PingFederate®

WebSphere Integration Kit

Version 2.0

User Guide

PingIdentity®

PingFederate WebSphere Integration Kit *User Guide*
Version 2.0
May, 2011

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: www.pingidentity.com

Trademarks

Disclaimer

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.

For more information, refer to the WebSphere server documentation (`http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp`).

> **Note**: To integrate with WebSphere on the IdP side, use the Java Integration Kit for the PingFederate OpenToken Adapter.

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 2.4.1 (or higher)

  See Installation and Setup on page 6 for more information.
- WebSphere Application Server 7.0.x

ZIP Manifest

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

- `GettingStarted.pdf` – contains links to this online documentation
- `/dist` – contains libraries needed for the adapter:

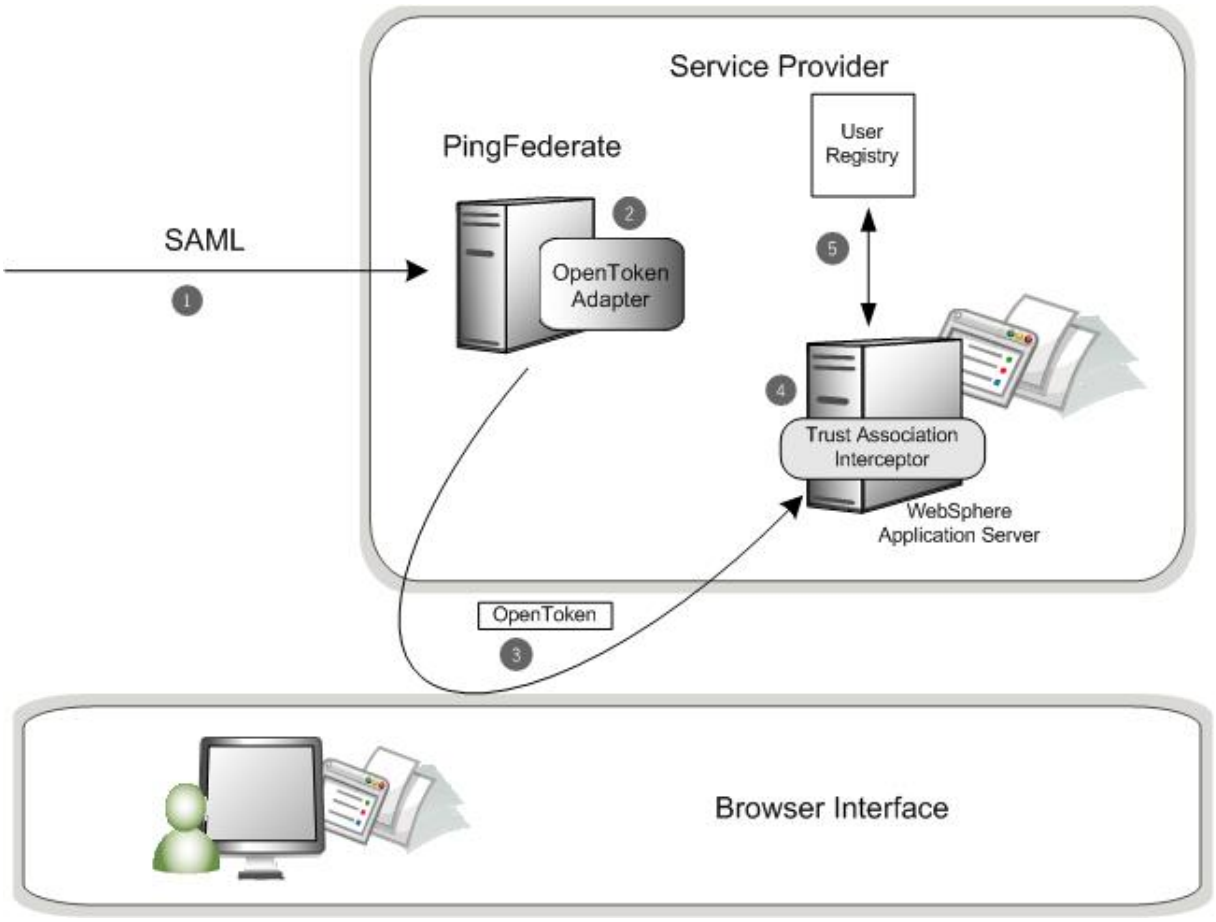
  > **Note**: The OpenToken Adapter is bundled with the PingFederate installation. Verify that you have the latest version of the `OpenToken` jar file in the directory: `<PF_install>/pingfederate/server/default/deploy`

  – `opentoken-adapter-2.4.1.jar` – the OpenToken Adapter JAR file

- `opentoken-agent-2.4.jar` – the OpenToken Agent JAR file for the WebSphere Application Server
- `pf-websphere-interceptor-2.0.jar` – PingFederate TAI for the WebSphere Application Server

Processing Overview

The following figure shows 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

1. PingFederate server receives a SAML assertion.
2. 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`.
3. 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.
4. PingFederate Trust Association Interceptor for WebSphere retrieves the User ID from `OpenToken` and returns the User ID to the WebSphere Application Server.

5. WebSphere Application Server queries the registry, but does not validate the user's password (if the User ID is not found in the registry, the assertion fails). 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

Adapter Installation and PingFederate Setup

Note: For PingFederate 6.5 and higher, it is not necessary to replace the OpenToken adapter supplied with the product—skip steps 1 and 2 in the following procedure.

To install the OpenToken Adapter and configure PingFederate:

1. From the integration kit `dist` directory, copy the file `opentoken-adapter-2.4.1.jar` into:

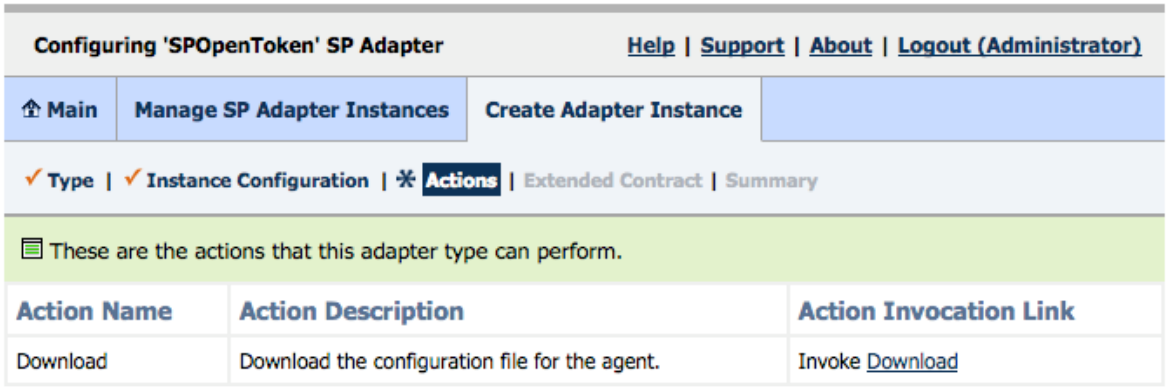
   `<PF_install>/server/default/deploy`

2. Start or restart PingFederate.
3. Create an instance of the OpenToken Adapter for your SP configuration using settings on the Instance Configuration screen as indicated in the table below. (Fields not specified are optional. For more information, 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. The SP Adapter redirects a user to the protected resource directly.

4. 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.



5. (Optional) On the Extended Contract screen, click **Next**. (For more information, see Adapter Contracts in the the PingFederate *Administrator's Manual*.)
6. Configure or modify the connection(s) to your IdP partner(s) using the instance of the OpenToken Adapter you configured in the last steps.

   For more information, see Service Provider SSO Configuration in the PingFederate *Administrator's Manual*.

WebSphere Application Server Configuration

Configuring the WebSphere Application Server for your application involves the following steps:

- Install the PingFederate TAI
- Configure WebSphere Application Server security

PingFederate Trust Association Interceptor Installation

This section provides the steps to install the TAI onto the WebSphere Application Server.

1. Store the following jar files at `app_server_root/lib/ext`:
   - `opentoken-agent-2.4.jar`
   - `pf-websphere-interceptor-2.0.jar`
2. From the WebSphere Application Server administrative console, go to Security | Global security and ensure that the Enable application security check box and the LTPA option button are selected.
3. From the right side of the page, select **Web and SIP security** and then **Trust association**.
4. Under General Properties, select the **Enable trust association** checkbox and click **Apply**.
5. Return to the Trust association page (Web and SIP security | Trust association) and click **Interceptors**.
6. Click **New** and enter the following into the Interceptor class name box:

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

   Click **Apply** when you finish.

7. Click the link of the interceptor class name you added in the last step.
8. Enter the following Name (key) and Value and click **Apply** when you finish:

Name	Value
agentPropertiesFileName	Path to the properties file exported when setting up the OpenToken Adapter (see Installation and Setup for more information). For example, `C:/Program Files/IBM/WebSphere/AppServer/lib/ext/agent-config.txt`

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

Server Security

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

- Define the user registry.
- Create users with the same User ID that is passed from the IdP side.
- 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 (`http://www-128.ibm.com/developerworks/java/jdk/security/60/`).

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