PingFederate®

OAM Integration Kit

Version 3.0

User Guide

Ping Identity®

PingFederate OAM Integration Kit *User Guide*
Version 3.0
May, 2016

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: May 20, 2016

Contents

Introduction

The PingFederate Oracle Access Manager (OAM) Integration Kit adds Identity Provider (IdP) and Service Provider (SP) Adapters to PingFederate. The OAM IdP Adapter allows an IdP enterprise to extend an existing OAM investment by using the SAML or WS-Federation protocols to expand the reach of the OAM domain to partner applications. The OAM SP Adapter allows an SP enterprise to accept SAML or WS-Federation assertions and provide SSO to OAM-protected applications.

Intended Audience

This document is intended for system administrators with experience in the configuration and maintenance of the OAM Access Server. Please consult documentation provided with your server or access-management tools if you encounter any difficulties in areas not directly associated with the PingFederate or integration-kit setups.

System Requirements

The following software must be installed in order to implement the OAM Integration Kit:

- PingFederate 8.x (or higher)
- OAM Server 11g R2
- OAM Access SDK 11.1.2.3.0 (installed on the same machine running the PingFederate server)
- OAM 11g Webgate running on Apache 2.4
- Redhat 6.7 (if using the precompiled module included in this distribution)

ZIP Manifest

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

- `ReadMeFirst.pdf`
- `/dist` – contains libraries needed to run the adapter:
  - `pf-oam-adapter-3.0.jar` – OAM Adapter `JAR` file
  - `mod_pfoam.so` – Apache 2.4 Module, compiled on Redhat 6.7
  - `PingOpenTokenAuthPlugin.jar` – OAM Authentication Plugin Plugin used for SP use case
- `/conf` – contains libraries needed to run the adapter:
  - `httpd-pfoam.conf` – Sample apache configuration file for mod_pfoam.so
  - `jps-config.xml` – OAM configuration file

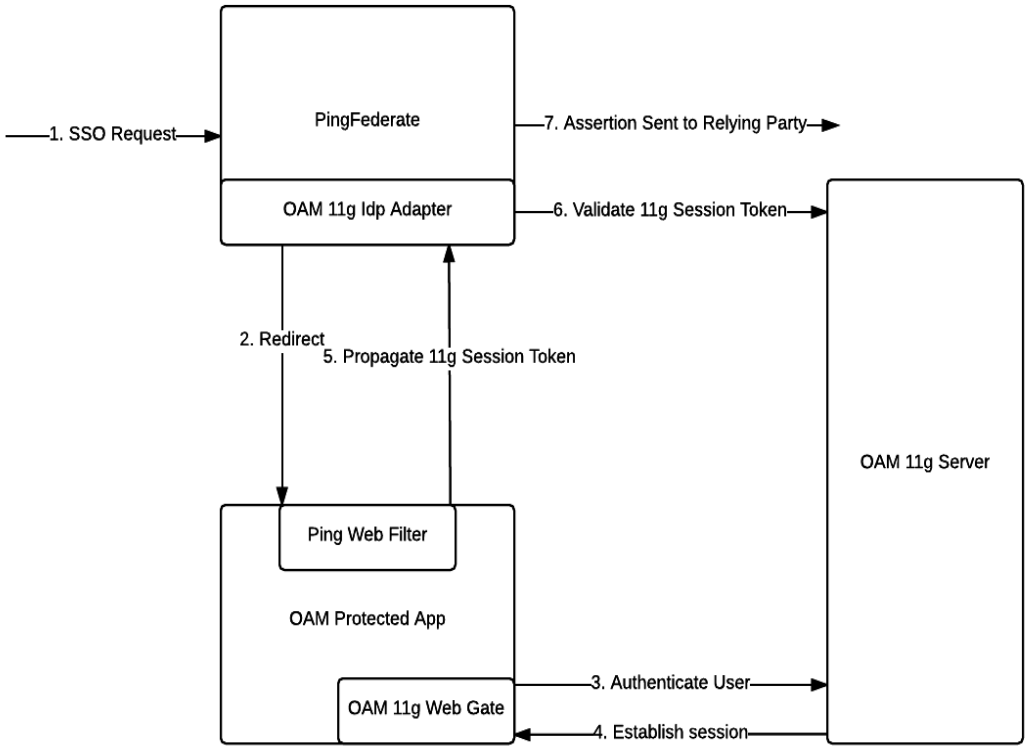
IdP Implementation

This section describes using the OAM Integration Kit as an IdP.

IdP Process Overview

The OAM IdP Adapter uses the Access Server SDK to decrypt the OAM session cookie and pass attributes to the PingFederate server. You can then add attribute values to the Attribute Contract in the PingFederate administrative console and transfer them to a partner application in a SAML assertion. (For more information, see: Creating an Attribute Contract in the PingFederate *Administrator's Manual*.)

The following figure illustrates the request flow and how the OAM IdP Adapter is used to facilitate generating a SAML WS-Federation assertion from the `ObSSOCookie`:



Processing Steps

1. User initiates single sign on through PingFederate.
2. The OAM IdP Adapter redirects the user to an OAM Protected Resource.
3. OAM Webgate authenticates the user.
4. After successful authentication an OAM 11g session is established and a host level cookie is created for the Webgate.

5. User is allowed access to the OAM protected resource at which point the Ping Web Filter intercepts this request and sends the host level OAM Session token to PingFederate.

6. OAM IdP Adapter validates the session token using Access Server APIs.

7. The user information is passed to PingFederate, which can create an assertion and send it to the required relying party (aka service provider).

OAM IdP Configuration

1. Create an OAM Apache 11g Webgate (or use an existing one).

2. Create a new folder in the PingFederate Server, to store the Webgate configuration files. This folder will henceforth be referred to as the `Agent Config Location`. This path must be specified during the PingFederate Configuration.

3. Copy the Webgate configuration files to the `Agent Config Location` folder.

Note: For more information on the Webgate configuration files, please refer to OAM documentation for configuring Webgates.

Apache Module Installation

1. Install the Apache module and configuration file from the integration kit into the Apache server:
   a. Copy `dist/mod_pfoam.so` to:

      `<apache installation>/modules`

   b. Copy `conf/httpd-pfoam.conf` to:

      `<apache installation>/conf/extra`

2. Add the following directives to the Apache server configuration file, httpd.conf:
   a. LoadModule pfoam_module modules/mod_pfoam.so

Important: This module must be loaded first, so ensure it's above all other `LoadModule` directives

---

   b. `Include conf/extra/httpd-pfoam.conf`

Apache Module Configuration

The configuration options for the Apache module are listed in the table below. Update the module's configuration file as needed: `<apache installation>/conf/extra/httpd-pfoam.conf`.

Field	Description	Default Value
OAMCookieName	Cookie name containing the OAM 11g Session Token. Example: OAMAuthnCookie_webgate.mydomain.com:80	N/A

PFResumePath	Parameter containing the relative sso url passed from PingFederate	resumePath
SessionTokenParameterName	Parameter Name used to pass OAM session token to PingFederate	OAMAuthnCookie
PFBaseUrl	Base URL for PingFederate used in conjunction with resumePath. Example: https://mydomain.com:9031	N/A

Important: Restart the Apache server after making configuration changes.

PingFederate IdP Configuration

1. Unzip the distribution ZIP file and copy the following files to the `server/default/deploy` folder in your PingFederate server installation:
   `dist/pf-oam-adapter-3.0.jar`
2. Copy the following file to the `Agent Config Location` folder, which was created in Step 2 of OAM Configuration:
   `conf/jps-config.xml`
3. Add the following to run.properties within <PF_HOME>/bin folder:
   `oracle.security.jps.config=<AGENT_CONFIG_LOCATION>/jps-config.xml`

   Important: Ensure that the `Agent Config Location` path uses forward slashes (/), as shown above.
4. Install and configure the OAM Access Server SDK. For information on the Access Server SDK, refer to your OAM documentation.

   Note: The Access Server SDK functions as a gate to the OAM Access Server and some files will need to be copied to the server where PingFederate is running.
5. Copy the following files from the Access Server SDK to the `server/default/deploy` folder in your PingFederate installation:
   - `oamasdk-api.jar`
   - opss_standalone/modules/
     - oracle.idm_11.1.1/`identitystore.jar`
     - oracle.pki_11.1.1/`oraclepki.jar`
     - oracle.jps_11.1.1/jps-ee.jar
     - oracle.jps_11.1.1/jps-api.jar
     - oracle.jps_11.1.1/jps-unsupported-api.jar
     - oracle.jps_11.1.1/jps-common.jar

– oracle.jps_11.1.1/jps-internal.jar

– oracle.osdt_11.1.1/`osdt_cert.jar`

– oracle.osdt_11.1.1/`osdt_core.jar`

– oracle.osdt_11.1.1/`osdt_xmlsec.jar`

Note: The files listed above pertain to the specified version of the OAM SDK in the System Requirements. Other versions may require different files.

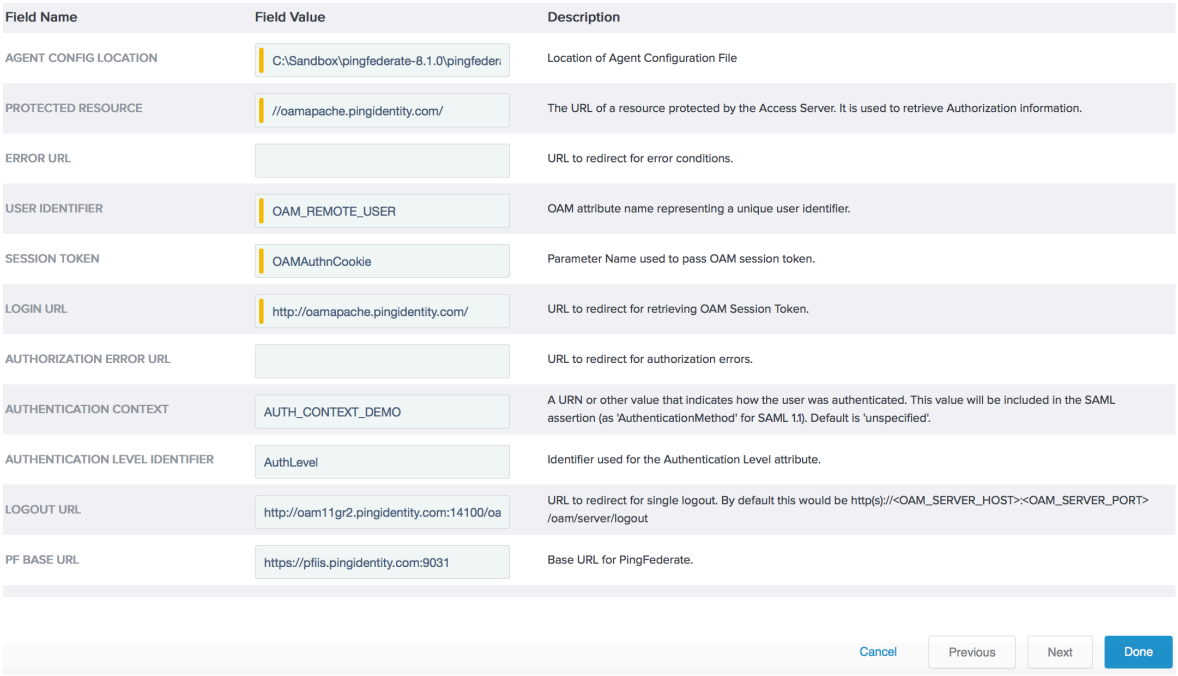
6. Start or restart the PingFederate server.

Configuring an IdP Adapter Instance

After installing the OAM Integration Kit and the Access Server SDK library, you can configure your SP connection to use an instance of the OAM Adapter. The first part of this process is configuring the adapter instance.

To configure an instance of the IdP adapter:

1. Log on to the PingFederate administrative console and click **Adapters** under IdP Configuration on the Main Menu screen.
2. On the Manage IdP Adapter Instances screen, click **Create New Instance**.
3. Enter the Adapter Name and Adapter ID. Select *OAM 11g IdP Adapter 3.0* as the Adapter Type and click **Next**.
4. On the IdP Adapter screen, enter the values for adapter configuration as described on the screen and click **Next**.



Note: The Authentication Level Identifier is taken from the user's `session token`. The default/recommended value is `authLevel`. For the user's Authentication Level to be sent in the assertion, you must add the Authentication Level Identifier to the Adapter Contract (see step 5, below).

5. Optionally, on the Extended Adapter Contract screen, you can configure additional attributes for the adapter. (See the Extending an Adapter Contract in the PingFederate *Administrator's Manual*.)

   For instance, you can use the extended adapter contract for Policy Server response-object attributes.

6. Click **Next**.

7. Select **userId** as the unique id. You may also select any extended attributes specified in the previous screen.

8. On the Summary screen, verify that the information is correct and click **Done**.

9. On the Manage Adapter Instances screen, click **Save** to complete the adapter configuration.

You can now use this adapter instance for an SP connection. For information on setting up or modifying a connection, see Managing SP Connections in the PingFederate *Administrator's Manual.*

Testing the IdP Adapter

You can test this adapter using the SP sample application that ships with PingFederate. Follow this procedure to verify adapter functions:

1. Set up PingFederate to run the SP sample application according to instructions in the Sample Application *Quick Start Guide*.

2. Configure an instance of the OAM Adapter (see OAM Configuration on page 6).

3. Reconfigure the SP connection to the sample application to use the OAM Adapter Instance.

   Delete the existing adapter instance and map the OAM Adapter instance in its place (see IdP Adapter Mapping the PingFederate *Administrator's Manual*).

Note: Use the default setting on the Assertion Mapping screen. On the Attribute Contract Fulfillment screen, map SAML_SUBJECT to the Adapter value userId. If you have extended the Adapter Contract and wish to send the extended-attribute value to the SP during SSO, you will need to add a corresponding attribute to the Attribute Contract for the SP connection. Then map this attribute to the additional adapter attribute value (for example, `authLevel`).

For any attributes in the Attribute Contract for which there are no related Adapter attributes, select Text in the Source drop-down list for each attribute and enter "test" (or any other text) in the associated text boxes.

4. On a web page protected by the OAM Access Gate, create an "SSO" link to the PingFederate `startSSO` endpoint, including the sample SP's connection ID, in the following format:

   `http[s]://<PF_host>:<port>/IdP/startSSO.ping?PartnerIdPId=<connection_id>`

   `<PF_host>` is the machine running the PingFederate server,
   `<port>` is the PingFederate port,
   `<connection_id>` is the Connection ID of the SP connection to the sample application.

5. Access the protected web page by authenticating through OAM Webgate, and click the SSO link.

   You will be logged on to the sample SP application. If you have modified the connection Attribute Contract to include Authentication Level and extended the Adapter Contract, you should see the authLevel displayed in the "User Attributes" table.

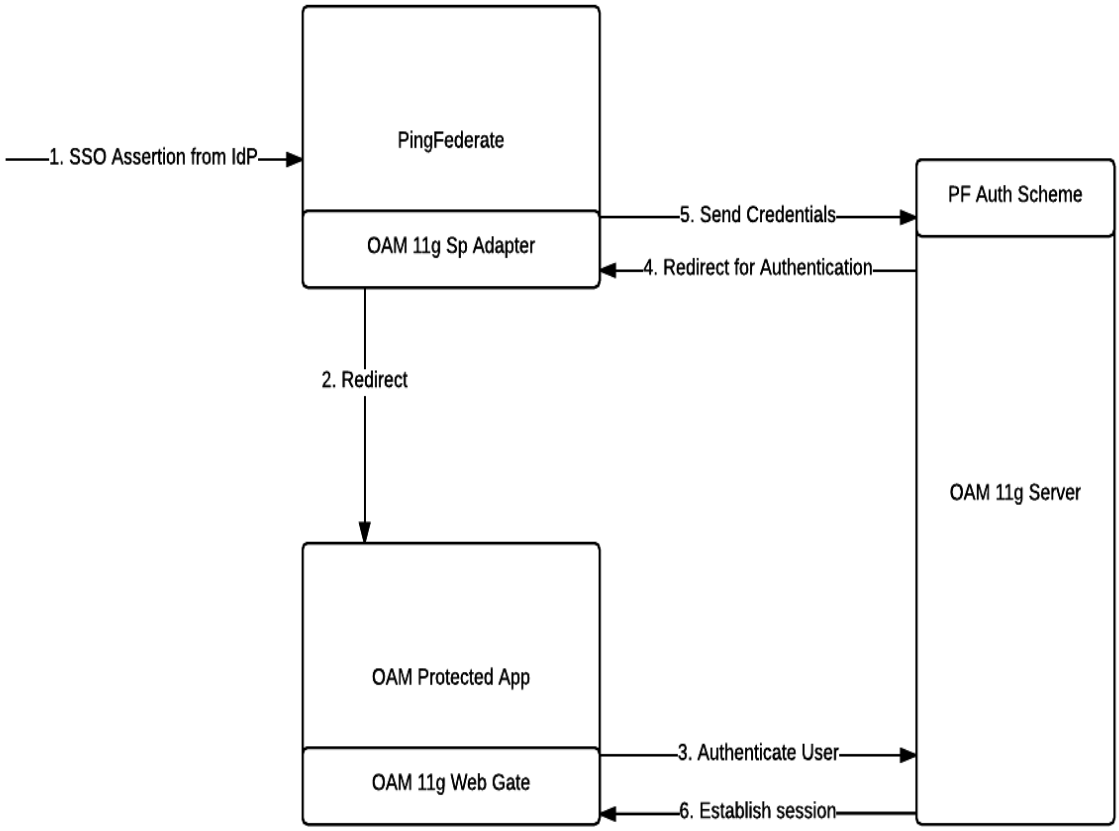
SP Implementation

This section describes using the OAM Integration Kit as an SP.

SP Process Overview

The OAM SP Adapter uses an authentication scheme deployed within Oracle Access Manager to create a session for the user.

The following figure illustrates the request flow and how the OAM SP Adapter is used to facilitate using a SAML WS-Federation assertion to create an OAM session:



Processing Steps

1. An SSO assertion is sent to PingFederate acting as an SP.
2. The OAM Sp Adapter redirects the user to an OAM Protected Resource secured with a PingFederate custom authentication scheme.
3. OAM Webgate sends a request to authenticate the user.
4. OAM Server redirects the authentication request to PingFederate.
5. OAM SP Adapter sends the required credentials back to the OAM Server.
6. The OAM Server validates the credentials and an 11g session is established.

OAM SP Configuration

1. Deploy the included authentication plug-in jar (*PingOpenTokenAuthPlugin.jar*) within OAM 11g and create an Authentication Module. For information on authentication plugins please refer to OAM Documentation for Authentication Plug-ins.
2. The authentication plugin requires the opentoken configuration file (agent-config.txt) which can be obtained through the SP adapter configuration as described in the section below . Specify the location of this file for the authentication plugin property ***opentokenConfigFile***.
3. Create or update an authentication scheme to use the plug-in deployed in Step 1. Use the following values for the authentication scheme parameters.

Parameter	**Value**
Challenge Method	Form
Challenge Redirect URL	/oam/server/
Authentication Module	Select the authentication module from Step 1.
Challenge URL	http(s)://<PF_HOST:PF_PORT>/ext/pf-oam-authn/sso.ping
Context Type	external

4. Configure an OAM Webgate to use the updated authentication scheme.

PingFederate SP Configuration

1. Unzip the distribution ZIP file and copy the following file to the `server/default/deploy` folder in your PingFederate server installation:
   `dist/pf-oam-adapter-3.0.jar`
2. Add the following to run.properties within <PF_HOME>/bin folder:

   pf.oam.ik.ssoUrl=<PF_SSO_URL>

   where PF_SSO_URL is the Sp-initiated Single sign on URL. For example: https://<PF_HOST>:<PF_PORT>/sp/startSSO.ping?PartnerIdpId=<PARTNER_ID>&TargetResource=<TARGET_RESOURCE_URL>
3. Start or restart the PingFederate Server

Configuring an SP Adapter Instance

After installing the OAM Integration Kit, you can configure your SP connection to use an instance of the OAM SP Adapter. The first part of this process is configuring the adapter instance.

To configure an instance of the SP adapter:

1. Log on to the PingFederate administrative console and click **Adapters** under SP Configuration on the Main Menu screen.
2. On the Manage SP Adapter Instances screen, click **Create New Instance**.
3. Enter the Adapter Name and Adapter ID. Select *OAM 11g SP Adapter 3.0* as the Adapter Type and click **Next**.

4. On the SP Adapter screen, enter the values for adapter configuration as described on the screen and click **Next**.

Field Name	Field Value	Description
AUTHENTICATION SERVICE	http://oam11gr2.pingidentity.com:14100/c	URL for posting credentials to OAM Server. By default this would be http(s)://<OAM_SERVER_HOST>:<OAM_SERVER_PORT>/oam/server/auth_cred_submit
ERROR URL		URL to redirect for error conditions.
LOGOUT URL	http://oam11gr2.pingidentity.com:14100/oa	URL to redirect for single logout. By default this would be http(s)://<OAM_SERVER_HOST>:<OAM_SERVER_PORT>/oam/server/logout
PF BASE URL	https://pfiis.pingidentity.com:9031	Base URL for PingFederate.
OPENTOKEN NAME	pluginSecret	The name of the request attribute that contains the OpenToken.
OPENTOKEN PASSWORD	••••••••••	The password used for encrypting opentoken.

5. Download the opentoken configuration file (agent-config.txt). This will be used during authentication plugin configuration for oam server. Click **Next.**
6. Optionally, on the Extended Adapter Contract screen, you can configure additional attributes for the adapter. (See the Extending an Adapter Contract in the PingFederate *Administrator's Manual*.)

   Note: Extended attributes are not supported in this version of OAM Integration Kit.

7. Click **Next**.
8. On the Summary screen, verify that the information is correct and click **Done**.
9. On the Manage Adapter Instances screen, click **Save** to complete the adapter configuration.

You can now use this adapter instance for an IdP connection. For information on setting up or modifying a connection, see Managing IdP Connections in the PingFederate *Administrator's Manual.*

Testing the SP Adapter

You can test this adapter using the IdP sample application that ships with PingFederate. Follow this procedure to verify adapter functions:

1. Set up PingFederate to run the IdP sample application according to instructions in the Sample Application *Quick Start Guide*.
2. Configure an instance of the OAM SP Adapter (see ConfiguringtheSPAdapter).
3. Reconfigure the IdP connection to the sample application to use the OAM Adapter instance.

   Delete the existing adapter instance for the connection and map the OAM Adapter instance in its place (see Configuring Adapter Mapping and User Lookup in the PingFederate *Administrator's Manual*).

4. From the Main Menu, click **Adapters** under My SP Configuration on the Main Menu screen.

5. Delete the Adapter Instance that was previously used by the sample-application connection.
6. Configure an OAM 11g Webgate to use the custom authentication plug-in.
7. Access am OAM protected resource within the OAM 11g Webgate from Step 6.

   You should arrive at the IdP sample application's login page.
8. Add at least one of the users in the username drop-down list to the OAM Identity Manager.

   Refer to your OAM documentation for more information.

   Alternatively, you can add users already in OAM Identity Manager to the sample application's user-properties file (see the *Quick Start Guide* for the location of this file).
9. Add the same user(s) to the Authorization Rule in the Policy Domain governing the protected Web page.
10. On the IdP sample application's login page, log in with a username managed by OAM.

    You should be allowed access to OAM-protected Web page.