THALES

Microsoft Active Directory Certificate Services: Integration Guide

THALES LUNA HSM AND LUNA CLOUD HSM

Document Information

Document Part Number	007-008669-001
Revision	AC
Release Date	20 April 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
Prerequisites	5
Configuring Luna HSM	5
Configuring Luna Cloud HSM	6
Integrating Luna HSM with Microsoft AD CS on Windows Server	7
Configure SafeNet Key Storage Provider (KSP)	7
Install Microsoft AD CS on Windows Server using SafeNet KSP	9
Enroll Certification Authority Certificate	16
Archive CA Key	20
Perform Key Recovery	33
Migrating CA keys from Microsoft Software Key Storage Provider to SafeNet Key Storage Provider	35
Configure SafeNet KSP	35
Back up the CA	37
Migrate a MS CA onto a Luna HSM or Luna Cloud HSM service using ms2Luna	38
Install Microsoft Active Directory Certificate Services on Windows Server using SafeNet Key Storage	
Provider with migrated key	40
Restore MS CA	48
Installing and Configuring the CA cluster using SafeNet Key Storage Provider	51
Set up the CA server role on the first cluster node	51
Set up the CA server role on the second cluster node	54
Set up the Failover Cluster feature on the cluster nodes	66
Create a Failover Cluster	69
Configure AD CS Failover Cluster	71
Create CRL objects in the Active Directory	75
Modify CA configuration in Active Directory	76
Migrating AD CS Cluster keys from Microsoft Software KSP to SafeNet KSP	80
Contacting Customer Support	91
Customer Support Portal	91
Telephone Support	91

Overview

This document explains how to integrate Microsoft Active Directory Certificate Services (AD CS) with Luna HSM or Luna Cloud HSM. The Microsoft AD CS provides customizable services for creating and managing public key certificates used in software security systems employing public key infrastructure. Organizations use public key certificates to enhance their digital security by binding the identity of a person, device, or service to a corresponding private key.

The root of trust in a public key infrastructure is the certificate authority (CA). Fundamental to this trust is the CA's root encryption key, which is used to sign the public keys of certificate holders and more importantly its own public key. Microsoft AD CS integrates with Luna HSM or Luna Cloud HSM service to secure the root encryption key.

Using Luna HSMs to secure the Microsoft AD CS root encryption key provides the following benefits:

- > Secure generation, storage and protection of the Identity signing private key on FIPS 140-2 level 3 validated hardware
- > Full life cycle management of the keys
- > HSM audit trail
- > Load balancing and fail-over by clustering the HSMs
- > Using cloud services with confidence

NOTE: Luna Cloud HSM does not have access to the secure audit trail

Certified Platforms

This integration is certified on the following platforms:

- Certified platforms on Luna HSM
- <u>Certified platforms on Luna Cloud HSM</u>

Certified platforms on Luna HSM

Platforms Tested
Windows Server 2022
Windows 2019 Server
Windows 2016 Server
Windows Server 2012R2

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 CloudHSM Classic.

Certified	platforms	on Luna	Cloud	HSM

НЅМ Туре	Platforms Tested
Luna Cloud HSM	Windows Server 2022
	Windows 2019 Server
	Windows 2016 Server
	Windows Server 2012R2
	1

Luna Cloud HSM: Luna Cloud HSM services provide on-demand, cloud-based storage, management, and generation of cryptographic keys 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 only those services that you need.

Prerequisites

Before you begin the integration process, ensure that you have completed the following tasks:

Configuring Luna HSM Configuring Luna Cloud HSM

Configuring Luna HSM

To configure Luna HSM:

- 1. Ensure the HSM is setup, initialized, provisioned and ready for deployment.
- 2. Create a partition, establish a Network Trust Link (NTL) between the HSM and client, and enable the client to access the partition. Refer to Luna Network HSM documentation for the detailed process.
- 3. Initialize Crypto Officer and Crypto User roles for the partition.
- 4. Use the following command to validate that the partition is successfully registered and configured:

```
Path to lunacm utility>lunacm
```

```
lunacm.exe (64-bit) v7.3.0-139. Copyright (c) 2018 SafeNet. All rights reserved.
```

Available HSMs:

Slot Id ->	0
Label ->	ms-adcs
Serial Number ->	1238696044953
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

NOTE: For a detailed description of the steps involved in Luna HSM configuration, refer to Luna Network HSM documentation.

To configure Luna HSM HA (High-Availability)

Please refer to the Luna HSM documentation for HA steps and details regarding configuring and setting up two or more HSM appliances on Windows and UNIX systems. You must enable the HAOnly setting in HA for failover to work so that if primary stop functioning for some reason, all calls automatically routed to secondary till primary starts functioning again.

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

Configuring Luna Cloud HSM

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 <u>Supported</u> <u>Mechanisms</u>.

Integrating Luna HSM with Microsoft AD CS on Windows Server

This section outlines the steps to install and integrate Microsoft Active Directory Certificate Services (AD CS) on Windows Server with a Luna HSM or Luna Cloud HSM service. Microsoft AD CS uses the SafeNet Luna KSP (Key Storage Provider) for integration.

We recommend familiarizing yourself with Microsoft Active Directory Certificate Services. Refer to the <u>Microsoft AD CS Configuration</u> documentation for more information.

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

To configure the SafeNet Key Storage Provider:

- 1. Navigate to the <SafeNet HSM Client installation Directory>/KSP directory.
- 2. Run the KspConfig.exe (KSP configuration wizard).
- 3. Double-click Register Or View Security Library.
- 4. Browse the library cryptoki.dll from the Luna HSM Client installation directory or Luna Cloud HSM service client package and click **Register**.

N	- SafeNet-Inc Key Storage Provider, Config Wizard	-	x
File Help			
SafeNet KSP Config Register Or View Security Library Register HSM Slots	LibraryPath C1Program FilestSafeNetLunaClienttcryptoki dil Browse		
Ready	, 		- //

5. On successful registration, you will see the following message:

Success registering the security library!

N	- SafeNet-Inc Key Storage Provider, Config Wizard	_ 🗆 X
File Help		
B SafeNet KSP Config Register Or View Security Library Register HSM Slots	LibraryPath C:IProgram FilesISafeNetLunaClienticryptoki.dll Browse Success Success registering the security library! OK	Register
Ready		

- 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, a message "The slot was successfully and securely registered" displays.

N	- SafeNet-Inc Key Storage Provider, Config Wizard	_ D X
File Help		
SafeNet KSP Config Register Or View Security Library Register HSM Slots	Register For User Domain Administrator Invite Notice Noti	Register By
Ready		

N	- SafeNet	-Inc Key Storage Provider, Config Wizard	– D X
File Help			
SafeNet KSP Config Register Or View Security Library Register HSM Slots	Register For User SYSTEM Available Slots 1 part1 Registered Slots SlotLabel:part1 The slot	Domain INT AUTHORITY Slot Password Success Was successfully and securely registered! OK	Register By Stot Label Stot Number Register Stot View Registered Stots
			Delete Registered Slot

9. Register the same slot for NT AUTHORITY\SYSTEM.

NOTE: Both slots have been registered, despite only one entry appearing for the service in the **Registered Slots** section of the KSP interface.

Install Microsoft AD CS on Windows Server using SafeNet KSP

You must configure Microsoft AD CS to use the Luna HSM or Luna Cloud HSM service when you configure the Microsoft Certificate Authority (CA) user role. To install Microsoft AD CS:

- 1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
- 2. Ensure you have configured the SafeNet KSP. Refer to the section Configure SafeNet Key Storage Provider (KSP) section for more information.
- 3. Open the Server Manager under Configure this Local Sever and click Add Roles and Features.
- 4. The Add Roles wizard displays.
- 5. Click Next.
- 6. Select the Role-based or feature-based installation radio button and click Next.

7. Select the **Select a server from the server pool** radio button and select your server from the **Server Pool** menu.

on server			DESTINATION SERVI D1.noida.co
Select a server or a vir Select a server fro Select a virtual har	rtual hard disk on which m the server pool rd disk	to install roles and features.	
Filter:			
Name	IP Address	Operating System	1
D1.noida.com	172.25.11.92	Microsoft Windows Server 20	112 Standard
1 Computer(s) found	ers that are running Wir	dows Server 2012, and that have	e been added by using 1
	ON SETVET Select a server or a vii Select a server fro Select a virtual hai Server Pool Filter: Name D1.noida.com	ON SETVET Select a server or a virtual hard disk on which Select a server from the server pool Select a virtual hard disk Server Pool Filter: Name IP Address D1.noida.com 172.25.11.92 1 Computer(s) found	ON SETVET Select a server or a virtual hard disk on which to install roles and features. Select a server from the server pool Select a virtual hard disk Server Pool Filter: Name IP Address Operating System D1.noida.com 172.25.11.92 Microsoft Windows Server 20 1 Computer(s) found

8. Click Next.Select the Active Directory Certificate Services check box.

elect server role	25	DESTINATION SERVE D1_noida.com
Before You Begin Installation Type	Select one or more roles to install on the selected server, Roles	Description
Server Roles Features Confirmation Results	Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Federation Services Active Directory Rights Management Services Application Server DHCP Server DNS Server Fax Server V File And Storage Services (Installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services	 Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

- **9.** A window displays stating **Add features that are required for Active Directory Certificate Services?** To add a feature, click the **Add Features** button.
- 10. Click Next to continue.
- **11.** On the Active Directory Certificate Services page click **Next** to continue.
- 12. Select the Certification Authority check box from the Role services list and click Next.

A	Add Roles and Features Wizard	- D X
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Select the role services to install for Active Directory Certific Role services Certification Authority Certificate Enrollment Policy Web Service Certification Authority Certification Authority Certification Authority Online Responder	DESTINATION SERVER D1.noida.com Cate Services Description Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.
	< Previous	Vex Install Cancel

- 13. Click Install.
- 14. When installation is complete, click **Configure Active Directory Certificate Services on the destination server** and the AD CS Configuration wizard displays.

	Add Roles and Features Wizard	
Installation proc	jress	DESTINATION SERVER D1.noida.com
Before You Begin Installation Type Server Selection Server Roles	View installation progress Feature installation Configuration required. Installation succeeded on D1.noida.com.	_
Features AD-CS Role Services Confirmation Results	Active Directory Certificate Services Additional steps are required to configure Active Directory Certificate Server Configure Active Directory Certificate Services on the destination server Certification Authority Remote Server Administration Tools Role Administration Tools Active Directory Certificate Services Tools Certification Authority Management Tools	vices on the destination
	You can close this wizard without interrupting running tasks. View task page again by clicking Notifications in the command bar, and then Tas Export configuration settings	c progress or open this sk Details.
	< Previous Next >	Close Cancel

15. On the Credentials page of AD CS Configuration wizard, click Next to continue.



16. Select the Certification Authority check box and click Next.

- 17. Select the Enterprise CA radio button and click Next.
- 18. Select the Root CA radio button and click Next.
- 19. Setup the Private Key for the CA to generate and issue certificates to clients. If you would like to create a new private key select the Create a new private key radio button. Click Next. If you would like to use an existing private key, proceed to step 24.



20. Open the Select a cryptographic provider: drop-down menu and select an algorithm using a SafeNet Key Storage Provider. Open the Key length: drop-down menu and select a key-length.

Cryptography fo	or CA		DESTINATION SERVED D1.noida.com
Credentials Role Services	Specify the cryptographic options		P. J. al.
Setup Type	BCAMAR	-	Ney length:
CA Type Private Kev	RSA#Wicrosoft Software Key Storage Provider	2	2048
Cryptography CA Name	Microsoft Base Cryptographic Provider v1.0 ECDSA_P521#Microsoft Software Key Storage Provider ECDSA_P256#Microsoft Software Key Storage Provider		
Validity Period	Microsoft Strong Cryptographic Provider	_	
Certificate Database	ECDSA_P256#SafeNet Key Storage Provider		
Confirmation Progress Results	ECDSA_P384#Microsoft Software Key Storage Provider Microsoft Base DSS Cryptographic Provider RSA#Microsoft Smart Card Key Storage Provider	HI.	y the CA.
	DSA#Microsoft Software Key Storage Provider DSA#SafeNet Key Storage Provider		
	ECDSA_P384#Microsoft Smart Card Key Storage Provider ECDH P256#SafeNet Key Storage Provider	~	

- **21.** Select the **Hash Algorithm** for signing certificates issued by this Certificate Authority and key length settings for your installation.
- 22. Select the Allow administrator interaction when the private key is accessed by the CA check box.
- 23. Click Next. Proceed to step 27.

L	AD CS Configuration		×
Cryptography fo	or CA		DESTINATION SERVER D1.noida.com
Credentials Role Services Setup Type	Specify the cryptographic options Select a cryptographic provider:		Key length:
CA Type	ECDSA_P256#SafeNet Key Storage Provider		256 💌
Private Key	Select the hash algorithm for signing certificates issued	by this CA:	
Cryptography	SHA256		
CA Name Validity Period Certificate Database	SHA384 SHA512 SHA1		
Confirmation Progress Results	Allow administrator interaction when the private key	/ is accessed b	ay the CA.
	More about Cryptography		
	< Previous Ne	ext N	Configure Cancel

24. Select the Use existing private key check box. Setup the Private Key for CA to generate and issue certificates to clients. Select Use existing private key and Select an existing private key on this computer. Click Next to continue.



25. Click Change. Select the SafeNet Key Storage Provider algorithm that you have used to generate the private keys and clear the CA Common name, click Search.

xisting Key		DESTINATION SERVEI D1.noida.con
Credentials	Select an existing key	
Role Services	🚡 Change Cryptographic Provider 🗖 🗖	
Setup Type		le on the target computer matching
CA Type	Search for keys on the target computer using the	
Private Key	tollowing criteria:	
Existing Key	Cryptographic provider:	nge Provider
Cryptography.	ECDSA_P256#SafeNet Key Storage Provider	
CA Name	Type certification authority (CA) common name	
Validity Period	(optional):	Change
Certificate Database	noida-D1-CA	
Continnation	Search Cancel	
Progress		
	Allow administrator interaction when the private key	is accessed by the CA.
	More about Existing Key	
	< Previnus Nex	t > Configure Cancel

26. Select the Existing Key and click Next.

	- SPOTISTICAL OF
xisting Key	DESTINATION SET D1.noida
Credentials	Select an existing key
Role Services	
Setup Type	Select a key from the list. The listed keys are the keys available on the target computer matching
CA Type	the search criteria. You may change the search criteria.
Private Key	Search criteria for key
Existing Key	Cryptographic provider: ECDSA_P256#SafeNet Key Storage Provider
Cryptography	CA common name: noida-D1-CA
CA Name	
Validity Period	Change.
Certificate Database	Search results:
Confirmation	noida-D1-CA
Progress	
Results	
	Allow administrator interaction when the private key is accessed by the CA.
	More about Existing Key

27. Configure a common name to identify this Certificate Authority. Click Next.

ē.	AD CS Configuration	×
CA Name	DE	STINATION SERVER D1.noida.com
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Specify the name of the CA Type a common name to identify this certification authority (CA). This name is certificates issued by the CA. Distinguished name suffix values are automatical be modified. Common name for this CA: noida-D1-CA Distinguished name suffix: DC=noida,DC=com Preview of distinguished name: CN=noida-D1-CA,DC=noida,DC=com	added to all y generated but can
	< Previous Next > Config	ure Cancel

- Proceed to set the Certificate Validity Period. Click Next. Configure the Certificate database location. It records all the certificate requests, issued certificates, and revoked or expired certificates. Click Next.
- 29. Click Configure to configure the selected roles, role services, or features.
- 30. Click Close to exit the AD CS Configuration wizard after viewing the installation results.

A private key for the CA will be generated and stored on the HSM.

- **31.** Open a command prompt and run the following command to verify that service is running: sc query certsvc
- 32. Open a command prompt and run the following command to verify the CA key:

```
certutil -verifykeys
```

The result of the command shows the CA keys have successfully been verified.

Enroll Certification Authority Certificate

1. Create a CA template that uses SafeNet Key Storage Provider.

Open a command prompt and run certtmpl.msc.

Right click the **Administrator** template.Click Duplicate Template.

Certificate Templates (WIN-AA7	Template D	isplay Name	Schema Version	Versi	~	Actions	
	Adm -		- Maria	4.1		Certificate Templates (MIN-AA	74
	a Auth	Duplicate Template	1	3.1		Man Aniana	6.4m
	🗟 Basic	All Tasks	▶ 1	3.1		More Actions	
	🗟 CA E	Properties	2	106.0		Administrator	
	CEP E	i i ap as ass	1	4.1		More Actions	
	🗟 Code	Help	1	3.1		- more reading	
	Compute	er	1	5.1			
	Copy of .	Administrator	3	100.3			
	🗟 Cross Ce	rtification Authority	2	105.0			
	d Directory	Email Replication	2	115.0			
	🗟 Domain	Controller	1	4.1			
	🗟 Domain	Controller Authentication	2	110.0			
	EFS Reco	very Agent	1	6.1	=		
	Enrollme	nt Agent	1 4.1				
	🖳 Enrollme	nt Agent (Computer)	1	5.1			
	Exchange	e Enrollment Agent (Offline n	equ 1	4.1			
	🗟 Exchange	e Signature Only	1	6.1			
	Exchange	e User	1	7.1			
	IPSec		1	8.1			
	🗟 IPSec (Of	fline request)	1	7.1			
	🗟 Kerberos	Authentication	2	110.0			
	🗟 Key Reco	ivery Agent	2	105.0			
	🗃 OCSP Re	sponse Signing	3	101.0			
	RAS and	IAS Server	2	101.0			
	🗟 Root Cer	tification Authority	1	5,1			
	🗟 Router (0	Offline request)	1	4.1	1		
	🗟 Smartcar	d Logon	1	6.1			
	🗟 Smartcar	d User	1	11.1	1		
	🗟 Subordin	ate Certification Authority	1	5.1			
	🗟 Test Adn	ninistrator	4	100.3	v		

2. Select Windows Server 2008 for both Certification Authority and Certificate recipient under Compatibility Settings, Click OK.

		Certificate	Templates Consol	e		- 0 X
ile Action View Help						
					u	
Certificate Templates (WIN-AA/	Template L	Propertie	s of New Template	x	Actions	
	Authent		and a second		Certificate Templates (WI	N-AA74
	Resig FE	tName S	erver Issuanc	e Requirements	More Actions	
	CA Evolution	seded Templates	Extensions	Security	. Manufatana ang	
	CEP End	dity General	Request Handling	Cryptography	Administrator	
	² Code Sic ² Comput ² Comput ² Comput ² Comput ² Comput ² Comput ² Comput ² Shown ² Shown	ate options available et in Compatibility Sel resulting changes bility Settings ation Authority was Server 2008 ate recipient was XP / Server 2003 was YP / Server 2003 was YP / Server 2003 was XP / Server 2003	are based on the earliest tings.	from using this		
	😨 Subordi 📃 😨 Test Administrator	territoria de la	4	100.3	T	
ш	<		2.162	>		

- 3. Verify the changes on the Resulting Changes window. Click **OK**.
 - a. Select the General tab. Enter template name.
 - **b.** Go to the Cryptography tab. Select Key Storage Provider for Provider Category.
 - c. Select the Requests must use one of the following providers radio button.
 - d. In the Providers field select the SafeNet Key Storage Provider only.
 - e. For Algorithm Name select an algorithm.
 - f. Select Request Hash.
 - g. Go to the Subject Name tab.
 - h. Uncheck the Include e-mail name in subject name check box

Compatibility	ompatibility General		st Handling	Cryptography
Superseded Te	emplates	Ext	ensions	Security
Subject Name	Se	erver	Issuance	Requirements
C Supply in the re	quest			
renewal rec	t information f juests (*)	tom existing	g certificates to	r autoenrollment
Build from this A	Active Directo	ry informati	on	
Select this optio simplify certificat	n to enforce o e administrati	consistency	among subjec	t names and to
Subject name fo	ormat:			
Fully distinguish	ned name			~
🗌 Include e-ma	ail name in sut	oject name	(
Include this infe	instice in site	mata aubia	at pamar	
	madori in alle	anate subje	ict name.	
User princip	al name (LIPN	ĩ		
	cinal name (SI	PNI		
hand a contract of the second s	о н	19760		

i. Uncheck the E-mail name check box.

- j. Click Apply to save the template. Click OK.
- **k.** Open the command prompt and run **certsrv.msc**.
- I. Double-click the CA name.
- m. Right-click the Certificate Templates node.

Certification Aut	hority (Local)	Name	Intended Purpose
noida-D1-CA	A Certificates ertificates, Requests quests e Templates		There are no items to show in this view.
	Manage		Cartificate Tamplate to Issue
	View		Compare to pare
	Refresh Export List		
	Help		

n. Select New -> Certificate Template to Issue

o. Select the template you recently created and click OK.

Select one Certificate Template to enable Note: If a certificate template that was red	on this Certification Authority. cently created does not appear on	this list, you may need to wait until
nformation about this template has been All of the certificate templates <u>in the orga</u> r	replicated to all domain controllers nization may not be available to yo	ur CA.
for more information, see <u>Certificate</u>	Template Conceptsi	
Name	Intended Purpose	^
🗐 Administrator	Microsoft Trust List Sign	ing, Encrypting File System, Secure E
📟 Authenticated Session	Client Authentication	
💹 Basic EFS	Encrypting File System	-
폜 CA Exchange	Private Key Archival	
CEP Encryption	Certificate Request Age	nt
😨 Code Signing	Code Signing	
R Computer	Client Authentication, Se	erver Authentication
😨 Copy 2 of Administrator	Client Authentication, Se	ecure Email, Encrypting File System, N
R Copy of Adriatistrator	Client Authentication, Se	ecure Email, Encrypting File System, N
R Cross Certification Authority	<all></all>	×. × ×
		>

- 4. Request a certificate based on the template.
 - a. Request a certificate based on the template.
 - **b.** Open the command prompt and run the **certmgr.msc** command.
 - c. Right-click the Personal node.
 - d. Select All Tasks -> Request New Certificate...

-	certmgr - [C	ertificates - Current User\Personal]
File Action	View Help	
🗢 🔿 🙇	🖬 🔲 🖻 🖻 🛅	1
Certificates	- Current User Obje	ct Type Tricates
þ 🧾 Ente 🗌	All Tasks	Find Certificates
b Solution	View	Request New Certificate
þ 🚰 Trus Þ 🧰 Untr	Refresh Export List	Import Advanced Operations
D Initial District Stress of the second stress o	Help	
þ 🎽 Client A Þ 🎒 Smart C	uthentication Issuers ard Trusted Roots	
< III	> <	ш
Request a new c	ertificate from a certificatior	authority (CA) in your domain

- e. Click Next.
- f. Click Next.
- g. Enable the check box for the template you created above.
- h. Click Enroll.
- i. Verify the certificate is enrolled successfully. The UI enrollment wizard shows if the certificate enrollment was successful.

Archive CA Key

You can verify that the configurations that are possible with the Luna HSM or Luna Cloud HSM service can be used and do not interfere with the CA key archival functionality. To complete archiving the CA-Key you must complete the following tasks:

NOTE: If you wish to secure the key on Luna HSM that is used to encrypt the Archived Keys then you need to select the SafeNet Key Storage Provider for generating the keys for Key Recovery Agent certificate.

Archive the CA key

- 1. Install the Enterprise Certificate Server using the SafeNet Key Storage Provider and ECC key.
- 2. Verify the CA is installed correctly.
- 3. Add a Key Recovery Agent (KRA) template to CA for issuing.
- 4. Open the command prompt and run the **certsrv.msc** command.
- 5. Right-click the **Certificate Templates** node. Select **New -> Certificate Template to Issue**.

	certsrv - [Certi	fication Authority (Local)]	_ - ×
File Action View Help			
(= +) 🔒 🚺 🕨 🖷			
🙀 Certification Authority (Loca	al) Name	Description	
 finoida-D1-CA Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Template 	anoida-D1-CA	Certification Authority	
Ceruncate remained	Manage		
	New 🔹 🕨 Certifica	ate Template to Issue	
	Refresh		
	Help		

6. Select the Key Recovery Agent template and click OK.

elect one Certificate Template to ena ote: If a certificate template that was formation about this template has been Il of the certificate templates in the or or more information, see <u>Certifica</u>	ble on this Certification Authority. recently created does not appear on this list, you may need to wait until en replicated to all domain controllers. ganization may not be available to your CA. <u>ate Template Concepts.</u>	
Name	Intended Purpose	1
😟 Exchange User	Secure Email	Г
🖳 IPSec	IP security IKE intermediate	
😟 IPSec (Offline request)	IP security IKE intermediate	
🕺 Kerberos Authentication	Client Authentication, Server Authentication, Smart Card Logo	c
😡 Key Racovery Agent	Key Recovery Agent	
🕺 OCSP Response Signing	OCSP Signing	=
🖳 RAS and IAS Server	Client Authentication, Server Authentication	1
😨 Router (Offline request)	Client Authentication	
园 Smartcard Logon	Client Authentication, Smart Card Logon	
Smartcard User	Secure Email Client Authentication, Smart Card Locon	1
		1

Issue the KRA Certificate.

- 1. Request the KRA certificate. Open the command prompt and run the **certmgr.msc** command.
- 2. Right-click Personal node. Select All Tasks -> Request new certificate....

Certific	ates - Current User Find Certificates	Logica	l Store Name sonal stad Root Certification Authorities	
🗧 🖾 En	All Tasks	*	Find Certificates	
int 🖸 🔤	Refresh		Req St New Certificate	
Tr	Help		Import	
📔 Unt	rusted Certificates		Advanced Operations	
Tru: Clie Clie Cert	sted People int Authentication Issuers tificate Enrollment Reque art Card Trusted Roots	Thu Tru Clie Cer	rd-Party Root Certification Authorities sted People nt Authentication Issuers tificate Enrollment Requests art Card Trusted Roots	
			7.44	

3. Click Next.

4. Select Active Directory Enrollment Policy and click Next.



5. Select the Key Recovery Agent check box template and click Enroll.

You can request the following types of click Enroll.	certificates. Select the certificates you want t	o request, and then
Active Directory Enrollment Policy		
Copy 2 of Administrator	i) STATUS: Available	Details 🔹
Vev Recovery Agent	i) STATUS: Available	Details N
Showall templater		

6. Verify the enrollment is pending and click **Finish**.



Issue the KRA certificate from the CA snap-in.

- 1. Open the command prompt and run the **certsrv.msc** command.
- 2. Select the **Pending Requests** node. Right-click on the latest request for the KRA template. Select **All Tasks** and click **Issue**.



3. Click on Issued Certificates. Verify that the new certificate is issued.

Retrieve the issued certificate from CA

- 1. Open the command prompt and run certmgr.msc command.
- 2. Right click Certificates Current User
- 3. Select All Tasks and click Automatically enroll and retrieve certificates...



- 4. Click Next.
- 5. Select the KRA certificate you just issued and enroll it.

Configure the CA to support Key Archival.

- 1. Open the command prompt and run the certsrv.msc command.
- 2. Right-click CA Name and select Properties.
- 3. Select the Recovery Agent tab.
- 4. Select the Archive the key radio button.

5. Click the **Add** button.

T 11 1 2 2 1 2 7 1 2 7	Storage	Certifica	ate Managers
General	Policy Modu	ile 🛛	Exit Module
Enrollment Agents	Auditing	Recovery Agent:	s Security
 Archive the key Number of recover 	rvey ny agents to use:		
Ney recovery ager Subject	Issuer	Expiration Date	e Status
	Add	Remove	View

6. Select the KRA certificate you just issued, Click OK.



- 7. Click OK
- 8. Verify the CA service must be restarted, click Yes.

Create a template with Key Archival enabled

1. Open the command prompt and run the **certtmpl.msc** command.

2. Right-click the User template and click **Duplicate Template**.

Certificate Templates Console						_		×
File Action View Help								
Certificate Templates (WIN-78P)	Template Display Name	Schema Version	Version '	^ [Actions			
	R Cross Certification Authority	2	105.0		Certificate Templates (V	VIN-78	РĠЗККВ	B 🔺
	Directory Email Replication	2	115.0		More Actions			•
	🗷 Domain Controller	1	4.1					
	Representation Provided Authentication	2	110.0		User			•
	🗷 EFS Recovery Agent	1	6.1		More Actions			•
	🗷 Enrollment Agent	1	4.1					
	🐵 Enrollment Agent (Computer)	1	5.1					
	🐵 Exchange Enrollment Agent (Offline requ	1	4.1					
	🚇 Exchange Signature Only	1	6.1					
	🚇 Exchange User	1	7.1					
	🖳 IPSec	1	8.1					
	🚇 IPSec (Offline request)	1	7.1					
	Rerberos Authentication	2	110.0					
	🖳 Key Recovery Agent	2	105.0					
	Response Signing	3	101.7					
	RAS and IAS Server	2	101.0					
	Root Certification Authority	1	5.1					
	Router (Offline request)	1	4.1					
	🗷 Smartcard Logon	1	6.1					
	🖳 Smartcard User	1	11.1					
	Representation Authority	1	5.1					
	🖳 Trust List Signing	1	3.1					
	🖉 User		31					
	🖳 User Signature Only	Duplicate Template	.1					
	🖳 Web Server	All Tasks >	.1					
	Representation Authentication	Properties	01.0					
< >>	<	Help	>					

3. Select **Windows Server 2008** for both Certification Authority and Certificate recipient under **Compatibility Settings**, Click **OK**.

셴		Certific	ate Templa	tes Consoli	e		
File Action View Help							
Certificate Templates (WIN-AA7	Template D	Prope	rties of Nev	v Template	×	Actions	
	Adminis	Trope	rues of rues			Certificate Templates (WI	N-AA74
	Authent Subje	st Name	Server	Issuance	e Requirements	More Actions	1200202020200000
	Basic EF Supe	seded Templates	s E	tensions	Security	() and () and () and ()	
	Compati	ulity Gener	ral Requ	est Handling	Cryptography	Administrator	
	CEP Eng	late ontions avai	lable are based	on the earliest	operating system	More Actions	
	Coure Sil	set in Compatibilit	y Settings.	on the composition.	oporating operatin		
	Comput						
	Cross C	resulting change	s				
	Director						
	Domain Compa	bility Settings					
	Domain C-vo	and a state of					
		ation Authority					
	Wind Enrollm	ows Server 2008		*			
	Enrollm Certifie	nate recipient					
	Exchance Free	de recipion	teres.	-			
	Wind Wind	ows XP / Server	2003	Y			
	Rechand	ows XP / Server	2003				
	IPSec Wind	ows 7 / Server 2	038 R2				
	IPSec (C	ows 87 Windows	Server 2012				
	Rerhero						
	Rev Rec						
	OCSP R. These se	ttings may not pro	event earlier op	erating systems	from using this		
	RAS and template.		Maria 20020001				
	Root Ce						
	Router						
	R Smartca						
	🗐 Smartca	OK	Canaal	Applu	Hala		
	R Subordi	UN	Cancer	Арру	treih		
	I Test Administrator		4		100.3 🗸	-	
ш	< III				>		
						1*	

4. On the Resulting Changes menu click OK.

Тар	Template Option
Request Handling	For automatic renewal of smart card certificates, use the existing key if a new
Cryptography	Use alternate signature format
Cryptography	Key Storage Provider

5. Go to the General tab and enter a name for the template (UserKeyArchival).

6. Go to the **Request Handling** tab and enable the **Archive subject's encryption private key** check box.

Subject Nan	ne S	erver	Issuance	Requirements
Supersedec	d Templates	E	tensions	Security
Compatibility	General	Requ	est Handling	Cryptography
^o urpose:	Signature and	d encryptio	n	~
	Delete rev	oked or ex	nired certificates	(do not archive)
	Include syr	nmetric alg	orithms allowed	by the subject.
	Archive su	biect's enc	votion private k	ev
	- NE			
-				
Allow private	e key to be expo	orted		
Allow private	e key to be expo	orted		
Allow private	e key to be expo the same key (orted		
✓ Allow private ☐ Renew with ☐ For automat	e key to be expo the same key (ic renewal of sm	orted ') hart card ce	rtificates, use th	ne existing key if a
✓ Allow private Benew with For automat new key car	e key to be expo the same key (ic renewal of sm nnot be created	orted ') hart card cr	rtificates, use th	ne existing key if a
✓ Allow private ☐ Renew with ☐ For automat ☐ new key car	e key to be expr the same key (ic renewal of sm nnot be created	orted ') hart card ce	rtificates, use th	ne existing key if a
Allow private Benew with For automat new key car Do the following	the same key (the same key (ic renewal of sm nnot be created a when the subi	orted ') aart card co ect is en roi	rtificates, use th	ne existing key if a
Allow private Renew with For automat new key can Do the following sesociated with	the same key to be expo the same key (ic renewal of sm nnot be created g when the subj this certificate i	orted ') hart card co ect is enrol s used:	rtificates, use the	ne existing key if a ne private key
Allow private Benew with For automat new key car to the following associated with	e key to be expr the same key (ic renewal of sm nnot be created g when the subj this certificate i	orted ") hart card ce ect is enrol s used:	ntificates, use the	ne existing key if a ne private key
Allow private Renew with For automat new key car to the following ssociated with Enroll subject	the same key (the same key (ic renewal of sm not be created g when the subj this certificate i ct without requir	orted ") hart card ce ect is enrol s used: ing any use	rtificates, use th ed and when th r input	ne existing key if a ne private key
✓ Allow private Renew with For automat new key car the following issociated with Enroll subject Enroll subject	the same key (the same key (ic renewal of sm nnot be created g when the subj this certificate ct without requir	orted ') aart card or ect is enrol s used: ing any use	rtificates, use th ed and when th r input	ne existing key if a ne private key
Allow private Benew with For automat new key car oo the following ssociated with Enroll subjec Prompt the t	a key to be expo the same key (ic renewal of sm nnot be created g when the subj this certificate st without requir user during enro	orted) hart card co ect is enrol s used: ing any uso liment	ntificates, use th ed and when th r input	ne existing key if a ne private key
Allow private Renew with For automat new key cai bo the following sssociated with Enroll subjee Prompt the to Prompt the to private key i	the same key (the same key (ic renewal of sm nnot be created g when the subj this certificate is this certificate st without requir user during enro is used	onted) aart card ci s used: ing any usi Ilment Ilment and	rtificates, use th ed and when th r input require user inp	ne existing key if a ne piivate key ut when the

- 7. Select the Subject Name tab.
- 8. Uncheck the Include e-mail name in subject name check box.
- 9. Uncheck the E-mail name check box.



10. Click Apply and then OK.

Add a new template to CA for issuing

- 1. Open the command prompt and run the **certsrv.msc** command.
- 2. Right-click the Certificate Templates node.
- 3. Select New -> Certificate Template to Issue.

		Hanne		Laboration Difference in the	
Certification d di noida-D Revo Issue Peno Faile Certi	n Authonity (Local) 1-CA ed Certificates ed Certificates ding Requests d Requests Gente Tomolates	Nam Re	e y Recovery Agent	Intended Purpose Key Recovery Agent	
	Manage	_	Cartificate Template to Issue	-	
	View		Vertice and the considered in the		
	Refresh Export List				
	Help				

4. Select new template for key archival, click **OK**.

En En	able Certificate Templates	x
Select one Certificate Template to enable Note: If a certificate template that was rec information about this template has been re All of the certificate templates in the organ For more information, see <u>Certificate</u>	on this Certification Authority. ently created does not appear on this list, you may need to wait until eplicated to all domain controllers. ization may not be available to your CA. <u>Template Concepts.</u>	
Name	Intended Purpose	
🚇 Router (Offline request)	Client Authentication	
💀 Smartcard Logon	Client Authentication, Smart Card Logon	
🚇 Smartcard User	Secure Email, Client Authentication, Smart Card Logon	
🚇 Test Administrator	Client Authentication, Secure Email, Encrypting File System, N	,
🚇 Trust List Signing	Microsoft Trust List Signing	
🚇 User Signature Only	Secure Email, Client Authentication	
🚇 UserKArchival	Client Authentication, Secure Email, Encrypting File System	
🚇 UserKeyArchival	Client Authentication, Secure Email, Encrypting File System	
Workstation Authentication	Client Authentication	
		\mathbf{r}
<		
	OK	el 🗌

Issue a user template with key archival enabled

- 1. Open the command prompt and run the certmgr.msc command.
- 2. Right-click Personal node.
- 3. Select All Tasks -> Request New Certificate.



- 4. Click Next
- 5. Click Next.

6. Select the new template for key archival check box and click Enroll.



7. The Enrollment Wizard UI displays. Verify the enrollment is successful.

Certificate Installation Res	ults	
Active Directory Enrollment P	en enrolled and installed on this computer.	
🗹 UserKArchival	V STATUS: Succeeded	Details

8. Click Finish.

Perform Key Recovery

You can recover archived keys. To perform a key recovery:

- 1. Log on to the system as Domain Administrator and ensure that the private key is still recoverable by viewing the Archived Key column in the Certification Authority console.
 - a. Log on as Domain Administrator.
 - **b.** From Administrative Tools, open Certification Authority.
 - c. In the console tree, double-click CA, and then click Issued Certificates.
 - d. From the View menu, click Add/Remove Columns.
 - e. In Add/Remove Columns, in Available Column, select Archived Key, and then click Add. Archived Key should now appear in Displayed Columns.
 - f. Click OK and then, in the details pane, scroll to the right and confirm that the last issued certificate to UserKeyArchival has a Yes value in the Archived Key column.

NOTE: A certificate template must have been modified so that the Archive bit and Mark Private Key as Exportable attributes were enabled. The private key is only recoverable if there is data in the Archived Key column.

- g. Double-click the Archive User certificate.
- h. Click the Details tab.

Write down the serial number of the certificate. (Do not include spacing between digit pairs.) This is required for recovery.

The serial number is a hexadecimal string which is 20 characters long. The serial number of the private key is the same as the serial number of the certificate. For the purpose of this walkthrough, the serial number will be referred to as **serialnumber**.

- i. Click OK.
- j. Close Certification Authority.
- 2. Recover the private key into a BLOB output file by using certutil.exe.
 - a. On the taskbar, click the **Start** button, click **Run**, type **cmd**, then click **OK** to open command prompt window.
 - **b.** Type **cd** \ and then press **ENTER**.
 - c. Ensure that you are in the c:\ directory.
 - d. At the command prompt, type:

Certutil -getkey serialnumber outputblob

e. At the command prompt, type

dir outputblob

NOTE: If the file outputblob does not exist, you probably typed the serial number incorrectly for the certificate.

The outputblob file is a PKCS#7 file containing the KRA certificates and the user certificate and chain. The inner content is an encrypted PKCS#7 containing the private key (encrypted by the KRA certificates).

- 3. Recover the original private/public key pair using Certutil.exe
 - a. On the taskbar, click the **Start** button, click **Run**, type **cmd**, and click **OK** to open a command prompt window.
 - **b.** At the command prompt, type:

Certutil -recoverkey outputblob user.pfx

c. When prompted, enter the following information:

Enter new password: password

Confirm new password: password

- d. Type exit, and then press ENTER.
- e. Close all windows and log off as the current user.
- 4. Import the recovered private key/certificate.
 - a. At the command prompt, type certmgr.msc
 - b. Right click Certificates (Current User), and then click Find Certificates.
 - c. In Find Certificates, under Contains, type CA Name and then click Find Now.
 - d. In Find Certificates, on the Edit menu, click Select All.
 - e. In Find Certificates, on the File menu, click Delete.
 - f. In Certificates, click Yes.
 - g. Close Find Certificates.
- **5.** Import the certificate at c:\user.pfx and let the certificates be placed by the system.
 - a. In the console tree, right-click **Personal** and then click **All Tasks** and then click **Import**.
 - b. In the Certificate Import Wizard, click Next.
 - c. On Files to Import, in the File name box, type c:\user.pfx, and then click Next.
 - d. In Password, type password and then click Next.
 - e. On Certificate Store, click Automatically select the certificate store based on the type of certificate and then click Next.
 - f. On Completing the Certificate Import Wizard, click Finish.
- 6. Verify the serial number of the imported certificate.
 - a. In the console tree, double-click **Personal** and then click **Certificates**.
 - b. Double-click certificate.
 - c. In Certificate, go to the Details tab. Verify that the serial number matches the original.

This completes the key recovery process when your key recovery keys are in Luna HSMs.

Microsoft Certificate Services Integration using Luna HSM for signing keys has been completed now as we have secured the CA signing keys and CA recovery keys on Luna HSMs.

Migrating CA keys from Microsoft Software Key Storage Provider to SafeNet Key Storage Provider

This chapter outlines the steps to migrate a CA signing key from Microsoft software storage to the Luna HSM or Luna Cloud HSM service on Windows Server using the Ms2luna utility for both CSP and KSP.

Configure SafeNet 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 using a Luna HSM, the KSP package must be installed during the Luna Client software installation. If using Luna Cloud HSM service, the KSP package is included in the service client package inside of the **/KSP** folder.

- 1. Navigate to the KSP installation directory.
- 2. Run the KspConfig.exe (KSP configuration wizard).
- 3. Double-click Register Or View Security Library on the left side of the pane.

N	- SafeNet-Inc Key Storage Provider, Config Wizard	_ D X
File Help		
- SafeNet KSP Config - Register Or View Security Library - Register HSM Slots		

4. Browse the library cryptoki.dll from Luna Network HSM Client installation directory and click **Register**.

81	- SafeNet-Inc Key Storage Provider, Config Wizard	_ 🗆 X
File Help		
SafeNet KSP Config Register Of View Security Library Register HSM Slots	LibraryPath C:1Program FilestSafeNettLunaClienttcryptoki.dll Browse	

- File
 Help

 B: SafeNet KSP Config
 Register Or View Security Library

 Register Or View Security Library
 LibraryPath

 C1Program Files\SafeNetULunaClienteryptoki.dll
 Browse

 Register
 Success

 Success registering the security library!
 OK
- 5. On successful registration, a message "Success registering the security library" displays.

- 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, a message "The slot was successfully and securely registered" displays.

51	- SafeNet-Inc Key Storage Provider, Config Wizard	_ 🗆 X
File Help		
BareNet KSP Config Register Or View Security Library Register HSM Slots	Register For User Domain Administrator NOIDA Available Stots Stot Password 1 part1 	Register By Slot Label C Slot Number
	Registered Slots SlotLabel:part1 The slot was successfully and securely registered! OK	Register Slot
		Delete Registered Slot
8	- SafeNet-Inc Key Storage Provider, Config Wizard	_ 🗆 X
---	--	--
Sile Help Image: SafeNet KSP Config Image: SafeNet KSP Config Image: Register Or View Security Library Register HSM Slots	- SafeNet-Inc Key Storage Provider, Config Wizard Register For User SYSTEM Available Slots Slot Password part1 Success Registered Slots	Register By Slot Label Slot Number Register Slot View Registered Slots
	Registered Slots SlotLabel:part1 The slot was successfully and securely registered! OK	Delete Registered Slot
Ready		

9. You need to register the same slot for NT AUTHORITY\SYSTEM.

NOTE: Both slots have been registered, despite only one entry appearing for the service in the **Registered Slots** section of the KSP interface.

Back up the CA

You can enable and configure the location where the CA backup files will be stored using the Active Directory certificate services management console. To back up the CA:

- 1. Click the **Start** button, click **Run**, type **certsrv.msc**, and then click **OK**.
- 2. Select the CA node in the left pane. On the Action menu, click All Tasks and then Backup CA.

📮 certsrv - [Certi	ication Auth	ority (Local)\lu	natest-ADC	S-CA]	
File Action View Help					
♦ ♦ 2 0 4 6 10 10 10 10 10 10 10 10 10 10 10 10 10					
Certification Authority (Local) Name					
All Tasks	Start Ser	vice			
View +	Stop Ser	/ice			
Refresh	Submit r	ew request			
Export List	Back up	CA			
Properties	Restore	CA			
Help	Renew C	A Certificate			

3. Click **Next** on the Welcome page of the CA backup wizard.

4. Select the **Private key and CA certificate** check box and provide a directory name where the system will temporarily store the CA certificate and optionally the key. Click **Next**.

Certification Authority Backup Wizard
Items to Back Up You can back up individual components of the certification authority data.
Select the items you wish to back up: Image: Private key and CA certificate Image: Certificate database and certificate database log Image: Perform incremental backup Back up to this location: C:\Users\Administrator.LUNATEST\Desktop Browse Note: The backup directory must be empty.
< Back Next > Cancel Help

- 5. Provide a password to protect the CA key and click Next.
- 6. Click Finish.

Migrate a MS CA onto a Luna HSM or Luna Cloud HSM service using ms2Luna

The Keys stored in the Software is not secure and can be compromised anytime. So to enforce operational and logical security of the CA it is required to be migrated onto HSM. Also migration ensures that the same key created in previous section is used for verification of CA. To migrate a MS CA onto a Luna HSM using ms2Luna:

- **1.** Copy the CA certificate thumbprint.
- 2. Open a command prompt and run ms2Luna.exe from "<SafeNet HSM Client installation Directory>/KSP directory" in case of KSP registration.

NOTE: You need to register a slot using KSP before migrating MSCA to Luna HSM.

3. Enter the Thumbprint of CA certificate when prompted, and press Enter.



4. Verify that CA provider changes to SafeNet Key Storage Provider.

Console1 - [Console Root\Certification Authority (Local)\lunatest-ADCS-CA]	_ 🗆 X
🖀 File Action View Favorites Window Help	- 6 ×
Console Root Name	Actions
A Cetification Authority (Local) Revoked Cetificates	lunatest-ADCS-CA
lunatest-ADCS-CA Properties ? X	More Actions
Extensions Strange Certificate Managers Enclineer Agents Auding Recovery Agents Security General Policy Module Ext Module Ext Module	
Certification authority (CA)	
Nate: Under-NUSCA	
Centrade #0 View Centrade View Centrade Cystographic settings Provider: Self-ext Key Stange Provider Hadh signthm: SH4/256	
OK Cancel Apply Help	

- 5. Restart the CA services and after restarting CA services will use the keys from Luna HSM for signing new certificate request and verify the already signed certificates.
- Now you can restore the CA certificate database that you have backed up before migration. To restore the CA database follow the steps to <u>Restore MS CA</u>.

In case if CA Services are not restarting even after CA keys are migrated to Luna HSM using ms2luna then uninstall the CA services and follow the instructions to Install Microsoft Active Directory Certificate Services on Windows Server using SafeNet Key Storage Provider with migrated key.

Install Microsoft Active Directory Certificate Services on Windows Server using SafeNet Key Storage Provider with migrated key

To install the Microsoft Active Directory Certificate Services software:

- 1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
- 2. Open Server Manager under Configure this Local Server and click Add Roles and Features.
- 3. The Add Roles and Features Wizard displays.
- 4. On the Before you Begin page click Next.
- 5. Select the Role-based or feature-based installation radio button and click Next.

	Add Roles and Features Wizard	
elect installatic	on type	DESTINATION SERVER D1.noida.com
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	 Select the installation type. You can install roles and featmachine, or on an offline virtual hard disk (VHD). Role-based or feature-based installation Configure a single server by adding roles, role service Remote Desktop Services installation Install required role services for Virtual Desktop Infra or session-based desktop deployment. 	itures on a running physical computer or virtual es, and features. istructure (VDI) to create a virtual machine-based

6. Select the Select a server from the server pool radio button and from Server Pool select your server.

alact dactionti				DESTINATION SERVI
elect desunati	on server			D1.noida.co
Before You Begin	Select a server or a vir	rtual hard disk on which	to install roles and features.	
Installation Type	Select a server fro	m the server pool		
Server Selection	O Select a virtual har	rd disk		
Server Roles	Server Pool			
Features				
	Filter:			
	Name	IP Address	Operating System	
	D1.noida.com	172.25.11.92	Microsoft Windows Server 20	12 Standard
	1 Computer(s) found			
	This page shows serve	ers that are running Wir	dows Server 2012, and that have	been added by using
	Add Servers comman collection is still incor	d in Server Manager. Of nolete are not shown.	fline servers and newly-added se	rvers from which data

- 7. Click Next.
- 8. Select the Active Directory Certificate Services check box from the Server Roles.

	Add Roles and Features Wizard	-
Select server ro Before You Begin Installation Type Server Selection Server Roles Features	Select one or more roles to install on the selected server. Roles Active Directory Certificate Services Active Directory Domain Services C Active Directory Federation Services	DESTINATION SERVER D1.noida.com Description Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue
	Active Directory Lightweight Directory Services Active Directory Rights Management Services Application Server DHCP Server DNS Server Fax Server File And Storage Services (Installed) Hyper-V Network Policy and Access Services	and manage certificates used in a variety of applications.
	Print and Document Services Remote Access Remote Desktop Services	Install Cancel

 A window stating "Add features that are required for Active Directory Certificate Services?" displays. To add a feature, click Add Features.



10. Click Next twice to continue until the Role Services options are displayed.

Calast and Calasta and Calasta and Calasta		
Features	ver. Description	
INET Framework 3.5 Features INET Framework 4.5 Features (Installed) Background Intelligent Transfer Service (BITS) BitLocker Drive Encryption BitLocker Network Unlock BranchCache Client for NFS Data Center Bridging Enhanced Storage Fallover Clustering Group Policy Management Ink and Handwriting Services Internet Printing Client IP Address Management (IPAM) Server Torket Storage	 .NET Framework 3.5 combin power of the .NET Framework APIs with new technologies building applications that of appealing user interfaces, pr your customers' personal idd information, enable seamles secure communication, and the ability to model a range business processes. 	es the k 2.0 for fer otect entity s and provid of
	INET Framework 3.5 Features Image: Net Framework 4.5 Features (Installed) Image: Background Intelligent Transfer Service (BITS) Image: BitLocker Drive Encryption BitLocker Drive Encryption BitLocker Network Unlock Image: BranchCache Client for NFS Data Center Bridging Enhanced Storage Failover Clustering Group Policy Management Ink and Handwriting Services Internet Printing Client IP Address Management (IPAM) Server	Features Description Image: NET Framework 3.5 Features (Installed) Image: NET Framework 3.5 combine power of the .NET Framework 2.5 combine power of the .NET Framework 3.5 combine power of the .NET Framework 2.5 combine power of the .NET Framework 3.5 combine power of the .NET Framework 3.5 combine power and the sublempt of the ability to move and the power set to combine power set to combine power and the set to combine power and the ability to model a range business processes. Data Center Bridging Enhanced Storage Failover Clustering Enhanced Storage

11. Select the **Certification Authority** check box from the **Role services** list and click **Next**.

b	Add Roles and Features Wizard	×
Select role serv Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Select the role services to install for Active Directory Certificat Role services Certification Authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder	DESTINATION SERVER D1.noida.com ate Services Description Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.
	< Previous Ne	et Install Cancel

12. Verify that the role you are about to install is appropriate and click **Install**.

tion selections	DESTINATION SERVE D1.noida.co
To install the following roles, role services, or features on select Restart the destination server automatically if required Optional features (such as administration tools) might be displa been selected automatically. If you do not want to install these their check boxes. Active Directory Certificate Services Certification Authority Bemote Server Administration Tools	ted server, click Install. ayed on this page because they have optional features, click Previous to cle
Role Administration Tools Role Administration Tools Active Directory Certificate Services Tools Certification Authority Management Tools	
	To install the following roles, role services, or features on select Restart the destination server automatically if required Optional features (such as administration tools) might be displuteen selected automatically. If you do not want to install these their check boxes. Active Directory Certificate Services Certification Authority Remote Server Administration Tools Role Administration Tools Active Directory Certificate Services Tools Certification Authority Management Tools Restriction Authority Management Tools

13. Once installation is complete, click the link **Configure Active Directory Certificate Services on the destination server** it opens AD CS Configuration wizard.

6	Add Roles and Features Wizard	
Installation pro	DESTINATION SERVER D1_noida.com	
Before You Begin Installation Sype Server Selection Server Roles	View installation progress Feature installation Configuration required. Installation succeeded on D1.noida.com.	
Features AD-CS Role Services Confirmation Results	Active Directory Certificate Services Additional steps are required to configure Active Directory Certificate Services on the destination server Configure Active Directory Certificate Services on the destination server Certification Authority Remote Server Administration Tools Role Administration Tools Active Directory Certificate Services Tools Certification Authority Management Tools	
	You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details. Export configuration settings	
	< Previous Next > Close Cancel	

14. On the Credentials page of AD CS Configuration wizard, click Next to continue.

1	AD CS Configuration	×
Credentials		DESTINATION SERVER D1.noida.com
Credentials Role Services Confirmation Progress Results	Specify credentials to configure role services To install the following role services you must belong to the local Admin	istrators group:
	< Previous Nex 2	Configure Cancel

- **15.** Select the **Certification Authority** check box and click Next.
- 16. Select the Enterprise CA radio button and click Next.
- 17. Select the Root CA radio button and click Next.
- 18. Proceed to setup the **Private Key** for CA to generate and issue certificates to clients. Select **Use** existing private key and Select an existing private key on this computer. Click Next to continue.

DESTINATION SERVE
D1.noida.com
Specify the type of the private key
To generate and issue certificates to clients, a certification authority (CA) must have a private key.
O Create a new private key
Use this option if you do not have a private key or want to create a new private key.
Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.
Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.
Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to
use a private key from an alternate source.
More about Private Key

19. Click **Change...** Select the **SafeNet Key Storage Provider** algorithm that you used to generate the private keys. Clear the CA Common name. Click **Search**.

E	AD CS Configuration		_ 🗆 X
Existing Ke	зу	DEST A	TINATION SERVER DCS.lunatest.com
Credentials Role Services Setup Type CA Type	Select an existing key Change Cryptographic Provider Search for keys on the target computer using the following criteria:	eys available on the target com teria.	puter matching
Private Key Existing Key Cryptograp CA Name Validity Perio Certificate Data Confirmation	Cryptographic provider: RSA#SafeNet Key Storage Provider Type certification authority (CA) common name (optional): lunatest-ADCS-CA Search Cancel	vare Key Storage Provider	Change
Progress Results	Allow administrator interaction when the priv More about Existing Key	vate key is accessed by the CA.	e Cancel

20. Select the existing key and click Next. Select the Allow administrator interaction when the private key is accessed by the CA check box.

b	AD CS Configuration	_ D ×
Existing Key	DEST	INATION SERVER DCS.lunatest.com
Credentials Role Services Setup Type CA Type Private Key Existing Key	Select an existing key Select a key from the list. The listed keys are the keys available on the target comp the search criteria. You may change the search criteria. Search criteria for key Cryptographic provider: RSA#SafeNet Key Storage Provider	puter matching
Cryptography CA Name Validity Period Certificate Database	CA common name: lunatest-ADCS-CA Search results:	Change
Confirmation Progress Results	Iunatest-ADCS-CA ✓ Allow administrator interaction when the private key is accessed by the CA.	
	More about Existing Key < Previous	2 Cancel

21. Select the **Hash Algorithm** for signing certificates issued by this Certificate Authority and key length settings for your installation.

a	AD CS Configuration	_ D X
Cryptography for	CA	DESTINATION SERVER ADCS.lunatest.com
Credentials	Specify the cryptographic options	
Role Services		
Setup Type	Select a hash algorithm for signing certificates issued by this certificate	tion authority (CA).
CA Type	Cryptographic provider:	
Private Key	RSA#SafeNet Key Storage Provider	
Existing Key		
Cryptography	Hash algorithm:	
CA Name	SHA256	
Validity Period	SHA504 =	
Certificate Database	SHA1	
Confirmation	· ·	
Progress		
Results		
	More about Cryptography	
	< Previous Next >	Configure Cancel

- 22. Click Next to continue.
- 23. Configure a common name to identify this Certificate Authority. Click Next to continue.

a	AD CS Configuration	_ □ X
CA Name		DESTINATION SERVER ADCS.lunatest.com
Credentials	Specify the name of the CA	
Role Services		
Setup Type	Type a common name to identify this certification authority (CA). This	s name is added to all
СА Туре	certificates issued by the CA. Distinguished name suffix values are au be modified.	tomatically generated but can
Private Key		
Existing Key	Common name for this CA:	
Cryptography	lunatest-ADCS-CA	
CA Name	Distinguished name suffix:	
Validity Period	DC=lunatest,DC=com	
Certificate Database	Preview of distinguished name:	
Confirmation	CN=lunatest-ADCS-CA,DC=lunatest,DC=com	
Progress		
Results		
	More about CA Name	
	< Previous Next >	Configure Cancel

24. Proceed to set the Certificate Validity Period. Click Next to continue.

b	AD CS Configurati	on 📃 🗖 👗
Validity Period		DESTINATION SERVER D1.noida.com
Credentials Role Services Setup Type	Specify the validity period Select the validity period for the certifica	e generated for this certification authority (CA):
CA Type	5 Years 💌	
Private Kev	CA expiration Date: 4/30/2018 11:44:00 P	M
Cryptography CA Name	The validity period configured for this CA certificates it will issue.	certificate should exceed the validity period for the
Validity Period		
Certificate Database		
Confirmation		
Progress		
Results		
	More about Validity Period	
	< Pre	vious Next Configure Cancel

25. Configure the **Certificate Database**. It records all the certificate requests, issued certificates, and revoked or expired certificates. Click **Next** to continue.

	AD CS Configuration	
CA Database		DESTINATION SERVER D1.noida.com
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation	Specify the database locations Certificate database location: C:\Windows\system32\CertLog Certificate database log location: C:\Windows\system32\CertLog	
Progress Results	More about CA Database	Configure

26. Click **Configure** to configure the selected roles, role services, or features.

27. Click Close to exit the AD CS Configuration wizard after viewing the installation results.

After successful installation, the CA certificate database needs to be restore which you have backed up before beginning the key migration.

Restore MS CA

You can restore a backed-up MS CA database account. To restore an MS CA:

- 1. Click the Start button, click Run, type certsrv.msc, and then click OK.
- 2. Select the CA node in the left pane.
- 3. On the Action menu, click All Tasks and then Restore CA.

ia cert	srv - [Certification Authority (Local)\lunatest-ADCS-CA]
File Action View Help Image: Second s	
Certification Authority (Local)	Name
All Tasks	Start Service
View 🕨	Stop Service
Refresh	Submit new request
Export List	Back up CA
Properties	Restore CA
Help	Renew CA Certificate

- 4. Click Next on the Welcome page of the CA Restore wizard.
- 5. Select the **Certificate database and certificate database log** check box and provide a directory name where you want to temporarily store the CA certificate and optionally the key. Click **Next**.

Certification Authority Restore Wizard	x
Items to Restore You can restore individual components of the backup file.	I
Select the items you want to restore: Private key and CA certificate Certificate database and certificate database log	
Restore from this location: C:\Users\Administrator.LUNATEST\Desktop Browse Note: For incremental restores, first select the full backup file and complete the wize Then re-run the wizard, selecting subsequent incremental backup files.	ard.
< Back Next > Cancel	Help

6. Enter password to protect the CA key and click Next.

- Corten/ If artification Authority (Local) Junatoet Au
Certification Authority Restore Wizard
Provide Password For encryption and decryption of messages, both a public key and a private key are required. You must provide the password for the private key.
This password is required to gain access to the private key and the CA certificate file.
Password:
To maintain private key security, do not share your password.
< Back Next > Cancel Help

- 7. Click Finish.
- 8. The "Do you want to start Active directory certificate services" window displays. Click Yes.



9. Verify that Active Directory Services has been successfully restarted.

🗔 cert	tsrv - [Certification Authority (Local)\lunatest-ADCS-CA]	_ 🗆 X
File Action View Help		
🗢 🏟 🙍 🗐 🕼 🌾		
Certification Authority (Local)	Name Revoked Certificates Pending Requests Failed Requests Certificate Templates	

This completes the CA keys migration from Microsoft Key Storage Provider to SafeNet Key Storage Provider which uses Luna HSM for accessing the CA keys when CA Services needs the keys.

Installing and Configuring the CA cluster using SafeNet Key Storage Provider

The following sections describe the installation and configuration of a CA on a failover cluster running on Windows Server. Register SafeNet Luna KSP using KSPConfig.exe. (Refer to the <u>Configure the</u> <u>SafeNet HSM Key Storage Provider</u> section.)

Set up the CA server role on the first cluster node

This section explains how to install certificate services on the first cluster node. To setup the CA server role on the first cluster node:

- 1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
- The steps to install the Microsoft Active Directory Certificate Services are same as the <u>Install Active</u> <u>Directory Certificate Services</u> section. After Microsoft AD CS is successfully installed on first node, continue with the below steps.
- 3. Click the Start button, point to Run, type certsrv.msc, and then click OK.
- 4. Select the CA node in the left pane.
- 5. On the Action menu, click All Tasks and then Backup CA.
- 6. Click **Next** on the Welcome page of the CA backup wizard.
- 7. Select **Private key and CA certificate** and provide a directory name where you will temporarily store the CA certificate and optionally the key. Click **Next**.

	Certification Authority Backup Wizard
ltems Y	to Back Up ou can back up individual components of the certification authority data.
S	elect the items you wish to back up:
V	Private key and CA certificate
Б	Certificate database and certificate database log Perform incremental backup ack up to this location;
C	:\Backup Browse
N	ote: The backup directory must be empty.

- 8. Provide a password to protect the CA key and click **Next**.
- 9. Click Finish.

Ce	rtification Authority Backup Wizard	×
	Completing the Certification Authority Backup Wizard	
Self.	You have successfully completed the Certification Authorit Backup wizard	y
	You have selected the following settings: Private Key and CA Certificate	
	< III 3	2
	To close this wizard and begin backup, click Finish,	
	Kenter Ke	elp

NOTE: You will receive a warning message that the private key cannot be exported. This is expected behavior because the private key will never leave the Luna HSM.

10. Click OK to continue.

NOTE: You need to run the *ksputil.exe* utility to migrate keys to the cluster. Please contact Customer Support, in case you do not have the ksputil.exe utility.

11. Create a cluster key for second node using existing key as the keys generated by KSP is bound with the system on which they are generated. Creating the cluster key will duplicate the CA key and bind the same key with second node.

12. Run the ksputil.exe utility to make the keys visible to the secondary node in the cluster. You will be prompted to enter the partition password.

ksputil clusterKey /s <slotNum> /n <CA_Name> /t <TargetHost_Name>

Where,

slotNum – slot number

CA_name - name of the CA

TargetHost_Name – FQDN of the second node

Note: This steps is need to be executed for each node if you have more nodes in your cluster and bind all your nodes with the same CA key to access the key from each node when these nodes will be part of your AD CS Cluster.

	Administrator: Gommand Prompt
10	
C:\Program Files CA /t D2.noida.c	\SafeNet\LunaClient\KSP>ksputil.exe clusterKey /s 1 /n noida-D1 com
This Servers Hos ENOIDA	t Name is: D1.noida.com and the logged on user is: Administrator
Enter challenge	for slot '1' :*******
Successfully mig blic key: 119	rated CA key to host: "D2.noida.com" with private key: 27 and pu
C:\Program Files	<pre>\SafeNet\LunaClient\KSP></pre>

13. Click the Action menu, All Tasks and then Stop Service.

NOTE: After the successful migration of keys to the second node, the CA service must be shut down to unlock the disk resources.

14. Close the CA management snap-in.

To detach the shared storage form the cluster node

1. Go to the Server Manager MMC snap-in. Click the File and Storage Services. Click Disks, select shared disk resource, right click on it and select Take Offline.

ē.		Serve	r Manager	r.	100	- • ×
\mathbf{E}	🔊 🕶 😽 Volum	nes • Disks		🕝 🚩 Manage	Tools	View Help
	Servers Volumes Disks Storage Pools Shares iSCSI	DISKS All disks 2 total Filter Number Virtual Disk DI (2) 0 1	Status Online Onlin	P (■) ▼ (R) Capacity Unallocated 127 GB 0.00 B New Volume	Partition MBR GPT	TASKS Read Only
		C Last refreshed on 5/1/	W 2013 11:34:2	Bring Online Reset Offine Reset Disk		>
		VOLUMES	_	STORAGE PO	OL	~

To release the HSM from the cluster node

- 1. Since Luna HSM is a network attached HSM, therefore disable the network connection to release it from cluster node one.
- **2.** Logoff from the first node.

The installation of the Certification Authority on the first node is completed now.

Set up the CA server role on the second cluster node

This section explains how to set up the second cluster node. If you have more than two cluster nodes you need to follow the steps for each cluster node.

To install the CA on the second node, complete the following tasks:

Configure the secondary cluster node:

- Log on to the cluster node with a user having permissions to install the second cluster node. To install
 an enterprise CA, logon with enterprise admin permissions to the Active Directory domain. To install a
 standalone CA you may logon with local admin permissions if you don't want to register the CA in the
 Active Directory configuration container.
- 2. Click the Start button open Run, type servermanager.msc, and click OK.
- 3. The Server Manager MMC snap-in opens. Click the File and Storage Services. Click Disks.
- 4. Ensure that the shared disk that is used for the CA is online.

- 5. Copy the previously exported CA certificate to the second cluster node.
- 6. Click the Start button, point to Run, type mmc, and then click OK.
- 7. From the File menu, click Add/remove Snap-in...
- 8. Select Certificates from the list of available snap-ins and click Add.
- 9. Select the **Computer Account** radio button and click **Next**.
- 10. Select the Local Computer radio button and click Finish.
- 11. Click OK.

Import an existing CA certificate

- 1. In the Certificate Manager MMC snap-in, expand the Certificates (Local Computer) node and select the Personal store.
- 2. From the Action menu click All Tasks and then Import ...

-		Console1 - [Console Ro	oot\Certificates (Local Computer)\Personal]	X
🚡 File	Action View Favorites Window	Help		_ 8 ×
🗢 🔿	Find Certificates		-	
Cons	All Tasks 🕨 🕨	Find Certificates		Actions
4 🙀 C	New Window from Here	Request New Certificate	p items to show in this view.	Personal
	New Taskpad View	Import		More Actions 🕨
	Refresh	Advanced Operations	•	
	Export List			
Þ 🗹	Help			
	Third-Party Root Certification			
₽ 🖬	Client Authentication Issuers			
▶ 🛄	Remote Desktop			
	Trusted Devices			
15.1	 Transferences and sources areas 			

3. In the Certificate Import Wizard, click Next.

4. Enter the filename of the CA certificate that was previously created on the first node and click **Next**. If you use the Browse button to find the certificate, change the file type to *Personal Information Exchange* **pfx*,*.*p12*).

Specify the file you want to import.	
File name:	
C:\Backup\noida-D1-CA.p12	Browse
Note: More than one certificate can be store Personal Information Exchange- PKCS #1 Cryptographic Message Syntax Standard- Microsoft Serialized Certificate Store (.SS	ed in a single file in the following format: 2 (.PFX,.P12) - PKCS #7 Certificates (.P7B) T)
arn more about certificate file formats	

5. Type the password previously used to protect the private key. The password is required even if there is no private key in the PFX file. Click **Next.**

NOTE: Do not select the Mark this key a	as exportable check box.
---	--------------------------

riva	te key protection
1	To maintain security, the private key was protected with a password.
	Type the password for the private key.
	Password:
	••••••
	Display Password
	Import options:
	Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
	Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
	Include all extended properties.

6. Select the Place all certificates in the following store radio button and select the **Personal** certificate store.



- 7. Click Next.
- 8. Click Finish to import the certificate.
- 9. Click **OK** to confirm the successful import.
- 10. Repair the association between the certificate and the private key that is stored in the HSM.
- 11. In the Certificate manager, expand the **Personal** store and select the **Certificates** container.
- 12. Select the imported certificate and select Open from the Action menu. Go to the Details tab.
- 13. Select the field Serial Number and copy the serial number into the clipboard. Click OK.



14. Open the command prompt and type certutil -repairstore My "{Serial number}" and press Enter.



Add the AD CS role

- 1. Open Server Manager under Configure this Local Sever and click Add Roles and Features.
- 2. The Add Roles and Features Wizard displays.
- 3. Click Next.
- 4. Select the Role-based or feature-based installation radio button and click Next.

	Add Roles and Features Wizard	
Select installati	on type	DESTINATION SERVER D2.noida.com
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	 Select the installation type. You can install roles and features on a runnin machine, or on an offline virtual hard disk (VHD). Role-based or feature-based installation Configure a single server by adding roles, role services, and features. Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to or session-based desktop deployment. 	ig physical computer or virtual
	< Previous Net >	Install

5. Select the Select a server from the server pool radio button and from Server Pool select your server.

B	Add R	oles and Features \	Wizard
Select destinati	on server		DESTINATION SERVER D2.noida.com
Before You Begin Installation Type Server Selection Server Roles Features	Select a server or a vir Select a server from Select a virtual har Server Pool Filter:	tual hard disk on which n the server pool d disk	to install roles and features.
Results	Name D2.noida.com	IP Address 172.25.11.99	Operating System Microsoft Windows Server 2012 Standard
	1 Computer(s) found This page shows serve Add Servers command collection is still incon	ers that are running Wir d in Server Manager. Of uplete are not shown.	dows Server 2012, and that have been added by using the fline servers and newly-added servers from which data
		< Pre	rvious Nert> Install Cancel

- 6. Click Next.
- 7. Select the Active Directory Certificate Services check box from the Server Roles.

	Add Roles and Features Wizard	
Before You Begin Installation Type Server Selection Server Roles Features Confirmation	Select one or more roles to install on the selected server. Roles Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Lightweight Directory Services	DESTINATION SERVE D2noida.co Description Active Directory Certificate Service (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
	Active Directory Rights Management Services Application Server DHCP Server DNS Server Fax Server Fax Server Fax Server Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services	variety of applications.
	Remote Desktop Services	

8. The Add features that are required for Active Directory Certificate Services window will appear. To add a feature, click the Add Features button.

- 9. Click Next to continue.
- 10. Click Next to continue.

elect features		DESTINATION SERV D2.noida.co
Before You Begin Installation Type	Select one or more features to install on the selected server. Features	Description
Server Selection Server Roles Features AD CS Role Services Confirmation Results		.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provid the ability to model a range of business processes.

11. Click **Next** to continue.

ctive Directory	y Certificate Services	DESTINATION SERVER D1_noida.com
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Active Directory Certificate Services (AD CS) provides the o such as secure wireless networks, virtual private networks, Access Protection (NAP), encrypting file system (EFS) and s Things to note: • The name and domain settings of this computer cannot (CA) has been installed. If you want to change the comp server to a domain controller, complete these changes to information, see certification authority naming.	ertificate infrastructure to enable scenarios Internet Protocol Security (IPSec), Network smart card log on. be changed after a certification authority uter name, join a domain, or promote this before installing the CA. For more
	Active Directory Certificate Services Overview	

12. Select the Certification Authority check box from the Role services list and click Next.

	Add Roles and Features Wizard	
Select role serv Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Select the role services to install for Active Directory Certifice Role services	DESTINATION SERVER D2.noida.com Description Certification Authority (CA) is used to issue and manage certificates, Multiple CAs can be linked to form a public key infrastructure.
	< Previous N	ext>

13. Click Install.



14. Once installation is complete, click the link **Configure Active Directory Certificate Services on the destination server** the AD CS Configuration wizard displays.

k	Add Roles and Features Wizard	_ _ ×
Installation pro	gress	DESTINATION SERVER D2.noida.com
Before You Begin Installation Type Server Selection Server Roles	View installation progress Feature installation Configuration required. Installation succeeded on D2.noida.com.	_
Features ADICS Role Services Confirmation Results	Active Directory Certificate Services Additional steps are required to configure Active Directory Certificate Services <u>Configure Active Directory Certificate Services on the destination server</u> Certification Authority Remote Server Administration Tools Role Administration Tools Active Directory Certificate Services Tools Certification Authority Management Tools	vices on the destination
	You can close this wizard without interrupting running tasks. View task page again by clicking Notifications in the command bar, and then Tas Export configuration settings	c progress or open this sk Details.
	< Previous Next >	Close Cancel

To configure the AD CS Role

1. On the Credentials page of the AD CS Configuration wizard click Next to continue.



2. Select the Certification Authority check box and click Next.

	AD CS Configuration	
ole Services		DESTINATION SERVER D2.noida.com
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Certificate Request Certificate Database Confirmation Progress Results	Select Role Services to configure	
	More about AD CS Server Roles	

3. Select Enterprise CA as Setup Type and click Next.

6	AD CS Configuration - D
Credentials Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Certificate Request Certificate Database Confirmation Progress Results	AD CS Configuration
	More about Setup Type < Previous Next > Configure Cancel

4. Select Root CA as type of CA and click Next.



5. Select the Use existing private key radio button and choose the option Select a certificate and use its associated private key and click Next.



6. Select the CA certificate that was generated on the first node and click Next.

Tim.	AD CS Configuration	= • ×
Existing Certific	ate	DESTINATION SERVER D2.noida.com
Credentials Role Services Setup Type CA Type Private Key	Select an existing certificate for the CA To use a private key associated with a certificate, select that certifica certificate if it is not available on the target computer. The selected of will be used for this certification authority (CA). Certificates:	ite. You may have to import a certificate and its properties
Existing Certificate	Subject Issued By Expiration Date	Import
Continuation Progress Results	noida-D1-CA 5/1/2018	Properties
	Allow administrator interaction when the private key is accessed	by the CA.
	More about Existing Certificate	
	< Previous Next >	Configure Cancel

7. Change the default paths for the database log location. Click **Next** to continue.

ř.	AD CS Configuration	- - X
CA Database		DESTINATION SERVER D2.noida.com
Credentials Role Services Setup Type	Specify the database locations	
CA Type	E:\	
Private Key Existing Certificate	Certificate database log location:	
Certificate Database Confirmation Progress Results	More about CA Database	
	< Previous Mext >	Configure Cancel

8. A dialog box displays stating that an existing database was found displays, click **Yes** to overwrite.

9. On the Confirmation page click **Configure**.

a	AD CS Con	figuration		- 6	3	×
Credentials Credentials Role Services Setup Type CA Type Private Key Existing Certificate Certificate Database Confirmation Progress Results	AD CS Con To configure the following roles Active Directory Certificat Certification Authority CA Type: Allow Administrator Interaction: Certificate Validity Period: Distinguished Name: Certificate Database Location: Certificate Database Log Location:	figuration , role services, or features, click Configure. ce Services Enterprise Root Disabled 5/1/2018 11:39:39 PM CN=noida-D2-CA,DC=noida,DC=com E:\ E:\	DESTINATI D	ION SI	ERVE da.co	X ER m
		< Previous Next > Co	infigure	Car	ncel	

- 10. Click **Close** to finish the **Role** installation.
- **11.** Log off from the second cluster node.

Set up the Failover Cluster feature on the cluster nodes

Repeat the following steps on each node of the cluster nodes:

- 1. Log on to the cluster node with local administrator permissions.
- 2. Open Server Manager under Configure this Local Sever and click Add Roles and Features.
- 3. The Add Roles and Features Wizard displays.
- 4. Click Next.
- 5. Select the Role-based or feature-based installation radio button and click Next.

6. Select the Select a server from the server pool radio button option and from Server Pool select your server.

elect destinati	on server			DESTINATION SERVER D2.noida.com
Before You Begin Installation Type Server Selection	Select a server or a vir Select a server from Select a virtual har	tual hard disk on which n the server pool d disk	to install roles and features.	
Server Roles Features Confirmation	Server Pool			
	Name	IP Address	Operating System	
	D2.noida.com	172.25.11.99	Microsoft Windows Server 20	12 Standard
	1 Computer(s) found	us that are supping Win	dowe Server 2012 and that have	heen added by using t
	Add Servers command collection is still incon	d in Server Manager. Of plete are not shown.	fline servers and newly-added se	rvers from which data

7. Click Next twice. From the list of available features, select the Failover Clustering check box and click Next.

Coloct footuror			DESTINATION SERVER
Before You Begin Installation Type	Select one or more features to install on the selected ser Features	ver.	D2.noida.com
Server Selection Server Roles Features Confirmation Results	INET Framework 3.5 Features INET Framework 4.5 Features (Installed) Background Intelligent Transfer Service (BITS) BitLocker Drive Encryption BitLocker Network Unlock BranchCache Client for NFS Data Center Bridging Enhanced Storage		.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
	Failover Clustering Group Policy Management Ink and Handwriting Services Internet Printing Client IP Address Management (IPAM) Server	>	

- 8. A pop up displays stating Add features that are required for Failover Clustering, click the Add Features button.
- 9. Click Next.

elect features			DESTINATION SERV D2.noida.co
Before You Begin Installation Type	Select one or more features to install on the selected se Features	rver.	Description
Server Selection Server Roles Features Confirmation Results	 INET Framework 3.5 Features. INET Framework 4.5 Features (Installed) Background Intelligent Transfer Service (BITS) BitLocker Drive Encryption BitLocker Network Unlock BranchCache Client for NFS Data Center Bridging Enhanced Storage 	<	Failover Clustering allows multiple servers to work together to provid high availability of server roles. Failover Clustering is often used fo File Services, virtual machines, database applications, and mail applications.
		~	

10. Click Install.

i.	Add Roles and Features Wizard	
Confirm install	ation selections	DESTINATION SERVER D2.holda.com
Before You Begin Installation Type Server Selection Server Roles	To install the following roles, role services, or features on selected services. Restart the destination server automatically if required Optional features (such as administration tools) might be displayed on been selected automatically. If you do not want to install these optional their check boxes.	er, click Install. this page because they have al features, click Previous to clear
Features Confirmation	Failover Clustering	
Results	Feature Administration Tools Failover Clustering Tools Failover Cluster Management Tools Failover Cluster Module for Windows PowerShell	
	Export configuration settings Specify an alternate source path	
	< Previous Next >	Install

11. Click Close.

	Add Roles and Features Wizard	X
Installation pro	gress	INATION SERVER D2.noida.com
Before You Begin Installation Type Server Selection Server Roles	View installation progress Feature installation Installation succeeded on D2.noida.com.	
Features Continuation Results	Failover Clustering Remote Server Administration Tools Feature Administration Tools Failover Clustering Tools Failover Cluster Management Tools Failover Cluster Module for Windows PowerShell	
	You can close this wizard without interrupting running tasks. View task progress page again by clicking Notifications in the command bar, and then Task Details. Export configuration settings	or open this
	< Previous Next > Close	Cancel

Create a Failover Cluster

To create a Failover Cluster:

- 1. Log on to the cluster node where the shared storage is attached and available.
- 2. Open Server Manager, Click Tools and select Failover Cluster Manager. From the Action menu, click Create a Cluster.

調査	Failover Cluster Manager	X
File Action View Help		
Failover Cluster Manager	Failover Cluster Manager	Actions
	Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.	Failover Cluster Manager W Validate Configuration Create Cluster Connect to Cluster View Refresh Properties Help
	More Information Falover cluster concess on the Web Falover cluster communities on the Web Microsoft support page on the Web Microsoft support page on the Web	

- 3. On the Before You Begin page, click Next.
- 4. Enter the cluster node name (computer name) of the first cluster node in the Enter Server Name field and click Add.
- 5. Enter the cluster node name of the second cluster node in the Enter Server Name field and click Add.
- 6. Click **Next** to continue.
- 7. Enter the Cluster Name and click Next until you reach the Summary page. .

	Create Cluster Wizard
Access P	Point for Administering the Cluster
Before You Begin Select Servers Administering the Cluster Confirmation Creating New Cluster Summary	Type the name you want to use when administering the cluster. Cluster Name: ClusterADCS The NetBIOS name is limited to 15 characters. One or more DHCP IPv4 addresses were configured automatically. Image: The NetBIOS name is limited to 15 characters. One or more DHCP IPv4 addresses were configured automatically.
	< Previous Cancel

8. Verify the cluster configuration is appropriate and click **Finish**.

3		Create Cluster Wizard	
Summary	У		
Before You Begin Select Servers	You have such	cessfully completed the Create Cluster Wizard.	
Access Point for Administering the Cluster		Create Cluster	^
Confirmation			
Creating New Cluster			
Summany	Cluster:	ClusterADCS	
	Node:	D2.noida.com	
	IP Address:	DHCP address on 172.25.11.0/24	
	2222		~
	Warnings		
	To view the report crea	ated by the wizard, click View Report.	View Report
	I o close this wizard, c	lick Finish.	
			Finith

Configure AD CS Failover Cluster

You need to configure an AD CS Failover configuration for certificate services. To configure the AD CS failover cluster:

1. In the Failover Cluster Management snap-in, right-click Role and select Configure Role.

		Fa	ailover Cluster Manager	_ 0	x
File Action	View Help				1
(n 📫 🖄 🖬					
Failover Clust	ter Manager Cluste	r ClusterADCS.noida.com		Actions	
⊿ 間 ClusterAE	DCS.noida.com			ClusterADCS.noida.com	*
⊳ Ne	Configure Role	ummary of Cluster Cluster	ADCS	lo Configure Role	
🛛 🞑 Sti	Virtual Machines	sterADCS has 0 clustered roles and 2 r	nodes.	Walidate Cluster	
	Create Empty Role	IsterADCS.noida.com	Networks: Cluster Network 1	📲 View Validation Report	
Þ 🏐 Ne	Refresh	- ost Server: D2	Subnets: 1 IPv4 and 0 IPv6	🍄 Add Node	
E CI	Help	ster Events: None in the last hour	r i	🔑 Close Connection	
10				Reset Recent Events	
	A Co	nfigure		🛃 More Actions	•
	Config	jure high availability for a specific clustered	role, add one or more servers (nodes), or migrate services and	View	•
	applic	ations from a cluster running Windows Serv	ver 2012, Windows Server 2008 H2, or Windows Server 2008.	🔯 Refresh	
		Unique hole		Properties 🛛	
		alidate Liuster	Understanding cluster validation tests	🔢 Help	
		dd Node	Adding a server to your cluster	Name: ClusterADCS	
		ligrate Roles	Migrating a cluster from Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008.	Ra Bring Online	
		Juster-Aware Updating	Applying software updates to the nodes in the cluster	🚮 Take Offline	
				Show Critical Events	
	▲ Navigate		More Actions		
	E E	toles	Nodes Nodes	Properties	
	💽 S	torage	Networks	👔 Help	
	2 5	luster Events			
	- Ch	uster Core Resources			
	Name		Status		
	Cluste	er Name Name: ClusterADCS	(Daline		
		NUME CASICIANS	O Olimo		

2. On the Before you Begin page, click Next.



3. From the role list, select Generic Service and click Next.

Before You Begin	Select the role that you want to configure for high available	ailability:	
Select Hole Select Service	BES Mamaanaga Sarvar		Description
Client Access Point	DHCP Server	Â	You can configure high availability for
Select Storage	Distributed Transaction Coordinator (DTC)	=	some services that were not originally
Replicate Registry Settings	File Server Generic Application		information, see <u>Configuring Generic</u> Applications, Scripts, and Services
Confirmation	Generic Script		
Configure High	Ceneno Service		
Availability	GriscSI Target Server	×	
Summary			a 1 D0
	More about roles that you can configure for high avail	lability	

4. From the service list, select Active Directory Certificate Services and click Next.

9 7	High Availability	/ Wizard	
to Select	ervice		
Before You Begin Select Role	Select the service you want to use from the list		1100
Select Service	Name	Description	^
Client Access Point Select Storage Replicate Registry Settings Confirmation Configure High Availability Summary	Application Experience Application Host Helper Service Application Identity Application Information Application Layer Gateway Service Application Management ASP.NET State Service Background Intelligent Transfer Service	Processes application compatibility cache requ Provides administrative services for IIS, for exa Determines and verifies the identity of an applic Facilitates the running of interactive application Provides support for 3rd party protocol plug-ins f Processes installation, removal, and enumeratio Provides support for out-of-process session stat Transfers files in the background using idle net	
		< Previous Nyst > Cancel	
5. On the Client Access Point page enter the service name in the **Name** field and click **Next**.

80	High Availability Wizard
Client Ac	ccess Point
Before You Begin Select Role Select Service	Type the name that clients will use when accessing this clustered role: Name: SfntCLustGen
Client Access Point Select Storage Replicate Registry Settings Confirmation Configure High Availability Summary	The NetBIOS name is limited to 15 characters. One or more DHCP IPv4 addresses were configured automatically. All networks were configured automatically.
	<

6. Select the disk storage that is still mounted to the node and click Next.

Hig	gh Availability \	Wizard		X
orage				
Select only the storage volu You can assign additional st	mes that you want to orage to this clustere	assign to this clustered role. d role after you complete this wizard.		
Name	Status			
🕑 🖽 📺 Cluster Disk 1	T Unline			
		< Previous Ne	Cancel	
	Select only the storage volu You can assign additional st Name ☑ ഈ Cluster Disk 1	Select only the storage volumes that you want to You can assign additional storage to this clustere Name Status Maine Cluster Disk 1 Online	Select only the storage volumes that you want to assign to this clustered role. You can assign additional storage to this clustered role after you complete this wizard. Name Status T B Cluster Disk 1 Online	Select only the storage volumes that you want to assign to this clustered role. You can assign additional storage to this clustered role after you complete this wizard. Name Status I I Cluster Disk 1 O Online

7. Configure a shared registry hive, click the Add button, enter "SYSTEM\CurrentControlSet\Services\CertSvc" and click OK.

80 81	High Availability Wizard
Replicate	e Registry Settings
Before You Begin Select Role Select Service Client Access Point Select Storage Replicate Registry Settings Confirmation Configure High Availability Summary	Programs or services may store data in the registry. Therefore, it is important to have this data available on the node on which they are running. Specify the registry keys under HKEY_LOCAL_MACHINE that should be replicated to all nodes in the cluster. SYSTEM\CurrentControlSet\Services\CertSvc Add Modify
	Kervious Cancel

8. Click **Next** on the Confirmation page.

81	Н	igh Availability Wizard	X
tonfirma	tion		
Before You Begin Select Role	You are ready to configure	high availability for a Generic Service.	
Select Service Client Access Point Select Storage Replicate Registry Settings Confirmation Configure High	Service: Storage: Network Name: OU: IP Address: Registry Key: Parameters:	Active Directory Certificate Services (CertSvc) Cluster Disk 1 SfntCLustGen CN=Computers,DC=noida,DC=com DHCP address on 172.25.11.0/24 SYSTEM\CurrentControlSet\Services\CertSvc This Generic Service has no startup parameters.	~
Availability Summary	To continue, click Next.		*
		< Previous Next C	Cancel

- 9. Click **Finish** to complete the failover configuration for certificate services.
- **10.** Open the Failover Cluster Manager and verify that the newly created service's **Status** is in the **Running** state.

Roles (1)					
Search			PQue	eries 🔻 🔛 💌	•
Name	Status	Туре	Owner Node	Priority	lr
G SfntCLustGen	(1) Running	Generic Service	D2	Medium	
<	101				
10					-
Y StritCLust	Gen		Preferred	i Owners: Any n	ode
Status:	Running				
Priority:	Medium				
Owner Node:	D2				

Create CRL objects in the Active Directory

The default AD permissions for the CA cluster do not permit publishing the CRL into the Active Directory. Alternatively, the user can create a CRL container to publish the CRL into the Active Directory.

You must use the certutil command with the –f option to create the CRL container. To create CRL objects in the Active Directory:

- 1. Log on to the active cluster node with enterprise permissions.
- 2. Click the Start button, point to Run, type cmd, and then click OK.
- 3. At the command line, type cd %WINDIR%\System32\CertSrv\CertEnroll and press Enter.

4. To publish the CRL into Active Directory, type certutil -f -dspublish {CRLfile}.



Modify CA configuration in Active Directory

The AIA object in Active Directory stores the CA's certificate. You can enable both the cluster nodes to update the CA certificate when required.

You can perform the following tasks from any computer in your Active Directory configuration where the Active Directory Sites and Services snap-in and ADSIEDIT is installed. To modify the CA configuration in the Active Directory:

- 1. Log on to the computer with enterprise permissions.
- 2. Click the Start button, point to Run, type dssite.msc and then click OK.
- 3. Select the top node in the left pane. In the View menu, select the Show services node.
- 4. In the left pane, expand the Services and Public Key Services and select AIA.

2	Active Directo	ry Sites and Sei	rvices	_ D X
File Action View Help				
🕨 🔿 🙍 🔚 🖾 🛸				
 Active Directory Sites and Services Services Claims Configuration Group Key Distribution S Microsoft SPP Microsoft SPP NetServices Public Key Services AIA COP Certificate Template; Certification Authori Enrollment Services KRA OID 	Name noida-D1-CA noida-WIN-AA,74V0SV	Type certificationAu certificationAu	Description	

- 5. In the middle pane, select the CA name as it shows in the **Certification Authority** MMC snap-in.
- 6. From the Action menu select Properties. Click the Security tab and select Add....

- 7. Click Object Types and select the Computers check box and click OK.
- 8. In the Enter the object names to select field enter the computer name of the second cluster node. Click OK.

Jsers, Computers, Groups, or Built-in security principals Object Types from this location: holda.com Locations inter the object names to select (examples): D2I Check Name	Select this object type:	
rom this location: noida.com Locations inter the object names to select (<u>examples</u>): D2I Check Name	Users, Computers, Groups, or Built-in security principals	Object Types.
noida.com Locations inter the object names to select (<u>examples</u>): D2 Check Name	From this location:	
inter the object names to select (<u>examples</u>): D2	noida.com	Locations
D2i Check Name	Enter the object names to select (examples):	
	D2	Check Names
		-11
	02	Check Nan

- 9. Ensure that the computer accounts of both the cluster nodes have Full Control permissions.
- 10. Click OK.
- **11.** In the left pane, select **Enrollment Services**.

(1) 9	Active Di	rectory Sites and	d Services	_ 0 X
File Action View Help				
🍬 🏟 🙍 📻 🗶 🖬 🖉 🗟				
Active Directory Sites and Servic	Name	Туре	Description	
 Sites Services Claims Configuration Group Key Distribution S Microsoft SPP Microsoft SPP MetServices Public Key Services AIA CDP Certificate Template: Certificate Template: Certificate Autori Enrollment Services KRA CIS RRAS Windows NT 	norda-D1-CA	pKIEnrolime	et	
<				

- **12.** In the middle pane, select the CA name.
- 13. From the Action menu, select Properties click the Security tab and select Add....

- 14. Click Object Types and select the Computers check box and click OK.
- **15.** In the **Enter the object names to select** field enter the computer name of the second cluster node. Click **OK**.

Select this object type:		
Users, Computers, Groups, or Built-in security print	sipals	Object Types
From this location:		
noida.com		Locations
Enter the object names to select (examples):		
D2		Check Names
		11
2007/00/00/00/00/00/00/00/00/00/00/00/00/		(P 1

- 16. Ensure that the computer accounts of both the cluster nodes have Full Control permissions.
- 17. Click OK.
- **18.** In the left pane, select **KRA**.

a R	Active Directo	ry Sites and Se	rvices	_ _ ×
File Acting View Help				
Active Directory Sites and Servic Sites	Name Monda-D1-CA	Type msPKI-Private	Description	
 Services Claims Configuration Group Key Distribution S Microsoft SPP MismqServices Public Key Services AIA CDP Certificate Templates Certification Authorit Enrollment Services KRA OlD RRAS Windows NT 	noida-WIN-AA74VOSV	msPKI-Private		
				1

- **19.** In the middle pane, select the CA name.
- 20. From the Action menu select Properties click the Security tab and select Add....

21. Click Object Types and select the Computers check box and click OK.

Object Types	? ×
Select the types of objects you want to find. Object types:	
Built-in security principals Service Accounts Service Accou	
	K Cancel

22. Type the computer name of the second cluster node as object name and click OK.

Select this object type:	
Users, Computers, Groups, or Built-in security principals	Object Types
From this location:	
noida.com	Locations
Enter the object names to select (<u>examples</u>):	
D2i	Check Names
	1 1 1 1

- 23. Verify that the computer accounts of both the cluster nodes have Full Control permissions.
- 24. Click OK.
- **25.** Close the Sites and Services MMC snap-in.

This completes the creation of ADSC cluster with 2 cluster nodes using the keys secured on the Luna HSMs.

Migrating AD CS Cluster keys from Microsoft Software KSP to SafeNet KSP

This section explains the procedure for migrating the CA Keys used by the AD CS from the Microsoft Software Key Storage Provider to the SafeNet Key Storage Provider. After the migration is completed, the AD CS cluster will use the CA signing keys stored in the Luna HSM.

Before initiating the migration process, ensure that:

- > The AD CS Cluster is currently operational using the Microsoft Software Key Storage Provider.
- > The Luna Client is installed and a partition is registered on each node of the cluster.
- > The SafeNet KSP is registered and configured on every node of the cluster.

For migrating the AD CS Cluster from Microsoft KSP to SafeNet KSP, the CA key must be associated with the SafeNet KSP on each node of the cluster. The steps for performing the migration process are outlined below.

1. Log on to the first node of the cluster and ensure that the AD CS Cluster service is running and owned by the first cluster node where the CA keys were initially generated.



 Navigate to the Resources tab, select Active Directory Certificate Services, and then click on Remove in the Actions pane to remove the AD CS service from the cluster. When prompted, click Yes to remove the service.

👪 Failover Cluster Manager							- X
File Action View Help							
🗢 🄿 🙍 📰 🚺 🖬							
📲 Failover Cluster Manager	Roles (1)						Actions
EYHSM-Cluster.EYHSM.cor	Search				🔎 Queries 🔻	. • •	Roles
Nodes	Name	Status	Туре	Owner Node	Priority	Information	lonfigure Role
> 🧾 Storage	EYHSM-CA-Clust	Running	Generic Service	DC	Medium		Virtual Machines
Networks							📸 Create Empty Role
							View
							Refresh
						-	👔 Help
	Remove Ge	meric Service			×		Active Directory Certificate Services
	- AI	e vou sure vou w	ant to remove A	ctive Directory	Certificate		🙀 Bring Online
	Se Se	ervices?		,			🙀 Take Offline
							👪 Information Details
				Vec	No		Show Critical Events
				Tes	140		More Actions
							🗙 Remove
	<					>	Properties
	Y 🏠 EYHSM-CA4	Clust			Preferred Owners	Any node	🛛 Help
	Name			Status	Information	^	
	Roles						
	Active Directory C	ertificate Services		(1) Online			
	Storage						
	🕀 📇 Cluster Disk 2			Online			
	Server Name						
	Name: EYHSM-C	A-Clust		(🔹 Online		>	
< >	Summary Resources						

- 3. Launch the Certificate Authority snap-in from the Administrative Tools menu.
- Before proceeding with the backup of the existing CA database and keys, ensure that CA certificate services are running. If the services are not running, start them before proceeding with the backup process.
- 5. Select the CA in the Certificate Authority, and then click on Action in the menu bar. From there, select All Tasks and then choose Back up CA... to initiate the backup process.

둵 ce	ertsrv -	[Certifica	ation Auth	ority	(Local)\EYHSM-CA]	
File	Actio	n View	Help			
← ■ ↓ 0		All Tasks > Refresh Export List Properties			Start Service Stop Service Submit new request Back up CA Restore CA	
		•			Renew CA Certificate	

6. Open the **Certificate Authority Backup Wizard** and follow the steps provided by the wizard to create a backup of the CA certificate database. When prompted to select a directory for the backup, make sure to choose an empty directory.

Items to Back Up	up Wizard	n authoritu data					
Tou can back up individual components of the certification authority data.							
Select the items you wish	h to back up:						
Private key and CA c	certificate						
Certificate database a	and certificate database log mental backup						
Back up to this location:							
C:\CA Backup		Browse					
, Note: The backup direct	ory must be empty.						

- 7. Follow the steps provided by the wizard to complete the backup process and then click on the **Finish** button to close the wizard.
- 8. In the certificate authority snap-in, select the CA-Name, then click on the Action menu and then click Properties. This will open the CA Properties window where you can view the current provider and CA Name. Next, click on View Certificate and when the certificate is displayed, click on Details. In the Field section click Thumbprint.

Take note of the certificate Thumbprint and CA-Name, as you will need them later when migrating the key.

For example:

CA-Name: EYHSM-CA

Certification Authority (Loca j j EYH5M-CA	Name Revoked Centificates Issued Cantificates Pending Requests Fieled Requests	
	EYHSM-CA Properties ? ×	Certificate X
	Ennore Sunge Carlos Reage Enterter Spen Auto Reamy Earth San Main State Reading Auto Carlos Auto Ream Balance Cardinat References Main State References	General (100 Gesthaten-halt) Preti data Frett Version State (100 Gesthaten-halt) Frett Version State (100 Gesthaten-halt) Character (100 Gesthaten-halt)
	Crystoyrabitic settings Provider: Microsoft Sothware Key Storage Provider Hash algottim: SH4256	Batt Proverties. Capy to File
	OF Court And Ha	OK

9. Close the Certificate and Properties window by clicking the OK button twice.

10. Open the command prompt and run the below command to find the unique key container. Take note of the container name as you will need it later when migrating the keys to Luna HSM. For example:

certutil -verifystore my <CA Certificate Thumbprint>



11. Go to the KSP folder of Luna Client and open the command prompt. Run the ms2luna command and provide the CA certificate thumbprint when prompted to migrate the CA key.



12. Ensure that CA service provider is now set to SafeNet Key Storage Provider. You can confirm this in two ways. First, check the CA Service Properties window in the Certificate Authority snap-in. Alternatively, you can use the following command to verify the store:

certutil -verifystore My <CA Certificate Thumbprint>

Make sure to replace <CA_Certificate_Thumbprint> with the thumbprint of the certificate for which you migrated the key using the "ms2luna" command. Check that the Unique container name and Provider have been changed accordingly.

C:\Program Files\SafeNet\LunaClient\KSP>certutil -verifystore my da205e29cb1e1ebaebc50dbe4458e0443baa769a my "Personal"
Certificate 0
Serial Number: 7753a9d82dccedbc41c6f204cd5e2cc5
Issuer: CN=EYHSM-CA, DC=EYHSM, DC=com
NotBefore: 3/17/2023 3:13 PM
NotAfter: 3/17/2028 3:23 PM
Subject: CN=EYHSM-CA, DC=EYHSM, DC=com
Certificate Template Name (Certificate Type): CA
CA Version: V0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Template: CA, Root Certification Authority
Cert Hash(sha1): da205e29cb1e1ebaebc50dbe4458e0443baa769a
Key Container = EYHSM-CA
Unique container name: 7b48bdd9-3032-43bc-88fb-50680e620f43
Provider = SafeNet Key Storage Provider
Private key is NOT plain text exportable
Encryption test passed
Verified Issuance Policies: All
Verified Application Policies: All
Certificate is valid
CertUtil: -verifystore command completed successfully.
C:\Program Files\SafeNet\LunaClient\KSP>

13. Ensure that the output shows **Encryption test passed.** If the command output does not show the association of CA certificate with the key migrated to Luna HSM, run the Repair store command.

```
certutil -repairstore -csp "SafeNet Key Storage Provider" My
<CA Certificate Thumbprint>
```

Replace <CA_Certificate_Thumbprint> with the thumbprint of the CA certificate.

14. Ensure that AD CS services are running correctly after the key migration by stopping and then restarting the services.

🙀 certsrv - [Certification Authority (Local)]									
File Action View Help									
(= =]									
Certification Authority (Local)	Name J EYHSM-CA	Description Certification Authority							

15. Use the ksputil utility to create a key for all the other nodes in the AD CS Cluster. Provide the partition password when prompted.

ksputil clusterKey /s <SlotNum> /n <CA_Name> /t <TargetCluster_Host>
Where.

<SlotNum> : Luna HSM partition slot id

<CA_Name>: Name of the CA

<TargetCluster_Host>: Fully qualified domain name of cluster node

Note: You must create a key for every node in the cluster. The above command will duplicate the same key and associate it with the cluster node so that each node has access to the same key.



16. Log in to the other cluster nodes and associate the CA certificate with the key migrated and created in the HSM for that particular node.

Note: Ensure to create key for every node in the cluster.

17. Open the command prompt and run the following command to check that the CA certificate is initially associated with Software Key Storage Provider:

certutil -verifystore My <CA Certificate Thumbprint>

The thumbprint must be the same on all the nodes of the cluster because the cluster is using the same key and certificate for each node. From the output of the command note the **Unique key container** which contains the key.



18. Go to the C:\ProgramData\Microsoft\Crypto\Keys directory and locate the Unique key container associated with the CA certificate. Right-click on container and select Delete to delete the key container.

Note: Ensure that you are deleting the correct key container that matches the Unique Key Container from the previous step.

📕 🗹 📕 🖛	Keys						-	
File Home	Share	View						
$\leftarrow \rightarrow \star \uparrow$	📕 > Thi	is PC > Local Disk (C:) > ProgramData > Microsoft > Crypto > Keys			ٽ ~	Search Keys		
🛨 Quick acces		Name		Date modified	Туре	Size		
	, ,	597367cc37b886d7ee6c493e3befb421_7063a7b6-8af0-4d7e-a122-cb7d22e49bda		3/13/2023 8:13 PM	System file		3 KB	
		a7a766fc7fe7bbc77d7e87c8f3016943_7063a7b6-8af0-4d7e-a122-cb7d22e49bda		3.47.0003 3.00 BL4	<u> </u>		2 KB	
Download	s ∦°	b6d44b4eff160d7ca7a49950252db12e_7063a7b6-8af0-4d7e-a122-cb7d22e49bda	le Sh	hare			3 KB	
🛅 Document	s ≉	ef90fba0ff65873755193041f0466ee5_7063a7b6-8af0-4d7e-a122-cb7d22e49bda	O	pen with			3 KB	
Pictures	A	f0e91f6485ac2d09485e4ec18135601e_7063a7b6-8af0-4d7e-a122-cb7d22e49bda	Re	estore previous versions	;		3 KB	
🐛 Local Disk	(C:)		Se	end to	>			
System32			Cu	ut				
🗢 This PC			Co	рру				
🧊 3D Objects	;		Cr	reate shortcut				
📃 Desktop			De	elete				
🗎 Document	s		Re	ename				
🕹 Download	s		Pr	operties				
Music			L					
Not the second s								

19. Run the repair store command below in the command prompt, to associate the CA certificate with the key migrated to Luna HSM.

```
certutil -repairstore -csp `SafeNet Key Storage Provider" My
<CA Certificate Thumbprint>
```

20. When the command is successfully completed, it will show that the Provider now points to SafeNet Key Storage Provider and Unique container name has been changed.



21. Open the registry editor and navigate to the following path:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ <CA-Name>\CSP. Then, change the value of **Provider form** Microsoft Software Key Storage Provider to SafeNet Key Storage Provider.

🔛 Registry Editor			
File Edit View Favorites Help			
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Se	ervices\CertSvc\Config	uration\EYHSM-CA\	CSP
COPUserSvc CDPUserSvc CertPropSvc CertPropSvc CertPropSvc CertSvc CertSvc CertSvc CertSvc Configuration EVHSM-CA DicyModules DolicyModules PolicyModules DolicyModules Ctt4iscsi cht4vbd CldFt CLFS CldFt CLFS ClipSVC clusDit clusDit ClusDisk	Name Name Name Name Name Name Name Name	Type REG_SZ REG_SZ REG_DWORD REG_SZ REG_DWORD REG_SZ REG_DWORD	Data (value not set) SHA256 RSA 0xffffffff (4294967295) 0x00000001 (1) Microsoft Software Key Storage Provider 0x00000000 (0) X OK Cancel

Where the <CA-Name> is the actual name of your CA.

22. Launch the Failover Cluster Manager, navigate to the Roles section and then select the cluster service. In the Actions pane, choose the Move option and then select the Best Possible Node to assign the shared disk to the node that's currently in use.

📲 Failover Cluster Manager							- 0	×
File Action View Help								
🗢 🄿 🙍 📰 🚺 🖬								
Hailover Cluster Manager	Roles (1)						Actions	
✓ 聲 EYHSM-Cluster.EYHSM.cor	Search				ρ (Queries 🔻 🕁 👻	Roles	<u>^</u>
Nodes	Name	Status	Туре	Owner Node	Priority	Information	len Konfigure Role	
> 📇 Storage	CYHSM-CA-Clust	🕥 Running	Generic Service	DR	Medium		Virtual Machines	•
Cluster Events							📑 Create Empty Role	
							View	•
							Q Refresh	
							👔 Help	
							EYHSM-CA-Clust	•
							🛟 Start Role	
							🛟 Stop Role	
							🗋 Add File Share	
	<					>	Move 😥	•
	V 🗞 EYHSM-CA-C	Just			Prefe	erred Owners: <u>Any node</u>	🔞 Change Startup Priority	•
							🚯 Information Details	
	Status:	Running					Show Critical Events	
	Priority:	Medium					🛃 Add Storage	
	Owner Node: Client Access Name:	DR EYHSM:CA:Clust					Add Resource	•
	IP Addresses:	10.164.76.83					More Actions	•
							🗙 Remove	
< >	Summary Resources						Properties	~

23. Open the certificate authority snap-in and start the CA service. When it starts successfully, ensure that provider is **SafeNet Key Storage Provider**.

certsrv - [Certification Authority	(Local)]							100		×
File Action View Help						1				
	EYHSM-CA Properties	EYHSM-CA Properties ? X								
Certification Authority (Local)	Name	Extensions	Storage	Certificate	Managers					
> 👩 EYHSM-CA	EYHSM-CA	Enrollment Agents General	Auditing Policy Modul	Recovery Agents e Ex	Security it Module					
		Certification authority	(CA)							
		Name:	EYHSM-CA							
		CA certificates:								
				View	Certificate					
		Cryptographic setting Provider: Hash algorithm:	js <mark>SafeNet Key Sto</mark> SHA256	rage Provider						
		ОК	Cancel	Apply	Help					

- 24. Perform steps 16-23 on each node of the cluster. Proceed to next step only after you have associated the CA certificate to the key on Luna HSM using SafeNet Key Storage Provider and confirmed that CA Services are active when the shared disk is connected to that node.
- 25. Log on to any node where the shared storage is available and CA services are operational.
- 26. In the Failover Cluster Manager, navigate to the Roles section and select the service. Then, click on Resources, followed by Add Resource>Generic Service.

🗟 Failover Cluster Manager							-			
<u>File Action View H</u> elp										
🗢 🔿 🙍 🖬										×
🍓 Failover Cluster Manager	Roles (1)						Actions		-	× ?
EYHSM-Cluster.EYHSM.cor	Search				P Queri	es 🔻 🕁 👻 👻	Roles	▲ ^	Search Administrative Tools	٩
Nodes	Name	Status	Туре	Owner Node	Priority	Information	len Configure Role			^
> 🧾 Storage	CA-Clust	Running	Generic Service	DR	Medium		Virtual Machines	•		
Networks							🔚 Create Empty Role			
El clase creita							View	•		
							Refresh			
							Help			
							EYHSM-CA-Clust			
							🛟 Start Role	_		
							🛟 Stop Role			
							dd File Share			
	<					>	Move	•		
		uat			Preferred (Owners: Any node	🔞 Change Startup Priority	•		
		usi			Thereared	owners. Any node	Information Details			
	Name			Status	Information	^	Show Critical Events			
	Storage			0.01			🛃 Add Storage			
	Cluster Disk 2			(1) Online			Add Resource	•	Client Access Point	
	Server Name	0.4		(a) Ontare			More Actions	•	Generic Application	
	<	Ciusi		(m) ornine		>	🗙 Remove		Generic Script	
< >	Summary Resources						Properties		Generic Service	
									More Resources >	

27. In New Resource Wizard, select Active Directory Certificate Services and follow the instructions to complete the Wizard.

🚰 New Resource W	Vizard		×
Select S	ervice		
Select Service	Select the service you want to use from the list	t	
Confirmation			_
Configure Generic	Name	Description	^
Service	Active Directory Certificate Services	Creates, manages, and removes X.509 certifica	
Summary	ActiveX Installer (AxInstSV)	Provides User Account Control validation for th	
	AllJoyn Router Service	Routes AllJoyn messages for the local AllJoyn c	
	App Readiness	Gets apps ready for use the first time a user sig	
	Application Identity	Determines and verifies the identity of an applic	
	Application Information	Facilitates the running of interactive application	
	Application Layer Gateway Service	Provides support for 3rd party protocol plug-ins f	
	Application Management	Processes installation, removal, and enumeratio	
	App X Deployment Service (App XSVC)	Provides infrastructure support for deploving St	*
		Next > Cancel	
		Next > Cancer	100

28. Navigate to the Resources section and choose Active Directory Certificate Services. Click on Properties to open the property window, select Registry Replication, and then click Add. Enter the registry value for CA services as "SYSTEM\CurrentControlSet\Services\CertSvc" and then click OK to save the changes.

Failover Cluster Manager File Action View Help							—	×
(= =) (2 II						1		
聰 Failover Cluster Manager Roles (1)		Active Directory Certificate Services Properties X				Actions		
V B EYHSM-Cluster.EYHSM.cor			General	Dependencies	Policies		Poler	•
Roles			Advanced Policies Registry Replication		<u> </u>	Bra Confinence Bala	_	
	Name	Status	Programs or services may store data in the registry. Therefore, it is		_	Configure Role		
> Storage	CA-Clust	Partially Rur	important to have this data available on the node on which they are				Virtual Machines	•
Cluster Events			should be replicated to all nodes in the cluster.				Create Empty Role	
							View	•
							Refresh	
	Re	jistry Key			×	Help		
		Re	Root registry key:				Active Directory Certificate Services	
		KEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\CertSvc				💀 Bring Online		
			OK Cancel			Take Offline		
			on outdo				🛃 Information Details	
	<				>	Show Critical Events		
	V CA-Clust					- 4-	More Actions	•
						000	🔀 Remove	
	Name	a				^	Properties	
	IP Address: 10.164.76.83		Add Edit Remove				7 Help	
							· ·	
	Roles		OK Cancel Apply					
	Active Directory Ce	rtificate Services				~		
	× × × × × × × × × × × × × × × × × × ×							
< >	Summary Resources						I	

- 29. Click OK to close the Properties window and save the settings.
- **30.** In the **Failover Cluster Manager**, go to **Roles** and select the service. Click **Stop Role** in the **Actions** pane to stop the cluster service.
- **31.** Click **Start Role** in the Actions pane to restart the cluster service. Verify that the service is starting and is running properly.

- **32.** Log in to each node of the cluster one by one and verify that the cluster services are running on each node.
- **33.** Open the **Failover Cluster Manager** and select the cluster service under **Roles**. In the **Actions** pane, click **Move** and then click **Best Possible Node**. If the cluster service starts and runs on the currently logged-in node, then everything is working properly and you have successfully migrated the CA keys from the Microsoft Provider to the Luna HSM Provider.



With the execution of the preceding steps, the migration of the failover cluster from the software provider to the Luna HSM provider has been successfully accomplished.

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 <u>Thales Customer Support</u>. 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 <u>https://supportportal.thalesgroup.com</u>, 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.