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:

- Office 365 Enterprise
- Windows 10 Enterprise
- Enterprise Mobility + Security (EMS)

Deployment phases

	Networking	Identity	Windows 10 Enterprise	Office 365 ProPlus	Mobile Device Management	Information Protection
Goal	**Admins:** The organization network is optimized for access to the Microsoft network. **Users:** I get consistent performance when accessing Microsoft 365 cloud services.	**Admins:** Authentication is secured and identities are protected and managed at scale using hybrid and governance. **Users:** Authentication is secured and it's easy to manage my authentication methods, such as passwords and other factors.	**Admins:** The infrastructure is in place to deploy Windows 10 Enterprise to new and existing Windows devices and keep them updated. **Users:** It's easy to upgrade and ongoing update installation is transparent.	**Admins:** The infrastructure is in place to deploy Office 365 ProPlus to Windows 10 Enterprise and other devices and keep it updated. **Users:** My version of Office client applications always have the latest features.	**Admins:** The infrastructure is in place to enroll devices, use application and conditional access policies, and secure my organization's resources. **Users:** I can easily and safely access my work email and files on my device.	**Admins:** The infrastructure is in place to implement and monitor data compliance and information protection. **Users:** It's easy to apply sensitivity labels to documents.

Services, features, and tools	Network connectivity, performance, and latency measuring tools	• Secure user accounts
		  • Multi-factor authentication (MFA) or password-less
		  • Azure 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 writeback
		• Dynamic and self-service group membership, automatic license assignment, access reviews
			• Windows Analytics
			• System Center Configuration Manager
			• Microsoft Deployment Toolkit (MDT)
			• Deployment Image Servicing and Management (DISM)
			• Windows Autopilot
			• Windows Update for Business
			• Windows Defender Antivirus
			• Windows Defender Exploit Guard
			• Windows Defender Advanced Threat Protection (E5 only)
				• Office Deployment Tool (ODT)
				• Office Customization Tool
				• Readiness Toolkit
				• System Center Configuration Manager
					• Cloud-only with Intune (part of EMS)
					• Co-management with Intune and Configuration Manager (part of EMS)
					• Mobile device management for enrolled devices
					• Mobile application management for all devices
					• Conditional access using Azure AD Premium P1 and P2 (part of EMS)
					• Compliance policies and control device features
						• Office 365 sensitivity and retention labels
						• Office 365 Data Loss Prevention (DLP)
						• Microsoft Cloud App Security (E5 only)
						• Office 365 Advanced Threat Protection (ATP) (E5 only)
						• Secure Score
						• Office 365 privileged access management (E5 only)

Key design decisions	• Which local offices need Internet connections
	• Which network hairpins to bypass and for what types of traffic
	• Which edge devices to configure traffic bypass and for what types of traffic
		• Which identity model: cloud-only or hybrid
		• Which authentication method: PHS, PTA, or federated
		• Use of Azure AD Seamless SSO
		• Which conditional access policies to enforce MFA, force password resets, etc.
		• Which MFA methods to support
		• How 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 passwords
		• How to manage group membership: Manual, dynamic, or self-service
		• How to manage licenses: manual or group-based
		• Which groups to manage for access reviews
			• Choose a deployment strategy
			  • In-place upgrade
			  • PC imaging
			  • Autopilot
			• Choose deployment and configuration tools:
			  • System Center Configuration Manager
			  • MDT
			  • Intune
			  • Group Policy
			  • Windows PowerShell
			• Create a phased deployment plan
			• Plan a servicing strategy
			  • Assign devices to update rings
			  • Optimize update delivery
			  • Analyze and validate updates
				• How to manage licenses and address network capability and application compatibility
				• How to install: upgrade or clean install
				• How to deploy:
				  • System Center Configuration Manager
				  • Office Deployment Tool
				  • Self-install from the Office portal
				• Where to deploy from: cloud or local source on your network
				• What to include in Office installation packages: which Office apps, languages, and architectures
				• How to manage updates and which update channels to use
					• Choose cloud-only or co-management device management
					• Choose how Android, macOS, iOS, and Windows devices are managed
					• Use Azure AD groups for app and device access
					• Deploy Office, Win32, and other apps to devices
					• Force compliance with conditional access rules
					• Allow or block device features and settings
						• Which security and information protection levels
						• How to use sensitivity labels and Azure Information Protection labels
						• Which sensitive information types for DLP
						• Which Office 365 ATP policies
						• How to use Microsoft Cloud App Security (E5 only)
						• How to use privileged access management (E5 only)

Configuration results	• All offices have local Internet connections with local DNS servers
	• Appropriate network hairpins are bypassed
	• Edge devices and browsers are configured for traffic bypass
		• Azure AD Connect settings for PHS, PTA, SSO, password writeback
		• Global admin account protection with MFA and Azure AD PIM (E5 only)
		• Security groups for:
		  • Identity-based conditional access policies
		  • Password writeback and self-service reset enabled
		  • Dynamic group membership and automatic licensing
			Infrastructure and settings for:
			• Deploying new devices
			• Deploying OS upgrades
			• Deploying OS updates
			• Enabling Windows Defender Antivirus
			• Deploying Windows Defender Advanced Threat Protection
			• Deploying attack surface reduction rules
				• Deployment infrastructure is in place
				• Update management infrastructure is in place
				• Installation packages are defined
				• All client devices are assigned to deployment groups
				• Office applications, architectures, and languages are assigned to go to client devices
					• Access is controlled using new or existing Azure AD groups
					• Devices are enrolled, and apps, features, and settings are applied
					• Users with personal devices get secure access to organization apps, such as email
					• Conditional access is enforced when devices are compliant with IT rules
						• Information protection levels
						• Sensitive information types
						• Sensitivity or Azure Information Protection labels
						• Retention labels
						• DLP policies
						• Microsoft 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: • Identity-based conditional access policies • Password reset • Automatic licensing	Add computer account/HW ID/other or group to the appropriate security groups for: • Windows Autopilot • Device upgrades • Windows 10 Enterprise security features	Add the client device to the appropriate deployment group.	• Add users to your Azure AD security groups • Add devices to your Azure AD security groups • Assign licenses • Enroll devices to receive policies	• Add user accounts to security groups for sensitivity or Azure Information Protection labels • Train users on how to apply labels to documents
Monitor and update	Check bandwidth utilization for each office monthly and increase or decrease as needed.	• Monitor directory synchronization health with Azure AD Connect Health • Monitor sign-in activity with Azure AD Identity Protection (E5 only) and Azure AD reporting	• Monitor device health and compliance with Windows Analytics • Monitor Windows antivirus and intrusion activity with System Center Configuration Manager or Microsoft Intune • Manage and deploy updates for Windows 10 Enterprise	• If updates are automatic, they'll occur without any administrative overhead • To manage updates directly, download the updates and deploy them from distribution points with Configuration Manager	• Get inventory of devices accessing organization services • Use Intune reports to monitor apps, device compliance, and configuration profiles • Use Power BI and the Intune Data Warehouse	Monitor with: • Microsoft Secure Score • Office 365 DLP dashboard • Microsoft Cloud App Security dashboard (E5 only)

http://aka.ms/m365edeployfoundation

May 2019

Microsoft