PingFederate®

Agentless Integration Kit

Version 1.2

User Guide

Ping Identity®

PingFederate Agentless Integration Kit *User Guide*
Version 1.2
October, 2012

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

Phone: 877.898.2905 (+1 303.468.2882 outside North America)
Fax: 303.468.2909
Web Site: www.pingidentity.com

Trademarks

Disclaimer

This document is provided for informational purposes only, and the information herein is subject to change without notice. Ping Identity Corporation (“Ping”) owns or control all right, title and license in and to the Ping Agentless Integration Kit, including, but not limited to, all code samples and documentation provided therein (“the AIK”). Ping hereby grants you the limited, revocable, non-transferable, non-sublicensable, worldwide, non-exclusive right to use the AIK for development of software for use in connection with Ping Federate. Ping is providing the AIK “as is” without warranty of any kind and disclaims any responsibility for any harm resulting from your use of the AIK.

Contents

Introduction

The PingFederate Agentless Integration Kit includes the ReferenceID Adapter, which allows developers to integrate applications with a PingFederate server acting as either an Identity Provider (IdP) or a Service Provider (SP). The ReferenceID Adapter allows an IdP server to receive user attributes from an IdP application. On the SP side, the adapter allows an SP application to receive user attributes from the SP server.

The ReferenceID Adapter does not require the application to include *agent* PingFederate software libraries to interact with the Adapter. Instead, user attributes are passed via direct HTTP calls between the application and PingFederate.

For IdP integration, after user authentication, the application makes a direct HTTP call to PingFederate with user attributes, which PingFederate temporarily stores, sending a reference to them in the HTTP response. The IdP application redirects the browser to PingFederate, including the reference.

For SP integration, PingFederate parses the SAML assertion and temporarily stores the user attributes, generating a reference to them and sending the reference in a redirect to the SP application. The application makes a direct HTTP call back to PingFederate with the reference, and PingFederate returns the attributes in the HTTP response.

The sample distribution consists of two IdP and SP Java Web Applications and a PingFederate configuration archive, which enables the sample applications to work on a single instance of PingFederate. The Web Applications are implemented as Java Server Pages (JSP) so that the applications are easy to build and deploy, and provide a way to test an end-to-end Identity Provider (IdP) and Service Provider (SP) integration with PingFederate.

Intended Audience

This document is intended for PingFederate administrators and for Web-application developers with a working knowledge of Internet user authentication and HTTP transport methodology.

It is recommended that you review the PingFederate Administrator's Manual—specifically the information on adapters and integration kits. You should have an understanding of how PingFederate uses adapters and how they are configured. After the initial installation steps are followed in this Guide, it would also be helpful to complete the tasks in the Sample Applications section on page 18 to have a working example of a completed configuration.

System Requirements

The ReferenceID Adapter requires installation of PingFederate 6.x or higher.

ZIP Manifest

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

- `ReadMeFirst.pdf` – contains links to this online documentation.

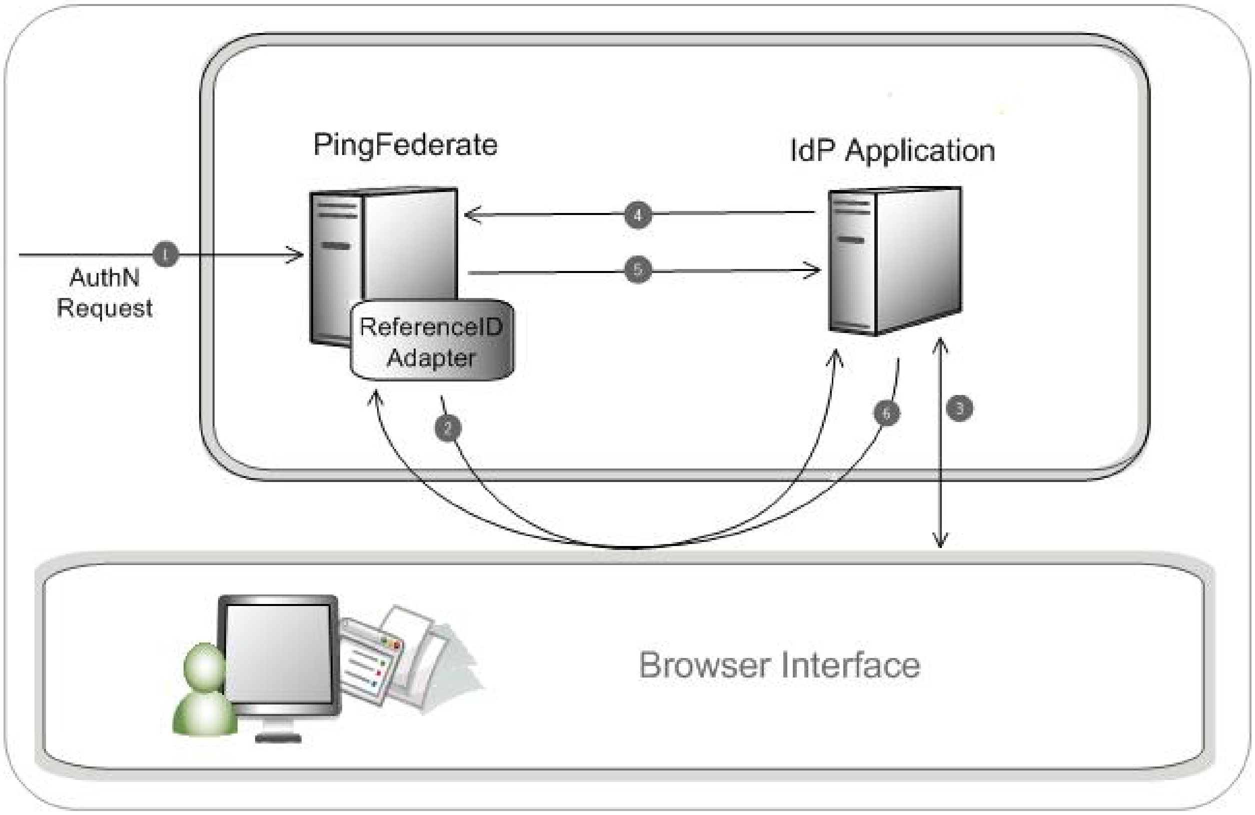
- `/legal` – contains this document:
    - `Legal.pdf` – copyright and license information
- `/dist` – contains the Java libraries needed to run the adapter:
    - `pf-referenceid-adapter-1.2.jar` – ReferenceID Adapter JAR file
    - `json_simple-1.1.jar` – JavaScript Object Notation (JSON) JAR file, used for attribute formatting (see Attribute Formatting on page 18).
- `/Samples` – contains sample applications demonstrating use of kit
    - `README.txt` – contains debugging tips and sample application design description
    - `data.zip` – PingFederate configuration archive for the Sample Applications
    - `AgentlessIntegrationKitSampleIdP` – contains Java Web application for sample IdP – JSP with Java code
    - `AgentlessIntegrationKitSampleSP` – contains Java Web application for sample SP – JSP with Java code
    - `/certificates` – contains Client SSL private certificate and key PKCS12 (`sampleClientSSLCert.p12`) file and the corresponding public certificate X509 file (`pfserverSSLCert.crt`)

Implementing IdP Functionality

The following figure displays an example SSO process flow between PingFederate and the IdP application using the ReferenceID Adapter. The figure illustrates an SP-initiated scenario, but IdP-initiated SSO would be similar and processing could be optimized.

IdP Process Overview

This section provides an overview of SSO processing using the IdP ReferenceID Adapter



Processing Steps

1. PingFederate receives an authentication request for a SAML assertion.
2. The PingFederate server redirects the browser to the IdP application for authentication, including the resume path as a query parameter.

   The server needs the resume path back from the application to continue SSO processing after the user authenticates.
3. The IdP application authenticates the user (if not already authenticated).

Note: The IdP applications must authenticate to PingFederate using one of three mechanisms. If authentication fails, the HTTP request results in an HTTP response 401 – Unauthorized status code message. See Authenticating to PingFederate on page 16.

4. The IdP application uses a direct HTTP call to send the user attributes (as JSON-encoded objects) to PingFederate. For example: `https://pingfederate.example.com:9031/ext/ref/dropoff`
5. PingFederate stores the attributes and returns a reference in the HTTP response to the IdP application. See Reference Value on page 17.
6. The IdP application redirects the browser to the PingFederate resume path (received in Step 2) with the reference in the query string. For example: `https://pingfederate.example.com:9031/[resume-path]?REF=<refid>`

Note: For IdP-initiated SSO, an optimized flow is possible where steps 1 and 2 above do not apply. In step 6, the IdP application includes the reference (from step 5) as a query parameter when sending the user to the PingFederate SSO endpoint. For example:
`https://pingfederate.example.com:9031/idp/startSSO.ping?<startSSO parameters>&REF=<refid>`

7. (Not shown) PingFederate creates a SAML assertion using the attributes associated with the ReferenceID and sends the assertion to the Service Provider.

IdP Adapter Installation and Setup

This section provides instructions for installation and setup of the ReferenceID Adapter in PingFederate.

To install the ReferenceID Adapter:

1. Stop the PingFederate server.
2. In the directory `<PF-install>/server/default/deploy`, delete the file `pf-referenceid-adapter-1.x.jar`, if it exists.
3. Unzip the distribution ZIP file.
4. From the integration-kit `dist` directory, copy *both* the `pf-referenceid-adapter-1.2.jar` and the `json_simple-1.1.jar` into:

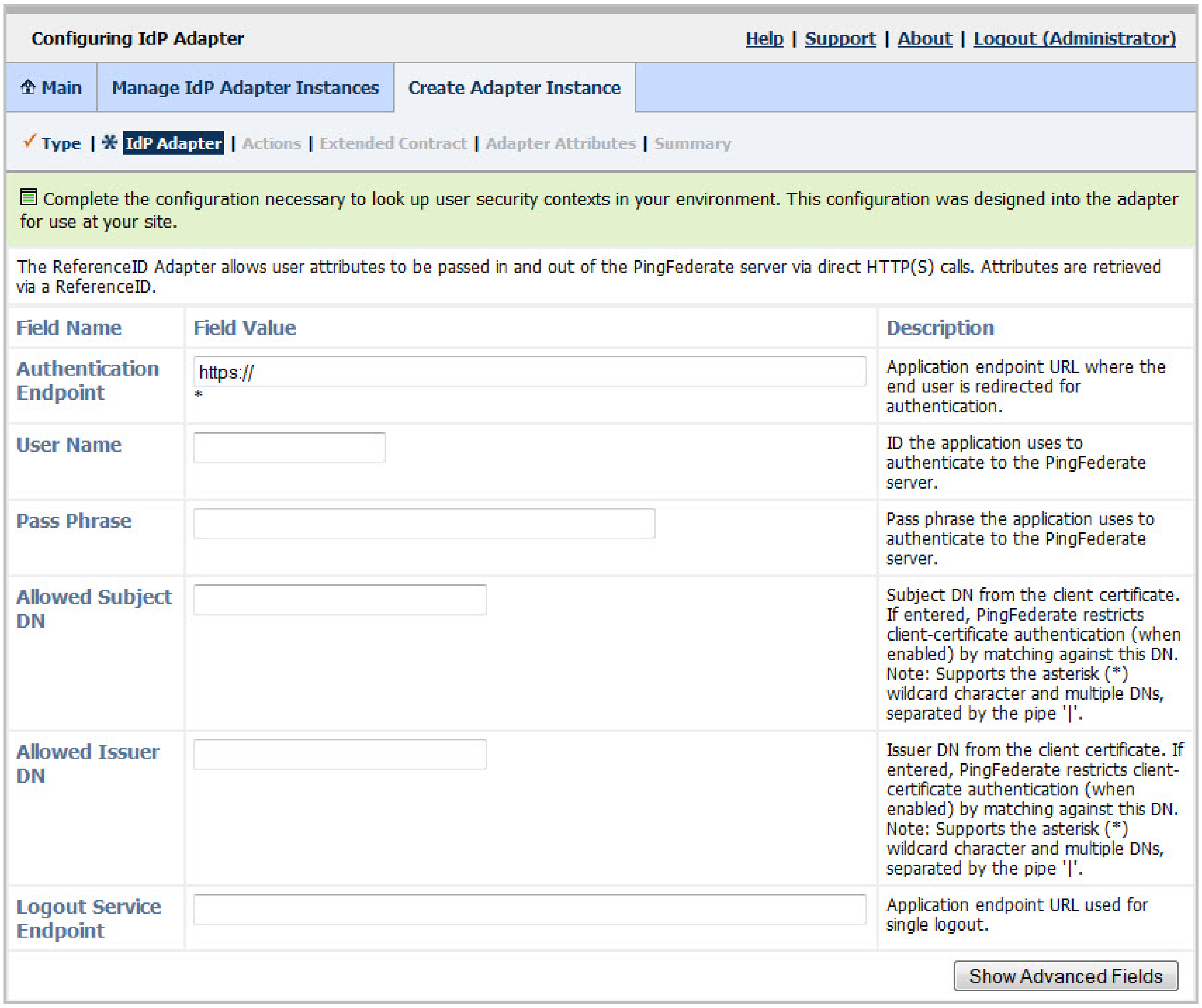
   `<PF-install>/server/default/deploy`
5. Start or restart PingFederate.

To setup the ReferenceID Adapter:

1. Log on to the PingFederate administrative console and click **Adapters** from the My IdP Configuration side of the Main Menu screen.

   Tip: You may skip this and subsequent steps in this setup if you want to install and deploy the sample applications first, before configuring the Adapter instance for your own application. The sample distribution (in the sample directory) contains a configuration archive that includes preconfigured ReferenceID Adapter instances for both the IdP and SP sample applications.

   For more information, see Configuring IdP Adapters in the PingFederate *Administrator's Manual*.
2. Click **Create New Instance**.
3. Enter the Instance Name and Instance Id. Select ReferenceID Adapter 1.2 as the Type and click **Next**.



Configuring IdP Adapter

Help | Support | About | Logout (Administrator)
Main
Manage IdP Adapter Instances
Create Adapter Instance
✓ Type | ✱ IdP Adapter | Actions | Extended Contract | Adapter Attributes | Summary

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.

The ReferenceID Adapter allows user attributes to be passed in and out of the PingFederate server via direct HTTP(S) calls. Attributes are retrieved via a ReferenceID.

Field Name	Field Value	Description
Authentication Endpoint	https:// *	Application endpoint URL where the end user is redirected for authentication.
User Name		ID the application uses to authenticate to the PingFederate server.
Pass Phrase		Pass phrase the application uses to authenticate to the PingFederate server.
Allowed Subject DN		Subject DN from the client certificate. If entered, PingFederate restricts client-certificate authentication (when enabled) by matching against this DN. Note: Supports the asterisk (*) wildcard character and multiple DNs, separated by the pipe '|'.
Allowed Issuer DN		Issuer DN from the client certificate. If entered, PingFederate restricts client-certificate authentication (when enabled) by matching against this DN. Note: Supports the asterisk (*) wildcard character and multiple DNs, separated by the pipe '|'.
Logout Service Endpoint		Application endpoint URL used for single logout.

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

Field Name	Description
Authentication Endpoint	Enter the application URL to which PingFederate redirects the end user for authentication.
User Name	Enter an ID for the application to use for authentication. **Note**: This field is optional if either Allowed Subject DN or Allowed Issuer DN is specified, which enables client-certificate authentication.
Pass Phrase	Use the next screen to display the clear-text value of the pass phrase you enter here, for copying to the application. **Note**: This field is optional if either Allowed Subject DN or Allowed Issuer DN is specified, which enables client-certificate authentication.
Allowed Subject DN	(Optional) To enable client-certificate authentication, specify an acceptable Subject DN of the client certificate. This field supports the asterisk (*) wildcard character in the Common Name (CN) and supports multiple Subject DN(s), separated by the pipe (|).

Field Name	Description
	Note: For information about configuring PingFederate to use this form of authentication in certain cases, see Using Mutual SSL and TLS Authentication on page 16. **Note:** To disable client-certificate authentication, see Disabling Certificate Authentication on page 21.
Allowed Issuer DN	(Optional) To enable client-certificate authentication, specify an acceptable Issuer DN of the incoming client certificate. This field supports the asterisk (*) wildcard character in the CN and supports multiple Issuer DN(s), separated by the pipe (|). See Using Mutual SSL and TLS Authentication on page 16.
Logout Service Endpoint	(Optional) Enter the IdP-application URL where the user can initiate SAML single logout (SLO). SLO allows a user to log out of both the IdP and the SP sites with one action (for more information, see Supported Standards in *Getting Started*). For more information, see Logout Mode in the table for Advanced Fields under the next step.

5. (Optional) Click **Show Advanced Fields** to view additional configuration settings.

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

Field Name	Description
Transport Mode	(Required) `Transport Mode` defines how the data (such as Reference ID) is transported to and from the application, either via a Query Parameter or as a Form POST (default). This is applicable to the **Front Channel** only. Form POST sends data using the POST request, and data resides within the body of the request. Query Parameter sends data along with the URL string, and the values are embedded within the query string. Data is exposed when transported using the Query Parameter option. The Agentless adapter uses the **Front Channel** to communicate to and from PingFederate. The **Back Channel** is used for direct requests to PingFederate for pick-up and drop-off transactions. Applications (such as the IdP and SP Samples for Agentless) make use of the **Back Channel**.
Reference Duration	PingFederate caches the reference and attributes for this minimum period of time. This field is provided for administrators to make adjustments, as needed, to address network latency issues.
Reference Length	Increasing the length of the reference makes it more difficult to replicate when security is a concern.
Require SSL/TLS	(Optional) We recommend using the secure transport protocol unless a secure, dedicated network segment exists between the application server and PingFederate.

Field Name	Description
Outgoing Attribute Format	As an option, you can change the format in which PingFederate encodes attribute values on the HTTP response to the application (see Attribute Formatting on page 18).
Incoming Attribute Format	As an option, you can change the format in which the application encodes attribute values on the HTTP request to PingFederate (see Attribute Formatting on page 18).
Logout Mode	Use these options to define how to handle application logout. **Front Channel** (the default) redirects the browser to the application endpoint, including the reference as a query parameter. When resolved, this reference gives all of the user attributes as well as the resume path for the application to use in a logout response. **Back Channel** sends a direct HTTP request from the server to the application. The variable `${attribute-name}` may be used for any attribute to build a dynamic URL.
Skip Host Name Validation	(Optional) Select the check box to skip host name validation, for example, when testing or when the host name validation cannot be performed.

6. Click **Next.**

7. (Optional) On the Actions screen, click **Show Pass Phrase**.

   Use this option to copy and paste the pass phrase into the application to facilitate HTTP Basic authentication between the application and the PingFederate server.

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 on using the Extended Contract screen, see Extending an Adapter Contract in the PingFederate *Administrator's Manual*.)

10. On the Adapter Attributes screen, select subject as the **Pseudonym**.

    Pseudonyms are opaque subject identifiers used for SAML account linking, which may not be applicable for many SP connections. To ensure correct PingFederate performance under all circumstances, however, a selection is required. (For information about account linking, refer to Account Linking in the PingFederate *Administrator's Manual*.)

11. (Optional) Select the **Mask Log Values** check box for each attribute you want to mask in the log file.

    Note: If OGNL expressions might be used to map derived values into outgoing assertions and you want those values masked, select the associated check box below the Attribute list. (For more information, see Using Attribute Mapping Expressions in the PingFederate *Administrator's Manual*.)

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

13. On the Manage IdP Adapter Instances screen, click **Save** to complete the Adapter configuration.

14. Configure or modify the connection(s) to your SP partner(s) using the ReferenceID Adapter Instance.

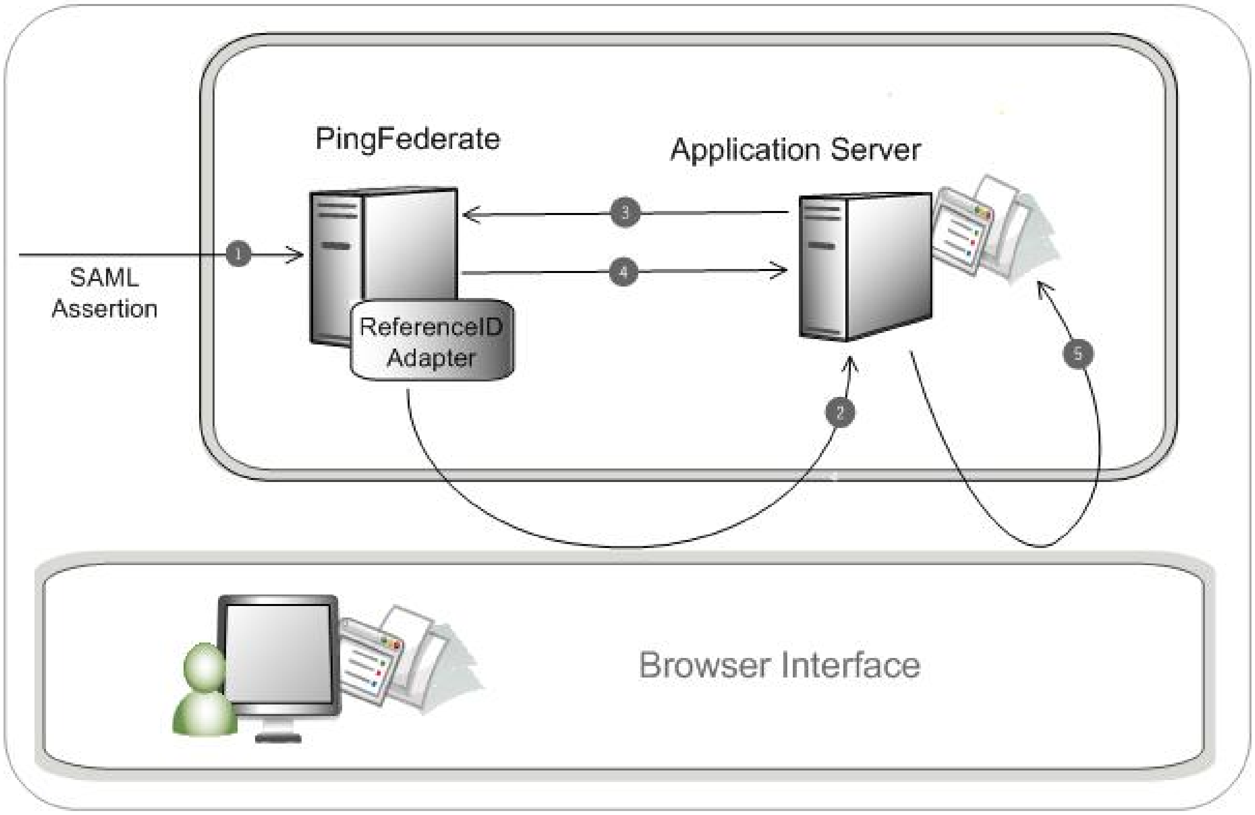
    For more information, see Identity Provider SSO Configuration in the PingFederate *Administrator's Manual.*

Implementing SP Functionality

The following figure displays a typical SSO process flow between PingFederate and the SP application using the ReferenceID Adapter.

SP Process Overview

This section provides an overview of SSO processing using the SP ReferenceID Adapter.



Processing Steps

1. PingFederate receives a SAML assertion from an IdP partner. The assertion is validated and parsed into the user attributes, which are temporarily maintained within PingFederate.
2. The PingFederate server redirects the user to the target SP application with a reference to the user attributes. The reference is included in the URL query string. For example: `https://target.example.com?REF=ABC123`

3. The target application makes an authenticated direct HTTP(S) call to PingFederate to retrieve the user attributes. For example:
   `https://pingfederate.example.com:9031/ext/ref/pickup?REF=ABC123`

Note: The applications must authenticate to PingFederate using one of three mechanisms. If authentication fails, the HTTP request results in an HTTP response 401 – Unauthorized status code message. See Authenticating to PingFederate on page 16.

4. PingFederate looks up the attributes (in the above example, referenced by ABC123) and provides them to the target application in the HTTP response. See Reference Value on page 17.
5. The target application uses the attributes to create a user session, enabling access to the target resource.

SP Installation and Setup

This section provides instructions for setting up the ReferenceID Adapter in PingFederate.

To install the ReferenceID Adapter:

1. Stop the PingFederate server.
2. In the directory `<PF-install>/server/default/deploy`, delete the file `pf-referenceid-adapter-1.x.jar`, if it exists.
3. Unzip the distribution ZIP file.
4. From the integration-kit `dist` directory, copy *both* the `pf-referenceid-adapter-1.2.jar` and the `json_simple-1.1.jar` into:

   `<PF-install>/server/default/deploy`
5. Start or restart PingFederate.

To setup the ReferenceID Adapter:

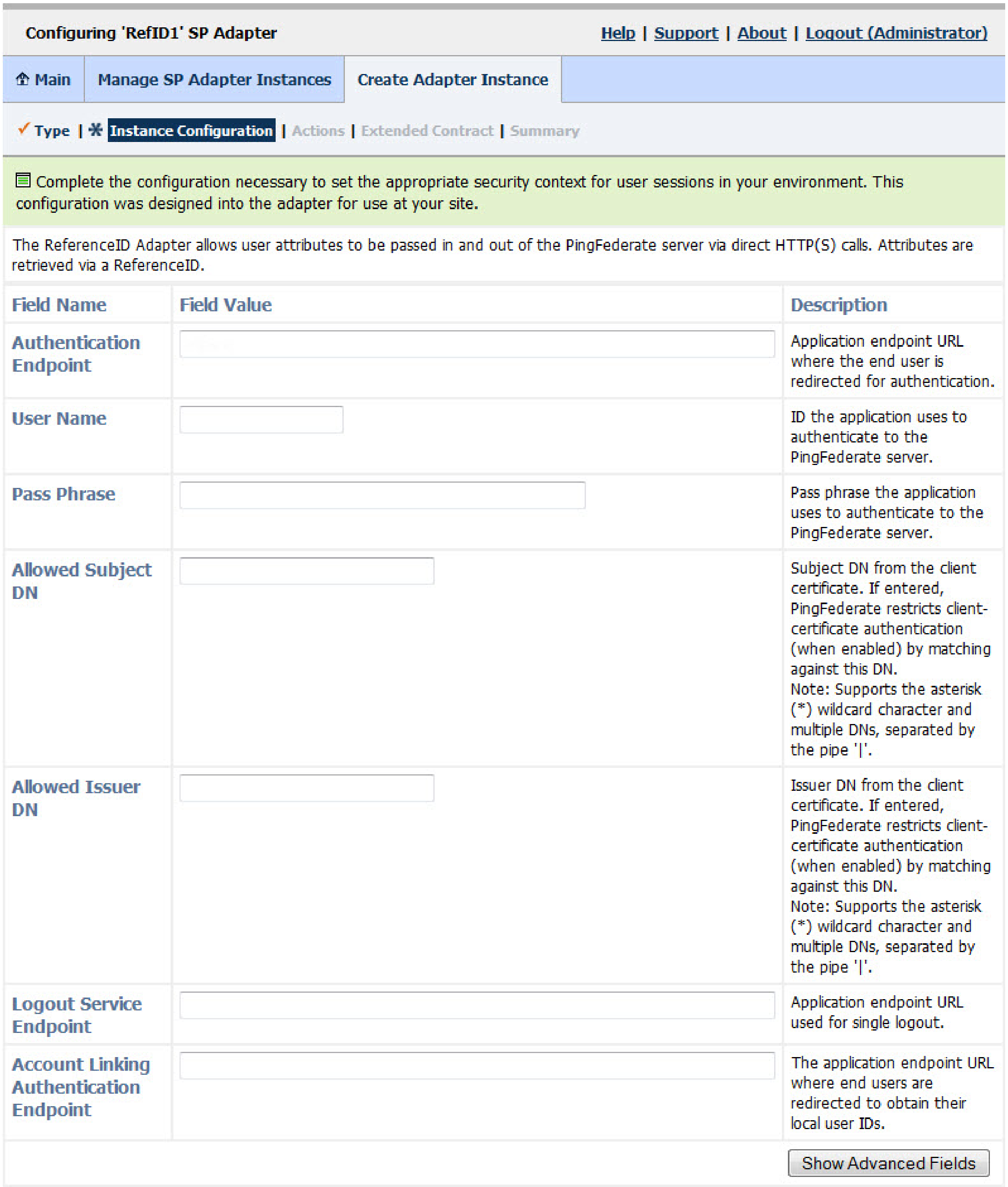
1. Log on to the PingFederate administrative console and click Adapters from the My SP Configuration side of the Main Menu screen.

Tip: You may skip this and subsequent steps in this setup if you want to install and deploy the sample applications first, before configuring the Adapter instance for your own application. The sample distribution (in the sample directory) contains a configuration archive that includes preconfigured ReferenceID Adapter Instances for both the IdP and SP sample applications.

For more information about SP adapters, see Configuring SP Adapters in the PingFederate *Administrator's Manual*.

2. Click **Create New Instance**.

3. Enter the Instance Name and Instance Id. Select ReferenceID Adapter 1.2 as the Type and click **Next**.



Configuring 'RefID1' SP Adapter
Help | Support | About | Logout (Administrator)
Main
Manage SP Adapter Instances
Create Adapter Instance
✓ Type | Instance Configuration | Actions | Extended Contract | Summary

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.

The ReferenceID Adapter allows user attributes to be passed in and out of the PingFederate server via direct HTTP(S) calls. Attributes are retrieved via a ReferenceID.

Field Name	Field Value	Description
Authentication Endpoint		Application endpoint URL where the end user is redirected for authentication.
User Name		ID the application uses to authenticate to the PingFederate server.
Pass Phrase		Pass phrase the application uses to authenticate to the PingFederate server.
Allowed Subject DN		Subject DN from the client certificate. If entered, PingFederate restricts client-certificate authentication (when enabled) by matching against this DN. Note: Supports the asterisk (*) wildcard character and multiple DNs, separated by the pipe '|'.
Allowed Issuer DN		Issuer DN from the client certificate. If entered, PingFederate restricts client-certificate authentication (when enabled) by matching against this DN. Note: Supports the asterisk (*) wildcard character and multiple DNs, separated by the pipe '|'.
Logout Service Endpoint		Application endpoint URL used for single logout.
Account Linking Authentication Endpoint		The application endpoint URL where end users are redirected to obtain their local user IDs.

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

Field Name	**Description**
Authentication Endpoint	Enter the application URL to which PingFederate redirects the end user for authentication. When specifying a reference to the SP Sample application as the default login service or as an authentication endpoint, use the following URL to ensure the attributes are picked up and successfully displayed: `https://localhost:9031/AgentlessIntegrationKitSampleSP/ShowAttributes.jsp`
User Name	Enter an ID for the application to use when retrieving referenced attributes from PingFederate. **Note**: This field is optional if either Allowed Subject DN or Allowed Issuer DN is specified, which enables client-certificate authentication.
Pass Phrase	Use the next screen to display the clear-text value of the pass phrase you enter here, for copying to the application. **Note**: This field is optional if either Allowed Subject DN or Allowed Issuer DN is specified, which enables client-certificate authentication.
Allowed Subject DN	(Optional) To enable client-certificate authentication, specify the acceptable Subject DN of the client certificate. This field supports the asterisk (*) wildcard character in the CN and supports multiple Subject DN(s), separated by the pipe (|). **Note**: For information about configuring PingFederate to use this form of authentication in certain cases, see Using Mutual SSL and TLS Authentication on page 16. **Note:** To disable client-certificate authentication, see Disabling Certificate Authentication on page 21.
Allowed Issuer DN	(Optional) To enable client-certificate authentication, specify the acceptable Issuer DN of the incoming client certificate. This field supports the asterisk (*) wildcard character in the CN and supports multiple Issuer DN(s), separated by the pipe (|). See Using Mutual SSL and TLS Authentication on page 16.
Logout Service Endpoint	(Optional) Enter the SP-application URL where the user can initiate SAML single logout (SLO). SLO allows a user to log out of both the IdP and the SP sites with one action (for more information, see Supported Standards in *Getting Started*). For more information, see Logout Mode in the table for Advanced Fields under the next step.
Account Linking Authentication Endpoint	(Optional) Enter the SP-application URL where incoming SSO users can access IDs for local accounts, via SAML account linking. (For information about account linking, see Account Linking in the PingFederate *Administrator's Manual*.)

5. (Optional) Click **Show Advanced Fields** to view additional configuration settings.

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

Field Name	Description
Transport Mode	(Required) `Transport Mode` defines how the data (such as Reference ID) is transported to and from the application, either via a Query Parameter or as a Form POST (default). This is applicable to the **Front Channel** only. Form POST sends data using the POST request, and data resides within the body of the request. Query Parameter sends data along with the URL string, and the values are embedded within the query string. Data is exposed when transported using the Query Parameter option. The Agentless adapter uses the **Front Channel** to communicate to and from PingFederate. The **Back Channel** is used for direct requests to PingFederate for pick-up and drop-off transactions. Applications (such as the IdP and SP Samples for Agentless) make use of the **Back Channel**.
Reference Duration	PingFederate caches the reference and attributes for this amount of time. This field is provided for administrators to make adjustments, as needed, to address network latency issues.
Reference Length	Increasing the length of the reference makes it more difficult to replicate when security is a concern.
Require SSL/TLS	(Optional) We recommend using the secure transport protocol unless a secure, dedicated network segment exists between the application server and PingFederate.
Outgoing Attribute Format	As an option, you can change the format in which PingFederate encodes attribute values on the HTTP response to the application (see Attribute Formatting on page 18).
Incoming Attribute Format	As an option, you can change the expected format in which the application decodes attribute values on the HTTP request to PingFederate (see Attribute Formatting on page 18).
Logout Mode	Use these options to define how to handle application logout. **Front Channel** (the default) redirects the browser to the application endpoint, including the reference as a query parameter. When resolved, this reference gives all of the user attributes as well as the resume path for the application to use in a logout response. **Back Channel** sends a direct HTTP request from the server to the application. The variable `${`*`attribute-name`*`}` may be used for any attribute to build a dynamic URL.
Skip Host Name Validation	(Optional) Select the check box to skip host name validation, for example, when testing or when the host name validation cannot be performed.

6. Click **Next.**

7. (Optional) On the Actions screen, click **Show Pass Phrase**.

   Use this option to copy and paste the pass phrase into the application to facilitate HTTP Basic authentication between the application and the PingFederate server.

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 on using the Extended Contract screen, see Extending an Adapter Contract in the PingFederate *Administrator's Manual.*)

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

11. On the Manage SP Adapter Instances screen, click **Save** to complete the Adapter configuration.

12. Configure or modify the connection(s) to your IdP partner(s) using the ReferenceID Adapter Instance.

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

Using Mutual SSL and TLS Authentication

In addition to Basic authentication, applications may use client-certificate authentication to communicate with PingFederate and the ReferenceID Adapter. To use this authentication for PingFederate 6.x and higher, the secondary SSL port must be configured, and application calls must use this port.

Your server may already be configured to use the secondary port for other back-channel SSO scenarios (for example, using SOAP). If not, follow this procedure:

1. In the `<pf-install>/pingfederate/bin` directory, open the file `run.properties` and change the `pf.secondary.https.port` value from `-1` to a valid port number.

   For more information about this property and related configuration settings, see Changing Configuration Parameters in the PingFederate *Administrator's Manual.*

2. Start or restart PingFederate.

Application Integration

This section provides information developers need to integrate applications with PingFederate and the ReferenceID Adapter.

Authenticating to PingFederate

Applications must authenticate to PingFederate using one of three mechanisms, listed below.

- Basic HTTP Authorization - Username and password (as specified in the ReferenceID Adapter configuration) sent as Basic HTTP Authorization header (base 64 encoded).

- Special request properties - Username and password sent via the special request properties `ping.uname` and `ping.pwd`. These special HTTP headers simplify integration on platforms that do not provide native base-64 encoding support.
- Trusted client certificates (as specified in ReferenceID Adapter configuration) - Client SSL private certificate and key PKCS12 (`sampleClientSSLCert.p12`) file and the corresponding public certificate X509 file (`pfserverSSLCert.crt`)

Either IdP or SP applications can authenticate to PingFederate via HTTP Basic authentication when making direct HTTP calls to drop off or pick up attributes. Additionally, the application may present a trusted client certificate to PingFederate (see Using Mutual SSL and TLS Authentication on page 16).

If authentication fails, the HTTP request results in an HTTP response 401 – Unauthorized status code message.

Reference Value

The reference value is a long hexadecimal String. Length is determined by the Reference Length setting in the ReferenceID Adapter configuration. The default is 30 bytes.

Example: "`A9C020F7CF8C21002CDC774B48A7CFE6B3ECA5FC6CCA507EE419B4432DB`"

The reference value is short-lived (the default is three seconds) as specified by the Reference Duration setting in the ReferenceID Adapter configuration.

The reference value is specific to the instance of the ReferenceID Adapter that issued it. If the ReferenceID Adapter is used both for IdP and SP integration, for example, there are two distinct reference values.

The reference value is used only one time to prevent replay attacks. If the specified reference value is bad, the ReferenceID adapter returns an empty set of attributes.

PingFederate ReferenceID Adapter Endpoints

The PingFederate URL an application uses for dropping off attributes is:

```
http[s]://<pf-host>:<pf-port>/ext/ref/dropoff
```

The PingFederate URL an application uses for picking up attributes is:

```
http[s]://<pf-host>:<pf-port>/ext/ref/pickup
```

Using HTTPS

Due to the sensitive nature of the authentication information and user attributes, SSL/TLS should always be used for communication between the application and PingFederate unless a secure and dedicated network segment exists between them.

SSL/TLS is the default transport setting for the ReferenceID Adapter configuration.

Attribute Formatting

Attribute formatting specifies how attribute names and values are passed between the application and PingFederate. Attribute formatting options are provided in the Advanced Fields section of the adapter configuration. By default PingFederate formats outgoing attributes and parses incoming attributes using JSON, a standard data structure for sending attributes in HTTP requests and responses.

Outgoing Attributes

Outgoing attribute formatting specifies how attributes are encoded into the HTTP Response from PingFederate to the application at the pickup endpoint. This affects how the application parses the attributes from the HTTP response body. The default is JSON. Alternatively, the attributes can be encoded as Java Properties, allowing the application to use the `java.util.Properties` class to parse them.

Incoming Attributes

Incoming attribute formatting specifies how attributes are encoded into the HTTP Request from the application to the PingFederate dropoff endpoint. The default format is JSON, in which case the application writes the JSON representation of the attributes into the request body. Alternatively, the attributes can be formatted as Query Parameters, in which case they are passed as URL-encoded name/value query string parameters.

Sample Applications

This section provides instructions for installing, configuring, and using the sample Java applications bundled with the PingFederate Agentless Integration Kit. These sample applications provide a way to test an end-to-end Identity Provider (IdP) and Service Provider (SP) integration with PingFederate using this integration kit.

The sample distribution consists of two Java Web Applications and a PingFederate configuration archive which enables the sample applications to work on a single instance of PingFederate. The Web Applications are implemented as JavaServer Pages (JSP) so that the applications are easy to build and deploy, and the source can be readily viewed by developers.

Note: The purpose of these samples is to demonstrate the use of the Agentless Integration Kit and is not intended as best practices for application development. For the sake of simplicity, the sample applications are not complete in terms of configurability, error handling, input validation, robustness, completeness, security, nor performance. It is assumed that the user is reasonably familiar with Java and PingFederate.

System Requirements for the Sample Applications

The following software must be installed in order to run the Agentless sample applications:

- Agentless Integration Kit 1.2
- PingFederate 6.x or higher
- JavaScript-enabled Web browser

Installation

The sample application distribution is located in the `<integration_kit_install_dir>/sample` directory and consists of:

- Two Web Application Archive folders containing the IdP and SP sample applications (`AgentlessIntegrationKitSampleIdP` and `AgentlessIntegrationKitSampleSP`)
- A `data.zip` file containing the PingFederate server configuration necessary to support the sample applications

  Note: This configuration archive assumes the PingFederate servlet container is hosting both sample applications.

- A certificates folder that contains the needed certificates

Installing the sample applications requires configuring PingFederate and deploying the applications, as described in the following sections.

Configuring PingFederate

Use the `data.zip` file to configure PingFederate automatically.

Caution: Deploying `data.zip` overwrites any existing configuration settings. If you have configured adapters or connections outside the scope of this document, and you want to keep the settings, ensure that you archive them for later recovery. (For further details, see System Administration in the PingFederate *Administrator's Manual*.)

To configure PingFederate to use the sample applications:

1. Deploy the Agentless Integration Kit included in this distribution to PingFederate per instructions provided in this document.
2. Ensure the PingFederate server is running.
3. Copy the `data.zip` file into:

   `<pf_install_dir>/pingfederate/server/default/data/drop-in-deployer/`

   This step uses PingFederate's configuration-archive hot-deployment feature to set up the complete server configuration needed. The file is renamed with a timestamp when the configuration is deployed to the PingFederate server (the `drop-in-deployer` directory is checked frequently when the server is running).
4. Enable the secondary HTTPS port by setting the `run.properties pf.secondary.https.port` value to an appropriate port number for example, port `9032`. Restart PingFederate after changing this value.

Note: To simplify deployment, the `data.zip` archive configures a single PingFederate instance to serve both the IdP and SP roles. It automatically populates the IdP and SP ReferenceID Adapter with defaults values.

The default configuration (contained in `data.zip`) specifies username/password authentication and Certificate Authentication for both the IdP and SP. The certificates required by the sample applications are included in the `<integration_kit_install_dir>/sample/certificates` directory.

There are two files provided:

- `sampleClientSSLCert.p12` - the private certificate and key for use by the IdP and SP application
- `pfserverSSLCert.crt` - the public certificate used by PingFederate by default

Deploying the Sample Applications

1. Copy the `AgentlessIntegrationKitSampleIdP` and `AgentlessIntegrationKitSampleSP` folders into the directory: `<pf_install_dir>/pingfederate/server/default/deploy`
2. Modify the sample application configuration files (`configuration.jsp`) to point to the two certificate files in the `/sample/certificates/` directory. Modify the two constants `CLIENT_KEY_FILE_PATH` and `SERVER_CERTIFICATE_PATH`.

   This applies to the following two configuration files:

   ```
   <pf_install_dir>/pingfederate/server/default/
       deploy/AgentlessIntegrationKitSampleIdP/configuration.jsp
   ```

   ```
    <pf_install_dir>/pingfederate/server/default/
       deploy/AgentlessIntegrationKitSampleSP/configuration.jsp
   ```

Using the Sample Applications

The sample IdP and SP applications demonstrate both IdP-initiated and SP-initiated SSO to and from your PingFederate server. The IdP provides a pre-configured list of users and attributes that are passed to the SP, which displays them.

Running IdP-initiated SSO

1. Start the sample IdP using the following entry point URL: `https://localhost:9031/AgentlessIntegrationKitSampleIdP/`
2. Select a user and click **Login.**
3. Review or modify user attribute values and click **Submit**.

   The Service Provider page displays the picked-up attributes.

Running SP-initiated SSO

1. Start the sample SP using the following entry URL: `https://localhost:9031/AgentlessIntegrationKitSampleSP/` and click **Login**.
2. The IdP Select User Page is shown. Select a user and **Login**.
3. Review or modify user attribute values and click **Submit**.

   The Service Provider page displays the picked-up attributes.

Certificate Authentication Configuration

Configuring Certificate Authentication between the client application and the ReferenceID Adapter requires the following steps:

1. Store the Client SSL private certificate file (`sampleClientSSLCert.p12`) in the file system and specify the `configuration.jsp` file `CLIENT_KEY_FILE_PATH` constant. If the public certificate is not self-signed, additional public certificates may be needed to complete the trust chain.

   Import the public certificate into the PingFederate Trusted CAs list using the administrative console, along with any supporting certificates.

2. Store the PingFederate server public SSL certificate X509 (`pfserverSSLCert.crt`) file in the file system and point the `configuration.jsp` file constant `SERVER_CERTIFICATE_PATH` to the SSL certificate X509 file.

3. Enable PingFederate to use a secondary SSL port. In the `run.properties` file, set property `pf.secondary.https.port` to the appropriate port for example, `9032`. The default value is -1.

   Set the Samples `configuration.jsp` to the same port value.

4. Modify the Samples `configuration.jsp` constants `PF_SECONDARY_SSL_PORT` and `CLIENT_KEY_FILE_PATH.`

   Set `CLIENT_KEY_FILE_PASSWORD` and `SERVER_CERTIFICATE_PATH` appropriately and set `CERTIFICATE_AUTHENTICATION` to `True`.

   Set the constant `SKIP_HOSTNAME_VERIFICATION` to `True` if the URL's hostname and the server's identification hostname mismatch, and you want to accept all hostnames.

5. Configure the ReferenceID Adapter to require a certificate by specifying the allowed subject and/or issuer DN using the administrative console.

Troubleshooting

Certificate Authentication SSL Validation

Certificates being used are not exempt from regular SSL certificate validation. Ensure that the certificate you are using as the client certificate is issued by a trusted Internet root CA, or alternatively, add the intermediate and root CA certificates that verify their authenticity.

Enabling Debug Messaging

To obtain a debug message, you need to enable the SSL Debugging property in the JVM options: `javax.net.debug=ssl` or `javax.net.debug=all`

You may need to run PingFederate in a console, or the messages appear in the server log. Restart PingFederate for this change to take effect.

Disabling Certificate Authentication

This section provides instructions for disabling Certificate Authentication for the Agentless Sample Applications.

To disable Certificate Authentication:

A user would need to perform the following steps:

1. Set the `CERTIFICATE_AUTHENTICATION` flag to `False` in `configuration.jsp` in both the IdP and SP sample applications.
2. Remove the value in Allowed Subject DN and Allowed Issuer DN in the Agentless Adapter configuration for both the IdP and SP sides.