

Configure Email Encryption Add-in Using Microsoft O365

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Best Practices for Deploying the Cisco Secure Email Encryption Service Add-In](#)

[Configure](#)

[Cisco Secure Email Encryption Service Add-in Application Registration](#)

[Configure Domain and Add-in Settings on Cisco Secure Email Encryption \(CRES\) Admin Portal](#)

[Upload Manifest File to Microsoft 365 to Deploy Email Encryption Service Add-in](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to configure Cisco Email Encryption Service Add-in Centralized Deployment via Microsoft Office 365.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

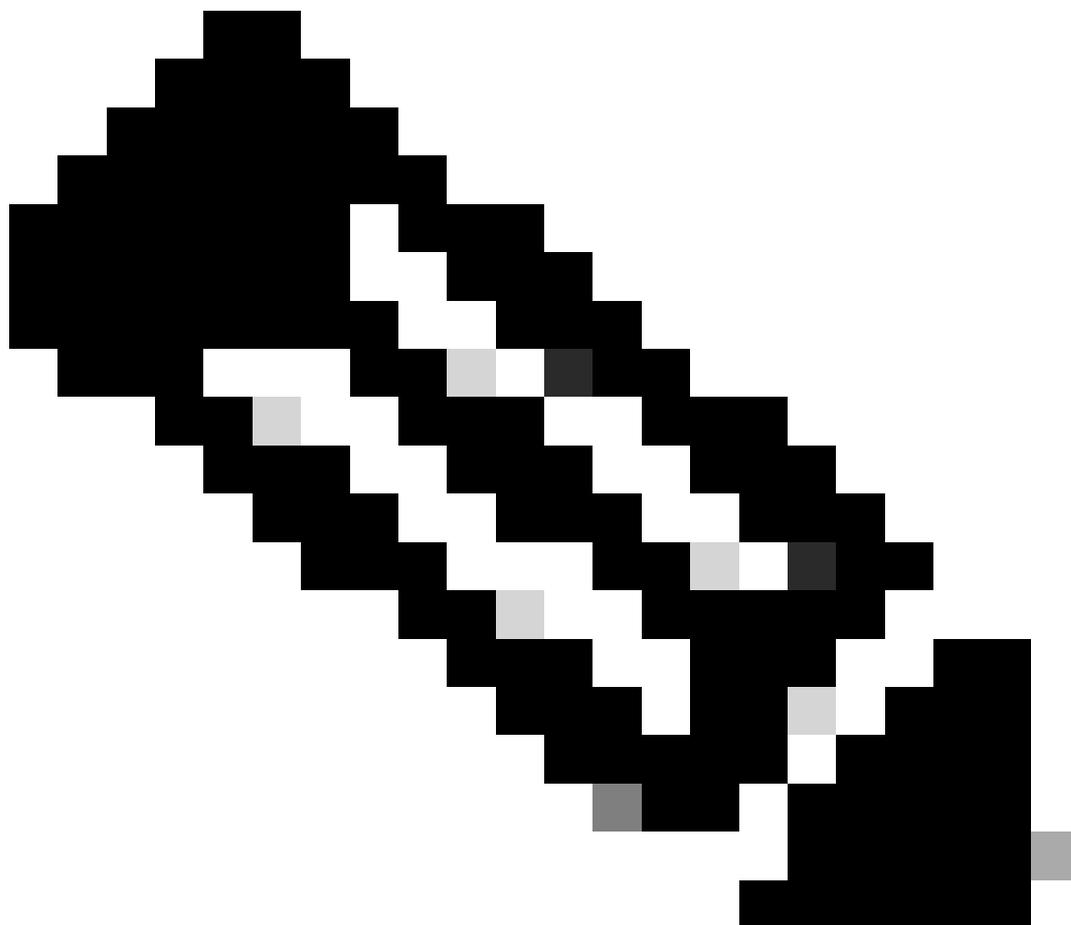
The information in this document is based on these software and hardware versions:

- Cisco Email Encryption Add-in 10.0.0
- Microsoft Exchange Online
- Microsoft Entra ID (formerly known as Azure AD)
- Outlook for 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The Cisco Secure Email Encryption Service Add-in allows your end users to encrypt their messages directly from Microsoft Outlook with a single click. This Add-in can be deployed on Microsoft Outlook (for Windows and macOS) and Outlook Web App.



Note: This document is ideal for all the end users who plan to use the add-in use Office 365/Microsoft 365 subscription and all the end users who plan to use the Add-in are registered Cisco Secure Email Encryption Service Users.

Best Practices for Deploying the Cisco Secure Email Encryption Service Add-In

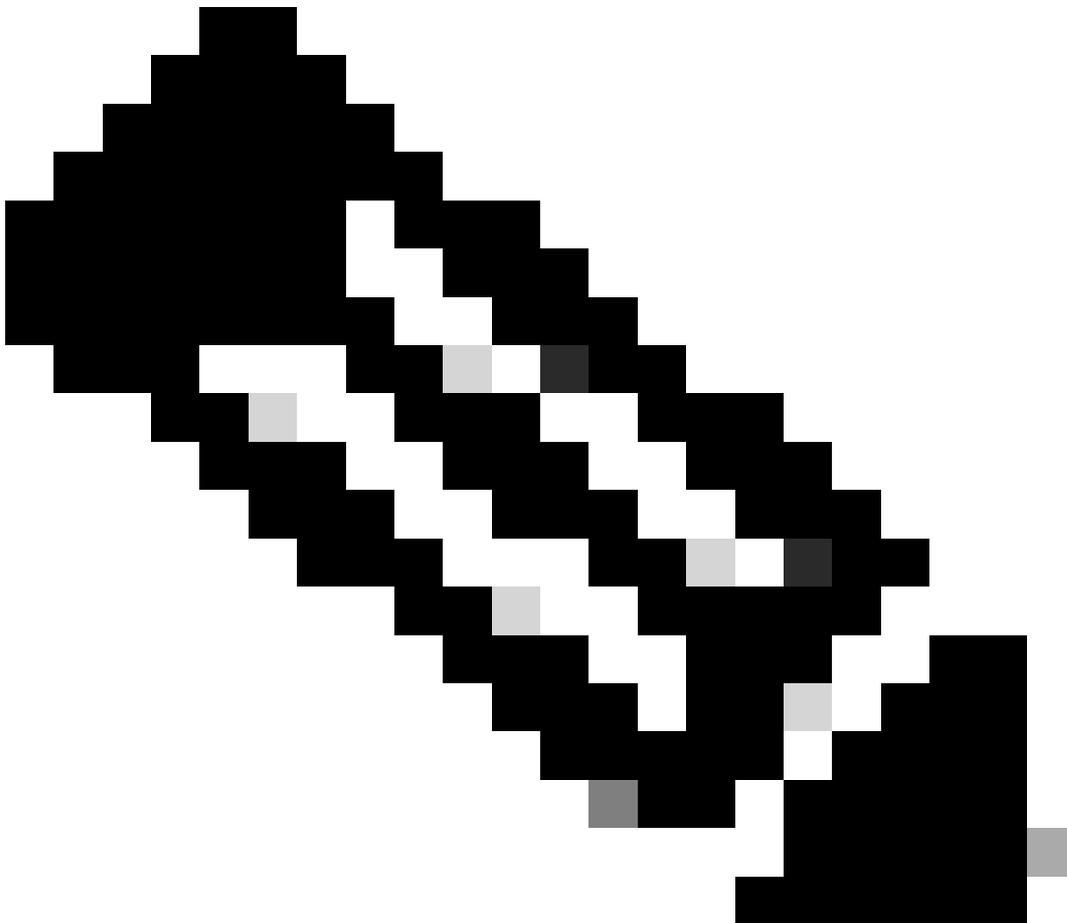
- Test Phase - Deploy the Add-in to a small set of end users within a department or function. Evaluate the results and, if successful, move to the next phase.
- Pilot Phase - Deploy the Add-in to more end users from different departments and functions. Evaluate the results and, if successful, move to the next phase.

- Production Phase - Deploy the Add-in to all users.

Configure

Cisco Secure Email Encryption Service Add-in Application Registration

1. Log in to Microsoft 365 Admin Center as at least a Cloud Application Administrator ([Microsoft 365 Admin Center](#)).
 2. In the left-hand menu, expand Admin Centers and click Identity.
 3. Navigate to Identity > Applications > App registrations and select New registration.
-



Note: If you have access to multiple Tenants, use the Settings Icon in the top right menu to switch to the Tenant in which you want to register the application from the Directories + Subscriptions menu.

4. Enter a Display Name for the Application, select accounts that can use the Application and click 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

Register Application

5. After successful registration, navigate to the Application to configure Client Secret under Certificates & Secrets. Choose the expiration according to organization regulatory compliance.

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 a token (instead of a certificate). 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

Configure Client Secret

6. From Overview page of the Registered Application, copy the Application (client) ID and Directory (tenant) ID. Copy the **Client Secret** from Certificates & Secrets generated in the previous step.

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 :

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

Directory (tenant) ID :

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

Entra ID Application Overview

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

Copy Client Secret

7. Navigate to the **Registered Email Encryption Application** and then navigate to API permissions. Click Add a permission and select required Microsoft Graph Application Permissions:

- Mail.Read
- Mail.ReadWrite
- Mail.Send
- User.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](#)

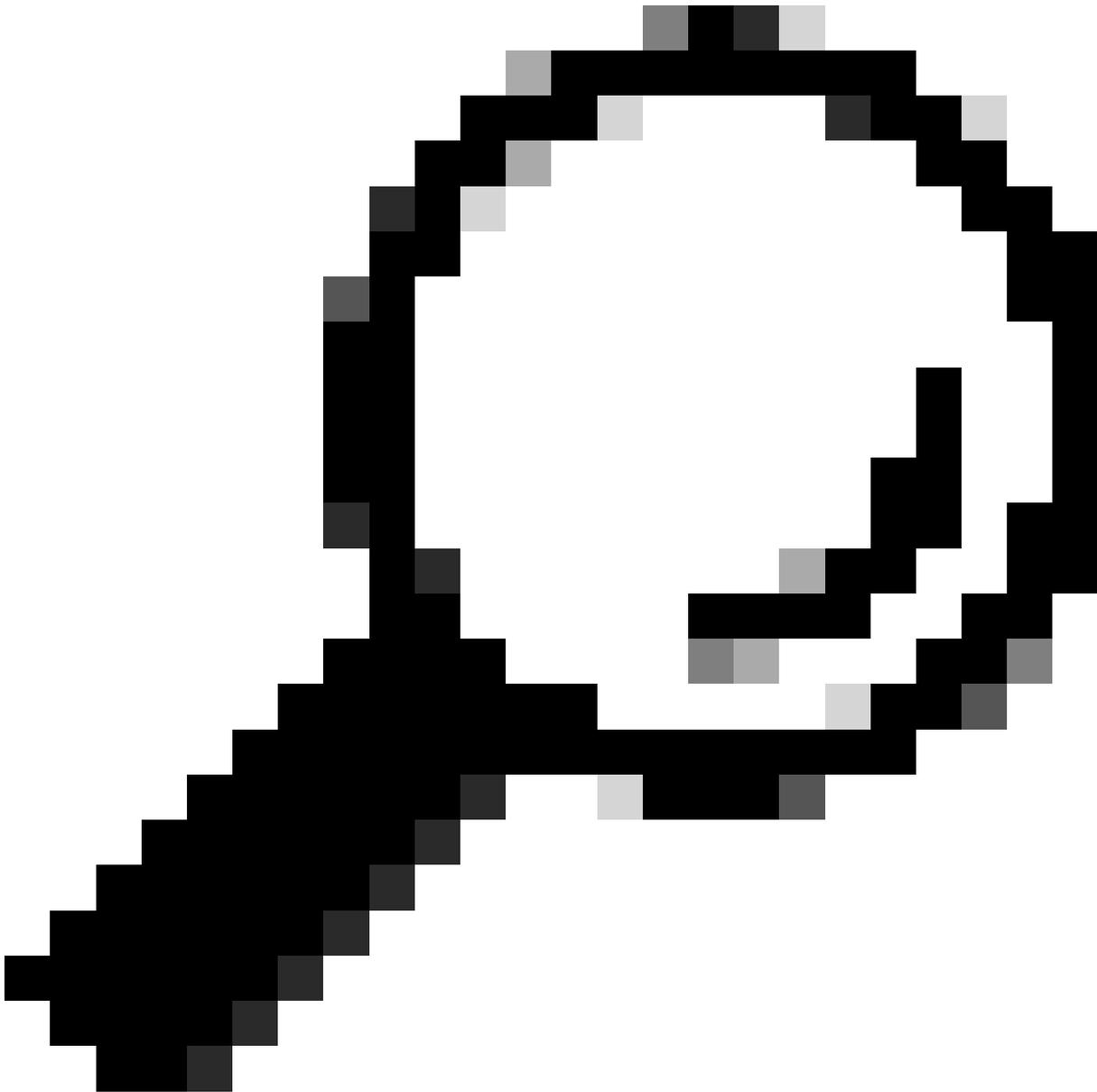
Microsoft Graph Permission Configuration

7. Click Grant Admin Consent for <tenant-name> to give the Application access to Permissions on behalf of the Organization.

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] ...

Configure Domain and Add-in Settings on Cisco Secure Email Encryption (CRES) Admin Portal

1. Log in to Cisco Secure Email Encryption Service (CRES) Admin Portal as an Account Administrator. ([Secure Email Encryption Service](#))
 2. Navigate to Accounts > Manage Accounts. Click the account number assigned to your organization or the account on which you plan to configure Email Encryption Add-in.
 3. Navigate to Profiles, select the **Name type** as Domain and enter your **email domain name** under Values. Click **Add Entries** and wait for 5 to 10 seconds. (Do not refresh the browser page or navigate to a different page until it is added successfully).
-



Tip: Repeat the same steps to add other Email Domains that are going to use Email Encryption Service in your organization.

Note: Contact Cisco Technical Assistance Center to get the Email Domains added on CRES Admin Portal.

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

Name **Domain** Or other

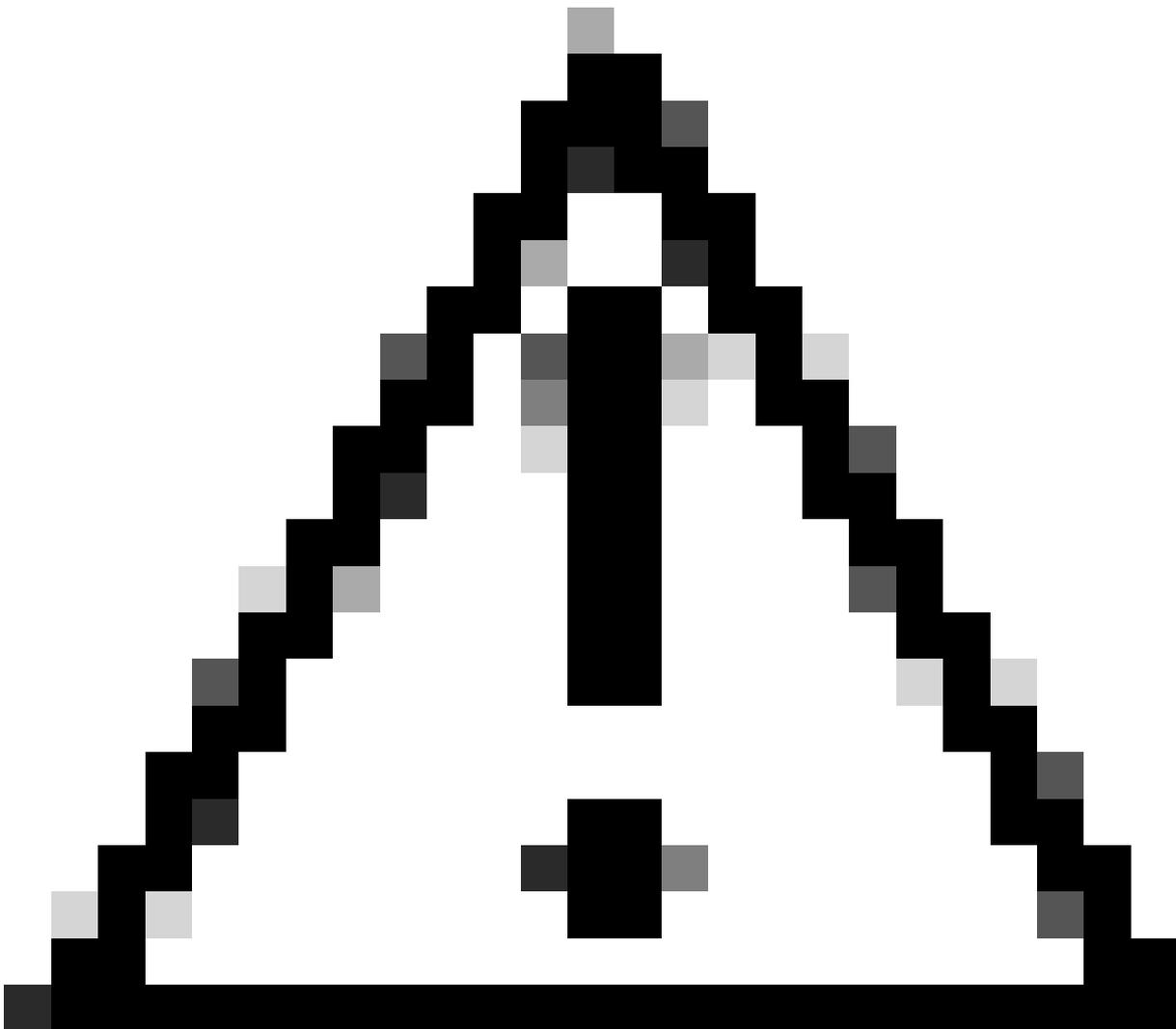
Values (comma or semicolon separated)* **Add Entries**

CRES Admin Portal Profiles

4. Navigate to Add-in Config tab.

Step 1: Enter the Tenant, Client ID and Secret obtained from Entra ID under Azure AD Details. Click Save Details.

Step 2: Select the domain, Encryption Type, and click Save Configuration. Use Save Configuration for All Domains to apply the same settings to all added Domains.



Caution: Do not navigate to a different page without completing Step 1. and Step 2. together. If Step 2. is not completed concurrently, Azure AD details are not saved.

Step 3: Click 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 Config

Upload Manifest File to Microsoft 365 to Deploy Email Encryption Service Add-in

1. Log in to Microsoft 365 Admin Center as an Administrator. ([Microsoft 365 Admin Center](#)).
2. Navigate to Settings > Integrated apps and click **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 1 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

1 2

3. Click Deploy Add-in and choose Upload Custom Apps. Select I have the manifest file (.xml) on this device and upload the file downloaded from Cisco Email Encryption Service Admin Portal from the previous step. Click Upload.
4. On the next step, assign users who need access to Cisco Secure Email Encryption Service. For a phased manner deployment, choose Specific Users/groups and click 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

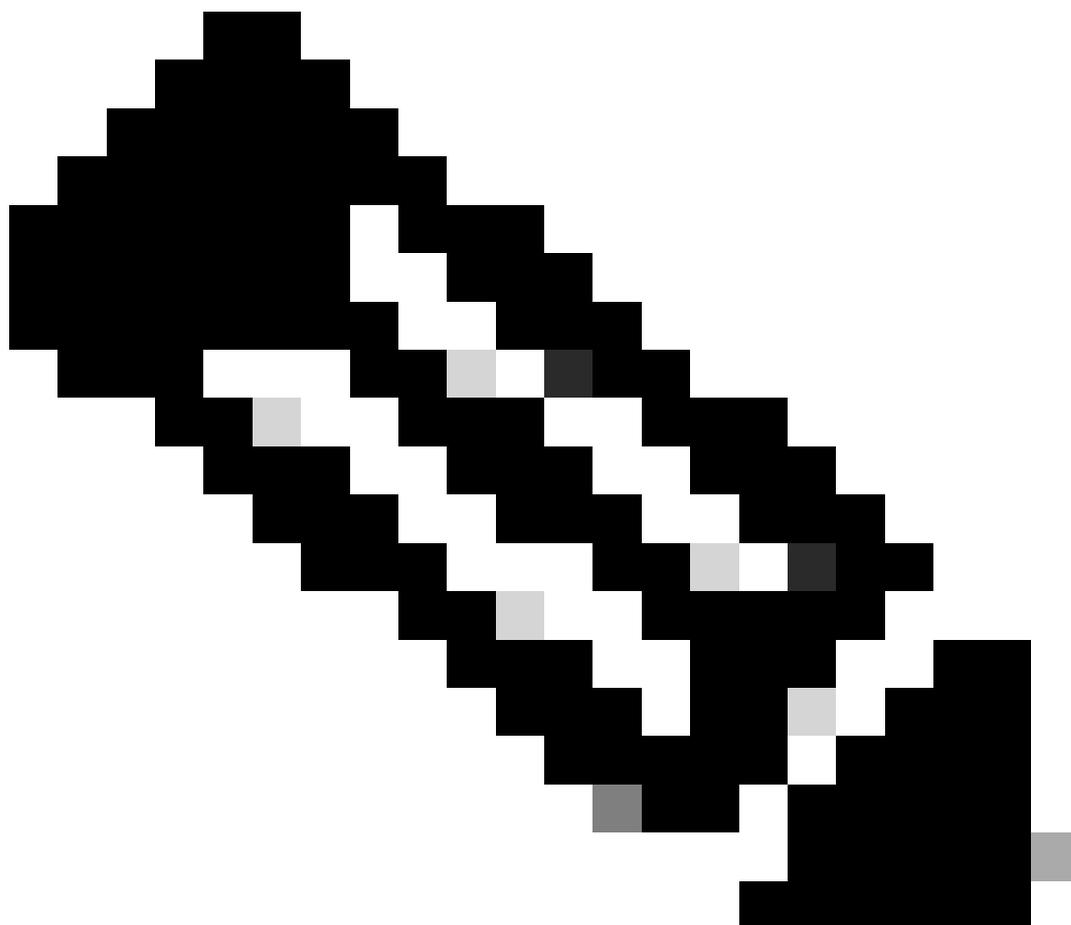
After you choose Deploy, the add-in will be available on assigned users' ribbons the next time they open their app.

5. Once the Add-in is successfully deployed, it can take up to 12 hours to be displayed on end users' Ribbons (Outlook Client).

Verify

Use this section in order to confirm that your configuration works properly.

1. Launch Outlook for Office 365/Microsoft 365 or Outlook Web App, compose the message that you want to encrypt, and add at least one valid recipient to it.



Note: If the Encryption Type (set by the administrator) is Encrypt, ensure that you have completed your message and added valid recipients before proceeding to the next step. After Step 3, the message is encrypted and sent immediately.

2. Open/Click the Cisco Secure Email Encryption Service add-in.

- On Outlook Web App, click the ellipsis icon (located near the Send and Discard buttons), and click Cisco Secure Email Encryption Service.
- On Outlook for Windows or MacOS, click **Encrypt** from the Ribbon or Toolbar.
- If you are on Outlook for MacOS version 16.42 or later and using the New Outlook interface, click Cisco Secure Email Encryption Service from the Toolbar.

3. Enter your credentials and click Sign in. (Only if the Encryption Type is Flag, click Send).

The screenshot displays an email interface in Microsoft Outlook. The email header shows the sender as 'Udupi Kris' and the subject as 'Testing New Encryption'. A file attachment named 'securedoc_2024050...' is visible. The email body contains the text: 'Hello, This is a test email. Regards'. On the right side, a 'Cisco Secure Email...' notification is present, along with an 'Encryption Flow Summary' section. This summary lists five steps: 'Encryption Initiated', 'Successfully Authenticated', 'Message Encrypted', and 'Message Sent', all with green checkmarks and timestamps from May 1, 2024. Two red arrows point to the 'Message Encrypted' and 'Message Sent' steps.

Microsoft Outlook Encryption Status

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [Cisco Secure Email Encryption Service Account Administrator User Guide](#)
- [Cisco Secure Email Encryption Service Add-in User Guide](#)
- [Microsoft Entra Application Registration Guide](#)
- [Cisco Technical Support & Downloads](#)