Configura la cassetta postale condivisa di Cloud Email Security con O365

Sommario

Introduzione

In questo documento vengono descritte le configurazioni per visualizzare la quarantena di Cisco Secure Email Gateway Spam in una cassetta postale condivisa in Exchange Online (O365).

Prerequisiti

Requisiti

Per procedere con la configurazione, verificare che siano soddisfatti i seguenti requisiti:

- Implementazione dell'autenticazione SAML per l'accesso alla quarantena SPAM.
- Informazioni sugli utenti e sulle cassette postali condivise in Exchange Online.
- Assegnazione degli utenti alle necessarie cassette postali condivise.
- Accedere al portale EntraID per creare un'applicazione.
- Accesso alla console di reporting CES per attivare il servizio Cassette postali condivise.

Una volta soddisfatti tutti i requisiti, è possibile seguire i passaggi di configurazione riportati di seguito.

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

Sono disponibili anche configurazioni alternative per la gestione di tali messaggi di posta elettronica. Tra queste, l'abilitazione delle notifiche SPAM per consentire il rilascio della posta elettronica senza autenticazione o la creazione di criteri personalizzati per reindirizzare i messaggi contrassegnati alla cartella Posta indesiderata della cassetta postale corrispondente in Exchange Online.

Configurazione

Passaggio 1. Creazione di un'applicazione in EntraID

Prima di configurare Cisco Secure Email Gateway, stabilire l'accesso necessario in EntraID:

1. Accedere a EntraID.
2. Selezionare Registrazioni app.
3. Fare clic su Nuova registrazione e come nome, utilizzare "Cisco CES Shared Mailbox".
4. Scegliere Account solo in questa directory organizzativa (solo emailsecdemo - Singolo tenant).
5. In URL di reindirizzamento, selezionare Web e immettere il collegamento all'area di quarantena della posta indesiderata, nel formato likehttps://XXXXX-YYYY.iphmx.com/.
6. Fare clic su Registra.

Assegna autorizzazioni

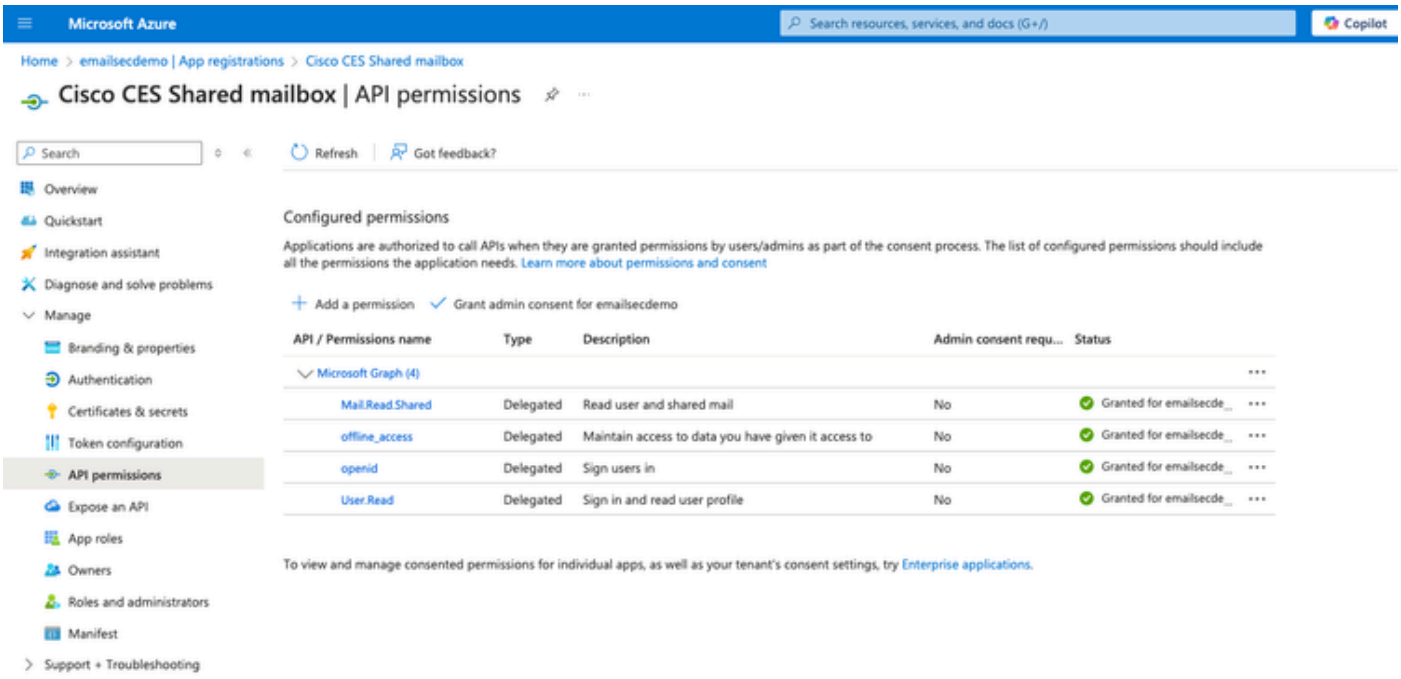
1. Aprire l'applicazione appena creata.

2. Andare a Autorizzazioni API.

3. Assegnare le seguenti autorizzazioni di Microsoft Graph:

    - Mail.Read.Shared: Delegato, consente la lettura della posta utente e condivisa
    - accesso_offline: Delegato, consente di mantenere l'accesso ai dati concessi
    - openid: Delegato, consente agli utenti di accedere
    - User.Read: Delegato, consente di accedere e leggere il profilo utente

4. Infine, fare clic su Concedi il consenso dell'amministratore per emailsecdemo.

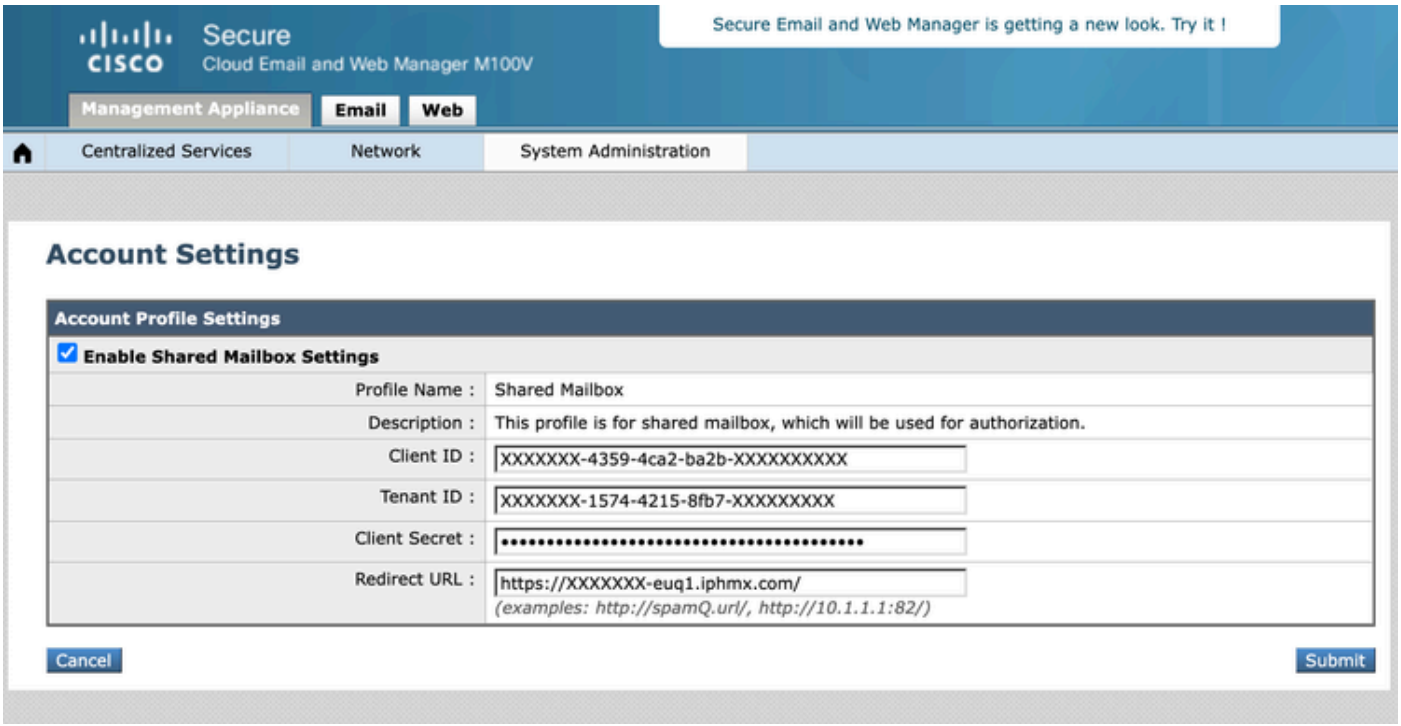


Crea credenziali

1. Nella schermata Panoramica dell'applicazione, andare a Credenziali client.
2. Creare un "segreto client" e salvarne il valore in un luogo sicuro, poiché scompare dopo il salvataggio.

Passaggio 2. Configurare Cisco Cloud Email Security

1. Aprire la console di reporting e accedere a Amministrazione sistema -> Impostazioni account.
2. Attiva e configura il servizio Cassette postali condivise.
3. Fare clic su Modifica impostazioni, abilitare il servizio e aggiungere i campi obbligatori. Utilizzare le informazioni dell'applicazione creata in EntraID e Client Secret.
4. Configurare l'URL di reindirizzamento in modo coerente con la configurazione EntraID.
5. Fare clic su Invia e verificare se un utente ha accesso a una cassetta postale condivisa.



Test

Eseguire un test con un utente che ha accesso a una cassetta postale condivisa.

Nella quarantena della posta indesiderata è disponibile una nuova opzione Visualizza messaggi per la cassetta postale, che consente di aggiungere tutte le cassette postali condivise a cui si ha accesso.

1. Aprire la quarantena e accedere con un utente normale che utilizza SAML.
2. Fare clic su Visualizza messaggi per la cassetta postale.
3. Scrivere l'indirizzo di posta elettronica della cassetta postale condivisa a cui l'utente ha accesso e fare clic su Aggiungi cassetta postale.
4. Fare clic su Visualizza messaggi per cassetta postale e selezionare la cassetta postale condivisa da rivedere.

Ulteriori informazioni

Nel registro GUI di quarantena della posta indesiderata, è possibile verificare quando un utente rilascia un'e-mail. Se autenticato, è possibile identificare l'autore del rilascio. Per le cassette postali condivise, analizza l'ID di traccia del log e verifica quale utente ha lo stesso 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
```

Nel log viene mostrato che sia user1@domainabc.com che shared1@domainabc.com utilizzano lo stesso identificatore di sessione 5RwUAJcoaVYxN6nZ3xcW. Ciò significa che entrambi gli utenti condividono o utilizzano la stessa sessione nel sistema. Ciò indica che shared1 agisce nella sessione avviata in origine da user1.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).