PingFederate®

Java Integration Kit

Version 2.5.1

Sample Application Startup Guide

PingIdentity®

PingFederate Java Integration Kit
Sample Application User Guide
Version 2.5.1
November, 2012

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

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

Trademarks

Disclaimer

Document Lifetime

Ping Identity may occasionally update online documentation between releases of the related software. Consequently, if this PDF was not downloaded recently, it may not contain the most up-to-date information. Please refer to documentation.pingidentity.com for the most current information.

From the Web site, you may also download and refresh this PDF if it has been updated, as indicated by a change in this date: **November 30, 2012**

Contents

Overview

This document provides instructions for installing, configuring, and using the sample applications bundled with the PingFederate Java Integration Kit. The applications provide a means of testing an end-to-end Identity Provider (IdP) and Service Provider (SP) integration with PingFederate using this integration kit.

This distribution also includes Java source code and server pages (JSPs) and style sheets that can be modified, either to change the behavior or appearance of the sample applications or to develop your own applications for production-ready deployment. The primary intent of the source code is to demonstrate methods of Java application integration using the OpenToken application programming interface (API).

The sample-application distribution provides startup components that automatically configure PingFederate to act as both an IdP and an SP:

- The IdP server is configured to look up authentication information via the OpenToken Adapter and create a SAML (Security Assertion Markup Language) assertion to send to the SP for single sign-on (SSO).
- The SP server is configured to forward this information, again via OpenToken, to the SP sample application to create the local user session. The SP server is also configured to send authentication requests to the IdP on behalf of local users.

Intended Audience

The installation and basic usage portions of this *Guide* are intended for PingFederate administrators and Web-application architects and developers wanting to test the deployment of the Java Integration Kit or validate end-to-end integration. Some knowledge of the PingFederate administrative console and identity federation using SAML is helpful but not required.

Sections describing the optional use of the Java source code and advanced alternative deployment scenarios are intended, respectively, for experienced Java developers and administrators with some expertise using and deploying PingFederate in a production environment.

System Requirements for the Sample Applications

The following software must be installed and operational in order to run the Java sample applications:

- PingFederate 5.x (or higher)
- OpenToken Adapter 2.5.1 or newer

Note: For installation steps (applicable to PingFederate 6.2 and earlier versions), please refer to Installation and Setup in the Java Integration Kit *User Guide*.

- JavaScript-enabled Web browser
- Apache Ant (if rebuilding the sample applications)

Sample Applications Installation and Setup

The sample-application distribution is located in the `<integration_kit_install_dir>/sample` directory and consists of:

- Two extracted WAR directories containing the IdP and SP sample applications (`IdpSample.war` and `SpSample.war`)

  Note: The sample applications are preconfigured with the OpenToken Java Agent library file (`opentoken-agent-2.5.1.jar`) as well as other required libraries. (See Installation and Setup in the Java Integration Kit *User Guide* for more details.)

- A `data.zip` file containing the PingFederate server configuration necessary to support the sample applications

  Note: This configuration archive assumes the PingFederate servlet container is hosting the sample applications.

Installing the sample applications requires setting up PingFederate and then deploying the applications, as described in the following sections.

Setting Up PingFederate

Use the `data.zip` file (discussed in the previous section) to configure PingFederate automatically.

Caution: Deploying `data.zip` overwrites any existing configuration settings. If you have configured adapters, data stores, or partner connections outside the scope of this document and you wish to keep the settings, ensure that you archive them for later recovery. (For further details, see System Administration in the PingFederate *Administrator's Manual*.)

To configure PingFederate to use the sample applications:

1. Deploy the OpenToken Adapter included in this distribution to PingFederate per instructions provided in the Java Integration Kit *User Guide*.
2. Ensure the PingFederate server is running.
3. Copy the `data.zip` file into:

   `<pf_install_dir>/pingfederate/server/default/data/drop-in-deployer/`

   This step uses the PingFederate configuration-archive hot-deployment feature to set up the complete server configuration needed. The file is renamed with a timestamp when the configuration is deployed to the PingFederate server (the `drop-in-deployer` directory is checked frequently when the server is running).

   Note: To simplify deployment, the `data.zip` archive configures a single PingFederate instance to serve both the IdP and SP roles. In such a deployment, PingFederate performs SSO and single logout (SLO) transactions in a loopback configuration. While this scenario is valid for demonstration and testing and keeps the deployment and setup simple, it is not applicable to a real situation. In production circumstances, you may wish to deploy the

configurations into instances of PingFederate running on different hosts and then make necessary configuration updates manually (see Advanced Installation and Configuration on page 14).

Deploying the Sample Applications

To deploy the sample applications:

1. Copy the `IdpSample.war` and `SpSample.war` directories into the directory:

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

   Note: For convenience and simplicity, this procedure deploys the applications into the PingFederate servlet container. You may choose instead to deploy the applications in a separate container on your network and then make the necessary configuration changes (see Advanced Installation and Configuration on page 14).

2. Start or restart the PingFederate server.

   If you are new to PingFederate, see Starting and Stopping PingFederate in the PingFederate *Administrator's Manual*.

Using the Sample Applications

The sample IdP and SP applications demonstrate SSO and SLO processing to and from your PingFederate server. Each application also:

- Displays attributes provided by the OpenToken Adapter on an IdP-application Web page and attributes received in SSO assertions on an SP-application Web page.

  Tip: You can also see artifacts of these transactions in the command window running PingFederate or in the server log file.

- Provides several configurable SSO and operational options that may be adjusted for testing alternative deployment and configuration scenarios (see Advanced Installation and Configuration on page 14).

You can initiate SSO from either the IdP application (see the next section, Using the IdP Sample Application) or the SP application (see Using the SP Sample Application on page 10).

Note: Developers can adjust the look and feel of the sample applications and modify the source code to change functionality for testing and demonstration. Developers may also use the source files to implement SSO/SLO functionality in their own Web applications for enterprise deployment (see Modifying Sample Source Files on page 13).

Using the IdP Sample Application

When loaded first, the IdP sample application simulates 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

may be accessing a company portal, for example, that provides links to partner Web resources such as HR or 401(k) information.

To use the IdP sample application:

1. Ensure the PingFederate server is running.
2. In a Web browser, open the sample application:

   `https://localhost:9031/IdpSample`

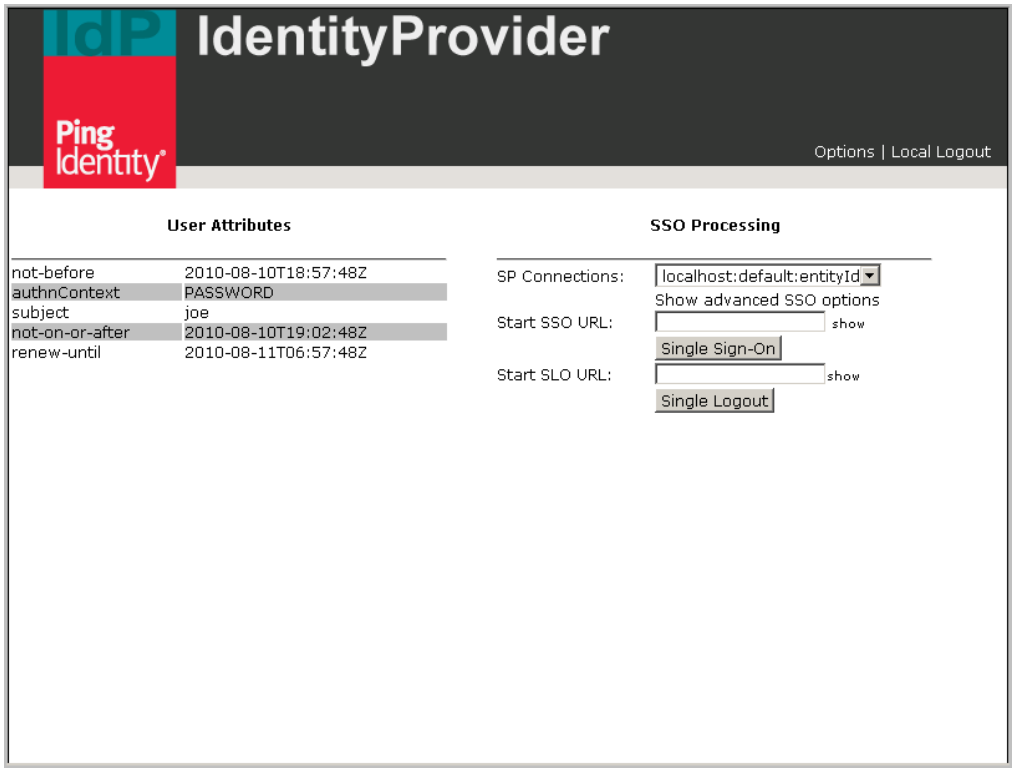
   (Change the host specifications if you have deployed the application elsewhere—see Advanced Installation and Configuration on page 14.)
3. On the home page, click **Login Locally**.
4. On the Identity Provider Local Login page, use the following values:

   Username: `joe`

   Password: `test`

   You can select a different user from the Username drop-down list. The password is `test` for all users.
3. Click **Login**.

   When you authenticate locally to the IdP sample application, no communication occurs between the application and PingFederate; the user authenticates using the local user store. No SSO use cases are invoked until PingFederate is called on the home page via the **Single Sign-On** button.



4. After logging on to the IdP sample application, the Identity Provider home page is redisplayed.

   In addition to SSO/SLO information and controls, this page now shows attributes that will be sent to the SP in the SAML assertion.

Note: If you have chosen not to deploy the sample application in the same servlet container running PingFederate, click **Options** to update the PingFederate host and any other information as needed (see Advanced IdP Deployment and SSO Options on page 8).

Tip: (Optional) To view the PingFederate endpoint URLs used to start SSO or SLO, click **show** next to the fields above each of the associated buttons.

If you have created an additional SP connection and wish to test it, choose the connection name from the SP Connections drop-down list. For information about additional SSO configuration options that may apply, see Advanced IdP Deployment and SSO Options on page 8.

The steps below describe how to exercise the basic SSO/SLO functionality of this page:

a. Click **Single Sign-On** to begin IdP-initiated SSO to the SP sample application. A user session on the SP is created, and you are logged-in to the SP sample application. (See Using the SP Sample Application, on page 10 for more information.)

b. To demonstrate IdP-initiated SLO, return to this Identity Provider page by changing the browser location back to `https://localhost:9031/IdpSample`. Then click **Single Logout** to initiate an SLO request to the SP. When the user session on the remote SP is destroyed, the local session is destroyed as well (clicking **Single Sign-on** here or on the SP application page redirects to the IdP logon page).

Note that if you initiate SSO from the SP, the **Single Logout** button is operational and will also end both sessions. If you click **Local Logout** on this screen, the SP session is still in force; you can access the SP application directly in the browser and see the attributes passed in from the original SAML assertion.

Advanced IdP Deployment and SSO Options

The IdP sample application provides options that may be used to change settings to accommodate advanced, alternative deployment scenarios or to test different SSO configurations.

To change deployment options:

1. In the top menu on the IdP home page, click **Options**.
2. If needed, change entries under IdP Sample Application Configuration, as described in the following table, and then click **Save**.

Field Name	Description
PF Host Name	The host for the PingFederate runtime engine. Change this entry if the sample applications are not deployed on the same host.
Use SSL*	When checked, the application connection to PingFederate uses the secure channel (HTTPS).

Field Name	Description
PF HTTP Port*	The PingFederate server does not normally use the clear-channel port. It is disabled by default for versions 5.1 and higher. The previous default port number is shown here. Change the value if your configuration uses HTTP but on a different port (as set in the `run.properties` file in the `pingfederate/bin` directory).
PF HTTPS Port*	The PingFederate secure-channel port. The installation default is shown. Change the value if the port is not the same as that specified in the PingFederate runtime configuration file (`run.properties`).
PF Web Service Username*	The username specified in PingFederate for access to the built-in IdP SSO Directory Service (see Web Service Interfaces in the PingFederate *Administrator's Manual*).
PF Web Service Password*	The password for the Web Service described above.
Attribute Names List*	May be used to test and demonstrate passing multi-value attributes in the assertion.
*Click Show advanced options.	

3. Locate and **Upload** the IdP OpenToken Configuration file.

   This option is *not required* for the automated PingFederate configuration using the `data.zip` archive (see Setting Up PingFederate on page 5). When you deploy the applications, the associated configuration file (`agent-config.txt`) is located in the directory:

   `<deploy_dir>/IdPSample.war/config`

   where `<deploy_dir>` is `pingfederate/server/default/deploy` in the PingFederate installation, or the deployment directory chosen for a different Web container (see Advanced Installation and Configuration on page 14).

   If, however, you change the default OpenToken Adapter configuration or create a different adapter instance and configure it into the SP connection, then download the configuration file in the administrative console and upload it here. (Alternatively, replace the existing file in the `config` directory and restart the application.)

To change SSO configuration options:

1. Click **Show advanced SSO options**.
2. Change entries as needed for the fields displayed, as described in the following table:

Field Name	Description
Target URL	If you are testing a connection targeting an SP application other than the installed sample, enter the application's identifying URL.
IdP Adapters	If you have added another adapter instance to the SP connection configuration for the SP sample (or if you are using a different connection with more than one adapter instance

Field Name	Description
	configured), choose the adapter instance from the drop-down list.

Using the SP Sample Application

When accessed first, the SP sample application simulates SP-initiated SSO and SLO scenarios. The application also provides a simulated target resource for SSO/SLO transactions initiated from the IdP.

To use the SP sample application:

1. Ensure the PingFederate server is running.
2. In a Web browser, open the sample application:

   `https://localhost:9031/SpSample`

   (Change the host specifications if you have deployed the application elsewhere—see Advanced Installation and Configuration on page 14.)

   Note: Before proceeding to the next step, if the IdP PingFederate server is not deployed on the same host running the sample application, click **Options** in the top menu to update the host and other information as needed (see Advanced SP Deployment and SSO Options on page 11).

   Tip: On the Service Provider main page, if you have created an additional IdP connection and wish to test it, choose its connection name from the IdP Connections drop-down list.

   ---

3. Click **Single Sign-On** to begin SP-initiated SSO.

   You are redirected to the IdP logon page.

   Note: If you are already logged on at the IdP, this step simply redisplays the page (unless ForceAuthn is checked under **Show advanced options**—see Advanced SP Deployment and SSO Options on page 11). Click **Single Logout** to try again.

   Tip: (Optional) To view the PingFederate endpoint URL used to start SSO, click **show** next to the field above the **Single Sign-On** button.

   ---

4. On the Identity Provider login page, enter the following values:

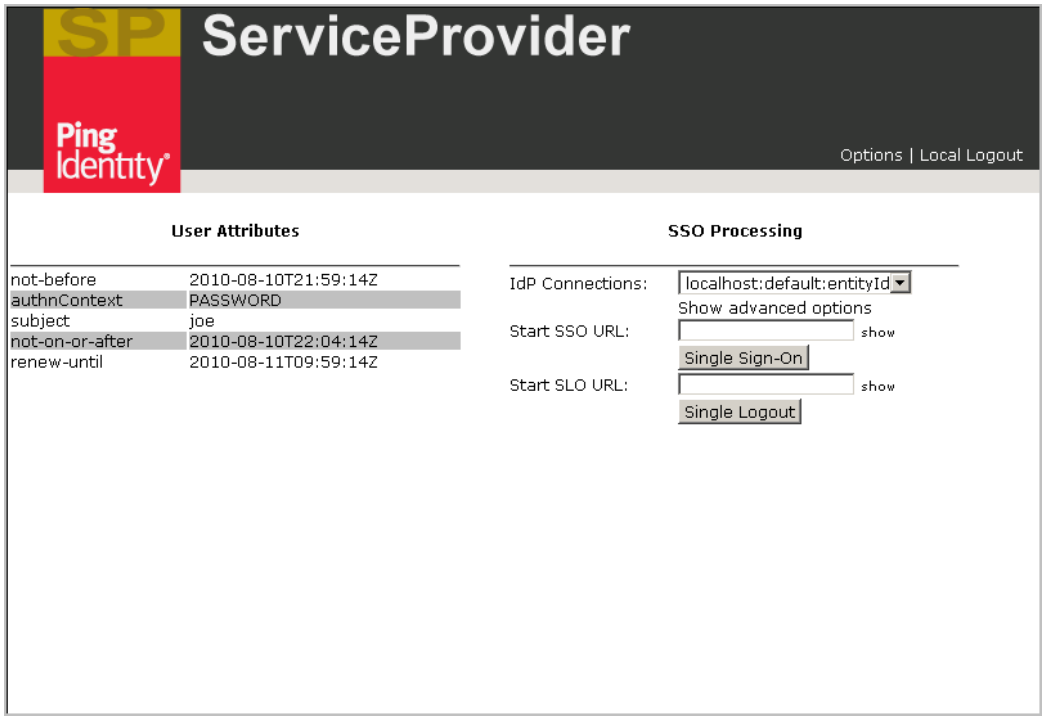
   Username: `joe`

   Password: `test`

   You can select a different user name from the Username drop-down list. The password is `test` for all users.

5. Click **Login**.

   Having completed an SP-initiated SSO, you are redirected back to the Service Provider main page, which now displays attributes sent from the IdP in the SAML assertion.



6. Click **Single Logout** to begin an SP-initiated SLO transaction.

   Upon successful completion of this transaction, the Service Provider main page is redisplayed but without attributes listed.

Note: Clicking **Local Logout** in the top menu has the same effect. However, since you are still logged on at the IdP, if you click **Single Sign-On** again (either here or at the IdP), you are not required to re-authenticate. This page is redisplayed immediately with SSO attributes available from a new IdP-generated SAML assertion.

Advanced SP Deployment and SSO Options

The SP sample application provides options that may be used to change settings to accommodate alternative deployment scenarios or to test different SSO configurations.

To change deployment options:

1. In the top menu on the SP home page, click **Options**.
2. If needed, change entries under SP Application Configuration, as described in the following table, and click **Save**.

Field Name	Description
PF Host Name	The host for the PingFederate runtime engine. Change this entry if the sample applications are not deployed on the same host.
Use SSL*	When checked, the application connection to PingFederate uses the secure channel (HTTPS).

Field Name	Description
PF HTTP Port*	The PingFederate server does not normally use the clear-channel port. It is disabled by default for versions 5.1 and higher. The previous default port number is shown here. Change the value if your configuration uses HTTP but on a different port (as set in the `run.properties` file in the `pingfederate/bin` directory).
PF HTTPS Port*	The PingFederate secure-channel port. The installation default is shown. Change the value if the port is not the same as that specified in the PingFederate runtime configuration file (`run.properties`).
PF Web Service Username*	The username specified in PingFederate for access to the built-in IdP SSO Directory Service (see Web Service Interfaces in the PingFederate *Administrator's Manual*).
PF Web Service Password*	The password for the Web Service described above.
Attribute Names List*	May be used to test and demonstrate passing multi-value attributes in the assertion.
*Click Show advanced options.	

3. Locate and **Upload** the SP OpenToken Configuration file.

   This option is *not required* for the automated PingFederate configuration using the `data.zip` archive (see Setting Up PingFederate on page 5). When you deploy the applications, the associated configuration file (`agent-config.txt`) is located in the directory:

   `<deploy_dir>/SpSample.war/config`

   where `<deploy_dir>` is `pingfederate/server/default/deploy` in the PingFederate installation (or the deployment directory you have chosen for a different Web container—see Advanced Installation and Configuration on page 14).

   If, however, you change the default OpenToken Adapter configuration or you want to use a new adapter instance mapped into the IdP connection, then download the configuration file in the administrative console and upload it here. (Alternatively, replace the existing file in the `config` directory and restart the application.)

To change SSO configuration options:

1. Click **Show advanced options**.
2. Change entries as needed for the fields displayed, as described in the following table:

Field Name	Description
SP Adapters	If you have added another adapter instance to the same IdP connection configuration in PingFederate (or if you are using a different connection with more than one adapter instance configured), choose the adapter instance from the drop-down list.

Field Name	Description
Is Passive	When selected, the IdP is requested not to visibly take control of the user's browser. (Thus, if the user is not authenticated at the IdP site, SSO will fail.)
Force Authn	When selected, IdP authentication is required regardless of whether the user is already authenticated at the IdP site.

Modifying Sample Source Files

The Java Integration Kit distribution provides the source files for the sample applications in the `sample_src` directory, including Java code and supporting JSPs, images, style sheets and other components. Developers can use these files to change the appearance and behavior of the samples, to create different samples for testing, or to develop actual prototypes for production purposes. In addition, the commented Java code is engineered into discrete classes and methods that can be repurposed to work with existing Web applications.

This section further identifies the source file directories and describes how to rebuild the sample applications, as a means of highlighting file locations and build scripts that developers may use for other customizing purposes.

JSPs and Web-Page Components

You can modify the JSPs, images, and cascading style sheets (CSSs) to customize the look and feel of the installed sample applications.

The JSP files are located in the following directories in the Java Integration Kit distribution:

```
sample_src/<sample>/webapp/WEB-INF/jsp
```

where `<sample>` is either is either `IdpSample` or `SpSample`

Images and CSS files are located in:

```
sample_src/<sample>/webapp/images
```

Rebuilding the Sample Applications

As a Java developer, you can make changes to the source code for either of the sample applications in the project under:

```
sample_src/<sample>/java
```

Then, you can build and repackage the application using `ant` commands executed from the `<sample>` directory for the `build.xml` file included in that directory. You can package either another WAR directory or a compressed WAR file (depending on deployment needs) using the following commands:

Note: For backward compatibility, the build.xml configuration file is set to use version 1.5 of the Java Development Kit (JDK). To recompile using the current JDK version, change the version number in the build.xml file.

To create a WAR *directory*:

- From the `<sample>` directory, enter:

```
ant
```

To create a WAR *file*:

- From the `<sample>` directory, enter:

```
ant war
```

In each case, the output is targeted to the `<sample>` directory.

Advanced Installation and Configuration

PingFederate system administrators may choose to override the automated PingFederate configuration and simplified deployment of the sample applications. Although the distribution is intended primarily for quick end-to-end testing and demonstration, it may also be used as a configuration exercise or to test more production-like deployments.

This section provides guidelines for alternative uses for the sample-application distribution, including:

- Configuring the Administrative Console Manually
- Using Separate IdP and SP Servers
- Deploying the Applications to Separate Servlet Containers

Important: Detailed instructions for configuring separate PingFederate servers and deploying applications in different servlet containers are beyond the scope of this document. General information is provided; however, it may not be complete or applicable for every deployment configuration.

Configuring the Administrative Console Manually

As an optional exercise, you may wish to configure the PingFederate server manually for use with the sample applications—that is, without relying on the automatic configuration supplied in `data.zip`. Because data-entry errors are likely, manual configuration is not recommended for the purpose of testing or demonstrating the sample applications. However, if you want to configure the administrative console manually for the applications, first deploy `data.zip` (described in the previous section) and look over the **Adapters** and **IdP/SP Connections** configuration in the administrative console.

Tip: Refer to the context-sensitive **Help** or see Identity Provider SSO Configuration and Service Provider SSO Configuration in the PingFederate *Administrator's Manual* for information about particular screens and links to background material.

Then, start by creating new Adapter Instances for the IdP and SP Configurations (see Installation and Setup in the Java Integration Kit *User Guide*): use Instance IDs and Names of your own choosing. For your reference, the required adapter setup values applicable to the sample applications are listed in the following tables:

> **Note**: The endpoints indicated in these tables assume the sample applications are deployed in the same servlet container running PingFederate. If you deploy the applications elsewhere, change the hostname (`localhost`) and port (as needed) in the URLs specified in these tables (see Deploying the Applications to Separate Servlet Containers on page 16).

IdP Adapter Instance

Field Name	Value
Password	Any string at least 6 characters long, containing at least one upper case letter, at least one lower case letter, and at least one number. The password is part of the exported configuration file used by the application. (See Installation and Setup in the Java Integration Kit *User Guide* for more information.) The sample applications are preconfigured to use the password: `Changeme1` Enter this value to avoid exporting and replacing the existing configuration file.
Authentication Service	https://localhost:9031/IdpSample/?cmd=sso
Logout Service*	https://localhost:9031/IdpSample/?cmd=slo
*Click Show Advanced Fields.	

SP Adapter Instance

Field Name	Value
Password	See the IdP Adapter Instance table above.
Account Link Service (Optional)*	https://localhost:9031/SpSample/?cmd=accountlink
Logout Service*	https://localhost:9031/SpSample/?cmd=slo
*Click Show Advanced Fields.	

Next, on the SP Default URLs screen, define pages for successful SSO and SLO (click **Default URLs** on the Main Menu under Application Integration Settings for the SP side). Correct values are shown in the following table:

SP Default URLs

Field	Value
For SSO URL:	https://localhost:9031/SpSample/MainPage/
For SLO URL	https://localhost:9031/SpSample/MainPage/

Finally, create new SP and IdP Connections from the Main Menu.

Tip: You can log on to the administrative console a second time in a separate browser window and refer to the `data.zip` connection configuration while creating a new connection. (Click **Next** to bypass the warning that you are already logged on.)

Replicate the connection settings deployed from `data.zip`—with *two exceptions*:

- On the General Info screens in the SP/IdP Connections task flows, use Connection IDs and Connection Names of your own choosing.
- In the IdP and SP Adapter Mapping setup, choose the Adapter Instance you created.

Be sure to activate both the IdP and SP connections on the connection Summary pages.

Important: To ensure unimpeded sample-application behavior, deactivate the connections deployed from the configuration archive (`data.zip`).

Using Separate IdP and SP Servers

Note: This configuration requires some familiarity with PingFederate and SSL certificate management.

You may also choose to deploy the `data.zip` archive on separate PingFederate servers functioning as in a specific identity-federation role. To do this, deploy the archive on each server, and then deactivate the IdP federation role on one server and the SP role on the other (on the Roles and Protocols screens under **Server Settings**).

You will then need to change the Base URL on the General Info screens for each connection to the respective partner's host and port (to update SSO/SLO partner protocol endpoints).

Finally, you may need to install and exchange new SSL server certificates on each server to re-establish trust between them.

Deploying the Applications to Separate Servlet Containers

Note: This configuration requires some familiarity with Web-application deployment and the target-container configuration, as well as SSL certificate management.

You can deploy either or both of the sample applications into their own servlet containers (such as Tomcat), rather than the container running PingFederate. If you do this, you will need to update the URLs indicated under Configuring the Administrative Console Manually on page 14.

You may also need to update the Trusted CAs in PingFederate with the container's SSL server certificate, depending on the container's SSL configuration, and ensure the container server trusts the PingFederate certificate.

Note: If you deploy either application in a separate container, update the PingFederate server hostname in the associated sample application. (For the IdP application, see Advanced IdP Deployment and SSO Options on page 8; for the SP application, see Advanced SP Deployment and SSO Options on page 11.)