

Identity and Device Protection for Office 365

Recommended capabilities for protecting identities and devices that access Office 365, other SaaS services, and on-premises applications published with Azure AD Application Proxy

More architecture resources like this
aka.ms/cloudarch

See topics 2-4 for more information and resources.

Three tiers of protection for data, identities, and devices

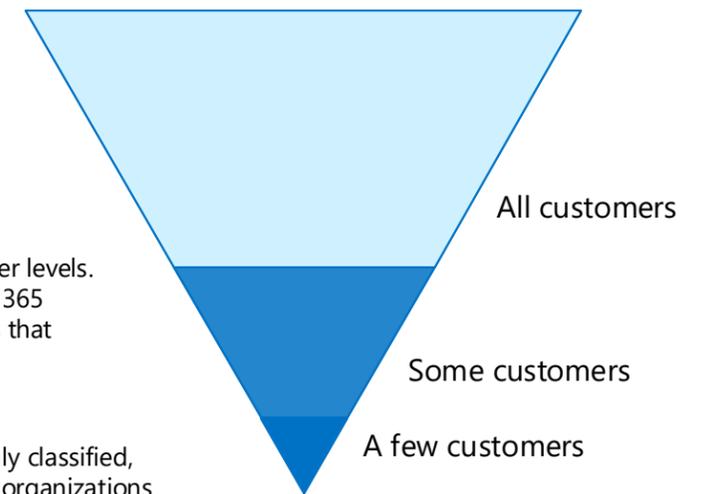
Microsoft provides many protection capabilities across our cloud services. We know it can be challenging to choose the right set of capabilities for your organization.

This document recommends the most common capabilities to help you secure your data, identities, and devices.

Capabilities are recommended in three tiers — baseline protection, sensitive protection, and protection for environments with highly regulated or classified data.

It's important to use consistent levels of protection across your data, identities, and devices. For example, if you protect sensitive data at a higher level, be sure to protect the identities and devices that access this data at a comparable level. This document shows you which capabilities are comparable.

- 1 Baseline protection**
 Microsoft recommends you establish a minimum standard for protecting data, as well as the identities and devices that access your data. Microsoft provides strong default protection that meets the needs of many organizations. Some organizations require additional capabilities to meet their baseline requirements.
- 2 Increased protection**
 Some customers have a subset of data that must be protected at higher levels. You can apply increased protection to specific data sets in your Office 365 environment. Microsoft recommends protecting identities and devices that access sensitive data with comparable levels of security.
- 3 Protection for highly regulated environments**
 Some organizations may have a very small amount of data that is highly classified, trade secret, or regulated data. Microsoft provides capabilities to help organizations meet these requirements, including added protection for identities and devices.



Summary of capabilities

	Baseline protection	Sensitive data protection	Highly regulated or classified data
Data protection Find more information about these capabilities here: File Protection Solutions in Office 365 .	<ul style="list-style-type: none"> Default file encryption Permissions for SharePoint and OneDrive for Business libraries External sharing policies Device access policies for SharePoint Online and OneDrive for Business 	<ul style="list-style-type: none"> Classification, labeling, and protection Data Loss Prevention (DLP) in Office 365 Office 365 service encryption with Customer Key (coming soon) Windows 10 capabilities: Bitlocker and Windows Information Protection (WIP) 	<ul style="list-style-type: none"> Bring Your Own Key (BYOK) with Azure Information Protection and SharePoint Online Hold Your Own Key (HYOK) with Active Directory Rights Management Service and SharePoint Online
Identity and device protection Identity and device capabilities work together to secure access to your data. This document includes more information about these capabilities plus additional recommendations.	<ul style="list-style-type: none"> Intune device management of PCs 	<ul style="list-style-type: none"> Mobile apps protection Intune device management of PCs and phones/tablets Azure Active Directory multi-factor authentication Azure Active Directory conditional access Azure Active Directory Identity Protection Microsoft Cloud App Security -or- Office 365 Cloud App Security Azure Active Directory Privileged Identity Management 	

Recommended policies for baseline, sensitive, and highly regulated protection

This page illustrates a set of policies Microsoft recommends for achieving protection at the three tiers.

For help implementing these policies, including policies for protecting email and SharePoint sites, see [Identity and device access configurations](#).

Protection level	Device type	Azure AD conditional access policies	Azure AD Identity Protection user risk policy	Intune device compliance policy	Intune app protection policies
Baseline	Laptop	Require multi-factor authentication (MFA) when sign-in risk is <i>medium</i> or <i>high</i>	Require compliant PCs	High risk users must change password (Forces users to change their password when signing in if high risk activity is detected for their account)	Define compliance policies (One policy for each platform)
	Phone	Require approved apps (Enforces mobile app protection for phones and tablets)	Block clients that don't support modern authentication (Clients that do not use modern authentication can bypass conditional access rules, so it's important to block these)		Define app protection policies (One policy per platform — iOS, Android)
Sensitive	Laptop	Require MFA when sign-in risk is <i>low</i> , <i>medium</i> , or <i>high</i>	Require compliant PCs <i>and</i> mobile devices (Enforces Intune management for PCs and phone/tablets)		
	Phone				
Highly regulated	Laptop	Always require MFA			
	Phone				

Start by implementing Azure Multi-Factor authentication (MFA). First, use an Identity Protection MFA registration policy to register users for MFA. After users are registered you can enforce MFA for sign-in.

Using multi-factor authentication is recommended before enrolling devices into Intune for assurance that the device is in the possession of the intended user.

Be sure to start using the pre-configured MFA policy for Admins — **Baseline policy: Require MFA for admins.**

For other SaaS apps in your environment, configure single sign-on with Azure AD and apply these rules or create new conditional access rules.

For all conditional access rules in Azure AD, configure an Azure AD group for 'Exclusion' and add this group to these rules. This gives you a way allow access to a critical user while you troubleshoot access issues.

Enroll devices for management with Intune before implementing device compliance policies.

Device compliance policies define the requirements devices must meet. Intune let's Azure AD know if devices pass and are compliant. Recommended requirements include:

- Use passwords with strong parameters (alphanumeric, at least six characters, expiration of no more than 90 days).
- Be patched, have anti-virus, and firewalls enabled.
- Use encryption, lock on inactivity, and wipe on multiple sign-in failures.
- Not be jailbroken or rooted.

App policies define which apps are allowed and what actions these apps can take with your organization content.

Product key

- All Office 365 Enterprise plans
- Microsoft 365 E3, Enterprise Mobility + Security (EMS) E3, Azure AD P1
- Microsoft 365 E5, EMS E5, Azure AD P2

Additional capabilities for baseline protection

These recommendations and capabilities increase the baseline level of protection across your environment.

Protect identities

Follow Microsoft's recommended guidelines for passwords

[Whitepaper: Microsoft Password Guidance](#)

This paper provides Microsoft's recommendations for password management based on current research and lessons from our own experience as one of the largest Identity Providers (IdPs) in the world.

- Maintain an 8-character minimum length requirement (and longer is not necessarily better).
- Eliminate character-composition requirements.
- Eliminate mandatory periodic password resets for user accounts.
- Ban common passwords, to keep the most vulnerable passwords out of your system.
- Educate your users not to re-use their password for non-work-related purposes.
- Combine these guidelines with MFA registration and risk-based challenges.

Use Azure AD password protection on premises

Eliminate weak passwords on premises by monitoring for banned passwords.

[Eliminate weak passwords on-premises](#)

Enable Azure AD Identity Protection Policies for your users

Enable Identity Protection (even in trial mode) to see the user and sign in risk of logins. Even without enabling policies, you will gain insights from the signals.

[Azure Active Directory Identity Management](#)

Protect admin accounts with PIM and privileged access management

[Start using Azure AD Privileged Identity Management](#)

[Use privileged access management in Office 365](#)

Manage the user lifecycle holistically

Remove manual steps from your employee account lifecycle everywhere you can to prevent unauthorized access:

- Synchronize identities from your source of truth (HR System) to Azure AD.
- Use Dynamic Groups to automatically assign users to groups based on their attributes from HR (or your source of truth), such as department, title, region, and other attributes.
- Use group-based licensing to assign services to your users automatically as soon as they arrive in the cloud. (Coming soon.)
- Use group-based access management/provisioning to automatically provision users for SaaS applications.

[Managing access to resources with Azure Active Directory groups](#)

[What is Microsoft Azure Active Directory licensing?](#)

Enable self-service password reset

Allow your users to reset their passwords, with no administrator intervention, when and where they need to.

[Quickstart: Self-service password reset](#)

[Password writeback to on-premises directories](#)

Migrate your external accounts to Azure AD B2B collaboration

External accounts on premises are a threat that you can mitigate by moving the accounts to Azure AD B2B collaboration.

Azure AD B2B Collaboration enables secure collaborate between business-to-business partners. Any accounts that are needed for SaaS application access or SharePoint Online collaboration can be moved to Azure AD B2B.

[Azure Active Directory B2B collaboration](#)

Implement Azure AD Connect Health

Monitor and gain insight into your on-premises identity infrastructure and the synchronization services with Azure AD Connect Health.

This enables you to maintain a reliable connection to Office 365 and Microsoft Online Services by providing monitoring capabilities for your key identity components such as AD FS Servers, Azure AD Connect servers (aka Sync Engine), Active Directory Domain Controllers etc.

It also makes the key data points about these components easily accessible, making it easy to get usage and other important insights to take informed decisions.

[What is Azure AD Connect Health?](#)

Protect devices

Configure basic password policies for mobile device access to Outlook Web Access (OWA)

Configure basic password policies for Outlook Web Access (OWA).

If you implement password policies using Intune later, these settings are disregarded. Intune password policies require device enrollment.

[Mobile device mailbox policies in Exchange Online](#)

Use Intune to manage applications on mobile devices

Manage applications on mobile devices regardless of whether the devices are enrolled for mobile device management.

Deploy apps, including LOB apps. Restrict actions like copy, cut, paste, and save as, to only apps managed by Intune. Enable secure web browsing using the Intune Managed Browser App. Enforce PIN and encryption requirements, offline access time, and other policy settings.

[What are app protection policies?](#)

Use Azure AD Join with Windows 10 devices

Azure AD offers a simplified joining experience, efficient device management, automatic mobile device management enrollment, and single sign-on capability for Azure AD and on-premises resources. An incremental step in this direction is to auto-Azure-AD join your on-premises joined Windows 10 devices.

[Extending cloud capabilities to Windows 10 devices through Azure Active Directory Join](#)

Implement Windows 10 native protection capabilities

BitLocker — Use this on all PCs to encrypt all data at rest and protect it against offline attacks.

Credential Guard — Prevents attacks by protecting NTLM password hashes and Kerberos Ticket Granting tickets.

Device Guard — Prevents tampering by users or malware, only allows trusted applications. AppLocker can also be used.

Enable Windows Hello for Business on all Windows 10 PCs

Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

[Windows Hello for Business](#)

Windows 10 PCs

Additional capabilities for sensitive and classified data

You can greatly increase protection with capabilities on this page. Choose the capabilities that are best for your environment.

Sensitive protection

Protect identities

Increase protections with Azure AD Identity Protection Policies for user accounts

For users who access highly regulated or classified data, use more risk-averse policies. For example, require MFA when sign in risk is low. Change risk access from high to medium or low.

[Azure Active Directory Identity Protection](#)

Enable Azure AD Privileged Identity Management

Enable 'just in time' Privileged Identity Management (PIM) for your privileged administrator accounts in the cloud. With PIM, your administrator accounts are not able to perform administrative actions until they request their role to be activated. Additionally, you can set parameters for a specific action. For example, you can require MFA, require them to fill out a service request number, or just notify other admins.

[Azure AD Privileged Identity Management](#)

Use Office 365 Advanced Security Management or Microsoft Cloud App Security

Use Office 365 Advanced Security Management to evaluate risk, to alert on suspicious activity, and to automatically take action. Requires Office 365 E5 plan.

Or, use Microsoft Cloud App Security to obtain deeper visibility even after access is granted, comprehensive controls, and improved protection for all your cloud applications, including Office 365. Requires EMS E5 plan.

Start with default policies and settings.

[Overview of Office 365 Cloud App Security](#)

[Microsoft Cloud App Security](#)

Protection for highly regulated data

Use Microsoft Cloud App Security with additional policies

For highly regulated or classified data, implement more advanced policies to alert you and to take action on suspicious activity or leaked data.

[Microsoft Cloud App Security](#)

Increase protection with Azure AD Privileged Identity Management

For admins who work with services that host highly regulated or classified data, increase protection by requiring MFA on activation of their role. Also activate roles for shorter time windows.

[Azure AD Privileged Identity Management](#)

For an HYOK solution, add partner accounts to your on-premises directory

If you are using an HYOK solution to protect data stored in SharePoint Online, add necessary partner accounts to your on-premises directory. HYOK solutions for files stored in SharePoint Online require federated identity integration with Office 365. These solutions do not work with synchronized identities.

Protect devices

Use device health attestation features with Windows 10 devices

If you choose to enable "Windows Device Health Attestation" in a device compliance policy, create a separate policy. When you create the corresponding conditional access policy in Azure AD, configure the policy to apply only to the Windows platform. Use caution with this policy because it will deny access to Windows devices that do not support Device Health Attestation.

The Health Attestation Service is a trusted cloud service operated by Microsoft that reports what security features are enabled on the device.

[Device Health Attestation](#)

Use Windows Information Protection (WIP) to protect apps on Windows 10 devices

Windows Information Protection allows you to protect data within Microsoft Intune-managed applications.

[Create a Windows Information Protection \(WIP\) policy using Microsoft Intune](#)

Deploy a 3rd party, real-time threat detection solution for non-Windows devices

Microsoft provides Lookout Mobile Endpoint Security integration with Microsoft Enterprise Mobility + Security (EMS). Lookout provides real-time application, OS, and network-level protection for devices.

[Microsoft and Lookout: Securing all your endpoints begins today](#)

Windows 10 PCs