

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](#).

Microsoft Azure Active Directory Connect

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 ?

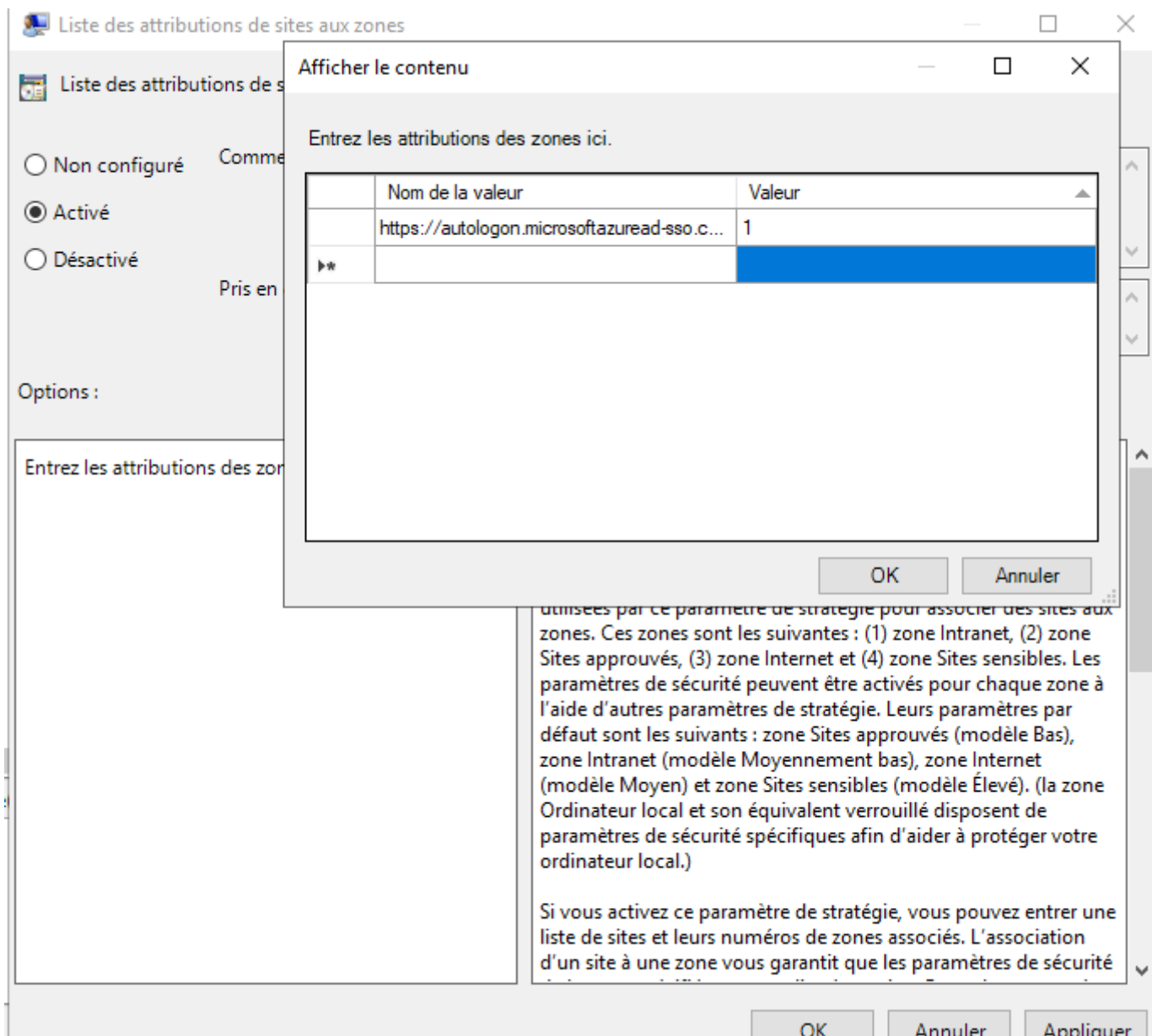
Précédent

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-sso.com` .



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

On ajoute aussi :

BZH-FP-U-HybridAzureADJoin

Étendue Détails Paramètres Délégation

Délégation

[afficher](#)

Configuration ordinateur (activée)

[masquer](#)

Aucun paramètre n'est défini.

Configuration utilisateur (activée)

[masquer](#)

Stratégies

[masquer](#)

Modèles d'administration

[masquer](#)

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Composants Windows/Internet Explorer/Panneau de configuration Internet/Onglet Sécurité/Zone intranet

Stratégie

Paramètre

Commentaire

Autoriser 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--->

Revision #9

Created 6 June 2021 21:26:52 by Khroners

Updated 29 October 2023 13:24:43 by Khroners