Web Access Management

Contents

Overview of Web Access Management integrations

PingFederate Web Access Management Integration Kit

The PingFederate Web Access Management (WAM) Integration Kit allows developers to integrate their applications with a PingFederate server acting as either an Identity Provider (IdP) or a Service Provider (SP).

PingFederate Web Access Management Token Translator
The PingFederate Web Access Management (WAM) Token Translator provides a Token Processor and a Token Generator for use with the PingFederate WS-Trust Security Token Service (STS).

Web Access Management (WAM) Integration Kit

The PingFederate WAM Integration Kit allows developers to integrate their applications with a PingFederate server acting as either an Identity Provider (IdP) or a Service Provider (SP).

The WAM IdP Adapter allows an IdP enterprise to extend an existing investment by using the SAML or WS-Federation protocols to expand the reach of the WAM domain to partner applications. The WAM SP Adapter allows an SP enterprise to accept SAML or WS-Federation assertions and provide secure Internet Single sign-on (SSO) to applications protected by a supported WAM system.

ⓘ **Important:**

This kit is designed to work with WAM products from multiple vendors. A WAM plug-in is required to connect the integration kit with each third-party system. This kit ships with WAM plug-ins compatible with Oracle Access Manager (OAM) 11g R2, and with RSA Access Manager 6.1.

ⓘ **Important:**

The current RSA plugin does not support Adaptive Authentication. It is only qualified against Authentication Manager.

A simple software development kit (SDK) is also included to create custom WAM plug-ins for other systems. If you are creating a WAM plug-in for any third-party product other than OAM and RSA Access Manager, you must complete the tasks in the WAM plug-in SDK `README.txt` file located in the `<integration_kit_install_dir>/sdk` directory.

Intended audience

This document is intended for PingFederate administrators with experience in the configuration and maintenance of the OAM Access Server or RSA Access Manager and other WAM tools, as well as developers with experience using JAVA SDKs

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

- *Identity provider SSO configuration*
- *Managing IdP adapters*

Please consult the WAM tool documentation if you encounter any difficulties in areas not directly associated with PingFederate or the WAM Integration Kit.

System requirements

- PingFederate 6.x or later
- WAM plug-in for the desired third-party system, built and deployed per the WAM plug-in SDK documentation
- Associated vendor-supplied libraries to support the WAM plug-in you are using
- Fully functional WAM plug-ins for OAM and RSA are included in the WAM Integration Kit package
- Separate third-party Web Agent configured using the WAM server administrative software

> ⓘ **Important**:
>
> PingFederate must be running in the same domain as the third-party WAM Web Agent for the applicable WAM Server.

Setup

WAM plug-in installation for RSA

About this task

This section describes how to deploy the pre-built RSA-compatible WAM plug-in for both IdP and SP adapters.

Steps

1. The additional RSA API libraries for creating a WAM plug-in to interact with PingFederate are included in the `<integration_kit_install_dir>/dist/rsa` directory.
    - `axm-runtime-api-6.1.4.jar`
    - `jsafeFIPS-6.1.jar`
    - `jsafeJCEFIPS-6.1.jar`
2. Copy the RSA API libraries,from the `<integration_kit_install_dir>/dist/rsa` directory into:

    `<PF_install>/pingfederate/server/default/deploy` directory.
3. Copy the `pf-rsa-plugin.jar` from the `<integration_kit_install_dir>/dist/rsa` directory into:

    `<PF_install>/pingfederate/server/default/deploy`
4. Complete the *Install or upgrade the adapter* on page 6 prior to restarting the PingFederate server.

WAM plug-in installation for OAM

About this task

This section describes how to deploy the pre-built OAM-compatible WAM plug-in for both IdP and SP adapters.

For information on configuring the WAM plug-in for OAM, see *OAM-specific configuration* on page 5

Steps

1. Get the necessary OAM API library from the Oracle Identity Management Download site `(http://www.oracle.com/technetwork/middleware/downloads/oid-11g-161194.html)`:

   `oamasdk-api.jar`
2. Copy the OAM API library provided by the vendor into the `<PF_install>/pingfederate/server/default/deploy` directory.
3. (Conditional) If OAM 10g is being used, copy the `pf-oam-plugin.jar` from the `<integration_kit_install_dir>/dist/oam` directory into:

   `<PF_install>/pingfederate/server/default/deploy`
4. (Conditional) If OAM 11g is being used, copy the `pf-oam-11g-plugin.jar` from the `<integration_kit_install_dir>/dist/oam11g` directory into:

   `<PF_install>/pingfederate/server/default/deploy`
5. Complete the *Install or upgrade the adapter* on page 6 prior to restarting the PingFederate server (see next section).

OAM-specific configuration

When configuring the OAM adapter, the following values are needed:

Field	Description	Example Value
Cookie Path	Relative path in the URL where the cookie is active.	/
Protected Resource	The path (and optionally, the hostname) that defines the protected resource. This value comes from your OAM configuration.	`http://<OAM Host Identifier>/<Resource Path>`
Error URL	Optional field containing a URL used as a redirection target in the event of an error during SSO when using this adapter.	
User Identifier	HTTP header used to identify the end userID.	OAM_REMOTE_USER
Session Token Name	The name of the encrypted cookie used for SSO.	ObSSOCookie
Session Token Loggedoff Value	The value the Session Token should be set to when the user has logged out of OAM.	loggedoutcontinue

ⓘ **Note:** The above values are examples and are dependent on the OAM environment. Ask your Oracle administrator for the values required in your environment.

For more information about this configuration, see the Oracle Access Manager documentation.

Custom WAM plug-in installation

About this task

This section describes how to deploy a custom WAM plug-in for both IdP and SP adapters.

Steps

1. If you are creating a WAM plug-in for a third-party WAM product not bundled with this kit, you must complete the tasks in the WAM plug-in SDK `README.txt` file located in the `<integration_kit_install_dir>/sdk` directory.

   > ⓘ **Note:** Contact the third-party vendor support department to obtain required third-party API libraries for creating a WAM plug-in to interact with PingFederate.

2. After completing the tasks in the WAM plug-in SDK `README.txt` file, copy the resultant WAM plug-in output JAR file `pf-<WAM_TYPE>-plugin.jar` from the `<integration_kit_install_dir>SDK/lib` directory into the `<PF-install>/pingfederate/server/default/deploy` directory.

Results

The WAM Integration Kit requires a plug-in to connect with a specific WAM product (see the WAM plug-in SDK in the distribution package for sample code and more details on building the plug-in). The SDK consists of build scripts, libraries, and sample code.

> ⓘ **Note:** The WAM plug-in SDK is designed specifically to connect the WAM Integration Kit with a third-party WAM product, using an API provided by the vendor.

Install or upgrade the adapter

About this task

This section describes how to install the WAM Integration Kit for both the IdP and the SP adapters.

> ⓘ **Note:** If you have already deployed version 2.5.1 (or higher) of the OpenToken Adapter, skip steps *1* on page 6 through *3* on page 6 in the following procedure.

Steps

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

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

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

   The WAM adapter JAR file is `pf-wam-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 the same directory.

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

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

5. Copy the `pf-wam-adapter-2.0.0.jar` file from the `/dist` directory to the PingFederate directory in the previous step.

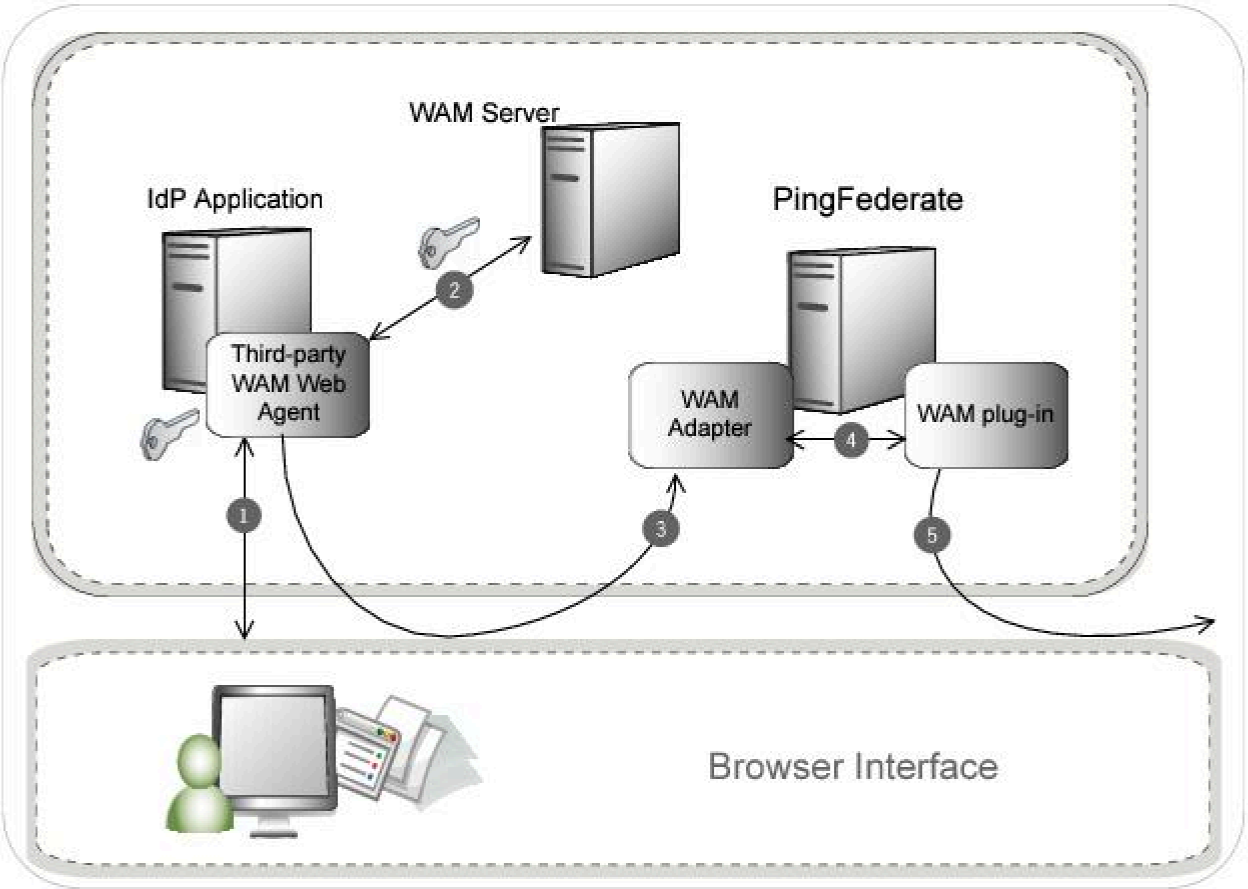
6. *If* you are running PingFederate 6.0 as a Windows service, *then*:

   Edit the `Java Library Path` section of the configuration file `pingfederate/sbin/wrapper/PingFederateService.conf`, adding the line:

   ```
   wrapper.java.library.path.append_system_path=true
   ```
7. Start the PingFederate server.

IdP process overview

The following figure illustrates the request flow and how the WAM IdP Adapter is leveraged in generating a SAML/WS-Federation assertion using a WAM session cookie.



Processing Steps

1. The user's browser attempts to access the IdP application. The third-party WAM Web Agent intercepts the request and asks for the user's identity. The user enters the requested credentials and submits the login page.
2. The WAM Server validates the user's credentials and creates a WAM session cookie. The user now has access to the application.
3. The user clicks a link that initiates an SSO transaction to the partner application. The request is redirected to the PingFederate IdP Server. The WAM session cookie generated in step *2* is included in the request.
4. The PingFederate WAM IdP Adapter uses the WAM plug-in to decrypt the WAM session cookie and then transfers the attributes to the PingFederate IdP Server. You can create an attribute contract to map the WAM session cookie and response attributes. For more information, see *Defining an attribute contract* in the PingFederate documentation.

5. The PingFederate IdP server generates a SAML/WS-Federation assertion and redirects the request, with the assertion, back through the user’s browser to the SP site.

Configuring an IdP adapter instance

This section describes how to configure the WAM Integration Kit for an identity provider (IdP).

About this task

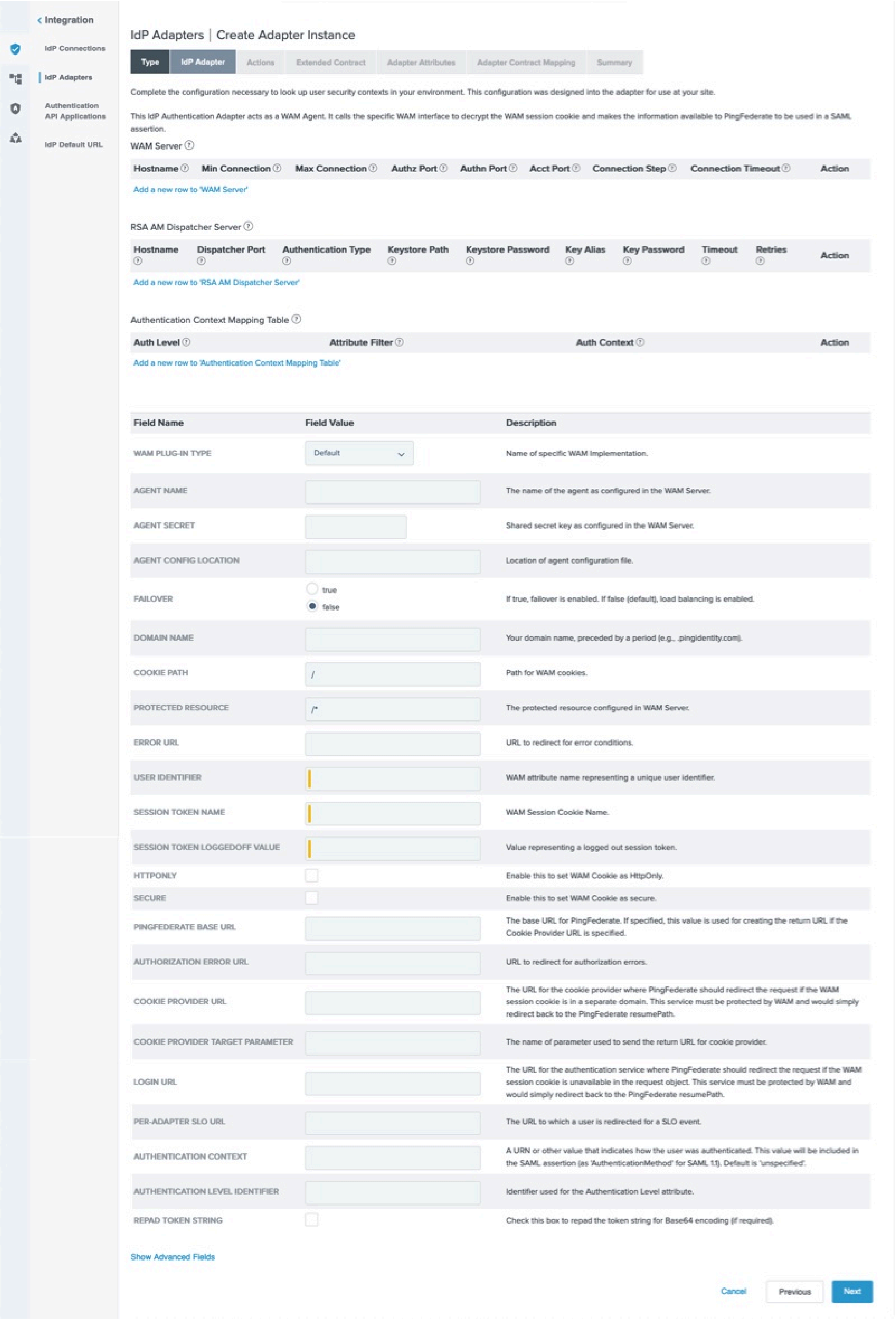
ⓘ **Important:** You must first create a third-party WAM Web Agent within your WAM tool. Several properties used to configure the agent are then used on the IdP Adapter screen discussed below. Refer to your WAM Server documentation for details on agent configuration.

Steps

1. In the PingFederate administrative console, create a new IdP adapter instance:
   - For PingFederate 10.1 or later: go to **Authentication**# **Integration**# **IdP Adapters**. Click **Create New Instance**.
   - For PingFederate 10.0 or earlier: go to **Identity Provider**# **Adapters**. Click **Create New Instance**.

2. On the **Type** tab, set the basic adapter instance attributes.
    a. In the **Instance Name** field, enter a name for the adapter instance.
    b. In the **Instance ID** field, enter a unique identifier for the adapter instance.
    c. From the **Type** list, select **WAM IdP Adapter**. Click **Next**.

> ⓘ **Note:** If you are configuring the adapter for a custom plug-in (not bundled with this kit), then continue to step *5*. If you are configuring the RSA AM Dispatcher server, continue with step *6*. If you are configuring OAM, continue at step *7*.



IdP Adapters | Create Adapter Instance

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

This IdP Authentication Adapter acts as a WAM Agent. It calls the specific WAM interface to decrypt the WAM session cookie and makes the information available to PingFederate to be used in a SAML assertion.

WAM Server ⓘ

Hostname ⓘ	Min Connection ⓘ	Max Connection ⓘ	Authz Port ⓘ	Authn Port ⓘ	Acct Port ⓘ	Connection Step ⓘ	Connection Timeout ⓘ	Action

Add a new row to 'WAM Server'

RSA AM Dispatcher Server ⓘ

Hostname ⓘ	Dispatcher Port ⓘ	Authentication Type ⓘ	Keystore Path ⓘ	Keystore Password ⓘ	Key Alias ⓘ	Key Password ⓘ	Timeout ⓘ	Retries ⓘ	Action

Add a new row to 'RSA AM Dispatcher Server'

Authentication Context Mapping Table ⓘ

Auth Level ⓘ	Attribute Filter ⓘ	Auth Context ⓘ	Action

Add a new row to 'Authentication Context Mapping Table'

Field Name	Field Value	Description
WAM PLUG-IN TYPE	Default	Name of specific WAM implementation.
AGENT NAME		The name of the agent as configured in the WAM Server.
AGENT SECRET		Shared secret key as configured in the WAM Server.
AGENT CONFIG LOCATION		Location of agent configuration file.
FAILOVER	○ true ● false	If true, failover is enabled. If false (default), load balancing is enabled.
DOMAIN NAME		Your domain name, preceded by a period (e.g., .pingidentity.com).
COOKIE PATH	/	Path for WAM cookies.
PROTECTED RESOURCE	/*	The protected resource configured in WAM Server.
ERROR URL		URL to redirect for error conditions.
USER IDENTIFIER		WAM attribute name representing a unique user identifier.
SESSION TOKEN NAME		WAM Session Cookie Name.
SESSION TOKEN LOGGEDOFF VALUE		Value representing a logged out session token.
HTTPONLY	□	Enable this to set WAM Cookie as HttpOnly.
SECURE	□	Enable this to set WAM Cookie as secure.
PINGFEDERATE BASE URL		The base URL for PingFederate. If specified, this value is used for creating the return URL if the Cookie Provider URL is specified.
AUTHORIZATION ERROR URL		URL to redirect for authorization errors.
COOKIE PROVIDER URL		The URL for the cookie provider where PingFederate should redirect the request if the WAM session cookie is in a separate domain. This service must be protected by WAM and would simply redirect back to the PingFederate resumePath.
COOKIE PROVIDER TARGET PARAMETER		The name of parameter used to send the return URL for cookie provider.
LOGIN URL		The URL for the authentication service where PingFederate should redirect the request if the WAM session cookie is unavailable in the request object. This service must be protected by WAM and would simply redirect back to the PingFederate resumePath.
PER-ADAPTER SLO URL		The URL to which a user is redirected for a SLO event.
AUTHENTICATION CONTEXT		A URN or other value that indicates how the user was authenticated. This value will be included in the SAML assertion (as 'AuthenticationMethod' for SAML 1.1). Default is 'unspecified'.
AUTHENTICATION LEVEL IDENTIFIER		Identifier used for the Authentication Level attribute.
REPAD TOKEN STRING	□	Check this box to repad the token string for Base64 encoding (if required).

Show Advanced Fields

3. (Only for custom plug-ins for WAM servers other than OAM or RSA) On the IdP Adapter screen, click **Add a new row to ‘WAM Server’** and provide the following information into the table:

    a. Enter the Hostname or the IP address where the WAM server is running.

    b. Specify the remaining WAM server values required for your configuration.

    c. Click **Update** in the Action column.

    d. Repeat this step as needed for additional custom WAM plug-ins.

    Skip the next step.

4. (Only for the RSA bundled plug-in) On the IdP Adapter screen, click **Add a new row to ‘RSA AM Dispatcher Server’** and provide the following information in the table:

    ⓘ **Note:** You must specify at least one RSA AM Dispatcher Server.

    a. Enter the Hostname or the IP address and the (optional) Dispatcher Port where the RSA AM Dispatcher server is running.

    ⓘ **Note:** You must specify the authentication method that is used by the dispatcher server. If you have specified multiple dispatcher servers, each server can have individual authentication methods.

    b. Specify the Authentication Type used by the RSA Dispatcher Server.

    - **Clear** – clear text, no encryption
    - **Anon** – anonymous SSL, SSL encryption only
    - **Auth** – mutually authenticated SSL, SSL encryption with certificate-based encryption

    c. If the selected Authentication Type is **Auth**, you must specify the following RSA server values:

    - **Keystore Path** – String filename of the private Keystore file (PKCS12 only)
    - **Keystore Password** – password for the private Keystore
    - **Key Alias** – the alias to your private key in the Keystore
    - **Key Password** – private Key Password for Keystore

    d. Optional: Specify the Timeout value required for your configuration.

    e. Click **Update** in the Action column.

    f. Repeat this step as needed for additional RSA Servers.

5. (Only for custom plug-ins for WAM servers and the OAM bundled plug-in) On the IdP Adapter screen, click **Add a new row to ‘Authentication Context Mapping Table’** and provide the following information into the table:

    - Authentication Level – A specific value for a WAM system indicating the level of authentication an end-user has gone through.
    - Authentication Context – This is part of the SAML assertion.

    Click **Update** in the Action column. Repeat this step as needed.

6. Provide entries on the IdP Adapter screen, as described on the screen and in the table below.

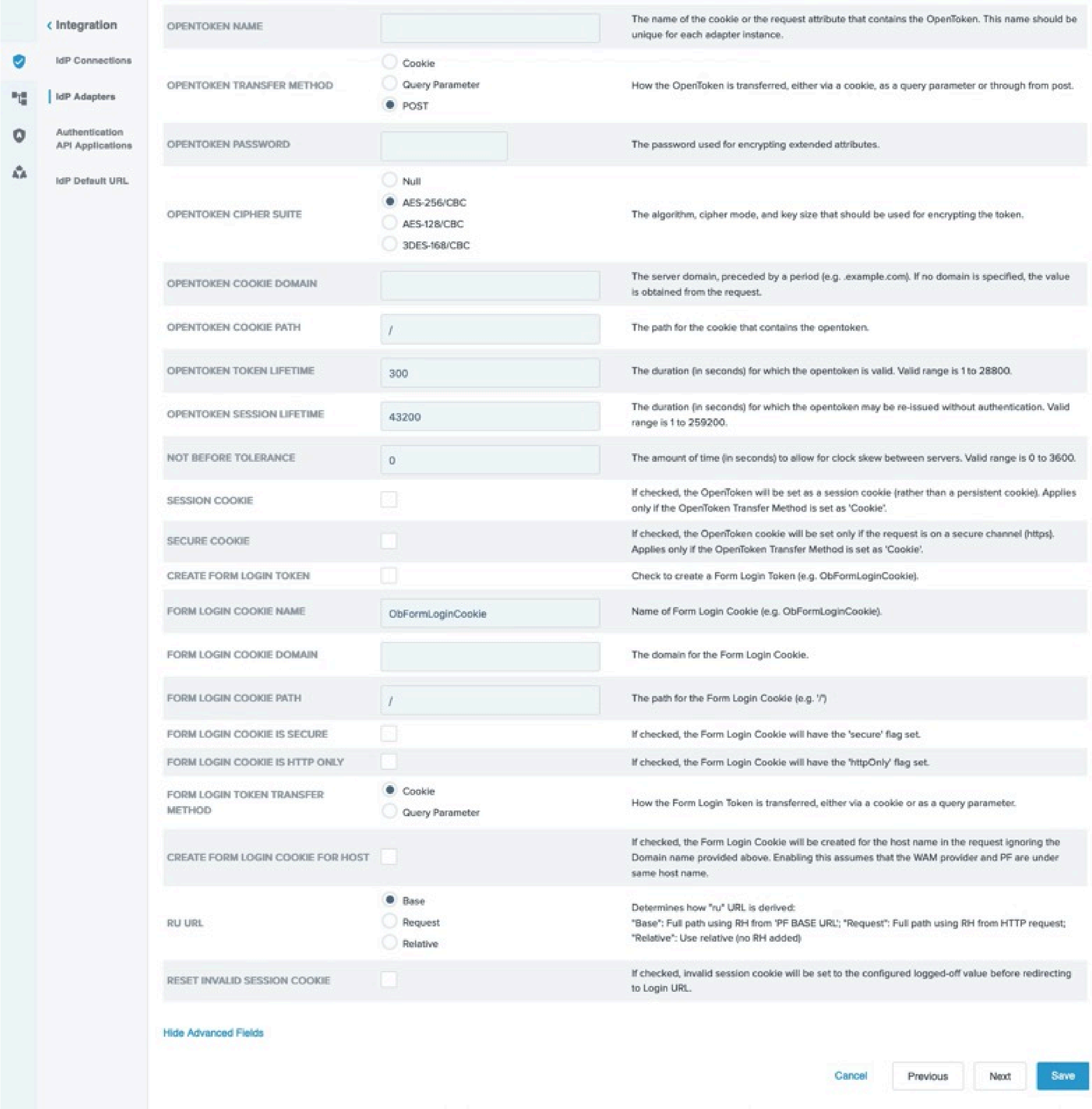
ⓘ **Note:** The selected WAM Plug-in Type may override optional/required fields. For example, if the selected WAM Plug-in Type is OAM, the Agent Config Location becomes a required field. Leaving this field blank generates an error message.

Field	Description
WAM Plug-in Type	Class name for the specific WAM implementation. **Note:** The WAM Plug-in Type determines optional/required fields.
Agent Name	This value must match the value used when the third-party WAM Web Agent was configured.

Field	Description
Agent Secret	This value must match the value used when the third-party WAM Web Agent was configured.
Agent Config Location	Required for OAM, this value must contain the full path to an XML network-configuration file generated by the access-management system.
Failover	The default is false, indicating load balancing is enabled and user-session states and configuration data are shared among multiple WAM servers. Select **true** to enable failover, indicating that when one server fails, the next server is used.
Domain Name	Enter the fully-qualified domain name (Cookie Domain where the WAM session cookie is stored), preceded by a period. For example: `.pingidentity.com`
Cookie Path	(Required) The root (/) directory is the default. Specify a different path for the WAM session cookie location, if necessary. Refer to your WAM Server documentation for details.
Protected Resource	(Required) All files in the root directory (/*) is the default. Specify a different path to the resources in the protected realm, if necessary.
Error URL	Enter a URL for redirecting the user if there are errors: for example, incorrect parameters in the link. This URL may contain query parameters. The URL has an `errorMessage` query parameter appended to it, which contains a brief description of the error that occurred. The error page can optionally display this message on the screen to provide guidance on remedying the problem. When employing the `errorMessage` query parameter in a custom error page, adhere to Web-application security best practices to guard against common content injection vulnerabilities. If no URL is specified, the appropriate default error landing page appears. For more information, see *Customizable user-facing Screens* in the PingFederate documentation. **Note:** If you define an error redirect URL, errors are sent to the error URL as well as logged in the PingFederate server log, but are not logged to the PingFederate audit log.
User Identifier	(Required) Defines which attribute that is parsed from the WAM session cookie is the user identifier for use in the assertion.
Session Token Name	(Required) WAM session cookie name.
Session Token LOGGEDOFF Value	(Required) Value representing a logged-out session token.
HTTP Only	Enable this option to set the WAM Session Cookie as HTTP Only. If this option is enabled, the browser will send the WAM Session Cookie via HTTP or HTTPS.
Secure	Enable this option to set the WAM Session Cookie as secure. If this option is enabled, the browser will send the WAM Session Cookie via HTTPS only.

Field	Description
PingFederate Base URL	The base URL for PingFederate. If specified, this value is used for creating the return URL if the Cookie Provider URL is used.
Authorization Error URL	URL to redirect for authorization errors.
Cookie Provider URL	The URL for the cookie provider where PingFederate should redirect the request if the WAM session cookie is in a separate domain. This service must be protected by the WAM server and would simply redirect back to the PingFederate `resumePath`.
Cookie Provider Target Parameter	The name of the parameter used to send the return URL for the cookie provider.
Login URL	An optional URL for the authentication service. If the WAM session cookie is not found in the request, PingFederate redirects the request to the URL page along with the relative `resumePath`. This service must be protected by the WAM Agent.
Per-Adapter SLO URL	If a URL is entered into this field, it will be used as the redirect target during SLO for this adapter instance, instead of the default value from Pingfederate.
Authentication Context	This may be any value agreed upon with your SP partner that indicates how the user was authenticated. The value is included in the SAML assertion. Standard URIs are defined in the SAML specifications. For details, see the *Authentication Context for the OASIS Security Assertion Markup Language(SAML) V2.0* PDF on the OASIS site.
Authentication Level Identifier	Identifier used for the Authentication Level attribute.

Field	Description
Repad Token String	Enable this to pad the incoming session token (if required).



OPENTOKEN NAME		The name of the cookie or the request attribute that contains the OpenToken. This name should be unique for each adapter instance.
OPENTOKEN TRANSFER METHOD	○ Cookie ○ Query Parameter ● POST	How the OpenToken is transferred, either via a cookie, as a query parameter or through from post.
OPENTOKEN PASSWORD		The password used for encrypting extended attributes.
OPENTOKEN CIPHER SUITE	○ Null ● AES-256/CBC ○ AES-128/CBC ○ 3DES-168/CBC	The algorithm, cipher mode, and key size that should be used for encrypting the token.
OPENTOKEN COOKIE DOMAIN		The server domain, preceded by a period (e.g. .example.com). If no domain is specified, the value is obtained from the request.
OPENTOKEN COOKIE PATH	/	The path for the cookie that contains the opentoken.
OPENTOKEN TOKEN LIFETIME	300	The duration (in seconds) for which the opentoken is valid. Valid range is 1 to 28800.
OPENTOKEN SESSION LIFETIME	43200	The duration (in seconds) for which the opentoken may be re-issued without authentication. Valid range is 1 to 259200.
NOT BEFORE TOLERANCE	0	The amount of time (in seconds) to allow for clock skew between servers. Valid range is 0 to 3600.
SESSION COOKIE	□	If checked, the OpenToken will be set as a session cookie (rather than a persistent cookie). Applies only if the OpenToken Transfer Method is set as 'Cookie'.
SECURE COOKIE	□	If checked, the OpenToken cookie will be set only if the request is on a secure channel (https). Applies only if the OpenToken Transfer Method is set as 'Cookie'.
CREATE FORM LOGIN TOKEN	□	Check to create a Form Login Token (e.g. ObFormLoginCookie).
FORM LOGIN COOKIE NAME	ObFormLoginCookie	Name of Form Login Cookie (e.g. ObFormLoginCookie).
FORM LOGIN COOKIE DOMAIN		The domain for the Form Login Cookie.
FORM LOGIN COOKIE PATH	/	The path for the Form Login Cookie (e.g. '/')
FORM LOGIN COOKIE IS SECURE	□	If checked, the Form Login Cookie will have the 'secure' flag set.
FORM LOGIN COOKIE IS HTTP ONLY	□	If checked, the Form Login Cookie will have the 'httpOnly' flag set.
FORM LOGIN TOKEN TRANSFER METHOD	● Cookie ○ Query Parameter	How the Form Login Token is transferred, either via a cookie or as a query parameter.
CREATE FORM LOGIN COOKIE FOR HOST	□	If checked, the Form Login Cookie will be created for the host name in the request ignoring the Domain name provided above. Enabling this assumes that the WAM provider and PF are under same host name.
RU URL	● Base ○ Request ○ Relative	Determines how "ru" URL is derived: "Base": Full path using RH from 'PF BASE URL'; "Request": Full path using RH from HTTP request; "Relative": Use relative (no RH added)
RESET INVALID SESSION COOKIE	□	If checked, invalid session cookie will be set to the configured logged-off value before redirecting to Login URL.

7. Optional: Click **Show Advanced Fields** to specify OpenToken configuration values or settings, depending on your network configuration and other requirements at your site. The Advanced Fields

also contain fields for configuring tokens capturing the original request information if necessary. This functionality is based on the ObFormLoginCookie from OAM.

> ⓘ **Note:** If you want to configure the use of OpenToken as part of the WAM adapter configuration, then complete the fields as described on the screen and in the table below.

Field	Description
OpenToken Name	The name of the cookie or the request attribute that contains the OpenToken. This name should be unique for each adapter instance.
OpenToken Transfer Method	How the OpenToken is transferred, either via a cookie, as a query parameter, or through Form Post.
OpenToken Password	The password used for encrypting extended attributes. Note: This is also used for generating the configuration file used by the OpenToken agent, and is thus required even if the Cipher Suite is set to NULL.
OpenToken Cipher Suite	The algorithm, cipher mode, and key size that should be used for encrypting the token.
OpenToken Cookie Domain	The server domain, preceded by a period (e.g. .example.com). If no domain is specified, the value is obtained from the request.
OpenToken Cookie Path	The path for the cookie that contains the OpenToken.
OpenToken Token Lifetime	The duration (in seconds) for which the OpenToken is valid. Range is 1 to 28800.
OpenToken Session Lifetime	The duration (in seconds) for which the OpenToken may be re-issued without authentication. Range is 1 to 259200.
Not Before Tolerance	The amount of time (in seconds) to allow for clock skew between servers. Range is 0 to 3600.
Session Cookie	If checked, the OpenToken cookie will be set as a session cookie (rather than a persistent cookie). Applies only if the OpenToken Transfer Method is set as ‘Cookie’.
Secure Cookie	If checked, the OpenToken cookie will be set only if the requests is on a secure channel (HTTPS). Applies only if the OpenToken Transfer Method is set as 'Cookie'.
Create Form Login Token	If checked, a Token will be created containing the information needed to retain the original request information if a redirect to a form authentication page is required. The token contents are implemented based on the requirements of the ObFormLoginCookie from OAM.
Form Login Cookie Name	The name to be given to the created Form Login Cookie (Ex: ObFormLoginCookie)
Form Login Cookie Domain	The server domain, preceded by a period (e.g. .example.com).
Form Login Cookie Path	The path for the cookie that contains the Form Login Cookie.
Form Login Cookie is Secure	Set the “secure” flag on the Form Login Cookie.
Form Login Cookie is HTTP Only	Set the “httpOnly” flag on the Form Login Cookie.

Field	Description
Form Login Token Transfer Method	How the Form Login Token is transferred, either via a cookie or as a query parameter.
Create Form Login Cookie for Host	If checked, the form login Cookie will be created for the host name in the request ignoring the Domain name provided above.
RU URL	Determines how "ru" URL is derived: "Base": Full path using RH from 'PF BASE URL'; "Request": Full path using RH from HTTP request; "Relative": Use relative (no RH added)
Reset Invalid Session Cookie	If checked, invalid session cookie will be set to the configured logged-off value before redirecting to Login URL.

8. Click **Next**.
9. On the **Actions** screen, click the **Test Connection** link to validate the WAM configuration.

> **Note:** If you're using an OpenToken Adapter Configuration, click the **Invoke Download** link and then click **Export** to download the `agent-config.txt` properties to a directory that is readable by the WAM Web Agent.

10. On the **Extended Contract** tab, add any attributes that you want to include in the contract. Click **Next**.
11. On the **Adapter Attributes** screen, select **userId** or **wamSessionToken** under **Pseudonym**. You may also select any extended attributes specified on the previous screen. Click **Next**.

    For help, see *Set pseudonym and masking options* in the PingFederate documentation. Click **Next**.
12. On the **Summary** tab, check and save your configuration:
    - For PingFederate 10.1 or later: click **Save**.
    - For PingFederate 10.0 or earlier: click **Done**. On the **Manage IdP Adapter Instances** tab, click **Save**.

IdP deployment note

The adapter configuration supports a “login URL” parameter. If the WAM session cookie is not found in the request, then the PingFederate server redirects the request to the URL page along with the relative `resumePath`, which is generated from PingFederate and intended for asynchronous communication between the adapter and the external application. (The state is saved in PingFederate, and processing is resumed when the application redirects to the `resumePath`.)

The login URL page can authenticate the user and redirect the request back to PingFederate. An example of a JSP code snippet for redirecting the request is shown below.

```
<%
    String resumePath = request.getParameter("resumePath");
      if(resumePath != null) {
        resumePath =
            <PingFed_URL>
          + resumePath;
        response.sendRedirect(resumePath);
       }
%>
```

where `<PingFed_URL>` is the fully-qualified URL of the PingFederate server.

Test the IdP adapter

About this task
You can test this adapter using the samples applications that are included in the Java Integration Kit.

Follow this procedure to verify adapter functions:

Steps

1. Download the Java Integration kit from the *PingFederate server add-ons page*.
2. Complete the steps in *Sample application setup* in the Java Integration Kit documentation to set up an IdP application.
3. Configure an instance of the WAM Adapter.
4. Reconfigure the SP connection to use the WAM Adapter instance.

   Delete the existing adapter instance and map the WAM Adapter instance in its place. For details, see *Managing Mappings* in the PingFederate documentation.
5. On a web page protected by the third-party WAM web Agent, 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
   ```

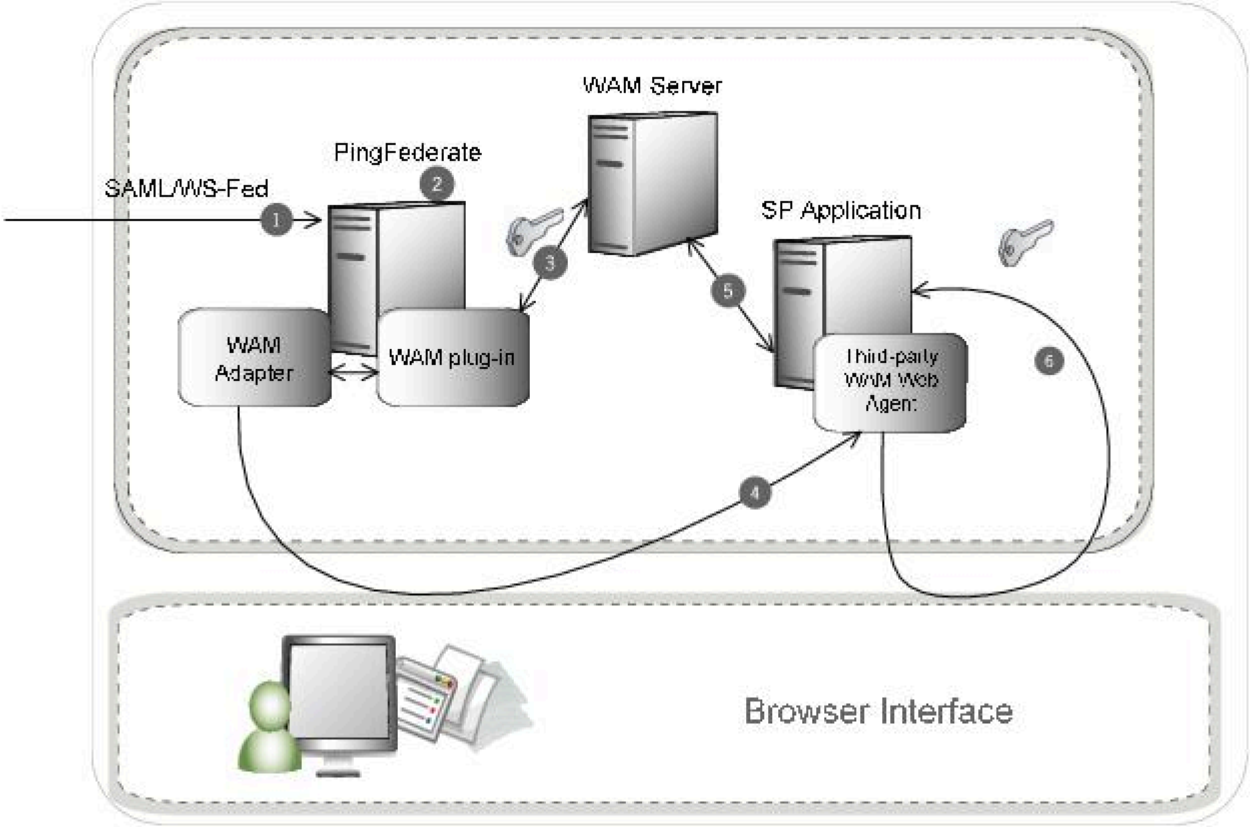
   ```
   ?PartnerSpId=<connection_id>
   ```

   where:

   - `<PF_host>` is the machine running the PingFederate server.
   - `<port>` is the PingFederate port (default value: `9031`).
   - `<connection_id>` is the Connection ID of the SP connection.
6. Access the protected web page by authenticating through the WAM web Agent and click the SSO link.
7. You are logged on to the Java sample application.

SP process overview

The following figure illustrates the request flow and how the WAM SP Adapter leverages a SAML/WS-Federation assertion to create a WAM session cookie.



Processing Steps

1. The PingFederate SP server receives a SAML/WS-Federation assertion from the IdP.
2. PingFederate parses the assertion.
3. The WAM SP Adapter uses the WAM plug-in to create a WAM session cookie and embeds the cookie in the response.
4. A request containing the WAM session cookie is redirected to the browser.
5. The request is then redirected to the SP Application, which is protected by the third-party WAM Web Agent.
6. The third-party WAM Web Agent intercepts the request, extracts and validates the WAM session cookie, and allows access to the application.

Configuring an SP adapter instance

This section describes how to configure the WAM Integration Kit for a service provider (SP).

About this task

This section describes how to configure the WAM Integration Kit for an SP. If you are using OAM please see *Creating a Custom Authentication Scheme for OAM* on page 27 for configuration information.

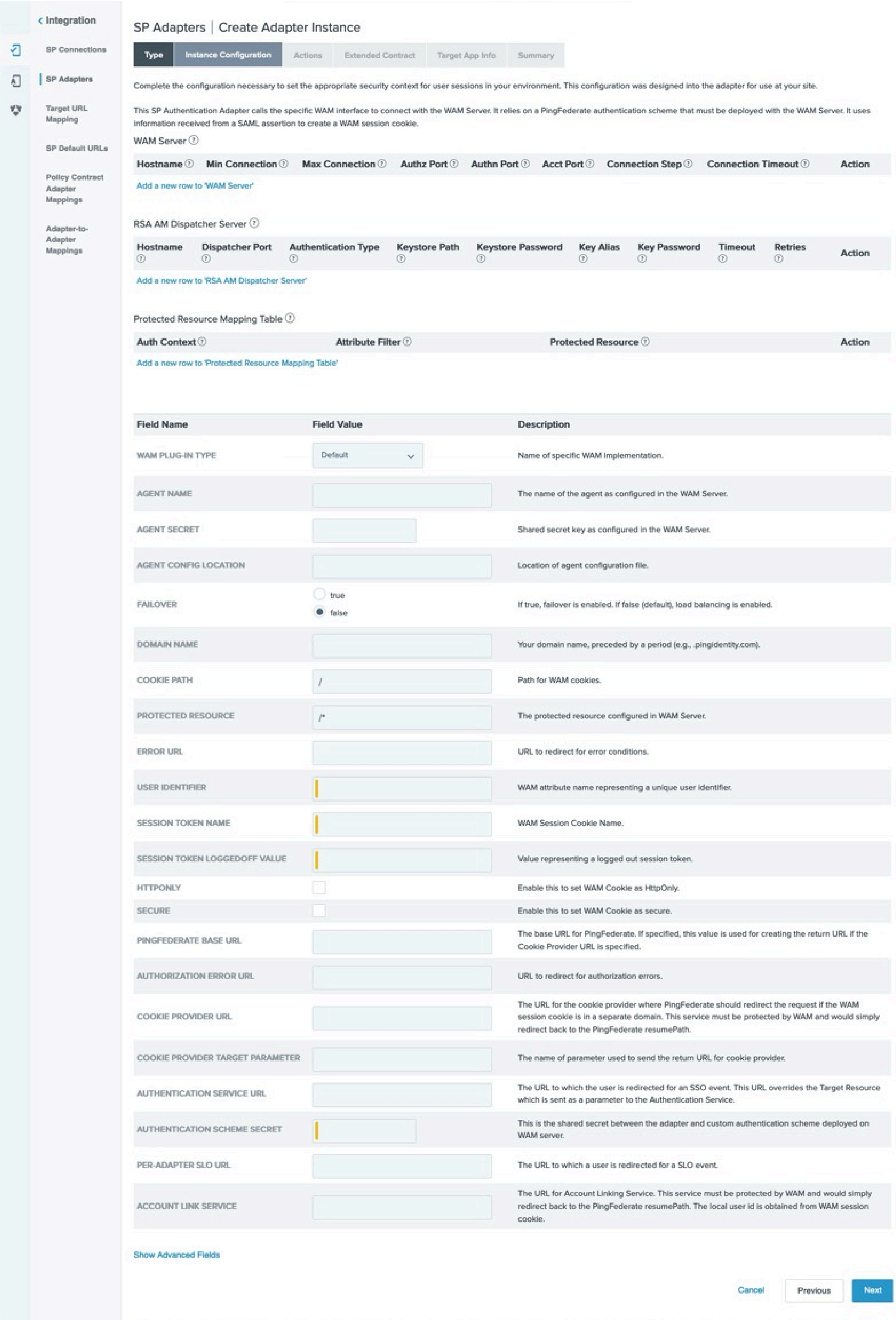
ⓘ **Important:** You must first create a third-party WAM Web Agent within your WAM tool. Several properties used to configure the agent are then used on the Instance Configuration tab discussed below. Refer to your WAM Server documentation for details on agent configuration.

Steps

1. In the PingFederate administrative console, create a new SP adapter instance.
    - For PingFederate 10.1 or later: go to **Applications**# **Integration**# **SP Adapters**. Click **Create New Instance**.
    - For PingFederate 10.0 or earlier: go to **Service Provider**# **Adapters**. Click **Create New Instance**.

2. On the **Type** tab, set the basic adapter instance attributes.
   a. In the **Instance Name** field, enter a name for the adapter instance.
   b. In the **Instance ID** field, enter a unique identifier for the adapter instance.
   c. In the **Type** list, select **WAM SP Adapter**. Click **Next**.

> ⓘ **Note:** If you are configuring the adapter for a custom plug-in (not bundled with this kit), then continue to step *5*. If you are configuring the RSA AM Dispatcher server, then continue with step *6*. If you are configuring OAM, continue at step *7*.



SP Adapters | Create Adapter Instance

Complete the configuration necessary to set the appropriate security context for user sessions in your environment. This configuration was designed into the adapter for use at your site.

This SP Authentication Adapter calls the specific WAM interface to connect with the WAM Server. It relies on a PingFederate authentication scheme that must be deployed with the WAM Server. It uses information received from a SAML assertion to create a WAM session cookie.

WAM Server

Hostname	Min Connection	Max Connection	Authz Port	Authn Port	Acct Port	Connection Step	Connection Timeout	Action

Add a new row to 'WAM Server'

RSA AM Dispatcher Server

Hostname	Dispatcher Port	Authentication Type	Keystore Path	Keystore Password	Key Alias	Key Password	Timeout	Retries	Action

Add a new row to 'RSA AM Dispatcher Server'

Protected Resource Mapping Table

Auth Context	Attribute Filter	Protected Resource	Action

Add a new row to 'Protected Resource Mapping Table'

Field Name	Field Value	Description
WAM PLUG-IN TYPE	Default	Name of specific WAM Implementation.
AGENT NAME		The name of the agent as configured in the WAM Server.
AGENT SECRET		Shared secret key as configured in the WAM Server.
AGENT CONFIG LOCATION		Location of agent configuration file.
FAILOVER	○ true ● false	If true, failover is enabled. If false (default), load balancing is enabled.
DOMAIN NAME		Your domain name, preceded by a period (e.g., .pingidentity.com).
COOKIE PATH	/	Path for WAM cookies.
PROTECTED RESOURCE	/*	The protected resource configured in WAM Server.
ERROR URL		URL to redirect for error conditions.
USER IDENTIFIER		WAM attribute name representing a unique user identifier.
SESSION TOKEN NAME		WAM Session Cookie Name.
SESSION TOKEN LOGGEDOFF VALUE		Value representing a logged out session token.
HTTPONLY	□	Enable this to set WAM Cookie as HttpOnly.
SECURE	□	Enable this to set WAM Cookie as secure.
PINGFEDERATE BASE URL		The base URL for PingFederate. If specified, this value is used for creating the return URL if the Cookie Provider URL is specified.
AUTHORIZATION ERROR URL		URL to redirect for authorization errors.
COOKIE PROVIDER URL		The URL for the cookie provider where PingFederate should redirect the request if the WAM session cookie is in a separate domain. This service must be protected by WAM and would simply redirect back to the PingFederate resumePath.
COOKIE PROVIDER TARGET PARAMETER		The name of parameter used to send the return URL for cookie provider.
AUTHENTICATION SERVICE URL		The URL to which the user is redirected for an SSO event. This URL overrides the Target Resource which is sent as a parameter to the Authentication Service.
AUTHENTICATION SCHEME SECRET		This is the shared secret between the adapter and custom authentication scheme deployed on WAM server.
PER-ADAPTER SLO URL		The URL to which a user is redirected for a SLO event.
ACCOUNT LINK SERVICE		The URL for Account Linking Service. This service must be protected by WAM and would simply redirect back to the PingFederate resumePath. The local user id is obtained from WAM session cookie.

Show Advanced Fields

3. (Only for custom plug-ins for WAM servers other than OAM or RSA) On the Instance Configuration tab, click **Add a new row to 'WAM Server'** and provide the following information into the table :

   a. Enter the Hostname or the IP address where the WAM server is running.

   b. Specify the remaining WAM server values required for your configuration.

   c. Click **Update** in the Action column.

   d. Repeat this step as needed for additional WAM plug-ins.

   Skip the next step.

4. (Only for the RSA bundled plug-in) On the Instance Configuration tab, click **Add a new row to 'RSA AM Dispatcher Server'** and provide the following information into the table

   ⓘ **Note:** You must specify at least one RSA AM Dispatcher Server.

   a. Enter the Hostname or the IP address and the (optional) Dispatcher Port where the RSA AM Dispatcher server is running.

      ⓘ **Note:** You must specify the authentication method that is used by the dispatcher server. If you have specified multiple dispatcher servers, each server can have individual authentication methods.

   b. Specify the Authentication Type used by the RSA Dispatcher Server.

      - **Clear** – clear text, no encryption
      - **Anon** – anonymous SSL, SSL encryption only
      - **Auth** – mutually authenticated SSL, SSL encryption with certificate-based encryption

   c. If the selected Authentication Type is **Auth**, you must specify the following RSA server values:

      - **Keystore Path** – String filename of the private Keystore file (PKCS12 only)
      - **Keystore Password** – password for the private Keystore
      - **Key Alias** – the alias to your private key in the Keystore
      - **Key Password** – private Key Password for Keystore

   d. Optional: Specify the Timeout value required for your configuration.

   e. Click **Update** in the Action column.

   f. Repeat this step as needed for additional RSA Servers.

5. (Optional: only for custom plug-ins for WAM servers and the OAM bundled plug-in) On the SP Adapter tab, click **Add a new row to 'Protected Resource Mapping Table'** and provide the following information into the table:

   - Authentication Context – This is part of the SAML assertion.
   - Attribute Filter – The names and values of attributes that the assertion must contain for this Protected Resource.
   - Protected Resource – The protected resource to be accessed if the Authentication Context and Attribute Filters in the assertion match the provided values.

   Click **Update** in the Action column. Repeat this step as needed.

6. Provide entries on the Instance Configuration tab, as described on the tab and in the table below.

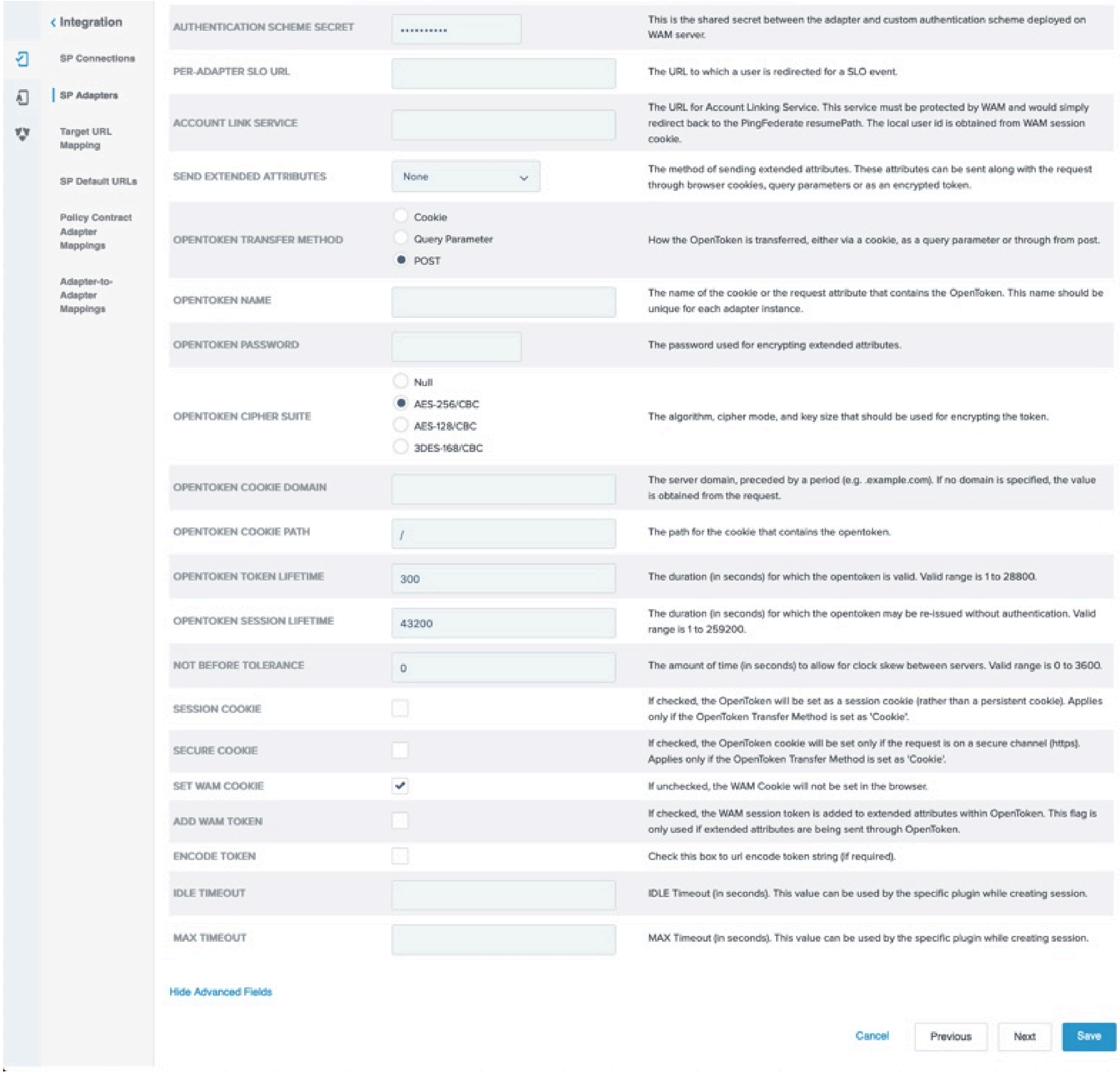
   ⓘ **Note:** The selected WAM Plug-in Type may override optional/required fields. For example, if the selected WAM Plug-in Type is OAM, the Agent Config Location becomes a required field. Leaving this field blank generates an error message.

Field	Description
WAM Plug-in Type	Class name for the specific WAM implementation. **Note:** WAM Plug-in Type determines optional/required fields.

Field	Description
Agent Name	This value must match the value used when the third-party WAM Web Agent was configured.
Agent Secret	This value must match the value used when the third-party WAM Web Agent was configured.
Agent Config Location	Required for OAM, this value must contain the full path to an XML network-configuration file generated by the access-management system.
Failover	The default is false, indicating load balancing is enabled and user-session states and configuration data are shared among multiple WAM servers. Select **true** to enable failover, indicating that when one server fails, the next server is used.
Domain Name	Enter the fully-qualified domain name (Cookie Domain where the WAM session cookie is stored), preceded by a period. For example: `.pingidentity.com`
Cookie Path	(Required) The root (/) directory is the default. Specify a different path for the WAM session cookie location, if necessary. Refer to your WAM Server documentation for details.
Protected Resource	(Required) All files in the root directory (/*) is the default. Specify a different path to the resources in the protected realm, if necessary.
Error URL	Enter a URL for redirecting the user if there are errors: for example, incorrect parameters in the link. This URL may contain query parameters. The URL has an `errorMessage`query parameter appended to it, which contains a brief description of the error that occurred. The error page can optionally display this message on the tab to provide guidance on remedying the problem. When employing the `errorMessage` query parameter in a custom error page, adhere to Web-application security best practices to guard against common content injection vulnerabilities. If no URL is specified, the appropriate default error landing page appears. For more information, see *Customizable user-facing tabs* in the PingFederate documentation. **Note:** If you define an error redirect URL, errors are sent to the error URL as well as logged in the PingFederate server log, but are not logged to the PingFederate audit log.
User Identifier	(Required) Defines which attribute that is parsed from the WAM session cookie is the user identifier for use in the assertion.
Session Token Name	(Required) WAM session cookie name.
Session Token LOGGEDOFF Value	(Required) Value representing a logged-out session token.
HTTP Only	Enable this option to set WAM Session Cookie as HTTP Only. If this option is enabled, the browser will send the WAM Session Cookie via HTTP or HTTPS.

Field	Description
Secure	Enable this option to set WAM Session Cookie as secure. If this option is enabled, the browser will only send the WAM Session Cookie via HTTPS only.
PingFederate Base URL	The base URL for PingFederate. If specified, this value is used for creating the return URL if Cookie Provider URL is being used.
Authorization Error URL	URL to redirect for authorization errors.
Cookie Provider URL	The URL for the cookie provider where PingFederate should redirect the request if the WAM session cookie is in a separate domain. This service must be protected by WAM and would simply redirect back to the PingFederate `resumePath`.
Cookie Provider Target Parameter	The name of the parameter used to send the return URL for the cookie provider.
Authentication Service URL	The URL to which the user is redirected for an SSO event. This URL overrides the Target Resource which is sent as a parameter to the Authentication Service.
Authentication Scheme Secret	(Required, except for RSA) The shared secret between the adapter and the custom authentication scheme deployed on the WAM server.
Per-Adapter SLO URL	If a URL is entered into this field, it will be used as the redirect target during SLO for this adapter instance, instead of the default value from Pingfederate.

Field	Description
Account Link Service	The URL for the Account Linking Service. This service must be protected by the WAM Web Agent and would simply redirect back to the PingFederate `resumePath`. The local user id is obtained from the WAM session cookie.



AUTHENTICATION SCHEME SECRET	••••••••••	This is the shared secret between the adapter and custom authentication scheme deployed on WAM server.
PER-ADAPTER SLO URL		The URL to which a user is redirected for a SLO event.
ACCOUNT LINK SERVICE		The URL for Account Linking Service. This service must be protected by WAM and would simply redirect back to the PingFederate resumePath. The local user id is obtained from WAM session cookie.
SEND EXTENDED ATTRIBUTES	None	The method of sending extended attributes. These attributes can be sent along with the request through browser cookies, query parameters or as an encrypted token.
OPENTOKEN TRANSFER METHOD	○ Cookie ○ Query Parameter ● POST	How the OpenToken is transferred, either via a cookie, as a query parameter or through from post.
OPENTOKEN NAME		The name of the cookie or the request attribute that contains the OpenToken. This name should be unique for each adapter instance.
OPENTOKEN PASSWORD		The password used for encrypting extended attributes.
OPENTOKEN CIPHER SUITE	○ Null ● AES-256/CBC ○ AES-128/CBC ○ 3DES-168/CBC	The algorithm, cipher mode, and key size that should be used for encrypting the token.
OPENTOKEN COOKIE DOMAIN		The server domain, preceded by a period (e.g. .example.com). If no domain is specified, the value is obtained from the request.
OPENTOKEN COOKIE PATH	/	The path for the cookie that contains the opentoken.
OPENTOKEN TOKEN LIFETIME	300	The duration (in seconds) for which the opentoken is valid. Valid range is 1 to 28800.
OPENTOKEN SESSION LIFETIME	43200	The duration (in seconds) for which the opentoken may be re-issued without authentication. Valid range is 1 to 259200.
NOT BEFORE TOLERANCE	0	The amount of time (in seconds) to allow for clock skew between servers. Valid range is 0 to 3600.
SESSION COOKIE	□	If checked, the OpenToken will be set as a session cookie (rather than a persistent cookie). Applies only if the OpenToken Transfer Method is set as 'Cookie'.
SECURE COOKIE	□	If checked, the OpenToken cookie will be set only if the request is on a secure channel (https). Applies only if the OpenToken Transfer Method is set as 'Cookie'.
SET WAM COOKIE	☑	If unchecked, the WAM Cookie will not be set in the browser.
ADD WAM TOKEN	□	If checked, the WAM session token is added to extended attributes within OpenToken. This flag is only used if extended attributes are being sent through OpenToken.
ENCODE TOKEN	□	Check this box to url encode token string (if required).
IDLE TIMEOUT		IDLE Timeout (in seconds). This value can be used by the specific plugin while creating session.
MAX TIMEOUT		MAX Timeout (in seconds). This value can be used by the specific plugin while creating session.

7. Optional: Click **Show Advanced Fields** to configure the sending of extended attributes or to specify OpenToken configuration values or settings. For more information, see *Configuring an OpenToken SP Adapter instance* in the PingFederate documentation.

> ⓘ **Note:** If you want to configure the use of OpenToken as part of the WAM adapter configuration, then complete the fields as described on the tab and in the table below.

You can change default values or settings, depending on your network configuration and other requirements at your site.

Field	Description
Send Extended Attributes	The method of sending extended attributes. These attributes can be sent along with the request through browser cookies, query parameters, or as an encrypted token. Note: To define the attributes on the Extended Contract tab (see step *12*).
OpenToken Transfer Method	How the OpenToken is transferred, either via a cookie, as a query parameter, or as a Form Post.
OpenToken Name	The name of the cookie or the request attribute that contains the OpenToken. This name should be unique for each adapter instance.
OpenToken Password	The password used for encrypting extended attributes. Note: This is also used for generating the configuration file used by the OpenToken agent, and is thus required even if the Cipher Suite is set to NULL.
OpenToken Cipher Suite	The algorithm, cipher mode, and key size that should be used for encrypting the token.
OpenToken Cookie Domain	The server domain, preceded by a period (e.g. .example.com). If no domain is specified, the value is obtained from the request.
OpenToken Cookie Path	The path for the cookie that contains the OpenToken.
OpenToken Token Lifetime	The duration (in seconds) for which the OpenToken is valid. Range is 1 to 28800.
OpenToken Session Lifetime	The duration (in seconds) for which the OpenToken may be re-issued without authentication. Range is 1 to 259200.
Not Before Tolerance	The amount of time (in seconds) to allow for clock skew between servers. Range is 0 to 3600.
Session Cookie	If checked, OpenToken will be set as a session cookie (rather than a persistent cookie). Applies only if the OpenToken Transfer Method is set as ‘Cookie’.
Secure Cookie	If checked, the OpenToken cookie will be set only if the requests is on a secure channel (https). Applies only if the OpenToken Transfer Method is set as 'Cookie'.
Set WAM Cookie	If unchecked, the WAM Cookie will not be set in the browser.
Add WAM Token	If checked, the WAM session token is added to extended attributes within OpenToken. This flag is only used if extended attributes are being sent through OpenToken.

Field	Description
Encode Token	Check this box to URL encode the token string if required by the WAM provider.
Idle Timeout	IDLE Timeout (in seconds). This value can be used by the specific plugin while creating session if required.
Max Timeout	MAX Timeout (in seconds). This value can be used by the specific plugin while creating session.

8. Click **Next**.
9. On the **Actions** tab, click the **Test Connection** link to validate the WAM configuration.

> ⓘ **Note:** If you're using an OpenToken Adapter Configuration, click the **Invoke Download** link and then click **Export** to download the `agent-config.txt` properties to a directory that is readable by the WAM Web Agent.

10. On the **Extended Contract** tab, add any attributes that you want to include in the request header. Click **Next**.
11. On the **Summary** tab, check and save your configuration.
    - For PingFederate 10.1 or later: click **Save**.
    - For PingFederate 10.0 or earlier: click **Done**. On the **Manage SP Adapter Instances** tab, click **Save**.

Creating a Custom Authentication Scheme for OAM

About this task

The SP Adapter uses a custom authentication scheme when creating a WAM session and validates authentication requests coming from PingFederate. This section describes how to deploy the OAM-compatible Java-based PingFederate Custom Authentication Scheme.

Steps

1. From the `<integration_kit_install_dir>/dist` directory, import the following file into the OAM:

   `PingCustomAuthPlugin.jar`

   The `PingCustomAuthPlugin.jar` file is a custom authentication scheme that supports OAM.
2. Configure your Access Server to use the custom authentication plug-in by creating or modifying a custom authentication scheme.

   For more information, see *Creating Custom Authentication Plug-ins* in the Oracle documentation.

> ⓘ **Note:** The secret you specify when creating the custom authentication scheme must match the secret stored in the PingFederate SP Adapter.

SP deployment notes

The following notes provide additional information for using the WAM Integration Kit as an SP:

- The WAM SP Adapter relies on a custom authentication scheme to validate the authentication request coming from the PingFederate SP Adapter. The secret specified in the SP Adapter is verified against the one configured with the scheme. You can create custom authentication schemes for specific WAM systems using their API.

The authentication scheme for OAM is included in the samples folder at the following location: `<integration_kit_install_dir> /sdk/samples/oam/PingCustomAuthPlugin.java`

- To support Account Linking, the Account Linking Service has to be implemented and then protected by the WAM Web Agent. This could be done as a `JSP` page that redirects back to PingFederate. The relative `resumePath` is sent as part of the request and the `JSP` page needs to create the absolute URL and redirect, as shown below.

```
<%
  String resumePath = request.getParameter("resumePath");
    if(resumePath != null) {
       resumePath = <PingFed_URL> + resumePath;
       response.sendRedirect(resumePath);
    }
%>
```

where `<PingFed_URL>` is the fully-qualified URL of the PingFederate server.

`resumePath` is generated from PingFederate and intended for asynchronous communication between the adapter and the external application. The state is saved in PingFederate and processing is resumed when the application redirects to the `resumePath`.

The WAM SP Adapter retrieves the user information from the WAM session cookie and resumes SSO.

Test the SP adapter

About this task

You can test this adapter using the samples applications that are included in the Java Integration Kit.

Steps

1. Download the Java Integration kit from the *PingFederate server add-ons page*.
2. Complete the steps in *Sample application setup* in the Java Integration Kit documentation to set up an SP application.
3. Configure an instance of the WAM Adapter as shown in *Setting Up the SP Adapter*.
4. Reconfigure the IdP connection to use the WAM Adapter instance.

   Delete the existing adapter instance for the connection and map the WAM Adapter instance in its place.
5. From the Main Menu, click **Adapters** under My SP Configuration.
6. Protect a web page using the WAM web Agent.
7. On the same web server, create an unprotected web page with a hyperlink to PingFederate's SP-initiated SSO endpoint in the following format:

   `http[s]://<PF_host>:<port>/sp/startSSO.ping`

   `?TargetResource=<protected_resource>`

   `&PartnerIdpId=<connection_id>`

   where:

   - `<PF_host>` is the machine running the PingFederate server.
   - `<port>` is the port (default value: `9031`).
   - `<protected_resource>` is the web page protected in the previous step.
   - `<connection_id>` is the Connection ID of the IdP connection.

8. Click the SSO link on the unprotected web page.

   You should arrive at the IdP application's login page.
9. Add at least one of the users in the username drop-down list to the WAM Server.

   Refer to your WAM platform documentation for more information.
10. On the IdP application's login page, log in with a username managed by your WAM platform.

    You should be redirected to a WAM platform-protected web page. Independently, you can view cookies from your browser to see that a WAM session cookie has been created.

Release notes

Changelog

Web Access Management Integration Kit 2.0 – August 2014 (Current Release)

- Added a per-adapter SLO URL field
- Added an Authentication Mapping Table with an attribute filter for the IdP adapter
- Added a Protected Resource Mapping Table to the SP adapter with an attribute filter
- Enabled cookie provider functionality during SLO
- Added an encode token field to the SP adapter
- Added support for ObFormLoginCookie with customizable rh value

Web Access Management Integration Kit 1.2 – August 2013

- Added support for Cookie Provider
- Added OpenToken support within WAM Adapter
- Added Authentication Level to Authentication Context mapping table

Web Access Management Integration Kit 1.1 – March 2013

- WAM kit now includes WAM plug-in compatible with RSA Access Manager

Web Access Management Integration Kit 1.0.1 – December 2012

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

Web Access Management Integration Kit 1.0 – November 2012

- Initial Release
- Redesigned former product-specific kits to provide consistent functionality across multiple WAM products

Download manifest

The following files are included in the `.zip` archive:

- `ReadMeFirst.pdf` – contains links to this online documentation
- `/legal` – contains this document:
  - `Legal.pdf` – copyright and license information
- `/dist` – contains libraries needed to run the adapter:
  - `pf-wam-adapter-2.0.jar` – the WAM Adapter JAR file
  - `opentoken-adapter-2.5.1.jar` – OpenToken Adapter JAR file

- `/dist/oam` – contains Oracle Access Manager libraries needed to run the adapter:
  - `pf-oam-plugin.jar` – Pre-built OAM-compatible WAM plug-in JAR file
  - `PingCustomAuthPlugin.jar` – a Java-based PingFederate Custom Authentication Scheme
- `/dist/rsa` – contains RSA libraries needed to run the adapter:
  - `pf-rsa-plugin.jar` – Pre-built RSA-compatible WAM plug-in JAR file
  - `axm-runtime-api-6.1.4.jar` - RSA API library
  - `jsafeFIPS-6.1.jar` – RSA API library
  - `jsafeJCEFIPS-6.1.jar` – RSA API library
- `/sdk` – contains build scripts, documents, libraries, and sample code to build a WAM plug-in:
  - `README.txt` – contains instructions for creating a third-party WAM plug-in to interact with PingFederate.
  - `/docs` – contains documentation on how to build a WAM plug-in.
  - `/lib` – contains libraries and supporting files needed to build a WAM plug-in.
  - `/samples` – contains sample code used to build a WAM plug-in.

Web Access Management (WAM) Token Translator

The PingFederate Web Access Management (WAM) Token Translator provides a Token Processor and a Token Generator for use with the PingFederate WS-Trust Security Token Service (STS).

The Token Processor allows an Identity Provider (IdP) STS to accept and validate a WAM session token from a Web Service Client (WSC) and then map user attributes into a SAML token for the WSC to send to a Web Service Provider (WSP). The Token Generator allows a Service Provider (SP) STS to issue a WAM session token for a WSP, including mapped attributes from an incoming SAML token.

> ⓘ **Important**:
>
> The Token Translator is designed to work with WAM products from multiple vendors. A WAM plug-in is required to connect the Token Translator with each third-party system. This kit ships with WAM plug-ins compatible with Oracle Access Manager (OAM) 10g and 11g, and with RSA Access Manager 6.1. A simple software development kit (SDK) is also included to create custom WAM plug-ins for other systems.

If you are creating a WAM plug-in for any third-party product other than OAM and RSA Access Manager, you must complete the tasks in the WAM plug-in SDK `README.txt` file located in the `<token_translator_install_dir>/sdk` directory.

> ⓘ **Important**:
>
> Ping Identity provides an SDK for enabling Web Service applications (Client or Provider) to interact with the PingFederate STS. The SDK is available for download on the *PingFederate server add-ons page*.

Intended audience

This document is intended for PingFederate administrators.

If you need help during the setup process, see the following resources:

- The following sections of the PingFederate documentation:
  - *WS-Trust STS configuration*

Please consult the WAM documentation tool if you encounter any difficulties in areas not directly associated with PingFederate or the WAM Token Translator.

System requirements

- PingFederate 6.x or later
- WAM plug-in for the desired third-party system, built and deployed per the WAM plug-in SDK documentation
- Associated vendor-supplied libraries to support the WAM plug-in you are using
- Fully functional WAM plug-ins for OAM and RSA are included in the WAM Token Translator package.
- Separate third-party Web Agent configured using the WAM server administrative software

Setup

WAM plug-ins

This kit ships with WAM plug-ins compatible with OAM 10g and 11g, RSA Access Manager 6.1, as well as a simple SDK to create custom WAM plug-ins for other systems.

Custom WAM plug-in installation

About this task

This section describes how to deploy a custom WAM plug-in for both Token Processors and Token Generators.

Steps

1. If you are creating a WAM plug-in for any third-party WAM product not bundled with this kit, you must complete the tasks in the WAM plug-in SDK `README.txt` file located in the `<token_translator_install_dir>/sdk` directory.

   ⓘ **Note:** Contact the third-party vendor support department to obtain required third-party WAM API libraries for creating a WAM plug-in to interact with PingFederate.

2. If you are deploying for a third-party WAM product, copy the resultant WAM plug-in output JAR file `pf-<WAM_TYPE>-plugin.jar` from the `<token_translator_install_dir>/sdk/samples/<WAM_TYPE>` directory into the `<PF_install>/pingfederate/server/default/deploy` directory.

Results

The WAM Token Translator requires a plug-in to connect with a specific WAM product (see the WAM plug-in SDK in the distribution package for sample code and more details on building the plug-in).

ⓘ **Note:** The WAM plug-in SDK is designed specifically to connect the WAM Token Translator with a third-party WAM product, using an API provided by the vendor.

WAM plug-in installation for RSA

About this task

This section describes how to deploy the pre-built RSA-compatible WAM plug-in for both Token Processor and Token Generators.

Steps

1. The additional RSA API libraries for creating a WAM plug-in to interact with PingFederate are included in the `<token_translator_install_dir>/dist/rsa` directory.
   - `axm-runtime-api-6.1.4.jar`
   - `jsafeFIPS-6.1.jar`
   - `jsafeJCEFIPS-6.1.jar`
2. Copy the RSA API libraries from the `<token_translator_install_dir>/dist/rsa` into:

   `<PF_install>/pingfederate/server/default/deploy` directory.
3. Copy the `pf-rsa-plugin.jar` from the `<token_translator_install_dir>/dist/rsa` directory into:

   `<PF_install>/pingfederate/server/default/deploy`
4. Complete the *Token translator installation* on page 32 prior to restarting the PingFederate server.

WAM plug-in installation for OAM

About this task

This section describes how to deploy the pre-built OAM-compatible WAM plug-in for both Token Processors and Token Generators.

Steps

1. Get the necessary OAM API library from the *Oracle Identity Management Download site*
   - `oamasdk-api.jar`
2. Copy the OAM API library provided by the vendor into the `<PF_install>/pingfederate/server/default/deploy` directory.
3. Copy the `pf-oam-plugin.jar` file from the `<token_translator_install_dir>/dist/` directory into:

   `<PF_install>/pingfederate/server/default/deploy`.
4. Complete the *Token translator installation* on page 32 prior to restarting the PingFederate server (see next section).

Token translator installation

About this task

This section describes how to install the WAM Token Translator to configure the Token Processor, the Token Generator, or both.

ⓘ **Note:** If you have already deployed version 2.5.1 (or higher) of the OpenToken Adapter, skip steps *1* through *3* 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 the same directory.

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

   `<PF_install>/pingfederate/server/default/deploy`
4. From this distribution, copy the following file to the `/server/default/deploy` directory in your PingFederate server installation:

   `pf-wam-token-translator-2.0.jar`
5. *If* you are running PingFederate 6.0 as a Windows service, *then*:

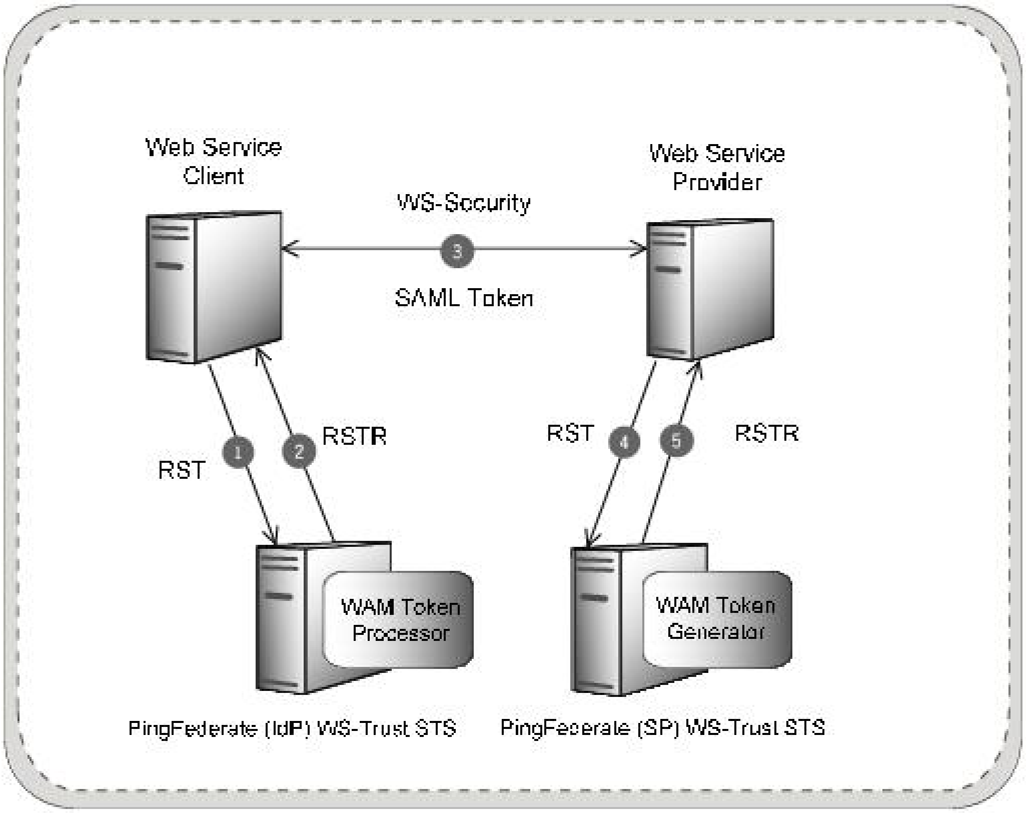
   Edit the `Java Library Path` section of the configuration file

   `pingfederate/sbin/wrapper/PingFederateService.conf`, adding the line:

   `wrapper.java.library.path.append_system_path=true`
6. Start the PingFederate server.

WS-Trust STS processing

The following illustration displays a basic Web Services scenario using the PingFederate WS Trust STS in the role of both IdP and SP:



Processing Steps

1. A WSC sends a Request Security Token (RST) message containing a WAM session token to the PingFederate STS IdP endpoint.
2. The PingFederate WAM Token Processor extracts, decrypts, parses, and validates the WAM session token. If the WAM session token is valid, PingFederate maps attributes from the WAM session token into a SAML token. PingFederate issues the SAML token based on the SP connection configuration and embeds the token in a Request Security Token Response (RSTR), which is returned to the WSC.
3. The WSC binds the issued SAML token into a Web Service Security (WSS) header and sends it via a SOAP request to the WSP.
4. The WSP sends an RST Issue request containing the SAML token to the PingFederate STS SP endpoint. PingFederate validates the SAML token and, if valid, maps attributes from the SAML token into a WAM session. PingFederate issues the WAM session token based on the WAM Token Generator configuration and embeds the token in an RSTR, which is returned to the WSP.
5. The WSP receives the WAM session token in the RSTR for local domain processing.

Configuring the IdP token processor

About this task

If you are using PingFederate as an IdP server, configure the Token Processor using the following steps:

> ⓘ **Important:** You must first create a third-party WAM Web Agent within your WAM tool. Several properties used to configure the agent are then used on the Instance Configuration screen. Refer to your WAM documentation for details on agent configuration.

Steps

1. Log on to the PingFederate administrative console and click **Token Processors** under Application Integration Settings in the IdP Configuration section of the Main Menu.

   If you do not see **Token Processors** on the Main Menu, enable WS-Trust under Server Settings on the Roles & Protocols screen by selecting WS-Trust for the IdP role.

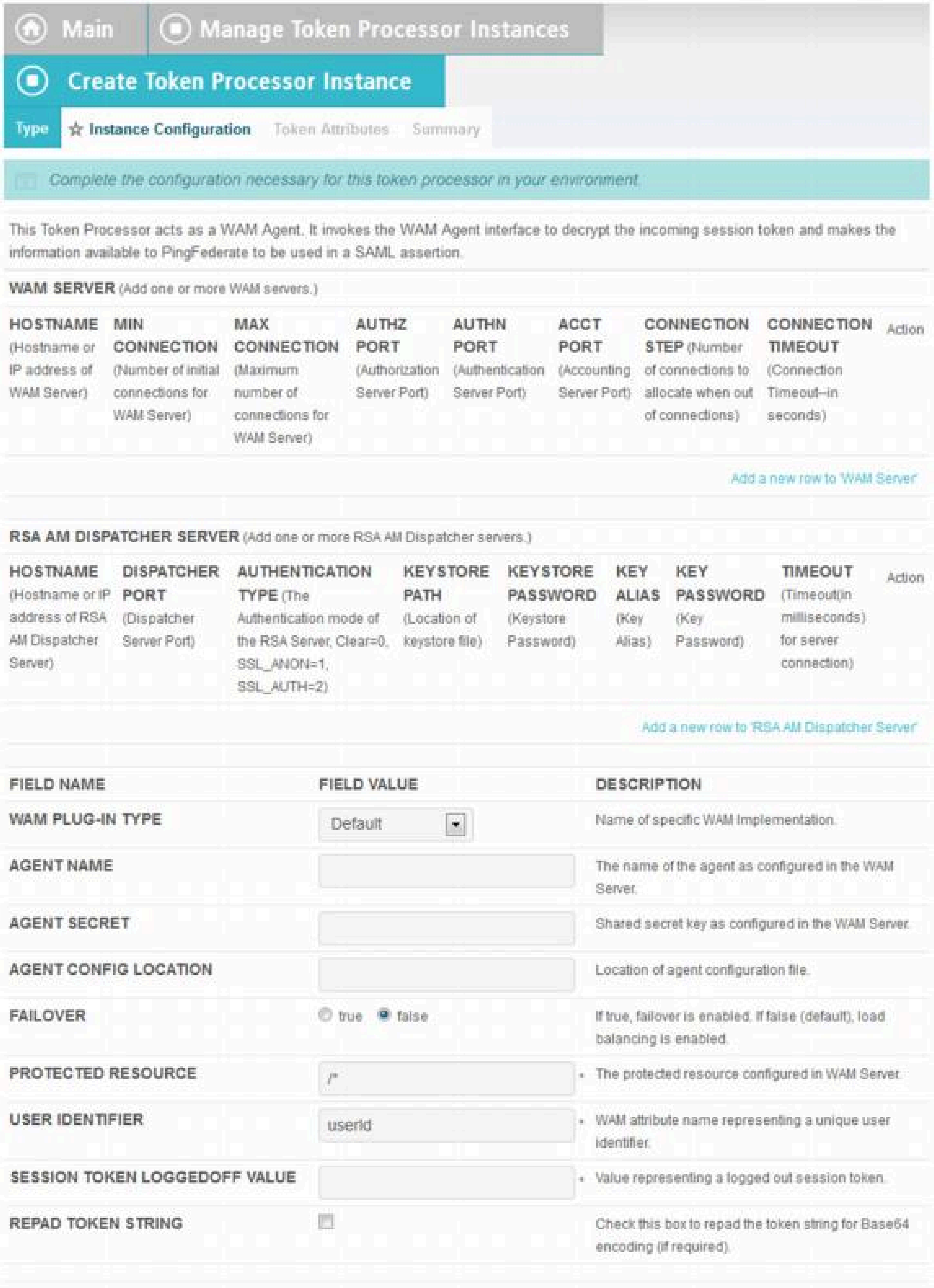
   > ⓘ **Note:** To enable token exchange, you may be prompted to provide SAML 1.x and SAML 2.0 federation identifiers for the STS on the Federation Info screen. Refer to the Federation Info screen’s **Help** page for more information.

2. On the Manage Token Processor Instances screen, click **Create New Instance**.
3. On the Type screen, enter an Instance Name and Instance Id.

   The Name is any you choose for identifying this instance. The ID is used internally and may not contain spaces or non-alphanumeric characters.

4. Select WAM Token Processor 2.0 as the Type and click **Next**.

> ⓘ **Note:** If you are configuring the adapter for a custom plug-in (not bundled with this kit), then continue to step *5*. If you are configuring the RSA Dispatcher server, then continue with step *6*. If you are configuring OAM, continue at step *7*.


Main
Manage Token Processor Instances
Create Token Processor Instance
Type
☆ Instance Configuration
Token Attributes
Summary

Complete the configuration necessary for this token processor in your environment.

This Token Processor acts as a WAM Agent. It invokes the WAM Agent interface to decrypt the incoming session token and makes the information available to PingFederate to be used in a SAML assertion.

WAM SERVER (Add one or more WAM servers.)

HOSTNAME (Hostname or IP address of WAM Server)	MIN CONNECTION (Number of initial connections for WAM Server)	MAX CONNECTION (Maximum number of connections for WAM Server)	AUTHZ PORT (Authorization Server Port)	AUTHN PORT (Authentication Server Port)	ACCT PORT (Accounting Server Port)	CONNECTION STEP (Number of connections to allocate when out of connections)	CONNECTION TIMEOUT (Connection Timeout–in seconds)	Action

Add a new row to 'WAM Server'

RSA AM DISPATCHER SERVER (Add one or more RSA AM Dispatcher servers.)

HOSTNAME (Hostname or IP address of RSA AM Dispatcher Server)	DISPATCHER PORT (Dispatcher Server Port)	AUTHENTICATION TYPE (The Authentication mode of the RSA Server, Clear=0, SSL_ANON=1, SSL_AUTH=2)	KEYSTORE PATH (Location of keystore file)	KEYSTORE PASSWORD (Keystore Password)	KEY ALIAS (Key Alias)	KEY PASSWORD (Key Password)	TIMEOUT (Timeout(in milliseconds) for server connection)	Action

Add a new row to 'RSA AM Dispatcher Server'

FIELD NAME	FIELD VALUE	DESCRIPTION
WAM PLUG-IN TYPE	Default ▾	Name of specific WAM Implementation.
AGENT NAME		The name of the agent as configured in the WAM Server.
AGENT SECRET		Shared secret key as configured in the WAM Server.
AGENT CONFIG LOCATION		Location of agent configuration file.
FAILOVER	○ true ● false	If true, failover is enabled. If false (default), load balancing is enabled.
PROTECTED RESOURCE	/*	* The protected resource configured in WAM Server.
USER IDENTIFIER	userId	* WAM attribute name representing a unique user identifier.
SESSION TOKEN LOGGEDOFF VALUE		* Value representing a logged out session token.
REPAD TOKEN STRING	□	Check this box to repad the token string for Base64 encoding (if required).

5. (Only for custom plug-ins for WAM servers other than OAM or RSA) On the Instance Configuration screen, click **Add a new row to 'WAM Server'** and provide the following information into the table:

   a. Enter the Hostname or the IP address where the WAM server is running.
   b. Specify the remaining WAM server values required for your configuration.
   c. Click **Update** in the Action column.
   d. Repeat this step as needed, for additional WAM plug-ins.

   Skip the next step.

6. (Only for the RSA bundled plug-in) On the Instance Configuration screen, click **Add a new row to 'RSA AM Dispatcher Server'** and provide the following information in the table:

   ⓘ **Note:** You must specify at least one RSA AM Dispatcher Server

   a. Enter the Hostname or the IP address and the (optional) Dispatcher Port where the RSA AM Dispatcher server is running.

      ⓘ **Note:** You must specify the authentication method that is used by the dispatcher server. If you have specified multiple dispatcher servers, each server can have individual authentication methods.

   b. Specify the Authentication Type used by the RSA Dispatcher Server.
      - **Clear** – clear text, no encryption
      - **Anon** – anonymous SSL, SSL encryption only
      - **Auth** – mutually authenticated SSL, SSL encryption with certificate-based encryption

   c. If the selected Authentication Type is **Auth**, you must specify the following RSA server values:
      - **Keystore Path** – String filename of the private Keystore file (PKCS12 only)
      - **Keystore Password** – password for the private Keystore
      - **Key Alias** – the alias to your private key in the Keystore
      - **Key Password** – private Key Password for Keystore

   d. Optional: Specify the Timeout value required for your configuration.
   e. Click **Update** in the Action column.
   f. Repeat this step as needed for additional RSA Servers.

7. Provide entries on the Instance Configuration screen, as described on the screen and in the following table.

   ⓘ **Note:** selected WAM Plug-in Type may override optional/required fields. For example, if the selected WAM Plug-n Type is `OAM`, the Agent Config Location becomes a required field. Leaving this field blank generates an error message.

Field	Description
WAM Plug-in Type	Class name for the specific WAM implementation. ⓘ **Note:** WAM Plug-in Type determines optional/required fields.
Agent Name	This value must match the value used when the third-party WAM Web Agent was configured.
Agent Secret	This value must match the value used when the third-party WAM Web Agent was configured.
Agent Config Location	Required for OAM, this value must contain the full path to an XML network-configuration file generated by the access-management system.

Field	Description
Failover	The default is false, indicating load balancing is enabled and user-session states and configuration data are shared among multiple WAM servers. Select **true** to enable failover, indicating that when one server fails, the next server is used.
Protected Resource	(Required) All files in the root directory (/*) is the default. Specify a different path to the resources in the protected realm, if necessary.
User Identifier	(Required) Defines which attribute that is parsed from the WAM session token is the user identifier for use in the assertion.
Session Token LOGGEDOFF Value	(Required) Value representing a logged-out session token.
Repad Token String	Enable this to pad the incoming session token string for Base64 encoding (if required).

8. Click **Next**.
9. Optional: On the Token Attributes screen, select any or all attributes whose value you want to mask in the PingFederate log file.

   For more information about this screen, see the PingFederate *Administrator's Manual*. More information is available on the **Help** page.
10. Click **Next**.
11. On the Summary screen, verify that the information is correct and click **Done**.
12. On the Manage Token Processor Instances screen, click **Save**.

Configuring the SP token generator

About this task

If you are using PingFederate as a Service Provider (SP), configure the Token Generator using the following steps:

> ⓘ **Important:** You must first create a third-party WAM Web Agent within your WAM tool. Several properties used to configure the agent are then used on the Instance Configuration screen. Refer to your WAM documentation for details on agent configuration.

Steps

1. Log on to the PingFederate administrative console and click **Token Generators** under Application Integration Settings in the SP Configuration section of the Main Menu.

   If you do not see **Token Generators** on the Main Menu, enable WS-Trust under Server Settings on the Roles & Protocols screen by selecting WS-Trust for the SP role.

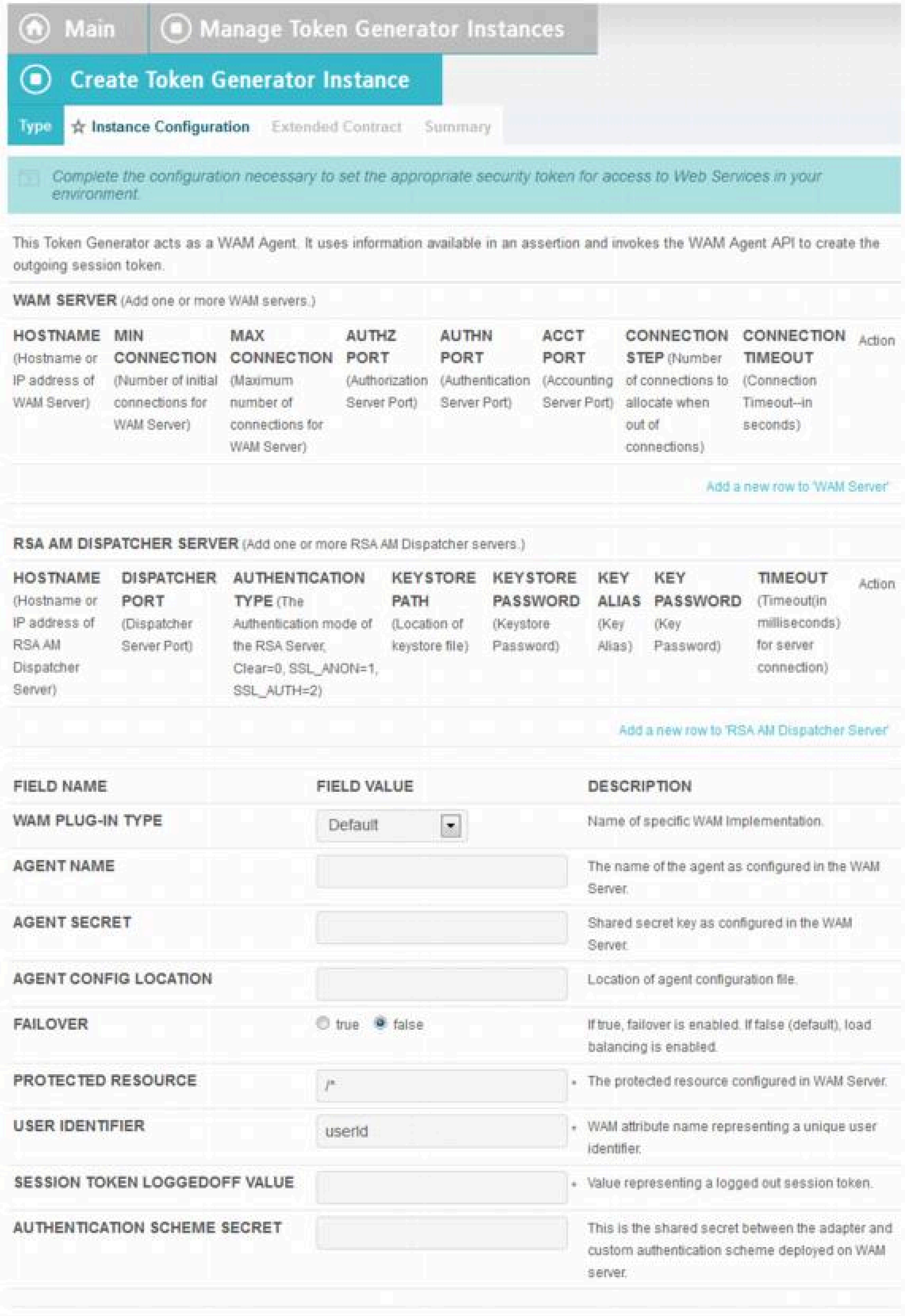
   > ⓘ **Note:** To enable token exchange, you may be prompted to provide SAML 1.x and SAML 2.0 federation identifiers for the STS on the Federation Info screen. Refer to the Federation Info screen's **Help** page for more information.
2. On the Manage Token Generator Instances screen, click **Create New Instance**.

3. On the Type screen, enter an Instance Name and Instance Id.

   The Name is any you choose for identifying this instance. The ID is used internally and may not contain spaces or non-alphanumeric characters.

4. Select WAM Token Generator 2.0 as the Type and click **Next**.

   ⓘ **Note:** If you are configuring the adapter for a custom plug-in (not bundled with this kit), then continue to step *5*. If you are configuring the RSA Dispatcher server, then continue with step *6*. If you are configuring OAM, continue at step *7*.



Create Token Generator Instance

Complete the configuration necessary to set the appropriate security token for access to Web Services in your environment.

This Token Generator acts as a WAM Agent. It uses information available in an assertion and invokes the WAM Agent API to create the outgoing session token.

WAM SERVER (Add one or more WAM servers.)

HOSTNAME (Hostname or IP address of WAM Server)	**MIN CONNECTION** (Number of initial connections for WAM Server)	**MAX CONNECTION** (Maximum number of connections for WAM Server)	**AUTHZ PORT** (Authorization Server Port)	**AUTHN PORT** (Authentication Server Port)	**ACCT PORT** (Accounting Server Port)	**CONNECTION STEP** (Number of connections to allocate when out of connections)	**CONNECTION TIMEOUT** (Connection Timeout--in seconds)	Action

Add a new row to 'WAM Server'

RSA AM DISPATCHER SERVER (Add one or more RSA AM Dispatcher servers.)

HOSTNAME (Hostname or IP address of RSA AM Dispatcher Server)	**DISPATCHER PORT** (Dispatcher Server Port)	**AUTHENTICATION TYPE** (The Authentication mode of the RSA Server, Clear=0, SSL_ANON=1, SSL_AUTH=2)	**KEYSTORE PATH** (Location of keystore file)	**KEYSTORE PASSWORD** (Keystore Password)	**KEY ALIAS** (Key Alias)	**KEY PASSWORD** (Key Password)	**TIMEOUT** (Timeout(in milliseconds) for server connection)	Action

Add a new row to 'RSA AM Dispatcher Server'

FIELD NAME	FIELD VALUE	DESCRIPTION
WAM PLUG-IN TYPE	Default ▾	Name of specific WAM Implementation.
AGENT NAME		The name of the agent as configured in the WAM Server.
AGENT SECRET		Shared secret key as configured in the WAM Server.
AGENT CONFIG LOCATION		Location of agent configuration file.
FAILOVER	○ true ● false	If true, failover is enabled. If false (default), load balancing is enabled.
PROTECTED RESOURCE	/* •	The protected resource configured in WAM Server.
USER IDENTIFIER	userId •	WAM attribute name representing a unique user identifier.
SESSION TOKEN LOGGEDOFF VALUE	•	Value representing a logged out session token.
AUTHENTICATION SCHEME SECRET		This is the shared secret between the adapter and custom authentication scheme deployed on WAM server.

5. (Only for custom plug-ins for WAM servers other than OAM or RSA) On the Instance Configuration screen, click **Add a new row to 'WAM Server'** and provide the following information into the table:
   a. Enter the Hostname or the IP address where the WAM server is running.
   b. Specify the remaining WAM server values that are required for your configuration.
   c. Click **Update** in the Action column.
   d. Repeat this step as needed, for additional WAM plug-ins.

   Skip the next step.
6. (Only for the RSA bundled plug-in) On the Instance Configuration screen, click **Add a new row to 'RSA AM Dispatcher Server'** and provide the following information in the table:

   > ⓘ **Note:** You must specify at least one RSA AM Dispatcher Server

   a. Enter the Hostname or the IP address and the (optional) Dispatcher Port where the RSA AM Dispatcher server is running.

   > ⓘ **Note:** You must specify the authentication method that is used by the dispatcher server. If you have specified multiple dispatcher servers, each server can have individual authentication methods.

   b. Specify the Authentication Type used by the RSA Dispatcher Server.
      - **Clear** – clear text, no encryption
      - **Anon** – anonymous SSL, SSL encryption only
      - **Auth** – mutually authenticated SSL, SSL encryption with certificate-based encryption
   c. If the selected Authentication Type is **Auth**, you must specify the following RSA server values:
      - **Keystore Path** – String filename of the private Keystore file (PKCS12 only)
      - **Keystore Password** – password for the private Keystore
      - **Key Alias** – the alias to your private key in the Keystore
      - **Key Password** – private Key Password for Keystore
   d. Optional: Specify the Timeout value required for your configuration.
   e. Click **Update** in the Action column.
   f. Repeat this step as needed for additional RSA Servers.
7. Provide entries on the Instance Configuration screen, as described on the screen and in the table below.

   > ⓘ **Note:** The selected WAM Plug-in Type may override optional/required fields. For example, if the selected WAM Plug-n Type is `OAM`, the Agent Config Location becomes a required field. Leaving this field blank generates an error message.

Field	Description
WAM Plug-in Type	Class name for the specific WAM implementation. ⓘ **Note:** WAM Plug Type determines optional/required fields.
Agent Name	This value must match the value used when the third-party WAM Web Agent was configured.
Agent Secret	This value must match the value used when the third-party WAM Web Agent was configured.
Agent Config Location	Required for OAM, this value must contain the full path to an XML network-configuration file generated by the access-management system.

Field	Description
Failover	The default is false, indicating load balancing is enabled and user-session states and configuration data are shared among multiple WAM servers. Select **true** to enable failover, indicating that when one server fails, the next server is used.
Protected Resource	(Required) All files in the root directory (/*) is the default. Specify a different path to the resources in the protected realm, if necessary.
User Identifier	(Required) Defines which attribute that is parsed from the WAM session token is the user identifier for use in the assertion.
Session Token LOGGEDOFF Value	(Required) Value representing a logged out session token.
Authentication Scheme Secret	(Required, except for RSA) The shared secret between the adapter and the custom authentication scheme deployed on the WAM server.
Encode Token (Advanced Field)	The default is false. Check this box to url encode token string (if required).

8. Click **Next**.
9. Optional: On the Extended Contract screen, add attributes you expect to retrieve in addition to the SAML subject (user ID). For more information, see *Extending an SP adapter contract* in the PingFederate documentation.
10. Click **Next**.
11. On the Summary screen, verify that the information is correct and click **Done**.
12. On the Manage Token Generator Instances screen, click **Save**.

Creating a custom authentication scheme for OAM

About this task

The Token Generator uses a custom authentication scheme when creating a WAM session and validates authentication requests coming from PingFederate. This section describes how to deploy the OAM-compatible Java-based PingFederate Custom Authentication Scheme.

Steps

1. From the `<token_translator_install_dir>/dist` directory, import the following file into the OAM:

   `PingCustomAuthPlugin.jar`

   The `PingCustomAuthPlugin.jar` file is a custom authentication scheme that supports OAM.
2. Configure your Access Server to use the custom authentication plug-in by creating or modifying a custom authentication scheme.

   Refer to *Oracle Support documentation* for additional information.

> ⓘ **Note:** The secret you specify when creating the custom authentication scheme must match the secret stored in the PingFederate Token Generator.

Using the STS client SDK

Ping Identity provides a Java STS-Client SDK for enabling Web Service applications (Client or Provider) to interact with the PingFederate STS. The SDK is available for download on the *PingFederate server add-ons page*.

The SDK provides functionality for sending a security token to the PingFederate STS for exchange with a returned SAML token, which can then be used to access Web Services across domains. The following code examples show how to send a token and request the exchange. Refer to the SDK documentation for modifications that apply to your site.

Token processor - sample code

The code snippet below demonstrates using the PingFederate Java STS Client SDK to send a WAM session token to the PingFederate STS.

```
// Example method for obtaining the WAM Session token.
// You will need to implement this for your environment.
String wamSessionToken = getWAMSessionToken();

// Configure STS Client (IdP side / SP Connection)
STSClientConfiguration stsConfig = new STSClientConfiguration();
stsConfig.setAppliesTo("http://sp.domain.com");
stsConfig.setStsEndpoint("https://idp.domain.com:9031/idp/sts.wst");
stsConfig.setInTokenType(TokenType.BINARY);

// Instantiate the STSClient
STSClient stsClient = new STSClient(stsConfig);

// Send an RST Issue request to PingFederate STS
Element samlToken = stsClient.issueToken(wamSessionToken);
```

Token generator - sample code

The code snippet below demonstrates using the PingFederate Java STS Client SDK to retrieve a WAM session token through the PingFederate STS.

```
// Configure STS Client (SP side / IdP Connection)
STSClientConfiguration stsConfig = new STSClientConfiguration();
stsConfig.setStsEndpoint("https://sp.domain.com:9031/sp/sts.wst");
stsConfig.setOutTokenType(TokenType.BINARY);

// Instantiate the STSClient
STSClient stsClient = new STSClient(stsConfig);

// Send an RST Issue request to PingFederate STS
Element wamsessionToken = stsClient.issueToken(samlToken);
```

Release notes

Changelog

Web Access Management Token Translator 2.0 – August 2014 (Current Release)

- Updated Token Translator with the WAM Agent Plugin 2.0

- Added “encode Token” field

Web Access Management Token Translator 1.2 – August 2013

- Updated Token Translator with the WAM Agent Plugin 1.2

Web Access Management Token Translator 1.1 – March 2013

- WAM Token Translator now includes WAM plug-in compatible with RSA Access Manager

Web Access Management Token Translator 1.0.1 – December 2012

- Updated to address security issues found since previous release
- Added support for OpenToken Adapter 2.5.1

Web Access Management Token Translator 1.0 – November 2012

- Initial Release
- Redesigned former product-specific kits to provide consistent functionality across multiple WAM products

Known issues and limitations

Known Limitations

- Due to a limitation with PingFederate 8.1 and earlier versions, when configuring two SP connections with the same provisioner, the second connection built may be pre-populated with the channel from the first connection. To avoid conflicts, delete this pre-populated channel and create a unique channel for each connection.

Download manifest

The distribution `.zip` archive for the WAM Token Translator contains the following:

- `ReadMeFirst.pdf` – contains links to this online documentation
- /legal – contains this document:
  - Legal.pdf – copyright and license information
- `/dist` – contains libraries needed to run the Token Translator:
  - `pf-wam-token-translator-2.0.jar` – the WAM Token Translator JAR file
  - `opentoken-adapter-2.5.1.jar` – OpenToken Adapter JAR file
- `/dist/oam` – contains Oracle Access Manager libraries needed to run the adapter:
  - `pf-oam-plugin.jar` – Pre-built OAM-compatible WAM plug-in JAR file
  - `PingCustomAuthPlugin.jar` – a Java-based PingFederate Custom Authentication Scheme
- `/dist/rsa` – contains RSA libraries needed to run the adapter:
  - `pf-rsa-plugin.jar` – Pre-built RSA-compatible WAM plug-in JAR file
  - `axm-runtime-api-6.1.4` - RSA API library
  - `jsafeFIPS-6.1.jar` – RSA API library
  - `jsafeJCEFIPS-6.1.jar` – RSA API library
- `/sdk` – contains build scripts, documents, libraries, and sample code to build a WAM plug-in:
  - `README.txt` – contains documentation on how to build a WAM plug-in
  - `/docs` – contains documentation on how to build a WAM plug-in
  - `/lib` – contains libraries and supporting files needed to build WAM plug-in
  - `/samples` – contains sample code used to build a WAM plug-in