Citrix Federated Authentication Service: Integration Guide

THALES LUNA HSM

Document Information

Document Part Number	007-001424-001
Revision	B
Release Date	9 November 2021

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Overview

Citrix Federated Authentication Service (FAS) is a privileged component designed to integrate with Active Directory Certificate Services. It dynamically issues certificates for users, allowing them to log on to an Active Directory environment as if they had a smart card. Thales Luna HSM is used to generate and store the FAS server's Authorization/Registration Authority (RA) key. The benefits of integrating Citrix FAS with Thales Luna HSM include:

> Full life cycle management of keys.

> Access to the HSM audit trail.

> Significant performance improvements by off-loading cryptographic operations from servers.

Certified Platforms

The following platforms are certified for integrating Citrix FAS with Luna HSM:

Third Party Details	Operating System	Luna HSM Version	Luna Firmware Version
Citrix FAS 10.6	Windows Server 2019	Appliance Version 7.7.0	7.7.0

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.

Prerequisites

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

> Configure Luna HSM

> Set up Citrix FAS

Configure Luna HSM

If you are using Luna HSM:

1. Verify the HSM is set up, initialized, provisioned and ready for deployment. Refer to Luna HSM documentation for more information.
2. Create a partition that will be later used by Citrix FAS.

   > **NOTE:** If you are using SKS partition for integration you need to create v1 partition. Refer to Luna HSM documentation for detailed steps for creating v1 partition.

3. If using a Luna Network HSM, register a client for the system and assign the client to the partition to create an NTLS connection. Initialize the 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:

   ```
   C:\Program Files\SafeNet\LunaClient>lunacm.exe

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

   Available HSMs:

   Slot Id ->                0

   Label ->                  lunahsm1

   Serial Number ->          1312109861427

   Model ->                  LunaSA 7.7.0

   Firmware Version ->       7.7.0

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

   Slot Description ->       Net Token Slot

   FM HW Status ->           Non-FM
   ```

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.

   > **NOTE**: For PED-based Luna HSM, ensure that ProtectedAuthenticationPathFlagStatus is set to ‘1’ in the Misc Section of Chrystoki.conf file.

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 are 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 for Luna Client 7.x.

Set up Citrix FAS

To install Citrix FAS, refer to https://docs.citrix.com/en-us/federated-authentication-service. You also need to have a domain controller and a certificate authority. For the purpose of this demonstration, we have used two Windows Server 2019:

- First Windows Server with a Domain Controller and Certificate Authority
- Second Windows Server with Citrix FAS and joined to the domain

Integrating Citrix FAS with a Luna HSM

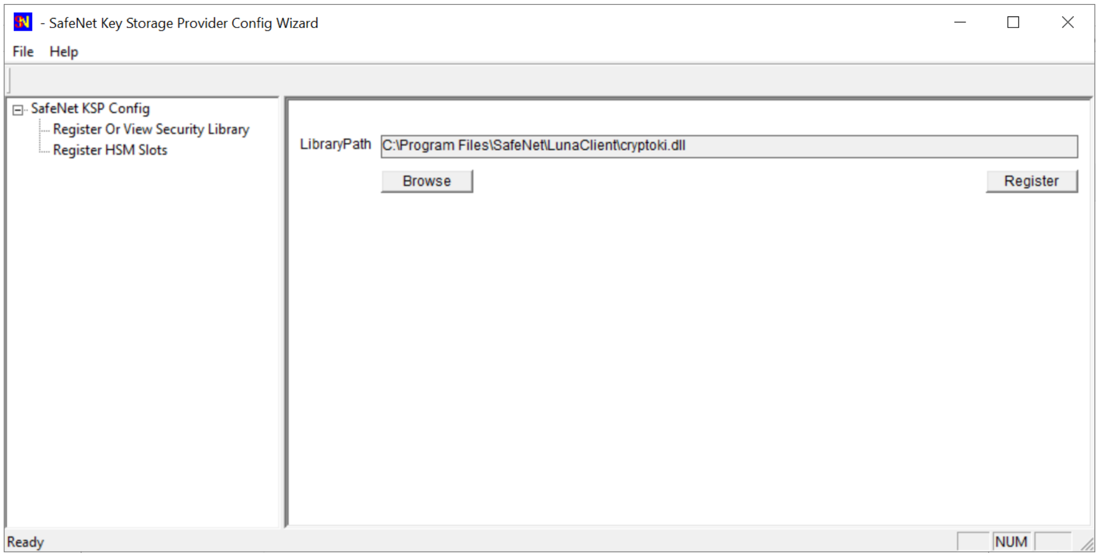
Follow these steps to integrate Citrix FAS with Luna HSM:

- Configure SafeNet Key Storage Provider (KSP)
- Configure Citrix FAS server to use Luna HSM
- Renewing the authorization (RA) key and certificate (optional)

Configure SafeNet Key Storage Provider (KSP)

To configure the SafeNet Key Storage provider on Citrix FAS server:

1. Navigate to the <Luna HSM Client installation Directory>/KSP directory.
2. Double-click the KspConfig.exe file to launch the KSP configuration wizard.
3. Double-click **Register Or View Security Library** on the left side of the pane.
4. Click **Browse.** Select the cryptoki.dll file, available in the Luna Client installation folder. Click **Register**.


- SafeNet Key Storage Provider Config Wizard
File
Help
SafeNet KSP Config
Register Or View Security Library
Register HSM Slots
Browse
Register
Ready
NUM

LibraryPath C:\Program Files\SafeNet\LunaClient\cryptoki.dll

NOTE: If you are using SKS partition refer to Integrating Citrix FAS with a Luna HSM using SKS Partition for detailed steps.

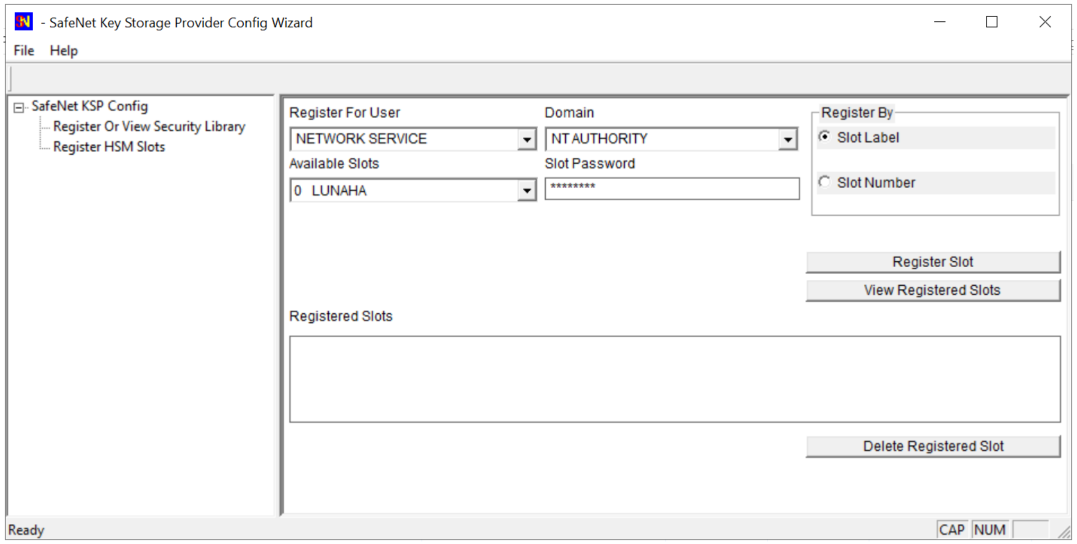
On successful registration, the following message will appear on screen: **Success registering the security library!**

5. Double-click **Register HSM Slots** on the left side of the pane.

6. Register the slot as follows:
   a. Open the **Register for User** drop-down menu and select **NETWORK SERVICE**.
   b. Open the **Domain** drop-down menu and select **NT AUTHORITY**.
   c. Open the **Available Slots** drop-down menu and select the relevant partition.
   d. Enter the **Slot Password**.
   e. Click **Register Slot**. On successful registration, the following message will appear on screen:

      The slot was successfully and securely registered!

   f. Click **OK**.



- SafeNet Key Storage Provider Config Wizard

Register For User: NETWORK SERVICE

Domain: NT AUTHORITY

Available Slots: 0 LUNAHA

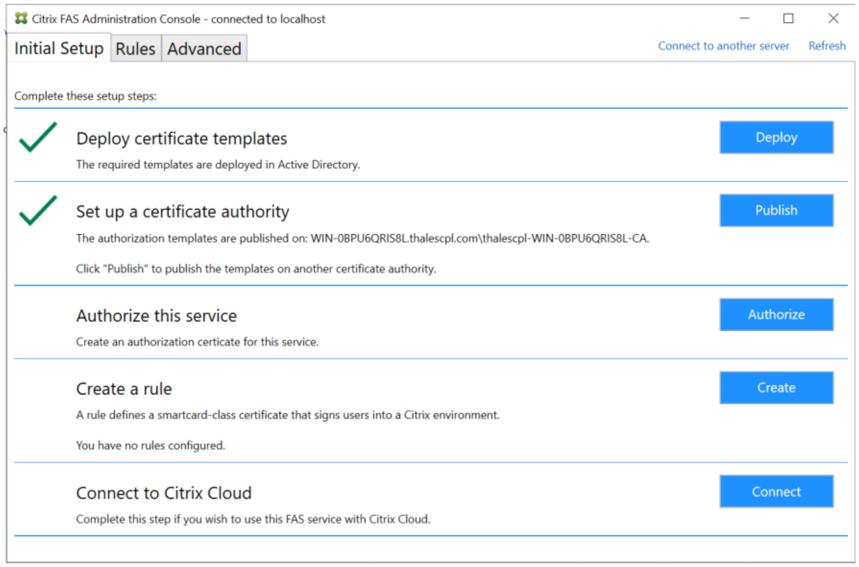
Slot Password: ********

Register By: ● Slot Label ○ Slot Number

Configure Citrix FAS server to use Luna HSM

To configure Citrix FAS server to use Luna HSM:

1. Open Citrix FAS Administration Console and in **Initial Setup** tab make sure that the certificate templates are deployed and certificate authority setup is completed.



Citrix FAS Administration Console - connected to localhost

Complete these setup steps:

✓ Deploy certificate templates

The required templates are deployed in Active Directory.

✓ Set up a certificate authority

The authorization templates are published on: WIN-0BPU6QRIS8L.thalescpl.com\thalescpl-WIN-0BPU6QRIS8L-CA.

Click "Publish" to publish the templates on another certificate authority.

Authorize this service

Create an authorization certicate for this service.

Create a rule

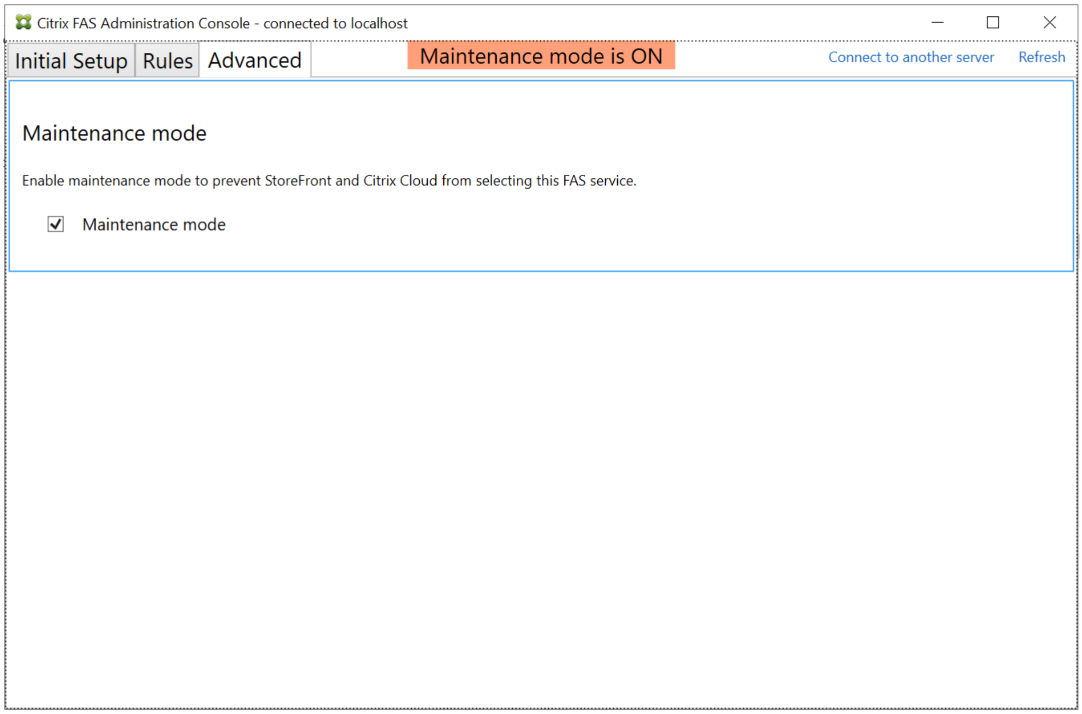
A rule defines a smartcard-class certificate that signs users into a Citrix environment.

You have no rules configured.

Connect to Citrix Cloud

Complete this step if you wish to use this FAS service with Citrix Cloud.

2. Click the **Advanced** tab and select **Maintenance mode** check box.


Citrix FAS Administration Console - connected to localhost
Initial Setup
Rules
Advanced
Maintenance mode is ON
Connect to another server
Refresh

Maintenance mode

Enable maintenance mode to prevent StoreFront and Citrix Cloud from selecting this FAS service.

☑ Maintenance mode

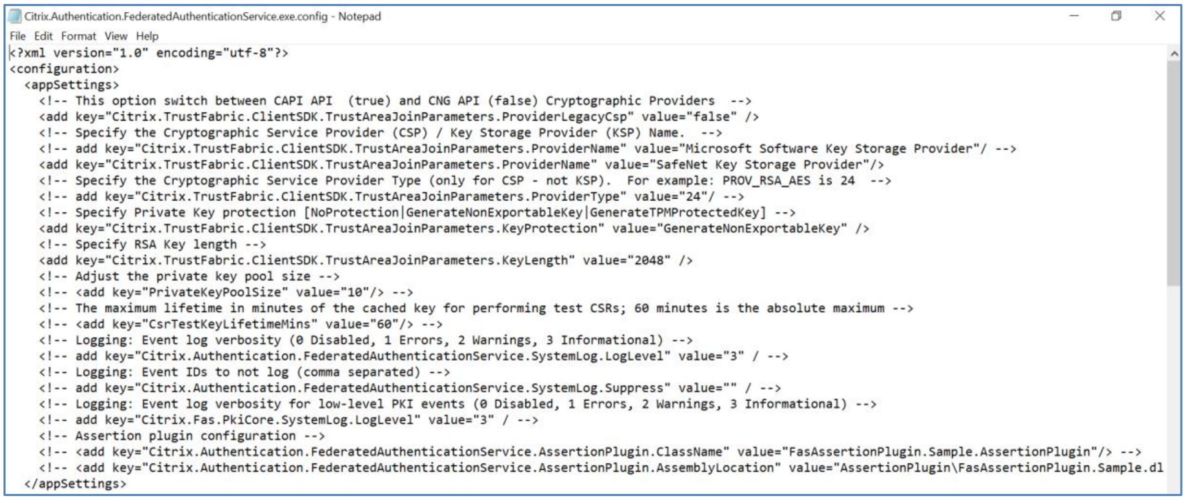
3. Open the C:\Program Files\Citrix\Federated Authentication Service\ Citrix.Authentication.FederatedAuthenticationService.exe.config file and make the following changes:

   i. Delete the following code, if present.

   ```
   <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
   value="Microsoft Software Key Storage Provider"/>
   ```

   ii. Add the following code:

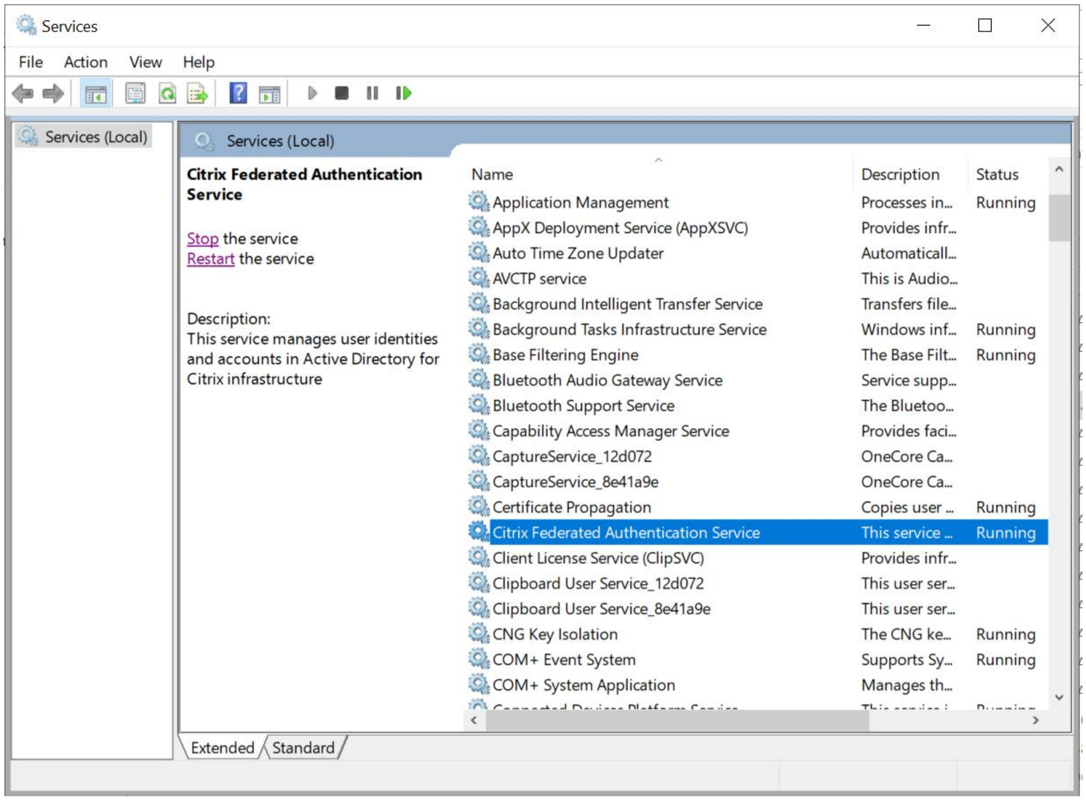
   ```
   <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
   value="SafeNet Key Storage Provider"/>
   ```


Citrix.Authentication.FederatedAuthenticationService.exe.config - Notepad
File Edit Format View Help

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false" />
    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="SafeNet Key Storage Provider"/>
    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->
    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey" />
    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048" />
    <!-- Adjust the private key pool size -->
    <!-- <add key="PrivateKeyPoolSize" value="10"/> -->
    <!-- The maximum lifetime in minutes of the cached key for performing test CSRs; 60 minutes is the absolute maximum -->
    <!-- <add key="CsrTestKeyLifetimeMins" value="60"/> -->
    <!-- Logging: Event log verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.FederatedAuthenticationService.SystemLog.LogLevel" value="3" / -->
    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.FederatedAuthenticationService.SystemLog.Suppress" value="" / -->
    <!-- Logging: Event log verbosity for low-level PKI events (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Fas.PkiCore.SystemLog.LogLevel" value="3" / -->
    <!-- Assertion plugin configuration -->
    <!-- <add key="Citrix.Authentication.FederatedAuthenticationService.AssertionPlugin.ClassName" value="FasAssertionPlugin.Sample.AssertionPlugin"/> -->
    <!-- <add key="Citrix.Authentication.FederatedAuthenticationService.AssertionPlugin.AssemblyLocation" value="AssertionPlugin\FasAssertionPlugin.Sample.dl
  </appSettings>
```

4. Save and close the file.

5. Open **Services** and restart the **Citrix Federated Authentication Service**.



Citrix Federated Authentication Service

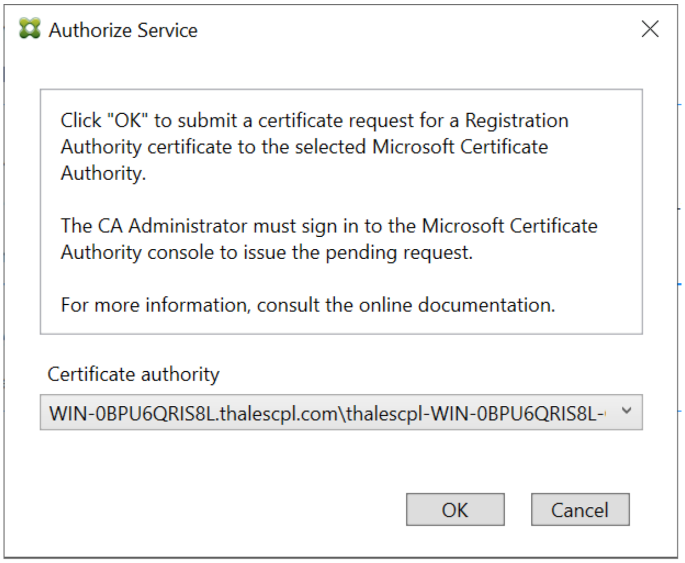
Stop the service
Restart the service

Description:
This service manages user identities and accounts in Active Directory for Citrix infrastructure

Name	Description	Status
Application Management	Processes in...	Running
AppX Deployment Service (AppXSVC)	Provides infr...	
Auto Time Zone Updater	Automaticall...	
AVCTP service	This is Audio...	
Background Intelligent Transfer Service	Transfers file...	
Background Tasks Infrastructure Service	Windows inf...	Running
Base Filtering Engine	The Base Filt...	Running
Bluetooth Audio Gateway Service	Service supp...	
Bluetooth Support Service	The Bluetoo...	
Capability Access Manager Service	Provides faci...	
CaptureService_12d072	OneCore Ca...	
CaptureService_8e41a9e	OneCore Ca...	
Certificate Propagation	Copies user ...	Running
Citrix Federated Authentication Service	This service ...	Running
Client License Service (ClipSVC)	Provides infr...	
Clipboard User Service_12d072	This user ser...	
Clipboard User Service_8e41a9e	This user ser...	
CNG Key Isolation	The CNG ke...	Running
COM+ Event System	Supports Sy...	Running
COM+ System Application	Manages th...	
Connected Devices Platform Service	This service i...	Running

6. Open Citrix FAS Administration Console and in **Initial Setup** tab, click on **Authorize**.

7. Select **Certificate Authority** from drop down menu and click **OK**.



Click "OK" to submit a certificate request for a Registration Authority certificate to the selected Microsoft Certificate Authority.

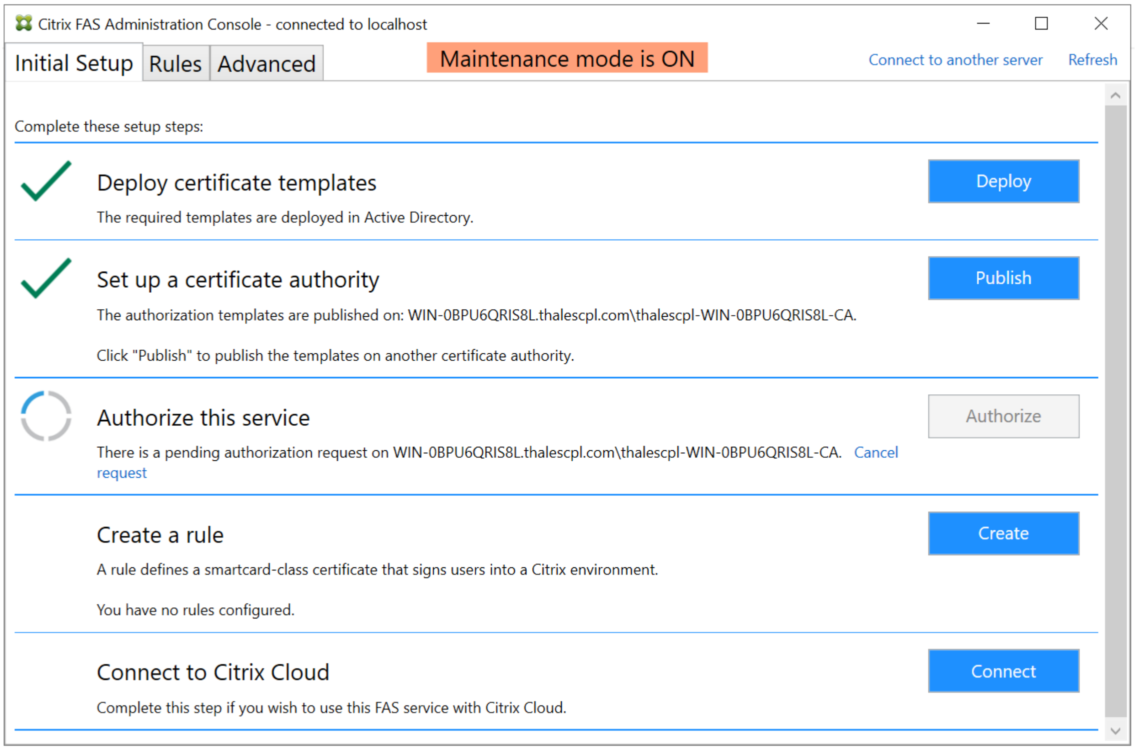
The CA Administrator must sign in to the Microsoft Certificate Authority console to issue the pending request.

For more information, consult the online documentation.

Certificate authority

WIN-0BPU6QRIS8L.thalescpl.com\thalescpl-WIN-0BPU6QRIS8L-

8. This will send a certificate request to the selected certificate authority.



Complete these setup steps:

✓ Deploy certificate templates

The required templates are deployed in Active Directory.

✓ Set up a certificate authority

The authorization templates are published on: WIN-0BPU6QRIS8L.thalescpl.com\thalescpl-WIN-0BPU6QRIS8L-CA.

Click "Publish" to publish the templates on another certificate authority.

Authorize this service

There is a pending authorization request on WIN-0BPU6QRIS8L.thalescpl.com\thalescpl-WIN-0BPU6QRIS8L-CA. Cancel request

Create a rule

A rule defines a smartcard-class certificate that signs users into a Citrix environment.

You have no rules configured.

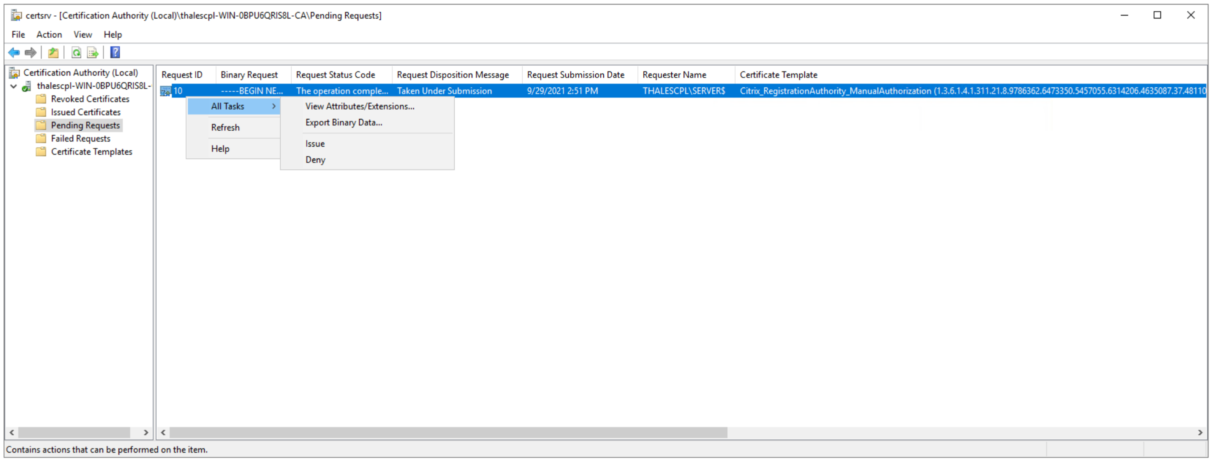
Connect to Citrix Cloud

Complete this step if you wish to use this FAS service with Citrix Cloud.

9. Go to Certificate Authority server and open **Certificate Authority** console.

10. Click on **Pending Requests** from left pane.

11. Right click the certificate with Certificate Template **Citrix_RegistrationAuthority_ManualAuthorization**, click on **All Tasks**, and select **Issue**.

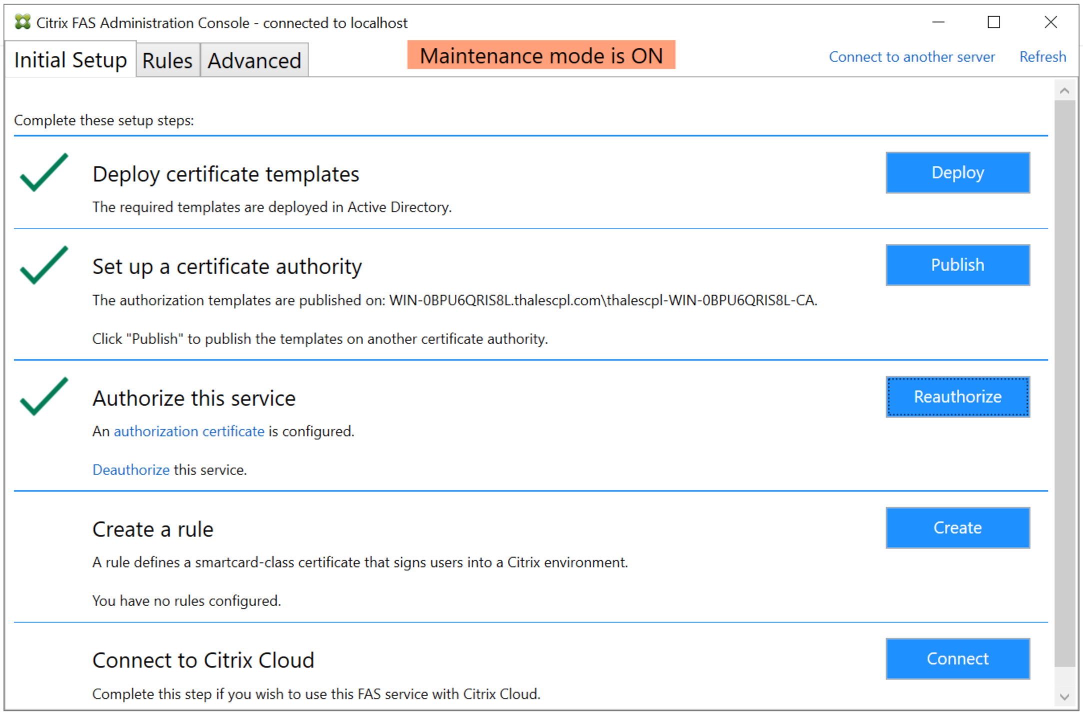

certsrv - [Certification Authority (Local)\thalescpl-WIN-0BPU6QRIS8L-CA\Pending Requests]
File
Action
View
Help
Certification Authority (Local)
thalescpl-WIN-0BPU6QRIS8L-
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
All Tasks
Refresh
Help
View Attributes/Extensions...
Export Binary Data...
Issue
Deny

Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Certificate Template
10	-----BEGIN NE...	The operation comple...	Taken Under Submission	9/29/2021 2:51 PM	THALESCPL\SERVER$	Citrix_RegistrationAuthority_ManualAuthorization (1.3.6.1.4.1.311.21.8.9786362.6473350.5457055.6314206.4635087.37.48110

Contains actions that can be performed on the item.

To automatically obtain the Citrix_RegistrationAuthority certificate that is valid for two years by default, FAS uses the Citrix_RegistrationAuthority_ManualAuthorization certificate. As soon as the FAS server obtains the Citrix_RegistrationAuthority certificate, it deletes the certificate and key for Citrix_RegistrationAuthority_ManualAuthorization.

12. Go to Citrix FAS server and in **Citrix FAS Administration Console**, verify that **Authorize this service** is marked with green arrow.



Complete these setup steps:

✓ Deploy certificate templates

The required templates are deployed in Active Directory.

✓ Set up a certificate authority

The authorization templates are published on: WIN-0BPU6QRIS8L.thalescpl.com\thalescpl-WIN-0BPU6QRIS8L-CA.

Click "Publish" to publish the templates on another certificate authority.

✓ Authorize this service

An authorization certificate is configured.

Deauthorize this service.

Create a rule

A rule defines a smartcard-class certificate that signs users into a Citrix environment.

You have no rules configured.

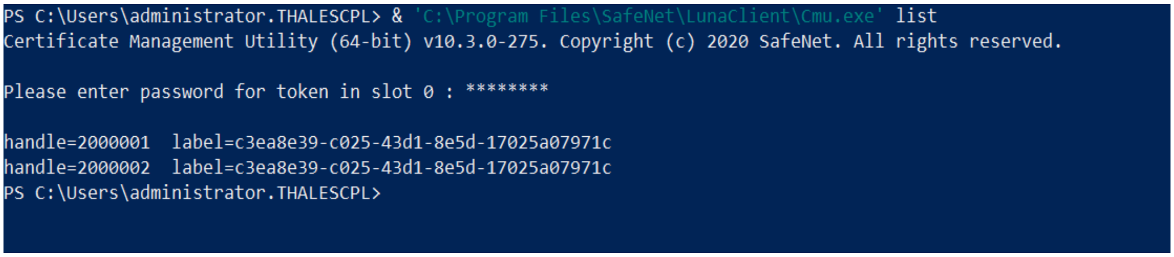
Connect to Citrix Cloud

Complete this step if you wish to use this FAS service with Citrix Cloud.

13. Verify that the keys were successfully generated on the Luna HSM partition by running cmu list command:

```
'C:\Program Files\SafeNet\LunaClient\Cmu.exe' list
```

Provide partition password, when prompted.



```
PS C:\Users\administrator.THALESCPL> & 'C:\Program Files\SafeNet\LunaClient\Cmu.exe' list
Certificate Management Utility (64-bit) v10.3.0-275. Copyright (c) 2020 SafeNet. All rights reserved.

Please enter password for token in slot 0 : ********

handle=2000001  label=c3ea8e39-c025-43d1-8e5d-17025a07971c
handle=2000002  label=c3ea8e39-c025-43d1-8e5d-17025a07971c
PS C:\Users\administrator.THALESCPL>
```

14. Open the C:\Program Files\Citrix\Federated Authentication Service\ Citrix.Authentication.FederatedAuthenticationService.exe.config file and revert the setting back to Microsoft Software Key Storage Provider.

    i. Delete the following code.

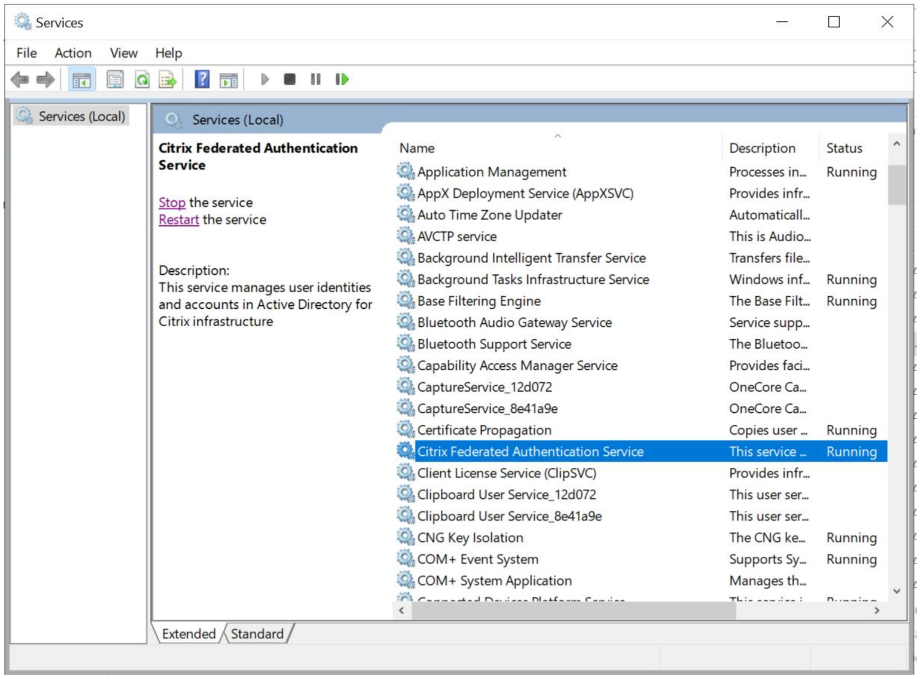
    ```
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
    value="SafeNet Key Storage Provider"/>
    ```

    ii. Add the following code.

    ```
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
    value="Microsoft Software Key Storage Provider"/>
    ```

15. Save and close the file.

16. Open **Services** and restart **Citrix Federated Authentication Service**.



Citrix Federated Authentication Service

Stop the service
Restart the service

Description:
This service manages user identities and accounts in Active Directory for Citrix infrastructure

Name	Description	Status
Application Management	Processes in...	Running
AppX Deployment Service (AppXSVC)	Provides infr...	
Auto Time Zone Updater	Automaticall...	
AVCTP service	This is Audio...	
Background Intelligent Transfer Service	Transfers file...	
Background Tasks Infrastructure Service	Windows inf...	Running
Base Filtering Engine	The Base Filt...	Running
Bluetooth Audio Gateway Service	Service supp...	
Bluetooth Support Service	The Bluetoo...	
Capability Access Manager Service	Provides faci...	
CaptureService_12d072	OneCore Ca...	
CaptureService_8e41a9e	OneCore Ca...	
Certificate Propagation	Copies user ...	Running
Citrix Federated Authentication Service	This service ...	Running
Client License Service (ClipSVC)	Provides infr...	
Clipboard User Service_12d072	This user ser...	
Clipboard User Service_8e41a9e	This user ser...	
CNG Key Isolation	The CNG ke...	Running
COM+ Event System	Supports Sy...	Running
COM+ System Application	Manages th...	
Connected Devices Platform Service	This service i...	Running

17. Open **Citrix FAS Administration Console**.

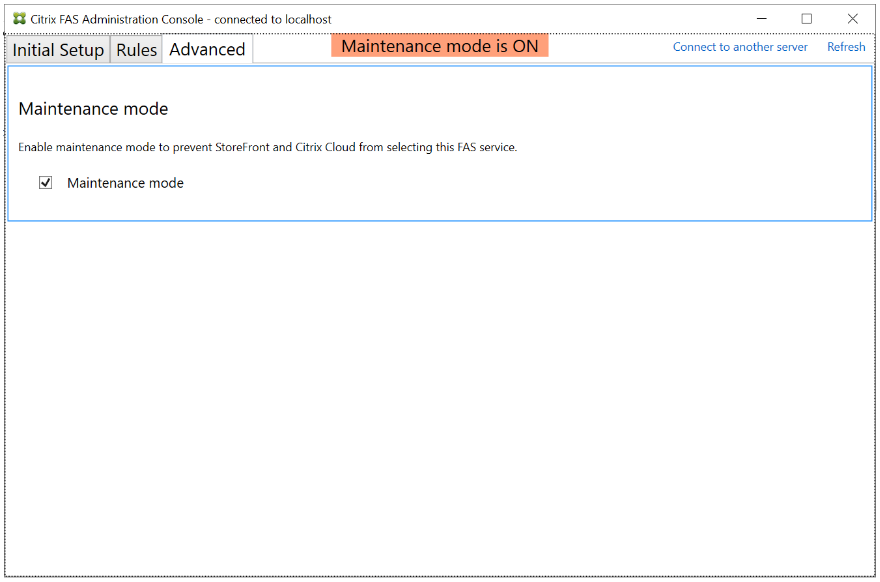
18. Click on Advanced tab and uncheck the **Maintenance mode** check box to take the FAS server out of maintenance mode.

Renewing the Authorization (RA) key and certificate (Optional)

When Authorization (RA) certificate expires after 2 years by default, renew it as follows:

1. Open Citrix FAS Administration Console.

2. Click on **Advanced** tab and select **Maintenance mode** check box.



Citrix FAS Administration Console - connected to localhost
Initial Setup
Rules
Advanced
Maintenance mode is ON
Connect to another server
Refresh

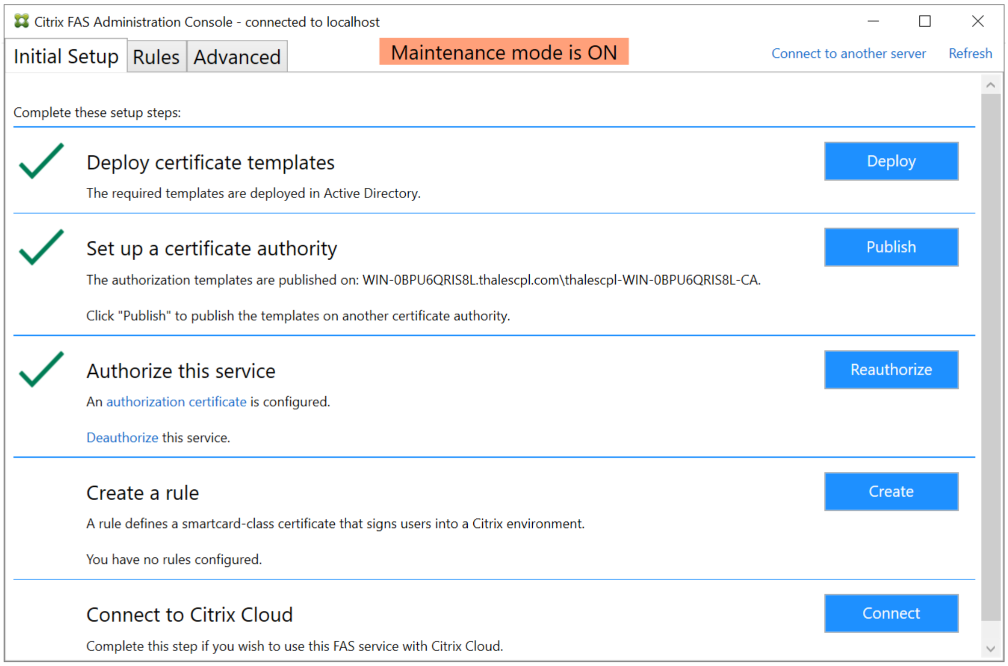
Maintenance mode

Enable maintenance mode to prevent StoreFront and Citrix Cloud from selecting this FAS service.

☑ Maintenance mode

3. Click on **Initial Setup**.

4. Under the **Authorize this service** section, click the **Deauthorize this service** option.



Complete these setup steps:

✓ Deploy certificate templates

The required templates are deployed in Active Directory.

✓ Set up a certificate authority

The authorization templates are published on: WIN-0BPU6QRIS8L.thalescpl.com\thalescpl-WIN-0BPU6QRIS8L-CA.

Click "Publish" to publish the templates on another certificate authority.

✓ Authorize this service

An authorization certificate is configured.

Deauthorize this service.

Create a rule

A rule defines a smartcard-class certificate that signs users into a Citrix environment.

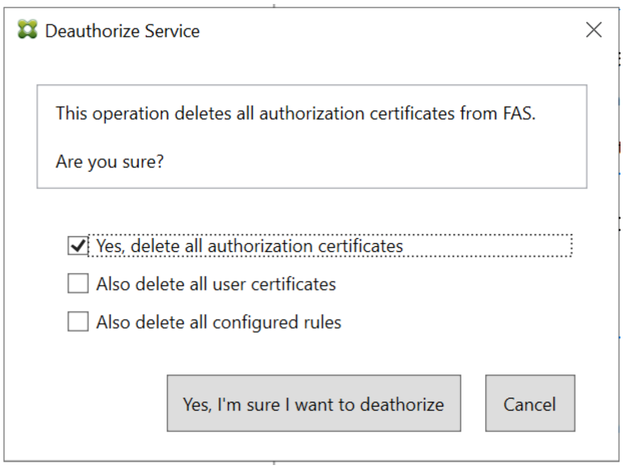
You have no rules configured.

Connect to Citrix Cloud

Complete this step if you wish to use this FAS service with Citrix Cloud.

> **CAUTION!** When Deauthorizing a FAS server, all the user certificates/keys on that FAS server gets deleted. Ensure that no users with existing sessions are relying on use of in-session certificates from the FAS server that is being Deauthorized.

5. Select **Yes, delete all authorization certificates** and click on **Yes, I'm sure I want to deauthorize**.



This operation deletes all authorization certificates from FAS.

Are you sure?

☑ Yes, delete all authorization certificates

☐ Also delete all user certificates

☐ Also delete all configured rules

6. Repeat the steps 3 to 18 from Configure Citrix FAS server to use Luna HSM section.

This completes the integration of Citrix FAS with Thales Luna HSM.

Integrating Citrix FAS with a Luna HSM using SKS Partition

Follow these steps to integrate Citrix FAS with Luna HSM using SKS Partition:

> Configure SKS

> Configure SafeNet Key Storage Provider (KSP) to use SKS Partition

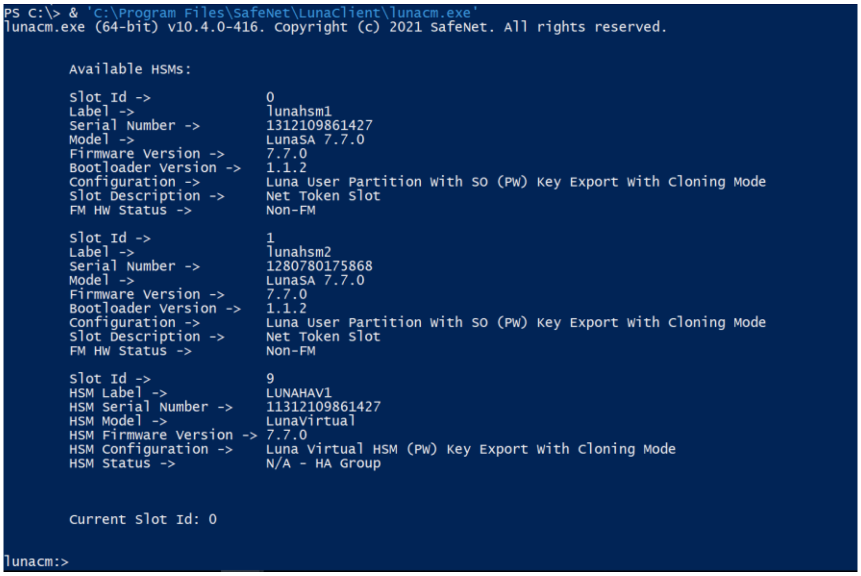
Configure SKS

Complete the following steps to configure SKS:

> **NOTE:** This is only supported with Luna Client version 10.4 and Luna Firmware Version 7.7.0 or above.

1. Make sure that the partitions are assigned to Citrix FAS server and if required, HA is created using the assigned partitions.

2. Open “C:\Program Files\SafeNet\LunaClient\lunacm.exe” and note down the label, model, and serialNumber of the HSM slot that you want to use.



```
PS C:\> & 'C:\Program Files\SafeNet\LunaClient\lunacm.exe'
lunacm.exe (64-bit) v10.4.0-416. Copyright (c) 2021 SafeNet. All rights reserved.


        Available HSMs:

        Slot Id ->              0
        Label ->                lunahsm1
        Serial Number ->        1312109861427
        Model ->                LunaSA 7.7.0
        Firmware Version ->     7.7.0
        Bootloader Version ->   1.1.2
        Configuration ->        Luna User Partition With SO (PW) Key Export With Cloning Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         Non-FM

        Slot Id ->              1
        Label ->                lunahsm2
        Serial Number ->        1280780175868
        Model ->                LunaSA 7.7.0
        Firmware Version ->     7.7.0
        Bootloader Version ->   1.1.2
        Configuration ->        Luna User Partition With SO (PW) Key Export With Cloning Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         Non-FM

        Slot Id ->              9
        HSM Label ->            LUNAHAV1
        HSM Serial Number ->    11312109861427
        HSM Model ->            LunaVirtual
        HSM Firmware Version -> 7.7.0
        HSM Configuration ->    Luna Virtual HSM (PW) Key Export With Cloning Mode
        HSM Status ->           N/A - HA Group


        Current Slot Id: 0

lunacm:>
```

3. Open crystoki.ini file present in <Luna HSM Client installation Directory> and modify the values, as below:

```
[Chrystoki2]

LibNT=C:\Program Files\SafeNet\LunaClient\shim.dll

. . . . . . .


[Shim2]

LibNT=C:\Program Files\SafeNet\LunaClient\cryptoki.dll

. . . . . . .
```

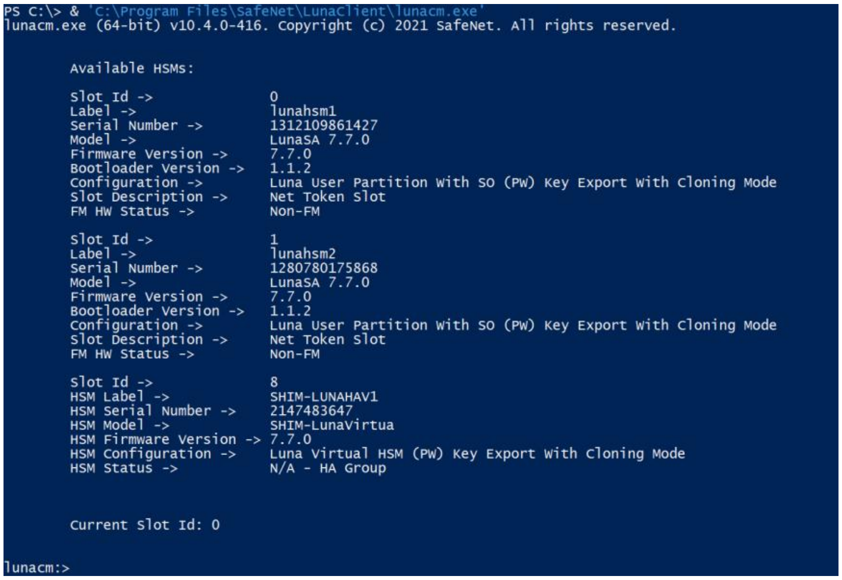
```
[SimTokenManager]
SimTokenDir=C:\Temp\simtoken\
. . . . . . .

[Misc]
ApplicationInstance=SIM_ENGINE
. . . . . . .
```

4. Make directory C:\Temp\simtoken\001\ and create the INF file at path "C:\Temp\simtoken\001\simtoken.inf"

```
[simtoken]
dbtype = sqlite
label = LUNAHAV1
manufacturerID = Safenet, Inc.
model = LunaVirtual
serialNumber = 11312109861427
```

> **NOTE:** To ensure that SHIM works properly, enter the correct values for label, model, and serialNumber as noted down in step 2.
>
> **NOTE:** Ensure that the user or service account using SKS partition must have read and write permission on C:\Temp\simtoken\001\ directory and files.

5. Verify that the partition is listed in C:\Program Files\SafeNet\LunaClient\lunacm.exe utility.



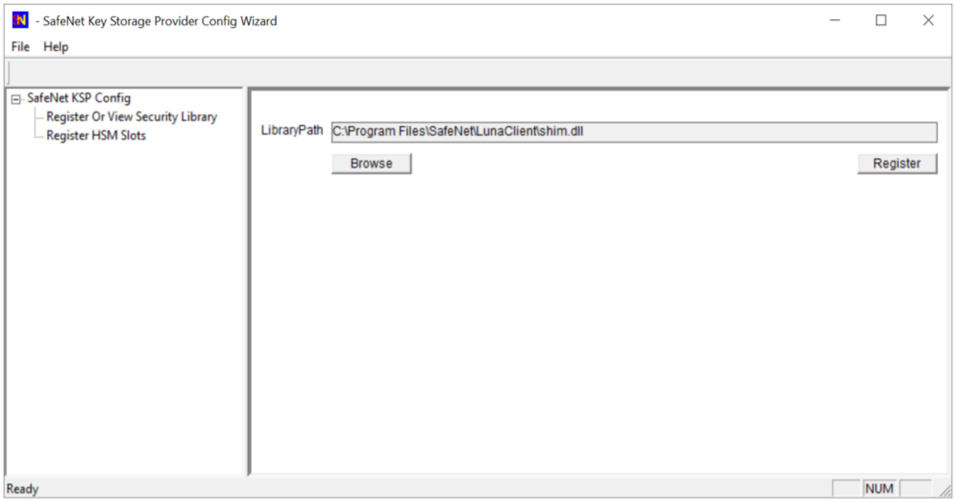
```
PS C:\> & 'C:\Program Files\SafeNet\LunaClient\lunacm.exe'
lunacm.exe (64-bit) v10.4.0-416. Copyright (c) 2021 SafeNet. All rights reserved.


        Available HSMs:

        Slot Id ->              0
        Label ->                lunahsm1
        Serial Number ->        1312109861427
        Model ->                LunaSA 7.7.0
        Firmware Version ->     7.7.0
        Bootloader Version ->   1.1.2
        Configuration ->        Luna User Partition With SO (PW) Key Export With Cloning Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         Non-FM

        Slot Id ->              1
        Label ->                lunahsm2
        Serial Number ->        1280780175868
        Model ->                LunaSA 7.7.0
        Firmware Version ->     7.7.0
        Bootloader Version ->   1.1.2
        Configuration ->        Luna User Partition With SO (PW) Key Export With Cloning Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         Non-FM

        Slot Id ->              8
        HSM Label ->            SHIM-LUNAHAV1
        HSM Serial Number ->    2147483647
        HSM Model ->            SHIM-LunaVirtua
        HSM Firmware Version -> 7.7.0
        HSM Configuration ->    Luna Virtual HSM (PW) Key Export With Cloning Mode
        HSM Status ->           N/A - HA Group


        Current Slot Id: 0

lunacm:>
```

> **NOTE:** If SHIM is configured correctly for SKS partition you will see the partition label with **SHIM-** as prefix.

Configure SafeNet Key Storage Provider (KSP) to use SKS Partition

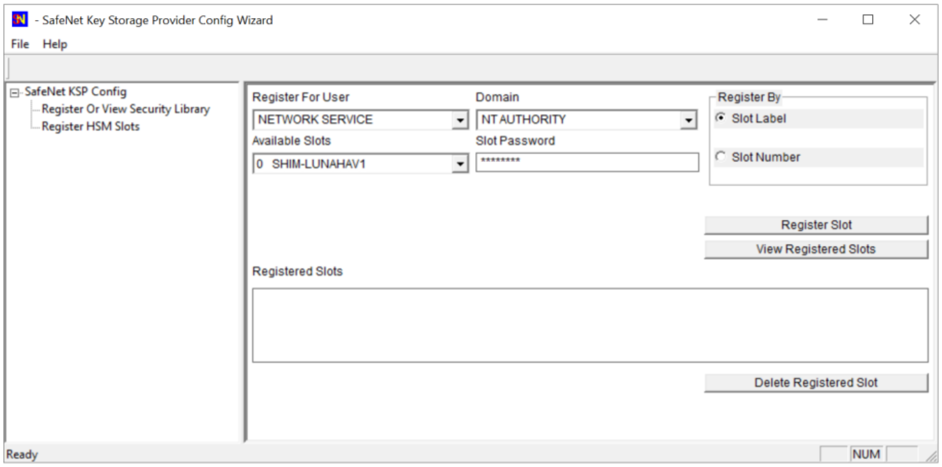
To configure the SafeNet Key Storage provider to use SKS partition on Citrix FAS server:

1. Allow read and write access to **NETWORK SERVICE** user for C:\Temp\simtoken\ directory and subdirectory files.
2. Navigate to the <Luna HSM Client installation Directory>/KSP directory.
3. Double-click the KspConfig.exe file to launch the KSP configuration wizard.
4. Double-click **Register Or View Security Library** on the left side of the pane.
5. Click **Browse**. Select the shim.dll file, available in the Luna Client installation folder. Click **Register**.


- SafeNet Key Storage Provider Config Wizard
File
Help
SafeNet KSP Config
Register Or View Security Library
Register HSM Slots
Browse
Register
Ready
NUM

LibraryPath C:\Program Files\SafeNet\LunaClient\shim.dll

6. On successful registration, the following message will appear on screen: **Success registering the security library!**
7. Double-click **Register HSM Slots** on the left side of the pane.
8. Register the slot as follows:
   a. Open the **Register for User** drop-down menu and select **NETWORK SERVICE**.
   b. Open the **Domain** drop-down menu and select **NT AUTHORITY**.
   c. Open the **Available Slots** drop-down menu and select the relevant partition.
   d. Enter the **Slot Password**.



Register For User: NETWORK SERVICE

Domain: NT AUTHORITY

Available Slots: 0 SHIM-LUNAHAV1

Slot Password: ********

Register By: ● Slot Label ○ Slot Number

e. Click **Register Slot**. On successful registration, the following message will appear on screen:

   The slot was successfully and securely registered!

f. Click **OK**.

Now follow the links to Configure Citrix FAS server to use Luna HSM and Renewing the Authorization (RA) key and certificate (Optional).

This completes the integration of Citrix FAS with Luna HSM using SKS Partition.

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.