AYI NEDJIMI Consultants

Sécuriser Entra ID : configuration avancée et pratiques

Catégorie : IAM et Gestion des Identités Lecture : 6 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Sécurisez votre tenant Entra ID avec ce guide avancé : accès conditionnel, PIM, protection des identités et durcissement des configurations Azure AD.

Entra ID, anciennement Azure Active Directory, est devenu le plan de contrôle identitaire de millions d'organisations dans le monde. Chaque jour, des milliards d'authentifications transitent par cette plateforme, ce qui en fait une cible de choix pour les attaquants. Pourtant, la majorité des tenants Entra ID fonctionnent avec des configurations par défaut qui laissent des portes ouvertes béantes. Consentement applicatif non restreint, absence de politiques d'accès conditionnel sur les comptes admins, PIM non activé — la liste des failles courantes est longue. Ce guide détaille les configurations avancées à implémenter pour transformer votre tenant Entra ID en forteresse. De la protection des comptes Global Admin à la détection des attaques par Identity Protection, chaque recommandation est accompagnée de la procédure technique et du niveau de priorité. Nous nous appuyons sur les benchmarks CIS Microsoft 365 et les retours d'expérience de dizaines d'audits réalisés sur des tenants de toutes tailles. Vous repartirez avec une checklist actionnable et priorisée pour votre environnement.

Points clés à retenir

- Réduisez le nombre de **Global Admins** à 2 comptes break-glass maximum
- Activez **PIM** (Privileged Identity Management) pour tous les rôles d'administration
- Bloquez le **consentement applicatif utilisateur** et centralisez les approbations
- Déployez au minimum 5 politiques d'**accès conditionnel** fondamentales
- Configurez **Identity Protection** avec des actions automatiques sur les risques élevés

Durcissement des comptes Global Admin

Le rôle **Global Administrator** dans Entra ID donne un contrôle total sur le tenant. C'est l'équivalent du compte Domain Admin dans Active Directory, mais avec une surface d'attaque encore plus large puisqu'il couvre aussi Exchange Online, SharePoint, Teams et toutes les applications intégrées. La première action est de réduire le nombre de Global Admins au strict minimum. Deux comptes break-glass (comptes d'urgence) suffisent. Ces comptes doivent être exclus des politiques d'accès conditionnel classiques mais protégés par des alertes de connexion spécifiques.

Les comptes break-glass suivent des règles strictes : mots de passe de 30 caractères stockés dans deux coffres-forts physiques distincts, pas de MFA (pour garantir l'accès en cas de panne de l'IdP), monitoring de chaque connexion via une règle d'alerte dans les journaux d'audit Microsoft 365. Pour l'administration quotidienne, tous les autres rôles passent par **PIM** avec activation Just-In-Time.

Cinq politiques d'accès conditionnel indispensables

L'accès conditionnel est le moteur de sécurité d'Entra ID. Voici les cinq politiques à déployer en priorité. Première politique : MFA obligatoire pour tous les utilisateurs, toutes les applications, sans exception. Deuxième politique : blocage des connexions depuis les pays où votre organisation n'a pas de présence (named locations). Troisième politique : **exigence de terminal conforme** (Intune compliant device) pour accéder aux données sensibles SharePoint et Exchange.

Quatrième politique : blocage des protocoles d'authentification legacy (IMAP, POP3, SMTP Auth, ActiveSync avec basic auth) — ces protocoles ne supportent pas le MFA et sont le vecteur n°1 des attaques par password spraying. Cinquième politique : session restreinte pour les connexions à risque moyen (fréquence de reauthentification à 1 heure, pas de persistent browser session). Ces cinq politiques couvrent 90% des vecteurs d'attaque courants sur Entra ID.

PIM : l'administration Just-In-Time

Privileged Identity Management (PIM) transforme les attributions de rôles permanentes en activations temporaires avec approbation. Un administrateur Exchange n'a plus le rôle en permanence : il l'active pour 4 heures quand il en a besoin, avec justification obligatoire et, pour les rôles critiques, approbation par un pair. PIM réduit drastiquement la fenêtre d'exposition en cas de compromission de compte.

La configuration recommandée : activation maximale de 8 heures pour les rôles standards, 4 heures pour Global Admin et Security Admin. Approbation requise pour les 5 rôles les plus sensibles. Notification par email à chaque activation. Revue d'accès trimestrielle automatisée via les *Access Reviews* d'Entra ID Governance. Les risques liés à Entra Connect renforcent encore la nécessité de contrôler finement les rôles hybrides.

Contrôle du consentement applicatif

Par défaut, les utilisateurs Entra ID peuvent consentir à des applications tierces qui demandent des permissions sur leurs données. C'est un vecteur d'attaque redoutable : un attaquant crée une application malveillante avec un nom légitime, obtient le consentement d'un utilisateur et accède à ses emails, ses fichiers OneDrive, voire son calendrier. L'attaque par **illicit consent grant** est simple, efficace et souvent indétectable.

La configuration recommandée : désactivez le consentement utilisateur (User consent settings > Do not allow user consent). Mettez en place un workflow d'approbation admin (Admin consent workflow) pour que les demandes légitimes soient évaluées par l'équipe sécurité. Auditez les consentements existants avec le script PowerShell `Get-AzureADServicePrincipal` et révoquez les permissions excessives. Microsoft documente en détail cette procédure.

Identity Protection et détection automatisée

Entra ID Identity Protection utilise les signaux de Microsoft (analyse de milliards d'authentifications quotidiennes) pour détecter les comportements suspects : connexion depuis un IP anonyme, impossible travel, token anomaly, password spray détecté. Chaque risque est classé en faible, moyen ou élevé. La puissance de l'outil réside dans sa capacité à déclencher des actions automatiques : forcer le changement de mot de passe, bloquer la connexion ou exiger un MFA renforcé.

Configurez trois politiques Identity Protection : user risk policy (risque élevé → changement de mot de passe obligatoire), sign-in risk policy (risque élevé → blocage, risque moyen → MFA), et une intégration vers votre SOC via les alertes Microsoft Sentinel ou un SIEM tiers. Les signaux Identity Protection alimentent aussi les règles de détection d'attaques sur Azure AD, créant une boucle de défense continue.

Sécurisation des applications enregistrées

Les *App Registrations* dans Entra ID sont un angle mort fréquent. Chaque application enregistrée possède un Service Principal avec des permissions potentiellement élevées (Mail.Read, Directory.ReadWrite.All). Les secrets et certificats associés à ces applications expirent — ou n'expirent pas, ce qui est pire. Un secret d'application avec des permissions Directory.ReadWrite.All qui n'expire jamais, c'est une porte dérobée permanente dans votre tenant.

Actions prioritaires : inventoriez toutes les App Registrations avec `Get-MgApplication`, identifiez celles avec des permissions élevées, vérifiez les dates d'expiration des secrets et certificats, supprimez les applications orphelines. Mettez en place une politique de rotation des secrets tous les 90 jours et privilégiez les **managed identities** quand l'architecture le permet. Le monitoring des ajouts de credentials sur les Service Principals est un indicateur avancé de compromission que votre SIEM doit surveiller.

Configuration	Défaut	Recommandation	Priorité
Global Admins	Illimité	2 break-glass + PIM	Critique
Consentement utilisateur	Autorisé	Bloqué + workflow admin	Critique
Legacy auth	Autorisé	Bloqué par CA policy	Critique
MFA	Security defaults	CA policy + FIDO2/Passkeys	Élevée
PIM activation	Non configuré	4-8h, approbation, justification	Élevée
App Registration secrets	Pas de rotation	Rotation 90j, managed identity	Moyenne

Audit et monitoring continu

La sécurisation d'Entra ID n'est pas un exercice ponctuel. Les journaux d'audit et de connexion doivent être exportés vers un SIEM avec une rétention de 365 jours minimum (la rétention native Entra ID est de 30 jours en P1, 30 jours en P2). Les événements critiques à monitorer : ajout d'un Global Admin, modification d'une politique d'accès conditionnel, création d'un secret sur une App Registration, consentement admin accordé, et désactivation du MFA sur un compte.

Créez des alertes temps réel pour ces événements et intégrez-les dans votre processus de réponse à incident. Le guide de journalisation de l'ANSSI fournit un cadre de référence applicable à Entra ID. Un playbook de réponse à incident spécifique aux compromissions Entra ID doit être préparé et testé régulièrement.

Questions fréquentes sur la sécurité Entra ID

Quelle licence Entra ID faut-il pour sécuriser correctement un tenant ?

Les fonctionnalités de sécurité avancées requièrent Entra ID P2 (inclus dans Microsoft 365 E5). Cela couvre PIM, Identity Protection, Access Reviews et Conditional Access avancé. Entra ID P1 (inclus dans M365 E3) offre l'accès conditionnel de base et le MFA. Pour un tenant de production, P2 est le minimum recommandé pour les comptes administrateurs, P1 pour les utilisateurs standards.

Comment détecter les comptes compromis dans Entra ID ?

Trois sources de détection : Identity Protection (signaux automatiques Microsoft), les règles personnalisées dans votre SIEM (connexions impossibles, MFA bypass attempts) et les audits réguliers des permissions (rôles attribués, consentements applicatifs, App Registration secrets). La combinaison de ces trois approches couvre l'essentiel des scénarios de compromission. Un outil comme Microsoft Sentinel avec les connecteurs Entra ID natifs simplifie cette surveillance.

Peut-on sécuriser Entra ID sans licence P2 ?

Oui, mais avec des limitations significatives. Sans P2, vous n'avez pas accès à PIM ni à Identity Protection. Vous pouvez néanmoins déployer l'accès conditionnel de base (P1), bloquer les legacy protocols, restreindre le consentement applicatif et configurer des alertes manuelles via les journaux d'audit. Ces mesures couvrent environ 60% des vecteurs d'attaque. Pour les comptes sensibles, l'investissement P2 est fortement recommandé au regard du risque.

Sources et références : ANSSI · MITRE ATT&CK

Synthèse et plan d'action

La sécurisation d'Entra ID est un chantier continu qui nécessite une approche méthodique. Commencez par les quick wins à fort impact : réduction des Global Admins, activation du MFA universel, blocage des legacy protocols. Enchaînez avec PIM et le contrôle du consentement applicatif. Terminez par le monitoring avancé et l'intégration SIEM. Chaque étape renforce la posture de sécurité de votre tenant et vous rapproche d'une architecture Zero Trust mature. Testez votre configuration avec l'outil Microsoft Secure Score et visez un score supérieur à 80%.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr