Comment archiver des e-mails de Microsoft 365 (Authentification moderne) ?

Philippe - 2021-02-11 - Mailstore

Avant d'archiver les boîtes aux lettres Microsoft 365, il est nécessaire d'enregistrer MailStore Server auprès de votre console Microsoft 365.

Il est également fortement recommandé de synchroniser les utilisateurs du serveur MailStore directement avec celui-ci (Azure AD) pour récupérer toutes les informations pertinentes pour l'archivage, telles que les adresses électroniques.

Connexion du serveur MailStore et de Microsoft 365

Afin de synchroniser les informations des utilisateurs de Microsoft 365, le serveur MailStore doit être connecté à votre console Microsoft 365 et avoir reçu les autorisations nécessaires.

Microsoft 365 s'appuie sur Azure Active Directory comme service d'annuaire. Chaque Tenant de Microsoft 365 correspond à un Tenant d'Azure AD qui stocke ses informations utilisateur.

Enregistrement du serveur MailStore en tant qu'application dans Azure AD

Grâce à l'enregistrement, MailStore Server obtient une identité dans Azure AD qui permet de s'authentifier auprès des services du Tenant et d'utiliser leurs ressources.

■ Connectez-vous au portail Azure en tant qu'administrateur global de votre Tenant Microsoft 365.
■ Dans le menu de navigation (☰), sélectionnez l'option Azure Active Directory.
■ Sur la page suivante, sélectionnez Inscriptions d'applications dans la section **Gérer** du menu de navigation de gauche.
■ Sélectionnez + Nouvelle inscription.
■ Dans le champ Nom, entrez un nom d'affichage significatif, par exemple MailStore Server. Ce nom sera affiché aux utilisateurs lors de la connexion ultérieure, par exemple.
■ Laissez tous les autres paramètres de cette page à leurs valeurs par défaut.
■ Cliquez sur "S'inscrire". Si l'enregistrement a réussi, la page d'aperçu de l'application

nouvellement enregistrée s'affiche.

L'ID de l'application (client) indiqué sur cette page identifie le serveur MailStore de votre Tenant Azure AD et doit être copié dans le serveur MailStore ensuite, avec l'ID du répertoire (Tenant).

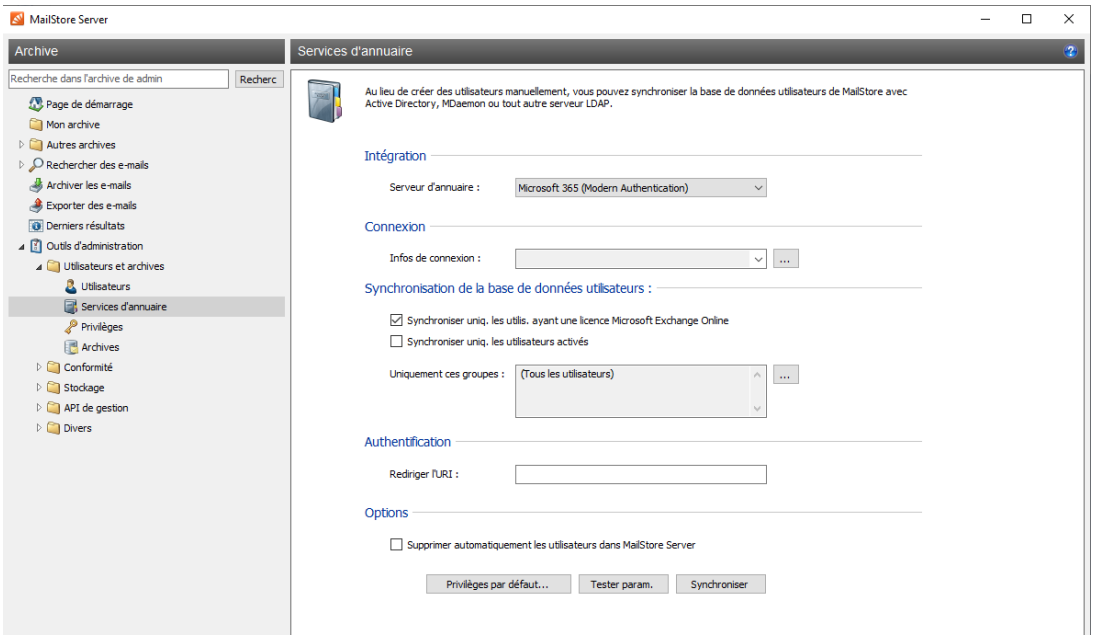
Par conséquent, pour les étapes suivantes, laissez la page d'aperçu ouverte dans votre navigateur web.

Création de références dans le serveur MailStore

Les références pour Microsoft 365 sont constituées des identifiants mentionnés ci-dessus et d'un secret que MailStore Server utilise pour prouver son identité à Azure AD.

Microsoft recommande d'utiliser les certificats comme secrets pour identifier les applications dans Azure AD. Lors de la création des identifiants, un tel certificat est généré automatiquement par MailStore Server mais peut également être recréé ultérieurement.

■ Connectez-vous au client MailStore en tant qu'administrateur du serveur MailStore.
■ Cliquez sur Outils d'administration > Utilisateurs et archives > Services d'annuaire.
■ Dans la section Intégration, changez le type de service d'annuaire en Microsoft 365 (Modern Authentication).



■ Dans la section Infos de Connexion, cliquez sur le bouton (...)

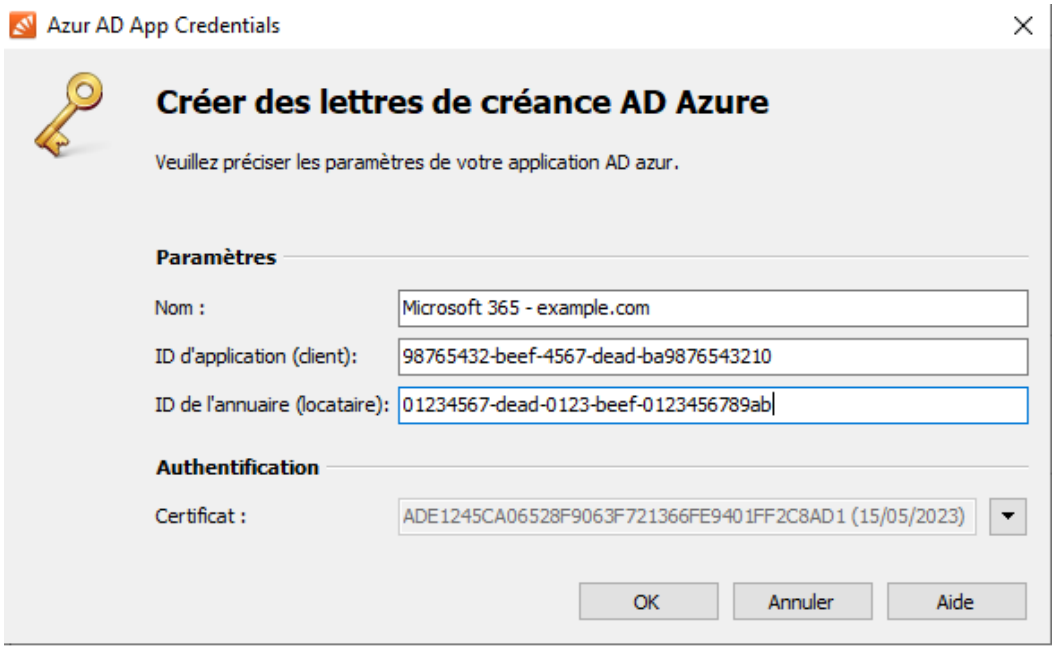
■ Dans le gestionnaire des titres de compétences qui apparaît, cliquez sur Créer...

■ Dans le dialogue Azure AD App Credentials, entrez les informations suivantes dans la section Paramètres :

■ Nom
Un nom d'affichage significatif pour les références, par exemple le nom de votre tenant Microsoft 365.

■ ID d'application (client)
La valeur du champ correspondant que vous pouvez copier à partir de la page de présentation de l'application Azure AD dans votre navigateur web.

■ ID de l'annuaire (locataire)
La valeur du champ correspondant que vous pouvez copier à partir de la page de présentation de l'application Azure AD dans votre navigateur web.



■ Dans la section Authentification, cliquez sur le bouton déroulant à côté de la zone de texte du certificat et sélectionnez Télécharger le certificat. Enregistrez le certificat sur votre disque dur.

■ Confirmez vos entrées en cliquant sur OK.

■ Les nouveaux certificats créés sont répertoriés dans le gestionnaire de certificats sous

le nom que vous avez saisi avec le type Microsoft 365. Vous pouvez également y modifier ou supprimer des références existantes si nécessaire.

■ Quittez le Azur AD App Credentials en cliquant sur la croix

■ Les nouveaux justificatifs d'identité sont sélectionnés par défaut dans la liste déroulante correspondante.

Publication des "Credentails" sur Azure AD

Pour que Azure AD puisse valider l'identité du serveur MailStore, le certificat créé doit être publié dans Azure AD.

- Sélectionnez votre application "Mailstore" dans Applications détenues dans Inscriptions d'applications.

- Sélectionnez Certificats & secrets dans la section Gérer du menu de navigation de gauche.

- Cliquez sur Télécharger le certificat dans la section Certificats. Sélectionnez le fichier de certificat que vous avez sauvegardé précédemment et téléchargez-le dans Azure AD en cliquant sur Ajouter.

- Si le téléchargement a réussi, l'empreinte du certificat ainsi que ses dates de début et d'expiration apparaissent dans la liste des certificats.
Vous pouvez comparer l'empreinte et la date d'expiration avec celles qui figurent dans le gestionnaire de certificats de MailStore pour vérifier que vous avez téléchargé le bon certificat.

Configuration de l'authentification des applications dans Azurz AD

Pour qu'Azure AD renvoie le résultat de la demande d'authentification d'un utilisateur au serveur MailStore, le point final où le serveur MailStore attend des réponses d'authentification, appelé URI de redirection, doit être transmis à Azure AD.

Dans le portail Azure , sélectionnez Authentification dans la section Gérer du menu de navigation de gauche.
Cliquez sur le bouton Ajouter une plate-forme .

Sélectionnez Web dans la section Applications Web de la page du menu Configurer des plates-formes.

Dans le champ Redirect URI, entrez un URI au format (sans crochets)

https://<fqdn>[:<port>]/oidc/signin

Avec les éléments suivants :

https://

La spécification du protocole https:// est obligatoire. Pour éviter les avertissements du certificat lors de la connexion de l'utilisateur, les navigateurs web des machines clientes doivent faire confiance au certificat utilisé par le serveur MailStore.

FQDN

Le nom de domaine pleinement qualifié (FQDN) de votre serveur MailStore qui se compose du nom de la machine et du domaine DNS, par exemple mailstore.example.com. Ce nom doit pouvoir être résolu par tous les clients à partir desquels les utilisateurs pourront se connecter au serveur MailStore.

Port

Le port TCP du MailStore Web Access (8462 par défaut). Cette valeur doit être égale au port configuré dans la section Configuration de base > Paramètres réseau > MailStore Web Access / Outlook Add-in (HTTPS) de la configuration du service MailStore Server.

Le port TCP ne doit être spécifié que s'il est différent du port par défaut du protocole HTTPS (443).

/oidc/signin

Le point d'extrémité où le serveur MailStore attend les réponses d'authentification d'Azure AD. Ce chemin doit être spécifié exactement comme indiqué ici à la fin de l'URI de redirection.

Examples d'URIs de redirection valide

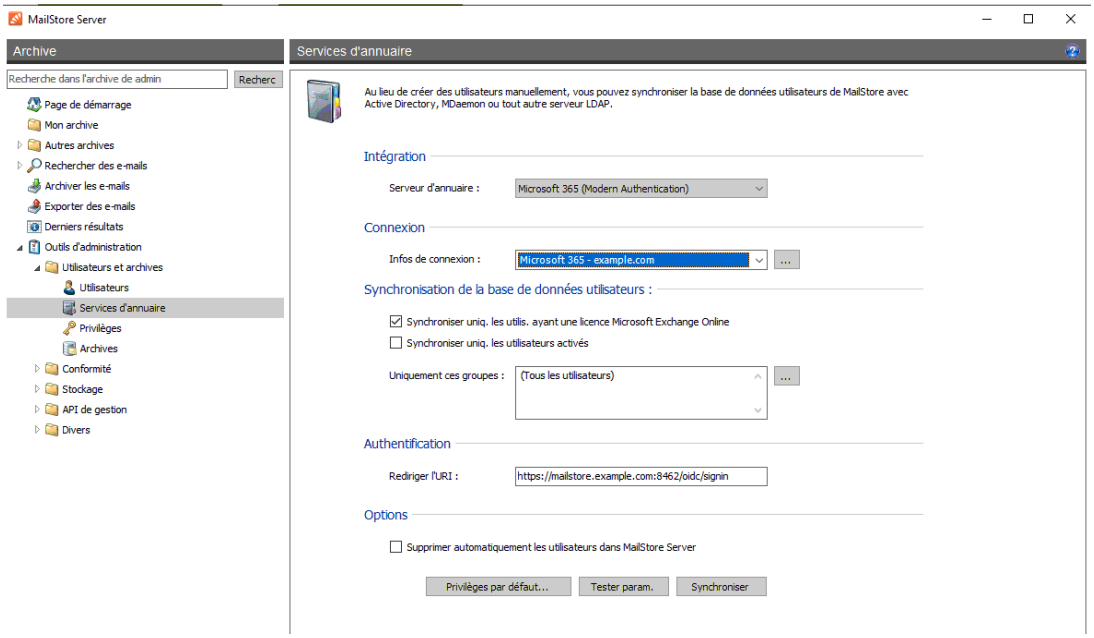
Nom de la Machine	DNS Domain	TCP Port	Resulting Redirect URI
mailstore	example.com	8462	`https://mailstore.example.com:8462/oidc/signin`
mailstore	example.com	443	`https://mailstore.example.com/oidc/signin` Le port peut être omis si le port par défaut HTTPS 443 a été configuré pour l'accès Web au MailStore ou comme port source d'une redirection de port sur le pare-feu ou le routeur..

- Laissez le champ URL de déconnexion du canal avant vide.
- Activez l'option Jetons d'ID (utilisés pour les flux implicites et hybrides)
- Cliquez sur Configurer pour terminer la configuration de l'authentification de l'application dans Azure AD.

Configuration de l'URI de redirection dans le serveur MailStore

Pour que le serveur MailStore puisse transmettre l'URI de redirection aux clients demandeurs, il doit être configuré à cet endroit également.

■ Connectez-vous au client MailStore en tant qu'administrateur du serveur MailStore.
■ Cliquez sur Outils d'administration > Utilisateurs et archives > Services d'annuaire.
■ Saisissez l'URI de redirection dans le champ correspondant de la section Authentification. Copiez simplement la valeur précédemment configurée dans Azure AD.



Configurer les autorisations API sur Azure AD

■ Sur votre console Azure AD, sélectionnez API autorisées dans la section Gérer du menu de navigation de gauche.
■ Cliquez sur le bouton Ajouter une autorisation dans la section Autorisations configurées.

■ Sur la page de menu Demander des autorisations API, sélectionnez l'API Microsoft Graph dans la section API Microsoft couramment utilisées.

■ Sélectionnez l'option autorisations des applications.

■ Activez l'autorisation Directory > Directory.Read.All

■ Cliquez sur Ajouter des autorisations.

■ Les autorisations sont mises à jour et l'autorisation Directory.Read.All apparaît dans la liste des autorisations de l'API sous Microsoft Graph.

■ Cliquez à nouveau sur le bouton Ajouter une autorisation dans la section Autorisations configurées.

■ Sur la page de menu Demander les autorisations API, sélectionnez API utilisée par mon organisation.

■ Recherchez Office 365 Exchange Online et cliquez sur l'entrée correspondante.

■ Sélectionnez l'option autorisations des applications.

■ Activez la permission full_access_as_app.

■ Cliquez sur Ajouter des autorisations.

■ Les autorisations sont mises à jour et l'autorisation full_access_as_app apparaît dans la liste des autorisations API sous Exchange Online.

■ Cliquez maintenant sur le bouton Accorder un consentement d'administrateur pour <votre nom de societé> dans la section Autorisations configurées.

■ Accusez réception de l'avis suivant en cliquant sur Oui.

■ Le statut de toutes les autorisations accordées est mis à jour et devient Accorder pour <votre nom de societé>.

La configuration de la connexion du serveur MailStore à Microsoft 365 dans Azure AD est maintenant terminée.

Vous pouvez vous déconnecter de votre Tenant Azure AD et fermer la fenêtre du navigateur.