Golden SAML et Attaques ADFS 2026 : Exploitation et Remédiation

Attaques Golden SAML contre ADFS en 2026 : extraction clé Token Signing, forgerie d assertions, Shimmers, détection et remédiation vers Microsoft Entra ID.

Les attaques Golden SAML contre Active Directory Federation Services représentent en 2026 l'une des techniques les plus sophistiquées et les plus dévastatrices disponibles dans l'arsenal des groupes APT ciblant les environnements hybrides Microsoft. Contrairement au célèbre Golden Ticket Kerberos qui nécessite d'abord de compromettre un contrôleur de domaine pour obtenir le hash KRBTGT, le Golden SAML permet à un attaquant de forger des assertions SAML valides et de s'authentifier comme n'importe quel utilisateur — y compris les administrateurs globaux — auprès de n'importe quelle application fédérée avec ADFS, sans jamais toucher le contrôleur de domaine. Cette technique, popularisée par Shaked Reiner de CyberArk en 2017 et exploitée massivement lors de la compromission SolarWinds en 2020, reste extrêmement pertinente en 2026 car des milliers d'organisations françaises maintiennent encore ADFS on-premises pour la fédération d'identité avec Office 365, Salesforce, AWS et des centaines d'autres applications SaaS. Notre équipe a rencontré cette configuration lors d'une mission de red team pour un cabinet d'avocats parisien comptant 800 collaborateurs : le serveur ADFS, installé cinq ans auparavant et jamais mis à jour, exposait un vecteur de compromission permettant de prendre le contrôle de l'ensemble des accès Microsoft 365 de l'organisation sans déclencher la moindre alerte dans le SIEM — lequel n'ingérait d'ailleurs aucun log ADFS. La leçon est claire : ADFS est un composant critique qui mérite autant d'attention sécurité que les contrôleurs de domaine eux-mêmes, et dont la migration vers Entra ID est la recommandation principale de Microsoft pour 2026.

En France, le déploiement d'ADFS reste significatif malgré la poussée vers le cloud. Selon les estimations de plusieurs intégrateurs et cabinets de conseil en sécurité opérant en France, entre 30 et 40 % des organisations françaises de plus de 500 salariés maintiennent encore un ADFS on-premises en 2026, souvent en parallèle avec Entra ID dans une configuration hybride. Cette proportion est plus élevée dans les secteurs régulés (finances, santé, défense) où la souveraineté des données et les contraintes de certification (SecNumCloud, HDS) ralentissent la migration vers le cloud Microsoft. De nombreuses administrations publiques, établissements de santé (sous la supervision de l'ANS et de l'ANSSI), grandes entreprises du CAC40 et ETI du secteur industriel maintiennent des infrastructures ADFS on-premises pour des raisons de souveraineté des données, de contraintes réglementaires (SecNumCloud, HDS) ou simplement d'inertie informatique. La directive NIS 2, transposée en droit français en 2024, impose à ces entités une gestion rigoureuse de leurs systèmes d'authentification fédérée, ce qui inclut explicitement la sécurisation d'ADFS et la collecte de ses logs dans un SIEM. L'ANSSI a publié en 2025 une note technique spécifique sur les risques liés aux tokens SAML forgés, qui constitue le référentiel de conformité pour les entités soumises à la réglementation française en matière de cybersécurité.

Rappel : Qu'est-ce que SAML et ADFS ?

SAML (Security Assertion Markup Language) est un standard XML pour l'échange d'informations d'authentification et d'autorisation entre un fournisseur d'identité (IdP) et un fournisseur de service (SP). ADFS (Active Directory Federation Services) est l'implémentation Microsoft de l'IdP SAML, permettant aux utilisateurs Active Directory de s'authentifier auprès d'applications externes via des tokens SAML signés numériquement.

> ⚡ **Retour terrain**
>
> Dans mes missions de hardening Active Directory, le point le plus sous-estimé est la gestion du groupe 'Opérateurs de compte' et des délégations personnalisées créées au fil des années. Pour un groupe logistique de 1 500 utilisateurs, j'ai trouvé 312 ACL personnalisées dont 89 accordaient des permissions d'écriture sur des attributs sensibles (adminCount, memberOf sur groupes privilégiés) à des comptes d'utilisateurs standards. La dette technique en sécurité AD est souvent invisible jusqu'au premier audit sérieux.

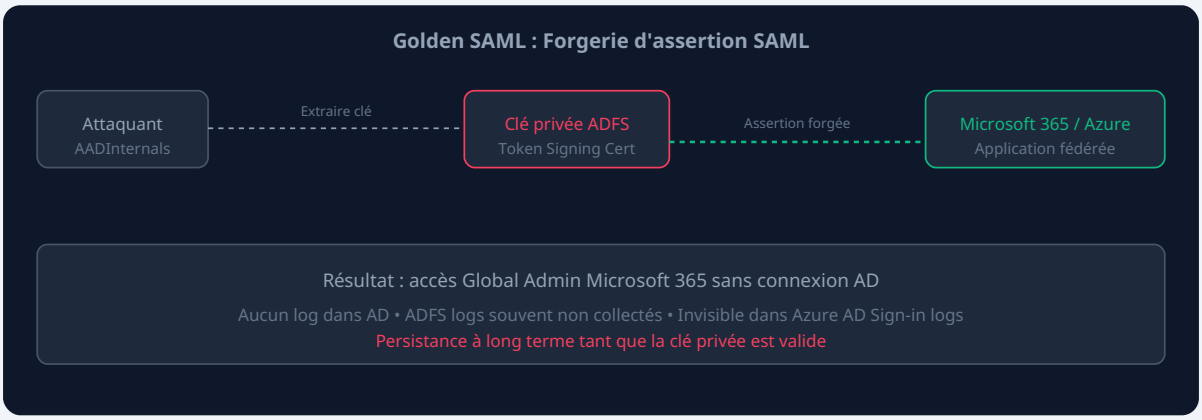
Le mécanisme fondamental d'ADFS repose sur un certificat de signature de tokens (Token Signing Certificate). Lorsqu'un utilisateur s'authentifie via ADFS, le serveur génère une assertion SAML XML et la signe avec ce certificat. L'application cible vérifie la signature en utilisant la clé publique du certificat. Si la signature est valide, l'utilisateur est authentifié avec les attributs présents dans l'assertion (identité, rôles, groupes).

Golden SAML : Principes et Différence avec le Golden Ticket

L'attaque **Golden SAML** consiste à extraire la clé privée du certificat de signature de tokens d'ADFS, puis à forger des assertions SAML arbitraires signées avec cette clé. L'attaquant peut ainsi se faire passer pour n'importe quel utilisateur auprès de n'importe quelle application fédérée, avec n'importe quel attribut (y compris Administrator, Global Admin, etc.).

Critère	Golden Ticket Kerberos	Golden SAML
Prérequis	Hash KRBTGT (nécessite DA)	Clé privée ADFS Token Signing Cert
Portée	Ressources du domaine AD	Toutes applications fédérées SAML/ADFS
Durée de vie	10 ans par défaut	Tant que la clé privée est valide
Réinitialisation	Rotation KRBTGT 2 fois	Renouvellement certificat ADFS
Détection	Événement 4769 (ticket Kerberos)	Logs ADFS (souvent non collectés)
Impact cloud	Limité à l'AD on-prem	Microsoft 365, Azure, apps SaaS

Flux d'authentification ADFS normal vs Golden SAML



Extraction de la Clé Privée ADFS : Techniques et Outils

L'extraction de la clé privée du certificat de signature ADFS est l'étape centrale du Golden SAML. Elle nécessite un accès administrateur local sur le serveur ADFS, qui est souvent moins bien protégé que les DC car considéré comme un serveur applicatif. Les techniques d'extraction incluent :

```
 # Methode 1 : ADFSDump (Mandiant/FireEye) - extraction depuis le serveur ADFS
ADFSDump.exe /domain:domaine.local /output:adfs_dump.json

# Methode 2 : AADInternals (Dr. Nestori Syynimaa)
# Exporte le certificat de signing depuis la base de donnees ADFS
Import-Module AADInternals
Export-AADIntADFSSigningCertificate -pfx_password "motdepasse" -filename "adfs_signing.pfx"

# Methode 3 : Acces direct a la base DKM (Distributed Key Manager)
# La cle privee est stockee dans AD sous : CN=ADFS,CN=Microsoft,CN=Program Data,DC=...
# Accessible via LDAP avec droits suffisants
Get-ADObject -SearchBase "CN=ADFS,CN=Microsoft,CN=Program Data,DC=domaine,DC=local" -Filter

# Methode 4 : Extraction via DPAPI si cle exportable
mimikatz "crypto::certificates /systemstore:LOCAL_MACHINE /store:My /export"
```

Forger une Assertion Golden SAML avec AADInternals

Une fois la clé privée extraite, l'attaquant peut forger des assertions SAML pour n'importe quel utilisateur. L'outil **AADInternals**, développé par le chercheur finlandais Nestori Syynimaa (Dr. Azuresecurity), est le plus utilisé pour cette étape.

```
 # Charger le certificat ADFS extrait
$cert = Get-PfxCertificate -FilePath "adfs_signing.pfx" -Password (ConvertTo-SecureString "

# Forger une assertion SAML pour l'administrateur global
$saml = New-AADIntSAMLToken `
    -ImmutableID "Base64_ImmutableID_Admin" `
    -Issuer "http://adfs.domaine.local/adfs/services/trust" `
    -PfxFileName "adfs_signing.pfx" `
    -PfxPassword "motdepasse"

# Utiliser le token pour obtenir un access token Microsoft 365
Get-AADIntAccessTokenForEXO -SAMLToken $saml

# Acceder aux emails de l'administrateur
Read-AADIntUserMail -AccessToken $at
```

Conditions Préalables à une Attaque Golden SAML : La Chaîne de Compromission

Pour réussir un Golden SAML, l'attaquant doit franchir plusieurs étapes préalables qui constituent la chaîne de compromission menant à l'extraction du certificat. La première est d'obtenir un accès administrateur local sur le serveur ADFS, ce qui nécessite généralement une compromission initiale du réseau interne via phishing, exploitation de vulnérabilité ou NTLM Relay. La deuxième est d'identifier et d'accéder au stockage de la clé privée ADFS.

Il existe deux modes de stockage de la clé privée ADFS :

Certificat auto-signé généré par ADFS : stocké dans le magasin de certificats Windows LOCAL_MACHINE, protégé par DPAPI. Extractible via Mimikatz ou ADFSDump avec des droits SYSTEM sur le serveur ADFS.

Certificat PKI fourni par l'entreprise : stocké dans le magasin de certificats Windows mais potentiellement avec marquage non exportable. Dans ce cas, l'attaquant peut utiliser des outils comme Mimikatz pour extraire la clé même si le certificat est marqué non exportable via CryptoAPI.

La troisième étape est optionnelle mais recommandée par les attaquants sophistiqués : identifier le mécanisme DKM (Distributed Key Manager) d'ADFS. ADFS stocke en fait le certificat de signing dans Active Directory sous un chemin LDAP spécifique, protégé par une clé symétrique stockée dans le Local Security Authority (LSA). Cette clé est accessible depuis le serveur ADFS avec des droits élevés et permet de décrypter le certificat stocké dans AD sans même accéder au magasin de certificats Windows. Cette méthode via DKM est particulièrement furtive car elle ne génère pas d'événements dans le magasin de certificats Windows et peut passer inaperçue même avec un EDR déployé sur le serveur ADFS, si les règles de détection n'incluent pas les accès LDAP aux chemins AD spécifiques au DKM.

Une donnée important pour les défenseurs : le serveur ADFS n'a besoin d'accéder au chemin DKM dans AD que lors du démarrage du service ADFS et lors de la rotation de certificats. Un accès LDAP au chemin DKM en dehors de ces moments est donc un indicateur d'investigation à fort potentiel, facilement détectable via la surveillance des événements d'accès aux objets AD (5140) si l'audit est correctement configuré.

Cas SolarWinds : Golden SAML en Action Réelle

L'attaque SolarWinds de 2020, attribuée au groupe APT29 (Cozy Bear, lié aux services de renseignement russes), a mis en lumière le potentiel dévastateur du Golden SAML à grande échelle. Les attaquants ont compromis des serveurs ADFS dans des dizaines d'organisations gouvernementales et d'entreprises américaines, en ont extrait les certificats de signing, et ont forgé des tokens SAML pour accéder à Microsoft 365 pendant des mois sans être détectés.

La durée de la campagne — estimée à plus de neuf mois avant détection — illustre l'un des problèmes majeurs du Golden SAML : les assertions forgées sont cryptographiquement valides et indiscernables d'assertions légitimes du point de vue du fournisseur de service. Microsoft 365, par exemple, ne peut pas distinguer un token SAML légitime émis par ADFS d'un token forgé avec la même clé privée.

Analyse Forensique d'un Token Golden SAML

Un token SAML forgé par Golden SAML est cryptographiquement valide — c'est précisément ce qui le rend si dangereux. Cependant, une analyse forensique minutieuse peut révéler des anomalies structurelles :

NameID ou ImmutableID : l'attaquant doit connaître l'ImmutableID de l'utilisateur qu'il usurpe. Des outils comme AADInternals permettent d'énumérer ces identifiants si l'attaquant dispose d'un accès au tenant Entra ID, mais une valeur ImmutableID incorrecte ou mal formatée peut trahir un token forgé.

Attributs non standards : les tokens forgés incluent souvent uniquement les attributs minimaux nécessaires (identité, rôles), omettant des attributs que le vrai ADFS inclurait normalement (SessionIndex, AuthnContext, etc.).

Timestamp : les tokens SAML ont une durée de validité encodée (NotBefore, NotOnOrAfter). Des tokens avec des durées de validité inhabituellement longues ou des timestamps dans le passé peuvent indiquer un forging.

```
 # Decoder et analyser un token SAML base64 (PowerShell)
$token_b64 = "..." # token SAML encode en base64
$token_xml = [System.Text.Encoding]::UTF8.GetString([Convert]::FromBase64String($token_b64))
$xml = [xml]$token_xml

# Extraire les informations cles
$xml.Response.Assertion.Subject.NameID.'#text'           # Identite usurpee
$xml.Response.Assertion.Conditions.NotBefore             # Debut validite
$xml.Response.Assertion.Conditions.NotOnOrAfter          # Fin validite
$xml.Response.Assertion.AuthnStatement.AuthnContext.AuthnContextClassRef  # Methode auth
```

Détection des Attaques Golden SAML via les Logs ADFS

La détection du Golden SAML repose principalement sur les logs ADFS, qui sont malheureusement rarement collectés dans les SIEM des organisations. Les logs ADFS se trouvent dans l'Observateur d'événements Windows sous :

Applications and Services Logs > AD FS > Admin : événements d'administration ADFS

Applications and Services Logs > AD FS Auditing : logs d'audit des tokens émis (événements 299, 324, 500)

```
 # Activer les logs d'audit ADFS
Set-AdfsProperties -AuditLevel Verbose
auditpol /set /subcategory:"Application Generated" /success:enable /failure:enable

# Evenements ADFS cles a surveiller
# 299 : Token emis (succes d'authentification)
# 324 : Token emis via assertion externe (SAML)
# 500 : Erreur de token
# 1202 : Claim emis (attributs inclus dans le token)

# PowerShell : rechercher les tokens emis pour des comptes sensibles
Get-WinEvent -LogName "AD FS/Admin" | Where-Object {$_.Message -like "*admin*"}

# Indicateurs de Golden SAML dans les logs :
# - Token emis depuis une IP inconnue (pas le serveur ADFS habituel)
# - Assertion SAML referencant un ImmutableID existant mais depuis une source inhabituelle
# - Connexion Microsoft 365 sans evenement 4624 correspondant dans AD
```

Détection dans Microsoft Entra ID (Azure AD) Sign-In Logs

Les logs de connexion Entra ID offrent des indicateurs supplémentaires pour détecter les Golden SAML en environnement hybride :

Connexion réussie avec l'authentification method "federated" depuis une IP inhabituelle

Absence d'événement MFA correspondant alors que la Conditional Access l'exige

Heure de connexion incohérente avec les habitudes de l'utilisateur

Agent utilisateur inhabituel (script, outil de test)

```
 # KQL pour Microsoft Sentinel : détecter les connexions SAML suspectes
SigninLogs
| where AuthenticationProtocol == "saml20"
| where ResultType == 0  // Succes
| where IPAddress !in (known_adfs_ips)
| project TimeGenerated, UserDisplayName, IPAddress, UserAgent, Location
| where not(Location has_any ("France", "Europe"))
| sort by TimeGenerated desc
```

Shimmers ADFS : Backdoor Persistante dans le Processus ADFS

Au-delà du Golden SAML, les attaquants sophistiqués utilisent des **Shimmers ADFS** (aussi appelés DLL hijacking dans ADFS) pour implanter une backdoor persistante dans le processus ADFS. Un Shimmer ADFS est une DLL malveillante qui s'injecte dans le processus Microsoft.IdentityServer.ServiceHost.exe et intercepte toutes les authentifications, permettant à l'attaquant de capturer les credentials ou de modifier les assertions SAML à la volée.

```
 # Detecter les DLL suspectes dans le repertoire ADFS
Get-ChildItem "C:\Windows\ADFS\" -Recurse | Where-Object {$_.LastWriteTime -gt (Get-Date).A

# Verifier l'integrite des DLL ADFS avec Get-FileHash
Get-ChildItem "C:\Windows\ADFS\*.dll" | ForEach-Object {
    [PSCustomObject]@{
        File = $_.Name
        Hash = (Get-FileHash $_.FullName -Algorithm SHA256).Hash
        Modified = $_.LastWriteTime
    }
}

# Surveiller les processus chargeant des DLL depuis des chemins inhabituels
Get-Process -Name "Microsoft.IdentityServer.ServiceHost" | Select-Object -ExpandProperty Mo
```

Playbook de Réponse à Incident Golden SAML : Les 72 Premières Heures

Lorsqu'un incident Golden SAML est confirmé ou fortement suspecté, les 72 premières heures sont critiques pour contenir la compromission et limiter l'impact. Voici le playbook que nous recommandons, structuré par priorité temporelle :

Heure 0-2 : Confinement immédiat — Renouveler le certificat ADFS de signing en mode urgent, révoquer toutes les sessions Microsoft 365 et Entra ID, couper l'accès réseau du serveur ADFS compromis le temps de l'investigation forensique (maintenir un accès hors bande), et notifier le RSSI, DPO et direction juridique pour déclencher les processus de notification réglementaire.

Heure 2-24 : Investigation forensique — Analyser les logs ADFS des 12 derniers mois (événements 299, 324), identifier tous les comptes qui auraient pu être impersonnés via des tokens forgés, rechercher des backdoors dans Entra ID (nouvelles applications OAuth, nouveaux service principals, Federation Trust modifiée), et analyser l'intégrité des DLL du serveur ADFS (Shimmers).

Heure 24-72 : Remédiation approfondie — Reconstruire le serveur ADFS sur une base saine si des Shimmers sont détectés, réinitialiser les mots de passe de tous les comptes administrateurs potentiellement impersonnés, supprimer toutes les applications OAuth et service principals créés pendant la période de compromission, et activer des Conditional Access Policies renforcées en attendant la migration vers Entra ID.

Remédiation Immédiate après Compromission ADFS

Si une compromission Golden SAML est suspectée ou confirmée, voici les actions de remédiation à effectuer dans les plus brefs délais :

Renouveler immédiatement le certificat de signing ADFS : cette action invalide tous les tokens forgés avec l'ancienne clé

Révoquer toutes les sessions actives dans Entra ID : forcer la ré-authentification de tous les utilisateurs

Analyser les logs ADFS sur 12 mois minimum pour identifier l'étendue de la compromission

Réinitialiser les mots de passe de tous les comptes administrateurs qui auraient pu être impersonnés

Auditer les configurations de Conditional Access Entra ID pour détecter des modifications malveillantes

```
 # Renouveler le certificat de signing ADFS
Update-AdfsCertificate -CertificateType Token-Signing -Urgent

# Revoquer toutes les sessions Entra ID (PowerShell Entra)
Connect-MgGraph -Scopes "User.ReadWrite.All"
Get-MgUser -Filter "userType eq 'Member'" | ForEach-Object {
    Revoke-MgUserSignInSession -UserId $_.Id
}

# Verifier les certificats ADFS actuels
Get-AdfsCertificate -CertificateType Token-Signing | Select-Object Thumbprint, Certificate
```

Migration vers Entra ID : La Recommandation Microsoft pour 2026

La recommandation de Microsoft pour 2026 est claire et sans ambiguïté : migrer d'ADFS vers l'authentification managée Entra ID (anciennement Azure AD). Cette migration élimine définitivement le vecteur Golden SAML en supprimant la dépendance à un certificat de signing local et en confiant l'émission de tokens directement à Microsoft, qui dispose d'une infrastructure de sécurité de premier niveau incluant la détection comportementale, la géolocalisation et le machine learning pour détecter les anomalies d'authentification.

Les étapes de migration vers Entra ID incluent :

Inventaire exhaustif des applications fédérées avec ADFS et évaluation de la compatibilité Entra ID pour chacune

Migration des applications vers Entra ID Application Proxy ou enregistrement SAML/OIDC direct dans Entra ID

Configuration de PHS (Password Hash Sync) ou PTA (Pass-Through Authentication) comme méthode d'authentification principale

Activation des Conditional Access Policies dans Entra ID pour remplacer les règles de claim ADFS, en commençant par les applications les plus critiques

Phase de cohabitation ADFS/Entra ID (typiquement 3-6 mois) pendant laquelle les deux systèmes fonctionnent en parallèle

Décommissionnement d'ADFS après validation complète de toutes les applications migrées et confirmation que aucune n'utilise encore ADFS

Microsoft fournit un outil dédié à l'analyse de la migration ADFS vers Entra ID : le module PowerShell AzureADConnect, qui peut identifier automatiquement les obstacles à la migration pour chaque application fédérée. L'utilisation de cet outil en phase de planification permet d'éviter les mauvaises surprises lors de la migration effective.

Pour les aspects d'identité hybride et la sécurisation d'Entra ID, consultez notre article sur les attaques sur les fournisseurs d'identité Okta et Entra ID et notre analyse de la protection Entra ID pour les CSP Microsoft.

Impact Business d'une Compromission Golden SAML

Les conséquences d'une compromission Golden SAML réussie vont bien au-delà du simple accès technique initial : elles impactent l'ensemble de l'écosystème numérique de l'organisation. Si l'application cible est Microsoft 365, l'attaquant dispose d'un accès complet aux emails de l'exécutif, aux documents SharePoint les plus confidentiels, aux Teams contenant les discussions stratégiques, et — via des permissions administrateur Global Admin — à l'ensemble des services Azure et Microsoft 365 du tenant.

Dans des secteurs réglementés comme la finance (DORA), la santé (HDS) ou les infrastructures critiques (NIS 2), une telle compromission déclenche des obligations de notification réglementaire. En France, les entités soumises à NIS 2 doivent notifier l'ANSSI dans les 24

heures pour les incidents de sécurité majeurs, et dans les 72 heures pour les violations de données personnelles concernant la CNIL. La gestion de crise post-Golden SAML implique donc simultanément la réponse technique et la conformité réglementaire, ce qui nécessite une coordination entre le RSSI, le DPO, la direction juridique et la direction générale.

ADFS Proxy (WAP) : Vecteur d'Attaque Supplémentaire

Le **Web Application Proxy (WAP)**, utilisé comme proxy ADFS exposé sur Internet, représente un vecteur d'attaque additionnel. Les CVE affectant le WAP (comme CVE-2024-21320 et plusieurs autres publiés ces dernières années) peuvent permettre l'exécution de code ou le contournement d'authentification depuis Internet, sans nécessiter un accès réseau interne préalable. Le WAP est donc une cible prioritaire pour les attaquants cherchant à atteindre le serveur ADFS interne.

```
 # Tester l'exposition WAP via curl (verifier les endpoints exposes)
curl -v https://adfs.entreprise.fr/adfs/ls/idpinitiatedsignon.aspx
curl -v https://adfs.entreprise.fr/adfs/services/trust/mex

# Verifier la version ADFS exposee (peut trahir les patchs manquants)
# L'entete "x-ms-gateway-slice" revele la version du WAP
# Surveiller les tentatives d acces aux endpoints ADFS depuis Internet
# Evenement 411 ADFS (echec d'authentification) en masse = bruteforce ou spray
```

Hardening ADFS pour les Organisations Maintenant ADFS On-Premises

Pour les organisations qui ne peuvent pas migrer vers Entra ID immédiatement, voici les mesures de hardening ADFS prioritaires recommandées par l'ANSSI :

Isoler le serveur ADFS dans un VLAN dédié avec accès restreint (seulement depuis les DC et les proxies WAP)

Activer l'audit verbose ADFS et collecter les logs dans le SIEM (événements 299, 324, 500, 1202)

Configurer Smart Lockout ADFS pour bloquer les tentatives de bruteforce

Activer le monitoring de l'intégrité des DLL ADFS via Windows Defender Application Control (WDAC)

Restreindre l'accès admin au serveur ADFS aux seuls comptes Tier 0 via PAW

Mettre à jour ADFS régulièrement — de nombreuses CVE ADFS sont publiées annuellement

Mesure	Priorité	Effort	Impact sécurité
Collecte logs ADFS dans SIEM	Critique	Faible	Détection Golden SAML
Isolation réseau ADFS	Critique	Moyen	Réduction surface d'attaque
MFA sur accès admin ADFS	Critique	Faible	Blocage extraction clé
Migration vers Entra ID	Haute	Élevé	Élimination du vecteur
Monitoring intégrité DLL	Haute	Moyen	Détection Shimmers

Comparaison des Outils d'Exploitation Golden SAML

Plusieurs outils permettent l'exploitation Golden SAML. Leur connaissance est indispensable pour les équipes red team et les défenseurs qui souhaitent tester leurs propres environnements :

Outil	Auteur	Fonctionnalités	Langage
AADInternals	Dr. Nestori Syynimaa	Export cert ADFS, forge tokens, accès M365	PowerShell
ADFSDump	Mandiant (ex-FireEye)	Dump complet config ADFS, export certificats	C#
Mimikatz	Benjamin Delpy	Export certificats non exportables via CryptoAPI	C
DSInternals	Michael Grafnetter	Accès au DKM ADFS dans AD, déchiffrement certificats	PowerShell/ C#
ROADtools	Dirk-jan Mollema	Post-exploitation Entra ID après Golden SAML	Python

Évaluer la Priorité de Migration ADFS vs Entra ID dans votre Organisation

La décision de migrer ADFS vers Entra ID n'est pas uniquement technique : elle implique des considérations budgétaires, opérationnelles et réglementaires. Pour aider à prioriser cette décision, voici les facteurs qui doivent pousser à accélérer la migration :

Serveur ADFS en fin de support : Windows Server 2012/2016 avec ADFS 3.0 ou 4.0 non supportés sont une priorité absolue

Absence de logs ADFS dans le SIEM : si vous ne pouvez pas détecter un Golden SAML, la migration élimine le risque plutôt que de le gérer

Nombre élevé d'applications fédérées critiques : plus les applications sont critiques, plus l'impact d'un Golden SAML est grave, et plus la migration est urgente

Contraintes SecNumCloud/HDS levées ou évoluées : certaines certifications commencent à accepter Entra ID comme alternative valide

Capacité IT limitée pour maintenir ADFS : la maintenance d'ADFS (patches, certificats, WAP) requiert une expertise Windows Server spécialisée qui peut manquer dans les petites équipes

Notre recommandation aux RSSI est de traiter la migration ADFS vers Entra ID comme un projet de sécurité prioritaire en 2026, non pas comme un projet IT ordinaire. Le risque Golden SAML est trop élevé pour justifier le maintien d'ADFS plus longtemps que nécessaire, sauf

contrainte réglementaire formelle et documentée. Pour les sujets d'identité liés à Entra ID après migration, voir notre guide sur l'implémentation Zero Trust pour Microsoft 365.

Ressources Microsoft et MITRE sur ADFS et Golden SAML

La documentation officielle Microsoft sur la sécurité ADFS est disponible en ligne et constitue la référence pour les équipes en charge de maintenir un ADFS on-premises sécurisé :

Références officielles Golden SAML et ADFS

Microsoft Docs : Fédération avec Azure AD et ADFS

MITRE ATT&CK T1606.002 : SAML Tokens (Golden SAML)

Scénario d'Attaque Complet : De l'Accès Initial au Golden SAML

Pour illustrer la dangerosité concrète du Golden SAML, voici un scénario d'attaque réaliste que nos équipes red team ont reconstitué lors de plusieurs engagements :

Étape 1 — Accès initial : L'attaquant envoie un email de phishing à un employé du département IT avec une pièce jointe XLS contenant une macro. L'employé, qui dispose de droits administrateur local sur son poste, exécute la macro. L'attaquant obtient un accès initial via un agent Beacon (Cobalt Strike) ou Sliver.

Étape 2 — Reconnaissance interne : L'attaquant utilise BloodHound/SharpHound pour cartographier l'Active Directory. Il identifie le serveur ADFS (souvent accessible via DNS : adfs.entreprise.fr) et les chemins vers celui-ci depuis le poste compromis.

Étape 3 — Mouvement latéral vers ADFS : Via Pass-the-Hash ou NTLM Relay, l'attaquant obtient des droits administrateur sur le serveur ADFS. Cette étape est facilitée si l'ADFS tourne sur le même serveur que d'autres services ou si des comptes de service partagés sont utilisés.

Étape 4 — Extraction du certificat de signing : Sur le serveur ADFS, l'attaquant exécute ADFSDump.exe ou AADInternals pour extraire le certificat Token Signing avec sa clé privée. L'opération prend moins d'une minute.

Étape 5 — Forging de tokens Golden SAML : Depuis sa machine de C2, l'attaquant forge des tokens SAML pour le compte Global Admin du tenant Microsoft 365 de l'organisation. Il accède aux emails du PDG, aux documents stratégiques et à l'interface d'administration Microsoft 365.

Étape 6 — Persistance longue durée : L'attaquant crée une nouvelle application OAuth dans Entra ID avec des permissions larges (Mail.ReadWrite, User.ReadWrite.All), garantissant un accès persistant même après rotation du certificat ADFS si ce vecteur n'est pas identifié et supprimé lors de la remédiation.

WAP et ADFS : Vecteurs d'Attaque Depuis Internet

Le serveur ADFS est typiquement exposé sur Internet via un **Web Application Proxy (WAP)** pour permettre l'authentification des utilisateurs hors réseau. Cette exposition crée des vecteurs d'attaque additionnels importants que les attaquants n'hésitent pas à exploiter avant même d'avoir un accès au réseau interne. Les endpoints ADFS accessibles depuis Internet incluent /adfs/ls/idpinitiatedsignon.aspx (sign-on initié par l'IdP), /adfs/services/trust/mex (WS-Federation metadata), et /adfs/oauth2/ (OAuth 2.0 endpoints). Chacun de ces endpoints expose une surface d'attaque différente.

Des techniques comme le Password Spray (tester un même mot de passe courant — typiquement "Saison+Année" ou "Entreprise2026!" — contre des milliers de comptes en dessous du seuil de verrouillage) sont fréquemment utilisées contre les endpoints ADFS exposés. Cette technique est d'autant plus efficace que les lockout policies AD ne s'appliquent souvent pas aux tentatives d'authentification via ADFS externe si le Smart Lockout n'est pas configuré. L'activation du

Smart Lockout ADFS et la supervision des événements d'échec d'authentification (411) sont indispensables pour détecter ces tentatives de spray avant qu'elles n'aboutissent.

La migration vers Entra ID offre une protection intégrée contre le password spray via le Smart Lockout cloud, le Identity Protection avec détection d'IP malveillantes, et les Conditional Access Policies basées sur la réputation IP en temps réel — des capacités absentes du WAP ADFS on-premises.

Conditional Access ADFS vs Entra ID : Comparaison des Contrôles

La migration vers Entra ID offre des contrôles de Conditional Access bien supérieurs à ce que propose ADFS nativement :

Entra ID Conditional Access : évaluation en temps réel basée sur l'IP, le device, l'application, le risque utilisateur (IA Microsoft), la géolocalisation et l'heure. Intègre le Continuous Access Evaluation (CAE) qui révoque les sessions en moins d'une minute si une anomalie est détectée.

ADFS Claims Rules : règles statiques basées sur des attributs LDAP ou des tables d'autorisation. Pas d'évaluation comportementale dynamique. Pas de révocation de session en temps réel.

Cette différence explique pourquoi Microsoft recommande si fortement la migration vers Entra ID pour les organisations soucieuses de leur posture de sécurité en 2026. Consultez notre guide complet sur le durcissement Active Directory 2025 pour le contexte AD on-premises associé.

Impact des Golden SAML sur les Applications Non-Microsoft

Le Golden SAML ne se limite pas à Microsoft 365 et Azure. Toute application fédérée avec ADFS via SAML 2.0 est vulnérable : Salesforce, ServiceNow, Workday, AWS IAM, Google Workspace (avec fédération), Okta (si ADFS est configuré comme IdP upstream), et des centaines d'applications SaaS d'entreprise. Une compromission ADFS avec Golden SAML peut

donc potentiellement affecter l'ensemble de l'écosystème applicatif de l'organisation, bien au-delà de l'infrastructure Microsoft.

La cartographie de toutes les applications fédérées avec ADFS est donc un prérequis indispensable à toute analyse d'impact lors d'une réponse à incident Golden SAML. Cette cartographie doit être maintenue à jour dans une CMDB ou un tableau de bord de gestion des identités, et doit inclure pour chaque application : le nom, l'URL du Relying Party Trust, les attributs SAML transmis, et les contacts responsables côté application pour coordonner la rotation de certificat en urgence. Cette cartographie est également utile pour prioriser la migration : les applications les plus critiques (finance, RH, direction) doivent migrer vers Entra ID en priorité pour réduire la fenêtre d'exposition.

Exercice de Table-Top : Simulation d'Incident Golden SAML

Nos recommandations pour les équipes sécurité incluent l'organisation d'un exercice de table-top annuel simulant un incident Golden SAML. Le scénario permet de tester : la capacité de l'équipe SIEM à détecter des connexions SAML anormales dans les logs Entra ID, la procédure de renouvellement d'urgence du certificat ADFS, la coordination avec les équipes métier pour valider les connexions légitimes avant de révoquer toutes les sessions, et la notification réglementaire à l'ANSSI et la CNIL si des données personnelles ont été exposées.

Ce type d'exercice révèle systématiquement des gaps dans les procédures — notamment l'absence de liste à jour des applications fédérées avec ADFS et l'absence de procédure documentée de renouvellement d'urgence du certificat. Ces deux lacunes, faciles à corriger en temps normal, deviennent critiques lors d'un incident réel. L'exercice doit idéalement impliquer à la fois les équipes techniques (SIEM, IAM, infrastructure Windows) et les équipes métier qui utilisent les applications fédérées, car la coordination inter-équipes est souvent le facteur limitant lors d'une réponse à incident réelle.

Score de Risque ADFS : Comment Évaluer la Posture de Sécurité

Pour aider les RSSI à prioriser les investissements sécurité liés à ADFS, nous proposons un score de risque basé sur les critères suivants :

Critère	Score risque	Recommandation
ADFS non patché (>6 mois)	Critique	Patcher immédiatement
Logs ADFS non collectés dans SIEM	Critique	Ingérer en priorité
Accès admin ADFS sans MFA	Critique	Activer MFA immédiatement
ADFS exposé sans WAP	Élevé	Ajouter un WAP ou WAF
Pas de plan de migration Entra ID	Élevé	Lancer le projet de migration
IdP-initiated sign-on actif	Moyen	Désactiver si inutile

Golden SAML et Attaques sur Entra ID en 2026

En 2026, les attaques ont évolué au-delà du Golden SAML classique vers des techniques ciblant directement **Entra ID** sans passer par ADFS. Les techniques documentées incluent le vol de tokens via des applications OAuth malveillantes, l'abus des service principals avec des permissions trop larges, et l'exploitation des Primary Refresh Tokens (PRT) pour obtenir des accès persistants. Notre article dédié sur BadSuccessor et les attaques Entra ID 2026 détaille ces nouveaux vecteurs.

La migration d'ADFS vers Entra ID réduit le risque Golden SAML mais ouvre d'autres surfaces d'attaque qu'il faut sécuriser avec des Conditional Access Policies strictes, la désactivation des applications legacy (Basic Auth), et la surveillance des connexions via Microsoft Defender for Cloud Apps.

Protéger les Applications Web Proxy et Réduire l'Exposition Internet

La sécurisation du Web Application Proxy (WAP) ADFS exposé sur Internet est une priorité souvent négligée. Les mesures recommandées pour les organisations maintenant ADFS incluent la restriction des endpoints exposés aux seuls chemins strictement nécessaires, l'activation du Smart Lockout pour bloquer les attaques de password spray, la surveillance des logs WAP (souvent distincts des logs ADFS) et l'intégration de ces logs dans le SIEM, et l'activation d'Azure AD Application Proxy comme alternative au WAP pour les applications internes.

Une mesure souvent négligée est la désactivation de l'IdP-initiated sign-on sur l'endpoint ADFS public. Cette fonctionnalité, accessible à /adfs/ls/idpinitiatedsignon.aspx, permet d'initier une authentification directement depuis ADFS sans demande initiale d'une application. Elle est rarement nécessaire en production et représente une surface d'attaque additionnelle pour les techniques de reconnaissance et de password spray.

```
 # Desactiver l'IdP-initiated sign-on
Set-AdfsProperties -EnableIdPInitiatedSignonPage $false

# Activer Smart Lockout ADFS (bloquer apres N echecs)
Set-AdfsProperties -ExtranetLockoutEnabled $true -ExtranetLockoutThreshold 10 -ExtranetObse

# Configurer l'Extranet Lockout Mode (Hard Lockout = blocage total, Soft Lockout = ralentis
Set-AdfsProperties -ExtranetLockoutMode AdfsSmartLockoutEnabled

# Surveiller les tentatives d'echec (Smart Lockout logs)
Get-AdfsAccountActivity -Identity utilisateur@domaine.fr
```

Gestion du Cycle de Vie des Certificats ADFS

La gestion du cycle de vie des certificats ADFS est un aspect souvent négligé qui peut créer des problèmes opérationnels lors d'une remédiation d'urgence. Les certificats ADFS auto-signés ont une durée de validité d'un an par défaut et sont renouvelés automatiquement par ADFS.

Cependant, cette rotation automatique peut passer inaperçue et créer des interruptions si les applications fédérées ne sont pas mises à jour avec le nouveau certificat.

Notre recommandation est de mettre en place un monitoring proactif des certificats ADFS avec des alertes 60 jours avant expiration, et de documenter la procédure de rotation de certificat — à la fois la rotation planifiée et la rotation d'urgence post-compromission. Cette procédure doit être testée annuellement pour s'assurer qu'elle fonctionne correctement et que les équipes savent l'appliquer sous pression.

```
 # Verifier les certificats ADFS actuels et leur date d'expiration
Get-AdfsCertificate | Select-Object CertificateType, Thumbprint, @{N='Expiry';E={$_.Certifi

# Configurer le renouvellement automatique des certificats
Set-AdfsProperties -AutoCertificateRollover $true

# Rotation manuelle d'urgence (post-compromission)
Update-AdfsCertificate -CertificateType Token-Signing -Urgent
Update-AdfsCertificate -CertificateType Token-Decrypting -Urgent

# Apres rotation : mettre a jour les Relying Party Trusts
Get-AdfsRelyingPartyTrust | ForEach-Object {
    Update-AdfsCertificate -TargetRelyingParty $_.Name -CertificateType Token-Signing
}
```

Intégration ADFS dans un Programme de Purple Team

La thématique Golden SAML est idéale pour un exercice purple team ciblé sur les environnements ADFS. Notre approche recommandée pour les organisations souhaitant tester leur résilience face à cette attaque comprend trois phases distinctes : une phase de red team (extraction du certificat et forging d'un token en lab ou en environnement de test isolé), une phase blue team (vérification que les alertes SIEM se déclenchent correctement sur les indicateurs attendus), et une phase de consolidation (correction des gaps de détection identifiés et validation de la procédure de réponse à incident).

Les indicateurs clés à valider lors du purple team ADFS sont : déclenchement d'une alerte SIEM sur la création d'un processus ADFSDump sur le serveur ADFS (événement Sysmon 1 avec commandline suspect), déclenchement d'une alerte sur la connexion Microsoft 365 depuis une IP hors des plages habituelles avec authentification SAML, et déclenchement de la procédure de renouvellement d'urgence dans les délais définis (objectif : moins de 30 minutes entre la détection et le renouvellement du certificat).

Foire Aux Questions sur le Golden SAML et ADFS

Le MFA protège-t-il contre le Golden SAML ?

Non. C'est l'un des aspects les plus dangereux du Golden SAML : l'assertion forgée peut inclure n'importe quel attribut d'authentification, y compris des claims indiquant que le MFA a été effectué, que la machine est conforme aux politiques de l'organisation, et que l'utilisateur est membre des groupes d'administrateurs. L'application cible (comme Microsoft 365) fait confiance à l'assertion SAML signée par ADFS et considère que toutes les exigences d'authentification ont été satisfaites, même si aucune vérification MFA réelle n'a eu lieu. C'est une différence fondamentale avec les attaques de phishing qui tentent de capturer des codes MFA en temps réel : le Golden SAML n'en a tout simplement pas besoin.

Comment savoir si mon organisation a été victime d'un Golden SAML ?

La détection est difficile sans logs ADFS dans le SIEM, et c'est précisément pourquoi la collecte de ces logs est une priorité absolue. Les indicateurs à rechercher sont : connexions

Microsoft 365 réussies en dehors des heures habituelles, depuis des IPs inconnues, sans activité correspondante dans les logs AD (événement 4624) ; tokens SAML émis pour des comptes sensibles sans request initiale dans les logs ADFS (événement 299 sans événement 410 ou 411 préalable) ; alertes Microsoft Defender for Cloud Apps sur des activités administratives anormales comme la création de nouvelles applications OAuth ou la modification des paramètres du tenant. Un audit forensique des logs ADFS sur les 12 derniers mois est recommandé si une compromission est suspectée, en commençant par les comptes les plus privilégiés (Global Admin, Exchange Admin, etc.).

Renouveler le certificat ADFS suffit-il à éradiquer une compromission Golden SAML ?

Non, le renouvellement du certificat est nécessaire mais insuffisant. Il invalide les tokens forgés avec l'ancienne clé, mais ne remédie pas aux backdoors que l'attaquant aurait pu installer lors de son accès au serveur ADFS (Shimmers, tâches planifiées, comptes de service cachés). Une remédiation complète nécessite obligatoirement : l'analyse forensique complète du serveur ADFS, la vérification de l'intégrité de toutes les DLL ADFS avec des hashes de référence, l'audit exhaustif des comptes et applications dans Entra ID pour détecter des backdoors (nouvelles applications OAuth, nouveaux service principals avec permissions, Conditional Access gaps), et la rotation de tous les secrets d'application qui auraient pu être compromis ou utilisés pendant la période de compromission. Dans les cas graves, la reconstruction complète du serveur ADFS sur une base saine est la seule garantie d'éradication totale.

À RETENIR

Points clés à retenir sur le Golden SAML et ADFS 2026

Le Golden SAML contourne le MFA — l'assertion forgée peut inclure n'importe quel claim d'authentification, y compris les claims MFA satisfait

La clé privée ADFS est la clé du royaume — son extraction permet l'accès permanent et persistant à toutes les applications fédérées SAML

Les logs ADFS sont indispensables — sans leur collecte dans un SIEM, la détection Golden SAML est quasi impossible même avec MDI et Defender

Le DKM ADFS stocke la clé dans AD — surveiller les accès LDAP au chemin CN=ADFS dans AD Data est un indicateur de détection précoce

La migration vers Entra ID est la seule solution définitive — recommandée par Microsoft pour 2026, elle élimine le vecteur Golden SAML

Les Shimmers ADFS assurent la persistance — un serveur ADFS compromis doit être reconstruit, pas simplement patché et redémarré

Renouveler le certificat immédiatement en cas de compromission suspectée, même sans preuve formelle, comme mesure conservatoire

Cartographier les applications fédérées — connaître la liste complète est indispensable pour évaluer l'impact et coordonner la rotation d'urgence