Filename: microsoft-ms101-3-3-1-plan-device-comanagement
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Plan for Devices and Apps
EpisodeName: Plan Device Co-management
Description: Adam and Wes discuss how to plan for device co-management using Intune and System Center Configuration Manager (SCCM).

Plan Device Co-management

Implement Modern Device Services (30-35%)

Plan for Devices and Apps
• Create and Configure Microsoft Store for Business
• Plan App Deployment
• Plan Device Co-management
• Plan Device Monitoring
• Plan for Device Profiles
• Plan for Mobile Application Management
• Plan Mobile Device Security

==========

Plan Device Co-management

Co-management enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Microsoft Intune.

Prerequisites:

Licensing -

```
• Azure AD Premium
• EMS or Intune license for all users
```

NOTE: An Enterprise Mobility + Security (EMS) subscription includes both Azure Active Directory Premium and Microsoft Intune.

PRO TIP: Make sure you assign an Intune license to the account that you use to sign in to your tenant. Otherwise, sign in fails with the error message "User not recognized". :(

Configuration Manager -

Co-management requires Configuration Manager version 1710 or later.

Starting in Configuration Manager version 1806, you can connect multiple Configuration Manager instances to a single Intune tenant.

Azure AD -

Windows 10 devices must be joined to Azure AD. They can be either of the following types:

```
• Hybrid Azure AD-joined, where the device is joined to your on-premises
```

Active Directory and registered with your Azure Active Directory.

```
• Azure AD-joined only - (This type is sometimes referred to as
```

"cloud domain-joined")

Intune -

If you have a hybrid MDM environment (Intune integrated with Configuration Manager), you can not enable co-management.

However, you can start migrating users to Intune standalone and then enable their associated Windows 10 devices for co-management.

https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/migrate-hybridmdm-to-intunesa

NOTE: If you are using mixed authority, first complete the migration to Intune standalone. Then, set the MDM authority to Intune before setting up co-management.

Windows 10 - Upgrade your devices to Windows 10, version 1709 or later.

NOTE: Windows 10 mobile devices do not support co-management

Permissions and roles -

Action	Role
Set up a cloud management gateway in Configuration Manager	Azure Subscription Manager
Create Azure AD apps from Configuration Manager	Azure AD Global Administrator
Import Azure apps in Configuration Manager	Configuration Manager Full Administrator
Enable co-management in	Configuration Manager Full

Configuration Manager	Administrator with All scope
	rights
==========	==========

Scenarios -

1. Domain joined devices with ConfigMgr: Supports customers that are transitioning on-prem device management to Intune

NOTE: Devices are HYBRID Azure AD Joined

2. Azure AD joined devices with Intune: Supports customers that have Azure AD joined devices managed using Intune, BUT still require ConfigMgr for certain tasks such as using AutoPilot for new device deployments

NOTE: Devices are Azure AD joined & ConfigMgr sites need a Cloud Management Gateway (CMG) deployed. The CMG allows Intune to deploy the ConfigMgr client to devices

Plan for the cloud management gateway in Configuration Manager:
https://docs.microsoft.com/en-us/sccm/core/clients/manage/cmg/plan-cloud-management-gateway

Workloads -

Co-management supports the following workloads:

```
• Compliance policies
• Windows Update policies
• Resource access policies
• Endpoint Protection
• Device configuration
• Office Click-to-Run apps
• Client apps
```

Let's connect !!!

1. Open the SCCM Console
2. Click the Administrative Workspace
3. Under Overview expand Cloud Services
4. Click Co-Management
5. In the ribbon, select Configure Co-Management
6. In the Wizard, on the subscription page, click sign-in and enter your Azure AD credentials, then click next

NOTE: The account being used DOES NOT need to be an administrator, BUT IT DOES REQUIRE an Intune license to be assigned

7. On the Enablement page, select pilot from the drop down and click next. (this will enable automatic enrollment to Intune for a limited number of devices in a pilot device collection)
8. On the workloads page, move each of the sliders to the Pilot Intune column, to shift the workloads to your pilot device collection
9. On the settings page, click Browse, select a device collection that you want to pilot co-management with.
10. On the Summary page, review and click next
11. On the Completion page, confirm the process was successful then click Close