

# Tenant Attach Guide for SCCM Logs Data Flow Troubleshooting Intune



In [Configuration Manager, production version 2002](#), Microsoft introduced a new feature called “**Tenant attach**.” With this feature, you can synchronize ConfigMgr agents to Intune without enrolling in Intune. Once synchronized, the ConfigMgr device will be visible in **Microsoft Endpoint Manager Admin Center (MEMAC)**.

The key point is that the ConfigMgr client is in Intune console without enrolling in Intune. This means your ConfigMgr managed device does not need co-managed to avail of some Cloud benefits.

You can refer to more details on Tenant attach troubleshooting details from the blog post-[SCCM Tenant Attach Background Process Walkthrough via Logs](#).



**Related Posts** – [SCCM 2002 Installation Step By Step Guide | MEMCM | ConfigMgr & PowerShell Script To Enable Opt-In Version Of SCCM 2002 Early Update Ring](#)

## Introduction

Both tenants attached and [co-managed devices](#) will be visible in a single MEMAC console, but they are not the same.

- Co managed device = SCCM agent + Intune enrolled
- Tenant attach device = SCCM agent synced to MEM (Not Intune enrolled)

The co-managed device got many more options available in Microsoft Endpoint Manager Admin Center (MEMAC). However, we can expect a lot more features for tenant-attached devices in the MEMAC console in the future. Below are some of the cloud benefits ConfigMgr tenant attach provide:

- Single Microsoft Endpoint Admin Console (MEMAC) to manage ConfigMgr and intune devices.
- ATP Integration
- Helpdesk troubleshooting
- User Experience Analytics
- Web front-end [CMPivot](#)

**Note:** Above listed benefits announced in ignite 2019 are not yet available to the public. Only limited features are available at the time of writing. We will discuss some of the features currently available.

## Prerequisites

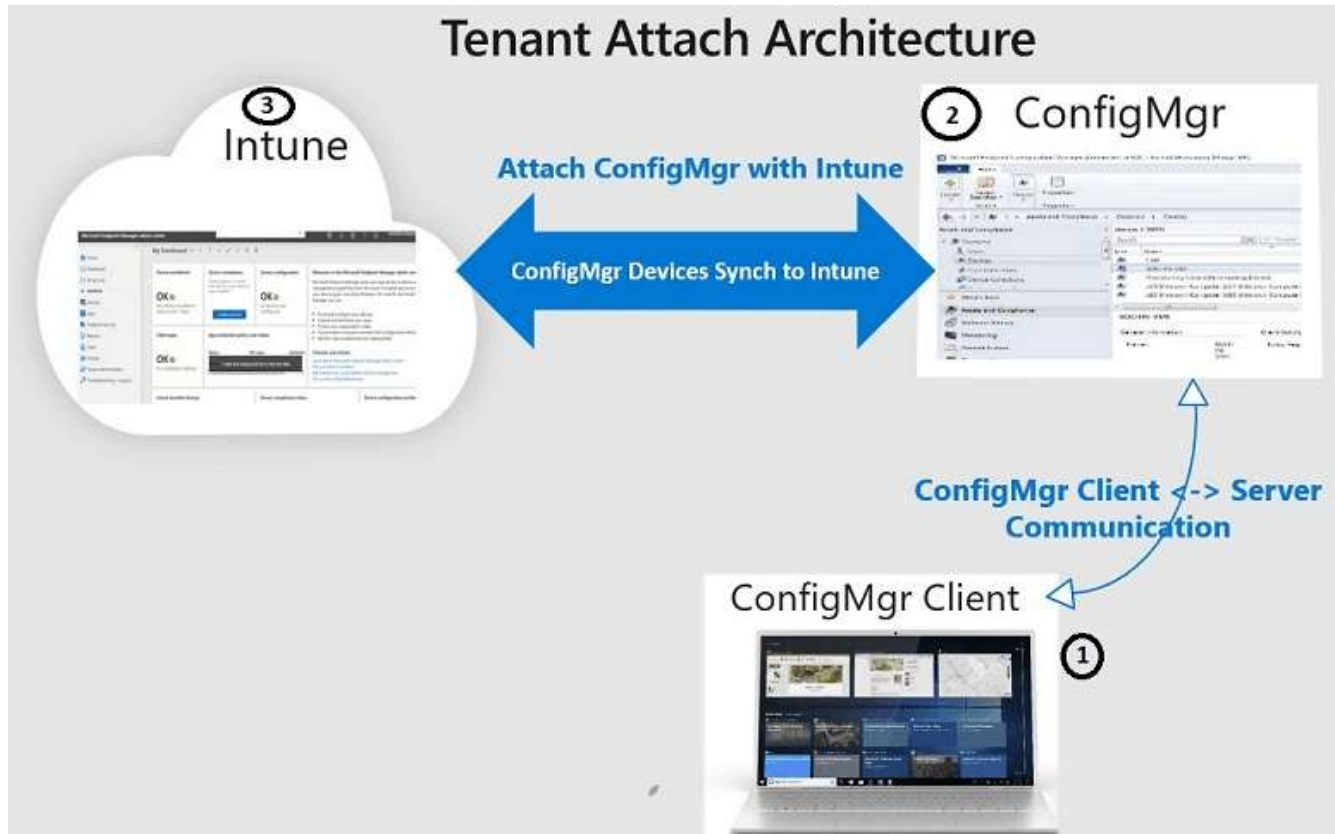
More updated details about prerequisites are given in [Microsoft docs](#).

- Appropriate access to SCCM infra (Full Admin preferably)
- Recommended to perform this activity from the Tier 1 server in ConfigMgr Hierarchy (CAS) or standalone primary server
- *Global Administrator* account for signing in the **Tenant onboarding** page (configuration in SCCM).
- An Azure public cloud environment.
- The user account triggering device actions has the following prerequisites:
  - Discovered with [Azure Active Directory user discovery](#)
  - Discovered with [Active Directory user discovery](#)
  - The **Notify Resource** permission under **Collections** object class in Configuration Manager.
  - On-Prem user synchronized to **azure using AADconnect**
- SCCM server should have access to below Internet endpoints
  - <https://aka.ms/configmgrgateway>
  - <https://gateway.configmgr.manage.microsoft.com>
  - <https://us.gateway.configmgr.manage.microsoft.com>
  - <https://eu.gateway.configmgr.manage.microsoft.com>

**NOTE!** – Permissions for Tenant attach is updated. You don't need to give permissions to *Configuration Manager Microservice* <https://docs.microsoft.com/en-us/mem/configmgr/tenant-attach/client-details#permissions>

## Tenant attach high level Architecture

There are three components in Tenant attach Architecture.



SCCM Tenant Attach Device Sync Architecture – Tenant Attach Guide for SCCM Logs Data Flow Troubleshooting Intune

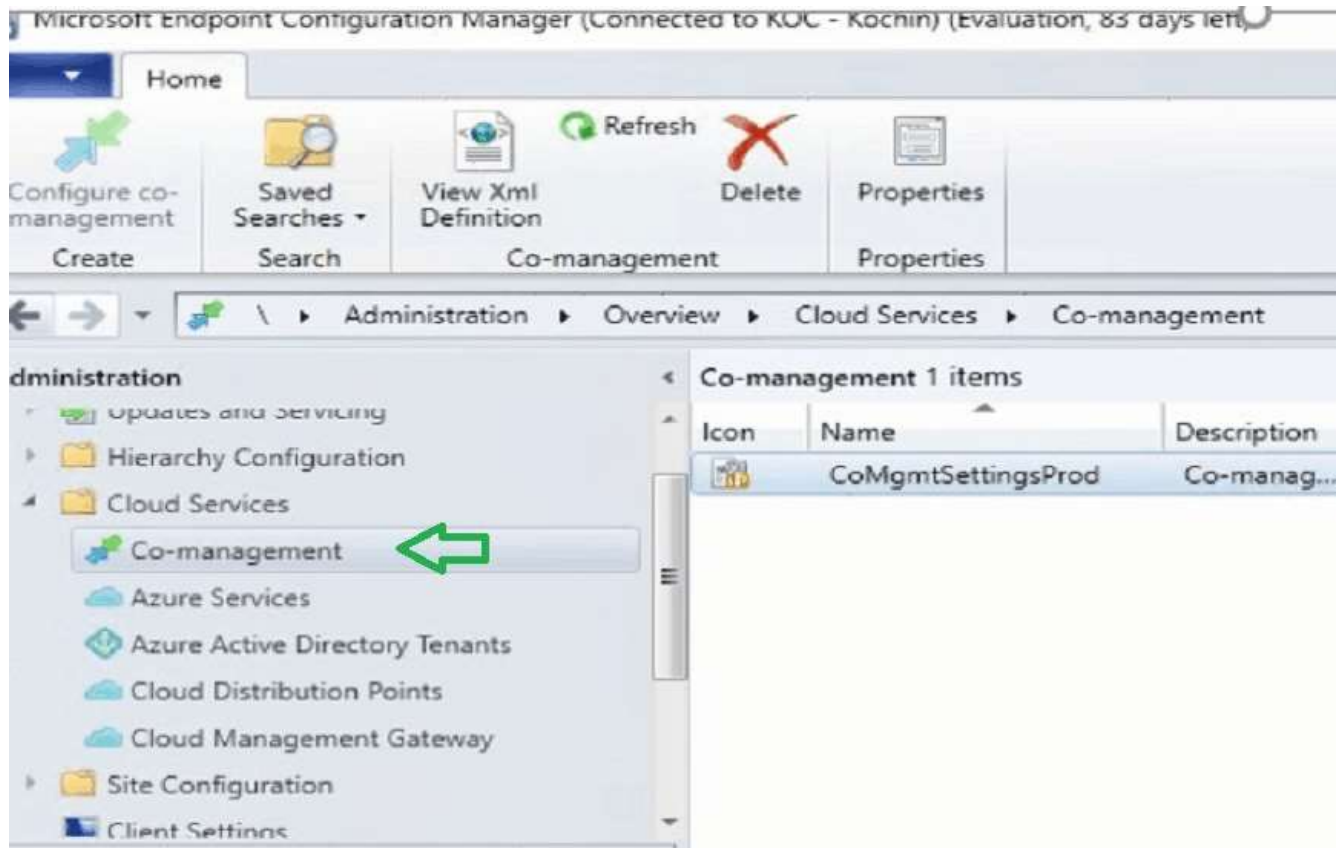
- ConfigMgr agent:
  - ConfigMgr client communicate with ConfigMgr server as normal.
  - There is no change. In addition, there is no need to enroll to Intune.
- ConfigMgr server:
  - ConfigMgr synchronizes devices to Microsoft Endpoint Manager Admin Center (MEMAC).
  - ConfigMgr server receive instructions from Microsoft Endpoint Manager Admin Center (MEMAC) and forward the instructions to ConfigMgr clients.
  - ConfigMgr server plays middleman between Intune and ConfigMgr client.
- Intune:
  - MEMAC console show the SCCM Devices synchronized from SCCM server to Intune.

Note: The entire ConfigMgr database will not be synchronized to Intune in this architecture. It is an on-demand architecture. MEMAC console connects to SCCM only when required or admin initiate action.

## How to configure Tenant Attach?

The configuration required for the tenant attach within the co-management wizard. If you have not enabled co-management wizard, follow the steps mentioned [here](#).

In Configuration Manager Admin console, go to **Administration > Overview > Cloud Services > Co-management**.



*SCCM Tenant Attach – CoMgmtSettingsProd – Tenant Attach Guide for SCCM Logs Data Flow Troubleshooting Intune*

Ensure your Azure environment is AzurePublicCloud. Tenant is boarded to azure by signing in using your *Global Administrator* account.

**Properties**

Tenant onboarding | Configure upload | Enablement | Workloads | Staging | Reporting

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 at Microsoft Intune account portal.

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

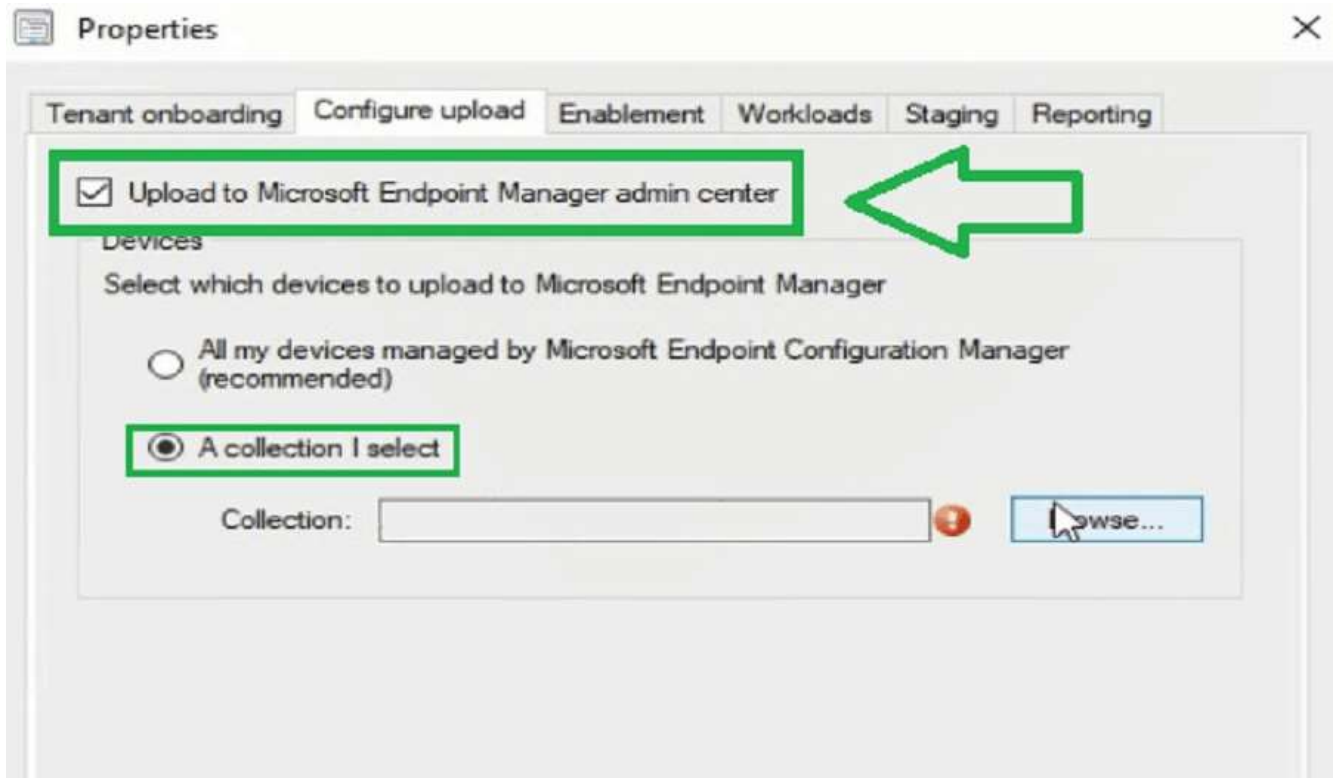
[Read the Configuration Manager privacy statement online.](#)

OK Cancel Apply

*Tenant Onboarding SCCM Infra – Tenant Attach Guide for SCCM Logs Data Flow Troubleshooting Intune*

Ensure you select the option “upload to MEM admin center.”

Please make sure you select a collection for which you want devices to synchronize. Its recommended selecting a test device collection to start with. Also, ensure you exclude the servers managed by ConfigMgr.



*Tenant Attach Guide for SCCM Logs Data Flow Troubleshooting Intune*

**Tenant attach sync setting has nothing** to do with [co-management](#). However, tenant attaches settings are available within the co-management wizard.

Note: I do not have any co-managed devices in my scenario, so I configured it as none for Intune enrollment. It would help if you decided on the configuration based on your scenario.

Properties

Tenant onboarding | Configure upload | Enablement | Workloads | Staging | Reporting

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


[Learn more](#)

Automatic enrollment in Intune: None

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](#)

 Please ensure the proper prerequisites are installed.

OK Cancel Apply

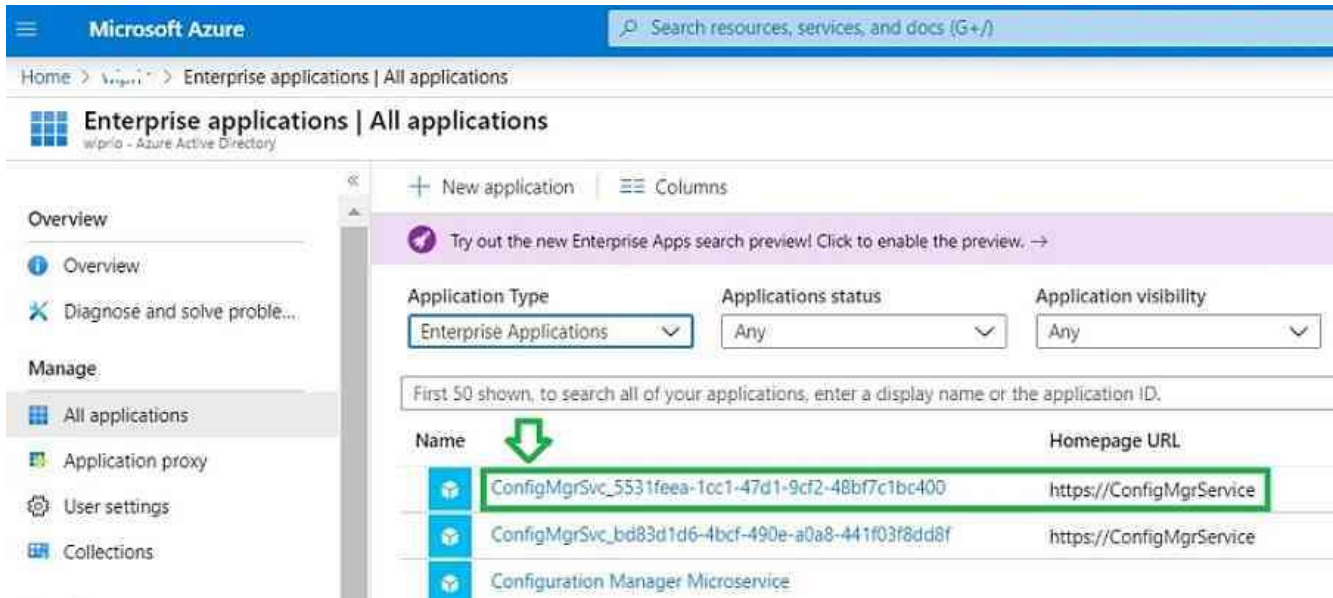
*Tenant Attach Guide for SCCM Logs Data Flow Troubleshooting Intune*

Below azure AD application gets created automatically after completing the configuration in ConfigMgr. You can see the events for troubleshooting from the log SmsAdminUI.log.

You can see the application name starts with "ConfigMgrSVC\_..."

The ConfigMgr server communicates with the cloud using this Azure AD Web application.





*Tenant Attach Guide for SCCM Logs Data Flow Troubleshooting Intune*

We completed the configuration. Let us discuss how the ConfigMgr server connects Intune and uploads the devices.

**NOTE!** – Let's add your admin user to this (**Configuration Manager Microservice**) enterprise app to get appropriate permissions to initiate SCCM actions from Intune portal.

- CMPivot
- Run Script
- Collections
- etc..

## Log Files – Troubleshooting

Let's see how log files can help troubleshoot the issue with device sync and tenant attach.

### ConfigMgr Device Upload to Intune Workflow

GatewaySyncUploadWorker.log :

This log tracks the connectivity between ConfigMgr and Intune. You can use this log to troubleshoot if ConfigMgr devices do not upload to the MEMAC console.

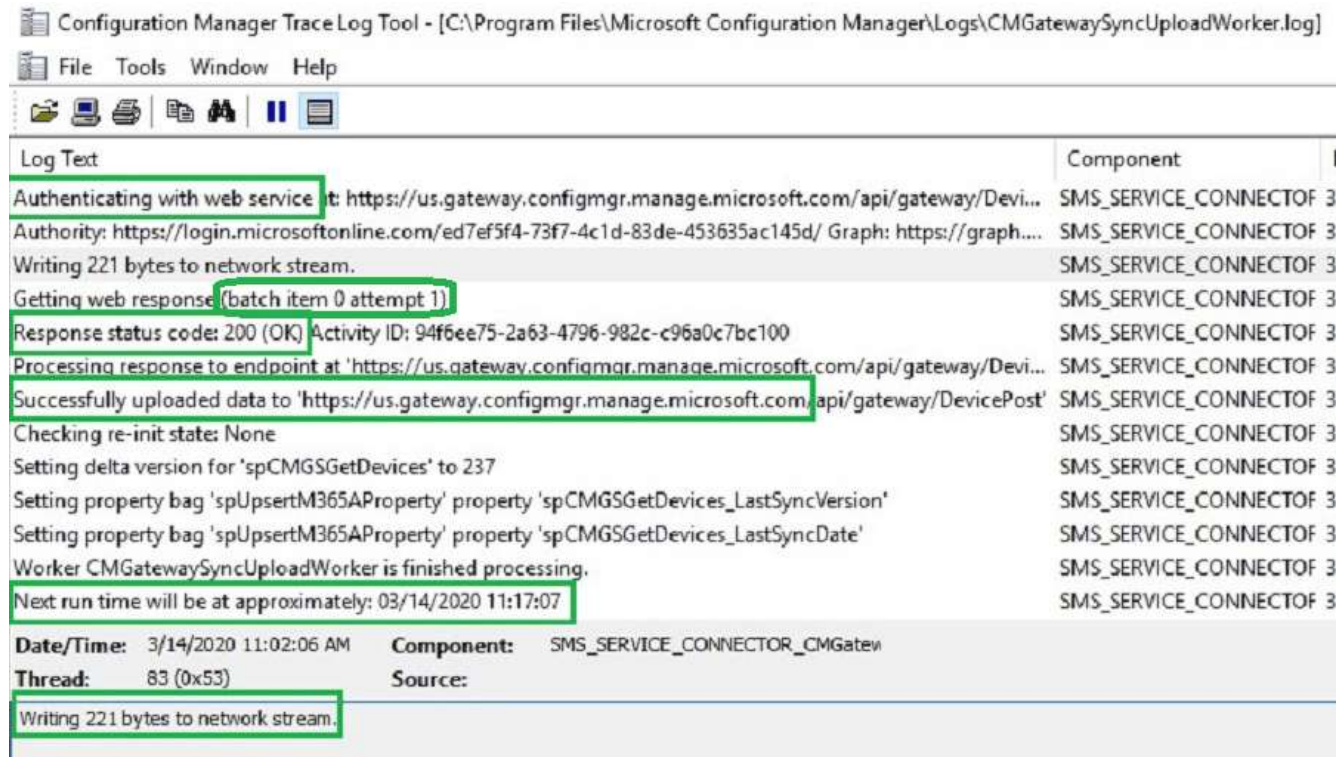
- ConfigMgr server selects the gateway to upload the device based on the location.
  - For the US the gateway URL is <https://us.gateway.configmgr.manage.microsoft.com>
  - For Europe gateway URL is <https://eu.gateway.configmgr.manage.microsoft.com>
- Next, the ConfigMgr server will authenticate and establish the connection.



- Once succeeded, ConfigMgr agent uploads to Intune through the gateway.
- You can see the ConfigMgr client records uploaded in batch

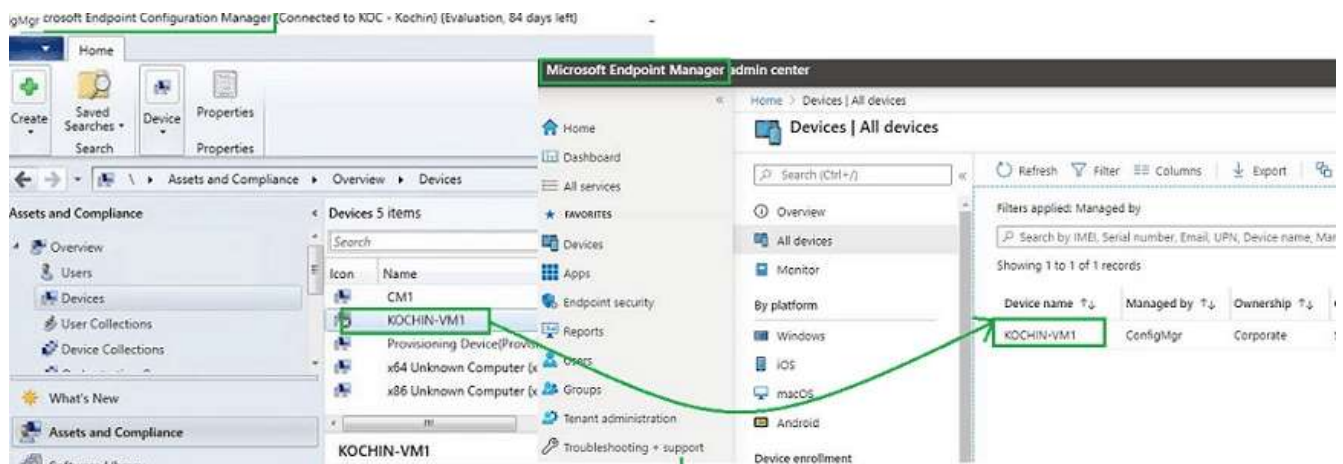
If you enable verbose logging, a log will tell the bytes written to the network for upload. Based on my testing, this network traffic is less. Moreover, the follow-up device synch will be delta only.

- The default upload sync interval is 15 min (delta)
- Response code 200 state the connection between ConfigMgr and Intune is successful



Tenant Attach Guide for SCCM Logs Data Flow Troubleshooting Intune 16

After successful upload, You can start seeing your ConfigMgr client in the Microsoft endpoint manager admin center console.



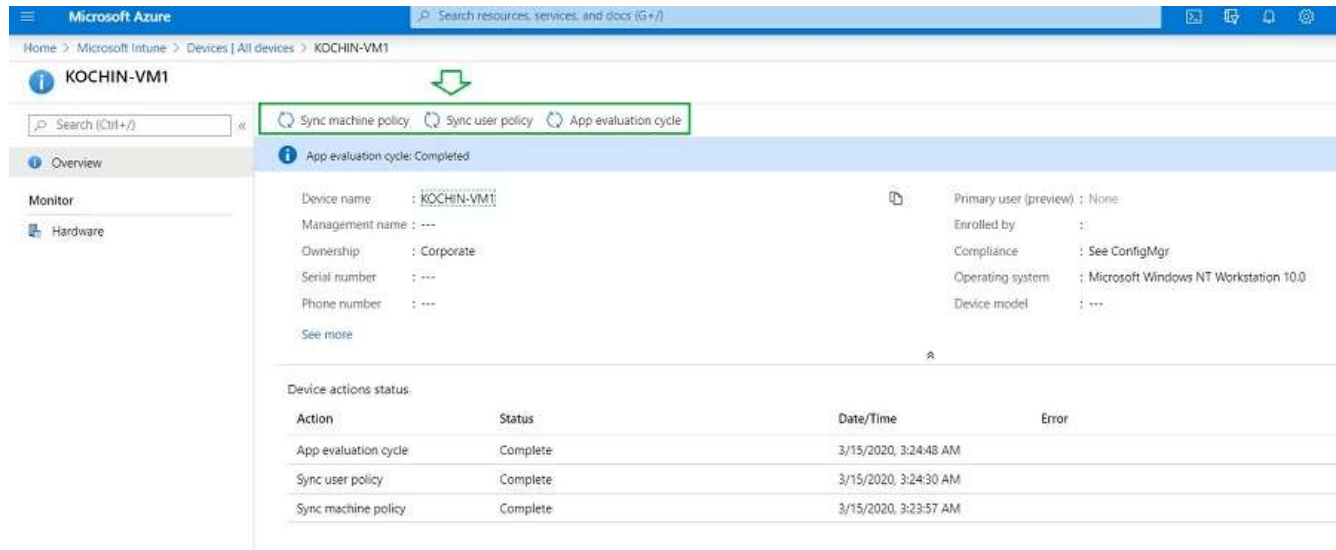
Tenant Attach Guide for SCCM Logs Data Flow Troubleshooting Intune

Until now, we discussed the device upload events from ConfigMgr to intune. Next, let us discuss the workflow from MEM admin console to ConfigMgr.

## Intune to SCCM event workflow

At the time of writing this post, only limited features are available in the MEM admin console for ConfigMgr clients, as listed below

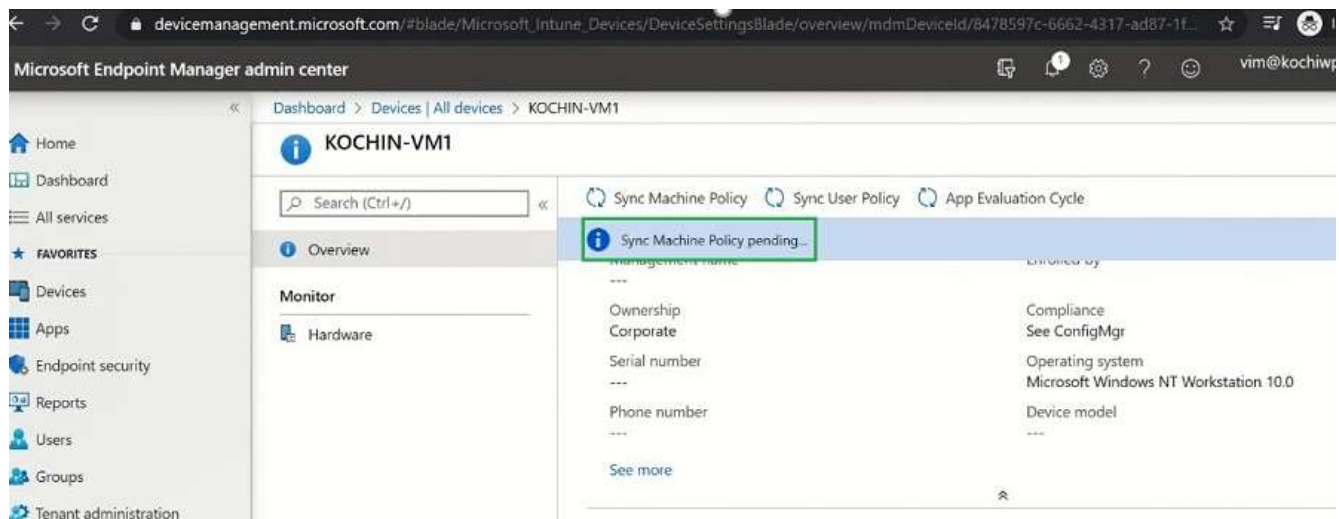
- **Machine policy synch**
- **User policy synch**
- **Application evaluation**



*Tenant Attach Guide for SCCM Logs Data Flow Troubleshooting Intune 17*

Let us see what happens when I trigger a machine policy from the MEM admin console. Below are the high-level activities

1. MEM admin console sent instruction for triggering machine policy to ConfigMgr server
  2. ConfigMgr server receive notification from MEM gateway and authenticate
  3. Forwards as BGB instruction and process
  4. ConfigMgr server sent the notification to ConfigMgr client
  5. ConfigMgr client receive the instruction from ConfigMgr server and process
- MEM admin console sent the machine policy instruction to the ConfigMgr server. Initially, you can see the status will show pending.

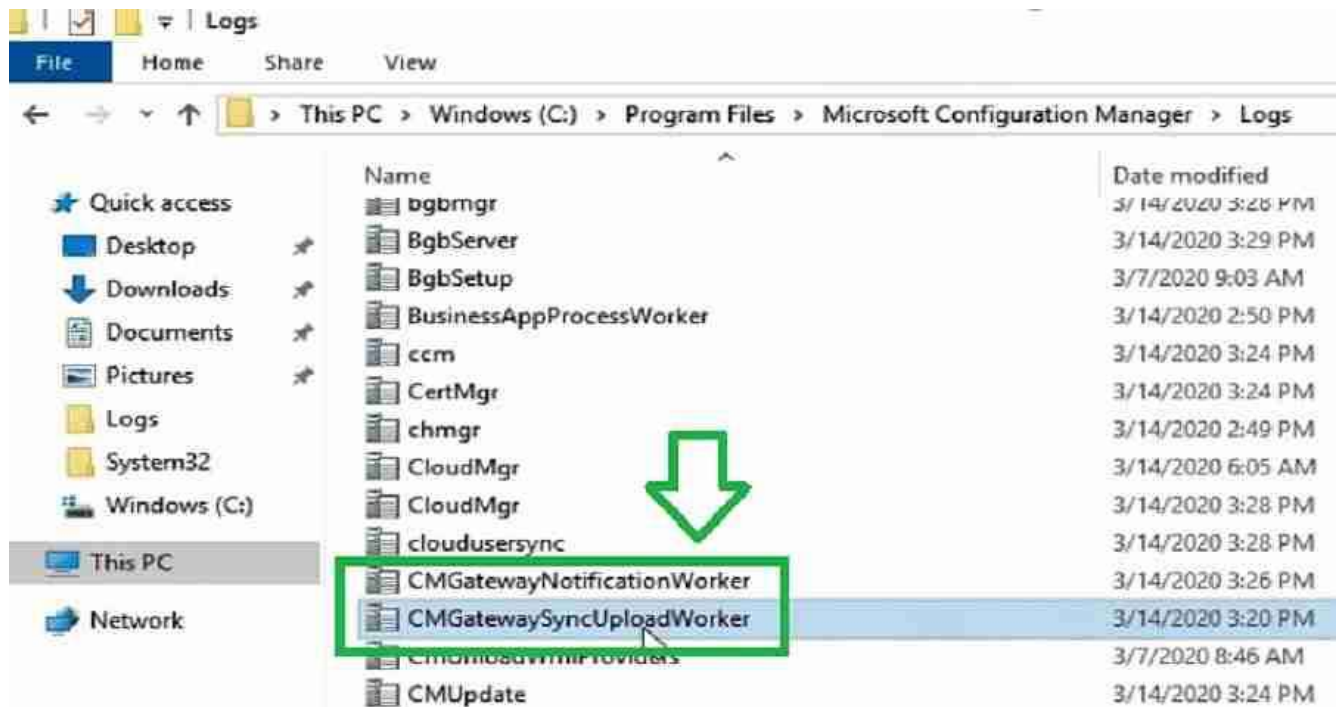


<a href="#">Troubleshooting + support</a>		<div>Device actions status</div> <table> <thead> <tr> <th>Action</th><th>Status</th><th>Date/Time</th></tr> </thead> <tbody> <tr> <td>Sync Machine Policy</td><td>Pending</td><td>3/15/2020, 3:23:57 AM</td></tr> </tbody> </table>	Action	Status	Date/Time	Sync Machine Policy	Pending	3/15/2020, 3:23:57 AM
Action	Status	Date/Time						
Sync Machine Policy	Pending	3/15/2020, 3:23:57 AM						

SCCM Device Sync Troubleshooting – Tenant Attach Guide for SCCM Logs Data Flow Troubleshooting Intune

cmgatewaynotificationworker.log :

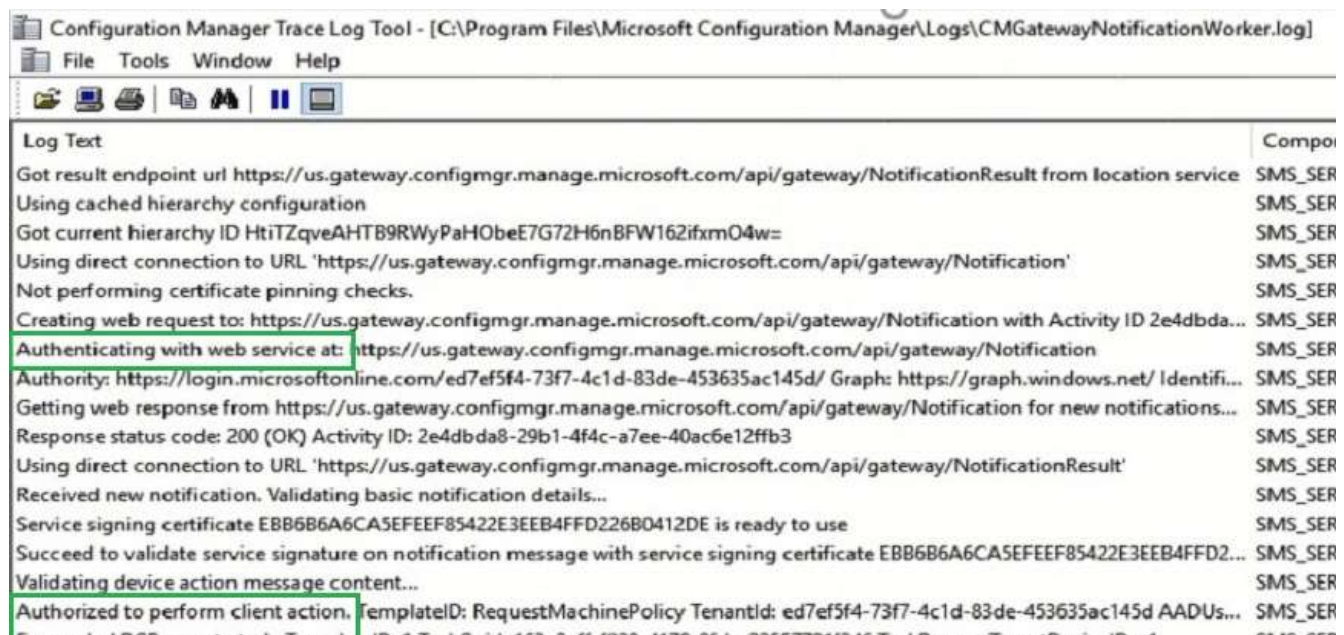
This log tracks the events from Intune to ConfigMgr. You can refer to this log while troubleshooting communication between Intune and ConfigMgr.



SCCM Device Sync Troubleshooting

ConfigMgr server receives the notification and authenticates the user who initiated the policy from the MEM console.

If user authentication is successful, the ConfigMgr BGB remote task will process further.





## SCCM Device Sync Troubleshooting

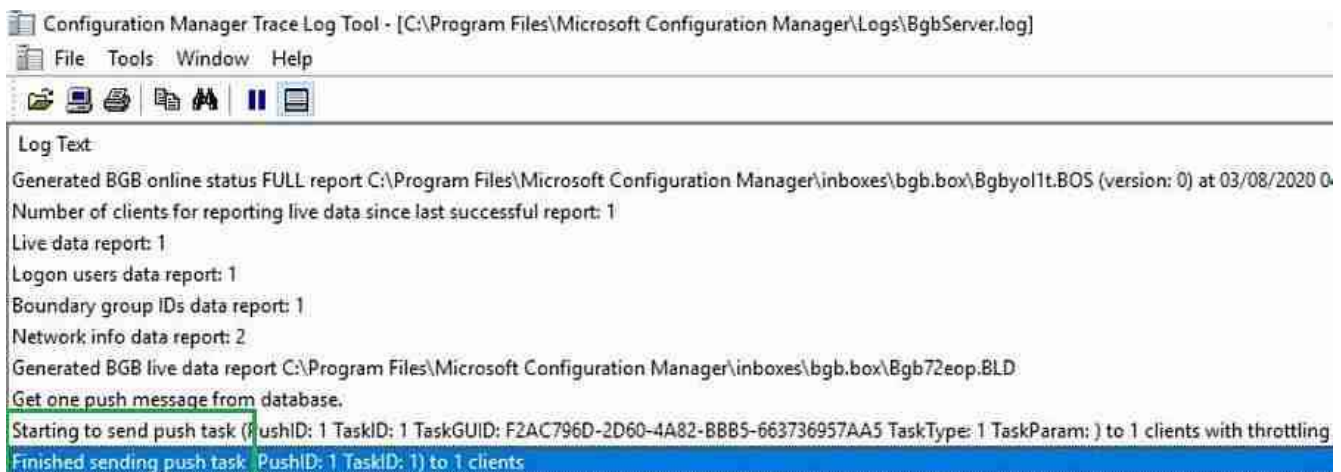
You may get the below error if the user is not having the necessary ConfigMgr permission as mentioned in pre-req. Also, If the user is not an on Prem user id and not synchronized to azure, we see the below error.

Unauthorized to perform client action. TemplateID: RequestMachinePolicy TenantId: ed7ef5f4-73f7-4c1d-83de-453635ac145d AADUserID: f91c3e40-4c30-42e0-b0eb-c5663d549b75.



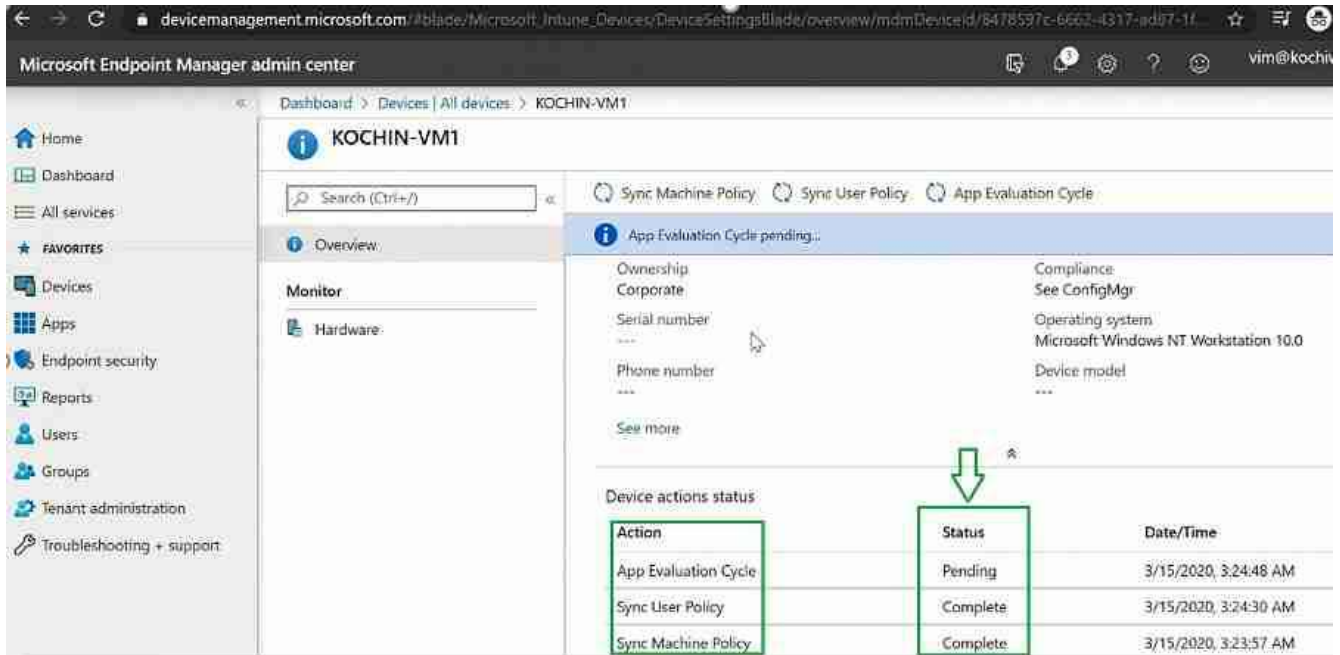
## SCCM Device Sync Troubleshooting

ConfigMgr processes the BGB notification service. Then sent the notification to the ConfigMgr client.



## SCCM Device Sync Troubleshooting

You can also track the ConfigMgr client Machine policy status, which you initiated from the MEM console. The different statuses are Complete or pending or failed, as shown below.



SCCM Device Sync Troubleshooting – Tenant Attach Guide for SCCM Logs Data Flow Troubleshooting Intune

I used the MEM admin portal from my mobile phone for this post to manage the SCCM agent. We could manage my SCCM agent from a mobile web browser. This is a great step.

## Resources

## Author

**Vimal** has more than 10 years of experience in SCCM device management solutions. His main focus is on Device Management technologies like Microsoft Intune, ConfigMgr (SCCM), OS Deployment, and Patch Management. He writes about the technologies like SCCM, Windows 10, Microsoft Intune, and MDT.