SAP NetWeaver Integration Kit

Version 2.3

User Guide

Ping Identity®

PingFederate SAP NetWeaver *User Guide*
Version 2.3
December, 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: **December 17, 2015**

Contents

Introduction

The PingFederate Integration Kit for SAP NetWeaver provides Identity Provider (IdP) and Service Provider (SP) functionality to PingFederate. This kit allows an enterprise to extend its existing NetWeaver investment by expanding the reach of the NetWeaver domain to federated partner applications.

In addition, this kit enables an SP enterprise to accept SAML assertions and provide single sign-on (SSO) to NetWeaver applications. The assertions may be sent using either the SAML protocol (version 2.0 or 1.x) or the WS-Federation passive-requestor protocol (see Supported Standards in *Getting Started*).

Intended Audience

This document is intended for system administrators with experience in the configuration and maintenance of SAP NetWeaver. Please consult the SAP NetWeaver documentation if you encounter any difficulties in areas not directly associated with the PingFederate or integration kit setups.

ZIP Manifest

The distribution ZIP file for the PingFederate Integration Kit for SAP NetWeaver contains the following:

- `ReadMeFirst.pdf` – contains links to this online documentation
- `/legal` – contains this document:
  - `Legal.pdf` – copyright and license information
- `/dist` – contains the following libraries that are needed to run the adapter:
  - `pf-netweaver-adapter-1.0.jar` – the NetWeaver IdP Adapter JAR file (IdP only)
  - `PFLoginModuleJAR.jar` – PingFederate Login Module JAR file that can be used to create a custom Software Development Archive (SDA) or Enterprise Archive (EAR)
  - `PFLoginModuleLibrary.sda` – SDA for NetWeaver 7.0 that contains `PFLoginModule`
  - `PFLoginModuleLibrary.ear` – EAR for NetWeaver 7.3 and 7.4 that contains `PFLoginModule`
  - `opentoken-adapter-2.5.1.jar` – OpenToken Adapter JAR file
  - `opentoken-agent-2.5.1.jar` – OpenToken Agent JAR file
  - `commons-collections-3.2.jar` – Apache Commons Collections library
  - `commons-beanutils.jar` – Apache Commons Bean Utility library
  - `commons-logging.jar` – Apache Commons Logging library

System Requirements

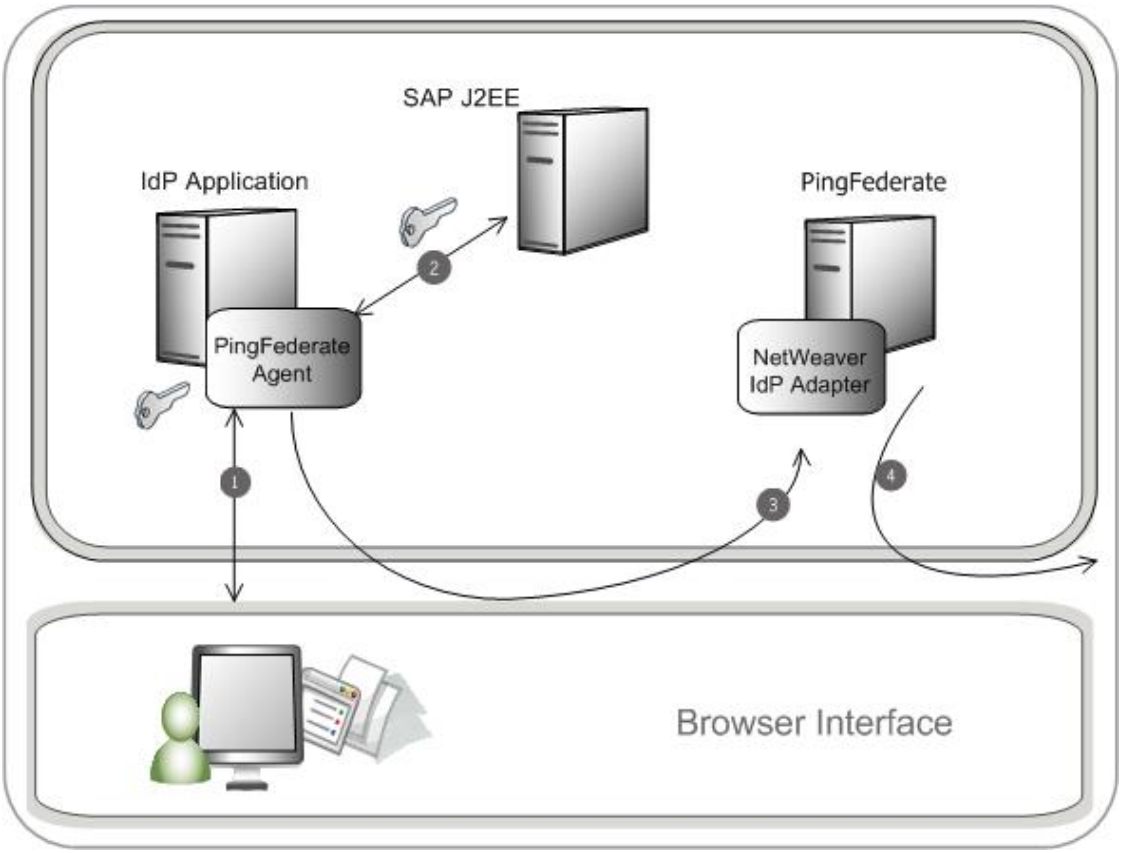
The following software must be installed in order to implement the PingFederate Integration Kit for SAP NetWeaver:

- PingFederate 6 (or higher) server
- NetWeaver Application Server 7.0 ,NetWeaver Application Server 7.3 or NetWeaver Application Server 7.4
- For an IdP:
    - SAP Single Sign-on (SSO) Extension Library (`sapssoext`), which existing customers can obtain from SAP. Please refer to the SAP documentation.
- For an SP:
    - The PingFederate OpenToken Adapter 2.5.1 (or higher) installed on PingFederate
    - `PFLoginModule`, installed on the SAP NetWeaver Application Server

Implementing IdP Functionality

The NetWeaver IdP Adapter uses the SAP SSO extension library to decrypt the session ticket and pass the attributes to the PingFederate server, which maps the values into an assertion and sends the assertion to the SP's federation gateway. For more information about configuration setup and attribute mapping, see Configuring IdP Adapters and About Attributes in the PingFederate *Administrator's Manual*.

The following figure illustrates the request flow and how the NetWeaver IdP Adapter is used in generating a SAML assertion:



Processing Steps

1. The user's browser accesses the IdP application.
2. The SAP J2EE Server authenticates the user and creates a session ticket.
3. The user clicks a link that initiates a Single Sign-on (SSO) transaction to the partner application. The request is redirected to the PingFederate IdP Server.
4. The NetWeaver IdP Adapter retrieves the session ticket from the session cookie, decrypts the session ticket, and then transfers the attributes to the PingFederate IdP Server.
5. The PingFederate IdP server generates a SAML assertion and redirects the request, with the assertion, back through the user's browser to the SP site.

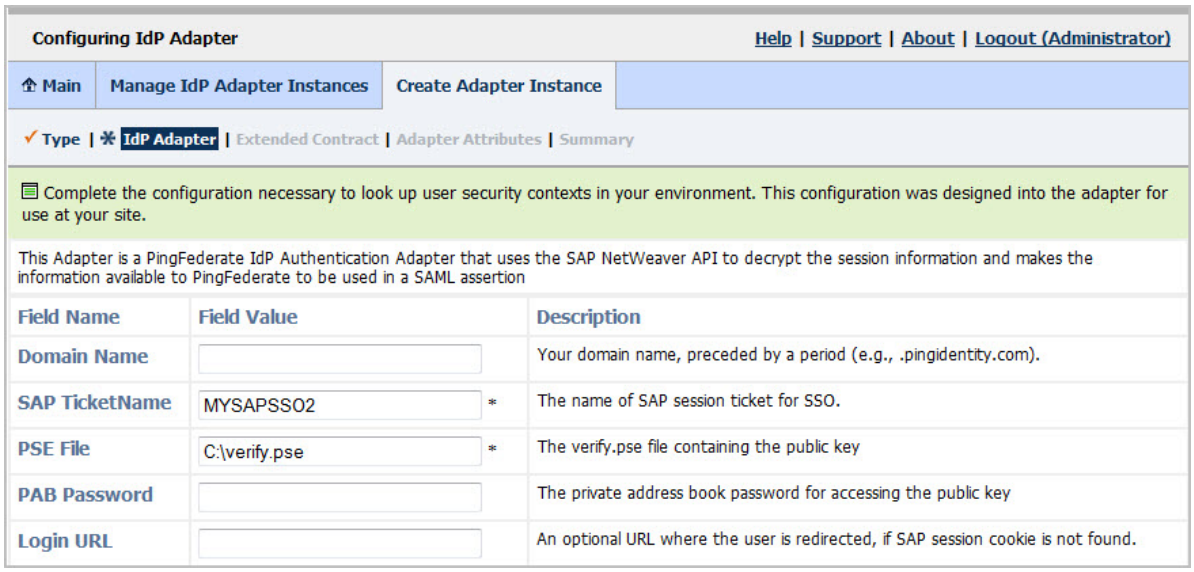
IdP Installation and Setup

This section describes how to install and configure the PingFederate Integration Kit for SAP NetWeaver for an IdP.

1. Unzip the distribution ZIP file and copy the following file from `dist` to the `server/default/deploy` directory in your PingFederate server installation:

   `pf-netweaver-adapter-1.0.jar`

2. Obtain the SSO extension library from SAP and install the libraries on the system running PingFederate (see System Requirements on page 4).
3. Log on to the PingFederate administrative console and click **Adapters** from the My IdP Configuration side of the Main Menu screen.
4. For more information, see Configuring IdP Adapters in the PingFederate *Administrator's Manual*.
5. Click **Create New Adapter Instance**.
6. Enter the Instance Name and Instance ID. Select PF4 NetWeaver IdP Adapter v1.0 as the Type and click **Next**.



7. Enter the values for adapter configuration described below and click **Next**.

Property	Description
Domain Name	Your domain name, preceded by a period (e.g., ".pingidentity.com").
SAP TicketName	The name of SAP session ticket for SSO.
PSE File	The path to `verify.pse`. This file contains the public key for verifying the digital signature. Contact SAP support to obtain this file.
PAB Password	The private address-book password for accessing the public key.
Login URL	An optional URL where the user is redirected if SAP session ticket is not found.

8. Optionally, on the Extended Contract screen, you can configure additional attributes for the adapter. (See Key Concepts in the PingFederate *Administrator's Manual*.)
9. For instance, you can use the extended adapter contract for Policy Server response-object attributes. Click **Next**.
10. On the Adapter Attributes screen, select userId under Pseudonym. You may also select any extended attributes specified in the previous screen. Click **Next**.
11. For more information about this screen, see Setting Pseudonym Values and Masking in the PingFederate *Administrator's Manual*.
12. On the Summary screen, verify that the information is correct and click **Done**.
13. Click **Save** to complete the adapter configuration.

SAP J2EE Setup

➢ Configure NetWeaver J2EE to create SSO tickets.

For instructions, see the SAP Help.

Testing the IdP Adapter

You can test this adapter using the IdP Quick-Start Applications that ships with PingFederate 5.x-6.2. For PingFederate versions 6.3 and later, the Quick-Start Applications are available from the Ping Identity download site. Follow this procedure to verify adapter functions:

1. Set up PingFederate to run the SP Application according to instructions in the PingFederate *Quick-Start Guide*.
2. Configure an instance of the NetWeaver IdP Adapter (see IdP Installation and Setup on page 6.)
3. Reconfigure the SP connection to use the NetWeaver Adapter instance.

   Delete the existing adapter instance and map the NetWeaver Adapter instance in its place. See IdP Adapter Mapping in the PingFederate *Administrator's Manual* for detailed information.
4. On a Web page protected by the NetWeaver Application Server, create an "SSO" link to the PingFederate `startSSO` endpoint, including the sample SP's connection ID, in the following format:

   ```
   http[s]://<PF_host>:<port>/IdP/startSSO.ping
   ?PartnerSpId=<connection_id>
   ```

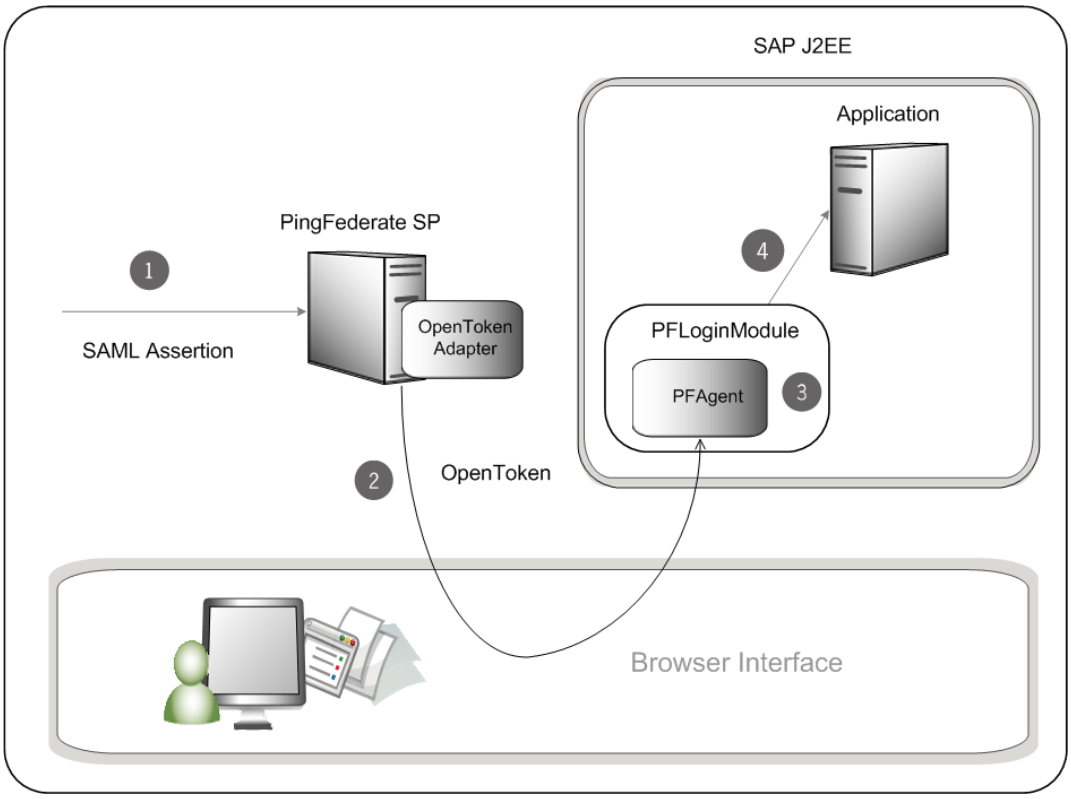
   where:

   - `<PF_host>` is the machine running the PingFederate server,
   - `<port>` is the PingFederate port (refer to the PingFederate *Administrator's Manual*),
   - `<connection_id>` is the Connection ID of the SP connection.
5. Access the protected Web page by authenticating through NetWeaver, and click the SSO link.
6. You are logged on to the Quick-Start SP Application.

Implementing SP Functionality

The PingFederate SP server receives an assertion (see Service Provider SSO Configuration in the PingFederate *Administrator's Manual*), wraps the received attributes into `OpenToken`, and redirects to an application protected by NetWeaver. The `PFLoginModule` configured in NetWeaver extracts the `UserID` from `OpenToken` and authenticates the user. Note that `UserID` is the value of the "subject" attribute in the `OpenToken`.

The following figure illustrates the request flow and how the PingFederate OpenToken SP Adapter wraps attributes from the assertion into `OpenToken` and passes them to SAP NetWeaver (J2EE Engine):



Processing Steps

1. The PingFederate SP server receives a SAML assertion from the IdP.
2. The PingFederate SP server wraps the attributes from the SAML assertion into an `OpenToken` and redirects the token through the user's browser to the application(s) deployed on the SAP J2EE Server.
3. `PFLoginModule`, installed in SAP J2EE Server, parses the `OpenToken` and retrieves the `UserID`.
4. The SAP J2EE server authenticates the user using this UserID and grants access to the SAP Application.

SP Installation and Setup

This section describes how to install and configure the PingFederate Integration Kit for SAP NetWeaver for an SP, as well as NetWeaver administrative information.

OpenToken Adapter Setup

Note: If you have already deployed version 2.5.1 (or higher) of the OpenToken Adapter skip steps 1 through 4 in the following procedure.

1. Stop the PingFederate server if it is running.
2. Remove any existing OpenToken Adapter files (`opentoken*.jar`) from the directory:

   `<PF_install>/pingfederate/server/default/deploy`

   The adapter JAR file is `opentoken-adapter-<version>.jar`.

   Note: In the same directory (`..server/default/deploy`), delete the file `opentoken-java-1.x.jar`, if it exists.

   Important: Delete the file `opentoken-adapter.jar`, if it exists, from the directory: `<PF_install>/pingfederate/server/default/lib`

3. Unzip the integration-kit distribution file and copy opentoken-adapter-2.5.1.jar from the /dist directory to the PingFederate directory:

   `<PF_install>/pingfederate/server/default/deploy`

4. Start or restart the PingFederate server.
5. Configure an instance of the OpenToken Adapter. (See OpenToken Adapter Configuration in the PingFederate *Administrator's Manual*.)
6. On the Adapter Actions screen in the adapter setup steps, click the **Invoke Download** link and then click **Export** to download the `agent-config.txt` properties file to a directory that is readable by the SAP J2EE Server.

SAP J2EE Setup for NetWeaver 7.0

1. Deploy the login module included with this distribution (`PFLoginModuleLibrary.sda`) to NetWeaver using the Software Deployment Manager (SDM).

   Note: For information on how to deploy a login module, please refer to SAP Help.

2. Add a reference to the `Classloader` through the Config Tool, using this value for the library:
3. PingIdentity~PFLoginModuleLibrary

   Note: For information on how to add a reference, please refer to the SAP Help for the Config Tool.

4. Configure the login module through the Visual Administrator, using the class name `com.pingidentity.adapters.netweaver.sp.PFLoginModuleClass` and the following options:

Option	Description
agentPropertiesFileName	Filename with full path to the location of OpenToken properties file (for example, C:\`agent-config.txt`).
pfBaseUrl	Base URL to the PingFederate SP instance.
enableSPSSO	If `true`, `PFLoginModule` redirects to the `ssoUrl` (below) if

Option	Description
	`OpenToken` is not found in the request. This enables SP-initiated SSO functionality for NetWeaver. (Default: `false`)
ssoUrl	URL for redirect if SP-initiated SSO, required only if is enabled (above). The value required is PingFederate's application endpoint to start the SSO: `http[s]://<PF_host>:<port>/SP/startSSO.ping ?PartnerIdpId=<connection_id>` For more information, see Developer Notes below.
excludeUrl	List of excluded resource URIs using regular expressions. For example: `.*/webdynpro.*`
enableSSOCookie	If `true` and `enableSPSSO` is set to `true`, `PFLoginModule` redirects *only* if a cookie (an SSO Cookie, defined below) is found in the request. The SP sets an SSO Cookie in the user's browser during an initial IdP-initiated SSO event. When the user arrives at the NetWeaver SP in the future, with the SSO Cookie, the user is redirected to the `ssoUrl`. If `false` and `enableSPSSO` is set to `true`, the PFLoginModule redirects any user to the `ssoUrl`, regardless of any SSO Cookie. (Default: `false`)
ssoCookieName	The name of the SSO cookie to set in the user's browser, required only if `enableSSOCookie` is set to `true`.

Note: For information on how to configure a login module, please refer to the SAP Help.

5. Configure an application to use the login module. A sample configuration, which allows for both SSO and direct authentication, is shown below:

Login Module	Flag
EvaluateTicketLoginModule	SUFFICIENT
PFLoginModule	REQUISITE
BasicPasswordLoginModule	REQUISITE
CreateTicketLoginModule	OPTIONAL

Note: For information on how to configure an application, please refer to the SAP Help.

Developer Notes

- To allow for deep linking for SP-initiated SSO, the login module appends the target-resource URL to the `ssoUrl` property. This feature is supported only for NetWeaver portals; for other applications the target resource is not appended and the user will go to the Default URL configured in PingFederate. (For more information, see Configuring Default URLs in the PingFederate *Administrator's Manual*.)
- The login module JAR file (`PFLoginModuleJAR.jar`), along with supporting JARS included with this distribution, can be used to create a custom SDA for the NetWeaver platform. For more information see the SAP Help.

SAP J2EE Setup for NetWeaver 7.3 or 7.4

1. Deploy the login module included with this distribution (`PFLoginModuleLibrary.ear`) to NetWeaver using the appropriate version of SAP NetWeaver Developer Studio.

Note: For information on how to deploy a login module, including how to deploy through shell scripts, please refer to SAP Help.

2. Configure the login module through the NetWeaver Administrator, using the following options:

Option	Description
agentPropertiesFileName	Filename with full path to the location of OpenToken properties file (for example, C:\`agent-config.txt`).
pfBaseUrl	Base URL to the PingFederate SP instance.
enableSPSSO	If `true`, `PFLoginModule` redirects to the `ssoUrl` (below) if `OpenToken` is not found in the request. This enables SP-initiated SSO functionality for NetWeaver. (Default: `false`)
ssoUrl	URL for redirect if SP-initiated SSO, required only if is enabled (above). The value required is PingFederate's application endpoint to start the SSO: `http[s]://<PF_host>:<port>/SP/startSSO.ping`

Option	Description
	`?PartnerIdpId=<connection_id>` For more information, see Developer Notes below.
excludeUrl	List of excluded resource URIs using regular expressions. For example: `.*/webdynpro.*`
enableSSOCookie	If `true` and `enableSPSSO` is set to `true`, `PFLoginModule` redirects *only* if a cookie (an SSO Cookie, defined below) is found in the request. The SP sets an SSO Cookie in the user's browser during an initial IdP-initiated SSO event. When the user arrives at the NetWeaver SP in the future, with the SSO Cookie, the user is redirected to the `ssoUrl`. If `false` and `enableSPSSO` is set to `true`, the PFLoginModule redirects any user to the `ssoUrl`, regardless of any SSO Cookie. (Default: `false`)
ssoCookieName	The name of the SSO cookie to set in the user's browser, required only if `enableSSOCookie` is set to `true`.

Note: For information on how to configure a login module, please refer to the SAP Help.

3. Configure an application to use the login module. A sample configuration which allows for both SSO and direct authentication is shown below:

Login Module	Flag
EvaluateTicketLoginModule	SUFFICIENT
PFLoginModule	REQUISITE
BasicPasswordLoginModule	REQUISITE
CreateTicketLoginModule	OPTIONAL

Note: For information on how to configure an application, please refer to the SAP Help.

Developer Notes

- To allow for deep linking for SP-initiated SSO, the login module appends the target-resource URL to the `ssoUrl` property. This feature is supported only for NetWeaver portals; for other applications the target resource is not appended and the user will go to the Default URL configured in PingFederate. (For more information, see Configuring Default URLs in the PingFederate *Administrator's Manual*.)
- The login module JAR file (`PFLoginModuleJAR.jar`), along with supporting JARS included with this distribution, can be used to create a custom EAR for the NetWeaver platform. For more information see the SAP Help.

Testing the SP Adapter

You can test this adapter using the IdP Quick-Start Applications that ship with PingFederate 5.x-6.2. For PingFederate versions 6.3 and later, the Quick-Start Applications are available from the Ping Identity download site. Follow this procedure to verify adapter functions:

1. Set up PingFederate to run the IdP Application according to instructions in the PingFederate *Quick-Start Guide*.
2. Configure an instance of the OpenToken SP Adapter and PFLoginModule (see SP Installation and Setup on page 9.)
3. Reconfigure the IdP connection to use the OpenToken Adapter instance configured for NetWeaver.

   Delete the existing adapter instance for the connection and map the OpenToken Adapter instance in its place. See Configuring Adapter Mapping and User Lookup in the PingFederate *Administrator's Manual*.
4. Protect a Web page using NetWeaver.
5. On the same NetWeaver server, create an unprotected Web page with a hyperlink to PingFederate's SP-initiated SSO endpoint in the following format:

   ```
   http[s]://<PF_host>:<port>/sp/startSSO.ping
   ?TargetResource=<protected_resource>
   ?PartnerIdpId=<connection_id>
   ```

   where:

   - `<PF_host>` is the machine running the PingFederate server,
   - `<port>` is the port (refer to the PingFederate *Administrator's Manual*),
   - `<protected_resource>` is the Web page protected in the previous step,
   - `<connection_id>` is the Connection ID of the IdP connection.
6. Click the SSO link on the unprotected Web page.

   You should arrive at the IdP Quick-Start Application's login page.
7. Add at least one of the users in the username drop-down list to NetWeaver.

   Alternatively, you can add users already in NetWeaver to the Quick-Start Application's user properties file.
8. On the IdP Application's login page, log in with a username managed by NetWeaver.

   You should be redirected to NetWeaver-protected Web page.