.
Logout URL	(Optional) Enter the URL that receives and processes logout requests and responses.
Perform Logout	Select the checkbox if you want PingFederate to perform Single Logout (SLO). The Generic OpenID provider does not support SLO. A custom OpenID provider may support SLO as long as you specify the logout URL and the domain.
Authentication Context Value	(Optional) This may be any value agreed to with your SP partner. Standard URIs are defined in the SAML specifications (see the OASIS document saml-authn-context-2.0-os.pdf).
Provider List Type	While *not recommended* for optimal security, this selection allows you to use the OpenID Providers list as a “Black” list of untrusted Generic providers, rather than as a “White” list of trusted ones (the default).
PAPE 1.0	(Optional) Select the checkbox to enable Provider Authentication Policy Extension (PAPE) as the attribute extension used by the OpenID provider. This extension allows for a relying party to request previously agreed upon authentication policies to be applied by the OpenID provider and for a provider to inform the relying party which authentication policies were used.
PAPE Max Auth Age	(Optional) Specifies the length of time (in seconds) in which the user must authenticate with the OpenID provider. If this time expires, the provider must re-authenticate the user using the agreed upon authentication policies. **Note**: Value applies only if you select the PAPE 1.0 checkbox.

Field	Description

PAPE Authentication Policy	(Optional) Specify a list of preferred authentication policy URIs. The URIs represent authentication policies the OpenID provider must satisfy when authenticating a user. If multiple policies are requested, the OpenID provider must satisfy as many of them as possible and then indicate which authentication policies were satisfied in the response.
	Separate URIs with a space, for example:
	`http://schemas.openid.net/pape/policies/2007/06/phishing-resistant`
	`http://schemas.openid.net/pape/policies/2007/06/multi-factor`
	Note: Values apply only if you select the PAPE 1.0 checkbox.

PAPE Authentication Level	(Optional) Specify a list of preferred authentication level URIs. Authentication level values determine the level of trust placed in the authentication of the user. Relying parties request information about these authentication levels from the OpenID provider. Each authentication level must include the name and type separated by a comma and a space placed between URIs.
	Example:
	`nist,http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf`
	`jisa,http://www.jisa.or.jp/spec/auth_level.html`
	Note: Values apply only if the PAPE 1.0 checkbox is selected.

SREG 1.0	(Optional) Select to enable the Simple Registration extension 1.0 as the attribute extension used by the OpenID provider. This extension is a lightweight profile exchange used by the OpenID provider to pass commonly requested pieces of information about the user to the Service provider when a user attempts to register a new account.
SREG 1.1	(Optional) Select to enable the Simple Registration extension 1.1 as the attribute extension used by the OpenID provider.
AX 1.0	(Optional) Select to enable the Attribute Exchange extension 1.0 for exchanging identity information between endpoints.

AX Attribute List	(Optional) Specify a list of extended attribute URIs. Each item must include the name and type separated by a comma and a space placed between URIs.
	Example:
	`nickname,http://axschema.org/namePerson/friendly`
	`email,http://axschema.org/contact/email`
	Note: Values apply only if you select the AX 1.0 checkbox.

OpenID 2.0 Only	Select to accept only OpenID 2.0 requests.

8. Click **Next.**
9. (Optional) On the Extended Contract screen, click **Next**.

   Extended attributes are not needed in most cases. (For more information, see Adapter Contracts in the PingFederate *Administrator's Manual.*)

10. On the Adapter Attributes screen, select any checkbox under Pseudonym.

    Pseudonyms are opaque subject identifiers used for SAML account linking and are not applicable in the context of cloud-identity deployments. To ensure correct PingFederate performance under all circumstances, however, a selection is required. (For more information, see Account Linking in the PingFederate *Administrator's Manual*.)

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

12. 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 on page 11).

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 OpenID 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 OpenID 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 OpenID 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.

Step 3 -- Application Integration

To authenticate using the OpenID Cloud Identity Connector, users must go to PingFederate to initiate OpenID authentication:

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=<IdPAdapterId>
    [&openid.identifier=<OpenIdProvider>]
```

where:

- `<pf_host>` is the host name or IP address where PingFederate is running.
- `<pf_port>` is the port number for PingFederate.
- `<IdPAdapterId>` is the Instance ID defined in the OpenID IdP Adapter set up earlier.
- `<OpenIdProvider>` is the target provider—required when Generic providers are used and a specific Domain Name is not designated in the adapter configuration.

For an SP-connection configuration:

Use the following URL in a hypertext link in your Web-application link to the target application:

```
https://<pf_host>:<pf_port>/idp/startSSO.ping?PartnerSpId=<ConnectionId>&
    IdpAdapterId=<IdPAdapterId>[&openid.identifier=<OpenIdProvider>]
```

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 OpenID adapter instance.
- `<IdPAdapterId>` is the applicable Instance ID for the OpenID Adapter used in the SP-connection.
- `<OpenIdProvider>` is the target provider—required when Generic providers are used and a specific Domain Name is not designated in the adapter configuration.

Optional System Properties

The following table lists properties you can add to the Java Virtual Machine (JVM) running PingFederate. To add a property, locate and open the `<PF-install>/bin/run.properties` file and add each property as a separate line at the bottom of the file.

Property	Information
`openid.startSSOUrl`	The SSO URL to be used if PingFederate receives an unsolicited assertion. Example: `openid.startSSOUrl=https://pic.com:9031/idp/startSSO.ping?PartnerSpId=<ConnectionId>&IdpAdapterId=<IdPAdapterId>`

`openid.minAssocSessEnc`	The minimum level of encryption accepted for OpenID association sessions. Valid values include:
	`NO_ENCRYPTION_SHA1MAC`
	`NO_ENCRYPTION_COMPAT_SHA1MAC`
	`NO_ENCRYPTION_SHA256MAC`
	`DH_SHA1`
	`DH_COMPAT_SHA1`
	`DH_SHA256`
	Example: `openid.minAssocSessEnc=DH_SHA1`

`https.proxyUser`	A username to be used by the connector to work behind an outgoing enterprise proxy. Example: `https.proxyUser=joe`
`https.proxyPassword`	A password associated with the username to be used by the connector to work behind an outgoing enterprise proxy. Example: `https.proxyPassword=test`
`https.proxyDomain`	A domain to be used by the connector to work behind an outgoing enterprise proxy in cases where NTLM authentication is required. Example: `https.proxyDomain=domainTest`

Troubleshooting

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

Problem	Possible Cause/Solution
User is redirected to the configured Error URL (in the Adapter UI) with an error_msg parameter appended to the URL.	• The user either fails to authenticate or cancels the logon. • PingFederate either cannot find a discovery endpoint or cannot determine an authentication endpoint for a Generic OpenID provider. • An OpenID provider is either listed on the black list or not listed on the white list.
User performs a Single Logout from the Service Provider page but is not logged out of the OpenID provider.	Perform Logout is not enabled within the adapter instance (see Configuring an IdP Adapter on page 6 for more information).

Problem	Possible Cause/Solution
User is presented with a general error from the OpenID provider during an SSO attempt.	If Realm is being used in the Adapter instance, ensure that the URL is accurate. Some OpenID providers support only standard HTTP(80) and HTTPS(443) ports. If you are using a nonstandard port, verify that the OpenID provider supports it (see Configuring an IdP Adapter on page 6 for more information).
The following error appears in the `server.log`: "`org.openid4java.discovery.yadis.YadisException: 0x704: I/O transport error: peer not authenticated`"	This error indicates that the OpenID provider SSL certificate is not trusted by the JVM running PingFederate. To resolve this issue, import the CA certificate for the provider into PingFederate (see Trusted Certificate Authorities in the PingFederate *Administrator's Manual*).