AYI NEDJIMI Consultants

Microsoft Intune : Politiques de Conformité et : Guide

Catégorie : Microsoft 365 Lecture : 4 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide complet Microsoft Intune : politiques de conformité, configuration profiles, App Protection, Autopilot, Conditional Access et stratégie Zero.

```
{
  "displayName": "ZT-Compliance-Android-Enterprise",
  "platform": "androidForWork",
  "settings": {
    "devicePropertySettings": {
      "osMinimumVersion": "13.0",
      "securityPatchMinimumLevel": "2026-01-01"
    },
    "systemSecuritySettings": {
      "passwordRequired": true,
      "passwordMinimumLength": 6,
      "passwordRequiredType": "atLeastAlphanumeric",
      "storageRequireEncryption": true,
      "requireDeviceLock": true
    },
    "deviceHealthSettings": {
      "rootedDevicesBlocked": true,
      "googlePlayServicesVerified": true,
      "safetyNetDeviceAttestation": "certifiedDevice",
      "requireCompanyPortalAppIntegrity": true
    }
  }
}
```

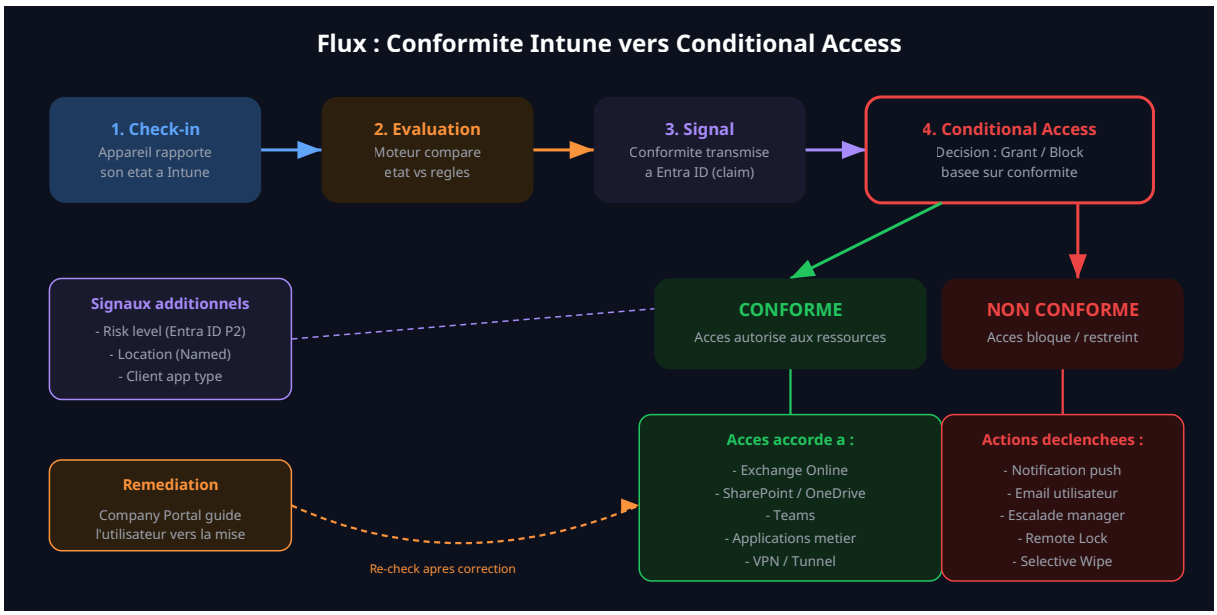
3.3 Grace period et actions de non-conformite

Intune permet de definir un **grace period** (delai de grace) qui donne a l'utilisateur le temps de corriger les problemes de conformite avant que des actions ne soient declenchees. Cette approche est essentielle pour equilibrer securite et experience utilisateur. Un appareil qui perd temporairement sa conformite (par exemple, apres une mise a jour systeme qui necessite un redemarrage) ne devrait pas immediatement bloquer l'acces aux ressources. Guide complet Microsoft Intune : politiques de conformité, configuration profiles, App Protection, Autopilot, Conditional Access et stratégie Zero. Ce guide couvre les aspects essentiels de intune politiques conformite zero trust : méthodologie structurée, outils recommandés et retours d'expérience opérationnels. Les professionnels y trouveront des recommandations directement applicables.

Les actions echelonnees recommandees pour un deploiement Zero Trust :

Delai	Action	Impact
Immediat (J+0)	Notification utilisateur + push email	Information seulement
J+1	Marquage "Non conforme" dans Entra ID	Blocage Conditional Access
J+3	Notification d'escalade (manager + helpdesk)	Visibilite management
J+7	Verrouillage distant de l'appareil	Blocage total
J+30	Retrait (retire) de l'appareil	Suppression profil corporate

```
# Script PowerShell - Configuration des actions de non-conformite via Graph API
$params = @{
    scheduledActionConfigurations = @(
        @{
            actionType = "notification"
            gracePeriodHours = 0
            notificationTemplateId = "default"
        },
        @{
            actionType = "markNonCompliant"
            gracePeriodHours = 24
        },
        @{
            actionType = "pushNotification"
            gracePeriodHours = 72
        },
        @{
            actionType = "remoteLock"
            gracePeriodHours = 168
        },
        @{
            actionType = "retire"
            gracePeriodHours = 720
        }
    )
}

# Application via Microsoft Graph PowerShell SDK
Import-Module Microsoft.Graph.DeviceManagement
Connect-MgGraph -Scopes "DeviceManagementConfiguration.ReadWrite.All"

$policyId = "votre-policy-id"
Update-MgDeviceManagementDeviceCompliancePolicyScheduledAction `
    -DeviceCompliancePolicyId $policyId `
    -BodyParameter $params
```



Cas concret

Les campagnes de phishing via Microsoft Teams se sont multipliées en 2024, avec des attaquants créant des tenants externes pour envoyer des messages directement aux employés ciblés. L'exploitation de la fédération Teams par défaut a permis de contourner les protections email traditionnelles.

Les regles ASR (Attack Surface Reduction) constituent une couche de defense proactive deployable via Intune. Elles bloquent les comportements malveillants courants utilises par les attaquants, notamment les techniques de Living-off-the-Land et les vecteurs d'initial access. Voici les regles ASR essentielles a activer :

```
# Configuration ASR via Intune - Profil Endpoint Security
# Les regles sont identifiees par leur GUID

$asrRules = @{
    # Bloquer le contenu executable des clients email
    "BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550" = "Block"

    # Bloquer les processus non approuves depuis USB
    "B2B3F03D-6A65-4F7B-A9C7-1C7EF74A9BA4" = "Block"

    # Bloquer les appels API Win32 depuis les macros Office
    "92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B" = "Block"

    # Bloquer la creation de processus enfants par les apps Office
    "D4F940AB-401B-4EFC-AADC-AD5F3C50688A" = "Block"

    # Bloquer les injections de code dans les processus
    "75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84" = "Block"

    # Bloquer le vol de credentials depuis LSASS
    "9E6C4E1F-7D60-472F-BA1A-A39EF669E4B2" = "Block"

    # Bloquer les processus PSExec et WMI
    "D1E49AAC-8F56-4280-B9BA-993A6D77406C" = "Audit"

    # Bloquer les scripts offusques
    "5BEB7EFE-FD9A-4556-801D-275E5FFC04CC" = "Block"

    # Bloquer l'abus de drivers signes vulnerables
    "56A863A9-875E-4185-98A7-B882C64B5CE5" = "Block"

    # Bloquer la persistence via WMI event subscription
    "E6DB77E5-3DF2-4CF1-B95A-636979351E5B" = "Block"
}

# Note: Commencer en mode "Audit" pendant 30 jours
# avant de passer en mode "Block" en production
```

Attention : mode Audit avant Block
Deployez TOUJOURS les regles ASR en mode **Audit** pendant un minimum de 30 jours avant de passer en mode Block. Certaines regles (notamment le blocage de PSExec/WMI - D1E49AAC) peuvent impacter les outils d'administration legitimement utilises par les equipes IT. Analysez les evenements Windows Event ID 1121 et 1122 pour identifier les faux positifs. Les techniques d'escalade de privileges Windows exploitent souvent des binaires legitimes que les regles ASR peuvent bloquer.

4.4 Custom OMA-URI et Settings Catalog

Pour les parametres non couverts par les templates natifs, Intune offre deux mecanismes : les profils **Custom OMA-URI** (pour Windows, utilisant le CSP - Configuration Service Provider) et le **Settings Catalog** (interface graphique unifiant plus de 5 000 parametres). Le Settings Catalog est la methode recommandee car il offre une interface plus accessible et un suivi de version des parametres.

```
<!-- Exemple OMA-URI : Desactiver le protocole LLMNR (anti-NTLM relay) -->
<!-- OMA-URI: ./Device/Vendor/MSFT/Policy/Config/ADMX_DnsClient/Turn_Off_Multicast -->
<!-- Type: String -->
<!-- Value: <enabled/> -->

<!-- Desactiver NetBIOS over TCP/IP -->
<!-- OMA-URI: ./Device/Vendor/MSFT/Policy/Config/MSSLegacy/IPSourceRoutingProtectionLevel
-->
<!-- Type: Integer -->
<!-- Value: 2 (Highest protection) -->

<!-- Forcer SMB signing -->
<!-- OMA-URI: ./Device/Vendor/MSFT/Policy/Config/MSSecurityGuide/
ConfigureSMBV1ClientDriver -->
<!-- Type: Integer -->
<!-- Value: 4 (Disable driver) -->
```

Pre-Provisioning (White Glove) : permet a l'equipe IT ou au partenaire de demarrer le processus de provisionnement avant la livraison a l'utilisateur. La phase technique (jointure Azure AD, installation apps, application baselines) est completee en avance, et l'utilisateur n'a plus qu'a se connecter pour finaliser la personnalisation.

```
# Enregistrement d'un appareil Autopilot et creation du profil

# 1. Recuperer le hardware hash de l'appareil
Install-Script -Name Get-WindowsAutopilotInfo
Get-WindowsAutopilotInfo -OutputFile C:\hwid.csv

# 2. Importer dans Intune via Graph API
Import-Module Microsoft.Graph.DeviceManagement.Enrollment
Connect-MgGraph -Scopes "DeviceManagementServiceConfig.ReadWrite.All"

$importData = @{
    serialNumber = "SN-12345-ABCDE"
    hardwareIdentifier = (Get-Content C:\hwid.csv |
        ConvertFrom-Csv).HardwareHash
    groupTag = "ZeroTrust-Corporate"
}

New-MgDeviceManagementImportedWindowsAutopilotDeviceIdentity `
    -BodyParameter $importData

# 3. Creer le profil Autopilot
$autopilotProfile = @{
    displayName = "ZT-Autopilot-UserDriven"
    description = "Profil Autopilot Zero Trust - Corporate"
    language = "fr-FR"
    extractHardwareHash = $true
    deviceNameTemplate = "ZT-%SERIAL%"
    outOfBoxExperienceSettings = @{
        hidePrivacySettings = $true
        hideEULA = $true
        userType = "standard"
        skipKeyboardSelectionPage = $true
        hideEscapeLink = $true
    }
    enrollmentStatusScreenSettings = @{
        hideInstallationProgress = $false
        allowDeviceUseBeforeProfileAndAppInstallComplete = $false
        blockDeviceSetupRetryByUser = $false
        allowLogCollectionOnInstallFailure = $true
        installProgressTimeoutInMinutes = 60
    }
}

New-MgDeviceManagementWindowsAutopilotDeploymentProfile `
    -BodyParameter $autopilotProfile
```

6.3 Enrollment Status Page (ESP)

L'**Enrollment Status Page** (page d'etat d'enrollment) est un composant critique du deploiement Zero Trust via Autopilot. Elle bloque l'acces au bureau Windows tant que les politiques de securite essentielles ne sont pas appliquees. Sans ESP, un utilisateur pourrait commencer a travailler sur un appareil qui n'a pas encore recu ses baselines de securite, son antivirus ou son chiffrement BitLocker - une violation directe du principe Zero Trust.

Configuration recommandee de l'ESP pour un deploiement Zero Trust : bloquer l'utilisation de l'appareil jusqu'a ce que tous les profils et applications critiques soient installes, definir un timeout de 60 minutes (permettant le deploiement complet y compris les mises a jour Windows),

autoriser la collecte de logs en cas d'echec pour le diagnostic, et configurer les applications critiques qui doivent etre installees avant l'acces (Company Portal, Defender for Endpoint, VPN client, navigateur Edge).

Bonne pratique : Autopilot + Conditional Access
Combinez Autopilot avec une politique Conditional Access qui exige la conformite de l'appareil pour acceder aux ressources M365. Creez un groupe dynamique Azure AD qui inclut automatiquement les appareils avec le tag Autopilot `ZeroTrust-Corporate`. Ce groupe sera la cible des politiques de conformite les plus strictes. Ainsi, des le premier login, l'appareil doit satisfaire les exigences de conformite avant que l'utilisateur puisse acceder a Exchange, Teams ou SharePoint.

Pour une visibilite complete dans un SOC, les logs Intune doivent etre integres dans **Microsoft Sentinel** via le connecteur natif. Les tables suivantes sont particulierement pertinentes pour le monitoring Zero Trust : `IntuneDeviceComplianceOrg` (etat de conformite), `IntuneOperationalLogs` (operations administratives), `IntuneDevices` (inventaire appareils), et `SigninLogs` (contexte Conditional Access).

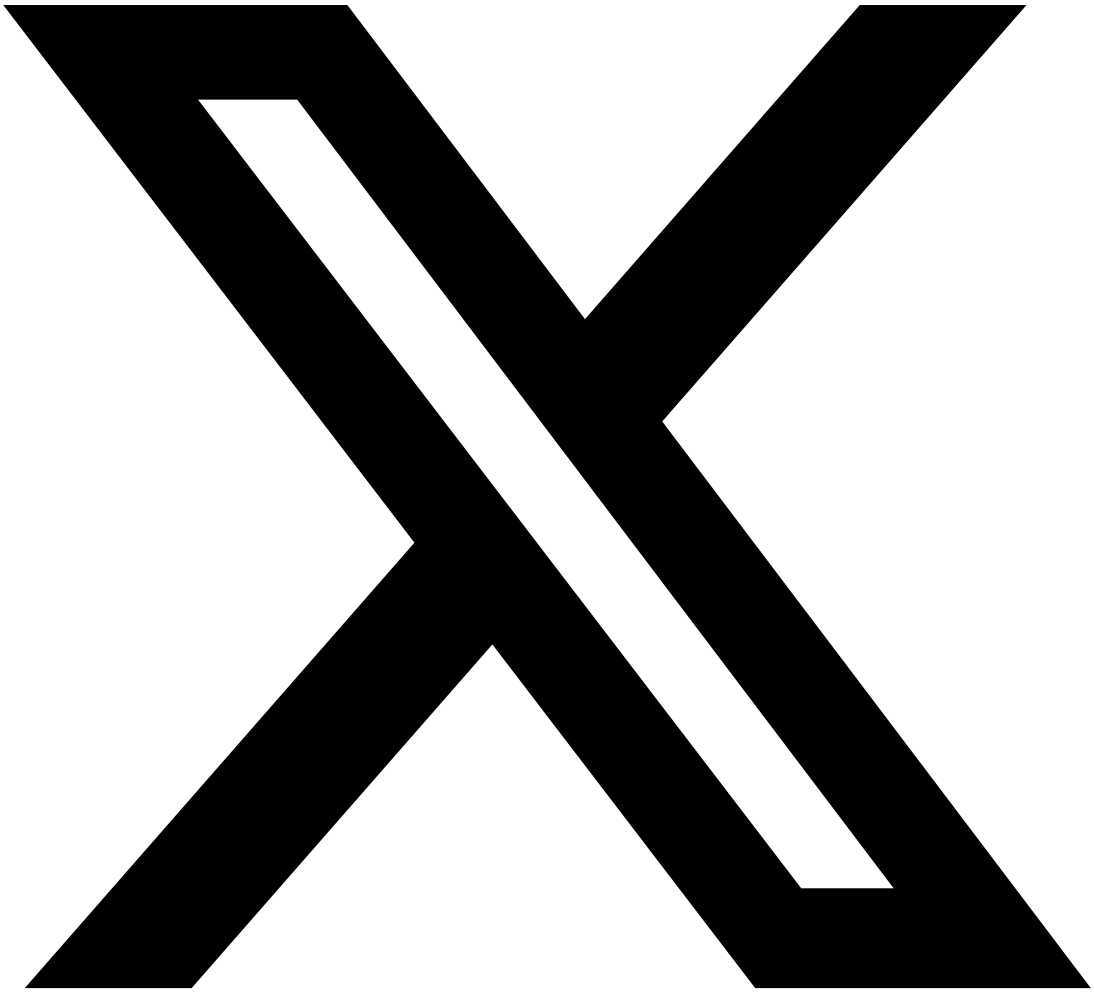
```
// KQL - Detection d'appareils qui deviennent non conformes
// Utile pour detecter des tentatives d'evasion de la conformite

IntuneDeviceComplianceOrg
| where TimeGenerated > ago(24h)
| where ComplianceState == "noncompliant"
| summarize
    NonCompliantCount = count(),
    Platforms = make_set(OS),
    FirstSeen = min(TimeGenerated)
    by DeviceName, UserName
| where NonCompliantCount > 1
| sort by NonCompliantCount desc

// Detection de patterns suspects - appareil qui alterne
// entre conforme et non conforme (possible evasion)
IntuneDeviceComplianceOrg
| where TimeGenerated > ago(7d)
| summarize
    StateChanges = dcount(ComplianceState),
    States = make_set(ComplianceState)
    by DeviceName, UserName
| where StateChanges > 3
| sort by StateChanges desc
```

9.3 KPIs et metriques Zero Trust

Pour mesurer l'efficacite de votre deploiement Zero Trust via Intune, suivez ces indicateurs cles de performance (KPIs) :

KPI	Cible	Frequence	Source
Taux de conformite global	> 95%	Quotidien	Intune Dashboard
Chiffrement BitLocker/FileVault	100%	Hebdomadaire	Encryption Report
Appareils avec OS a jour	> 90%	Mensuel	Software Updates
Defender for Endpoint actif	100%	Quotidien	MDE Dashboard
Legacy auth bloquee	100%	Hebdomadaire	CA Report-Only
Baseline coverage	> 98%	Mensuel	Profile Assignment
Delai moyen de remediation	< 24h	Mensuel	Compliance Trends
Appareils avec admins locaux	0%	Mensuel	EPM Reports

Cet article vous a ete utile ? Partagez-le avec votre reseau professionnel !

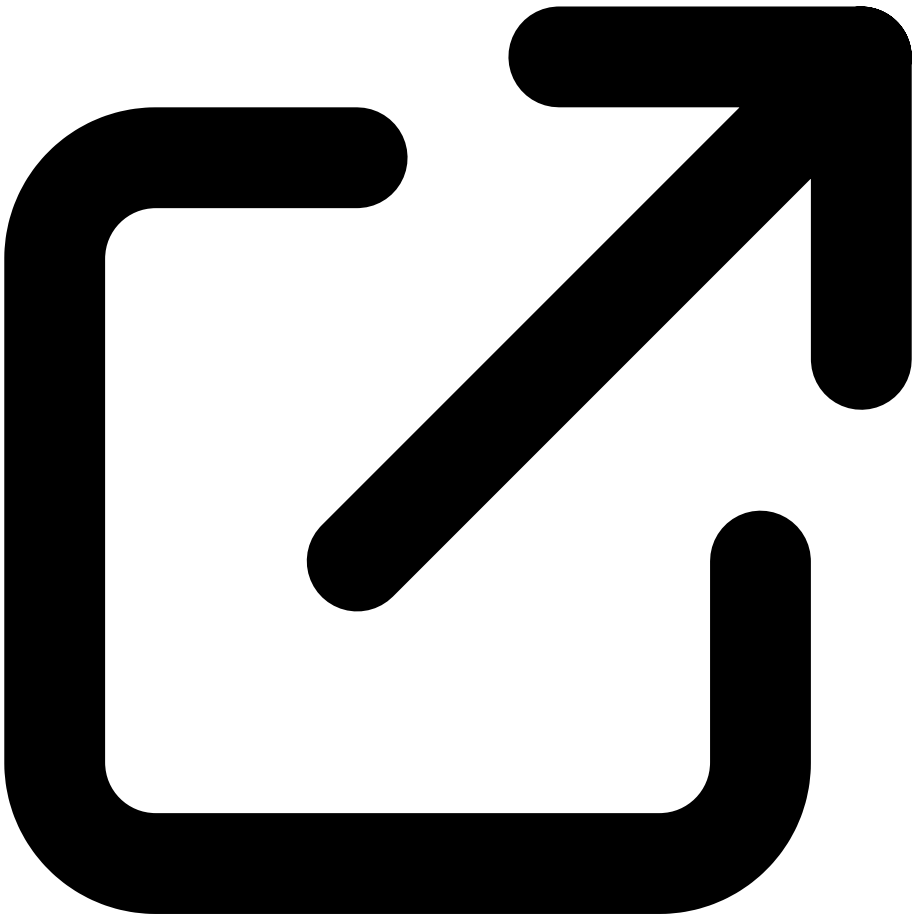


Partager sur X

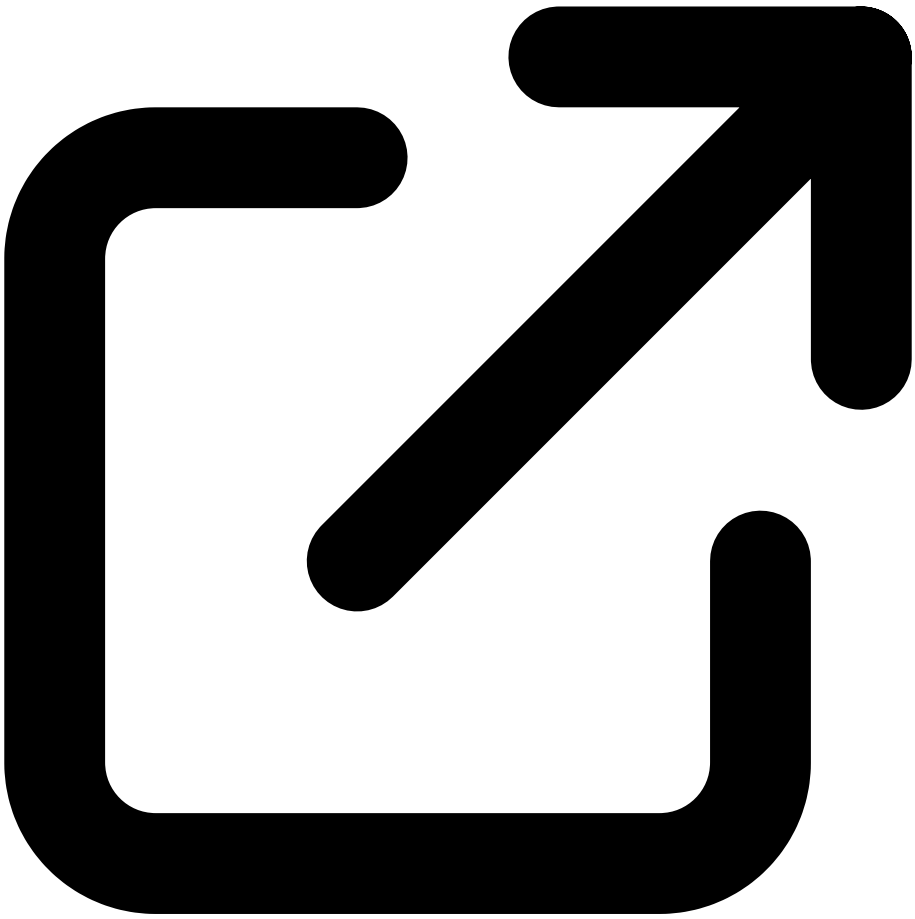
Partager sur LinkedIn

Ressources & References Officielles

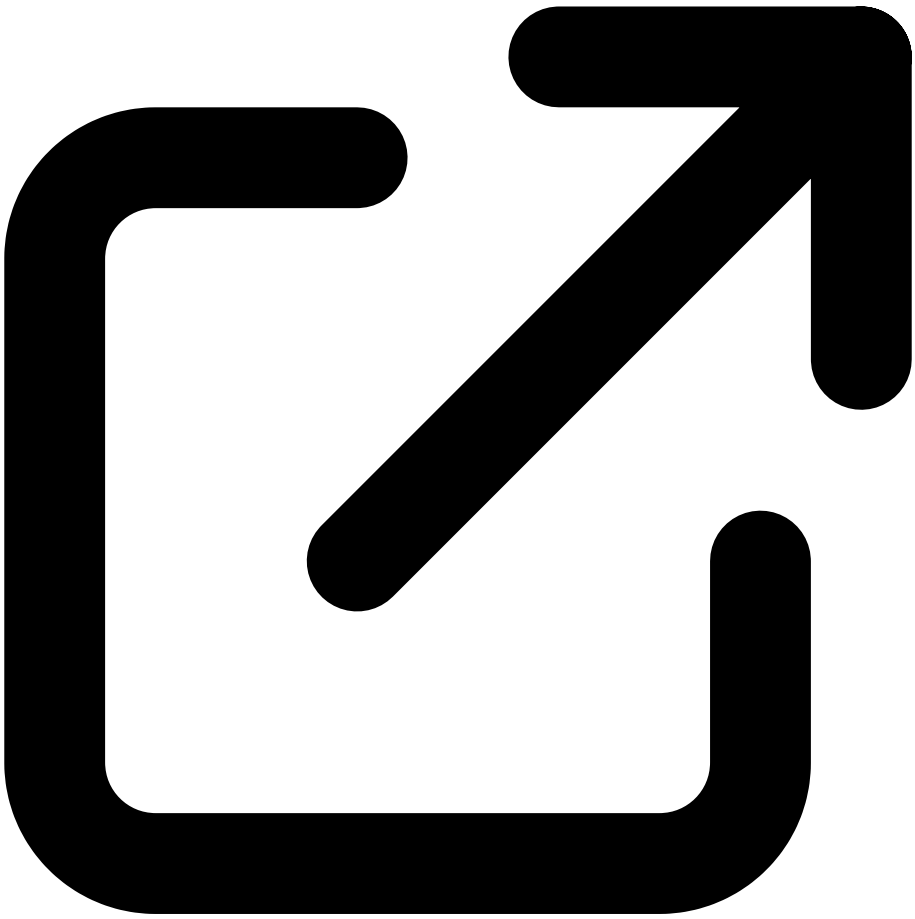
Documentations officielles Microsoft et ressources de reference



Microsoft Intune Documentation
learn.microsoft.com



Microsoft Zero Trust Framework
learn.microsoft.com



Conditional Access Documentation
learn.microsoft.com

Ayi NEDJIMI

Expert en Cybersecurite & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'experience en securite offensive, audit d'infrastructure et developpement de solutions IA. Certifie OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, securite Cloud et conformite reglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

References et ressources externes

- Microsoft - Device Compliance Policies -- Documentation officielle des politiques de conformite Intune
- Microsoft - Security Baselines -- Guide des baselines de securite deploiement via Intune
- Microsoft - Windows Autopilot -- Documentation complete du deploiement zero-touch
- CIS Benchmark - Microsoft Intune -- Benchmark de durcissement CIS pour Intune
- Microsoft - App Protection Policies -- Guide des politiques MAM pour la protection des applications

Sources et références : Microsoft Security Docs · CERT-FR

Articles connexes

- Audit Avancé Microsoft 365 : Corréler Journaux et Logs Azure
- PIM Entra ID : Gestion des Accès Privilégiés Just-in-Time

FAQ

Qu'est-ce que Microsoft Intune ?

Microsoft Intune désigne l'ensemble des concepts, techniques et méthodologies abordés dans cet article. Les fondamentaux sont détaillés dans les premières sections du guide.

Pourquoi intune politiques conformite zero trust est-il important ?

La maîtrise de intune politiques conformite zero trust est devenue essentielle pour les équipes de sécurité. Les enjeux et le contexte opérationnel sont développés tout au long de l'article.

Comment appliquer ces recommandations en entreprise ?

Chaque section de cet article propose des méthodologies et des outils directement utilisables. Les recommandations tiennent compte des contraintes d'environnements de production réels.

> Points clés à retenir
>
> • Microsoft Intune : Politiques de Conformité et : Guide

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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