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 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.

© 2016 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.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Enrollment</td>
<td>198</td>
</tr>
<tr>
<td>Key Archival</td>
<td>211</td>
</tr>
<tr>
<td>Installing and configuring the CA cluster using SafeNet Key Storage Provider</td>
<td>233</td>
</tr>
<tr>
<td>Setting up the CA server role on the first cluster node</td>
<td>233</td>
</tr>
<tr>
<td>Setting up the CA server role on the second cluster node</td>
<td>260</td>
</tr>
<tr>
<td>Setting up the Failover Cluster feature on both the cluster nodes</td>
<td>289</td>
</tr>
<tr>
<td>Creating a Failover Cluster</td>
<td>297</td>
</tr>
<tr>
<td>Configuring the Active Directory Certificate Services Failover Cluster</td>
<td>303</td>
</tr>
<tr>
<td>Creating CRL objects in Active Directory</td>
<td>314</td>
</tr>
<tr>
<td>Adjusting the CA configuration in Active Directory</td>
<td>315</td>
</tr>
</tbody>
</table>
Preface

This document guides security administrators on obtaining the necessary information to install, configure, and integrate Microsoft ADCS with SafeNet Luna HSM.

Scope

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

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.
# Command Syntax and Typeface Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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 *Installation Guide* for more information.) |
| Consolas   | Denotes syntax, prompts, and code examples. |
Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>US</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>


1 – Introduction

Introduction

Overview

The Microsoft Active Directory Certificate Services 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. However, in order to realize the enhanced security made possible by certificates, organizations need a cost effective, efficient, secure way to manage the distribution and use of certificates.

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. Active Directory Certificate Services provides customizable services for managing certificates for a particular CA and for the enterprise.

The heart 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. The compromise of a CA’s root key by malicious intent, inadvertent errors, or system failures can be of catastrophic proportions. Hence, this root-signing key must be diligently protected by the best technologies and practices within the cryptographic community such as using the HSM (Hardware Security Module) device.

3rd Party Application Details

• Microsoft Active Directory Certificate Services

Supported Platforms

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Luna Client Software Version</th>
<th>SafeNet Luna HSM Appliance Software &amp; Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 R2</td>
<td>Luna v6.1.0-5</td>
<td>Luna SA v6.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HSM f/w 6.23</td>
</tr>
<tr>
<td></td>
<td>Luna v5.4.1</td>
<td>Luna v5.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>K6 HSM f/w 6.21.0</td>
</tr>
<tr>
<td>Operating System</td>
<td>Luna Client Software Version</td>
<td>SafeNet Luna HSM Appliance Software &amp; Firmware Version</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Luna v5.4</td>
<td>Luna v5.3.0, K6 HSM f/w 6.21.0</td>
</tr>
<tr>
<td></td>
<td>Luna v5.2</td>
<td>Luna v5.2.1, K6 HSM f/w 6.10.1</td>
</tr>
<tr>
<td></td>
<td>Luna G v1.2</td>
<td>Luna G5 v1.2, G5 HSM f/w 6.0.8</td>
</tr>
<tr>
<td></td>
<td>Luna v5.1</td>
<td>Luna SA v5.1, K6 HSM f/w 6.2.1</td>
</tr>
<tr>
<td></td>
<td>Luna v5.0</td>
<td>Luna SA v5.0, K6 HSM f/w 6.0.8</td>
</tr>
<tr>
<td></td>
<td>Luna v4.4.1</td>
<td>Luna SA v4.4.1, K5 HSM f/w 4.6.8</td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>Luna v5.2.1</td>
<td>Luna SA v5.2.1, K6 HSM f/w 6.10.1</td>
</tr>
<tr>
<td>Windows Server 2012 R2</td>
<td>Luna v6.2.0</td>
<td>Luna v6.2, K6 HSM f/w 6.10.9 &amp; 6.24.0</td>
</tr>
<tr>
<td></td>
<td>Luna v5.4.1</td>
<td>Luna v5.4.1, K6 HSM f/w 6.21.0</td>
</tr>
<tr>
<td></td>
<td>Luna v5.4</td>
<td>Luna v5.4, K6 HSM f/w 6.21.0</td>
</tr>
</tbody>
</table>
Prerequisites

SafeNet Network HSM Setup

Refer to the SafeNet Network HSM documentation for installation steps and details regarding configuring and setting up the box on Windows systems. Before you get started, ensure the following:

1. SafeNet Network HSM appliance has a secure admin password.
2. SafeNet Network HSM has a hostname suitable for your network.
3. SafeNet Network HSM network parameters are set to work with your network.
4. Initialize the SafeNet Network HSM.
5. Create a partition on the HSM and allocate a partition password to be used later.
6. Create and exchange certificates between the SafeNet Network HSM and the "Client" system.
7. Run the command, vtl verify to display a registered partition with SafeNet Network HSM.

Using Luna 6.x 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, please make the following change in the configuration file:

```
[Misc]
RSAKeyGenMechRemap = 1
```

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

---

**NOTE:** SafeNet Luna HSM Configuration settings are required only for Luna HSM f/w 6.22.0 or above. All other SafeNet Luna HSM f/w does not require this setting for FIPS mode.
Integrating Microsoft ADCS with SafeNet Luna HSM on Windows Server 2008 R2

This chapter outlines the steps to install and integrate Microsoft Active Directory Certificate Services on Windows Server 2008 R2. Microsoft Active Directory Certificate Services uses the SafeNet Luna HSM KSP (Key Storage Provider) for integration. SafeNet Luna HSM CSP (Cryptographic Service Provider) will only be used while upgrading Microsoft Certificate Services on Windows Server 2003 to Active Directory Certificate Services on Windows Server 2008 R2.

You should familiarize yourself with Microsoft Active Directory Certificate Services. Refer to the Windows Server 2008 R2 help files for more information.

Configure the SafeNet Luna HSM Key Storage Provider

1. KSP must be installed in a separate step following completion of the main SafeNet Luna HSM Client software installation.
2. Traverse to the KSP installation directory.
3. Run the KspConfig.exe (KSP configuration wizard).

4. Double-click **Register Or View Security Library** on the left side of the pane.
5. Browse the library `cryptoki.dll` from SafeNet Luna HSM Client installation directory and click **Register**.
6. On successful registration, a message "Success registering the security library" displays.
7. Double-click **Register HSM Slots** on the left side of the pane.

8. Enter the Slot (Partition) password.
9. Click **Register Slot** to register the slot for Domain\User. On successful registration, a message “**The slot was successfully and securely registered**” displays.
10. Register the slot for NT AUTHORITY\SYSTEM.

Install Microsoft ADCS on Windows Server 2008 R2 Enterprise Server Core using SafeNet KSP with an ECC Key

Refer to Configure the SafeNet Luna HSM Key Storage Provider section at the beginning to configure SafeNet KSP.

1. Install the Certificate Server Role
   a. Open the command prompt and run the following command:
      
      `start /w ocsetup CertificateServices`

      **NOTE:** This only installs the binaries and CA service. You still need to configure the CA in the next steps.

2. Configure CA via CA Setup APIs.
   a. Configure the CA using the provided VBScript.

   Install CA using SafeNet KSP and ECC algorithms.
   Verify CA script finished successfully.
NOTE: you can download the setupca.vbs file from Microsoft site to install the CA on Server Core installation where no GUI is available.

Example of running a script to install an Enterprise Root CA using ECDSA_P256 and SHA256 from the SafeNet KSP.

cscript setupca.vbs /ie /sp "ECDSA_P256#SafeNet Key Storage Provider" /sk 256 /sa SHA256 /sn MyCAName

NOTE: you can use the other algorithms also to generate the CA Certificate and Private on SafeNet Luna HSM.

3. Verify the CA service has successfully started.
   a. Open the command prompt and run the following command to verify that Service is running:
      sc query certsvc

4. Verify the CA Key.
   a. Open the command prompt and run the following command to verify the CA key:
      certutil -verifykeys
      The result of the command shows the CA keys have successfully been verified.

Install Microsoft ADCS on Windows Server 2008 R2 Enterprise Full using SafeNet KSP

1. Log in as an Enterprise Admin/Domain Admin with administrative privileges.
2. Refer to Configure the SafeNet Luna HSM Key Storage Provider section at the beginning to configure SafeNet KSP.
3. Click Start, point to Administrative tools, and then click Server Manager. The Server Manager snap-in displays.
4. Select **Roles** in the console tree.

5. Right-click **Roles** and then click, **Add roles**. The **Add Roles** wizard displays.

6. Click **Next**.
7. Select **Active Directory Certificate Services** check box from **Server Roles** to install.
8. Click **Next**.

9. Click **Next** to continue.
10. Select the **Certification Authority** check box from the **Role Services** list to install for **Active Directory Certificate Services**.

![Select Role Services](image)

11. Click **Next** to continue.
12. Specify the **Setup Type**.

13. Click **Next** to continue.
14. Specify the **CA Type**.

![Specify CA Type](image)

A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

- **Root CA**
  - Select this option if you are installing the first or only certification authority in a public key infrastructure.

- **Subordinate CA**
  - Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

More about public key infrastructure (PKI)

15. Click **Next** to continue.
16. Setup the **Private Key** for CA to generate and issue certificates to clients. Select **Create a new private key**.

![Add Roles Wizard: Private Key Setup](image)

- **Before You Begin**
- **Server Roles**
  - **AD CS**
  - **Role Services**
  - **Setup Type**
  - **CA Type**
- **Private Key**
  - **Cryptography**
  - **CA Name**
  - **Validity Period**
  - **Certificate Database**
- **Confirmation**
- **Progress**
- **Results**

17. Click **Next** to continue.
18. To create a new private key, select a cryptographic service provider and key length. Select an algorithm for SafeNet Key Storage Provider from the CSP list.

19. Select the Hash Algorithm for signing certificates issued by this Certificate Authority and key length.
20. Click the check box "Allow administrator interaction when the private key is accessed by the CA".

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

![Configure CA Name](image)

23. Click **Next** to continue.
24. Set the **Certificate Validity Period**.

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

![Configure Certificate Database](image)

27. Click **Next** to continue.

28. Confirm the installation selections.
29. Click **Install** to install the selected roles, role services, or features.
30. Click **Close** to exit the **Add Roles Wizard** after viewing the installation results.

![Add Roles Wizard](image)

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

31. Verify the CA service has been successfully started, open the command prompt and run the following command to verify that service is running:

```
sc query certsvc
```

32. Open the command prompt and run the following command to verify the CA key:

```
certutil -verifykeys
```

The result of the command shows the CA keys have been successfully verified.
Install Microsoft ADCS on Windows Server 2008 R2 Standard using Existing SafeNet Luna HSM Key

To install the Microsoft Active Directory Certificate Services software, perform the following steps:

1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
2. Refer to **Configure the SafeNet Luna HSM Key Storage Provider** section at the beginning to configure SafeNet KSP.
3. Click **Start**, point to **Administrative tools**, and then click **Server Manager**. The Server Manager snap-in window displays.
4. Select **Roles** in the console tree.
5. Right-click **Roles** and then click **Add roles**. The **Add Roles** wizard displays.
6. Click **Next**.
7. Select **Active Directory Certificate Services** check box from **Server Roles** to install on this server.

![Select Server Roles](Image)

<table>
<thead>
<tr>
<th>Server Roles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Directory Certificate Services</strong></td>
<td>Used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.</td>
</tr>
<tr>
<td>Active Directory Domain Services</td>
<td></td>
</tr>
<tr>
<td>Active Directory Federation Services</td>
<td></td>
</tr>
<tr>
<td>Active Directory Lightweight Directory Services</td>
<td></td>
</tr>
<tr>
<td>Active Directory Rights Management Services</td>
<td></td>
</tr>
<tr>
<td>Application Server</td>
<td></td>
</tr>
<tr>
<td>DHCP Server</td>
<td></td>
</tr>
<tr>
<td>DNS Server</td>
<td></td>
</tr>
<tr>
<td>Fax Server</td>
<td></td>
</tr>
<tr>
<td>File Services</td>
<td></td>
</tr>
<tr>
<td>Hyper-V</td>
<td></td>
</tr>
<tr>
<td>Network Policy and Access Services</td>
<td></td>
</tr>
<tr>
<td>Print and Document Services</td>
<td></td>
</tr>
<tr>
<td>Remote Desktop Services</td>
<td></td>
</tr>
<tr>
<td>Web Server (IIS) (Installed)</td>
<td></td>
</tr>
<tr>
<td>Windows Deployment Services</td>
<td></td>
</tr>
<tr>
<td>Windows Server Update Services</td>
<td></td>
</tr>
</tbody>
</table>

![Add Roles Wizard](Image)
8. Click **Next**.

9. Click **Next** to continue.
10. Select the **Certification Authority** check box from the **Role Services** list to install for **Active Directory Certificate Services**.

11. Click **Next** to continue.
12. Specify the **Setup Type**.

Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an **Enterprise** or **Standalone CA**.

- **Enterprise**
  - Select this option if the CA is a member of a domain and can use Directory Service to issue and manage certificates.

- **Standalone**
  - Select this option if the CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

**More about the differences between enterprise and standalone setup**

13. Click **Next** to continue.
14. Specify the **CA Type**.

![Specify CA Type](image)

15. Click **Next** to continue.
16. 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**.

![Add Roles Wizard]

To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

- **Create a new private key**
  - Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.

- **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 the 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.

17. Click **Next** to continue.
18. Click the **Edit...** button.

![Add Roles Wizard](image)

**Select Existing Key**

**Search criteria for key**

- **CSP:** RSA#Microsoft Software Key Storage Provider
- **CA common name:** HSMServer-HSMAPPL-C

**Search results**

**Select the key that you want to use for this CA:**

![Edit Search Criteria](image)

**Search**

19. Select the SafeNet Key Storage Provider algorithm that you have used to generate the private keys and clear the CA Common name, click **Search**.
20. Select existing key and click **Next**.
21. Select the **Hash Algorithm** for signing certificates issued by this Certificate Authority and key length settings for your installation and select the **Allow administrator interaction when the private key is accessed by the CA** check box.

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

24. Click **Next** to continue.
25. Set the **Certificate Validity Period**.

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

![Configure Certificate Database](image)

28. Click **Next** to continue.

29. Confirm the installation selections.
30. Click **Install** to install the selected roles, role services, or features.

![Add Roles Wizard](image)

---

**Active Directory Certificate Services**

**Certification Authority**

- **CA Type**: Standalone Root
- **CSP**: ECDSA _P_ (SafeNet Luna Key Storage Provider)
- **Hash Algorithm**: SHA1
- **Enabled**: Yes
- **Certificate Validity Period**: 12/23/2014 11:24 AM
- **Distinguished name**: CN=KEYCOUNTING-CA
- **Certificate Database Location**: C:\(Windows\system32)\Cert\log
- **Certificate Database Log Location**: C:\(Windows\system32)\Cert\log

---
31. Click **Close** to exit the **Add Roles Wizard** after viewing the installation results.

A private key that was earlier generated and stored on HSM will be used for the CA.

32. Verify the CA service has been successfully started, open the command prompt and run the following command to verify that service is running:

```sql
sc query certsvc
```

33. Open the command prompt and run the following command to verify the CA key:

```certutil -verifykeys```

The result of the command displays the CA keys have successfully been verified.
Certificate Enrollment

Enroll CA Certificate using SafeNet KSP

1. Install Enterprise Certificate Server using SafeNet Key Storage Provider. Refer section: Configure the SafeNet Luna HSM Key Storage Provider.

2. Verify CA is installed correctly.

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

![Certificate Templates Console](image)

Using this template as a base, creates a template that supports Windows Server 2003 Enterprise Cls.
- Select Windows Server 2008 Enterprise, Click **OK**.

![Duplicate Template](image)

- Click the **General** tab. Enter template name.

![Properties of New Template](image)
- Click the **Cryptography** tab. Select the **Requests must use one of the following providers** radio button.
• In the **Providers** field, select the **SafeNet Key Storage Provider** check box.
- Select an algorithm from the **Algorithm name** drop-down menu.
- Select **Request Hash.**
• Click the **Subject Name** tab.
• Uncheck the **Include e-mail name in subject name** check box
• Uncheck the **E-mail name** check box.

![Copy of Administrator Properties](image)

• Click **OK** to save the template.
• Open the command prompt and run **certsrv.msc**.
- Double-click the CA name.

- Right-click the CA template node.
- **Select New -> Certificate Template to Issue.**

![Certificate Template Image]

- **Select the template you just created above, click OK.**

![Enable Certificate Templates]

4. **Request a certificate based on the template.**
   - Open the command prompt and run the `certmgr.msc` command.
• Right-click the **Personal** node.

• **Select All Tasks** -> **Request New Certificate**…

![Image](image.png)

• **Click Next** twice.
• Enable check box for the template you created above.

![Certificate Enrollment](image)

- Click the **Enroll** button.

5. Verify the certificate is enrolled successfully.
The UI enrollment wizard shows if the certificate enrollment was successful.

![Certificate Enrollment](image)

### Key Archival

Enterprise CA’s key archival when SafeNet Luna HSM is being used for the CA private key. The main objective is to verify that the various configurations that are possible with the SafeNet Luna HSM device/software can be used and do not interfere with the CA key archival functionality.

1. Install Enterprise Certificate Server using SafeNet Key Storage Provider and ECC key. Refer section **Configure the SafeNet Luna HSM Key Storage Provider**.

2. Verify the CA is installed correctly.

3. Add Key Recovery Agent (KRA) template to the CA for issuing:
   - Open the command prompt and run the `certtmpl.msc` command.
   - Right-click the **Key Recovery Agent** template.
   - Click **Duplicate Template**.
• Select **Windows Server 2008 Enterprise** and click **OK**.
• In the **General** tab, enter Template Name and select the **Publish certificate in Active Directory** check box.

![Properties of New Template](image)

- **Template display name:** KeyRecoveryAgent-2008
- **Minimum Supported CAs:** Windows Server 2008 Enterprise
- **Template name:** KeyRecoveryAgent-2008
- **Validity period:** 2 years
- **Renewal period:** 5 weeks
- **Publish certificate in Active Directory**
- **Do not automatically reenroll if a duplicate certificate exists in Active Directory**
- **For automatic renewal of smart card certificates, use the existing key if a new key cannot be created**

[Image: Properties of New Template.png]
In the Cryptography tab, select the Request must use one of the following providers radio button.

Select SafeNet Key Storage Provider.

Click Apply and then OK to save the template.

Open the command prompt and run the certsrv.msc command.

Right-click the certificate template nodes.
- Select **New -> Certificate Template to Issue**
• Select **Key Recovery Agent** template, click **OK**.

![Enable Certificate Templates](image)

   - Request the KRA certificate. Open the command prompt and run the `certmgr.msc` command.
   - Right-click **Personal**.
• **Select All Tasks -> Request a new certificate.**

![Request a new certificate](image)

• **Click Next twice.**
• Select **Key Recovery Agent** Template.

5. Issue the KRA certificate from the CA snap-in.
• Open the command prompt and run the `certsrv.msc` command.

• Select pending requests.

• Right-click on the latest request for the KRA template.
• Select **All Tasks -> Issue**.

6. **Retrieve issued certificate from CA.**
   - Click **Issued certificates**….Verify the new certificate is issued.
   - Open the command prompt and run the **certmgr.msc** command.
   - Right-click **Certificates – Current User**.
• Select All Tasks -> Automatically enroll and retrieve certificates.

![Image of certificate management interface]

• Click Next.
• Select the KRA certificate just issued.

7. Configure the CA to support Key Archival.
   • Open the command prompt and run the certsrv.msc command.
   • Right-click the CA Name and select Properties.
• Select the **Recovery Agents** tab.

![Image of CertSrv-KeyCounting-CA Properties dialog box]

- Do the following when a certificate request includes key archival:
  - Do not archive the key
  - Archive the key
  - Number of recovery agents to use: [0]

- Key recovery agent certificates:

<table>
<thead>
<tr>
<th>Subject</th>
<th>Issuer</th>
<th>Expiration Date</th>
<th>Status</th>
</tr>
</thead>
</table>

- Add... | Remove | View | OK | Cancel | Apply | Help
- Select the **Archive the key** radio button.

![CertSrv-KEYCOUNTING-CA Properties](image)

Do the following when a certificate request includes key archival:
- Do not archive the key
- Archive the key

Number of recovery agents to use:

1

Key recovery agent certificates:

<table>
<thead>
<tr>
<th>Subject</th>
<th>Issuer</th>
<th>Expiration Date</th>
<th>Status</th>
</tr>
</thead>
</table>

- Click **Add**.
- Select the KRA certificate you just issued, Click **OK**.

![Windows Security](image)
• Ensure that the CA service must be restarted, click Yes.

**Certification Authority**

You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now?

[Yes][No]

8. Create Template with Key Archival enabled.
   • Open the command prompt and run the `certtmpl.msc` command.
   • Right-click the User template and click Duplicate Template.
• Select **Windows Server 2008 Enterprise**, click **OK**.

**Duplicate Template**

You can create certificate templates with advanced properties. However, not all Windows CAs support all certificate template properties. Select the version of Windows Server (minimum supported CAs) for the duplicate certificate template.

- Windows Server 2003 Enterprise
- Windows Server 2008 Enterprise

Learn more about **Certificate Template Versions**.

[Image: Duplicate Template]

• Click the **General** tab and enter a name for the template (UserKeyArchival).

**Properties of New Template**

<table>
<thead>
<tr>
<th>Issuance Requirements</th>
<th>Superseded Templates</th>
<th>Extensions</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td>Request Handling</td>
<td>Cryptography</td>
<td>Subject Name</td>
</tr>
</tbody>
</table>

**Template display name:**

UserKeyArchival

Minimum Supported CAs: Windows Server 2008 Enterprise

**Template name:**

UserKeyArchival

**Validity period:**

1 years

**Renewal period:**

6 weeks

- Publish certificate in Active Directory
  - Do not automatically reenroll if a duplicate certificate exists in Active Directory
  - For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

[Image: Properties of New Template]
Click the Request Handling tab and select the Archive subject’s encryption private key and Use advanced symmetric algorithm to send the key to the CA check box.
• Select **Subject Name** tab.
• Uncheck the **Include e-mail name in subject name** check box
• Uncheck the **E-mail name** check box.

![Copy of Administrator Properties](image)

• Click **OK** to save the template.

9. Add new template to CA for issuing.
• Open the command prompt and run the `certsrv.msc` command.
• Right-click **Certificate Templates** nodes.
• Select **New -> Certificate Template to Issue.**

![Certificate Template Image]

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

![Enable Certificate Templates]

10. Issue User template with key archival.

• **Open the command prompt and run the certmgr.msc command.**

• **Right-click the Personal node.**
• Select All Tasks -> Request New Certificate.

![Certificate Request Window]

• Click Next twice.

• Select the new template for key archival.
• Click **Enroll**.
• Verify enrollment succeeds via the enrollment wizard UI.

![Certificate Enrollment](image)

**Performing 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.

   ![Certificate Installation Results](image)

   **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.
2 – Integrating Microsoft ADCS with SafeNet Luna HSM on Windows Server 2008 R2

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, then 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. On the taskbar, click the Start button, click Run, type cmd, click OK to open a command prompt window.
   b. At the command prompt, type certmgr.msc
   c. Right click Certificates (Current User), and then click Find Certificates.
   d. In Find Certificates, under Contains, type CA Name and then click Find Now.
   e. In Find Certificates, on the Edit menu, click Select All.
f. In Find Certificates, on the File menu, click Delete.
g. In Certificates, click Yes.
h. Close Find Certificates.
5. Import the certificate at c:\user.pfx and let the certificates be placed automatically.
   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.
6. Verify the serial number of the imported certificate.
   a. In the console tree, double-click Personal and then click Certificates.
   b. Double-click the certificate
   c. In Certificate, click the Details tab. Verify that the serial number matches the original.
Upgrade from legacy OS to Windows Server 2008 R2

This scenario covers verification that there are no issues with the SafeNet Luna HSM after an OS upgrade. The scenario will require upgrading from both Windows Server 2003 and Windows Server 2008 machine to Windows Server 2008 R2. The OS upgrade will upgrade both the OS functionality and the Certificate Server functionality. After upgrade, verify that the SafeNet Luna HSM is still recognized and configured correctly and also SafeNet Luna HSM client software is still installed and correctly configured.

1. Install Windows Server 2003 or Windows Server 2008 with the latest service packs
2. Install SafeNet Luna HSM client software.

   **NOTE**: Before installing SafeNet Luna HSM v4.4.1 client software on Windows Server 2003 x64, install .Net framework, else Luna CSP won’t be listed while configuring the Certificate services.
   
   For SafeNet Luna HSM v5.0 client software on Windows Server 2003 x64, run RegisterCSP64.exe instead of register.exe.
   
   Also, run RegisterCSP64.exe /l after the above step, else SafeNet Luna CSP won’t be listed while configuring the Certificate services.

3. Install Certificate Server using:
   a. SafeNet Luna HSM CSP for Windows Server 2003 x64
   b. SafeNet KSP with ECC key for Windows Server 2008
4. Verify HSM hardware and software is functioning correctly before upgrade.
6. After upgrade:
   a. Verify SafeNet Luna HSM is functioning correctly.
Preparing the Active Directory Certificate Services Cluster Environment

This section focuses on the preparation of the environment for 2-node Active Directory Certificate Services Cluster in Windows Server 2008 R2.


Setting up a shared storage

To setup a shared storage disk for certificate services, refer to the configuration procedures that apply for your shared storage solution. Plan the size of the shared storage depending on the number of certificates that you are enrolling.

Configure and setup SafeNet Luna HSM

Refer to the SafeNet Luna HSM documentation for installation steps and details regarding configuration and setup. Before starting, ensure the following:

1. SafeNet Luna HSM appliance has a secure admin password
2. SafeNet Luna HSM, and a hostname suitable for your network
3. SafeNet Luna HSM network parameters are set to work with your network.
4. Initialize the SafeNet Luna HSM.
5. Create a partition on the SafeNet Luna HSM, remember the partition password that will be later used by the Microsoft ADCS. Register the Client with the partition. Run the "vtl verify" command on the client system to display a registered partition. The general form of command is
   \[C:\Program Files\SafeNet\LunaClient > vtl verify\]
   for Windows.
6. Create and exchange certificates between the SafeNet Luna HSM and Client system.
8. Ensure that both nodes have access to the same set of keys in SafeNet Luna HSM.
Installing and configuring the CA cluster using SafeNet Key Storage Provider

The following sections describe the installation and configuration of a CA on a failover cluster running on Windows Server 2008 R2.

1. Register Luna KSP using KSPConfig.exe. (Refer to Configure the SafeNet Luna 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.

1. Logon to the cluster node with permissions to install the first 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, click Run, type servermanager.msc, and then click OK.
3. The Server Manager MMC snap-in opens. Expand the Storage node and select Disk Management.
4. Ensure that the shared disk that is used for the CA is online.
5. In the left pane, select the **Roles** node.

6. From the **Action** menu, click **Add Roles**.
7. On the **Select Server Roles** page, select the **Active Directory Certificate Services** check box and click **Next** twice.
8. On the **Select Role Services** page, ensure that only the **Certification Authority** check box is selected and click **Next**.

**NOTE:** No other CA service than the CA is supported in a clustered environment.
9. Select the setup type for the CA and click **Next**.
10. Select **Create a new private key** and click **Next**.
11. Select **SafeNet Key Storage Provider** from the CSP list and set the desired key character length. Click **Next**.
12. Enter the CA name and click **Next**.
13. Select the validity period. Click **Next**.
14. Change the default paths for the database and log files to the desired location on the shared storage. Click Next.
15. Click **Install**.
16. Click **Close** to finish the **Role** installation.

After the successful installation, the CA certificate must be exported.

- Click the **Start** button, click **Run**, type **certsrv.msc**, and then click **OK**.
- Select the CA node in the left pane.
- On the **Action** menu, click **All Tasks** and then **Backup CA**.
17. Click **Next** on the Welcome page of the CA backup wizard.
18. Select **Private key and CA certificate** and provide a directory name where you want to temporarily store the CA certificate and optionally the key. Click **Next**.
19. Provide a password to protect the CA key and click **Next**.

![Select a Password](image_url)

**Select a Password**

For encryption and decryption of messages, both a public key and a private key are required. You must supply a password for the private key.

This password is required to gain access to the private key and the CA certificate file.

**Password:**

[Password field]

**Confirm password:**

[Confirm password field]

To maintain private key security, do not share your password.
20. Click **Finish**.

![Certification Authority Backup Wizard](image)

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

21. Click **OK** to continue.

![Certification Authority Backup Wizard](image)

**NOTE:** You need to run the `ksputil.exe` utility so that the keys are visible to the second node in the cluster. Please contact SafeNet Technical Support, in case you do not have the `ksputil.exe` utility.
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

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

- Click the Action menu and then All Tasks and then Stop Service.
- Close the CA management snap-in.

To detach the shared storage form the cluster node, continue with the next two steps.

- Go to the Server Manager MMC snap-in. Expand the Storage node and select Disk Management.
- Change the state of the disk keeping the CA database to offline.

To release the HSM from the cluster node one, perform these steps:

- Since SafeNet Luna HSM is a network attached HSM, therefore disable the network connection to release it from cluster node one.
- Logoff from 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, follow these steps:
1. Logon 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, click Run, type servermanager.msc, and then click OK.

3. The Server Manager MMC snap-in opens. Expand the Storage node and select Disk Management.

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, click 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 Computer account and click Next.

10. Select **Local Computer** and click **Finish**.
11. Click OK.

![Add or Remove Snap-ins dialog](image)

12. In the Certificate Manager MMC snap-in, expand the **Certificates (Local Computer)** node and select the **Personal** store.

13. From the **Action** menu, click **All Tasks** and then **Import ...**
14. In the Certificate Import Wizard, click **Next**.
15. 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).

![Certificate Import Wizard](image)

**File name:**

C:\Users\administrator.HSM\Server\Desktop\Backup\HSM\Server-H

**Note:** More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.pfx, .p12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.p7b)
- Microsoft Serialized Certificate Store (.sst)

Learn more about [certificate file formats](#).
16. Type the password that you have previously used to protect the private key. The password is required even if there is no private key in the PFX file. Do not mark this key as exportable. Click **Next**.
17. Place the certificate in the **Personal** certificate store and click **Next**.
18. Click **Finish** to finally import the certificate.

![Certificate Import Wizard](image)

19. Click **OK** to confirm the successful import.

![Certificate Import Wizard](image)

20. Repair the association between the certificate and the private key that is stored in the HSM.

21. In the Certificate manager, expand the **Personal** store and select the **Certificates** container.

22. Select the imported certificate and click **Open** from the **Action** menu.

23. Go to the **Details** tab.
24. Select the field **Serial Number** and copy the serial number into the clipboard. Click **OK**.
25. Open the command prompt and type `certutil -repairstore My "{Serial number}"` and press **Enter**.

26. Go to the **Server Manager** MMC snap-in.

27. In the left pane, select the **Roles** node.
28. From the **Action** menu, click **Add Roles**.

29. On the **Select Server Roles** page, mark **Active Directory Certificate Services** and click **Next** twice.
30. On the Select Role Services page, ensure that only the Certification Authority check box is selected and click Next.

**NOTE:** No other CA service than the CA is supported in a clustered environment.
31. Select the exact same setup type for the CA as you have chosen for the first node and click **Next**.
32. Select the exact same CA type for the CA as you have chosen for the first node and click **Next**.
33. Select **Use existing private key** and choose the option **Select a certificate and use its associated private key**. Click **Next**.
34. Select the CA certificate that was generated on the first node and click **Next**.

![Select Existing Certificate](image)

35. Change the default paths for the database. In the dialog box stating that an existing database was found, select **Yes** to overwrite it.

36. Change the default paths for the database log location. In the dialog box stating that an existing database was found, select **Yes** to overwrite it.

![Add Roles Wizard](image)
37. Click **Next** to continue.
38. Click **Install**.

![Add Roles Wizard]

39. Click **Close** to finish the Role installation.

40. Logoff from 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 both the cluster nodes with local administrator permissions.
2. Click the Start button, click **Run**, type *servermanager.msc*, and then click **OK**.
3. The Server Manager MMC snap-in opens. In the left pane, select the **Features** node.
4. From the **Action** menu, click **Add Features**.
5. From the list of available features, select the **Failover Clustering** check box and click **Next**.
6. Click **Install**.
7. Click **Close**.

![Add Features Wizard](image-url)

The following roles, role services, or features were installed successfully:

- **Failover Clustering**
  - Installation succeeded

*Print, e-mail, or save the installation report*
Creating a Failover Cluster

**NOTE:** Logon to cluster node where the storage is attached.

1. Click the **Start** button, point to **Run**, type **Cluadmin.msc**, and then click **OK**.
2. From the **Action** menu, select **Create a cluster**.
3. **If the Before you begin page appears, click Next.**

4. **Enter the cluster node name (computer name) of the first cluster node and click Add.**

5. **Enter the cluster node name of the second cluster node and click Add.**
6. Click **Next** to continue.
7. To perform the validation tests, select the **Yes** radio button and click **Next** twice.
8. Keep the default option to **Run all tests** and click **Next** twice.
9. Click **Next** to confirm the settings.
10. Verify the cluster test report and click **Finish**.
11. Enter the cluster name.
12. Click **Next** to confirm.
13. View the cluster creation report and click Finish.
Configuring the Active Directory Certificate Services Failover Cluster

To configure the ADCS failover cluster, perform the following steps:

1. In the Failover Cluster Management snap-in, select the Services and Applications node in the left pane.
2. From the Action menu, click Configure a service or Application.
3. Click **Next** on the **Before You Begin** page if it displays.
4. From the list of services and applications, select **Generic Service** and click **Next**.
5. From the list of services, select **Active Directory Certificate Services** and click **Next**.
6. Choose the service name and click **Next**.
7. Mark the disk storage that is still mounted to the node and click **Next**.
8. To configure a shared registry hive, click the **Add** button and enter `SYSTEM\CurrentControlSet\Services\CertSvc` and click **OK**.
9. Click **Next** twice.
10. Click **Finish** to failover configuration for certificate services.
NOTE: You need to run the ksputil.exe utility to migrate keys to the cluster. Please contact SafeNet Technical Support, in case you do not have the ksputil.exe utility.
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 Active Directory

With the permissions that the CA cluster has in Active Directory until now, it was not able to publish the CRL into Active Directory. Therefore, the CRL container has to be created and the CRL must be published. To create the CRL container, you must use the certutil command with the –f option as the following steps explain:

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}"`.

![Command output](image)

### Adjusting the CA configuration in Active Directory

You can perform the following tasks from any computer in your Active Directory forest where the Active Directory Sites and Services snap-in and ADSIEDIT is installed. The AIA object in Active Directory stores the CA’s certificate. To enable both the cluster nodes to update the CA certificate when required, perform the following steps:

1. Logon 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.
4. From the **View** menu, select the **Show services** node.
5. In the left pane, expand the **Services** and **Public Key Services** and then select **AIA**.

6. In the middle pane, select the CA name as it shows in the Certification Authority MMC snap-in.

7. From the Action menu select **Properties**.

8. Click the **Security** tab.

9. Use the **Add...** button.
10. Click **Object Types** and select **Computers**, and click **OK**.

![Object Types](image1)

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

![Select Users, Computers, or Groups](image2)
12. Ensure that the computer accounts of both the cluster nodes have **Full Control** permissions.

13. Click **OK**.
14. In the left pane, select **Enrollment Services**.

![Enrollment Services](image)

15. In the middle pane, select the CA name.

16. From the **Action** menu, select **Properties**.

17. Click the **Security** tab.

18. Use the **Add...** button.
19. Click **Object Types** and select **Computers** and click **OK**.

![Object Types](image1)

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

![Select Users, Computers, or Groups](image2)
21. Ensure that the computer accounts of both the cluster nodes have **Full Control** permissions.

22. Click **OK**.
23. In the left pane, select KRA.

24. In the middle pane, select the CA name.

25. From the Action menu select Properties.

26. Click the Security tab.

27. Use the Add... button.
28. Click **Object Types** and select **Computers** and click **OK**.

29. Type the computer name of the second cluster node as object name and click **OK**.
30. Ensure that the computer accounts of both the cluster nodes have **Full Control** permissions.

31. Click **OK**.

![Image of Security tab with Full Control permissions highlighted]

32. Close the Sites and Services MMC snap-in.
This chapter outlines the steps to install and integrate Microsoft Active Directory Certificate Services on Windows Server 2012/2012 R2. Microsoft Active Directory Certificate Services will use the SafeNet Luna KSP (Key Storage Provider) for integration.

You should familiarize yourself with Microsoft Active Directory Certificate Services. Refer to the appropriate Windows Server 2012/2012 R2 help files for more information.

Configure the SafeNet Luna HSM Key Storage Provider

1. KSP must be installed with Luna Client software installation.
2. Traverse to the KSP installation directory.
3. Run the KspConfig.exe (KSP configuration wizard).
4. Double-click **Register Or View Security Library** on the left side of the pane.
5. Browse the library `cryptoki.dll` from SafeNet Luna HSM Client installation directory and click **Register**.

![Image of SafeNet Luna HSM Client configuration](image1)

6. On successful registration, a message “**Success registering the security library**” displays.

![Image of successful registration](image2)

7. Double-click **Register HSM Slots** on the left side of the pane.
8. Enter the Slot (Partition) password.

9. Click **Register Slot** to register the slot for Domain\User. On successful registration, a message “The slot was successfully and securely registered” displays.

10. You need to register the slot for NT AUTHORITY\SYSTEM.
Install Microsoft Active Directory Certificate Services on Windows Server 2012/2012 R2 Enterprise Server using SafeNet Key Storage Provider with an ECC Key

Refer to the Configure the SafeNet Luna HSM Key Storage Provider section at the beginning to configure SafeNet KSP.

1. Install the Certificate Server Role
   a. Open the command prompt and run the following command:
      
      ```
      start /w ocsetup CertificateServices
      ```

      **NOTE:** This only installs the binaries and CA service. You still need to configure the CA in the next steps.

2. Configure CA via CA Setup APIs.
   a. Configure the CA using the provided VBScript.
      - Install CA using SafeNet KSP and ECC algorithms.
      - Verify CA script finished successfully.

      **NOTE:** You can download the setupca.vbs file from Microsoft site to install the CA on Server Core installation where no GUI is available.

      Example of running a script to install an Enterprise Root CA using ECDSA_P256 and SHA256 from the SafeNet KSP.
      
      ```
      cscript setupca.vbs /ie /sp "ECDSA_P256#SafeNet Key Storage Provider" /sk 256 /sa SHA256 /sn MyCAName
      ```

      **NOTE:** You can use the other algorithms also to generate the CA Certificate and Private Keys on SafeNet Luna HSM.

3. Verify the CA service has successfully started:
   a. Open the command prompt and run the following command to verify that Service is running:
      
      ```
      sc query certsvc
      ```

4. Verify the CA Key
   a. Open the command prompt and run the following command to verify the CA key:
      
      ```
      certutil -verifykeys
      ```

      The result of the command shows the CA keys have successfully been verified.
Install Microsoft Active Directory Certificate Services on Windows Server 2012/2012 R2 Enterprise using SafeNet Key Storage Provider

To install the Microsoft Active Directory Certificate Services software, perform the following steps:

1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
2. Refer to the Configure the SafeNet Luna HSM Key Storage Provider section at the beginning to configure SafeNet KSP.
3. Open Server Manager under Configure this Local Sever and click Add Roles and Features.
4. The **Add Roles** wizard displays.

   ![Add Roles Wizard](image)

   - **Before you begin**
   - **Installation Type**
   - **Server Selection**
   - **Server Roles**
   - **Features**
   - **Confirmation**
   - **Results**

   - **Skip this page by default**

   - **Before you continue, verify that the following tasks have been completed:**
     - The Administrator account has a strong password
     - Network settings, such as static IP addresses, are configured
     - The most current security updates from Windows Update are installed

   - If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

   - To continue, click **Next**.

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 from **Server Pool** select your server.

8. Click **Next**.
9. Select **Active Directory Certificate Services** check box from the **Roles**.
10. A pop up 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. Click **Next** to continue.
13. Select the **Certification Authority** check box from the **Role services** list and click **Next**.

![Add Roles and Features Wizard](image)

14. Click **Install**.

![Add Roles and Features Wizard](image)
15. Once installation is complete, click on the link **Configure Active Directory Certificate Services on the destination server** and it displays the AD CS Configuration wizard.
16. On the **Credentials** page of AD CS Configuration wizard, click **Next** to continue.
17. Select the **Certification Authority** check box and click **Next**.
18. Select **Enterprise CA** as setup type and click **Next**.

19. Select **Root CA** as type of CA and click **Next**.
20. Proceed to setup the Private Key for CA to generate and issue certificates to clients. Select **Create a new private key**. Click **Next** to continue.
21. To create a new private key, you must select a cryptographic service provider and key length. Select algorithm for **SafeNet Key Storage Provider** from the CSP list.

![AD CS Configuration](image)

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 **Next**.
24. Configure a common name to identify this Certificate Authority. Click **Next** to continue.
25. Proceed to set the **Certificate Validity Period**. Click **Next** to continue.
26. Configure the **Certificate Database**. It records all the certificate requests, issued certificates, and revoked or expired certificates. Click **Next** to continue.
27. Click **Configure** to configure the selected roles, role services, or features.
28. Click **Close** to exit the **AD CS Configuration** wizard after viewing the installation results.

![AD CS Configuration](image)

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

29. Verify the CA service has been successfully started, open the command prompt and run the following command to verify that service is running:

```
sc query certsvc
```

30. Verify the CA key. Open the command prompt and run the following command to verify the CA key:

```
certutil -verifykeys
```

The result of the command shows the CA keys have successfully been verified.
Install Microsoft Active Directory Certificate Services on Windows Server 2012/2012 R2 Standard using Existing SafeNet Luna HSM Key

To install the Microsoft Active Directory Certificate Services software, perform the following steps:

1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
2. Refer to the Configure the SafeNet Luna HSM Key Storage Provider section at the beginning to configure SafeNet KSP.
3. Open Server Manager under Configure this Local Sever and click Add Roles and Features.

![Server Manager Dashboard](image-url)
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 from **Server Pool** select your server.

8. Click **Next**.

9. Select the **Active Directory Certificate Services** check box from the **Roles**.
10. A pop up 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. Click **Next** to continue.
13. Select the **Certification Authority** check box from the **Role services** list and click **Next**.

![Select Certification Authority](image1)

14. Click **Install**.

![Confirm installation selections](image2)
15. Once installation is complete, click on the link **Configure Active Directory Certificate Services on the destination server** it opens AD CS Configuration wizard.

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

18. Select **Enterprise CA** as setup type and click **Next**.
19. Select **Root CA** as type of CA and click **Next**.
20. 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.

![Private Key Configuration](image)

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

![Existing Key Configuration](image)
22. Select the existing key and click **Next**.

23. Select the **Hash Algorithm** for signing certificates issued by this Certificate Authority and key length settings for your installation.
24. Click the **Allow administrator interaction when the private key is accessed by the CA** check box. Click **Next** to continue.
25. Configure a common name to identify this Certificate Authority. Click **Next** to continue.
26. Proceed to set the **Certificate Validity Period**. Click **Next** to continue.
27. Configure the **Certificate Database**. It records all the certificate requests, issued certificates, and revoked or expired certificates. Click **Next** to continue.
28. Click **Configure** to configure the selected roles, role services, or features.
29. Click **Close** to exit the **AD CS Configuration** wizard after viewing the installation results.

![AD CS Configuration results](image)

A private key that was earlier generated and stored on HSM will be used for the CA.

30. Verify the CA service has been successfully started, open the command prompt and run the following command to verify that service is running:

```bash
sc query certsvc
```

31. Verify the CA key. Open the command prompt and run the following command to verify the CA key:

```bash
certutil -verifykeys
```

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

**Certificate Enrollment**

**Enroll CA Certificate using SafeNet Key Storage Provider**

2. Verify CA is installed correctly.
3. Create a CA template that uses SafeNet Key Storage Provider.
   - Open the command prompt and run `certtmpl.msc`
   - Right click the Administrator template
   - Click Duplicate Template.
Select **Windows Server 2008** for both Certification Authority and Certificate recipient under **Compatibility Settings**, Click OK.
• Click OK for Resulting changes.
Select the **General** Tab. Enter template name.

- Go to the **Cryptography** tab. Select **Key Storage Provider** for **Provider Category**.
- Select **Requests must use one of the following providers** radio button.
- In the **Providers** field select the **SafeNet Key Storage Provider** only.
- For **Algorithm Name** select an algorithm.
- Select **Request Hash**.

- Select **Subject Name** tab.

- Uncheck the **Include e-mail name in subject name** check box
• Uncheck the **E-mail name** check box.

![Properties of New Template](image)

• **Click Apply** and **OK** to save the template.

• Open the command prompt and run **certsrv.msc**.

• Double-click the CA name.

• Right-click the CA template node.
• Select New -> Certificate Template to Issue
• Select the template you just created above, click **OK**.

![Enable Certificate Templates dialog box](image)

Select one Certificate Template to enable on this Certification Authority. Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers. All of the certificate templates in the organization may not be available to your CA. For more information, see [Certificate Template Concepts](#).

<table>
<thead>
<tr>
<th>Name</th>
<th>Intended Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Microsoft Trust List Signing, Encrypting File System, Secure EFS</td>
</tr>
<tr>
<td>Authenticated Session</td>
<td>Client Authentication</td>
</tr>
<tr>
<td>Basic EFS</td>
<td>Encrypting File System</td>
</tr>
<tr>
<td>CA Exchange</td>
<td>Private Key Archival</td>
</tr>
<tr>
<td>CEP Encryption</td>
<td>Certificate Request Agent</td>
</tr>
<tr>
<td>Code Signing</td>
<td>Code Signing</td>
</tr>
<tr>
<td>Computer</td>
<td>Client Authentication, Server Authentication</td>
</tr>
<tr>
<td>Copy 2 of Administrator</td>
<td>Client Authentication, Secure Email, Encrypting File System, Mailing Key</td>
</tr>
<tr>
<td>Copy of Administrator</td>
<td>Client Authentication, Secure Email, Encrypting File System, Mailing Key</td>
</tr>
<tr>
<td>Cross Certification Authority</td>
<td>Client Authentication, Secure Email, Encrypting File System, Mailing Key, (All)</td>
</tr>
</tbody>
</table>
4. Request a certificate based on the template.
   - Open the command prompt and run the `certmgr.msc` command.
   - Right-click the Personal node.
   - Select All Tasks -> Request New Certificate…
• Click **Next**.
• Click **Next**.
• Enable check box for the template you created above.

• Click the Enroll button.
5. Verify the certificate is enrolled successfully.
   - The UI enrollment wizard shows if the certificate enrollment was successful.

Key Archival

Enterprise CA’s key archival when SafeNet Luna HSM is being used for the CA private key. The main goal is to verify that the various configurations that are possible with the SafeNet Luna HSM device/software can be used and do not interfere with the CA key archival functionality.

**NOTE:** If you wish to secure the key on SafeNet Luna HSM that is used to encrypt the Archived Keys then you need to select the SafeNet Key Storage Provider for generating the keys for Key Recovery Agent certificate. Please refer the Chapter 2 Key Recovery section to generate the encryption keys on Luna HSM.

1. Install Enterprise Certificate Server using SafeNet Key Storage Provider and ECC key. Refer Chapter 2.
2. Verify CA is installed correctly.
3. Add Key Recovery Agent (KRA) template to CA for issuing:
   - Open the command prompt and run the `certsrv.msc` command.
   - Right-click the **certificate template** nodes.
• **Select New -> Certificate Template to Issue**
• Select **Key Recovery Agent** template, click **OK**.
4. Issue the KRA Certificate.
   - Request the KRA certificate. Open the command prompt and run the `certmgr.msc` command.
   - Right-click **Personal**.
   - Select **All Tasks -> Request a new certificate...**
• Click **Next**.
• Click **Next**.
- Select **Key Recovery Agent** Template and Click **Enroll**.
• Verify enrollment is pending, click **Finish**.

![Certificate Enrollment](image)

**Certificate Enrollment**

**Certificate Installation Results**

The following certificates have been enrolled and installed on this computer:

<table>
<thead>
<tr>
<th>Active Directory Enrollment Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Recovery Agent</td>
</tr>
</tbody>
</table>

![Finish](image)
5. Issue the KRA certificate from the CA snap-in.
   - Open the command prompt and run the `certsrv.msc` command.
   - Select pending requests.
   - Right-click on the latest request for the KRA template.
   - Select All Tasks -> Issue.

   ![Image of certsrv window with selected Issue option]

   - Click on Issued certificates. Verify the new certificate is issued.
6. Retrieve issued certificate from CA.
   - Open the command prompt and run the `certmgr.msc` command.
   - Right click **Certificates – Current User**
   - Select **All Tasks -> Automatically enroll and retrieve certificates**…
• Click **Next**.
3 – Integrating Microsoft ADCS with SafeNet Luna HSM on Windows Server 2012/2012 R2

- Select KRA certificate just issued and enroll it.

![Certificate Enrollment](image)

**Certificate Installation Results**

The following certificates have been enrolled and installed on this computer.

- **Active Directory Enrollment Policy**
  - Key Recovery Agent: **on**
  - Status: **Succeeded**

7. Configure CA to support Key Archival.
   - Open the command prompt and run the `certsrv.msc` command.
   - Right-click CA Name and select Properties.
   - Select the Recovery Agent tab.
   - Select the Archive the key radio button.
Click the **Add** button.
• Select the KRA certificate you just issued, Click OK.

![Windows Security](image)

• Click **OK**

• Verify the CA service must be restarted, click **Yes**.

8. Create Template that with Key Archival enabled.

• Open the command prompt and run the `certtmpl.msc` command.
Right-click the User template and click **Duplicate Template**.
- Select **Windows Server 2008** for both Certification Authority and Certificate recipient under **Compatibility Settings**, Click **OK**.
• Click **OK** for **Resulting changes**.

![Resulting changes dialog box](image)

The compatibility changes will add the following template options:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Template Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Handling</td>
<td>For automatic renewal of smart card certificates, use the existing key if a new ...</td>
</tr>
<tr>
<td>Cryptography</td>
<td>Use alternate signature format</td>
</tr>
<tr>
<td>Cryptography</td>
<td>Key Storage Provider</td>
</tr>
</tbody>
</table>

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

![General tab properties](image)

- Template display name: UserKeyArchival
- Template name: UserKeyArchival
- Validity period: 1 year
- Renewal period: 6 weeks
- Publish certificate in Active Directory
  - Do not automatically reenroll if a duplicate certificate exists in Active Directory
• Go to the **Request Handling** tab and enable the **Archive subject's encryption private key**.

![](Image)

• Click **OK**.

9. Add new template to CA for issuing.

• Open the command prompt and run the **certsrv.msc** command.

• Right-click **Certificate Templates** nodes.
• Select **New -> Certificate Template to Issue**.

• Select new template for key archival, click **OK**.
10. Issue User template with key archival

- Open the command prompt and run the `certmgr.msc` command.
- Right-click **Personal** node.
- Select **All Tasks -> Request New Certificate**.
• Click Next.

[Image of Certificate Enrollment interface showing Before You Begin section]

Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network.
You have credentials that can be used to verify your right to obtain the certificate.

Learn more about digital certificates.

[Image of Certificate Enrollment interface showing Certificate Enrollment Policy selection]

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator
Active Directory Enrollment Policy

Configured by you
Add New

Learn more about certificate enrollment policy.

[Image of Certificate Enrollment interface showing Next and Cancel buttons]
- Select new template for key archival click **Enroll**.

```
<table>
<thead>
<tr>
<th>Active Directory Enrollment Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Recovery Agent</td>
</tr>
<tr>
<td>User/Archival</td>
</tr>
</tbody>
</table>
```

Learn more about certificate.
• Verify enrollment succeeds via the enrollment wizard UI.

![Certificate Enrollment](image)

• Click Finish.

## Installing and configuring the CA cluster using SafeNet Key Storage Provider

The following sections describe the installation and configuration of a CA on a failover cluster running on Windows Server 2012/2012 R2.

Register SafeNet Luna KSP using KSPConfig.exe. (Refer to the Configure the SafeNet Luna 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.

1. Logon to the cluster node with permissions to install the first 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. Log in as an Enterprise Admin/Doman Admin with Administrative privileges.

3. Refer to the Before you install section at the beginning to configure SafeNet KSP.
4. Open Server Manager under **Configure this Local Sever** click on **Add Roles and Features.**
5. The **Add Roles and Features Wizard** displays.

6. Click **Next**.
7. Select **Role-based or feature-based installation** option and click **Next**.
8. Select option **Select a server from the server pool** option and from **Server Pool** select your server.

9. Click **Next**.
10. Select the **Active Directory Certificate Services** check box from **Roles**.
11. A pop up displays stating "Add features that are required for Active Directory Certificate Services?". To add a feature click the Add Features button.
12. Click **Next** to continue.
13. Click **Next** to continue.
14. Select **Certification Authority** from the **Role services** list and click **Next**.
15. Click **Install**.

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

16. Once installation is complete click the link **Configure Active Directory Certificate Services on the destination server** and it shows the AD CS Configuration wizard.
17. On **Credentials** page of AD CS Configuration wizard click **Next** to continue.
18. Select the **Certification Authority** check box and click **Next**.

19. Select **Enterprise CA** as setup type and click **Next**.
20. Select **Root CA** as type of CA and click **Next**.
21. Proceed to setup the Private Key for CA to generate and issue certificates to clients. Select the **Create a new private key** radio button. Click **Next** to continue.
22. To create a new private key, you must select a cryptographic service provider and key length. Select algorithm for SafeNet Key Storage Provider from the CSP list.

23. Select the Hash Algorithm for signing certificates issued by this Certificate Authority and key length settings for your installation.
24. Select the **Allow administrator interaction when the private key is accessed by the CA** check box. Click **Next** to continue.
25. Configure a common name to identify this Certificate Authority. Click **Next** to continue.
26. Proceed to set the **Certificate Validity Period**. Click **Next** to continue.
27. Change the default paths for the database and log files to the desired location on the shared storage. Click Next.
28. Click **Configure**.
29. Click Close to finish the **Role** Configuration.

![AD CS Configuration Results](image)

After the successful installation, the CA certificate must be exported.

30. Click the **Start** button, point to **Run**, type **certsrv.msc**, and then click **OK**.

31. Select the CA node in the left pane.

32. On the **Action** menu, click **All Tasks** and then **Backup CA**.
33. Click **Next** on the Welcome page of the CA backup wizard.

![Certification Authority Backup Wizard](image)

To continue, click **Next**.

34. Select **Private key and CA certificate** and provide a directory name where you want to temporarily store the CA certificate and optionally the key. Click **Next**.

![Certification Authority Backup Wizard](image)
35. Provide a password to protect the CA key and click **Next**.
36. Click Finish.

![Certification Authority Backup Wizard]

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

37. Click **OK** to continue.

**NOTE:** You need to run the *ksputil.exe* utility so that the keys are visible to the second node in the cluster.
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

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

38. Click the **Action** menu and then **All Tasks** and then **Stop Service**.

39. Close the CA management snap-in.
To detach the shared storage form the cluster node, perform the following steps:

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

To release the HSM from the cluster node one, perform these steps:

- Since SafeNet Luna HSM is a network attached HSM, therefore disable the network connection to release it from cluster node one.
- 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, follow these steps:

1. Logon 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, point to Run, type servermanager.msc, and then 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 Computer account and click Next.

![Certificates snap-in window](image)
10. Select **Local Computer** and click **Finish**.
11. Click **OK**.

![Add or Remove Snap-ins](image)

12. In the Certificate Manager MMC snap-in, expand the **Certificates (Local Computer)** node and select the **Personal** store.

13. From the **Action** menu click **All Tasks** and then **Import ...**

![Certificate Manager](image)
14. In the **Certificate Import Wizard**, click **Next**.
15. 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).
16. Type the password that you have previously used to protect the private key. The password is required even if there is no private key in the PFX file. Do not mark this key as exportable. Click Next.
17. Place the certificate in the **Personal** certificate store and click **Next**.
18. Click **Finish** to import the certificate.

![Certificate Import Wizard](image1)

19. Click **OK** to confirm the successful import.

![Certificate Import Wizard](image2)

20. Repair the association between the certificate and the private key that is stored in the HSM.

21. In the Certificate manager, expand the **Personal** store and select the **Certificates** container.

22. Select the imported certificate and select from the **Action** menu **Open**.

23. Go to the **Details** tab.
24. Select the field **Serial Number** and copy the serial number into the clipboard. Click **OK**.

![Certificate dialog box with Serial Number field highlighted]

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

![Command prompt output showing certificate repair information]
26. Open Server Manager under **Configure this Local Server** and click **Add Roles and Features**.
27. The **Add Roles and Features Wizard** displays.

28. Click **Next**.
29. Select the **Role-based or feature-based installation** radio button and click **Next**.
30. Select the **Select a server from the server pool** radio button and from **Server Pool** select your server.

31. Click **Next**.
32. Select the **Active Directory Certificate Services** check box from the **Roles**.
33. A pop up displays stating "Add features that are required for Active Directory Certificate Services?". To add a feature, click the **Add Features** button.
34. Click **Next** to continue.
35. Click **Next** to continue.
36. Click **Next** to continue.
37. Select the **Certification Authority** check box from the **Role services** list and click **Next**.
38. Click **Install**.
39. Once installation is complete, click on the link **Configure Active Directory Certificate Services on the destination server** it displays AD CS Configuration wizard.
40. On the **Credentials** page of the AD CS Configuration wizard click **Next** to continue.

![Credentials page](image)
41. Select the **Certification Authority** check box and click **Next**.
42. Select **Enterprise CA** as setup type and click **Next**.
43. Select **Root CA** as type of CA and click on **Next**.
44. Select the **Use existing private key** radio button and choose the option **Select a certificate and use its associated private key** and click **Next**.
45. Select the CA certificate that was generated on the first node and click **Next**.

46. Change the default paths for the database. In the dialog stating that an existing database was found, select **Yes** to overwrite it.

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

49. A dialog box displays stating that an existing database was found displays, click **Yes** to overwrite.
50. Click **Configure**.

![Configure](image_url)

51. Click **Close** to finish the **Role** installation.

52. Logoff from 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 both the cluster nodes with local administrator permissions.
2. Open Server Manager under Configure this Local Sever and click Add Roles and Features.

![Server Manager Screenshot](image-url)
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**.

![Add Roles and Features Wizard](image)

Select installation type

- **Role-based or feature-based installation**
  - Configure a single server by adding roles, role services, and features.

- **Remote Desktop Services installation**
  - Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

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

![Add Roles and Features Wizard](image)

Select destination server

- **Select a server from the server pool**
  - Select a server or a virtual hard disk on which to install roles and features.

- **Select a virtual hard disk**

**Server Pool**

Filter:

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>D2.noida.com</td>
<td>172.25.11.99</td>
<td>Microsoft Windows Server 2012 Standard</td>
</tr>
</tbody>
</table>

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
7. Click **Next** twice.
8. From the list of available features, select the **Failover Clustering** check box and click **Next**.
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**.
11. Click **Install**.
12. Click **Close**.
Creating a Failover Cluster

**NOTE:** Log on to the cluster node where the storage is attached.

1. Open Server Manager, Click Tools and select Failover Cluster Manager.
2. From the **Action** menu, click **Create a Cluster**.
3. If the *Before you begin* page displays, click **Next**.

4. Enter the cluster node name (computer name) of the first cluster node and click **Add**.
5. Enter the cluster node name of the second cluster node and click **Add**.
6. Click **Next** to continue.
7. Enter cluster name and click **Next** twice.
8. Click Finish.
Configuring the Active Directory Certificate Services Failover Cluster

To configure the ADCS failover cluster, perform the following steps:

1. In the Failover Cluster Management snap-in, right-click on Role and select Configure Role.
2. Click **Next** on **Before You Begin** page.
3. From the list of Role, select **Generic Service** and click **Next**.
4. From the list of services, select **Active Directory Certificate Services** and click **Next**.
5. Enter the service name and click **Next**.
6. Select the disk storage that is still mounted to the node and click **Next**.
7. To configure a shared registry hive, click the **Add** button and enter **SYSTEM\CurrentControlSet\Services\CertSvc** and click **OK**.
8. Click **Next** on the Confirmation page.
9. Click **Finish** to failover configuration for certificate services.
10. Newly created service should be in Running State.

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

With the permissions that the CA cluster has in Active Directory until now, it was not able to publish the CRL into Active Directory. Therefore, the CRL container has to be created and the CRL must be published. To create the CRL container, you must use the certutil command with the -f option as the following steps explain:

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}`.

![Certificate Util - DS Publish](image-url)
Adjusting the CA configuration in Active Directory

You can perform the following tasks from any computer in your Active Directory forest where the Active Directory Sites and Services snap-in and ADSIEDIT is installed. The AIA object in Active Directory stores the CA's certificate. To enable both the cluster nodes to update the CA certificate when required, perform the following steps:

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.
4. In the View menu, select the Show services node.
5. In the left pane, expand the Services and Public Key Services and then select AIA.
6. In the middle pane, select the CA name as it shows in the Certification Authority MMC snap-in.
7. From the Action menu select Properties.
8. Click the Security tab.
9. Use the Add... button.
10. Click **Object Types**... and select **Computers** and click **OK**.

![Object Types dialog box]

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

![Select Users, Computers, Service Accounts, or Groups dialog box]

12. Ensure that the computer accounts of both the cluster nodes have **Full Control** permissions.
13. Click **OK**.
14. In the left pane, select **Enrollment Services**.

![Image of Active Directory Sites and Services](image)

15. In the middle pane, select the CA name.
16. From the **Action** menu, select **Properties**.
17. Click the **Security** tab.
18. Use the **Add...** button.
19. Click **Object Types**... and select **Computers** and click **OK**.

![Object Types dialog box]

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

![Select Users, Computers, Service Accounts, or Groups dialog box]

20. Ensure that the computer accounts of both the cluster nodes have **Full Control** permissions.

21. Click **OK**.
23. In the left pane, select **KRA**.

24. In the middle pane, select the CA name.
25. From the **Action** menu select **Properties**.
26. Click the **Security** tab.
27. Use the **Add...** button.
28. Click **Object Types**... and select Computers and click **OK**.

![Object Types](image)

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

![Select Users, Computers, Service Accounts, or Groups](image)

30. Ensure that the computer accounts of both the cluster nodes have **Full Control** permissions.

31. Click **OK**.

32. **Close** the Sites and Services MMC snap-in.