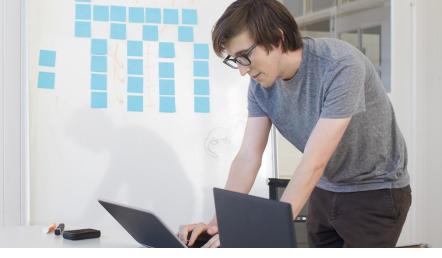Microsoft

Better together: Windows 10 + EMS

Personal, productive, and always protected

Windows 10 is the best Windows ever and provides a foundation for protection against modern threats and continuous management while enabling your users to be more productive. To get the most out of your mobile security and productivity strategy, integrate the Microsoft Enterprise Mobility Suite (EMS) with Windows 10 for greater protection of users, devices, apps, and data.

Protect access to applications

Windows 10 provides a foundation for secure user access with authentication options to protect identities and credentials. Azure Active Directory is built into Windows 10 to provide single sign-on for users, simplifying their experience and making it easy to set up company devices, access on-premises web apps, and access thousands of SaaS apps hosted in any public cloud. IT can use EMS to take advantage of unique Windows 10 device health data to help build conditional access policies to provide greater security when users access corporate applications.

☺

Hello Christopher

Flexible device and application management

Continue to use System Center Configuration Manager (included in EMS) to deploy and manage Windows 10. In addition, you can take advantage of the mobile device management (MDM) capabilities in Windows 10 by automatically enrolling Windows 10 devices into MDM. EMS gives you a single tool to manage devices and applications across Windows, iOS, and Android. Mobile application management (MAM) for line-of-business and Office Mobile apps makes it possible to confine corporate information to use within corporate apps. Management flexibility with EMS and Windows 10 makes it possible for users to work with the tools they need, on the devices they trust, while meeting IT-defined security and compliance standards.

Help secure data everywhere

Extend Windows 10 security to protect your corporate data. Automatic encryption of data stored on the device gives your mobile employees a secure start. Make sure your sensitive information is always protected, even when employees share and work collaboratively. With EMS you can extend security capabilities beyond internal sharing to also protect data shared outside your organization. EMS includes data encryption with identity-based access policies for any file type for consistent performance across multiple device platforms. You can track and revoke access to files and run advanced security reports to detect threats and security issues. Now you can protect your data inside and outside your organization—and even in motion.

EMS benefits for Windows

	Windows 10 →	Enterprise Mobility Suite
Identity and access management	• Single sign-on for business cloud apps • Device set up and registration for Windows devices	• Conditional access policies for enhanced single sign-on security • MDM auto enrollment • Self-service group and application management • Password reset with write-back to on-premises directory • Cloud-based advanced security reports • Microsoft Identity Manager
Mobile device and app management	• Windows Store for Business • Traditional domain join manageability • Manageability via MDM and MAM	• Mobile device management • Mobile app management • Secure content viewer • Certificate, WiFi, VPN, email profile provisioning • Agent-based management of Windows devices (domain joined via ConfigMgr and internet-based via Intune)
Information protection	• Encryption for data at rest and generated on device • Encryption for data included in roaming settings	• Encryption for files shared off Windows 10 devices • Tracking and notifications for shared documents • Protection for content stored in Office and Office 365 • Protection for on-premises Windows Server file shares • Behavioral analytics for advanced threat detection

■ Microsoft