Configure Cloud Email Security Shared Mailbox with O365

Contents

Introduction

This document describes the configurations to view the Cisco Secure Email Gateway Spam Quarantine to a shared mailbox in Exchange Online (O365).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Implementation of Security Assertion Markup Language (SAML) authentication for access to the SPAM quarantine
- Information on users and shared mailboxes in Exchange Online
- Assignment of users to the necessary shared mailboxes
- Access to the EntraID portal to create an application
- Access to the Cisco Cloud Email Security (CES) reporting console to activate the Shared Mailbox service

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Alternative configurations are also available to manage such emails. These include enabling SPAM notifications in order to allow email release without authentication or creating a custom policy to redirect flagged emails to the **Junk** folder of the corresponding mailbox in Exchange Online.

Configuration

With all requirements met, you can follow these configuration steps:

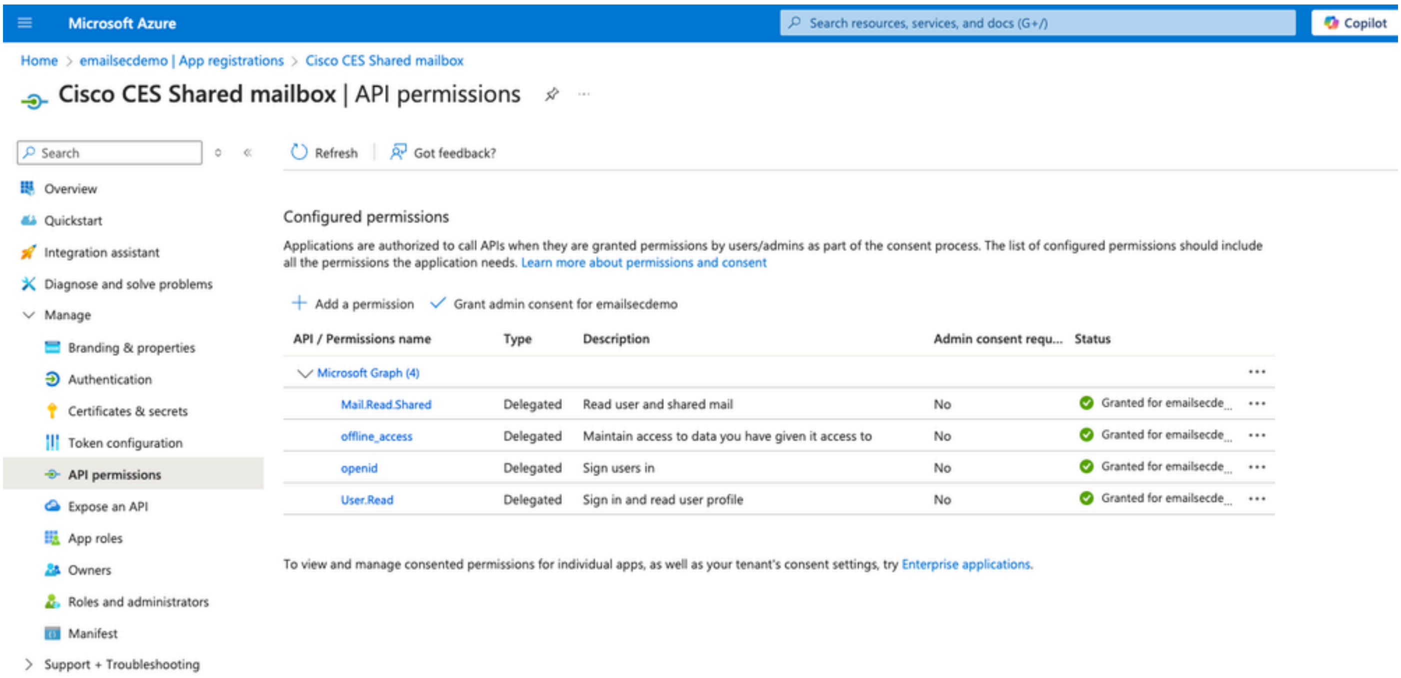
Step 1. Create an Application in EntraID

Before configuring Cisco Secure Email Gateway, establish the necessary access in EntraID:

1. Access EntraID.
2. Choose **App Registrations**.
3. Click **New Registration** and use 'Cisco CES Shared Mailbox' as the name.
4. Choose **Accounts** in this organizational directory only (**emailsecdemo** only - **Single tenant**).
5. In **Redirect URL**, choose web and enter the link to your SPAM Quarantine area, formatted likehttps://XXXXX-YYYY.iphmx.com/.
6. Click **Register**.

Assign Permissions

1. Open the newly created application.
2. Navigate to **API Permissions**.
3. Assign these Microsoft Graph permissions:
   Mail.Read.Shared: Delegated, allows reading user and shared mail
   offline_access: Delegated, allows maintaining access to granted data
   openid: Delegated, allows users to sign in
   User.Read: Delegated, allows signing in and reading user profile
4. Finally, click **Grant admin Consent for emailsecdemo**.



Cisco CES Shared mailbox | API permissions

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

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...

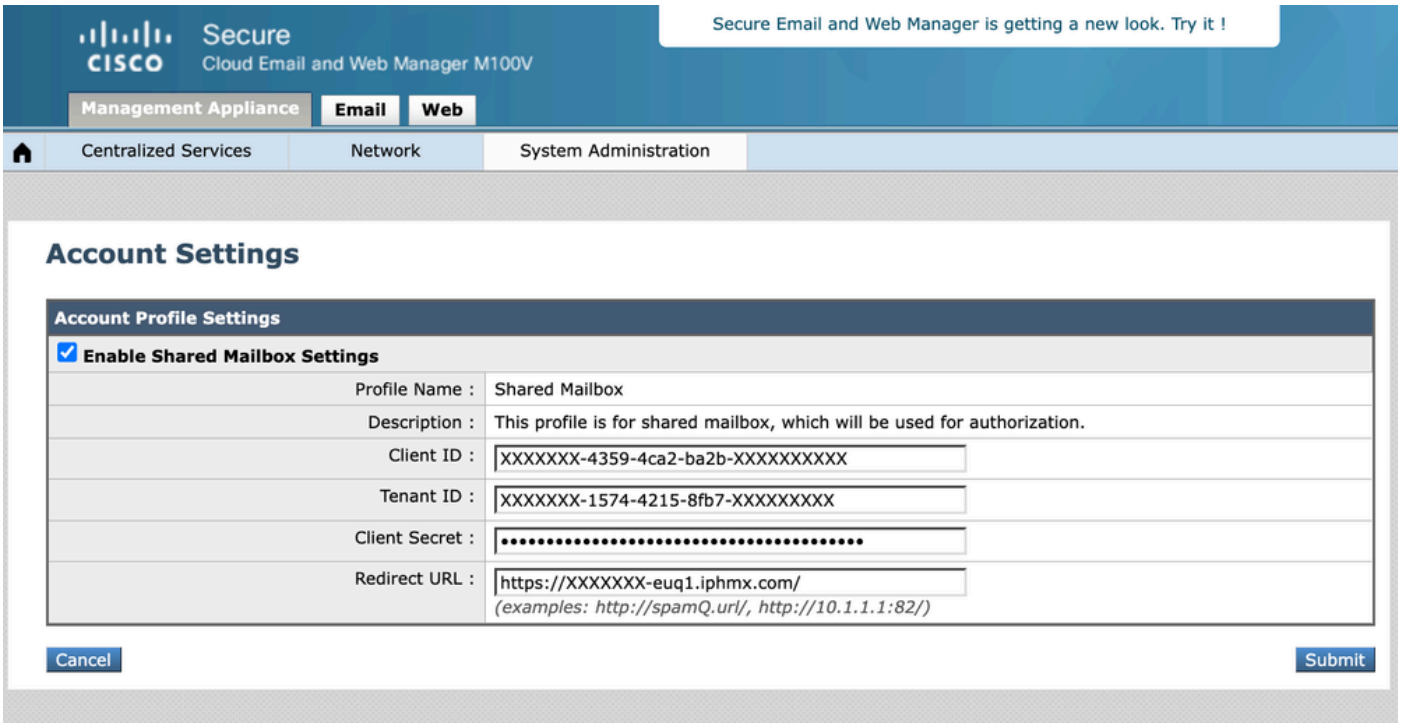
To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

Create Credentials

1. In the application **Overview** screen, navigate to **Client Credentials**.
2. Create a 'Client Secret' and save its value in a secure place, as it disappears after saving.

Step 2. Configure Cisco Cloud Email Security

1. Open the reporting console and access **System Administration** > **Account Settings**.
2. Activate and configure the Shared Mailbox service.
3. Click **Edit Settings**, enable the service, and add the required fields. Use the information from the application created in EntraID and the Client Secret.
4. Configure the **Redirect URL** consistently with the EntraID configuration.
5. Click **Submit** and test with a user who has access to a shared mailbox.



Account Settings

Account Profile Settings

☑ Enable Shared Mailbox Settings

Profile Name :	Shared Mailbox
Description :	This profile is for shared mailbox, which will be used for authorization.
Client ID :	XXXXXXX-4359-4ca2-ba2b-XXXXXXXXXX
Tenant ID :	XXXXXXX-1574-4215-8fb7-XXXXXXXXX
Client Secret :	••
Redirect URL :	https://XXXXXXX-euq1.iphmx.com/ *(examples: http://spamQ.url/, http://10.1.1.1:82/)*

Testing

Perform a test with a user who has access to a shared mailbox.

In the SPAM quarantine, there is a new option **View Messages for mailbox**, where you can add all shared mailboxes you have access to.

1. Open the SPAM Quarantine and log in with a normal user using SAML.
2. Click **View Messages for Mailbox**.
3. Write the shared mailbox email address that the user has access to and click **Add Mailbox**.
4. Click **View Messages for Mailbox** and choose the **Shared Mailbox** to review.

Additional Information

In the **Spam Quarantine GUI Log**, you can verify when a user releases an email. If authenticated, you can identify who released it. For shared mailboxes, analyze the log trace ID and verify which user has the same 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.comsession:5RwUAJcoaVYxN6nZ3xc
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
```

The log shows that both **user1@domainabc.com** and **shared1@domainabc.com** are using the same session identifier 5RwUAJcoaVYxN6nZ3xcW. This means that both users are sharing or using the same session in the system. This indicates that shared1 is acting under the session originally initiated by user1.