

14 Microsoft 365 and Azure security settings to check

Groupe Conseil GRD. Sources accessed October 29, 2026. NIST CSF 2.0 mapping: GV, ID, PR, DE, RS, RC (https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.29.pdf, published February 26, 2024).

1. **MFA for all users (Conditional Access).** According to Microsoft, multifactor authentication combined with blocking legacy authentication blocks 99.9% of common identity-related attacks. NIST: PR (Protect). Source: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-mfa-strength> and <https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>
2. **Security defaults (without a Premium licence).** Microsoft recommends them for organizations using the free tier of Microsoft Entra ID. Once enabled, all users must register for multifactor authentication. NIST: PR. Source: <https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>
3. **Block legacy authentication.** According to Microsoft, more than 97% of credential stuffing attacks and more than 99% of password spray attacks use legacy authentication. NIST: PR. Source: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-legacy-authentication>
4. **Limit Global Administrators.** Microsoft recommends fewer than five people with the Global Administrator role. NIST: PR. Source: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices>
5. **Privileged Identity Management (PIM).** Approved, just-in-time privileged access. NIST: PR. Source: <https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure>
6. **Emergency access accounts.** Microsoft recommends creating two or more. NIST: RC (Recover). Source: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access>
7. **Track Microsoft Secure Score.** A measure of security posture: the higher the score, the more recommended actions have been applied. NIST: ID (Identify). Source: <https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score>
8. **Defender for Office 365 preset security policies (Standard or Strict).** NIST: PR and DE (Detect). Source: <https://learn.microsoft.com/en-us/defender-office-365/preset-security-policies>
9. **Audit logging on.** Check that unified auditing is enabled. NIST: DE. Source: <https://learn.microsoft.com/en-us/purview/audit-log-enable-disable>
10. **External sharing and "Anyone" links.** "Anyone" links allow access without authentication; they can be restricted (expiration, read-only). NIST: PR. Source: <https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off>
11. **Data loss prevention (Purview DLP).** Tools to protect sensitive items wherever they are. NIST: PR. Source: <https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp>

Azure

1. **Microsoft Defender for Cloud:** a cloud-native application protection platform (CNAPP) that evaluates configuration against frameworks such as CIS, NIST or PCI. NIST: ID and DE. Source: <https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction>

2. **Microsoft Cloud Security Benchmark (MCSB)**: maps to the CIS Controls, NIST and PCI-DSS frameworks. NIST: GV. Source: <https://learn.microsoft.com/en-us/security/benchmark/azure/introduction>
3. **Azure RBAC, least privilege**: Microsoft recommends a maximum of 3 subscription owners. NIST: PR. Source: <https://learn.microsoft.com/en-us/azure/role-based-access-control/best-practices>

Need help? Request a quote: info@grdinc.ca