

E-Mail-Verschlüsselungs-Add-In mit Microsoft O365 konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Best Practices für die Bereitstellung des Add-Ins für den Cisco Secure Email Encryption Service](#)

[Konfigurieren](#)

[Registrierung der Add-In-Anwendung für den Cisco Secure Email Encryption Service](#)

[Konfigurieren der Domänen- und Add-In-Einstellungen im Cisco Secure Email Encryption \(CRES\)-Administratorportal](#)

[Manifestdatei in Microsoft 365 hochladen, um das Add-In für den E-Mail-Verschlüsselungsdienst bereitzustellen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie das Cisco Email Encryption Service Add-in für die zentrale Bereitstellung über Microsoft Office 365 konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Email Gateway
- Cisco Secure Email Encryption Service (ehemals Cisco Registered Envelope Service)
- Microsoft O365 Suites (Exchange, Entra ID, Outlook)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

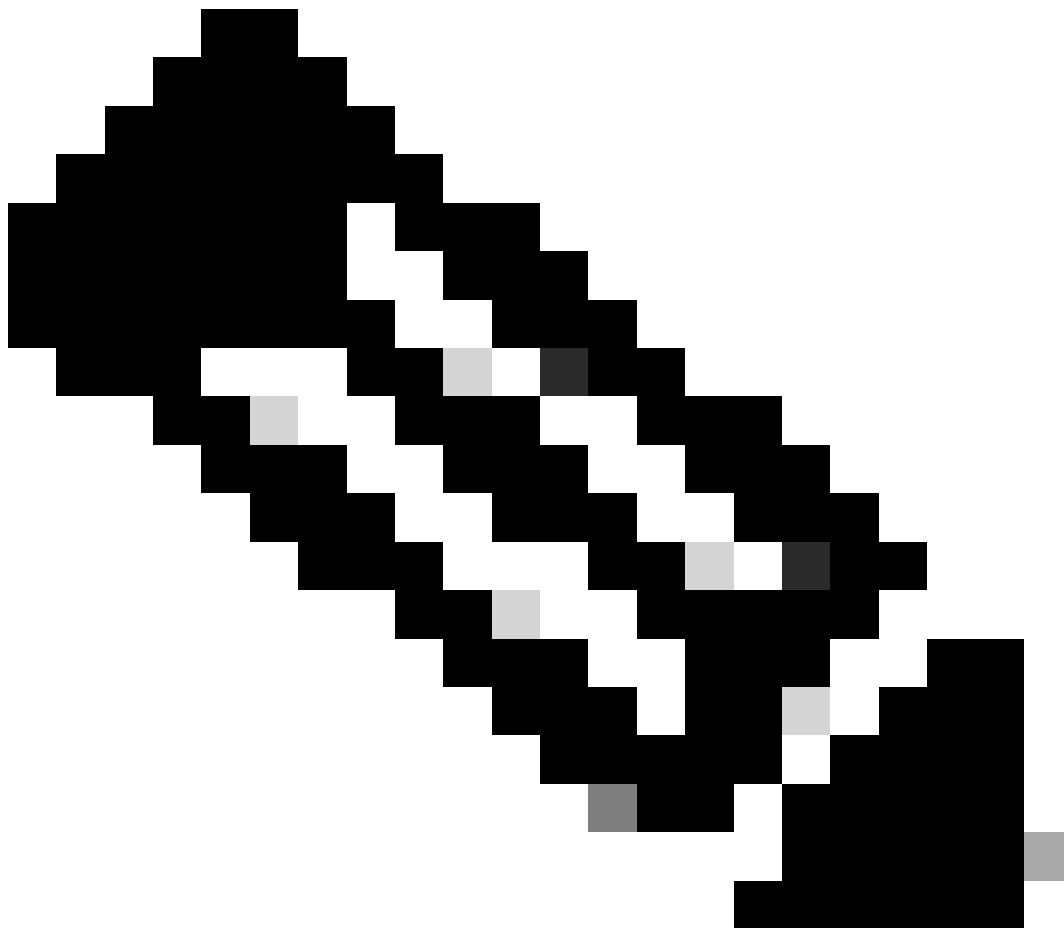
- Cisco Email Encryption Add-in 10.0.0

- Microsoft Exchange Online
- Microsoft Entra ID (ehemals Azure AD)
- Outlook für O365 (MacOS, Windows)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Mit dem Cisco Secure Email Encryption Service Add-in können Ihre Endbenutzer ihre Nachrichten direkt in Microsoft Outlook mit einem einzigen Mausklick verschlüsseln. Dieses Add-In kann in Microsoft Outlook (für Windows und MacOS) und Outlook Web App bereitgestellt werden.



Hinweis: Dieses Dokument ist ideal für alle Endbenutzer, die das Add-In verwenden möchten, Office 365/Microsoft 365-Abonnement verwenden möchten, und alle

Endbenutzer, die das Add-In verwenden möchten, sind registrierte Benutzer des Cisco Secure Email Encryption Service.

Best Practices für die Bereitstellung des Add-Ins für den Cisco Secure Email Encryption Service

- Testphase: Bereitstellung des Add-Ins für eine kleine Gruppe von Endbenutzern in einer Abteilung oder einem Bereich. Evaluieren Sie die Ergebnisse, und gehen Sie bei Erfolg zur nächsten Phase über.
- Pilotphase: Bereitstellung des Add-Ins für mehr Endbenutzer aus verschiedenen Abteilungen und Funktionen. Evaluieren Sie die Ergebnisse, und gehen Sie bei Erfolg zur nächsten Phase über.
- Produktionsphase: Bereitstellung des Add-Ins für alle Benutzer

Konfigurieren

Registrierung der Add-In-Anwendung für den Cisco Secure Email Encryption Service

1. Melden Sie sich beim Microsoft 365 Admin Center als mindestens Cloud Application Administrator ([Microsoft 365 Admin Center](#)) an.
 2. Erweitern Sie das Menü auf der linken Seite, Admin Centers und klicken Sie auf Identity.
 3. Navigieren Sie zu , Identity > Applications > App registrations und wählen Sie New registration.
-
-



Hinweis: Wenn Sie Zugriff auf mehrere Tenants haben, wechseln Sie über das Einstellungssymbol oben rechts zum Tenant, in dem Sie die Anwendung registrieren möchten. Dies geschieht über das Menü Verzeichnisse + Abonnements.

4. Geben Sie einen Anzeigenamen für die Anwendung ein, wählen Sie Konten aus, die die Anwendung verwenden können, und klicken Sie auf Register.

Register an application ...

* Name

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

 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.

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

Anwendung registrieren

5. Navigieren Sie nach erfolgreicher Registrierung zur Anwendung, um den Clientschlüssel zu konfigurieren unter Certificates & Secrets. Wählen Sie den Ablauftermin gemäß den gesetzlichen Vorschriften des Unternehmens aus.

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

Client-Schlüssel konfigurieren

6. Kopieren Sie auf der Seite "Übersicht" der registrierten Anwendung das Application (client) ID und Directory (tenant) ID. Kopieren Sie die **Client Secret** aus den im vorherigen Schritt generierten Zertifikaten und Schlüsseln.

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](#)

Übersicht über die Entra-ID-Anwendung

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

Client-Schlüssel kopieren

7. Navigieren Sie zur **registrierten E-Mail-Verschlüsselungsanwendung**, und navigieren Sie dann zu API permissions. Klicken Sie auf Add a permission, und wählen Sie die erforderlichen Microsoft Graph Application Permissions:

- Mail.Read
- Mail.ReadWrite
- E-Mail senden
- Benutzer.Lesen.Alle

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
<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](#)

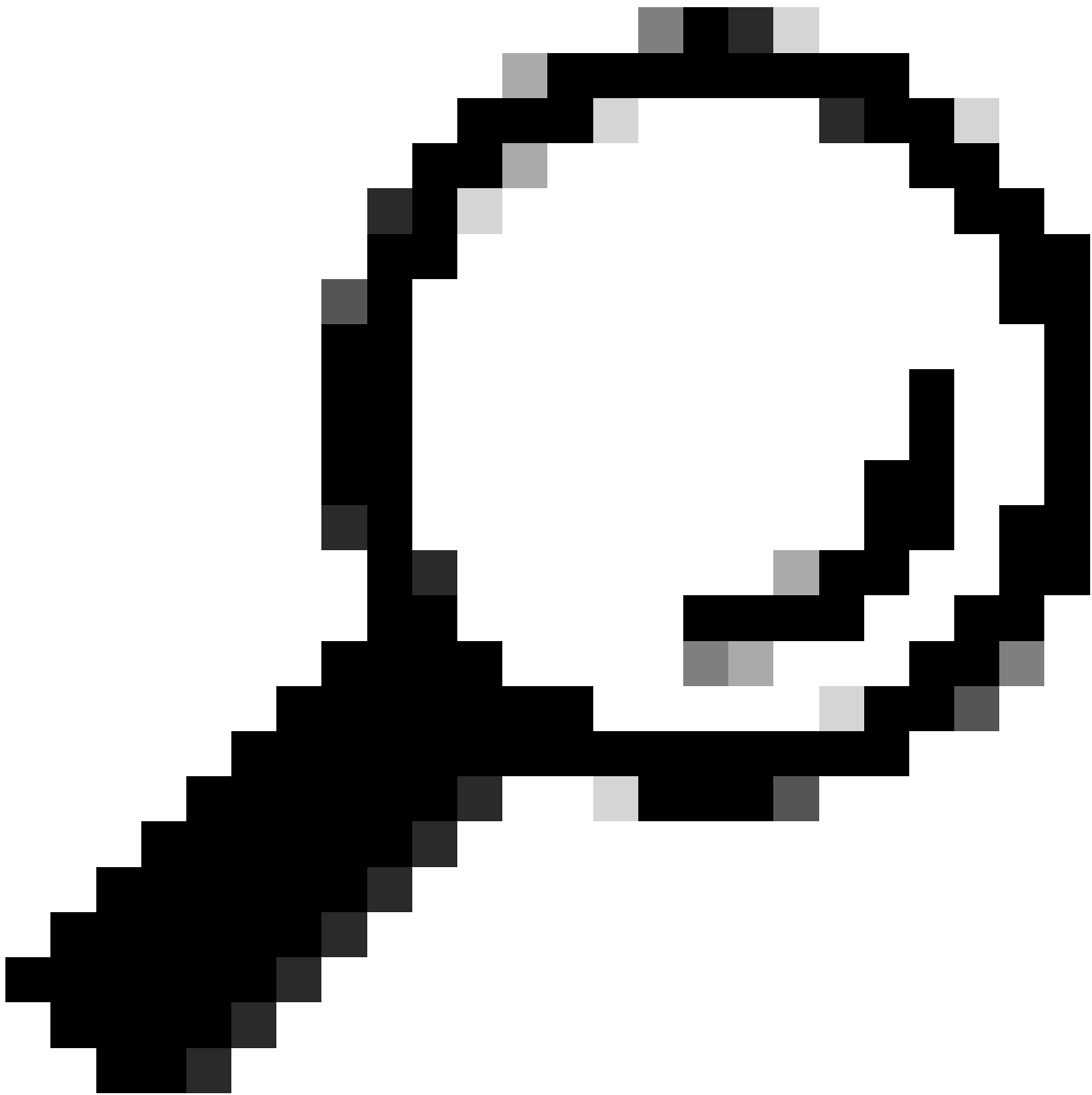
Microsoft Graph-Berechtigungskonfiguration

7. Klicken Sie Grant Admin Consent for <tenant-name> hier, um der Anwendung im Namen der Organisation Zugriff auf Berechtigungen zu gewähren.

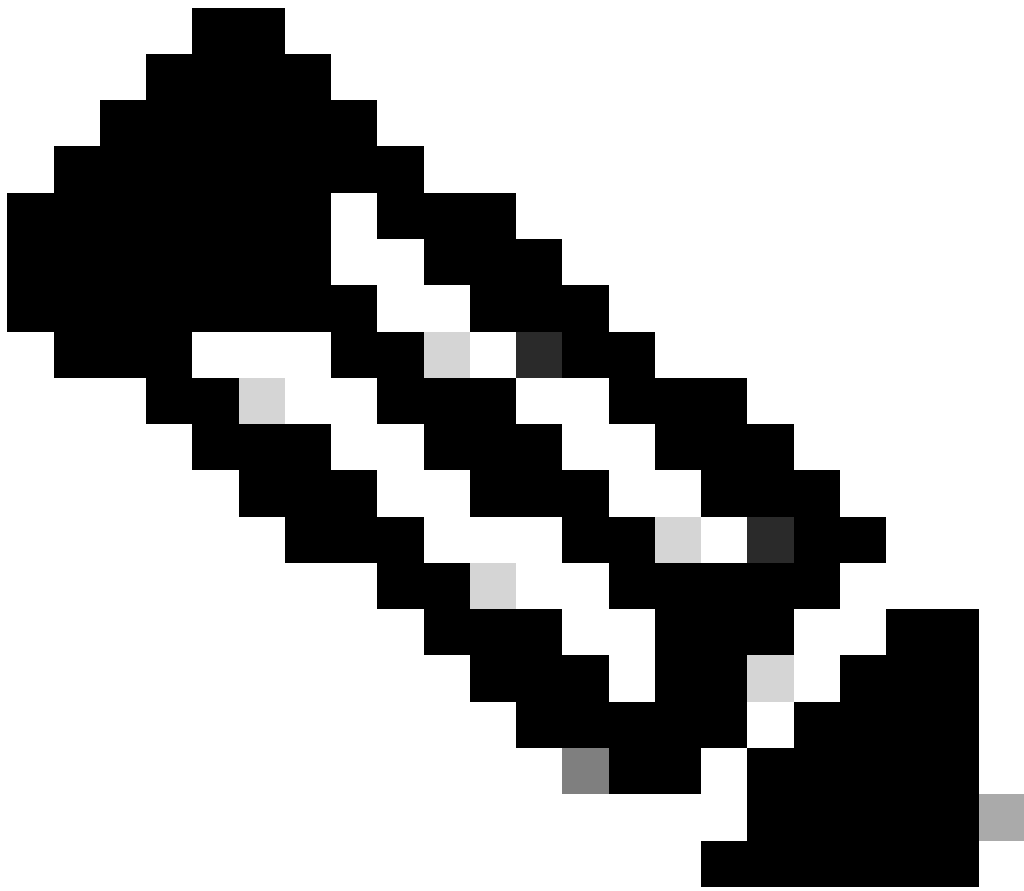
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				...
Mail.Read	Application	Read mail in all mailboxes	Yes	✔ Granted for [redacted] ...
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✔ Granted for [redacted] ...
Mail.Send	Application	Send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

Konfigurieren der Domänen- und Add-In-Einstellungen im Cisco Secure Email Encryption (CRES)-Administratorportal

1. Melden Sie sich als Kontoadministrator beim Administratorportal des Cisco Secure Email Encryption Service (CRES) an. ([Sicherer E-Mail-Verschlüsselungsservice](#))
 2. Navigieren Sie zu Accounts > Manage Accounts. Klicken Sie auf die Kontonummer, die Ihrer Organisation zugewiesen ist, oder auf das Konto, für das Sie das E-Mail-Verschlüsselungs-Add-In konfigurieren möchten.
 3. Navigieren Sie zu Profiles, wählen Sie den **Namenstyp** als Domäne und geben Sie Ihren **E-Mail-Domännennamen** unter Werte ein. Klicken Sie, **Add Entries** und warten Sie 5 bis 10 Sekunden. (Aktualisieren Sie die Browserseite nicht, und navigieren Sie erst zu einer anderen Seite, wenn die Seite erfolgreich hinzugefügt wurde.)
-
-



Tipp: Wiederholen Sie die gleichen Schritte, um weitere E-Mail-Domänen hinzuzufügen, die den E-Mail-Verschlüsselungsdienst in Ihrer Organisation nutzen werden.



Hinweis: Wenden Sie sich an das Cisco Technical Assistance Center, um die E-Mail-Domänen im CRES-Admin-Portal hinzuzufügen.

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

Name **Domain** Or other

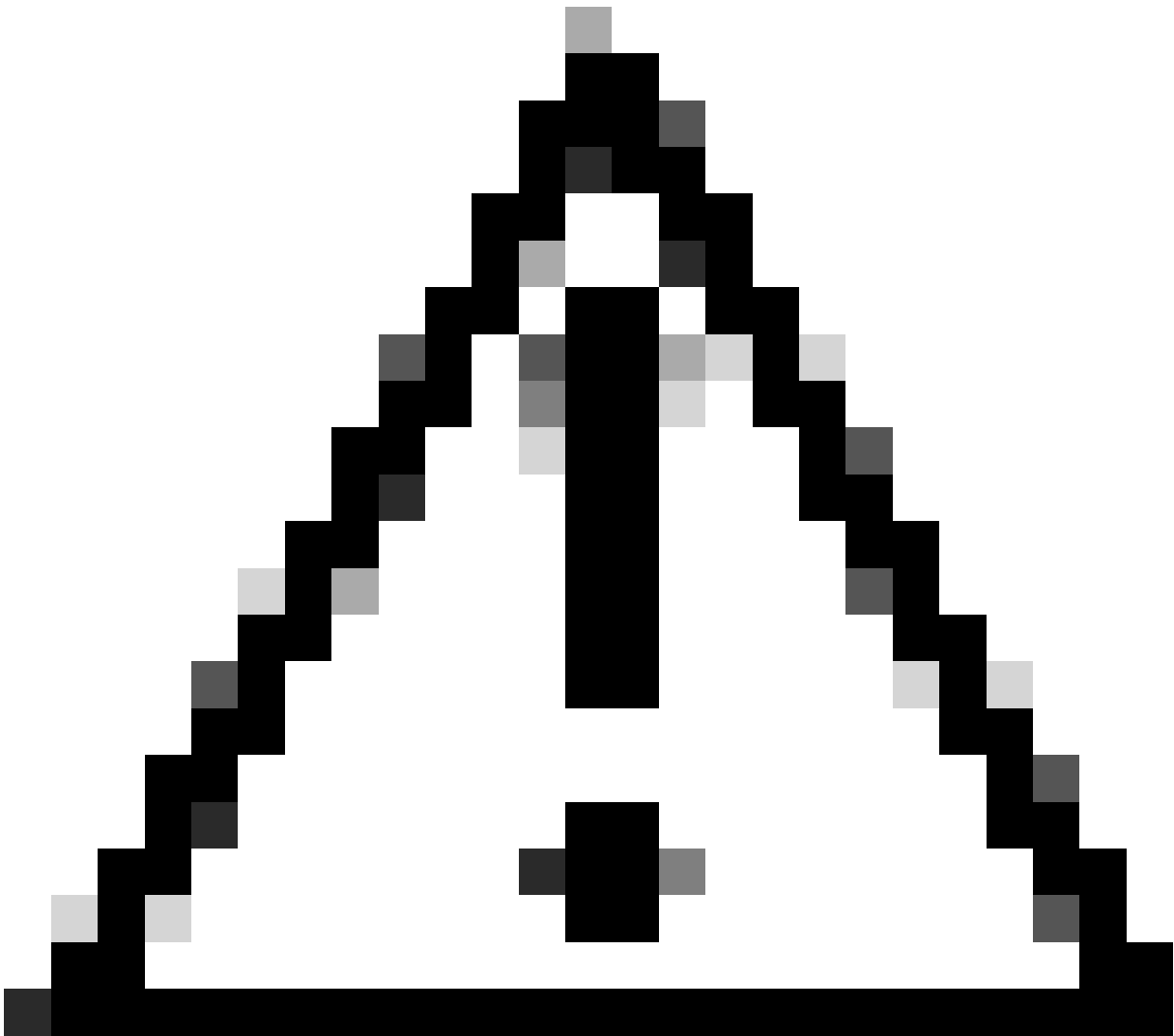
Values (comma or semicolon separated)* **Add Entries**

CRES-Administratorportalprofile

4. Navigieren Sie zur Add-in Config Registerkarte.

Schritt 1: Geben Sie den Tenant, die Client-ID und den Schlüssel ein, die Sie von der Entra-ID unter Azure AD-Details erhalten haben. Klicken Sie auf .Save Details

Schritt 2: Wählen Sie die Domäne, Verschlüsselungstyp, und klicken Sie auf Save Configuration. Verwenden Sie Save Configuration diese Option für alle Domänen, um die gleichen Einstellungen auf alle hinzugefügten Domänen anzuwenden.



Vorsicht: Navigieren Sie nicht zu einer anderen Seite, ohne die Schritte 1. und 2. gemeinsam auszuführen. Wenn Schritt 2. nicht gleichzeitig abgeschlossen wird, werden Azure AD-Details nicht gespeichert.

Schritt 3: Klicken Sie auf 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

CRES-Admin-Portal - ADDIN-Konfiguration

Manifestdatei in Microsoft 365 hochladen, um das Add-In für den E-Mail-Verschlüsselungsdienst bereitzustellen

1. Melden Sie sich als Administrator beim Microsoft 365 Admin Center an. ([Microsoft 365 Admin Center](#)).

2. Navigieren Sie zu Settings > Integrated apps und klicken Sie auf **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...**

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. Klicken Sie Deploy Add-in und wählen Sie Upload Custom Apps. Wählen Sie die Datei aus, die Sie aus dem Cisco Email Encryption Service-Administratorportal heruntergeladen haben, I have the manifest file (.xml) on this device und laden Sie sie hoch. Klicken Sie auf .Upload

4. Weisen Sie im nächsten Schritt Benutzer zu, die Zugriff auf den Cisco Secure Email Encryption Service benötigen. Um die Bereitstellung schrittweise umzusetzen, wählen Sie Specific Users/groups und klicken Sie auf 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.

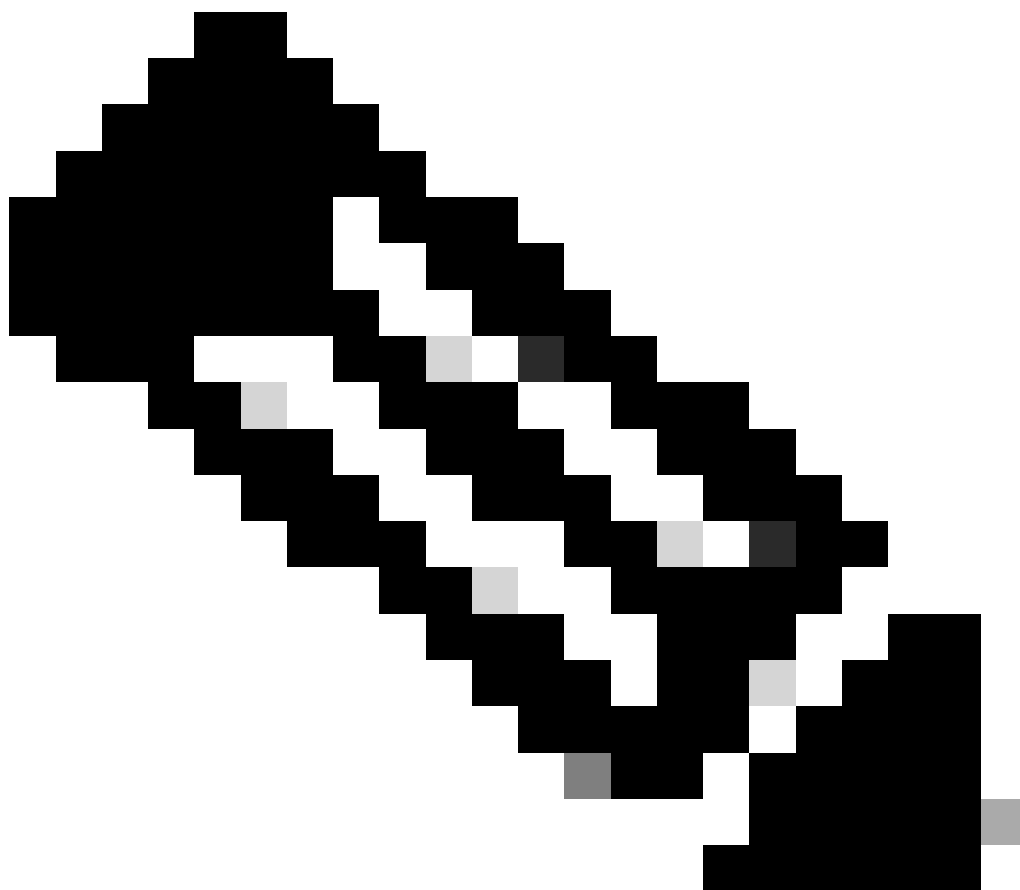
5. Nach der erfolgreichen Bereitstellung des Add-Ins kann es bis zu 12 Stunden dauern, bis es auf den Multifunktionsleisten des Endbenutzers

(Outlook-Client) angezeigt wird.

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Starten Sie Outlook für Office 365/Microsoft 365 oder Outlook Web App, erstellen Sie die Nachricht, die Sie verschlüsseln möchten, und fügen Sie mindestens einen gültigen Empfänger hinzu.



Hinweis: Wenn der vom Administrator festgelegte Verschlüsselungstyp "Verschlüsseln" lautet, stellen Sie sicher, dass die Nachricht vervollständigt und gültige Empfänger hinzugefügt wurden, bevor Sie mit dem nächsten Schritt fortfahren. Nach Schritt 3 wird die Nachricht verschlüsselt und sofort gesendet.

2. Öffnen Sie das Add-In Cisco Secure Email Encryption Service, und klicken Sie darauf.

- Klicken Sie in Outlook Web App auf das Auslassungszeichen (neben den Schaltflächen Senden und Verwerfen), und klicken Sie auf Cisco Secure Email Encryption Service.
- Klicken Sie in Outlook für Windows oder MacOS in der Multifunktionsleiste oder Symbolleiste auf **Verschlüsseln**.
- Wenn Sie Outlook für MacOS Version 16.42 oder höher verwenden und die neue Outlook-Schnittstelle verwenden, klicken Sie in der Symbolleiste auf klickenCisco Secure Email Encryption Service.

3. Geben Sie Ihre Anmeldeinformationen ein, und klicken Sie auf Sign in. (Nur wenn der Verschlüsselungstyp Flag ist, klicken Sie auf Send).

From: Udupi Kris (onmicrosoft.com) v

To: Udupi

Subject: Testing New Encryption

securedoc_2024050...
141.3 KB

Aptos (Body) 11

Hello,
This is a test email.
Regards

Cisco Secure Email... x My Day

You must use encryption only for business purposes.

Encryption Flow Summary

- ✓ 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

Microsoft Outlook-Verschlüsselungsstatus

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Benutzerleitfaden für Kontoadministratoren zum Cisco Secure Email Encryption Service](#)
- [Cisco Secure Email Encryption Service Add-in - Benutzerhandbuch](#)
- [Microsoft Entra Application Registration Guide](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.