

Configurar el complemento Cifrado de correo electrónico mediante Microsoft O365

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Prácticas recomendadas para implementar el complemento Cisco Secure Email Encryption Service](#)

[Configurar](#)

[Registro de la aplicación del complemento Cisco Secure Email Encryption Service](#)

[Configuración de los parámetros de dominio y complemento en el portal de administración de Cisco Secure Email Encryption \(CRES\)](#)

[Cargar archivo de manifiesto en Microsoft 365 para implementar el complemento Servicio de cifrado de correo electrónico](#)

[Verificación](#)

[Troubleshoot](#)

[Información de relación](#)

Introducción

Este documento describe cómo configurar la implementación centralizada del complemento Cisco Email Encryption Service a través de Microsoft Office 365.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

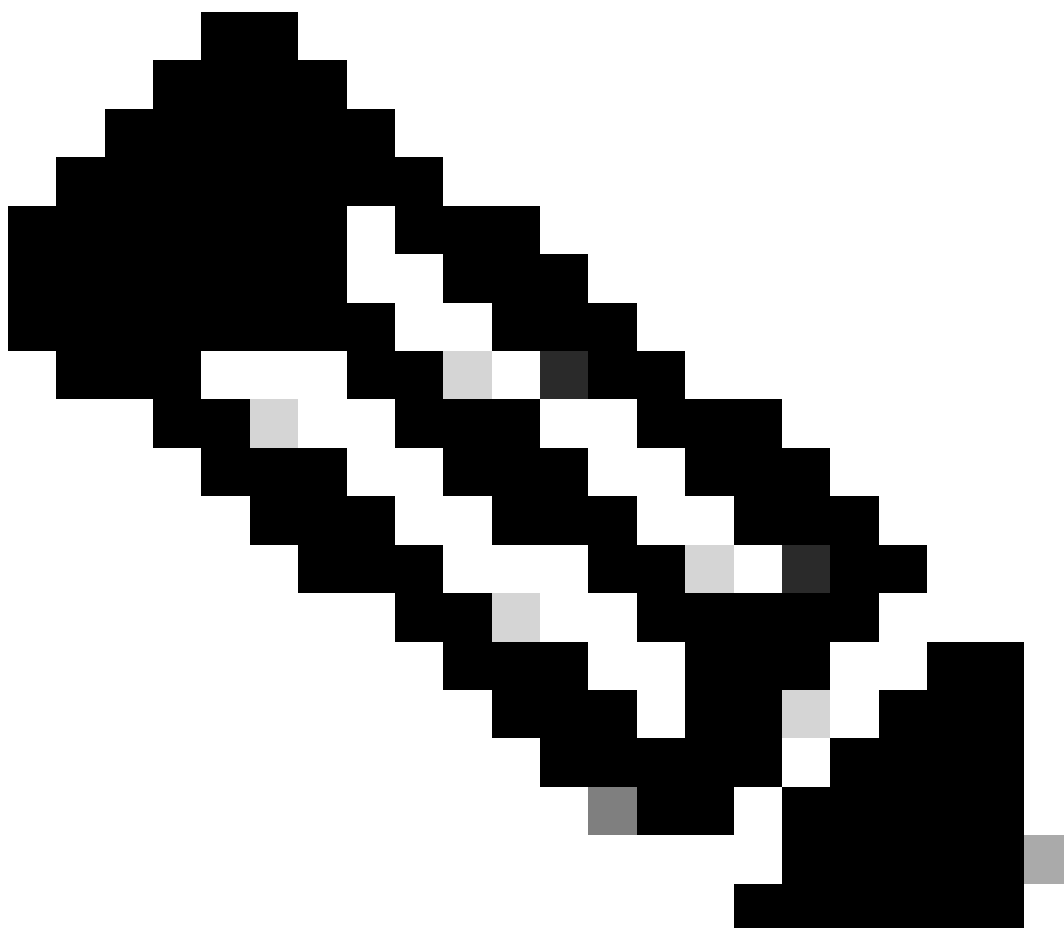
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Email Encryption Add-in 10.0.0
- Microsoft Exchange Online
- ID de Microsoft Entry (anteriormente conocido como Azure AD)
- Outlook para O365 (macOS, Windows)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El complemento Cisco Secure Email Encryption Service permite a los usuarios finales cifrar sus mensajes directamente desde Microsoft Outlook con un solo clic. Este complemento se puede implementar en Microsoft Outlook (para Windows y macOS) y Outlook Web App.



Nota: este documento es ideal para todos los usuarios finales que planean utilizar el

complemento y usan la suscripción de Office 365/Microsoft 365, y todos los usuarios finales que planean usar el complemento son usuarios registrados del servicio Cisco Secure Email Encryption.

Prácticas recomendadas para implementar el complemento Cisco Secure Email Encryption Service

- Fase de prueba: implementa el complemento en un conjunto reducido de usuarios finales de un departamento o función. Evalúe los resultados y, si tiene éxito, pase a la siguiente fase.
- Fase piloto: implemente el complemento para más usuarios finales de diferentes departamentos y funciones. Evalúe los resultados y, si tiene éxito, pase a la siguiente fase.
- Fase de producción: implementa el complemento para todos los usuarios.

Configurar

Registro de la aplicación del complemento Cisco Secure Email Encryption Service

1. Inicie sesión en el Centro de administración de Microsoft 365 como mínimo administrador de aplicaciones en la nube ([Centro de administración de Microsoft 365](#)).
 2. En el menú de la izquierda, expanda Admin Centersy haga clic en Identity.
 3. Acceda a Identity > Applications > App registrationsy seleccione New registration.
-
-



Nota: Si tiene acceso a varios arrendatarios, utilice el icono Configuración del menú superior derecho para cambiar al arrendatario en el que desea registrar la aplicación desde el menú Directorios + Suscripciones.

4. Introduzca un nombre para mostrar para la aplicación, seleccione las cuentas que pueden utilizar la aplicación y haga clic en 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

Registrar aplicación

5. Después de registrarse correctamente, acceda a la aplicación en la que desea configurar el secreto de cliente Certificates & Secrets. Elija la fecha de caducidad de acuerdo con la normativa de la organización.

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

Configurar secreto de cliente

6. En la página Visión General de la Aplicación Registrada, copie el Application (client) ID y Directory (tenant) ID. Copie el **Client Secret** de Certificados y secretos generados en el paso anterior.

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](#)

Descripción general de la aplicación 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

Copiar secreto de cliente

7. Acceda a la aplicación de cifrado de correo electrónico registrado y vaya a API permissions. Haga clic en Add a permission y seleccione los permisos de aplicación de Microsoft Graph necesarios:

- Correo.Leer
- Correo.LecturaEscritura
- Correo.Enviar
- Usuario.Leer.Todo

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

Configuración de permisos de Microsoft Graph

7. Haga clic Grant Admin Consent for <tenant-name> para otorgar a la aplicación acceso a permisos en nombre de la organización.

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] ...

Permisos de API de Microsoft Graph

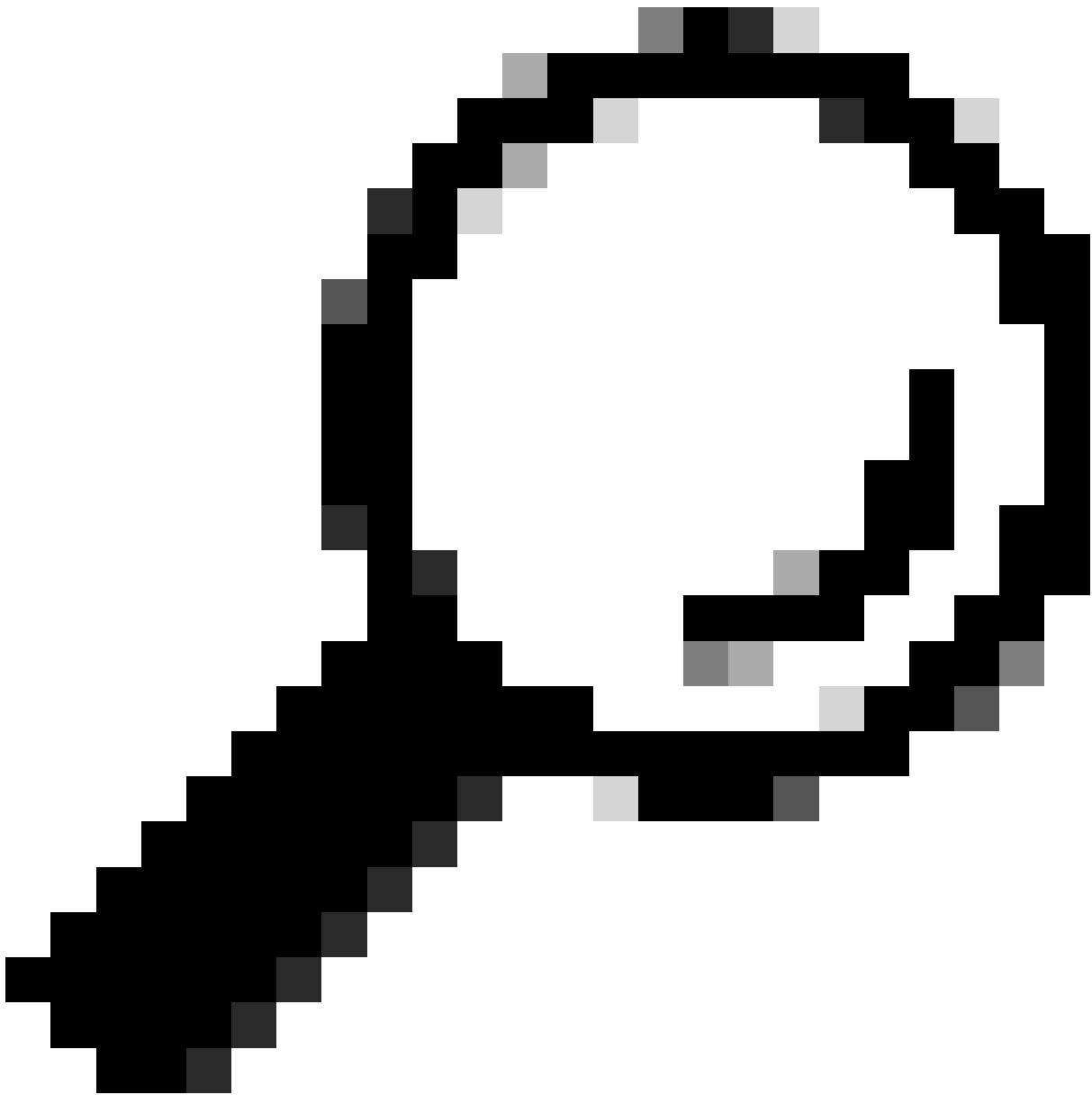
Configuración de los parámetros de dominio y complemento en el portal de administración de Cisco Secure Email Encryption (CRES)

1. Inicie sesión en el portal de administración de Cisco Secure Email Encryption Service (CRES) como administrador de cuentas.

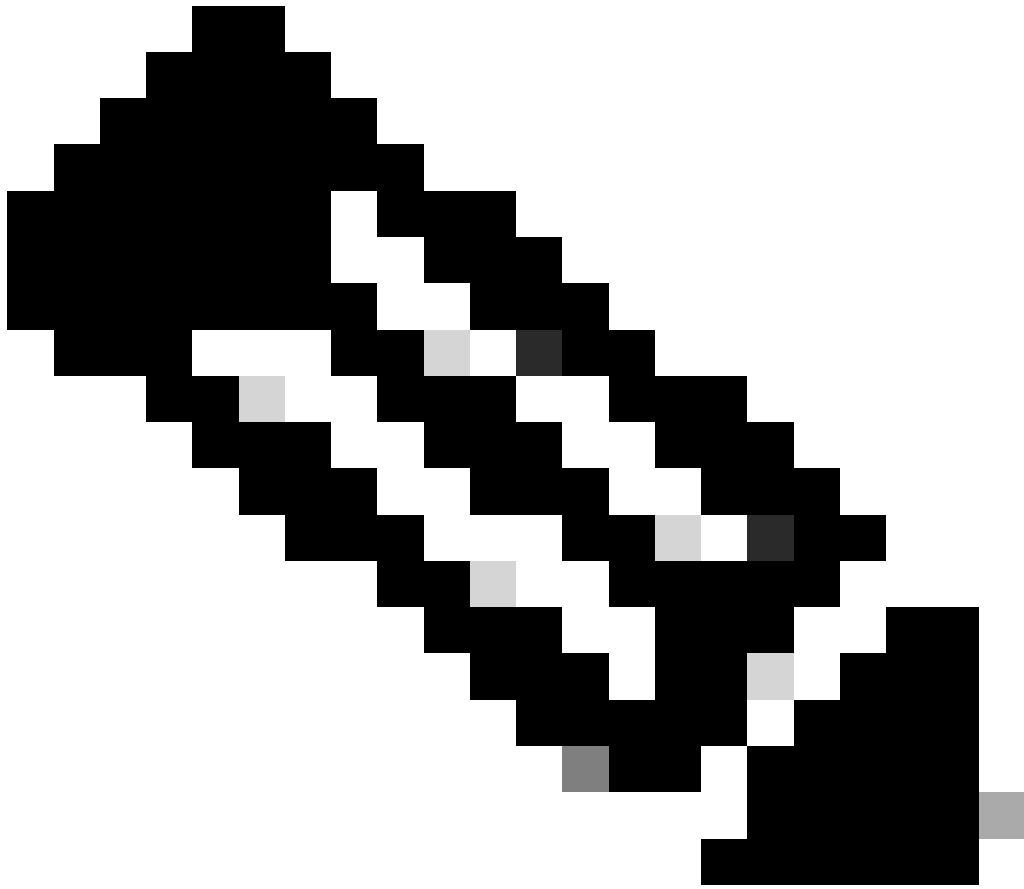
<https://res.cisco.com/admin>

2. Acceda a Accounts > Manage Accounts. Haga clic en el número de cuenta asignado a su organización o en la cuenta en la que planea configurar el complemento Cifrado de correo electrónico.

3. Desplácese hasta Profiles, seleccione el tipo de nombre como Dominio e introduzca el nombre de dominio de correo electrónico en Valores. Haga clic **Add Entries** y espere de 5 a 10 segundos. (No actualice la página del explorador ni desplácese a otra página hasta que se haya agregado correctamente).



Sugerencia: repita los mismos pasos para agregar otros dominios de correo electrónico que vayan a utilizar el servicio de cifrado de correo electrónico en su organización.



Nota: Póngase en contacto con el centro de asistencia técnica de Cisco para que se agreguen los dominios de correo electrónico en el portal de administración de CRES.

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

Name **Domain** Or other

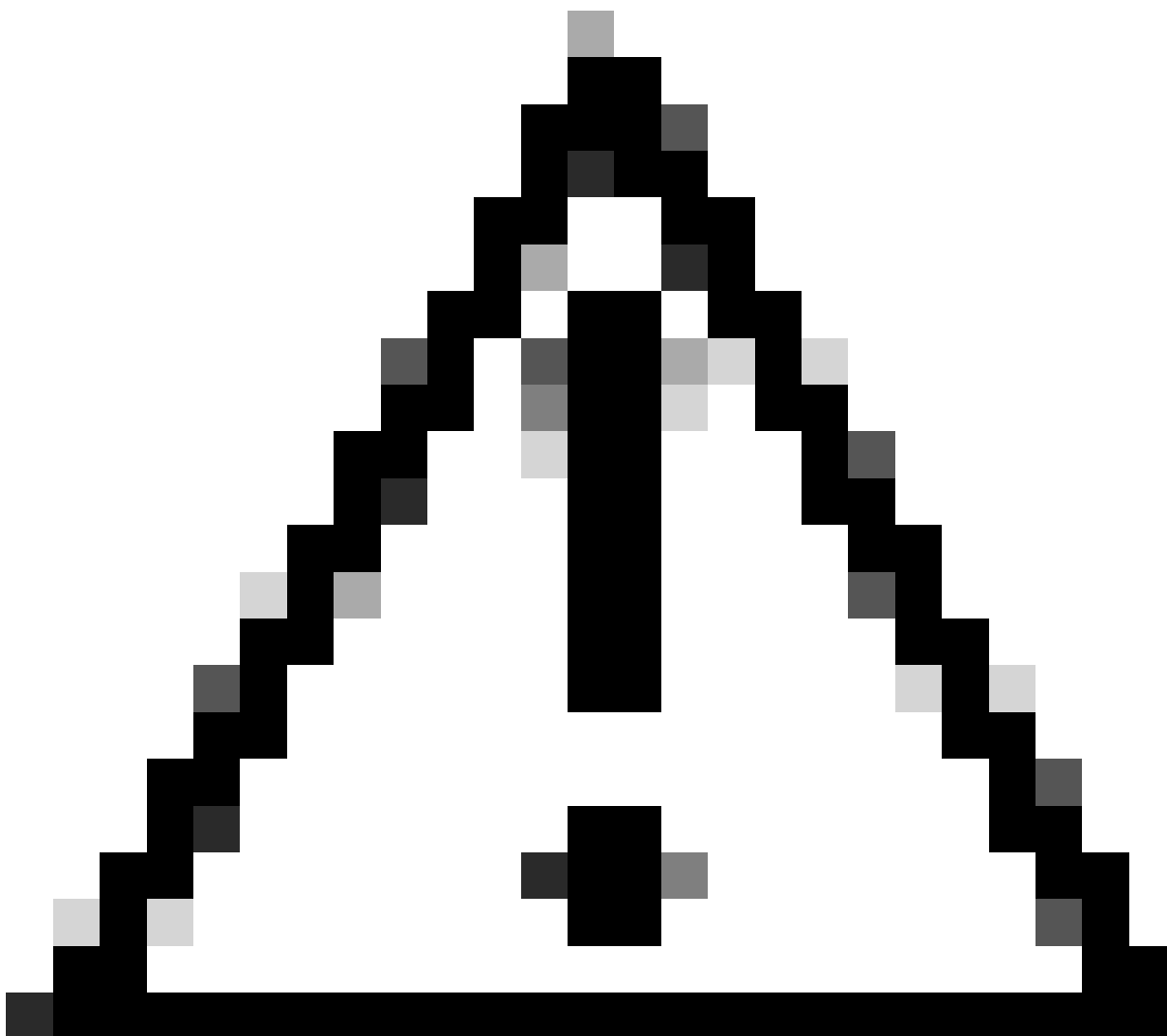
Values (comma or semicolon separated)* **Add Entries**

Perfiles del portal de administración de CRES

4. Acceda a la Add-in Configpestaña.

Paso 1: introduzca el arrendatario, la ID de cliente y el secreto obtenidos de la ID de Entra en Detalles de Azure AD. Haga clic en Save Details.

Paso 2: Seleccione el dominio, Tipo de cifrado y haga clic en Save Configuration. Utilice Save Configuration para todos los dominios para aplicar la misma configuración a todos los dominios agregados.



Precaución: no navegue a una página diferente sin completar el paso 1 y el paso 2 juntos. Si el paso 2. no se completa simultáneamente, los detalles de Azure AD no se guardarán.

Paso 3: Haga clic en 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*

Client ID* 2

Client Secret*

3 →

Step 2: Configure the Add-In Settings

Domain 4

Encryption Type 5

Password remembered in Add-In client for days

Flag Type Subject Flag Header Flag

Flag Value

6 →

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

7 →

Configuración del complemento del portal de administración de CRES

Cargar archivo de manifiesto en Microsoft 365 para implementar el complemento Servicio de cifrado de correo electrónico

1. Inicie sesión en el Centro de administración de Microsoft 365 como administrador. ([Microsoft 365 Admin Center](#)).

2. Desplácese hasta Settings > Integrated apps y haga clic en Complementos.

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...

Adobe Acrobat for Mi...

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

CodeTwo for Outlook

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

[View more apps](#)

3. Haga clic Deploy Add-iny seleccione Upload Custom Apps. Seleccione I have the manifest file (.xml) on this devicey cargue el archivo descargado desde el portal de administración del servicio Cisco Email Encryption del paso anterior. Haga clic en Upload.

4. En el siguiente paso, asigne los usuarios que necesiten acceso a Cisco Secure Email Encryption Service. Para una implementación por fases, elija Specific Users/groupsy haga clic en 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.

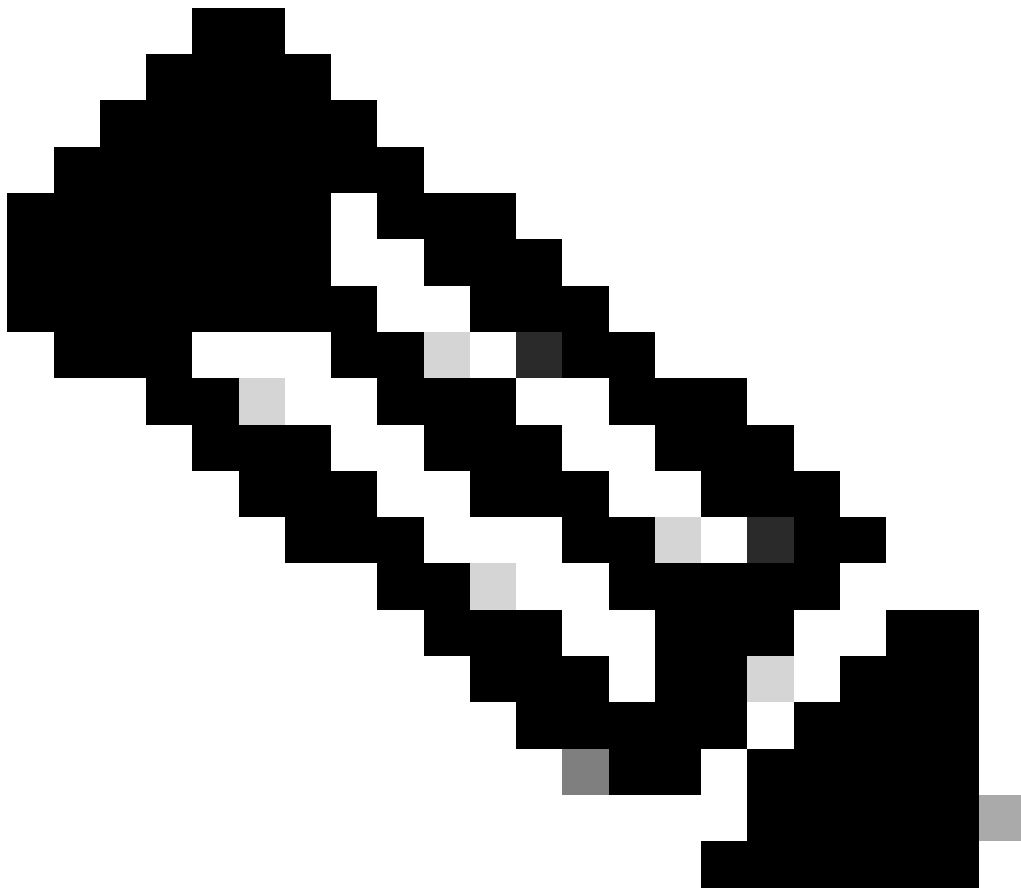
5. Una vez implementado correctamente el complemento, puede tardar hasta 12 horas en mostrarse en las cintas de opciones de los usuarios

finales (Cliente de Outlook).

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

1. Inicie Outlook para Office 365/Microsoft 365 o Outlook Web App, redacte el mensaje que desea cifrar y agregue al menos un destinatario válido.



Nota: si el tipo de cifrado (establecido por el administrador) es Cifrar, asegúrese de que ha completado el mensaje y agregado destinatarios válidos antes de continuar con el siguiente paso. Después del paso 3, el mensaje se cifra y se envía inmediatamente.

2. Abra/haga clic en el complemento Cisco Secure Email Encryption Service.

- En Outlook Web App, haga clic en el icono de puntos suspensivos (situado junto a los botones Enviar y Descartar) y haga clic en Cisco Secure Email Encryption Service.
- En Outlook para Windows o MacOS, haga clic en Cifrar en la cinta de opciones o en la barra de herramientas.
- Si se encuentra en Outlook para MacOS versión 16.42 o posterior y utiliza la nueva interfaz de Outlook, haga clic Cisco Secure Email Encryption Service en de la barra de herramientas.

3. Introduzca sus credenciales y haga clic en Sign in. (Sólo si el tipo de cifrado es Indicador, haga clic en Send).

The screenshot displays an Outlook email composition window. The header shows the sender as 'Udupi Kris [redacted]@onmicrosoft.com' and the recipient as 'Udupi [redacted]'. The subject is 'Testing New Encryption'. A file attachment named 'securedoc_2024050...' (141.3 KB) is visible. The body text reads: 'Hello, This is a test email. Regards'. On the right side, a 'Cisco Secure Email...' tab is active, showing a notification: 'You must use encryption only for business purposes.' Below this, an 'Encryption Flow Summary' section lists 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), and 'Message Sent' (May 1, 2024; 08:42:51 AM IST). Red arrows point to the 'Message Encrypted' and 'Message Sent' steps.

Estado de cifrado de Microsoft Outlook

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información de relación

- [Guía del usuario del administrador de cuentas del servicio Cisco Secure Email Encryption](#)
- [Guía del usuario de Cisco Secure Email Encryption Service Add-in](#)
- [Guía de registro de aplicaciones de Microsoft Entra](#)
- [**Soporte técnico y descargas de Cisco**](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).