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

## Microsoft 365 Enterprise Foundation Infrastructure

**Microsoft 365 Enterprise brings together:**

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

### Goals

- **Advisers:** The organization network is optimized for access to the Microsoft network.
- **Users:** Get consistent performance when accessing Microsoft 365 cloud services.

### Services, features, and tools

<table>
<thead>
<tr>
<th>Networking</th>
<th>Identity</th>
<th>Windows 10 Enterprise</th>
<th>Office 365 ProPlus</th>
<th>Mobile Device Management</th>
<th>Information Protection</th>
</tr>
</thead>
</table>
| - Secure user accounts  
- Multi-factor authentication (MFA) or password-less  
- Azure Active Directory (AAD) 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 Password Single Sign-On (SSO), self-service password reset, password rewrite  
- Dynamic and self-service group membership, automatic license assignment, access reviews | - Choose a deployment strategy  
- In-place upgrade  
- PC imaging  
- Autopilot  
- Choose deployment and configuration tools: System Center Configuration Manager (SCCM)  
- Intune  
- Group Policy  
- Windows Powershell  
- Create a phased deployment plan  
- Plan a servicing strategy  
- Analyze devices to update rings  
- Optimize update delivery  
- Analyze and validate updates | - 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- Enabled Threat Protection  
- Cloud App Management (CCM)  
- Intune  
- System-Center Configuration Manager  | - Office Deployment Tool (ODT)  
- Office Customization Tool  
- Baseline Toolkit  
- System-Center Configuration Manager | - Cloud-only with Intune (part of E5)  
- Co-management with Intune and Configuration Manager (part of E5)  
- Mobile device management for enrolled devices  
- Mobile application management for all devices  
- Conditional access using Azure AD Premium P1 and P2 (part of E5)  
- Compliance policies and control device features | - Office 365 sensitivity and retention labels  
- Office 365 Data Loss Prevention (DLP)  
- Microsoft Cloud App Security (CAS)  
- Microsoft 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 hampers to bypass and for what types of traffic  
- Which edge devices to configure traffic bypasses and for what types of traffic  
- Which identity model: cloud-only or hybrid  
- Which authentication method: PHS, PTA, or federated  
- Use of Azure AD B2B  
- 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 (PIM)  
- How to simplify password management (password rewrite 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  
- Which are the local offices that need internet connections  
- Which network hampers to bypass and for what types of traffic  
- Which edge devices to configure traffic bypasses and for what types of traffic  
- Which identity model: cloud-only or hybrid  
- Which authentication method: PHS, PTA, or federated  
- Use of Azure AD B2B  
- 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 (PIM)  
- How to simplify password management (password rewrite 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  
- Which identity model: cloud-only or hybrid  
- Which authentication method: PHS, PTA, or federated  
- Use of Azure AD B2B  
- 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 (PIM)  
- How to simplify password management (password rewrite 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 (SCCM)  
- Intune  
- Group Policy  
- Windows Powershell  
- Create a phased deployment plan  
- Plan a servicing strategy  
- Analyze 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 or upgrade or clean install  
- How to deploy  
- System Center Configuration Manager  
- Office Deployment Tool  
- Self-service from the Office portal  
- Where to deploy from cloud or local source on your network  
- What to include in O365 installation packages: which Office apps, languages, and architectures  
- How to manage updates and which update channels to use  
- Which identity model: cloud-only or hybrid  
- Which authentication method: PHS, PTA, or federated  
- Use of Azure AD B2B  
- 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 (PIM)  
- How to simplify password management (password rewrite 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 cloud-only or co-management device management  
- Which cloud-based Windows, macOS, iOS, and Windows devices are managed  
- Use Azure AD groups for app and device access  
- Deploy Office O365 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  
- Which Windows, macOS, iOS, and Android devices are managed  
- Which cloud-based Windows, macOS, iOS, and Windows devices are managed  
- Use Azure AD groups for app and device access  
- Deploy Office O365 and other apps to devices  
- Force compliance with conditional access rules  
- Allow or block device features and settings | - How to use privileged access management (E5 only) |

### Configuration results

- All offices have local internet connections with local DNS servers  
- Appropriate network hampers are bypassed  
- Edge devices and browsers are configured for traffic bypasses  
- Azure AD Connect settings for PHS, PTA, SSO, password rewrite  
- Global admin account protection with MFA and Azure AD PIM (E5 only)  
- Security groups for: Identity-based conditional access policies  
- Passwords rewritten and self-service reset enabled  
- Dynamic group membership and automatic licensing  | - 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, architecture, 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  
- Sensitivity labels  
- Sensitivity and Azure Information Protection labels  
- Retention labels  
- DSP policies  
- Microsoft Cloud App Security settings (E5 only)  
- Privileged access management policies (E5 only) | - Information protection levels  
- Sensitivity labels  
- Sensitivity and Azure Information Protection labels  
- Retention labels  
- DSP 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  
- Self-service reset  
- Automatic licensing  | - Add users to your Azure AD security groups  
- Add devices to your Azure AD security groups  
- Assign licenses  
- Enroll devices to receive policies  | - Add users to your Azure AD security groups  
- Add devices to your Azure AD security groups  
- Assign licenses  
- Enroll devices to receive policies |

### 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 pigging in activity with Azure AD Identity Protection (E5 only) and Azure AD reporting  
- Monitor device health and compliance with Windows Analytics  
- Monitor Windows antiviruses and intrusion activity with System Center Configuration Manager or Microsoft Defender for Business  
- Manage and deploy updates for Windows 10 Enterprise  
- Monitor device health and compliance with Windows Analytics  
- Monitor Windows antiviruses and intrusion activity with System Center Configuration Manager or Microsoft Defender for Business  
- 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 update and deploy them from distribution points with Configuration Manager  
- Get inventory of devices accessing organization services  
- Use Intune reports to monitor apps, settings, 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  
- Power BI and the Intune Data Warehouse  | - Monitor with:  
- Microsoft Secure Score  
- Office 365 O365 dashboard  
- Microsoft Cloud App Security dashboard (E5 only) |

---

**http://aka.ms/m365edeployfoundation**

**August 2019**

© 2019 Microsoft Corporation. All rights reserved. To send feedback about this documentation, please write to msfeedback@microsoft.com.