

RBAC for DSS Support Group

In this post, I will show you how to create a new RBAC and provide DSS Support group the permission to install/reinstall/uninstall configuration manager client from Primary Site Console.

We want DSS Support group techs to install configuration manager client from the console to workstations running Windows 7 that has old configuration manager client and old software center.

As you can see from below screen shots there is no DSS Support RBAC or DSS Users within the console.

The screenshot displays the Primary Site Console interface, showing the 'Security Roles' and 'Administrative Users' sections. The 'Security Roles' section lists 15 built-in roles, and the 'Administrative Users' section lists 3 users.

Security Roles 15 items

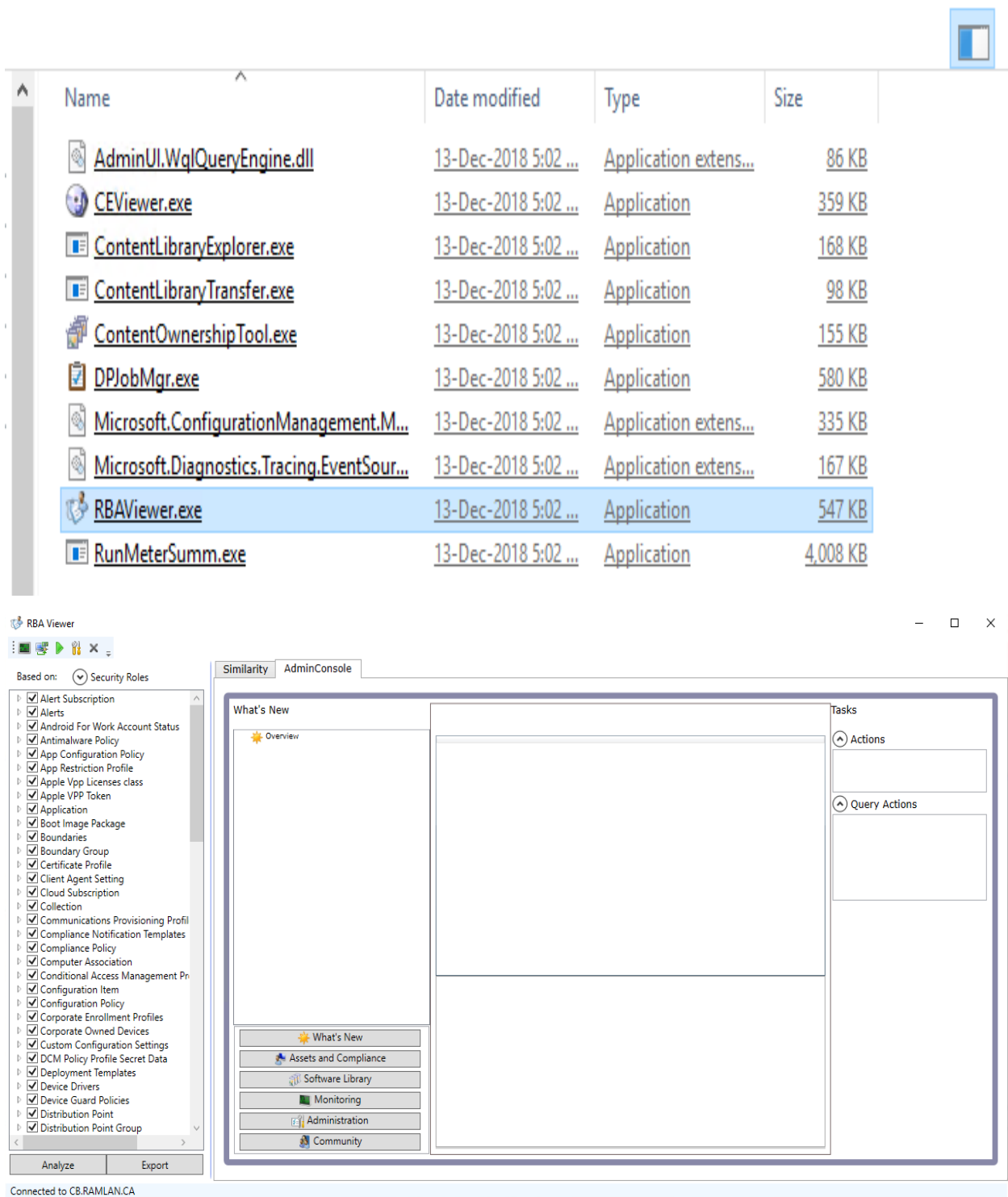
Icon	Name	Role Type	User Count
	Application Administrator	Built-in role	0
	Application Author	Built-in role	0
	Application Deployment Manager	Built-in role	0
	Asset Manager	Built-in role	0
	Company Resource Access Manager	Built-in role	0
	Compliance Settings Manager	Built-in role	0
	Endpoint Protection Manager	Built-in role	0
	Full Administrator	Built-in role	3
	Infrastructure Administrator	Built-in role	0
	Operating System Deployment Manager	Built-in role	0
	Operations Administrator	Built-in role	0
	Read-only Analyst	Built-in role	0
	Remote Tools Operator	Built-in role	0
	Security Administrator	Built-in role	0
	Software Update Manager	Built-in role	0

Administrative Users 3 items

Icon	Account Name	Account Display Name	Security Roles
	RAMLAN\Administrator	Administrator	"Full Administrator"
	RAMLAN\ram	Ram	"Full Administrator"
	RAMLAN\ramlan	Ram Lan	"Full Administrator"

We will create a new RBAC for DSSSupport Group. For this we need to open this tool from the server.

CB > OS (C:) > Program Files > Microsoft Configuration Manager > cd.latest > SMSSETUP > TOOLS > ServerTools

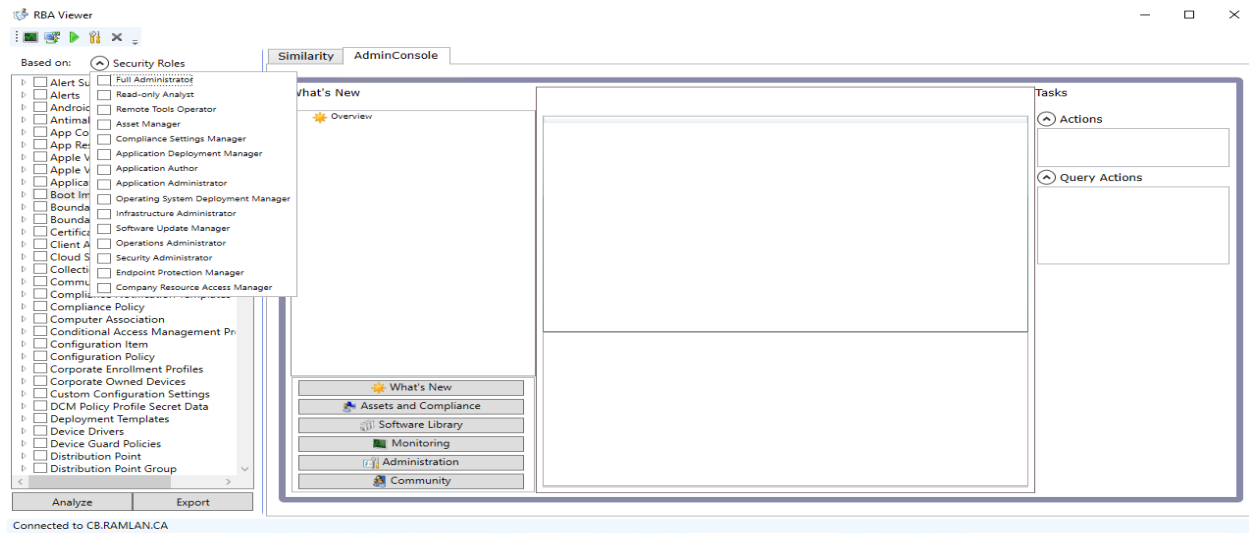


The first screenshot shows a file explorer window with the following table of files:

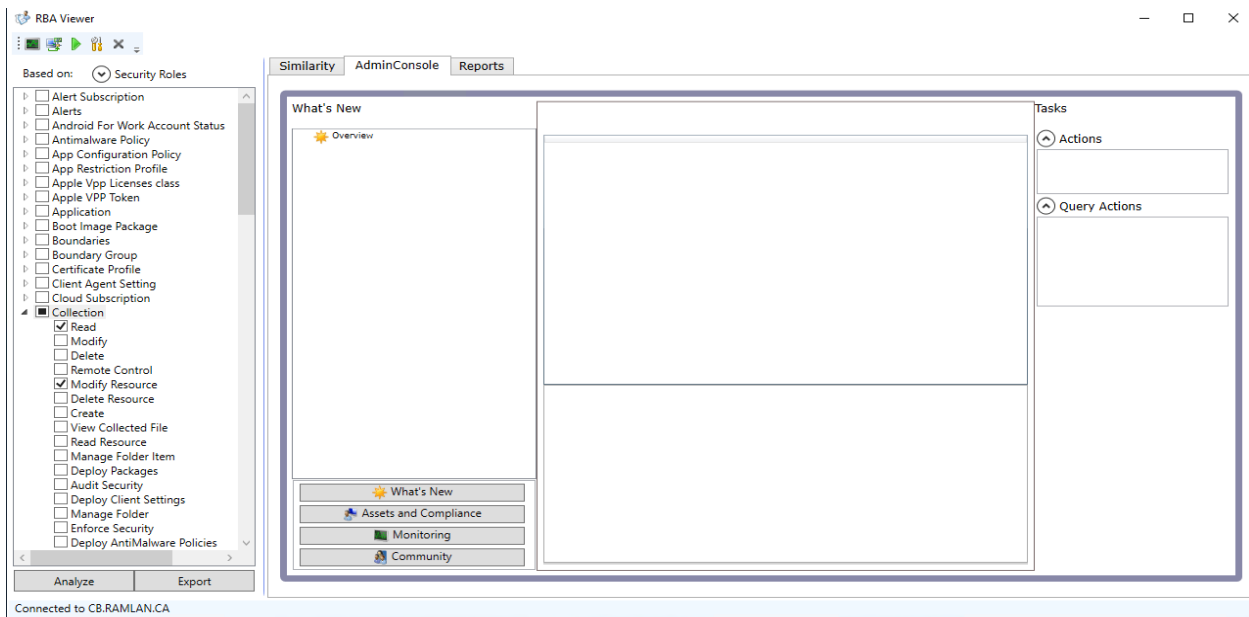
Name	Date modified	Type	Size
AdminUI.WqlQueryEngine.dll	13-Dec-2018 5:02 ...	Application extens...	86 KB
CEViewer.exe	13-Dec-2018 5:02 ...	Application	359 KB
ContentLibraryExplorer.exe	13-Dec-2018 5:02 ...	Application	168 KB
ContentLibraryTransfer.exe	13-Dec-2018 5:02 ...	Application	98 KB
ContentOwnershipTool.exe	13-Dec-2018 5:02 ...	Application	155 KB
DPJobMgr.exe	13-Dec-2018 5:02 ...	Application	580 KB
Microsoft.ConfigurationManagement.M...	13-Dec-2018 5:02 ...	Application extens...	335 KB
Microsoft.Diagnostics.Tracing.EventSour...	13-Dec-2018 5:02 ...	Application extens...	167 KB
RBAViewer.exe	13-Dec-2018 5:02 ...	Application	547 KB
RunMeterSumm.exe	13-Dec-2018 5:02 ...	Application	4,008 KB

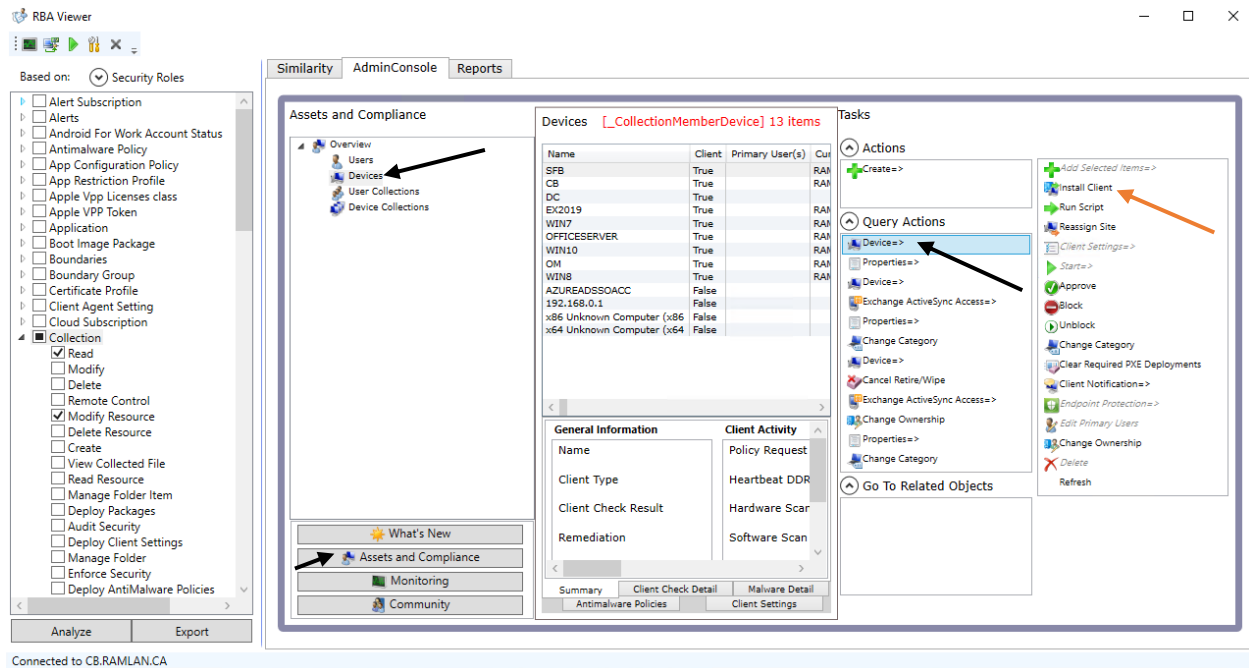
The second screenshot shows the RBA Viewer application interface. It has a 'Based on:' dropdown set to 'Security Roles'. A list of roles is shown on the left, including 'Alert Subscription', 'Alerts', 'Android For Work Account Status', 'Antimalware Policy', 'App Configuration Policy', 'App Restriction Profile', 'Apple Vpp Licenses class', 'Apple VPP Token', 'Application', 'Boot Image Package', 'Boundaries', 'Boundary Group', 'Certificate Profile', 'Client Agent Setting', 'Cloud Subscription', 'Collection', 'Communications Provisioning Profil', 'Compliance Notification Templates', 'Compliance Policy', 'Computer Association', 'Conditional Access Management Pn', 'Configuration Item', 'Configuration Policy', 'Corporate Enrollment Profiles', 'Corporate Owned Devices', 'Custom Configuration Settings', 'DCM Policy Profile Secret Data', 'Deployment Templates', 'Device Drivers', 'Device Guard Policies', 'Distribution Point', and 'Distribution Point Group'. The 'AdminConsole' tab is active, showing a 'What's New' section with 'Overview' and a 'Tasks' section with 'Actions' and 'Query Actions'. At the bottom, there are buttons for 'Analyze' and 'Export'. The status bar at the bottom indicates 'Connected to CB.RAMLAN.CA'.

Click Security Roles and deselect Full Administrator first. Then select Remote Tools Operator. We will be using this group to create a new RBAC for DSSSupport.

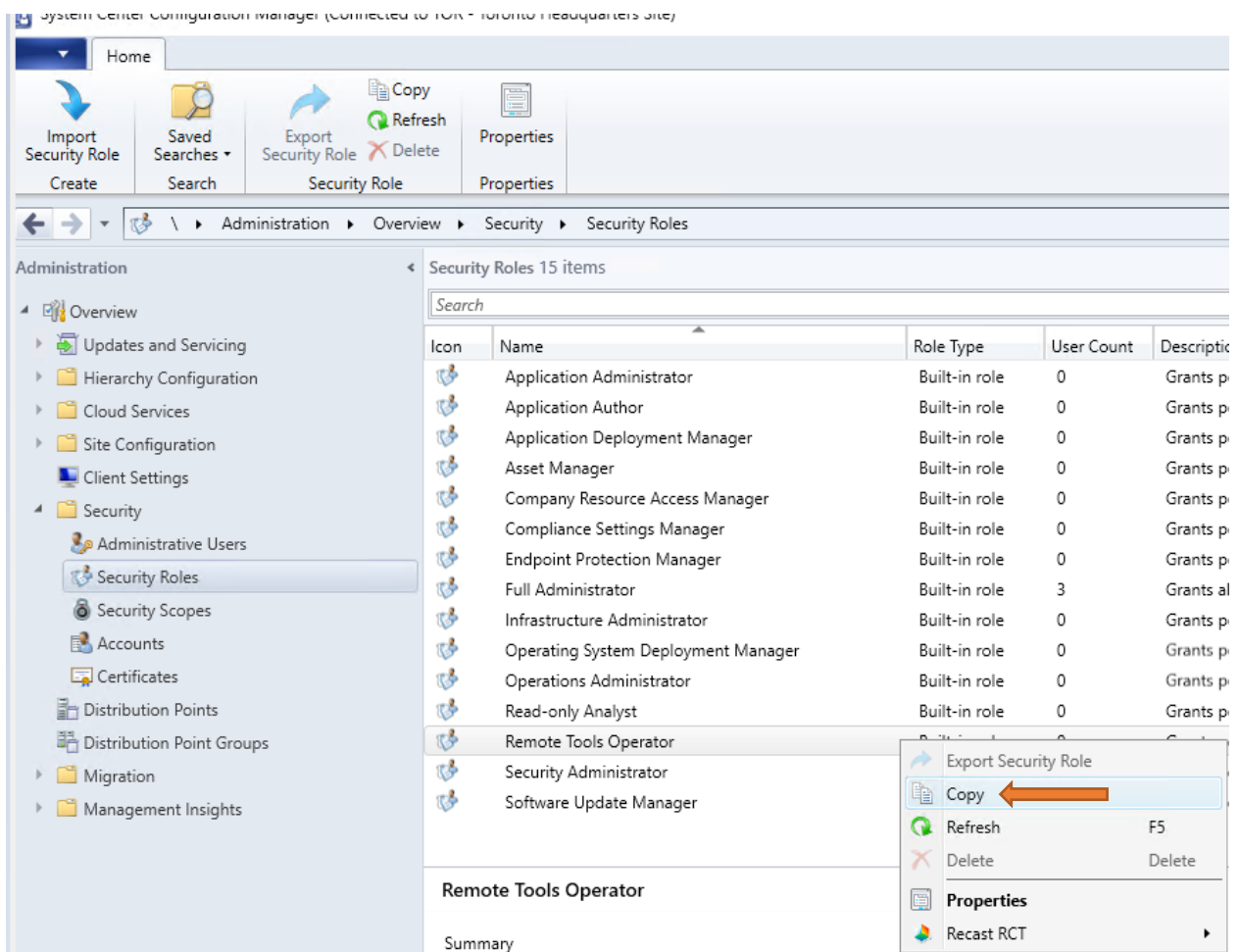


Select these and click Analyze






Now we know what permission we want for DSSSupport Group. We will do the following.



For Collection – Read and Modify Resource = Yes

 Copy Security Role ✕

Specify details for the customized copy of the selected security role.

Name:

Description:


Based on: Remote Tools Operator

Customize the permissions for this copy of the security role.

Permissions:

>	Certificate Profile	
>	Client Agent Setting	
>	Cloud Subscription	
✓	Collection	Read, Modify Resource
	Audit Security	No
	Control OOB	No
	Create	No
	Delete	No
	Delete Resource	No
	Deploy Antimalware Policies	No
	Deploy Applications	No
	Deploy Client Settings	No
	Deploy Configuration Items	No
	Deploy Configuration Policies	No
	Deploy Packages	No
	Deploy Software Updates	No

For Site – Read = Yes

 Copy Security Role ✕

Specify details for the customized copy of the selected security role.

Name:

Description:

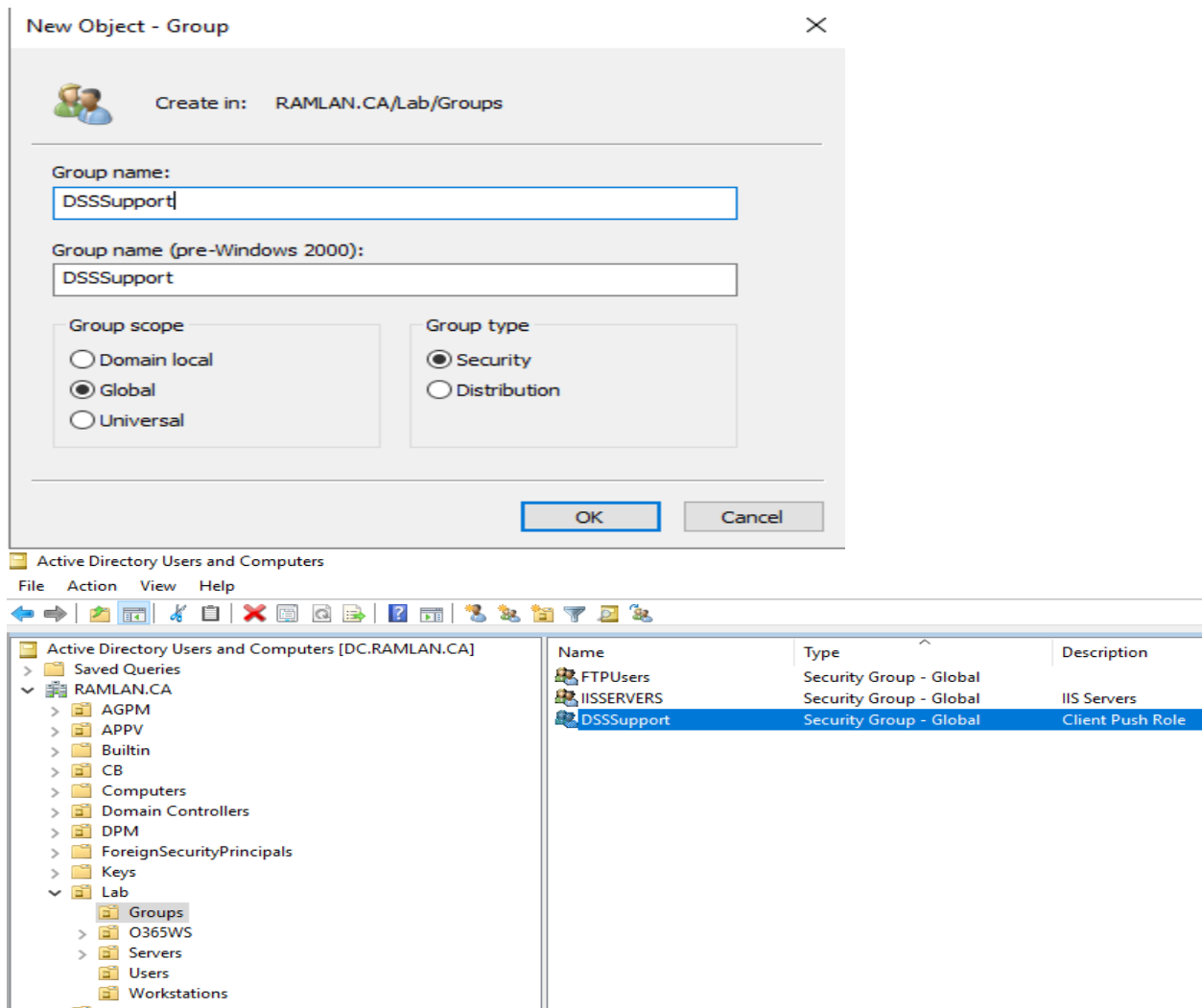
Based on: Remote Tools Operator

Customize the permissions for this copy of the security role.

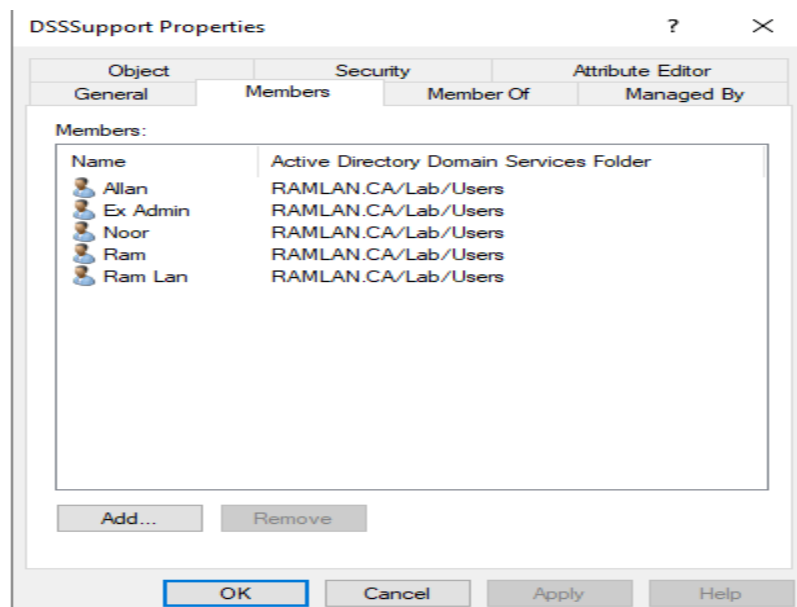
Permissions:

>	Sideload Key	
✓	Site	Read
	Create	No
	Delete	No
	Import Computers	No
	Manage Certificates for Operating System	No
	Manage Status Filters	No
	Meter Site	No
	Modify	No
	Modify Client Status Settings	No
	Modify Exchange Server Connector Policy	No
	Modify Report	No
	Read	Yes
	Read Client Status Settings	No
	Run Report	No
	Set Security Scope	No

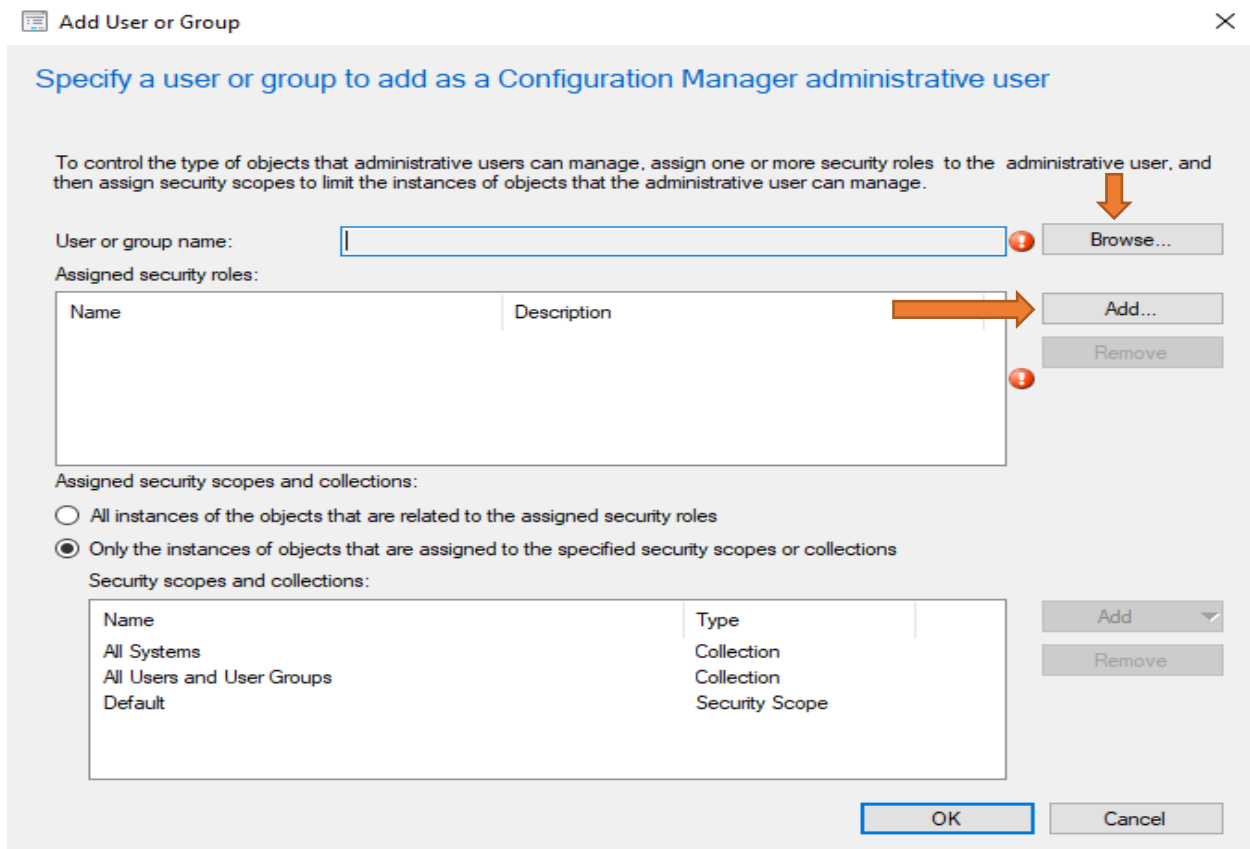
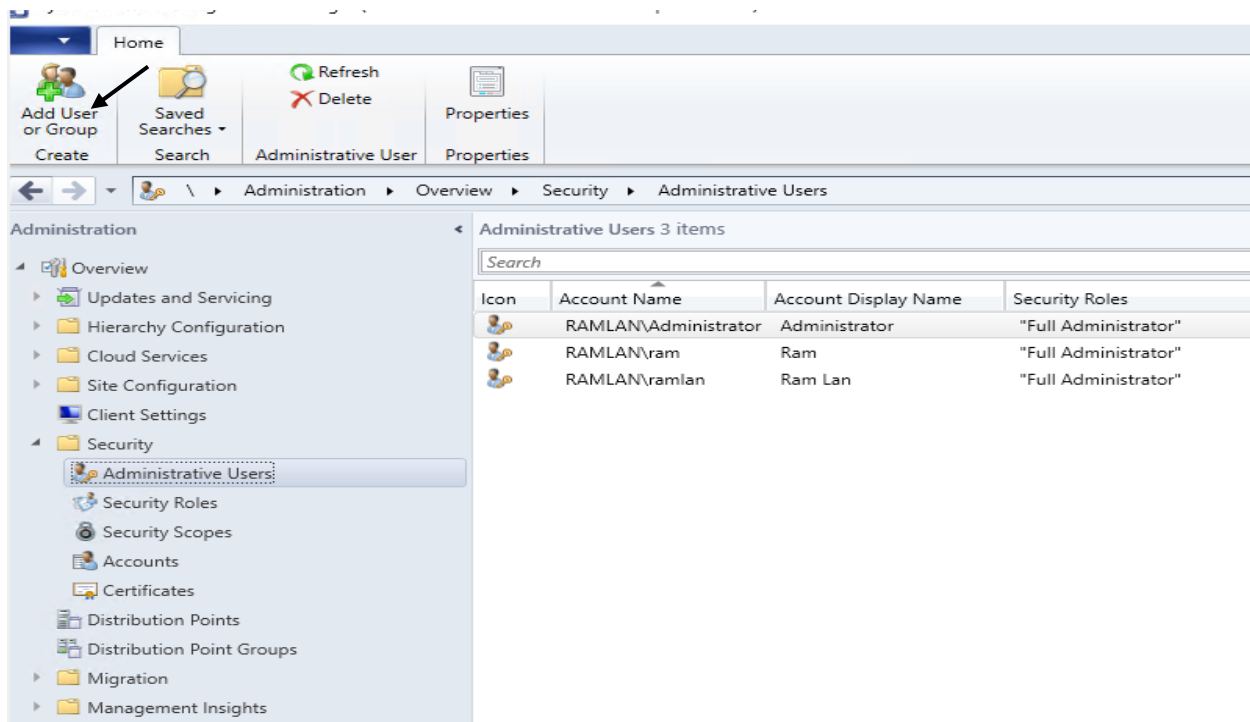
I have created a Security Group Called DSSSupport.



Then added few users to this group for testing.



Now we will go back to Console and Add a Group.



Add Security Role



Select one or more security roles to associate with this administrative user or group. Only unassigned roles that you have permission to delegate appear in the list.

Available security roles:

- ☐ Application Administrator
- ☐ Application Author
- ☐ Application Deployment Manager
- ☐ Asset Manager
- ☐ Company Resource Access Manager
- ☐ Compliance Settings Manager
- ☒ DSS Support Client Push Role
- ☐ Endpoint Protection Manager
- ☐ Full Administrator
- ☐ Infrastructure Administrator
- ☐ Operating System Deployment Manager
- ☐ Operations Administrator
- ☐ Read-only Analyst
- ☐ Remote Tools Operator
- ☐ Security Administrator

Description:

OK

Cancel

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:

RAMLAN\DSSSupport

Browse...

Assigned security roles:

Name	Description
DSS Support Client Push Role	This will provide permission for this group to install ...

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:

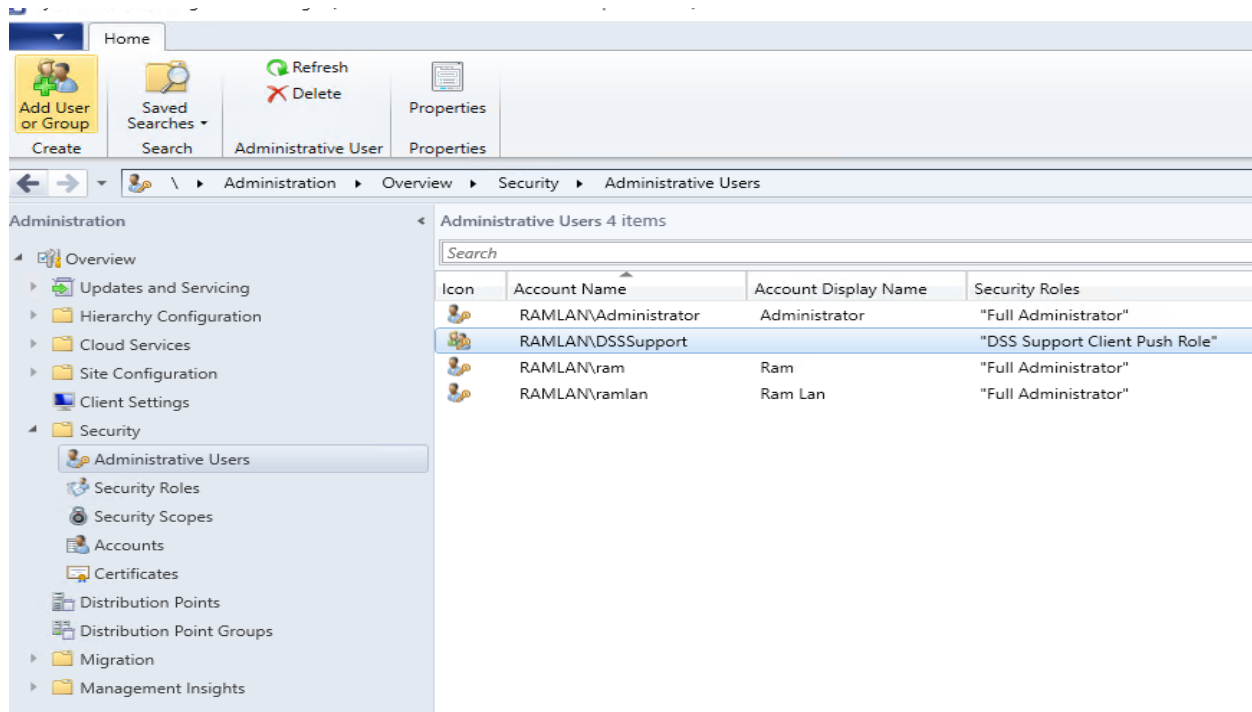
Name	Type
All Systems	Collection
All Users and User Groups	Collection
Default	Security Scope

Add

Remove

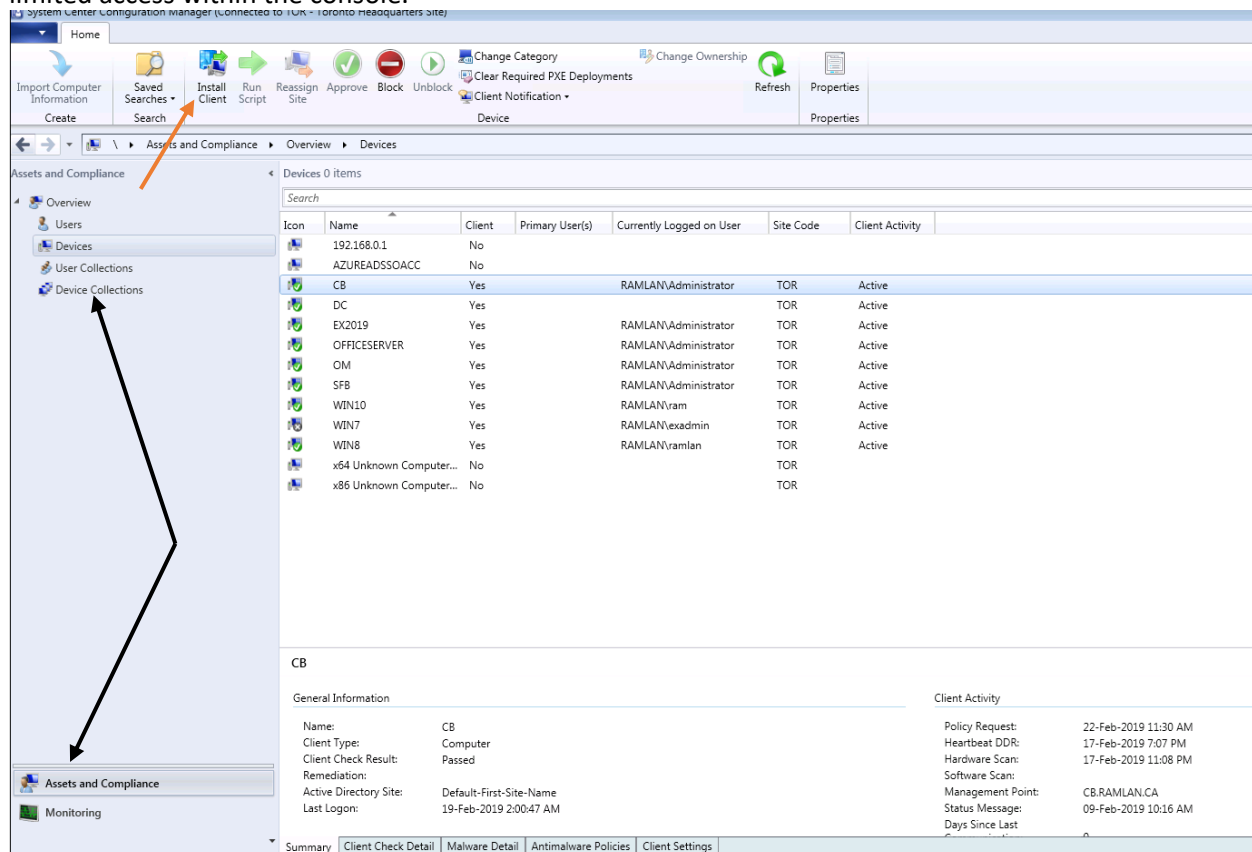
OK

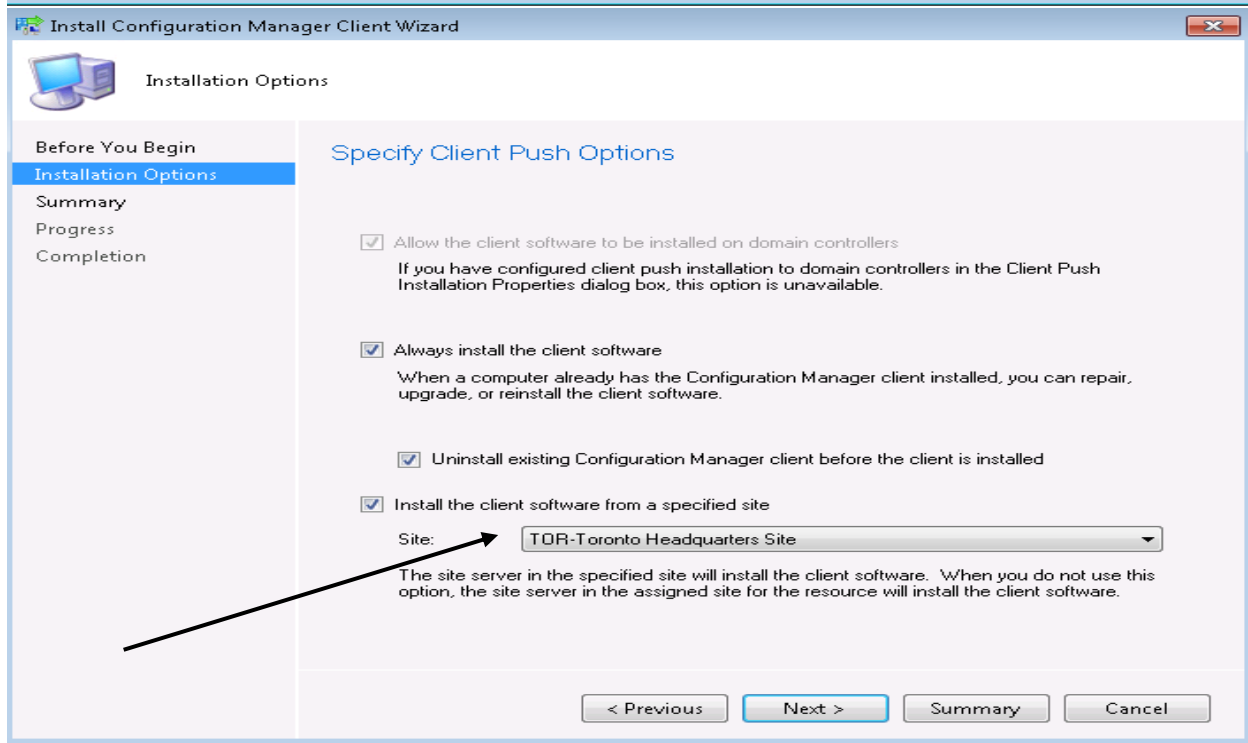
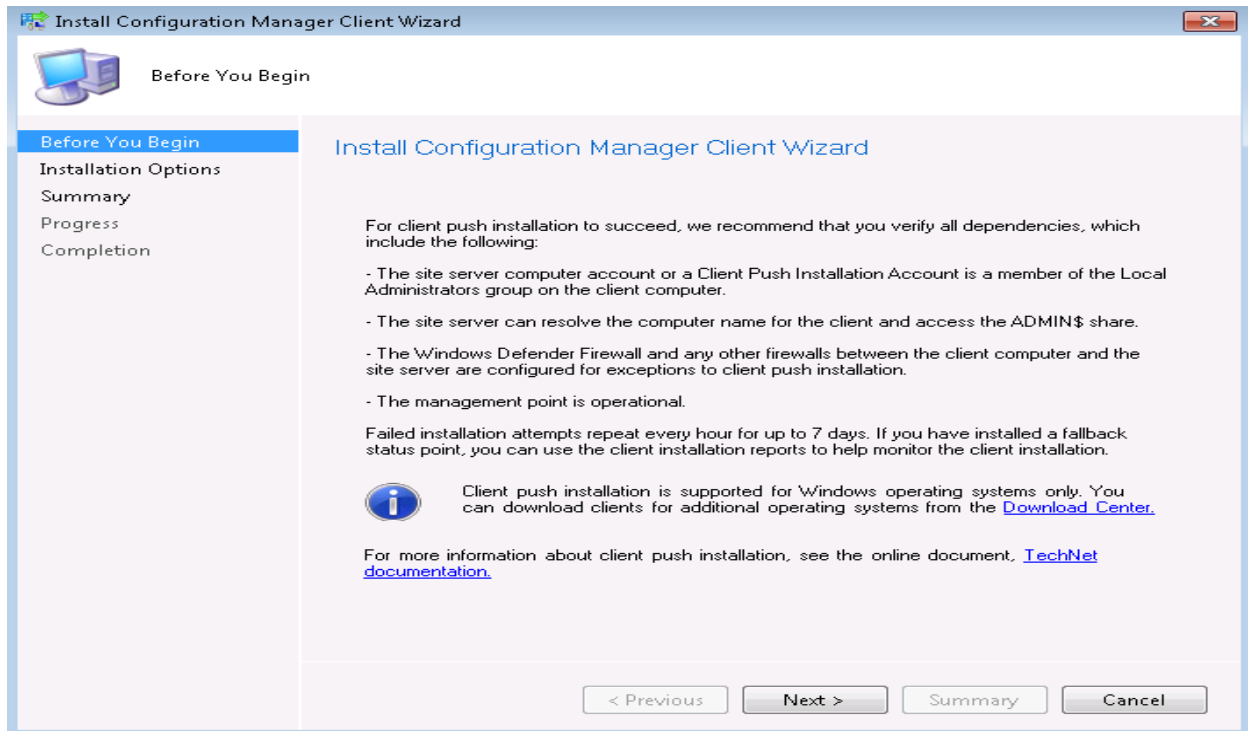
Cancel



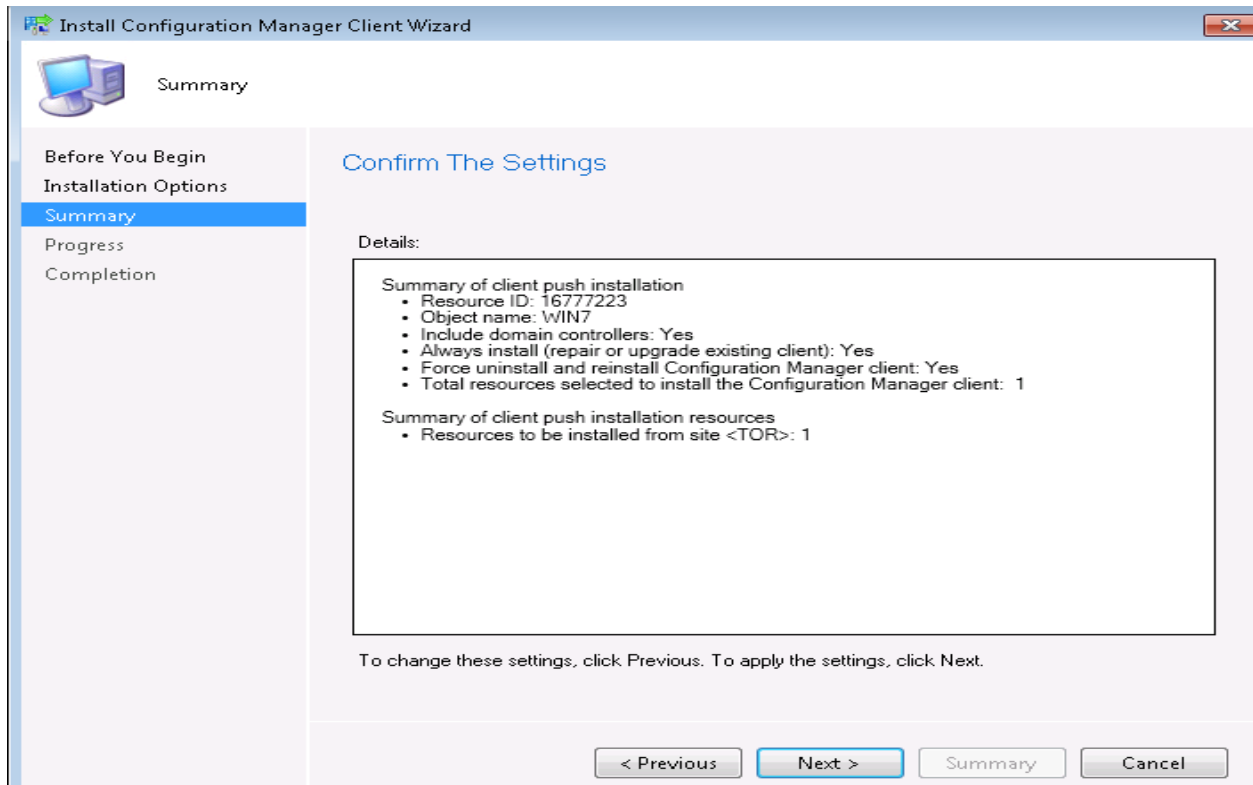
Now DSSupport group techs can install SCCM console from Software Center to their laptop and start pushing new configuration manager client to Windows 7 workstations that are scheduled for Win 10 migration.

Here is screen shot of the console for DSSupport Group user **EXADMIN**. As you can see the user has limited access within the console.





The site we should select PR1. Above is just an example from my lab.



When the new configuration manager client is installed the software center will be new version.

I just want to reiterate DSSSupport group should be part of Local Administrators group in order to install client – other wise the whole purpose of creating the group within SCCM console will be of no use to anybody.

Thanks

Ram Lan

22nd Feb 2019