

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 guest access and Teams, see [Identity and device access configurations](#) (aka.ms/m365goldenconfig).

<http://aka.ms/m365goldenconfig>

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 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)	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						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 and 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

Recommended additions for allowing guest access

1

Create this new rule and apply it only to guests and external users. Under sign-in risk, leave all options unchecked to always enforce MFA.

2

Modify these rules to exclude guest and external users.

Users and groups

Include

Exclude

☒




All guest and external users (Preview) ⓘ

☐

Directory roles (Preview) ⓘ

☐

Users and groups

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) always for guests and external users  New	Require multi-factor authentication (MFA) when sign-in risk is <i>medium</i> or <i>high</i>  Exclude guest and external users		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)	Require compliant PCs Exclude guest and external users 	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)				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 and mobile devices (Enforces Intune management for PCs and phone/tablets)		
	Phone							
Highly regulated	Laptop		Always require MFA					
	Phone							

For help implementing these policies, including policies for protecting guest access and Teams, see [Identity and device access configurations](https://aka.ms/m365goldenconfig) (aka.ms/m365goldenconfig).

[http://aka.ms/m365goldenconfig](https://aka.ms/m365goldenconfig)