Configuration des paramètres de compte de messagerie sécurisée Cisco pour l'API Microsoft Azure (Microsoft 365)

Table des matières

- Introduction
  - Flux du processus de résolution automatique des boîtes aux lettres
- Conditions préalables
- Enregistrer une application Azure pour l'utiliser avec la messagerie sécurisée Cisco
  - Enregistrement des applications
  - Certificats et secrets
  - Autorisations API
  - Obtention de votre ID client et de votre ID locataire
- Configuration de votre passerelle de messagerie sécurisée/passerelle cloud Cisco
  - Créer un profil de compte
  - Vérifier la connexion
  - Activer la correction automatique des boîtes aux lettres (MAR) pour la protection avancée contre les programmes malveillants dans la stratégie de messagerie
  - Activer la correction automatique des boîtes aux lettres (MAR) pour le filtrage des URL
- Exemples de rapports de correction automatique de boîte aux lettres
- Journalisation de la résolution automatique des boîtes aux lettres
- Dépannage de la passerelle de messagerie sécurisée Cisco
- Dépannage d'Azure AD
- Annexe A
  - Création d'une paire de clés et de certificats publics et privés
    - Certificat : Unix/Linux (avec openssl)
    - Certificat : Windows (utilisation de PowerShell)
- Annexe B
  - Autorisations API (AsyncOS 11.x, 12.x)
- Informations connexes

Introduction

Ce document fournit une procédure pas à pas pour l'enregistrement d'une nouvelle application dans Microsoft Azure (Azure Active Directory) afin de générer l'ID client, l'ID du locataire et les informations d'identification du client nécessaires, puis la configuration des paramètres de compte sur une passerelle de messagerie sécurisée Cisco ou une passerelle cloud. La configuration des paramètres de compte et du profil de compte associé est requise lorsqu'un administrateur de messagerie configure Mailbox Auto Remediation (MAR) pour Advanced Malware Protection (AMP) ou le filtrage des URL, ou lorsqu'il utilise l'action Remediate de Message Tracking sur

Cisco Secure Email and Web Manager ou Cisco Secure Gateway/Cloud Gateway.

Flux du processus de résolution automatique des boîtes aux lettres

Une pièce jointe (fichier) dans votre e-mail ou une URL peut être considérée comme malveillante à tout moment, même après avoir atteint la boîte de messagerie d'un utilisateur. AMP sur Cisco Secure Email (via Cisco Secure Malware Analytics) peut identifier ce développement à mesure que de nouvelles informations apparaissent et enverra des alertes rétrospectives à Cisco Secure Email. Cisco Talos offre les mêmes fonctionnalités d'analyse d'URL qu'AsyncOS 14.2 pour Cisco Secure Email Cloud Gateway. Si votre entreprise utilise Microsoft 365 pour gérer les boîtes aux lettres, vous pouvez configurer Cisco Secure Email pour exécuter des actions de correction automatique sur les messages de la boîte aux lettres d'un utilisateur lorsque ces verdicts de menace changent.

Cisco Secure Email communique directement et en toute sécurité avec Microsoft Azure Active Directory pour accéder aux boîtes aux lettres Microsoft 365. Par exemple, si un e-mail avec une pièce jointe est traité via votre passerelle et analysé par AMP, la pièce jointe (SHA256) est fournie à AMP pour la réputation des fichiers. La disposition AMP peut être marquée comme propre (étape 5, Figure 1), puis remise à la boîte aux lettres Microsoft 365 du destinataire final. Par la suite, lorsque la disposition AMP devient Malveillante, Cisco Malware Analytics envoie une mise à jour de verdict rétrospective (étape 8, Figure 1) à toute passerelle ayant traité ce SHA256 spécifique. Une fois que la passerelle reçoit la mise à jour de verdict rétrospective de Malveillante (si elle est configurée), elle effectue l'une des actions de correction automatique de boîte aux lettres suivantes : Transférer, Supprimer ou Transférer et supprimer.

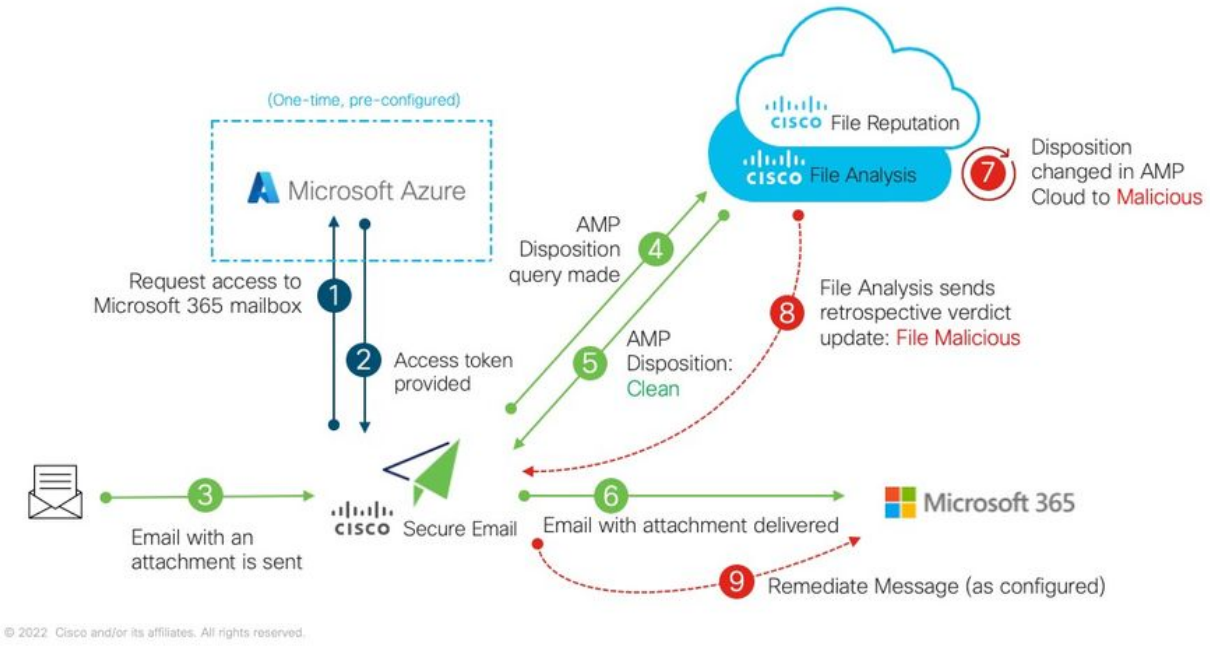


Figure 1 : MAR (pour AMP) sur Cisco Secure Email

Ce guide explique comment configurer la messagerie sécurisée Cisco avec Microsoft 365 pour la correction automatique des boîtes aux lettres uniquement. AMP (File Reputation and File Analysis) et/ou le filtrage des URL sur la passerelle doivent déjà être configurés. Pour plus de détails sur la File Reputation et l'analyse de fichiers, veuillez consulter le Guide de l'utilisateur pour la version d'AsyncOS que vous avez déployée.

Conditions préalables

1. Abonnement à un compte Microsoft 365 (Vérifiez que votre abonnement à un compte Microsoft 365 inclut l'accès à Exchange, tel qu'un compte Enterprise E3 ou Enterprise E5.)

2. Compte administrateur Microsoft Azure et accès à http://portal.azure.com

3. Les comptes Microsoft 365 et Microsoft Azure AD sont correctement liés à une adresse e-mail « user@domain.com » active et vous pouvez envoyer et recevoir des e-mails via cette adresse.

Vous allez créer les valeurs suivantes afin de configurer la communication de l'API de la passerelle de messagerie sécurisée Cisco à Microsoft Azure AD :

- ID client
- ID du locataire
- Secret client

Remarque : à partir d'AsyncOS 14.0, les paramètres de compte permettent la configuration à l'aide d'un secret client lors de la création de l'inscription de l'application Microsoft Azure. C'est la méthode la plus facile et la plus préférée.

Facultatif - Si vous n'utilisez PAS le secret client, vous devez créer et disposer des éléments suivants :

- Empreinte
- La clé privée (fichier PEM)

La création de l'empreinte numérique et de la clé privée est traitée dans l'annexe du présent guide :

1. Un certificat public (ou privé) actif (CER) et la clé privée utilisée pour signer le certificat (PEM), ou la possibilité de créer un certificat public (CER) et la possibilité d'enregistrer la clé privée utilisée pour signer le certificat (PEM). Cisco propose deux méthodes dans ce document pour effectuer cette opération en fonction de vos préférences d'administration :
    1. Certificat : Unix/Linux/OS X (utilisant OpenSSL)
    2. Certificat : Windows (utilisation de PowerShell)

2. Accès à Windows PowerShell, généralement administré à partir d'un hôte ou d'un serveur

Windows - ou - accès à l'application Terminal via Unix/Linux

Afin de créer ces valeurs requises, vous devrez suivre les étapes fournies dans ce document.

Enregistrer une application Azure pour l'utiliser avec la messagerie sécurisée Cisco

Enregistrement des applications

Connectez-vous à votre portail Microsoft Azure

1. Cliquez sur Azure Active Directory (Figure 2)

2. Cliquez sur Inscriptions d'applications

3. Cliquez sur + Nouvelle inscription

4. Sur la page <<Enregistrer une demande>> :

    a. Nom : Cisco Secure Email MAR (ou le nom de votre choix)
    b. Types de comptes pris en charge : comptes de ce répertoire d'organisation uniquement (Nom du compte)
    c. URI de redirection : (facultatif)

    [Remarque : vous pouvez laisser ce champ vide ou utiliser https://www.cisco.com/sign-on pour le compléter]
    d. Au bas de la page, cliquez sur Register

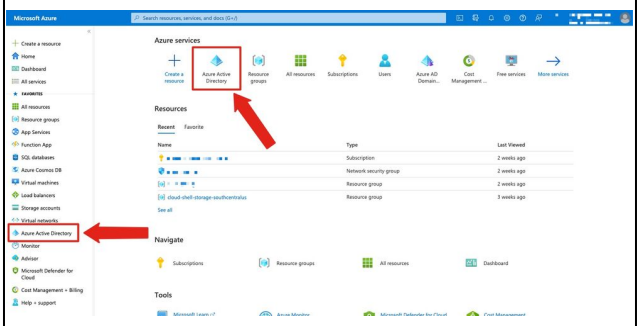


Figure 2 : exemple de portail Microsoft Azure

Une fois que vous aurez terminé les étapes ci-dessus, votre demande vous sera présentée :

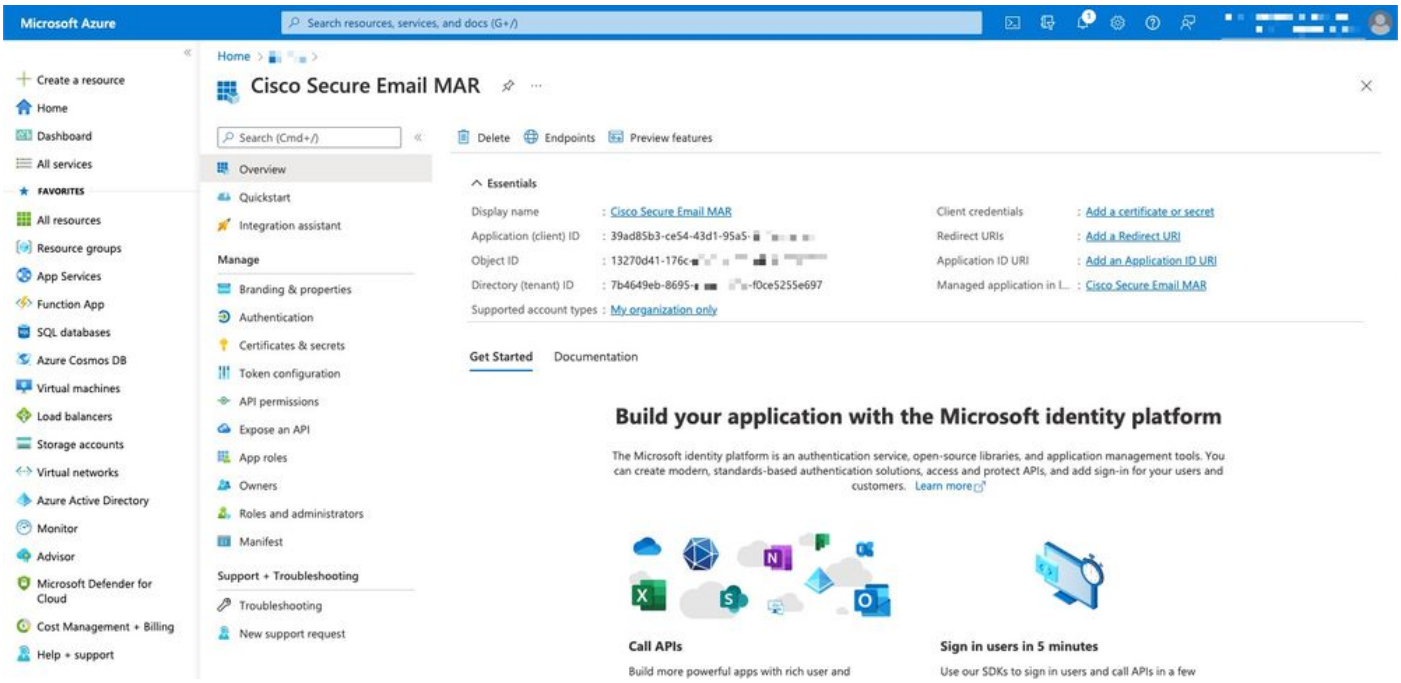


Figure 3 : page de l'application Microsoft Azure Active Directory

Certificats et secrets

Si vous exécutez AsyncOS 14.0 ou une version ultérieure, Cisco recommande de configurer votre application Azure pour utiliser un secret client. Dans le volet Application, dans les options Gérer :

1. Sélectionnez Certificats et secrets

2. Dans la section Secrets client, cliquez sur + Nouveau secret client

3. Ajoutez une description pour vous aider à identifier à quoi sert ce secret client, par exemple « Cisco Secure Email Remise »

4. Sélectionnez une période d'expiration

5. Cliquez sur Add

6. Placez le pointeur de la souris à droite de la valeur générée, puis cliquez sur l'icône Copier dans le Presse-papiers

7. Enregistrez cette valeur dans vos notes, notez-la comme « Client secret »

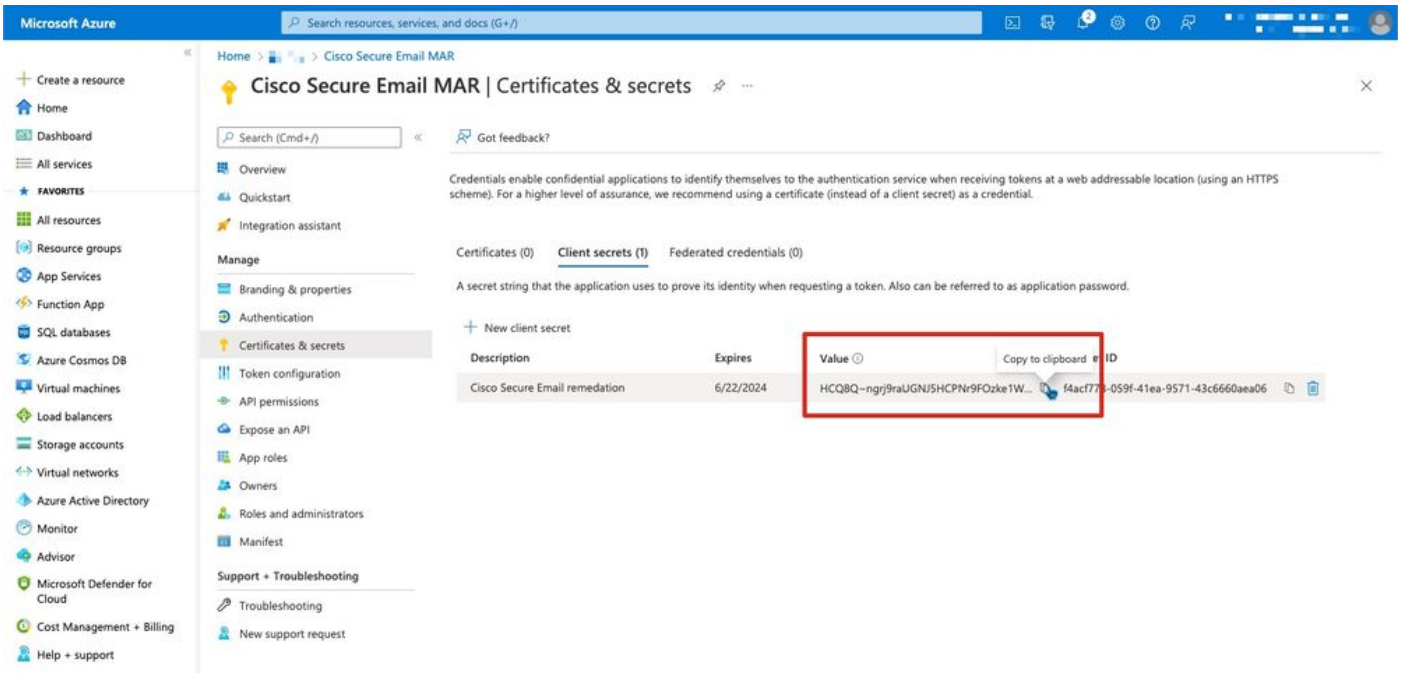


Figure 4 : Exemple de création de secret client par Microsoft Azure

Remarque : une fois que vous avez quitté votre session Microsoft Azure active, la valeur du secret client que vous venez de générer *** sortira de la valeur. Si vous n'enregistrez pas et ne sauvegardez pas la valeur avant de quitter, vous devrez recréer le secret client afin de voir la sortie en texte clair.

Facultatif - Si vous ne configurez pas votre application Azure avec un secret client, configurez votre application Azure pour qu'elle utilise votre certificat. Dans le volet Application, dans les options Gérer :

1. Sélectionner les certificats et les secrets
2. Cliquez sur Télécharger le certificat
3. Sélectionnez le fichier CRT (tel que créé précédemment)
4. Cliquez sur Add

Autorisations API

Remarque : à partir d'AsyncOS 13.0 pour la sécurité de la messagerie, les autorisations API requises pour les communications de messagerie sécurisée Microsoft Azure à Cisco sont passées de Microsoft Exchange à Microsoft Graph. Si vous avez déjà configuré MAR et que vous mettez à niveau votre passerelle de messagerie électronique sécurisée Cisco existante vers AsyncOS 13.0, vous pouvez simplement mettre à jour/ajouter les nouvelles autorisations API. (Si vous utilisez une version antérieure d'AsyncOS, 11.x ou 12.x, consultez l'annexe B avant de continuer.)

Dans le volet Application, dans les options Gérer :

1. Sélectionner les autorisations API
2. Cliquez sur + Ajouter une autorisation
3. Sélectionner Microsoft Graph
4. Sélectionnez les autorisations ci-dessous sur les autorisations d'application :
    1. Mail > "Mail.Read" (Lire le courrier dans toutes les boîtes aux lettres)
    2. Mail > "Mail.ReadWrite" (Lire et écrire le courrier dans toutes les boîtes aux lettres)
    3. Mail > "Mail.Send" (Envoyer le mail comme n'importe quel utilisateur)
    4. Répertoire > "Directory.Read.All" (Lire les données du répertoire) [*Facultatif : si vous utilisez la synchronisation LDAP/Connecteur LDAP, activez. Si ce n'est pas le cas, cela n'est pas obligatoire.]
5. Facultatif : vous verrez que Microsoft Graph est activé par défaut pour les autorisations « Utilisateur.Lecture » ; vous pouvez le laisser configuré ou cliquer sur Lecture et sur Supprimer l'autorisation pour le supprimer de vos autorisations API associées à votre application.
6. Cliquez sur Ajouter des autorisations (ou sur Mettre à jour les autorisations, si Microsoft Graph était déjà répertorié)
7. Enfin, cliquez sur Grant admin consent for... pour vous assurer que vos nouvelles autorisations sont appliquées à l'application
8. Une fenêtre contextuelle s'affiche dans le volet et demande :

    "Voulez-vous accorder l'autorisation pour les autorisations demandées pour tous les comptes dans <Azure Name> ? Cela mettra à jour tous les enregistrements de consentement d'administrateur existants que cette application doit déjà faire correspondre à ceux répertoriés ci-dessous."

    Cliquez sur Oui

À ce stade, vous devriez voir un message de réussite vert et la colonne « Admin Consent Required » (Consentement admin requis) s'afficher.

Obtention de votre ID client et de votre ID locataire

Dans le volet Application, dans les options Gérer :

1. Cliquez sur Aperçu
2. Placez le pointeur de la souris sur la droite de votre ID d'application (client) et cliquez sur l'icône Copier dans le Presse-papiers
3. Enregistrez cette valeur dans vos notes, notez-la comme « ID client »
4. Placez le pointeur de la souris sur la droite de votre ID de répertoire (service partagé) et cliquez sur l'icône Copier dans le Presse-papiers
5. Enregistrez cette valeur dans vos notes, notez-la sous le nom « ID du locataire »

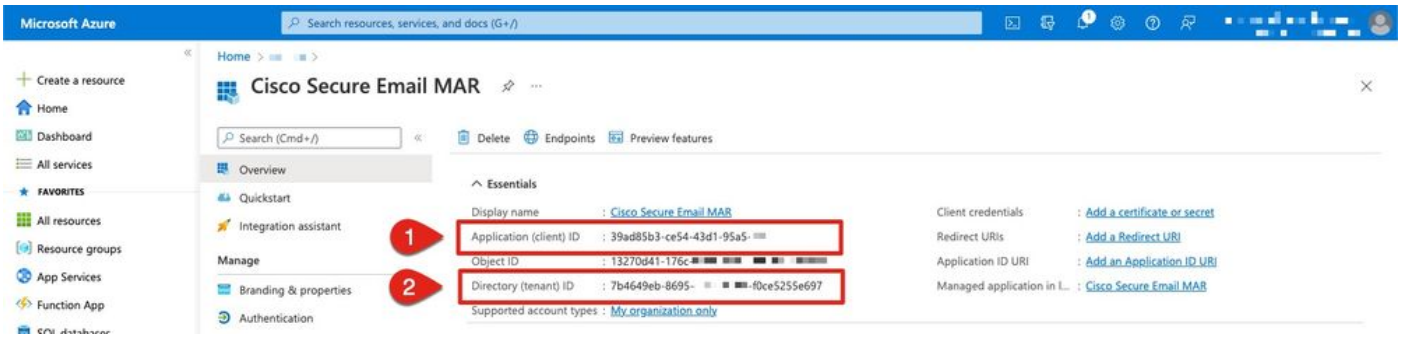


Figure 5 : Microsoft Azure... ID client, exemple d'ID de locataire

Configuration de votre passerelle de messagerie sécurisée/passerelle cloud Cisco

À ce stade, les valeurs suivantes doivent être préparées et enregistrées dans vos notes :

- ID client
- ID du locataire
- Secret client

Facultatif, si vous n'utilisez pas Client secret :

- Empreinte
- La clé privée (fichier PEM)

Vous êtes prêt à utiliser les valeurs créées à partir de vos notes et à configurer les paramètres de compte sur la passerelle de messagerie sécurisée Cisco !

Créer un profil de compte

1. Connectez-vous à votre passerelle
2. Accédez à Administration système > Paramètres du compte
    - Remarque : si vous exécutez une version antérieure à AsyncOS 13.x, il s'agit de Administration système > Paramètres de boîte aux lettres
3. Cliquez sur Activer
4. Cochez la case Enable Account Settings et cliquez sur Submit
5. Cliquez sur Create Account Profile
6. Entrez un nom de profil et une description (qui décrira votre compte de manière unique si vous avez plusieurs domaines)
7. Lorsque vous définissez une connexion Microsoft 365, conservez le type de profil Office 365

/ Hybrid (Graph API)
8. Saisissez votre ID client
9. Saisissez votre ID de locataire
10. Pour les informations d'identification du client, effectuez l'une des actions suivantes, comme vous l'avez configuré dans Azure :
    1. Cliquez sur Client Secret et collez votre secret client configuré, ou...
    2. Cliquez sur Client Certificate et saisissez votre empreinte numérique et fournissez également votre PEM en cliquant sur "Choose File"
11. Cliquez sur Submit
12. Cliquez sur Commit Changes dans l'angle supérieur droit de l'interface utilisateur
13. Saisissez des commentaires et effectuez les modifications de configuration en cliquant sur Valider les modifications

Vérifier la connexion

L'étape suivante consiste uniquement à vérifier la connexion de l'API de votre passerelle de messagerie sécurisée Cisco à Microsoft Azure :

1. Dans la même page Détails du compte, cliquez sur Tester la connexion
2. Entrez une adresse e-mail valide pour le domaine géré dans votre compte Microsoft 365
3. Cliquez sur Test Connection
4. Vous devriez recevoir un message de réussite (Figure 6)
5. Cliquez sur Terminé pour terminer

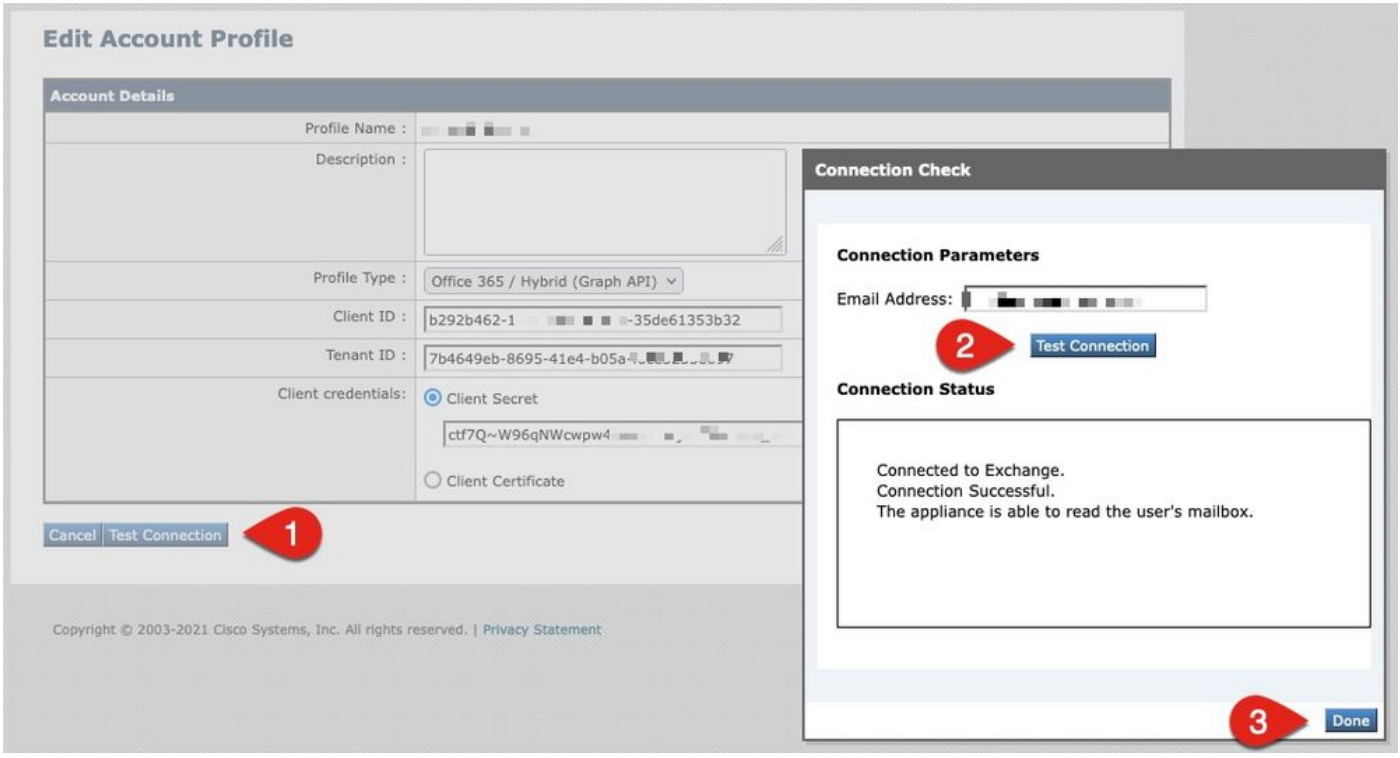


Figure 6 : Exemple de vérification du profil/de la connexion du compte

6. Dans la section Domain Mapping, cliquez sur Create Domain Mapping

7. Entrez dans votre ou vos noms de domaine qui sont associés au compte Microsoft 365 pour lequel vous venez de valider la connexion API

La liste suivante répertorie les formats de domaine valides pouvant être utilisés pour mapper un profil de boîte aux lettres :

- Le domaine peut être le mot clé spécial « ALL » pour correspondre à tous les domaines afin de créer un mappage de domaine par défaut.

- Noms de domaine tels que « example.com » - Fait correspondre n'importe quelle adresse avec ce domaine.

- Noms de domaine partiels tels que '@.partial.example.com' - Correspond à toute adresse se terminant par ce domaine

- Vous pouvez entrer plusieurs domaines à l'aide d'une liste de domaines séparés par des virgules.

8. Cliquez sur Soumettre

9. Cliquez sur Commit Changes dans le coin supérieur droit de l'interface utilisateur

10. Entrez des commentaires et effectuez les modifications de configuration en cliquant sur Valider les modifications

Activer la correction automatique des boîtes aux lettres (MAR) pour la protection avancée contre les programmes malveillants dans la stratégie de messagerie

Complétez cette étape pour activer MAR dans la configuration AMP pour les stratégies de messagerie.

1. Naviguez jusqu'à Politiques de messagerie > Politiques de messages entrants
2. Cliquez sur les paramètres de la colonne Advanced Malware Protection correspondant au nom de la stratégie que vous souhaitez configurer (par exemple, Figure 7) :

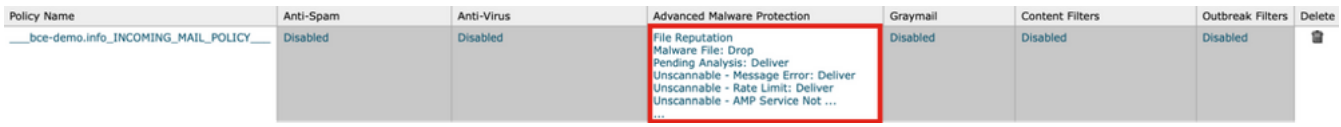


Figure 7 : activation de MAR (stratégies de messages entrants)

3. Faites défiler la page jusqu'en bas
4. Cochez la case Enable Mailbox Auto Remediation (MAR)
5. Sélectionnez l'une des actions suivantes que vous souhaitez effectuer pour le MAR (par exemple, Figure 8) :
    - Transférer à : <saisissez l'adresse e-mail>
    - DELETE
    - Transférer à : <saisissez l'adresse e-mail> et Supprimer

Figure 8 : Exemple de configuration d'activation de MAR pour AMP

6. Cliquez sur Submit
7. Cliquez sur Commit Changes dans l'angle supérieur droit de l'interface utilisateur
8. Saisissez des commentaires et effectuez les modifications de configuration en cliquant sur Valider les modifications

Activer la correction automatique des boîtes aux lettres (MAR) pour le filtrage des URL

Depuis AsyncOS 14.2 pour Cisco Secure Email Cloud Gateway, le filtrage des URL inclut désormais le verdict rétrospectif des URL et la correction des URL.

1. Naviguez jusqu'à Security Services > URL Filtering
2. Si le filtrage des URL n'est pas déjà configuré, cliquez sur Enable
3. Cochez la case Activer les filtres de catégorie et de réputation d'URL.
4. Paramètres avancés avec les paramètres par défaut
5. Cliquez sur Submit

Votre filtrage d'URL doit ressembler à ce qui suit :

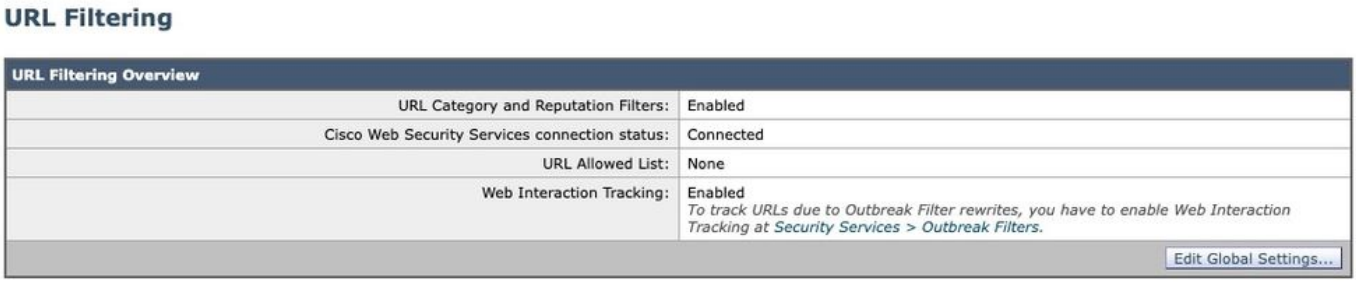


Figure 9 : Exemple de post-activation du filtrage des URL

Afin de voir la rétrospection des URL avec le filtrage des URL intégré, effectuez les opérations suivantes, ou demandez à Cisco d'ouvrir un dossier d'assistance pour effectuer :

<#root>

```
esa1.hcxxyy-zz.iphmx.com>

urlretroservice enable


URL Retro Service is enabled.

esa1.hcxxyy-zz.iphmx.com>

websecurityconfig


URL Filtering is enabled.
No URL list used.
Web Interaction Tracking is enabled.
URL Retrospective service based Mail Auto Remediation is disabled.
URL Retrospective service status - Unavailable

Disable URL Filtering? [N]>

Do you wish to disable Web Interaction Tracking? [N]>

Do you wish to add URLs to the allowed list using a URL list? [N]>


Enable URL Retrospective service based Mail Auto Remediation to configure remediation actions.

Do you wish to enable Mailbox Auto Remediation action? [N]>

y


URL Retrospective service based Mail Auto Remediation is enabled.

Please select a Mailbox Auto Remediation action:
1. Delete
2. Forward and Delete
3. Forward
[1]>

1
```

```
esa1.hcxxyy-zz.iphmx.com>
commit

Please enter some comments describing your changes:
[]>

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Tue Mar 29 19:43:48 2022 EDT
```

Une fois terminé, actualisez votre interface utilisateur sur la page de filtrage des URL et vous devriez maintenant voir ce qui suit :

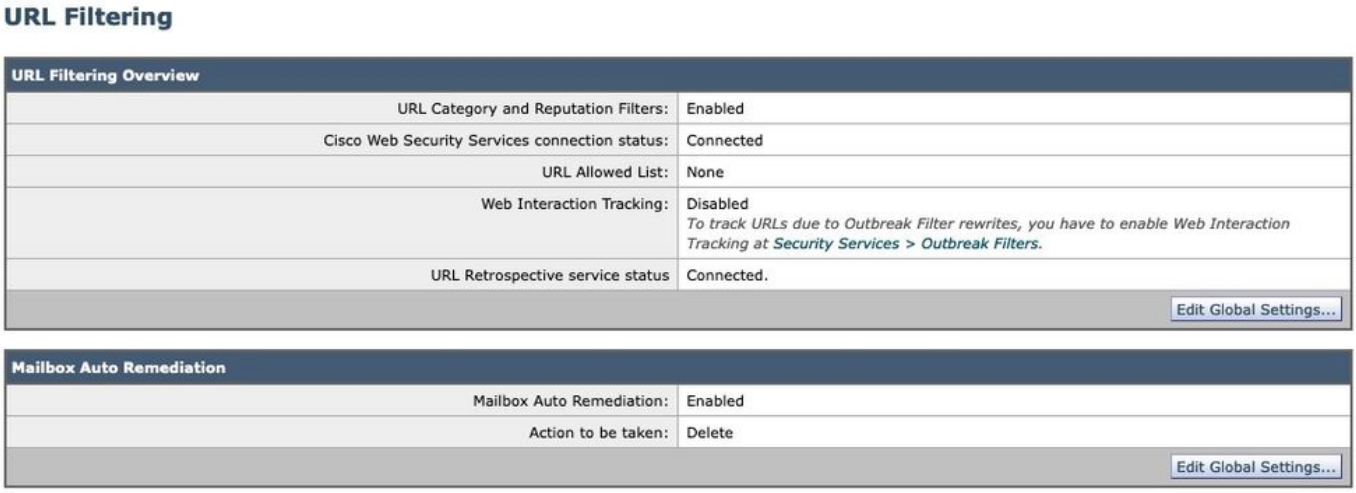


Figure 10 : Filtrage des URL (AsyncOS 14.2 pour Cisco Secure Email Cloud Gateway)

La protection d'URL est désormais prête à exécuter des actions correctives lorsqu'un verdict change de score. Pour plus d'informations, consultez Protection contre les URL malveillantes ou indésirables dans le Guide de l'utilisateur pour AsyncOS 14.2 pour Cisco Secure Email Cloud Gateway.

Configuration terminée !

À ce stade, Cisco Secure Email est prêt à évaluer en permanence les menaces émergentes à mesure que de nouvelles informations deviennent disponibles et à vous avertir des fichiers considérés comme des menaces après leur entrée sur votre réseau.

Lorsqu'un verdict rétrospectif est produit à partir de File Analysis (Cisco Secure Malware Analytics), un message d'information est envoyé à l'administrateur de la sécurité du courrier électronique (s'il est configuré). Exemple :

```
The Info message is:

Retrospective verdict received for Book1.xls.

SHA256: 7d06fd224e0de7f26b48dc2daf7f099b3770080d98bd38c49ed049087c416c4b
Timestamp: 2019-06-03T23:40:36Z
Verdict: MALICIOUS
Spyname: W32.7D06FD224E-95.SBX.TG

Total users affected: 1
---------- Affected Messages ---------------


Message 1
   MID              : 348938
   Subject          : [WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]test Mon, 03 Jun 2019 16:50:18 -0400
   From             : [redacted]
   To               : [redacted]
   File name        : Book1.xls
   Parent SHA256    : unknown
   Parent File name : unknown
   Date             : 2019-06-03T20:52:33Z

-------------------------------------------------


Version: 12.1.0-087
Serial Number: 420DE3B51AB744C7F092-9F0[redacted]
Timestamp: 04 Jun 2019 04:40:36 +0500
```

La correction automatique de la boîte aux lettres sera prise comme configurée si elle est configurée par rapport à la stratégie de messagerie.

Exemples de rapports de correction automatique de boîte aux lettres

La création de rapports pour tout SHA256 qui a été corrigé figurera dans le rapport Mailbox Auto Remediation disponible à la fois sur la passerelle de messagerie sécurisée Cisco et sur Cisco Secure Email and Web Manager.

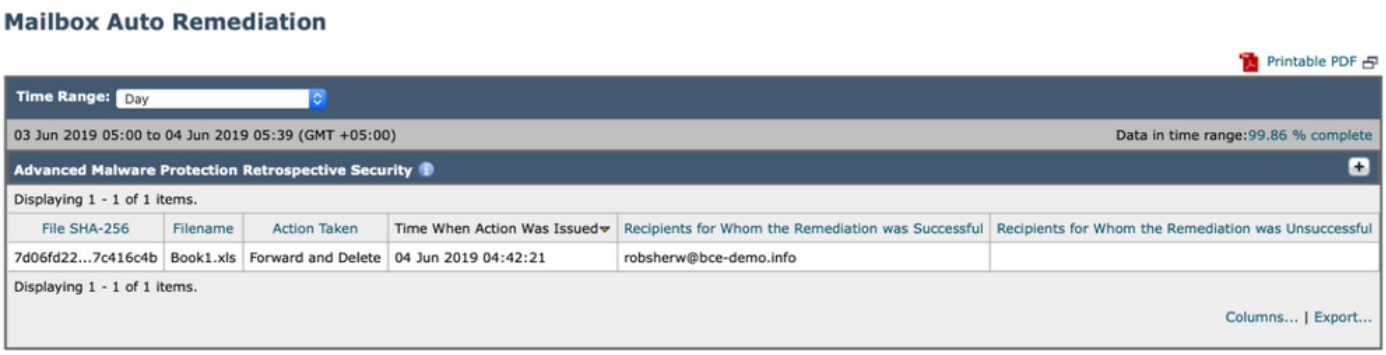


Figure 11 : Rapport de correction automatique des boîtes aux lettres (interface utilisateur héritée)

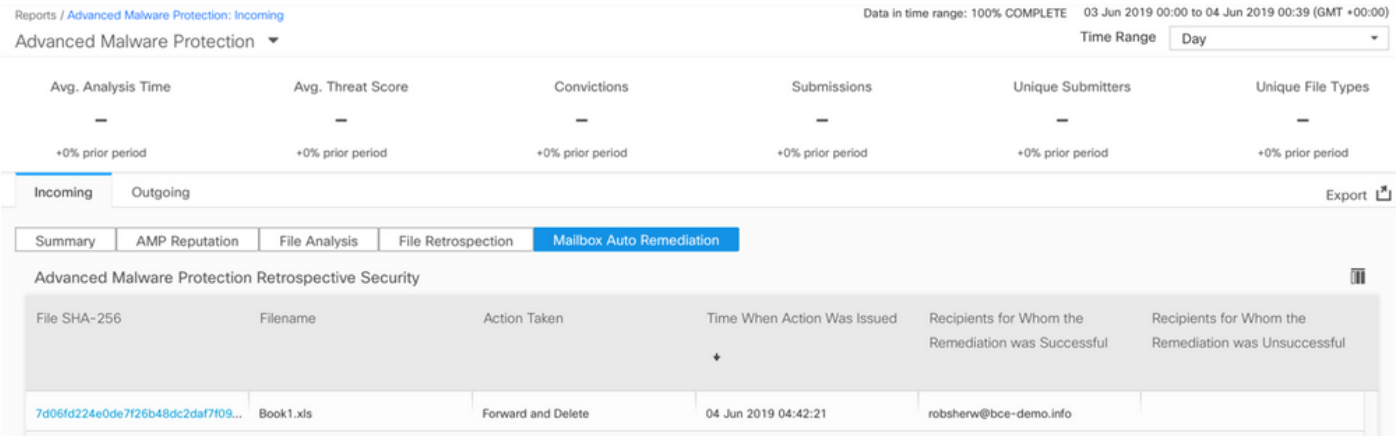


Figure 12 : Rapport de correction automatique des boîtes aux lettres (interface utilisateur NG)

Journalisation de la résolution automatique des boîtes aux lettres

La correction automatique des boîtes aux lettres a un journal individuel, « mar ». Les journaux de correction automatique de la boîte aux lettres contiendront toutes les activités de communication entre votre passerelle de messagerie sécurisée Cisco et Microsoft Azure, Microsoft 365.

Exemple de journaux de marques :

```
Mon May 27 02:24:28 2019 Info: Version: 12.1.0-087 SN: 420DE3B51AB744C7F092-9F0000000000
Mon May 27 02:24:28 2019 Info: Time offset from UTC: 18000 seconds
Fri May 31 01:11:53 2019 Info: Process ready for Mailbox Auto Remediation
Fri May 31 01:17:57 2019 Info: Trying to connect to Azure AD.
Fri May 31 01:17:57 2019 Info: Requesting token from Azure AD.
Fri May 31 01:17:58 2019 Info: Token request successful.
Fri May 31 01:17:58 2019 Info: The appliance is able to read the user's(robsherw@bce-demo.info) mailbox
Fri May 31 04:41:54 2019 Info: Trying to perform the configured action on MID:312391 SHA256:de4dd03acda
Fri May 31 04:41:55 2019 Info: Message containing attachment(s) for which verdict update was(were) avai
Tue Jun  4 04:42:20 2019 Info: Trying to perform the configured action on MID:348938 SHA256:7d06fd224e0
Tue Jun  4 04:42:21 2019 Info: Message containing attachment(s) for which verdict update was(were) avai
```

Dépannage de la passerelle de messagerie sécurisée Cisco

Si vous ne voyez pas de résultats positifs pour le test d'état de la connexion, vous pouvez revoir l'enregistrement de l'application effectué à partir de Microsoft Azure AD.

À partir de la passerelle de messagerie sécurisée Cisco, définissez vos journaux MAR au niveau « trace » et testez à nouveau la connexion.

En cas d'échec de connexion, les journaux peuvent afficher les informations suivantes :

```
Thu Mar 30 16:08:49 2017 Info: Trying to connect to Azure AD.
Thu Mar 30 16:08:49 2017 Info: Requesting token from Azure AD.
Thu Mar 30 16:08:50 2017 Info: Error in requesting token: AADSTS70001: Application with identifier '445
 Trace ID: 4afd14f4-ca97-4b15-bba4-e9be19f30d00
 Correlation ID: f38e3388-729b-4068-b013-a08a5492f190
 Timestamp: 2017-03-30 20:08:50Z
Thu Mar 30 16:08:50 2017 Info: Error while requesting token AADSTS70001: Application with identifier '4
 Trace ID: 4afd14f4-ca97-4b15-bba4-e9be19f30d00
 Correlation ID: f38e3388-729b-4068-b013-a08a5492f190
 Timestamp: 2017-03-30 20:08:50Z
```

Confirmez l'ID d'application, l'ID de répertoire (identique à l'ID de locataire) ou d'autres identificateurs associés dans le journal avec votre application dans Azure AD. Si vous n'êtes pas sûr des valeurs, supprimez l'application du portail Azure AD et recommencez.

Pour une connexion réussie, les journaux doivent être similaires à :

```
Thu Mar 30 15:51:58 2017 Info: Trying to connect to Azure AD.
Thu Mar 30 15:51:58 2017 Info: Requesting token from Azure AD.
Thu Mar 30 15:51:58 2017 Trace: command session starting
Thu Mar 30 15:52:00 2017 Info: Token request successful.
Thu Mar 30 15:52:00 2017 Info: The appliance is able to read the user's(myuser@mydomain.onmicrosoft.com
```

Dépannage d'Azure AD

Remarque : le centre d'assistance technique Cisco et l'assistance Cisco ne sont pas autorisés à résoudre les problèmes côté client avec Microsoft Exchange, Microsoft Azure AD ou Office 365.

Pour les problèmes côté client avec Microsoft Azure AD, vous devrez faire appel au support technique Microsoft. Consultez l'option « Aide + support » de votre tableau de bord Microsoft Azure. Vous pourrez peut-être ouvrir des demandes d'assistance directes auprès du support Microsoft à partir du tableau de bord.

Annexe A

Remarque : cette opération n'est nécessaire que si vous n'utilisez PAS le secret client pour configurer votre application Azure.

Création d'une paire de clés et de certificats publics et privés

Conseil : enregistrez les résultats localement pour $base64Value, $base64Thumbprint et $keyid, car ils seront requis plus tard dans les étapes de configuration. Veuillez disposer du .crt et du .pem associé de votre certificat dans un dossier local disponible sur votre ordinateur.

Remarque : si vous disposez déjà d'un certificat (format x509/standard) et d'une clé privée, ignorez cette section. Assurez-vous d'avoir à la fois des fichiers CRT et PEM, car vous en aurez besoin dans les prochaines sections !

Certificat : Unix/Linux (avec openssl)

Valeurs à créer :

- Empreinte numérique
- Certificat public (fichier CRT)
- Clé privée (fichier PEM)

Pour les administrateurs utilisant Unix/Linux/OS X, pour les besoins et l'exécution du script fourni, il est supposé que vous avez OpenSSL installé.

Remarque : exécutez les commandes « which openssl » et « openssl version » afin de vérifier l'installation d'OpenSSL. Installez OpenSSL s'il n'est pas présent !

Consultez le document suivant pour obtenir de l'aide : [Script de configuration Azure AD pour la messagerie sécurisée Cisco]

Depuis votre hôte (UNIX/Linux/OS X) :

1. À partir d'une application de terminal, d'un éditeur de texte (ou de tout autre outil permettant de créer un script shell), créez un script en copiant ce qui suit : https://raw.githubusercontent.com/robsherw/my_azure/master/my_azure.sh
2. Coller le script
3. Assurez-vous de rendre le script exécutable ! Exécutez la commande suivante : chmod u+x my_azure.sh
4. Exécutez le script : ./my_azure.sh

```
################################################################################
Next, log-in to Microsoft Azure and use the following for your App registration:
################################################################################

Complete the Azure App registration (Certificate & secrets) using this certificate (public key): MARforO365.crt
Complete the Azure App registration (API permissions)
View & save your Client ID and Tenant ID

######################################################
After successful Azure App registration, from Cisco ESA:
######################################################

Use the Client ID and Tenant ID copied from your Azure App registration
The Thumbprint to use for your ESA configuration: cY8JViuV1oFRVFje/HC9J9ZGvl8=
The Certificate Private Key to use for your ESA configuration: MARforO365.pem

Do you wish to review this certificate in detail? (y/n) n
Thank you!  Be sure to keep up-to-date from https://docs.ces.cisco.com
```

Figure 13 : résultat d'écran de my_azure.sh

Comme vous le voyez dans la Figure 2, le script génère et appelle le certificat public (fichier CER) nécessaire pour l'inscription de l'application Azure. Le script appelle également la clé privée ThumbprintandCertificate (fichier PEM) que vous utiliserez dans la section Configuration de la messagerie sécurisée Cisco.

vous disposez des valeurs nécessaires pour enregistrer votre application dans Microsoft Azure !

[Ignorez la section suivante ! Veuillez passer à « Enregistrer une application Azure pour l'utiliser avec Cisco Secure Email »]

Certificat : Windows (utilisation de PowerShell)

Pour les administrateurs qui utilisent Windows, vous devez utiliser une application ou disposer des connaissances nécessaires pour créer un certificat auto-signé. Ce certificat est utilisé afin de créer l'application Microsoft Azure et d'associer la communication de l'API.

Valeurs à créer :
• Empreinte numérique • Certificat public (fichier CRT) • Clé privée (fichier PEM)

Notre exemple pour ce document afin de créer un certificat auto-signé est l'utilisation de XCA (https://hohnstaedt.de/xca/, https://sourceforge.net/projects/xca/).

Remarque : XCA peut être téléchargé pour Mac, Linux ou Windows.

1. Créez une base de données pour votre certificat et vos clés : a. Sélectionnez Fichier dans la barre	

d'outils

b. Sélectionnez Nouvelle base de données

c. Créez un mot de passe pour votre base de données

(vous en aurez besoin dans les étapes suivantes, alors n'oubliez pas !)

2. Cliquez sur l'onglet Certificats, puis sur Nouveau certificat

3. Cliquez sur l'onglet Objet et renseignez les champs suivants :

a. Nom interne

b. nom du pays

c. stateOrProvinceName

d. localityName

e. nom de l'organisation

f. NomUnitéOrganisation (OU)

g. CommonName (CN)

h. adresseEmail

4. Cliquez sur Generate a New Key

5. Dans la fenêtre contextuelle, vérifiez les informations fournies

(à modifier selon les besoins) :

a. Nom

b. Type de clé : RSA

c. Taille de clé : 2048 bits

d. Cliquez sur Créer

e. Reconnaissez la fenêtre contextuelle « Nom » de la clé privée RSA créée en cliquant sur OK

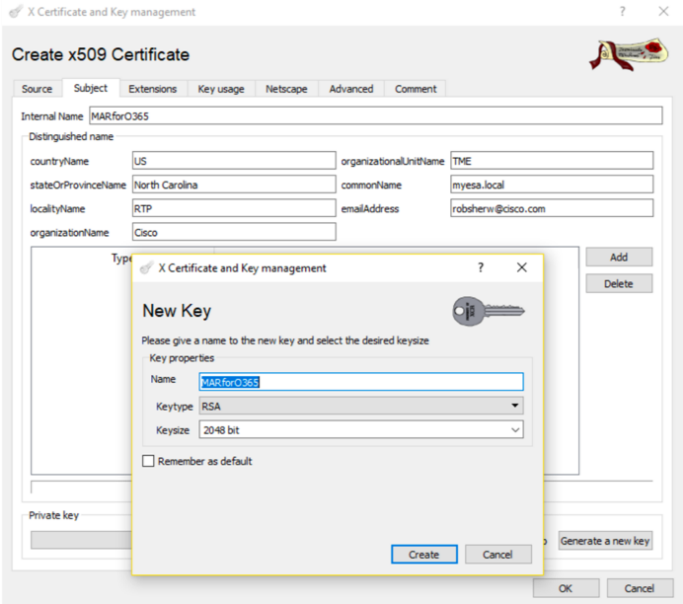
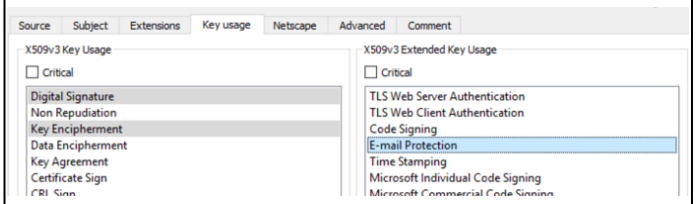
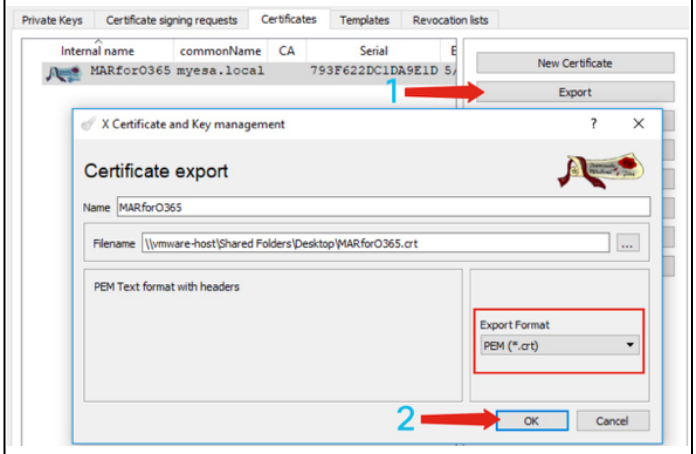


Figure 14 : Utilisation de XCA (étapes 3 à 5)

6. Cliquez sur l'onglet Utilisation des clés et sélectionnez les options suivantes : a. Sous Utilisation de la clé X509v3 : Signature numérique, chiffrement de clé b. Sous X509v3 Extended Key Usage : Protection de la messagerie électronique	 Figure 15 : Utilisation de XCA (étape 6)
7. Cliquez sur OK pour appliquer les modifications à votre certificat 8. Reconnaissez la fenêtre contextuelle « Le certificat 'Name' a été créé avec succès » en cliquant sur OK	

Ensuite, vous voudrez exporter à la fois le certificat public (fichier CER) et la clé privée de certificat (fichier PEM) pour une utilisation dans les commandes PowerShell suivantes, et pour une utilisation dans les étapes Configuration de la messagerie électronique sécurisée Cisco :

1. Cliquez et mettez en surbrillance le nom interne du certificat que vous venez de créer. 2. Cliquez sur Exporter a. Définissez le répertoire de sauvegarde pour en faciliter l'accès (en le modifiant comme vous le souhaitez) b. Vérifiez que le format d'exportation est défini sur PEM (.crt) c. Cliquez sur OK	 Figure 16 : Utilisation de XCA (export CRT) (étapes 1 et 2)

3. Cliquez sur l'onglet Clés privées

4. Cliquez et mettez en surbrillance le nom interne du certificat que vous venez de créer.

5. Cliquez sur Exporter

   a. Définissez le répertoire de sauvegarde pour en faciliter l'accès (en le modifiant comme vous le souhaitez)

   b. Vérifiez que le format d'exportation est défini sur PEM private (.pem)

   c. Cliquez sur OK

6. Quitter et fermer XCA

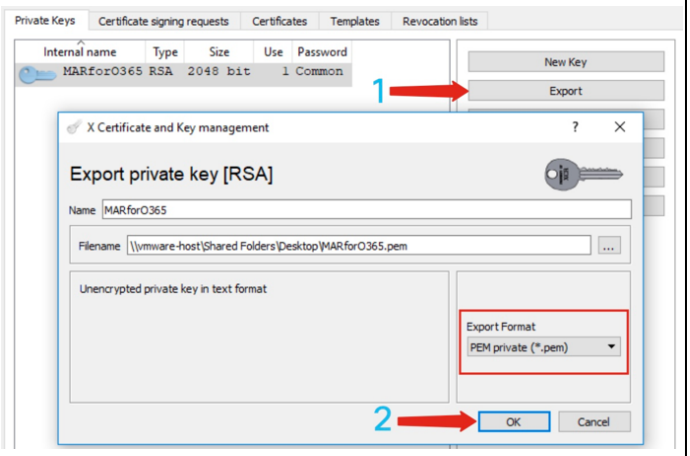


Figure 17 : Utilisation de XCA (export PEM) (étapes 3 à 5)

Enfin, vous prendrez votre certificat créé et extrayez l'empreinte numérique, qui est nécessaire pour la configuration de la messagerie électronique sécurisée Cisco.

1. À l'aide de Windows PowerShell, exécutez les commandes suivantes :

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import("c:\Users\joe\Desktop\myCert.crt")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)
$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)
$keyid = [System.Guid]::NewGuid().ToString()[Note: “c:\Users\joe\Desktop...” is the location on your PC
```

2. Afin d'obtenir des valeurs pour les étapes à venir, l'enregistrement dans un fichier ou à copier dans votre Presse-papiers :

```
$base64Thumbprint | Out-File c:\Users\joe\Desktop\base64Thumbprint.txt
$base64Thumbprint
```

Remarque : « c:\Users\joe\Desktop... » est l'emplacement sur votre PC où vous enregistrez le résultat.

Le résultat attendu lors de l'exécution de la commande PowerShell doit être similaire à ce qui suit :

```
PS C:\Users\joe\Desktop> $base64Thumbprint
75fA1XJEJ4I1ZVFOB2xqkoCIh94=
```

Comme vous le voyez, la commande PowerShell appelle l'empreinte numérique base64, qui est l'empreinte numérique requise pour la configuration de la passerelle de messagerie sécurisée Cisco.

Vous avez également terminé la création du certificat public (fichier CER) nécessaire pour l'inscription de l'application Azure. Et vous avez créé la clé privée de certificat (fichier PEM) que vous utiliserez dans la section Configuration de la messagerie électronique sécurisée Cisco.

Vous disposez des valeurs nécessaires pour enregistrer votre application dans Microsoft Azure !

[Passez à la section « Enregistrer une application Azure pour l'utiliser avec la messagerie sécurisée Cisco »]

Annexe B

Remarque : cette opération est uniquement requise si vous exécutez AsyncOS 11.x ou 12.x pour la messagerie électronique sur votre passerelle.

Autorisations API (AsyncOS 11.x, 12.x)

Dans le volet Application, dans les options Gérer...

1. Sélectionner les autorisations API
2. Cliquez sur + Ajouter une autorisation
3. Faites défiler jusqu'à Supported legacy APIs et sélectionnez Exchange
4. Sélectionnez les autorisations suivantes sur les autorisations déléguées :

    1. EWS > « EWS.AccessAsUser.All » (Accéder aux boîtes aux lettres en tant qu'utilisateur connecté via les services Web Exchange)
    2. Mail > "Mail.Read" (Lire le message de l'utilisateur)
    3. Mail > "Mail.ReadWrite" (Lire et écrire le message utilisateur)
    4. Mail > "Mail.Send" (Envoyer un mail en tant qu'utilisateur)
5. Faites défiler jusqu'en haut du volet...
6. Sélectionnez les autorisations ci-dessous sur les autorisations d'application :
    1. « full_access_as_app » (utiliser les services Web Exchange avec un accès complet à toutes les boîtes aux lettres)
    2. Mail > "Mail.Read" (Lire le message de l'utilisateur)
    3. Mail > "Mail.ReadWrite" (Lire et écrire le message utilisateur)
    4. Mail > "Mail.Send" (Envoyer un mail en tant qu'utilisateur)
7. Facultatif : vous verrez que Microsoft Graph est activé par défaut pour les autorisations « Utilisateur.Lecture » ; vous pouvez le laisser configuré ou cliquer sur Lecture et sur Supprimer l'autorisation pour le supprimer de vos autorisations API associées à votre application.
8. Cliquez sur Ajouter des autorisations (ou sur Mettre à jour les autorisations, si Microsoft Graph était déjà répertorié)
9. Enfin, cliquez sur Grant admin consent for... pour vous assurer que vos nouvelles autorisations sont appliquées à l'application
10. Une fenêtre contextuelle s'affiche dans le volet et demande :

    "Voulez-vous accorder l'autorisation pour les autorisations demandées pour tous les comptes dans <Azure Name> ? Cela mettra à jour tous les enregistrements de consentement d'administrateur existants que cette application doit déjà faire correspondre à ceux répertoriés ci-dessous."

    Cliquez sur Oui

À ce stade, vous devriez voir un message de réussite vert et la colonne « Admin Consent Required » (Consentement administrateur requis) s'afficher comme suit :

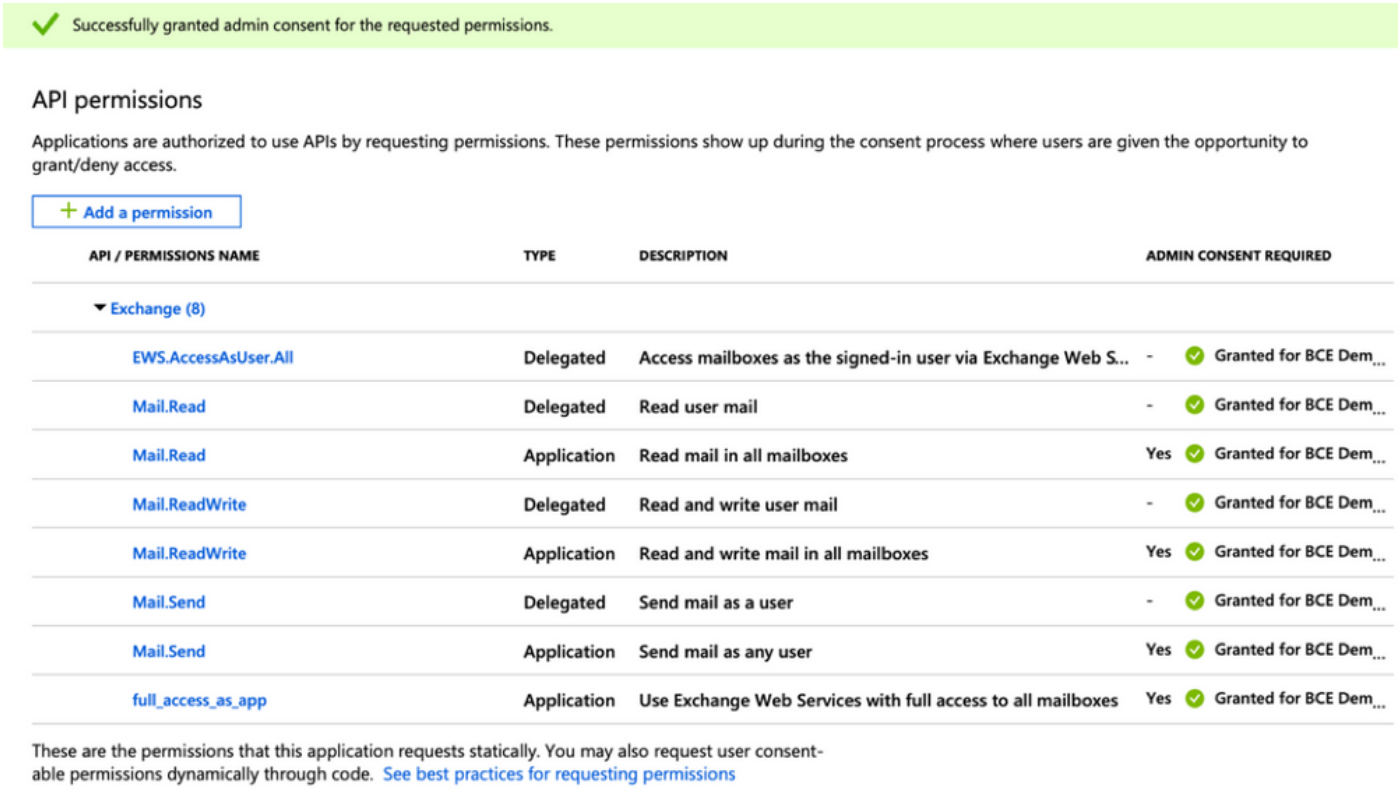


Figure 18 : Enregistrement de l'application Microsoft Azure (autorisations API requises)

[Passez à la section « Enregistrer une application Azure pour l'utiliser avec la messagerie sécurisée Cisco »]

Informations connexes

- Appliance de sécurisation de la messagerie Cisco - Assistance produit
- Appliance de sécurisation de la messagerie Cisco - Notes de version
- Appliance de sécurisation de la messagerie Cisco - Guide de l'utilisateur

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.