

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



# Three tiers of protection for data, identities, and devices

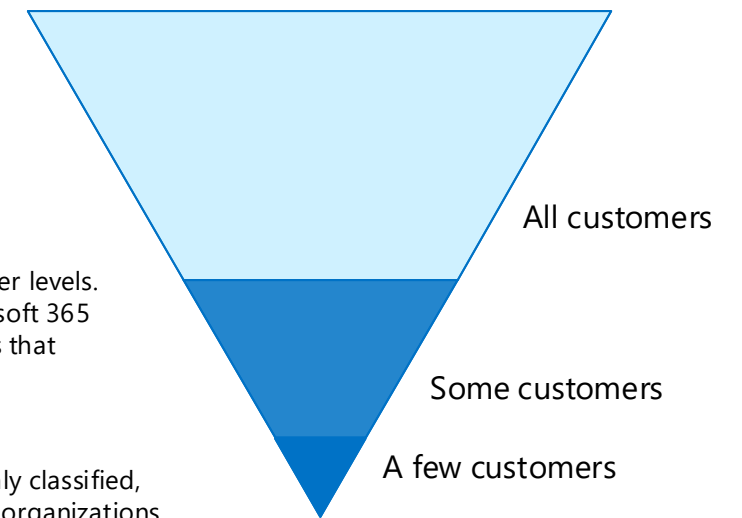
It's important to use consistent levels of protection across your data, identities, and devices. For example, if you protect sensitive data at a higher level, be sure to protect the identities and devices that access this data at a comparable level. This document shows you which capabilities are comparable.

- 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 Microsoft 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
<b>Data protection</b> Find more information about these capabilities here: <a href="#">Deploy information protection for data privacy regulations.</a>	Default file encryption	Classification, labeling, and protection	Bring Your Own Key (BYOK) with Azure Information Protection and SharePoint
	Permissions for SharePoint and OneDrive libraries	Data Loss Prevention (DLP) in Microsoft 365	Hold Your Own Key (HYOK) with Active Directory Rights Management Service and SharePoint
	External sharing policies	Microsoft 365 service encryption with Customer Key	
	Device access policies for SharePoint and OneDrive	Windows 10 capabilities: Bitlocker and Windows Information Protection (WIP)	

	Baseline protection	Sensitive data protection	Highly regulated or classified data
<b>Identity and device protection</b>  Identity and device capabilities work together to secure access to your data. This document includes more information about these capabilities plus additional recommendations.	Mobile apps protection		
	Intune device management of PCs	Intune device management of PCs and phones/tablets	
	Azure Multi-Factor Authentication		
	Azure AD Conditional Access		
	Azure AD Identity Protection		
		Microsoft Cloud App Security	
		Azure AD 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 Teams, Exchange 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	PCs	Require multi-factor authentication (MFA) when sign-in risk is <i>medium</i> or <i>high</i>	Require approved apps This policy 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 policies.	Require compliant PCs	High risk users must change password  This policy forces users to change their password when signing in if high risk activity is detected for their account.	Define compliance policies (one for each platform)	Apply Level 2 App Protection Policies (APP) data protection (one for each platform)
	Phones and tablets							
Sensitive	PCs	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  This policy enforces Intune management for PCs, phones, and tablets.			
	Phones and tablets							
Highly regulated	PCs	Require MFA <i>always</i>  This is also available for all Office 365 Enterprise plans.						
	Phones and tablets							

Start by implementing 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 MFA is recommended before enrolling devices into Intune for assurance that the device is in the possession of the intended user.

For other SaaS apps in your environment, configure single sign-on with Azure AD and apply these policies or create new Conditional Access policies.

For all Conditional Access policies in Azure AD, configure an Azure AD exclusion group and add this group to these policies. This gives you a way to allow access to a critical user while you troubleshoot access issues for them.

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

Device compliance policies define the requirements devices must meet. Intune lets Azure AD know if devices are compliant. Recommended requirements include:

- Use passwords with strong parameters (alphanumeric, at least six characters, expiration of no more than 90 days).
- Be patched and 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.

**PCs** include devices running the Windows or macOS platforms

**Phones and tablets** include devices running the iOS, iPadOS, or Android platforms

Requires Microsoft 365 E5, Microsoft 365 E3 with the Identity & Threat Protection add-on, Office 365 with EMS E5, or individual Azure AD Premium P2 licenses

Additional capabilities for baseline protection

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

Protect identities	<div>Follow Microsoft’s recommended guidelines for passwords</div> <p>The <a href="#">Microsoft Password Guidance</a> paper provides recommendations for password management based on current research and lessons from Microsoft’s experience as one of the largest Identity Providers (IdPs) in the world.</p> <ul style="list-style-type: none"><li>Maintain an 8-character minimum length requirement (and longer is not necessarily better).</li><li>Eliminate character-composition requirements.</li><li>Eliminate mandatory periodic password resets for user accounts.</li><li>Ban common passwords, to keep the most vulnerable passwords out of your system.</li><li>Educate your users not to re-use their password for non-work-related purposes.</li><li>Combine these guidelines with MFA registration and risk-based challenges.</li></ul>	<div>Use Azure AD password protection on premises</div> <p>Eliminate weak passwords on premises by monitoring for banned passwords. <a href="#">Eliminate weak passwords on-premises</a></p> <div>Enable Azure AD Identity Protection policies for your users</div> <p>Enable Identity Protection to see the user and sign in risk of logins. Even without enabling policies, you will gain insights from the signals. <a href="#">Azure AD Identity Protection</a></p> <div>Protect admin accounts with PIM and privileged access management</div> <p><a href="#">Azure AD Privileged Identity Management</a> <a href="#">Privileged access management in Microsoft 365</a></p>	<div>Manage the user lifecycle holistically</div> <p>Remove manual steps from your employee account lifecycle everywhere you can to prevent unauthorized access:</p> <ul style="list-style-type: none"><li>Synchronize identities from your source of truth (HR System) to Azure AD.</li><li>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.</li><li>Use group-based licensing to assign services to your users automatically as soon as they arrive in the cloud.</li><li>Use group-based access management/provisioning to automatically provision users for SaaS applications.</li></ul> <p><a href="#">Manage access to resources with Azure AD groups</a> <a href="#">Microsoft Azure AD licensing</a></p>	<div>Enable self-service password reset</div> <p>Allow your users to reset their passwords, with no administrator intervention, when and where they need to. <a href="#">Self-service password reset</a> <a href="#">Password writeback to on-premises directories</a></p> <div>Migrate your external accounts to Azure AD B2B collaboration</div> <p>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 collaboration can be moved to Azure AD B2B. <a href="#">Azure AD B2B collaboration</a></p>	<div>Implement Azure AD Connect Health</div> <p>Monitor and gain insight into your on-premises identity infrastructure and the synchronization services with Azure AD Connect Health.</p> <p>This enables you to maintain a reliable connection to Microsoft 365 by providing monitoring capabilities for your key identity components such as Azure AD Connect servers, Active Directory Domain Services (AD DS) domain controllers, and Active Directory Federation Services (AD FS) servers.</p> <p>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. <a href="#">Azure AD Connect Health</a></p>
	<div>Configure basic password policies for mobile device access to Outlook Web Access (OWA)</div> <p>Configure basic password policies for Outlook Web Access (OWA).</p> <p>If you implement password policies using Intune later, these settings are disregarded. Intune password policies require device enrollment. <a href="#">Mobile device mailbox policies in Exchange Online</a></p>	<div>Use Intune to manage applications on mobile devices</div> <p>Manage applications on mobile devices regardless of whether the devices are enrolled for mobile device management.</p> <p>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. <a href="#">Intune app protection policies</a></p>	<div>Use Azure AD Join with Windows 10 devices</div> <p>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.</p> <p>An incremental step in this direction is to auto-Azure-AD join your on-premises joined Windows 10 devices. <a href="#">Extending cloud capabilities to Windows 10 devices through Azure AD Join</a></p>	<div>Implement Windows 10 native protection capabilities</div> <p><b>BitLocker</b> — Use this on all PCs to encrypt all data at rest and protect it against offline attacks.</p> <p><b>Credential Guard</b> — Prevents attacks by protecting NTLM password hashes and Kerberos Ticket Granting tickets.</p> <p><b>Device Guard</b> — Prevents tampering by users or malware and only allows trusted applications. AppLocker can also be used.</p>	<div>Enable Windows Hello for Business on all Windows 10 PCs</div> <p>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. <a href="#">Windows Hello for Business</a></p>

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.

## Protect identities

### Sensitive protection

Increase protection with Azure AD Identity Protection policies for user accounts	Enable Azure AD Privileged Identity Management	Use Microsoft Cloud App Security
<p>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.</p> <p><a href="#">Azure AD Identity Protection</a></p>	<p>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.</p> <p><a href="#">Azure AD Privileged Identity Management</a></p>	<p>Microsoft Cloud App Security is a Cloud Access Security Broker that supports various deployment modes including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services. Requires Microsoft 365 E5.</p> <p><a href="#">Microsoft Cloud App Security</a></p>

### Protection for highly regulated data

Use Microsoft Cloud App Security with advanced policies	Increase protection with Azure AD Privileged Identity Management	For an HYOK solution, add partner accounts to your on-premises directory
<p>For highly regulated or classified data, implement more advanced policies to alert you and to take action on suspicious activity or leaked data.</p> <p><a href="#">Microsoft Cloud App Security</a></p>	<p>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.</p> <p><a href="#">Azure AD Privileged Identity Management</a></p>	<p>If you are using a Hold Your Own Key (HYOK) solution to protect data stored in SharePoint, add necessary partner accounts to your on-premises directory. HYOK solutions for files stored in SharePoint require federated identity integration with Microsoft 365. These solutions do not work with synchronized identities.</p>

## Protect devices

Use device health attestation features with Windows 10 devices	Use Windows Information Protection (WIP) to protect apps on Windows 10 devices
<p>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.</p>	<p>The Health Attestation Service is a trusted cloud service operated by Microsoft that reports what security features are enabled on the device.</p> <p>WIP allows you to protect data within Intune-managed applications.</p> <p><a href="#">Create a WIP policy using Microsoft Intune</a></p>

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

Windows 10 PCs