Configuración del buzón compartido de Cloud Email Security con O365

Contenido

Introducción

Este documento describe las configuraciones para ver la cuarentena de spam de Cisco Secure Email Gateway en un buzón compartido en Exchange Online (O365).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Implementación de la autenticación de Lenguaje de marcado de aserción de seguridad (SAML) para el acceso a la cuarentena de SPAM
- Información sobre usuarios y buzones compartidos en Exchange Online
- Asignación de usuarios a los buzones compartidos necesarios
- Acceso al portal EntraID para crear una aplicación
- Acceso a la consola de informes de Cisco Cloud Email Security (CES) para activar el servicio de buzón compartido

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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

También hay configuraciones alternativas disponibles para administrar dichos correos electrónicos. Entre ellas, se incluyen habilitar las notificaciones de SPAM para permitir la liberación de correo electrónico sin autenticación o crear una política personalizada para redirigir los correos electrónicos marcados a la carpeta Junk del buzón correspondiente en Exchange Online.

Configuración

Una vez cumplidos todos los requisitos, puede seguir estos pasos de configuración:

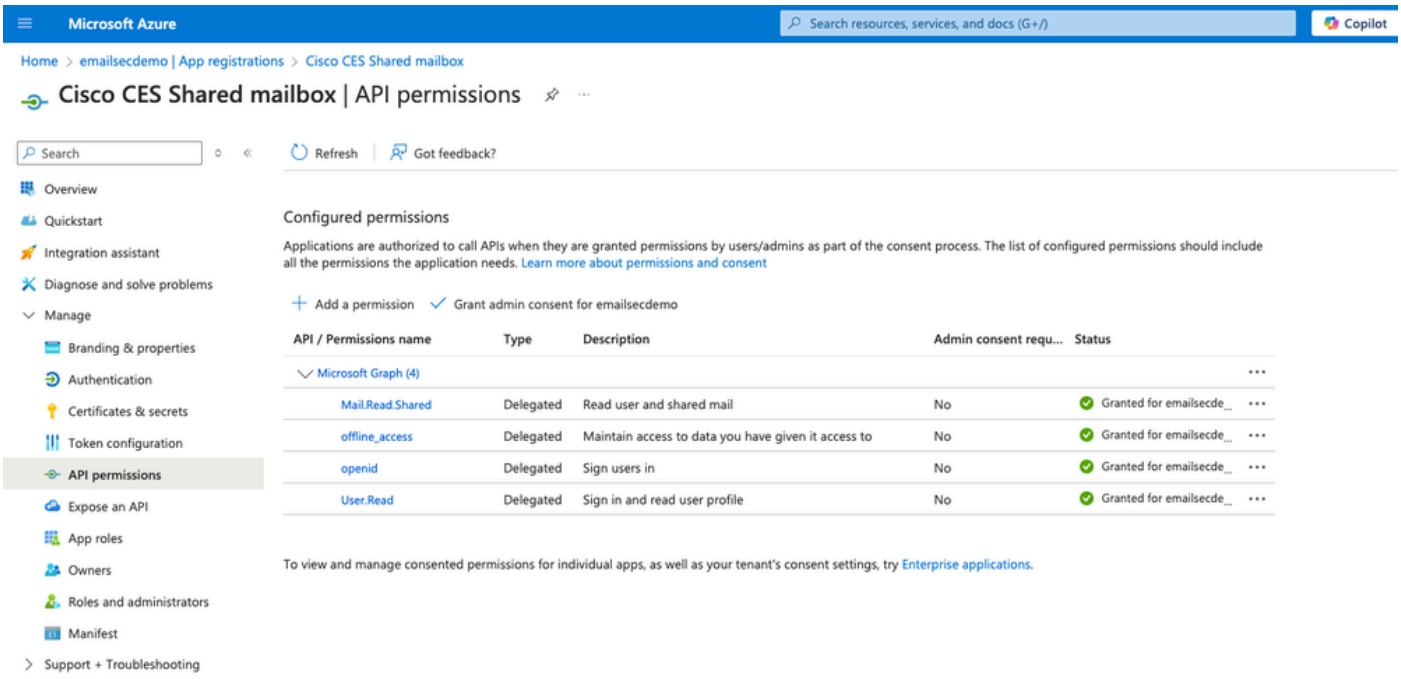
Paso 1. Crear una aplicación en EntraID

Antes de configurar Cisco Secure Email Gateway, establezca el acceso necesario en EntraID:

1. Acceda a EntraID.
2. Elija App Registations.
3. Haga clic en New Registration y utilice 'Cisco CES Shared Mailbox' como nombre.
4. Elija Accounts en este directorio organizativo solamente (emailsecdemo solamente - Single tenant).
5. En Redirigir URL, elija web e ingrese el link a su área de Cuarentena de SPAM, con formato likehttps://XXXXX-YYYY.iphmx.com/.
6. Haga clic en Register.

Asignar permisos

1. Abra la aplicación recién creada.
2. Navegue hasta Permisos API.
3. Asigne estos permisos de Microsoft Graph:
   Mail.Read.Shared: Delegado, permite leer correo compartido y de usuario
   offline_access: Delegado, permite mantener el acceso a los datos concedidos
   openid: Delegado, permite a los usuarios iniciar sesión
   Usuario.Lectura: Delegado, permite iniciar sesión y leer el perfil de usuario
4. Por último, haga clic en Conceder consentimiento del administrador para la demo por correo electrónico.

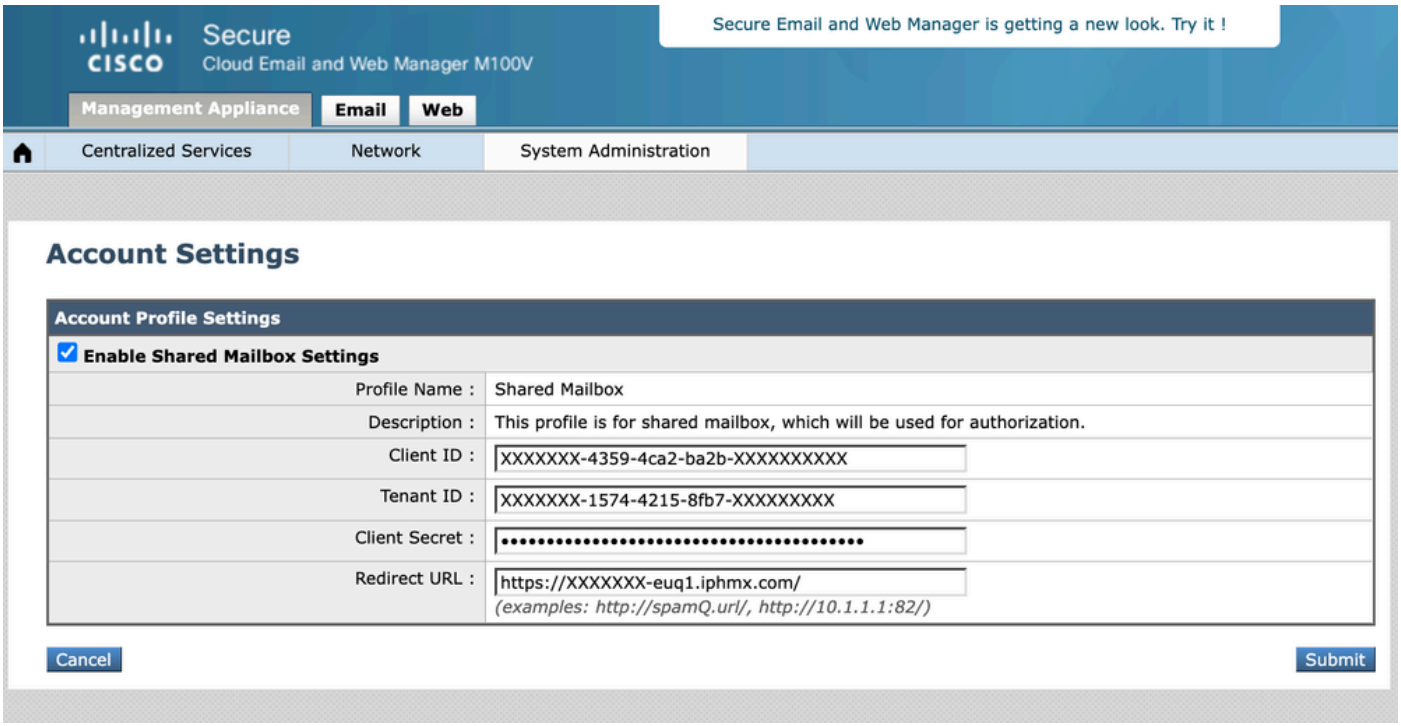


Crear credenciales

1. En la pantalla Application Overview, navegue hasta Client Credentials.
2. Cree un 'Secreto de cliente' y guarde su valor en un lugar seguro, ya que desaparece después de guardar.

Paso 2. Configuración de Cisco Cloud Email Security

1. Abra la consola de informes y acceda a Administración del sistema > Configuración de la cuenta.
2. Active y configure el servicio de buzón compartido.
3. Haga clic en Edit Settings, habilite el servicio y agregue los campos requeridos. Utilice la información de la aplicación creada en EntraID y Client Secret.
4. Configure la URL de redireccionamiento de manera consistente con la configuración de EntraID.
5. Haga clic en Enviar y pruebe con un usuario que tenga acceso a un buzón compartido.



Prueba

Realice una prueba con un usuario que tenga acceso a un buzón compartido.

En la cuarentena de SPAM, hay una nueva opción Ver mensajes para el buzón, donde puede agregar todos los buzones compartidos a los que tiene acceso.

1. Abra la cuarentena de SPAM e inicie sesión con un usuario normal utilizando SAML.
2. Haga clic en Ver mensajes para el buzón.
3. Escriba la dirección de correo electrónico del buzón compartido al que tiene acceso el usuario y haga clic en Agregar buzón.
4. Haga clic en Ver mensajes para el buzón y elija el Buzón compartido para revisar.

Additional Information

En el Registro de la GUI de Spam Quarantine, puede verificar cuando un usuario publica un correo electrónico. Si está autenticado, puede identificar quién lo liberó. Para los buzones compartidos, analice el ID de seguimiento de registro y verifique qué usuario tiene el mismo 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
```

El registro muestra que tanto user1@domainabc.com como shared1@domainabc.com están utilizando el mismo identificador de sesión 5RwUAJcoaVYxN6nZ3xcW. Esto significa que ambos usuarios comparten o usan la misma sesión en el sistema. Esto indica que shared1 actúa bajo la sesión iniciada originalmente por user1.

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).