Cloud-e-mail security gedeelde postvak met OSC365 configureren

Inhoud

Inleiding

Dit document beschrijft de configuraties om de Cisco Secure Email Gateway Spam Quarantine te bekijken in een gedeelde postvak in Exchange Online (O365).

Voorwaarden

Vereisten

Om verder te gaan met de configuratie, zorg ervoor dat u aan deze vereisten voldoet:

- Implementatie van SAML-verificatie voor toegang tot de SPAM-quarantaine.
- Informatie over gebruikers en gedeelde mailboxen in Exchange Online.
- Toewijzing van gebruikers aan de noodzakelijke gedeelde postvakken.
- Toegang tot het EntraID portal om een applicatie te maken.
- Toegang tot de CES-rapportageconsole om de gedeelde mailboxservice te activeren.

Als aan alle vereisten is voldaan, kunt u de onderstaande configuratiestappen volgen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Er zijn ook alternatieve configuraties beschikbaar voor het beheer van dergelijke e-mails. Deze omvatten het toelaten van SPAM berichten om e-mailversie zonder authentificatie toe te staan of het creëren van een douanebeleid om gemarkeerde e-mails aan de map van de Junk van de overeenkomstige brievenbus in Exchange Online om te leiden.

Configuratie

Stap 1. Maak een toepassing in EntraID

Alvorens Cisco Secure Email Gateway te configureren, moet u de benodigde toegang in EntraID instellen:

1. Toegang tot EntraID.
2. Selecteer App-registraties.
3. Klik op Nieuwe registratie en gebruik als naam, "Cisco CES gedeelde postvak".
4. Kies Accounts alleen in deze organisatiegids (e-mailsecdemo alleen - Eén huurder).
5. In Redirect URL, selecteer web en voer de link naar uw SPAM Quarantaine gebied, opgemaakt likehttps://XXXXX-YYYY.iphmx.com/.
6. Klik op Registreren.

Toewijzen van toegangsrechten

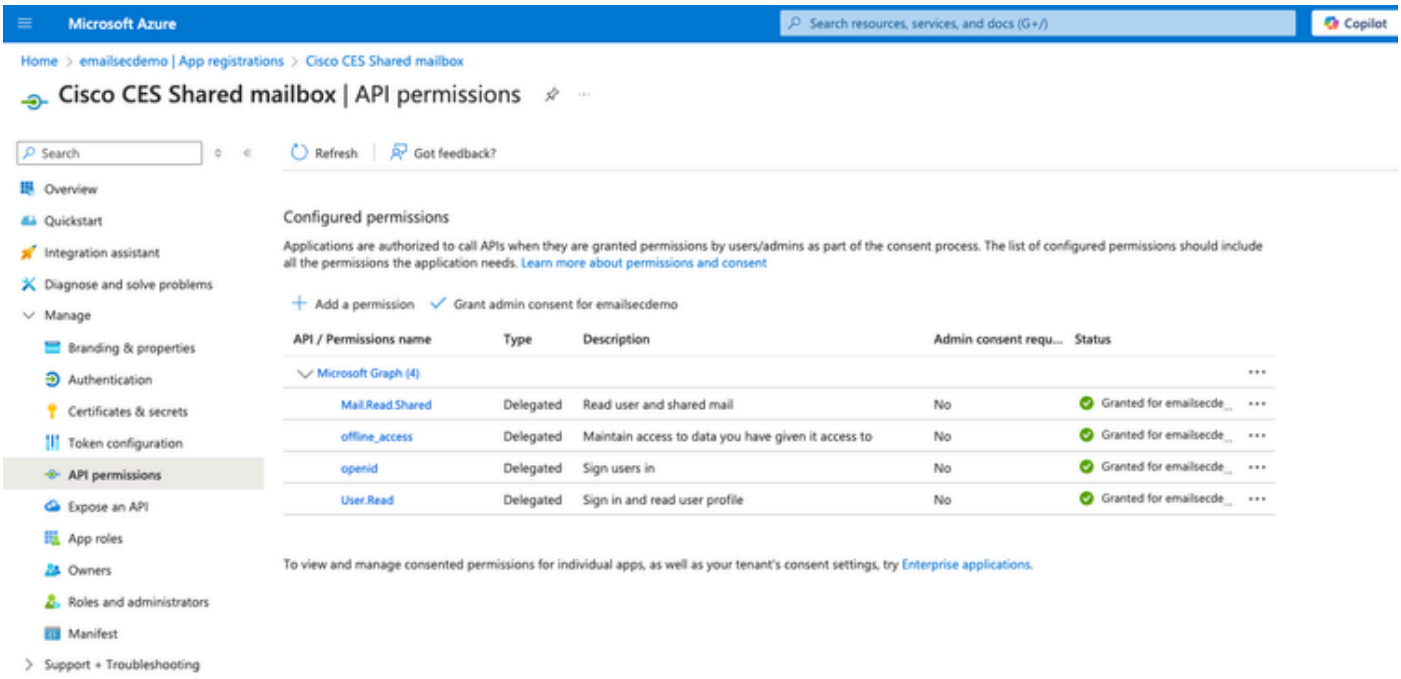
1. Open de nieuwe toepassing.

2. Ga naar API-toegangsrechten.

3. Wijs deze Microsoft Graph-rechten toe:

    - Mail.Read.Shared: Gedelegeerd, laat leesgebruiker en gedeelde post toe
    - offline_toegang: Gedelegeerd, staat het handhaven van toegang tot verleende gegevens toe
    - Openbaar: Gedelegeerd, laat gebruikers toe om in te loggen
    - Gebruiker.Lezen: Gedelegeerd, kunt u inloggen en gebruikersprofiel lezen

4. Klik tot slot op Toestemming verlenen voor e-maildemo.

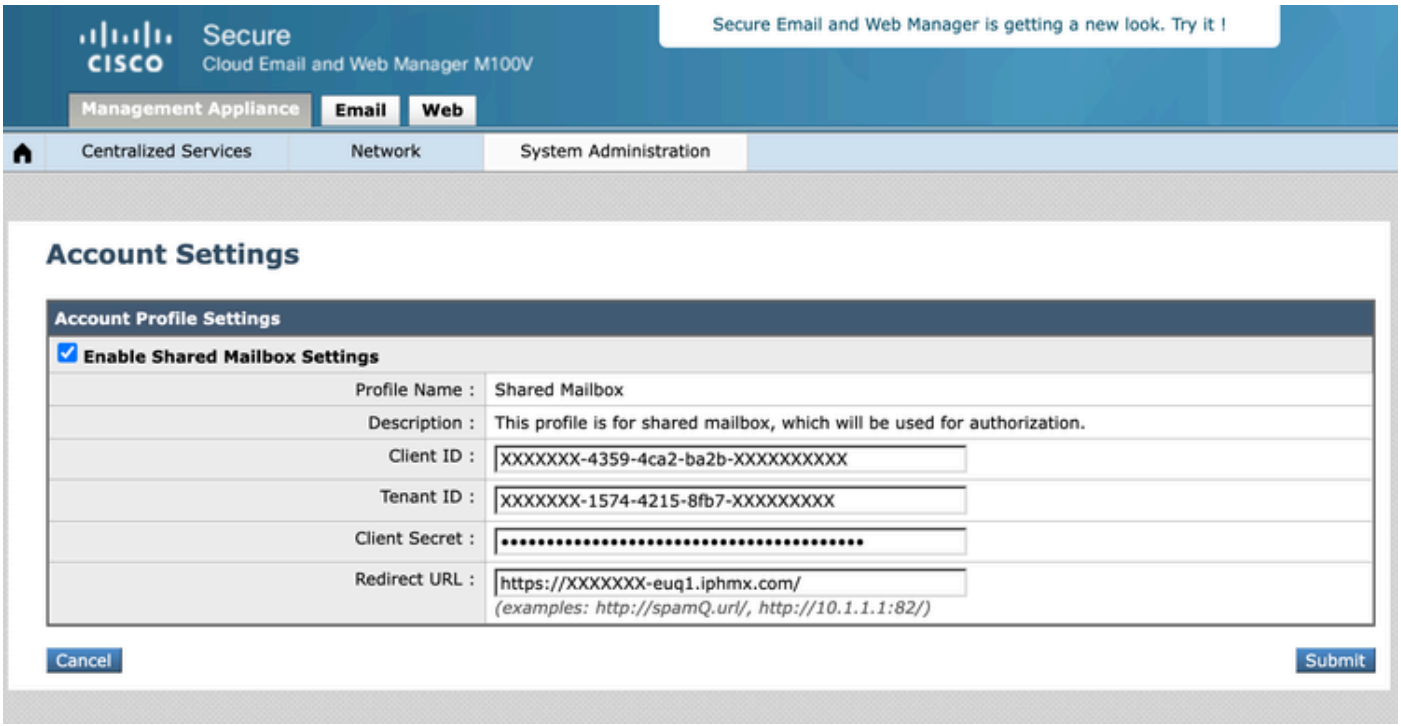


Credentials aanmaken

1. Ga in het scherm Overzicht van toepassingen naar Clientreferenties.
2. Maak een "Clientgeheim" en bewaar de waarde op een veilige plaats, omdat deze verdwijnt na het opslaan.

Stap 2. Cisco Cloud e-mail security configureren

1. Open de rapportageconsole en open systeembeheer -> Accountinstellingen.
2. Activeer en configureer de gedeelde mailboxservice.
3. Klik op Instellingen bewerken, schakel de service in en voeg de gewenste velden toe. Gebruik de informatie van de toepassing die in EntraID en het Clientgeheim wordt gemaakt.
4. Configureer de Redirect URL consistent met de EntraID-configuratie.
5. Klik op Indienen en test met een gebruiker die toegang heeft tot een gedeeld postvak.



Testen

Voer een test uit met een gebruiker die toegang heeft tot een gedeelde mailbox.

In de SPAM quarantaine, is er een nieuwe optie Beeld Berichten voor brievenbus, waar u alle gedeelde brievenbussen kunt toevoegen u toegang tot hebt.

1. Open de spamquarantaine en log in bij een normale gebruiker met behulp van SAML.
2. Klik op Berichten bekijken voor postvak.
3. Schrijf het gedeelde e-mailadres van het postvak dat de gebruiker heeft en klik op Mailbox toevoegen.
4. Klik op Berichten bekijken voor postvak en selecteer de gedeelde postvak om te bekijken.

Aanvullende informatie

In het GUI Log van Spam Quarantine, kunt u controleren wanneer een gebruiker een e-mail vrijgeeft. Indien geverifieerd, kunt u identificeren wie het vrijgegeven heeft. Voor gedeelde mailboxen, analyseer logboekspoor-ID en controleer welke gebruiker zelfde ID heeft:

```
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
```

Het logbestand toont aan dat user1@domainabc.com en shared1@domainabc.com dezelfde sessie-identifier 5RwUAJcoaVYxN6nZ3xcW gebruiken. Dit betekent dat beide gebruikers dezelfde sessie in het systeem delen of gebruiken. Dit geeft aan dat shared1 werkt in het kader van de sessie die oorspronkelijk door gebruiker1 is gestart.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.