Configurar o Suplemento de Criptografia de Email Usando o Microsoft O365

Contents

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:

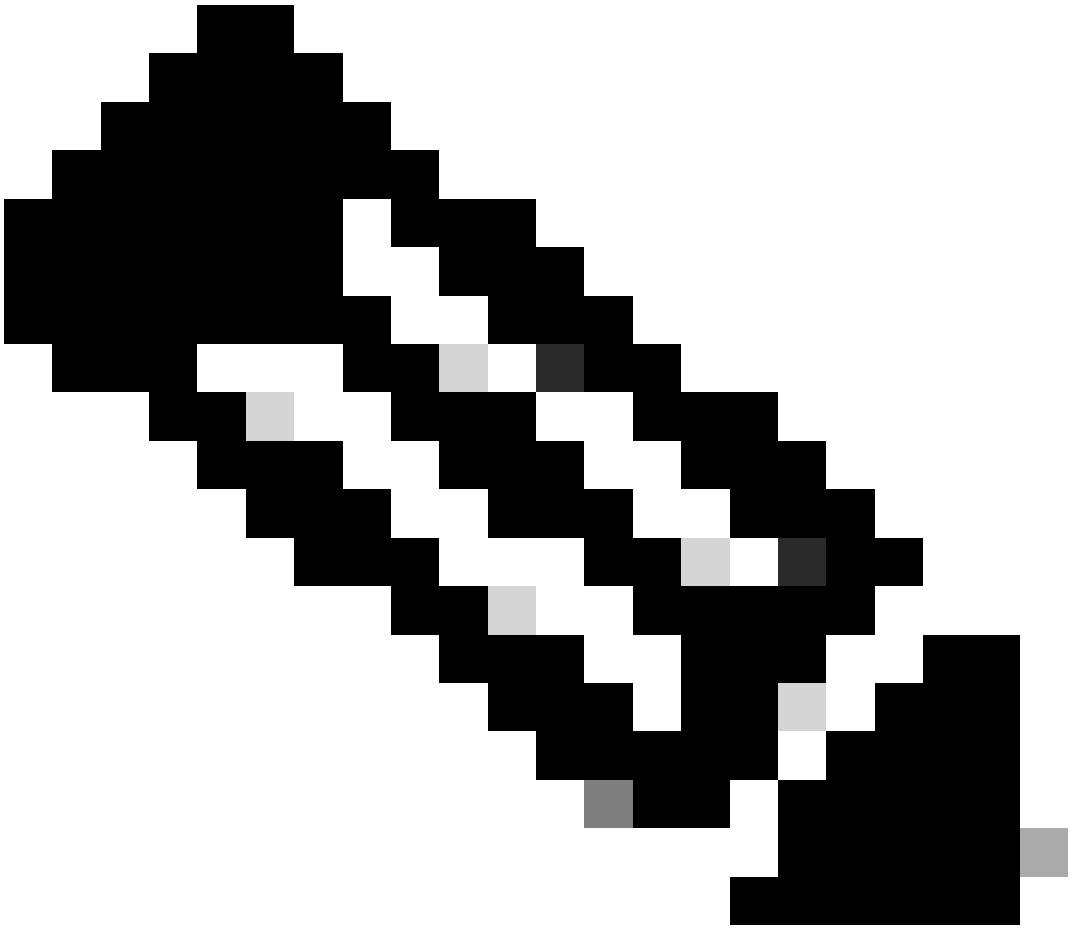
- Suplemento de criptografia de e-mail da Cisco 10.0.0

- 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.

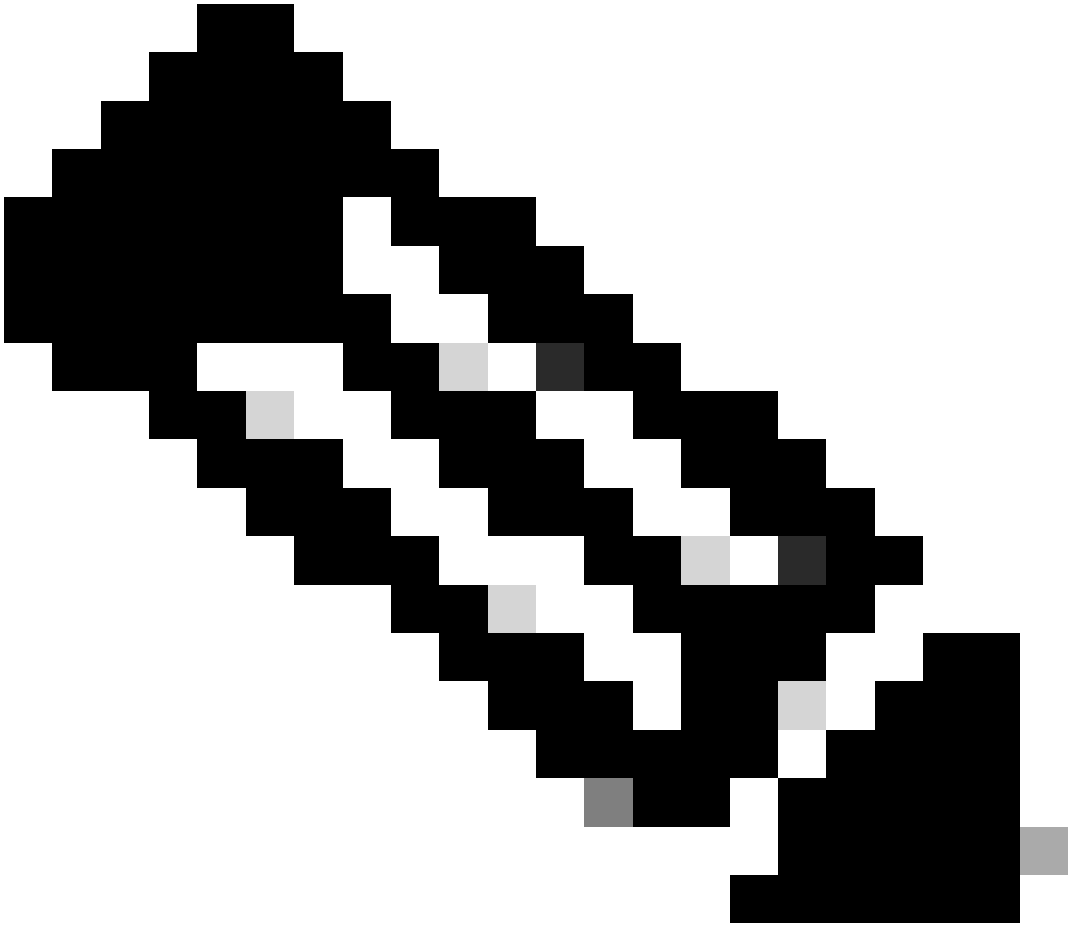
Configurar

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).

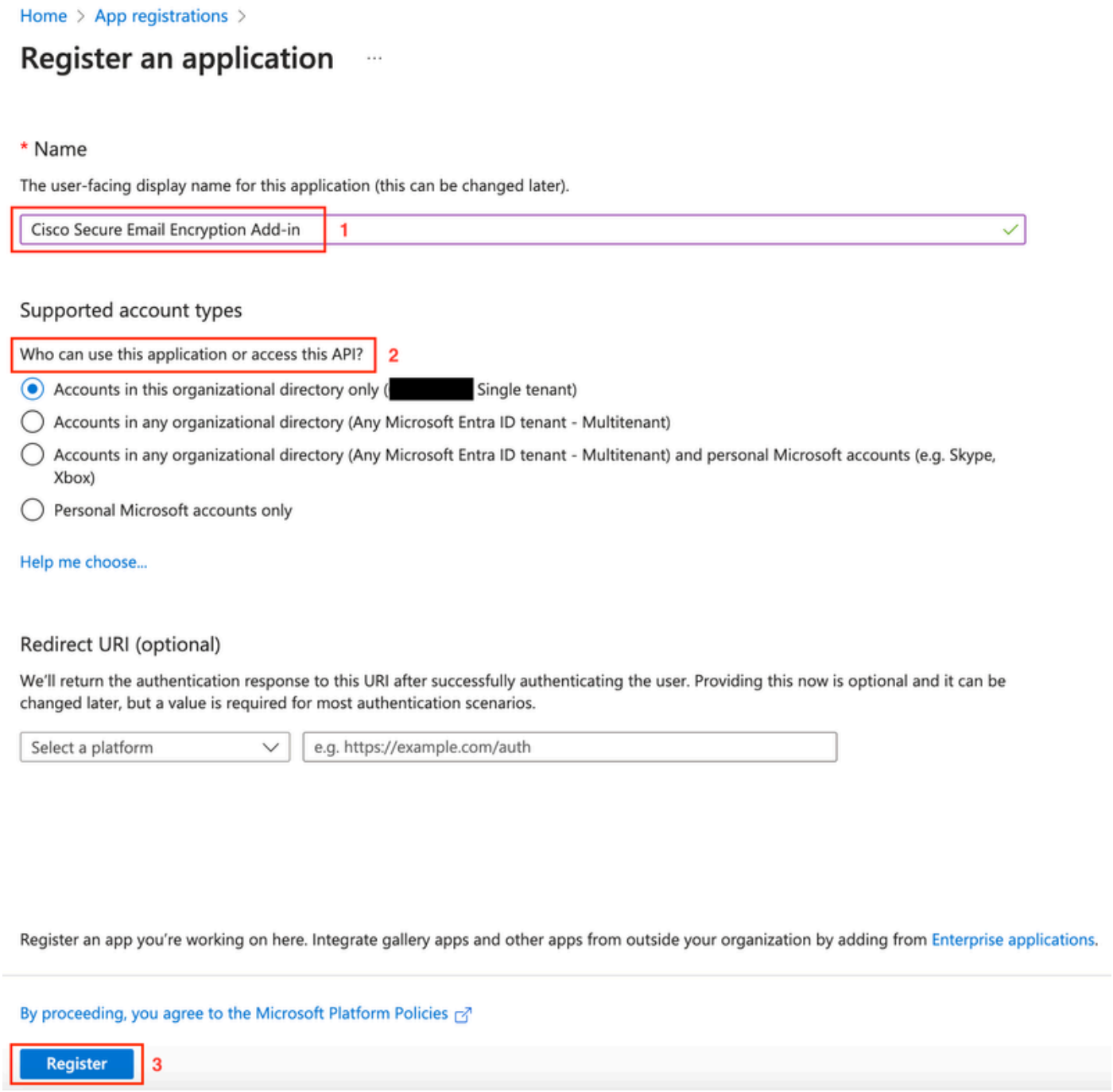
2. No menu à esquerda, expanda Admin Centerse clique em Identity.

3. Navegue até Identity > Applications > App registrationse selecione New registration.



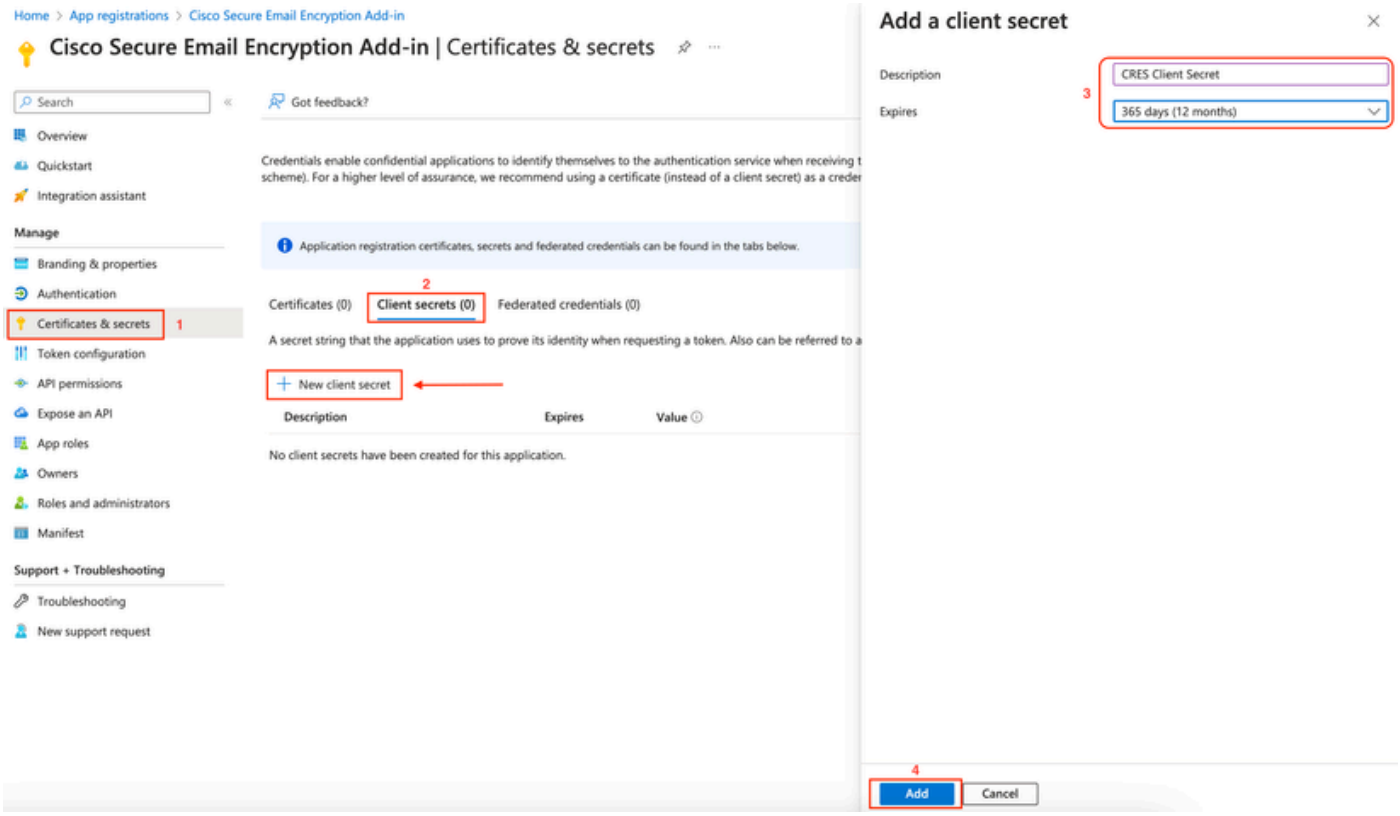
Observação: se você tiver acesso a vários Locatários, use o ícone Configurações no menu superior direito para alternar para o Locatário no qual deseja registrar o aplicativo no menu Diretórios + Assinaturas.

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



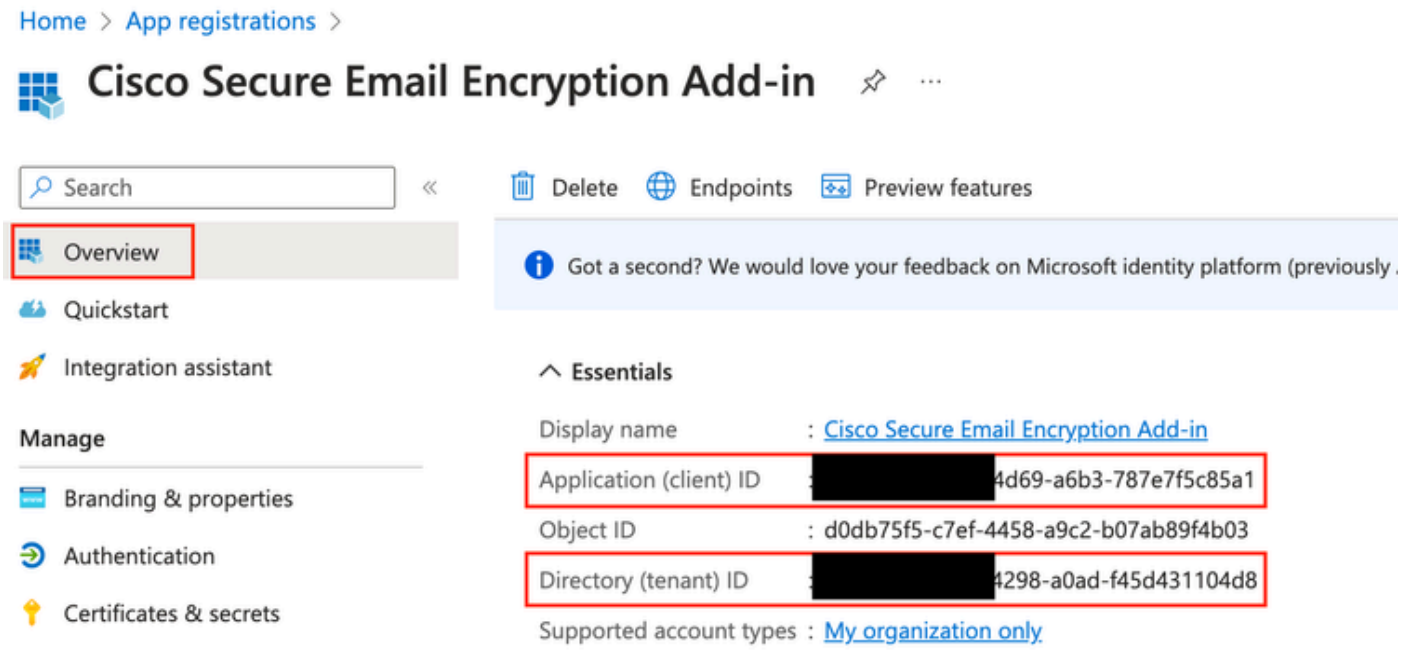
Registrar aplicativo

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.

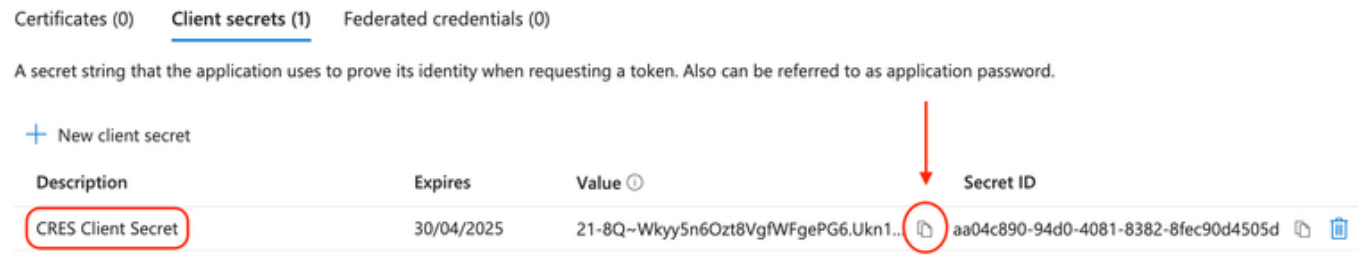


Configurar Segredo do Cliente

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.



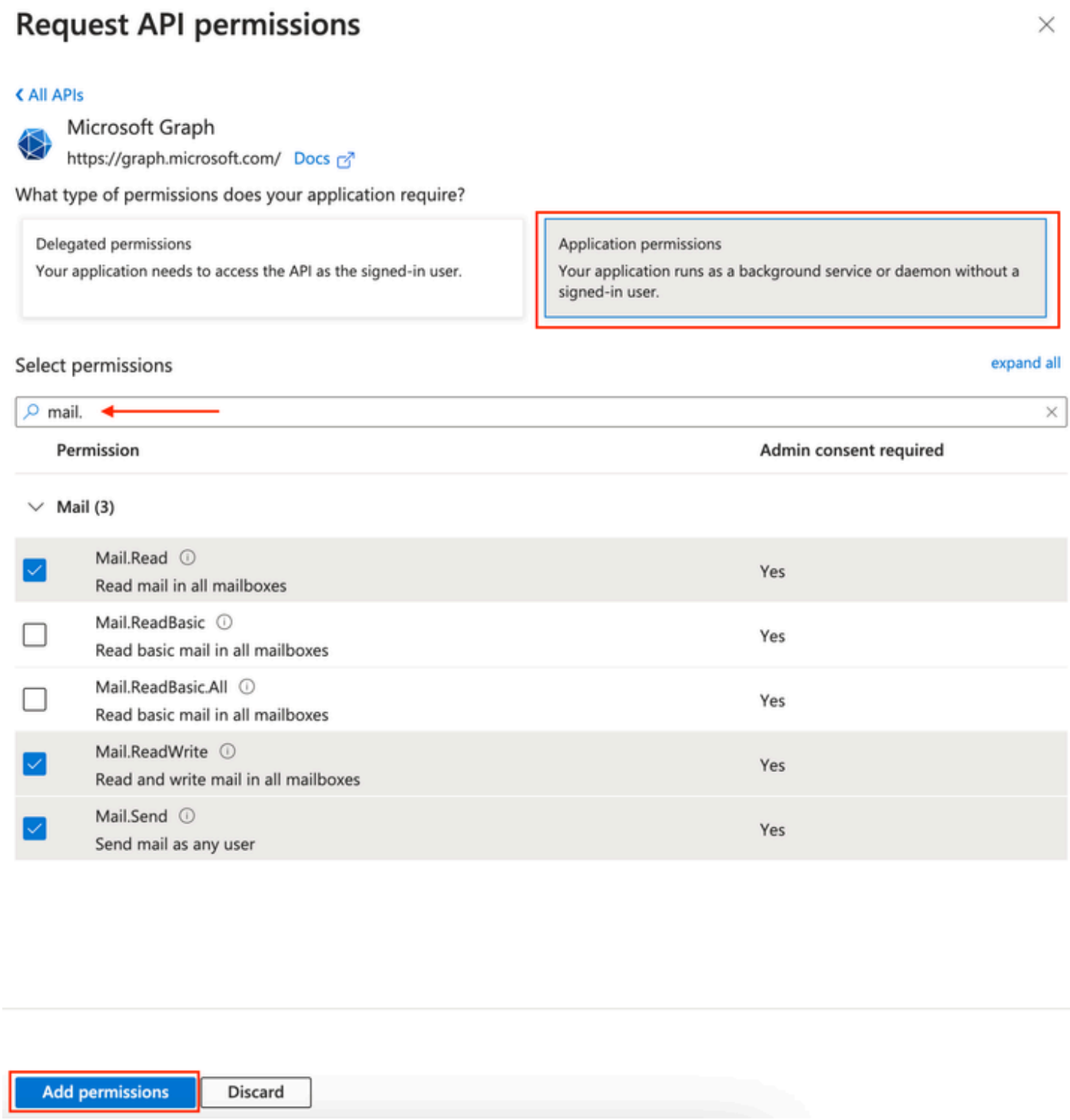
Visão geral do aplicativo Entra ID



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



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.

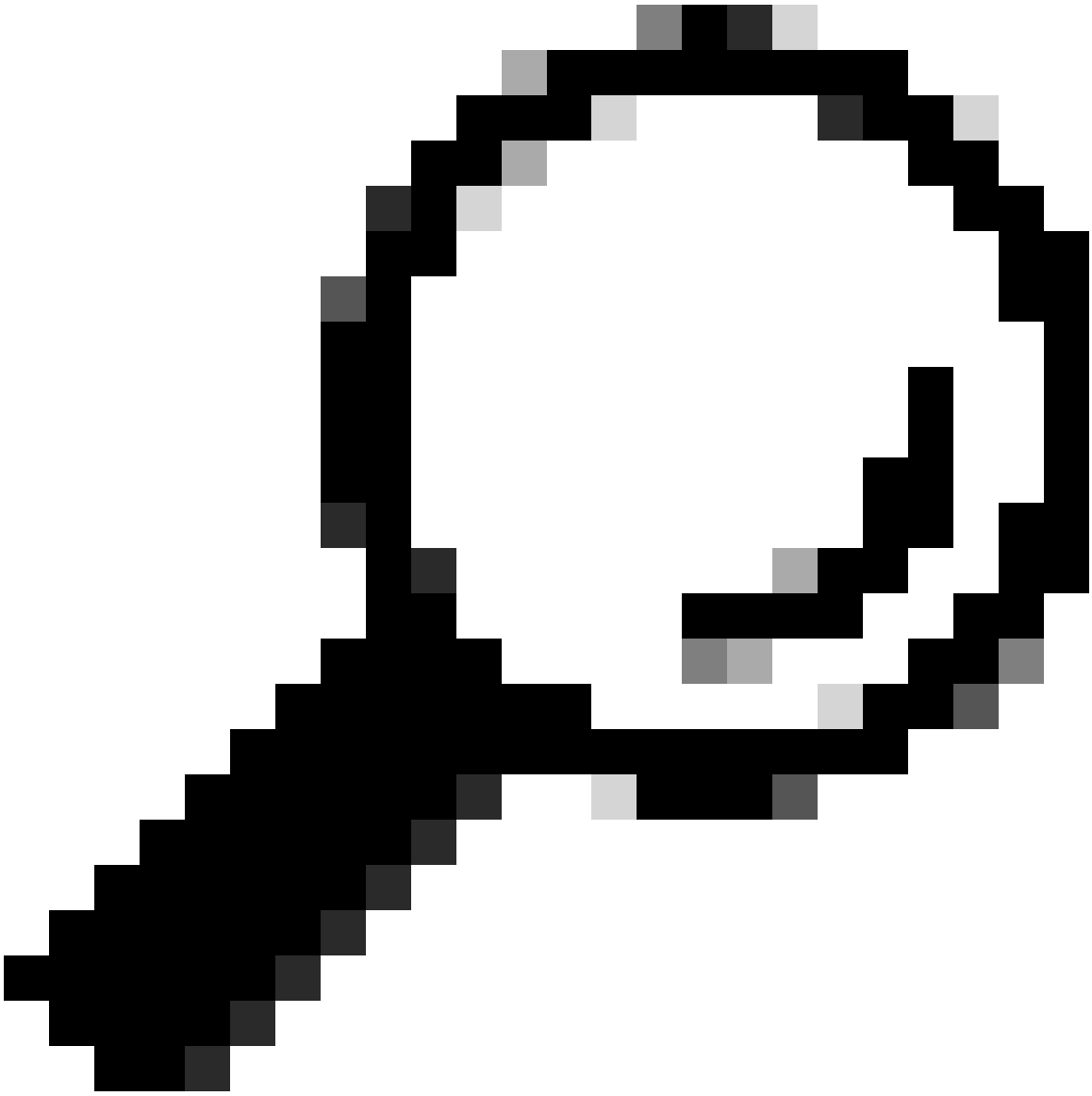
Permissões de API do Microsoft Graph

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

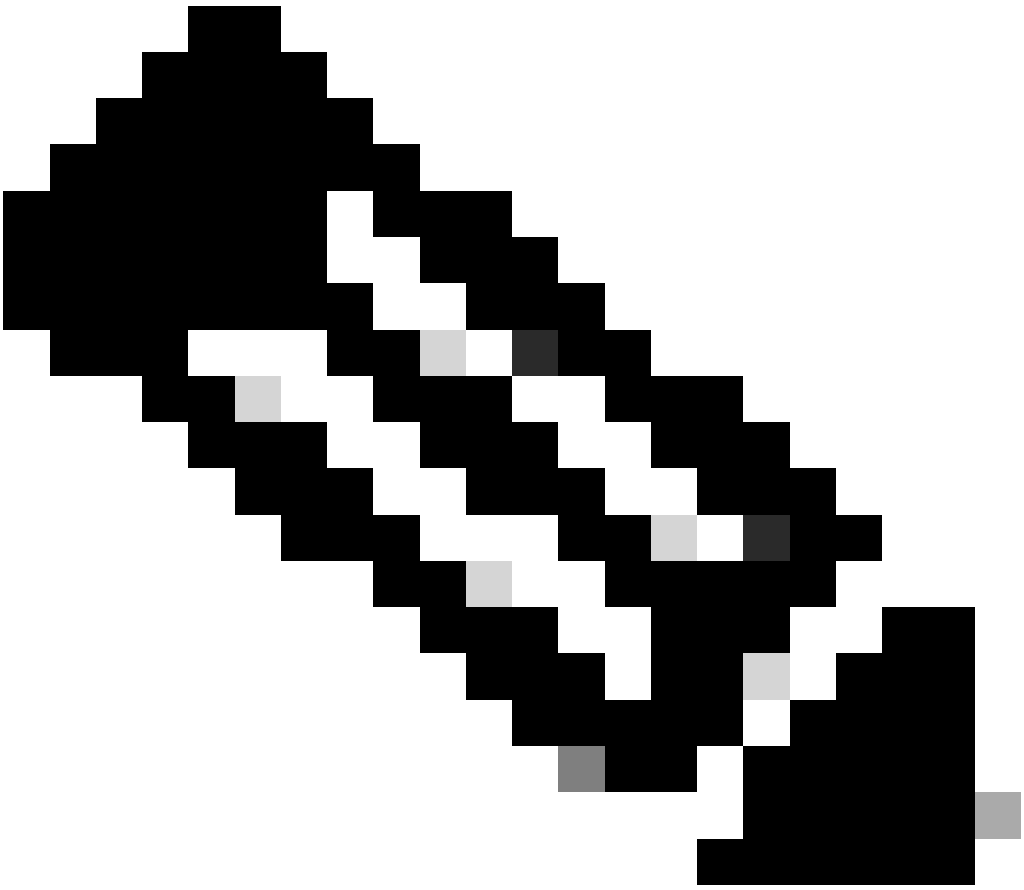
1. Faça login no portal de administração do Cisco Secure Email Encryption Service (CRES) como administrador de conta. (Serviço de criptografia de e-mail seguro)

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.

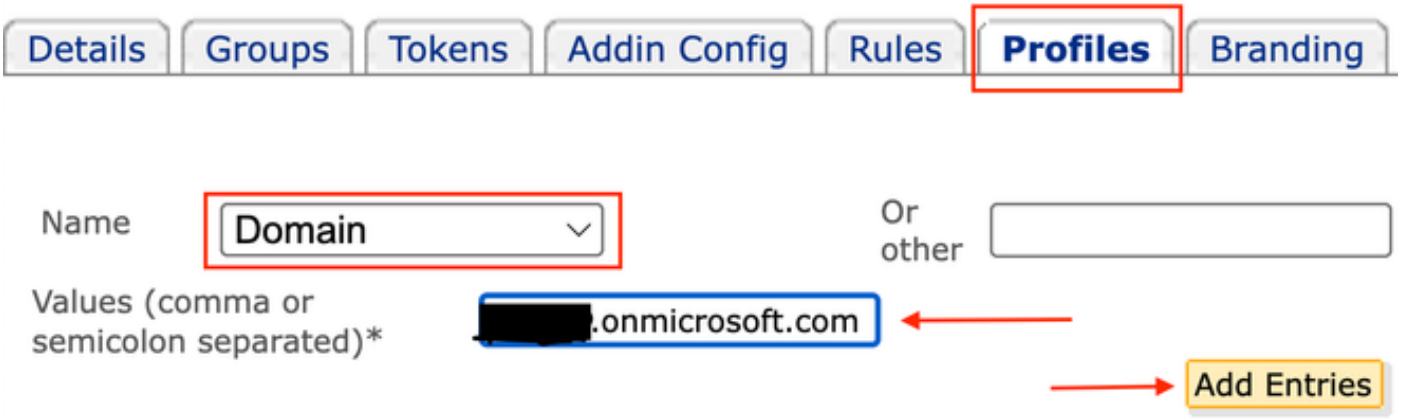
3. Navegue até Profiles, selecione o **tipo de Nome** como Domínio e insira seu **nome de domínio de e-mail** em Valores. Clique **Add Entries** e aguarde de 5 a 10 segundos. (Não atualize a página do navegador ou navegue para uma página diferente até que ela seja adicionada com êxito).



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.

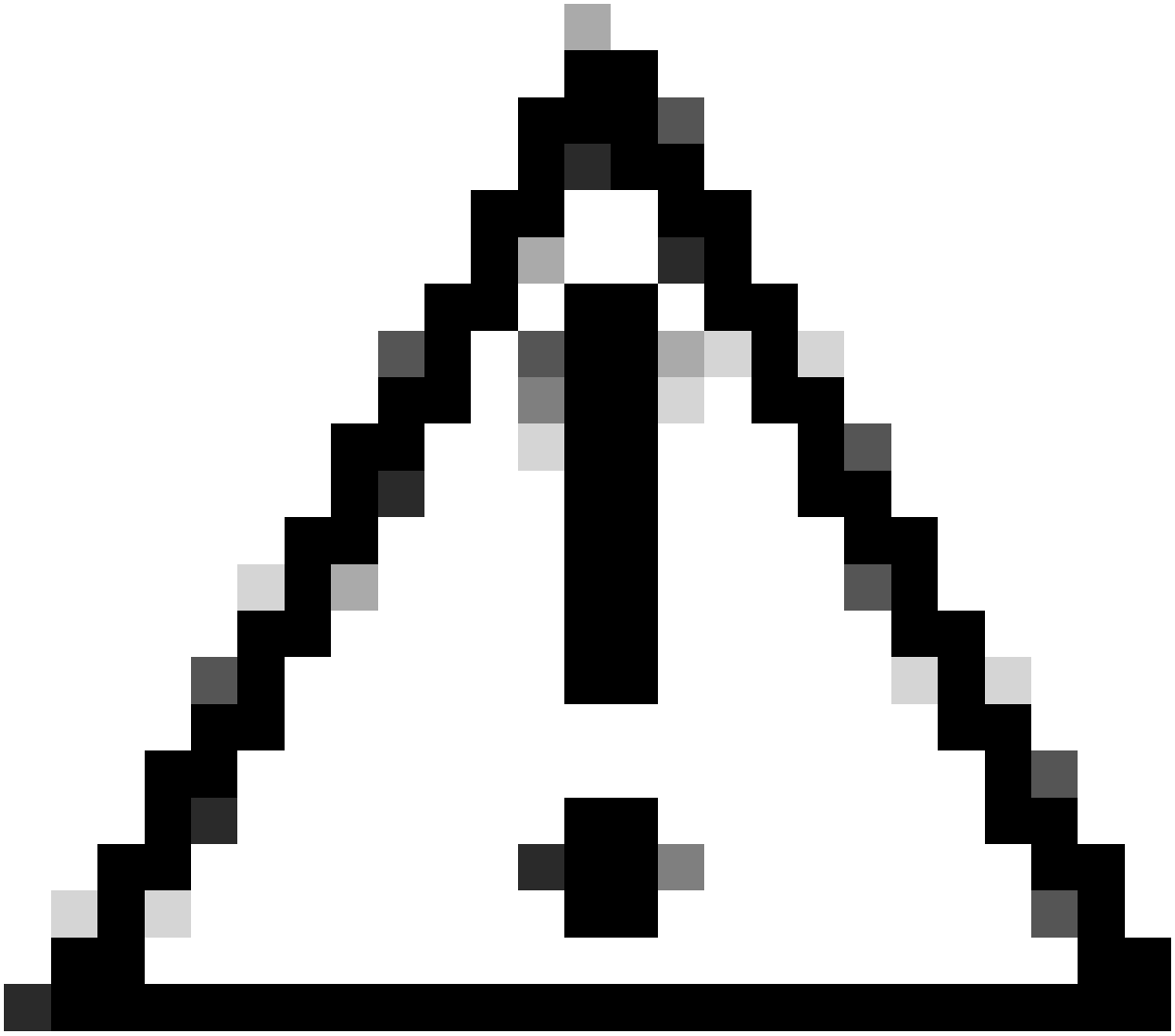


Perfis do portal de administração do CRES

4. Navegue até a Add-in Config guia.

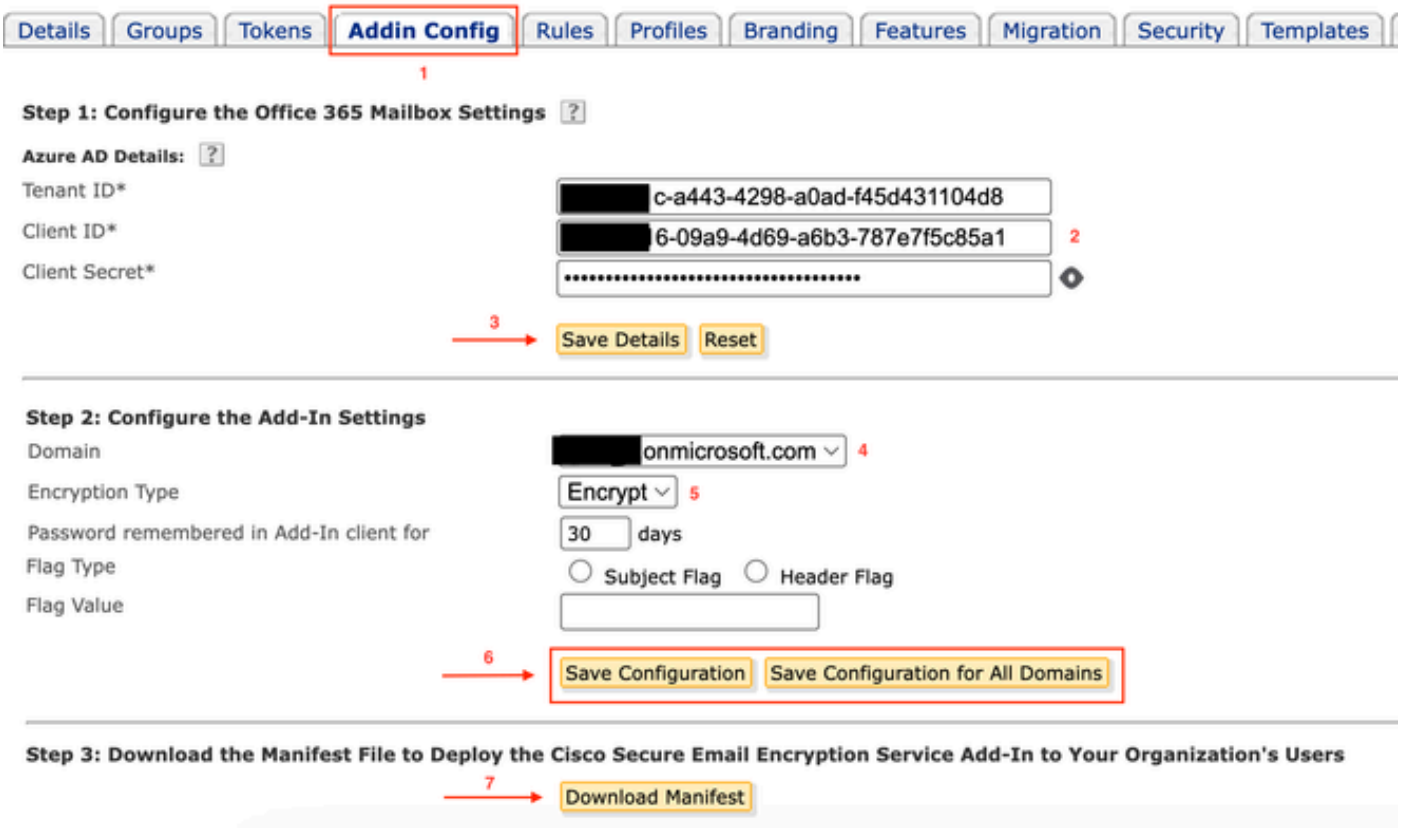
Etapa 1: Insira o Espaço, a ID do Cliente e o Segredo obtidos da ID da Entra em Detalhes do Azure AD. Clique em Save Details.

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.

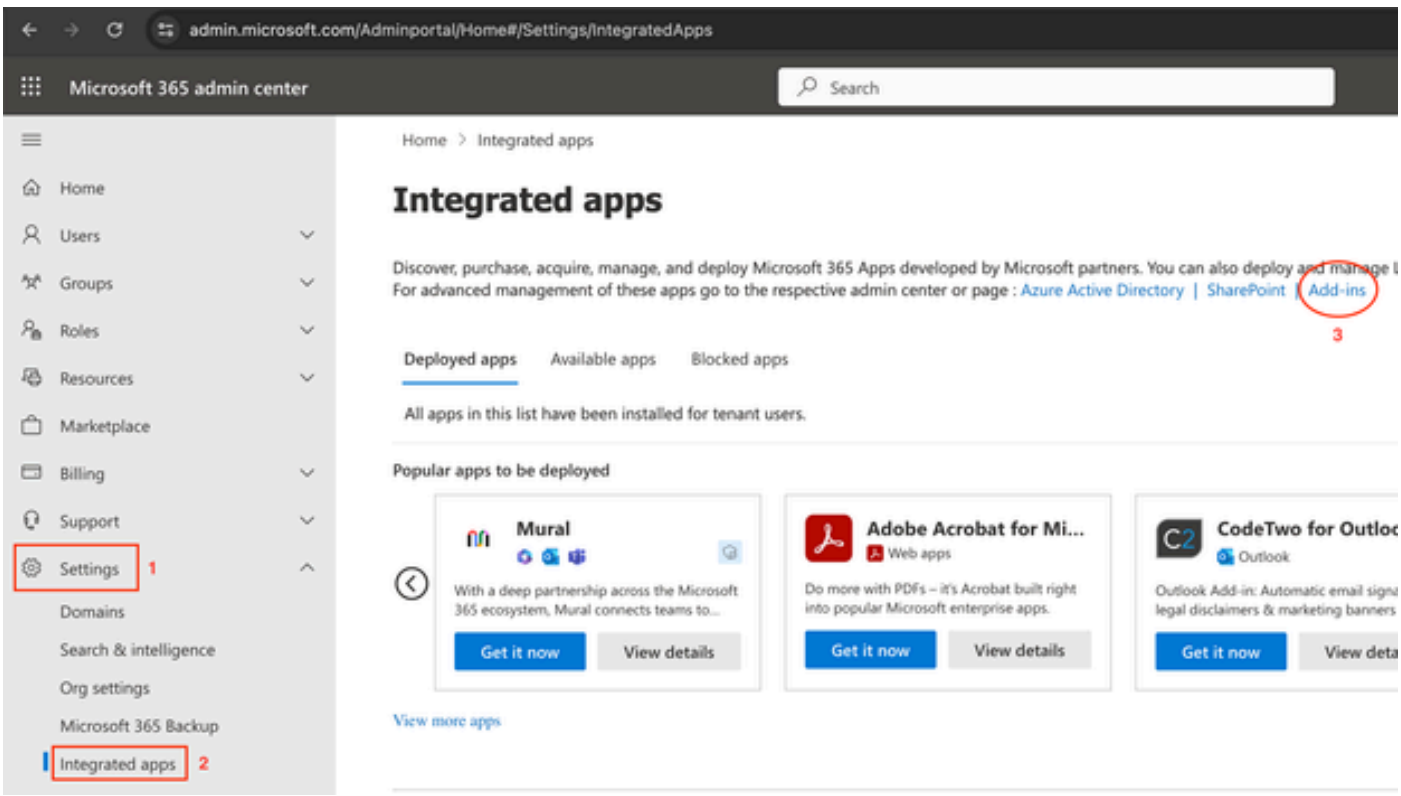


Configuração de suplemento do portal de administração do CRES

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

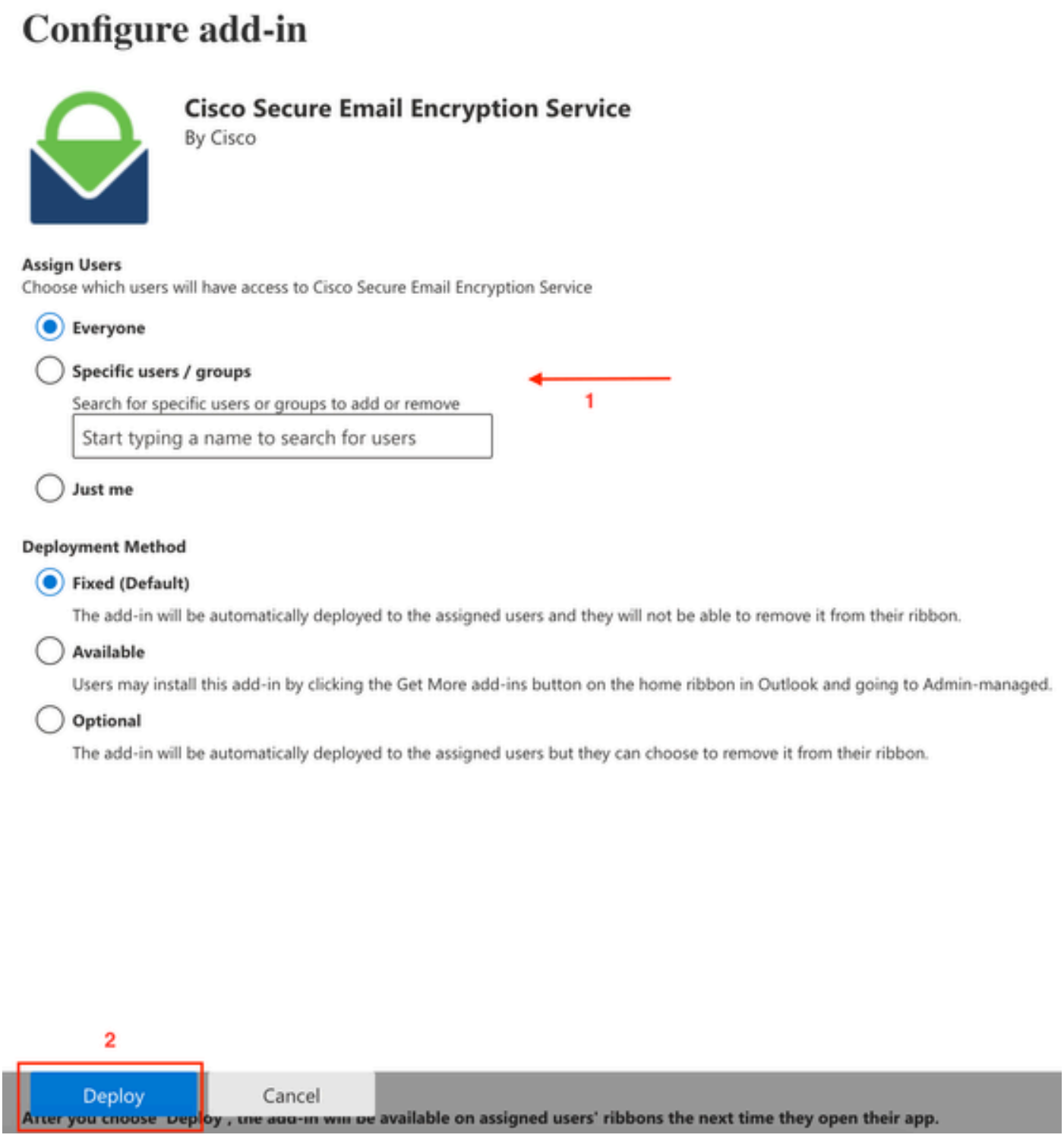
1. Efetue login no Microsoft 365 Admin Center como Administrador. (Centro de administração do Microsoft 365).

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



3. Clique Deploy Add-ine 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 Specifc Users/groupse clique em Deploy.



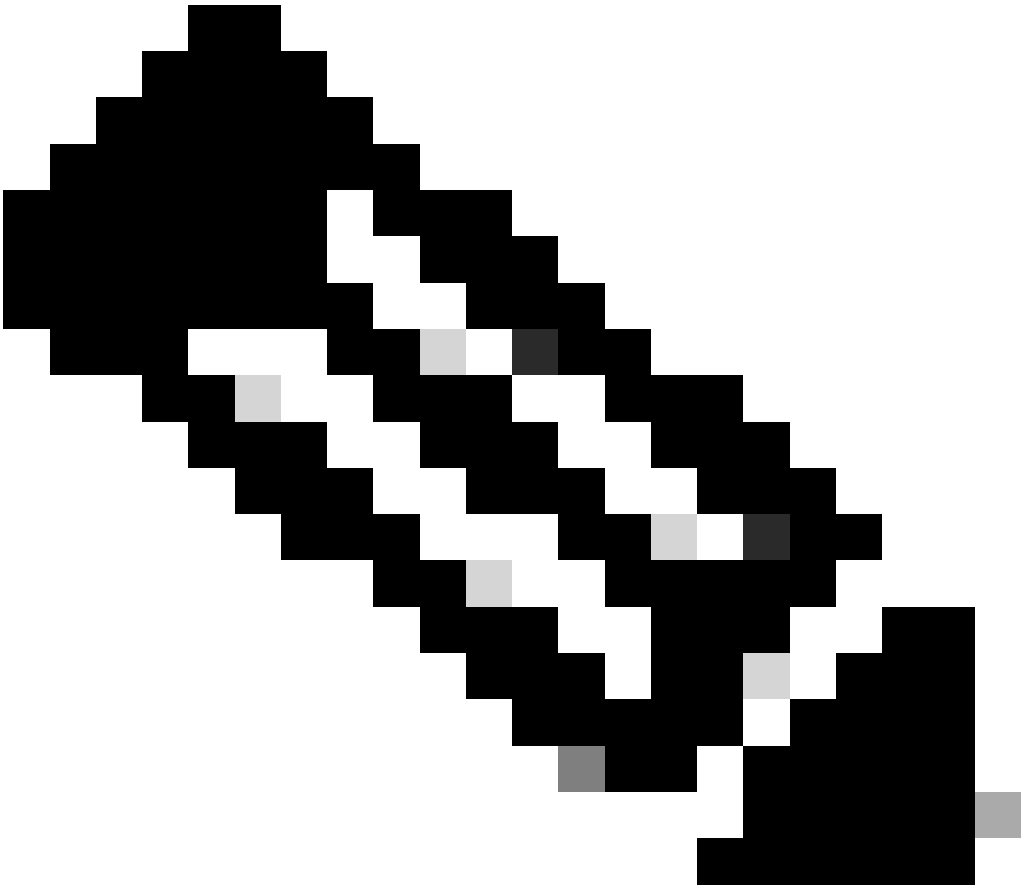
5. Depois que o Suplemento for implantado com êxito, ele poderá levar até 12 horas para ser exibido nas Faixas dos usuários finais (Cliente

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.



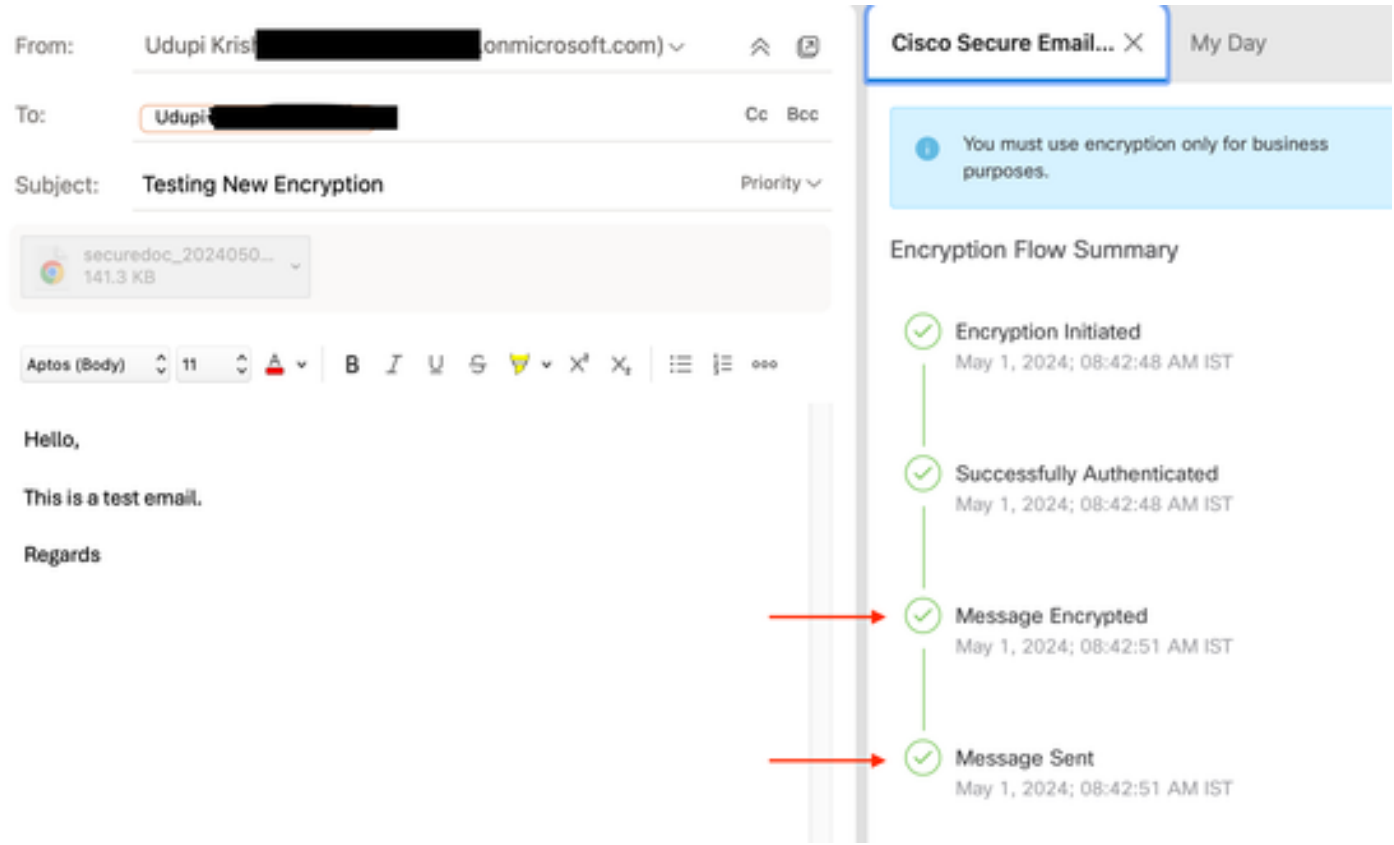
Observação: se o Tipo de criptografia (definido pelo administrador) for Criptografar, certifique-se de ter concluído sua mensagem e adicionado destinatários válidos antes de prosseguir para a próxima etapa. Após a Etapa 3, a mensagem é criptografada e enviada imediatamente.

---

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).



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.