PingFederate®

WebSphere Integration Kit

Version 2.1.1

User Guide

Ping Identity®

PingFederate WebSphere *User Guide*
Version 2.1.1
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

The information provided in this document is provided "as is" without warranty of any kind. Ping Identity disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Ping Identity or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Ping Identity or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Document Lifetime

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

From the Web site, you may also download and refresh this PDF if it has been updated, as indicated by a change in this date: **December 17, 2012**

Contents

Introduction

The PingFederate WebSphere Integration Kit allows a Service Provider (SP) enterprise to accept SAML assertions and provide single sign-on (SSO) to WebSphere-protected applications by using the PingFederate OpenToken Adapter and IBM's Trust Association Interceptor (TAI) interface.

The Adapter uses the TAI interface to create an interceptor used for Web authentication by the WebSphere domain. HTTP clients can pass identity information to the WebSphere Application Server by using the PingFederate interceptor. This interceptor provides a way for WebSphere to use an external component to authenticate the user and then assert the identity to the WebSphere container.

This kit also supports SP-initiated SSO functionality from inside WebSphere, enabling users to obtain SSO access to applications by clicking a Web portal link that redirects to PingFederate and the OpenToken Adapter. This feature is enabled in WebSphere (see step 9 under Step One – Install the PingFederate TAI on page 7).

For more information, refer to the WebSphere server documentation (`http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp`).

Intended Audience

This document is intended for system administrators with experience in the configuration and maintenance of a WebSphere Application Server. Knowledge of networking and user-management configuration is assumed. Please consult WebSphere documentation if you encounter any difficulties in areas not directly associated with PingFederate or integration kit setup.

System Requirements

The following prerequisites must exist in order to implement the WebSphere Integration Kit:

- PingFederate 6.x (or higher) server installed with the OpenToken Adapter version 2.5.1 (or higher)
- WebSphere Application Server 8.0.x (or higher)

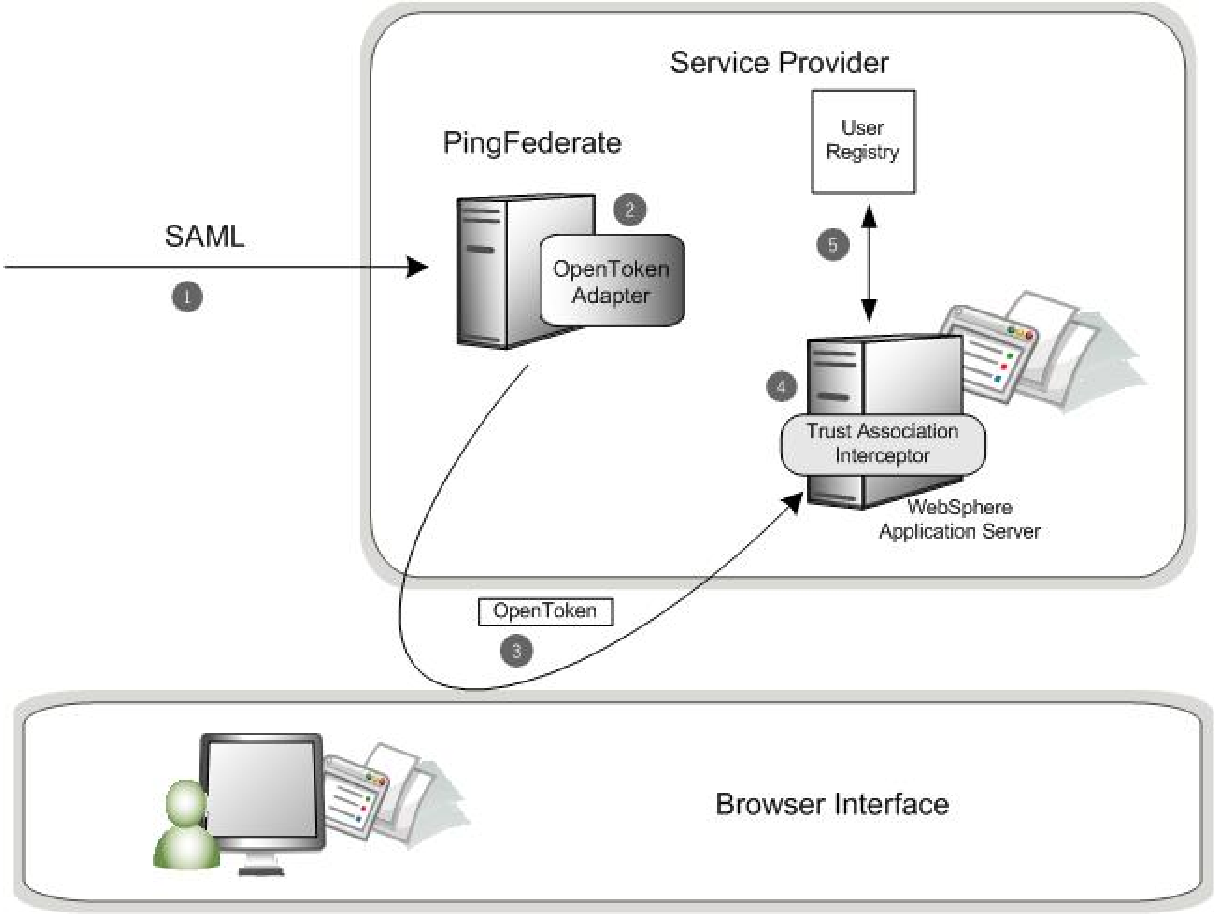
Zip Manifest

The distribution ZIP file for the WebSphere Integration Kit contains the following:

- `ReadMeFirst.pdf` – contains links to this online documentation
- `/dist` – contains libraries needed to run this adapter:
  - `opentoken-adapter-2.5.1.jar` – the OpenToken Adapter JAR file
  - `opentoken-agent-2.5.1.jar – the OpenToken Agent JAR file for the WebSphere Application Server`
  - `pf-websphere-interceptor-2.1.1.jar` – PingFederate TAI for the WebSphere Application Server

Processing Overview

The following figure illustrates a basic SSO scenario in which the PingFederate SP server leverages the OpenToken Adapter and the PingFederate TAI to allow SSO to a WebSphere domain.



Processing Steps

PingFederate server receives a SAML assertion.

1. The PingFederate SP server parses the SAML assertion and passes the user attributes to the OpenToken Adapter. The Adapter encrypts the data internally and generates an `OpenToken`.
2. A request containing the `OpenToken` is redirected to the SP application. `OpenToken` and additional attributes can be configured to transfer as part of the Request Header or as Cookies.
3. PingFederate Trust Association Interceptor for WebSphere retrieves the User ID from `OpenToken` and returns the User ID to the WebSphere Application Server.
4. WebSphere Application Server queries the registry. If the user is found, permissions to the resource are verified for the user, and a local security context is created. The user is given access to the protected resource.

Installation and Setup

Setting up the WebSphere Integration Kit involves:

- Installation and configuration of the OpenToken Adapter in PingFederate
- Configuration of the WebSphere Application Server

Installing the OpenToken Adapter and Configure PingFederate

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

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

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

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

   Note: If the adapter JAR filename indicates version 2.1 or less, also delete the supporting library `opentoken-java-1.x.jar` from same directory.

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

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

   Note: From the integration kit `/dist` directory, copy the `opentoken-agent-2.5.1.jar` into `app_server_root/lib/ext`.

4. Start or restart the PingFederate server.
5. Configure an instance of the OpenToken Adapter for your SP configuration using settings on the Instance Configuration screen as indicated in the table below.

   For detailed instructions, see Configuring the SP OpenToken Adapter in the PingFederate *Administrator's Manual.*

Option	Description
Password	Enter any password you choose.
Confirm Password	Password confirmation.

Note: In the Advanced Fields section, be sure to leave Authentication Service blank as the SP Adapter redirects a user to the protected resource directly.

On the Actions screen, click the **Download** link and then click **Export** to save the properties file to any directory on the machine running WebSphere.

Note: Additional attributes can be passed to WebSphere. See Passing Additional Attributes to WebSphere for more information.

6. Configure or modify the connection(s) to your IdP partner(s) to use the instance of the OpenToken Adapter you configured in the last steps.

Configuring the WebSphere Application Server

This section describes how to:

- Install the PingFederate Trust Association Interceptor (TAI)
- Configure WebSphere Application Server Security

Step One – Install the PingFederate TAI

Note: If this is a first-time installation of the WebSphere Integration Kit, proceed directly to step 2 in the following procedure.

If you are upgrading this integration, we strongly recommend reinstalling the OpenToken Agent and WebSphere Interceptor in the WebSphere Application Server.

1. If you are upgrading this integration:
   a. Temporarily stop your WebSphere Application Server if it is running.
   b. Remove the existing OpenToken Agent (`opentoken-agent-2.5.0.jar` or lower) and WebSphere Interceptor (`pf-websphere-interceptor-2.1.0.jar` or lower).
2. From the `/dist` folder in the directory where you unzipped the distribution file, copy the following jar files to your `app_server_root/lib/ext/` directory:
   - `opentoken-agent-2.5.1.jar`
   - `pf-websphere-interceptor-2.1.1.jar`
3. From the WebSphere Application Server administrative console, go to Security | Global security and ensure that the Enable application security checkbox and the LTPA option button are selected.
4. From the right side of the page, select **Web and SIP security** and then **Trust association**.
5. Under General Properties, select the **Enable trust association** checkbox and click **Apply**.
6. Return to the Trust association page (Web and SIP security | Trust association) and click **Interceptors**.
7. Click **New** and enter the following into the Interceptor class name box:

   ```
   com.pingidentity.adapters.websphere.sp.PingFederateTrustAssociationInterceptor
   ```

   Click **Apply** when you finish.
8. Click the link of the interceptor class name you added in the last step.
9. Provide entries for the following Name (key) and Value properties, as needed, and click **Apply** when you finish:

Name	Value
agentPropertiesFileName (required)	Path to the properties file exported when setting up the OpenToken Adapter. See Configuring the WebSphere Application Server for more information. For example: `C:/Program Files/IBM/WebSphere/AppServer/lib/ext/agent-config.txt`
enableSPSSO	The `enableSPSSO` option enables SP-initiated functionality for WebSphere. If `enableSPSSO` is set to true, the Websphere Interceptor redirects to the indicated `ssoUrl` (below) if OpenToken is not found in the request. By default, the `enableSPSSO` option is set to `false`. `(Default: false)`
ssoUrl	URL for redirect if SP-initiated SSO, required only if is (`enableSPSSO`) is enabled (above). The Websphere Interceptor redirects to the indicated `ssoUrl` if OpenToken is not found in the request. The value required is PingFederate's application endpoint to start the SSO: `http[s]://<PF_host>:<port>/sp/startSSO.ping?PartnerIdpId=<connection_id>` `For more information, see` Developer Notes.

10. Save your configuration and restart the WebSphere Application Server.

Developer Notes

To allow for deep linking for SP-initiated SSO, the Websphere Interceptor appends the target-resource URL to the ssoURL property. The `Target Resource Parameter` is how users are redirected to an URL specified in the query parameter.

Example: `http[s]://<WS_host>:<port>/<Application>/?TargetResource=<URL>`

Passing Additional Attributes to WebSphere

Additional attributes may be supplied within the `TAIResult` object via a `javax.security.auth.Subject` object. To get additional attributes, invoke `getPublicCredentials()` on the Subject object. The returned object is of type `java.lang.String`, a JSON String representation of the additional parameters.

Example String Representation:`{"not-on-or-after":"2012-06-21T15:41:44Z", "last_name":"test", "not-before":"2012-06-21T15:36:44Z", "authnContext":"urn:oasis:names:tc:SAML:2.0:ac:classes:Password", "email":"joe@pingidentity.com", "subject":"joe", "renew-until":"2012-06-22T03:36:44Z"}`

Step Two – Configure WebSphere Application Server Security

When configuring WebSphere Application Server Security, be sure to do the following:

- Define the user registry.
- Create UserIDs that are identical to UserIDs in PingFederate.

- Give users access to the protected resource.

Note: PingFederate TAI works only with protected resources.

- Install Unlimited jurisdiction policy files, if necessary.

  Due to import control restrictions, the standard Java Runtime Environment (JRE) distribution supports strong but not unlimited encryption. To use the strongest AES encryption, when permissible, download and install the appropriate version of "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy" from the IBM Security information page (`www-128.ibm.com/developerworks/java/jdk/security/60/`).

  Place these files in the JRE's `jre/lib/security/directory`.