Configurar el complemento Cifrado de correo electrónico mediante Microsoft O365

Contenido

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

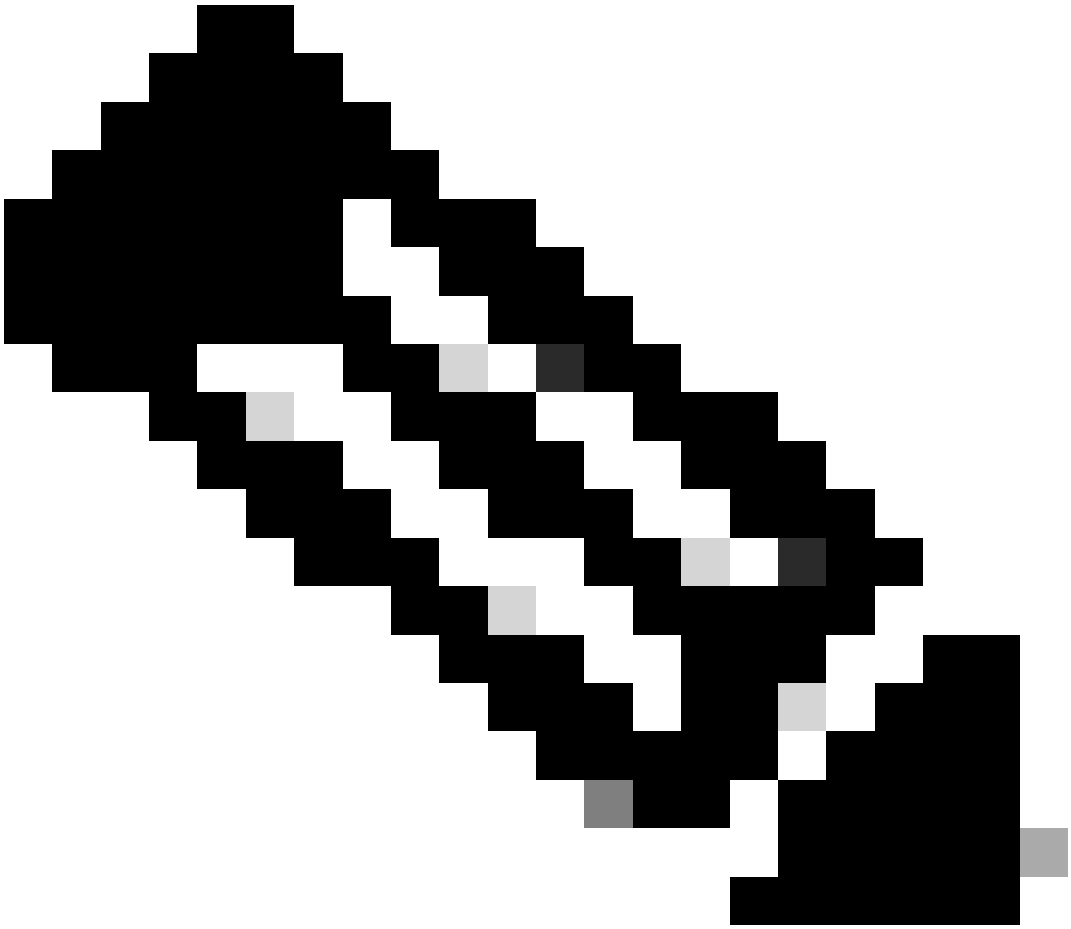
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 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.

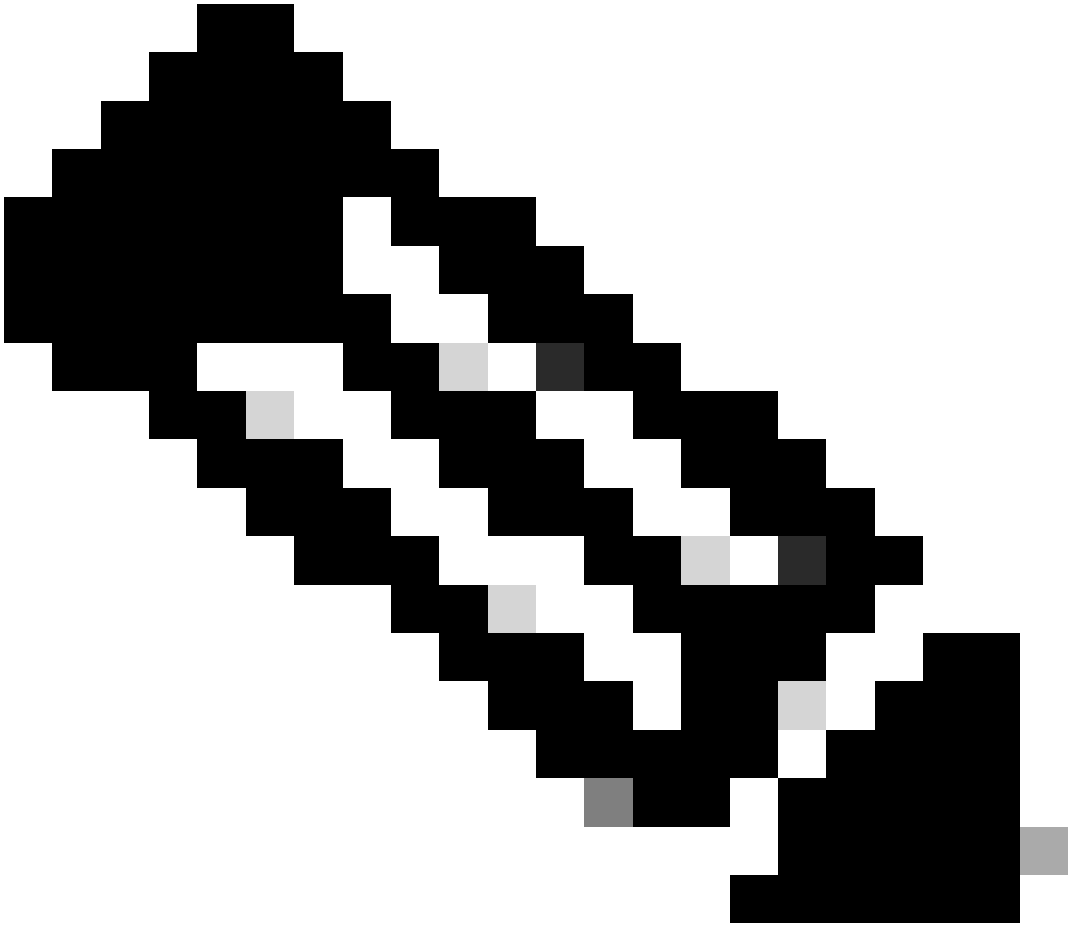
Configurar

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).

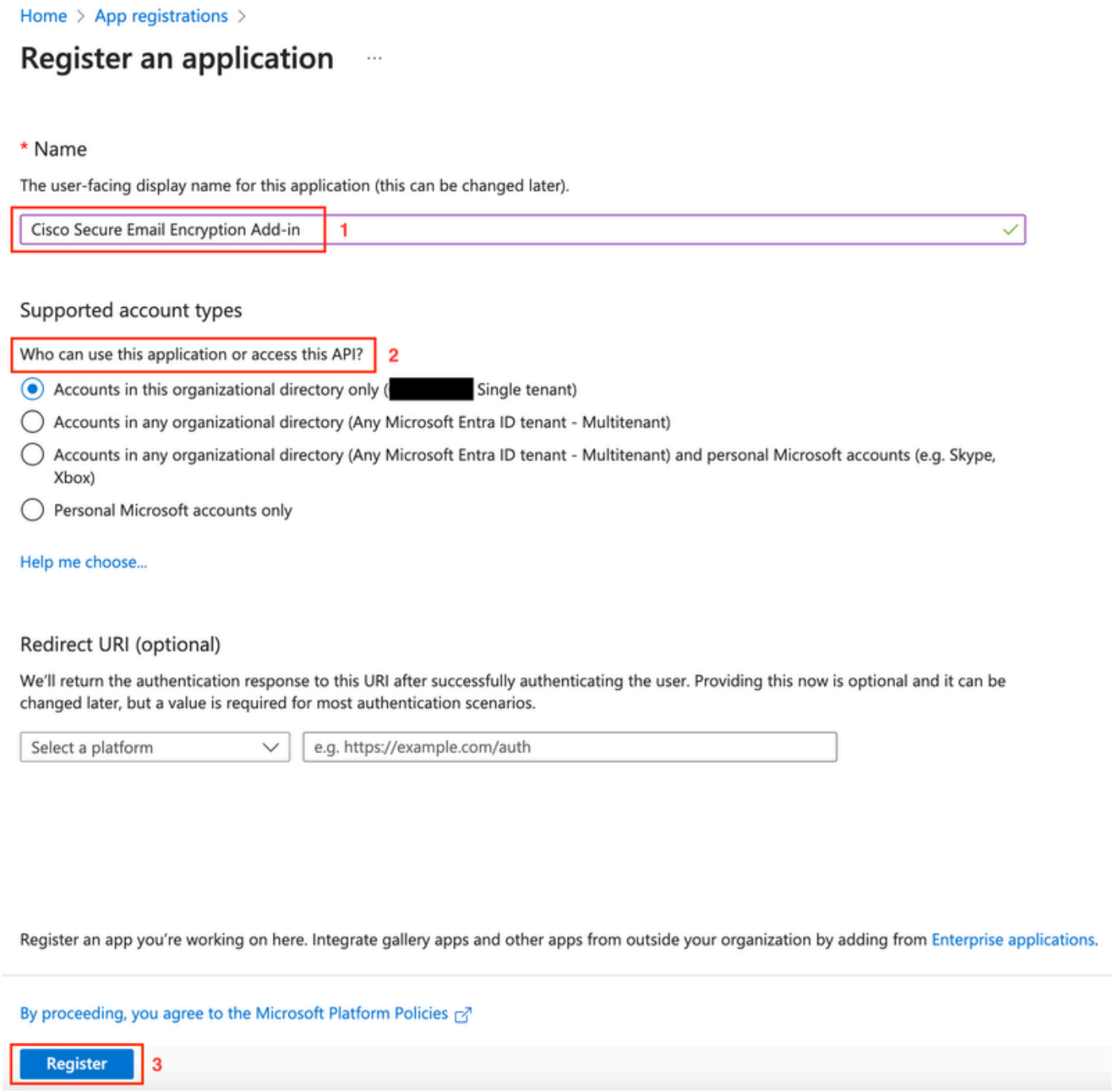
2. En el menú de la izquierda, expanda Admin Centersy haga clic en Identity.

3. Acceda a Identity > Applications > App registrationsy seleccione New registration.



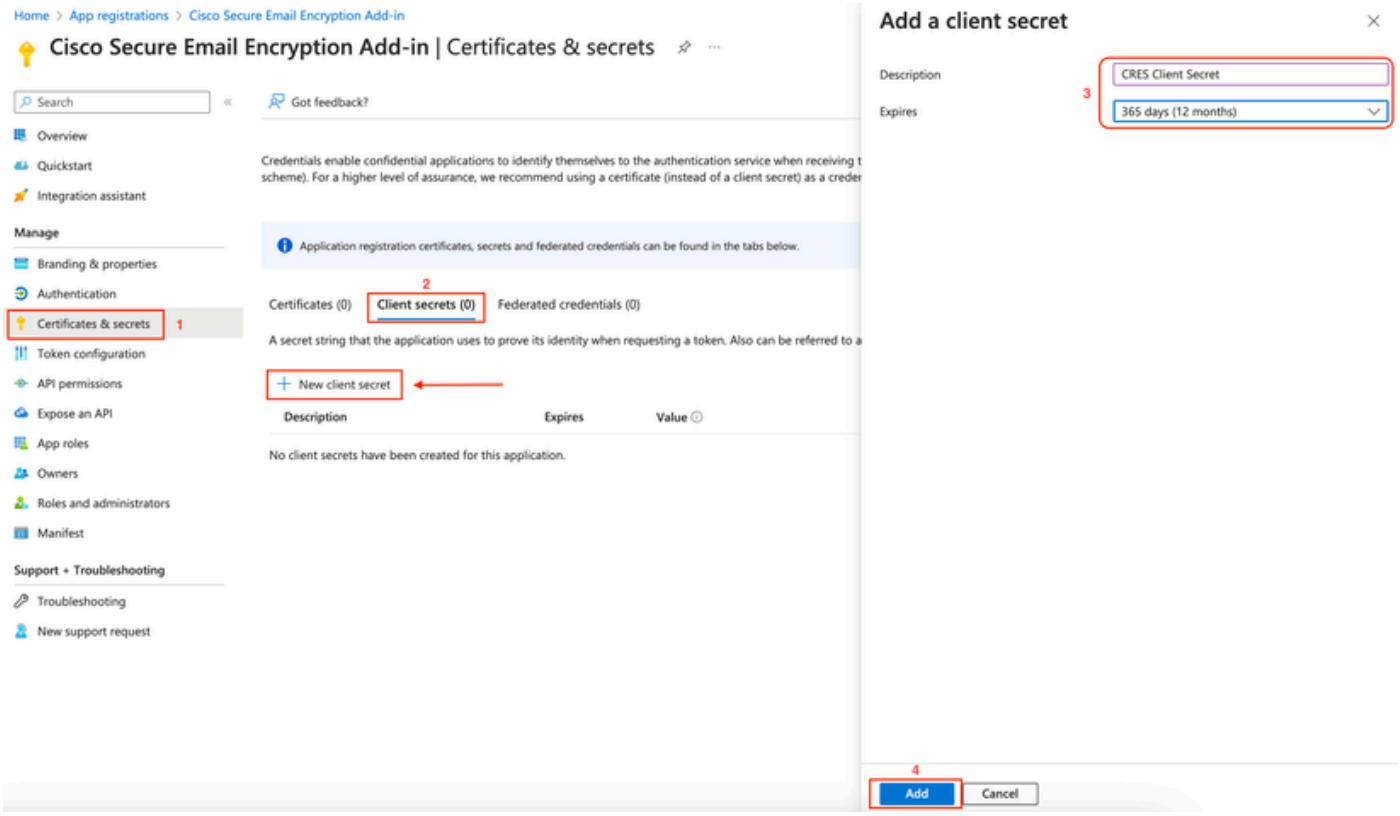
Nota: Si tiene acceso a varios arrendatarios, utilice el icono Configuración del menú superior derecho para cambiar al arrendatario en el que desea registrar la aplicación desde el menú Directorios + Suscripciones.

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



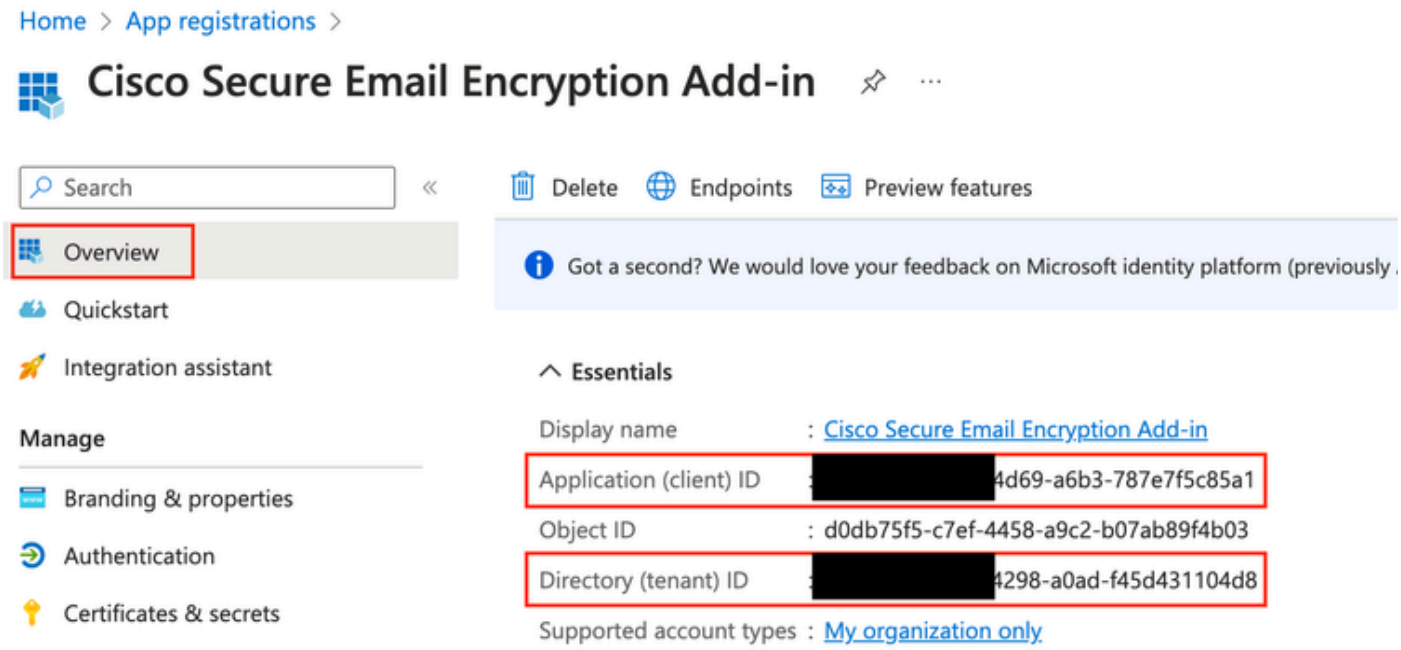
Registrar aplicación

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.

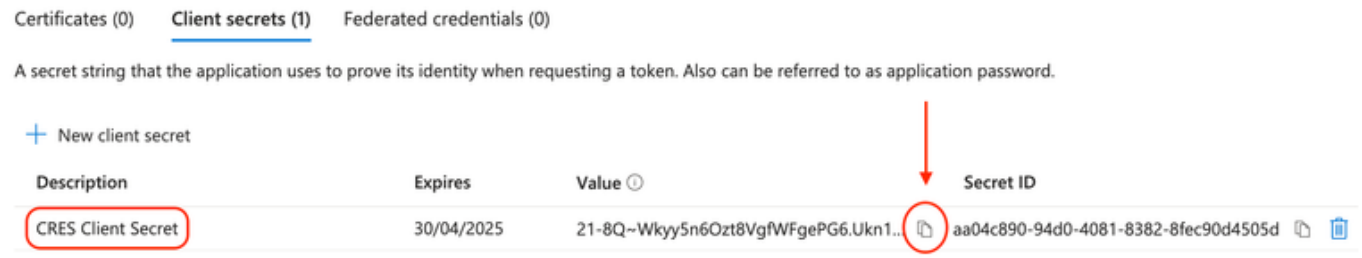


Configurar secreto de cliente

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.



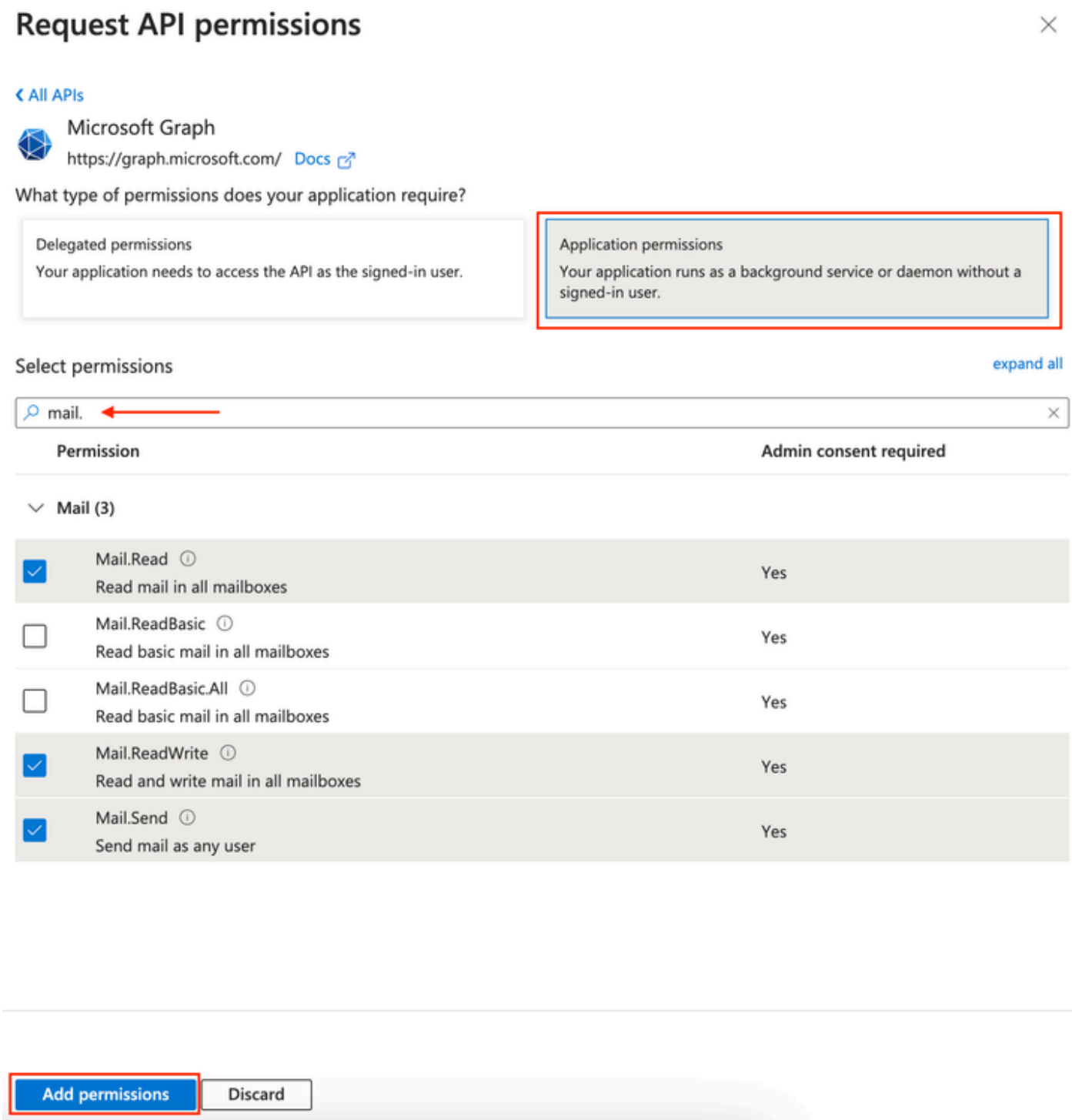
Descripción general de la aplicación Entra ID



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



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]

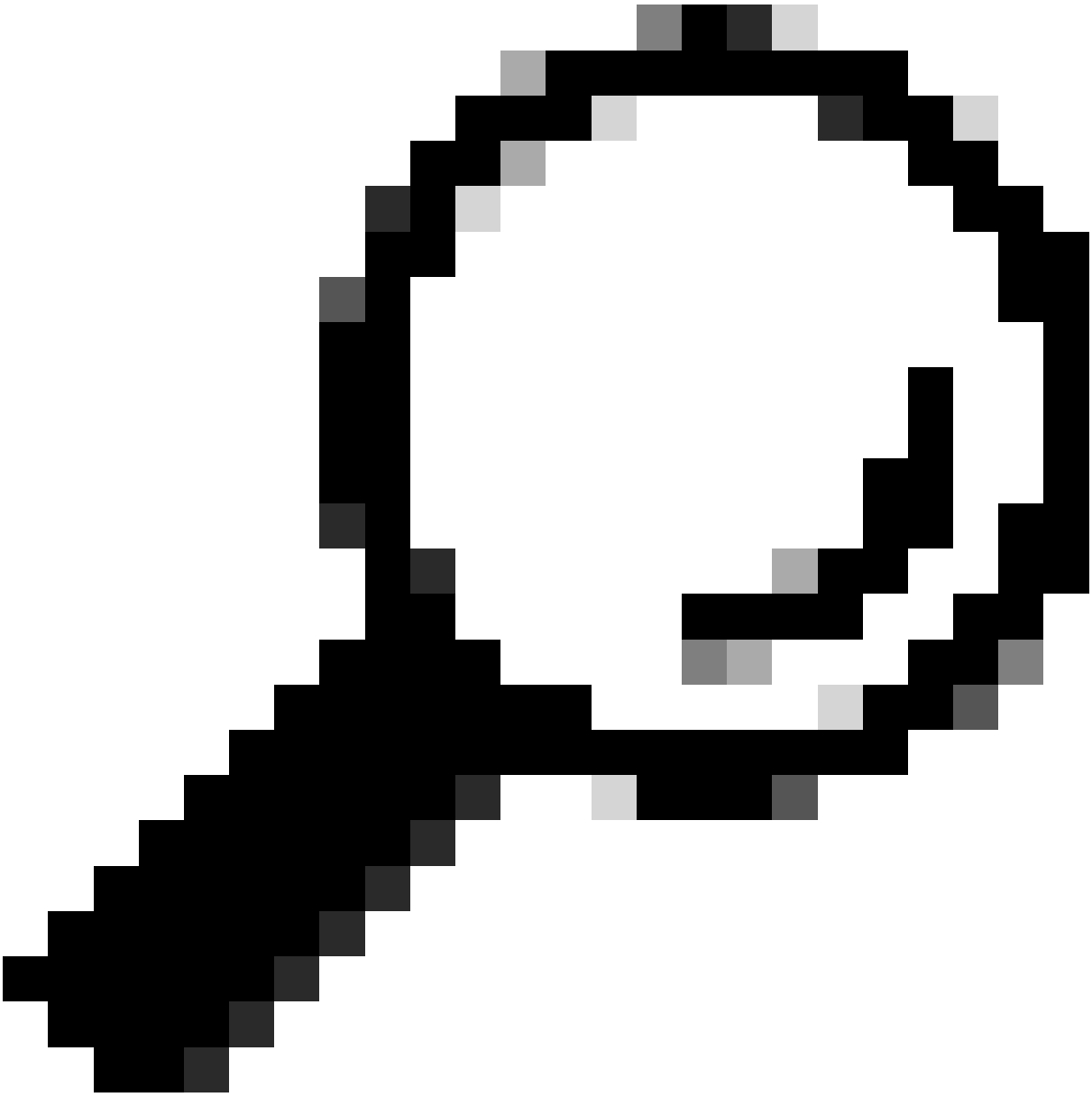
Permisos de API de Microsoft Graph

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

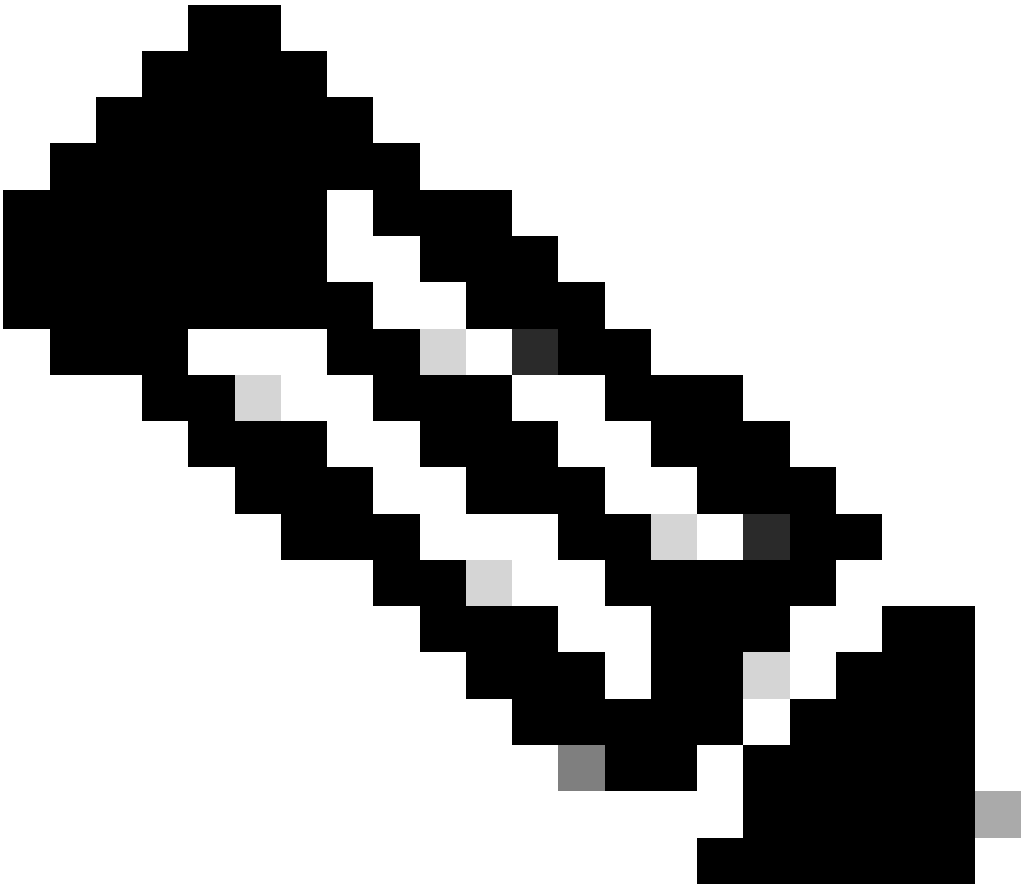
1. Inicie sesión en el portal de administración de Cisco Secure Email Encryption Service (CRES) como administrador de cuentas. (https://res.cisco.com/admin)

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.

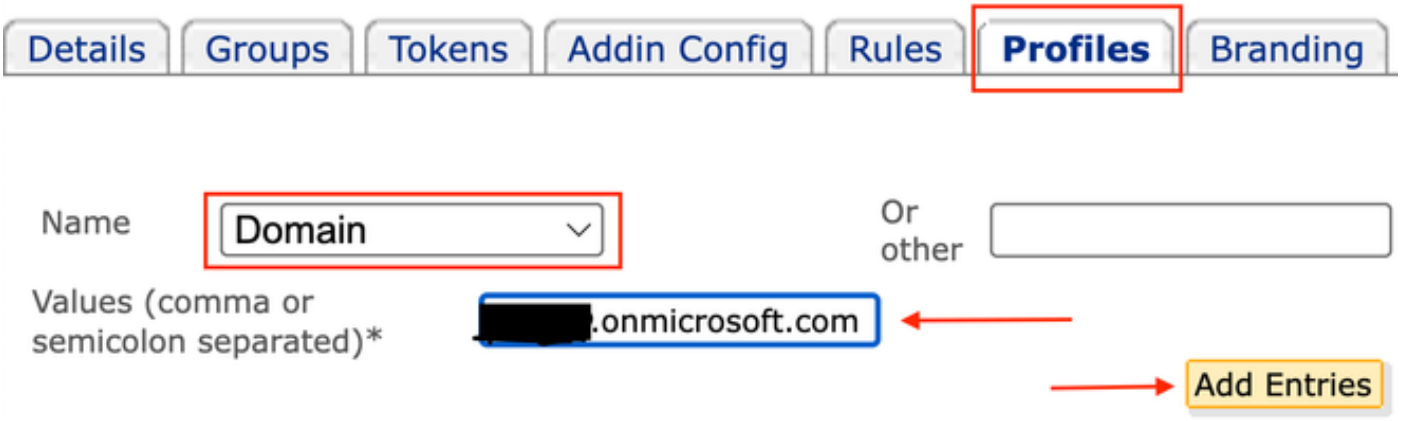
3. Desplácese hastaProfiles, seleccione el tipo de nombre como Dominio e introduzca el nombre de dominio de correo electrónico en Valores. Haga clic **Add Entries** y espere de 5 a 10 segundos. (No actualice la página del explorador ni desplácese a otra página hasta que se haya agregado correctamente).



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.

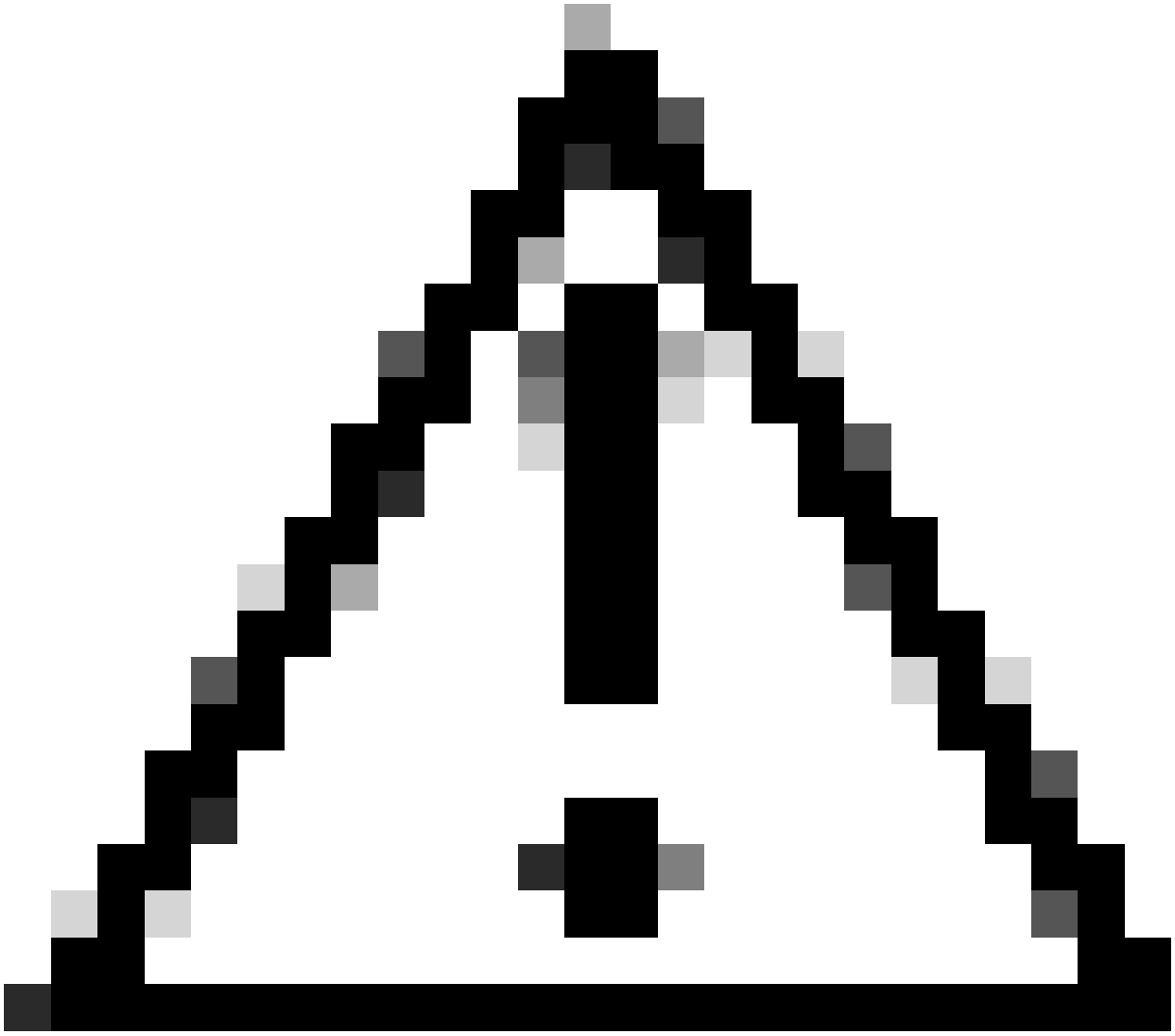


Perfiles del portal de administración de CRES

4. Acceda a la Add-in Configpestaña.

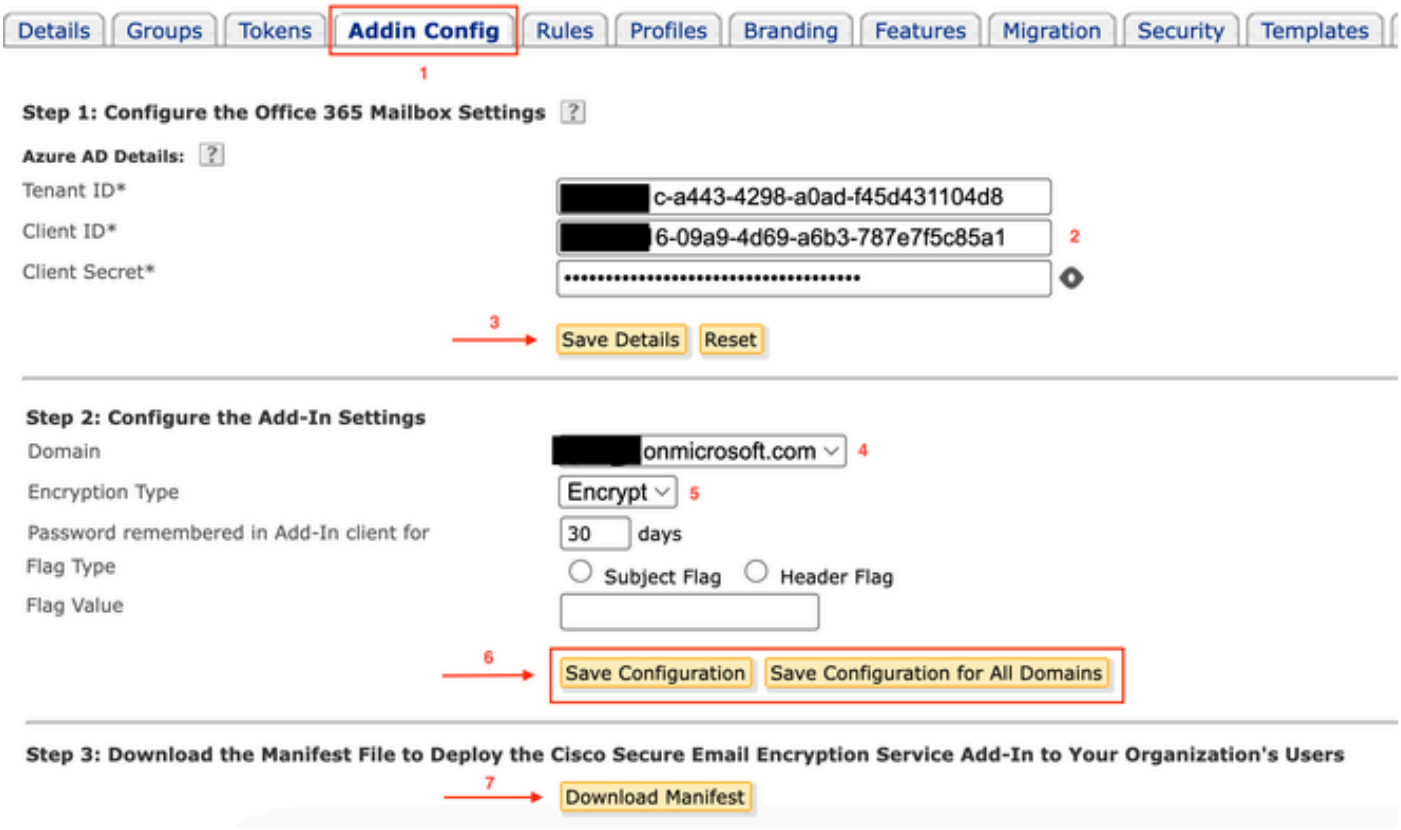
Paso 1: introduzca el arrendatario, la ID de cliente y el secreto obtenidos de la ID de Entra en Detalles de Azure AD. Haga clic en Save Details.

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.

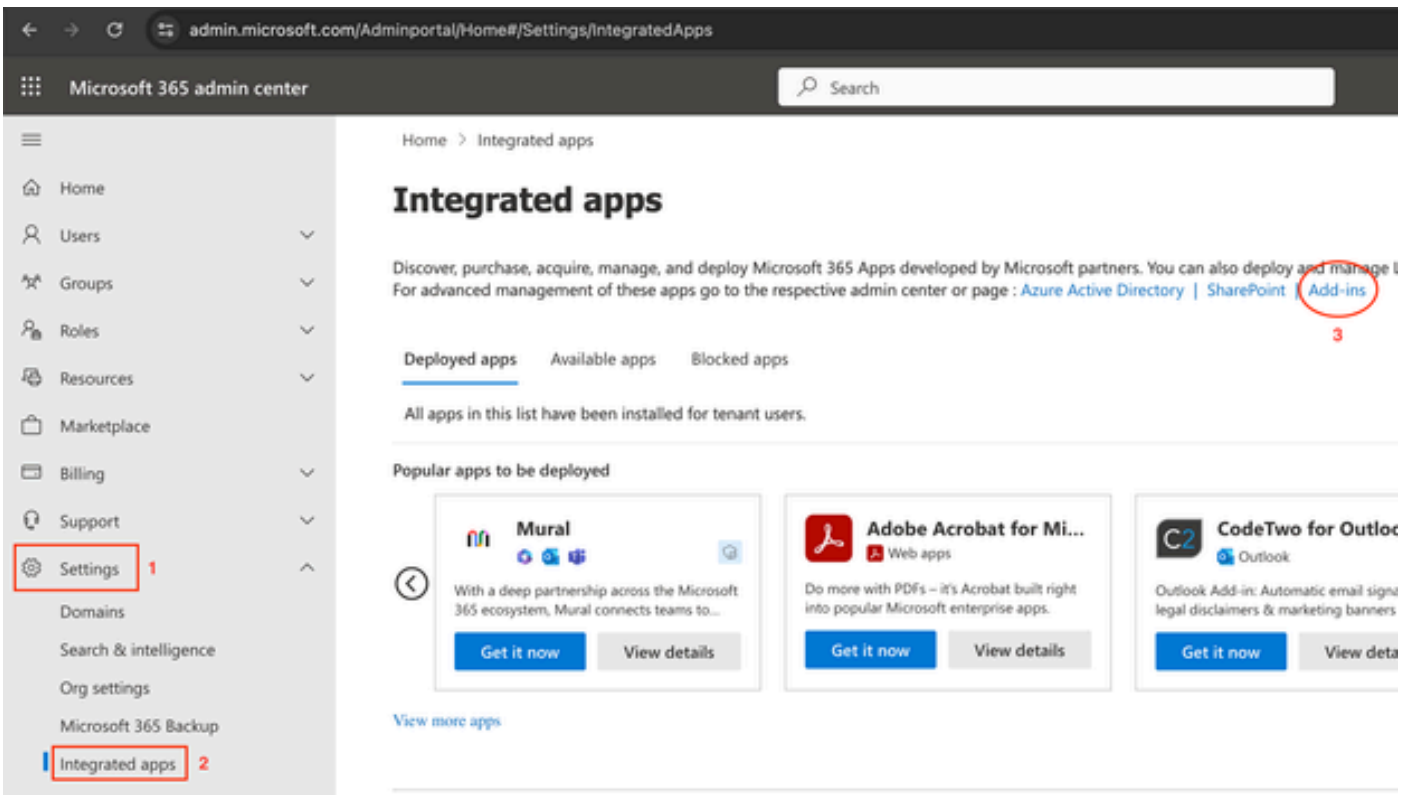


Configuración del complemento del portal de administración de CRES

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

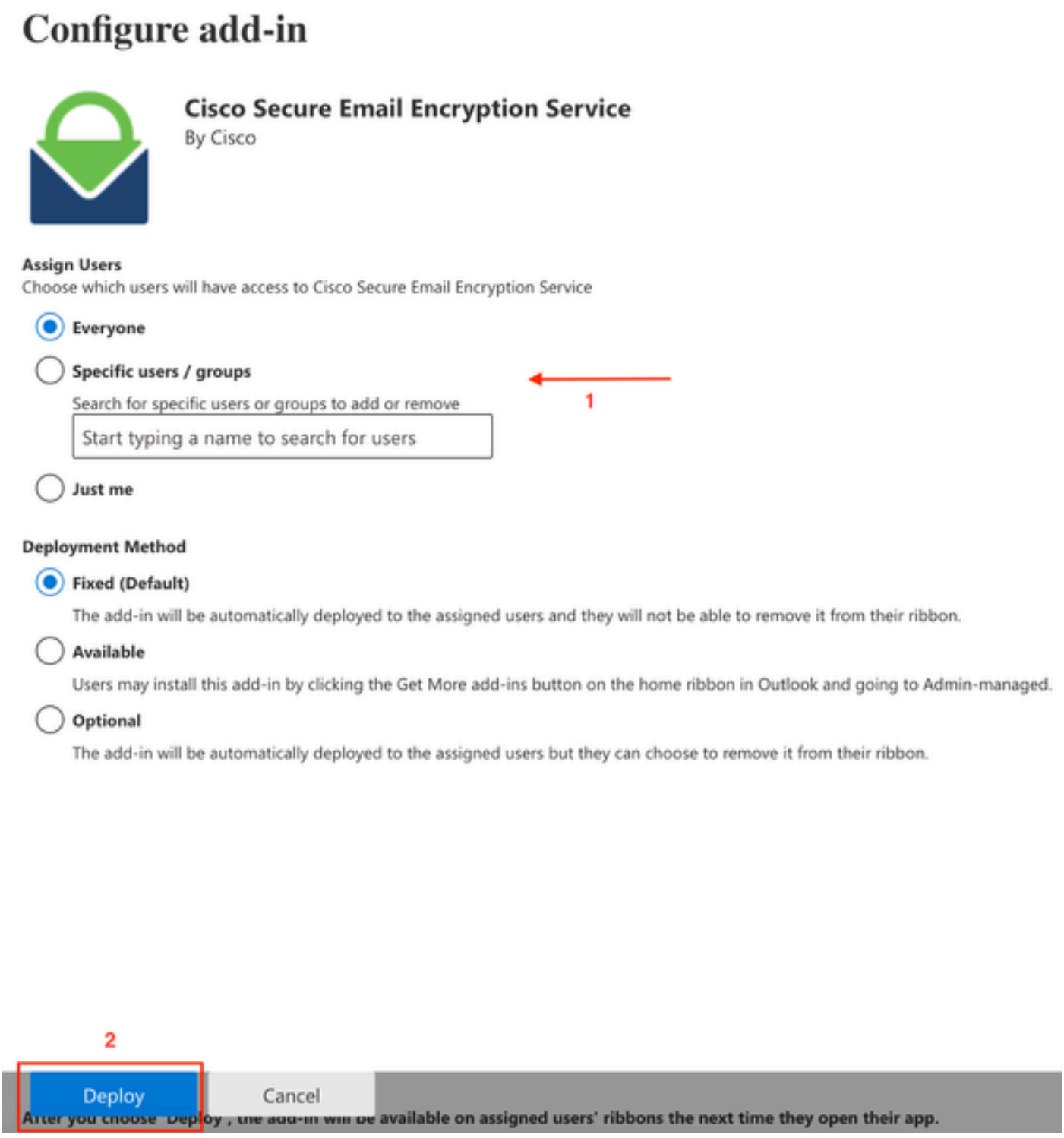
1. Inicie sesión en el Centro de administración de Microsoft 365 como administrador. (Microsoft 365 Admin Center).

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



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 Specifc Users/groupsy haga clic en Deploy.



Configuración del complemento O365 de Microsoft

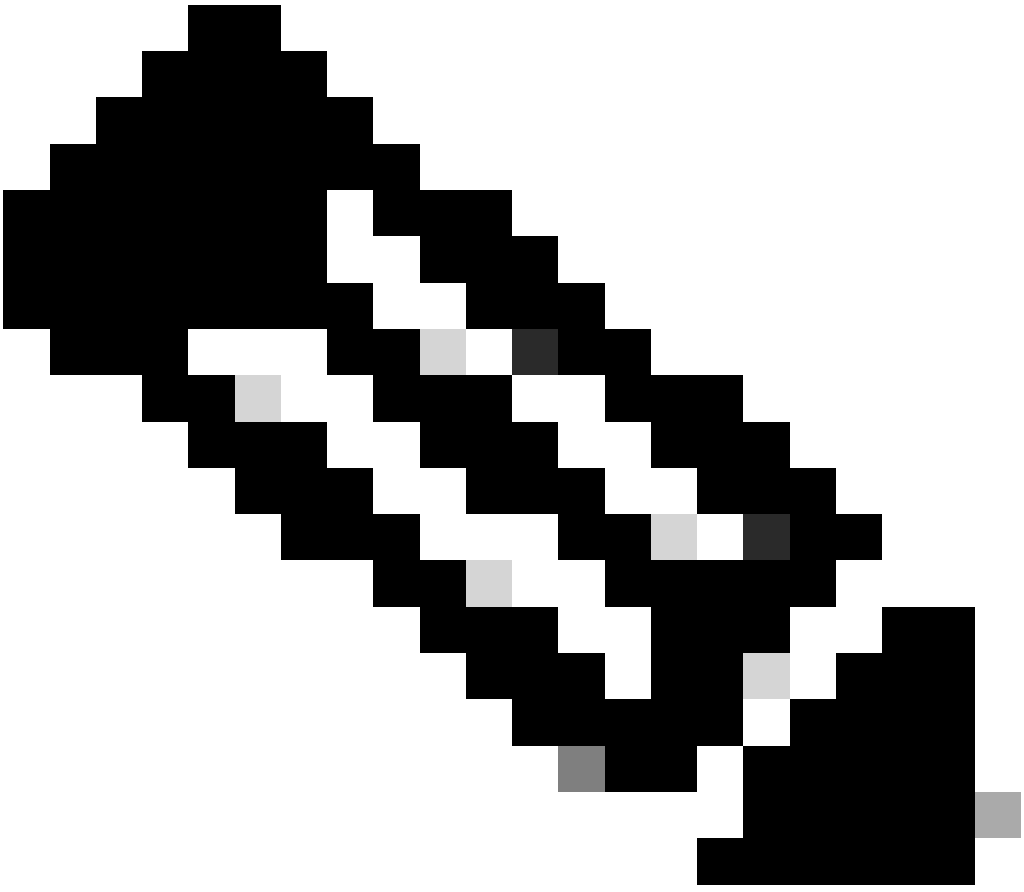
5. Una vez implementado correctamente el complemento, puede tardar hasta 12 horas en mostrarse en las cintas de opciones de los usuarios

finales (Cliente de Outlook).

Verificación

Utilize 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.



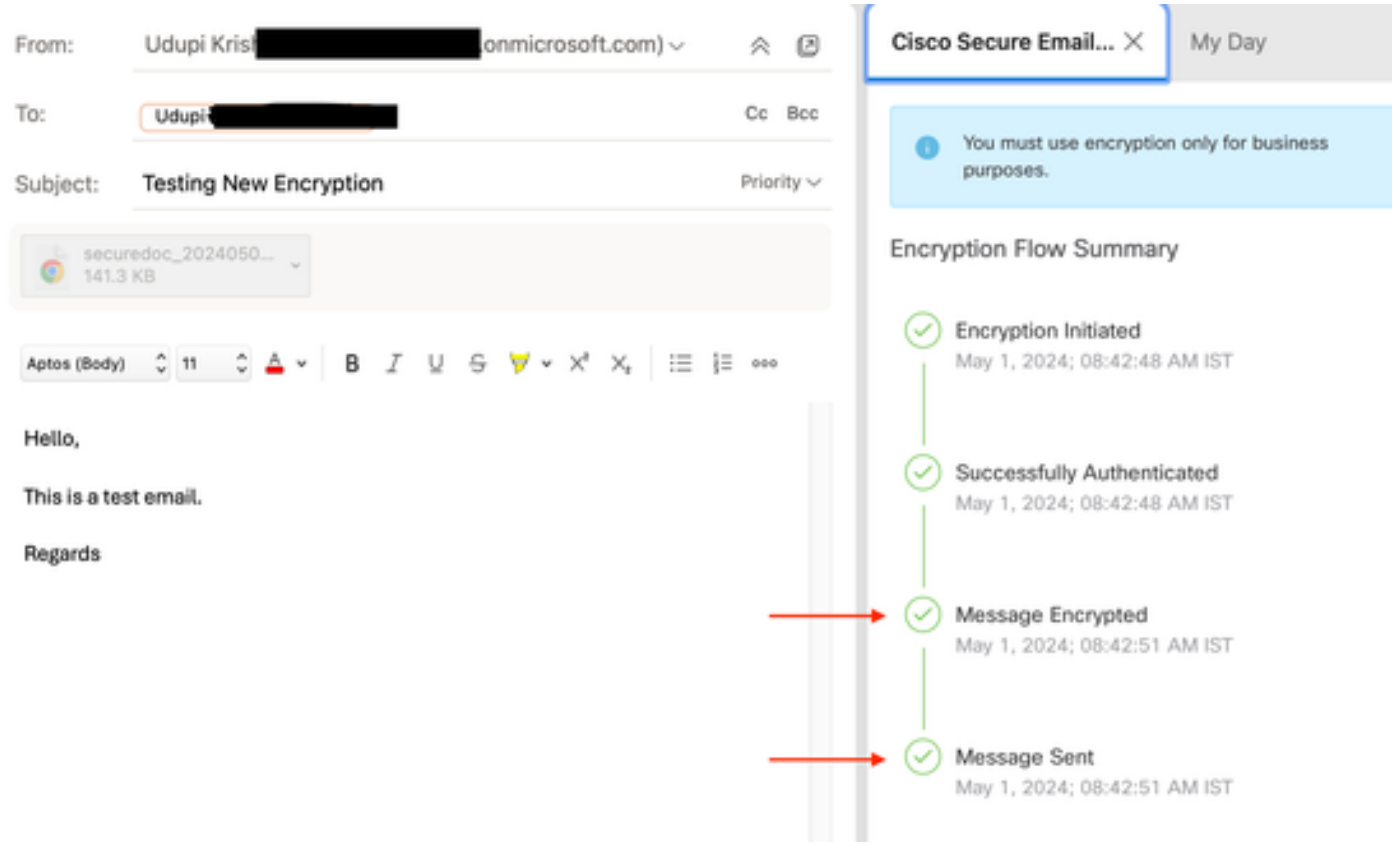
Nota: si el tipo de cifrado (establecido por el administrador) es Cifrar, asegúrese de que ha completado el mensaje y agregado destinatarios válidos antes de continuar con el siguiente paso. Después del paso 3, el mensaje se cifra y se envía inmediatamente.

---

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).



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).