Microsoft OCSP: Integration Guide

THALES LUNA HSM AND DPOD LUNA CLOUD HSM

Document Information

Document Part Number	007-011100-001
Revision	T
Release Date	13 January 2021

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Overview

This document guides security administrators through the procedure for installing, configuring and integrating Microsoft Online Certificate Status Protocol (OCSP) with a Luna HSM or Luna Cloud HSM service. Microsoft OCSP uses the Luna HSM or Luna Cloud HSM service to secure signing keys for OCSP operations. The Microsoft online responder service implements the OCSP by decoding revocation status requests for specific certificates. The service evaluates the status request for these certificates and sends back a signed response containing the requested certificate status information.

The integration between Luna HSMs or Luna Cloud HSM service and OCSP uses the industry standard PKCS#11 interface to generate the identity keys and provide security by protecting the Identity private keys within a hardware security module. The benefits of using Luna HSMs to generate the signing keys for OCSP are:

- Secure generation, storage, and protection of the private keys on FIPS 140-2 level 3 validated hardware.
- Full life cycle management of the keys.
- Access to the HSM audit trail*.
- Significant performance improvements by off-loading cryptographic operations from signing servers.

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

About the Microsoft Online Responder

The Microsoft OCSP implementation is separated into client and server components.

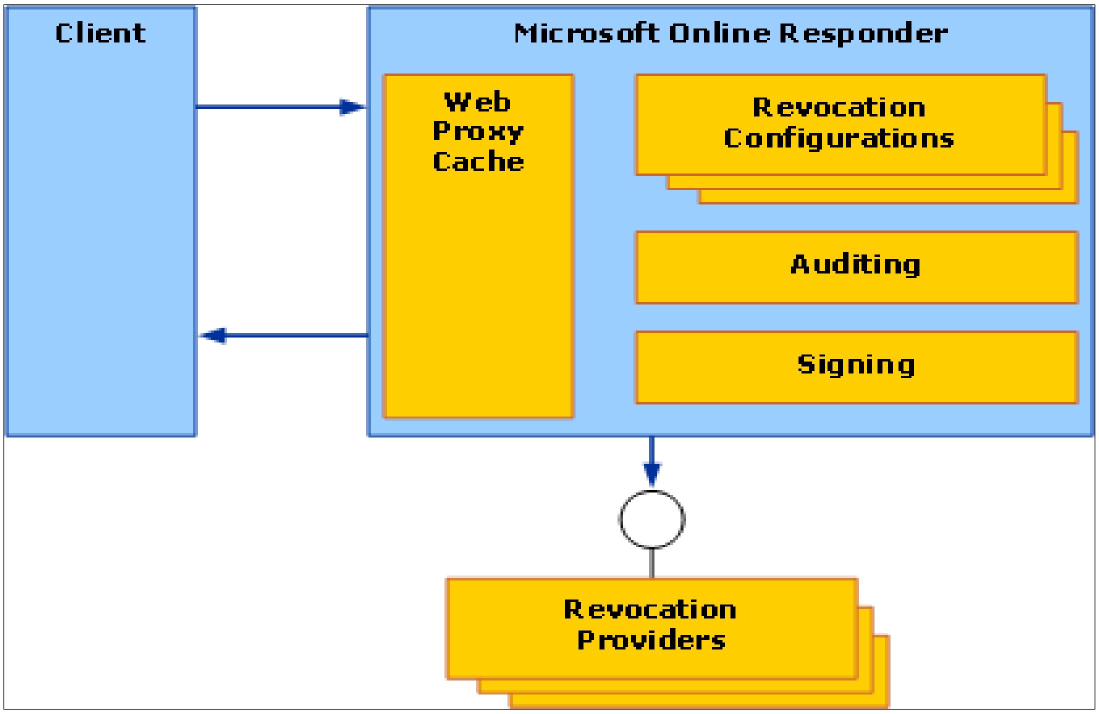


Figure 1: The client component is built into the Crypto API 2.0 library

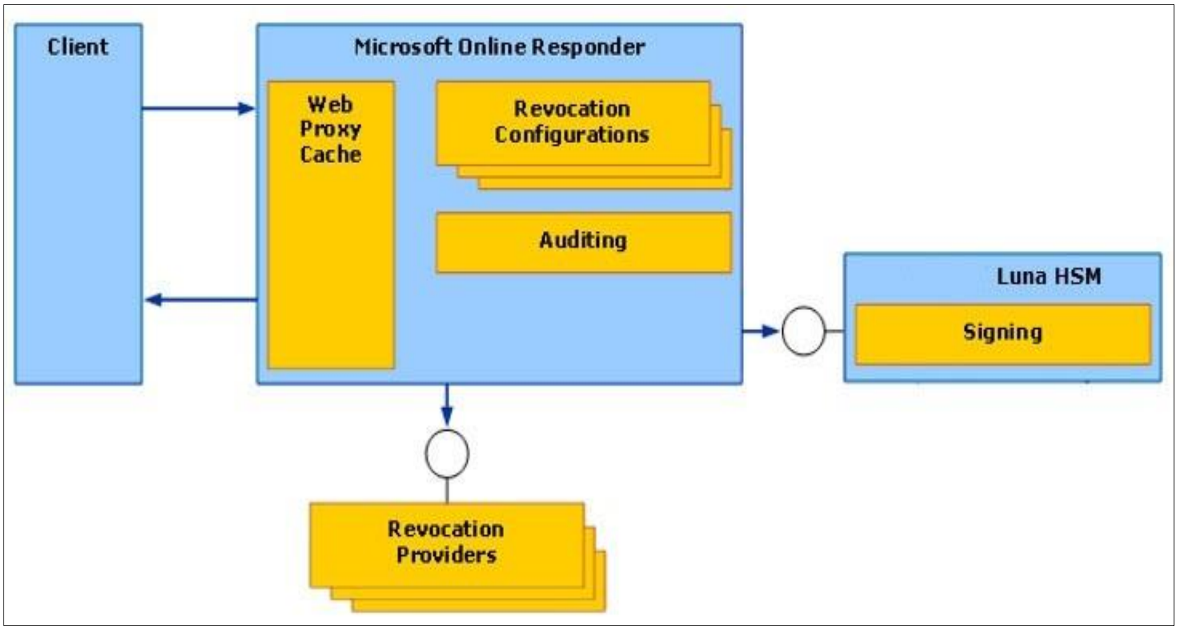


Figure 2: Microsoft Online Responder Components after integration with Luna HSM

Certified Platforms

This integration is certified on the following platforms:

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

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, 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.

> **NOTE:** This integration is tested with Luna HSM clients in both HA and FIPS Mode.

Luna Cloud HSM: Luna Cloud HSM is a cloud-based platform that 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.

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

Prerequisites

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

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 MS OCSP.
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) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights
reserved.

Available HSMs:

Slot Id ->              0

Label ->                OCSP

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. 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 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 for Luna Client 7.x.

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.

```
[Windws]
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 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. Copy the server and partition certificates from the Cloud HSM service client directory to Luna client certificates directory:

   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\Safenet\Lunaclient\cert\
[Linux default location for Luna Client]
/usr/safenet/lunaclient/cert/
```

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

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

   ```
   [Windows]
   ```

   ```
   crystoki.ini
   ```

   ```
   [Linux]
   ```

   ```
   Chrystoki.conf
   ```

7. Edit the Luna Client configuration file and add the XTC and REST sections copied from Cloud HSM service client configuration file.

8. Change server and partition certificates path from step 5 in XTC and REST sections. Do not change any other entries provided in these sections.

   [XTC]

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

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

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

9. 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\Safenet\Lunaclient\plugins\
   ```

   ```
   [Linux Default]
   ```

   ```
   /usr/safenet/lunaclient/plugins/
   ```

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

11. 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/
```

12. 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:** Refer to Luna Cloud HSM documentation for detailed steps about creating service, client, and initializing various user roles.

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.

To 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.

Set up Microsoft OCSP

> **NOTE:** All machines in the OCSP setup require Domain Administrator privileges.

Microsoft OCSP must be installed on the target machine using the following setup:

- Windows Server machine that will be used as a Domain Controller.
- Windows Server machine that will be used as CA and OCSP Server.
- Windows machine, which will become a client to submit enrolment requests to the CA.

The three machines utilized are denoted in the setup as follows:

- **OCSPDC**: Windows Server Domain Controller machine.
- **OCSPSERV**: Windows Server CA and OCSP Server machine.
- **OCSPCL**: Windows Server client machine.

You can install Microsoft OCSP and CA on separate machines. If you are configuring your OCSP on separate machines, the following setup is recommended:

- **OCSPCA:** Windows Server machine, which will become a Domain Controller and CA.
- **OCSPSERV:** Windows Server machine, which will become an OCSP Server.
- **OCSPCL:** Windows machine, which will become a client to submit enrolment requests to the CA.

Register Security Library

Install the KSP for generating the CA certificate keys on the Luna HSM or Luna Cloud HSM service. Refer to Register SafeNet Key Storage Provider section below for more information about configuring and registering SafeNet KSP. The tool **KspConfig.exe** is included in the Luna Client installation directory or is available in the HSMoD service client package.

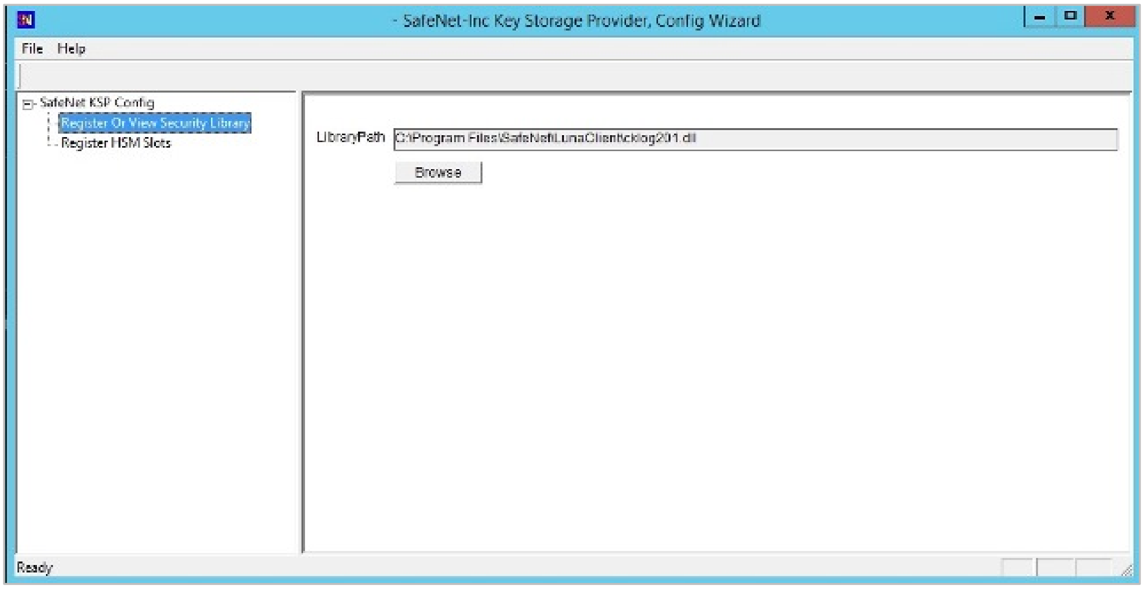
Alternatively, you can use the CSP to generate the OCSP signing keys. To use CSP for OCSP signing keys, you also need to register the CSP. See Register the SafeNet CSP section for more information about configuring and registering SafeNet CSP.

> **NOTE:** If you are configuring Microsoft OCSP on multiple systems, the SafeNet Key Storage Provider must be configured on the Certificate Authority and OCSP server systems.

Register SafeNet Key Storage Provider

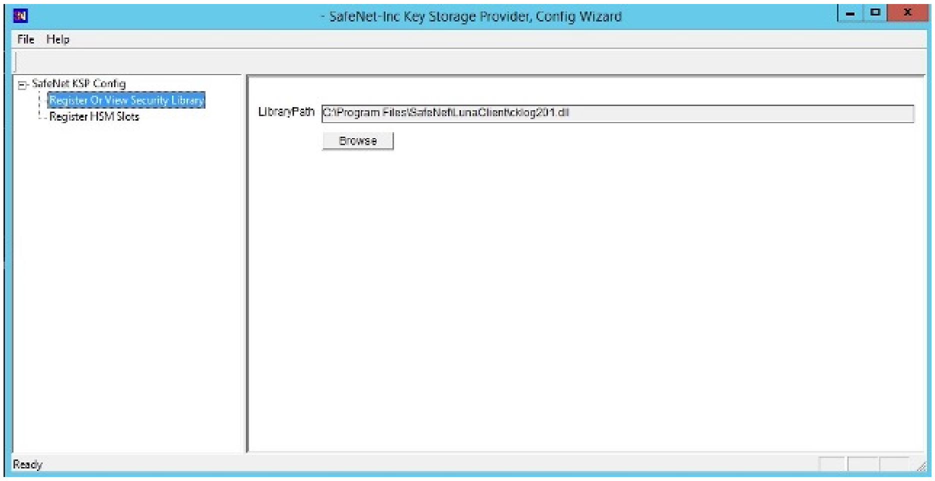
To register the SafeNet Key Storage provider:

1. Navigate to the KSP installation directory. Execute **KspConfig.exe**.
2. Double-click **Register Or View Security Library** on the left side of the pane.


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

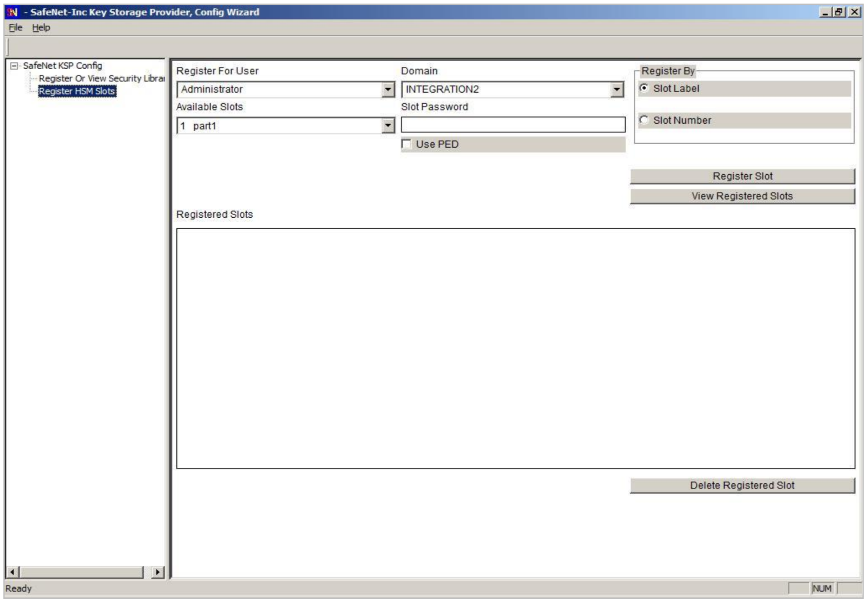
LibraryPath C:\Program Files\SafeNet\LunaClient\cklog201.dll

3. Click **Browse.** Select the cryptoki.dll file, available in the Luna Client installation folder or Luna Cloud HSM service client package. Click **Register.**


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

LibraryPath: C:\Program Files\SafeNet\LunaClient\cklog201.dll

4. On successful registration a confirmation message appears on the screen. Click **OK**.
5. Double-click **Register HSM Slots** on the left side of the pane.
6. Register the slot for the Administrator user as follows:
   a. Open the **Register for User** drop-down menu and select **ADMINISTRATOR**.
   b. Open the **Domain** drop-down menu and select your domain
   c. Open the **Available Slots** drop-down menu and select the relevant service or partition.
   d. Enter the **Slot Password**
   e. Click **Register Slot**.
   f. On successful registration, a confirmation message will appear on the screen. Click **OK**.



Register For User: Administrator

Domain: INTEGRATION2

Available Slots: 1 part1

Slot Password:

□ Use PED

Register By: ● Slot Label ○ Slot Number

7. Register the same service or partition for the **NT_AUTHORITY\SYSTEM** user.

Register the SafeNet CSP

To register the SafeNet CSP, SafeNet Luna CSP should be installed on the OCSP Server machine for OCSP signing using CSP generated keys. The steps involved are as follows:

> **NOTE:** If you want to use CSP generated OCSP signing keys you must register the SafeNet CSP. If you are configuring the Microsoft OCSP on multiple systems, the CSP must be configured and registered on both the Certificate Authority and OCSP server systems.

1. Log on to the OCSP Server as domain administrator.
2. Run the command, register.exe to register Luna CSP. The general form of command is:
   ```
   C:\Program Files\SafeNet\LunaClient\CSP>register.exe
   ```
3. Provide the partition password when asked.
4. List the Luna Cryptographic Services for Microsoft Windows and verify that the Luna CSP is available.
   ```
   C:\Program Files\SafeNet\LunaClient\CSP>register.exe /l
   ```
5. Restart the server for the changes to take effect.

Integrating Microsoft Online Certificate Service Protocol with Luna HSM

To setup Luna HSMs for Online Certificate Status Protocol (OCSP), complete the following steps:

> Set up an enterprise root certificate authority

> Install online responder service

> Configure CA to issue OCSP response signing certificates

> Creating a revocation configuration

> Verify auto-enrollment

> Verify OCSP integration

Set up an enterprise root certificate authority

An enterprise root CA is used to issue certificates to the Online Responder service, client computers, and publish certificate information to the Active Directory Domain Services (ADDS). To set up an enterprise root certificate authority, you need to:

Install ADCS and CA role

Configure ADCS and CA role

> **NOTE:** If you are installing both the CA and OCSP on the same machine, you need to log on to OCSPSERV to install the CA role.

Install ADCS and CA role

To install ADCS and CA role:

1. Log on to **OCSPCA** as a Domain Administrator.
2. From the **Start menu**, select **Administrative Tools** and click **Server Manager**.
3. In the Server Manager Dashboard (in the right pane of the window), click **Manage** and then select **Add Roles and Features.**
4. In the **Add Roles and Features Wizard**, click **Next**.
5. On the Installation Type page select the **Role-based or feature-based installation** check box. Click **Next**.
6. On the Server Selection screen select a server from the server pool and select the listed server then click **Next**.
7. Select **Active Directory Certificate Services** from the Roles list. The Add Features dialog displays. Click **Add Features**. Click **Next.**
8. On the Features page, click **Next.**
9. On the ADCS page, click **Next.**
10. On the **Role Services page**, select the **Certificate Authority** and **Certificate Authority Web Enrollment** check boxes in the **Role Services** list. The Add Features dialog displays.
11. Click **Add Features** and click **Next**.
12. On the Web Server Role (IIS) page, click **Next**.
13. On the Role Services page, click **Next**.
14. Select the **Restart the destination server automatically if required** check box. A confirmation message displays, click **Yes**.
15. Click **Install** on the Confirmation page and wait to finish the installation.

Configure ADCS and CA role

To configure ADCS and CA role:

1. If continuing from the last procedure, click **Configure Active Directory Certificate Server** on the destination server.
2. Alternatively, you can open the ADCS configuration wizard by clicking the **Notification Flag** and configuring the server role. The ADCS Configuration Wizard will be displayed.
3. On the **Credentials** page, click **Next**.
4. On the Role services page select the **Certificate Authority** and **Certification Authority Web Enrollment** check boxes. Click **Next**.
5. On the Setup Type page, select **Enterprise CA** . Click **Next**.
6. On the CA Type page, select the **Root CA** radio button and click **Next**. Click **Next**.
7. On the Private Key page, select the **Create a new private key** check box. Click **Next**.
8. In the **Cryptography for CA** window, select and set up the provider you wish to use for the CA.
9. The following Cryptographic Providers should be available for use:

NOTE: If the following objects are not available under the Cryptographic Provider drop-down menu, you need to verify your KSP/CSP Registration.

```
- RSA#SafeNet Key Storage Provider
- DSA#SafeNet Key Storage Provider
- ECDSA_P256#SafeNet Key Storage Provider
- ECDSA_P384#SafeNet Key Storage Provider
- ECDSA_P521#SafeNet Key Storage Provider
```

NOTE: Ensure that sha’ hashing algorithm is used.

10. After selecting and setting up the Cryptographic Provider, click **Next**.
11. On the Configure CA Name page enter the **CA Name** or accept the default CA name. Click **Next**.
12. On the Validity Period page specify the certificate validity period. Click **Next**.
13. Specify the database location or accept the default location on the Certificate Database page and click **Next**.
14. Verify that the CA you are about to configure is appropriate. Click **Configure** and wait for the confirmation message. If everything is correct, the Configuration succeeded message will display when the configuration completes.
15. Click **Close** to exit the ADCS Configuration wizard.

Install online responder service

To install the Online Responder service:

1. Log on to **OCSPSERV** as a domain administrator.
2. From the **Start menu**, select **Administrative Tools** and click **Server Manager**.
3. In the **Server Manager Dashboard** (in the right pane of the window), click **Manage** and then click **Add Roles and Features**.
4. In the **Add Roles and Features Wizard**, click **Next**.
5. On the Installation Type page, select the **Role-based or feature-based installation** check box. Click **Next**.
6. On the Server Selection screen, click the **Select a server from the server pool** check box and select the listed server. Click **Next**.
7. Select the **Active Directory Certificate Services** check box in the Roles list. The **Add features** dialog displays. Click **Add Features** to add the required features for the server role. Click **Next**.
8. On the Features page, click **Next**.
9. On the ADCS page, click **Next**.
10. On the Role Services page, deselect the **Certification Authority** check box and select the **Online Responder check box.** The **Add Features** dialog displays. Click **Add Features** to add the required features for the server role. Click **Next**.
11. On the features page, click **Next**.
12. Select the **Restart the destination server automatically if required** check box. A confirmation message displays. Click **Yes**.

13. On the Confirmation page click **Install**.
14. Click **Configure Active Directory Certificate Server** on the destination server. The **ADCS Configuration Wizard** displays.

> **NOTE**: You can access the ADCS Configuration Wizard by clicking the **Notification Flag**.

15. On the Credentials page, click **Next**.
16. On the Role Services page, select the **Online Responder** check box. Click **Next**.
17. On the **Confirmation** page, click **Configure** and wait for the confirmation message. A message displays after successful configuration.
18. On the Results page, click **Close** to exit the ADCS Configuration Wizard.

Configure CA to issue OCSP response signing certificates

To configure the CA to support the Online Responder Service, you must configure the certificate templates and issuing properties for OCSP Response Signing Certificates.

> **NOTE:** If you have installed the CA and OCSP on same machine then you need to complete this procedure on OCSPSERV to configure OCSP Response Signing Certificate.

Configure certificate templates using SafeNet KSP

To configure certificate templates using SafeNet KSP:

> **NOTE:** To generate the OCSP signing keys using SafeNet CSP instead of SafeNet KSP, refer to Configure certificate templates using SafeNet CSP.

1. Log in to **OCSPCA** as a domain administrator.
2. Click **Search**, type **MMC** and press **Enter** to open the console.
3. In the **mmc** console, select **File** and click **Add/Remove Snap-in…**
4. In the **Add or Remove Snap-Ins** dialog box, select the **Certificate Templates** snap-in (under the Available snap-ins section).
5. Click **Add**, and then click **OK**.
6. Under **Console Root**, expand the **Certificate Templates** snap-in. The middle section lists all of the available certificate templates that CA can issue.
7. Scroll down the list until you locate the **OCSP Response Signing template**. Right-click the template and select **Properties**. The Template properties dialog displays.
8. Click the **General** tab**,** and select the **Publish Certificate in the Active Directory** check box.
9. Set the **Validity Period** and **Renewal period**.

> **NOTE:** For testing purpose, this guide assumes the **Validity period** and **Renewal period** for four hours and one hour for **Auto Renewal.**

10. Click the **Security** tab and select **Add**. The **Select User, Computers, Service Accounts, or Groups** dialog displays.
11. Enter the name of the machine which is hosting the Online Responder service. In this case, the machine name is **OCSPSERV.**
12. Click **OK**. The system should not be able to locate the machine, instead another dialog displays.
13. Click **Object Types.** Select the **Computers** check box. Click **OK**.
14. Re-enter **OCSPSERV** in the **Select User, Computers, Service Accounts, or Groups** dialog. Click **OK**. The machine hosting the Online Responder will be added to the Group and user names area under the **Security** tab.
15. Click on **OCSPSERV** in the Group and user names area.
16. Select the **Read**, **Enroll**, and **Autoenroll** check boxes.
17. Ensure that the **Read**, **Write**, **Enroll**, and **Autoenroll** check boxes are selected for both **Domain Admins** and **Enterprise Admins**. Click **Apply**.
18. Select the **Cryptography tab**. Select the **Requests must use one of the following providers** radio button. The dialog below the radio button activates.
19. Select **SafeNet Key Storage Provider**.
20. Click **Apply** and then **OK**.

Configure certificate templates using SafeNet CSP

To generate OCSP signing keys using the SafeNet CSP:

> **NOTE:** Ensure that you have registered the CSP on both the OCSPCA and OCSPSERV systems.

1. Log on to **OCSPCA** as a domain administrator.
2. Click the **Search** menu, type **MMC** and press **Enter** to open the console.
3. In the **mmc** console, select **File** and click **Add/Remove Snap-in…**
4. In the **Add or Remove Snap-Ins dialog box**, select the **Certificate Templates** snap-in (under the Available snap-ins section).
5. Click **Add**, and then click **OK**.
6. Under Console Root, expand the **Certificate Templates** snap-in. The middle section lists all of the available certificate templates that your CA can issue.
7. Scroll down the list until you locate the **OCSP Response Signing template**. Right-click the **OCSP Response Signing Template** and click **Duplicate Template.**
8. In the pop-up dialog box, click the **Compatibility tab**.
9. In Compatibility Settings, under **Certificate Authority** select **Windows Server 2003.** The Resulting Changes window displays. Click **OK**.
10. Under Certificate recipient, select **Windows XP / Server 2003.** The Resulting Changes window displays**.** Click **OK**.
11. Click the **General** tab. Enter the **name of template** in Template display name.
12. Select the **Publish Certificate in the Active Directory** check box.

13. Set the **Validity period** and **Renewal period**.

> **NOTE: For testing purpose, this guide assumes the Validity period and Renewal period for four hours and one hour for Auto Renewal.**

14. Click the **Security** tab and select **Add**. The **Select User, Computers, Service Accounts, or Groups** dialog displays. Enter the name of the machine (**OCSPSERV)** which is hosting the Online Responder service.
15. Click **OK**. The system should not be able to locate the machine, instead another dialog displays.
16. Click **Object Types.** Select the **Computers** check box. Click **OK**.
17. Re-enter **OCSPSERV** in the **Select User, Computers, Service Accounts or Groups dialog**. Click **OK**. The machine hosting the Online Responder will be added to the Group and user names area under the **Security** tab.
18. Click **OCSPSERV** in the Group and user names area.
19. Select the **Read**, **Enroll**, and **Autoenroll** check boxes.
20. Ensure that the **Read**, **Write**, **Enroll**, and **Autoenroll** check boxes are selected for both **Domain Admins** and **Enterprise Admins**. Click **Apply**.
21. Select the **Cryptography** tab. Select the **Requests must use one of the following providers** radio button. The dialog below the radio button activates.
22. Select **Luna Cryptographic Services for Microsoft Windows**.
23. Click **Apply** and then **OK**.

To configure the CA to support the Online Responder service

1. Log on to **OCSPCA** as a domain administrator.
2. From the **Start** menu, select **Administrative Tools** and click **Certification Authority**.
3. In the console tree (left-hand section), click the **CA** name.
4. Open the **Action menu** and click **Properties**.
5. Click the **Security tab** and select **Add**. The **Select User, Computers, Service Accounts, or Groups** dialog displays.
6. Enter the name of the machine which is hosting the Online Responder service. In this case, the machine name is **OCSPSERV**.
7. Click **OK**. The system should not be able to locate the machine, instead another dialog displays.
8. Click **Object Types**. Select the **Computers** checkbox. Click **OK**.
9. Re-enter **OCSPSERV** in the **Select User, Computers, Service Accounts or Groups** dialog. Click **OK**. The machine hosting the Online Responder will be added to the Group and user names area under the **Security tab**.
10. Click **OCSPSERV** in the Group and user names area.
11. In the **Permissions area**, select the **Request Certificate** check box.
12. Ensure that the **Issue and Manage Certificates**, **Manage CA**, and **Request Certificates** check boxes are selected for **Domain Admins**, **Enterprise Admins**, and **Administrators**.
13. Select the **Extensions tab**. In the **Select extension** list, click **Authority Information Access (AIA).**

14. Click **Add.** In the **Add Location** dialog type under Location.

    `http://<computer_name_hosting_OCSP>/ocsp.`

    For example, the address when using **OCSPSERV** would be `http://OCSPSERV/ocsp.`
15. Click **OK**.
16. On the **Extensions tab**
    a. Ensure that the recently added URL is highlighted.
    b. Ensure that the **Include in the AIA extension of issued certificates** and **Include in the online certificate status protocol (OCSP) extension** check boxes are selected.
17. Click **Apply.** Click **Yes** to restart the Active Directory Certificate Services.
18. When the services restarts, click **OK**.
19. In the console tree of the Certification Authority snap-in, right-click **Certificate Templates**, and then click **New Certificate Templates to Issue**.
20. In **Enable Certificates Templates**, select the **OCSP Response Signing template** and any other previously configured certificate templates. Click **OK**.
21. Open Certificate Templates in the Certification Authority and verify that the modified certificate templates are included in the list.

Create a revocation configuration

A revocation configuration includes all of the settings that are needed to respond to status requests regarding certificates that have been issued by using a specific CA key. Creating a revocation configuration involves the following:

> Modify online responder service to use Luna HSMs

> Set up revocation configuration

Modify online responder service to use Luna HSMs

To use OCSP in conjunction with Luna HSMs or Luna Cloud HSM services, configure the Online Responder service to use the HSM to protect the OCSP signing keys. To modify the Online Responder service to use Luna HSMs:

1. Log on to **OCSPSERV** as a domain administrator.
2. From the **Start menu** select **Administrative Tools** and then click **Services.**
3. Locate the **Online Responder Service** in the list of services.
4. **Right-click** on the **Online Responder Service** and select **Properties**.
5. In the dialog box select the **Log on** tab.
6. Under **Log on as**, select the **Local System Account** radio button and then select the **Allow services to interact with desktop** check box.
7. Click **Apply** and then **OK**.
8. Return to the services window. Right-click the **Online Responder Service** and click **Restart.** Wait to start the service again. Close the service window.

Set up revocation configuration

Once the Online responder Service is configured to use the HSM to protect the OCSP singing keys, set up the certificate revocation configuration. To set up the revocation configuration:

1. Log on to **OCSPSERV** as a domain administrator.
2. From the **Start** menu, select **Administrative Tools** and then click **Online Responder Management**.
3. In the left-hand pane select **Revocation Configuration**.
4. In the right-hand pane, under Actions, click **Add Revocation Configuration**. A dialog window displays.
5. On the **Getting started with adding a revocation configuration section** click **Next.**
6. In the **Name the Revocation Configuration** section, enter a name for the configuration in the text box (For Example: Test). Click **Next**.
7. In the **Select CA Certificate Location** window, ensure that the **Select a certificate for an Existing enterprise CA** radio button is selected and click **Next**.
8. In the **Choose CA Certificate** section, ensure that the **Browse CA certificates published in Active Directory** radio button is selected and then click **Browse**.
9. In the Select **Certification Authority** dialog box, select the **CA authority** (in this case **OCSPCA**) and click **OK**. Click **Next**.
10. In the **Select Signing Certificate** window, accept the default setting **Automatically select a signing certificate** and select the **Auto-enroll for OCSP signing certificate** check box. Click **Next**.
11. In the **Revocation Provider** window, click **Finish**.

    Once the wizard completes, the Revocation Configuration **Status Box** displays the Online Responder status. The status should display **Bad Signing on Array Controller**.
12. To correct this, click on **Revocation Configuration** in the left hand pane. The certificate displays in the right-pane.
13. Right-click on the certificate and select **Edit Properties**.
14. Click the **Signing** tab. Deselect the **Do not prompt for credentials for cryptographic operations** check box. Click **OK**.
15. Return to the **Online Responder Management** tool. Open **Actions** and click **Refresh**.
16. In the left-hand pane click **Online Responder: Computer Name** and verify that the Revocation Configuration **Status Box** displays **Working**.

Verify auto-enrollment

Verification of auto renewal involves the expiration of the generated certificate and renewal of the certificate using a new key pair. Verify that auto-enrollment of a newly generated certificate is operating successfully by completing the following procedures:

> View a generated certificate and key pair

> View a renewed certificate and key pair

View a generated certificate and key pair

1. Log on to **OCSPSERV** as a domain administrator.
2. Click **Search**, type **MMC** and press **Enter** to open the console.
3. In the **mmc** console, select **File** and click **Add/Remove Snap-in…**
4. In the **Add or Remove Snap-Ins** dialog box, find the **Certificate snap-in** (under the Available snap-ins section) and select it.
5. Click **Add**, select **Service Account** and click **Next**.
6. Select **Local Computer**, and click **Next.**
7. Under **Certificate Snap-in**, click on the **Online Responder Services** in Service Account and click **Finish**.
8. Click **OK** and expand the **Online Responder Services** tree.
9. Expand the **OCSPSvc\CertificateName** (for example "OCSPSvc_test_") and double-click on **Certificates**.
10. A certificate displays, double-click the certificate to view the properties of the certificate.
11. Click the **Details** tab and verify the **Valid From** and **Valid To** date of the certificate. It will state that the certificate expires in the next four hours.
12. Luna HSM partition shows the key pair for CA certificate and Online Responder Service certificate. Wait for four hours to verify the auto-renewal of the certificate because the validity period of the certificate is four hours.

View a renewed certificate and key pair

After four hours have passed, you can verify that the **Valid From** and **Valid To** dates of the certificate have been updated. The new certificate is valid for the next four hours, and a new key pair on Luna HSM partition for the renewed certificate has been generated.

This demonstrates that the certificate renews automatically every four hours.

> **NOTE:** It was set for four hours for testing purposes only, but in a production environment, it is recommend to set the validity periods as required by your organization's security infrastructure.

Validate OCSP integration

To validate that OCSP is operating properly following the integration with Luna HSM or Luna Cloud HSM service, perform following steps:

- Generate a certificate request
- Test the certificate’s origin
- Verify the OCSP integration

Generate a certificate request

1. Log on to the **OCSPCL** machine and generate a certificate request.

   > **NOTE:** We recommend using the below template structure. (Try to use different vendors’ cryptographic service providers.)

   ```
   [Version]
   Signature = "$Windows NT$"
   [NewRequest]
   Subject = "C=IN,CN=OCSPCL"
   HashAlgorithm = SHA256
   KeyAlgorithm = RSA
   KeyLength = 2048
   ProviderName = "<Provider_to_be_used>"
   KeyUsage = 0xf0
   MachineKeySet = True
   RequestType = PKCS10
   [EnhancedKeyUsageExtension]
   OID = 1.3.6.1.5.5.7.3.1
   [Extensions]
   1.3.6.1.5.5.7.48.1.5 = Empty
   ```

2. Save the above template as test.inf file. Ensure that the Provider Name variable is provided with the quotation marks around it.
3. Open the command prompt window and execute the following command:

   ```
   certreq -new test.inf test.req
   ```

   A certificate request called `test.req` will be generated.
4. Execute the following command in command prompt:

   ```
   certreq -submit -attrib “CertificateTemplate:WebServer” test.req
   ```

   A pop up window displays confirming which CA to use. Select the **OCSPCA** entry and click **OK**.
5. A dialog displays to save the certificate to a file.
6. Save the certificate file and click OK. After a short pause, a message “Certificate Successfully Generated” displays on the command prompt and a certificate file is generated.

Test the certificate’s origin

1. Log on to **OCSPCA** and go to the Certification Authority tool by navigating to **Start** -> **Administrative Tools** -> **Certification Authority.**

2. In the **Certification Authority snap-in**, publish a new CRL by clicking **Certification Authority (Computer)/CA name/Revoked Certificates** in the console tree. Then, right-click on the **Revoked Certificates** folder, point to **All Tasks**, and click **Publish**.
3. Select **New CRL** and click **OK**.
4. Open the **Certification Authority snap-in** and right-click on the CA. Click **Properties**.
5. On the **Extensions tab,** verify that the extension is set to CRL Distribution Point (CDP) in the drop-down menu**.** Select any listed **CRL distribution points,** click **Remove,** and click **OK.**
6. Click **Apply**. A dialog displays stating that you need to restart the service.
7. Click **OK** and wait for the service restart.
8. Verify that clients can still obtain revocation data. Execute the following on **OCSPCL**:

   ```
   certutil -url test.cer
   ```

9. The URL Retrieval Tool dialog displays. Select the **CRLs (From CDP)** radio button and click **Retrieve**.
10. Select the **OCSP (From AIA)** radio button and click **Retrieve**. The list should contain an OCSP entry showing the web address of the OCSP server. If it is working correctly, the word **Verified** displays in the first column in the list.
11. Select the **Certs (from AIA)** radio button and click **Retrieve**. One or two entries should be listed, with **Verified** next to them.

> **NOTE:** If Certificate Authority Web Enrollment is not installed on the CA, an entry with AIA may display as Failed. However, as long as one of the entries in the Certs (from AIA) section reads Verified there should be no problems with the set-up.

Verify the OCSP integration

1. Open a command prompt and execute:

   ```
   certutil –verify test.cer > test.txt
   ```

2. When the above command has been completed, open the test.txt file. The file should contain the information like this:

   ```
   Issuer:
       CN=Integration-OCSPSERV-CA
       DC=Integration
       DC=com
   Subject:
       CN=OCSPCL
       C=IN
   Cert Serial Number: 611362e4000000000003

   dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x20000000)
   dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000)
   ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000)
   HCCE_LOCAL_MACHINE
   CERT_CHAIN_POLICY_BASE
   -------- CERT_CHAIN_CONTEXT --------
   ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
   ChainContext.dwRevocationFreshnessTime: 17 Minutes, 42 Seconds

   SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
   ```

```
SimpleChain.dwRevocationFreshnessTime: 17 Minutes, 42 Seconds

CertContext[0][0]: dwInfoStatus=102 dwErrorStatus=0
  Issuer: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
  NotBefore: 5/23/2013 3:55 PM
  NotAfter: 5/23/2015 3:55 PM
  Subject: CN=OCSPCL, C=IN
  Serial: 611362e4000000000003
  Template: WebServer
  f0 e3 6b 9f f4 59 a6 64 18 f4 6f f6 a1 90 52 5b a3 3a 40 8c
  Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2)
  Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
    CRL 02:
    Issuer: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
    c1 32 12 a5 2f 82 d9 69 06 c0 28 1c 75 9d b1 5b 4c c5 4f 6d
    Delta CRL 02:
    Issuer: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
    b1 63 03 a3 b8 d0 c5 41 7c d9 2c 3f ae 87 b4 a3 27 bd e7 73
  Application[0] = 1.3.6.1.5.5.7.3.1 Server Authentication

CertContext[0][1]: dwInfoStatus=10c dwErrorStatus=0
  Issuer: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
  NotBefore: 5/23/2013 3:30 PM
  NotAfter: 5/23/2018 3:40 PM
  Subject: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
  Serial: 6236c444f91af2a04fafdd311517307a
  c3 3b 1c 6a 7f 07 3d f9 63 2a d1 fd 62 ca eb 16 e5 04 0a d3
  Element.dwInfoStatus = CERT_TRUST_HAS_NAME_MATCH_ISSUER (0x4)
  Element.dwInfoStatus = CERT_TRUST_IS_SELF_SIGNED (0x8)
  Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)

Exclude leaf cert:
  e9 a1 9d 87 ea 5f 8b 9f b1 cc 2d d5 3a 55 f2 d1 12 14 b8 a2
Full chain:
  e5 79 bc 47 e8 b8 05 11 fa e4 0d 47 a8 3e 73 99 3d df cf 4f
------------------------------------
Verified Issuance Policies: None
Verified Application Policies:
    1.3.6.1.5.5.7.3.1 Server Authentication
Leaf certificate revocation check passed
         CertUtil: -verify command completed successfully.
```

3. Ensure that the above output includes the following:

   ```
   Verified Issuance Policies: None
   Verified Application Policies:
   1.3.6.1.5.5.7.3.1 Server Authentication
   Leaf certificate revocation check passed
   CertUtil: -verify command completed successfully.
   ```

   These commands demonstrate that the OCSP server is operating correctly without any errors. The most important component of the above example is the **Leaf certificate revocation check passed** line as this demonstrates that the OCSP service is returning the certificate status as **Good**.

If the log generated by the verify command does not include the above section (or similar) and has errors in the output, we recommend you restart the OCSP server and client machine, and run the **verify** command again on the certificate file.

Troubleshooting

Bad signing certificate on array controller

Problem: Online Responder reports “Bad Signing Certificate on Array Controller”.

Reason: This error displays when the CA certificate cannot be located by the Online Responder client.

Solution: Ensure that the points mentioned in the Create Revocation Configuration have been correctly carried out. Verify that the CA is correctly configured and that a valid CA certificate Exists for OCSP Signing.

‘Failed’ next to AIA entry in URL Retrieval tool

Problem: Using certutil –url <certnamehere.cer> and selecting Certs (from AIA) shows an entry in the list called AIA with “Failed” next to it.

Reason: This error displays when Certificate Authority Web Enrollment is not installed on the CA.

Solution: Install Certificate Authority Web Enrollment on the CA machine.

> **NOTE:** AIA failing does not adversely impact the OCSP setup. As long as both items in the Certs (from AIA) do not fail, there should not be a problem with the setup.

Unrecognized/Untrusted Certificate Authority

Problem: When viewing a newly generated certificate from the CA it is reported as untrusted.

Reason: This error displays when the CA has not been added to the **Trusted Root Certification Authorities** certificate store.

Solution: Double-click the newly generated certificate. Under the **General** tab, click I**nstall Certificate…** On the first screen that is displayed click **Next**, select the radio button next to **Place all certificates in the following store** and click **Browse**. In the **Select Certificate Store** window that is displayed click **Trusted Root Certification Authorities** and click **OK**. When the window disappears click **Next** and on the next window click **Finish**.

‘Invalid Provider Specified’ error when using ‘certreq –new’ command

Problem: Using the certreq –new <.req file here> command throws an **Invalid Provider Specified error**.

Reason: This error displays when the CSPs are not installed and set up on the client machine not set up correctly.

Solution: Ensure that the SafeNet Luna CSP or CNG providers are correctly installed and set up. (To overcome this issue, execute the CSP Install Wizard and CNG Configuration Wizard under the Luna HSM Installation folder) or you can use Microsoft Cryptographic Service Provider or any other service provider that is registered on the client machine.

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.