✓ 100 XP

Planning and configuration for co-management

5 minutes

Before switching over to co-management, you need to figure out what workloads you want to switch over. You don't have to switch all workloads at once. You can do them individually when you're ready. Configuration Manager will continue to manage all other workloads, including those workloads that you don't switch to Intune, and all other features of Configuration Manager that co-management doesn't support.

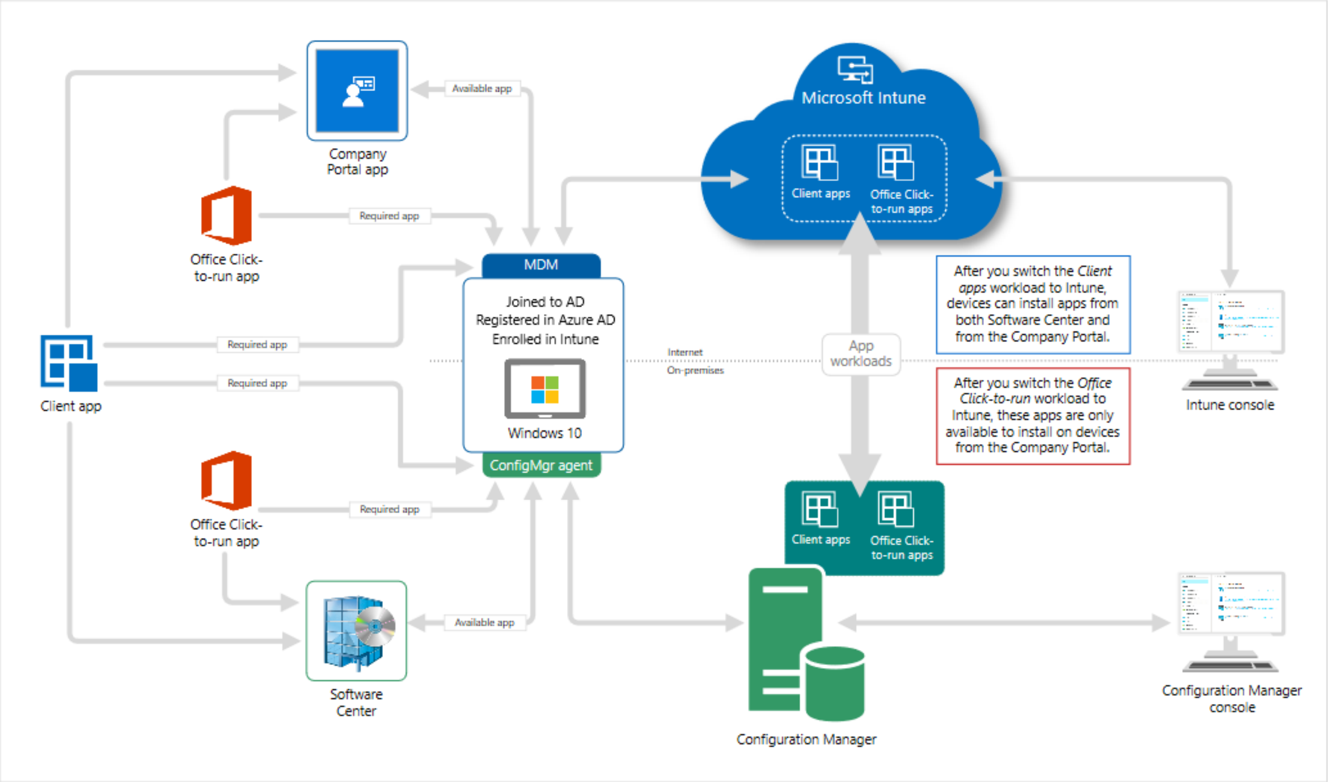
Co-management supports the following workloads:

Policy	Description
Compliance policies	Compliance policies define the rules and settings that a device must comply with to be considered compliant by conditional access policies. Also use compliance policies to monitor and remediate compliance issues with devices independently of conditional access.
Windows Update policies	Windows Update for Business policies let you configure deferral policies for Windows 10 feature updates or quality updates for Windows 10 devices managed directly by Windows Update for Business.
Resource access policies	Resource access policies configure VPN, Wi-Fi, email, and certificate settings on devices.
Endpoint Protection	The Endpoint Protection workload includes the Windows Defender suite of antimalware protection features: • Windows Defender Antimalware • Windows Defender Application Guard • Windows Defender Firewall • Windows Defender SmartScreen • Windows Encryption • Windows Defender Exploit Guard • Windows Defender Application Control • Windows Defender Security Center • Microsoft Defender for Endpoint • Windows Information Protection
Device configuration	Starting in Configuration Manager 1806, the device configuration workload includes settings that you manage for devices in your organization. Switching this workload also moves the Resource Access and Endpoint Protection workloads.

Policy	Description
Office Click-to-Run apps	This workload manages Office apps on co-managed devices. • After moving the workload, the app shows up in the Company Portal on the device • Office updates may take around 24 hours to show up on client unless the devices are restarted • There's a new global condition, Are Microsoft 365 applications managed by Intune on the device. This condition is added by default as a requirement to new Microsoft 365 applications. When you transition this workload, co-managed clients don't meet the requirement on the application. Then they don't install Microsoft 365 deployed via Configuration Manager.
Client apps	Use Intune to manage client apps and PowerShell scripts on co-managed Windows 10 devices. After you transition this workload, any available apps deployed from Intune are available in the Company Portal. Apps that you deploy from Configuration Manager are available in Software Center.

> **Note**
>
> The supported workloads are updated after each new release of System Center Configuration Manager, check the official documentations on **Co-management workloads** for updates.

Diagram for app workloads



Paths to co-management

There are two primary ways for you to set up co-management. It's important to understand the prerequisites for each path. They each require some combination of Azure Active Directory (Azure AD), Configuration Manager, Microsoft Intune, and Windows 10.

There are two main paths to reach to co-management:

Path 1: Auto-enroll existing clients	You have Windows 10 devices that are already Configuration Manager clients. You set up hybrid Azure AD and enroll them into Intune. Taking this path can get your existing Configuration Manager-managed devices quickly enrolled into Intune. The management of these devices from Configuration Manager is no different from before you enable co-management. Now you get all the cloud-based benefits. This path is transparent to your users.
Path 2: Bootstrap with modern provisioning	You have new Windows 10 devices that join Azure AD and automatically enroll to Intune. You install the Configuration Manager client to reach a co-management state.

Auto-enrolling existing clients

With co-management, you can keep your well-established processes for using Configuration Manager to manage PCs in your organization. At the same time, you're investing in the cloud through use of Intune for security and modern provisioning.

To set up co-management of your Windows 10 devices that are already enrolled in Configuration Manager, complete the steps outlined in Tutorial: Enable co-management for existing Configuration Manager clients.

Bootstrap with modern provisioning

To set up co-management of Windows 10 devices in an environment where you use both Azure Active Directory (AD) and an on-premises AD but don't have a hybrid Azure Active Directory (AD), complete the steps outlined in Tutorial: Enable co-management for new internet-based devices.

Next unit: Implementing conditional access

Continue ›