21 octobre 2025 - PARIS

Comment gérer les stratégies de mots de passe AD/Entra ID

Hakim TAOUSSI
Thierry DEMAN

AGENDA DE LA CONFÉRENCE

Hakim TAOUSSI
Architecte Technique
MVP Security
Dinosaure et fan de Star Wars

Thierry DEMAN
Architecte d'Infrastructure Senior
MS MVP x 24, Security&M365
45 ans dans l'IT
Auteur, Speaker, Blogger
ALT-UP

- Stratégies de mots de passe dans les environnements (Hybrides) AD DS et Microsoft Entra ID
- Impact du mode Hybride géré par Entra Connect
- Vision d'ensemble des strategies AD, Cloud
- Standardiser la configuration et aligner le Cloud et le On-Premises
- Conclusions, risques (Activer MFA et planifier la transition vers passwordless (TAP, FIDO2, passkeys).

Stratégies de mots de passe en mode hybride AD DS et Entra ID

Portée et ciblage des stratégies de mots de passe

	AD DS (on-prem)	Microsoft Entra ID (Azure AD)
Où s'applique la stratégie	Par domaine AD	Au tenant Entra (tous les comptes cloud-only). Expiration par domaine de messagerie
Ciblage fin	FGPP (Fine-Grained Password Policies) pour appliquer des jeux de paramètres différents à des groupes/utilisateurs (privilégiés vs standard).	Pas d'équivalent à FGPP. On peut cibler par groupes les méthodes d'authentification (MFA, passkeys, TAP), mais pas définir des longueurs/complexités différentes par groupe.

Complexité et longueur des mots de passe

Critère	AD DS	Entra ID
Complexité	Règle classique « 3 sur 4 catégories » + ne pas contenir le nom/d'affichage — implémentée par Passfilt.dll (non modifiable sans filtre personnalisé).	Password Protection : blocage des mots de passe trop faibles via une liste globale bannie (Microsoft) + liste personnalisée (organisation). Pas de règle « 3/4 », l'évaluation est contextuelle (variantes, substitutions…).
Longueur minimale	Paramètre configurable (via GPO/FGPP).	Longueur mini 8 caractères pour les comptes cloud ; non personnalisable aujourd'hui (même en P1/P2).
Filtres personnalisés	Possible via Password Filter DLL (développement spécifique).	Pas de filtres DLL, mais liste bannie personnalisée (jusqu'à des centaines de termes métiers, marques, lieux, etc.).
Extension on-prem	—	Entra Password Protection on-prem : agent DC + proxy pour étendre les listes bannies à AD DS (mode Audit puis Enforce).

Âge, historique des mots de passe, verrouillage (Lockout)

	AD DS	Entra ID
Âge min/max, **Historique**	Entièrement configurable - âge min/max, - historique, - réversible, Au niveau du domaine ou via FGPP.	Expiration cloud-only : par défaut, Microsoft 365/Entra positionne l'organisation à « ne jamais expirer » (recommandation moderne). Vous pouvez réactiver une expiration 14–730 jours au niveau de l'organisation (ou par domaine). L'historique est géré côté service (impossibilité d'utiliser l'ancien mot de passe immédiat).
Lockout	Se règle par GPO Domain ou FGPP - **seuil**, - **durée** - **fenêtre d'observation**.	Smart Lockout (toujours actif) - par défaut 10 tentatives ⇒ 1 minute de blocage puis durée croissante, déduplication des 3 dernières mauvaises saisies, réglages personnalisables (P1+).

Scénarios hybrides (Qui « gagne », Quand?)

Scénario	Ce qu'il faut retenir
PHS (Password Hash Sync)	Pour la connexion cloud, Entra applique ses contrôles (Smart Lockout, listes bannies). L'expiration pour les utilisateurs synchronisés **n'est pas appliquée** sauf si vous activez **CloudPasswordPolicyForPasswordSyncedUsersEnabled** Quand activé, la politique d'expiration cloud Entra s'applique aussi aux comptes synchronisés.
PTA/Fédération (AD FS)	L'authentification se fait on-prem : c'est surtout la politique AD DS qui s'applique pour la complexité/expiration. En parallèle, Smart Lockout protège la « porte d'entrée » cloud (mais la déduplication des hachages de mauvais mots de passe ne s'applique pas en PTA). Pour AD FS, utiliser Extranet Smart Lockout.
SSPR avec writeback Changement de mot de passe	Si l'utilisateur réinitialise dans le cloud (SSPR) avec writeback activé, le contrôle AD DS (historique, complexité, filtres, âges) est appliqué avant de mettre à jour le mot de passe dans AD. Le retour est synchronisé en temps réel.

Différences principales

	AD DS	Entra ID
Modèle de complexité	Règle Statique, filtre DLL possible	Evaluation de force Listes de mots de passe bannis
Granularité (Durée, Taille,...)	FGPP pour ciblage fin	Stratégie liée au tenant Granularité sur les méthodes d'authentification
Longueur minimale	Configurable	8 caractères minimum **Non Modifiable** Passer par PassPhrases et PasswordLess pour augmenter la longueur
Expiration(CloudOnly)		Par défaut: N'expire jamais (avant c'était 90 jours) Modifiable 14(Notification)-730(Expiration) jours Par domaine
Expiration(Synchronisés)	Configurable	CloudPasswordPolicyForpasswordSyncedUsers permet d'aligner l'expiration sur le cloud.
Parcours passwordless		TAP(Temporary Access Pass) permet d'amorcer une configuration passwordLess (FIDO2/passkeys

Impact du mode Hybride géré par Entra Connect

Importance du Password write-back activé

Il permet de s'assurer que toutes les stratégies AD s'appliquent pour les utilisateurs synchronisés pour les actions suivantes

- SSPR
- Ou changement de mot de passe

Pb: il faut des licences AD premium P1
Pb: La stratégie AD ne s'applique qu'aux utilisateurs synchronisés

Les authentifications PTA et ADFS ne sont pas impactées.

Risques identifiés (Notamment sans Write-Back activé)

- Le mot de passe modifié dans le cloud (Office 365 / Azure AD) n'est pas répliqué vers l'Active Directory local.
- Les mots de passe expirés dans AD peuvent encore fonctionner O365 (jusqu'à la mise à jour)
- Les stratégies de mot de passe définies dans Active Directory ne sont pas appliquées lors de ce changement.
- Le mot de passe est uniquement soumis aux règles de sécurité d'Azure AD, qui sont distinctes de celles de l'AD local.

Conséquences de cette configuration

- Cela peut entraîner une divergence entre les mots de passe utilisés dans le cloud et ceux attendus dans l'environnement local.
- Les utilisateurs peuvent se retrouver avec des mots de passe non conformes aux exigences de complexité, longueur ou expiration définies dans l'Active Directory.
- En cas de retour vers un environnement hybride ou d'accès à des ressources locales, cela peut poser des problèmes d'authentification (Verrouillage).

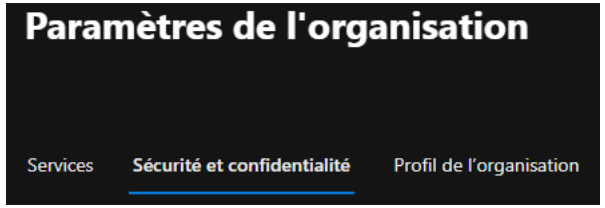
Problème de l’expiration différente (même avec WriteBack)

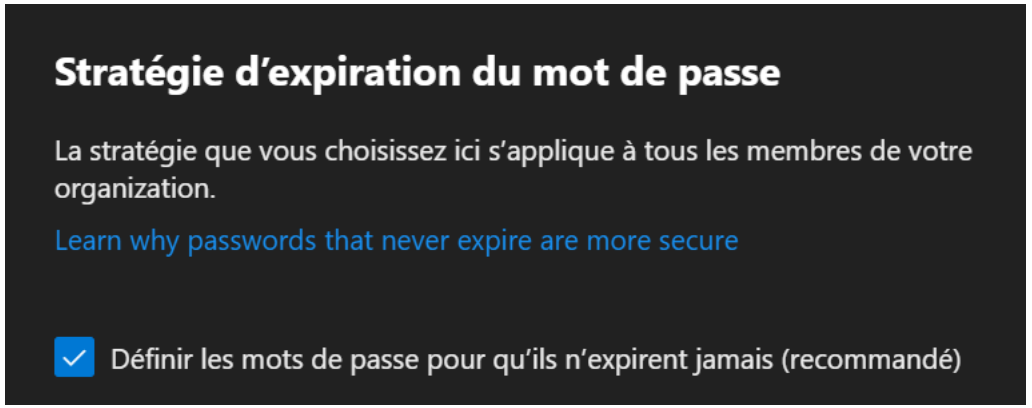
- Les dates d’expiration de compte ne sont pas synchronisées et ne sont donc pas prises en compte par Azure AD.
- Les utilisateurs Cloud/O365 ont une expérience différente

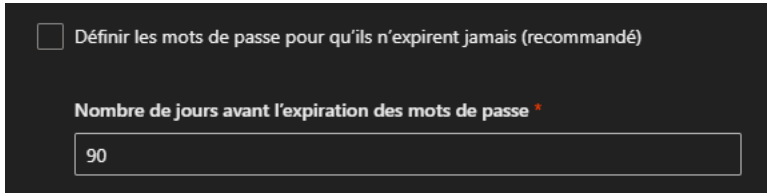
- Le suivi des utilisateurs « Cloud-Only » est souvent moins rigoureux.
- Certains clients demandent un comportement identique, notamment sur l’intervalle de changement des mots de passe.

Faut il activer une expiration sur le Cloud ?

- Attention, ce paramètre s'applique et **Remplace toutes** les stratégies par domaines qui ont pu être mises en place (Activation ou Désactivation)








```
PS C:\Users\DEMANThierry> Get-MgDomain -Property * | ft id,*password*

Id                                 PasswordNotificationWindowInDays PasswordValidityPeriodInDays
--                                 -------------------------------- ----------------------------
faqexchange.info                                                 14                   2147483647
FrenchExchangeFAQ.onmicrosoft.com                                14                   2147483647
athou.com                                                        14                          730
FrenchExchangeFAQ.mail.onmicrosoft.com                           14                   2147483647
```

Faut il activer l'expiration Cloud pour les utilisateurs synchronisés ?

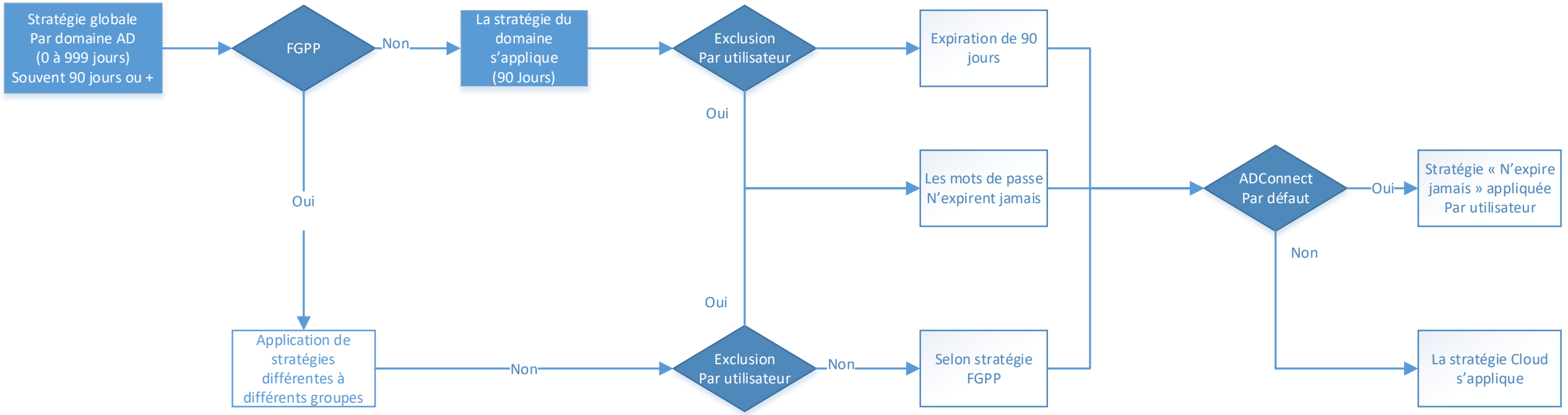
- Par défaut, tous les utilisateurs synchronisés ont l'expiration désactivée (Propriété définie sur chaque utilisateur).
- On peut modifier ce comportement pour que la stratégie Cloud s'applique (si elle a été définie).

```
# Connection via Graph
Connect-MgGraph -Scopes "Policy.ReadWrite.AuthenticationMethods","Directory.ReadWrite.All"
 # Lire l'état
(Get-MgDirectoryOnPremiseSynchronization).Features
 # Activer
$sync = Get-MgDirectoryOnPremiseSynchronization
$sync.Features.CloudPasswordPolicyForPasswordSyncedUsersEnabled = $true
Update-MgDirectoryOnPremiseSynchronization -OnPremisesDirectorySynchronization $sync
```

Vision d’ensemble des stratégies

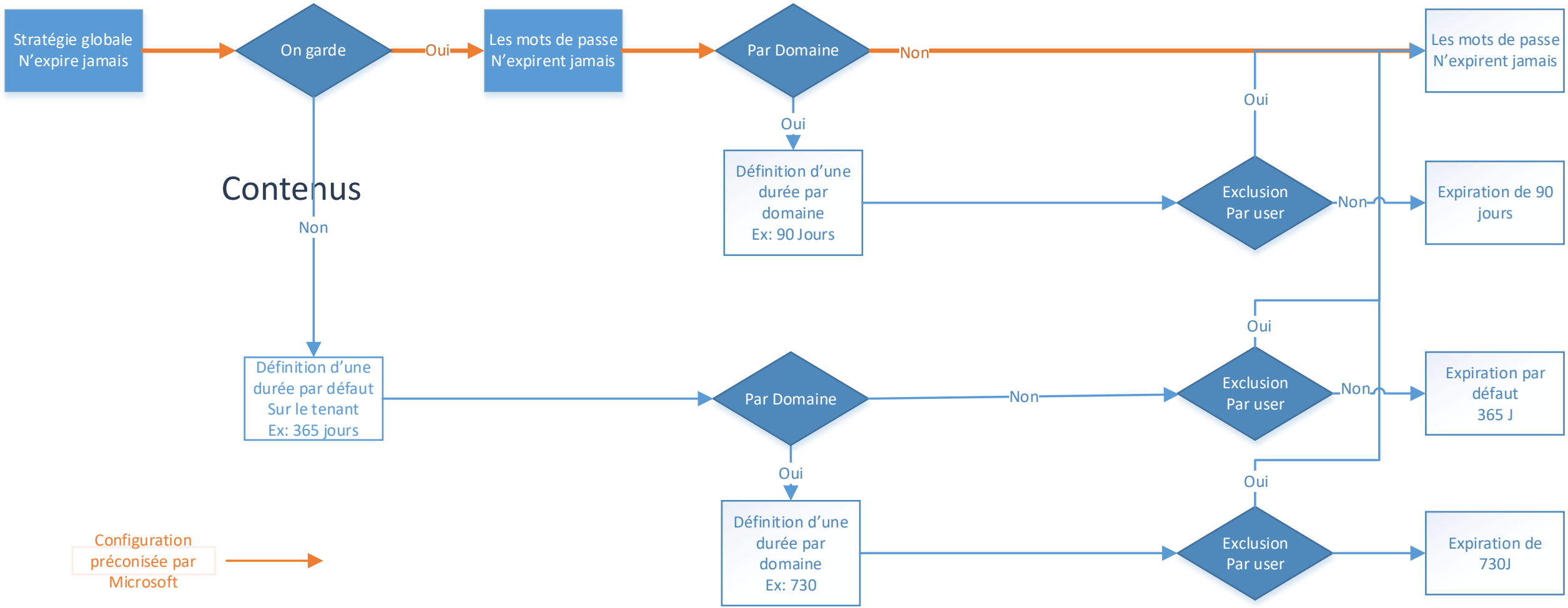
Stratégies sur AD

Configuration des stratégies d'expiration (AD DS)



Stratégies Cloud

Configuration des stratégies d'expiration (Mode Cloud)



Points importants de la configuration à définir

- L’expiration par défaut (durée) ou la non expiration sur le cloud
- L’expiration pour chaque domaine (Cloud et AD selon UPN)
- La synchronization ADConnect de la stratégie « NeverExpire by default » après chaque création, mise à jour du mot de passe
- Les exclusions (quels comptes gardent la stratégie “NeverExpires”).

Bonnes pratiques

- Eviter de modifier la stratégie générale (Ne plus y toucher après modification)
- Eviter de modifier la stratégie des domaines OnMicrosoft
- Ne cibler que les domaines ajoutés en fonction des besoins

⇒ Vérifier l'impact sur les éventuels changements de mots de passe « en masse »
(**Regarder les dates de derniers changements de mots de passe**)

- Activer SSPR (P1) et Write-Back Password (license P1 Premium)

⇒ Mettre la granularité sur les stratégies AD (8 caractères ou +)

Standardiser la configuration
Aligner le Cloud et le On-Premises

Différentes possibilités selon la configuration

- **Standardiser par domaine (stratégie par défaut ou FGPP)**
- **Attribuer les FGPP à des groupes (automatiser l'appartenance)**
- **Gérer les exceptions (PasswordNeverExpires) par un groupe On-Premises et CloudOnly**
- **Activer l'option « CloudPasswordPolicyForPasswordSyncedUsersEnabled »**
  - **⇒ Le cloud doit appliquer une stratégie équivalente sur les comptes synchronisés**
  - **⇒ Configurer l'expiration équivalente pour les domaines sur le Cloud**
- **Gérer les changements d'expiration de compte**
  - **⇒ En plaçant les utilisateurs dans les groupes appropriés (pour AD, comptes synchronisés)**
  - **⇒ Groupes appropriés pour O365 (+ Scripts de modification des utilisateurs)**

Automatisation/alignement des stratégies

	AD	Azure AD	Scripts - Automatisation
Stratégies à vérifier	GPO standard X Jours	Stratégie par défaut qui positionne la « non expiration » Stratégie Cloud sur X Jours (A positionner comme AD)	Modification par domaine (Utilisés dans l'UPN)
User Standard	Expiration par GPO	Pas d'expiration	Situation par défaut qui doit être modifiée initialement
Script quotidien	MDP changé dans les 24H Nouveau compte	⇒ Retirer la stratégie de « nonExpiration »	Exclure les comptes qui n'expirent jamais
Service, Admins	N'expire jamais, MDP changé dans les 24H	Non expiration par défaut	Laisser la valeur par défaut (script initial de vérification)

- Les scripts peuvent fonctionner en taches planifiées (quotidiennes)
  ⇒ On considère qu'un intervalle de 24H est suffisant

Exemple de modification des stratégies d'expiration

```
Connect-MgGraph -Scopes {Directory.AccessAsUser.All}

Update-MgDomain -domainId athou.com -PasswordValidityPeriodInDays 365 `
    -PasswordNotificationWindowInDays:30
```

- L'important est qu'il n'y ait le moins de décalage possible entre l'application des stratégies AD et Azure AD.

Script de modification des stratégies d'expiration

```
#Install-Module -Name Microsoft.Graph.Authentication -Scope AllUsers
#Connect-MgGraph -Scopes "OnPremDirectorySynchronization.ReadWrite.All"
#Connect-MgGraph -Scopes "User.ReadWrite.All","Group.ReadWrite.All"
$date=date; $DateRef=$date.AddDays(-1)
$AllUsers = Get-ADUser -SearchBase 'DC=DEMAN,DC=local' -Filter { passwordNeverExpires -eq $False –and
enabled -eq $true -and PasswordLastSet -gt $dateRef } -properties pwdlastset,passwordlastset |select
userprincipalname,pwdlastset,passwordlastset
foreach ($account in $AllUsers{
    $t = (Get-MgUser -ObjectID $account.userPrincipalName).passwordpolicies
    if ($t -eq "DisablePasswordExpiration") {
#    Set-MgUser -ObjectID $account.userPrincipalName -PasswordPolicies "DisablePasswordExpiration"
     Set-MgUser -ObjectID $account.userPrincipalName -PasswordPolicies "None"
    }
}
#get-Mguser -userID $UPN -Property passwordpolicies, lastpasswordchangedateTime | ft
userprincipalname,PasswordPolicies,lastpasswordchangedateTime
```

Désactivation des comptes expirés

- **Incohérence de sécurité** : un compte censé être expiré peut encore accéder aux ressources cloud si vous êtes en PHS.

- **Risque de conformité** : si vous utilisez la date d'expiration pour gérer les fins de contrat, Azure AD ne reflète pas automatiquement cet état.

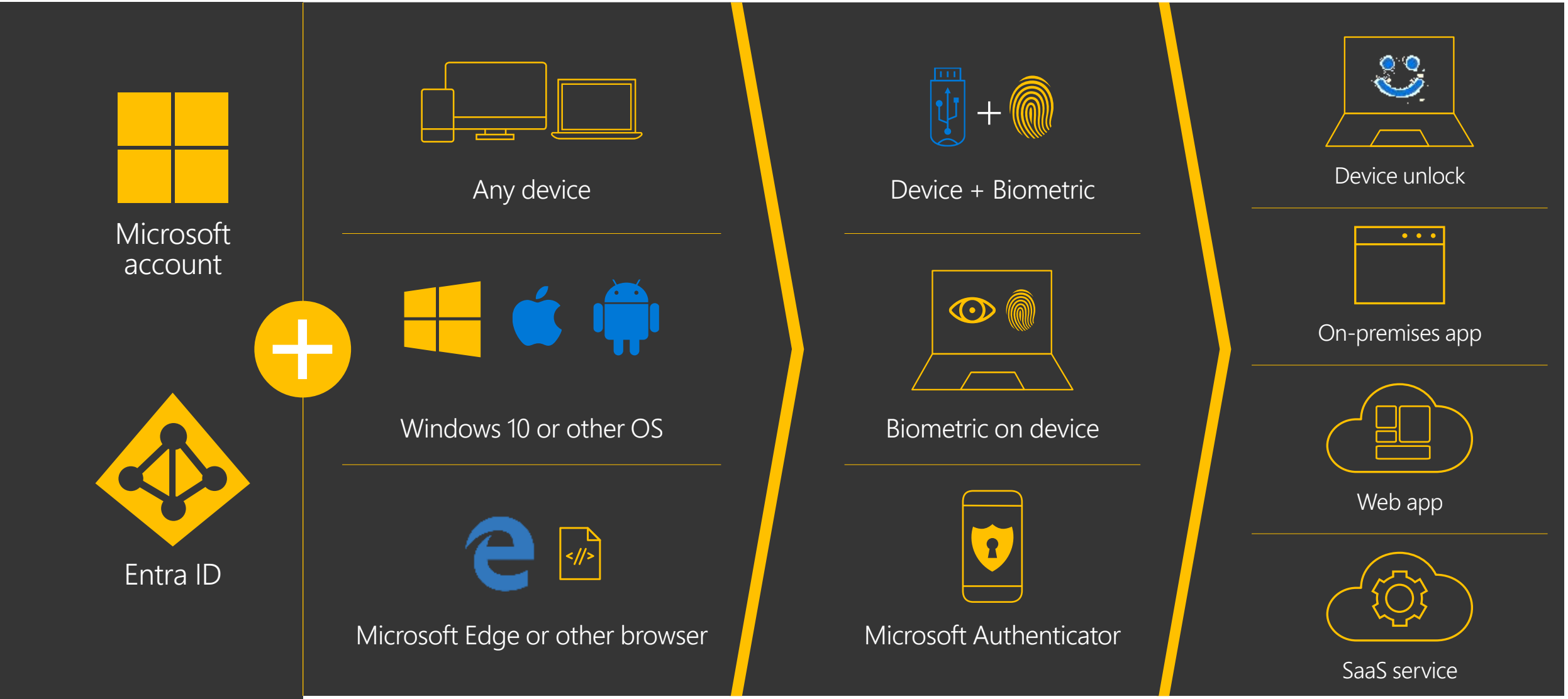
- **Solution de contournement** :

  Mettre en place un script ou une tâche planifiée qui désactive dans AD DS les comptes expirés, ce qui est bien synchronisé vers Azure AD (l'attribut *accountEnabled* est pris en compte).

```
Search-ADAccount -AccountExpired -UsersOnly | Disable-ADAccount -PassThru
```

Planifier la transition vers le passwordless
Conclusions

The roadmap to no more passwords



Feature summary	PTA + sSSO	PHS + sSSO	ADFS
Authentication against credentials held on-premises	Yes	No	Yes
Single-Sign-On	Yes	Yes	Yes
Passwords remain on premises	Yes	Salted hash synced	Yes
On-premises MFA solution	No	No	Yes
Azure AD MFA	Yes	Yes	Yes
On-premises password policies	**Yes**	**Partial**	**Yes**
On-premises account enable/disable	**Yes**	**Delayed (30 mins)**	**Yes**
On-premises password lockout	**Yes**	**No**	**Yes**
Conditional access	Yes++	Yes++	Yes
Credentials captured from user via Azure AD UI	Yes	Yes	No
Protection against on-premise account lockout	Smart Lockout	N/A	Extranet Lockout
Cost of implementation	Medium	Low	High
Scalability/fault tolerance	Cloud scalability	Cloud scalability	Complex
AuthN **fails** for remote workers if the on-premises Internet connection is down. Requires HA solution.	Yes	No	Yes
On-going maintenance for authentication	Automated	None	SSL certificate management
Azure AD Connect Health monitoring	Not integrated	Limited	Yes
Azure AD Identity Protection (requires P2 license)	Yes	Yes	No

Conclusions

- Le point essentiel est l'expiration des comptes et leurs mots de passe qui doivent être synchronisés.
- Les autres paramètres n'ont pas de correspondant sur Azure AD et ne peuvent pas être synchronisés.
- Vérifier bien tous les comptes expirés et connexions anormales sur le Cloud
- **Les mots de passe restent essentiels à de nombreuses configurations.**
- **Protéger les comptes de récupérations (et leurs mots de passe)**

Toute modification doit être mesurée précisément, avant sa mise en place (progressive après analyse des dates de derniers changements de mot de passe).


MERCI

21 octobre 2025 - PARIS

IDENTITY DAYS

@IdentityDays
#identitydays2025