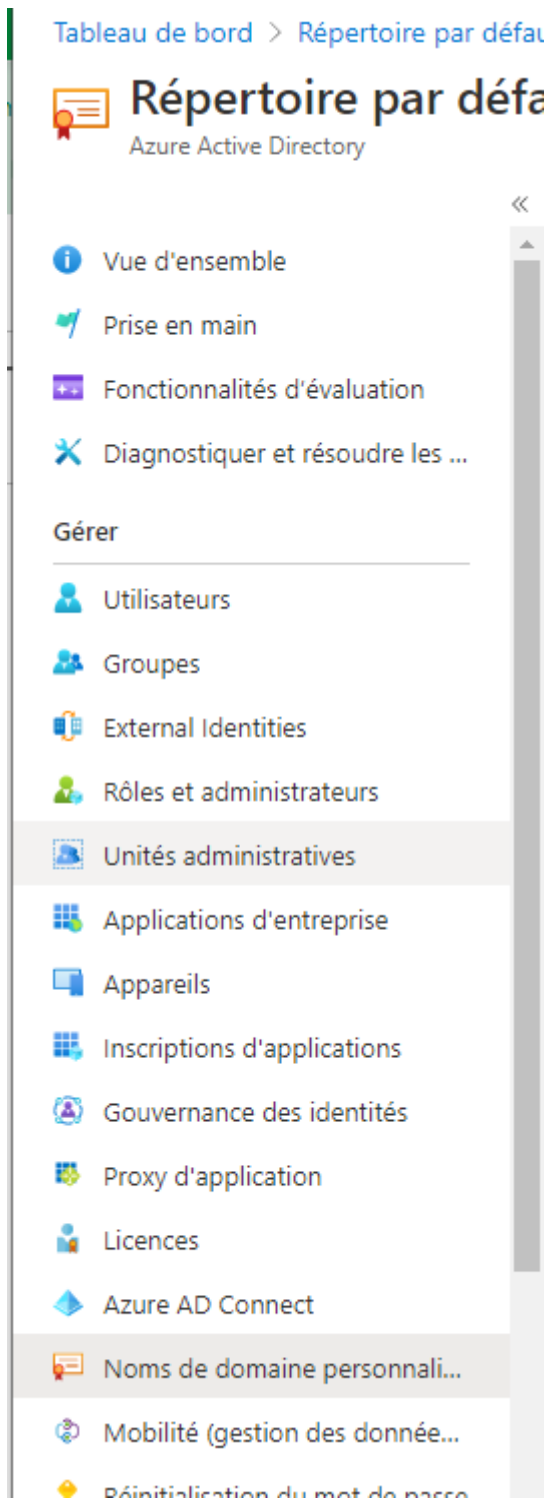


Azure Active Directory

- [Création d'un nom de domaine personnalisé](#)
- [Azure AD Connect](#)
- [Activer l'authentification unique Azure AD](#)
- [Usage Location](#)
- [Hybrid Azure AD Join](#)
- [Activer l'inscription automatique dans Intune](#)
- [Recréer l'objet Ordinateur AzureADSSOACC](#)
- [Synchroniser dans Azure uniquement les membres d'un groupe](#)
- [Activer la synchronisation des mots de passe entre Azure AD et l'AD local](#)
- [Personnel vs Entreprise, Registered vs Azure AD joined](#)
- [Différences entre l'authentification unique à l'aide d'un jeton d'actualisation principal ou authentification unique fluide \(Seamless SSO\)](#)
- [Ajouter un suffixe UPN pour la synchronisation Azure AD](#)
- [Rester connecté à toutes vos applications](#)
- [Enterprise State Roaming](#)
- [Ajouter un administrateur local d'appareils joints à Azure AD \(AAD Joined\)](#)
- [Limiter le nombre d'appareils par utilisateur](#)
- [Supprimer un groupe orphelin issu d'un domaine local](#)
- [Empêcher les utilisateurs de joindre leur PC à Entra ID \(Azure AD\)](#)

Création d'un nom de domaine personnalisé

Dans "Azure Active Directory", on sélectionne "Noms de domaine personnalisé".



On clique sur "Ajouter un domaine personnalisé".

Nom de domaine personnalisé * ⓘ

lab.khroners.fr ✓

On nous demande d'ajouter un enregistrement TXT dans notre bureau d'enregistrement de noms de domaine, dans mon cas OVH.

lab.khroners.fr ...

Nom de domaine personnalisé

 Supprimer |  Des commentaires ?

i Pour utiliser lab.khroners.fr avec votre compte Azure AD, créez un enregistrement TXT dans votre bureau d'enregistrement de noms de domaine à l'aide des informations ci-dessous.

Type d'enregistrement

TXT

MX

Alias ou nom d'hôte

@

Adresse de destination ou de pointage

[REDACTED]

Durée de vie

3600

[Partager ces paramètres par e-mail](#)

La vérification ne réussit pas tant que vous n'avez pas configuré le domaine dans votre bureau d'enregistrement comme décrit ci-dessus.

Ce qui donne pour OVH :

Ajouter une entrée à la zone DNS

Étape 2 sur 3

* Les champs suivis d'un astérisque sont obligatoires.

Sous-domaine

lab .khroners.fr.

TTL

Personnalisé 3600 s.

Valeur *

MS=ms78650005

Le champ TXT actuellement généré est le suivant :

lab 3600 IN TXT " [REDACTED] "

Annuler

Précédent

Suivant

On clique ensuite sur "Vérifier".

✓ Vérifier le nom de domaine 19:03 ✕

Nom de domaine lab.khroners.fr vérifié pour une utilisation dans Répertoire par défaut

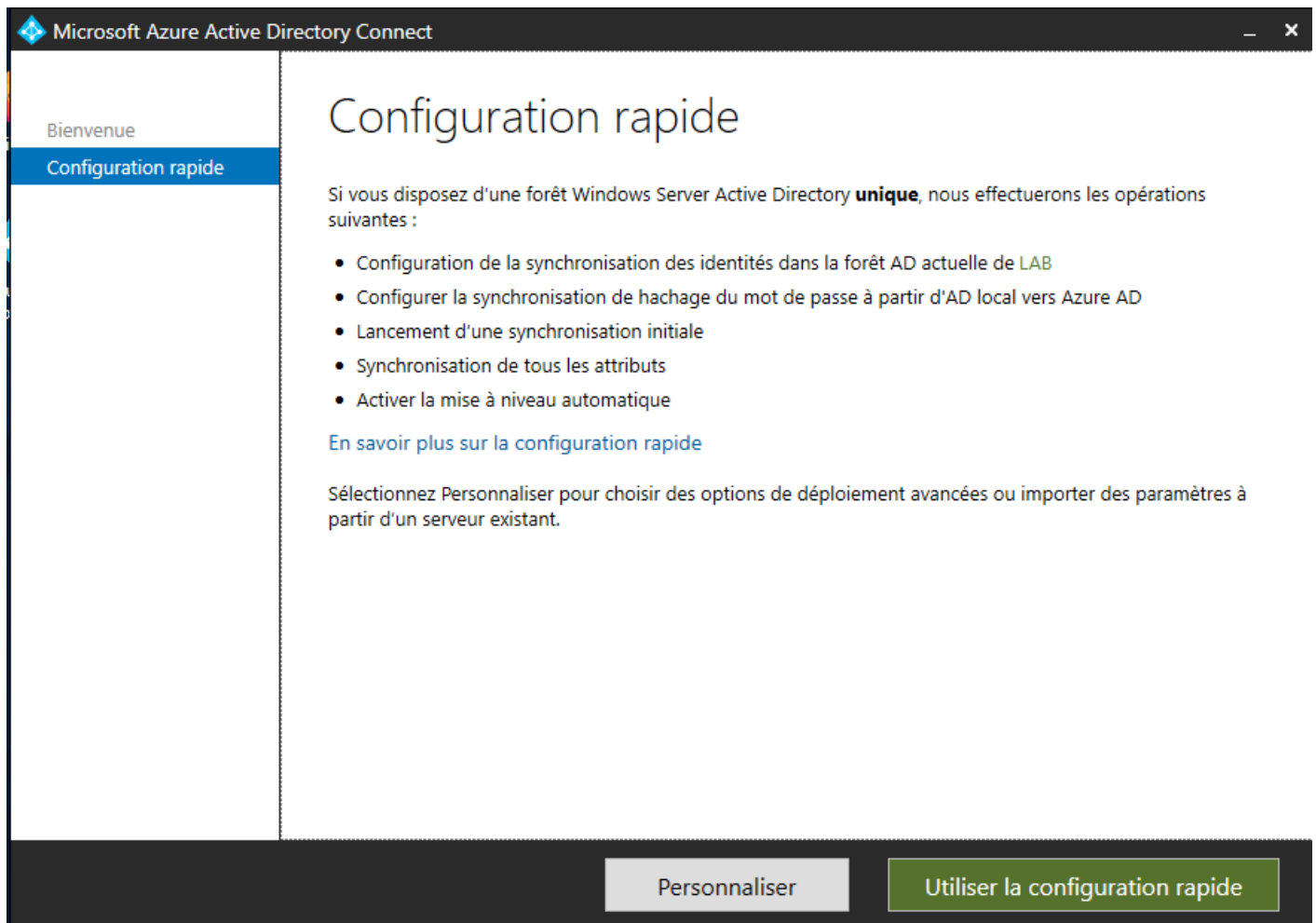
Le nom de domaine est vérifié.

Nom	Statut
lab.khroners.fr	✓ Vérifié

On peut le définir comme domaine par défaut.

Azure AD Connect

On télécharge [Azure AD Connect](#). On utilise la configuration rapide.



On se connecte via un compte avec le rôle Administrateur général.

Bienvenue

Configuration rapide

Connexion à Azure AD

Connexion à AD DS

Configurer

Connexion à Azure AD

Saisissez vos informations d'identification d'administrateur général Azure AD. ?

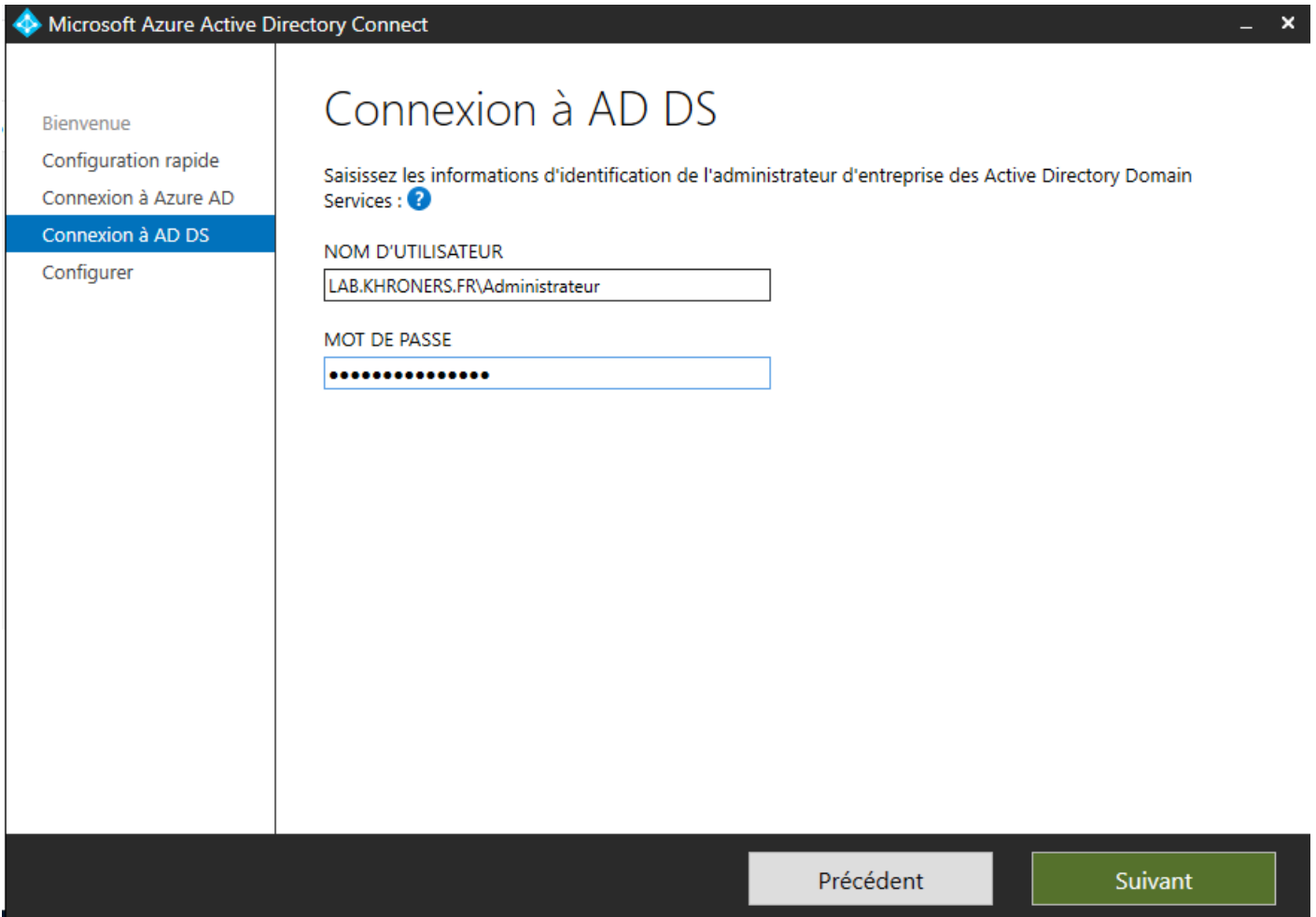
NOM D'UTILISATEUR

MOT DE PASSE

Précédent

Suivant

On se connecte ensuite à l'AD DS local.



On installe ensuite.

Bienvenue

Configuration rapide

Connexion à Azure AD

Connexion à AD DS

Configurer

Prêt pour la configuration

Cliquer sur Installer entraîne les actions suivantes :

- Installer le moteur de synchronisation
- Configurer Azure AD Connecteur
- Configurer lab.khroners.fr Connecteur
- Activer Synchronisation de hachage du mot de passe
- Activer Mise à niveau automatique
- Configuration des services de synchronisation sur cet ordinateur

Démarrez le processus de synchronisation une fois la configuration terminée.

Précédent

Installer

Activer l'authentification unique Azure AD

Présentation

L'authentification unique permet aux utilisateurs d'être automatiquement connectés aux applications via leur compte AD.

Cela peut être nécessaire lorsque les ordinateurs ne sont pas joints en mode hybride (Active Directory Joined).

Activation de l'authentification unique

Dans Azure AD Connect (application sur le serveur), on choisit "Connexion utilisateur" puis on coche "Activer l'authentification unique" avec "Synchronisation de hachage du mot de passe". (choisie par défaut) On peut également choisir "Authentification directe" si on a besoin de stratégies de compte locales.

Avec l'authentification directe (PTA), si le contrôleur de domaine est inaccessible (DC non fonctionnel, réseau interrompu...), l'authentification ne fonctionnera pas. Pour contrer cela, on peut ajouter des agents sur d'autres réseaux où un contrôleur de domaine répliqué est présent ; ou activer la synchronisation de hachage du mot de passe en modifiant les options après installation, et de basculer manuellement l'authentification vers ce mode quand le contrôleur de domaine est indisponible. Pour plus d'informations, cliquez [ici](#).

[Bienvenue](#)[Tâches](#)[Connexion à Azure AD](#)[Connexion utilisateur](#)[Authentification unique](#)[Configurer](#)

Connexion utilisateur

Sélectionnez la méthode d'authentification. ?

- Synchronisation de hachage du mot de passe ?
- Authentification directe ?
- Fédération avec AD FS ?
- Fédération avec PingFederate ?
- Ne pas configurer ?

Sélectionnez cette option pour activer l'authentification unique pour les utilisateurs d'ordinateurs de bureau d'entreprise :

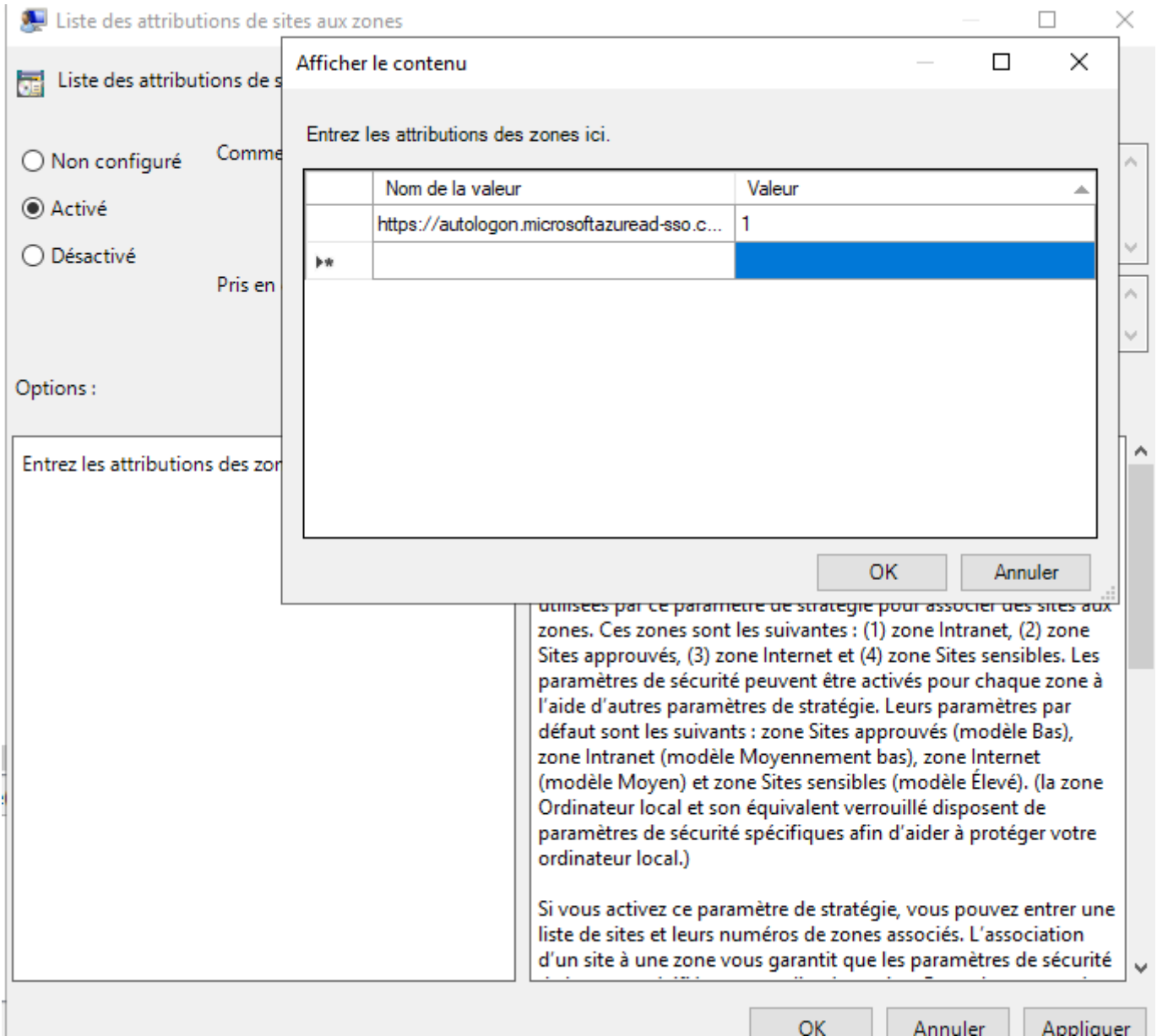
- Activer l'authentification unique ?

[Précédent](#)[Suivant](#)

Il faut ensuite ajouter une stratégie de groupe.

Configuration utilisateur > Stratégie > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Onglet Sécurité

On ajoute ici `https://autoLogon.microsoftazuread-ss0.com` .



On applique ensuite cette GPO à l'OU contenant nos utilisateurs.

On ajoute aussi :

BZH-FP-U-HybridAzureADJoin

Étendue Détails Paramètres Délégation

The screenshot shows the 'Délégation' (Delegation) tab in the Azure AD Join configuration interface. It features several expandable sections:

- Délégation**: Includes an 'afficher' (show) button.
- Configuration ordinateur (activée)**: Includes a 'masquer' (hide) button and the text 'Aucun paramètre n'est défini.' (No parameter is defined).
- Configuration utilisateur (activée)**: Includes a 'masquer' (hide) button.
- Stratégies**: Includes a 'masquer' (hide) button.
- Modèles d'administration**: Includes a 'masquer' (hide) button and the text 'Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.' (Strategy definitions (ADMX files) retrieved from the local computer).
- Composants Windows/Internet Explorer/Panneau de configuration Internet/Onglet Sécurité/Zone intranet**: Contains a table of strategies.

Stratégie	Paramètre	Commentaire
Autoniser les mises à jour de la barre d'état via le script	Activé	
Mises à jour de la barre d'état via un script	Activé	

Voir : <https://docs.microsoft.com/fr-fr/azure/active-directory/hybrid/how-to-connect-sso-quick-start#step-3-roll-out-the-feature>

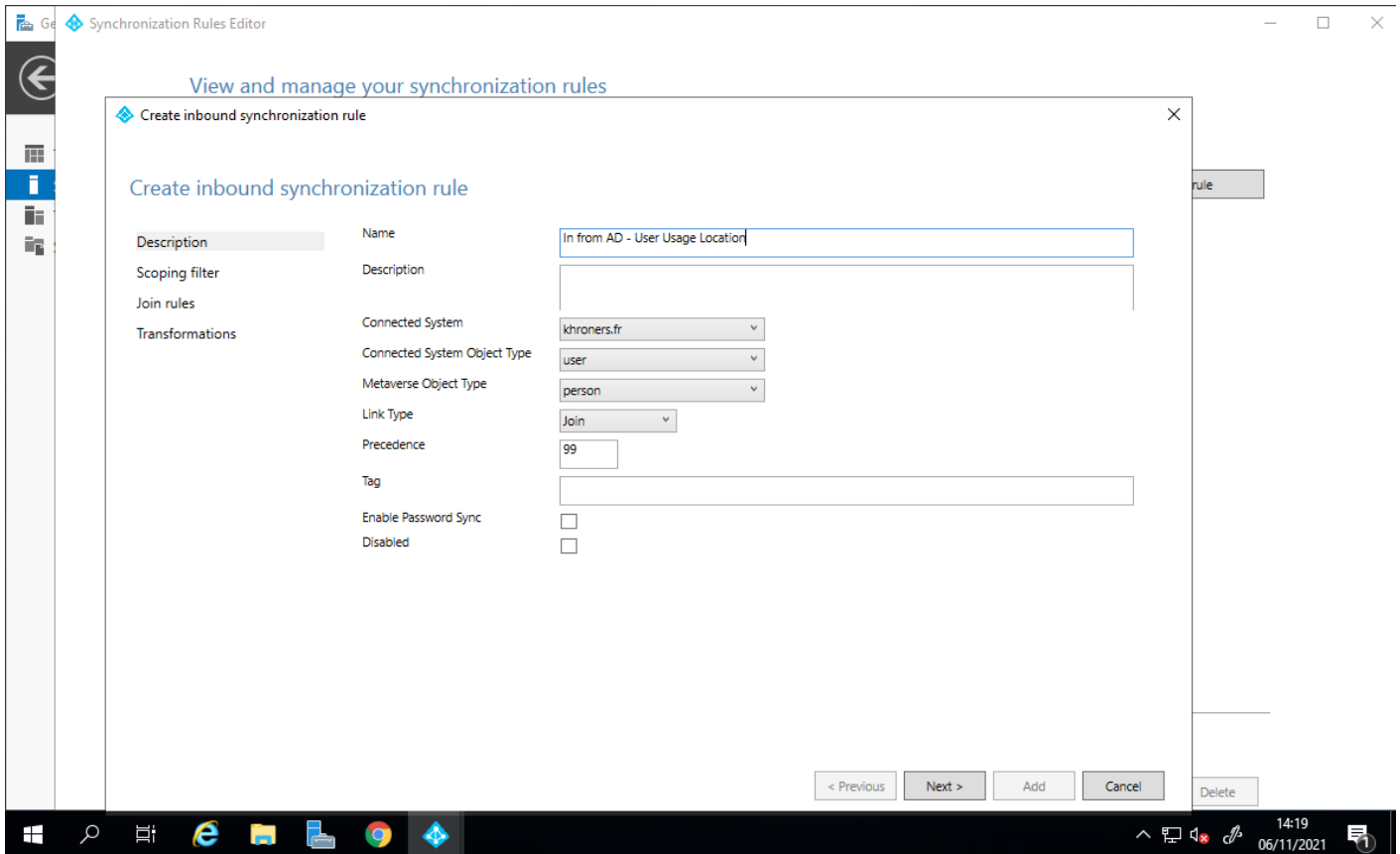
Tests

Via un compte utilisateur, on se rend sur <https://myapps.microsoft.com/lab.khroners.fr> (remplacez le domaine par le votre).

Il est recommandé de substituer la clé de déchiffrement Kerberos du compte d'ordinateur "AZUREADSSO" au moins tous les 30 jours. <https://docs.microsoft.com/fr-fr/azure/active-directory/hybrid/how-to-connect-sso-faq#comment-puis-je-substituer-la-cl--de-d-chiffrement-kerberos-du-compte-d-ordinateur---azureadsso---->

Usage Location

Dans Synchronization Rules Editor, on crée un règle Inbound.



Dans la prochaine page, on clique sur "Suivant". Idem sur la suivante.

View and manage your synchronization rules

Create inbound synchronization rule

Create inbound synchronization rule

- Description
- Scoping filter
- Join rules
- Transformations

Add transformations

FlowType	Target Attribute	Source	Apply Or	Merge Type
Constant	usageLocation	FR	<input type="checkbox"/>	Update

< Add transformation Remove >

< Previous Next > Add Cancel Delete

Hybrid Azure AD Join

<https://www.orbid365.be/hybrid-azure-ad-join-p1/>

<https://docs.microsoft.com/fr-fr/azure/active-directory/devices/hybrid-azuread-join-managed-domains#configure-the-local-intranet-settings-for-device-registration><https://www.orbid365.be/hybrid-azure-ad-join-p1/>

Dans Azure AD Connect, on modifie les options d'appareil et on configure Hybrid Azure AD Joined en ajoutant le SCP. Si on veut faire un déploiement ciblé, on ne configure pas le SCP en cliquant simplement sur suivant. ([Targeted deployments of hybrid Azure AD join - Microsoft Entra | Microsoft Learn](#))

Dans Azure AD Connect, on choisit "Options d'appareils", on active le mode hybride et on ajoute notre SCP pour le domaine.

Il faut également que les appareils soient synchronisés.

Si vous ne synchronisez pas tous les objets automatiquement, mais uniquement des objets membres d'un groupe précis ou placés dans une OU précise, il faut que les PC y soient membres.

Pour le déploiement ciblé : [Targeted deployments of hybrid Azure AD join - Microsoft Entra | Microsoft Learn](#)

Une simple GPO ordinateur comme celle-ci :

RN-FP-O-HybridTargeted

Data collected on: 3/14/2023 8:53:38 PM

[show all](#)

General

[hide](#)

Details

[show](#)

Links

[show](#)

Security Filtering

[show](#)

Delegation

[show](#)

Computer Configuration (Enabled)

[hide](#)

Preferences

[hide](#)

Windows Settings

[hide](#)

Registry

[hide](#)

TenantID (Order: 1)

[hide](#)

General

[hide](#)

Action	Update
Properties	
Hive	HKEY_LOCAL_MACHINE
Key path	SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AAD
Value name	TenantID
Value type	REG_SZ
Value data	8e63

Common

[show](#)

TenantName (Order: 2)

[hide](#)

General

[hide](#)

Action	Update
Properties	
Hive	HKEY_LOCAL_MACHINE
Key path	SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AAD
Value name	TenantName
Value type	REG_SZ
Value data	khroners.fr

On vérifie sur un poste via la commande :

```
dsregcmd /status
```

On peut forcer la jonction via :

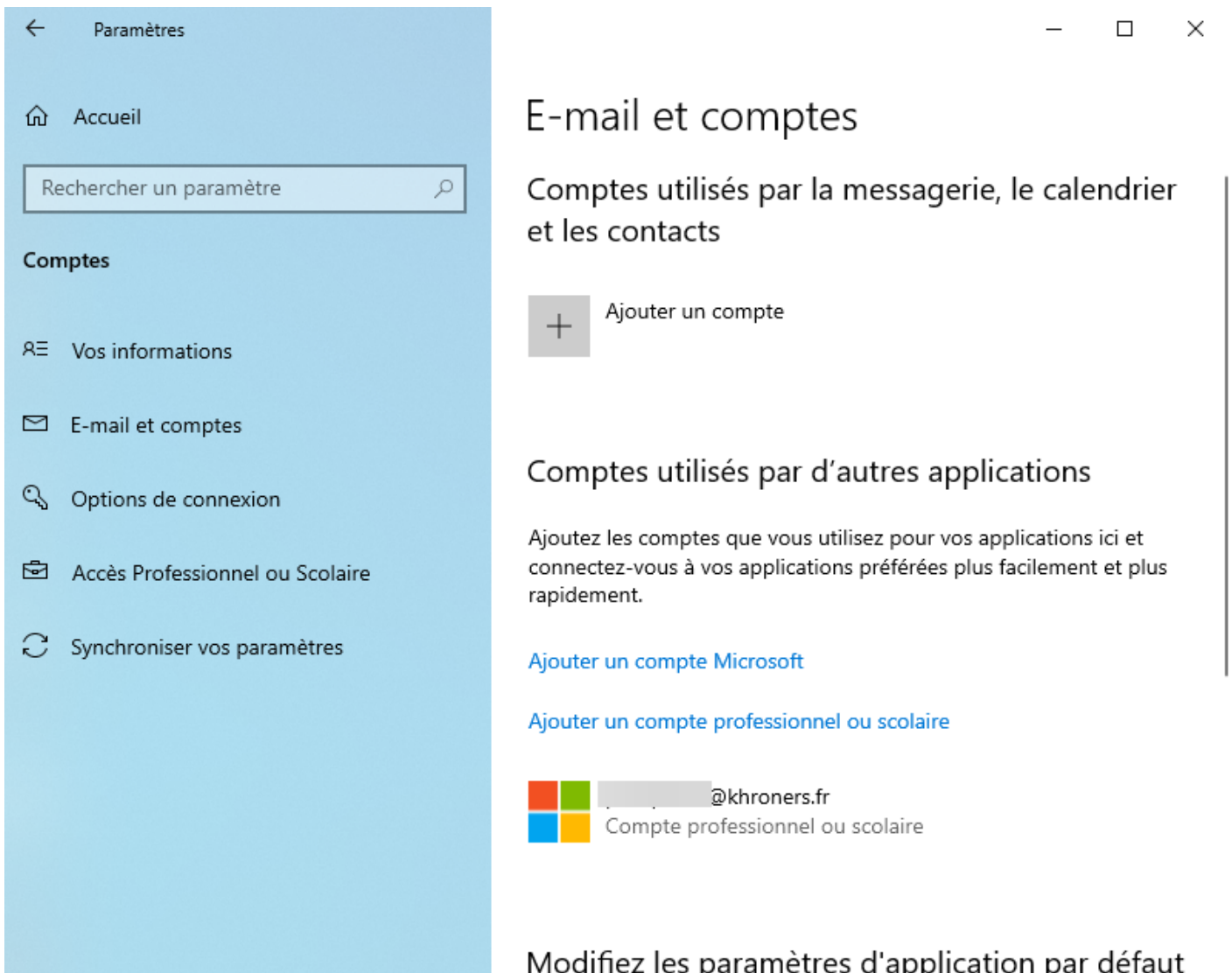
```
dsregcmd /join
```

```
PS C:\Users\Administrateur> dsregcmd /status

+-----+
| Device State |
+-----+

AzureAdJoined : YES
EnterpriseJoined : NO
DomainJoined : YES
DomainName : AD
Device Name : W10-01.ad.khroners.fr
```

Le compte Windows de l'utilisateur s'ajoute automatiquement dans les comptes utilisés par d'autres applications.



L'écran de connexion de l'utilisateur sera différent :



Paul Pierre

... Bienvenue

Activer l'inscription automatique dans Intune

<https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#enable-windows-10-automatic-enrollment>

Dans le cas de PC Hybrid AD Joined, il faut créer une GPO Ordinateur :

RN-FP-O-IntuneEnroll		show all
Data collected on: 3/14/2023 9:40:20 PM		
General		
		hide
Details		show
Links		show
Security Filtering		show
Delegation		show
Computer Configuration (Enabled)		
		hide
Policies		
		hide
Administrative Templates		
		hide
Policy definitions (ADMX files) retrieved from the central store.		
Windows Components/MDM		
		hide
Policy	Setting	Comment
Enable automatic MDM enrollment using default Azure AD credentials	Enabled	
Select Credential Type to Use:		User Credential
MDM Application ID:		
MDM Application ID represents the ID of your MDM application that is configured in Azure AD. This is optional and only required for automatic MDM enrollment using device credentials when multiple MDM applications are configured in Azure AD.		

Inutile de remplir l'ID d'application dans notre cas.

Recréer l'objet Ordinateur AzureADSSOACC

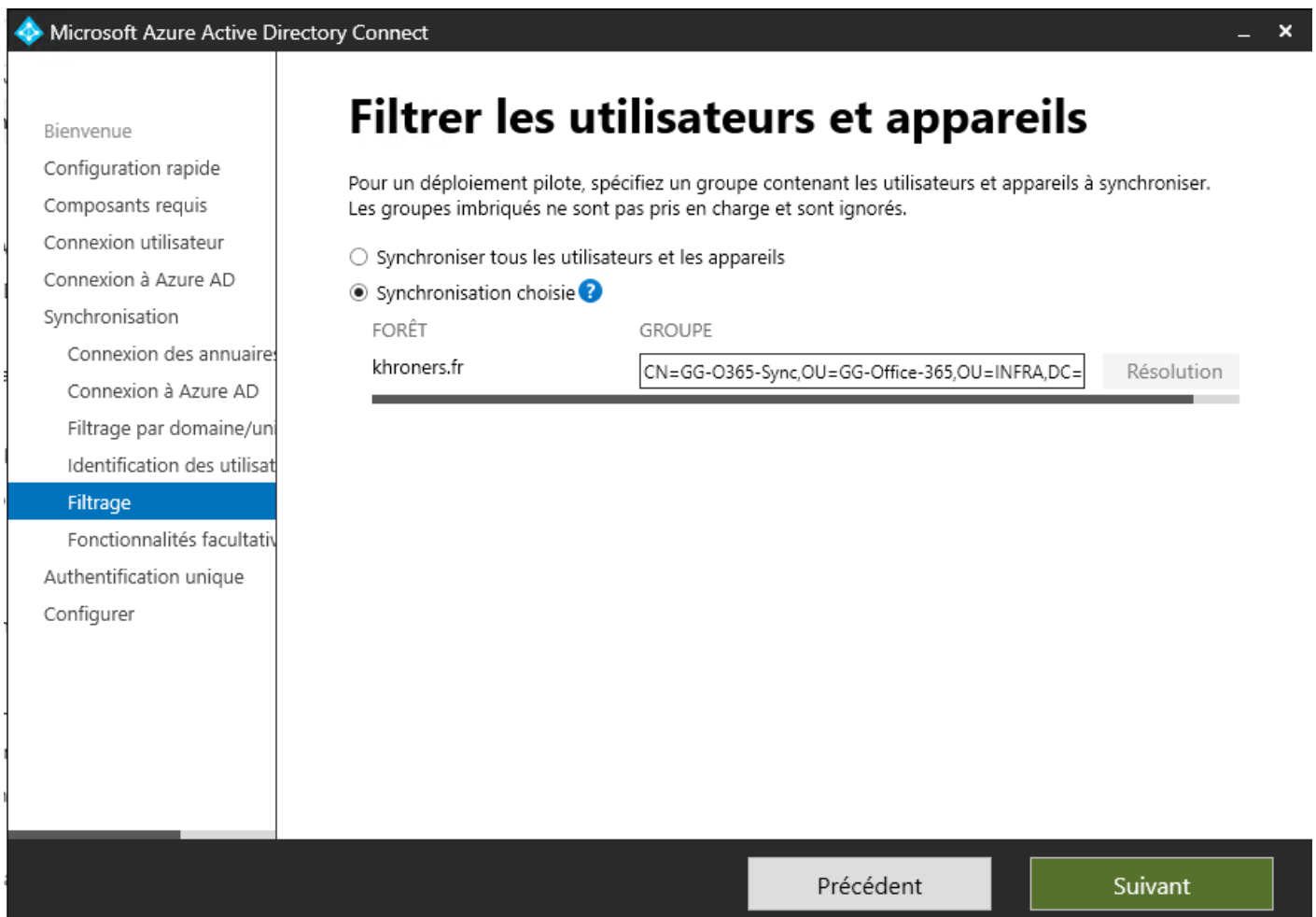
Voici la liste des commandes Powershell à exécuter (une par une) :

```
cd 'C:\Program Files\Microsoft Azure Active Directory Connect\  
Import-Module .\AzureADSSO.psd1  
New-AzureADSSOAuthenticationContext  
Get-AzureADSSOStatus  
Enable-AzureADSSOForest  
Enable-AzureADSSO -Enable $true
```

Synchroniser dans Azure uniquement les membres d'un groupe

Dans les options d'Azure Active Directory Connect (AADC), on peut filtrer par domaine/unité d'organisation ou encore par utilisateurs et appareils.

Pour filtrer avec un groupe, on modifie les options d'AADC et on définit le groupe dont font parti les utilisateurs & appareils à synchroniser.



The screenshot shows the 'Microsoft Azure Active Directory Connect' application window. The left sidebar contains a navigation menu with the following items: Bienvenue, Configuration rapide, Composants requis, Connexion utilisateur, Connexion à Azure AD, Synchronisation, Connexion des annuaires, Connexion à Azure AD, Filtrage par domaine/unité, Identification des utilisateurs, **Filtrage** (highlighted), Fonctionnalités facultatives, Authentification unique, and Configurer. The main content area is titled 'Filtrer les utilisateurs et appareils'. Below the title, there is a descriptive text: 'Pour un déploiement pilote, spécifiez un groupe contenant les utilisateurs et appareils à synchroniser. Les groupes imbriqués ne sont pas pris en charge et sont ignorés.' There are two radio button options: 'Synchroniser tous les utilisateurs et les appareils' (unselected) and 'Synchronisation choisie' (selected). Below these options, there are two input fields: 'FORÊT' with the value 'khroners.fr' and 'GROUPE' with the value 'CN=GG-O365-Sync,OU=GG-Office-365,OU=INFRA,DC='. To the right of the 'GROUPE' field is a 'Résolution' button. At the bottom of the window, there are two buttons: 'Précédent' and 'Suivant'.

Dans mon cas, il se nomme "GG-O365-Sync" (**GG** pour **Groupe Général**, **O365** pour **Office365** et **Sync** pour **Synchronisation**).

Si vous voulez synchroniser un groupe ou un utilisateur, il faudra alors qu'il soit membre du groupe.

Activer la synchronisation des mots de passe entre Azure AD et l'AD local

Dans le cas où un utilisateur change son mot de passe dans **Azure (Office365 par exemple)**, son mot de passe ne sera pas synchroniser dans l'AD local par défaut. Cela est obligatoire (pas techniquement) si vous activez le SSPR (**Réinitialisation autonome du mot de passe**, a.k.a **Mot de passe oublié**)

Pour cela, il existe une fonction à activer dans **Azure Active Directory Connect (AADC)** nommé "**Réécriture du mot de passe**" ou en anglais "**Password Writeback**".

Microsoft Azure Active Directory Connect

Bienvenue

Configuration rapide

Composants requis

Connexion utilisateur

Connexion à Azure AD

Synchronisation

Connexion des annuaires

Connexion à Azure AD

Filtrage par domaine/un

Identification des utilisat

Filtrage

Fonctionnalités facultatives

Extensions d'annuaire

Authentification unique

Configurer

Fonctionnalités facultatives

Sélectionnez la fonctionnalité améliorée que vous souhaitez activer.

- Déploiement Exchange hybride
- Dossiers publics de la messagerie
- Filtrage des applications et des services
- Synchronisation de hachage de mot de passe
- Réécriture du mot de passe
- Écriture différée de groupe
- Réécriture d'appareil
- Synchronisation des attributs des extensions d'annuaire

[En savoir plus](#)

[En savoir plus](#) à propos de la réécriture du mot de passe.

[En savoir plus](#) à propos des fonctionnalités facultatives.

Précédent Suivant

Désormais, un utilisateur qui change son mot de passe dans Office365 verra son mot de passe local changé.

Personnel vs Entreprise, Registered vs Azure AD joined

Personnel

Azure AD joined uniquement

Entreprise

Hybrid joined, Autopiloté ou changé manuellement en entreprise

Azure AD registered

Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.



Alternate actions:

These actions will set up the device as your organization's and give your organization full control over this device.

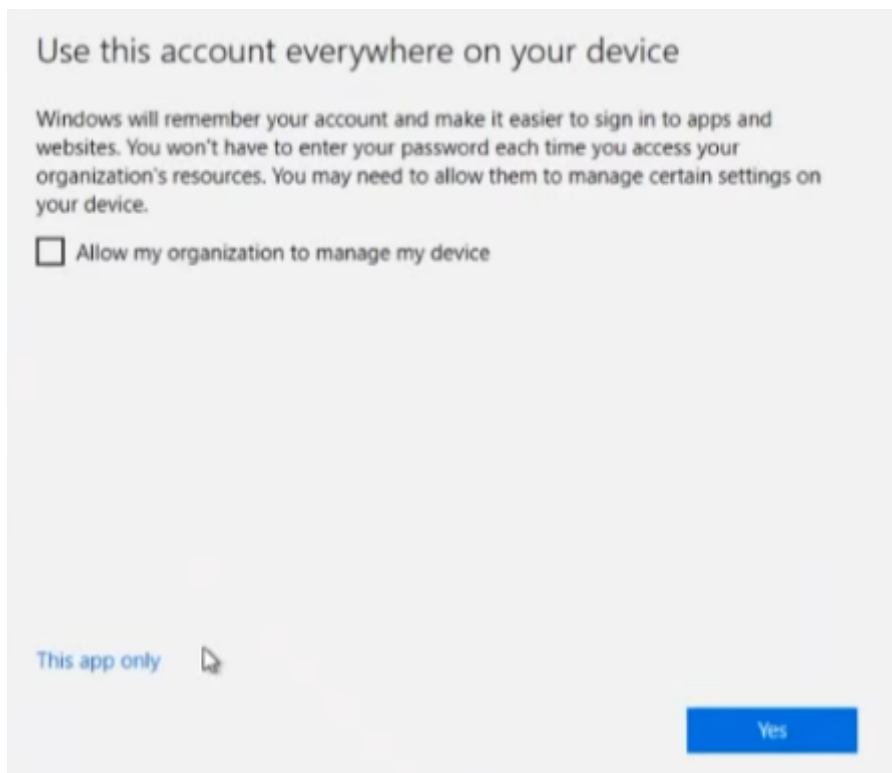
[Join this device to Azure Active Directory](#)

[Join this device to a local Active Directory domain](#)

Next

Sans cliquer sur une des deux options en bas.

ou



Sans cocher. Le compte apparaîtra dans "Accès scolaire ou professionnel". Avec "This app only", il n'apparaîtra pas.

Azure AD Joined

Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.



Alternate actions:

These actions will set up the device as your organization's and give your organization full control over this device.

[Join this device to Azure Active Directory](#)

[Join this device to a local Active Directory domain](#)

Next

En cliquant sur la première option.

Ensuite on nous demande de se connecter au poste avec notre compte Azure AD.

Différences entre l'authentification unique à l'aide d'un jeton d'actualisation principal ou authentification unique fluide (Seamless SSO)

Le Seamless SSO (authentification unique fluide) est utilisé pour les postes uniquement joint au domaine Active Directory local.

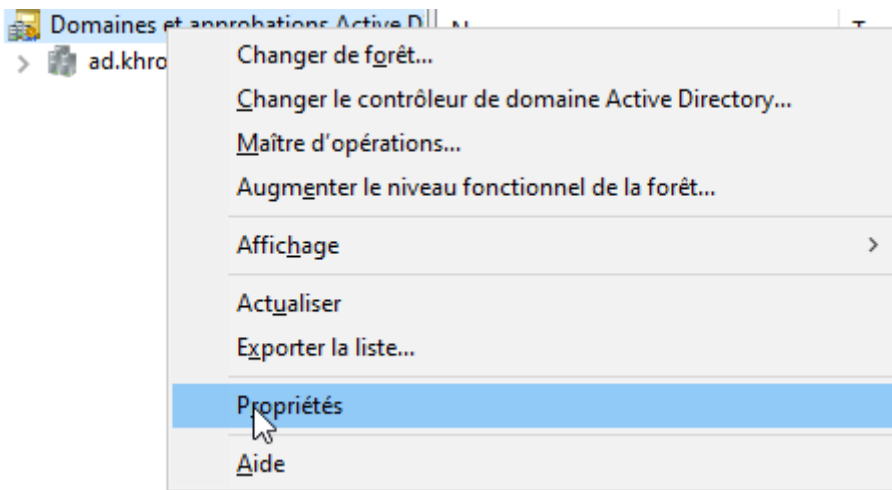
Le SSO via PRT (authentification unique à l'aide d'un jeton d'actualisation principal) est utilisé pour les postes joints Azure AD, Azure AD registered ou Hybrid Azure AD joined ([inscrits via Ajouter un compte professionnel ou scolaire](#)).

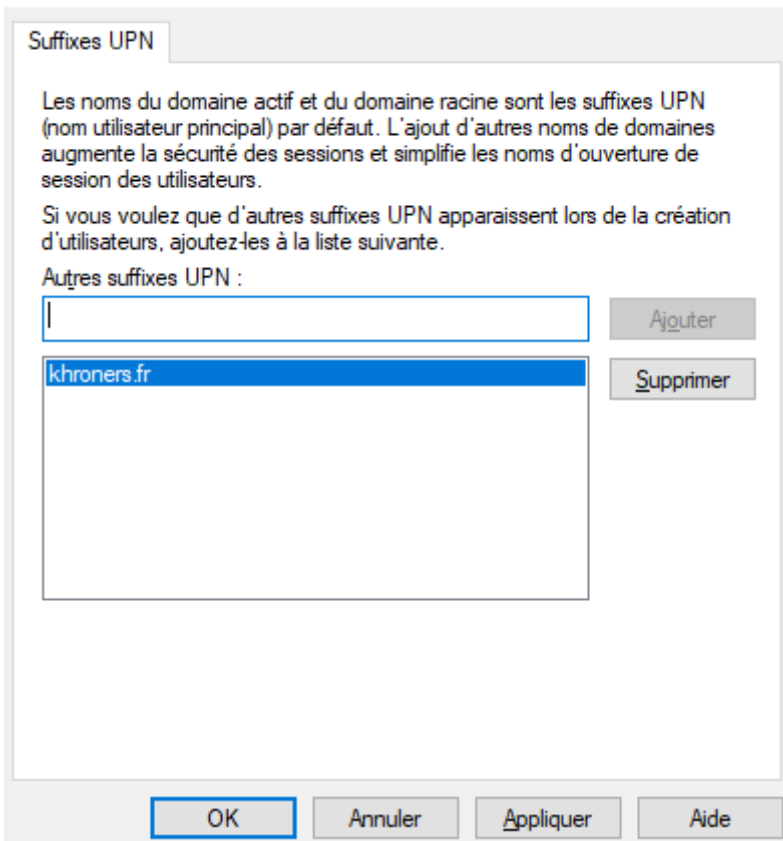
Plus d'informations [ici](#).

Ajouter un suffixe UPN pour la synchronisation Azure AD

Etape 1 : rajouter un suffixe UPN

L'UPN principal de mon AD est ad.khroners.fr. On va rajouter khroners.fr.
Dans "Domaines et approbations Active Directory", :





Etape 2 : modifier l'UPN de tous nos utilisateurs via PowerShell

```
$LocalUsers = Get-ADUser -Filter "UserPrincipalName -like '*ad.khroners.fr'" -Properties userPrincipalName -ResultSetSize $null  
$LocalUsers | foreach {$newUpn =  
$_ .UserPrincipalName.Replace("@ad.khroners.fr","@khroners.fr"); $_ | Set-ADUser -  
UserPrincipalName $newUpn}
```

Pensez à remplacer khroners.fr par votre domaine.

On vérifie :

Nom d'ouverture de session de l'utilisateur :

paul.pierre

@khroners.fr

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

AD\
AD\

paul.pierre

Horaires d'accès...

Se connecter à...

Rester connecté à toutes vos applications



Bienvenue d
Microsoft Ec
le plus perf
Windows

Commençons par vous
de passe, votre historiq
encore à partir du cloud

Connectez-vous p

Commenc

[Déclaration de confidentialité Microsoft](#)

Rester connecté à toutes vos applications

Windows se souviendra de votre compte et vous connectera automatiquement à vos applications et sites web sur cet appareil. Cela permet de réduire le nombre de fois où vous êtes invité à vous connecter.

Autoriser mon organisation à gérer mes appareils

ⓘ Si vous sélectionnez cette option, votre administrateur peut installer des applications, contrôler les paramètres et réinitialiser votre appareil à distance. Votre organisation peut vous demander d'activer cette option pour accéder aux données et applications sur cet appareil.

[Non, se connecter à cette application uniquement](#)

OK

Enterprise State Roaming

Enterprise State Roaming permet de synchroniser les paramètres et les données d'applications sur différents appareils. C'est le cas par défaut pour un compte Microsoft "personnel".

The screenshot shows the Windows Settings application for a user named PC-ALEXIS. The main heading is "Comptes > Sauvegarde Windows". Below the heading, there are four navigation options: "OneDrive Synchronisation", "Liste des applications Sauvegardé", and "Préférences Sauvegardé".

The main content area is divided into several sections:

- Synchronisation du dossier OneDrive:** A section with a blue cloud icon and a button labeled "Gérer les paramètres de synchronisation". The text below reads: "Les dossiers que vous sélectionnez seront protégés et disponibles sur tous vos appareils."
- Se rappeler de mes applications:** A section with a list icon, the text "Accédez rapidement à vos applications sur n'importe quel appareil", and a toggle switch labeled "Activé".
- Mémoriser mes préférences:** A section with a gear icon, the text "Vos dossiers OneDrive sont accessibles sur tous vos appareils", and a toggle switch labeled "Activé".
- Checklist of items to sync:** Three items are listed with checkmarks: "Mots de passe", "Préférences linguistiques", and "Autres paramètres Windows".
- Aide pour la sauvegarde Windows:** A section with a globe icon and an upward arrow.
- Additional links:** Two links are listed at the bottom: "Résolution des problèmes de synchronisation OneDrive" and "Synchronisation des favoris Microsoft Edge".



Appareils | Enterprise State Roaming ...


khroners - Azure Active Directory





Enregistrer




Ignorer


 Vue d'ensemble

 Tous les appareils


 Paramètres de l'appareil


 Enterprise State Roaming

 Clés BitLocker (préversion)


 Diagnostiquer et résoudre les problèmes


Activité

 Journaux d'audit

 Résultats de l'opération en bloc (préversion)

Dépannage + support

 Nouvelle demande de support

Les utilisateurs peuvent synchroniser les paramètres et les données d'application sur différents appareils 

Tout

Sélectionné

Aucun

Sélectionné

Aucun membre sélectionné

Ajouter un administrateur local d'appareils joints à Azure AD (AAD Joined)

Dans le portail d'Azure, on se rend dans "Appareils" puis "Paramètres de l'appareil".

The screenshot shows the Azure portal interface for device management. The page title is "Appareils | Paramètres de l'appareil" with a subtitle "khroners - Azure Active Directory". On the left, a navigation menu includes "Vue d'ensemble", "Tous les appareils", "Paramètres de l'appareil" (highlighted), "Enterprise State Roaming", "Clés BitLocker (préversion)", and "Diagnostiquer et résoudre les problèmes". The main content area features a back arrow, action buttons for "Enregistrer", "Ignorer", and "Des commentaires?", and two sections for user permissions. The first section, "Les utilisateurs peuvent joindre des appareils à Azure AD", has a filter bar with "Tout" (selected), "Sélectionné", and "Aucun", and a status of "Sélectionné" with "Aucun membre sélectionné". The second section, "Les utilisateurs peuvent inscrire leurs appareils sur Azure AD", has a filter bar with "Tout" (selected) and "Aucun", and no status text.

Les utilisateurs peuvent joindre des appareils à Azure AD ⓘ

Tout Sélectionné Aucun

Sélectionné

Aucun membre sélectionné

Les utilisateurs peuvent inscrire leurs appareils sur Azure AD ⓘ

Tout Aucun

i En savoir plus sur le fonctionnement de ce paramètre

Exiger l'authentification multifacteur pour inscrire ou joindre des appareils avec Azure AD ⓘ

Oui Non

⚠ Nous vous recommandons d'exiger l'authentification multifacteur pour inscrire ou joindre des appareils avec Azure AD à l'aide de l'[accès conditionnel](#). Définissez ce paramètre d'appareil sur Non si vous avez besoin d'utiliser l'authentification multifacteur avec l'accès conditionnel.

Nombre maximal d'appareils par utilisateur ⓘ

50

Administrateurs locaux supplémentaires sur tous les appareils joints à Azure AD

[Gérer Administrateurs locaux supplémentaires sur tous les appareils joints à Azure AD](#)

On y ajoute un utilisateur.



Device Administrators | Affectations ...

Tous les rôles

✖ Diagnostiquer et résoudre les problèmes



Ajouter des affectations



Supprimer les attributions



Télécharger les a

Limiter le nombre d'appareils par utilisateur

Dans le portail d'Azure, on clique sur "Appareils" puis "Paramètres de l'appareil".

Appareils | Paramètres de l'appareil ...
khroners - Azure Active Directory

« Enregistrer Ignorer | Des commentaires ?

- Vue d'ensemble
- Tous les appareils
- Paramètres de l'appareil**
- Enterprise State Roaming
- Clés BitLocker (préversion)
- Diagnostiquer et résoudre les problèmes

Les utilisateurs peuvent joindre des appareils à Azure AD ⓘ

Tout Sélectionné Aucun

Sélectionné
Aucun membre sélectionné

Les utilisateurs peuvent inscrire leurs appareils sur Azure AD ⓘ

Tout Aucun

On limite le nombre en bas.

Nombre maximal d'appareils par utilisateur ⓘ

Supprimer un groupe orphelin issu d'un domaine local

En cas de groupe synchronisé depuis un domaine Active Directory local qui n'est plus disponible, il est nécessaire de passer par PowerShell pour le supprimer. On remplace "**DisplayName**" par le nom du groupe à supprimer.

```
Install-Module -Name MSOnline  
Connect-MsolService  
Get-MsolGroup  
Get-MsolGroup -SearchString "DisplayName" | Remove-MsolGroup
```

Empêcher les utilisateurs de joindre leur PC à Entra ID (Azure AD)

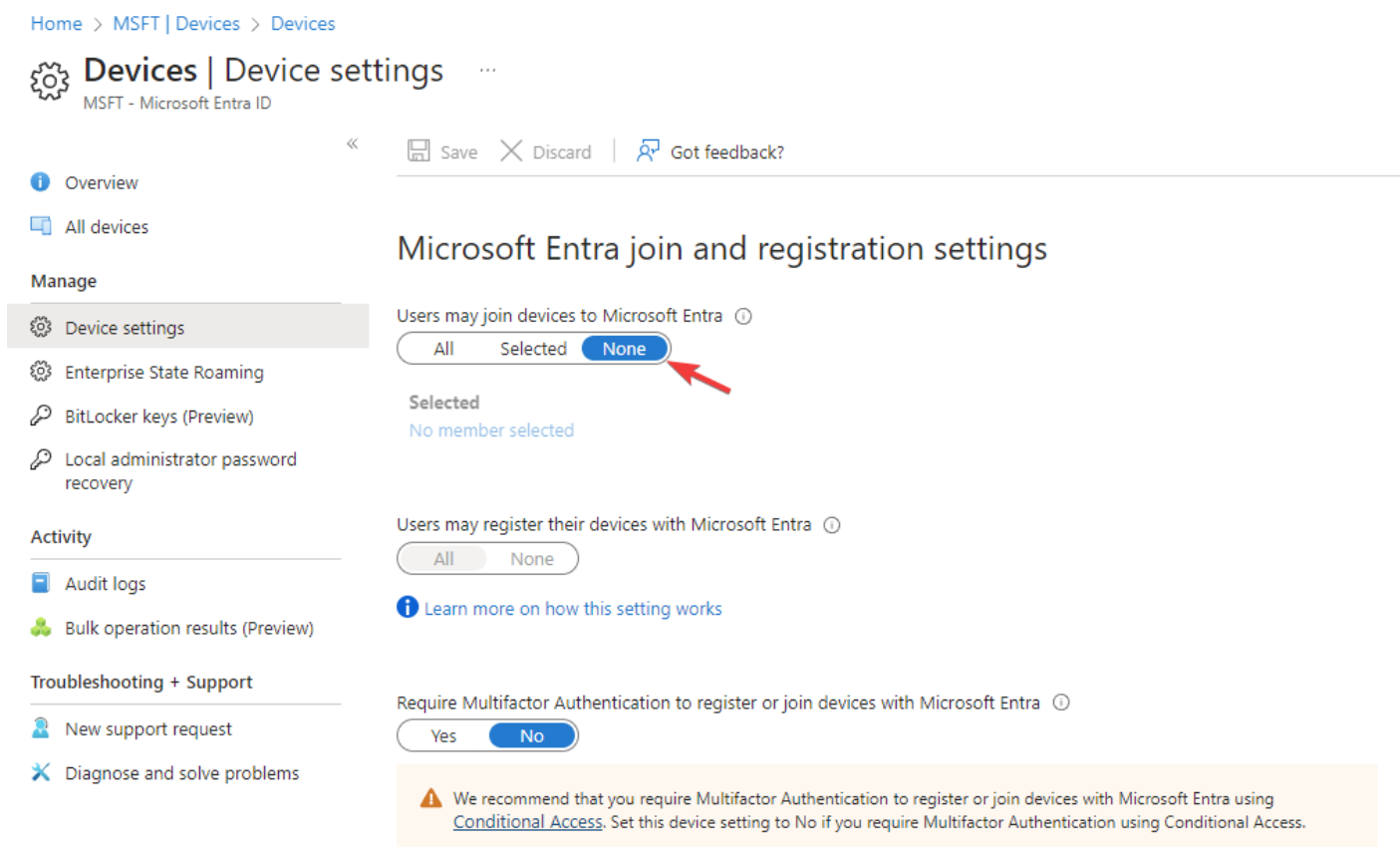
Pour empêcher les utilisateurs de joindre leur PC à Entra ID (Azure AD joined),

On se rend sur cette page :

https://portal.azure.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/_/DeviceSettings/menuld~/null

On choisit "None" ou "Aucun" en français.

On peut également choisir un groupe d'utilisateurs.



Home > MSFT | Devices > Devices

Devices | Device settings ...
MSFT - Microsoft Entra ID

« Save Discard Got feedback?

Overview
All devices

Manage

- Device settings
- Enterprise State Roaming
- BitLocker keys (Preview)
- Local administrator password recovery

Activity

- Audit logs
- Bulk operation results (Preview)

Troubleshooting + Support

- New support request
- Diagnose and solve problems

Microsoft Entra join and registration settings

Users may join devices to Microsoft Entra ⓘ

All Selected **None**

Selected
No member selected

Users may register their devices with Microsoft Entra ⓘ

All None

Learn more on how this setting works

Require Multifactor Authentication to register or join devices with Microsoft Entra ⓘ

Yes **No**

⚠ We recommend that you require Multifactor Authentication to register or join devices with Microsoft Entra using [Conditional Access](#). Set this device setting to No if you require Multifactor Authentication using Conditional Access.