




# Microsoft 365 for enterprise Foundation Infrastructure

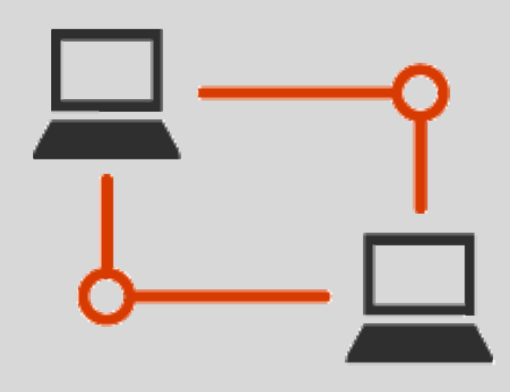





Build a firm IT foundation upon which Microsoft 365 applications and services can unlock creativity and teamwork in a secure environment.

Microsoft 365 for enterprise brings together:

 Office 365 Enterprise

 Windows 10 Enterprise

 Enterprise Mobility + Security (EMS)

Deployment phases						
	 Networking	 Identity	 Windows 10 Enterprise	 Microsoft 365 Apps for enterprise	 Mobile Device Management	 Information Protection
Goals	<p><b>Admins:</b> The organization network is optimized for access to the Microsoft network.</p> <p><b>Users:</b> I get consistent performance when accessing Microsoft 365 cloud services.</p>	<p><b>Admins:</b> Authentication is secured and identities are protected and managed at scale using hybrid and governance.</p> <p><b>Users:</b> Authentication is secured and it's easy to manage my authentication methods, such as passwords and other factors.</p>	<p><b>Admins:</b> The infrastructure is in place to deploy Windows 10 Enterprise to new and existing Windows devices and keep them updated.</p> <p><b>Users:</b> It's easy to upgrade and ongoing update installation is transparent.</p>	<p><b>Admins:</b> The infrastructure is in place to deploy Microsoft 365 Apps for enterprise to Windows 10 Enterprise and other devices and keep it updated.</p> <p><b>Users:</b> My version of Office client applications always have the latest features.</p>	<p><b>Admins:</b> The infrastructure is in place to enroll devices, use application and conditional access policies, and secure my organization's resources.</p> <p><b>Users:</b> I can easily and safely access my work email and files on my device.</p>	<p><b>Admins:</b> The infrastructure is in place to implement and monitor data compliance and information protection.</p> <p><b>Users:</b> It's easy to apply sensitivity labels to documents.</p>
Services, features, and tools	Network connectivity, performance, and latency measuring tools	<ul style="list-style-type: none"><li>Secure user accounts</li><li>Multi-factor authentication (MFA) or password-less</li><li>Azure Active Directory (Azure AD) Privileged Identity Management (PIM) for admin accounts (E5 only)</li><li>Azure AD Connect with password hash synchronization (PHS) or pass-through authentication (PTA)</li><li>Authentication and password maintenance with password protection, Azure AD Seamless Single Sign-On (SSO), self-service password reset, password writeback</li><li>Dynamic and self-service group membership, automatic license assignment, access reviews</li></ul>	<ul style="list-style-type: none"><li>Windows Analytics</li><li>Microsoft Endpoint Configuration Manager</li><li>Microsoft Deployment Toolkit (MDT)</li><li>Deployment Image Servicing and Management (DISM)</li><li>Windows Autopilot</li><li>Windows Update for Business</li><li>Windows Defender Antivirus</li><li>Windows Defender Exploit Guard</li><li>Windows Defender Advanced Threat Protection (E5 only)</li></ul>	<ul style="list-style-type: none"><li>Office Deployment Tool (ODT)</li><li>Office Customization Tool</li><li>Readiness Toolkit</li><li>Microsoft Endpoint Configuration Manager</li></ul>	<ul style="list-style-type: none"><li>Cloud-only with Intune (part of EMS)</li><li>Co-management with Intune and Microsoft Endpoint Configuration Manager (part of EMS)</li><li>Mobile device management for enrolled devices</li><li>Mobile application management for all devices</li><li>Conditional access using Azure AD Premium P1 and P2 (part of EMS)</li><li>Compliance policies and control device features</li></ul>	<ul style="list-style-type: none"><li>Office 365 sensitivity and retention labels</li><li>Office 365 Data Loss Prevention (DLP)</li><li>Microsoft Cloud App Security (E5 only)</li><li>Office 365 Advanced Threat Protection (ATP) (E5 only)</li><li>Secure Score</li><li>Office 365 privileged access management (E5 only)</li></ul>
Key design decisions	<ul style="list-style-type: none"><li>Which local offices need Internet connections</li><li>Which network hairpins to bypass and for what types of traffic</li><li>Which edge devices to configure traffic bypass and for what types of traffic</li></ul>	<ul style="list-style-type: none"><li>Which identity model: cloud-only or hybrid</li><li>Which authentication method: PHS, PTA, or federated</li><li>Use of Azure AD Seamless SSO</li><li>Which conditional access policies to enforce MFA, force password resets, etc.</li><li>Which MFA methods to support</li><li>How to protect global admin accounts (MFA, Azure AD Privileged Identity Management [E5 only])</li><li>How to simplify password management (password writeback and self-service password reset)</li><li>Which custom words to prevent in passwords</li><li>How to manage group membership: Manual, dynamic, or self-service</li><li>How to manage licenses: manual or group-based</li><li>Which groups to manage for access reviews</li></ul>	<ul style="list-style-type: none"><li>Choose a deployment strategy<ul style="list-style-type: none"><li>In-place upgrade</li><li>PC imaging</li><li>Autopilot</li></ul></li><li>Choose deployment and configuration tools:<ul style="list-style-type: none"><li>Microsoft Endpoint Configuration Manager</li><li>MDT</li><li>Intune</li><li>Group Policy</li><li>Windows PowerShell</li></ul></li><li>Create a phased deployment plan</li><li>Plan a servicing strategy<ul style="list-style-type: none"><li>Assign devices to update rings</li><li>Optimize update delivery</li><li>Analyze and validate updates</li></ul></li></ul>	<ul style="list-style-type: none"><li>How to manage licenses and address network capability and application compatibility</li><li>How to install: upgrade or clean install</li><li>How to deploy:<ul style="list-style-type: none"><li>Microsoft Endpoint Configuration Manager</li><li>Office Deployment Tool</li><li>Self-install from the Office portal</li></ul></li><li>Where to deploy from: cloud or local source on your network</li><li>What to include in Office installation packages: which Office apps, languages, and architectures</li><li>How to manage updates and which update channels to use</li></ul>	<ul style="list-style-type: none"><li>Choose cloud-only or co-management device management</li><li>Choose how Android, macOS, iOS, and Windows devices are managed</li><li>Use Azure AD groups for app and device access</li><li>Deploy Office, Win32, and other apps to devices</li><li>Force compliance with conditional access rules</li><li>Allow or block device features and settings</li></ul>	<ul style="list-style-type: none"><li>Which security and information protection levels</li><li>How to use sensitivity labels and Azure Information Protection labels</li><li>Which sensitive information types for DLP</li><li>Which Office 365 ATP policies</li><li>How to use Microsoft Cloud App Security (E5 only)</li><li>How to use privileged access management (E5 only)</li></ul>
Configuration results	<ul style="list-style-type: none"><li>All offices have local Internet connections with local DNS servers</li><li>Appropriate network hairpins are bypassed</li><li>Edge devices and browsers are configured for traffic bypass</li></ul>	<ul style="list-style-type: none"><li>Azure AD Connect settings for PHS, PTA, SSO, password writeback</li><li>Global admin account protection with MFA and Azure AD PIM (E5 only)</li><li>Security groups for:<ul style="list-style-type: none"><li>Identity-based conditional access policies</li><li>Password writeback and self-service reset enabled</li><li>Dynamic group membership and automatic licensing</li></ul></li></ul>	Infrastructure and settings for: <ul style="list-style-type: none"><li>Deploying new devices</li><li>Deploying OS upgrades</li><li>Deploying OS updates</li><li>Enabling Windows Defender Antivirus</li><li>Deploying Windows Defender Advanced Threat Protection</li><li>Deploying attack surface reduction rules</li></ul>	<ul style="list-style-type: none"><li>Deployment infrastructure is in place</li><li>Update management infrastructure is in place</li><li>Installation packages are defined</li><li>All client devices are assigned to deployment groups</li><li>Office applications, architectures, and languages are assigned to go to client devices</li></ul>	<ul style="list-style-type: none"><li>Access is controlled using new or existing Azure AD groups</li><li>Devices are enrolled, and apps, features, and settings are applied</li><li>Users with personal devices get secure access to organization apps, such as email</li><li>Conditional access is enforced when devices are compliant with IT rules</li></ul>	<ul style="list-style-type: none"><li>Information protection levels</li><li>Sensitive information types</li><li>Sensitivity or Azure Information Protection labels</li><li>Retention labels</li><li>DLP policies</li><li>Microsoft Cloud App Security settings (E5 only)</li><li>Privileged access management policies (E5 only)</li></ul>
Onboard a new user	Connect them to an on-premises network (wired or wireless)	Add user account to the Azure AD security groups for: <ul style="list-style-type: none"><li>Identity-based conditional access policies</li><li>Password reset</li><li>Automatic licensing</li></ul>	Add computer account/HW ID/other or group to the appropriate security groups for: <ul style="list-style-type: none"><li>Windows Autopilot</li><li>Device upgrades</li><li>Windows 10 Enterprise security features</li></ul>	Add the client device to the appropriate deployment group.	<ul style="list-style-type: none"><li>Add users to your Azure AD security groups</li><li>Add devices to your Azure AD security groups</li><li>Assign licenses</li><li>Enroll devices to receive policies</li></ul>	<ul style="list-style-type: none"><li>Add user accounts to security groups for sensitivity or Azure Information Protection labels</li><li>Train users on how to apply labels to documents</li></ul>
Monitor and update	Check bandwidth utilization for each office monthly and increase or decrease as needed.	<ul style="list-style-type: none"><li>Monitor directory synchronization health with Azure AD Connect Health</li><li>Monitor sign-in activity with Azure AD Identity Protection (E5 only) and Azure AD reporting</li></ul>	<ul style="list-style-type: none"><li>Monitor device health and compliance with Windows Analytics</li><li>Monitor Windows antivirus and intrusion activity with Microsoft Endpoint Configuration Manager or Microsoft Intune</li><li>Manage and deploy updates for Windows 10 Enterprise</li></ul>	<ul style="list-style-type: none"><li>If updates are automatic, they'll occur without any administrative overhead</li><li>To manage updates directly, download the updates and deploy them from distribution points with Microsoft Endpoint Configuration Manager</li></ul>	<ul style="list-style-type: none"><li>Get inventory of devices accessing organization services</li><li>Use Intune reports to monitor apps, device compliance, and configuration profiles</li><li>Use Power BI and the Intune Data Warehouse</li></ul>	Monitor with: <ul style="list-style-type: none"><li>Microsoft Secure Score</li><li>Office 365 DLP dashboard</li><li>Microsoft Cloud App Security dashboard (E5 only)</li></ul>