

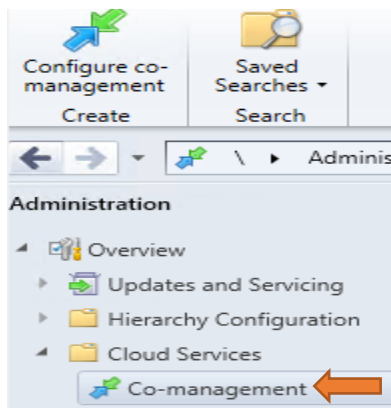
How to install Co-Management – Configuration Manager

In this post, I will show you the steps involved in deploying Co-Management within Current Branch 2006 (Configuration Manager). In the previous post we completed Cloud Management Gateway (CMG). With this we can tie Configuration Manager with Configuration Manager Admin Center in Cloud and Intune.

When you enable co-management, you can gain immediate value. Then once you're ready, you can start transitioning workloads as needed and if desired in your environment.

CO-MANAGEMENT SCCM 1902 PREREQUISITES

- Azure Subscription
- Azure Active Directory Premium
- Microsoft Intune subscription **OR** Enterprise Mobility + Security (EMS) subscription
- Client computer using [Hybrid Azure AD Joined](#) (domain + AAD joined) using [Azure AD Connect](#).



Co-management Configuration Wizard



Tenant onboarding

Tenant onboarding

- Configure upload
- Enablement
- Workloads
- Staging
- Summary
- Progress
- Completion

Microsoft Intune Subscription

Azure environment:

Sign in to Microsoft Intune with your Microsoft Intune organizational account

If you do not have a Microsoft Intune organizational account, you can subscribe a [Microsoft Intune](#) account portal

Upload to Microsoft Endpoint Manager admin center

Optionally import a separate web app to synchronize Configuration Manager client data to Microsoft Endpoint Manager admin center

Enable automatic client enrollment for co-management

[Read the Microsoft Intune privacy statement online.](#)
[Read the Configuration Manager privacy statement online.](#)

< Previous **Next >** Summary Cancel



Tenant onboarding

Tenant onboarding

Configure upload

Enablement

Workloads

Staging

Summary

Progress

Completion

Microsoft Intune Subscription

Azure environment: AzurePublicCloud

Sign in to Microsoft Intune with your Microsoft Intune organizational account [Sign In]

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

[x] Upload to Microsoft Endpoint Manager admin center

[] Optionally import a separate web app to synchronize Configuration Manager client data to Microsoft Endpoint Manager admin center

[] [Import]

[x] Enable automatic client enrollment for co-management

[Read the Microsoft Intune privacy statement online.](#)

[Read the Configuration Manager privacy statement online.](#)

[< Previous] [Next >] [Summary] [Cancel]

Create AAD Application



This action will register an application in the AAD tenant ramlan to authorize the synchronization of data to Intune. Do you want to continue?



Yes

No



Configure upload

Tenant onboarding

Configure upload

Enablement

Workloads

Staging

Summary

Progress

Completion

Configure upload to Microsoft Endpoint Manager Cloud Console

Devices

Select which devices to upload to Microsoft Endpoint Manager

[x] All my devices managed by Microsoft Endpoint Configuration Manager (recommended)

[] Specific collection

Collection: [] [Browse...]

[Learn more](#)

Endpoint Analytics

[x] Enable Endpoint Analytics for devices uploaded to Microsoft Endpoint Manager

[Learn More](#)

[< Previous] [Next >] [Summary] [Cancel]



Enablement

Tenant onboarding

Configure upload

Enablement

Workloads

Staging

Summary

Progress

Completion

Enable co-management

To enable co-management for devices managed by Configuration Manager, configure automatic enrollment in [Microsoft Intune](#).

[Learn more](#)

Automatic enrollment in Intune

Intune Auto Enrollment

Browse...

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

[Learn more](#)

```
CCMSETUPCMD="CCMHOSTNAME=RAMLANCMG.CLOUDAPP.NET/  
CCM_Proxy_MutualAuth/72057594037957956 SMSiteCode=TOR"
```

Copy

< Previous

Next >

Summary

Cancel

For Workload, I am leaving everything to default. Will reconfigure workload later.



Workloads

Tenant onboarding

Configure upload

Enablement

Workloads

Staging

Summary

Progress

Completion

Configure Workloads

Configuration Manager

Pilot Intune

Intune

Compliance policies:

Device Configuration:

Endpoint Protection:

Resource access policies:

Client apps:

Office Click-to-Run apps:

Windows Update policies:

< Previous

Next >

Summary

Cancel

For Staging will do it later.

Co-management Configuration Wizard

Staging

Tenant onboarding
Configure upload
Enablement
Workloads
Staging
Summary
Progress
Completion

Configure roll out collections

[Learn more](#)

Compliance policies:	<input type="text"/>	<input type="button" value="Browse..."/>
Device Configuration:	<input type="text"/>	<input type="button" value="Browse..."/>
Endpoint Protection:	<input type="text"/>	<input type="button" value="Browse..."/>
Resource access policies:	<input type="text"/>	<input type="button" value="Browse..."/>
Client Apps:	<input type="text"/>	<input type="button" value="Browse..."/>
Office Click-to-Run apps:	<input type="text"/>	<input type="button" value="Browse..."/>
Windows Update Policies:	<input type="text"/>	<input type="button" value="Browse..."/>

< Previous Next > Summary Cancel

Co-management Configuration Wizard

Summary

Tenant onboarding
Configure upload
Enablement
Workloads
Staging
Summary
Progress
Completion

Confirm the settings

Details:

- Azure environment: AzurePublicCloud
- Import data to Intune for cloud console: True

Data Upload

- Collection to upload: All devices

Enablement

- Devices to auto-enroll into Microsoft Intune: Configuration Manager

Workloads Configuration

- Compliance policies: Configuration Manager
- Device Configuration: Configuration Manager
- Endpoint Protection: Configuration Manager
- Resource access policies: Configuration Manager
- Client apps: Configuration Manager
- Office Click-to-Run apps: Configuration Manager
- Windows Update policies: Configuration Manager

Staging

- Compliance policies Pilot group: None
- Device Configuration Pilot group: None
- Endpoint Protection Pilot group: None


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

< Previous **Next >** Summary Cancel

Co-management Configuration Wizard

Completion

Tenant onboarding
Configure upload
Enablement
Workloads
Staging
Summary
Progress
Completion

 **The Co-management Configuration Wizard completed successfully**

Details:

- Tenant onboarding
 - Azure environment: AzurePublicCloud
 - Import data to Intune for cloud console: True
- Data Upload
 - Collection to upload: All devices
- Enablement
 - Devices to auto-enroll into Microsoft Intune: Configuration Manager
- Workloads Configuration
 - Compliance policies: Configuration Manager
 - Device Configuration: Configuration Manager
 - Endpoint Protection: Configuration Manager
 - Resource access policies: Configuration Manager
 - Client apps: Configuration Manager
 - Office Click-to-Run apps: Configuration Manager
 - Windows Update policies: Configuration Manager

To exit the wizard, click Close.

< Previous Next > Summary **Close**

Azure Active Directory Tenants 1 items			
Tenant Name	Tenant ID		
ramlan	5E11113D-DA15-40E6-B616-07C2F4956166		

Applications			
Application Name	Tenant ID	Client ID	Secret Key Expiry (UTC)
Configuration Manager Client App	16777217	dda513a6-1345-4ffe-8130-7835a6403d3f	
Configuration Manager Server App	16777217	6a348579-aca6-4503-a712-eb52ca3bcdfa	05-Oct-2022 4:27 PM
ConfigMgrSvc_b708273c-f54b-4e17-aad4-b25caa7e49d9	16777217	e6de1694-7069-4de5-8318-1735365e82e7	06-Oct-2021 7:03 PM

CLIENT SETTINGS

The Client Cloud Services node in the client settings policy allows you to configure devices to automatically register in Azure Active Directory instead of using a GPO as was previously necessary.

Open a Client Settings policy and select Cloud Services.

Set Automatically register new Windows 10 domain joined devices with Azure Active Directory to Yes then Click OK.

Default Settings

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

Specify if client computers can use cloud-based services.

Device Settings

- Automatically register new Windows 10 domain joined devices with Azure Active Directory: Yes
- Enable clients to use a cloud management gateway: Yes

Device/User Settings

- Allow access to cloud distribution point: Yes

We have completed Co-Management implementation. In order to tie with Intune, we need one of these licenses.

In order to have full access to Intune features and functionalities, you'll need an Intune licence. Below is a list of all the licenses containing the Intune features and functionalities.

- Intune
- Microsoft 365 E5
- Microsoft 365 E3
- Enterprise Mobility + Security E5
- Enterprise Mobility + Security E3
- Microsoft 365 Business Premium
- Microsoft 365 F1
- Microsoft 365 F3
- Microsoft 365 Government G5
- Microsoft 365 Government G3

As of now, I don't have any. So, I am unable to show or take screen shot. Will have another blog later to cover Intune and Configuration Manager Endpoint Admin Center in the cloud.

Thanks

Ram Lan

8th Oct 2020