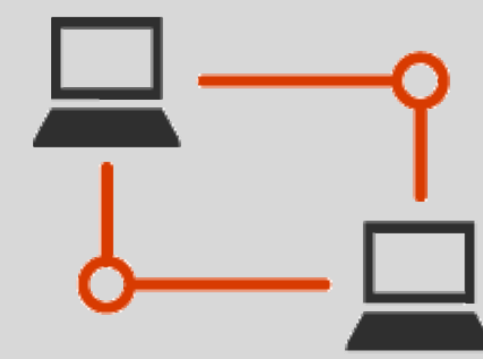







Microsoft 365 Enterprise Foundation Infrastructure

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

Microsoft 365 Enterprise brings together:



Deployment phases						
	 Networking	 Identity	 Windows 10 Enterprise	 Office 365 ProPlus	 Mobile Device Management	 Information Protection
Goals	<p>Admins: The organization network is optimized for access to the Microsoft network.</p> <p>Users: I get consistent performance when accessing Microsoft 365 cloud services.</p>	<p>Admins: Authentication is secured and identities are protected and managed at scale using hybrid and governance.</p> <p>Users: Authentication is secured and it's easy to manage my authentication methods, such as passwords and other factors.</p>	<p>Admins: The infrastructure is in place to deploy Windows 10 Enterprise to new and existing Windows devices and keep them updated.</p> <p>Users: It's easy to upgrade and ongoing update installation is transparent.</p>	<p>Admins: The infrastructure is in place to deploy Office 365 ProPlus to Windows 10 Enterprise and other devices and keep it updated.</p> <p>Users: My version of Office client applications always have the latest features.</p>	<p>Admins: The infrastructure is in place to enroll devices, use application and conditional access policies, and secure my organization's resources.</p> <p>Users: I can easily and safely access my work email and files on my device.</p>	<p>Admins: The infrastructure is in place to implement and monitor data compliance and information protection.</p> <p>Users: 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">Secure user accountsMulti-factor authentication (MFA) or password-lessAzure Active Directory (Azure AD) Privileged Identity Management (PIM) for admin accounts (E5 only)Azure AD Connect with password hash synchronization (PHS) or pass-through authentication (PTA)Authentication and password maintenance with password protection, Azure AD Seamless Single Sign-On (SSO), self-service password reset, password writebackDynamic and self-service group membership, automatic license assignment, access reviews	<ul style="list-style-type: none">Windows AnalyticsSystem Center Configuration ManagerMicrosoft Deployment Toolkit (MDT)Deployment Image Servicing and Management (DISM)Windows AutopilotWindows Update for BusinessWindows Defender AntivirusWindows Defender Exploit GuardWindows Defender Advanced Threat Protection (E5 only)	<ul style="list-style-type: none">Office Deployment Tool (ODT)Office Customization ToolReadiness ToolkitSystem Center Configuration Manager	<ul style="list-style-type: none">Cloud-only with Intune (part of EMS)Co-management with Intune and Configuration Manager (part of EMS)Mobile device management for enrolled devicesMobile application management for all devicesConditional access using Azure AD Premium P1 and P2 (part of EMS)Compliance policies and control device features	<ul style="list-style-type: none">Office 365 sensitivity and retention labelsOffice 365 Data Loss Prevention (DLP)Microsoft Cloud App Security (E5 only)Office 365 Advanced Threat Protection (ATP) (E5 only)Secure ScoreOffice 365 privileged access management (E5 only)
Key design decisions	<ul style="list-style-type: none">Which local offices need Internet connectionsWhich network hairpins to bypass and for what types of trafficWhich edge devices to configure traffic bypass and for what types of traffic	<ul style="list-style-type: none">Which identity model: cloud-only or hybridWhich authentication method: PHS, PTA, or federatedUse of Azure AD Seamless SSOWhich conditional access policies to enforce MFA, force password resets, etc.Which MFA methods to supportHow to protect global admin accounts (MFA, Azure AD Privileged Identity Management [E5 only])How to simplify password management (password writeback and self-service password reset)Which custom words to prevent in passwordsHow to manage group membership: Manual, dynamic, or self-serviceHow to manage licenses: manual or group-basedWhich groups to manage for access reviews	<ul style="list-style-type: none">Choose a deployment strategy<ul style="list-style-type: none">In-place upgradePC imagingAutopilotChoose deployment and configuration tools:<ul style="list-style-type: none">System Center Configuration ManagerMDTIntuneGroup PolicyWindows PowerShellCreate a phased deployment planPlan a servicing strategy<ul style="list-style-type: none">Assign devices to update ringsOptimize update deliveryAnalyze and validate updates	<ul style="list-style-type: none">How to manage licenses and address network capability and application compatibilityHow to install: upgrade or clean installHow to deploy:<ul style="list-style-type: none">System Center Configuration ManagerOffice Deployment ToolSelf-install from the Office portalWhere to deploy from: cloud or local source on your networkWhat to include in Office installation packages: which Office apps, languages, and architecturesHow to manage updates and which update channels to use	<ul style="list-style-type: none">Choose cloud-only or co-management device managementChoose how Android, macOS, iOS, and Windows devices are managedUse Azure AD groups for app and device accessDeploy Office, Win32, and other apps to devicesForce compliance with conditional access rulesAllow or block device features and settings	<ul style="list-style-type: none">Which security and information protection levelsHow to use sensitivity labels and Azure Information Protection labelsWhich sensitive information types for DLPWhich Office 365 ATP policiesHow to use Microsoft Cloud App Security (E5 only)How to use privileged access management (E5 only)
Configuration results	<ul style="list-style-type: none">All offices have local Internet connections with local DNS serversAppropriate network hairpins are bypassedEdge devices and browsers are configured for traffic bypass	<ul style="list-style-type: none">Azure AD Connect settings for PHS, PTA, SSO, password writebackGlobal admin account protection with MFA and Azure AD PIM (E5 only)Security groups for:<ul style="list-style-type: none">Identity-based conditional access policiesPassword writeback and self-service reset enabledDynamic group membership and automatic licensing	Infrastructure and settings for: <ul style="list-style-type: none">Deploying new devicesDeploying OS upgradesDeploying OS updatesEnabling Windows Defender AntivirusDeploying Windows Defender Advanced Threat ProtectionDeploying attack surface reduction rules	<ul style="list-style-type: none">Deployment infrastructure is in placeUpdate management infrastructure is in placeInstallation packages are definedAll client devices are assigned to deployment groupsOffice applications, architectures, and languages are assigned to go to client devices	<ul style="list-style-type: none">Access is controlled using new or existing Azure AD groupsDevices are enrolled, and apps, features, and settings are appliedUsers with personal devices get secure access to organization apps, such as emailConditional access is enforced when devices are compliant with IT rules	<ul style="list-style-type: none">Information protection levelsSensitive information typesSensitivity or Azure Information Protection labelsRetention labelsDLP policiesMicrosoft Cloud App Security settings (E5 only)Privileged access management policies (E5 only)
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">Identity-based conditional access policiesPassword resetAutomatic licensing	Add computer account/HW ID/other or group to the appropriate security groups for: <ul style="list-style-type: none">Windows AutopilotDevice upgradesWindows 10 Enterprise security features	Add the client device to the appropriate deployment group.	<ul style="list-style-type: none">Add users to your Azure AD security groupsAdd devices to your Azure AD security groupsAssign licensesEnroll devices to receive policies	<ul style="list-style-type: none">Add user accounts to security groups for sensitivity or Azure Information Protection labelsTrain users on how to apply labels to documents
Monitor and update	Check bandwidth utilization for each office monthly and increase or decrease as needed.	<ul style="list-style-type: none">Monitor directory synchronization health with Azure AD Connect HealthMonitor sign-in activity with Azure AD Identity Protection (E5 only) and Azure AD reporting	<ul style="list-style-type: none">Monitor device health and compliance with Windows AnalyticsMonitor Windows antivirus and intrusion activity with System Center Configuration Manager or Microsoft IntuneManage and deploy updates for Windows 10 Enterprise	<ul style="list-style-type: none">If updates are automatic, they'll occur without any administrative overheadTo manage updates directly, download the updates and deploy them from distribution points with Configuration Manager	<ul style="list-style-type: none">Get inventory of devices accessing organization servicesUse Intune reports to monitor apps, device compliance, and configuration profilesUse Power BI and the Intune Data Warehouse	Monitor with: <ul style="list-style-type: none">Microsoft Secure ScoreOffice 365 DLP dashboardMicrosoft Cloud App Security dashboard (E5 only)