THALES

PingFederate: Integration Guide

THALES LUNA HSM AND LUNA CLOUD HSM

Document Information

Document Part Number	007-000345-001
Revision	B
Release Date	18 August 2021

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Overview

PingFederate is an enterprise federation server and identity bridge for user authentication and standards-based single sign-on (SSO) for employee, partner, and customer identity types. PingFederate enables outbound and inbound solutions for SSO, federated identity management, customer identity and access management, mobile identity security, API security, and social identity integration. Browser-based SSO extends employee, customer, and partner identities across domains without passwords using standard identity protocols, such as SAML, WS-Federation, WS-Trust, OAuth, OpenID Connect, and System for Cross-domain Identity Management (SCIM). The benefits of securing the SSO signing and SSL keys within Luna HSM includes:

- Secure generation, storage, and protection of the signing private key on FIPS 140-2 level 3 validated hardware.
- Full life cycle management of the keys.
- Access to the HSM audit trail*.
- The advantage of cloud services with confidence.

*Luna Cloud HSM services do not have access to the secure audit trail.

Certified Platforms

Certified platforms for Luna HSM
Certified platforms for Luna Cloud HSM

Certified Platforms for Luna HSM

The following platforms are certified for integrating PingFederate with Luna HSM:

HSM Type	PingFederate Version	Platforms Certified
Luna SA 7.7.0 Firmware 7.7.0 Luna Client 10.3.0	PingFederate v10.3	RHEL 8.2
Luna SA 7.2.0 Firmware 7.2.0 Luna Client 7.2.0	PingFederate v9.2	RHEL 7.6 Windows Server 2016 Standard
Luna SA 6.3.0 Firmware 6.27.0 Luna Client 6.3.0	PingFederate v9.2	RHEL 7.6 Windows Server 2016 Standard

NOTE: PingFederate Integration is tested in HA as well as FIPS mode.

NOTE: Luna Client 10.3.0 must be installed to integrate PingFederate with JDK11.

Luna HSM: Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. Luna HSM on premise offerings include the Luna Network HSM, Luna PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

Certified Platforms for Luna Cloud HSM

The following platforms are certified for integrating Entrust with Luna Cloud HSM:

HSM Type	PingFederate Version	Platforms Certified
Luna Cloud HSM	PingFederate v9.2	RHEL 7.6 Windows Server 2016 Standard

Luna Cloud HSM: Luna Cloud HSM provides on-demand HSM and Key Management services through a simple graphical user interface. With Luna Cloud HSM, security is simple, cost effective and easy to manage because there is no hardware to buy, deploy and maintain. As an Application Owner, you click and deploy services, generate usage reports and maintain just the services you need.

Prerequisites

Before you proceed with the integration, complete the following tasks:

> Configure Luna HSM

> Configure Luna Cloud HSM Service

> Install PingFederate

Configure Luna HSM

To configure Luna HSM:

1. Ensure that the HSM is set up, initialized, provisioned, and ready for deployment. Refer to Luna HSM documentation for help.
2. Create a partition that will be later used by PingFederate.
3. Create and exchange certificate between the Luna Network HSM and Client system. Register client and assign partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition.

4. Ensure that the partition is successfully registered and configured. The command to see the registered partitions is:

```
# /usr/Luna/lunaclient/bin/lunacm

lunacm (64-bit) v10.3.0-275. Copyright (c) 2020 Luna. All rights
reserved.

Available HSMs:

Slot Id ->              0

Label ->                INTG_PF01

Serial Number ->        1213475834492

Model ->                LunaSA 7.7.0

Firmware Version ->     7.7.0

Bootloader Version ->   1.1.2

Configuration ->        Luna User Partition With SO (PW) Signing With
Cloning Mode

Slot Description ->     Net Token Slot

FM HW Status ->         FM Ready
```

5. For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

> **NOTE:** Refer to Luna HSM documentation for detailed steps about creating NTLS connection, initializing the partitions, and assigning various user roles.

Set up Luna HSM High-Availability

Refer to Luna HSM documentation for HA steps and details regarding configuring and setting up two or more HSM boxes on host systems. You must enable the HAOnly setting in HA for failover to work so that if the primary goes down due to any reason all calls automatically route to the secondary until the primary recovers and starts up.

Set up Luna HSM in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the Luna HSM in FIPS mode, you have to make the following change in the configuration file:

```
[Misc]
RSAKeyGenMechRemap=1
```

The above setting redirects the older calling mechanism to a new approved mechanism when Luna HSM is in FIPS mode.

> **NOTE:** The above setting is not required for Universal Client. This setting is applicable only till Luna Client 7.x.

Control User Access to the HSM

By default, only the root user has access to the HSM. You can specify a set of non-root users that are permitted to access the HSM by adding them to the hsmusers group. The client software installation automatically creates the hsmusers group. The hsmusers group is retained when you uninstall the client software. This allows you to upgrade your client software while retaining your hsmusers group configuration.

To add users to hsmusers group

To allow non-root users or applications access to the HSM, assign the users to the hsmusers group. The users you have assigned to the hsmusers group must exist on the client workstation. The HSM can be accessed only by the users whom you have added to the hsmusers group. To add a user to the hsmusers group:

a. Ensure that you have sudo privileges on the client workstation.

b. Add a user to the hsmusers group.

```
sudo gpasswd --add <username> hsmusers
```

where <username> is the name of the user you want to add to the hsmusers group.

To remove users from hsmusers group

To revoke a user's access to the HSM, you can remove them from the hsmusers group. To remove a user from the hsmusers group:

a. Ensure that you have sudo privileges on the client workstation.

b. Remove a user from the hsmusers group.

```
sudo gpasswd -d <username> hsmusers
```

where `<username>` is the name of the user you want to remove from the hsmusers group. To see the change, you need to log in again.

> **NOTE:** The user you delete will continue to have access to the HSM until you reboot the client workstation.

Configure Luna Cloud HSM Service

You can configure Luna Cloud HSM Service in the following ways:

> Standalone Cloud HSM service using minimum client package

> Standalone Cloud HSM service using full Luna client package

> Luna HSM and Luna Cloud HSM service in hybrid mode

> **NOTE:** Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Standalone Cloud HSM service using minimum client package

To configure Luna Cloud HSM service using minimum client package:

1. Transfer the downloaded .zip file to your client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

   ```
   [Windows]
   cvclient-min.zip
   [Linux]
   cvclient-min.tar
   # tar -xvf cvclient-min.tar
   ```

4. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

   ```
   [Windows]
   Right-click setenv.cmd and select Run as Administrator.
   [Linux]
   Source the setenv script.
   # source ./setenv
   ```

5. Run the LunaCM utility and verify the Cloud HSM service is listed.

Standalone Cloud HSM service using full Luna client package

To configure Luna Cloud HSM service using full Luna client package:

1. Transfer the downloaded .zip file to your client workstation using pscp, scp, or other secure means.
2. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

   ```
   [Windows]
   cvclient-min.zip
   [Linux]
   cvclient-min.tar
   # tar -xvf cvclient-min.tar
   ```

3. Run the setenv script to create a new configuration file having information required by Luna Cloud HSM service.

   ```
   [Windows]
   Right-click setenv.cmd and select Run as Administrator.
   [Linux]
   Source the setenv script.
   # source ./setenv
   ```

4. Copy the server and partition certificates from the Cloud HSM service client directory to Luna client certificates directory:

   NOTE: Skip this step for Luna Client v10.2 or higher.

   Cloud HSM Certificates:

   ```
   server-certificate.pem
   partition-ca-certificate.pem
   partition-certificate.pem
   ```

   LunaClient Certificate Directory:

   ```
   [Windows default location for Luna Client]
   C:\Program Files\Luna\Lunaclient\cert\
   [Linux default location for Luna Client]
   /usr/Luna/lunaclient/cert/
   ```

5. Open the configuration file from the Cloud HSM service client directory and copy the XTC and REST section.

   ```
   [Windows]
   crystoki.ini
   [Linux]
   Chrystoki.conf
   ```

6. Edit the Luna Client configuration file and add the XTC and REST sections copied from Cloud HSM service client configuration file.
7. Change server and partition certificates path from step 5 in XTC and REST sections. Do not change any other entries provided in these sections.

   NOTE: Skip this step for Luna Client v10.2 or higher.

   ```
   [XTC]
   . . .
   PartitionCAPath=<LunaClient_cert_directory>\partition-ca-certificate.pem
   PartitionCertPath00=<LunaClient_cert_directory>\partition-certificate.pem
   . . .

   [REST]
   . . .
   SSLClientSideVerifyFile=<LunaClient_cert_directory>\server-certificate.pem
   . . .
   ```

8. Edit the following entry from the Misc section and update the correct path for the plugins directory:

```
[Misc]

PluginModuleDir=<LunaClient_plugins_directory>

[Windows Default]

C:\Program Files\Luna\Lunaclient\plugins\

[Linux Default]

/usr/Luna/lunaclient/plugins/
```

   Save the configuration file. If you wish, you can now safely delete the extracted Cloud HSM service client directory.

9. Reset the ChrystokiConfigurationPath environment variable and point back to the location of the Luna Client configuration file.

   Windows

   In the Control Panel, search for "environment" and select Edit the system environment variables. Click Environment Variables. In both list boxes for the current user and system variables, edit ChrystokiConfigurationPath and point to the crystoki.ini file in the Luna client install directory.

   Linux

   Either open a new shell session, or export the environment variable for the current session pointing to the location of the Chrystoki.conf file:

```
# export ChrystokiConfigurationPath=/etc/
```

10. Run the LunaCM utility and verify that the Cloud HSM service is listed. In hybrid mode, both Luna and Cloud HSM service will be listed.

> **NOTE:** Follow the Luna Cloud HSM documentation for detailed steps for creating service, client, and initializing various user roles.

Configure Luna HSM and Luna Cloud HSM service in hybrid mode

To configure Luna HSM and Luna Cloud HSM service in hybrid mode, follow the steps mentioned under the Standalone Cloud HSM service using full Luna client package section above.

> **NOTE:** Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Use Luna Cloud HSM Service in FIPS mode

Cloud HSM service operates in both FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, enable the Allow non-FIPS approved algorithms check box when configuring your Cloud HSM service. The FIPS mode is enabled by default. Refer to the Mechanism List in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Install PingFederate

PingFederate server is based on J2EE application server technology. The user documentation for PingFederate is available at https://support.pingidentity.com/s/PingFederate-help. Please refer the documentation for installing the product, applying the license and initializing configuration required to start integrating with Luna HSMs. The PingFederate Administration Console will be accessible using the URL https://<pf_host>:9999/pingfederate/app.

> **Note:** For PingFederate 10.1 and earlier, the administrative console is accessed at https://<pf_host>:9999/pingfederate/app, where <pf_host> is the network address of your PingFederate server. It can be an IP address, a host name, or a fully qualified domain name. It must be reachable from your computer.

Integrating PingFederate with Luna HSM

This section describes how to integrate PingFederate with Luna HSMs. Luna HSM or Luna Cloud HSM Service integrates with PingFederate to secure the SSL certificate private key and SSO signing keys. For demonstration purpose, SSO feature is using Java Integration Kit deployed with PingFederate to show how to use Luna HSM generated keys for token signing.

> Configuring PingFederate with Luna HSMs

> Generating keys and certificate for PingFederate

> Configuring SSL using Luna HSM generated key

> Configuring SSO with PF integration kit using Luna HSM generated key

Configuring PingFederate with Luna HSMs

To configure PingFederate with Luna HSMs:

1. Set the JAVA_HOME environment variable pointing to the Java installation directory path and add its bin directory to the PATH environment variable.

   For Linux:

   ```
   # export JAVA_HOME=<java installation directory path>
   # export PATH=$JAVA_HOME/bin:$PATH
   ```

   For Windows:

   Set the JAVA_HOME environment variable and modify the PATH environment variable at the system level.

2. Configure Java Interface to use Luna Provider.

   For JDK 11:

   a. Edit the Java Security Configuration file $JAVA_HOME/conf/security/java.security and add the Luna Provider to the java.security file. Adjust the provider list:

   ```
   security.provider.1=SUN
   security.provider.2=SunEC
   security.provider.3=SunJSSE
   security.provider.4=SunJCE
   security.provider.5=SunJGSS
   security.provider.6=SunSASL
   security.provider.7=XMLDSig
   security.provider.8=SunPCSC
   security.provider.9=JdkLDAP
   security.provider.10=JdkSASL
   security.provider.11=SunPKCS11
   security.provider.12=com.safenetinc.luna.provider.LunaProvider
   security.provider.13=SunRsaSign
   ```

   b. Create a file setenv.sh file and save that file in <pf_install>/pingfederate/bin directory with the following variables:

   ```
   #!/bin/sh
   export PF_CLASSPATH=/usr/safenet/lunaclient/jsp/lib/LunaProvider.jar
   export JAVA_OPTS=-Djava.library.path=/usr/safenet/lunaclient/jsp/lib/
   ```

   c. Change the directory to <pf_install>/pingfederate/bin and set the environment variables defined in the setenv.sh file.

   ```
   # . setenv.sh
   ```

NOTE: With JDK 11 and Luna HSM configured, the above environment variables required to be set every time when the PingFederate service start/restart. Failing to do so will fail to start the service.

For JDK 8:

a. Edit the Java Security Configuration file $JAVA_HOME/conf/security/java.security and add the Luna Provider to the java.security file. Adjust the provider list:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=sun.security.rsa.SunRsaSign
security.provider.3=com.Lunainc.luna.provider.LunaProvider
security.provider.4=sun.security.ec.SunEC
security.provider.5=com.sun.net.ssl.internal.ssl.Provider
security.provider.6=com.sun.crypto.provider.SunJCE
security.provider.7=sun.security.jgss.SunProvider
security.provider.8=com.sun.security.sasl.Provider
security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI
security.provider.10=sun.security.smartcardio.SunPCSC
```

b. Copy the Luna library and program files to the Java installation:

Operating System	Steps

Windows	Copy the `<Luna installation directory>\jsp\lib\LunaAPI.dll` file to an arbitrary directory and add the directory's path as a system variable. Alternatively, you can copy the file to the Windows system directory (`C:\Windows\System32`).
	
	Copy the `<Luna installation directory>\jsp\lib\LunaProvider.jar` file to the `JAVA_HOME\jre\lib\ext` directory.
	
	`LunaProvider.jar` and `libLunaAPI.dll` for HSMoD are available at below location:
	
	`<DPoD client directory>/LunaProvider.jar`
	
	`<DPoD client directory>/libLunaAPI.dll`

Linux	Copy the `libLunaAPI.so` and `LunaProvider.jar` files from the `<Luna installation directory>/jsp/lib` directory to the `JAVA_HOME/jre/lib/ext` directory.
	
	`LunaProvider.jar` and `libLunaAPI.so` for HSMoD are available at below location:
	
	`<DPoD client directory>/jsp/LunaProvider.jar`
	
	`<DPoD client directory>/jsp/64/libLunaAPI.so`

3. Edit the hivemodule.xml file in the <pf_install>/pingfederate/server/default/conf/META-INF directory and update the <!-- Crypto provider --> section.

   a. For the JCEManager service endpoint, change the value of the construct class:

   ```
   <construct class="com.pingidentity.crypto.LunaJCEManager"/>
   ```

   b. For the CertificateService service endpoint, change the value of the construct class:

   ```
   <construct class="com.pingidentity.crypto.LunaCertificateServiceImpl"/>
   ```

4. Edit the <pf_install>/pingfederate/bin/run.properties file.

   a. Change the value of the pf.hsm.mode property from OFF to LUNA.

   ```
   pf.hsm.mode=LUNA
   ```

   b. Change the value of the pf.hsm.hybrid property to true.

   ```
   pf.hsm.hybrid=true
   ```

   If you are setting up a new PingFederate installation, set the value of the pf.hsm.hybrid property to false. When the value of pf.hs.hybrid property is set to false, then the certificates that are being created or imported, such as your signing certificate or encryption key, are stored on your HSM.

   If you are configuring an existing PingFederate installation, set the pf.hsm.hybrid to true, which provides the flexibility to store each relevant key and certificate on the HSM or the local trust store. This capability allows you to transition the storage of keys and certificates to your HSM without the need to deploy a new PingFederate environment and to mirror the setup.

5. From the <pf_install>/pingfederate/bin directory, run the hsmpass.bat batch file for Windows, or the hsmpass.sh script for Linux. Enter the NTLS password when prompted. This procedure sets and securely stores the password for NTLS communication to the HSM from PingFederate.

6. Edit the com.pingidentity.crypto.LunaPartitions.xml file in the <pf_install>/pingfederate/server/default/data/config-store directory and update the <con:config> section. For the con:item, change the value of name as explained here:

   - `<con:item name="DefaultPartitionSlotOrLabel">tokenlabel:label</con:item>`
   - `<con:item name="DefaultPartitionSlotOrLabel">slot:id</con:item>`

   Where `label` is the HSM partition name and `id` refers the `slot_id` of the partition.

7. If using an HSMoD service, create the soft link that points to the HSMoD configuration file in the /etc directory.

   ```
   # ln -sf <DPoD client directory>/Chrystoki.conf /etc/Chrystoki.conf
   ```

This completes the configuration of PingFederate with Luna HSMs. You are required start or restart the PingFederate server for changes to take effect.

Generating keys and certificate for PingFederate

Generate keys and certificates on the Luna HSMs through the PingFederate administrative console.

> Managing SSL server certificates

> Managing SSL client keys and certificates

> Managing digital signing certificates and decryption keys

Managing SSL server certificates

Click the **Security** > **SSL Server Certificates** screen to establish and maintain the certificates presented for access to the PingFederate administrative console and for incoming HTTPS connections at runtime.

Create a new certificate

To create a new certificate:

1. On the **SSL Server Certificates** screen, click **Create new**.
2. On the **Create Certificate** screen, enter the required information. For information about each field, refer to the following table:

Field	Description
Common Name	The common name (CN) identifying the certificate.
Subject Alternative Names	The additional DNS names or IP addresses that can be associated with the certificate.
Organization	The organization (O) or company name creating the certificate.
Organizational Unit	The specific unit within the organization (OU).
City	The city or other primary location (L) where the company operates.
State	The state (ST) or other political unit encompassing the location.
Country	The country (C) where the company is based.
Validity (days)	The time during which the certificate is valid.
Cryptographic Provider	The storage facility of the certificate. Select **HSM** to store the certificate in the HSM.
Key Algorithm	A cryptographic formula used to generate a key. PingFederate uses either of two algorithms, RSA or EC.
Key Size (bits)	The number of bits used in the key.
Signature Algorithm	The signing algorithm of the certificate.

3. When finished, click **Next**.
4. Ensure that check boxes **Make this an active certificate for the Runtime Server** and **Make this an active certificate for the Admin Console** are selected. Click **Done**.
5. On the **Summary** screen, review your configuration, amend as needed, and click **Save**.

Create a certificate-authority signing request

To create a certificate authority signing request (CSR):

1. On the **SSL Server Certificates** screen, select **Certificate Signing** under **Action** for the certificate.

   NOTE: This selection is inactive if you have not yet saved a newly created or imported certificate. Click Save and then return to this screen to initiate the process.

2. On the **Certificate Signing** screen, select the **Generate CSR** option.
3. On the **Generate CSR** screen, click **Export** to save the CSR file, and then click **Done**.
4. Once saved, you can submit this CSR file to a certificate authority (CA) to obtain a CA-signed certificate.

Import a certificate-authority response (CSR response)

1. On the **SSL Server Certificates** screen, select **Certificate Signing** under **Action** for the certificate.
2. On the **Certificate Signing** screen, select the **Import CSR Response** option.
3. On the **Import CSR Response** screen, choose the applicable CSR response file.
4. On the **Summary** screen, review your configuration, click **Save** to keep your configuration or click **Cancel** to discard it.

Import a certificate and its private key

1. On the **SSL Server Certificates** screen, click **Import**.
2. On the **Import Certificate** screen, choose the applicable certificate file and enter its password.
3. Select **HSM** to store the certificate in the HSM.
4. On the **Summary** screen, review your configuration and amend as needed.
5. Click **Save** to keep your configuration, or click **Cancel** to discard it.

Managing SSL client keys and certificates

Click the **Security** > **SSL Client Keys & Certificates** screen on PingFederate administrative console to create and manage your authentication private keys and the certificates your server presents as a client in an outbound SSL/TLS transaction. Steps to manage the SSL Client Keys & Certificates on Luna HSMs are similar to Manage SSL Server Certificates.

Managing digital signing certificates and decryption keys

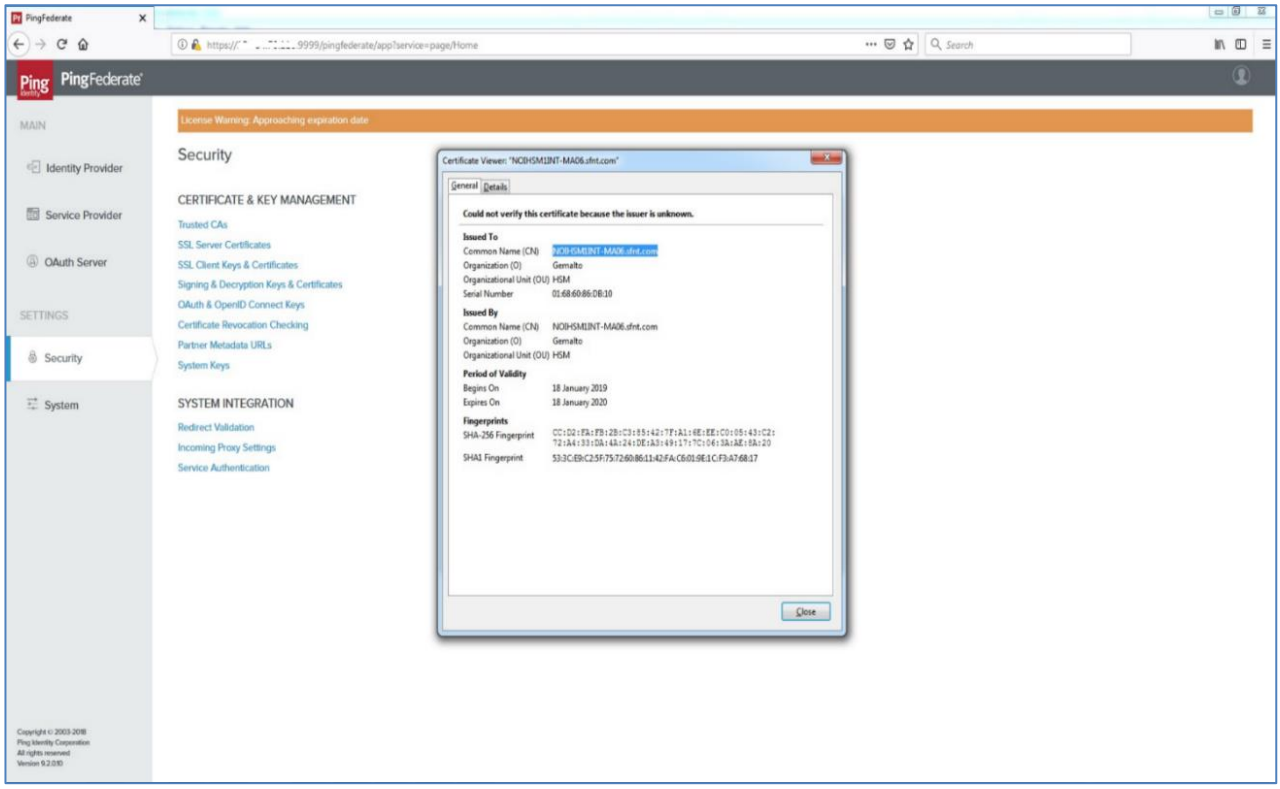
Click the **Security** > **Signing & Decryption Keys & Certificates** screen on PingFederate administrative console to create and maintain certificates for the purpose of signing outgoing requests, responses, assertions, and access tokens, and for the purpose of decryption. Steps to manage the Digital Signing Certificates and Decryption Keys on Luna HSMs are similar to Manage SSL Server Certificates.

Configuring SSL using Luna HSM generated key

In PingFederate administrative console, click **Security** > **SSL Server Certificates** screen to configure the SSL certificate for PingFederate server. To configure SSL using Luna HSM generated key:

1. On the **SSL Server Certificates** screen, under **Action** for the HSM generated certificate, select **Activate Default for Admin Console**.
2. On the **SSL Server Certificates** screen, under **Action** for the HSM generated certificate, select **Activate Default for Runtime Server**.
3. Click **Save**.

Open the administrative console again and verify that the default SSL certificate is replaced with HSM generated certificate for SSL.



Configuring SSO with PF integration kit using Luna HSM generated key

The PF Integration Kit distribution contains sample IdP and SP applications. The applications may be installed quickly for testing OpenToken processing and to provide a working demonstration of end-to-end single sign-on (SSO) and single logout (SLO). The PF Integration Kit can be downloaded from Ping Identity Add-ons resource page. https://www.pingidentity.com/en/resources/downloads/pingfederate.html

We have tested the following PF integration kits:

- `Agentless Integration Kit`
- `Java Integration Kit`

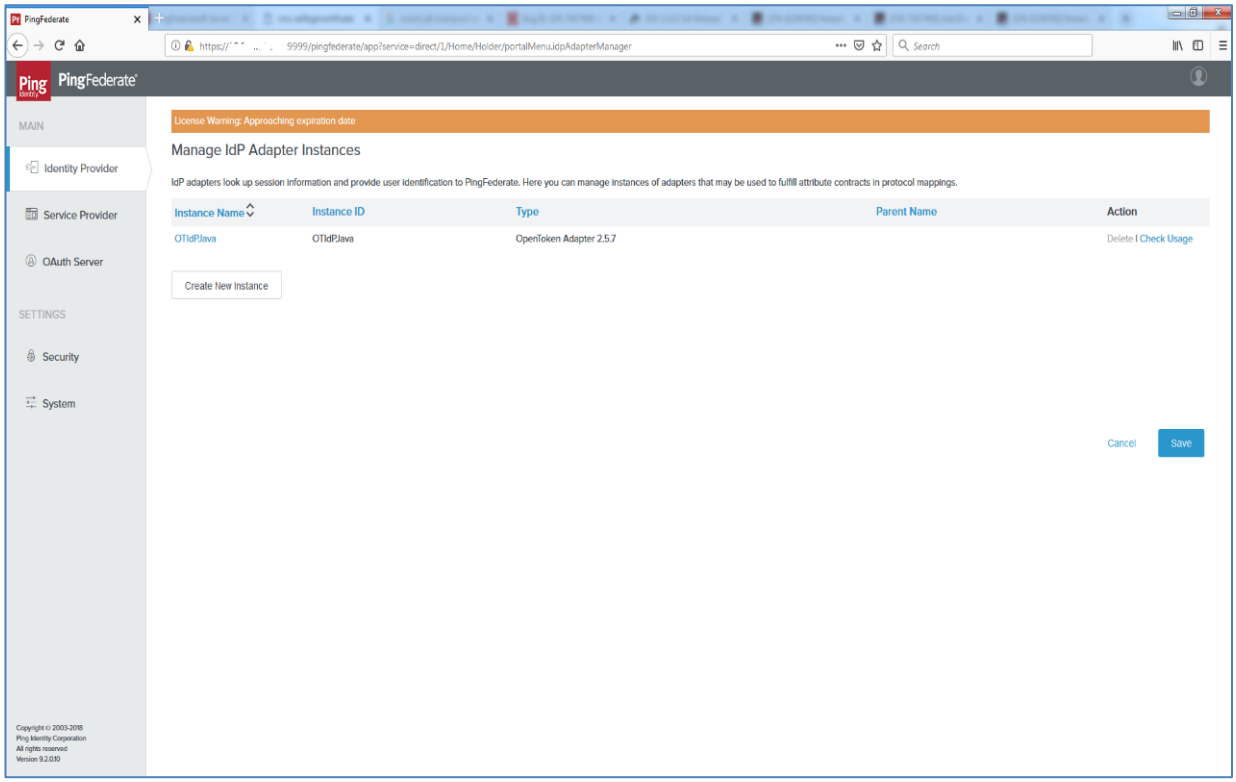
NOTE: Ensure the Sample Apps provided in Integration Kit are installed and configured before configuring the Luna HSM or Luna Cloud HSM with PingFederate.

Follow the Ping Federate integration kit documentation to install and configure the PF integration kit Sample App for both an IdP and an SP.

https://docs.pingidentity.com/bundle/integrations/page/opp1563995022670.html

NOTE: Sample App provided by integration kits can be used for demonstration and testing only.

After installation, verify that your Sample Applications are deployed successfully.



Configure PingFederate to use HSM by steps provided in Integrating PingFederate with Luna HSMs and generate the Signing & Decryption Keys & Certificates. To use the signing key generated on Luna HSM for SSO and Sample App Token signing, perform the steps explained here.

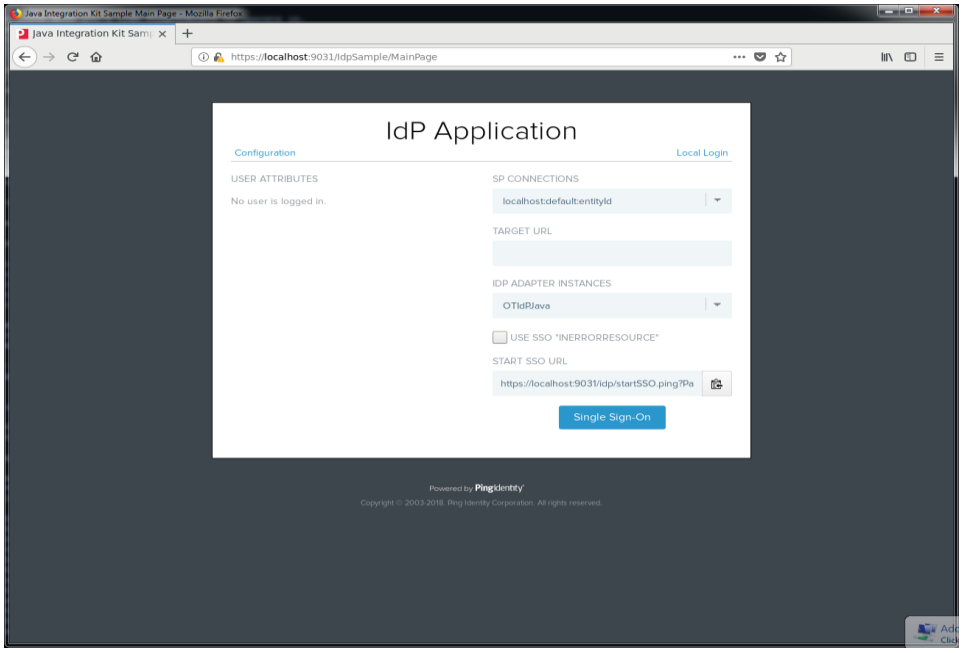
Verify the SSO feature provided by integration kit using Luna HSMs

To verify the SSO feature provided by integration kit using Luna HSMs:

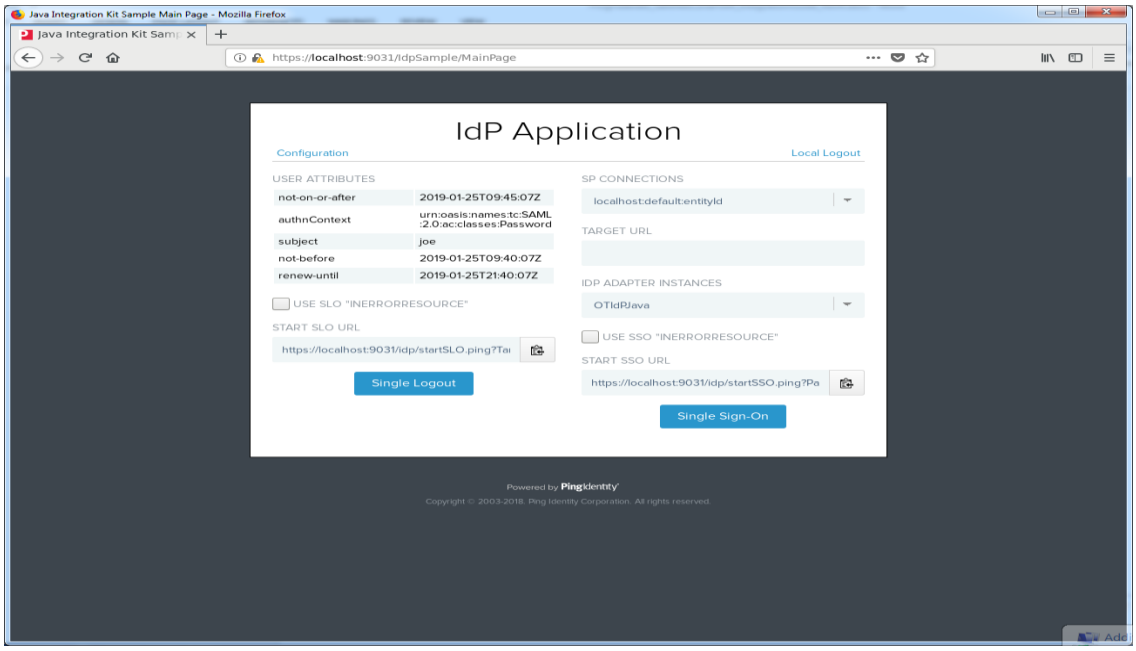
1. Log in to the PingFederate Administrative Console.
2. Click **Security** > **Signing & Decryption Keys & Certificates**.
3. Under **Action**, click **Export**.
4. Click **Next**, and then click **Export** to export the certificate.
5. Click **Save File** when prompted, and then click **Done**.

6. Click **Identity Provider**.
7. Under **Idp Connections**, click the **SAML2.0** entity.
8. On **Idp Connection Page**, click **Credentials** > **Configure Credentials** > **Digital Signature Settings**.
9. Select the **Signing Certificate** generated on the Luna HSM and the **Signing Algorithm**. Click **Next**.
10. Click **Manage Signature Verification Settings** > **Signature Verification Certificates** > **Manage Certificates** > **Import**.
11. Import the certificate. Click **Choose File** and select the certificate exported from HSM in step 4. Click **Next**.
12. Ensure that the **Make this an active verification certificate** check box is selected. Click **Done**.
13. Click **Done** to confirm the certificate. Click **Save.**
14. Click **Service Provider**.
15. Under **Sp Connections** click the **SAML2.0** entity.
16. On **Sp Connection** Page, Click **Credentials** > **Configure Credentials** > **Digital Signature Settings**.
17. Select the **Signing Certificate** generated on Luna HSM and the **Signing Algorithm**. Click **Next**.
18. Click **Manage Signature Verification Settings** > **Signature Verification Certificates** > **Manage Certificates** > **Import**.
19. To import certificate, click **Choose File** and select the certificate exported from HSM in step 4. Click **Next**.
20. Ensure that **Make this an active verification certificate** check box is selected. Click **Done**.
21. Click **Done** to confirm the certificate. Click **Save.**
22. Restart the PingFederate service for changes to take effect.
23. Open the browser and access the IdP Sample application URL.

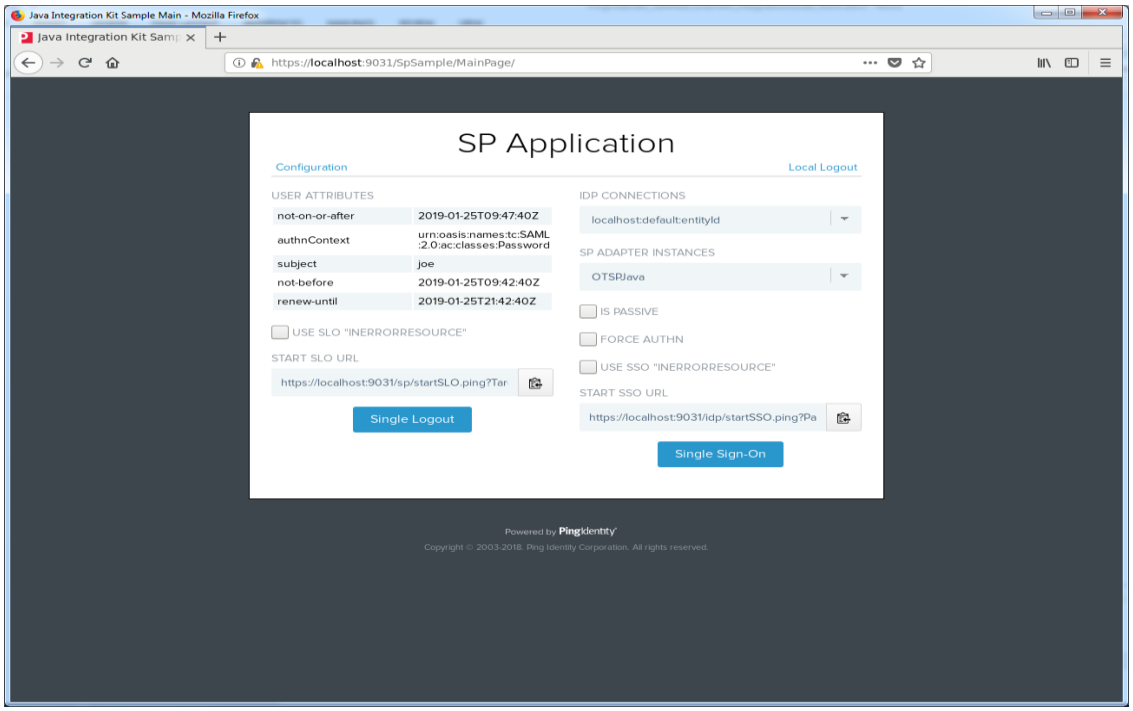
    https://localhost:9031/IdpSample



24. Click on **Local Login**. Enter credentials (joe/test) and click **Login**. After logging in, you will be able to see the user attributes for Idp Application.



25. Click on **Single Sign-On** and you will be automatically logged in SP application without any credential using SSO.



This verifies that PingFederate SSO feature is working and that every token generated by the application are signed by the signing and decryption key secured in the Luna HSM.

Contacting Customer Support

If you encounter a problem during this integration, contact your supplier or Thales Customer Support. Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.