

---

# Venafi Platform: Integration Guide

THALES LUNA HSM AND LUNA CLOUD HSM

**Document Information**

<b>Document Part Number</b>	007-000357-001
<b>Revision</b>	G
<b>Release Date</b>	21 June 2023

**Trademarks, Copyrights, and Third-Party Software**

Copyright © 2023 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

# CONTENTS

Overview .....	4
Certified Platforms .....	4
Certified Platforms for Luna HSM .....	4
Certified Platforms for Luna Cloud HSM .....	5
Prerequisites .....	5
Configure Luna HSM .....	5
Configure Luna Cloud HSM Service .....	6
Install Microsoft Visual C++ .....	7
Install Venafi Platform .....	7
Integrating Venafi Platform with Luna HSM .....	8
Create an HSM (Cryptoki) Connector .....	8
Enable Venafi Advanced Key Protect .....	9
Use Luna HSM in Venafi Platform .....	10
Contacting Customer Support .....	29
Customer Support Portal .....	29
Telephone Support .....	29

## Overview

This guide presents a systematic approach for integrating Thales Luna HSMs and Cloud HSMs with the Venafi Platform. By following the step-by-step procedure outlined in this guide, organizations can successfully integrate these HSMs with the Venafi Platform, and reap a multitude of advantages, including:

- > Ensuring secure key generation, storage, and protection through FIPS 140-2 level 3 validated hardware.
- > Providing full life cycle management of the keys.
- > Maintaining an audit trail through HSM.
- > Achieving significant performance enhancements by offloading cryptographic operations from application servers.

**Note:** The Luna Cloud HSM service does not have access to the secure audit trail.

## Certified Platforms

[Certified Platforms for Luna HSM](#)

[Certified Platforms for Cloud Luna HSM](#)

### Certified Platforms for Luna HSM

The integration between Venafi Trust Protection Platform and Luna HSM has been certified on the following platforms:

HSM Type	Platforms Certified
Luna HSM	Windows Server 2019 Windows 2016 Server Windows 2012 R2 Server

**NOTE:** This integration is tested in both HA and FIPS mode.

**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. The 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 integration between Venafi Trust Protection Platform and Luna Cloud HSM has been certified on the following platforms

HSM Type	Platforms Certified
Luna Cloud HSM	Windows 2016 Server Windows 2012 R2 Server

**Luna Cloud HSM:** Luna Cloud HSM platform provides on-demand, cloud-based 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 Microsoft Visual C++](#)

[Install Venafi Platform](#)

## Configure Luna HSM

If you are using Luna HSM:

1. Verify the HSM is set up, initialized, provisioned and ready for deployment. Refer to the [Luna HSM Product Documentation](#) for more information.
2. Create a partition that will be later used by Venafi TPP.
3. Generate a certificate for the Luna Network HSM and exchange it between the Luna HSM and the client system. This certificate is required to establish a secure connection (NTLS) between the Luna HSM and the client system. During this process, register the client system and assign the previously created partition to establish a connection. Assign the Crypto Officer and Crypto User roles to the registered partition. These roles define the access privileges and permissions for managing cryptographic operations within the partition.
4. Validate that the registered partition and its associated configuration have been properly set up by executing the following command to view the registered partitions:

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

Upon successful execution, you should observe an output similar to the example provided below:

```
lunacm.exe (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
```

```
Available HSMs:
```

```
Slot Id ->          0
Label ->           Venafi
```

```
Serial Number ->      1213475834492
Model ->              LunaSA 7.3.0
Firmware Version ->  7.3.0
Configuration ->     Luna User Partition With SO (PW) Signing With Cloning
Mode
Slot Description ->  Net Token Slot
```

5. Enable partition policies 22 and 23 for PED-authenticated HSM. These policies allow activation and auto-activation within the designated partition.

**NOTE:** Please refer to the [Luna HSM documentation](#) for comprehensive instructions on creating an NTLS connection, initializing partitions, and assigning different user roles.

### Set up Luna HSM High-Availability

Follow the instructions provided in the [Luna HSM documentation](#) to configure and set up two or more HSM boxes on host systems for high availability. Ensure that the HAOnly setting is enabled to enable failover functionality. In the event of the primary HSM going down, all calls will automatically route to the secondary HSM until the primary recovers and restarts.

### Set up Luna HSM in FIPS Mode

To configure Luna HSM in FIPS Mode, update the configuration file by adding or modifying the following setting within the [Misc] section:

```
RSAKeyGenMechRemap=1
```

This setting ensures that older calling mechanisms are redirected to the approved RSA key generation methods (186-3 with primes and 186-3 with aux primes) required for FIPS compliance. By making this configuration change, Luna HSM will be properly set up to operate in FIPS mode, adhering to the approved RSA key generation standards.

**NOTE:** The configuration setting mentioned above, `RSAKeyGenMechRemap=1`, is not required for the Universal Client. It is specifically applicable only for Luna Client 7.x.

## Configure Luna Cloud HSM Service

Follow these steps to set up your Luna Cloud HSM:

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 using the following command:

```
tar -xvf cvclient-min.tar
```

**NOTE:** Do not extract to a new subdirectory. Place the files in the client install directory.

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

```
source ./setenv
```

**NOTE:** To add the configuration to an already installed UC client, use the `-addcloudhsm` option when running the setenv script.

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

**NOTE:** If your organization requires non-FIPS algorithms for your operations, ensure that the Allow non-FIPS approved algorithms check box is checked. For more information, refer to [Supported Mechanisms](#).

## Install Microsoft Visual C++

Install Microsoft Visual C++ on the Venafi Platform server. Microsoft Visual C++ is required to access some HSM on Demand applications and utilities. Refer to [Microsoft Visual C++ Download Portal](#) for more information on installing Microsoft Visual C++.

## Install Venafi Platform

Install Venafi Trust Protection Platform on the target machine. For Venafi Code Signing, the installable components are:

- > Venafi Platform with Venafi Code Signing components
- > CSP for code signing workstations

Refer to [Venafi Documentation](#) for detailed instructions.

## Integrating Venafi Platform with Luna HSM

This section contains the following topics:

- > [Create an HSM \(Cryptoki\) Connector](#)
- > [Enable Venafi Advanced Key Protect](#)
- > [Use Luna HSM in Venafi Platform](#)

### Create an HSM (Cryptoki) Connector

To create an HSM connector, follow these steps:

1. Launch the **Venafi Configuration Console**.
2. In the **Venafi Configuration** pane on the right-hand side, select **Connectors**.



3. Click **Create HSM Connector** from the **Actions** pane on the right.
4. Enter the Venafi Trust Protection Platform administration credentials if needed, and then click **OK**.
5. In the **Create new HSM (Cryptoki) Connector** window that appears, fill out the **Name**, **Cryptoki Dll Path**, **Slot**, **User Type** and **Pin** fields, and then click the **Verify** button.

Create new HSM (Cryptoki) Connector

Please fill out all fields to create a new HSM connector.

Name:

Cryptoki Dll Path:

Slot:

User Type:

Pin:



- Click the **Create** button that appears under the **Permitted Keys** field.

Create new HSM (Cryptoki) Connector

Please fill out all fields to create a new HSM connector.

Name:

Cryptoki DLL Path:

Slot:

User Type:

Pin:

Permitted Keys:

(Ctrl-Click to multi-select)

Allow Key Storage (Private Keys are non-exportable)

- Verify that the HSM connector appears under the **Platform Connectors** pane.

Component	Detail	Description
Encryption Connectors		
Software	Key Generation & Data Encryption	Connector providing software-based encryption
Null	Data Encryption	Pass-through encryption driver. For data that does not need to be encrypted.
HSM	Key Generation & Data Encryption	HSM

## Enable Venafi Advanced Key Protect

Venafi Advanced Key Protect enables you to orchestrate HSM-based generation and storage of cryptographically strong keys. To enable Venafi Advanced Key Protect:

- Open the **Venafi Configuration Console** and click the **Connectors** node from the left pane.
- In the Actions panel, click **Enable Advanced Key Protect**.
- Review the information in the dialog boxes and confirm the action.
- Restart the IIS service by going to the **Product** node, selecting **Website** service, and then clicking **Restart**.
- Restart the Venafi Platform service by selecting **Venafi Platform** service, and then clicking **Restart**.
- Restart the Logging service by selecting **Logging** service, and then clicking **Restart**.

For more information on Venafi Advanced Key Protect module, refer to <https://www.venafi.com/platform/advanced-key-protect>.

## Use Luna HSM in Venafi Platform

Venafi Platform leverages Luna HSMs in the following use cases:

[Use Case I – Database Protection with HSM encryption](#)

[Use Case II - Central HSM Key Generation](#)

[Use Case III - Remote HSM Key Generation](#)

[Use Case IV – Next-Gen Code Signing](#)

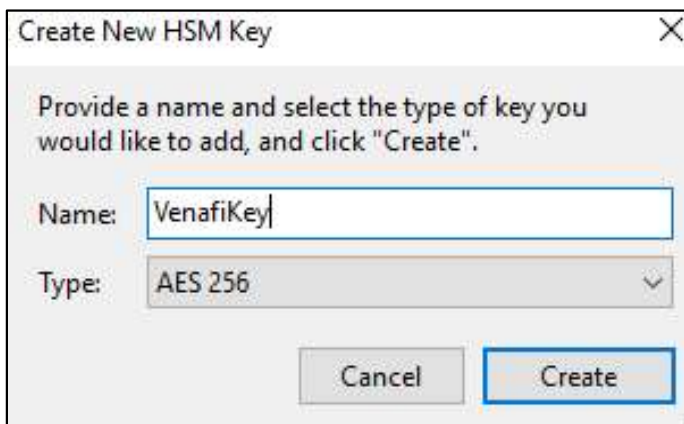
### Use Case I – Database Protection with HSM encryption

Venafi Platform maintains all system information, including configuration settings, managed server and certificate information, credentials, archived certificates, and private keys, in a database. The platform uses Luna HSMs to encrypt the information used to connect to the database, as well as to secure the encryption assets within the database, including certificate private keys, credential objects, and SSH keys.

**NOTE:** Ensure that the HSM client is configured on the system and HSM partition is accessible from the HSM client. If you are using HSM in HA mode, ensure that HAOnly is enabled from the HSM client.

### Create the encryption key

1. In **Venafi Configuration Console**, select **HSM connector** and click **Properties**.
2. In **Permitted Keys** field, click the **New Key** button to create a new encryption key on the HSM partition or service.
3. In the **Create New HSM Key** window, specify the name of the encryption key in the **Name** field, select **AES 256** from the **Type** drop down menu, and then click **Create**.



Create New HSM Key

Provide a name and select the type of key you would like to add, and click "Create".

Name: VenafiKey

Type: AES 256

Cancel Create

- Select the new key in the **Permitted Keys** field and click **Create**.

Create new HSM (Cryptoki) Connector

Please fill out all fields to create a new HSM connector.

Name:

Cryptoki DLL Path:

Slot:

User Type:

Pin:

Permitted Keys:

(Ctrl-Click to multi-select)

- The encryption key is generated on the partition. You can confirm the existence of the encryption key by executing the `partition contents` command in `lunacm` and inspecting the results.

```
C:\Program Files\SafeNet\LunaClient>lunacm.exe
lunacm.exe (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.

Available HSMs:

Slot Id ->          0
Label ->            Venafi
Serial Number ->   1254270083886
Model ->           LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration ->   Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot

Current Slot Id: 0

lunacm:> role login -n co

enter password: *****

Command Result : No Error

lunacm:> partition contents

The 'Crypto Officer' is currently logged in. Looking for objects
accessible to the 'Crypto Officer'.

Object list:

Label:              VenafiKey
Handle:             972
Object Type:        Symmetric Key
Object UID:         7a0400002c0000351380800

Number of objects: 1
```

## Use Case II - Central HSM Key Generation

Luna HSM enables you to centrally generate the private keys for certificates and SSH keys. Centrally generated private keys are exported from the HSM and stored as cipher text in the Venafi database. The private keys and certificates are installed on the target machines that will use them.

**NOTE:** Central HSM Key Generation is supported by HSM on Demand with Key Export service in Non-FIPS mode and Luna HSM with Key Export in Non-FIPS mode. Ensure that the HSM client is configured on the system and the HSM partition is accessible from the client. If you are using HSM in HA mode, ensure that HAOnly is enabled and HASync is disabled from HSM client. Ensure that the application is configured on the target machine and can be reached by Venafi Platform server.

To complete Central HSM Key Generation in Venafi Platform, you need to perform the following procedures:

- > [Create HSM connector](#)
- > [Enable Venafi Advanced Key Protect](#)
- > [Create the Certificate Authority \(CA\) template](#)
- > [Configure Certificate Object for Central HSM Key Generation](#)

---

### Create HSM Connector

To create an HSM Connector, please refer to the detailed instructions outlined in the [Creating the HSM Connector](#) section.

---

### Enable Venafi Advanced Key Protect

To enable Venafi Advanced Key Project, please refer to detailed instructions outlined in the [Enabling Venafi Advanced Key Protect](#) section.

---

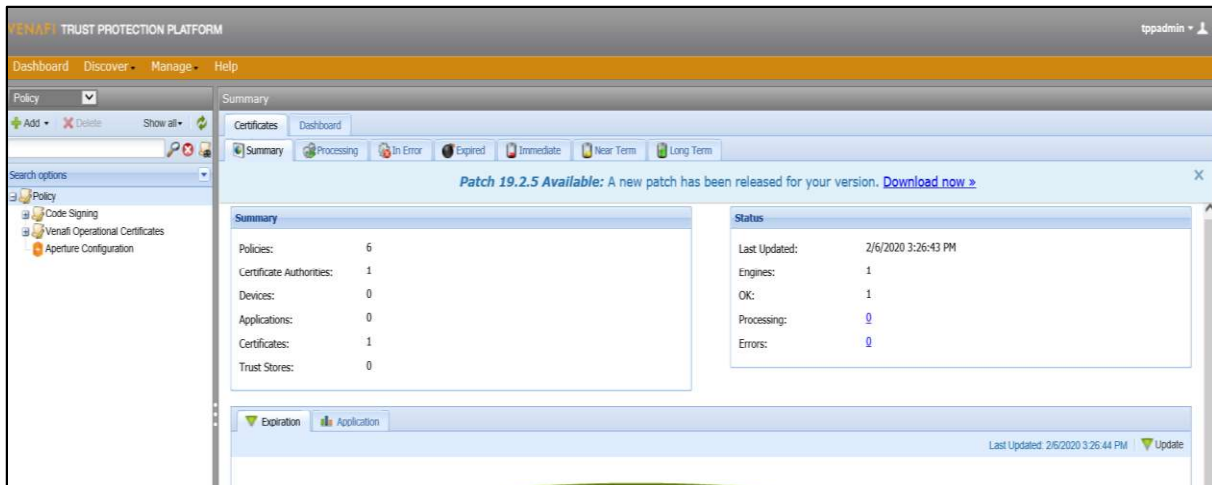
### Create the Certificate Authority (CA) template

During the certificate enrollment and provisioning procedures, every certificate object must reference a CA template object. The CA template objects provide the information that Trust Protection Platform needs to submit the certificate signing request (CSR) to the CA and retrieve the signed certificate. You can create a self-signed CA template, a DigiCert CA template, or a Microsoft CA template. Refer to [Venafi Documentation](#) for details.

## Configure Certificate Object for Central HSM Key Generation

Configure and update the Venafi platform policies to allow and use the Luna HSM for central HSM key generation. To configure test certificate for Central HSM Key Generation:

1. Log in to admin console from `https://[IP_address_of_Venafi_TPP]/vedadmin`. Select policy from the **Policy** tree in Venafi Platform.



2. Select **Policy > Settings > Certificate** tab.
3. Specify the **HSM** in the **Key Generation** drop-down menu.

Other Information

CA Template:

Key Generation:

Encryption Key:

Disable Automatic Renewal:

Allow Simple Passwords for Private Key Downloads:

Private Key PBE Algorithm:

Each algorithm type has a corresponding security/compatibility value. Generally, they are inversely related due to their adoption by software applications.

Renewal Window:  days

4. Click **Save**.
5. Right click on the selected policy.
  - a. Click **Add > Certificates > Certificate**.
  - b. Specify the details of the certificate in **General Information** tab.

- c. Open the **Management Type** drop-down menu and select **Provisioning** or **Enrollment**.

General Information

Certificate Name: ClientCertificate

Description: for client

Contact(s): local:TPPAdmin (\VED\Identity\TPPAdmin)

Approver(s): local:TPPAdmin (\VED\Identity\TPPAdmin)

Processing Disabled:

Management Type: Provisioning

Managed By:

- d. Enable the **Service Generated CSR** radio button in the **CSR Generation** field.
- e. Set Generate Key/CSR on Application to **NO**.
- f. Fill out the details in the **Subject DN** tab.
- g. Specify the key type in the **Private Key** tab.

Private Key

Private Key Stored: No

Key Algorithm: RSA

Key Strength (bits): 2048

Elliptic Curve: P256

- h. Choose the configured **CA template** in **Other Information** tab.

Other Information

CA Template: \VED\Policy\SafeNetHSM\SafeNetCA

Disable Automatic Renewal: No

Renewal Window: 30 days

- i. Click **Save**. The certificate gets generated with **Certificate Status** as **OK**.

ClientCertificate : Summary

Certificate Monitoring Validation General Support

Summary Settings Associations Compliance History

Restart Retry Reset Renew Now Check Revocation Validate Now Revoke Change Certificate Type Print

Certificate Status

OK

Expiration Date: Lifecycle Stage: none

Revocation: Last Check: never SSL/TLS Result: State: File Result:

- j. Click the **Renew Now** button. The **Certificate Status** changes from **OK** to **Queued for Renewal**. Wait for a few moments and then click the **Refresh** button located in the top right corner of the screen. Scroll down to view the certificate details. If the certificate is categorized as Provisioning, proceed with associating the certificate to the application object. Additionally, verify that the certificate has been successfully installed on the application server.



### Use Case III - Remote HSM Key Generation

To complete Remote HSM Key Generation in Venafi Platform, you need to perform the following tasks:

- > [Configure remote machine](#)
- > [Enable Venafi Advanced Key Protect on Venafi Platform](#)
- > [Create the Certification Authority \(CA\) template](#)
- > [Configure Certificate Object for Remote HSM Key Generation](#)

#### Configure remote machine

Perform the following steps on remote machine where you want to install the certificate:

1. Install Luna HSM client on the target machine and configure the partition.
2. Configure the application on the remote machine to use Luna HSM.

Refer to [Venafi Documentation](#) for the list of supported applications.

#### Enable Venafi Advanced Key Protect on Venafi Platform

To enable Venafi Advanced Key Protect, refer to the [Enabling Venafi Advanced Key Protect](#) section.

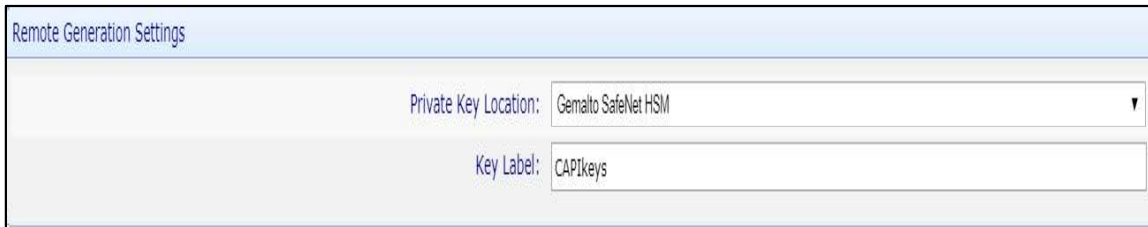
#### Create the Certificate Authority (CA) template

During certificate enrollment and provisioning procedures, every certificate object must reference a CA template object. CA template objects provide the information Trust Protection Platform needs to submit the certificate signing request (CSR) to the CA and retrieve the signed certificate. You can create a self-signed CA template, a DigiCert CA template, or a Microsoft CA template. Refer to [Venafi Documentation](#) for details.

## Configure Certificate Object for Remote HSM Key Generation

To configure the Certificate object for remote HSM key generation:

1. Log in to the admin console: `https://[IP_address_of_Venafi_TPP]/vedadmin`
2. Select the policy from the **Policy** tree in Venafi Platform.
3. Choose the application that you have configured on the target machine.
4. In the **Remote Generation Settings** window, choose **Gemalto SafeNet HSM** under the **Private Key Location** drop down and specify the key label in **Key Label** field.

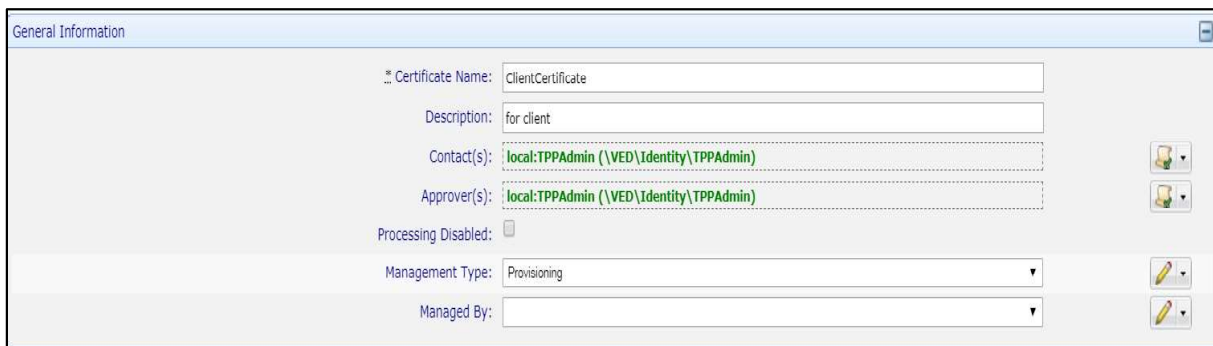


Remote Generation Settings

Private Key Location: Gemalto SafeNet HSM

Key Label: CAPIkeys

5. Click **Save** to save the application object.
6. Perform the following actions:
  - a. Right-click on the policy.
  - b. Select **Add > Certificates > Certificate**.
  - c. Provide the details of the certificate in the **General Information** tab.
  - d. Open the **Management Type** drop-down menu and select **Provisioning**.



General Information

.. Certificate Name: ClientCertificate

Description: for client

Contact(s): local:TPPAdmin (\VED\Identity\TPPAdmin)


Approver(s): local:TPPAdmin (\VED\Identity\TPPAdmin)

Processing Disabled:

Management Type: Provisioning

Managed By:

- e. Enable the **Service Generated CSR** radio button in the **CSR Generation** field.
- f. Set **Generate Key/CSR on Application** to **Yes**.



CSR Handling

CSR Generation:  Service Generated CSR  
 User Provided CSR

Generate Key/CSR on Application: Yes

Hash Algorithm: SHA-256

- g. Complete the required fields in the **Subject DN** tab.



- h. Specify the desired key type in the **Private Key** tab.

Private Key	
Private Key Stored:	No
Key Algorithm:	RSA
Key Strength (bits):	2048
Elliptic Curve:	P256

- i. In the **Other Information** tab, select the appropriate CA template.

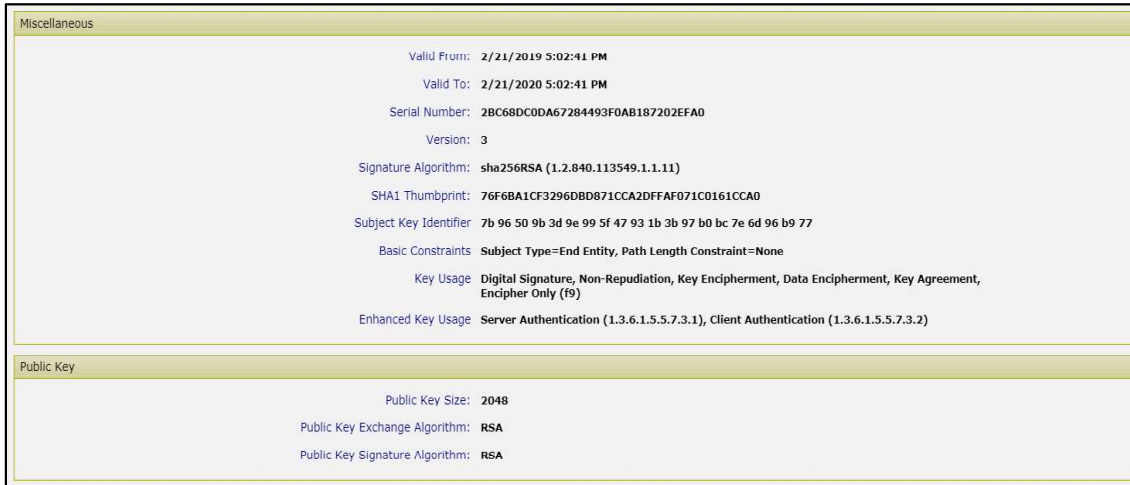
**NOTE:** Remote HSM key generation is not compatible with self-signed CA template.

7. Click **Save**. The certificate will be generated with the **Status OK**.

The screenshot shows the 'ClientCertificate : Summary' page. The 'Certificate Status' section displays a green checkmark and the text 'OK'. Below this, there are four fields: 'Expiration Date', 'Lifecycle Stage' (set to 'none'), 'Revocation', and 'Validation'. The 'Validation' section shows 'Last Check: never', 'SSL/TLS Result:', 'State:', and 'File Result:'.

8. Navigate to the application object where you want to associate the certificate. In the Certificate section, choose the renewed certificate from the **Associated Certificate** field. Click **Save**.
9. Return to the certificate object and click **Renew Now**. The certificate status will change from **OK** to **Queued for Renewal**.

10. Wait for some time and then click refresh icon in top-right corner. Scroll down to view the details of the renewed certificate.



11. Once the installation process is completed on the target machine, the status will return to **OK**.
12. Verify that the certificate is installed and that the keys are created on the HSM.

```
C:\Program Files\SafeNet\LunaClient>lunacm.exe
lunacm.exe <64-bit> v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.

Available HSMs:

Slot Id ->          0
Label ->            Venafi
Serial Number ->   1254270003886
Model ->            LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration ->   Luna User Partition With SO <PW> Key Export With Cloning Mode
Slot Description -> Net Token Slot

Current Slot Id: 0

lunacm:> role login -n co

enter password: *****

Command Result : No Error

lunacm:> partition contents

The 'Crypto Officer' is currently logged in. Looking for objects
accessible to the 'Crypto Officer'.

Object list:

Label:              CAPIkeys
Handle:              2217
Object Type:         Private Key
Object UID:          a60e00002e00000351380800

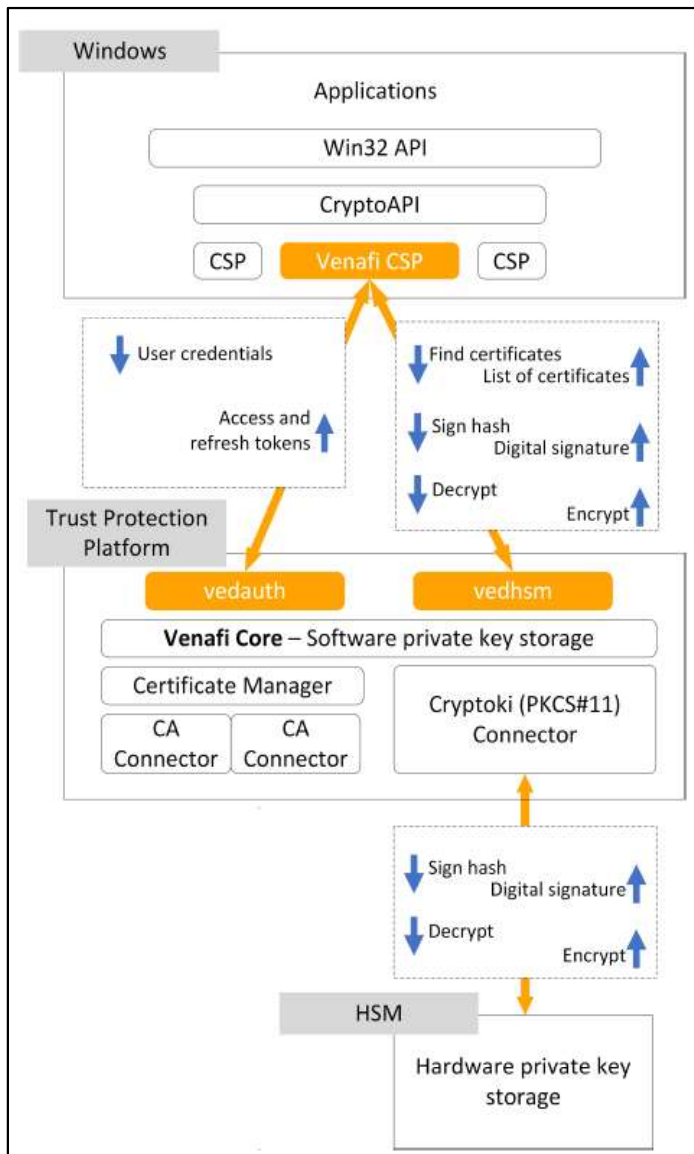
Label:              CAPIkeys
Handle:              2219
Object Type:         Public Key
Object UID:          a50e00002e00000351380800
```

### Use Case IV – Next-Gen Code Signing

Venafi Next-Gen Code Signing secures all private keys, automates code-signing workflows, and maintains a record of all code signing activities. To leverage Luna HSMs for secure storage of code signing keys, it is necessary to establish a connection between the HSMs and the Venafi Platform. Once the connection is established, the Luna HSMs can be utilized as a trusted key storage option when configuring code signing projects.

**NOTE:** Before proceeding with the integration, the Venafi Next-Gen Code Signing software license must be enabled to ensure proper functioning of the solution.

Trust Protection Platform uses the vedauth and vedhsm endpoints to facilitate authentication and HSM functions, as shown in the figure below.



To complete code signing in Venafi Platform, you need to perform the following procedures:

1. [Enable Key Storage in the HSM Connector](#)
2. [Enable Venafi Advanced Key Protect](#)
3. [Assign the Code Signing Administrator](#)
4. [Create the Certificate Authority \(CA\) template](#)
5. [Create the Signing Flow](#)
6. [Create the Environment Template](#)
7. [Create the Code Signing Project](#)
8. [Edit an existing environment](#)
9. [Approve the Code Signing Project](#)
10. [Install and Configure the Venafi Crypto Service Provider \(CSP\)](#)
11. [Sign code using Venafi Code Signing](#)

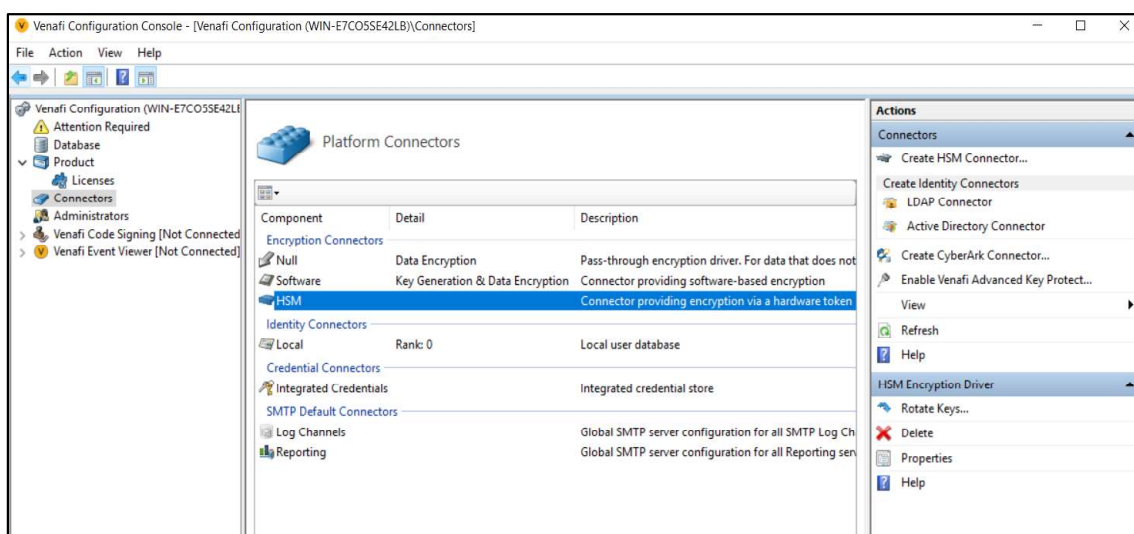
## 1. Enable Key Storage in HSM Connector

**NOTE:** Ensure that the HSM service client is configured on the host system and that the HSM partition or Luna Cloud HSM service is accessible over **lunacm**.

The HSM connector provides the HSM credential information to Venafi, allowing Venafi to access the signing keys stored on the HSM. You create the HSM connector using the **Venafi Configuration Console**. To create the HSM Connector, refer to [Creating a HSM \(Cryptoki\) connector](#).

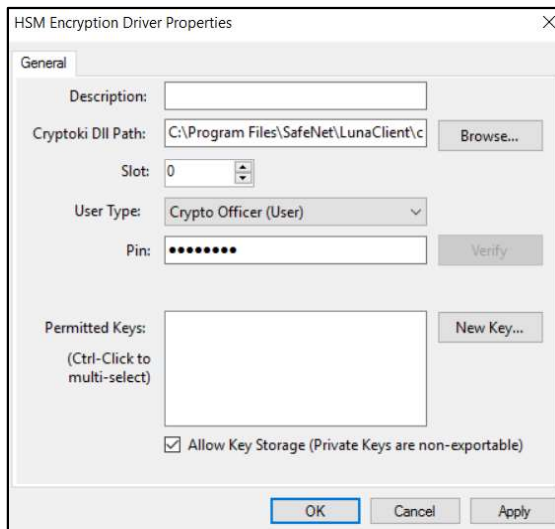
To enable Key Storage in HSM connector:

- a. Open the Venafi Configuration Console, and click the **Connectors** node from the **Venafi Configuration** pane.



- b. Select HSM connector under Encryption Connectors and click **Properties** in Actions pane. **HSM Encryption Connector Properties** screen will appear.

- c. Select the **Allow Key Storage** check box and click **Apply > OK**.



- d. Restart the Venafi services.

## 2. Enable Venafi Advanced Key Protect on Venafi Platform

To enable Venafi Advanced Key Protect, please refer to the [Enabling Venafi Advanced Key Protect](#) section.

## 3. Assign the Code Signing Administrator

The **Administrators** node allows you to view, assign, and delete Code Signing Administrator users. Add the Code Signing Administrator capability to an existing Venafi user. To assign the Code Signing Administrator:

- Click the **Administrators** node in Venafi Configuration Console.
- In the Actions panel, click on **Add Code Signing Administrator**.
- Search for the user you want to assign as a Code Signing Administrator and click **Select**.

## 4. Create the Certificate Authority (CA) template

Each environment in a code-signing project requires a CA template. You can create a self-signed CA template, a DigiCert CA template, or a Microsoft CA template. Refer to [Venafi Documentation](#) for details.

## 5. Create the Signing Flow

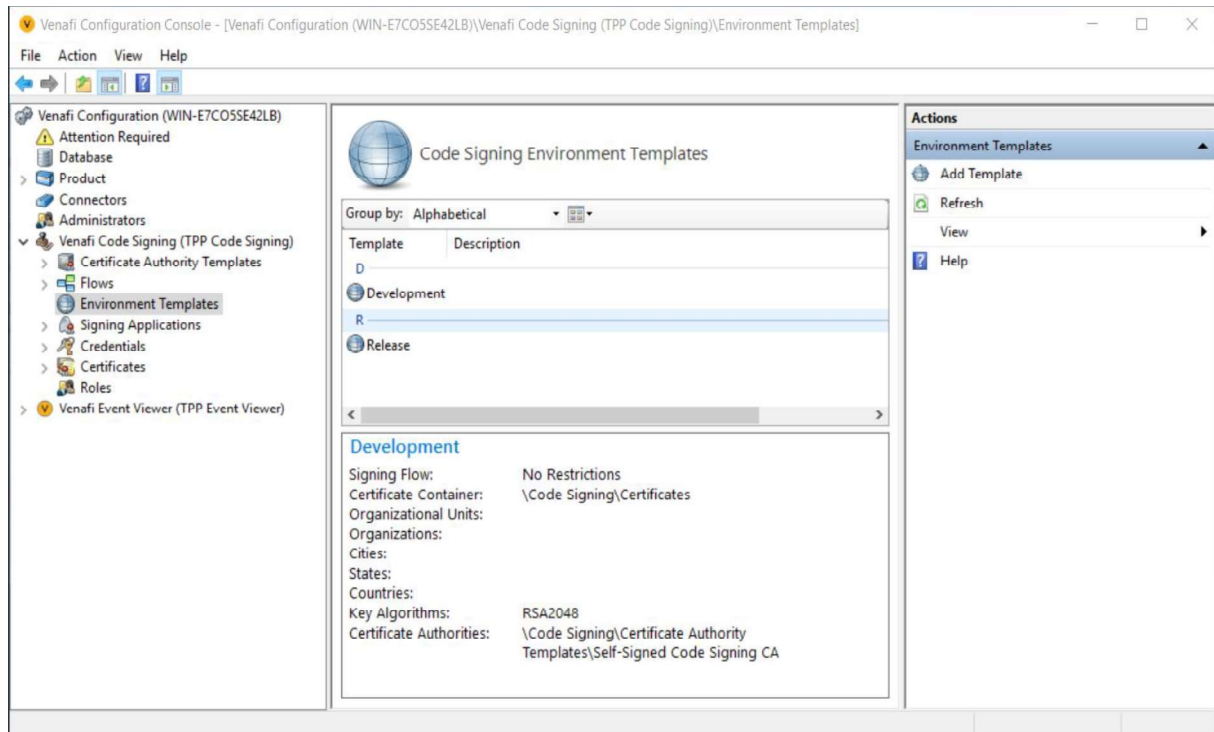
Flows in Venafi Code Signing define the approvals that must be granted before a signing can take place using a given private key. Create the Venafi approval flow to define the required approvals for code signing. To create the Signing Flow:

- In the Flows node, click Add a new Code Signing Flow in the Actions Panel.
- Specify the name of the flow and click **Create**.
- Record the Signing Flow name; it is required for an upcoming procedure.
- Configure the flow by adding Approvers. Refer to [Venafi Documentation](#) for details.

## 6. Create the Environment Template

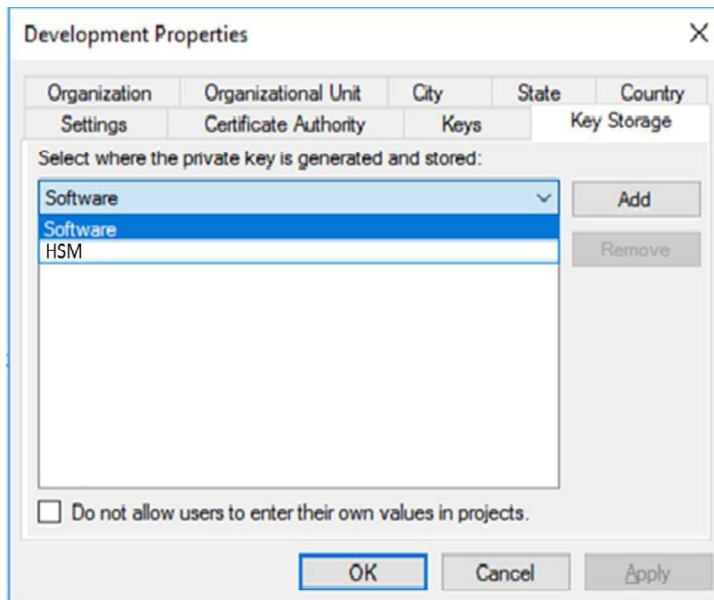
Code Signing Environment Templates allow the Code Signing Administrator to suggest or require specific values to be used in code signing Projects. Each project requires at least one environment. To create the Environment Template:

- a. In the **Venafi Code Signing** node of the Venafi Configuration Console, select **Environment Templates**.



- b. Click **Add Template** from the Actions panel.
- c. Specify the name of the template. The **Development Properties** wizard displays.
- d. Under **Settings**, specify **Description**, **Certificate Container** and the **Signing Flow** created in the previous procedure.
- e. Under the **Certificate Authority** tab, specify the CA template created in the earlier procedure.
- f. Under the **Keys** tab, select the RSA key length values you want to allow. This algorithm and key length appears as part of the certificate.

- g. Under the **Key Storage** tab, click on the drop-down menu and select the **HSM Connector** created in a previous procedure. Click **Add**.



- h. You can specify additional details, such as the **Subject Domain Name** of the certificate, in the remaining tabs, but they are not required to complete the integration.

## 7. Create the Code Signing Project

Code signing projects govern the use of private code signing keys. Code signing projects rely on settings defined in the Environment Template. To create a Code Signing Project with the Venafi platform, follow these steps:

- a. Log in to Aperture by navigating to `https://[IP_address_of_Venafi_TPP]/Aperture/codesigning`.
- b. On the project list screen, click on **Add Project** to initiate the project configuration wizard.
- c. Provide a **Project Name** and **Description**, and then click **Next**. You'll be prompted to select the **Environment** to associate with the Project.

**NOTE:** If you intend to use an existing key and certificate, you can skip step d.

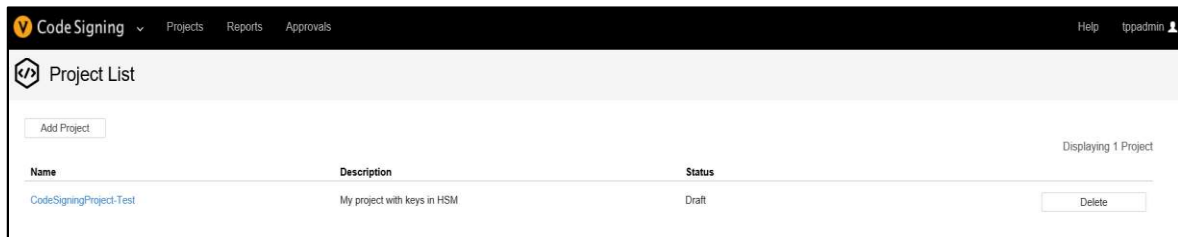
- d. To create an environment that generates a new certificate and private key, follow these steps:
  - i. Click the **Add Environment** card.
  - ii. From the **Environment Type** drop-down, select the desired environment type.
  - iii. Choose the appropriate certificate provider from the **Certificate Provider** drop-down list. If only one certificate provider is assigned to this environment, it will be automatically selected.
  - iv. Enter a name for the environment in the **Environment Name** box.
  - v. Ensure that **Key Storage** location is set to HSM connector.
  - vi. Fill in the remaining fields based on the Subject DN of the certificate.
  - vii. Click **Add** to create the environment.

- e. Click **Next** to proceed.
- f. Assign the appropriate Users and Approvers to the project.
- g. Click **Next** to continue.
- h. Optionally, you can specify the signing applications that are allowed to use this project by entering them in the **Permitted Applications** field.
- i. If you want to create new certificate and private key on approval, click **Submit for Approval**. Skip the [Edit an existing environment](#) section and proceed to the [Approving the Code Signing Project](#) section.
- j. If you prefer to use an existing key or certificate, click **Save as Draft**.

## 8. Edit an existing environment

If you want to use existing key or certificate as a code signing key, follow these steps:

- a. From the project list, select the Draft project created in previous section.



- b. Click **Environments**.
- c. Select **Use Existing Key in HSM**.
- d. Select **Environment Template** from drop down and specify **Environment Name**.

**Add New Environment**

Choose an Environment Template

Development

Environment Name

ExistingKey

Cancel OK

- e. Click **OK**. **Import Key from Existing HSM** will appear.
- f. Select **HSM connector** name in **Key Storage Location** drop down.
- g. Select existing key pair on HSM in **Private Key** and **Public key** drop downs.



- h. Specify **Certificate Provider** and Certificate DN details in respective fields.

- i. Click **Save**.
- j. Click **Submit for Approval**.
- k. The project will be submitted for approval by the Code Signing Administrator.

## 9. Approve the Code Signing Project

After the code-signing project is submitted for approval, the Code Signing Administrators receive an email informing them that a project is ready for review. The Code Signing Administrators needs to follow these steps for reviewing and approving the code-signing project:

- Sign into Aperture at [https://\[IP\\_address\\_of\\_Venafi\\_TPP\]/Aperture/codesigning](https://[IP_address_of_Venafi_TPP]/Aperture/codesigning).
- In the Code Signing menu, click **Approvals > Pending Approvals**.
- Click **Approve** for the Code Signing Project created in the previous procedure. At this point, if you have selected to generate new key pair on HSM, the keys are created.

```
lunacm:> partition contents

The 'Crypto Officer' is currently logged in. Looking for objects
accessible to the 'Crypto Officer'.

Object list:

Label:      RSA 2048 26956599
Handle:     618
Object Type: Private Key
Object UID: 5e0d00002e00000554380800

Label:      RSA 2048 26956599
Handle:     140
Object Type: Public Key
Object UID: 5d0d00002e00000554380800
```

This completes the configuration for Venafi Code Signing Project.

## 10. Install and Configure the Venafi Cryptographic Service Provider (CSP)

The Venafi Cryptographic Service Provider (CSP) is the bridge between the workstation on which code signing operations take place and the Venafi Platform server that stores and manages use of private code signing keys. Install the Venafi CSP on every workstation where code will be signed using private keys managed by Venafi Platform. The Venafi CSP communicates with the Venafi Platform server over a TLS-encrypted REST API.

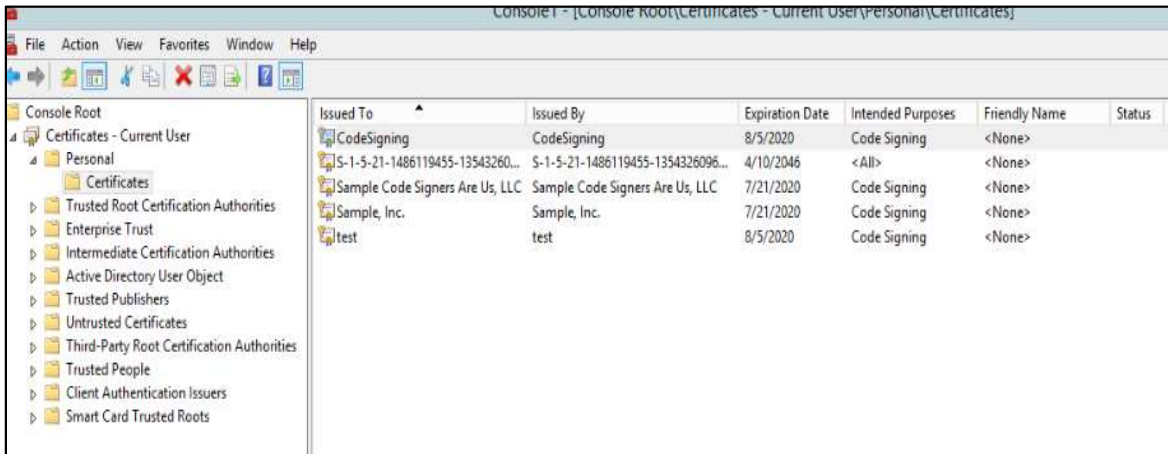
The Venafi CSP supports both CSP and KSP. The Venafi CSP only supports RSA certificates.

To install and configure the Venafi CSP:

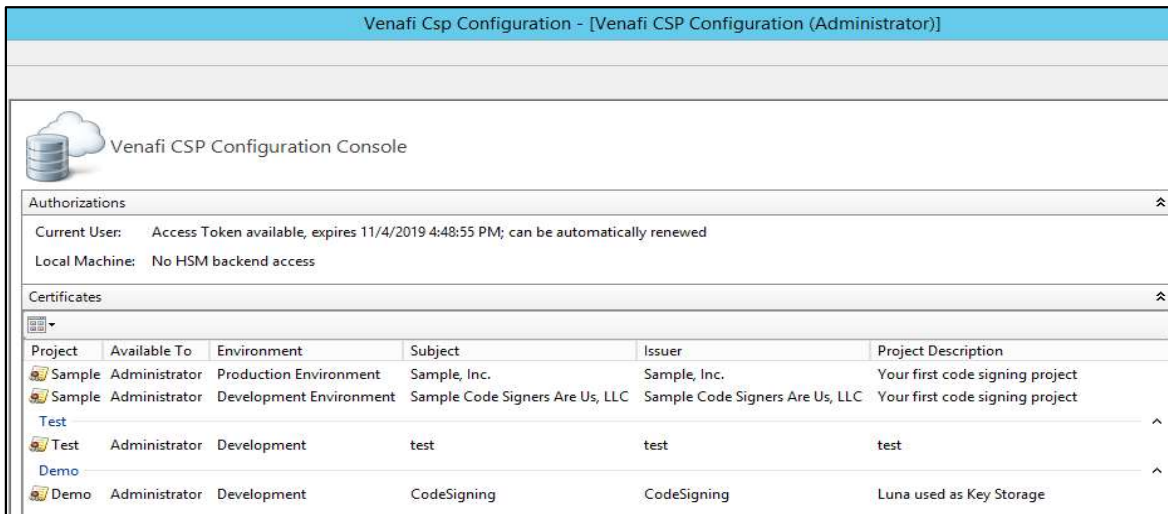
- a. Obtain the appropriate Venafi CSP installation file: VenafiCSP-x64.msi for 64-bit Windows or VenafiCSP-x86.msi for 32-bit Windows.
- b. Run the CSP installation file as an administrator on the client machine. This will launch the CSP installation wizard.
- c. Accept the license agreement, and click **Next** to proceed.
- d. Select the location where you want the CSP to be installed, and then click **Next**.
- e. Click **Install** to begin the installation process. On the Welcome screen, you can select whether you want to use an answer file for this installation. Click **Next** to continue.
- f. On the **Before You Begin** screen, verify that you have all the information you need to complete installation.
- g. On the **Host URLs** screen, enter the URL addresses for the **Authentication Server** and the **HSM Server**.
  - **Authentication Server URL:** `https://<IP_address_of_Venafi_TPP>/vedauth`
  - **HSM Server URL:** `https://<IP_address_of_Venafi_TPP>/vedhsm`
- h. Click **Next** to proceed.
- i. On the **Access Authorization** screen, enter your Trust Protection Platform user name and password. Check whether you want to enable access for the Current User only, Local Machine only, or both.
- j. On the **Configure CSP** screen, specify the location where the configuration progress and errors will be logged.
- k. Click **Finish**.

## 11. Sign code using Venafi Code Signing

When a Key User or a Local Machine is issued a grant, the associated certificates permitted to be used by that user or machine are installed in the CAPI store. These certificates can be used by the signing applications as code signing certificates.



The certificate and Project Details are visible in Venafi CSP Configuration Console and on the client machine.



This integration guide provides example material to sign applications:

Example 1: Using jarsigner

Example 2: Using signtool

---

### Example 1: Using jarsigner

Execute the `jarsigner` command to sign the `.jar` files on the target machine using the installed Code Signing Certificate.

```
C:\Program Files\Java\jdk1.8.0_101\bin>jarsigner.exe -storetype Windows-My -keystore NONE sample.jar -signedjar signedsample.jar CodeSigning
jar signed.

Warning:
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not be able to validate this jar after the sign
evocation date.

C:\Program Files\Java\jdk1.8.0_101\bin>jarsigner -verify signedsample.jar
jar verified.
```

---

### Example 2: Using signtool

Execute the `signtool` command to sign the `.exe` or `.dll` files on target machine using the installed Code Signing Certificate.

```
C:\Users\Administrator\Desktop>signtool sign /n "codesigning" sample.dll
Done Adding Additional Store
Successfully signed: sample.dll

C:\Users\Administrator\Desktop>signtool sign /n "codesigning" sample.exe
Done Adding Additional Store
Successfully signed: sample.exe
```

This completes the Venafi Code Signing integration with the Luna HSM or Luna Cloud HSM service.

---

## 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.