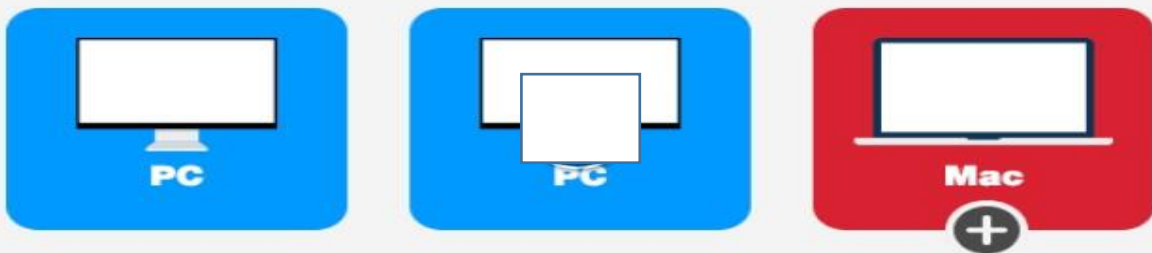


### What is Parallels Mac Management for SCCM?

For companies that already use Microsoft® SCCM for managing PCs, Parallels® Mac Management for Microsoft SCCM allows IT to maximize investments. It enables administrators to leverage existing processes by using SCCM as the single pane of glass to manage both PCs and Mac® computers.

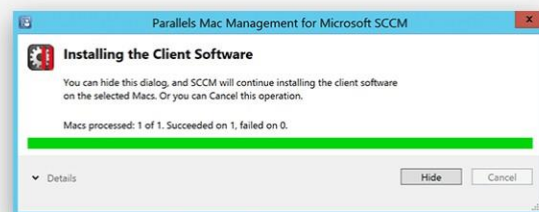
- Unified endpoint management for PCs and Mac® computers
- Effortlessly plugs in to existing SCCM infrastructure
- Full Mac lifecycle management
- Maximize your Microsoft® SCCM investment



**Extend your Microsoft SCCM to  
manage Mac computers like you  
manage Windows PCs.**

#### Mac Discovery and Enrollment

- Scan and discover Mac computers on your network.
- Enroll Mac computers via SCCM Active Directory System Discovery.
- Enroll Mac computers into SCCM via unique integration of Apple® Device Enrollment Program (DEP) and Parallels Mac Management.



#### macOS® Image Deployment and Patch Management

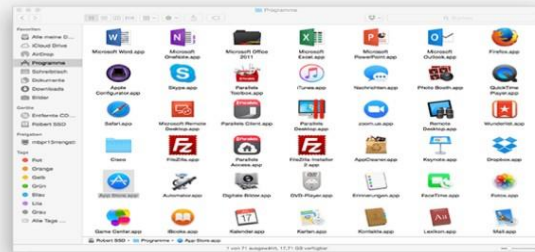
- Use familiar SCCM Task Sequence steps to deploy your corporate macOS base image, applications, and settings to Mac computers.
- Support for macOS updates is seamlessly integrated with SCCM software update features.

[Learn More »](#)



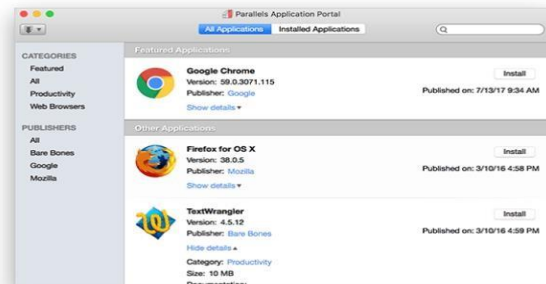
## Software Deployment via SCCM

- Deploy a wide range of packages: .dmg, .pkg, .iso, .app, scripts, and stand-alone files.
- Support for SCCM package and application deployment models.
- Flexible deployment options allow you to customize all aspects of the software deployment experience.



## Parallels Applications Portal

- Create a self-service library of approved applications for your end users.
- Allow end users to browse and install applications approved by IT.
- The end users can install approved applications even if they don't have administrative privileges on their Mac.



## Enforce Compliance via SCCM Baselines

- Enforce compliance on the Mac via SCCM configuration items and baselines.
- Configuration items tailored for Mac: macOS configuration profiles, FileVault® 2 disk encryption settings, and shell scripts.
- Monitor compliance status via SCCM reporting.



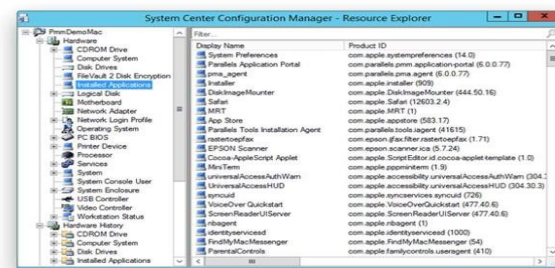
## New! Remote Lock and Wipe

- Initiate a remote wipe of a Mac that was lost, stolen, or for any other reason needs data to be erased.
- Lock Mac devices remotely.



## Inventory and Reporting

- Gather hardware and software inventory of your Mac computers.
- Report information about user log-ons.
- Leverage native Microsoft SCCM reports for details on Mac computers.



<https://www.parallels.com/ca/products/mac-management/>

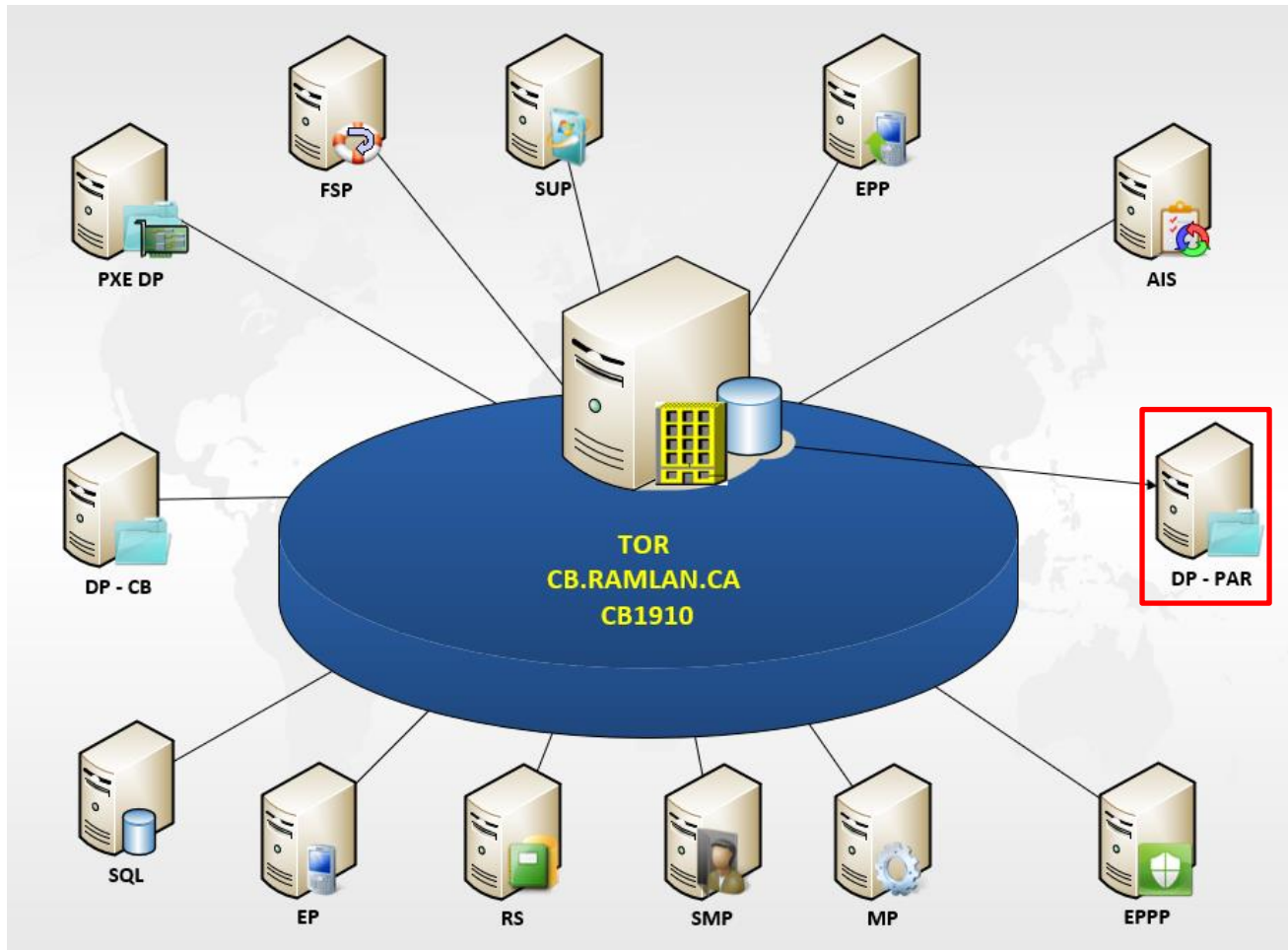
## PARALLEL MAC MANAGEMENT 8.1 FOR SCCM INSTALLATION NOTES

In this demo, I will walk you through the process of installing Parallel Mac Management 8.1 on CB1910 and Member Server **PAR**. This product will help manage Mac inventory through CB1910.

### My lab setup is as follows:

Configuration Manager CB1910 (**CB**) - Primary Site



Parallel Mac Management Member Server (**PAR**)

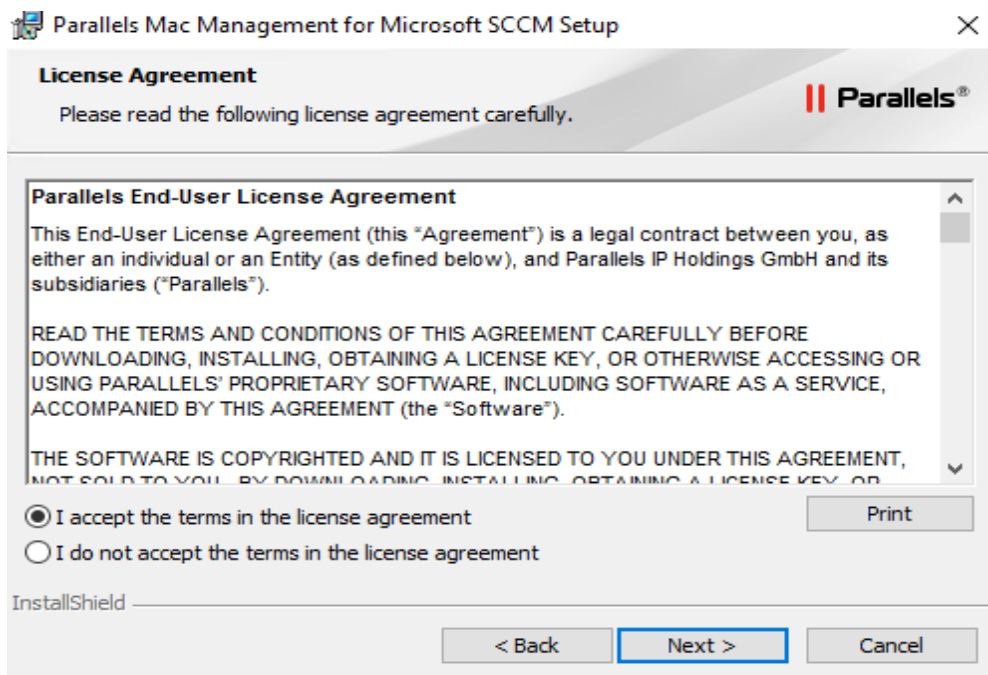
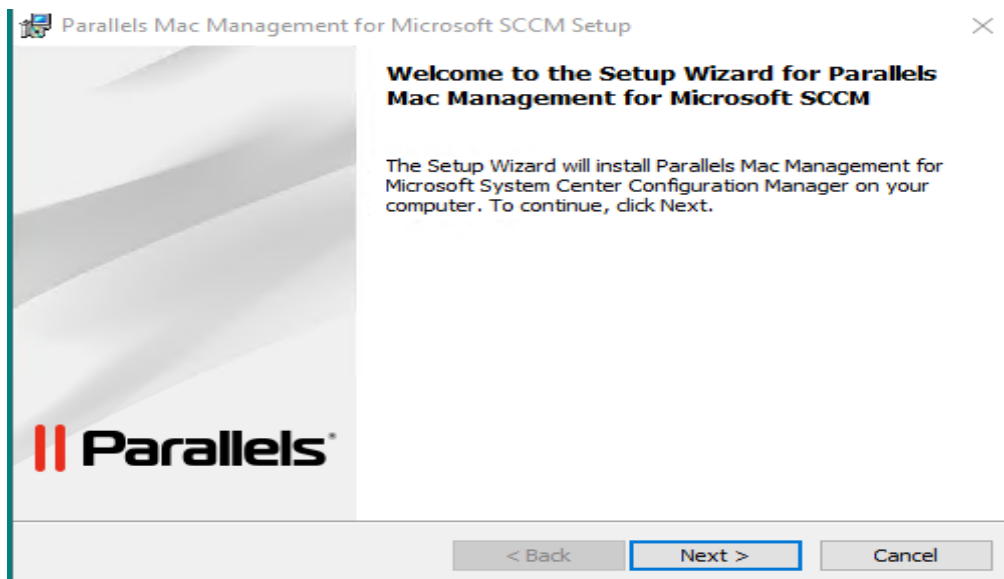


**PAR** is a member server running Windows Server 2019. I will be installing all the roles that are required to manage Parallel Mac Management.

**CB** is Primary Site Server running Windows Server 2019. On this server, I will install Parallel Mac Management Console extension only. Here is the screen shot.

Click Parallels Mac Management for SCCM.exe

Name	Date modified	Type	Size
 <a href="#">Parallels Mac Management for SCCM.exe</a>	<a href="#">12-Feb-2020 3:20 ...</a>	<a href="#">Application</a>	<a href="#">230,503 KB</a>
 <a href="#">PMM Prerequisites Checker.exe</a>	<a href="#">12-Feb-2020 3:19 ...</a>	<a href="#">Application</a>	<a href="#">7,393 KB</a>





Parallels Mac Management for Microsoft SCCM Setup



### Select Components

Check the components you want to install and uncheck the components you don't want to install.



☒ ConfigMgr Console Extension

☐ Configuration Manager Proxy

☐ IBCM Proxy

☐ MDM Server

☐ NetBoot Server

☐ OS X Software Update Point

Configuration Manager Console Extension extends the Configuration Manager console to provide a graphical user interface enabling you to manage Mac computers

Back

Next

Cancel

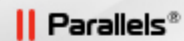


Parallels Mac Management for Microsoft SCCM Setup



### Ready to Install the Program

The wizard is ready to begin installation.



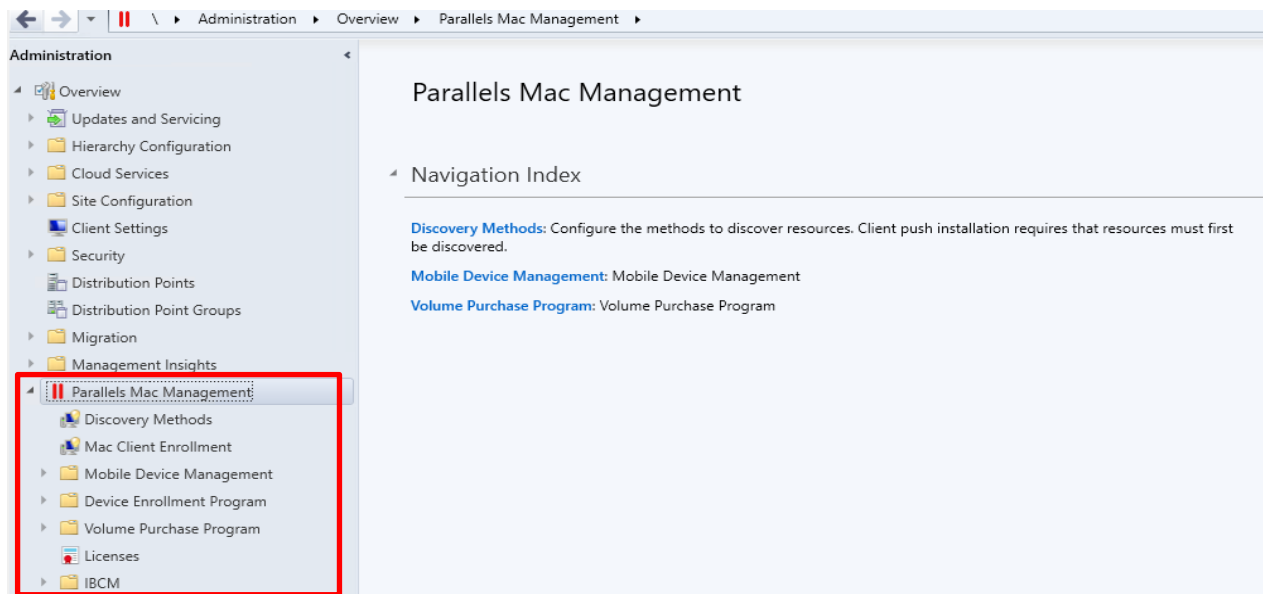
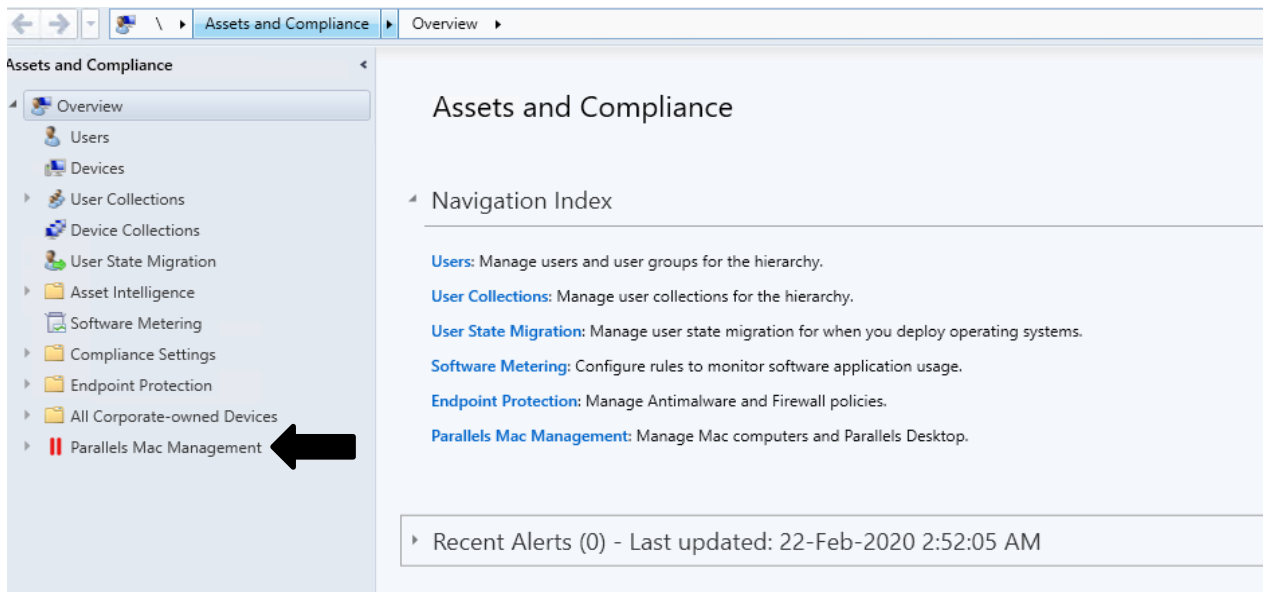
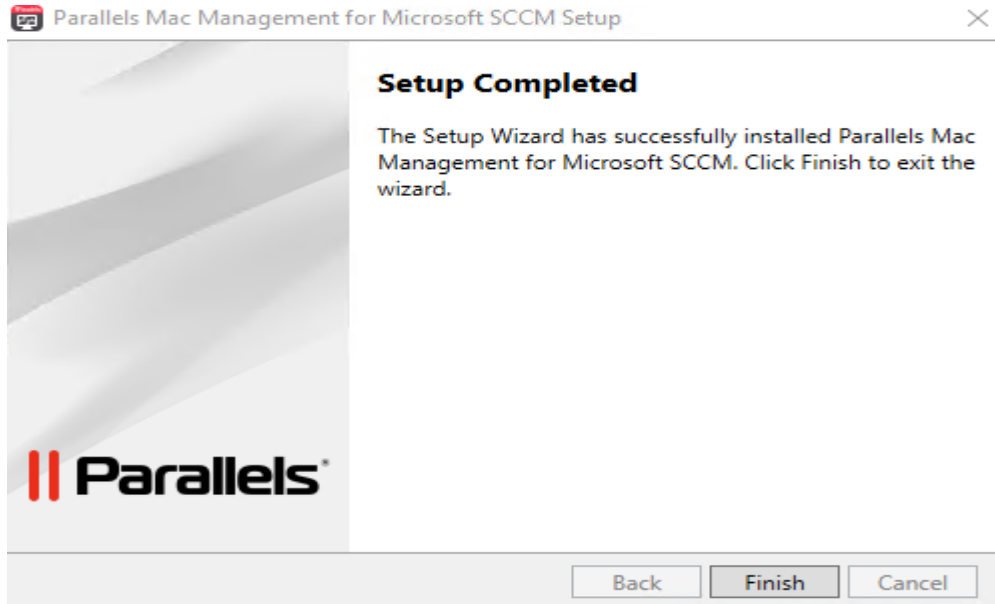
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Back

Install

Cancel



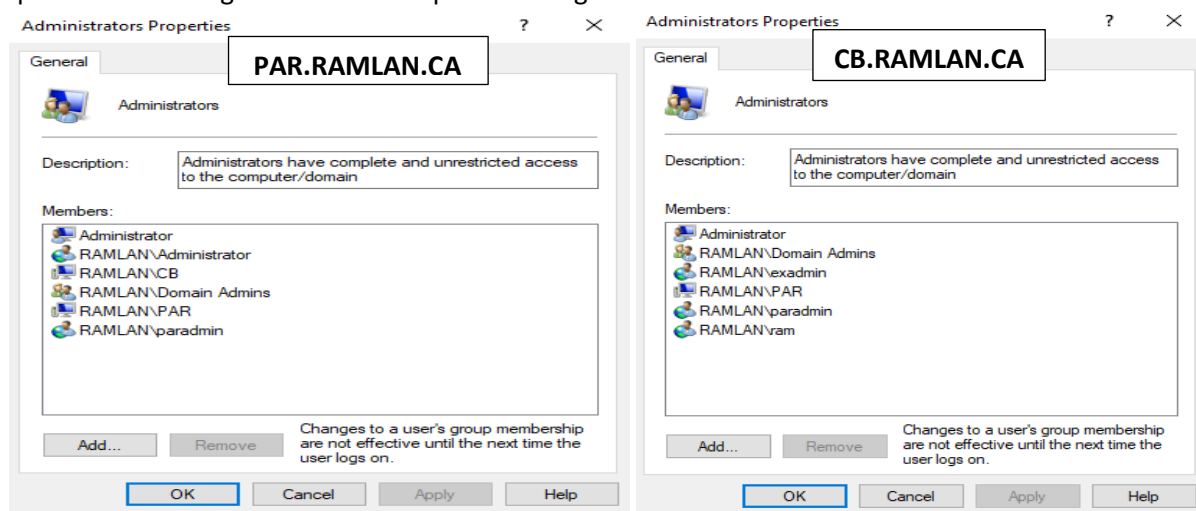


Now we move on to the Member server (**PAR**) and install remaining roles. Before we do, we need to take care of these pre req:

- Local Admin rights on this server (**PAR**) for Administrator user
- DCOM remote activation permission
- Administrator rights on Configuration Manager Console
- Permission in ADSI for ParallelServices / Program Data container
- Permission to SCCM Network share
- Certificates (Web Server & Workstation Authentication)
- DP Roles & Features, WSUS Roles & Features, WSUS Certificate
- DP Installation

### Local Admin Rights – PAR & CB

Open Server Manager – Tools – Computer Management

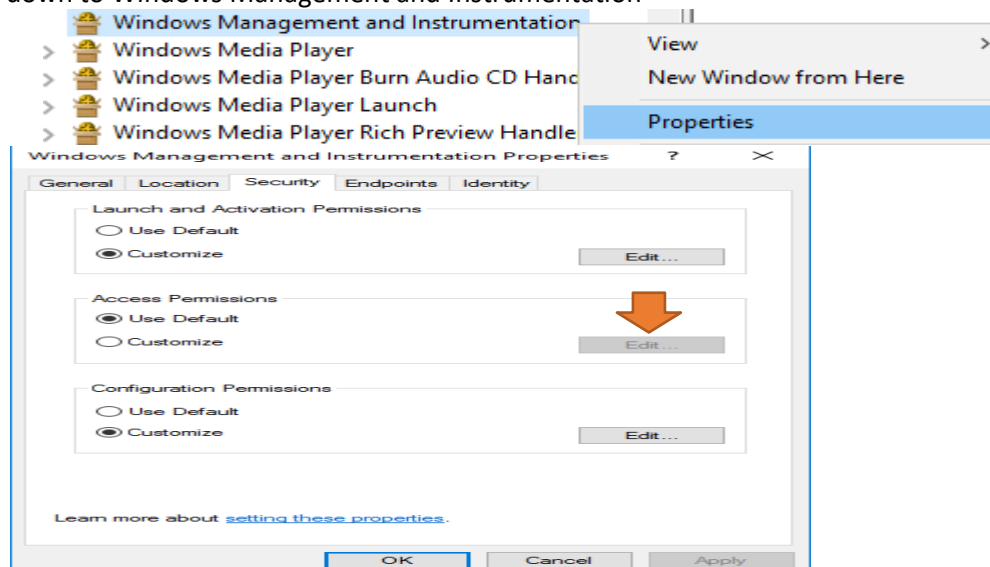


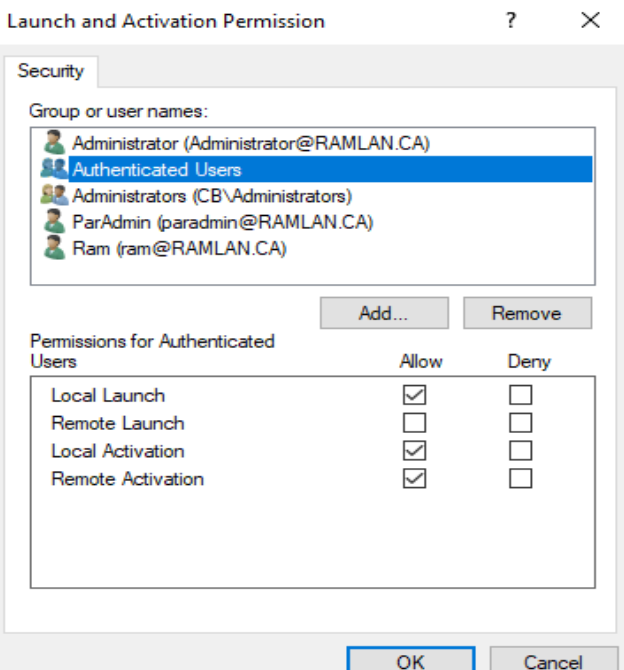
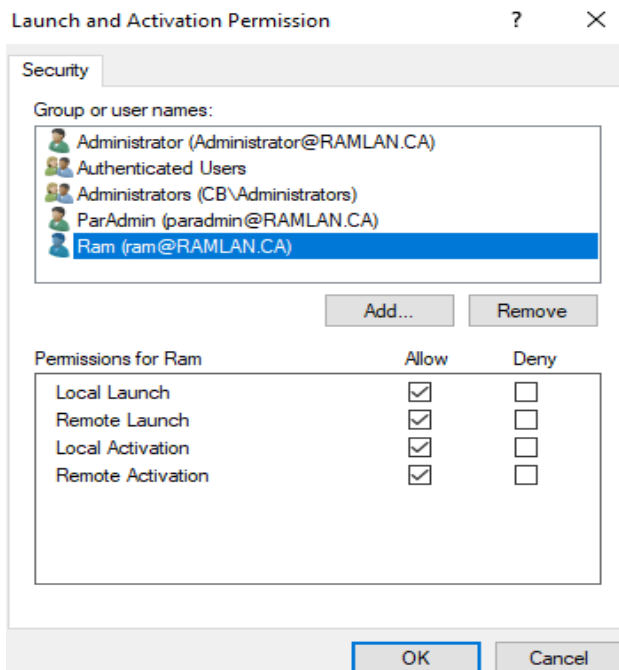
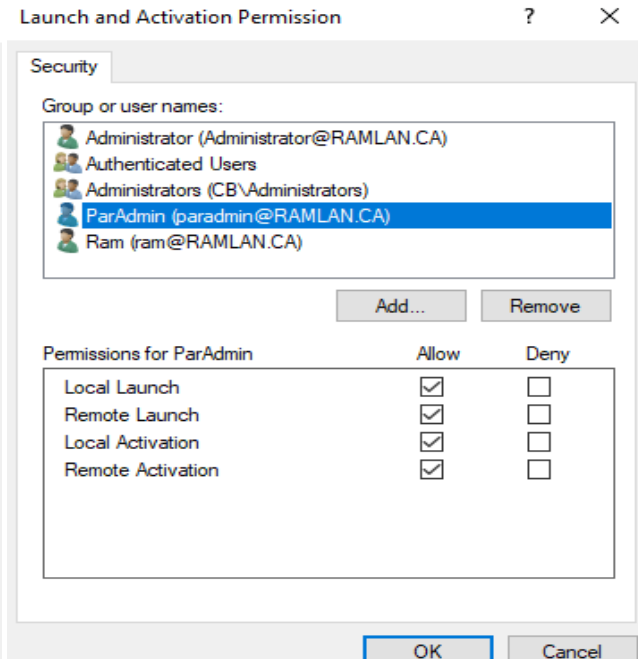
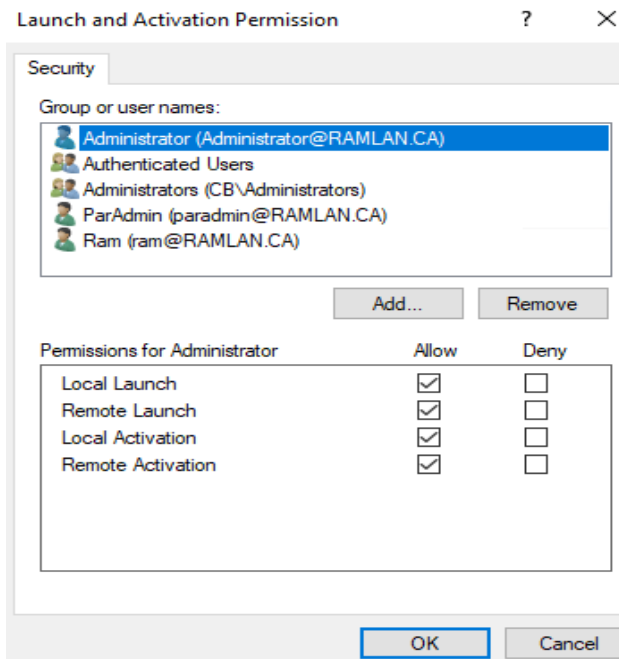
### DCOM Permission:

This we have to do it on the Configuration Manager Server (**CB**).

Click Start > Administrative Tools > Component Services.

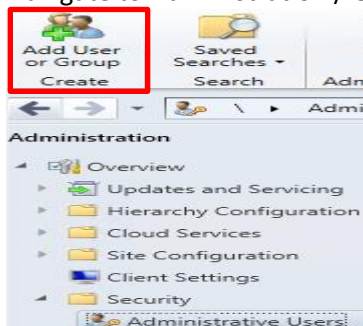
Navigate to Console Root / Component Services / Computers / My Computer / DCOM Config. Scroll down to Windows Management and Instrumentation





### Administrator rights Configuration Manager Console:

Navigate to Administration / Overview / Security





**Add User or Group**

Specify a user or group to add as a Configuration Manager administrative user

To control the type of objects that administrative users can manage, assign one or more security roles to the administrative user, and then assign security scopes to limit the instances of objects that the administrative user can manage.

User or group name:  Browse...

Assigned security roles:

Name	Description
Full Administrator	Grants all permissions in Configuration Manager. T...

Add... Remove

Assigned security scopes and collections:

☒ All instances of the objects that are related to the assigned security roles

☐ Only the instances of objects that are assigned to the specified security scopes or collections

Security scopes and collections:

Name	Type
------	------

Add Remove

OK Cancel

#### Permission in AD for ParallelsServices container:

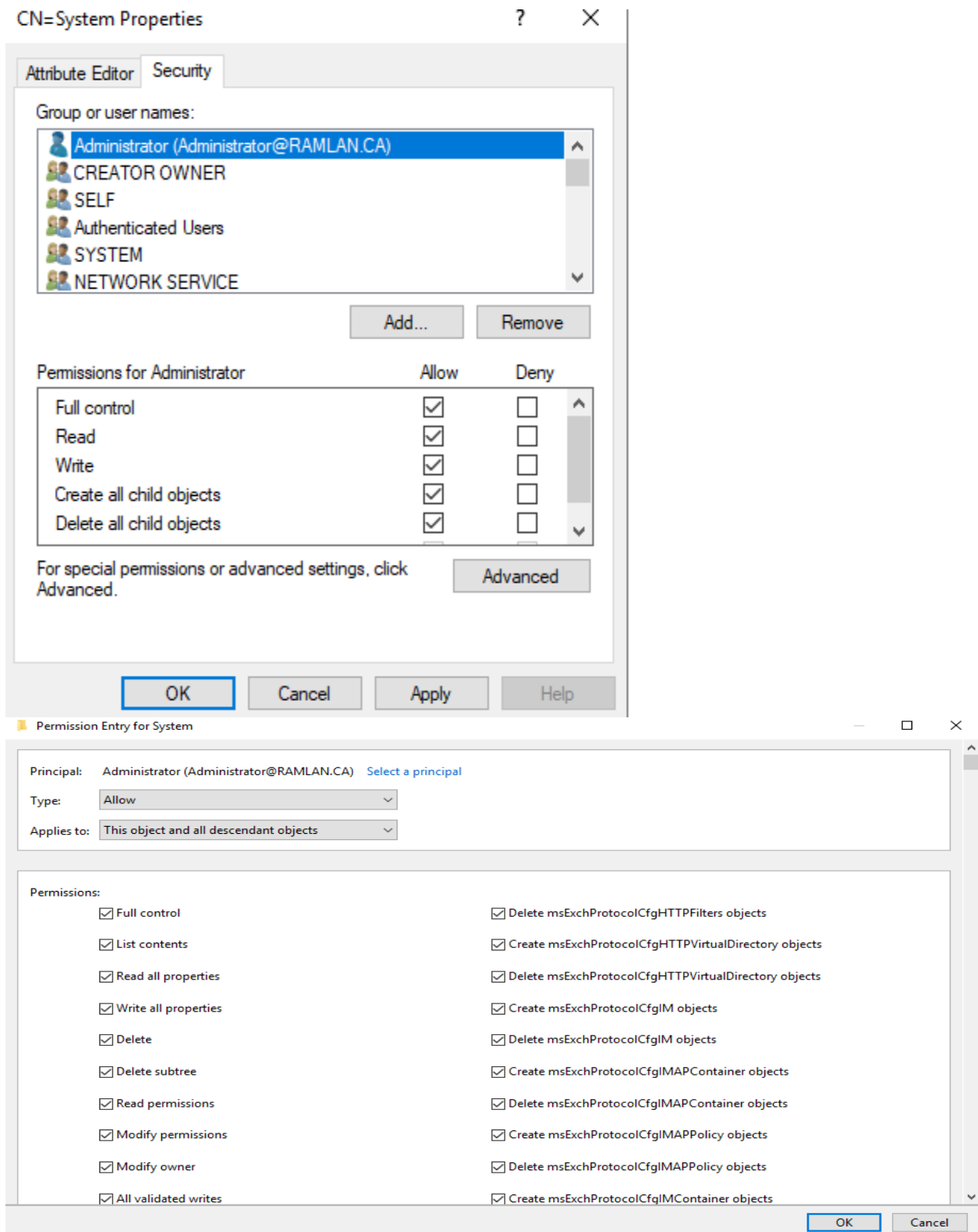
This we have to do it on the Domain Controller using ADSI Edit. I am going to give System Container (CN=System) full permission, so that when we install the roles. Required container for Parallels Mac Management will be created accordingly during the install.

- ▼ **CN=System**
  - CN=AdminSDHolder
  - CN=ComPartitions
  - CN=ComPartitionSets
  - CN=Default Domain Policy
  - CN=Dfs-Configuration
  - CN=DFSR-GlobalSettings
  - CN=DomainUpdates
  - CN=File Replication Service
  - CN=FileLinks
  - CN=IP Security
  - CN=Meetings
  - CN=MicrosoftDNS
  - CN=Password Settings Container
  - CN=Policies
  - CN=PSPs
  - CN=RAS and IAS Servers Access Check
  - CN=RpcServices
  - CN=System Management
  - CN=WinsockServices
  - CN=WMIPolicy
  - CN=TPM Devices
  - CN=Users

AS YOU CAN SEE THE CN=SYSTEM CONTAINER DOES NOT HAVE PARALLELSSERVICES CONTAINER YET.

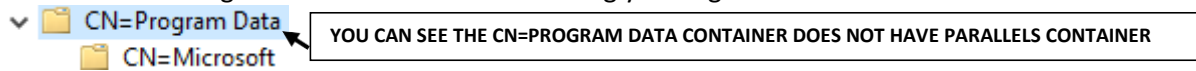
Right click CN=System – Properties – Security - Add – Administrator – Full Control – Click Advanced – Allow – This object and all descendant objects.

**Repeat the same for Ram, ParAdmin & PAR - Full Control - Click Advanced**



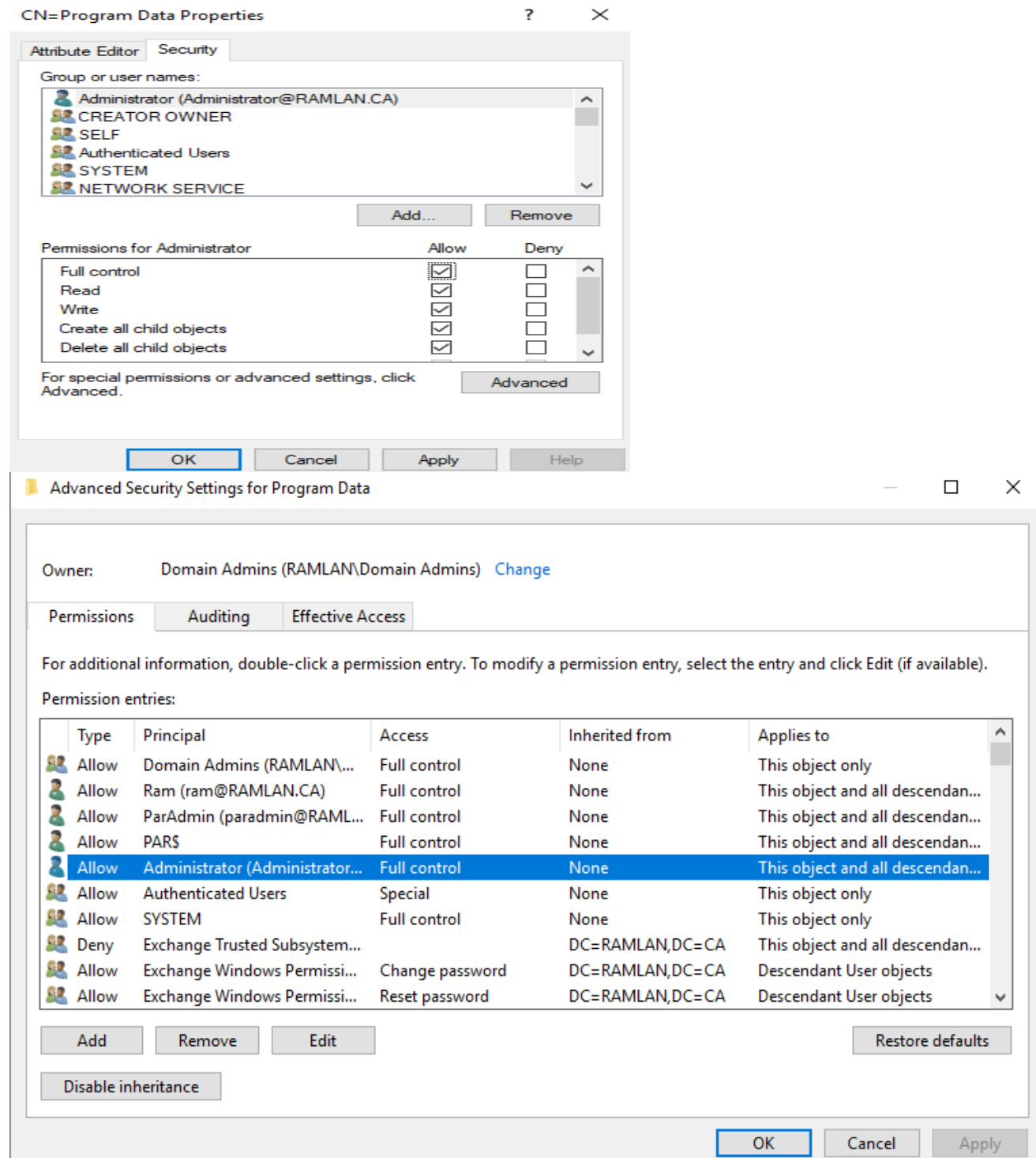
### Permission in AD for Program Data container:

This we have to do it on the Domain Controller using ADSI Edit. I am going to give Program Data Container (**CN=Program Data**) full permission so that when we install the roles. Required container for Parallels Mac Management will be created accordingly during the install.



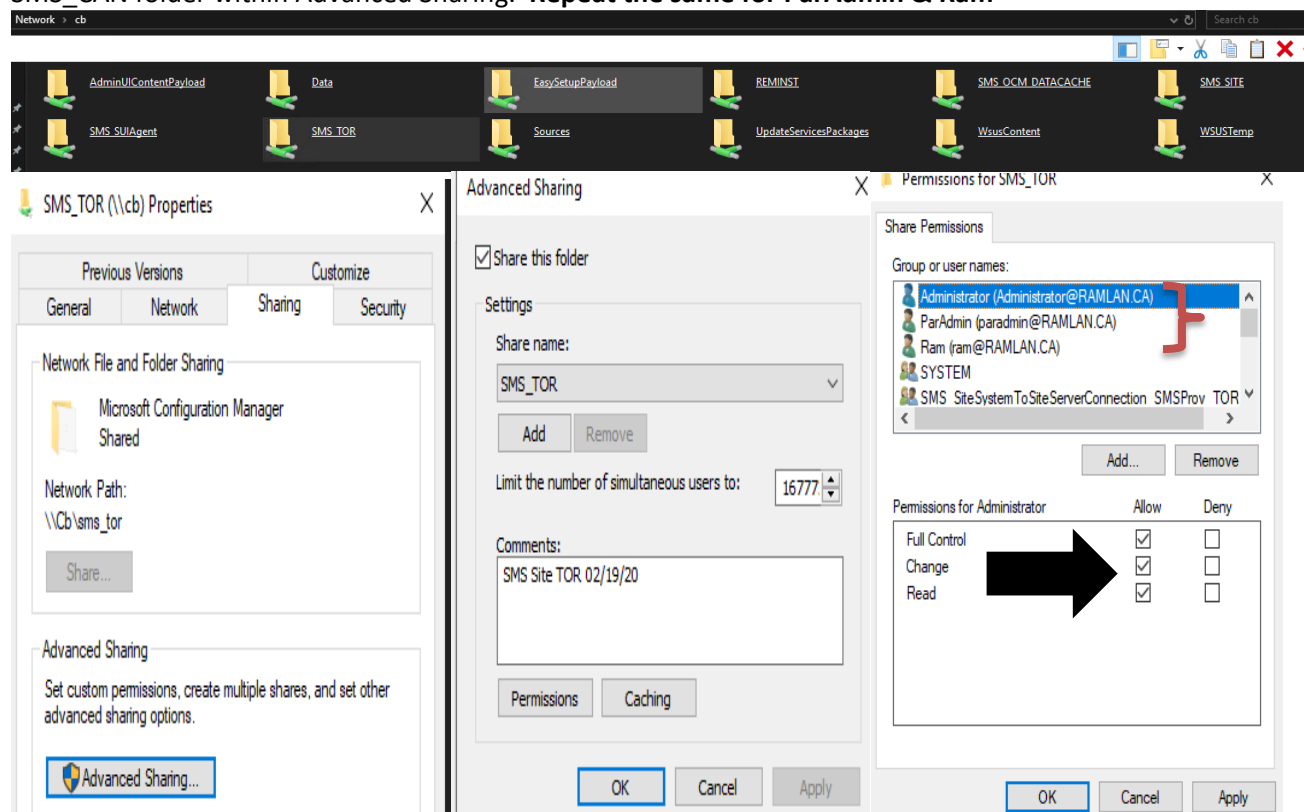
Right click CN=Program Data – Properties – Security – Add – Administrator – Full Control – Click Advanced – Allow – This object and all descendant objects.

**Repeat the same for Ram, ParAdmin & PAR - Full Control - Click Advanced**

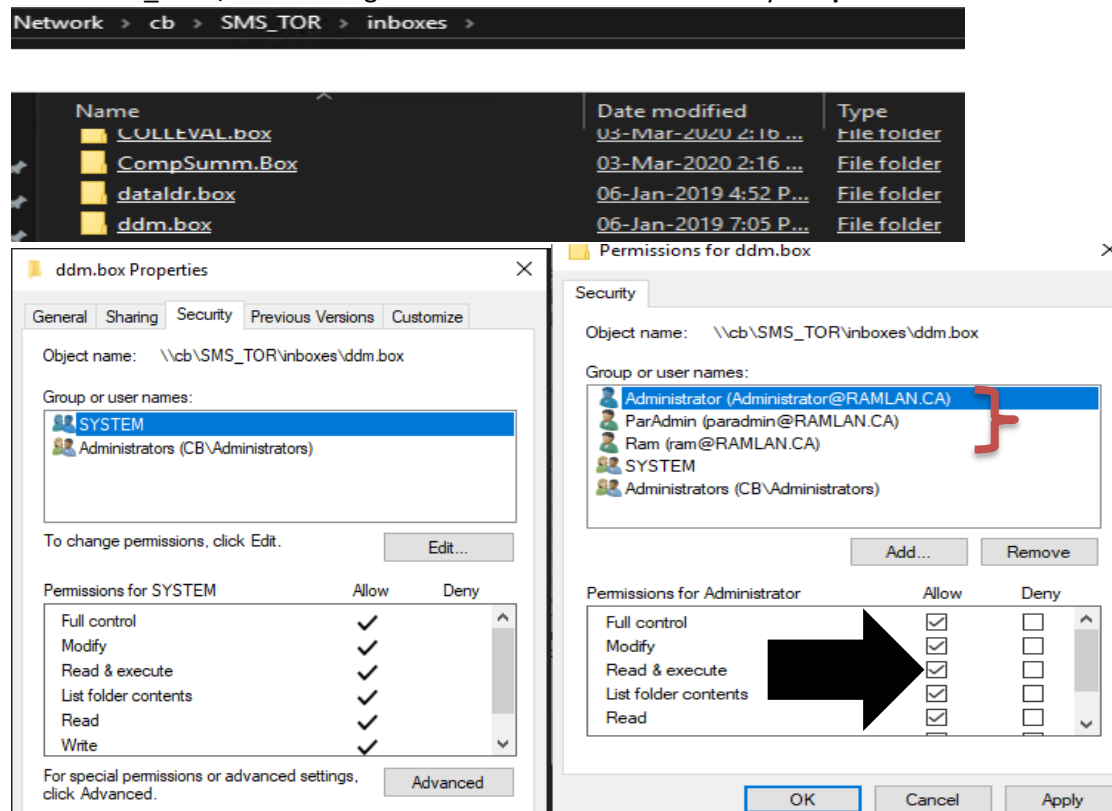


### Permission to SCCM Network Share:

We have to do it on the Configuration Manager Server (CB). We have to give Administrator- Full Control to SMS\_CAN folder within Advanced Sharing. **Repeat the same for ParAdmin & Ram**



Do for SMS\_CAN\inboxes – Right Click ddm.box folder – Security - **Repeat the same for ParAdmin & Ram**



## Web Server Certificate Template:

We have to create a web server certificate template for Parallels Proxy Configuration.

Open Certification Authority – Right Click Certificate Template – Right Click Web Server – Click Duplicate

Properties of New Template

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
Cryptography	Key Attestation	

The template options available are based on the earliest operating system versions set in Compatibility Settings.

☒ Show resulting changes

Compatibility Settings

Certification Authority: Windows Server 2008

Certificate recipient: Windows 7 / Server 2008 R2

These settings may not prevent earlier operating systems from using this template.

OK Cancel Apply Help

Properties of New Template

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
Cryptography	Key Attestation	

Template display name: Parallels Proxy

Template name: ParallelsProxy

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

OK Cancel Apply Help

Properties of New Template

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
Cryptography	Key Attestation	

Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

☐ Requests can use any provider available on the subject's computer

☒ Requests must use one of the following providers:

Providers:

- ☒ Microsoft RSA SChannel Cryptographic Provider
- ☒ Microsoft DH SChannel Cryptographic Provider
- ☐ Microsoft Base Smart Card Crypto Provider
- ☐ Microsoft Enhanced Cryptographic Provider v1.0
- ☐ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr

Request hash: Determined by CSP

☐ Use alternate signature format

OK Cancel Apply Help

Properties of New Template



Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
	Cryptography	Key Attestation

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 (\*)

Key Permissions...

☒ 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](#).

OK Cancel Apply Help

Properties of New Template



Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
Subject Name	Server	Cryptography
	Issuance Requirements	Key Attestation

☒ Supply in the request

☒ Use subject information from existing certificates for autoenrollment renewal requests

☐ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

☐ Include e-mail name in subject name

Include this information in alternate subject name:

☐ E-mail name

☐ DNS name

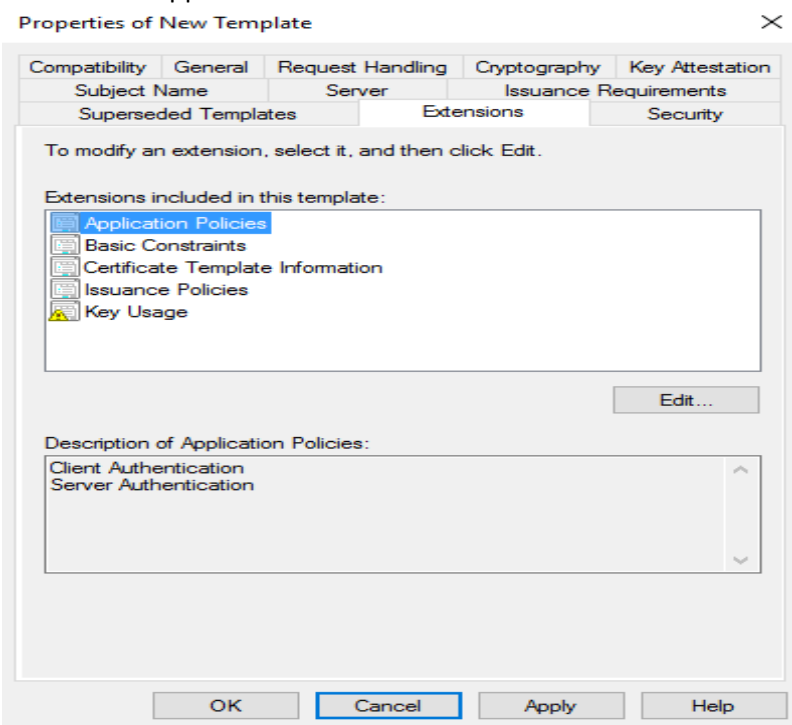
☐ User principal name (UPN)

☐ Service principal name (SPN)

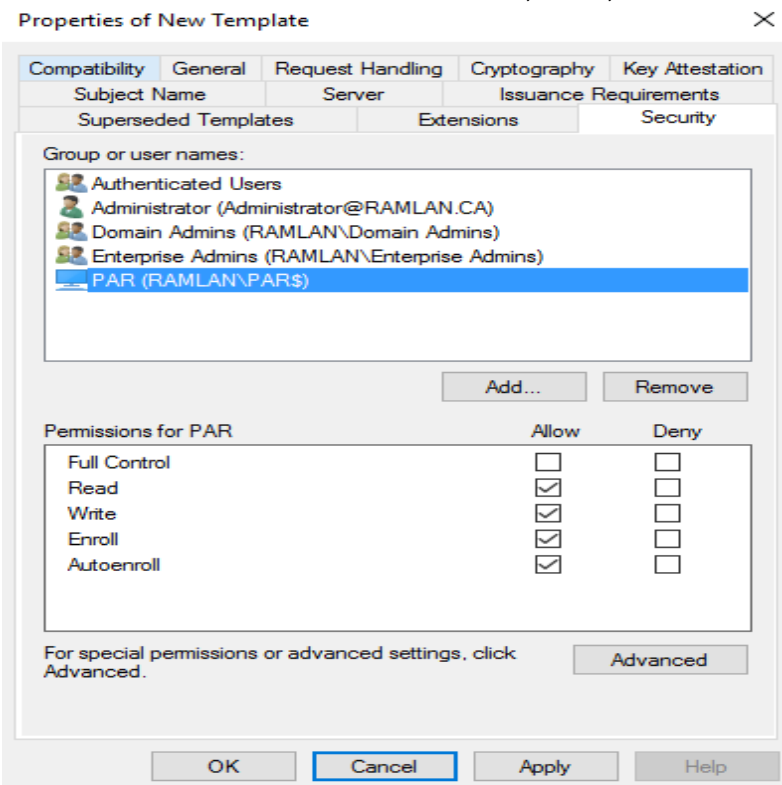
OK Cancel Apply Help



Double click Application Policies and Add Client Authentication



Make sure to Administrator & PAR has Read, Write, Enroll and Autoenroll permission.



Right-click Certificate Templates again and choose New > Certificate Template to Issue  
Select Parallels Proxy and Click OK

## Workstation Authentication Certificate Template:

Open Certification Authority – Right Click Certificate Template – Right Click Workstation Authentication  
– Click Duplicate

Properties of New Template ✕

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
Cryptography	Key Attestation	

The template options available are based on the earliest operating system versions set in Compatibility Settings.

☒ Show resulting changes

Compatibility Settings

Certification Authority  
Windows Server 2008 ▾

Certificate recipient  
Windows 7 / Server 2008 R2 ▾

These settings may not prevent earlier operating systems from using this template.

OK Cancel Apply Help

Properties of New Template ✕

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
	Cryptography	Key Attestation

Template display name:

Template name:

Validity period:  
 years

Renewal period:  
 weeks

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

OK Cancel Apply Help

Properties of New Template ✕

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
	Cryptography	Key Attestation

Provider Category:

Algorithm name:

Minimum key size:

Choose which cryptographic providers can be used for requests  
☐ Requests can use any provider available on the subject's computer  
☒ Requests must use one of the following providers:

Providers:

<input checked="" type="checkbox"/> Microsoft RSA SChannel Cryptographic Provider	↑
<input type="checkbox"/> Microsoft Base Smart Card Crypto Provider	
<input type="checkbox"/> Microsoft DH SChannel Cryptographic Provider	
<input type="checkbox"/> Microsoft Enhanced Cryptographic Provider v1.0	
<input type="checkbox"/> Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr	↓

Request hash:

☐ Use alternate signature format

OK Cancel Apply Help

Properties of New Template

Superseded Templates		Server	Issuance Requirements	
Compatibility	General	Request Handling	Cryptography	Key Attestation

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 (\*)

Key Permissions...

☒ 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](#).

OK Cancel Apply Help

Properties of New Template

Superseded Templates		Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation

Subject Name

☒ Supply in the request

☒ Use subject information from existing certificates for autoenrollment renewal requests

☐ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

☐ Include e-mail name in subject name

Include this information in alternate subject name:

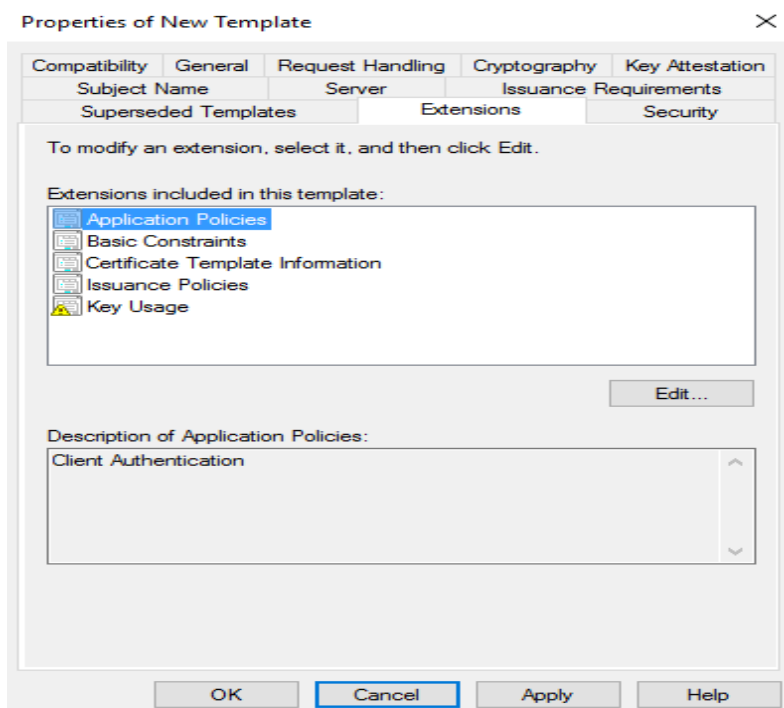
☐ E-mail name

☐ DNS name

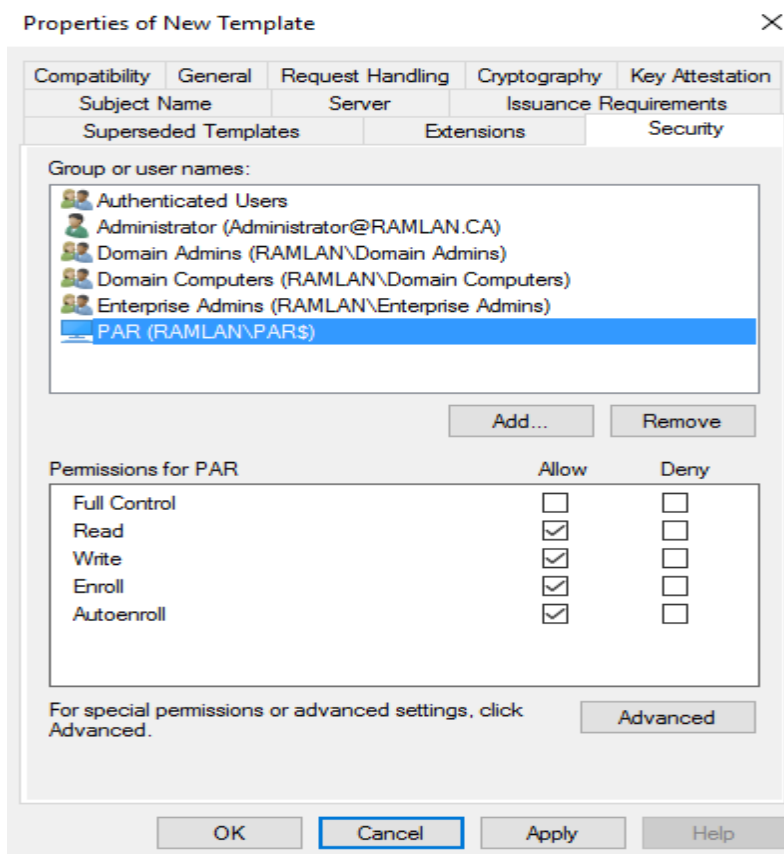
☐ User principal name (UPN)

☐ Service principal name (SPN)

OK Cancel Apply Help



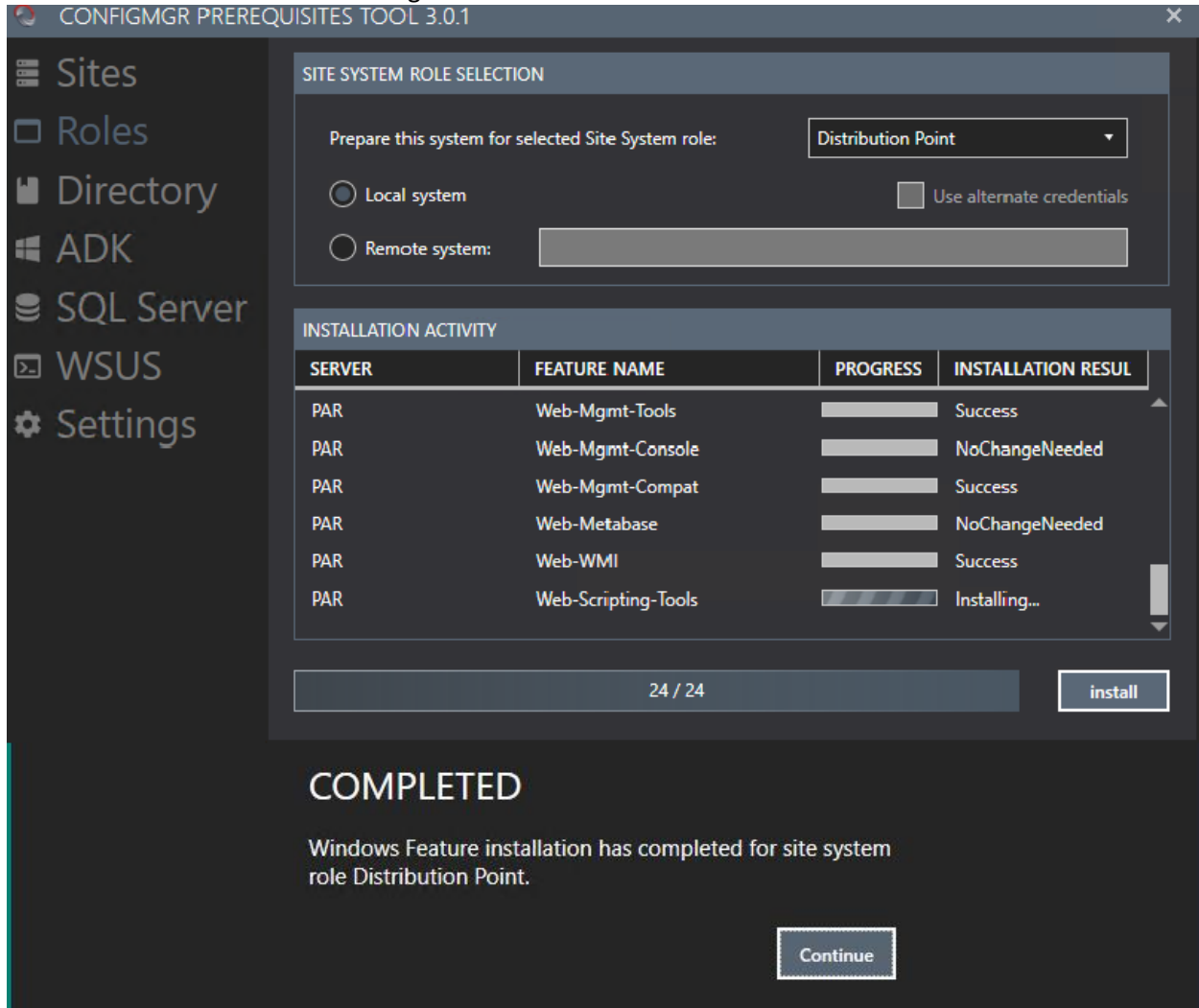
Make sure to Administrator & PAR has Read, Write, Enroll and Autoenroll permission



Right-click Certificate Templates again and choose New > Certificate Template to Issue  
Select Parallels Proxy Client and Click OK

### Distribution Point:

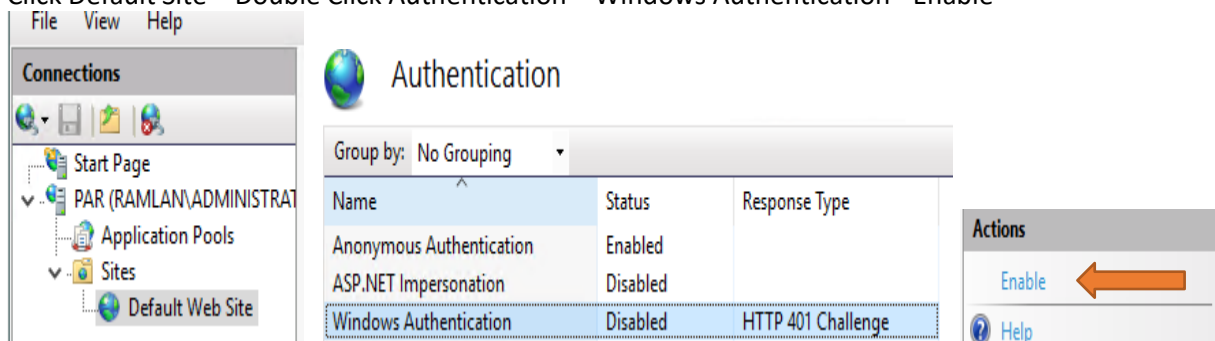
I am using Configmgr Prerequisites tool 3.0.1 to install DP on PAR. Pretty easy – Just select the role and click install. Wait for success message.



Also add these roles and features manually (URL Authorization & BITS) from Server Manager

Open IIS Manager and complete the following:

Click Default Site – Double Click Authentication – Windows Authentication - Enable





## WSUS Install:

### Open Server Manager – Add Roles and Features – Select WSUS

Add Roles and Features Wizard

DESTINATION SERVER  
PAR.RAMLAN.CA

### Select installation type

Before You Begin  
**Installation Type**  
Server Selection  
Server Roles  
Features  
Confirmation  
Results

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

- ☒ **Role-based or feature-based installation**  
Configure a single server by adding roles, role services, and features.
- ☐ **Remote Desktop Services installation**  
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous   Next >   Install   Cancel

Add Roles and Features Wizard

DESTINATION SERVER  
PAR.RAMLAN.CA

### Select destination server

Before You Begin  
Installation Type  
**Server Selection**  
Server Roles  
Features  
Confirmation  
Results

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

- ☒ Select a server from the server pool
- ☐ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
PAR.RAMLAN.CA	192.168.0.16	Microsoft Windows Server 2016 Datacenter

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous   Next >   Install   Cancel

## Select server roles

DESTINATION SERVER  
PAR.RAMLAN.CA

Before You Begin

Installation Type

Server Selection

**Server Roles**

Features

WSUS

Role Services

Content

Confirmation

Results

Select one or more roles to install on the selected server.

## Roles

- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ☒ File and Storage Services (2 of 12 installed)
  - ☐ Host Guardian Service
  - ☐ Hyper-V
  - ☐ MultiPoint Services
  - ☐ Network Controller
  - ☐ Network Policy and Access Services
  - ☐ Print and Document Services
  - ☐ Remote Access
  - ☐ Remote Desktop Services
  - ☐ Volume Activation Services
- ☒ Web Server (IIS) (18 of 43 installed)
  - ☐ Windows Deployment Services
  - ☐ Windows Server Essentials Experience
  - ☒ Windows Server Update Services

## Description

Windows Server Update Services allows network administrators to specify the Microsoft updates that should be installed, create separate groups of computers for different sets of updates, and get reports on the compliance levels of the computers and the updates that must be installed.

&lt; Previous

Next &gt;

Install

Cancel

## Select role services

DESTINATION SERVER  
PAR.RAMLAN.CA

Before You Begin

Installation Type

Server Selection

Server Roles

Features

WSUS

**Role Services**

Content

DB Instance

Confirmation

Results

Select the role services to install for Windows Server Update Services

## Role services

- ☐ WID Connectivity
- ☒ WSUS Services
- ☒ SQL Server Connectivity

## Description

Installs the feature that enables WSUS to connect to a Microsoft SQL Server database.

&lt; Previous

Next &gt;

Install

Cancel

## Content location selection

DESTINATION SERVER  
PAR.RAMLAN.CA

Before You Begin

Installation Type

Server Selection

Server Roles

Features

WSUS

Role Services

Content

DB Instance

Confirmation

Results

If you have a drive formatted with NTFS and at least 6 GB of free disk space, you can use it to store updates for client computers to download quickly.

If you need to save disk space, clear the check box to store updates on Microsoft Update; downloads will be slower.

If you choose to store updates locally, updates are not downloaded to your WSUS server until you approve them. By default, when updates are approved, they are downloaded for all languages.

☒ Store updates in the following location (choose a valid local path on PAR.RAMLAN.CA, or a remote path) :

&lt; Previous

Next &gt;

Install

Cancel

## Database Instance Selection

DESTINATION SERVER  
PAR.RAMLAN.CA

Before You Begin

Installation Type

Server Selection

Server Roles

Features

WSUS

Role Services

Content

DB Instance

Confirmation

Results

Specify an existing database server (Machine name\Instance name) to install the WSUS database:

Successfully connected to server

&lt; Previous

Next &gt;

Install

Cancel

## Confirm installation selections

DESTINATION SERVER  
PAR.RAMLAN.CA

Before You Begin

Installation Type

Server Selection

Server Roles

Features

WSUS

Role Services

Content

DB Instance

Confirmation

Results

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

☐ Restart the destination server automatically if required

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

.NET Framework 4.7 Features  
WCF Services  
HTTP Activation

Remote Server Administration Tools  
Role Administration Tools  
Windows Server Update Services Tools  
API and PowerShell cmdlets  
User Interface Management Console

Windows Internal Database  
Windows Process Activation Service

[Export configuration settings](#)  
[Specify an alternate source path](#)

&lt; Previous

Next &gt;

Install

Cancel

## Installation progress

DESTINATION SERVER  
PAR.RAMLAN.CA

Before You Begin

Installation Type

Server Selection

Server Roles

Features

WSUS

Role Services

Content

DB Instance

Confirmation

Results

View installation progress

 Feature installation

Configuration required. Installation succeeded on PAR.RAMLAN.CA.

Windows Server Update Services  
Additional configuration must be performed before continuing  
Launch Post-Installation tasks  
SQL Server Connectivity  
WSUS Services

.NET Framework 4.6 Features  
ASP.NET 4.6  
WCF Services  
HTTP Activation

Remote Server Administration Tools  
Role Administration Tools



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

[Export configuration settings](#)

&lt; Previous

Next &gt;

Close

Cancel



## Post-deployment Configuration

Configuration required for Windows Server Update Services at PAR

[Launch Post-Installation tasks](#)

## Feature installation

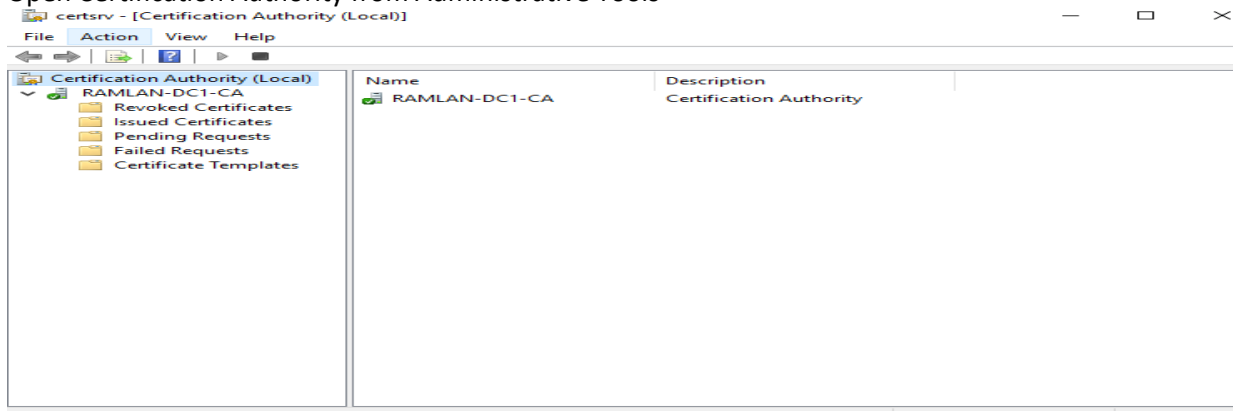
Configuration required. Installation succeeded on PAR.RAMLAN.CA.

[Add Roles and Features](#)

## WSUS Certificate:

One of the pre-req required for the OS X Software Update service is to install a WSUS code signing certificate. This can be obtained from the certificate authority in your environment.

Open Certification Authority from Administrative Tools



Right click Certificate Templates – Manage – Code Signing – Right Click – Duplicate Template

Properties of New Template

Properties of New Template

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
	Cryptography	Key Attestation

The template options available are based on the earliest operating system versions set in Compatibility Settings.

☒ Show resulting changes

Compatibility Settings

Certification Authority  
Windows Server 2003

Certificate recipient  
Windows XP / Server 2003

These settings may not prevent earlier operating systems from using this template.

OK Cancel Apply Help

Properties of New Template

Properties of New Template

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
	Cryptography	Key Attestation

Template display name:  
WSUS Code Signing Cert

Template name:  
WSUSCodeSigningCert

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

OK Cancel Apply Help

Properties of New Template



Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
Cryptography	Key Attestation	

Purpose: Signature

☐ Delete revoked or expired certificates (do not archive)

☐ Include symmetric algorithms allowed by the subject

☐ Archive subject's encryption 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](#).

OK Cancel Apply Help

Properties of New Template



Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
Cryptography	Key Attestation	

Subject Name

Server

Issuance Requirements

☐ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests (\*)

☒ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

Common name

☐ Include e-mail name in subject name

Include this information in alternate subject name:

☐ E-mail name

☐ DNS name

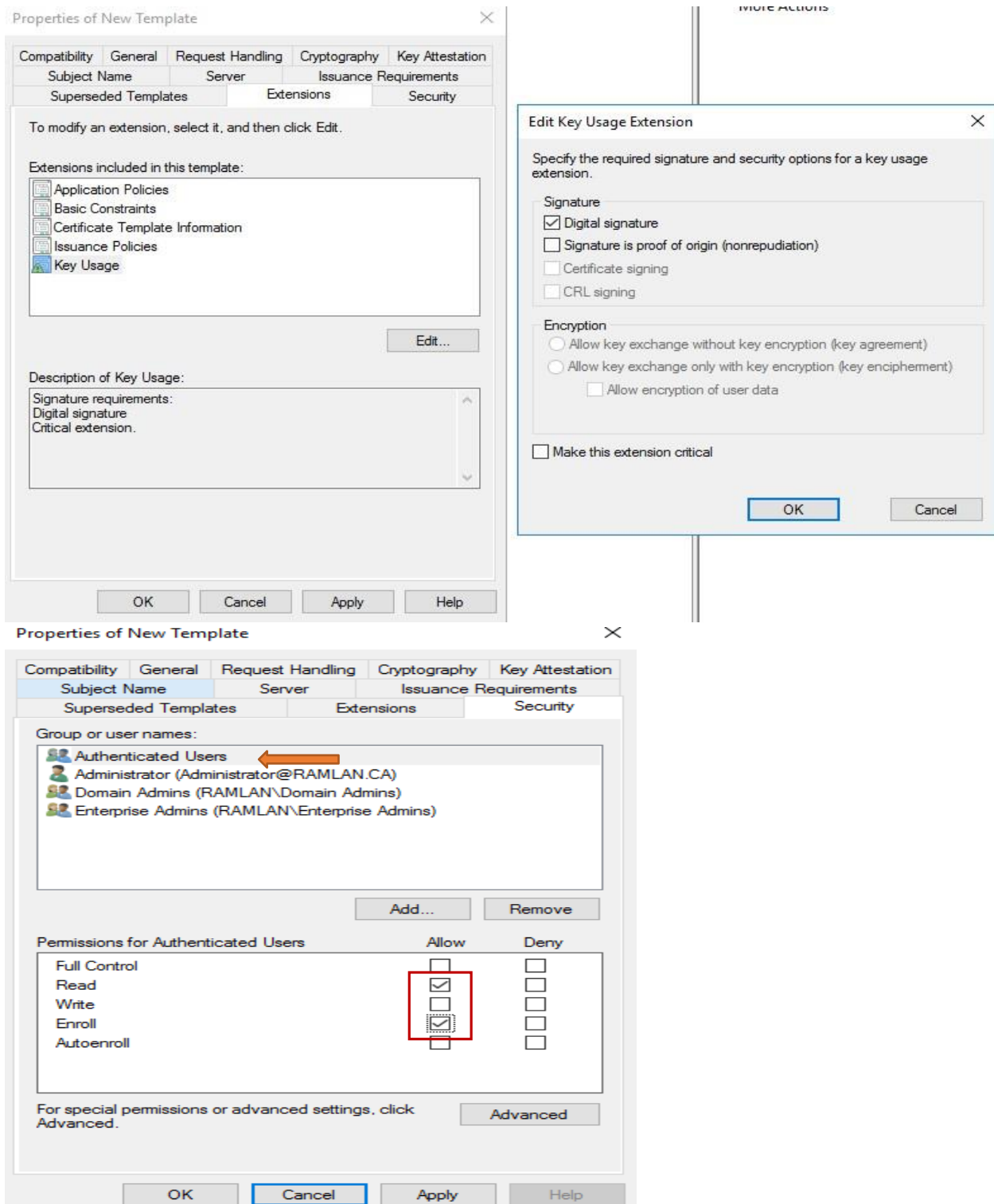
☒ User principal name (UPN)

☐ Service principal name (SPN)

\* Control is disabled due to [compatibility settings](#).

OK Cancel Apply Help

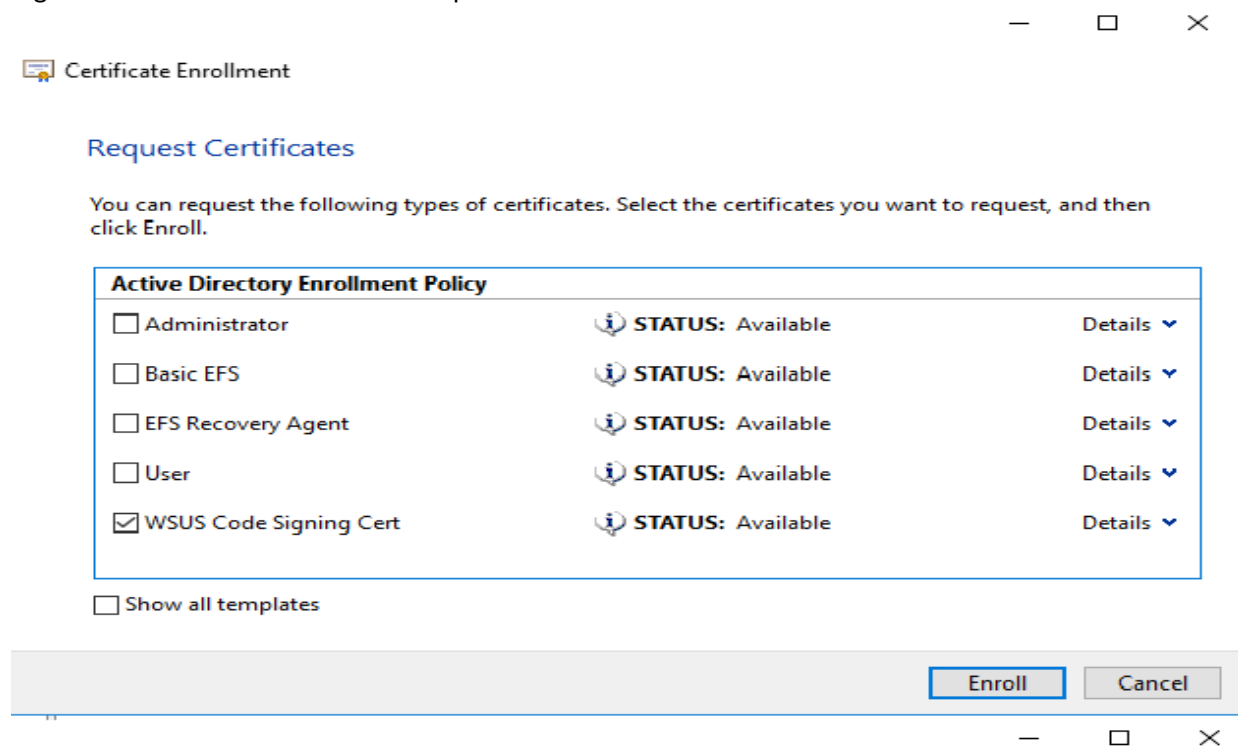




In Certificate Authority console right click Certificate Templates>New>Certificate Template to Issue -  
Select WSUS Code Signing Cert - OK

### Request WSUS Code Signing Cert on PAR Server:

Click - Run – Type MMC - Add/Remove Snap-in - Certificates – Add - My User Account – Finish  
Right click Personnel – All Tasks – Request New Certificate



Certificate Enrollment

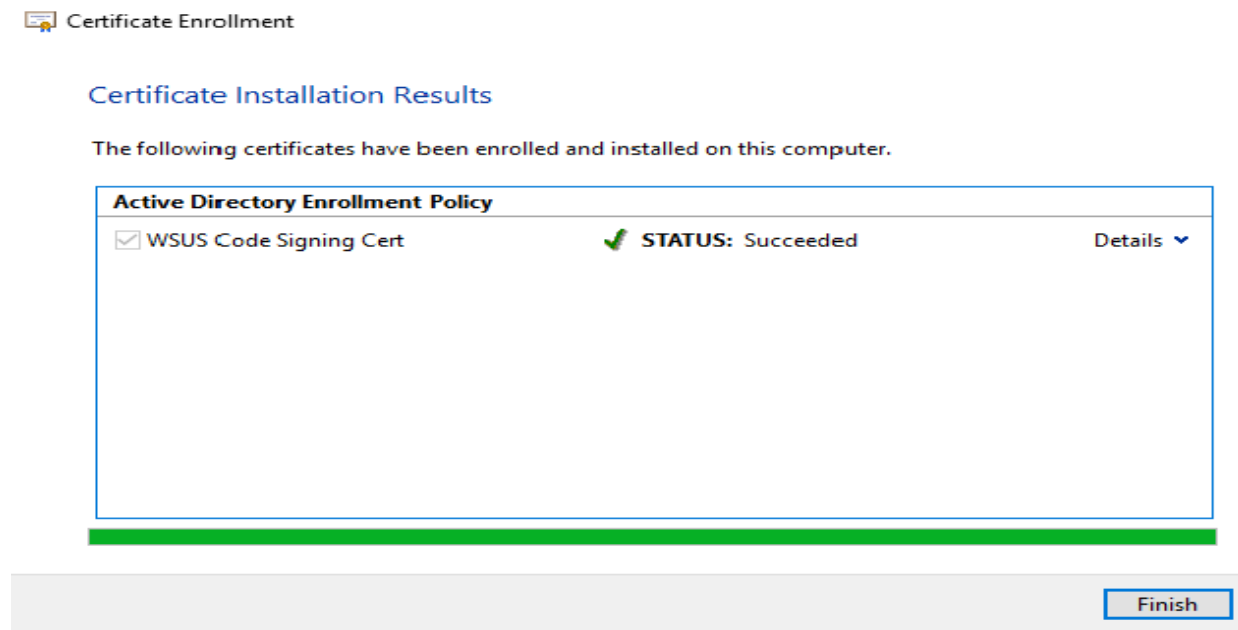
#### Request Certificates

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

Active Directory Enrollment Policy		
<input type="checkbox"/> Administrator	<b>STATUS:</b> Available	Details ▾
<input type="checkbox"/> Basic EFS	<b>STATUS:</b> Available	Details ▾
<input type="checkbox"/> EFS Recovery Agent	<b>STATUS:</b> Available	Details ▾
<input type="checkbox"/> User	<b>STATUS:</b> Available	Details ▾
<input checked="" type="checkbox"/> WSUS Code Signing Cert	<b>STATUS:</b> Available	Details ▾

☐ Show all templates

**Enroll** Cancel



Certificate Enrollment

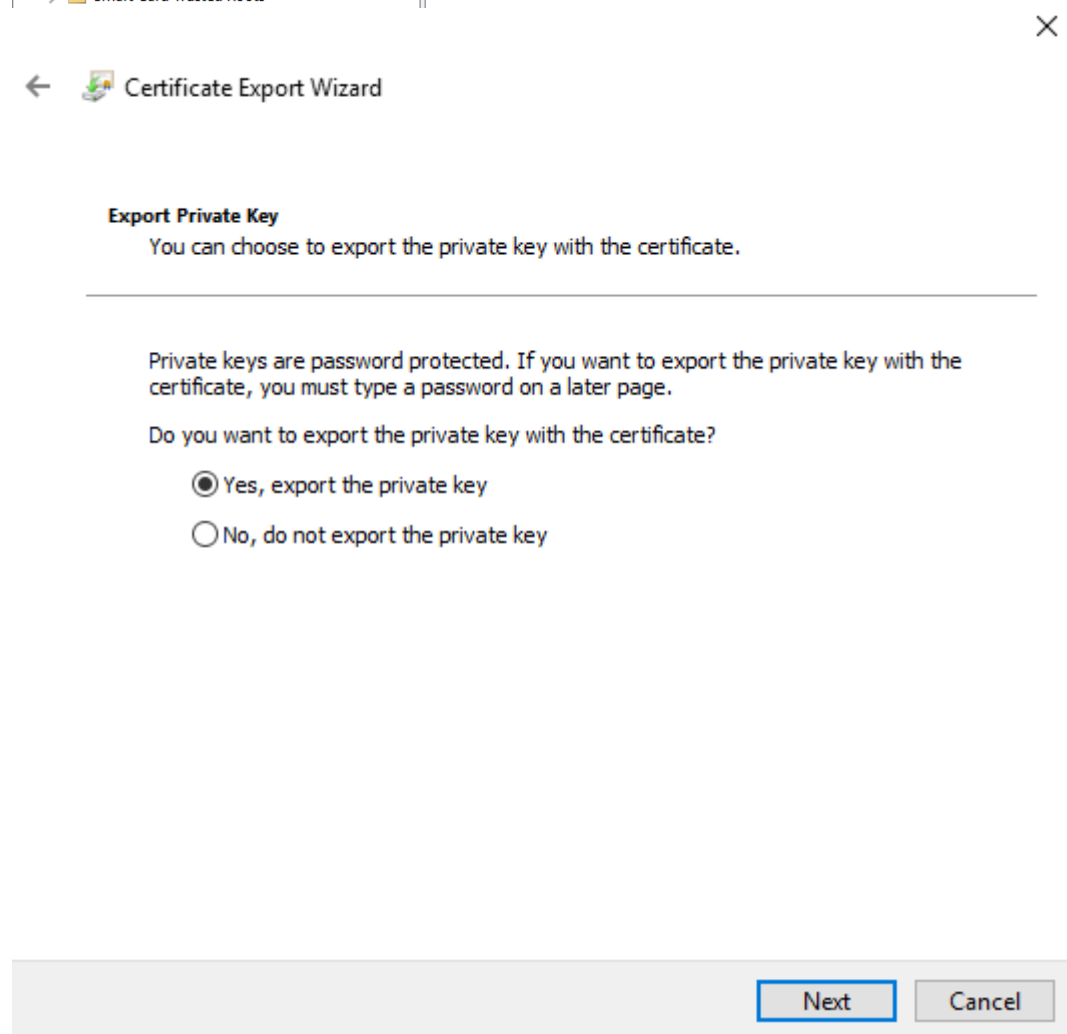
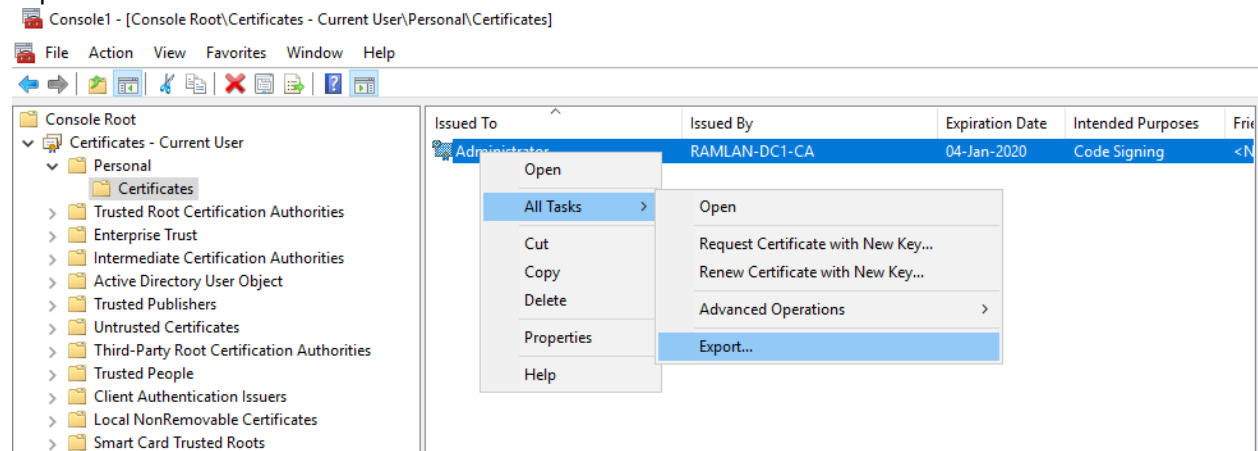
#### Certificate Installation Results

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

Active Directory Enrollment Policy		
<input checked="" type="checkbox"/> WSUS Code Signing Cert	<b>STATUS:</b> Succeeded	Details ▾

**Finish**

## Export the certificate



### 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)

Next

Cancel

### Security

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

☐ Group or user names (recommended)

Add

Remove

☒ Password:

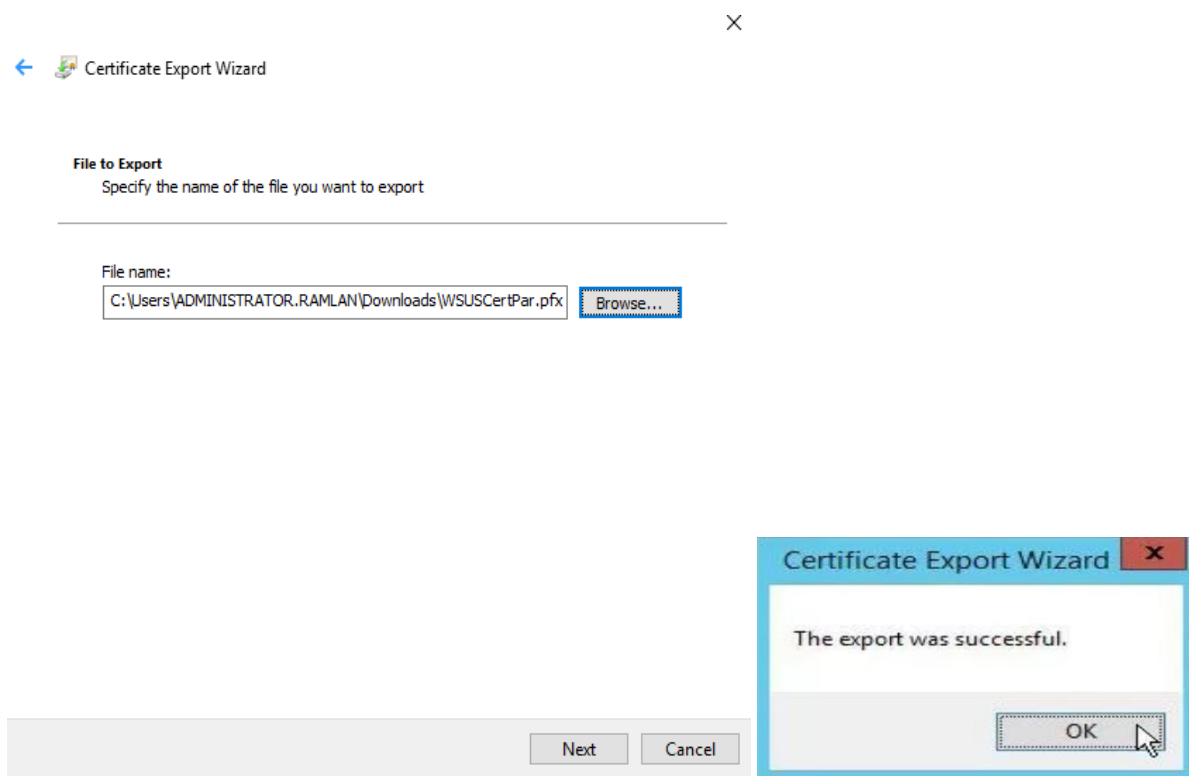
••••••••

Confirm password:

••••••••

Next

Cancel



Open PowerShell as administrator and run these commands one at a time

```
[Reflection.Assembly]::LoadWithPartialName("Microsoft.UpdateServices.Administration")
$updateServer = [Microsoft.UpdateServices.Administration.AdminProxy]::GetUpdateServer()
$config = $updateServer.GetConfiguration()
$config.SetSigningCertificate("C:\Users\ADMINISTRATOR.RAMLAN\Downloads\WSUSCertPar.pfx",
"),"01Jan2009")
$config.Save()
```

The image shows a screenshot of an 'Administrator: Windows PowerShell' window. The title bar includes the PowerShell icon, the text 'Administrator: Windows PowerShell', and standard window controls. The terminal content is as follows:

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

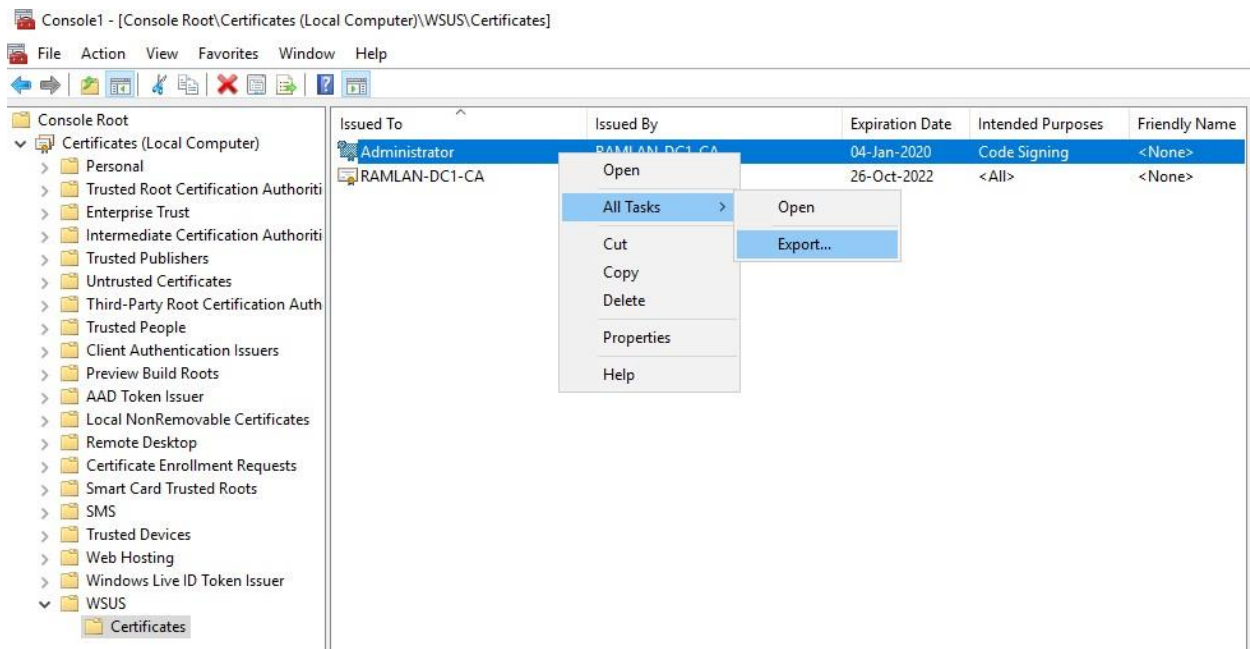
PS C:\Users\ADMINISTRATOR.RAMLAN> [Reflection.Assembly]::LoadWithPartialName("Microsoft.UpdateServices.Administration")

GAC      Version      Location
----      -
True     v4.0.30319    C:\Windows\Microsoft.Net\assembly\GAC_MSIL\Microsoft.UpdateServices.Administration\v4.0.4.0.0__31bf3856ad36...

PS C:\Users\ADMINISTRATOR.RAMLAN> $updateServer = [Microsoft.UpdateServices.Administration.AdminProxy]::GetUpdateServer()
PS C:\Users\ADMINISTRATOR.RAMLAN> $config = $updateServer.GetConfiguration()
PS C:\Users\ADMINISTRATOR.RAMLAN> $config.SetSigningCertificate("C:\Users\ADMINISTRATOR.RAMLAN\Downloads\WSUSCertPar.pfx", "01Jan2009")
PS C:\Users\ADMINISTRATOR.RAMLAN> $config.Save()
PS C:\Users\ADMINISTRATOR.RAMLAN>
```

We need to export the certificate added via PowerShell from PAR server.

Click - Run – Type MMC - Add/Remove Snap-in - Certificates – Add – Computer Account – Finish



## ← 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

Next

Cancel



←

 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)

Next

Cancel

×

←

 Certificate Export Wizard

×

File to Export

Specify the name of the file you want to export

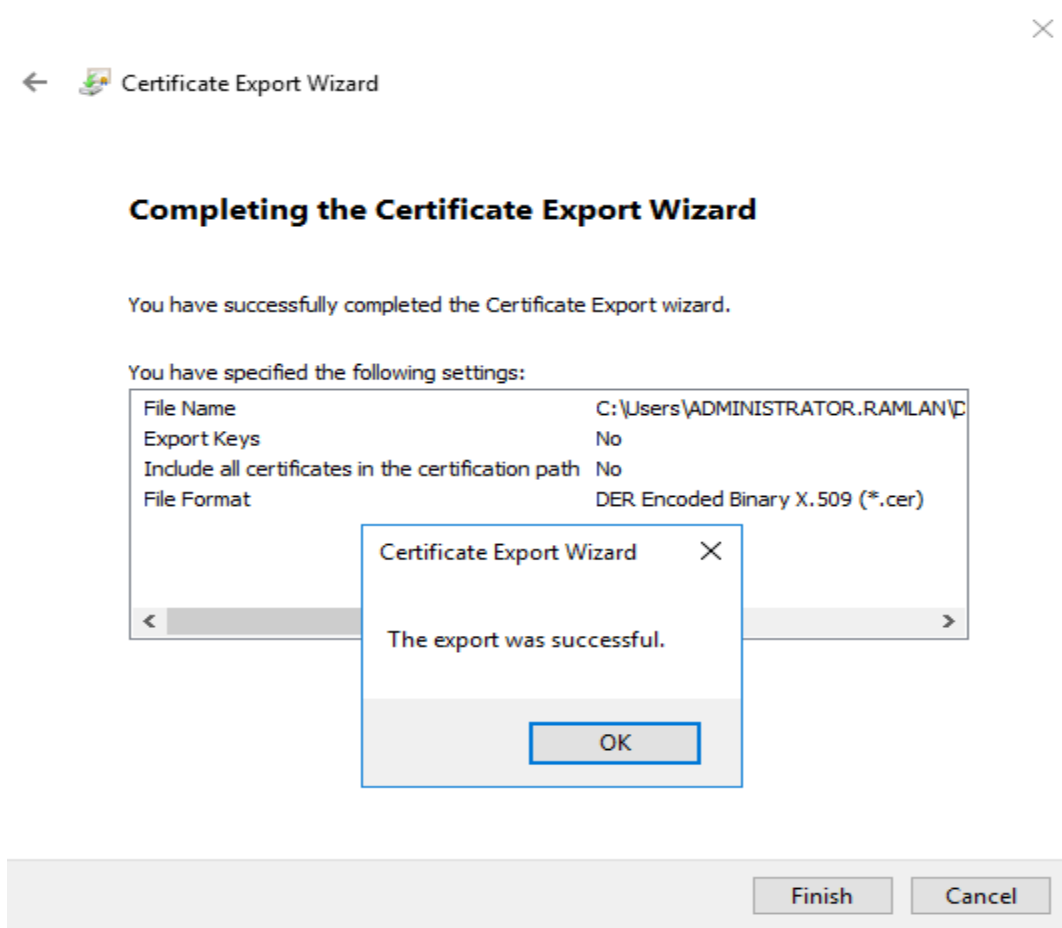
File name:

C:\Users\ADMINISTRATOR.RAMLAN\Downloads\WSUSCertPar.cer

Browse...

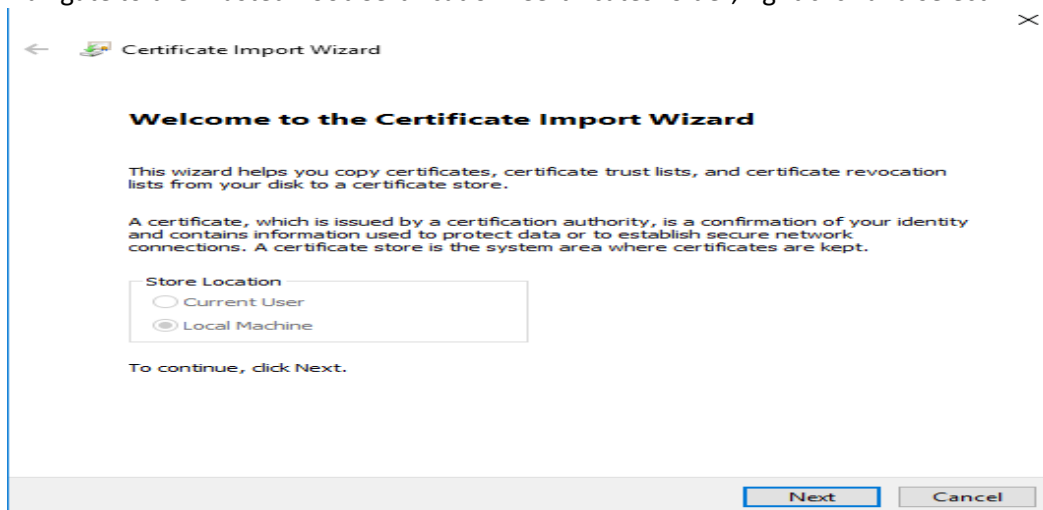
Next

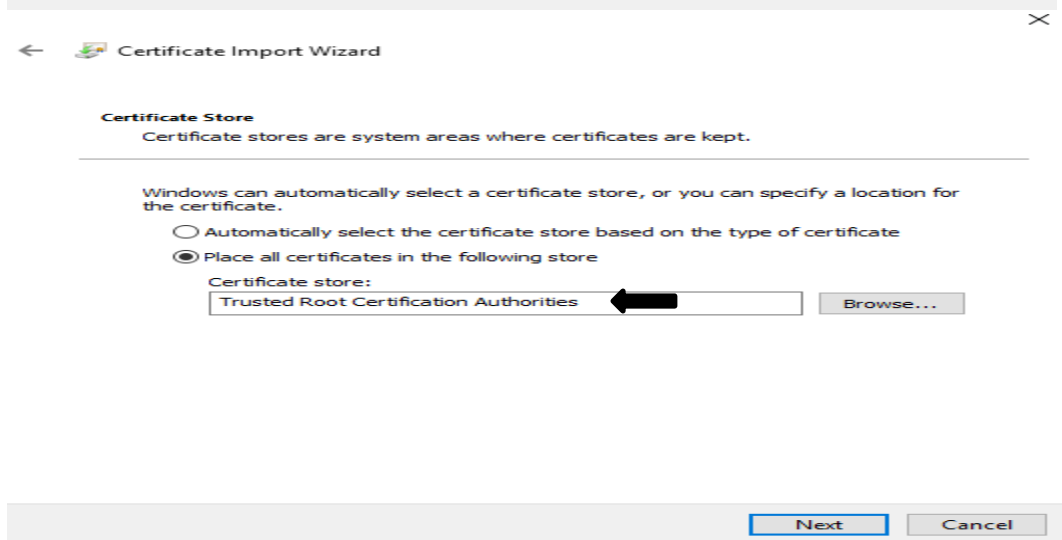
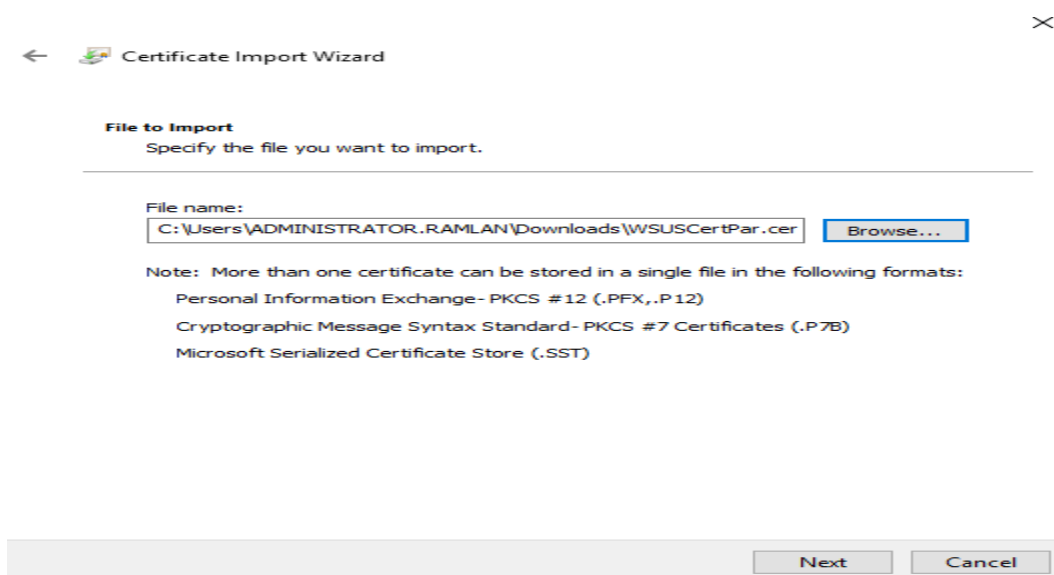
Cancel




### Import Certificate To: (Trusted Root Certification & Trusted Publishers Folders)

Navigate to the Trusted Root Certification>Certificates folder, right click and select All Tasks>Import





Certificate Import Wizard

 The import was successful.



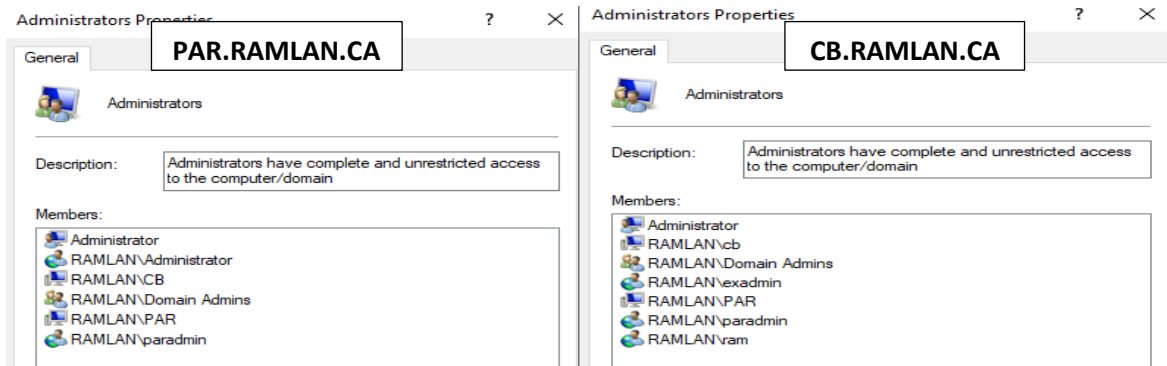
Administrator RAMLAN-DC1-CA 04-Jan-2020 Code Signing <None> WSUS Code Si...

Repeat above steps (Import Certificate) to the Trusted Publishers folder as well.

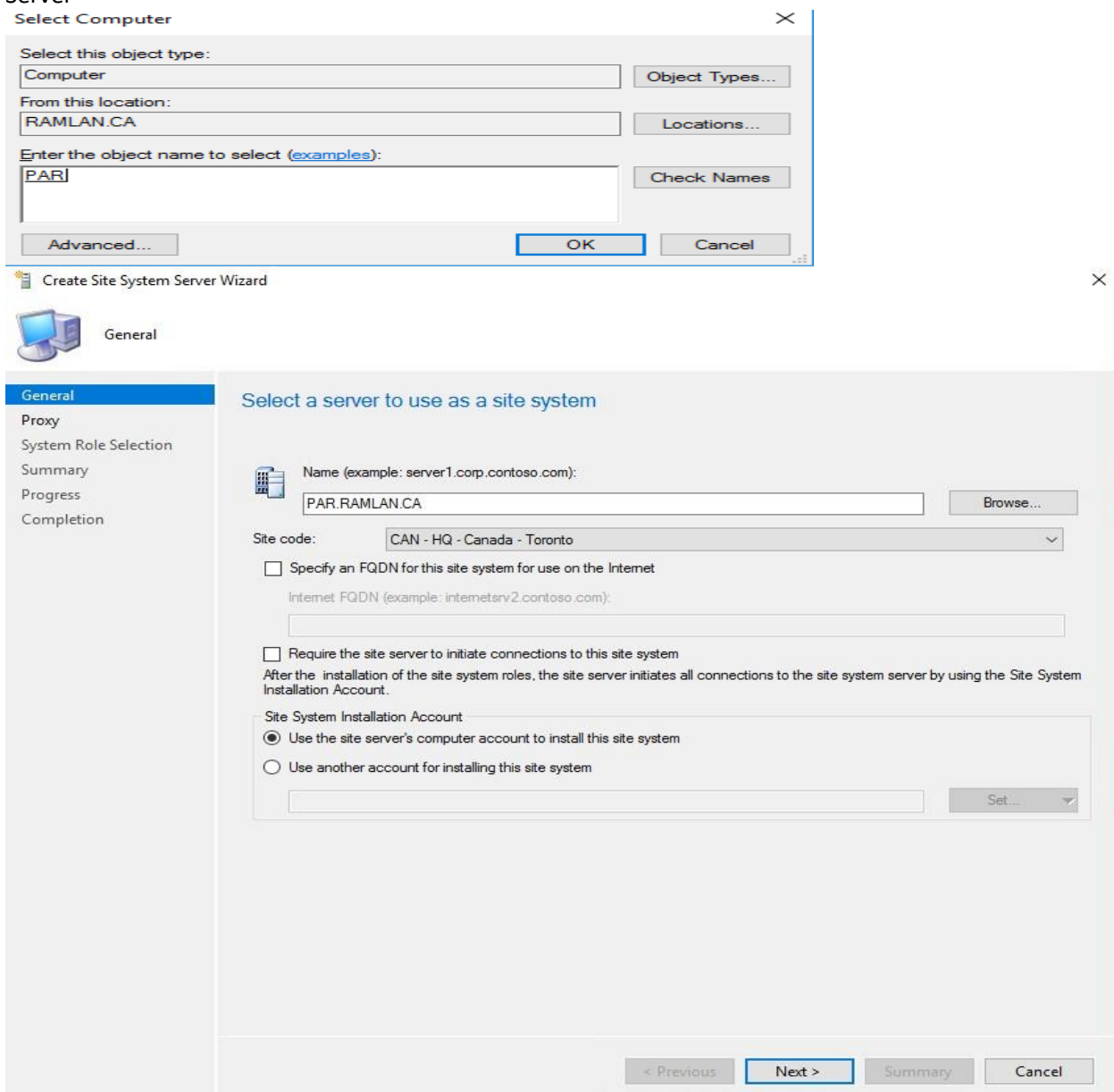
If your SMS Provider is remote, and in my case, it resides on my site server (CB), then repeat the process of importing the wsuscertpar.cer into the Trusted Root Certification and Trusted Publishers folders on that server (CB) as well.

## DP Installation:

We have to carry out the DP install from Config Manager Site Server (CB). **Before you start make sure to add CB to Administrators Group on PAR member server.**



Go to Administration – Site Configuration – Right click Server and Site System Roles – Create Site System Server





## System Role Selection

General

Proxy

**System Role Selection**

Distribution point

Drive Settings

Pull Distribution Point

PXE Settings

Multicast

Content Validation

Boundary Groups

Summary

Progress

Completion

### Specify roles for this server

Available roles:

- ☐ Application Catalog web service point
- ☐ Application Catalog website point
- ☐ Certificate registration point
- ☐ Cloud management gateway connection point
- ☐ Data Warehouse service point
- ☒ **Distribution point**
- ☐ Enrollment point
- ☐ Enrollment proxy point
- ☐ Fallback status point
- ☐ Management point
- ☐ Reporting services point
- ☐ Software update point
- ☐ State migration point

Description:

A distribution point contains source files for clients to download. You can control content distribution by using bandwidth, throttling, and scheduling options.

< Previous

Next >

Summary

Cancel



## Distribution point

General

Proxy

System Role Selection

**Distribution point**

Communication

Drive Settings

Pull Distribution Point

PXE Settings

Multicast

Content Validation

Boundary Groups

Summary

Progress

Completion

### Specify distribution point settings

Description:

Parallel Mac Management DP

- ☒ Install and configure IIS if required by Configuration Manager
- ☒ Enable and configure BranchCache for this distribution point
- ☒ Adjust the download speed to use the unused network bandwidth (Windows LEDBAT)
- ☒ Enable this distribution point for prestaged content
- ☒ Enable this distribution point to be used as Microsoft Connected Cache server

[Learn more](#)

[View Microsoft Connected Cache server License Terms](#)

- ☒ By checking this box, I acknowledge that I accept the License Terms.

Select the drive and disk space to be used for cache location. If you select Automatic, Configuration Manager selects the drive that has the most free space.

Local drive to be used:

Automatic

Disk space:

GB

100

- ☐ Retain cache when disabling the Connected Cache server

< Previous

Next >

Summary

Cancel



## Communication

General

Proxy

System Role Selection

Distribution point

Communication

Drive Settings

Pull Distribution Point

PXE Settings

Multicast

Content Validation

Boundary Groups

Summary

Progress

Completion

Specify how client computers or mobile devices communicate with this distribution point.

☐ HTTP

Does not support mobile devices or Mac computers.

☐ Allow clients to connect anonymously☒ HTTPS

Requires computers to have a valid PKI client certificate.

Allow intranet-only connections

If you manage Mac computers or have mobile devices that are enrolled by Configuration Manager, select an option that allows Internet client connections.

☒ Allow mobile devices to connect to this distribution point

Create a self-signed certificate or import a PKI client certificate.

☐ Create self-signed certificate

Set expiration date:

03-Mar-2119

1:18 PM

☒ Import certificate

Certificate:

C:\Temp\DPCertForParallel.pfx

Browse...

Password:

••••••••

&lt; Previous

Next &gt;

Summary

Cancel



## Drive Settings

General

Proxy

System Role Selection

Distribution point

Communication

Drive Settings

Pull Distribution Point

PXE Settings

Multicast

Content Validation

Boundary Groups

Summary

Progress

Completion

## Specify drive settings for this distribution point

Specify the space to reserve on each drive that is used by this distribution point. You can use drive space reserve to determine the space that remains free on the drive after content is stored on it.

Drive space reserve (MB):

50

The content library contains content that is distributed to this distribution point. To optimize hard disk space, the content library stores only one instance of each content files. The package share is used when you configure a package to allow clients to run a program from the distribution point.

Specify the locations for the content library and package share on this distribution point. If you select Automatic, Configuration Manager selects the drive that has the most free space when the distribution point is installed. Configuration Manager uses the secondary content library location only when insufficient space remains on the primary location.

Primary content library location:

Automatic

Secondary content library location:

Automatic

Primary package share location:

Automatic

Secondary package share location:

Automatic

&lt; Previous

Next &gt;

Summary

Cancel



## Pull Distribution Point

## General

## Proxy

## System Role Selection

## Distribution point

## Communication

## Drive Settings

## Pull Distribution Point

## PXE Settings

## Multicast

## Content Validation

## Boundary Groups

## Summary

## Progress

## Completion

## Specify settings to configure a pull distribution point

The site server notifies pull distribution points when there is content for them to download from a source distribution point.

☒ Enable this distribution point to pull content from other distribution points

Select source distribution points for this pull distribution point. Each entry is tried in turn, until the content is found. Source distribution points with the same priority will be randomly selected.

Source distribution points:

Name	Type	Priority
CB.RAMLAN.CA	On-premises	1

[Add...](#)[Remove](#)

&lt; Previous

Next &gt;

Summary

Cancel



## PXE Settings

## General

## Proxy

## System Role Selection

## Distribution point

## Communication

## Drive Settings

## Pull Distribution Point

## PXE Settings

## Multicast

## Content Validation

## Boundary Groups

## Summary

## Progress

## Completion

## Specify settings to install operating systems by using PXE boot

☒ Enable PXE support for clients

Windows Deployment Services will be installed if required

☒ Allow this distribution point to respond to incoming PXE requests

☒ Enable unknown computer support

☐ Enable a PXE responder without Windows Deployment Service

☒ Require a password when computers use PXE

Password:

••••••••

Confirm password:

••••••••

User device affinity:

Do not use user device affinity

Network interfaces

☒ Respond to PXE requests on all network interfaces

☐ Respond to PXE requests on specific network interfaces



Specify the PXE server response delay (seconds):

10

&lt; Previous

Next &gt;

Summary

Cancel



## Multicast

General

Proxy

System Role Selection

Distribution point

Communication

Drive Settings

Pull Distribution Point

PXE Settings

Multicast

Content Validation

Boundary Groups

Summary

Progress

Completion

## Specify multicast settings for operating system deployment

- ☐ Enable multicast to simultaneously send data to multiple clients  
Windows Deployment Services will be installed if required

## Multicast Connection Account

- ☒ Use the computer account of this distribution point to connect to the primary site database  
☐ Use another account

Set...

## Multicast address settings

- ☒ Use IPv4 addresses within any range  
☐ Use IPv4 addresses from the following range:

Start: End: 

## UDP port range for multicast:

Start: End: 

Maximum clients:

- ☐ Enable scheduled multicast

Session start delay (minutes):

Minimum session size (clients):

&lt; Previous

Next &gt;

Summary

Cancel



## Content Validation

General

Proxy

System Role Selection

Distribution point

Communication

Drive Settings

Pull Distribution Point

PXE Settings

Multicast

Content Validation

Boundary Groups

Summary

Progress

Completion

## Specify the content validation settings

Content validation verifies the integrity of packages on this distribution point. To review the validation states for packages, check the Content Status node in the Monitoring workspace.

- ☒ Validate content on a schedule

Occurs every 1 weeks on Saturday effective 03-Mar-2020 12:00 AM

Schedule...

## Content validation priority

Select the priority that you want to use for content validation. A high priority value might increase the CPU usage and disk activity on the distribution point during content validation.

&lt; Previous

Next &gt;

Summary

Cancel





## Boundary Groups

## General

## Proxy

## System Role Selection

Distribution point

Communication

Drive Settings

Pull Distribution Point

PXE Settings

Multicast

Content Validation

**Boundary Groups**

Summary

Progress

Completion

## Specify the boundary groups to associate with this site system

You can associate a site system role to a boundary group.

During content deployment, clients in a boundary group that is associated with this site system will use it as a source location for content.

Boundary groups:

Filter...	
Name	Description
Toronto	
Default-Site-Boundary-Group<TOR>	

Create...

Add...

Remove

&lt; Previous

Next &gt;

Summary

Cancel



## Summary

## General

## Proxy

## System Role Selection

Distribution point

Communication

Drive Settings

Pull Distribution Point

PXE Settings

Multicast

Content Validation

Boundary Groups

**Summary**

Progress

Completion

## The wizard will create a new site system server with the following settings

Details:

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

- Site System Name
  - PAR.RAMLAN.CA
- Site Code
  - TOR - Toronto Headquarters Site
- Settings
  - Public FQDN: Not specified
  - Installation Account: Computer Account
  - BranchCache - enabled: Yes
  - LEDBAT - enabled: Yes
  - Prestaged content - enabled: Yes
  - Delivery Optimization cache - enabled: Yes
- Roles
  - Distribution point
  - Description: Parallel Mac Management DP
  - Content pulling enabled: Yes
  - PXE-enabled: Yes
  - Multicast-enabled: No
- Proxy Settings
  - Proxy will not be enabled
- Source distribution points:
  - CB.RAMLAN.CA(1)
- Boundary Settings
  - Boundary Groups
    - Toronto
    - Default-Site-Boundary-Group<TOR>

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

&lt; Previous

Next &gt;

Summary

Cancel



## Completion

General

Proxy

System Role Selection

Distribution point

Communication

Drive Settings

Pull Distribution Point

PXE Settings

Multicast

Content Validation

Boundary Groups

Summary

Progress

Completion



## The Create Site System Server Wizard completed successfully

Details:

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

- ✓ Success: Site System Name
  - PAR.RAMLAN.CA
- ✓ Success: Site Code
  - TOR - Toronto Headquarters Site
- ✓ Success: Settings
  - Public FQDN: Not specified
  - Installation Account: Computer Account
  - BranchCache - enabled: Yes
  - LEDBAT - enabled: Yes
  - Prestaged content - enabled: Yes
  - Delivery Optimization cache - enabled: Yes
- ✓ Success: Roles
  - Distribution point
  - Description: Parallel Mac Management DP
  - Content pulling enabled: Yes
  - PXE-enabled: Yes
  - Multicast-enabled: No
- ✓ Success: Proxy Settings
  - Proxy will not be enabled
- Source distribution points:
  - CB.RAMLAN.CA(1)
- ✓ Success: Boundary Settings
- ✓ Success: Boundary Groups
  - Toronto
  - Default-Site-Boundary-Group<TOR>

To exit the wizard, click Close.

&lt; Previous

Next &gt;

Summary

Close

Wait for some time to get all the packages distributed to **PAR** (Out new DP). When you check Monitoring tab for Content Status – You should see this.

Overview ▶ Distribution Status ▶ Distribution Point Configuration Status

## Distribution Point Configuration Status 2 items

Icon	Distribution Point Name	Pull Distribution Point	PXE	Content Validation	Multicast	Messages	Last Status Date
✓	CB.RAMLAN.CA	No	Yes	Yes	No	384	02-Mar-2020 2:23 AM
✓	PAR.RAMLAN.CA	Yes	Yes	Yes	No	6	03-Mar-2020 1:30 PM

## PAR.RAMLAN.CA

## Distribution Point Properties

Status Type:	Success
Content Validation:	Yes
Multicast:	No
PXE:	Yes
Pull Distribution Point:	Yes

## Completion Statistics

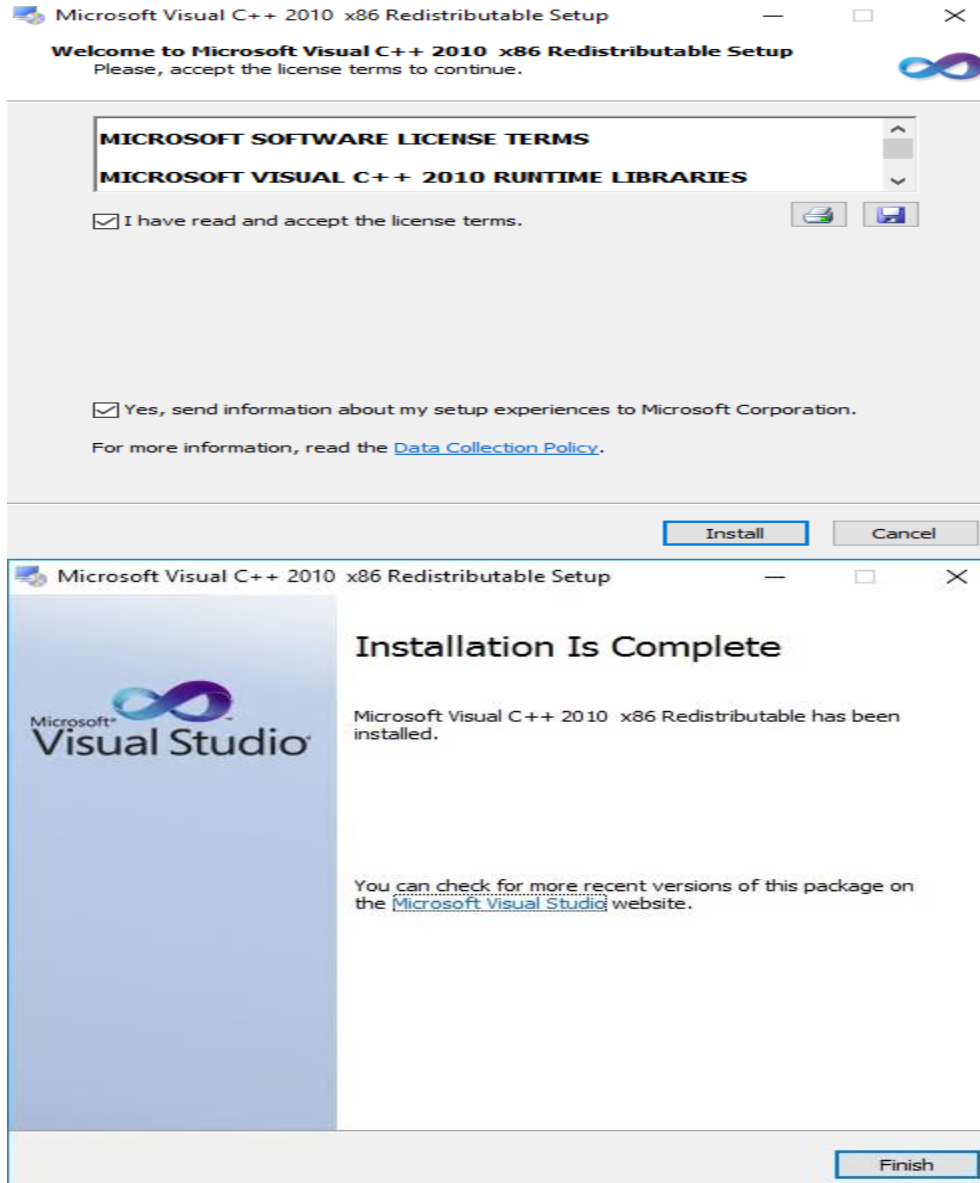


2 Targeted (Last Update: 03-Mar-2020 1:30 PM)

Success: 2  
 In Progress: 0  
 Failed: 0  
 Unknown: 0

### Parallel Mac Management Role Install:

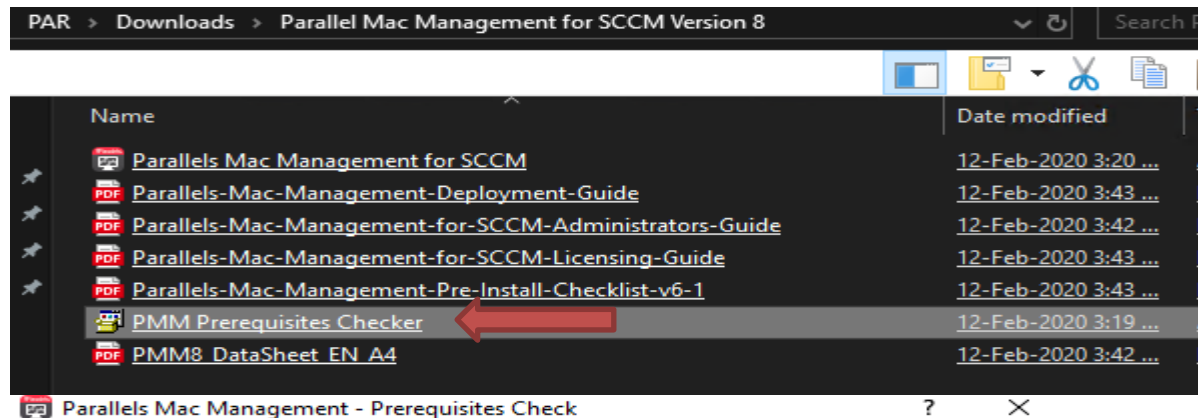
Now we are ready to install the roles on the member server **PAR**. If you haven't installed Microsoft Visual C++ 2010 Redistributable Package (x86), please do. Also make sure you have .NET 3.5, 4.0 are also installed.



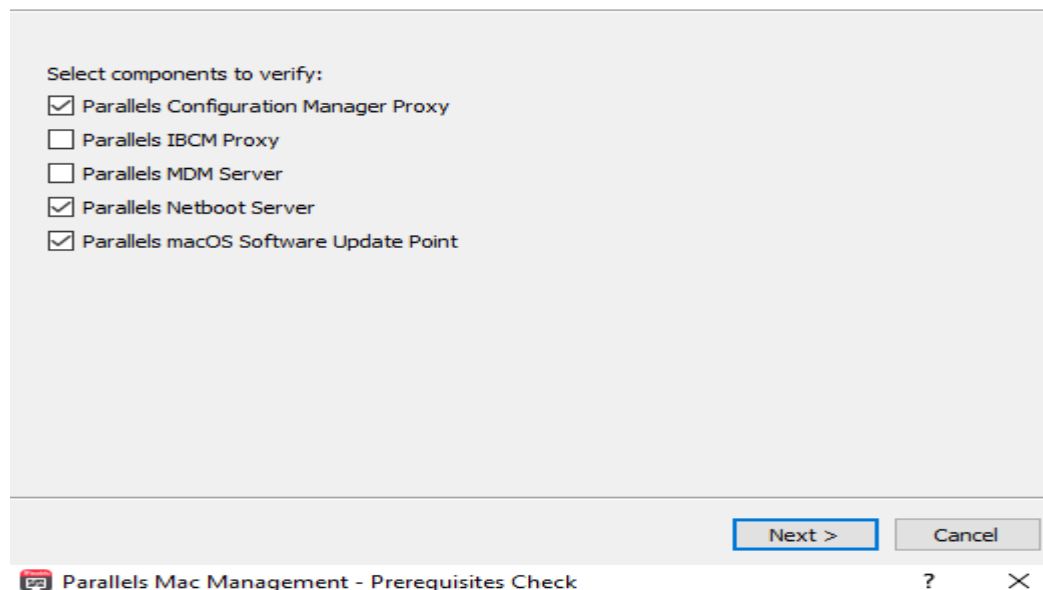
I checked within Server Manager for .NET 3.5 & 4.x installation. Both are installed.

- ▲ ■ .NET Framework 3.5 Features (1 of 3 installed)
  - ✓ .NET Framework 3.5 (includes .NET 2.0 and 3.0) (Installed)
  - ☐ HTTP Activation
  - ☐ Non-HTTP Activation
- ▲ ■ .NET Framework 4.6 Features (2 of 7 installed)
  - ✓ .NET Framework 4.6 (Installed)

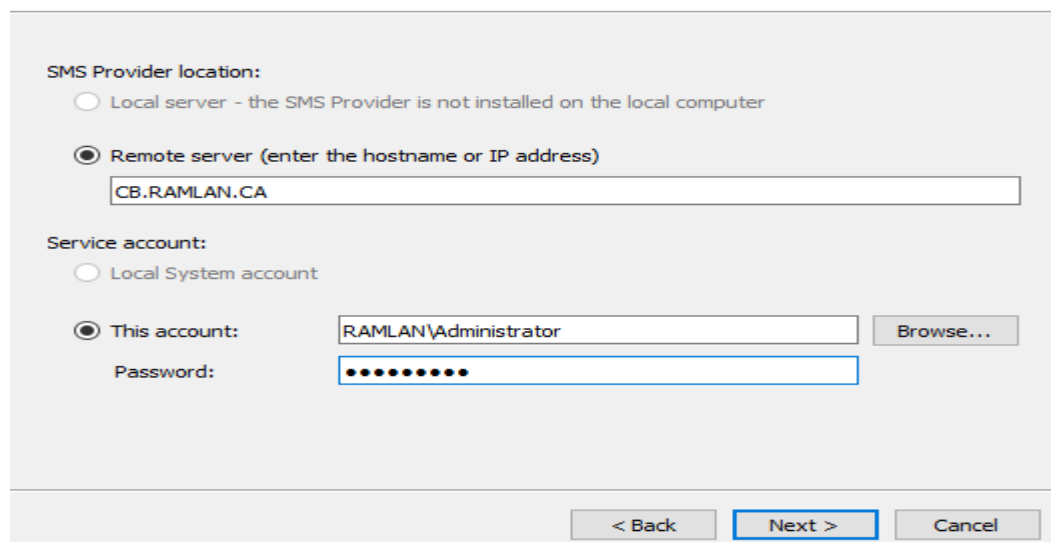
Before we start Parallel install, I want to run Pre Req-checker to make sure our install will go without any issue. You can run it from here



**The Prerequisites Check Wizard allows you to verify that your infrastructure meets Parallels Mac Management system requirements**



**Parallels Configuration Manager Proxy Settings**



**Parallels Configuration Manager Proxy Prerequisites Check**

Passed: 12 Failed: 0 Warnings: 0

Rerun

- ✓ The minimum supported version of MS Windows must be installed.
- ✓ Microsoft .NET Framework 4 must be installed.
- ✓ Current user "RAMLAN\Administrator" must have local administrator rights.
- ✓ Current user "RAMLAN\Administrator" must have Access, Launch, and Activation permissions for SMS WMI Provider on host "CB.RAMLAN.CA".
- ✓ Current user "RAMLAN\Administrator" must have full administrative rights in the Configuration Manager (domain: "ramlan.ca").
- ✓ "ParallelsServices" Active Directory container must exist, or current user "RAMLAN\Administrator" must have Read and Create All Child Objects permissions on the "System" Active Directory container (domain: "ramlan.ca").
- ✓ "Parallels" Active Directory container must exist, or current user "RAMLAN\Administrator" must have Read and Create All Child Objects permissions on the "Program Data" Active Directory container (domain: "ramlan.ca").
- ✓ Current user "RAMLAN\Administrator" must have the permissions to Read and Write the "ServicePrincipalName" property on the "Administrator" Active Directory object (domain: "ramlan.ca").
- ✓ Current user "RAMLAN\Administrator" must have the permissions to configure the "PMM\_TOR" database on the "CB.RAMLAN.CA" SQL Server. Or, in case the database haven't been created yet, the permissions to create databases on the server.
- ✓ Current user "RAMLAN\Administrator" must have the permissions to configure the "CM\_TOR" database on the "CB.RAMLAN.CA" SQL Server.
- ✓ Proxy service account "RAMLAN\Administrator" must have the permissions to List, Read(&Execute), and Write the content of the "\\CB.RAMLAN.CA\\SMS\_TOR\\INBOXES\\DDM.BOX" SCCM site server folder (domain: "ramlan.ca").
- ✓ The proxy service must not be installed on the other hosts within "TOR" site.

&lt; Back

Next &gt;

Cancel

**Parallels Netboot Server Prerequisites Check**

Passed: 8 Failed: 0 Warnings: 0

Rerun

- ✓ The minimum supported version of MS Windows must be installed.
- ✓ Microsoft .NET Framework 4 must be installed.
- ✓ The server must be configured as PXE enabled distribution point.
- ✓ WebServer (IIS) role must be installed and started.
- ✓ Windows Deployment Services role must be installed and started.
- ✓ Windows Deployment Services UDP ports must be set up.
- ✓ If DHCP is running on this computer, then Windows Deployment Services must not listen on port 67, otherwise it must listen on port 67.
- ✓ Windows Deployment Services TFTP root directory path must exist ('REMINST' share).

&lt; Back

Next &gt;


Cancel

**Parallels macOS Software Update Point Service Account**

Account name: RAMLAN\Administrator

Browse...

Password: ●●●●●●●●

 The account you choose must be able to publish local updates to WSUS.

&lt; Back

Next &gt;

Cancel

**Parallels macOS Software Update Point Prerequisites Check**

Passed: 8 Failed: 0 Warnings: 0

Rerun

- ✓ Microsoft .NET Framework 4 must be installed.
- ✓ Windows Server Update Service 3.0 or above must be installed.
- ✓ The current user ("RAMLAN\Administrator") must have local administrator rights.
- ✓ The specified "RAMLAN\Administrator" account must be a member of the "WSUS Administrators" group.
- ✓ The WSUS signing certificate must be deployed and accessible by "RAMLAN\Administrator".
- ✓ The WSUS signing certificate must not be expired.
- ✓ The public key for the WSUS signing certificate must be installed in the Root store.
- ✓ The public key for the WSUS signing certificate must be installed in the Trusted Publishers store.

&lt; Back

Next &gt;

Cancel

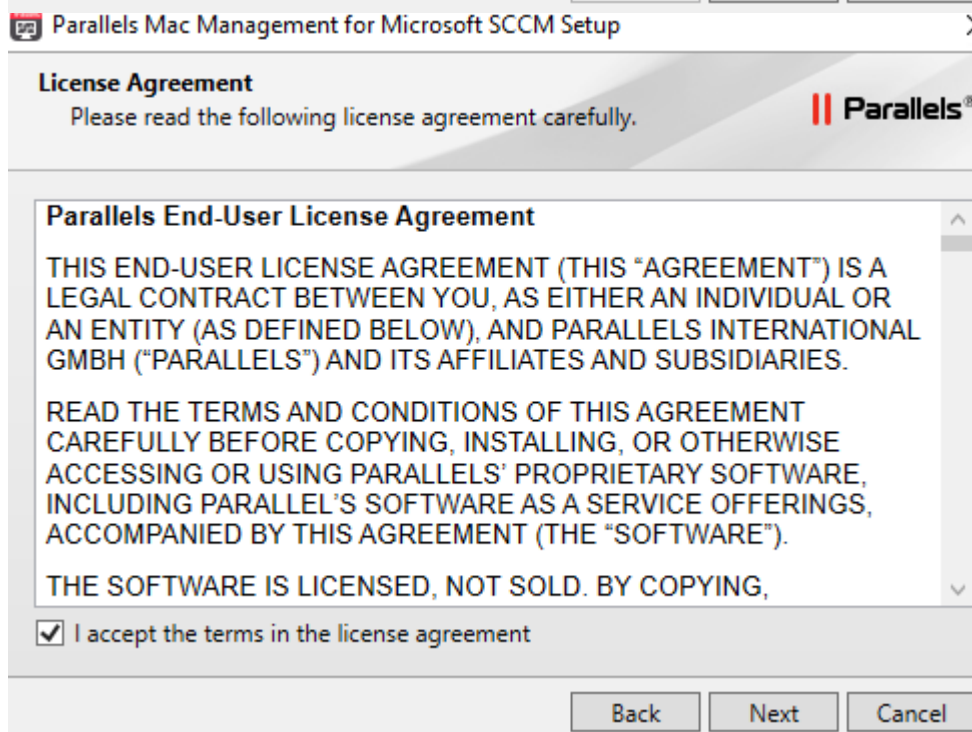
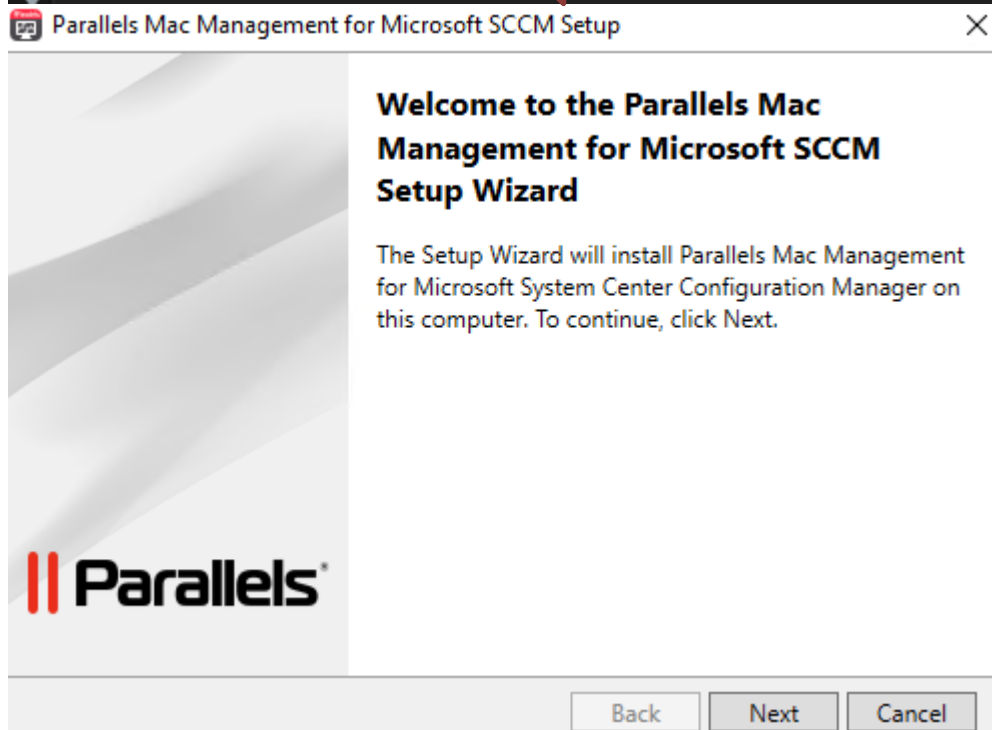
**Summary**

Parallels Mac Management prerequisites check is complete.  
You can review the results below.

Component Name	Warnings	Errors	Status
Parallels Configuration Manager Proxy	0	0	Passed
Parallels IBCM Proxy	-	-	Skipped
Parallels MDM Server	-	-	Skipped
Parallels Netboot Server	0	0	Passed
Parallels macOS Software Update Point	0	0	Passed

Close

Name	Date modified	Type
 <a href="#">Parallels Mac Management for SCCM</a>	12-Feb-2020 3:20 ...	Application






### Select Components

Check the components you want to install and uncheck the components you don't want to install.



☐ ConfigMgr Console Extension 

☒ Configuration Manager Proxy

☐ IBCM Proxy

☐ MDM Server

☒ NetBoot Server

☒ OS X Software Update Point

The OS X Software Update Point service publishes Apple software updates to Configuration Manager. It must be installed on a server where Windows Server Update Services (WSUS) is installed.

Back

Next

Cancel

### Ready to Install the Program

The wizard is ready to begin installation.



Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Back

Install

Cancel

## Setup Completed

The Setup Wizard has successfully installed Parallels Mac Management for Microsoft SCCM. Click Finish to exit the wizard.



Back

Finish


Cancel

### SMS Provider location

Specify the server where the SMS Provider is installed.

☐ Local server - the SMS Provider is not installed on the local computer

☒ Remote server (enter the hostname or IP address)

 The SMS Provider is a WMI provider that allows read and write access to the Configuration Manager site database. The SMS Provider can be installed on a dedicated server or on a local computer.



Next &gt;

Cancel

**Configuration Manager Proxy service account**

Specify the service account for the Configuration Manager Proxy. The account you choose must have read/write access to the SMS Provider.

☐ Local System account

☒ This account:

RAMLAN\Administrator

Browse...

Password:

••••••••



The Configuration Manager Proxy service enables Mac Clients to communicate with the Configuration Manager. The LocalSystem account is normally used when the SMS Provider is located on the same server as the Proxy service. A specific account may also be used if you want to manage the Configuration Manager Proxy service access rights.



< Back

Next >

Cancel

**Prerequisites Check**

Passed: 10 Failed: 0 Warnings: 0

Rerun

- ✓ Current user "RAMLAN\Administrator" must have Access, Launch, and Activation permissions for SMS WMI Provider on host "CB.RAMLAN.CA".
- ✓ Current user "RAMLAN\Administrator" must have full administrative rights in the Configuration Manager (domain: "ramlan.ca").
- ✓ "ParallelsServices" Active Directory container must exist, or current user "RAMLAN\Administrator" must have Read and Create All Child Objects permissions on the "System" Active Directory container (domain: "ramlan.ca").
- ✓ "Parallels" Active Directory container must exist, or current user "RAMLAN\Administrator" must have Read and Create All Child Objects permissions on the "Program Data" Active Directory container (domain: "ramlan.ca").
- ✓ Current user "RAMLAN\Administrator" must have the permissions to Read and Write the "ServicePrincipalName" property on the "Administrator" Active Directory object (domain: "ramlan.ca").



< Back

Next >

Cancel

**Prerequisites Check**

Passed: 13 Failed: 0 Warnings: 0

Rerun

- ✓ Current user "RAMLAN\ADMINISTRATOR" must have local administrator rights.
- ✓ Current user "RAMLAN\ADMINISTRATOR" must have Access, Launch, and Activation permissions for SMS WMI Provider on host "CM.RAMLAN.CA".
- ✓ Current user "RAMLAN\ADMINISTRATOR" must have full administrative rights in the Configuration Manager.
- ✓ "ParallelsServices" Active Directory container must exist, or current user "RAMLAN\ADMINISTRATOR" must have Read and Create All Child Objects permissions on the "System" Active Directory container.
- ✓ Current user "RAMLAN\ADMINISTRATOR" must have Read, Write, and Create All Child Objects permissions on the "ParallelsServices" Active Directory container.
- ✓ "Parallels" Active Directory container must exist, or current user "RAMLAN\ADMINISTRATOR" must have Read and Create All Child Objects permissions on the "Program Data" Active Directory container.
- ✓ "Parallels Management Suite" Active Directory container must exist, or current user "RAMLAN\ADMINISTRATOR" must have Read and Create All Child Objects permissions on the "Parallels" Active Directory container.
- ✓ Current user "RAMLAN\ADMINISTRATOR" must have Read, Write, and Create All Child Objects permissions on the "Parallels Management Suite" Active Directory container.
- ✓ Current user "RAMLAN\ADMINISTRATOR" must have policy administrative rights within the "Authorization Store" AzMan store Active Directory container.
- ✓ Current user "RAMLAN\ADMINISTRATOR" must have the permissions to Read and Write the "ServicePrincipalName" property on the "Administrator" Active Directory object.
- ✓ Current user "RAMLAN\ADMINISTRATOR" must have the permissions to configure the "PMM\_CAN" database on the "CM.RAMLAN.CA" SQL Server. Or, in case the database haven't been created yet, the permissions to create databases on the server.
- ✓ The proxy service must not be installed on the other hosts within "CAN" site.
- ✓ Proxy service account "RAMLAN\Administrator" must have the permissions to List, Read(&Execute), and Write the content of the "\\CM.RAMLAN.CA\SMS\_CAN\INBOXES\DDM.BOX" SCCM site server folder.

**Parallels Client certificate management settings**

Specify which connection Parallels Proxy and Mac clients use to communicate with distribution points and management points

☐ HTTP

There are no management points and no distribution points on this site that allow HTTP connection.

☒ HTTPS

Certificate Authority:

DC.RAMLAN.CA\RAMLAN-DC-CA

Browse...

Parallels Proxy certificate template:

Parallels Proxy

Browse...

Mac Client certificate template:

Parallel Proxy Client

Browse...



< Back

Next >

Cancel

Add required accounts to each of the roles below as per your requirement.

**Role-based security**

Review and modify, if necessary, the Configuration Manager Proxy role-based security settings.

**Roles**

Problem Monitor Users

Administrator

Enrollers

FileVault Key Administrators

**Users/Groups**

BUILTIN\Administrators

RAMLAN\Administrator

+

-



< Back

Next >

Cancel

**Role-based security**

Review and modify, if necessary, the Configuration Manager Proxy role-based security settings.

Roles	Users/Groups
Problem Monitor Users	BUILTIN\Administrators
Administrator	RAMLAN\Administrator
Enrollers	
FileVault Key Administrators	

+ -

Parallels® < Back Next > Cancel

**Role-based security**

Review and modify, if necessary, the Configuration Manager Proxy role-based security settings.



Roles	Users/Groups
Problem Monitor Users	BUILTIN\Users
Administrator	RAMLAN\Domain Admins
Enrollers	RAMLAN\Domain Users
FileVault Key Administrators	RAMLAN\Administrator

+ -

Parallels® < Back Next > Cancel

**Role-based security**

Review and modify, if necessary, the Configuration Manager Proxy role-based security settings.

Roles	Users/Groups
Problem Monitor Users	 RAMLAN\Domain Admins
Administrator	 RAMLAN\Administrator
Enrollers	
FileVault Key Administrators	

+ -

Parallels® < Back Next > Cancel


**Configuration Manager Proxy communication ports**

Specify TCP ports that the Configuration Manager Proxy will use to communicate with the Configuration Manager console and Mac Clients.

☐ Use custom ports


Port for incoming connections to SCCM Proxy:

Port for downloading Mac Client installation package:

 Configuration Manager Proxy uses these ports to serve requests from the Configuration Manager console and Mac Clients. It also publishes its current port configuration in Active Directory and the DNS in order to be discoverable by its clients if the port configuration changes.

**Customer Experience Program**

Parallels Customer Experience Program helps us to improve the quality and reliability of Parallels Mac Management.

-  If you accept, we will collect information about the way you use Parallels Mac Management. We will not collect any personal data, like your name, address, phone number, or keyboard input.  
[Click here](#) for more information.

- ☒ Yes, I am willing to participate in the Customer Experience Improvement Program.  
(Recommended)
- ☐ No, I don't wish to participate.



&lt; Back

Next &gt;

Cancel

**Configuration settings summary**

Review the Configuration Manager Proxy settings below. Click the Finish button to apply the new settings.

SMS provider host:	CB.RAMLAN.CA
SMS site code:	TOR
SCCM Proxy service account name:	RAMLAN\Administrator
Certificate management:	Using corporate Certificate Authority
Certificate Authority:	DC.RAMLAN.CA\RAMLAN-DC-CA
SCCM Proxy certificate template:	Parallels Proxy
Mac Client certificate template:	Parallel Proxy Client



&lt; Back

Finish

Cancel



Parallels Configuration Manager Proxy Configuration Wizard



Configuration Manager Proxy settings have been updated successfully.

To reconfigure Configuration Manager Proxy, run this Wizard again. The Wizard can be accessed from the Windows Start menu.

OK

Parallels NetBoot Server Configuration Wizard

**SMS Provider location**

Specify the server where the SMS Provider is installed.

☐ Local server - the SMS Provider is not installed on the local computer

☒ Remote server (enter the hostname or IP address)

CB.RAMLAN.CA

The SMS Provider is a WMI provider that allows read and write access to the Configuration Manager site database. The SMS Provider can be installed on a dedicated server or on a local computer.

Parallels®

Next >

Cancel

Parallels NetBoot Server Configuration Wizard

**Parallels NetBoot Server service account**

Specify the service account for the NetBoot Server. The account you choose must have read/write access to the SMS Provider.

☐ Local System account

☒ This account:

RAMLAN\Administrator

Browse...

Password:

••••••••

NetBoot server enables Macs to boot from the network. The LocalSystem account is normally used when the SMS Provider is located on the same server as the NetBoot server. A specific account may also be used if you want to manage the NetBoot service access rights.

Parallels®

< Back

Next >

Cancel

**NetBoot image path**

Specify a location for NetBoot images

Path:

C:\pmmimages

Browse...



The NetBoot server will store disk image files (.dmg) in the folder you specify here. The disk should have enough space to accommodate large image files.



&lt; Back

Next &gt;

Cancel

**Configuration settings summary**

Review the NetBoot Server settings below. Click the Next button to apply the new settings.

SMS provider host:	CB.RAMLAN.CA
SMS site code:	TOR
NetBoot Server service account name:	RAMLAN\Administrator
Boot files path:	C:\RemoteInstall\pmmboot
Images path:	C:\pmmimages



&lt; Back

Next &gt;

Cancel

**Configuration progress**

Applying configuration.

Applying configuration changes ...  
Set NetBoot Server service account to RAMLAN\Administrator  
Set NetBoot Server service options  
Write NetBoot Server settings  
Configuring WDS options  
Configuring IIS options  
Registering WDS Provider Dll  
Restarting WDS Server  
Starting Parallels NetBoot Service...  
Configuration was applied successfully.



&lt; Back

Finish

Cancel

**Parallels OS X Software Update Point service account**

Specify the service account for the Parallels OS X Software Update Point. The account you choose must be able to publish local updates to WSUS.

Account Name: RAMLAN\Administrator

Browse...

Password: ●●●●●●●●



The Parallels OS X Software Update Point service publishes Apple software updates to Windows Server Update Services so they can be distributed to Macs using Configuration Manager.



Next &gt;

Cancel

**Prerequisites Check**

Passed: 6 Failed: 0 Warnings: 0

Rerun

- ✓ The current user ("RAMLAN\Administrator") must have local administrator rights.
- ✓ The specified "RAMLAN\Administrator" account must be a member of the "WSUS Administrators" group.
- ✓ The WSUS signing certificate must be deployed and accessible by "RAMLAN\Administrator".
- ✓ The WSUS signing certificate must not be expired.
- ✓ The public key for the WSUS signing certificate must be installed in the Root store.
- ✓ The public key for the WSUS signing certificate must be installed in the Trusted Publishers store.



&lt; Back

Next &gt;

Cancel

**Configuration settings summary**

Review the Parallels OS X Software Update Point settings below. Click the Finish button to apply the new settings.

Parallels OS X Software Update Point service account name: RAMLAN\Administrator



&lt; Back

Finish

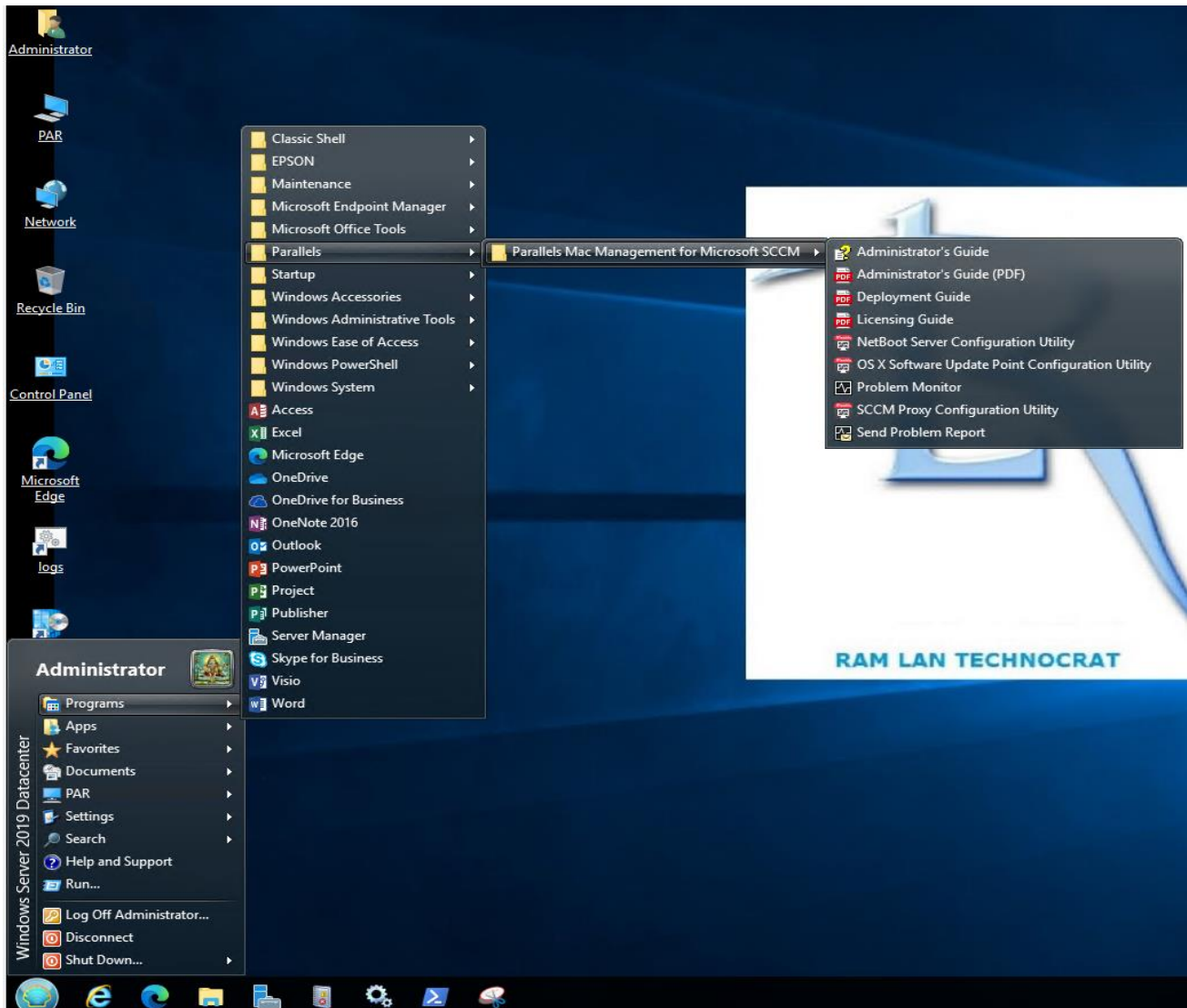
Cancel



Parallels Software Update Point service configuration settings have been applied successfully.

To reconfigure, run this Wizard again.

OK



Now we have to re-run PowerShell commands

Open PowerShell as administrator and run these commands one at a time

```
[Reflection.Assembly]::LoadWithPartialName("Microsoft.UpdateServices.Administration")
$updateServer = [Microsoft.UpdateServices.Administration.AdminProxy]::GetUpdateServer()
$config = $updateServer.GetConfiguration()
$config.SetSigningCertificate("C:\Users\ADMINISTRATOR.RAMLAN\Downloads\WSUSCertPar.pfx","01Jan
2009")
$config.Save()
```

The screenshot shows a Windows PowerShell window titled 'Administrator: Windows PowerShell'. The window displays the following commands and their output:

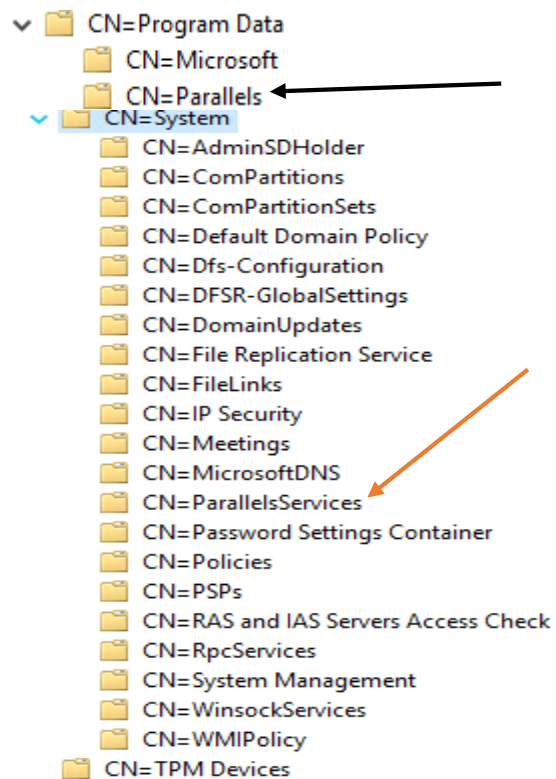
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\administrator.RAMLAN> [Reflection.Assembly]::LoadWithPartialName("Microsoft.UpdateServices.Administration")

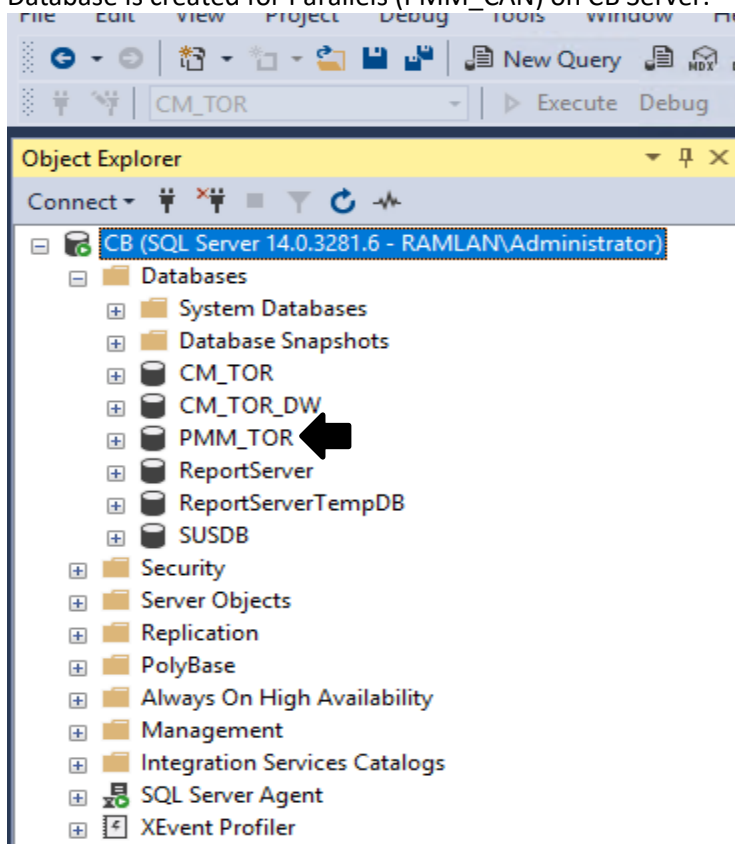
GAC      Version      Location
---      -
True     v4.0.30319    C:\Windows\Microsoft.Net\assembly\GAC_MSIL\Microsoft.UpdateServices.Administration\v4.0.4.0.0...
```

```
PS C:\Users\administrator.RAMLAN> $updateServer = [Microsoft.UpdateServices.Administration.AdminProxy]::GetUpdateServer()
PS C:\Users\administrator.RAMLAN> $config = $updateServer.GetConfiguration()
PS C:\Users\administrator.RAMLAN> $config.SetSigningCertificate("C:\Users\ADMINISTRATOR.RAMLAN\Downloads\WSUSCertPar.pfx","01Jan2009")
PS C:\Users\administrator.RAMLAN> $config.Save()
PS C:\Users\administrator.RAMLAN>
```

When you open ADSI Edit and look at the containers – we can see CN=Parallels within CN=Program Data and CN=ParallelsServices within CN=System.



Database is created for Parallels (PMM\_CAN) on CB Server.



## Activation Process:

We will complete the activation process. If you have trial edition – you can skip this step.

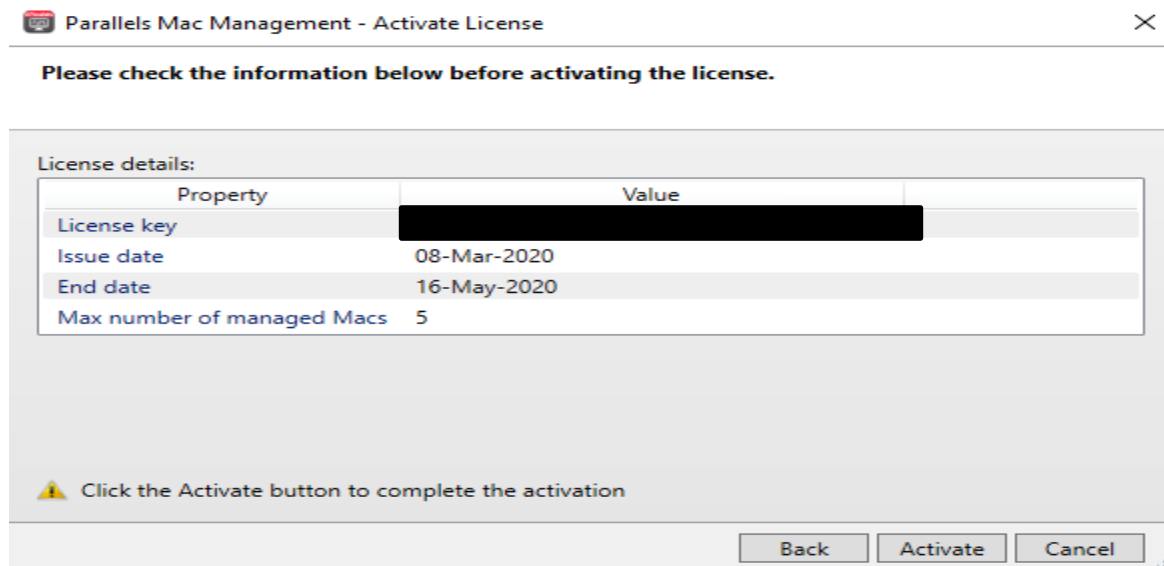
Open Configuration Manager Console –

Go to Administration – Parallels Mac Management – License

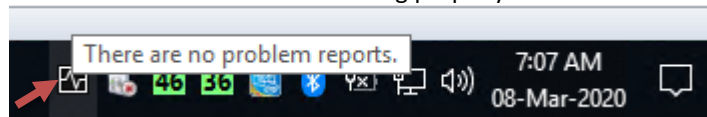
Click Activate License

Enter License Key

Click Activate



You should see this message – There is no problem reports which means the entire configuration is working and both **CB** and **PAR** are communicating properly.



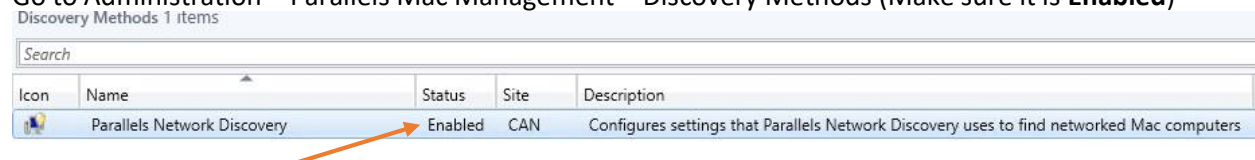
## Discover the Mac devices:

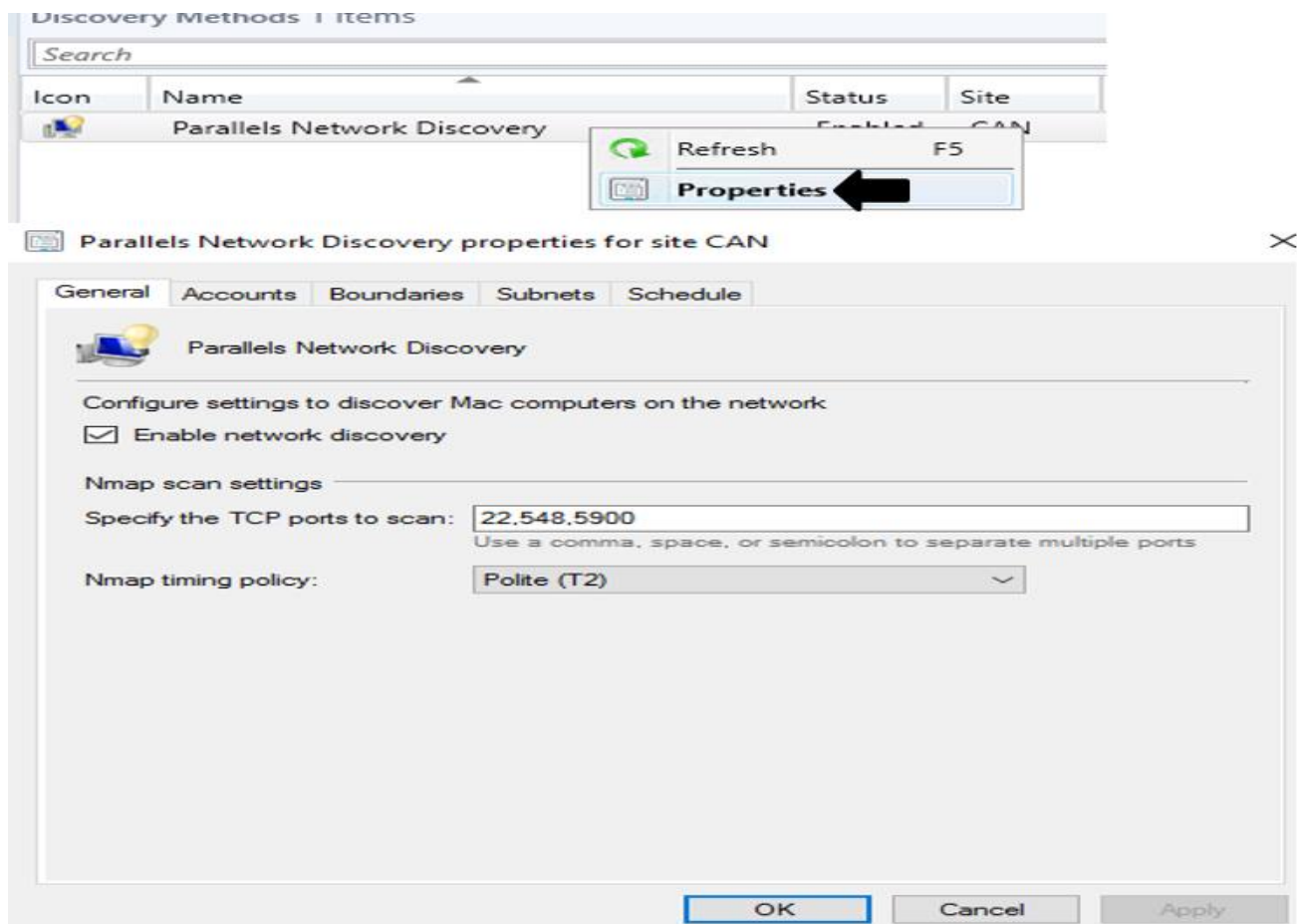
Parallels can leverage two methods to discover Mac devices in your environment. It can use the built-in ConfigMgr AD System Discovery, if the devices are domain joined or Parallels have their own Parallels Network Discovery. This can discover both AD join Macs and those that are not connected to a domain.

I will be using Parallels Network Discovery in this post since my Mac device is not joined to domain.

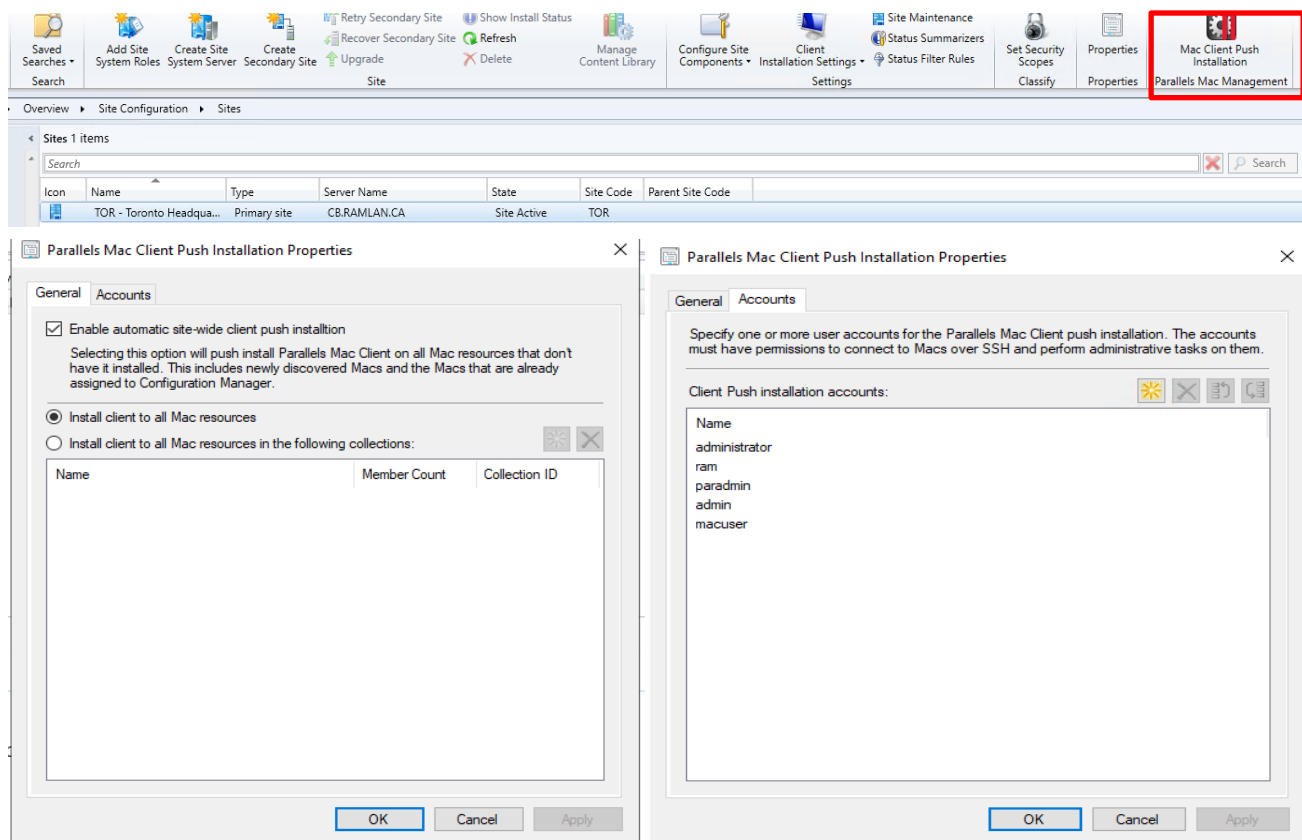
<http://kb.parallels.com/ca/122595>

Go to Administration – Parallels Mac Management – Discovery Methods (Make sure it is **Enabled**)





Go to Administration – Site Configuration - Sites





Client Push installation accounts:

Name

Mac OS X User Account

Specify an account with Mac OS X administrative privileges

User name: ram

Password: .....

Confirm password: .....

OK Cancel Help

I have added 5 accounts that, I have used on the Mac Machines. I have 1 Physical Mac and 2 Virtual Mac machines.

User Accounts – ram, admin, macuser, paradmin, administrator

Parallels Mac Client Push Installation Properties

General Accounts

☒ Enable automatic site-wide client push installation  
Selecting this option will push install Parallels Mac Client on all Mac resources that don't have it installed. This includes newly discovered Macs and the Macs that are already assigned to Configuration Manager.

☒ Install client to all Mac resources

☐ Install client to all Mac resources in the following collections:

Name	Member Count	Collection ID
------	--------------	---------------

Parallels Network Discovery properties for site TOR

General Accounts Boundaries Subnets Schedule

Select boundary groups or individual boundaries to be scanned by Parallels Network Discovery for Macs.

Boundary Groups:

Name	Boundaries Total/Selected
Boundary Groups	
Toronto	1/0

Boundaries: Filter...

Boundary	Type	Description
----------	------	-------------

Check All Uncheck All

OK Cancel Apply

Parallels Network Discovery properties for site TOR

General Accounts Boundaries Subnets Schedule

ConfigMgr can search specific subnets to discover resources. Specify the subnets for ConfigMgr to search.

Subnets to search:

Subnet	Mask	Name	Search
192.168.0.0	255.255.255.0	192.168.0.0	Enabled

☐ Search local subnets

OK Cancel Apply

Parallels Network Discovery properties for site TOR

General Accounts Boundaries Subnets Schedule

Specify when you want Parallels Network Discovery to run.

Schedule:

Occurs on 08-Mar-2020 7:18 AM, with a duration of 1 days

OK Cancel Apply

When discovery runs pma\_discovery.log will be created in C:\Windows\Logs folder on **PAR Server**

If devices are discovered they will appear in the ConfigMgr console. After some time, you will see Parallel Mac Management ICON under System Preferences on the Mac machine. Below is the screen shot.

Overview ▸ Devices

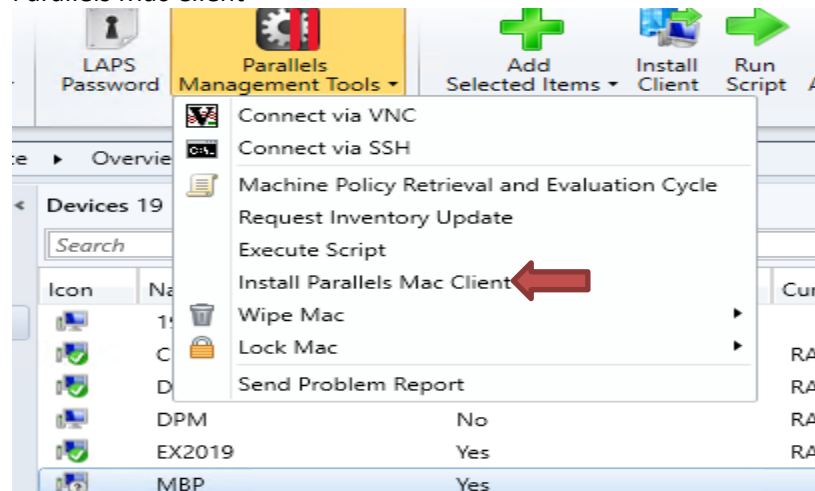
Devices 19 items

Search

Icon	Name	Client	Primary User(s)	Currently Logged on User	Site Code	Client Activity	Client Type	Client Version
	192.168.0.1	No					None	
	CB	Yes		RAMLAN\Administrator	TOR	Active	Computer	5.00.8913.1032
	DC	Yes		RAMLAN\Administrator	TOR	Active	Computer	5.00.8913.1032
	DPM	No		RAMLAN\Administrator			None	5.00.8913.1008
	EX2019	Yes		RAMLAN\Administrator	TOR	Active	Computer	5.00.8913.1032
	MBP	Yes			TOR	Active	Computer	5.8.1.2-1-PMA

You can also install Parallel Mac Client manually as detailed below:

Go to Assets and Compliance – Device – Select Mac Device – Click Parallels Management Tools – Install Parallels Mac Client



Push Install Parallels Mac Clients

Specify an account for establishing an SSH connection with Mac computers

☒ Use accounts from Parallels Mac Client push installation properties

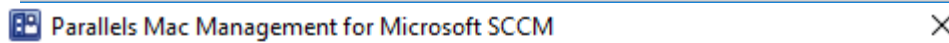
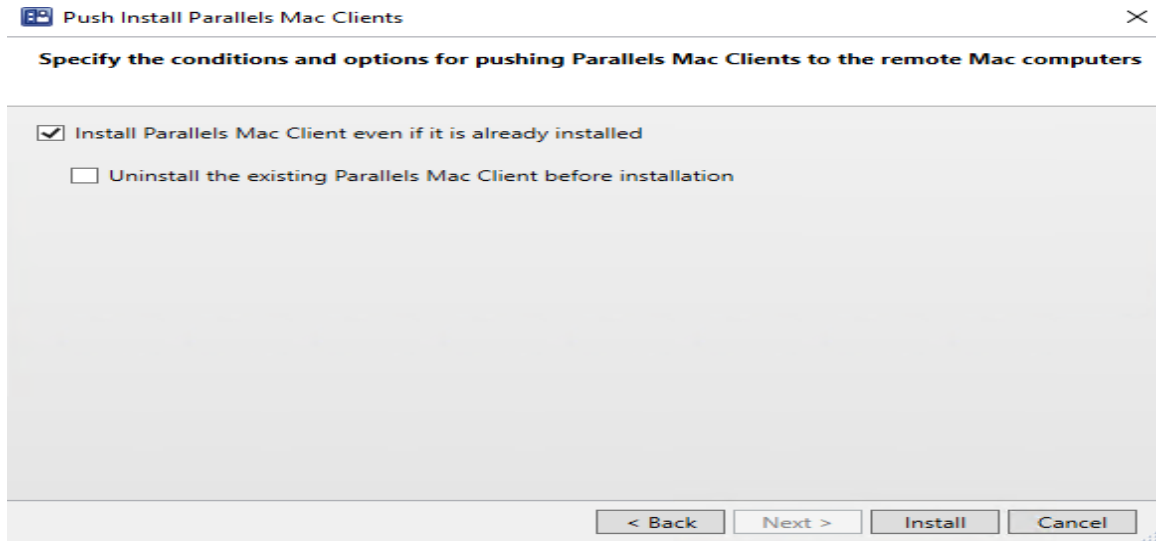
ram  
ramlan  
macuser  
admin

☐ Specify a user account

User name:  Browse...

Password:

< Back Next > Install Cancel



## Installing the Client Software

You can hide this dialog, and SCCM will continue installing the client software on the selected Macs. Or you can Cancel this operation.

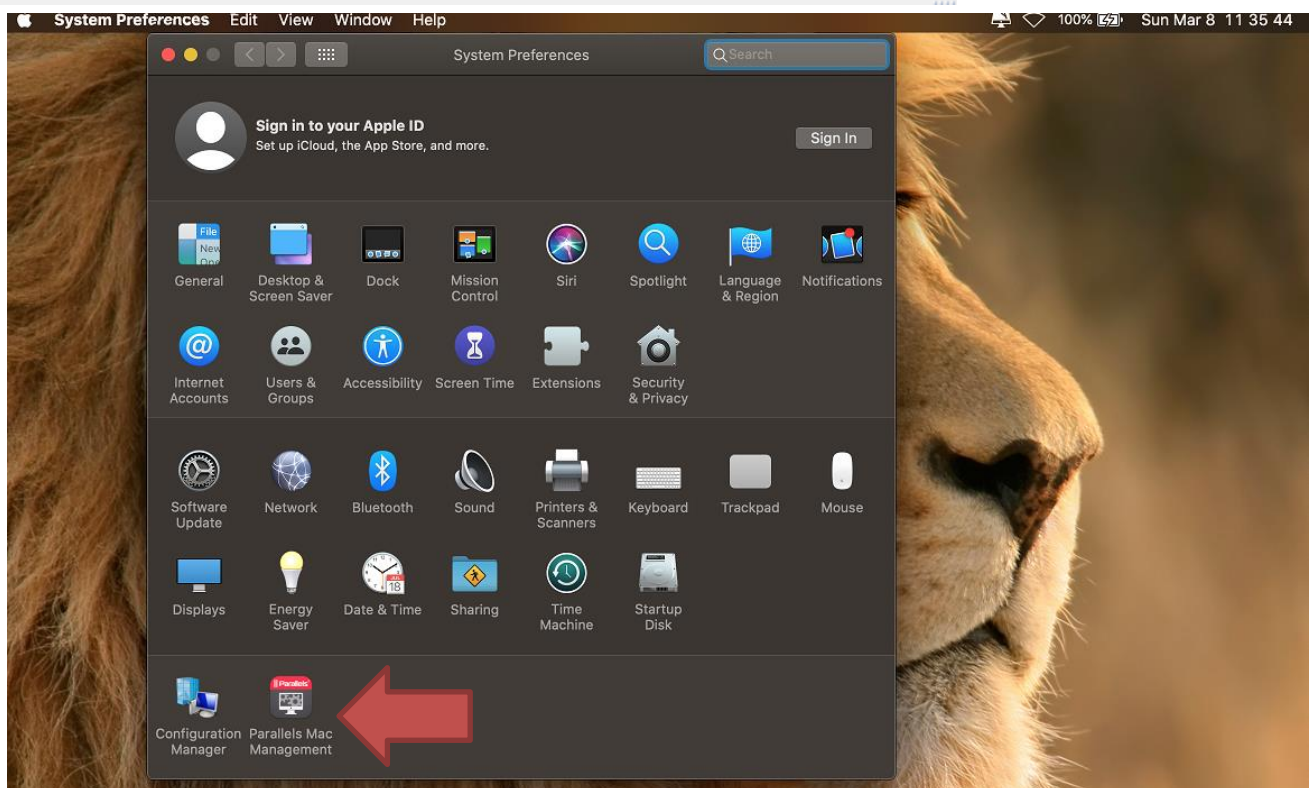
Macs processed: 1 of 1. Succeeded on 1, failed on 0.



Details

Hide

Cancel



Now we have completed all the steps required in implementing Parallels Mac Management version 8.1 for SCCM.

Next series, I will cover the following:

1. Creating boot & system image
2. Creating build and capture image
3. Create and deploy task sequence
4. Create mac application and deploy to mac collection
5. Deploy mac updates

Thanks

**Ram Lan**  
**8<sup>th</sup> Jan 2020**