DigiCert® PKI Platform

HSM Installation and Configuration for SafeNetAT (Assured Technologies)

Version 8.21.3

June 10, 2021

digicert®

Legal Notice

DigiCert, Inc.
2801 North Thanksgiving Way, Suite 500
Lehi, UT 84043
https://www.digicert.com/

Table of Contents

INTRODUCTION 4

REVISION HISTORY 4

SUPPORTED HSMS 5

SAFENETAT NETWORK HSM 6

INSTALLING THE SAFENETAT LUNA CLIENT SOFTWARE 7

CONFIGURE LUNA HSM CLIENT 12
CONFIGURE HA (HIGH AVAILABILITY) 14
CONFIGURE CSP 15
CONFIGURE KSP 18
GENERATE CSR AND INSTALL CERTIFICATE 21

INTEGRATION FOR JAVA ENVIRONMENT 22

REGISTER LUNA PROVIDER 22
INSTALL RA CERTIFICATE 23

GET RA CERTIFICATE IN PKI-MANAGER 23

Introduction

This document describes the installation and configuration steps for SafeNetAT Network HSM to be used by the DigiCert PKI Enterprise Gateway and Autoenrollment server.

Revision History

No.	Date	Summary
1.	2020/11/04	Create a new entry
2.	2021/06/10	Added support for SafeNetAT Luna SA5

Supported HSMs

HSM Type	Client Version	Software Version	Firmware Version
SafeNetAT Network HSM (*a, *b)	7.10.1	7.10.1	7.10.1
SafeNetAT Network HSM (*a, *b)	5.4.9	5.4.7	6.11.2

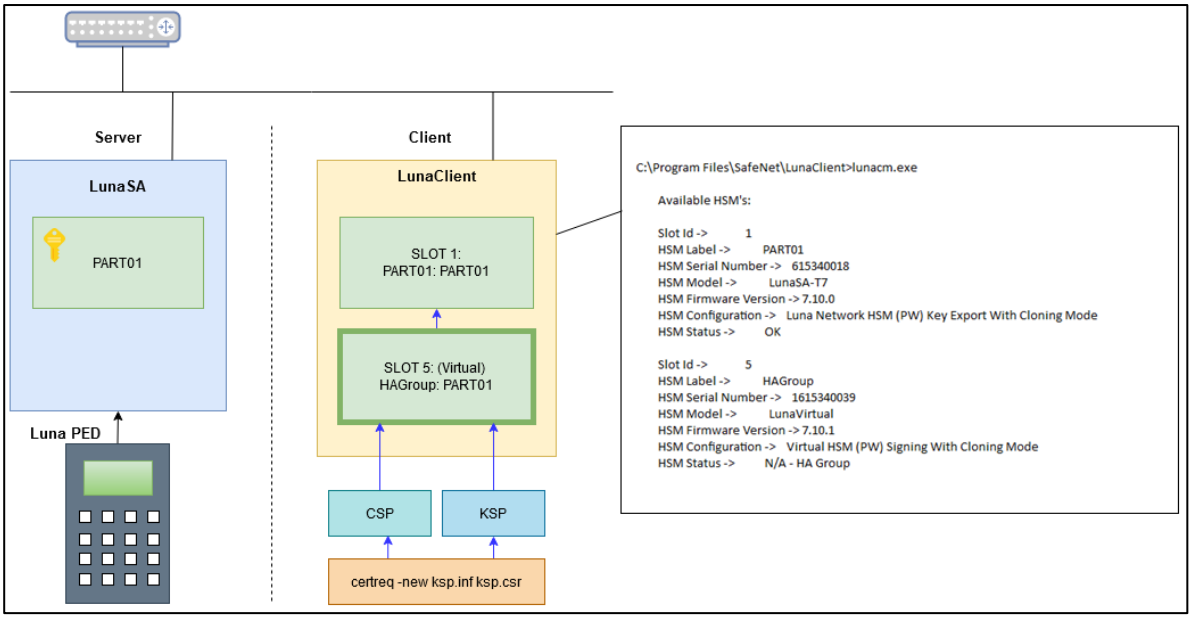
*a : Both Export and Signing variants were qualified with the supported HSM types.

*b : SafeNetAT Network HSM 5 and 7 supports FIPS and non-FIPS Mode, Cloning and Export Mode.

SafeNetAT Network HSM

The SafeNetAT Network HSM T-7 is network HSM which allows to create a partition to store a key, such as the RA key required to strongly authenticate to the DigiCert PKI Platform. It includes many features that increase security, connectivity, and ease-of-administration in dedicated and shared security applications.

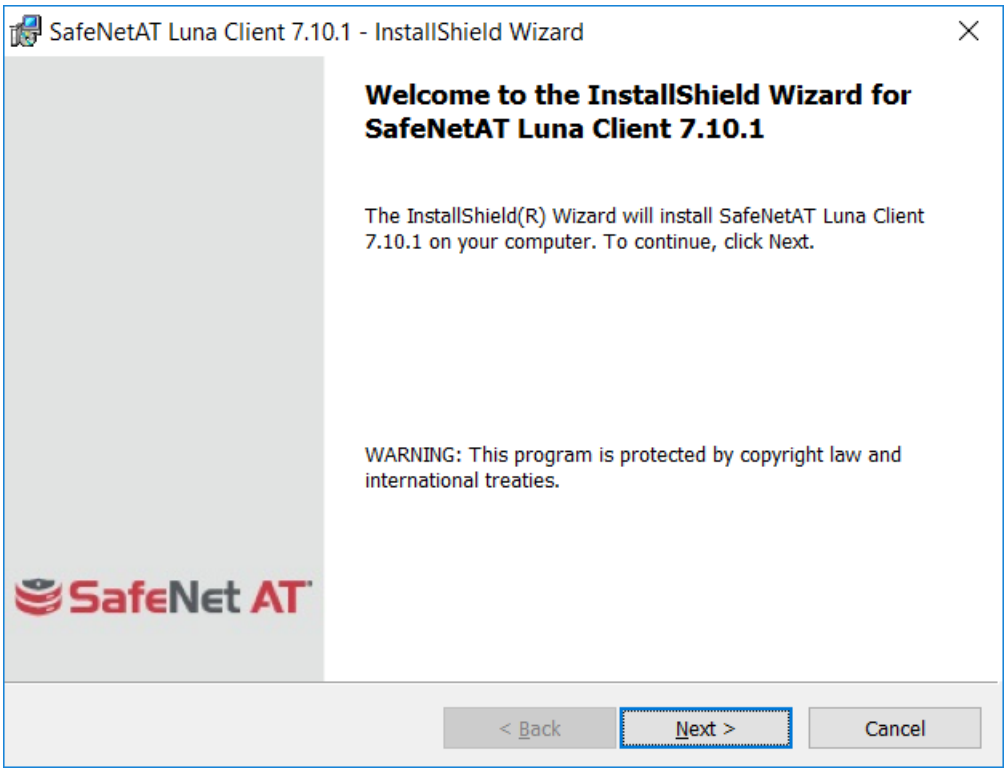
To access the partition of SafeNetAT Network HSM T-7, we can use the Luna HSM Client through Network Trust Link Service (NTLS).



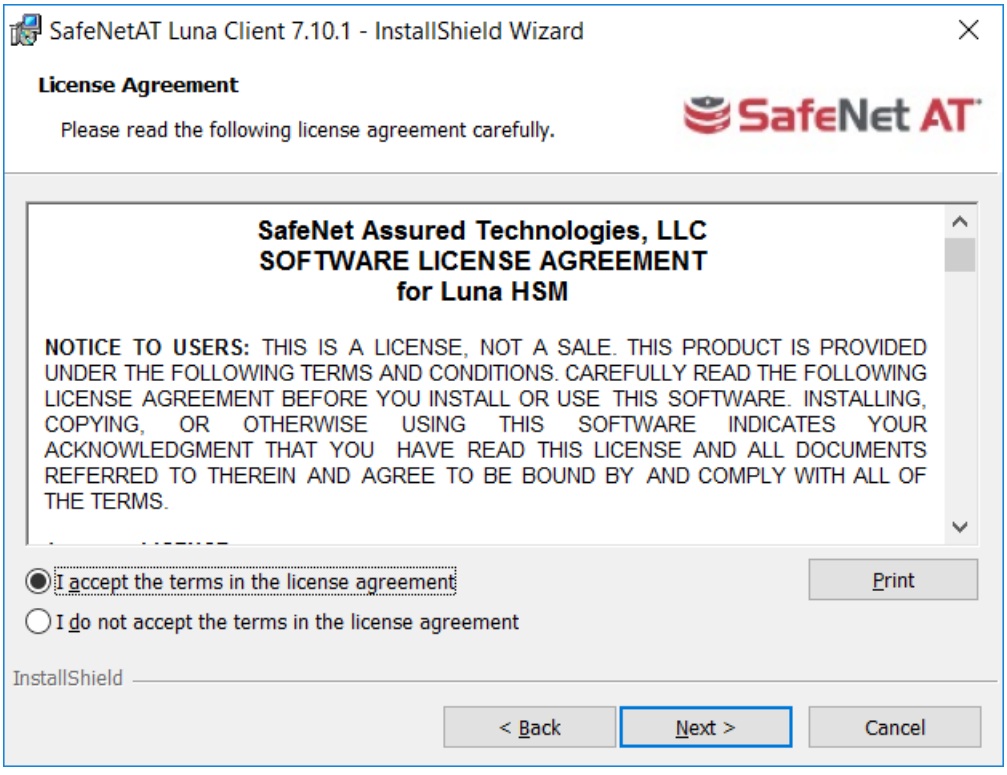
Installing the SafeNetAT Luna Client Software

In the client location, follow the steps below to install the Luna Client software.

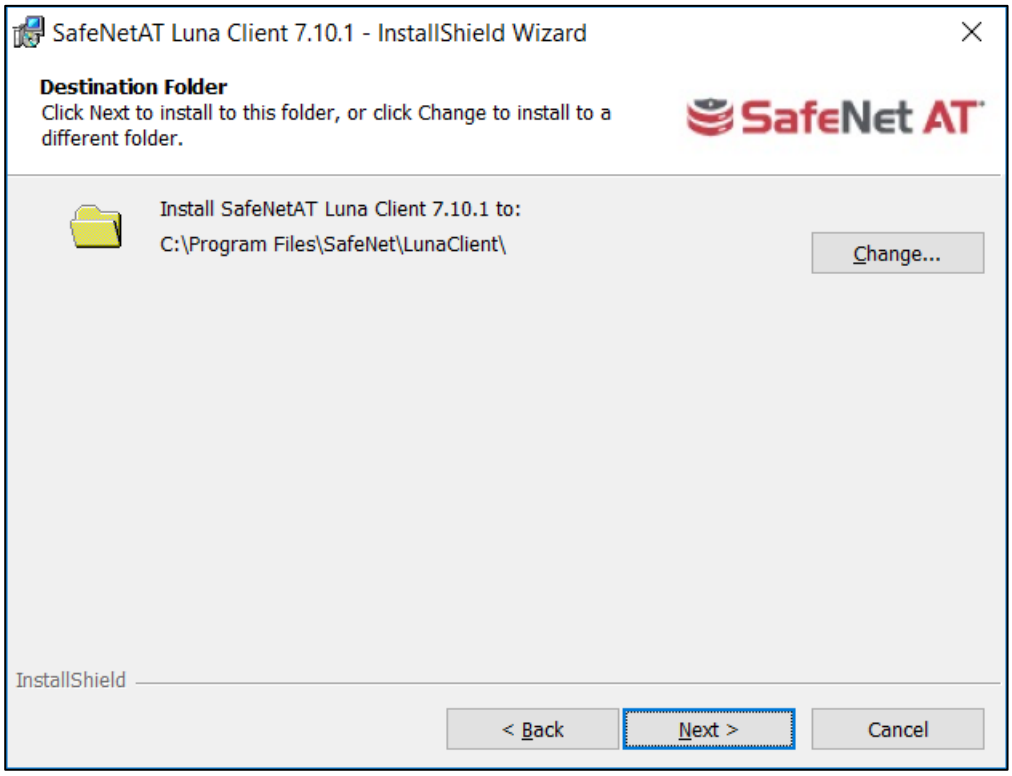
1. Run **LunaClient.msi** as Administrator and click **Next**.



2. Select "I accept the terms in the license agreement" and click **Next**.



3. Proceed and click **Next**.



4. Select the features to be Installed and click **Next**.

   Here select Luna SA -> This feature, and all subfeatures, will be installed on local hard drive.

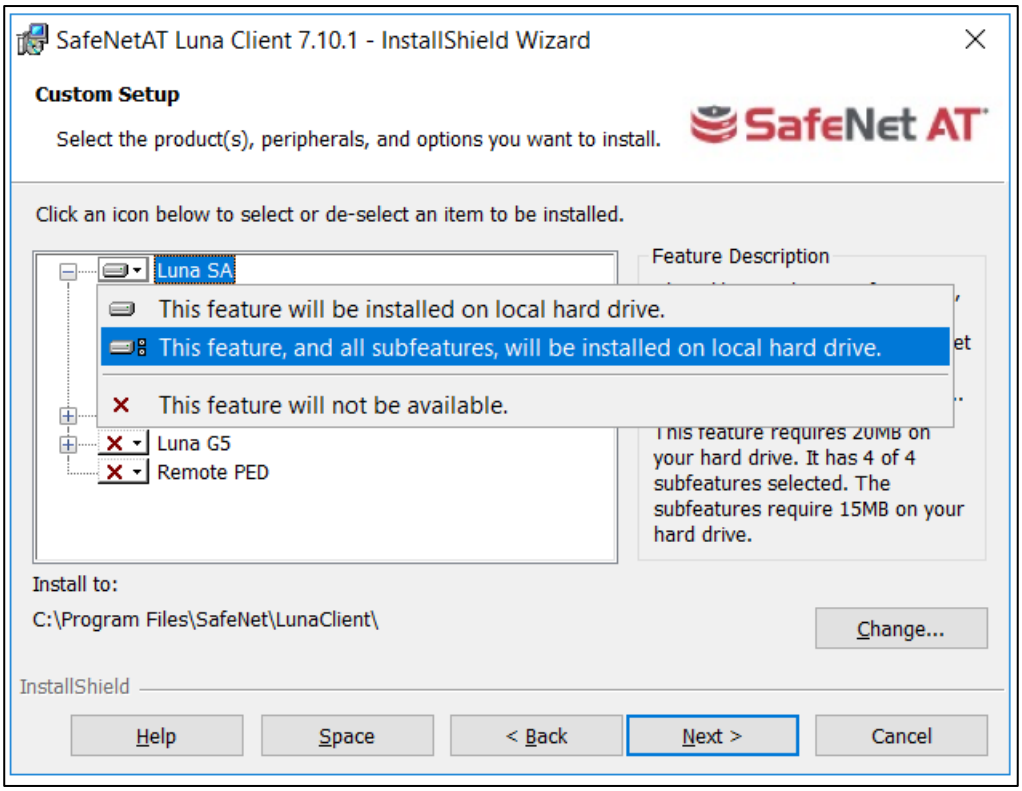
   Check the following **Features**. (Option: depends on your environment):

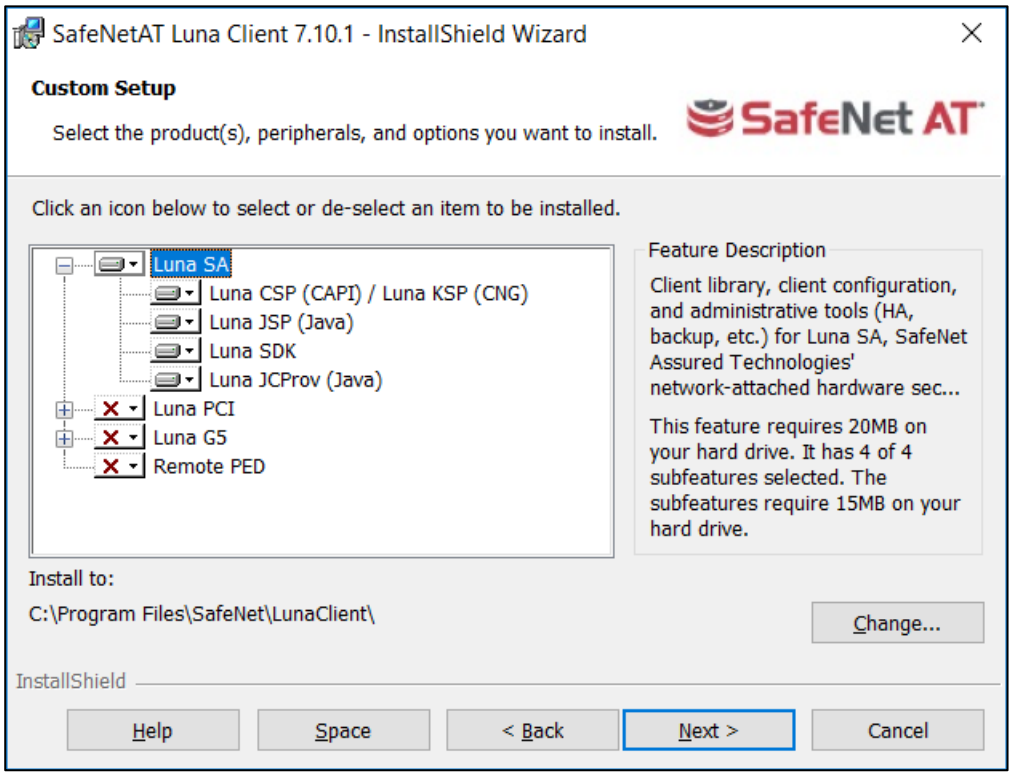
   a) Luna CSP (CAPI) / Luna KSP (CNG)

   b) Luna JSP (Java)

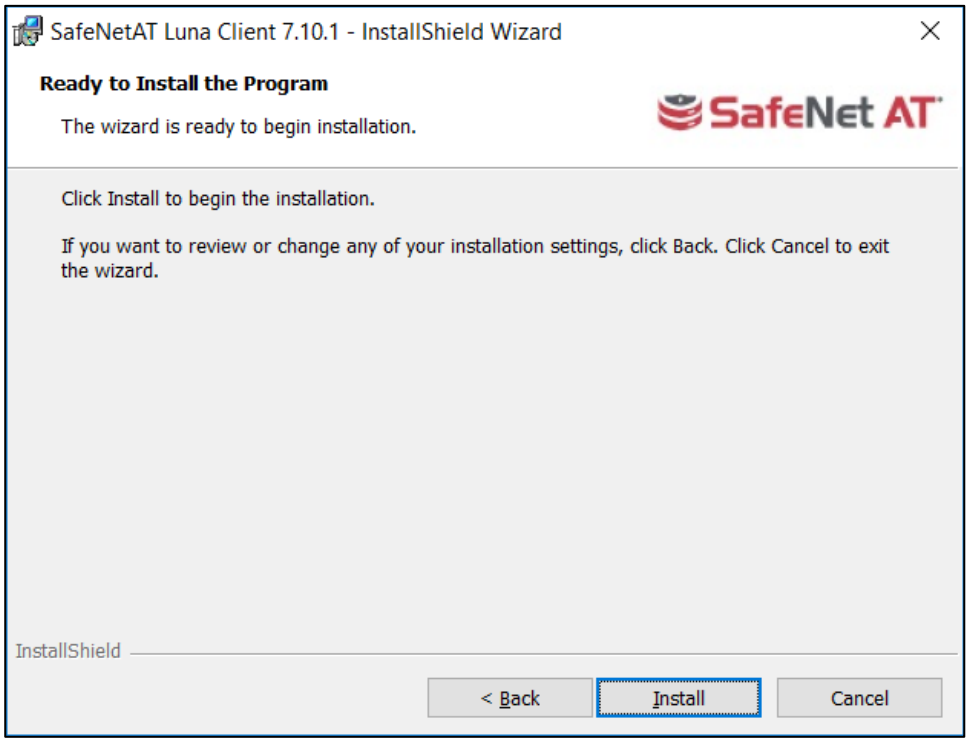
   c) Luna SDK

   d) Luna JCProv (Java)


SafeNetAT Luna Client 7.10.1 - InstallShield Wizard
Custom Setup
Select the product(s), peripherals, and options you want to install.
SafeNet AT
Click an icon below to select or de-select an item to be installed.
Luna SA
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.
Luna G5
Remote PED
Feature Description
This feature requires 20MB on your hard drive. It has 4 of 4 subfeatures selected. The subfeatures require 15MB on your hard drive.
Install to:
C:\Program Files\SafeNet\LunaClient\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

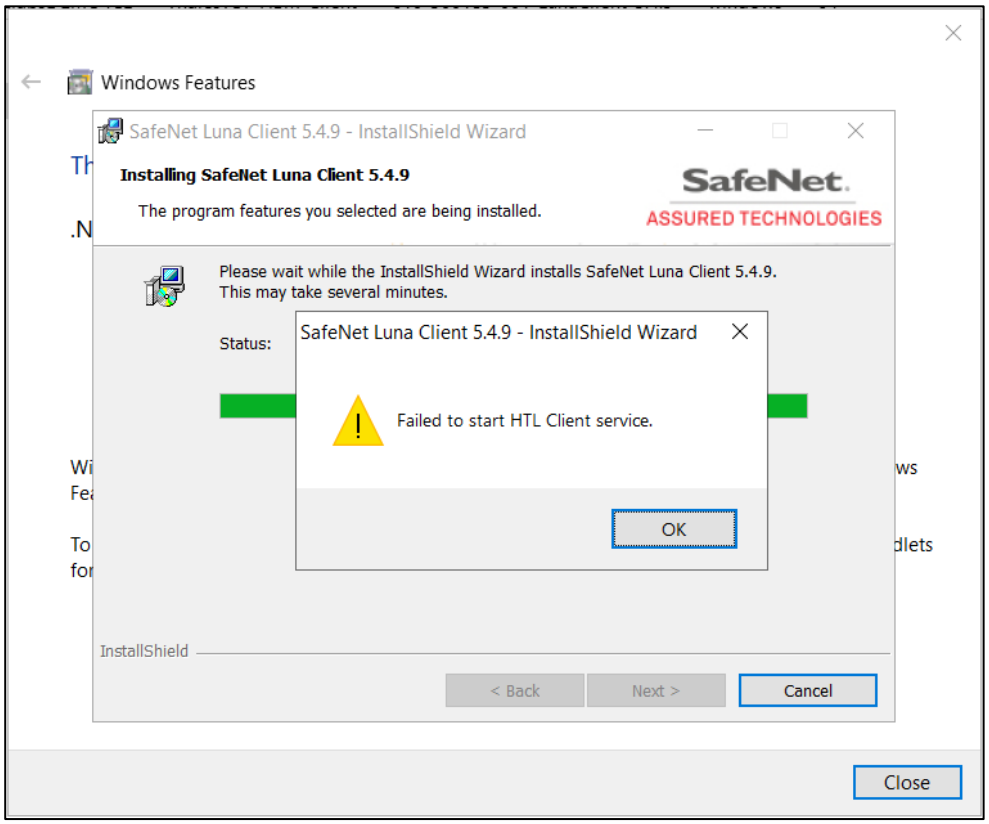

SafeNetAT Luna Client 7.10.1 - InstallShield Wizard
Custom Setup
Select the product(s), peripherals, and options you want to install.
SafeNet AT
Click an icon below to select or de-select an item to be installed.
Luna SA
Luna CSP (CAPI) / Luna KSP (CNG)
Luna JSP (Java)
Luna SDK
Luna JCProv (Java)
Luna PCI
Luna G5
Remote PED
Feature Description
Client library, client configuration, and administrative tools (HA, backup, etc.) for Luna SA, SafeNet Assured Technologies' network-attached hardware sec...
This feature requires 20MB on your hard drive. It has 4 of 4 subfeatures selected. The subfeatures require 15MB on your hard drive.
Install to:
C:\Program Files\SafeNet\LunaClient\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

5. Click **Install**.

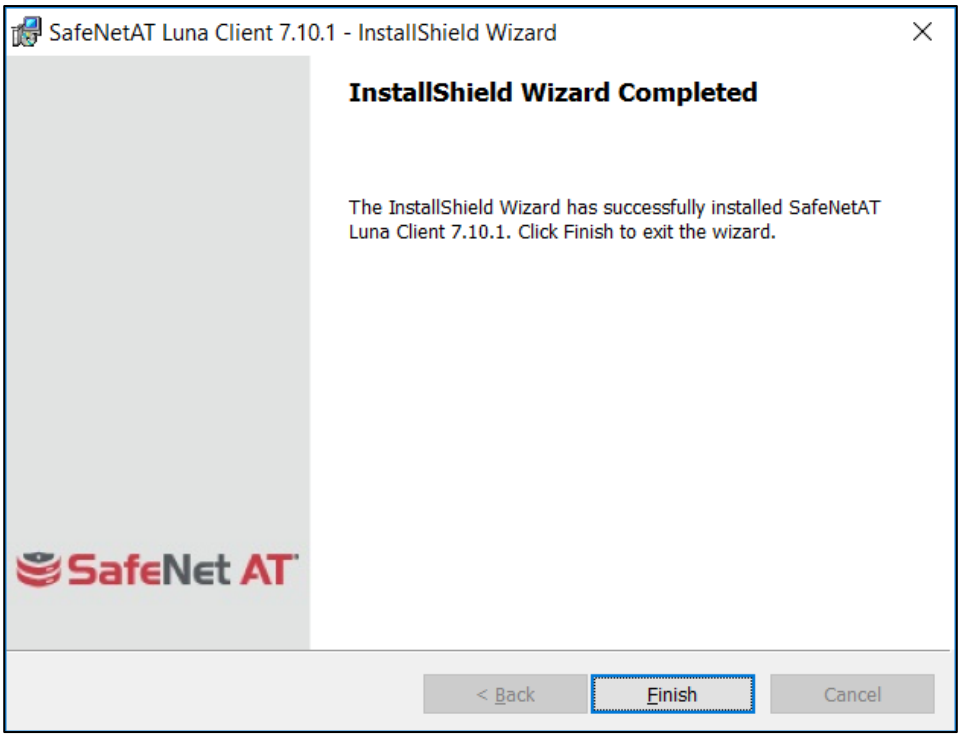


NOTE: If you see below error when installing Luna Client version 5.4.9 on Windows Server 2019, Ignore the error and proceed with installation and configuration.

Click OK and Click Finish and Close “Windows Features” window



6. Once the Installation is completed, click Finish.



NOTE: Both “Configure CSP” and “Configure KSP” must be configured again if you run the steps above.

Configure Luna HSM Client

Before following the steps, a partition must be created, named as <PARTITION-NAME> throughout the rest of this document.

In the client location, follow the below steps to configure the Luna HSM Client:

1. Open command prompt and run the following commands.

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

2. Obtain the server certificate.

   The server certificate has been created on the HSM. Copy it from the server.

```
> pscp -scp admin@<SERVER-HOSTNAME>:server.pem .
```

3. Add server for the client side.

```
> vtl addServer -n <SERVER-HOSTNAME> -c server.pem
New server <SERVER-HOSTNAME> successfully added to server list.
```

4. Create client certificate.

```
> vtl createCert -n <CLIENT-HOSTNAME>
```

```
Private Key created and written to: C:\Program
Files\SafeNet\LunaClient\cert\client\<CLIENT-HOSTNAME>Key.pem
Certificate created and written to: C:\Program
Files\SafeNet\LunaClient\cert\client\<CLIENT-HOSTNAME>.pem
```

5. Upload the client certificate to the server.

```
> pscp -scp cert\client\<CLIENT-HOSTNAME>.pem admin@<SERVER-HOSTNAME>:
admin@<SERVER-HOSTNAME>'s password:
<CLIENT-HOSTNAME>.pem         | 1 kB |   1.1 kB/s | ETA: 00:00:00 | 100%
```

Now, at the server,

a) Register the client and connect to the HSM via SSH.

```
lunash:> client register -client <CLIENT-HOSTNAME> -hostname <CLIENT-
HOSTNAME>
'client register' successful.
Command Result : 0 (Success)
```

b) Assign a partition to a client and connect to the HSM via SSH.

```
lunash:> client assignPartition -client <CLIENT-HOSTNAME> -partition
<PARTITION-NAME>
'client assignPartition' successful.
Command Result : 0 (Success)
```

Now, at the client,

6. Confirm connection settings.

The working directory is "C:\Program Files\SafeNet\LunaClient".

```
> vtl listServers
Server: <SERVER-HOSTNAME> HTL required: no

> vtl verify

The following Luna SA Slots/Partitions were found:

Slot    Serial #        Label
====    ========        =====
 1      615340068       <PARTITION-NAME>
```

7. Configure logging (optional)

The working directory is "C:\Program Files\SafeNet\LunaClient". The name of the log folder is "c:\temp" in the following example and it can be changed.

```
> vtl logging configure c:\temp
Success setting log path to c:\temp
> vtl logging show
Client logging written to: c:\temp\LunaCryptokiLog.htm
```

Configure HA (High Availability)

1. Create an HA Group.

   Open command prompt and run the following client commands.

```
> cd C:\Program Files\SafeNet\LunaClient
> lunacm.exe
lunacm:> slot set -s <SLOT-NUMBER>
lunacm:> hagroup creategroup -se <SERIALNUMBER> -label <HA-LABEL>

Enter the password: ************

New group with label "HAGroup" created with group number <SERIALNUMBER>.
Group configuration is:

HA Group Label: <HA-LABEL>
HA Group Number:  1615340039
HA Group Slot ID:  Not Available
Group Members:  615340039
Needs sync:  no
Standby Members:  <none>

Slot # Member S/N Member Label Status
====== ========== ============ ======
1 615340039  <PARTITION-NAME>   alive

It is recommended that you restart LunaCM to refresh the list of available
slots.

Command Result : No Error

lunacm v7.10.1 - Copyright (c) 2006-2020 SafeNet Assured Technologies, LLC.

Available HSMs:

Slot Id ->              1
HSM Label ->            '<PARTITION-NAME>'
HSM Serial Number ->    615340039
HSM Model ->            LunaSA-T7
HSM Firmware Version -> 7.10.1
HSM Configuration ->    Luna Network HSM (PW) Signing With Cloning Mode
HSM Status ->           OK
Slot Id ->              3
HSM Label ->            <HA_LABEL>
HSM Serial Number ->    1615340039
HSM Model ->            LunaVirtual
HSM Firmware Version -> 7.10.1
HSM Configuration ->    Virtual HSM (PW) Signing With Cloning Mode
HSM Status ->           N/A - HA Group

Current Slot Id: 1
```

NOTE: Both “Configure CSP” and “Configure KSP” must be configured again if you run the steps above.

2. Enable "HA Only".

```
lunacm:> slot set -s <HA-SLOT-NO>
        Current Slot Id:    <HA-SLOT-NO>     (Virtual HSM 7.10.1 (PW) Signing
With Cloning Mode)
Command Result : No Error

lunacm:> hagroup ho -e
        "HA Only" has been enabled.
Command Result : No Error

lunacm:> hagroup ho -s
        This system is configured to show only HA slots.  (HA Only is
enabled)
Command Result : No Error
```

Configure CSP

NOTE: Please note that for the deployment of the Autoenrollment Server, you need to configure CSP.

For SafeNet CSP, the utility **register.exe** (64-bit version) takes care of the registry. To configure CSP, open a command prompt and run the following commands.

Register CSP Library

```
C:\Program Files\SafeNet\LunaClient\CSP>register.exe /library
register v7.10.1
Success registering SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Luna
enhanced RSA and AES provider for Microsoft Windows !
Success registering SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Luna
Cryptographic Services for Microsoft Windows !
Success registering SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Luna
SChannel Cryptographic Services for Microsoft Windows !
```

Register the partition

```
C:\Program Files\SafeNet\LunaClient\CSP>register.exe

register v7.10.1

 ************************************************************************

 *   SafeNet Assured Technologies, LLC. LunaCSP, Partition Registration    *

 *                                                                        *

 *       Protect the HSM's challenge for the selected partitions.         *

 *       NOTE:                                                            *

 *            This is a WEAK protection of the challenge!!                *

 *            After you have configured all applications that will use    *

 *            the LunaCSP, and ran them once, you MUST run:               *

 *                register /partition /strongprotect                      *

 *            to strongly protect the registered challenges!!             *

 ************************************************************************


This procedure is a destructive procedure and will completely replace any
previous settings!!

Do you wish to continue?: [y/n]y

Do you want to register the partition named '<PARTITION-NAME>'?[y/n]: y

Enter challenge for partition '<PARTITION-NAME>' :************

Success registering the ENCRYPTED challenge for partition '<PARTITION-
NAME>:1'.

Only the LunaCSP will be able to use this data!


Registered 1 partition(s) for use by the LunaCSP!
```

Register the HA partition

Run the following commands if HA is configured.

```
C:\Program Files\SafeNet\LunaClient\CSP>register.exe /h

register v7.10.1


 ********************************************************************************
 *                                                                              *
 *                                                                              *
 *   SafeNet Assured Technologies, LLC. LunaCSP, Partition Registration         *
 *                                                                              *
 *       Protect the HSM's challenge for the selected partitions.               *
 *       NOTE:                                                                  *
 *            This is a WEAK protection of the challenge!!                      *
 *            After you have configured all applications that will use          *
 *            the LunaCSP, and ran them once, you MUST run:                     *
 *                register /partition /strongprotect                            *
 *            to strongly protect the registered challenges!!                   *
 ********************************************************************************


This procedure is a destructive procedure and will completely replace any
previous settings!!

Do you wish to continue?: [y/n]y

Do you want to register the partition named '<HA-LABEL>'?[y/n]: y

Enter challenge for partition '<HA-LABEL>' :************

Success registering the ENCRYPTED challenge for partition '<HA-LABEL>:1'.

Only the LunaCSP will be able to use this data!


Registered 1 partition(s) for use by the LunaCSP!
```

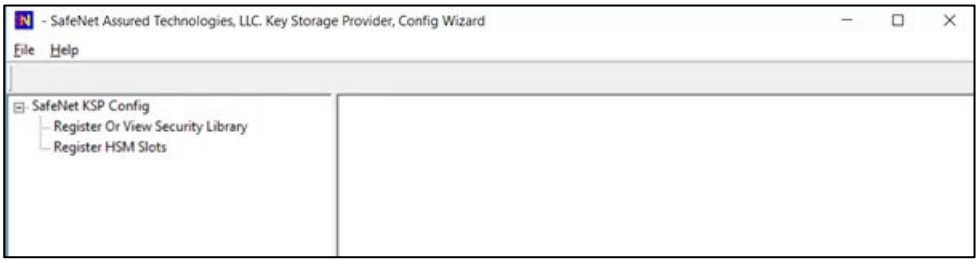
Configure KSP

NOTE: Please note that for the deployment of the Enterprise Gateway Server, you need to Configure KSP.

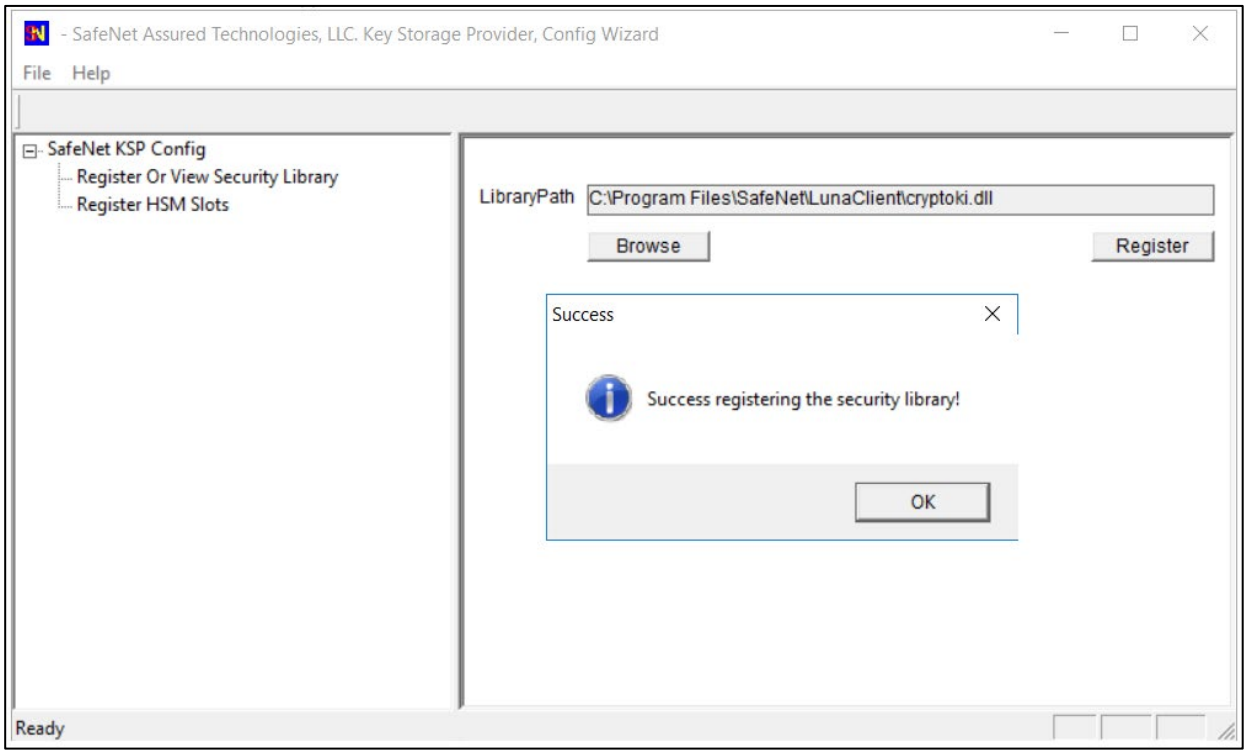
To configure KSP (CNG), run KspConfig.exe (Default location is "C:\Program Files\SafeNet\LunaClient\KSP\").

Follow instructions for the use of the graphical KspConfig.exe as described in KSP for CNG in the SDK Reference Guide.

The following window will appear.



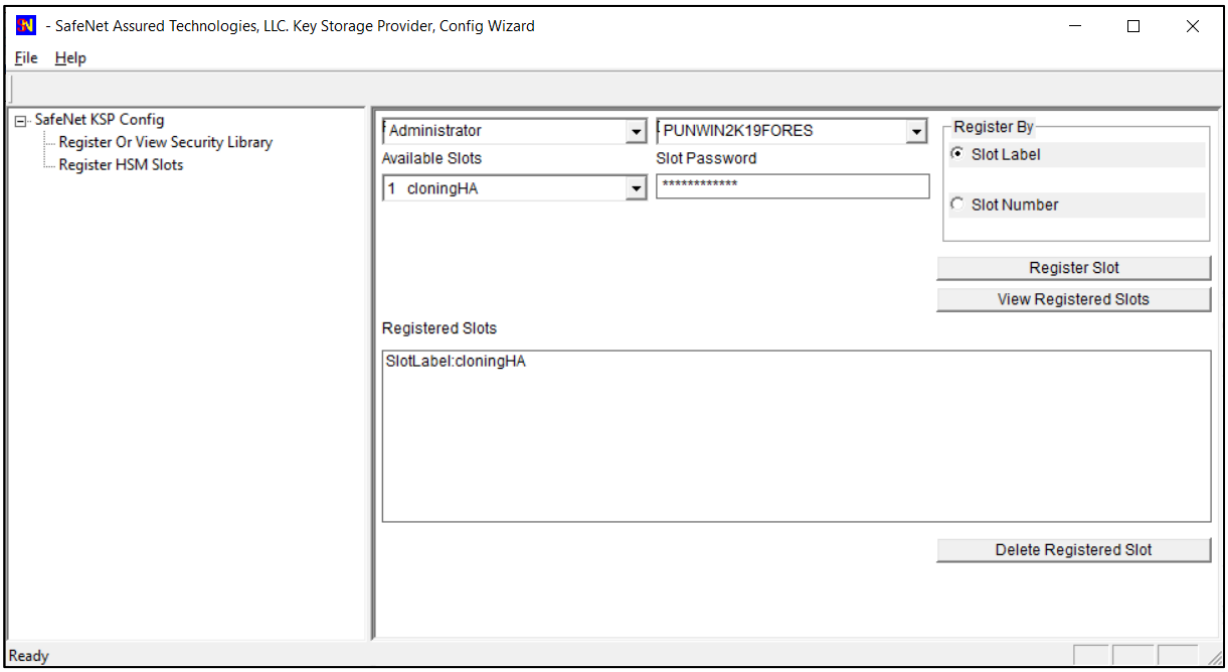
Double-click Register Or View Security Library, then confirm the value "C:\Program Files\SafeNet\LunaClient\cryptoki.dll", and click Register.



Double-click **Register HSM Slots** for Administrator/<Domain Name>

- Select Administrator
- Select <Domain Name>
- Select "HA Group" for **Available Slots**
- Enter Slot Password

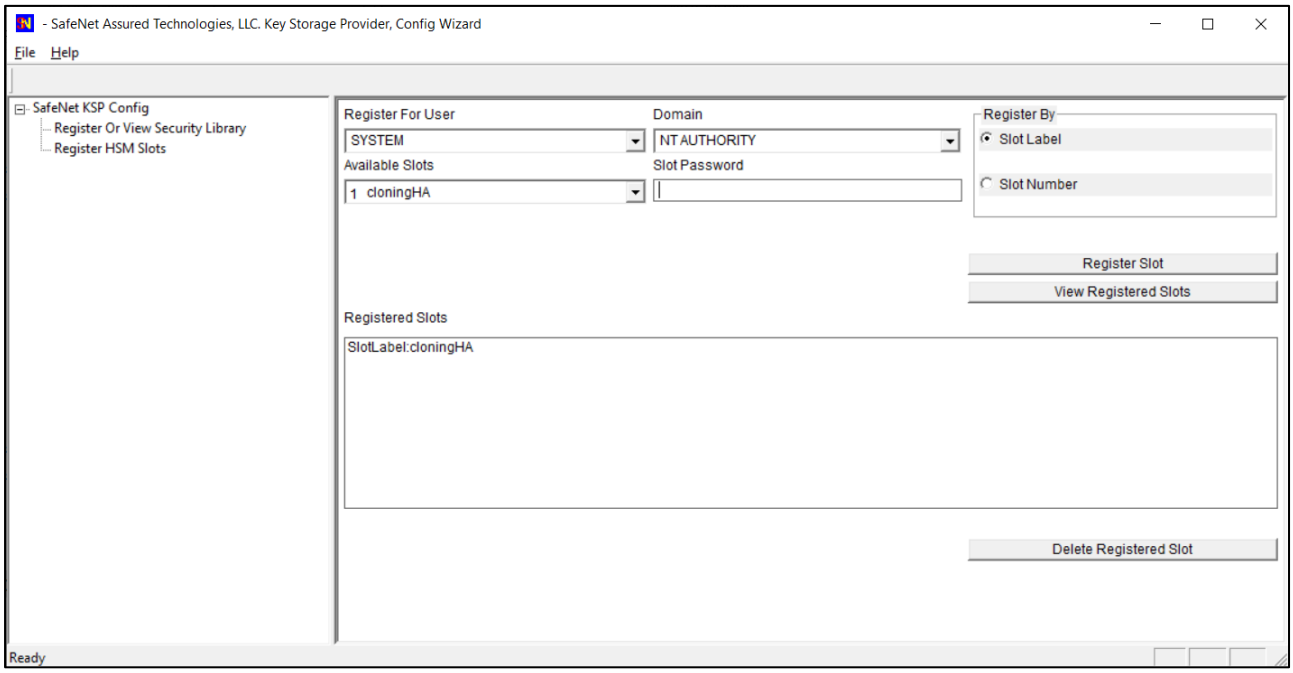
Click **Register Slot**.



Double-click **Register HSM Slots** for SYSTEM/NT AUTHORITY.

- Select SYSTEM
- Select NT AUTHORITY
- Select "HA Group" for **Available Slots**
- Enter Slot Password

Click **Register Slot.**



NOTE: When you click "Register Slot", there is no change on "Registered Slot", but this step is necessary.

When registering the Luna KSP (with the Luna KSPConfig utility), use the following user and domain combinations:

- The user and domain performing these procedures.
- The user and domain running the web application and using the private key.
- The local user and NT Authority domain user.
- The LocalSystem and NTAuthority of the system.

NOTE: If you implement the Autoenrollment server, you must also install and register the Luna CSP. Refer to the SafeNetAT product documentation for details.

Generate CSR and Install Certificate

1. Create the information file for CSR.

    a) To generate CSR using certreq.exe through CSP, the ProviderName must be "Luna Cryptographic Services for Microsoft Windows". The sample of inf file is as follows.

```
[NewRequest]
KeyUsageProperty = "NCRYPT_ALLOW_ALL_USAGES"
RequestType = PKCS10
ProviderName = "Luna Cryptographic Services for Microsoft Windows"
ProviderType = 1
Subject = "CN=Registration Authority"
KeyContainer = "CSPRA20201104"
MachineKeySet = TRUE
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
```

    b) To generate CSR using certreq.exe through KSP, the ProviderName must be "SafeNet Key Storage Provider". The sample of inf file is as follows.

```
[NewRequest]
KeyUsageProperty = "NCRYPT_ALLOW_ALL_USAGES"
RequestType = PKCS10
ProviderName = "SafeNet Key Storage Provider"
ProviderType = 0
Subject = "CN=Registration Authority"
KeyContainer = KSPRAID20201104
MachineKeySet = TRUE
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
KeyUsage = 0xf0
```

2. Generate CSR through HSM.

NOTE: <inf-file> is the file created at step #1, <csr-file> is an output file.

    a) Open command prompt and run the following command.

```
> certreq -new <inf-file> <csr-file>
```

    b) The CSR file will be generated as follows.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDjzCCAncCAQAwITEfMB0GA1UEAwwWUmVnaXN0cmF0aW9uIEF1dGhvcml0eTCC
....
C610uaqncn6FvLu5pygZYFEVtOanCXNQRRUWiDGWKjHF+10GMh+V5YUur55T4W80
0uwK
-----END NEW CERTIFICATE REQUEST-----
```

3. Get RA Certificate

   See "Get RA Certificate in PKI-Manager"

4. Install a certificate.

   a) Open command prompt (on the folder where the PKCS#7 file exists) and run the following command.

   ```
   > certreq -accept <issued-cert>
   ```

   b) Before running the command, the trusted root certificate must be installed. If not, the following error will be displayed.

   ```
   Certificate Request Processor: A certificate chain could not be built to a
   trusted root authority. 0x800b010a (-2146762486 CERT_E_CHAINING)
   ```

NOTE: Repeat the above commands to download and install RA certificate for both CSP and KSP CSR's.

Integration for Java Environment

Register Luna Provider

You must update the java.security configuration file to use the SafeNet security providers and the HSM.

To configure the java.security file:

1. Open the Java security configuration file java.security in a text editor. The file is available at <JDK_installation_directory>\jre\lib\security.
2. Update the Luna Providers in the java.security file so they appear as follows:

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

3. Save the changes to the java.security file.

Enabling the HSM keystore

You must configure the Java Code Signing utility to use the keystore located on the HSM.

To enable the HSM keystore

1. Copy the **LunaAPI.dll** and the **LunaProvider.jar** files from the **<Luna_installation_directory>\JSP\lib** to the Java extension folder located at **<JDK_installation_directory>\jre\lib\ext.**
2. Set the environment variables for **JAVA_HOME** and **PATH**.

NOTE: We recommend setting the PATH variable in Windows environments using the System Environments menu.

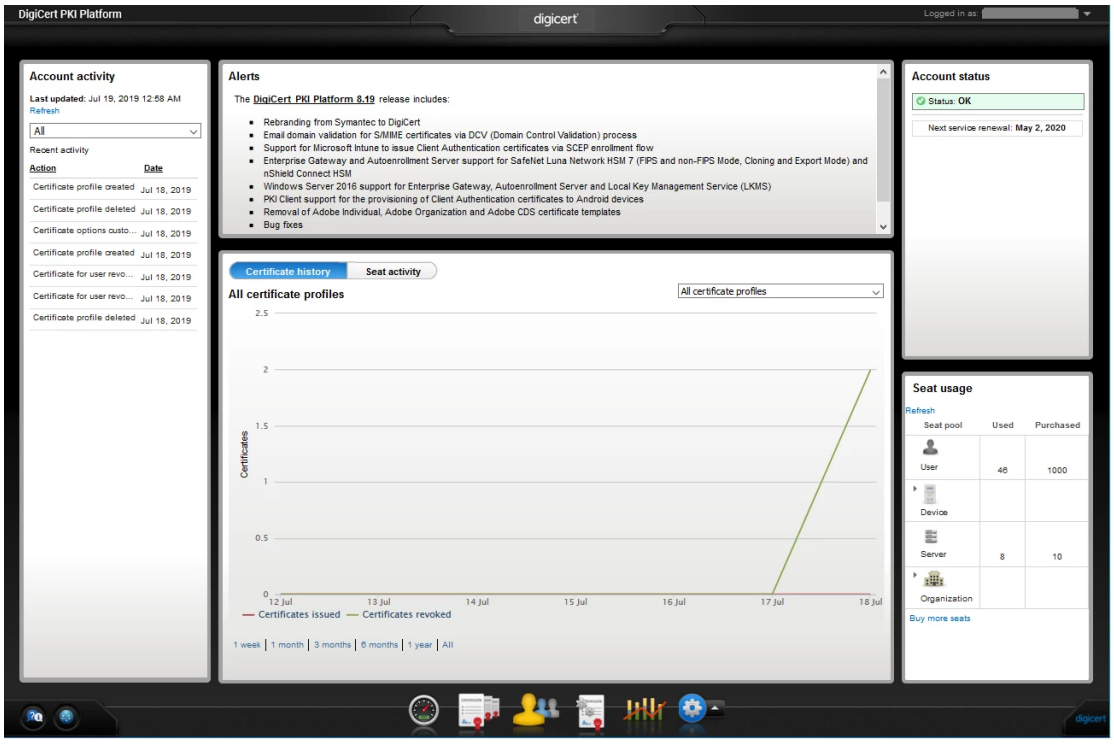
Install RA Certificate

Refer section "Using an RA Certificate on HSM" of **DigiCert® PKI Enterprise Gateway Deployment Guide** document.

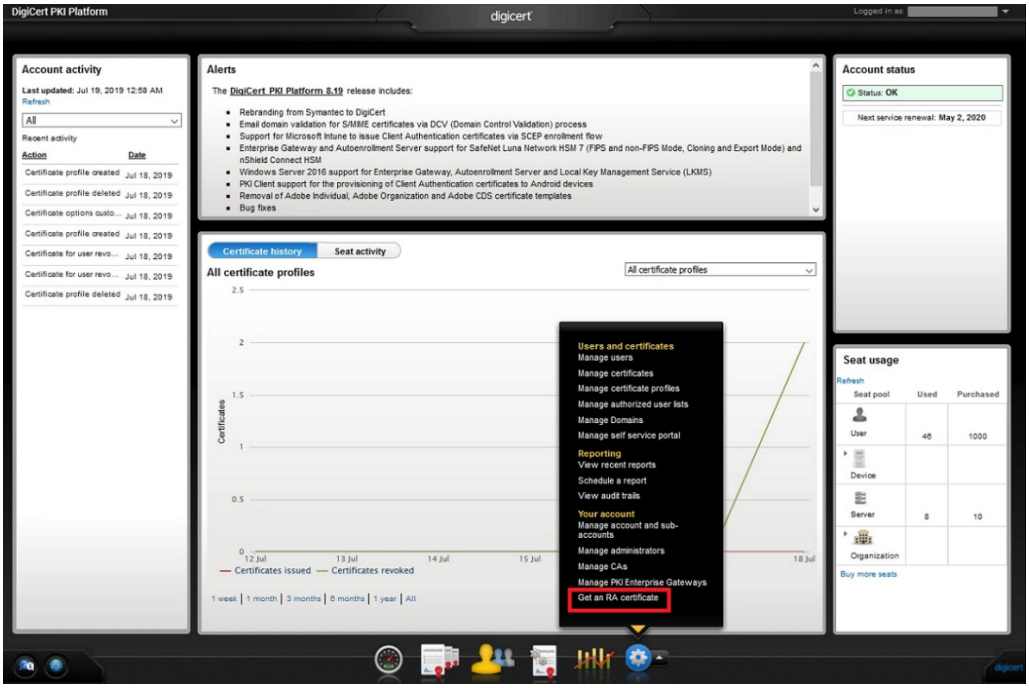
Get RA Certificate in PKI-Manager

The generated CSR(PKCS#10) can be copied and pasted onto the "**Get an RA certificate**" page on PKI Manager (by an authorized PKI Administrator) and save the resulting RA (PKCS#7) certificate onto a local folder.

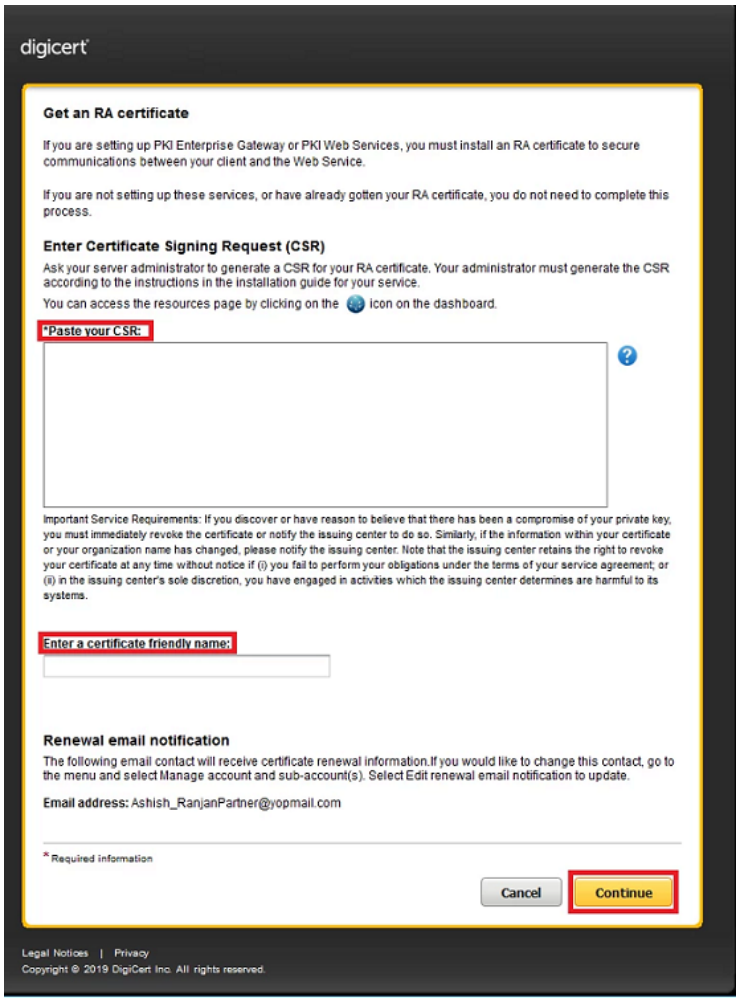
1. Go to PKI Manager and sign in by using your certificate.



2. Click Menu and select "Get an RA Certificate".



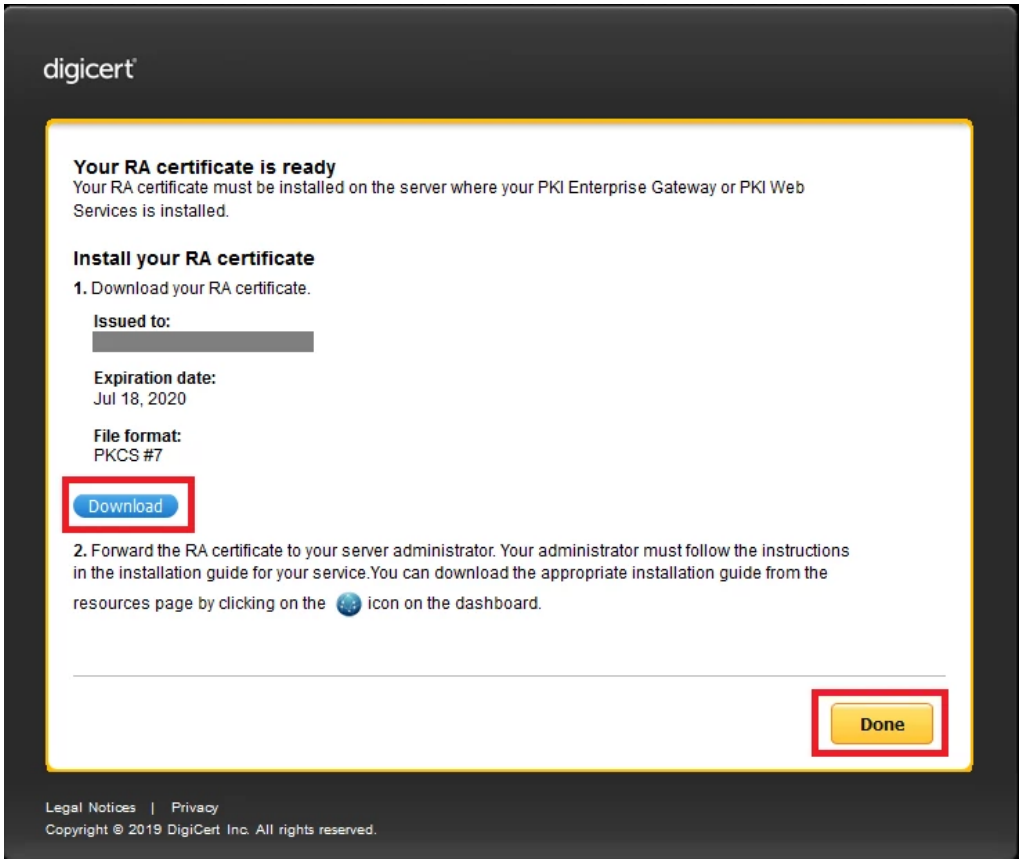
3. Paste your CSR and enter a certificate friendly name and then click "Continue".



The CSR looks as follows; Please paste it.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDjzCCAncCAQAwITEfMB0GA1UEAwwWUmVnaXN0cmF0aW9uIEF1dGhvcml0eTCC
...
zbnTmg1IIY4NSgFcRsbs5j5GQDN86gSKmQ8/EvOjbpC62X3ZDhVmYSMBJUO1Jgv6
1tyz
-----END NEW CERTIFICATE REQUEST-----
```

4. Click "Download" and then the PKCS#7 file will be downloaded.



5. Click "Done" to go back to the PKI Dashboard.