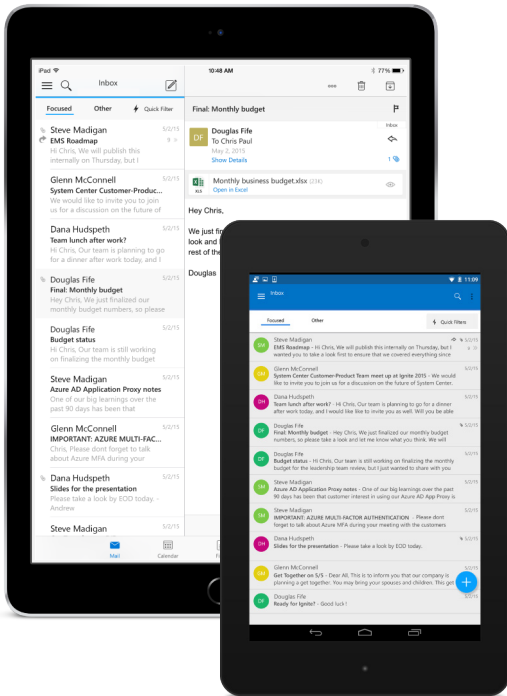


Manage mobile productivity with Microsoft Enterprise Mobility Suite



Familiar email and productivity experience

In a mobile-first, cloud-first world, access to corporate email, documents, and robust productivity tools is crucial for employees to stay productive while on the go. However, the amount of confidential data that is stored within corporate emails and documents can create a significant security risk for organizations, if the corporate data ends up in the wrong hands.

Enterprise Mobility Suite (EMS) helps to provide employees with secure and seamless access to corporate email and documents, as well as familiar email and productivity experiences with Office mobile apps such as Outlook, Word, Excel, and PowerPoint. EMS helps protect corporate data on the device itself and beyond with four layers of protection—all without affecting the personal data on the device.

Microsoft Outlook for iOS and Android brings together the core tools that employees need to get things done—email, calendar, contacts, and files—helping them to accomplish more even on the smallest screen. Additionally, they can view and edit email attachments and documents using familiar productivity tools such as Microsoft Word, Excel, PowerPoint, and OneDrive. With Office mobile apps and Enterprise Mobility Suite (EMS), employees get a consistent user experience and the ability to do more from virtually anywhere while EMS helps protect corporate data at the same time.

A better way to manage access to email and documents

Employees expect to have a seamless experience accessing corporate email and documents on the devices of their choice without going through several complex steps or calling the help desk. IT, on the other hand, wants to keep corporate data protected wherever it is.

With EMS, organizations can enable conditional access to Office 365 (Exchange Online and SharePoint Online) as well as on-premises Exchange Server to help ensure that employees can only access corporate email and documents from devices that are managed and compliant based upon policies set by IT. When employees try to access corporate resources from unmanaged devices, they are blocked and then provided with simple steps to quickly obtain access to email and other corporate resources. With the cloud architecture of EMS, IT does not need to install and configure email gateways, servers in the perimeter network, or develop custom scripts. EMS is directly integrated with Office 365 to give employees a seamless experience while also enabling IT to manage access to corporate resources.

Key benefits



Better Office management

EMS directly integrates with Office mobile apps and is the only solution that brings managed mobile productivity with Office across device platforms.



Single identity for accessing corporate resources

EMS manages access to all corporate resources, both on-premises and in the cloud, with a single identity.



Extensive protection of corporate email and documents across four layers

EMS helps to protect at the identity, device, application, and data layers.



Flexible architecture

EMS is designed to run in the cloud from the ground up and work seamlessly with cloud services such as Office 365, as well as with on-premises infrastructure.

Extensive protection of corporate email and documents

EMS has unique capabilities that help to protect corporate data such as email and documents across four layers: *identity, device, application, and data*.

Identity

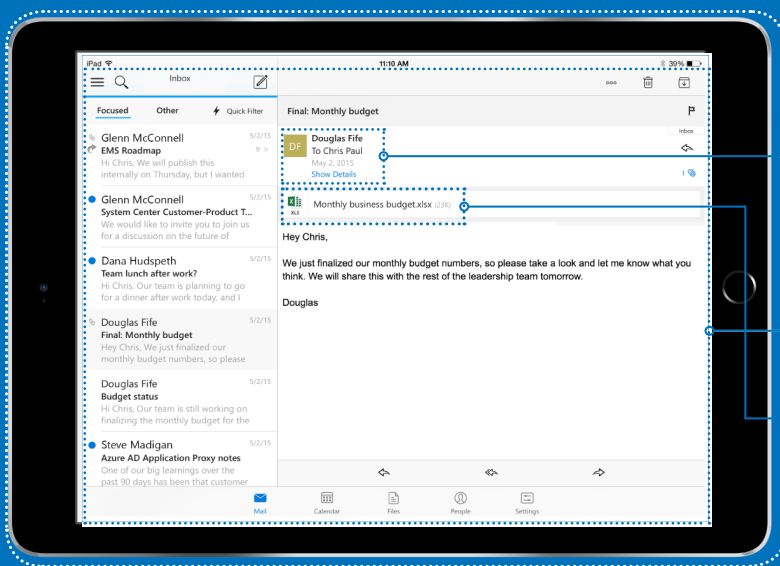
EMS helps to ensure that only authorized users are permitted to access corporate email and documents by using security features such as cloud-based authentication and authorization, multi-factor authentication, and advanced security reports that leverage Microsoft Azure machine learning capabilities.

Device

Mobile device management (MDM) capabilities in EMS help organizations to manage and enforce device-level settings such as encryption and password requirements and resource access profiles such as email, WiFi, certificates, and VPN that enable seamless access to corporate resources.

Application

Mobile application management (MAM) capabilities in EMS help prevent corporate data leaks by restricting actions in Office mobile apps such as cut, copy, paste, and save as. Employees can also use a single app (such as Outlook) for both personal and corporate use while EMS helps to ensure that the corporate data is separated and protected.



Identity

Device

Application

Data

Data

The information protection capabilities in EMS help to secure highly confidential documents at the file layer. Employees can encrypt virtually any type of a file, set granular permissions, and track usage to ensure that only the right people inside and outside of the organization can access email attachments and documents, wherever the files are.

Flexible architecture

Each organization has unique needs that define their architectural requirements. That's why EMS is designed to work with both cloud services and on-premises infrastructure. Office 365 and EMS are directly integrated and designed to run in the cloud from the ground up to provide easily configurable and powerful tools for organizations to solve new business challenges without worrying about scale, maintenance, or updates. EMS also integrates with existing on-premises investments such as Active Directory, Exchange Server, and System Center Configuration Manager. This flexibility provides additional benefits such as the ability to connect on-premises Active Directory with EMS, enabling organizations to provide employees with access to all of their company resources such as email, documents, and applications both on-premises and in the cloud with a single username and password.

Learn more

EMS overview: microsoft.com/ems

Watch demo: aka.ms/managedemaildemo

Try EMS: aka.ms/tryems

