

# Configurar a Caixa de Correio Compartilhada do Cloud Email Security com O365

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configuração](#)

[Etapa 1. Criar um Aplicativo no EntraID](#)

[Atribuir permissões](#)

[Criar Credenciais](#)

[Etapa 2. Configurar o Cisco Cloud Email Security](#)

[Testando](#)

[Informações adicionais](#)

---

## Introdução

Este documento descreve as configurações para exibir a Quarentena de spam do Cisco Secure Email Gateway em uma caixa de correio compartilhada no Exchange Online (O365).

## Pré-requisitos

### Requisitos

Para continuar com a configuração, certifique-se de atender a estes requisitos:

- Implementação da autenticação SAML para acesso à quarentena de SPAM.
- Informações sobre usuários e caixas de correio compartilhadas no Exchange Online.
- Atribuição de usuários às caixas de correio compartilhadas necessárias.
- Acesso ao portal EntraID para criar um aplicativo.
- Acesso ao console de relatórios CES para ativar o serviço Caixa de Correio Compartilhada.

Com todos os requisitos atendidos, você pode seguir as etapas de configuração abaixo.

### Componentes Utilizados

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

Configurações alternativas também estão disponíveis para gerenciar esses e-mails. Isso inclui habilitar notificações de SPAM para permitir liberação de email sem autenticação ou criar uma política personalizada para redirecionar emails sinalizados para a pasta Lixo Eletrônico da caixa de correio correspondente no Exchange Online.

## Configuração

### Etapa 1. Criar um Aplicativo no EntraID

Antes de configurar o Cisco Secure Email Gateway, estabeleça o acesso necessário no EntraID:

1. Acesse o EntraID.
2. Selecione Registros do aplicativo.
3. Clique em New Registration e, como nome, use "Cisco CES Shared Mailbox".
4. Escolha Contas somente neste diretório organizacional (emailsecdemo somente - Locatário único).
5. Em URL de redirecionamento, selecione Web e insira o link para sua área Quarentena de SPAM, formatada como [likehttps://XXXXX-YYYY.iphmx.com/](https://XXXXX-YYYY.iphmx.com/).
6. Clique em Registrar.

### Atribuir permissões

1. Abra o aplicativo recém-criado.
2. Vá para Permissões de API.
3. Atribua estas permissões do Microsoft Graph:
  - Mail.Read.Shared: Delegado, permite a leitura de e-mails do usuário e compartilhados
  - acesso\_offline: Delegado, permite a manutenção do acesso aos dados concedidos
  - openid: Delegado, permite que os usuários entrem
  - Usuário.Leitura: Delegado, permite entrar e ler o perfil do usuário
4. Por fim, clique em Conceder consentimento administrativo para emailsecdemo.

Microsoft Azure Search resources, services, and docs (G+)

Home > emailsecdemo | App registrations > Cisco CES Shared mailbox

## Cisco CES Shared mailbox | API permissions

Search Refresh Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
  - Branding & properties
  - Authentication
  - Certificates & secrets
  - Token configuration
  - API permissions**
  - Expose an API
  - App roles
  - Owners
  - Roles and administrators
  - Manifest
- Support + Troubleshooting

### Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for emailsecdemo

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				
Mail.Read.Shared	Delegated	Read user and shared mail	No	Granted for emailsecde... ***
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for emailsecde... ***
openid	Delegated	Sign users in	No	Granted for emailsecde... ***
User.Read	Delegated	Sign in and read user profile	No	Granted for emailsecde... ***

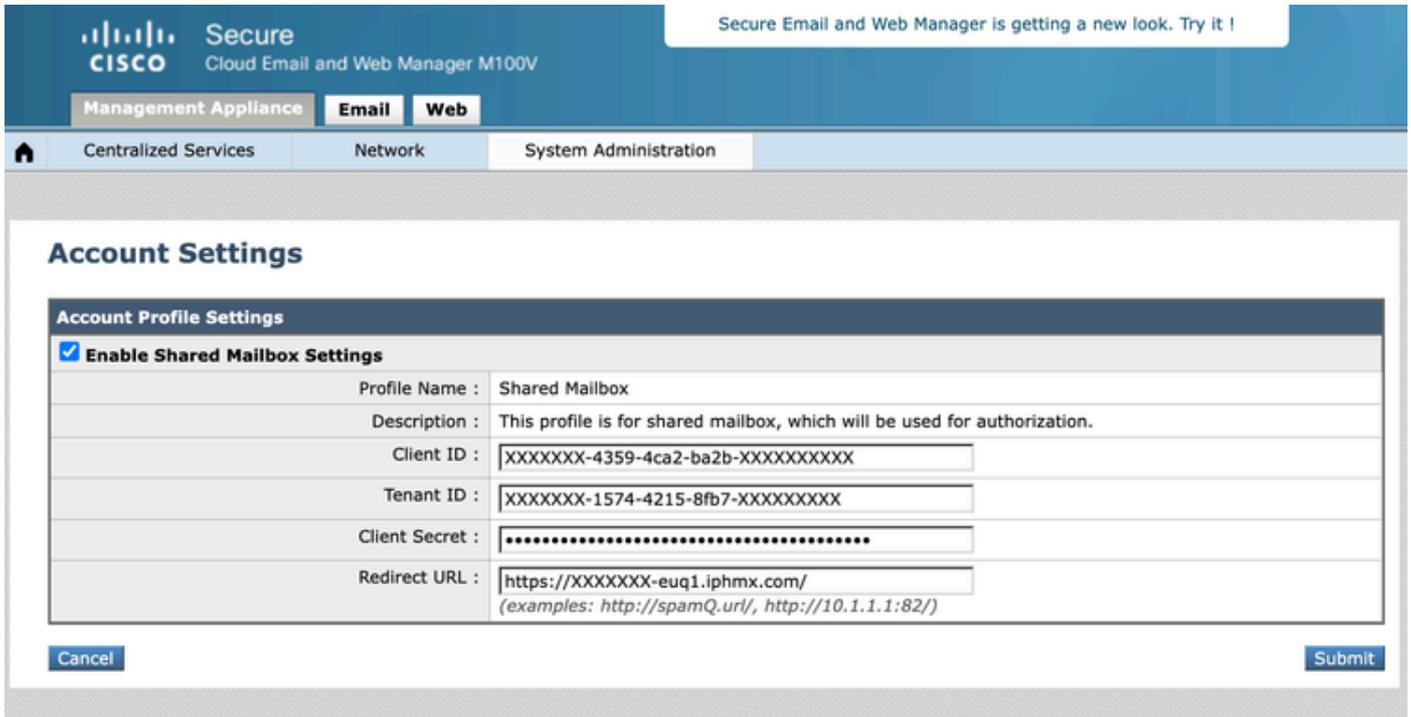
To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

## Criar Credenciais

1. Na tela Visão geral do aplicativo, vá para Credenciais do cliente.
2. Crie um "Segredo de Cliente" e salve seu valor em um local seguro, pois ele desaparecerá após a gravação.

## Etapa 2. Configurar o Cisco Cloud Email Security

1. Abra o console de relatórios e acesse System Administration -> Account Settings.
2. Ative e configure o serviço Caixa de Correio Compartilhada.
3. Clique em Edit Settings, ative o serviço e adicione os campos necessários. Use as informações do aplicativo criado no EntraID e o Segredo do Cliente.
4. Configure a URL de Redirecionamento de forma consistente com a configuração do EntraID.
5. Clique em Enviar e teste com um usuário que tenha acesso a uma caixa de correio compartilhada.



## Testando

Execute um teste com um usuário que tenha acesso a uma caixa de correio compartilhada.

Na quarentena de SPAM, há uma nova opção View Messages for mailbox, onde você pode adicionar todas as caixas de correio compartilhadas às quais tem acesso.

1. Abra a Quarentena de spam e faça login com um usuário normal usando SAML.
2. Clique em View Messages for Mailbox.
3. Escreva o endereço de email da caixa de correio compartilhada que o usuário tem acesso e clique em Adicionar Caixa de Correio.
4. Clique em View Messages for Mailbox e selecione a Shared Mailbox para revisar.

## Informações adicionais

Na GUI de registro de quarentena de spam, você pode verificar quando um usuário libera um e-mail. Se estiver autenticado, você poderá identificar quem o liberou. Para caixas de correio compartilhadas, analise a ID de rastreamento de log e verifique qual usuário tem a mesma ID:

```
Wed Jan 15 20:00:43 2025 Info: req:68.232.128.211 user:user1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW 200
Wed Jan 15 20:00:56 2025 Info: req:68.69.70.212 user:user1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW releas
Wed Jan 15 20:00:56 2025 Info: req:68.69.70.212 user:user1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW 303 PO
Wed Jan 15 20:00:56 2025 Info: req:68.69.70.212 user:user1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW 200 GE
Wed Jan 15 20:00:56 2025 Info: req:68.69.70.212 user:user1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW 200 GE
Wed Jan 15 20:01:15 2025 Info: login:68.69.70.212 user:shared1@domainabc.com session:5RwUAJcoaVYxN6nZ3xcW
Wed Jan 15 20:01:15 2025 Info: req:68.69.70.212 user:user1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW 200 PO
Wed Jan 15 20:01:15 2025 Info: req:68.69.70.212 user:shared1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW 200
```

O registro mostra que user1@domainabc.com e shared1@domainabc.com estão usando o mesmo identificador de sessão 5RwUAJcoaVYxN6nZ3xcW. Isso significa que ambos os usuários estão compartilhando ou usando a mesma sessão no sistema. Isso indica que shared1 está atuando na sessão iniciada originalmente pelo user1.

## 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.