

Les 14 réglages de sécurité Microsoft 365 et Azure à vérifier

Groupe Conseil GRD. Sources ouvertes le 29 octobre 2026. Correspondance NIST CSF 2.0 : GV, ID, PR, DE, RS, RC (<https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.29.pdf>, publié le 26 février 2024).

1. **Authentification multifacteur pour tous (accès conditionnel).** Selon Microsoft, l'authentification multifacteur combinée au blocage de l'authentification héritée bloque 99,9 % des attaques courantes liées à l'identité. NIST : PR (Protéger). Source : <https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-mfa-strength> et <https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>
2. **Paramètres de sécurité par défaut (si pas de licence Premium).** Microsoft les recommande aux organisations utilisant le niveau gratuit de Microsoft Entra ID. Une fois activés, tous les utilisateurs doivent s'inscrire à l'authentification multifacteur. NIST : PR. Source : <https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>
3. **Bloquer l'authentification héritée.** Selon Microsoft, plus de 97 % des attaques par bourrage d'identifiants et plus de 99 % des attaques par pulvérisation de mots de passe utilisent l'authentification héritée. NIST : PR. Source : <https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-legacy-authentication>
4. **Limiter les administrateurs généraux.** Microsoft recommande moins de cinq personnes avec le rôle Administrateur général. NIST : PR. Source : <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices>
5. **Privileged Identity Management (PIM).** Accès privilégié juste à temps et approuvé. NIST : PR. Source : <https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure>
6. **Comptes d'accès d'urgence.** Microsoft recommande d'en créer deux ou plus. NIST : RC (Rétablir). Source : <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access>
7. **Suivre Microsoft Secure Score.** Mesure de la posture de sécurité : plus le score est élevé, plus il y a d'actions recommandées appliquées. NIST : ID (Identifier). Source : <https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score>
8. **Stratégies prédéfinies Defender pour Office 365 (Standard ou Strict).** NIST : PR et DE (Détecter). Source : <https://learn.microsoft.com/en-us/defender-office-365/preset-security-policies>
9. **Journal d'audit activé.** Vérifier que l'audit unifié est activé. NIST : DE. Source : <https://learn.microsoft.com/en-us/purview/audit-log-enable-disable>
10. **Partage externe et liens « Tout le monde ».** Les liens « Tout le monde » permettent l'accès sans authentification; on peut les restreindre (expiration, lecture seule). NIST : PR. Source : <https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off>
11. **Protection contre la perte de données (Purview DLP).** Outils pour protéger les éléments sensibles où qu'ils se trouvent. NIST : PR. Source : <https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp>

Volet Azure

1. **Microsoft Defender for Cloud.** : plateforme de protection des applications infonuagiques (CNAPP), évalue la configuration selon des cadres comme CIS, NIST ou PCI. NIST : ID et DE. Source : <https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction>
2. **Microsoft Cloud Security Benchmark (MCSB).** : correspond aux cadres CIS Controls, NIST et PCI-DSS. NIST : GV. Source : <https://learn.microsoft.com/en-us/security/benchmark/azure/introduction>
3. **RBAC Azure, moindre privilège.** : Microsoft recommande au maximum 3 propriétaires d'abonnement. NIST : PR. Source : <https://learn.microsoft.com/en-us/azure/role-based-access-control/best-practices>

Besoin d'aide ? Demander une soumission : info@grdinc.ca