Konfigurieren des gemeinsam genutzten Cloud Email Security-Postfachs mit O365

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

Konfiguration

- Schritt 1: Erstellen einer Anwendung in EntraID
  - Berechtigungen zuweisen
  - Anmeldeinformationen erstellen
- Schritt 2: Konfigurieren von Cisco Cloud Email Security

Testen

Zusätzliche Informationen

Einleitung

In diesem Dokument werden die Konfigurationen für die Anzeige von Cisco Secure Email Gateway Spam Quarantine in einem freigegebenen Postfach in Exchange Online (O365) beschrieben.

Voraussetzungen

Anforderungen

Um mit der Konfiguration fortzufahren, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Implementierung der SAML-Authentifizierung für den Zugriff auf die SPAM-Quarantäne
- Informationen zu Benutzern und freigegebenen Postfächern in Exchange Online.
- Zuweisung von Benutzern zu den erforderlichen freigegebenen Mailboxen
- Zugriff auf das EntraID-Portal zum Erstellen einer Anwendung.
- Zugriff auf die CES-Reporting-Konsole zur Aktivierung des Shared Mailbox-Service

Wenn alle Anforderungen erfüllt sind, können Sie die unten aufgeführten Konfigurationsschritte durchführen.

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Für die Verwaltung solcher E-Mails stehen auch alternative Konfigurationen zur Verfügung. Dazu gehört die Aktivierung von SPAM-Benachrichtigungen, um die Freigabe von E-Mails ohne Authentifizierung zu ermöglichen, oder die Erstellung einer benutzerdefinierten Richtlinie, um gekennzeichnete E-Mails an den Junk-Ordner des entsprechenden Postfachs in Exchange Online umzuleiten.

Konfiguration

Schritt 1: Erstellen einer Anwendung in EntraID

Stellen Sie vor der Konfiguration von Cisco Secure Email Gateway den erforderlichen Zugriff in EntraID her:

1. Zugriff auf EntraID.
2. Wählen Sie App-Registrierungen aus.
3. Klicken Sie auf New Registration (Neue Registrierung), und verwenden Sie als Namen "Cisco CES Shared Mailbox".
4. Wählen Sie "Accounts" (Konten) nur in diesem Unternehmensverzeichnis aus (nur E-Mail-Demo - Single-Tenant).
5. Wählen Sie unter Redirect URL (URL umleiten) die Option Web aus, und geben Sie den Link zu Ihrem SPAM Quarantine-Bereich mit dem Format likehttps://XXXXX-YYYY.iphmx.com/ein.
6. Klicken Sie auf Registrieren.

Berechtigungen zuweisen

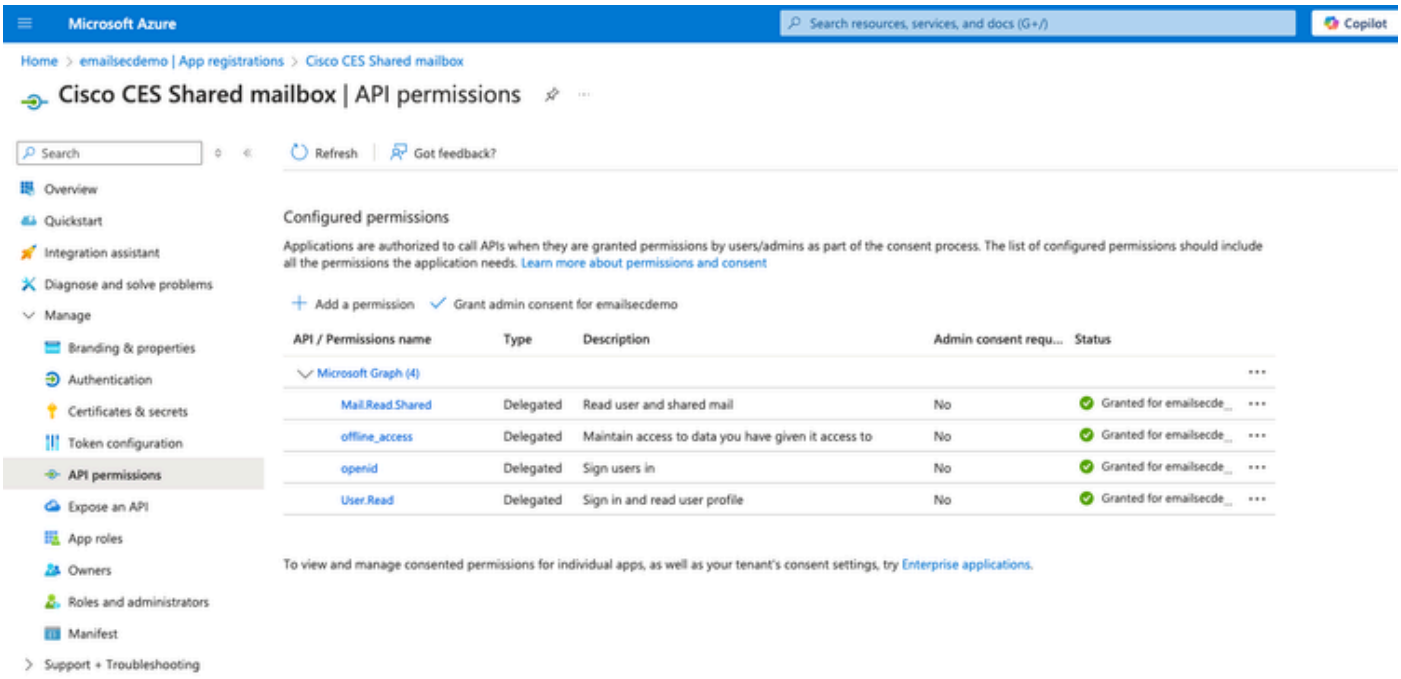
1. Öffnen Sie die neu erstellte Anwendung.

2. Wechseln Sie zu API-Berechtigungen.

3. Weisen Sie folgende Microsoft Graph-Berechtigungen zu:

    - Mail.Read.Shared: Delegiert, ermöglicht das Lesen von Benutzer- und freigegebenen E-Mails
    - Offline-Zugriff: Delegiert, ermöglicht die Aufrechterhaltung des Zugriffs auf gewährte Daten
    - openid: Delegiert; ermöglicht die Anmeldung von Benutzern
    - Benutzer.Lesen: Delegiert, ermöglicht das Anmelden und Lesen von Benutzerprofilen

4. Klicken Sie abschließend auf Zustimmung des Administrators für E-Mail-Demo erteilen.

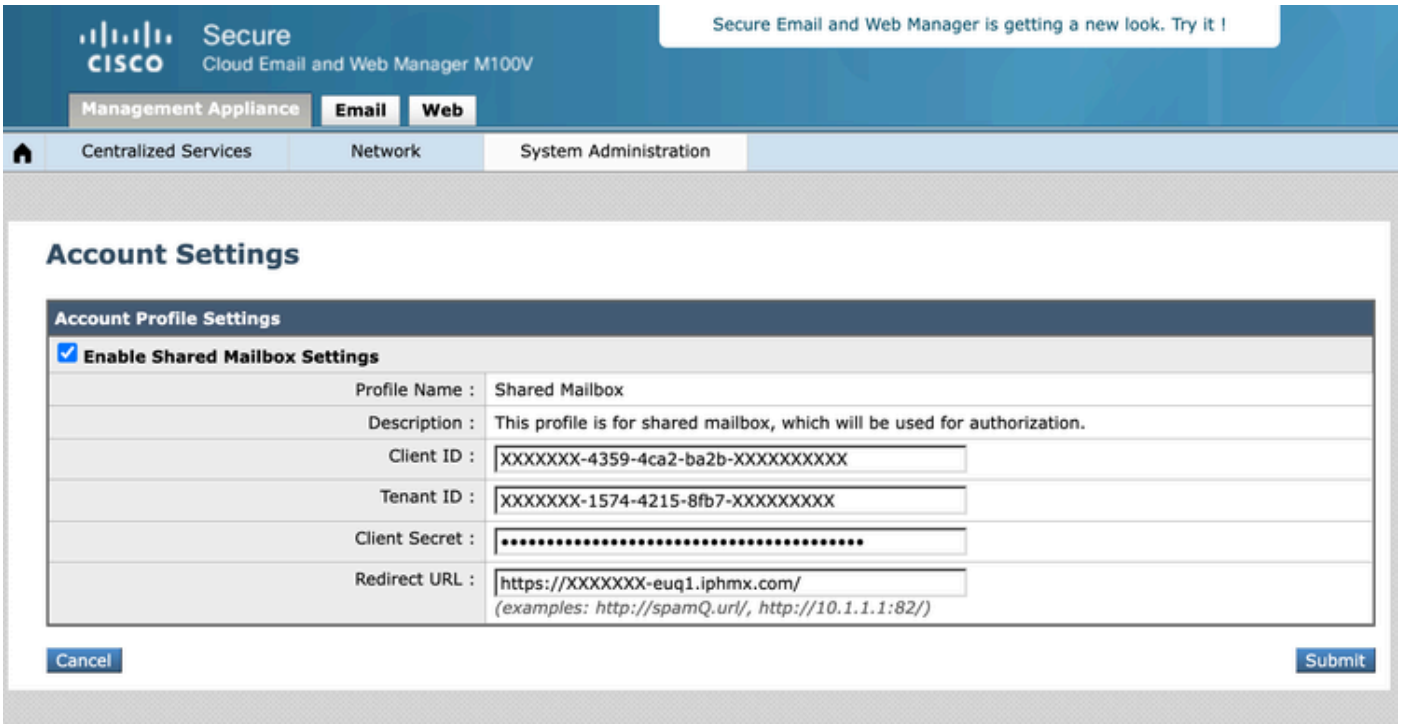


Anmeldeinformationen erstellen

1. Navigieren Sie im Bildschirm Übersicht der Anwendung zu Client-Anmeldeinformationen.
2. Erstellen Sie einen "Client Secret" und speichern Sie seinen Wert an einem sicheren Ort, wie es verschwindet nach dem Speichern.

Schritt 2: Konfigurieren von Cisco Cloud Email Security

1. Öffnen Sie die Berichtskonsole, und greifen Sie auf Systemverwaltung -> Kontoeinstellungen zu.
2. Aktivieren und konfigurieren Sie den Dienst für freigegebene Mailboxen.
3. Klicken Sie auf Einstellungen bearbeiten, aktivieren Sie den Dienst, und fügen Sie die erforderlichen Felder hinzu. Verwenden Sie die Informationen aus der Anwendung, die in EntraID und dem Clientschlüssel erstellt wurde.
4. Konfigurieren Sie die Umleitungs-URL konsistent mit der EntraID-Konfiguration.
5. Klicken Sie auf Senden, und führen Sie einen Test mit einem Benutzer durch, der Zugriff auf eine freigegebene Mailbox hat.



Testen

Führen Sie einen Test mit einem Benutzer durch, der Zugriff auf ein freigegebenes Postfach hat.

In der SPAM-Quarantäne gibt es eine neue Option Nachrichten für Mailbox anzeigen, mit der Sie alle freigegebenen Mailboxen hinzufügen können, auf die Sie Zugriff haben.

1. Öffnen Sie die Spam-Quarantäne, und melden Sie sich mit einem normalen Benutzer über SAML an.
2. Klicken Sie auf Nachrichten für Postfach anzeigen.
3. Schreiben Sie die freigegebene E-Mail-Adresse, auf die der Benutzer Zugriff hat, und klicken Sie auf Postfach hinzufügen.
4. Klicken Sie auf Nachrichten für Postfach anzeigen, und wählen Sie das freigegebene Postfach zur Überprüfung aus.

Zusätzliche Informationen

Im GUI-Protokoll der Spamquarantäne können Sie überprüfen, wann ein Benutzer eine E-Mail-Nachricht veröffentlicht. Wenn die Authentifizierung erfolgt ist, können Sie feststellen, wer sie freigegeben hat. Analysieren Sie bei freigegebenen Postfächern die Protokollverfolgungs-ID, und überprüfen Sie, welcher Benutzer dieselbe ID hat:

```
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 
```

Aus dem Protokoll geht hervor, dass user1@domainabc.com und shared1@domainabc.com dieselbe Sitzungskennung verwenden wie 5RwUAJcoaVYxN6nZ3xcW. Das bedeutet, dass beide Benutzer dieselbe Sitzung im System teilen oder verwenden. Dies zeigt an, dass shared1 unter der ursprünglich von user1 initiierten Sitzung agiert.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.