

Devices

Assessment results

Config

Assessment results

The results presented below are based on the security principles detailed in the [Configuring Microsoft Intune for increased security guide](#).

Search by name...

Risk:

High

Medium

Low

Status:

Failed

Skipped

Filter by SFI Pillar:

Showing 36 of 36 tests

Protect identities and secrets

Protect networks

Protect tenants and isolate production

Protect tenants and isolate production systems

Name ↑↓	Category ↑↓	Risk ↑↓	Status ↑↓
Conditional Access policies block access from noncompliant devices	Data	↑ High	Skipped
Conditional Access policies block access from unmanaged apps	Data	↑ High	Skipped
Data on Android is protected by app protection policies	Data	↑ High	Skipped
Data on iOS/iPadOS is protected by app protection policies	Data	↑ High	Skipped
Secure Wi-Fi profiles protect Android devices from unauthorized network access	Data	↑ High	Skipped

Secure Wi-Fi profiles protect iOS devices from unauthorized network access	Data	↑	High	Skipped
Secure Wi-Fi profiles protect macOS devices from unauthorized network access	Data	↑	High	Skipped
Attack Surface Reduction rules are applied to Windows devices to prevent exploitation of vulnerable system components	Device	↑	High	Skipped
Authentication on Windows uses Windows Hello for Business	Device	↑	High	Skipped
Data on Windows is protected by BitLocker encryption	Device	↑	High	Skipped
Defender Antivirus policies protect macOS devices from malware	Device	↑	High	Skipped
Defender Antivirus policies protect Windows devices from malware	Device	↑	High	Skipped
FileVault encryption protects data on macOS devices	Device	↑	High	Skipped
Local account usage on Windows is restricted to reduce unauthorized access	Device	↑	High	Skipped
Local administrator credentials on macOS are protected during enrollment by macOS LAPS	Device	↑	High	Skipped
Local administrator credentials on Windows are protected by Windows LAPS	Device	↑	High	Skipped

macOS Firewall policies protect against unauthorized network access	Device	→ Medium	Skipped
Update policies for iOS/iPadOS are enforced to reduce risk from unpatched vulnerabilities	Device	↑ High	Skipped
Update policies for macOS are enforced to reduce risk from unpatched vulnerabilities	Device	↑ High	Skipped
Windows Firewall policies protect against unauthorized network access	Device	↑ High	Skipped
Windows Update policies are enforced to reduce risk from unpatched vulnerabilities	Device	↑ High	Skipped
Windows automatic device enrollment is enforced to eliminate risks from unmanaged endpoints	Tenant	↑ High	Failed
Company Portal branding and support settings enhance user experience and trust	Tenant	→ Medium	Skipped
Compliance policies protect fully managed and corporate-owned Android devices	Tenant	↑ High	Skipped
Compliance policies protect iOS/iPadOS devices	Tenant	↑ High	Skipped
Compliance policies protect macOS devices	Tenant	↑ High	Skipped
Compliance policies protect personally owned Android devices	Tenant	↑ High	Skipped

Compliance policies protect Windows devices	Tenant	↑ High	Skipped
Defender for Endpoint automatic enrollment is enforced to reduce risk from unmanaged Android threats	Tenant	↑ High	Skipped
Device cleanup rules maintain tenant hygiene by hiding inactive devices	Tenant	↓ Low	Skipped
Device enrollment notifications are enforced to ensure user awareness and secure onboarding	Tenant	→ Medium	Skipped
Endpoint Analytics is enabled to help identify risks on Windows devices	Tenant	↓ Low	Skipped
Platform SSO is configured to strengthen authentication on macOS devices	Tenant	→ Medium	Skipped
Scope tag configuration is enforced to support delegated administration and least-privilege access	Tenant	→ Medium	Skipped
Security baselines are applied to Windows devices to strengthen security posture	Tenant	↑ High	Skipped
Terms and Conditions policies protect access to sensitive data	Tenant	→ Medium	Skipped



Zero Trust Assessment

An automated assessment tool that evaluates your Microsoft tenant's zero trust security posture.

Resources

Zero Trust Assessment

Zero Trust Workshop

Support

Share Feedback

Report Issues

 [GitHub](#)

© 2025 Microsoft Corporation. All rights reserved.

This is a community project and not an official Microsoft product.

[Privacy](#) • [Terms](#) • December 1, 2025