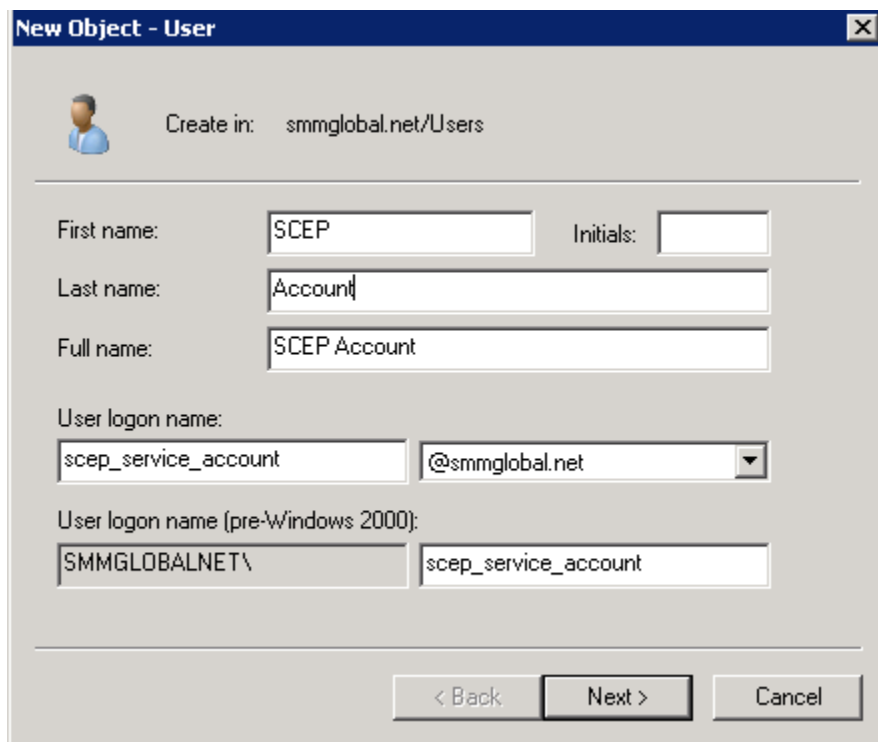


How to setup MSCA with Symantec Mobility | iOS

Deploy a MSCA (Microsoft Certificate Authority) Server:

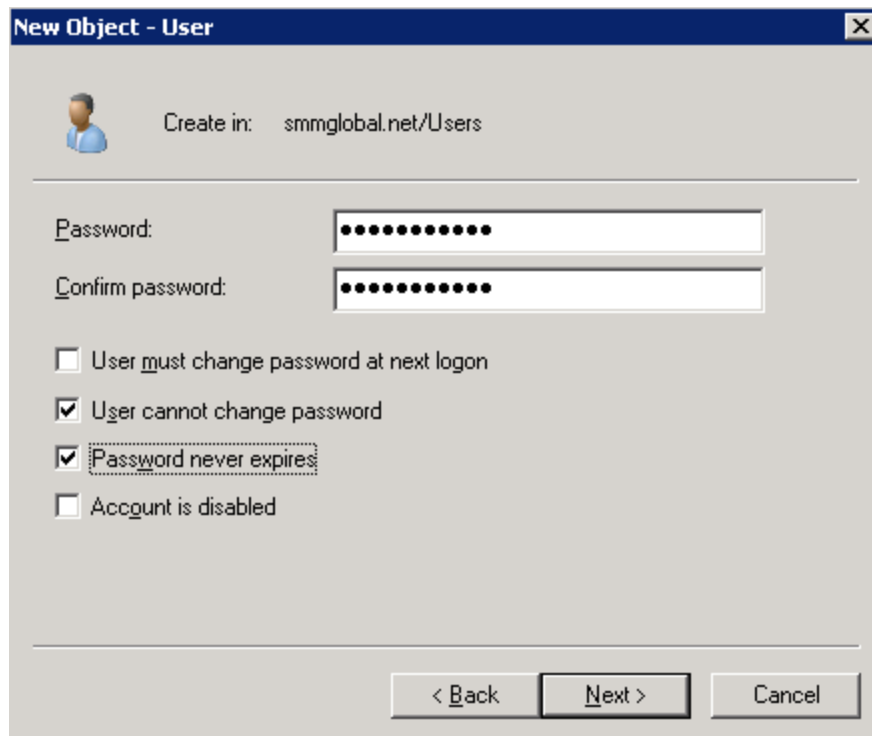
Note: The Enterprise Windows Server 2008 R2 box must be a member of an Active Directory domain. A production off-box RabbitMQ server is required. To deploy a HA (High Availability) RabbitMQ server see [HOWTO110356](#). This document assumes that the admin has already created an MDM, Code-signing, Provisioning profile and APNS certificates. See the Mobility A to Z document and relevant sections for step-by-step instructions on creating these certificates prior to continuing with this article.

1. From AD create a new user:



The screenshot shows the 'New Object - User' dialog box in Active Directory. The 'Create in' field is set to 'smmglobal.net/Users'. The 'First name' field contains 'SCEP', the 'Last name' field contains 'Account', and the 'Full name' field contains 'SCEP Account'. The 'User logon name' field contains 'scep_service_account' and the domain dropdown is set to '@smmglobal.net'. The 'User logon name (pre-Windows 2000)' field contains 'SMMGLOBALNET\scep_service_account'. The 'Initials' field is empty. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

2. Set a static password for this user account as the NDES (Network Device Enrollment Service) will use this account to enroll users:



New Object - User

Create in: smmglobal.net/Users

Password: [password field]

Confirm password: [password field]

☐ User must change password at next logon

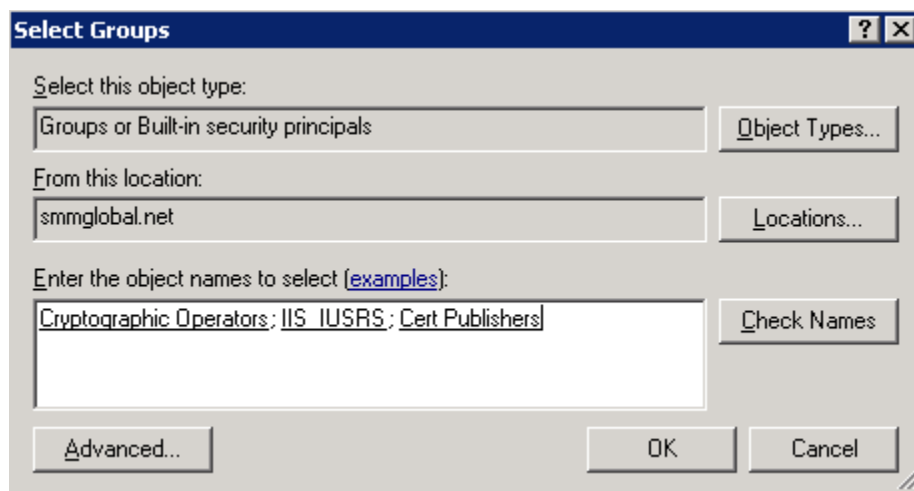
☒ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

3. Click **Next** and **Finish**.
4. Add the user to the Cryptographic_Operators, Cert Publishers and IIS_USERS groups; by right-clicking on the user and selecting **Add to group**:



Select Groups

Select this object type:
Groups or Built-in security principals Object Types...

From this location:
smmglobal.net Locations...

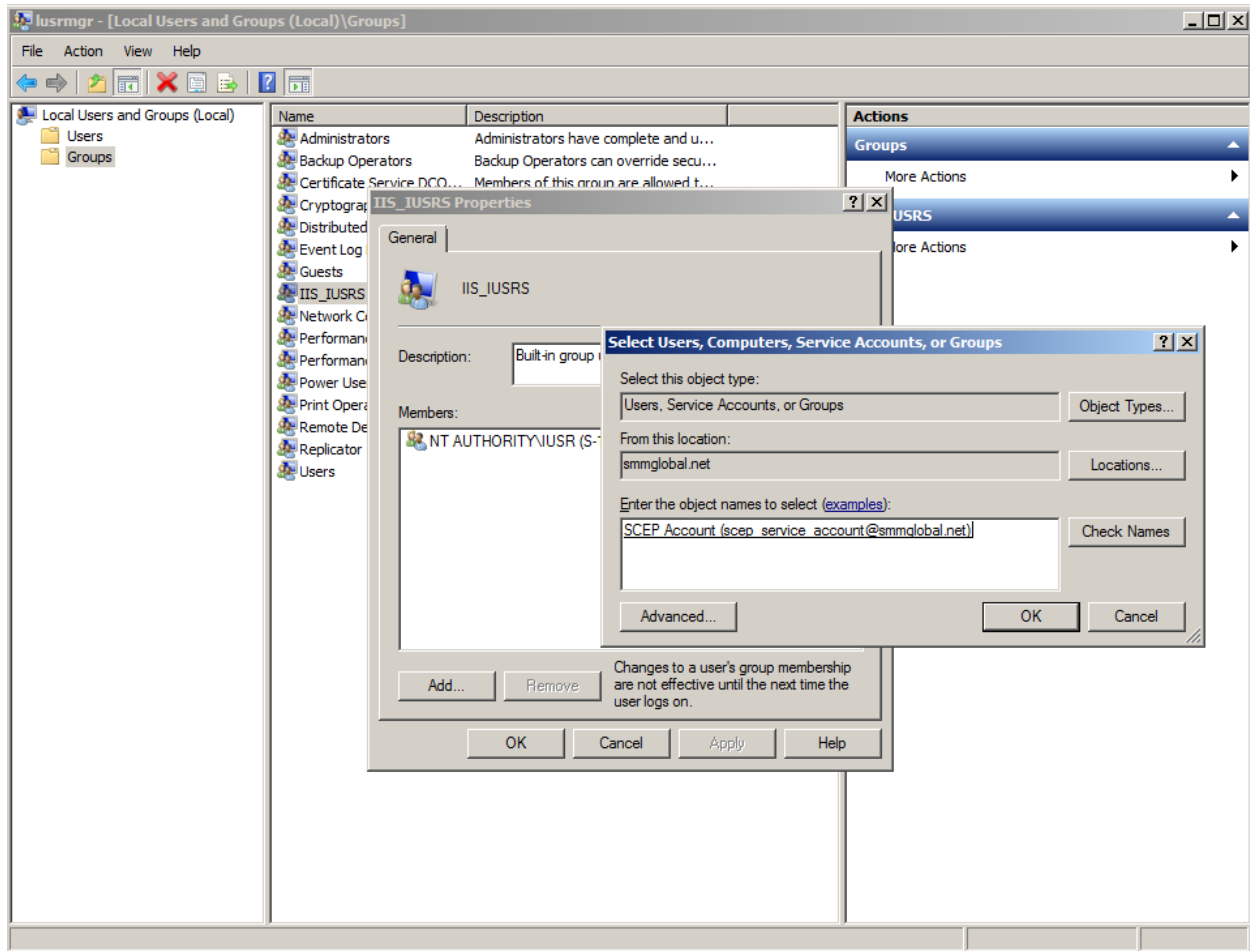
Enter the object names to select (examples):
Cryptographic Operators ; IIS_IUSRS ; Cert Publishers Check Names

Advanced... OK Cancel

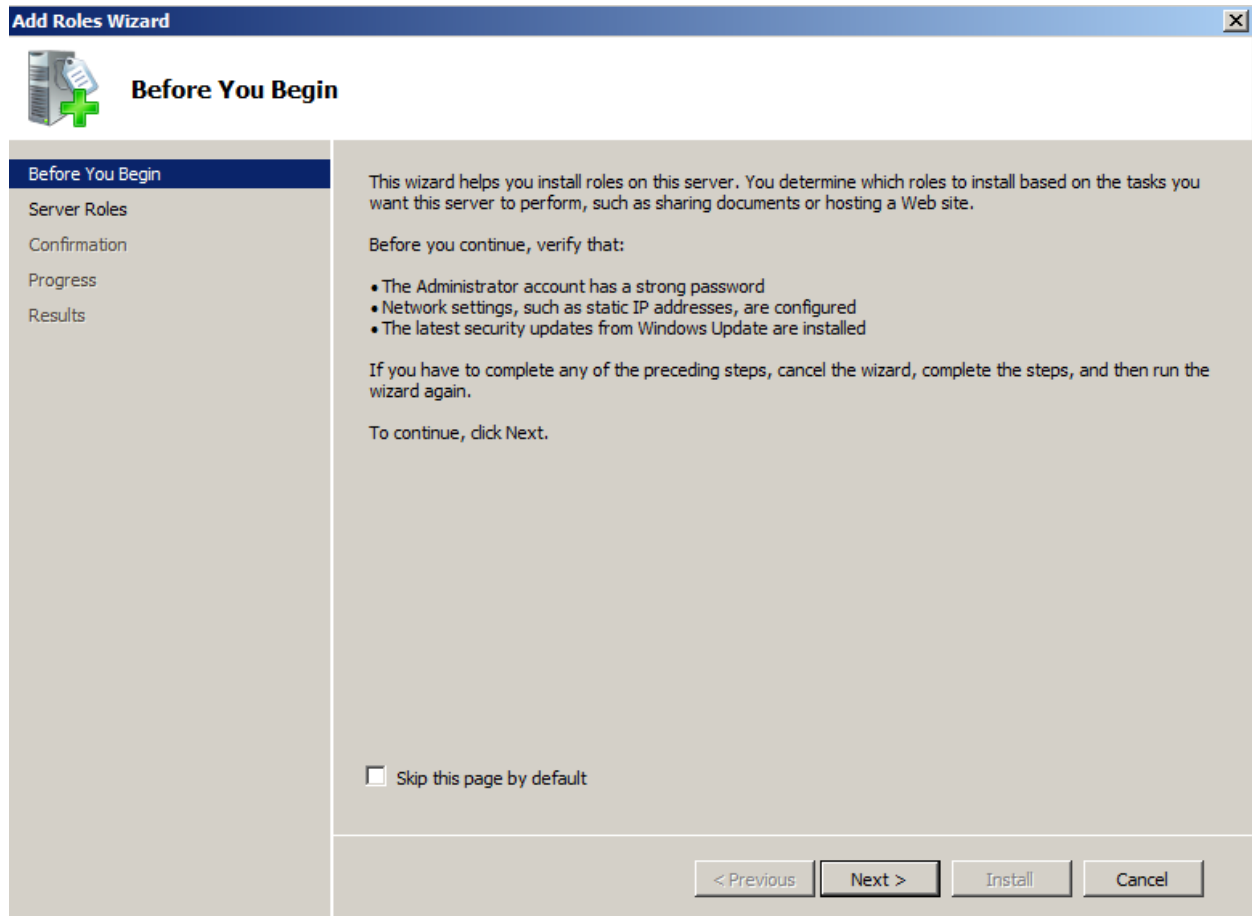
5. Log into the future MSCA server as a **Domain Administrator**.
6. From **Start > Run** enter:
lusrmgr.msc

Adding a user to the machine's local IIS_USERS group

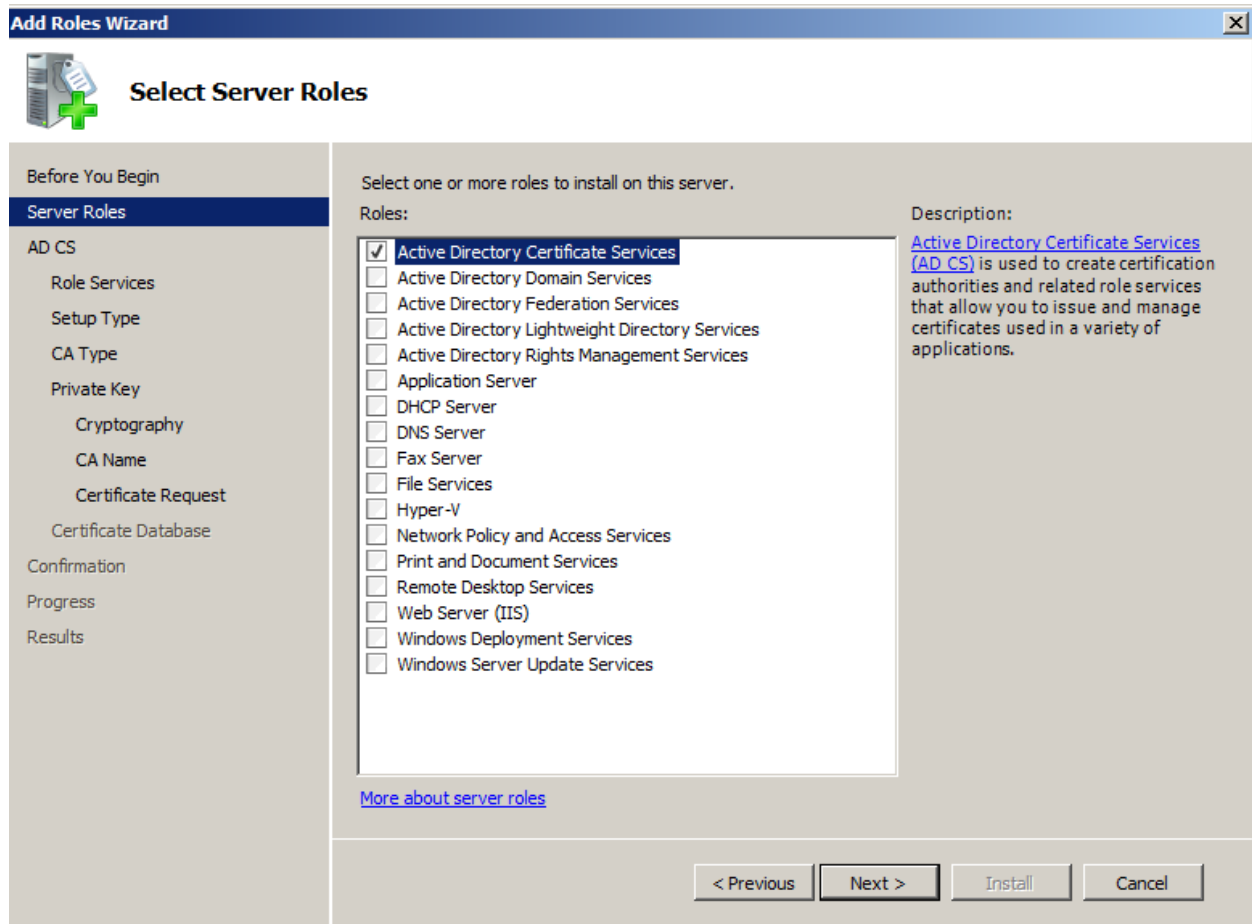
7. From the User Manager Console, add the SCEP user to that machine's local **IIS_USERS** group:



8. Click **OK** to apply the settings.
9. Open the **Server Management Console** from **Start > Run** by entering:
servermanager.msc
10. Under Server Manager right-click on **Roles** and select **Add Roles**:



11. Click **Next**, from the next window check **Active Directory Certificate Services** and **Next** to continue.



12. **Next** through the Introduction page and on the Select Role Services page ensure that only **Certificate Authority** is checked and **Next**.

13. Select **Enterprise** and **Next** to continue.


Note: If the enterprise option is greyed out, this machine is either not a member of the domain, the user account is a local account or this is not an Enterprise version of Windows 2008 R2.

14. The CA type is important, if there is an existing MSCA in the environment, it is recommended to set this up as a Subordinate CA. If there is no CA in the environment the Root CA option is acceptable. Follow below whether Root or Subordinate is selected.

Root CA Option:

15. Select **Root CA** and **Next**. From the Private Key section select **Create a new private key** and **Next** to continue:

Add Roles Wizard

 **Set Up Private Key**

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

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 this computer or if you want to import a certificate and use its associated private key.
 - ☐ *Select an existing private key on this computer*
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about public and private keys](#)

< Previous Next > Install Cancel

16. Select **SHA256** for the key's signing algorithm and **2048** or **4092** for the character length.

Add Roles Wizard

 **Configure Cryptography for CA**

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

To create a new private key, you must first select a [cryptographic service provider](#), [hash algorithm](#), and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.

Select a cryptographic service provider (CSP):
RSA#Microsoft Software Key Storage Provider

Key character length:
2048

Select the hash algorithm for signing certificates issued by this CA:
SHA256
SHA384
SHA512
SHA1

☐ Allow administrator interaction when the private key is accessed by the CA.

[More about cryptographic options for a CA](#)


< Previous Next > Install Cancel

Note: iOS does not validate CA/RA certificates which are greater than 4096.

17. Accept the default common name and DN for the CA and **Next**.

18. Set the validity period to **10 years** and **Next**:

Add Roles Wizard [X]

 **Set Validity Period**

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

A certificate will be issued to this CA to secure communications with other CAs and with clients requesting certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA.

Select validity period for the certificate generated for this CA:

Years

CA expiration Date: 8/25/2025 5:40 PM

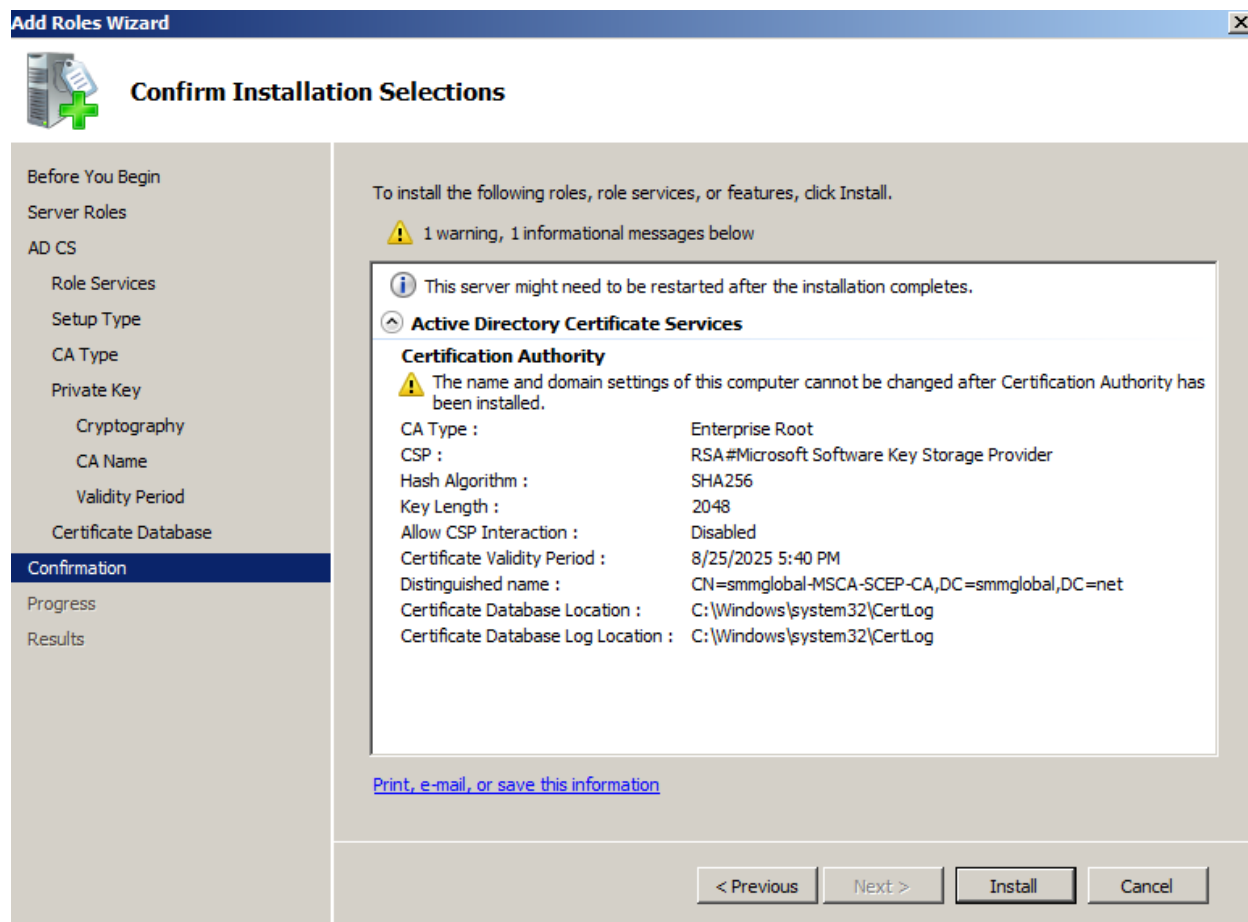
Note that CA will issue certificates valid only until its expiration date.

[More about setting the certificate validity period](#)

< Previous Next > Install Cancel

19. Accept the default database locations and **Next**.

20. Review the configurations and click **Install**:




Note: The service role usually takes about 10 minutes to install. Skip the below **Subordinate CA Option** and continue to [Install the DNES service role](#).

Subordinate CA Option

21. Select **Subordinate CA** and **Next**.
22. Ensure that **Create a new private key** is selected and **Next**.
23. Select **SHA256** for the key's signing algorithm and **2048** or **4092** for the character length.

Add Roles Wizard

 **Configure Cryptography for CA**

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

To create a new private key, you must first select a [cryptographic service provider](#), [hash algorithm](#), and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.

Select a cryptographic service provider (CSP):
RSA#Microsoft Software Key Storage Provider

Key character length:
2048

Select the hash algorithm for signing certificates issued by this CA:
SHA256
SHA384
SHA512
SHA1

☐ Allow administrator interaction when the private key is accessed by the CA.

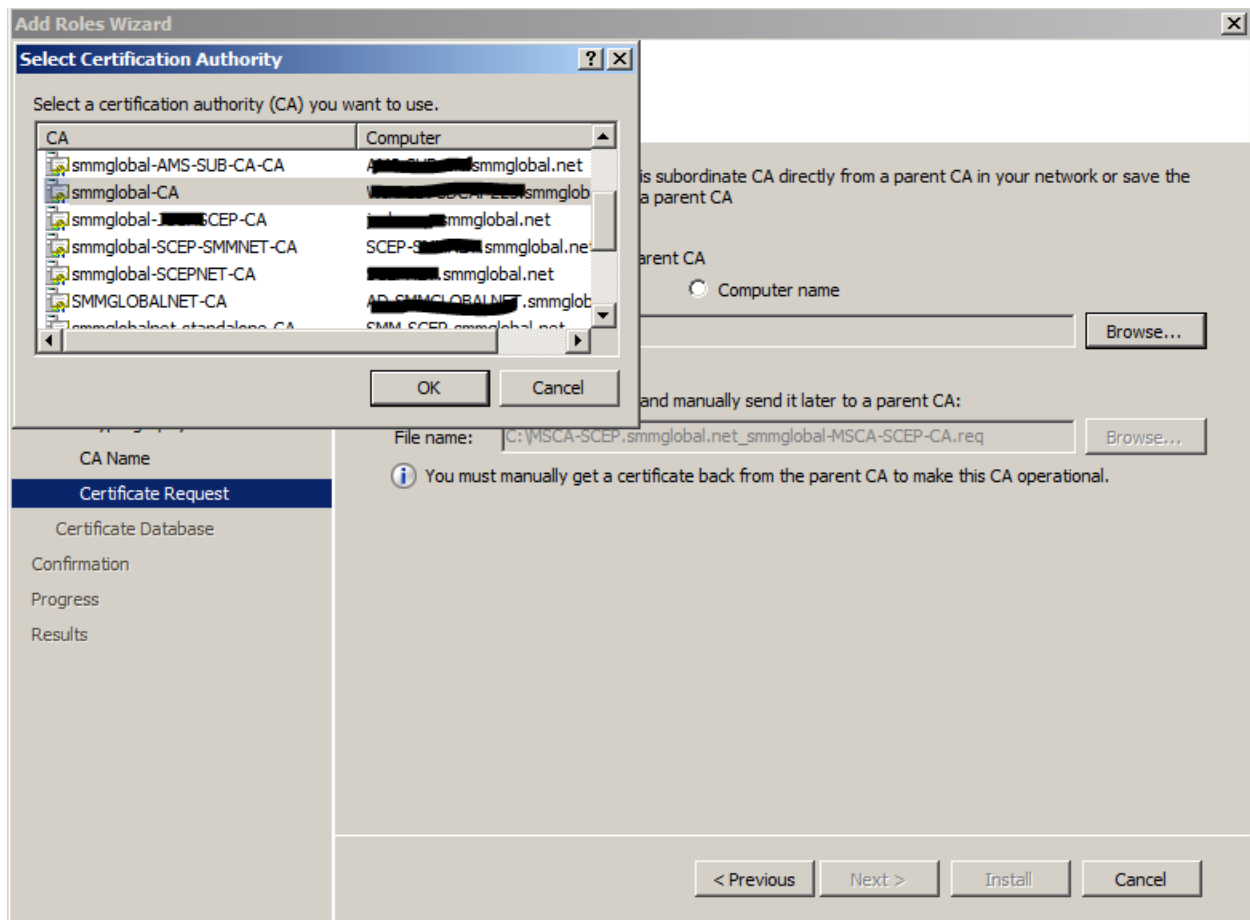
[More about cryptographic options for a CA](#)

< Previous Next > Install Cancel

Note: iOS does not validate CA/RA certificates which are greater than 4096.

24. Accept the default common name and DN for the CA and **Next**.

25. Select **Send a certificate request to a parent CA** and click **Browse...**

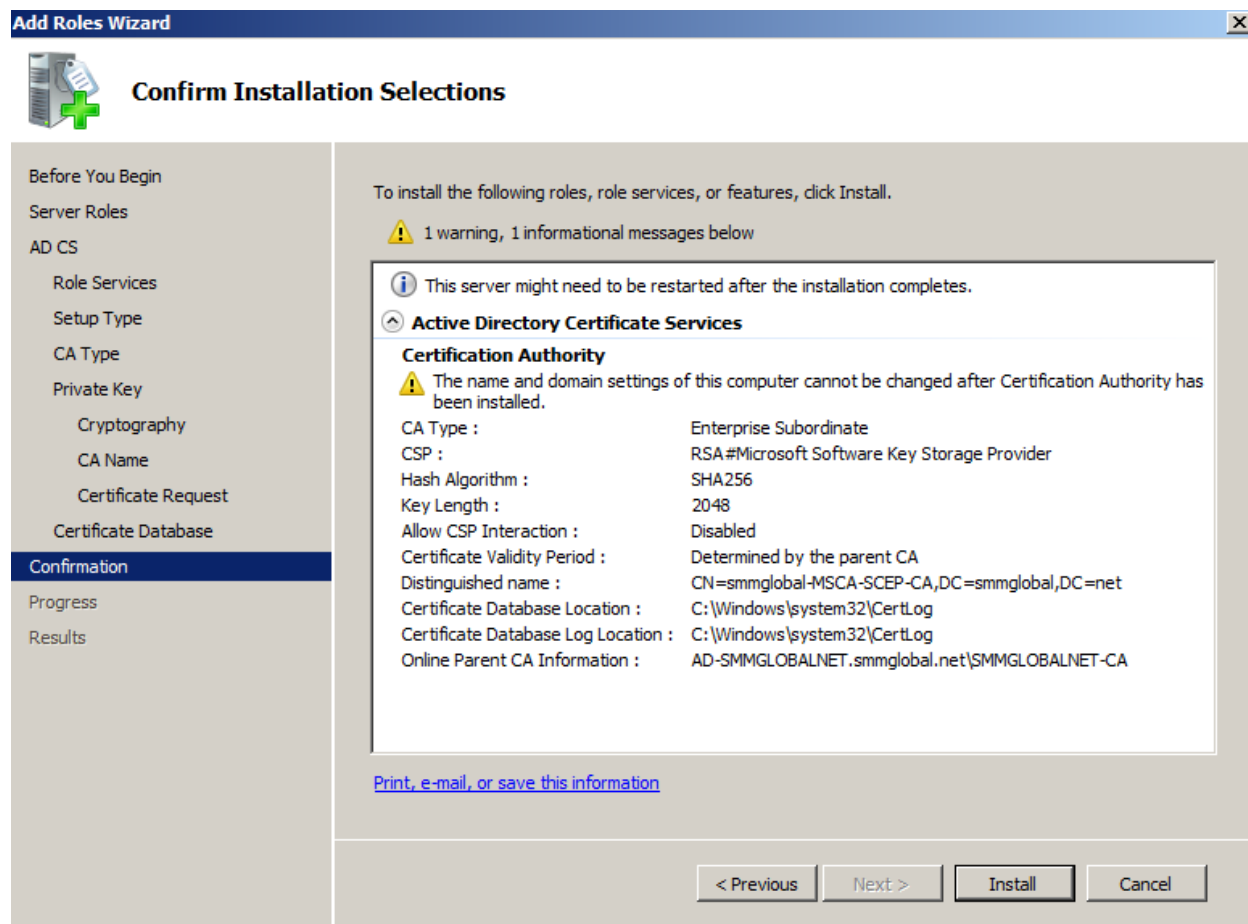


26. Select the CA from the list and **OK** from the selection window and click **Next**.

Note: If no CA is displayed the [Root CA Option](#) is recommended.

27. Review the default database directories and **Next**.

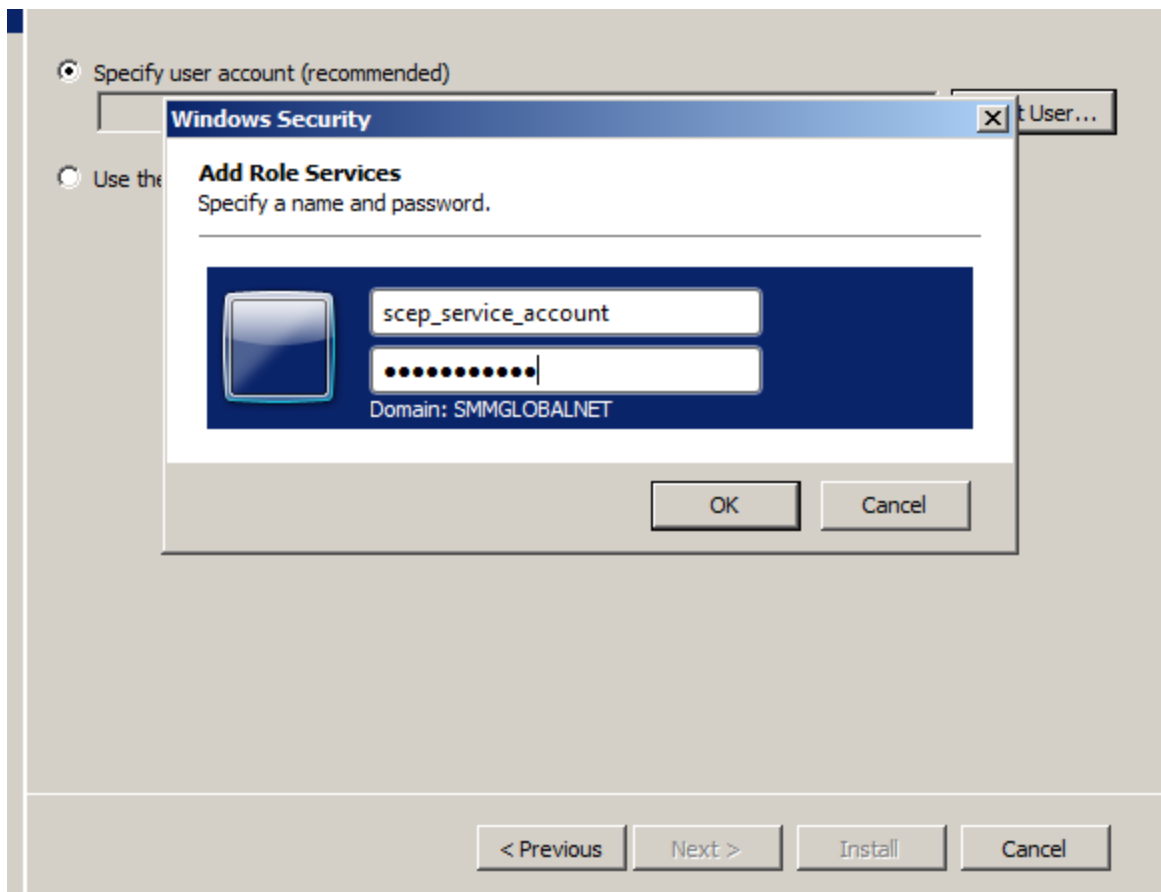
28. Review the subordinate CA's configuration and click **Install**:



Note: The installation can take up to 10 minutes.

Install the DNES service role


29. From the Server Manager console, expand **Roles** right-click on the **Active Directory Certificate Services** and click **Add Role Services**.
30. Check the **Network Device Enrollment Service**, when prompted click **Add Required Role Services** and **Next** to continue.
31. Click **Select User...** and add the SCEP user account created earlier:



Note: If a notification appears that the user is not a member of the IIS_USERS group on the local machine repeat [Adding a user to the machine's local IIS_USERS group](#).

32. **Next** to continue to the RA (Registration Authority) Information section.
33. Optionally enter the certificate administrator's contact information. Ensure to not abbreviate the State/Province name:

Add Role Services

 **Specify Registration Authority Information**

Role Services
User Account
RA Information
Cryptography
Web Server (IIS)
 Role Services
Confirmation
Progress
Results

A registration authority will be set up to manage Network Device Enrollment Service certificate requests. Enter the requested information to enroll for an RA certificate.

Required Information

RA Name:

Country/Region:

Optional Information

E-mail:

Company:

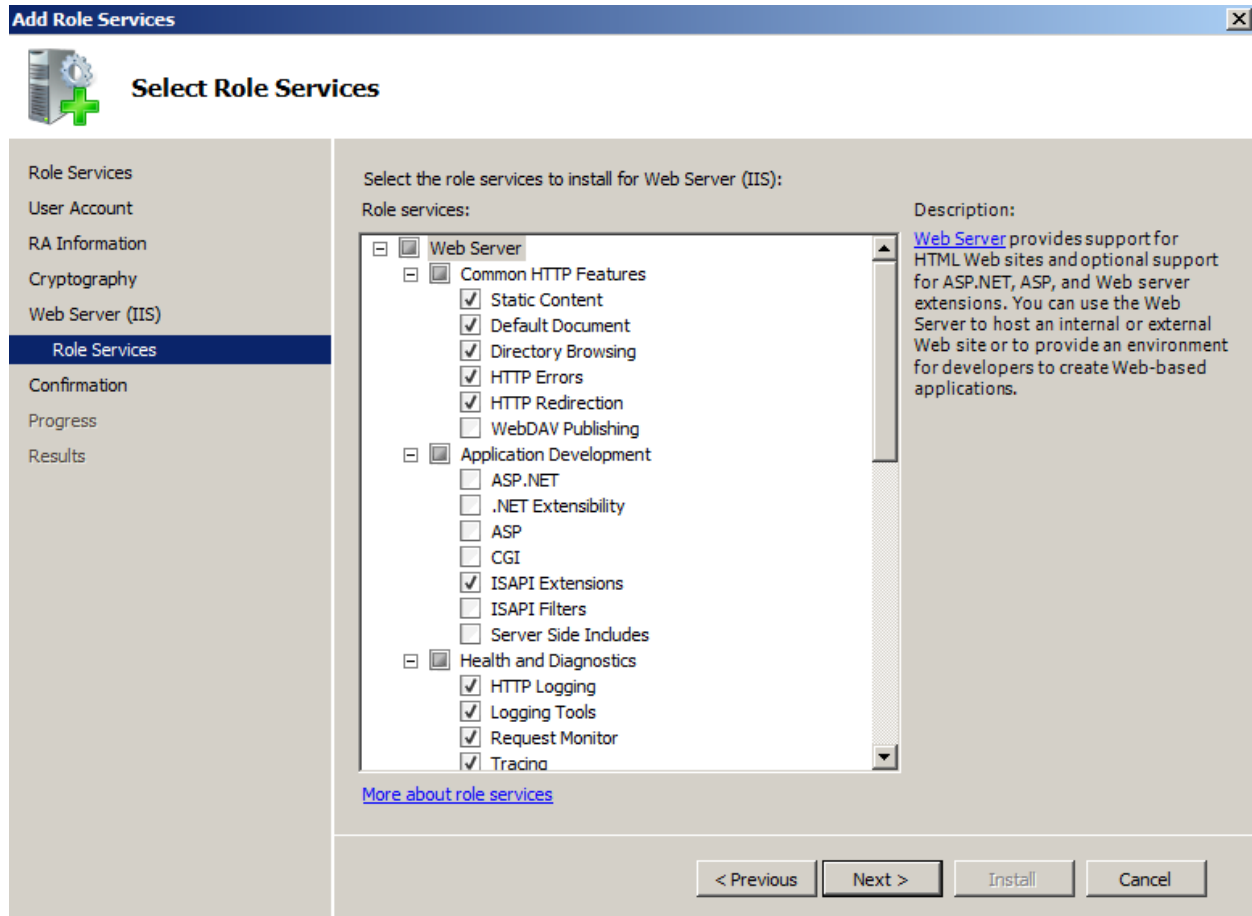
Department:

City:

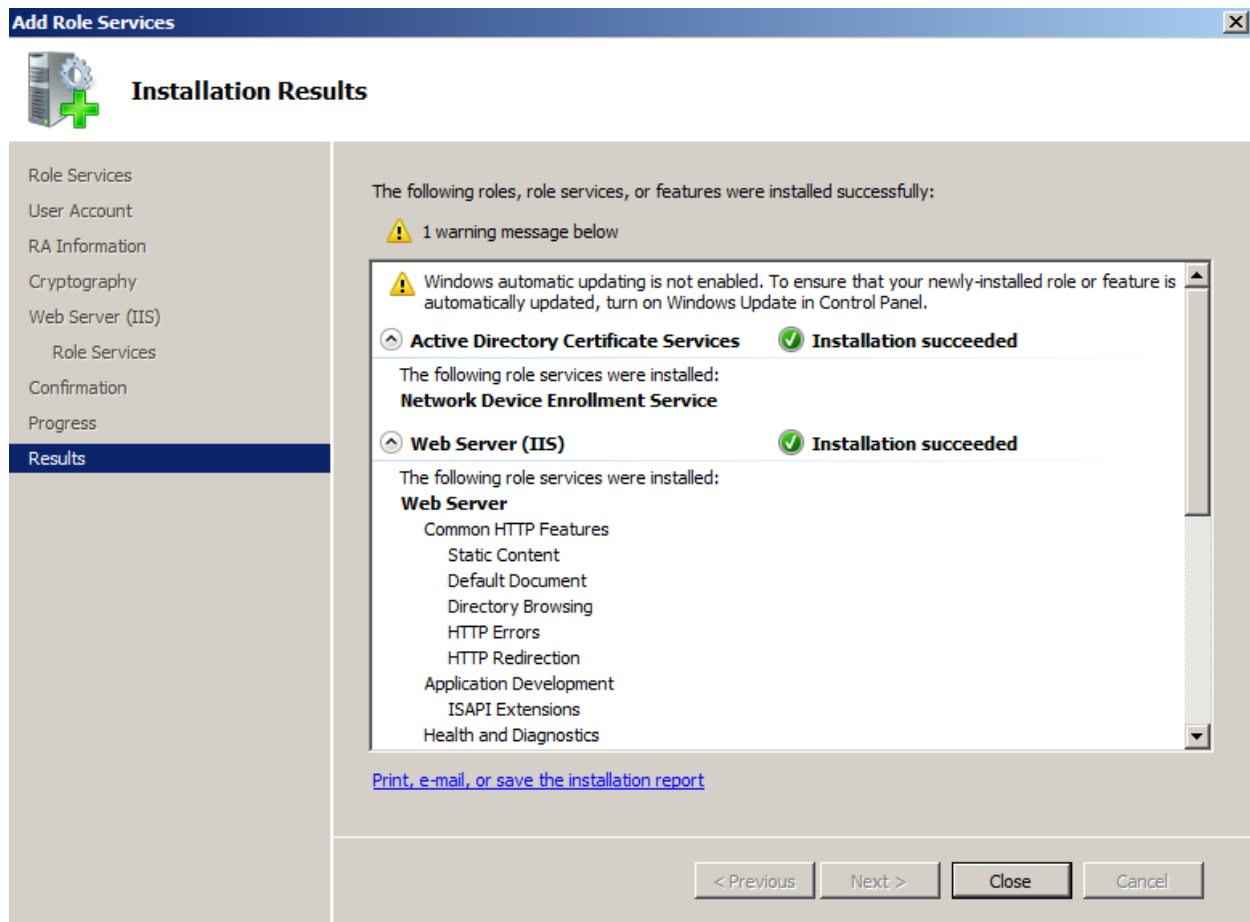
State/Province:

< Previous **Next >** Install Cancel

34. Click **Next** and ensure that 2048 or 4096 are selected for the key character lengths and **Next**.
35. **Next** through the Web Server (IIS) Introduction page.
36. Accept the default features and **Next**:



37. Review the configuration and click **Install**:

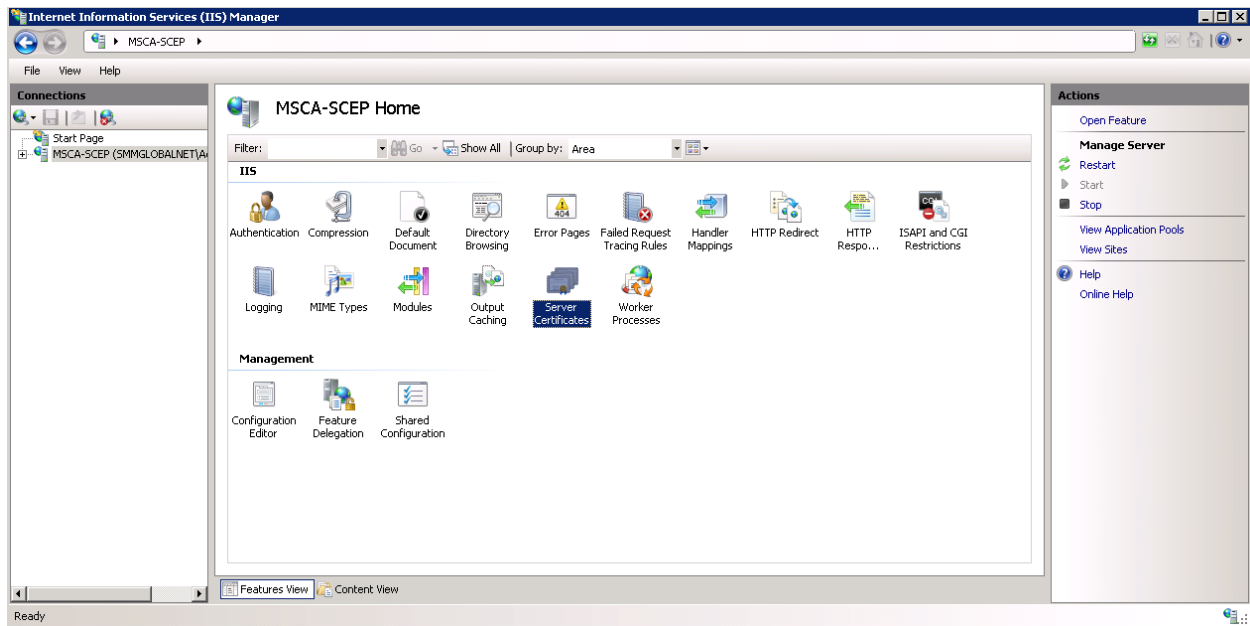


Adding a Certificate to the IIS

38. **Start > Run:**

inetmgr

39. From the IIS Manager console select the SCEP server's name on the left and open **Server Certificates** from the **Features View** on the right:



40. If an SSL certificate is already issued to this machine, it will be displayed along with the CA certificate. Select one of the three options below to bind an SSL certificate to this machine.

Temporary Self-Signed Certificate

41. On the right, click **Create Self-Signed Certificate...**
42. Enter a friendly name for this certificate to identify it and OK.

Import a PKCS Certificate


43. Transfer the PKCS certificate to the machine.
44. From the IIS **Manager > Server Certificates** click **Import...** on the right.
45. Browse to the certificate file and click **OK**.
46. Enter the passphrase for the certificate file.

Request a Certificate from a Certificate Authority

47. From the IIS **Manager > Server Certificates** click **Create Certificate Request...** on the right.
48. Enter the server information into the request.

Note: The Common Name must match the published domain name of the server. Do not abbreviate the State/Province field. Contact your public certificate authority for how to fill in this request:

Request Certificate [?] [X]

 **Distinguished Name Properties**

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: *.acme.company.org

Organization: ACME

Organizational unit: Security

City/locality: Springfield


State/province: Oregon

Country/region: US

Previous Next Finish Cancel

49. **Next** to the Cryptographic properties and ensure that 2048 or 4096 are selected for the **Bit Length** and **Next**.

Request Certificate [?] [X]

 **Cryptographic Service Provider Properties**

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:

Microsoft RSA SChannel Cryptographic Provider

Bit length:

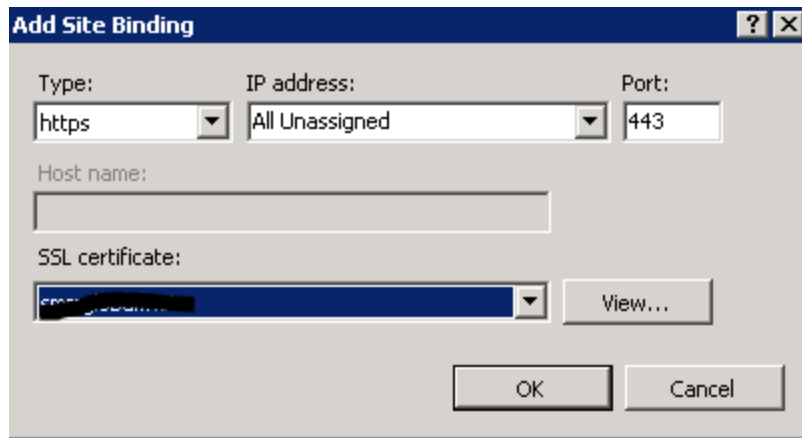
2048

Previous Next Finish Cancel

50. Save the CSR (Certificate Signing Request) file and **Finish**.
51. Send the CSR to the CA, following their instructions.
52. Once a certificate is issued click **Complete Certificate Request...** from the IIS Manager > Certificates console and follow the wizard to import the new certificate.

HTTPS Bindings

53. From within the IIS Manager, expand the **Sites** and right-click on the **Default Web Site** and select **Edit Bindings**.
54. Click **Add** and select **HTTPS** for the **type** and the **new SSL certificate**:



Add Site Binding

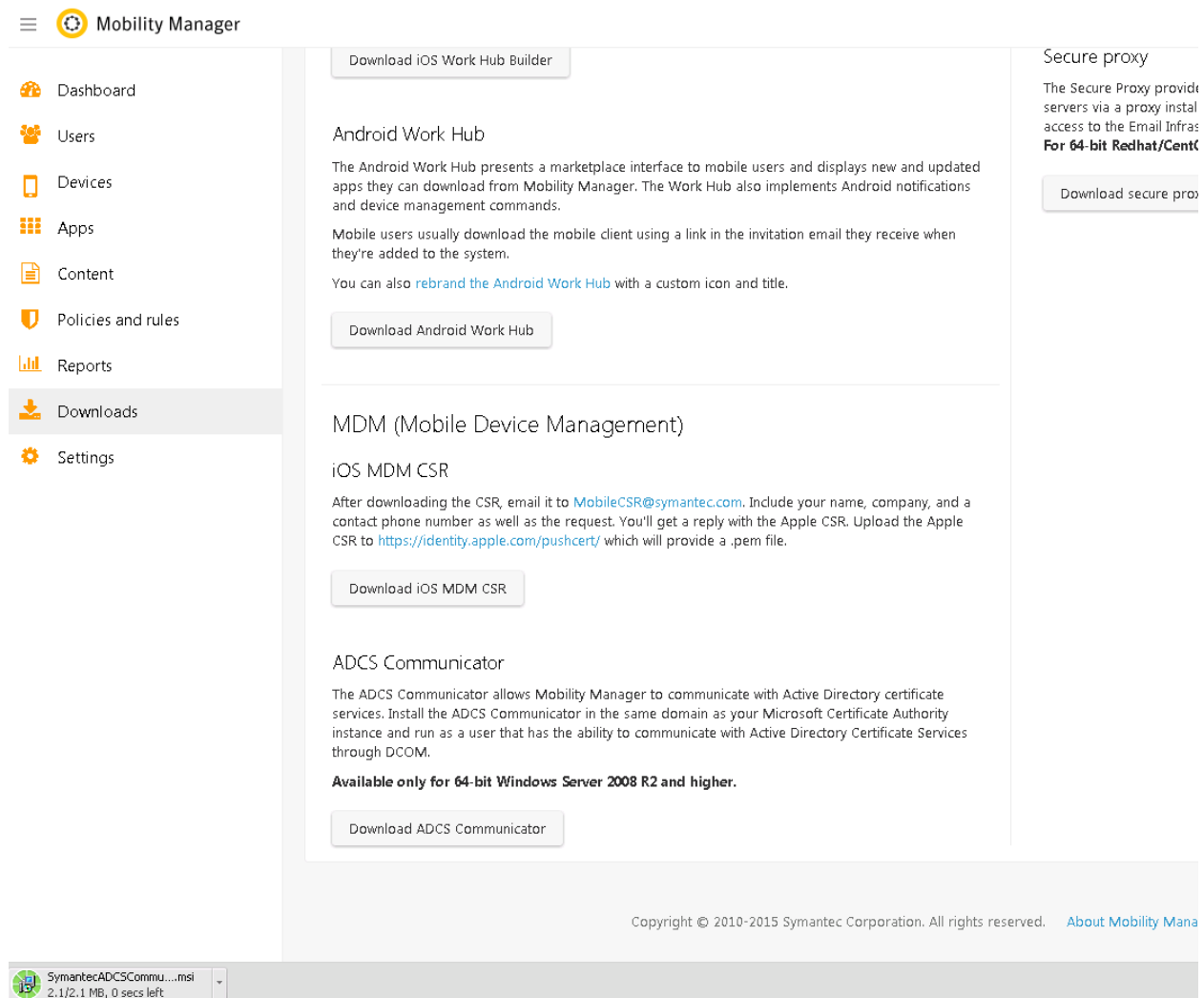
Type: IP address: Port:

Host name:

SSL certificate:

55. Click **OK** and **Close** out of the Site Bindings window.

56. Download and transfer the ADSC Communicator installer to the MSCA server:



Mobility Manager

- Dashboard
- Users
- Devices
- Apps
- Content
- Policies and rules
- Reports
- Downloads**
- Settings

Download iOS Work Hub Builder

Android Work Hub

The Android Work Hub presents a marketplace interface to mobile users and displays new and updated apps they can download from Mobility Manager. The Work Hub also implements Android notifications and device management commands.

Mobile users usually download the mobile client using a link in the invitation email they receive when they're added to the system.

You can also [rebrand the Android Work Hub](#) with a custom icon and title.

Download Android Work Hub

MDM (Mobile Device Management)

iOS MDM CSR

After downloading the CSR, email it to MobileCSR@symantec.com. Include your name, company, and a contact phone number as well as the request. You'll get a reply with the Apple CSR. Upload the Apple CSR to <https://identity.apple.com/pushcert/> which will provide a .pem file.

Download iOS MDM CSR

ADCS Communicator

The ADCS Communicator allows Mobility Manager to communicate with Active Directory certificate services. Install the ADCS Communicator in the same domain as your Microsoft Certificate Authority instance and run as a user that has the ability to communicate with Active Directory Certificate Services through DCOM.

Available only for 64-bit Windows Server 2008 R2 and higher.

Download ADCS Communicator

Secure proxy

The Secure Proxy provides access to the Email Infrastructure for 64-bit Redhat/CentOS.

Download secure proxy

Copyright © 2010-2015 Symantec Corporation. All rights reserved. [About Mobility Manager](#)

SymantecADSCComm...msi
2.1/2.1 MB, 0 secs left

57. Download and install the .NET Framework 4:

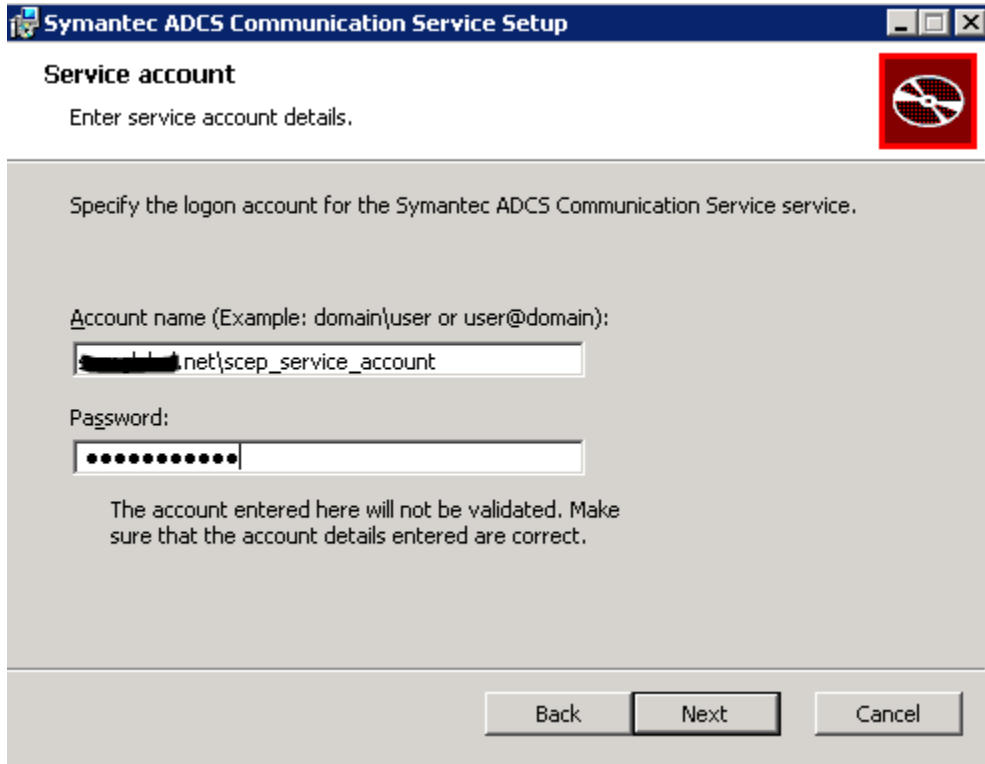
<http://www.microsoft.com/en-us/download/details.aspx?id=17851>

Note: A system reboot is required after installing .NET 4.

58. Run the SymantecADCSCommunicator.msi file, to begin, click **Next**.

59. Take note of the installation path, click **Next**.

60. Enter the scep user's credentials for the **Account name** and **Password**; click **Next**:

The image shows a Windows-style dialog box titled "Symantec ADCS Communication Service Setup". The main heading is "Service account" with a subtitle "Enter service account details." and a red square icon with a white circle and a diagonal line. The instruction text says "Specify the logon account for the Symantec ADCS Communication Service service." There are two input fields: "Account name (Example: domain\user or user@domain):" with the text ".net\scep_service_account" and "Password:" with masked characters. A warning message states "The account entered here will not be validated. Make sure that the account details entered are correct." At the bottom are "Back", "Next", and "Cancel" buttons.

Symantec ADCS Communication Service Setup

Service account
Enter service account details.

Specify the logon account for the Symantec ADCS Communication Service service.

Account name (Example: domain\user or user@domain):
[.net\scep_service_account]

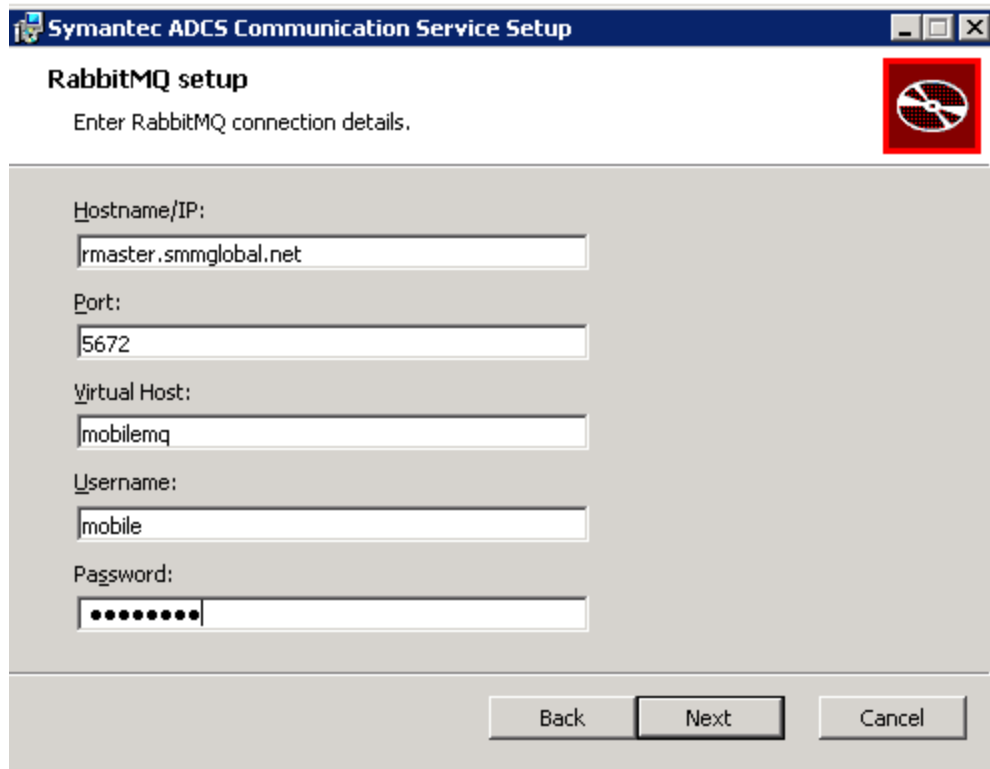
Password:
[.....]

The account entered here will not be validated. Make sure that the account details entered are correct.

Back Next Cancel

61. Enter the RabbitMQ information for the Mobility server.

Important: If a local RabbitMQ service was used, STOP and [read the beginning of this article](#). A production RabbitMQ service is required. See [HOWTO110356](#) to deploy a production RabbitMQ cluster. If this article was followed, all this information is stored on the Rabbit server in /var/log/rabbit-install.log



The image shows a Windows-style dialog box titled "Symantec ADCS Communication Service Setup". Inside the dialog, the section "RabbitMQ setup" is active, with the instruction "Enter RabbitMQ connection details." and a red RabbitMQ logo. The form contains six input fields: "Hostname/IP:" with the value "rmaster.smmglobal.net", "Port:" with "5672", "Virtual Host:" with "mobilemq", "Username:" with "mobile", and "Password:" with masked characters. At the bottom are "Back", "Next", and "Cancel" buttons.

Symantec ADCS Communication Service Setup

RabbitMQ setup

Enter RabbitMQ connection details.

Hostname/IP:
rmaster.smmglobal.net

Port:
5672

Virtual Host:
mobilemq

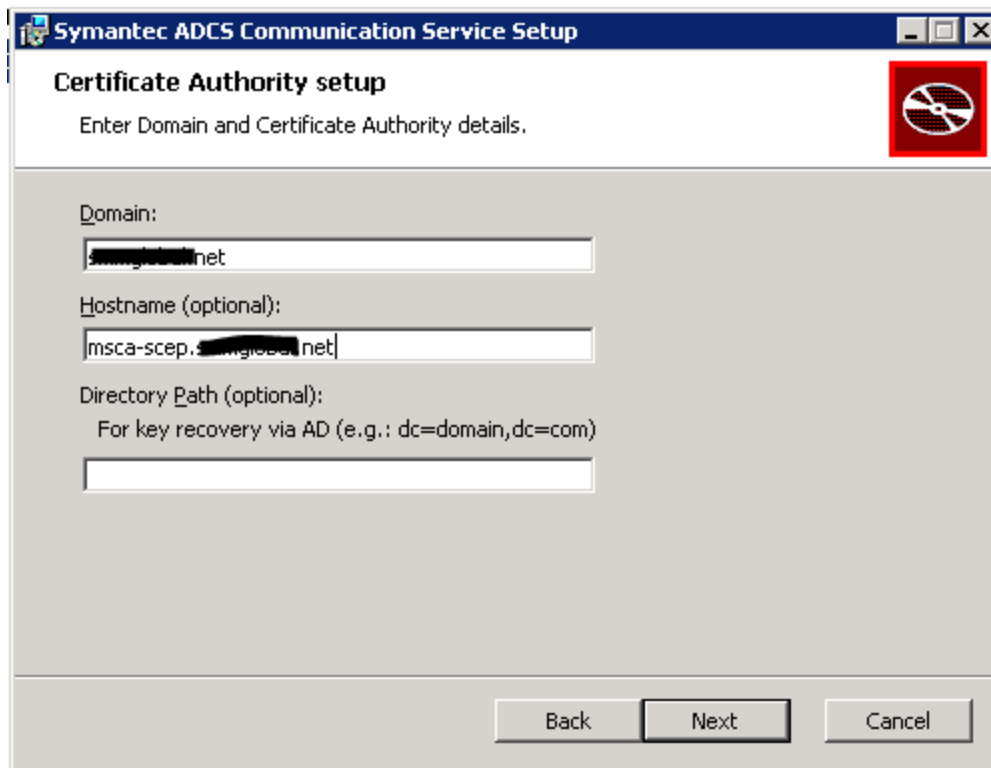
Username:
mobile

Password:
.....

Back Next Cancel

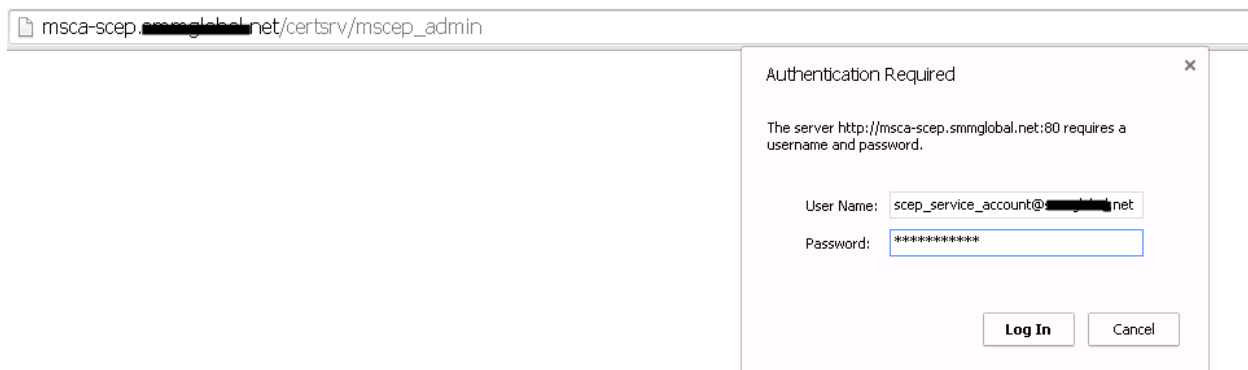
62. Verify that the domain information is correct and enter the server's published hostname, click **Next**.

Note: The server's hostname is the name used for the CN (Common Name) in the certificate, unless the certificate is wildcard. This hostname needs to be resolvable from the Mobility FE (front-end):

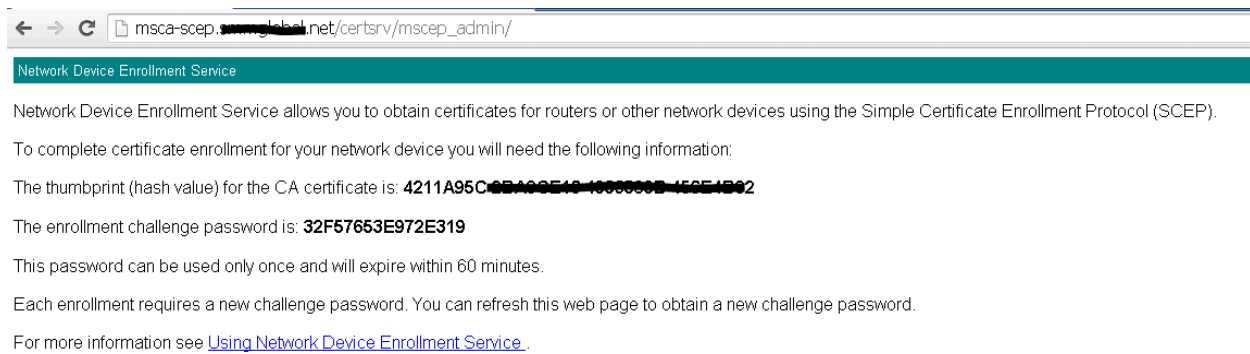


63. Enter the MSCA's SCEP/NDES admin URL and see the tip below...

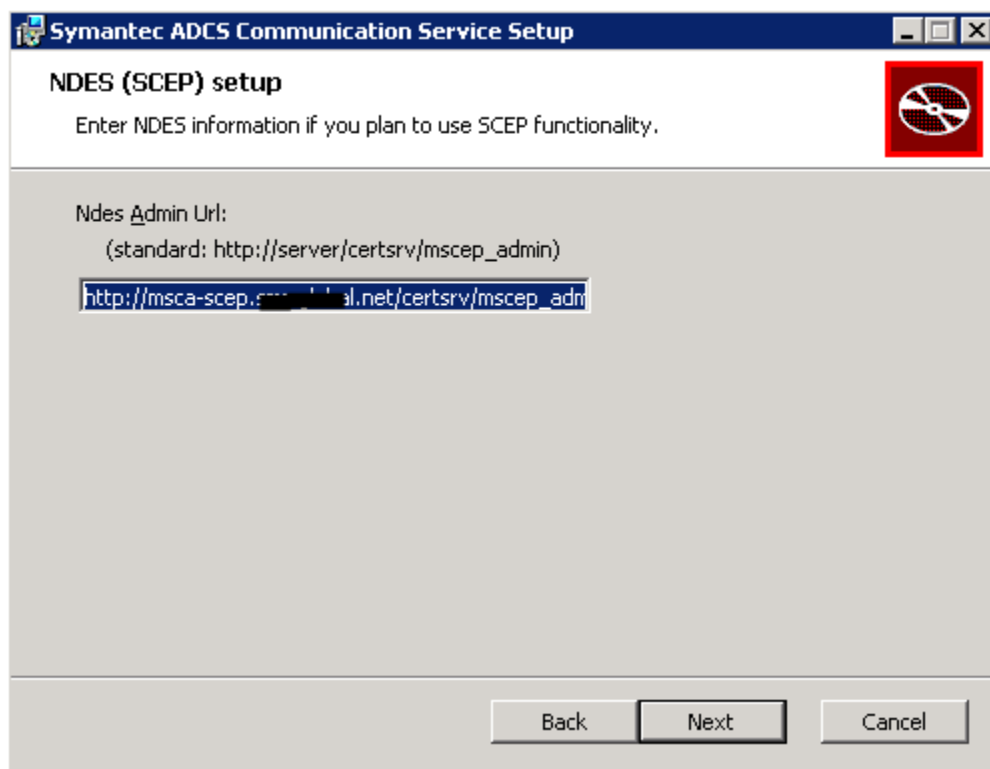
Tip: To test this URL, enter it into a browser, enter the SCEP user's credentials, click **Log In**:



After log in:



Once the URL is confirmed, click **Next**.



64. Click **Install**.

Add a Certificate Authority to Mobility

65. From the MSCA server, click **Start > Run** and enter **MMC**.
66. Click **File > Add remove snap-in**, select **Certificates** and click **Add**.
67. Select **Computer Account** and **Next**.
68. Ensure **Local computer** is selected and click **Finish**.
69. Click **OK**.

70. Expand the Certificates (Local computer) tree to **Personal Certificates**.
71. Right-click on the CA certificate and select **All tasks > Export**.
72. Click, **Next**; select **No, do not export the private key** and click **Next**.
73. Select **Base-64** and click **Next**.
74. Save the file as **CA_cert.cer** and click **Next**.

Note: This certificate needs to be accessible from the workstation accessing the Mobility admin console as it will be uploaded to the server.

75. From the Mobility **Admin console > Policies and rules > Device profiles**, click the + (plus) symbol next to **CERTIFICATE AUTHORITY**:
76. Name it, MSCA and select **Microsoft Certificate Authority** for **Type**:

New Certificate authority profile

| | |
|-------------|--|
| Name* | <input type="text" value="MSCA"/> |
| Description | <input type="text"/> |
| Type* | <input type="text" value="Microsoft Certificate Authority"/> |

77. Under **Settings** enter the **Domain Name** and **Hostname** from step 62, click **Test connection**. A green checkbox is displayed. If after some time it errors, verify that the Mobility server can resolve this hostname. Add it to the DNS or modify the server's /etc/hosts file.

New Certificate authority profile

| | |
|-------------|--|
| Name* | <input type="text" value="MSCA"/> |
| Description | <input type="text"/> |
| Type* | <input type="text" value="Microsoft Certificate Authority"/> |

Settings

Domain name and hostname must match the values specified in the Active Directory Certificate Services installer.

| | |
|---|---|
| Domain Name* | <input type="text" value="msca-scep:example.lan.net"/> |
| Hostname | <input type="text" value="msca-scep:example.lan.net"/> |
| New root certificate | <input type="button" value="Choose File"/> No file chosen |
| File type must be .cer, .crt, .der, or .pem | |

☒

78. Finally, click **Choose File** and browse to the certificate exported /saved in step 74. Click **Save**.
79. Click the + (plus) symbol next to the **CERTIFICATE TEMPLATE** profile.

80. Name it, IPsec and select the MSCA as the **Certificate Authority**.

81. For the template name, enter **IPSEIntermediateOnline** and click **Validate Template Name**:

New Certificate template profile

Name*

IPSec

Description

Settings

Certificate authority*

MSCA

Microsoft CA template name*

IPSEIntermediateOnline

Validate Template Name

✓

Policy details*

Key Size

2048 bits

Certificate template variables

Specify the source for the following values. Source can be hardcoded text, from user properties, the device, or user's directory (e.g. AD) information.

Lookups are specified as {user.lookup}, {device.lookup}, or {ldap.lookup}. You can specify any combination of tokens and hardcoded text.

| Name | Value |
|-------------|--------------------------|
| SubjectName | CN={user.first_name} {u: |
| SAN_UPN | {user.email} |

Tokens

| Device tokens | User tokens | LDAP tokens |
|----------------------------|-------------------|--------------------------|
| {device.device_class} | {user.email} | {ldap.*} |
| {device.IMEI} | {user.first_name} | * means any LDAP setting |
| {device.name} | {user.id} | |
| {device.platform} | {user.last_name} | |
| {device.product_string} | {user.username} | |
| {device.serial_number} | | |
| {device.udid} | | |
| {device.unique_identifier} | | |

Save

Cancel

82. Click **Save**.

83. Click the **+** (**plus**) symbol next to **SCEP**.

84. Name the Profile **SCEP** and enter the URL of the MSCA enrollment service. The FQDN is this URL needs to be resolvable from the Mobile Devices. EG <https://msca-scep.acme.company.org/certsrv/mscep/mscep.dll>

Tip: Test this URL in a workstation to ensure that it arrives at the device enrollment page of the MSCA/NDES server.

85. Select **Generate Per Request** for the **Challenge Password**.

86. Navigate, from the workstation, to the SCEP admin URL from step 63 and copy the CA's thumbprint as the **Fingerprint**.

Note: Spaces in the Fingerprint/Thumbprint are okay.

87. Select **IPSec** as the **Template** and 2048 as the **Key strength**; click **Save**:

New SCEP profile

Missing data: URL cannot be blank or an empty string.

Name^{*} SCEP

Description

Settings

URL^{*} <https://msca-scep.smmglobal.net/certsrv/mscep/mscep.dll>

Challenge password
☐ None
☒ Generate Per Request
☐ Master Challenge Password

Retry count 3 ▼

Retry period 5 ▼ minutes

Fingerprint 4211A95C 2BA8CE16 4036580B 456E4B82

Certificate template IPSec ▼

Subject^{*} CN={user.first_name}{user.last_name}

SAN type None

Subject alternative name {user.email}

Key Usage ☒ Signing and verification ☒ Encryption and decryption

Key strength 2048 bits ▼

Save

Cancel

88. Click the + (plus) symbol next to **CREDENTIALS** and name the credential **Device Enrollment**.
89. For **Certificate type** select **SCEP**.
90. For the SCEP Profile select **SCEP**, and click **Save**:

New Credentials profile

| | |
|-------------|--|
| Name* | <input type="text" value="Device Enrollment"/> |
| Description | <input type="text"/> |
| OS | <input type="text" value="iOS"/> |

Settings

Select the certificate profile that will be pushed to a device and stored in the general keystore to use with browsers and apps.

| | |
|------------------|-----------------------------------|
| Certificate type | <input type="text" value="SCEP"/> |
| SCEP profile | <input type="text" value="SCEP"/> |

Add the SCEP Profile to a Device Policy

91. If not device profile has been created, create one.
92. Select the profile and click the edit symbol (Pencil).
93. Ensure enable MDM for iOS devices is checked and scroll down to the bottom of the edit window.
94. Under **Credentials** click **Add** and select **Device Enrollment**.
95. Save the profile and test it by enrolling a new iOS device that does not already have an MDM profile installed.
96. Verify that the server has issued a SCEP certificate by going to the Server Manager and expand **Active Directory Certificate Authority > Server_Name > Issued Certificates**. There should be a new certificate(s) issued to users by the First and Last names:

