# CONTENT INDEX

**http://www.scconfigmgr.com/2017/11/23/how-to-setup-co-management-part-1/ - Check this link for detailed notes**

## PRE-REQUISITES:

1. PKI IMPLEMENTATION WITHIN CB 1710 INFRASTRUCTURE
2. AZURE SUBSCRIPTION
3. INTUNE, EMS, O365 TRIAL / FULL LICENSE REQUIRED

# CLOUD MANAGEMENT GATEWAY PROCESS

Login to Azure Portal

Click New - Type Cloud Service - Click Create

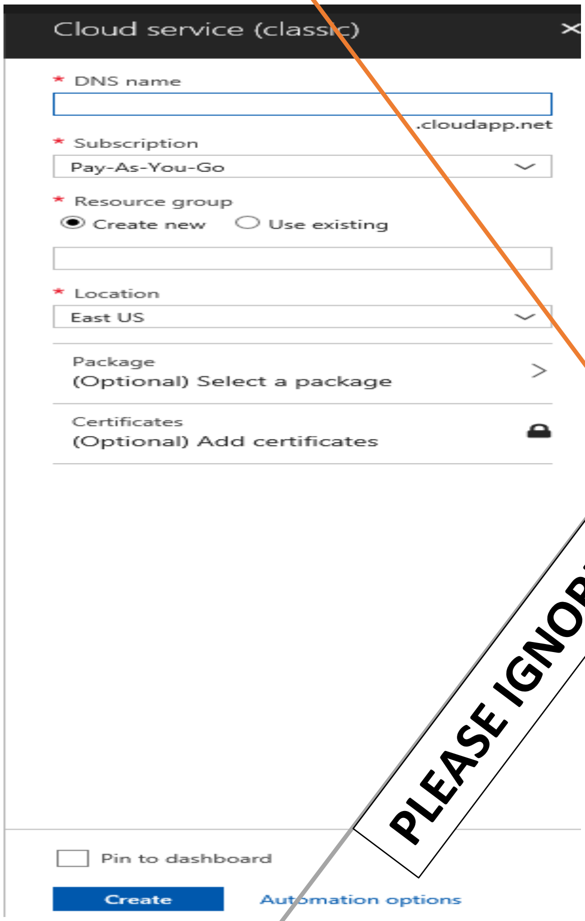
For DNS name type your domain name – in my example it is RAMLAN

For Resource Group – Create New – Call it CMG

Location – East US (this depends on where you are located).

You can leave AS IS for Package and Certificates

Click Create



Cloud service (classic)

* DNS name

.cloudapp.net

* Subscription

Pay-As-You-Go

* Resource group

● Create new ○ Use existing

* Location

East US

Package

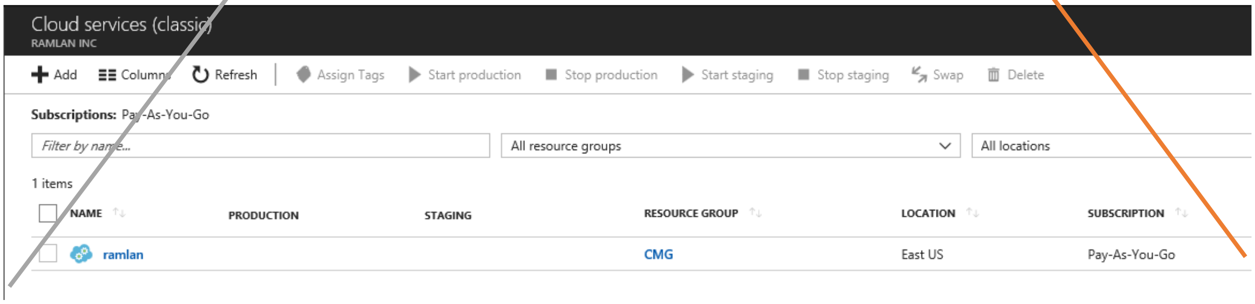
(Optional) Select a package

Certificates

(Optional) Add certificates

□ Pin to dashboard

This is what you will see at the end of creation



Cloud services (classic)

RAMLAN INC

Subscriptions: Pay-As-You-Go

Filter by name...

All resource groups

All locations

1 items

| NAME | PRODUCTION | STAGING | RESOURCE GROUP | LOCATION | SUBSCRIPTION |
|---|---|---|---|---|---|
| ramlan | | | CMG | East US | Pay-As-You-Go |

PLEASE IGNORE THIS STEPS/PAGE AS PART OF INSTALL NOTES

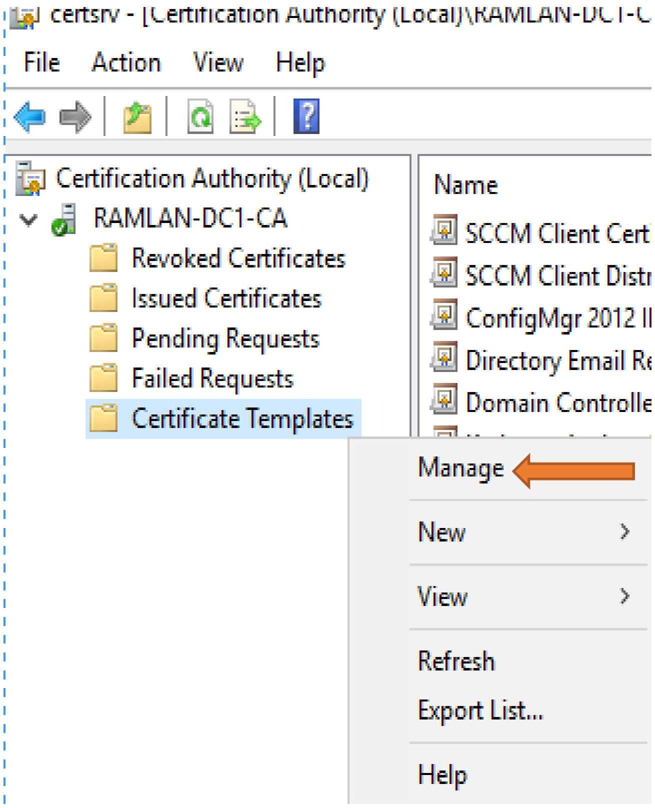
We will create following certificates using Internal Certificate Authority

**Management, Web Server, Trusted Root & Client Authentication Certificate**

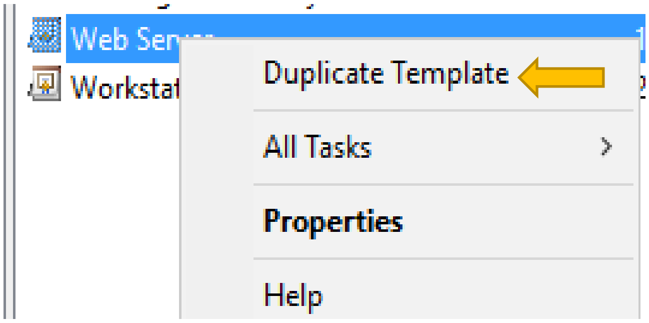
Open Certificate Authority from Administrative Tools

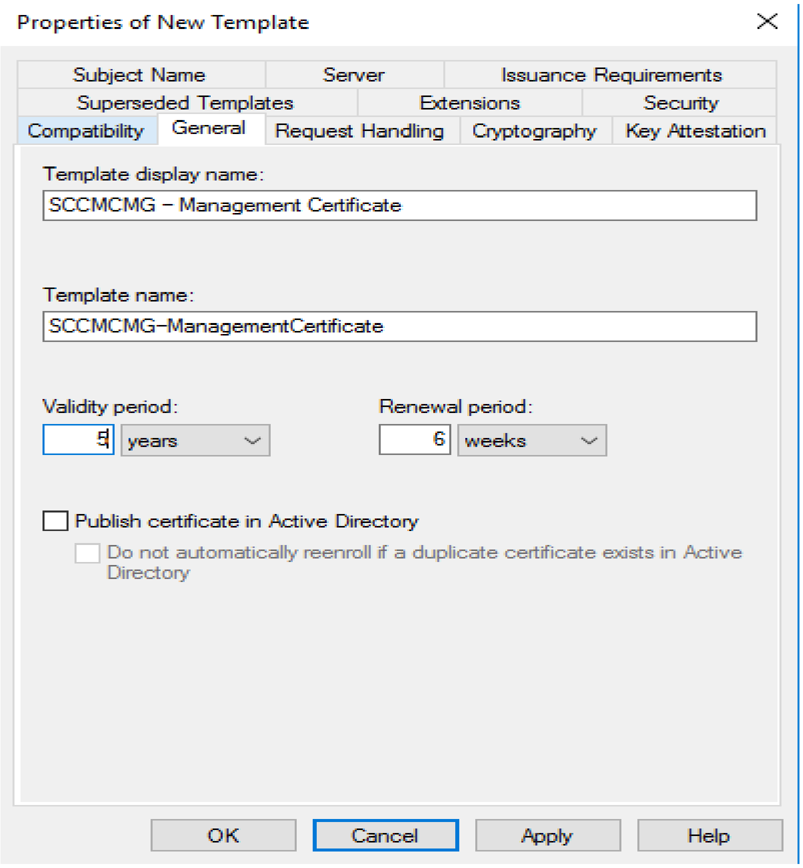
**MANAGEMENT CERTIFICATE**

Right Click Certificate Template – Manage



Right Click Web Server – Click Duplicate Template





Template display name:
SCCMCMG – Management Certificate

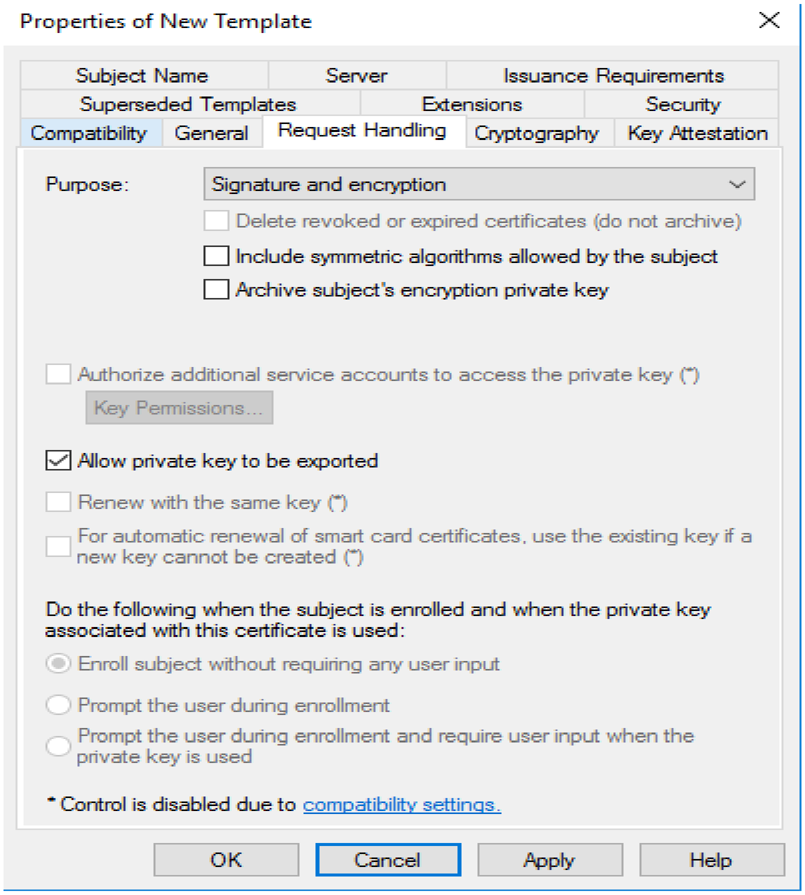
Template name:
SCCMCMG–ManagementCertificate

Validity period: 5 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory



Purpose: Signature and encryption

□ Delete revoked or expired certificates (do not archive)

□ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

□ Authorize additional service accounts to access the private key (*)

☑ Allow private key to be exported

□ Renew with the same key (*)

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

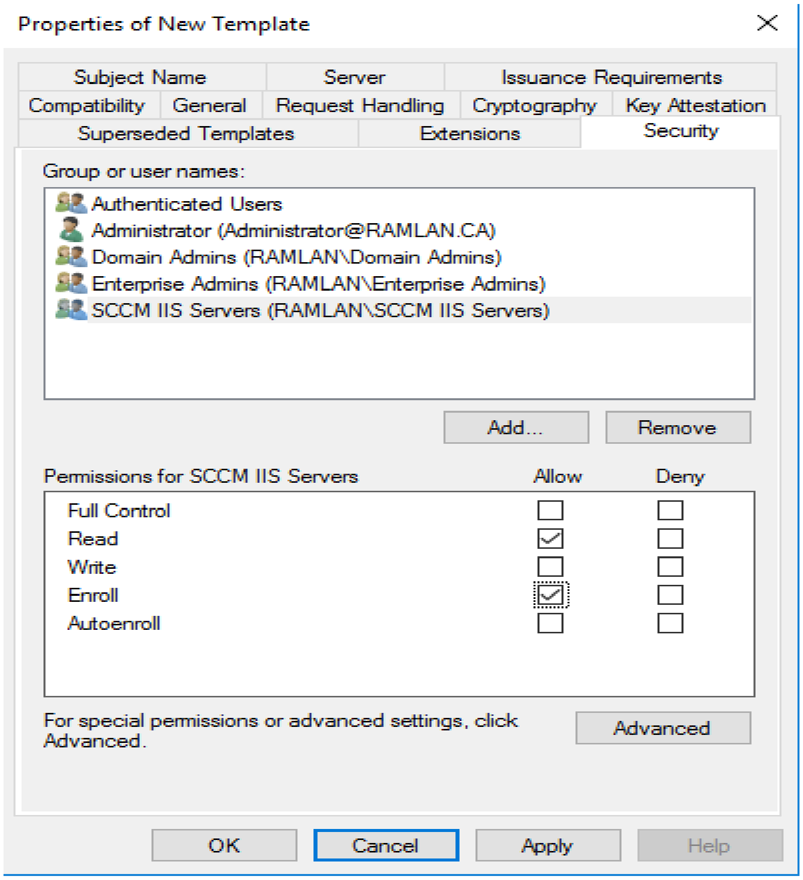
Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to compatibility settings.



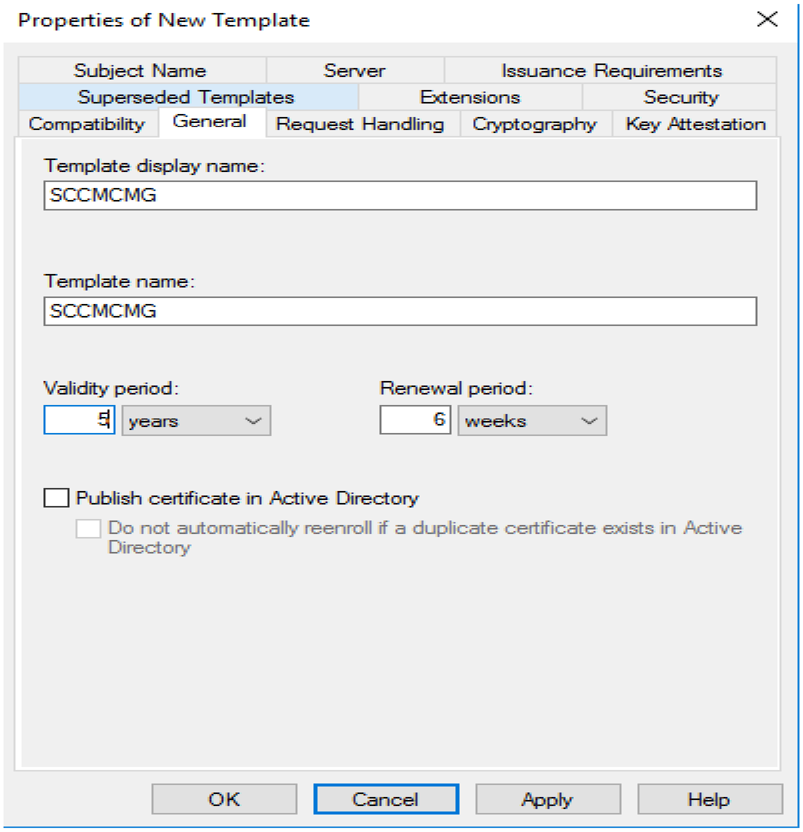
Group or user names:

- Authenticated Users
- Administrator (Administrator@RAMLAN.CA)
- Domain Admins (RAMLAN\Domain Admins)
- Enterprise Admins (RAMLAN\Enterprise Admins)
- SCCM IIS Servers (RAMLAN\SCCM IIS Servers)

| Permissions for SCCM IIS Servers | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Read | ☑ | □ |
| Write | □ | □ |
| Enroll | ☑ | □ |
| Autoenroll | □ | □ |

For special permissions or advanced settings, click Advanced.

## WEB SERVER CERTIFICATE



Template display name:
SCCMCMG

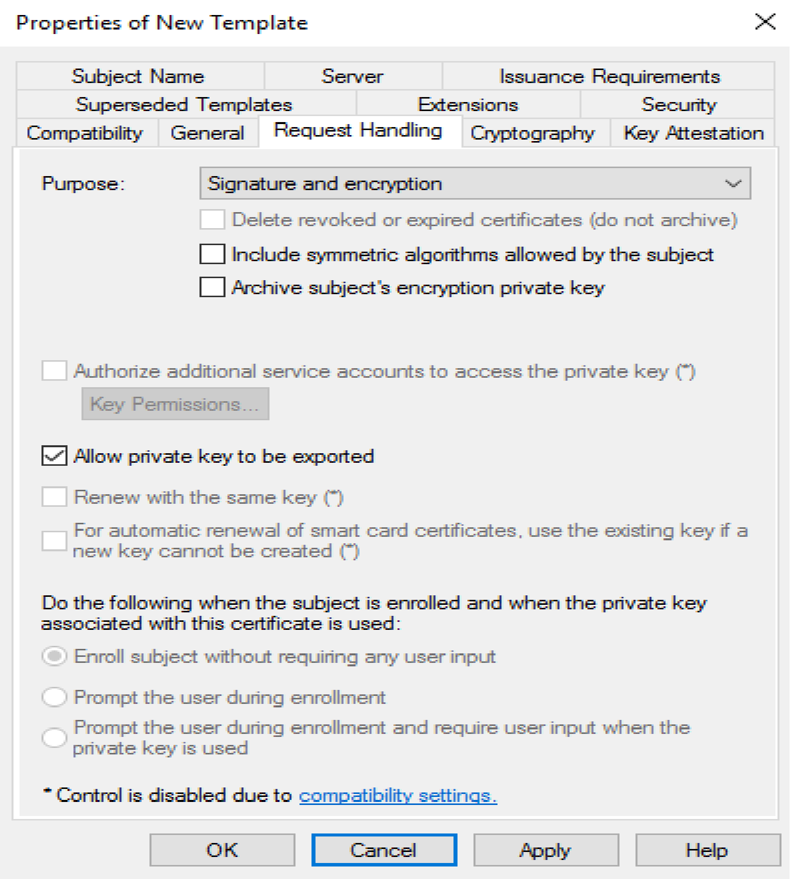
Template name:
SCCMCMG

Validity period: 5 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory



Properties of New Template

Purpose: Signature and encryption

□ Delete revoked or expired certificates (do not archive)

□ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

□ Authorize additional service accounts to access the private key (*)

☑ Allow private key to be exported

□ Renew with the same key (*)

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

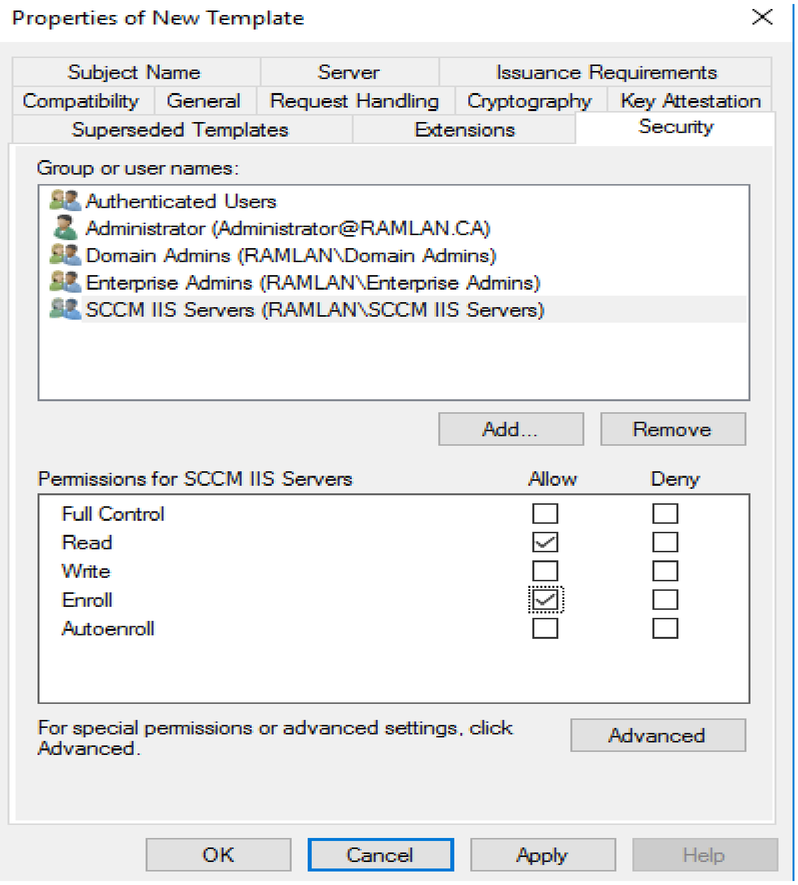
Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to compatibility settings.



Properties of New Template

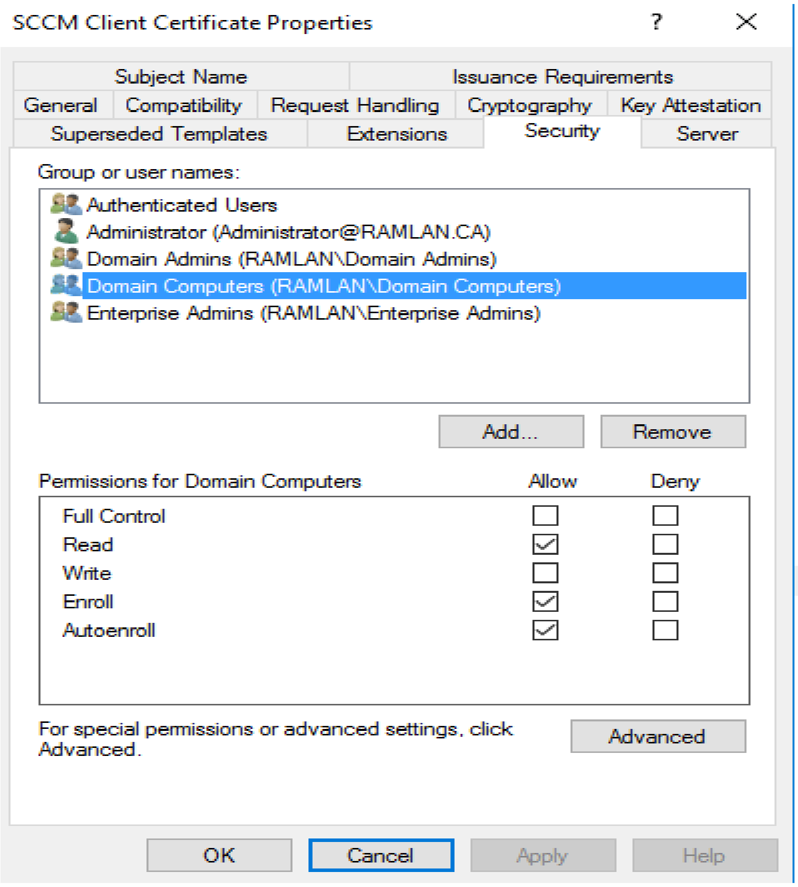
Group or user names:

- Authenticated Users
- Administrator (Administrator@RAMLAN.CA)
- Domain Admins (RAMLAN\Domain Admins)
- Enterprise Admins (RAMLAN\Enterprise Admins)
- SCCM IIS Servers (RAMLAN\SCCM IIS Servers)

| Permissions for SCCM IIS Servers | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Read | ☑ | □ |
| Write | □ | □ |
| Enroll | ☑ | □ |
| Autoenroll | □ | □ |

For special permissions or advanced settings, click Advanced.

If you have not implemented PKI within your SCCM infrastructure, then you need to create another Workstation Authentication template for client authentication.  You can call it SCCM Client Cert – CMG. Make sure the security settings will be as follows



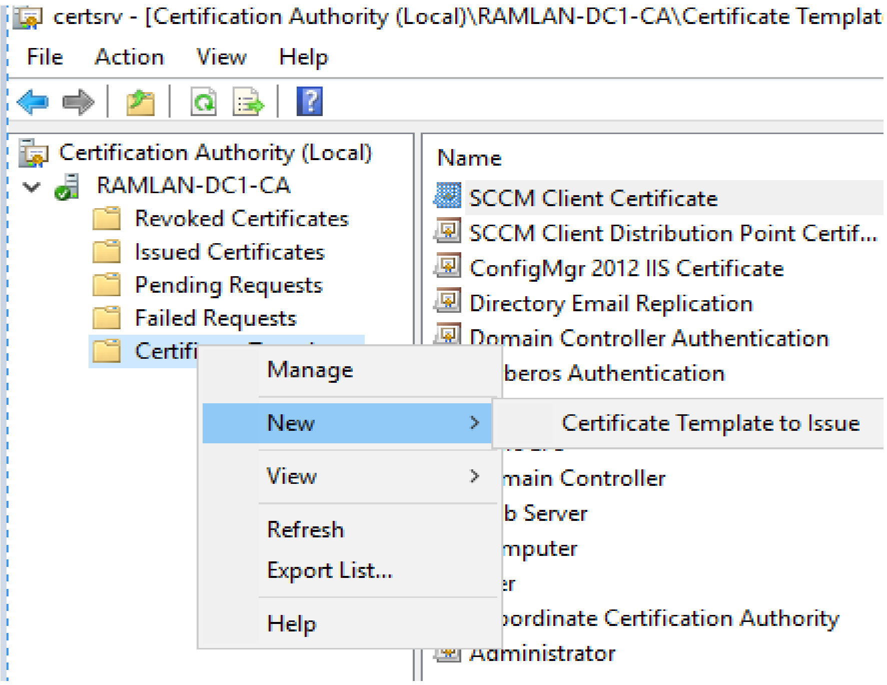
Group or user names:

- Authenticated Users
- Administrator (Administrator@RAMLAN.CA)
- Domain Admins (RAMLAN\Domain Admins)
- Domain Computers (RAMLAN\Domain Computers)
- Enterprise Admins (RAMLAN\Enterprise Admins)

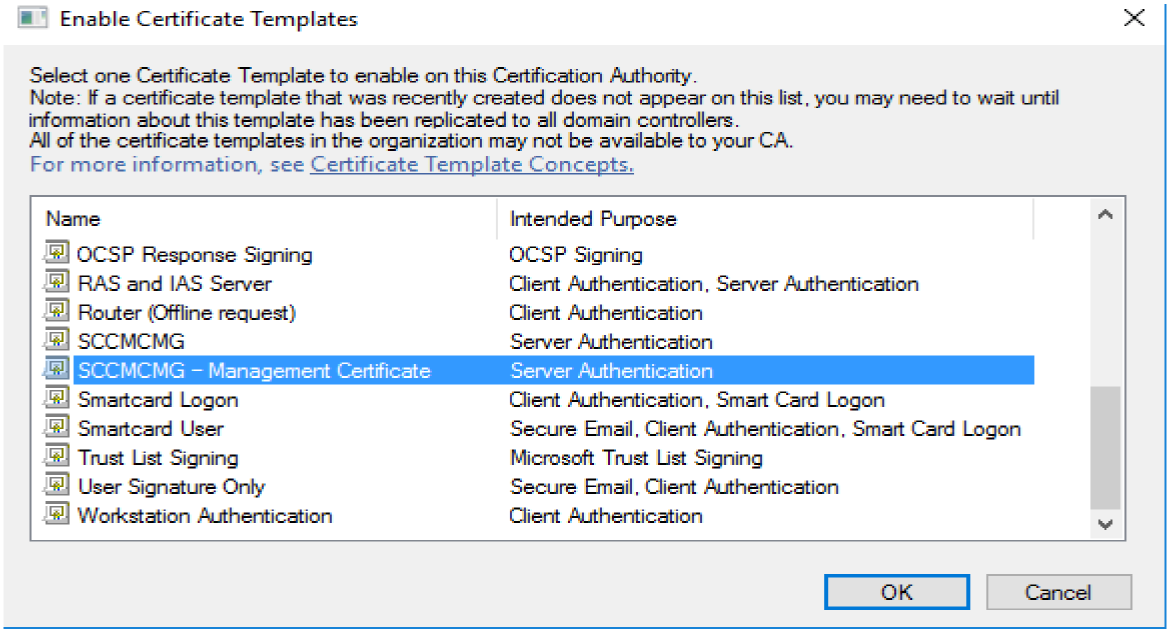
| Permissions for Domain Computers | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Read | ☑ | □ |
| Write | □ | □ |
| Enroll | ☑ | □ |
| Autoenroll | ☑ | □ |

For special permissions or advanced settings, click Advanced.

Now all the certificates are ready – we will issue them



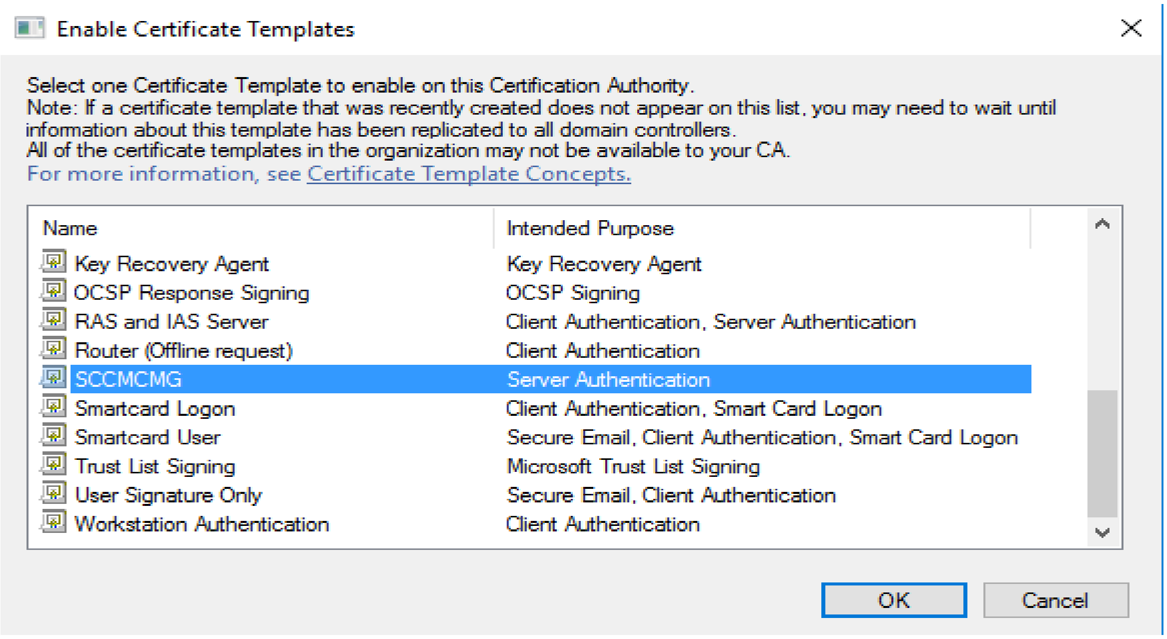
- SCCM Client Certificate
- SCCM Client Distribution Point Certif...
- ConfigMgr 2012 IIS Certificate
- Directory Email Replication
- Domain Controller Authentication
- beros Authentication
- main Controller
- b Server
- mputer
- er
- ordinate Certification Authority
- Administrator



Enable Certificate Templates

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.

| Name | Intended Purpose |
|---|---|
| OCSP Response Signing | OCSP Signing |
| RAS and IAS Server | Client Authentication, Server Authentication |
| Router (Offline request) | Client Authentication |
| SCCMCMG | Server Authentication |
| SCCMCMG – Management Certificate | Server Authentication |
| Smartcard Logon | Client Authentication, Smart Card Logon |
| Smartcard User | Secure Email, Client Authentication, Smart Card Logon |
| Trust List Signing | Microsoft Trust List Signing |
| User Signature Only | Secure Email, Client Authentication |
| Workstation Authentication | Client Authentication |

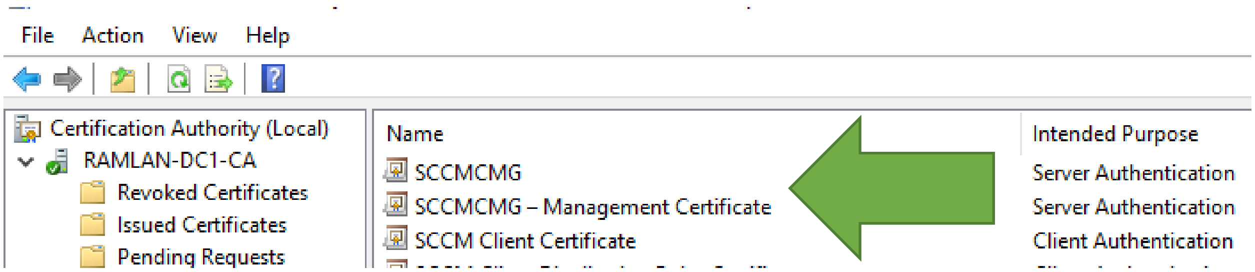


Enable Certificate Templates

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.

| Name | Intended Purpose |
|---|---|
| Key Recovery Agent | Key Recovery Agent |
| OCSP Response Signing | OCSP Signing |
| RAS and IAS Server | Client Authentication, Server Authentication |
| Router (Offline request) | Client Authentication |
| SCCMCMG | Server Authentication |
| Smartcard Logon | Client Authentication, Smart Card Logon |
| Smartcard User | Secure Email, Client Authentication, Smart Card Logon |
| Trust List Signing | Microsoft Trust List Signing |
| User Signature Only | Secure Email, Client Authentication |
| Workstation Authentication | Client Authentication |

You will see these certificates under Certificate Templates that are available for enrollment

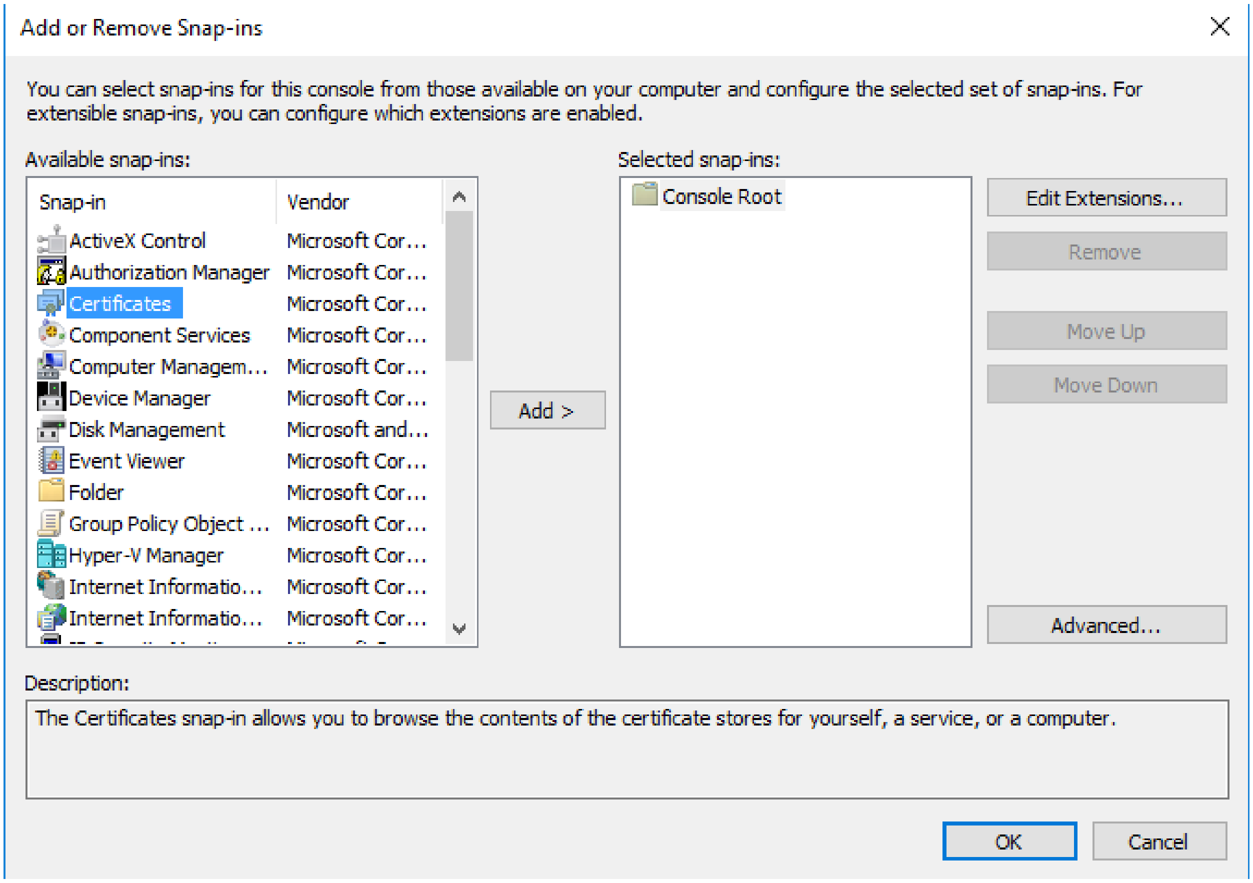


| Name | Intended Purpose |
|---|---|
| SCCMCMG | Server Authentication |
| SCCMCMG – Management Certificate | Server Authentication |
| SCCM Client Certificate | Client Authentication |

Now we will request the certificate.  I am going to request it on Configuration Manager Computer

Click Run – MMC

File – Add/Remove Snap IN



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

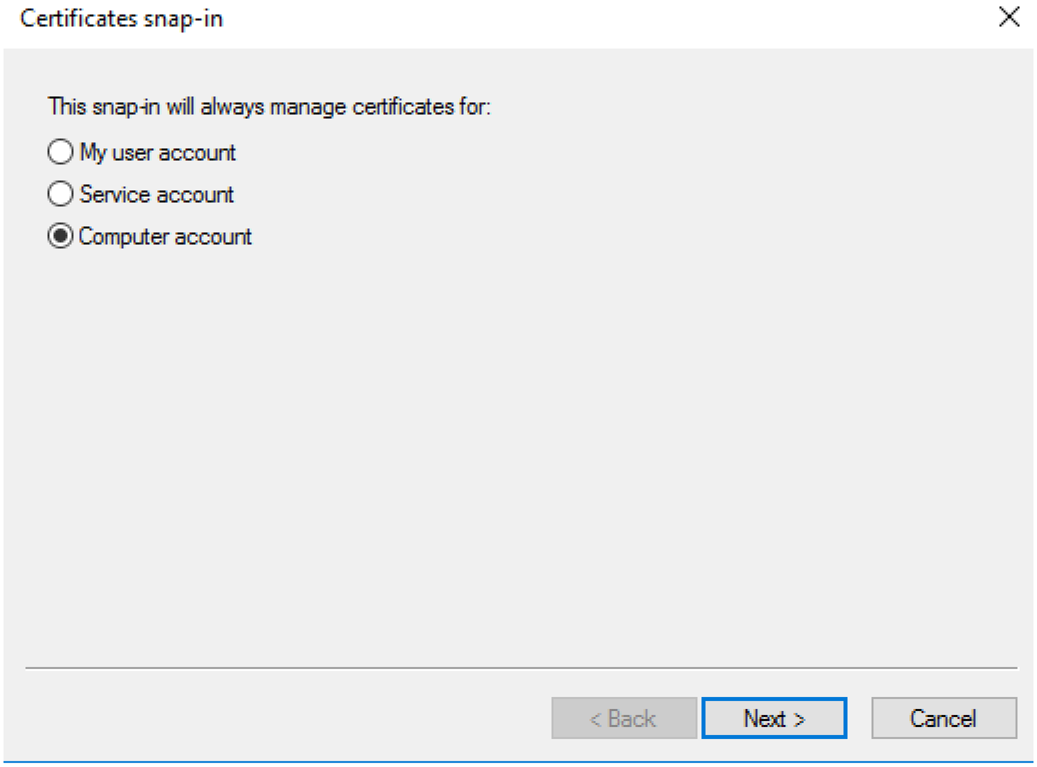
| Snap-in | Vendor |
|---|---|
| ActiveX Control | Microsoft Cor… |
| Authorization Manager | Microsoft Cor… |
| Certificates | Microsoft Cor… |
| Component Services | Microsoft Cor… |
| Computer Managem… | Microsoft Cor… |
| Device Manager | Microsoft Cor… |
| Disk Management | Microsoft and… |
| Event Viewer | Microsoft Cor… |
| Folder | Microsoft Cor… |
| Group Policy Object … | Microsoft Cor… |
| Hyper-V Manager | Microsoft Cor… |
| Internet Informatio… | Microsoft Cor… |
| Internet Informatio… | Microsoft Cor… |

Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.



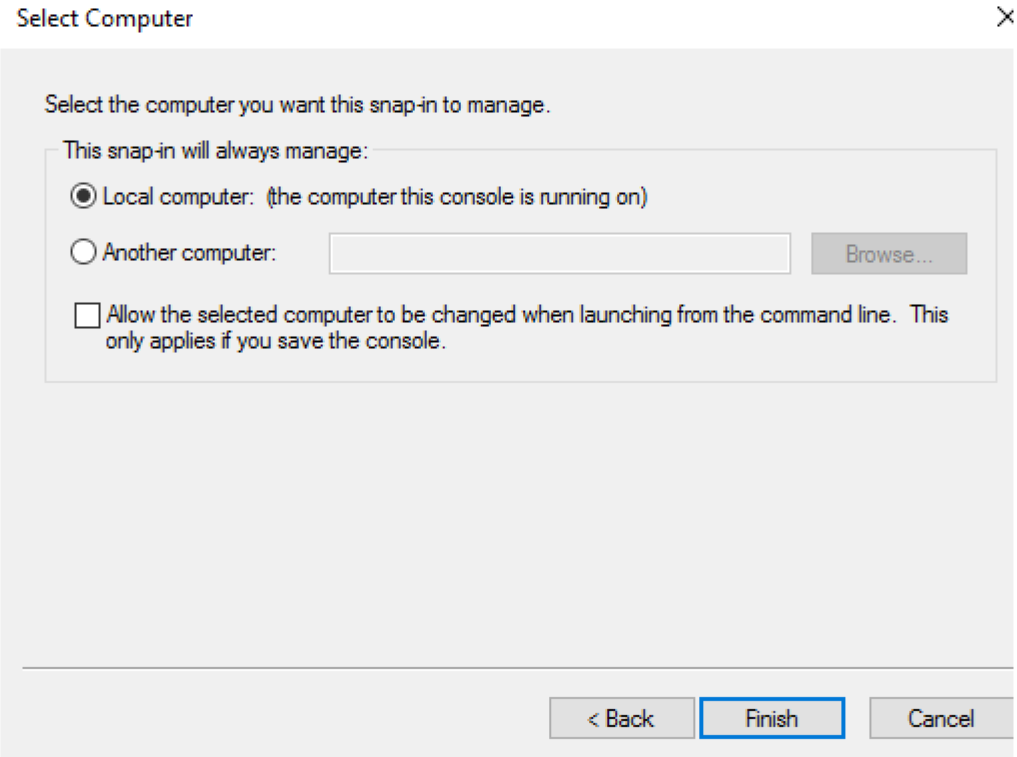
Certificates snap-in

This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account



Select Computer

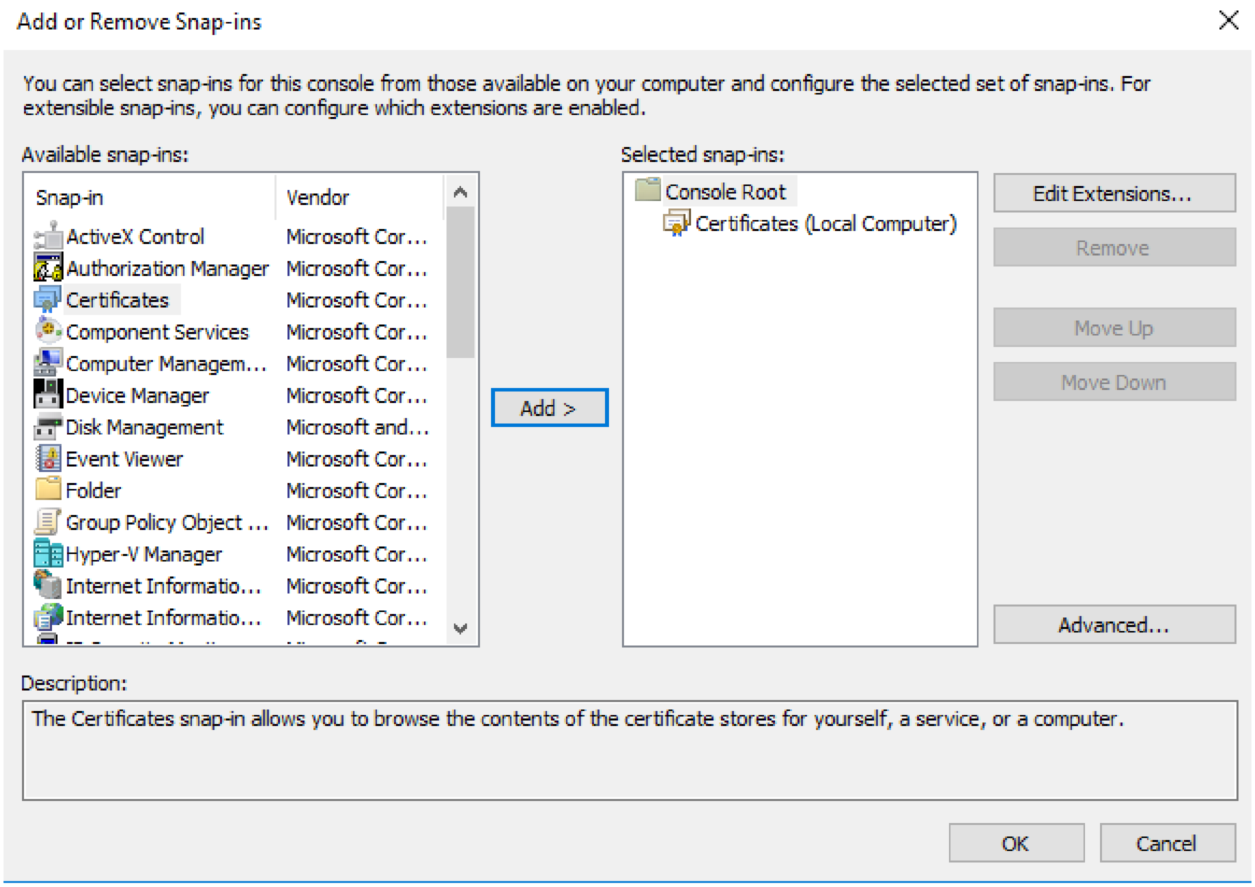
Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

| Snap-in | Vendor |
|---|---|
| ActiveX Control | Microsoft Cor… |
| Authorization Manager | Microsoft Cor… |
| Certificates | Microsoft Cor… |
| Component Services | Microsoft Cor… |
| Computer Managem… | Microsoft Cor… |
| Device Manager | Microsoft Cor… |
| Disk Management | Microsoft and… |
| Event Viewer | Microsoft Cor… |
| Folder | Microsoft Cor… |
| Group Policy Object … | Microsoft Cor… |
| Hyper-V Manager | Microsoft Cor… |
| Internet Informatio… | Microsoft Cor… |
| Internet Informatio… | Microsoft Cor… |

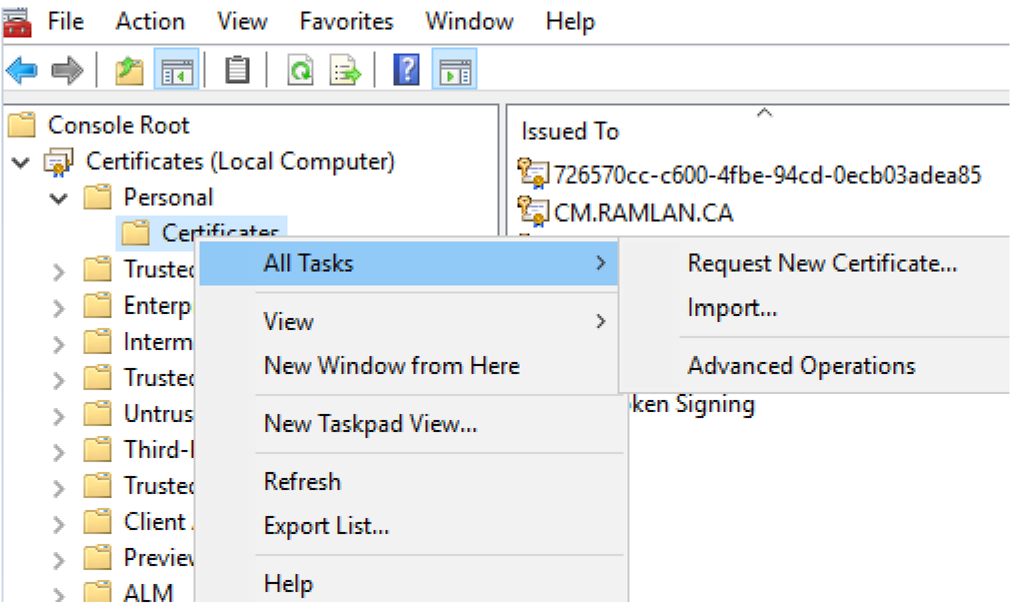
Selected snap-ins:

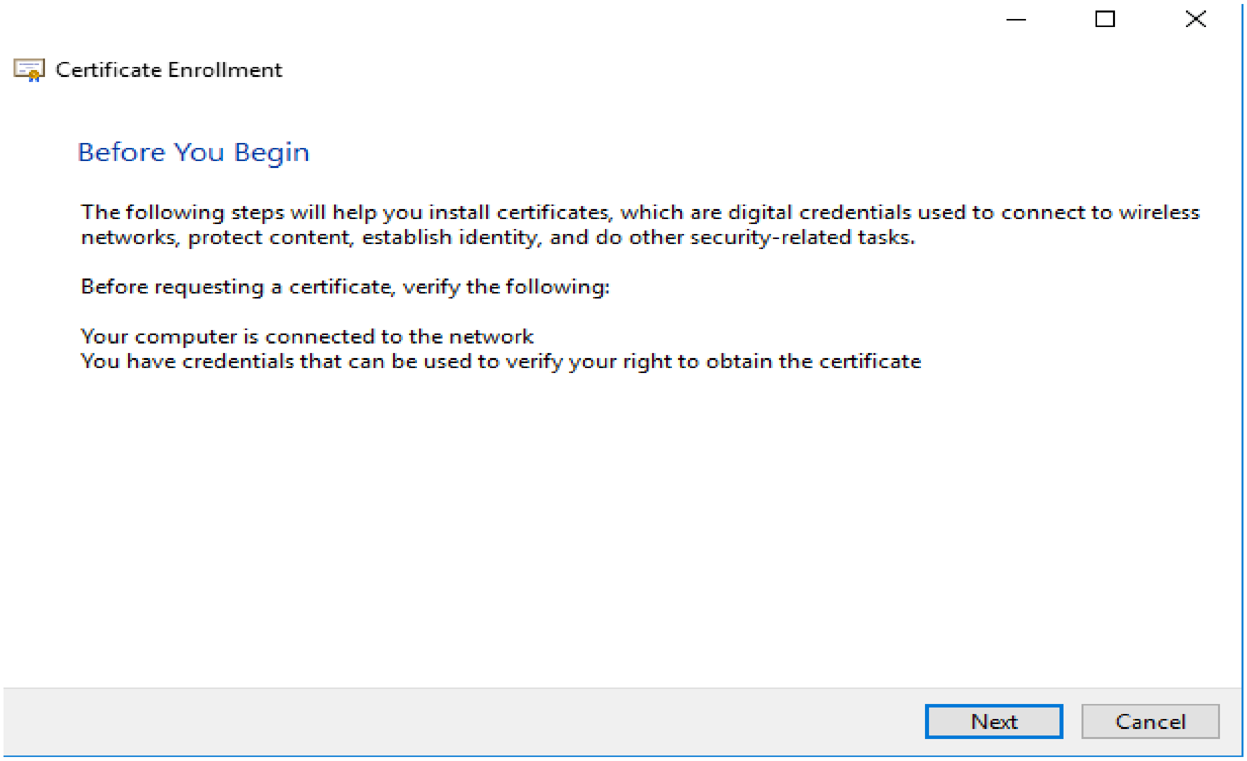
- Console Root
  - Certificates (Local Computer)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Go to Personal – Request New Certificate





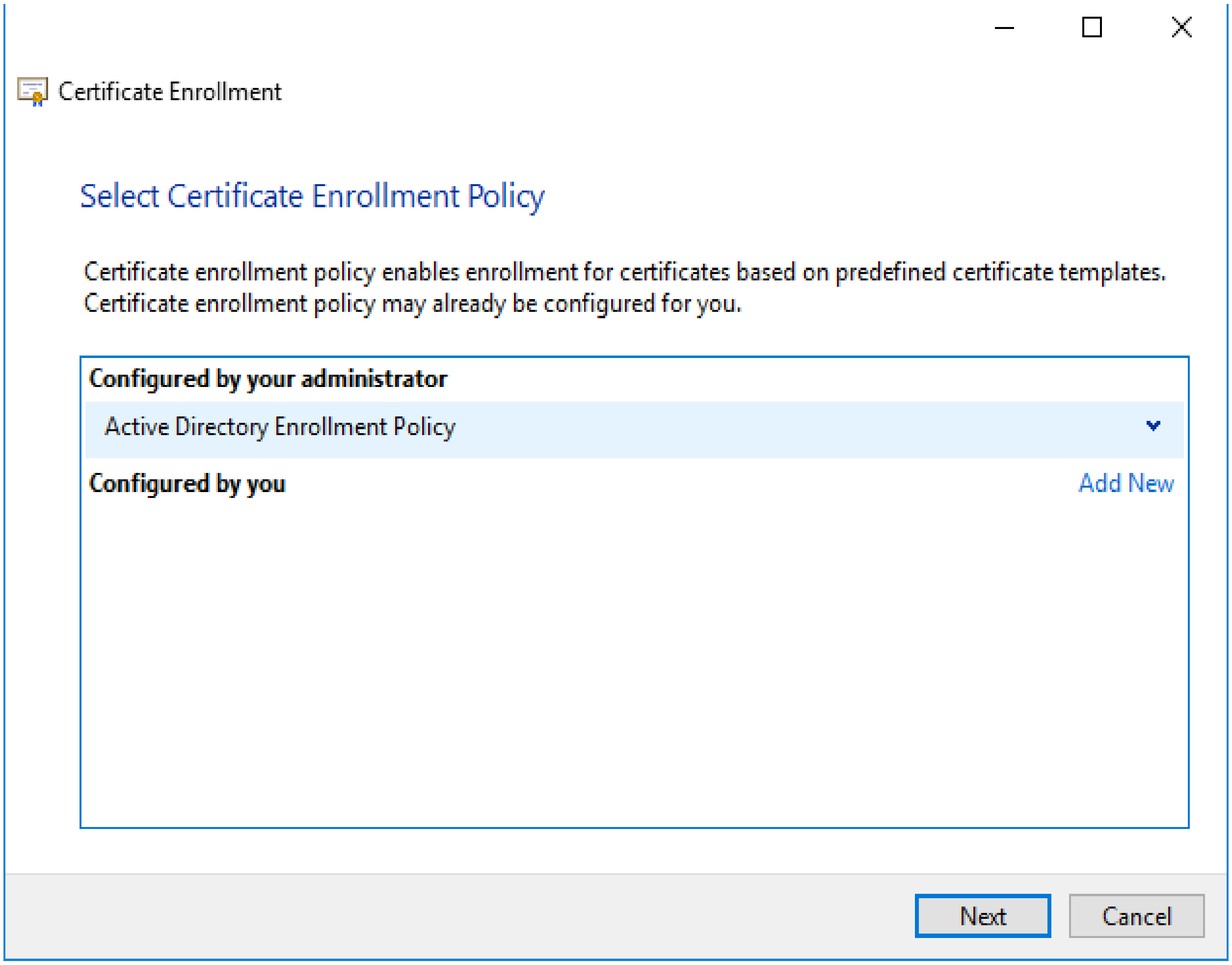
Certificate Enrollment

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



Certificate Enrollment

Select Certificate Enrollment Policy

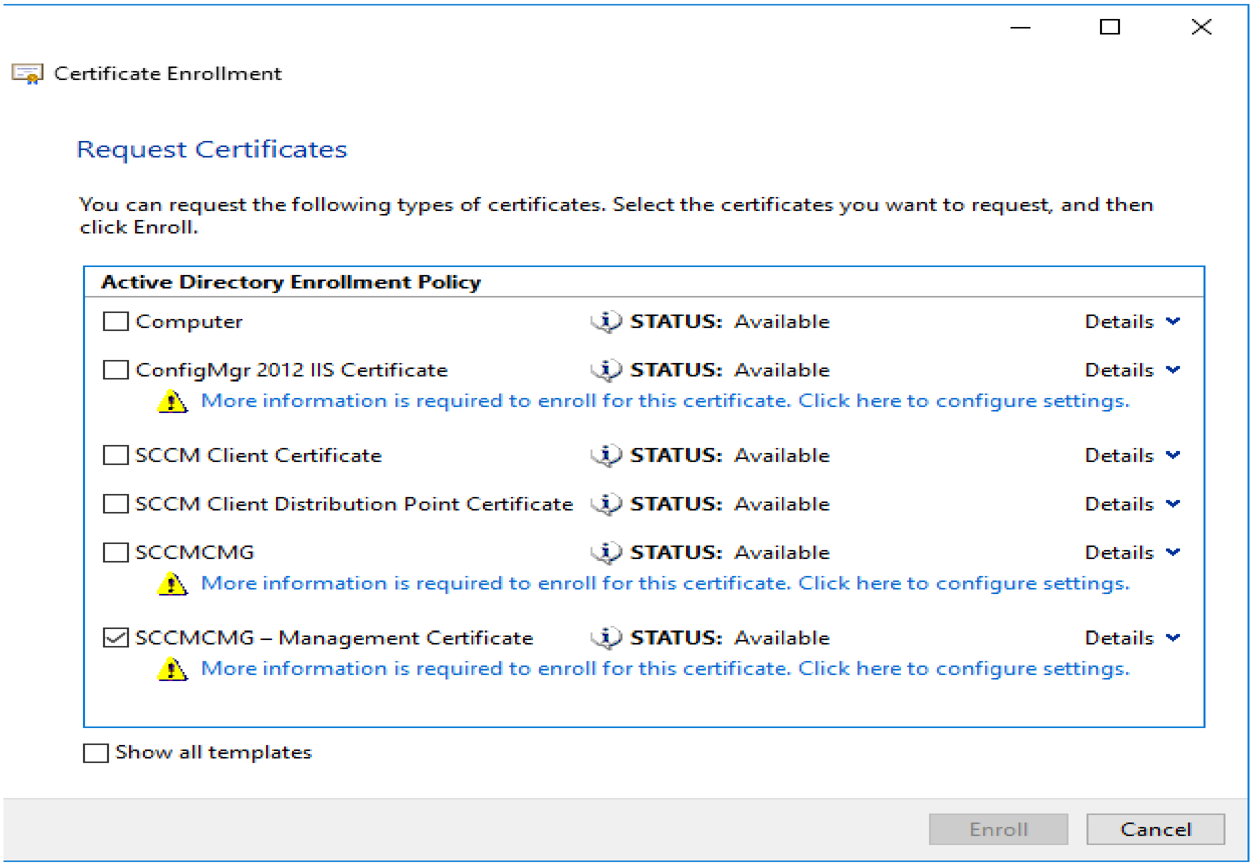
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

**Configured by your administrator**

Active Directory Enrollment Policy

**Configured by you**

Select SCCMCMG – Management Certificate and click More Information



Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

**Active Directory Enrollment Policy**

□ Computer **STATUS:** Available Details

□ ConfigMgr 2012 IIS Certificate **STATUS:** Available Details
More information is required to enroll for this certificate. Click here to configure settings.

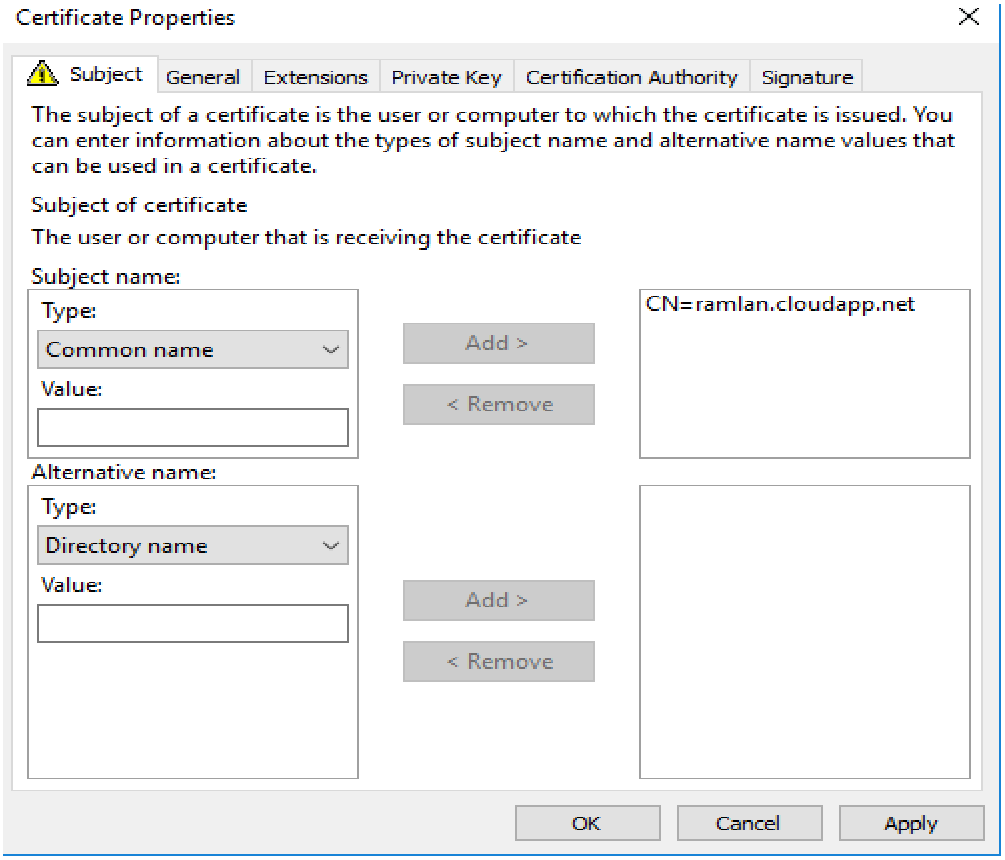
□ SCCM Client Certificate **STATUS:** Available Details

□ SCCM Client Distribution Point Certificate **STATUS:** Available Details

□ SCCMCMG **STATUS:** Available Details
More information is required to enroll for this certificate. Click here to configure settings.

☑ SCCMCMG – Management Certificate **STATUS:** Available Details
More information is required to enroll for this certificate. Click here to configure settings.

□ Show all templates



Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Common name

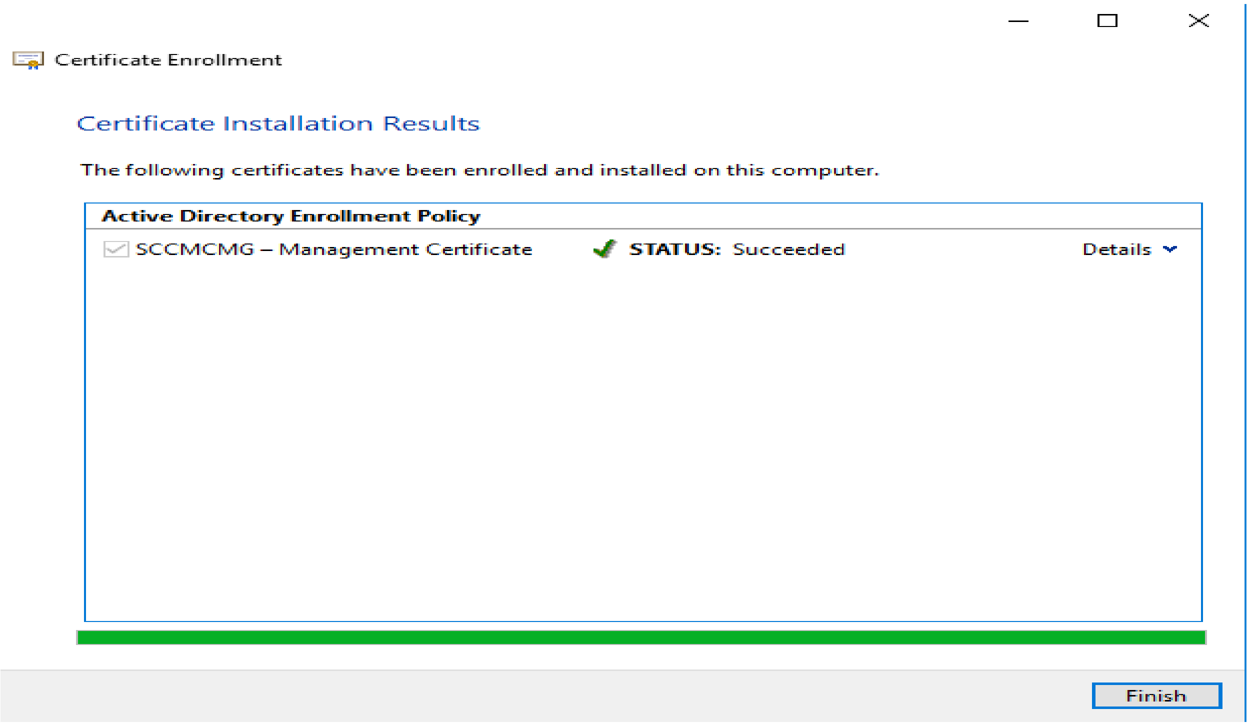
Value:

CN=ramlan.cloudapp.net

Alternative name:

Type: Directory name

Value:


Certificate Enrollment

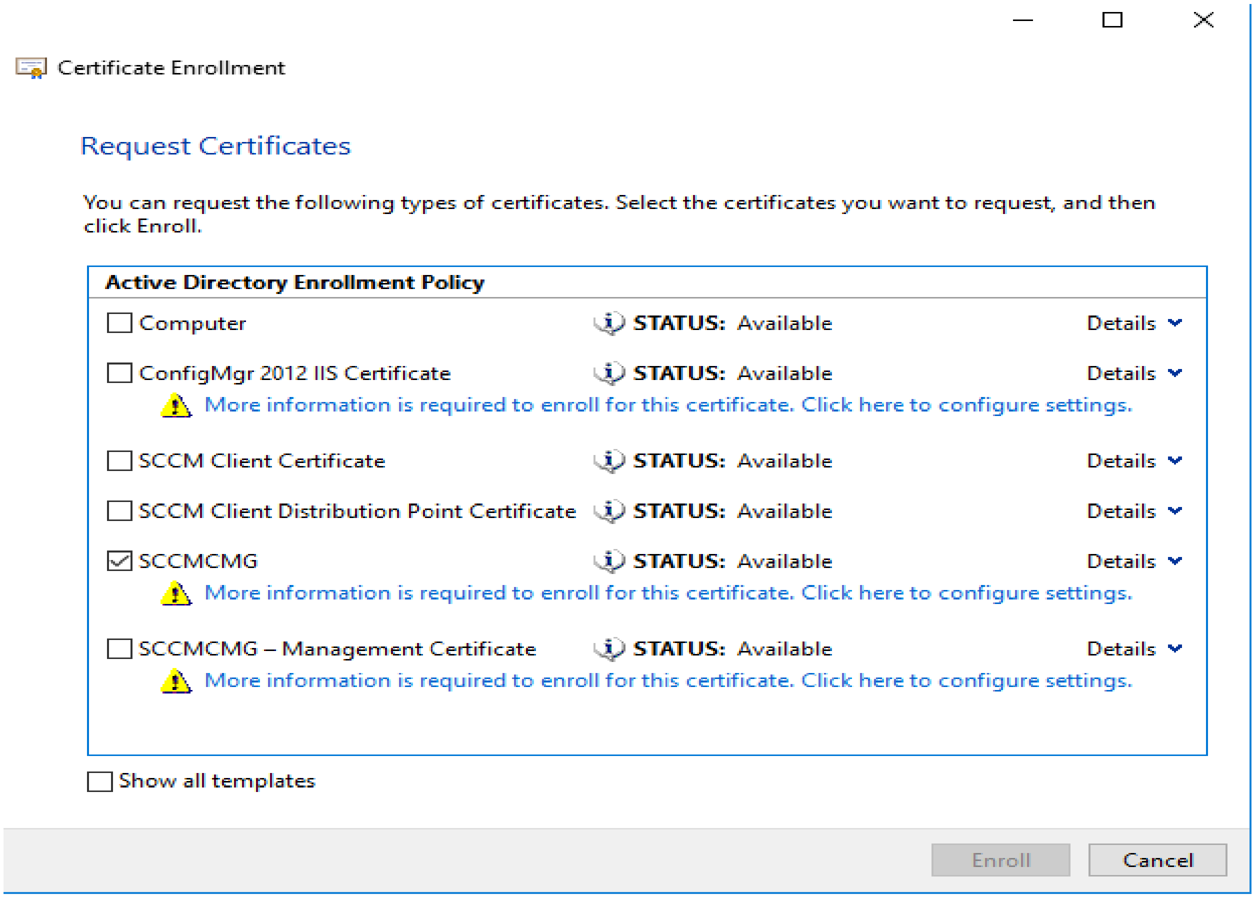
Certificate Installation Results

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

**Active Directory Enrollment Policy**

☑ SCCMCMG – Management Certificate ✓ **STATUS:** Succeeded Details

Do the same for Web Server Certificate


Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

**Active Directory Enrollment Policy**

□ Computer **STATUS:** Available Details

□ ConfigMgr 2012 IIS Certificate **STATUS:** Available Details
⚠ More information is required to enroll for this certificate. Click here to configure settings.

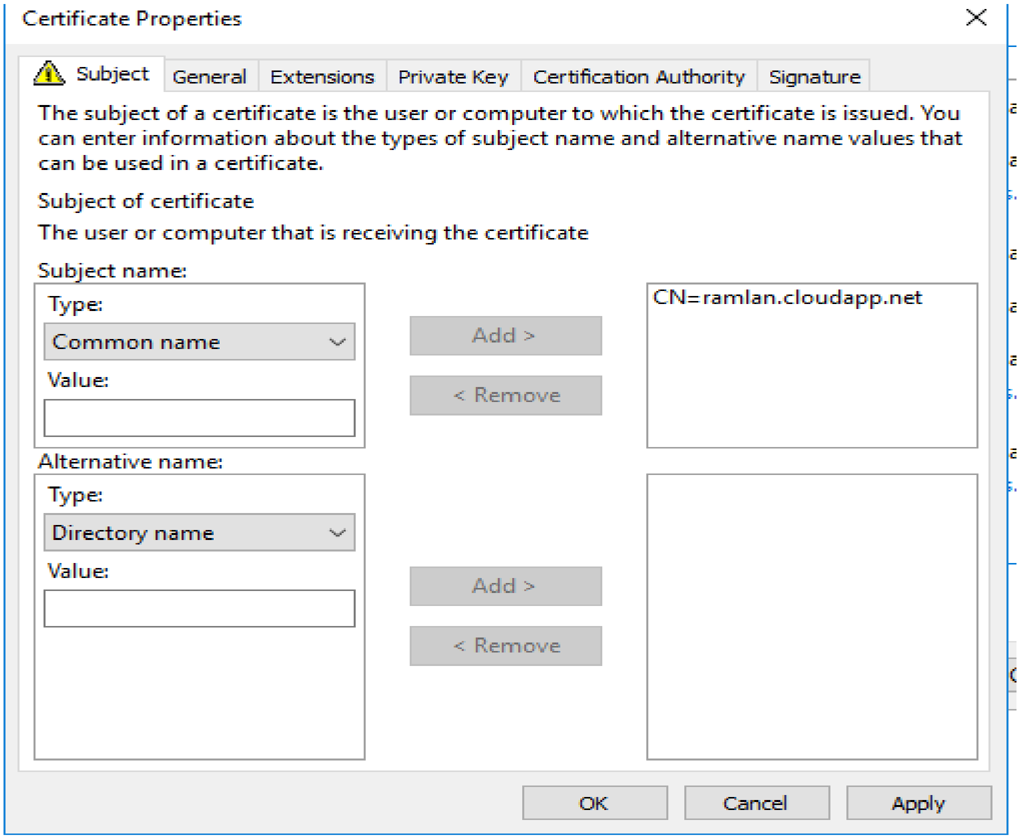
□ SCCM Client Certificate **STATUS:** Available Details

□ SCCM Client Distribution Point Certificate **STATUS:** Available Details

☑ SCCMCMG **STATUS:** Available Details
⚠ More information is required to enroll for this certificate. Click here to configure settings.

□ SCCMCMG – Management Certificate **STATUS:** Available Details
⚠ More information is required to enroll for this certificate. Click here to configure settings.

□ Show all templates


Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Common name

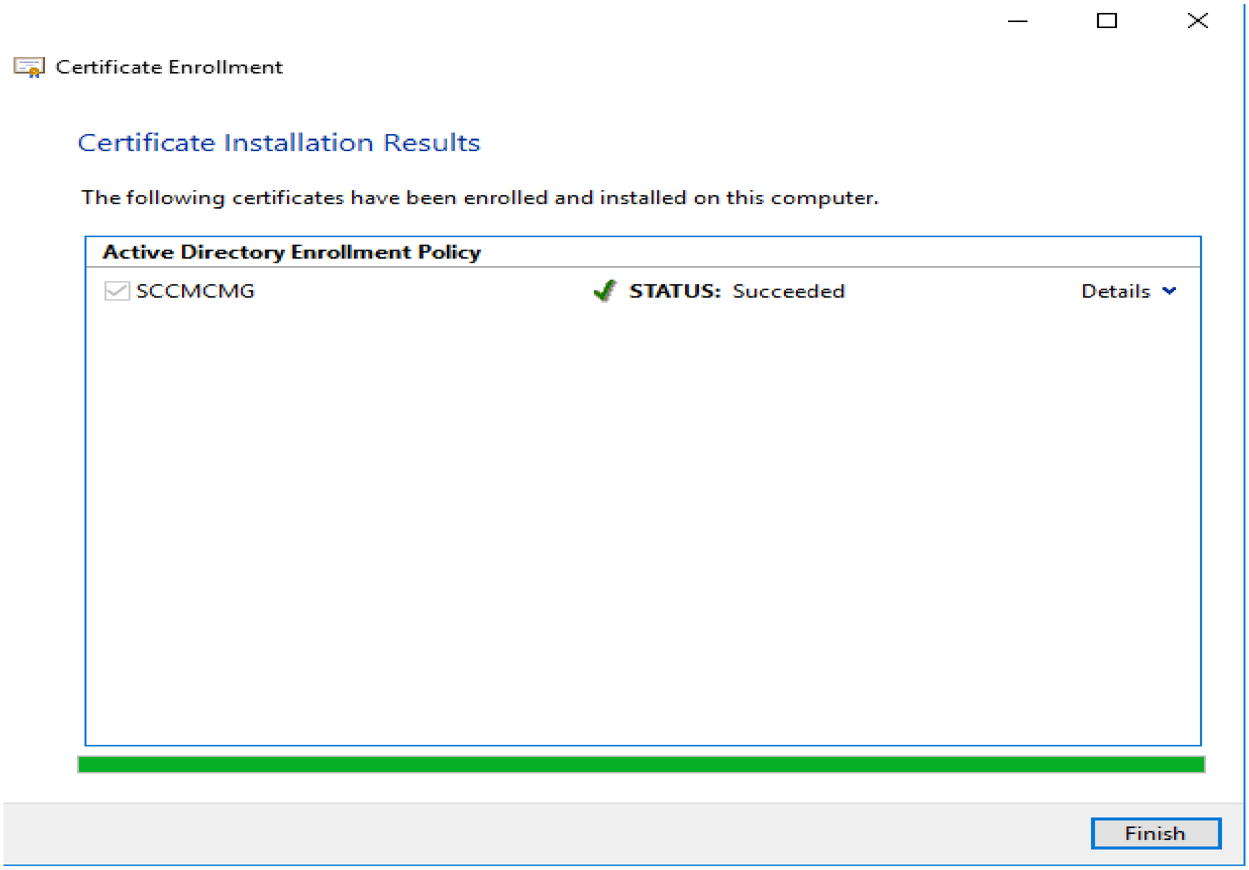
Value:

CN=ramlan.cloudapp.net

Alternative name:

Type: Directory name

Value:


Certificate Enrollment

Certificate Installation Results

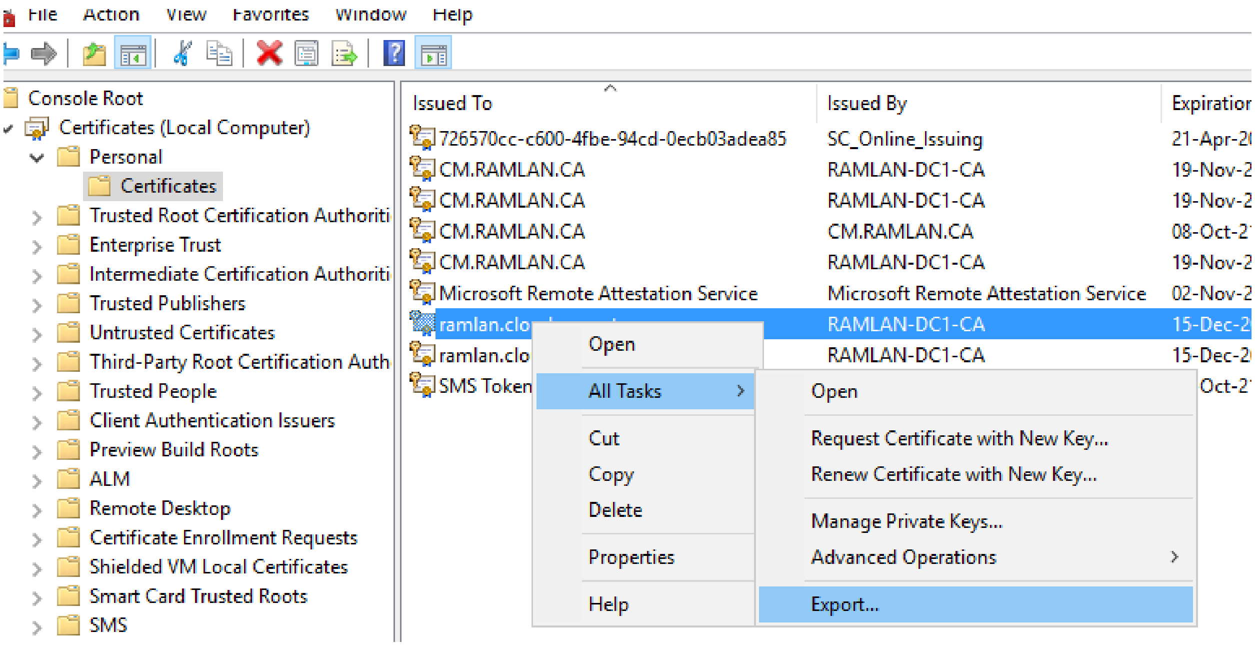
The following certificates have been enrolled and installed on this computer.

**Active Directory Enrollment Policy**

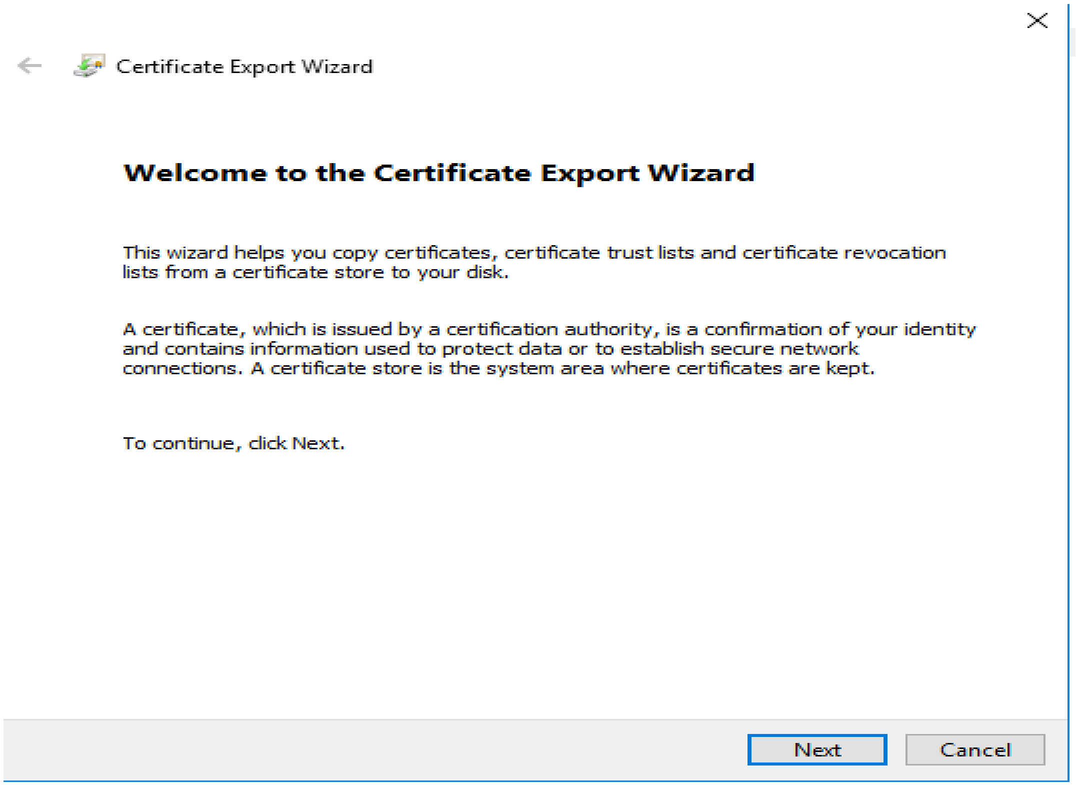
☑ SCCMCMG ✓ **STATUS:** Succeeded

Now we will export the certificates for later user with CMG configuration.

## WITHOUT PRIVATE KEY: MANAGEMENT CERTIFICATE


File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authoriti
Enterprise Trust
Intermediate Certification Authoriti
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Auth
Trusted People
Client Authentication Issuers
Preview Build Roots
ALM
Remote Desktop
Certificate Enrollment Requests
Shielded VM Local Certificates
Smart Card Trusted Roots
SMS
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Manage Private Keys...
Advanced Operations
Export...

| Issued To | Issued By | Expiratior |
|---|---|---|
| 726570cc-c600-4fbe-94cd-0ecb03adea85 | SC_Online_Issuing | 21-Apr-20 |
| CM.RAMLAN.CA | RAMLAN-DC1-CA | 19-Nov-2 |
| CM.RAMLAN.CA | RAMLAN-DC1-CA | 19-Nov-2 |
| CM.RAMLAN.CA | CM.RAMLAN.CA | 08-Oct-2 |
| CM.RAMLAN.CA | RAMLAN-DC1-CA | 19-Nov-2 |
| Microsoft Remote Attestation Service | Microsoft Remote Attestation Service | 02-Nov-2 |
| ramlan.clo | RAMLAN-DC1-CA | 15-Dec-2 |
| ramlan.clo | RAMLAN-DC1-CA | 15-Dec-2 |
| SMS Token | | Oct-2 |

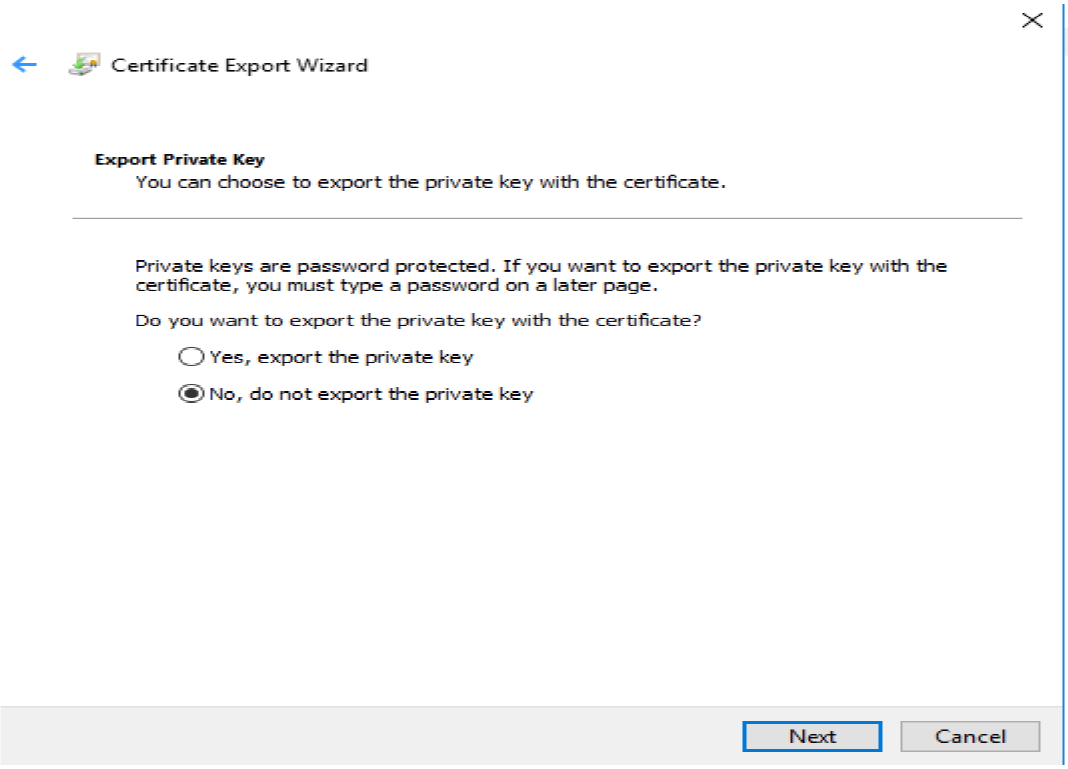


### Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.



Certificate Export Wizard

**Export Private Key**

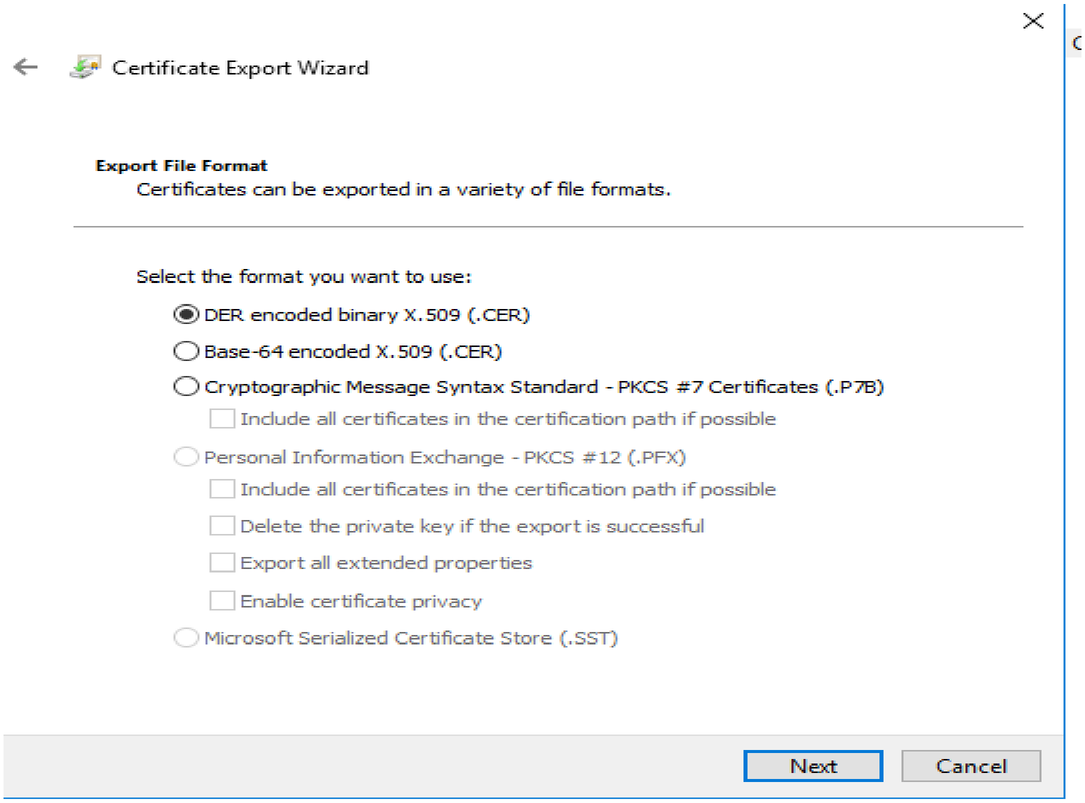
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key



Certificate Export Wizard

**Export File Format**

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

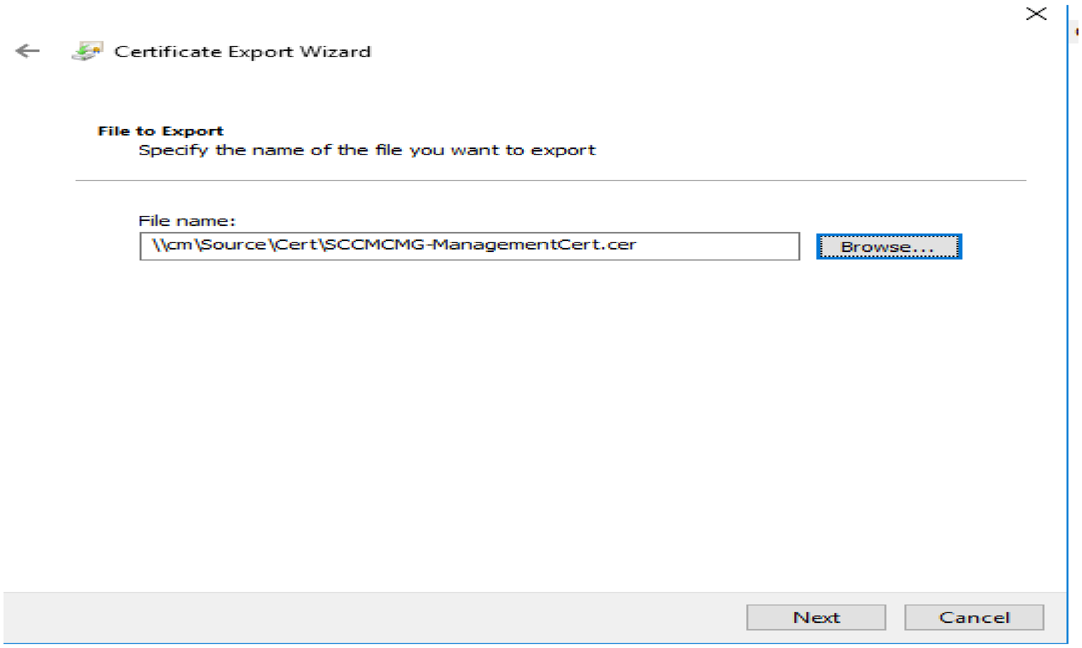
□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

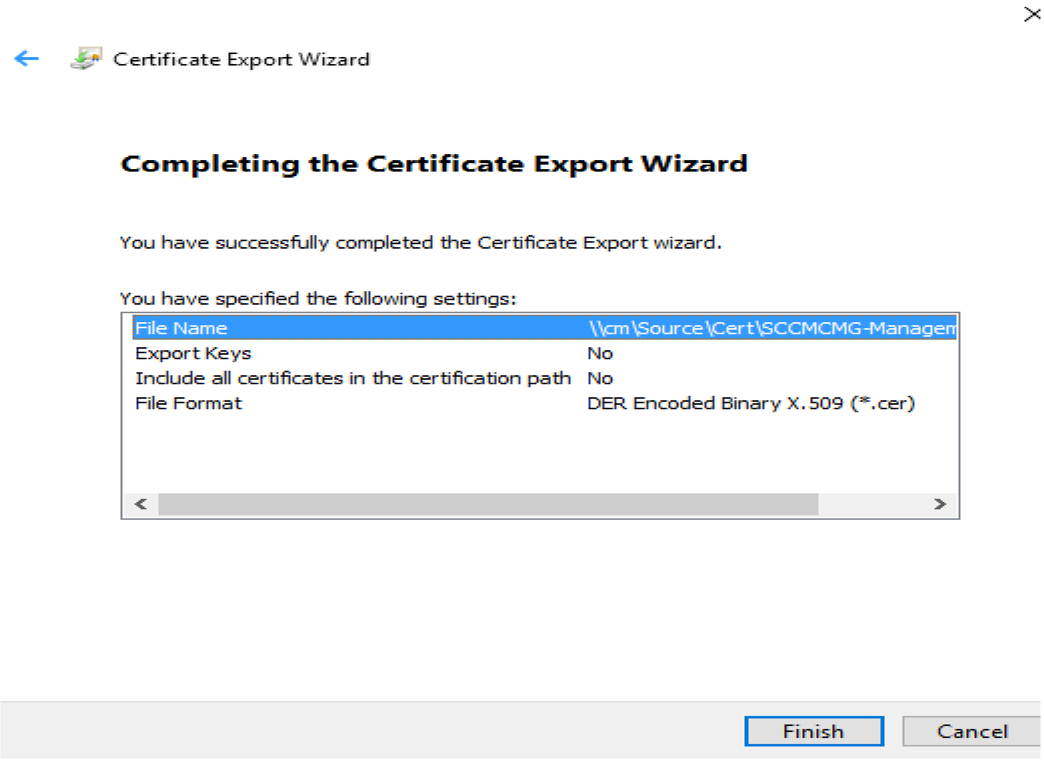


**File to Export**

Specify the name of the file you want to export

File name:

\\cm\Source\Cert\SCCMCMG-ManagementCert.cer

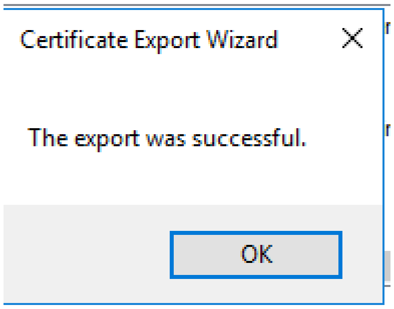


**Completing the Certificate Export Wizard**

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

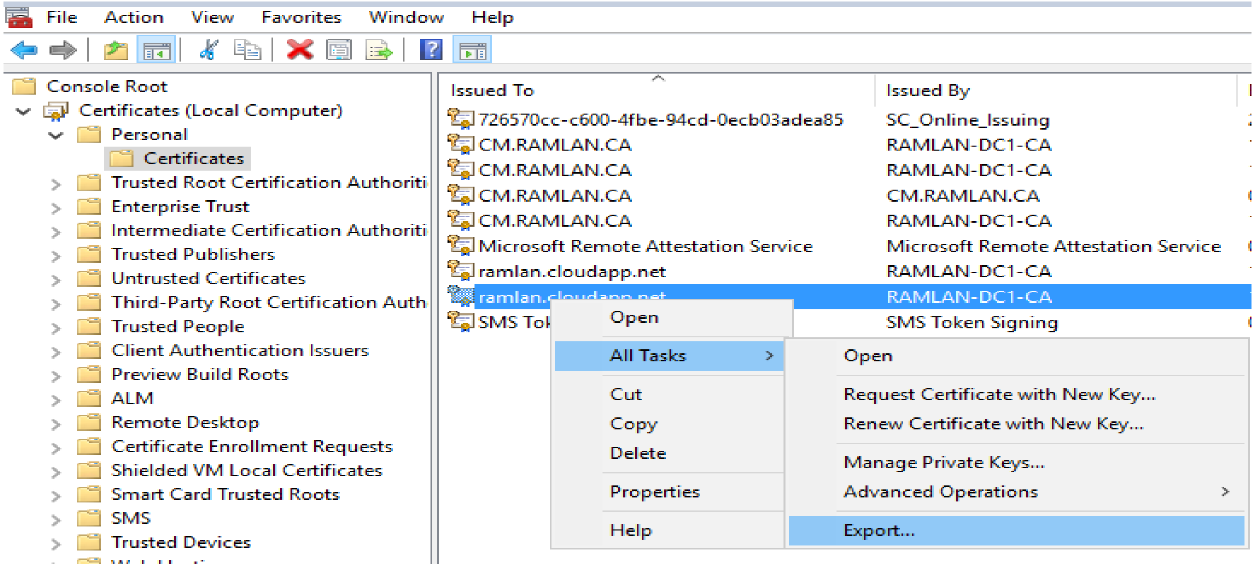
| | |
|---|---|
| File Name | \\cm\Source\Cert\SCCMCMG-Managem |
| Export Keys | No |
| Include all certificates in the certification path | No |
| File Format | DER Encoded Binary X.509 (*.cer) |



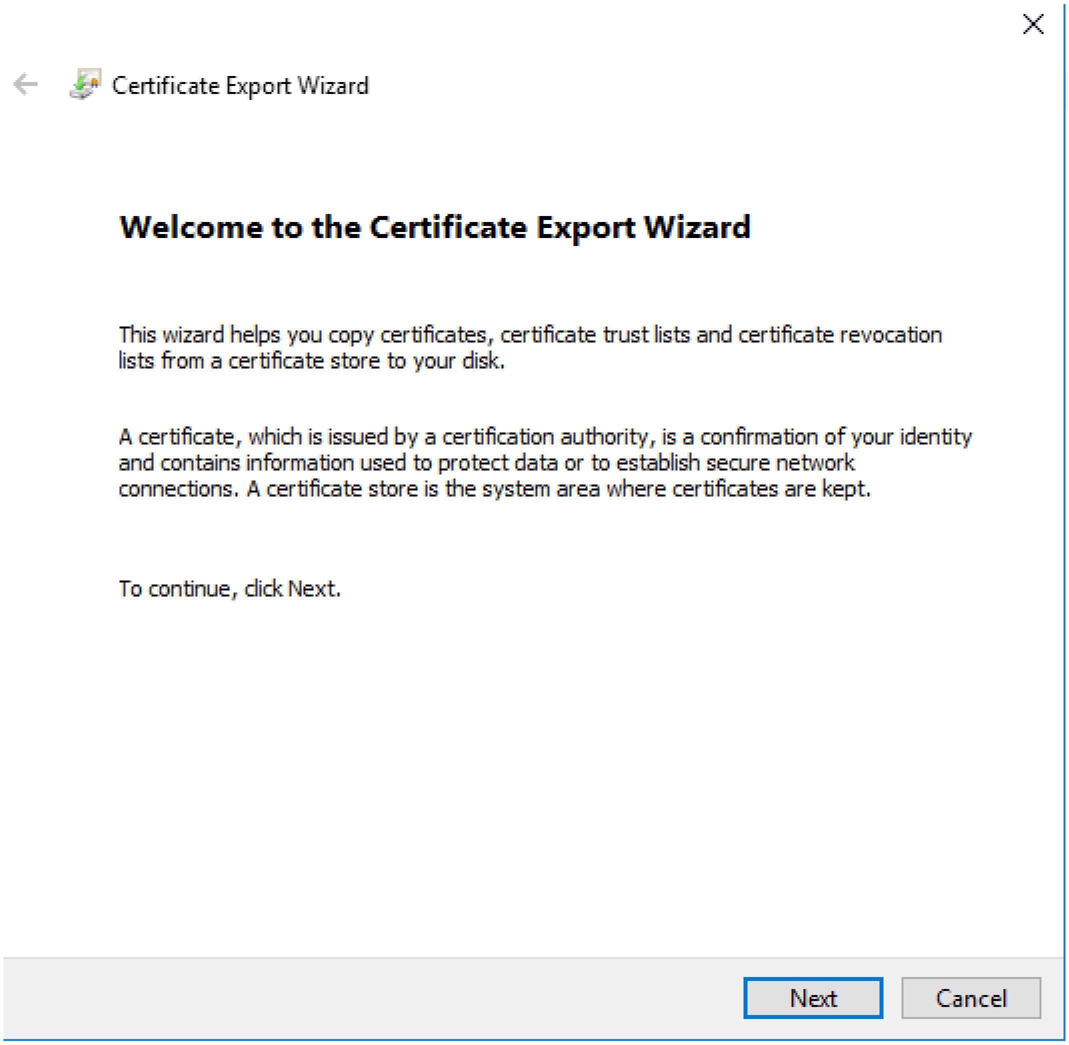
The export was successful.

**WITHOUT PRIVATE KEY: WEB SERVER CERTIFICATE**

Do the same for Web Server Certificate



| Issued To | Issued By |
|---|---|
| 726570cc-c600-4fbe-94cd-0ecb03adea85 | SC_Online_Issuing |
| CM.RAMLAN.CA | RAMLAN-DC1-CA |
| CM.RAMLAN.CA | RAMLAN-DC1-CA |
| CM.RAMLAN.CA | CM.RAMLAN.CA |
| CM.RAMLAN.CA | RAMLAN-DC1-CA |
| Microsoft Remote Attestation Service | Microsoft Remote Attestation Service |
| ramlan.cloudapp.net | RAMLAN-DC1-CA |
| ramlan.cloudapp.net | RAMLAN-DC1-CA |
| SMS Tok | SMS Token Signing |

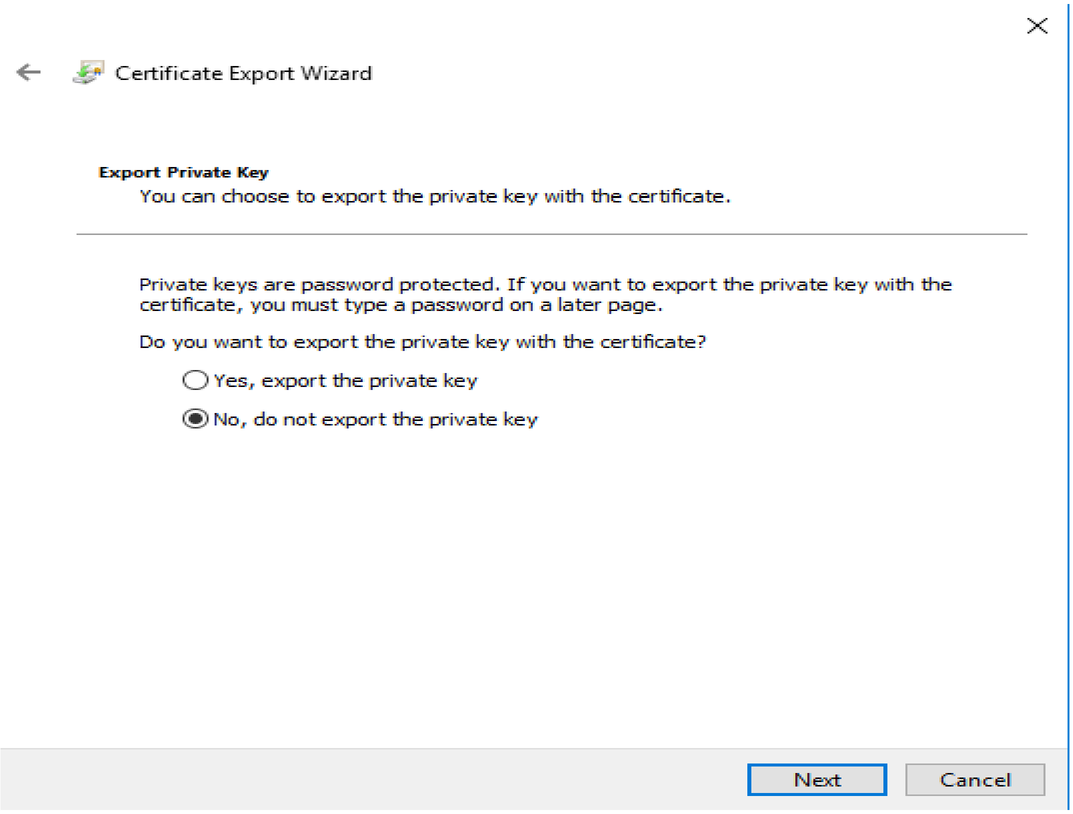


**Welcome to the Certificate Export Wizard**

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.



**Export Private Key**

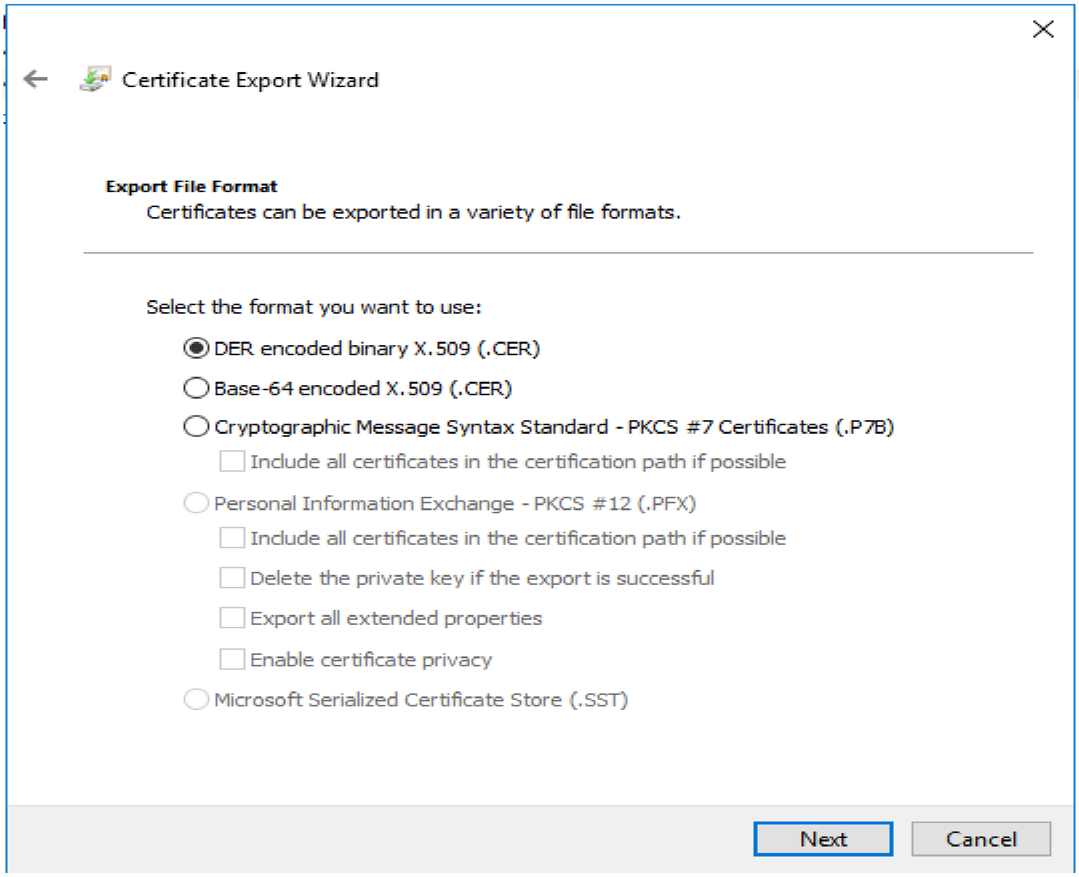
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key



**Export File Format**

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

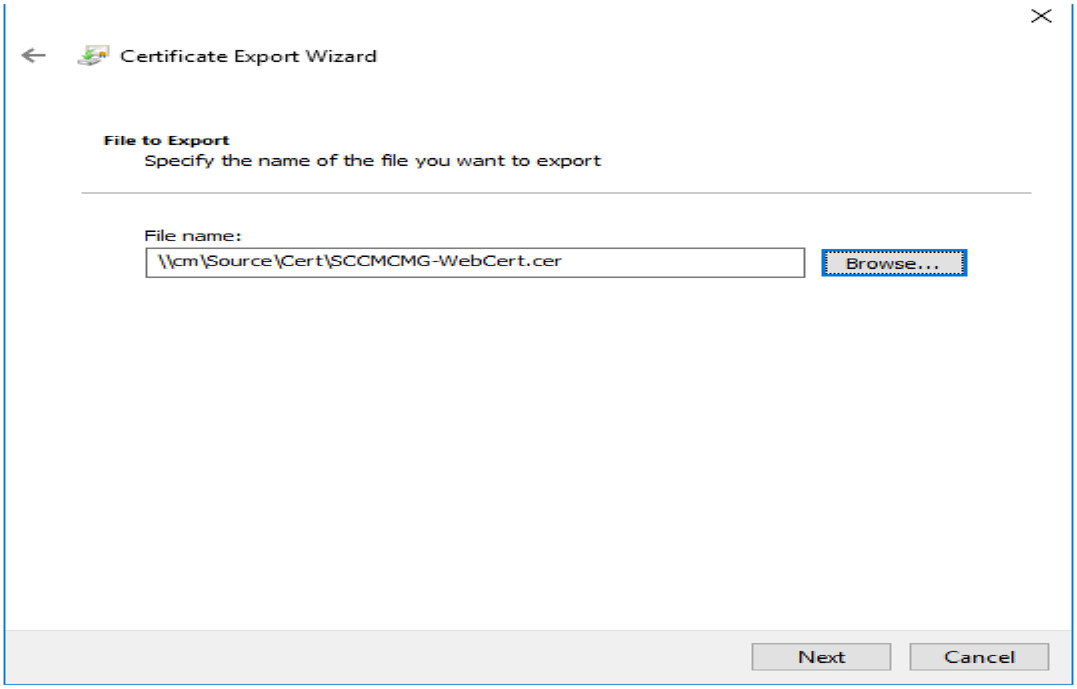
□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

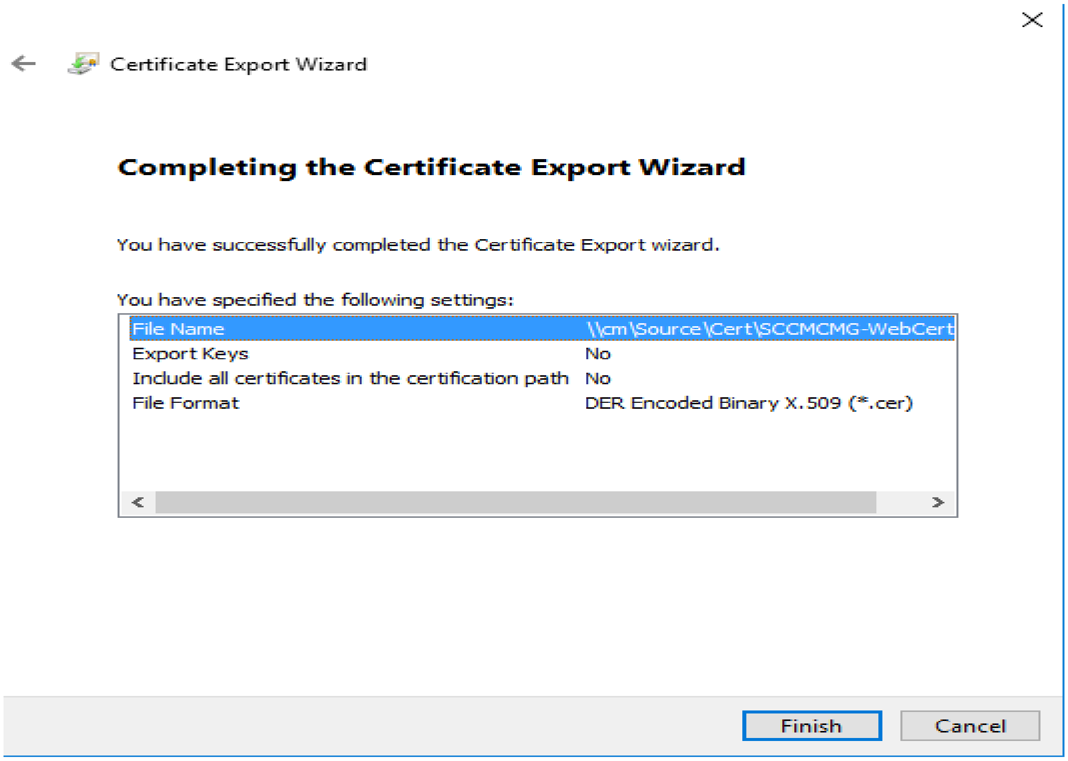
□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)



**File to Export**
Specify the name of the file you want to export

File name:
\\cm\Source\Cert\SCCMCMG-WebCert.cer

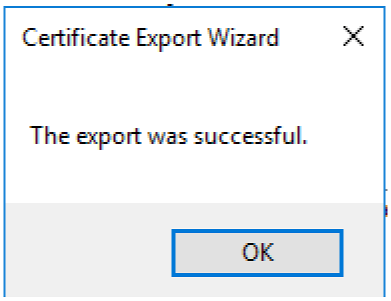


**Completing the Certificate Export Wizard**

You have successfully completed the Certificate Export wizard.

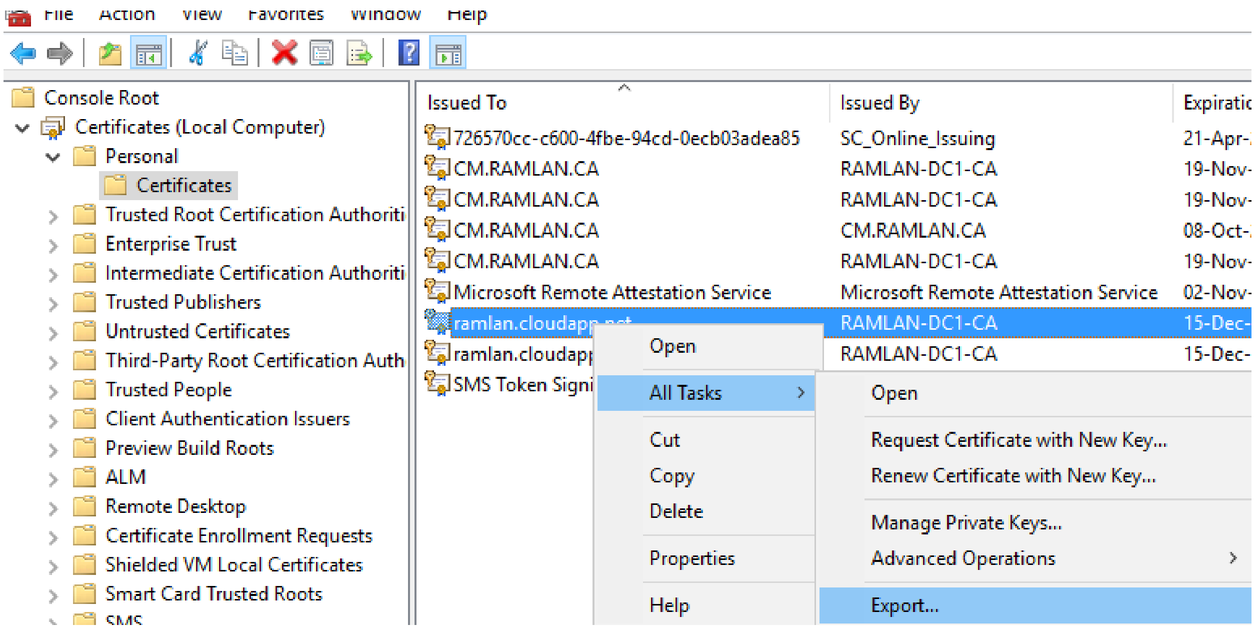
You have specified the following settings:

| | |
|---|---|
| File Name | \\cm\Source\Cert\SCCMCMG-WebCert |
| Export Keys | No |
| Include all certificates in the certification path | No |
| File Format | DER Encoded Binary X.509 (*.cer) |

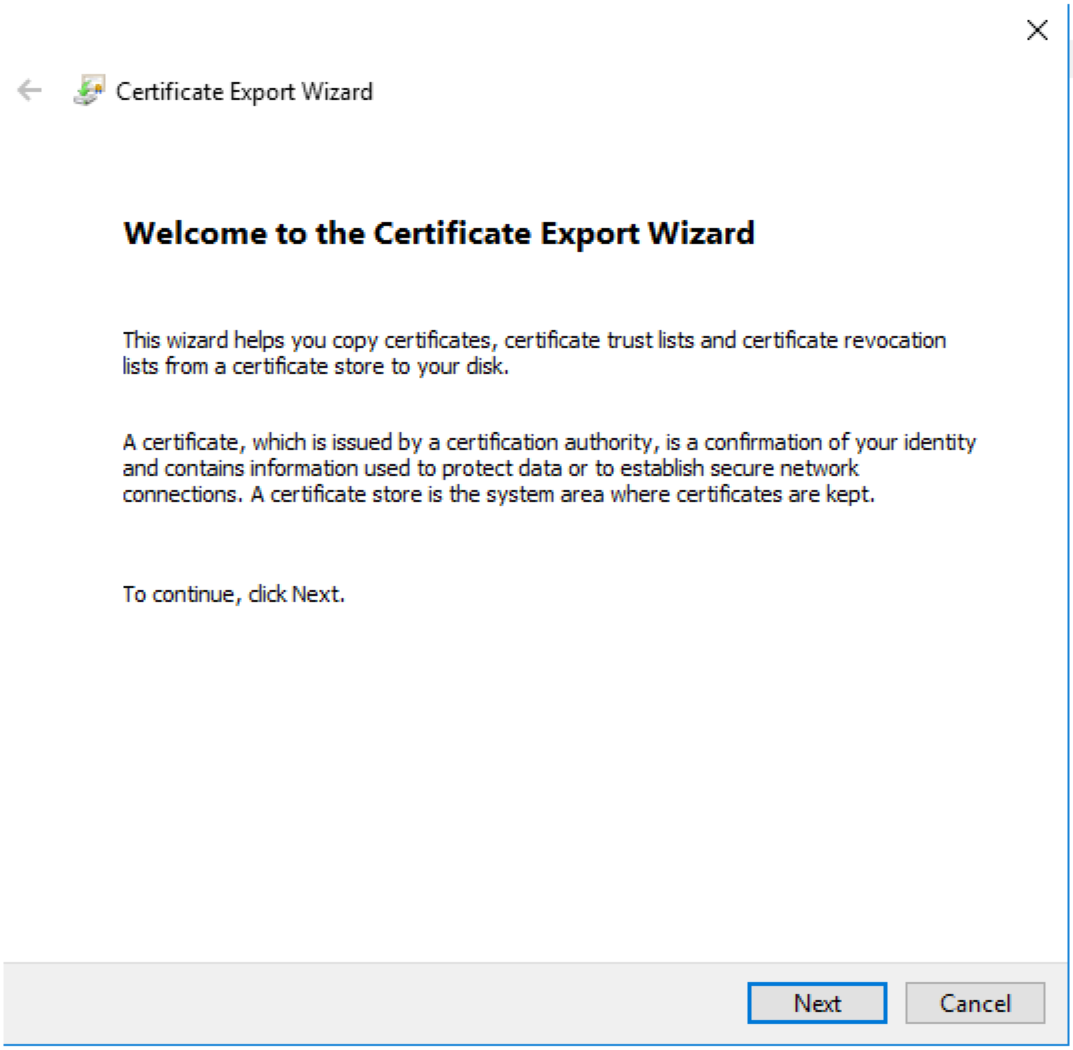


The export was successful.

## WITH PRIVATE KEY: MANAGEMENT CERTIFICATE


File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authoriti
Enterprise Trust
Intermediate Certification Authoriti
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Auth
Trusted People
Client Authentication Issuers
Preview Build Roots
ALM
Remote Desktop
Certificate Enrollment Requests
Shielded VM Local Certificates
Smart Card Trusted Roots
SMS
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Manage Private Keys...
Advanced Operations
Export...

| Issued To | Issued By | Expiratic |
|---|---|---|
| 726570cc-c600-4fbe-94cd-0ecb03adea85 | SC_Online_Issuing | 21-Apr- |
| CM.RAMLAN.CA | RAMLAN-DC1-CA | 19-Nov- |
| CM.RAMLAN.CA | RAMLAN-DC1-CA | 19-Nov- |
| CM.RAMLAN.CA | CM.RAMLAN.CA | 08-Oct- |
| CM.RAMLAN.CA | RAMLAN-DC1-CA | 19-Nov- |
| Microsoft Remote Attestation Service | Microsoft Remote Attestation Service | 02-Nov- |
| ramlan.cloudapp.net | RAMLAN-DC1-CA | 15-Dec- |
| ramlan.cloudapp | RAMLAN-DC1-CA | 15-Dec- |
| SMS Token Signi | | |

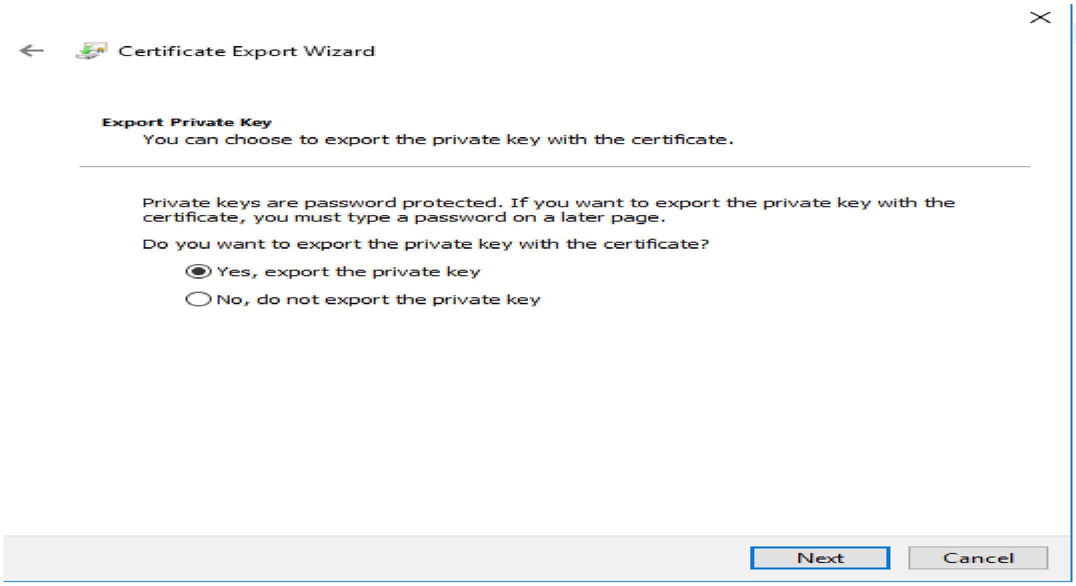


**Welcome to the Certificate Export Wizard**

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.



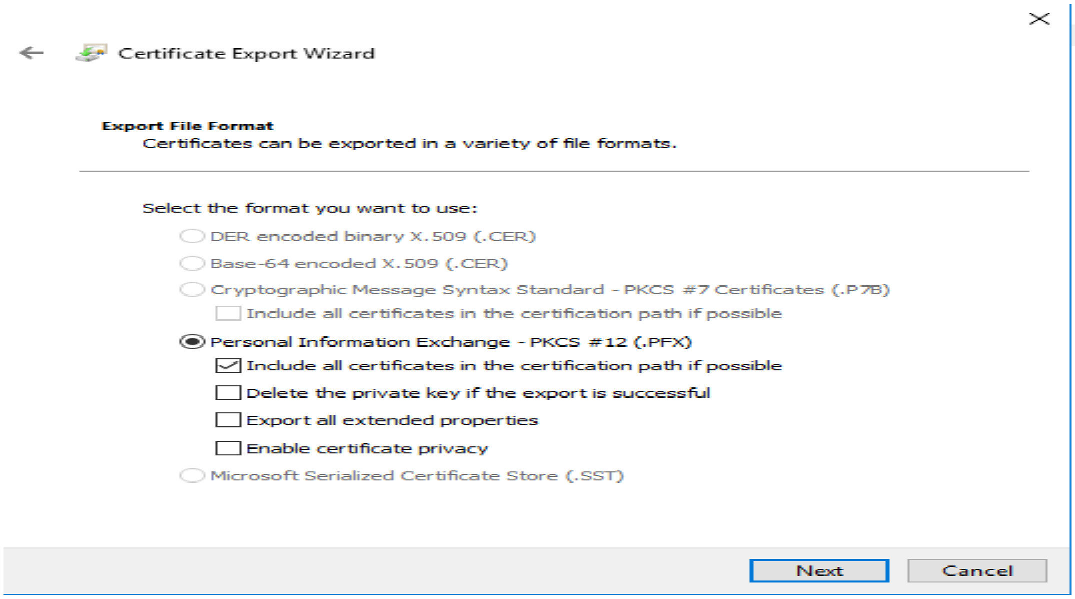
**Export Private Key**
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key



**Export File Format**
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

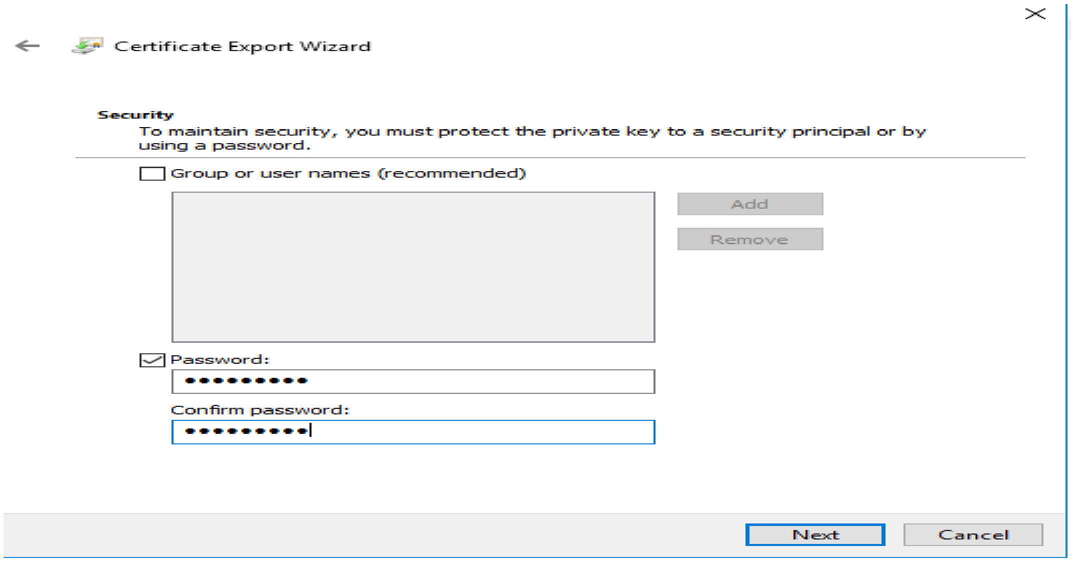
☑ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)



**Security**
To maintain security, you must protect the private key to a security principal or by using a password.

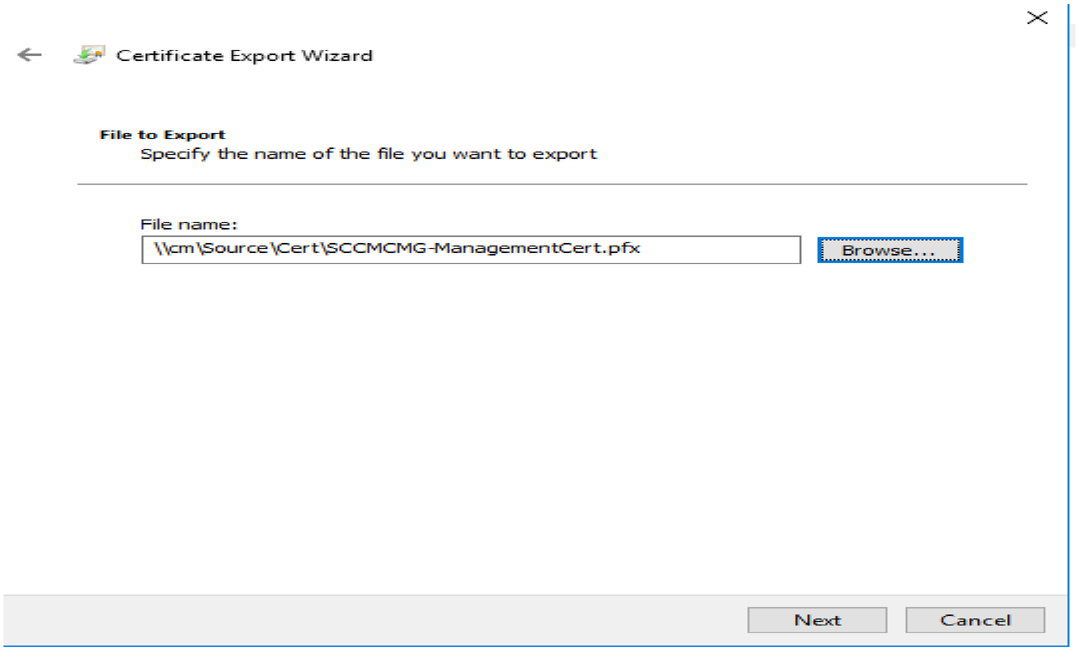
□ Group or user names (recommended)

☑ Password:

●●●●●●●●●●

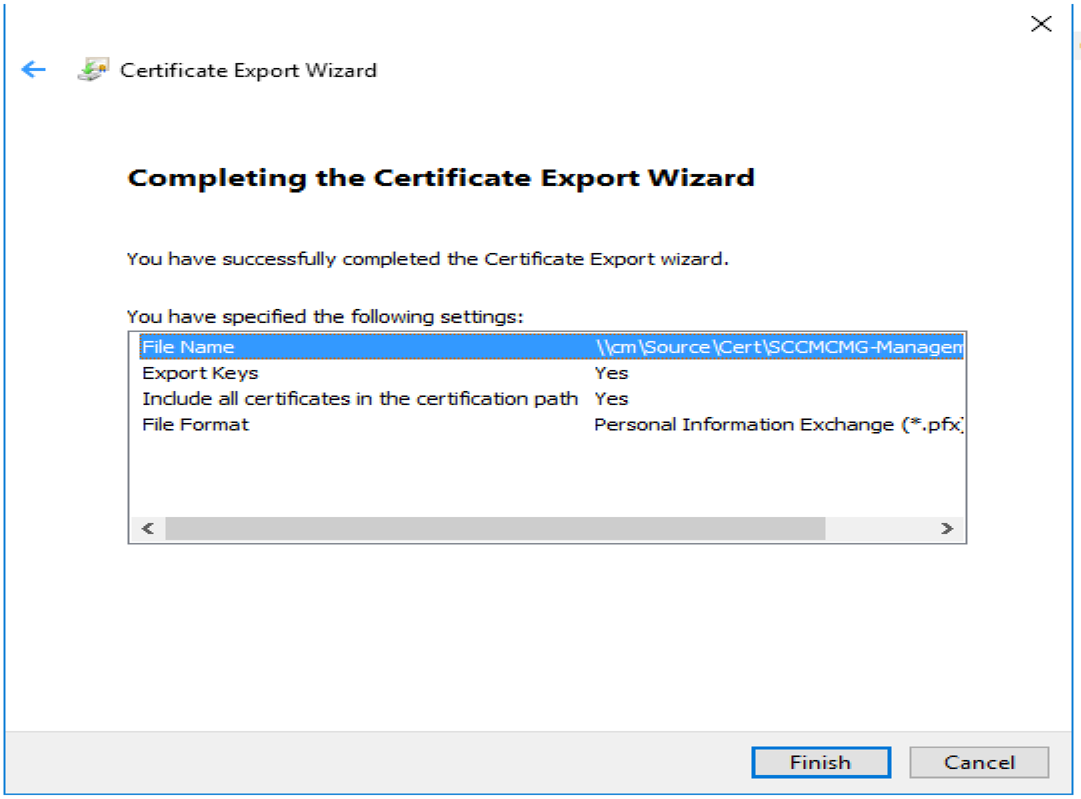
Confirm password:

●●●●●●●●●●


Certificate Export Wizard

**File to Export**
Specify the name of the file you want to export

File name:
\\cm\Source\Cert\SCCMCMG-ManagementCert.pfx

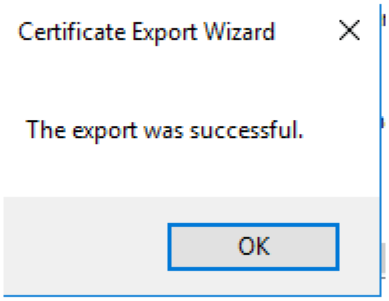

Certificate Export Wizard

**Completing the Certificate Export Wizard**

You have successfully completed the Certificate Export wizard.

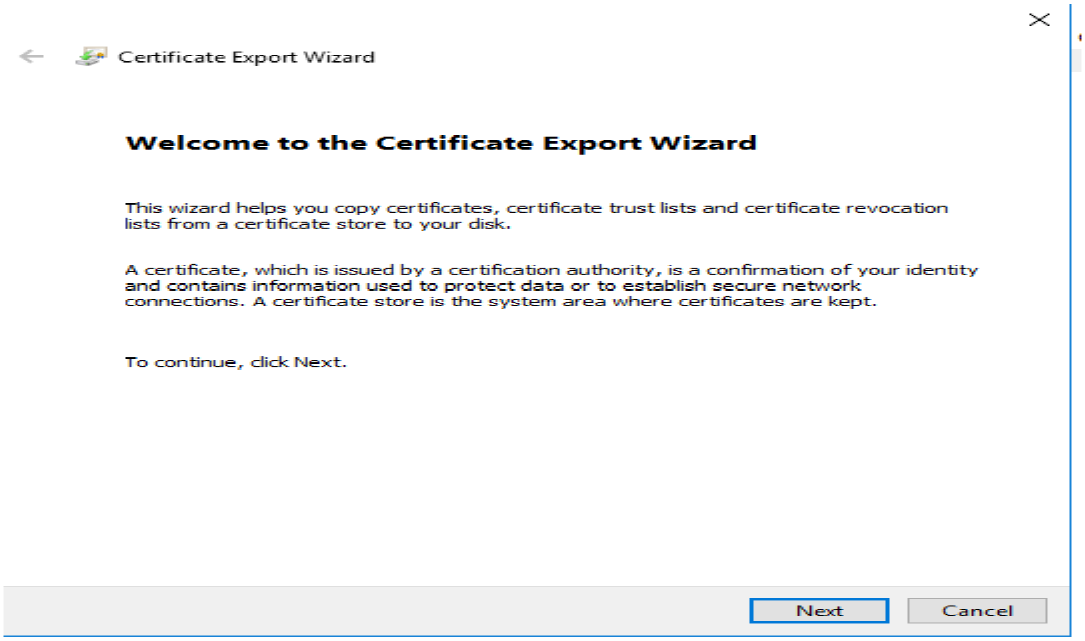
You have specified the following settings:

```
File Name                                        \\cm\Source\Cert\SCCMCMG-Managem
Export Keys                                      Yes
Include all certificates in the certification path  Yes
File Format                                      Personal Information Exchange (*.pfx)
```


Certificate Export Wizard

The export was successful.

## WITH PRIVATE KEY: WEB SERVER CERTIFICATE

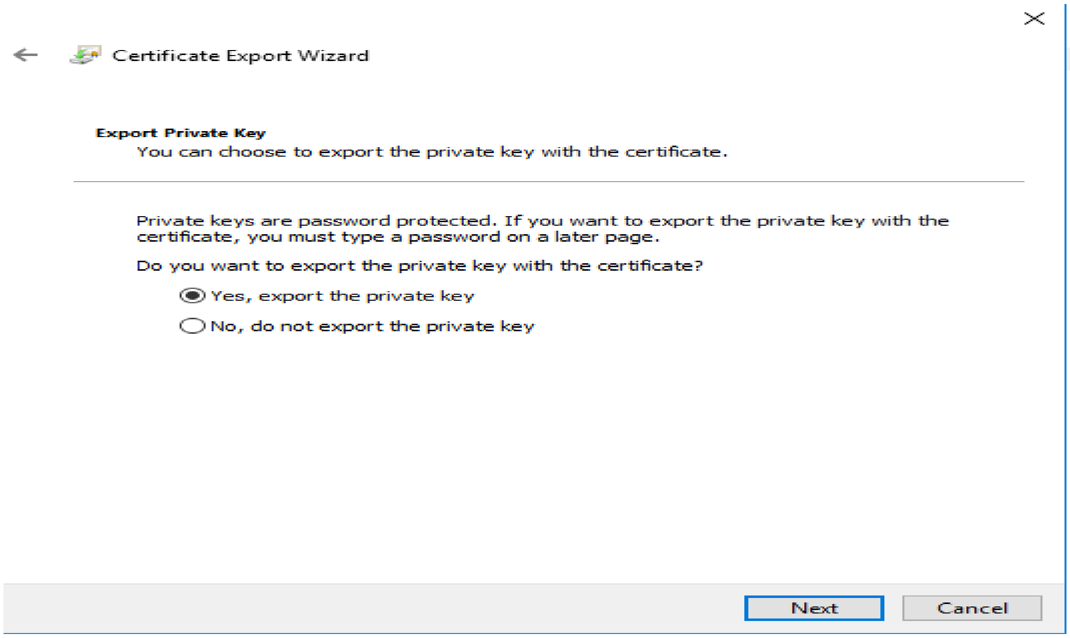


**Welcome to the Certificate Export Wizard**

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.



**Export Private Key**

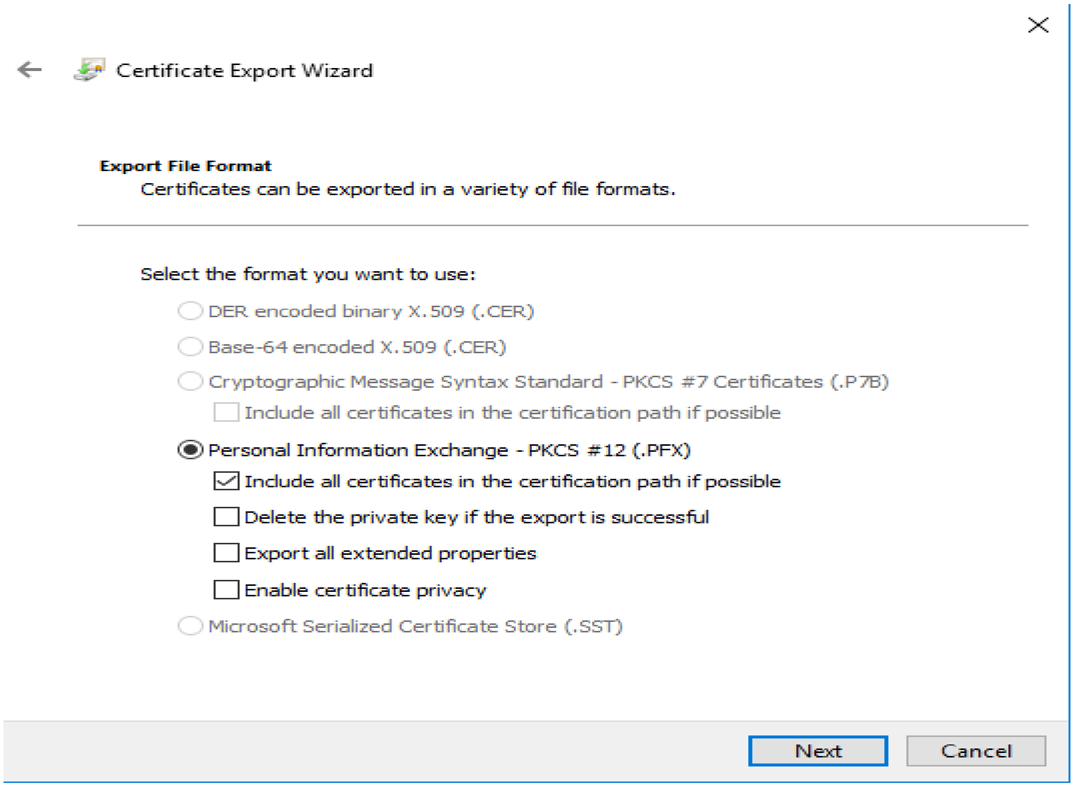
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key



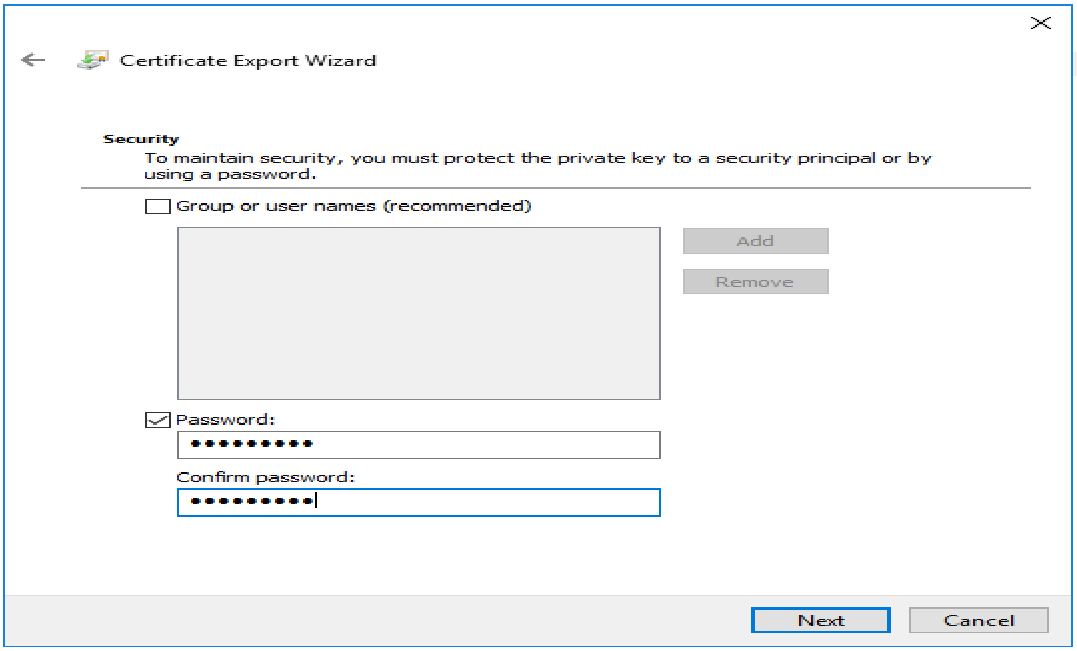
Certificate Export Wizard

**Export File Format**

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ○ DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ● Personal Information Exchange - PKCS #12 (.PFX)
  - ☑ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
  - □ Enable certificate privacy
- ○ Microsoft Serialized Certificate Store (.SST)



Certificate Export Wizard

**Security**

To maintain security, you must protect the private key to a security principal or by using a password.

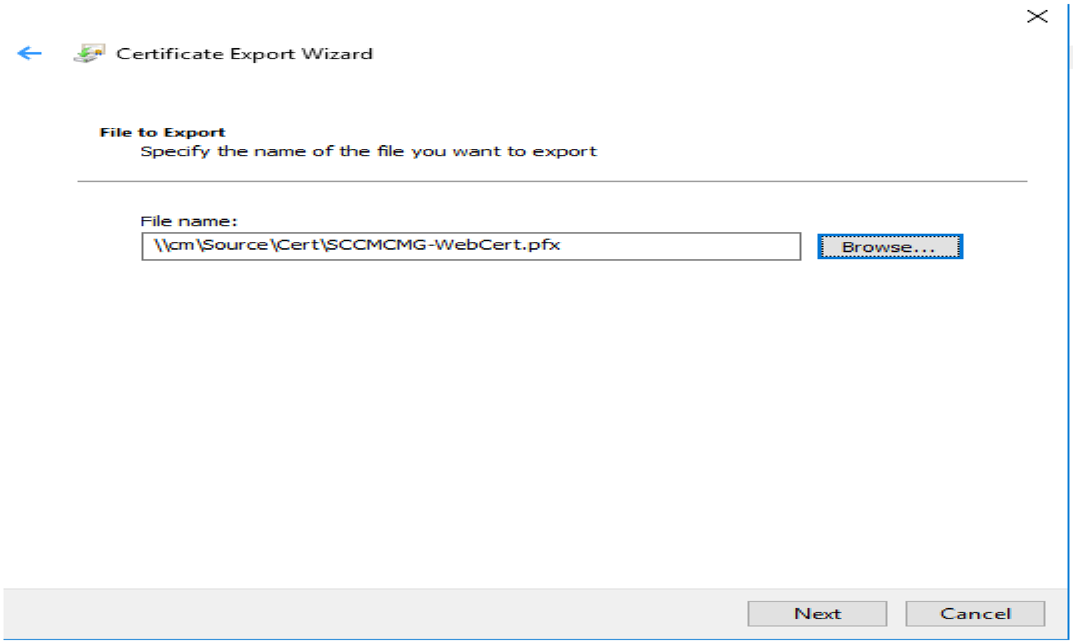
□ Group or user names (recommended)

☑ Password:

●●●●●●●●●

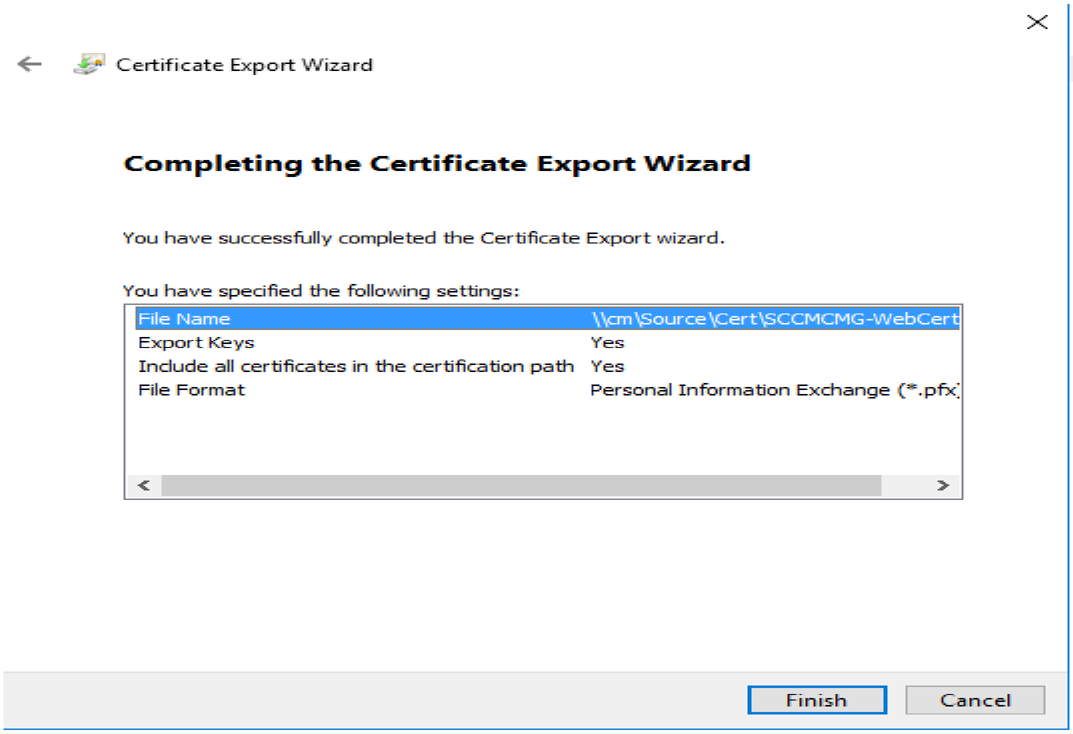
Confirm password:

●●●●●●●●●



**File to Export**
Specify the name of the file you want to export

File name: \\cm\Source\Cert\SCCMCMG-WebCert.pfx

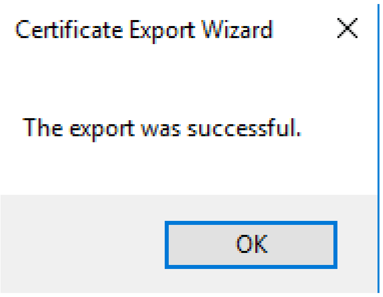


**Completing the Certificate Export Wizard**

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

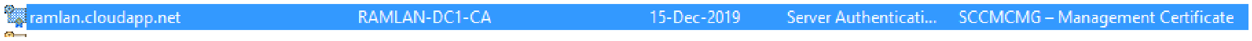
| | |
|---|---|
| File Name | \\cm\Source\Cert\SCCMCMG-WebCert |
| Export Keys | Yes |
| Include all certificates in the certification path | Yes |
| File Format | Personal Information Exchange (*.pfx) |



The export was successful.

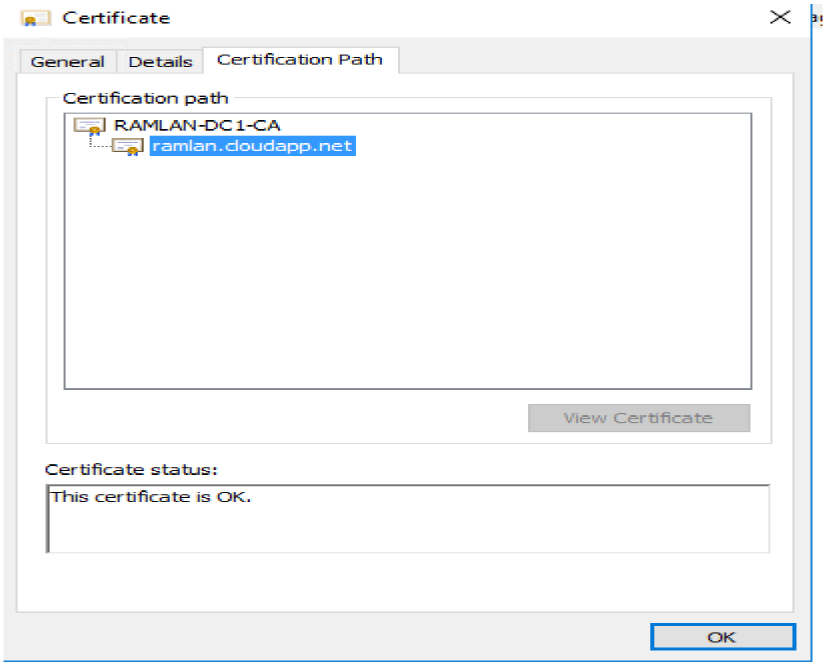
Now we will complete Trusted Root Certificate export steps

To do this double click Management Certificate or Web Certificate



| | | | | |
|---|---|---|---|---|
| ramlan.cloudapp.net | RAMLAN-DC1-CA | 15-Dec-2019 | Server Authenticati... | SCCMCMG – Management Certificate |

Go to Certification Path

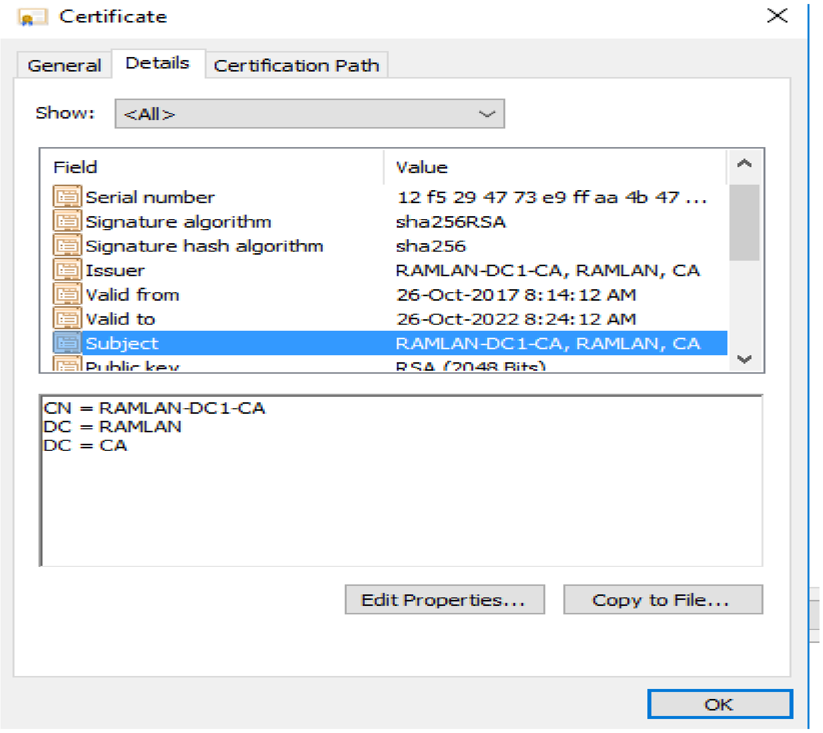


RAMLAN-DC1-CA
ramlan.cloudapp.net

Certificate status:

This certificate is OK.

Select RAMLAN-DC1-CA – Click View Certificate – Go to Details- Subject

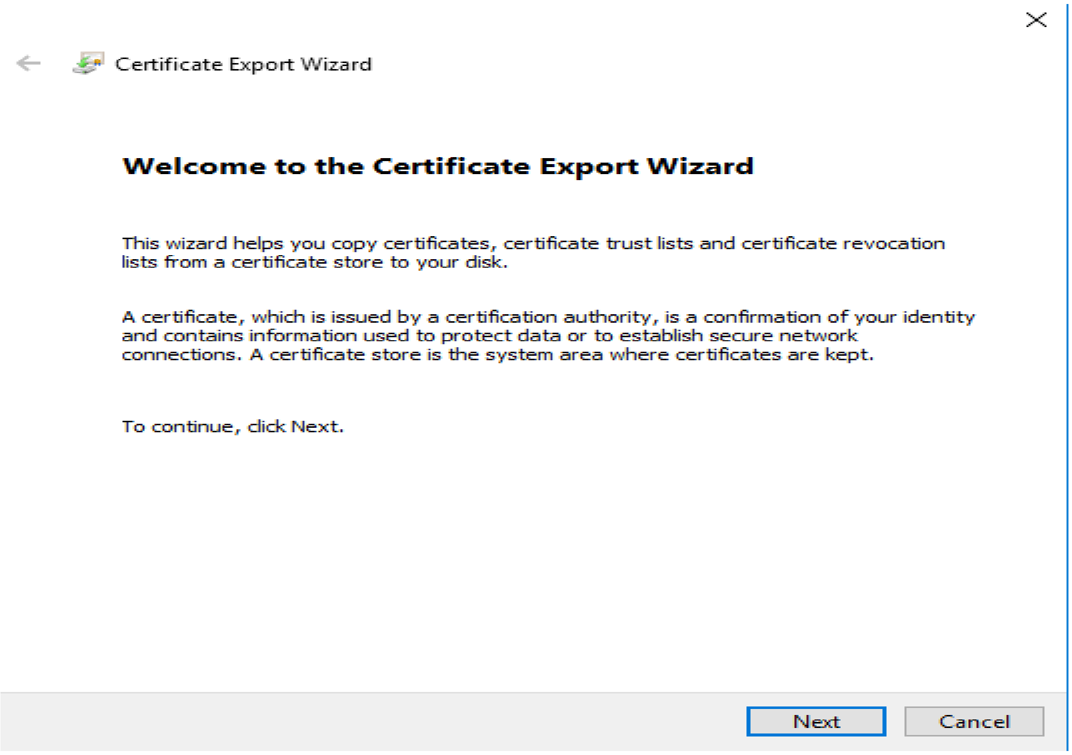


Show: <All>

| Field | Value |
|---|---|
| Serial number | 12 f5 29 47 73 e9 ff aa 4b 47 ... |
| Signature algorithm | sha256RSA |
| Signature hash algorithm | sha256 |
| Issuer | RAMLAN-DC1-CA, RAMLAN, CA |
| Valid from | 26-Oct-2017 8:14:12 AM |
| Valid to | 26-Oct-2022 8:24:12 AM |
| Subject | RAMLAN-DC1-CA, RAMLAN, CA |
| Public key | RSA (2048 Bits) |

```
CN = RAMLAN-DC1-CA
DC = RAMLAN
DC = CA
```

Click Copy to File

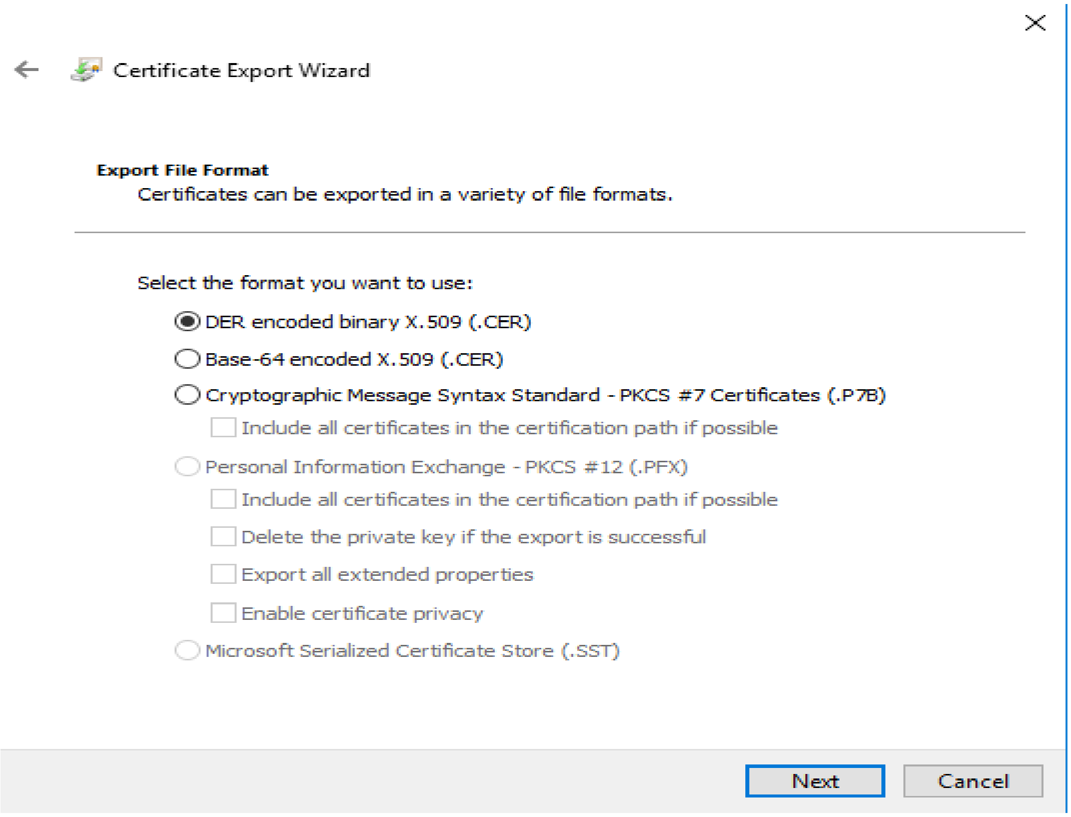


**Welcome to the Certificate Export Wizard**

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

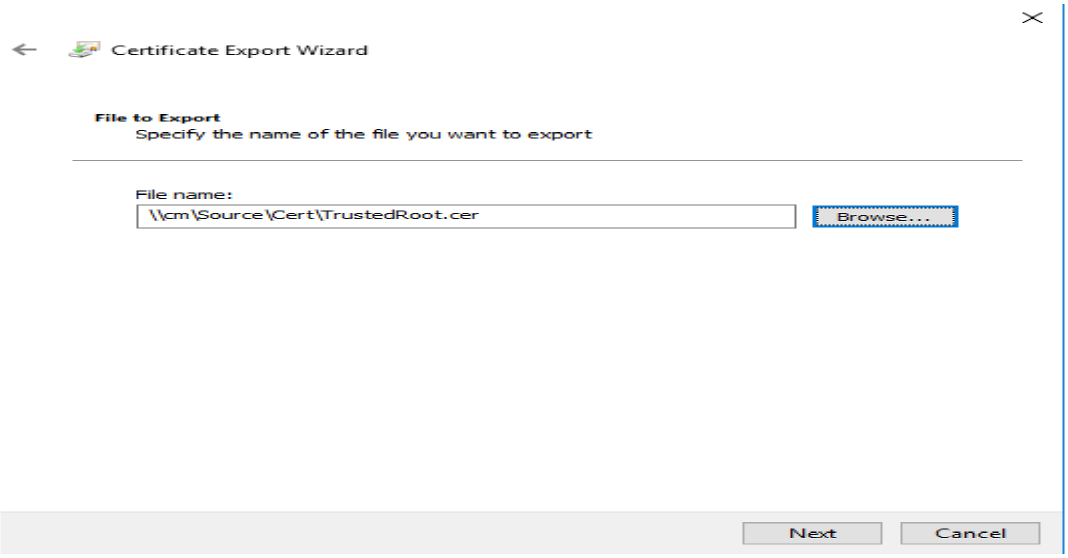
To continue, click Next.



**Export File Format**
Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  □ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
  □ Include all certificates in the certification path if possible
  □ Delete the private key if the export is successful
  □ Export all extended properties
  □ Enable certificate privacy
○ Microsoft Serialized Certificate Store (.SST)

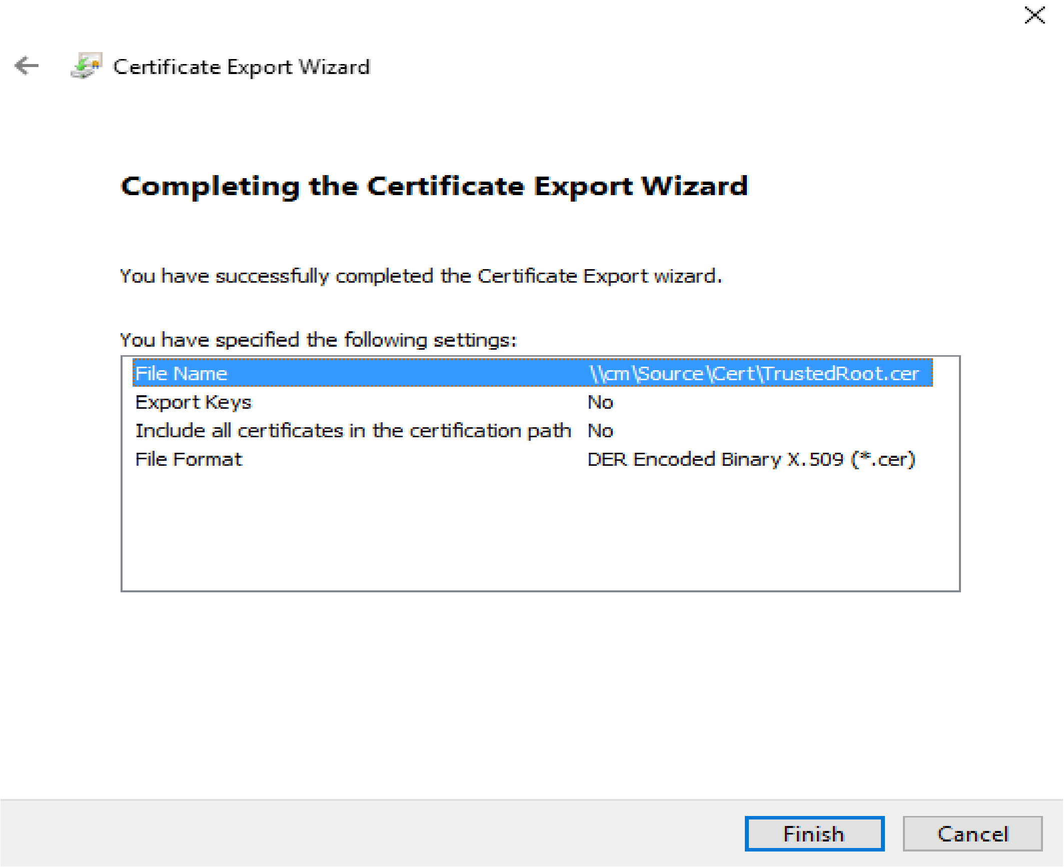


**File to Export**

Specify the name of the file you want to export

File name:

\\cm\Source\Cert\TrustedRoot.cer

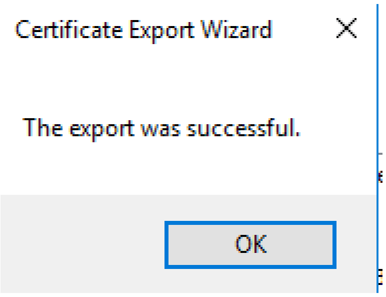


Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

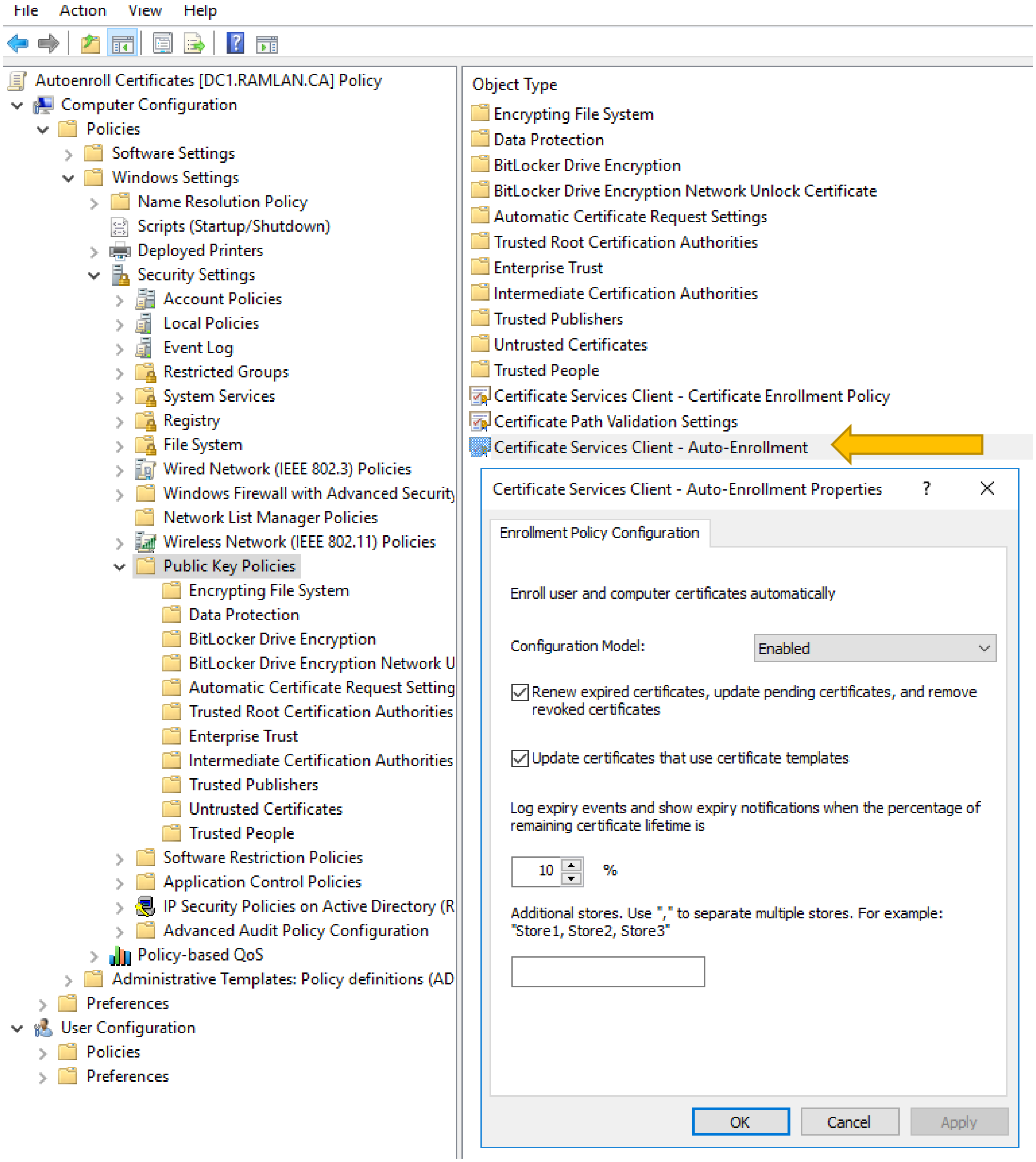
| | |
|---|---|
| File Name | \\cm\Source\Cert\TrustedRoot.cer |
| Export Keys | No |
| Include all certificates in the certification path | No |
| File Format | DER Encoded Binary X.509 (*.cer) |



The export was successful.

Since, I have already implemented PKI in my infrastructure – The GPO is already set and enabled.  You can do the same – The GPO steps are as follows:

Open GPMC


File
Action
View
Help
Autoenroll Certificates [DC1.RAMLAN.CA] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network U
Automatic Certificate Request Setting
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (R
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (AD
Preferences
User Configuration
Policies
Preferences
Object Type
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlock Certificate
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Services Client - Certificate Enrollment Policy
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment
?
OK
Cancel
Apply

Certificate Services Client - Auto-Enrollment Properties

Enrollment Policy Configuration

Enroll user and computer certificates automatically

Configuration Model: Enabled

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

☑ Update certificates that use certificate templates

Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is

10 %

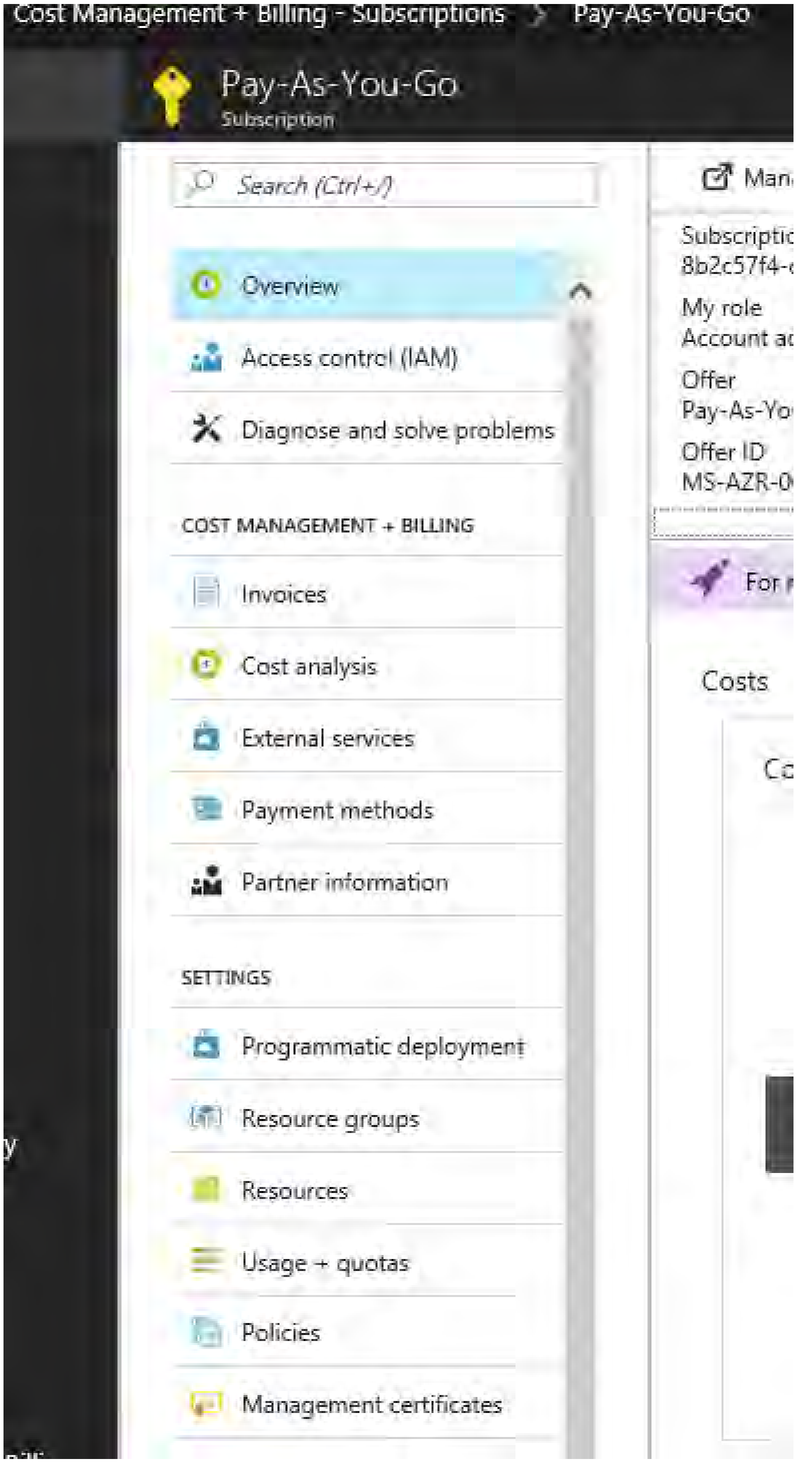
Additional stores. Use "," to separate multiple stores. For example: "Store1, Store2, Store3"

Now we will complete the steps at Azure Portal

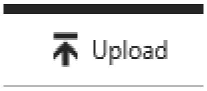
Login to Azure Portal – Go to

Cost Management + Billing - Subscriptions > Pay-As-You-Go

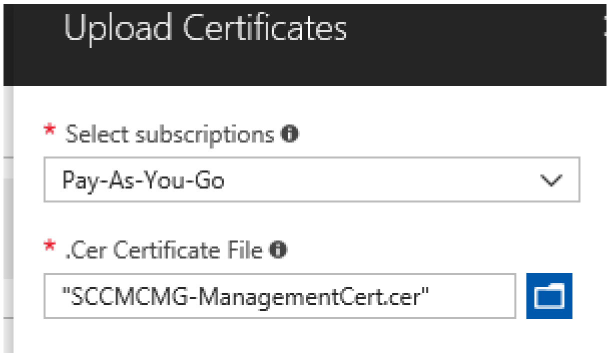
Select Management Certificates



Click Upload



Select Management Certificate

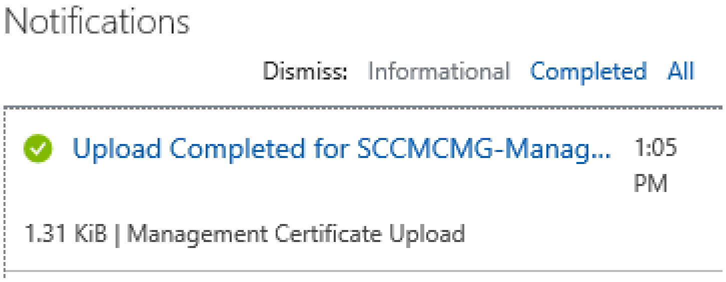

Upload Certificates

* Select subscriptions

Pay-As-You-Go

* .Cer Certificate File

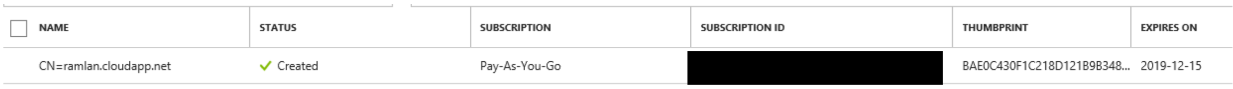
"SCCMCMG-ManagementCert.cer"


Notifications

Dismiss: Informational Completed All

Upload Completed for SCCMCMG-Manag... 1:05 PM

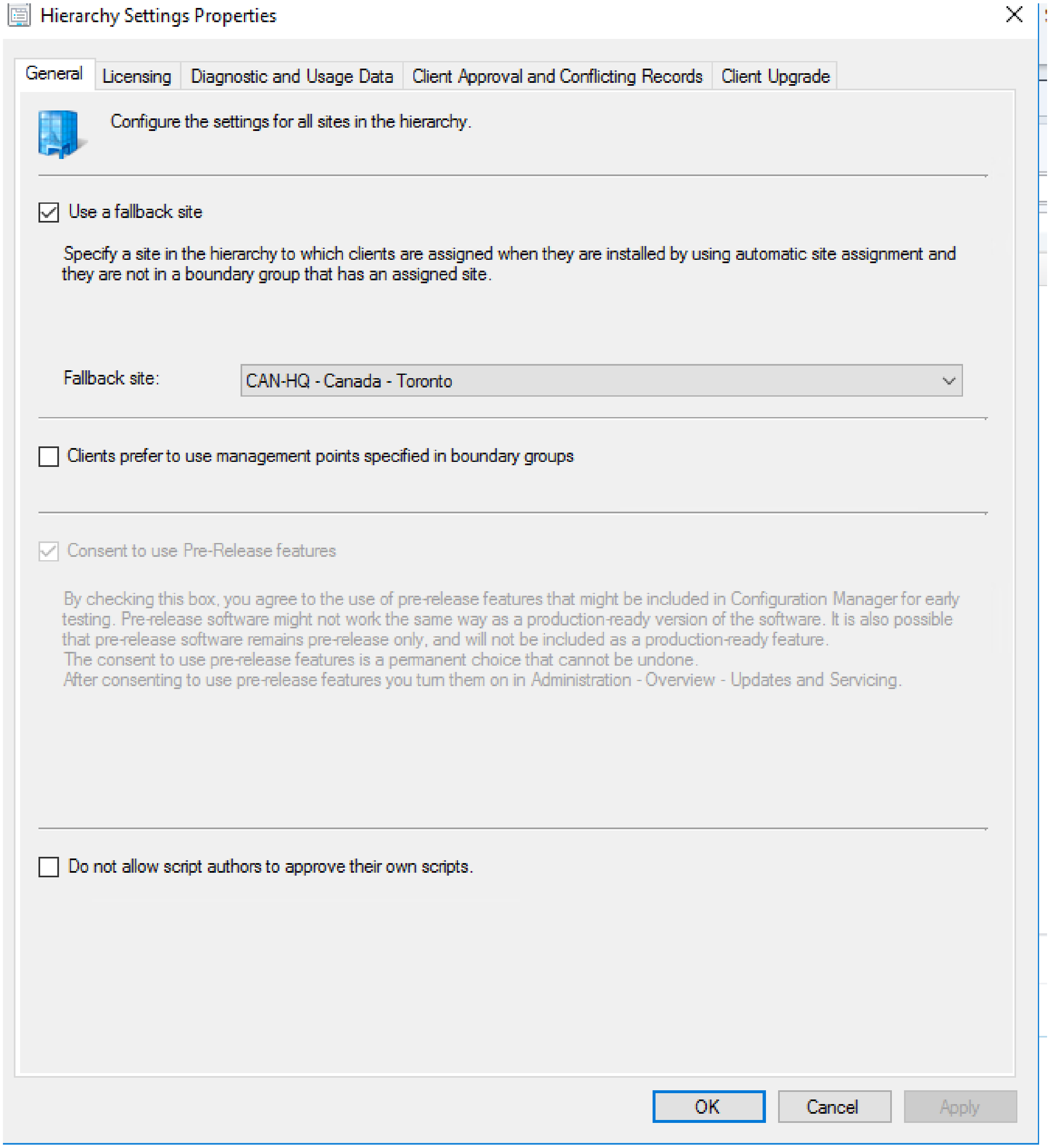
1.31 KiB | Management Certificate Upload



| □ NAME | STATUS | SUBSCRIPTION | SUBSCRIPTION ID | THUMBPRINT | EXPIRES ON |
|---|---|---|---|---|---|
| CN=ramlan.cloudapp.net | ✓ Created | Pay-As-You-Go | [redacted] | BAE0C430F1C218D121B9B348... | 2019-12-15 |

Now we are ready to implement Cloud Management Gateway within CB1710

First we have to make sure the feature is enabled – Since it is Pre Release Feature we have to agree to MS consent – You can do this from Administration – Sites – Hierarchy Setting



Hierarchy Settings Properties

General
Licensing
Diagnostic and Usage Data
Client Approval and Conflicting Records
Client Upgrade

Configure the settings for all sites in the hierarchy.

☑ Use a fallback site

Specify a site in the hierarchy to which clients are assigned when they are installed by using automatic site assignment and they are not in a boundary group that has an assigned site.

Fallback site: CAN-HQ - Canada - Toronto

☐ Clients prefer to use management points specified in boundary groups

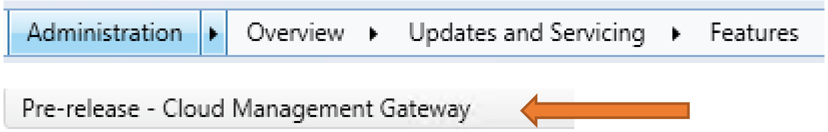
☑ Consent to use Pre-Release features

By checking this box, you agree to the use of pre-release features that might be included in Configuration Manager for early testing. Pre-release software might not work the same way as a production-ready version of the software. It is also possible that pre-release software remains pre-release only, and will not be included as a production-ready feature.
The consent to use pre-release features is a permanent choice that cannot be undone.
After consenting to use pre-release features you turn them on in Administration - Overview - Updates and Servicing.

☐ Do not allow script authors to approve their own scripts.

It is grayed out for me – as I have already accepted the Consent

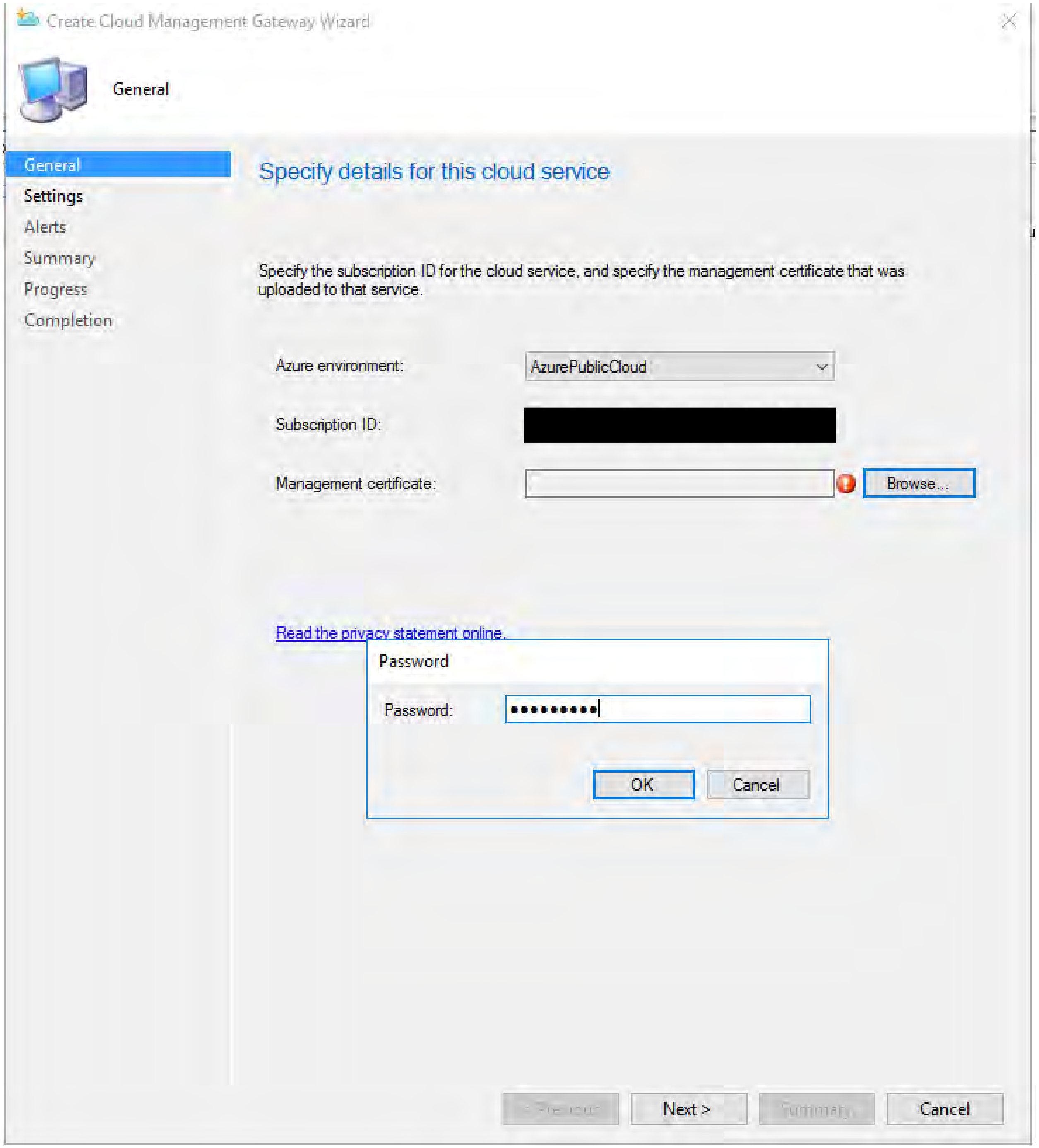
Go to – Turn On CMG Feature Pre Release



Administration ▸ Overview ▸ Updates and Servicing ▸ Features

Pre-release - Cloud Management Gateway

Click Create Cloud Management Gateway



Specify details for this cloud service

Specify the subscription ID for the cloud service, and specify the management certificate that was uploaded to that service.

Azure environment: AzurePublicCloud

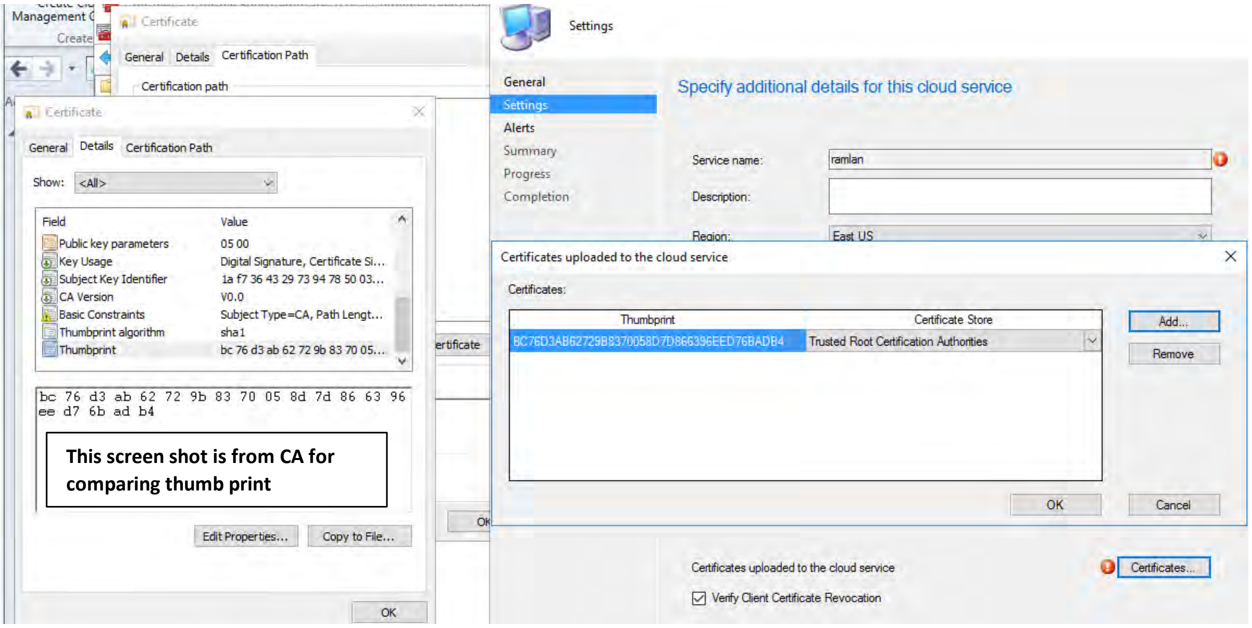
Subscription ID: [redacted]

Management certificate:

Read the privacy statement online.

Password

Password: ••••••••••



Certificate

General | Details | Certification Path

Show: <All>

| Field | Value |
|---|---|
| Public key parameters | 05 00 |
| Key Usage | Digital Signature, Certificate Si... |
| Subject Key Identifier | 1a f7 36 43 29 73 94 78 50 03... |
| CA Version | V0.0 |
| Basic Constraints | Subject Type=CA, Path Lengt... |
| Thumbprint algorithm | sha1 |
| Thumbprint | bc 76 d3 ab 62 72 9b 83 70 05... |

```
bc 76 d3 ab 62 72 9b 83 70 05 8d 7d 86 63 96
ee d7 6b ad b4
```

**This screen shot is from CA for comparing thumb print**

Settings

Specify additional details for this cloud service

Service name: ramlan

Description:

Region: East US

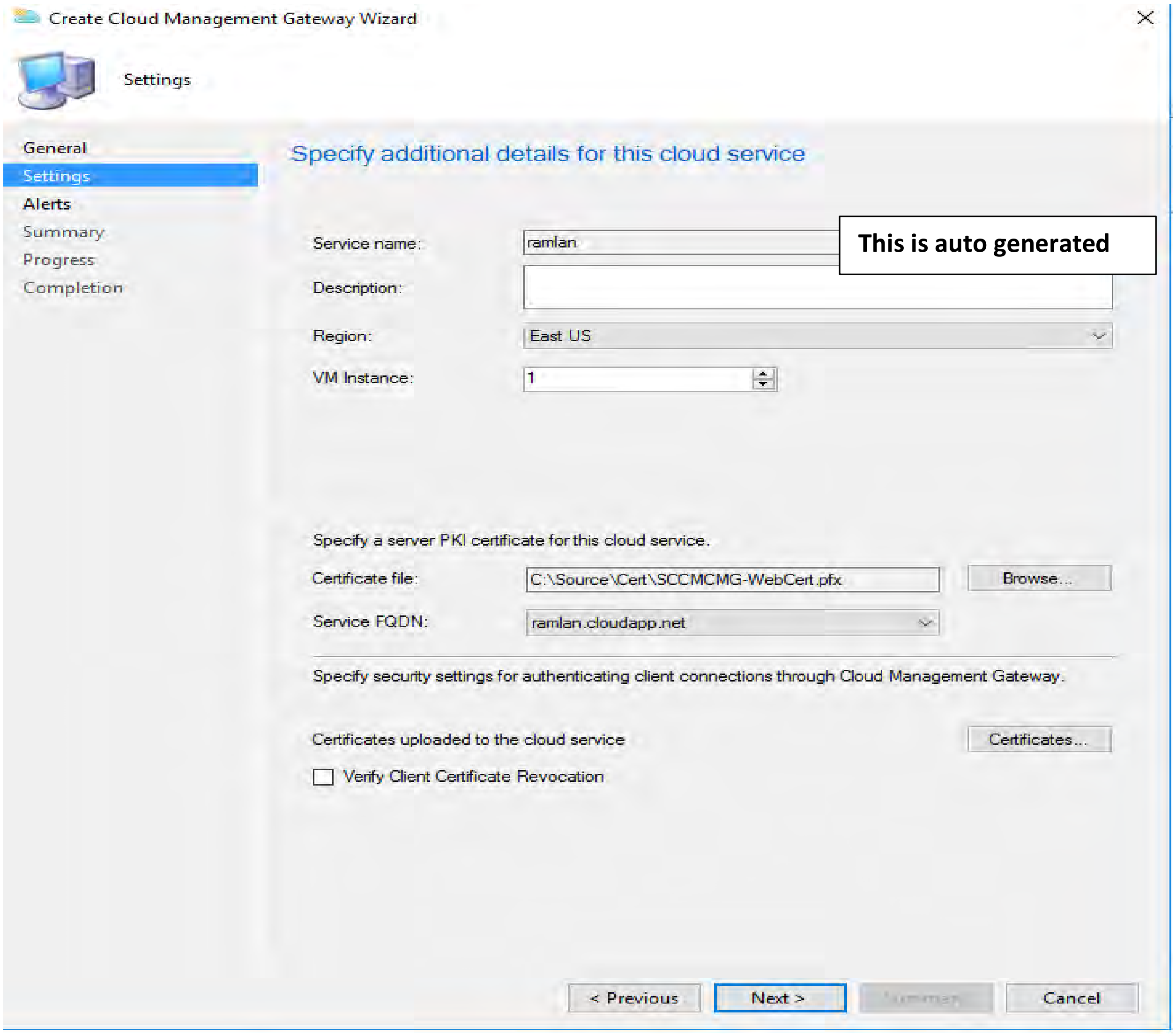
Certificates uploaded to the cloud service

Certificates:

| Thumbprint | Certificate Store |
|---|---|
| BC76D3AB62729B8370058D7D866396EED76BADB4 | Trusted Root Certification Authorities |

Certificates uploaded to the cloud service

☑ Verify Client Certificate Revocation



Create Cloud Management Gateway Wizard

Settings

Specify additional details for this cloud service

Service name: ramlan

**This is auto generated**

Description:

Region: East US

VM Instance: 1

Specify a server PKI certificate for this cloud service.

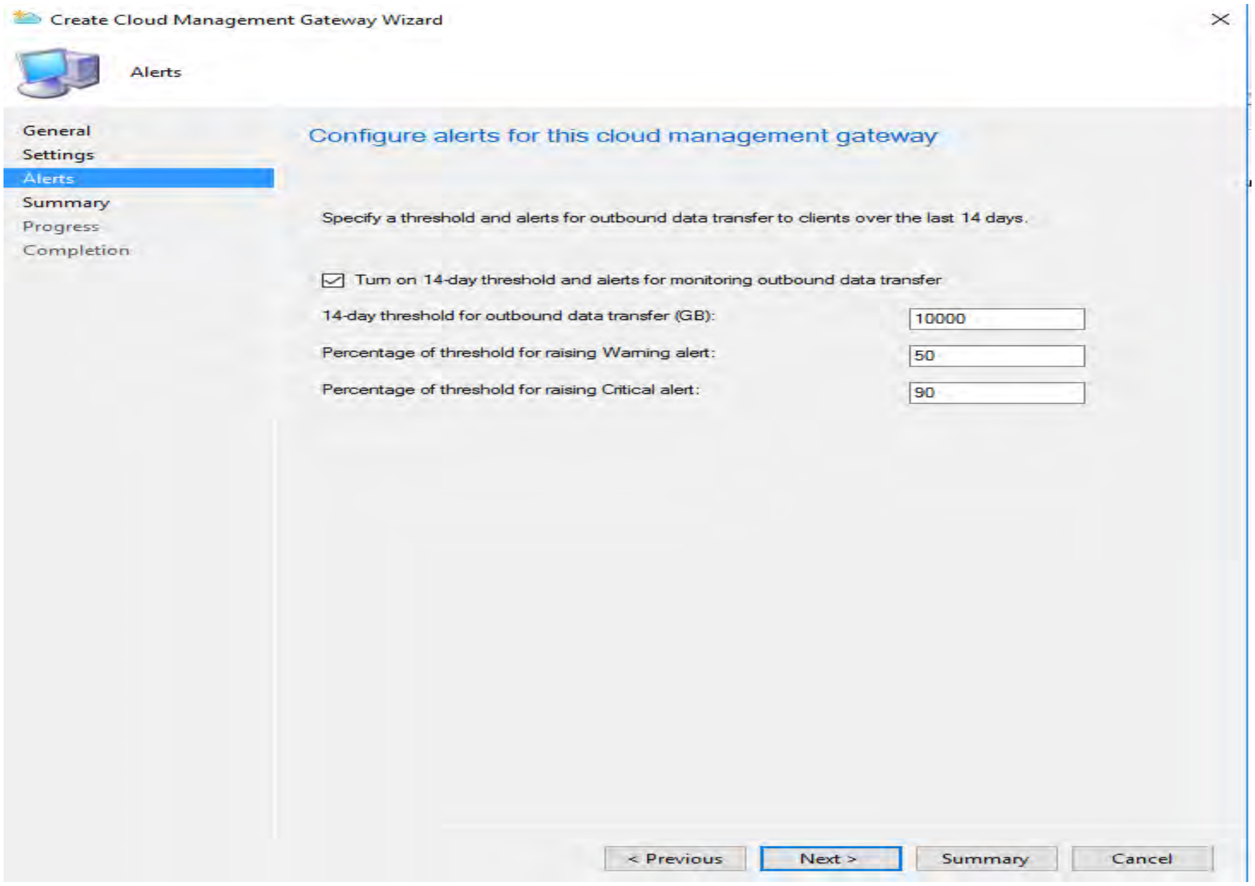
Certificate file: C:\Source\Cert\SCCMCMG-WebCert.pfx

Service FQDN: ramlan.cloudapp.net

Specify security settings for authenticating client connections through Cloud Management Gateway.

Certificates uploaded to the cloud service

□ Verify Client Certificate Revocation



Configure alerts for this cloud management gateway

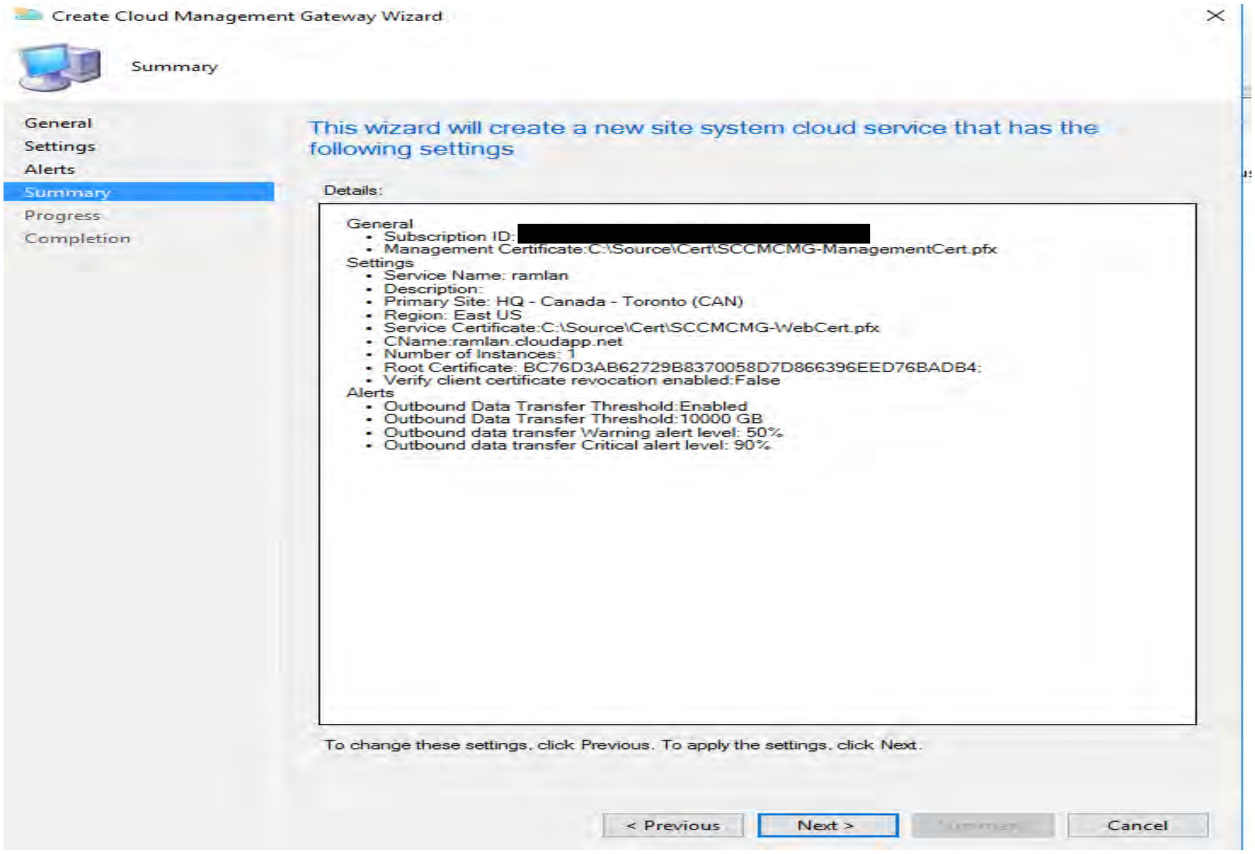
Specify a threshold and alerts for outbound data transfer to clients over the last 14 days.

☑ Turn on 14-day threshold and alerts for monitoring outbound data transfer

14-day threshold for outbound data transfer (GB): 10000

Percentage of threshold for raising Warning alert: 50

Percentage of threshold for raising Critical alert: 90

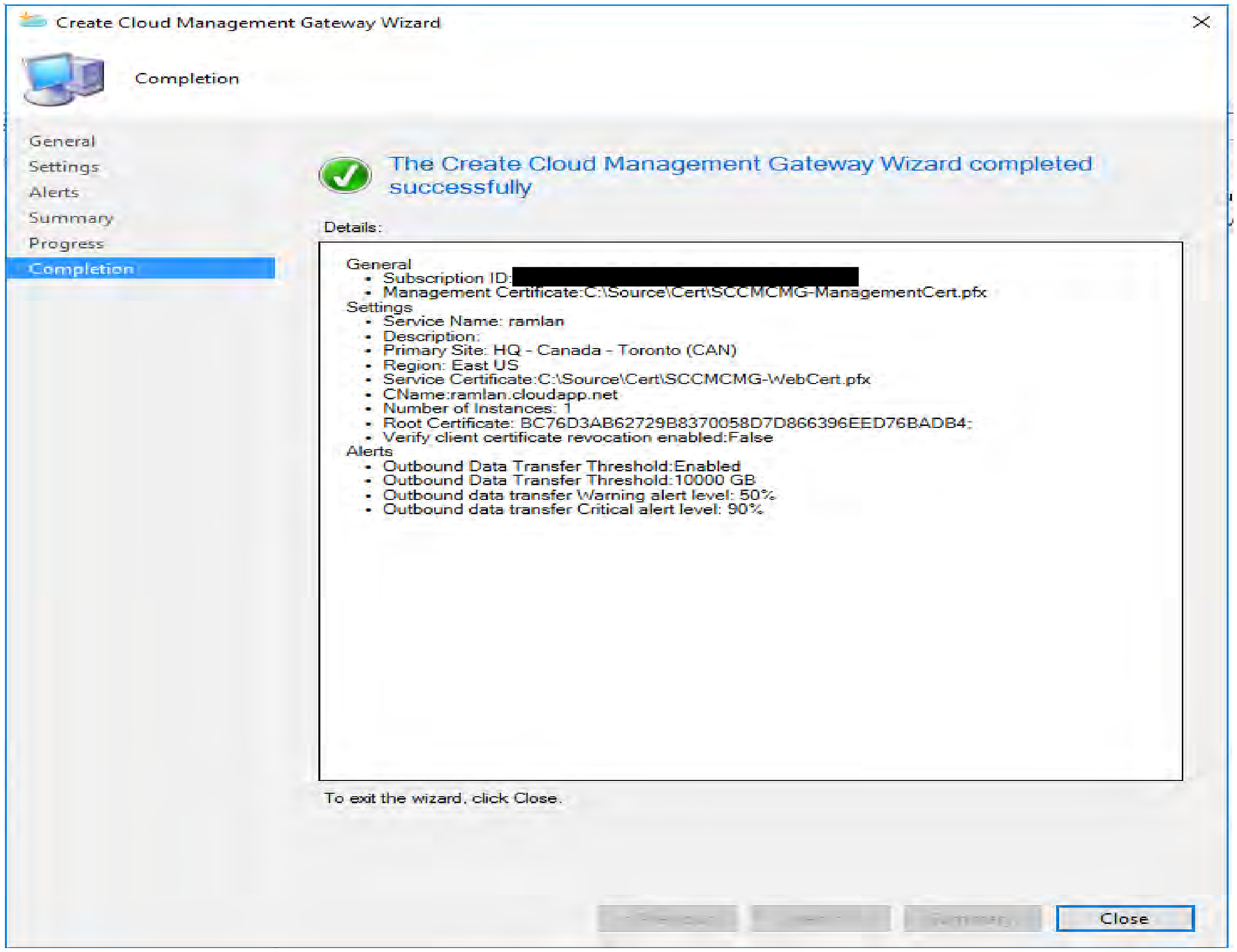


This wizard will create a new site system cloud service that has the following settings

Details:

```
General
  • Subscription ID: [redacted]
  • Management Certificate:C:\Source\Cert\SCCMCMG-ManagementCert.pfx
Settings
  • Service Name: ramlan
  • Description:
  • Primary Site: HQ - Canada - Toronto (CAN)
  • Region: East US
  • Service Certificate:C:\Source\Cert\SCCMCMG-WebCert.pfx
  • CName:ramlan.cloudapp.net
  • Number of Instances: 1
  • Root Certificate: BC76D3AB62729B8370058D7D866396EED76BADB4;
  • Verify client certificate revocation enabled:False
Alerts
  • Outbound Data Transfer Threshold:Enabled
  • Outbound Data Transfer Threshold:10000 GB
  • Outbound data transfer Warning alert level: 50%
  • Outbound data transfer Critical alert level: 90%
```

To change these settings, click Previous. To apply the settings, click Next.



The Create Cloud Management Gateway Wizard completed successfully

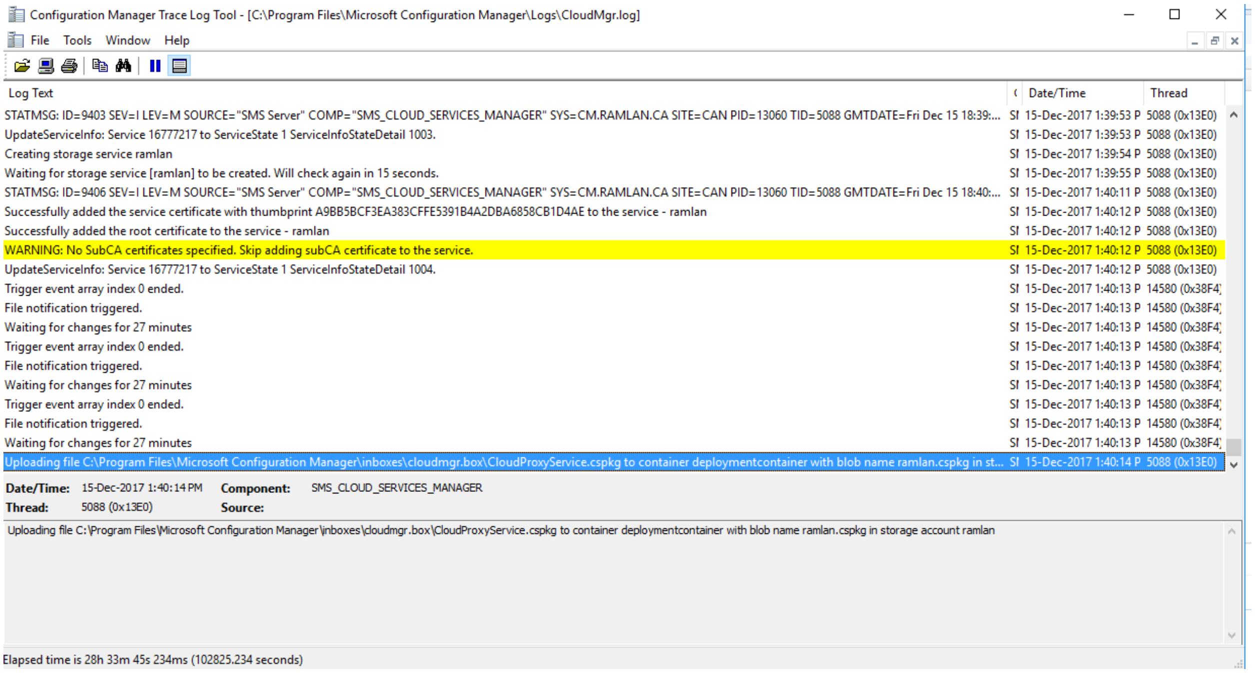
Details:

General
- Subscription ID: [redacted]
- Management Certificate:C:\Source\Cert\SCCMCMG-ManagementCert.pfx

Settings
- Service Name: ramlan
- Description:
- Primary Site: HQ - Canada - Toronto (CAN)
- Region: East US
- Service Certificate:C:\Source\Cert\SCCMCMG-WebCert.pfx
- CName:ramlan.cloudapp.net
- Number of Instances: 1
- Root Certificate: BC76D3AB62729B8370058D7D866396EED76BADB4;
- Verify client certificate revocation enabled:False

Alerts
- Outbound Data Transfer Threshold:Enabled
- Outbound Data Transfer Threshold:10000 GB
- Outbound data transfer Warning alert level: 50%
- Outbound data transfer Critical alert level: 90%

To exit the wizard, click Close.


Configuration Manager Trace Log Tool - [C:\Program Files\Microsoft Configuration Manager\Logs\CloudMgr.log]
File
Tools
Window
Help

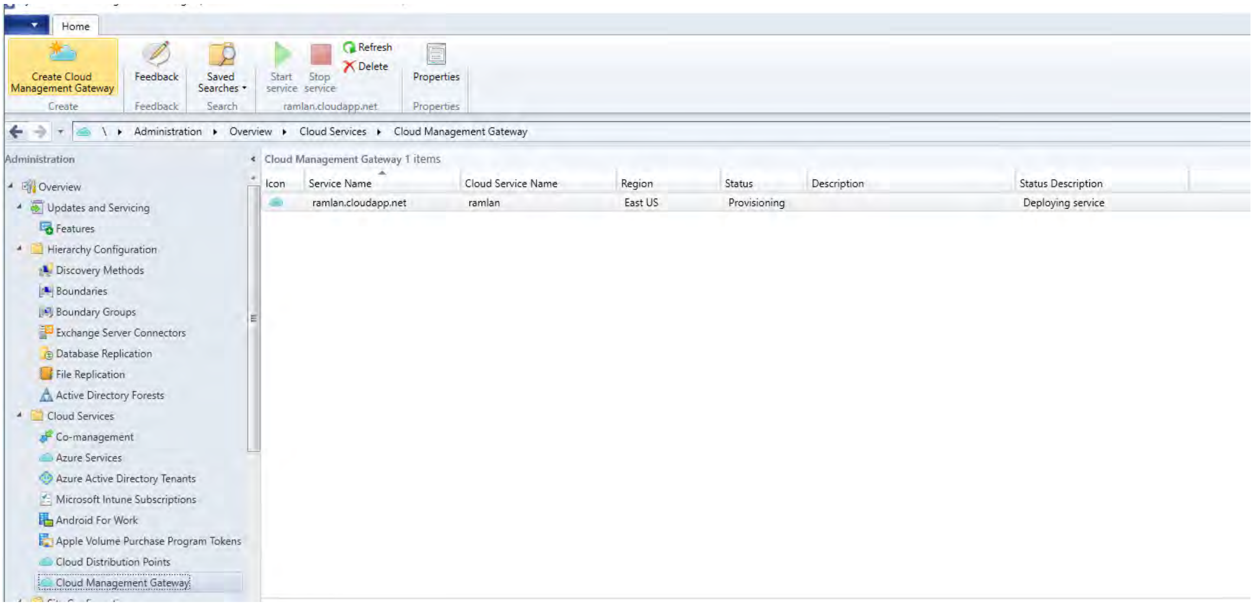
```
Log Text                                                                                                                                          ( Date/Time            Thread
STATMSG: ID=9403 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_CLOUD_SERVICES_MANAGER" SYS=CM.RAMLAN.CA SITE=CAN PID=13060 TID=5088 GMTDATE=Fri Dec 15 18:39:...  SI 15-Dec-2017 1:39:53 P  5088 (0x13E0)
UpdateServiceInfo: Service 16777217 to ServiceState 1 ServiceInfoStateDetail 1003.                                                                  SI 15-Dec-2017 1:39:53 P  5088 (0x13E0)
Creating storage service ramlan                                                                                                                     SI 15-Dec-2017 1:39:54 P  5088 (0x13E0)
Waiting for storage service [ramlan] to be created. Will check again in 15 seconds.                                                                 SI 15-Dec-2017 1:39:55 P  5088 (0x13E0)
STATMSG: ID=9406 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_CLOUD_SERVICES_MANAGER" SYS=CM.RAMLAN.CA SITE=CAN PID=13060 TID=5088 GMTDATE=Fri Dec 15 18:40:...  SI 15-Dec-2017 1:40:11 P  5088 (0x13E0)
Successfully added the service certificate with thumbprint A9BB5BCF3EA383CFFE5391B4A2DBA6858CB1D4AE to the service - ramlan                         SI 15-Dec-2017 1:40:12 P  5088 (0x13E0)
Successfully added the root certificate to the service - ramlan                                                                                     SI 15-Dec-2017 1:40:12 P  5088 (0x13E0)
WARNING: No SubCA certificates specified. Skip adding subCA certificate to the service.                                                             SI 15-Dec-2017 1:40:12 P  5088 (0x13E0)
UpdateServiceInfo: Service 16777217 to ServiceState 1 ServiceInfoStateDetail 1004.                                                                  SI 15-Dec-2017 1:40:12 P  5088 (0x13E0)
Trigger event array index 0 ended.                                                                                                                  SI 15-Dec-2017 1:40:13 P  14580 (0x38F4)
File notification triggered.                                                                                                                        SI 15-Dec-2017 1:40:13 P  14580 (0x38F4)
Waiting for changes for 27 minutes                                                                                                                  SI 15-Dec-2017 1:40:13 P  14580 (0x38F4)
Trigger event array index 0 ended.                                                                                                                  SI 15-Dec-2017 1:40:13 P  14580 (0x38F4)
File notification triggered.                                                                                                                        SI 15-Dec-2017 1:40:13 P  14580 (0x38F4)
Waiting for changes for 27 minutes                                                                                                                  SI 15-Dec-2017 1:40:13 P  14580 (0x38F4)
Trigger event array index 0 ended.                                                                                                                  SI 15-Dec-2017 1:40:13 P  14580 (0x38F4)
File notification triggered.                                                                                                                        SI 15-Dec-2017 1:40:13 P  14580 (0x38F4)
Waiting for changes for 27 minutes                                                                                                                  SI 15-Dec-2017 1:40:13 P  14580 (0x38F4)
Uploading file C:\Program Files\Microsoft Configuration Manager\inboxes\cloudmgr.box\CloudProxyService.cspkg to container deploymentcontainer with blob name ramlan.cspkg in st...  SI 15-Dec-2017 1:40:14 P  5088 (0x13E0)
```

**Date/Time:** 15-Dec-2017 1:40:14 PM **Component:** SMS_CLOUD_SERVICES_MANAGER

**Thread:** 5088 (0x13E0) **Source:**

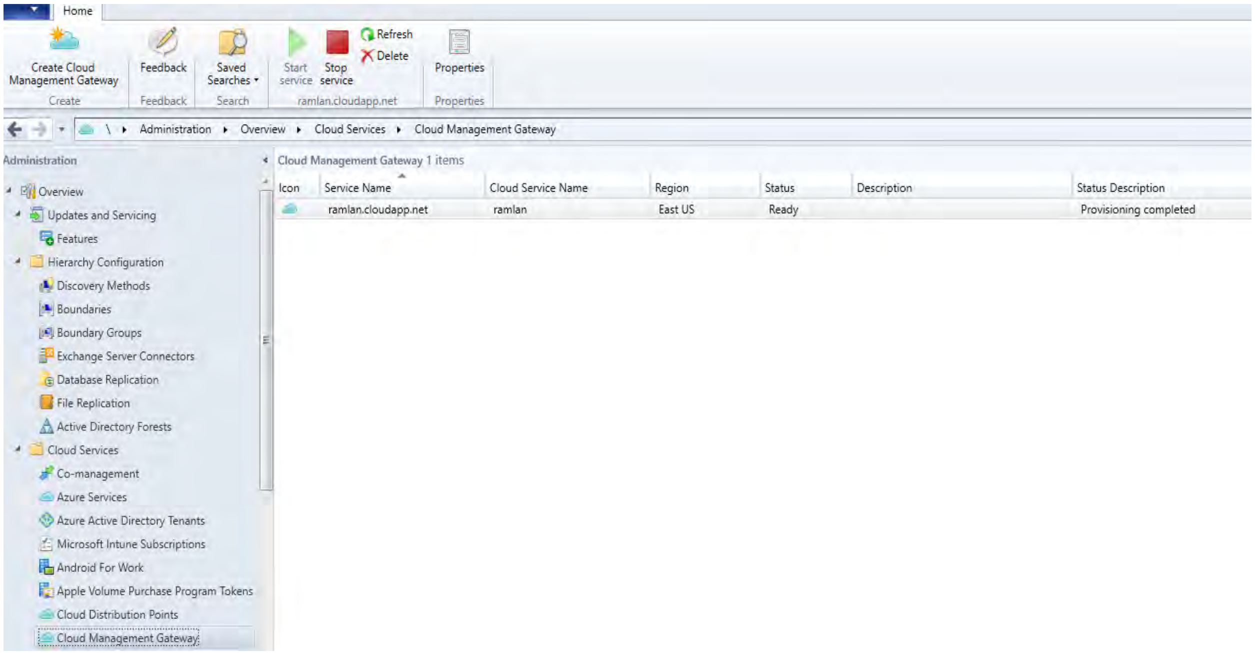
```
Uploading file C:\Program Files\Microsoft Configuration Manager\inboxes\cloudmgr.box\CloudProxyService.cspkg to container deploymentcontainer with blob name ramlan.cspkg in storage account ramlan
```

Elapsed time is 28h 33m 45s 234ms (102825.234 seconds)



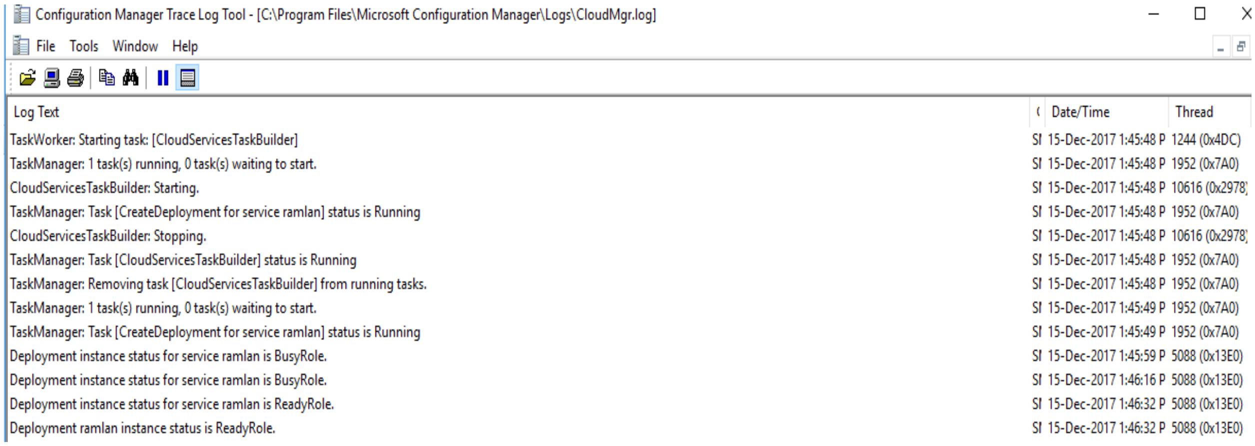
Cloud Management Gateway 1 items

| Icon | Service Name | Cloud Service Name | Region | Status | Description | Status Description |
|---|---|---|---|---|---|---|
| | ramlan.cloudapp.net | ramlan | East US | Provisioning | | Deploying service |

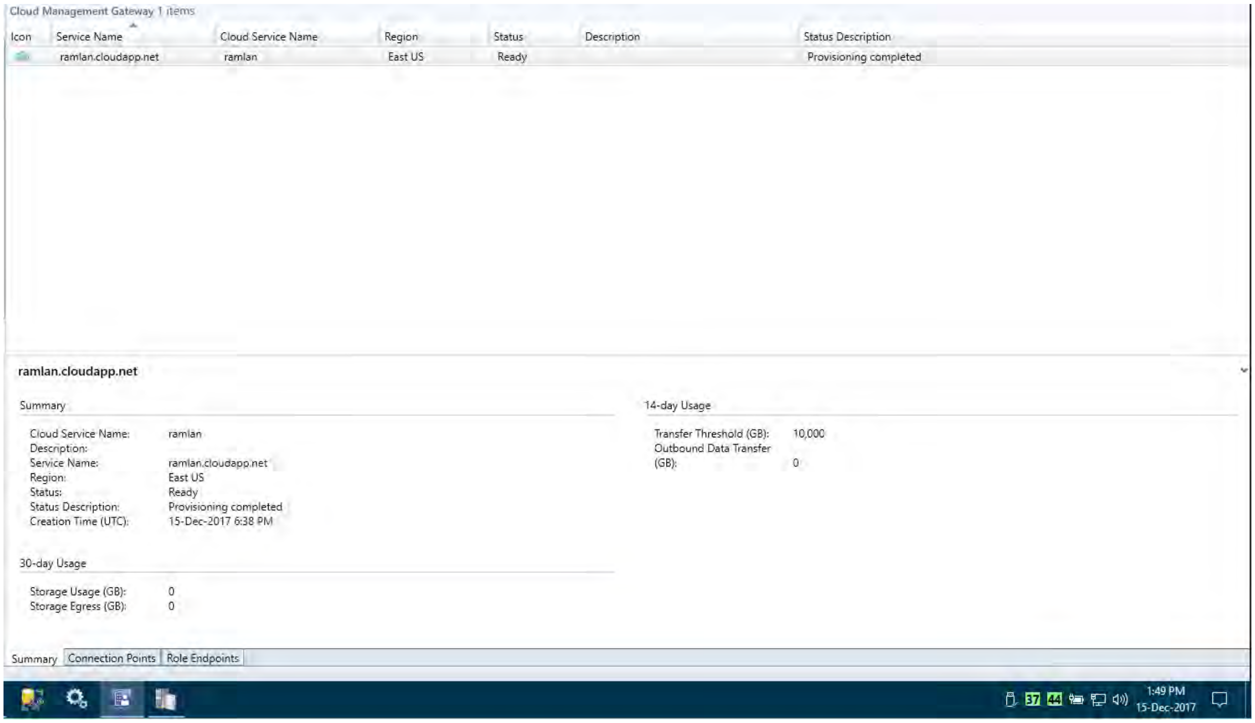


Cloud Management Gateway 1 items

| Icon | Service Name | Cloud Service Name | Region | Status | Description | Status Description |
|---|---|---|---|---|---|---|
| | ramlan.cloudapp.net | ramlan | East US | Ready | | Provisioning completed |


Configuration Manager Trace Log Tool - [C:\Program Files\Microsoft Configuration Manager\Logs\CloudMgr.log]
File Tools Window Help

```
Log Text                                                                  ( Date/Time            Thread
TaskWorker: Starting task: [CloudServicesTaskBuilder]                     SI 15-Dec-2017 1:45:48 P 1244 (0x4DC)
TaskManager: 1 task(s) running, 0 task(s) waiting to start.               SI 15-Dec-2017 1:45:48 P 1952 (0x7A0)
CloudServicesTaskBuilder: Starting.                                       SI 15-Dec-2017 1:45:48 P 10616 (0x2978)
TaskManager: Task [CreateDeployment for service ramlan] status is Running SI 15-Dec-2017 1:45:48 P 1952 (0x7A0)
CloudServicesTaskBuilder: Stopping.                                       SI 15-Dec-2017 1:45:48 P 10616 (0x2978)
TaskManager: Task [CloudServicesTaskBuilder] status is Running            SI 15-Dec-2017 1:45:48 P 1952 (0x7A0)
TaskManager: Removing task [CloudServicesTaskBuilder] from running tasks. SI 15-Dec-2017 1:45:48 P 1952 (0x7A0)
TaskManager: 1 task(s) running, 0 task(s) waiting to start.               SI 15-Dec-2017 1:45:49 P 1952 (0x7A0)
TaskManager: Task [CreateDeployment for service ramlan] status is Running SI 15-Dec-2017 1:45:49 P 1952 (0x7A0)
Deployment instance status for service ramlan is BusyRole.                SI 15-Dec-2017 1:45:59 P 5088 (0x13E0)
Deployment instance status for service ramlan is BusyRole.                SI 15-Dec-2017 1:46:16 P 5088 (0x13E0)
Deployment instance status for service ramlan is ReadyRole.               SI 15-Dec-2017 1:46:32 P 5088 (0x13E0)
Deployment ramlan instance status is ReadyRole.                           SI 15-Dec-2017 1:46:32 P 5088 (0x13E0)
```



Cloud Management Gateway 1 items

| Icon | Service Name | Cloud Service Name | Region | Status | Description | Status Description |
|---|---|---|---|---|---|---|
| | ramlan.cloudapp.net | ramlan | East US | Ready | | Provisioning completed |

**ramlan.cloudapp.net**

Summary

| | |
|---|---|
| Cloud Service Name: | ramlan |
| Description: | |
| Service Name: | ramlan.cloudapp.net |
| Region: | East US |
| Status: | Ready |
| Status Description: | Provisioning completed |
| Creation Time (UTC): | 15-Dec-2017 6:38 PM |

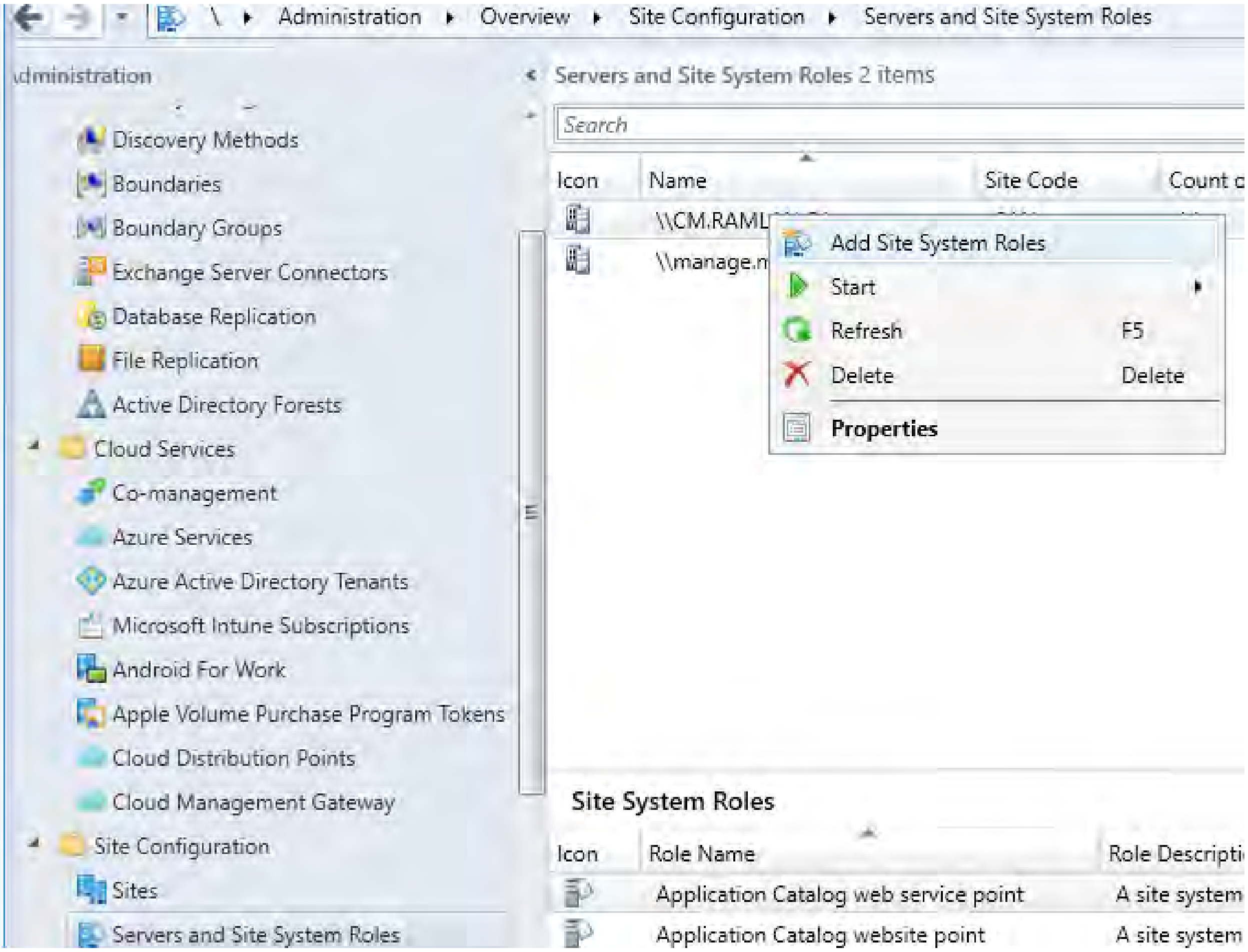
14-day Usage

| | |
|---|---|
| Transfer Threshold (GB): | 10,000 |
| Outbound Data Transfer (GB): | 0 |

30-day Usage

| | |
|---|---|
| Storage Usage (GB): | 0 |
| Storage Egress (GB): | 0 |

Now we will create CMG connection point

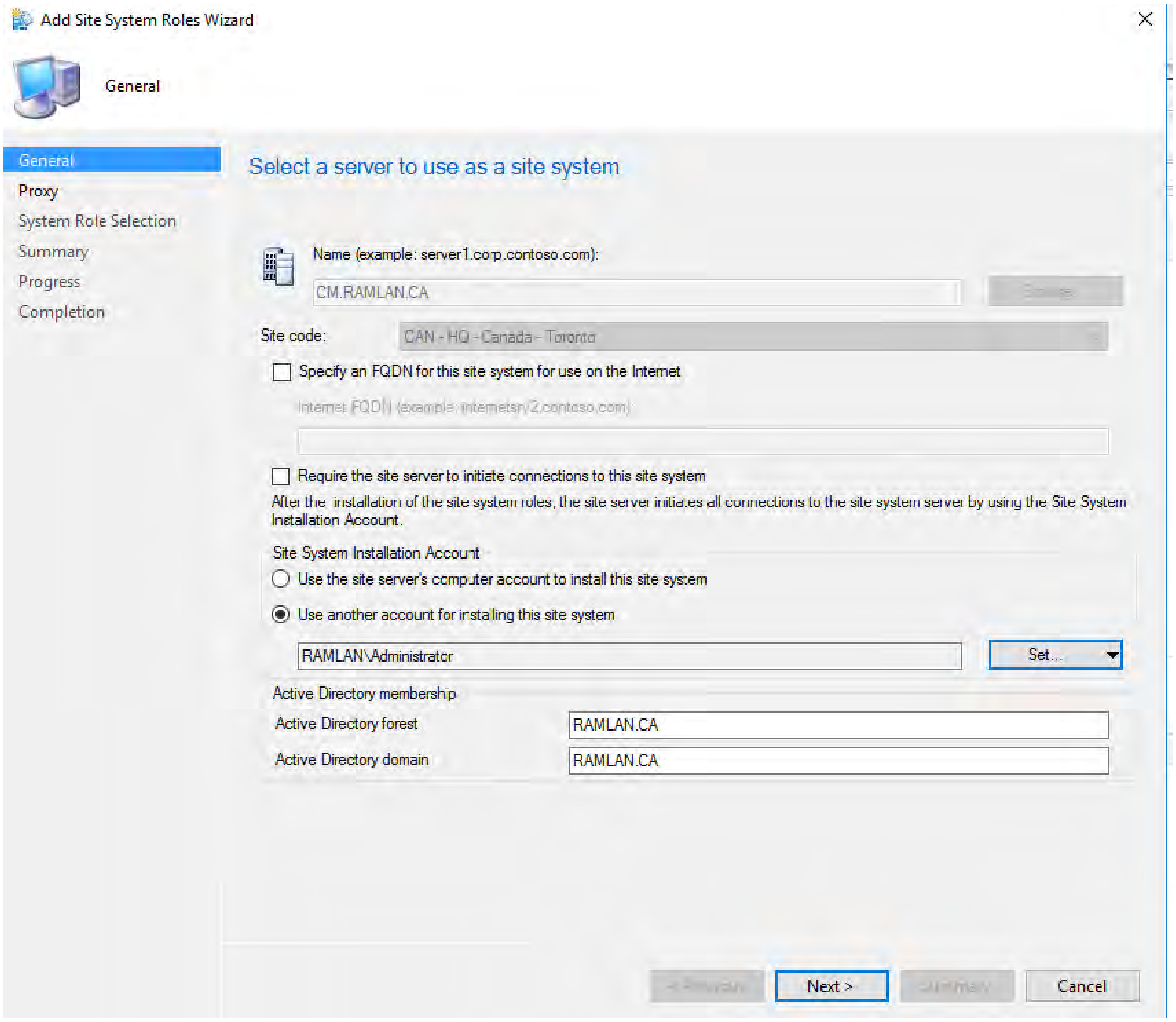


\ ▸ Administration ▸ Overview ▸ Site Configuration ▸ Servers and Site System Roles
dministration
Discovery Methods
Boundaries
Boundary Groups
Exchange Server Connectors
Database Replication
File Replication
Active Directory Forests
Cloud Services
Co-management
Azure Services
Azure Active Directory Tenants
Microsoft Intune Subscriptions
Android For Work
Apple Volume Purchase Program Tokens
Cloud Distribution Points
Cloud Management Gateway
Site Configuration
Sites
Servers and Site System Roles
Servers and Site System Roles 2 items
Search
Add Site System Roles
Start
Refresh F5
Delete Delete
Properties

| Icon | Name | Site Code | Count c |
|---|---|---|---|
| | \\CM.RAML | | |
| | \\manage.n | | |

Site System Roles

| Icon | Role Name | Role Descripti |
|---|---|---|
| | Application Catalog web service point | A site system |
| | Application Catalog website point | A site system |



Select a server to use as a site system

Name (example: server1.corp.contoso.com): CM.RAMLAN.CA

Site code: CAN - HQ - Canada - Toronto

☐ Specify an FQDN for this site system for use on the Internet

Internet FQDN (example: internetsrv2.contoso.com)

☐ Require the site server to initiate connections to this site system

After the installation of the site system roles, the site server initiates all connections to the site system server by using the Site System Installation Account.

Site System Installation Account

○ Use the site server's computer account to install this site system

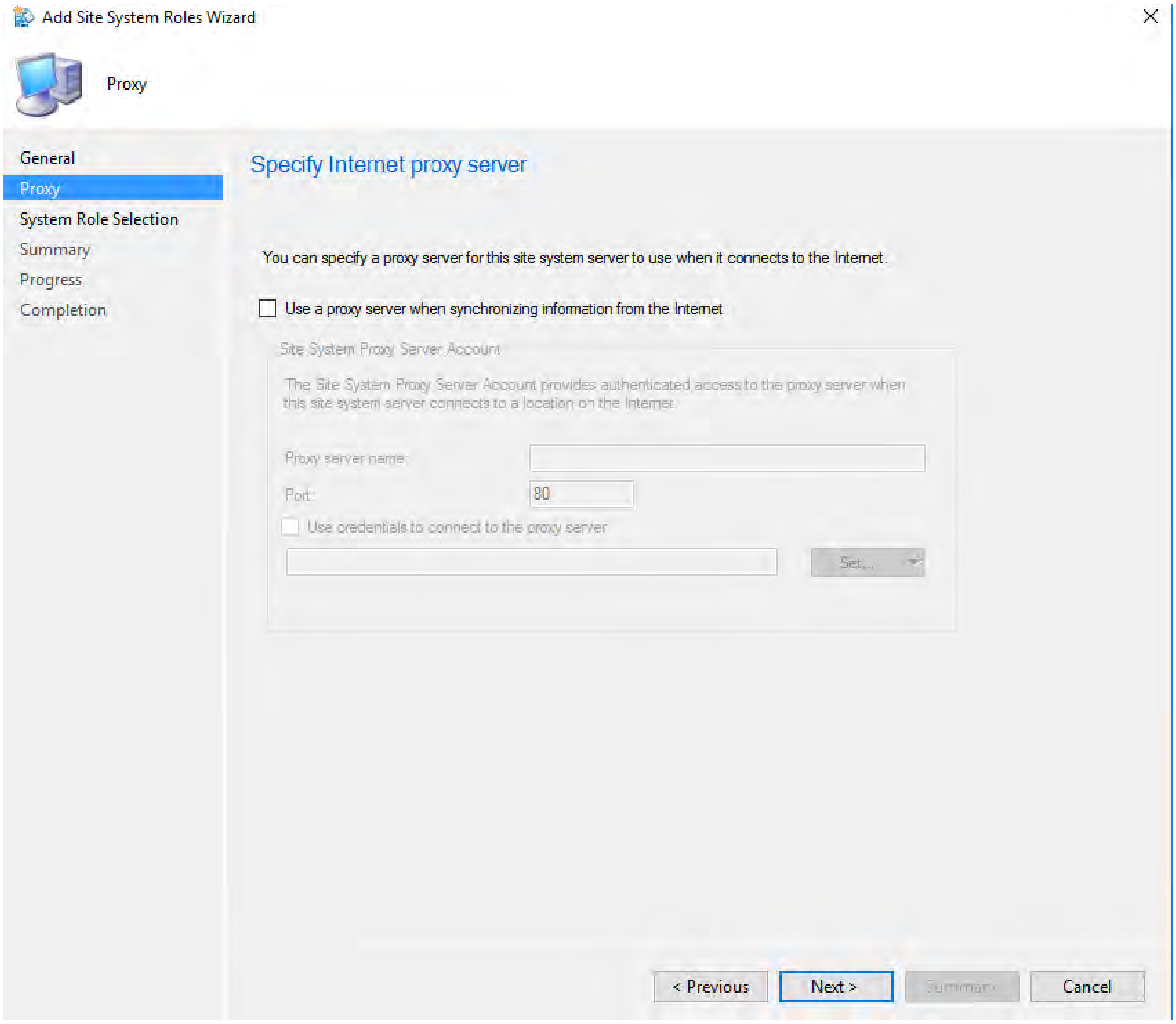
● Use another account for installing this site system

RAMLAN\Administrator

Active Directory membership

Active Directory forest: RAMLAN.CA

Active Directory domain: RAMLAN.CA



Specify Internet proxy server

You can specify a proxy server for this site system server to use when it connects to the Internet.

□ Use a proxy server when synchronizing information from the Internet

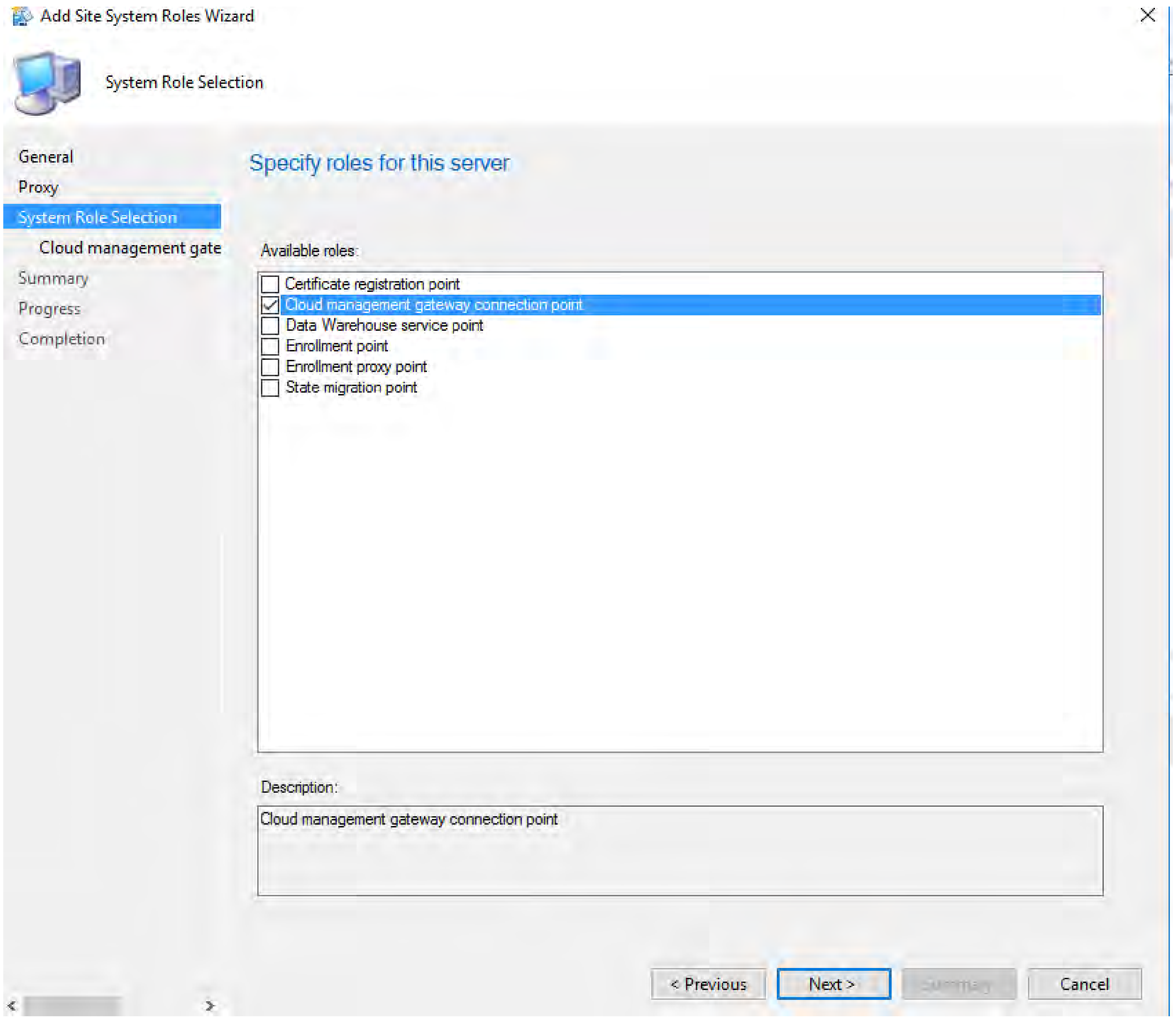
Site System Proxy Server Account

The Site System Proxy Server Account provides authenticated access to the proxy server when this site system server connects to a location on the Internet.

Proxy server name:

Port: 80

□ Use credentials to connect to the proxy server



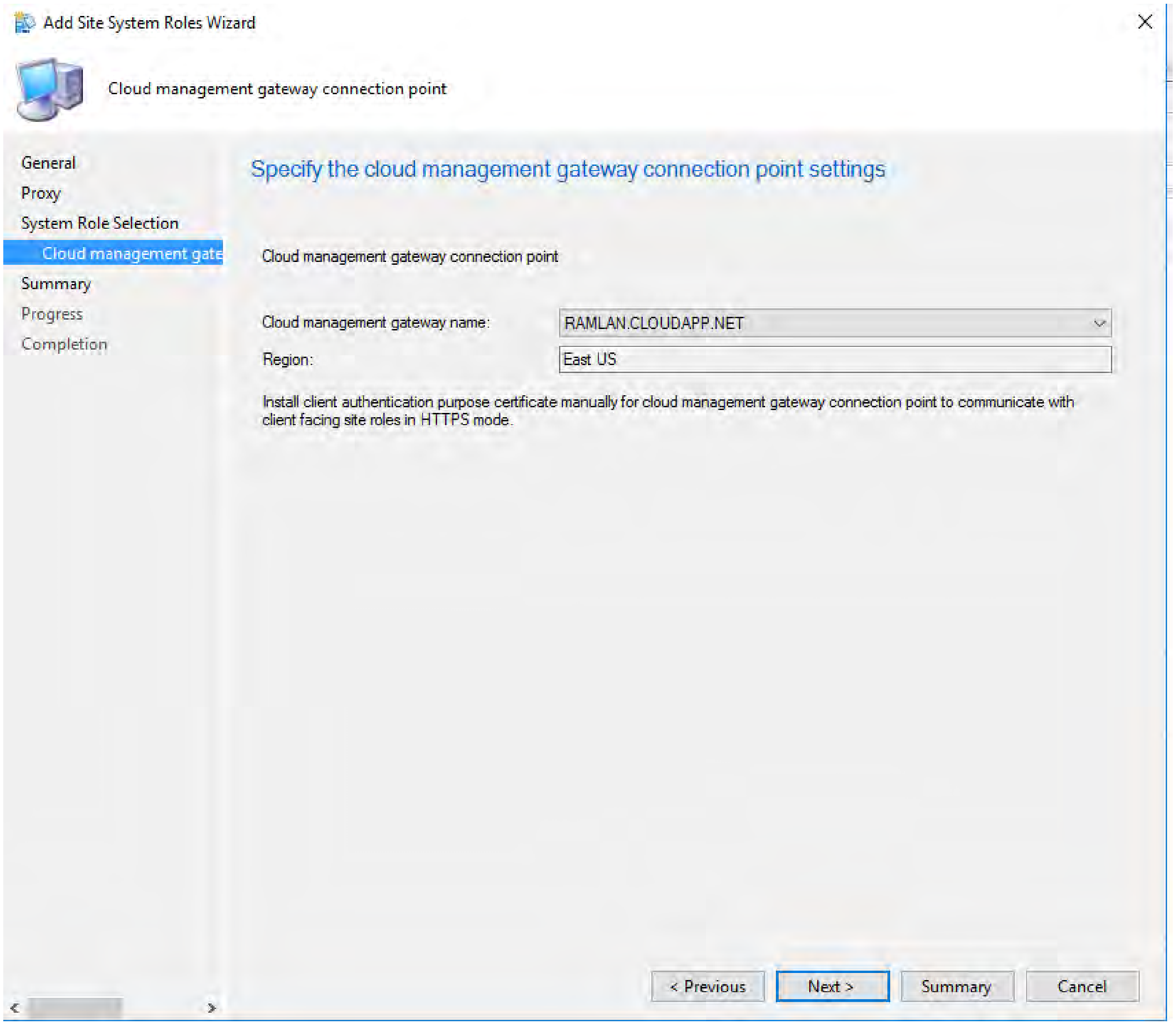
Specify roles for this server

Available roles:

- □ Certificate registration point
- ☑ Cloud management gateway connection point
- □ Data Warehouse service point
- □ Enrollment point
- □ Enrollment proxy point
- □ State migration point

Description:

Cloud management gateway connection point



Add Site System Roles Wizard

Cloud management gateway connection point

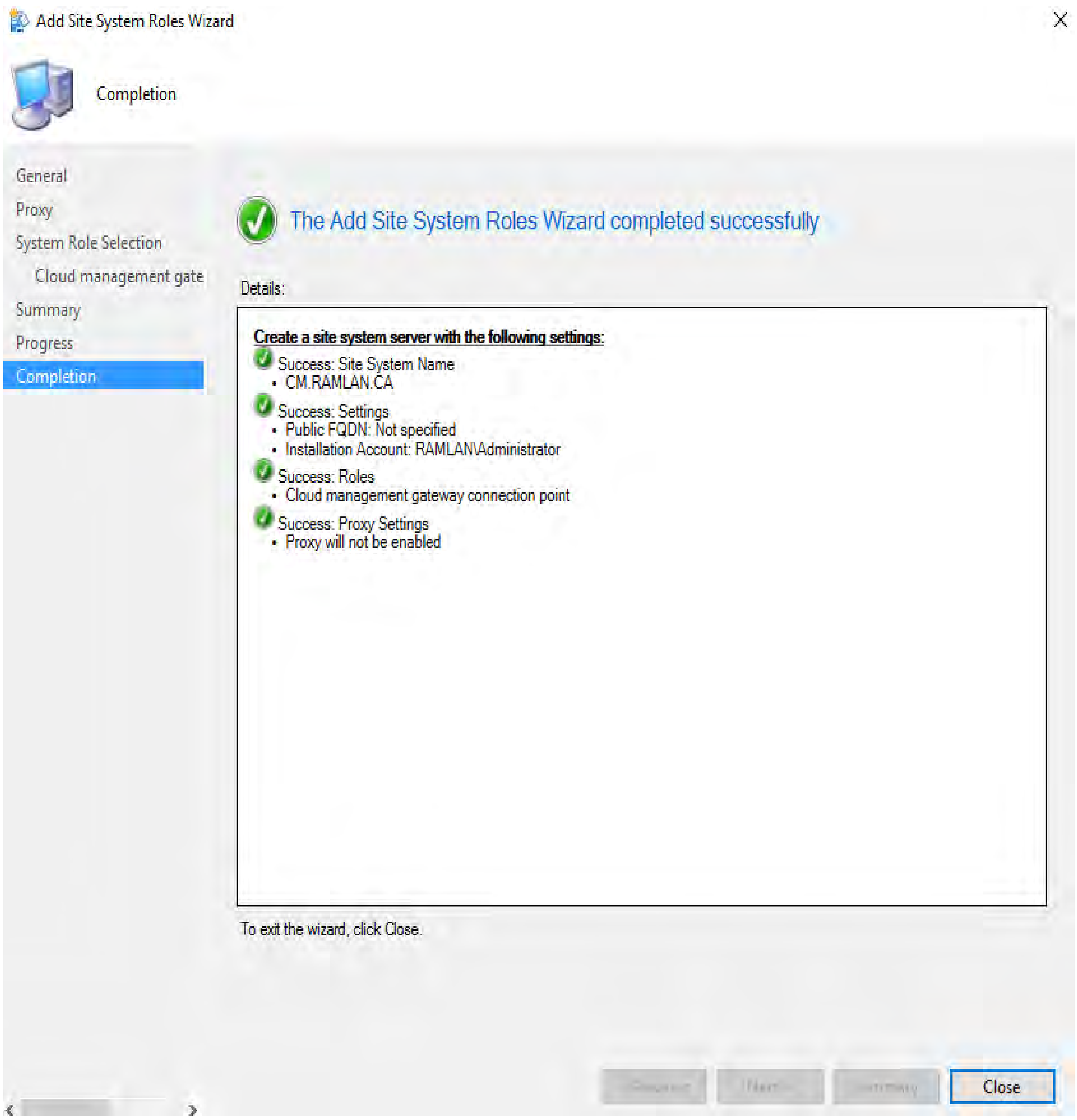
Specify the cloud management gateway connection point settings

Cloud management gateway connection point

Cloud management gateway name: RAMLAN.CLOUDAPP.NET

Region: East US

Install client authentication purpose certificate manually for cloud management gateway connection point to communicate with client facing site roles in HTTPS mode.



The Add Site System Roles Wizard completed successfully

Details:

**Create a site system server with the following settings:**

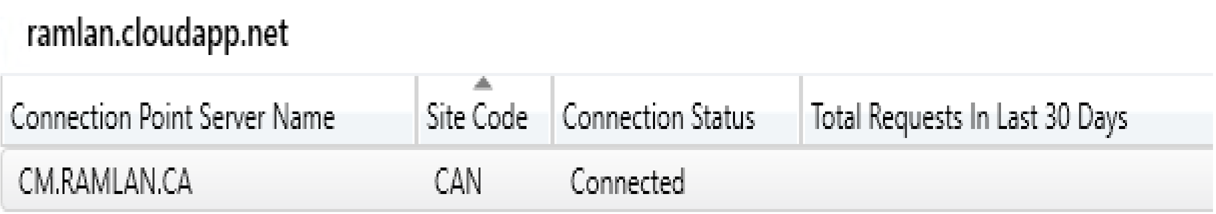
✓ Success: Site System Name
- CM.RAMLAN.CA

✓ Success: Settings
- Public FQDN: Not specified
- Installation Account: RAMLAN\Administrator

✓ Success: Roles
- Cloud management gateway connection point

✓ Success: Proxy Settings
- Proxy will not be enabled

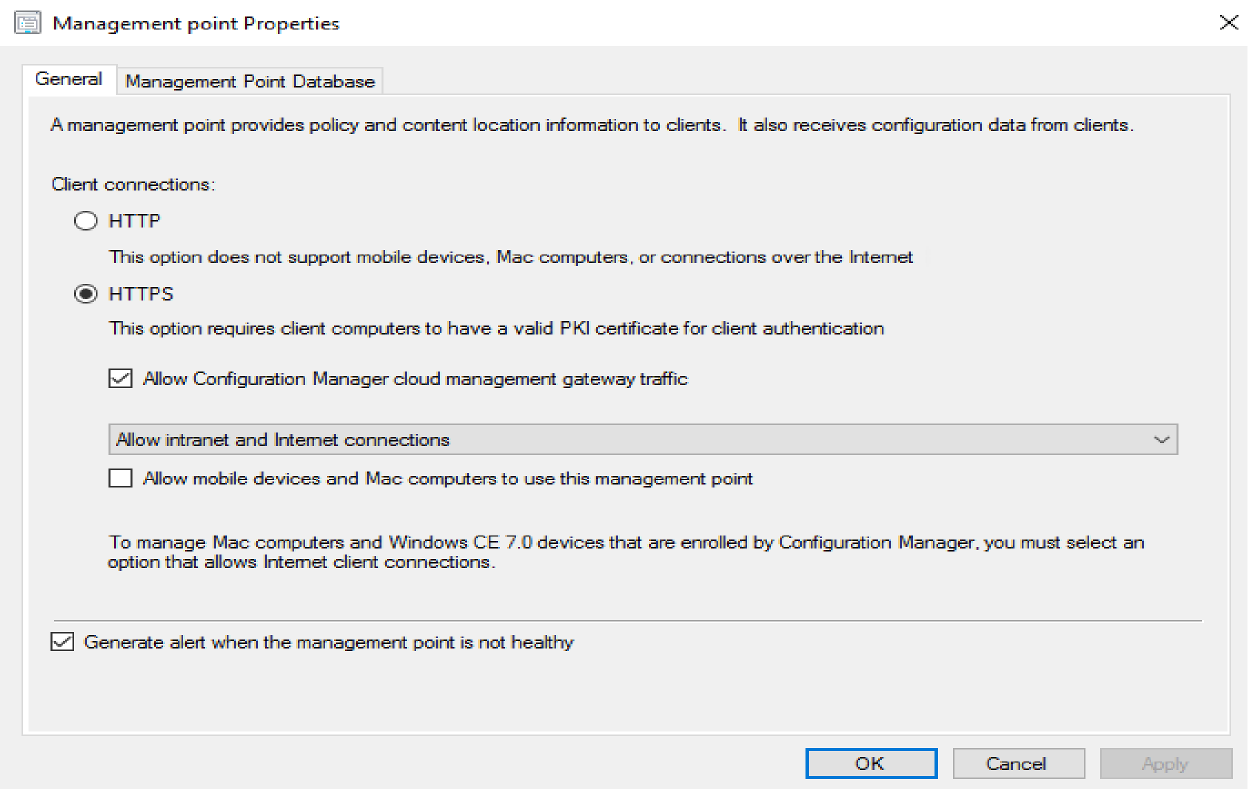
To exit the wizard, click Close.



ramlan.cloudapp.net

| Connection Point Server Name | Site Code | Connection Status | Total Requests In Last 30 Days |
|---|---|---|---|
| CM.RAMLAN.CA | CAN | Connected | |

Now we can enable MP and SUP to allow CMG traffic within our network



Management point Properties

A management point provides policy and content location information to clients. It also receives configuration data from clients.

Client connections:

○ HTTP

This option does not support mobile devices, Mac computers, or connections over the Internet

● HTTPS

This option requires client computers to have a valid PKI certificate for client authentication

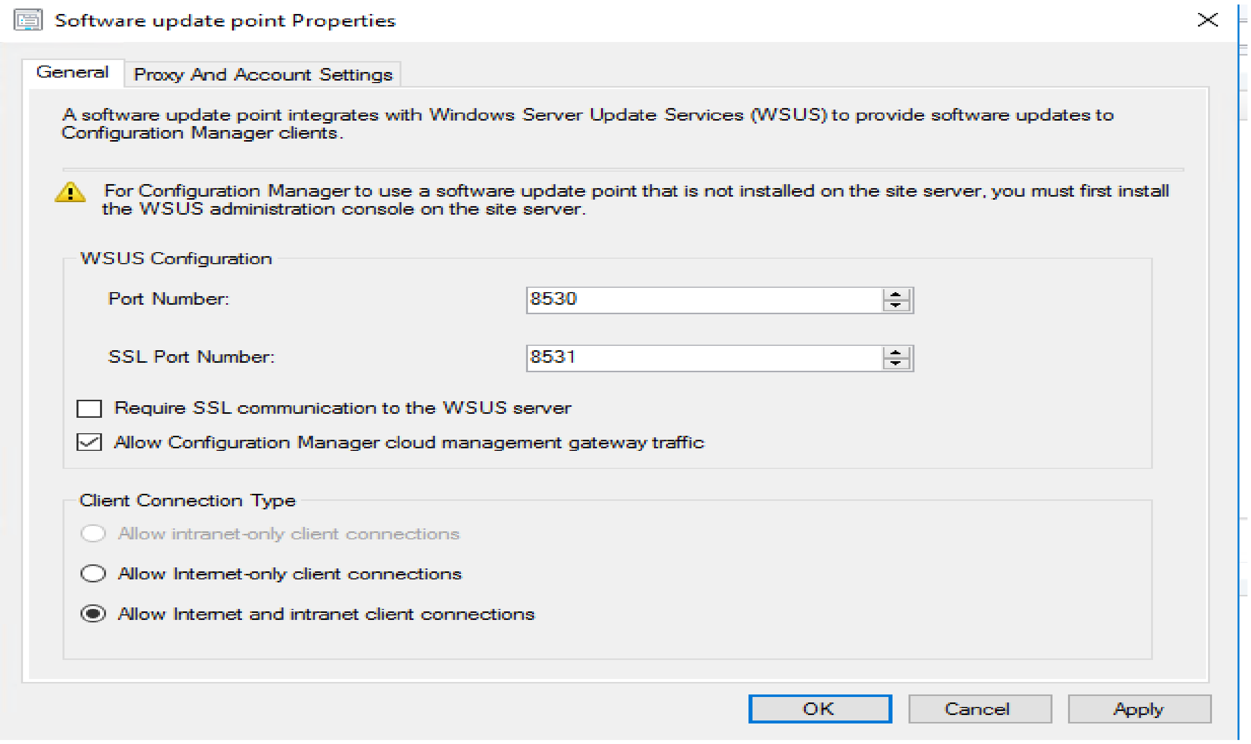
☑ Allow Configuration Manager cloud management gateway traffic

Allow intranet and Internet connections

□ Allow mobile devices and Mac computers to use this management point

To manage Mac computers and Windows CE 7.0 devices that are enrolled by Configuration Manager, you must select an option that allows Internet client connections.

☑ Generate alert when the management point is not healthy



Software update point Properties

A software update point integrates with Windows Server Update Services (WSUS) to provide software updates to Configuration Manager clients.

For Configuration Manager to use a software update point that is not installed on the site server, you must first install the WSUS administration console on the site server.

WSUS Configuration

Port Number: 8530

SSL Port Number: 8531

□ Require SSL communication to the WSUS server

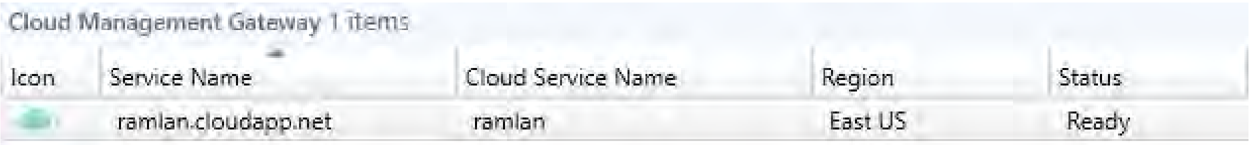
☑ Allow Configuration Manager cloud management gateway traffic

Client Connection Type

○ Allow intranet-only client connections

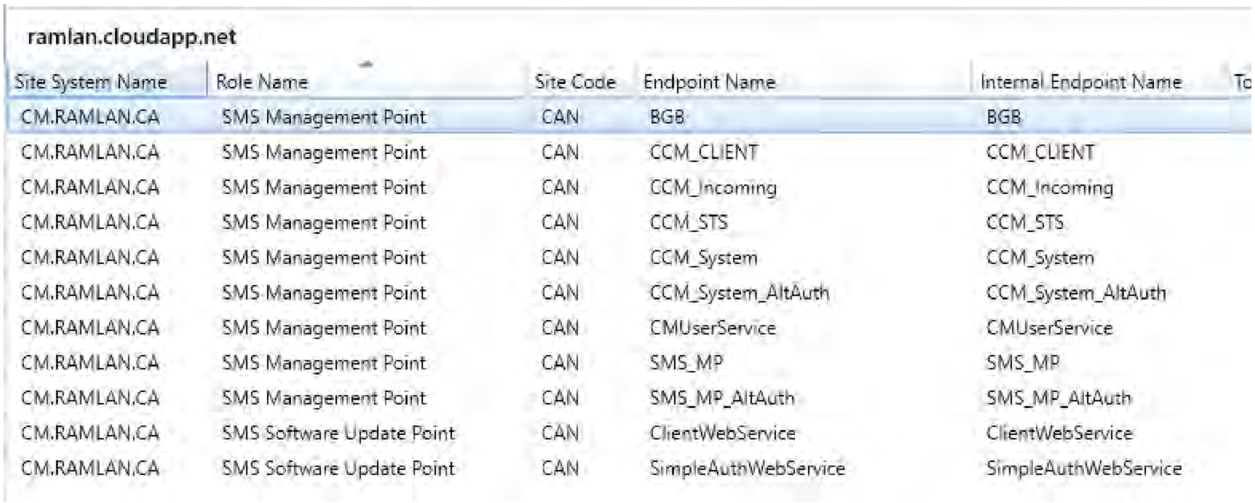
○ Allow Internet-only client connections

● Allow Internet and intranet client connections



Cloud Management Gateway 1 items

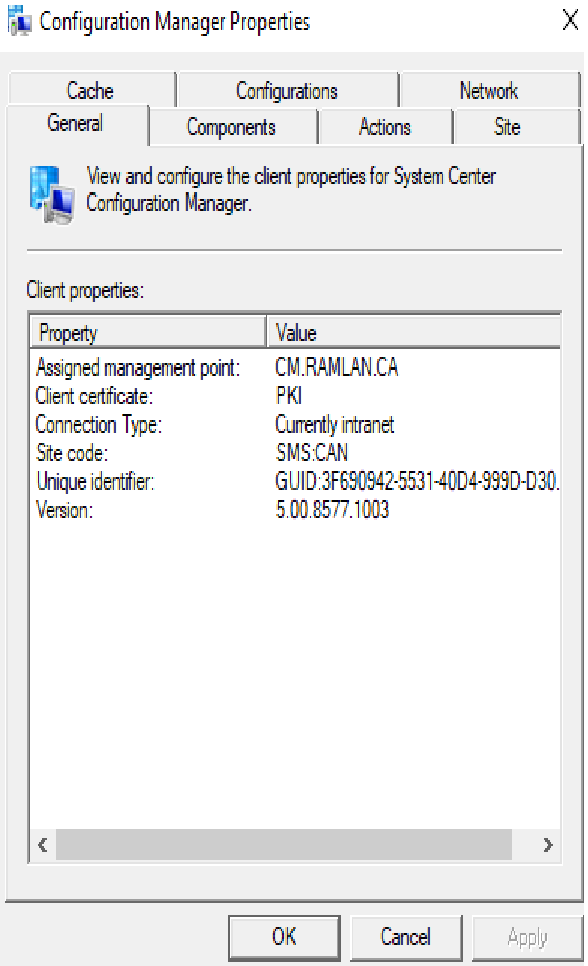
| Icon | Service Name | Cloud Service Name | Region | Status |
|---|---|---|---|---|
|  | ramlan.cloudapp.net | ramlan | East US | Ready |



ramlan.cloudapp.net

| Site System Name | Role Name | Site Code | Endpoint Name | Internal Endpoint Name | To |
|---|---|---|---|---|---|
| CM.RAMLAN.CA | SMS Management Point | CAN | BGB | BGB |  |
| CM.RAMLAN.CA | SMS Management Point | CAN | CCM_CLIENT | CCM_CLIENT |  |
| CM.RAMLAN.CA | SMS Management Point | CAN | CCM_Incoming | CCM_Incoming |  |
| CM.RAMLAN.CA | SMS Management Point | CAN | CCM_STS | CCM_STS |  |
| CM.RAMLAN.CA | SMS Management Point | CAN | CCM_System | CCM_System |  |
| CM.RAMLAN.CA | SMS Management Point | CAN | CCM_System_AltAuth | CCM_System_AltAuth |  |
| CM.RAMLAN.CA | SMS Management Point | CAN | CMUserService | CMUserService |  |
| CM.RAMLAN.CA | SMS Management Point | CAN | SMS_MP | SMS_MP |  |
| CM.RAMLAN.CA | SMS Management Point | CAN | SMS_MP_AltAuth | SMS_MP_AltAuth |  |
| CM.RAMLAN.CA | SMS Software Update Point | CAN | ClientWebService | ClientWebService |  |
| CM.RAMLAN.CA | SMS Software Update Point | CAN | SimpleAuthWebService | SimpleAuthWebService |  |

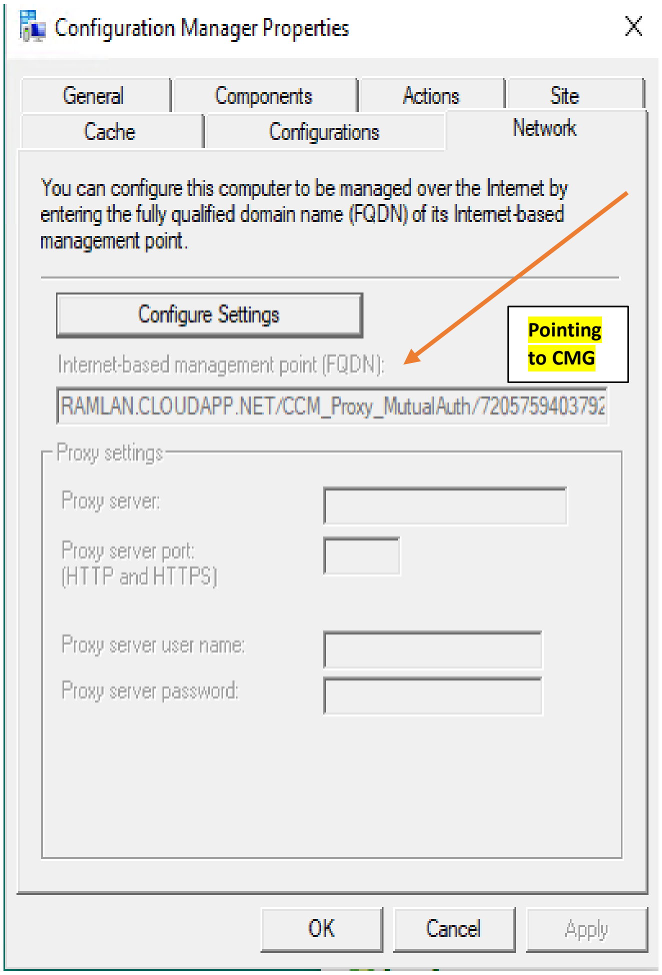
Now we will check client connection type



View and configure the client properties for System Center Configuration Manager.

Client properties:

| Property | Value |
|---|---|
| Assigned management point: | CM.RAMLAN.CA |
| Client certificate: | PKI |
| Connection Type: | Currently intranet |
| Site code: | SMS:CAN |
| Unique identifier: | GUID:3F690942-5531-40D4-999D-D30. |
| Version: | 5.00.8577.1003 |



You can configure this computer to be managed over the Internet by entering the fully qualified domain name (FQDN) of its Internet-based management point.

Internet-based management point (FQDN): RAMLAN.CLOUDAPP.NET/CCM_Proxy_MutualAuth/7205759403792

Proxy settings

Proxy server:

Proxy server port: (HTTP and HTTPS)

Proxy server user name:

Proxy server password:

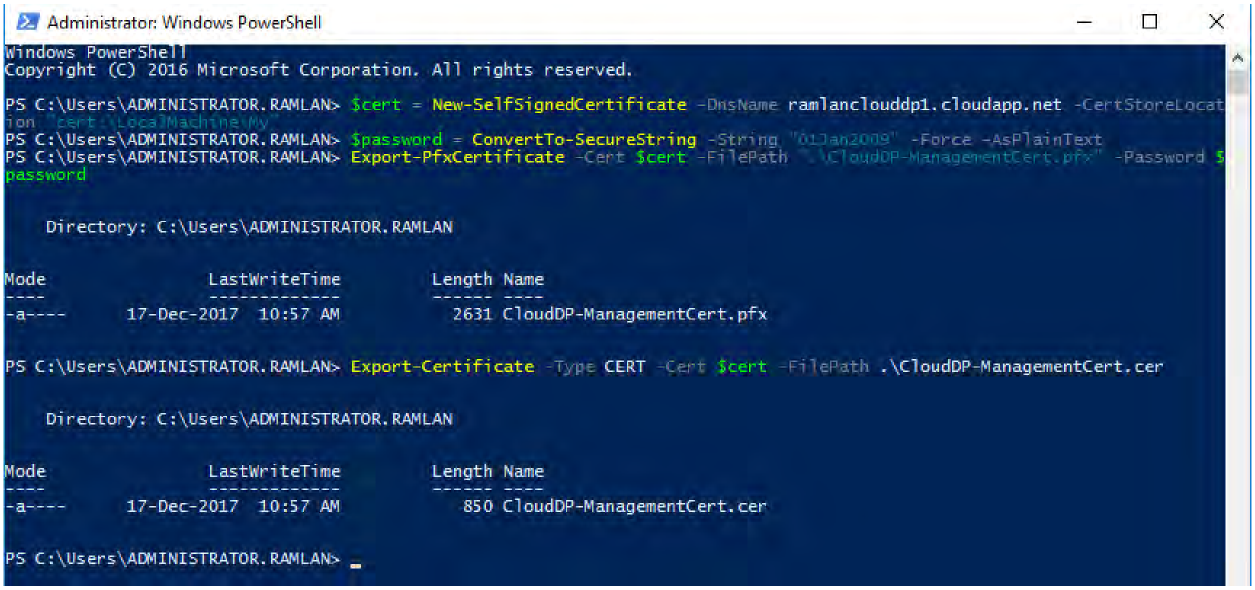
Pointing to CMG

# CLOUD DISTRIBUTION POINT PROCESS

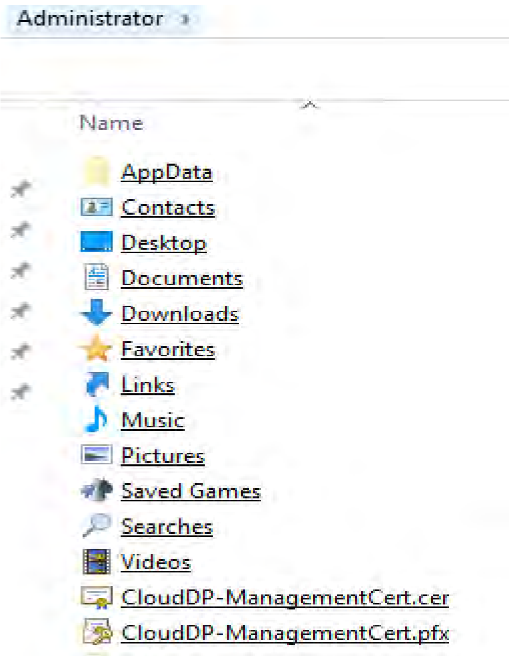
First we have to create certificates (**Management & Web Server**) for Cloud DP's. For Cloud DP – Management Certificate, I am going to use PowerShell command to generate.

**POWERSHELL COMMAND**: Please Open PowerShell as Administrator

1. $cert = New-SelfSignedCertificate -DnsName ramlanclouddp1.cloudapp.net -CertStoreLocation "cert:\LocalMachine\My"
2. $password = ConvertTo-SecureString -String "01Jan2009" -Force –AsPlainText
3. Export-PfxCertificate -Cert $cert -FilePath ".\CloudDP-ManagementCert.pfx" -Password $password
4. Export-Certificate -Type CERT -Cert $cert -FilePath .\CloudDP-ManagementCert.cer
5. `PS C:\Users\Administrator>` - At this location you will see both the certificates



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\ADMINISTRATOR.RAMLAN> $cert = New-SelfSignedCertificate -DnsName ramlanclouddp1.cloudapp.net -CertStoreLocat
ion "cert:\LocalMachine\My"
PS C:\Users\ADMINISTRATOR.RAMLAN> $password = ConvertTo-SecureString -String "01Jan2009" -Force -AsPlainText
PS C:\Users\ADMINISTRATOR.RAMLAN> Export-PfxCertificate -Cert $cert -FilePath ".\CloudDP-ManagementCert.pfx" -Password $
password


    Directory: C:\Users\ADMINISTRATOR.RAMLAN


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----      17-Dec-2017  10:57 AM           2631 CloudDP-ManagementCert.pfx


PS C:\Users\ADMINISTRATOR.RAMLAN> Export-Certificate -Type CERT -Cert $cert -FilePath .\CloudDP-ManagementCert.cer


    Directory: C:\Users\ADMINISTRATOR.RAMLAN


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----      17-Dec-2017  10:57 AM            850 CloudDP-ManagementCert.cer


PS C:\Users\ADMINISTRATOR.RAMLAN> _
```

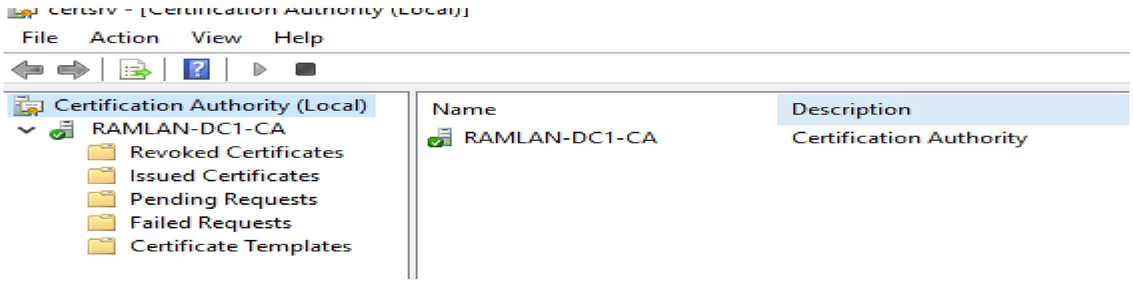


Name

- AppData
- Contacts
- Desktop
- Documents
- Downloads
- Favorites
- Links
- Music
- Pictures
- Saved Games
- Searches
- Videos
- CloudDP-ManagementCert.cer
- CloudDP-ManagementCert.pfx

**CLOUD DP WEB SERVER CERTIFICATE - REGULAR WAY – FROM CERTIFICATE AUTHORITY:**

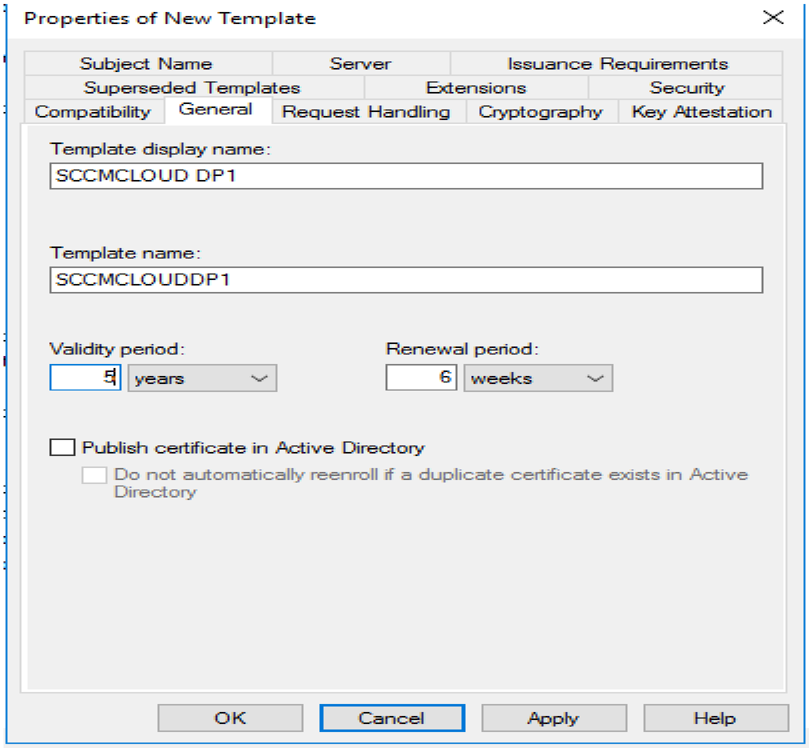
Open Certificate Authority from Administrative Tools



- Certification Authority (Local)
  - RAMLAN-DC1-CA
    - Revoked Certificates
    - Issued Certificates
    - Pending Requests
    - Failed Requests
    - Certificate Templates

| Name | Description |
|---|---|
| RAMLAN-DC1-CA | Certification Authority |

Right Click Certificate Templates – Manage - Right Click Web Server – Duplicate Template



Template display name: SCCMCLOUD DP1

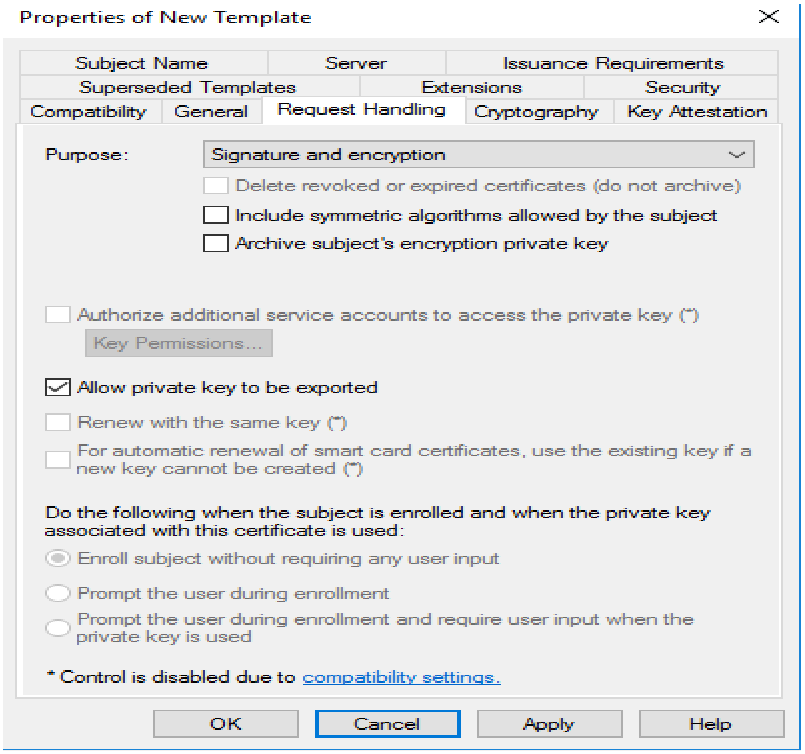
Template name: SCCMCLOUDDP1

Validity period: 5 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory



Purpose: Signature and encryption

□ Delete revoked or expired certificates (do not archive)

□ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

□ Authorize additional service accounts to access the private key (*)

☑ Allow private key to be exported

□ Renew with the same key (*)

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

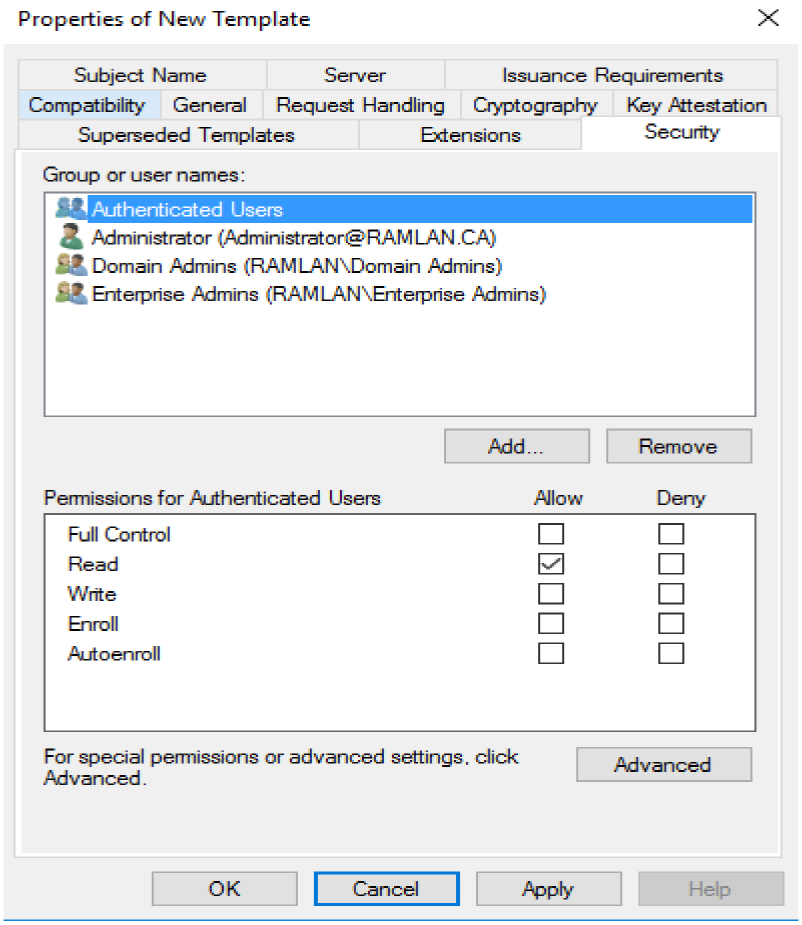
Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to compatibility settings.

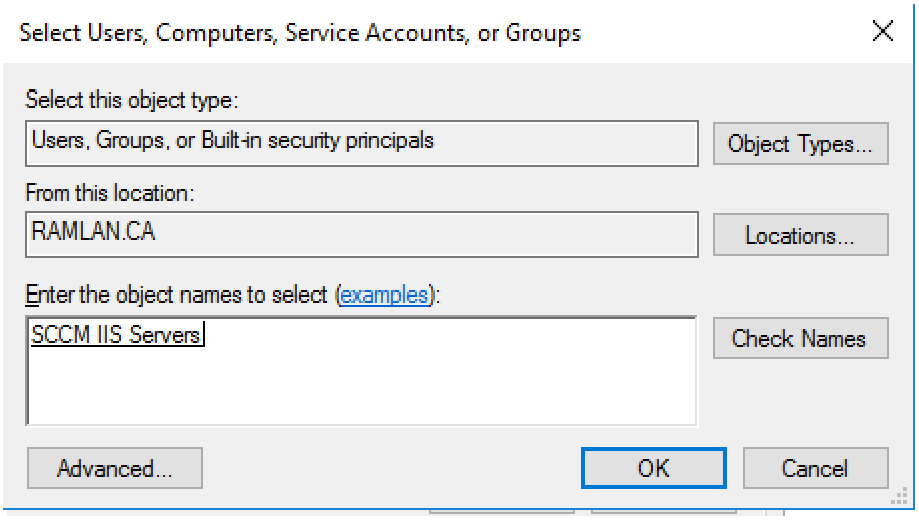


Group or user names:

- Authenticated Users
- Administrator (Administrator@RAMLAN.CA)
- Domain Admins (RAMLAN\Domain Admins)
- Enterprise Admins (RAMLAN\Enterprise Admins)

| Permissions for Authenticated Users | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Read | ☑ | □ |
| Write | □ | □ |
| Enroll | □ | □ |
| Autoenroll | □ | □ |

For special permissions or advanced settings, click Advanced.

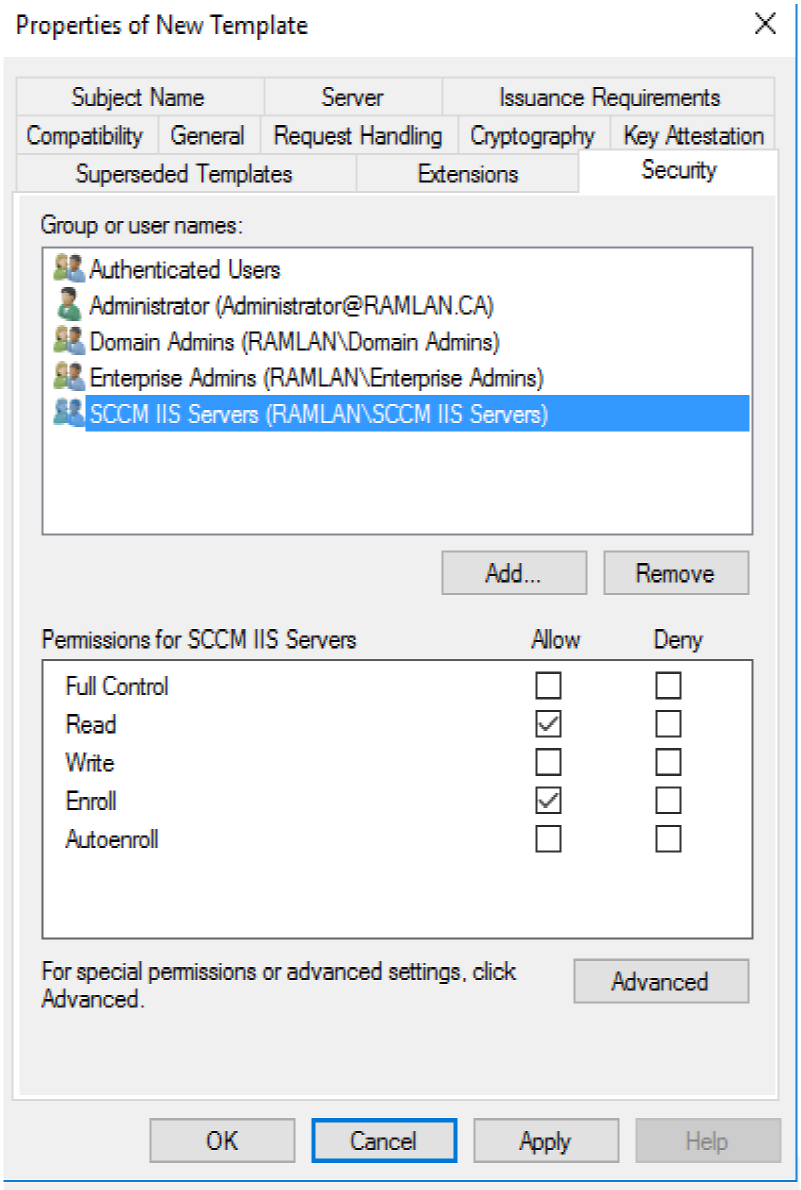


Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
RAMLAN.CA

Enter the object names to select (examples):
SCCM IIS Servers



Properties of New Template

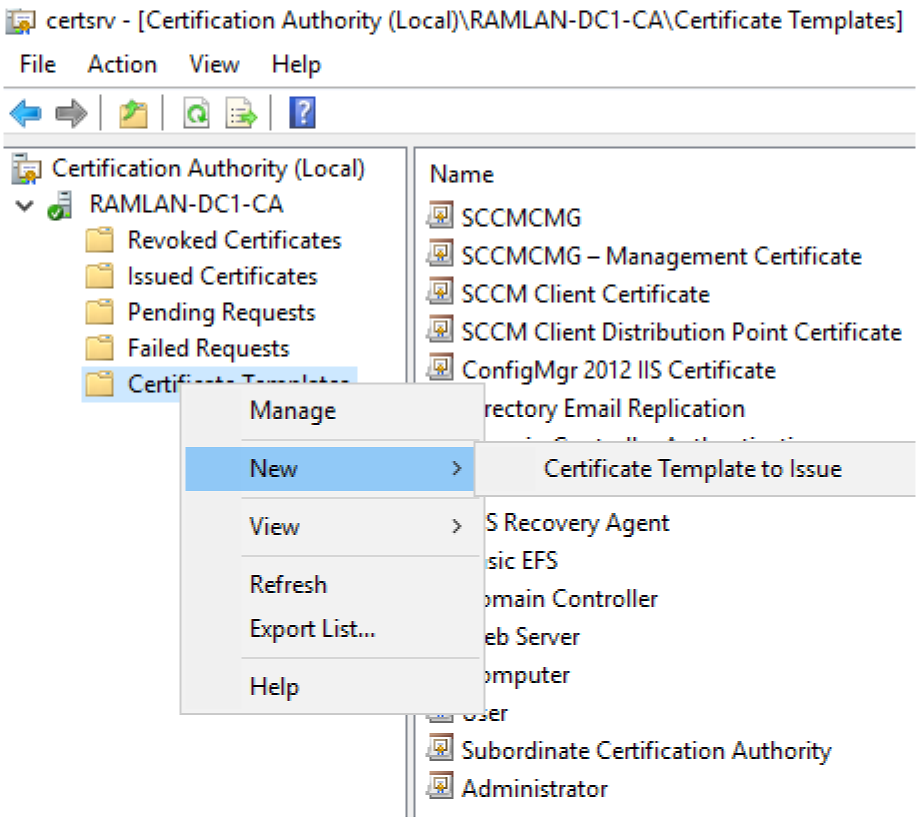
Group or user names:

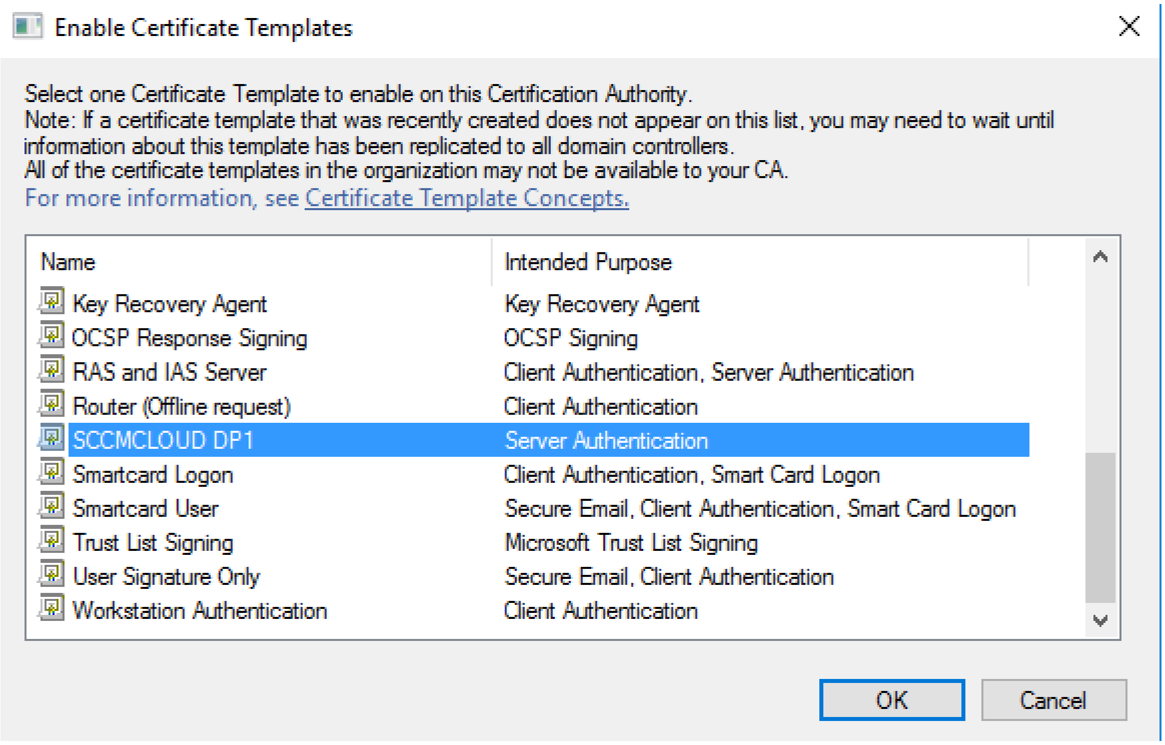
- Authenticated Users
- Administrator (Administrator@RAMLAN.CA)
- Domain Admins (RAMLAN\Domain Admins)
- Enterprise Admins (RAMLAN\Enterprise Admins)
- SCCM IIS Servers (RAMLAN\SCCM IIS Servers)

| Permissions for SCCM IIS Servers | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Read | ☑ | □ |
| Write | □ | □ |
| Enroll | ☑ | □ |
| Autoenroll | □ | □ |

For special permissions or advanced settings, click Advanced.

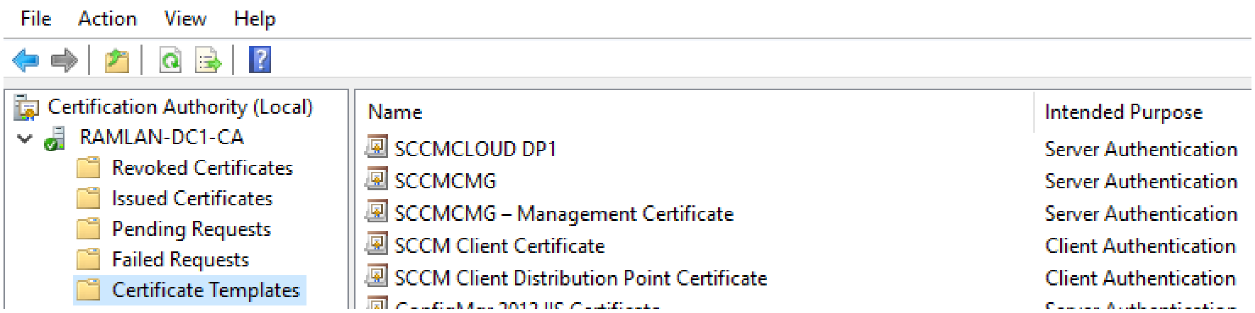
Now we have to issue the template certificate we created.


certsrv - [Certification Authority (Local)\RAMLAN-DC1-CA\Certificate Templates]
File
Action
View
Help
Certification Authority (Local)
RAMLAN-DC1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Manage
New
View
Refresh
Export List...
Help
Certificate Template to Issue
Name
SCCMCMG
SCCMCMG – Management Certificate
SCCM Client Certificate
SCCM Client Distribution Point Certificate
ConfigMgr 2012 IIS Certificate
rectory Email Replication
S Recovery Agent
sic EFS
omain Controller
eb Server
omputer
User
Subordinate Certification Authority
Administrator



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.

| Name | Intended Purpose |
|---|---|
| Key Recovery Agent | Key Recovery Agent |
| OCSP Response Signing | OCSP Signing |
| RAS and IAS Server | Client Authentication, Server Authentication |
| Router (Offline request) | Client Authentication |
| SCCMCLOUD DP1 | Server Authentication |
| Smartcard Logon | Client Authentication, Smart Card Logon |
| Smartcard User | Secure Email, Client Authentication, Smart Card Logon |
| Trust List Signing | Microsoft Trust List Signing |
| User Signature Only | Secure Email, Client Authentication |
| Workstation Authentication | Client Authentication |



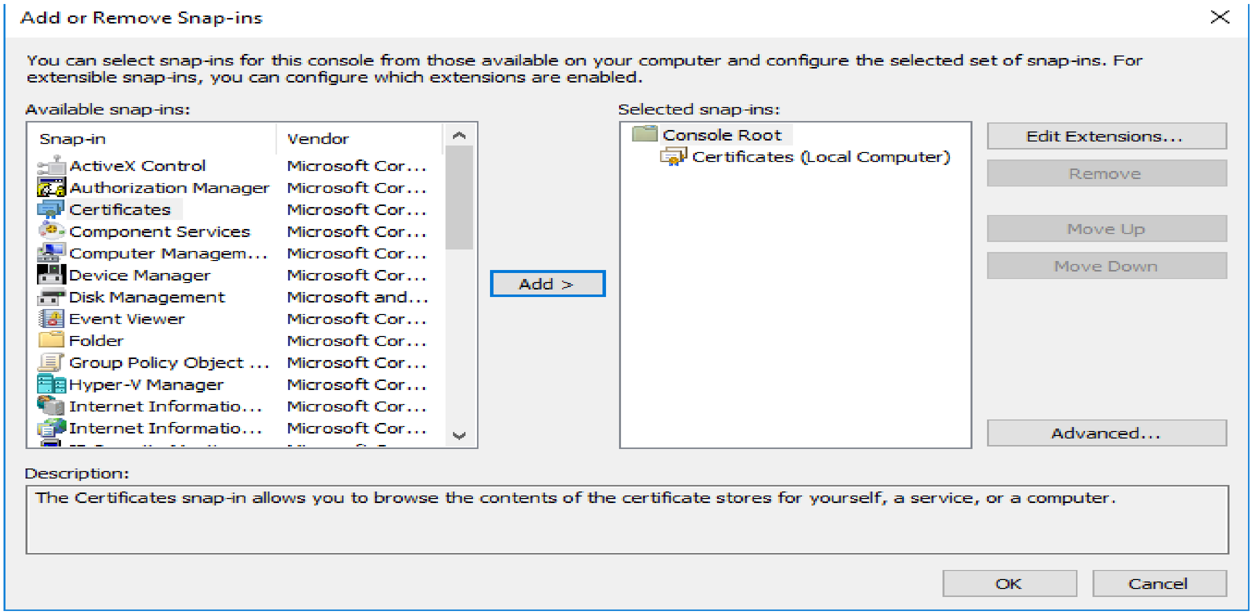
- Certification Authority (Local)
  - RAMLAN-DC1-CA
    - Revoked Certificates
    - Issued Certificates
    - Pending Requests
    - Failed Requests
    - Certificate Templates

| Name | Intended Purpose |
|---|---|
| SCCMCLOUD DP1 | Server Authentication |
| SCCMCMG | Server Authentication |
| SCCMCMG – Management Certificate | Server Authentication |
| SCCM Client Certificate | Client Authentication |
| SCCM Client Distribution Point Certificate | Client Authentication |
| ConfigMgr 2012 IIS Certificate | Server Authentication |

Now we have to request the certificate.  This will be done on my SCCM Server (CM.RAMLAN.CA)

Start – Run – MMC - File – Add/Remove Snap-in

Select Certificates – Add – Computer Account – Local Computer - OK


Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

| Snap-in | Vendor |
|---|---|
| ActiveX Control | Microsoft Cor... |
| Authorization Manager | Microsoft Cor... |
| Certificates | Microsoft Cor... |
| Component Services | Microsoft Cor... |
| Computer Managem... | Microsoft Cor... |
| Device Manager | Microsoft Cor... |
| Disk Management | Microsoft and... |
| Event Viewer | Microsoft Cor... |
| Folder | Microsoft Cor... |
| Group Policy Object ... | Microsoft Cor... |
| Hyper-V Manager | Microsoft Cor... |
| Internet Informatio... | Microsoft Cor... |
| Internet Informatio... | Microsoft Cor... |

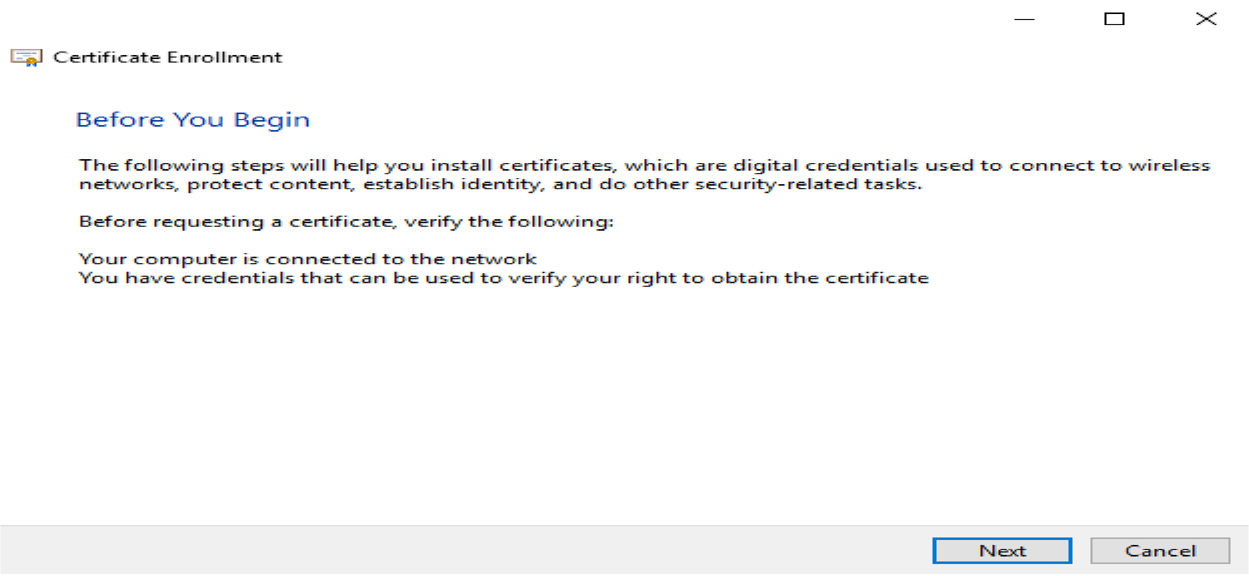
Selected snap-ins:

- Console Root
  - Certificates (Local Computer)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Click – Personal – Right Click Certificates – All Task – Request New Certificate

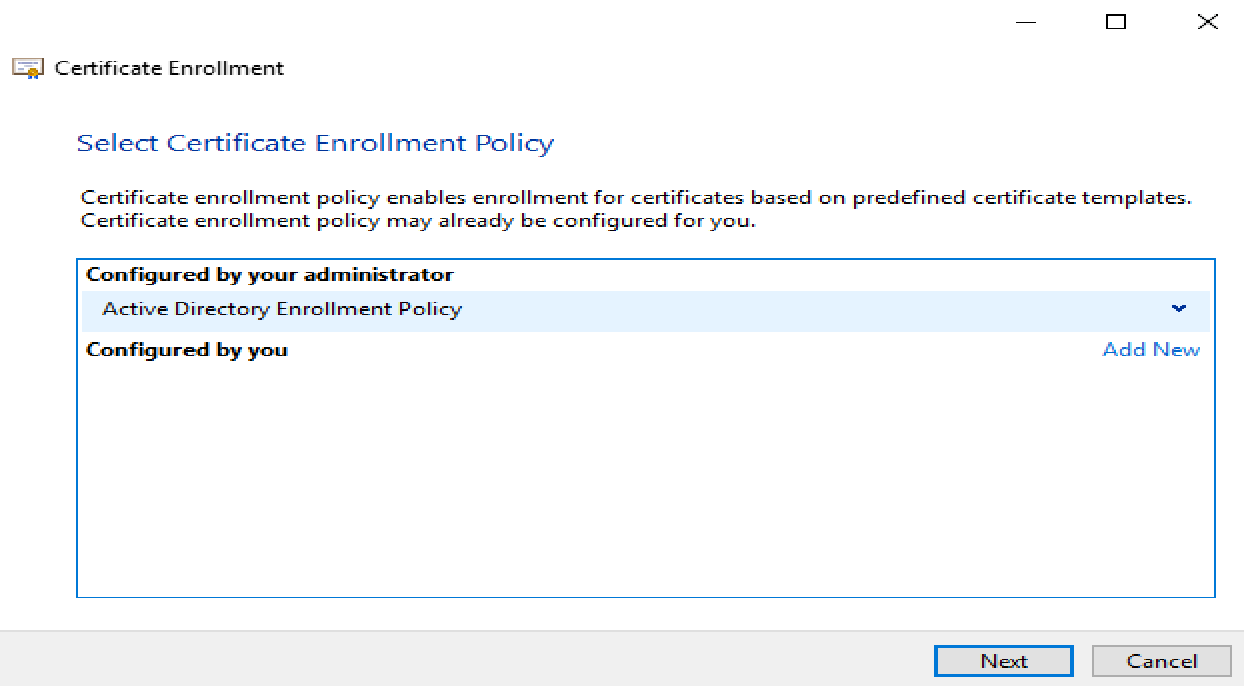

Certificate Enrollment

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



Certificate Enrollment

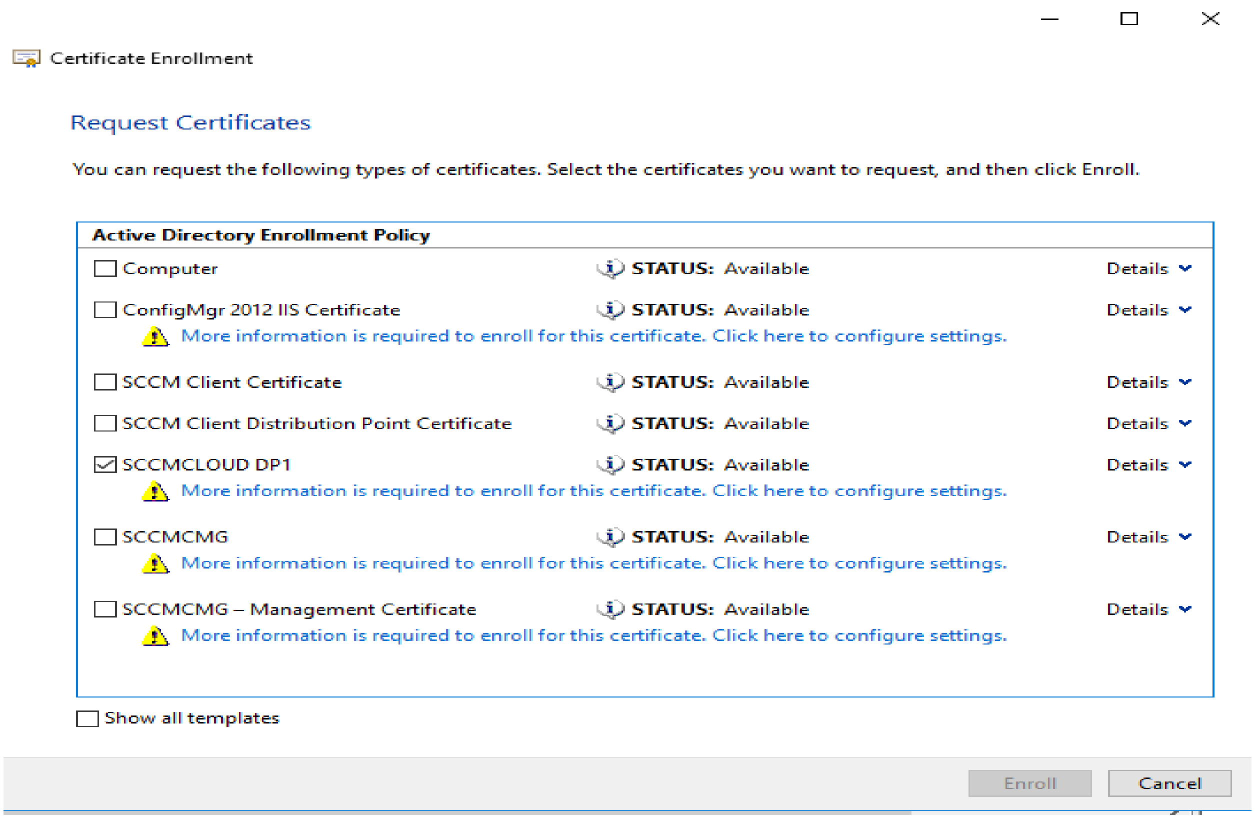
Select Certificate Enrollment Policy

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**



Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

**Active Directory Enrollment Policy**

☐ Computer — **STATUS:** Available — Details

☐ ConfigMgr 2012 IIS Certificate — **STATUS:** Available — Details
⚠ More information is required to enroll for this certificate. Click here to configure settings.

☐ SCCM Client Certificate — **STATUS:** Available — Details

☐ SCCM Client Distribution Point Certificate — **STATUS:** Available — Details

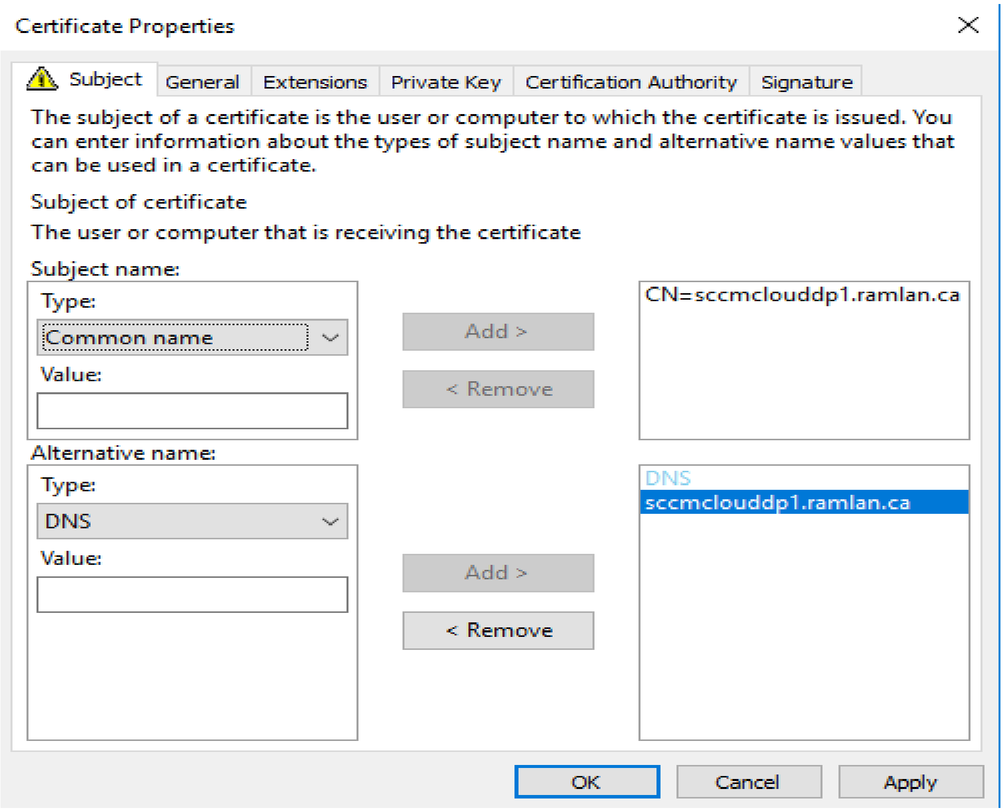
☑ SCCMCLOUD DP1 — **STATUS:** Available — Details
⚠ More information is required to enroll for this certificate. Click here to configure settings.

☐ SCCMCMG — **STATUS:** Available — Details
⚠ More information is required to enroll for this certificate. Click here to configure settings.

☐ SCCMCMG – Management Certificate — **STATUS:** Available — Details
⚠ More information is required to enroll for this certificate. Click here to configure settings.

☐ Show all templates

Click More


Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Common name

Value:

CN=sccmclouddp1.ramlan.ca

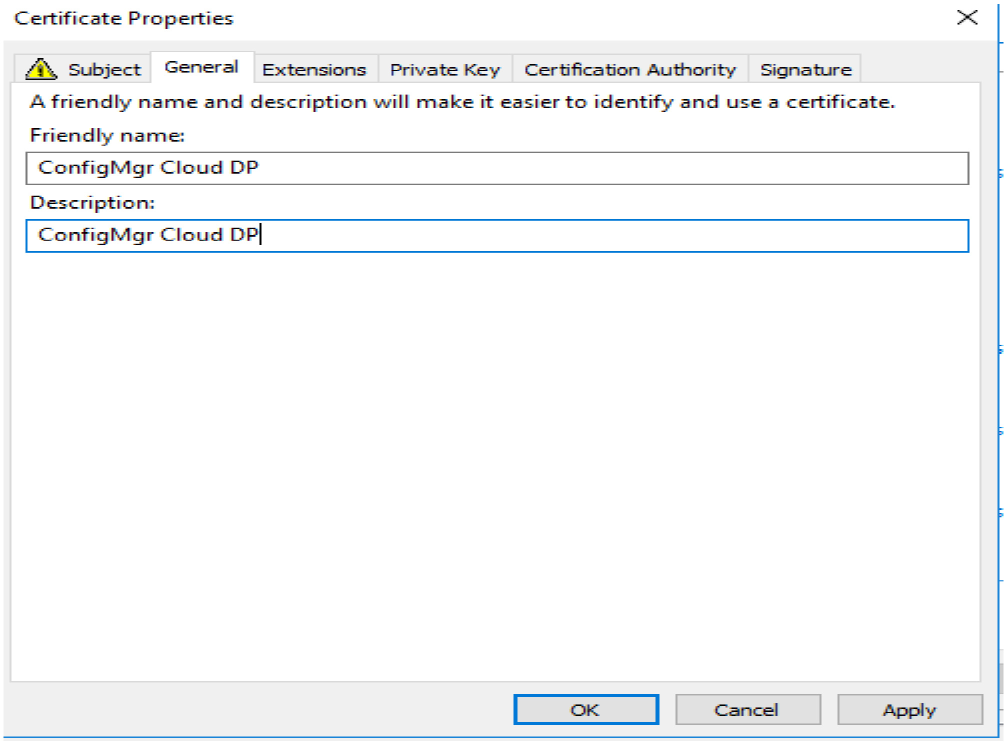
Alternative name:

Type: DNS

Value:

DNS

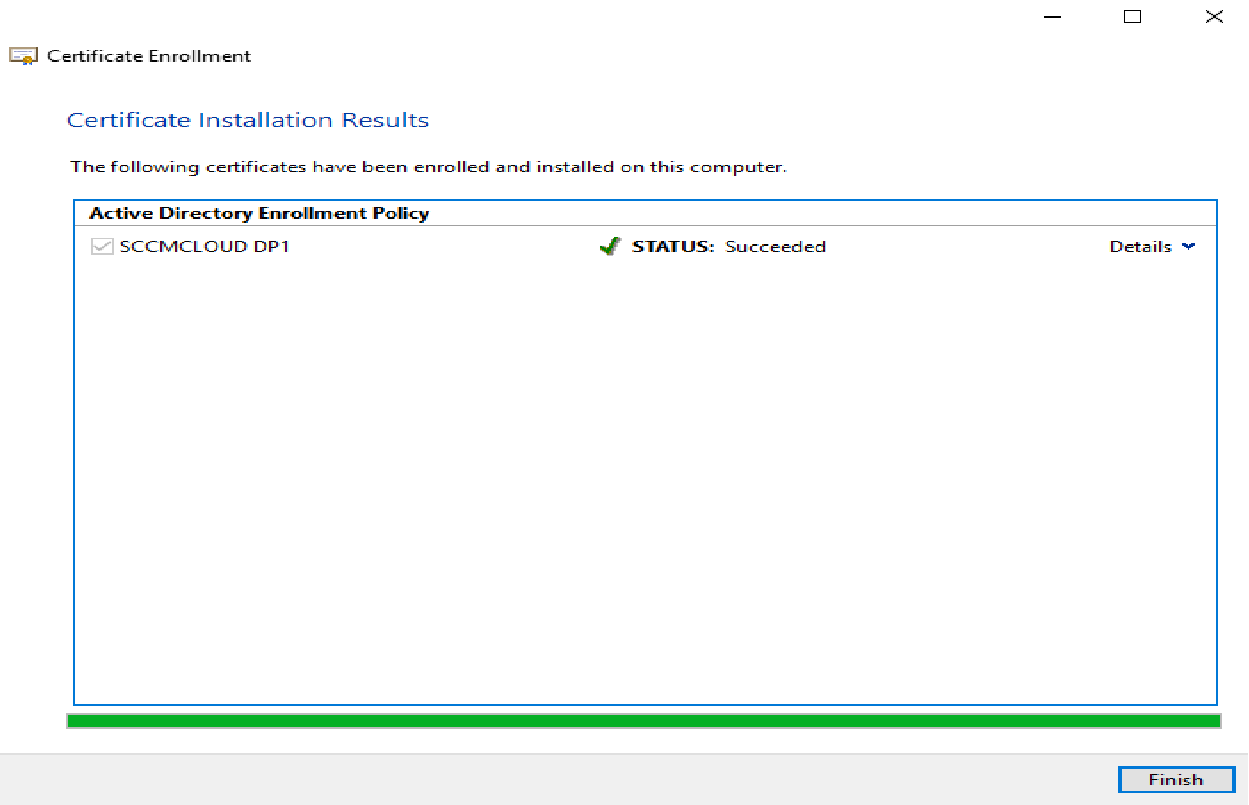
sccmclouddp1.ramlan.ca


Certificate Properties

A friendly name and description will make it easier to identify and use a certificate.

Friendly name: ConfigMgr Cloud DP

Description: ConfigMgr Cloud DP



Certificate Enrollment

Certificate Installation Results

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

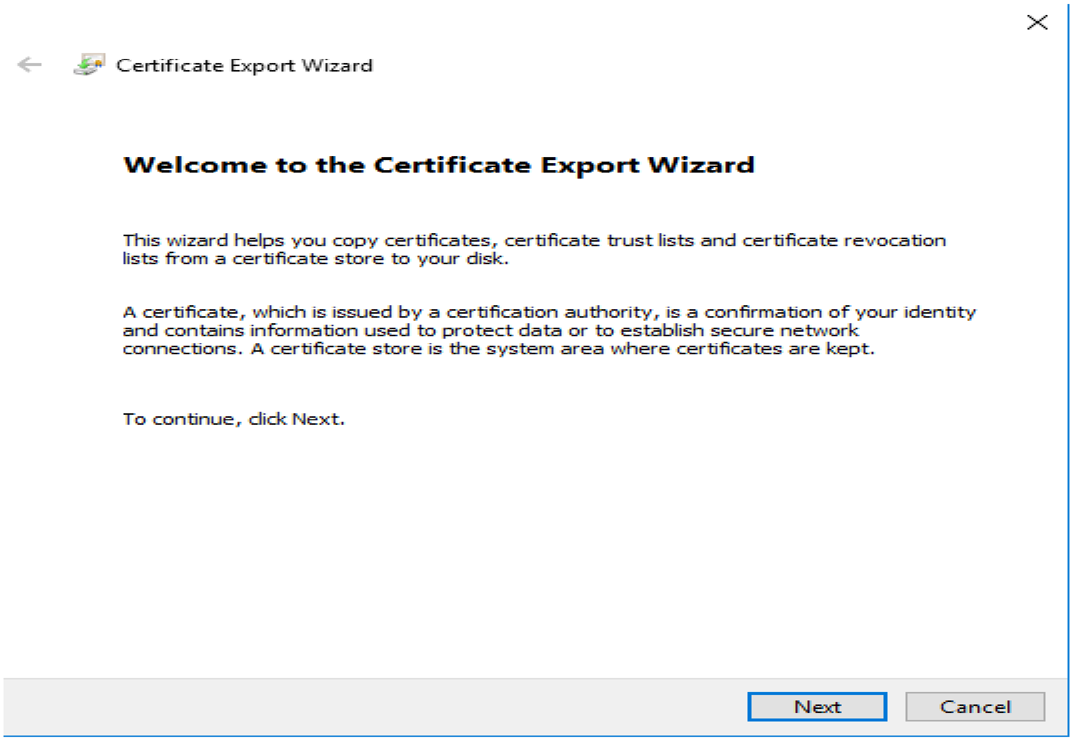
**Active Directory Enrollment Policy**

☑ SCCMCLOUD DP1 ✓ **STATUS:** Succeeded Details

Now we have to export the certificate.

**Without Private Key: Web Server**

Certificates – Right Click sccmclouddp1 – All Tasks – Export



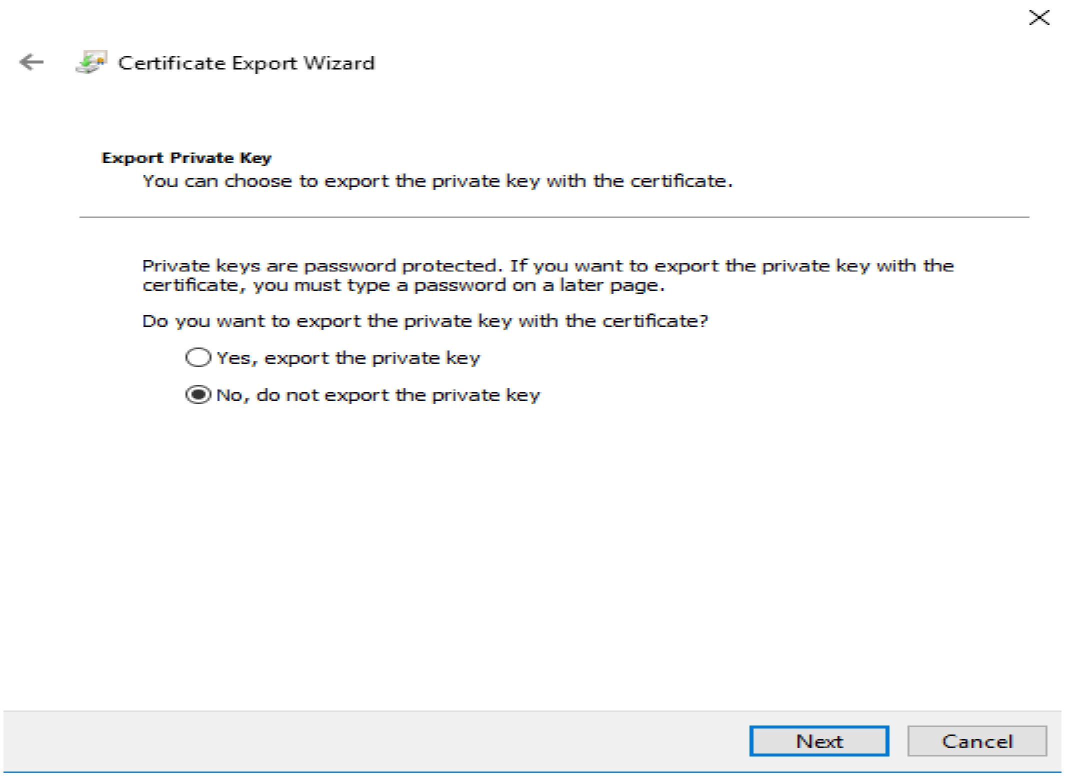
Certificate Export Wizard

**Welcome to the Certificate Export Wizard**

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.



Certificate Export Wizard

**Export Private Key**

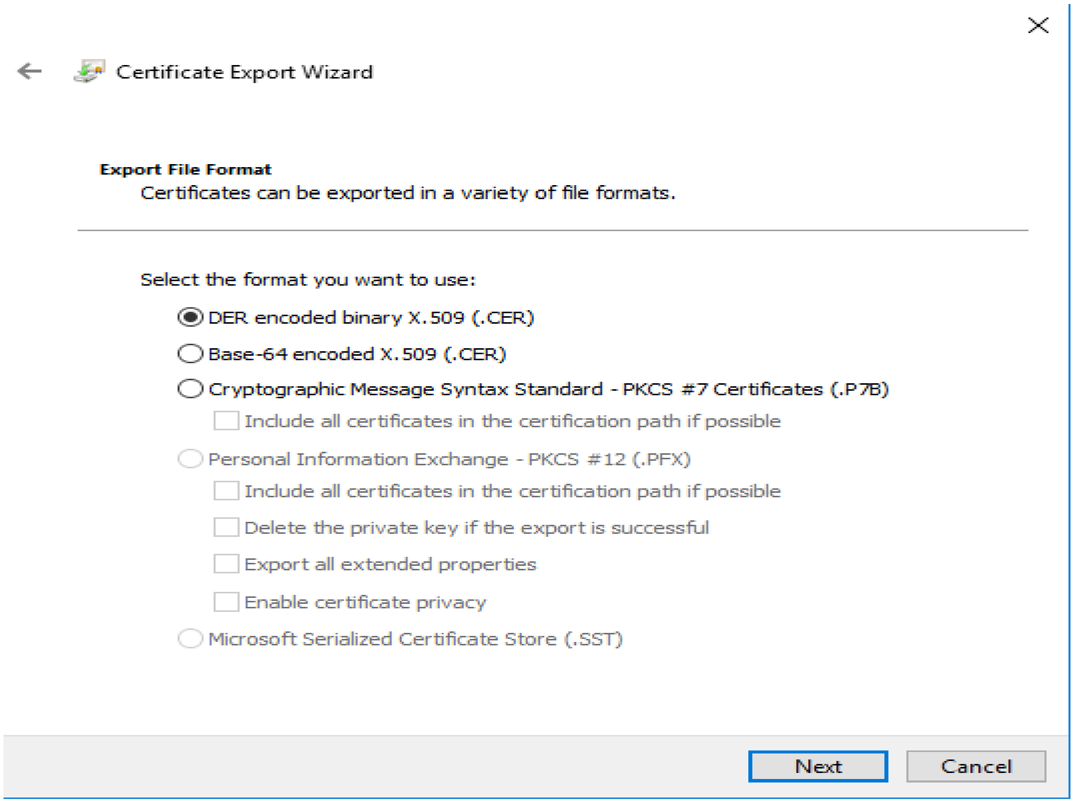
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key



Certificate Export Wizard

**Export File Format**

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

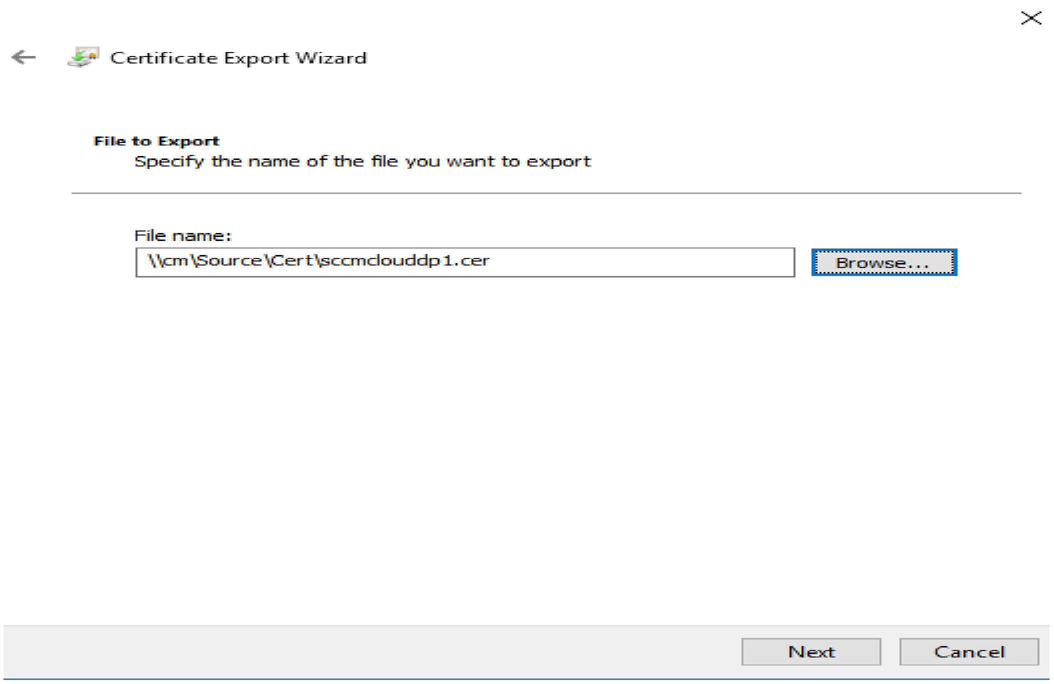
□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

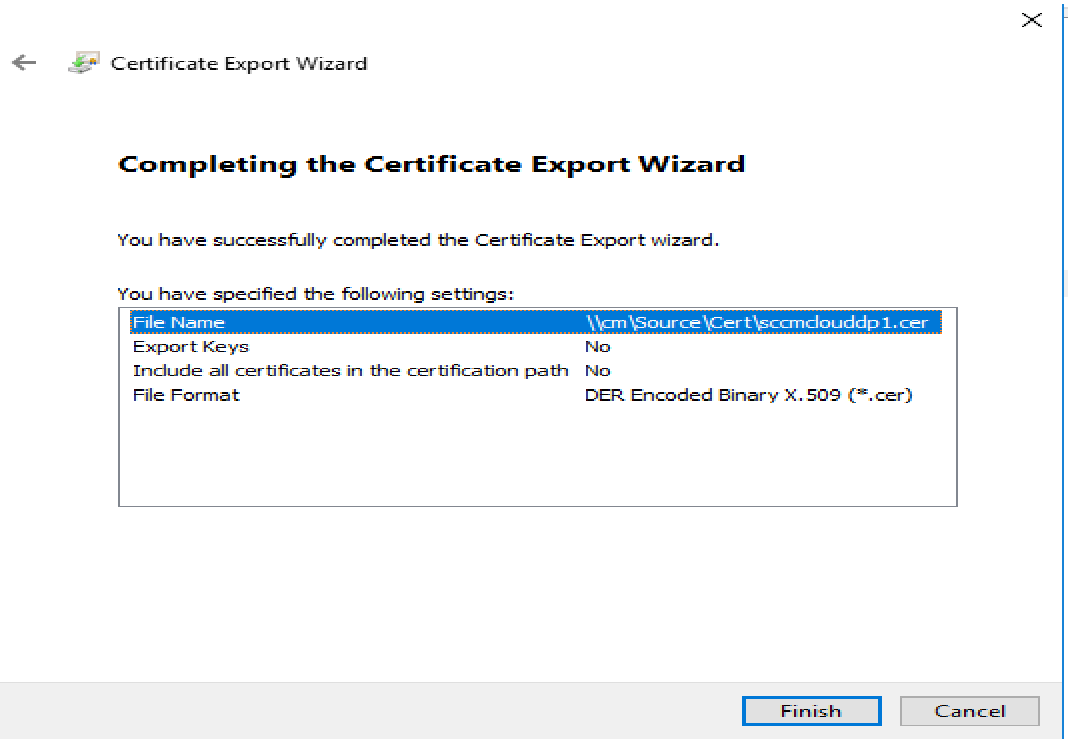
○ Microsoft Serialized Certificate Store (.SST)



Certificate Export Wizard

**File to Export**
Specify the name of the file you want to export

File name:
\\cm\Source\Cert\sccmclouddp1.cer



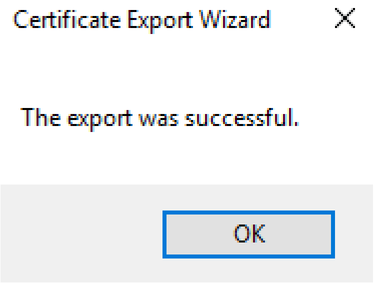
Certificate Export Wizard

**Completing the Certificate Export Wizard**

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

| | |
|---|---|
| File Name | \\cm\Source\Cert\sccmclouddp1.cer |
| Export Keys | No |
| Include all certificates in the certification path | No |
| File Format | DER Encoded Binary X.509 (*.cer) |

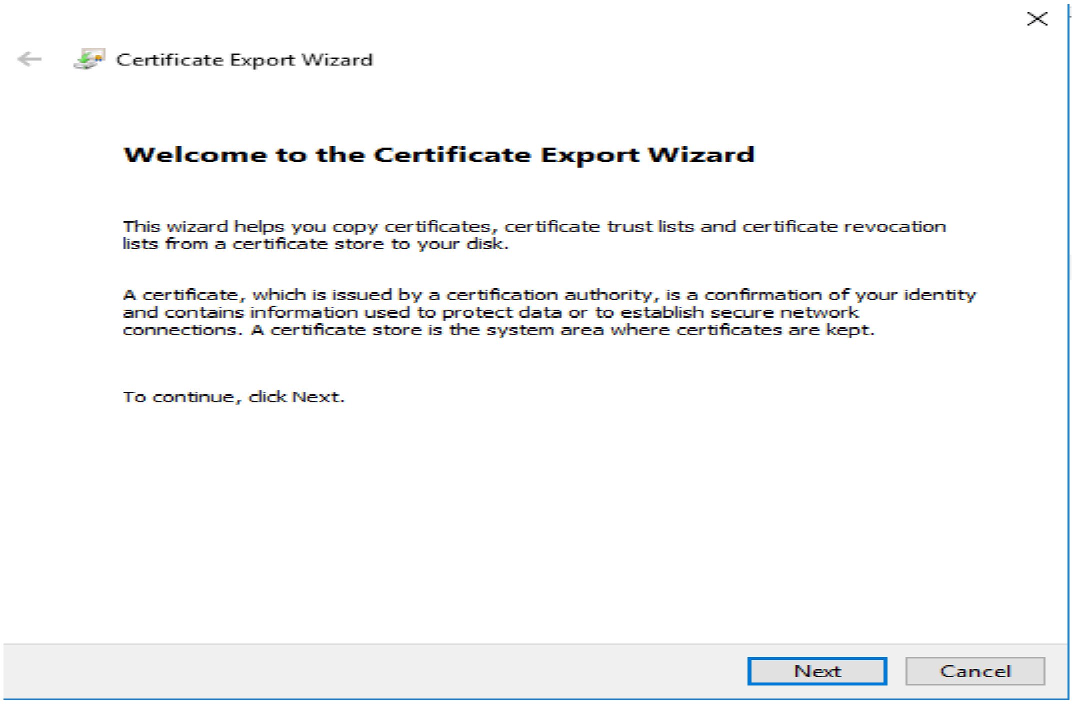


Certificate Export Wizard

The export was successful.

**With Private Key: Web Server**

Certificates – Right Click sccmclouddp1 – All Tasks – Export

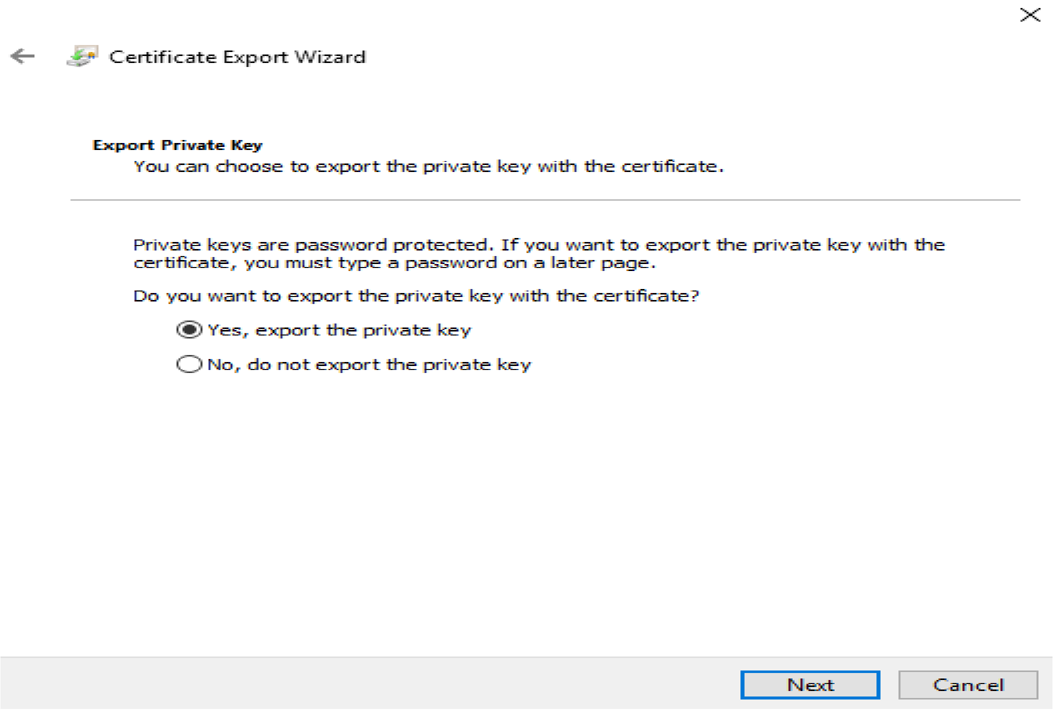


**Welcome to the Certificate Export Wizard**

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.



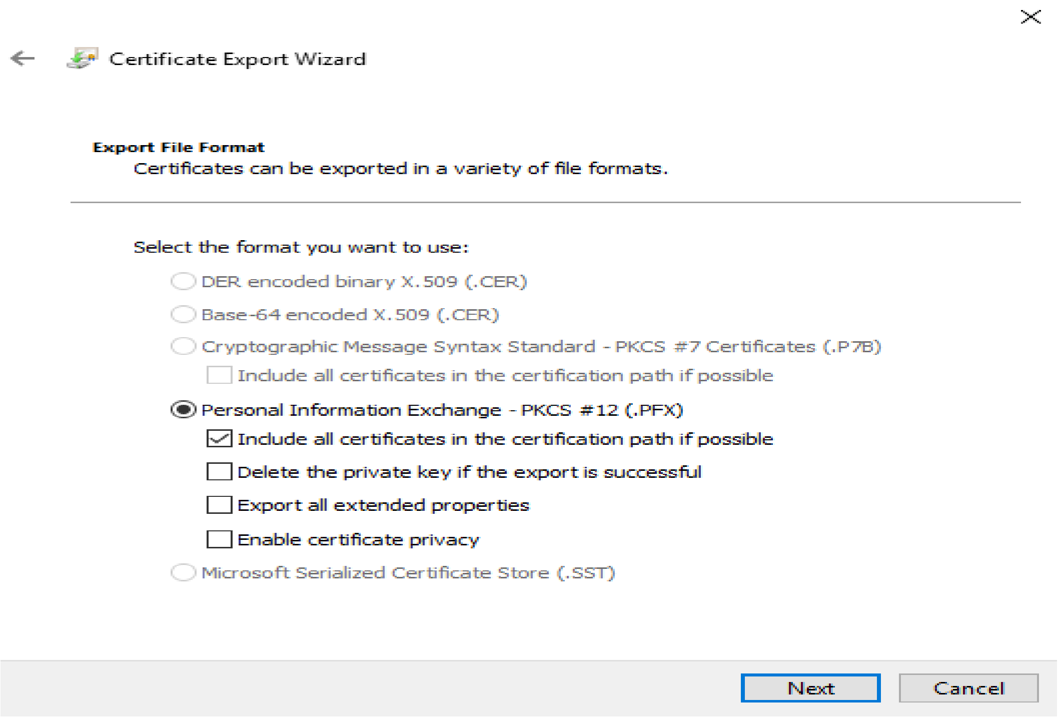
**Export Private Key**
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key



**Export File Format**

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

☐ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

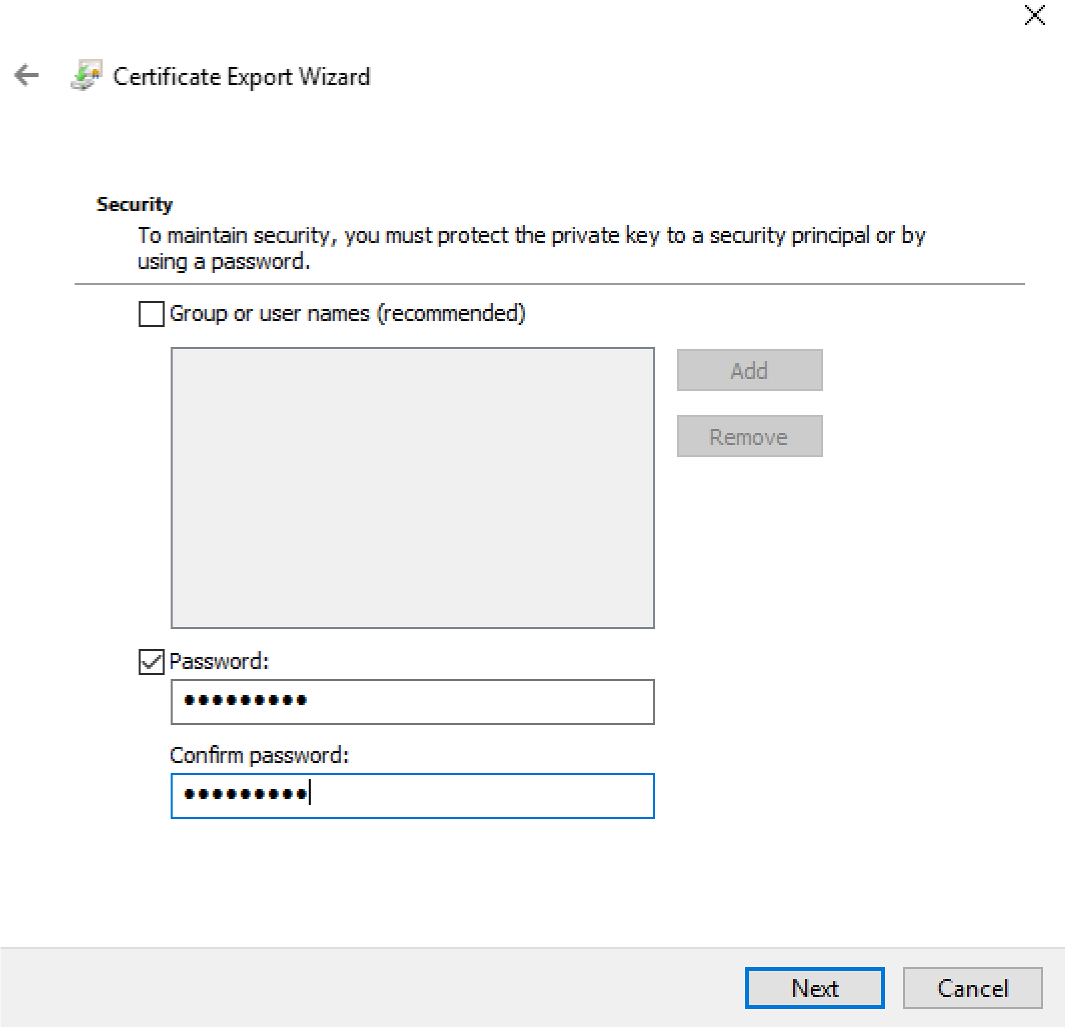
☑ Include all certificates in the certification path if possible

☐ Delete the private key if the export is successful

☐ Export all extended properties

☐ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)



**Security**

To maintain security, you must protect the private key to a security principal or by using a password.

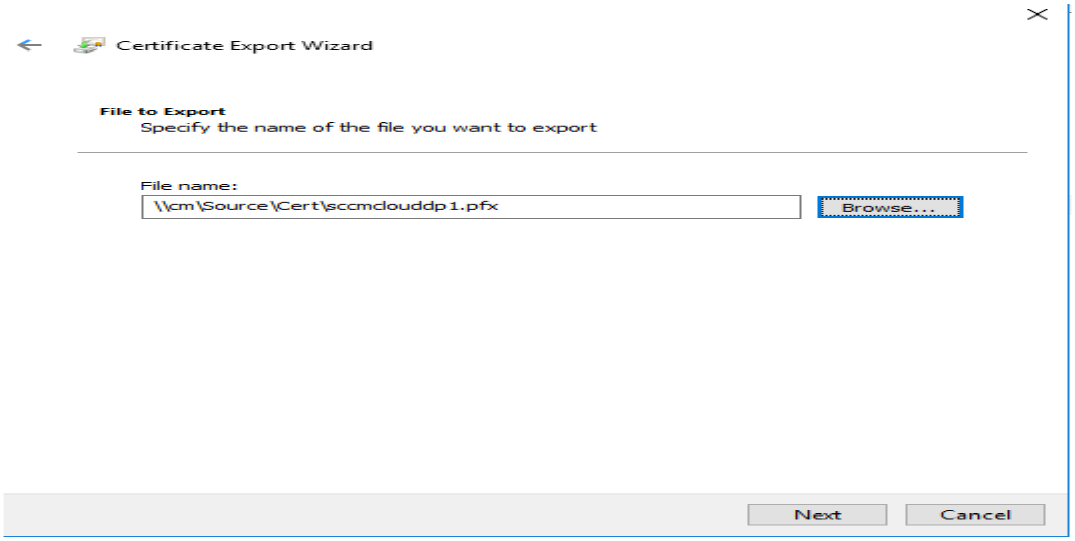
☐ Group or user names (recommended)

☑ Password:

●●●●●●●●●

Confirm password:

●●●●●●●●●



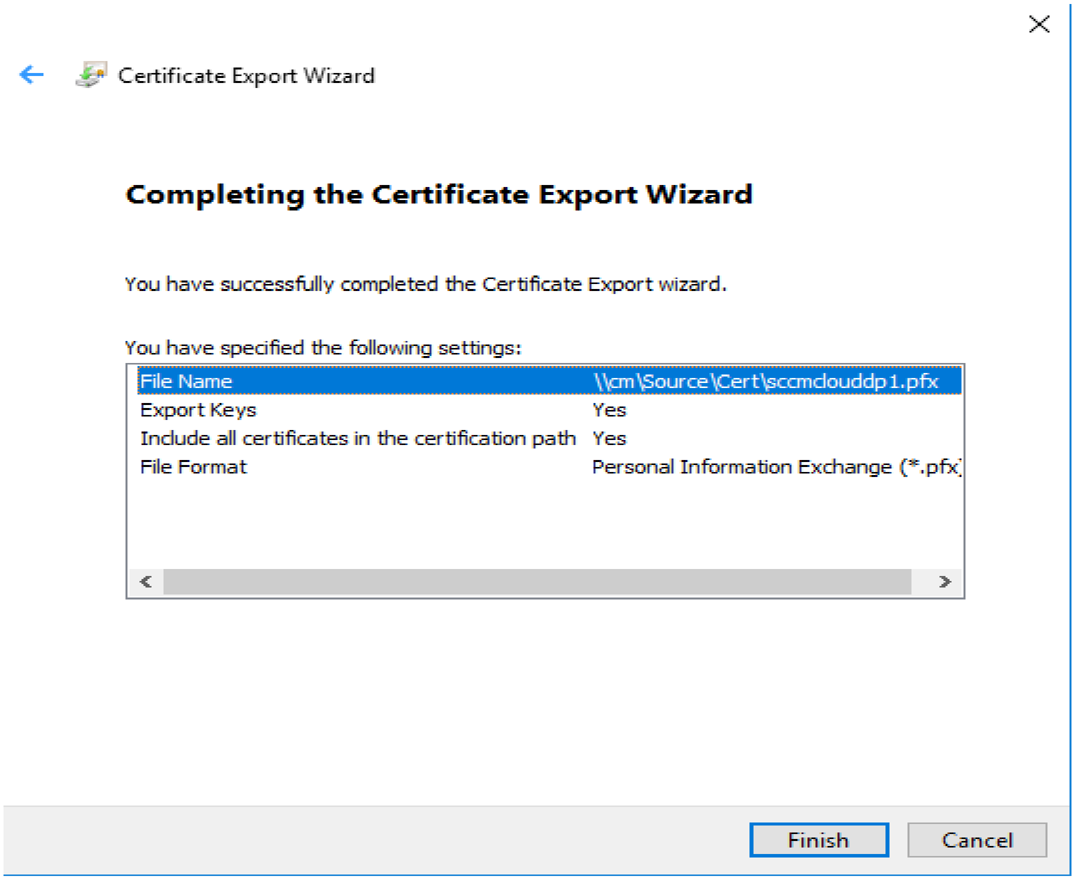
Certificate Export Wizard

**File to Export**

Specify the name of the file you want to export

File name:

\\cm\Source\Cert\sccmclouddp1.pfx



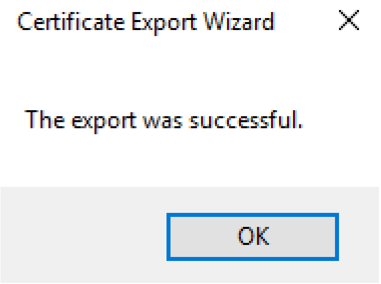
Certificate Export Wizard

## Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

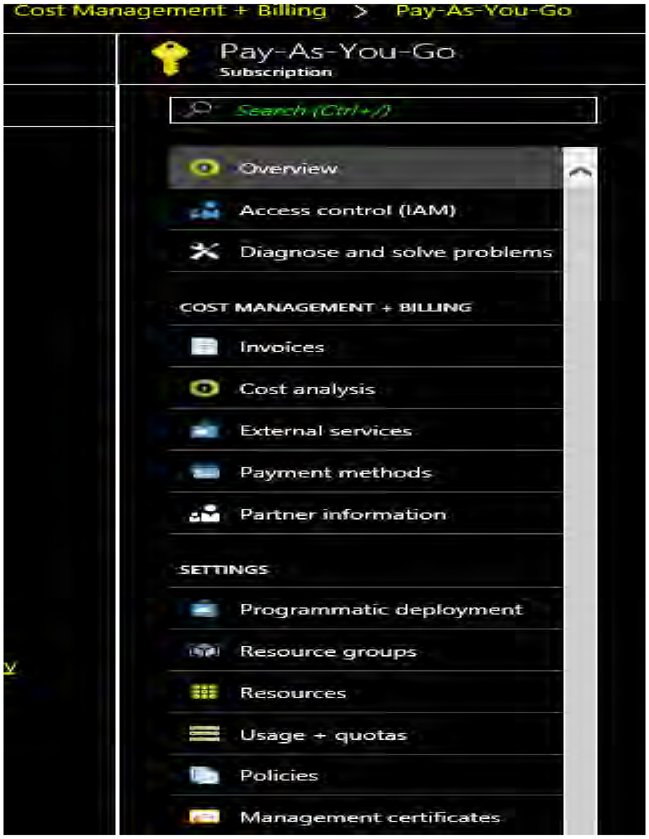
| | |
|---|---|
| File Name | \\cm\Source\Cert\sccmclouddp1.pfx |
| Export Keys | Yes |
| Include all certificates in the certification path | Yes |
| File Format | Personal Information Exchange (*.pfx) |



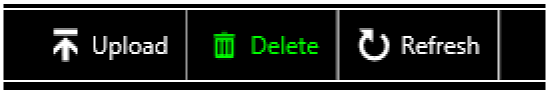
Certificate Export Wizard

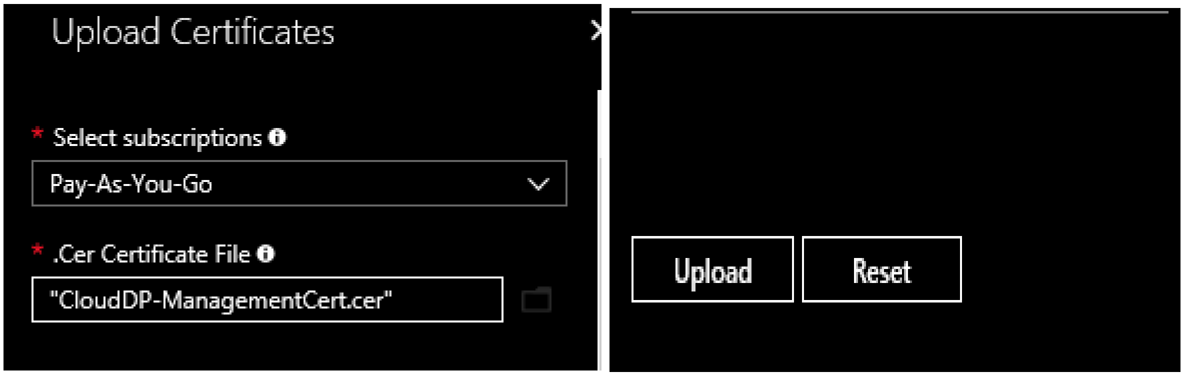
The export was successful.

Now we will upload Cloud DP Management Certificate in Azure



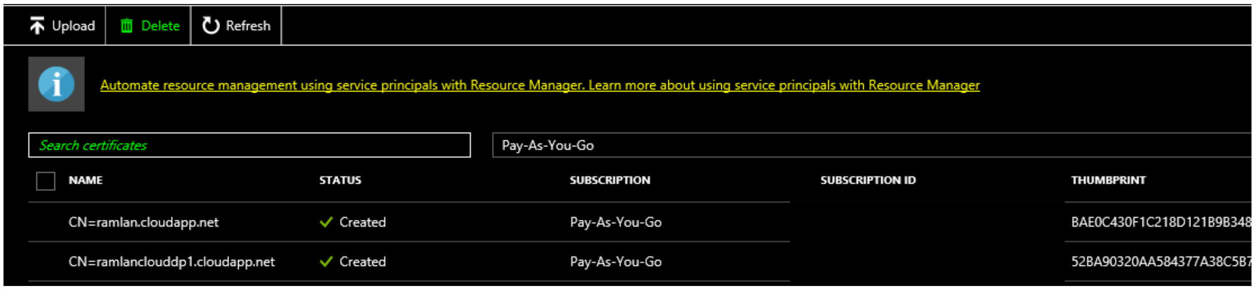
Click Management Certificates




Upload Certificates

* Select subscriptions: Pay-As-You-Go

* .Cer Certificate File: "CloudDP-ManagementCert.cer"



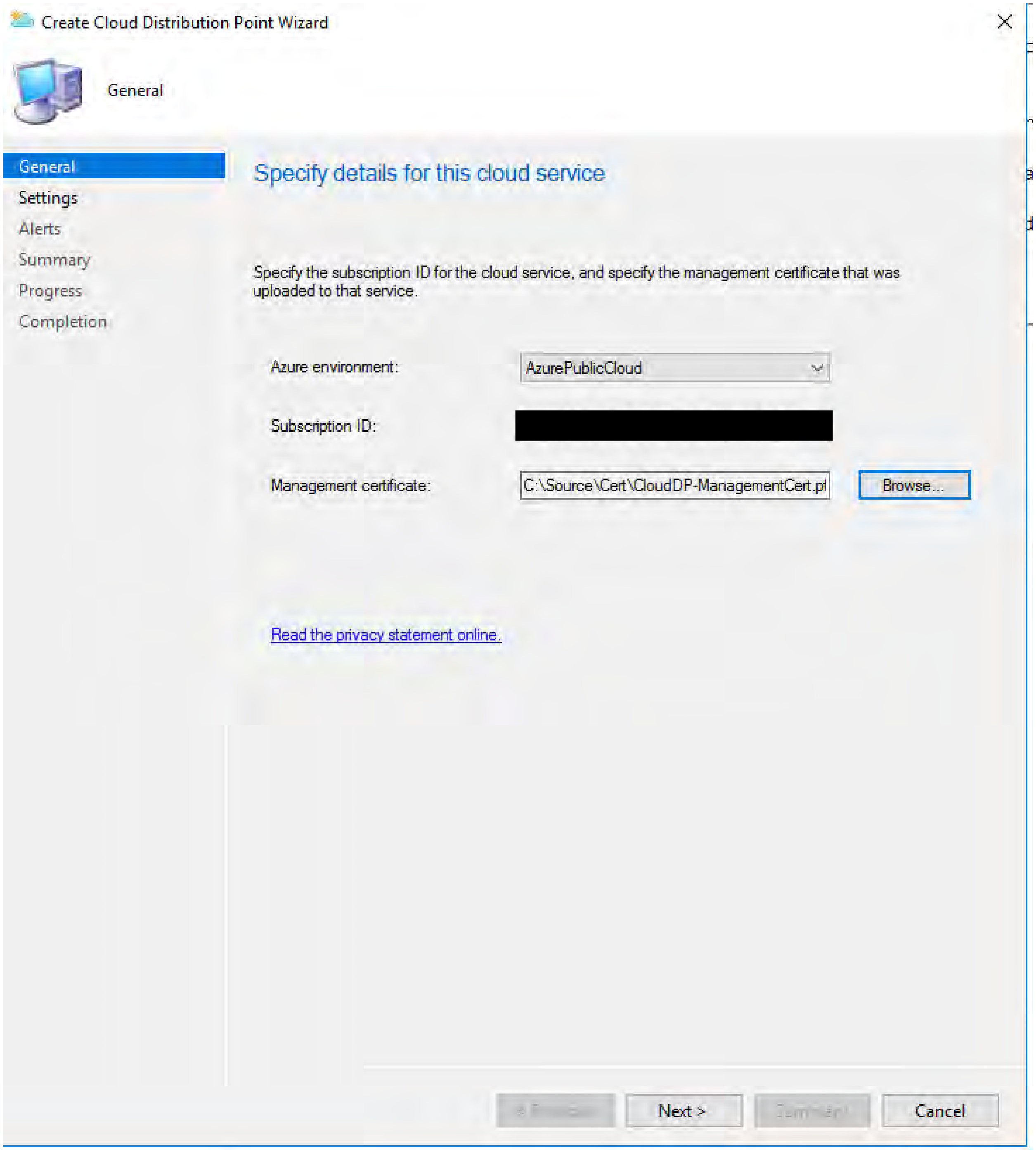
Automate resource management using service principals with Resource Manager. Learn more about using service principals with Resource Manager

Pay-As-You-Go

| NAME | STATUS | SUBSCRIPTION | SUBSCRIPTION ID | THUMBPRINT |
|---|---|---|---|---|
| CN=ramlan.cloudapp.net | ✓ Created | Pay-As-You-Go | [redacted] | BAE0C430F1C218D121B9B348 |
| CN=ramlanclouddp1.cloudapp.net | ✓ Created | Pay-As-You-Go | [redacted] | 52BA90320AA584377A38C5B7 |

Now we will install Cloud Distribution Point within CB1710

Administration – Cloud Services – Cloud DP – Create Cloud DP



Create Cloud Distribution Point Wizard

General

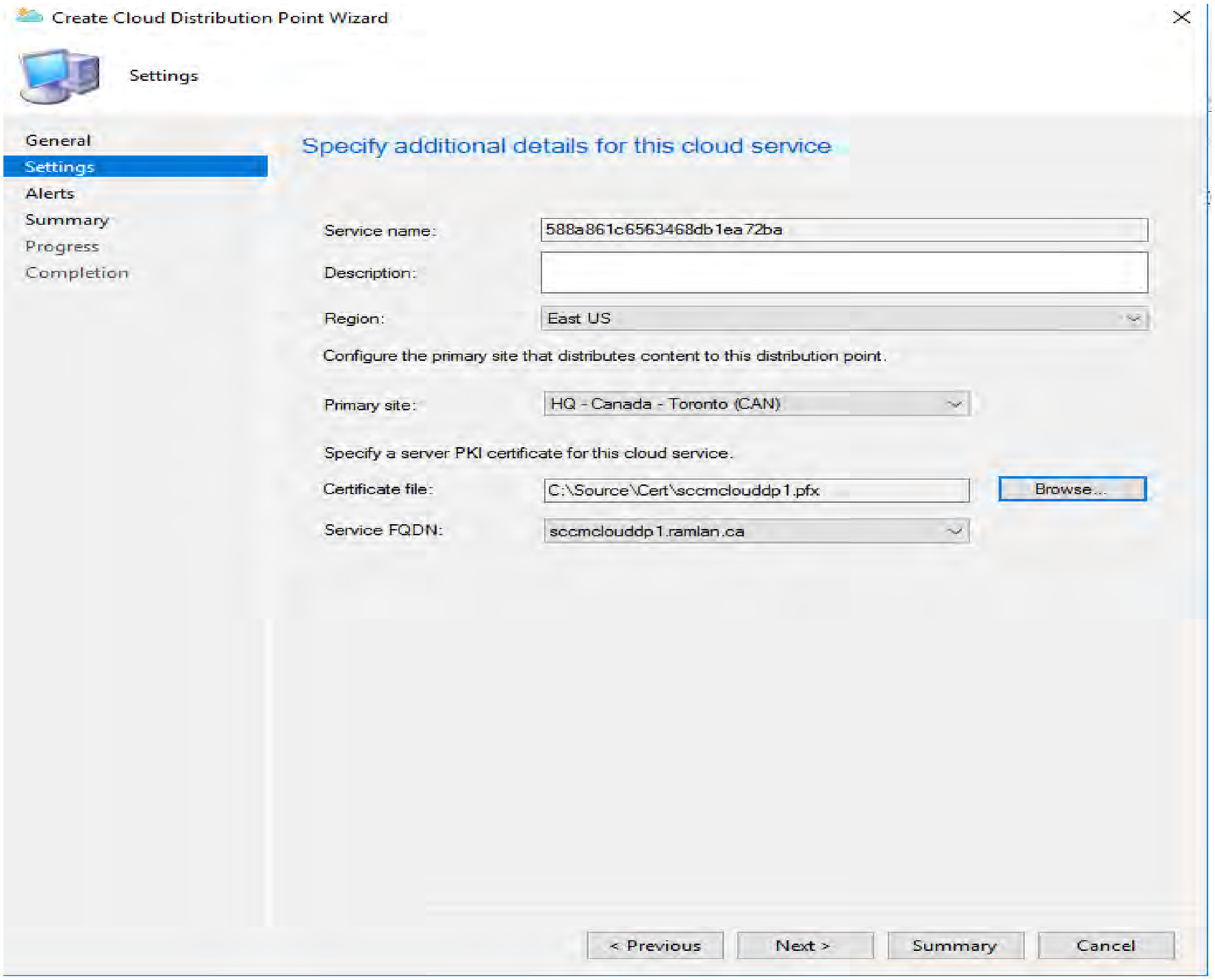
Specify details for this cloud service

Specify the subscription ID for the cloud service, and specify the management certificate that was uploaded to that service.

Azure environment: AzurePublicCloud

Subscription ID: [redacted]

Management certificate: C:\Source\Cert\CloudDP-ManagementCert.pf



Specify additional details for this cloud service

Service name: 588a861c6563468db1ea72ba

Description:

Region: East US

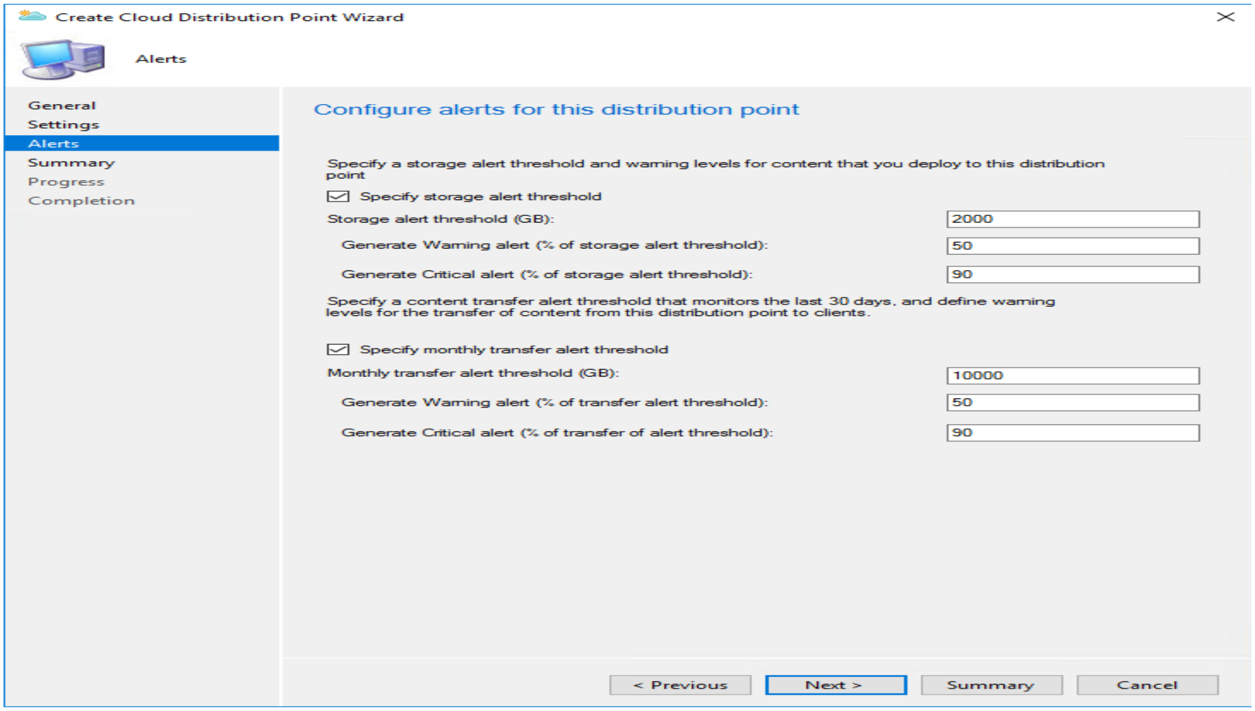
Configure the primary site that distributes content to this distribution point.

Primary site: HQ - Canada - Toronto (CAN)

Specify a server PKI certificate for this cloud service.

Certificate file: C:\Source\Cert\sccmclouddp1.pfx

Service FQDN: sccmclouddp1.ramlan.ca



Configure alerts for this distribution point

Specify a storage alert threshold and warning levels for content that you deploy to this distribution point

☑ Specify storage alert threshold

Storage alert threshold (GB): 2000

Generate Warning alert (% of storage alert threshold): 50

Generate Critical alert (% of storage alert threshold): 90

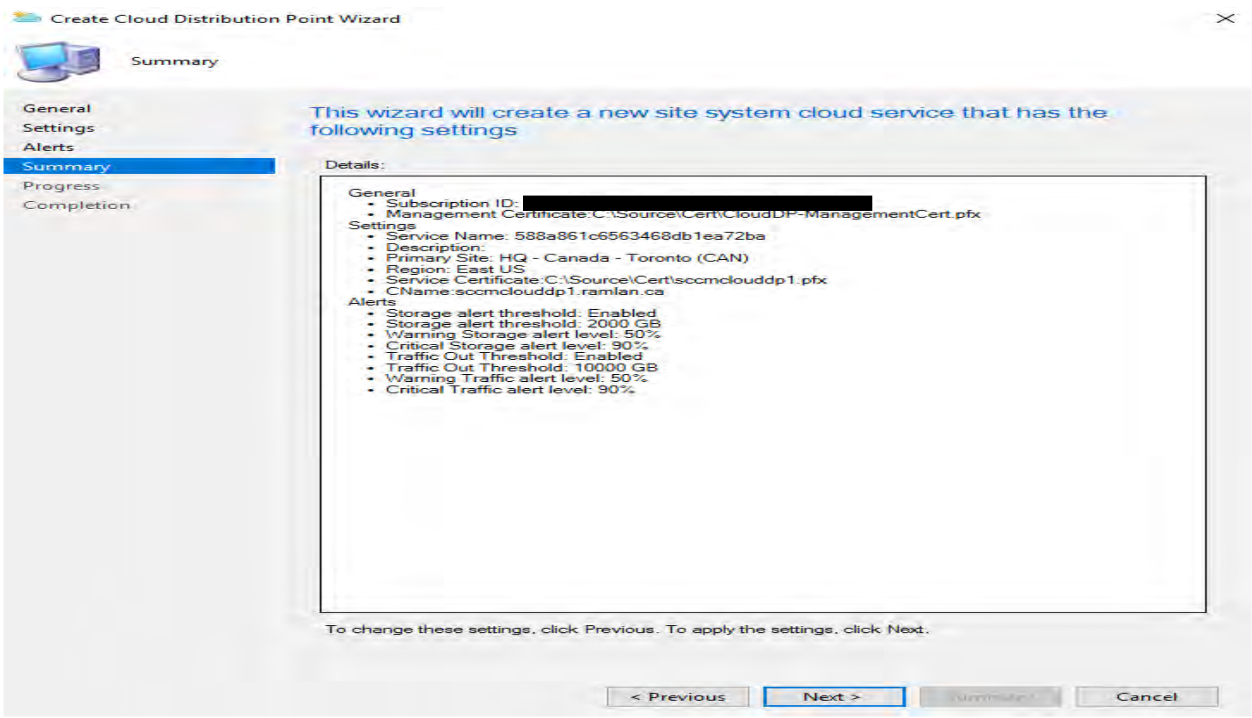
Specify a content transfer alert threshold that monitors the last 30 days, and define warning levels for the transfer of content from this distribution point to clients.

☑ Specify monthly transfer alert threshold

Monthly transfer alert threshold (GB): 10000

Generate Warning alert (% of transfer alert threshold): 50

Generate Critical alert (% of transfer of alert threshold): 90



This wizard will create a new site system cloud service that has the following settings

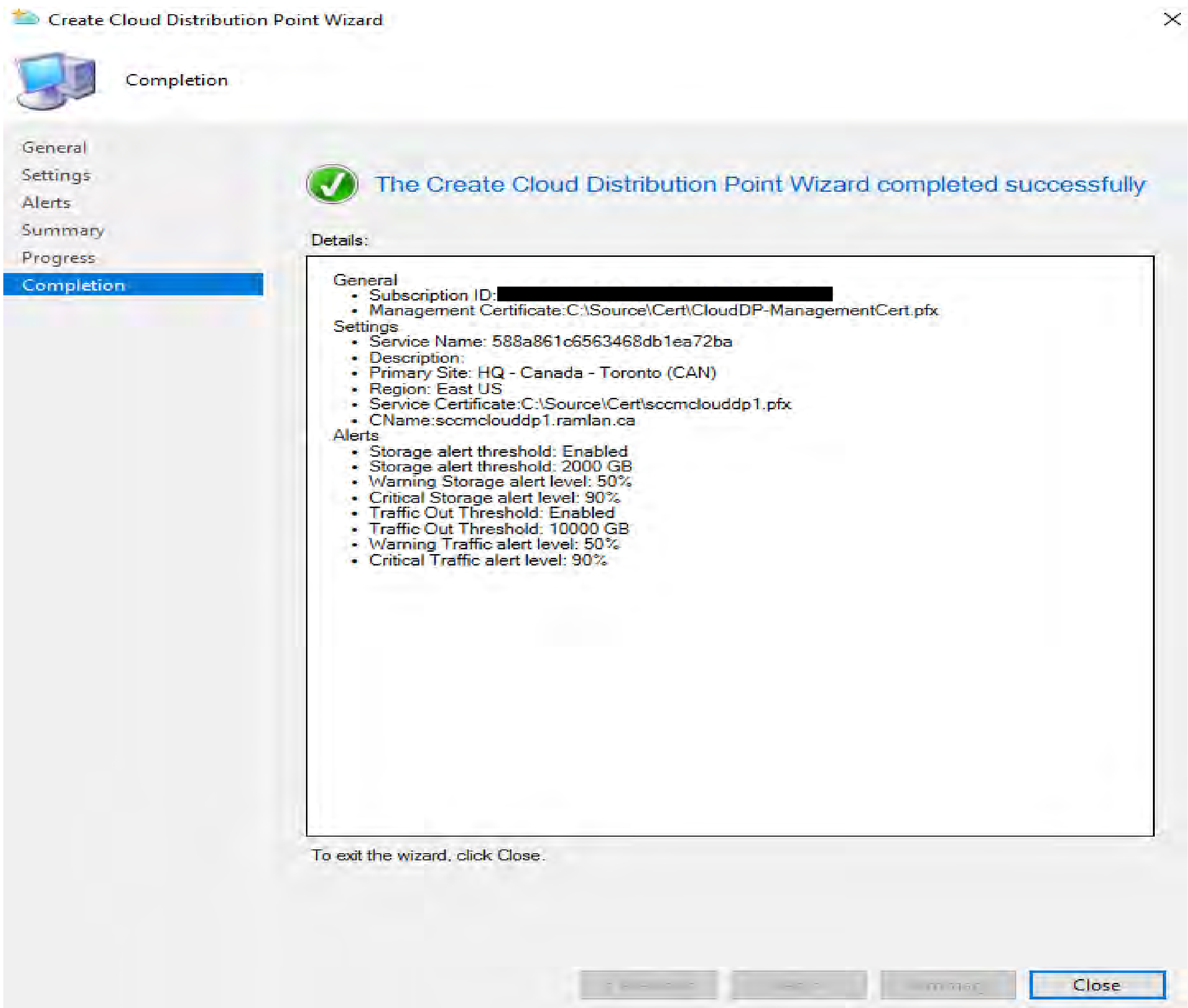
Details:

General
- Subscription ID: [redacted]
- Management Certificate:C:\Source\Cert\CloudDP-ManagementCert.pfx

Settings
- Service Name: 588a861c6563468db1ea72ba
- Description:
- Primary Site: HQ - Canada - Toronto (CAN)
- Region: East US
- Service Certificate:C:\Source\Cert\sccmclouddp1.pfx
- CName:sccmclouddp1.ramlan.ca

Alerts
- Storage alert threshold: Enabled
- Storage alert threshold: 2000 GB
- Warning Storage alert level: 50%
- Critical Storage alert level: 90%
- Traffic Out Threshold: Enabled
- Traffic Out Threshold: 10000 GB
- Warning Traffic alert level: 50%
- Critical Traffic alert level: 90%

To change these settings, click Previous. To apply the settings, click Next.



The Create Cloud Distribution Point Wizard completed successfully

Details:

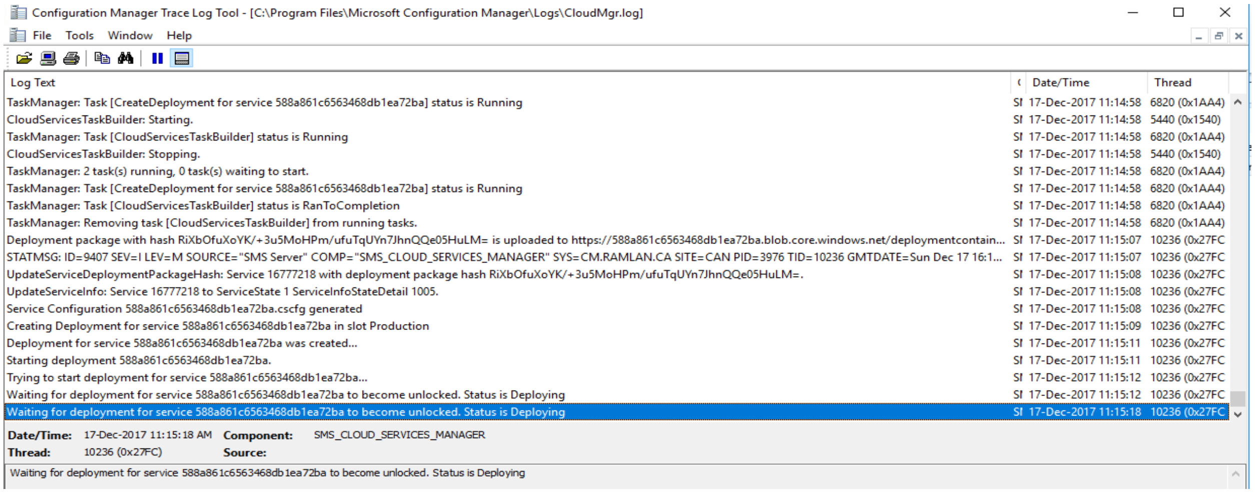
General
- Subscription ID: [redacted]
- Management Certificate:C:\Source\Cert\CloudDP-ManagementCert.pfx

Settings
- Service Name: 588a861c6563468db1ea72ba
- Description:
- Primary Site: HQ - Canada - Toronto (CAN)
- Region: East US
- Service Certificate:C:\Source\Cert\sccmclouddp1.pfx
- CName:sccmclouddp1.ramlan.ca

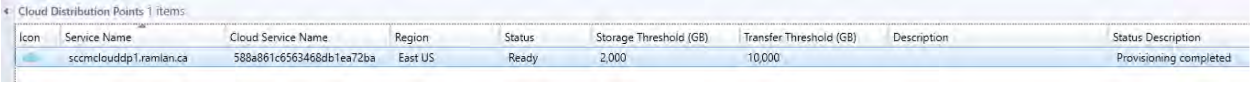
Alerts
- Storage alert threshold: Enabled
- Storage alert threshold: 2000 GB
- Warning Storage alert level: 50%
- Critical Storage alert level: 90%
- Traffic Out Threshold: Enabled
- Traffic Out Threshold: 10000 GB
- Warning Traffic alert level: 50%
- Critical Traffic alert level: 90%

To exit the wizard, click Close.

You can monitor the progress with this log


Configuration Manager Trace Log Tool - [C:\Program Files\Microsoft Configuration Manager\Logs\CloudMgr.log]
File
Tools
Window
Help

```
Log Text                                                                                                                             ( Date/Time             Thread
TaskManager: Task [CreateDeployment for service 588a861c6563468db1ea72ba] status is Running                                          SI 17-Dec-2017 11:14:58 6820 (0x1AA4)
CloudServicesTaskBuilder: Starting.                                                                                                  SI 17-Dec-2017 11:14:58 5440 (0x1540)
TaskManager: Task [CloudServicesTaskBuilder] status is Running                                                                       SI 17-Dec-2017 11:14:58 6820 (0x1AA4)
CloudServicesTaskBuilder: Stopping.                                                                                                  SI 17-Dec-2017 11:14:58 5440 (0x1540)
TaskManager: 2 task(s) running, 0 task(s) waiting to start.                                                                          SI 17-Dec-2017 11:14:58 6820 (0x1AA4)
TaskManager: Task [CreateDeployment for service 588a861c6563468db1ea72ba] status is Running                                          SI 17-Dec-2017 11:14:58 6820 (0x1AA4)
TaskManager: Task [CloudServicesTaskBuilder] status is RanToCompletion                                                               SI 17-Dec-2017 11:14:58 6820 (0x1AA4)
TaskManager: Removing task [CloudServicesTaskBuilder] from running tasks.                                                            SI 17-Dec-2017 11:14:58 6820 (0x1AA4)
Deployment package with hash RiXbOfuXoYK/+3u5MoHPm/ufuTqUYn7JhnQQe05HuLM= is uploaded to https://588a861c6563468db1ea72ba.blob.core.windows.net/deploymentcontain... SI 17-Dec-2017 11:15:07 10236 (0x27FC
STATMSG: ID=9407 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_CLOUD_SERVICES_MANAGER" SYS=CM.RAMLAN.CA SITE=CAN PID=3976 TID=10236 GMTDATE=Sun Dec 17 16:1... SI 17-Dec-2017 11:15:07 10236 (0x27FC
UpdateServiceDeploymentPackageHash: Service 16777218 with deployment package hash RiXbOfuXoYK/+3u5MoHPm/ufuTqUYn7JhnQQe05HuLM=.     SI 17-Dec-2017 11:15:08 10236 (0x27FC
UpdateServiceInfo: Service 16777218 to ServiceState 1 ServiceInfoStateDetail 1005.                                                   SI 17-Dec-2017 11:15:08 10236 (0x27FC
Service Configuration 588a861c6563468db1ea72ba.cscfg generated                                                                       SI 17-Dec-2017 11:15:08 10236 (0x27FC
Creating Deployment for service 588a861c6563468db1ea72ba in slot Production                                                          SI 17-Dec-2017 11:15:09 10236 (0x27FC
Deployment for service 588a861c6563468db1ea72ba was created...                                                                       SI 17-Dec-2017 11:15:11 10236 (0x27FC
Starting deployment 588a861c6563468db1ea72ba.                                                                                        SI 17-Dec-2017 11:15:11 10236 (0x27FC
Trying to start deployment for service 588a861c6563468db1ea72ba...                                                                   SI 17-Dec-2017 11:15:12 10236 (0x27FC
Waiting for deployment for service 588a861c6563468db1ea72ba to become unlocked. Status is Deploying                                  SI 17-Dec-2017 11:15:12 10236 (0x27FC
Waiting for deployment for service 588a861c6563468db1ea72ba to become unlocked. Status is Deploying                                  SI 17-Dec-2017 11:15:18 10236 (0x27FC

Date/Time:  17-Dec-2017 11:15:18 AM   Component:  SMS_CLOUD_SERVICES_MANAGER
Thread:     10236 (0x27FC)             Source:

Waiting for deployment for service 588a861c6563468db1ea72ba to become unlocked. Status is Deploying
```

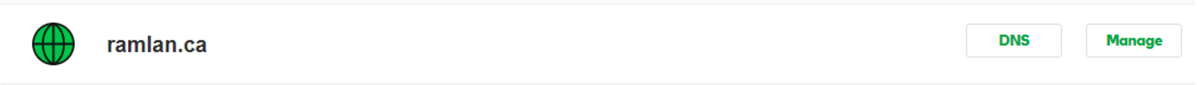


Cloud Distribution Points 1 items

| Icon | Service Name | Cloud Service Name | Region | Status | Storage Threshold (GB) | Transfer Threshold (GB) | Description | Status Description |
|---|---|---|---|---|---|---|---|---|
|  | sccmclouddp1.ramlan.ca | 588a861c6563468db1ea72ba | East US | Ready | 2,000 | 10,000 |  | Provisioning completed |

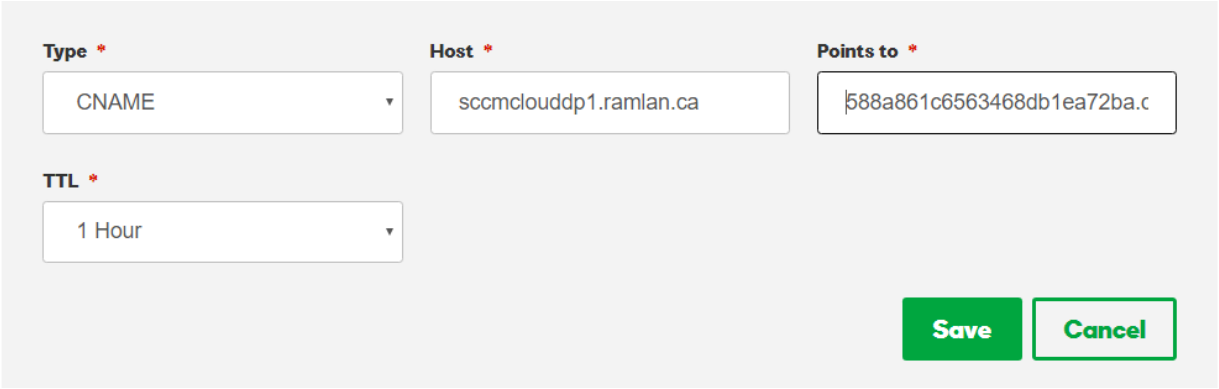
Now, I am going to create CNAME record at GoDaddy so Cloud DP/GoDaddy will know Azure details:

Log in to GoDaddy



Click DNS – Click Add

ADD



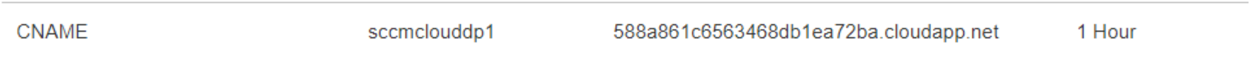
Type * CNAME

Host * sccmclouddp1.ramlan.ca

Points to * 588a861c6563468db1ea72ba.c

TTL * 1 Hour

Now you will see this entry in your PUBLIC DNS at GoDaddy

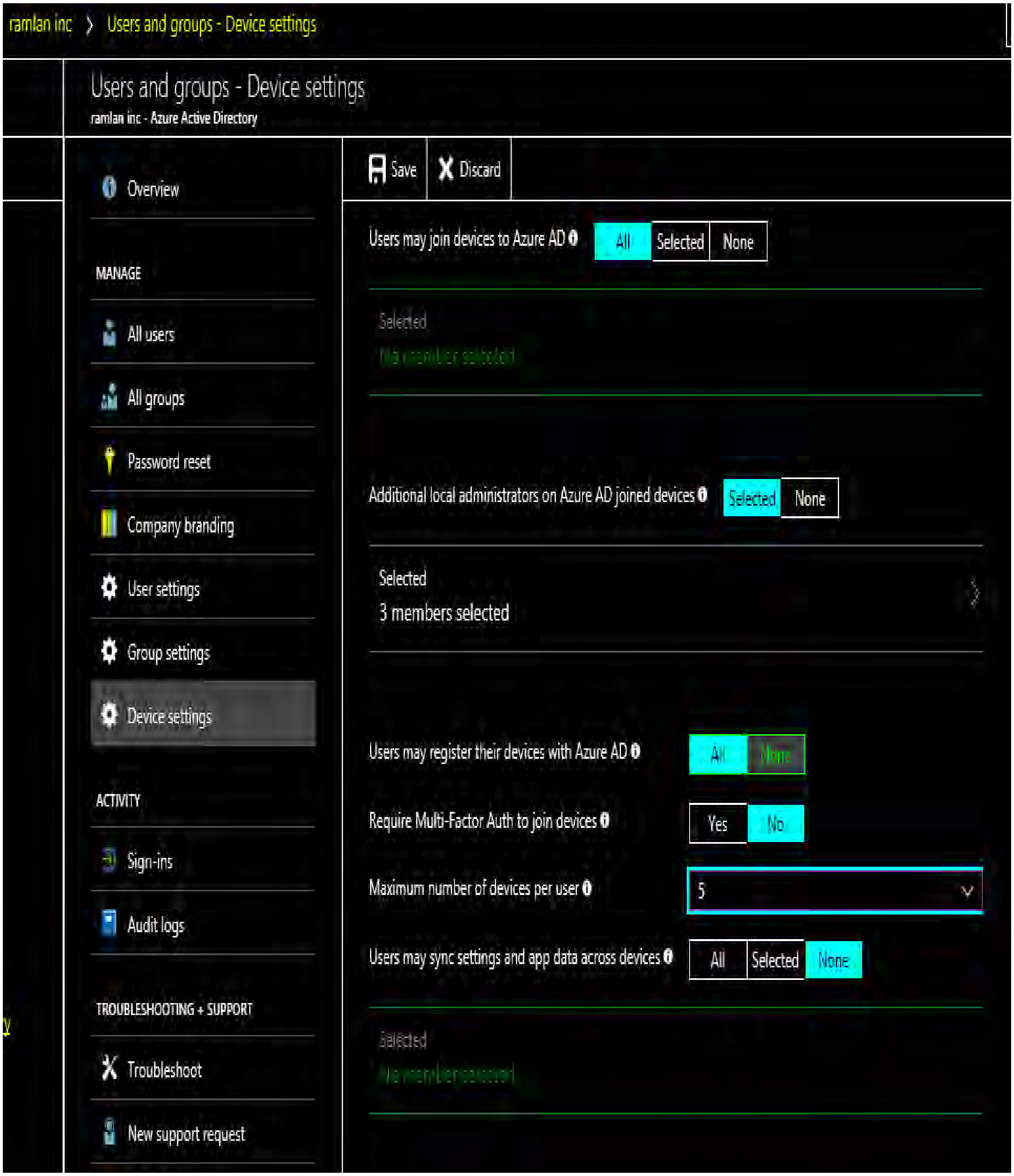


CNAME    sccmclouddp1    588a861c6563468db1ea72ba.cloudapp.net    1 Hour

Now we have fully configured Cloud Management Gateway (CMG) & Cloud Distribution Point (CDP) in Azure & CB1710.

# CLOUD CO-MANAGEMENT PROCESS

Go to Azure Active Directory – Users and Groups – Device Settings – Complete as below



Users may join devices to Azure AD [✓ All] Selected None

Selected
No member selected

Additional local administrators on Azure AD joined devices [✓ Selected] None

Selected
3 members selected

Users may register their devices with Azure AD [✓ All] None

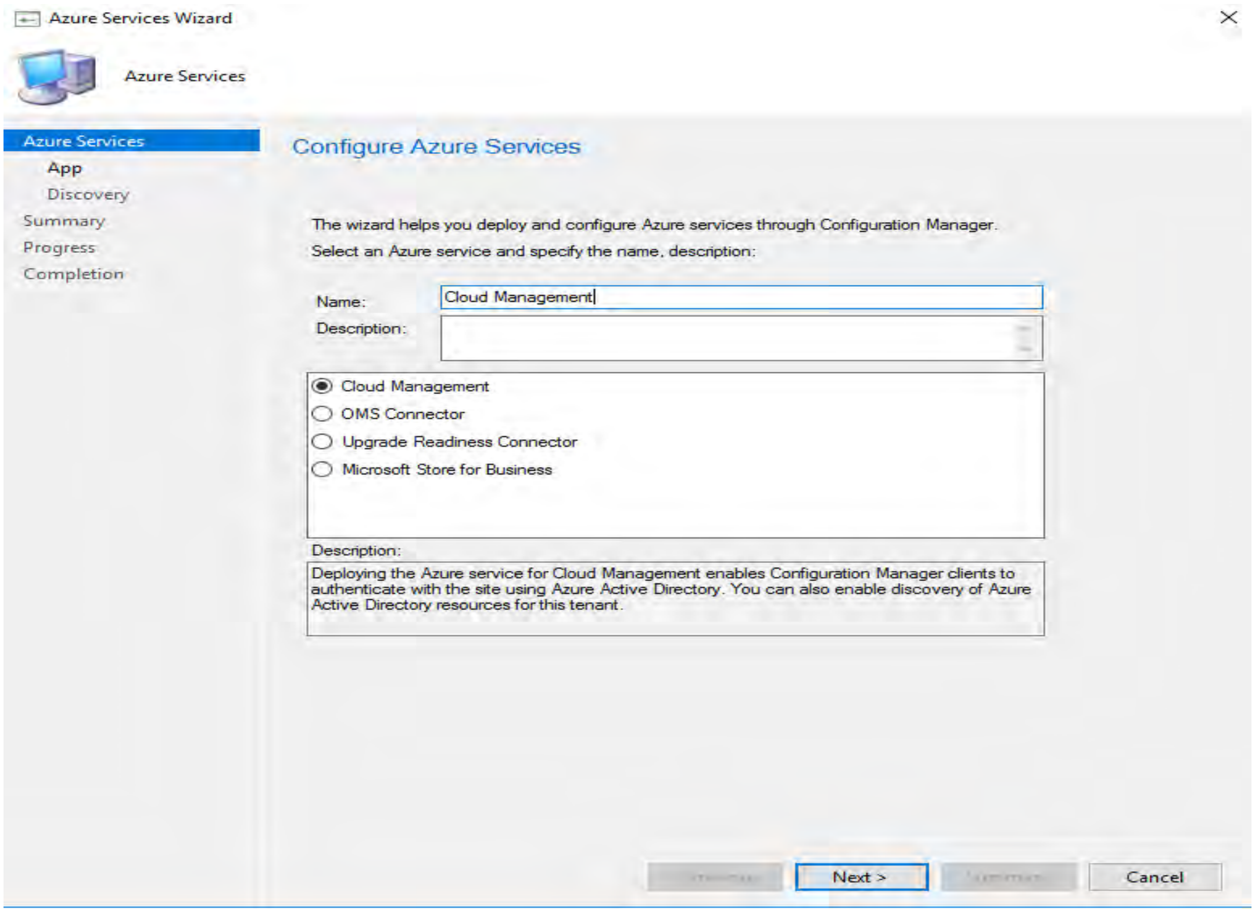
Require Multi-Factor Auth to join devices Yes [✓ No]

Maximum number of devices per user 5

Users may sync settings and app data across devices All Selected [✓ None]

Selected
No member selected

Go to Configuration Manager Console – Administration - Azure Services – Configure Azure Services



Configure Azure Services

The wizard helps you deploy and configure Azure services through Configuration Manager.
Select an Azure service and specify the name, description:

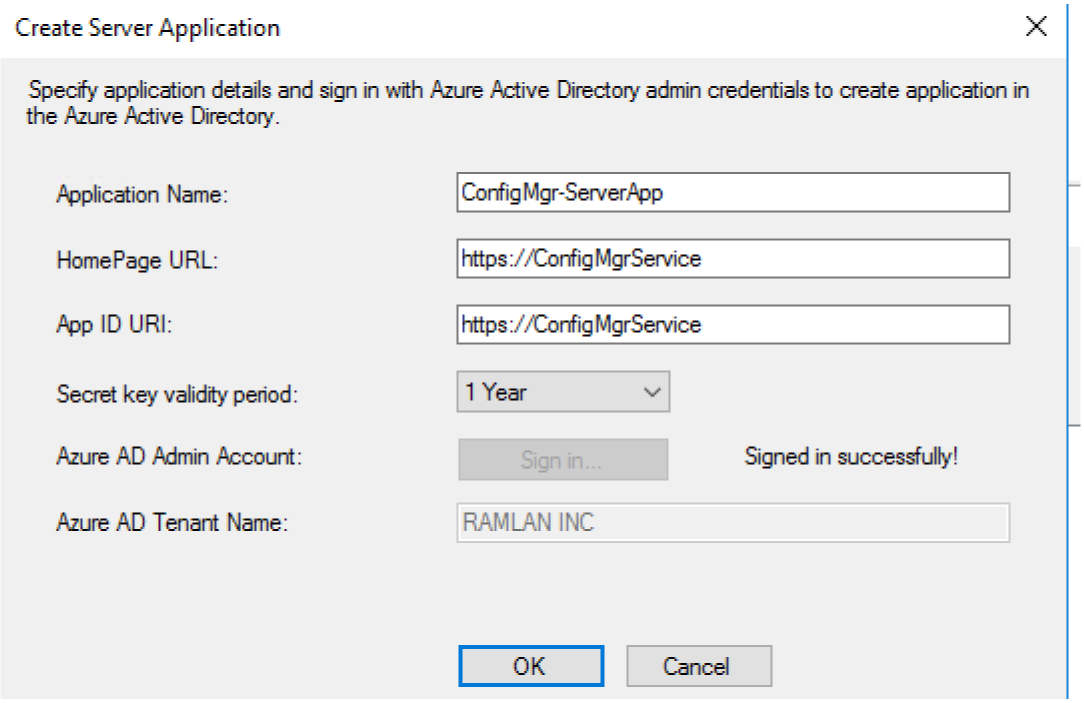
Name: Cloud Management
Description:

● Cloud Management
○ OMS Connector
○ Upgrade Readiness Connector
○ Microsoft Store for Business

Description:
Deploying the Azure service for Cloud Management enables Configuration Manager clients to authenticate with the site using Azure Active Directory. You can also enable discovery of Azure Active Directory resources for this tenant.

Click Browse – Web App – Create – For Application Name type ConfigMgr-ServerApp

Click Sign-in (enter your Azure Credentials) – Click OK



Specify application details and sign in with Azure Active Directory admin credentials to create application in the Azure Active Directory.

Application Name: ConfigMgr-ServerApp

HomePage URL: https://ConfigMgrService

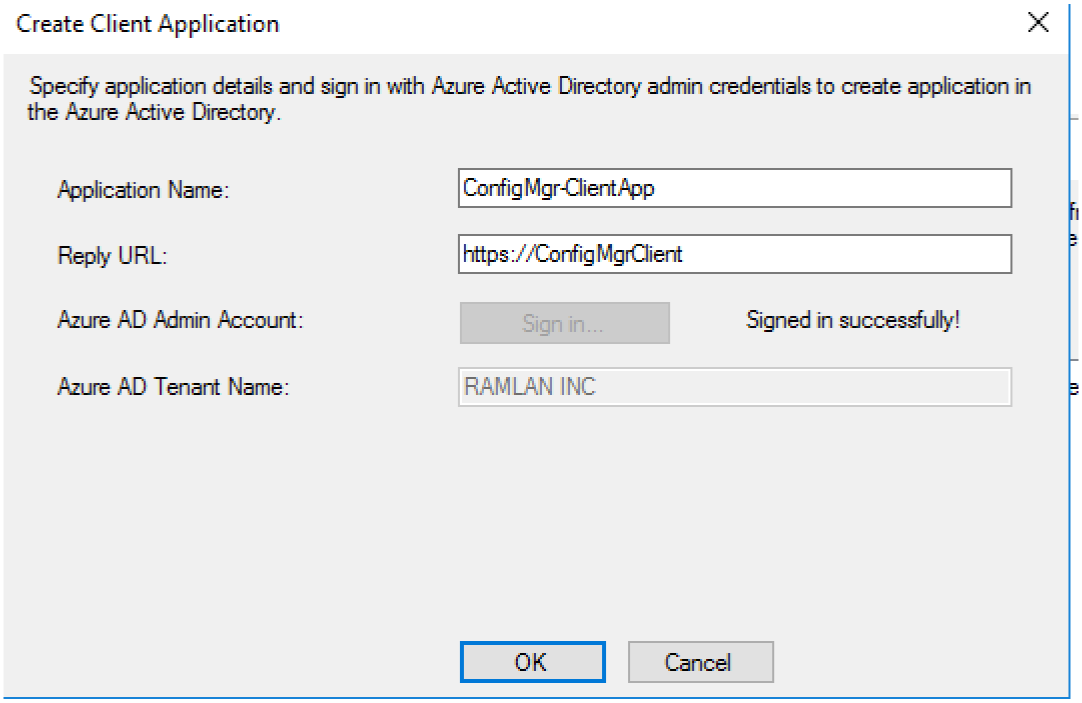
App ID URI: https://ConfigMgrService

Secret key validity period: 1 Year

Azure AD Admin Account: Signed in successfully!

Azure AD Tenant Name: RAMLAN INC

Do the same for Native Client App



Create Client Application

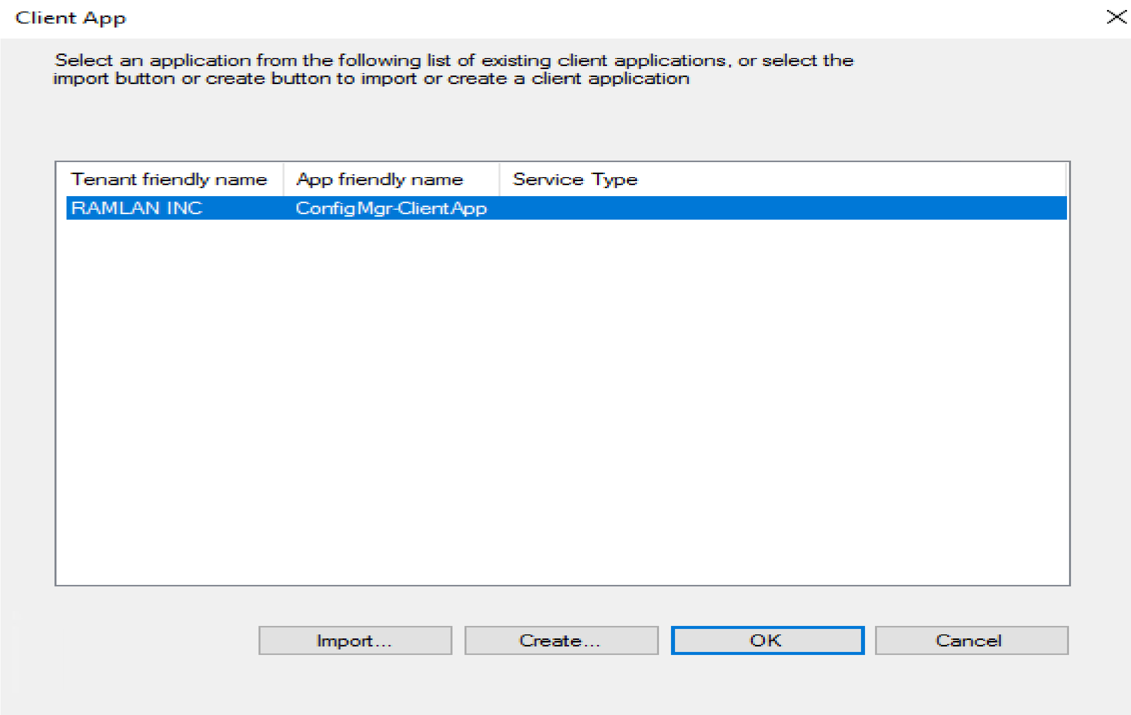
Specify application details and sign in with Azure Active Directory admin credentials to create application in the Azure Active Directory.

Application Name: ConfigMgr-ClientApp

Reply URL: https://ConfigMgrClient

Azure AD Admin Account: Sign in... Signed in successfully!

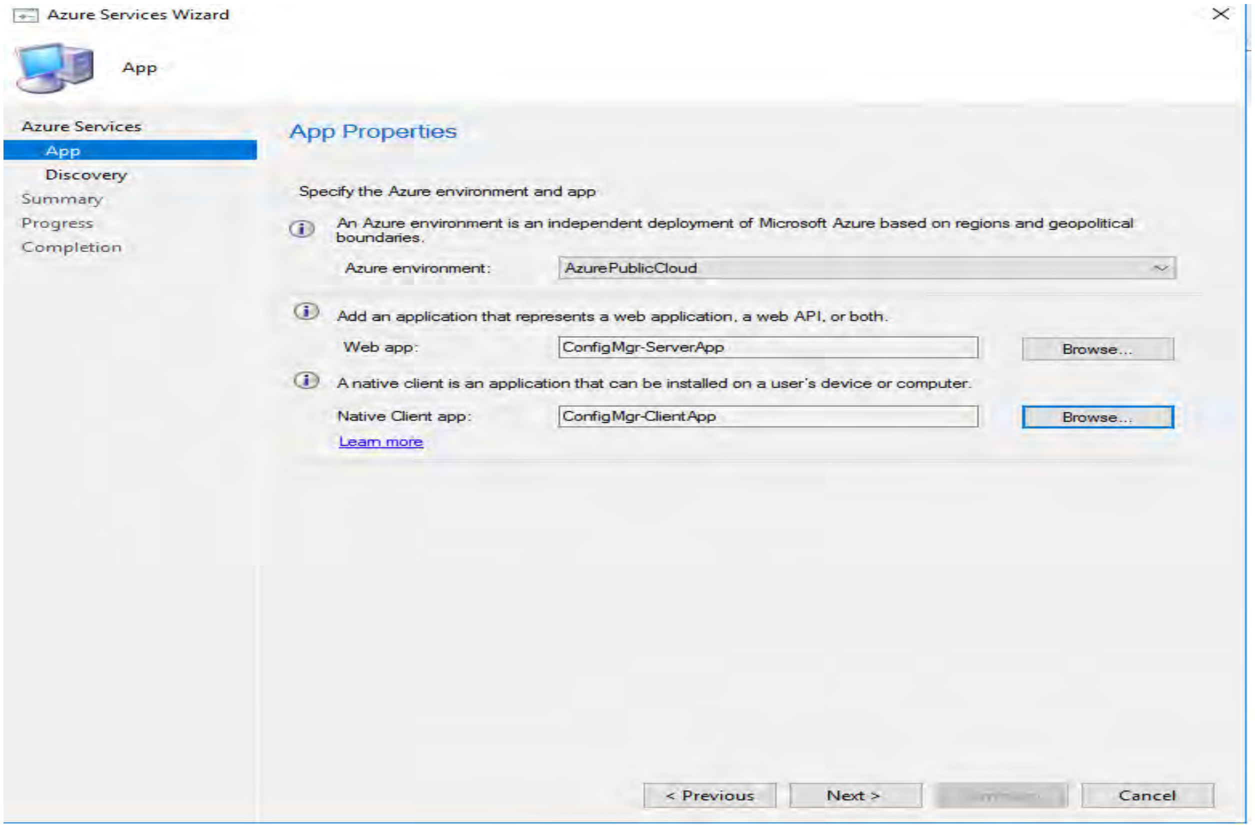
Azure AD Tenant Name: RAMLAN INC



Client App

Select an application from the following list of existing client applications, or select the import button or create button to import or create a client application

| Tenant friendly name | App friendly name | Service Type |
|---|---|---|
| RAMLAN INC | ConfigMgr-ClientApp | |



App Properties

Specify the Azure environment and app

An Azure environment is an independent deployment of Microsoft Azure based on regions and geopolitical boundaries.

Azure environment: AzurePublicCloud

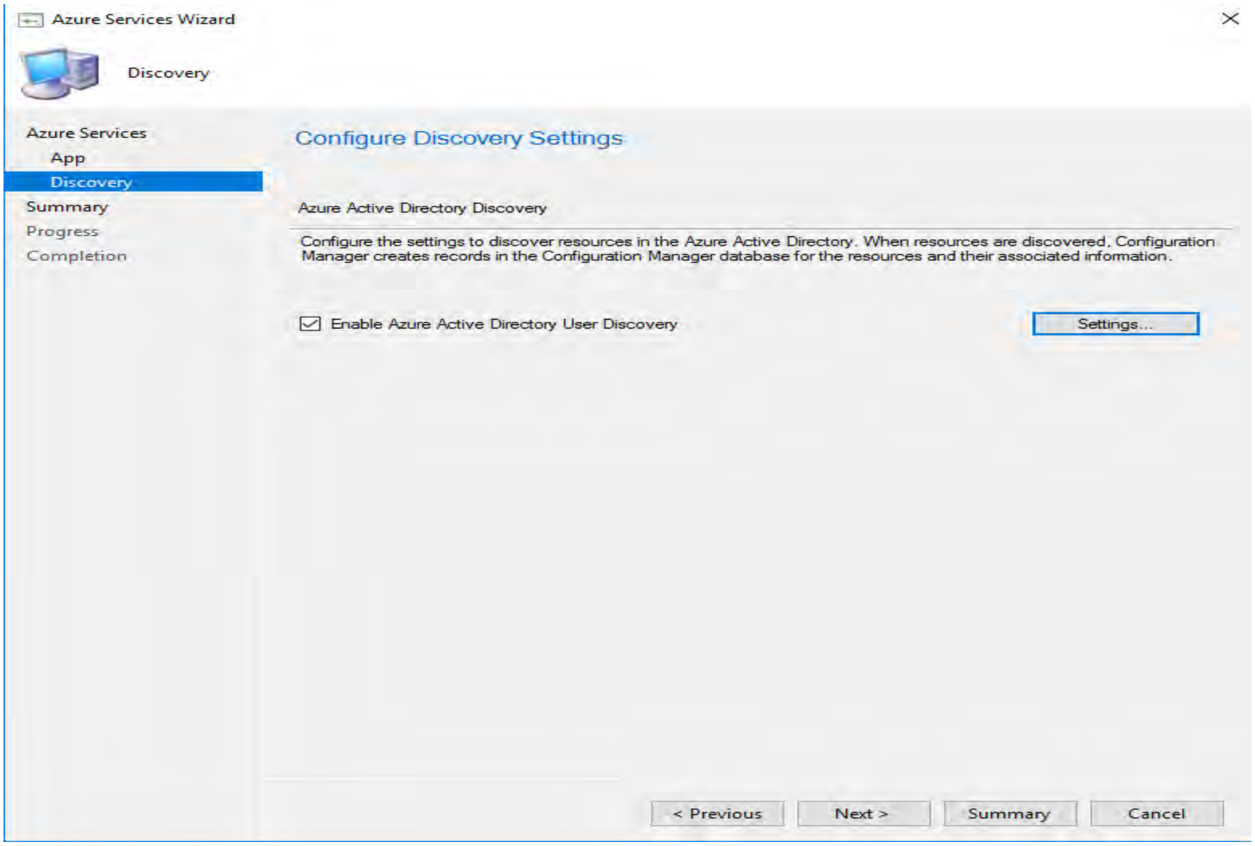
Add an application that represents a web application, a web API, or both.

Web app: ConfigMgr-ServerApp

A native client is an application that can be installed on a user's device or computer.

Native Client app: ConfigMgr-ClientApp

Learn more

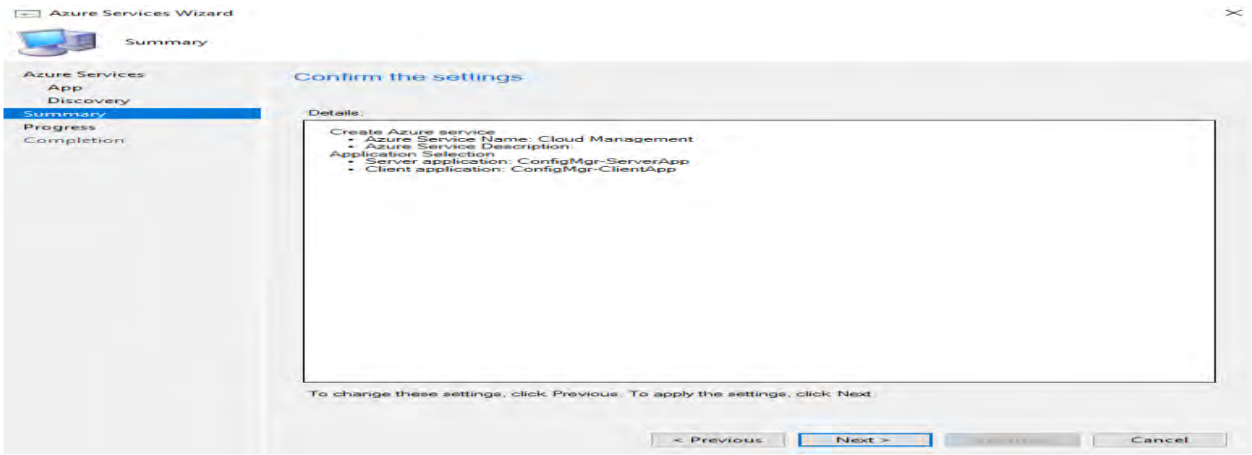


Configure Discovery Settings

Azure Active Directory Discovery

Configure the settings to discover resources in the Azure Active Directory. When resources are discovered, Configuration Manager creates records in the Configuration Manager database for the resources and their associated information.

☑ Enable Azure Active Directory User Discovery



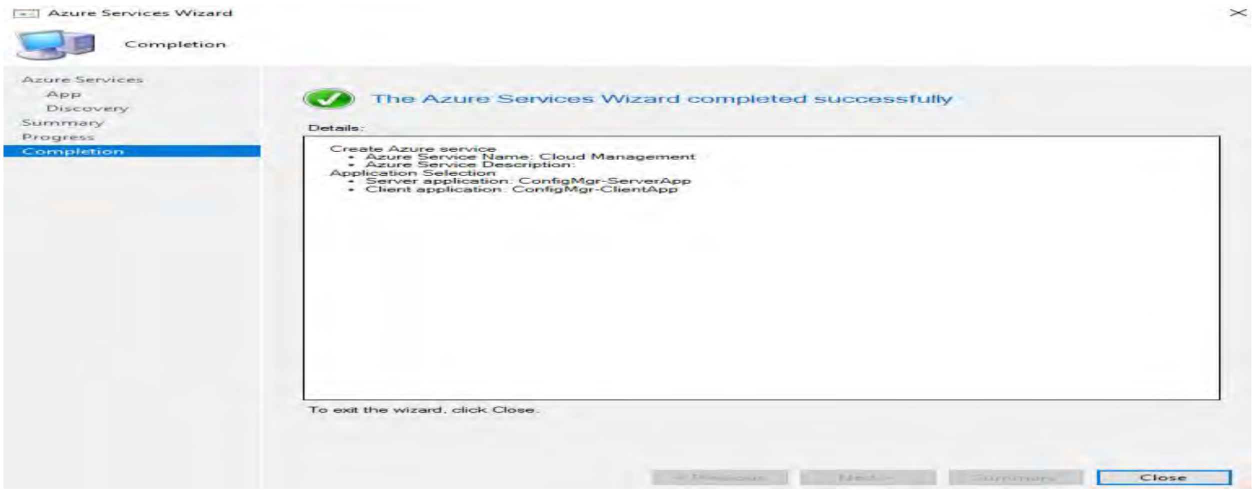
Confirm the settings

Details:

Create Azure service
- Azure Service Name: Cloud Management
- Azure Service Description:

Application Selection
- Server application: ConfigMgr-ServerApp
- Client application: ConfigMgr-ClientApp

To change these settings, click Previous. To apply the settings, click Next.



The Azure Services Wizard completed successfully

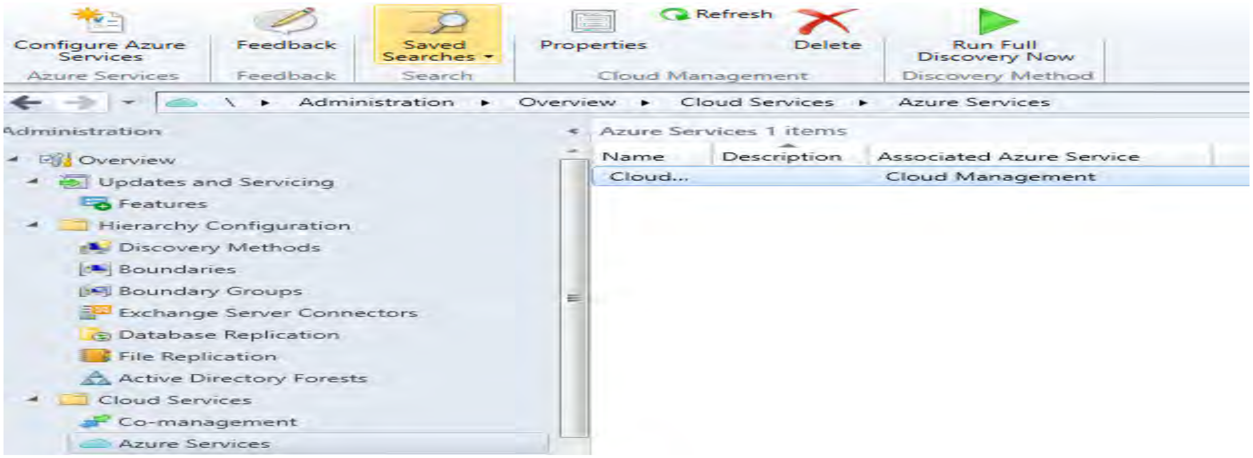
Details:

Create Azure service
- Azure Service Name: Cloud Management
- Azure Service Description:

Application Selection
- Server application: ConfigMgr-ServerApp
- Client application: ConfigMgr-ClientApp

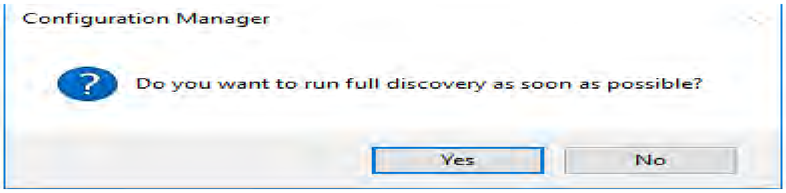
To exit the wizard, click Close.

Click Run Full Discovery Now



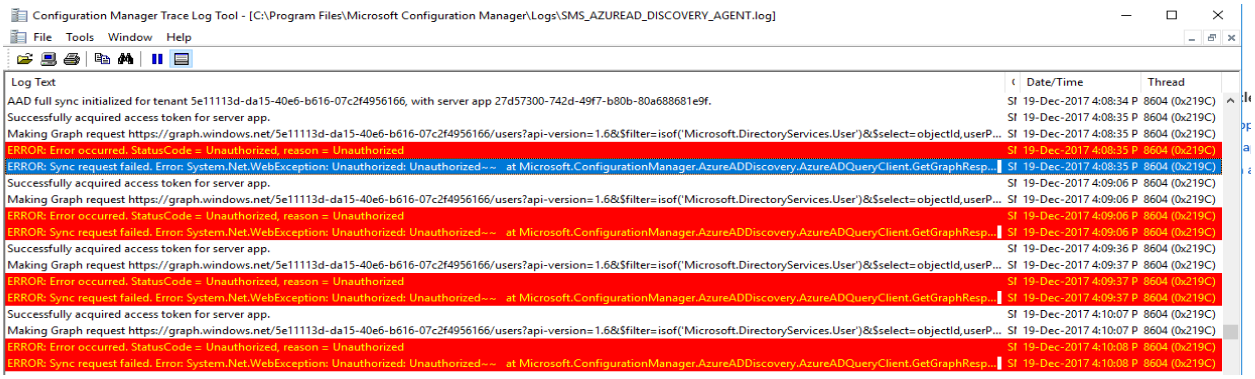
Azure Services 1 items

| Name | Description | Associated Azure Service |
|---|---|---|
| Cloud... | | Cloud Management |



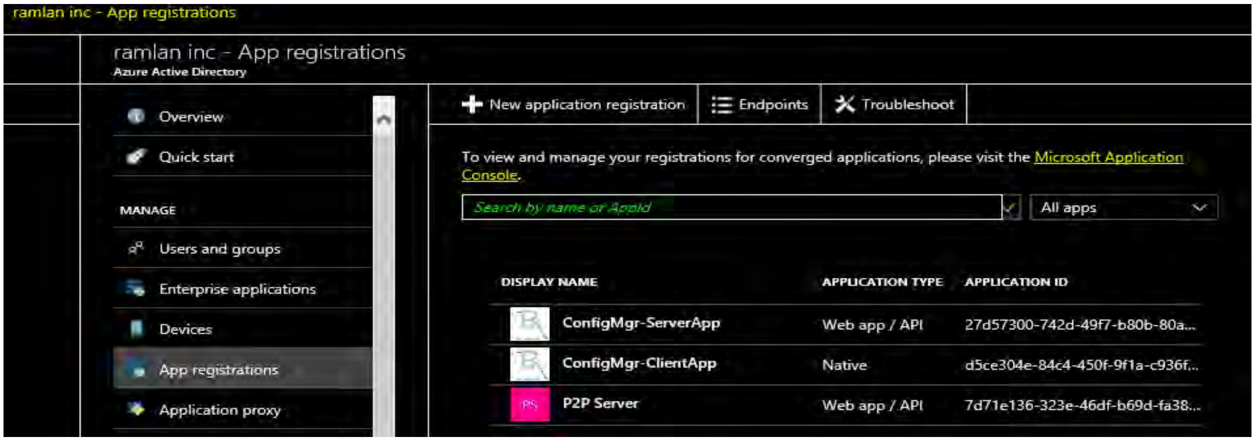
Do you want to run full discovery as soon as possible?

I was getting error during full discovery.  Had to do the following:



Configuration Manager Trace Log Tool - [C:\Program Files\Microsoft Configuration Manager\Logs\SMS_AZUREAD_DISCOVERY_AGENT.log]
File Tools Window Help

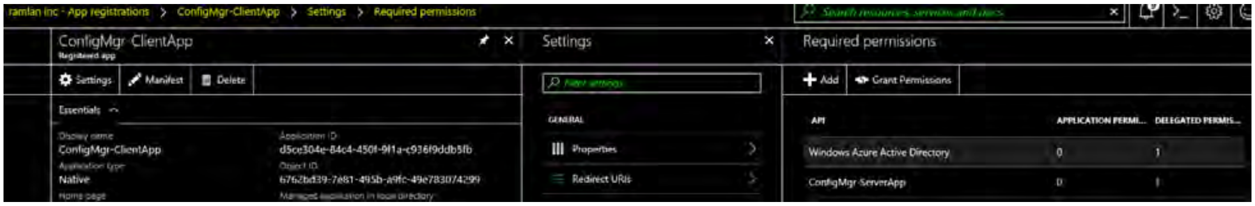
```
Log Text                                                                                                                                  ( Date/Time             Thread
AAD full sync initialized for tenant 5e11113d-da15-40e6-b616-07c2f4956166, with server app 27d57300-742d-49f7-b80b-80a688681e9f.          SI 19-Dec-2017 4:08:34 P 8604 (0x219C)
Successfully acquired access token for server app.                                                                                       SI 19-Dec-2017 4:08:35 P 8604 (0x219C)
Making Graph request https://graph.windows.net/5e11113d-da15-40e6-b616-07c2f4956166/users?api-version=1.6&$filter=isof('Microsoft.DirectoryServices.User')&$select=objectId,userP... SI 19-Dec-2017 4:08:35 P 8604 (0x219C)
ERROR: Error occurred. StatusCode = Unauthorized, reason = Unauthorized                                                                  SI 19-Dec-2017 4:08:35 P 8604 (0x219C)
ERROR: Sync request failed. Error: System.Net.WebException: Unauthorized: Unauthorized~~   at Microsoft.ConfigurationManager.AzureADDiscovery.AzureADQueryClient.GetGraphResp... SI 19-Dec-2017 4:08:35 P 8604 (0x219C)
Successfully acquired access token for server app.                                                                                       SI 19-Dec-2017 4:09:06 P 8604 (0x219C)
Making Graph request https://graph.windows.net/5e11113d-da15-40e6-b616-07c2f4956166/users?api-version=1.6&$filter=isof('Microsoft.DirectoryServices.User')&$select=objectId,userP... SI 19-Dec-2017 4:09:06 P 8604 (0x219C)
ERROR: Error occurred. StatusCode = Unauthorized, reason = Unauthorized                                                                  SI 19-Dec-2017 4:09:06 P 8604 (0x219C)
ERROR: Sync request failed. Error: System.Net.WebException: Unauthorized: Unauthorized~~   at Microsoft.ConfigurationManager.AzureADDiscovery.AzureADQueryClient.GetGraphResp... SI 19-Dec-2017 4:09:06 P 8604 (0x219C)
Successfully acquired access token for server app.                                                                                       SI 19-Dec-2017 4:09:36 P 8604 (0x219C)
Making Graph request https://graph.windows.net/5e11113d-da15-40e6-b616-07c2f4956166/users?api-version=1.6&$filter=isof('Microsoft.DirectoryServices.User')&$select=objectId,userP... SI 19-Dec-2017 4:09:37 P 8604 (0x219C)
ERROR: Error occurred. StatusCode = Unauthorized, reason = Unauthorized                                                                  SI 19-Dec-2017 4:09:37 P 8604 (0x219C)
ERROR: Sync request failed. Error: System.Net.WebException: Unauthorized: Unauthorized~~   at Microsoft.ConfigurationManager.AzureADDiscovery.AzureADQueryClient.GetGraphResp... SI 19-Dec-2017 4:09:37 P 8604 (0x219C)
Successfully acquired access token for server app.                                                                                       SI 19-Dec-2017 4:10:07 P 8604 (0x219C)
Making Graph request https://graph.windows.net/5e11113d-da15-40e6-b616-07c2f4956166/users?api-version=1.6&$filter=isof('Microsoft.DirectoryServices.User')&$select=objectId,userP... SI 19-Dec-2017 4:10:07 P 8604 (0x219C)
ERROR: Error occurred. StatusCode = Unauthorized, reason = Unauthorized                                                                  SI 19-Dec-2017 4:10:08 P 8604 (0x219C)
ERROR: Sync request failed. Error: System.Net.WebException: Unauthorized: Unauthorized~~   at Microsoft.ConfigurationManager.AzureADDiscovery.AzureADQueryClient.GetGraphResp... SI 19-Dec-2017 4:10:08 P 8604 (0x219C)
```



To view and manage your registrations for converged applications, please visit the Microsoft Application Console.

| DISPLAY NAME | APPLICATION TYPE | APPLICATION ID |
|---|---|---|
| ConfigMgr-ServerApp | Web app / API | 27d57300-742d-49f7-b80b-80a... |
| ConfigMgr-ClientApp | Native | d5ce304e-84c4-450f-9f1a-c936f... |
| P2P Server | Web app / API | 7d71e136-323e-46df-b69d-fa38... |

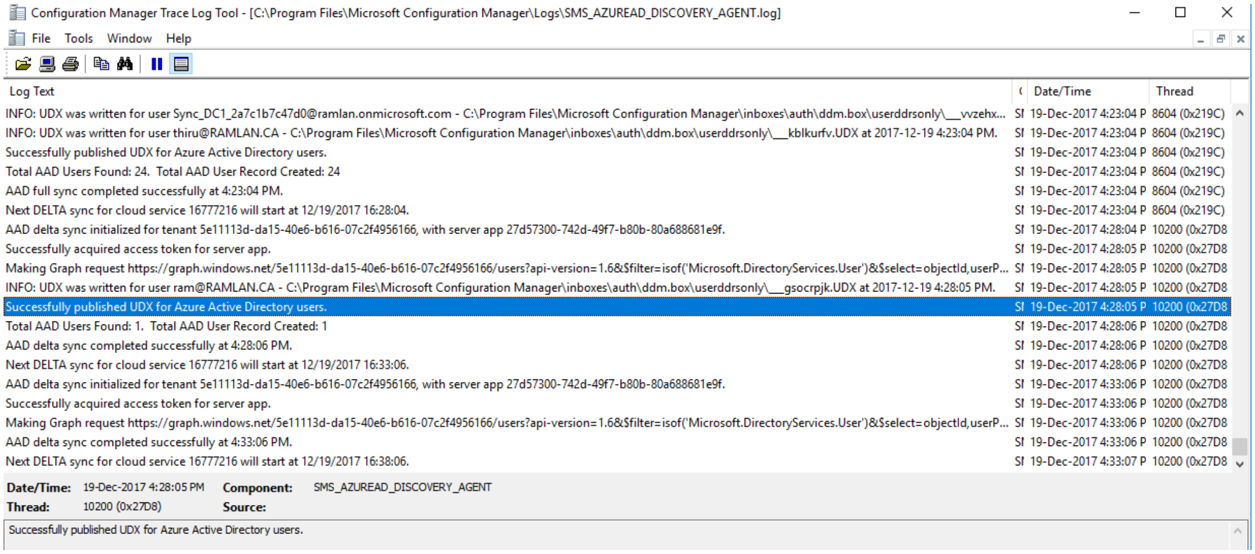
Select ConfigMgr-ServerApp – Settings – Required Permissions – Grant Permissions



Display name
ConfigMgr-ClientApp
Application type
Native
Home page

Application ID
d5ce304e-84c4-450f-9f1a-c936f9ddb5fb
Object ID
6762bd39-7e81-495b-a9fc-49e783074299
Managed application in local directory

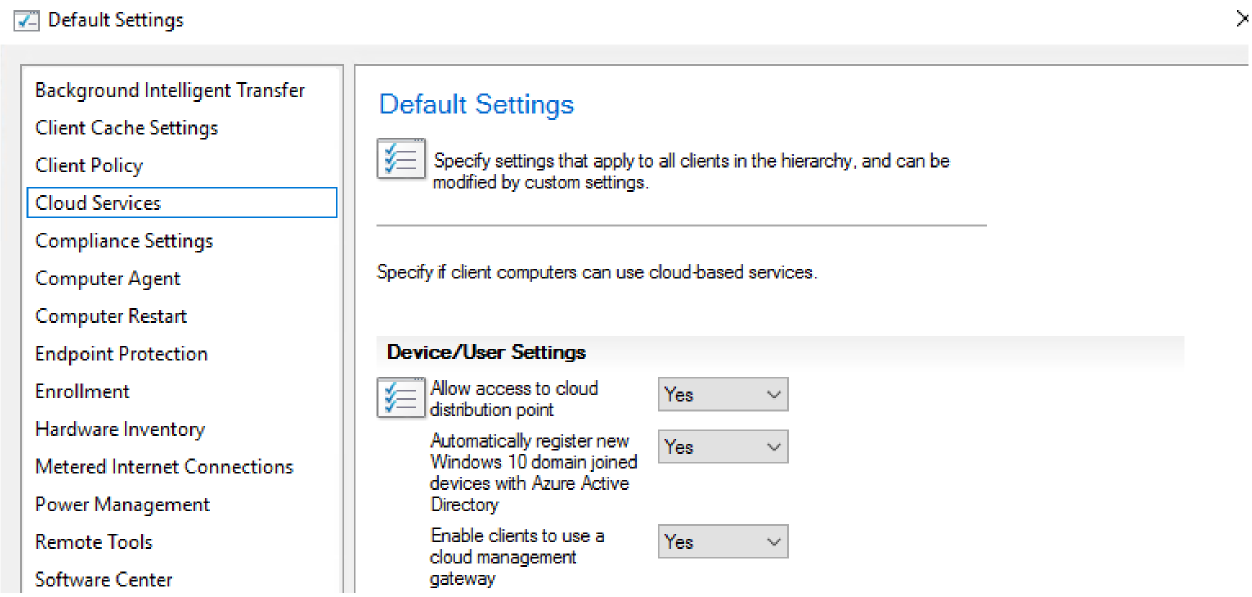
| API | APPLICATION PERMI... | DELEGATED PERMIS... |
|---|---|---|
| Windows Azure Active Directory | 0 | 1 |
| ConfigMgr-ServerApp | 0 | 1 |



Configuration Manager Trace Log Tool - [C:\Program Files\Microsoft Configuration Manager\Logs\SMS_AZUREAD_DISCOVERY_AGENT.log]
File Tools Window Help

```
Log Text                                                                                                                                  ( Date/Time             Thread
INFO: UDX was written for user Sync_DC1_2a7c1b7c47d0@ramlan.onmicrosoft.com - C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\userddrsonly\__vvzehx... SI 19-Dec-2017 4:23:04 P 8604 (0x219C)
INFO: UDX was written for user thiru@RAMLAN.CA - C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\userddrsonly\__kblkurfv.UDX at 2017-12-19 4:23:04 PM. SI 19-Dec-2017 4:23:04 P 8604 (0x219C)
Successfully published UDX for Azure Active Directory users.                                                                             SI 19-Dec-2017 4:23:04 P 8604 (0x219C)
Total AAD Users Found: 24.  Total AAD User Record Created: 24                                                                            SI 19-Dec-2017 4:23:04 P 8604 (0x219C)
AAD full sync completed successfully at 4:23:04 PM.                                                                                      SI 19-Dec-2017 4:23:04 P 8604 (0x219C)
Next DELTA sync for cloud service 16777216 will start at 12/19/2017 16:28:04.                                                            SI 19-Dec-2017 4:23:04 P 8604 (0x219C)
AAD delta sync initialized for tenant 5e11113d-da15-40e6-b616-07c2f4956166, with server app 27d57300-742d-49f7-b80b-80a688681e9f.         SI 19-Dec-2017 4:28:04 P 10200 (0x27D8
Successfully acquired access token for server app.                                                                                       SI 19-Dec-2017 4:28:05 P 10200 (0x27D8
Making Graph request https://graph.windows.net/5e11113d-da15-40e6-b616-07c2f4956166/users?api-version=1.6&$filter=isof('Microsoft.DirectoryServices.User')&$select=objectId,userP... SI 19-Dec-2017 4:28:05 P 10200 (0x27D8
INFO: UDX was written for user ram@RAMLAN.CA - C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\userddrsonly\__gsocrpjk.UDX at 2017-12-19 4:28:05 PM. SI 19-Dec-2017 4:28:05 P 10200 (0x27D8
Successfully published UDX for Azure Active Directory users.                                                                             SI 19-Dec-2017 4:28:05 P 10200 (0x27D8
Total AAD Users Found: 1.  Total AAD User Record Created: 1                                                                              SI 19-Dec-2017 4:28:06 P 10200 (0x27D8
AAD delta sync completed successfully at 4:28:06 PM.                                                                                     SI 19-Dec-2017 4:28:06 P 10200 (0x27D8
Next DELTA sync for cloud service 16777216 will start at 12/19/2017 16:33:06.                                                            SI 19-Dec-2017 4:28:06 P 10200 (0x27D8
AAD delta sync initialized for tenant 5e11113d-da15-40e6-b616-07c2f4956166, with server app 27d57300-742d-49f7-b80b-80a688681e9f.         SI 19-Dec-2017 4:33:06 P 10200 (0x27D8
Successfully acquired access token for server app.                                                                                       SI 19-Dec-2017 4:33:06 P 10200 (0x27D8
Making Graph request https://graph.windows.net/5e11113d-da15-40e6-b616-07c2f4956166/users?api-version=1.6&$filter=isof('Microsoft.DirectoryServices.User')&$select=objectId,userP... SI 19-Dec-2017 4:33:06 P 10200 (0x27D8
AAD delta sync completed successfully at 4:33:06 PM.                                                                                     SI 19-Dec-2017 4:33:06 P 10200 (0x27D8
Next DELTA sync for cloud service 16777216 will start at 12/19/2017 16:38:06.                                                            SI 19-Dec-2017 4:33:07 P 10200 (0x27D8

Date/Time:  19-Dec-2017 4:28:05 PM     Component:  SMS_AZUREAD_DISCOVERY_AGENT
Thread:     10200 (0x27D8)             Source:

Successfully published UDX for Azure Active Directory users.
```

Update Client Settings as follows:



Default Settings

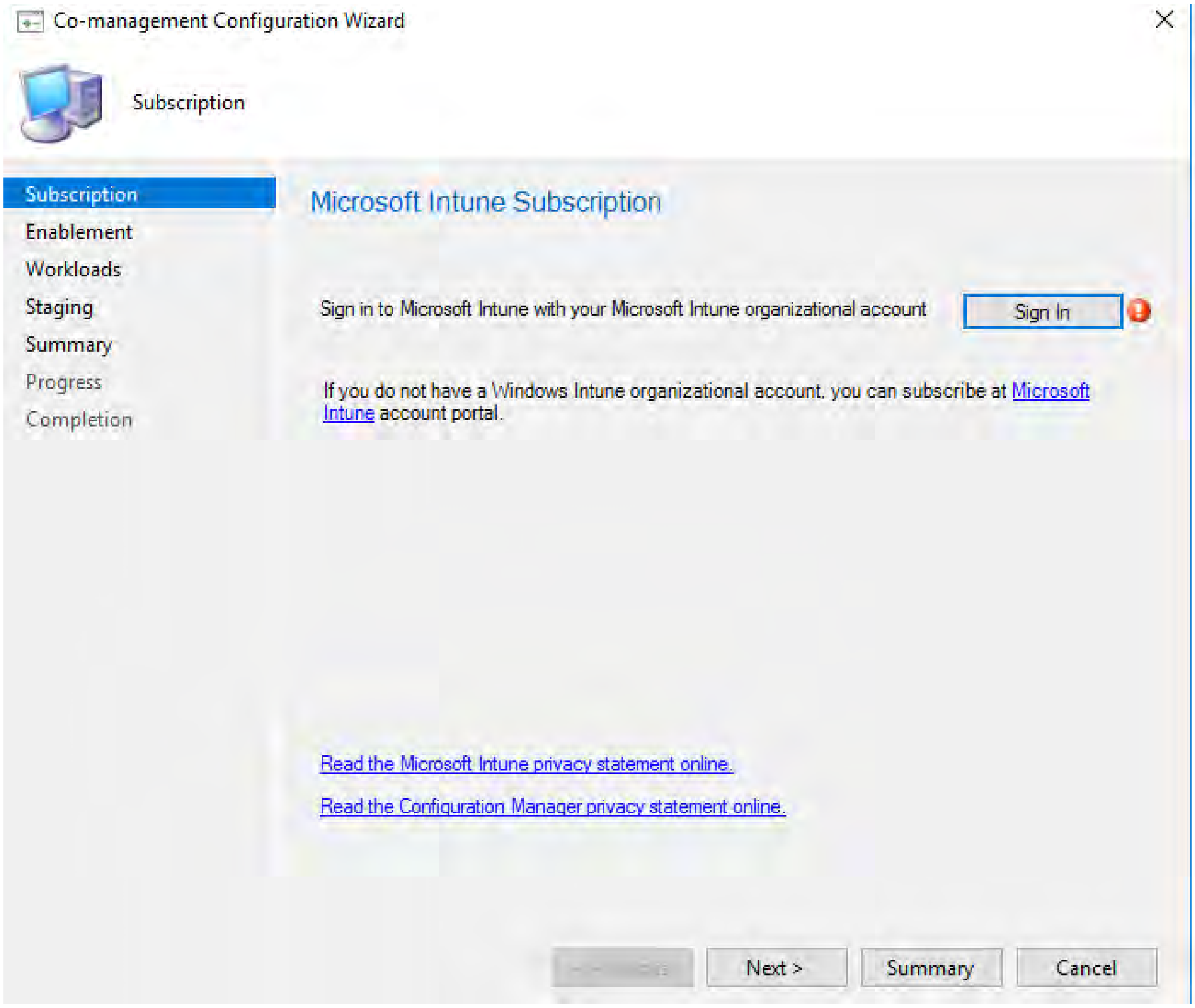
Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.

Specify if client computers can use cloud-based services.

**Device/User Settings**

| | |
|---|---|
| Allow access to cloud distribution point | Yes |
| Automatically register new Windows 10 domain joined devices with Azure Active Directory | Yes |
| Enable clients to use a cloud management gateway | Yes |

Now we will complete co-management



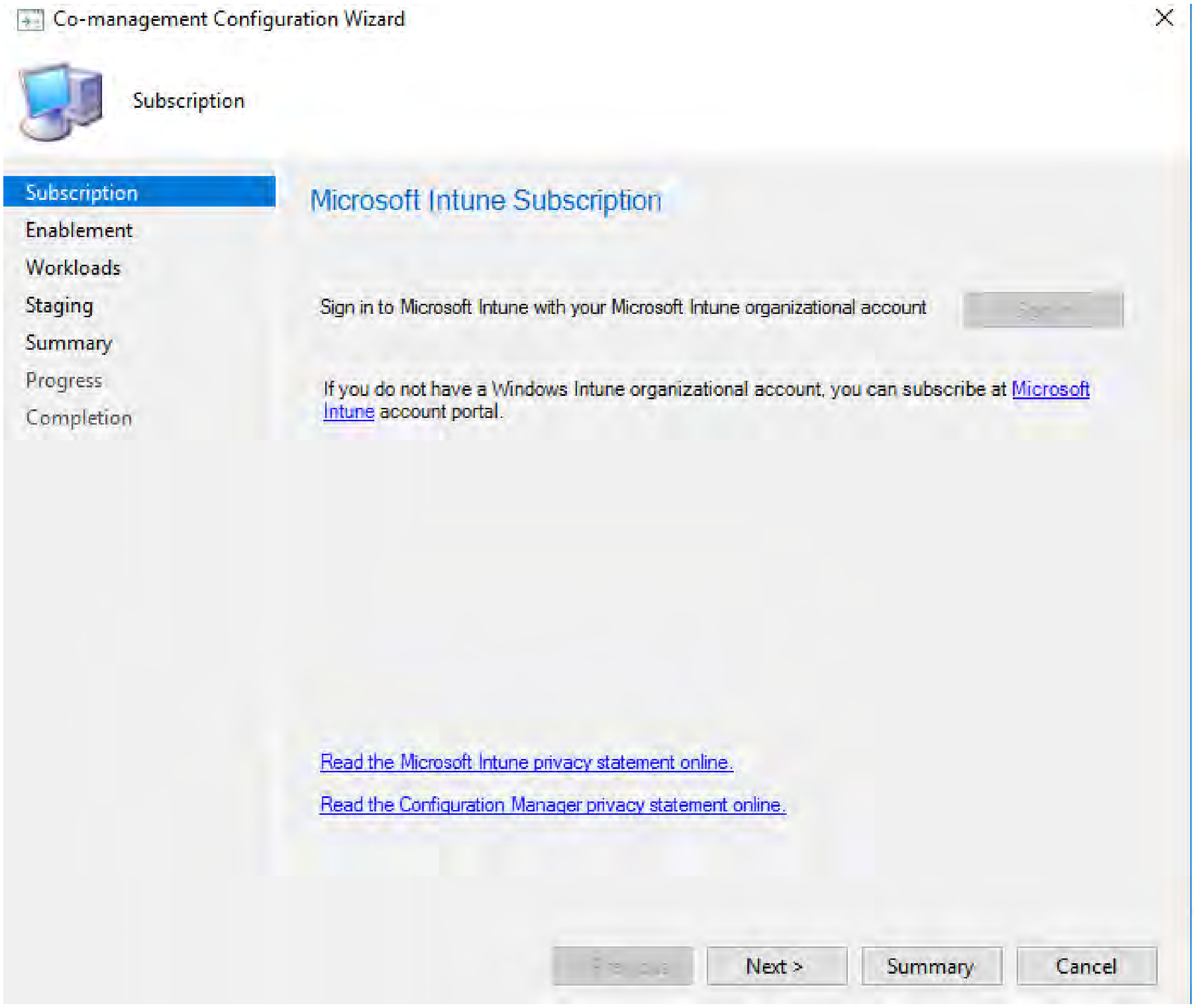
Microsoft Intune Subscription

Sign in to Microsoft Intune with your Microsoft Intune organizational account

If you do not have a Windows Intune organizational account, you can subscribe at Microsoft Intune account portal.

Read the Microsoft Intune privacy statement online.

Read the Configuration Manager privacy statement online.



Microsoft Intune Subscription

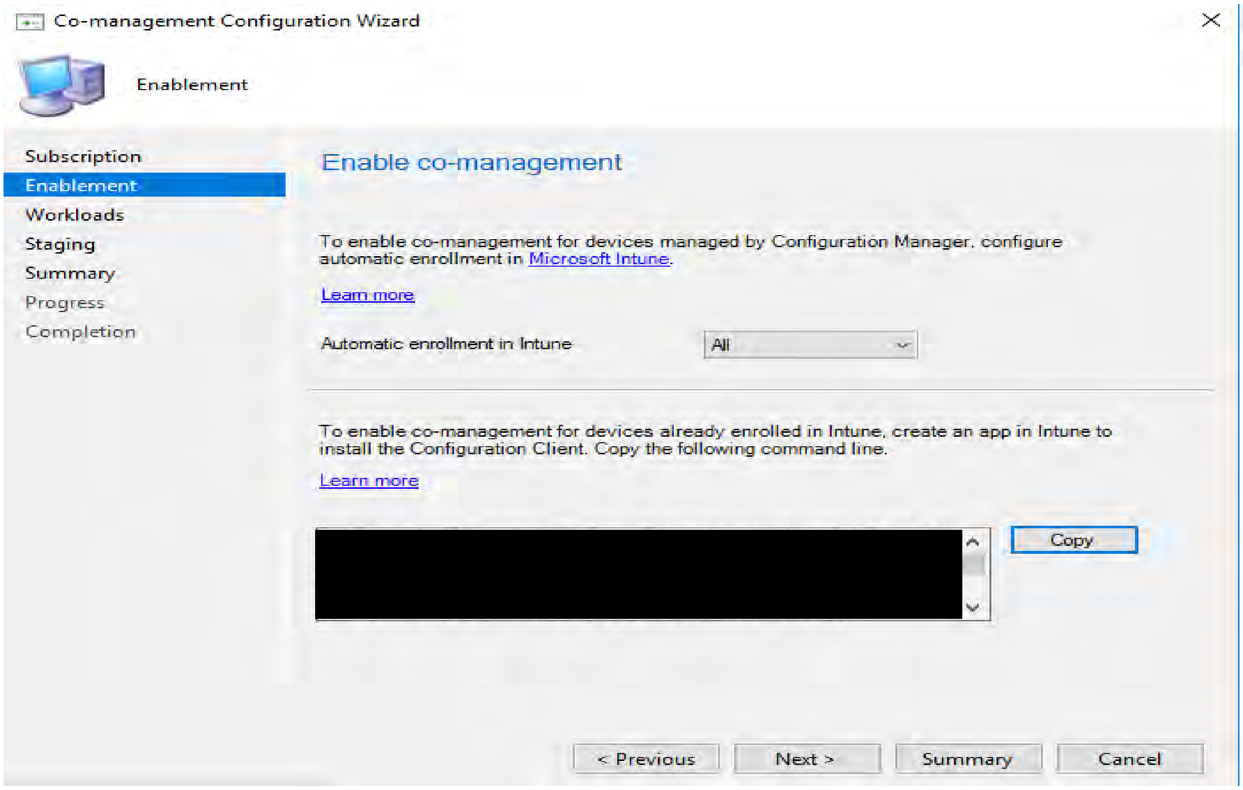
Sign in to Microsoft Intune with your Microsoft Intune organizational account

If you do not have a Windows Intune organizational account, you can subscribe at Microsoft Intune account portal.

Read the Microsoft Intune privacy statement online.

Read the Configuration Manager privacy statement online.

```
CCMSETUPCMD="/mp:https://RAMLAN.CLOUDAPP.NET/CCM_Proxy_MutualAuth/72057594037927939
CCMHOSTNAME=RAMLAN.CLOUDAPP.NET/CCM_Proxy_MutualAuth/72057594037927939
SMSSiteCode=CAN SMSMP=https://CM.RAMLAN.CA AADTENANTID=5E11113D-DA15-40E6-B616-
07C2F4956166 AADCLIENTAPPID=d5ce304e-84c4-450f-9f1a-c936f9ddb5fb
AADRESOURCEURI=https://ConfigMgrService
SMSPublicRootKey=0602000000A400005253413100080000010001003396EEFE03BC76E34B4B1D12735
08F0E3AC25FC4D3D16A384A7A28DA2AB3777AB15A355D61FC873BD1905E2DB587F329EADD0E4CE888
5B8A29F54BE99BCECDE30FD31CAC3A56CA296D2FDFBBF5AE0A15AFDCEDE70B7986008D2772B143F06
3DB35220811180B852DBB9FC7385E6D2BC4DA5259E80A89E3785EAABD6C9B2A2FE0F47F24F21029409
2CAE66A60214BA17120448972223A7A529B5C7864420D33CFCE4CFE1AA527B817A8C67838B1328233C
6D6C10C58318D4658C7026E34E70253D59D4212FDFFEE086A8A0EBD5CAE6C19A5A890118A6D5CF462
D7966A0B90E51C0E4E4A74E476774E10A38563C2DFB62CE16068AD401013EE82AA4DAD66C8A9AE"
```



Enable co-management

To enable co-management for devices managed by Configuration Manager, configure automatic enrollment in Microsoft Intune.

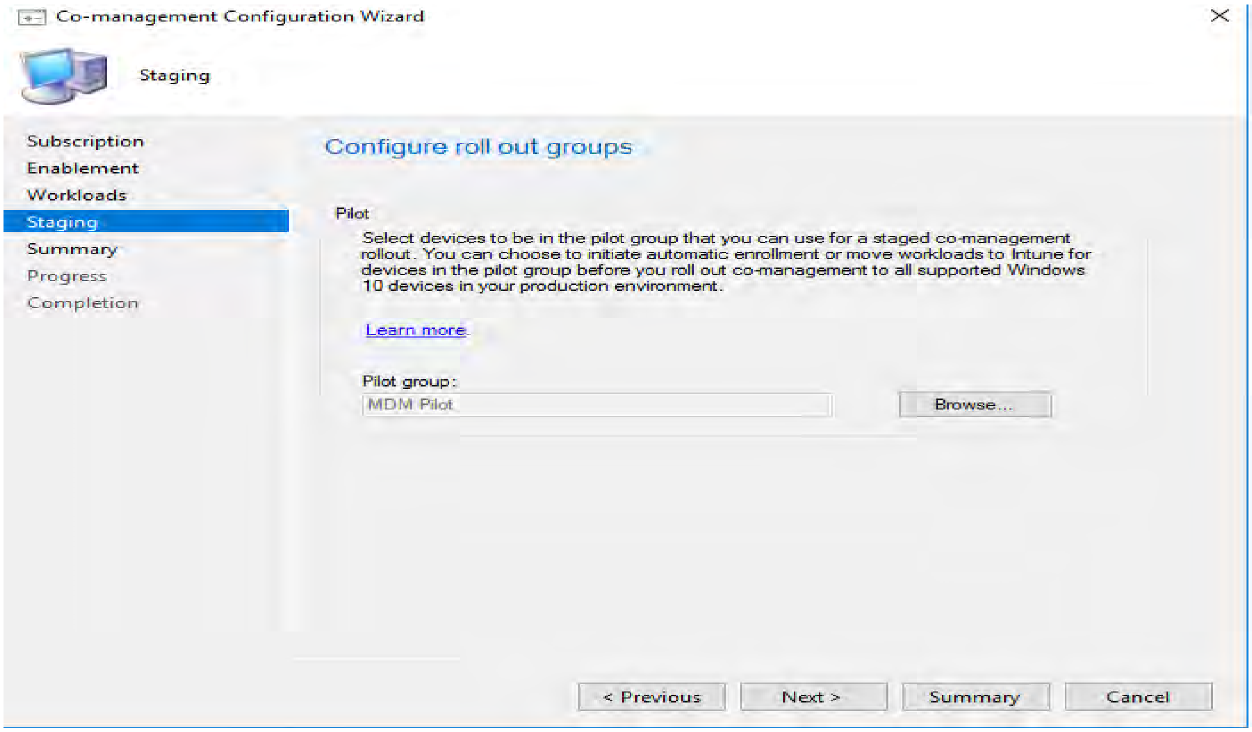
Learn more

Automatic enrollment in Intune: All

To enable co-management for devices already enrolled in Intune, create an app in Intune to install the Configuration Client. Copy the following command line.

Learn more

[redacted]



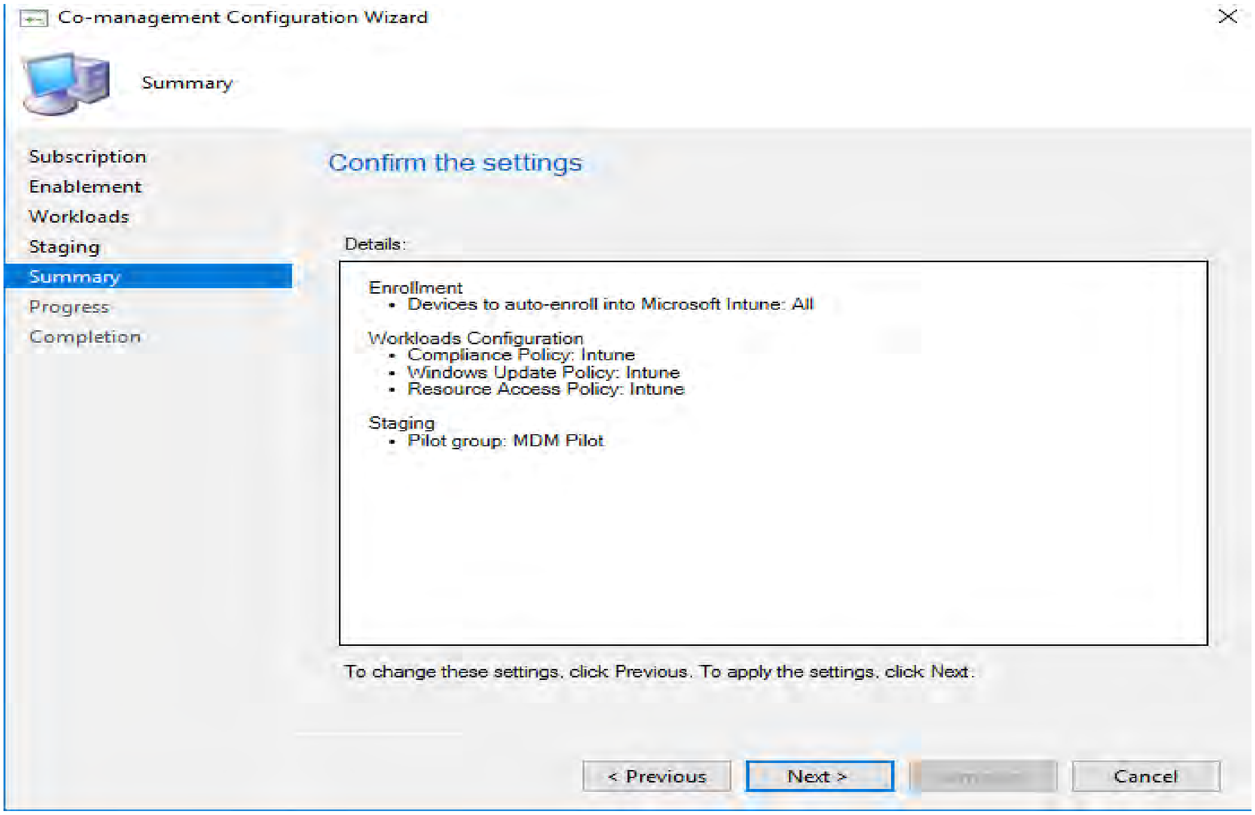
Configure roll out groups

Pilot

Select devices to be in the pilot group that you can use for a staged co-management rollout. You can choose to initiate automatic enrollment or move workloads to Intune for devices in the pilot group before you roll out co-management to all supported Windows 10 devices in your production environment.

Learn more

Pilot group: MDM Pilot



Confirm the settings

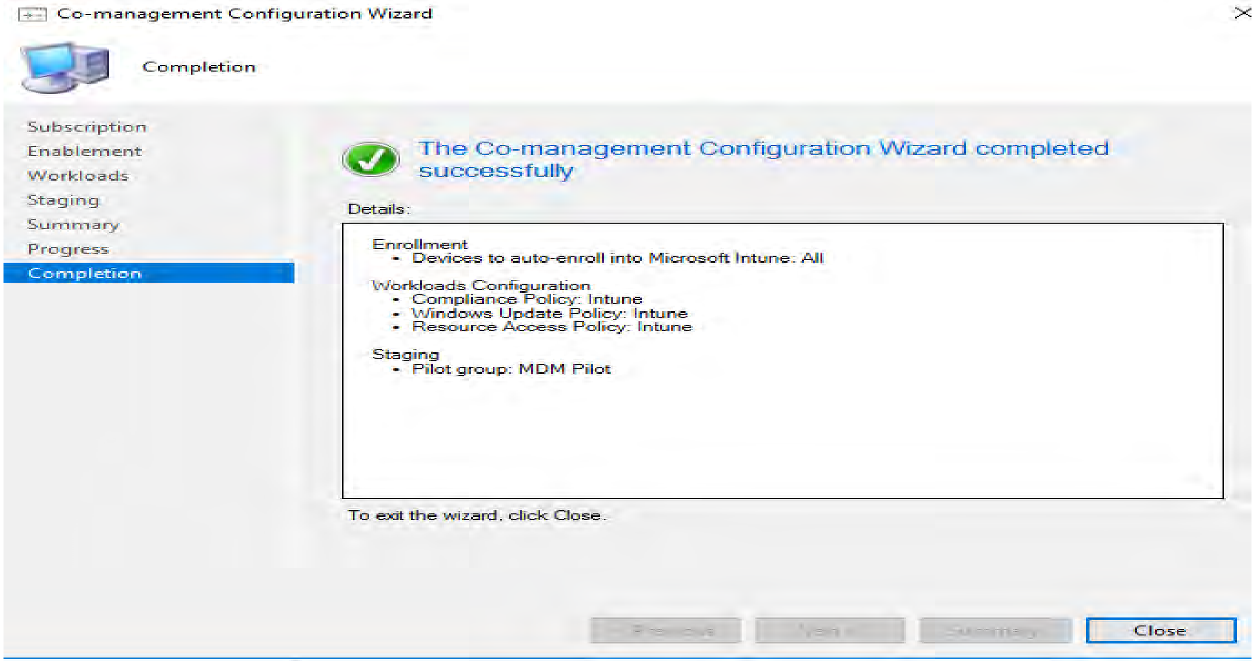
Details:

Enrollment
- Devices to auto-enroll into Microsoft Intune: All

Workloads Configuration
- Compliance Policy: Intune
- Windows Update Policy: Intune
- Resource Access Policy: Intune

Staging
- Pilot group: MDM Pilot

To change these settings, click Previous. To apply the settings, click Next.



The Co-management Configuration Wizard completed successfully

Details:

Enrollment
- Devices to auto-enroll into Microsoft Intune: All

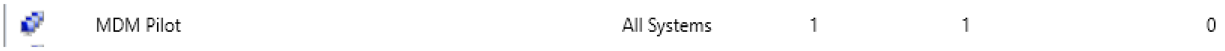
Workloads Configuration
- Compliance Policy: Intune
- Windows Update Policy: Intune
- Resource Access Policy: Intune

Staging
- Pilot group: MDM Pilot

To exit the wizard, click Close.

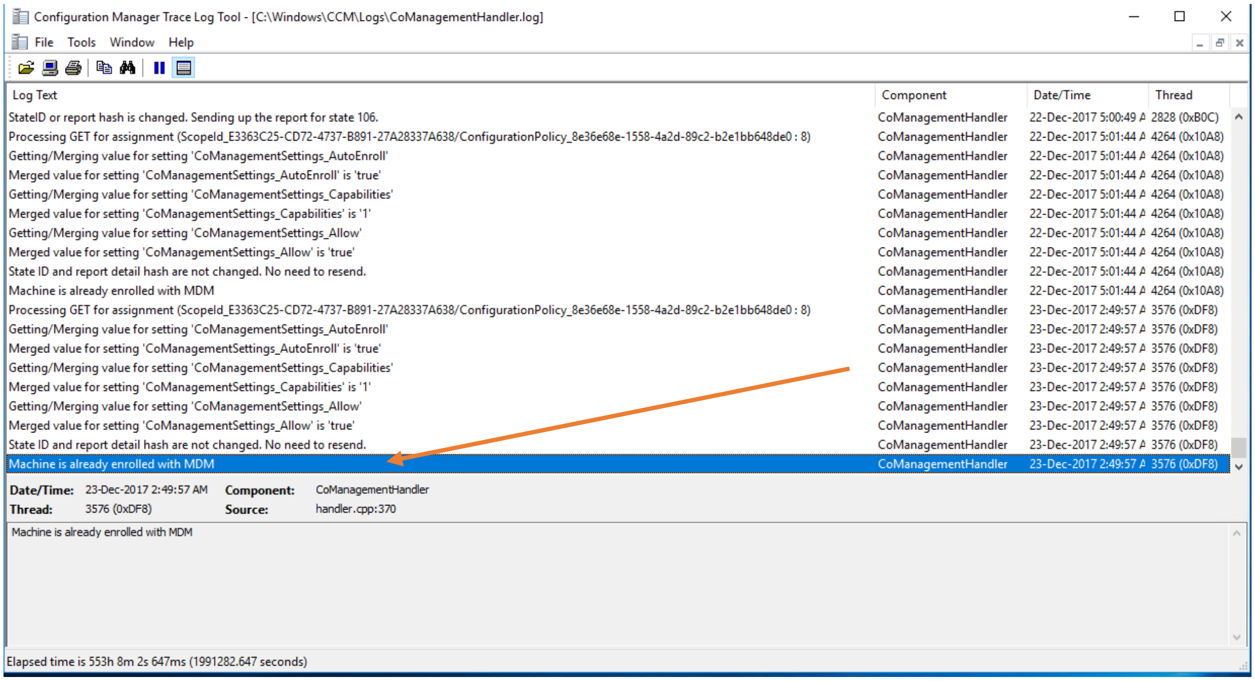
You might be wondering what is MDM pilot (Pilot Group). It is a collection that, I created and added 1 Windows 10 machine for co management testing. Here is the screen shot

Assets and Compliance – Device Collections – MDM Pilot



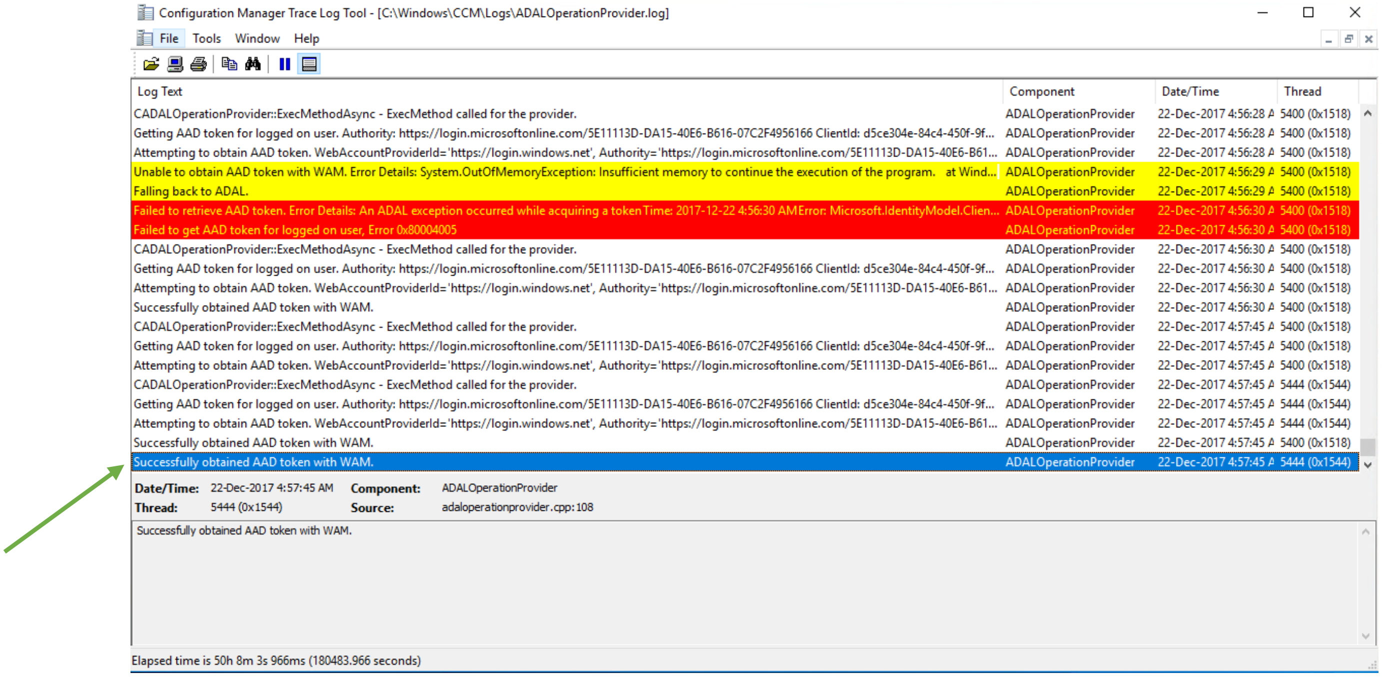
| | | | | |
|---|---|---|---|---|
| MDM Pilot | All Systems | 1 | 1 | 0 |

These are the logs you have to monitor for co management successful MDM enrollment:



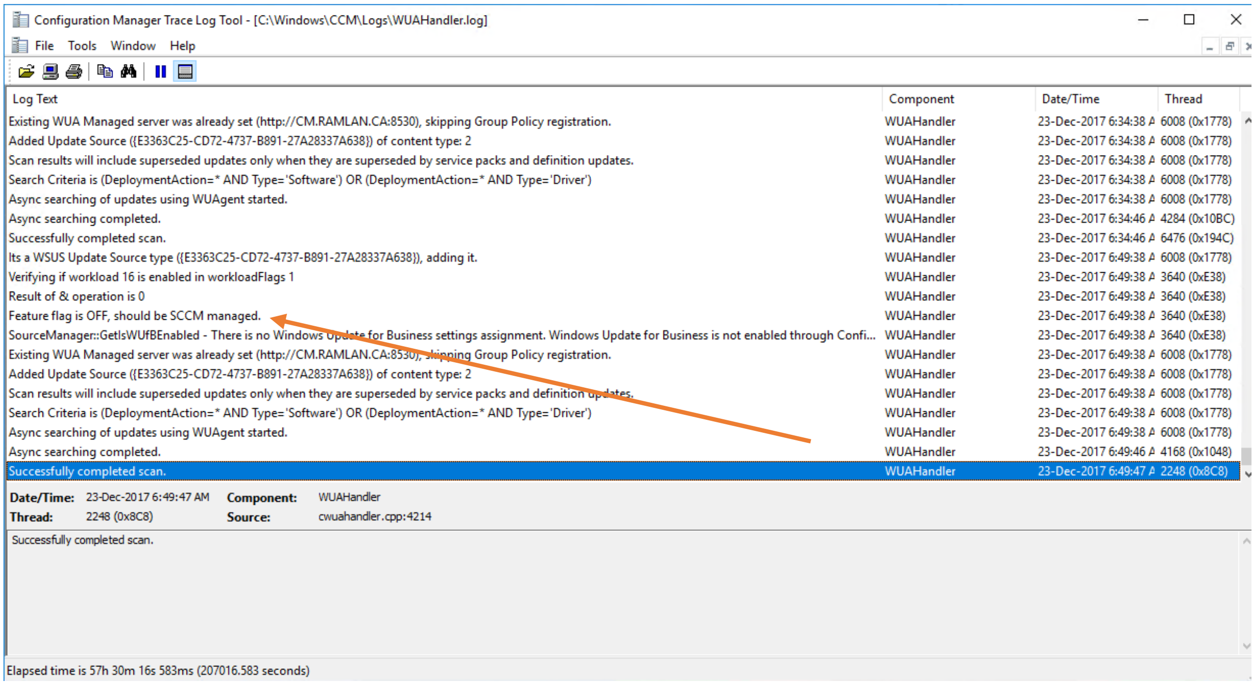
Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\CoManagementHandler.log]

```
Log Text                                                                                                                      Component              Date/Time               Thread
StateID or report hash is changed. Sending up the report for state 106.                                                        CoManagementHandler    22-Dec-2017 5:00:49 A   2828 (0xB0C)
Processing GET for assignment (ScopeId_E3363C25-CD72-4737-B891-27A28337A638/ConfigurationPolicy_8e36e68e-1558-4a2d-89c2-b2e1bb648de0 : 8)   CoManagementHandler    22-Dec-2017 5:01:44 A   4264 (0x10A8)
Getting/Merging value for setting 'CoManagementSettings_AutoEnroll'                                                            CoManagementHandler    22-Dec-2017 5:01:44 A   4264 (0x10A8)
Merged value for setting 'CoManagementSettings_AutoEnroll' is 'true'                                                           CoManagementHandler    22-Dec-2017 5:01:44 A   4264 (0x10A8)
Getting/Merging value for setting 'CoManagementSettings_Capabilities'                                                          CoManagementHandler    22-Dec-2017 5:01:44 A   4264 (0x10A8)
Merged value for setting 'CoManagementSettings_Capabilities' is '1'                                                            CoManagementHandler    22-Dec-2017 5:01:44 A   4264 (0x10A8)
Getting/Merging value for setting 'CoManagementSettings_Allow'                                                                 CoManagementHandler    22-Dec-2017 5:01:44 A   4264 (0x10A8)
Merged value for setting 'CoManagementSettings_Allow' is 'true'                                                                CoManagementHandler    22-Dec-2017 5:01:44 A   4264 (0x10A8)
State ID and report detail hash are not changed. No need to resend.                                                            CoManagementHandler    22-Dec-2017 5:01:44 A   4264 (0x10A8)
Machine is already enrolled with MDM                                                                                           CoManagementHandler    22-Dec-2017 5:01:44 A   4264 (0x10A8)
Processing GET for assignment (ScopeId_E3363C25-CD72-4737-B891-27A28337A638/ConfigurationPolicy_8e36e68e-1558-4a2d-89c2-b2e1bb648de0 : 8)   CoManagementHandler    23-Dec-2017 2:49:57 A   3576 (0xDF8)
Getting/Merging value for setting 'CoManagementSettings_AutoEnroll'                                                            CoManagementHandler    23-Dec-2017 2:49:57 A   3576 (0xDF8)
Merged value for setting 'CoManagementSettings_AutoEnroll' is 'true'                                                           CoManagementHandler    23-Dec-2017 2:49:57 A   3576 (0xDF8)
Getting/Merging value for setting 'CoManagementSettings_Capabilities'                                                          CoManagementHandler    23-Dec-2017 2:49:57 A   3576 (0xDF8)
Merged value for setting 'CoManagementSettings_Capabilities' is '1'                                                            CoManagementHandler    23-Dec-2017 2:49:57 A   3576 (0xDF8)
Getting/Merging value for setting 'CoManagementSettings_Allow'                                                                 CoManagementHandler    23-Dec-2017 2:49:57 A   3576 (0xDF8)
Merged value for setting 'CoManagementSettings_Allow' is 'true'                                                                CoManagementHandler    23-Dec-2017 2:49:57 A   3576 (0xDF8)
State ID and report detail hash are not changed. No need to resend.                                                            CoManagementHandler    23-Dec-2017 2:49:57 A   3576 (0xDF8)
Machine is already enrolled with MDM                                                                                           CoManagementHandler    23-Dec-2017 2:49:57 A   3576 (0xDF8)

Date/Time:  23-Dec-2017 2:49:57 AM     Component:  CoManagementHandler
Thread:     3576 (0xDF8)               Source:     handler.cpp:370

Machine is already enrolled with MDM

Elapsed time is 553h 8m 2s 647ms (1991282.647 seconds)
```



Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\ADALOperationProvider.log]

```
Log Text                                                                                                                            Component              Date/Time               Thread
CADALOperationProvider::ExecMethodAsync - ExecMethod called for the provider.                                                         ADALOperationProvider  22-Dec-2017 4:56:28 A   5400 (0x1518)
Getting AAD token for logged on user. Authority: https://login.microsoftonline.com/5E11113D-DA15-40E6-B616-07C2F4956166 ClientId: d5ce304e-84c4-450f-9f...   ADALOperationProvider  22-Dec-2017 4:56:28 A   5400 (0x1518)
Attempting to obtain AAD token. WebAccountProviderId='https://login.windows.net', Authority='https://login.microsoftonline.com/5E11113D-DA15-40E6-B61...   ADALOperationProvider  22-Dec-2017 4:56:28 A   5400 (0x1518)
Unable to obtain AAD token with WAM. Error Details: System.OutOfMemoryException: Insufficient memory to continue the execution of the program.   at Wind...   ADALOperationProvider  22-Dec-2017 4:56:29 A   5400 (0x1518)
Falling back to ADAL.                                                                                                                 ADALOperationProvider  22-Dec-2017 4:56:29 A   5400 (0x1518)
Failed to retrieve AAD token. Error Details: An ADAL exception occurred while acquiring a token Time: 2017-12-22 4:56:30 AM Error: Microsoft.IdentityModel.Clien...   ADALOperationProvider  22-Dec-2017 4:56:30 A   5400 (0x1518)
Failed to get AAD token for logged on user, Error 0x80004005                                                                          ADALOperationProvider  22-Dec-2017 4:56:30 A   5400 (0x1518)
CADALOperationProvider::ExecMethodAsync - ExecMethod called for the provider.                                                         ADALOperationProvider  22-Dec-2017 4:56:30 A   5400 (0x1518)
Getting AAD token for logged on user. Authority: https://login.microsoftonline.com/5E11113D-DA15-40E6-B616-07C2F4956166 ClientId: d5ce304e-84c4-450f-9f...   ADALOperationProvider  22-Dec-2017 4:56:30 A   5400 (0x1518)
Attempting to obtain AAD token. WebAccountProviderId='https://login.windows.net', Authority='https://login.microsoftonline.com/5E11113D-DA15-40E6-B61...   ADALOperationProvider  22-Dec-2017 4:56:30 A   5400 (0x1518)
Successfully obtained AAD token with WAM.                                                                                             ADALOperationProvider  22-Dec-2017 4:56:30 A   5400 (0x1518)
CADALOperationProvider::ExecMethodAsync - ExecMethod called for the provider.                                                         ADALOperationProvider  22-Dec-2017 4:57:45 A   5400 (0x1518)
Getting AAD token for logged on user. Authority: https://login.microsoftonline.com/5E11113D-DA15-40E6-B616-07C2F4956166 ClientId: d5ce304e-84c4-450f-9f...   ADALOperationProvider  22-Dec-2017 4:57:45 A   5400 (0x1518)
Attempting to obtain AAD token. WebAccountProviderId='https://login.windows.net', Authority='https://login.microsoftonline.com/5E11113D-DA15-40E6-B61...   ADALOperationProvider  22-Dec-2017 4:57:45 A   5400 (0x1518)
CADALOperationProvider::ExecMethodAsync - ExecMethod called for the provider.                                                         ADALOperationProvider  22-Dec-2017 4:57:45 A   5444 (0x1544)
Getting AAD token for logged on user. Authority: https://login.microsoftonline.com/5E11113D-DA15-40E6-B616-07C2F4956166 ClientId: d5ce304e-84c4-450f-9f...   ADALOperationProvider  22-Dec-2017 4:57:45 A   5444 (0x1544)
Attempting to obtain AAD token. WebAccountProviderId='https://login.windows.net', Authority='https://login.microsoftonline.com/5E11113D-DA15-40E6-B61...   ADALOperationProvider  22-Dec-2017 4:57:45 A   5444 (0x1544)
Successfully obtained AAD token with WAM.                                                                                             ADALOperationProvider  22-Dec-2017 4:57:45 A   5400 (0x1518)
Successfully obtained AAD token with WAM.                                                                                             ADALOperationProvider  22-Dec-2017 4:57:45 A   5444 (0x1544)

Date/Time:  22-Dec-2017 4:57:45 AM     Component:  ADALOperationProvider
Thread:     5444 (0x1544)              Source:     adaloperationprovider.cpp:108

Successfully obtained AAD token with WAM.

Elapsed time is 50h 8m 3s 966ms (180483.966 seconds)
```

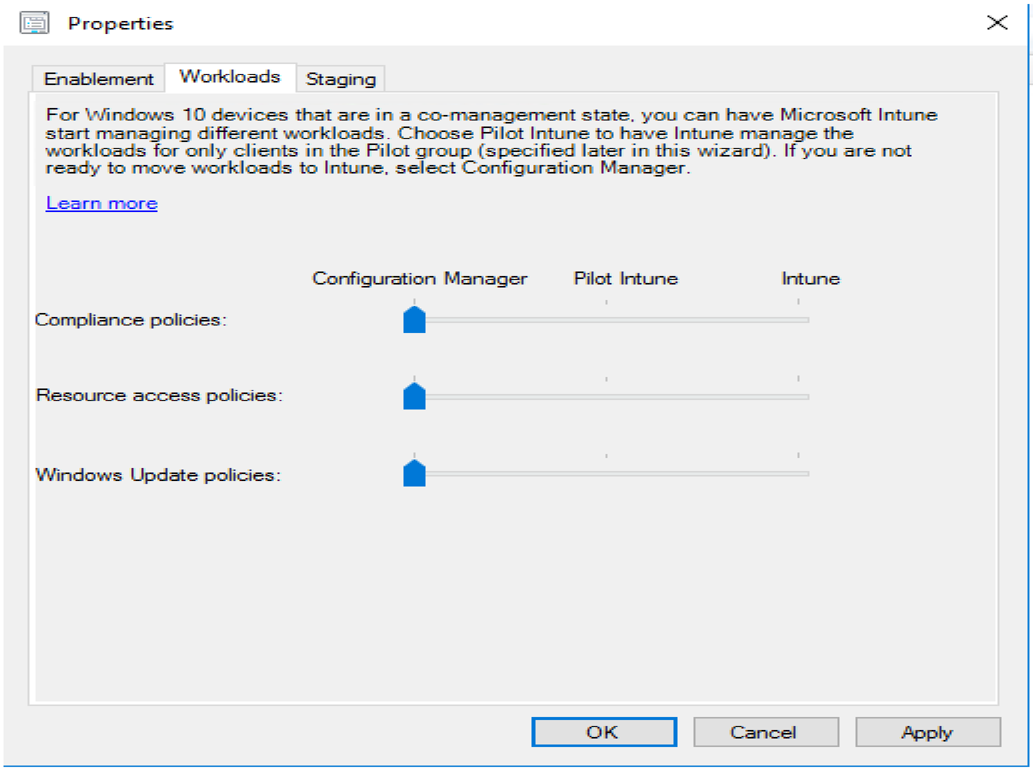


Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\WUAHandler.log]
File
Tools
Window
Help

```
Log Text                                                                                                              Component     Date/Time              Thread
Existing WUA Managed server was already set (http://CM.RAMLAN.CA:8530), skipping Group Policy registration.             WUAHandler    23-Dec-2017 6:34:38 A  6008 (0x1778)
Added Update Source ({E3363C25-CD72-4737-B891-27A28337A638}) of content type: 2                                         WUAHandler    23-Dec-2017 6:34:38 A  6008 (0x1778)
Scan results will include superseded updates only when they are superseded by service packs and definition updates.     WUAHandler    23-Dec-2017 6:34:38 A  6008 (0x1778)
Search Criteria is (DeploymentAction=* AND Type='Software') OR (DeploymentAction=* AND Type='Driver')                  WUAHandler    23-Dec-2017 6:34:38 A  6008 (0x1778)
Async searching of updates using WUAgent started.                                                                       WUAHandler    23-Dec-2017 6:34:38 A  6008 (0x1778)
Async searching completed.                                                                                              WUAHandler    23-Dec-2017 6:34:46 A  4284 (0x10BC)
Successfully completed scan.                                                                                            WUAHandler    23-Dec-2017 6:34:46 A  6476 (0x194C)
Its a WSUS Update Source type ({E3363C25-CD72-4737-B891-27A28337A638}), adding it.                                      WUAHandler    23-Dec-2017 6:49:38 A  6008 (0x1778)
Verifying if workload 16 is enabled in workloadFlags 1                                                                  WUAHandler    23-Dec-2017 6:49:38 A  3640 (0xE38)
Result of & operation is 0                                                                                              WUAHandler    23-Dec-2017 6:49:38 A  3640 (0xE38)
Feature flag is OFF, should be SCCM managed.                                                                            WUAHandler    23-Dec-2017 6:49:38 A  3640 (0xE38)
SourceManager::GetIsWUfBEnabled - There is no Windows Update for Business settings assignment. Windows Update for Business is not enabled through Confi...  WUAHandler    23-Dec-2017 6:49:38 A  3640 (0xE38)
Existing WUA Managed server was already set (http://CM.RAMLAN.CA:8530), skipping Group Policy registration.             WUAHandler    23-Dec-2017 6:49:38 A  6008 (0x1778)
Added Update Source ({E3363C25-CD72-4737-B891-27A28337A638}) of content type: 2                                         WUAHandler    23-Dec-2017 6:49:38 A  6008 (0x1778)
Scan results will include superseded updates only when they are superseded by service packs and definition updates.     WUAHandler    23-Dec-2017 6:49:38 A  6008 (0x1778)
Search Criteria is (DeploymentAction=* AND Type='Software') OR (DeploymentAction=* AND Type='Driver')                  WUAHandler    23-Dec-2017 6:49:38 A  6008 (0x1778)
Async searching of updates using WUAgent started.                                                                       WUAHandler    23-Dec-2017 6:49:38 A  6008 (0x1778)
Async searching completed.                                                                                              WUAHandler    23-Dec-2017 6:49:46 A  4168 (0x1048)
Successfully completed scan.                                                                                            WUAHandler    23-Dec-2017 6:49:47 A  2248 (0x8C8)

Date/Time:  23-Dec-2017 6:49:47 AM    Component:  WUAHandler
Thread:     2248 (0x8C8)              Source:     cwuahandler.cpp:4214

Successfully completed scan.

Elapsed time is 57h 30m 16s 583ms (207016.583 seconds)
```

As you can see from WUAHandler log it says SCCM managed.  It should say managed by INTUNE.  I had to play around to get MDM enrollment successful for a while and finally had to change the settings from Pilot to Configuration Manager.  This is where you can change the settings.

### Administration – Co Management - Properties



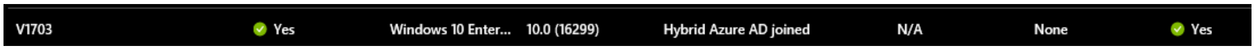
For Windows 10 devices that are in a co-management state, you can have Microsoft Intune start managing different workloads. Choose Pilot Intune to have Intune manage the workloads for only clients in the Pilot group (specified later in this wizard). If you are not ready to move workloads to Intune, select Configuration Manager.

Learn more

| | Configuration Manager | Pilot Intune | Intune |
|---|---|---|---|
| Compliance policies: | ● | | |
| Resource access policies: | ● | | |
| Windows Update policies: | ● | | |

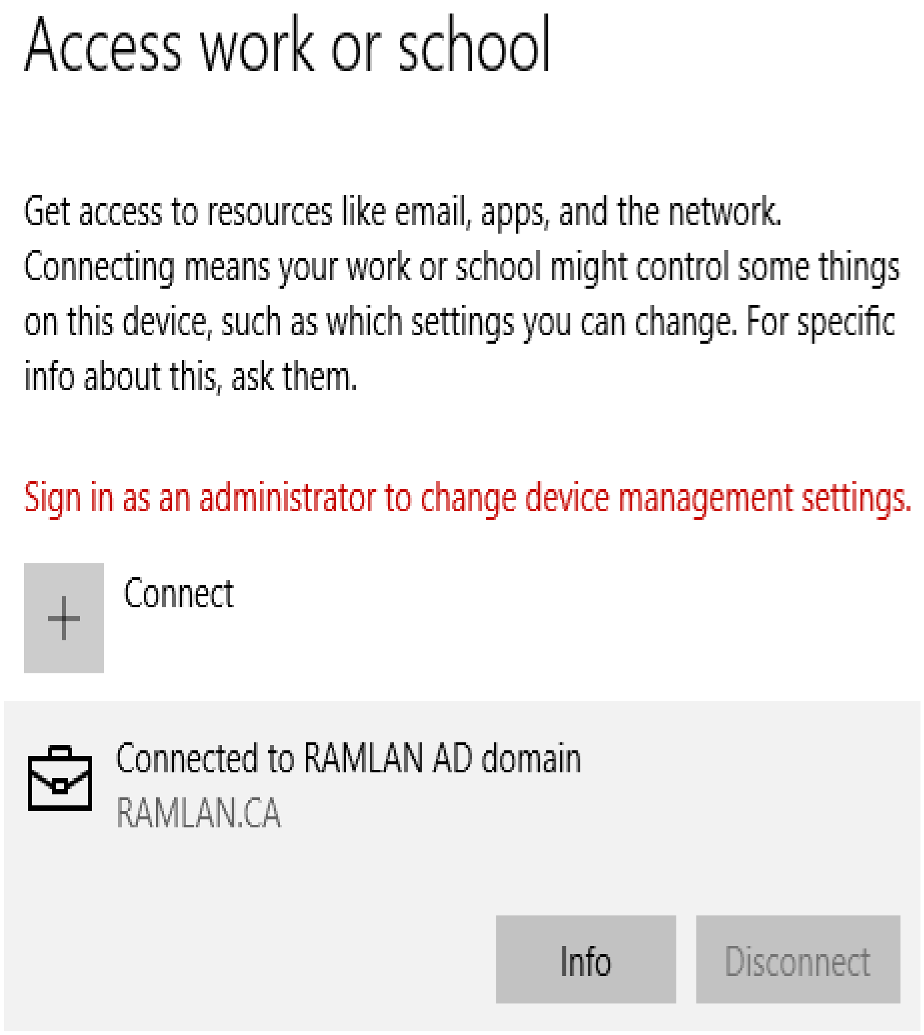
You can also check whether the device is enrolled to INTUNE from Azure, from Windows 10 machine & Configuration Manager Console as well.  Below are the screen shots

**Azure – Microsoft Intune – Device – Azure AD Devices**



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| V1703 | ✓ Yes | Windows 10 Enter... | 10.0 (16299) | Hybrid Azure AD joined | N/A | None | ✓ Yes |

**From Windows 10 System – Settings – Account**

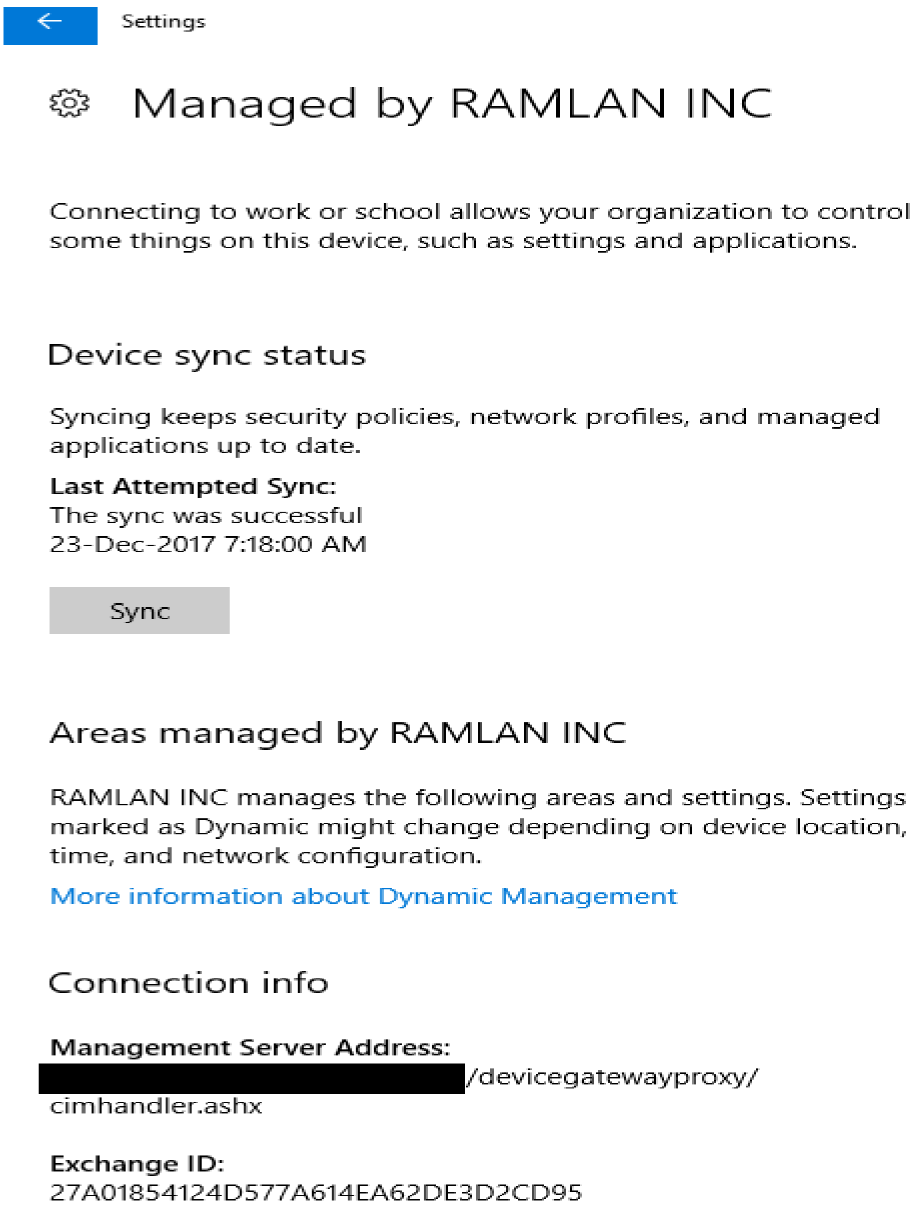


Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Sign in as an administrator to change device management settings.

Connected to RAMLAN AD domain
RAMLAN.CA



← Settings

## Managed by RAMLAN INC

Connecting to work or school allows your organization to control some things on this device, such as settings and applications.

### Device sync status

Syncing keeps security policies, network profiles, and managed applications up to date.

**Last Attempted Sync:**
The sync was successful
23-Dec-2017 7:18:00 AM

Sync

### Areas managed by RAMLAN INC

RAMLAN INC manages the following areas and settings. Settings marked as Dynamic might change depending on device location, time, and network configuration.

More information about Dynamic Management

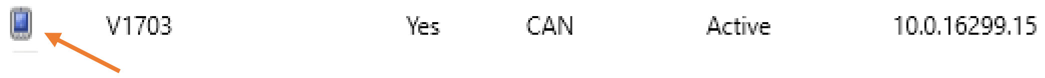
### Connection info

**Management Server Address:**
[redacted]/devicegatewayproxy/cimhandler.ashx

**Exchange ID:**
27A01854124D577A614EA62DE3D2CD95

From Configuration Manager Console

**Asset and Compliance - Devices**



| | | | | | |
|---|---|---|---|---|---|
| 📱 | V1703 | Yes | CAN | Active | 10.0.16299.15 |

See the ICON for Windows 10 V1703 – looks like Phone because it is treated as MOBILE device.

This concludes CMG, CDP and CO-MANAGEMENT configuration within CB1710.

**Just a note to all those who want to carry out this configuration in Home Lab. It will cost you around $2 per day within Azure for CMG and CDP service provided by Microsoft. So plan accordingly.**

Thanks

**Ram – 23rd Dec 2017**