Microsoft Internet Information Services: Integration Guide

THALES LUNA HSM AND DPOD LUNA CLOUD HSM

Document Information

Document Part Number	007-011955-001
Revision	P
Release Date	30 December 2020

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Overview....................4
Certified Platforms....................4
Prerequisites....................5
Configure Luna HSM....................5
Configure Luna Cloud HSM Service....................6
Integrating Luna HSM with Microsoft Internet Information Services....................9
Configure the SafeNet Key Storage Provider (KSP)....................9
Create a Certificate Request using Microsoft IIS....................12
Contacting Customer Support....................14
Customer Support Portal....................14
Telephone Support....................14
Email Support....................14

Overview

This document is intended to guide security administrators through the steps for integrating Microsoft Internet Information Services (IIS) with Thales Luna HSM devices or DPoD Luna Cloud HSM services. We recommend that you familiarize yourself with the *Microsoft IIS Documentation* for more information on installation and setup procedures. The benefits of integrating Microsoft IIS with Luna HSM devices or Luna Cloud HSM services include:

> Secure generation, storage and protection of the signing private key on FIPS 140-2 level 3 validated hardware.

> Full life cycle management of the keys.

> Access to the HSM audit trail*.

> The advantage of cloud services with confidence.

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

Certified Platforms

This integration is certified on the following platforms:

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

NOTE: Microsoft IIS 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.

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

Luna Cloud HSM: Luna Cloud HSM services provide 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 specific services that you need.

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 the Luna HSM documentation for more information.
2. Create a partition that will be later used by MS IIS.
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 ->                IIS

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 the Luna HSM documentation for detailed steps on 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 the 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.

   ```
   [Windows]

   Right-click setenv.cmd and select Run as Administrator.

   [Linux]

   Source the setenv script.
   ```

```
# source ./setenv
```

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

Standalone Cloud HSM service using full Luna client package

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

1. Transfer the downloaded .zip file to your Client workstation using pscp, scp, or other secure means.
2. Extract 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/
```

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

10. 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/
```

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

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

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.

Integrating Luna HSM with Microsoft Internet Information Services

This section outlines the steps to integrate Microsoft IIS with Luna HSM. Microsoft IIS uses the SafeNet KSP (Key Storage Provider) for integration.

Configure the SafeNet Key Storage Provider (KSP)

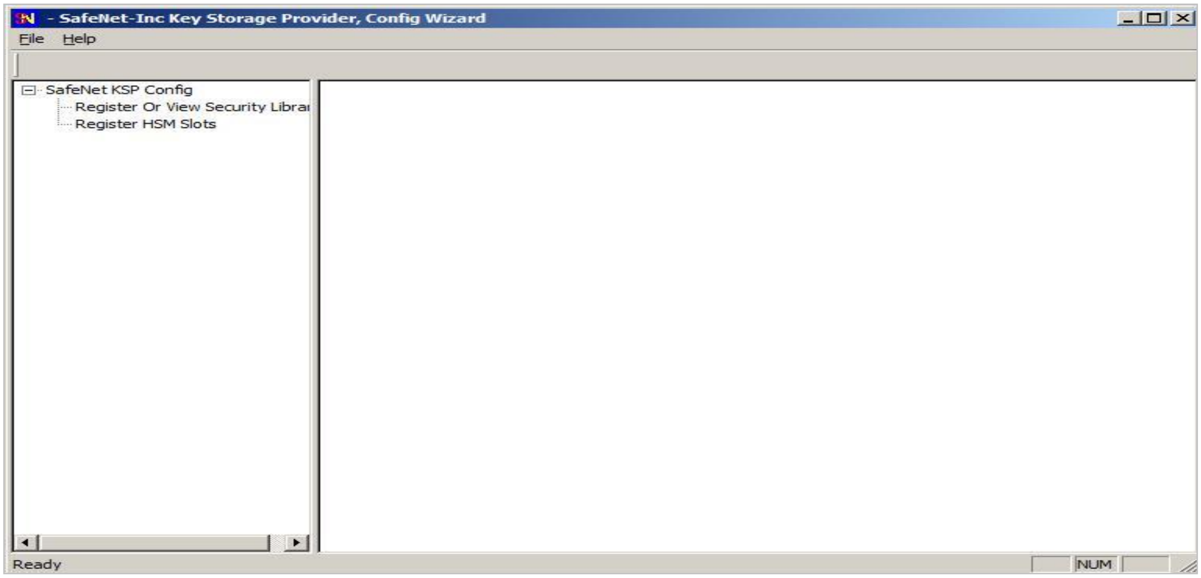
You must configure the SafeNet Key Storage Provider (KSP) to allow the user account and system to access the Luna HSM or Luna Cloud HSM service.

- If you are integrating a Luna HSM, the KSP package must be installed during the Luna Client software installation.
- If you are integrating Luna Cloud HSM service, the KSP package is included in the Cloud HSM service client package inside of the /KSP folder.

To configure the SafeNet Key Storage Provider

1. Navigate to the <Luna HSM Client installation Directory>/KSP directory. If you are using Luna Cloud HSM service, the /KSP folder is available in the service client package.

2. Double-click the KspConfig.exe file to launch the SafeNet KSP configuration wizard.

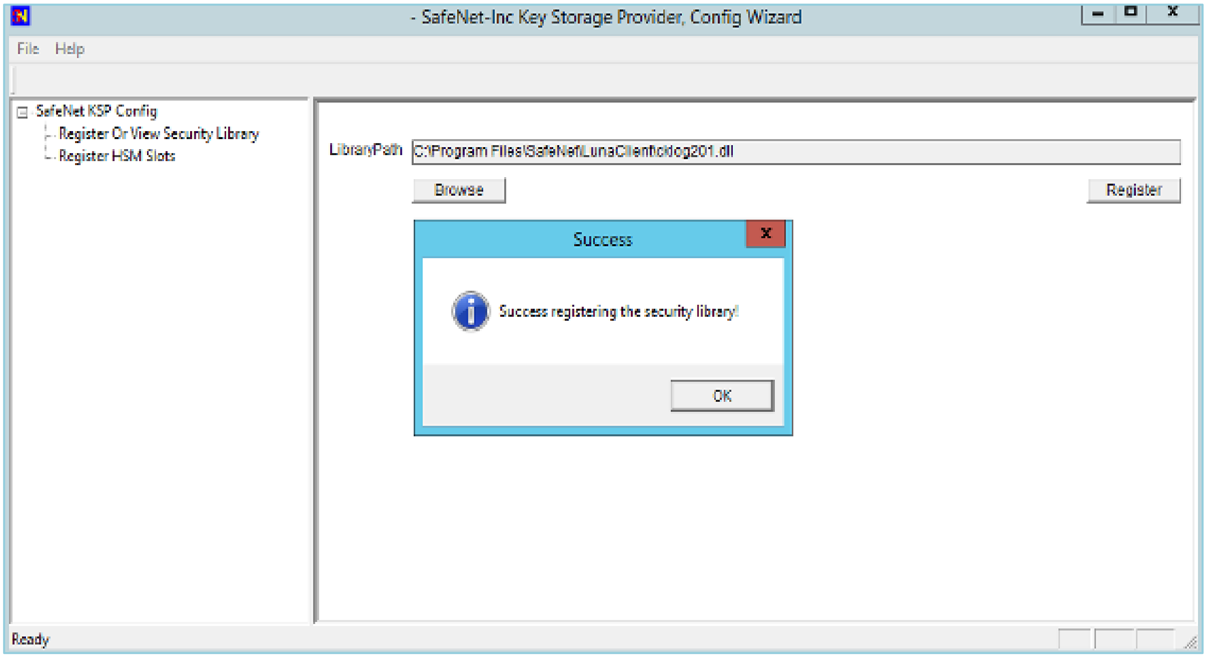

- SafeNet-Inc Key Storage Provider, Config Wizard
File
Help
SafeNet KSP Config
Register Or View Security Librar
Register HSM Slots
Ready
NUM

3. Double-click **Register or View Security Library** on the left side of the pane.

4. Click **Browse**, navigate to the Luna HSM Client installation directory and select the cryptographic library file named cryptoki.dll. Click **Register**. If you are using Luna Cloud HSM service, the cryptographic libraries are available in the service client package.

5. On successful registration, the following message will appear on screen:

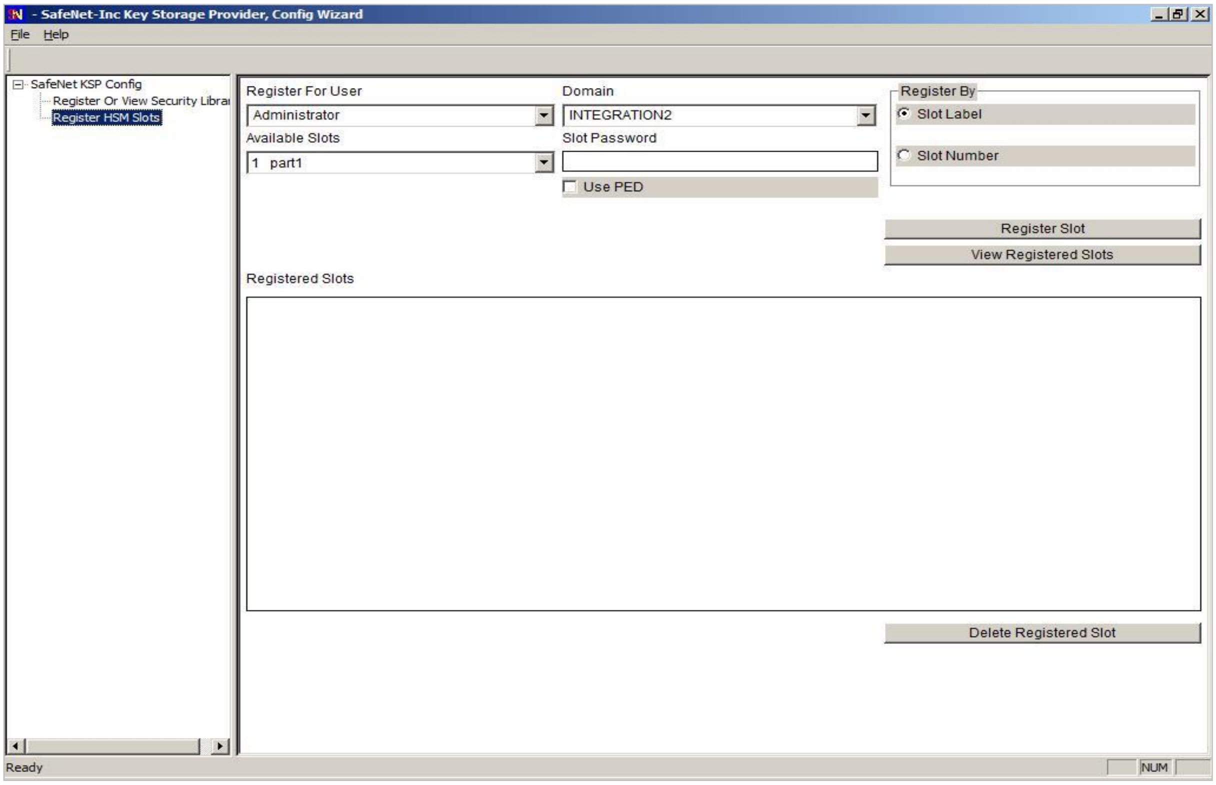
Success registering the security library!


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

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

Success registering the security library!

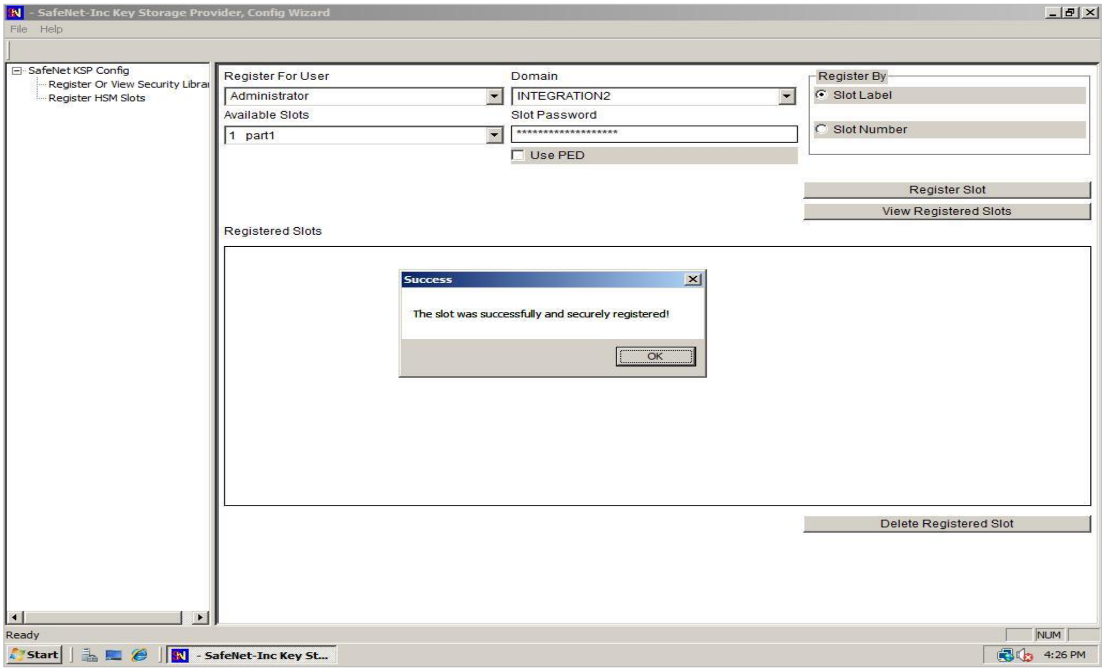
6. Double-click **Register HSM Slots** on the left side of the pane.



7. Enter the Slot (Partition) password.

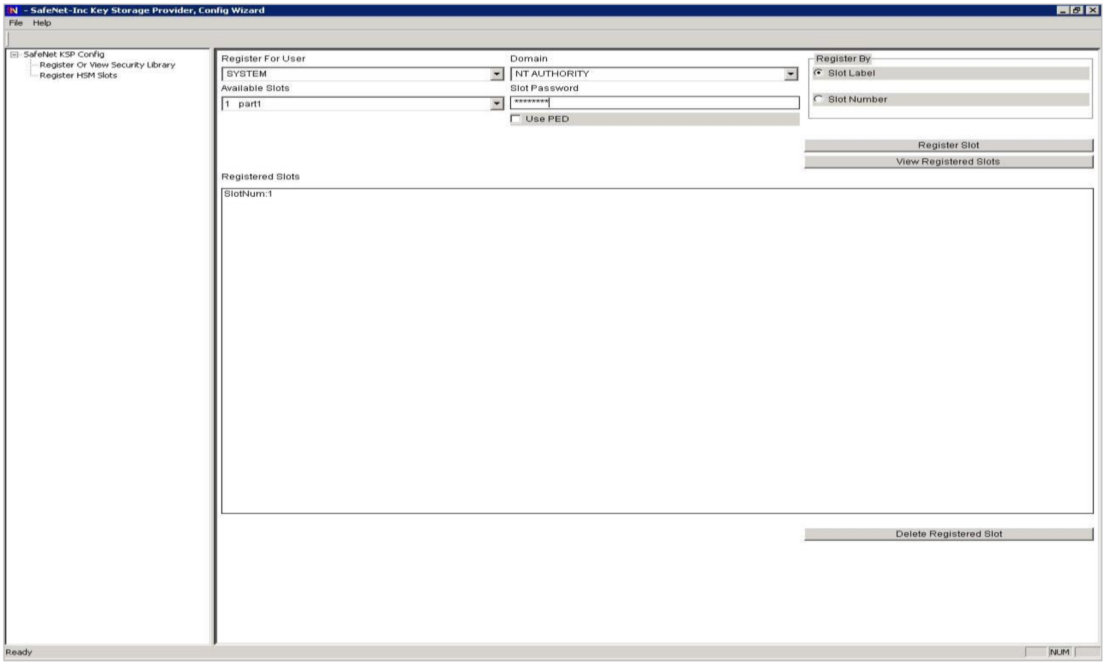
8. Click **Register Slot** to register the slot for Domain\User. On successful registration, the following message will appears on screen:

   The slot was successfully and securely registered!



The slot was successfully and securely registered!

9. Register the same slot for **NT_AUTHORITY\SYSTEM**.



Register For User: SYSTEM

Domain: NT AUTHORITY

Available Slots: 1 part1

Slot Password: ********

□ Use PED

Register By: ● Slot Label ○ Slot Number

Registered Slots: SlotNum:1

To install IIS

1. Open Server Manager. Click **Configure this local server**, select **Add roles and features**, and click **Web Server (IIS)**.
2. Select the Default (or desired) components from within the wizard and complete the Microsoft IIS installation.

Create a Certificate Request using Microsoft IIS

You can generate a certificate request linked to an encryption key using the Microsoft IIS.

> **NOTE:** IIS Manager does not support the creation of certificates protected by CNG keys. To use a CNG key you must create the key using the Microsoft command line utility.

To generate a certificate request

1. Create a certificate request file named request.inf having the following information:
   - Subject details of the issuing certificate
   - Key algorithm and key length as required (e.g. RSA).
   - Provider name as "SafeNet Key Storage Provider".

   For example:

   ```
   [Version]
   Signature= "$Windows NT$"
   ```

```
[NewRequest]
Subject = "C=IN,CN=IIS.com,O=Thales,OU=HSM,L=Noida,S=UP"
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
ProviderName = "Safenet Key Storage Provider"
KeyUsage = 0xf0
MachineKeySet = True
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
```

2. Create the certificate signing request for the Certification Authority:

   ```
   certreq.exe -new request.inf request.req
   ```

   This creates a certificate request file called `request.req` that can be sent to a Certificate Authority.

To install the certificate

1. Submit the CSR file to a CA such as VeriSign or Entrust. Request the CA authenticates the certificate and returns a signed certificate and certificate chain. Save the reply in the current working directory.
2. Make the certificate available for use in Microsoft IIS.

   ```
   certreq.exe -accept signed.cer
   ```

   Where `signed.cer` is the binary signed certificate received from the CA.

To bind the certificate with a secure IIS web server

1. Open the IIS Manager from **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Under Sites on the left hand side of the IIS Manager Window, select the desired web site.
3. On the right side of the IIS Manager, click **Bindings**.
4. In the Site Bindings window, click **Add**.
5. Select the **https** protocol.
6. Select the IP address of the machine running IIS from the IP Address drop-down list.
7. Select the certificate from the drop-down list.
8. Click **OK** to complete the certificate binding for SSL connection.
9. Open a browser and enter https://<machine_name>:443.

This completes the integration of Microsoft IIS with Luna HSM or DPoD Luna Cloud HSM service.

Contacting Customer Support

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, 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.