PingFederate® 4.4

Quick Start Guide:

Using the Sample Applications

Ping Identity™

Part Number 3007-152
Version 4.4
April, 2007

Ping Identity Corporation
1099 18th Street, Suite 2950
Denver, CO 80202
U.S.A.

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

Trademarks

Disclaimer

Contents

About This Guide

The PingFederate sample application *Quick Start Guide* provides procedures for setting up a deployment of the PingFederate server and using it with the accompanying sample applications. This deployment establishes a simple identity federation between two Web sites. You can use these procedures either for evaluation or to familiarize yourself with PingFederate for future in-depth implementations.

Intended Audience

This manual is intended for security and network administrators and other IT professionals responsible for identity management among both internal and external business entities.

Overview

The manual consists of the following chapters:

- Chapter 1, "Introduction"— System requirements, overview, installation requirements and possible paths through this book.
- Chapter 2, "Server and Adapter Setup"— Starting PingFederate and configuring server settings.
- Chapter 3, "Connection Scenarios"— Configuring the four different identity-federation scenarios: IdP-initiated SSO and SLO, and SP-initiated SSO and SLO.
- Chapter 4, "Using the Sample Applications"— Installing and using the sample applications (for both Java and .Net).
- Appendix A, "Automating the Configuration"— Using a script to configure PingFederate and the sample applications.

Other Documentation

- The *Administrator's Manual*, located in `<pf_install_dir>/pingfederate/docs`, provides important background information and key concepts you may need for understanding identity federation and the PingFederate server-setup procedures in this *Guide*. (`<pf_install_dir>` is the topmost folder where the PingFederate server is installed.)
- This *Guide* provides a sample configuration of the Standard Adapter. The sample applications use the predeployed Java and .NET agent toolkits. For additional information on the Standard Adapter, see *Appendix A: Standard Adapter Configuration* in the PingFederate *Administrator's Manual*. For additional information on agent deployment, download the Integration Kit that matches your environment from www.pingidentity.com and view the Integration Kit *User Guide* in the `docs` directory.

Tip: PingFederate also provides context-sensitive online Help. Click **Help** in the upper-right portion of the administrative console for immediate guidance, along with links to related information.

PingFederate documents include hypertext links to Web sites that provide installation instructions, file downloads, and reference documentation. These links were tested prior to publication, but they may not remain current throughout the life of these documents. Please contact Ping Identity Support (support@pingidentity.com) if you encounter a problem.

Text Conventions

This document uses text conventions identified below.

Table 1: Text Convention Definitions

Convention	Description
`Fixed Width`	Indicates text that must be typed exactly as shown in the instructions. Also used to represent program code, file names, and directory paths.
Blue text	Used in online documents to indicate hypertext links.
Italic	Used for emphasis and to identify document titles.
▶ [text]	Used for procedures where only one step is required.
Sans serif	Identifies GUI text as shown on a screen. Example: "Print Document dialog"
Sans serif bold	Identifies menu items, navigational links, or buttons. For example: Click **Save**.

Chapter 1

Introduction

PingFederate is a best-of-breed identity federation server that implements multiple standards-based federation protocols to provide cross-domain single sign-on (SSO) and attribute exchange. This *Quick Start Guide* provides instructions for using PingFederate on Windows with the sample applications.

Overview

These procedures allow you to set up PingFederate to act as both an Identity Provider (IdP) and a Service Provider (SP).

- You will configure the IdP server to look up and send authentication information to the SP.
- You will configure the SP server to forward this information to the SP sample application to create the local user session. For complete scenarios, you may also configure the SP server to send authentication requests to the IdP on behalf of local users.

The SAML 2.0 protocol offers numerous use cases and configuration options for implementing connections with partners. This *Guide* presents PingFederate configuration options that demonstrate a few of these scenarios using the sample applications.

Tip: For a complete discussion of identity federation and the SAML 2.0 protocol, refer to the "Key Concepts" and "Supported Protocols" chapters in the *Administrator's Manual*.

Context-sensitive Help is also available for all configuration screens and may provide links to related information.

Sections in the *Guide* cover the following configuration topics:

- **Server Settings** (see "Configure Server Settings" on page 10) – Configures the local server settings necessary to operate PingFederate. This section includes deployment of IdP and SP adapters that look up and create a user session with the sample application.

  Tip: This *Guide* provides instructions for using the Standard Adapter with either the Java sample application or the .NET sample application. For information about adapters, see the "Key Concepts" chapter in the PingFederate *Administrator's Manual*.

- **IdP-Initiated SSO** (see "IdP-Initiated SSO" on page 28) – Walks through the steps needed to set up IdP and SP connection partners. This section includes: identity mapping, attribute contract creation, configuration of the POST Profile, and application of certificates.
- **IdP-Initiated SLO** (see "IdP-Initiated SLO" on page 45) – Builds on the IdP-initiated SSO scenario by adding configuration information needed to enable the use case where SLO is initiated from the IdP application.
- **SP-Initiated SSO** (see "SP-Initiated SSO" on page 50) – Builds on the previous configurations to demonstrate how partners can implement a use case where the user starts at the destination application (SP application) for sign-on.
- **SP-Initiated SLO** (see "SP-Initiated SLO" on page 52) – Builds on the preceding SSO scenarios by adding configurations between IdP and SP partners that are needed to enable the use case where SLO is initiated from the SP application.
- **Sample Applications** (see "Using the Sample Applications" on page 55) – Provides installation and operation instructions for using the sample applications to execute common federation scenarios.
- **Quickstart Automation Script** (see "Automating the Configuration" on page 65) – Detailed instructions for running the configuration- automation script.

Possible Paths Through This Guide

Fully Automated Path	Install PingFederate, run the configuration script, and install and run the sample applications.
Basic Manual Path	Install PingFederate, configure local server settings, configure IdP-initiated SSO, install and run the sample applications, and then return to the configuration sections to set up other scenarios.
Complete Manual Path	Install PingFederate, configure local server settings, configure IdP-initiated SSO, add IdP-initiated SLO, add SP-initiated SSO, add SP-initiated SLO, and then install and run the sample applications.

Each path is discussed in detail below.

Fully Automated Path

This is the quickest path to demonstrate all the SSO/SLO scenarios with the sample applications. You can use a prepackaged auto-configuration script to fully configure the PingFederate server and deploy the sample applications (see "Automating the Configuration" on page 65).

After auto-configuration, you can also follow the screen-by-screen configurations in the chapters "Server and Adapter Setup" and "Connection Scenarios" to gain a feel for the configuration process.

Basic Manual Configuration – IdP-Initiated SSO

For a quick, hands-on learning experience, follow the manual configuration steps for IdP-initiated SSO only. When the configuration is complete, you can jump directly to the sample applications to test this use case. After this test, you can build out other scenarios, starting with IdP-initiated SLO.

To configure a basic configuration (IdP-Initiated SSO):

1. Follow the steps in "Server and Adapter Setup" on page 9.
2. Configure the IdP and SP connections – see "IdP-Initiated SSO" on page 28.
3. Install and run the sample applications – see "Using the Sample Applications" on page 55.

Complete Manual Configuration

For an in-depth learning experience, configure all SSO/SLO scenarios before testing with the sample applications.

1. Follow the steps in "Server and Adapter Setup" on page 9.
2. Configure IdP-initiated SSO – see "IdP-Initiated SSO" on page 28.
3. Add IdP-initiated SLO – see "IdP-Initiated SLO" on page 45.
4. Add SP-initiated SSO – see "SP-Initiated SSO" on page 50.
5. Add SP-initiated SLO – see "SP-Initiated SLO" on page 52.
6. Install and run the sample applications – see "Using the Sample Applications" on page 55.

Extended Uses For the Sample Applications

This guide demonstrates one set of SAML 2.0 use cases. The PingFederate server supports other protocols and many additional value-added configuration options. After practicing with the basic options provided, you can add and test configurations that more closely match your desired implementation. (Sample configurations are not provided for these other implementations—please consult the *Administrator's Manual* for information.)

Other scenarios that can be configured with the sample applications include:

- **Other protocols** – SAML 1.0, SAML 1.1, and WS-Federation
- **Different Bindings** – The basic scenarios illustrate the POST profile. You can extend this to include Artifact or Redirect binding types. You can also adjust the security policy settings if you change binding types.
- **Different Identity Mapping** – You can choose to test out transient- or pseudonym-based identity mapping styles in the SP connection and account-linking-based identity mapping in the IdP connection.

System Requirements

You need the following software installed on your system in order to run PingFederate and the sample applications:

For PingFederate:

Please refer to the "System Requirements" section of the PingFederate *Administrator's Manual.*

For the Java Sample Application:

- Apache Jakarta Tomcat 5.5 (or higher) – available at http://jakarta.apache.org/tomcat/index.html

  Set the environment variable `CATALINA_HOME` to the Tomcat installation directory. Retain the default port of 8080.

- J2SE 1.4 (or higher) – available at http://java.sun.com/j2se/1.4.0/download.html

  Set the environment variable `JAVA_HOME` to the installation directory. Add the location of the Java installation `\bin` directory to your `PATH` environment variable.

- Javascript-enabled Web browser

For the .NET Application:

- Microsoft Internet Information Services (IIS) v5 and above.
- On Windows 2003 servers, Microsoft .NET Framework 1.1 or 2.0 must be installed and registered. Please refer to Windows Update (under Tools in Internet Explorer) for the download.

  Important: The .NET sample applications depend on a third-party library (`ManagedZLib.dll`), which in turn depends on the Microsoft Visual C++ library. If you are running .NET 2.0, the C++ library might not be installed on your Windows server. The library is available in the "Microsoft C++ 2005 Redistributable Package" at: http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=32BC1BEE-A3F9-4C13-9C99-220B62A191EE

  On Windows 2000 servers, only the .NET Framework 1.1 is supported; the .NET 2.0 Framework has not been tested.

  You can register the framework by entering the following command:

  ```
  <WINDOWS>\Microsoft.NET\Framework\<VERSION>\
     aspnet_regiis -i -enable
  ```

  where <*WINDOWS*> is the location of the operating system files and <*VERSION*> is the exact version of .NET Framework.

If the .NET Framework was previously registered without the `-enable` option, `.aspx` pages will not be registered in IIS. You can resolve this in one of two ways:

▶ Either uninstall Microsoft .NET Framework by entering the following command:

```
<WINDOWS>\Microsoft.NET\Framework\<VERSION>\
   aspnet_regiis -u
```

Then reinstall Microsoft .NET Framework with the `-enable` option as specified above.

OR:

Add `default.aspx` in the **Documents** tab of the virtual directories for `IdpSample` and `SpSample` (see "Using the Sample Applications" on page 55).

For the Quick Start Script:

Apache Ant 1.6.2 (or newer) – available at http://ant.apache.org/bindownload.cgi

Ant is used only if you want to configure the sample applications and the PingFederate server automatically (see "Automating the Configuration" on page 65).

Set the environment variable `ANT_HOME` to the `Ant` installation directory. Add the location of the `Ant` installation `\bin` directory to the `PATH` variable.

Install PingFederate

This section provides a brief installation procedure for PingFederate. For a more complete description of the procedure, see the "Installation" chapter in the PingFederate *Administrator's Manual*.

To install PingFederate from the `zip` file.

1 Request a license key.

   Go to the Ping Identity Web page (http://www.pingidentity.com/support/licensing).

2. Make sure you are logged into your system with appropriate privileges to install and run an application.
3. Verify that the J2SDK 1.5 (or higher) is installed and environment and `PATH` variables are set correctly.
4. Create an installation directory.

   ✓ **Important:** The installation path and the directory name must *not* contain spaces.

5. Unzip the PingFederate distribution file into the installation directory.
6. Verify that the license key file is named:

   `pingfederate.lic`

7. Save the license key file in the directory:

   `<pf_install_dir>\pingfederate\server\default\conf`

Chapter 2

Server and Adapter Setup

This chapter describes how to start PingFederate and configure settings for the server and the standard adapter, which PingFederate uses to communicate with the sample applications.

Tip: A part of this configuration requires that you know the machine name(s) and port numbers where the IdP and SP sample applications will be deployed. You might wish to follow the procedures in either "Setting Up the Java Sample Applications" on page 56 or "Setting Up the .NET Sample Applications" on page 57 before proceeding. Otherwise, use placeholders for the information; you can easily update the configuration later.

Start PingFederate

To start PingFederate:

1. Run the following script:

   (Windows) `<pf_install_dir>/pingfederate/bin/run.bat`

   (Linux) `<pf_install_dir>/pingfederate/bin/run.sh`

   Wait a moment for the server to start up—the last message displayed in the sequence is:
   `Started in XXs:XXms`

2. Access the PingFederate administrative console using the following URL:

   `https://<hostname>:9999/pingfederate/app`

   where `<hostname>` is the fully qualified domain name of the server running PingFederate.

3. If you are running the server console for the first time, enter the default Username and Password:

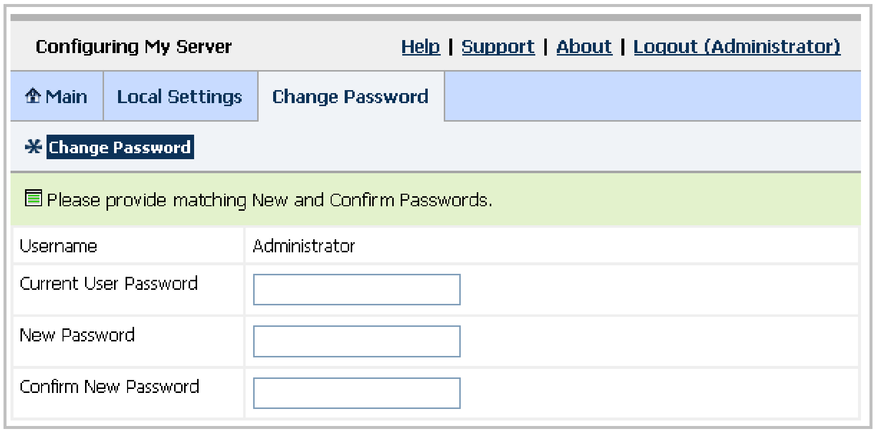
   Username: `Administrator`

   Password: `2Federate`

   If you have already run through the initial setup, enter the Username and Password of an administrator with Admin and Crypto Admin privileges (for more information, see the "System Administration" chapter in the *Administrator's Manual*).

   Click **Login**.

4. If you are running the server console for the first time, you will be required to change the Administrator password.



Please provide matching New and Confirm Passwords.

Username	Administrator
Current User Password	
New Password	
Confirm New Password	

   Update the password and click **Save**.

Configure Server Settings

Follow the procedures in this section to configure My Server after installing PingFederate.

Note: If you have already gone through these post-installation steps, click **Server Settings** on the Main Menu and skip to Step 8 below. Ensure that SAML 2.0 protocols are enabled according to Step 8 and change your configuration to match directions in Step 10. Then continue with the adapter setup procedures in the rest of this chapter.

1. At the Welcome screen, click **Next**. This screen describes the benefits of PingFederate.
2. At the Additional Resources screen, click **Next**. This screen describes supplemental information available for PingFederate.
3. On the Licensing screen, read the agreement. If you agree to the terms, select **Accept the license agreement** and click **Next**.

4. On the System Administration screen, choose **Single-user Administration** or **Multi-user Administration** and click **Next.**

   Base your choice of user administration on the style of application management your company uses.

   Note: This *Guide* assumes multi-user configuration. If you choose single-user administration, the Server Settings list of steps near the top of the administrative console screen will not include "Account Management," as shown in the screen illustrations in this chapter. This difference will not affect the operation the server or the sample applications.

5. (Optional) On the System Info screen, you can enter the indicated information. Click **Next**.

6. (Optional) On the Notification Options screen, you can choose whether to designate an email address to receive licensing notices that affect the operation of the server.

   Note: If you have a perpetual, unlimited license, this option does not appear. If you have such a license *and* you chose single-user administration at the System Administration step, this step is not presented.

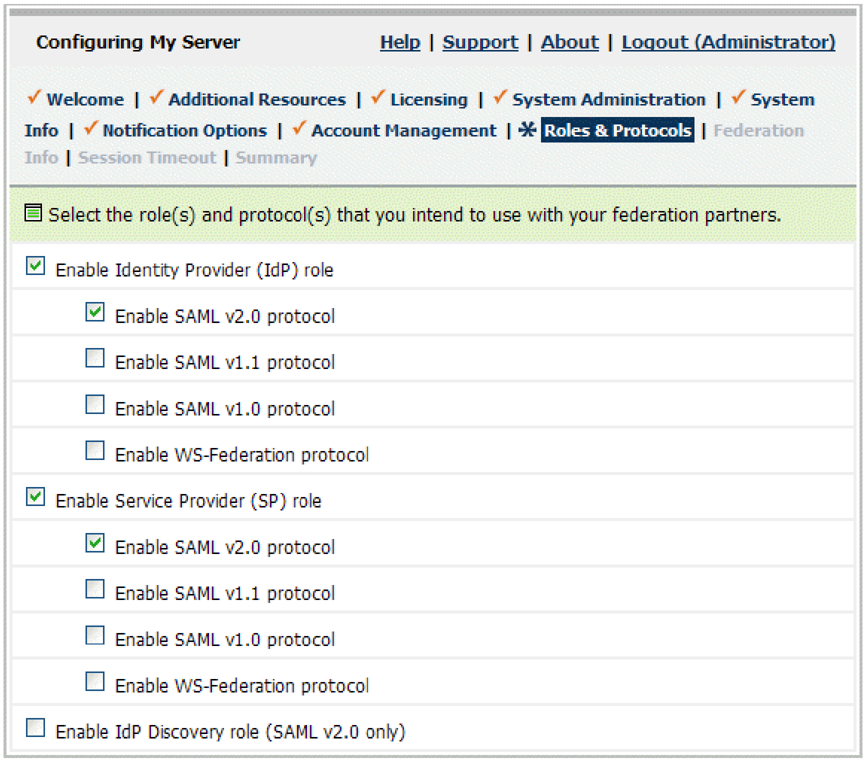
   For multi-user administration, you can also specify whether password changes are sent to a user's email account.

   If you make either selection, then you will be required to set up a connection with your SMTP server.

7. On the Account Management screen, if you have chosen multi-user administration, you can manage existing administrator accounts as well as add new administrators. No changes are required at this time; click **Next**.

8. On the Roles & Protocols screen, check the Enable Identity Provider (IdP) and Enable Service Provider (SP) role checkboxes; also check the Enable SAML v2.0 protocol checkboxes under each role.

   Note: To expedite demonstration of the sample applications, both IdP and SP configurations are made on the same server.


Configuring My Server
Help | Support | About | Logout (Administrator)
✓ Welcome | ✓ Additional Resources | ✓ Licensing | ✓ System Administration | ✓ System Info | ✓ Notification Options | ✓ Account Management | ✱ Roles & Protocols | Federation Info | Session Timeout | Summary

Select the role(s) and protocol(s) that you intend to use with your federation partners.

- ☑ Enable Identity Provider (IdP) role
  - ☑ Enable SAML v2.0 protocol
  - ☐ Enable SAML v1.1 protocol
  - ☐ Enable SAML v1.0 protocol
  - ☐ Enable WS-Federation protocol
- ☑ Enable Service Provider (SP) role
  - ☑ Enable SAML v2.0 protocol
  - ☐ Enable SAML v1.1 protocol
  - ☐ Enable SAML v1.0 protocol
  - ☐ Enable WS-Federation protocol
- ☐ Enable IdP Discovery role (SAML v2.0 only)

9. Click **Next**.

10. On the Federation Info screen, enter the following values:

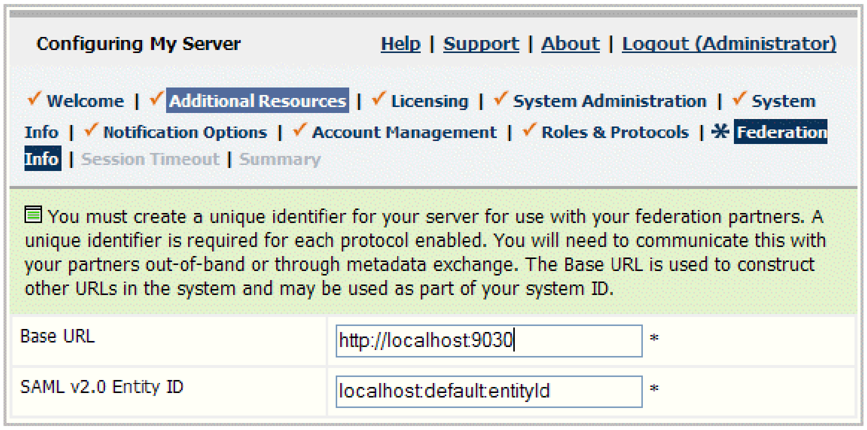
    For Base URL: `http://`*`<pf_host>`*`:9030`

    where *`<pf_host>`* is the fully qualified domain name of the server running PingFederate.

    and:

    For SAML v 2.0 Entity Id: `localhost:default:entityId`

    Click **Next**.

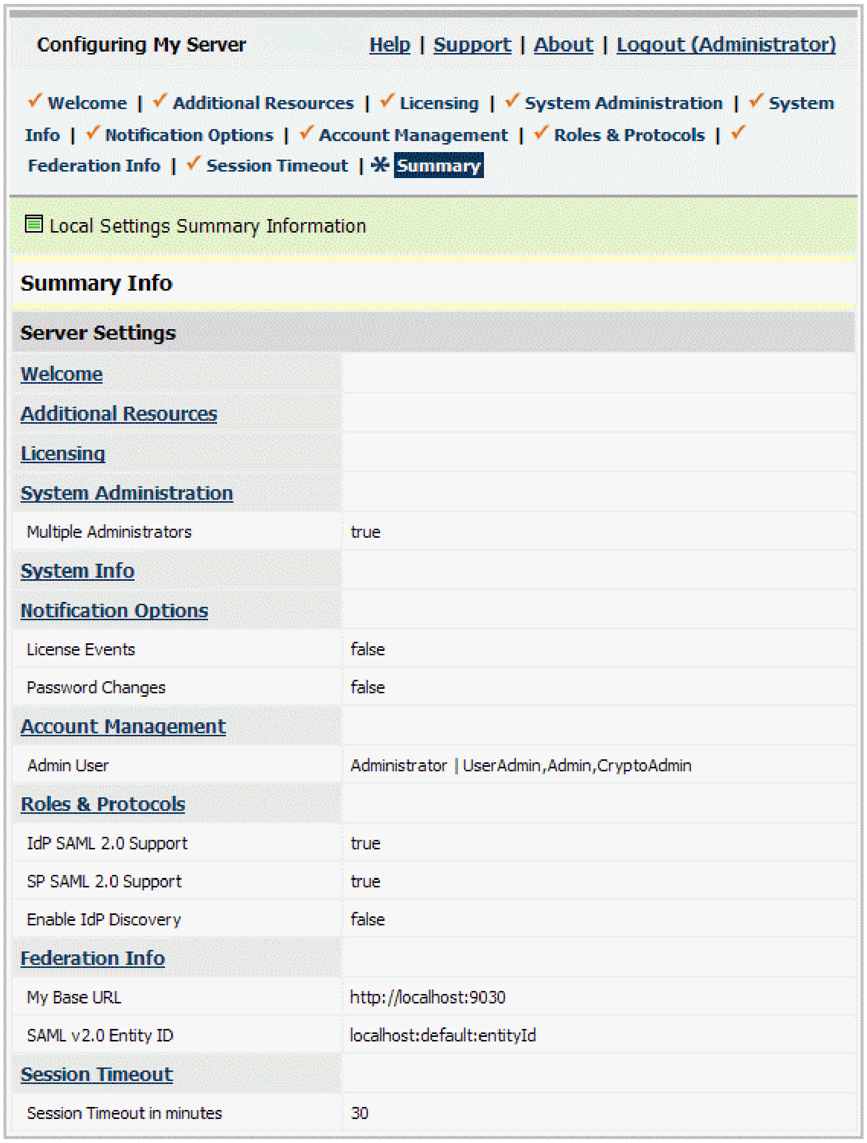

Configuring My Server
Help | Support | About | Logout (Administrator)
✓ Welcome | ✓ Additional Resources | ✓ Licensing | ✓ System Administration | ✓ System Info | ✓ Notification Options | ✓ Account Management | ✓ Roles & Protocols | ✱ Federation Info | Session Timeout | Summary

You must create a unique identifier for your server for use with your federation partners. A unique identifier is required for each protocol enabled. You will need to communicate this with your partners out-of-band or through metadata exchange. The Base URL is used to construct other URLs in the system and may be used as part of your system ID.

Base URL	http://localhost:9030 *
SAML v2.0 Entity ID	localhost:default:entityId *

11. On the Session Timeout screen, you can change the session timeout value or use the default. Click **Next**.

12. The Summary screen displays the completed Server Settings. Click **Save**.



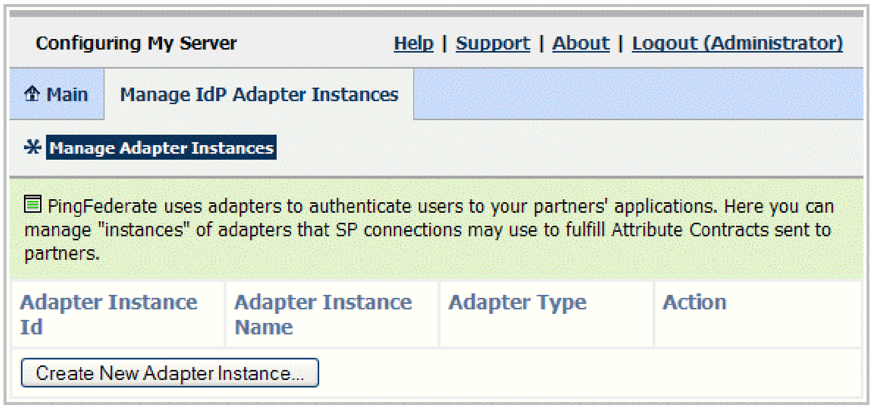
Configuring My Server
Help | Support | About | Logout (Administrator)
✓ Welcome | ✓ Additional Resources | ✓ Licensing | ✓ System Administration | ✓ System Info | ✓ Notification Options | ✓ Account Management | ✓ Roles & Protocols | ✓ Federation Info | ✓ Session Timeout | ✱ Summary
Local Settings Summary Information

Summary Info

Server Settings	
Welcome	
Additional Resources	
Licensing	
System Administration	
Multiple Administrators	true
System Info	
Notification Options	
License Events	false
Password Changes	false
Account Management	
Admin User	Administrator | UserAdmin,Admin,CryptoAdmin
Roles & Protocols	
IdP SAML 2.0 Support	true
SP SAML 2.0 Support	true
Enable IdP Discovery	false
Federation Info	
My Base URL	http://localhost:9030
SAML v2.0 Entity ID	localhost:default:entityId
Session Timeout	
Session Timeout in minutes	30

Configure the IdP Adapter

1. On the Main Menu under My IdP Configuration, click **Adapters**.
2. On the Manage Adapter Instances screen, click the **Create New Adapter Instance** button.

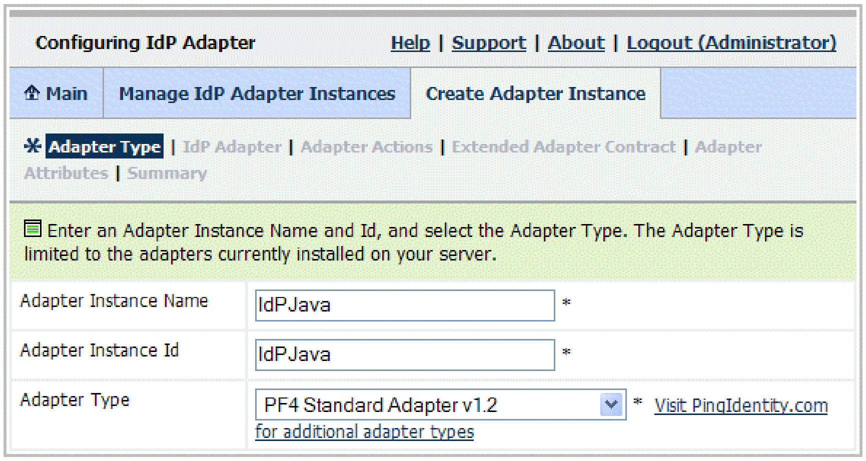

Configuring My Server
Help | Support | About | Logout (Administrator)
Main
Manage IdP Adapter Instances
Manage Adapter Instances
Create New Adapter Instance...

PingFederate uses adapters to authenticate users to your partners' applications. Here you can manage "instances" of adapters that SP connections may use to fulfill Attribute Contracts sent to partners.

Adapter Instance Id	Adapter Instance Name	Adapter Type	Action

3. On the Adapter Type screen, enter or select the values listed in the table below and click **Next**:

Field	Value
Adapter Instance Name	`IdPJava`
Adapter Instance ID	`IdPJava`
Adapter Type	PF4 Standard Adapter v1.2


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

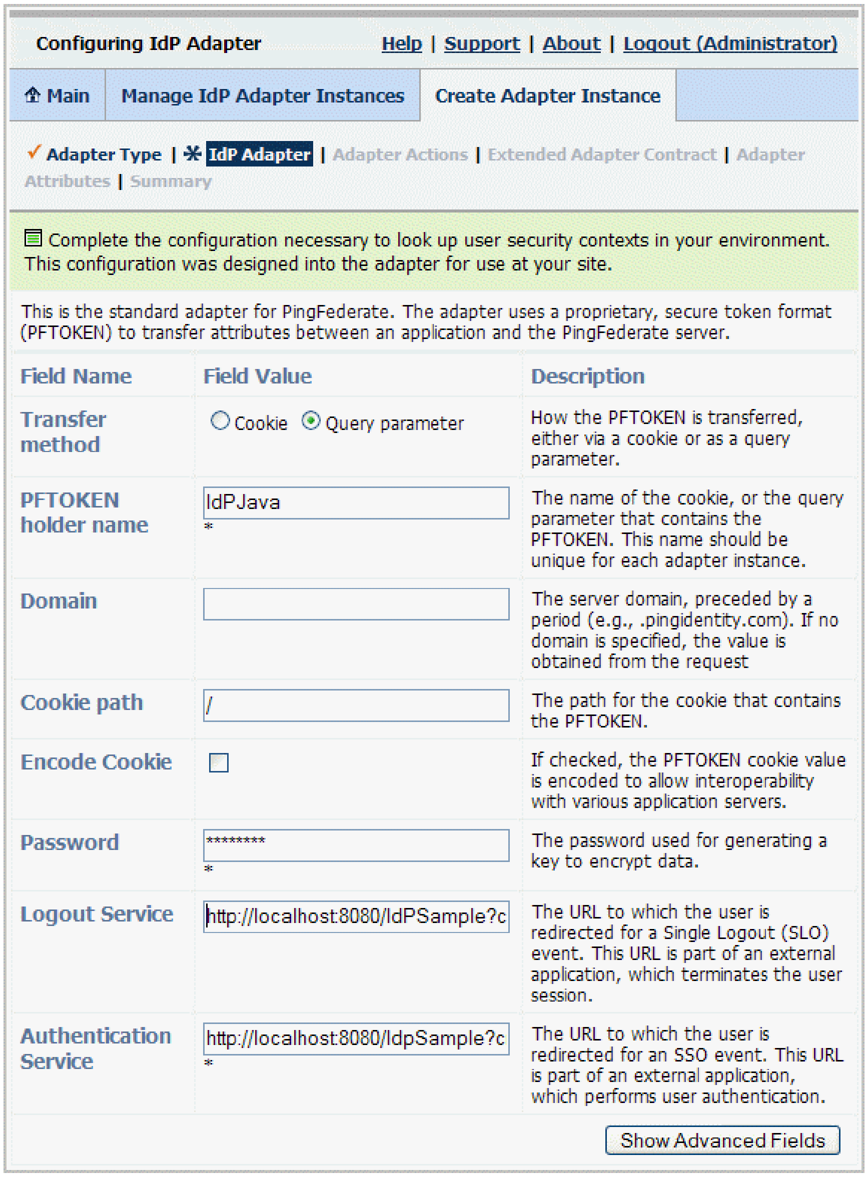
Enter an Adapter Instance Name and Id, and select the Adapter Type. The Adapter Type is limited to the adapters currently installed on your server.

Adapter Instance Name	IdPJava *
Adapter Instance Id	IdPJava *
Adapter Type	PF4 Standard Adapter v1.2 * Visit PingIdentity.com for additional adapter types

4. On the IdP Adapter screen, enter information as shown in the table below (retain default values for items not listed in the table; other fields are not required for the sample application).

Field	**Value**
PFTOKEN holder name	`IdPJava`
Password	A password of your choice to be used for generating a key to encrypt data. Remember this password for configuring the sample application.
Logout Service	`http://<sample_hostname>:<sample_port>/IdpSample/?cmd=slo`
Authentication Service	`http://<sample_hostname>:<sample_port>/IdpSample/?cmd=sso`

The variables `<sample_hostname>` and `<sample_port>` represent the fully qualified domain name and port number of the server running the Java or the .NET sample application (see "Using the Sample Applications" on page 55). The default port for Tomcat (for the Java application) is 8080.

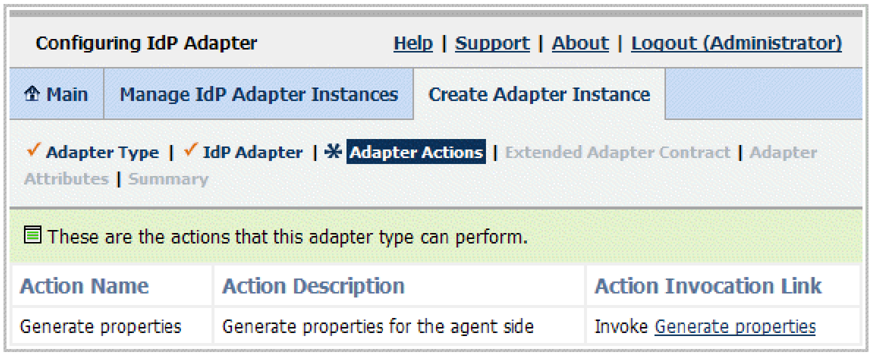

Configuring IdP Adapter
Help | Support | About | Logout (Administrator)
Main
Manage IdP Adapter Instances
Create Adapter Instance
✓ Adapter Type | ✱ IdP Adapter | Adapter Actions | Extended Adapter Contract | Adapter Attributes | Summary
Show Advanced Fields

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 is the standard adapter for PingFederate. The adapter uses a proprietary, secure token format (PFTOKEN) to transfer attributes between an application and the PingFederate server.

Field Name	Field Value	Description
Transfer method	○ Cookie ● Query parameter	How the PFTOKEN is transferred, either via a cookie or as a query parameter.
PFTOKEN holder name	IdPJava *	The name of the cookie, or the query parameter that contains the PFTOKEN. This name should be unique for each adapter instance.
Domain		The server domain, preceded by a period (e.g., .pingidentity.com). If no domain is specified, the value is obtained from the request
Cookie path	/	The path for the cookie that contains the PFTOKEN.
Encode Cookie	☐	If checked, the PFTOKEN cookie value is encoded to allow interoperability with various application servers.
Password	******** *	The password used for generating a key to encrypt data.
Logout Service	http://localhost:8080/IdPSample?c	The URL to which the user is redirected for a Single Logout (SLO) event. This URL is part of an external application, which terminates the user session.
Authentication Service	http://localhost:8080/IdpSample?c *	The URL to which the user is redirected for an SSO event. This URL is part of an external application, which performs user authentication.

5. Click **Next**.
6. On the Adapter Actions screen, click **Generate Properties**.


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

These are the actions that this adapter type can perform.

Action Name	Action Description	Action Invocation Link
Generate properties	Generate properties for the agent side	Invoke Generate properties

On the next screen, click **Export** and save the properties file to your file system.

The values in the resulting file `pfagent.properties` are established by the console configuration and are used by the IdP sample application.

7. Copy the `pfagent.properties` file to one of the following locations and change the filename as shown:

   For Java:

   ```
   <pf_install_dir>\quickstart\sample_app\java\IdpSample
      \config\pfagent-idp.properties
   ```

   For .NET:

   ```
   <pf_install_dir>\quickstart\sample_app\dotnet\
      IdpSample\config\pfagent-idp.config
   ```

   Important: Be sure to save the file as plain text using the filenames shown above.

8. Click **Next**.

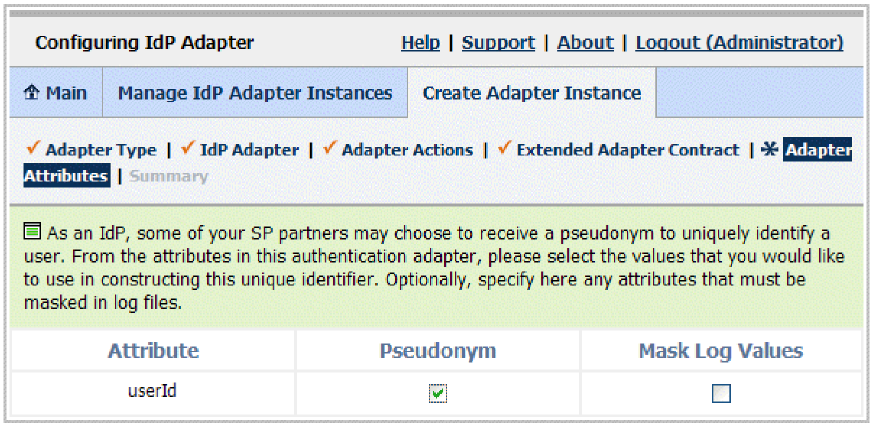
9. On the Extended Adapter Contract screen, you can configure additional attributes for the adapter. This step, however, is not necessary to run the sample application.

   This screen can be used to adjust your adapter contract attribute values after an adapter has already been deployed. (See the "Key Concepts" chapter in the *Administrator's Manual*).

   Click **Next**.

10. On the Adapter Attributes screen, click the checkbox under Pseudonym for userId and click **Next**.

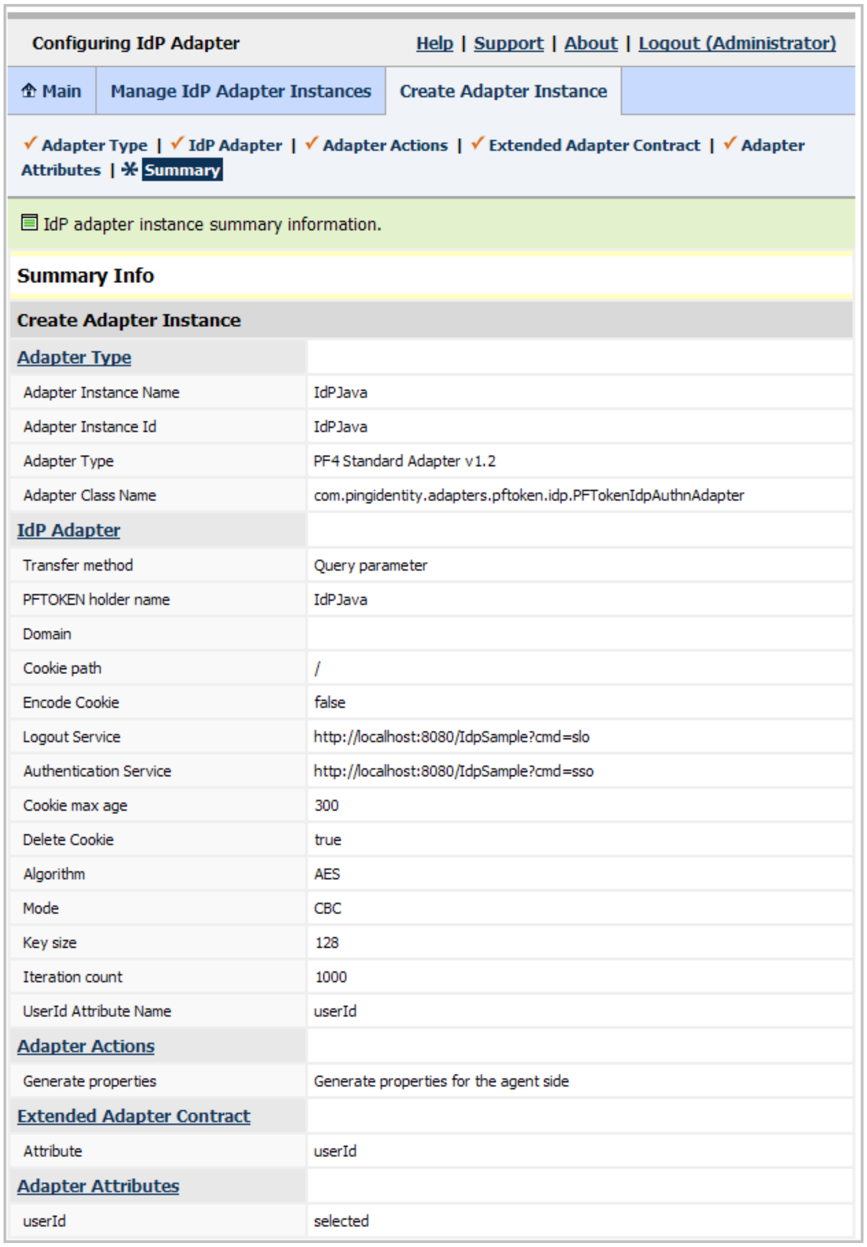
    Pseudonyms may be used for account linking. For information about this subject and about the option of masking log values, see the "Key Concepts" chapter of the *Administrator's Manual.*


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

As an IdP, some of your SP partners may choose to receive a pseudonym to uniquely identify a user. From the attributes in this authentication adapter, please select the values that you would like to use in constructing this unique identifier. Optionally, specify here any attributes that must be masked in log files.

Attribute	Pseudonym	Mask Log Values
userId	☑	☐

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


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

IdP adapter instance summary information.

Summary Info

Create Adapter Instance

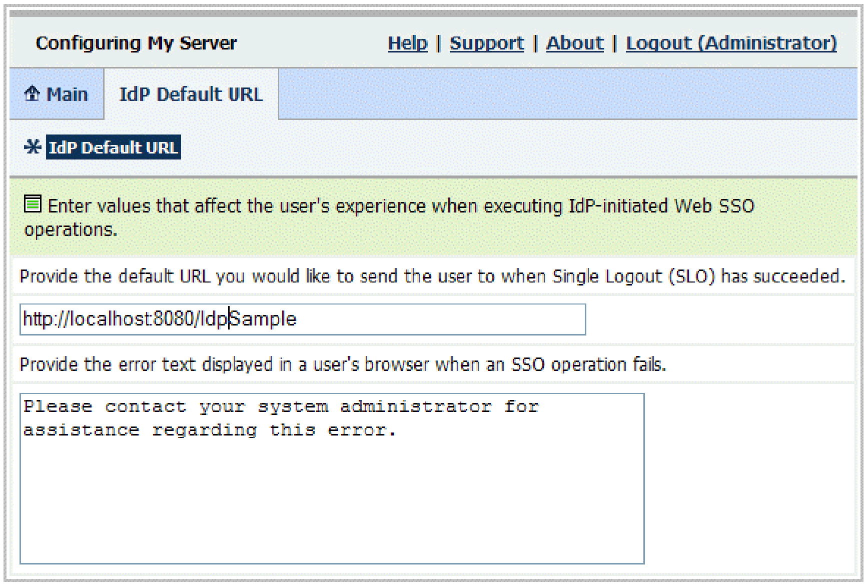
Adapter Type	
Adapter Instance Name	IdPJava
Adapter Instance Id	IdPJava
Adapter Type	PF4 Standard Adapter v1.2
Adapter Class Name	com.pingidentity.adapters.pftoken.idp.PFTokenIdpAuthnAdapter
IdP Adapter	
Transfer method	Query parameter
PFTOKEN holder name	IdPJava
Domain	
Cookie path	/
Encode Cookie	false
Logout Service	http://localhost:8080/IdpSample?cmd=slo
Authentication Service	http://localhost:8080/IdpSample?cmd=sso
Cookie max age	300
Delete Cookie	true
Algorithm	AES
Mode	CBC
Key size	128
Iteration count	1000
UserId Attribute Name	userId
Adapter Actions	
Generate properties	Generate properties for the agent side
Extended Adapter Contract	
Attribute	userId
Adapter Attributes	
userId	selected

12. On the Manage Adapter Instances screen, click **Save**.
13. On the Main Menu under My IdP Configuration, click **Default URL**.
14. On the Default URL screen, specify the URL to which the user is directed

for a successful SLO:

`http://<sample_hostname>:<sample_port>/IdpSample`

For more information about this screen, click **Help** or refer to the *Administrator's Manual.*



Enter values that affect the user's experience when executing IdP-initiated Web SSO operations.

Provide the default URL you would like to send the user to when Single Logout (SLO) has succeeded.

http://localhost:8080/IdpSample

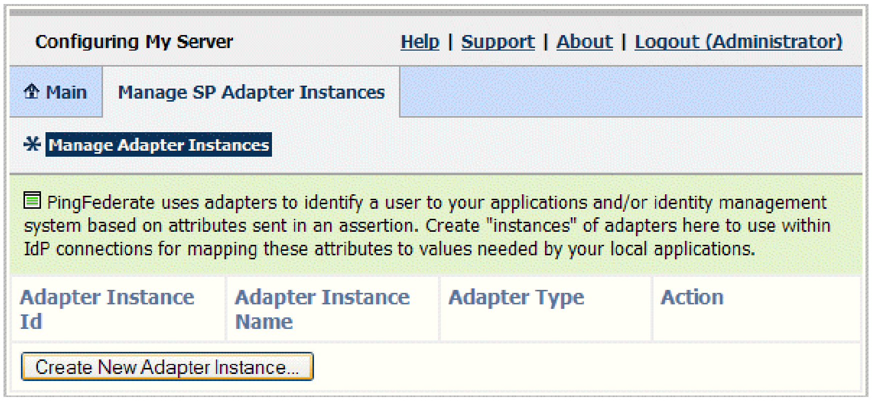
Provide the error text displayed in a user's browser when an SSO operation fails.

Please contact your system administrator for assistance regarding this error.

15. Click **Save**.

Configure the SP Adapter

1. On the Main Menu under My SP Configuration, click **Adapters**.
2. On the Manage Adapter Instances screen, click the **Create New Adapter Instance** button.

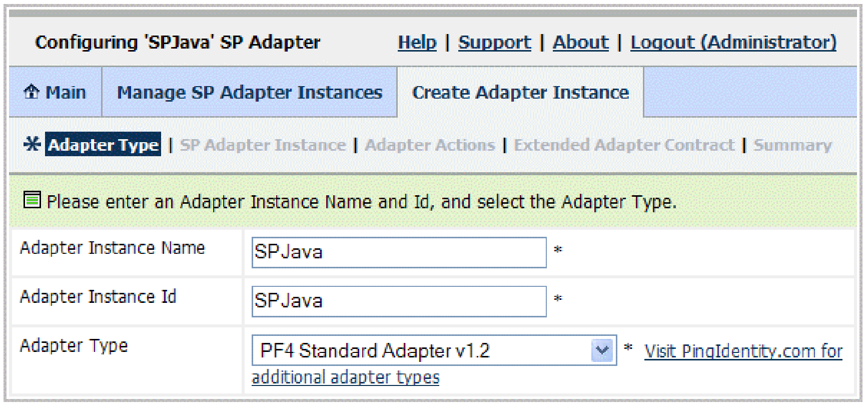

Configuring My Server
Help | Support | About | Logout (Administrator)
Main
Manage SP Adapter Instances
Manage Adapter Instances
Create New Adapter Instance...

PingFederate uses adapters to identify a user to your applications and/or identity management system based on attributes sent in an assertion. Create "instances" of adapters here to use within IdP connections for mapping these attributes to values needed by your local applications.

Adapter Instance Id	Adapter Instance Name	Adapter Type	Action

3. On the Adapter Type screen, enter the following values and select the adapter type from the drop-down menu:

Field	**Value**
Adapter Instance Name	`SPJava`
Adapter Instance ID	`SPJava`
Adapter Type	PF4 Standard Adapter v1.2


Configuring 'SPJava' SP Adapter
Help | Support | About | Logout (Administrator)
Main
Manage SP Adapter Instances
Create Adapter Instance
Adapter Type | SP Adapter Instance | Adapter Actions | Extended Adapter Contract | Summary

Please enter an Adapter Instance Name and Id, and select the Adapter Type.

Adapter Instance Name: SPJava *

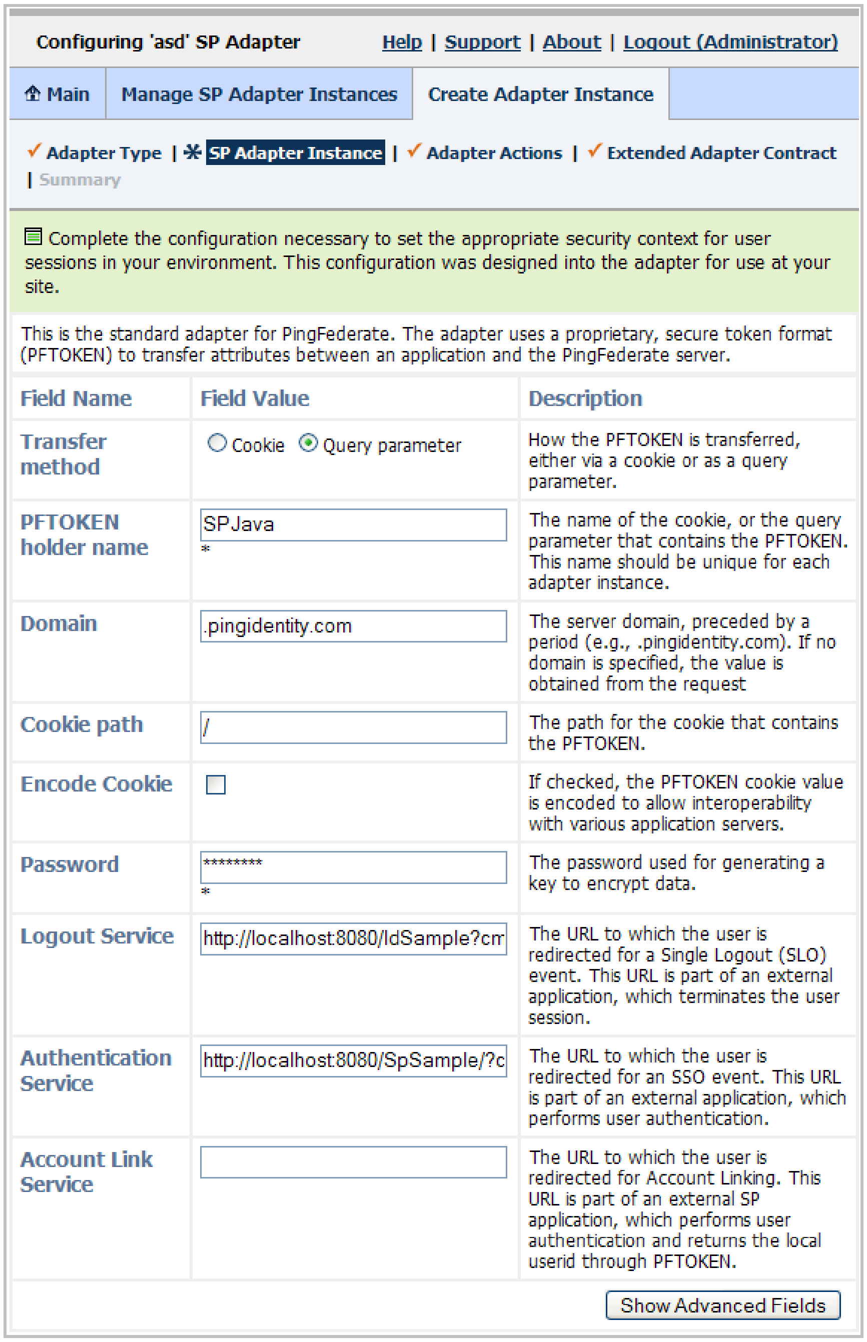
Adapter Instance Id: SPJava *

Adapter Type: PF4 Standard Adapter v1.2 * Visit PingIdentity.com for additional adapter types

4. Click **Next**.

5. On the SP Adapter Instance screen, enter information as shown in the table below (retain default values for items not listed in the table; other fields are not required for the sample application).

Field	**Value**
PFTOKEN holder name	`SPJava`
Password	A password of your choice to be used for generating a key to encrypt data. Remember this password for configuring the sample application.
Logout Service	`http://`*`<sample_hostname>`*`:`*`<sample_port>`*`/SpSample/?cmd=slo`
Authentication Service	`http://`*`<sample_hostname>`*`:`*`<sample_port>`*`/SpSample/?cmd=sso`
Account Link Service	(Optional) `http://`*`<sample_hostname>`*`:`*`<sample_port>`*`/SpSample/?cmd=accountlink`
The variables *`<sample_hostname>`* and *`<sample_port>`* represent the fully qualified domain name and port number of the server running the Java or .NET sample applications. The default port for Tomcat (for the Java application) is 8080.	

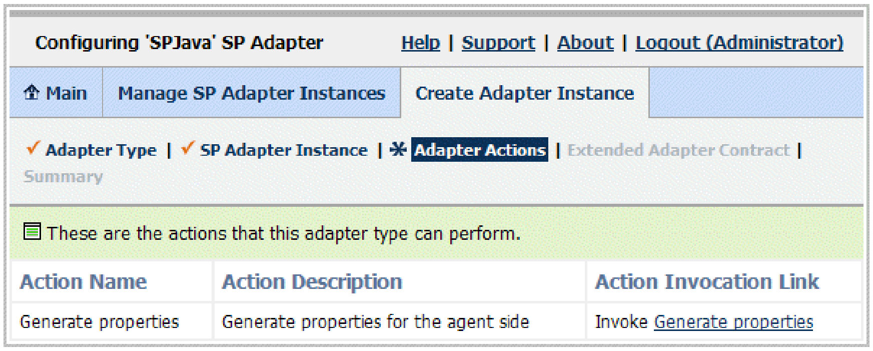

Configuring 'asd' SP Adapter
Help | Support | About | Logout (Administrator)
Main
Manage SP Adapter Instances
Create Adapter Instance
✓ Adapter Type | ✱ SP Adapter Instance | ✓ Adapter Actions | ✓ Extended Adapter Contract | Summary
Show Advanced Fields

Complete the configuration necessary to set the appropriate security context for user sessions in your environment. This configuration was designed into the adapter for use at your site.

This is the standard adapter for PingFederate. The adapter uses a proprietary, secure token format (PFTOKEN) to transfer attributes between an application and the PingFederate server.

Field Name	Field Value	Description
Transfer method	○ Cookie ● Query parameter	How the PFTOKEN is transferred, either via a cookie or as a query parameter.
PFTOKEN holder name	SPJava *	The name of the cookie, or the query parameter that contains the PFTOKEN. This name should be unique for each adapter instance.
Domain	.pingidentity.com	The server domain, preceded by a period (e.g., .pingidentity.com). If no domain is specified, the value is obtained from the request
Cookie path	/	The path for the cookie that contains the PFTOKEN.
Encode Cookie	☐	If checked, the PFTOKEN cookie value is encoded to allow interoperability with various application servers.
Password	******** *	The password used for generating a key to encrypt data.
Logout Service	http://localhost:8080/IdSample?cm	The URL to which the user is redirected for a Single Logout (SLO) event. This URL is part of an external application, which terminates the user session.
Authentication Service	http://localhost:8080/SpSample/?c	The URL to which the user is redirected for an SSO event. This URL is part of an external application, which performs user authentication.
Account Link Service		The URL to which the user is redirected for Account Linking. This URL is part of an external SP application, which performs user authentication and returns the local userid through PFTOKEN.

6. Click **Next**.
7. On the Adapter Actions screen, click **Generate properties**.


Configuring 'SPJava' SP Adapter
Help | Support | About | Logout (Administrator)
Main
Manage SP Adapter Instances
Create Adapter Instance
✓ Adapter Type | ✓ SP Adapter Instance | ✱ Adapter Actions | Extended Adapter Contract | Summary

These are the actions that this adapter type can perform.

Action Name	Action Description	Action Invocation Link
Generate properties	Generate properties for the agent side	Invoke Generate properties

On the next screen, click **Export** and save the properties file to your file system.

The values in the resulting file `pfagent.properties` are established by the console configuration and are used by the IdP sample application.

8. Copy the `pfagent.properties` file to one of the following locations and change the filename as shown:

   For Java:

   ```
   <pf_install_dir>\quickstart\sample_app\java\SpSample\
      config\pfagent-sp.properties
   ```

   For .NET:

   ```
   <pf_install_dir>\quickstart\sample_app\dotnet\
      SpSample\config\pfagent-sp.config
   ```

   Important: Be sure to save the file as plain text using the exact filenames shown above.

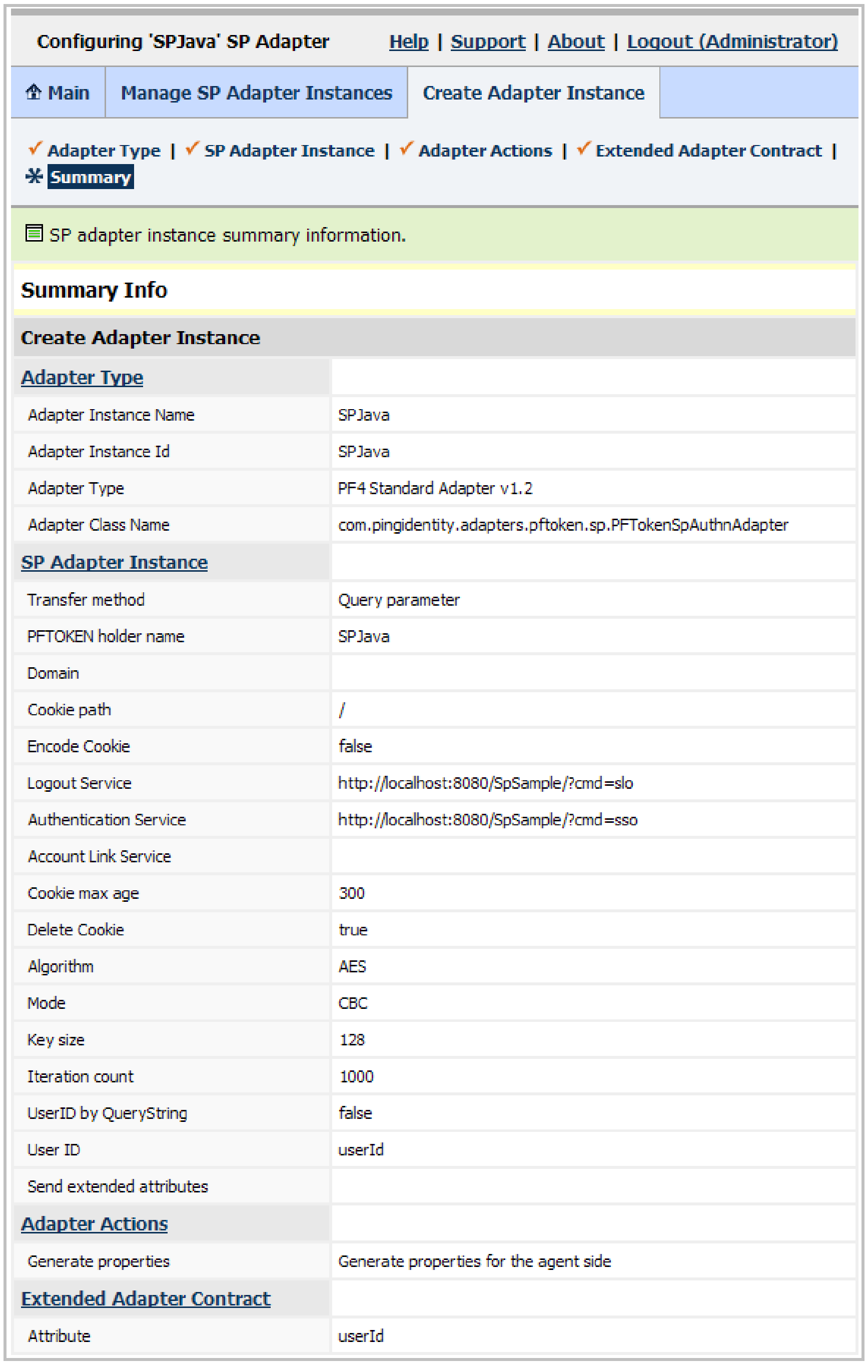
9. Click **Next**.

10. On the Extended Adapter Contract screen, you can configure additional attributes for the adapter. These attributes, however, are not necessary to run the sample applications.

    This screen is typically used to adjust your adapter contract attribute values after an adapter has already been deployed. (See the "Key Concepts" chapter in the *Administrator's Manual.)*

    Click **Next**.

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



Configuring 'SPJava' SP Adapter
Help | Support | About | Logout (Administrator)
Main
Manage SP Adapter Instances
Create Adapter Instance
✓ Adapter Type | ✓ SP Adapter Instance | ✓ Adapter Actions | ✓ Extended Adapter Contract |
Summary

SP adapter instance summary information.

Summary Info

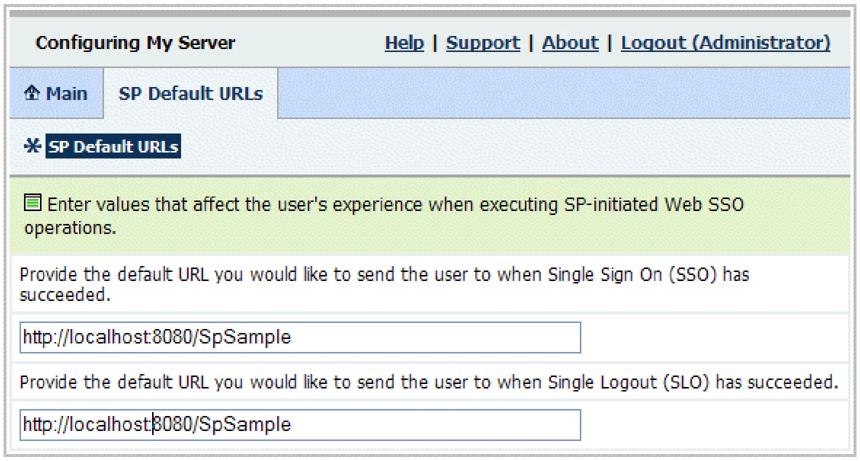
Create Adapter Instance

Adapter Type	
Adapter Instance Name	SPJava
Adapter Instance Id	SPJava
Adapter Type	PF4 Standard Adapter v1.2
Adapter Class Name	com.pingidentity.adapters.pftoken.sp.PFTokenSpAuthnAdapter
SP Adapter Instance	
Transfer method	Query parameter
PFTOKEN holder name	SPJava
Domain	
Cookie path	/
Encode Cookie	false
Logout Service	http://localhost:8080/SpSample/?cmd=slo
Authentication Service	http://localhost:8080/SpSample/?cmd=sso
Account Link Service	
Cookie max age	300
Delete Cookie	true
Algorithm	AES
Mode	CBC
Key size	128
Iteration count	1000
UserID by QueryString	false
User ID	userId
Send extended attributes	
Adapter Actions	
Generate properties	Generate properties for the agent side
Extended Adapter Contract	
Attribute	userId

12. On the Manage Adapter Instances screen, click **Save** to complete the adapter configuration.

13. On the Main Menu under My SP Configuration, click **Default URLs**.

14. On the SP Default URLs screen, configure URLs to which the user is directed for a successful SSO and SLO, and click **Save**.



Enter values that affect the user's experience when executing SP-initiated Web SSO operations.

Provide the default URL you would like to send the user to when Single Sign On (SSO) has succeeded.

http://localhost:8080/SpSample

Provide the default URL you would like to send the user to when Single Logout (SLO) has succeeded.

http://localhost:8080/SpSample

Field	Value

`SSO Success`	`http://`
	`<sample_hostname>:<sample_port>`
	`/SpSample/`

`SLO Success`	`http://`
	`<sample_hostname>:<sample_port>`
	`/SpSample/`

Chapter 3

Connection Scenarios

Overview

The SAML 2.0 standard focuses on four main federation use cases for Single Sign-on (SSO) and Single Logout (SLO).

The use cases are covered in the following sections:

- "IdP-Initiated SSO" on page 28
- "SP-Initiated SSO" on page 50
- "IdP-Initiated SLO" on page 45
- "SP-Initiated SLO" on page 52

Depending upon your specific environment, one or more of these profiles will be relevant to your organization's needs. Follow these instructions to configure PingFederate and the sample applications to support one or more of these profiles.

Note: To learn the basic elements of PingFederate, configure IdP-initiated SSO at a minimum. This profile is enough to run the sample applications. If you wish to skip manual configuration of these use cases, see "Automating the Configuration" on page 65.

For detailed information about SAML profile scenarios, see the *Administrator's Manual.*

IdP-Initiated SSO

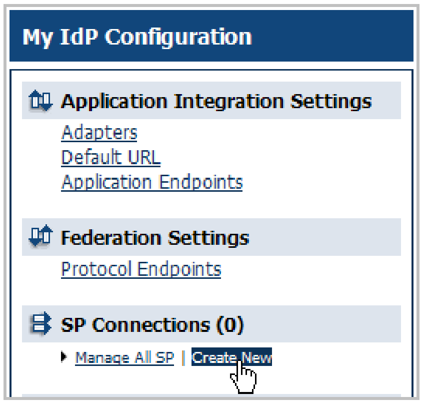
This section provides instructions for configuring both an IdP and an SP connection for IdP-initiated SSO.

Important: Follow the sections below in the order presented.

Configure the SP Connection

In this scenario, you are an IdP configuring a connection to an SP for IdP-initiated SSO using the POST binding.

1. On the Main Menu screen under My IdP Configuration, click **Create New** under SP Connections.



2. On the Role & Protocol screen, verify that the Connection Type is SP and that the Protocol is SAML v2.0. Click **Next.**
3. On the Import Metadata screen, click **Next**.

Note: This screen allows you to specify a metadata file from your connection partner, which would provide many of the parameters necessary to set up a real connection with that partner. For further information, see the *Administrator's Manual*.

4. On the General Info screen, enter the following values and click **Next**:

   Partner's Entity ID: `localhost:default:entityId`

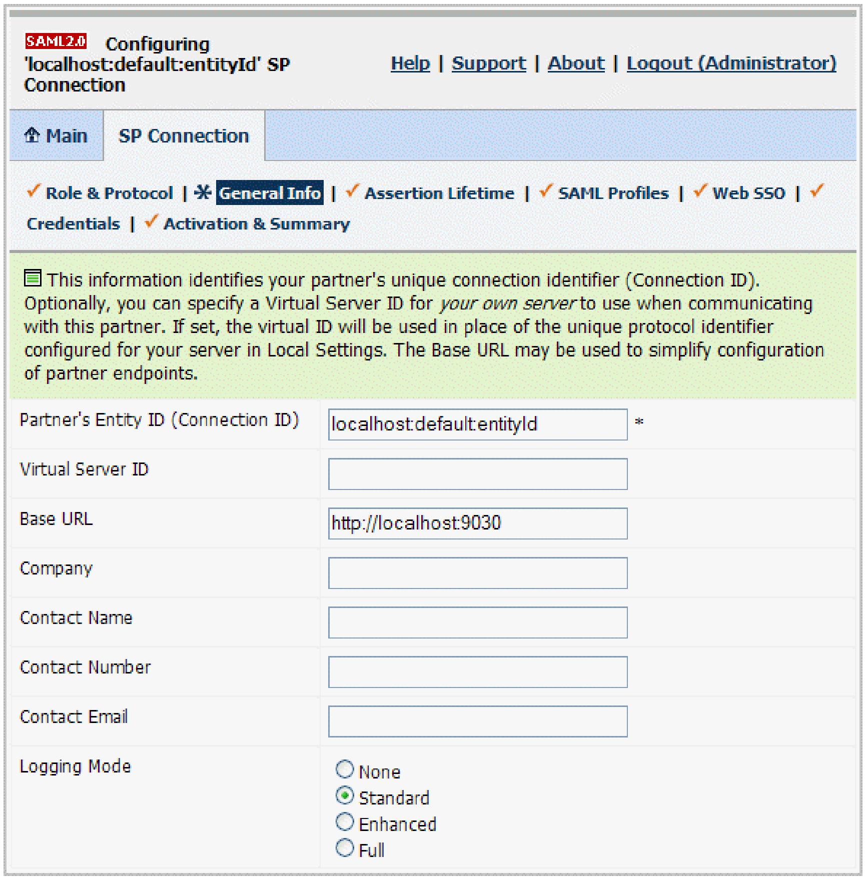
   The Connection ID is the same as the SAML 2.0 Entity ID entered on the Federation Info screen in when you configured Server Settings, since both ends of the connection are on the same server. In a configuration between you and a partner, you would enter the Connection ID provided to you by your partner.

Also enter:

Base URL: `http://<pf_host>:9030`

where *`<pf_host>`* is the fully qualified domain name of your PingFederate server instance.

Providing a Base URL allows you to more easily enter endpoints in the configuration of the connection, using only relative paths rather than repeatedly entering the same Base URL for each endpoint.

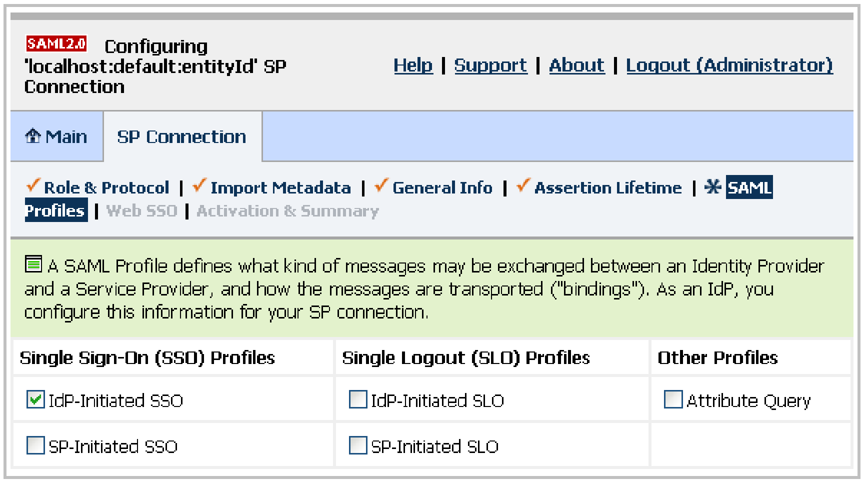

SAML2.0
Configuring 'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
✓ Role & Protocol | General Info | ✓ Assertion Lifetime | ✓ SAML Profiles | ✓ Web SSO | ✓ Credentials | ✓ Activation & Summary

This information identifies your partner's unique connection identifier (Connection ID). Optionally, you can specify a Virtual Server ID for *your own server* to use when communicating with this partner. If set, the virtual ID will be used in place of the unique protocol identifier configured for your server in Local Settings. The Base URL may be used to simplify configuration of partner endpoints.

Partner's Entity ID (Connection ID)	localhost:default:entityId *
Virtual Server ID	
Base URL	http://localhost:9030
Company	
Contact Name	
Contact Number	
Contact Email	
Logging Mode	○ None ● Standard ○ Enhanced ○ Full

5. On the Assertion Lifetime screen, click **Next**. This screen allows you to specify the period for which an assertion is valid.

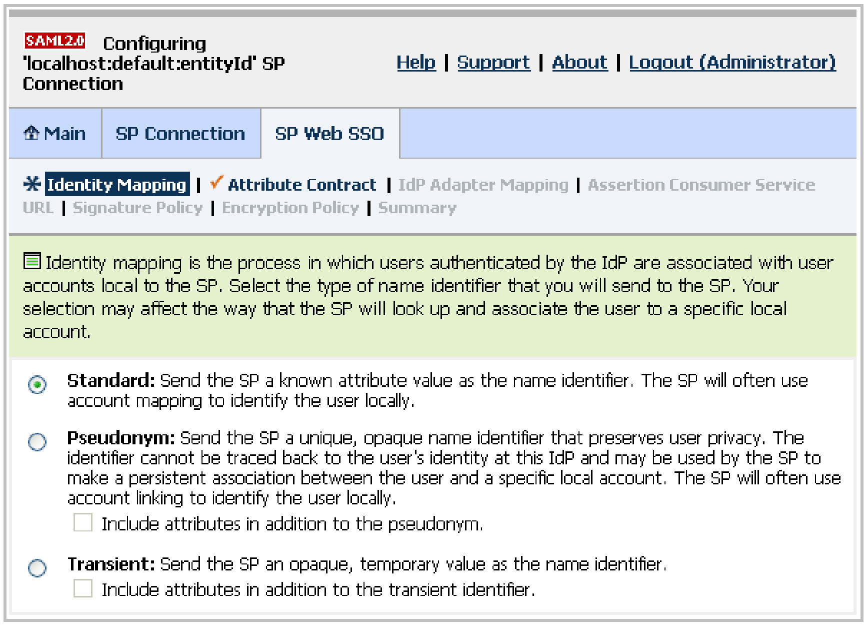
6. On the SAML Profiles screen, check the **IdP-Initiated SSO** checkbox and click **Next**.


SAML2.0
Configuring 'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
✓ Role & Protocol | ✓ Import Metadata | ✓ General Info | ✓ Assertion Lifetime | ✱ SAML Profiles | Web SSO | Activation & Summary

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider, and how the messages are transported ("bindings"). As an IdP, you configure this information for your SP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles	Other Profiles
☑ IdP-Initiated SSO	☐ IdP-Initiated SLO	☐ Attribute Query
☐ SP-Initiated SSO	☐ SP-Initiated SLO	

7. On the Web SSO screen, click the **Configure Web SSO** button.
8. On the Identity Mapping screen, verify that the **Standard** button is selected and click **Next**.


SAML2.0
Configuring 'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
SP Web SSO
✱ Identity Mapping | ✓ Attribute Contract | IdP Adapter Mapping | Assertion Consumer Service URL | Signature Policy | Encryption Policy | Summary

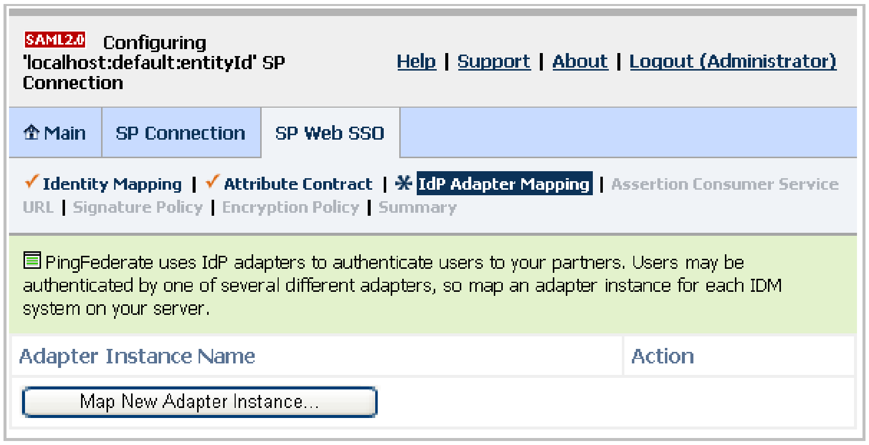
Identity mapping is the process in which users authenticated by the IdP are associated with user accounts local to the SP. Select the type of name identifier that you will send to the SP. Your selection may affect the way that the SP will look up and associate the user to a specific local account.

● **Standard:** Send the SP a known attribute value as the name identifier. The SP will often use account mapping to identify the user locally.

○ **Pseudonym:** Send the SP a unique, opaque name identifier that preserves user privacy. The identifier cannot be traced back to the user's identity at this IdP and may be used by the SP to make a persistent association between the user and a specific local account. The SP will often use account linking to identify the user locally.
☐ Include attributes in addition to the pseudonym.

○ **Transient:** Send the SP an opaque, temporary value as the name identifier.
☐ Include attributes in addition to the transient identifier.

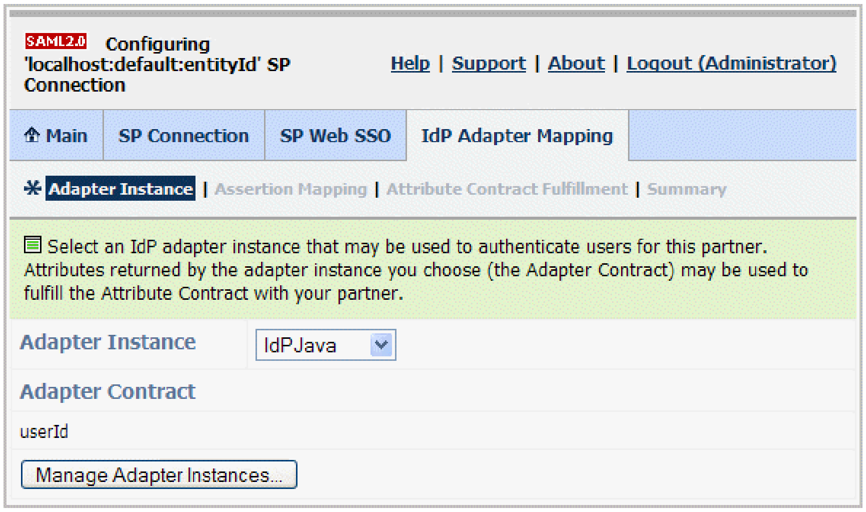
9. On the Attribute Contract screen, verify that the contract contains only SAML_SUBJECT and click **Next**.
10. On the IdP Adapter Mapping screen, click the **Map New Adapter Instance** button.


SAML2.0
Help | Support | About | Logout (Administrator)
Main
SP Connection
SP Web SSO
✓ Identity Mapping | ✓ Attribute Contract | ✱ IdP Adapter Mapping | Assertion Consumer Service URL | Signature Policy | Encryption Policy | Summary
Adapter Instance Name
Action
Map New Adapter Instance...

Configuring 'localhost:default:entityId' SP Connection

PingFederate uses IdP adapters to authenticate users to your partners. Users may be authenticated by one of several different adapters, so map an adapter instance for each IDM system on your server.

11. On the Adapter Instance screen, select (from the drop-down menu) the IdP adapter instance you created earlier. (For this exercise, you created IdPJava—see Step 3 on page 14.) Click **Next**.


SAML2.0
Help | Support | About | Logout (Administrator)
Main
SP Connection
SP Web SSO
IdP Adapter Mapping
✱ Adapter Instance | Assertion Mapping | Attribute Contract Fulfillment | Summary
Manage Adapter Instances...

Configuring 'localhost:default:entityId' SP Connection

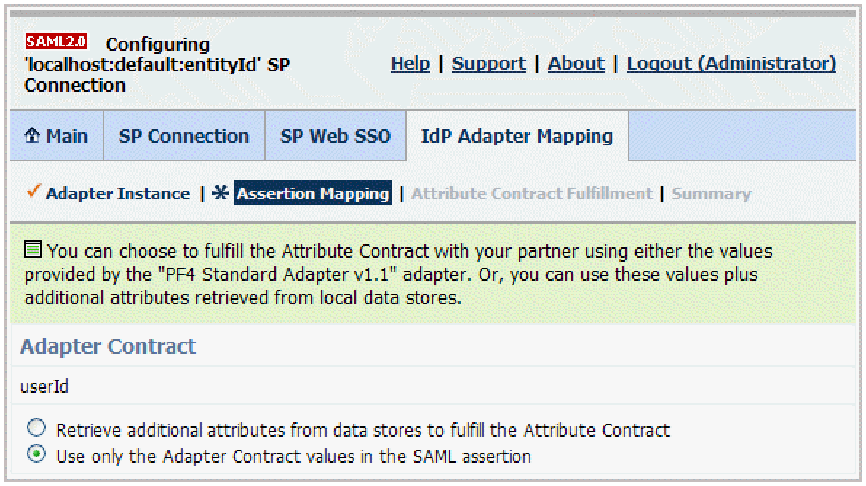
Select an IdP adapter instance that may be used to authenticate users for this partner. Attributes returned by the adapter instance you choose (the Adapter Contract) may be used to fulfill the Attribute Contract with your partner.

Adapter Instance: IdPJava

Adapter Contract

userId

12. On the Assertion Mapping screen, select the Use only the Adapter Contract values in the SAML assertion button. Click **Next**.



SAML2.0 Configuring 'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
SP Web SSO
IdP Adapter Mapping
✓ Adapter Instance | Assertion Mapping | Attribute Contract Fulfillment | Summary

You can choose to fulfill the Attribute Contract with your partner using either the values provided by the "PF4 Standard Adapter v1.1" adapter. Or, you can use these values plus additional attributes retrieved from local data stores.

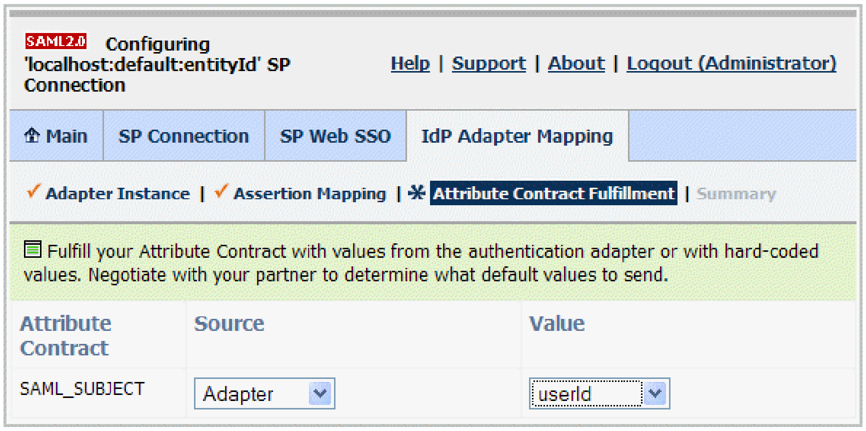
Adapter Contract

userId

○ Retrieve additional attributes from data stores to fulfill the Attribute Contract
● Use only the Adapter Contract values in the SAML assertion

13. On the Attribute Contract Fulfillment screen, select **Adapter** from the Source drop-down menu and **userId** from the Value drop-down menu. Click **Next.**

    The Attribute Contract column lists the attributes required to meet the attribute contract with your connection partner.

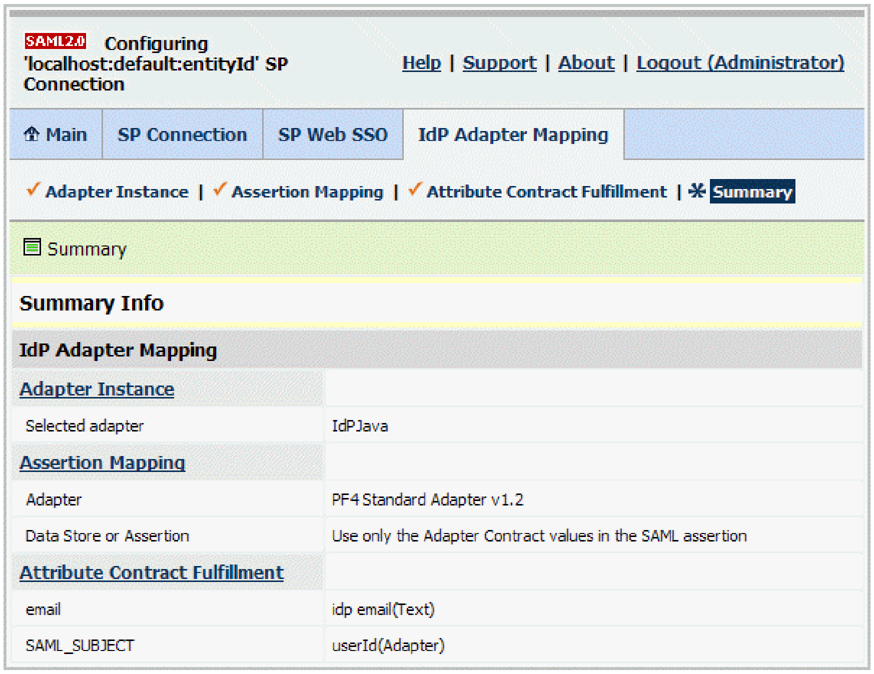


SAML2.0 Configuring 'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
SP Web SSO
IdP Adapter Mapping
✓ Adapter Instance | ✓ Assertion Mapping | Attribute Contract Fulfillment | Summary

Fulfill your Attribute Contract with values from the authentication adapter or with hard-coded values. Negotiate with your partner to determine what default values to send.

Attribute Contract	Source	Value
SAML_SUBJECT	Adapter	userId

14. On the Summary screen, verify that the information is entered correctly and click **Done**.


SAML2.0
Configuring 'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
SP Web SSO
IdP Adapter Mapping
✓ Adapter Instance | ✓ Assertion Mapping | ✓ Attribute Contract Fulfillment | Summary
Summary

Summary Info

IdP Adapter Mapping

Adapter Instance	
Selected adapter	IdPJava
Assertion Mapping	
Adapter	PF4 Standard Adapter v1.2
Data Store or Assertion	Use only the Adapter Contract values in the SAML assertion
Attribute Contract Fulfillment	
email	idp email(Text)
SAML_SUBJECT	userId(Adapter)

Tip: If you want to pause at any time during connection configuration, click the **Save Draft** button. To restart the configuration, click the **Manage All SP** link on the Main Menu and then, at the Select a Connection screen, click the **localhost:default:entityId** connection. You will return to where you left off.

15. On the IdP Adapter Mapping screen, verify that the Adapter Instance Name is IdPJava, and then click **Next**.

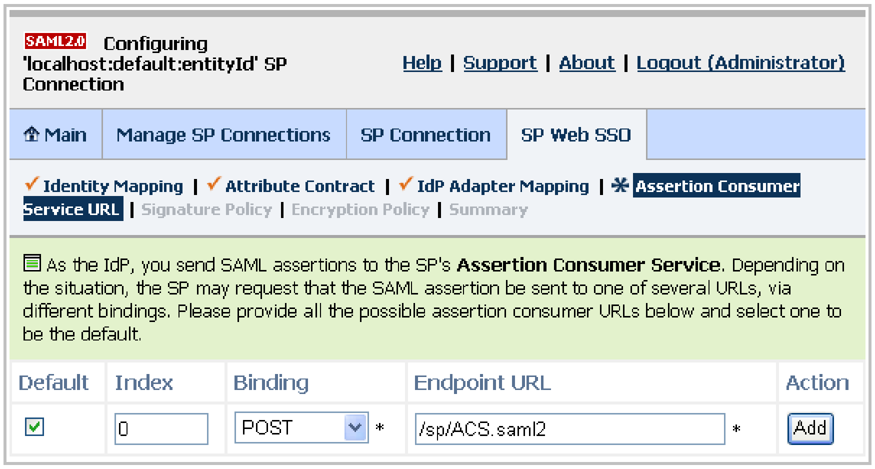
16. On the Assertion Consumer Service URL screen, enter or select the following values and click the **Add** button. Then click **Next**.

    - Default: checked
    - Index: `0`

    Note: This is set automatically.

    - Binding: `POST`
    - Endpoint URL: `/sp/ACS.saml2`

    Note that the '`l`' in '`saml2`' is the lower-case letter 'L'.

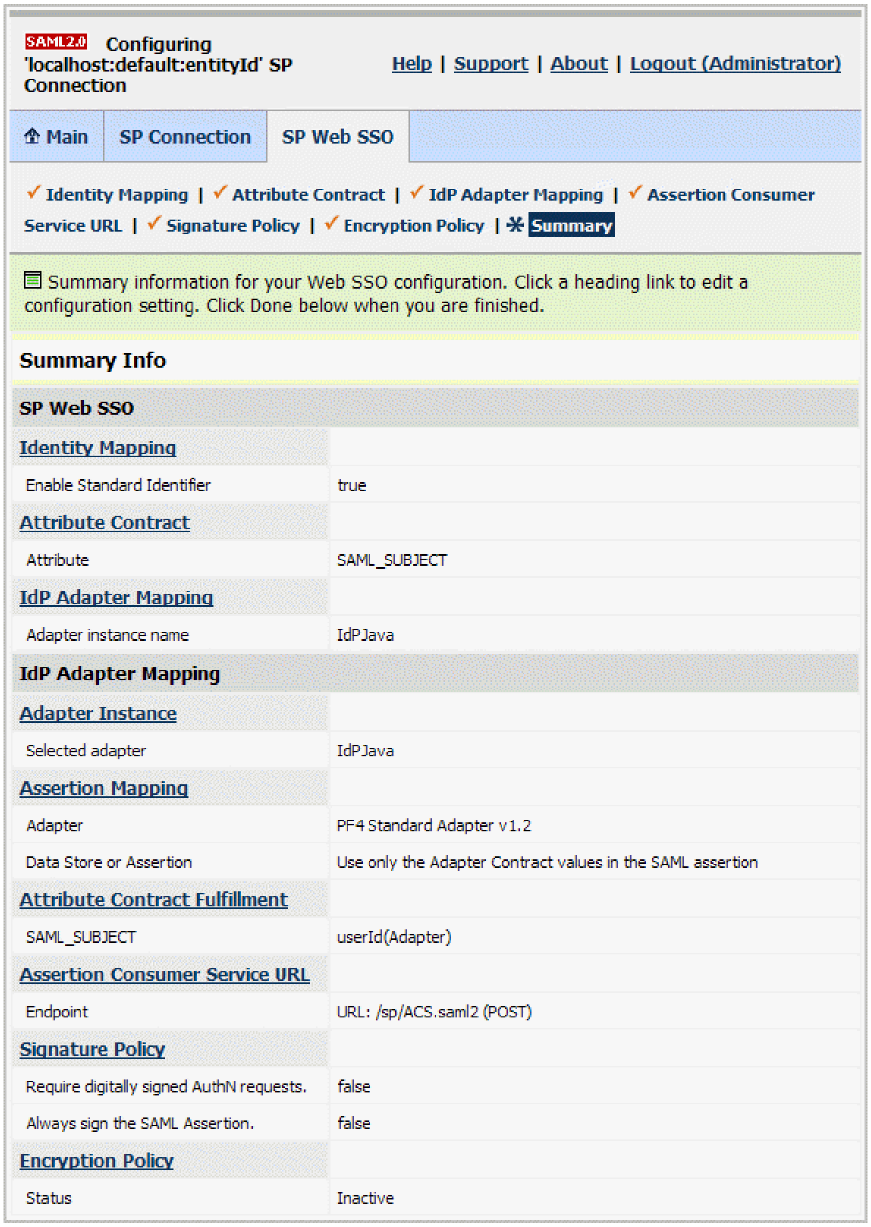


SAML2.0 Configuring 'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
Manage SP Connections
SP Connection
SP Web SSO
✓ Identity Mapping | ✓ Attribute Contract | ✓ IdP Adapter Mapping | Assertion Consumer Service URL | Signature Policy | Encryption Policy | Summary

As the IdP, you send SAML assertions to the SP's **Assertion Consumer Service**. Depending on the situation, the SP may request that the SAML assertion be sent to one of several URLs, via different bindings. Please provide all the possible assertion consumer URLs below and select one to be the default.

Default	Index	Binding	Endpoint URL	Action
☑	0	POST *	/sp/ACS.saml2 *	Add

17. On the Signature Policy screen, click **Next**.
18. On the Encryption Policy screen, click **Next**.
19. On the Summary screen, verify that the information is entered correctly and click **Done**.


SAML2.0
Help | Support | About | Logout (Administrator)
Main
SP Connection
SP Web SSO
✓ Identity Mapping | ✓ Attribute Contract | ✓ IdP Adapter Mapping | ✓ Assertion Consumer Service URL | ✓ Signature Policy | ✓ Encryption Policy | Summary

Configuring 'localhost:default:entityId' SP Connection

Summary information for your Web SSO configuration. Click a heading link to edit a configuration setting. Click Done below when you are finished.

Summary Info

SP Web SSO	
Identity Mapping	
Enable Standard Identifier	true
Attribute Contract	
Attribute	SAML_SUBJECT
IdP Adapter Mapping	
Adapter instance name	IdPJava
IdP Adapter Mapping	
Adapter Instance	
Selected adapter	IdPJava
Assertion Mapping	
Adapter	PF4 Standard Adapter v1.2
Data Store or Assertion	Use only the Adapter Contract values in the SAML assertion
Attribute Contract Fulfillment	
SAML_SUBJECT	userId(Adapter)
Assertion Consumer Service URL	
Endpoint	URL: /sp/ACS.saml2 (POST)
Signature Policy	
Require digitally signed AuthN requests.	false
Always sign the SAML Assertion.	false
Encryption Policy	
Status	Inactive

20. On the Web SSO screen, click **Next**.

21. On the Credentials screen, click **Configure Credentials** button.

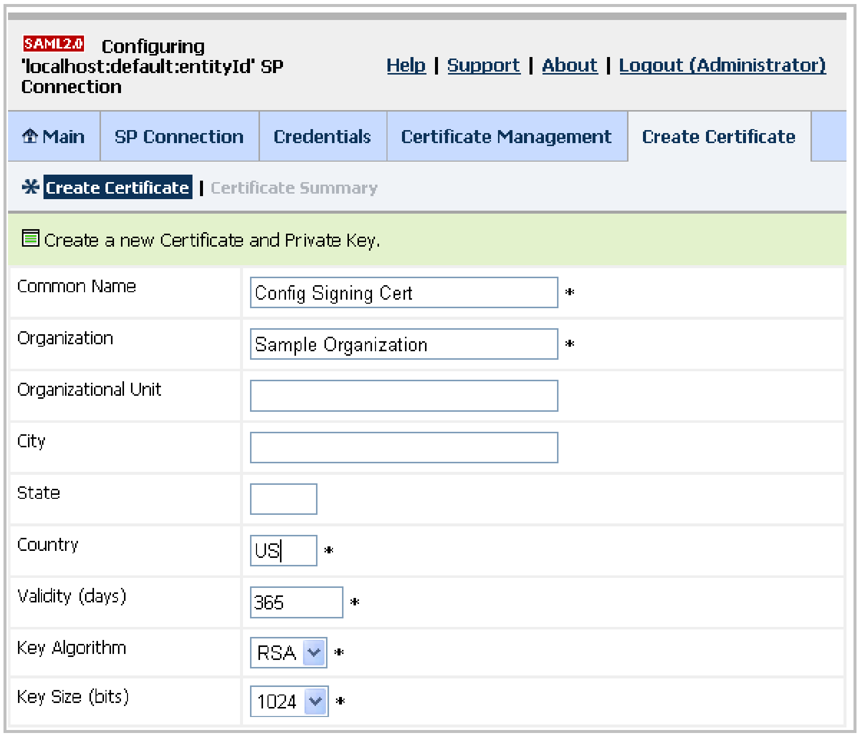
22. On the Digital Signature Settings screen, click the **Manage Certificates** button.

23. On the Manage Digital Signing Certificates screen, click **Create New**.

24. On the Create Certificate screen, enter or select the following values and then click **Next**:

    - Common Name: `Config Signing Cert`
    - Organization: `Sample Organization`
    - Country: `US`

- Validity (days): `365`
- Key Algorithm: `RSA`
- Key Size (bits): `1024`

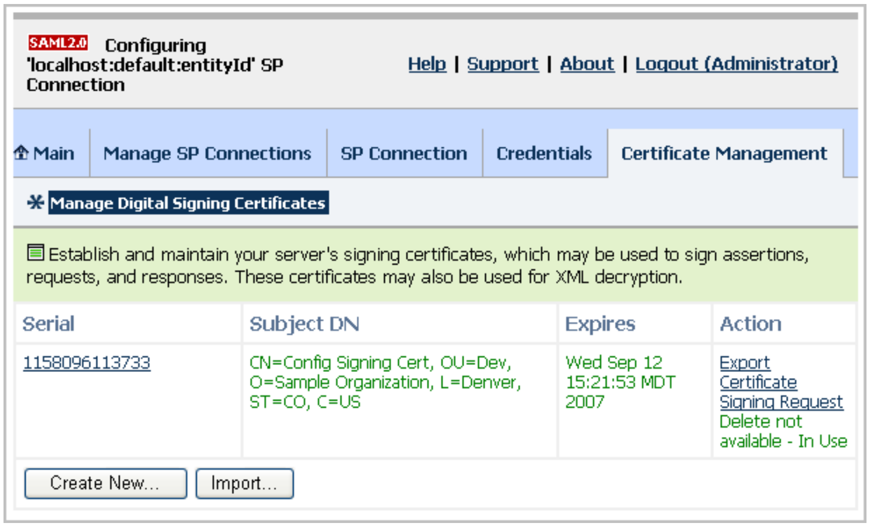

SAML2.0
Configuring 'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
Credentials
Certificate Management
Create Certificate
Create Certificate | Certificate Summary

Create a new Certificate and Private Key.

Common Name	Config Signing Cert *
Organization	Sample Organization *
Organizational Unit	
City	
State	
Country	US *
Validity (days)	365 *
Key Algorithm	RSA *
Key Size (bits)	1024 *

25. On the Certificate Summary screen, click **Done**.

26. On the Manage Digital Signing Certificates screen, click the **Export** link in the column to the right of the certificate you created.

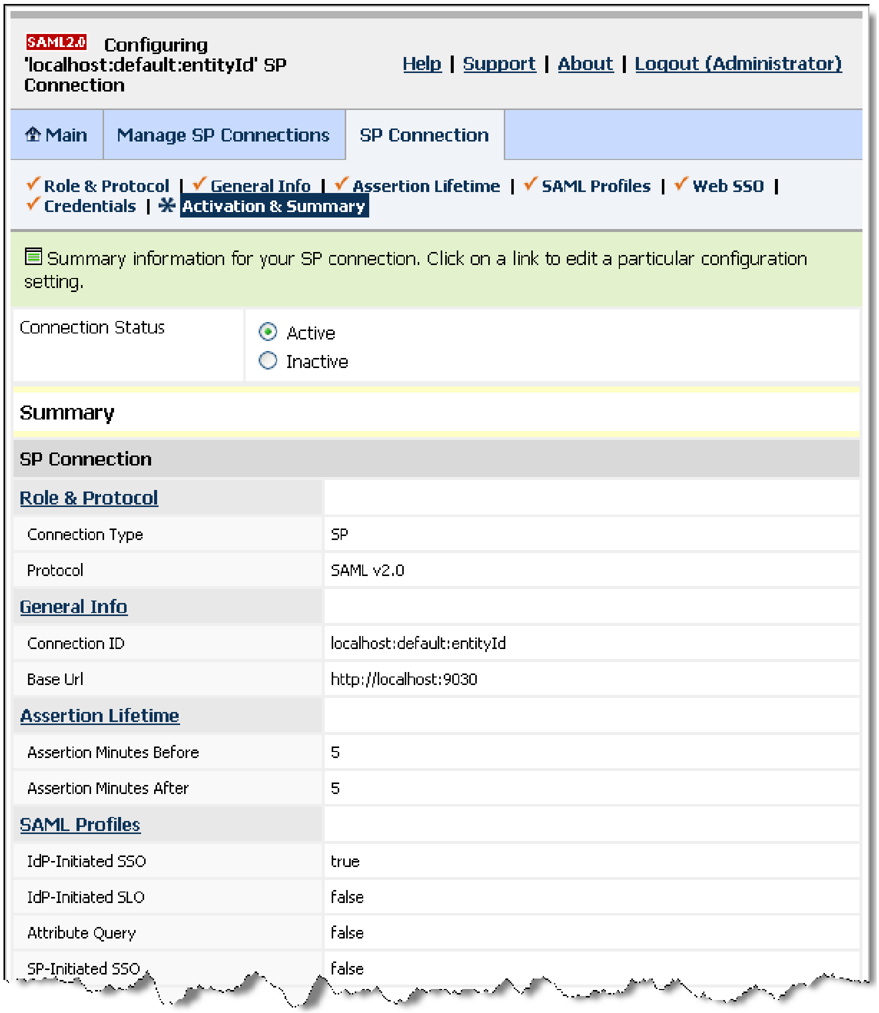

SAML2.0
Configuring 'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
Manage SP Connections
SP Connection
Credentials
Certificate Management
Manage Digital Signing Certificates

Establish and maintain your server's signing certificates, which may be used to sign assertions, requests, and responses. These certificates may also be used for XML decryption.

Serial	Subject DN	Expires	Action
1158096113733	CN=Config Signing Cert, OU=Dev, O=Sample Organization, L=Denver, ST=CO, C=US	Wed Sep 12 15:21:53 MDT 2007	Export Certificate Signing Request Delete not available - In Use

Note: Export and **Certificate Signing Request** are two different links. Make sure to click the **Export** link.

27. On the Export Certification screen, select **Certificate Only** and then click **Next**.
28. On the Certificate Summary screen, click **Export** to export the certificate and save it to any folder (The file has a ".crt" extension. Save it to a folder that you can access later in this process.)
29. Click **Done**.
30. On the Manage Digital Signing Certificates screen, click **Save**.
31. On the Digital Signature Settings screen, click **Next**.
32. On the Summary screen, click **Done**.
33. On the Credentials screen, click **Next**.
34. On the Activation & Summary screen, select **Active** for Connection Status.


SAML2.0
Help | Support | About | Logout (Administrator)
Main
Manage SP Connections
SP Connection
✓ Role & Protocol | ✓ General Info | ✓ Assertion Lifetime | ✓ SAML Profiles | ✓ Web SSO |
✓ Credentials | Activation & Summary

Configuring 'localhost:default:entityId' SP Connection

Summary information for your SP connection. Click on a link to edit a particular configuration setting.

Connection Status ● Active ○ Inactive

Summary

SP Connection	
Role & Protocol	
Connection Type	SP
Protocol	SAML v2.0
General Info	
Connection ID	localhost:default:entityId
Base Url	http://localhost:9030
Assertion Lifetime	
Assertion Minutes Before	5
Assertion Minutes After	5
SAML Profiles	
IdP-Initiated SSO	true
IdP-Initiated SLO	false
Attribute Query	false
SP-Initiated SSO	false

35. Click **Save.**

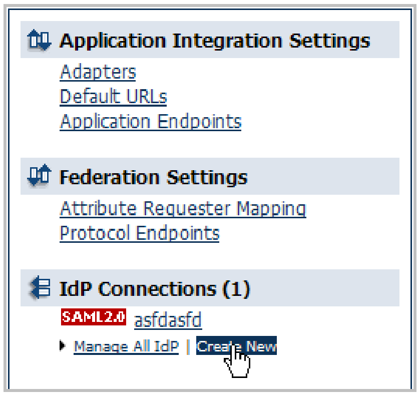
You have now configured the SP connection for IdP-initiated SSO. The next step is to configure the IdP connection.

Configure the IdP Connection

In this scenario, you are an SP configuring a connection to an IdP for IdP-initiated SSO using the POST binding.

To configure the IdP connection:

1. On the Main Menu screen under My SP Configuration, click **Create New** under IdP Connections.

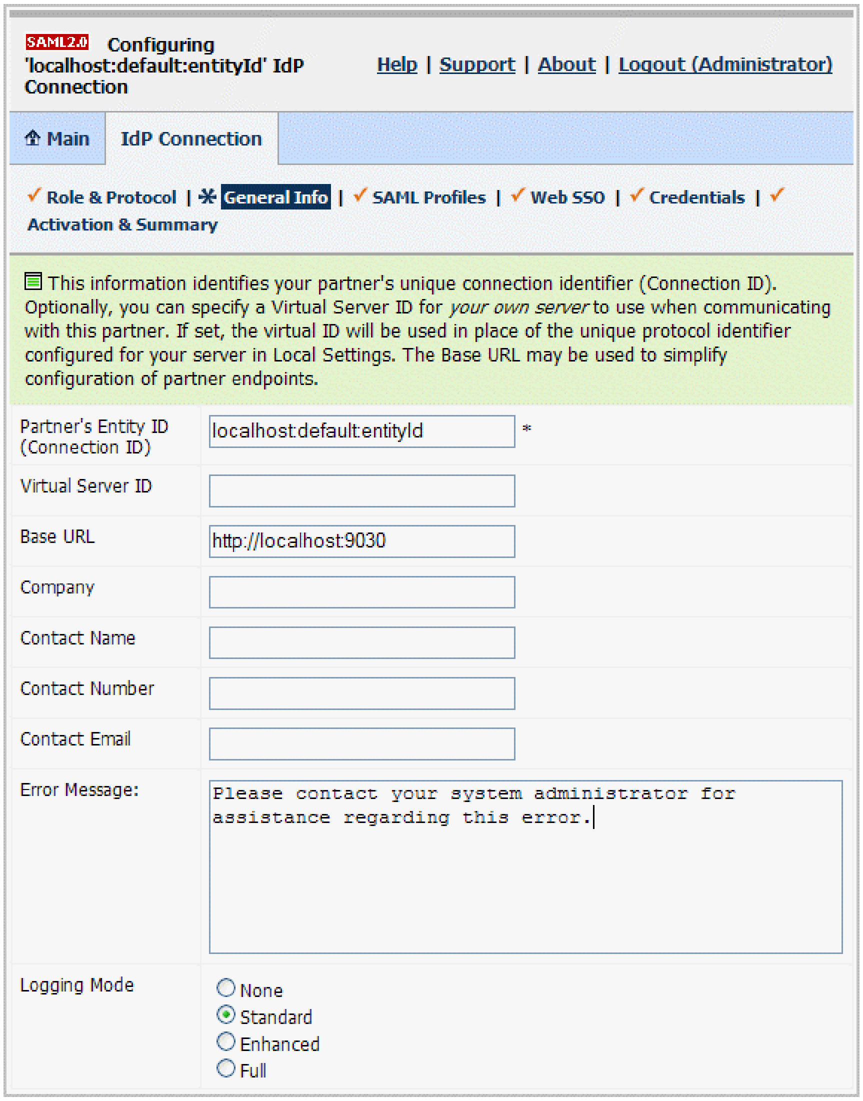


2. On the Role & Protocol screen, verify that the Connection Type is IdP and that the Protocol is SAML v2.0. Click **Next**.
3. On the Import Metadata screen, click **Next**.
4. On the General Info screen, enter the following values at a minimum and click **Next**:

   Partner's ID: `localhost:default:entityId`

   Base URL: `http://`*`<pf_host>`*`:9030`

   where *<pf_host>* is the fully qualified domain name of your PingFederate server instance.

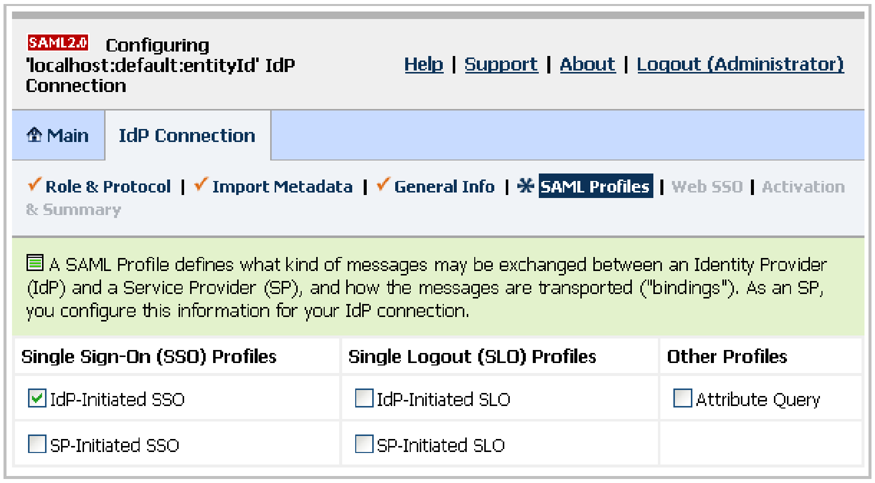

SAML2.0
Configuring 'localhost:default:entityId' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connection
✓ Role & Protocol | General Info | ✓ SAML Profiles | ✓ Web SSO | ✓ Credentials | ✓ Activation & Summary

This information identifies your partner's unique connection identifier (Connection ID). Optionally, you can specify a Virtual Server ID for *your own server* to use when communicating with this partner. If set, the virtual ID will be used in place of the unique protocol identifier configured for your server in Local Settings. The Base URL may be used to simplify configuration of partner endpoints.

Partner's Entity ID (Connection ID)	localhost:default:entityId *
Virtual Server ID	
Base URL	http://localhost:9030
Company	
Contact Name	
Contact Number	
Contact Email	
Error Message:	Please contact your system administrator for assistance regarding this error.
Logging Mode	○ None ● Standard ○ Enhanced ○ Full

For information about the Error Message and Logging Mode fields, refer to the online **Help** page.

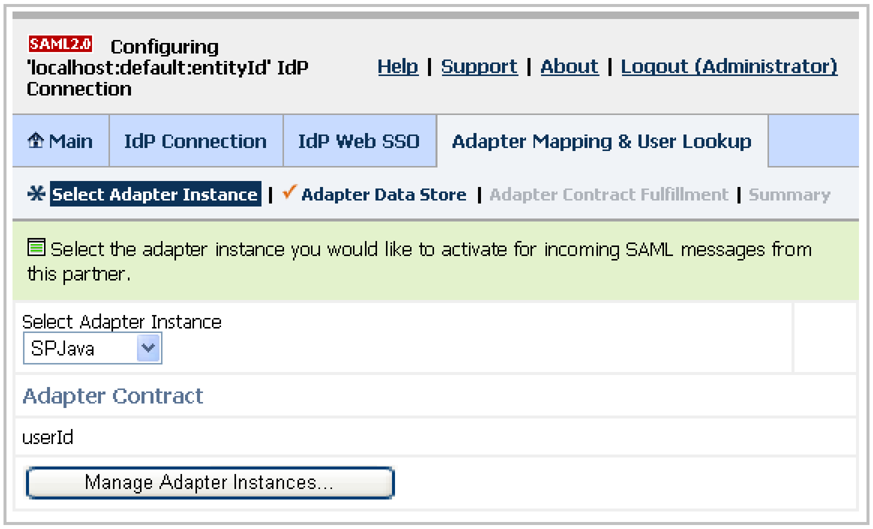
5. On the SAML Profiles screen, check the **IdP-initiated SSO** checkbox. Click **Next**.


SAML2.0
Configuring 'localhost:default:entityId' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connection
Role & Protocol | Import Metadata | General Info | SAML Profiles | Web SSO | Activation & Summary

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider (IdP) and a Service Provider (SP), and how the messages are transported ("bindings"). As an SP, you configure this information for your IdP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles	Other Profiles
☑ IdP-Initiated SSO	☐ IdP-Initiated SLO	☐ Attribute Query
☐ SP-Initiated SSO	☐ SP-Initiated SLO	

6. On the Web SSO screen, click **Configure Web SSO** button.
7. On the Identity Mapping screen, ensure that **Account Mapping** is selected and then click **Next**.
8. On the Attribute Contract screen, ensure that the Attribute Contract is SAML_SUBJECT and then click **Next**.
9. On the Adapter Mapping & User Look-up screen, click the **Map New Adapter Instance** button.
10. On the Adapter Instance screen, select SPJava in the Adapter Instance drop-down. The associated adapter contract appears on the screen. Click **Next**.


SAML2.0
Configuring 'localhost:default:entityId' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connection
IdP Web SSO
Adapter Mapping & User Lookup
Select Adapter Instance | Adapter Data Store | Adapter Contract Fulfillment | Summary
Manage Adapter Instances...

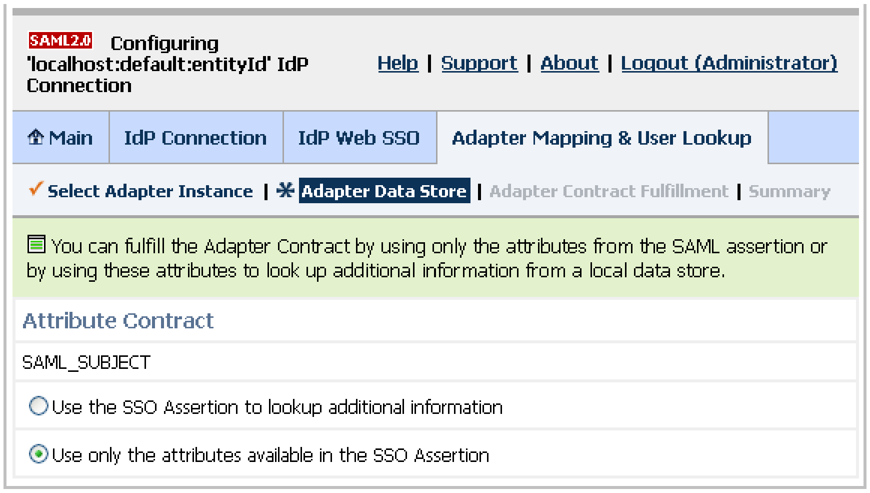
Select the adapter instance you would like to activate for incoming SAML messages from this partner.

Select Adapter Instance: SPJava

Adapter Contract

userId

11. On the Adapter Data Store screen, select the Use only the attributes available in the SSO Assertion button. Click **Next**.


SAML2.0
Configuring 'localhost:default:entityId' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connection
IdP Web SSO
Adapter Mapping & User Lookup
✓ Select Adapter Instance | ✱ Adapter Data Store | Adapter Contract Fulfillment | Summary

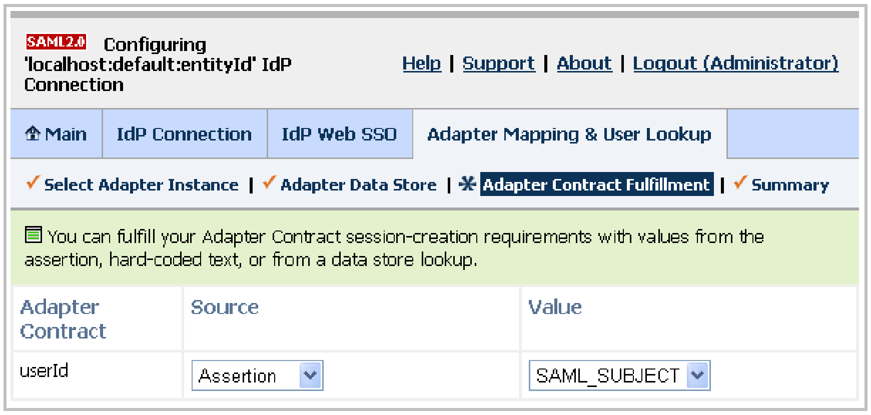
You can fulfill the Adapter Contract by using only the attributes from the SAML assertion or by using these attributes to look up additional information from a local data store.

Attribute Contract
SAML_SUBJECT

○ Use the SSO Assertion to lookup additional information

● Use only the attributes available in the SSO Assertion

12. On the Adapter Contract Fulfillment screen, select **Assertion** in the Source drop-down and **SAML_SUBJECT** in the Value drop-down. Click **Next**.


SAML2.0
Configuring 'localhost:default:entityId' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connection
IdP Web SSO
Adapter Mapping & User Lookup
✓ Select Adapter Instance | ✓ Adapter Data Store | ✱ Adapter Contract Fulfillment | ✓ Summary

You can fulfill your Adapter Contract session-creation requirements with values from the assertion, hard-coded text, or from a data store lookup.

Adapter Contract	Source	Value
userId	Assertion	SAML_SUBJECT

13. On the Summary screen, click **Done**.

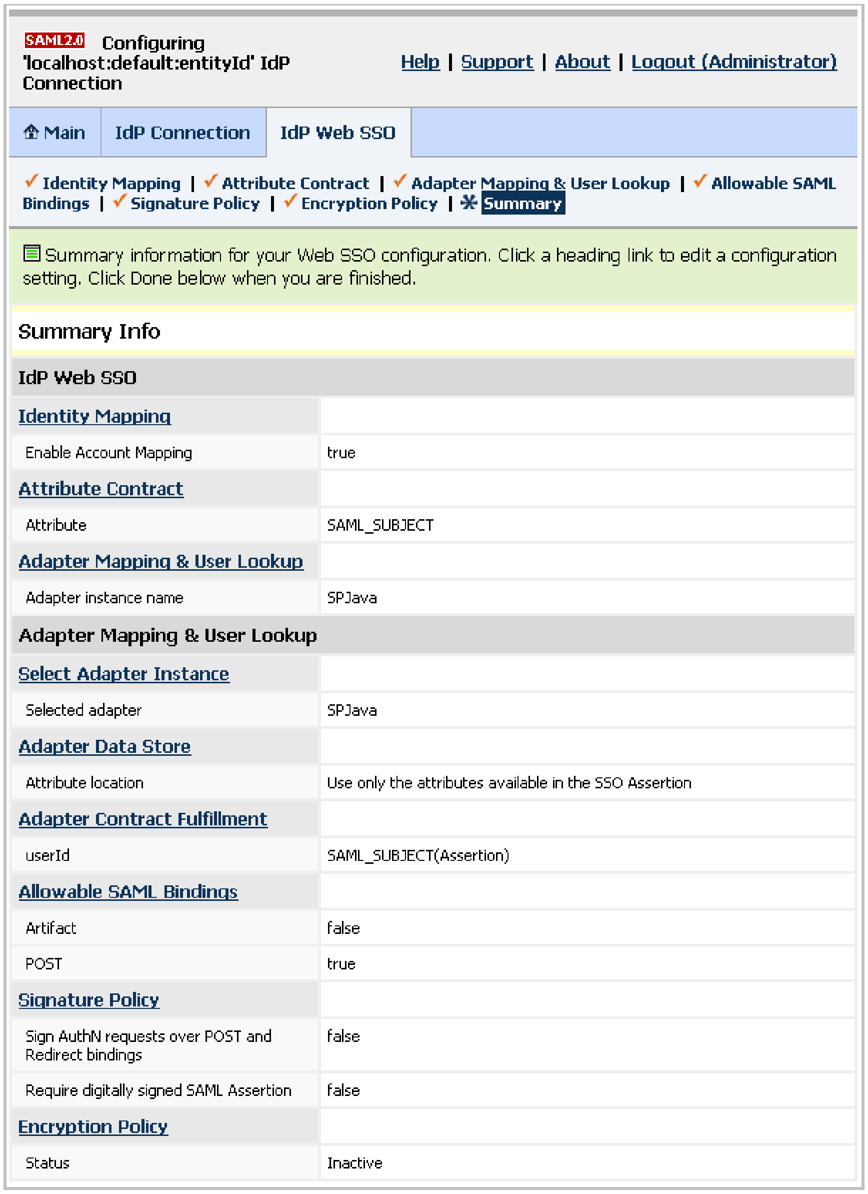
14. On the Adapter Mapping & User Look-up screen, click **Next**.

15. On the Allowable SAML Bindings screen, verify that only the **POST** checkbox is checked. (You may have to de-select **Artifact**.) Click **Next**.

16. On the Signature Policy screen, click **Next**.

17. On the Encryption Policy screen, verify that **None** is selected and then click **Next**.

18. On the Summary screen, click **Done**.


SAML2.0
Help | Support | About | Logout (Administrator)
Main
IdP Connection
IdP Web SSO
✓ Identity Mapping | ✓ Attribute Contract | ✓ Adapter Mapping & User Lookup | ✓ Allowable SAML Bindings | ✓ Signature Policy | ✓ Encryption Policy | ✱ Summary

Configuring 'localhost:default:entityId' IdP Connection

Summary information for your Web SSO configuration. Click a heading link to edit a configuration setting. Click Done below when you are finished.

Summary Info

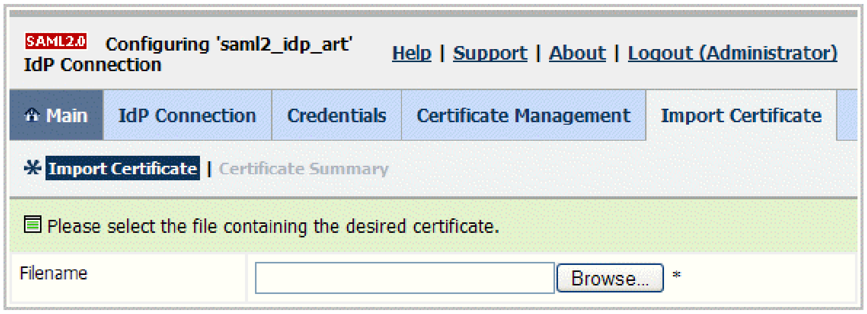
IdP Web SSO	
Identity Mapping	
Enable Account Mapping	true
Attribute Contract	
Attribute	SAML_SUBJECT
Adapter Mapping & User Lookup	
Adapter instance name	SPJava
Adapter Mapping & User Lookup	
Select Adapter Instance	
Selected adapter	SPJava
Adapter Data Store	
Attribute location	Use only the attributes available in the SSO Assertion
Adapter Contract Fulfillment	
userId	SAML_SUBJECT(Assertion)
Allowable SAML Bindings	
Artifact	false
POST	true
Signature Policy	
Sign AuthN requests over POST and Redirect bindings	false
Require digitally signed SAML Assertion	false
Encryption Policy	
Status	Inactive

19. On the Web SSO screen, click **Next**.

Tip: If you want to pause at any time during connection configuration, click the **Save Draft** button. To restart the configuration, click on the **Manage All IdP** link on the Main Menu and then, at the Select a Connection screen, click on the localhost:default:entityId connection. You will return to where you left off.

20. On the Credentials screen, click **Configure Credentials** button.
21. On the Signature Verification Certificate screen, click the **Manage Certificates** button.
22. On the Manage Digital Verification Certificates screen, click the **Import** button.

23. On the Import Certificate screen, click the Browse button and select the certificate you previously exported. (See Step 26 on page 36.) Click **Next**.


SAML2.0
Configuring 'saml2_idp_art' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connection
Credentials
Certificate Management
Import Certificate
Import Certificate | Certificate Summary
Browse...

Please select the file containing the desired certificate.

Filename *

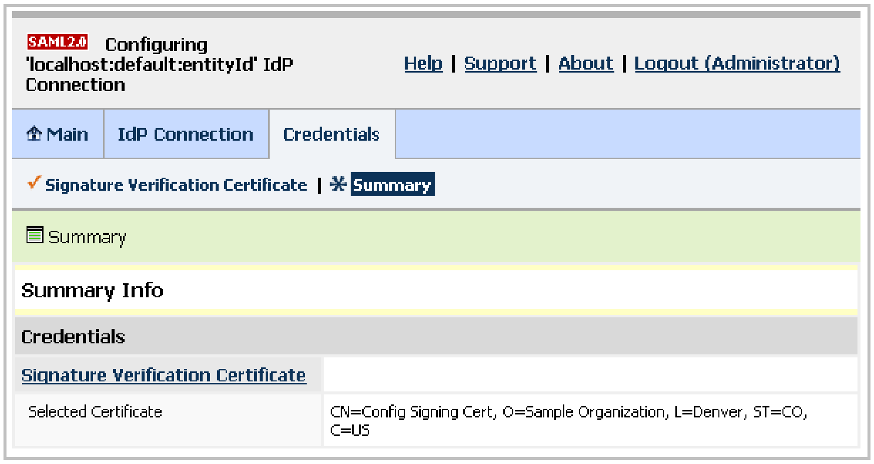
24. On the Certificate Summary screen, click **Done**.

25. On the Manage Digital Verification Certificates screen, click **Done**.

26. On the Signature Verification Certificates screen, ensure that the imported verification certificate is selected as the Primary verification certificate and click **Next**.

    The secondary verification certificate is optional.

27. On the Summary screen, click **Done**.


SAML2.0
Configuring 'localhost:default:entityId' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connection
Credentials
Signature Verification Certificate | Summary
Summary

Summary Info

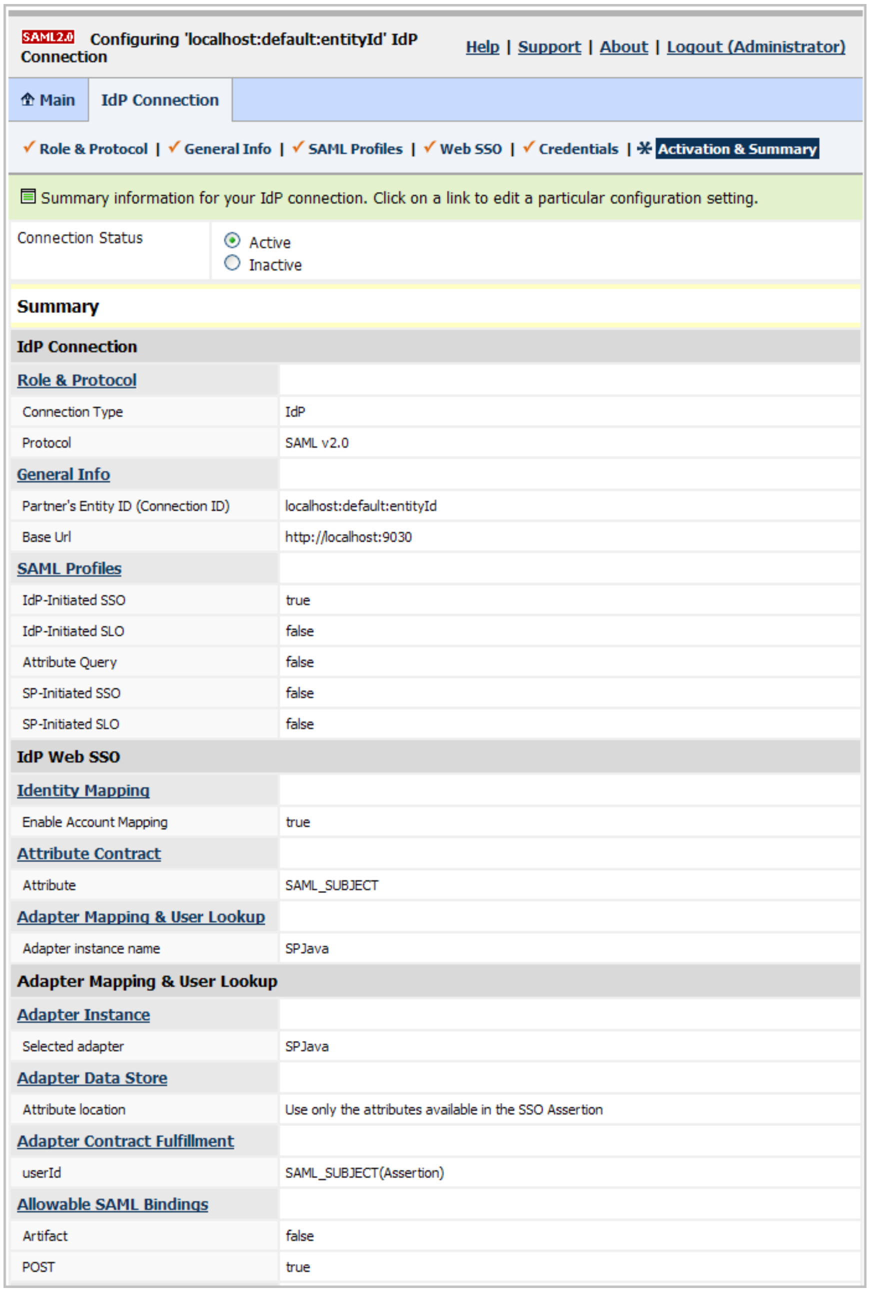
Credentials

Signature Verification Certificate

Selected Certificate	CN=Config Signing Cert, O=Sample Organization, L=Denver, ST=CO, C=US

28. On the Credentials screen, click **Next**.

29. On the Activation & Summary screen, select **Active** for the Connection Status.


SAML2.0
Configuring 'localhost:default:entityId' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connection
✓ Role & Protocol | ✓ General Info | ✓ SAML Profiles | ✓ Web SSO | ✓ Credentials | ✱ Activation & Summary

Summary information for your IdP connection. Click on a link to edit a particular configuration setting.

Connection Status
● Active
○ Inactive

Summary

IdP Connection	
Role & Protocol	
Connection Type	IdP
Protocol	SAML v2.0
General Info	
Partner's Entity ID (Connection ID)	localhost:default:entityId
Base Url	http://localhost:9030
SAML Profiles	
IdP-Initiated SSO	true
IdP-Initiated SLO	false
Attribute Query	false
SP-Initiated SSO	false
SP-Initiated SLO	false
IdP Web SSO	
Identity Mapping	
Enable Account Mapping	true
Attribute Contract	
Attribute	SAML_SUBJECT
Adapter Mapping & User Lookup	
Adapter instance name	SPJava
Adapter Mapping & User Lookup	
Adapter Instance	
Selected adapter	SPJava
Adapter Data Store	
Attribute location	Use only the attributes available in the SSO Assertion
Adapter Contract Fulfillment	
userId	SAML_SUBJECT(Assertion)
Allowable SAML Bindings	
Artifact	false
POST	true

30. Click **Save**.

You have now completed a basic SSO configuration setup. The next step is to test PingFederate using the sample applications (see "Using the Sample Applications" on page 55.)

If you choose to, either before testing or afterward, you can continue configuring additional scenarios. The following scenarios are described in the remainder of this chapter:

- "IdP-Initiated SLO" on page 45

- "SP-Initiated SSO" on page 50
- "SP-Initiated SLO" on page 52

IdP-Initiated SLO

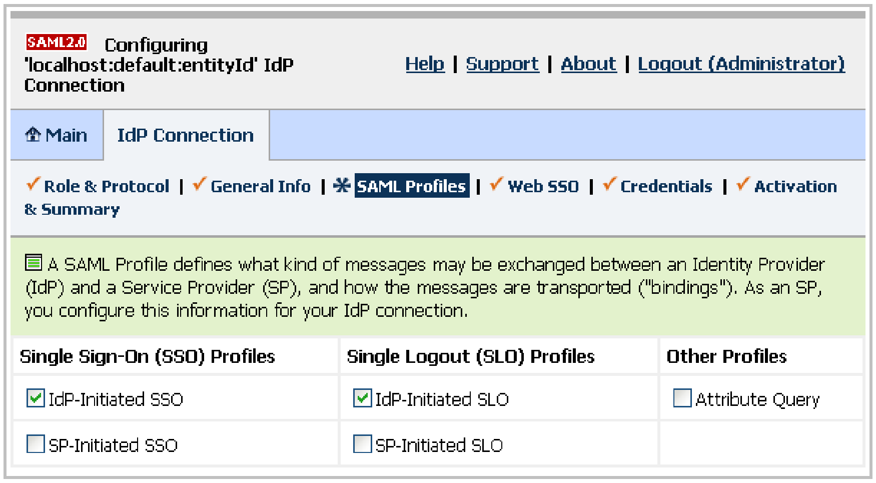
This section describes an optional configuration for IdP-initiated SLO. The steps include generating a signing certificate for the IdP connection.

Note: Ensure that all Server Settings and Connections configurations remain as described earlier in this document. The sample SLO scenarios build upon these settings.

Configure the IdP Connection

Follow these steps to configure the IdP connection for IdP-initiated SLO:

1. On the Main Menu screen, click the previously created **localhost:default:entityId** IdP connection.
2. On Activation and Summary screen, click the **SAML Profiles** step.
3. On the SAML Profiles screen, check IdP-Initiated SLO. Click **Next**.


SAML2.0
Configuring 'localhost:default:entityId' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connection
✓ Role & Protocol | ✓ General Info | ✱ SAML Profiles | ✓ Web SSO | ✓ Credentials | ✓ Activation & Summary

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider (IdP) and a Service Provider (SP), and how the messages are transported ("bindings"). As an SP, you configure this information for your IdP connection.

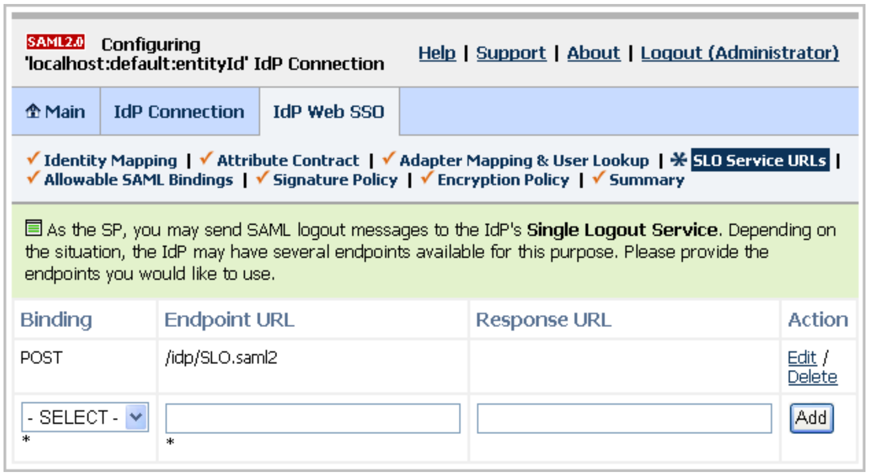
Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles	Other Profiles
☑ IdP-Initiated SSO	☑ IdP-Initiated SLO	☐ Attribute Query
☐ SP-Initiated SSO	☐ SP-Initiated SLO	

Note: You cannot select an SLO profile without also selecting an SSO profile. For further information about the two profiles, see the PingFederate *Administrator's Manual*.

4. On the Web SSO screen, click the **Configure Web SSO** button.
5. If not already selected, click the **SLO Service URLs** step.
6. On the SLO Service URLs screen, select or enter the following values:
   - Binding: `POST`

- Endpoint URL: `/idp/SLO.saml2`

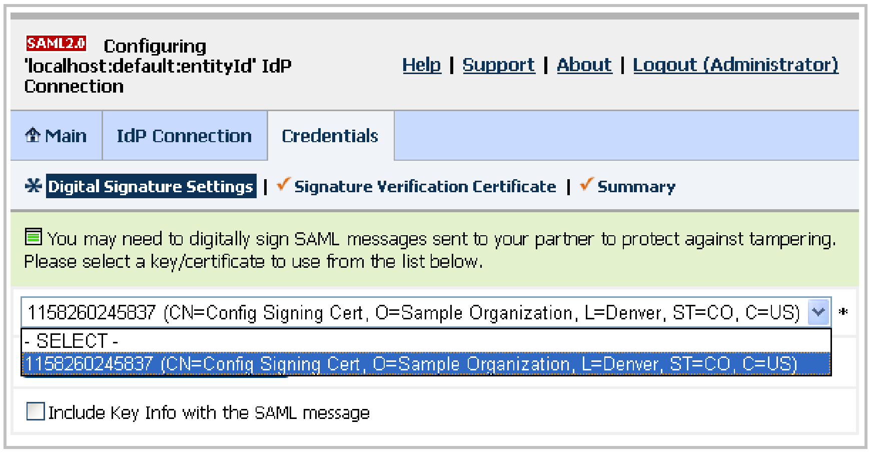
  Note that the ‘`l`’ in ‘`saml2`’ is the lower-case letter ‘L’.
- Response URL: Leave blank


SAML2.0
Configuring 'localhost:default:entityId' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connection
IdP Web SSO
✓ Identity Mapping | ✓ Attribute Contract | ✓ Adapter Mapping & User Lookup | SLO Service URLs |
✓ Allowable SAML Bindings | ✓ Signature Policy | ✓ Encryption Policy | ✓ Summary

As the SP, you may send SAML logout messages to the IdP's **Single Logout Service**. Depending on the situation, the IdP may have several endpoints available for this purpose. Please provide the endpoints you would like to use.

Binding	Endpoint URL	Response URL	Action
POST	/idp/SLO.saml2		Edit / Delete
- SELECT - *	*		Add

7. Click **Add** and then **Next**.
8. On the Allowable SAML Bindings screen, click **Next**. (Only **POST** should be checked. Click **Done** here if you want to skip to the summary screen.)
9. On the Signature Policy screen, click **Next**.
10. On the Encryption Policy screen, click **Next**.
11. On the Summary screen, click **Done**.
12. On the Web SSO screen, click **Next**.
13. On the Credentials screen, click the **Configure Credentials** button.
14. On the Digital Signature Settings screen, select the existing signing certificate from the drop-down menu and click **Next**.


SAML2.0
Configuring 'localhost:default:entityId' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connection
Credentials
Digital Signature Settings | ✓ Signature Verification Certificate | ✓ Summary

You may need to digitally sign SAML messages sent to your partner to protect against tampering. Please select a key/certificate to use from the list below.

1158260245837 (CN=Config Signing Cert, O=Sample Organization, L=Denver, ST=CO, C=US) *
- SELECT -
1158260245837 (CN=Config Signing Cert, O=Sample Organization, L=Denver, ST=CO, C=US)

☐ Include Key Info with the SAML message

15. If you still have the certificate file you exported when establishing the IdP-initiated SSO scenario, click **Next** and move to Step 16. If you do not have

the certificate file, follow the sub-steps below to re-export the verification certificate file from the SP:

  a. Click **Manage Certificates**.
  b. On the Manage Digital Signing Certificates screen, click **Export** in the column to the right of the certificate you created.
  c. On the Export Certification screen, select Certificate Only. Click **Next**.
  d. On the Certificate Summary screen, click **Export** to export the certificate and save it to any folder. Click **Done**.
  e. On the Manage Digital Signing Certificates screen, click **Save**.
  f. On the Digital Signature Settings screen, click **Next**.

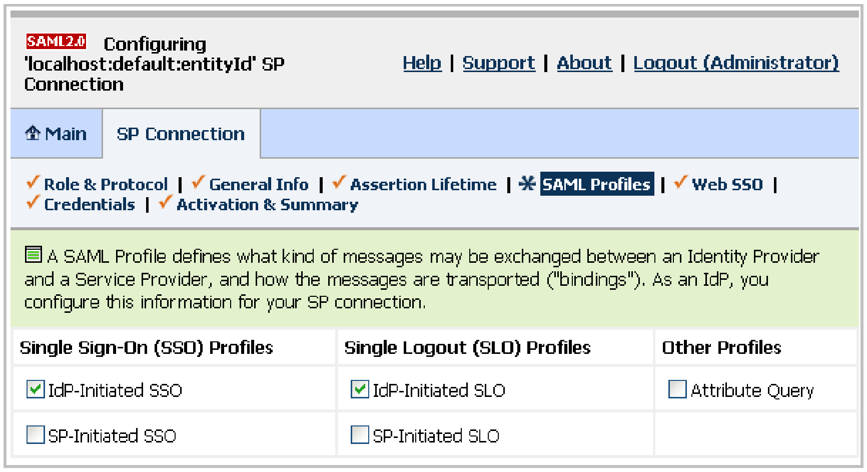
16. On the Signature Verification Certificate screen, click **Done**.
17. On the Credentials screen, click **Save**.

You have now completed configuring the IdP connection for IdP-initiated SLO. The next step is to configure the SP connection.

Configure the SP Connection

Follow these steps to configure the SP connection for IdP-initiated SLO:

1. On the Main Menu screen, click the previously created **localhost:default:entityId** SP connection.
2. On Activation and Summary screen, click the **SAML Profiles** step.
3. On the SAML Profiles screen, check IdP-Initiated SLO and click **Next**.


SAML2.0
Configuring 'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
✓ Role & Protocol | ✓ General Info | ✓ Assertion Lifetime | ✱ SAML Profiles | ✓ Web SSO | ✓ Credentials | ✓ Activation & Summary

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider, and how the messages are transported ("bindings"). As an IdP, you configure this information for your SP connection.

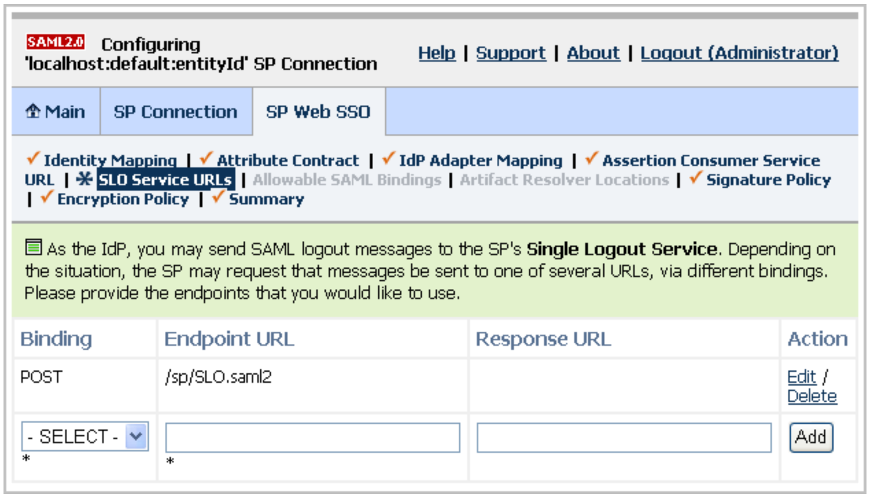
Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles	Other Profiles
☑ IdP-Initiated SSO	☑ IdP-Initiated SLO	☐ Attribute Query
☐ SP-Initiated SSO	☐ SP-Initiated SLO	

Note: You cannot create an SLO profile without an SSO profile. For further information about the two profiles, see the PingFederate *Administrator's Manual*.

4. On the Web SSO screen, click the **Configure Web SSO** button.

5. On the SLO Service URLs screen, select or enter the following values:
   - Binding: `POST`
   - Endpoint URL: `/sp/SLO.saml2`

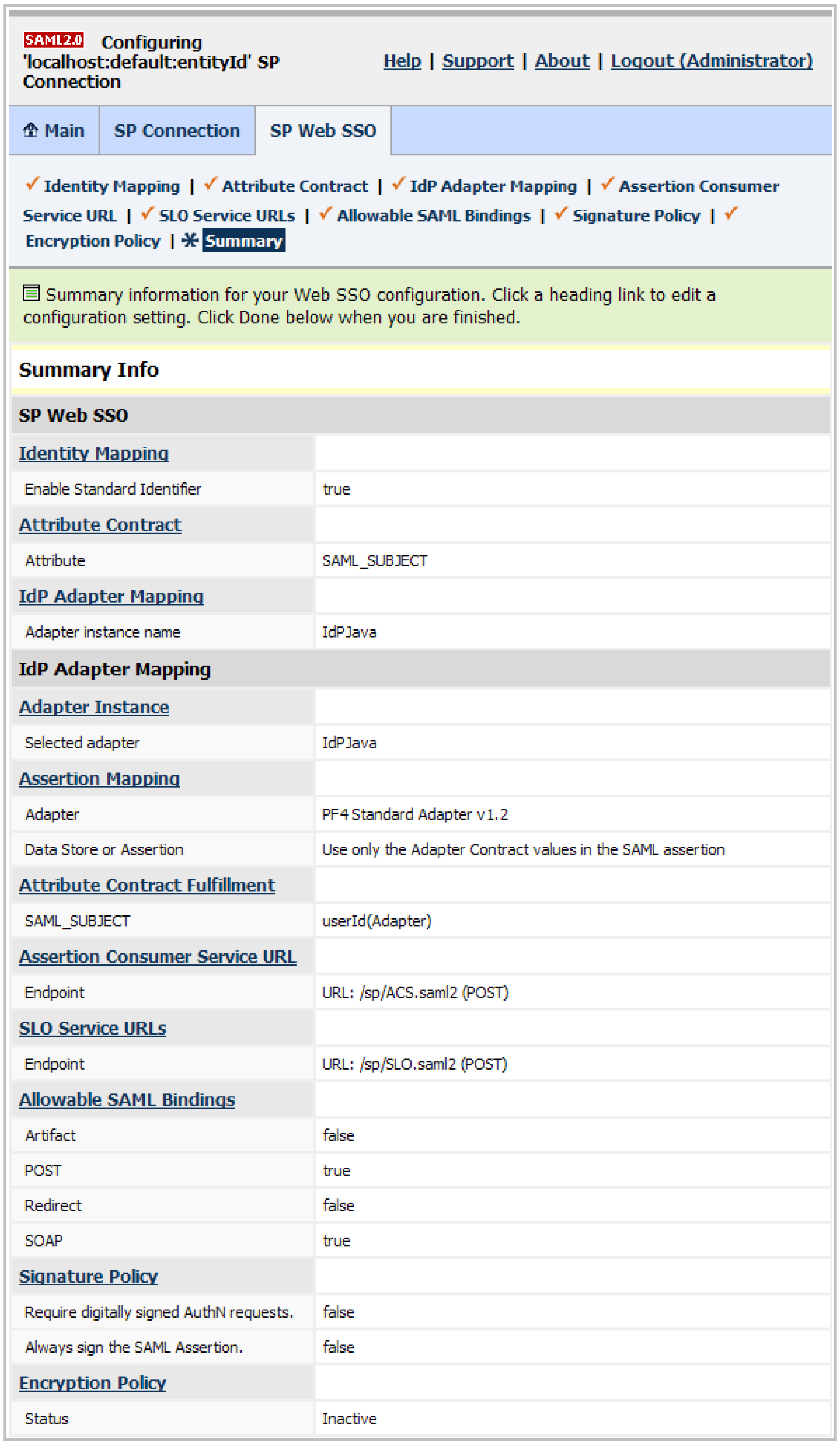
     Note that the ‘`l`’ in ‘`saml2`’ is the lower-case letter ‘L’.
   - Response URL: Leave blank


SAML2.0
Configuring
'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
SP Web SSO
✓ Identity Mapping | ✓ Attribute Contract | ✓ IdP Adapter Mapping | ✓ Assertion Consumer Service URL | ✱ SLO Service URLs | Allowable SAML Bindings | Artifact Resolver Locations | ✓ Signature Policy | ✓ Encryption Policy | ✓ Summary

As the IdP, you may send SAML logout messages to the SP's **Single Logout Service**. Depending on the situation, the SP may request that messages be sent to one of several URLs, via different bindings. Please provide the endpoints that you would like to use.

Binding	Endpoint URL	Response URL	Action
POST	/sp/SLO.saml2		Edit / Delete
- SELECT - *	*		Add

6. Click **Add** and then **Next**.
7. On the Allowable SAML Bindings screen, select **POST** only and click **Next**. (Deselect Artifact, Redirect, and SOAP.)
8. On the Signature Policy screen, click **Next**. (Do not require either additional method of guaranteeing privacy.)
9. On the Encryption Policy screen, click **Next**. (Leave the default at None.)
10. On the Summary screen, click **Done**.



Configuring 'localhost:default:entityId' SP Connection

Help | Support | About | Logout (Administrator)
Main
SP Connection
SP Web SSO
✓ Identity Mapping | ✓ Attribute Contract | ✓ IdP Adapter Mapping | ✓ Assertion Consumer Service URL | ✓ SLO Service URLs | ✓ Allowable SAML Bindings | ✓ Signature Policy | ✓ Encryption Policy | ✱ Summary

Summary information for your Web SSO configuration. Click a heading link to edit a configuration setting. Click Done below when you are finished.

Summary Info

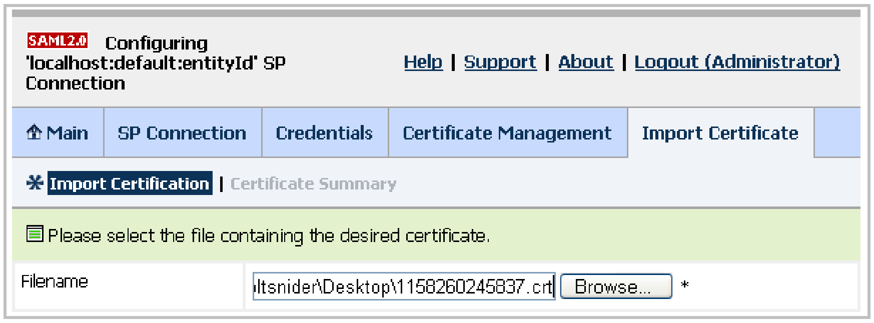
SP Web SSO	
Identity Mapping	
Enable Standard Identifier	true
Attribute Contract	
Attribute	SAML_SUBJECT
IdP Adapter Mapping	
Adapter instance name	IdPJava
IdP Adapter Mapping	
Adapter Instance	
Selected adapter	IdPJava
Assertion Mapping	
Adapter	PF4 Standard Adapter v1.2
Data Store or Assertion	Use only the Adapter Contract values in the SAML assertion
Attribute Contract Fulfillment	
SAML_SUBJECT	userId(Adapter)
Assertion Consumer Service URL	
Endpoint	URL: /sp/ACS.saml2 (POST)
SLO Service URLs	
Endpoint	URL: /sp/SLO.saml2 (POST)
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	false
SOAP	true
Signature Policy	
Require digitally signed AuthN requests.	false
Always sign the SAML Assertion.	false
Encryption Policy	
Status	Inactive

11. On the Web SSO screen, click **Next**.
12. On the Credentials screen, click **Configure Credentials**.
13. On the Signature Verification Certificate screen, the system automatically recognizes that a verification certificate has not been set up for SP-initiated

messages. Click the **Manage Certificates** button to establish the verification certificate.

14. On the Manage Digital Verification Certificate screen, click **Import** to import the verification certificate you created in Step 15 on page 46 of the IdP connection configuration for IdP-initiated SLO.

    On the Import Certification screen, browse to the IdP's verification certificate, which you previously exported, and click **Open**. Click **Next**.


SAML2.0
Configuring 'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
Credentials
Certificate Management
Import Certificate
Import Certification | Certificate Summary
Browse...

Please select the file containing the desired certificate.

Filename ltsnider\Desktop\1158260245837.crt *

15. On the Certificate Summary, click **Done**.
16. On the Manage Digital Verification Certificates screen, click **Done**.
17. On the Signature Verification Certificate screen, ensure that the imported certificate is configured as the Primary certificate. The Secondary certificate is optional. Click **Done**.
18. On the Credentials screen, click **Save**.

You have now completed configuring the SP Connection for IdP-initiated SLO. You can now either test PingFederate using the sample applications (see "Running the Sample Applications" on page 58) or work through the SP-initiated SSO scenario.

SP-Initiated SSO

Follow the steps in this section to configure the IdP and SP connections to enable SP-initiated SSO.

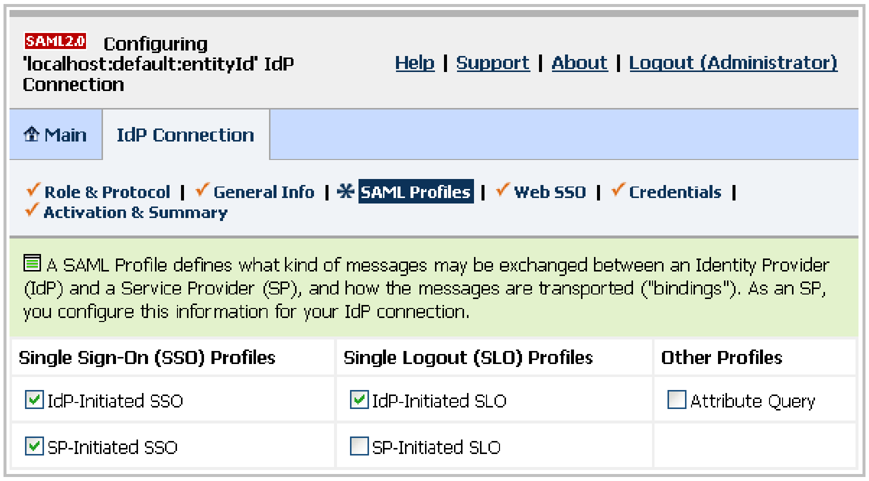
This section builds on configurations in previous sections.

Configure the IdP Connection

In this subsection, you will edit the SP's settings for the IdP connection to allow the SP to send an SSO authentication request to the IdP.

Follow these steps to configure the IdP connection for SSO:

1. On the Main Menu screen, click the previously created **localhost:default:entityId** IdP connection.
2. Click the **SAML Profiles** step.
3. On the SAML Profiles screen, check SP-Initiated SSO and click **Next**.


SAML2.0
Help | Support | About | Logout (Administrator)
Main
IdP Connection
Role & Protocol | General Info | SAML Profiles | Web SSO | Credentials |
Activation & Summary

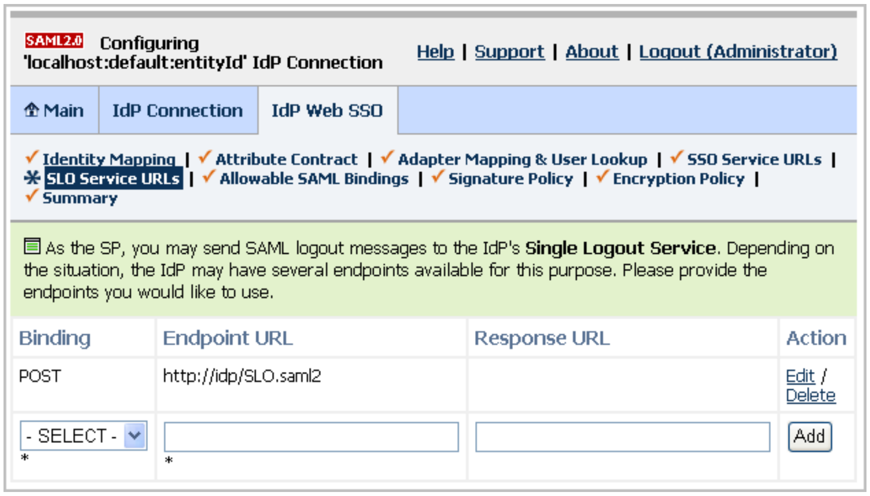
Configuring 'localhost:default:entityId' IdP Connection

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider (IdP) and a Service Provider (SP), and how the messages are transported ("bindings"). As an SP, you configure this information for your IdP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles	Other Profiles
☑ IdP-Initiated SSO	☑ IdP-Initiated SLO	☐ Attribute Query
☑ SP-Initiated SSO	☐ SP-Initiated SLO	

4. On the Web SSO screen, click the **Configure Web SSO** button.
5. On the SSO Service URLs screen, select and enter the following values: Click **Add** and then **Done**.
   - Binding: `POST`
   - Endpoint URL: `/idp/SSO.saml2`

     Note that the ‘`l`’ in ‘`saml2`’ is the lower-case letter ‘L’.
   - Response URL: Leave blank


SAML2.0
Help | Support | About | Logout (Administrator)
Main
IdP Connection
IdP Web SSO
Identity Mapping | Attribute Contract | Adapter Mapping & User Lookup | SSO Service URLs |
SLO Service URLs | Allowable SAML Bindings | Signature Policy | Encryption Policy |
Summary

Configuring 'localhost:default:entityId' IdP Connection

As the SP, you may send SAML logout messages to the IdP's **Single Logout Service**. Depending on the situation, the IdP may have several endpoints available for this purpose. Please provide the endpoints you would like to use.

Binding	Endpoint URL	Response URL	Action
POST	http://idp/SLO.saml2		Edit / Delete
- SELECT - *	*		Add

6. On the Web SSO screen, click **Save**.

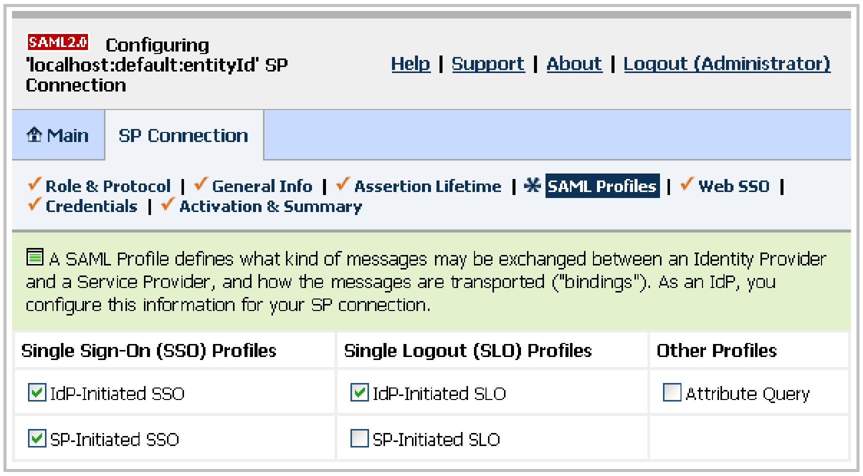
You have now completed configuring the IdP Connection for SP-initiated SSO. The next step is to configure the SP connection.

Configure the SP Connection

Use this configuration to edit the IdP’s settings for the SP connection to allow the IdP to process the SP’s SSO authentication request, which will be sent with SP-initiated SSO.

Follow these steps to configure the SP connection for SP-initiated SSO:

1. On the Main Menu screen, click the previously created **localhost:default:entityId** SP connection.
2. Click the **SAML Profiles** step.
3. On the SAML Profiles screen, check SP-Initiated SSO and click **Save**.


SAML2.0
Configuring 'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
✓ Role & Protocol | ✓ General Info | ✓ Assertion Lifetime | ✱ SAML Profiles | ✓ Web SSO |
✓ Credentials | ✓ Activation & Summary

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider, and how the messages are transported ("bindings"). As an IdP, you configure this information for your SP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles	Other Profiles
☑ IdP-Initiated SSO	☑ IdP-Initiated SLO	☐ Attribute Query
☑ SP-Initiated SSO	☐ SP-Initiated SLO	

You have now completed configuring the SP Connection for SP-initiated SSO. You can now either test PingFederate using the sample applications (see "Running the Sample Applications" on page 58) or configure the SP-initiated SLO scenario.

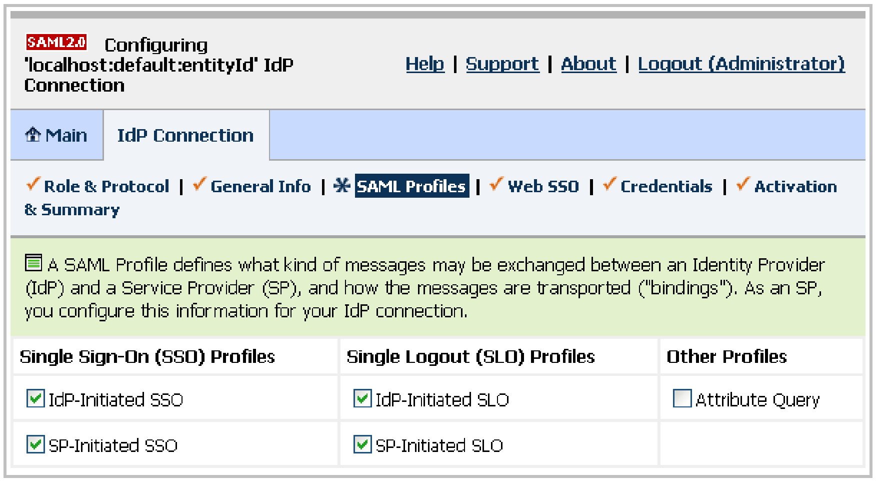
SP-Initiated SLO

This section describes the IdP and SP configurations for SP-initiated SLO. It builds on existing configurations.

Configure the IdP Connection

Follow these steps to configure the IdP connection for SLO:

1. On the Main Menu screen, click the previously created **localhost:default:entityId** IdP connection.
2. Click the **SAML Profiles** step.
3. On the SAML Profiles screen, check SP-initiated SLO and click **Save**.


SAML2.0
Configuring 'localhost:default:entityId' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connection
✓ Role & Protocol | ✓ General Info | ✱ SAML Profiles | ✓ Web SSO | ✓ Credentials | ✓ Activation & Summary

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider (IdP) and a Service Provider (SP), and how the messages are transported ("bindings"). As an SP, you configure this information for your IdP connection.

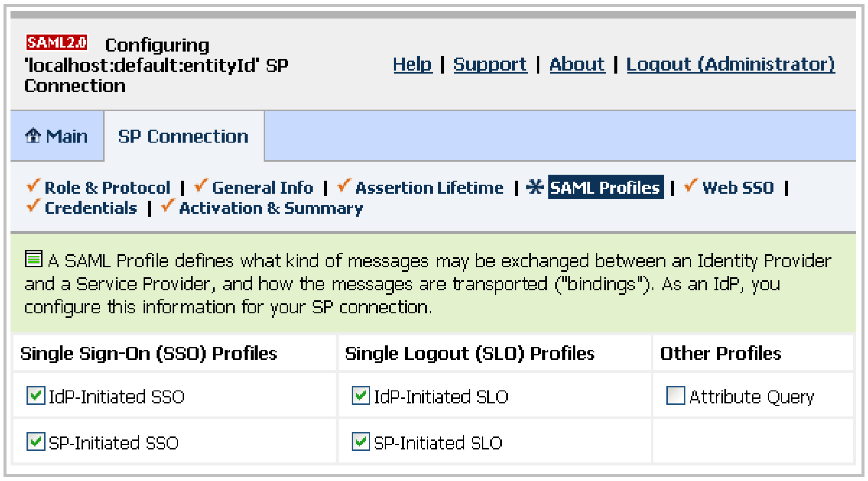
Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles	Other Profiles
☑ IdP-Initiated SSO	☑ IdP-Initiated SLO	☐ Attribute Query
☑ SP-Initiated SSO	☑ SP-Initiated SLO	

You have now completed configuring the IdP Connection for SP-initiated SLO. The next step is to configure the SP connection.

Configure the SP Connection

Follow these steps to configure the SP connection for SP-initiated SLO:

1. On the Main Menu screen, click the previously created **localhost:default:entityId** SP connection.
2. Click the **SAML Profiles** step.
3. Click the **SP-Initiated SLO** checkbox, then click **Save**.


SAML2.0
Configuring 'localhost:default:entityId' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
✓ Role & Protocol | ✓ General Info | ✓ Assertion Lifetime | ✱ SAML Profiles | ✓ Web SSO | ✓ Credentials | ✓ Activation & Summary

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider, and how the messages are transported ("bindings"). As an IdP, you configure this information for your SP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles	Other Profiles
☑ IdP-Initiated SSO	☑ IdP-Initiated SLO	☐ Attribute Query
☑ SP-Initiated SSO	☑ SP-Initiated SLO	

You have now completed configuring the SP Connection for SP-initiated SLO. You can now test PingFederate using the sample applications (see "Running the Sample Applications" on page 58).

Chapter 4

Using the Sample Applications

The sample applications demonstrate SSO and SLO processing to and from your IdP- and SP-configured PingFederate servers.

The IdP sample applications simulate the IdP-initiated SSO/SLO scenario in which users authenticate to an IdP locally in order to access a remote SP application. In this scenario, users can be accessing a company portal that provides links to partner applications such as local news and weather, stock market information, and HR and 401(k) benefits.

When you authenticate locally to the IdP sample application, no communication occurs between it and PingFederate. The user authenticates using the local user store and no SAML use cases are invoked. However, once you click a link to a third-party application, such as your company's 401(k) provider, the IdP initiates an SSO transaction.

The SP sample applications simulate the use case where users authenticate with a local application through a remote IdP. This scenario focuses on the SP-initiated SSO and SLO profiles.

Two sets of sample applications are included in the package: one for Java and one for .NET. The Java sample applications use the Java Integration Kit 1.2 for integration with PingFederate. The .NET sample applications use the .NET Integration Kit 1.2.

Tip: You can download either of these integration kits, among others, from the Ping Identity Web site to obtain documentation that will aid in developing your own applications.

Setting Up the Java Sample Applications

This section describes how to configure and deploy the Java sample applications for the IdP and the SP sides of an identity federation.

Configuring the IdP Sample Application

This section describes the specific values you have to configure to set up the Java sample application on the IdP side.

Important: This configuration depends on the properties that you saved from PingFederate into the `pfagent.properties` file during the Standard Adapter configuration — see Step 7 on page 17.

▶ Update the `pingfederate-idp-config.props` file in the `<pf_install_dir>\quickstart\sample_app\java\IdpSample\config` folder.

a. Enter the base URL for PingFederate:

```
hostPF=http://<pf_host>:9030
```

where `<pf_host>` is the fully qualified domain name of the IdP PingFederate server instance.

b. Use the default for `AttributeNamesList`.

c. Use the default for the Transfer Method, `query`.

d. Use the default for `idpDiscovery`.

e. Enter the password set in the IdP Standard Adapter configuration (see Step 4 under "Configure the IdP Adapter" on page 14).

f. Enter the PFToken holder name specified in the IdP Standard adapter configuration (see Step 4 under "Configure the IdP Adapter" on page 14).

Configuring the SP Sample Application

This section describes the specific values you must configure to set up the SP Java sample application.

Important: This configuration depends on the properties that you copied from PingFederate into the pfagent.properties file during the Standard Adapter configuration — see Step 8 on page 23.

▶ Update the `pingfederate-sp-config.props` file in the `<pf_install_dir>\quickstart\sample_app\java\SpSample\config` folder.

a. Enter the base URL for PingFederate:

   ```
   hostPF=http://<pf_host>:9030
   ```

b. Use the default for `AttributeNamesList`.

c. The Transfer Method must be the same as the setting you selected previously in the PingFederate setup (see Step 5 on page 21). The default for this setting is `query`.

d. Use the default for `accountLinking`.

e. Enter the password set in the SP Standard Adapter configuration (see Step 5 under "Configure the SP Adapter" on page 20).

f. Enter the PFToken holder name specified in the SP Standard adapter configuration (see Step 5 under "Configure the SP Adapter" on page 20).

Deploying the Java Sample Applications

▶ Copy the `IdpSample` and `SpSample` folders to the `webapps` folder in Tomcat.

Note: If you make any changes to either the IdP or SP sample application `props` files, you will need to redeploy the application to Tomcat.

Setting Up the .NET Sample Applications

This section describes how to configure and deploy the .NET sample applications for the IdP and SP.

Configuring the IdP Sample Application

To configure the sample application for .NET, update information in the `pingfederate-idp-config.xml` file in the folder: `<pf_install_dir>\quickstart\sample_app\dotnet\IdpSample\config`

▶ Open `pingfederate-idp-config.xml` in a text editor and update the information shown below in **boldface**:

```
<!--
   Specify the base URL for PingFederate. (We recommend
   using SSL for a production environment).
 -->
 <hostPF>http://localhost:9030</hostPF>
. . . .
   Specify the password specified in Standard Adapter
   configuration
 -->
 <password>Type your password here</password>
```

```
<!--
   Specify the PFTOKEN holder name specified in Standard
   Adapter configuration
-->
 <holderName>Type PFTOKEN Holder name here</holderName>
```

Configuring the SP Sample Application

To configure the sample application for .NET, update information in the `pingfederate-sp-config.xml` file in the folder: *`<pf_install_dir>`*`\quickstart\sample_app\dotnet\SpSample\config`

- Open `pingfederate-sp-config.xml` in a text editor and update the information shown below in **boldface**:

```
<!--
   Specify the base URL for PingFederate. (We recommend
   using SSL for a production environment).
 -->
 <hostPF>http://localhost:9030</hostPF>
. . . .
   Specify the password specified in Standard Adapter
   configuration
 -->
 <password>Type your password here</password>
<!--
   Specify the PFTOKEN holder name specified in Standard
   Adapter configuration
-->
 <holderName>Type PFTOKEN Holder name here</holderName>
```

Deploying the .NET Sample Applications

1. Copy the `IdpSample` and `SpSample` directories to the Internet Information Service (IIS) Web server root. By default the location is:

   `C:\Inetpub\wwwroot\`

2. Using Windows **Control Panel>Administrative Tools>Internet Information Services,** create virtual directories pointing to the `IdpSample` and `SpSample` directories.

   For more information on creating a virtual directory, refer to Microsoft IIS documentation.

Running the Sample Applications

Once you have successfully deployed the sample applications, ensure that your PingFederate server configuration is complete. Depending upon the steps you followed in configuring the server (see "Connection Scenarios" on page 27), you may be able to initiate SAML transactions from either the IdP sample application, the SP sample application, or both.

Note that some controls or links on the sample application pages may not work as expected until all connection scenarios have been configured.

Running the IdP Sample Application

Follow these steps to start the sample application and log in:

1. Start the PingFederate server (if it is not running). For more information, see "Start PingFederate" on page 9.
2. If you are using the Java application, start the Tomcat server by running `<tomcat_dir>\bin\startup.bat` (if the server is not currently running).

   For Linux, enter: `<tomcat_dir>/bin/startup.sh`
3. In a Web browser, open the sample application at one of the following locations:

   For the Java application:

   `http://<sample_hostname>:<sample_port>/IdpSample`

   where *<sample_hostname>* is the host name of the server running the sample application and *<sample_port>* is the port on which your Tomcat server is running (the default is 8080).

   For the .NET application:

   `http://<sample_hostname>:<sample_port>/IdpSample/ MainHandler.aspx`

   where *<sample_hostname>* is the host name of the server running the sample application and *<sample_port>* is the port on which IIS is running.

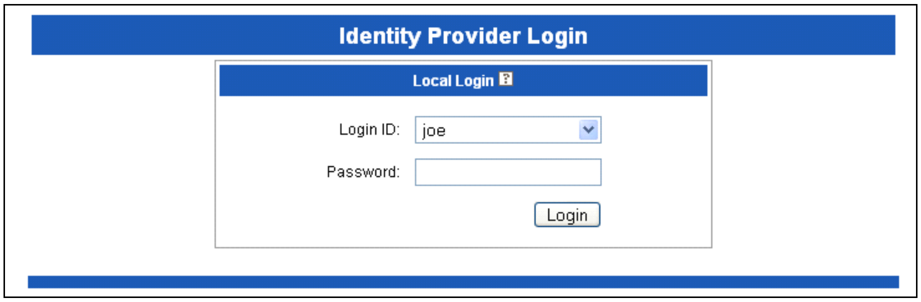
   Note: If you used the automation script, the browser used to access the sample applications must be on the machine that is hosting the PingFederate server (see "Automating the Configuration" on page 65.
4. On the Login screen, enter or select the following values:

   Login ID: `joe`

   Password: `test`

   User accounts other than `joe` may also be used. You can select a different appropriate username from the Login ID drop-down list and enter the corresponding password. Click **Login**.

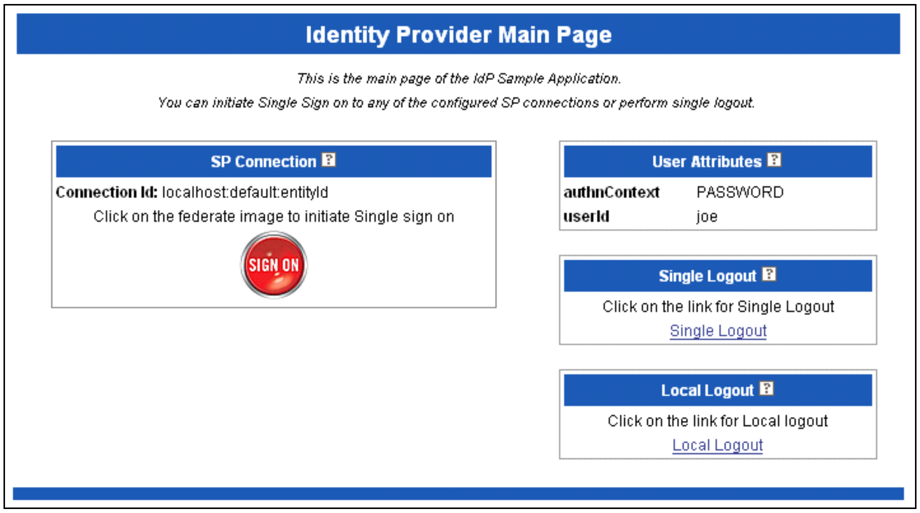
   Note: If you are running the .NET application and you encounter any errors, ensure that you have enabled `.aspx` pages (see "For the .NET Application:" on page 7).



Using the IdP Sample Application

The IdP sample application simulates the scenario in which users, having authenticated to an IdP locally, try to access a remote SP application—IdP-initiated SSO. This scenario represents IdP-initiated SSO and SLO profiles.

After logging in (see the previous section), the Identity Provider Main Page is displayed. The list below describes the effects of selecting each of the options on this screen.



This is the main page of the IdP Sample Application.
You can initiate Single Sign on to any of the configured SP connections or perform single logout.

Connection Id: localhost:default:entityId

Click on the federate image to initiate Single sign on

authnContext PASSWORD
userId joe

Click on the link for Single Logout

Click on the link for Local logout

- Click the **Sign On** button to begin an IdP-initiated SSO to the SP sample application. A user session on the SP will be started and you will be sent to the SP sample application. Upon successful SSO, the Service Provider Main Page screen appears. See "Using the SP Sample Application" on page 62 for more information.
- After returning the SP Application, click **Single Logout** to initiate an SLO request to the SP (if you have configured the IdP-initiated SLO profile).

Once your user session on the remote SP is closed, your local user session will be closed as well.

Note that if you try to initiate an SLO without first performing an SSO, nothing happens. Until you initiate SSO, your user session is local to the IdP sample application and does not exist for the SP.

If you initiated SSO from the SP (see the next sections) and you have enabled IdP-initiated SLO, then the **Single Logout** link is operational and will close both sessions.

▶ Click **Local Logout** to close your user session on the IdP sample application. You will go to the IdP Sample Application Login Page.

Running the SP Sample Application

Follow these steps to start the sample application and log in directly (rather than through the IdP):

1. Start the PingFederate server (if it is not running). For more information, see "Start PingFederate" on page 9.
2. If you are using the Java application, start the Tomcat server by running `<tomcat_dir>\bin\startup.bat` (if the server is not currently running).

   For Linux, enter: `<tomcat_dir>/bin/startup.sh`
3. In a Web browser, open the sample application at one of the following locations:

   For the Java application:

   `http://<sample_hostname>:<sample_port>/SpSample`

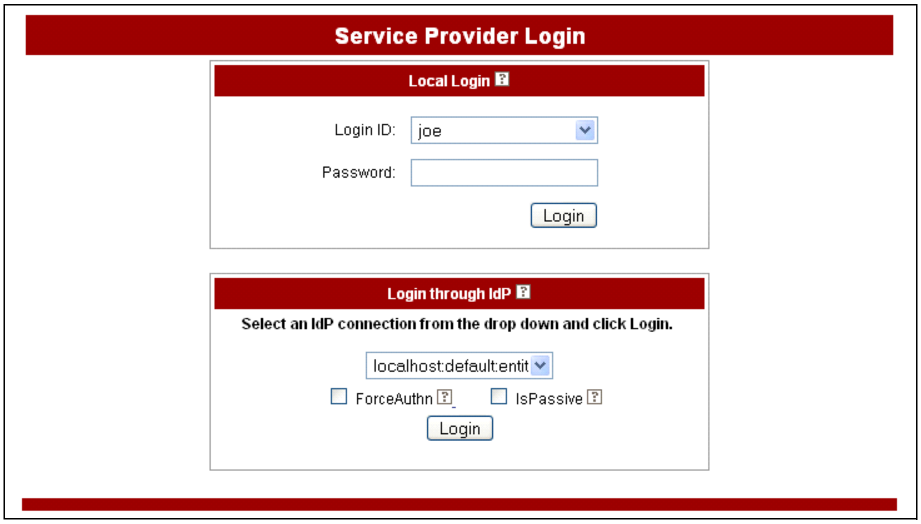
   where *<sample_hostname>* is the host name of the server running the sample application and *<sample_port>* is the port on which your Tomcat server is running (the default is 8080).

   For the .NET application:

   `http://<sample_hostname>:<sample_port>/SpSample/MainHandler.aspx`

   where *<sample_hostname>* is the host name of the server running the sample application and *<sample_port>* is the port on which IIS is running.

Note: If you used the automation script, the browser used to access the sample applications must be on the machine that is hosting the PingFederate server (see "Automating the Configuration" on page 65).



Service Provider Login

Local Login

Login ID: joe

Password:

Login

Login through IdP

Select an IdP connection from the drop down and click Login.

localhost:default:entit

☐ ForceAuthn ☐ IsPassive

Login

4. On the Login screen, enter or select the following values:

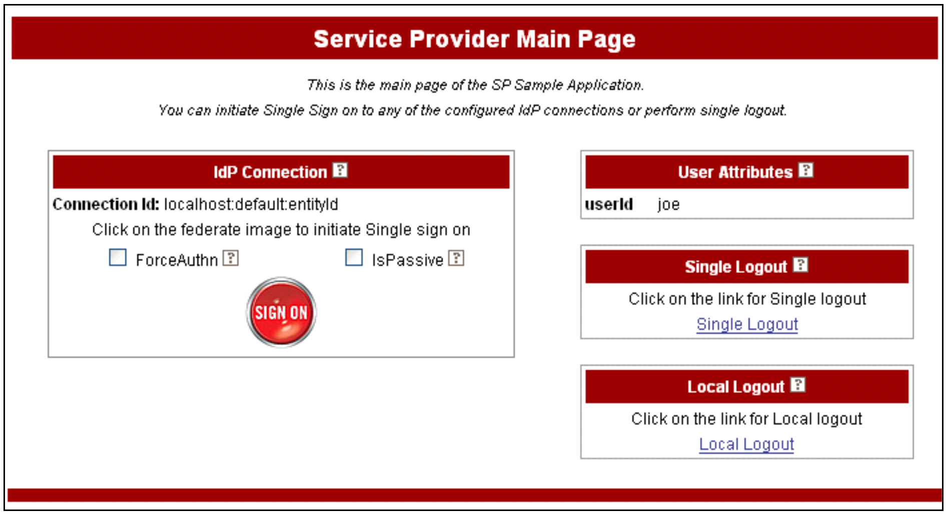
   Login ID: `joe`

   Password: `test`

Note: If you are running the .NET application and you encounter any errors, ensure that you have enabled `.aspx` pages (see "For the .NET Application:" on page 7).

Using the SP Sample Application

When you reach the Service Provider Main Page via the SP Login Page, you can demonstrate the scenario in which users authenticate with a local application through a remote IdP. This scenario focuses on the SP-initiated SSO and SLO profiles.



Service Provider Main Page

This is the main page of the SP Sample Application.

You can initiate Single Sign on to any of the configured IdP connections or perform single logout.

IdP Connection

Connection Id: localhost:default:entityId

Click on the federate image to initiate Single sign on

☐ ForceAuthn ☐ IsPassive

SIGN ON

User Attributes

userId joe

Single Logout

Click on the link for Single logout

Single Logout

Local Logout

Click on the link for Local logout

Local Logout

The list below describes the uses of this screen:

- Click **Sign On** to begin an SP-initiated SSO transaction.

  If you have already authenticated through the IdP, you will not be required to re-authenticate unless either the ForceAuthn or IsPassive option is checked.

- Click **Single Logout** to begin an SP-initiated SLO transaction. Upon successful completion of this transaction, you will be sent to the SP Sample Application Login Page.

  Note that if you try to initiate an SLO without first performing an SSO, nothing happens. Until you initiate SSO, either from this screen or from the IdP Application, your user session is local to the SP sample application and does not exist for the IdP.

- Click **Local Logout** to close your local-user session on the SP sample application. You will be sent to the SP Sample Application Login Page.

Once you have successfully tested PingFederate using the sample applications, you can revise the connection configurations to suit your actual federation needs and return to the sample applications for testing.

Appendix

A

Automating the Configuration

This *Guide* is intended to introduce IT personnel to PingFederate. We recommend that you follow the procedures in this document step-by-step to get the full experience of configuring the server, individual connections, and sample applications.

Because manual configuration can be error-prone, however, we provide a script to automate the procedure. You can use this script either in place of manual configurations or to expedite any troubleshooting required after following the procedures in this *Guide*. The script overlays the correct configuration into the PingFederate server files and sample-application configuration files.

Running the Setup Script

To use the script, you must install Ant (see "System Requirements" on page 6). Ant is a tool that performs specified tasks in response to a desired "target."

Warning: The script overwrites all configuration settings. If you have configured adapters or connections outside the scope of this document and you wish to keep the settings, ensure that you archive them for later recovery (see the "System Administration" chapter in the *Administrator's Manual*).

The Ant `build.xml` file is located in `<pf_install_dir>/quickstart/scripts/Java/` and `<pf_install_dir>/quickstart/scripts/dotnet/`.

In each of these locations there is also a `quickstart.properties` file that contains settings that you may need to adjust for your environment. The `quickstart.properties` file contains values that affect the PingFederate server and sample-application configuration settings made by Ant. The most common setting that may need to be adjusted is the Java configuration `sample_port` number. The default value is 8080; if your Web server listens on a different port, you will need to change that setting.

After you run the script, the only task remaining is to deploy the applications into your Tomcat or IIS server installation.

To run the setup script and deploy the sample applications:

1. Shut down the PingFederate server if it is running.

   Enter `Ctrl-C` in the command or terminal window running the server.

2. At a command prompt in the directory containing the `build.xml` file, enter:

   ```
   ant
   ```

3. Start the PingFederate server (see "Start PingFederate" on page 9).

4. Deploy the `IdpSample` and `SpSample` folders to your Web server installation.

   For more information, see either "Deploying the Java Sample Applications" on page 57 or "Deploying the .NET Sample Applications" on page 58.