PingFederate®

CoreBlox Integration Kit

Version 2.2

User Guide

Ping Identity®

PingFederate CoreBlox Integration Kit *User Guide*
Version 2.2
November, 2015

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

The information provided in this document is provided "as is" without warranty of any kind. Ping Identity disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Ping Identity or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Ping Identity or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Document Lifetime

Ping Identity may occasionally update online documentation between releases of the related software. Consequently, if this PDF was not downloaded recently, it may not contain the most up-to-date information. Please refer to documentation.pingidentity.com for the most current information.

From the Web site, you may also download and refresh this PDF if it has been updated, as indicated by a change in this date: **November 11, 2015**

Contents

Introduction

The PingFederate CoreBlox Integration Kit allows PingFederate administrators to integrate their applications protected by a CoreBlox Token Service (CTS) with a PingFederate server acting as either an Identity Provider (IdP) or a Service Provider (SP). The CoreBlox 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 CoreBlox domain to partner applications. The CoreBlox 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 CTS.

Intended Audience

This document is intended for system administrators with experience in the configuration of PingFederate adapters and an understanding about the CTS. Please consult the "CoreBlox Token Service Install and Configuration Guide" for additional information regarding the CTS.

We recommend 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.

ZIP Manifest

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

- `ReadMeFirst.pdf` – contains links to this online documentation
- `/legal` – contains the legal information:
  - `Legal.pdf` – copyright and license information
- `/dist` – contains libraries needed to run the adapter:
  - `coreblox-integration-kit-2.2.jar` – CoreBlox Adapter JAR file

System Requirements

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

- PingFederate 6.10 (or higher)
- A CTS acting as a secure token service between PingFederate and a policy server.

Installation and Setup

The following section describes how to install and configure the CoreBlox Adapter for both an IdP and an SP.

Installing the CoreBlox Adapter in PingFederate

1. Stop the PingFederate server if it is running.
2. Remove any existing CoreBlox Adapter files (`coreblox-integration-kit-*.jar`) from the directory:

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

3. Unzip the integration-kit distribution file and copy `coreblox-integration-kit-2.2.jar` from the `/dist` directory to the PingFederate directory:

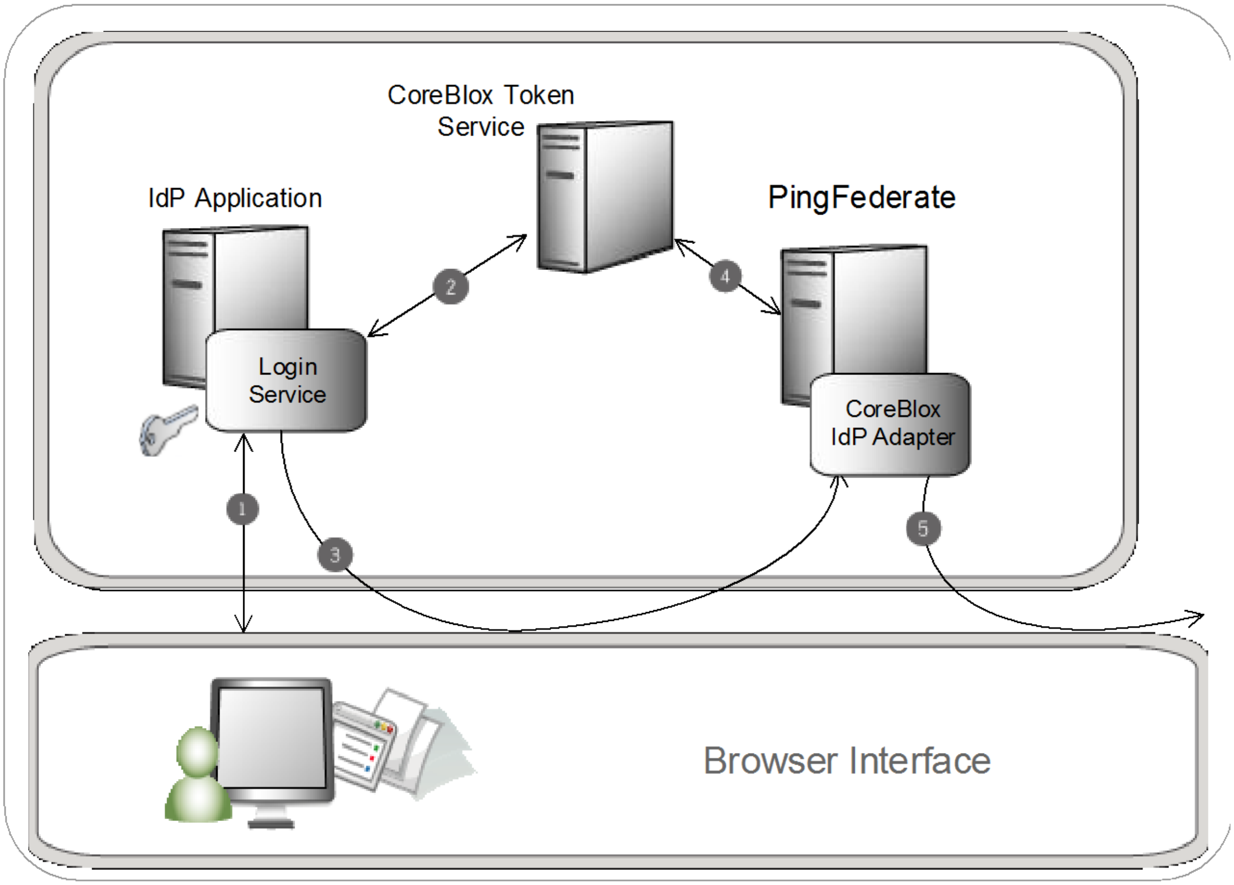
   ```
   <PF_install>\pingfederate\server\default\deploy
   ```

4. Start or restart the PingFederate server.

Implementing IdP Functionality

This CoreBlox IdP adapter uses the CTS to make requests for validating and authorizing tokens for use with the PingFederate server. You may add additional attribute values to the attribute contract in the PingFederate administrative console and transfer them to a partner application in a SAML or WS-Federation assertion (see Defining an Attribute Contract in the PingFederate *Administrator's Manual*).

IdP Processing Overview



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

Processing Steps

1. A user initiates an SSO transaction by authenticating with the IdP.
2. The login service authenticates the user with the CTS and sets the session cookie in the browser.
3. PingFederate uses the session cookie to query the CTS.
4. The CTS returns the user attributes associated with the session token and the adapter wraps the user attributes defined in the contract in a SAML/WS-Federation assertion.
5. The assertion is redirected through the browser to the SP site.

Setting up the IdP Adapter

This section describes how to configure the CoreBlox IdP adapter.

1. Log-on to the PingFederate administrative console and click **Adapters** under IdP Configuration on the Main Menu.
2. On the Manage IdP Adapter Instances screen, click **Create New Instance**.

3. On the Type screen, enter an Instance Name and Instance Id. The Instance Name is any name you choose for identifying this Adapter Instance.

   Note: The Instance Id is used internally and may not contain any spaces or non-alphanumeric characters and must be uniquely named.

4. Select CoreBlox IdP Adapter 2.2 as the Type and click **Next**.
5. Provide entries on the IdP Adapter screen as described below:

Field	**Description**
CoreBlox URL	The base URL for CTS requests.
Validate CoreBlox Certificate Hostname	If checked, the hostname of the server certificate presented by the CTS must match the hostname of the CoreBlox URL.
Client Certificate	The certificate used for authentication calls to the CTS.
CoreBlox Tokentype	The tokentype to be returned from the CTS. **Note:** At time of writing, the only permissible value is `SMSESSION`.
Cookie Name	The cookie name to be used when reading and writing cookies that contains the token to be used with the CTS.
Cookie Domain	The domain name to be used when writing cookies back to the response. The browser compares this value to the domain of subsequent requests to determine if the cookie should be submitted. **Note:** A blank value will use the domain name of the request. When sharing cookie across sub-domains, this value must be prefixed with a period.
Cookie Path	The path to be used when writing cookies back to the response. The browser compares this value to the path of subsequent requests to determine is the cookie should be submitted.
Cookie Secure Flag	If checked, cookies will be written only with URLs using `https://` requests.
Error URL	A URL used for redirecting users if there are errors. This URL may contain query parameters. The URL has an `errorMessage` appended to it, which contains a brief description of the error that has occurred.
Logged-out Cookie Value	The expected value of the cookie when the user has been logged-out.
HTTP Only Flag	Sets a flag on the cookie so that it can only be read via http requests, and prevents Javascript access. **Note**: Not all browsers respect the HTTP Only flag.

Field	Description
Login URL	An optional URL for the authentication service. **Note:** If the cookie is not found in the request, PingFederate redirects the request to this URL along with the relative resume path.
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.

6. (Optional) Click **Show Advanced Fields** to specify the adapter's authorization configuration settings.

Field	Description
Perform Authorize Request	If checked, the adapter will make an authorize request to the CTS before accessing the protected resource. **Note:** The following three fields are required for the adapter to make the authorize request.
Resource	The resource that is protected by the agent.
Instance	Refers to the name of the agent instance.
Action	The action to take when evaluating requests against the policy server.
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.
Cookie Provider URL	The URL for the cookie provider where PingFederate should redirect the request if the session cookie is in a separate domain.
Cookie Provider Target Parameter	The name of parameter used to send the return URL for cookie provider. This is required if there is a value in the Cookie Provider URL.

7. Click **Next**.

8. (Optional) On the Extended Contract screen, configure additional attributes for the adapter (See Key Concepts in the PingFederate *Administrator's Manual*).

9. Click **Next**.

10. On the Adapter Attributes screen, select the Pseudonym checkbox for the userId attribute. You may select any extended attribute specified on the previous screen. For more information about this screen, see Setting Pseudonym Values and Masking in the PingFederate *Administrator's Manual.*

11. Click **Next**.

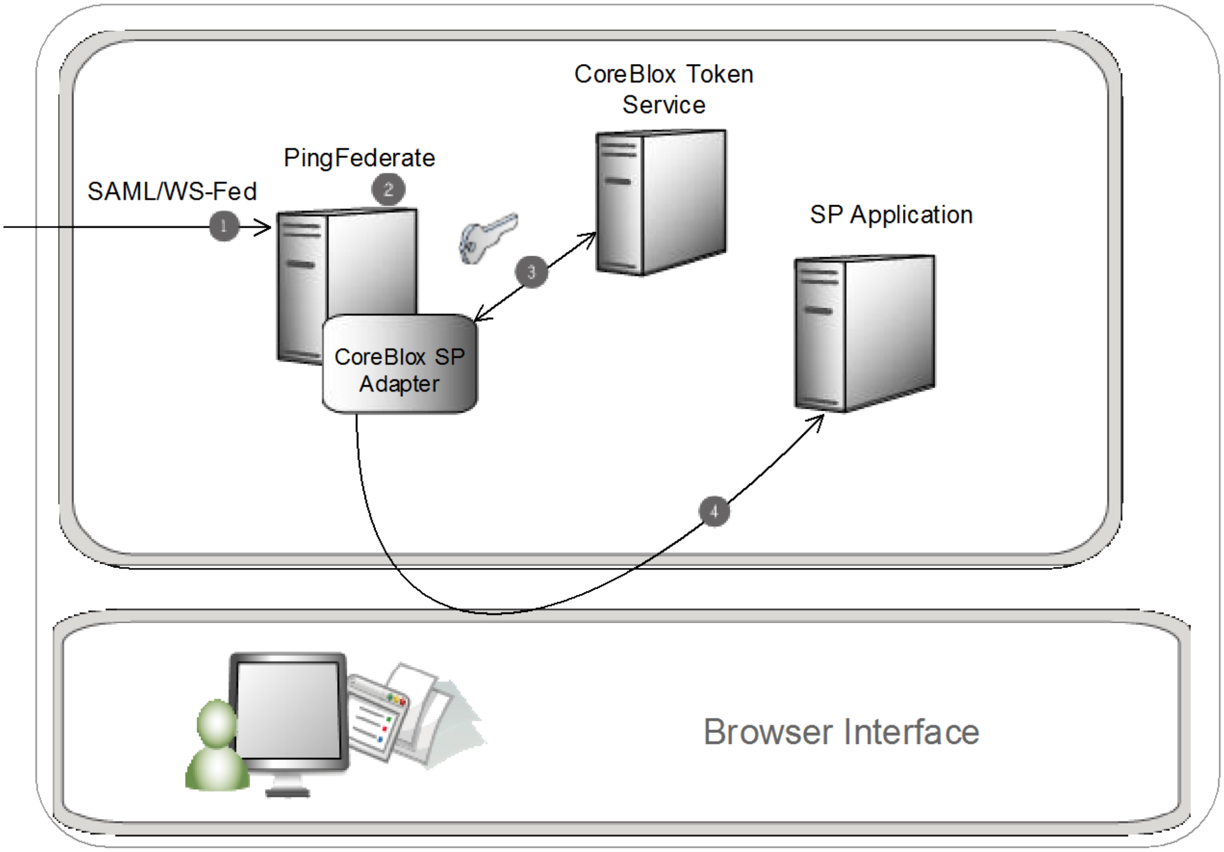
12. On the Summary screen, verify that the information is correct and click **Done**.

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

Implementing SP Functionality

The CoreBlox SP adapter uses the CTS to create a CoreBlox token based on the attributes received in the accepted assertion. After creating a new session, the adapter can be configured to authorize the token against a specific resource.

SP Processing Overview



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

Processing Steps

1. The PingFederate SP server recieves a SAML/WS-Federation assertion from the IdP.
2. PingFederate parses the assertion.
3. The CoreBlox SP Adapter uses the attributes available in the assertion to create and authorize a session with the CTS.
4. A request containing the session is redirected to the browser.

Setting Up the SP Adapter

This section describes how to configure the CoreBlox SP adapter.

1. Log on to the PingFederate administrative console and click **Adapters** under SP Configuration on the Main Menu.

2. On the Manage SP Adapter Instances screen, click **Create New Instance**.

3. On the Type screen, enter an Instance Name and Instance Id. The Instance Name is any name you choose for identifying this Adapter Instance.

Note: The Instance Id is used internally and may not contain any spaces or non-alphanumeric characters and must be uniquely named.

4. Select CoreBlox SP Adapter 2.2 as the Type and click **Next**.
5. (Optional) On the SP Adapter screen, 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 SP Adapter, as described on the screen and in the table below:

Field	**Description**
CoreBlox URL	The URL for the CTS.
Validate CoreBlox Certificate Hostname	If checked, the hostname of the server certificate presented by the CTS must match the hostname of the CoreBlox URL.
Client Certificate	The certificate used for authentication calls to the CTS.
CoreBlox Tokentype	The tokentype to be returned from the CTS. **Note:** At time of writing, the only permissible value is `SMSESSION`.
Cookie Name	The cookie name to be used when reading and writing cookies that contains the token to be used with the CTS.
Cookie Domain	The domain name to be used when writing cookies back to the response. The browser compares this value to the domain of subsequent requests to determine if the cookie should be submitted. **Note:** A blank value will use the domain name of the request. When sharing cookie across sub-domains, this value must be prefixed with a period.
Cookie Path	The path to be used when writing cookies back to the response. The browser compares this value to the path of subsequent requests to determine is the cookie should be submitted.

Field	Description
Cookie Secure Flag	If checked, cookies will be written only with URLs using `https://` requests.
Error URL	A URL used for redirecting users if there are errors. This URL may contain query parameters. The URL has an `errorMessage` appended to it that contains a brief description of the error that has occurred.
Logged-out Cookie Value	The expected value of the cookie when the user has been logged-out.
HTTP Only Flag	Sets a flag on the cookie so that it can only be read via http requests, and prevents Javascript access. **Note**: not all browsers respect the HTTP Only flag.
Account Link URL	The URL which to redirect the user for Account Linking.

7. (Optional) Click **Show Advanced Fields** to configure authorization values and the sending of extended attributes or to specify OpenToken configuration values or settings.

Note: For more information, see OpenToken Adapter Configuration in the PingFederate *Administrator's Manual*.

Field	Description
Perform Authorize Request	If checked, the adapter will make an authorize request to the CTS before accessing the protected resource. **Note:** The following three fields, **Resource**, **Instance**, and **Action** are required for the adapter to make the authorize request.
Resource	The resource that is protected by the agent.
Instance	Refers to the name of the agent instance.
Action	The action to take when evaluating requests against the policy server.
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.
Cookie Provider URL	The URL for the cookie provider where PingFederate should redirect the request if the session cookie is in a separate domain.
Cookie Provider Target Parameter	The name of parameter used to send the return URL for cookie provider. This is required if there is a value in the Cookie Provider URL.
Send Extended Attributes	The method of sending extended attributes. **Note:** These attributes can be sent along with the request through browser cookies, query parameters, or through a form POST.

Field	**Description**
OpenToken Transfer Method	How the OpenToken is transferred, either via a cookie, as a query parameter, or through a form POST.
OpenToken Name	The name of the cookie or request attribute that contains the OpenToken. **Note:** This name should be unique for each adapter instance.
OpenToken Password	The password used for encrypting extended attributes.

8. Click **Next**.
9. (Optional) Download the opentoken properties file if extended attributes are being sent through opentoken. This file can be used to decode the opentoken containing extended attributes. For more information please refer to the Java Integration Kit User Guide.

Note: The CoreBlox adapter settings must be saved before the downloaded properties file will reflect changes.

10. (Optional) On the Extended Contract screen for a connection, configure additional attributes for the adapter. Any attributes configured in this step are added to the request header.
11. Click **Next**.
12. On the Summary screen, verify that the information is correct and click **Done**.
13. On the Manage SP Adapter Instances screen, click **Save** to complete the adapter configuration.

Deployment Notes

The following note provides additional information for using the CoreBlox Integration Kit:

- For the CoreBlox IdP adapter, any of the attributes listed under the "userAttributes" key returned from the CTS may be used to extend the attribute contract. In addition, as of version 2.0 of the CoreBlox integration kit, the "token" key may also be included in the extended attribute contract to include the token returned from the CTS in the SAML assertion.