

Identity

Assessment results

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

[Search by](#)[Risk:](#) [High](#) [Medium](#) [Low](#) [Status:](#) [Passed](#) [Failed](#) [Planned](#) [Skipped](#)[Filter by SFI Pillar:](#) [Clear All \(7\)](#)[Clear All Filters](#)

Showing 130 of 130 tests

[Accelerate response and remediation](#)[Monitor and detect cyberthreats](#)[Protect engineering systems](#)[Protect identities and secrets](#)[Protect networks](#)[Protect tenants and isolate production systems](#)[Protect tenants and production systems](#)

Name ↑	Risk ↑	Status ↑
Admin consent workflow is enabled	↑ High	Failed
Enterprise applications with high privilege Microsoft Graph API permissions have owners	↑ High	Failed
User consent settings are restricted	↑ High	Failed
Limit the maximum number of devices per user to 10	↑ High	Failed
Security key attestation is enforced	↑ High	Failed
Restrict non-administrator users from recovering the BitLocker keys for their owned devices	↑ High	Failed
Permissions to create new tenants are limited to the Tenant Creator role	↑ High	Failed

Local Admin Password Solution is deployed	↑ High	Failed
Reduce the user-visible password surface area	↑ High	Failed
Tenant restrictions v2 policy is configured	↑ High	Failed
Manage the local administrators on Microsoft Entra joined devices	↑ High	Failed
Migrate from legacy MFA and SSPR policies	↑ High	Failed
Passkey authentication method enabled	↑ High	Failed
Outbound cross-tenant access settings are configured	↑ High	Failed
Block administrators from using SSPR	↑ High	Failed
Security key authentication method enabled	↑ High	Failed
High Global Administrator to privileged user ratio	↑ High	Failed
SMS and Voice Call authentication methods are disabled	↑ High	Passed
Privileged accounts have phishing-resistant methods registered	↑ High	Passed
Entra Connect Sync is configured with Service Principal Credentials	↑ High	Passed
Use cloud authentication	↑ High	Passed
Workload Identities are not assigned privileged roles	↑ High	Passed

Control	Risk	Status
App instance property lock is configured for all multitenant applications	↑ High	Passed
Inactive applications don't have highly privileged built-in roles	↑ High	Passed
App registrations use safe redirect URIs	↑ High	Passed
Global Administrators don't have standing access to Azure subscriptions	↑ High	Passed
Applications don't have client secrets configured	↑ High	Passed
Service principals use safe redirect URIs	↑ High	Passed
Microsoft services applications don't have credentials configured	↑ High	Passed
Application certificates must be rotated on a regular basis	↑ High	Passed
Password protection for on-premises is enabled	↑ High	Passed
Privileged accounts are cloud native identities	↑ High	Passed
High priority Microsoft Entra recommendations are addressed	↑ High	Passed
Guests are not assigned high privileged directory roles	↑ High	Passed
App registrations must not have dangling or abandoned domain redirect URIs	↑ High	Passed
All risk detections are triaged	↑ High	Planned
Require password reset notifications for administrator roles	↑ High	Planned

Azure subscriptions used by Identity Governance are secured consistently with Identity Governance roles	↑ High	Planned
ID Protection notifications are enabled	↑ High	Planned
Privileged users sign in with phishing-resistant methods	↑ High	Planned
Azure resources used by Microsoft Entra only allow access from privileged roles	↑ High	Planned
Authentication transfer is blocked	↑ High	Skipped
All privileged role assignments are activated just in time and not permanently active	↑ High	Skipped
User sign-in activity uses token protection	↑ High	Skipped
All risky workload identity sign-ins are triaged	↑ High	Skipped
All Microsoft Entra privileged role assignments are managed with PIM	↑ High	Skipped
Emergency access accounts are configured appropriately	↑ High	Skipped
Restrict high risk sign-ins	↑ High	Skipped
Privileged Microsoft Entra built-in roles are targeted with Conditional Access policies to enforce phishing-resistant methods	↑ High	Skipped
Restrict device code flow	↑ High	Skipped
Restrict access to high risk users	↑ High	Skipped

Secure the MFA registration (My Security Info) page	↑ High	Skipped
Require multifactor authentication for device join and device registration using user action	↑ High	Skipped
Conditional Access policies for workload identities based on known networks are configured	↑ High	Skipped
Conditional Access policies for Privileged Access Workstations are configured	↑ High	Skipped
All risky workload identities are triaged	↑ High	Skipped
All sign-in activity comes from managed devices	↑ High	Skipped
Diagnostic settings are configured for all Microsoft Entra logs	↑ High	Skipped
Maximum number of Global Administrators doesn't exceed five users	↓ Low	Passed
All certificates Microsoft Entra Application Registrations and Service Principals must be issued by an approved certification authority	↓ Low	Planned
Block legacy Microsoft Online PowerShell module	↓ Low	Planned
All users are required to register for MFA	↓ Low	Planned
No Active low priority Entra recommendations found	↓ Low	Planned
Directory Sync account credentials haven't been rotated recently	↓ Low	Planned
Directory sync account is locked down to specific named location	↓ Low	Planned

Application Certificate Credentials are managed using HSM	↓ Low	Planned
Activation alert for all privileged role assignments	↓ Low	Skipped
Activation alert for Global Administrator role assignment	↓ Low	Skipped
Enable protected actions to secure Conditional Access policy creation and changes	↓ Low	Skipped
Workload Identities are configured with risk-based policies	→ Medium	Failed
Microsoft Authenticator app shows sign-in context	→ Medium	Failed
Block legacy Azure AD PowerShell module	→ Medium	Failed
All Microsoft Entra recommendations are addressed	→ Medium	Failed
Guests have restricted access to directory objects	→ Medium	Failed
Resource-specific consent is restricted	→ Medium	Failed
Smart lockout threshold set to 10 or less	→ Medium	Failed
Guest access is limited to approved tenants	→ Medium	Failed
Restrict Temporary Access Pass to Single Use	→ Medium	Failed
Enforce standards for app secrets and certificates	→ Medium	Failed
Add organizational terms to the banned password list	→ Medium	Failed
Microsoft Authenticator app report suspicious activity setting is enabled	→ Medium	Failed

Guest access is limited to approved tenants	→ Medium	Failed
Inactive applications don't have highly privileged Microsoft Graph API permissions	→ Medium	Failed
Guests can't invite other guests	→ Medium	Failed
Creating new applications and service principals is restricted to privileged users	→ Medium	Failed
Enterprise applications must require explicit assignment or scoped provisioning	→ Medium	Passed
Password expiration is disabled	→ Medium	Passed
Enterprise applications have owners	→ Medium	Passed
All guests have a sponsor	→ Medium	Passed
Guests do not own apps in the tenant	→ Medium	Passed
Applications are configured for automatic user provisioning	→ Medium	Passed
Guests don't have long lived sign-in sessions	→ Medium	Passed
No usage of ADAL in the tenant	→ Medium	Passed
Guest self-service sign-up via user flow is disabled	→ Medium	Passed
Service principals don't have certificates or credentials associated with them	→ Medium	Passed
Applications don't have certificates with expiration longer than 180 days	→ Medium	Passed

Smart lockout duration is set to a minimum of 60	→ Medium	Passed
Turn off Seamless SSO if there is no usage	→ Medium	Planned
GDAP admin least privilege	→ Medium	Planned
Protected actions are enabled for high-impact management tasks	→ Medium	Planned
Guest access is protected by strong authentication methods	→ Medium	Planned
All registered redirect URIs must have proper DNS records and ownerships	→ Medium	Planned
All user sign-in activity uses strong authentication methods	→ Medium	Planned
No nested groups in PIM for groups	→ Medium	Planned
All app assignment and group membership is governed	→ Medium	Planned
No Active Medium priority Entra recommendations found	→ Medium	Planned
All supported access lifecycle resources are managed with entitlement management packages	→ Medium	Planned
All privileged role assignments have a recipient that can receive notifications	→ Medium	Planned
Use PIM for Microsoft Entra privileged roles	→ Medium	Planned
Enable self-service password reset	→ Medium	Planned
Require password reset notifications for user roles	→ Medium	Planned

Privileged roles aren't assigned to stale identities	→ Medium	Planned
Privileged roles have access reviews	→ Medium	Planned
No legacy authentication sign-in activity	→ Medium	Planned
Guest identities are lifecycle managed with access reviews	→ Medium	Planned
Self-service password reset doesn't use security questions	→ Medium	Planned
Guest access is restricted	→ Medium	Planned
Token protection policies are configured	→ Medium	Skipped
All entitlement management packages that apply to guests have expirations or access reviews configured in their assignment policies	→ Medium	Skipped
Named locations are configured	→ Medium	Skipped
Inactive guest identities are disabled or removed from the tenant	→ Medium	Skipped
All entitlement management policies that apply to External users require approval	→ Medium	Skipped
All entitlement management policies have an expiration date	→ Medium	Skipped
All entitlement management assignment policies that apply to external users require connected organizations	→ Medium	Skipped
Temporary access pass is enabled	→ Medium	Skipped

All groups in Conditional Access policies belong to a restricted management administrative unit	→ Medium	Skipped
Privileged users have short-lived sign-in sessions	→ Medium	Skipped
Users have strong authentication methods configured	→ Medium	Skipped
Block legacy authentication policy is configured	→ Medium	Skipped
All user sign in activity uses phishing-resistant authentication methods	→ 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