

# WebSphere Integration Kit



# Contents

<b>WebSphere Integration Kit.....</b>	<b>3</b>
<b>Overview of the SSO flow.....</b>	<b>3</b>
<b>Setup.....</b>	<b>5</b>
Install or upgrade the integration kit.....	5
Configure the WebSphere application server.....	6
Install the integration kit.....	6
Configure WebSphere application server security.....	7
<b>Release notes.....</b>	<b>8</b>
Changelog.....	8
Known issues and limitations.....	8
Download manifest.....	9

# WebSphere Integration Kit

---

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.

**i Attention:**

This integration kit has been deprecated in favor of a standard-based integration. For details, see [WebSphere Integration Guide](#). The availability of this user guide and the related product download is intended only for those who have existing solutions using this integration.

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 [Install the integration kit](#) on page 6).

For more information, see the WebSphere server documentation

## Intended audience

This document is intended for PingFederate administrators.

Before you start, you should be familiar with the following parts of the PingFederate documentation:

- [Identity provider SSO configuration](#)
- [Managing IdP adapters](#)

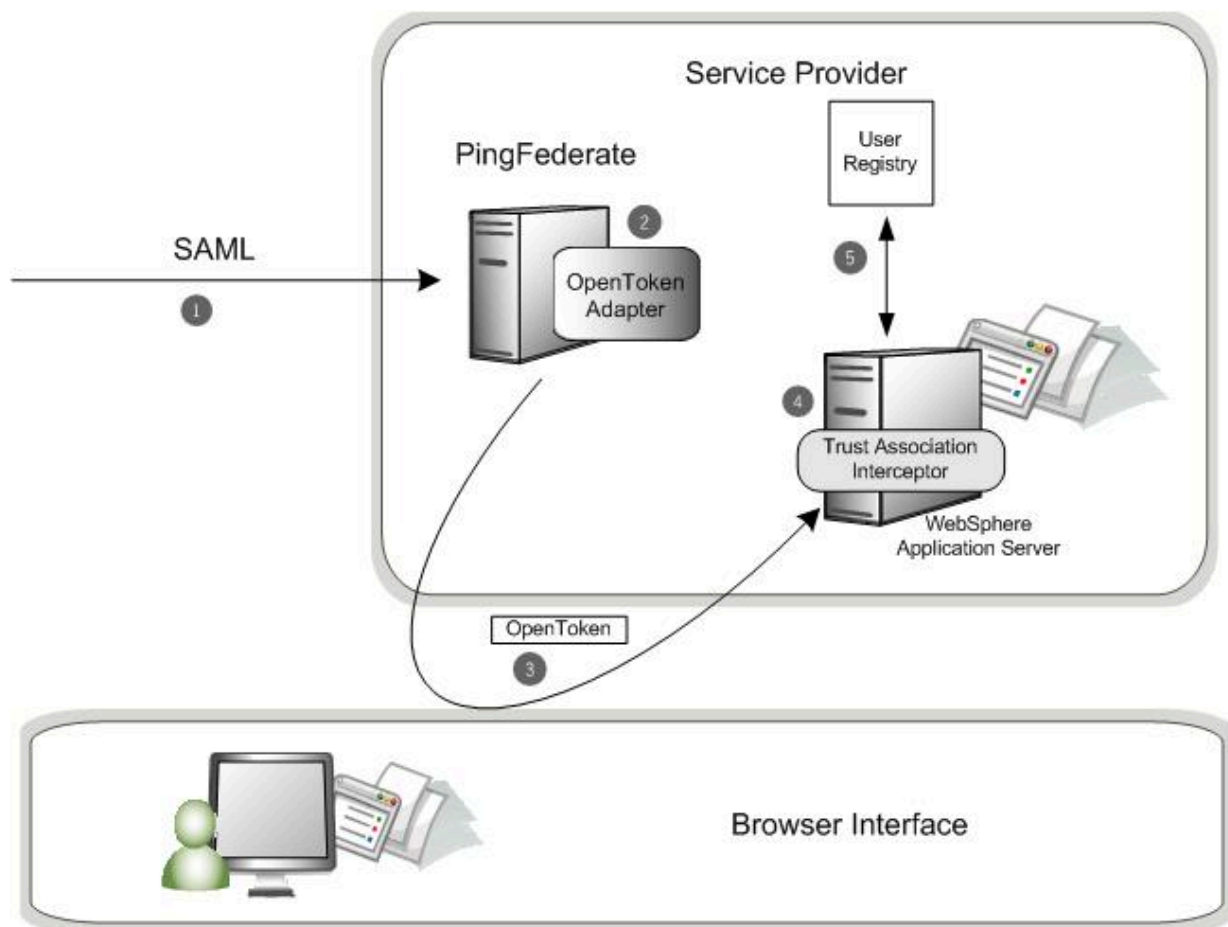
## System requirements

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

# Overview of the SSO flow

---

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

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. 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.

# Setup

---

## Install or upgrade the integration kit

---

About this task

**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.

Steps

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 [Pass additional attributes to WebSphere](#) on page 7 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.

## Configure the WebSphere application server

This section describes how to:

- [Install the integration kit](#) on page 6
- [Configure WebSphere application server security](#) on page 7

### Install the integration kit

About this task

**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.

- [Developer notes](#) on page 7
- [Pass additional attributes to WebSphere](#) on page 7

Steps

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 <a href="#">Configure the WebSphere application server</a> on page 6 for more information. For example:  C:/Program Files/IBM/WebSphere/AppServer/lib/ext/agent-config.txt

Name	Value
enableSPSSO	The <code>enableSPSSO</code> option enables SP-initiated functionality for WebSphere. If <code>enableSPSSO</code> is set to true, the Websphere Interceptor redirects to the indicated <code>ssoUrl</code> (below) if <code>OpenToken</code> is not found in the request. By default, the <code>enableSPSSO</code> option is set to false. (Default: false)
ssoUrl	URL for redirect if SP-initiated SSO, required only if is ( <code>enableSPSSO</code> ) is enabled (above). The Websphere Interceptor redirects to the indicated <code>ssoUrl</code> if <code>OpenToken</code> is not found in the request. The value required is PingFederate's application endpoint to start the SSO:  <pre>http[s]://&lt;PF_host&gt;:&lt;port&gt;/sp/startSSO.ping? PartnerIdpId=&lt;connection_id&gt;</pre> For more information, see <a href="#">Developer notes</a> on page 7.

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>`

### Pass 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"}`


## Configure WebSphere application server security

About this task

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

Steps

- 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 the "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy" from IBM.

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

## Release notes

---

### Changelog

---

#### WebSphere Integration Kit 2.1.1 – December 2012 (Current Release)

- Updated to address security issue found since the previous release.
- Added support for OpenToken 2.5.1 Adapter and the OpenToken 2.5.1 Agent

#### WebSphere Integration Kit 2.1 – July 2012

- Added support for Service Provider-initiated SSO.
- Added support for the 2.5.0 version of the OpenToken Agent and Adapter
- Added support for WebSphere Application Server v8.0
- Added support for passing additional attributes besides SAML\_subject

#### WebSphere Integration Kit 2.0 – May 2011

- Supports WebSphere Application Server v7.0
- Uses OpenToken for the encrypted token format rather than PFTOKEN

#### WebSphere Integration Kit 1.0 – March 2007

- Initial Release

### Known issues and limitations

---

#### Known Issues

- To allow for deep linking for SP-initiated SSO, the Websphere Interceptor appends the target-resource URL to the `ssoURL` property. The current implementation of the interceptor will inject a question mark after the target resource parameter URL value. Example: `http[s]://<WS_host>:<port>/<Application>/?TargetResource=<URL>?`
- To avoid a 405 POST not supported error page when accessing an application on the WebSphere Application Server that does not implement `do Post` function, the user can set the Transport Mode in their SP Adapter instance configuration to `Query Parameter` or `Cookie` rather than `Form POST`.

#### Workarounds

- In cases where the SP-initiated SSO property (`enableSPSSO`) is set to **true**, and the (`ssoURL`) property is set incorrectly, authentication through PingFederate and access to the administrative console is not possible. IdP-initiated SSO requests can be made along with the WebSphere administrative console URL as a Target Resource. This would temporarily allow access to the WebSphere administrative console to set the correct SSO URL. For example:

```
tps://<hostname>:<port>/idp/startSSO.ping?
```

```
PartnerSpId=<hostname>:default:entityId&TargetResource=http://<hostname>:<port>/ibm/console
```

#### Known Limitations

- WebSphere Integration Kit 2.1.1 does not support SLO.



## Download manifest

---

The distribution .zip archive 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