OpenID Login Integration Kit

Contents

OpenID Login Integration Kit

The PingFederate OpenID Login Integration Kit allows a service enterprise to provide consumer access to its Web applications by using OpenID-enabled organizations, such as Google and 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 integration kit, a Software-as-a-Service (SaaS) provider can provide customers direct SSO access to its applications, using any organization that supports OpenID for authentication. Additionally, a service provider can 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 the PingFederate Administrator's Manual.

Intended audience

This document is intended for PingFederate administrators.

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

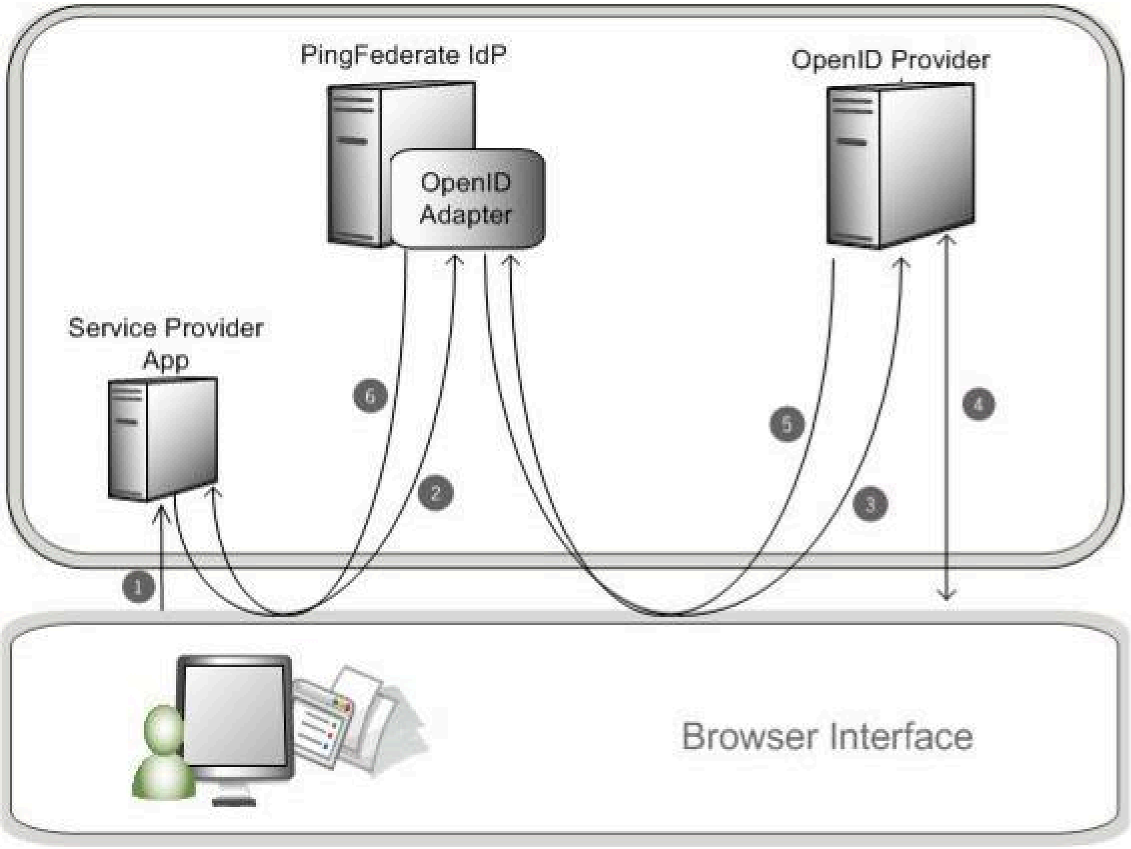
- PingFederate documentation:
  - *Identity provider SSO configuration*
  - *Managing IdP adapters*
  - *Authentication Policies*
  - *SP connection management*

System requirements

- PingFederate 6.3 or higher

Overview of the SSO flow

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



1. User navigates to a Web application and chooses to log on using an OpenID provider (for example, Google or 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*).

Setup

Install or upgrade the connector

About this task

To install the OpenID Adapter:

Steps

1. Stop the PingFederate server if it is running.
2. If you are upgrading the OpenID Adapter, remove the previous installation files:
   - `pf-openid-authn-adapter-1.x.jar`
   - `pf-openid-idp-consumer-app-1.x.war`

   from the directory:

   `<PF-install>/server/default/deploy`
3. From the OpenID Connector distribution `/dist` directory, copy:
   - `pf-openid-authn-adapter-1.3.jar`
   - `pf-openid-idp-consumer-app-1.3.war`

   into the directory:

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

Configure the IdP adapter

About this task

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

- Any of three preset, well-known OpenID providers: Google, Google Apps, and 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

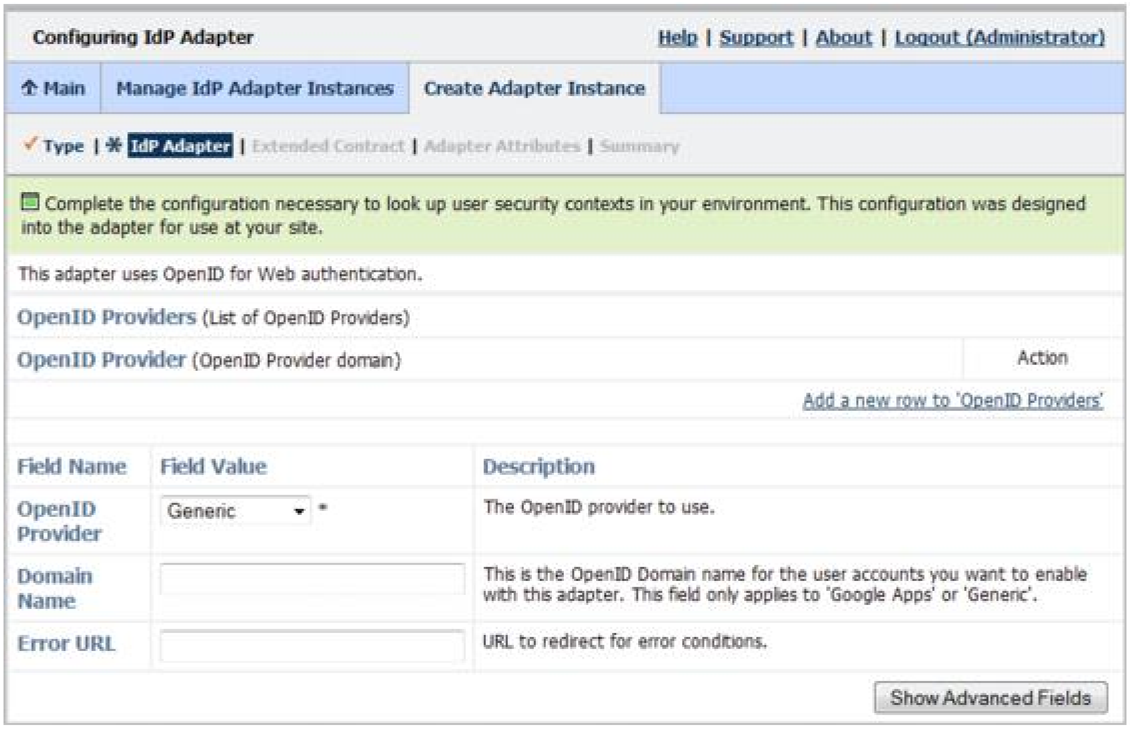
> ⓘ **Note:** You can configure multiple adapter instances as needed and then use them in different adapter-to-adapter configurations and/or SP connections and then in different links on your Web site (see *Complete the configuration* and *Application integration*).

Steps

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 OpenID IdP Adapter 1.3 from the Type list and click **Next**.



Configuring IdP Adapter

Help | Support | About | Logout (Administrator)
Main
Manage IdP Adapter Instances
Create Adapter Instance
✓ Type | ✻ IdP Adapter | Extended Contract | Adapter Attributes | Summary

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

This adapter uses OpenID for Web authentication.

OpenID Providers (List of OpenID Providers)

OpenID Provider (OpenID Provider domain)	Action

Add a new row to 'OpenID Providers'

Field Name	Field Value	Description
OpenID Provider	Generic *	The OpenID provider to use.
Domain Name		This is the OpenID Domain name for the user accounts you want to enable with this adapter. This field only applies to 'Google Apps' or 'Generic'.
Error URL		URL to redirect for error conditions.

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

Field	Description
OpenID Provider	Select a preset OpenID provider or leave the default Generic selection.
Domain Name	Required only if Google Apps is the selected OpenID provider or 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 *Customizable user-facing screens* in the PingFederate documentation.

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 listing supported providers here or entering a single domain in the Domain Name field on this screen. Otherwise, PingFederate will use any provider specified in the logon-link parameter.

   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** and make any desired changes to the default settings.

   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 dialog 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 the logout URL and the domain are specified.
Authentication Context Value	(Optional) This may be any value agreed to with your SP partner. Standard URIs are defined in the SAML specifications. See Authentication Context for the OASIS Security Assertion Markup Language(SAML) V2.0 in the OASIS documentation.
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 an OpenID Provider to inform the relying party of 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 OpenID Provider must re-authenticate the user using the agreed upon authentication policies.

> **Note:** Value applies only if the PAPE 1.0 checkbox is selected.

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 authentication policy 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 the PAPE 1.0 checkbox is selected.

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&#95;0&#95;2.pdfjisa, http://www.jisa.or.jp/spec/auth&#95;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/friendlyemail, http://axschema.org/contact/email` ⓘ **Note:** Values apply only if the AX 1.0 checkbox is selected.
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 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 information about account linking, refer to the PingFederate *Administrator's Manual*, or click **Help** on Adapter Attributes screen.)
11. On the Summary screen, verify that the information is correct and click **Done**.
12. On the Manage IdP Adapter Instances screen, click **Save**.

SSO to an enterprise service application

About this task

Steps

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.

   ⓘ **Note:** 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 *PingFederate server add-ons page*.
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 the PingFederate *Administrator's Manual* (or use the context-sensitive **Help**).

SSO to an SP partner

About this task

Steps

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

Results

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

For more information, see *Managing authentication source mappings* in the PingFederate documentation.

IdP-to-SP adapter mapping configuration

About this task

Steps

- 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.

SP connection configuration

About this task

Steps

- 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=

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

Problem: User is redirected to the configured Error URL (in the Adapter UI) with an error_msg parameter appended to the URL.	Possible cause/solution: 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.
Problem: User performs a Single Logout from the Service Provider page but is not logged out of the OpenID provider.	**Possible cause/solution:** Perform Logout is not enabled within the adapter instance (see *Configure the IdP adapter* on page 5 for more information).
Problem: User is presented with a general error from the OpenID provider during an SSO attempt.	**Possible cause/solution:** 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 *Configure the IdP adapter* on page 5 for more information).
Problem: The following error occurs sporadically: "Direct signature verification failed". This occurs in a clustered evironment.	Possible cause/solution: OpenID CIC will not work properly unless sticky sessions are enabled in a clustered environment. Ping Federate has a feature that forces "stateless mode", in which case which does not require sticky session. To enable stateless mode, add openid.maxAssocAttempts=0 to the Java Options for Ping Federate. For example, add the following to the $JAVA_OPTS in the run.sh script that starts Ping Federate: ▪ `-Dopenid.maxAssocAttempts=0`

Release notes

Changelog

OpenID Cloud Identity Connector 1.3.2 – January 2016 (Current Release)

- Maintenance update to support latest PingFederate release.

OpenID Cloud Identity Connector 1.3.1 – January 2013

- Addressed security issue found since the previous release
- Updated the Consumer Application to support PingFederate 6.9 and higher

OpenID Cloud Identity Connector 1.3 – May 2012

- Added support for NTLM authentication for an outgoing enterprise proxy
- Added compatibility support with IdP and SP Java sample applications

- Correctly handle Google “cancel” action while performing authentication
- Addressed data confusion vulnerability as described in: `http://openid.net/2012/03/14/vulnerability-report-data-confusion/`

OpenID Cloud Identity Connector 1.2 – January 2012

- Added support for OpenID PAPE (Provider Authentication Policy Extension) 1.0
- Added support for customizing the Attribute List for Attribute Exchange Extension
- Removed the Attribute Extension Type field and added checkboxes for each supported OpenID extension
- Added ability to reject non-OpenID 2.0 requests
- Added an XRDS document for OpenID Providers to verify Return URL

OpenID Cloud Identity Connector 1.1 – March 2011

- Modified error handling capabilities

OpenID Cloud Identity Connector 1.0 – December 2010

- Initial release

Known issues and limitations

Known Issues

This Connector is supported with PingFederate 6.3 and higher. PingFederate 6.2 returns an error in the user’s browser at runtime (“An error has occurred, please contact your system administrator.”) if Group RPC service (the default) is used for session-state management.

A workaround for 6.2 is to change the server’s session-state management service to use cookies and then restart the server.

The state-management setting is located in the file `hivemodule.xml` in the directory:

```
<pf_install>/pingfederate/server/default/conf/META-INF
```

For more information and instructions, see *Inter-Request State Management Service* in the PingFederate *Server Clustering Guide*.

ⓘ **Important:** Changing the session-state management service may have other implications to your PingFederate deployment. We recommend upgrading PingFederate to the current version rather than changing the session-state management service.

Known 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.
- Some OpenID Providers only allow connections using standard ports (http 80 and https 443).
- If a user tries to perform a single logout where the connection does not support ‘Perform Logout,’ the user is not logged out of the OpenID provider.
- If a GoogleApps connection is set up where the SSO user is able to specify the GoogleApps domain before they SSO (i.e., the adapter field Domain Name is left blank), there is a possibility that the user can log in to a non-GoogleApps provider. For example, the SSO user tries to SSO using yahoo.com as the GoogleApps domain, the user can then authenticate to yahoo.com. This is a limitation of the Step2 library. To prevent this behavior, preset the GoogleApps domain name by filling in the Domain Name Adapter field.
- If a user's SSO attempt fails just after PingFederate redirects the user to the OpenID Provider, the user may not be able to successfully SSO afterwards until the Web browser is closed and re-opened or if a

specific cookie is deleted. A cookie named pfidpaidtemp is stored in the user's Web browser temporarily and is cleared once the SSO is successful. In some cases where the SSO is unsuccessful, the cookie may stay in the Web browser, which causes problems for future SSO attempts. The user has to either close and then re-open their Web browser or delete this cookie.

- If a forward proxy is being used, all outbound HTTP(S) calls made by the OpenID Connector go through the proxy even if an exclusion list is specified. Other components of PingFederate, however, make use of an exclusion list if specified.

Download manifest

The following files are included in the `.zip` archive:

- `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-openid-authn-adapter-1.3.jar` – OpenID Adapter JAR file
  - `pf-openid-idp-consumer-app-1.3.war` – OpenID Web Archive