

# Configurar o Suplemento de Criptografia de Email Usando o Microsoft O365

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Práticas recomendadas para implantar o suplemento do Cisco Secure Email Encryption Service](#)

[Configurar](#)

[Registro do Aplicativo Suplementar do Serviço de Criptografia de Email Seguro da Cisco](#)

[Definir configurações de domínio e suplemento no portal de administração do Cisco Secure Email Encryption \(CRES\)](#)

[Carregar Arquivo de Manifesto no Microsoft 365 para Implantar o Suplemento de Serviço de Criptografia de Email](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve como configurar a implantação centralizada do suplemento do serviço de criptografia de e-mail da Cisco através do Microsoft Office 365.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Suplemento de criptografia de e-mail da Cisco 10.0.0

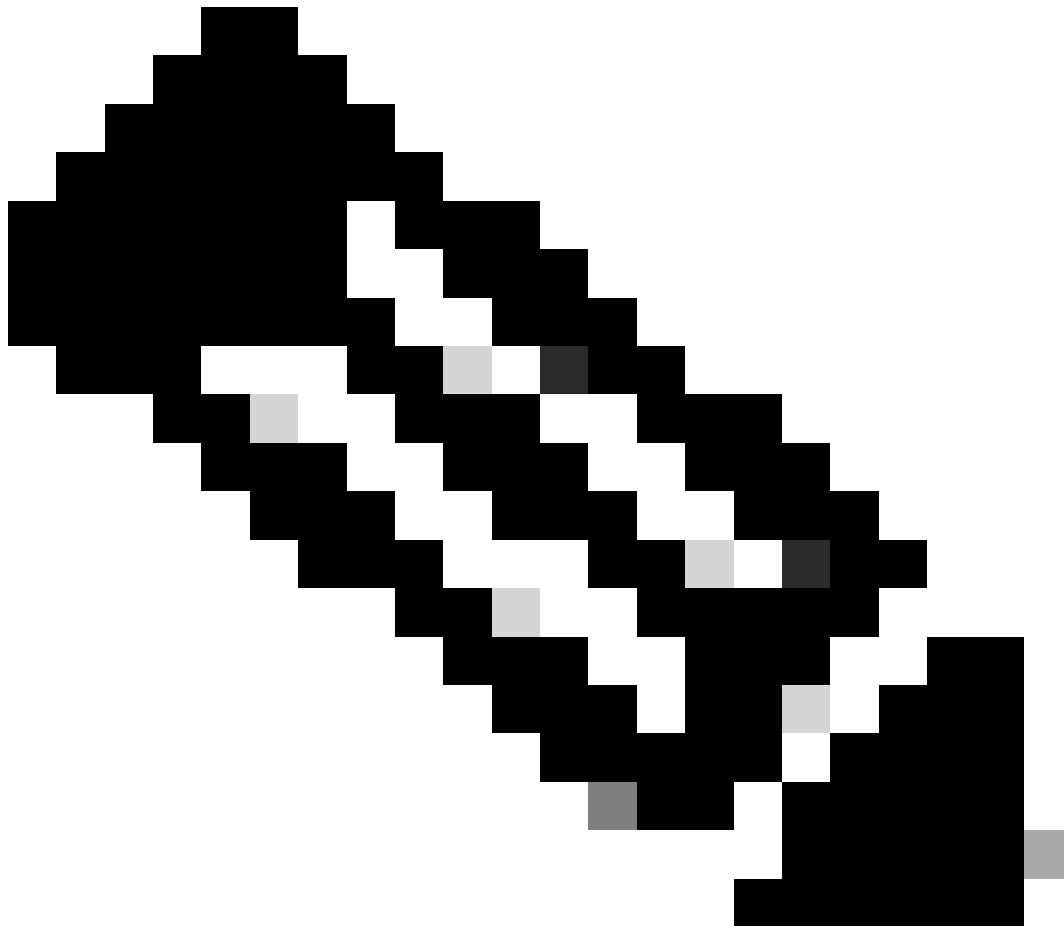
- Microsoft Exchange Online
- Microsoft Entra ID (anteriormente conhecido como Azure AD)
- Outlook para O365 (Mac OS, Windows)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

O Add-in Cisco Secure Email Encryption Service permite que seus usuários finais criptografem suas mensagens diretamente do Microsoft Outlook com um único clique. Este Suplemento pode ser implantado no Microsoft Outlook (para Windows e macOS) e no Outlook Web App.

---



Observação: este documento é ideal para todos os usuários finais que planejam usar o suplemento usarem a assinatura do Office 365/Microsoft 365 e todos os usuários finais

---

---

que planejam usar o suplemento são usuários registrados do Serviço de Criptografia de Email Seguro da Cisco.

---

## Práticas recomendadas para implantar o suplemento do Cisco Secure Email Encryption Service

- Fase de Teste - Implantar o Suplemento em um pequeno conjunto de usuários finais em um departamento ou função. Avalie os resultados e, se obtiver êxito, passe para a próxima fase.
- Fase piloto - Implantar o suplemento para mais usuários finais de diferentes departamentos e funções. Avalie os resultados e, se obtiver êxito, passe para a próxima fase.
- Fase de produção - Implantar o suplemento para todos os usuários.

## Configurar

### Registro do Aplicativo Suplementar do Serviço de Criptografia de Email Seguro da Cisco

1. Faça login no Microsoft 365 Admin Center como pelo menos um Administrador de Aplicativos de Nuvem ([Microsoft 365 Admin Center](#)).
  2. No menu à esquerda, **expanda** Admin Center e clique em Identity.
  3. Navegue até Identity > Applications > App registration e selecione New registration.
- 
-



**Observação:** se você tiver acesso a vários Locatários, use o ícone Configurações no menu superior direito para alternar para o Locatário no qual deseja registrar o aplicativo no menu Diretórios + Assinaturas.

---

4. Informe um Nome de Exibição para o Aplicativo, selecione as contas que podem usar o Aplicativo e clique em 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

*Registrar aplicativo*

5. Após o registro bem-sucedido, navegue até o Aplicativo para configurar o Segredo do Cliente em Certificates & Secrets. Escolha a expiração de acordo com a conformidade regulatória da organização.

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 Segredo do Cliente

6. Na página Visão Geral da Aplicação Registrada, copie o Application (client) ID e Directory (tenant) ID. Copie o **Client Secret** de Certificados e segredos gerados na etapa 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](#)

### Visão geral do aplicativo 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 Segredo do Cliente*

7. Navegue até o **Aplicativo de criptografia de e-mail registrado** e navegue até API permissions. Clique Add a permission e selecione as permissões necessárias do aplicativo Microsoft Graph:

- Email.Ler
- Email.LeituraGravação
- Email.Enviar
- Usuário.Ler.Tudo

# 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

Configuração de Permissão do Microsoft Graph

7. Clique Grant Admin Consent for <tenant-name> para conceder ao Aplicativo acesso a Permissões em nome da Organização.

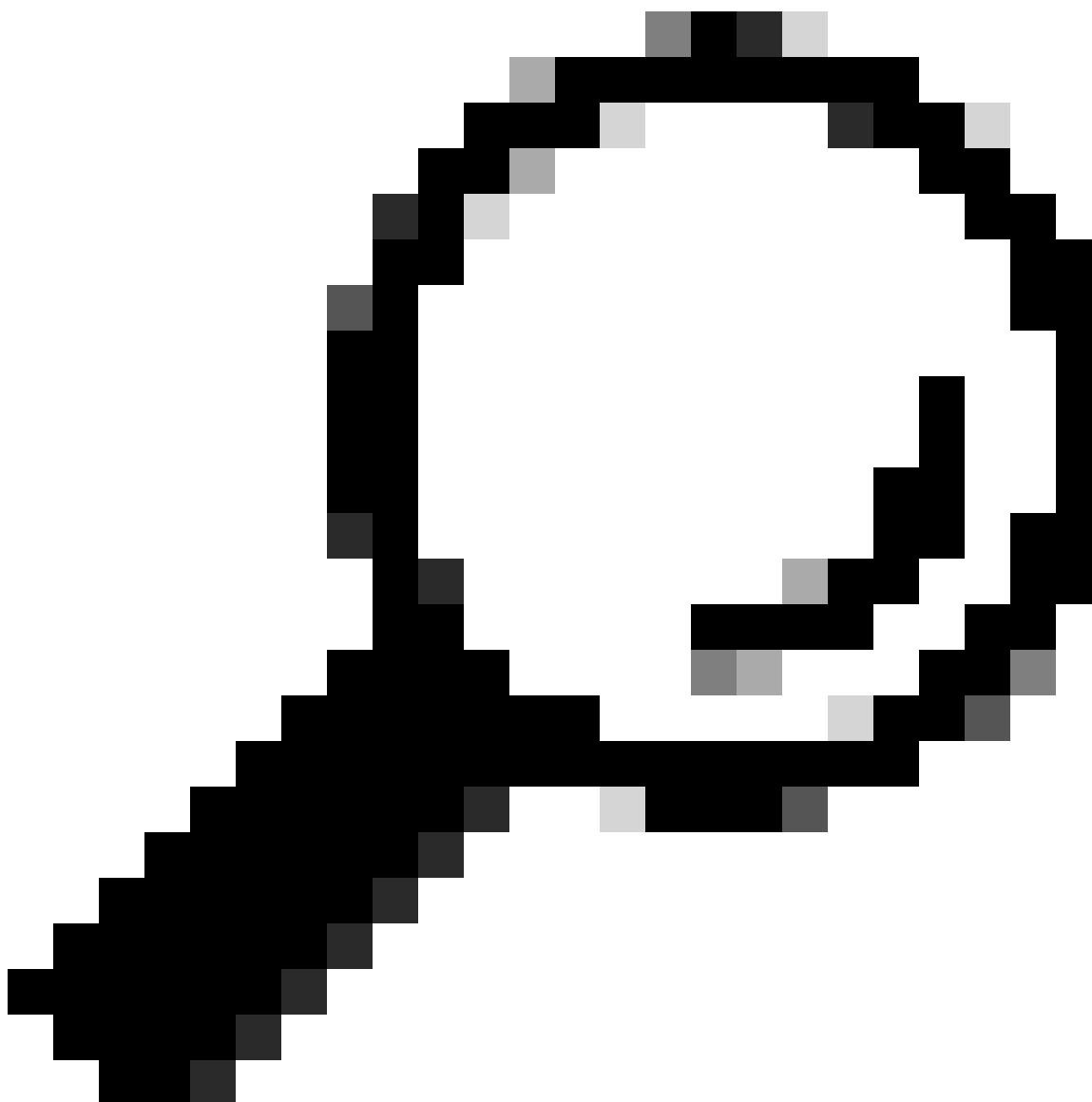
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				...
Mail.Read	Application	Read mail in all mailboxes	Yes	✔ Granted for [redacted] ...
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✔ Granted for [redacted] ...
Mail.Send	Application	Send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

Permissões de API do Microsoft Graph



Definir configurações de domínio e suplemento no portal de administração do Cisco Secure Email Encryption (CRES)

1. Faça login no portal de administração do Cisco Secure Email Encryption Service (CRES) como administrador de conta. ([Serviço de criptografia de e-mail seguro](#))
2. Navegue até Accounts > Manage Accounts. Clique no número de conta atribuído à sua organização ou na conta na qual você planeja configurar o Suplemento de Criptografia de Email.
3. Navegue até Profiles, selecione o **tipo de Nome** como Domínio e insira seu **nome de domínio de e-mail** em Valores. Clique **Add Entries** e aguarde de 5 a 10 segundos. (Não atualize a página do navegador ou navegue para uma página diferente até que ela seja adicionada com êxito).

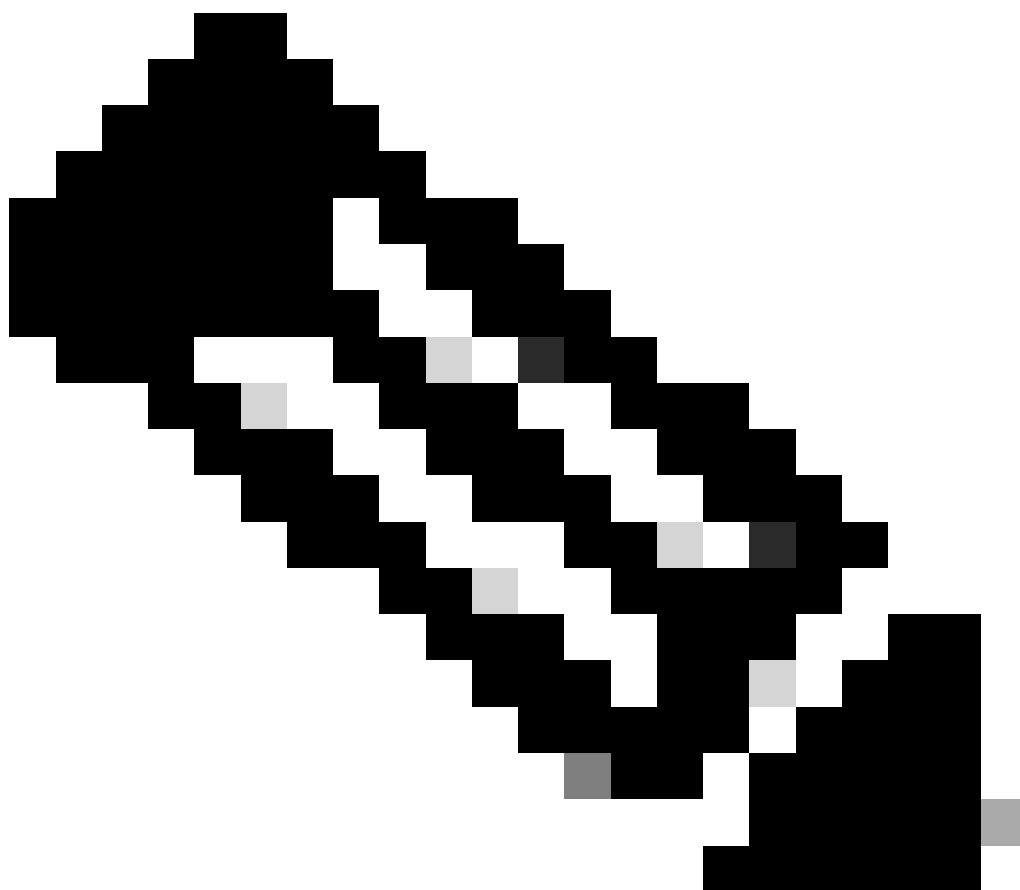


---

**Dica:** repita as mesmas etapas para adicionar outros domínios de e-mail que usarão o serviço de criptografia de e-mail em sua organização.

---

---



**Observação:** entre em contato com o Centro de assistência técnica da Cisco para adicionar os domínios de e-mail ao portal de administração do CRES.

---

The screenshot shows a navigation bar with tabs: Details, Groups, Tokens, Addin Config, Rules, Profiles (highlighted with a red box), and Branding. Below the tabs, the 'Name' field is a dropdown menu with 'Domain' selected (highlighted with a red box). To the right, there is a text input field labeled 'Or other'. Below the 'Name' field, the 'Values (comma or semicolon separated)\*' field contains a domain name (partially obscured by a black box, ending in '.onmicrosoft.com') which is highlighted with a blue box. A red arrow points from this field to the 'Add Entries' button, which is highlighted with a yellow box.

*Perfis do portal de administração do CRES*

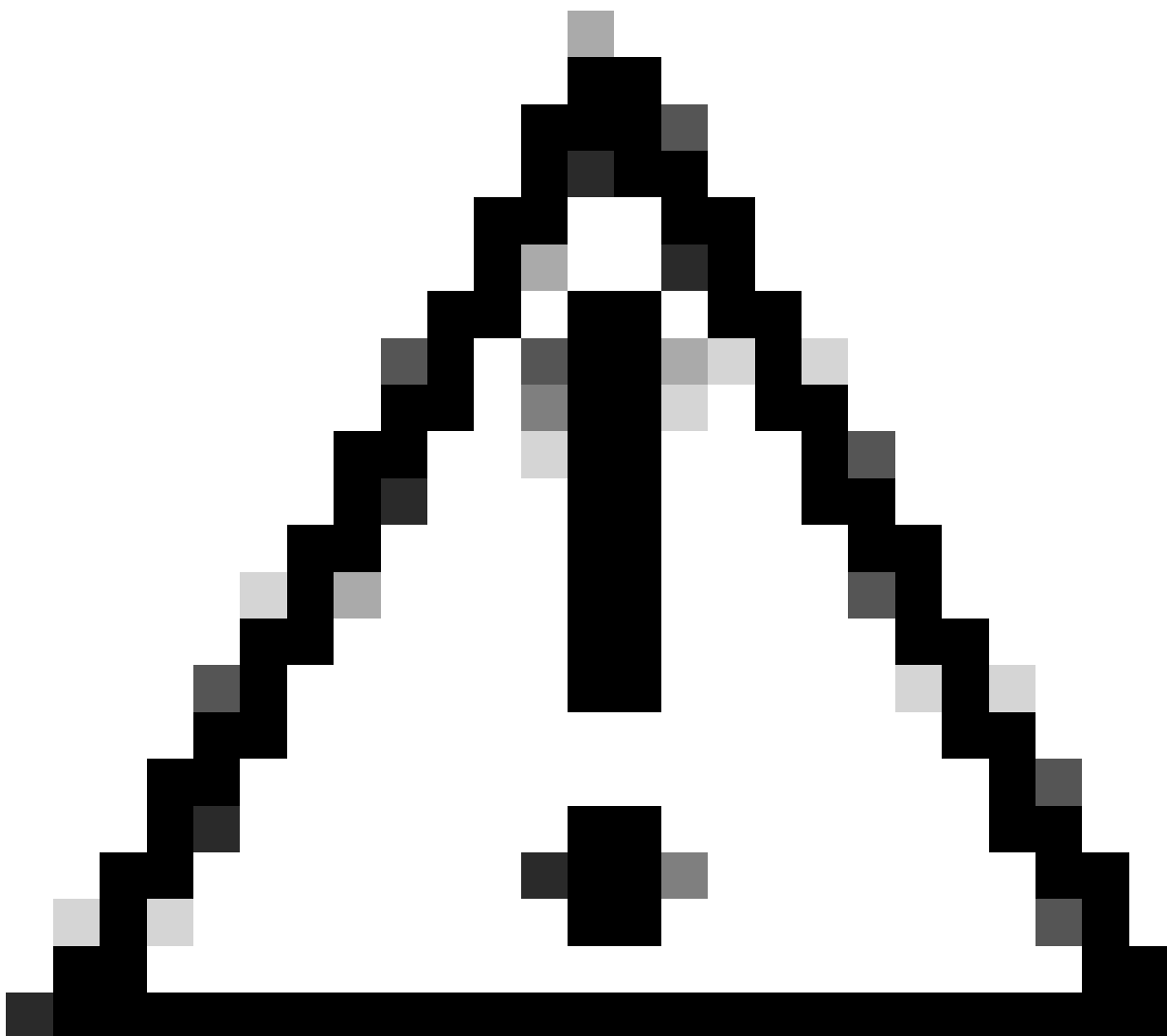
4. Navegue até a Add-in Config guia.

Etapa 1: Insira o Espaço, a ID do Cliente e o Segredo obtidos da ID da Entra em Detalhes do Azure AD. Clique em Save Details.

Etapa 2: selecione o domínio, Tipo de criptografia, e clique em Save Configuration. Use Save Configuration para todos os domínios para aplicar as mesmas configurações a todos os domínios adicionados.

---

---



**Cuidado:** não navegue até uma página diferente sem concluir as Etapas 1 e 2 juntas. Se a Etapa 2. não for concluída ao mesmo tempo, os detalhes do Azure AD não serão salvos.

---

Etapa 3: clique em 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**

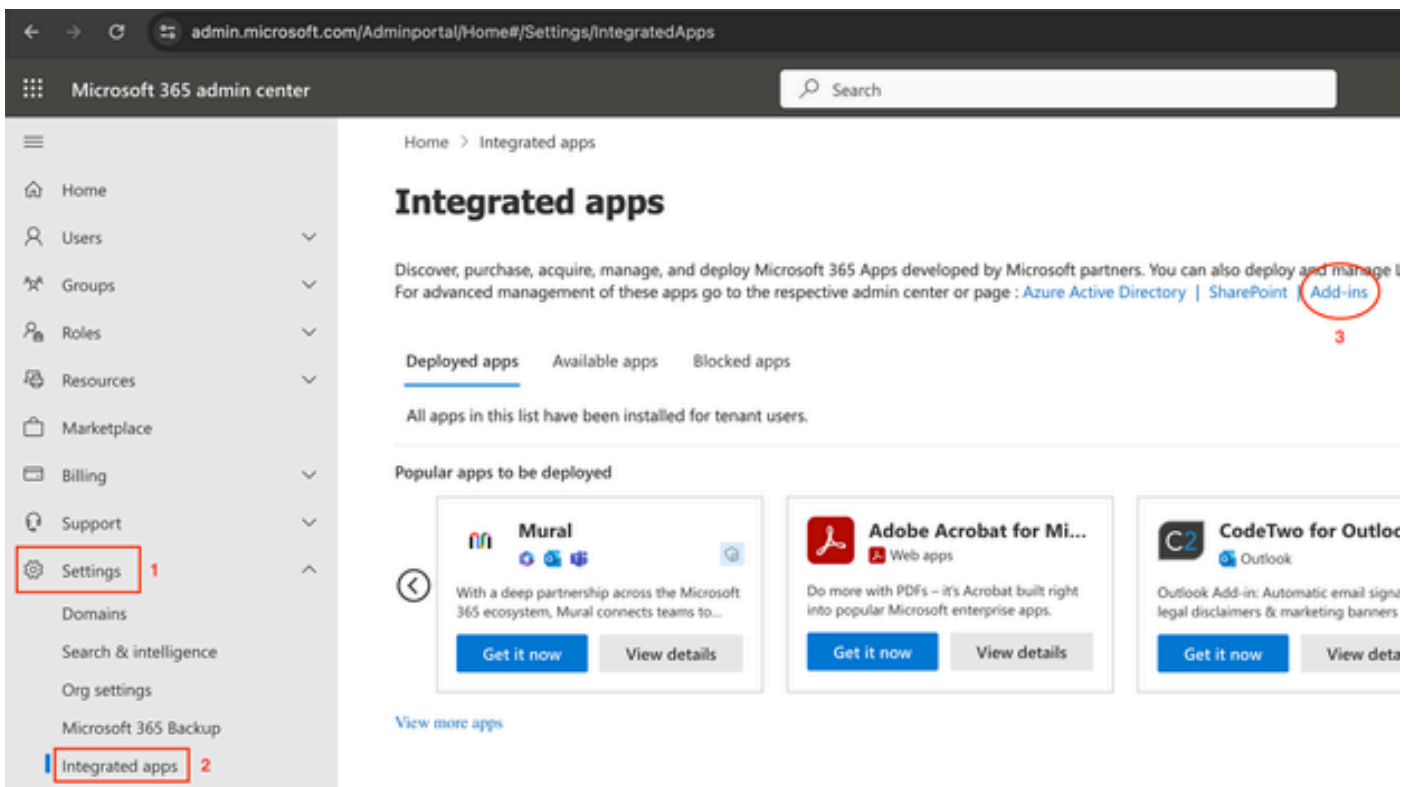
7 → Download Manifest

Configuração de suplemento do portal de administração do CRES

Carregar Arquivo de Manifesto no Microsoft 365 para Implantar o Suplemento de Serviço de Criptografia de Email

1. Efetue login no Microsoft 365 Admin Center como Administrador. ([Centro de administração do Microsoft 365](#)).

2. Navegue até Settings > Integrated apps e clique em **Suplementos**.



3. Clique Deploy Add-in escolha Upload Custom Apps. Selecione I have the manifest file (.xml) on this devicee carregue o arquivo baixado do portal de administração do serviço de criptografia de e-mail da Cisco na etapa anterior. Clique em Upload.

4. Na próxima etapa, atribua usuários que precisam acessar o Cisco Secure Email Encryption Service. Para uma implantação em fases, escolha Specific Users/groupse clique em 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.

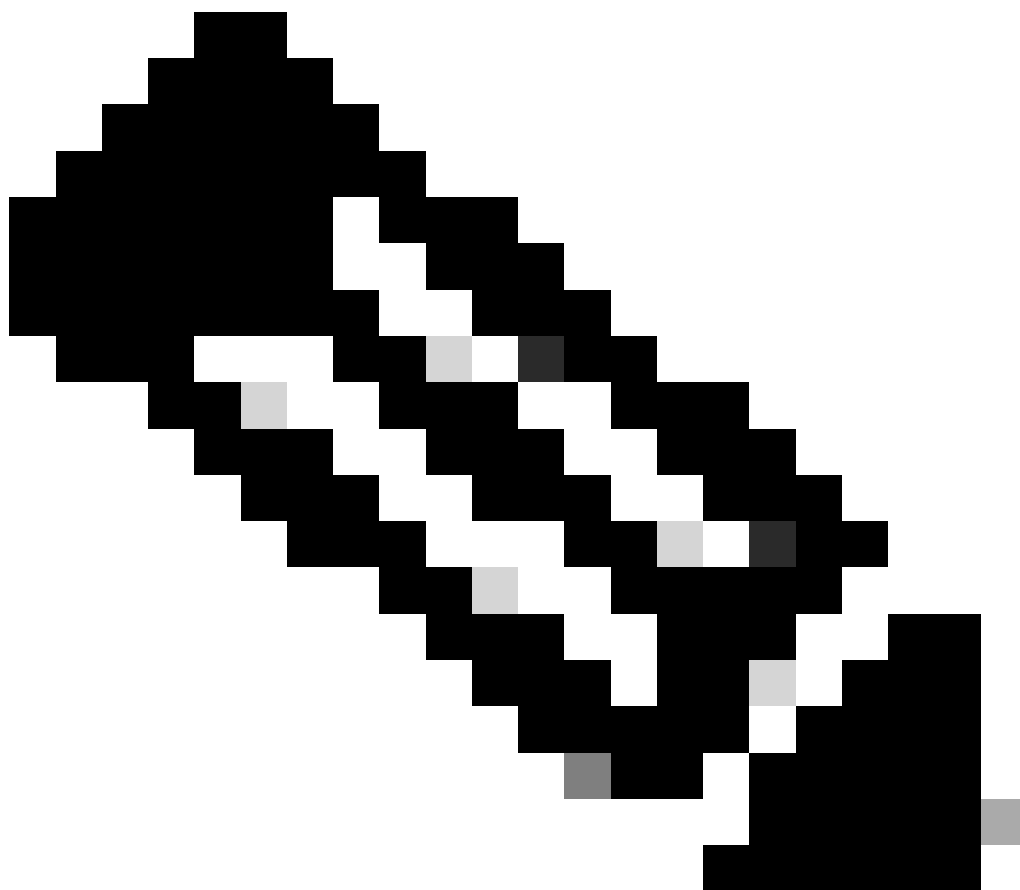
5. Depois que o Suplemento for implantado com êxito, ele poderá levar até 12 horas para ser exibido nas Faixas dos usuários finais (Cliente

Outlook).

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. Inicie o Outlook para Office 365/Microsoft 365 ou Outlook Web App, redija a mensagem que deseja criptografar e adicione pelo menos um destinatário válido a ela.



**Observação:** se o Tipo de criptografia (definido pelo administrador) for Criptografar, certifique-se de ter concluído sua mensagem e adicionado destinatários válidos antes de prosseguir para a próxima etapa. Após a Etapa 3, a mensagem é criptografada e enviada imediatamente.

---

2. Abra/clique no add-in Serviço de Criptografia de Email Seguro da Cisco.

- No Outlook Web App, clique no ícone de reticências (localizado próximo aos botões Enviar e Descartar) e clique em Cisco Secure Email Encryption Service.
- No Outlook para Windows ou MacOS, clique em **Criptografar** na Faixa de Opções ou na Barra de Ferramentas.
- Se você estiver no Outlook para MacOS versão 16.42 ou posterior e estiver usando a interface New Outlook, clique em Cisco Secure Email Encryption Service na Barra de ferramentas.

3. Informe suas credenciais e clique em Sign in. (Somente se o Tipo de criptografia for Sinalizador, clique em Send).

The screenshot displays the Outlook interface for an email titled "Testing New Encryption". The sender is "Udupi Kris" and the recipient is "Udupi". 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..." add-in is active, showing a notification: "You must use encryption only for business purposes." Below this, the "Encryption Flow Summary" is shown as a vertical timeline with four steps, each marked with a green checkmark: "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.

Status de Criptografia do Microsoft Outlook

## Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas



- [Guia do usuário do administrador da conta do serviço de criptografia de e-mail seguro da Cisco](#)
- [Guia do Usuário do Suplemento do Serviço de Criptografia de Email Seguro da Cisco](#)
- [Guia de Registro do Aplicativo Microsoft Entra](#)
- [Suporte técnico e downloads da Cisco](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.