Microsoft NDES: Integration Guide

THALES LUNA HSM AND LUNA CLOUD HSM

Document Information

Document Part Number	007-012725-001
Revision	C
Release Date	21 June 2022

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Introduction

This document outlines the steps to integrate Microsoft Network Device Enrollment Service (NDES) with Luna HSM devices and Luna Cloud HSM services. Microsoft NDES is one of the role services of the Microsoft Active Directory Certificate Services (ADCS) role. It implements Simple Certificate Enrollment Protocol (SCEP) that defines the communication between network devices and a Registration Authority (RA) for certificate enrollment. The goal of SCEP is to support the secure issuance of certificates to network devices in a scalable manner. To obtain more information on SCEP, refer to http://tools.ietf.org/html/draft-nourse-scep-18.

The Microsoft NDES service is mainly used by the enterprise customers and is available only on advanced and datacenter stock-keeping units (SKUs). It is not available on standard and WebServer SKUs for Windows Server. Microsoft NDES uses a Cryptographic Service Provider (CSP) to store the RSA signing keys on Luna HSM. Luna HSM secures the RSA signing keys generated and used by Microsoft NDES. You can integrate NDES with Luna HSM using the MS-CAPI interface. The benefits are:

- Secure storage of Microsoft NDES certificate encryption/signing keys
- Full life cycle management of the keys
- FIPS 140-2 level 3 support
- Failover support

Certified Platforms

Certified platforms on Luna HSM

Certified platforms on Luna Cloud HSM

Certified platforms on Luna HSM

HSM Type	Platforms Certified
Luna HSM	Windows Server 2016, Windows Server 2012 R2

Luna HSM: Luna HSM appliances are designed to provide a balance of security, performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. Luna HSM on premise offerings include Luna Network HSM, PCIe HSM, and Luna USB HSMs. Luna HSMs are also available as a cloud offering from providers such as IBM cloud HSM and AWS cloud HSM classic.

> **NOTE:** Do not use Luna Client UC 10.4 due to known issues with LUNA CSP.

> **NOTE:** This integration is tested with Luna HSM clients in both HA and FIPS Mode.

Certified platforms on Luna Cloud HSM

HSM Type	Platforms Certified
Luna Cloud HSM	Windows Server 2016

Luna Cloud HSM: Luna Cloud HSM is a cloud-based platform that provides on-demand HSM and Key Management services through a simple graphical user interface. With Luna Cloud HSM, security is simple, cost effective, and easy to manage because there is no hardware to buy, deploy, and maintain. As an Application Owner, you click and deploy services, generate usage reports, and maintain just the services you need.

Prerequisites

Before you proceed with the integration, complete the following tasks:

> Configure Luna HSM

> Configure Luna Cloud HSM Service

> Set up Microsoft NDES

> Register Security Library

Configure Luna HSM

If you are using Luna HSM:

1. Verify the HSM is set up, initialized, provisioned and ready for deployment. Refer to Luna HSM documentation for more details.
2. Create a partition that will be later used by Microsoft NDES.
3. Register a client for the system and assign the client to the partition to create an NTLS connection, if you are using a Luna Network HSM. Initialize the Crypto Officer and Crypto User roles for the registered partition.
4. Ensure that the partition is successfully registered and configured. The command to see the registered partitions is:

```
c:\Program Files\SafeNet\LunaClient>lunacm.exe
lunacm.exe (64-bit) v10.3.0-275. Copyright (c) 2020 SafeNet. All rights
reserved.

        Available HSMs:

        Slot Id ->              0
        Label ->                NDES1
        Serial Number ->        1312109862018
        Model ->                LunaSA 7.7.1
        Firmware Version ->     7.7.1
        Bootloader Version ->   1.1.2
        Configuration ->        Luna User Partition With SO (PW) Key Export
With Cloning Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         Non-FM
        Slot Id ->              1
        Label ->                NDES2
        Serial Number ->        1280780175880
        Model ->                LunaSA 7.7.1
        Firmware Version ->     7.7.1
        Bootloader Version ->   1.1.2
        Configuration ->        Luna User Partition With SO (PW) Key Export
With Cloning Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         Non-FM

        Slot Id ->              8
        HSM Label ->            HA
        HSM Serial Number ->    11312109862018
        HSM Model ->            LunaVirtual
        HSM Firmware Version -> 7.7.1
        HSM Configuration ->    Luna Virtual HSM (PW) Key Export With Cloning
Mode
        HSM Status ->           N/A - HA Group

        Current Slot Id: 0
lunacm:>
```

5. For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

> **NOTE:** Refer to Luna HSM documentation for detailed steps about creating NTLS connection, initializing the partitions, and assigning various user roles.

> **NOTE**: For PED-based Luna HSM ,ensure that ProtectedAuthenticationPathFlagStatus is set to ‘1’ in the Misc Section of Chrystoki.conf file.

Set up Luna HSM High-Availability

Refer to Luna HSM documentation for HA steps and details regarding configuring and setting up two or more HSM boxes on host systems. You must enable the HAOnly setting in HA for failover to work so that if the primary goes down due to any reason all calls automatically route to the secondary until the primary recovers and starts up.

Set up Luna HSM in FIPS Mode

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

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

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

> **NOTE:** The above setting is not required for Universal Client. This setting is applicable only for Luna Client 7.x.

Configure Luna Cloud HSM Service

You can configure Luna Cloud HSM Service in the following ways:

> Standalone Cloud HSM service using minimum client package

> Standalone Cloud HSM service using full Luna client package

> Luna HSM and Luna Cloud HSM service in hybrid mode

> **NOTE:** Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Standalone Cloud HSM service using minimum client package

To configure Luna Cloud HSM service using minimum client package:

1. Transfer the downloaded .zip file to your Client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

   ```
   [Windows]
   cvclient-min.zip
   [Linux]
   cvclient-min.tar
   # tar -xvf cvclient-min.tar
   ```

4. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

   ```
   [Windws]
   Right-click setenv.cmd and select Run as Administrator.
   [Linux]
   Source the setenv script.
   # source ./setenv
   ```

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

Standalone Cloud HSM service using full Luna client package

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

1. Transfer the downloaded .zip file to your Client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

   ```
   [Windows]
   cvclient-min.zip
   ```

```
[Linux]
cvclient-min.tar
# tar -xvf cvclient-min.tar
```

4. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

   ```
   [Windows]
   Right-click setenv.cmd and select Run as Administrator.
   [Linux]
   Source the setenv script.
   # source ./setenv
   ```

5. Copy the server and partition certificates from the Cloud HSM service client directory to Luna client certificates directory:

   Cloud HSM Certificates:

   ```
   server-certificate.pem
   partition-ca-certificate.pem
   partition-certificate.pem
   ```

   LunaClient Certificate Directory:

   ```
   [Windows default location for Luna Client]
   C:\Program Files\Safenet\Lunaclient\cert\
   [Linux default location for Luna Client]
   /usr/safenet/lunaclient/cert/
   ```

   > **NOTE:** Skip this step for Luna Client v10.2 or higher.

6. Open the configuration file from the Cloud HSM service client directory and copy the XTC and REST section.

   ```
   [Windows]
   crystoki.ini
   [Linux]
   Chrystoki.conf
   ```

7. Edit the Luna Client configuration file and add the XTC and REST sections copied from Cloud HSM service client configuration file.

8. Change server and partition certificates path from step 5 in XTC and REST sections. Do not change any other entries provided in these sections.

   [XTC]

```
. . .
PartitionCAPath=<LunaClient_cert_directory>\partition-ca-certificate.pem
PartitionCertPath00=<LunaClient_cert_directory>\partition-certificate.pem
. . .
```

```
[REST]
. . .
SSLClientSideVerifyFile=<LunaClient_cert_directory>\server-certificate.pem
. . .
```

> **NOTE:** Skip this step for Luna Client v10.2 or higher.

9. Edit the following entry from the Misc section and update the correct path for the plugins directory:

```
Misc]
PluginModuleDir=<LunaClient_plugins_directory>
```

```
[Windows Default]
```

```
C:\Program Files\Safenet\Lunaclient\plugins\
```

```
[Linux Default]
```

```
/usr/safenet/lunaclient/plugins/
```

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

11. Reset the ChrystokiConfigurationPath environment variable and point back to the location of the Luna Client configuration file.

    Windows: In the Control Panel, search for "environment" and select Edit the system environment variables. Click Environment Variables. In both list boxes for the current user and system variables, edit ChrystokiConfigurationPath and point to the crystoki.ini file in the Luna client install directory.

    Linux: Either open a new shell session, or export the environment variable for the current session pointing to the location of the Chrystoki.conf file:

    ```
    # export ChrystokiConfigurationPath=/etc/
    ```

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

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

Set up Luna HSM and Luna Cloud HSM service in hybrid mode

To configure Luna HSM and Luna Cloud HSM service in hybrid mode, follow the steps mentioned under the Standalone Cloud HSM service using full Luna client package section above.

> **NOTE:** Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Set up Luna Cloud HSM Service in FIPS mode

Cloud HSM service operates in both FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, enable the Allow non-FIPS approved algorithms check box when configuring your Cloud HSM service. The FIPS mode is enabled by default. Refer to the Mechanism List in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Set up Microsoft NDES

1. Use the following machines to set up Microsoft NDES service:
   - A Windows Server machine that will become Microsoft NDES server, also referred to as APP1 in the setup.
   - A Windows Server machine that will become a domain controller and CA, also referred to as DC1 in the setup.
2. Install the ADDS role on DC1 and join APP1 to the domain. This guide uses integration.com as an example for the domain.

> **NOTE:** You can find detailed information on Microsoft NDES on this Microsoft Wiki page.

Register Security Library

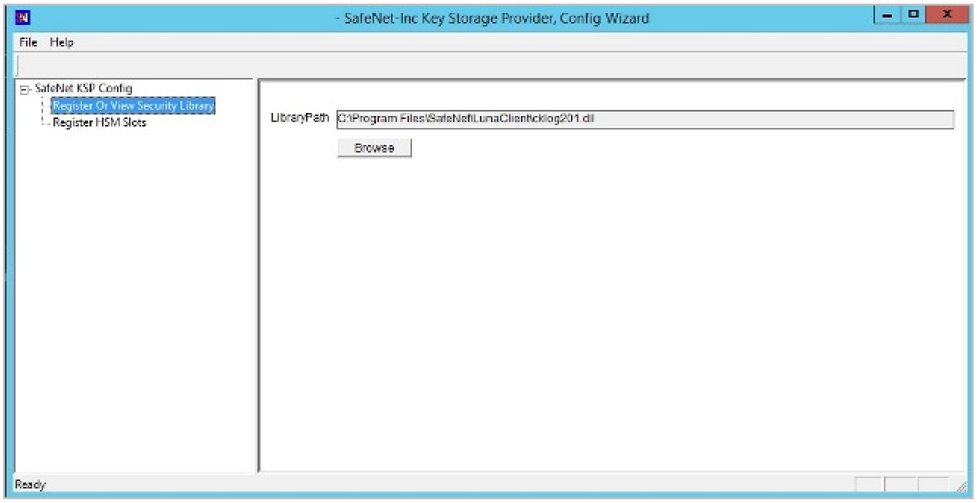
Install SafeNet KSP for generating the CA certificate keys on Luna HSM or Luna Cloud HSM. Refer to Register SafeNet Key Storage Provider section below for more information about configuring and registering SafeNet KSP. The tool KspConfig.exe is included in the Luna Client installation directory or is available in the DPoD service client package.

You can use SafeNet CSP to generate the Microsoft NDES signing keys. To use SafeNet CSP for Microsoft NDES signing keys, you also need to register SafeNet CSP. See Register the SafeNet CSP section for more information about configuring and registering SafeNet CSP.

Register SafeNet Key Storage Provider

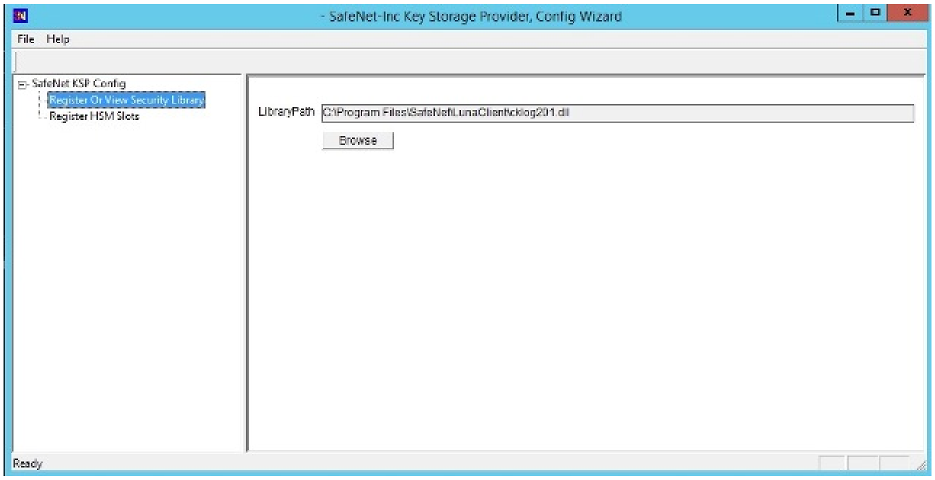
To register the SafeNet Key Storage provider:

1. Navigate to the KSP installation directory. Execute **KspConfig.exe**.
2. Double-click **Register Or View Security Library** on the left side of the pane.


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

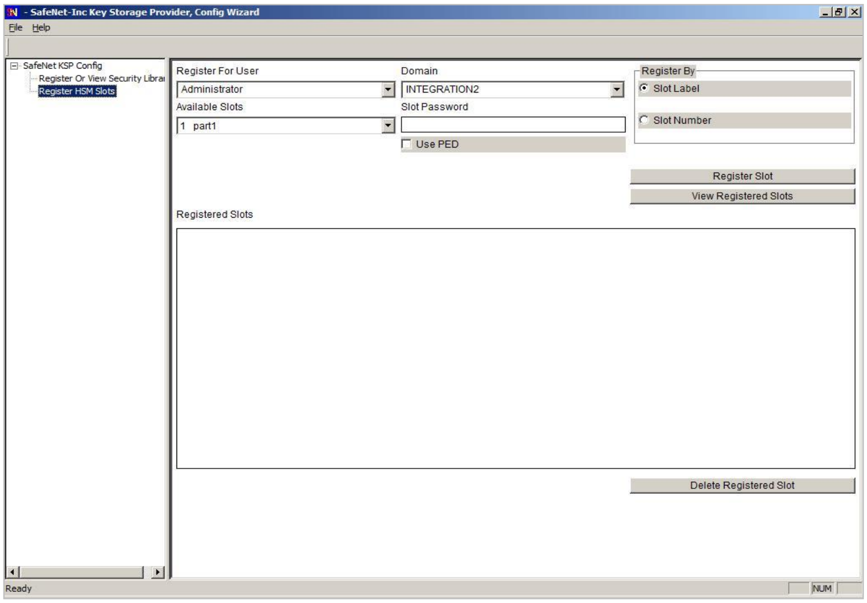
LibraryPath: C:\Program Files\SafeNet\LunaClient\cklog201.dll

3. Click **Browse.** Select the cryptoki.dll file, available in the Luna Client installation folder or Luna Cloud HSM service client package. Click **Register.**


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

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

4. On successful registration a confirmation message appears on the screen. Click **OK**.
5. Double-click **Register HSM Slots** on the left side of the pane.
6. Register the slot for the Administrator user as follows:
   a. Open the **Register for User** drop-down menu and select **ADMINISTRATOR**.
   b. Open the **Domain** drop-down menu and select your domain
   c. Open the **Available Slots** drop-down menu and select the relevant service or partition.
   d. Enter the **Slot Password**
   e. Click **Register Slot**.
   f. On successful registration, a confirmation message will appear on the screen. Click **OK**.



Register For User: Administrator

Domain: INTEGRATION2

Available Slots: 1 part1

Slot Password:

□ Use PED

Register By: ● Slot Label ○ Slot Number

7. Register the same service or partition for the **NT_AUTHORITY\SYSTEM** user.

Register the SafeNet CSP

To register the SafeNet CSP, SafeNet Luna CSP should be installed on the Microsoft NDES Server machine. The steps involved are as follows:

1. Log on to the Microsoft NDES Server as domain administrator.
2. Run the command register.exe to register Luna CSP. The general form of command is:

   C:\Program Files\SafeNet\LunaClient\CSP>register.exe
3. Provide the partition password when asked.
4. List the Luna Cryptographic Services for Microsoft Windows and verify that the Luna CSP is available:

   C:\Program Files\SafeNet\LunaClient\CSP>register.exe /l
5. Restart the server for the changes to take effect.

> **NOTE:** You need to register the SafeNet KSP on Microsoft NDES Server (APP1) also, if you want to configure SSL for delivering challenge password securely for device certificate enrollment. Perform the above steps on APP1 server also, else binding of SSL certificate failed.

Integrating Microsoft NDES with Luna HSM and Luna Cloud HSM

Following are the steps involved in integrating Microsoft NDES with Luna HSM or Luna Cloud HSM:

Setting up an enterprise root certificate authority

Installing Microsoft NDES role

Creating user account to enroll X.509 certificate

Configuring Microsoft NDES

Adding roles and features

Performing AD CS configuration

Setting up new templates for enrollment certificates

Configuring templates for certificate enrollment

Configuring IIS to use SSL to deliver the challenge password for certificate enrollment

Verifying Microsoft NDES

Setting up an enterprise root certificate authority

An enterprise root CA is used to issue certificates to the Microsoft NDES service that was requested by the Network Device like routers and VPN, and publish certificate information to the Active Directory Domain Services (ADDS). It is assumed that you have installed the ADDS on the DC1 and join the APP1 to the integration.com domain.

1. Log on to DC1 as a domain administrator.
2. From the Start menu, select **Administrative Tools > Server Manager**.

3. In the Server Manager Dashboard (in the right-hand part of the window), click **Manage > Add Roles and Features**.
4. In the **Add Roles and Features** Wizard, click **Next** on Before You Begin page.
5. Select **Role-based or feature-based installation** on Installation Type page and click **Next**.
6. On the Server Selection screen, click **Select a server from the server pool** and select the listed server then click **Next**.
7. Select **Active Directory Certificate Services** in Roles list and click **Add Features** on the pop up window to add required features on the Server Roles page and click **Next**.
8. Click **Next** on the Features page.
9. Click **Next** on the ADCS page.
10. On the **Role Services** page, select **Certificate Authority** and **Certificate Authority Web Enrollment** from the **Role Services** list. A pop up will show to add required features.
11. Click on **Add Features** and click **Next**.
12. Click **Next** on the **Web Server Role (IIS)** page.
13. Click **Next** on the **Role Services** page.
14. Select **Restart the destination server automatically if required**, a confirmation message will appear, click **Yes**.
15. Click **Install** on the Confirmation page and wait to finish the installation.
16. Click **Configure Active Directory Certificate Server on the destination server**. You can close the wizard and open the Configuration Wizard by clicking the Notification Flag in the right hand corner.
17. In the AD CS Configuration wizard click Next on the Credentials page.
18. Select **Certificate Authority** and **Certification Authority Web Enrollment** on the **Role Services** page and click **Next**.
19. Select **Enterprise CA** on the Setup Type page and click **Next**.
20. Select **Root CA** on the CA Type page and click **Next**.
21. Select **Create a new private key** on the Private Key page and click **Next**.
22. In the Cryptography for CA section, select and set up the provider you wish to use for the CA.
23. The following SafeNet providers are available for use (if they are installed and correctly set up, they will be displayed in the drop-down list under the Select a Cryptographic Provider heading):
    - RSA#SafeNet Key Storage Provider
    - DSA#SafeNet Key Storage Provider
    - ECDSA_P256#SafeNet Key Storage Provider
    - ECDSA_P384#SafeNet Key Storage Provider
    - ECDSA_P521#SafeNet Key Storage Provider

> **NOTE:** When using SafeNet providers, ensure that you use an ‘sha’ hashing algorithm. Provider list may differ for different client version.
>
> **NOTE:** Make sure that you have registered the Luna KSP on CA server.

24. Once the provider has been selected and set up on the Cryptography page, click **Next**.
25. Enter the CA Name or accept default on the CA Name page and click **Next**.
26. Specify the **Certificate Validity Period** on Validity Period page and click **Next**.
27. Specify the **Certificate Database location** or accept defaults on Certificate Database page and click **Next**.
28. Finally on the Confirmation page, click **Configure** and wait for the confirmation message. When everything is correct Configuration succeeded message will display.
29. Click **Close** on the Result page to close the AD CS Configuration wizard.

Installing Microsoft NDES role

Install the Microsoft NDES role on your server. Microsoft NDES (Network Device Enrollment Service) is Microsoft implementation of SCEP (Simple Certificate Enrollment Protocol) and is normally used to enroll X.509 certificates to devices that are unable to use a web browser to request a certificate but which require a certificate for authentication. Think about network devices like routers, switches and firewalls. There are two roles related to setting up and running the service:

Service Administrator

Service Account

Service Administrator

The user who logs on the service machine and installs the Network Device Enrollment Service. This user is referred to as **SCEPAdmin**. The permissions required for the CEPAdmin are:

- Must be part of the local administrators group.
- For setting up the service with an Enterprise CA, this user should have the following permissions as well.
  - Must have Enroll permission on the “Exchange Enrollment Agent (Offline request)” and “CEP Encryption” templates.
  - Must have permissions to add templates to the selected CA.
  - Must be a member of the Enterprise Administrator group (or have permissions to modify certificate templates).

Service Account

The credentials that will be used to run the service. This user is referred to as **SCEPSvc**. The following are the permissions required for SCEPSvc:

- Must be a member of the local IIS_IUSRS group.
- Must have request permission on the configured CA.
- Must be a domain user account and have Read AND Enroll permissions on the configured templates. For more information about the configured template, see CONFIGURING TEMPLATES FOR DEVICE ENROLLMENT.
- Must have SPN set in Active Directory.

Creating user account to enroll X.509 certificate

To create a user account for enrolling X.509 certificate:

1. Log on to the DC1 as a domain controller.
2. Click **Start > Administrative Tools > Active Directory Users and Computers**.
3. In the **Users** folder, right click and select **New User**. The new user will be called "SCEPAdmin". Click **Next** to continue.
4. Enter a strong password and click **Next.**
5. Click **Finish**.
6. Create another user called "SCEPSvc" using steps 2, 3, and 4 above.
7. Add the SCEPAdmin to the Enterprise Admin group.
8. Click **Start > Administrative Tools > Certificate Authority**.
9. Right click on the CA and click **Properties**.
10. Click **Security** tab and click **Add**, type **SCEPSvc** and click **OK**.
11. Select **SCEPSvc** in Group or user name and select **Read and Request Certificate permission**.
12. Restart the CA, Click **OK**, and close the Certificate Authority window.
13. Set SPN for SCEPSvc in Active Directory by executing the following command:

    ```
    setspn -s http/APP1.Integration.com Integration\SCEPSvc
    ```

14. Log on to the APP1 as Domain Administrator.
15. Click **Start > Computer Management > Local Users and Groups**.
16. In the Groups, right-click on the Administrators and select Add to group…
17. Click Add, type SCEPAdmin and click OK twice to close the properties window.
18. In the Groups right click on the IIS_IUSRS and select Add to group…
19. Click Add, type SCEPSvc and click OK twice to close the properties window.
20. Log off from the APP1.

Configuring Microsoft NDES

The following conditions must be verified before you begin the Microsoft NDES configuration process:

1. The issuing CA must be online.
2. The following templates must exist on the domain controller.
   a. Exchange Enrollment Agent (Offline requests)
   b. CEP Encryption
3. The user who's logged on must be a member of the Enterprise Administrator group.
4. Luna Client is installed and Luna CSP is registered.
5. The service certificates are enrolled. The Microsoft NDES service uses two certificates for two different scenarios. During setup, the service enrolls for the two service certificates based on two preconfigured certificate templates.

- **Enrollment agent certificate:** This certificate is used to send the enrollment request to the CA. It is enrolled using the Exchange Enrollment Agent (Offline request) template**.**
- **Key Exchange certificate:** This certificate is used by the device to encrypt all the communication with the service (essential for transmitting the password). It is enrolled using the **CEP Encryption template.**

> **NOTE:** These certificate templates are hard-coded to the Network Device Enrollment Service set up and cannot be modified.

In addition, set up will set the required permissions on the Certificate Template object and the CA that the service is configured with, for example, adding the required Certificate Templates to the list of templates supported by the CA.

Adding Roles and Features

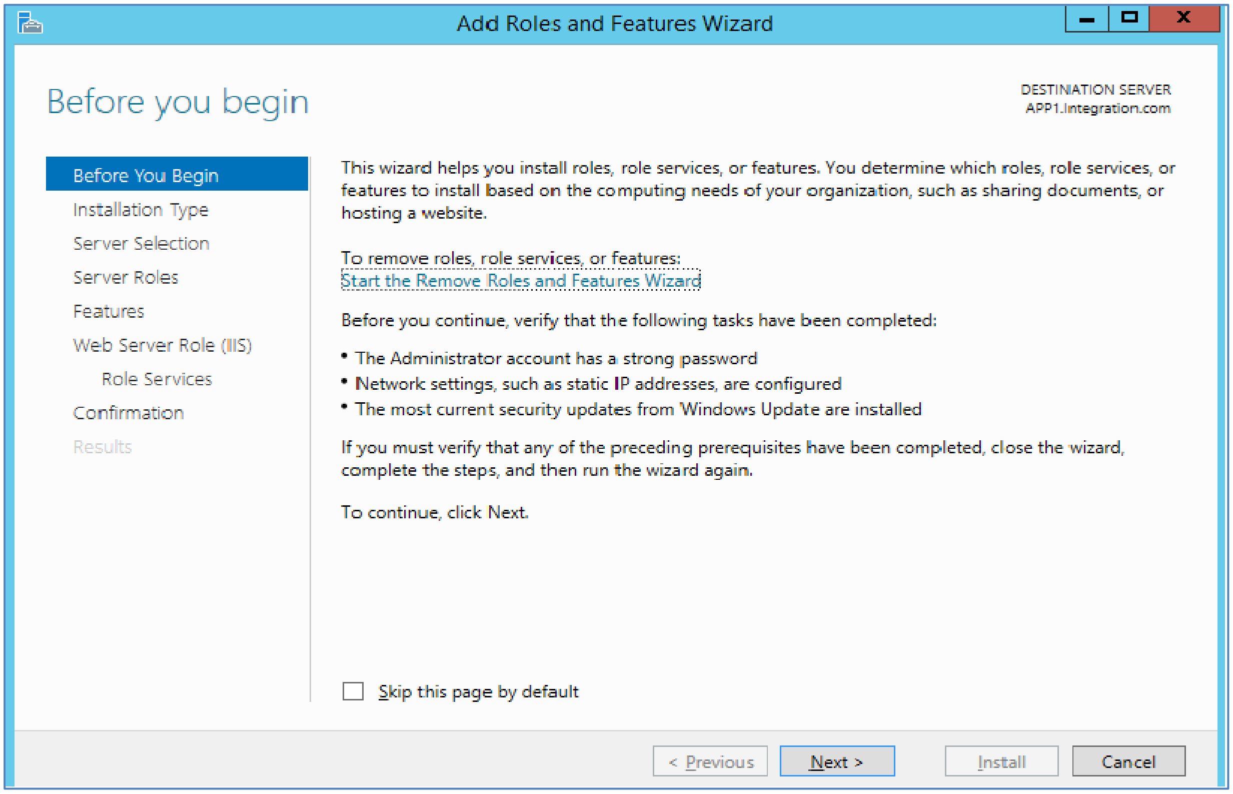
Installing and configuring the Network Device Enrollment Service are done through the Add Roles Wizard. This wizard collects the required information for installing Windows Server Roles.

1. Log on to APP1 as SCEPAdmin account.

   From the **Start** menu, select **Administrative Tools > Server Manager**.

2. In the Server Manager Dashboard (in the right-hand part of the window), click **Manage > Add Roles and Features**. The **Add Roles and Features Wizard** window will appear on the screen.

3. Select **Before You Begin** option from the left navigation pane and click **Next**.



Add Roles and Features Wizard

Before you begin

DESTINATION SERVER
APP1.Integration.com

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

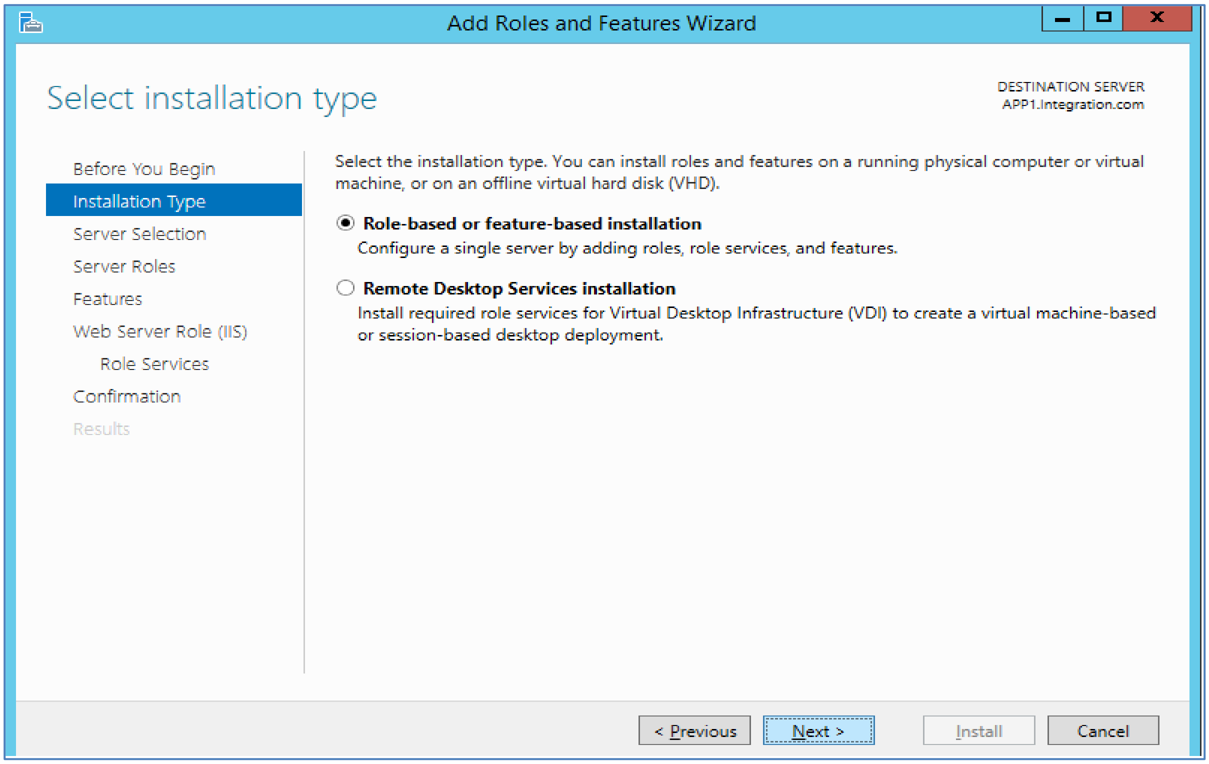
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

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.

☐ Skip this page by default

4. Select Role based or feature based installation and click **Next**.



Add Roles and Features Wizard

Select installation type

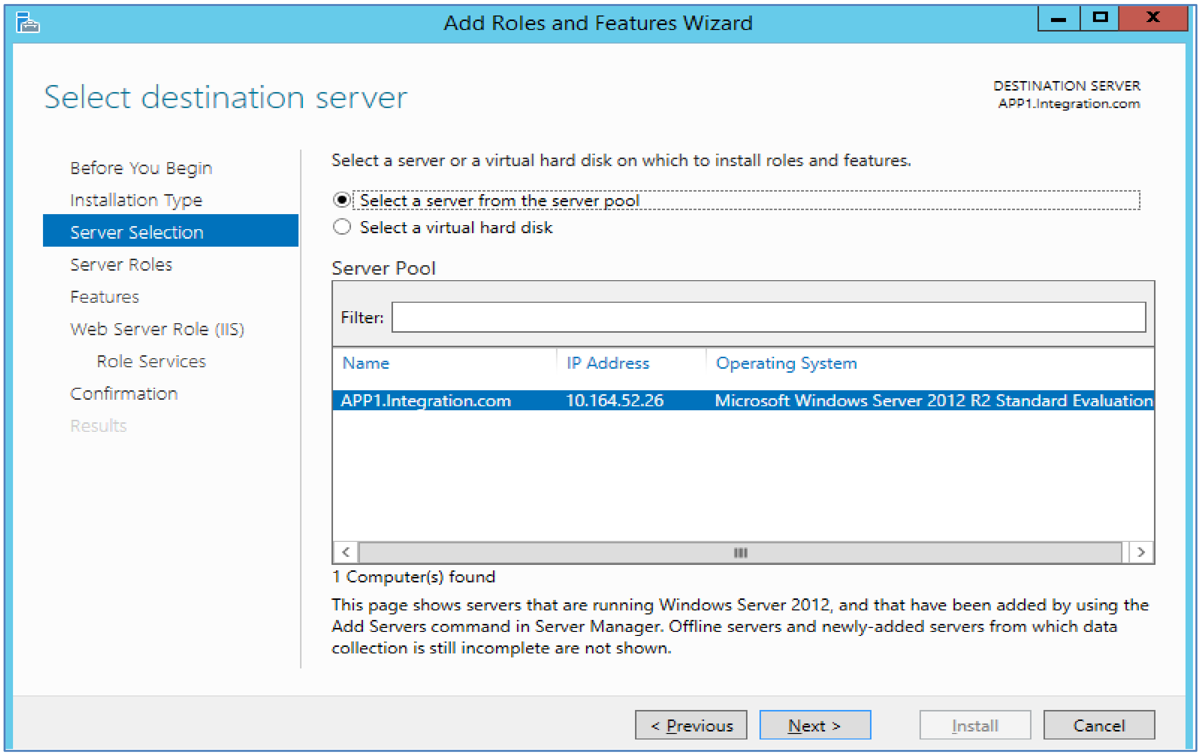
DESTINATION SERVER
APP1.Integration.com

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

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

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

5. Click **Next** on the **Server Selection** page.



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
APP1.Integration.com

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

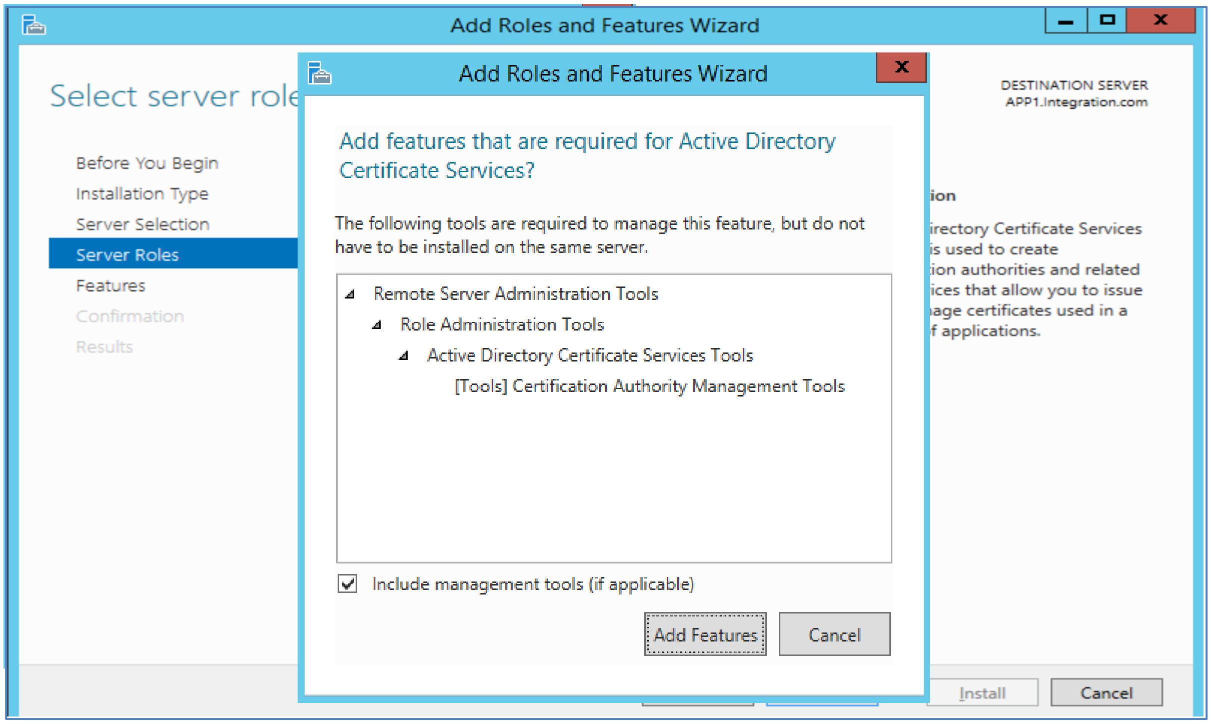
Filter:

Name	IP Address	Operating System
APP1.Integration.com	10.164.52.26	Microsoft Windows Server 2012 R2 Standard Evaluation

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.

6. Select **Active Directory Certificate Services** Role. It will prompt to add required role services, click on **Add Features**. Click **Next**.



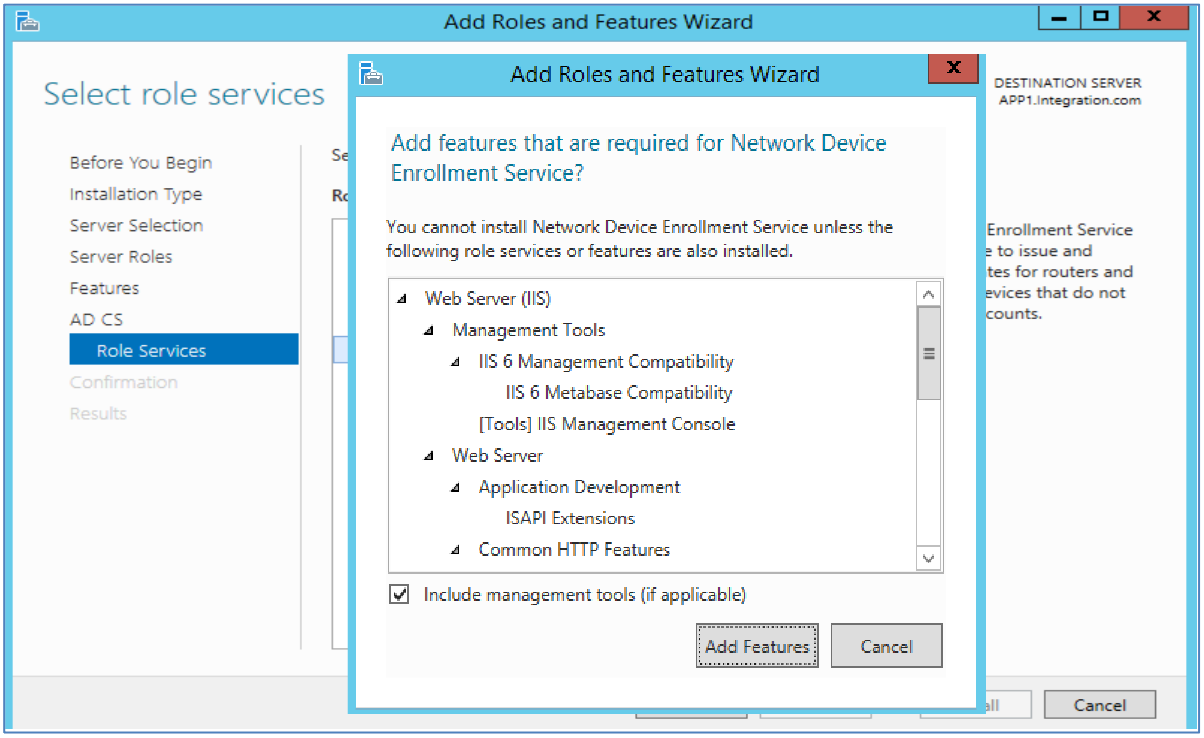
Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

```
◢ Remote Server Administration Tools
    ◢ Role Administration Tools
        ◢ Active Directory Certificate Services Tools
              [Tools] Certification Authority Management Tools
```

☑ Include management tools (if applicable)

7. Uncheck **Certificate Authority** and select **Network Device Enrollment Service** on **Role Services** page. It will prompt to add required role services, click on **Add Features**. Remove any other services if selected.



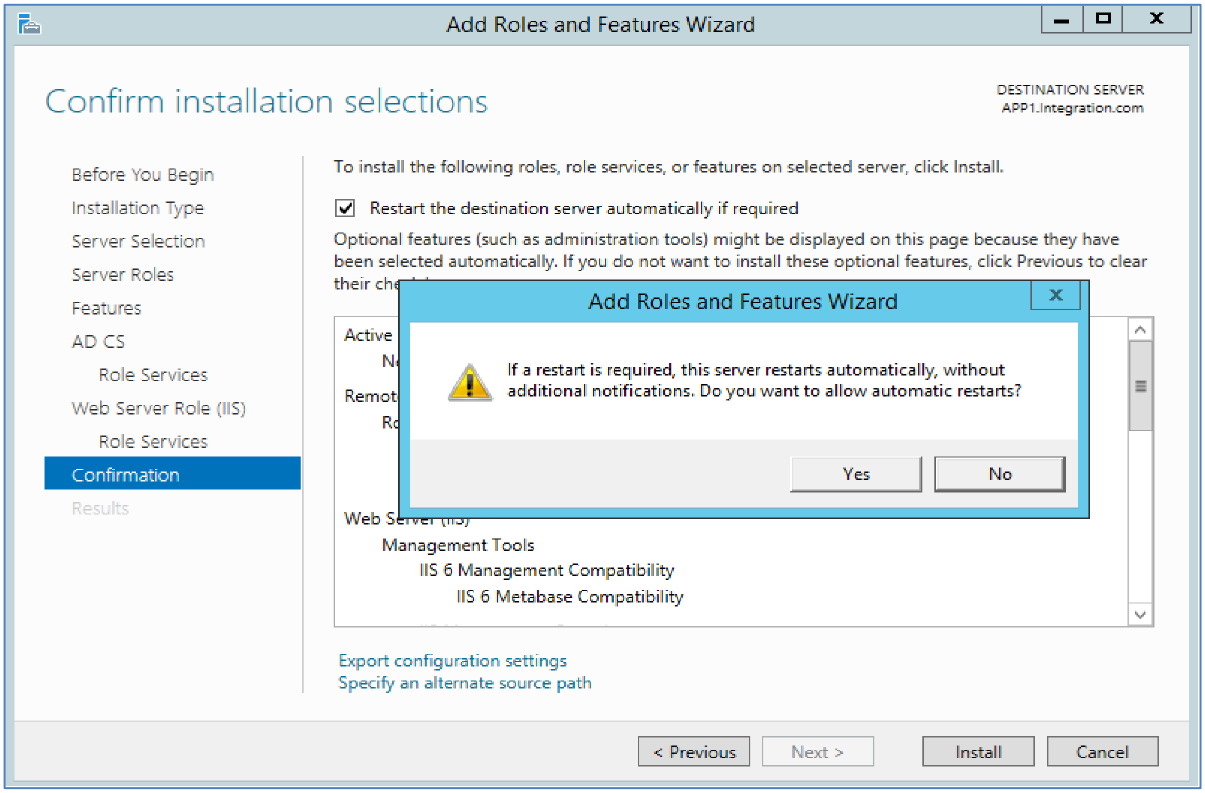
Add features that are required for Network Device Enrollment Service?

You cannot install Network Device Enrollment Service unless the following role services or features are also installed.

```
◢ Web Server (IIS)
    ◢ Management Tools
        ◢ IIS 6 Management Compatibility
              IIS 6 Metabase Compatibility
          [Tools] IIS Management Console
    ◢ Web Server
        ◢ Application Development
              ISAPI Extensions
        ◢ Common HTTP Features
```

☑ Include management tools (if applicable)

8. Click **Next** three times. Select restart destination server if required and click yes when prompt.



Confirm installation selections

DESTINATION SERVER
APP1.Integration.com

To install the following roles, role services, or features on selected server, click Install.

☑ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their che

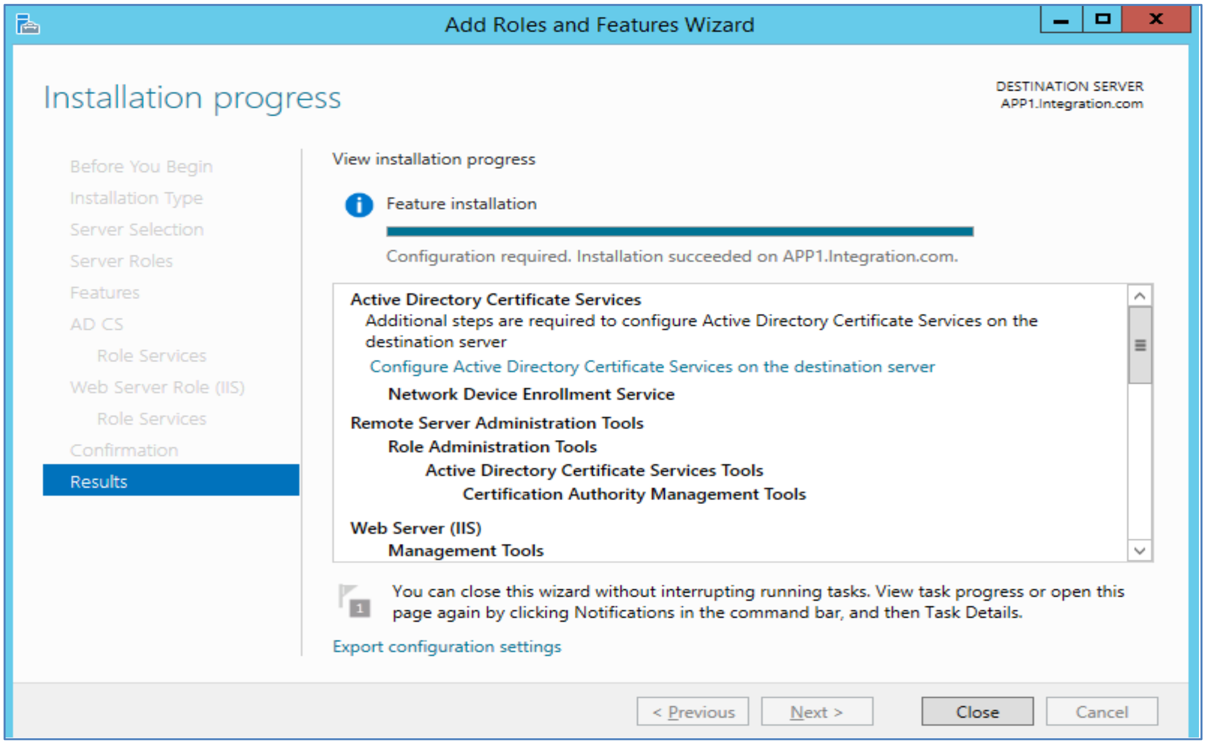
Add Roles and Features Wizard

If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?

Active
N
Remot
Ro
Web Server (IIS)
Management Tools
IIS 6 Management Compatibility
IIS 6 Metabase Compatibility

Export configuration settings
Specify an alternate source path

9. Click install and wait for installation to complete. When installation completes, click **Configure Active Directory Certificate Services** on the destination server.



Installation progress

DESTINATION SERVER
APP1.Integration.com

View installation progress

Feature installation

Configuration required. Installation succeeded on APP1.Integration.com.

Active Directory Certificate Services
Additional steps are required to configure Active Directory Certificate Services on the destination server
Configure Active Directory Certificate Services on the destination server
Network Device Enrollment Service
Remote Server Administration Tools
Role Administration Tools
Active Directory Certificate Services Tools
Certification Authority Management Tools
Web Server (IIS)
Management Tools

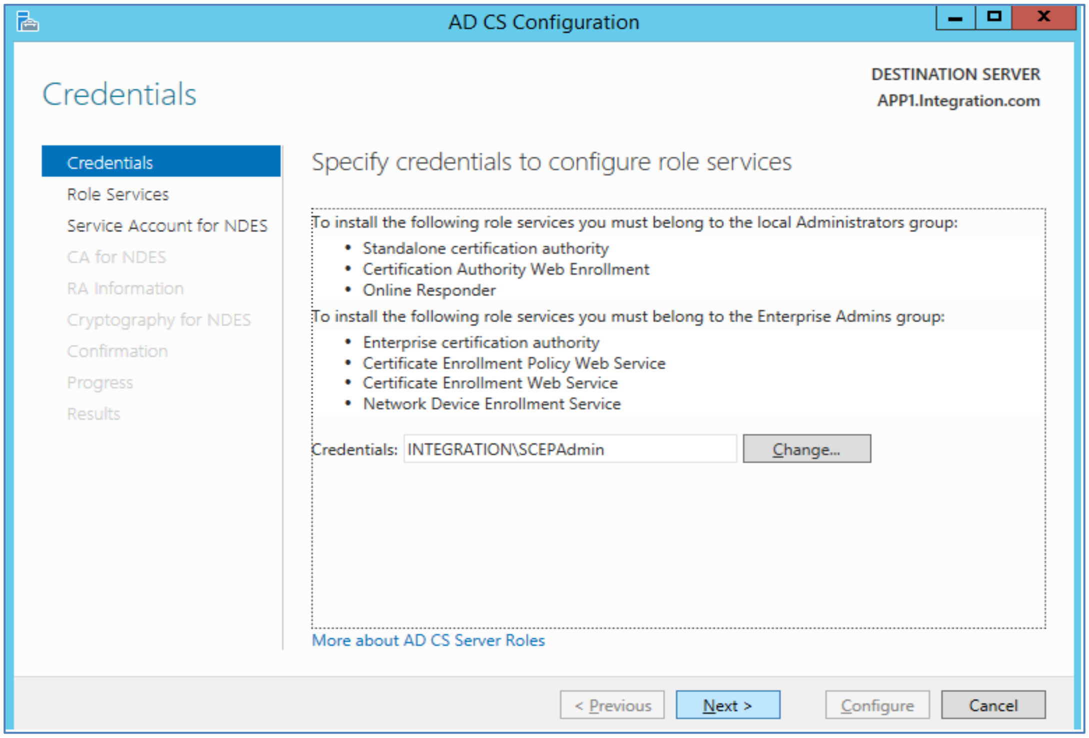
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Performing AD CS Configuration

To perform AD CS configuration:

1. Click **Next** on the Credentials page.



Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

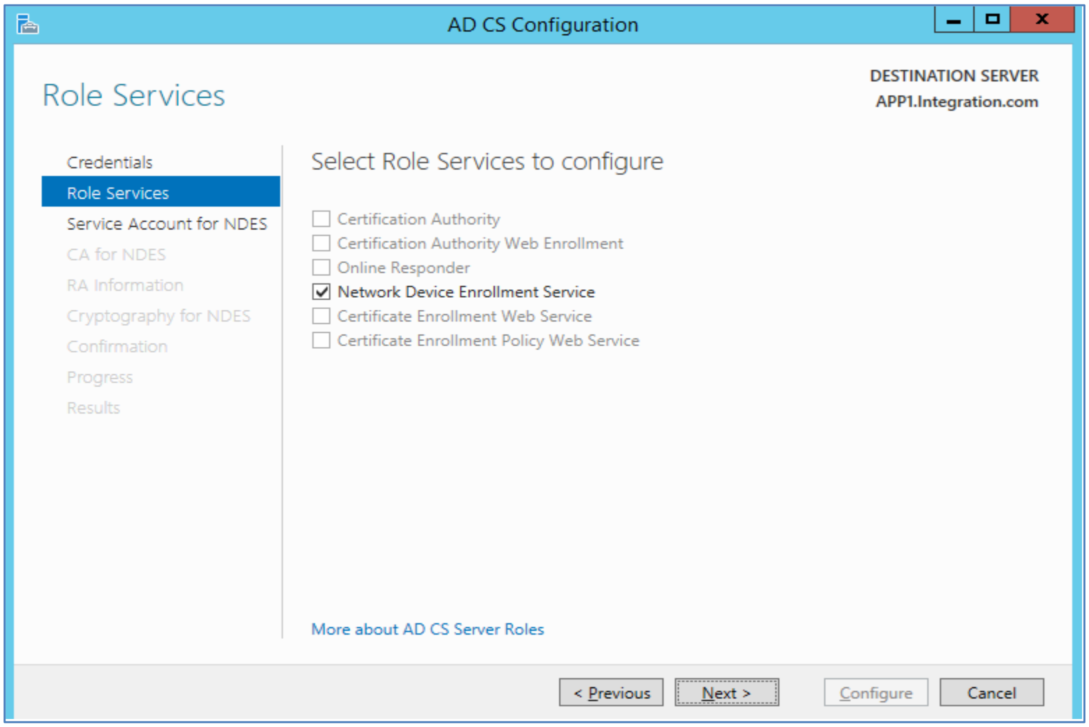
- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: INTEGRATION\SCEPAdmin

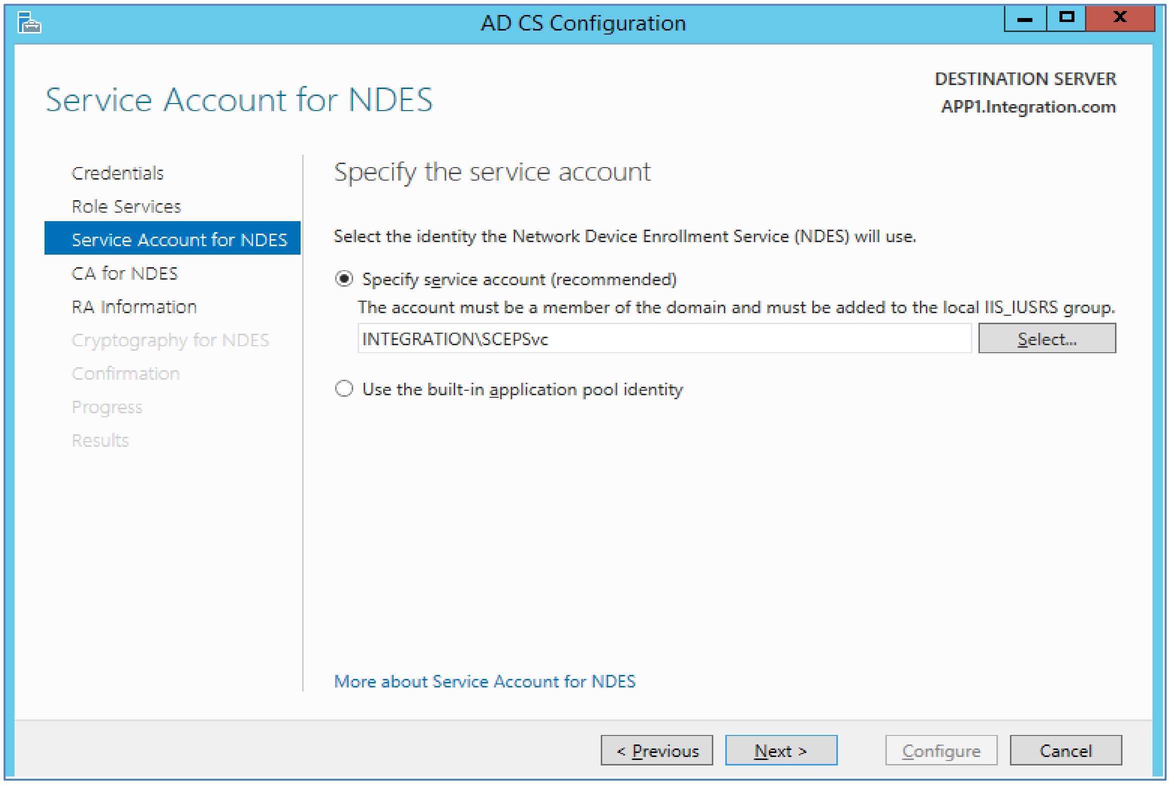
2. Select **Network Device Enrollment Service** and click **Next.**



Select Role Services to configure

□ Certification Authority
□ Certification Authority Web Enrollment
□ Online Responder
☑ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service

3. Click **Select** to add the SCEPSvc account in the Specify Service Account page and click **Next**.



Specify the service account

Select the identity the Network Device Enrollment Service (NDES) will use.

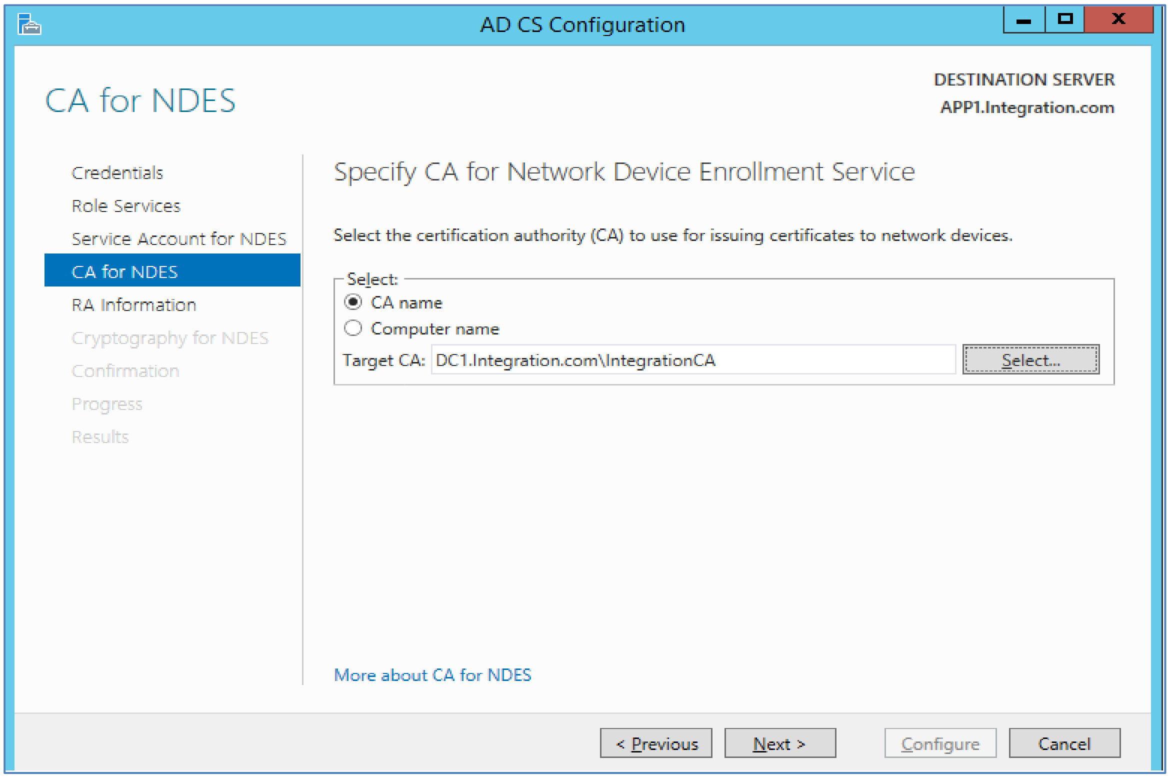
● Specify service account (recommended)

The account must be a member of the domain and must be added to the local IIS_IUSRS group.

INTEGRATION\SCEPSvc [Select...]

○ Use the built-in application pool identity

4. Click **Select** to add the CA Name on Specify CA for Microsoft NDES page and click **Next**.



Specify CA for Network Device Enrollment Service

Select the certification authority (CA) to use for issuing certificates to network devices.

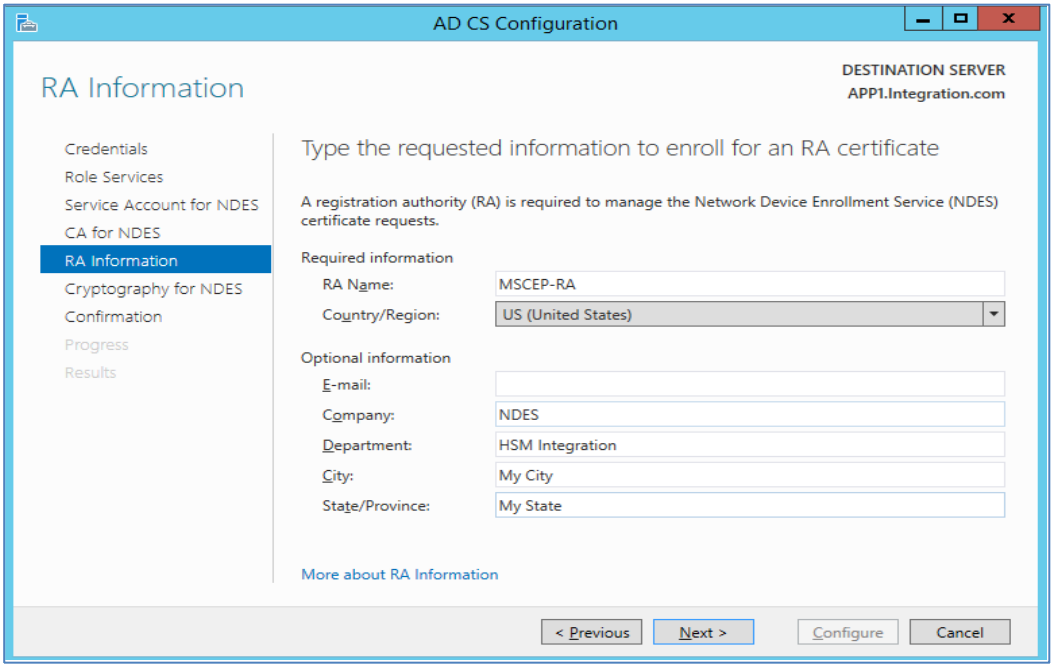
Select:

● CA name

○ Computer name

Target CA: DC1.Integration.com\IntegrationCA [Select...]

5. Enter the RA details on RA Information page and click **Next**.



RA Information

DESTINATION SERVER
APP1.Integration.com

Type the requested information to enroll for an RA certificate

A registration authority (RA) is required to manage the Network Device Enrollment Service (NDES) certificate requests.

Required information

RA Name: MSCEP-RA

Country/Region: US (United States)

Optional information

E-mail:

Company: NDES

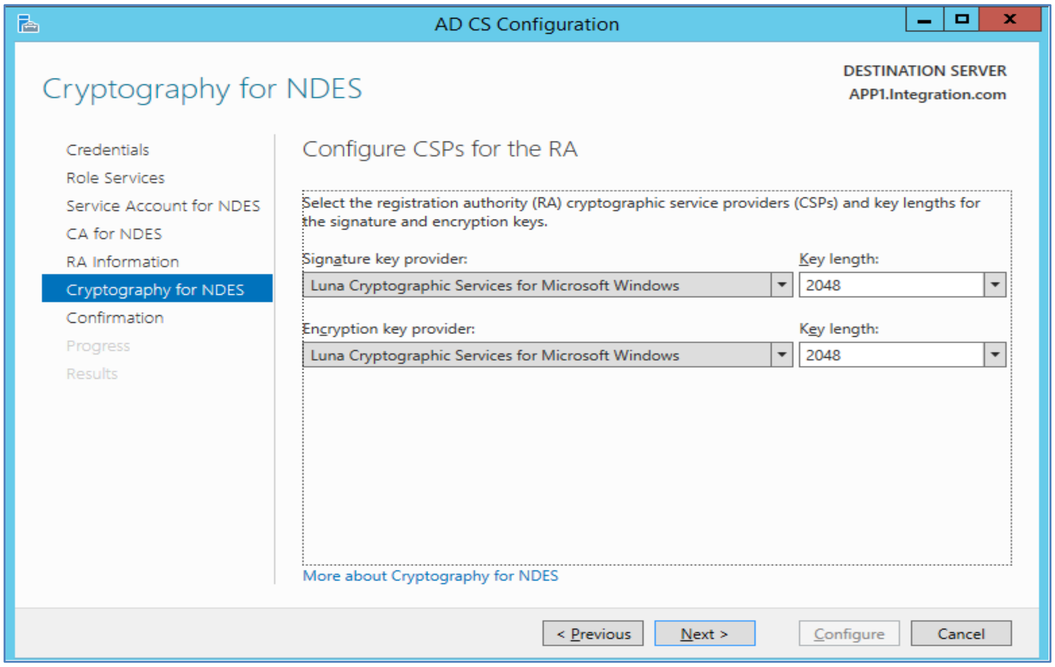
Department: HSM Integration

City: My City

State/Province: My State

6. Select **Luna Cryptographic Services for Microsoft Windows** for Signature key provider and Encryption key provider and select the Key length. Click **Next**.

> **NOTE:** Make sure that you have registered the Luna CSP on Microsoft NDES server using the steps mentioned in Before You Begin section.



Cryptography for NDES

DESTINATION SERVER
APP1.Integration.com

Configure CSPs for the RA

Select the registration authority (RA) cryptographic service providers (CSPs) and key lengths for the signature and encryption keys.

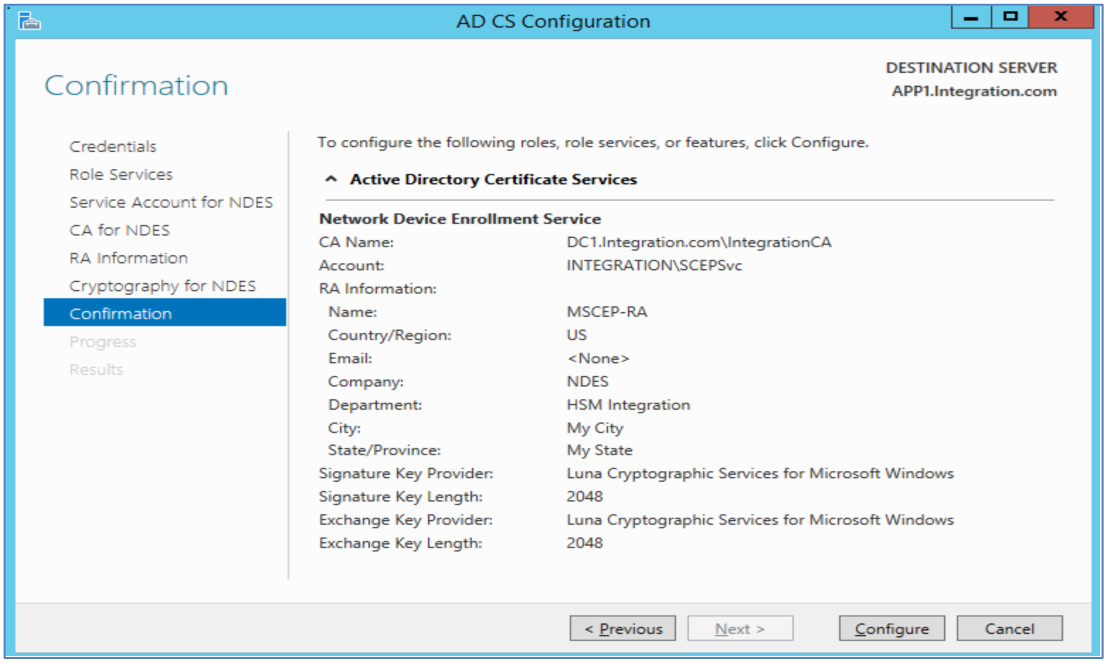
Signature key provider: Luna Cryptographic Services for Microsoft Windows

Key length: 2048

Encryption key provider: Luna Cryptographic Services for Microsoft Windows

Key length: 2048

7. Click **Configure** on the confirmation page.



DESTINATION SERVER
APP1.Integration.com

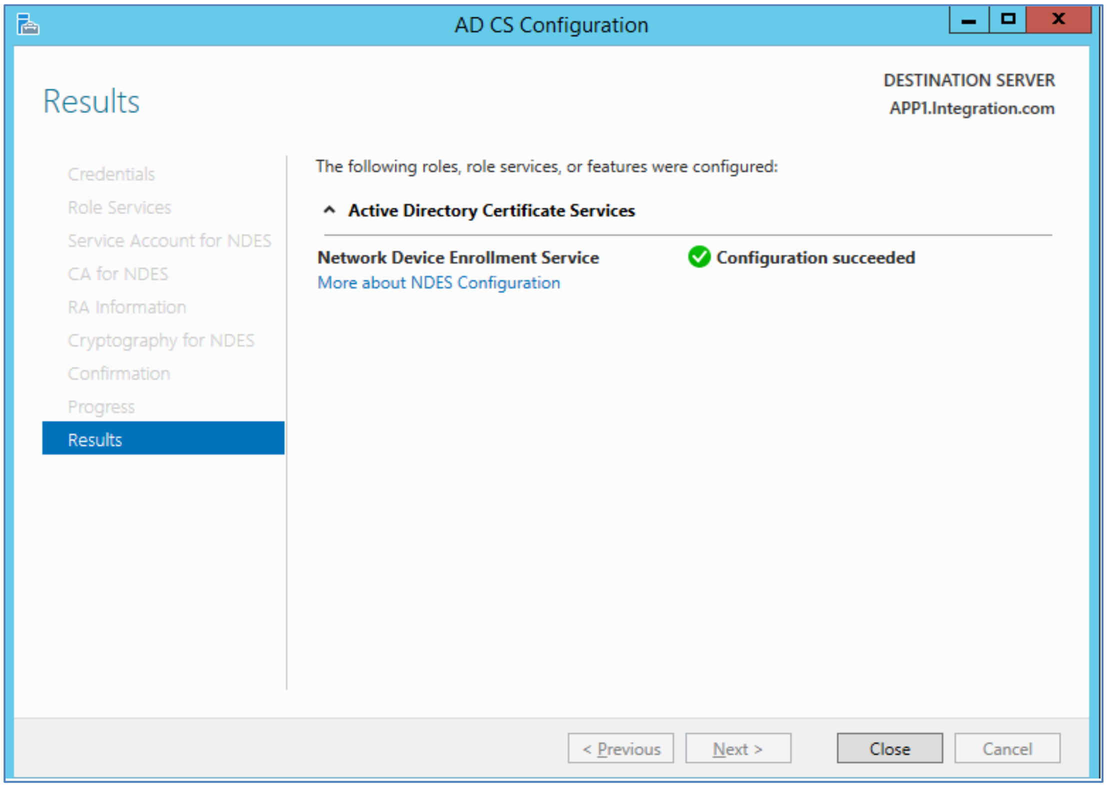
To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Network Device Enrollment Service

CA Name:	DC1.Integration.com\IntegrationCA
Account:	INTEGRATION\SCEPSvc
RA Information:	
Name:	MSCEP-RA
Country/Region:	US
Email:	<None>
Company:	NDES
Department:	HSM Integration
City:	My City
State/Province:	My State
Signature Key Provider:	Luna Cryptographic Services for Microsoft Windows
Signature Key Length:	2048
Exchange Key Provider:	Luna Cryptographic Services for Microsoft Windows
Exchange Key Length:	2048

8. Wait for installation to complete, click Close when Configuration succeeded.



DESTINATION SERVER
APP1.Integration.com

The following roles, role services, or features were configured:

Active Directory Certificate Services

Network Device Enrollment Service ✓ **Configuration succeeded**

9. See the contents of HSM partition to verify the keys generated for Microsoft NDES.

```
lunacm:> par con

           The 'Crypto Officer' is currently logged in. Looking for
   objects
           accessible to the 'Crypto Officer'.

           Object list:

           Label:         X-te-0e181a8e-3478-4efd-a5a0-46bd5f89faef
           Handle:        881
           Object Type:   Private Key
           Usage Limit:   none
           Object UID:    41090000590000025b990800

           Label:         X-te-0e181a8e-3478-4efd-a5a0-46bd5f89faef
           Handle:        859
           Object Type:   Public Key
           Usage Limit:   none
           Object UID:    40090000590000025b990800

           Label:         te-0e181a8e-3478-4efd-a5a0-46bd5f89faef
           Handle:        752
           Object Type:   Data
           Object UID:    3f090000590000025b990800

           Label:         S-te-fa4937d0-39c6-4151-9340-3b7792ba18f9
           Handle:        858
           Object Type:   Private Key
           Usage Limit:   none
           Object UID:    3e090000590000025b990800

           Label:         S-te-fa4937d0-39c6-4151-9340-3b7792ba18f9
           Handle:        785
           Object Type:   Public Key
           Usage Limit:   none
           Object UID:    3d090000590000025b990800

           Label:         te-fa4937d0-39c6-4151-9340-3b7792ba18f9
           Handle:        524
           Object Type:   Data
           Object UID:    3c090000590000025b990800
```

10. You can also verify the keys generated by Luna CSP in provider field using the following command on command prompt:

    Certutil –verifystore My

```
C:\Users\Administrator>Certutil -verifystore My
My "Personal"
================ Certificate 0 ================
Serial Number: 6c000000033ccd33f602284ed6000000000003
Issuer: CN=integration-DC1-CA, DC=integration, DC=com
 NotBefore: 26-04-2022 17:13
 NotAfter: 25-04-2024 17:13
```

```
Subject: CN=APP1-MSCEP-RA, OU=DIS, O=Thales, L=Noida, S=UP, C=IN
Certificate Template Name (Certificate Type): CEPEncryption
Non-root Certificate
Template: CEPEncryption, CEP Encryption
Cert Hash(sha1): a5 84 aa d8 04 46 d9 b9 44 22 c5 55 34 1f 84 4c 82 b8 f7
5a
  Key Container = te-0e181a8e-3478-4efd-a5a0-46bd5f89faef
  Provider = Luna Cryptographic Services for Microsoft Windows
Private key is NOT exportable
Encryption test passed
Verified Issuance Policies: None
Verified Application Policies:
    1.3.6.1.4.1.311.20.2.1 Certificate Request Agent
Certificate is valid

================ Certificate 1 ================
Serial Number: 6c00000002b03dd44694d011880000000000002
Issuer: CN=integration-DC1-CA, DC=integration, DC=com
 NotBefore: 26-04-2022 17:13
 NotAfter: 25-04-2024 17:13
Subject: CN=APP1-MSCEP-RA, OU=DIS, O=Thales, L=Noida, S=UP, C=IN
Certificate Template Name (Certificate Type): EnrollmentAgentOffline
Non-root Certificate
Template: EnrollmentAgentOffline, Exchange Enrollment Agent (Offline
request)
Cert Hash(sha1): 88 bd 77 39 26 24 16 02 79 73 d2 1b 2c e4 3c db 12 8f 6e
95
  Key Container = te-fa4937d0-39c6-4151-9340-3b7792ba18f9
  Provider = Luna Cryptographic Services for Microsoft Windows
Private key is NOT exportable
ERROR: Could not verify certificate public key against private key
Verified Issuance Policies: None
Verified Application Policies:
    1.3.6.1.4.1.311.20.2.1 Certificate Request Agent
Certificate is valid
CertUtil: -verifystore command completed successfully.

C:\Users\Administrator>
```

Microsoft NDES installation has been completed successfully and RA certificates keys are generated on Luna HSM.

Setting up new templates for enrollment certificates

The service uses two certificates. The encryption certificate is based on the “CEPEncryption” template, and the signature certificate is based on the “Exchange Enrollment Agent (Offline Request)” template. Since these are version 1 templates, they cannot be modified.

If the PKI administrator wants to change any of the service certificate templates, new ones will need to be created and enrolled. It is recommended that the default template should be duplicated and the duplicated templates should be used for enrollment.

Duplicating CEP Encryption template

To duplicate CEP encryption template:

1. Log on to DC1 as an Enterprise Administrator.
2. Run certtmpl.msc to start the Certificate Template snap-in. If the snap-in does not load, install the Remote Administration feature using the Role Management Tool.
3. In the Certificate Template snap-in, select the CEP Encryption template.
4. Right-click the template and select Duplicate Template.
5. Click on General tab and enter the Template display name as CEP Encryption V2.
6. Select validity period 2 years and select Publish certificate in Active Directory.
7. Click on Cryptography tab and select Request can use any provider available on subject computer.
8. Click on Security tab, add SCEPAdmin, SCEPSvc and APP1 (Computer Name hosting Microsoft NDES) account and provide the Read and Enroll permission for all added account.
9. Click on Subject Name tab and select Supply in the request.
10. Click OK.

Duplicating Exchange Enrollment Agent template

To duplicate Exchange Enrollment Agent template, also referred to as the Offline Request template:

1. Log on to DC1 as an Enterprise Administrator.
2. Run certtmpl.msc to start the Certificate Template snap-in. If the snap-in does not load, install the Remote Administration feature using the Role Management Tool.
3. In the Certificate Template snap-in, select the Exchange Enrollment Agent (Offline Request) template.
4. Right-click the template and select Duplicate Template.
5. Click on General tab and enter the Template display name as Exchange Enrollment Agent V2.
6. Select validity period 2 years and select Publish certificate in Active Directory.
7. Click on Cryptography tab and select Request can use any provider available on subject computer.
8. Click on Security tab, add SCEPAdmin, SCEPSvc and APP1 (Computer Name hosting Microsoft NDES) account and provide the Read and Enroll permission for all added account.
9. Click on Subject Name tab and select Supply in the request.
10. Click OK.

Duplicating Exchange IPSec (Offline Request) template

1. Log on to DC1 as an Enterprise Administrator.
2. Run certtmpl.msc to start the Certificate Template snap-in. If the snap-in does not load, install the Remote Administration feature using the Role Management Tool.
3. In the Certificate Template snap-in, select the IPSec (Offline Request) template.

4. Right-click the template and select Duplicate Template.
5. Click on General tab and enter the Template display name as Microsoft NDES Enroll.
6. Select validity period 2 years and select Publish certificate in Active Directory.
7. Click on Cryptography tab and select Request can use any provider available on subject computer.
8. Click on Security tab and add SCEPAdmin, SCEPSvc and APP1 (Computer Name hosting Microsoft NDES) account and provide the Read and Enroll permission for all added account.
9. Select the Extensions tab, select Application Policies and take a look at the Application Policies. We copied the IPSEC (Offline request) template and it's meant for IPSEC. We'll change it so this template can be used for client authentication. Click on Edit.
10. Right now we only have the IP security IKE intermediate Application policy. Remove this.
11. Click Add and select Client Authentication.
12. Click on Subject Name tab and select Supply in the request.
13. This template can now be used Client authentication. Click OK to continue.

Enabling CA to issue certificates based on CEP, Exchange Enrollment Agent, and Exchange IPSec templates

1. Run certsrv.msc.
2. Select the root node.
3. Right-click and select Retarget Certification Authority.
4. Select the CA that is configured for the Network Device Enrollment Service.
5. Expand the root node.
6. Select the Certificate Templates node.
7. Right-click, selects New, and then clicks Certificate Template to Issue. A dialog box will appear.
8. Select CEP Encryption V2, Exchange Enrollment Agent V2 and Microsoft NDES Enroll.

Now, the CA is ready to receive enrollment requests based on the configured certificate templates.

Configuring templates for certificate enrollment

By default, the service is configured to submit enrollment requests based on the IPSECIntermediateOffline certificate template. To change the default by modifying registry keys:

1. Log on to the computer hosting the Network Device Enrollment Service.
2. Run regedit.
3. Go to HKLM\Software\Microsoft\Cryptography\MSCEP.
   c. If your device sends a request with encryption and signing KeyUsage extensions, you will need to modify the GeneralPurposeTemplate registry value with the name of your new certificate template.
   d. If your device sends a request with encryption KeyUsage extension only, you will need to modify the EncryptionTemplate registry value with the name of your new certificate template.

e. If your device sends a request with signing KeyUsage extension only, you will need to modify the SignatureTemplate registry value with the name of your new certificate template.

> **NOTE:** The name used is the CN of the certificate template (with no spaces) not the DN.

4. To force the service to implement the configuration changes, restart IIS after changing the configured certificate templates.

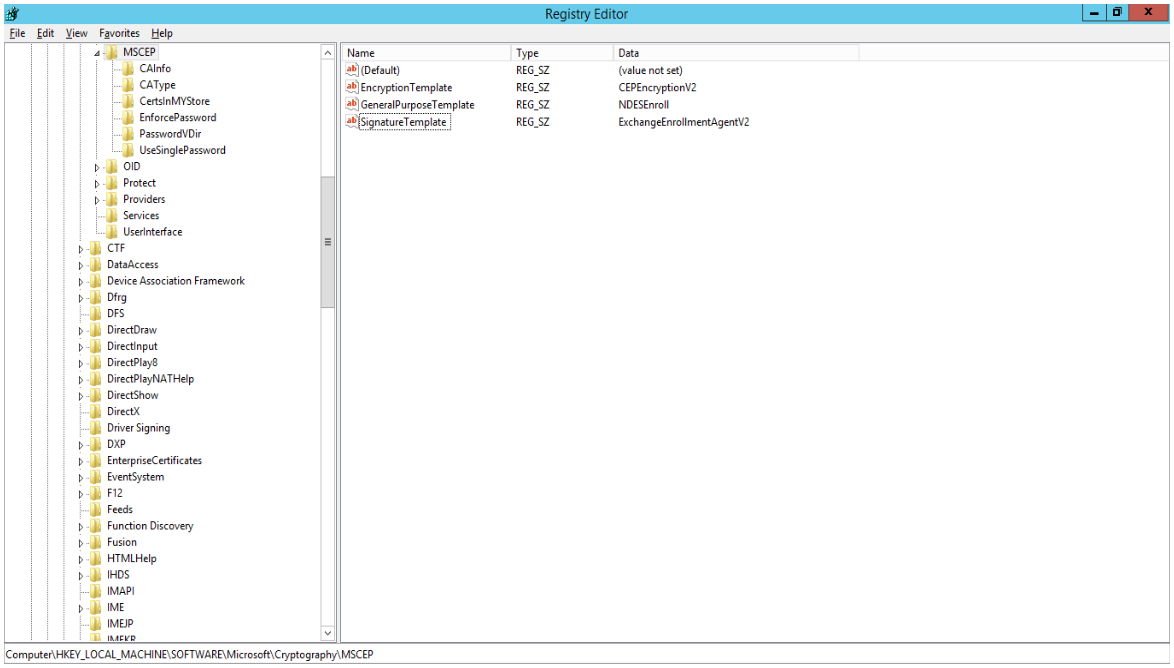
NDES/SCEP by default use the IPSECIntermediateOffline template when you enroll a certificate. The steps provided below are for configuring required templates for certificate enrollment.

1. Log on to APP1 as an Enterprise Admin.
2. Click on the Start button > type “regedit” (without the quotes) and hit enter.
3. Select HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP. Note that the default value is IPSECIntermediateOffline. We need to change all 3 values so double-click on them.
4. Change the Value data with appropriate certificate template name. Click OK to continue.

   EncryptionTemplate > CEPEncryptionV2

   GeneralPurposeTemplate > NDESEnroll

   SignatureTemplate > ExchangeEnrollmentAgentV2



Name	Type	Data
(Default)	REG_SZ	(value not set)
EncryptionTemplate	REG_SZ	CEPEncryptionV2
GeneralPurposeTemplate	REG_SZ	NDESEnroll
SignatureTemplate	REG_SZ	ExchangeEnrollmentAgentV2

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP

5. To make the changes in the registry take effect. restart IIS. Execute the following command in command prompt:

   iisreset

We are now ready to enroll the device certificate that supports the SCEP. To enroll the device certificate we need to perform the following steps:

Step 1: Generates a public-private key pair for the device.

Step 2: Obtains a password from the Network Device Enrollment Service at:

https://<NDES_Server>/certsrv/mscep_admin/

Step 3: Sets the device to trust the Enterprise PKI

Step 4: Submits a certificate enrollment request to the service

Step 5: Sends an enrollment request to the CA

Step 6: CA issues the device certificate.

> **NOTE:** You can test the above steps using any device like routers, VPN etc. that supports SCEP.

Configuring IIS to use SSL to deliver the challenge password for certificate enrollment

Two virtual directories are created for the service during set up. The first virtual directory is for requesting passwords and the second one is for sending the certificate request. The first virtual directory will authenticate the caller and verify that the caller has the required permissions to obtain a new password. If the validation succeeds, the service will generate a password and return it in clear text. Since the password should be secured, it is highly recommended that SSL be enabled on this virtual directory.

> **NOTE:** SSL is typically not supported for the certificate request. It is only supported for the request of challenge password.

To enable the SSL for IIS, either refer to Thales Microsoft IIS integration guide, or follow the steps below:

1. Log on to APP1 server as domain administrator.
2. Open the IIS Manager.
3. Click the Computer Name App 1 and double click on **Server Certificate**.
4. In the Action tab click **Create Certificate Request.**
5. Enter the details and click **Next**.

> **NOTE:** The DNS name included in the subject (Common Name) of the certificate must match the SPN set on the SCEPSvc account i.e. APP1.Integration.com

6. Select Cryptographic Service Provider as “Luna SChannel Cryptographic Services for Microsoft Windows” and Bit Length.
7. Click **Next** and specify the certificate request path and click **Finish**.
8. Send the certificate request to the CA and obtain the signed certificate form CA.
9. Click on **Complete Certificate Request**.
10. Select the Signed certificate and enter the Friendly Name and Certificate Store as Personal.
11. Click **OK**.
12. Go to the Default Web Sites and click **Bindings**.

13. Click **Add**, Select HTTPS and the certificate that you have added.

> **NOTE:** You must not enforce SSL for all connections. It should be for the virtual directory used to provide the challenge password. Make sure that you have registered the SafeNet KSP also before enabling SSL.

14. Click **OK** and then **Close**.

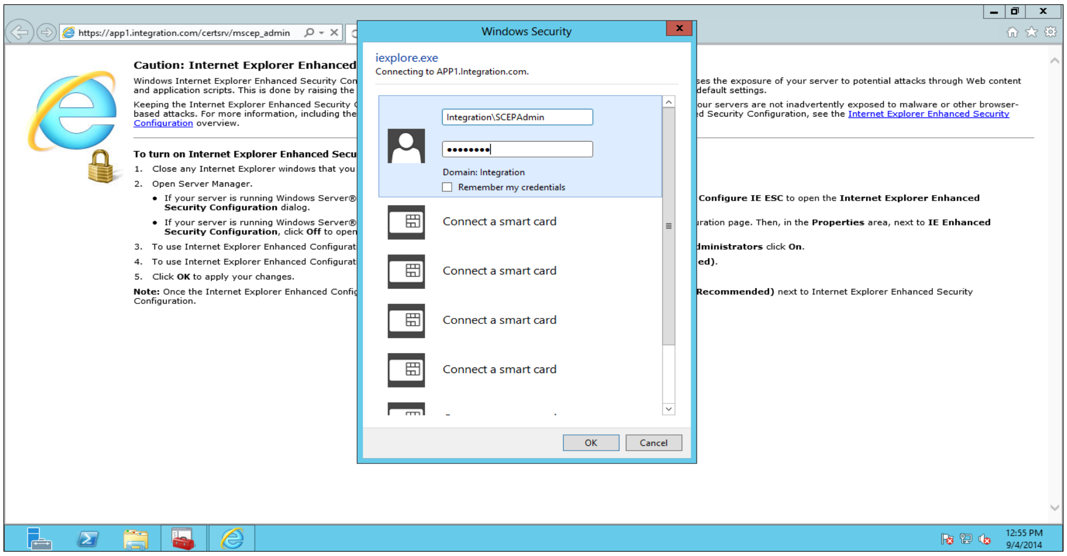
    Now you can browse the MSCEP and MSCEP Admin sites using SSL.

Verifying Microsoft NDES

1. Log on to any machine that is not the part of domain.
2. Download the Microsoft SCEP utility from http://secadmins.com/index.php/ndes-scep-windows-test-tool/.

   After downloading the toolbox and extracting the files, implement the following steps to verify your NDES/SCEP deployment.
3. Get a new SCEP challenge password from your SCEP/NDES server from either of these location: https://<NDES_Server>/certsrv/mscep_admin/

   https://APP1.Integration.com/certsrv/mscep_admin
4. Enter the credentials for Integration\SCEPAdmin and click **OK**. You will see the MSCEP Admin page with the challenge password for device certificate enrollment.



Windows Security

iexplore.exe
Connecting to APP1.Integration.com.

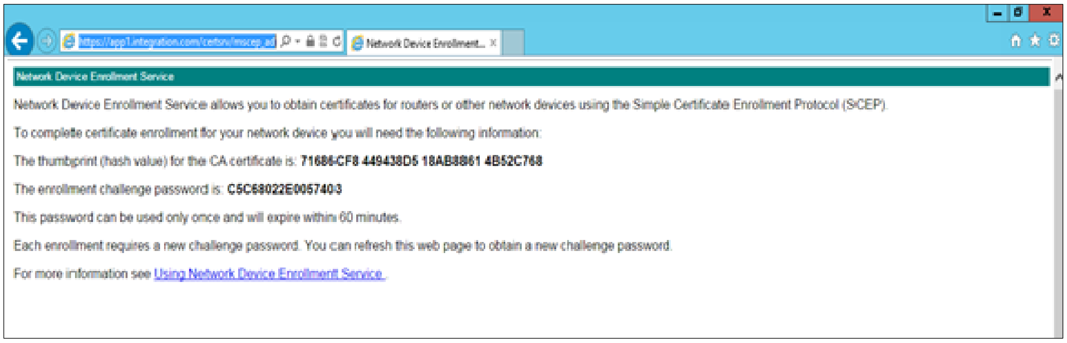
Integration\SCEPAdmin

••••••••

Domain: Integration

□ Remember my credentials

https://app1.integration.com/certsrv/mscep_admin
Caution: Internet Explorer Enhanced
To turn on Internet Explorer Enhanced Secu
Connect a smart card
Connect a smart card
Connect a smart card
Connect a smart card
OK
Cancel
12:55 PM
9/4/2014



https://app1.integration.com/certsrv/mscep_ad
Network Device Enrollment...

Network Device Enrollment Service

Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP).

To complete certificate enrollment for your network device you will need the following information:

The thumbprint (hash value) for the CA certificate is: **71686CF8 449438D5 18AB8861 4B52C768**

The enrollment challenge password is: **C5C68022E0057403**

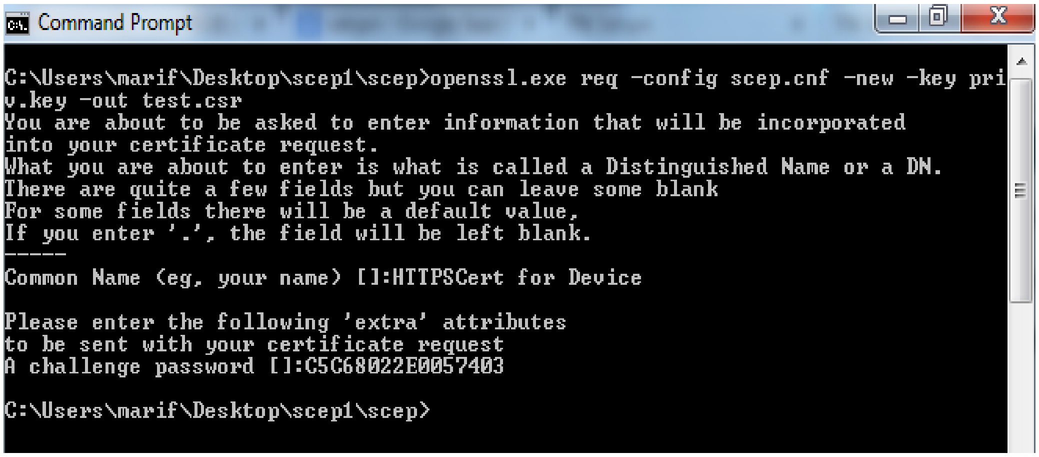
This password can be used only once and will expire within 60 minutes.

Each enrollment requires a new challenge password. You can refresh this web page to obtain a new challenge password.

For more information see Using Network Device Enrollment Service.

5. Open the command prompt and go to the directory where you extracted the MS SCEP utility. Generate a certificate request providing a Common Name and the Challenge Password when prompted by openssl. Use the following command:

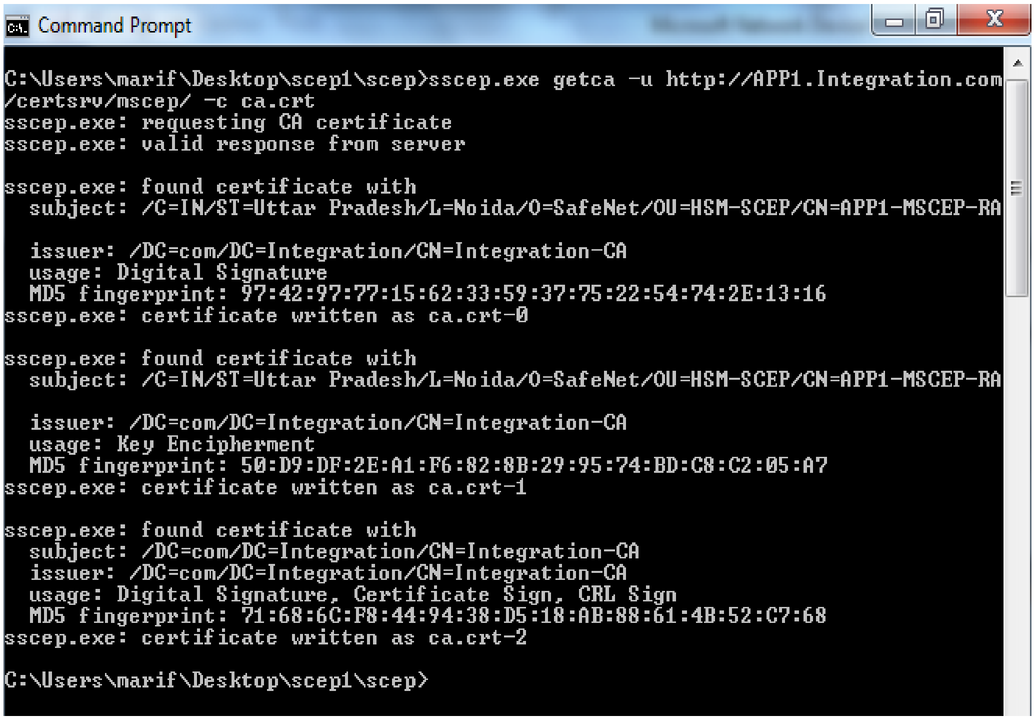
```
openssl.exe req -config scep.cnf -new -key priv.key -out test.csr
```



```
C:\Users\marif\Desktop\scep1\scep>openssl.exe req -config scep.cnf -new -key pri
v.key -out test.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg, your name) []:HTTPSCert for Device

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:C5C68022E0057403

C:\Users\marif\Desktop\scep1\scep>
```

6. Retrieve the CA and RA certificates from your SECP/NDES server using the command:

```
sscep.exe getca -u http://APP1.Integration.com/certsrv/mscep/ -c ca.crt
```

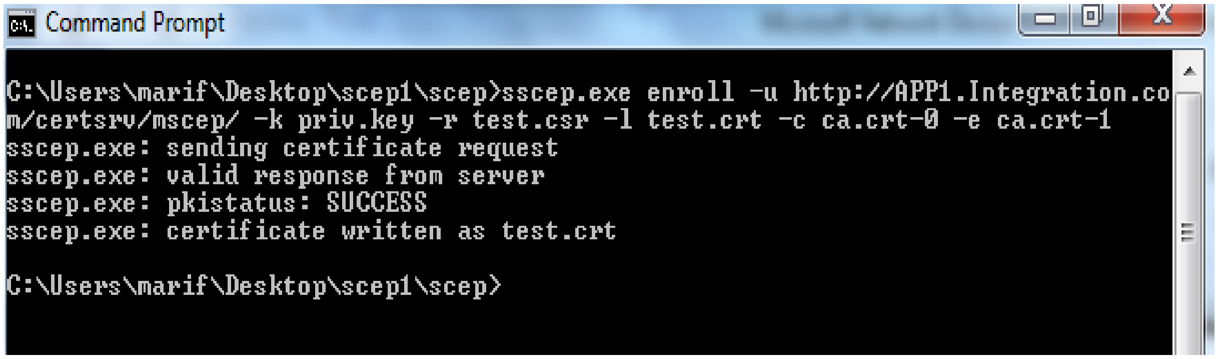


```
C:\Users\marif\Desktop\scep1\scep>sscep.exe getca -u http://APP1.Integration.com
/certsrv/mscep/ -c ca.crt
sscep.exe: requesting CA certificate
sscep.exe: valid response from server

sscep.exe: found certificate with
  subject: /C=IN/ST=Uttar Pradesh/L=Noida/O=SafeNet/OU=HSM-SCEP/CN=APP1-MSCEP-RA

  issuer: /DC=com/DC=Integration/CN=Integration-CA
  usage: Digital Signature
  MD5 fingerprint: 97:42:97:77:15:62:33:59:37:75:22:54:74:2E:13:16
sscep.exe: certificate written as ca.crt-0

sscep.exe: found certificate with
  subject: /C=IN/ST=Uttar Pradesh/L=Noida/O=SafeNet/OU=HSM-SCEP/CN=APP1-MSCEP-RA

  issuer: /DC=com/DC=Integration/CN=Integration-CA
  usage: Key Encipherment
  MD5 fingerprint: 50:D9:DF:2E:A1:F6:82:8B:29:95:74:BD:C8:C2:05:A7
sscep.exe: certificate written as ca.crt-1

sscep.exe: found certificate with
  subject: /DC=com/DC=Integration/CN=Integration-CA
  issuer: /DC=com/DC=Integration/CN=Integration-CA
  usage: Digital Signature, Certificate Sign, CRL Sign
  MD5 fingerprint: 71:68:6C:F8:44:94:38:D5:18:AB:88:61:4B:52:C7:68
sscep.exe: certificate written as ca.crt-2

C:\Users\marif\Desktop\scep1\scep>
```

NOTE: The getca operation will download the RA and CA certificates and save each cert in a file prefixed with a number: ca.crt-0, ca.crt-1, ca.crt-2

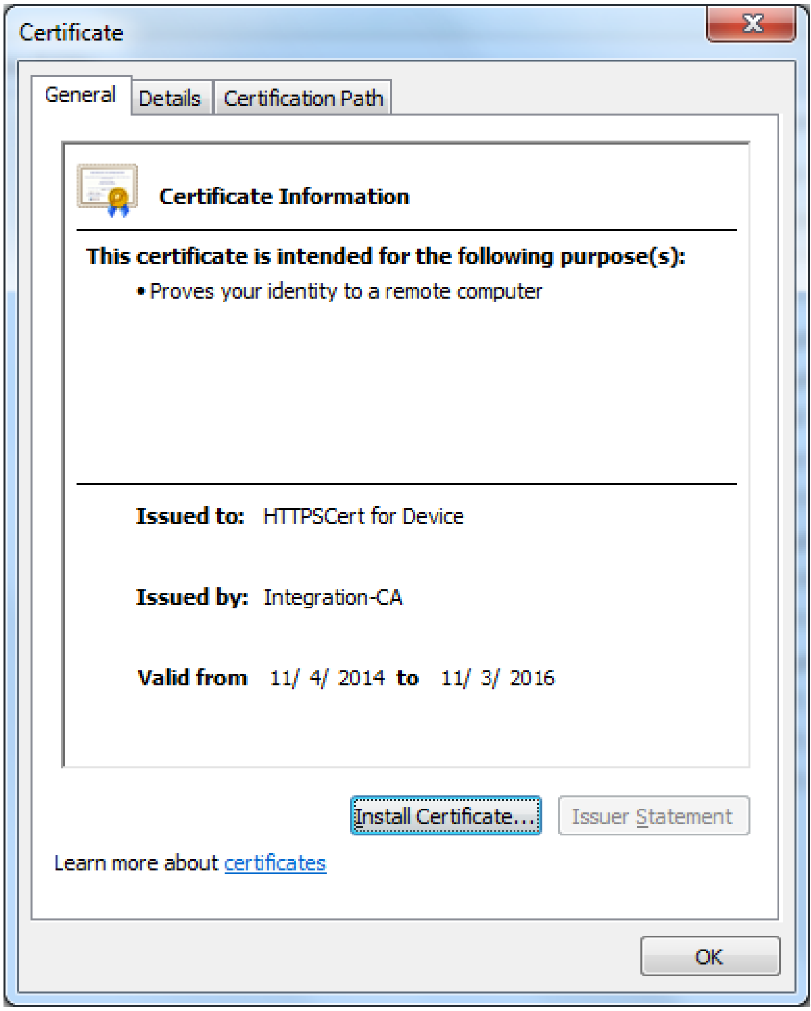
7. Enroll a new certificate and make sure to specify the correct RA (-c flag) & CA (-e flag) certificates using the command below:

   ```
   sscep.exe enroll -u http://APP1.Integration.com/certsrv/mscep/ -k priv.key
   -r test.csr -l test.crt -c ca.crt-0 -e ca.crt-1
   ```



```
C:\Users\marif\Desktop\scep1\scep>sscep.exe enroll -u http://APP1.Integration.co
m/certsrv/mscep/ -k priv.key -r test.csr -l test.crt -c ca.crt-0 -e ca.crt-1
sscep.exe: sending certificate request
sscep.exe: valid response from server
sscep.exe: pkistatus: SUCCESS
sscep.exe: certificate written as test.crt

C:\Users\marif\Desktop\scep1\scep>
```

8. Double click on the test.crt file to verify that the certificate is signed by your CA.



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer

Issued to: HTTPSCert for Device

Issued by: Integration-CA

Valid from 11/ 4/ 2014 to 11/ 3/ 2016

s

You can now sign the certificate for the device from the non-domain systems using Microsoft NDES Certificate Enrollment that uses Luna CSP for RA certificates whose keys are on Luna HSM.

This completes the integration of Microsoft NDES with Luna HSM. The Microsoft NDES and Microsoft CA signing keys are securely stored inside the Luna HSM.