

PingFederate[®]

CoreBlox Token Translator

Version 1.0

User Guide



© 2014 Ping Identity® Corporation. All rights reserved.

PingFederate CoreBlox Token Translator *User Guide*
Version 1.0
April, 2014

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

Ping Identity, the Ping Identity logo, PingFederate, PingOne, PingConnect, and PingEnable are registered trademarks of Ping Identity Corporation ("Ping Identity"). All other trademarks or registered trademarks are the property of their respective owners.

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: **April 25, 2014**

Contents

| | |
|--|----------|
| Introduction | 4 |
| Intended Audience | 4 |
| ZIP Manifest | 4 |
| System Requirements..... | 4 |
| Installation and Setup | 4 |
| Installing the CoreBlox Token Translator in PingFederate | 4 |
| Token Processor (IdP) Processing Overview | 5 |
| Configuring the IdP Token Processor | 6 |
| Token Generator (SP) Processing Overview..... | 7 |
| Configuring the SP Token Generator..... | 8 |
| Deployment Notes..... | 9 |

Introduction

The PingFederate CoreBlox Token Translator provides a Token Processor and Token Generator for use with the PingFederate's WS-Trust Security Token Service (STS). The Token Processor allows an Identity Provider (IdP) STS to validate and authorize a CoreBlox session token from a Web Service Client (WSC) and then map user attributes into a SAML token to a Web Service Provider (WSP). The Token Generator allows a Service Provider (SP) STS to issue a CoreBlox session token for a WSP, including mapped attributes from an incoming SAML token.

Intended Audience

This document is intended for system administrators with experience in the configuration and maintenance of PingFederate Token Translators and have an understanding about the CoreBlox Token Service (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 section on STS, for further information.

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-token-translator-1.0.jar` – CoreBlox Token Translator JAR file

System Requirements

The following software must be installed in order to implement the CoreBlox Token Translator:

- PingFederate 7.x (or higher)
- An installation either locally or remotely of a CTS

Installation and Setup

The following section describes how to install and configure the CoreBlox Token Processor and Token Generator for an IdP and an SP, respectively.

Installing the CoreBlox Token Translator in PingFederate

1. Stop the PingFederate server if it is running.

2. Remove any existing CoreBlox Token Translator files (coreblox-token-translator-*.jar) from the directory:

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

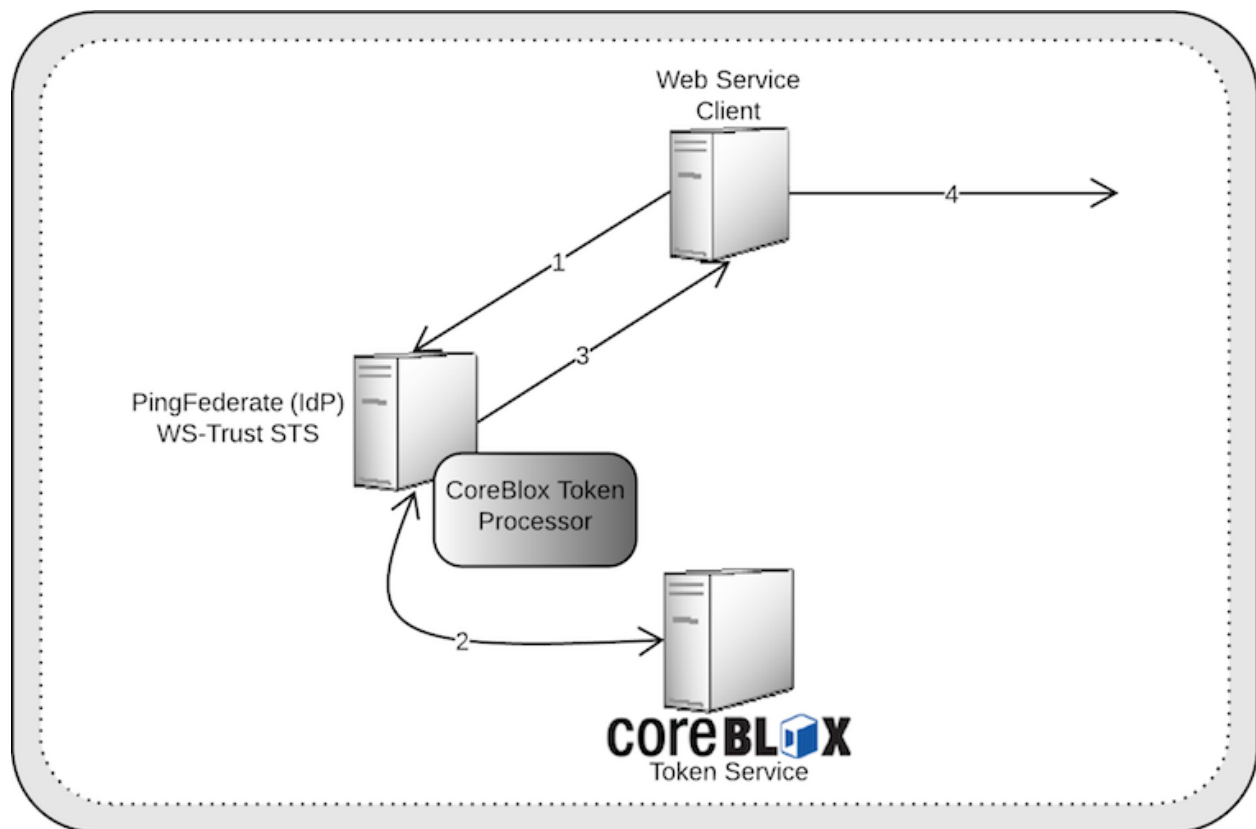
3. Unzip the distribution file and copy coreblox-token-translator-1.0.jar from the /dist directory to the PingFederate directory:

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

4. Start or restart the PingFederate server.

Token Processor (IdP) Processing Overview

The following figure illustrates how PingFederate and the Token Processor interacts with the CTS:



Processing Steps

1. A WSC sends a Request Security Token (RST) message containing a CoreBlox session token to the PingFederate STS IdP endpoint.
2. The CoreBlox Token Processor validates and authorizes the token from the WSC with the CTS and returns a valid token back to the Token Processor.
3. PingFederate STS embeds the mapped attributes in a SAML assertion wrapped in a Request Security Token Response (RSTR) back to the WSC.
4. The SAML assertion is sent to the WSP.

Configuring the IdP Token Processor

This section describes how to configure the CoreBlox Token Processor.

1. Log-on to the PingFederate administrative console and click **Token Processors** under IdP Configuration on the Main Menu.

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

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 Instance Name is any name you choose for identifying this Token Processor 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 Token Processor as the Type and click **Next**.
5. Provide entries on the Instance Configuration 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 and default value is <code>SMSESSION</code> . |

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

| Field | Description |
|---------------------------|---|
| Perform Authorize Request | If checked, the Token Processor 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. |

7. Click **Next**.

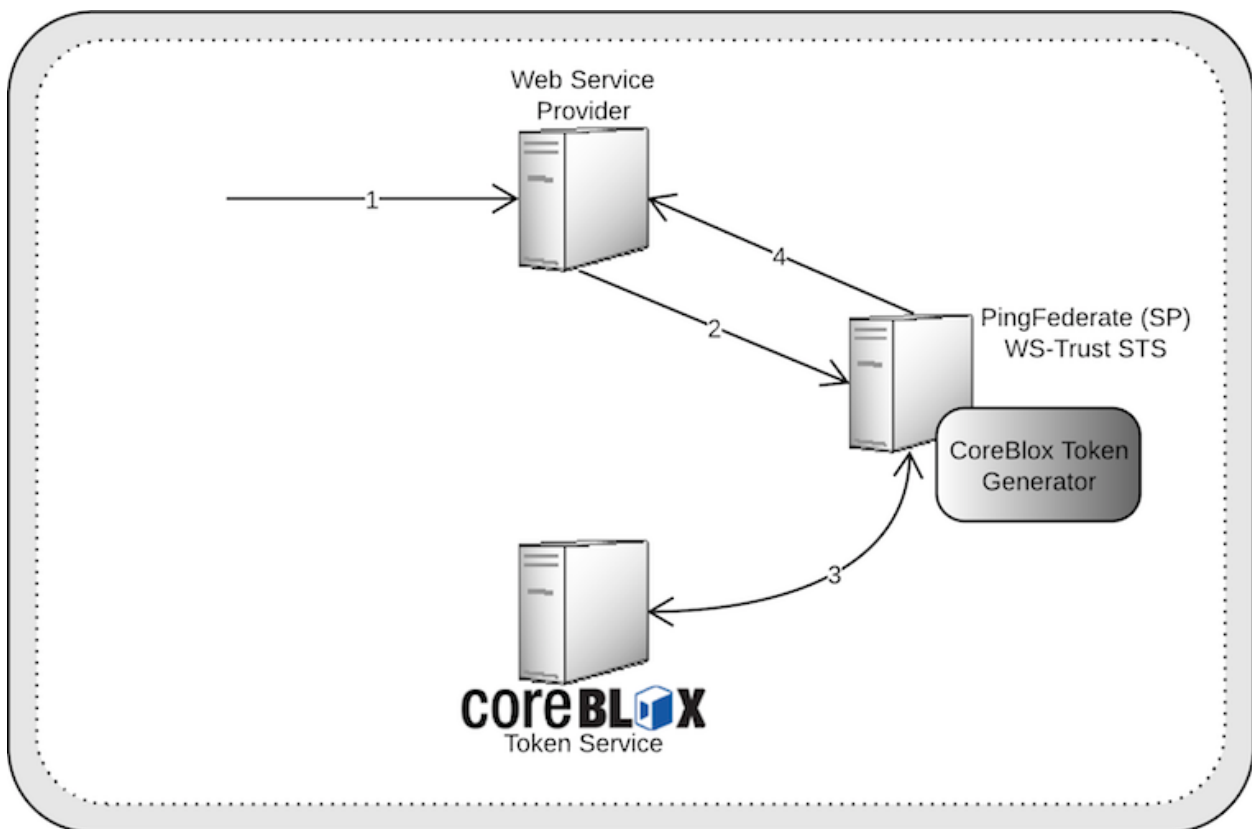
8. (Optional) On the Extended Contract screen, configure additional attributes for the adapter (See Key Concepts in the *PingFederate Administrator's Manual*).
9. Click **Next**.
10. On the Token Attributes screen, select the Pseudonym checkbox for the userId attribute. You may select any extended attribute 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 Token Processor Instances screen, click **Save** to complete the Token Generator configuration.

Token Generator (SP) Processing Overview

The following figure illustrates how PingFederate and the Token Generator interact with the CTS:



Processing Steps

1. The WSP accepts an incoming SAML assertion.
2. The WSP makes a RST to PingFederate STS.
3. The Token Generator parses the attributes in the SAML and queries the CTS for a valid token.

- The CoreBlox session token and mapped SAML attributes are embedded in a RSTR that is sent back to the WSP.

Configuring the SP Token Generator

This section describes how to configure the CoreBlox SP Token Generator.

- Log on to the PingFederate administrative console and click **Token Generators** under SP Configuration on the Main Menu.
- On the Manage Token Generator Instances screen, click **Create New Instance**.
- On the Type screen, enter an Instance Name and Instance Id. The Instance Name is any name you choose for identifying this Token Generator Instance.

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

- Select CoreBlox Token Generator X.0 as the Type and click **Next**.
- Provide entries on the Instance Configuration screen, as described 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. |

- (Optional) Click **Show Advanced Fields** to specify the Token Processor'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, 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. |

- Click **Next**.

8. (Optional) On the Extended Contract screen for a connection, configure additional attributes for the Token Generator. Any attributes configured in this step are added to the request header.
9. Click **Next**.
10. On the Summary screen, verify that the information is correct and click **Done**.

On the Manage Token Generator Instances screen, click **Save** to complete the Token Generator configuration.

Deployment Notes

- When configuring STS clients with PingFederate versions 6 or higher, a common issue with libraries parsing XML has been documented [here](#) with recommended steps to resolve it.