Configurer la correction automatique des boîtes aux lettres pour AsyncOS 13.0+

Table des matières

Problème

Ce document décrit comment configurer les fonctionnalités de Mailbox Auto Remediation (MAR) dans AsyncOS 13.0 et versions ultérieures pour les déploiements Exchange Online, Exchange sur site, hybrides et multilocataires.

MAR a été introduit dans AsyncOS 10.0 et ne prend en charge que Microsoft Office 365 Online.

AsyncOS 13.0 et les fonctionnalités plus récentes incluent :

- Microsoft Exchange Online - boîte aux lettres hébergée sur Microsoft Office 365
- Microsoft Exchange sur site - un serveur Microsoft Exchange local
- Configurations hybrides et multilocataires : combinaison de boîtes aux lettres configurées sur les déploiements Microsoft Exchange Online et Microsoft Exchange sur site

Les étapes de la configuration initiale sont disponibles dans le guide de configuration MAR d'origine pour Microsoft Office 365, ainsi qu'un addendum qui décrit les modifications apportées à AsyncOS 13.0 et versions ultérieures.

L'article d'origine reste valide et couvre une explication de la fonctionnalité, ainsi que les étapes de génération de certificats pour l'implémentation Microsoft Office 365 Azure, les paramètres ESA et le dépannage général.

Configuration des paramètres de boîte aux lettres Azure AD et Office 365 pour ESA

Nouvelles modifications apportées aux autorisations de l'API Azure pour 13.0

Le Guide de l'utilisateur actuel fournit des informations plus détaillées sur la fonction de correction automatique.

Reportez-vous au chapitre intitulé Résolution automatique des messages dans les boîtes aux

lettres.

Environnement

- AsyncOS 13.0 ou version ultérieure pour ESA
- Clés de licence pour File Reputation et File Analysis
- Déploiement sur site de Microsoft Office 365 ou Microsoft Exchange

Résolution

1. Pour les profils de compte Exchange Online, utilisez d'abord ces articles de configuration Azure pour créer l'application Azure, les certificats et les autorisations API requis par AsyncOS 13.0 et versions ultérieures :
    - Configuration des paramètres de boîte aux lettres Azure AD et Office 365 pour ESA
2. Créez les profils de compte requis dans l'ESA.
3. Configurez le mappage de domaine pour chaque profil.
4. Si le déploiement est hybride ou multilocataire, configurez des profils enchaînés.
5. Testez chaque profil de compte.

ESA 13.0 et versions ultérieures prennent en charge plusieurs profils de compte créés avec Exchange Online, Exchange sur site ou les deux :

- Les entreprises aux configurations complexes peuvent utiliser plusieurs profils de compte lorsque les domaines sont séparés et résident sur des déploiements différents.
- Les entreprises qui absorbent une nouvelle acquisition peuvent inclure le domaine acquis dans la fonctionnalité MAR.
    - La création de plusieurs profils de compte offre plus de flexibilité que les fonctionnalités ESA précédentes.

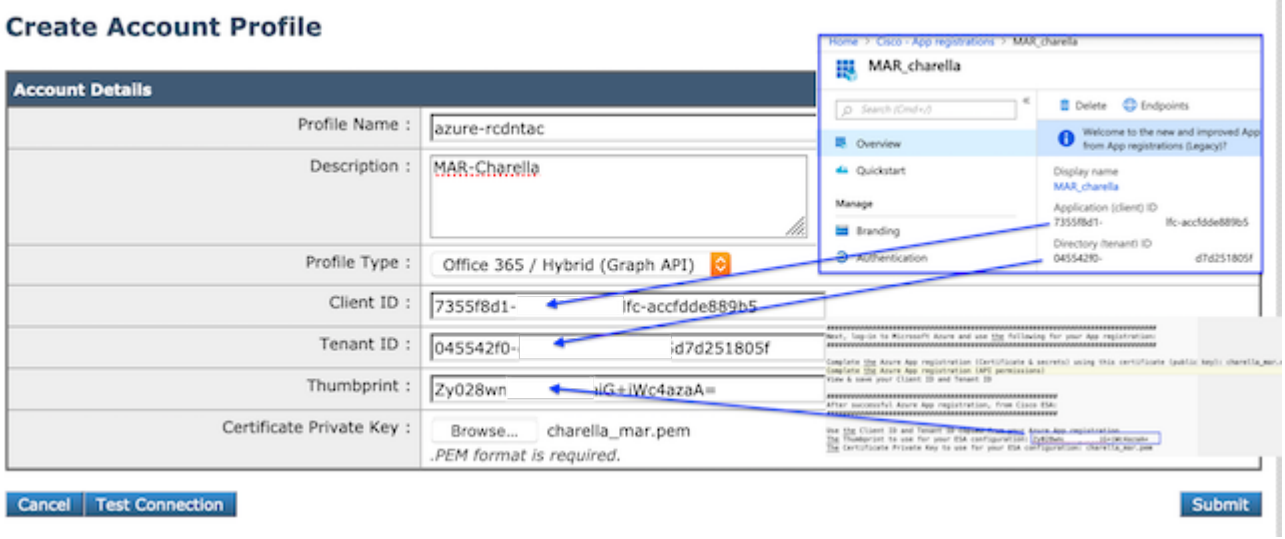
Configurer le profil Microsoft Office 365 Exchange Online

Les instructions de création d'un profil de compte pour Microsoft Office 365 dans Azure sont incluses dans les articles référencés dans la section Problème.

Sélectionnez API Graph hybride Office 365 pour configurer une boîte aux lettres déployée sur Exchange Online et entrez les détails suivants :

- ID client et ID locataire de l'application enregistrée dans Azure Management Portal.
- Empreinte numérique du certificat (valeur de $base64Empreinte numérique).

- Cliquez sur Choose File et sélectionnez le fichier .pem pour télécharger la clé privée du certificat.



Exemple de profil connecté à O365

Exemple de profil de compte Exchange Online

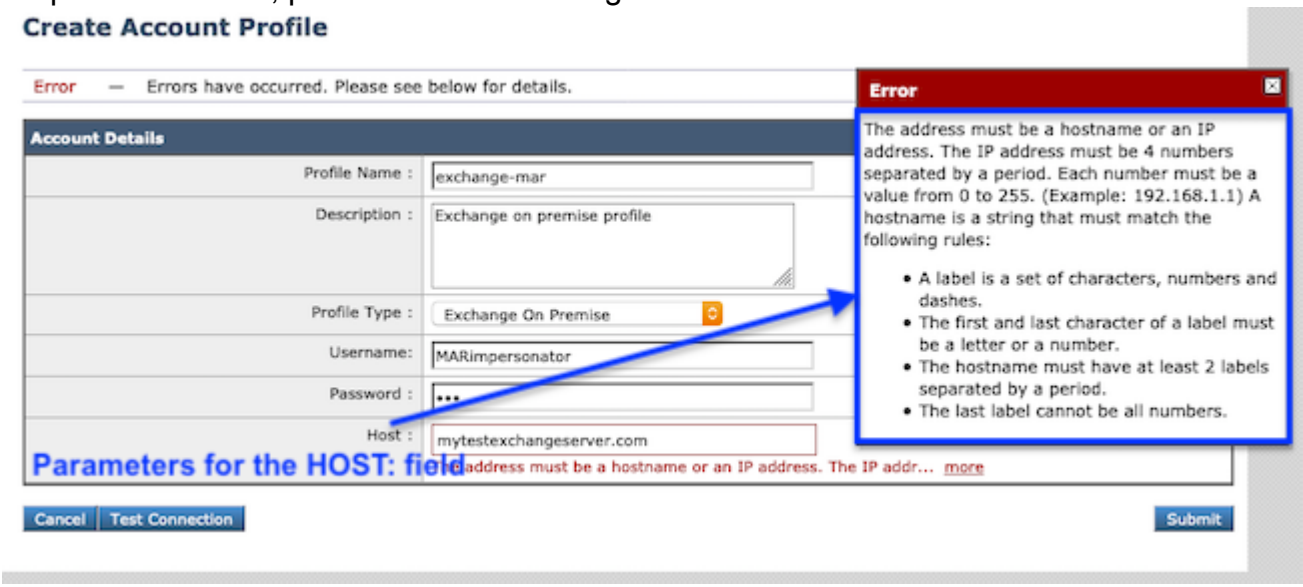
Configurer le profil Exchange sur site

La création d'un profil de compte pour une instance Exchange locale nécessite un compte d'utilisateur avec le rôle ApplicationImpersonation et une valeur d'hôte valide.

Cette méthode nécessite le compte de service local Exchange désigné avec le rôle ApplicationImpersonation.

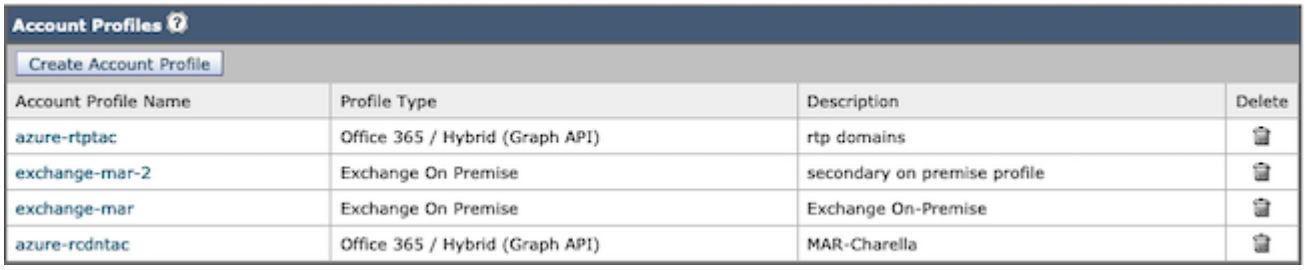
1. Dans un navigateur, ouvrez l'URL Exchange Admin Center pour votre environnement Exchange local. Exemple : https://mail.example.com/ecp/.
2. Après vous être connecté, accédez à Autorisations > Rôles admin.
3. Cliquez sur Ajouter pour créer un nouveau groupe de rôles.
4. Si un groupe de rôles existe déjà, ajoutez le compte d'utilisateur désigné en tant que membre.
5. Entrez le nom et la description du groupe de rôles.
6. Sous Rôles, cliquez sur Ajouter.
7. Sélectionnez ApplicationImpersonation, puis cliquez sur Add.
8. Click OK.
9. Retournez au groupe de rôles nouvellement créé, cliquez sur Membres : +, recherchez le compte d'utilisateur désigné et ajoutez-le pour l'utiliser sur l'ESA.
10. Validez toutes les modifications dans Exchange. Pour plus d'informations, reportez-vous à la documentation du support technique Microsoft.
11. Dans l'interface Web ESA, accédez à Administration système > Paramètres du compte.
12. Créez le profil de compte, puis entrez le nom et la description du profil.
13. Dans la liste déroulante Profile Type, sélectionnez Exchange On-Premise.

14. Saisissez le nom d'utilisateur, le mot de passe et la valeur Host.
15. Entrez un nom d'hôte de serveur Exchange valide pour la valeur Hôte.
16. Cliquez sur Submit, puis sur Commit Changes.



Exemple de profil Exchange sur site

Exemple de profil de compte Exchange local



Exemples de profils de compte MAR

Exemples de profils de compte MAR

Configurer le mappage de domaine

Le mappage de domaine est l'affectation d'un ou de plusieurs domaines à un profil de compte.

Chaque implémentation nécessite au moins un mappage de domaine :

1. Dans l'interface Web ESA, accédez à Administration système > Paramètres du compte > Créer un mappage de domaine.
2. Entrez les noms de domaine séparés par des virgules. Les formats de domaine acceptables sont indiqués dans l'image.
3. S'il n'y a qu'un seul profil de compte dans la configuration, entrez ALL dans le champ Domain Name.

4. Un domaine ne peut être utilisé qu'une seule fois.



Exemple de mappage de domaine

Exemple de mappage de domaine

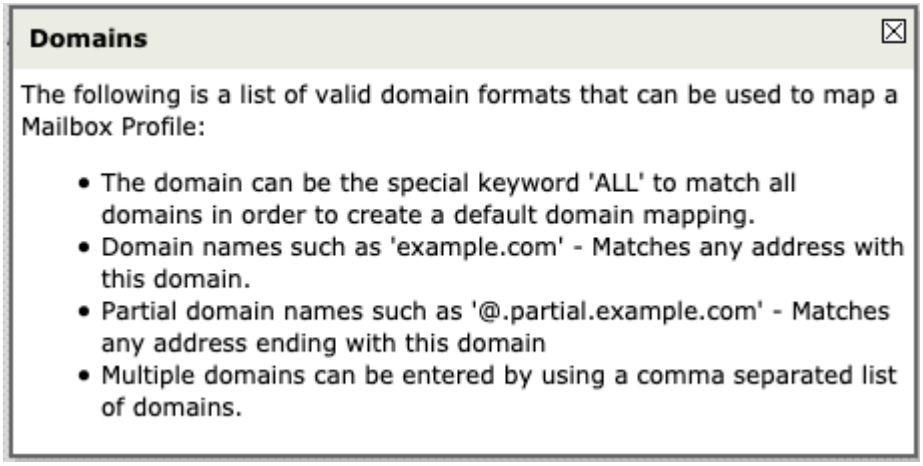
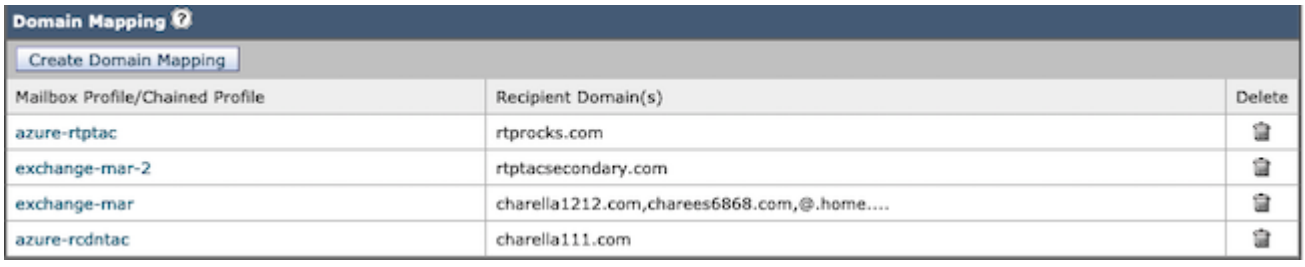


Image 1. Formats de domaine acceptables

Formats de domaine acceptables



Exemple de mappage de domaine

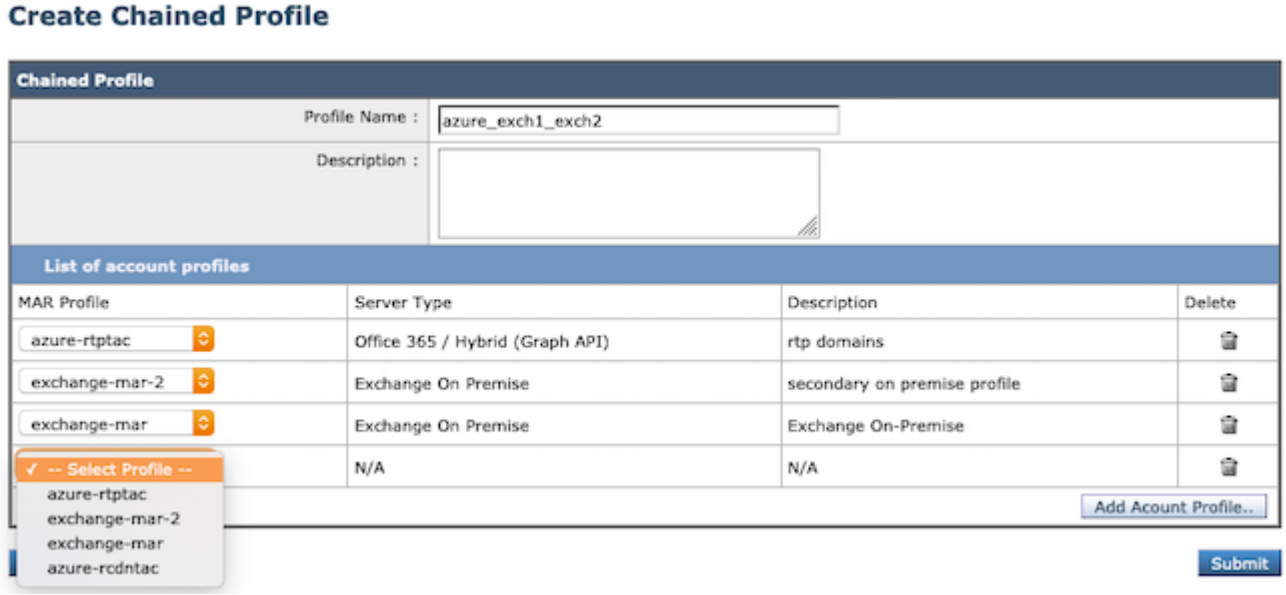
Exemple de mappage de domaine

Configuration des profils enchaînés

Configurez des profils enchaînés uniquement lorsque vous corrigez des messages dans des boîtes aux lettres qui font partie d'un déploiement hybride ou multilocataire.

Ajoutez les profils par ordre de priorité, en commençant par le profil de domaine le plus utilisé.

1. Dans l'interface Web ESA, accédez à Administration système > Paramètres du compte > Créer des profils chaînés.
2. Saisissez le nom et la description du profil.
3. Sélectionnez un domaine dans la liste déroulante MAR Profile.
4. Cliquez sur Add Account Profile pour ajouter un autre profil de domaine jusqu'à ce que tous les profils requis soient ajoutés.
5. Cliquez sur Submit, puis sur Commit Changes.



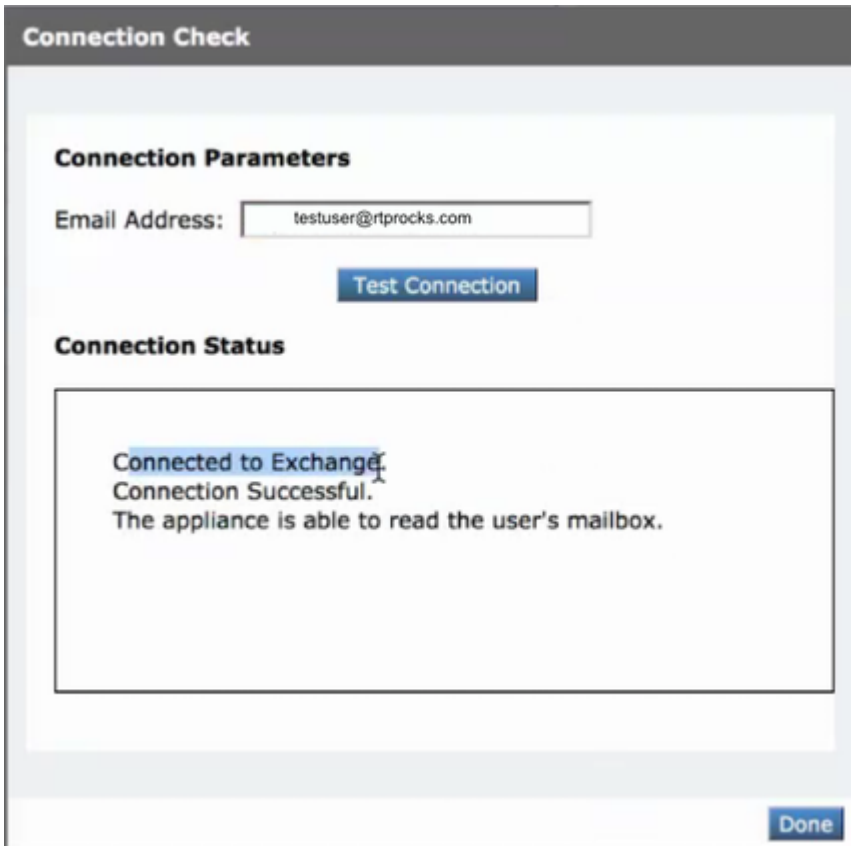
Création de profils en chaîne.

Création de profils enchaînés

Tester chaque profil de compte

Confirmez chaque profil de compte en cliquant sur le bouton Test Connection dans le profil individuel.

1. Dans l'interface Web ESA, accédez à Administration système > Paramètres du compte, puis choisissez l'un des profils de compte.
2. Cliquez sur le bouton Test Connection dans le coin inférieur gauche.
3. Saisissez l'adresse e-mail dans le champ Email Address, puis cliquez sur Test Connection.



Testez chaque profil pour vérifier la connectivité

Tester la connexion pour un profil de compte

Dépannage

Les journaux contiennent :

- journaux_courrier : Action corrective finale et résumé
- mar_logs : Séquence dans laquelle la correction a été effectuée
- Option Test Connection dans l'interface utilisateur : utilisé pour vérifier la connectivité et les autorisations

De nombreuses informations peuvent être déterminées par le test d'e-mail à partir des paramètres de compte.

Dépannage à l'aide de Test Connection

Aucune boîte aux lettres n'est associée à l'adresse SMTP.

La boîte aux lettres utilisateur en cours d'utilisation n'existe pas.

L'accès est refusé. Vérifiez les informations d'identification et réessayez.

L'application configurée dans Microsoft Azure ne dispose pas des autorisations API requises pour accéder à la boîte aux lettres Microsoft Office 365.

L'application avec l'identificateur <client_id> est introuvable dans le répertoire <tenant_id>.

L'ID client de la page Paramètres du profil de compte n'est pas valide.

Aucun espace de noms de service nommé <tenant_id> n'a été trouvé dans le magasin de données.

L'ID de locataire de la page Paramètres du profil de compte est incorrect.

Erreur de validation des informations d'identification. La validation des informations d'identification a échoué.

- L'empreinte numérique du certificat sur la page Profil de compte est incorrecte.
- Le type de profil utilisé pour accéder à la boîte aux lettres peut être incorrect. Par exemple, un profil Microsoft Office 365 permet d'accéder à une boîte aux lettres locale.
- Les autorisations requises pour accéder à la boîte aux lettres peuvent être manquantes.

Nom d'utilisateur ou mot de passe non valide entré pour le serveur Exchange.

Le nom d'utilisateur et le mot de passe du compte Impersonator saisis dans le profil ne sont pas valides.

Le compte n'est pas autorisé à emprunter l'identité de l'utilisateur demandé.

Les privilèges de rôle d'imitateur ne sont pas attribués au compte d'utilisateur configuré dans le profil.

Vérifiez que l'hôte <hostname> est une adresse de serveur Exchange valide.

Le nom d'hôte du serveur Exchange local entré dans le profil n'est pas valide.

Impossible d'accéder à la boîte aux lettres à l'aide de ce profil ou les autorisations requises peuvent être manquantes.

Un type de profil incorrect est utilisé pour accéder à une boîte aux lettres valide. Par exemple, un profil Microsoft Office 365 permet d'accéder à une boîte aux lettres locale.

Exemple de correction réussie pour un profil unique :

<#root>

```
Fri Aug 30 11:57:30 2019 Info: Process ready for Mailbox Remediation

Fri Aug 30 12:29:54 2019 Info: MID: 782107 Attempting to remediate using `o365-profile-1` profile for re


Fri Aug 30 12:29:54 2019 Info: MID: 782107 Trying to perform the forward and delete action on Office 36
1e6f324982d4eb71ad967e79261a6435aef928b57bc523dbb3e7de4ed65941ab recipient's (user@example.com) mailbox
Fri Aug 30 12:29:58 2019 Info: MID: 782107 Message forwarded successfully to admin@example.com.
Fri Aug 30 12:29:58 2019 Info: MID: 782107 Message deleted successfully from user@example.com mailbox.
Fri Aug 30 12:29:58 2019 Info: MID: 782107 Remediation succeeded with `o365-profile-1` profile for recip
```

Exemple de correction réussie pour un profil enchaîné :

<#root>

```
Mon Oct 14 15:01:01 2019 Info: MID: 24 Attempting to remediate using 'o365-profile-1' profile for recipi


Mon Oct 14 15:01:01 2019 Info: MID: 24 Trying to perform the delete action on Office 365 or Hybrid excha
recipient's (user@example.com) mailbox
Mon Oct 14 15:01:09 2019 Info: MID: 24 Unable to read message(s) from the recipient's (user@example.com)
permissions can be missing

Mon Oct 14 15:01:09 2019 Info: MID: 24 Attempting to remediate using 'exchange-profile-1' profile for re


Mon Oct 14 15:01:09 2019 Info: MID: 24 Trying to perform the delete action on Exchange on-premises for
recipient's (user@example.com) mailbox.
Mon Oct 14 15:01:16 2019 Info: MID: 24 Message deleted successfully from user@example.com mailbox.
Mon Oct 14 15:01:16 2019 Info: MID: 24 Remediation succeeded with 'exchange-profile-1' profile for recip
```

Motif

AsyncOS 13.0 et les versions ultérieures offrent une prise en charge étendue du déploiement MAR. Cette prise en charge étendue nécessite un profil de compte, un mappage de domaine et une configuration de profil chaîné supplémentaires, selon que le déploiement Exchange est Exchange Online, Exchange sur site, hybride ou multilocataire.

Autres informations utiles

- Configuration des paramètres de boîte aux lettres Azure AD et Office 365 pour ESA
- Assistance technique et documentation Cisco
- 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 - Guides de l'utilisateur final
- Cisco Content Security Management Appliance - Assistance produit
- Appliance de gestion de la sécurité du contenu Cisco - Notes de version
- Cisco Content Security Management Appliance - Guides d'utilisation

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.