PingFederate®

.NET Integration Kit

Version 2.5.1

Sample Application Startup Guide

PingIdentity®

PingFederate .NET 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 .NET 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 sample application distribution includes startup components that automatically configure PingFederate to act as both an IdP and an SP:

- The IdP server is configured to look up and send authentication information to the SP.
- The SP server is configured to forward this information to the SP sample application to create the local user session. The SP server will also be configured to send authentication requests to the IdP on behalf of local users.

System Requirements for the Sample Applications

The following software must be installed in order to run the .NET sample applications:

- PingFederate 5.x (or higher)
- OpenToken Adapter 2.5.1
- Microsoft Internet Information Services (IIS) 7
- Windows Server 2008 64-bit / 32-bit
- Microsoft .NET Framework 4.0 installed and registered with IIS
- JavaScript-enabled Web browser

Installation

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

- Two directories containing the IdP and SP sample applications (`IdpSample` and `SpSample`)

  Note: The sample applications are preconfigured with the OpenToken .NET library file (`opentoken-agent.dll`) from the `/dist` directory. Copying this file to your own application path is required before deployment. See Installation and Setup in the .NET Integration Kit *User Guide* for more details.

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

Installing the sample applications requires setting up PingFederate and then deploying the applications according to procedures for your .NET platform, 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 or connections outside the scope of this document and you want 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 the Installation and Setup instructions in the .NET Integration Kit *User Guide*.
2. Copy the `data.zip` file into:

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

   This step uses PingFederate's 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 a loopback, sending messages to and from itself. While this scenario is valid for demonstration and testing and keeps the setup simple, it is obviously not applicable to a real situation.

Alternative Manual Configuration

As an optional exercise, you may want to configure the 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. However, if you want to use the sample-application configuration as a learning tool, first deploy `data.zip` as described in the previous section and look over the configuration in the administrative console.

Then, start by creating new Adapter Instances for the IdP and SP Configurations (see Installation and Setup in the .NET 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 URL values listed assume that the IIS hosting the sample applications is on the same machine as PingFederate.

IdP Adapter Instance

Setup Field Name	Value
Password	Any string at least six characters long, containing at least one lowercase and one upper 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 .NET Integration Kit

Setup Field Name	Value
	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/IdpSample/?cmd=sso
Logout Service*	https://localhost/IdpSample/?cmd=slo
*Click **Show Advanced Fields**.	

SP Adapter Instance

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

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

> **Tip:** You can log on to the administrative console twice in separate browser windows and refer to an existing connection configuration while creating a new connection.

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.

Refer to Online Help or see OpenToken Adapter Configuration in the PingFederate *Administrator's Manual* for information about particular screens.

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`).

Deploying the Sample Applications

1. Deploy the .NET sample applications to IIS using Windows **Control Panel | Administrative Tools | Internet Information Services**, creating applications pointing to the `IdpSample` and `SpSample` directories within `<integration_kit_install_dir>/sample`. After the two applications are created, verify that the application pool is using version 4.0 of the Microsoft .NET framework and is running in Integrated Mode. In the Internet Information Services Manager, right-

click on the application and go to **Managed Application \Advanced Settings**. Make a note of the Application Pool account configured (typically DefaultAppPool). Go to Application Pool and verify that the account is using version 4.0 and running in Integrated Mode.

2. Verify that `Default.aspx` has been defined as a default content page. From the IIS Manager, click on the application and go to **Default Document**. Add `Default.aspx` if it is not found.

3. Grant ASP.NET Write access to both directories `\IdpSample\config` and `\SpSample\config`. ASP.NET has a base process identity (typically `IIS_IUSRS` on IIS 7). To grant ASP.NET access to a file, right-click the directory in Windows Explorer, choose **Properties** and select the Security tab. Highlight the appropriate ASP.NET account, IIS_IUSRS on IIS 7, and check the box for Write access. Click **Add** to add the account if it is not already listed.

Alternative Deployments

For simplicity, the sample-application deployment assumes that the IIS server hosting the sample applications is installed on the same machine as PingFederate. This allows for easier and quicker setup for testing or demonstration purposes. A more realistic scenario is to deploy the applications on a separate IIS server machine. If you do this, you will need to make these configuration changes:

- Change the URL settings of the IdP and SP adapter instances to point to the new host and port in the PingFederate administration console.
- Change the IdP and SP Default URL settings to point to the host and port of the new container in the PingFederate administration console.
- Verify that your server clocks are synchronized. If they are not synchronized, you can account for this by adjusting the Not Before Tolerance value in the OpenToken adapter configuration, which is the amount of time (in seconds) to allow for clock skew between servers. The default and recommended value is 0.
- Modify the PF Host Name property in the IdP and SP Sample Application Configuration Options screen.

Using the Sample Applications

The sample applications demonstrate single sign-on (SSO) and single logout (SLO) processing to and from your PingFederate server.

Note: The PingFederate server is configured for both the IdP and SP roles.

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 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 that application and PingFederate. The user authenticates using the local user store; no SAML use cases are invoked. However, when you click a link to a third-party application, such as your company's 401(k) provider, the IdP initiates an SSO transaction.

The IdP sample application simulates two different scenarios:

- IdP-initiated SSO
- IdP-initiated SLO

Using the IdP Sample Application

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

1. Start the PingFederate server and the IIS server.
2. In a Web browser, open the sample application:

   `https://localhost/IdpSample`
3. On the main page, click **Login Locally**.
4. On the Identity Provider Login page, 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 user name from the Login ID drop-down list and enter the same password. Click Login.
5. After logging on to the IdP sample application, the Identity Provider main page is displayed. The list below describes each option on this screen:

   - Click the Single Sign-On button to begin an IdP-initiated SSO to the SP sample application. A user session on the SP is started and you are sent to the SP sample application. Upon successful SSO, the Service Provider main page appears. See Using the SP Sample Application on page 8 for more information.
   - After SSO to the SP sample application and returning to the Identity Provider main page (`https://localhost/IdpSample`), click Single Sign-Out to initiate an SLO request to the SP. Once your user session on the remote SP is closed, your local session will be closed as well. The Identity Provider main page displays.
   - If you initiated SSO from the SP (see the next sections), then the Single Sign-Out link is operational and closes both sessions.

Using the SP Sample Application

The SP sample application simulates two different scenarios:

- SP-initiated SSO
- SP-initiated SLO

From the Service Provider Login page, you can demonstrate the scenario in which users authenticate with a local (SP) application through a remote IdP.

1. Start the PingFederate server and the IIS server.
2. In a Web browser, open the sample application:

   `https://localhost/SpSample`
3. Select an IdP connection from the drop-down list. Click **Single Sign-On** to begin an SP-initiated SSO transaction.
4. If you have already authenticated with the IdP, you are not required to re-authenticate unless either the ForceAuthn or IsPassive option is checked in the Advanced Options section of the application. Otherwise, on the Identity Provider login page, enter the following values:

   Login ID: `joe`

   Password: `test`

   (User accounts other than `joe` may also be used. You can select a different user name from the Login ID drop-down list and enter the same password.)
5. Click **Login**.

   Having completed SP-initiated SSO, you reach the Service Provider main page.
6. Click **Single Sign-Out** to begin an SP-initiated SLO transaction. Upon successful completion of this transaction, the Service Provider Login page is displayed.

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