Zero Trust Assessment Google

Assessment results Config

Device Configuration

Device configuration settings and options.

Windows automatic enrollment

Configure Windows devices to enroll when they join or register with Azure Active Directory. We recommend setting this to all instead of selected groups and using enrollment restrictions to configure the intake of users.

No Windows enrollment configuration found.

Enrollment device platform restrictions

Device enrollment restrictions let you restrict devices from enrolling in Intune based on certain device attributes. Device platform restrictions restrict devices based on device platform, version, manufacturer, or ownership type.

No device enrollment restrictions found.

Compliance policies

Device compliance policies define the rules and settings that devices must meet to be considered compliant. These policies help ensure that devices accessing organizational resources meet minimum security requirements.

No device compliance policies found.

App protection policies

App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.

No app protection policies found.

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

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

Privacy • Terms • December 1, 2025