Configurer le complément de cryptage du courrier électronique à l'aide de Microsoft O365

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Meilleures pratiques de déploiement du complément Cisco Secure Email Encryption Service

Configurer

- Enregistrement de l'application complémentaire Cisco Secure Email Encryption Service
- Configurer les paramètres de domaine et de complément sur le portail d'administration de Cisco Secure Email Encryption (CRES)
- Télécharger le fichier manifeste vers Microsoft 365 pour déployer le complément Service de cryptage des e-mails

Vérifier

Dépannage

Informations de relation

Introduction

Ce document décrit comment configurer le déploiement centralisé du complément de service de cryptage du courrier électronique Cisco via Microsoft Office 365.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Passerelle de messagerie sécurisée Cisco
- Cisco Secure Email Encryption Service (anciennement Cisco Registered Envelope Service)
- Suites Microsoft O365 (Exchange, Entra ID, Outlook)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

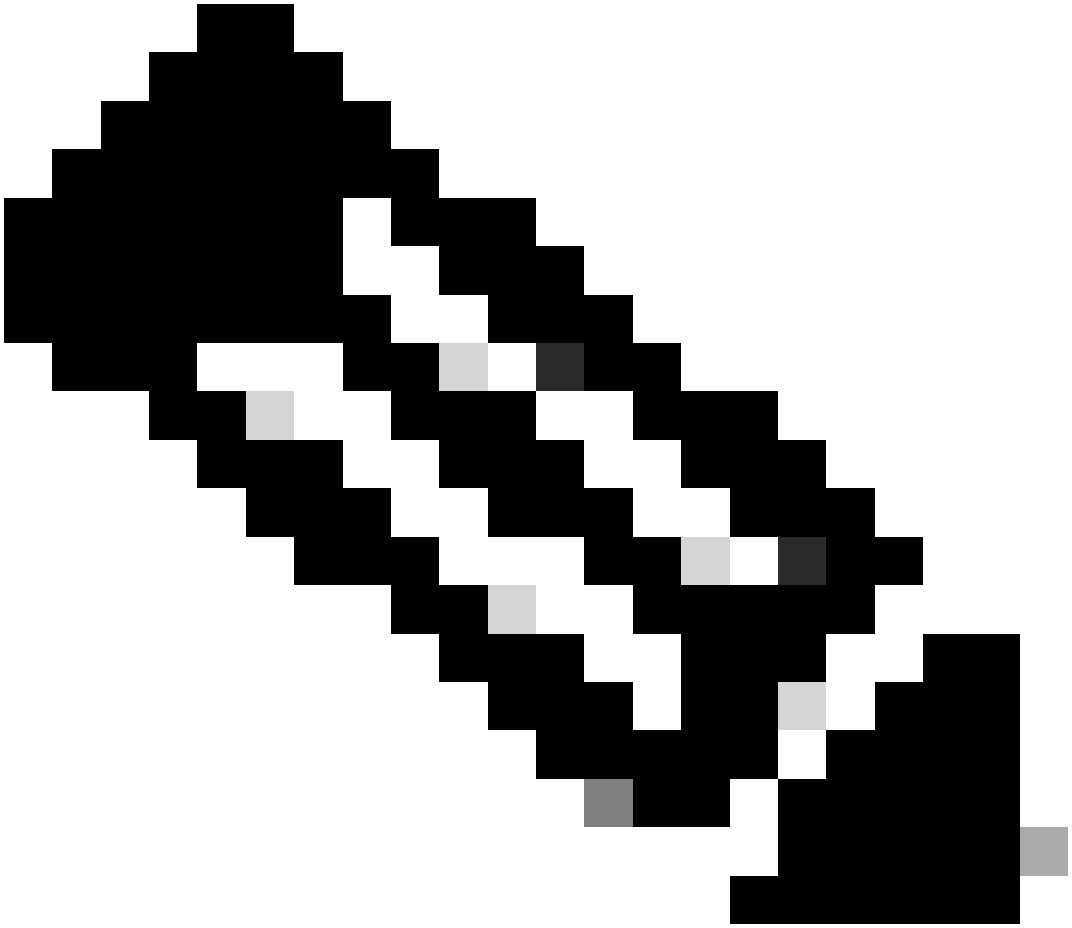
- Complément de cryptage de messagerie Cisco 10.0.0

- Microsoft Exchange Online
- Microsoft Entra ID (anciennement Azure AD)
- Outlook pour O365 (macOS, Windows)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Le complément Cisco Secure Email Encryption Service permet à vos utilisateurs finaux de chiffrer leurs messages directement à partir de Microsoft Outlook en un seul clic. Ce complément peut être déployé sur Microsoft Outlook (pour Windows et macOS) et Outlook Web App.



> Remarque : ce document est idéal pour tous les utilisateurs finaux qui prévoient d'utiliser le complément utilisent l'abonnement Office 365/Microsoft 365 et tous les utilisateurs finaux qui prévoient d'utiliser le complément sont des utilisateurs enregistrés du service

---

Cisco Secure Email Encryption Service.

Meilleures pratiques de déploiement du complément Cisco Secure Email Encryption Service

- Phase de test : déploiement du complément auprès d'un petit groupe d'utilisateurs finaux au sein d'un service ou d'une fonction. Évaluez les résultats et, si vous y parvenez, passez à la phase suivante.
- Phase pilote : déploiement du complément auprès d'un plus grand nombre d'utilisateurs finaux de différents services et fonctions. Évaluez les résultats et, si vous y parvenez, passez à la phase suivante.
- Phase de production - Déployez le composant logiciel enfichable pour tous les utilisateurs.

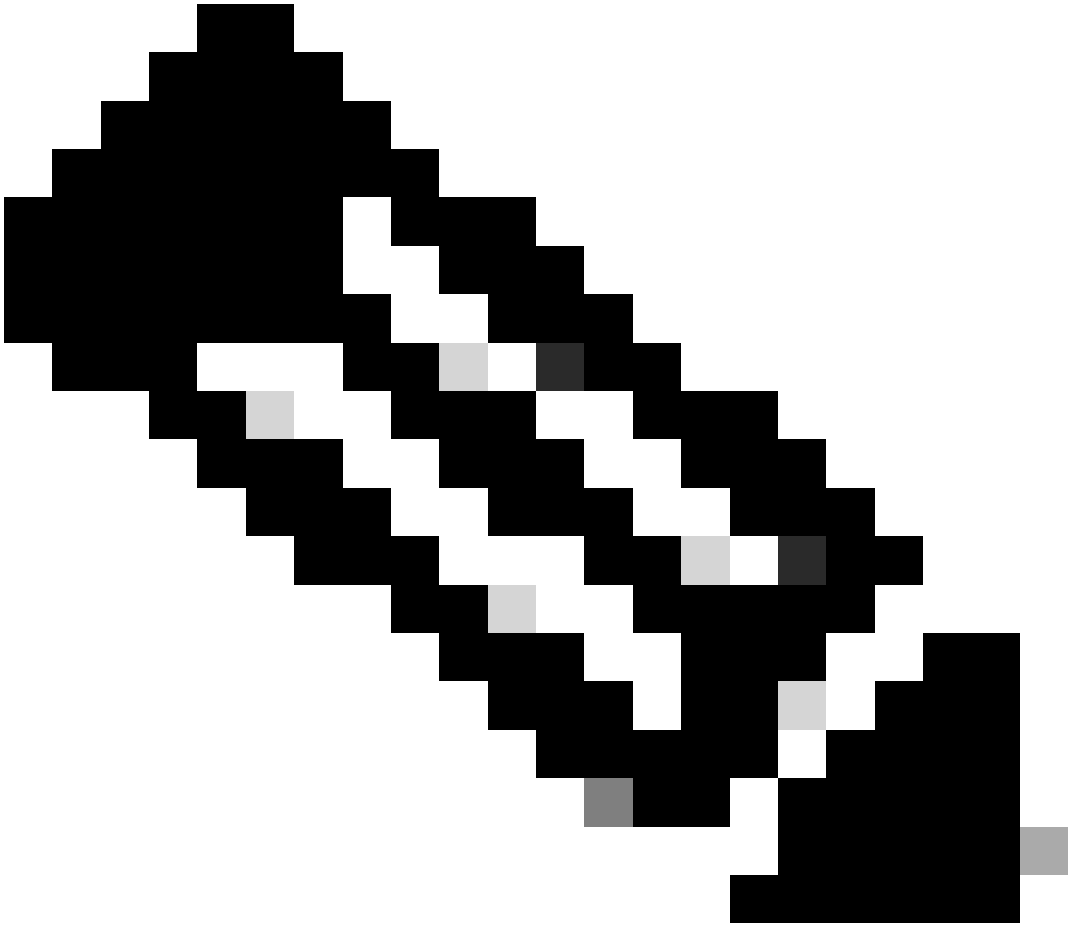
Configurer

Enregistrement de l'application complémentaire Cisco Secure Email Encryption Service

1. Connectez-vous au Centre d'administration Microsoft 365 en tant qu'administrateur d'applications cloud (Centre d'administration Microsoft 365).

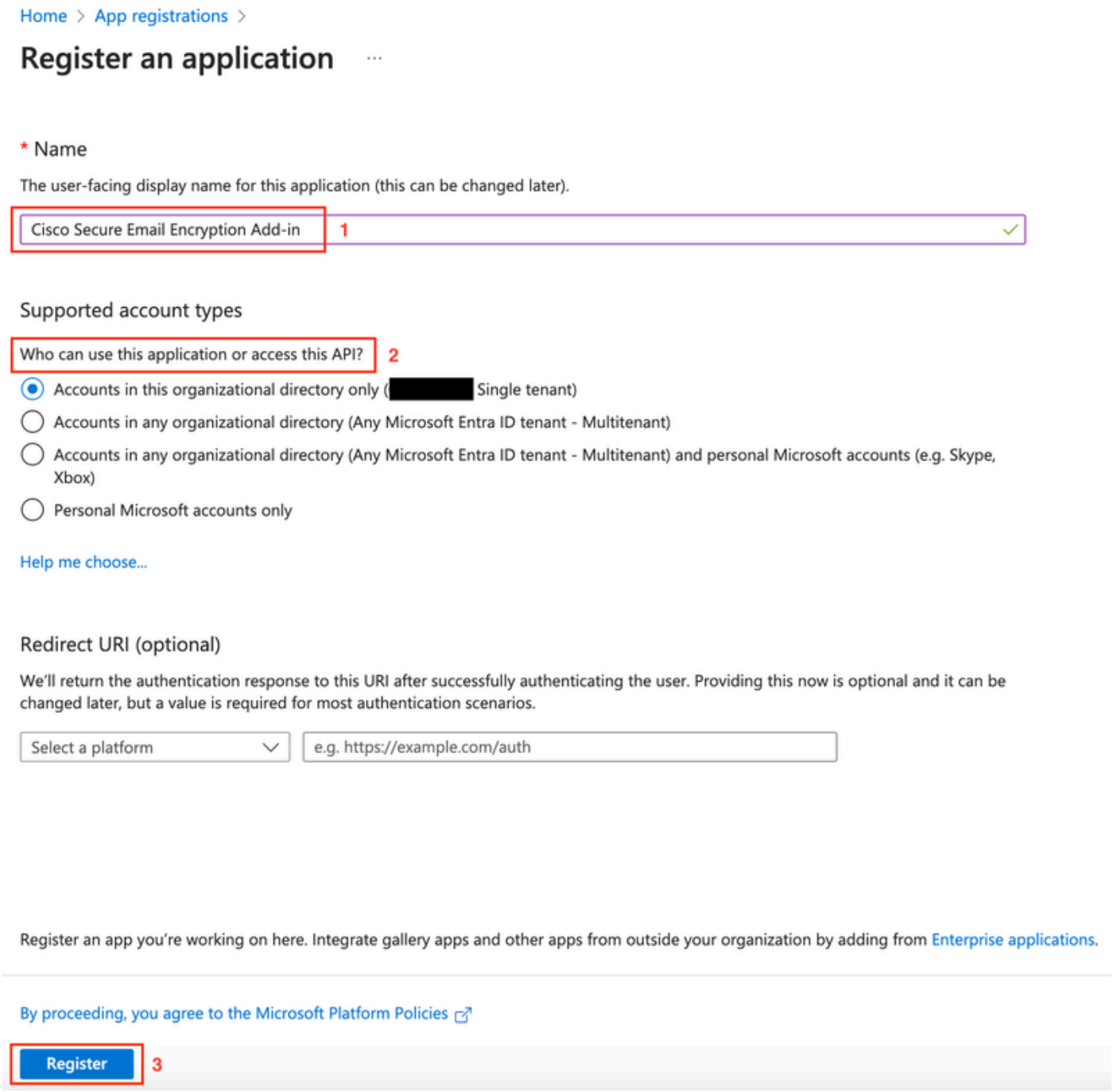
2. Dans le menu de gauche, développez Admin Centerset cliquez sur Identity.

3. Accédez à Identity > Applications > App registrationset sélectionnez New registration.



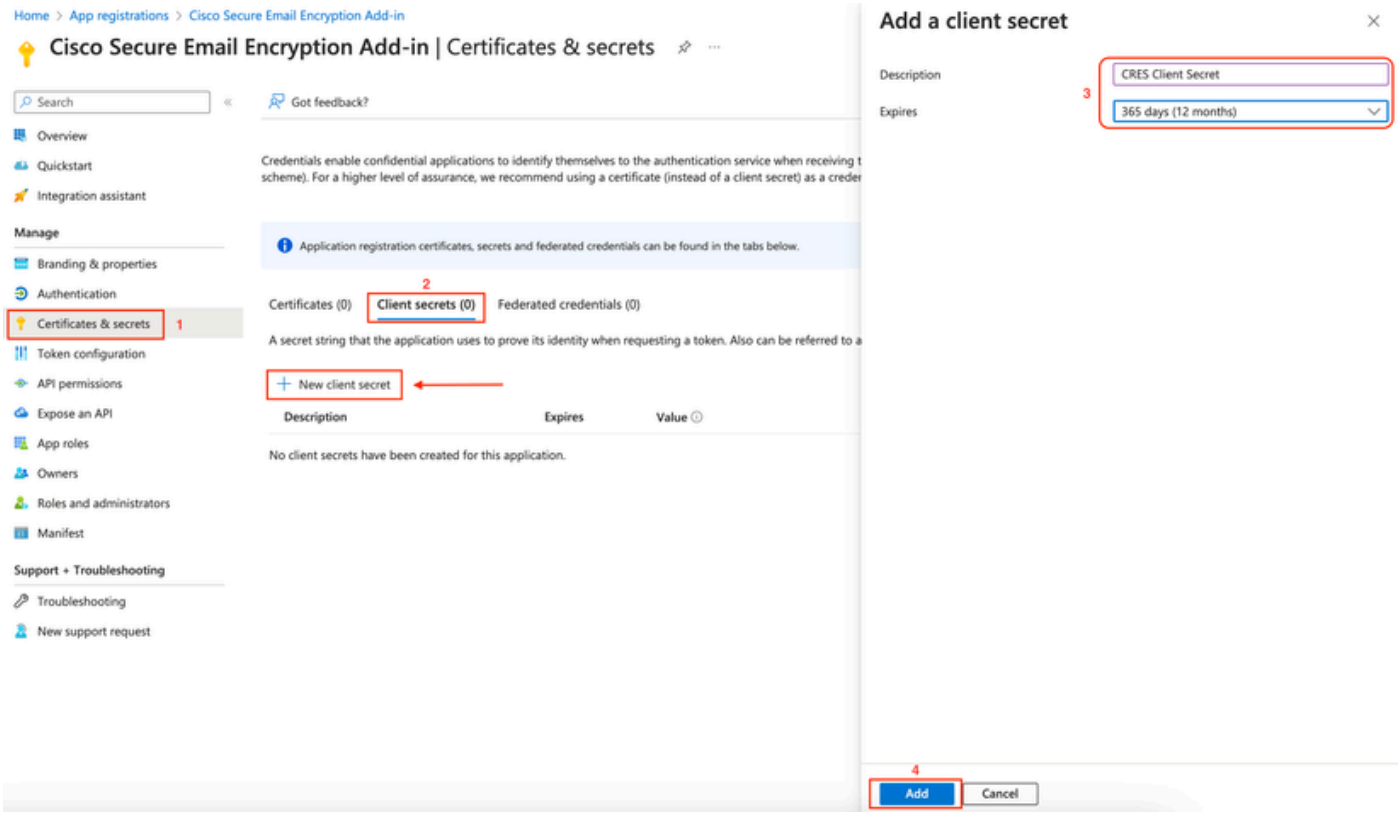
Remarque : si vous avez accès à plusieurs services partagés, utilisez l'icône Paramètres dans le menu supérieur droit pour basculer vers le service partagé dans lequel vous souhaitez enregistrer l'application à partir du menu Répertoires + Abonnements.

4. Entrez un nom d'affichage pour l'application, sélectionnez les comptes qui peuvent utiliser l'application et cliquez sur Register.



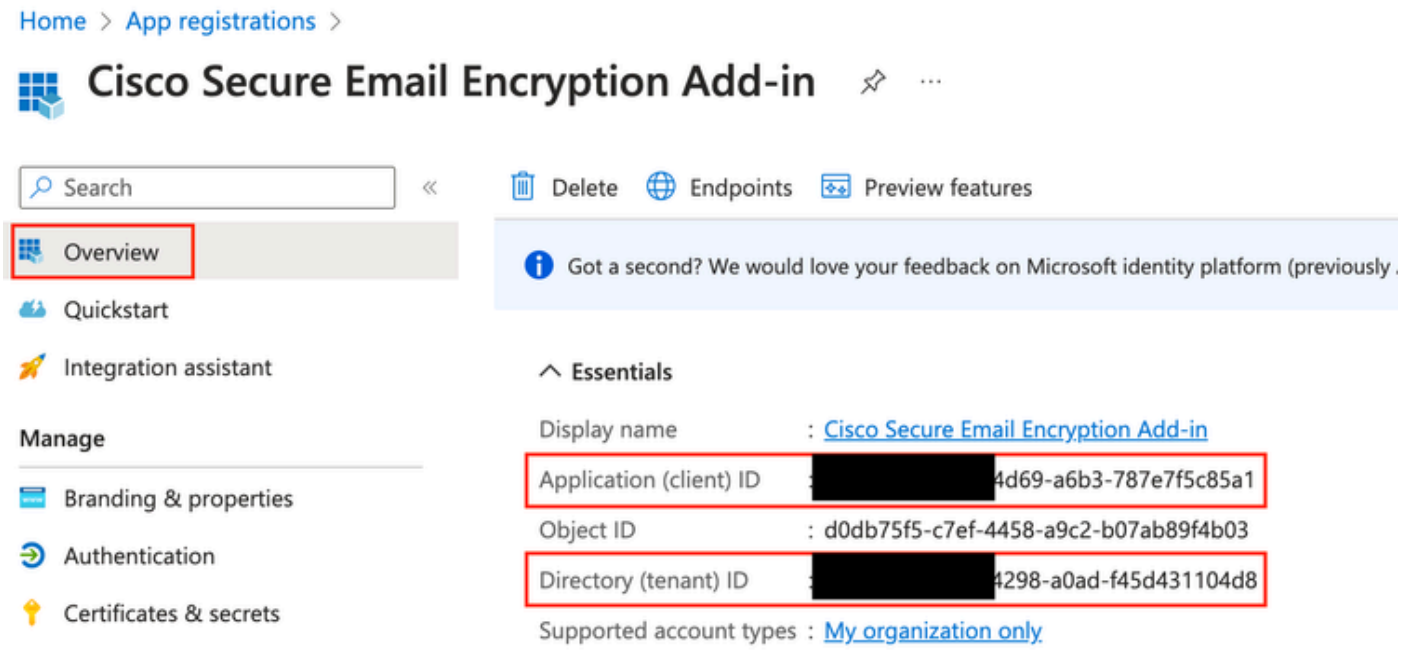
Enregistrer la demande

5. Une fois l'enregistrement réussi, accédez à l'application pour configurer le secret client sous Certificates & Secrets. Sélectionnez l'expiration en fonction de la conformité aux réglementations de l'entreprise.

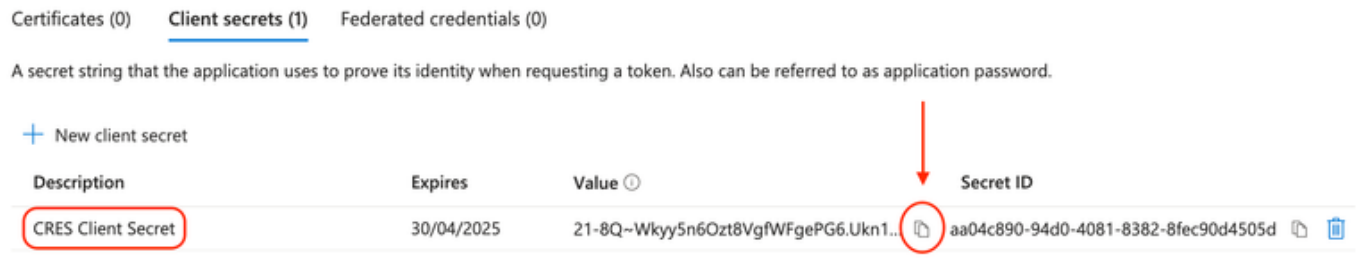


Configurer le secret client

6. Dans la page Aperçu de la demande enregistrée, copiez les Application (client) ID et Directory (tenant) ID. Copiez le **Client Secret** à partir des certificats et des secrets générés à l'étape précédente.



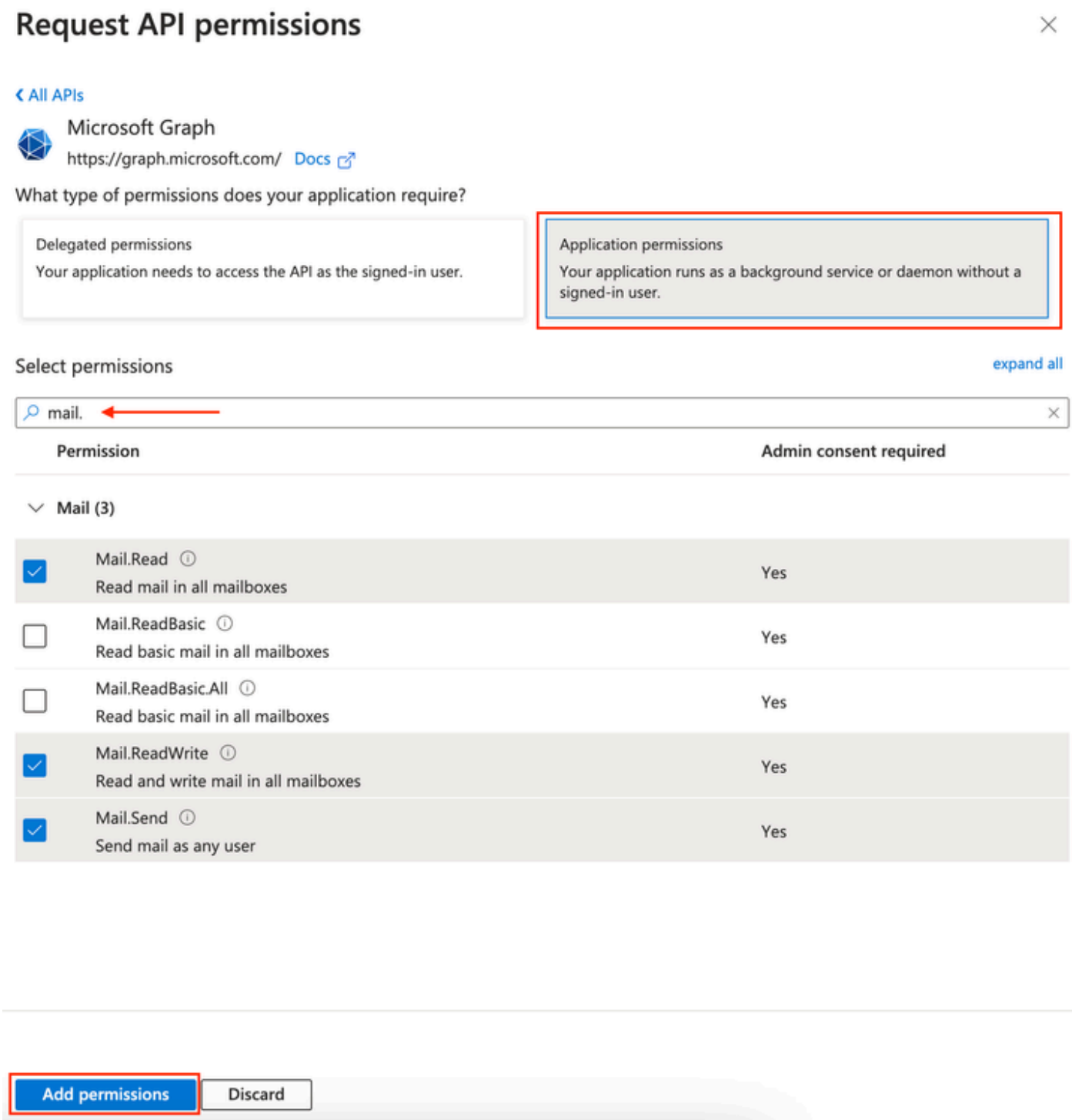
Présentation de l'application Entra ID



Copier le secret client

7. Accédez à l'application Registered Email Encryption et accédez à API permissions. Cliquez sur Add a permission et sélectionnez les autorisations d'application Microsoft Graph requises :

- Courrier.Lu
- Courrier.LectureÉcriture
- Courrier.Envoyer
- Utilisateur.Lire.Tout



Configuration des autorisations Microsoft Graph

7. Cliquez sur Grant Admin Consent for <tenant-name> pour accorder à l'application l'accès aux autorisations au nom de l'organisation.

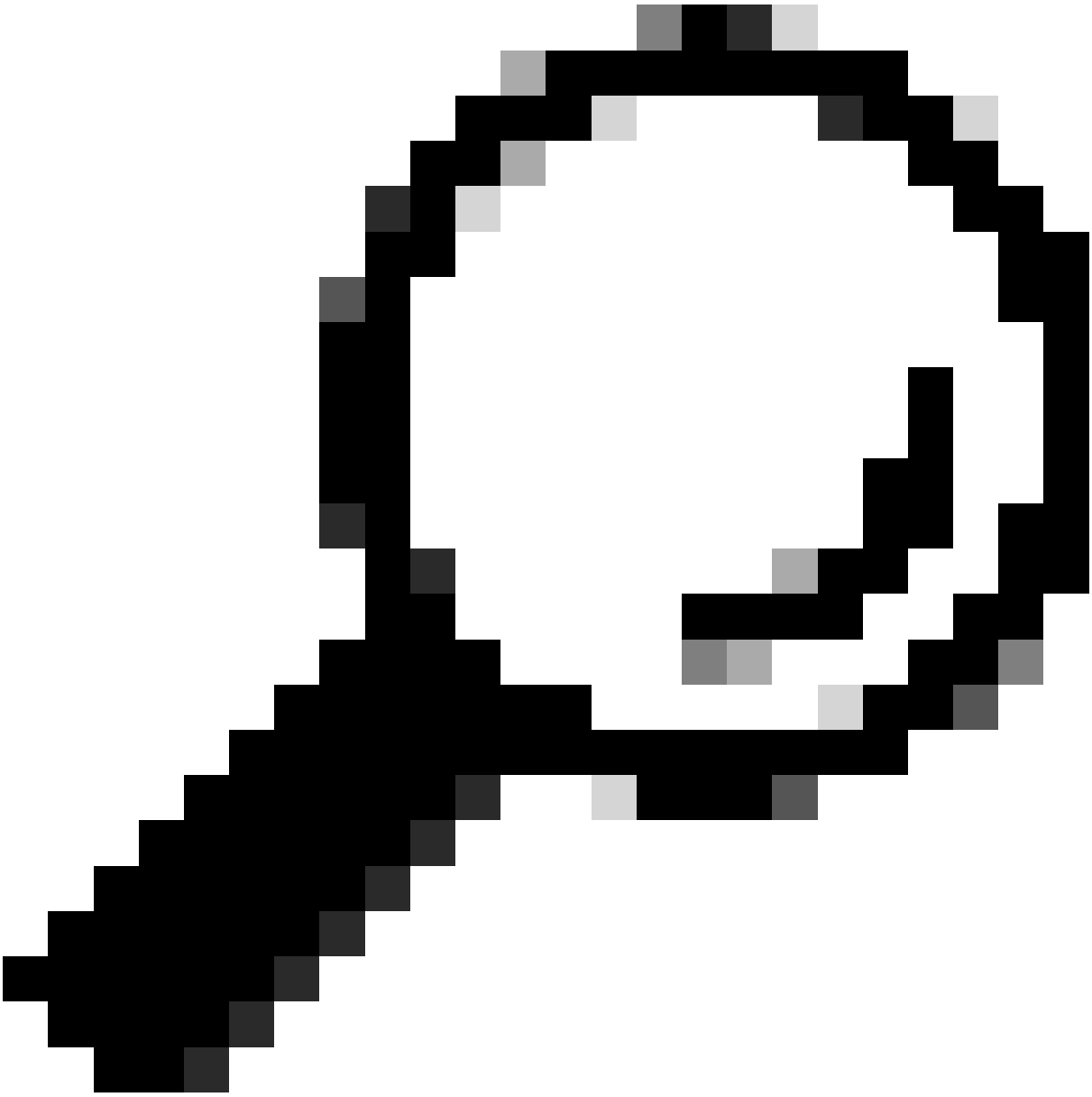
Autorisations API Microsoft Graph

Configurer les paramètres de domaine et de complément sur le portail d'administration de Cisco Secure Email Encryption (CRES)

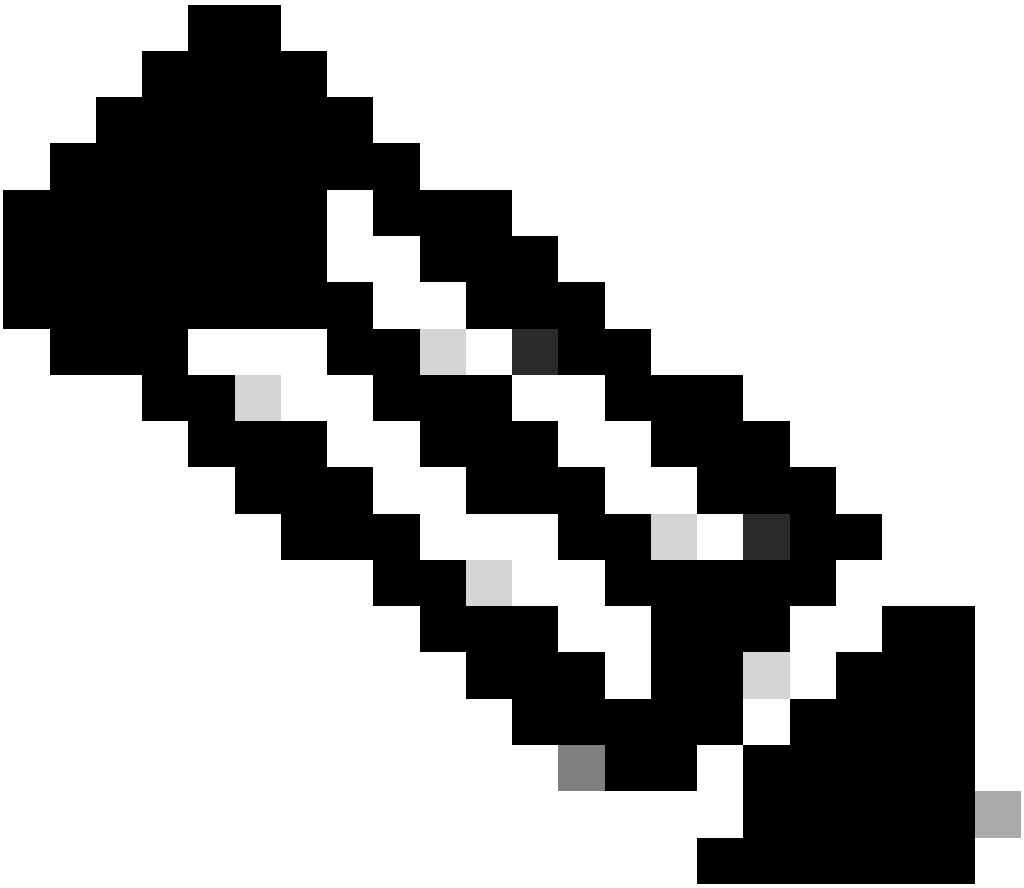
1. Connectez-vous au portail d'administration de Cisco Secure Email Encryption Service (CRES) en tant qu'administrateur de compte. (https://res.cisco.com/admin)

2. Accédez à Accounts > Manage Accounts. Cliquez sur le numéro de compte attribué à votre organisation ou sur le compte sur lequel vous prévoyez de configurer le complément de chiffrement des e-mails.

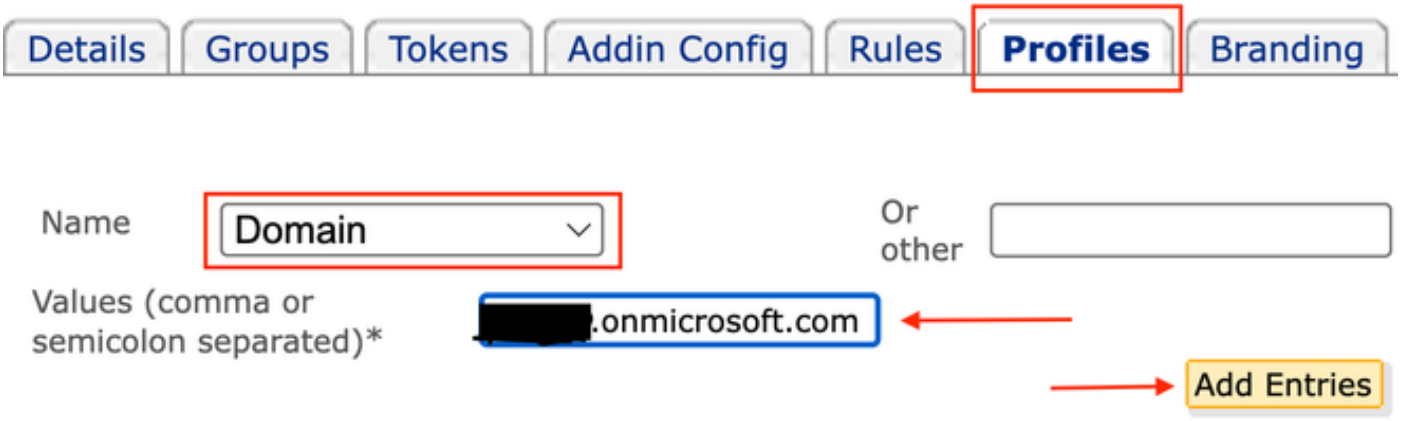
3. Naviguez jusquProfiles'à, sélectionnez le type de nom Domaine et entrez votre nom de domaine de messagerie sous Valeurs. Cliquez sur **Add Entries** et attendez 5 à 10 secondes. (N'actualisez pas la page du navigateur ou ne naviguez pas vers une autre page tant qu'elle n'a pas été ajoutée.)



Conseil : répétez les mêmes étapes pour ajouter d'autres domaines de messagerie qui vont utiliser le service de cryptage des e-mails dans votre organisation.



Remarque : contactez le centre d'assistance technique Cisco pour obtenir l'ajout des domaines de messagerie sur le portail d'administration CRES.

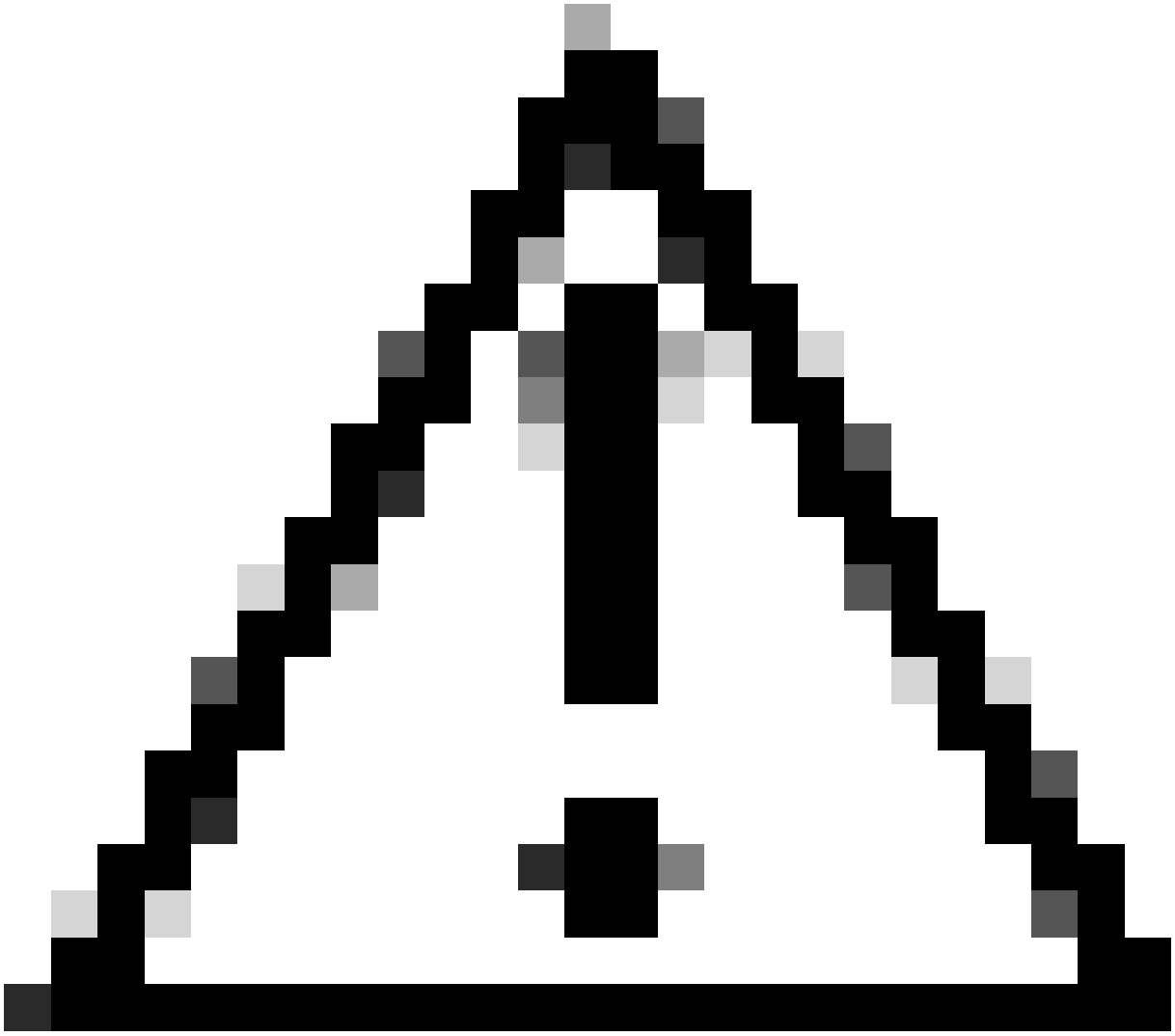


Profils du portail d'administration CRES

4. Accédez à l'Add-in Configonglet.

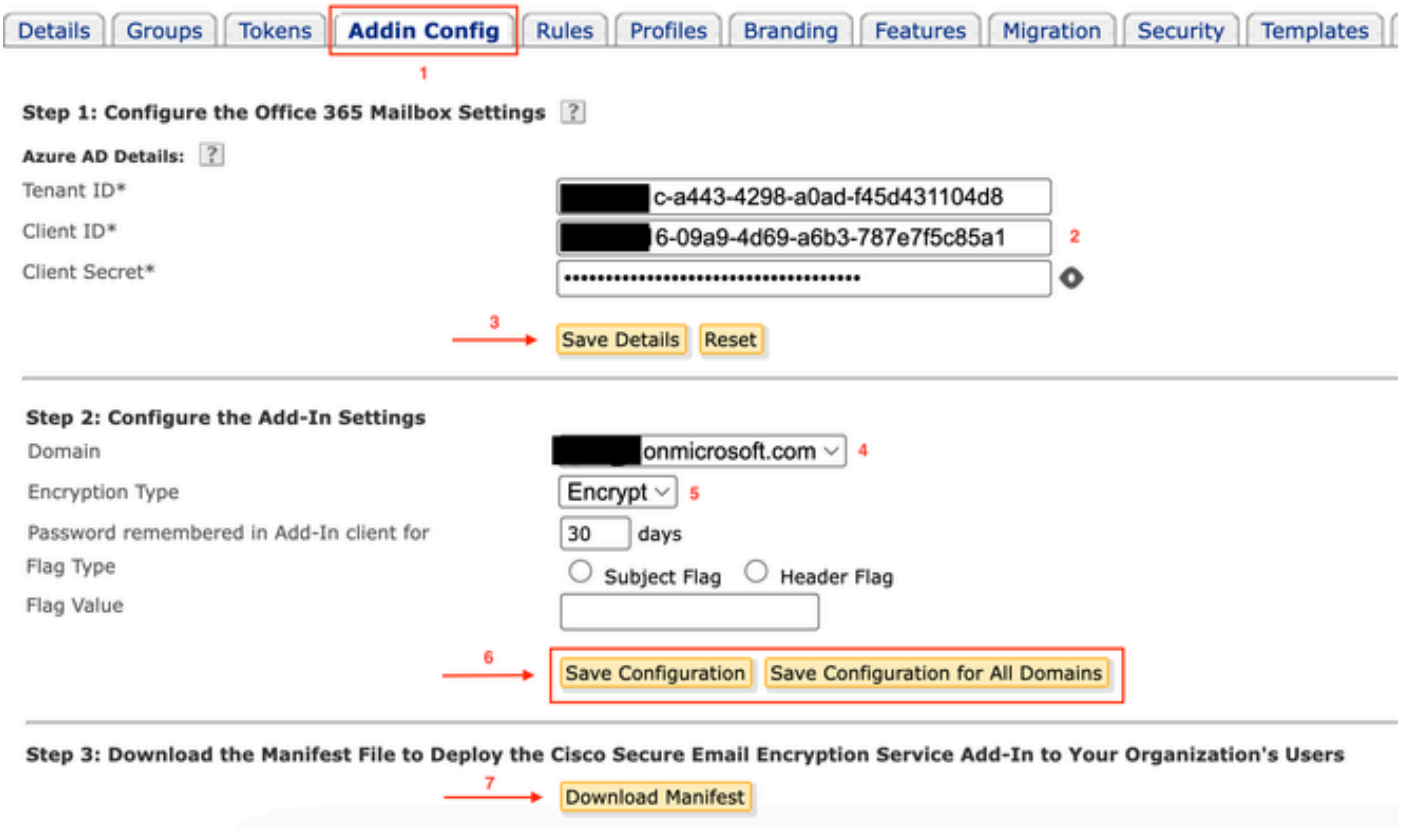
Étape 1 : saisissez le locataire, l'ID client et le secret obtenus à partir de l'ID d'entrée sous Azure AD Details. Cliquez sur Save Details.

Étape 2 : Sélectionnez le domaine, le type de cryptage et cliquez sur Save Configuration. Utilisez Save Configuration pour tous les domaines pour appliquer les mêmes paramètres à tous les domaines ajoutés.



Attention : ne naviguez pas vers une autre page sans avoir terminé les étapes 1 et 2 ensemble. Si l'étape 2. n'est pas terminée simultanément, les détails Azure AD ne seront pas enregistrés.

Étape 3 : Cliquez sur Download Manifest.

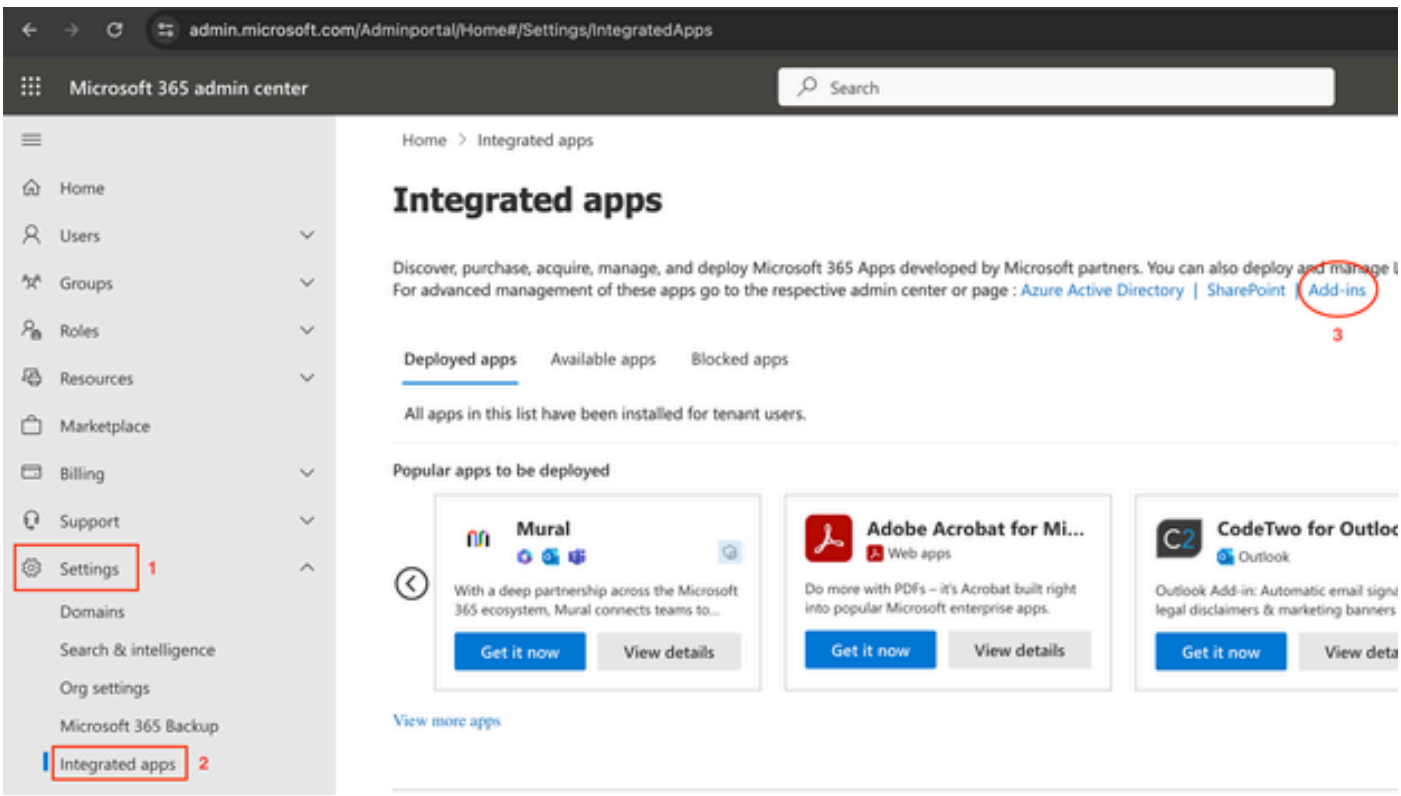


Config. admin. CRES Portal Addin

Télécharger le fichier manifeste vers Microsoft 365 pour déployer le complément Service de cryptage des e-mails

1. Connectez-vous au Centre d'administration Microsoft 365 en tant qu'administrateur. (Centre d'administration Microsoft 365).

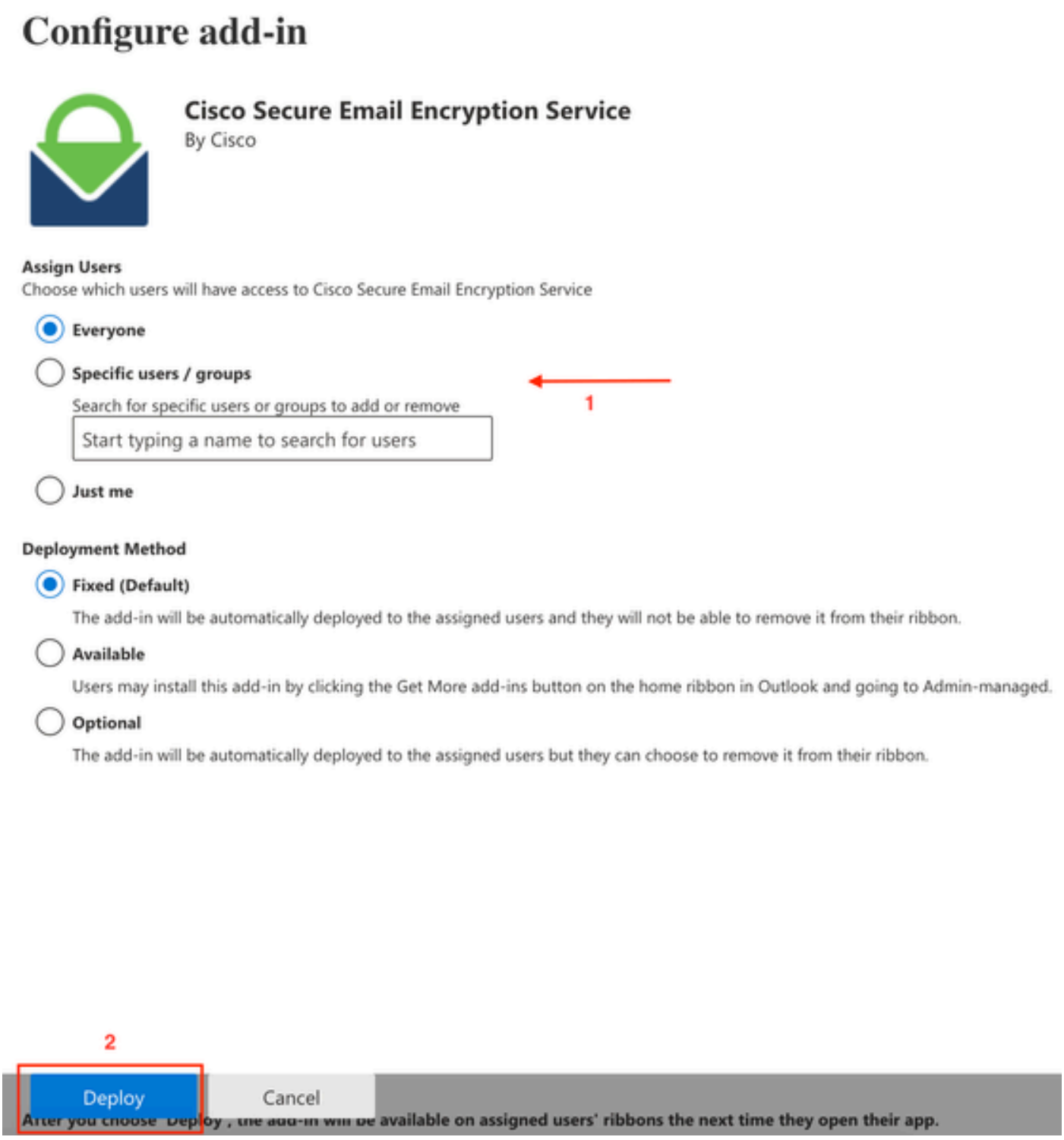
2. Accédez à Settings > Integrated apps et cliquez sur Compléments.



Paramètres d'ajout Microsoft O365

3. Cliquez sur Deploy Add-inet choisissez Upload Custom Apps. Sélectionnez I have the manifest file (.xml) on this deviceet téléchargez le fichier téléchargé à partir du portail d'administration du service de cryptage de messagerie Cisco à l'étape précédente. Cliquez sur Upload.

4. À l'étape suivante, affectez les utilisateurs qui ont besoin d'accéder au service de chiffrement sécurisé de la messagerie Cisco. Pour un déploiement par étapes, choisissez Specifc Users/groupset cliquez sur Deploy.



Configuration du complément Microsoft O365

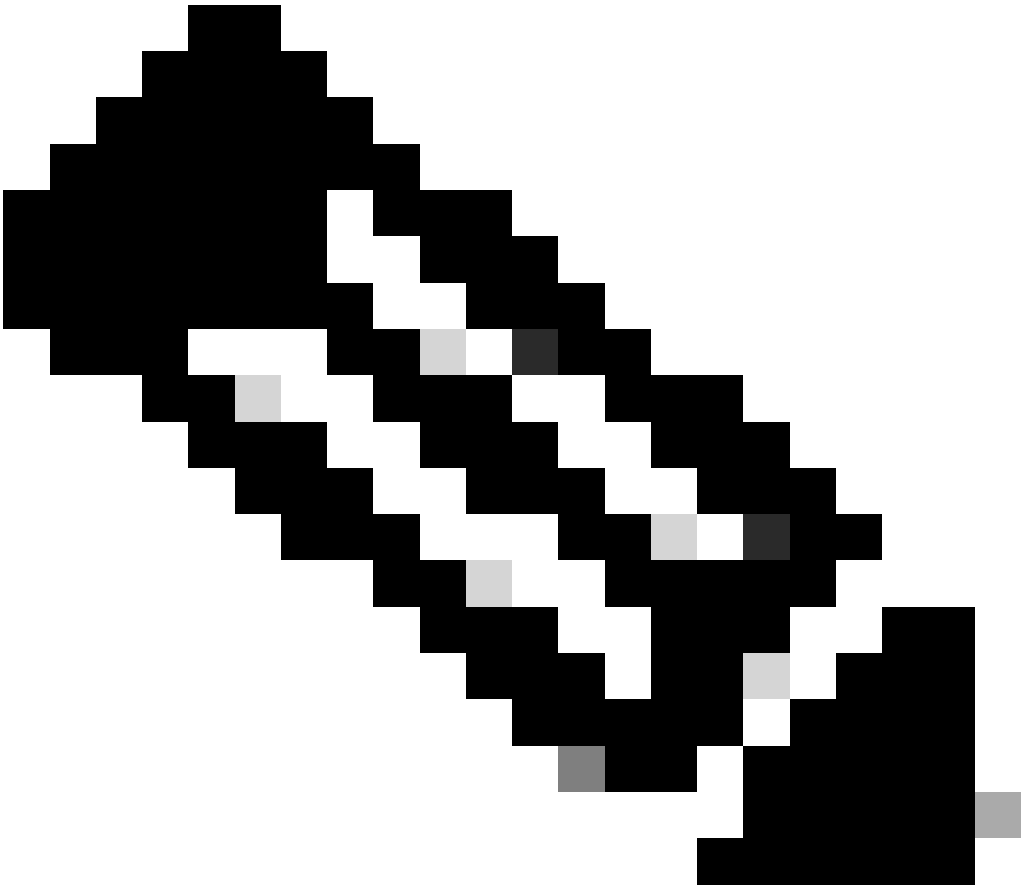
5. Une fois le complément déployé avec succès, son affichage sur les rubans des utilisateurs finaux (client Outlook) peut prendre jusqu'à 12

heures.

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Lancez Outlook pour Office 365/Microsoft 365 ou Outlook Web App, composez le message que vous souhaitez chiffrer et ajoutez au moins un destinataire valide.



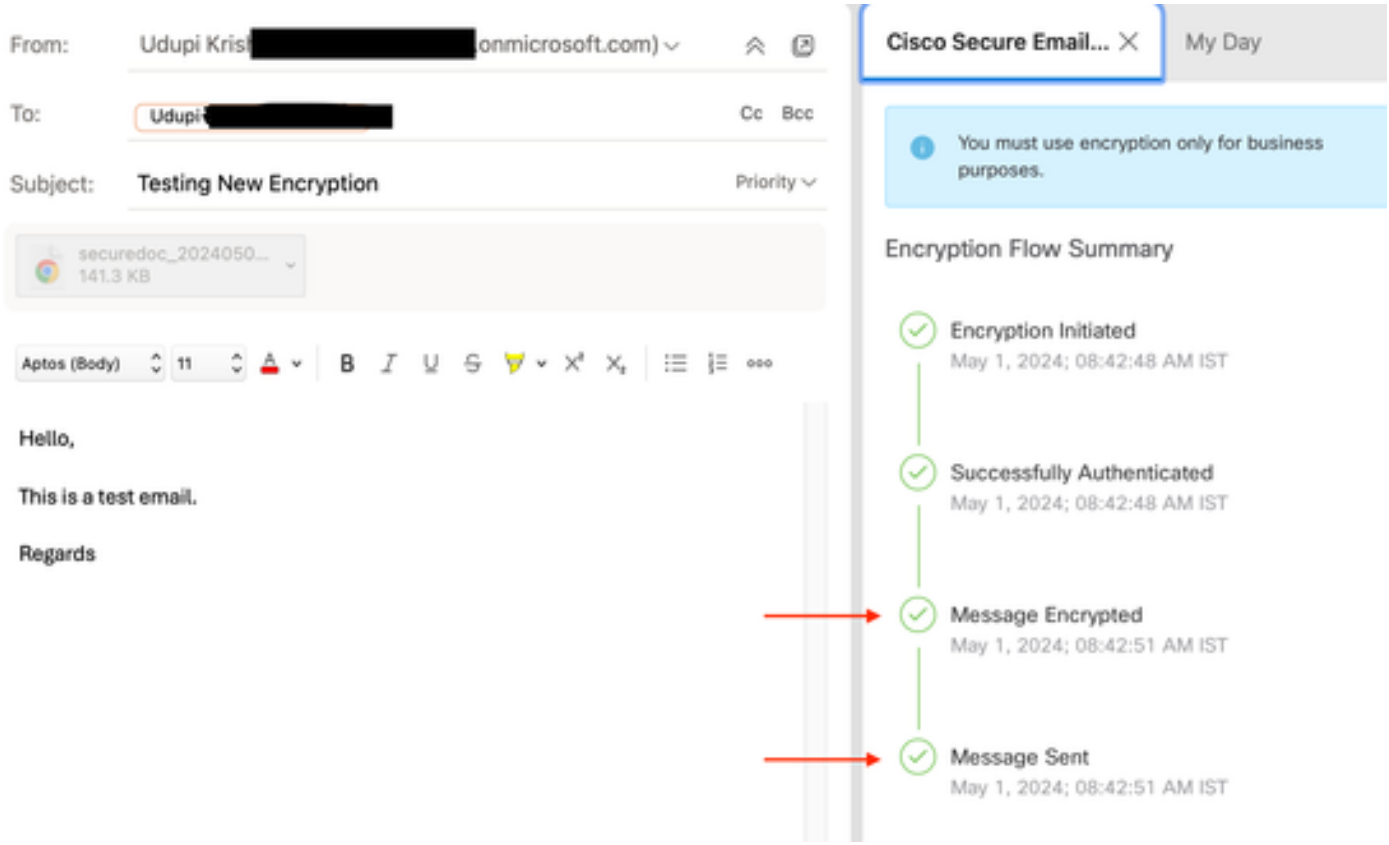
Remarque : si le type de cryptage (défini par l'administrateur) est Crypter, vérifiez que vous avez terminé votre message et ajouté des destinataires valides avant de passer à l'étape suivante. Après l'étape 3, le message est chiffré et envoyé immédiatement.

---

2. Ouvrez/cliquez sur le complément Cisco Secure Email Encryption Service.

- Dans Outlook Web App, cliquez sur l'icône de sélection (située près des boutons Envoyer et Ignorer), puis cliquez sur Cisco Secure Email Encryption Service.
- Dans Outlook pour Windows ou MacOS, cliquez sur Chiffrer dans le ruban ou la barre d'outils.
- Si vous utilisez Outlook pour MacOS version 16.42 ou ultérieure et que vous utilisez l'interface New Outlook, cliquez sur Cisco Secure Email Encryption Service dans la barre d'outils.

3. Entrez vos informations d'identification et cliquez sur Sign in. (Uniquement si le type de cryptage est Indicateur, cliquez sur Send).



État du chiffrement Microsoft Outlook

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations de relation

- Guide de l'administrateur de compte Cisco Secure Email Encryption Service
- Guide de l'utilisateur du complément Cisco Secure Email Encryption Service
- Guide d'enregistrement des applications Microsoft Entra
- **Assistance technique de Cisco et téléchargements**

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.