Ping Identity™

PingFederate®

ISAM Web IdP Adapter v1.2.7

User Guide

PingFederate ISAM Web IdP Adapter User Guide
Version 1.2.7
June 2018

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
USA

Phone: 877.898.2905 (+1 303.468.2882 outside North America)
Fax: 303.468.2909 E-mail: info@pingidentity.com
Web Site: http://www.pingidentity.com

Trademarks
Ping Identity, the Ping Identity logo, PingFederate, PingID, 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
This document is proprietary and not for general publication. It may be provided ad hoc for informational purposes only, and the information herein is subject to change without notice. Ping Identity does not provide any warranties and specifically disclaims any liability in connection with this document.

Note that Ping Identity may not provide support for any sample configurations provided in this document. The variability inherent among security environments prevents full testing and support for all possible platform configurations. If you need special assistance or would like to inquire about implementation or support programs, please contact Ping Identity Global Client Services (http://support.pingidentity.com).

Contents

Purpose

The PingFederate ISAM Web IdP Adapter allows developers and system administrators the ability to integrate their ISAM/TAM applications with a PingFederate server that acts as an Identity Provider. The ISAM IdP Adapter leverages SAML or WS-Federation protocols in order to integrate the ISAM/TAM domain to partner applications. This document will explain how to integrate ISAM/TAM with PingFederate.

Prerequisites

This document assumes that you already have the following installed and configured:

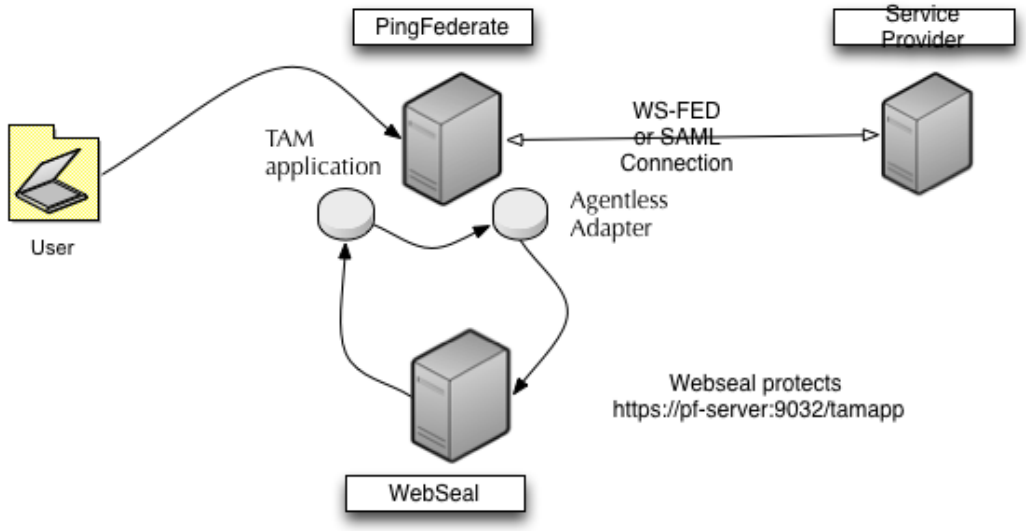
- A functional PingFederate environment, version 9.x+
- JDK version 8+
- ISAM/TAM environment

Installation

1. From the /dist folder in *pf-isam-web-idp-adapter-1.2.7.zip*, copy the noted files to the following directory in your PingFederate:
   - <PingFederateInstall>/pingfederate/server/default/deploy/
     - tamapp.war (entire folder and contents)
2. Follow the instructions under the ***Configuration*** section.
3. Repeat steps 1 and 2 on other clustered engine nodes.
4. Start or restart PingFederate.

Architecture

The following figure illustrates the architecture of ISAM/TAM solution.

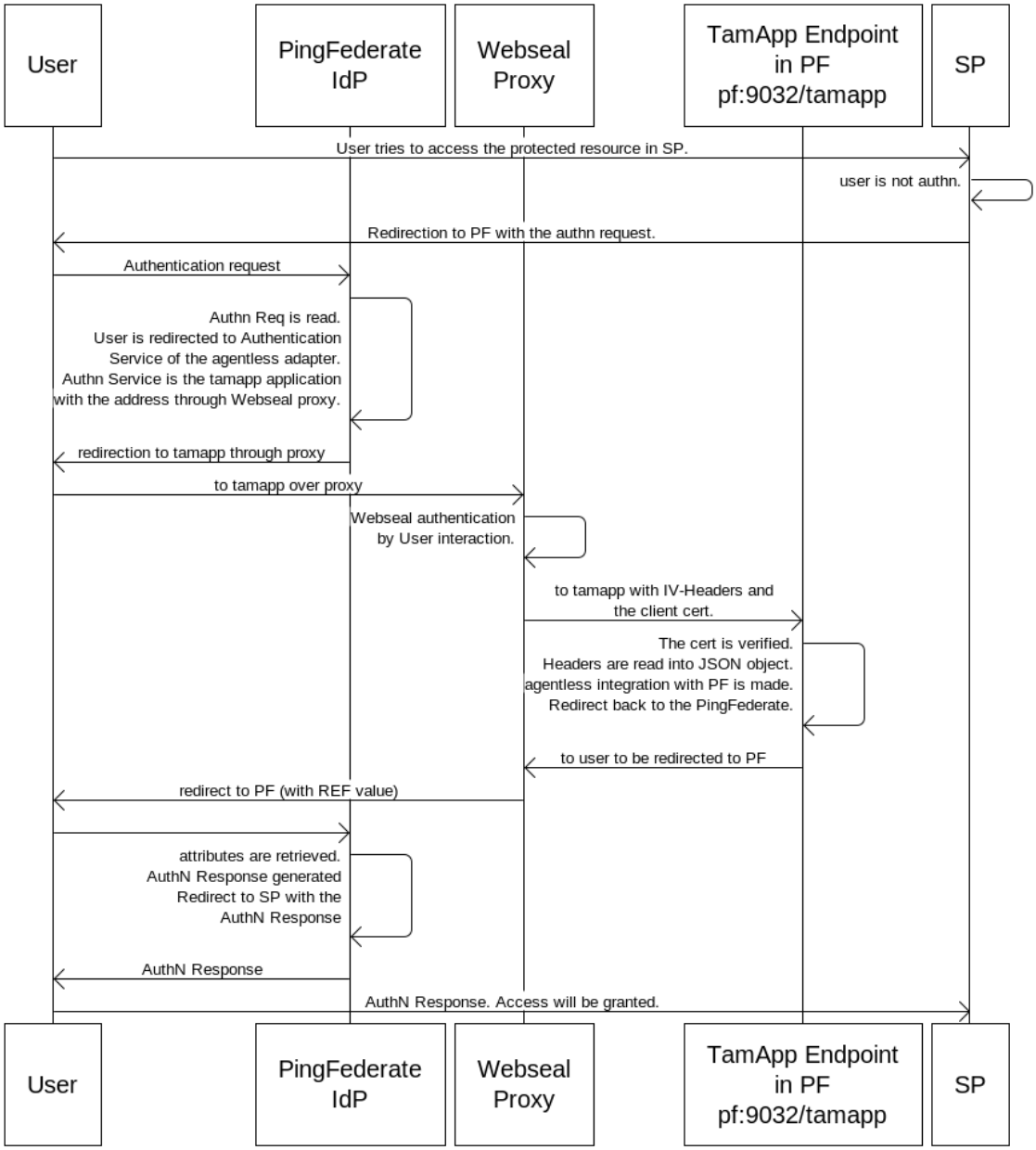


The following explains the workflow:

1. The user starts an IdP-init SSO process by using the ReferenceID (Agentless) Adapter. (It can be SP-init as well. The IdP will receive an authentication request from the Service Provider and the remaining flow will be the same).
2. The ReferenceID (Agentless) Adapter redirects the user to ISAM/TAM application through the WebSEAL proxy.
3. The user authenticates to WebSEAL, and reaches ISAM/TAM application.
4. The ISAM/TAM application passes attributes to the ReferenceID (Agentless) Adapter.
5. The authentication response (either SAML or WSFed assertion) is sent to the Service Provider.

Sequence Flow Diagram

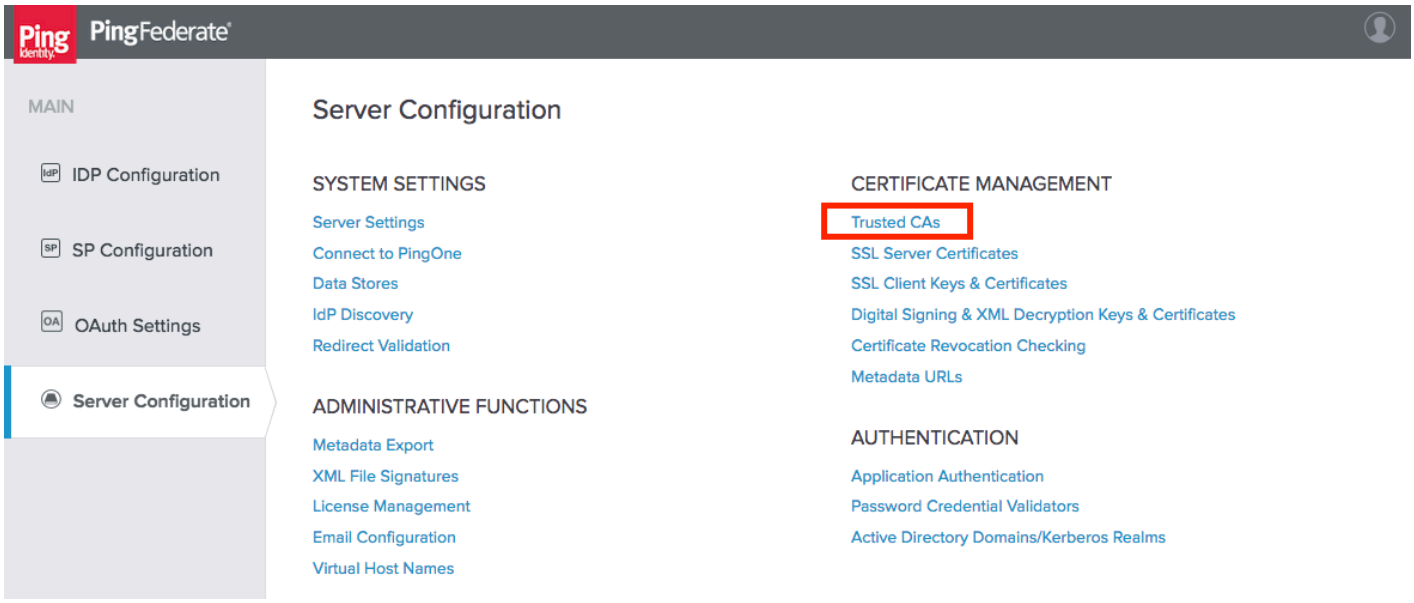
The sequence flow diagram for an SP-init SSO process can be found in the figure below. In this figure, mutual client certificate authentication is assumed to be enabled.



Configuration

Configuring the SSL Server Certificate

The SSL server certificate of PingFederate server should be put into the Trusted CAs store in PingFederate Admin Console (GUI) in order to provide the secure communication between the application and the adapter.



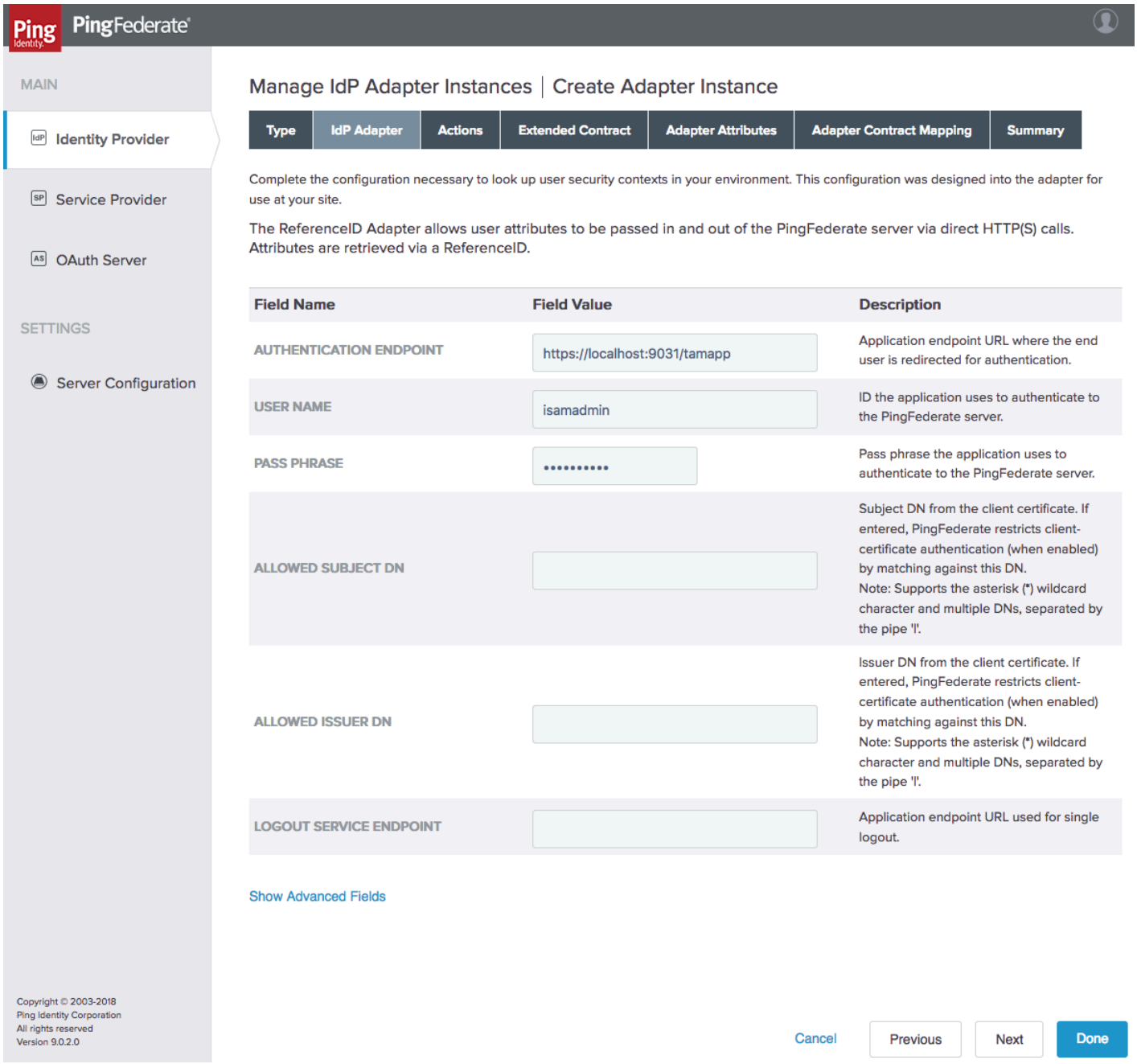
Configuring the Agentless Adapter

The connection that will do the first mile ISAM/TAM WebSEAL integration should have the ReferenceID (Agentless) Adapter as the mapped adapter.

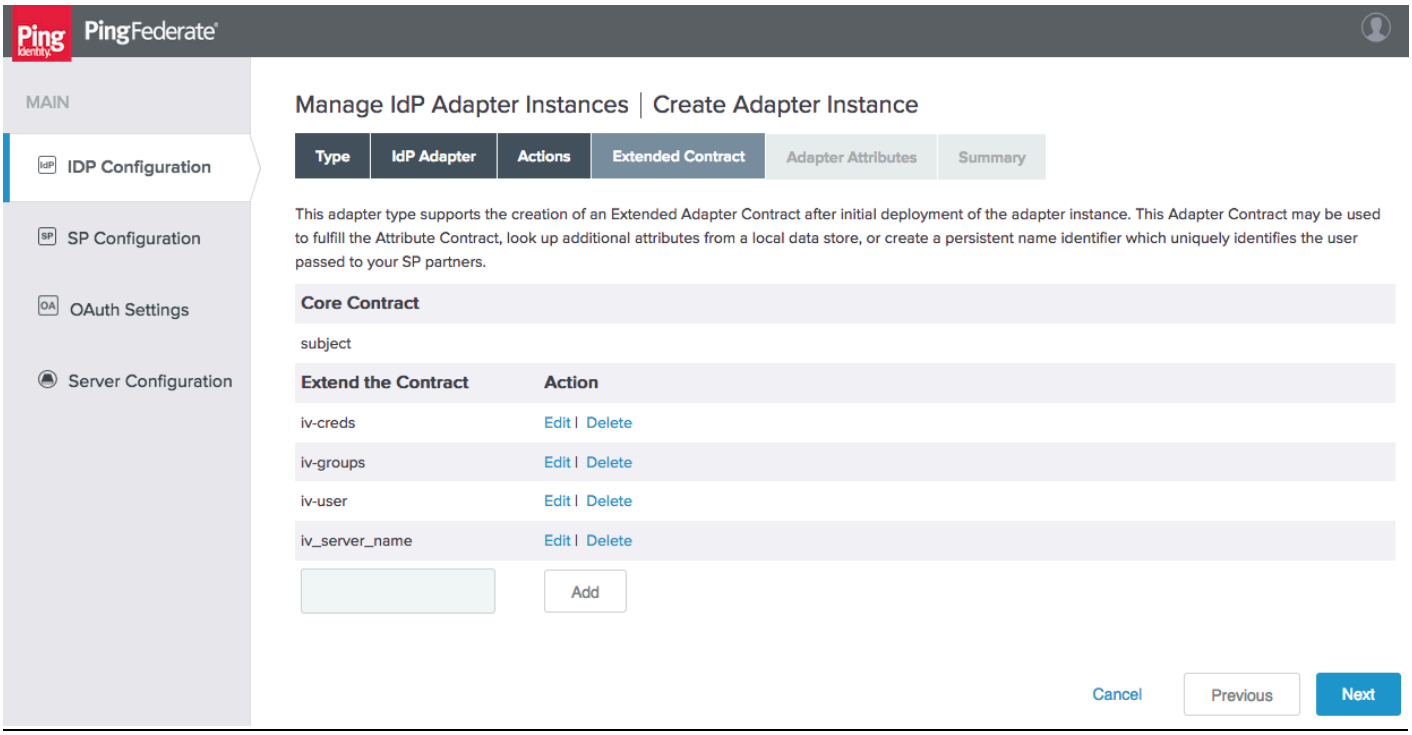
1. Log into PingFederate Administration and click on **Adapters** under **Identity Provider** >> **Application Integration**.
2. Click on **Create New Instance**.
3. Enter the **Instance Name**, **Instance ID**, and choose **Type** as **ReferenceID Adapter 1.2**, and click **Next**.
4. Enter the required fields for the adapter: **Authentication Endpoint**, **Username**, and **Pass Phrase**. Authentication service should point to the following *tamapp* endpoint through WebSEAL junction:

   https://[webseal host]/tamapp

   Username and password should be defined. These values and the adapter ID will be used in the configuration of the *tamapp* endpoint.



5. The desired IV-Headers should be entered as extended attributes in order to map them to the assertion in the SP connection. Please see the related figure below:



6. Adapter should be saved.

Modifying isamconfig.properties

1. Go to <YourPFInstall>/pingfederate/tamapp.war/WEB-INF/classes/isamconfig.properties
2. Modify the *isamconfig.properties* according to your environment. Below is an example of *isamconfig.properties*:

```
#[Required] The base URL of the PingFederate server.
pf.base.url=https://localhost:9031

#[Required] The back channel URL of the PingFederate server. In most cases it will be the same as base URL.
pf.back-channel.url=https://localhost:9031

#[Required] The username defined in the ReferenceID Adapter.
adapter.username=isamadmin

#[Required] The password defined in the ReferenceID Adapter.
#Obfuscate the password by running <YourPFInstall>/pingfederate/bin/obfuscate.sh [the password]
#The obfuscated password must be generated on the same PingFederate instance that the adapter is deployed on.
adapter.password=OBF:JWE:eyJhbGciOiJkaXIiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2Iiwia2lkIjoiMG1yRTNDZzZLYyIsInZl
cnNpb24iOiI4LjMuMS4zIn0..Lwpjcb1k-RO126Usay7fDA.PDdfT3fx5rUsEp53OFn99w.QOY-qGxkYN-x-p3wtFmGog

#[Required] The instance id of the ReferenceID Adapter.
adapter.id=ISAMRefIDIdPAdapter

#[Optional] if subject attribute is desired to be filled, the desired header name should be put
attribute.subject=iv-user

#[Required] It will always be set to iv for webseal, since user information comes as iv-header.
#1- If it is not defined at all, i.e. whole line is commented out, no values are passed. For this case attribute.subject value
should be configured.
#2- If it is left empty, i.e. no values after header.prefix=, then it is an empty filter which passes all header values. NOT
recommended.
header.prefix=iv
```

```
#[Optional] Is SSL enabled. Strongly recommended.
pf.requiressl=true

#[Optional]If it is set to true, then Client Cert Mutual Authentication is made. If it has another value or not set then it is not enabled.
pf.requiremutualauth=true

#[Optional] If Client Cert Mutual Authentication is enabled, checks if this value matches with the Subject DN of the incoming certificate.
pf.subjectdn=CN=sampleCN, O=sampleO, C=US

#[Optional] If Client Cert Mutual Authentication is enabled, checks if this value matches with the Issuer DN of the incoming certificate.
pf.issuerdn=CN=sampleCN, O=sampleO, C=US

#[Optional] Ignore URL validity check
ignoreURLValidCheck=false
```

3. Save the file.

Configuring WebSEAL

1. There should be a junction in WebSEAL configured for protecting https://<pf-server>:<port>/tamapp.
2. IV-Headers that will be used by PingFederate should be specified (i.e. iv-user, iv-groups, etc.)
3. PingFederate's SSL server certificate should be added to the trusted key store. (i.e., via gsk7ikm utility)

Enabling Mutual Authentication via Client Certificate

In order to enable Mutual Authentication via Client certificate between WebSEAL and the application, some additional configuration is required in PingFederate and in WebSEAL.

1. Make sure "WantClientAuth"property is set for the secondary HTTPS Connector in the *jetty-runtime.xml* file in the <PingFederateInstall>/pingfederate/etc/ directory:

```
<Call id="httpsSecondaryConnector" name="addConnector">
  <Arg>
    <New class="com.pingidentity.appserver.jetty.server.connector.ServerConnector">
      <Arg name="server"><Ref refid="RuntimeServer" /></Arg>
      <Arg name="acceptors" type="int"><Property name="ssl.acceptors" default="0"/></Arg>
      <Arg name="selectors" type="int"><Property name="ssl.selectors" default="1"/></Arg>
      <Arg name="factories">
        <Array type="org.eclipse.jetty.server.ConnectionFactory">
          <Item>
            <New class="org.eclipse.jetty.server.SslConnectionFactory">
              <Arg name="next">http/1.1</Arg>
              <Arg name="sslContextFactory"><Ref refid="secondarySSLContextFactory"/></Arg>
            </New>
          </Item>
          <Item>
            <New class="org.eclipse.jetty.server.HttpConnectionFactory">
              <Arg name="config"><Ref refid="sslHttpConfig"/></Arg>
            </New>
          </Item>
        </Array>
      </Arg>
```

```
            <Set name="host"><SystemProperty name="pf.engine.bind.address" default="0.0.0.0"/></Set>
            <Set name="port"><SystemProperty name="pf.secondary.https.port" default="-1" /></Set>
            <Set name="idleTimeout">30000</Set>
            <Set name="soLingerTime"><Property name="https.soLingerTime" default="-1"/></Set>
            <Set name="acceptorPriorityDelta"><Property name="ssl.acceptorPriorityDelta" default="0"/></Set>
            <Set name="selectorPriorityDelta"><Property name="ssl.selectorPriorityDelta" default="0"/></Set>
            <Set name="acceptQueueSize">512</Set>
            <Set name="WantClientAuth">true</Set>
          </New>
        </Arg>
      </Call>
```

2. Enable the secondary https port in the <YourPingFederateInstall>/pingfederate/bin/run.properties file by entering a valid/unused port number to pf.secondary.https.port parameter in the file. (i.e., pf.secondary.https.port=9032)

```
# This property defines the port on which PingFederate listens for
# encrypted HTTPS (SSL/TLS) traffic.

# Default is 9031.
pf.https.port=9031

# This property defines a secondary HTTPS port that can be used, for example,
# with SOAP or artifact SAML bindings or for WS-Trust STS calls.
# To use this port, change the placeholder value to the port number
# you want to use.
# Important: If you are using mutual SSL/TLS for either WS-Trust STS
# authentication or for SAML back-channel authentication, you must use this
# port for security reasons (or use a similarly configured new listener,
# with either "WantClientAuth" or "NeedClientAuth" set to "true".

pf.secondary.https.port=9032
```

3. Client certificate, which would be used by WebSEAL for mutual authentication should be added to Trusted CAs in PingFederate Admin Console
4. pf.requiremutualauth parameter should be set to true in the isamconfig.properties file. (pf.requiressl should be set to true if it is not already set as well.)
5. If additional Subject DN and Issuer DN matching will be made, required DN values should be configured in pf.subjectdn and pf.issuerdn parameters (please see ***Modifying isamconfig.properties***).

Configuring the Junction

1. The port for the junction should be pointing to the secondary https port. (i.e., port 9032). The junction type should be, at a minimum level of security, of type SSL.
2. The client certificate should be added to the WebSEAL keystore (i.e., via gsk7ikm utility).
3. Mutual authentication via client certificate should be enabled. (i.e. by adding –K <key_label> to the command creating the junction) or using the Web Portal Manager in ISAM.

Testing

1. Open a browser and go to the ISAM/TAM application and login with valid credentials.
   Results: The user should be able to login successfully.

2. Repeat the primary test case as defined above in a new browser session, but with invalid credentials.
   Results: The user should not be able to login successfully.

3. Repeat the primary test case as defined above, but in the same browser session.
   Results: The user should login successfully and seamlessly (will not need to re-enter valid credentials).

Logging

To enable logging in a separate log file (isamwebidpadapter.log) for the ISAM Web IdP Adapter, add the following to <PingFederateInstall>/pingfederate/server/default/conf/log4j2.xml (make sure a back up is made of this file prior to editing):

```
        <!-- ISAM Web IdP Adapter log : A time/date based rolling appender -->
        <RollingFile name="ISAMWebIdPAdapter"
fileName="${sys:pf.log.dir}/isamwebidpadapter.log"
            filePattern="${sys:pf.log.dir}/isamwebidpadapter.%d{yyyy-MM-dd}.log"
            ignoreExceptions="false">
            <PatternLayout>
               <!-- Uncomment this if you want to use UTF-8 encoding instead
                  of system's default encoding.
               <charset>UTF-8</charset> -->
               <pattern>%d %m%n</pattern>
            </PatternLayout>
            <Policies>
               <TimeBasedTriggeringPolicy />
            </Policies>
        </RollingFile>

        <Logger name="com.pingidentity.clientservices.product.adapter.idp.isam" level="DEBUG"
additivity="false" includeLocation="false">
            <appender-ref ref="ISAMWebIdPAdapter" />
        </Logger>
```

The ‘isamwebidpadapter.log’ will be created in <PingFederateInstall>/pingfederate/log upon usage.

Detailed training on using Log4j in PingFederate can be found at:
https://ping.force.com/Support/PingIdentityKnbSearchHome?searchText=log4j