# 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.**

## Deployment phases

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>Ensure network connectivity and monitoring tools are in place.</td>
</tr>
<tr>
<td>Windows 10 Enterprise</td>
<td>Ensure Windows 10 Enterprise is set up with the necessary security features.</td>
</tr>
<tr>
<td>Office 365 ProPlus</td>
<td>Ensure Office 365 ProPlus is configured with the appropriate licenses.</td>
</tr>
<tr>
<td>Mobile Device Management</td>
<td>Ensure mobile devices are configured and managed with Intune.</td>
</tr>
<tr>
<td>Information Protection</td>
<td>Ensure information protection policies are in place.</td>
</tr>
</tbody>
</table>

## Goals

- **Advisors:** 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

- **Networking:**
  - 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 Sign-On (SSO), self-service password reset, password writeback
  - Dynamic and self-service group membership, automatic license assignment, access reviews

- **Windows 10 Enterprise**
  - Windows Analytics
  - Microsoft Endpoint 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 (ATP) (E5 only)

- **Office 365 ProPlus**
  - Office Deployment Tool (ODT)
  - Office Customization Tool
  - Readiness Toolkit
  - Microsoft Endpoint Configuration Manager

- **Mobile Device Management**
  - Cloud only with Intune (part of EMS)
  - Co-management with Intune and Microsoft Endpoint 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 for device features

- **Information Protection**
  - 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 (PAM)

## Key design decisions

- **Which local offices need internet connections?
- Which network traffic bypasses for what types of traffic?
- Which edge devices can traverse 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 B2B services
- Which conditional access policies to enforce MFA, force password resets, etc.
- Which MFA methods to support?
- How to prevent global admin accounts (MFA, Azure AD Privileged Identity Management (PIM) for admin accounts (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

## Configuration results

- **All offices have local internet connections with local DNS servers.
- Appropriate network traffic bypasses are in place.
- Edge devices and browsers are configured for traffic bypass.
- Azure AD Connect settings for PHS, PTA, SSD, 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

## 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 to AVI (E5 or other group or to the appropriate security groups for: Windows Update
- Device upgrades
- Windows 10 Enterprise security features
- Add the client device to the appropriate deployment group
- Add users to your Azure AD security groups
- Assign licenses
- Add 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 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 Microsoft Endpoint Configuration Manager for Microsoft 365
- Manage and deploy updates for Microsoft 10 Enterprise
- If updates are automatic, they should be deployed to the appropriate security groups for:
  - Windows Update for Business
  - Windows Defender Antivirus
  - Windows Defender Exploit Guard
  - Windows Defender Advanced Threat Protection (ATP) (E5 only)

## Resources

- [Office 365 Enterprise](https://microsoft.com)
- [Windows 10 Enterprise](https://microsoft.com)
- [Enterprise Mobility + Security (EMS)](https://microsoft.com)

---

**December 2019**

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