PingFederate®

PHP Integration Kit

Version 2.5.1

Sample Application Startup Guide

PingIdentity®

PingFederate PHP Sample Application *Startup Guide*
Version 2.5.1
December, 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: **December 18, 2012**

Contents

Overview

This document provides instructions for installing, configuring, and using the sample applications bundled with the PingFederate PHP 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 a configuration data archive that automatically configures 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 is also configured to send authentication requests to the IdP on behalf of local users.

System Requirements

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

- PingFederate 6.x (or higher)
- PHP version 5.4.8
- OpenToken Adapter 2.5.1 (or higher)
- PHP-enabled Web Server with `mcrypt`, `mhash`, `zlib` and `curl` extensions
- JavaScript-enabled Web browser
- Set Correct Time zone in php.ini file (for example: `date.timezone = America/Halifax;`)

  (List of supported Time zones is available at the following location: http://php.net/manual/en/timezones.php)
- Set Appropriate Error reporting Level in php.ini file:

```
error_reporting = E_ALL & ~E_DEPRECATED & ~E_STRICT;
```

Installation

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

- Directories containing the IdP and SP sample applications and common files

  Note: The sample applications are preconfigured with the OpenToken PHP library files from the `/dist` directory. Copying these files to your own application is required before deployment.
- Directory containing configuration files for the IdP and SP sample applications.

Note: The installation script assumes the use of an Apache HTTP server on a Linux platform derived from Red Hat. The installation script has been validated on Red Hat Enterprise Linux 5.

- A `data.zip` file containing preconfigured PHP OpenToken Adapter settings necessary to support the sample applications. The URLs (such as Authentication Service and Logout Service) in IdP adapter configurations need to be updated to match your environment.

  For example: `http://<hostname>:<port>/sample/idp/idpmain.php`

Note: This configuration archive assumes the PHP server hosting the sample applications is installed on the same machine as PingFederate.

Installing the sample applications requires setting up PingFederate and then deploying the applications according to procedures for your PHP platform, as described in the following sections.

Configuring PingFederate

Use the `data.zip` file to configure PingFederate automatically.

Caution: Deploying `data.zip` will overwrite 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 instructions provided in the PHP 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 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. It automatically populates the IdP and SP OpenToken Adapter with default values. While this scenario is valid for demonstration and testing and keeps the setup simple, it is obviously not applicable to a real situation.

Manual Configuration

As an optional exercise, you may wish 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 Integrating with an IdP PingFederate Server and Integrating with an SP PingFederate Server in the PHP 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 PHP server 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 uppercase and one lowercase 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 PHP 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/sample/idp/login.php`
Logout Service*	`https://localhost/sample/idp/idpmain.php?localLogout=true`
Obfuscate Password*	Uncheck. The PHP agent does not support an encrypted password. The password is Base64 encoded.
*Click **Show Advanced Fields**.	

SP Adapter Instance

Setup Field Name	Value
Password	See the IdP Adapter Instance table above.
Authentication Service	`https://localhost/sample/sp/spmain.php`
Account Link Service (Optional)*	`https://localhost/sample/sp/accountlink.php`
Logout Service*	`https://localhost/sample/sp/spmain.php?localLogout=true`
Obfuscate Password*	Uncheck. The PHP agent does not support an encrypted password. The password is Base64 encoded.
*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 Identity Provider SSO Configuration and Service Provider SSO 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

To deploy the sample applications, refer to the procedures in one of the following sections:

Note: 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.

On Linux (Red Hat)

You can deploy the sample applications on Linux Red Hat using the included installation script. The script copies the sample applications to the Apache HTTP server `DocumentRoot`, copies configuration files, and changes file permissions and ownership. To deploy the sample applications using this script:

- Ensure that the Apache HTTP server is running.
- From the `httpd.conf` file, determine the `DocumentRoot` of the Apache HTTP server. The installation script will prompt for this information.

1. Place the `sample` directory on the server hosting the Apache HTTP server. (From here on out, the full path of this directory is referred to as `<sample_dir>`.)
2. Log on as `root` to the server hosting the Apache HTTP server.
3. At a shell command prompt, change the current directory to `<sample_dir>` and execute the installation script using the following commands:

   ```
   chmod u+x ./install.sh

   ./install.sh
   ```

4. Enter `y` (`yes`) to accept the detected Apache user.

   All commands executed within the script are "verbose" to inform the administrator of what actions are occurring.

On Other Linux Platforms or UNIX

1. Place the `sample` directory in the `DocumentRoot` of the Apache HTTP server at the root level so it is accessible via `https://<server_name>/sample`. (Hereafter, the full path is referred to as `<sample_dir>`.)
2. Move the `<sample_dir>/config` directory to some other location on the server: for security reasons, ensure the location is outside the `DocumentRoot` of the Apache server. (Hereafter, the full path of the `config` directory is referred to as `<config_dir>`.)
3. Modify the files `<sample_dir>/sp/pingidentity/opentoken/helpers/config.php` and `<sample_dir>/idp/pingidentity/opentoken/helpers/config.php` to reference the `<config_dir>` location of the respective agent configuration files.

   (For more information about the agent configuration files, see Installation and Setup in the PHP Integration Kit *User Guide*.)
4. Modify the files `<sample_dir>/idp/Const.php` and `<sample_dir>/sp/Const.php` to reference the `<config_dir>` location of the respective sample-application configuration files.

   Note: Modify only the first lines in each of the files.
5. Determine the user and/or group under which the Apache server is running and then change the ownership and permission of the sample-application configuration files:

   ```
   chown –R <apache_user> <config_dir>/*

   chmod u+w <config_dir>/*
   ```
6. Open the configuration Web pages for the SP and IdP sample applications and change the `PF Host Name` value for both sample applications to reference the PingFederate instance located on a different server:
   - `https://<server_name>/sample/idp/ConfigUI.php`
   - `https://<server_name>/sample/sp/ConfigUI.php`

On Windows

1. Place the `sample` directory in the `DocumentRoot` of the Apache HTTP server at the root level so it is accessible via `https://<server_name>/sample`. (Hereafter, the full path of the `sample` directory is referred to as `<sample_dir>`.)
2. Place the `config` directory elsewhere on the server: for security reasons, ensure the location is outside the `DocumentRoot` of the Apache HTTP server. (Hereafter, the full path of the `config` directory is referred to as `<config_dir>`.)
3. Modify the files `<sample_dir>\sp\pingidentity\opentoken\helpers\config.php` and `<sample_dir>\idp\pingidentity\opentoken\helpers\config.php` to reference the `<config_dir>` location of the respective agent configuration files.

   (For more information about the agent configuration files, see Installation and Setup in the PHP Integration Kit *User Guide*.)

4. Modify the files <sample_dir>\sp\Const.php and <sample_dir>\idp\Const.php to reference the <config_dir> location of the respective sample-application configuration files.

Note: Modify only the first lines in each of the files.

5. Use the Windows Task Manager to determine the User Name under which the Apache server is running (<apache_user>).
6. Change the security properties for the <config_dir> to allow full control to <apache_user>.
7. Open the configuration pages for the SP and IdP sample applications. Change the PF Host Name value for both sample applications to reference the PingFederate instance located on a different server:
    - https://<server_name>/sample/idp/ConfigUI.php
    - https://<server_name>/sample/sp/ConfigUI.php

Using the PHP Built-in Web Server

1. Ensure the PHP path environment variable has been updated to reference the correct location of PHP.
2. Create a directory to host the sample applications.

   (The full path of this directory is referenced hereafter as <public_html>.)
3. Place the sample directory in the directory created in the previous step.

   (The full path of the sample directory is referred to as <sample_dir>.)
4. Move the <sample_dir>/config directory to some other location on the server: for security reasons, ensure the location is outside the <public_html> directory in the PHP built-in Web Server. (The full path of the config directory is referred to as <config_dir>.)
5. Modify the files <sample_dir>/sp/pingidentity/opentoken/helpers/config.php and <sample_dir>/idp/pingidentity/opentoken/helpers/config.php to reference the <config_dir> location of the respective agent configuration files.

   (For more information about the agent configuration files, see Installation and Setup in the PHP Integration Kit *User Guide*.)
6. Modify the files <sample_dir>/idp/Const.php and <sample_dir>/sp/Const.php to reference the <config_dir> location of the respective sample-application configuration files
7. Execute the following command to start the PHP built-in Web Server from the directory containing <public_html>.

   ```
   php –s <hostname>:<port>
   ```

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.

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 and Apache HTTP servers or the PHP Built-in WebServer.
2. In a Web browser, open the sample application:

   `https://localhost/sample/idp/idpmain.php`
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.
5. Click **Login**.
6. After logging on to the IdP sample application, the Identity Provider main page is displayed. The list below describes each option on this screen:

   a. 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 for more information.

   b. After SSO to the SP sample application and returning to the Identity Provider main page (`https://localhost/sample/idp/idpmain.php`), click **Single Sign-Out** to initiate an SLO request to the SP. Once your user session on the remote SP is closed, your local user

session will be closed as well. The Identity Provider main page is displayed.

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.

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 and Apache HTTP servers or the PHP Built-in WebServer.
2. In a Web browser, open the sample application:

   `https://localhost/sample/sp/spmain.php`
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 will *not* be 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 an SP-initiated SSO, you reach the Service Provider main page.
6. Click **Single Sign-Out** to begin an SP-initiated SLO transaction (if you have configured the SP-initiated SLO profile). 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.