Konfigurieren der Cisco Secure Email Account-Einstellungen für Microsoft Azure (Microsoft 365)-API

Inhalt

Einleitung

Dieses Dokument enthält eine schrittweise Anleitung für die Registrierung einer neuen Anwendung in Microsoft Azure (Azure Active Directory), mit der die erforderliche Client-ID, Tenant-ID und Client-Anmeldeinformationen generiert werden können. Anschließend wird die Konfiguration für Kontoeinstellungen auf einem Cisco Secure Email Gateway oder Cloud Gateway konfiguriert. Die Kontoeinstellungen und das zugehörige Kontoprofil müssen konfiguriert werden, wenn ein Mail-Administrator MAR (Mailbox Auto Remediation) für AMP (Advanced Malware Protection) oder URL-Filterung konfiguriert oder die Aktion "Remediate" (Beheben) aus der Nachrichtenverfolgung auf dem Cisco Secure Email und Web Manager oder dem Cisco Secure Gateway/Cloud Gateway verwendet.

Ablauf des automatischen Mailbox-Korrekturprozesses

Ein Anhang (eine Datei) in Ihrer E-Mail oder eine URL kann jederzeit als schädlich bewertet werden, selbst wenn er die Mailbox eines Benutzers erreicht hat. AMP auf Cisco Secure Email (über Cisco Secure Malware Analytics) kann diese Entwicklung identifizieren, sobald neue Informationen verfügbar sind, und sendet retrospektive Warnmeldungen an Cisco Secure Email. Cisco Talos bietet die gleiche URL-Analyse wie AsyncOS 14.2 für Cisco Secure Email Cloud Gateway. Wenn Ihr Unternehmen Microsoft 365 für die Verwaltung von Mailboxen verwendet, können Sie Cisco Secure Email so konfigurieren, dass die Nachrichten in einem Benutzerpostfach automatisch repariert werden, wenn diese Bedrohungen Änderungen verwerfen.

Cisco Secure Email kommuniziert sicher und direkt mit Microsoft Azure Active Directory, um Zugriff auf Microsoft 365-Mailboxen zu erhalten. Wenn beispielsweise eine E-Mail mit einem Anhang über das Gateway verarbeitet und von AMP gescannt wird, wird der Dateianhang (SHA256) AMP zur Dateireputation bereitgestellt. Die AMP-Einstufung kann als "Clean" (Schritt 5, Abbildung 1) markiert und dann an die Microsoft 365-Mailbox des Endempfängers gesendet werden. Zu einem späteren Zeitpunkt wird die AMP-Einstufung in "bösartig" geändert. Cisco Malware Analytics sendet ein retrospektives Verdict-Update (Schritt 8, Abbildung 1) an *jedes* Gateway, das diesen spezifischen SHA256 verarbeitet hat. Sobald das Gateway das retrospektive Urteilsupdate von "Malicious" (Böswillig) erhält (falls konfiguriert), ergreift das Gateway eine der folgenden Mailbox-MAR-Aktionen (Auto Remediation): Weiterleiten, Löschen oder Weiterleiten und Löschen.

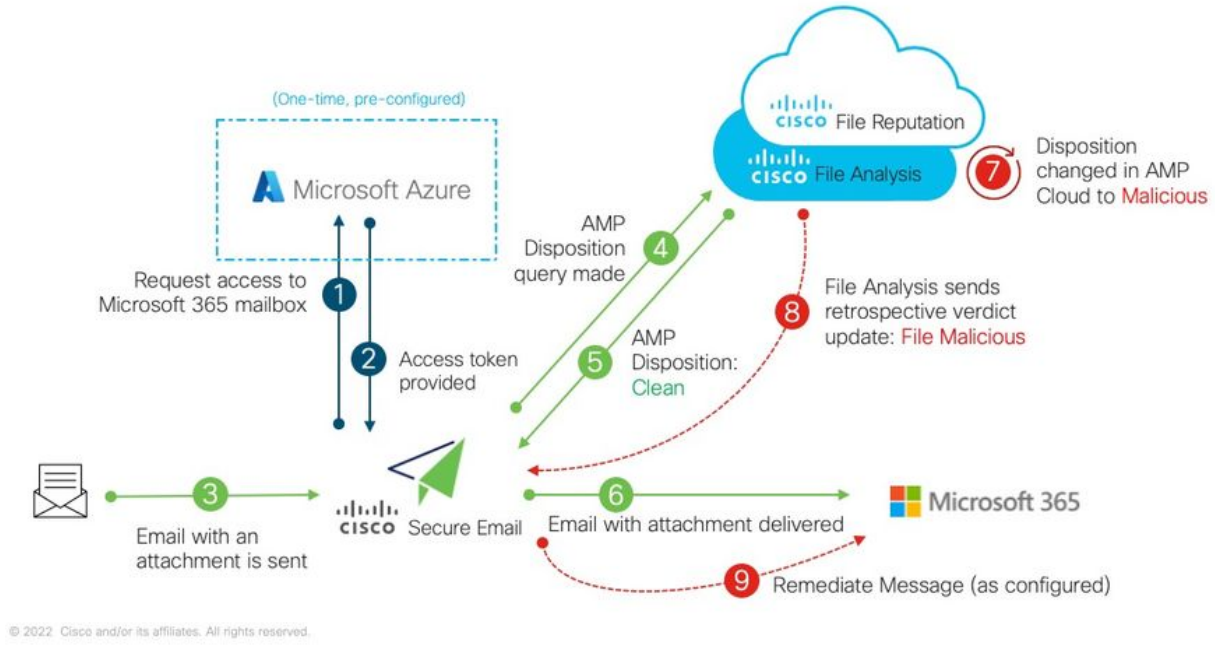

Abbildung 1: MAR (für AMP) für Cisco Secure Email

In diesem Leitfaden wird beschrieben, wie Cisco Secure Email mit Microsoft 365 nur für die automatische Mailbox-Problembehebung konfiguriert wird. AMP (File Reputation and File Analysis) und/oder URL Filtering auf dem Gateway sollte bereits konfiguriert sein. Weitere Informationen zur Dateireputation und Dateianalyse finden Sie im Benutzerhandbuch zur bereitgestellten AsyncOS-Version.

Voraussetzungen

1. Microsoft 365-Kontoabonnement (Bitte stellen Sie sicher, dass Ihr Microsoft 365-Kontoabonnement Zugriff auf Exchange enthält, z. B. ein Enterprise E3- oder Enterprise E5-Konto.)

2. Microsoft Azure-Administratorkonto und Zugriff auf http://portal.azure.com

3. Sowohl die Microsoft 365- als auch die Microsoft Azure AD-Konten sind ordnungsgemäß an eine aktive "user@domain.com"-E-Mail-Adresse gebunden. Sie können über diese E-Mail-Adresse E-Mails senden und empfangen.

Sie erstellen die folgenden Werte, um die API-Kommunikation von Cisco Secure Email Gateway zu Microsoft Azure AD zu konfigurieren:

- **Client-ID**
- **Tenant-ID**
- **Client-geheim**

  Anmerkung: Ab AsyncOS 14.0 ermöglichen **Kontoeinstellungen** bei der Erstellung der Microsoft Azure-App-Registrierung die Konfiguration mithilfe eines Client-geheimen Systems. Dies ist die einfachere und bevorzugte Methode.

Optional - Wenn Sie den Client-geheim NICHT verwenden, müssen Sie Folgendes erstellen und bereit sein:

- **Daumenabdruck**
- **Der private Schlüssel (PEM-Datei)**

Das Erstellen des Daumenabdrucks und des privaten Schlüssels wird im Anhang dieses Leitfadens behandelt:

1. Ein aktives öffentliches (oder privates) Zertifikat (CER) und der private Schlüssel, der zum Signieren des Zertifikats (PEM) verwendet wird, oder die Möglichkeit, ein öffentliches Zertifikat (CER) zu erstellen und den privaten Schlüssel zum Signieren des Zertifikats (PEM) zu speichern. Cisco stellt in diesem Dokument zwei Methoden bereit, um dies basierend auf Ihren Verwaltungsprioritäten zu erreichen: Zertifikat: Unix/Linux/OS X (mit OpenSSL)Zertifikat: Windows (mit PowerShell)

2. Zugriff auf Windows PowerShell, normalerweise über einen Windows-Host oder -Server verwaltet - oder - Zugriff auf Terminal-Anwendung über Unix/Linux

Zum Erstellen dieser erforderlichen Werte müssen Sie die in diesem Dokument beschriebenen Schritte ausführen.

Registrieren Sie eine Azure-App zur Verwendung mit Cisco Secure Email

Registrierung von Anwendungen

Melden Sie sich beim Microsoft Azure-Portal an.

1. Klicken Sie auf **Azure Active Directory** (Abbildung 2).
2. Klicken Sie auf **App-Registrierungen.**
3. Klicken Sie auf **+ Neue Registrierung**
4. Auf der Seite "Registrieren einer Anwendung":
   antwort: Name: **Cisco Secure Email MAR** (oder der Name Ihrer Wahl)
   b. Unterstützte Kontotypen: **Nur Konten in diesem Organisationsverzeichnis (Kontoname)**
   c. URI umleiten: (optional)
   [Hinweis: Sie können diese Felder leer lassen oder https://www.cisco.com/sign-on zum Ausfüllen verwenden.]
   d. Klicken Sie unten auf der Seite auf **Registrieren.**

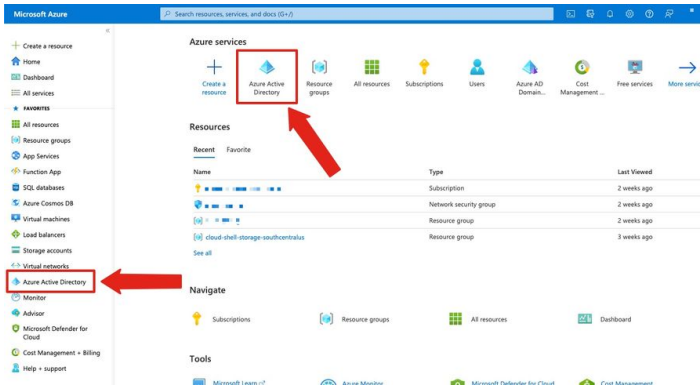

Abbildung 2: Microsoft Azure-Portal-Beispiel

Wenn Sie die oben genannten Schritte abgeschlossen haben, wird Ihnen Ihr Antrag angezeigt:

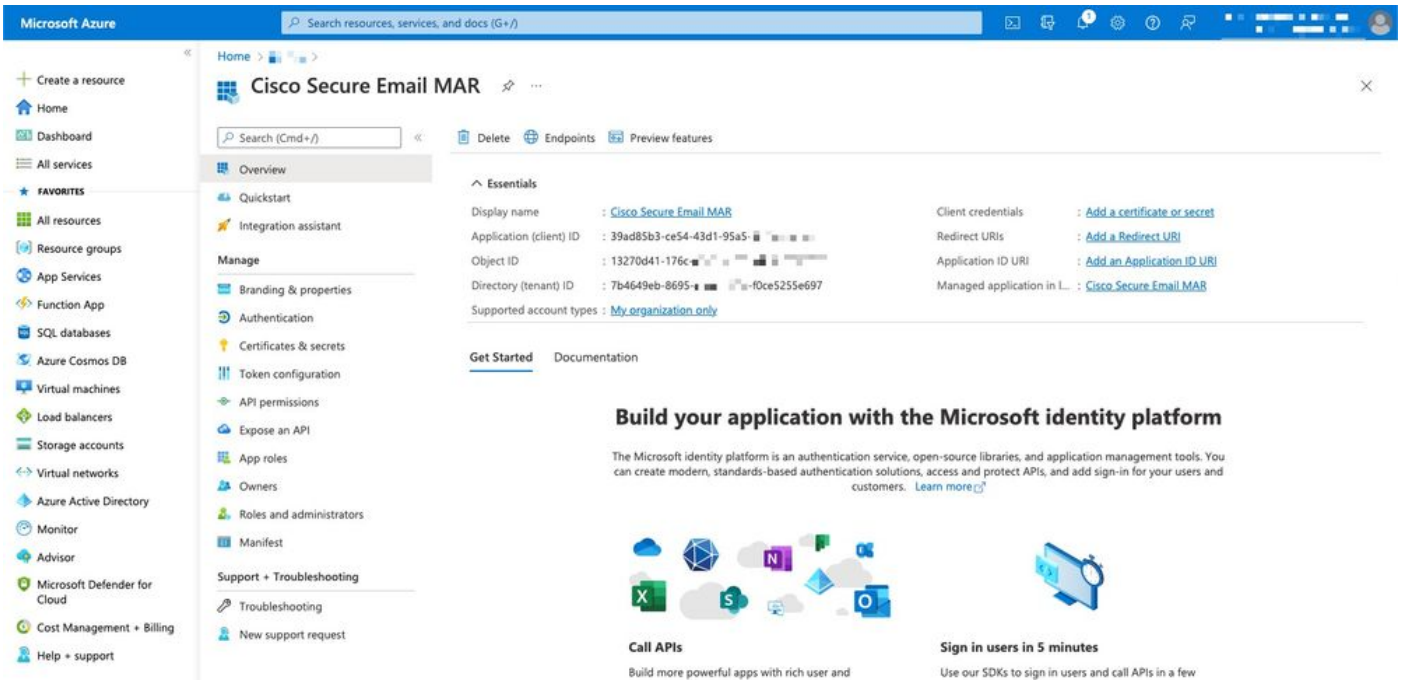

Abbildung 3: Microsoft Azure Active Directory-Anwendungs-Seite

Zertifikate und Geheimnisse

Wenn Sie AsyncOS 14.0 oder höher ausführen, empfiehlt Cisco, Ihre Azure-App zu konfigurieren,

um einen geheimen Client zu verwenden. Wählen Sie im Anwendungsbereich die Optionen Verwalten aus:

1. Wählen Sie **Zertifikate und Geheimnisse**

2. Klicken Sie im Abschnitt ***"Clientgeheimnisse"*** auf **+ Geheimhaltungsgrad für neuen Client.**

3. Fügen Sie eine Beschreibung hinzu, um herauszufinden, wofür dieser Client geheim ist, z. "Cisco Secure E-Mail Behebung"

4. Wählen Sie einen Ablaufzeitraum aus.

5. Klicken Sie auf **Hinzufügen**

6. Fahren Sie mit der Maus über den generierten Wert, und klicken Sie auf das Symbol **In Zwischenablage kopieren**.

7. Speichern Sie diesen Wert in Ihren Notizen. Beachten Sie diesen als "Client-geheim".

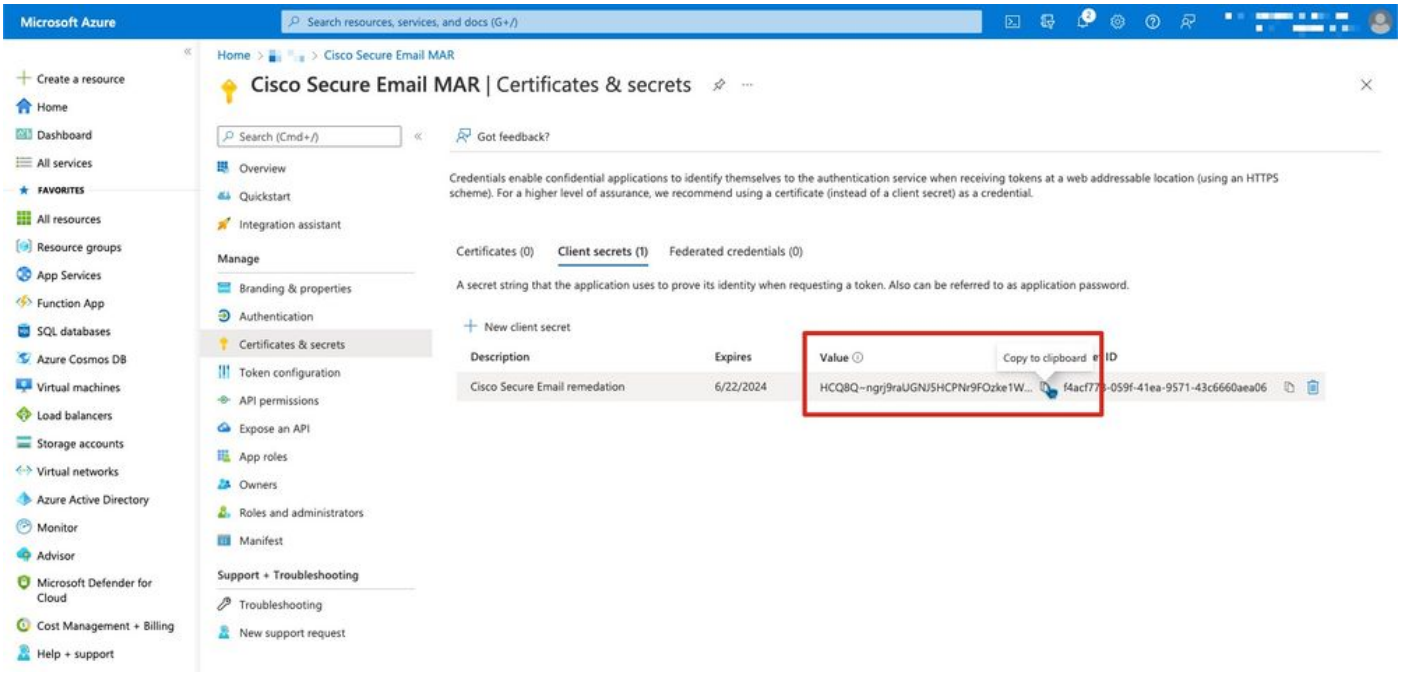

Abbildung 4: Microsoft Azure Erstellen ein Client-geheimes Beispiel

> **Anmerkung:** Sobald Sie Ihre aktive Microsoft Azure-Sitzung beenden, wird der Wert des soeben erstellten Client-Geheimnisses *** aus dem Wert herausfallen. Wenn Sie den Wert vor dem Beenden nicht aufzeichnen und sichern, müssen Sie den Client-geheim neu erstellen, um die Klartextausgabe zu sehen.

Optional: Wenn Sie Ihre Azure-Anwendung nicht mit einem Client-geheimen konfigurieren möchten, konfigurieren Sie die Azure-App so, dass sie Ihr Zertifikat verwendet. Wählen Sie im Anwendungsbereich die Optionen Verwalten aus:

1. Wählen Sie **Zertifikate und Geheimnisse**

2. Klicken Sie auf **Zertifikat hochladen.**
3. Wählen Sie die CRT-Datei aus (wie zuvor erstellt)
4. Klicken Sie auf **Hinzufügen**

API-Berechtigungen

Anmerkung: Ab AsyncOS 13.0 für E-Mail-Sicherheit mussten die API-Berechtigungen für Microsoft Azure in die sichere E-Mail-Kommunikation von Cisco geändert werden, anstatt Microsoft Exchange zu Microsoft Graph zu verwenden. Wenn Sie bereits MAR konfiguriert haben und Ihr bestehendes Cisco Secure Email Gateway auf AsyncOS 13.0 aktualisieren möchten, können Sie einfach die neuen API-Berechtigungen aktualisieren bzw. hinzufügen. (Wenn Sie eine ältere Version von AsyncOS, 11.x oder 12.x ausführen, lesen Sie zunächst Anhang B.)

Wählen Sie im Anwendungsbereich die Optionen Verwalten aus:

1. Wählen Sie **API-Berechtigungen aus**
2. Klicken Sie **+ Berechtigungen hinzufügen**
3. Wählen Sie **Microsoft Graph aus**
4. Wählen Sie die folgenden Berechtigungen für ***Anwendungsberechtigungen aus***: Mail > "Mail.Read" (E-Mail in allen Mailboxen lesen)Mail > "Mail.ReadWrite" (Lesen und Schreiben von E-Mails in allen Mailboxen)Mail > "Mail.Send" (E-Mail als beliebige Benutzer senden)Verzeichnis > "Directory.Read.All" (Verzeichnisdaten lesen) [*Optional: Wenn Sie LDAP Connector/LDAP-Synchronisierung verwenden, aktivieren Sie das Kontrollkästchen. Andernfalls ist dies nicht erforderlich.]
5. *Optional:* Sie sehen, dass Microsoft Graph standardmäßig für "User.Read"-Berechtigungen aktiviert ist. Sie können dies als konfiguriert lassen, oder klicken Sie auf **Lesen** und dann auf **Berechtigung entfernen,** um diese aus den API-Berechtigungen zu entfernen, die der Anwendung zugeordnet sind.
6. Klicken Sie auf **Berechtigungen hinzufügen** (oder **Berechtigungen aktualisieren**, wenn Microsoft Graph bereits aufgeführt wurde).
7. Klicken Sie abschließend auf "**Administratorgenehmigung gewähren" für..** um sicherzustellen, dass die neuen Berechtigungen auf die Anwendung angewendet werden
8. In einem Popup-Fenster werden folgende Fragen gestellt:
   "*Möchten Sie die Genehmigung der beantragten Berechtigungen für alle Konten in <Azure Name> erteilen? Dadurch werden alle vorhandenen Datensätze für die Administratorgenehmigung aktualisiert, die diese Anwendung bereits mit den unten aufgeführten Datensätzen abgleichen muss.*"

   Klicken Sie auf **Ja.**

An diesem Punkt sollten Sie eine grüne Erfolgsmeldung sehen und die Spalte "Admin Consent Required" (Zustimmung erforderlich) wird als "Granted" angezeigt.

Abrufen Ihrer Client-ID und Tenant-ID

Wählen Sie im Anwendungsbereich die Optionen Verwalten aus:

1. Klicken Sie auf **Übersicht**
2. Fahren Sie mit der Maus rechts neben Ihrer Anwendungs-(Client-)ID, und klicken Sie auf das Symbol **In Zwischenablage kopieren**.
3. Speichern Sie diesen Wert in Ihren Notizen. Beachten Sie, dass dies als "Client-ID" angezeigt wird.
4. Fahren Sie mit der Maus rechts neben Ihrer Directory (Tenant)-ID, und klicken Sie auf das Symbol **Copy to Clipboard (In Zwischenablage kopieren)**.
5. Speichern Sie diesen Wert in Ihren Notizen. Beachten Sie, dass dies als "Tenant-ID" gilt.

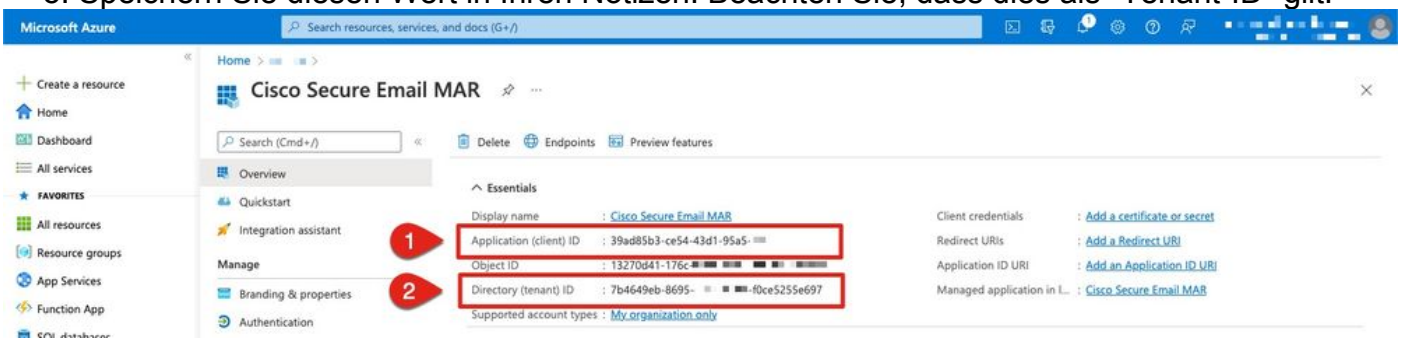

Abbildung 5: Microsoft Azure... Client-ID, Beispiel für Tenant-ID

Konfigurieren des Cisco Secure Email Gateway/Cloud Gateway

Zu diesem Zeitpunkt sollten Sie die folgenden Werte erstellen und in Ihren Notizen speichern lassen:

- **Client-ID**
- **Tenant-ID**
- **Client-geheim**

Optional, wenn der Client-geheim nicht verwendet wird:

- **Daumenabdruck**
- **Der private Schlüssel (PEM-Datei)**

Sie können die aus Ihren Notizen erstellten Werte verwenden und die Kontoeinstellungen auf dem Cisco Secure Email Gateway konfigurieren!

Kontoprofil erstellen

1. Melden Sie sich beim Kabelmodem an.
2. Navigieren Sie zu **Systemverwaltung > Kontoeinstellungen.** Anmerkung: Wenn Sie eine Version vor AsyncOS 13.x ausführen, lautet dies **Systemverwaltung > Mailbox-Einstellungen.**
3. Klicken Sie auf **Aktivieren.**

4. Aktivieren Sie das Kontrollkästchen Kontoeinstellungen aktivieren, und klicken Sie auf **Senden.**
5. Klicken Sie auf **Kontoprofil erstellen.**
6. Geben Sie einen Profilnamen und eine Beschreibung an (eine Beschreibung, die Ihr Konto eindeutig beschreibt, wenn Sie mehrere Domänen haben).
7. Wenn Sie eine Microsoft 365-Verbindung definieren, lassen Sie den Profiltyp **Office 365/Hybrid (Graph-API) unverändert.**
8. Geben Sie Ihre **Client-ID ein.**
9. Geben Sie Ihre **Tenant-ID ein.**
10. Für die Anmeldeinformationen des Clients führen Sie wie in Azure konfiguriert einen der folgenden Schritte aus: Klicken Sie auf **Client Secret** (Client-**geheim**), und fügen Sie den konfigurierten Clientgeheim ein.Klicken Sie auf **Client Certificate**, geben Sie den Daumenabdruck ein, und geben Sie das PEM durch Klicken auf "Choose File" (Datei auswählen) ein.
11. Klicken Sie auf **Senden**
12. Klicken Sie in der rechten oberen Ecke der Benutzeroberfläche auf **Änderungen bestätigen.**
13. Geben Sie Kommentare ein, und schließen Sie die Konfigurationsänderungen durch Klicken auf **Änderungen bestätigen ab.**

Verbindung überprüfen

Im nächsten Schritt wird lediglich die API-Verbindung vom Cisco Secure Email Gateway zu Microsoft Azure überprüft:

1. Klicken Sie auf derselben Seite mit den Kontodetails auf **Verbindung testen.**
2. Geben Sie eine gültige E-Mail-Adresse für die Domäne ein, die in Ihrem Microsoft 365-Konto verwaltet wird.
3. Klicken Sie auf **Verbindung testen.**
4. Sie sollten eine Erfolgsmeldung erhalten (Abbildung 6).
5. Klicken Sie zum Abschließen **auf Fertig**

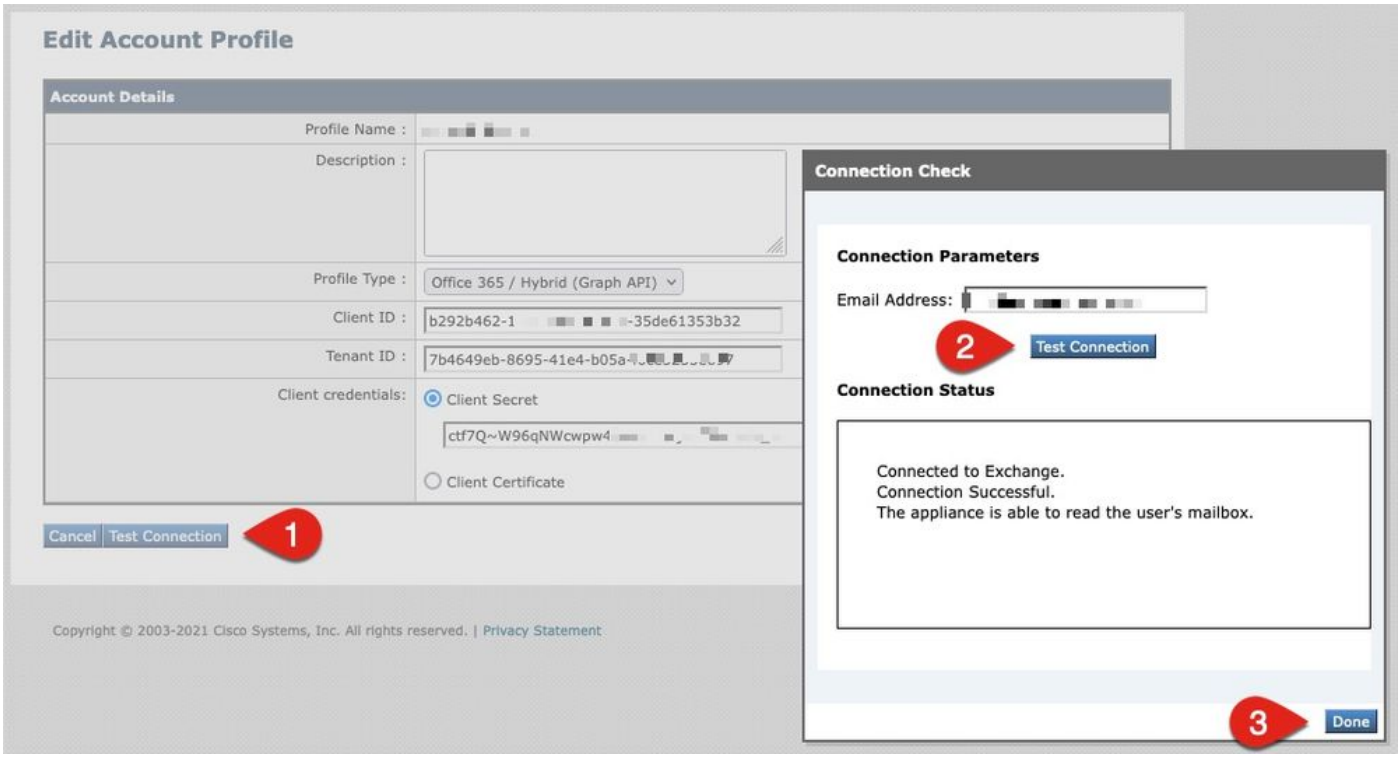

Abbildung 6: Kontenprofil/Verbindungsüberprüfung - Beispiel

6. Klicken Sie im Abschnitt *Domänenzuordnung* auf **Domänenzuordnung erstellen.**

7. Geben Sie die Domänennamen ein, die dem Microsoft 365-Konto zugeordnet sind und für die Sie die API-Verbindung gerade validiert haben für

Im Folgenden finden Sie eine Liste gültiger Domänenformate, mit denen ein Mailbox-Profil zugeordnet werden kann:

- Die Domäne kann das spezielle Schlüsselwort 'ALL' sein, um alle Domänen abzugleichen, um eine Standard-Domänenzuordnung zu erstellen.

- Domänennamen wie 'beispiel.com' - Ordnet jede Adresse dieser Domäne zu.

- Partielle Domänennamen wie '@.partielle.example.com' - Entspricht jeder Adresse, die mit dieser Domäne endet.

- Mehrere Domänen können über eine kommagetrennte Liste von Domänen eingegeben werden.

8. Klicken Sie auf **Senden**

9. Klicken Sie in der rechten oberen Ecke der Benutzeroberfläche auf **Änderungen bestätigen.**

10. Geben Sie Kommentare ein, und schließen Sie die Konfigurationsänderungen durch Klicken auf **Änderungen bestätigen ab.**

Automatische Mailbox-Bereinigung (MAR) für Advanced Malware Protection in Mail Policy aktivieren

Führen Sie diesen Schritt aus, um MAR in der AMP-Konfiguration für Mail-Richtlinien zu aktivieren.

1. Navigieren Sie zu **Mail-Policys > Richtlinien für eingehende E-Mails.**
2. Klicken Sie in der Spalte Advanced Malware Protection (erweiterter Malware-Schutz) auf die Einstellungen für den Richtliniennamen, den Sie konfigurieren möchten (z. B. Abbildung 7):

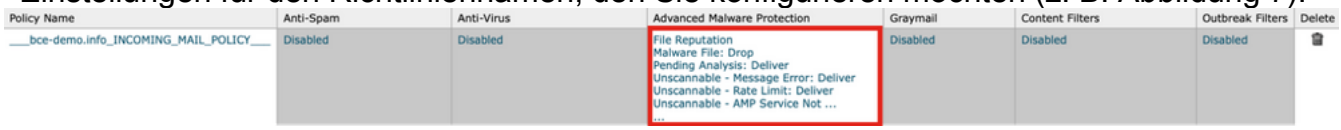

Abbildung 7: MAR aktivieren (Richtlinien für eingehende E-Mails)

3. Navigieren Sie zum Ende der Seite.
4. Aktivieren Sie das Kontrollkästchen Enable Mailbox Auto Remediation (Automatische Mailbox-Bereinigung aktivieren).
5. Wählen Sie eine der folgenden Aktionen für MAR aus (z. B. Abbildung 8): Weiterleiten an: <*E-Mail-Adresse eingeben*>LöschenWeiterleiten an: <*E-Mail-Adresse eingeben*> und Löschen

Abbildung 8: MAR für AMP-Konfigurationsbeispiel aktivieren

6. Klicken Sie auf **Senden**
7. Klicken Sie in der rechten oberen Ecke der Benutzeroberfläche auf **Änderungen bestätigen.**
8. Geben Sie Kommentare ein, und schließen Sie die Konfigurationsänderungen durch Klicken auf **Änderungen bestätigen ab.**

Automatische Mailbox-Bereinigung (MAR) für URL-Filterung aktivieren

Beginnend mit AsyncOS 14.2 für Cisco Secure Email Cloud Gateway umfasst die URL-Filterung jetzt URL-Retrospective Verdict und URL-Bereinigung.

1. Navigieren Sie zu **Sicherheitsdienste > URL-Filterung.**
2. Wenn Sie noch keine URL-Filterung konfiguriert haben, klicken Sie auf **Aktivieren.**
3. Aktivieren Sie das Kontrollkästchen URL-Kategorie und Reputationsfilter aktivieren.

4. Die *erweiterten Einstellungen* mit den Standardeinstellungen
5. Klicken Sie auf **Senden**

Die URL-Filterung sollte ähnlich wie folgt aussehen:

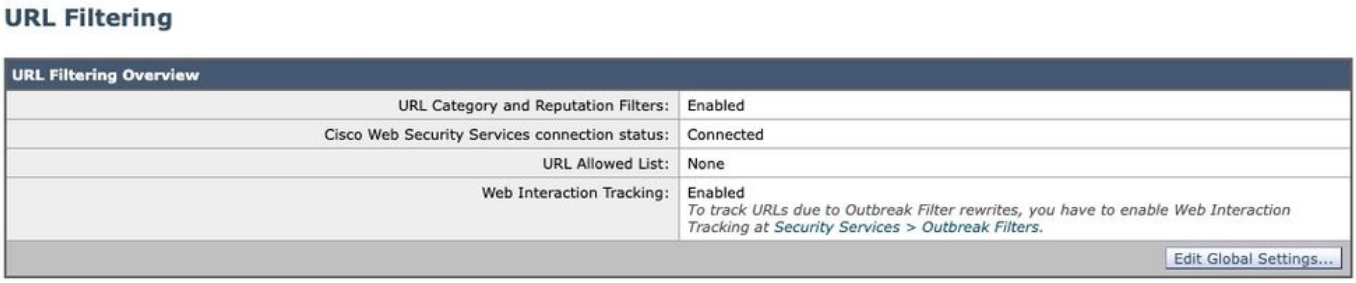

Abbildung 9: Beispiel für URL-Filterung nach der Aktivierung

Um URL-Retrospektion mit der URL-Filterung anzuzeigen, führen Sie die folgenden Schritte aus, oder lassen Sie ein Support-Ticket für Cisco öffnen, um Folgendes auszuführen:

```
esa1.hcxxyy-zz.iphmx.com> urlretroservice enable

URL Retro Service is enabled.

esa1.hcxxyy-zz.iphmx.com> websecurityconfig

URL Filtering is enabled.
No URL list used.
Web Interaction Tracking is enabled.
URL Retrospective service based Mail Auto Remediation is disabled.
URL Retrospective service status - Unavailable

Disable URL Filtering? [N]>

Do you wish to disable Web Interaction Tracking? [N]>

Do you wish to add URLs to the allowed list using a URL list? [N]>


Enable URL Retrospective service based Mail Auto Remediation to configure remediation actions.

Do you wish to enable Mailbox Auto Remediation action? [N]> y

URL Retrospective service based Mail Auto Remediation is enabled.

Please select a Mailbox Auto Remediation action:
1. Delete
2. Forward and Delete
3. Forward
[1]> 1

esa1.hcxxyy-zz.iphmx.com> commit

Please enter some comments describing your changes:
[]>

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Tue Mar 29 19:43:48 2022 EDT
```

Aktualisieren Sie nach dem Abschluss die Benutzeroberfläche auf der URL-Filterungsseite, und Sie sollten nun ähnlich wie folgt sehen:

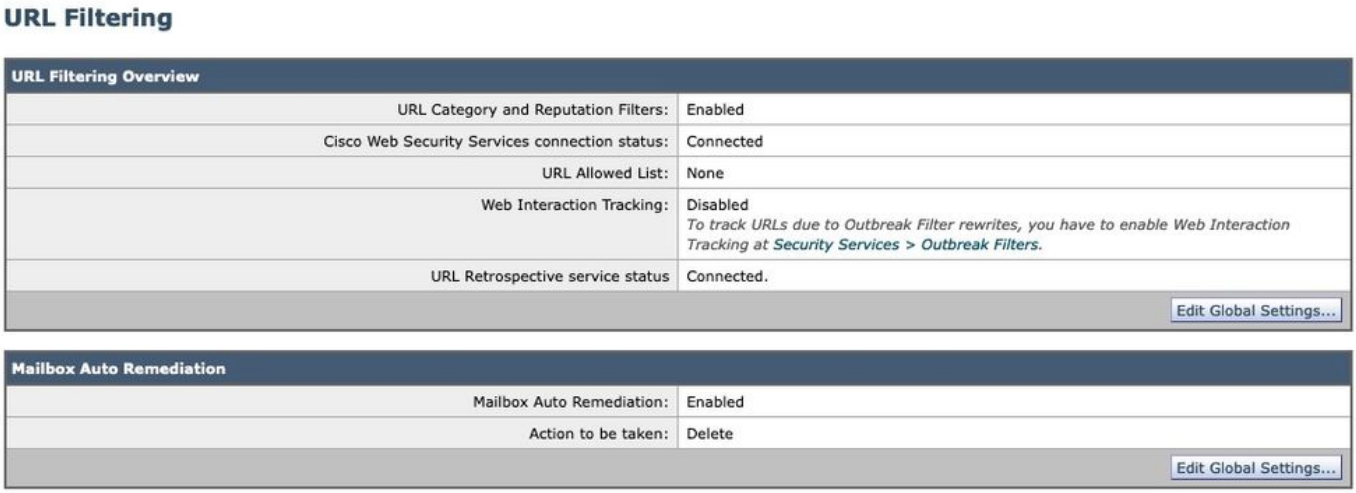

Abbildung 10: URL-Filterung (AsyncOS 14.2 für Cisco Secure Email Cloud Gateway)

Der URL-Schutz kann jetzt Abhilfemaßnahmen durchführen, wenn ein Urteil die Punktzahl ändert. Weitere Informationen finden Sie unter Schutz vor bösartigen oder unerwünschten URLs im Benutzerhandbuch für AsyncOS 14.2 für Cisco Secure Email Cloud Gateway.

Konfiguration abgeschlossen!

Cisco Secure Email ist derzeit bereit, neue Bedrohungen fortlaufend zu evaluieren, sobald neue Informationen verfügbar werden, und Sie über Dateien zu informieren, die als Bedrohungen erkannt werden, nachdem sie in Ihr Netzwerk eingedrungen sind.

Wenn ein retrospektives Urteil aus der Dateianalyse (Cisco Secure Malware Analytics) erstellt wird, erhält der Administrator der E-Mail-Sicherheit (falls konfiguriert) eine Informationsmeldung. Beispiel:

```
The Info message is:

Retrospective verdict received for Book1.xls.

SHA256: 7d06fd224e0de7f26b48dc2daf7f099b3770080d98bd38c49ed049087c416c4b
Timestamp: 2019-06-03T23:40:36Z
Verdict: MALICIOUS
Spyname: W32.7D06FD224E-95.SBX.TG

Total users affected: 1
---------- Affected Messages --------------


Message 1
   MID              : 348938
   Subject          : [WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]test Mon, 03 Jun 2019 16:50:18 -0400
   From             :
   To               :
   File name        : Book1.xls
   Parent SHA256    : unknown
   Parent File name : unknown
   Date             : 2019-06-03T20:52:33Z

------------------------------------------------


Version: 12.1.0-087
Serial Number: 420DE3B51AB744C7F092-9F0
Timestamp: 04 Jun 2019 04:40:36 +0500
```

Die automatische Mailbox-Bereinigung wird wie konfiguriert durchgeführt, wenn sie für die Mail-Richtlinie konfiguriert wurde.

Beispiele für automatische Mailbox-Bereinigung

Berichte für alle SHA256-Geräte, die saniert wurden, werden im Mailbox Auto Remediation-Bericht veröffentlicht, der sowohl auf dem Cisco Secure Email Gateway als auch auf dem Cisco Secure Email und Web Manager zur Verfügung steht.

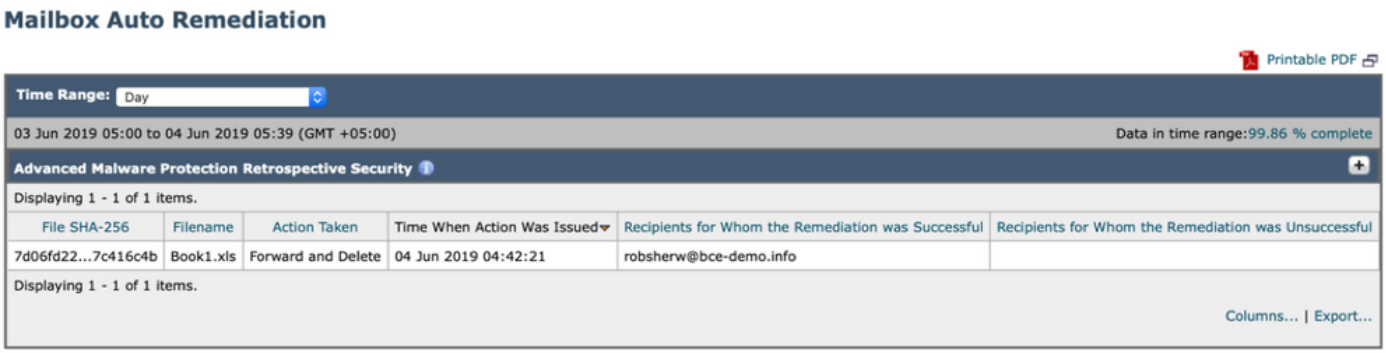

Abbildung 11: (Ältere Benutzeroberfläche) Mailbox-Automatischer Problembehebungsbericht

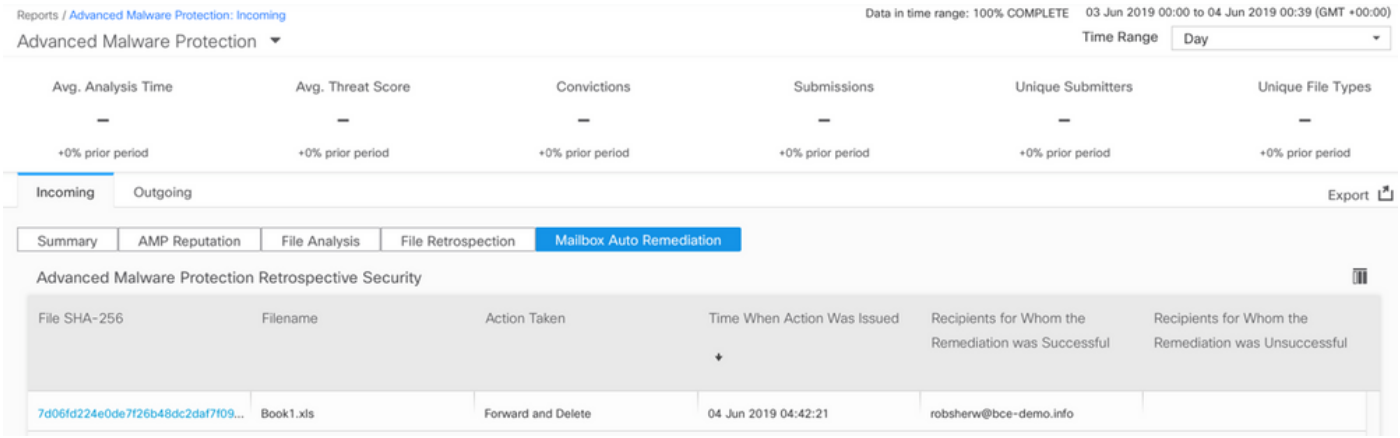

Abbildung 12: (NG-Benutzeroberfläche) Mailbox-Automatischer Problembehebungsbericht

Protokollierung der automatischen Mailbox-Bereinigung

Die automatische Mailbox-Bereinigung hat ein individuelles Protokoll, "mar". Die automatischen Mailbox-Bereinigungsprotokolle enthalten alle Kommunikationsaktivitäten zwischen Ihrem Cisco Secure Email Gateway und Microsoft Azure, Microsoft 365.

Ein Beispiel für die Protokolldateien:

```
Mon May 27 02:24:28 2019 Info: Version: 12.1.0-087 SN: 420DE3B51AB744C7F092-9F0000000000
Mon May 27 02:24:28 2019 Info: Time offset from UTC: 18000 seconds
Fri May 31 01:11:53 2019 Info: Process ready for Mailbox Auto Remediation
Fri May 31 01:17:57 2019 Info: Trying to connect to Azure AD.
Fri May 31 01:17:57 2019 Info: Requesting token from Azure AD.
Fri May 31 01:17:58 2019 Info: Token request successful.
Fri May 31 01:17:58 2019 Info: The appliance is able to read the user's(robsherw@bce-demo.info)
mailbox.
Fri May 31 04:41:54 2019 Info: Trying to perform the configured action on MID:312391
SHA256:de4dd03acda0a24d0f7e375875320538952f1fa30228d1f031ec00870ed39f62 Recipient:robsherw@bce-
demo.info.
Fri May 31 04:41:55 2019 Info: Message containing attachment(s) for which verdict update
was(were) available was not found in the recipient's (robsherw@bce-demo.info) mailbox.
Tue Jun  4 04:42:20 2019 Info: Trying to perform the configured action on MID:348938
SHA256:7d06fd224e0de7f26b48dc2daf7f099b3770080d98bd38c49ed049087c416c4b Recipient:robsherw@bce-
demo.info.
Tue Jun  4 04:42:21 2019 Info: Message containing attachment(s) for which verdict update
was(were) available was not found in the recipient's (robsherw@bce-demo.info) mailbox.
```

Fehlerbehebung: Cisco Secure Email Gateway

Wenn Sie keine erfolgreichen Ergebnisse für den Verbindungsstatustest sehen, können Sie die von Microsoft Azure AD durchgeführte Anwendungsregistrierung überprüfen.

Stellen Sie Ihre MAR-Protokolle vom Cisco Secure Email Gateway auf die Ebene 'trace' ein, und testen Sie die Verbindung erneut.

Bei nicht erfolgreichen Verbindungen werden Protokolle ähnlich angezeigt wie:

```
Thu Mar 30 16:08:49 2017 Info: Trying to connect to Azure AD.
Thu Mar 30 16:08:49 2017 Info: Requesting token from Azure AD.
Thu Mar 30 16:08:50 2017 Info: Error in requesting token: AADSTS70001: Application with
identifier '445796d4-8e72-4d06-a72c-02eb47a4c59a' was not found in the directory ed437e13-ba50-
479e-b40d-8affa4f7e1d7
Trace ID: 4afd14f4-ca97-4b15-bba4-e9be19f30d00
Correlation ID: f38e3388-729b-4068-b013-a08a5492f190
Timestamp: 2017-03-30 20:08:50Z
Thu Mar 30 16:08:50 2017 Info: Error while requesting token AADSTS70001: Application with
identifier '445796d4-8e72-4d06-a72c-02eb47a4c59a' was not found in the directory ed437e13-ba50-
479e-b40d-8affa4f7e1d7
Trace ID: 4afd14f4-ca97-4b15-bba4-e9be19f30d00
Correlation ID: f38e3388-729b-4068-b013-a08a5492f190
Timestamp: 2017-03-30 20:08:50Z
```

Bestätigen Sie die Anwendungs-ID, die Verzeichnis-ID (die mit der Tenant-ID identisch ist) oder andere zugeordnete IDs aus dem Protokoll mit Ihrer Anwendung in Azure AD. Wenn Sie sich über die Werte nicht sicher sind, löschen Sie die Anwendung aus dem Azure AD-Portal und beginnen Sie von vorne.

Für eine erfolgreiche Verbindung sollten Protokolle ähnlich sein wie:

```
Thu Mar 30 15:51:58 2017 Info: Trying to connect to Azure AD.
Thu Mar 30 15:51:58 2017 Info: Requesting token from Azure AD.
Thu Mar 30 15:51:58 2017 Trace: command session starting
Thu Mar 30 15:52:00 2017 Info: Token request successful.
Thu Mar 30 15:52:00 2017 Info: The appliance is able to read the
user's(myuser@mydomain.onmicrosoft.com) mailbox.
```

Fehlerbehebung Azure AD

> **Hinweis**: Das Cisco TAC und der Cisco Support sind nicht berechtigt, kundenseitige Probleme mit Microsoft Exchange, Microsoft Azure AD oder Office 365 zu beheben.

Bei Kundenproblemen mit Microsoft Azure AD müssen Sie den Microsoft Support einbeziehen. Weitere Informationen finden Sie in der Option "Help + Support" in Ihrem Microsoft Azure Dashboard. Sie können direkte Support-Anfragen über das Dashboard an den Microsoft Support

richten.

Anhang A

> **Hinweis**: Dies ist NUR erforderlich, wenn Sie den Client geheim nicht für die Einrichtung Ihrer Azure-Anwendung verwenden.

Erstellen eines öffentlichen und privaten Zertifikats und eines Schlüsselpaars

> **Tipp**: Legen Sie die Ausgabe für *$base64Value*, *$base64Thumbprint* und *$keyid* lokal fest, wie sie später in den Konfigurationsschritten erforderlich ist. Bitte halten Sie die .crt-Datei und die zugehörigen .pem-Dateien Ihres Zertifikats in einem verfügbaren lokalen Ordner auf Ihrem Computer.

> **Anmerkung:** Wenn Sie bereits über ein Zertifikat (x509-Format/Standard) und einen privaten Schlüssel verfügen, überspringen Sie diesen Abschnitt. Stellen Sie sicher, dass Sie sowohl CRT- als auch PEM-Dateien haben, da Sie diese in den nächsten Abschnitten benötigen werden!

Zertifikat: Unix/Linux (mit openssl)

Zu erstellende Werte:
* **Daumenabdruck**
* **Öffentliches Zertifikat (CRT-Datei)**
* **Privater Schlüssel (PEM-Datei)**

Administratoren, die Unix/Linux/OS X verwenden, gehen davon aus, dass Sie OpenSSL installiert haben, um das angegebene Skript zu verwenden.

> **Anmerkung:** Führen Sie die Befehle 'which openssl' und 'openssl version' aus, um die OpenSSL-Installation zu überprüfen. Installieren Sie OpenSSL, wenn es nicht vorhanden ist!

Im folgenden Dokument finden Sie weitere Informationen: Azure AD-Konfigurationsskript für Cisco

Secure Email

Von Ihrem Host aus (UNIX/Linux/OS X):

1. Erstellen Sie in einer Terminalanwendung, einem Texteditor (oder wenn Sie sich beim Erstellen eines Shell-Skripts anfühlen) ein Skript, indem Sie Folgendes kopieren: https://raw.githubusercontent.com/robsherw/my_azure/master/my_azure.sh

2. Skript einfügen
3. Stellen Sie sicher, dass Sie das Skript ausführbar machen! Führen Sie den folgenden Befehl aus: **chmod u+x my_azure.sh**
4. Führen Sie das Skript aus: **./my_azure.sh**

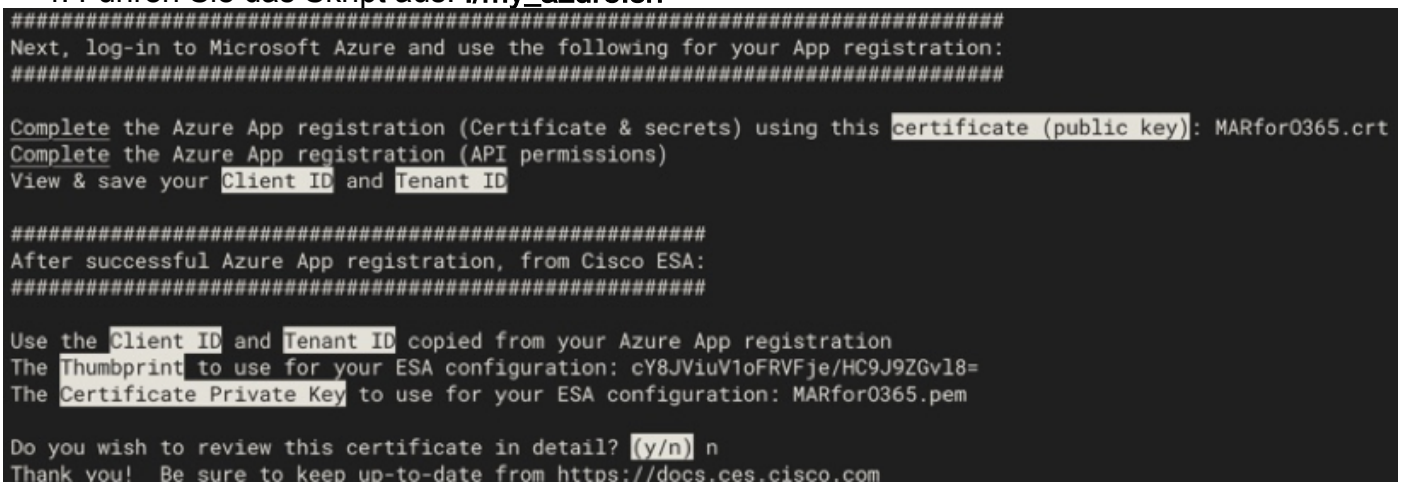

Abbildung 13: Bildschirmausgabe von my_azure.sh

Wie in Abbildung 2 dargestellt, erstellt und ruft das Skript das **Public Certificate (CER-Datei)** auf, das für die Azure-App-Registrierung erforderlich ist. Das Skript ruft auch die***Daumenabdruck***und***Privater Zertifikatschlüssel (PEM-Datei)***Sie werden im Abschnitt "Konfigurieren von Cisco Secure Email" verwendet.

Sie haben die notwendigen Werte, um unsere Anwendung in Microsoft Azure zu registrieren!

[Fahren Sie mit dem nächsten Abschnitt fort! Fahren Sie mit "Zur Verwendung mit Cisco Secure Email registrieren" fort.]

Zertifikat: Windows (mit PowerShell)

Für Administratoren, die Windows verwenden, müssen Sie eine Anwendung verwenden oder über die Kenntnisse verfügen, um ein selbstsigniertes Zertifikat zu erstellen. Dieses Zertifikat wird zur Erstellung der Microsoft Azure-Anwendung und zur dazugehörigen API-Kommunikation verwendet.

Zu erstellende Werte:

* **Daumenabdruck**
* **Öffentliches Zertifikat (CRT-Datei)**
* **Privater Schlüssel (PEM-Datei)**

Unser Beispiel für die Erstellung eines selbstsignierten Zertifikats in diesem Dokument ist XCA (https://hohnstaedt.de/xca/, https://sourceforge.net/projects/xca/).

Anmerkung: XCA kann für Mac, Linux oder Windows heruntergeladen werden.

1. Erstellen Sie eine Datenbank für das Zertifikat und die Schlüssel.
    antwort: Wählen Sie **Datei** in der Symbolleiste aus.
    b. **Neue Datenbank** auswählen
    c. Erstellen Sie ein Kennwort für Ihre Datenbank. (Sie werden es in späteren Schritten benötigen, denken Sie daran!)
2. Klicken Sie auf die Registerkarte Zertifikate, und klicken Sie dann auf **Neues Zertifikat.**
3. Klicken Sie auf die Registerkarte "Betreff", und geben Sie Folgendes ein:
    antwort: Interner Name
    b. CountryName
    c. stateOrProvinceName
    d. LocalityName
    e. organisationName
    f. organizational UnitName (OU)
    g. commonName (CN)
    h. E-Mail-Adresse
4. Klicken Sie auf **Neuen Schlüssel generieren.**
5. Überprüfen Sie im Popup-Fenster die bereitgestellten Informationen. (nach Wunsch ändern):
    antwort: Name
    b. Schlüsseltyp: RSA
    c. Keysieren: Bit 2048
    d. Klicken Sie auf Erstellen.
    e. Bestätigen Sie das Popup "RSA-Privater Schlüssel "Name" erfolgreich erstellt", indem Sie auf **OK** klicken.

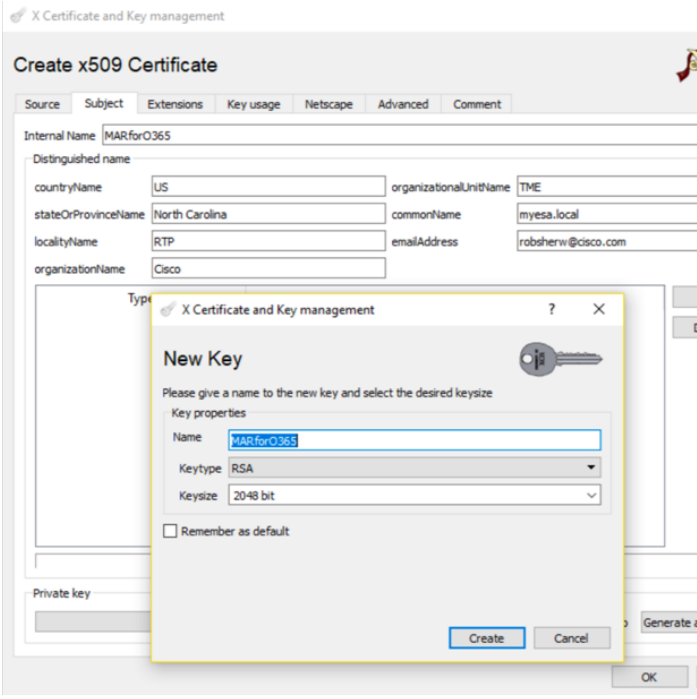

Abbildung 14: Verwenden von XCA (Schritte 3-5)

6. Klicken Sie auf die Registerkarte Schlüsselverwendung, und wählen Sie Folgendes aus:
    antwort: Unter Verwendung des X509v3-Schlüssels:
        Digitale Signatur, Schlüsselwahrnehmung
    b. Unter X509v3 Extended Key Usage:

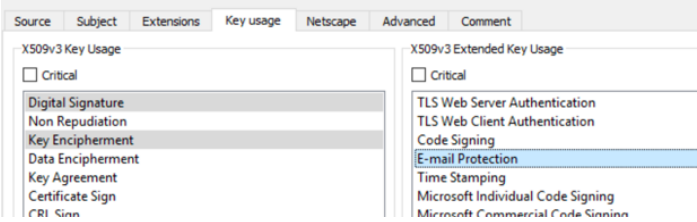

Abbildung 15: Verwenden von XCA (Schritt 6)

E-Mail-Schutz

7. Klicken Sie auf **OK**, um Änderungen am Zertifikat zu übernehmen.
8. Bestätigen Sie das Popup-Fenster "Erfolgreich erstelltes Zertifikat "*Name*", indem Sie auf **OK** klicken.

Als Nächstes exportieren Sie sowohl das **Public Certificate (CER-Datei)** als auch ***Certificate Private Key (PEM-Datei)*** zur Verwendung in den PowerShell-Befehlen und zur Verwendung in den Schritten Konfigurieren von Cisco Secure Email:

1. Klicken Sie auf und markieren Sie den internen Namen des neu erstellten Zertifikats.
2. Klicken Sie auf **Exportieren**
   antwort: Stellen Sie das Speicherverzeichnis ein, um den Zugriff zu vereinfachen (nach Wunsch ändern).
   b. Vergewissern Sie sich, dass das Exportformat auf **PEM (.crt)** festgelegt ist.
   c. Klicken Sie auf **OK**

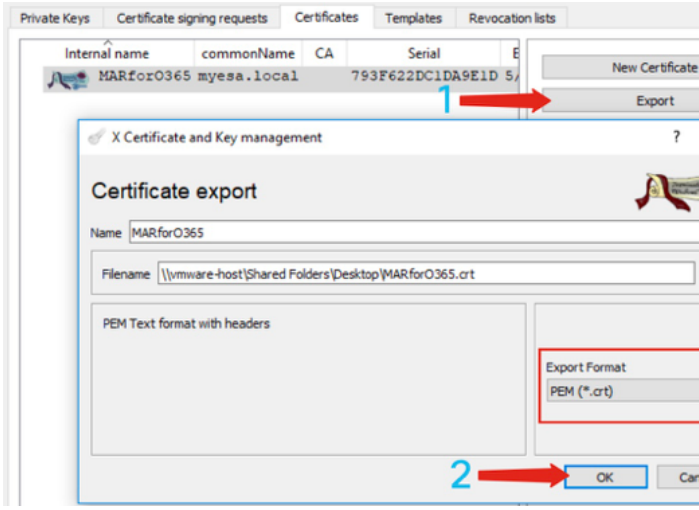

Abbildung 16: Verwenden von XCA (CRT exportieren)(Schritte 1-

3. Klicken Sie auf die Registerkarte **Privater Schlüssel**.
4. Klicken Sie auf und markieren Sie den internen Namen des neu erstellten Zertifikats.
5. Klicken Sie auf **Exportieren**
   antwort: Stellen Sie das Speicherverzeichnis ein, um den Zugriff zu vereinfachen (nach Wunsch ändern).
   b. Vergewissern Sie sich, dass das Exportformat auf **PEM private (PEM-Datei) (.pem) festgelegt** ist.
   c. Klicken Sie auf **OK**
6. Beenden und schließen Sie XCA

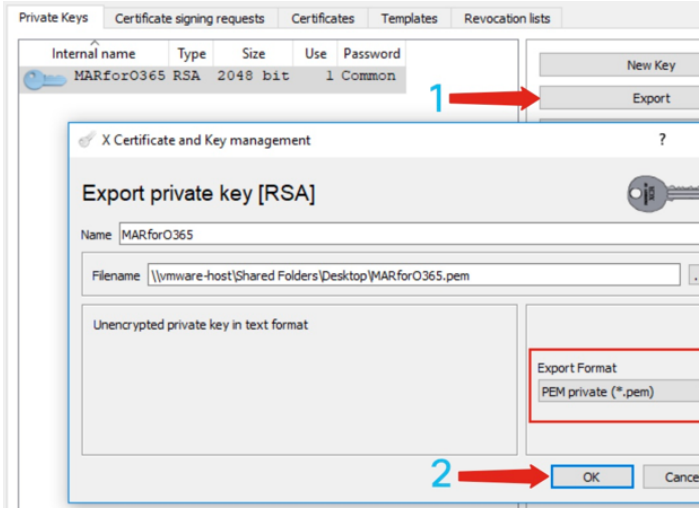

Abbildung 17: Verwenden von XCA (PEM exportieren) (Schritte 3

Schließlich nehmen Sie Ihr erstelltes Zertifikat und extrahieren den **Thumbprint**, der für die Konfiguration von Cisco Secure Email erforderlich ist.

1. Führen Sie unter Windows PowerShell Folgendes aus:

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import("c:\Users\joe\Desktop\myCert.crt")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)
$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)
$keyid = [System.Guid]::NewGuid().ToString()[Note: “c:\Users\joe\Desktop...” is the location on
your PC where your CRT file is saved.]
```

2. Um Werte für die nächsten Schritte abzurufen, in einer Datei speichern oder in die Zwischenablage kopieren zu können, gehen Sie wie folgt vor:

```
$base64Thumbprint | Out-File c:\Users\joe\Desktop\base64Thumbprint.txt
$base64Thumbprint
```

Anmerkung: “c:\Users\joe\Desktop..." ist der Speicherort auf Ihrem PC, an dem Sie die Ausgabe speichern.

Die erwartete Ausgabe beim Ausführen des PowerShell-Befehls sollte ähnlich wie folgt aussehen:

```
PS C:\Users\joe\Desktop> $base64Thumbprint
75fA1XJEJ4I1ZVFOB2xqkoCIh94=
```

Wie Sie sehen, ruft der PowerShell-Befehl den *base64Thumbprint auf*, den **Thumbprint**, der für die Konfiguration des Cisco Secure Email Gateways erforderlich ist.

Sie haben außerdem das **für die** Azure-App-Registrierung erforderliche **Public Certificate (CER-Datei)** erstellt. Außerdem haben Sie den ***Private Certificate Key (PEM-Datei)*** erstellt, den Sie im Abschnitt "Konfigurieren von Cisco Secure E-Mail" verwenden werden.

Sie haben die notwendigen Werte, um Ihre Anwendung in Microsoft Azure zu registrieren!

[Bitte fahren Sie mit "Eine Azure-App für die Verwendung mit Cisco Secure Email registrieren" fort.]

Anhang B

Hinweis: Dies ist NUR erforderlich, wenn Sie AsyncOS 11.x oder 12.x für E-Mail auf Ihrem

Gateway ausführen.

API-Berechtigungen (AsyncOS 11.x, 12.x)

Wählen Sie im Anwendungsbereich die Optionen Verwalten aus...

1. Wählen Sie **API-Berechtigungen aus**
2. Klicken Sie **+ Berechtigungen hinzufügen**
3. Blättern Sie nach unten zu **Unterstützte Legacy-APIs** und wählen Sie **Exchange**
4. Wählen Sie die folgenden Berechtigungen für delegierte Berechtigungen aus: EWS > "EWS.AccessAsUser.All" (greifen Sie als angemeldeter Benutzer über Exchange-Webdienste auf Mailboxen zu.)Mail > "Mail.Read" (Benutzermail lesen)Mail > "Mail.ReadWrite" (Lesen und Schreiben von Benutzermail)Mail > "Mail.Send" (Mail als Benutzer senden)
5. Navigieren Sie zum oberen Ende des Teilfensters...
6. Wählen Sie die folgenden Berechtigungen für Anwendungsberechtigungen aus: "full_access_as_app" (Exchange-Webdienste mit uneingeschränktem Zugriff auf alle Mailboxen verwenden)Mail > "Mail.Read" (Benutzermail lesen)Mail > "Mail.ReadWrite" (Lesen und Schreiben von Benutzermail)Mail > "Mail.Send" (Mail als Benutzer senden)
7. *Optional:* Sie sehen, dass Microsoft Graph standardmäßig für "User.Read"-Berechtigungen aktiviert ist. Sie können dies als konfiguriert lassen, oder klicken Sie auf **Lesen** und dann auf **Berechtigung entfernen,** um diese aus den API-Berechtigungen zu entfernen, die der Anwendung zugeordnet sind.
8. Klicken Sie auf **Berechtigungen hinzufügen** (oder **Berechtigungen aktualisieren**, wenn Microsoft Graph bereits aufgeführt wurde).
9. Klicken Sie abschließend auf **"Administratorgenehmigung gewähren" für..** um sicherzustellen, dass die neuen Berechtigungen auf die Anwendung angewendet werden
10. In einem Popup-Fenster werden folgende Fragen gestellt:
    "*Möchten Sie die Genehmigung der beantragten Berechtigungen für alle Konten in <Azure Name> erteilen? Dadurch werden alle vorhandenen Datensätze für die Administratorgenehmigung aktualisiert, die diese Anwendung bereits mit den unten aufgeführten Datensätzen abgleichen muss.*"

    Klicken Sie auf **Ja.**

An diesem Punkt sollten Sie eine grüne Erfolgsmeldung sehen, und die Spalte "Admin Consent Required" (Zustimmung erforderlich) wird ähnlich der folgenden angezeigt:

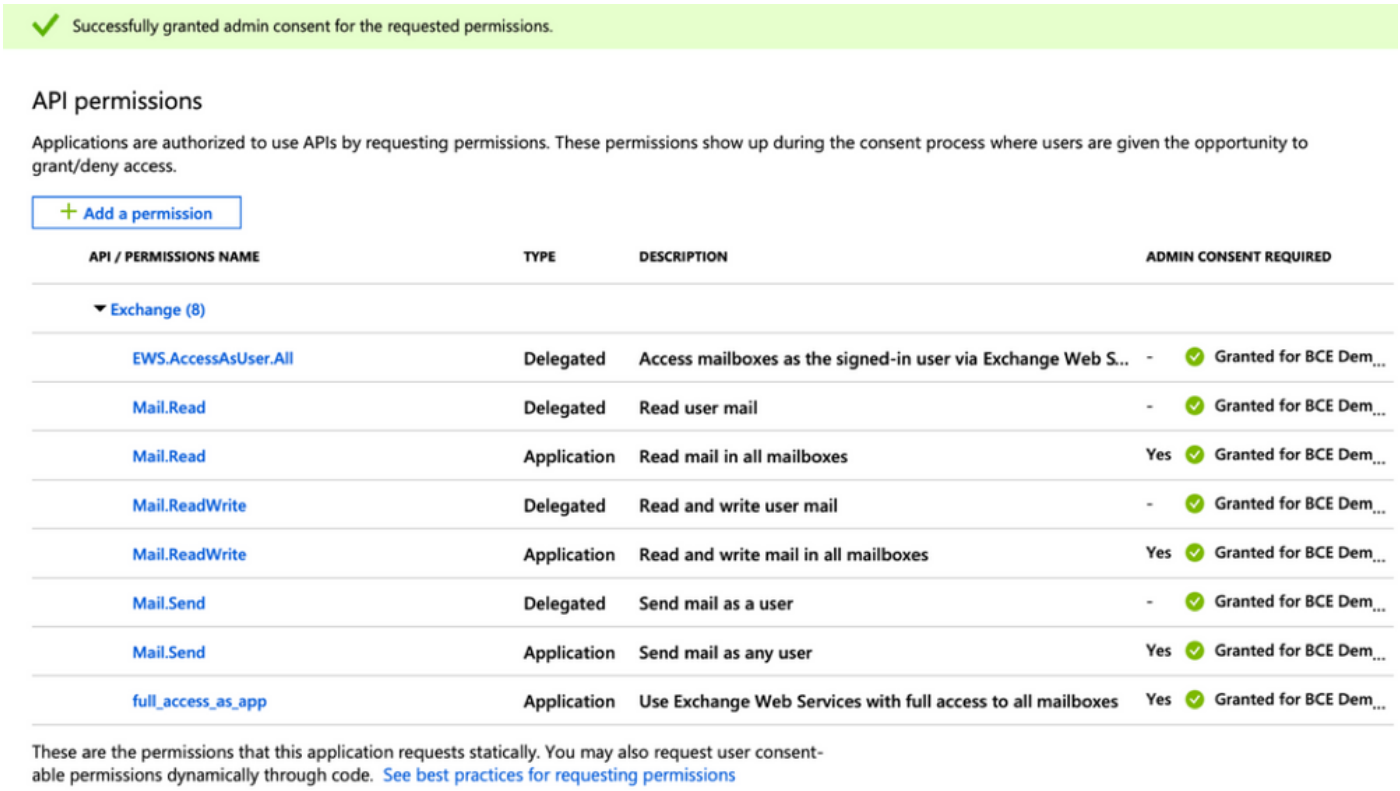

Abbildung 18: Microsoft Azure-App-Registrierung (API-Berechtigungen erforderlich)

[Bitte fahren Sie mit "Eine Azure-App für die Verwendung mit Cisco Secure Email registrieren" fort.]

Zugehörige Informationen

- Cisco Email Security Appliance - Produktsupport
- Cisco Email Security Appliance - Versionshinweise
- Cisco Email Security Appliance - Endbenutzeranleitung