Add Microsoft Intune subscription in Configuration Manager

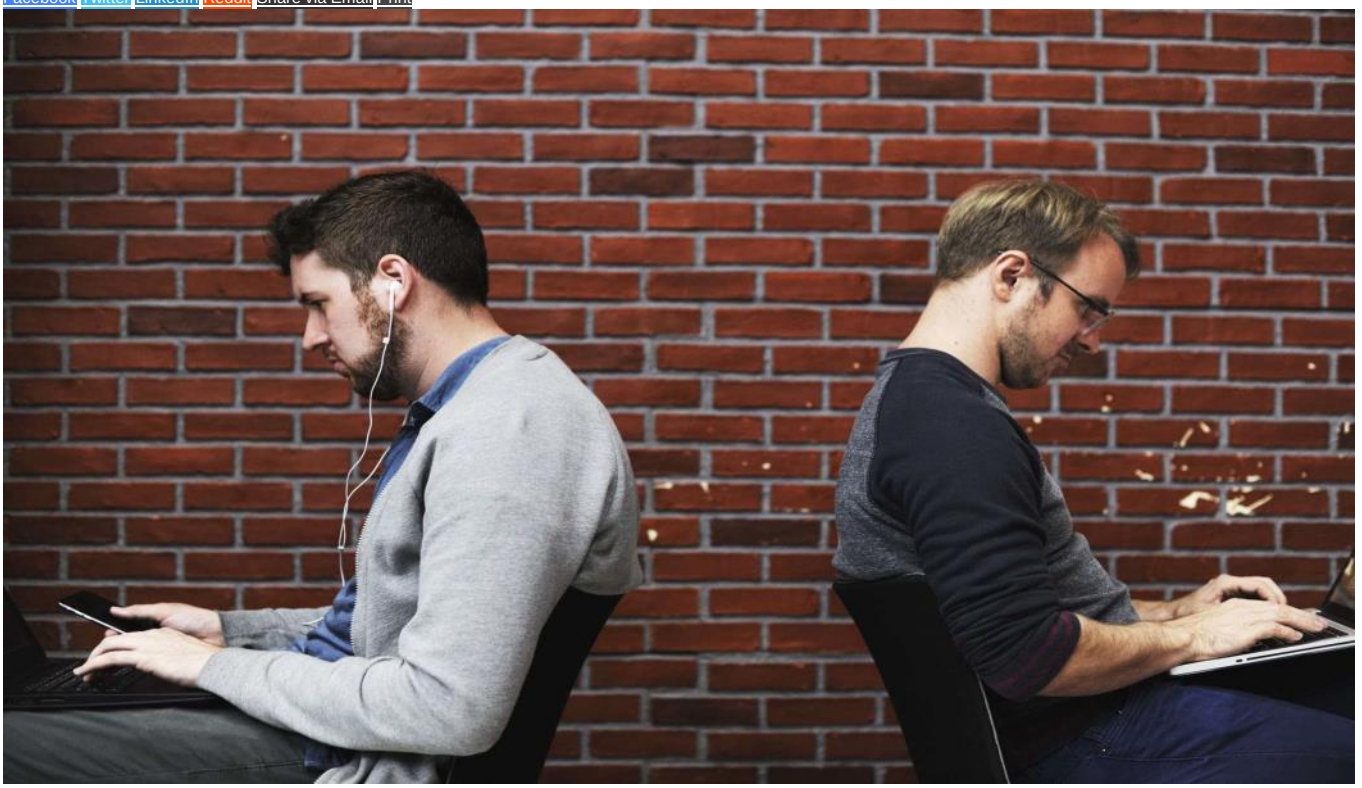
18 February, 2021 10:21 AM

www.prajwaldesai.com

Add Microsoft Intune subscription in Configuration Manager

Prajwal DesaiAugust 31, 2019
5 2 minutes read

Share
Facebook Twitter LinkedIn Reddit Share via Email Print



This post shows the steps to add Microsoft Intune subscription in Configuration Manager. You can also call it as integrating Intune and Configuration Manager. When you configure Intune subscription in Configuration Manager, it lets you manage devices over the internet.

Most of all you can configure only one Intune subscription at a time in hybrid mobile device management. However what if you need to switch to a different Intune subscription ?. The answer is simple, you must delete both Microsoft Intune Subscription and the Service connection point from the SCCM console. You can then add a new subscription.

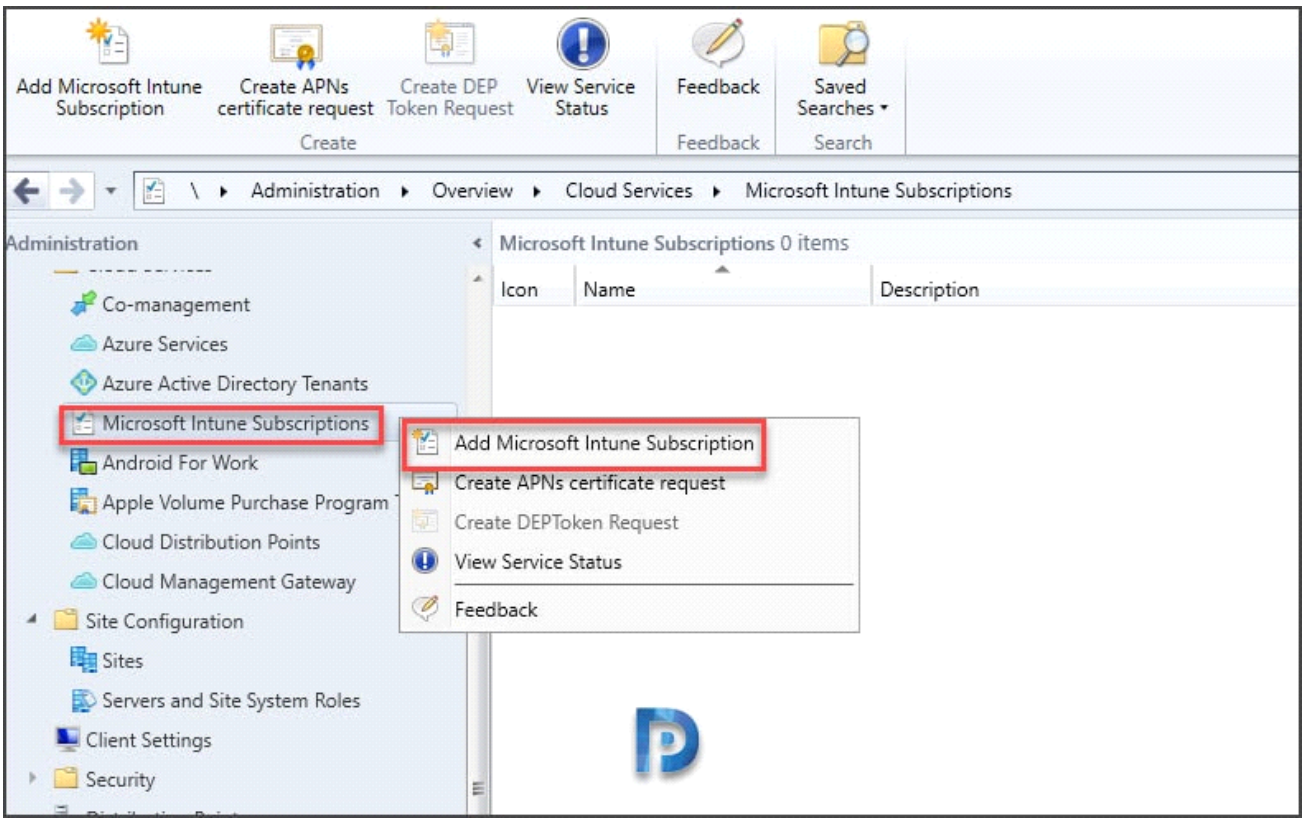
Before you proceed you should have Intune subscription details with you. You could sign

up for a Intune trial or paid subscription. Post then you can add the subscription to Configuration Manager.

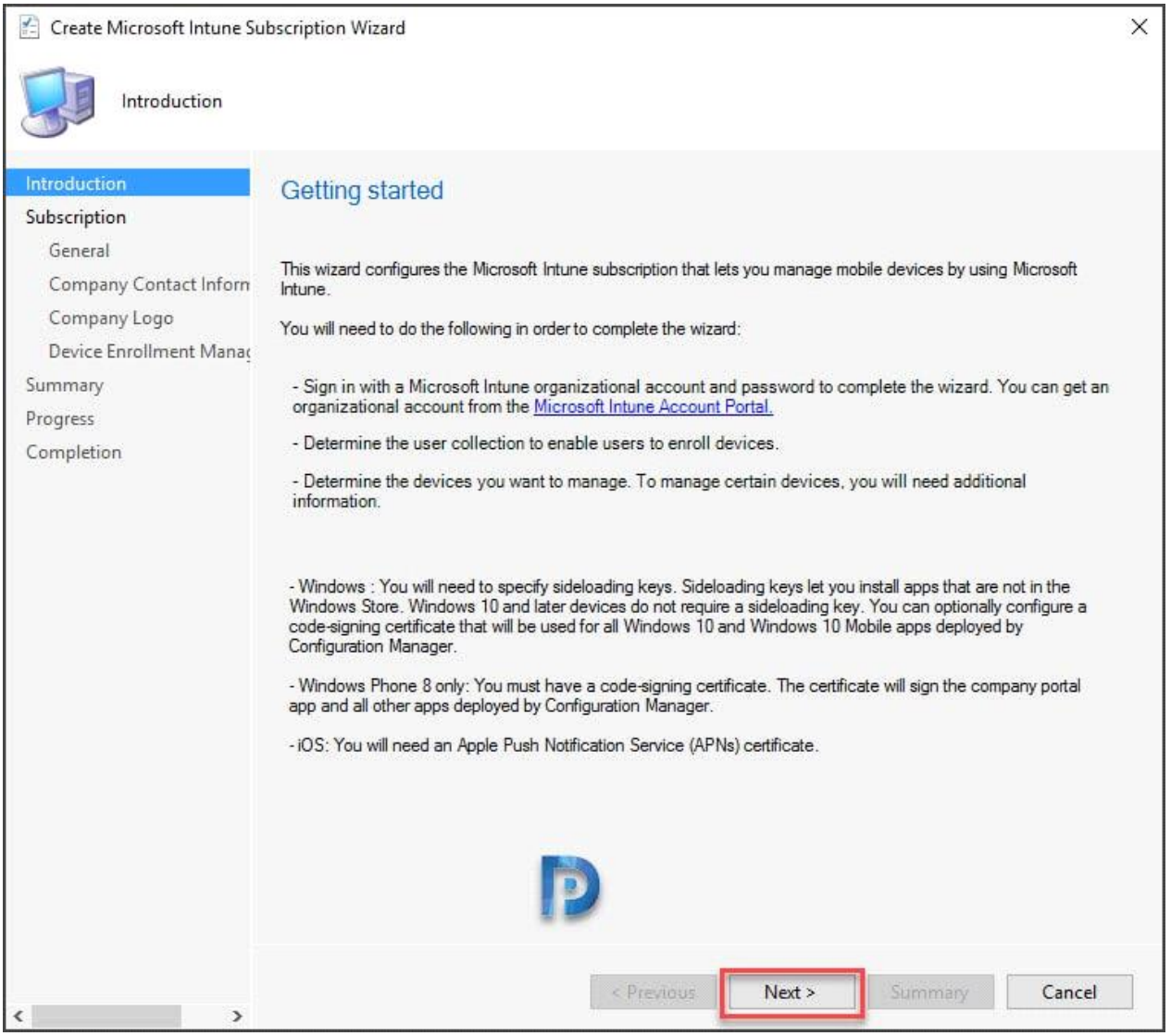
Add Microsoft Intune subscription in Configuration Manager

To add Microsoft Intune subscription in configuration manager, follow these steps.

Launch Configuration Manager console. Navigate to Administration > Overview > Cloud Services. Right click Microsoft Intune Subscriptions and click Add Microsoft Intune Subscription.

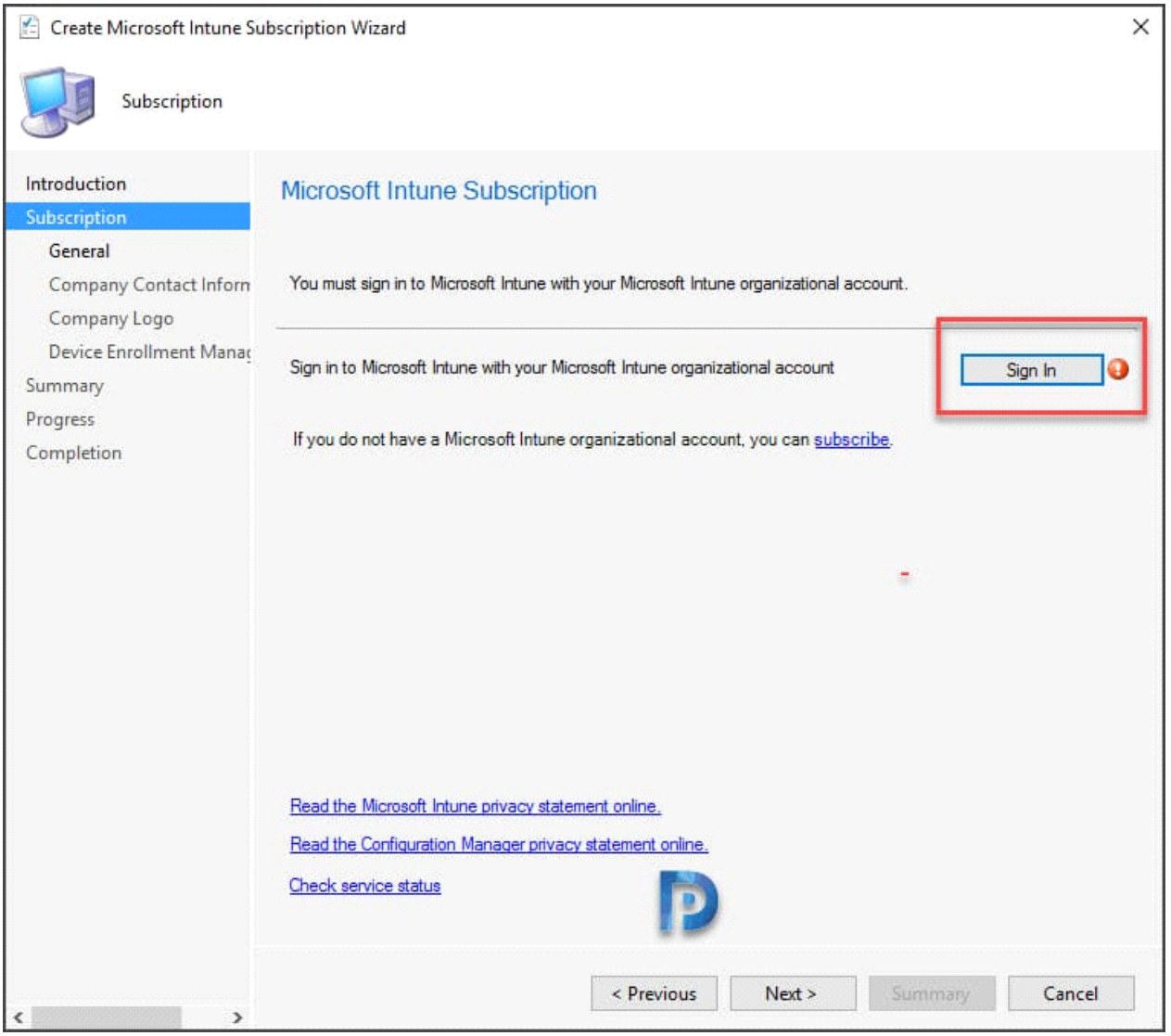


On Create Microsoft Intune Subscription wizard Intro page, click Next.

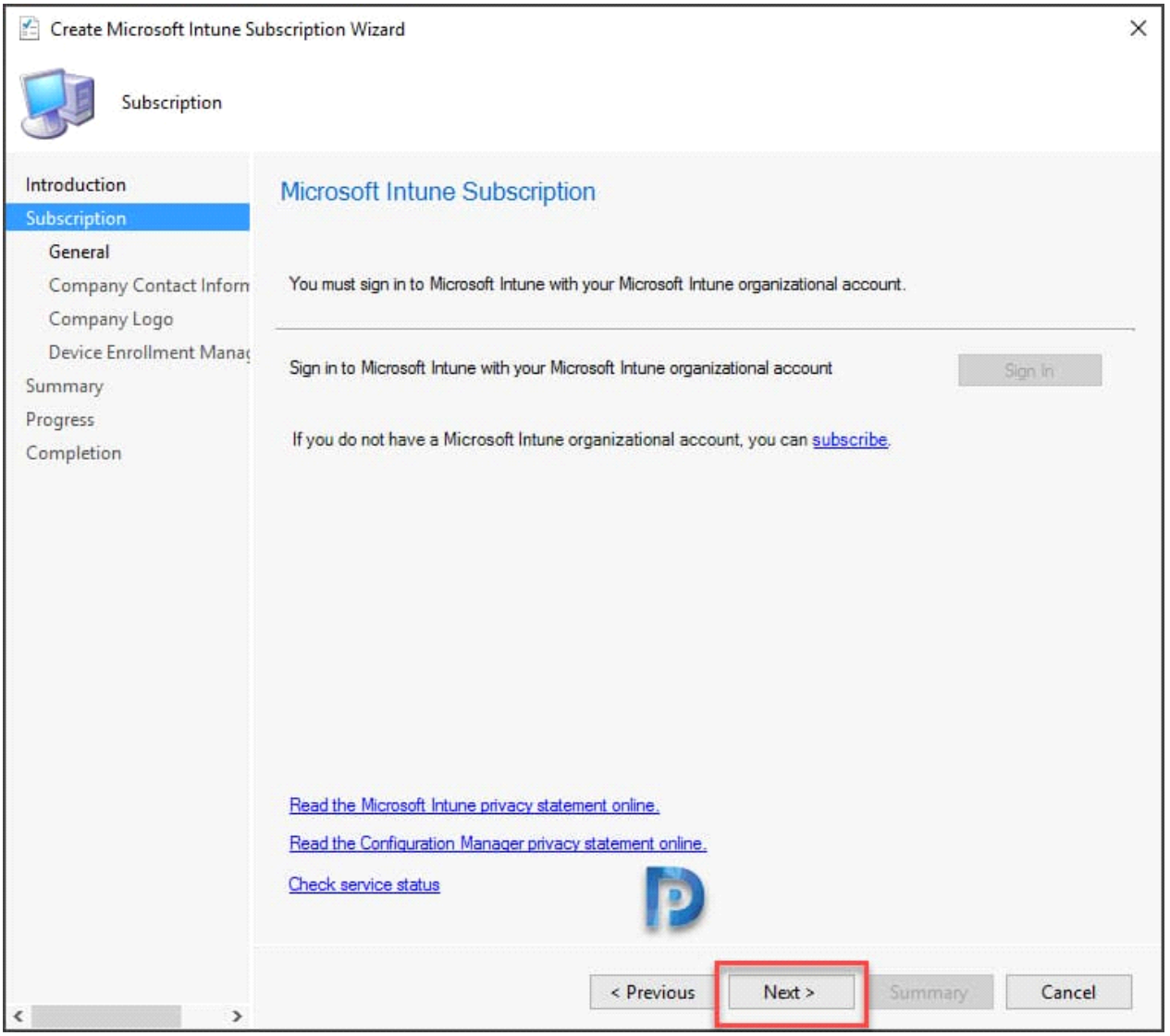


In this step click Sign In button. You will see a box where you must sign in to Microsoft

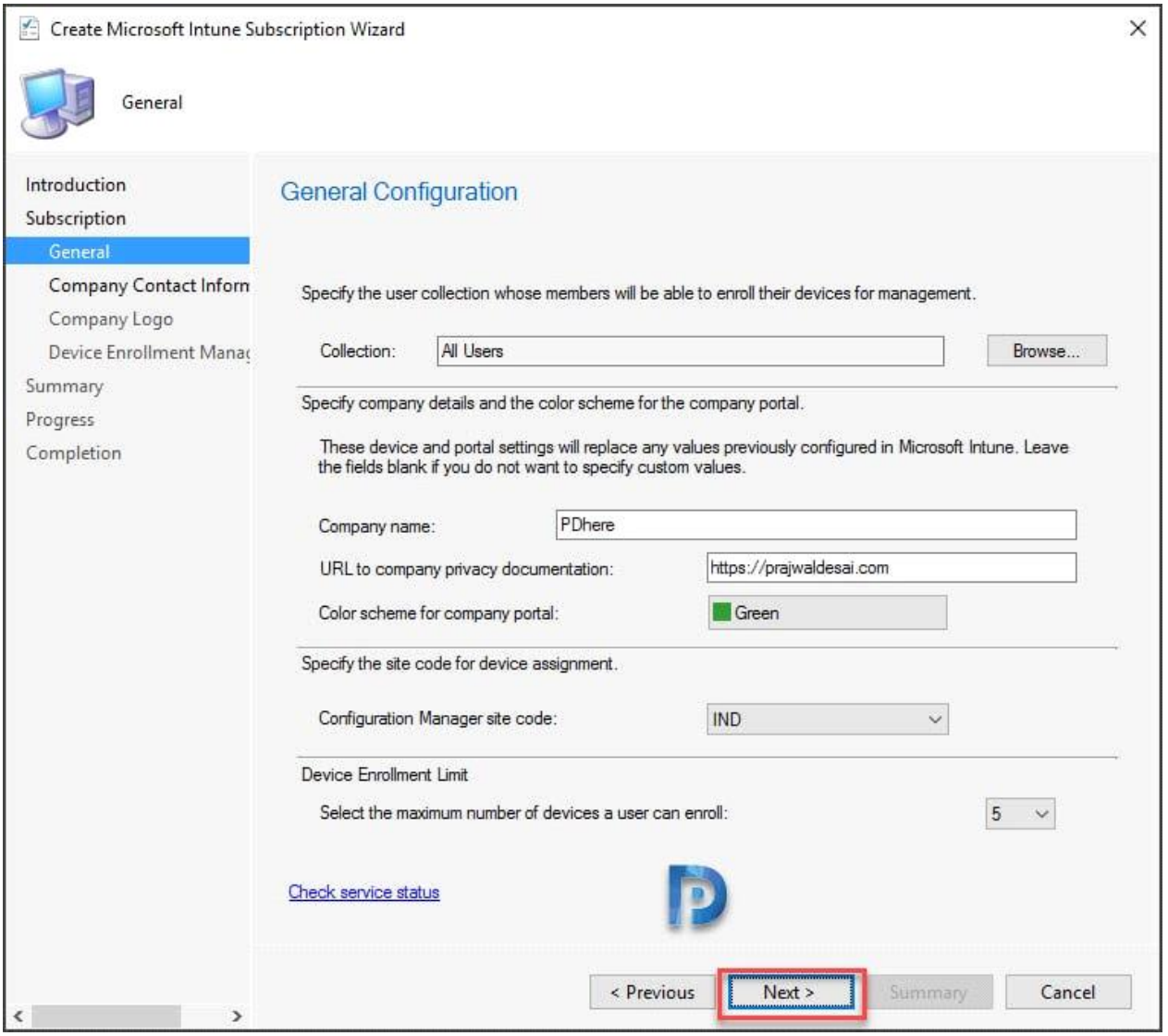
Intune with your Intune account. Click Next.



After you sign in, click Next.

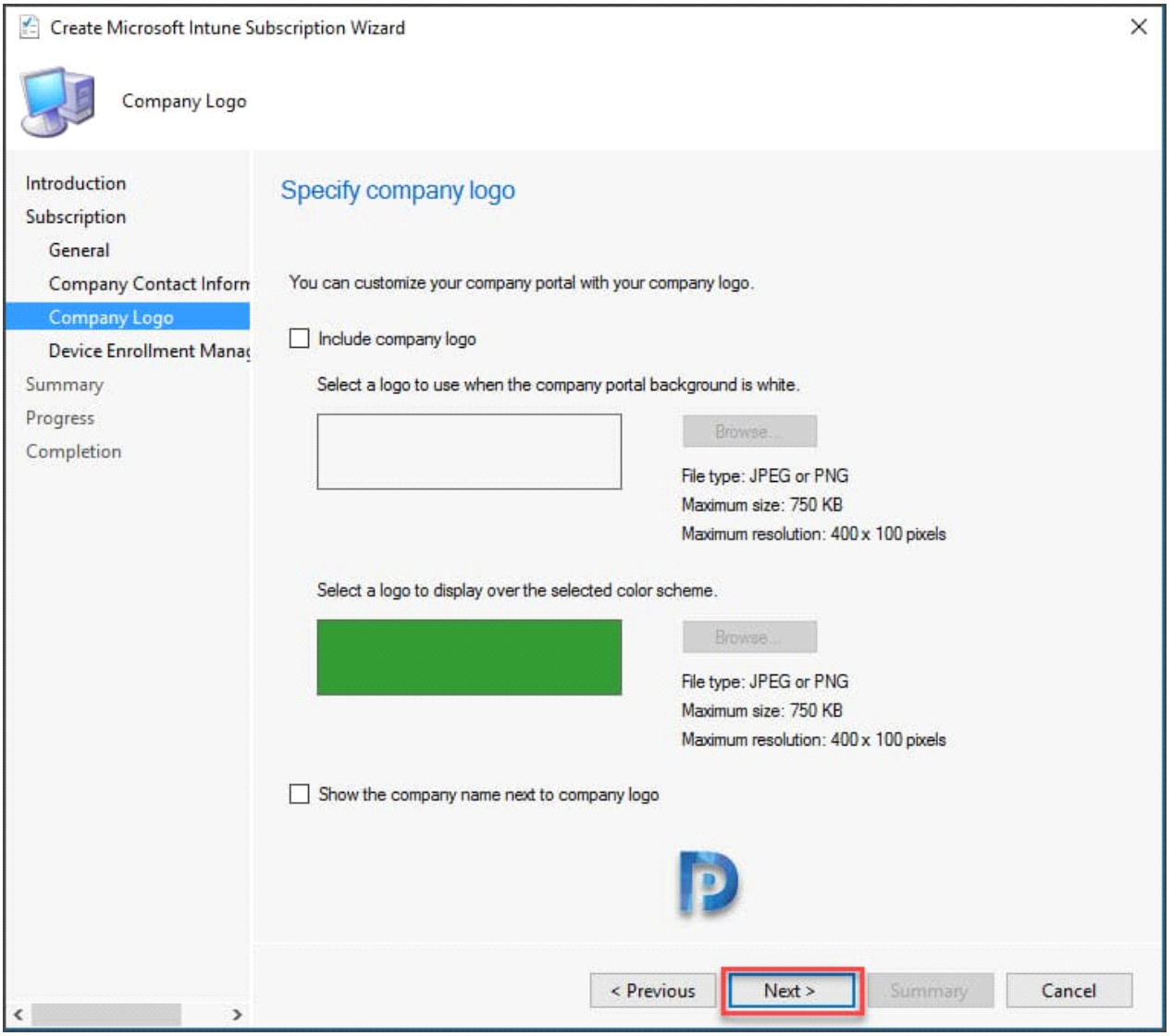


Click Browse and select the user collection. Users part of this collection can enroll their devices for management. Ideally you must specify a user collection and allow only users whom you want to enroll their devices. Since I am setting up this in lab setup, I have chosen All Users collection. Specify company name, company privacy doc URL, configuration manager site code. Specify Device enrollment limit and click Next.



This step is more of branding your company portal. You can specify your company logo and color scheme here. I will leave this to default because you can configure this later.

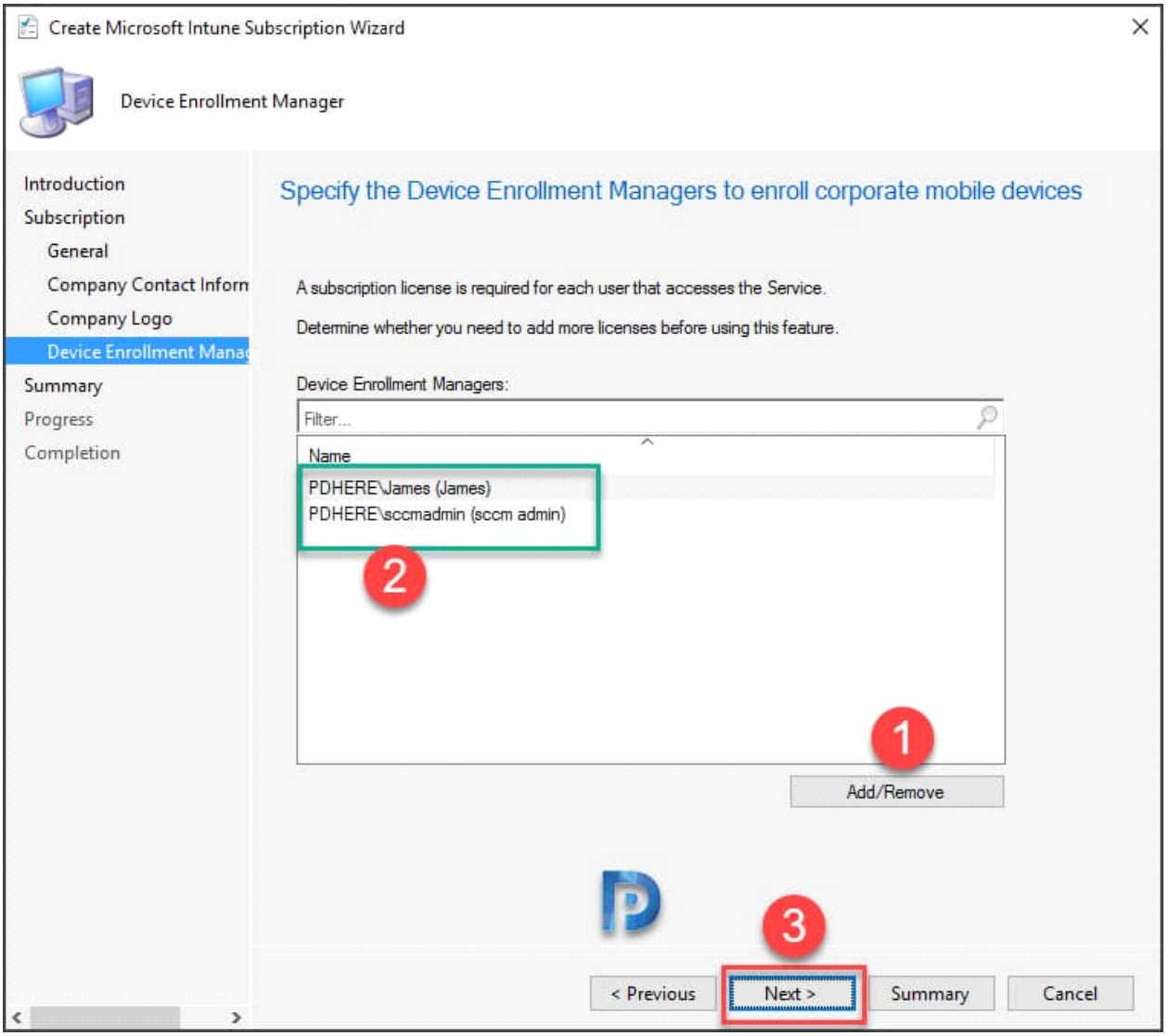
Click Next.



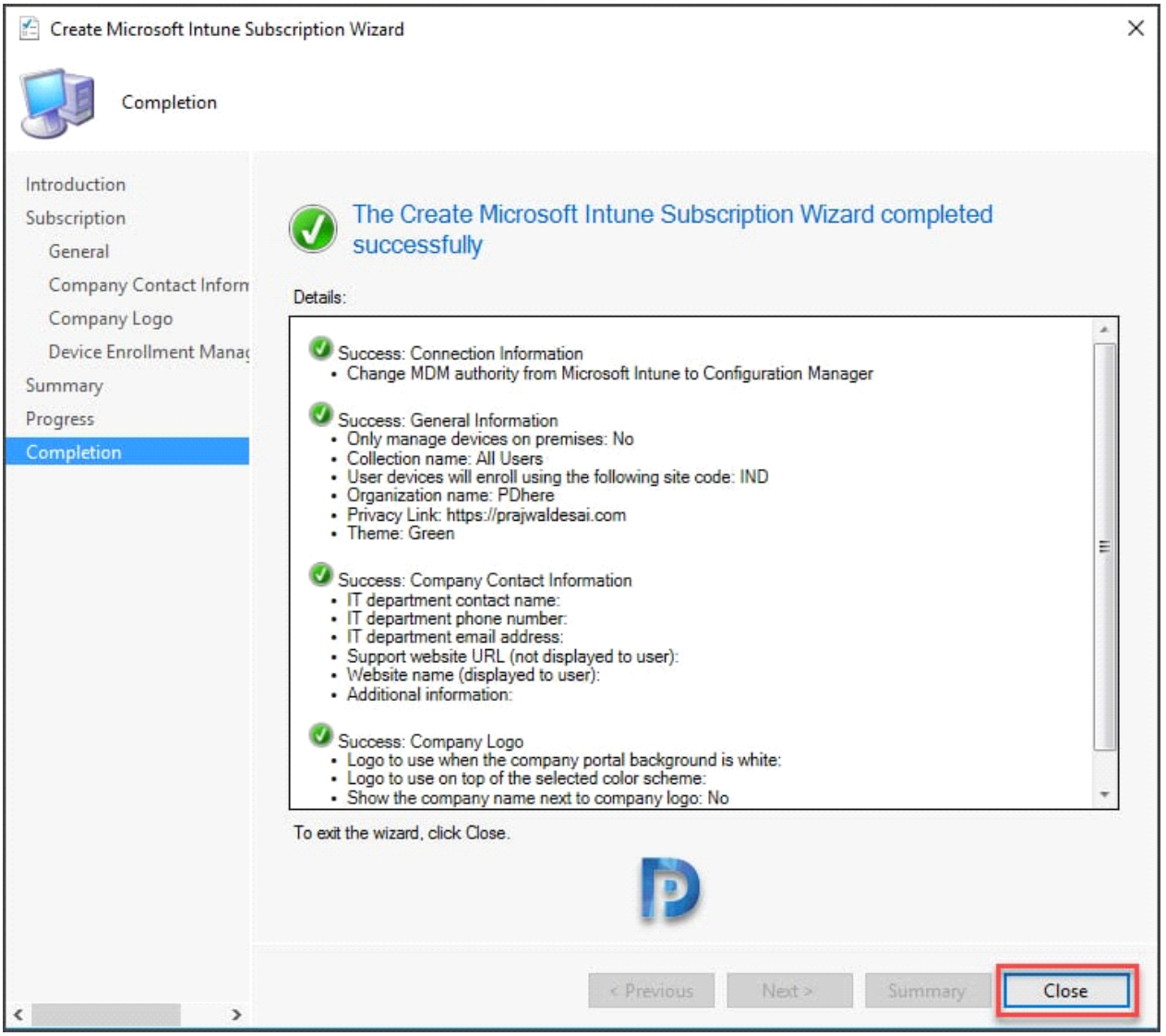
What is Device Enrollment Manager account ?

Device Enrollment Manager (DEM) account is a dedicated user account to enroll devices. Because in large organizations managing mobile devices using just one admin account becomes difficult. Therefore DEM accounts allows you to enroll devices in Intune. More info about adding Intune DEM is documented here

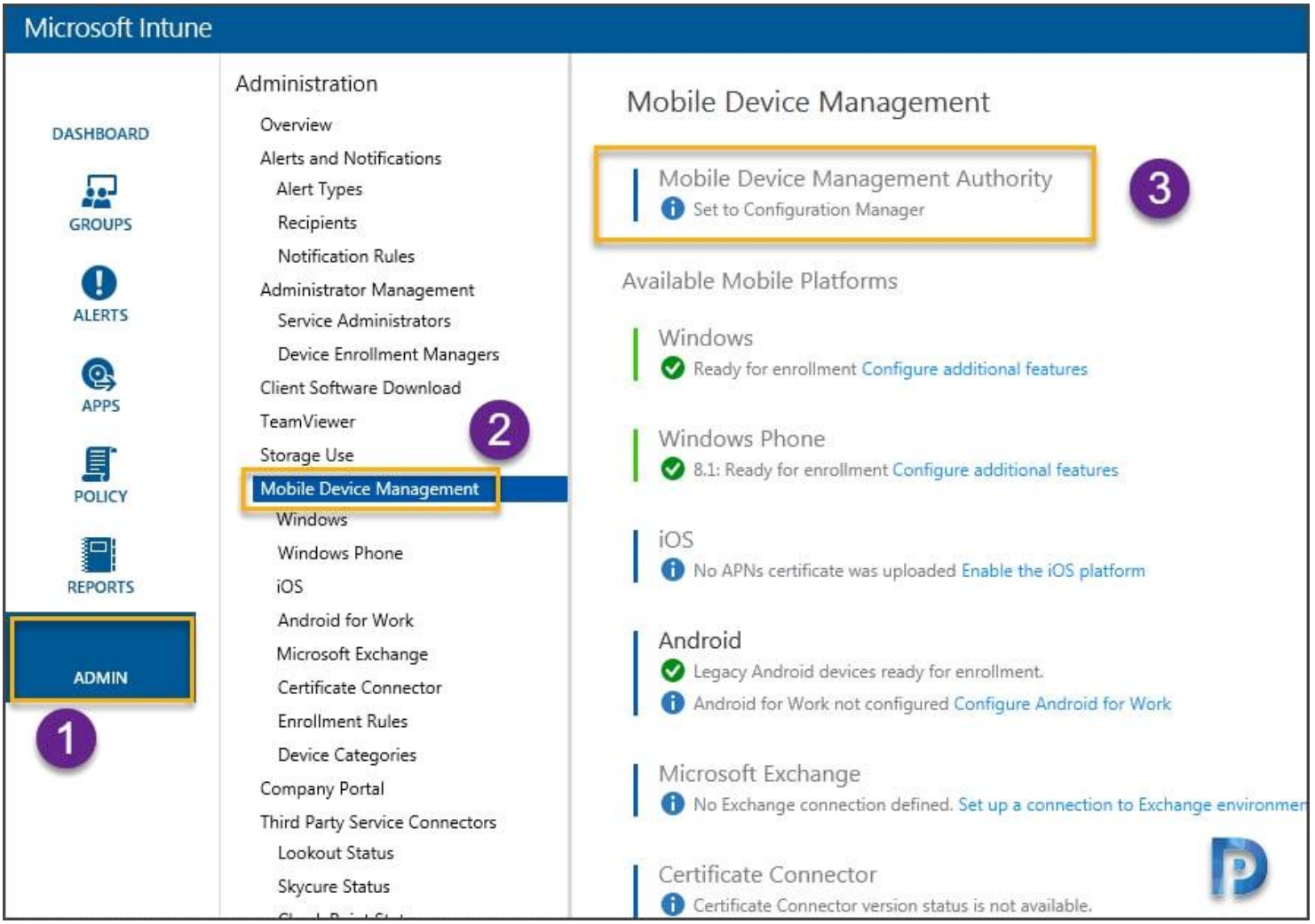
To add a device enrollment manager, click on Add/Remove button and choose the DEM accounts and click Next.



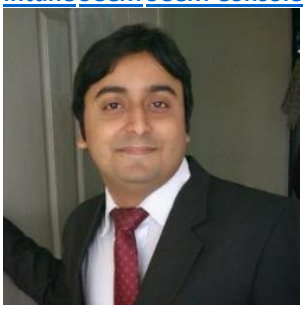
Click Next on Summary and Progress page. Finally on Completion page click Close.



Login to Microsoft Intune portal and click Admin. Under Administration click Mobile Device Management. You should see Mobile Device Management Authority set to Configuration Manager.



Intune SCCM SCCM Console



Prajwal Desai

Hi, I am Prajwal Desai. For last few years I have been working on multiple technologies such as SCCM / Configuration Manager, Intune, Azure, Security etc. I created this site so that I can share valuable information with everyone.

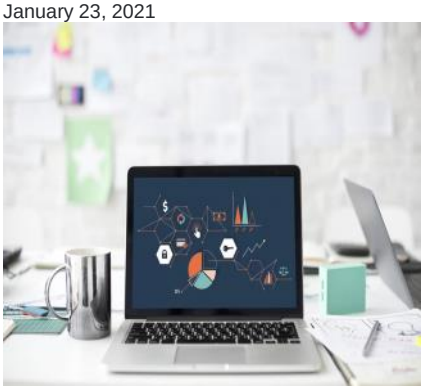
RELATED ARTICLES

[Early wave update for SCCM 1606 KB3180992]

August 9, 2016

[Step-by-Step Easy SCCM 2002 Upgrade Guide]

January 23, 2021



[SCCM SCUP – Manage SCUP software update catalogs]

April 12, 2018

5 Comments

David says:

April 1, 2020 at 5:42 pm

Getting error: “Unable to get MDM Authority.” when trying to sign in…

Reply

Michael Raae says:

January 28, 2020 at 6:36 pm

For some reason, the Microsoft Intune Subscribtion is missing under Cloud Services, i’m on current branch 1910, and havin same issue in my test LAB where im running Technical Preview 1911, and it is stuck on downloading TP 2001.

Any thoughts on how to get Intune Subscription back in my Clous Services,

pretty sure i have seen it there before??
Reply

Joaquín Luengas says:
October 30, 2019 at 3:35 am
Microsoft has removed Hybrid MDM.
Reply

MikeF says:
September 15, 2019 at 9:42 pm
Microsoft just dropped support for hybrid co-management on 9/1/2019.
Reply

stiber says:
December 3, 2018 at 2:19 pm
Hello.
My Intune MDM are Connected to a config manager site, but the config manager site (lab) is gone (SAN failure no backup). How can I change Device enrollment back to Intune ?

From <https://www.prajwaldesai.com/add-microsoft-intune-subscription-in-configuration-manager/>

Enable Tenant Attach in ConfigMgr | SCCM

19 February, 2021 8:32 AM

Easy Guide to Enable Tenant Attach in ConfigMgr | SCCM

Prajwal DesaiJanuary 12, 2021
2 4 minutes read

Share
Facebook Twitter LinkedIn Reddit Share via Email Print

This post is a step by step guide to enable tenant attach in ConfigMgr or SCCM. Using the Co-management configuration wizard, we will add Tenant Attach to our Configuration Manager instance.

Starting in Configuration Manager version 2002, you can upload your Configuration Manager devices to the cloud service and take actions from the Devices blade in the admin center.

The idea of Configuration Manager and Intune into a single console called Microsoft Endpoint Manager admin center is simply awesome. Lets connect SCCM site to Microsoft Intune.

Contents

- ConfigMgr Tenant Attach Log Files

What is SCCM Tenant Attach ?

Probably you have heard about the Co-management if you have been working on Configuration Manager. However let us understand what is ConfigMgr Tenant Attach and is it the same as Co-management?

Co-management is not new and has been around for quite a while now. A co-managed device is basically managed by both ConfigMgr and Intune at the same time.

Tenant Attach means the device can be either managed by ConfigMgr or Intune. The reason why we use the term “Tenant Attach” is because it simply a way to attach your ConfigMgr hierarchy to your tenant.

And when you do that you can perform several tasks such as discover cloud users and groups, synchronize Azure AD groups from a device collection and much more.

SCCM Tenant Attach Prerequisites

Before you perform Tenant Attach to the ConfigMgr instance, ensure you know or read the prerequisites.

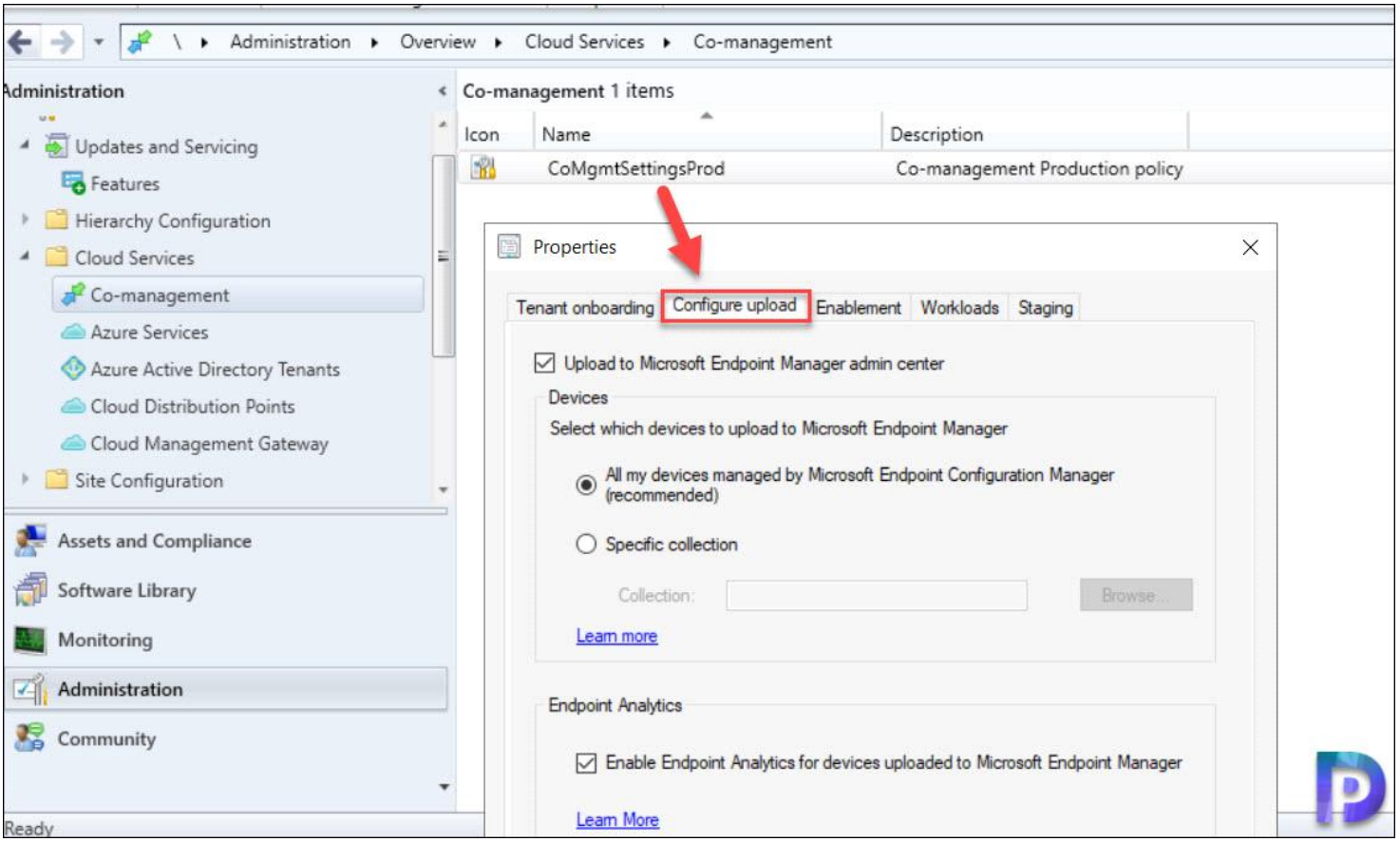
- An account that is a Global Administrator for signing in when applying this change.
- You need Configuration Manager current branch version 2002 and above. Microsoft Endpoint Manager tenant attach was one of the exciting feature of SCCM 2002.
- An Azure public cloud environment.
- The user accounts triggering device actions should meet the following conditions. First the users account should have been discovered with both Azure Active Directory user discovery and Active Directory user discovery. In other words, the user account needs to be a synced user object in Azure AD. Second, the Initiate Configuration Manager action permission under Remote tasks in the Microsoft Endpoint Manager admin center.

Enable device upload when co-management is already enabled

If you have already enabled the co-management in your setup, you’ll use the co-management properties to enable device upload. If the co-management isn’t already enabled, then jump to next step. You use the Configure co-management wizard to enable device upload instead.

Assuming that co-management is already enabled, simply edit the co-management properties to enable device upload using the steps below:

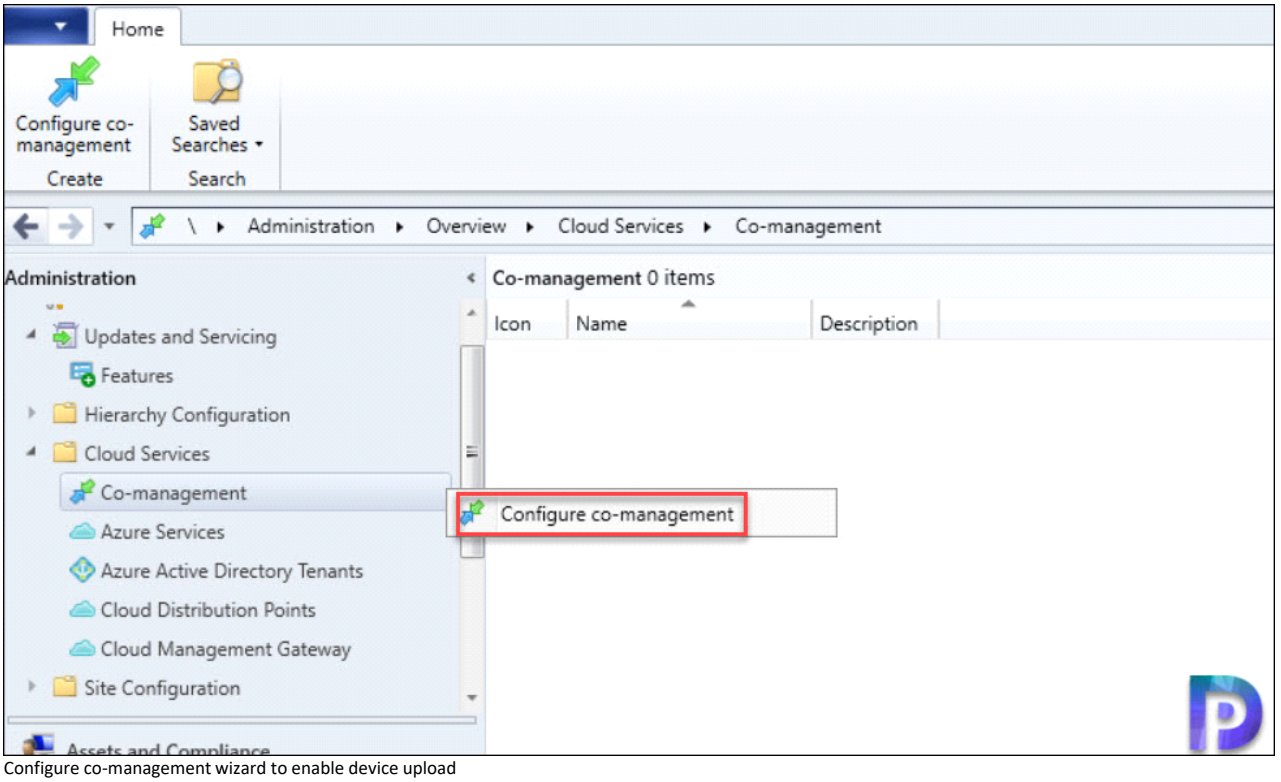
- In the Configuration Manager admin console, go to Administration > Overview > Cloud Services > Co-management.
- Right click CoMgmtSettingsProd and select Properties.
- In the Configure upload tab, select Upload to Microsoft Endpoint Manager admin center. Select Apply. The default setting for device upload is All my devices managed by Microsoft Endpoint Configuration Manager. If required, you can limit upload to a single device collection.
- Click Enable Endpoint analytics for devices uploaded to Microsoft Endpoint Manager if you want to get insights to optimize the end-user experience in Endpoint Analytics.
- Sign in with your Global Administrator account when prompted. Select Yes to Create AAD Application notification. Click OK to exit the co-management properties once you’ve done making changes.



Configure Co-Management in ConfigMgr

To configure the Co-management for the first time in the Configuration Manager setup.

- Launch the Configuration Manager console.
- Go to Administration > Overview > Cloud Services > Co-management.
- Right click Co-management and click Configure co-management.



Configure co-management wizard to enable device upload

ConfigMgr Tenant Onboarding

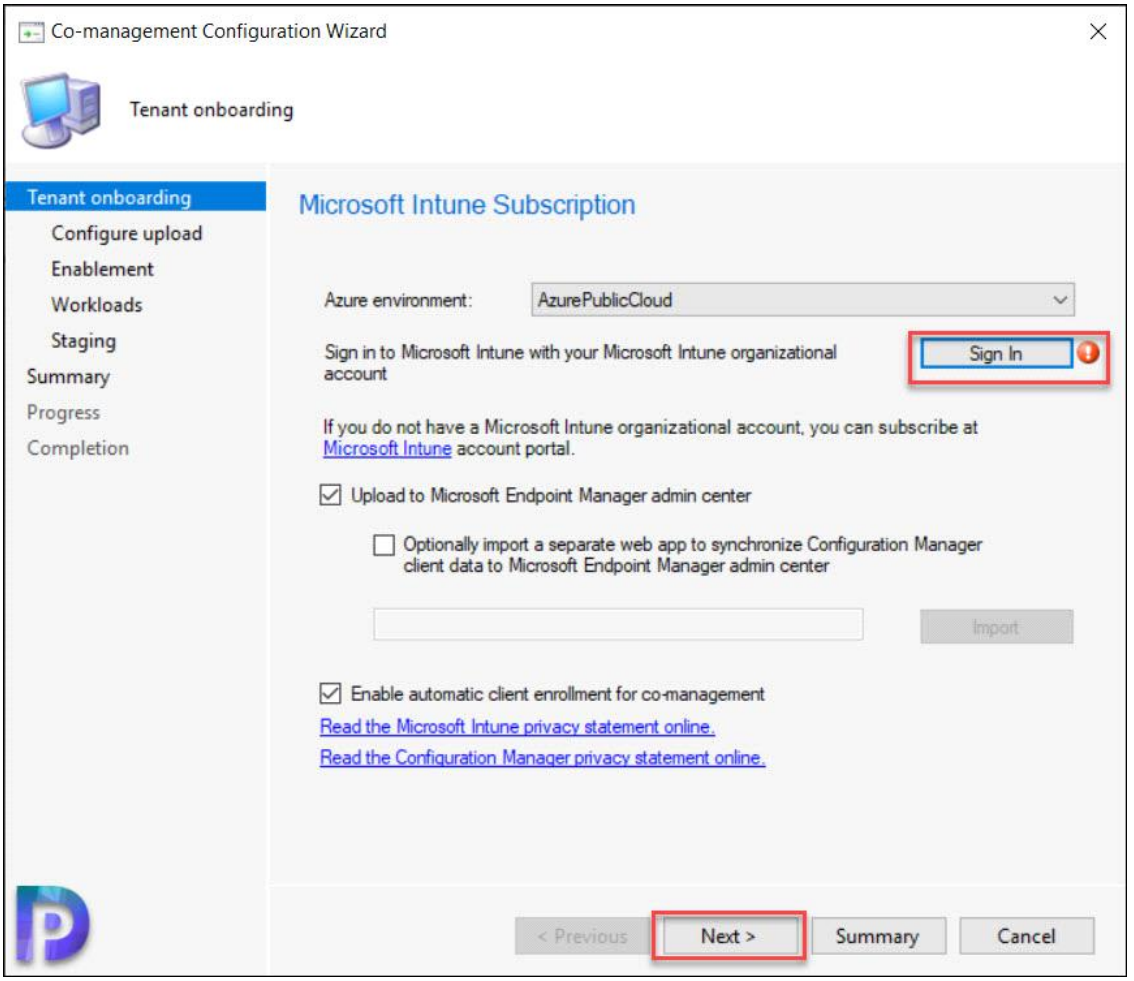
On the Tenant onboarding page, select AzurePublicCloud for your environment. Azure Government Cloud and Azure China 21Vianet aren't supported. Therefore don't select them.

Next, click Sign In. Use your Global Administrator account to sign in.

Ensure the Upload to Microsoft Endpoint Manager admin center option is selected on the Tenant onboarding page.

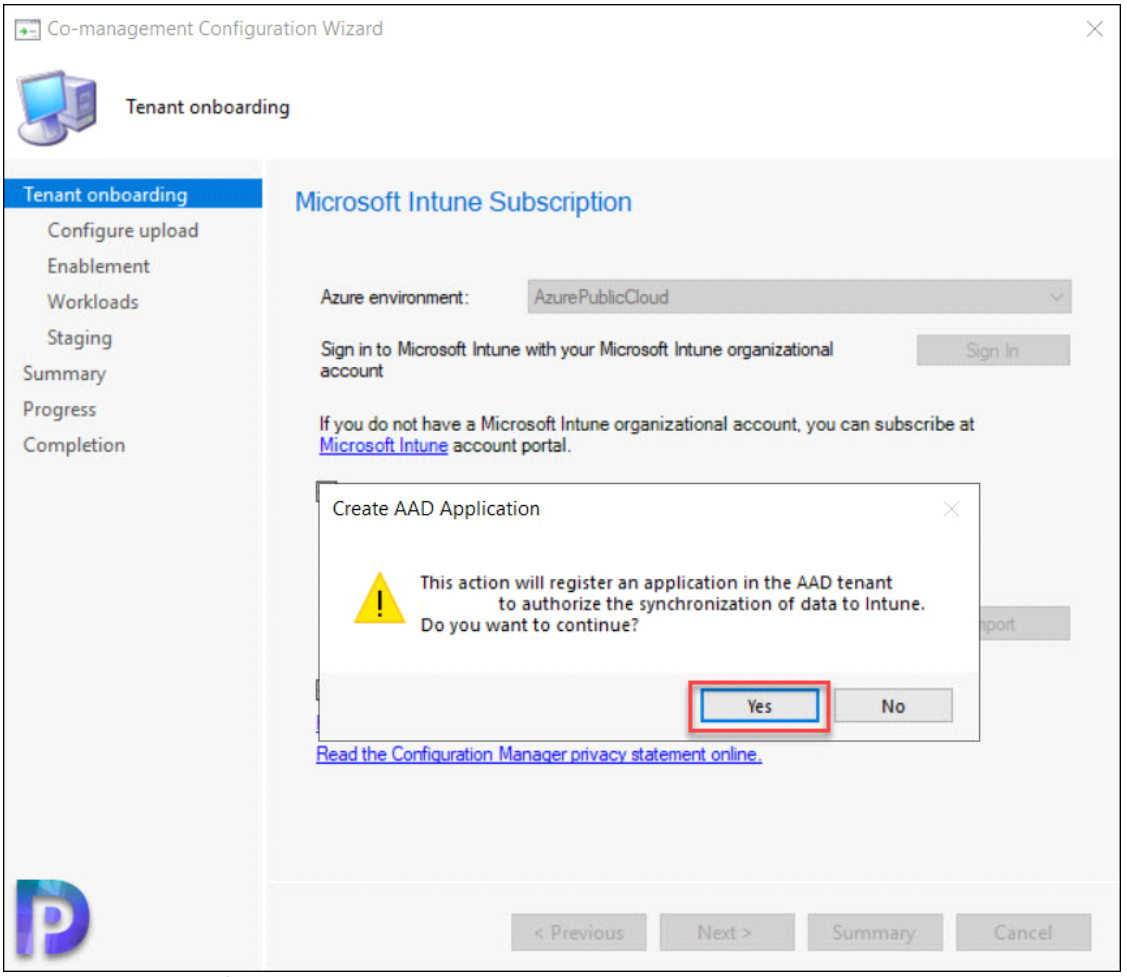
Make sure the option Enable automatic client enrollment for co-management isn't checked if you don't want to enable co-management now. However if you do want to enable co-management, select the option.

Click Next.



Tenant onboarding page

Click Yes to accept the Create AAD Application notification. This action provisions a service principal and creates an Azure AD application registration to facilitate the sync.



Enable Tenant Attach in ConfigMgr

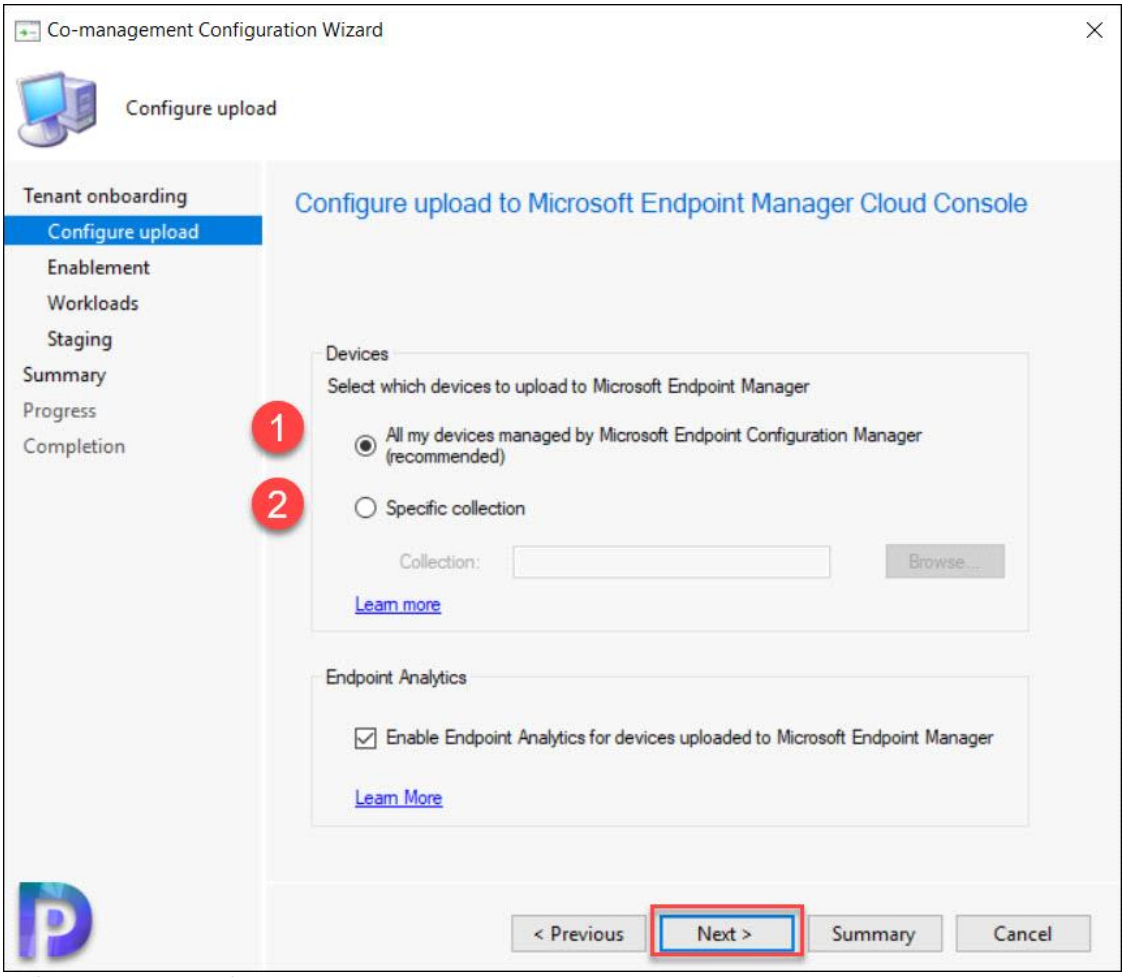
Configure Upload to Microsoft Endpoint Manager Cloud Console

On the Configure Upload page, select the devices that you want to upload to Microsoft Endpoint Manager.

- All devices managed by Microsoft Endpoint Configuration Manager – This is a recommended option.
- Specific Collection – If you don't wish to choose all devices, you can click and Browse and select a specific collection.

Endpoint Analytics – Enable Endpoint analytics for devices uploaded to Microsoft Endpoint Manager if you want to get insights to optimize the end-user experience in Endpoint Analytics.

Click Next.



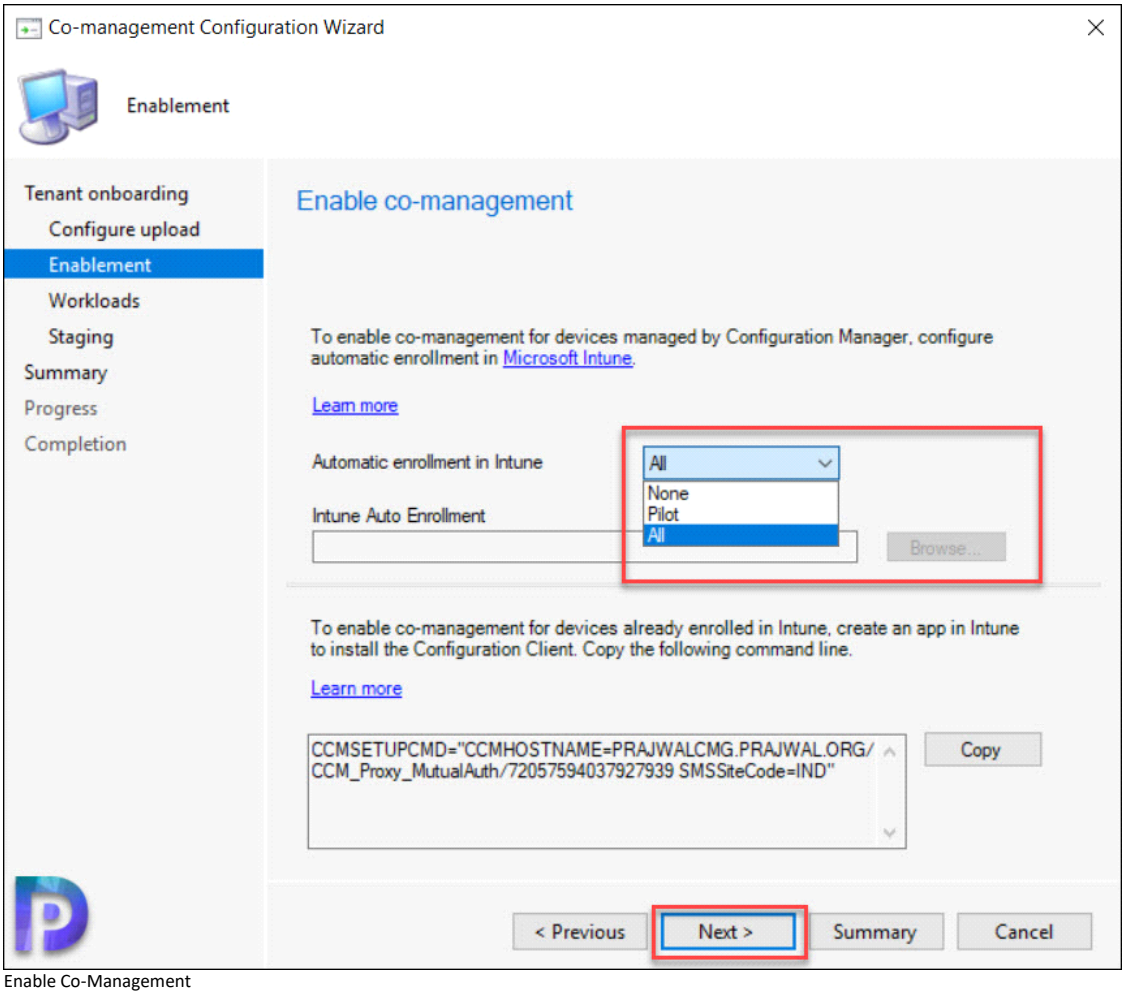
Configure Upload to Microsoft Endpoint Manager Cloud Console

Enable Co-Management in SCCM Console

To enable co-management for devices managed by Configuration Manager, you must configure the automatic enrollment.

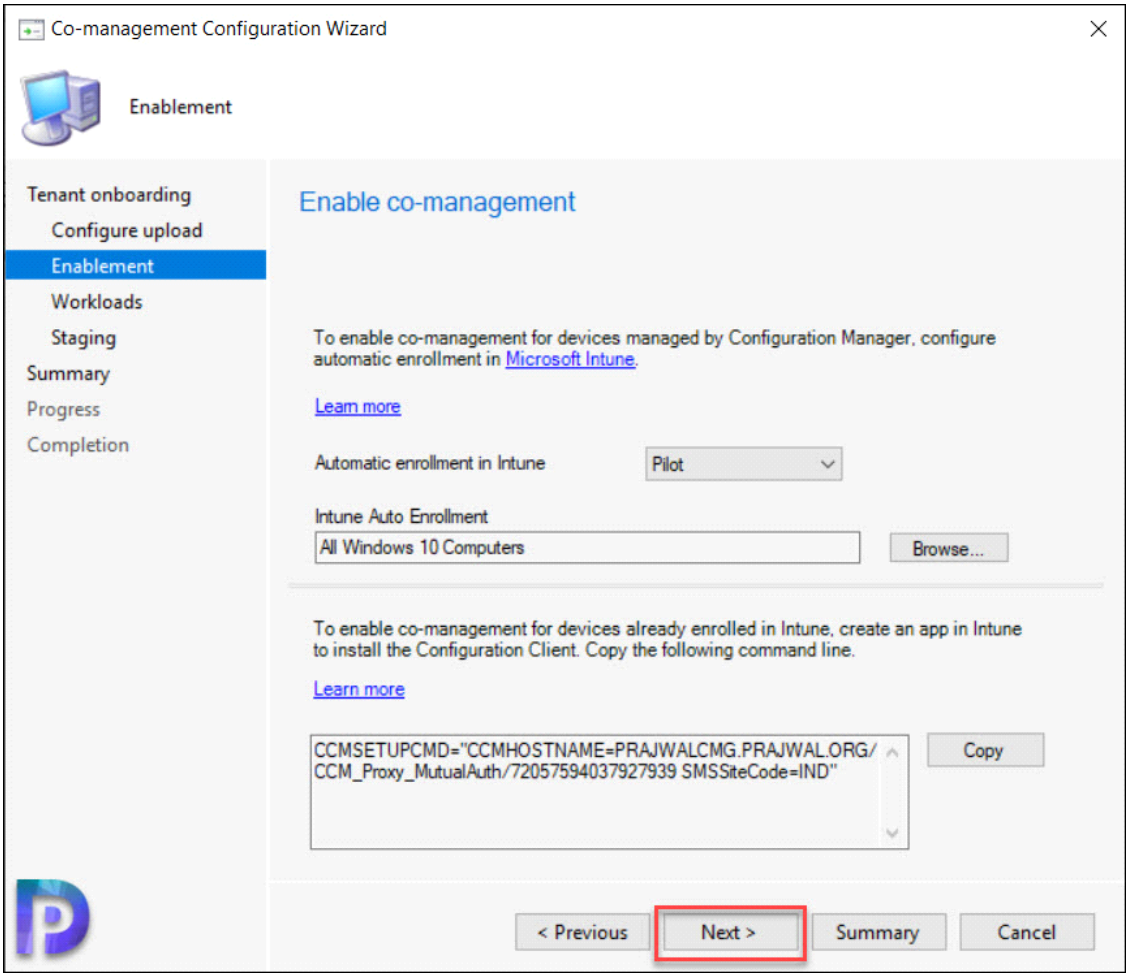
Next to Automatic enrollment in Intune, click the drop-down and select one of the following.

- None
- Pilot
- All



Enable Co-Management

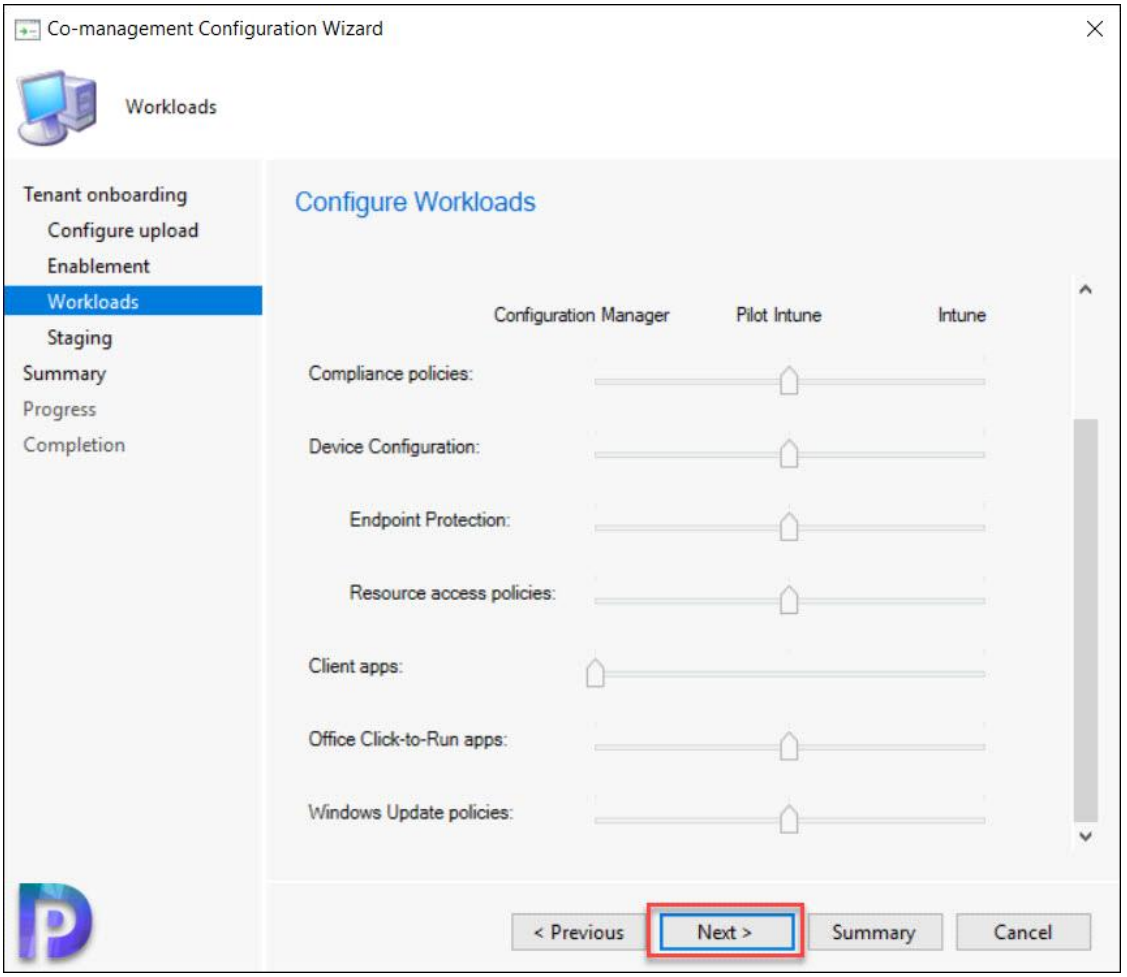
I have selected Pilot and for Intune Auto Enrollment, I have selected a Windows 10 device collection. This collection consists of only 4 devices running Windows 10. Click Next.



Configure Automatic enrollment in Intune

In this step, as an administrator you can configure specific workloads for Configuration Manager or Microsoft Intune.

Click Next.



Configure Workloads

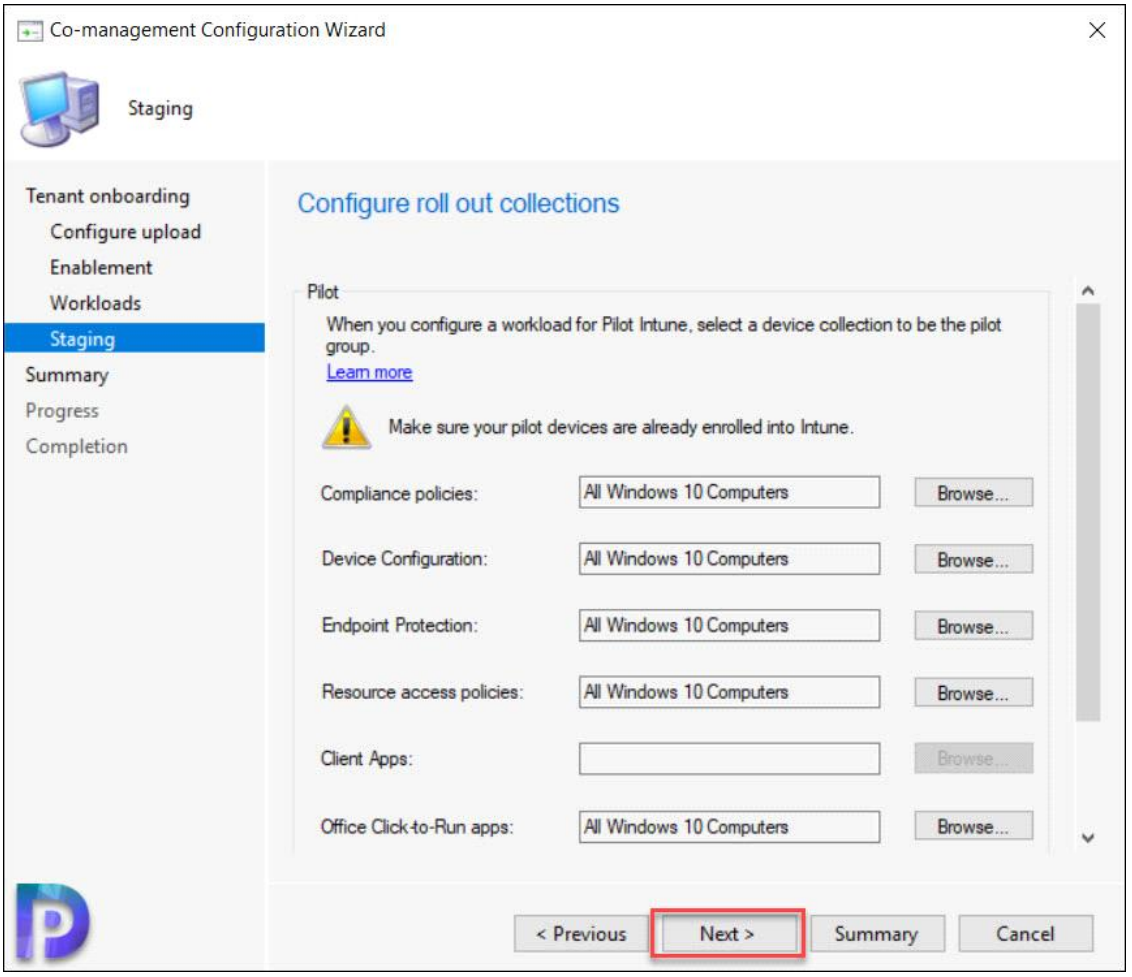
Staging – Configure Roll Out Collections

When you configure a workaround for Pilot Intune, you must select a device collection to each of the pilot group.

For each of the items listed below, click Browse and select a device collection.

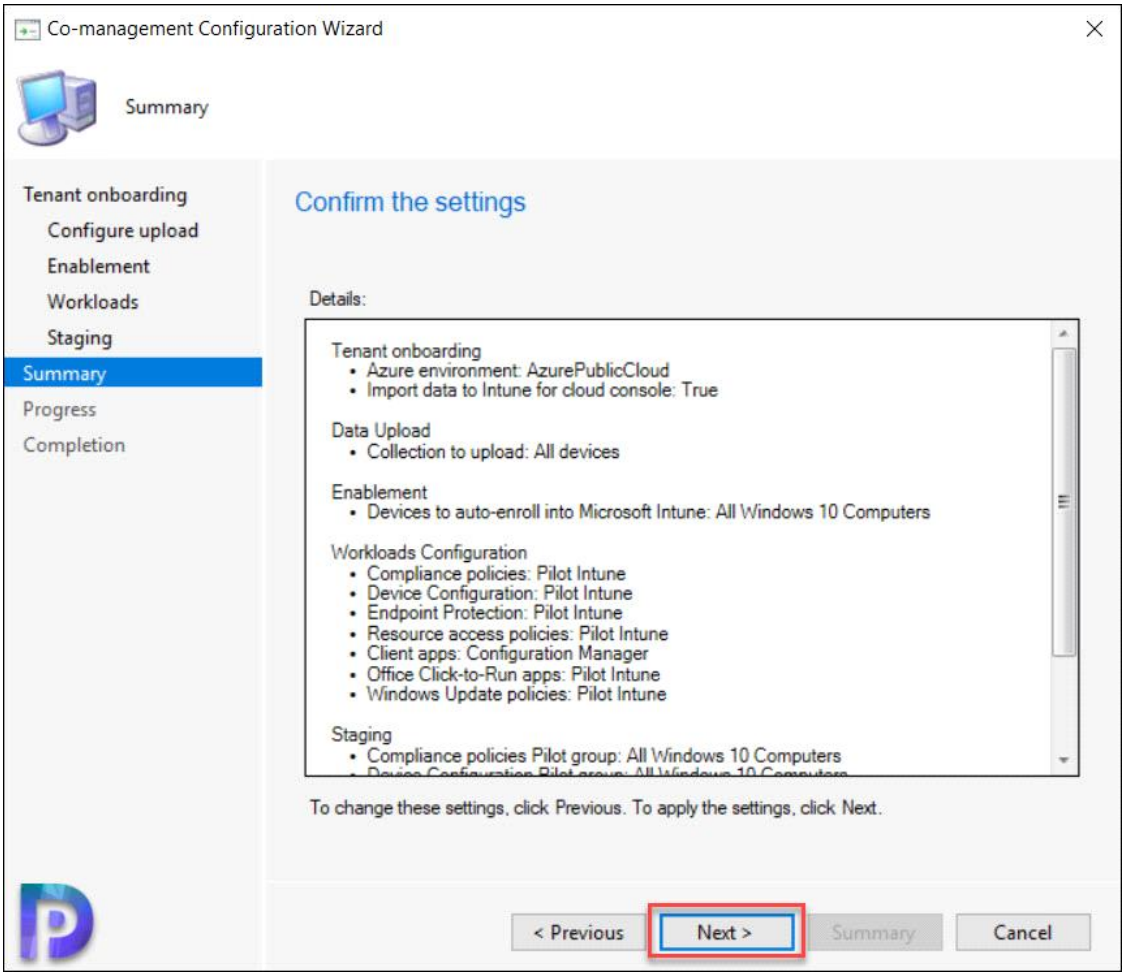
- Compliance Policies
- Device Configuration
- Endpoint Protection
- Resource access policies
- Office click-to-run apps

Finally click Next.

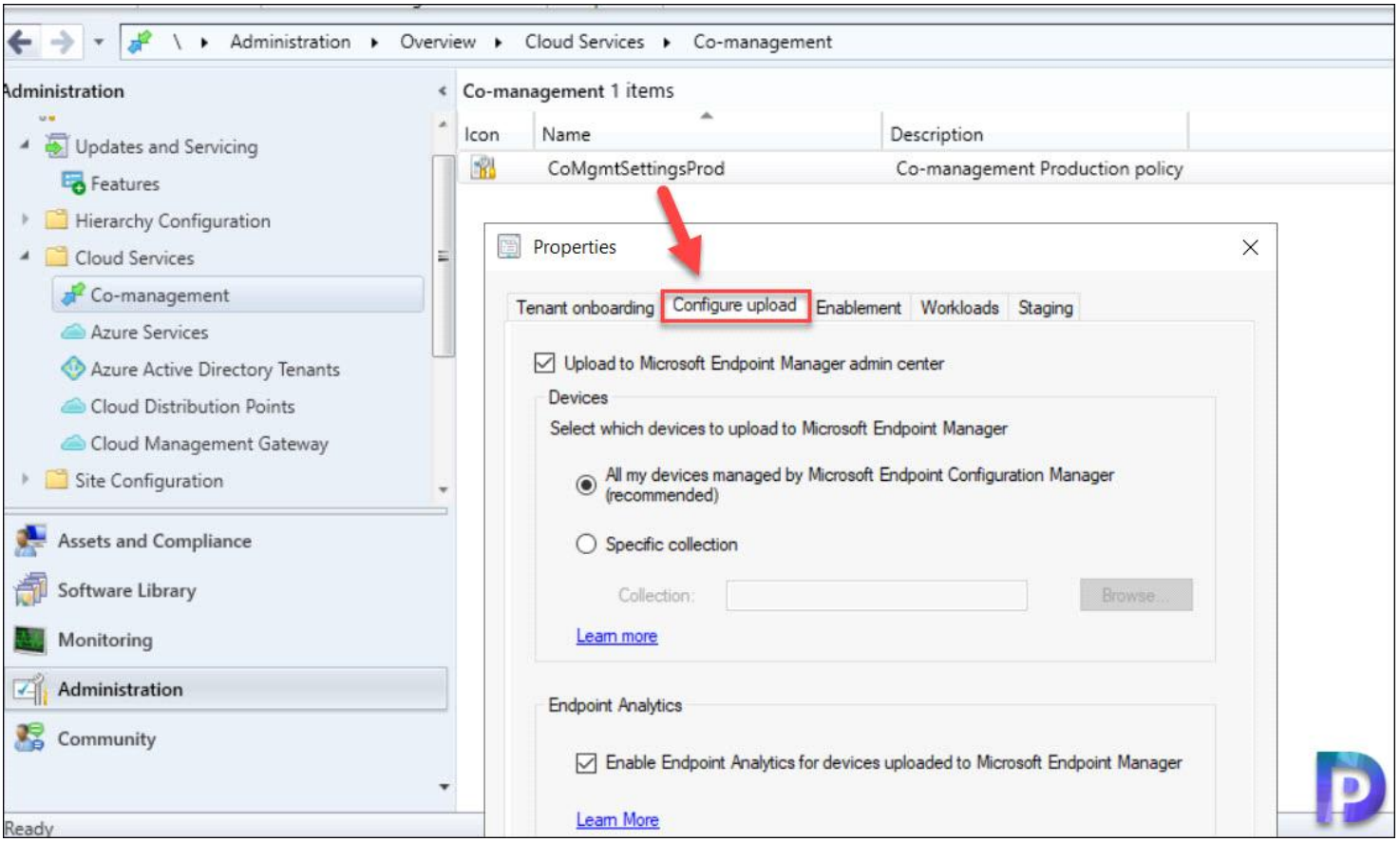


Staging – Roll out Collections

On the Summary page, click Next.

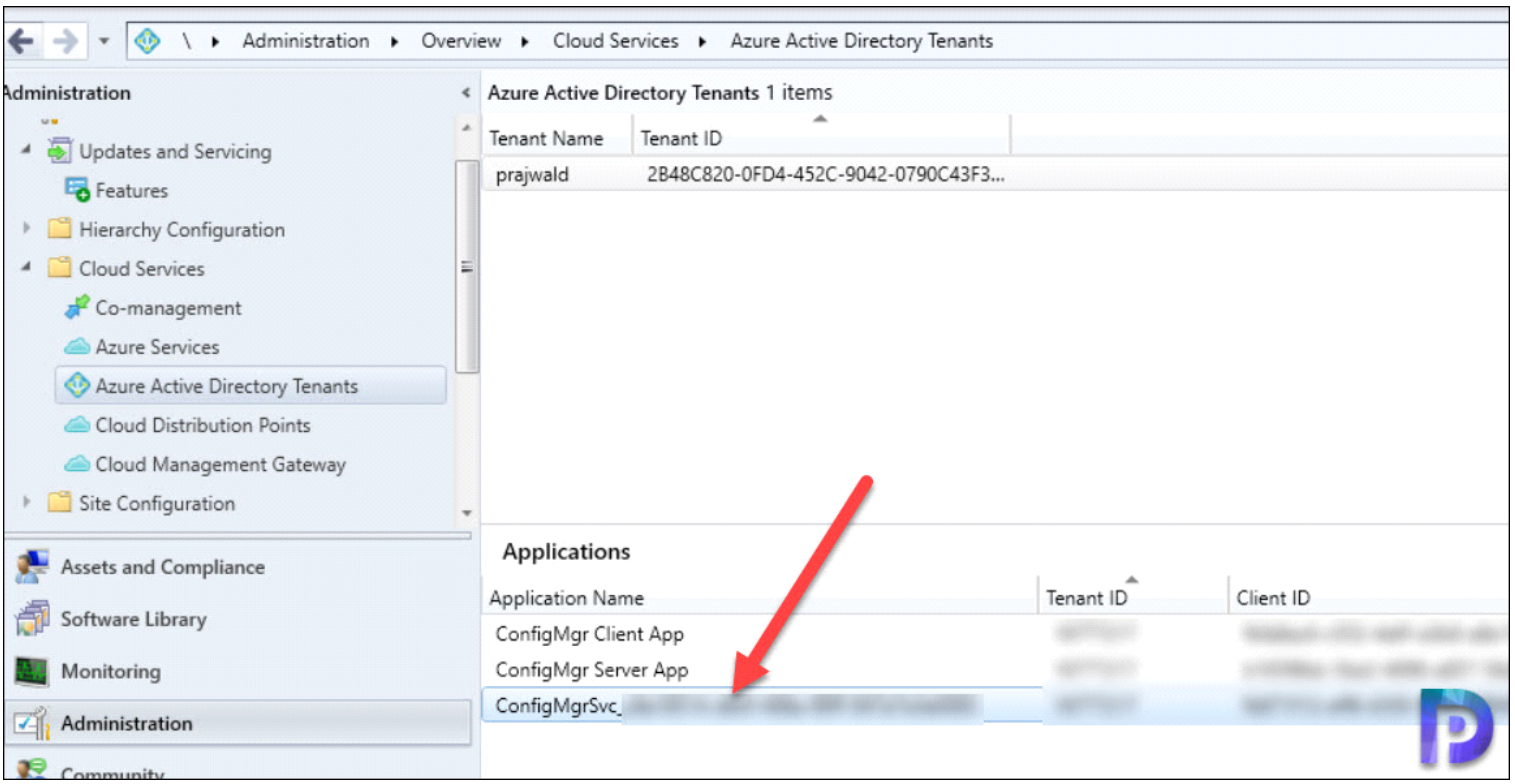


If you need to change or modify any of the co-management settings, you can edit co-management properties to enable device upload.



Enable Tenant Attach in ConfigMgr

In the Configuration Manager console, if you navigate to Cloud Services > Azure Active Directory Tenants, you should see a new application. The name begins with ConfigMgrSvc_id.



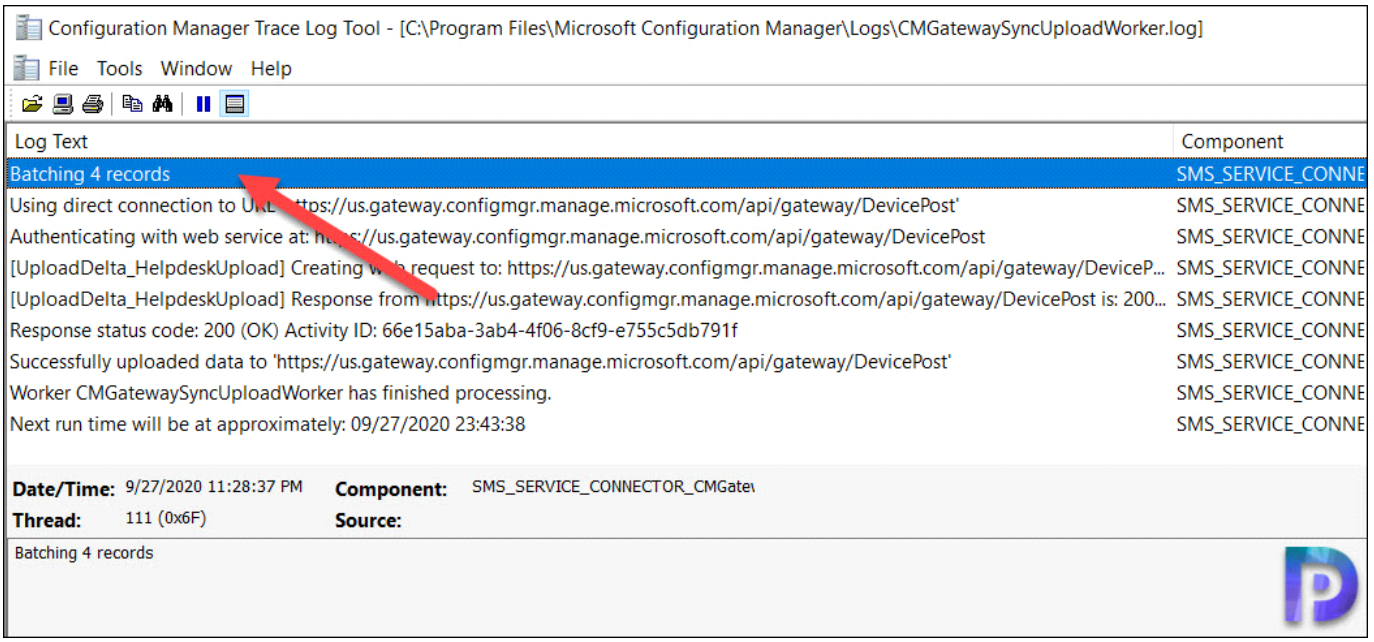
ConfigMgr Tenant Attach Log Files

If you are looking for Tenant Attach log files, then here they are. The below two

ConfigMgr logs are located on the service connection point. Use these log files for troubleshooting tenant attach and device actions.

- CMGatewayNotificationWorker.log
- CMGatewaySyncUploadWorker.log

Most of all, if you monitor the CMGatewaySyncUploadWorker.log, we see 4 devices uploaded to Intune. The device collection that i chose has got 4 devices running Windows 10.



ConfigMgr Tenant Attach Log Files

In the upcoming posts, I will show you what you can do after you have enabled tenant attach in SCCM. Until then stay excited.

Co-Management Configuration Manager Intune SCCM

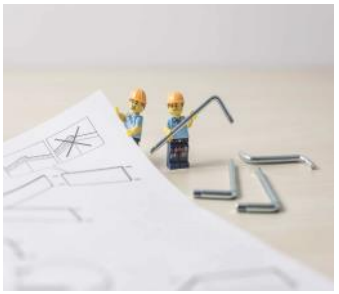
Prajwal Desai

Hi, I am Prajwal Desai. For last few years I have been working on multiple technologies such as SCCM / Configuration Manager, Intune, Azure, Security etc. I created this site so that I can share valuable information with everyone.

RELATED ARTICLES

Configuring Client Status in SCCM 2012

April 13, 2018



Distribution Point Job Queue Manager
December 12, 2018

Configuration Manager 1802 Hotfix KB4163547
July 14, 2018

2 Comments

Mattsays:
January 26, 2021 at 12:20 am
Hi, when I click on the Sign In button on the Co-management Configuration Wizard. I get prompted with “content within this application coming from the website listed below is being blocked in IE enhanced Security configurations.” However, I’ve added https://login.microsoftonline.com to my local security. Any thoughts
Reply

Sundaysays:
September 30, 2020 at 7:44 pm
Wonderful Article as always from you. Can you show picture of:
” Initiate Configuration Manager action permission under Remote tasks in the Microsoft Endpoint Manager admin center.” requirement?

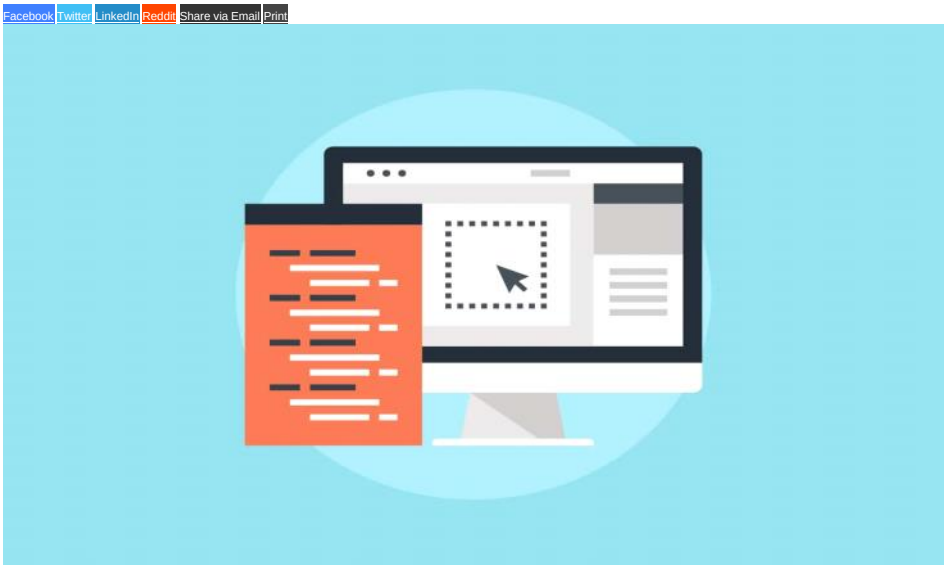
From <https://www.prajwaldesai.com/enable-tenant-attach-in-configmgr-sccm/>

Add User or Groups to Local Admin in Intune

19 February, 2021 8:33 AM

Add User or Groups to Local Admin in Intune

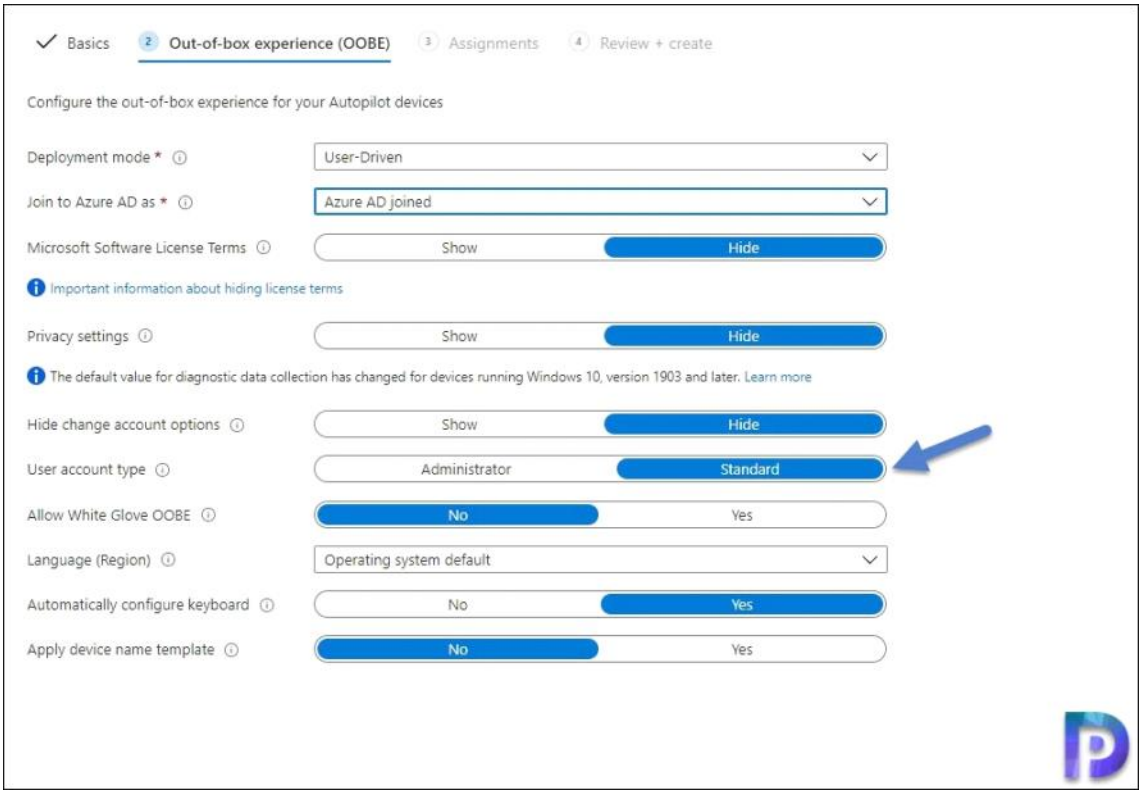
Dakhama MehdiJanuary 23, 2021
1 2 minutes read



In this post I will show you how to add user or groups to local admin in Intune. The machine could be a domain joined or without domain.

To manage a Windows device, you need to be a member of the local administrators group. Read this article to know more about managing local administrators on Azure AD joined devices.

Many people assume when you add a user in the first time with Autopilot, user becomes local admin. This happens if you leave the Profile Autopilot settings by default as Administrator.



Autopilot Standard User

But if you configure the OOBE profile to Standard, there will be no local admin, even local administrator is disabled. Furthermore there is no option that allows you to change it.

Add User or Groups to Local Admin in Intune

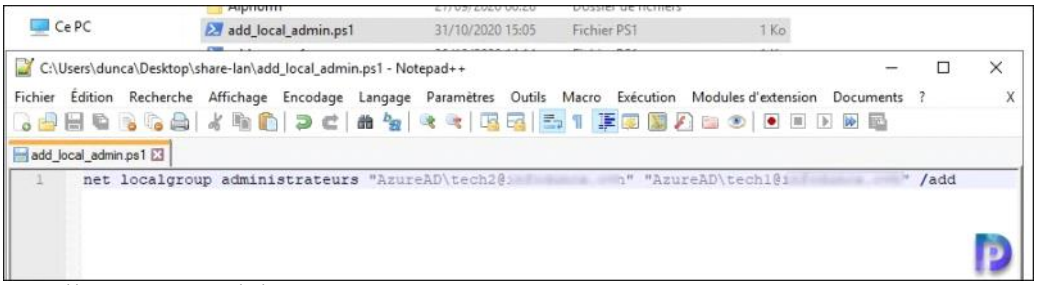
We will now look at the steps to add user or groups to local admin in Intune. First lets create a new text file and rename it add_localadmin.ps1.

You can edit this file either with PowerShell ISE or Notepad++. Paste the following command inside the file

```
Net localgroup administrators "AzureAD\yourgroups@domain.xx" /add
```

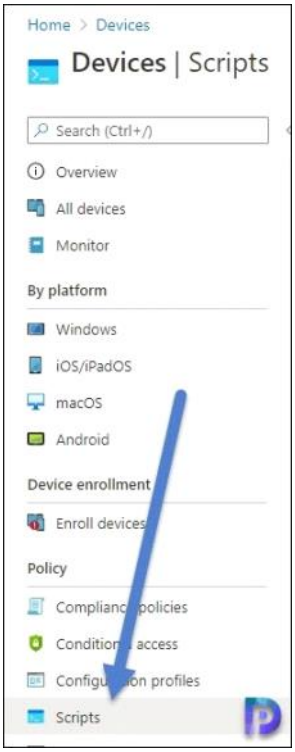
Replace “AzureAd\xxxx” with email account of your groups or user.

Tip – Don’t use the PowerShell command add-Localgroup because it creates an error, and doesn’t work on remote computer.



Intune Add User or Groups to Local Admin

After you have made the changes, save your ps1 script. Return to Intune portal. In the portal, create a new script.

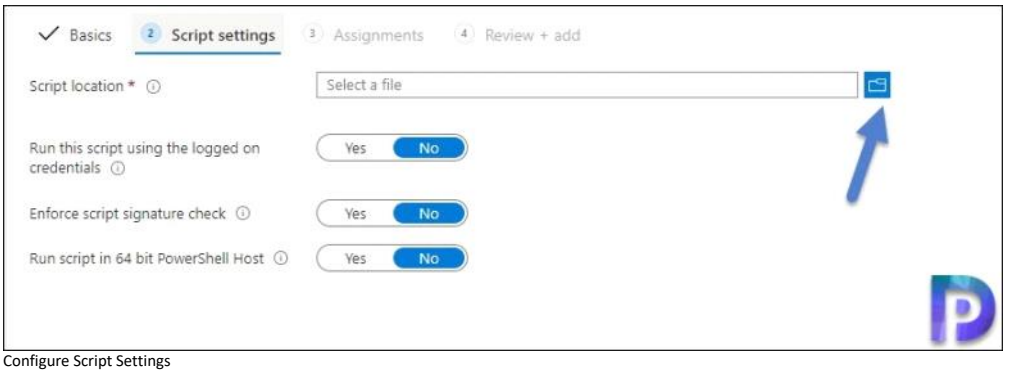


Create Script in Intune Portal

Add a Powershell script. Specify script name and add a description.

Add PowerShell Script

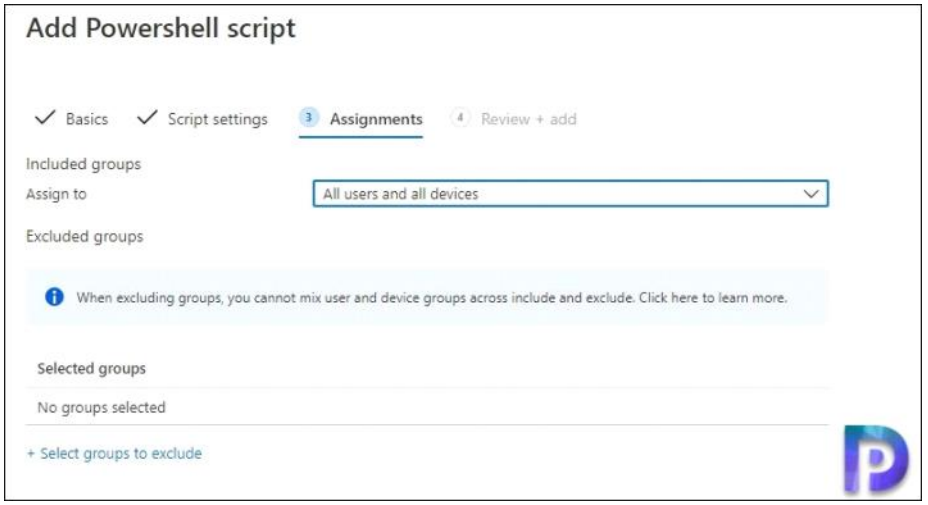
Import the add_localadmin.ps1 script. Leave the other settings to default.



Configure Script Settings

Select groups that you wish to assign your script. Don't forget the script will be assigned

to computer groups, or by default select all devices. Click Next.

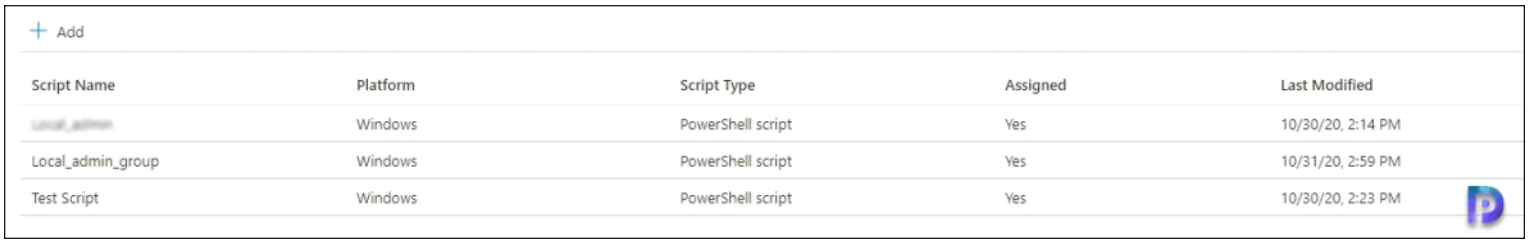


Script Assignments

Finally review the settings and click Create.

Intune Add User or Groups to Local Admin

Take a look at the script and ensure the Assigned value is set to Yes.

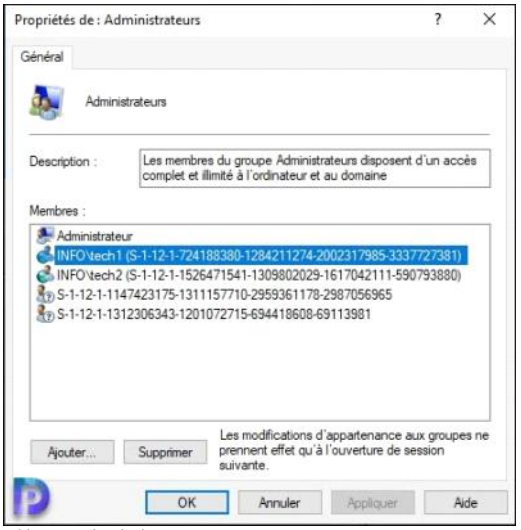


Verify the Assigned Field

After you have applied the script, wait for few minutes or manually trigger the sync.

Trigger Intune Sync

The script has done the changes. We see the users are now part of local administrator group. Do not forget to logoff and logon to see the results.



Add users to local admin

Administrator Intune

Dakhama Mehdi

Hello, I'm DAKHAMA MEHDI from FRANCE. I am currently working as a MICROSOFT consultant and trainer (infrastructure, cloud and server), and systems administrator for more than 12 years. I am also a developer desktop applications. I managed lot projects of different technology (SCCM, Server, MDT, ADFS, ADRMS, Security, Microsoft 365, Intune …). I like to share my knowledge and helping everyone through my articles and applications.

From <https://www.prajwaldesai.com/add-user-or-groups-to-local-admin-in-intune/>

Deploy Microsoft Teams Using Intune – Microsoft 365 Apps

Prajwal DesaiJanuary 23, 2021
2 3 minutes read

In this post we will go through the steps to deploy Microsoft Teams using Intune. We will use Microsoft Endpoint Manager Admin Center to add, create and deploy Teams.

Microsoft Teams is a proprietary business communication platform developed by Microsoft. It is your hub for teamwork and includes chat and threaded conversations, meetings & video conferencing, calling etc.

On April 21 2020, Microsoft announced new product name changes and these are already in effect. You can read the following article to know more about Microsoft product name changes.

- Office 365 Business Essentials is now Microsoft 365 Business Basic.
- Office 365 Business Premium is now Microsoft 365 Business Standard.
- Microsoft 365 Business is now Microsoft 365 Business Premium.
- Office 365 Business and Office 365 ProPlus is now Microsoft 365 Apps.

Deploying Teams via Configuration Manager involves downloading and packaging teams application. While with Intune you can easily deploy Microsoft Teams to end users.

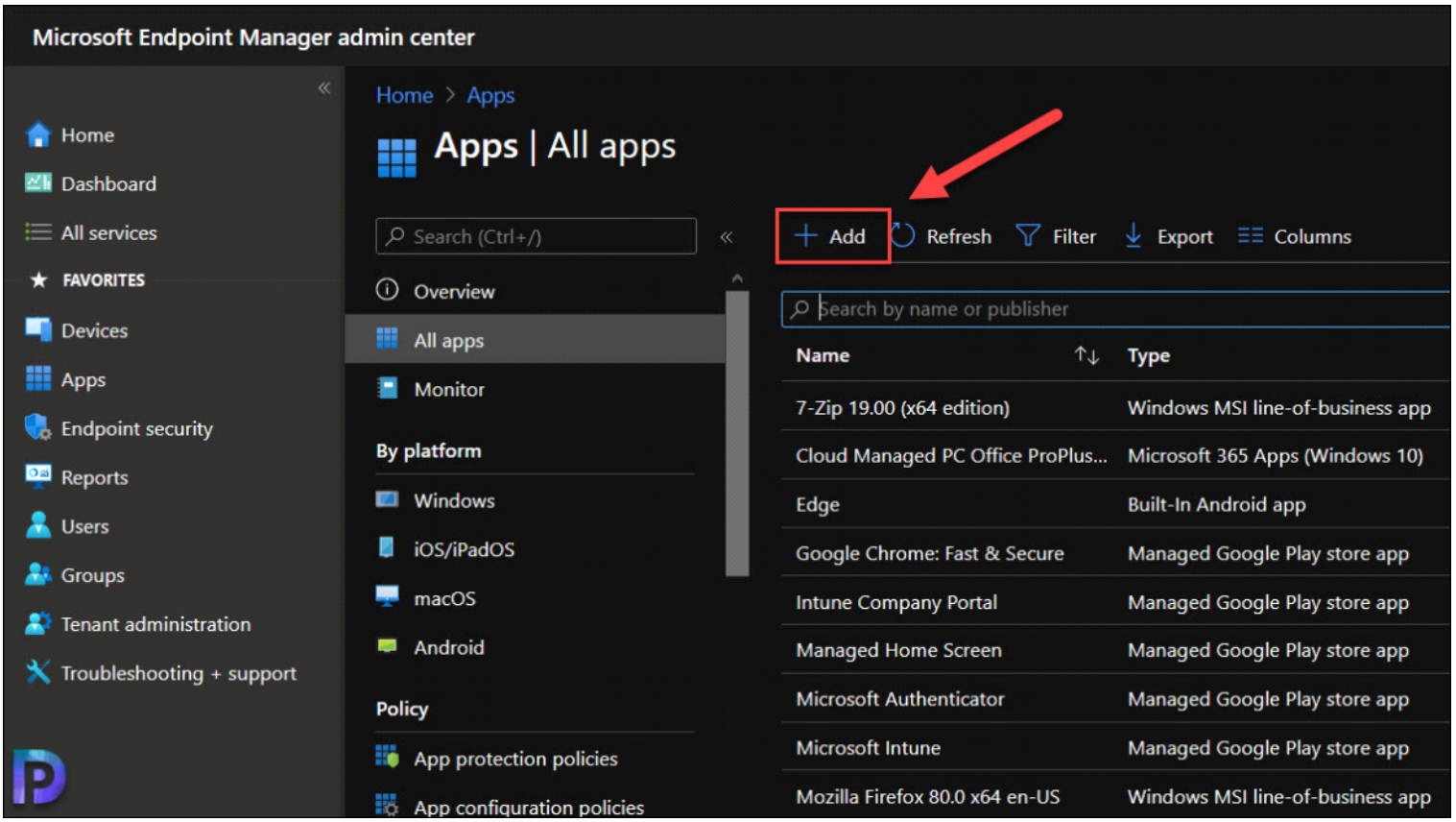
Contents

Deploy Microsoft Teams Using Intune – Microsoft 365 Apps

Follow the below steps to deploy Microsoft Teams using Intune

- Login to the Microsoft Endpoint Manager Admin Center.
- In the left pane, click Apps > All Apps.
- To add Microsoft Teams app, click Add button.
- Under App type select Microsoft 365 apps for Windows 10.
- In the next step, select Teams as Office app and complete the app assignment.

Let's look at the deployment steps in detail. In the Microsoft Endpoint Manager admin center, click Apps and then All Apps. Click the Add button.



Add New Application In Intune

In this step you must select app type. So click the drop down and under Microsoft 365 Apps select Windows 10.

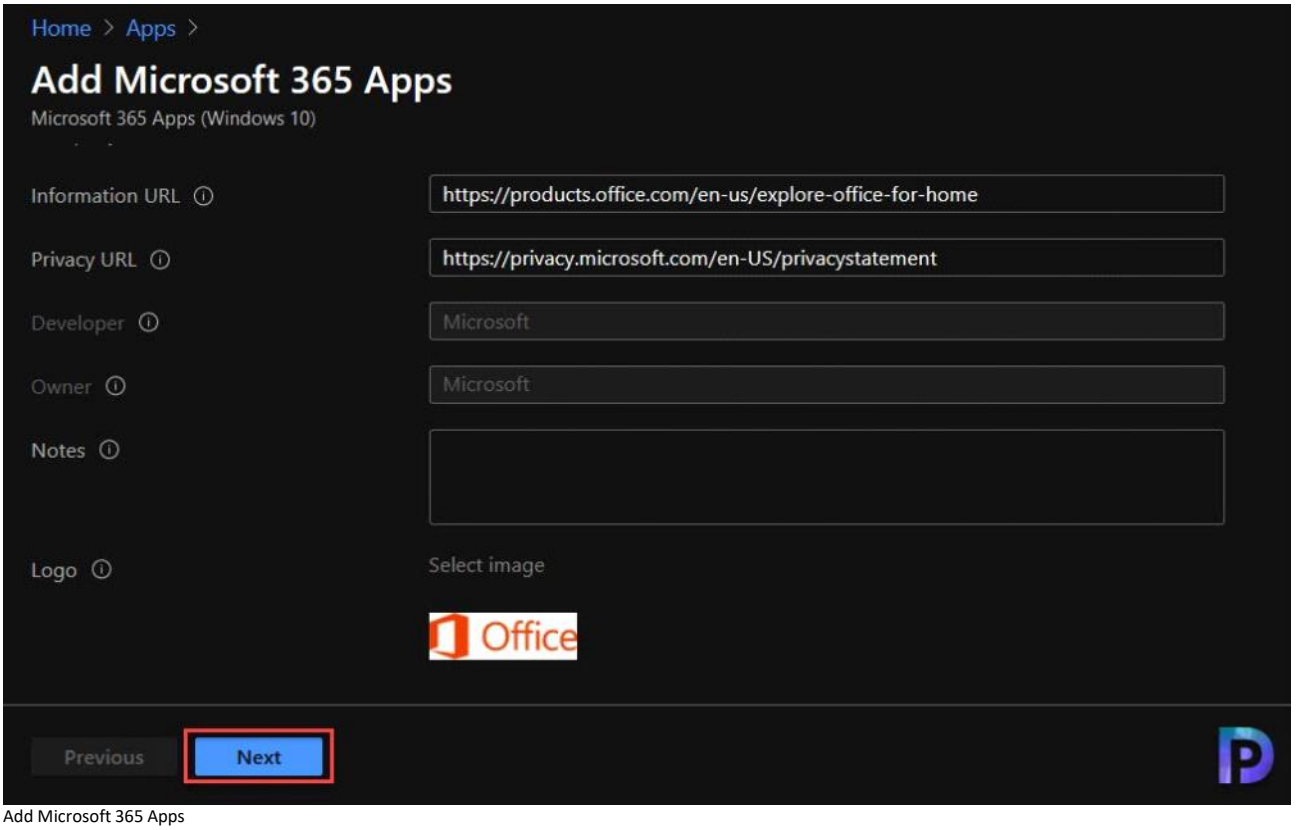
Microsoft 365 Apps for Windows 10

App Suite information – Add Microsoft 365 Apps

Under the App Suite information, you will find the following settings.

- Suite Name – The default name is Microsoft 365 Apps for Windows 10. However you can change it custom name such as Microsoft Teams.
- Suite Description – You may click Edit Description and add more info about the Teams application.
- Publisher – This is set to Microsoft by default.
- Category – Select the application category. I have selected the app category as Productivity.
- Show this as a featured app in the Company Portal – Select this option to display Teams as featured app in company portal.
- Information URL – A link that describes information about this app. The URL is already set by Microsoft.
- Privacy URL – Users may click this link to know more about Teams app privacy settings and terms.
- Developer – Set to Microsoft by default.
- Owner – Set to Microsoft by default.
- Notes – Admins can add some notes about the application here.
- Logo – Upload a custom logo and this will appear in company portal.

Once you have configured the above settings, click Next.

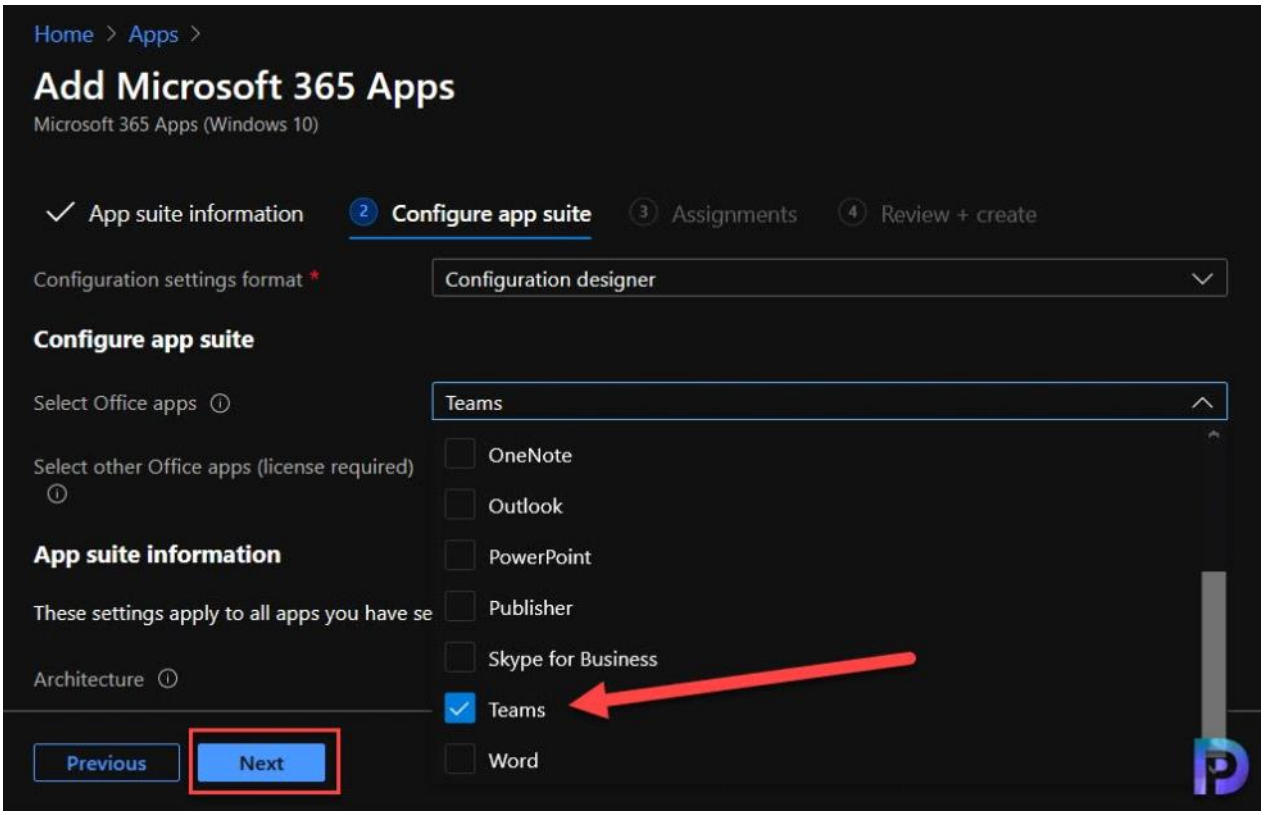


Add Microsoft 365 Apps

Configure App Suite – Microsoft Teams

In this step we actually select enable Teams app under Microsoft 365 apps for deployment. So configure the following settings.

- Configuration settings format – Set this to Configuration designer.
- Select Office apps – Click the drop-down and from the list of Microsoft 365 Apps, select Teams app.
- Select other Office apps – This is optional and in addition to above apps, you can select Visio and Project client. Note that a license is required.

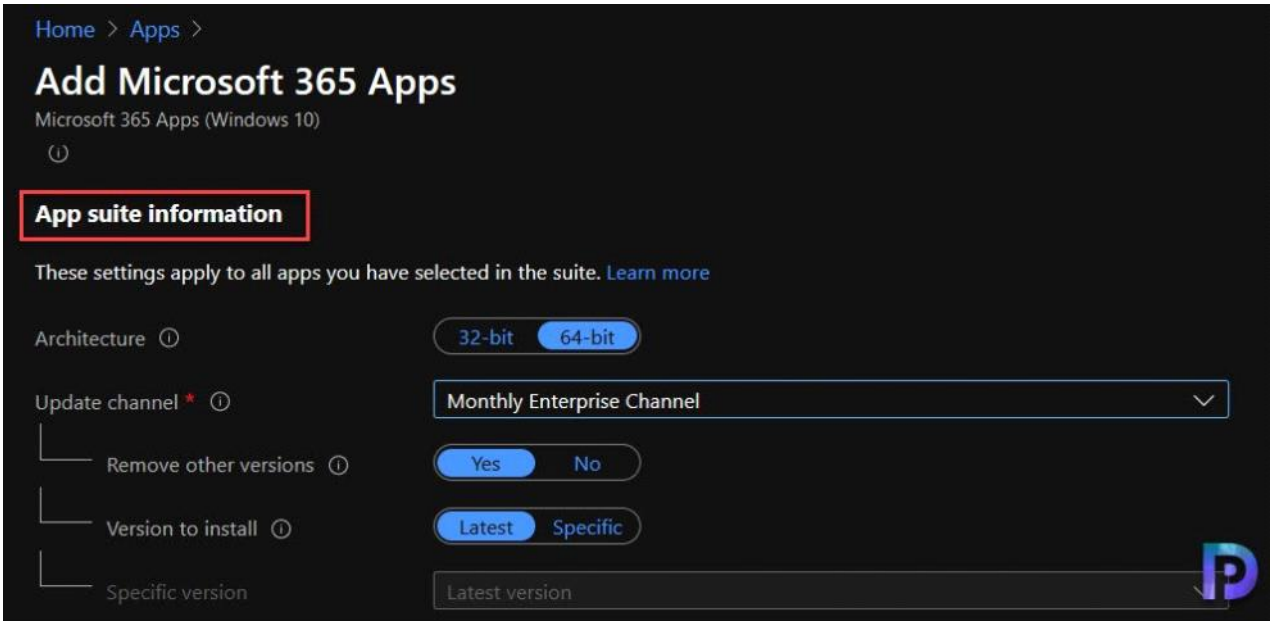


Deploy Microsoft Teams Using Intune

Teams App Suite Information

Based on the applications that we selected in the above step, now we define some important settings.

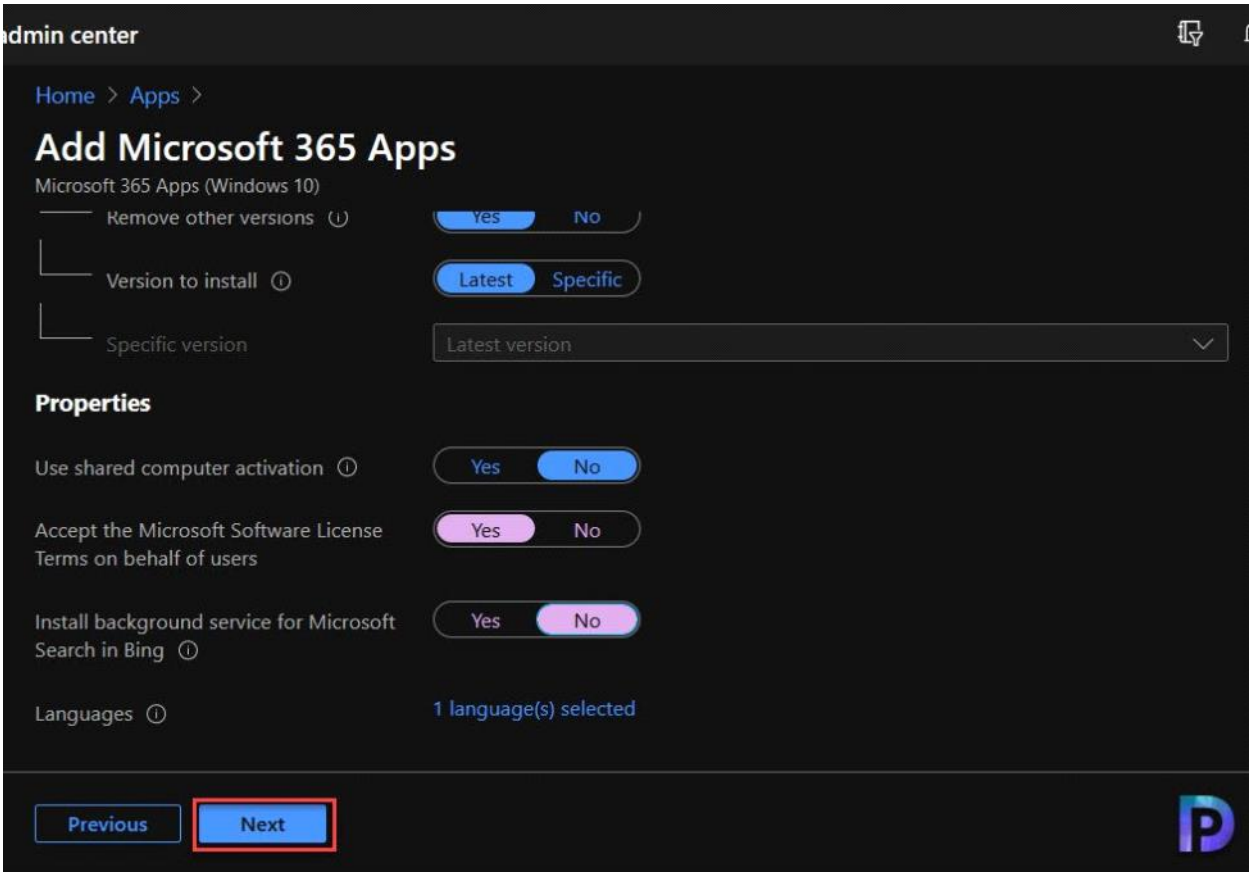
- Architecture – Choose either 32-bit or 64-bit Teams application.
- Update Channel – Select the update channel. I have selected Monthly Enterprise channel.
- Remove other versions – Select Yes to remove other versions of Office (MSI) from user devices.
- Versions to Install – Select the Latest version because that is the preferred option. To select an older version or a version of your choice, select Specific.



Deploy Microsoft Teams Using Intune

- Use shared computer activation – Shared computer activation lets you deploy Microsoft 365 Apps to computers that are used by multiple users. Normally, users can only install and activate Microsoft 365 Apps on a limited number of devices, such as 5 PCs. Using Microsoft 365 Apps with shared computer activation doesn't count against that limit.
- Accept the Microsoft Software license terms on behalf of users – Select Yes.
- Install background service for Microsoft search in Bing – If you wish to add or install background service for Microsoft search in bing, select Yes.
- Languages – Select additional languages to deploy it along with Teams.

Click Next.

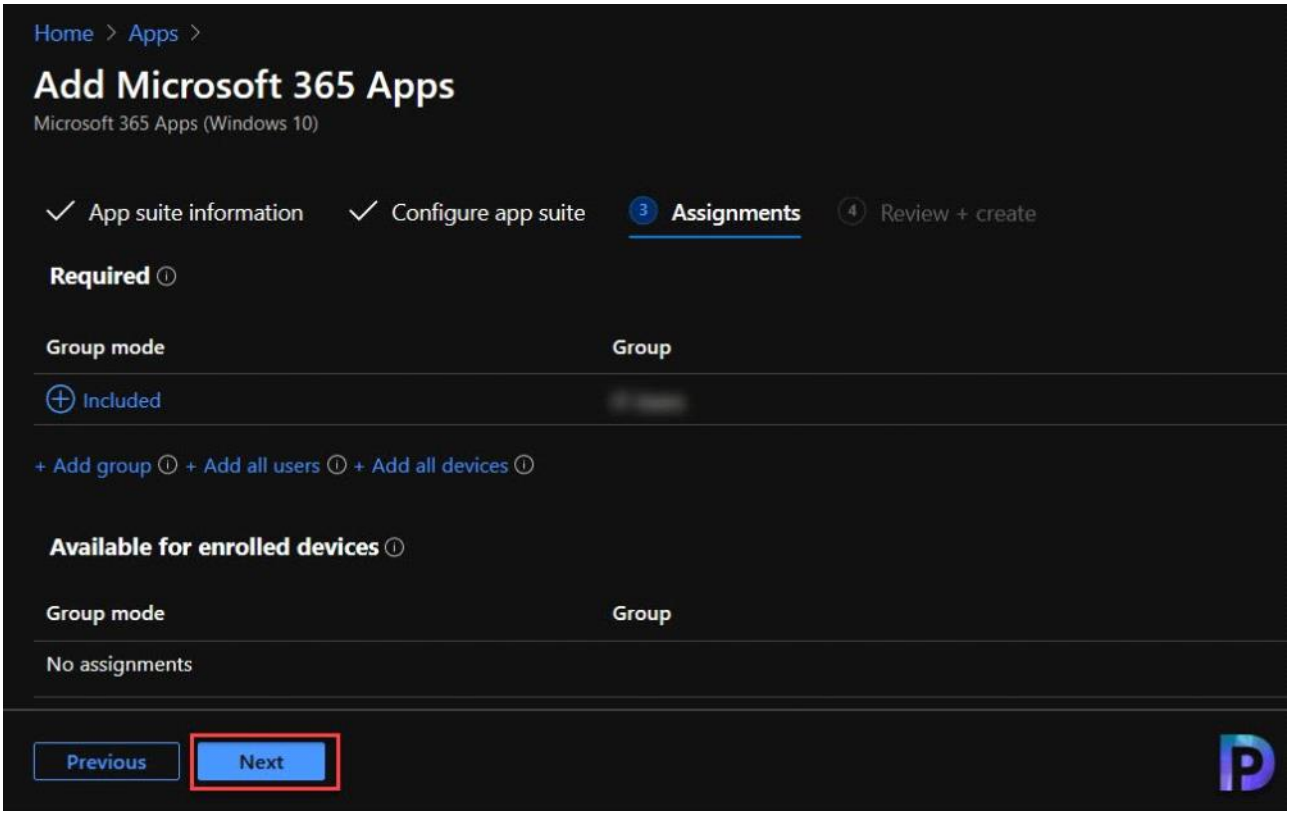


Deploy Microsoft Teams Using Intune

Teams Application Assignments in Intune

Finally the last step it to determine who needs to get this application. Before you assign groups to the app, you must set the assignment type for an app. The assignment type makes the app available, required, or uninstalls the app.

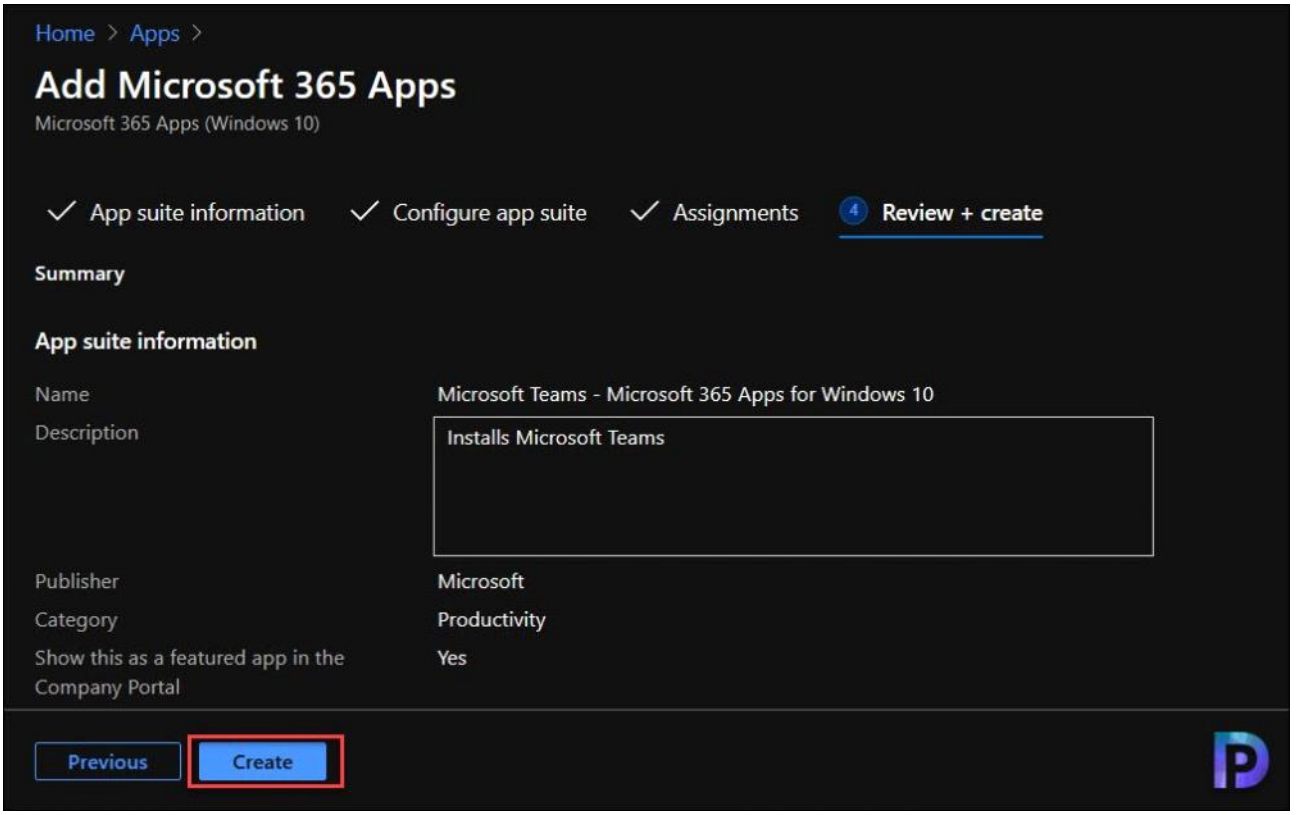
Perform the app assignment based on your requirement. Click Next.



App Assignments in Microsoft Intune

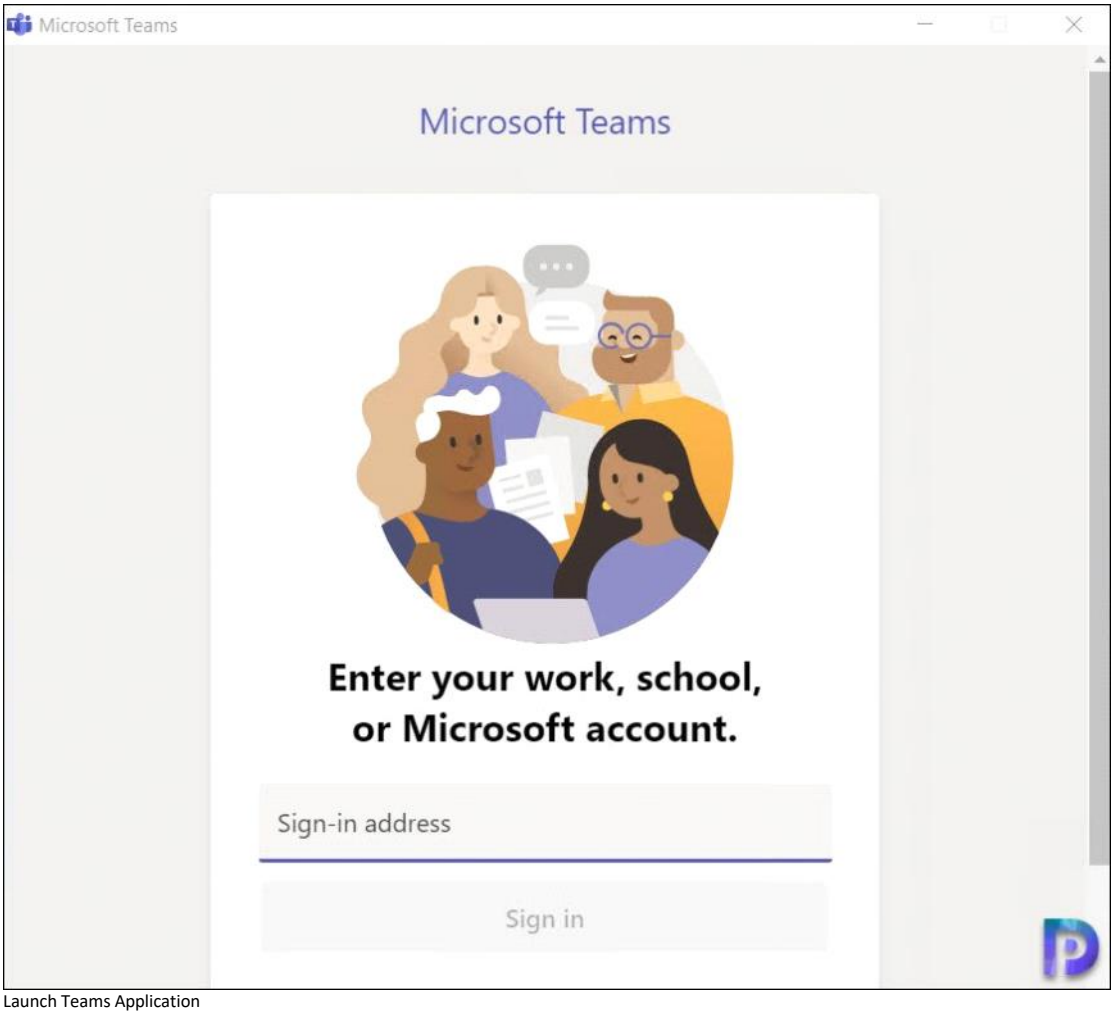
Review and Create Teams Application

In this step you review the entire configuration that you have done so far. If you find it perfect, hit the Create button.



Deploy Microsoft Teams Using Intune

On my Windows 10 machines, the Teams application got installed. But there is a catch here. The Teams application will launch at startup only when you restart the machines.



Launch Teams Application

Intune Microsoft Teams

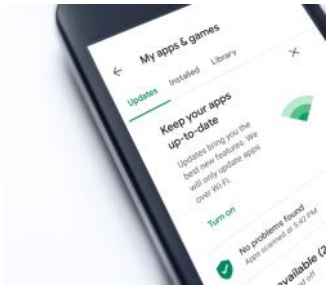
Prajwal Desai

Hi, I am Prajwal Desai. For last few years I have been working on multiple technologies such as SCCM / Configuration Manager, Intune, Azure, Security etc. I created this site so that I can share valuable information with everyone.

RELATED ARTICLES

Change Intune Primary User of Windows Device

April 21, 2020



Add the Google Chrome app to Intune

March 20, 2020

Add Incoming Webhook to a Teams channel

March 21, 2020

2 Comments

Nathan O says:

January 27, 2021 at 3:09 pm

Hi

Has anyone found issues when it comes to Teams updating on a MS Surface Pro device?

Finding that the client will update, but downgrades itself after a device reboot.

Thanks

Reply

Donald M says:

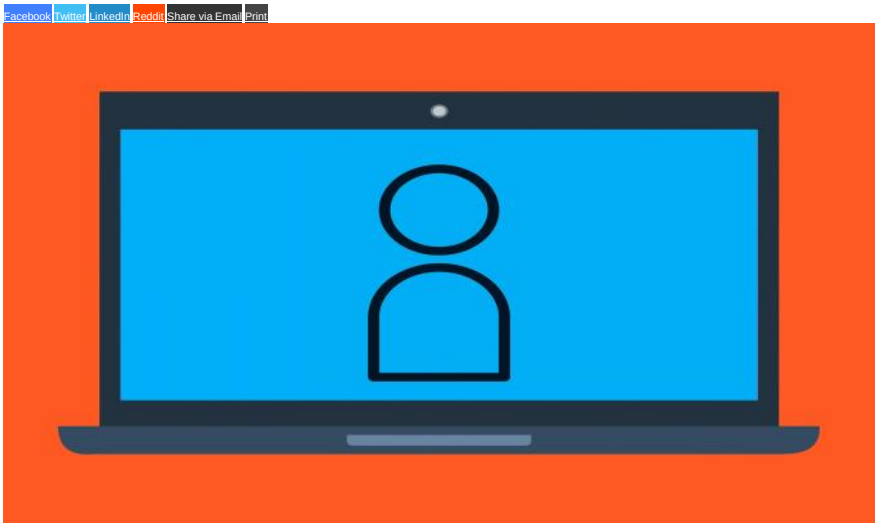
January 25, 2021 at 11:41 pm

Thank you for this step-by-step article! Very well done.

From <https://www.prajwaldesai.com/deploy-microsoft-teams-using-intune/>

Fix CNAME Validation Error in Intune Portal (MEM admin center)

Prajwal DesaiJanuary 24, 2021
0 2 minutes read



This post guides you to fix the CNAME Validation Error in Intune. In the MEM admin center (Intune Portal), when you perform a CNAME validation, you might see the following error. CNAME for domain is not configured or configured incorrectly.

You don't need to worry as the fix for this error is very simple.

Configuring a CNAME in your DNS server saves your users from having to enter the address of the MDM server while enrolling their Windows devices.

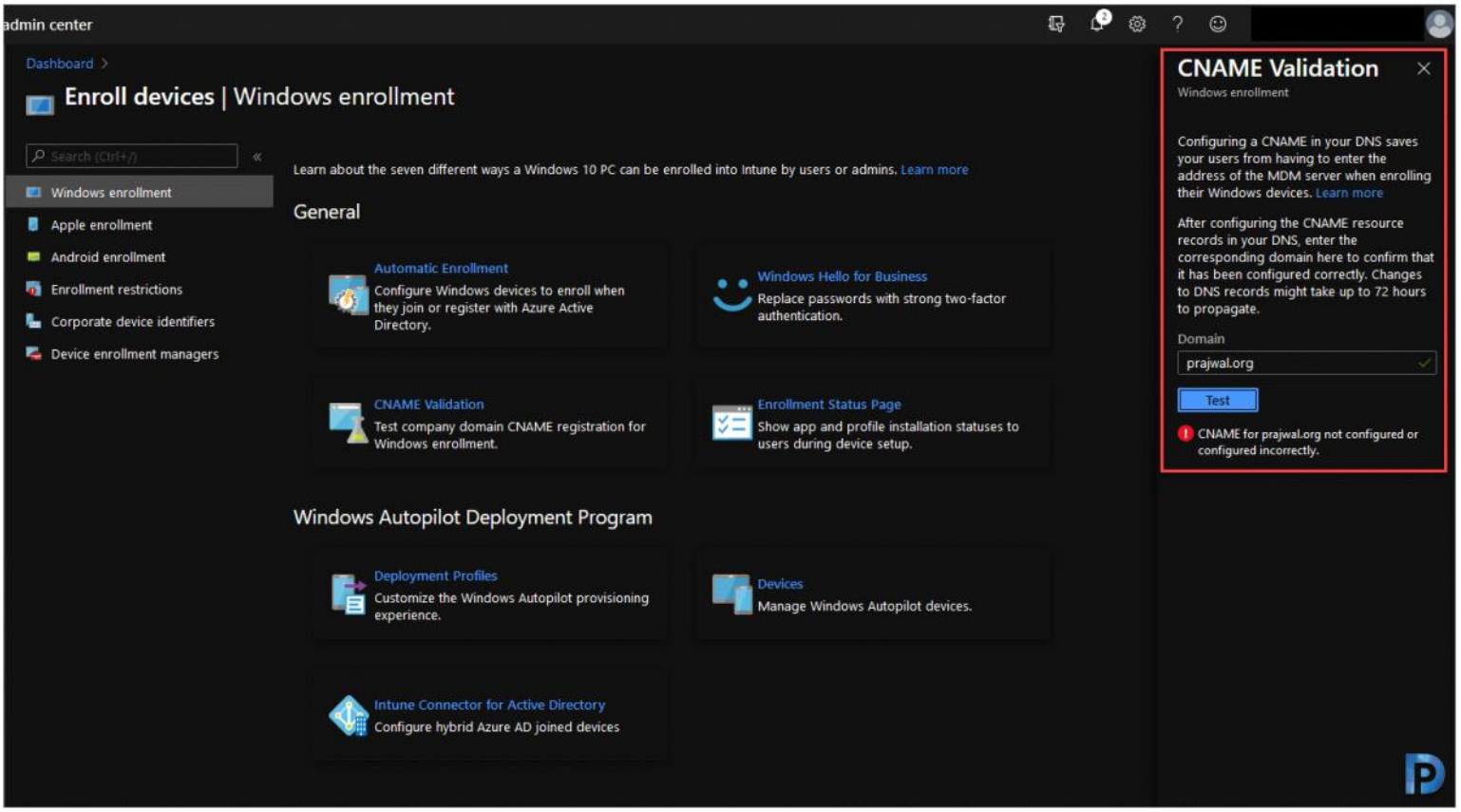
To simplify enrollment, you must create a domain name server (DNS) alias (CNAME record type) that redirects enrollment requests to Intune servers.

If no enrollment CNAME record is found, users will be prompted to manually enter the MDM server name, enrollment.manage.microsoft.com.

CNAME Validation Test

If you want to perform a CNAME validation test for your domain, here is how you do it.

- First of all login to Microsoft Endpoint Manager admin center.
- In the left pane click Dashboard. Now in the right pane, click Device Enrollment.
- Under the General, click CNAME Validation.
- You will see CNAME Validation box on right hand side of the screen.
- Enter your domain and click Test.
- If you see CNAME for domain not configured or configured incorrectly, follow the next steps.



CNAME for domain is not configured or configured incorrectly

How to Fix CNAME Validation Error in Intune Portal

So let's say you see this error during the CNAME Validation "CNAME for domain not configured or configured incorrectly".

All you need to do is add or create the below CNAME entries on your DNS server.

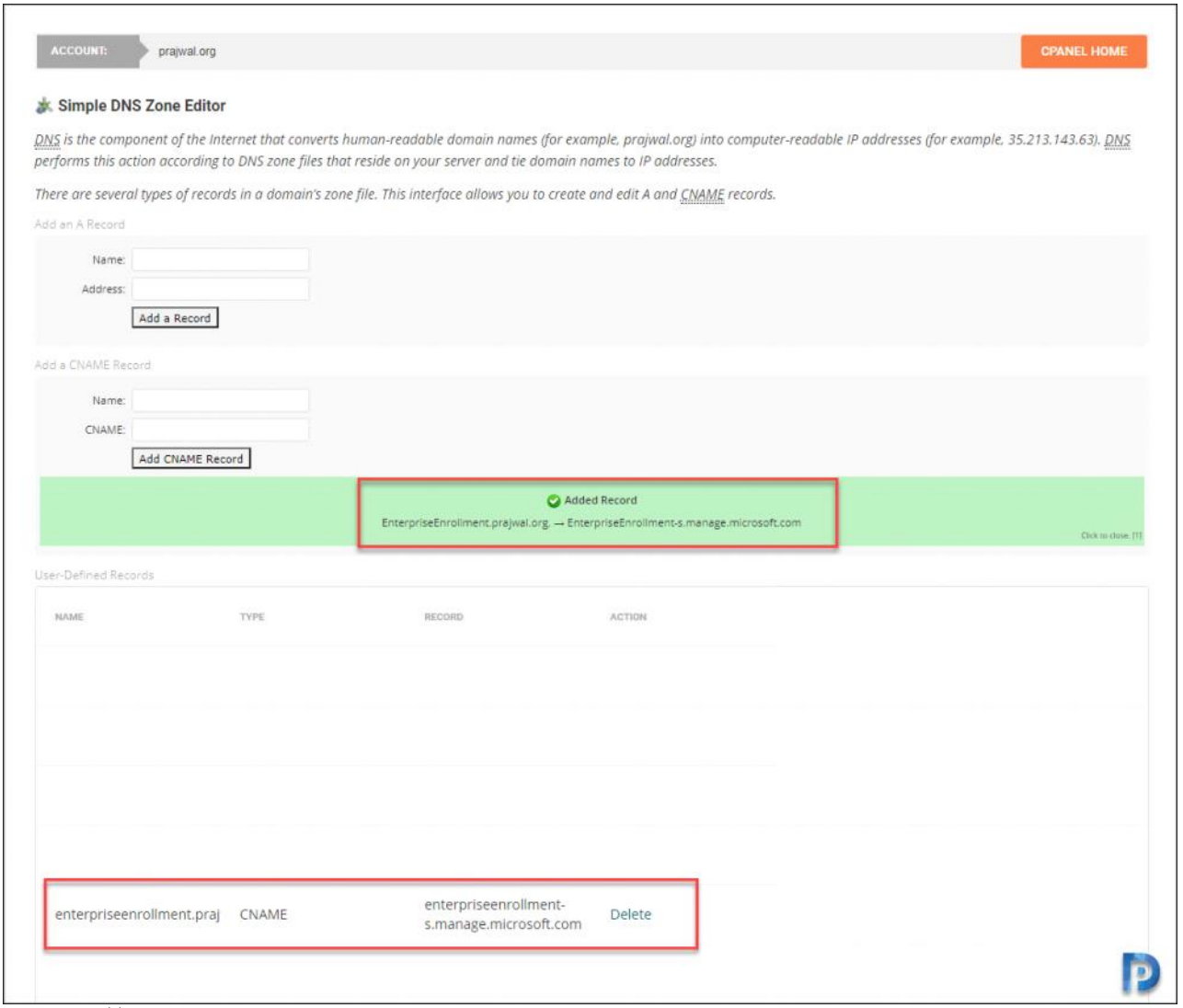
- You must create a CNAME in DNS that redirects EnterpriseEnrollment.contoso.com
- And a second CNAME that redirects to enterpriseenrollment-s.manage.microsoft.com.

For example, I will be creating two CNAME entries on my DNS server for the domain prajwal.org. The entries would look like this.

Type	Hostname	Redirects or Points to
CNAME	EnterpriseEnrollment.prajwal.org	EnterpriseEnrollment-s.manage.microsoft.com
CNAME	EnterpriseRegistration.prajwal.org	EnterpriseRegistration.windows.net

Some hosting providers require you to specify TTL values which would be 1 hour in this case.

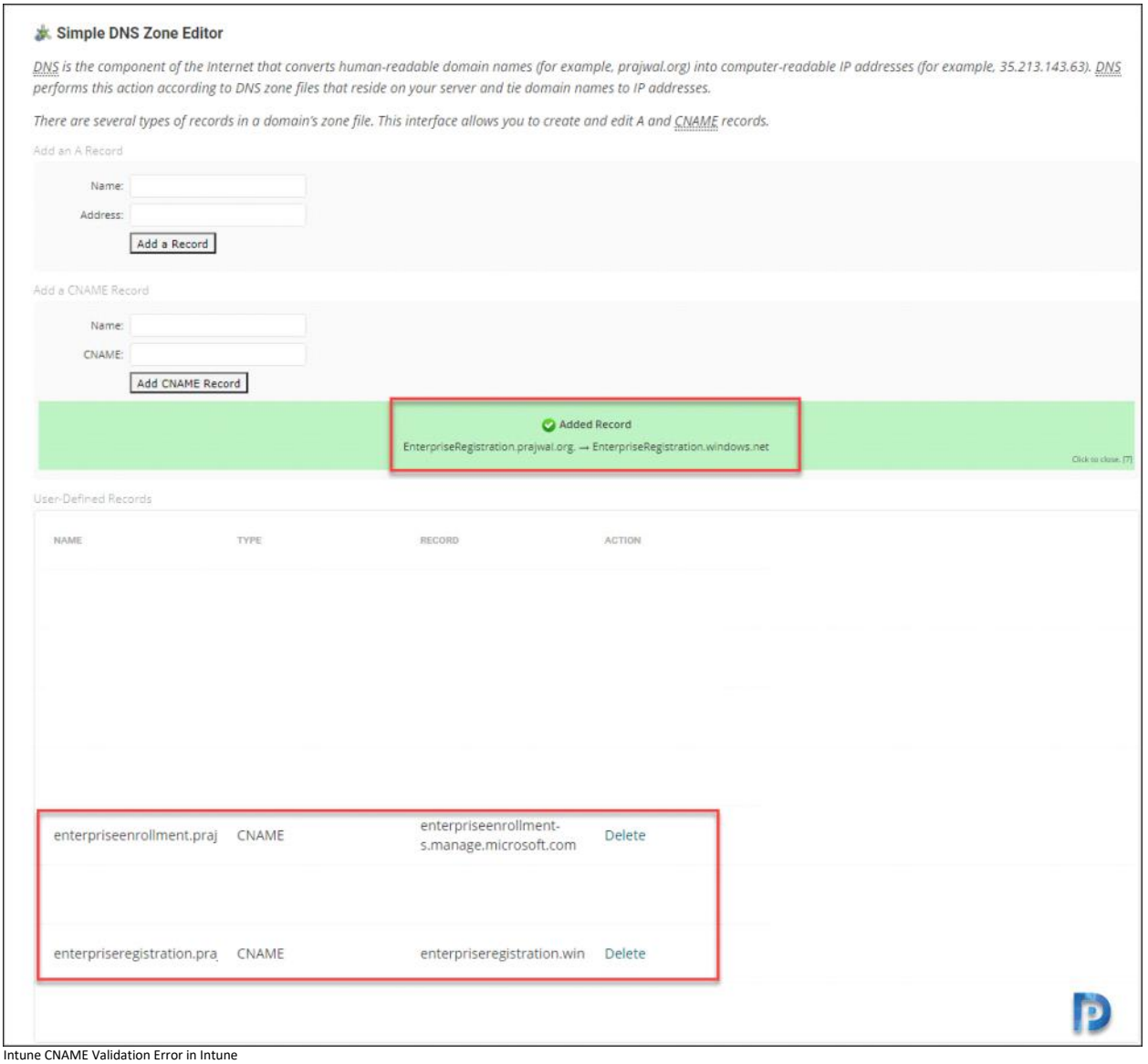
Let's add the first CNAME resource record which points EnterpriseEnrollment.yourdomain.com to EnterpriseEnrollment-s.manage.microsoft.com



Intune CNAME Validation Error in Intune

Now let's add the second CNAME resource record which points

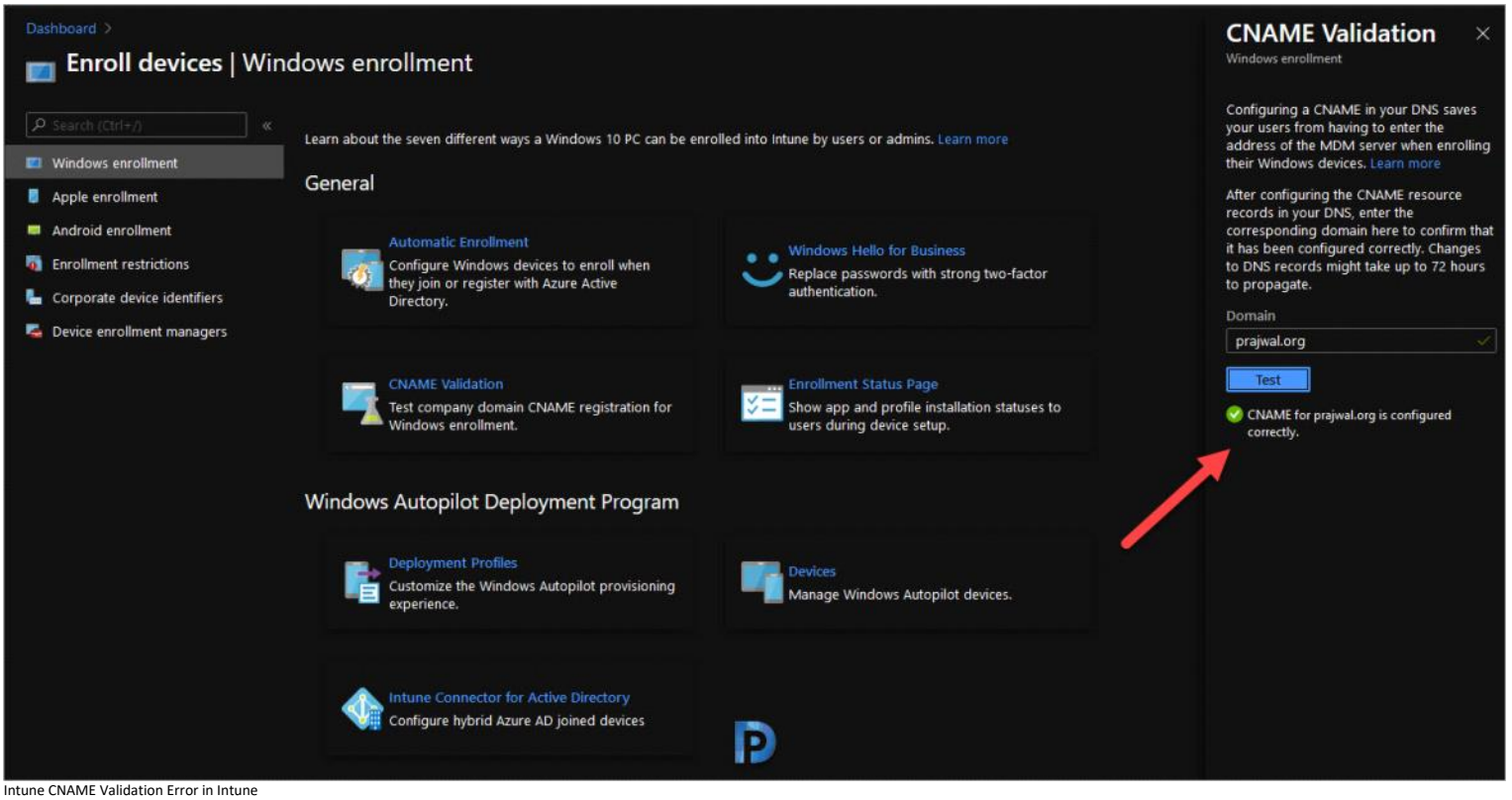
EnterpriseRegistration.yourdomain.com to EnterpriseRegistration.windows.net.



Intune CNAME Validation Error in Intune

Note – Changes to DNS records might take up to 72 hours to propagate. Hence wait until the DNS records propagate.

Finally after configuring the CNAME resource records in your DNS, login to Microsoft Endpoint Manager admin center. Enter the domain here to confirm that it has been configured correctly.



Intune CNAME Validation Error in Intune

CNAME Validation Intune

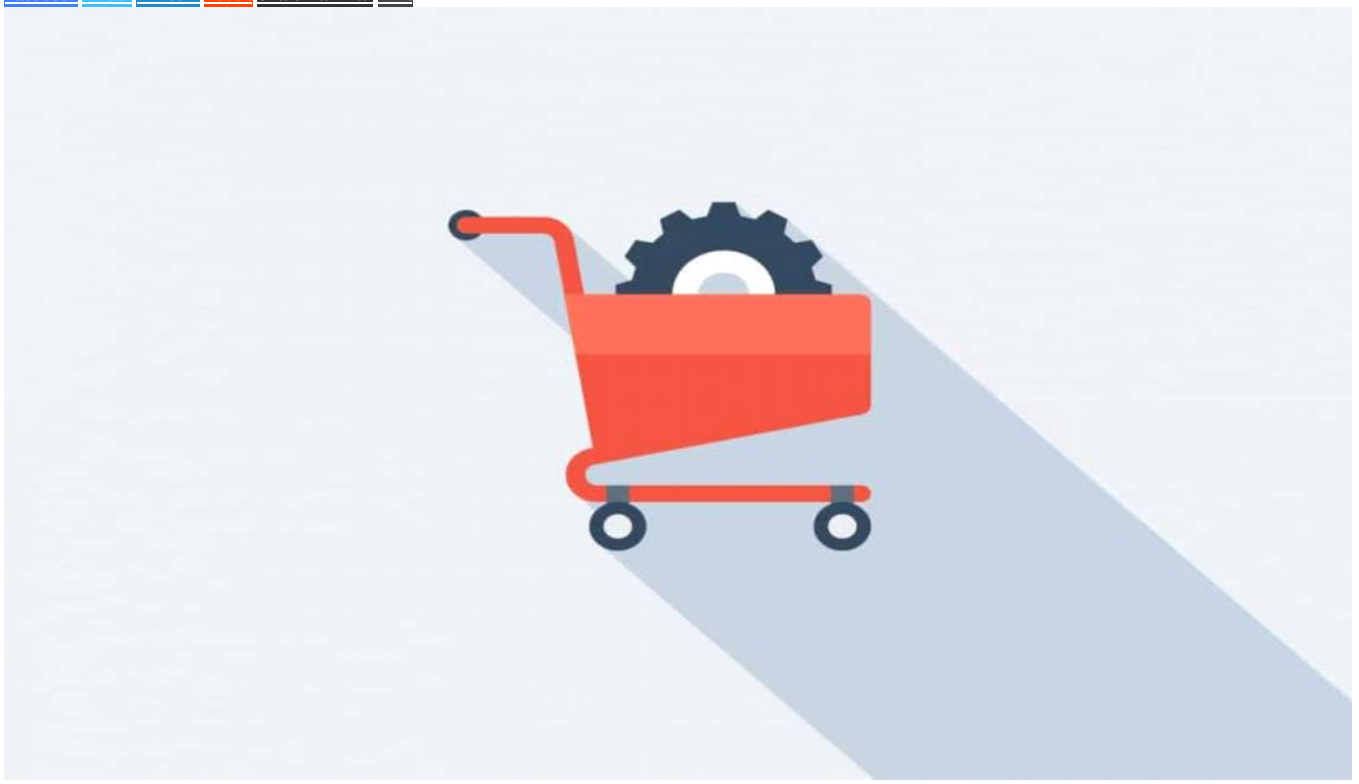
Prajwal Desai

Hi, I am Prajwal Desai. For last few years I have been working on multiple technologies such as SCCM / Configuration Manager, Intune, Azure, Security etc. I created this site so that I can share valuable information with everyone.

From <https://www.prajwaldesai.com/fix-cname-validation-error-in-intune-portal-mem-admin-center/>

Adding Microsoft Intune Device Enrollment Manager

Prajwal DesaiJune 24, 2017
4 1 minute read



In this short post we will look at steps for adding Microsoft Intune device enrollment manager. The question is what is device enrollment manager and why do you need it. The device enrollment manager is an account that can enroll devices in Intune. A device enrollment manager can enroll up to 1000 devices. Do not get confused with Intune admin account and a DEM account. However a device enrollment manager user cannot be an Intune admin. To designate the user as DEM the user account must be present in Intune console. In other words the users must be already created before you designate them as DEM.

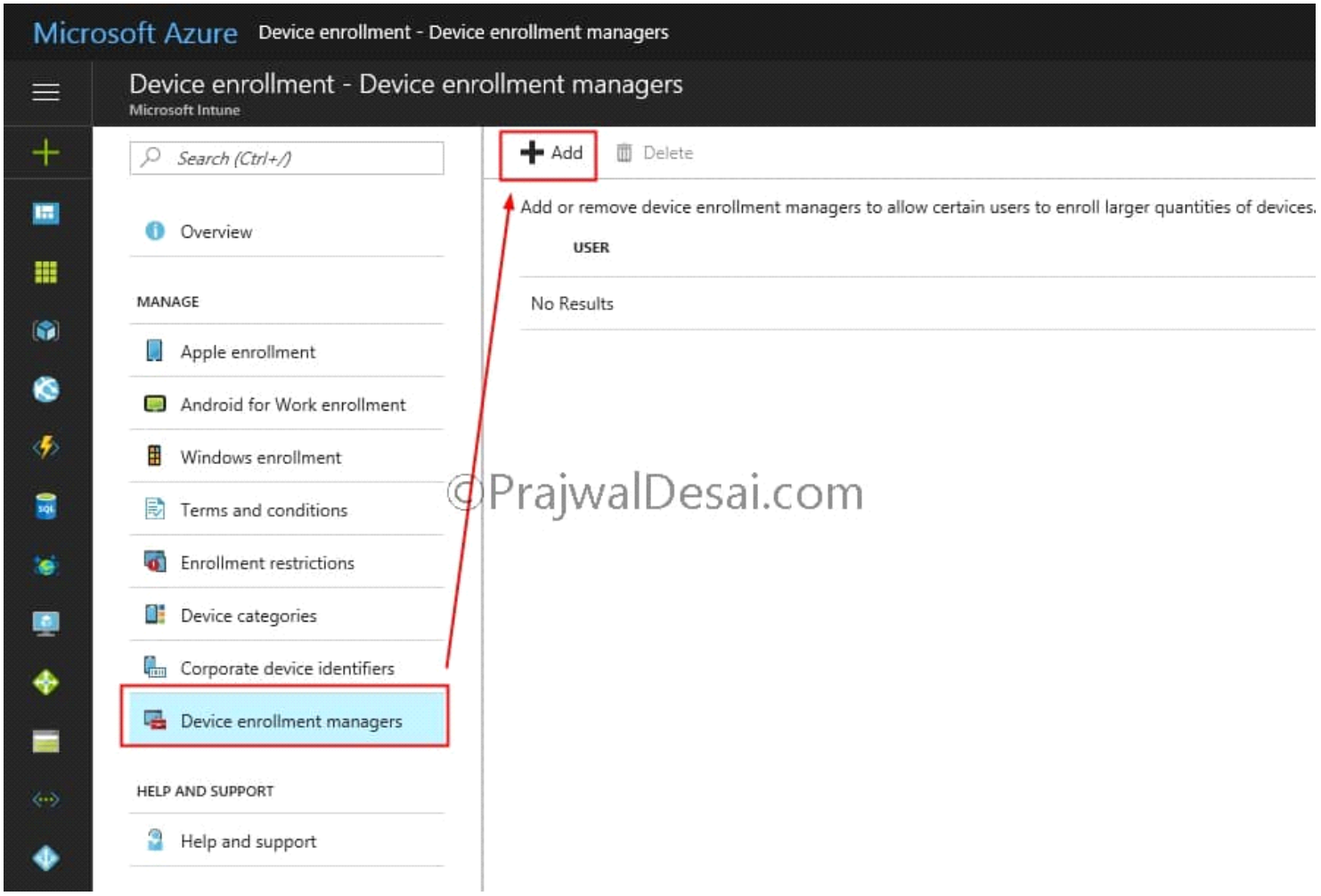
The devices enrolled by device enrollment manager comes with certain limitations. I wouldn't worry about the limitations much here. One important limitation that I see is the capability to unenroll the devices. The DEM user cannot unenroll DEM-enrolled devices on the device using the Company Portal. Only the Intune admin has this capability and not

the DEM user. Let's proceed further now and see how to add DEM.

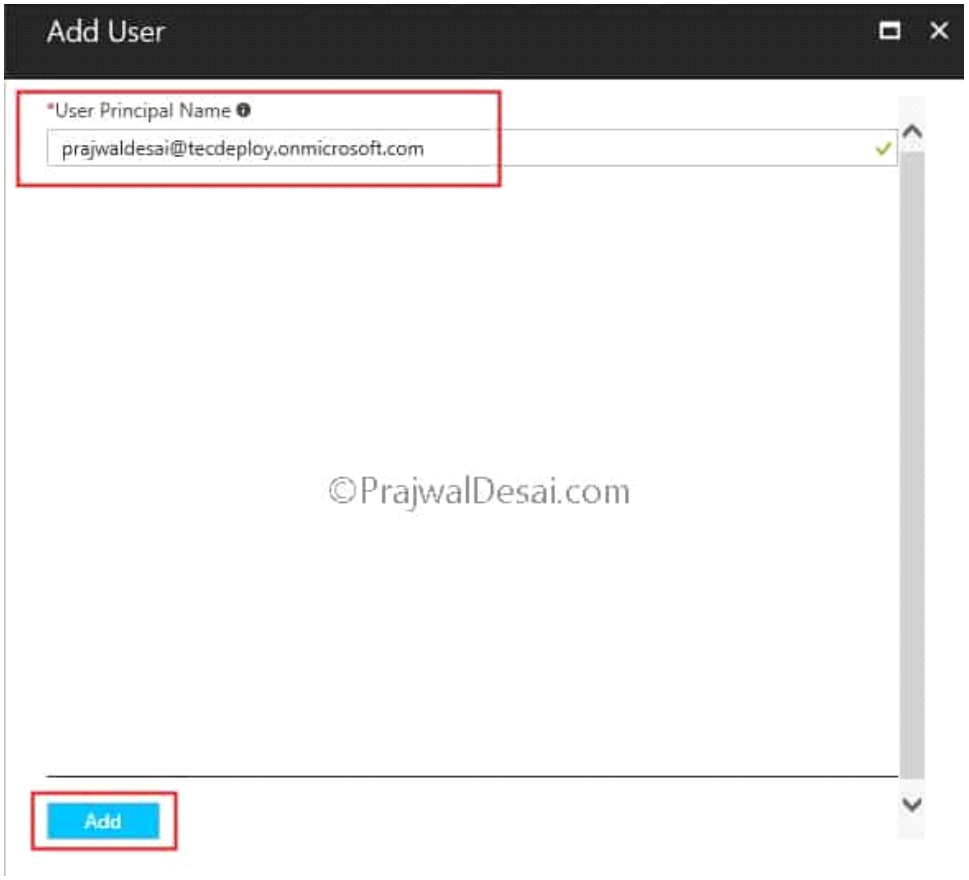
Adding Microsoft Intune Device Enrollment Manager

Let's look at the steps for adding Microsoft Intune device enrollment manager. In the Azure portal look for Device enrollment under Manage.

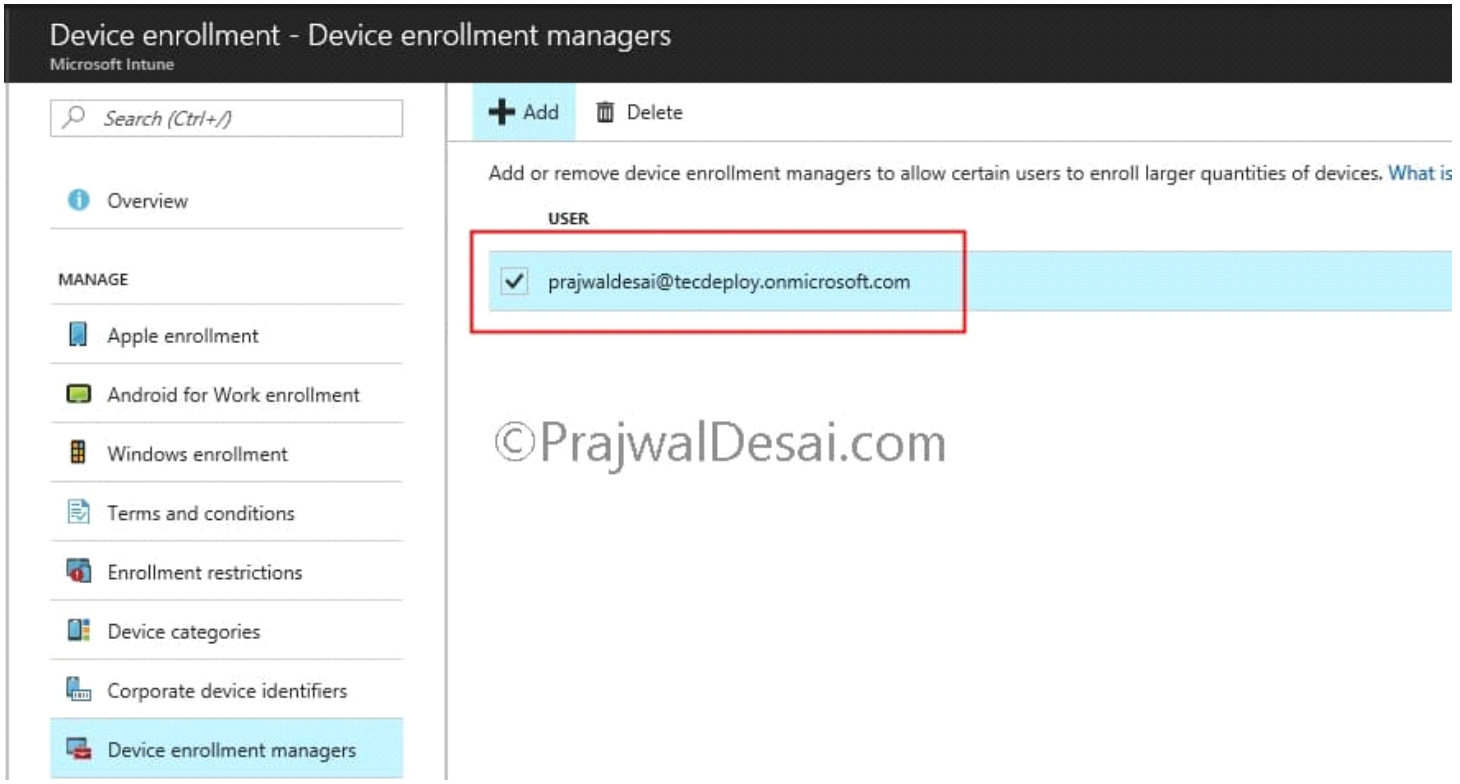
Click Device enrollment managers. On the right pane click on + Add.



Type the user principal name or the user account that will be a DEM. Click Add.



That's it. You have added a new device enrollment manager. This account can now enroll the devices.



How to delete device enrollment manager – To delete a device enrollment manager, select the account and hit delete. The user won't be deleted from Intune. However the

user cannot enroll the devices any further.

After deleting DEM, what happens to devices enrolled by DEM – There should be no issues there. Deleting DEM will not affect enrolled devices. Enrolled devices continue to be fully managed.

Device Enrollment Manager **Intune**

Prajwal Desai

Hi, I am Prajwal Desai. For last few years I have been working on multiple technologies such as SCCM / Configuration Manager, Intune, Azure, Security etc. I created this site so that I can share valuable information with everyone.

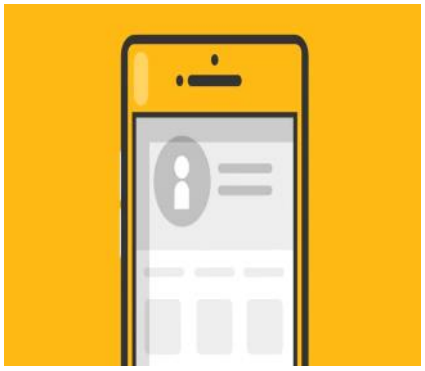
RELATED ARTICLES

Fix CNAME Validation Error in Intune Portal (MEM admin center)

January 24, 2021

How to setup create Microsoft Intune Account

November 15, 2017



Deploying Android Applications using Microsoft Intune

January 16, 2017

4 Comments

Gio Trevis says:

February 11, 2021 at 3:01 pm

Hi Prajwal,
nice article!!!
What happens if a DEM reaches 1000 enrolled devices? Should I fire him?

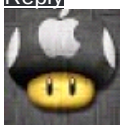
Reply

MikeG says:

November 22, 2017 at 12:58 am

Each DEM enrolled device consumes a single license.

Reply

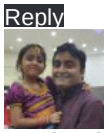


groovemaster17 says:

August 10, 2017 at 6:50 am

How does this affect licensing. The documentation clearly states that DEM can enroll up to 1000 devices. Is this all done with the same, single Intune license?

Reply



Prajwal Desai says:

August 10, 2017 at 1:06 pm

I think so.

From <https://www.prajwaldesai.com/adding-microsoft-intune-device-enrollment-manager/>

How to setup create Microsoft Intune Account

Prajwal DesaiNovember 15, 2017
0 1 minute read

image description

In this post we will see how to setup create Microsoft Intune account. This is one of the posts of Microsoft Intune step by step guide. In the previous post, we saw the Microsoft Intune overview and its features. You can start with a 30 day free trial or start with a paid subscription for Microsoft Intune. Getting started with a paid subscription of Intune shares many of the same steps as starting with a free 30-day trial. In this post we will start with setting up a free Microsoft Intune 30-day trial to manage our mobile devices and computers. The process is very quick and easy. With just a few simple steps in the trial, you can add up to 100 users and devices, set up groups, configure compliance policies, and enroll and manage mobile devices and computers.

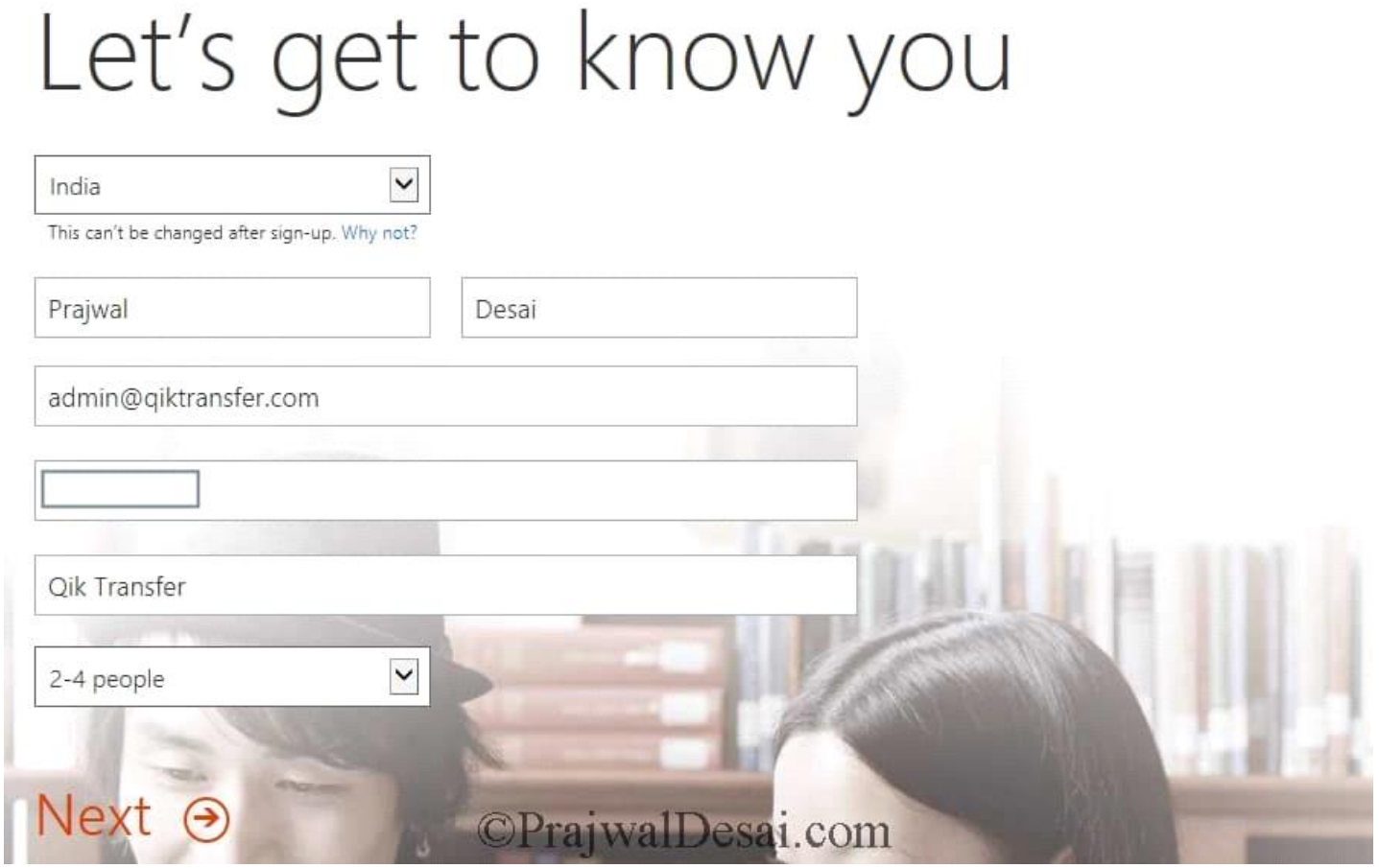
Before you either sign up or sign in to Intune, you should check the following :-

a) Check whether your organization already has a Microsoft Online Services work or school account.

b) Check whether you have an Enterprise Agreement or equivalent volume licensing agreement with Microsoft.

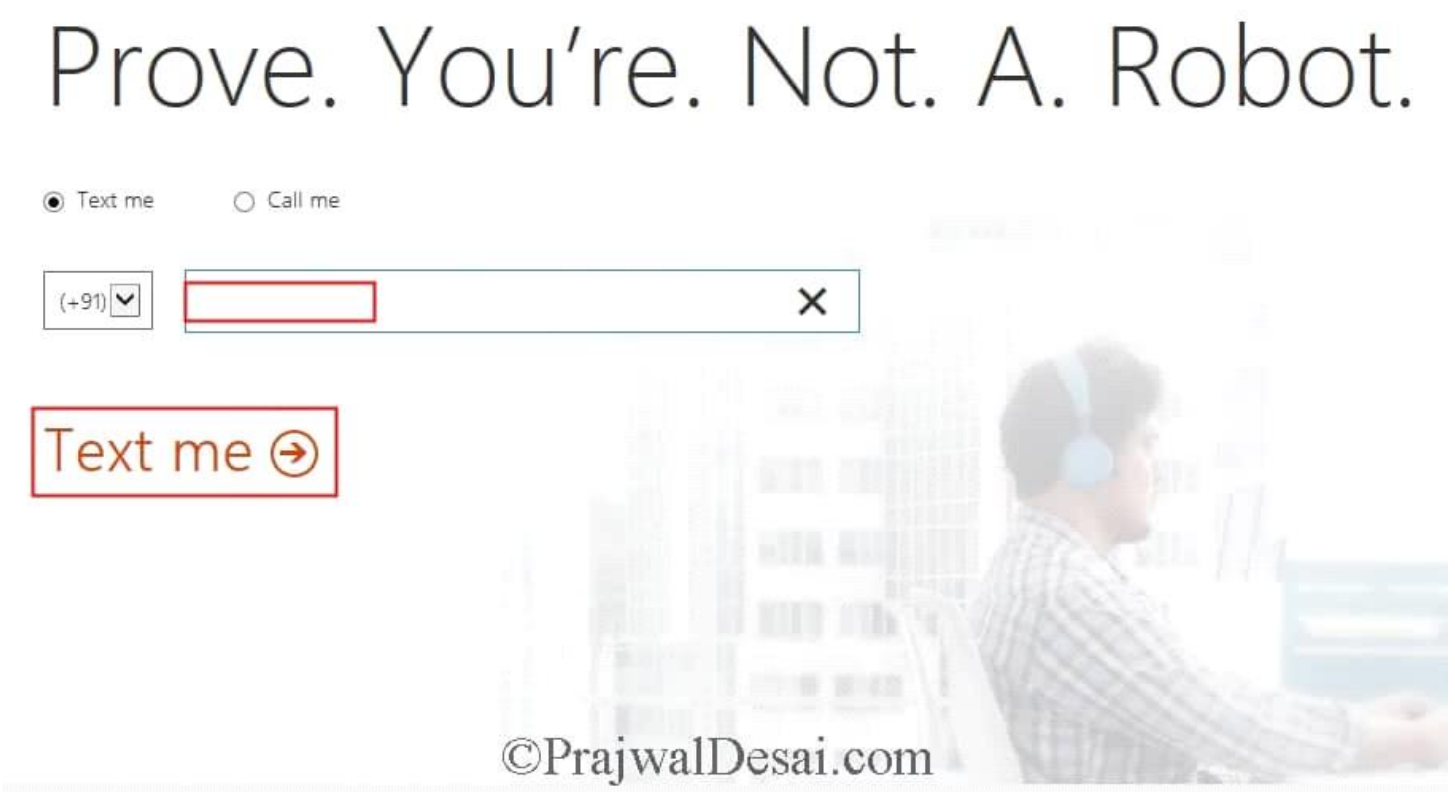
How to setup create Microsoft Intune Account

To create Microsoft Intune account, click here. When you open the link in the browser, click on Try Now. This will open the sign up form in another tab. Fill up the form by providing the required details and click Next.

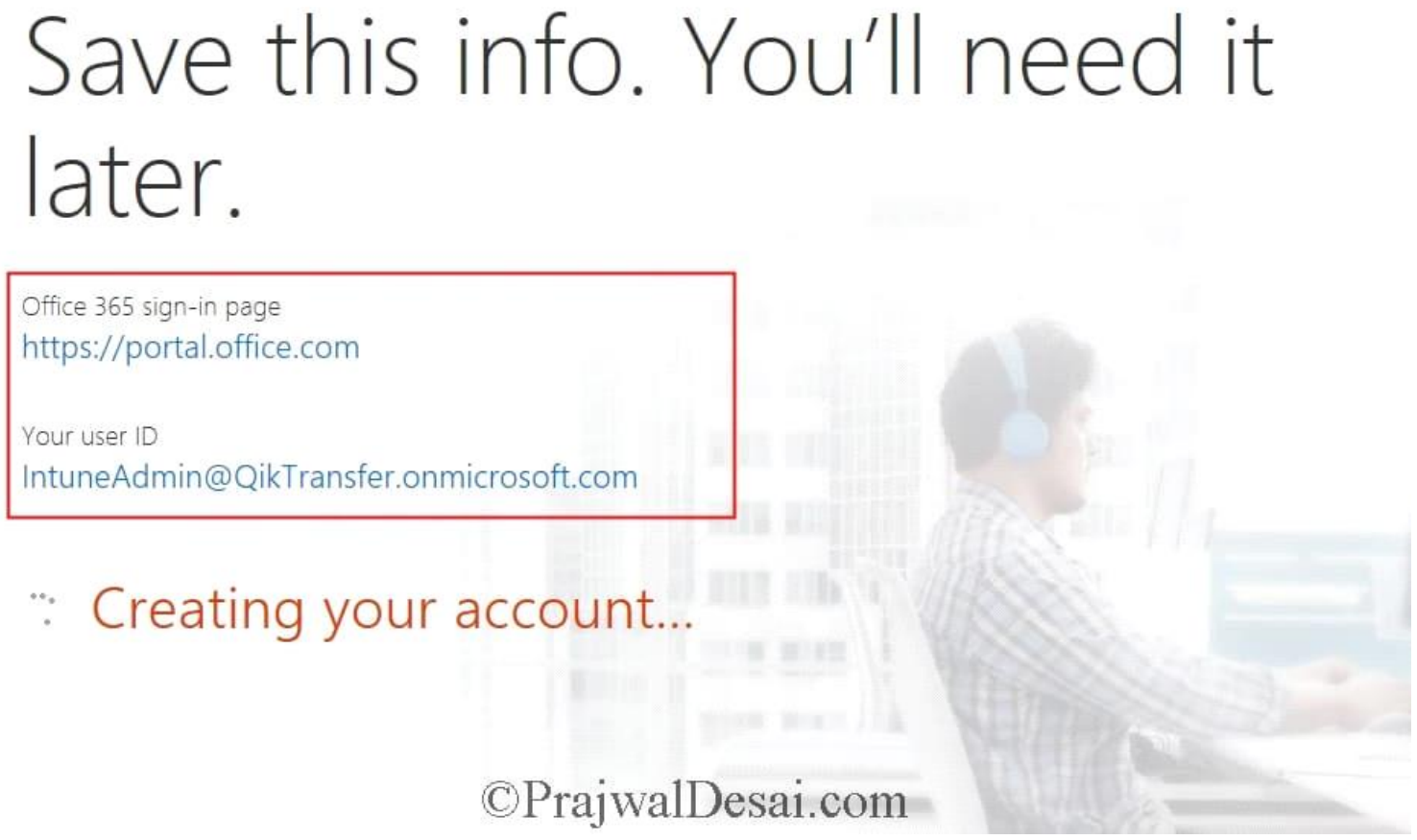


Next, create your user ID. Enter the user name, organization name and password. You login ID will be your name.organization.onmicrosoft.com. You'll use this ID to log in to the Intune portal to do your admin tasks.

In the next step, provide your mobile number and click Text me to validate your number.



Now that's your user ID. Save the information shown on the screen.



Once the account is created you can login with the user ID and the password. You can now evaluate Intune's features and capabilities.

Intune SCCM 1511

Prajwal Desai

Hi, I am Prajwal Desai. For last few years I have been working on multiple technologies such as SCCM / Configuration Manager, Intune, Azure, Security etc. I created this site so that I can share valuable information with everyone.

From <https://www.prajwaldesai.com/how-to-setup-create-microsoft-intune-account/>

Intune overview and its features

19 February, 2021 9:41 AM

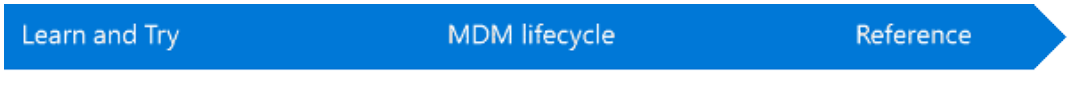
Microsoft Intune overview and its features

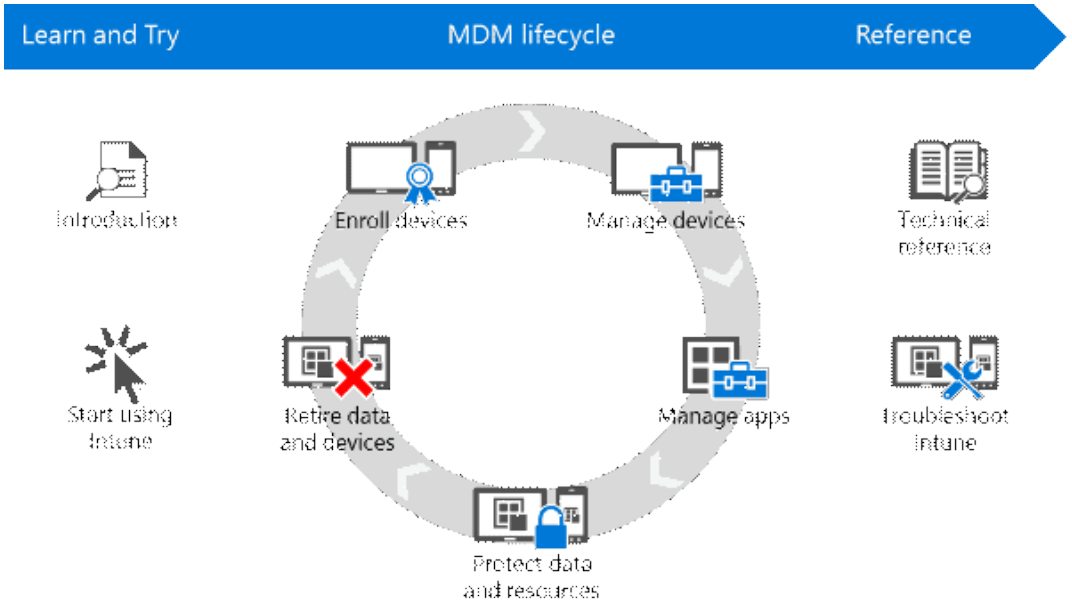
Prajwal DesaiNovember 15, 2017
5 4 minutes read

Share
Facebook Twitter LinkedIn Reddit Share via Email Print

Welcome to the post on Microsoft Intune overview and its features. In this post I will be giving a brief information about what is Microsoft Intune, what are the features of Intune and why is it popular. Microsoft Intune is a cloud-based service that lets you manage mobile devices, PCs, and apps. Using Intune, organizations can provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure. Microsoft Intune solves the network connectivity problem by delivering a reliable and secure service from the Internet, meaning that every user can access it no matter where they are physically located. The good part is Microsoft Intune provides the subscription service with a low cost per user per month. We can start with a single user, then add and remove users as required by our business needs. We can also add MDOP to the subscription to provide additional support options.

Microsoft Intune overview and its features





Pic Source – Technet

What are the benefits of Microsoft Intune

Choice of Device – With Microsoft Intune you can provide employees with the ability to register, enroll, and manage their devices as well as install corporate applications from the self-service Company Portal – all from the devices of their choice.

Management of Office mobile apps – With Microsoft Intune you can increase the Mobile productivity for your employees with access to corporate resources on Office mobile apps they know and love.

Data Protection – Secure corporate data, including Exchange email, Outlook email, and OneDrive for Business documents, based on the enrollment status of the device and the compliance policies set by the administrator.

No need to maintain Infrastructure – Eliminate the need to plan, purchase, and maintain hardware and infrastructure by managing mobile devices from the cloud with Intune.

Integration with Enterprise – Extend your existing System Center Configuration Manager infrastructure through integration with Intune to provide a consistent management experience across devices on-premises and in the cloud.

Flexible Licensing – Spend less time counting devices with per-user licensing for Intune.

Intune is also included as part of the Enterprise Mobility Suite, the most cost-effective way to acquire Intune, Azure Active Directory Premium, and Azure Rights Management.

Excellent Support from MS – Get answers to your questions with Microsoft support available online and by phone worldwide which is included with every Intune subscription.

Microsoft Intune Capabilities – Mobile Device Management

Let's look at some of the capabilities of Microsoft Intune. Intune helps minimize complexity by offering mobile device management through the cloud with integrated data protection and compliance capabilities.

Provide a self-service Company Portal for users to enroll their own devices and install corporate applications across the most popular mobile platforms.

Deploy certificates, WiFi, VPN, and email profiles automatically once a device is enrolled, enabling users to access corporate resources with the appropriate security configurations.

Deliver comprehensive settings management for mobile devices, enabling the execution of remote actions such as passcode reset, device lock, data encryption, and full wipe to protect corporate data on lost or stolen devices.

Protect corporate data by restricting access to Exchange email, Outlook email, and OneDrive for Business documents when a user tries to access resources on an unenrolled or non-compliant device based upon policies set by the administrator

Simplify enrollment of corporate devices with bulk enrollment using Apple Configurator or a single service account, enabling IT administrators to set policies and deploy applications on a large scale.

Streamline the enrollment of iOS devices purchased directly from Apple or an authorized reseller with the Device Enrollment Program (DEP).

Enable the enforcement of more strict “lock down” policies for Supervised iOS devices, Android devices using Kiosk Mode, and Windows Phone devices using Assigned Access

Microsoft Intune Capabilities – PC Management

As the number of device types allowed in corporate environments grows, management becomes more challenging. Intune provides a comprehensive management solution through a single administrative console that allows you to manage across a variety of devices, including PCs and laptops.

Integrate your existing System Center 2012 Configuration Manager infrastructure with Intune, further enhancing your ability to manage PCs, Macs, and Unix/Linux servers, as well as mobile devices from a single management console, while building on existing investments and skills.

Provide real-time protection against malware threats on managed computers, keep malware definitions up-to date, and automatically scan computers to help protect against malware infections and other potentially unwanted software.

Collect information about hardware configurations and software installed on managed computers, allowing you to generate reports, organize groups of computers, and more effectively target software deployments.

Simplify administration by deploying software and configuring Windows Firewall settings on computers based upon policies defined by the administrator.

Ways to manage your devices with Microsoft Intune

You have several options for using Intune. You can go with any of these options based on your requirements.

Intune as standalone – You can use Intune as a standalone solution for device management. As a cloud-based service, you manage devices and protect company data without the overhead of network infrastructure costs. Intune can manage iOS, Android, Mac OS X, and Windows Phone devices, as well as Windows RT and Windows 8.1 and Windows 10 devices as mobile devices.

Intune as an extension of Microsoft System Center 2012 Configuration Manager – If you already use Configuration Manager to manage on-premises devices and are looking for a way to manage many of today's mobile devices, you can use Intune as an extension of System Center 2012 Configuration Manager. Two key benefits of this option are a unified management experience for both on-premises and mobile device management, and scale. This hybrid implementation of Intune gives you the capacity to manage more than 50,000 devices.

Intune with Office 365 – If you have a commercial subscription to Office 365, you can use the Intune mobile device management capabilities built into Office 365. While this option is not as extensive as Intune standalone or Intune and Configuration Manager, you can still manage iOS, Android, and Windows Phone devices, create security policies, limit access to Office 365 email and documents on managed devices, and use selective wipe to remove Office 365 from managed devices.

Intune as part of the Microsoft Enterprise Mobility Suite – Intune is a core component of the Microsoft Enterprise Mobility Suite (EMS), a set of cloud-based services that provide threat detection, identity management on top of the data protection and device management that Intune standalone delivers.

Intune

Prajwal Desai

Hi, I am Prajwal Desai. For last few years I have been working on multiple technologies such as SCCM / Configuration Manager, Intune, Azure, Security etc. I created this site so that I can share valuable information with everyone.

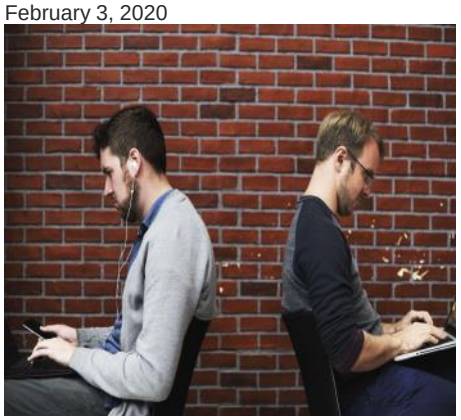
RELATED ARTICLES

[Easy Guide to Enable Tenant Attach in ConfigMgr | SCCM]

January 12, 2021

[Configure Delivery Optimization with Microsoft Intune via OMA-URI]

February 3, 2020



[Add Microsoft Intune subscription in Configuration Manager]

August 31, 2019

5 Comments

Simon Sharpesays:
June 5, 2020 at 1:20 am

Hi,
Great site.
I'm new to Intune, I'm configuring Intune to manage Android 9 Devices.
The main purpose is to deliver an application delivered to us by a Vendor from the appcenter as a line of business app.
All devices are compliant and policy compliant, both only add password requirements.
Blocking unknown apps is not configured.

If I look at the users, show all expected apps as required.
But my Line of business app doesn't appear in the company portal or install (it is configured to appear in company portal)
Many thanks
Simon
Reply

Sunil Shivannasays:
April 8, 2019 at 11:24 am
Hi Prajwal,
Could you please share me the features and main Compare between SCCM and Intune.
Thanks,
SM
Reply

Sachin Psays:
December 8, 2018 at 7:31 pm
Hi Prajwal ,
I would like to know more about intune and Azure, Do you know any good Training Center in Bangalore.
Reply

Prajwal Desaisays:
December 14, 2018 at 11:15 am
Have you tried to learn from MVA – https://www.microsoft.com/en-us/learning/azure-training.aspx
Reply

Bhavanishankersays:
January 8, 2018 at 3:14 pm
Hi Prajwal ,
I would like to know more about intune and Azure, Do i share some details where coaching is good for those technologies. Also it would be helpful if any documents related to the same are shared.

From <https://www.prajwaldesai.com/microsoft-intune-overview-and-its-features/>

SCCM Intune Videos

19 February, 2021 9:47 AM

[Microsoft Intune for SCCM Admins - Are you an SCCM Admin looking to learn Microsoft Intune #MSIntune]

Creating Exceptions Policies in the Endpoint Protection Manager
book

Article ID: 151461
calendar_today

Updated On: 29-08-2017

Products

Endpoint Protection

Issue/Introduction

A file, folder, file extension or application needs to be excluded from being scanned by one or more features of the Symantec Endpoint Protection (SEP) client.
Such exclusions can be configured for managed SEP clients using Centralized Exceptions policies in the Symantec Endpoint Protection Manager (SEPM) console.

Resolution

Exceptions policies contain exceptions for the following types of scans for Windows-based operating systems:

- Auto Protect (Extension Exception)
- Scheduled and on-demand (Extension Exception)
- All Scans (Extension Exception)
- Application Control (File Exception)
- Security Risk (File Exception)
- SONAR (File Exception)

Follow the instructions below to make the type of exception required:

Creating exceptions for Windows Platform

- Log into the SEPM and click **Policies**.
- Under View **Policies** click **Exceptions**.
- Under Tasks click Add a **Exception policy**. This will create and open a new **Exceptions Policy**.
- In the left pane, click **Exceptions**.
- Click the **Add** button to open a drop-down menu. Move the cursor over **Windows Exceptions** to open a second drop-down menu.
- Select one of the 9 available options: Application, Application to Monitor, Extension, File, Folder, Known Risks, Trusted Web Domains, Tamper Protection Exception, DNS or Host File Change Exception.

Creating exceptions for Mac Platform

- Log into the SEPM and click **Policies**.
- Under View **Policies** click **Exceptions**.
- Under Tasks click Add a **Exception policy**. This will create and open a new **Exceptions Policy**.
- In the left pane, click **Exceptions**.
- Click the **Add** button to open a drop-down menu. Move the cursor over **Mac Exceptions** to open a second drop-down menu.
- Click **Security RiskException for Files or Folder**.
- Select required prefix Variable and under File or folder enter the path. (For Mac Subfolders are included by default)

Creating exceptions for Linux Platform

- Log into the SEPM and click **Policies**.
- Under View **Policies** click **Exceptions**.
- Under Tasks click Add a **Exception policy**. This will create and open a new **Exceptions Policy**.
- In the left pane, click **Exceptions**.

- Click the **Add** button to open a drop-down menu. Move the cursor over **Linux Exceptions** to open a second drop-down menu.
- Select either **Folder** or **Extensions.**

Note: Wildcard variables such as * and ? are not required for Known Risks, File, or Folder exceptions for Window. As for file level exception you need to specify the complete path of the file and for Folder level exception you need to specify the folder path and when "Include Subfolder" is checked it will exclude every single file and folders inside the parent folder. The ? wildcard is supported for Extension exceptions. The * wildcard is supported for Trusted Web domains exceptions.

Note: For File and Folder-based exclusions, the Full Path to the file must be specified, unless a "Prefix Variable" is selected. If a "Prefix Variable" is selected, the path specified should be relative to the selected "Prefix Variable"

Note: If you are unsure about what type of exception to make please see the chapter entitled "**Managing Exceptions**" in the pdf "**Installation and Administration Guide**".

1. Enter the appropriate information for the item to be excluded. For Extensions, File, and Folder exclusions, specify the type of scans that will be excluded from the drop down menu or menus.
2. (Optional) Repeat steps 6 through 8 to add any other Security Risk Exceptions to the policy.
3. Click OK.
4. Assign the policy to a group within the SEPM.

References
Managing exceptions in Symantec Endpoint Protection, which is HOWTO80869
Installation and Administration Guide's DOC page DOC9449

From <https://knowledge.broadcom.com/external/article?legacyId=TECH104326>

15 April, 2021 11:24 AM

#1 Guide to Setup SCCM Cloud Management Gateway (SCCM CMG) – Easy and Detailed

Prajwal DesaiMarch 22, 2021
65 12 minutes read

Share
Facebook Twitter LinkedIn Reddit Share via Email Print

In this post I will cover the steps to setup SCCM cloud management gateway (SCCM CMG). we will configure SCCM CMG in the Configuration Manager 1902 setup.

Setting up the SCCM cloud management gateway is very easy. If you are using earlier versions of SCCM such as SCCM 1802 or SCCM 1806 you might not see some options that are included in SCCM 1902.

Contents

- Specify Unique SCCM CMG DNS Name
- Configure Azure Services for Cloud Management
- Verify Configuration Manager Azure Service
- Create and Issue Web Server SCCM CMG Certificate Template
- Import Web Server CMG certificate on the Primary Site Server
- Export CMG Web Server Certificate
- Setup SCCM Cloud Management Gateway (SCCM CMG)
- Cloud Management Gateway Status
- Install Cloud Management Gateway Connection Point
- Allow SCCM Cloud Management Gateway Traffic
- Allow access to cloud distribution points
- Associate SCCM CMG with Boundary groups
- Configure Clients for CMG
- Enable Remote Desktop on SCCM CMG (Cloud Management Gateway)
- Cloud Management Gateway Log Files for Troubleshooting
- SCCM CMG (Cloud Management Gateway) FAQ
- What is SCCM CMG ?
- PowerShell command to setup CMG ?
- Can a Primary site have multiple instances of the CMG ?

What is SCCM Cloud Management Gateway

The SCCM cloud management gateway also known as SCCM CMG, that provides a simple way to manage Configuration Manager clients on the internet. When you deploy the SCCM CMG as a cloud service in Microsoft Azure, you can manage internet clients without additional infrastructure.

The biggest advantage or benefits of SCCM cloud management gateway is you don't need to expose your on-premises infrastructure to the internet. If you are planning to use CMG, I would suggest you to read this article by Microsoft.

The SCCM CMG uses Azure Cloud Services as PaaS, this service uses virtual machines (VMs) that will involve compute costs. By default the CMG uses a Standard A2 V2 VM.

When you setup SCCM cloud management gateway, you select how many VM instances support the CMG. By default it 1 and 16 is the maximum.

SCCM CMG High Level Steps

- Setup SCCM CMG Server Authentication Certificate
- Setup SCCM CMG trusted root certificate to clients
- Setup Client trusted root certificate to SCCM CMG
- Configure HTTPS certs for Management Points
- Configure Azure management certificate

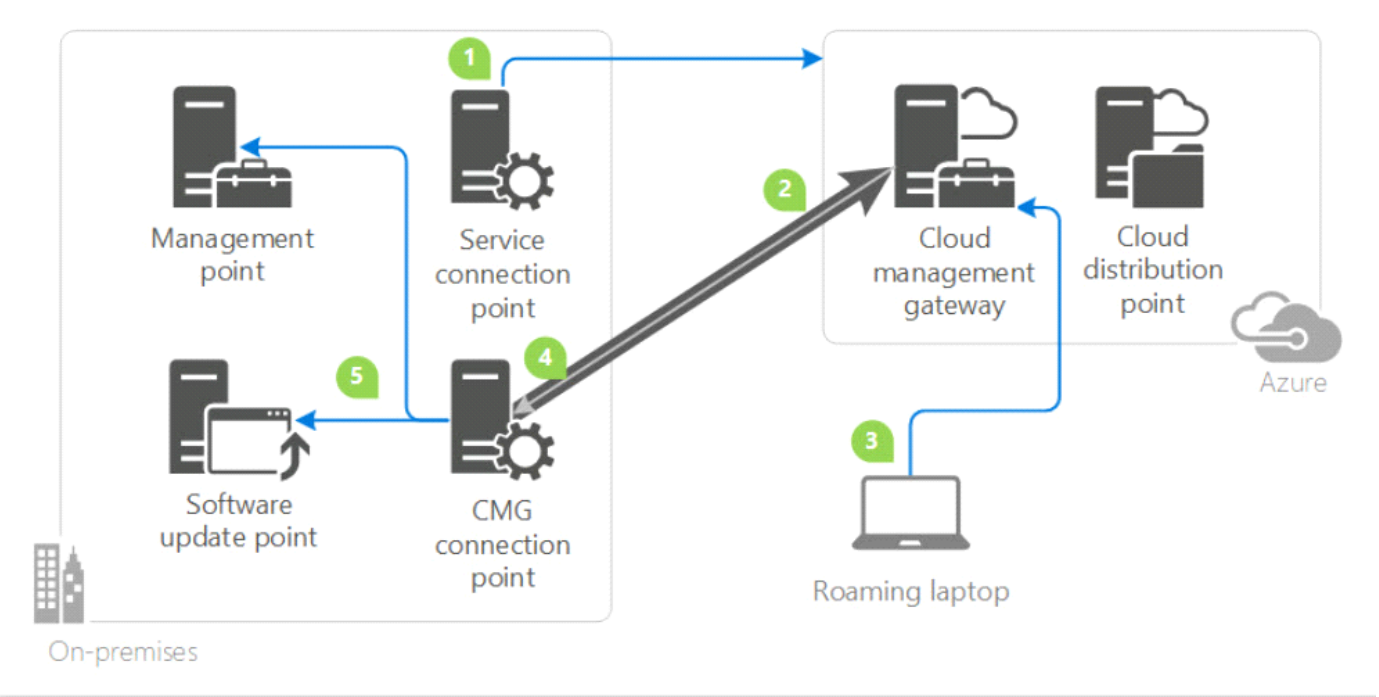
- Specify Unique SCCM CMG DNS Name
- Configure Azure Services for Cloud Management
- Verify Configuration Manager Azure Service
- Create and Issue Web Server SCCM CMG Certificate Template
- Import Web Server CMG certificate on the Primary Site Server
- Export CMG Web Server Certificate
- Setup SCCM Cloud Management Gateway (SCCM CMG)
- Install Cloud Management Gateway Connection Point
- Allow SCCM Cloud Management Gateway Traffic and cloud distribution points
- Associate SCCM CMG with Boundary groups
- Configure Clients for CMG

SCCM CMG Ports and Data Flow

When you plan to setup SCCM CMG, you don't need to open any inbound ports to your on-premises network. The service connection point and CMG connection point are the ones that initiate all communication with Azure and the CMG.

The service connection point deploys and monitors the service in Azure, hence it must be in online mode. The SCCM CMG connection point connects to the CMG to manage communication between the SCCM CMG and on-premises site system roles.

For complete information about SCCM cloud management gateway ports, read this article.



Copyright Microsoft – Conceptual data flow for the CMG

SCCM Cloud Management Gateway Requirements / SCCM CMG Prerequisites

Here are the important requirements or prerequisites for SCCM CMG :-

- First of all you need an Azure Subscription to host the cloud management gateway.
- If you are deploying SCCM CMG, you need a Subscription Admin. To integrate the site with Azure AD for deploying the CMG using Azure Resource Manager, you need a Global Admin.
- Ensure the SCCM service connection point is in online mode before setting up SCCM cloud management gateway.
- Integration with Azure AD for deploying the service with Azure Resource Manager.
- If you ask me use at-least SCCM 1806 and above if you are creating a CMG in your setup. I will explain the reason for this in next section.

- You need at-least one on-premises Windows Server to host the SCCM cloud management gateway.

Cost of Configuration Manager Cloud Management Gateway

The CMG comes with a cost because it uses several components in Azure. The cost charges are incurred to your Azure subscription account. The two main costs include the cost of virtual machine that hosts CMG service and the amount of data that you transfer to the CMG. For more information, refer cost of cloud management gateway article.

Certificates for Configuration Manager Cloud Management Gateway

One thing that you must really work on is the CMG certificates. I have not included this info under SCCM CMG prerequisites section because this topic is quite complex. However I will try my best to make it easy for you.

- CMG server authentication certificate
- CMG trusted root certificate to clients
- Server authentication certificate issued by public provider / Enterprise PKI
- Client Authentication Certificate
- Client trusted root certificate to SCCM CMG
- HTTPS certs for Management Points
- Azure Management Certificate

SCCM CMG Server Authentication Certificate

The SCCM CMG server authentication certificate is required while creating the cloud management gateway in the Configuration Manager console. When you setup a CMG, it basically creates a HTTPS service to which your internet clients connect.

For a valid Configuration Manager CMG server auth cert, you can either acquire a certificate from a public provider or issue it from your public key infrastructure (PKI). In this post, I will be issuing the cert from my PKI.

If you are using SCCM 1802 and above, you can use a wildcard certificates as CMG server cert. Before you create this certificate, ensure the Azure domain name that you use is unique.

SCCM CMG trusted root certificate to clients

This certificate is for clients that must trust the CMG server authentication certificate. There are two methods to accomplish this :-

- Use a certificate from a public and globally trusted certificate provider.
- Use a certificate issued by an enterprise CA from your public key infrastructure (PKI).

Client trusted root certificate to SCCM CMG

You supply this root certificate when you setup the cloud management gateway in the Configuration Manager console. The CMG must trust the client authentication certificates. If you're using PKI client authentication certificates, then you must add a trusted root certificate to the CMG.

HTTPS certs for Management Points

To configure HTTPS on Management points requires PKI and this topic is huge. Don't

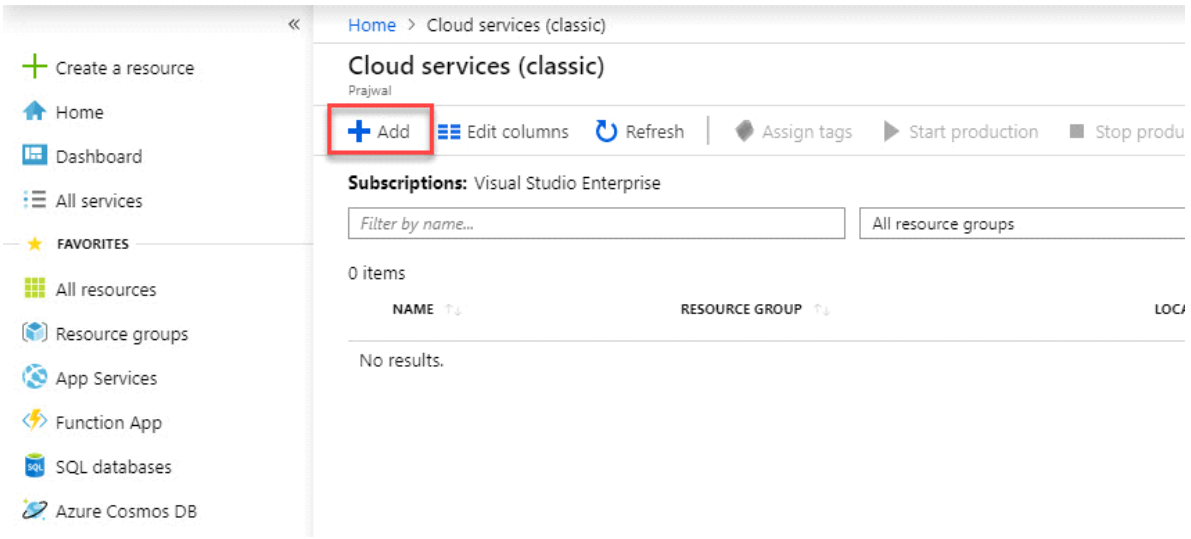
worry, I have covered step-by-step deployment of the PKI certificates for SCCM here.

Azure management certificate

The Azure management certificate is required for classic service deployments. With SCCM 1810 and above the classic service deployments in Azure are deprecated. So start using Azure Resource Manager deployments for the cloud management gateway.

Specify Unique SCCM CMG DNS Name

You must confirm that the Azure domain name you want is unique. You can check this in Azure portal. When you enter the DNS name, you should see either a green tick or red X. Green tick means yes the domain name is available and red X means it is not available.

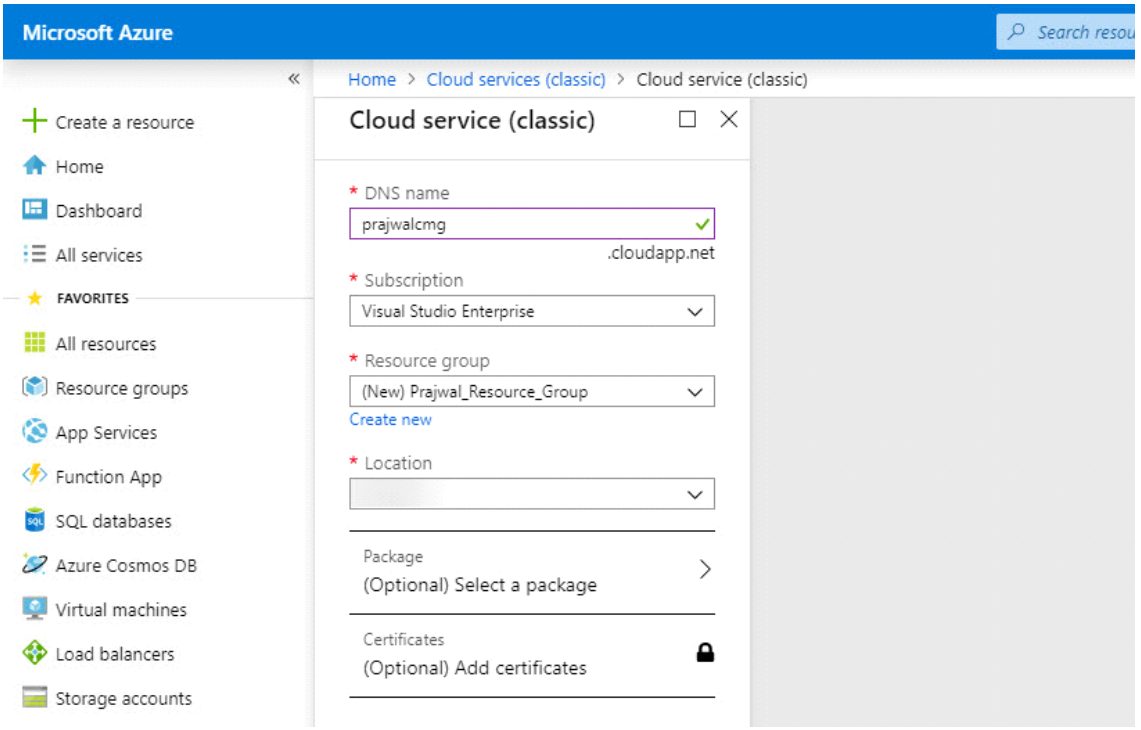


Specify Unique SCCM CMG DNS Name

Login to Azure portal and select Cloud Services (classic). Click +Add button.

Enter the DNS name which should be unique as I mentioned before. In my case I see a green tick so I will be prajwalcmg.cloudapp.net will be my unique Azure domain name or DNS name.

At this post there are two options. You can skip creating this service because it will be created automatically when we setup SCCM CMG. You may also create the service and use it while setting up SCCM CMG.

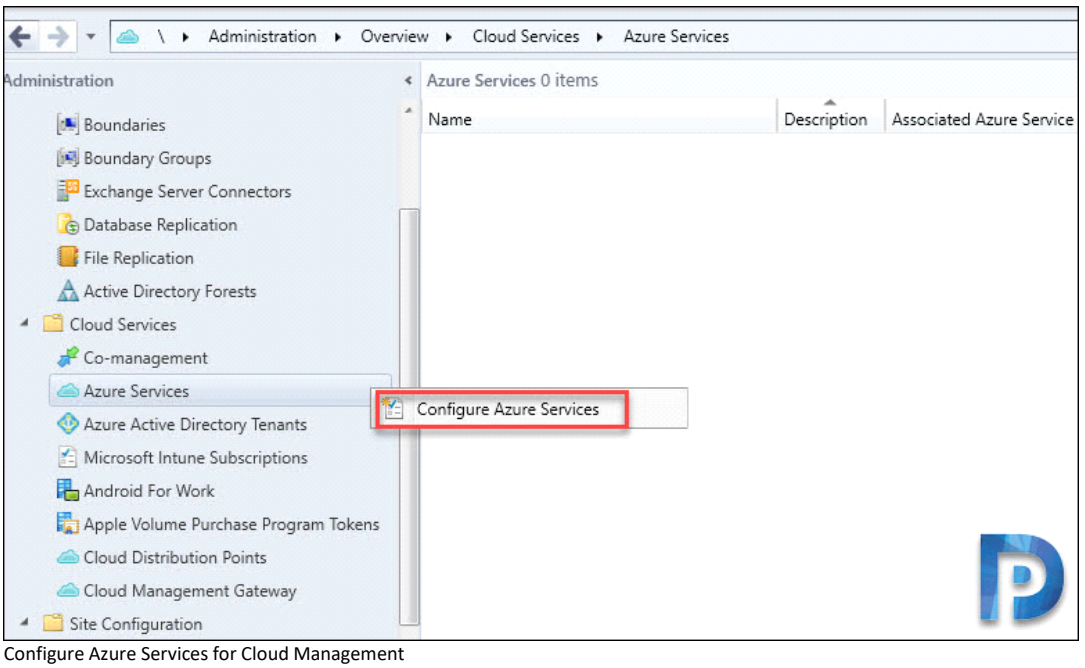


Specify Unique SCCM CMG DNS Name

Configure Azure Services for Cloud Management

We will now configure Azure cloud services that you can use with SCCM using the Azure Services Wizard. We will create web app and native client app that provide subscription and configuration details, and authenticate communications with Azure AD.

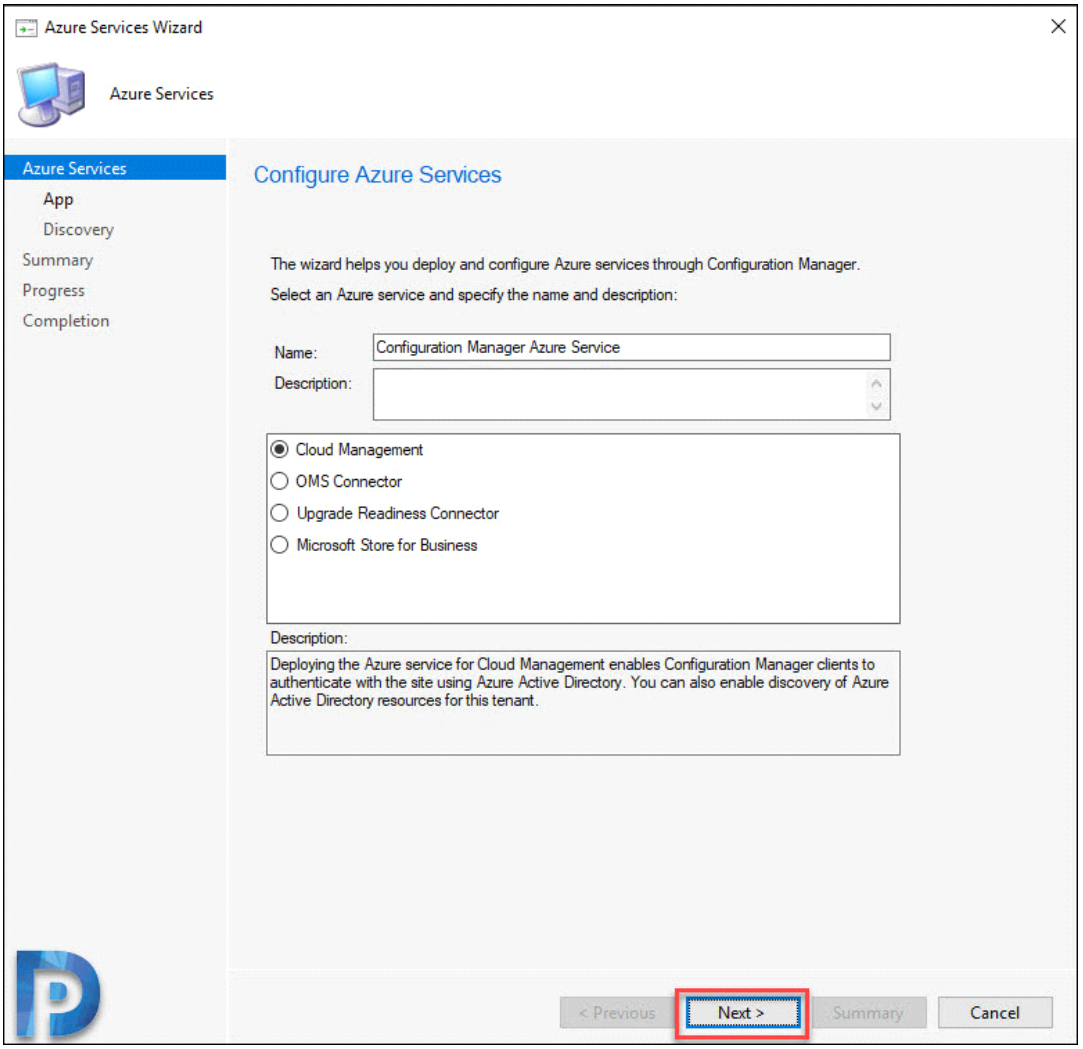
Go to Administration > Overview > Cloud Services > Azure Services. Right click Azure Services and click Configure Azure Services.



Configure Azure Services for Cloud Management

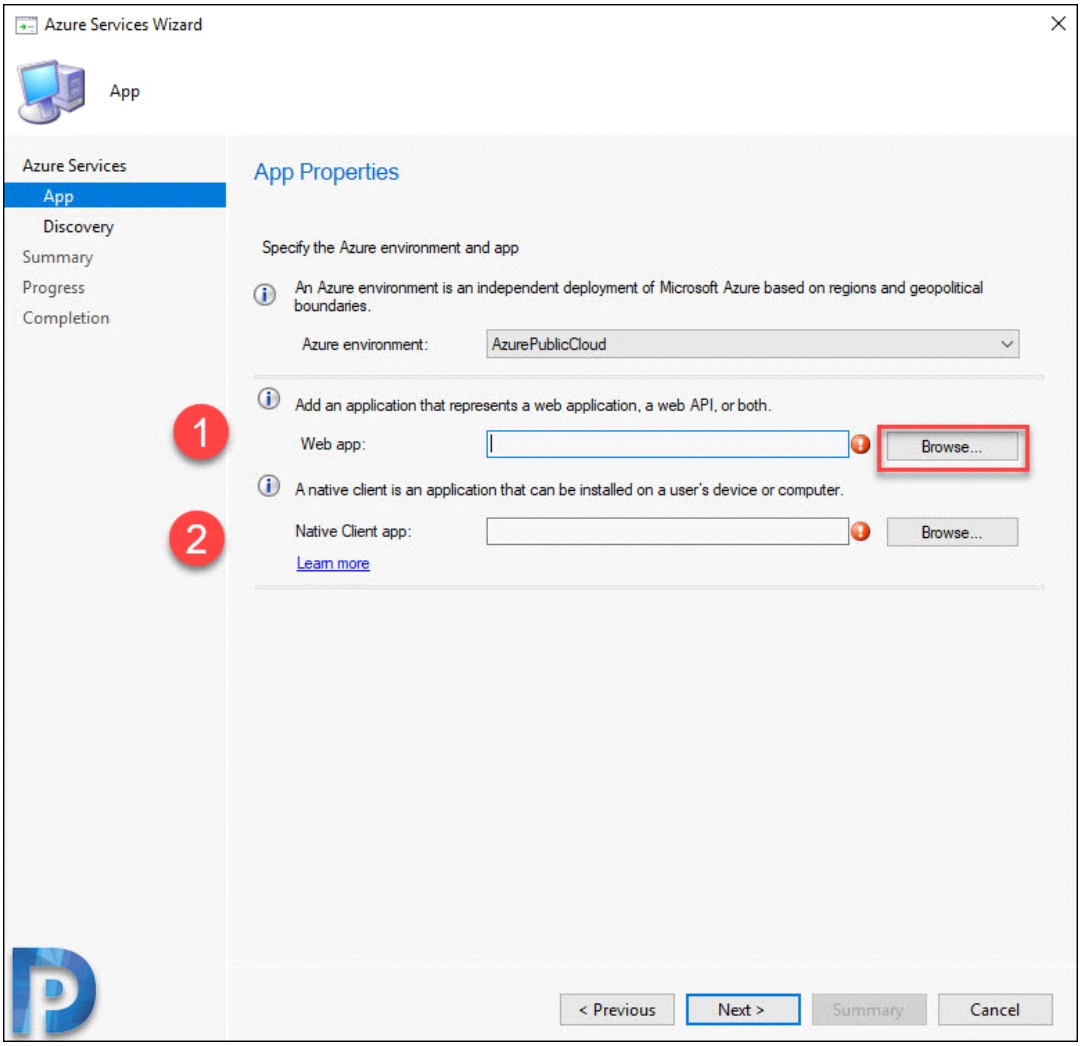
Select the Azure Services as Cloud Management and specify a name and description.

Click Next.



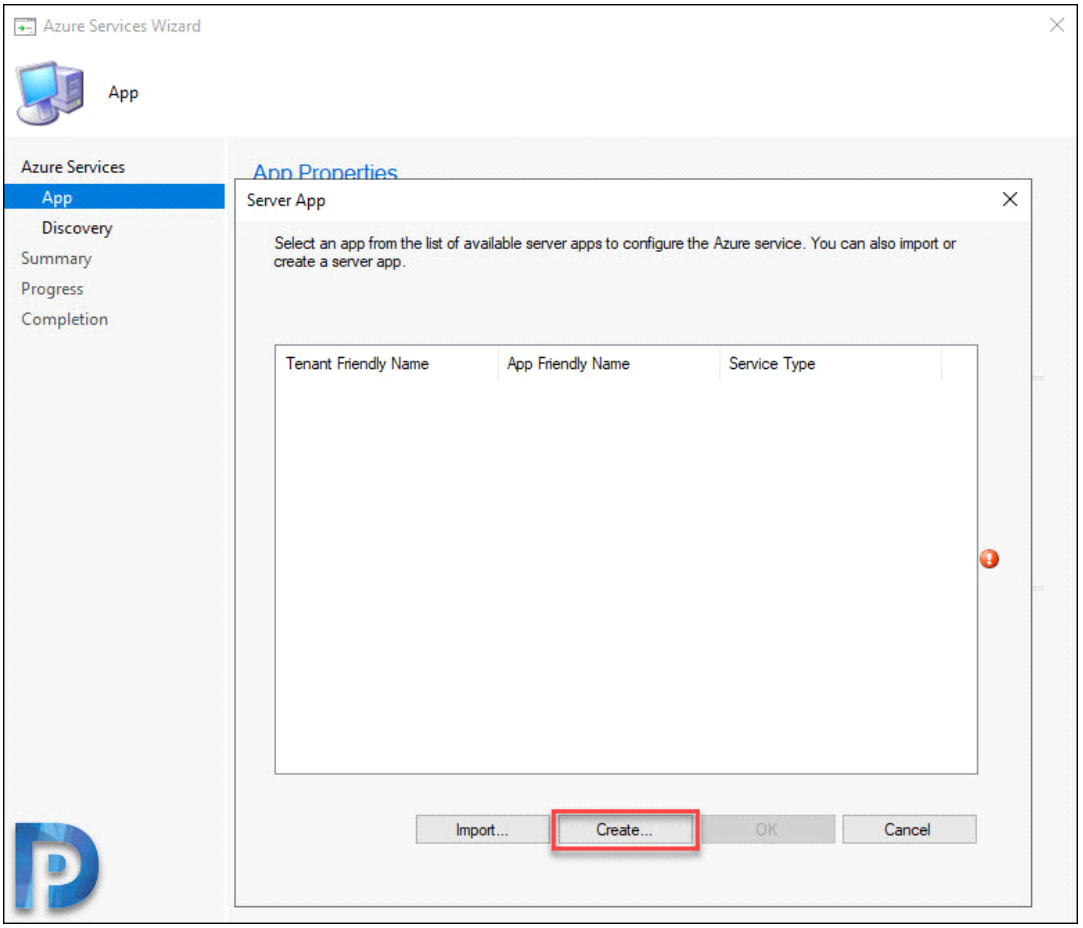
Configure Azure Services for Cloud Management

Select the Azure environment which is AzurePublicCloud. First we will create a web app, click Browse.



Create Web App for server

In the Server App box, click Create.



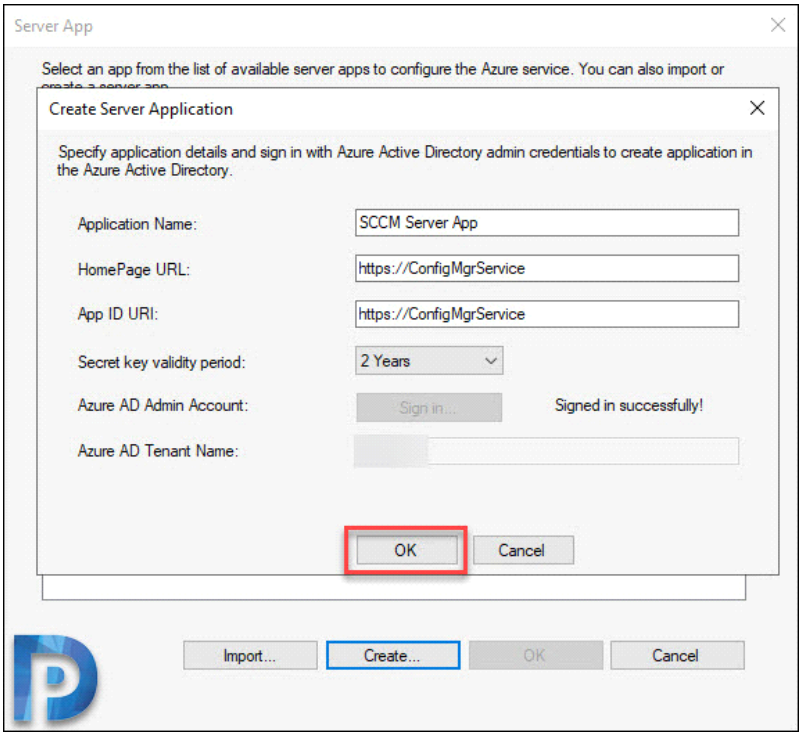
Create Web App for server

In the Create Server Application box, enter the application name. It can be anything.

Specify key validation period and next click Sign-in button.

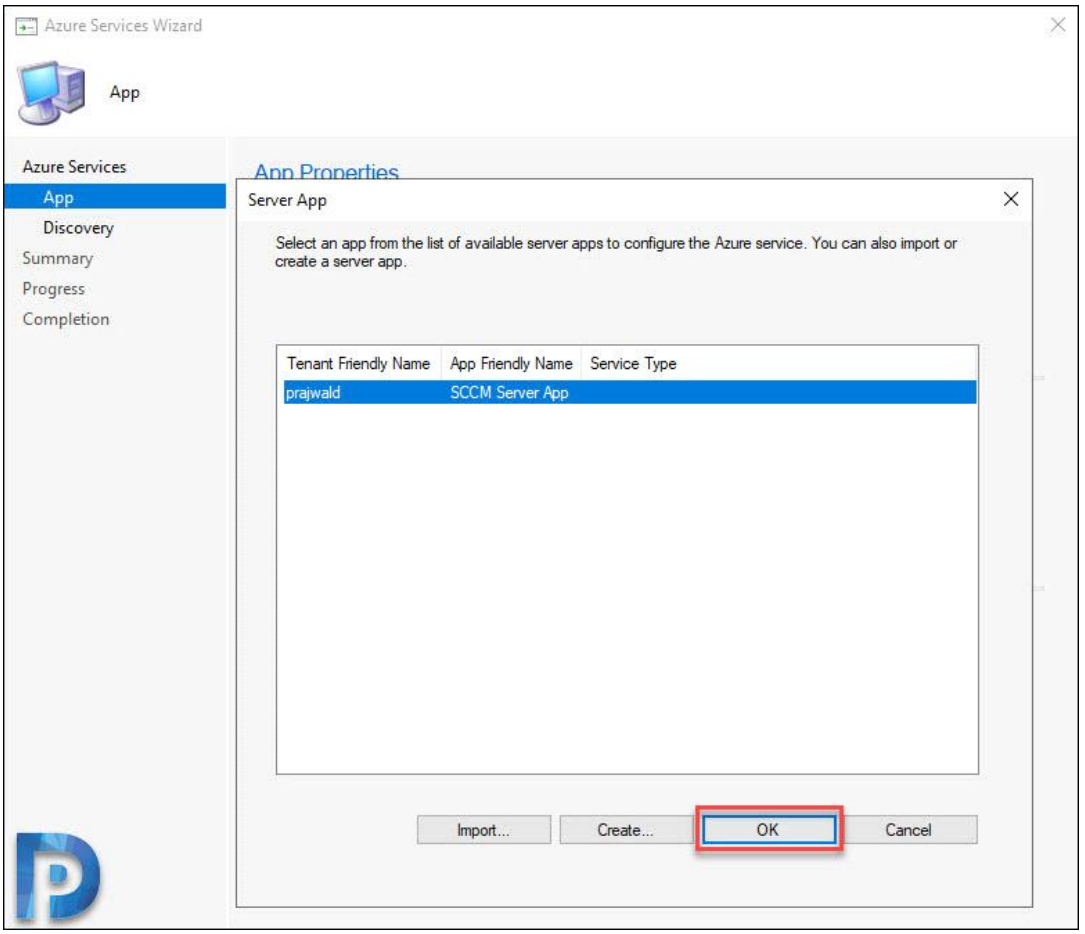
You should now see a box where-in you must sign in. Once you enter the correct credentials, you Azure AD tenant name will be shown along with Signed in successfully message.

Click OK.



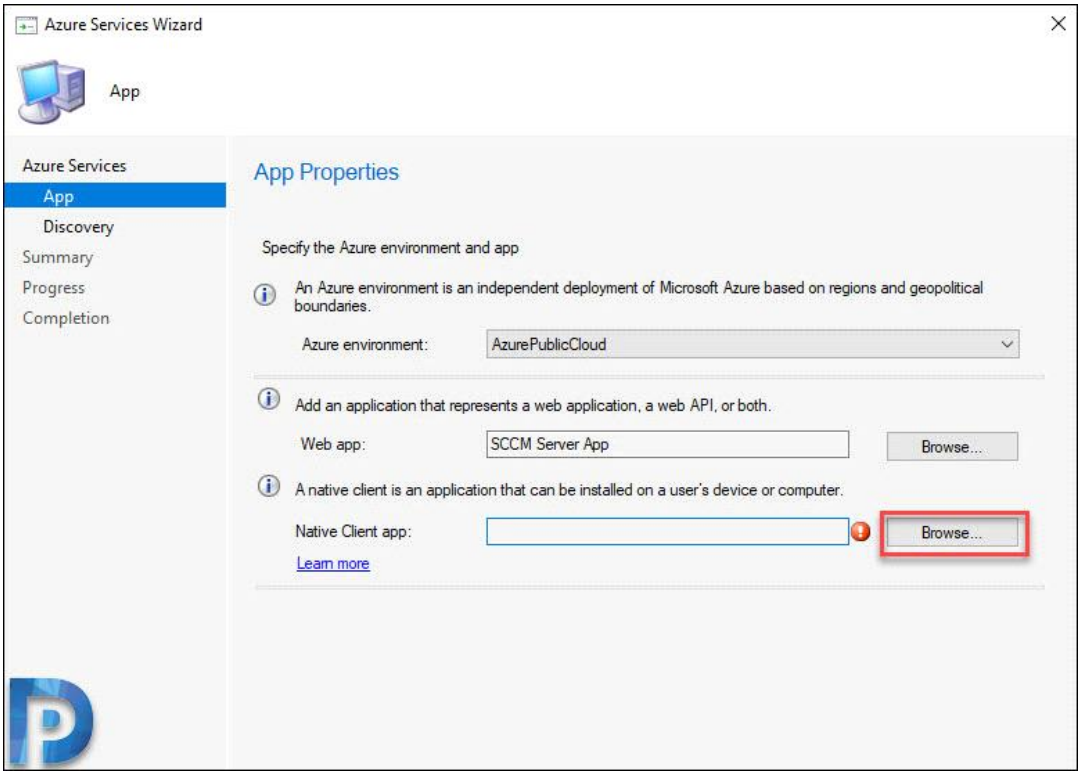
Create Web App for server

Select the server app that you just created and click OK.



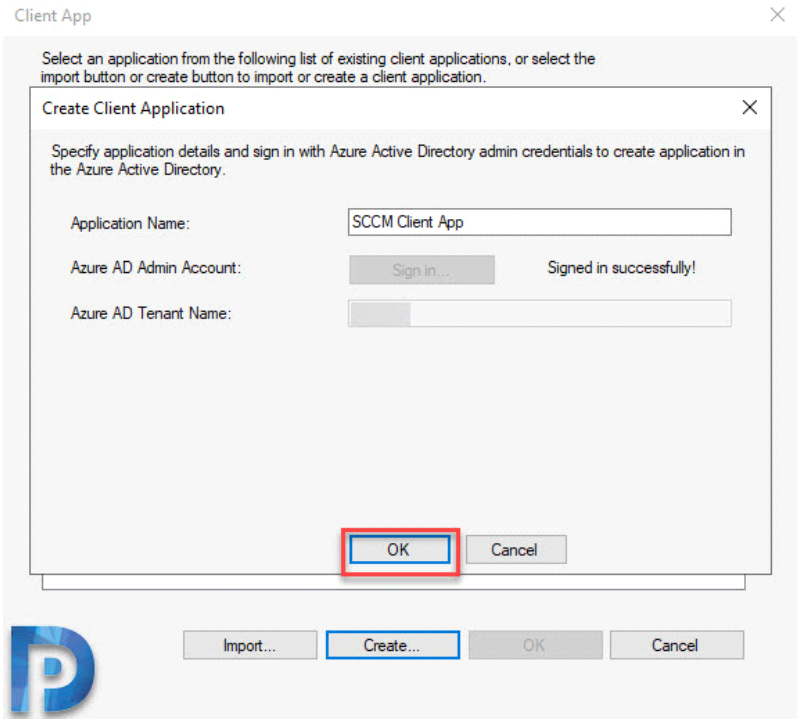
Create Web App for server

We will now create a native client app, so click Browse.



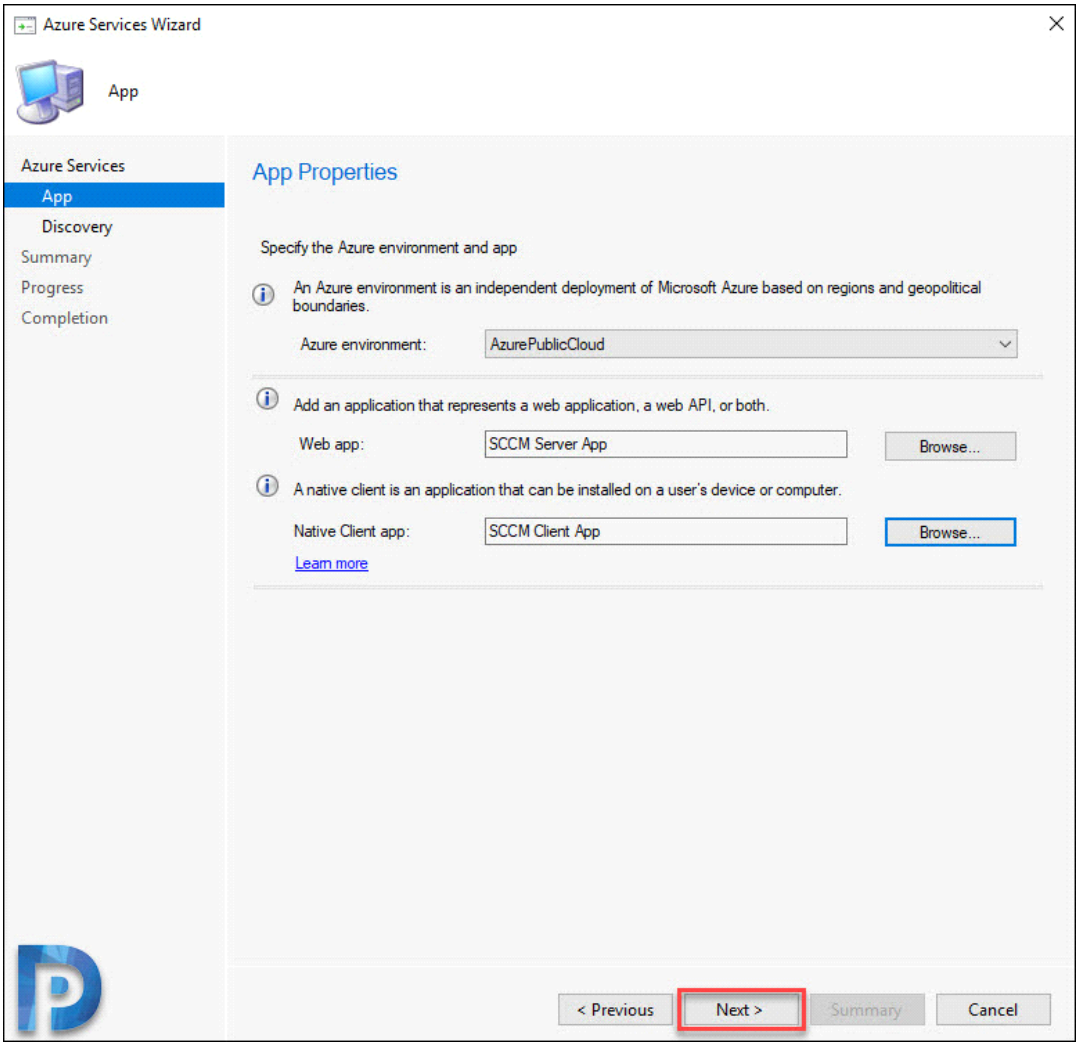
Create Native App for Client

Enter the application name and you must sign-in again. When you do that click OK.



Create Native App for Client

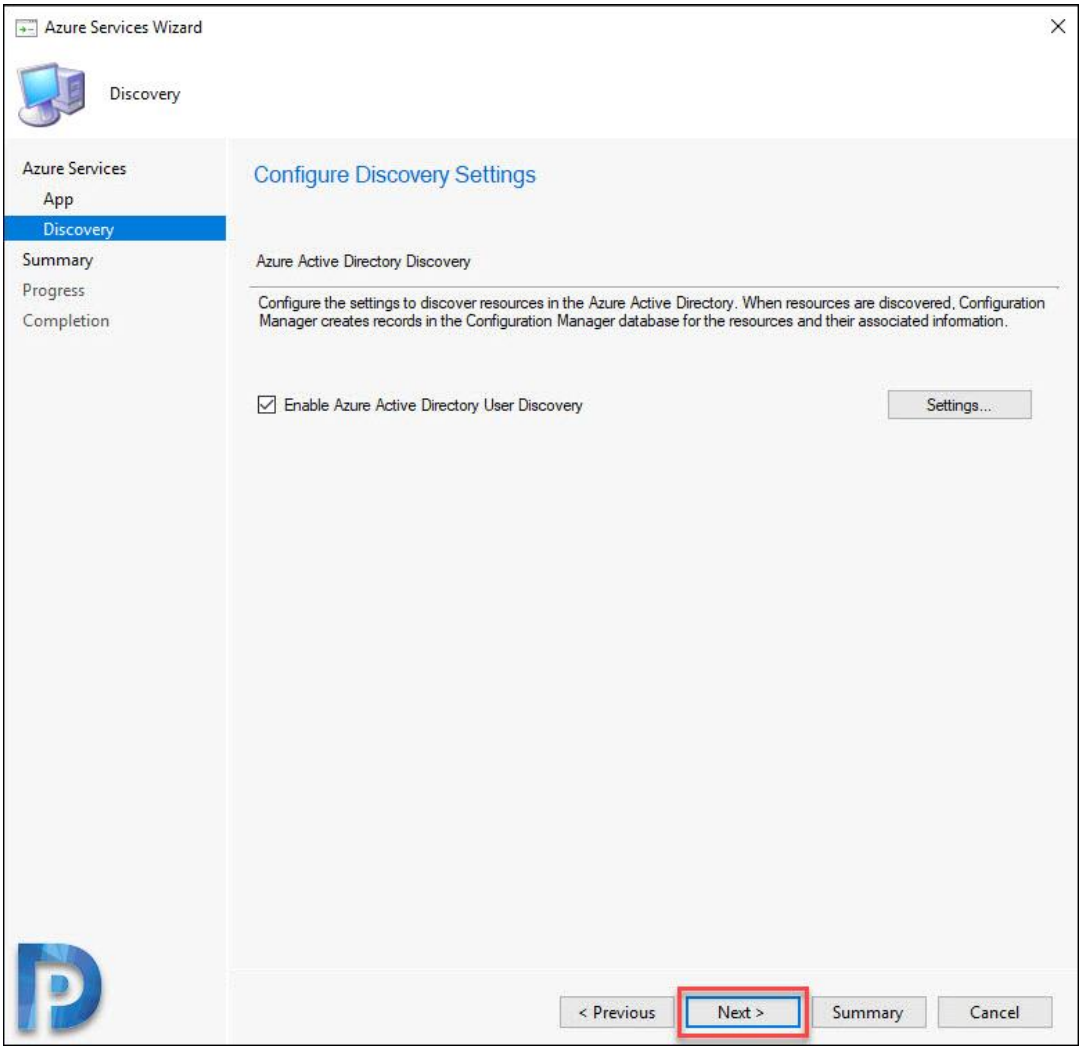
Now we have Server and Client app created. Click Next.



SCCM Azure Service

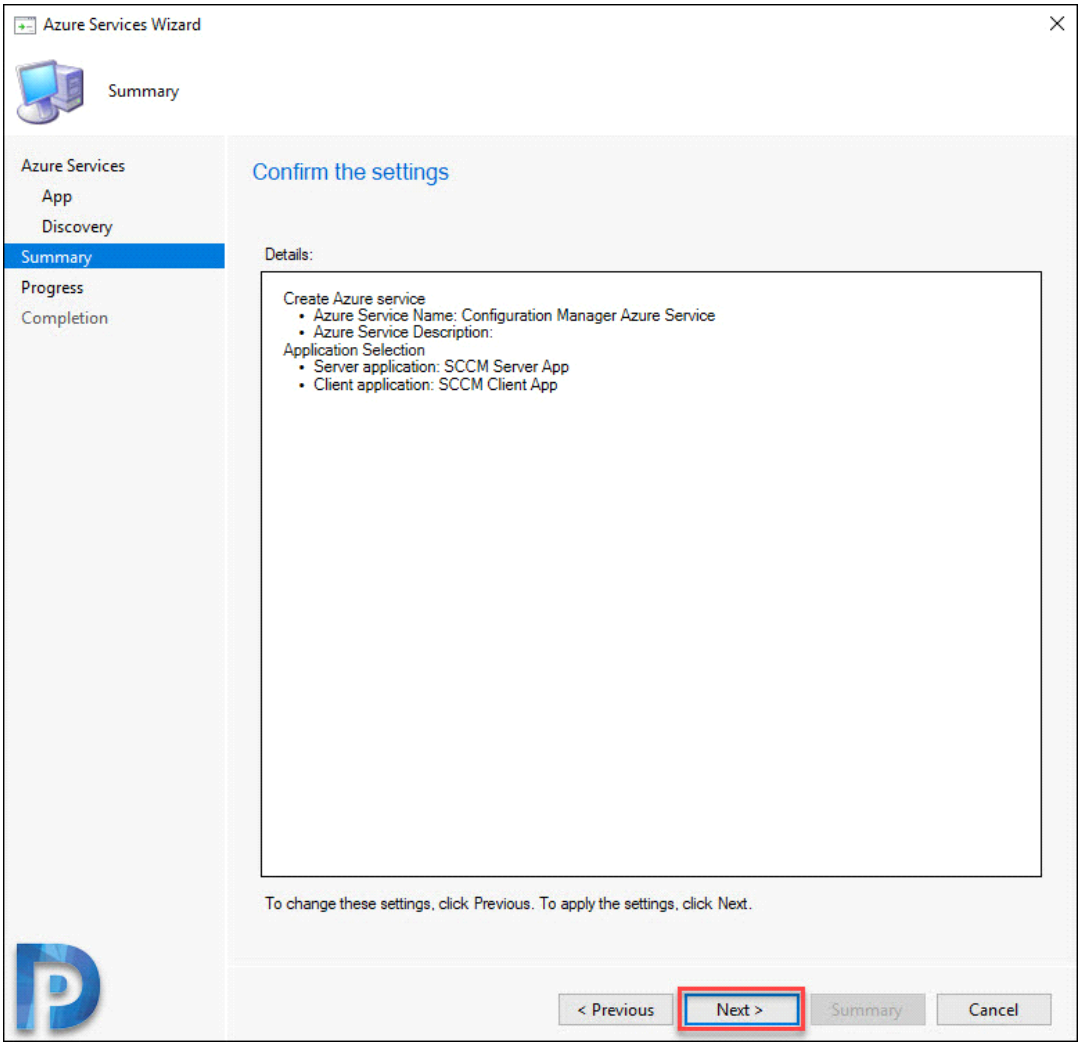
You can leave this option “Enable Azure Active Directory User Discovery” selected.

Click Next.



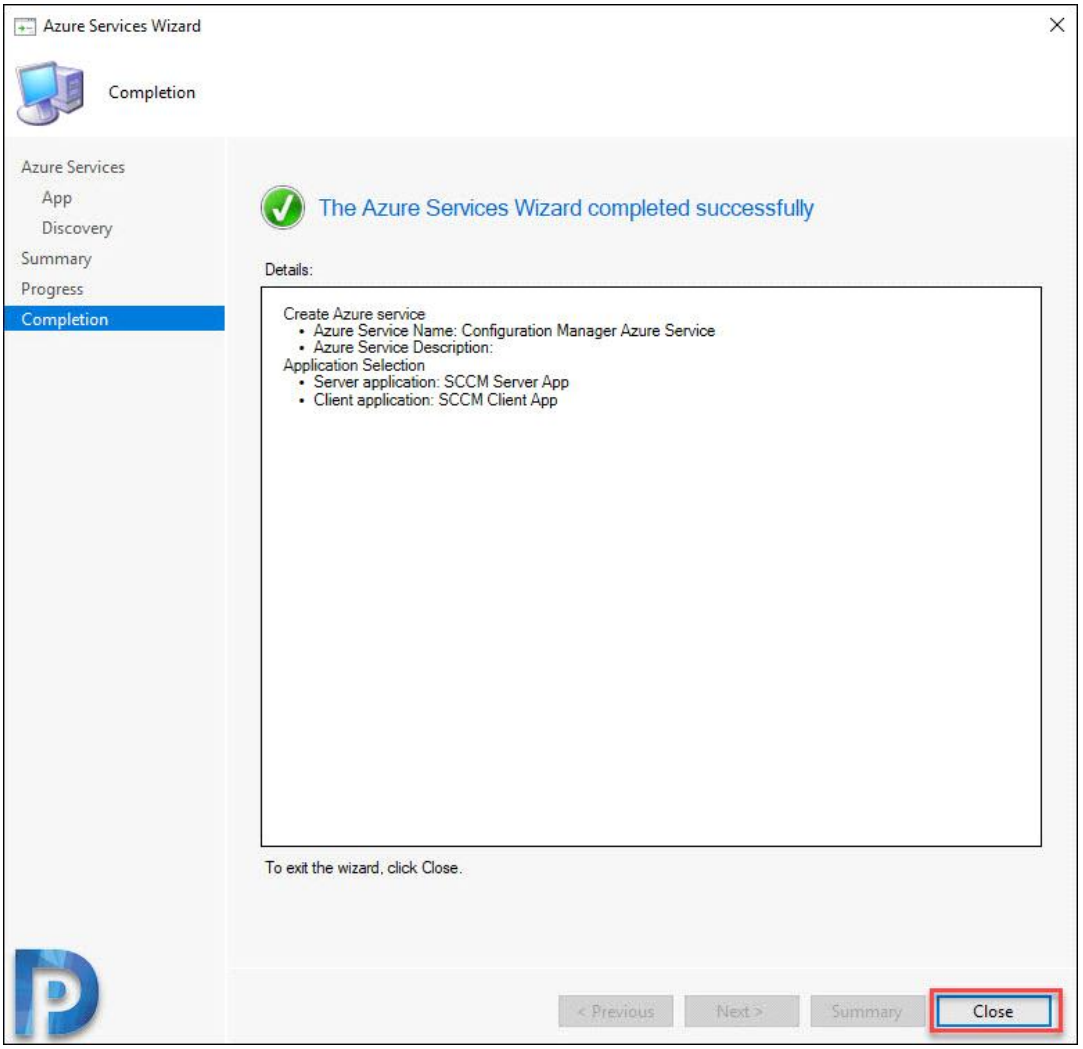
SCCM Azure Service

Click Next on Summary page.



SCCM Azure Service

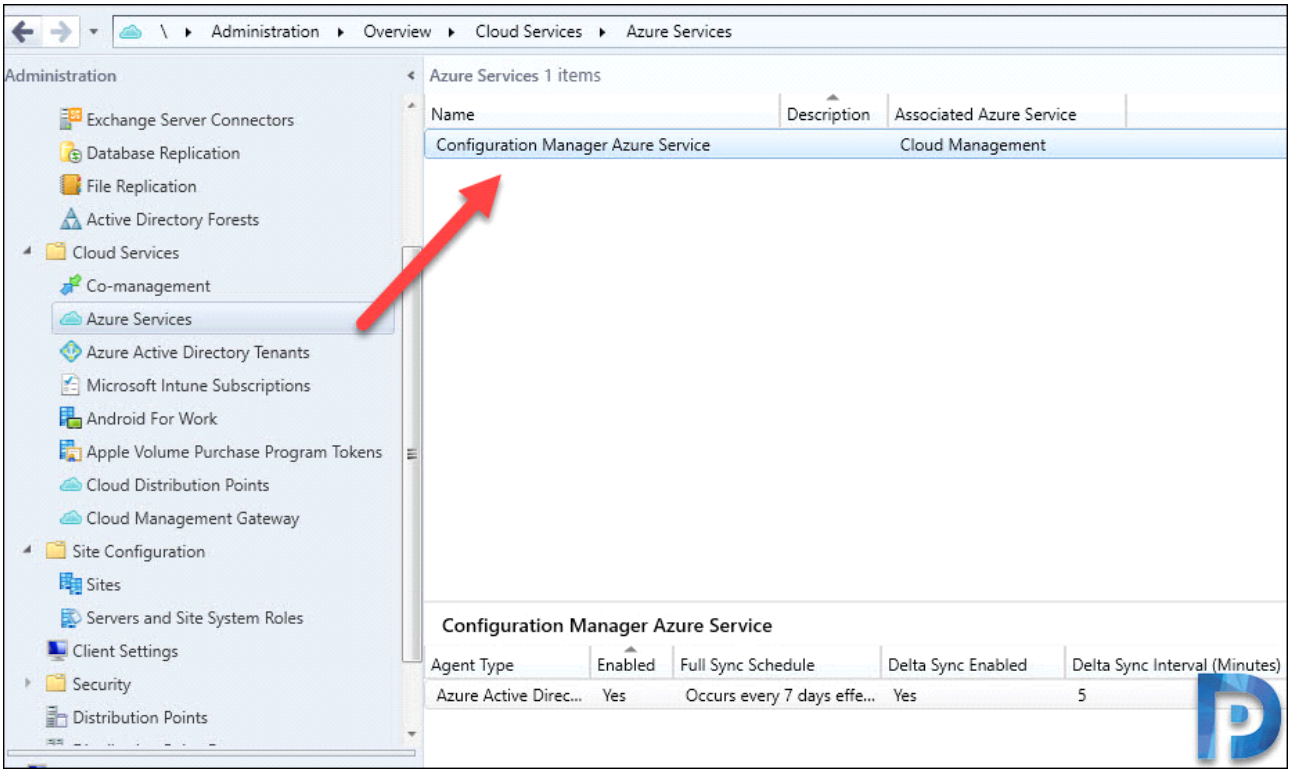
Finally on the Completion window, click Close.



Close Azure Services Wizard

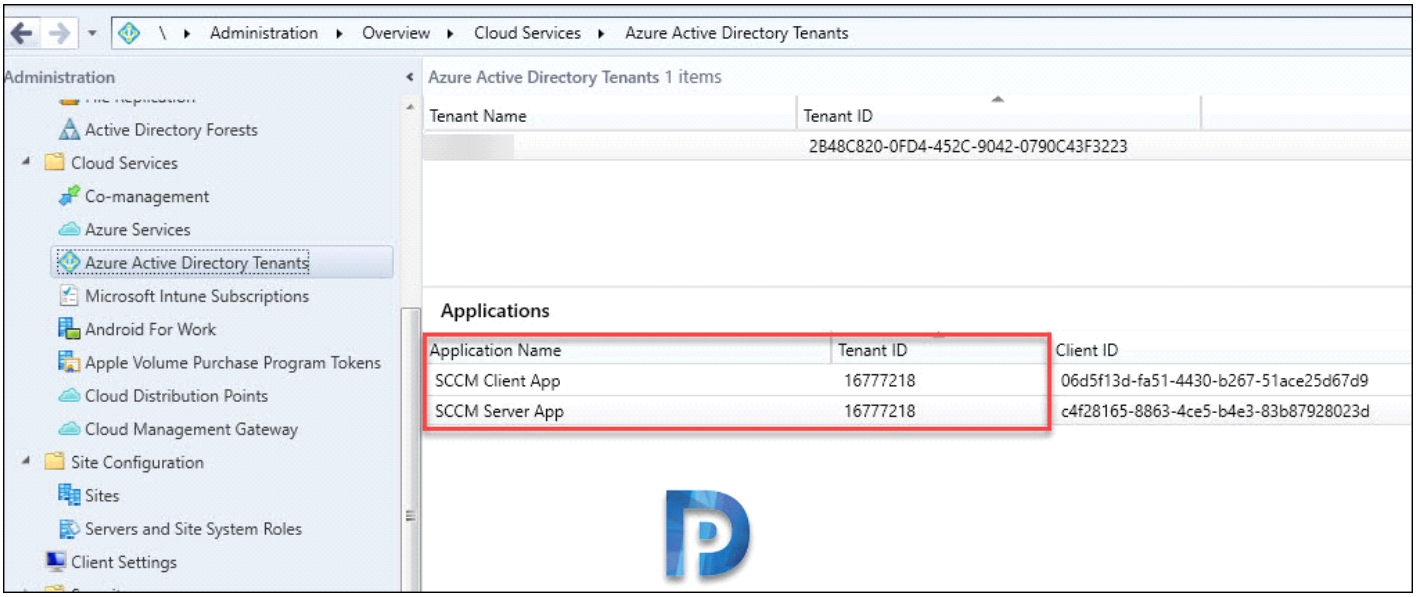
Verify Configuration Manager Azure Service

To verify the Azure Service that you created for Configuration Manager, click Azure Services. On the right pane you should see the Azure service and Associated Azure Service which is Cloud Management.



Configuration Manager Azure Service

If you click Azure Active Directory Tenants, you should see Tenant name and tenant ID. In addition to that, you will see the Application Name, Tenant ID, Client ID in the bottom pane.



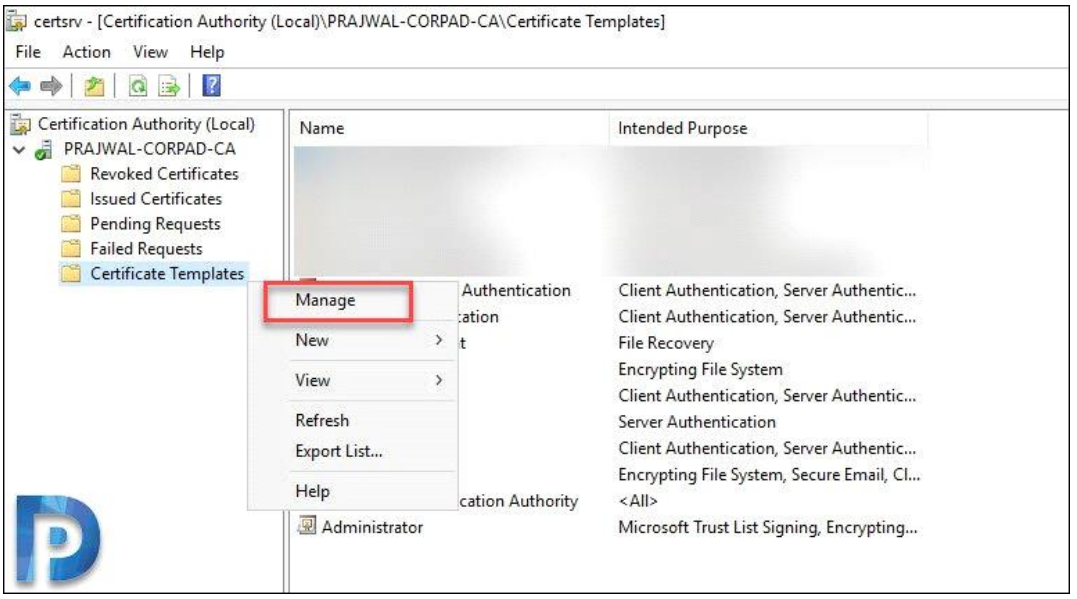
SCCM Client App and SCCM Server App

Create and Issue Web Server SCCM CMG Certificate Template

In this section we will create a new custom certificate which by using the web server certificate template. At this point, if you have templates created during implementing PKI, you can simply duplicate the SCCM IIS Certificate and use it.

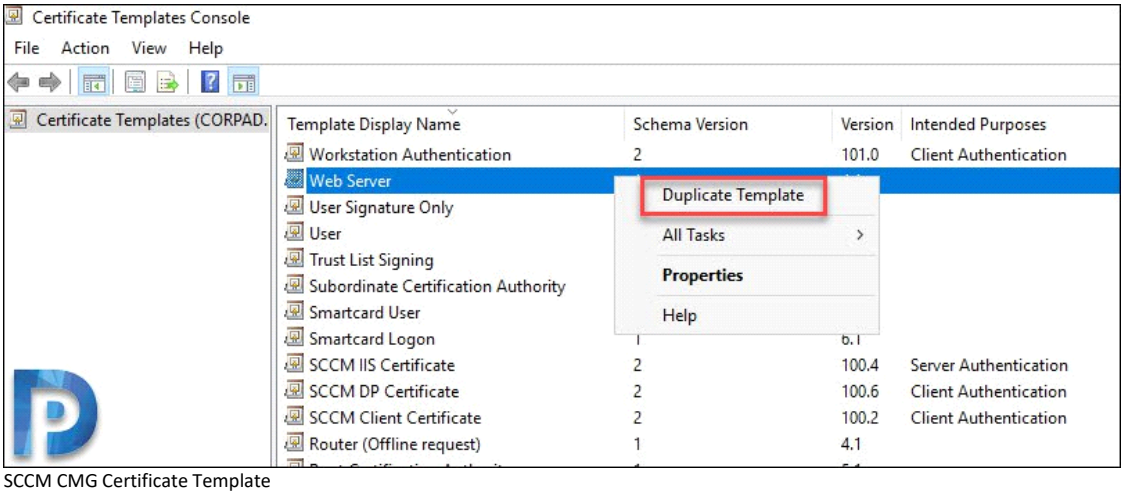
If not you can duplicate the web server template and configure it. This certificate will be used for the installation of the SCCM cloud management gateway.

Login to Certification Authority server, open the Certification Authority console. Right-click Certificate Templates and select Manage.



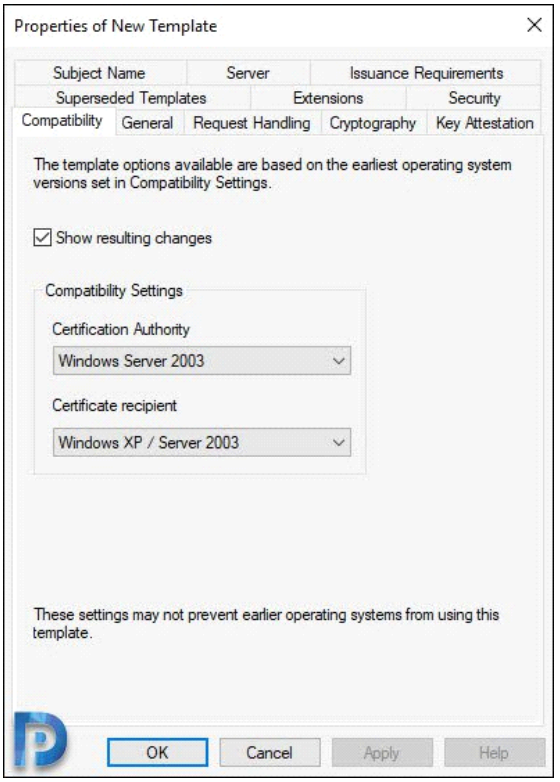
SCCM CMG Certificate Template

Right click Web Server and click Duplicate Template.



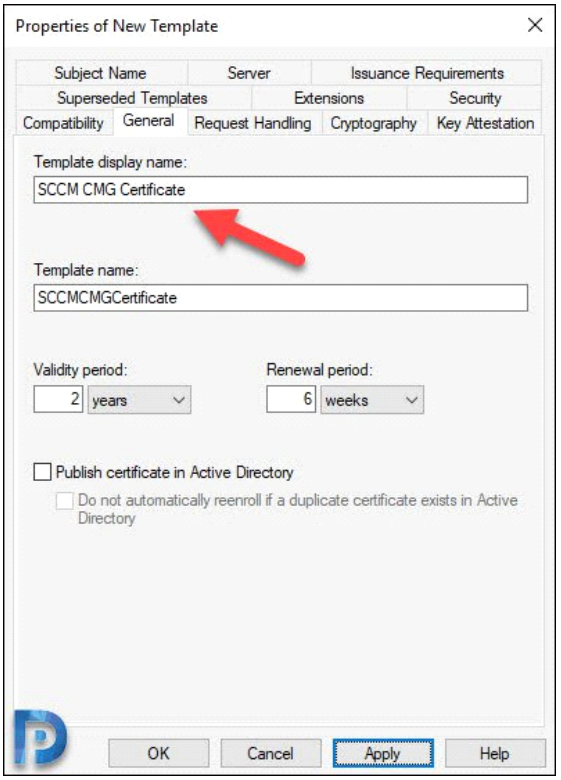
SCCM CMG Certificate Template

Click Compatibility tab and ensure the settings are same as per below screenshot.



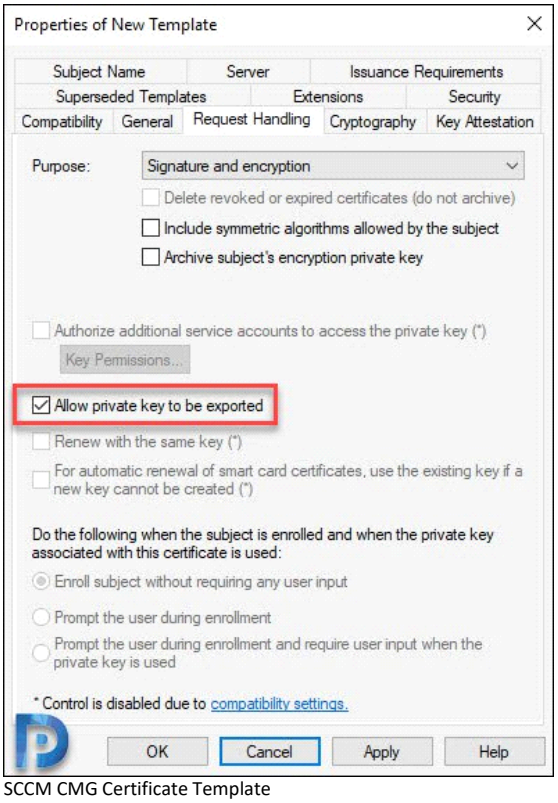
SCCM CMG Certificate Template

Click General tab and specify a name to this temple. I will name it as SCCM CMG Certificate.



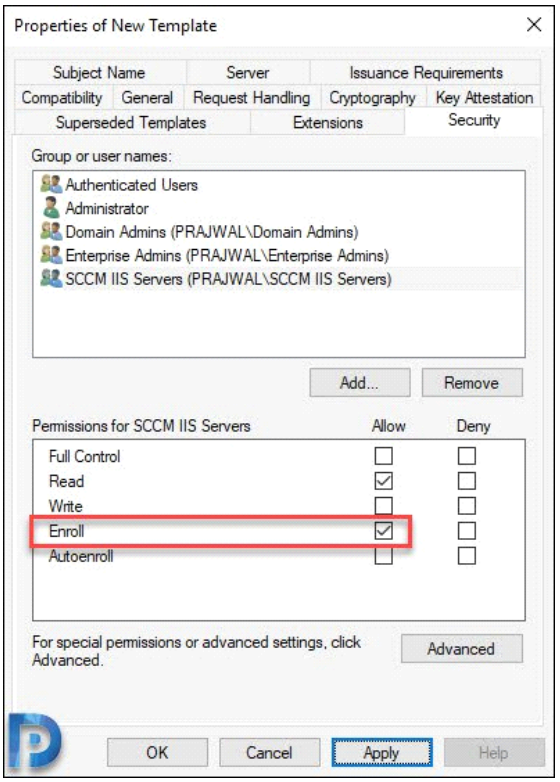
SCCM CMG Certificate Template

Click Request Handling and ensure Allow private key to be exported is checked.



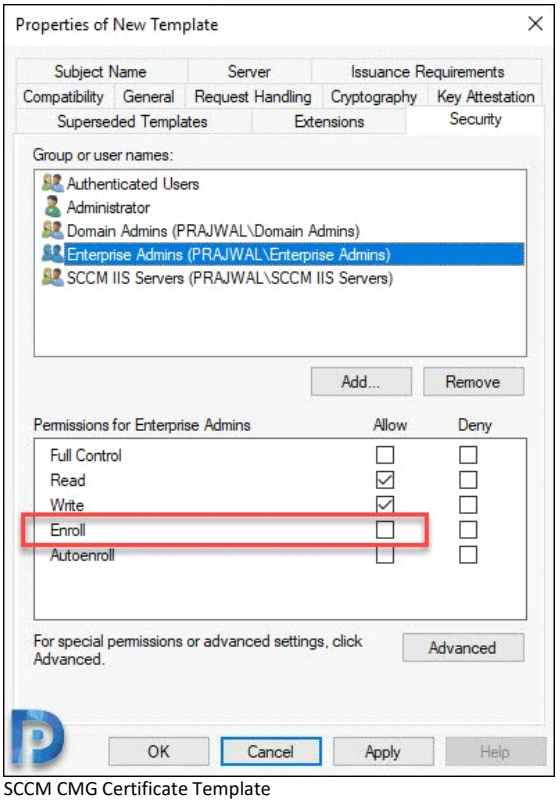
SCCM CMG Certificate Template

Now click Security tab, add the group that contains your SCCM Primary Site server computer account. Select the group and allow Enroll permission.



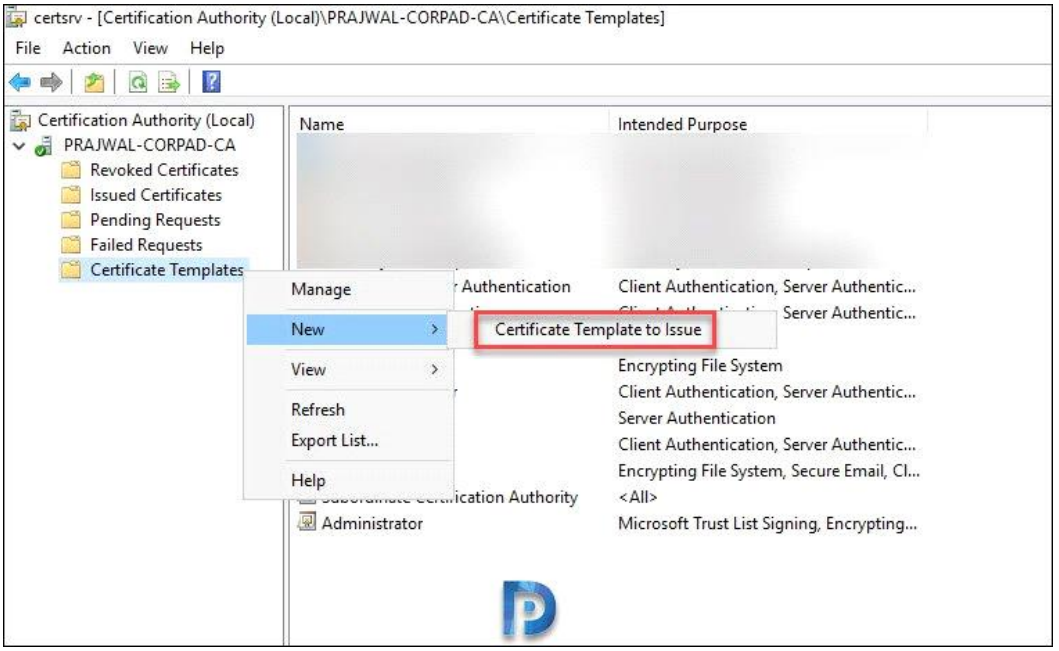
SCCM CMG Certificate Template

For Enterprise Admins, you can uncheck Enroll permission. Click Apply and OK. Close the console.



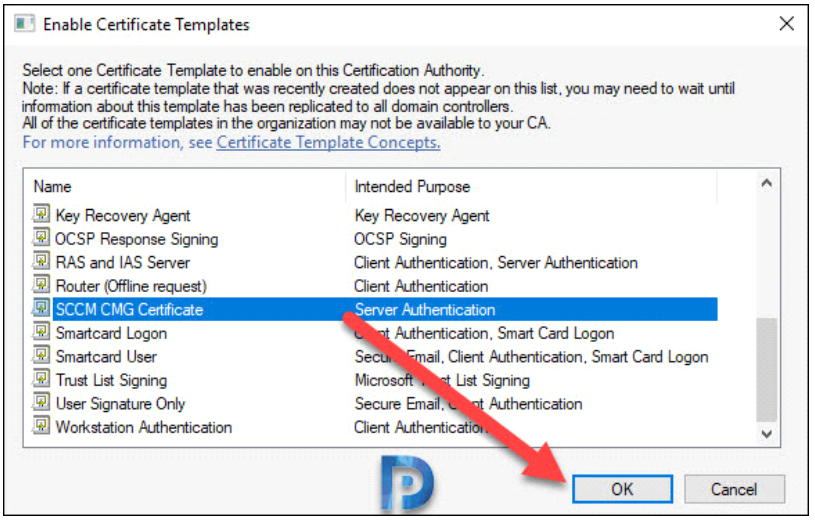
SCCM CMG Certificate Template

Now right click Certificate Templates and click New > Certificate Template to Issue.



SCCM CMG Certificate Template

Select the SCCM CMG Certificate and click OK.

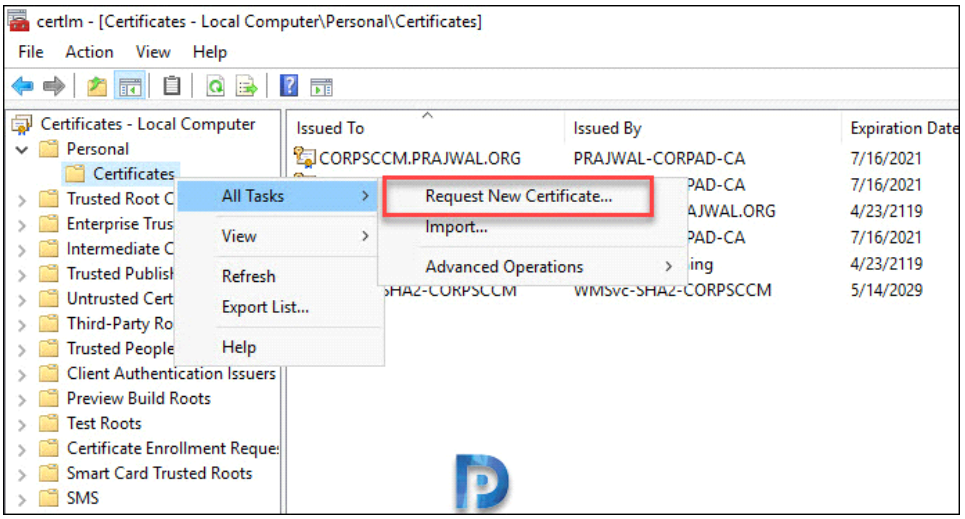


SCCM CMG Certificate Template

Import Web Server CMG certificate on the Primary Site Server

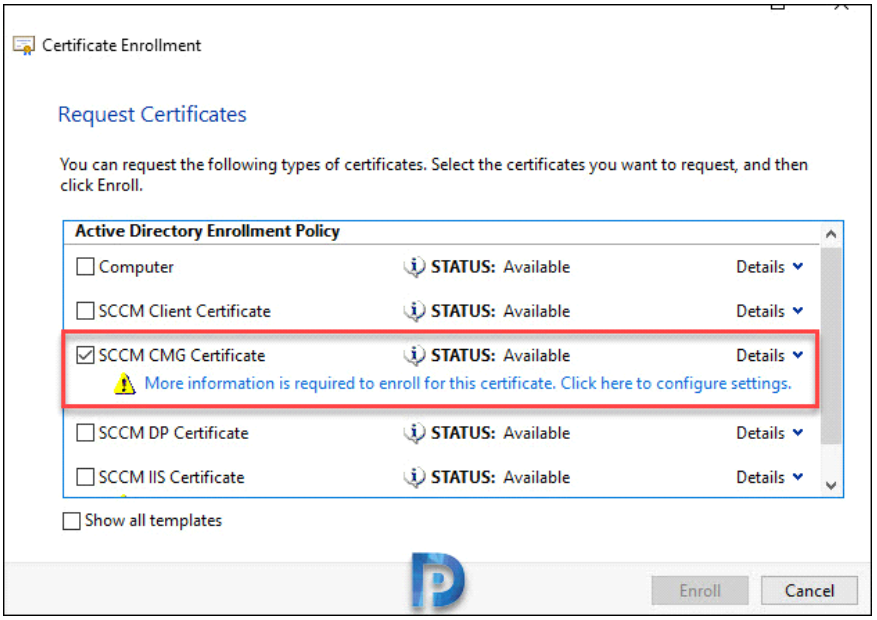
After you have created the SCCM CMG certificate, we will now import this certificate on our SCCM server.

Login to SCCM server. Open the Certificates console (run the command certlm.msc – this saves your time). Expand Personal > Certificates. Right click Certificates > All Tasks > Request New Certificate.



Import Web Server CMG certificate

From the list of certs, select SCCM CMG Certificate and click the link below it.

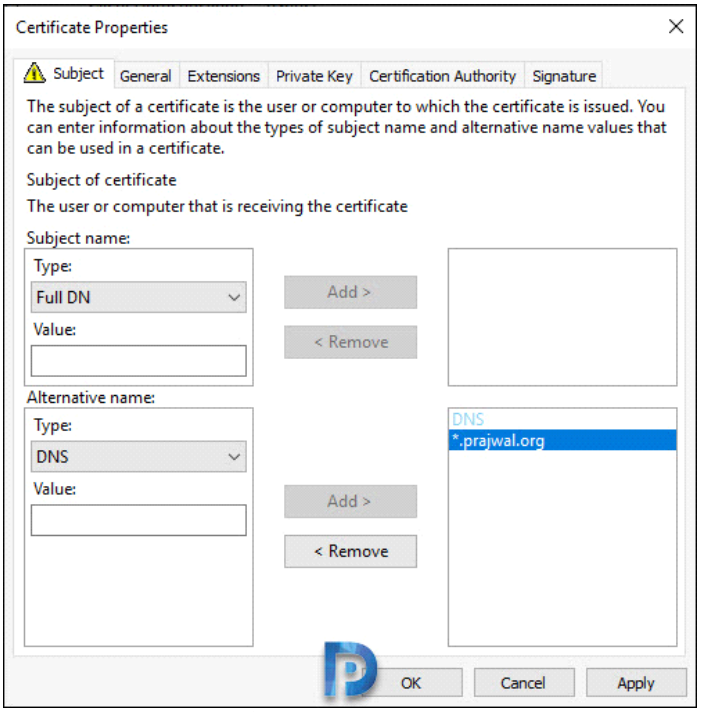


Import Web Server CMG certificate

In the Certificate Properties dialog box, under for Subject name, select Type as Full DN.

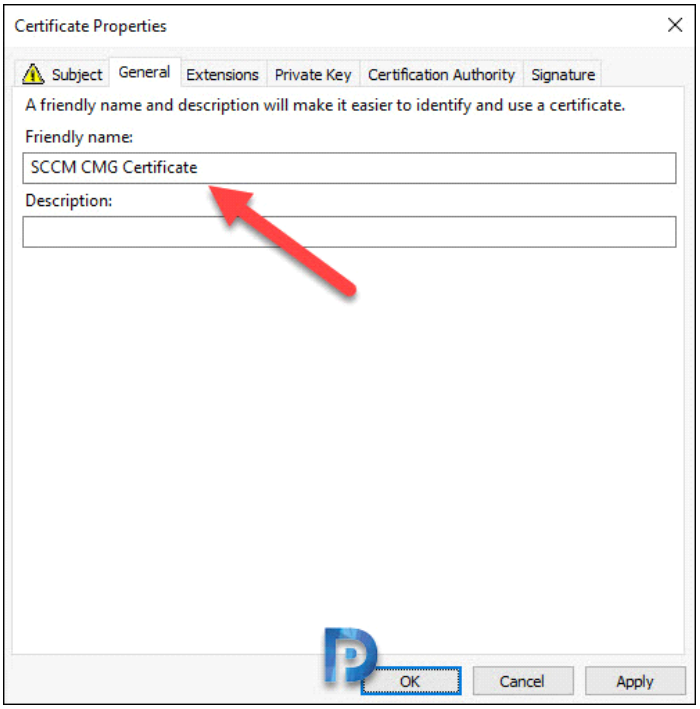
Under Alternative name, select Type as DNS and enter the service name.

Enter a public DNS name that you want to use with SCCM CMG. So I will enter *.prajwal.org here which allows me to use any subdomain for CMG.



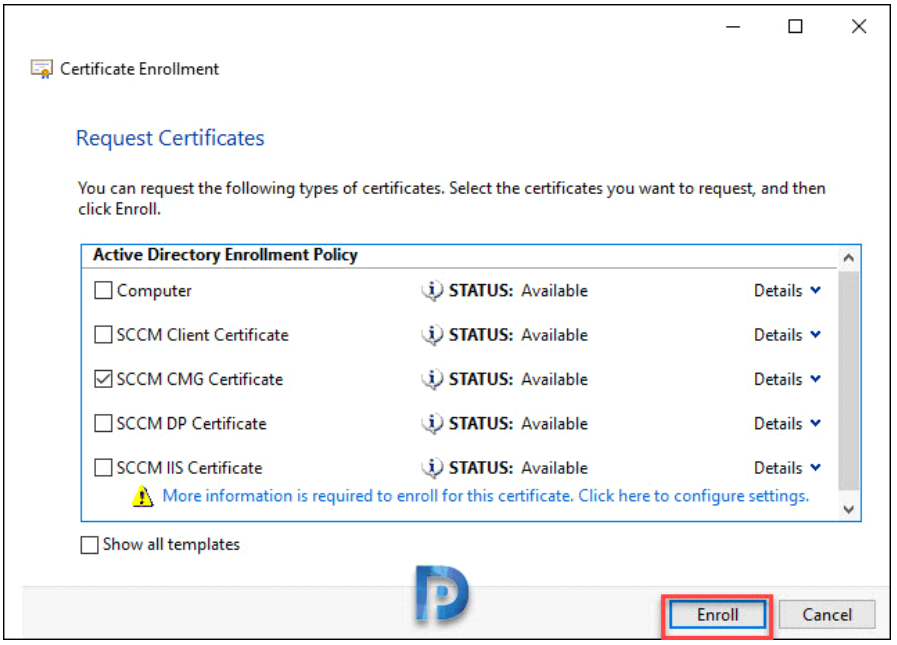
Import Web Server CMG certificate

Click General tab and specify a friendly name to this certificate and then click Apply and OK.



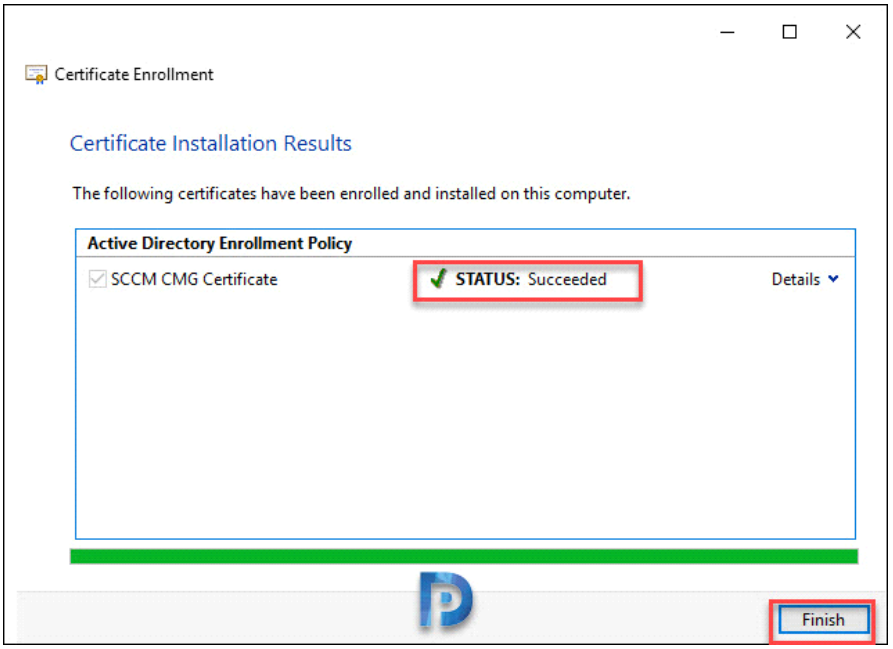
Import Web Server CMG certificate

Click Enroll.



Import Web Server CMG certificate

The certificate is enrolled successfully. Click Finish.



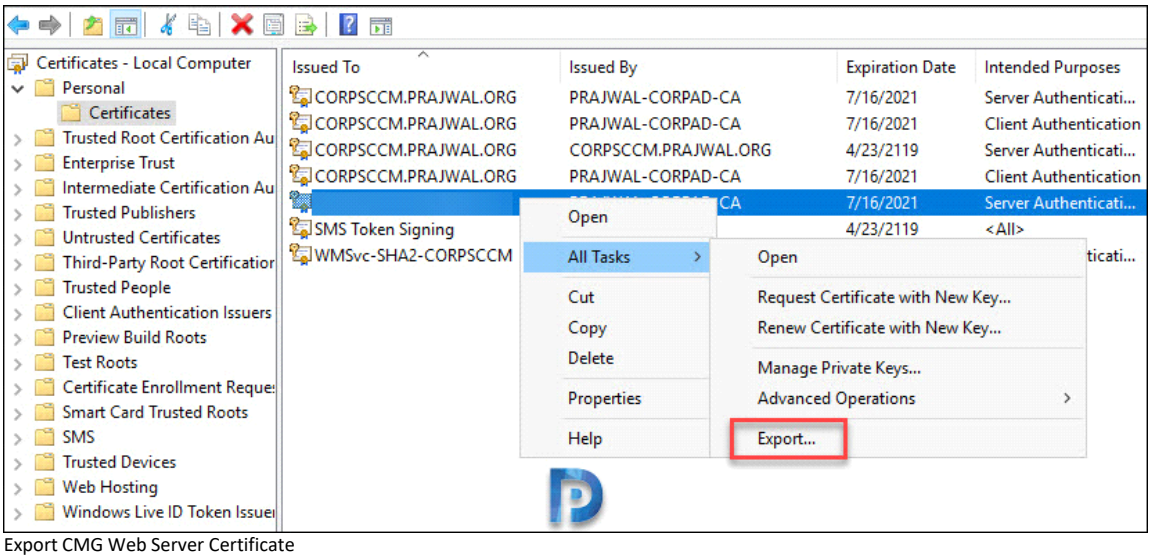
Import Web Server CMG certificate

Export CMG Web Server Certificate

In the above step, on the site server, you requested the CMG certificate and enrolled it.

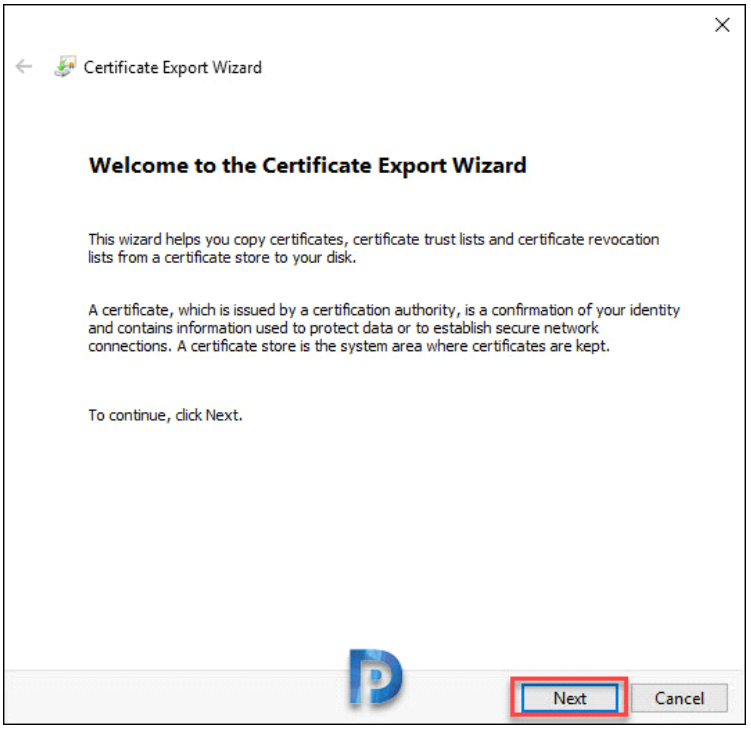
Now we will export this certificate in a .PFX format. This certificate will required while creating cloud management gateway.

Select the CMG certificate, right click and click All Tasks > Export.



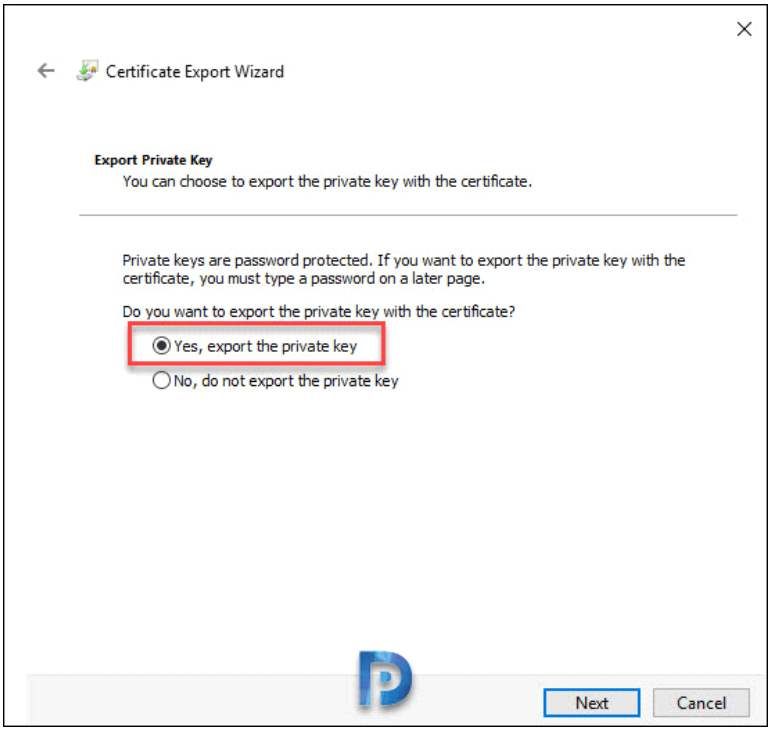
Export CMG Web Server Certificate

On welcome to certificate export wizard, click Next.



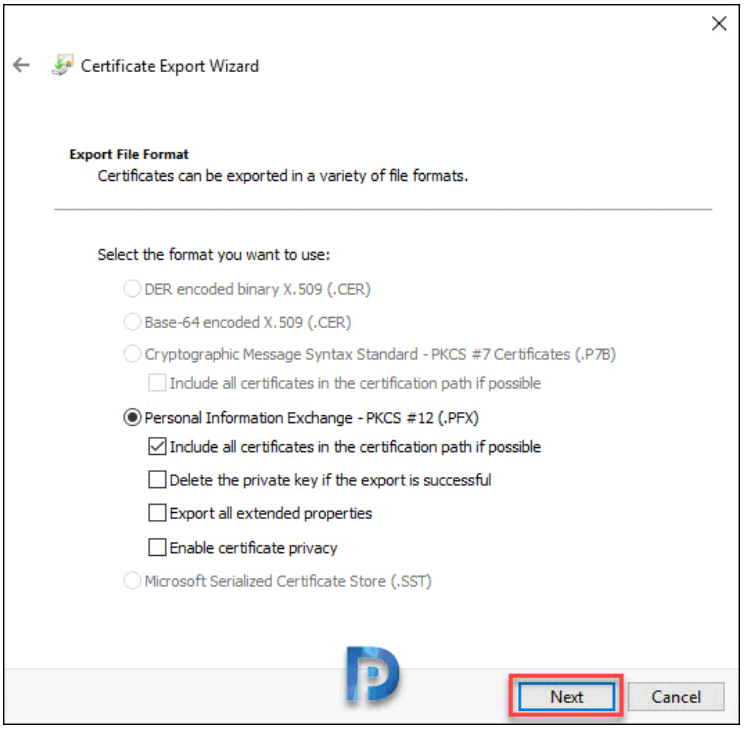
Export CMG Web Server Certificate

Select Yes, export the private key. Click Next.



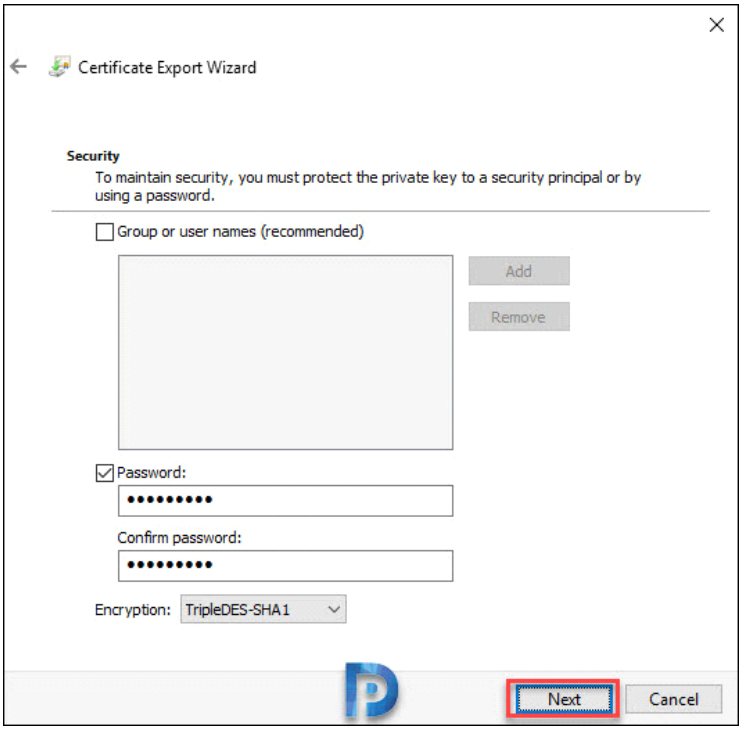
Export CMG Web Server Certificate

Make no changes here and click Next.



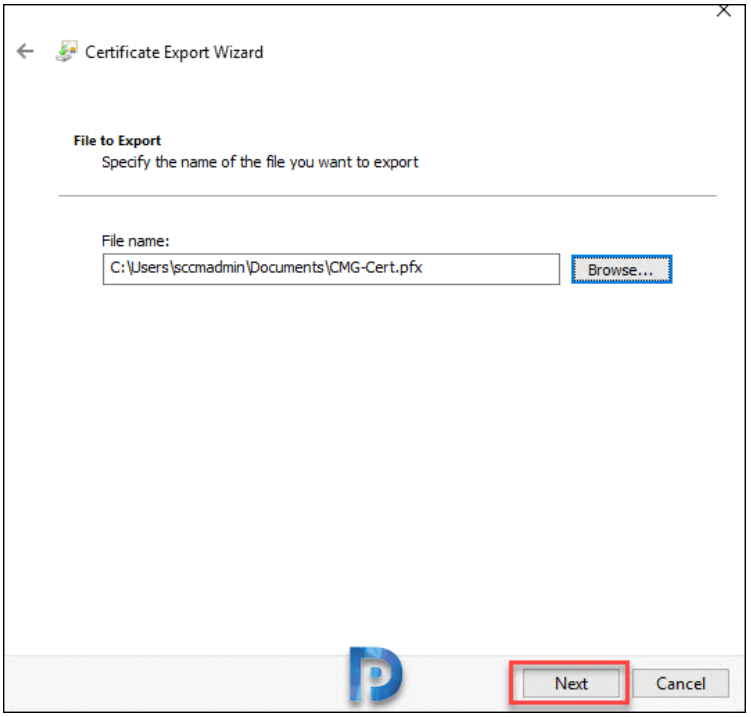
Export CMG Web Server Certificate

Enter a password and click Next.



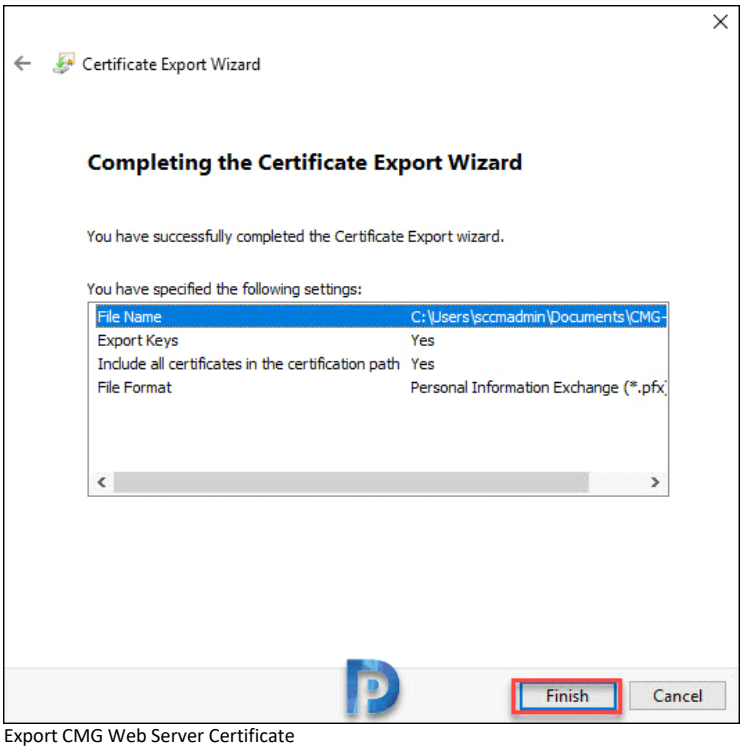
Export CMG Web Server Certificate

Save the CMG certificate on your computer. Click Next.



Export CMG Web Server Certificate

Click Finish. This completes the CMG certificate export process.

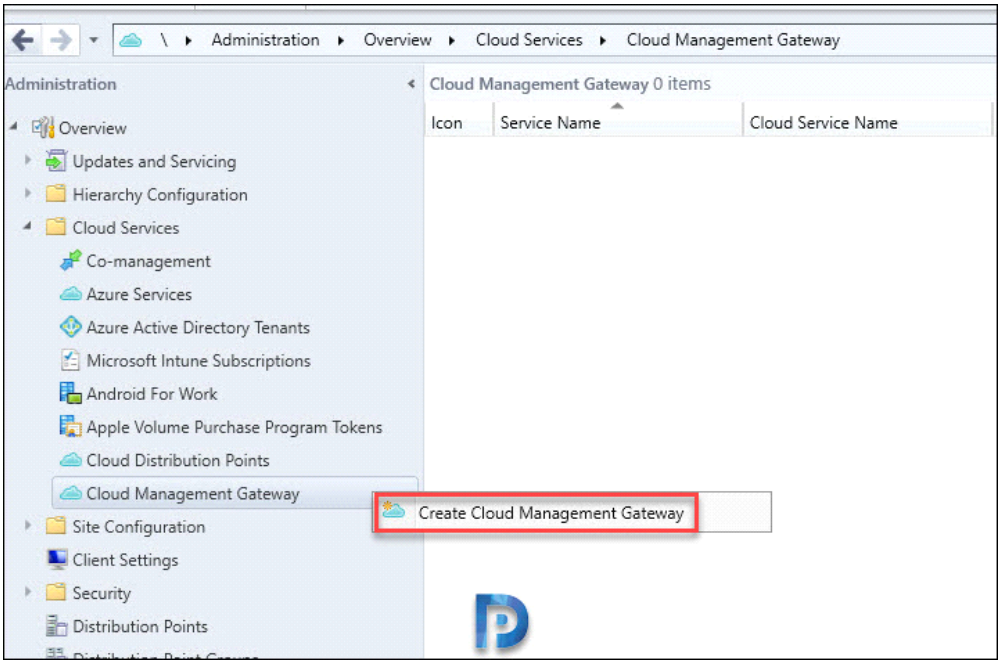


Export CMG Web Server Certificate

Setup SCCM Cloud Management Gateway (SCCM CMG)

To create or setup cloud management gateway in SCCM –

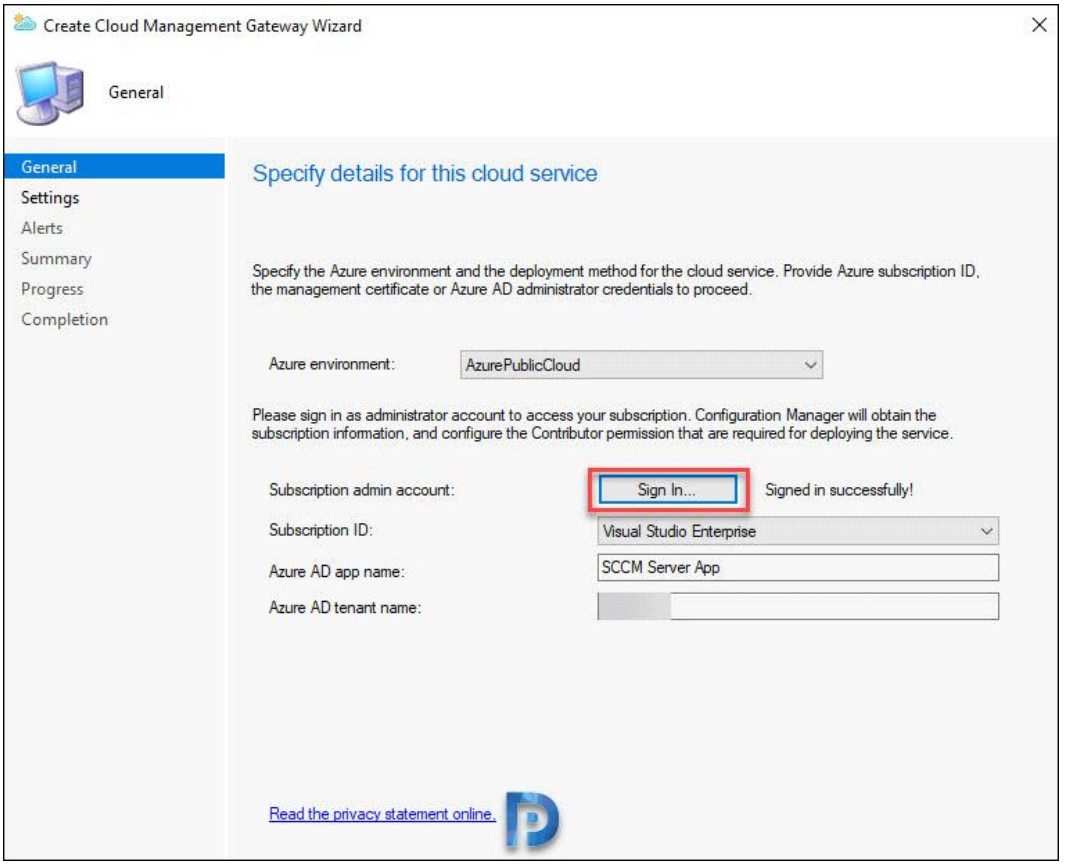
- Launch the SCCM console.
- Navigate to Administration > Cloud Services > Cloud Management Gateway.
- Right click Cloud Management Gateway and click Create Cloud Management Gateway



Setup SCCM Cloud Management Gateway (SCCM CMG)

You should now see the Create Cloud Management Gateway Wizard. Click Sign-in and login with your subscription admin account.

On successful sign-in you should see Subscription ID, Azure AD app name and tenant name automatically populated. Click Next



Setup SCCM Cloud Management Gateway (SCCM CMG)

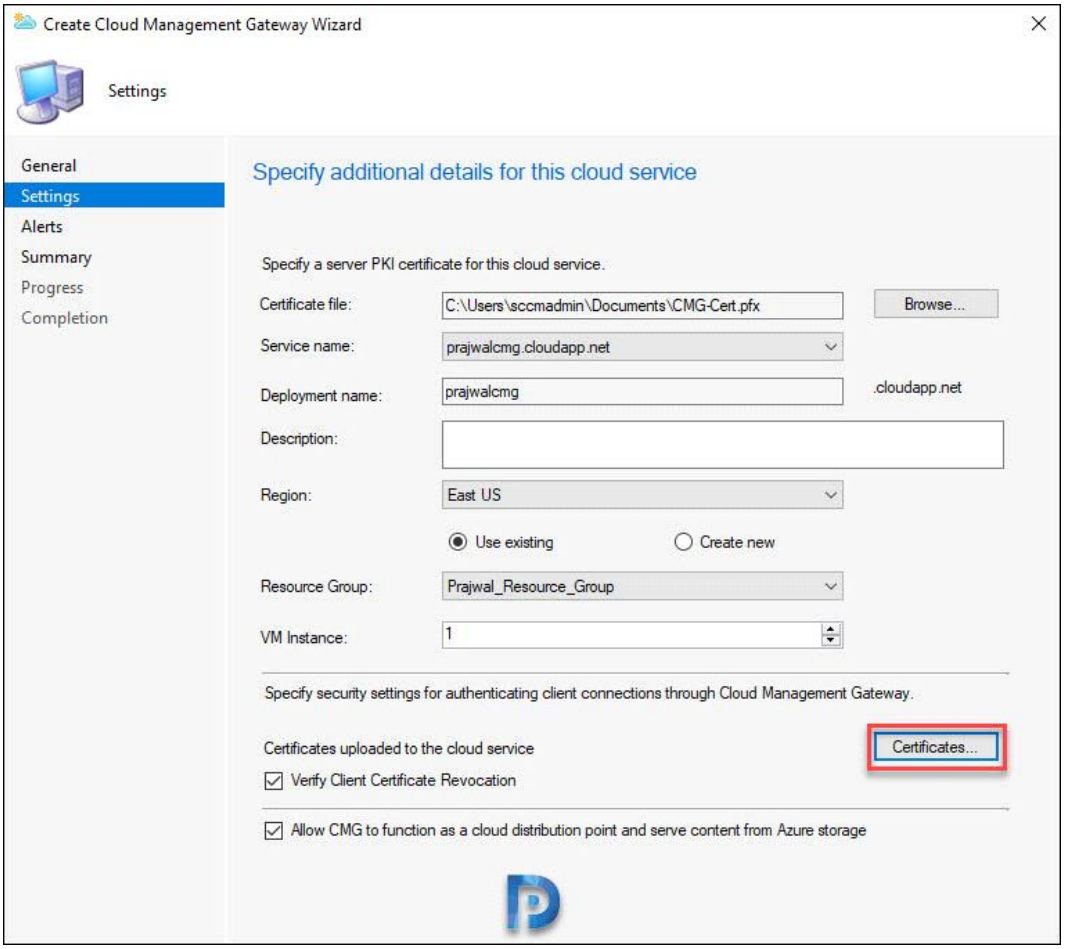
On the Settings page, click Browse and select the CMG certificate. The Service name and deployment name are populated automatically.

At this step you can use an existing resource group or create new resource group. I will go with just 1 VM instance.

You see two options and a certificates button.

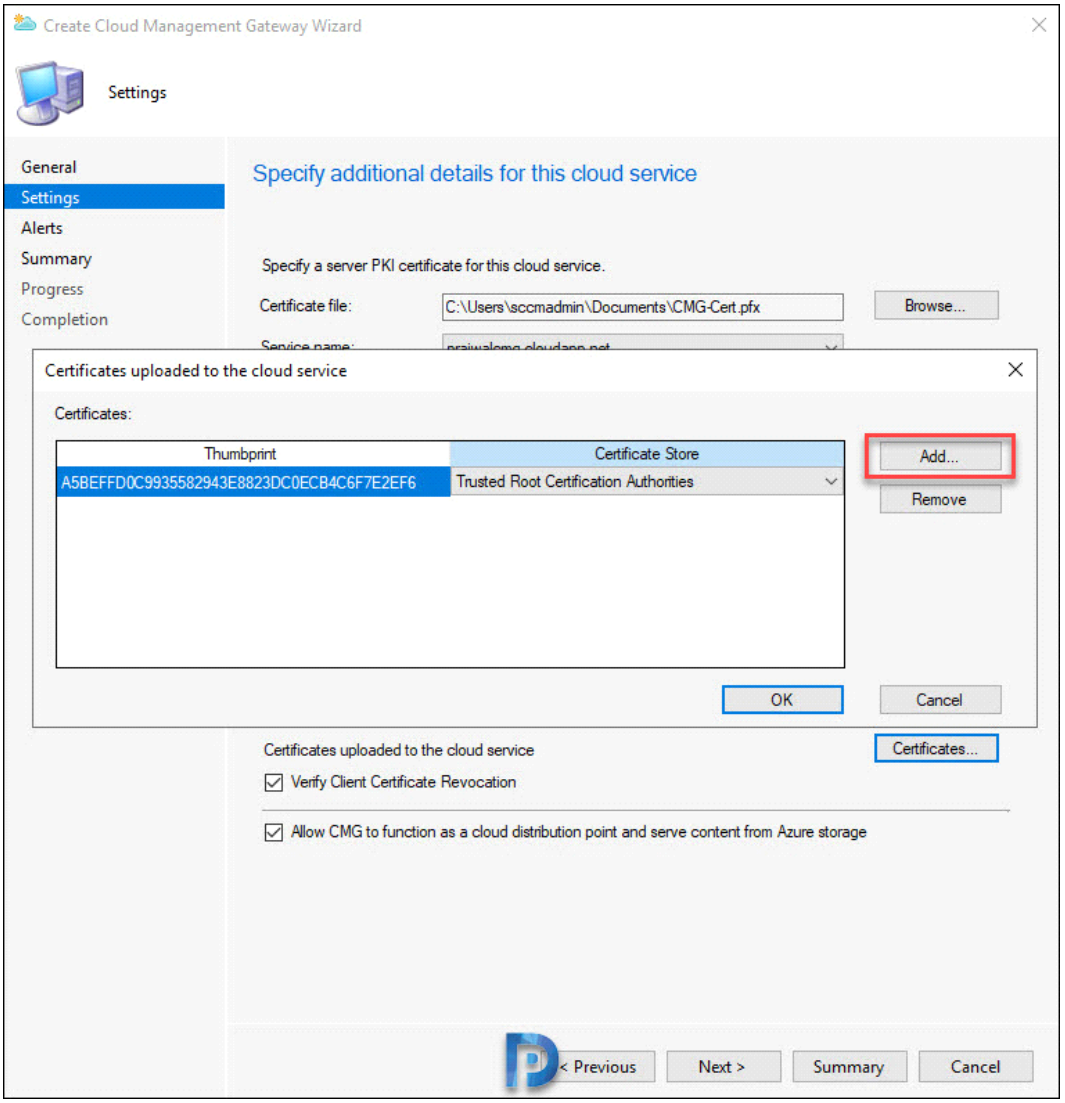
- Verify Client Certificate Revocation – To understand this refer this article.
- Allow CMG to function as a cloud distribution point and serve content from Azure storage – With SCCM 1806, you get this new option. Now a CMG can also serve content to clients. This functionality reduces the required certificates and cost of Azure VMs.

I will leave both the above options checked. Next click Certificates.



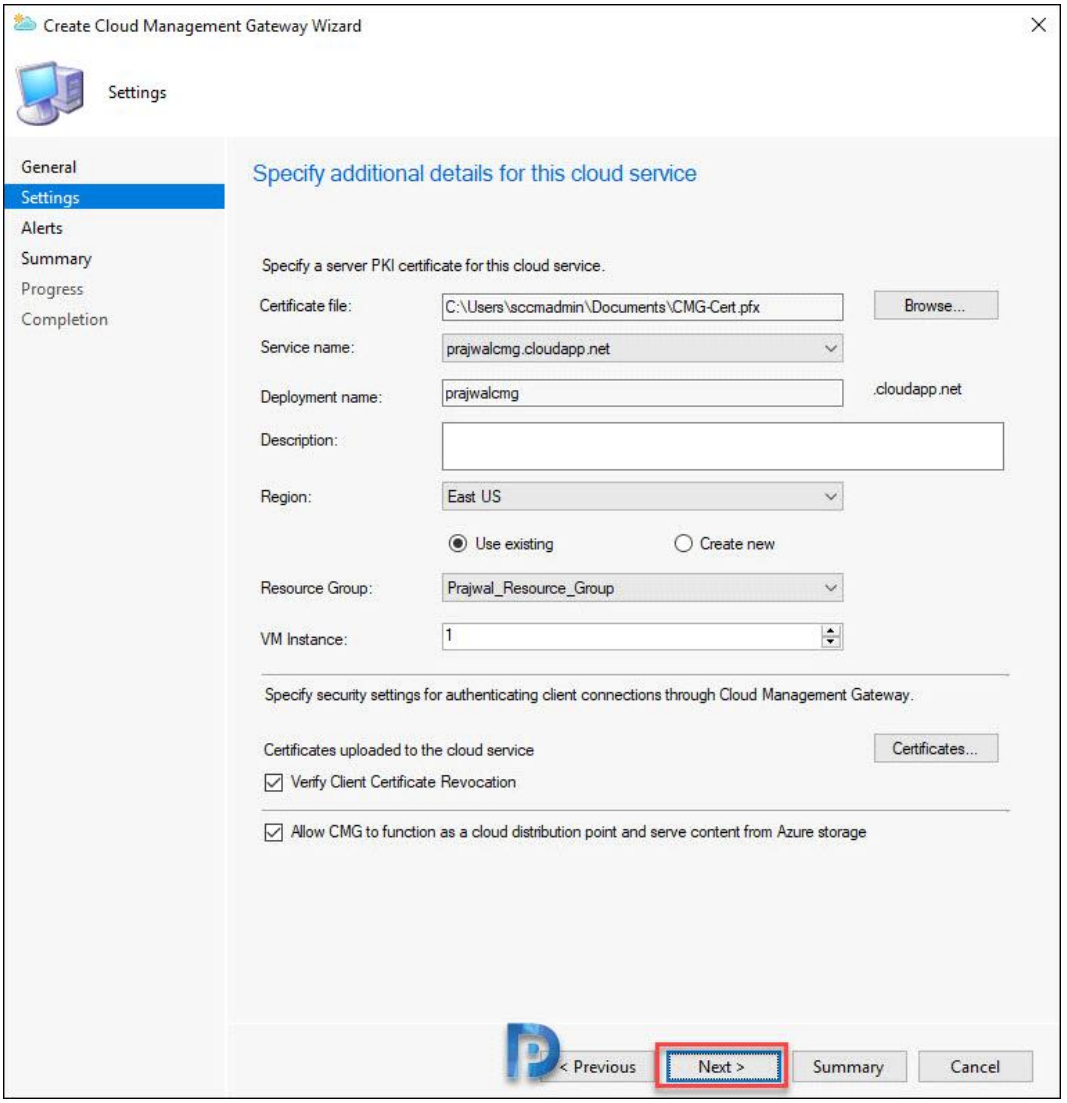
Setup SCCM Cloud Management Gateway (SCCM CMG)

You need to specify a certificate that tells CMG what certs it needs to trust. In my case I have got an PKI setup, so I will add the root certificate.



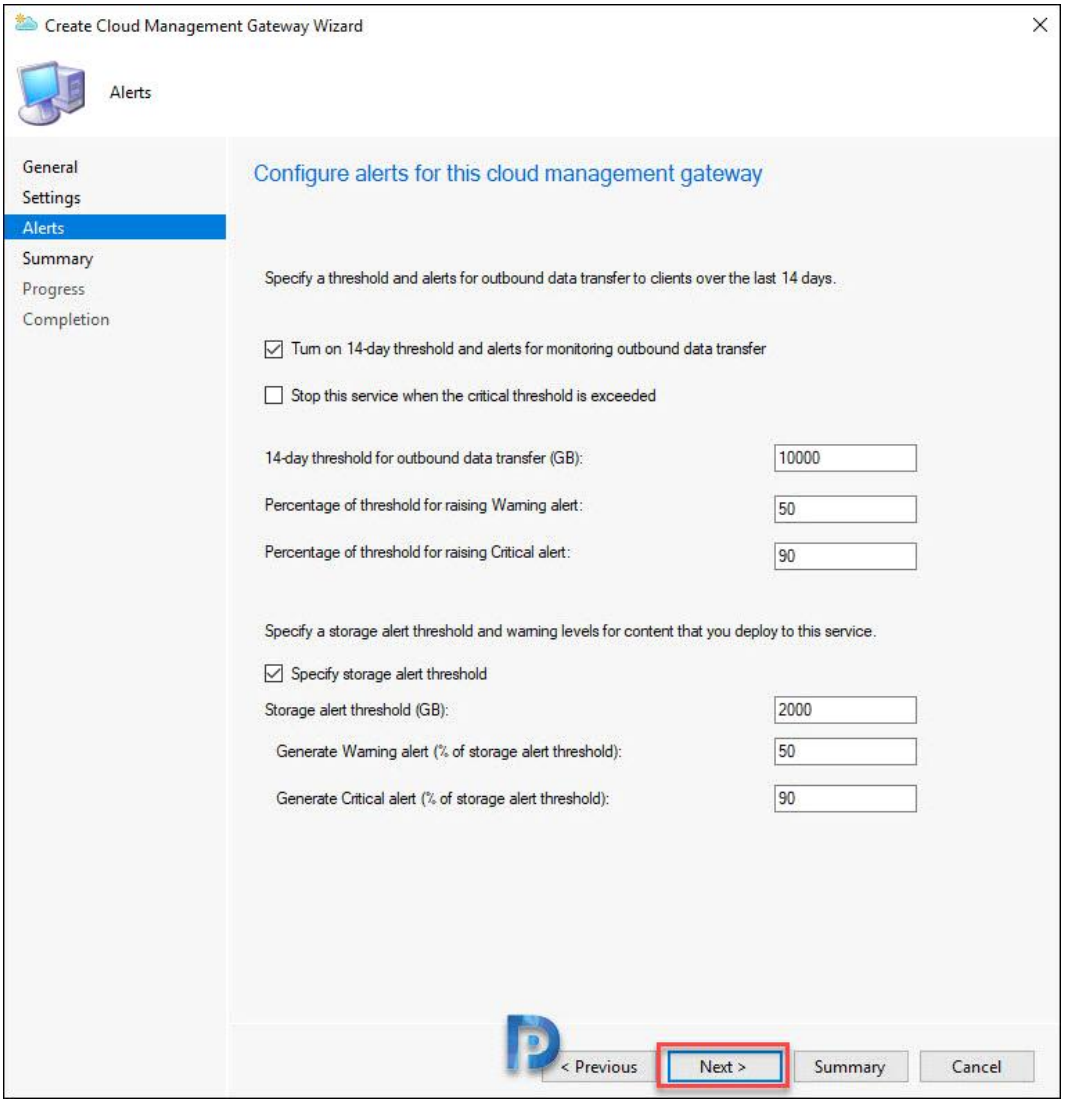
Setup SCCM Cloud Management Gateway (SCCM CMG)

Click Next.



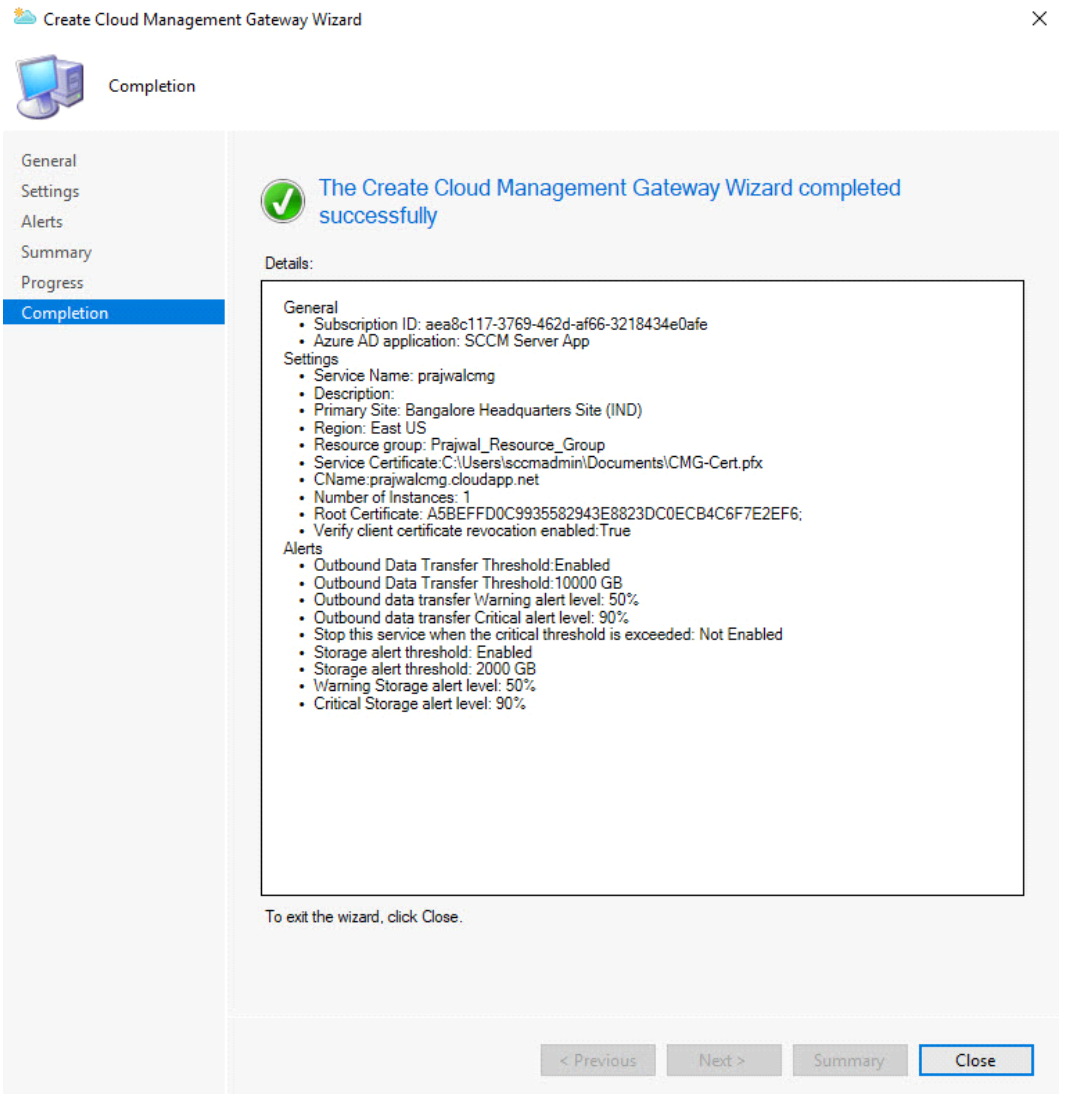
Setup SCCM Cloud Management Gateway (SCCM CMG)

On the Alerts page, click Next.



Setup SCCM Cloud Management Gateway (SCCM CMG)

On the completion page click Close.

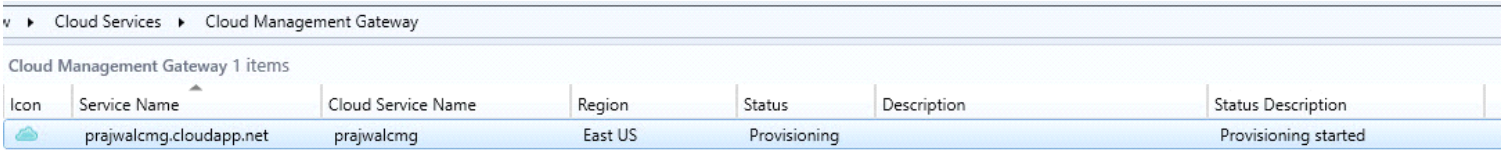


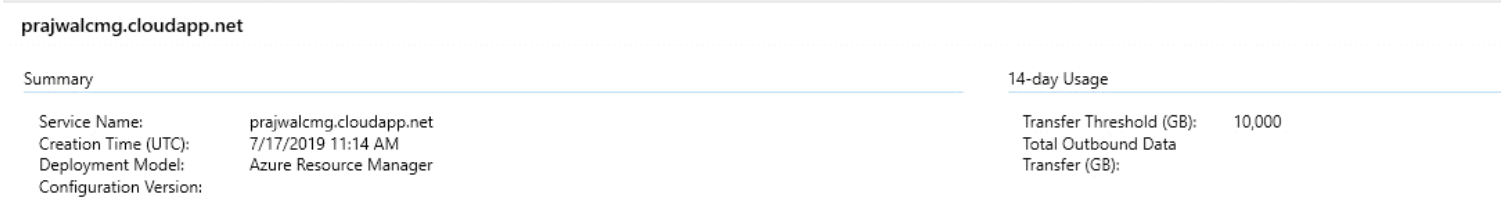
Setup SCCM Cloud Management Gateway (SCCM CMG)

Cloud Management Gateway Status

After you setup cloud management gateway, monitor the status in the SCCM console.

Right now the status in Provisioning.

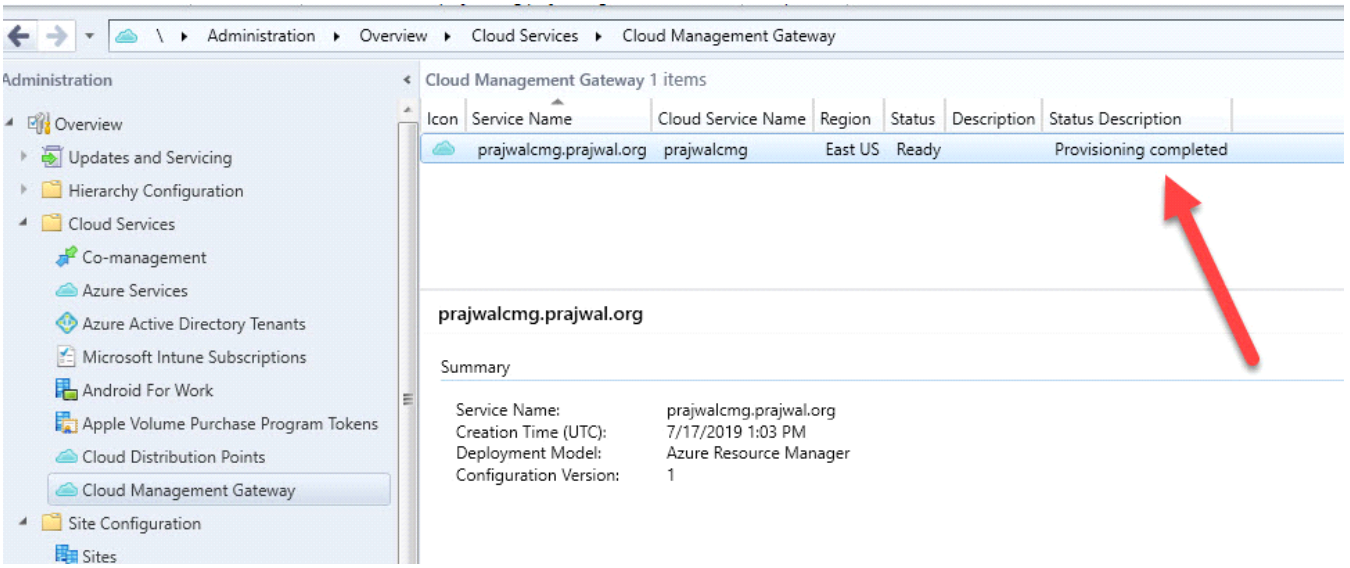




Cloud Management Gateway Status

After few minutes the status is changed to Provisioning Completed. Later I will cover what

log file do you need to monitor for this.

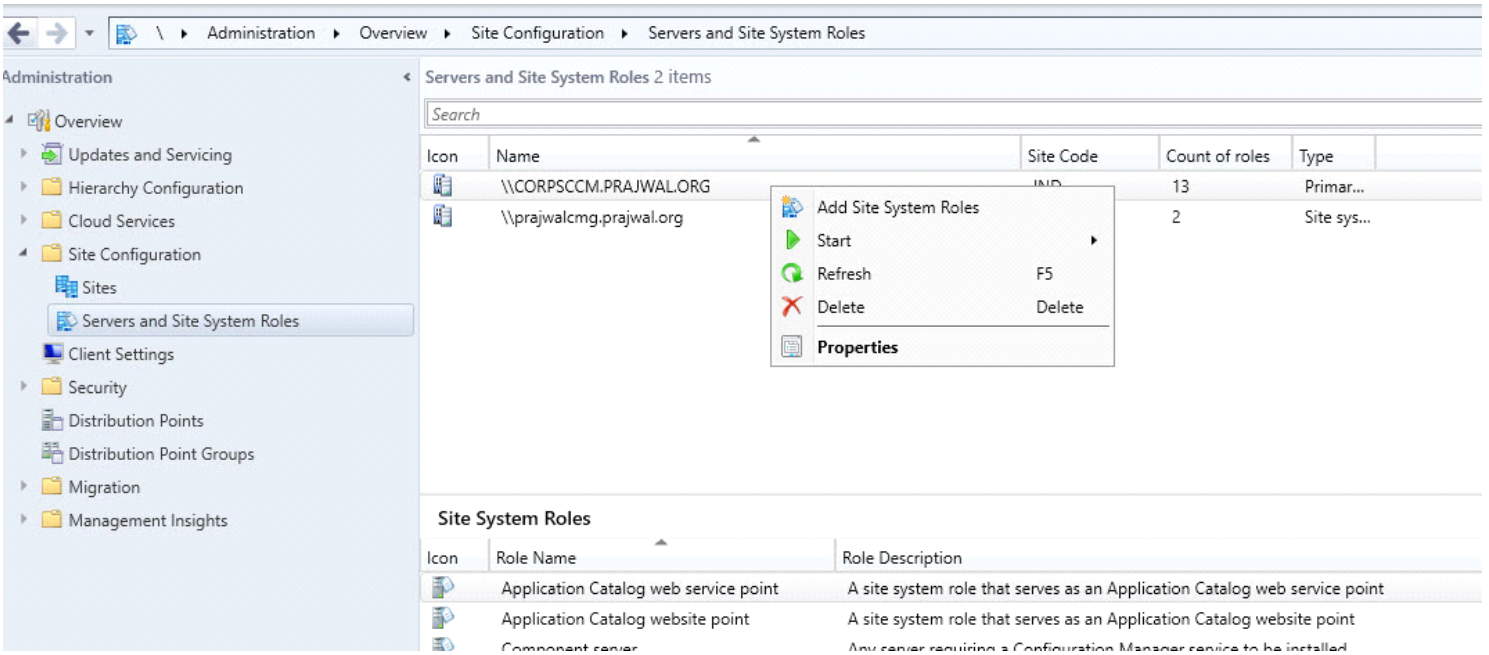


Cloud Management Gateway Status

Install Cloud Management Gateway Connection Point

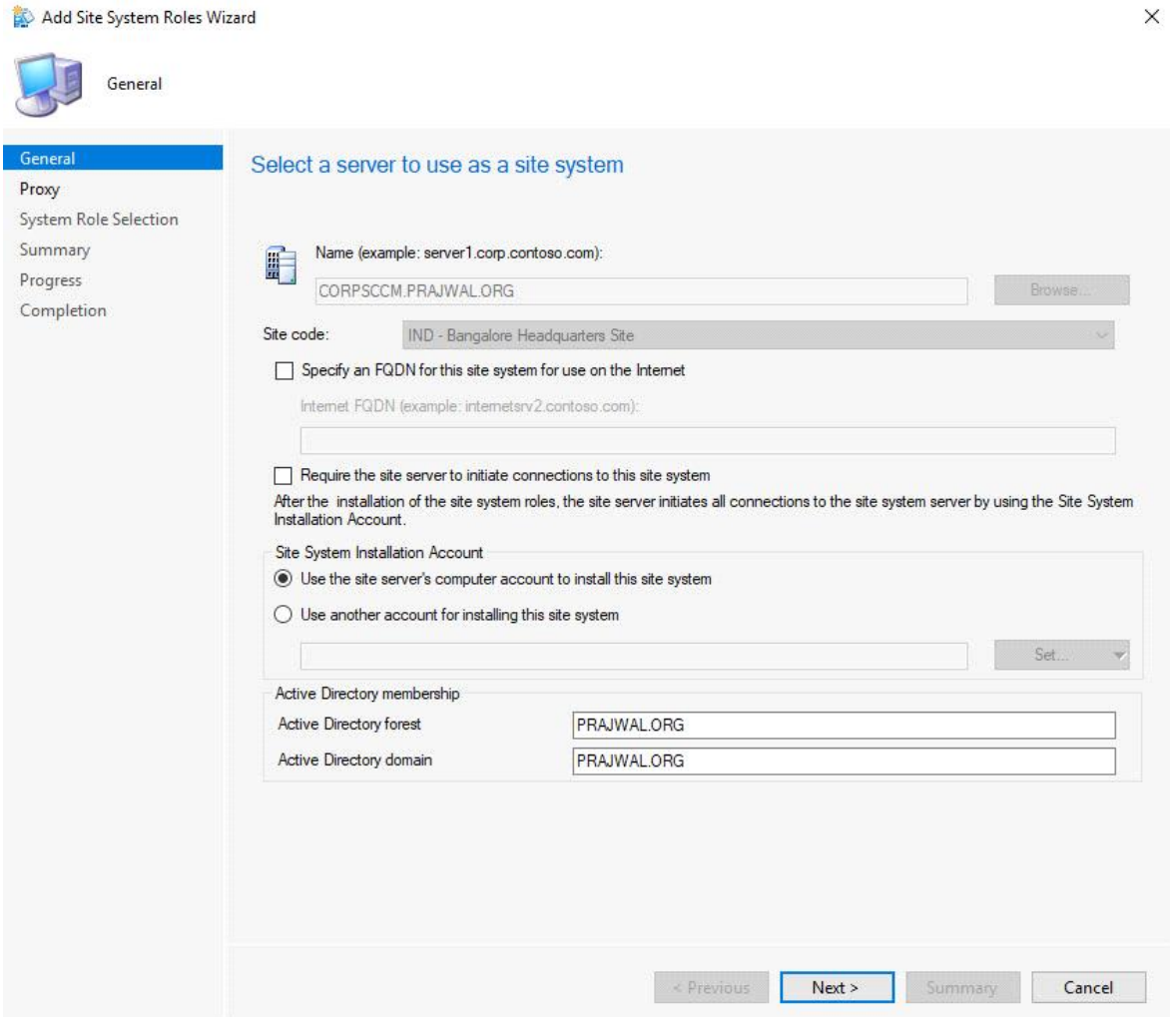
To install cloud management gateway connection point role in SCCM

- In SCCM console, go to Administration > Site Configuration > Servers and Site System Roles.
- Right click site server and click Add Site System Roles.



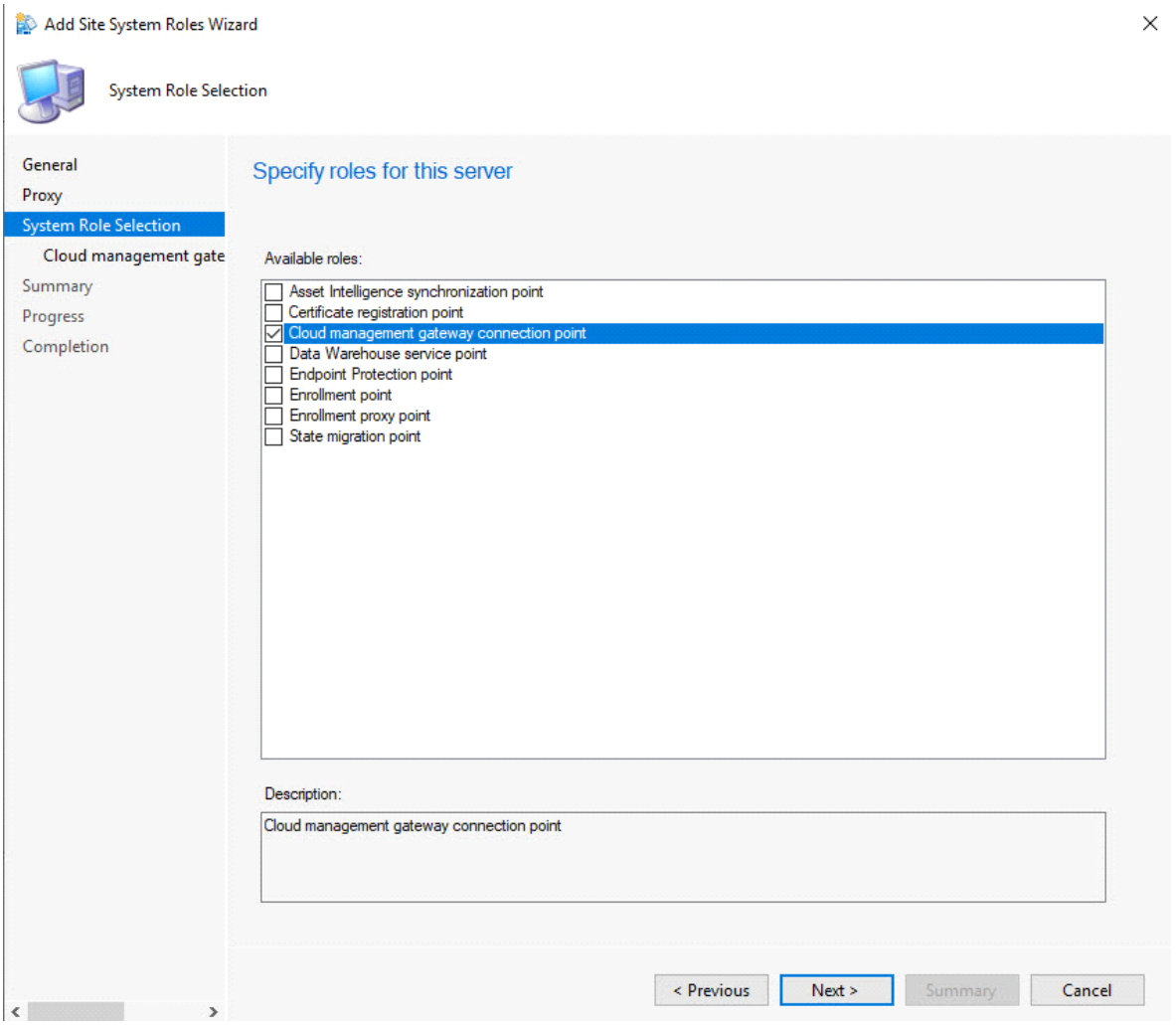
Install Cloud Management Gateway Connection Point

Click Next.



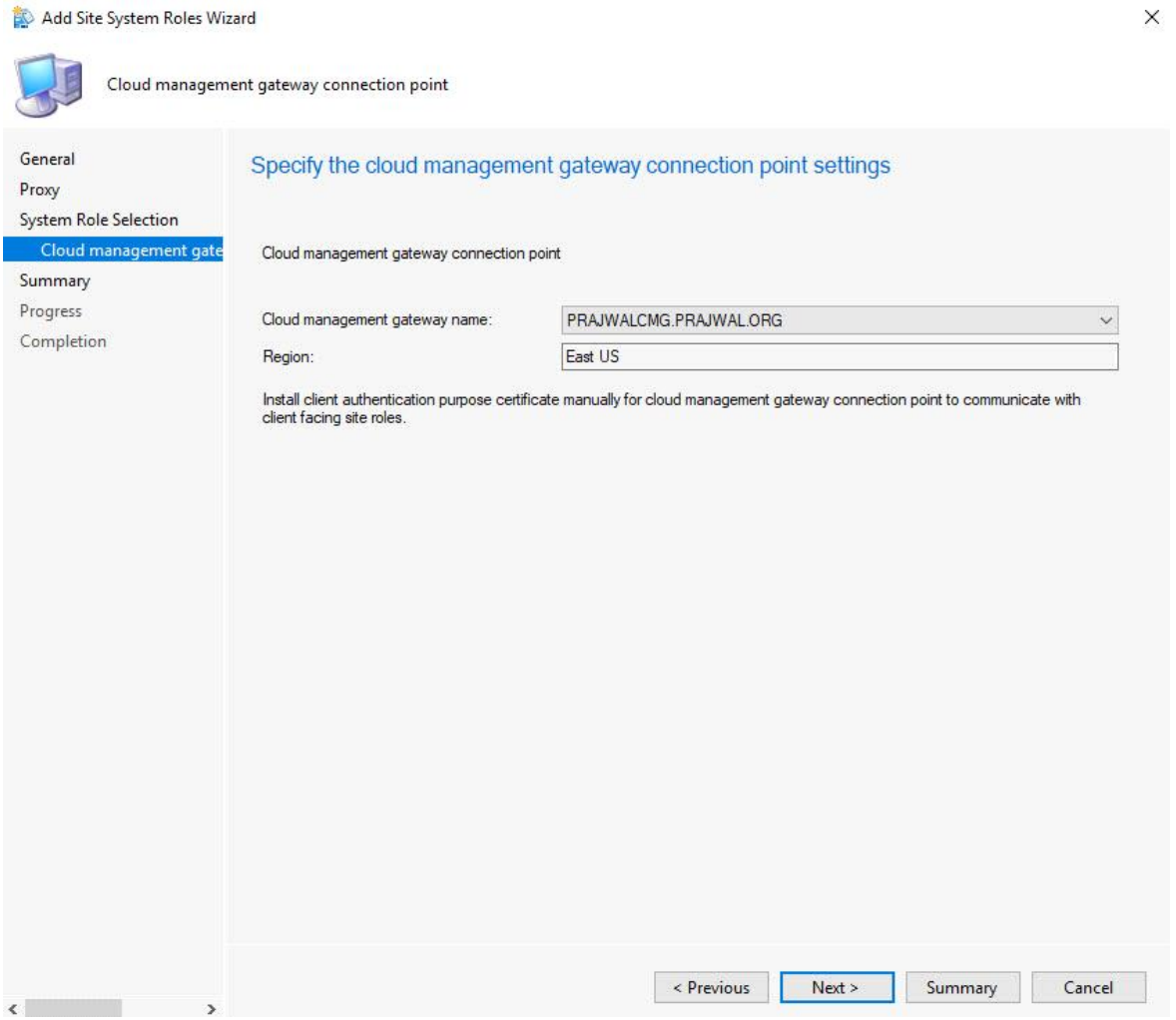
Install Cloud Management Gateway Connection Point

Check the box for Cloud Management gateway connection point. Click Next.



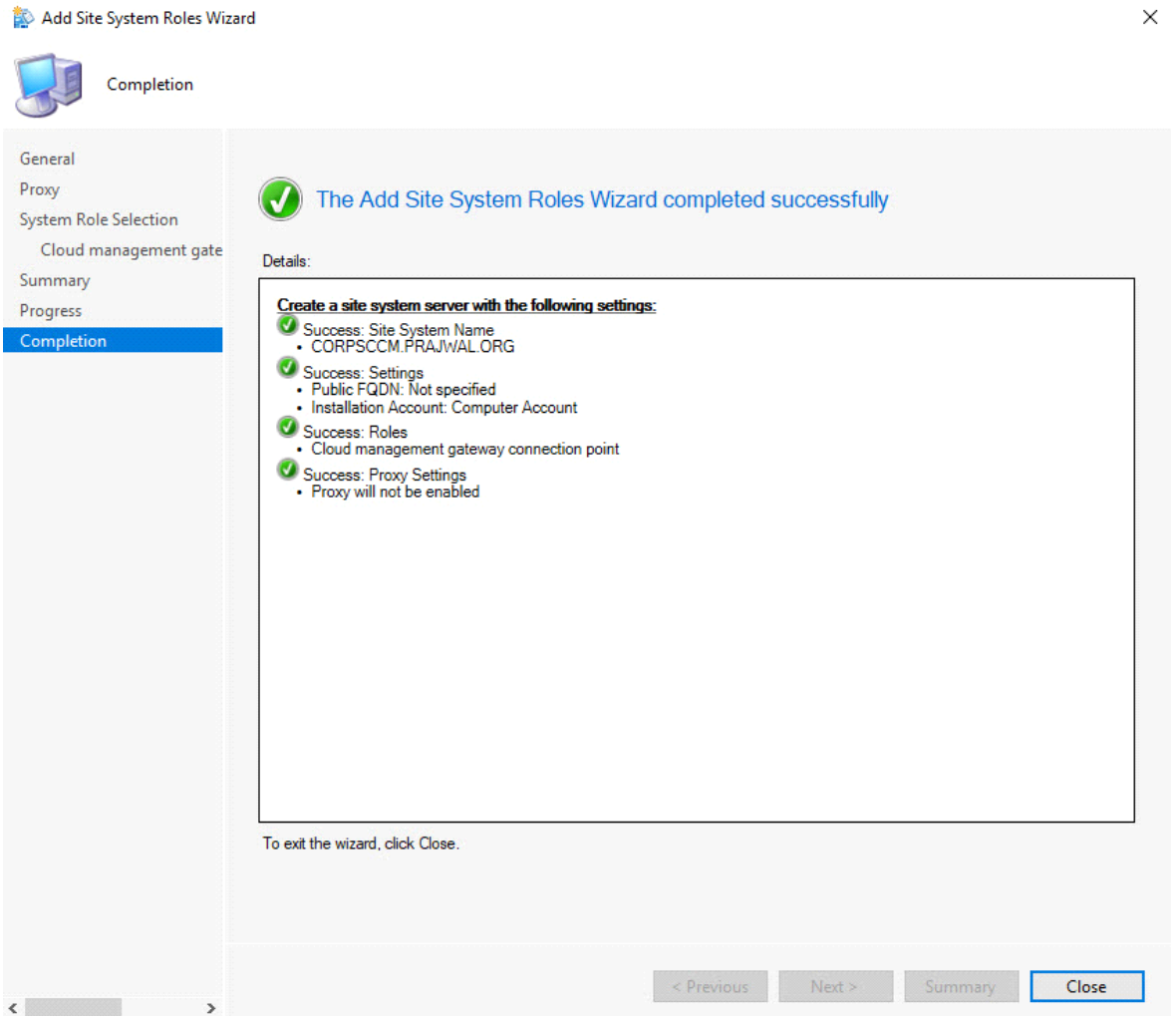
Install Cloud Management Gateway Connection Point

Select the cloud management gateway and click Next.



Install Cloud Management Gateway Connection Point

On the completion page, click Close.



Install Cloud Management Gateway Connection Point

Allow SCCM Cloud Management Gateway Traffic

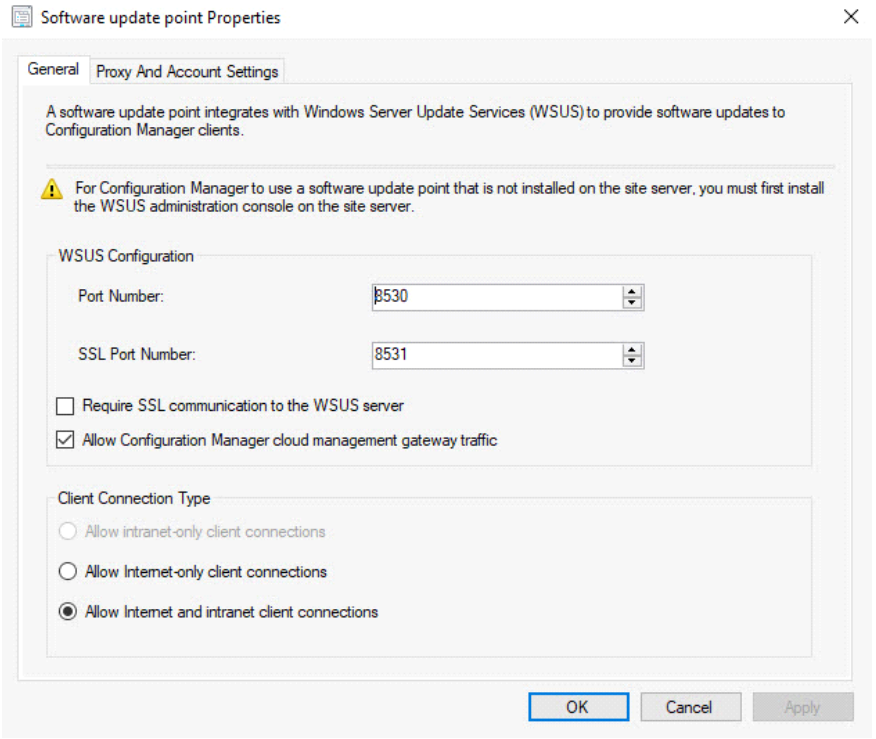
You must configure the management point and software update point site systems to accept SCCM cloud management gateway traffic. Do this procedure on the primary site, for all management points and software update points that service internet-based clients.

Go Administration > Site Configuration > Servers and Site System Roles. Select the site server and in the bottom pane, right click Management point and click Properties.

Under Management Point Properties, check the box Allow Configuration Manager cloud management gateway traffic. Click OK.

Allow SCCM Cloud Management Gateway Traffic

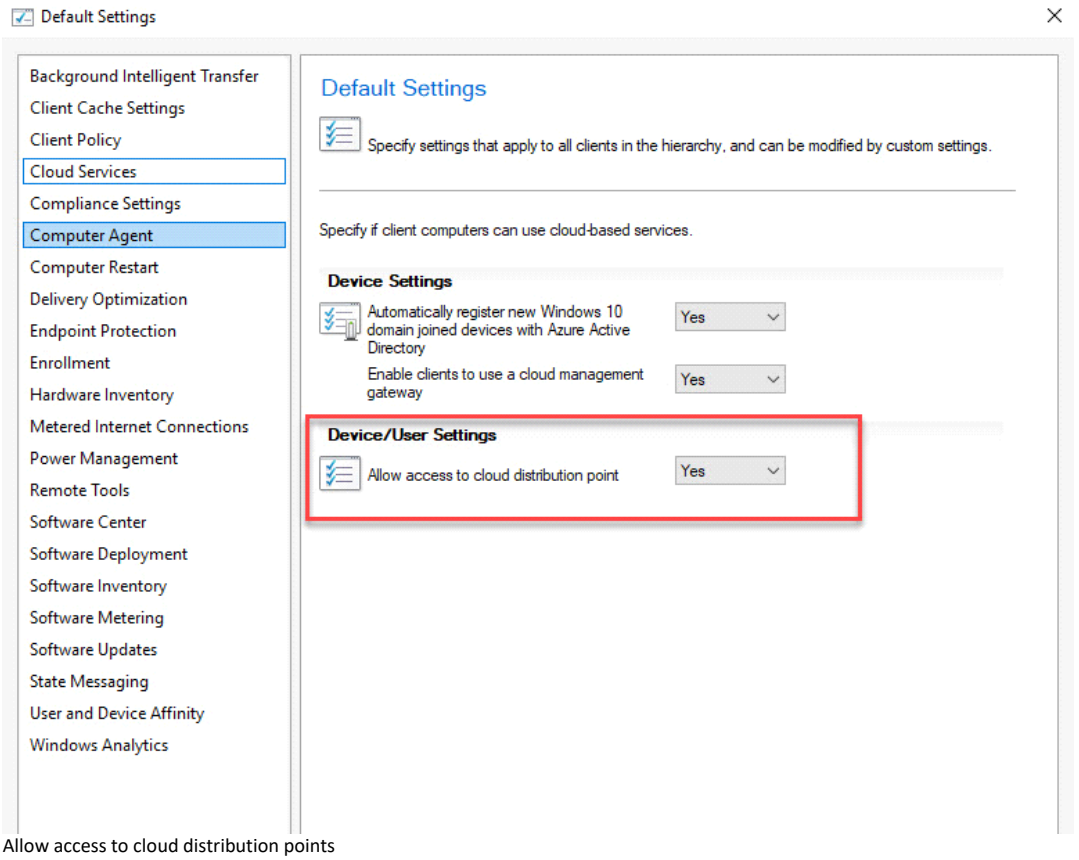
Under Software update point properties, check the box Allow Configuration Manager cloud management gateway traffic. Click OK.



Allow SCCM Cloud Management Gateway Traffic

Allow access to cloud distribution points

Under the client settings, click Cloud Services. Under Device/User Settings, set Allow access to cloud distribution point to Yes.



Allow access to cloud distribution points

Associate SCCM CMG with Boundary groups

If you are using Configuration Manager 1902, you can associate a SCCM Cloud Management Gateway with a boundary group. You can do this after you setup SCCM cloud

management gateway. When you create or configure a boundary group, on the References tab, add a cloud management gateway.

Associate SCCM CMG with Boundary groups

Configure Clients for CMG

Once you setup SCCM cloud management gateway and all the site system roles are running, clients get the location of the CMG service automatically on the next location request.

Most of all the clients must be on the intranet to receive the location of the SCCM CMG service. By default the polling cycle for location requests is every 24 hours. However to speed up the request, you can restart the SMS Agent Host service (ccmexec.exe) on the computer.

Sometimes when you switch the client to internet, the client still talks to your internal management point. In such cases you can force the client to always use the CMG with a registry key change. This configuration is useful for testing purposes, or for clients that you want to force to always use the CMG.

You can set the following registry key on the client. By setting ClientAlwaysOnInternet = 1, the clients will use SCCM CMG service.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM\Security, ClientAlwaysOnInternet = 1

To troubleshoot CMG client traffic, use CMGHttpHandler.log, CMGService.log, and SMS_Cloud_ProxyConnector.log. I will cover more about CMG troubleshooting and other stuff related to it in some other post.

Enable Remote Desktop on SCCM CMG (Cloud Management Gateway)

Once you setup the SCCM CMG, you can enable remote desktop on SCCM CMG. Once you enable remote desktop on CMG, you can the IIS log files from the CMG Virtual Machine. Here is a step by step guide on how to enable remote desktop in SCCM cloud management gateway.

Cloud Management Gateway Log Files for Troubleshooting

When you setup the SCCM cloud management gateway, you must know the CMG log files that can help you to troubleshoot CMG issues. There are very few CMG log files and I have listed all the CMG log files in this post.

SCCM CMG (Cloud Management Gateway) FAQ

Some of the common questions related to SCCM cloud management gateway setup.

What is SCCM CMG ?

CMG stands for cloud management gateway. The cloud management gateway (CMG) provides a simple way to manage Configuration Manager clients over the internet.

PowerShell command to setup CMG ?

You can use New-CMCloudManagementGateway to setup CMG using PowerShell.

Can a Primary site have multiple instances of the CMG ?

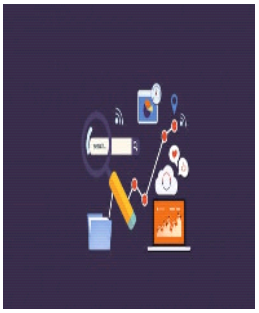
Yes, you can install multiple instances of the CMG connection point at primary sites.

Cloud Management Gateway CMG Configuration Manager SCCM

Prajwal Desai

Hi, I am Prajwal Desai. For last few years I have been working on multiple technologies such as SCCM / Configuration Manager, Intune, Azure, Security etc. I created this site so that I can share valuable information with everyone.

RELATED ARTICLES



Create SCCM Device Collection for Visual Studio

April 15, 2021

How to Manage SCCM duplicate hardware identifiers

April 24, 2018

Create & Deploy Third-Party Applications with SCCM – Patch Connect Plus

September 9, 2019

65 Comments

Van Laarhoven Gérard says:
February 25, 2021 at 11:53 pm
HI,
Thanks for this great post
I have a question: what boundaries should i add to the CMG boundary group for computer full internet (not on lan or vpn)
There is something i don't really understand as i want to use this CMG for internet only computers and not intranet and so impossible to know ip ranges
Thanks
Gérard
Reply

Nandu Ditto says:
February 25, 2021 at 11:19 pm
Hi , i tried all these and getting error while creating CMG.
Below is the error,
"Error occured when granting contributor permission to AzureAD app for resource group ****CMG. For more information, see SmsAdminUi.log"
Can you please help ?
Reply

Benny says:
October 23, 2020 at 12:58 pm
Hello Prajwal, I'm trying to install CMG but first i need configure Azure Services > Cloud Gestion. So i have an error with the app creation…Azure connexion failed (i'm Azure Administrator).
Do you have an idea ?
Reply

Mauvi says:
November 2, 2020 at 6:30 pm
I had the same problem, I then actived the Global Administrator role with PIM. And it worked for me.
Reply

Riz says:
October 16, 2020 at 9:36 pm
Hi Prajwal , Been following your videos for a long time . great work ,
How do you go about adding additional cloud management gateways in sccm . Can you please write a tutorial . thanks
Reply

jean-sebastien F says:
September 1, 2020 at 8:15 pm
Hello,
Is there a way to tell internet computer that a CMG exist? We got computer outside of our network, unable to access our network (no VPN access) that we want to add to a CMG. SCCM already have the client configuration to use CMG, but the location is unknown because it didn't exist at the time. Can we push a wmi entry or something (we can remote with skype in them)?
Thank you
Reply

Danny says:
July 16, 2020 at 7:59 pm
Hi,
Firstly let me thank you for your excellent job, your guides are awesome.
Actually we are implementing CMG but I've some concerns about the "Import Web server CMG certificate on the Primary Site Server". In this case you are creating a DNS for your domain but when you are importing the .pfx file to the CMG wizard it populates the services with yourname.cloudapp.net

Is required to create / match this DNS entry with the DNS created with de Azure Resource Group? In my company is required to create a CSR prior to create a CER file instead of using the common template issuing procedure.
Thanks in advance
Reply

Markussays:
June 19, 2020 at 2:55 pm
Hi, first of all thank you for all of your guides. They are so what of helpful for someone like me that I call myself a Rookie. And exatly this is why I am asking a professional for help.
Please have in mind I have said I am a rookie and have linited know how in troubleshooting ☹
Microsoft.ClassicCompute and Microsoft.Storage resource is registered
Under APP Registration/API Authorization I do have following entries for the SERVER APP
Microsoft Graph => Directory Read all => Administrator consent YES => granted for my enterprise
I do have a resource group in my case named CMG. But inside of this group there is no entry.
I did follow this guide to create a CMG and get below errors.
My guess is that the Server APP has not enough or the right permissions. But I can't find any how to with the Azure portal view.
Thanks for any support.
Markus
Azure Monitor
List Storage Account KeysEreignis initiiert von
SCCM Server APP
Fehlercode
ResourceNotFound
Meldung
The Resource 'Microsoft.Storage/storageAccounts/cmg' under resource group 'CMG' was not found. For more details please go to https://aka.ms/ARMResourceNotFoundFix
(PLEASE do not point me to this link as I do not have any idea how to check on all points)
CloudMgr.log:
ERROR: Resource Manager – Failed to list keys for storage service cmg with status code NotFound. Check [Monitor/Activity log] on Azure Portal for more information SMS_CLOUD_SERVICES_MANAGER 19.06.2020 09:27:34 18748 (0x493C)
ERROR: Exception occured during monitoring of service cmg : Exception Hyak.Common.CloudException: Failed to start deployment slot~~ bei Microsoft.ConfigurationManager.AzureManagement.ResourceManager.GetStorageServiceKey(String resourceGroupName, String storageServiceName)~~ bei Microsoft.ConfigurationManager.CloudServicesManager.ServiceMonitorTask.MonitorCloudDistributionPoint() SMS_CLOUD_SERVICES_MANAGER 19.06.2020 09:27:34 18748 (0x493C)
STATMSG: ID=9429 SEV=E LEV=M SOURCE="SMS Server" COMP="SMS_CLOUD_SERVICES_MANAGER" SYS=SC1.xy.com SITE=MSW PID=13240 TID=18748 GMTDATE=Fr. Jun 19 07:27:34.622 2020 ISTR0="cmg" ISTR1="Failed to start deployment slot" ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=1 AID0=404 AVAL0="["Display=\\cmg.xy.com\"]MSWNET:["SMS_SITE=MSW"]\\cmg.xy.com\" SMS_CLOUD_SERVICES_MANAGER 19.06.2020 09:27:34 18748 (0x493C)
WARNING: Warning: Exception during cloud service monitoring task for service cmg SMS_CLOUD_SERVICES_MANAGER 19.06.2020 09:27:34 18748 (0x493C)
WARNING: Exception Hyak.Common.CloudException:Failed to start deployment slot SMS_CLOUD_SERVICES_MANAGER 19.06.2020 09:27:34 18748 (0x493C)
WARNING: Stack trace: bei Microsoft.ConfigurationManager.AzureManagement.ResourceManager.GetStorageServiceKey(String resourceGroupName, String storageServiceName)~~ bei Microsoft.ConfigurationManager.CloudServicesManager.ServiceMonitorTask.MonitorCloudDistributionPoint()~~ bei Microsoft.ConfigurationManager.CloudServicesManager.ServiceMonitorTask.Start(Object taskState) SMS_CLOUD_SERVICES_MANAGER 19.06.2020 09:27:34 18748 (0x493C)
Reply

Markussays:
July 4, 2020 at 2:15 pm
HI
is my case no resolvable?
THX Markus
Reply

Naeem Mohammadsays:
September 24, 2020 at 8:30 pm
Hi Markus, Did u not get that resolved? I am having the same issue just now ☹ . does anyone else knows how to resolve this issue?
Reply
Markussays:
September 25, 2020 at 12:49 pm
Yes I could manage it to finalize the installation. It had to do with the cloud gateway service name. It has to be uniq. You can check this in Azure.
Reply
jean-sebastien Fsays:
June 8, 2020 at 11:20 pm
Hello. First off, thanks for this guide and all of the other post you do, it's really a lot of good and detailed information in this big world that is Microsoft.

Now, I got a simple question that I'm unsure how to answer myself. Currently, I got these site and roles

Site server with Service connection point (used for WSfB sync)
SUS server connected to SCCM (all updates are managed through sccm, no WUFB)
DPs, 1 for VPN connected users with speed throttling
Database server
Remote Content Library servers
Reporting Server

Now, I'm planning CMG deployment. Per the guide and others I've found out, do I need new servers? My current SUS server allow only SSL Intranet connection and I don't have the option to allow Internet Connection (maybe because I don't manage any Internet Connected computer that the option is grayed out). Do I need to create a new one that the CMG SUS role will sync to? Doing so, I guess I should used shared database WSUSDB?

For the other connection, is it better to host it on a seperate server?

Thank you!
Reply

Jeff Scharfenbergsays:
June 5, 2020 at 7:29 pm
One question, If I have a global need, can I add more connection points globally? Say 1 in APAC, 1 in Austrailia for better response? Like a normal distribution point?
Reply

Prajwal Desaisays:
July 4, 2020 at 7:22 pm
yes you can setup multiple CMG's.
Reply

Dustin Mobleysays:
May 30, 2020 at 7:44 am
Our CMG is up and running and successfully switching between Internet and Intranet. My question is what/how does it know to switch between internet and Intranet
Reply
Andrew Lysays:
May 25, 2020 at 9:52 pm
Hello Prajwal,
some reason I try multiple time create CMG in our ConfigMgr 2002 keep fail with status error.
here ERROR: TaskManager: Task [AnalyticsCollectionTask: Service parklandcmg] has failed. Exception Hyak.Common.CloudException, Failed to start deployment slot.
Is there anything you could help?
Reply
Shannonsays:
May 22, 2020 at 12:13 am
We currently don't have full PKI, but working towards it on our infrastructure. With that we went EHTTP on ConfigMgr 2002. How would you configure the MP in that scenario? We did use a PKI cert though on our CMG w/trusted root CA, and trying to use the new Bulk Token Registration, but we are failing to get the client installed. Also, in your guide above, I didn't see any mention of configuring DNS. If full PKI, do you need to configure CNAME record on internal and public facing DNS, or just public facing?

Reply

Paragsays:
March 20, 2021 at 5:24 pm
Hello Shannon,
Hope CMG is working for you.
Could you please help me to know on where exactly we need to create CNAME record?
Is it in public DNS & internal DNS or only public DNS.
Also what all entries we need to mentioned in Full DN & DNS field while importing CMG certificate.
Reply

Narendiransays:
May 7, 2020 at 11:58 am
Thank you for the post. really helpful. I just have a small hickup. All process completed but I am having the issue of the client not able to see the FQDN of the cloud DP in the configuration manager.
Reply

Santoshsays:
April 17, 2020 at 6:56 pm
Can i configure CMG on non PKI infra. As we don't have PKI setup and all are client Certificate is Self Signed Certificate.
Reply

Paulsays:
April 1, 2020 at 3:08 pm
Thanks for the write up, was very helpful. I have the CMG up and running and serving content. One issue I am having is with VPN users. I created a boundary and group based on the VPN IP range. It works but not if someones home physical IP address overlaps with one of the other internal company network boundary ranges. It seems SCCM sees more than one IP address from the client, the VPN adapter address and the machines local home wireless network IP. I find that if that home wireless IP overlaps an internal boundary IP range assigned to an internal DP, then it ignores the VPN boundary. Anyone have any experience on this issue? For now I blocked VPN users from being able to access some of those internal DPs and set fallbacks to the CMG, It works but certainly not a perfect solution.
Reply

Davidsays:
April 1, 2020 at 2:40 pm
How do you create a trusted root certificate?
When i import the CMG certificate it says: "The certificate is not a valid root"
Reply

Mathias Ottsensays:
April 1, 2020 at 1:18 pm
I keep getting this error on my trial environment:
{
"code": "DeploymentFailed",
"message": "At least one resource deployment operation failed. Please list deployment operations for details. Please see https://aka.ms/DeployOperations for usage details.",
"details": [
{
"code": "BadRequest",
"message": "{\r\n \"error\": {\r\n \"code\": \"OperationFailed\",\r\n \"message\": \"The operation '62b5e2289f8a7231870fdcf54f64ee3a' failed: 'The requested VM tier is currently not available in Central US for this subscription. Please try another tier or deploy to a different location.'.\"\r\n }\r\n}"
}
]
}
I've tried several other regions like:
South Central
North Europe
East US
Reply

Guilhem Clercsays:
April 9, 2020 at 1:48 pm
Have you find a solution for this one?
Reply

Mathiassays:
May 28, 2020 at 4:37 pm
Microsoft have disabled the function on trial environments. You need to upgrade to pay as you go
Reply

Z Ssays:
April 11, 2020 at 1:55 pm
I am experiencing same problem. I have tried every region and upgraded my Trial to Pay-As-You-go.
Reply

WeWantToDeployCMGTtoosays:
April 21, 2020 at 3:09 pm
We run into the same problem. We tried multiple regions EU and US and they always

fail with the same error message. When I try to deploy an A2_V2 VM manually then it deploys just fine. We have opened a support ticket at Microsoft about a week ago, but no solution yet. Anyone got this fixed?
Reply
Joseph Martinsays:
March 26, 2020 at 11:36 pm
What in your opinion or MS's is the optimal Check in Frequency for a partial CMG Environment.
Reply
Vagner Oliveirasays:
March 26, 2020 at 8:58 pm
@Prajwal, would you have any topology for implementing this CMG + Azure + SCCM configuration?
Reply
BackupMonkeysays:
March 12, 2020 at 10:40 pm
How do you get past when you import the cert that the 'Service Name' is always the site server name. The cert has the correct details but SCCM (1910) won't populate the 'Service Name' nor the 'Deployment name' with anything other than the site server name?
Doh! Fixed. Used the wrong template ☹
Reply
Dave Smithsays:
March 5, 2020 at 12:55 pm
I have followed these steps but always receive the error message "Failed to provision cloud service" error while setting up the SCCM Cloud Management Gateway (CMG) within my SCCM 1902 environment.
What steps can I take to determine what is causing this error so that I can fix it?
Reply
Ian Harrissays:
March 17, 2020 at 9:32 pm
Which region did you select to deploy to ?
Reply
Ian Harrissays:
March 17, 2020 at 9:33 pm
I would look at your Azure activity log
https://portal.azure.com/#blade/Microsoft_Azure_ActivityLog/ActivityLogBlade
This might give a clue, look at for the red errors.
Reply
Mathias Ottsensays:
March 31, 2020 at 3:50 pm
Had the same issue looking at the Azure activity log it said that i was missing resource Microsoft.ClassicCompute.
I had to go to subscriptions > Resource providers > Find microsoft.classicCompute > Press register
I guess if you create a trial subscription it will not automatically register.
After this you will need to delete and recreate the CMG in the SCCM console
Reply
Dave Smithsays:
March 3, 2020 at 6:34 am
I have followed the instructions in this posting but when I get to the "Create Cloud Management Gateway Wizard" portion and import the certificate file I get a message that says "The service certificate has the following errors/warnings.
[Warning] The service certificate has a wildcard DNS name. Ensure you update the Service CName with the correct FQDN."
How can I fix this?
How can I post a screenshot of this error message?
Reply
Dave Smithsays:
March 4, 2020 at 9:29 am
Here is a screenshot that shows the error I am receiving: https://imgur.com/6bqSpne
Reply
Ian Harrissays:
March 17, 2020 at 9:34 pm
link dead
Reply
Manuel Arcesays:
February 21, 2020 at 8:01 pm
Hello I followed the step by step but when I tried to create the CMG I get this message.
"A valid Azure AD App is required. Please Deploy the Azure Service for Cloud Management First."
Any ideas?
Reply
Tushar Singhsays:
April 6, 2020 at 3:05 am
Same for me…
Reply
Aad Lutgertsays:
September 30, 2020 at 11:20 pm

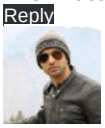
I had the same issue. I solved this by first adding the “Cloud Management” service in Azure Services.
Reply
Ian Harris says:
February 14, 2020 at 8:56 pm
Just a word of warning, make sure the CDP server name is NOT the same as your primary site name.
Reply
Ian Harris says:
February 14, 2020 at 8:17 pm
Add Site System Roles. option is greyed out when I try and add the role, I have run the console as admin and also tried the original installer account..
One thing that I have read is that the FQN of the server cannot be the same as the FQN of the CMG, and some suggest to remove the CMG and start again, however some people have said this will cause additonal issues ☹
Reply
Ian Harris says:
March 17, 2020 at 9:36 pm
Rolled back server to previous VM snapshot, something odd happened to our SCCM during deployment of CMG.
Reply
Randy says:
January 24, 2020 at 1:30 pm
InfoSec wants a layer of protection between the CMG and the on premise systems so what specific ports should we allow to build proper ACL’s?
Reply
Prajwal Desai says:
March 22, 2021 at 8:04 pm
I have covered that info under CMG ports section.
Reply
Mark Rogalski says:
September 18, 2019 at 1:36 am
Between the instructions:
“In the Certificate Properties dialog box, under for Subject name, select Type as Full DN. Under Alternative name, select Type as DNS and enter the service name.”
AND
“Enter a public DNS name that you want to use with CMG. So I will enter *.prajwal.org here which allows me to use any subdomain for CMG.”
I think you forgot to insert a screenshot, I could use an illustration for each step as my CMG cert seems to continue to fail or prompt errors when using as described above.
Reply
Sagar Mane says:
September 7, 2019 at 8:28 pm
We are having SCCM 1902 and configured CMG
So
Can we install sccm client in workgroup machines in CMG ?(machines which are not in Azure AD but connected to internet)
Reply
Sagar Mane says:
September 7, 2019 at 6:55 pm
Sir
thanks for this documents with SCCM 1902
few questions related to Prerequisites
is it compulsory to have Azure AD (as we have Azure subscription but our machines are not registered in Azure AD)
we are implementing CMG to manage laptops (roaming user) which are in workgroup (not in domain and not in Azure AD)
so it is possible to manage workgroup machine in CMG ?
we are facing error while installing sccm client on workgoup Pc which is connected to internet
Reply
Jordan Spencer says:
September 4, 2019 at 10:48 pm
I am setting up CMG for the first time. I am getting the following error in the last part of connection analyzer and can’t figure it out.
Failed to get ConfigMgr token with Azure AD token. Status code is ‘500’ and status description is ‘CMGConnector_InternalServerError’. Google results don’t help too much with this error.
Reply
Prajwal Desai says:
March 22, 2021 at 8:03 pm
Make sure you bind the right web server certificate to IIS or make sure the correct root- and/or intermediate CA is added.
Reply
Nagayya P says:
September 4, 2019 at 3:34 pm
there is not proper documents in Microsoft website about using Wilcard domain name which is issued by public CA.

i have got wildcard certificate from public authority but am not able to authenticate from clients . the client requires Client authentication certificate which am struggling to find out

Reply

Prajwal Desaisays:
March 22, 2021 at 8:02 pm
The wildcard cert should work in all cases. It worked even in my case.

Reply



Rohit Chaudharysays:
September 2, 2019 at 6:55 pm
HI Prajwal,
I have configure the things but its giving me a error during provisioning. error : Failed to start deployment slot …. in cloudmgr.log

Reply

Prajwal Desaisays:
September 2, 2019 at 7:12 pm
Can i see the complete log file instead of just one line ?.

Reply

Jasonsays:
July 22, 2019 at 8:05 pm
I have a question for you, we already have a PKI certificate setup for our Distribution Points and utilize Https internally. Do I need to setup another cert or can I use the existing one we are using already. I am asking as our main reason for using the gateway will be to patch machines that are domain joined but they are not using VPN often enough to get patched. Any guidance here would be appreciated.

Reply

Prajwal Desaisays:
March 22, 2021 at 8:01 pm
If you already have PKI setup, it's well and good. All you need to do is configure the CMG certificates that's all.

Reply

Petesays:
July 22, 2019 at 5:22 am
Do you recommend using a Service Account with temp Global Admin privileges to setup the Azure AD link or does it require permanent global admin role?
Just curious if i need to use a global admin account just for setup then its done or to use the service account from SCCM with global admin?

Reply

Prajwal Desaisays:
March 22, 2021 at 8:00 pm
use a global admin account while setting up CMG. It saves your time.

Reply

Ehabsays:
July 20, 2019 at 4:50 pm
Thank you for your effort, I would like to ask something I have two MPs is it required to make them work over https both, or shall I create a new one dedicated for that and regarding to boundary group that will be used for CMG what is the boundary configured

Reply

Qnapsays:

July 19, 2019 at 2:38 pm
Great……. got it working at last ☺
Reply

Prajwal Desaisays:
March 22, 2021 at 7:59 pm
Glad to hear that.
Reply

Cesarsays:
July 18, 2019 at 7:48 pm
Great Post!! Thanks Prajwal!
Reply

Prajwal Desaisays:
March 22, 2021 at 7:59 pm
Glad to hear that.
Reply

Robert Schaafsays:
July 18, 2019 at 4:35 pm
Great document! Setting this up and make it work isn't too difficult if u got the certificates in order. The problem we are having is that our clients are not Azure AD joined so we use the certificate for authentication. However the client in the internet doesn't report the status back of an installation, the status message query stays empty and the deployment keeps the status in progress. Microsoft has confirmed this to be a bug but it surprises me that I can't find any document on the internet about this or that anyone has this problem. Anyone recognizes this?
Reply

Prajwal Desaisays:
July 19, 2019 at 11:06 am
Can you send me the link where Microsoft says this is a bug ?.

From <https://www.prajwaldesai.com/setup-sccm-cloud-management-gateway/>

Intune by bala(infosys)

Monday, August 16, 2021 5:40 PM

Contents

1. Intune Enrolment & BitLocker Pre-Requisites

1. User Licensing (User Action)

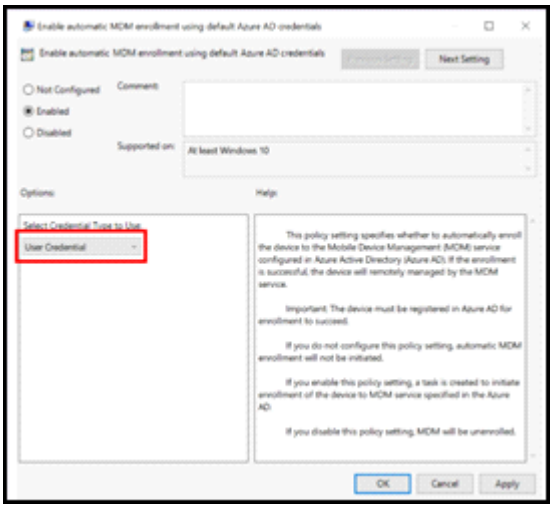
- Assign the user with Intune license (E3 / E5 / EMS)
- All NP licensed users are already added to the Azure AD group "**GR-CCNP-Intune-Win10-Enrolment**"
  - **NP new user**: Add the user to the Azure AD group "**GR-CCNP-Intune-Win10-Enrolment**"

2. Desktop / Laptop Domain Join (User Action)

- Ensure that the desktop / laptop has joins to the "**Workstation**" OU of Katmandu / Terai in the NP domain.

3. AD GPO for Intune enrolment (No User Action)

1. Active Directory (AD) Group Policy is created to trigger auto-enrollment to MDM for Active Directory (AD) domain-joined devices and linked to the "**Workstation**" OU of Katmandu / Terai in the NP domain.



2. The enrollment into Intune is triggered by a group policy created on the NP Active Directory and runs as scheduled task without any user interaction. Task can be found in

   Task Scheduler -> Microsoft -> Windows -> EntepriseMgmt

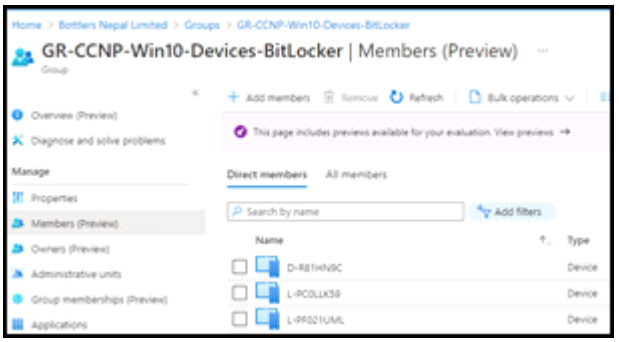
3. To verify the Intune MDM enrolment GPO is applied successfully to the machine, Pls run the below command in Administrative command prompt

```
C:\>gpresult /r /scope:computer
```

4. BitLocker Configuration Enablement (User Action)

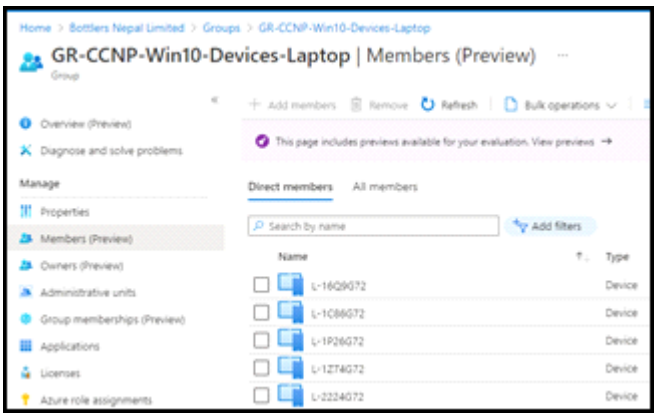
- To enable BitLocker **configuration**, add the devices (that needs BitLocker) to the Azure AD group

  "**GR-CCNP-Win10-Devices-BitLocker**"



5. BitLocker Compliance Policy (No User Action)

- BitLocker **compliance policy** is configured and pushed to the Laptop devices as per the dynamic group membership "**GR-CCNP-Win10-Devices-Laptop**" in Active Directory (AD)



2. **Intune Scenario 1** - Desktop / Laptop having BNL Image and do not have any SCCM client pre-installed

These devices are fresh BNL image install

- No SCCM client pre-installed
- No Bit Locker enabled

1. Azure AD Registration (No User Action)

1. Go to Azure Portal *(https://portal.azure.com)*
2. The device should be registered and available in Azure AD
3. The device enrolment in Intune shows “Microsoft Intune” in the **MDM** Column (sample shown below)

Note: It might takes 0-8 hours to reflect the AD registration status in the Azure portal.

2. Intune Enrolment (No User Action)

1. Go to Intune Portal (*https://endpoint.microsoft.com/)*
2. The device should be enrolled and available in Intune
3. The device enrolment in Intune shows “Intune” in the Managed By column (sample shown below)

Note: It might takes 0-8 hours to reflect the Intune device status in the Intune portal.

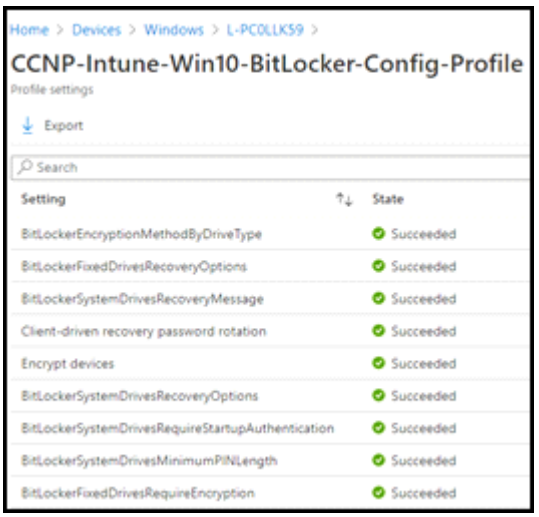
3. Bit Locker Enabling (User Action)

- Intune pushes the Bit Locker configuration to the laptops enrolled to Intune
    - Startup PIN is enabled and hence BitLocker must be manually triggered on

- Intune validates the Bit Locker compliance for the laptops enrolled to Intune
  Pre-Check:

  Wait for the BitLocker device configuration profile to appear as **succeeded** for the device in Intune.

Policy	User Principal Name	State
CCNP-Intune-Win10-BitLocker-Config-Profile	BMahato@coca-cola.com.np	Succeeded



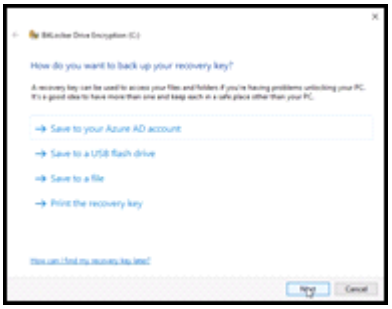
  After the policy is succeeded as shown in the above image, follow the steps below to enable Bitlocker on the BNL imaged laptops:

1. Go to My Computer -> C Drive -> Right Click –> Enable Bit Locker

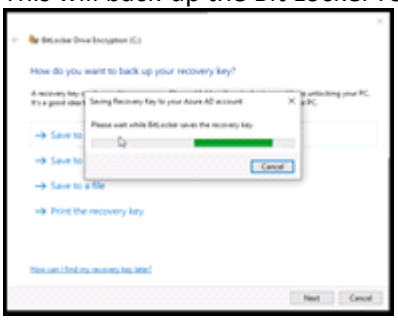
   Note: Ignore the Bit Locker pre-check pop-up, if it appears

2. Enter a 4 digit PIN.

3. Backup the recovery key to “Save to your Azure AD account”

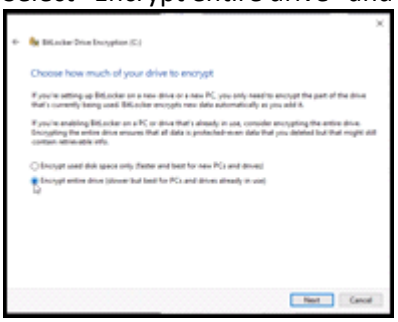


4. This will back-up the Bit Locker recovery key to the Azure AD Portal and Intune Portal



Note: Ignore the Bit Locker pre-check pop-up, if it appears

5. Select “Encrypt entire drive” and click Next



6. Wait for 1-2 hours for the full encryption to complete. User can continue their work while the encryption is progressing.

3. Intune Scenario 2 - Desktop / Laptop having BNL Image and have BNL SCCM client pre-installed

- SCCM client pre-installed. Clients are registered to BNL SCCM parent server
- Bit Locker enabled. Bit Locker configuration is enabled with startup PIN
- These devices will be registered with both BNL SCCM and Intune

1. Azure AD Registration (No User Action)

1. Go to Azure Portal *(https://portal.azure.com)*
2. The device should be registered and available in Azure AD
3. The device enrolment in Intune shows “System Center Configuration Manager” in the **MDM** Column (sample shown below)

***Note**: It might takes 0-8 hours to reflect the AD registration status in the Azure portal.*

2. Intune Enrolment (No User Action)

1. Go to Intune Portal (*https://endpoint.microsoft.com/*)
2. The device should be enrolled and available in Intune
3. The device enrolment in Intune shows “Co-managed” in the **Managed By** column (sample shown below)

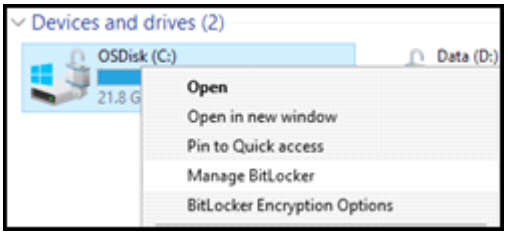
***Note**: It might takes 0-8 hours to reflect the Intune device status in the Intune portal.*

3. Bit Locker Recovery Key Backup (User Action)

- No changes needed to the existing BitLocker configuration
- Intune will validate the BitLocker compliance for the laptops enrolled to Intune

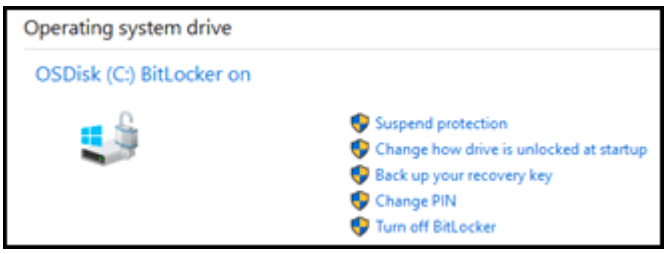
Follow the steps to backup the Bitlocker to Azure AD and Intune portal:

1. Go to My computer -> Right click on **C Drive** -> Select **Manage Bit locker**

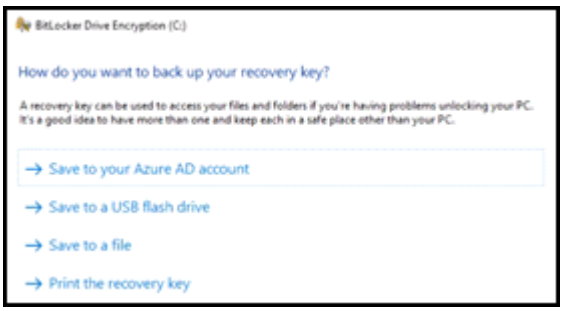


Note**: If Manage Bit Locker option is not available, Go to **Control Panel** and select **BitLocker Drive Encryption

2. Select “Backup your recovery key”



3.



Select “Save to your Azure AD / Cloud account”

4. Once saved, Exit the BitLocker screen

Note: *If the “Backup your recovery key” option is not available in both the above options, then select “Turn off BitLocker”. Wait for the disk decryption to complete. Restart the machine and enable BitLocker encryption again.*

4. Intune Scenario 3 - Desktop / Laptop have HCCBPL image

These devices are HCCBPL’s image installed

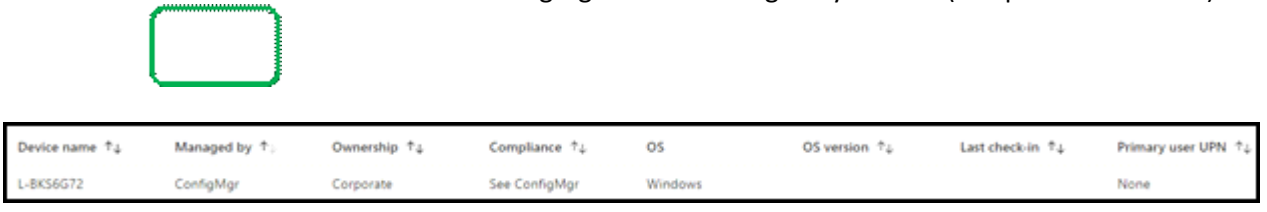
1. SCCM client pre-installed. Currently these clients are orphaned as the HCCBPL SCCM parent server cannot be contacted / registered.
2. Bit Locker enabled. Currently these Bit Locker configuration is enabled with startup PIN
3. **Special Machines:** [Bala1] TPM disabled in the BIOS and PIN not enabled. BitLocker enabled

1. Azure AD Registration (No User Action)

1. Go to Azure Portal *(https://portal.azure.com*)
2. The device should be registered and available in Azure AD
3. The device enrolment in Intune shows “None” in the **MDM** Column (sample shown below)

2. Intune Enrolment (No User Action)

1. Go to Intune Portal (*https://endpoint.microsoft.com/)*
2. The device will be listed in Intune but **NOT enrolled in Intune**
3. The device enrolment in Intune shows “ConfigMgr” in the Managed By column (sample shown below)



4. If the device is selected, all the device information will be unavailable.

Note: Intune **cannot manage this device**. This is due to the orphaned state of the SCCM client.

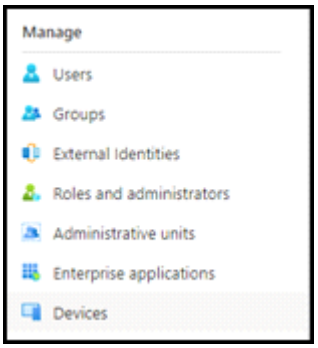
- All these machine scenarios, **can upload BitLocker keys to the Azure AD**, even though Intune enrollment is not successful.
- If BitLocker is already enabled, any changes to the BitLocker configuration will be applied only if the BitLocker is disabled (and disk fully decrypted) and enable BitLocker again

Action: *Use the steps provided in Appendix to remove the orphaned SCCM client and bring it to scenario 1/2*

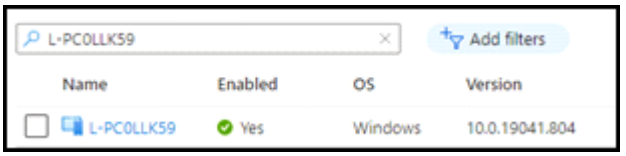
5. Verify Bit Locker Recovery Key Backup

1. Recovery key in Azure AD Portal (All domain joined devices and Azure AD Synced)

1. Go to Azure AD portal (https://portal.azure.com)
2. Select "**Devices**" on the left hand blade menu



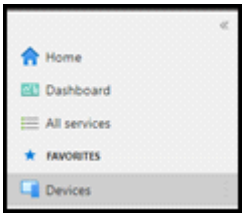
3. Search for the device in the search field



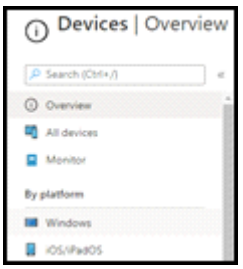
4. Select the device and the BitLocker recovery key will be shown as displayed below

2. Recovery key in Intune Portal (Only Intune enrolled devices)

1. Go to Intune Portal (https://endpoint.microsoft.com/)
2. Select “**Devices**” on the left hand blade menu

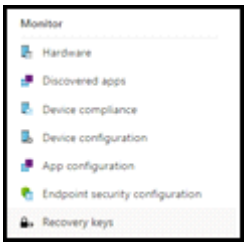


3. Select “**Windows**” on the platform menu

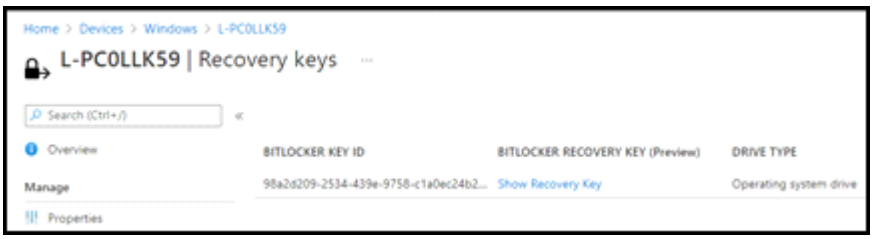


4. Search for the device in the search field and select the device

5. Select "**Recovery Keys**" on the Monitor menu



6. BitLocker recovery key will be shown as displayed below



6. Appendix A – Steps to cleanup SCCM client from HCCBPL image

Follow the below steps to un-install the SCCM client from existing HCCBPL imaged laptops / desktops.

1. Option 1: Native SCCM un-install method

1. Execute the below command in **Administrative command** prompt.

```
C:\>C:\Windows\ccmsetup\ccmsetup.exe /uninstall
```

2. On successful completion, perform the below command in **Administrative command** prompt.

```
C:\>gpupdate /force
```

3. On successful completion, restart the laptop / desktop and verify if the device is enrolled to Intune.

2. Option 2: Script based SCCM un-install method

1. Execute the following commands in PowerShell ISE as an **Administrator**.

~~~~~~

```
# Run SSCM remove
# $ccmpath is path to SCCM Agent's own uninstall routine.
$CCMpath = 'C:\Windows\ccmsetup\ccmsetup.exe'
# And if it exists we will remove it, or else we will silently fail.
```
~~~~~~

```
if (Test-Path $CCMpath) {
   Start-Process -FilePath $CCMpath -Args "/uninstall" -Wait -NoNewWindow
   # wait for exit
   $CCMProcess = Get-Process ccmsetup -ErrorAction SilentlyContinue
      try{
         $CCMProcess.WaitForExit()
         }catch{
         }
}
# Stop Services
Stop-Service -Name ccmsetup -Force -ErrorAction SilentlyContinue
Stop-Service -Name CcmExec -Force -ErrorAction SilentlyContinue
Stop-Service -Name smstsmgr -Force -ErrorAction SilentlyContinue
Stop-Service -Name CmRcService -Force -ErrorAction SilentlyContinue
# wait for services to exit
$CCMProcess = Get-Process ccmexec -ErrorAction SilentlyContinue
try{
   $CCMProcess.WaitForExit()
}catch{
}
 # Remove WMI Namespaces
Get-WmiObject -Query "SELECT * FROM __Namespace WHERE Name='ccm'" -Namespace root | Remove-WmiObject
Get-WmiObject -Query "SELECT * FROM __Namespace WHERE Name='sms'" -Namespace root\cimv2 | Remove-WmiObject
# Remove Services from Registry
# Set $CurrentPath to services registry keys
# $CurrentPath = HKLM:\SYSTEM\CurrentControlSet\Services
Remove-Item -Path HKLM:\SYSTEM\CurrentControlSet\Services\CCMSetup -Force -Recurse -ErrorAction SilentlyContinue
Remove-Item -Path HKLM:\SYSTEM\CurrentControlSet\Services\CcmExec -Force -Recurse -ErrorAction SilentlyContinue
Remove-Item -Path HKLM:\SYSTEM\CurrentControlSet\Services\smstsmgr -Force -Recurse -ErrorAction SilentlyContinue
Remove-Item -Path HKLM:\SYSTEM\CurrentControlSet\Services\CmRcService -Force -Recurse -ErrorAction SilentlyContinue
# Remove SCCM Client from Registry
# Update $CurrentPath to HKLM/Software/Microsoft
# $CurrentPath = HKLM:\SOFTWARE\Microsoft•
Remove-Item -Path HKLM:\SOFTWARE\Microsoft•\CCM -Force -Recurse -ErrorAction SilentlyContinue
Remove-Item -Path HKLM:\SOFTWARE\Microsoft•\CCMSetup -Force -Recurse -ErrorAction SilentlyContinue
Remove-Item -Path HKLM:\SOFTWARE\Microsoft•\SMS -Force -Recurse -ErrorAction SilentlyContinue
# Reset MDM Authority
# CurrentPath should still be correct, we are removing this key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DeviceManageabilityCSP
Remove-Item -Path HKLM:\SOFTWARE\Microsoft•\DeviceManageabilityCSP -Force -Recurse -ErrorAction SilentlyContinue
# Remove Folders and Files
# Tidy up garbage in Windows folder
$CurrentPath = $env:WinDir
Remove-Item -Path $CurrentPath\CCM -Force -Recurse -ErrorAction SilentlyContinue
Remove-Item -Path $CurrentPath\ccmsetup -Force -Recurse -ErrorAction SilentlyContinue
Remove-Item -Path $CurrentPath\ccmcache -Force -Recurse -ErrorAction SilentlyContinue
```

Remove-Item -Path $CurrentPath\SMSCFG.ini -Force -ErrorAction SilentlyContinue

Remove-Item -Path $CurrentPath\SMS*.mif -Force -ErrorAction SilentlyContinue

Remove-Item -Path $CurrentPath\SMS*.mif -Force -ErrorAction SilentlyContinue

~~~~~~

2. On successful completion, execute the below command in Administrative Command Prompt.

```
C:\>gpupdate /force
```

3. On successful completion, restart the laptop / desktop and verify if the device is enrolled to Intune.

Note: If none of the above method is successful, the device must be re-imaged with BNL image, to bring back the device to scenario-1 of Intune enrolment.

[Bala1]To be confirmed with Dinesh Ji.
~~~~~~