

# Add-in voor e-mailencryptie configureren met Microsoft O365

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Beste praktijken voor het implementeren van de Cisco Secure Email Encryption Service-add-in](#)

[Configureren](#)

[Cisco Secure Email Encryption Service - add-in toepassingsregistratie](#)

[Domain en Add-in-instellingen configureren op Cisco Secure Email Encryption \(CRES\) Admin-portal](#)

[Manifest File uploaden naar Microsoft 365 om e-mail encryptie-service add-in te implementeren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Relatie-informatie](#)

---

## Inleiding

Dit document beschrijft hoe u de Cisco Email Encryption Service add-in gecentraliseerde implementatie via Microsoft Office 365 kunt configureren.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco beveiligde e-mailgateway
- Cisco Secure Email Encryption-service (voorheen bekend als Cisco Registered Envelope Service)
- Microsoft O365 Suites (Exchange, Entra ID, Outlook)

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco e-mailencryptie add-in 10.0.0
- Microsoft Exchange Online

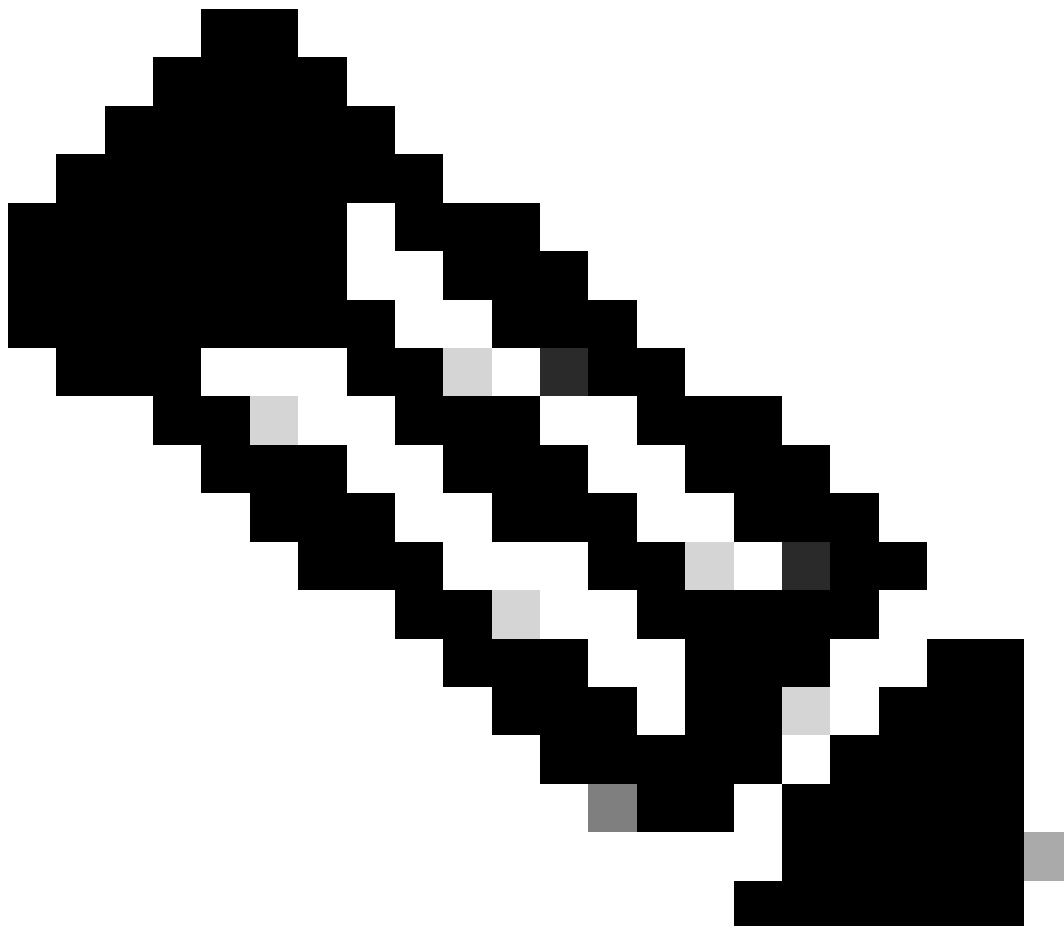
- Microsoft Entra ID (voorheen bekend als Azure AD)
- Outlook voor UCS O365 (macOS, Windows)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

Met de Cisco Secure Email Encryption Service Add-in kunnen uw eindgebruikers hun berichten rechtstreeks vanuit Microsoft Outlook met één klik versleutelen. Deze add-in kan worden ingezet op Microsoft Outlook (Windows en MacOS) en Outlook Web App.

---



Opmerking: dit document is ideaal voor alle eindgebruikers die van plan zijn het Office 365/Microsoft 365-abonnement te gebruiken en alle eindgebruikers die van plan zijn de invoegtoepassing te gebruiken, zijn geregistreerde Cisco Secure Email Encryption

---

---

Service-gebruikers.

---

## Beste praktijken voor het implementeren van de Cisco Secure Email Encryption Service-add-in

- Testfase - implementeer de invoegtoepassing op een kleine set eindgebruikers binnen een afdeling of functie. Evalueer de resultaten en ga, indien geslaagd, over naar de volgende fase.
- Proeffase - De invoegtoepassing implementeren voor meer eindgebruikers uit verschillende afdelingen en functies. Evalueer de resultaten en ga, indien geslaagd, over naar de volgende fase.
- Productiefase - implementeer de invoegtoepassing voor alle gebruikers.

## Configureren

### Cisco Secure Email Encryption Service - add-in toepassingsregistratie

1. Log in bij Microsoft 365 Admin Center als ten minste een Cloud Application Administrator ([Microsoft 365 Admin Center](#)).
  2. Vouw het linker menu op Admin Centersen klik op Identity.
  3. Navigeer naar Identity > Applications > App registrationsen selecteer New registration.
- 
-



**Opmerking:** Als u toegang hebt tot meerdere huurders, gebruik dan het pictogram Settings in het rechterbovenmenu om naar de huurder te switches waarin u de toepassing wilt registreren vanuit het menu Directories + abonnementen.

---

4. Voer een weergavenaam in voor de toepassing, selecteer accounts die de toepassing kunnen gebruiken en klik op Register.

# Register an application ...

## \* Name

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

Cisco Secure Email Encryption Add-in

1



## Supported account types

Who can use this application or access this API?

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.

Select a platform



e.g. https://example.com/auth

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](#)

Register

3

*Toepassing registreren*

5. Nadat de registratie is geslaagd, navigeer dan naar de Toepassing om het Clientgeheim te configureren onder Certificates & Secrets. Kies de verlooptdatum op basis van de naleving van de regelgeving van de organisatie.

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

Clientgeheim configureren

6. Kopieer de Application (client) ID en de inhoud van de pagina Overzicht van de geregistreerde toepassing Directory (tenant) ID. Kopieer de gegevens **Client Secret** van Certificaten en geheimen die in de vorige stap zijn gegenereerd.

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](#)

Entra ID Application - Overzicht

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

*Clientgeheim kopiëren*

7. Ga naar de toepassing voor geregistreerde e-mailencryptie en ga naar API permissions. Klik op Add a permission en selecteer de gewenste Microsoft Graph Application Permissions:

- Mail.Read
- Mail.ReadWrite
- Mail.Verzenden
- Gebruiker.Read.All

# 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

Microsoft Graph-toegangsconfiguratie

7. Klik Grant Admin Consent for <tenant-name> om de toepassing namens de organisatie toegang tot toegangsrechten te geven.

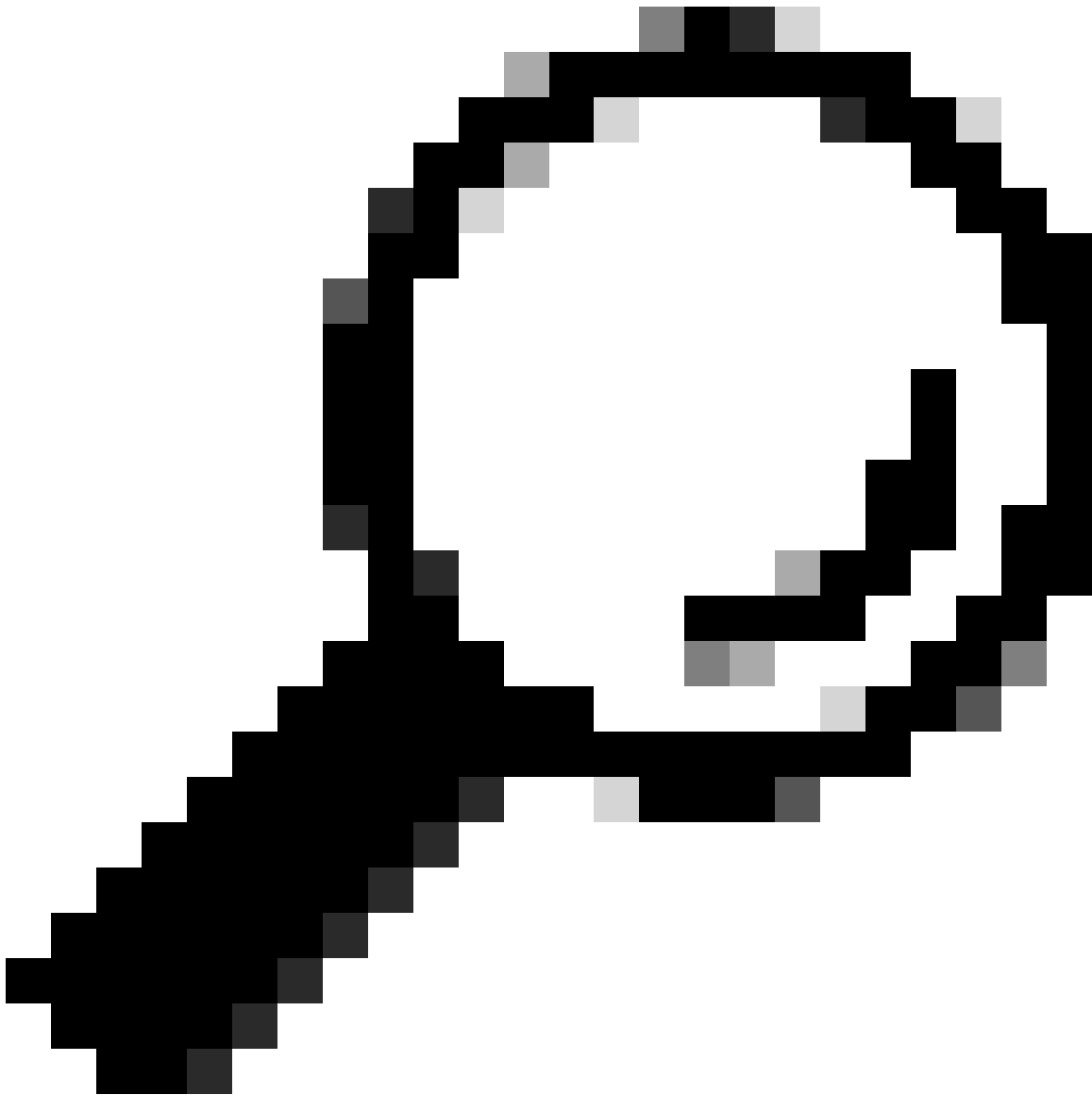
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				...
Mail.Read	Application	Read mail in all mailboxes	Yes	✔ Granted for [redacted] ...
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✔ Granted for [redacted] ...
Mail.Send	Application	Send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

Microsoft Graph API-toegangsrechten



## Domain en Add-in-instellingen configureren op Cisco Secure Email Encryption (CRES) Admin-portal

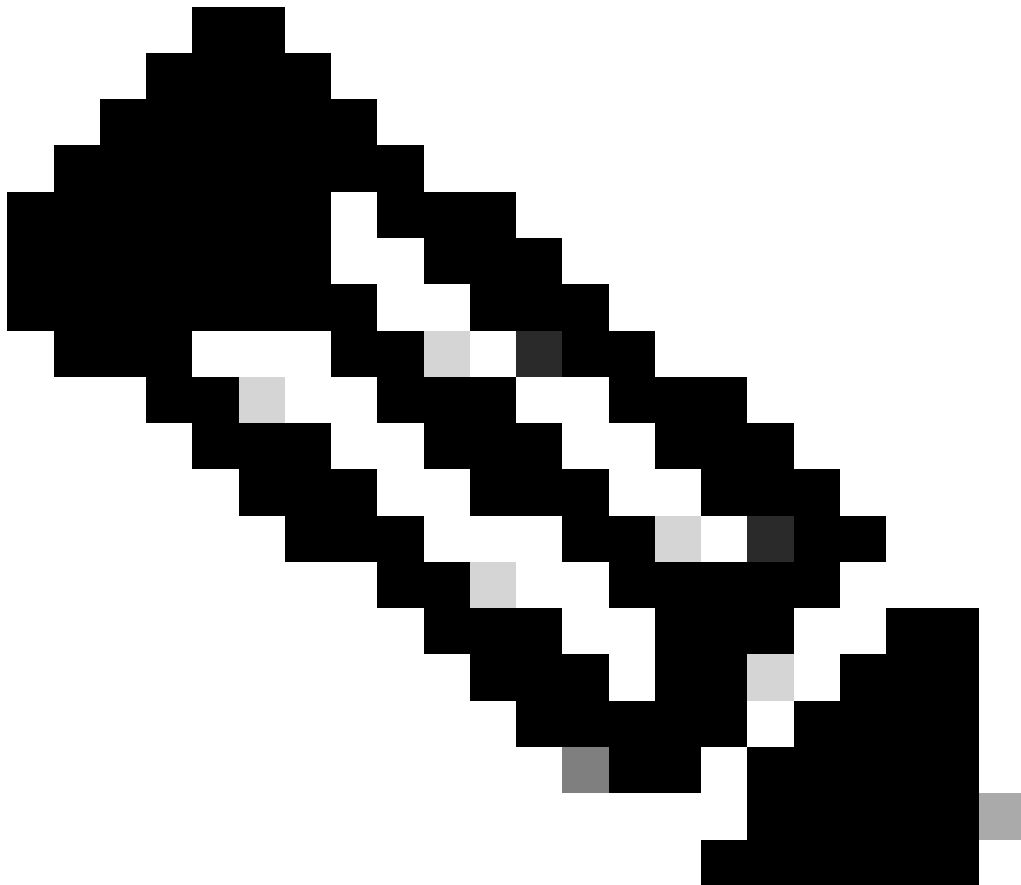
1. Meld u aan bij Cisco Secure Email Encryption Service (CRES) Admin Portal als accountbeheerder. (<https://res.cisco.com/admin>)
2. Navigeer naar Accounts > Manage Accounts. Klik op het accountnummer dat is toegewezen aan uw organisatie of de account waarop u e-mailencryptie-invoegtoepassing wilt configureren.
3. Navigeer Profiles naar, selecteer het type Naam als Domein en voer uw e-maildomeinnaam in onder Waarden. Klik **Add Entries** en wacht 5 tot 10 seconden. (Verfris de browser pagina niet en navigeer niet naar een andere pagina totdat deze met succes is toegevoegd).



---

**Tip:** herhaal dezelfde stappen om andere e-maildomeinen toe te voegen die gebruik zullen maken van de e-mailcryptieservice binnen uw organisatie.

---



**Opmerking:** neem contact op met het Cisco Technical Assistance Center om de e-maildomeinen toe te voegen aan het CRES Admin Portal.

---

---

---

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

Name **Domain** Or other

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

*Profielen van CRES-beheerportal*

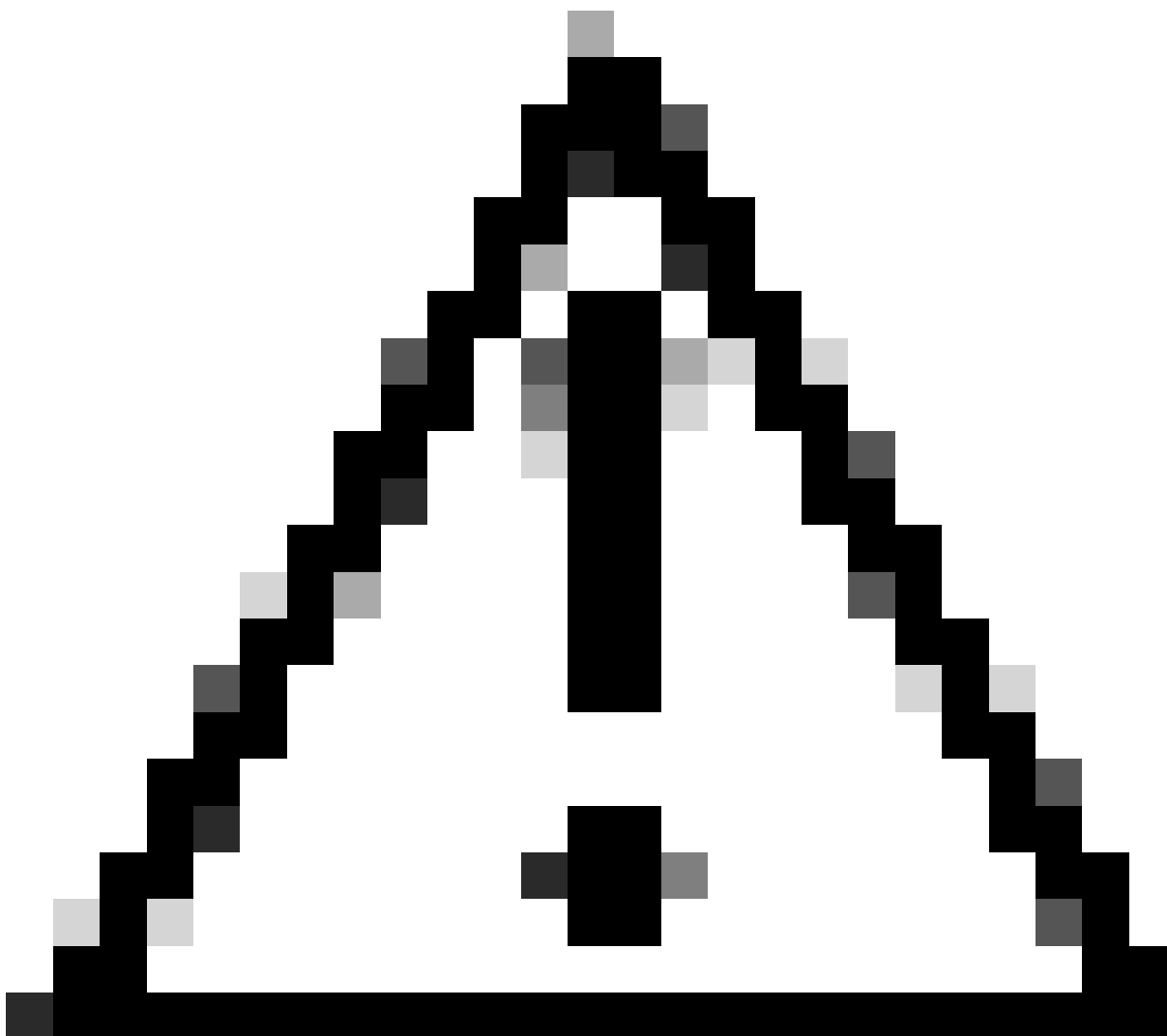
#### 4. Navigeren naar Add-in Configtabblad

Stap 1: Voer de huurder, client-ID en geheim in die verkregen zijn van Entra-ID onder Azure AD Details. Klik op de knop .Save Details

Stap 2: Selecteer het domein, Encryptie Type en klik Save Configuration. Gebruik Save Configuration voor Alle domeinen om dezelfde instellingen toe te passen op alle toegevoegde domeinen.

---

---



**Waarschuwing:** navigeer niet naar een andere pagina zonder Stap 1 en Stap 2 samen te voltooien. Als Stap 2. niet gelijktijdig wordt voltooid, worden Azure AD-gegevens niet opgeslagen.

---

Stap 3: Klik op 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

Admin-adresconfiguratie van CRES-beheerportal

Manifest File uploaden naar Microsoft 365 om e-mail encryptie-service add-in te implementeren

1. Log in bij Microsoft 365 Admin Center als beheerder. ([Microsoft 365 Admin Center](#))

2. Navigeer naar Settings > Integrated apps en klik op Add-ins.

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...**

Web apps

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

Get it now View details
- CodeTwo for Outlook**

Outlook

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

Get it now View deta

View more apps

3. Klik Deploy Add-inen kies Upload Custom Apps. Selecteer I have the manifest file (.xml) on this device en upload het bestand dat u hebt gedownload van de Cisco Email Encryption Service Admin Portal uit de vorige stap. Klik op de knop Upload

4. Wijs in de volgende stap gebruikers toe die toegang nodig hebben tot Cisco Secure Email Encryption Service. Voor een gefaseerde manier van plaatsing, kies Specific Users/groups en klik 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.

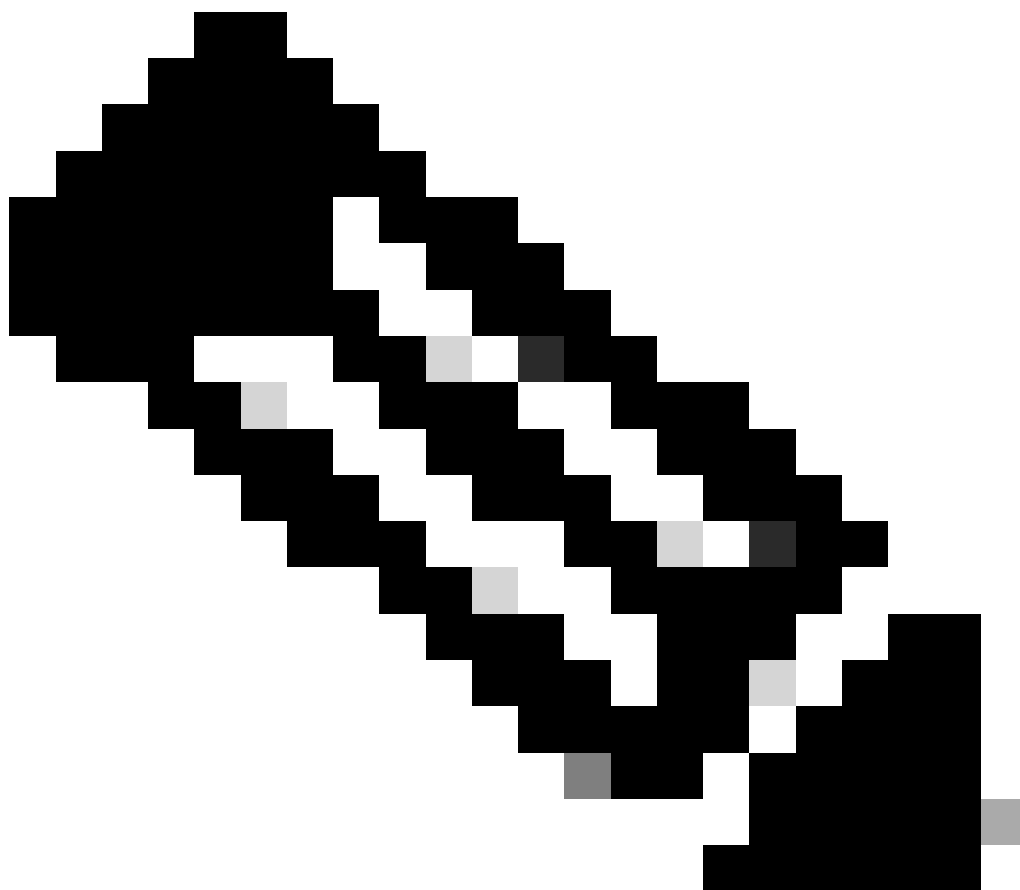
5. Zodra de Add-in met succes is geïmplementeerd, kan het tot 12 uur duren om op de Ribbons van eindgebruikers (Outlook-client) te worden

weergegeven.

## Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

1. Start Outlook voor Office 365/Microsoft 365 of Outlook Web App, maak het bericht dat u wilt versleutelen en voeg er ten minste één geldige ontvanger aan toe.



**Opmerking:** als het type versleuteling (ingesteld door de beheerder) is versleuteld, moet u ervoor zorgen dat u het bericht hebt vervolledigd en geldige ontvangers hebt toegevoegd voordat u naar de volgende stap gaat. Na Stap 3 wordt het bericht versleuteld en onmiddellijk verzonden.

---

2. Open/klik op de invoegtoepassing Cisco Secure Email Encryption Service.

- Klik op Outlook Web App op het ellipsiepietogram (in de buurt van de knoppen Verzenden en Verwerpen) en klik Cisco Secure Email Encryption Service.
- Klik op Outlook voor Windows of MacOS op Encrypt vanaf het lint of de werkbalk.
- Als u op Outlook voor MacOS versie 16.42 of hoger bent en de Nieuwe Outlook-interface gebruikt, klikt u op Cisco Secure Email Encryption Service vanuit de werkbalk.

3. Voer uw referenties in en klik op Sign in. (Alleen als het type versleuteling is gemarkeerd, klikt u op Send).

The screenshot shows the Microsoft Outlook interface during the encryption of an email. The email header includes the sender 'Udupi Kris', the recipient 'Udupi', and the subject 'Testing New Encryption'. A file attachment 'securedoc\_2024050...' (141.3 KB) is visible. The email body contains the text: 'Hello, This is a test email. Regards'. On the right side, the 'Cisco Secure Email Encryption Service' sidebar is open, displaying a notification: 'You must use encryption only for business purposes.' Below this, the 'Encryption Flow Summary' shows the following steps:

- 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)
- Message Sent (May 1, 2024; 08:42:51 AM IST)

Red arrows point to the 'Message Encrypted' and 'Message Sent' steps in the summary.

*Microsoft Outlook-coderingsstatus*

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Relatie-informatie



- [Gebruikershandleiding voor Cisco Secure Email Encryption Service-accountbeheerder](#)
- [Gebruikershandleiding voor Cisco Secure Email Encryption Service](#)
- [Microsoft Entra Application Registration Guide](#)
- [Cisco Technical Support en downloads](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.