

Microsoft Endpoint Manager: FAQs

What is Microsoft Endpoint Manager?

Microsoft Endpoint Manager is a unified, integrated management platform for managing all your endpoints. We're bringing ConfigMgr and Microsoft Intune together and removing licensing and migration barriers to leverage your existing ConfigMgr investments while taking advantage of the power of the Microsoft cloud.

We've taken all the various management-related names, brands, and consoles and we have massively simplified how we talk about it, and how you use it.

Now we'll refer to all our endpoint management solutions as "Microsoft Endpoint Manager", which will include the following products:

- Microsoft Endpoint Configuration Manager (formerly, System Center Configuration Manager)
- Microsoft Intune

With Microsoft Endpoint Manager, customers can take advantage of these integrated features in a single platform:

- Windows co-management
- Windows Autopilot
- Tenant-attached Helpdesk
- Desktop Analytics
- Azure Active Directory Conditional Access
- Endpoint security with Microsoft Defender ATP
- Apple, Android, Windows, and ruggedized device management
- Productivity Score, including the Technology Experience Score
- ... and much more!

Does this mean we don't need to buy Intune or Autopilot licenses anymore?

You still require appropriate active licenses to deploy Windows Autopilot, Desktop Analytics, Azure Active Directory Conditional Access, Microsoft Defender ATP, and other features according to their individual licensing terms. Microsoft Endpoint Manager provides an integrated platform to take advantage of these features in a simplified platform.

Is there any change in licensing for Microsoft Endpoint Manager? We are licensed for ConfigMgr already, but not Intune. Do we have to buy Intune to enable Microsoft Endpoint Manager?

Yes, there is simplified licensing announced as part of Microsoft Endpoint Manager with effect from December 1, 2019.

If you have an active license for ConfigMgr, you can enroll Windows PCs for co-management without the need to purchase and assign an additional Intune user license. If you want to leverage Intune for managing iOS, Android, or macOS devices, or enroll Windows PCs with a different method, then you need the appropriate Intune subscription through either standalone Intune license, Enterprise Mobility + Security (EMS), or Microsoft 365. Always refer to the [product licensing terms](#) website for the latest information.

As we announced at Microsoft Ignite 2019, we've removed the licensing barrier so you can start managing your Windows PCs today with ConfigMgr by attaching Intune as a part of Microsoft Endpoint Manager. If you are licensed for ConfigMgr, then you are also automatically licensed for Intune for co-managing your Windows PCs. Similarly, if you are licensed for Intune, then you are also automatically licensed for ConfigMgr for co-managing your Windows PCs.

[We are licensed for Intune. Do we have to buy ConfigMgr to enable Microsoft Endpoint Manager?](#)

No – ConfigMgr is already included via your entitlements. For details, see the Product and Licensing FAQ: <https://docs.microsoft.com/en-us/sccm/core/understand/product-and-licensing-faq>

[Is Intune for Devices still available?](#)

Yes, the Microsoft Intune device-only subscription is intended for management of kiosks, phone-room devices, IoT and other single-purpose devices that do not require any user-based security and management features This [blog](#) has more information.

[Is ConfigMgr going away? Can I still use the ConfigMgr console?](#)

No. Both Intune and ConfigMgr are core to the new experience under Microsoft Endpoint Manager. Microsoft Endpoint Manager creates a platform for ConfigMgr admins to continue using their on-premises infrastructure and start taking advantage of the Microsoft cloud by attaching Intune to their existing deployment. Many organizations will cloud-attach ConfigMgr and Microsoft Intune and continue to co-manage them in this way. Other organizations may choose to move workloads to Intune management over time, at their own pace. The decision is up to each organization, and Microsoft will continue to invest in both ConfigMgr and Intune as part of Microsoft Endpoint Manager.

And yes, you can still use the ConfigMgr console, while additionally leveraging the cloud console to bring you the benefits of the cloud now.

Is Intune going away?

No. Both Intune and ConfigMgr are core to the new experience under Microsoft Endpoint Manager. Both Intune and ConfigMgr will continue to be available as standalone products with their individual consoles, while additionally leveraging Microsoft Endpoint Manager admin center to bring you the benefits of the cloud.

Do we need to buy anything additional to get Productivity Score/Technology Experience analytics?

Productivity Score/Technology Experience analytics is included as an entitlement in most Microsoft 365 and EMS plans. If you only have ConfigMgr licenses, as soon as you attach Intune to your ConfigMgr deployment, you can start to leverage the available functionality for these services for Windows PCs. To manage non-Windows devices, you will need to buy one of the plans that provide entitlement to this feature. Learn more: <https://www.microsoft.com/en-us/licensing/product-licensing/microsoft-365-enterprise>

I thought co-management was supposed to be a “bridge” to modern management. Now you’re saying it’s a “destination”. Which is it?

It’s both! We want you to be able to take advantage of the immense intelligence of the Microsoft cloud – on all your endpoints whatever your current situation and long-term plans. For current ConfigMgr customers, co-management is a destination – you can get there immediately and stay if that solution suits your needs. If you’re planning to move some or all your PCs to MDM-based management, then you can use co-management as a bridge to ease the transition. The point is, we’ll meet you where you are, and take you where you want to go.

With Microsoft Endpoint Manager, we made comprehensive changes across the product experience, licensing entitlements and deployment guidance to deliver a crisp message for both existing and new customers. Co-management will be a destination for many organizations. This allows you to leverage your existing investment, while taking advantage of the power of the Microsoft cloud. But you can still move to MDM-based management for some or all your devices if you desire. New customers can choose to start directly in the cloud with Microsoft Intune or use Microsoft Endpoint Manager.

Will traditional ConfigMgr management for PCs now go away?

As we stated above, we're giving you the flexibility to meet your needs, whatever they may be. There are certain cases in which it simply makes sense to continue with traditional, image-based PC management (as with PCs that control manufacturing processes or lab data collection for pharma). You can continue to do that. But by enabling co-management, you can take advantage of the intelligence we've built into the cloud platform to provide increased automation and unparalleled insights into device performance and security.

The fact is, most organizations will want to adopt more modern approaches for most of their PCs by taking advantage of technologies like Windows Autopilot. We're making it easier than ever to do that by taking away all the impediments to moving to PCs to co-management right now.



Do we need to have Azure Active Directory (AAD) deployed to move to Microsoft Endpoint Manager?

Yes. Please refer to the product documentation for the pre-requisites. You'll at least need to federate your on-premises Active Directory deployment with Azure Active Directory to reap the advantages of co-management. More details: <https://docs.microsoft.com/en-us/sccm/comange/overview>

I currently use Microsoft BitLocker Administration and Monitoring (MBAM) to manage BitLocker across my enterprise. Can I move my BitLocker management to Microsoft Endpoint Manager?

Yes! Enterprise BitLocker management is moving to both [Microsoft Intune and Configuration Manager](#). With Windows 10, version 1909 and the Microsoft Endpoint Manager Admin Console, you'll get all the same features that you see today in MBAM. These features include enforcing and configuring BitLocker, key rolling for devices that have been started with the recovery key, compliance reporting, and a self-service recovery portal.