Microsoft Active Directory Certificate Services

Integration Guide



All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2012-18 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto 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.

Document Number: 007-008669-001, Rev. AA Release Date: August 2018

Contents

Pr	eface	4
Sc	ope	4
Do	cument Conventions	4
	Command Syntax and Typeface Conventions	5
	Support Contacts	6
1	Introduction	7
Ov	erview	7
0.	Third Party Application Details	
Su	pported Platforms	
	pported indication of the second s	
	Configuring SafeNet Luna HSM	
	Using SafeNet HSM in FIPS Mode	
	Provision your HSM on Demand Service	
2	Integrate SafeNet HSM with Microsoft ADCS on Windows Server	. 11
	Configuring the SafeNet Key Storage Provider (KSP)	
	Installing Microsoft ADCS on Windows Server using SafeNet KSP	14
	Enrolling the Certification Authority Certificate	
	Archiving the CA Key	
	Performing a Key Recovery	
Ins	tall and configure the CA cluster using SafeNet Key Storage Provider	
	Setting up the CA server role on the first cluster node	
	Setting up the CA server role on the second cluster node	
	Setting up the Failover Cluster feature on both the cluster nodes	57
	Creating a Failover Cluster	60
	Configuring the ADCS Failover Cluster	62
	Creating CRL objects in the Active Directory	67
	Modifying the CA configuration in Active Directory	68
3	Migrate CA keys from Microsoft Software Key Storage Provider to SafeNet Key Stora	ge
	Provider	. 72
Со	nfiguring the SafeNet KSP	72
	Backing up the CA	75
	Migrating a MS CA onto a SafeNet Luna HSM or HSM on Demand service using ms2Luna	76
	Installing Microsoft Active Directory Certificate Services on Windows Server using SafeNet Key Storag	
	Provider with migrated key Restoring an MS CA	
	Testoning an inio OA	07

Preface

This document guides security administrators through installing, configuring, and integrating Microsoft Active Directory Certificate Services (ADCS) with a SafeNet Luna HSM or an HSM on Demand service.

Scope

This document outlines the steps to integrate Microsoft Active Directory Certificate Services with SafeNet Luna HSM or HSM on Demand services.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:



NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:



CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:



WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Convention	Description		
bold	The bold attribute is used to indicate the following:		
	 Command-line commands and options (Type dir /p.) Button names (Click Save As.) 		
	• Check box and radio button names (Select the Print Duplex check box.)		
	• Window titles (On the Protect Document window, click Yes .)		
	• Field names (User Name: Enter the name of the user.)		
	• Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.)		
	• User input (In the Date box, type April 1 .)		
italic	The italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)		
Consolas	Denotes syntax, prompts, and code examples.		

Command Syntax and Typeface Conventions

Support Contacts

Contact Method	Contact Information Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA		
Address			
Phone	US International	1-800-545-6608 1-410-931-7520	
Technical Support Customer Portal	 https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in manage incidents, get the latest software upgrades, and access the Gemalto Kn Base. 		

1 Introduction

Overview

This document covers the necessary information to install, configure, and integrate Microsoft Active Directory Certificate Services (ADCS) on Windows with a SafeNet Luna Hardware Security Modules (HSM) or an HSM on Demand Service.

The Microsoft ADCS on Windows provides customizable services for creating and managing public key certificates used in software security systems employing public key infrastructure. Organizations use certificates to enhance security by binding the identity of a person, device, or service to a corresponding private key.

A server configured as a certification authority (CA) provides the management features needed to regulate certificate distribution and use. Active Directory Certificate Services is the Windows Server service that provides the core functionality for Windows Server CAs. ADCS provides customizable services for managing certificates for a particular CA and for the enterprise.

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

Using SafeNet HSMs to secure the Microsoft ADCS root 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.



NOTE: HSM on Demand services do not have access to the secure audit trail.

• Load balancing and fail-over by clustering the HSMs.

*Validation for HSMoD services in progress

Third Party Application Details

• Microsoft Active Directory Certificate Services

Supported Platforms

List of the platforms which are tested with the following HSMs:

SafeNet Luna HSM: SafeNet 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. SafeNet Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing.

The SafeNet Luna HSM on premise offerings include the SafeNet Luna Network HSM, SafeNet PCIe HSM, and SafeNet Luna USB HSMs. SafeNet Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

This integration is supported with SafeNet Luna HSM on the following operating systems:

• Windows 2016 Server

M

• Windows Server 2012R2

NOTE: If you are using Windows Server 2008 R2 you require a previous version of the SafeNet Luna HSM Integration Guide. See MicrosoftADCS_SafeNetLunaHSM_Integration Guide_RevW for more information about integrating a SafeNet Luna HSM with Microsoft ADCS on Windows Server 2008R2.



NOTE: This integration is tested with Luna Clients in HA and FIPS Mode.

SafeNet Data Protection on Demand (DPoD): It is a cloud-based platform that provides on-demand HSM and Key Management services through a simple graphical user interface. With DPoD, 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 the services that you need.

This integration is supported/verified with SafeNet DPoD on the following operating systems:

- Windows 2016 Server
- Windows Server 2012R2

Prerequisites

Before starting the integration of Microsoft ADCS with SafeNet Luna HSM or HSM on Demand Service, ensure you have completed configuring the SafeNet Luna Network HSM or provisioning HSM on Demand service as per the requirement.

Configuring SafeNet Luna HSM

Before you get started ensure you have the following:

- 1. Ensure the HSM is setup, initialized, provisioned and ready for deployment. Refer to the HSM product documentation for help.
- 2. Create a partition on the HSM that will be later used by Microsoft ADCS.

Microsoft Active Directory Certificate Services Integration Guide

3. If using a SafeNet Luna Network HSM, register a client for the system and assign the client to the partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition. Ensure that the partition is successfully registered and configured. The command to see the registered partition is:

```
<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: Follow the SafeNet Network Luna HSM documentation for detailed steps for creating NTLS connection, initializing the partitions and various user roles.

Using SafeNet HSM in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the SafeNet Luna HSM in FIPS mode, you have to make the following change in configuration file:

[Misc] RSAKeyGenMechRemap=1

The above setting redirects the older calling mechanism to a new approved mechanism when SafeNet Luna HSM is in FIPS mode.

Provision your HSM on Demand Service

This service provides your client machine with access to an HSM Application Partition for storing cryptographic objects used by your applications. Application partitions can be assigned to a single client, or multiple clients can be assigned to, and share, a single application partition.

To use the HSM on Demand Service you need to provision you application partition, starting by initializing the following roles:

- Security Officer (SO) responsible for setting the partition policies and for initialize the Crypto Officer.
- **Crypto Officer (CO)** responsible for creating, modifying and deleting crypto objects within the partition. The CO can use the crypto objects and initialize an optional, limited-capability role called Crypto User that can use the crypto objects but cannot modify them.

- Crypto User (CU) optional role that can use crypto objects while performing cryptographic operations.
 - **NOTE:** Refer to the "SafeNet Data Protection on Demand Application Owner Quick Start Guide" for procedural information on configuring the HSM on Demand service and create a service client.

The HSM on Demand Service client package is a zip file that contains system information needed to connect your client machine to an existing HSM on Demand service.

Constraints on HSM on Demand Services

Please consider the following if integrating an HSMoD service with Microsoft Active Directory Certificate Services.

HSM on Demand Service in FIPS mode

Ø

HSMoD services operate in a FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, ensure you enable the **Allow non-FIPS approved algorithms** check box when configuring your HSM on Demand service. The FIPS mode is enabled by default.

Refer to the "Mechanism List" in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Verify HSM on Demand <slot> value

LunaCM commands work on the current slot. If there is only one slot, then it is always the current slot. If you are completing an integration using HSMoD services, you need to verify which slot on the HSMoD service you send the commands to. If there is more than one slot, then use the **slot set** command to direct a command to a specified slot. You can use slot list to determine which slot numbers are in use by which HSMoD service.

Integrate SafeNet HSM with Microsoft ADCS on Windows Server

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

We recommend familiarizing yourself with Microsoft Active Directory Certificate Services. Refer to the *Microsoft ADCS Configuration* documentation for more information.

Configuring the SafeNet Key Storage Provider (KSP)

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

- If using a SafeNet Luna HSM, the KSP package must be installed during the Luna Client software installation.
- If using an HSM on Demand (HSMoD) service, the KSP package is included in the HSMoD 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 SafeNet Luna HSM Client installation directory or HSMoD 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 C:Program FilestSafeNettLunaClienttcryptoki.dll Browse		
Ready	,		- //

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

N	- SafeNet-Inc Key Storage Provider, Config Wizard	_ 🗆 X
File Help		
SafeNet KSP Config Register Or View Security Library Register HSM Slots	LibraryPath C:\Program Files\SafeNetLunaClientkryptoki.dll Browse Success X 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 Storag 	e Provider, Config Wizard	_ □ ×
File Help			
J			
□- SafeNet KSP Config Register Or View Security Library	Register For User	Domain	Register By
Register HSM Slots	Administrator 🗨	NOIDA	 Slot Label
	Available Slots	Slot Password	C Oldhumbar
	1 part1 🗨	*****	C Slot Number
	1		
			Register Slot
	Suc	cess ×	View Registered Slots
	Registered Slots		
	SlotLabel:part1 The slot was successfully a	nd securely registered!]
		ок	
	1		Delete Registered Slot
	1		Delete Registered olot
	1		
 Ready	1		

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

N	- SafeNet-Inc Key Storag	e Provider, Config Wizard	_ 🗆 X
File Help			
B 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 was successfully and successfulling and successfully and successfu		Register By Slot Label Slot Number Register Slot View Registered Slots Delete Registered Slot
Ready			

Ì

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

Installing Microsoft ADCS on Windows Server using SafeNet KSP

You must configure Microsoft ADCS to use the SafeNet Luna HSM or HSMoD service when you configure the Microsoft Certificate Authority (CA) user role.

To install Microsoft ADCS

- 1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
- 2. Ensure you have configured the SafeNet KSP. Refer to the section Configuring the 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.

elect destinati	on server			DESTINATION SERVE D1.noida.co
Before You Begin Installation Type Server Selection	Select a server or a vi Select a server fro Select a virtual ha	m the server pool	to install roles and features.	
Server Roles Féatures Confirmation	Server Pool			
Results	Name D1.noida.com	IP Address	Operating System Microsoft Windows Server	r 2012 Standard
		d in Server Manager. Of	ndows Server 2012, and that h filine servers and newly-added	

8. Click Next.

9. Select the Active Directory Certificate Services check box.

elect server rol	es	DESTINATION SERVE D1.noida.com
Before You Begin Installation Type Server Selection	Select one or more roles to install on the selected server. Roles	Description
Server Roles Features Confirmation Results	Active Directory Certificate Services Active Directory Poderation Services Active Directory Federation Services Active Directory Rights Management Services Remote Document Services Remote Desktop Services	

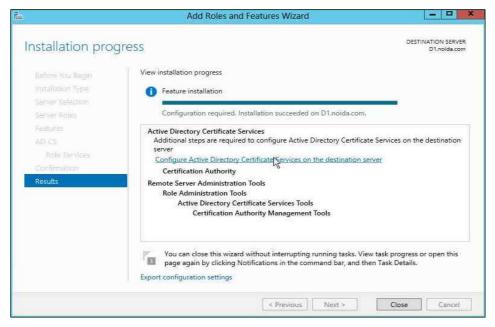
- 10. A window displays stating Add features that are required for Active Directory Certificate Services? To add a feature, click the Add Features button.
- 11. Click Next to continue.
- 12. On the Active Directory Certificate Services page click **Next** to continue.
- 13. Select the Certification Authority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

	Add Roles and Features Wizard	<u> </u>
Select role serv Before You Begin Installation Type Server Selection Server Roles Peatures AD CS Role Services Confirmation Results		DESTINATION SERVER D'Looida.com ertificate Services Description Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.
	< Previous	Nex Install Cancel

14. Click Install.

Microsoft Active Directory Certificate Services Integration Guide

15. When installation is complete, click **Configure Active Directory Certificate Services on the destination server** and the AD CS Configuration wizard displays.



- 16. On the Credentials page of AD CS Configuration wizard, click Next to continue.
- 17. Select the Certification Authority check box and click Next.

		DESTINATION SERVE
ole Services		DESTINATION SERVI
Credentials	Select Role Services to configure	
Role Services		
Setup Type	Certification Authority	
CA Type	Certification Authority Web Enrollment	
Private Key	Online Responder Network Device Enrollment Service	
Cryptography	Certificate Enrollment Web Service	
CA Name	Certificate Enrollment Policy Web Service	
Validity Period		
Certificate Database		
Confirmation		
	More about AD CS Server Roles	

- 18. Select the Enterprise CA radio button and click Next.
- 19. Select the Root CA radio button and click Next.
- 20. 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.

Microsoft Active Directory Certificate Services Integration Guide



21. 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 S	11.1.2.2.2
Credentials Role Services Setup Type	Specify the cryptographic options Select a cryptographic provider:		Key length:	
CA Type	RSA#Microsoft Software Key Storage Provider	*	2048	-
Private Key	RSA#Microsoft Software Key Storage Provider	^	5 C	
Cryptography CA Name Validity Period	Microsoft Base Cryptographic Provider v1.0 ECDSA_P521#Microsoft Software Key Storage Provider ECDSA_P256#Microsoft Software Key Storage Provider Microsoft Strong Cryptographic Provider			
Certificate Database Confirmation Progress Results	ECDSA_P256#SafeNet Key Storage Provider ECDSA_P521#SafeNet Key Storage Provider ECDSA_P384#Microsoft Software Key Storage Provider Microsoft Base DSS Cryptographic Provider RSA#Microsoft Smart Card Key Storage Provider DSA#Microsoft Software Key Storage Provider DSA#SafeNet Key Storage Provider ECDH_P384#SafeNet Key Storage Provider ECDSA_P384#Microsoft Smart Card Key Storage Provider ECDH_P256#SafeNet Key Storage Provider	 III 	y the CA.	

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

Click I	Next.	Proceed	to	step	27.
---------	-------	---------	----	------	-----

ryptography fo	or CA		D1.noida.
Credentials Role Services	Specify the cryptographic options		
Setup Type	Select a cryptographic provider:		Key length:
CA Type	ECDSA_P256#SafeNet Key Storage Provider		256
Private Key	Select the hash algorithm for signing certificates issue	ed by this CA:	
Cryptography	SHA256		
CA Name	SHA384		
Validity Period	SHA512		
Certificate Database	SHA1		
Confirmation			
	Allow administrator interaction when the private	key is accessed b	by the CA.
	More about Cryptography		

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.

the Marin	DESTINATION SERVE
ate Key	D1.noida.com
dentials Sp a Services	ecify the type of the private key
ир Туре То с	generate and issue certificates to clients, a certification authority (CA) must have a private key.
Type O i	Create a new private key
ate Key	Jse this option if you do not have a private key or want to create a new private key.
Cryptography U CA Name (Valiano) Period Ufficate Database	Use existing private key Jse 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.
Ma	re about Private Key
Mar	re about Private Key

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		D1.noida.co
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	following criteria:	age Provider
Existing Key	Cryptographic provider:	ige Provider
Cryptography.	ECDSA_P256#SigteNet Key Storage Provider	•
CAIName	Type certification authority (CA) common name	
validity/Period	(optional):	Change
Cemilicate Database	noida-D1-CA	
Confirmation	Search Cancel	
	4	
	Allow administrator interaction when the private key	is accessed by the CA.
	More about Existing Key	

26. Select the Existing Key and click Next.

xisting Key	DEST	INATION SERVE D1.noida.co
Credentials Role Services Setup Type CA Type Private Key Existing Key Cryptography CA Name Validity Period	Select an existing key Select a key from the list. The listed keys are the keys available on the target com the search criteria. You may change the search criteria. Search criteria for key Cryptographic provider: ECDSA_P256#SareNet Key Storage Provider CA common name: noida-D1-CA	puter matching Change
Certificate Database	Search results:	
Confirmation Progress Results	noida-D1-CA	
	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.

		DESTINATION SERV
CA Name		D1.noida.c
Credentials	Specify the name of the CA	
Role Services		
Setup Type	Type a common name to identify this certification authority (CA). This name	
СА Туре	certificates issued by the CA. Distinguished name suffix values are automation be modified.	cally generated but (
Private Key		
Cryptography	Common name for this CA:	
CA Name	noida-D1-CA	
Validity Period	Distinguished name suffix:	
Certificate Database	DC=noida,DC=com	
Confirmation	Preview of distinguished name:	
	CN=noida-D1-CA,DC=noida,DC=com	
	More about CA Name	

- 28. 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

certatii verifykeys

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

Enrolling the Certification Authority Certificate

- 1. Create a CA template that uses SafeNet Key Storage Provider.
 - a. Open a command prompt and run certtmpl.msc
 - b. Right click the Administrator template
 - c. Click Duplicate Template.

1	Certificate 1	Femplates Console			×
File Action View Help					
🗟 Certificate Templates (WIN-AA7		Schema Version	Versi	^	Actions
	Adm Duplicate Template	1	41		Certificate Templates (WIN-AA74
	20 AUUI	1	3.1		More Actions
	🗟 Basic All Pasks 🔹 🕨	1	3.1		inde Pearly.
	CAE Properties	2	106.0		Administrator
	CEP I Help		4.1		More Actions
	Code Help Computer	1	3.1 5.1		
	Computer Copy of Administrator	3	5.1		
	Cross Certification Authority	3	100.3		
	Directory Email Replication	2	115.0		
	Domain Controller	1	4.1		
	Domain Controller Authentication	2	110.0		
	EFS Recovery Agent	1	6.1	=	
	Enrollment Agent	1	4.1		
	Enrollment Agent (Computer)	1	5.1		
	Exchange Enrollment Agent (Offline regu	1	4.1		
	Rechange Signature Only	1	6.1		
	R Exchange User	1	7.1		
	IPSec	1	8.1		
	IPSec (Offline request)	1	7.1		
	🔄 Kerberos Authentication	2	110.0		
	💹 Key Recovery Agent	2	105.0		
	OCSP Response Signing	3	101.0		
	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		
	Subordinate Certification Authority Test Administrator	1	5.1		
	The second s	4	100.3	~	
: m >	< m		1	8	1

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

ile Action View Help						
• • 📅 🖬 😹 🖬 📷						
Certificate Templates (WIN-AA7	Template 0	Properties of M	lew Template	×	Actions	
	Admini:	rioperues or i	ien rempiare		Certificate Templates (WI	N-AA74
	Authent Subject Nam			e Requirements	More Actions	Dagita de Charles de C
			Extensions	Security	Variation and the second	
	CA Exch Compatibility	General Re	equest Handing	Cryptography	Administrator	
	The template of	ptions available are ba	ed on the earliest (operating system	More Actions	
	Comput versions set in I	Compatibility Settings.				
	Copy of					
	Cross C	ing changes				
	Director					
	Domain Compatibility S	Settings				
	Domain Certification	Authority				
	EFS Rect	and the second se	~			
	I Enrollm	51461 2000				
	🖳 Enrollm Certificate re	cipient				
	Exchang	P / Server 2003				
	Exchang Windows X	P / Server 2003				
	Exchang	sta / Server 2008 / Server 2008 R2 / Windows Server 201				
	IPSec Windows 7	/ Server 2608 R2 / Windows Server 201	2			
	IPSec (C					
	Rerbero					
	Rey Rec			a to take a second state of the second		
		may not prevent earlier	operating systems	from using this		
	28 RAS and					
	Root Ce					
	Router (Smartca					
	Smartca	11	10			
	Subordi	OK Canc	el Apply	Help		
	Test Administrator	4		100.3		
W >				100.3	•	

- 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
- i) Uncheck the **E-mail name** check box.

Compatibility	General	Reques	t Handling	Cryptography
	perseded Templates		ensions	Security
Subject Name	Se	erver	Issuance	e Requirements
O Supply in the r	equest			
Use subje renewal re		irom existing	certificates fo	at autoenrollment
Build from this		an infanna Ca	20	
simplify certifica			among subjec	t names and to
Subject name I				
Fully distinguis				~
	iail name in sul	piect name	0	
	iair rianie in sui	sleername		
Include this infi		ernate subje	ct name:	
E-mail name	2.84			
DNS name				
🕑 User princip	bal name (UPN	1		
Service prin	ncipal name (S	PN)		
* Control is disabl				

- 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.

	Contract of the		
Certification Authority (Local)		Name	Intended Purpose
issued C E Pending Failed Re	Certificates ertificates Requests		There are no items to show in this view.
Certainee	Manage		
	New		Certificate Template to Issue
	View	•	1
	Refresh Export List		
	Help	,	

n) Select New -> Certificate Template to Issue

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

	on this Certification Authority. ently created does not appear on this list, you may r	need to wait until
ormation about this template has been re of the certificate templates in the organi	plicated to all domain controllers. zation may not be available to your CA.	
r more information, see Certificate		
lame	Intended Purpose	1
Administrator	Microsoft Trust List Signing, Encrypting Fil	e System, Secure E
Authenticated Session	Client Authentication	
Basic EFS	Encrypting File System	-
🛛 CA Exchange	Private Key Archival	
CEP Encryption	Certificate Request Agent	
🛙 Code Signing	Code Signing	
Computer	Client Authentication, Server Authentication	on
Copy 2 of Administrator	Client Authentication, Secure Email, Encry	pting File System, N
Copy of Adnatistrator	Client Authentication, Secure Email, Encry	pting File System, N
Cross Certification Authority	<all></all>	N N
	III	>

- 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...

	certm	gr - [Ce	ertificates - Current User\Personal]	x
- Contraction of the second	s - Current User	🛛 🕅 Object	Туре	
 Person Trus Ente 	Find Certificates	l sa c	ficates	
▷ Crite ▷ Crite ▷ Crite ▷ Crite ▷ Crite ○ Activ			Find Certificates Request New Certificate	
Þ 🧾 Trus Þ <u> </u> Untr	Refresh Export List		Import Advanced Operations	
👌 🧰 Trus	⊳ 🚰 Thin ▶ 🚰 Trus 🛛 Help			
A CONTRACTOR	Authentication Issuers Card Trusted Roots			
< 1	1 >	<	10	>
Request a new	certificate from a certi	fication a	uthority (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.

Archiving the CA Key

You can verify that the configurations that are possible with the SafeNet Luna HSM or HSM on Demand 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:

- archive the CA key
- issue the KRA certificate from the CA snap-in
- issue the KRA certificate from the CA snap-in
- retrieve the issued certificate from CA
- configure CA to support Key Archival

Microsoft Active Directory Certificate Services Integration Guide

- create a template with Key Archival enabled
- add a new template to CA for issuing
- issue a user template with key archival enabled
- ß

NOTE: If you wish to secure the key on SafeNet 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.

To 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.

ile Action View Hel					
• • 🗟 🗟 🕨	Ľ.,				
Certification Authority (Local)	Name		Description	
A moida-D1-CA Revoked Certifica Issued Certificate Pending Request Failed Requests Certificate Term	5 5	anoida-D1-	CA	Certification Authority	
- centred et et	Mana	ige			
New Refre	New	· •		emplate to Issue	
	sh				
	Help				

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

ormation about this template has beer	ecently created does not appear on this list, you may need to wait until n replicated to all domain controllers. anization may not be available to your CA.	
Name	Intended Purpose	
🗷 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 Log	c
🕅 Key Recovery Agent	Key Recovery Agent	
OCSP Response Signing	OCSP Signing	
🖫 RAS and IAS Server	Client Authentication, Server Authentication	10
🔄 Router (Offline request)	Client Authentication	
ਭ Smartcard Logon	Client Authentication, Smart Card Logon	
Smartcard User	Secure Email: Client Authentication: Smart Card Loron	2
	III >	

To 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....

D Certifica	Find Certificates	lary	I Store Name sonal sted Root Certification Authorities	
þ 🧮 En	All Tasks	•	Find Certificates	
b 🧰 Inf b 📫 Ac	Refresh		Request New Certificate	
D 🚺 Tr			Import	
 ▷ Chir ▷ Chir ▷ Chir ○ Chir ○ Cert 	usted Certificates d-Party Root Certificatio ted People nt Authentication Issuers ificate Enrollment Reque rt Card Trusted Roots	Thi Tru Clie Cer	Advanced Operations	
	m >	<	m	

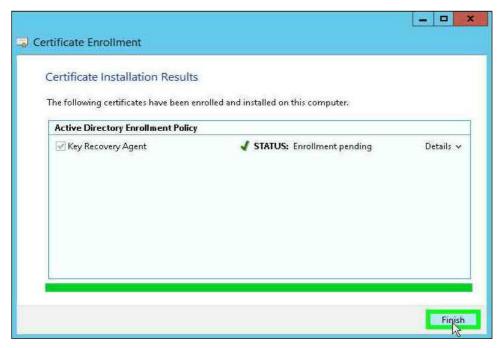
- 3. Click Next.
- 4. Select Active Directory Enrollment Policy and click Next.

Select Certificate Enrollment Policy	
Certificate enrollment policy enables enrollment for certi Certificate enrollment policy may already be configured	
Configured by your administrator	
Active Directory Enrollment Policy	
Configured by you	Add Ne

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

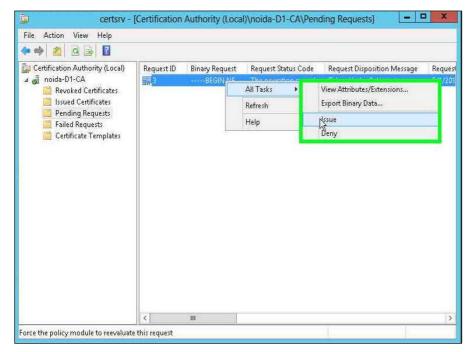
Request Certificates		
You can request the following types of click Enroll.	certificates. Select the certificates you want t	o request, and then
Active Directory Enrollment Policy		
Copy 2 of Administrator	i) STATUS: Available	Details
✔ Key Recovery Agent	😲 STATUS: Available	Details
Show all templates .earn more about certificates		

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



To 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.

To 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...

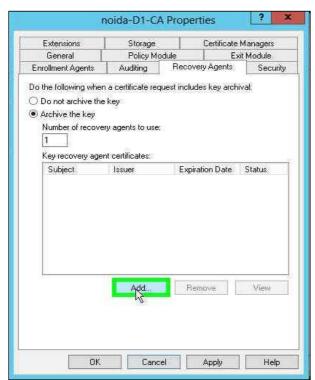
	certmg	- [Certificates - Current User]
File Action View P	felp	
 Certificates - Current I Personal 	Find Certifica	sl Stava Nama Sui
 Trusted Root Ce Enterprise Trust Intermediate Ce 	All Tasks View	Find Certificates Find Certificates All protocolly Enroll and Retrieve Certificates
 Active Directory Trusted Publishi Untrusted Certif 	Refresh Export List	User Object rs cates
 Third-Party Roo Trusted People Client Authenticat Client Authenticat Certificate Enrollm Smart Card Truster 	ion Issuers ent Reque: d Roots	and any much Certification Authorities Isted People ent Authentication Issuers rtificate Enrollment Requests art Card Trusted Roots
< m	> <	ш. У

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

To 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.



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



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

To 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 (WIN-78P)	Template Display Name	Schema Version	Version \land	Actions	
	R Cross Certification Authority	2	105.0	Certificate Templates (WIN-78PG	I3KKBB
	Replication	2	115.0	More Actions	
	Regulation Domain Controller	1	4.1	more redons	
	Representation Provided Authentication	2	110.0	User	
	🚇 EFS Recovery Agent	1	6.1	More Actions	
	🚇 Enrollment Agent	1	4.1		
	Rhrollment Agent (Computer)	1	5.1		
	Rechange Enrollment Agent (Offline requ	1	4.1		
	🚇 Exchange Signature Only	1	6.1		
	🚇 Exchange User	1	7.1		
	2 IPSec	1	8.1		
	Rec (Offline request)	1	7.1		
	Rerberos Authentication	2	110.0		
	Rey 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		
	Real Smartcard Logon	1	6.1		
	Real Smartcard User	1	11.1		
	Rest Subordinate Certification Authority	1	5.1		
	Trust List Signing	1	3.1		
	User		21		
	Regional User Signature Only	Duplicate Template	.1		
	🚇 Web Server	All Tasks	> .1		
	Representation Authentication		01.0		
		Properties	v		
>	<	Help	>		

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

	Certificate Templates Console	3
ile Action View Help		
Certificate Templates (WIN-AA7	Template C Dranaction of Now Template Actions	
	Adminic Properties of New Template Certificate Templa	tes (WIN-AA74
	Authent Subject Name Server Issuance Bequirements	
	Basic EF Superseded Templates Extensions Security	
	CA Exch Compatibility General Request Handling Cryptography Administrator	
	Image: Code Site The template options available are based on the earliest operating system vertices set in Compatibility Settings. More Actions: Image: Comput Show resulting changes Image: Compatibility Settings. Image: Compatibility Settings: Image: Compatibility Settings: Image: Compatibility Settings: Image: Compatib	
	Subordi Test Administrator 4 100.3	
	< m >	

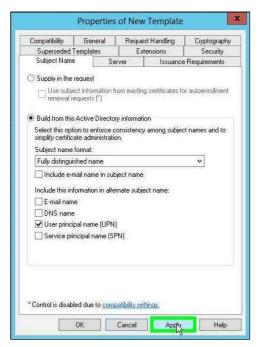
4. On the **Resulting Changes** menu click OK.

Tab	Template Option
Request Handling Cryptography Cryptography	For automatic renewal of smart card certificates, use the existing key if a new Use alternate signature format Key Storage Provider
Copy to clipboard	OK Cancel

- 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 Nar	me S	erver	Issuance	Requirements
Supersedeo	d Templates	Exte	ensions	Security
Compatibility	General	Reques	t Handling	Cryptography
Purpose:	Signature and	d encryption		~
	Delete revi	oked or expin	ad certificates	(do not archive)
	Include sur	mmetric algori	thms allowed	by the subject.
			otion private k	
	Le la	biocces circity	Mon billydic it	
Allow privat	e key to be expo	orted		
Renew with	the same key (1		
For automal new key ca	ic renewal of sm nnot be created	nart card certi I	ficates, use th	e existing key if a
Do the followin	a when the subi	ect is entolled	l and when th	e private ken
	this certificate i			o pinolo noj
associated with				
	ct without requir	ing any user i	nput	
Enroll subje			nput	
Enroll subje Prompt the	user during enro	ilment	2000) 10 - 10 - 10 - 10	ut when the
Enroll subje Prompt the	user during enro user during enro	ilment	2000) 10 - 10 - 10 - 10	ut when the
 Enroll subje Prompt the Prompt the private key 	user during enro user during enro is used	illment illment and re	quire user inpl	ut when the
 Enroll subje Prompt the Prompt the private key 	user during enro user during enro	illment illment and re	quire user inpl	it when the

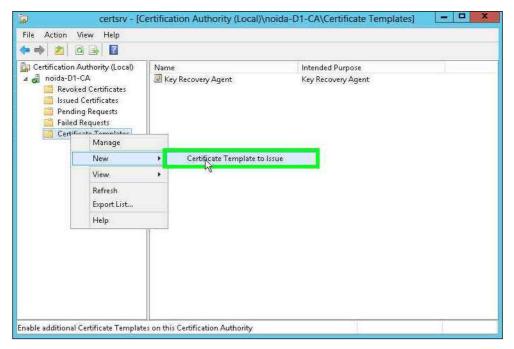
- 7. Select the Subject Name tab.
- 8. Uncheck the Include e-mail name in subject name check box.
- 9. Uncheck the E-mail name check box.



10. Click Apply and then OK.

To 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.

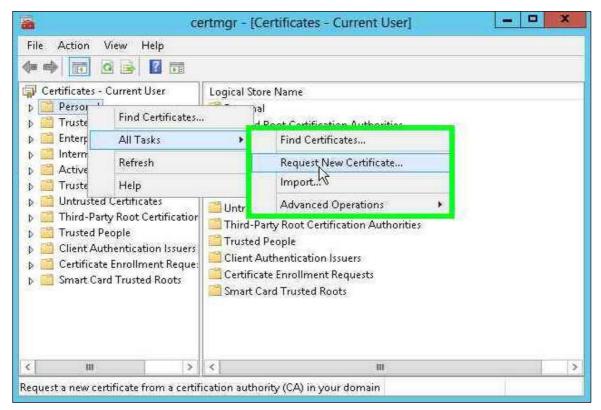


4. Select new template for key archival, click **OK**.

	Ena	ble Certificate Templates	x
Note inforr All of	ct one Certificate Template to enable or : If a certificate template that was recer- mation about this template has been rep i the certificate templates in the organiz- more information, see <u>Certificate Te</u>	ntly created does not appear on this list, you may need to wait until plicated to all domain controllers. ation may not be available to your CA.	
Na	me	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, 1	v
	Trust List Signing	Microsoft Trust List Signing	
	User Signature Only	Secure Email, Client Authentication	
	UserKArchival	Client Authentication, Secure Email, Encrypting File System	
凰	UserKeyArchival	Client Authentication, Secure Email, Encrypting File System	
	Workstation Authentication	Client Authentication	
		W >	Ľ
		III >	
		OK	el

To issue a user template with key archival enabled

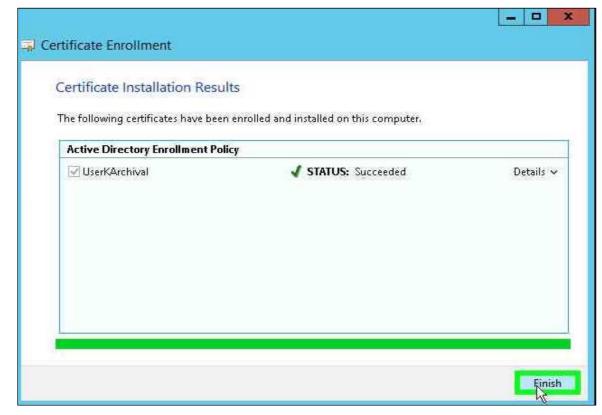
- 1. Open the command prompt and run the **certmgr.msc** command.
- 2. Right-click Personal node.
- 3. Select All Tasks -> Request New Certificate.



- 4. Click Next
- 5. Click Next.
- 6. Select the new template for key archival check box and click Enroll.

Request Certificates You can request the following types of certificates. Select the certificates you want to request, and then lick Enroll.		
Active Directory Enrollment Polic	y.	
🗌 Key Recovery Agent	(i) STATUS: Available	Details
✓ UserKArchival	i STATUS: Available	Details

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



9. Click Finish.

Performing a 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.

Install and configure 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 Configure the SafeNet HSM Key Storage Provider section.)

Setting 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.
- 2. The steps to install the Microsoft Active Directory Certificate Services are same as the Install Active Directory Certificate Services section. After Microsoft ADCS is successfully installed, 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**.

Cert	ification Authority	Backup W	lizard	
Items to Back Up You can back up indiv	idual components of the	certification au	thority data.	G
Select the items you wi	sh to back up:			
Private key and CA	certificate			
	e and certificate database	ellog		
Perform incre Back up to this location C:\Backup			Browsea	
Back up to this location	ĸ		Browse	

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

C	ertification Authority Backup Wizard
	Completing the Certification Authority Backup Wizard
	You have successfully completed the Certification Authority Backup wizard.
	You have selected the following settings: Private Key and CA Certificate
	<
	To close this wizard and begin backup, click Finish,
	Kack Finish Cancel Help

Ì

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 SafeNet HSM.

10. Click **OK** to continue.

B

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. 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.

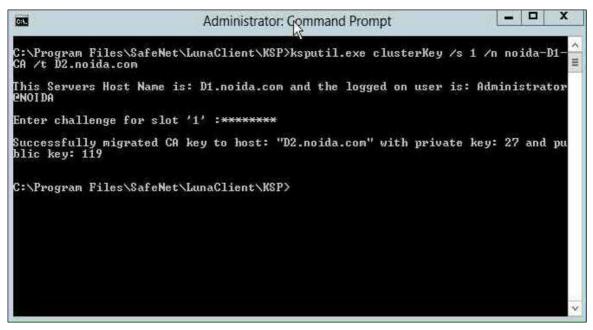
```
ksputil clusterKey /s <slotNum> /n <CA_Name> /t <TargetHost_Name>
Where,
```

slotNum - slot number

CA_name – name of the CA

TargetHost_Name - FQDN of the second node

2 - Integrate SafeNet HSM with Microsoft ADCS on Windows Server



- 12. 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.

13. 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**.

	Server M	anager	>
. ••	Volumes • Disks	• 🕝 🚩 Manage Tools	View Help
Servers Volumes	All disks 2 total	ρ (ii) ↓ (ii) ↓	TASKS 👻
Disks Storage P Shares iSCSI	▲ D1 (2)	tatus Capacity Unallocated Partition	Read Only
	1 0	Onlin GPT New Volume Bring Online	
		Take Offline Reset Disk	
	< III Last refreshed on 5/1/2013	11:34-28 PM	>
	VOLUMES	STORAGE POOL	

Microsoft Active Directory Certificate Services Integration Guide

To release the HSM from the cluster node

- 2. Since SafeNet Luna HSM is a network attached HSM, therefore disable the network connection to release it from cluster node one.
- 3. Logoff from the Cluster node one.

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

Setting up the CA server role on the second cluster node

This section explains how to set up the second cluster node. To install the CA on the second node, complete the following:

- To configure the secondary cluster node
- To import an existing CA certificate
- To add the AD CS role
- To configure the AD CS Role

To configure the secondary cluster node

- Log on to the cluster node with permissions to install the second cluster node. To install an enterprise CA, logon with enterprise 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**.

To 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 ...

2 - Integrate SafeNet HSM with Microsoft ADCS on Windows Server

-	Sec. 1		Console1 - [Console Root	\Certificates (Local Computer)\Personal]		- 🗆 X
File	Action View Favor	ites Window				_ 5 ×
(Find Certificates	a				47
📔 Cons		•	Find Certificates		Actions	
4 🛱 C	New Window from	n Here	Request New Certificate) items to show in this view.	Personal	
Þ 🛄	New Taskpad View	N	Import Advanced Operations		More Actions	•
	Refresh Export List		Advanced Operations			
D 🖸	Help Third-Party Root Certi	v				
	Client Authentication Remote Desktop Smart Card Trusted Rc Trusted Devices					
Add a cer	tificate to a store	A Restaura				

- 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*).

File to Import Specify the file you want to import.	
share Vice up And America utbact.	
File name:	
C:\Backup\noida-D1-CA.p12	Browse
Cryptographic Message Syntax Standard- PKCS # Microsoft Serialized Certificate Store (.SST)	*7 Certificates (.P7B)
earn 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.**

Certificate	e Import Wizard	×
- Contraction		
Private key prot	ection	
To maintair	n security, the private key was protected with a password.	
Type the p	assword for the private key.	2
Password:	••••	
L	lay Password	
Import opti		
prive	ile strong private key protection. You will be prompted every time the ate 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	
	at a later time.	
	ide all extended properties.	
a dana sa	ut protecting private keys	

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

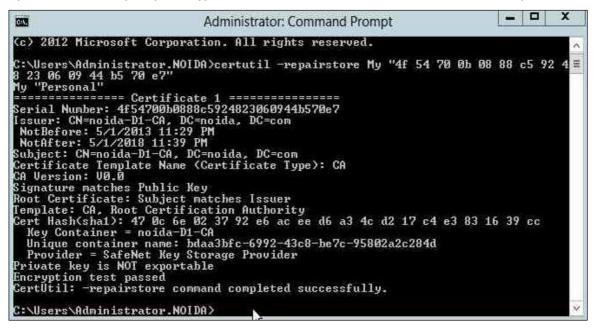
Certificate St	ore te stores are system	areas where certi	ficates are kept.	
10.000.000	58 A. 167 CONTLAND 4 CASES		1997.2007.000.0100.000	
Windows the certi	s can automatically s ficate,	elect a certificate s	tore, or you can spec	tify a location for
	utomatically select th	ne certificate store	based on the type of	certificate
• Pl	ace all certificates in	the following store		
G	ertificate store:			
1	Personal		1	Browse
learo more a	bout certificate store	><		
ream more a	Doue <u>certificate store</u>			

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

12. Select the field Serial Number and copy the serial number into the clipboard. Click OK.

anna anna anna anna anna anna anna ann	Details	Certification Pat	h	
Show:	<all></all>		Ý	
Field			Value	^
the second second	ersion		V3	
1000	erial numb	70	4f 54 70 0b 08 88 c5 92 48 23	=
100 million (1997)	gnature a		sha1RSA	
Annalise 1997	gnature h suer	ash algorithm	sha1	-
C	suer alid from		noida-D1-CA, noida, com Wednesday, May 1, 2013 11:	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	alid to		Tuesday, May 1, 2018 11:39:	
Su	bject		noida-D1-CA, noida, com	v
e7 [

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



To 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 installation Before You Begin Installation Type Server Selection Server Roles Features Confirmation		ysical computer	ON SERV nolda.c	om ual
Confirmation Results		te a virtual macl	hine-bi	ised
	< Previous Ner*>	Install	Cance	#

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

elect destinati	on server			DESTINATION SERV D2 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 from 	m the server pool		
Server Selection	O Select a virtual har	rd disk		
Server Roles	Server Pool			
Features	10-5 S			
	Filter:			
	Name	IP Address	Operating System	1
	D2.noida.com	172.25.11.99	Microsoft Windows Server 20	012 Standard
			dows Server 2012, and that hav fline servers and newly-added s	

6. Click Next.

1000

7. Select the Active Directory Certificate Services check box from the Server Roles.

elect server rol	es		DESTINATION SERVE D2.noida.co
Before You Begin Installation Type	Select one or more roles to install on the selected server.		Description
Server Selection	Active Directory Certificate Services	^	Active Directory Certificate Services (AD CS) is used to create
Server Roles Features Confirmation Results	Active Directory Domain Services Active Directory Federation Services 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 Print and Document Services		(AD C3) is used to create certification authorities and related role services that allow you to issu and manage certificates used in a variety of applications.
	Remote Access Remote Desktop Services	~	

- 8. The Add features that are required for Active Directory Certificate Services? window displays. To add a feature, click the Add Features button.
- 9. Click **Next** to continue.

10. Click Next to continue.

	Add Roles and Features Wizard	
Select features		DESTINATION SERV D2.noida.co
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Select one or more features to install on the selected server. Features	Description .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.
k Next to continue.	ہم Add Roles and Features Wizard	_ 0
		DESTINATION SERV
Active Directory Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	 Certificate Services (AD CS) provides the certific such as secure wireless networks, virtual private networks, Intern Access Protection (NAP), encrypting file system (EFS) and smart Things to note: The name and domain settings of this computer cannot be cl (CA) has been installed. If you want to change the computer server to a domain controller, complete these changes before information, see certification authority naming. 	et Protocol Security (IPSec), Networ card log on. hanged after a certification authority hame, join a domain, or promote this

< Previous

Next >

Install

Cancel

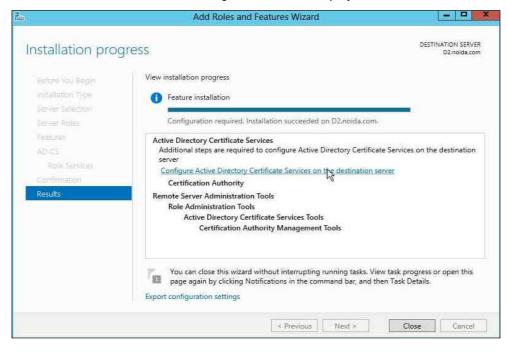
12. Select the **Certification Authority** check box from the **Role services** list and click **Next**.

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 Certification Authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder	ficate Services Description Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form public key infrastructure.

13. Click Install.

Confirm installa	ation selections	DESTINATION SERVI D2.noida.co
Before You Begin	To install the following roles, role services, or features on selecte	ed server, click Install.
Installation Type	Restart the destination server automatically if required	
Server Selection Server Roles Features	Optional features (such as administration tools) might be display been selected automatically. If you do not want to install these of their check boxes.	
AD CS Role Services	Active Directory Certificate Services Certification Authority	
Confirmation	Remote Server Administration Tools Role Administration Tools	
	Active Directory Certificate Services Tools Certification Authority Management Tools	
	Export configuration settings Specify an alternate source path	

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

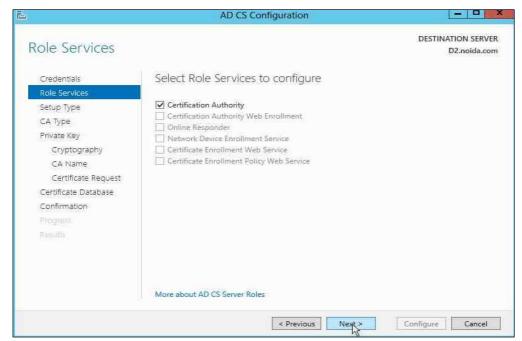


To configure the AD CS Role

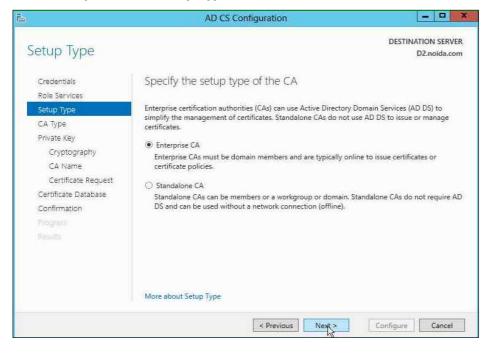
1. On the Credentials page of the AD CS Configuration wizard click Next to continue.

redentials		DESTINATION SERVER
regentials		D2.noida.con
Credentials	Specify credentials to configure role services	
Role Services		
	To install the following role services you must belong to the local Ad	ministrators group:
	Standalone certification authority	
	Certification Authority Web Enrollment Online Responder	
	To install the following role services you must belong to the Enterpris	se Admins group:
	Enterprise certification authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Network Device Enrollment Service	
	Credentials: NOIDA\Administrator Chang	e
	More about AD CS Server Roles	
	< Previous Next >	Configure Cancel

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



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



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

- A. T. 115 - 0	DESTINATION SERVE
LA Type	D2.noida.coi
Credentiais	Specify the type of the CA
Role Services	
Setup Type	When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its
СА Туре	own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI
Private Key	hierarchy.
Cryptography	Root CA
CA Name	Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
Validity Period	Subordinate CA
Certificate Database	Subordinate CA Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates b
Confirmation	the CA above them in the hierarchy.
Festilis	
	More about CA Type

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.

	AD CS Configuration	
Existing Certifica	te	DESTINATION SERVER
		DEMORIDACI
Credentials	Select an existing certificate for the CA	
Role Services		
Setup Type	To use a private key associated with a certificate, select that certif	
CA Type	certificate if it is not available on the target computer. The selecte will be used for this certification authority (CA).	d certificate and its properties
Private Key	and the second	
Existing Certificate	Certificates:	1
Certificate Database	Subject Issued By Expiration Date	Import
	noida-R1-CA noida-D1-CA 5/1/2018	Properties
	Allow administrator interaction when the private key is access	ed 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.

i	AD CS Configuration	×
CA Database		DESTINATION SERVER D2.noida.com
Credentials Role Services Setup Type	Specify the database locations Certificate database location:	
CA Type Private Key	E:\ Certificate database log location:	
Existing Certificate Certificate Database	EA	
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**.

Confirmation Credentials Role Services	To configure the following roles, Active Directory Certificat 	role services, or features, click Configure. e Services	D2.noida.co
Role Services Setup Type CA Type Private Key Existing Certificate Certificate Database Confirmation Progress Results	Certification Authority CA Type: Allow Administrator Interaction: Certificate Validity Period: Distinguished Name: Certificate Database Location: Certificate Database Log Location:	Enterprise Root Disabled 5/1/2018 11:39:39 PM CN=noida-D2-CA,DC=noida,DC=com E:\ E\	

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

Setting up the Failover Cluster feature on both the cluster nodes

Repeat the following steps on both the cluster nodes:

- 1. Log on to the cluster nodes 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 D2.nd	SERVE oida.co
Before You Begin	Select a server or a vi	rtual hard disk on which	to install roles and features.	
Installation Type	 Select a server from 	om the server pool		
Server Selection	Select a virtual ha	rd disk		
Server Roles	Server Pool			
Features	10-20			
Confirmation	Filter:			
	Name	IP Address	Operating System	
	D2.noida.com	172.25.11.99	Microsoft Windows Server 2012 Standard	
	1 Computer(s) found			
	Add Servers comman		dows Server 2012, and that have been added by u fline servers and newly-added servers from which o	

7. Click Next twice.

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

elect features		DESTINATION SERVER D2.noida.com
Before You Begin Installation Type	Select one or more features to install on the selected server. Features Descript	tion
Server Selection Server Roles Peatures Confirmation Results	NET Framework 3.5 Features (Installed) Background Intelligent Transfer Service (BITS) BitLocker Drive Encryption BitLocker Network Unlock BranchCache Cient for NPS	amework 3.5 combines the of the .NET Framework 2.0 th new technologies for a gapfications that offer ng user interfaces, protect stomers' personal identity ition, enable seamless and communication, and provide ity to model a range of s processes.
	IP Address Management (IPAM) Server	

- 9. A pop up displays stating **Add features that are required for Failover Clustering?** To add a feature, click the **Add Features** button.
- 10. Click Next.

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

11. Click Install.

onfirm installa	ition selections	DESTINATION SERVER
.orminin motane		02.10/03.00
Before You Begin	To install the following roles, role services, or features on selected	d server, click Install.
Installation Type	Restart the destination server automatically if required	
Server Selection	Optional features (such as administration tools) might be display	
Server Roles	been selected automatically. If you do not want to install these o their check boxes.	ptional features, click Previous to clea
Features		
Confirmation	Failover Clustering	
Results	Remote Server Administration Tools Feature Administration Tools Failover Clustering Tools Failover Cluster Management Tools Failover Cluster Module for Windows PowerShell	
	Export configuration settings Specify an alternate source path	

12. Click Close.

	Add Roles and Features Wizard
Installation prog	DESTINATION SERVED D2.noida.com
Before You Begin Installation Type	View installation progress
	Installation succeeded on D2.noida.com.
Peatures Continnation 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 or open this page again by clicking Notifications in the command bar, and then Task Details.
	< Previous Next > Close Cancel

Creating a Failover Cluster

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

調査	Failover Cluster Manager	_ _ ×
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	Failover Cluster Manager 🔶
	your failover clusters.	Validate Configuration
	▲ Overview	💐 Create Cluster
		🖶 Connect to Cluster
	A failover cluster is a set of independent computers that work together to increase the availability of server roles. The clustered servers (called nodes) are connected by physical cables and by software. If one of the nodes	View 🕨
	fails, another node begins to provide services (a process known as failover).	🙆 Refresh
	▲ Clusters	Properties
		🚺 Help
	▲ Management	Line (1) and
	To begin to use failover clustering, first validate your hardware configuration, and then create a cluster. After these steps are complete, you can manage the cluster. Managing a cluster can include migrating services and applications to it from a cluster running Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008.	
	Validate Configuration	
	Creating a failover cluster or adding a cluster node	
	Connect to Cluster	
	Migrating services and applications from a cluster	
	★ More Information	
	Eailover cluster topics on the Web	
	Eallover cluster communities on the Web	
	Microsoft support page on the Web	

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

8. Enter the Cluster Name and click Next until you reach the Summary page. .

4	Create Cluster Wizard
Access F	Point for Administering the Cluster
Before You Begin Select Servers Access: Point for Administering the Cluster Confirmation Creating New Cluster Summary	Type the name you want to use when administering the cluster. Cluster Name: ClusterADCS Image: 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 Next > Cancel

9. Verify the cluster configuration is appropriate and click Finish.



Configuring the ADCS Failover Cluster

You can configure an ADCS Failover configuration to support your certificate eservices.

To configure the ADCS failover cluster

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

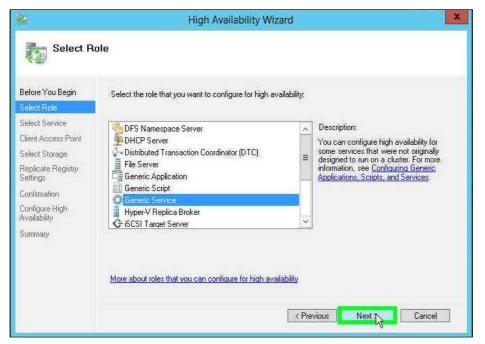
藩		F	ailover Cluster Manager	_ 0	×
File Action	View Help				
(* 🔿 🖄					
	ister Manager Cluste ADCS.noida.com	er ClusterADCS.noida.com		Actions	
a a contena a a a a contena a a a a a a a a a a a a a a a a a a a	Configure Role	Jmmary of Cluster Cluste sterADCS has 0 clustered roles and 2 sterADCS noida.com st Server: 02 nfiguration: Node Majority ster Events: None in the last hou	nodes. Networks: Cluster Network 1 Subnets: 1 IPv4 and 0 IPv6	ClusterADCS.noida.com	•
	Configuration applie	Unfigure gue high availability for a specific clustered zations from a cluster running Windows Ser Zarlidate Cluster Zalidate Cluster Alidate Roles Cluster-Aware Undating	Irole, add one or more servers (nodes), or migrate services and ver 2012, Windows Server 2008 R2; or Windows Server 2008. Continuum cleates for hinh availability Understanding cluster validation tests cluster as server to your cleater Windows Server 2008 R2; or Windows Server 2012, Windows Server 2008 R2; or Windows Server 2008, cluster from Windows Cleater to the cluster	More Actions View Refresh Properties Help Name: ClusterADCS Bring Online Take Offline	•
	▲ Ne	avigate	Nodes	Show Critical Events More Actions Properties	•
		Storage Cluster Events	Networks	I Help	
	Name	uster Core Resources er Name	Status		
	🖽 🐏	Name: ClusterADCS	📀 Online		

2. On the Before you Begin page click Next.

	High Availability Wizard
before `	You Begin
Before You Begin Select Role	This wizard configures high availability for a role. After you successfully complete this wizard, if a clustered server fails while running the role, another clustered server automatically begins running the role (a process known as failover). If the role tiself fails, it can be automatically restarted, either on the same server or on another server in the cluster, depending on options that you specify. If you want to cluster a complex application such as a mail server or database application, see that application's documentation for information about the correct way to install it.
	More about roles that you can configure for high availability Do not show this page again
	Next > Cancel

Microsoft Active Directory Certificate Services Integration Guide

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



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

ên e	High Availabilit	y Wizard	
Select Se	ervice		
Before You Begin Select Role	Select the service you want to use from the list		_
Select Service	Name	Description	^
Client Access Point Select Storage Replicate Registry Settings Confirmation Configure High Availability Summary	Active Directory Certificate Services Application Experience Application Host Helper Service Application Information Application Information Application Layer Gateway Service Application Management ASP.NET State Service Background Intelligent Transfer Service	Creates, manages, and removes X.509 certifica. 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	
		K Previous	

5. On the Client Access Point page enter the service name in the Name field and click Next.

9 7	High Availability Wizard
Client A	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.
	< Previous Cancel

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

	Hi	gh Availability W	izard	×
Select St	torage			
Before You Begin Select Role Select Service Client Access Point	Select only the storage volu You can assign additional s Name ☑ ⊞ Cluster Disk 1	imes that you want to a torage to this clustered Status (ক) Online	ssign to this clustered role. role after you complete this wizard.	
Select Storage Replicate Registry Settings Confirmation Configure High Availability		() Chillie		
Summary			< Previous Ne	Cancel

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

High Availability Wizard
e Registry Settings
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., Modily, Remove
< Previous Nexts

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

in .	3H	igh Availability Wizard	×
Confirma	ation		
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 Contimution	Service: Storage: Network Name: OU: IP Address: Registry Key:	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	^
Configure High Availability Summary	Parameters:	This Generic Service has no startup parameters.	Ŷ
	To continue, click Next,	< Previous Ca	incel

- 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			PQu	eries 🕶 🔛 💌 🗢
Name	Status (1) Running	Type Generic Service	Owner Node D2	Priority I Medium
<	83			3
👻 🍓 SintClust	lGen		Preferre	l Owners: <u>Any node</u>
Status: Priority:	Running Medium			
Owner Node:	D2			



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. Execute the ksputil.exe utility to migrate the keys to the cluster.

```
ksputil c /s <SlotNum> /t <CAClusterService_Name> /n <CA_Name>
Where,
```

<SlotNum> - slot number

<CAClusterService_Name> - name of the CA Cluster service configured

<CA_Name> - name of the CA

Creating 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}.

nistrator: Comr	nand Prompt	_ 0 X
		<u>^</u>
CDP,CN=Publi ateRevocatio	c Key Services,CN=	=Services, CN=Config 📒
pleted succe	ssfully.	
Enroll>	×	
	2,487 byte ,696,832 byt Enroll>certu CDP,CN=Publi ateRevocatio t	,696,832 bytes free Enroll>certutil -f -dspublish CDP,CN=Public Key Services,CN= ateRevocationList?base?objectC t pleted successfully.

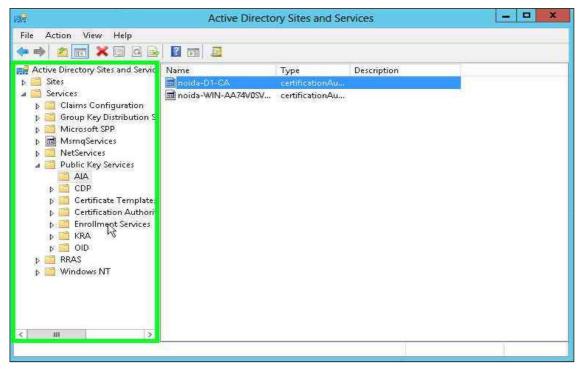
Modifying the CA configuration in Active Directory

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.



- 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.

Object Types
1994 B
Locations
Check Names
-11-

- 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.

2	Active Di	rectory Sites and	d Services	- 	
File Action View Help					
Active Directory Sites and Ser b Active Directory Sites	vic Name	Type pKIEnrollme	Description		
a 📋 Services	The second second		1024		
Claims Configuration Claims Configuration Claims Configuration	n S				
👂 🚞 Microsoft SPP					
▷ I MsmqServices ▷ I NetServices					
a 🧾 Public Key Services					
p 🧾 Cor p 🧾 Certificate Templa	tez				
Certification Authority Enrollment Service					
Enrollment Service KRA	3				
dið 🚞 🖉					
RRAS Mindows NT					
•					
ш —	>				

- 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.

Types
ions
Names

- 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.

NP .	Active Directo	ry Sites and Se	rvices	- D X
File Active View Help				
◆ ◆ 2 🖬 🗙 🖬 🏻 🗟				
Active Directory Sites and Servic Sites Claims Configuration Claims Configuration Claims Configuration Claims Configuration Microsoft SPP Microsoft SPP MetServices AlA Public Key Services AlA COP Cortification Authorit Enrollment Services KRA Cortification Authorit RRAS RA Microsoft SP Mindows NT	Name moida-D1-CA moida-WIN-AA74V0SV	Type msPK1-Private msPK1-Private	Description	

- 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**.

i	Object Types	? X
Select the types of objects you Object types:		
Service Accounts Computers Groups Users		
		OK 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:	17 - A.
noida.com	Locations
Enter the object names to select (<u>examples</u>):	
D2	Check Names

- 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.

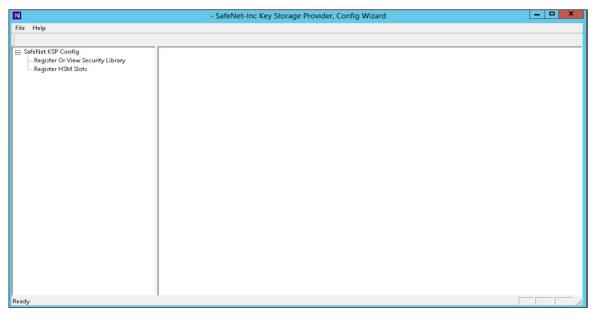
Migrate CA keys from Microsoft Software Key Storage Provider to SafeNet Key Storage Provider

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

Configuring the SafeNet KSP

You must configure the SafeNet Key Storage Provider (KSP) to allow the user account and system to access the SafeNet Luna HSM or HSM on Demand Service. If using a SafeNet Luna HSM, the KSP package must be installed during the Luna Client software installation. If using an HSM on Demand (HSMoD) service, the KSP package is included in the HSMoD 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.



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

N	- SafeNet-Inc Key Storage Provider, Config Wizard	-	x
File Help			
BisafeNet KSP Config Register Or View Security Library Register HSM Slots	LibraryPath C:Program Files\SafeNettLunaClienttcryptoki.dli Browse		
Ready			- //

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

N	- SafeNet-Inc Key Storage Provider, Config Wizard	- 0	X	
File Help Image: SafeNet KSP Config Register Or View Security Library Register Or View Security Library Register HSM Slots	- SafeNet-Inc Key Storage Provider, Config Wizard LibraryPath C:IProgram Files\SafeNettLunaClienttcryptoki.dll Browse Success Success OK OK	Regis]
Burk.				
Ready				11.

- 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.

R	 SafeNet-Inc Key Storag 	e Provider, Config Wizard	_ 🗆 X
File Help			
□- SafeNet KSP Config	Register For User	Domain	Register By
Register HSM Slots	Administrator	NOIDA	 Slot Label
	Available Slots	Slot Password	-
	1 part1 🗨	*****	C Slot Number
	Registered Slots SlotLabel:part		Register Slot View Registered Slots Delete Registered Slot
Ready			

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

N	- SafeNet-Inc Key Storage	e Provider, Config Wizard	_ 🗆 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 was successfully an		Register By Slot Label Slot Number Register Slot View Registered Slots Delete Registered Slot
Ready]		



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

Backing 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.
- 3. On the Action menu, click All Tasks and then Backup CA.

🤹 certsrv - [Certifi	cation Authority (Local)\lunatest-	ADCS-CA]	_ D X
File Action View Help			
🗢 🄿 🙍 🗔 🚇 🖉 🕨			
Certification Authority (Local) Name			
▷ Iunatest-ADCS-CA All Tasks ►	Start Service		
View 🕨	Stop Service		
Refresh	Submit new request		
Export List	Back up CA		
Properties	Restore CA		
Help	Renew CA Certificate		
Save CA certificates and configuration			

4. Click Next on the Welcome page of the CA backup wizard.

5. 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.	Ş
Select the items you wish to back up: ✓ Private key and CA certificate ✓ Certificate database and certificate database log ✓ 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

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

Migrating a MS CA onto a SafeNet Luna HSM or HSM on Demand 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.

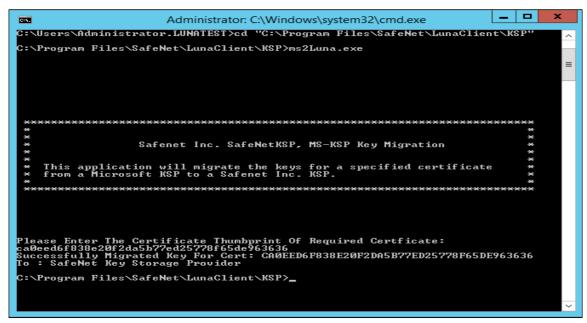
To migrate a MS CA onto a SafeNet HSM using ms2Luna

- 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 slot using KSP before migrating MSCA to SafeNet HSM.

3. Enter the Thumbprint of CA certificate and press Enter.



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

		Console1 - [Console Root\Certification Authority (Local)\lunatest-ADCS-CA]	_ 🗆 X
骗 File Action View Favorites Window H	Help		_ 8 ×
♦ ♦ 2 m 9 0 3 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0			
Console Root	Name		tions
A Dertification Authority (Local)	Revoked Certificates		
b 👩 lunatest-ADCS-CA	Issued Certificates	II.	inatest-ADCS-CA
lunatest-ADCS-	CA Properties ?	X	More Actions
Extensions Storage	Certificate Managers		
Enrolment Agents Auditing	Recovery Agents Security		
General Policy Mod	dule Exit Module		
Certification authority (CA)			
Name: kunatest-ADCS	ica.		
CA cetificates:			
Certificate #0			
	View Certificate		
0.1.11.11			
Cryptographic settings			
Provider: Safenet Key St	torage Provider		
Hash algorithm: SHA256			
OK Cancel	I Apply Help		
		ппп	

5. Uninstall the existing CA that the key was removed from.

Installing 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	
Select installation Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results		DESTINATION SERVER D1.noida.com nning physical computer or virtual es.
Installation Type Server Selection Server Poles Features Confirmation	 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 feature Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) 	es.
	< Previous Next >	Install

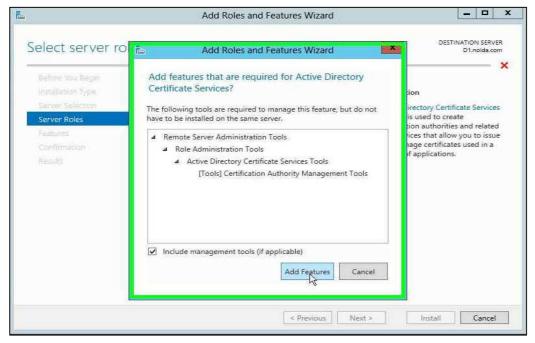
6. Select the Select a server from the server pool radio button and from Server Pool select your server.

elect destinati	on server			DESTINATION SERVI D1.noida.co
Before You Begin Installation Type	Select a server or a vir Select a server from Select a virtual har	m the server pool	to install roles and features.	
Server Selection	Server Pool	d disk		
Features Confirmation	Filter:			
Repulta	Name	IP Address	Operating System	
	D1.noida.com	172,25,11.92	Microsoft Windows Server 2	012 Standard
	Add Servers command		ndows Server 2012, and that hav	

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

elect server role	25	DESTINATION SERVE D1.noida.com
Beföre You Begin Installation Type Server Selection	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 Ederation Services Active Directory Rights Management 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 Decision Control of Cont

9. 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.

elect features			DESTINATION SERV D1.noida.co
Before You Begin Installation Type	Select one or more features to install on the selected ser Features	ver.	Description
Server Selection Server Roles Féatures AD CS Role Services Confirmation Results	INET Framework 3.5: Features MeT 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 Group Policy Management Ink and Handwriting Services Internet Printing Client	<	.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.
	IP Address Management (IPAM) Server	~	

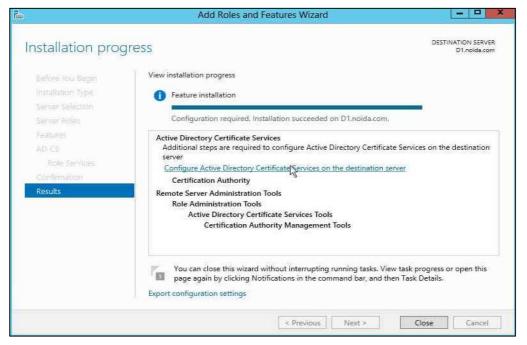
11. Select the **Certification Authority** check box from the **Role services** list and click **Next**.

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

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

	Add Roles and Features Wizard	
Confirm installa	ation selections	DESTINATION SERVER D1_noida.com
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation	To install the following roles, role services, or features on selected server, Restart the destination server automatically if required Optional features (such as administration tools) might be displayed on th been selected automatically. If you do not want to install these optional t their check boxes. Active Directory Certificate Services Certification Authority Remote Server Administration Tools Role Administration Tools	nis page because they have
	Active Directory Certificate Services Tools Certification Authority Management Tools Export configuration settings Specify an alternate source path	
	< Previous Next >	Cancel

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



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

	AD CS Configuration		
		DE	STINATION SERVE
Credentials			D1.noida.con
Credentials	Specify credentials to configure i	ole services	
Role Services			
Contimiation	To install the following role services you must b	elong to the local Administrator	s group:
7mgress	Standalone certification authority		
	 Certification Authority Web Enrollment Online Responder 		
	To install the following role services you must b	elong to the Enterprise Admins	group:
	Enterprise certification authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Network Device Enrollment Service		
	Credentials: NOIDA\Administrator	Change	
	More about AD CS Server Roles		
	< Previous	Nex Configu	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.

)	AD CS Configuration
Private Key	DESTINATION SERVER D1.noida.com
Credentials Role Services Setup Type	Specify the type of the private key To generate and issue certificates to clients, a certification authority (CA) must have a private key.
CA Type Private Key	 Create a new private key Use this option if you do not have a private key or want to create a new private key.
Existing Key Cryptography CA Name Valiany Period	 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.
Certificate Database Confirmation Progress Results	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
	< Previous Nert > Configure Cancel

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**.

	AD CS Configuration	_ D X
Existing Ke	еу	DESTINATION SERVER ADCS.lunatest.com
Credentials Role Services Setup Type CA Type Private Key Existing Key Cryptograp CA Name Validity Peri Certificate Data Confirmation	Search for keys on the target computer using the following criteria: Cryptographic provider: RSA#SafeNet Key Storage Provider Type certification authority (CA) common name (optional):	n the target computer matching e Provider Change
Progress Results	Allow administrator interaction when the private key is access More about Existing Key	sed by the CA.

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
Existing Key	DESTINATION SERVER ADCS.lunatest.com
Credentials Role Services Setup Type CA Type Private Key <u>Existing Key</u> Cryptography CA Name Validity Period	Select an existing key Select a key from the list. The listed keys are the keys available on the target computer matching the search criteria. You may change the search criteria. Search criteria for key Cryptographic provider: RSA#SafeNet Key Storage Provider CA common name: lunatest-ADCS-CA Change
Certificate Database Confirmation Prograss Results	Search results: Iunatest-ADCS-CA Image: Allow administrator interaction when the private key is accessed by the CA. More about Existing Key
	< Previous Next > Configure Cancel

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

	AD CS Configuration	_ D ×
Cryptography fo	or CA	DESTINATION SERVER ADCS.lunatest.com
Credentials Role Services Setup Type CA Type Private Key Existing Key	Specify the cryptographic options Select a hash algorithm for signing certificates issued Cryptographic provider: RSA#SafeNet Key Storage Provider	by this certification authority (CA).
Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Hash algorithm: SHA256 SHA384 SHA512 SHA1	
	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.

b	AD CS Configuration	_ 0 ×
CA Name		NATION SERVER CS.lunatest.com
Credentials Role Services Setup Type CA Type Private Key	Specify the name of the CA Type a common name to identify this certification authority (CA). This name is addr certificates issued by the CA. Distinguished name suffix values are automatically ge be modified.	
Existing Key Cryptography	Common name for this CA: Iunatest-ADCS-CA	
CA Name	Distinguished name suffix:	
Validity Period Certificate Database Confirmation	DC=lunatest,DC=com Preview of distinguished name:	
Progress Results	CN=lunatest-ADCS-CA,DC=lunatest,DC=com	
	More about CA Name	
	< Previous Next > Configure	Cancel

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

	AD CS Configuration
Validity Period	DESTINATION 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 validity period Select the validity period for the certificate generated for this certification authority (CA): 5 Years CA expiration Date: 4/30/2018 11:44:00 PM The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.
	More about Validity Period < Previous

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

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

- 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 must be imported.

Restoring an MS CA

You can restore a backed-up MS CA user 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.

<u>م</u> ة (certsrv - [Certification Authority (Local)\lunatest-ADCS-CA]			
File Action View Help				
🗢 🔿 🖄 🖾 🖾 🖌				
Certification Authority (Local)	Name			
De lun All Tasks	Start Service			
View	Stop Service			
Refresh	Submit new request			
Export List	Back up CA			
Properties	Restore CA			
Help	Renew CA Certificate			
Load previous CA certificates and configuration				
preserve and e				

- 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	:
Items to Restore You can restore individual components of the backup file.	P
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 wizard. Then re-run the wizard, selecting subsequent incremental backup files.	
< Back Next > Cancel Help	

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

Certification Authority Restore Wizard	x
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.	9
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

Microsoft Active Directory Certificate Services Integration Guide

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

🙀 cer	tsrv - [Certification Authority (Local)\lunatest-ADCS-CA]
File Action View Help	
🗢 🧆 🖄 🖾 🙆 📓	▶ ■
Certification Authority (Local) Iunatest-ADCS-CA	Name Revoked Certificates Ssued Certificates Pending Requests
	Certification Authority Restore Wizard
	The restore operation is complete. Do you want to start Active Directory Certificate Services? If you have additional incremental backup files to restore, click no and re-run the wizard until all files are restored. Yes No

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

certsrv - [Certification Authority (Local)\lunatest-ADCS-CA]		_	□ X
File Action View Help			
Certification Authority (Local)	Name Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates		