

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 :

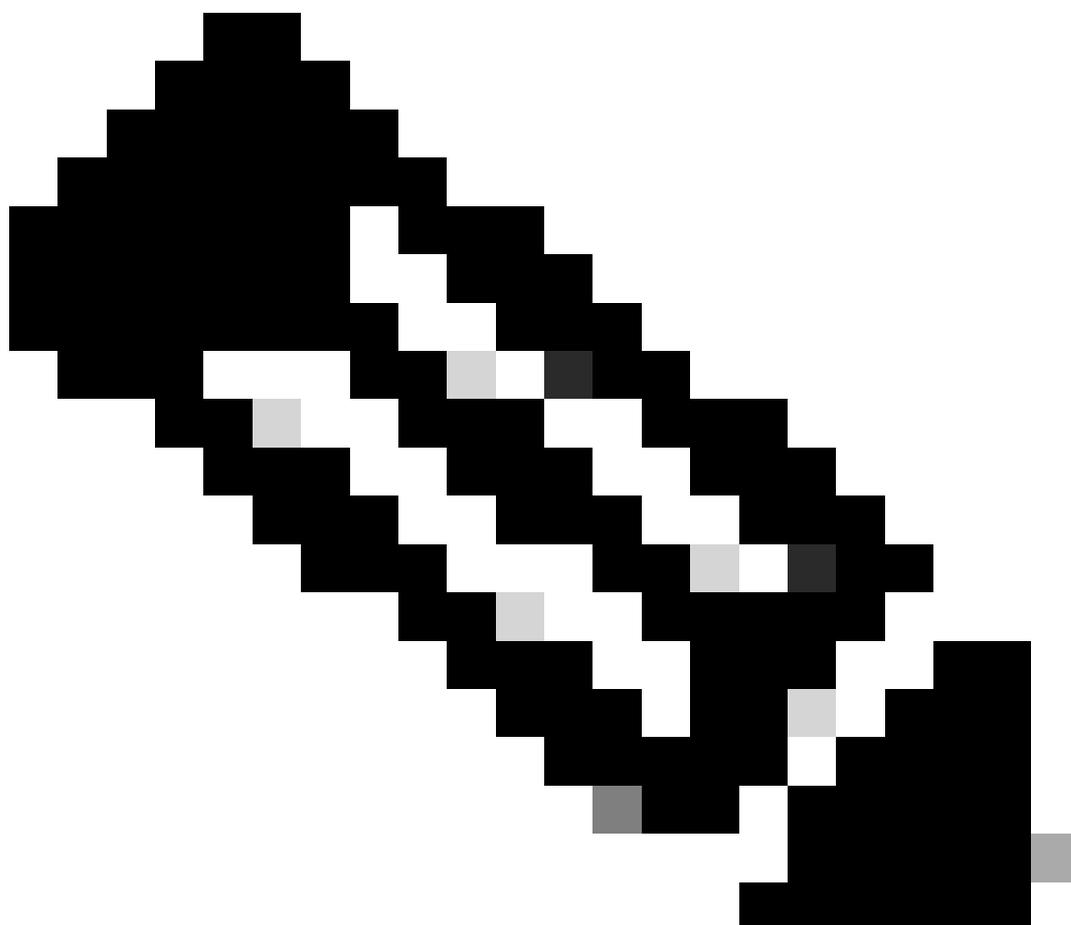
- Complément de cryptage de messagerie Cisco 10.0.0

- 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

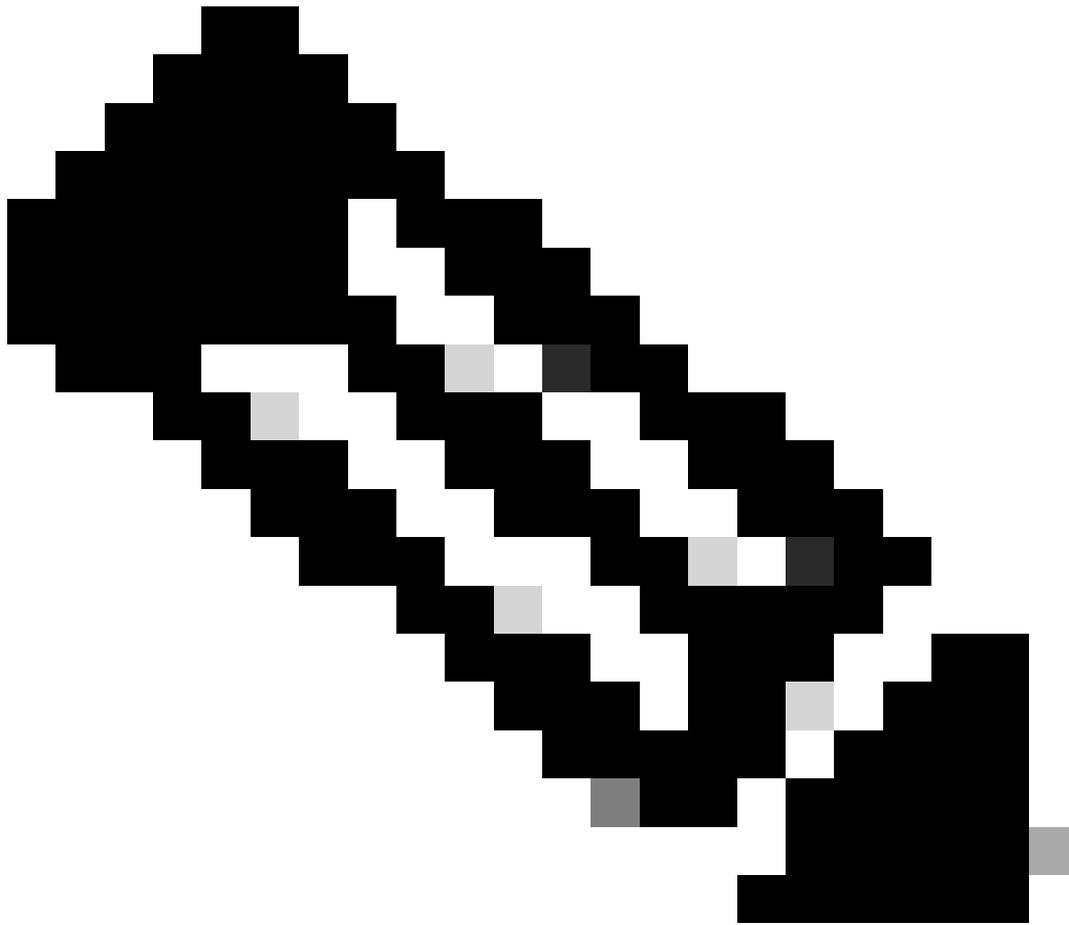
Meilleures pratiques de déploiement du complément Cisco Secure Email Encryption Service

- 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 Centers et cliquez sur Identity.
 3. Accédez à Identity > Applications > App registrations et 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.

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

 1 ✓

Supported account types

 2

- Accounts in this organizational directory only (██████████ Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

 3

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.

Home > App registrations > Cisco Secure Email Encryption Add-in

Cisco Secure Email Encryption Add-in | Certificates & secrets

Search Got feedback?

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets** 1
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens (using a certificate or a client secret scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** 2 Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as a client secret.

+ New client secret ←

Description	Expires	Value
No client secrets have been created for this application.		

Add a client secret ×

Description: 3

Expires: 3

4

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.

Home > App registrations >

Cisco Secure Email Encryption Add-in

Search Delete Endpoints Preview features

- Overview**
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets

Got a second? We would love your feedback on Microsoft identity platform (previously).

Essentials

Display name : [Cisco Secure Email Encryption Add-in](#)

Application (client) ID : ██████████4d69-a6b3-787e7f5c85a1

Object ID : d0db75f5-c7ef-4458-a9c2-b07ab89f4b03

Directory (tenant) ID : ██████████4298-a0ad-f45d431104d8

Supported account types : [My organization only](#)

Présentation de l'application Entra ID

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ	Secret ID
CRES Client Secret	30/04/2025	21-8Q~Wkyy5n6Ozt8VgFWFgePG6.Ukn1...	aa04c890-94d0-4081-8382-8fec90d4505d

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 :

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

Request API permissions



< All APIs



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

mail. ←

Permission	Admin consent required
Mail (3)	
<input checked="" type="checkbox"/> Mail.Read ⓘ Read mail in all mailboxes	Yes
<input type="checkbox"/> Mail.ReadBasic ⓘ Read basic mail in all mailboxes	Yes
<input type="checkbox"/> Mail.ReadBasic.All ⓘ Read basic mail in all mailboxes	Yes
<input checked="" type="checkbox"/> Mail.ReadWrite ⓘ Read and write mail in all mailboxes	Yes
<input checked="" type="checkbox"/> Mail.Send ⓘ Send mail as any user	Yes

Add permissions

Discard

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.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				...
Mail.Read	Application	Read mail in all mailboxes	Yes	✔ Granted for [redacted] ...
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✔ Granted for [redacted] ...
Mail.Send	Application	Send mail as any user	Yes	✔ Granted for [redacted] ...
User.Read.All	Application	Read all users' full profiles	Yes	✔ Granted for [redacted] ...

Autorisations API Microsoft Graph

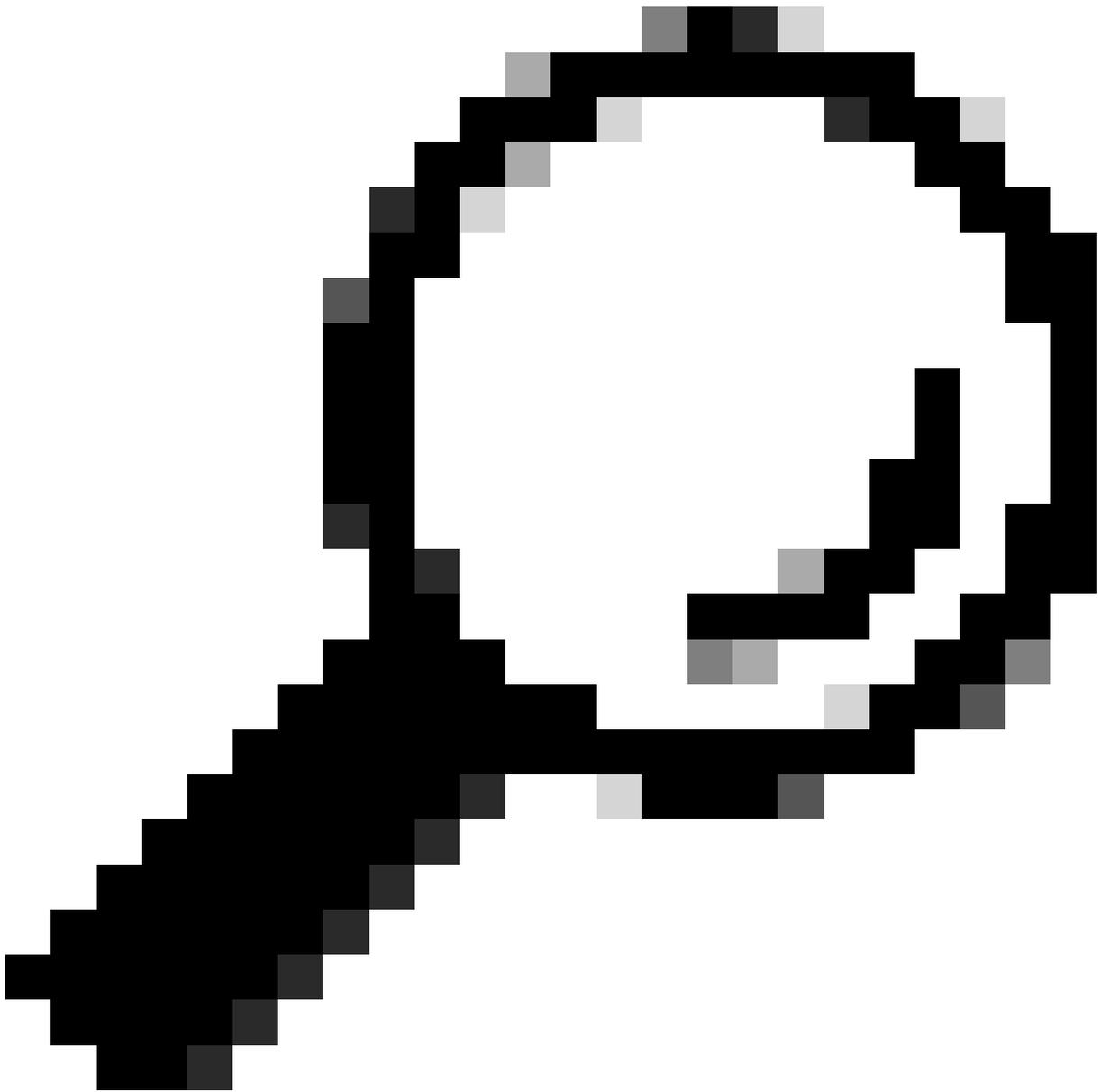
Configurer les paramètres de domaine et de complément sur le portail d'administration de Cisco Secure Email Encryption (CRES)

1. Connectez-vous au portail d'administration de Cisco Secure Email Encryption Service (CRES) en tant qu'administrateur de compte.

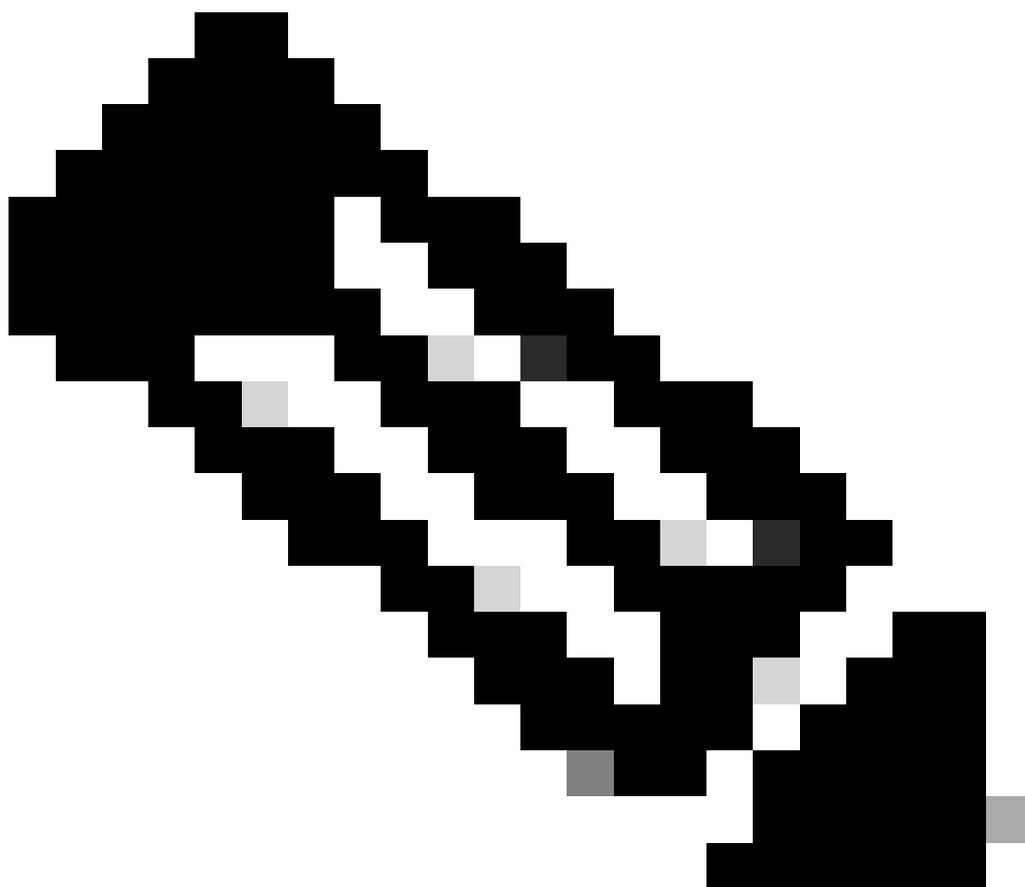
<https://res.cisco.com/admin>

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 jusqu'à **Profiles**, 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.

Details Groups Tokens Addin Config Rules **Profiles** Branding

Name **Domain** Or other

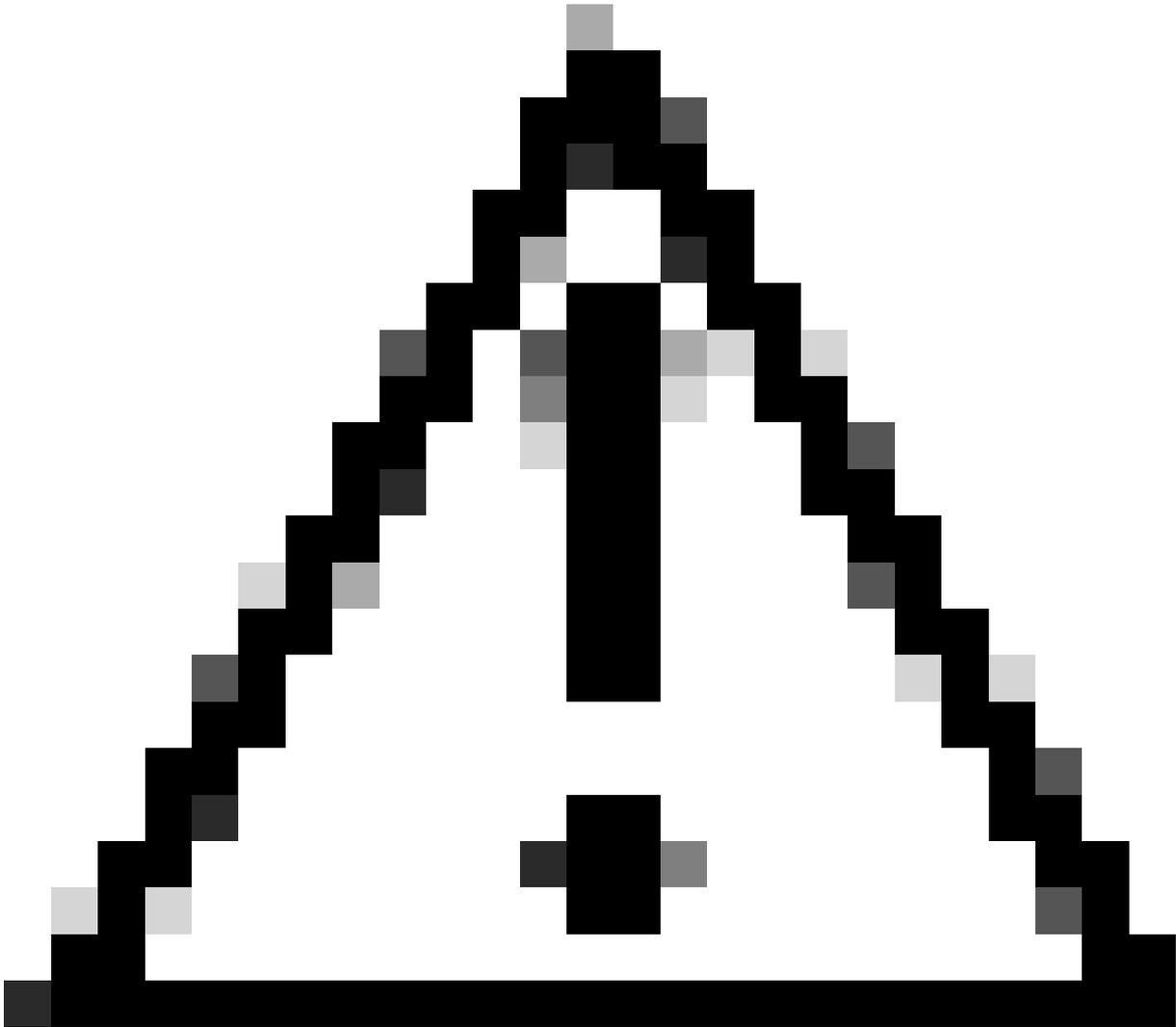
Values (comma or semicolon separated)* **Add Entries**

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.

Details Groups Tokens **Addin Config** Rules Profiles Branding Features Migration Security Templates

1

Step 1: Configure the Office 365 Mailbox Settings ?

Azure AD Details: ?

Tenant ID* [redacted] c-a443-4298-a0ad-f45d431104d8

Client ID* [redacted] 6-09a9-4d69-a6b3-787e7f5c85a1 2

Client Secret* [redacted]

3 → Save Details Reset

Step 2: Configure the Add-In Settings

Domain [redacted] onmicrosoft.com 4

Encryption Type Encrypt 5

Password remembered in Add-In client for 30 days

Flag Type Subject Flag Header Flag

Flag Value [redacted]

6 → Save Configuration Save Configuration for All Domains

Step 3: Download the Manifest File to Deploy the Cisco Secure Email Encryption Service Add-In to Your Organization's Users

7 → 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.

admin.microsoft.com/Adminportal/Home#/Settings/IntegratedApps

Microsoft 365 admin center

Home > Integrated apps

Integrated apps

Discover, purchase, acquire, manage, and deploy Microsoft 365 Apps developed by Microsoft partners. You can also deploy and manage l For advanced management of these apps go to the respective admin center or page : Azure Active Directory | SharePoint | **Add-ins** 3

Deployed apps Available apps Blocked apps

All apps in this list have been installed for tenant users.

Popular apps to be deployed

- Mural**

With a deep partnership across the Microsoft 365 ecosystem, Mural connects teams to...

Get it now View details
- Adobe Acrobat for Mi...**

Do more with PDFs – it's Acrobat built right into popular Microsoft enterprise apps.

Get it now View details
- CodeTwo for Outlook**

Outlook Add-in: Automatic email sign legal disclaimers & marketing banners

Get it now View deta

View more apps

3. Cliquez sur Deploy Add-in choisissez Upload Custom Apps. Sélectionnez I have the manifest file (.xml) on this device et 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 Specific Users/groupset cliquez sur Deploy.

Configure add-in



Cisco Secure Email Encryption Service By Cisco

Assign Users

Choose which users will have access to Cisco Secure Email Encryption Service

Everyone

Specific users / groups

Search for specific users or groups to add or remove

Start typing a name to search for users



Just me

Deployment Method

Fixed (Default)

The add-in will be automatically deployed to the assigned users and they will not be able to remove it from their ribbon.

Available

Users may install this add-in by clicking the Get More add-ins button on the home ribbon in Outlook and going to Admin-managed.

Optional

The add-in will be automatically deployed to the assigned users but they can choose to remove it from their ribbon.

2

Deploy

Cancel

After you choose Deploy, the add-in will be available on assigned users' ribbons the next time they open their app.

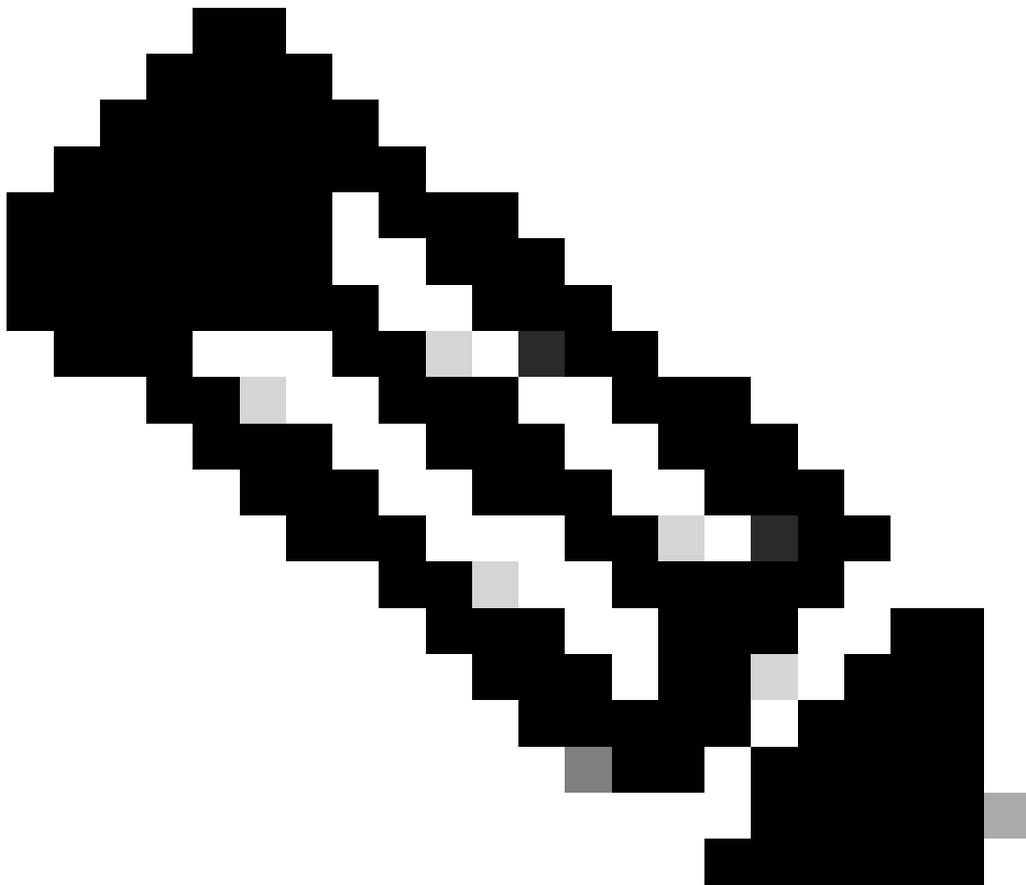
5. Une fois le complément déployé avec succès, son affichage sur les rubans des utilisateurs finaux (client Outlook) peut prendre jusqu'à 12

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).

The screenshot displays an Outlook email composition window. The 'From' field is 'Udupi Kris [redacted]@onmicrosoft.com', 'To' is 'Udupi [redacted]', and the subject is 'Testing New Encryption'. A file named 'securedoc_2024050...' (141.3 KB) is attached. The email body contains the text: 'Hello, This is a test email. Regards'. On the right side, a 'Cisco Secure Email...' pane is open, showing a notification: 'You must use encryption only for business purposes.' Below this is an 'Encryption Flow Summary' section with a vertical timeline of events: 'Encryption Initiated' (May 1, 2024; 08:42:48 AM IST), 'Successfully Authenticated' (May 1, 2024; 08:42:48 AM IST), 'Message Encrypted' (May 1, 2024; 08:42:51 AM IST), and 'Message Sent' (May 1, 2024; 08:42:51 AM IST). Red arrows point from the left side of the pane to the 'Message Encrypted' and 'Message Sent' steps.

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.