Hoe moet u Cisco Secure Email Account Settings voor Microsoft Messenger (Microsoft 365) API configureren

Inhoud

Inleiding
Stroom van automatische correctie van postbus
Voorwaarden
Registreer een app voor gebruik met Cisco Secure Email
Toepassingsregistratie
Certificaten en geheimen
API-toegangsrechten
Uw client-id verkrijgen
Uw Cisco beveiligde e-mailgateway/cloudgateway configureren
Accountprofiel maken
Controleer de verbinding
Auto Remediation (MAR) van postbus inschakelen voor geavanceerde Malware Protection in Mail Policy
Auto-revitatie van postvakjes (MAR) inschakelen voor URL-filtering
Voorbeelden van Auto Remediation van postbus
Vastlegging postbus voor automatische revisie
Probleemoplossing voor Cisco Secure E-gateway
Probleemoplossing:
Bijlage A
Bouwen aan een openbaar en particulier certificaat en een sleutelpark
Certificaat: Unix/Linux (met openssl)
Certificaat: Windows (met PowerShell)
Bijlage B
API-toegangsrechten (AsyncOS 11.x, 12.x)
Gerelateerde informatie

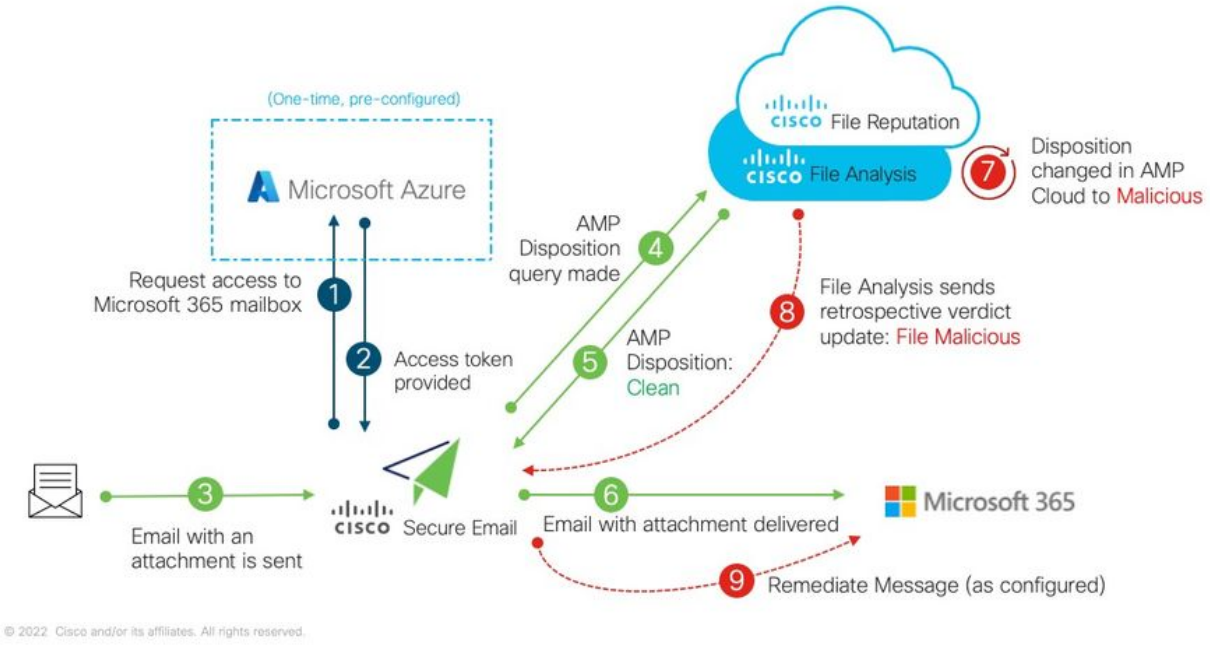
Inleiding

Dit document biedt een stap-voor-stap "Hoe-kan-ik" voor het registreren van een nieuwe toepassing in Microsoft Messenger (actieve map) voor het genereren van de benodigde client-ID, Tant-ID en clientreferenties, en vervolgens de configuratie voor accountinstellingen op een Cisco beveiligde e-mailgateway of cloudgateway. Configuratie van de accountinstellingen en het bijbehorende accountprofiel is vereist wanneer een e-mailbeheerder Auto Remediation (MAR) configureren voor Advanced Malware Protection (AMP) of URL-filtering of de korte actie vanuit Message Tracking gebruiken op Cisco Secure Email Manager of Cisco Secure Gateway/Cloud Gateway.

Stroom van automatische correctie van postbus

Een bijlage (bestand) in uw e-mail of een URL kan op elk moment als kwaadaardig worden gescand, zelfs nadat deze de brievenbus van een gebruiker heeft bereikt. AMP op Cisco Secure Email (via Cisco Secure Malware Analytics) kan deze ontwikkeling identificeren wanneer er nieuwe informatie verschijnt en zal retrospectieve waarschuwingen naar Cisco Secure Email doen. Cisco Talos biedt hetzelfde met URL-analyse, zoals van AsyncOS 14.2 voor Cisco Secure Email Cloud Gateway. Als uw organisatie Microsoft 365 gebruikt om mailboxen te beheren, kunt u Cisco Secure E-mail configureren om auto-corrigerende acties uit te voeren op de berichten in een gebruikershandleiding wanneer deze bedreigingsoordelen wijzigen.

Cisco Secure E-mail communiceert veilig en rechtstreeks naar Microsoft Outlook Active Directory om toegang te krijgen tot Microsoft 365-postboxen. Als een e-mail met een bijlage bijvoorbeeld via uw gateway wordt verwerkt en door AMP wordt gescand, wordt de bestandsbijlage (SHA256) aan AMP geleverd voor bestands reputatie. De AMP-indeling kan worden gemarkeerd als Schoonmaken (stap 5, afbeelding 1) en vervolgens worden geleverd aan de Microsoft 365-postvak van de eindontvanger. Op een later tijdstip wordt de AMP dispositie veranderd in Malicious, Cisco Malware Analytics stuurt een retrospectieve versie van het vonnis (stap 8, afbeelding 1) naar *elke* poort die die specifieke SHA256 heeft verwerkt. Zodra de poort de update van het retrospectieve oordeel van Malicious (indien geconfigureerd) ontvangt, zal de poort dan een van de volgende handelingen van de postbox Auto Remediation (MAR) uitvoeren: Doorsturen, verwijderen of doorsturen en verwijderen.



Afbeelding 1: MAR (voor AMP) op Cisco beveiligde e-mail

Deze gids is op hoe te om Cisco Secure Email met Microsoft 365 te configureren voor alleen postvakautomatisering. AMP (File Reputation and File Analysis) en/of URL Filtering op de gateway zou al ingesteld moeten worden. Raadpleeg de Gebruikershandleiding voor meer informatie over Bestandsreputatie en Bestandsanalyse voor de versie van AsyncOS die u hebt ingezet.

Voorwaarden

1. Microsoft 365-accountabonnement (Zorg ervoor dat uw Microsoft 365-accountabonnement toegang tot Exchange bevat, zoals een Enterprise E3- of Enterprise E5-account.)

2. Microsoft karwei-administratorrekening en toegang tot http://portal.azure.com

3. Zowel de Microsoft 365- als de Microsoft karwei-account zijn correct gekoppeld aan een actief "user@domain.com" e-mailadres en je kunt e-mails versturen en ontvangen via dat e-mailadres.

U maakt de volgende waarden om de Cisco Secure Email Gateway API-communicatie naar Microsoft Messenger AD te configureren:

- **Clientid**
- **AanbiedingsID**
- **Clientgeheim**

  Opmerking: Om te beginnen met AsyncOS 14.0, kunnen **rekeninginstellingen** configuratie toestaan met behulp van een clientgeheim wanneer u de Microsoft karwei App Registration maakt. Dit is de gemakkelijkere en voorkeursmethode.

Optioneel - Als u het clientgeheim NIET gebruikt, moet u:

- **Thumbprint**
- **De privé-toets (PEM-bestand)**

Het maken van de thumbnail- en privé-toets wordt behandeld in het aanhangsel van deze handleiding:

1. Een actief openbaar (of privé) certificaat (CER) en de privé sleutel die wordt gebruikt om het certificaat te ondertekenen (PEM), of de mogelijkheid om een openbaar certificaat (CER) te maken en de mogelijkheid om de privé sleutel op te slaan die wordt gebruikt om het certificaat te ondertekenen (PEM). Cisco biedt twee methoden in dit document om dit op basis van uw beheervoorkeur te doen: Certificaat: Unix/Linux/OS X (met OpenSSL)Certificaat: Windows (met PowerShell)

2. Toegang tot Windows PowerShell, gewoonlijk toegediend vanaf een Windows Host of Server-of-toegang tot terminaltoepassing via Unix/Linux

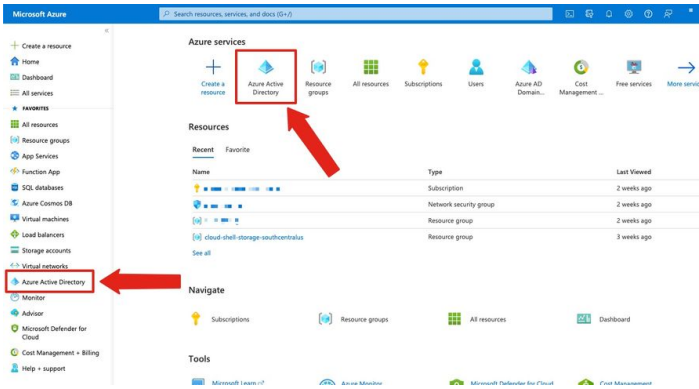
Om deze vereiste waarden te kunnen bouwen, moet u de stappen in dit document voltooien.

Registreer een app voor gebruik met Cisco Secure Email

Toepassingsregistratie

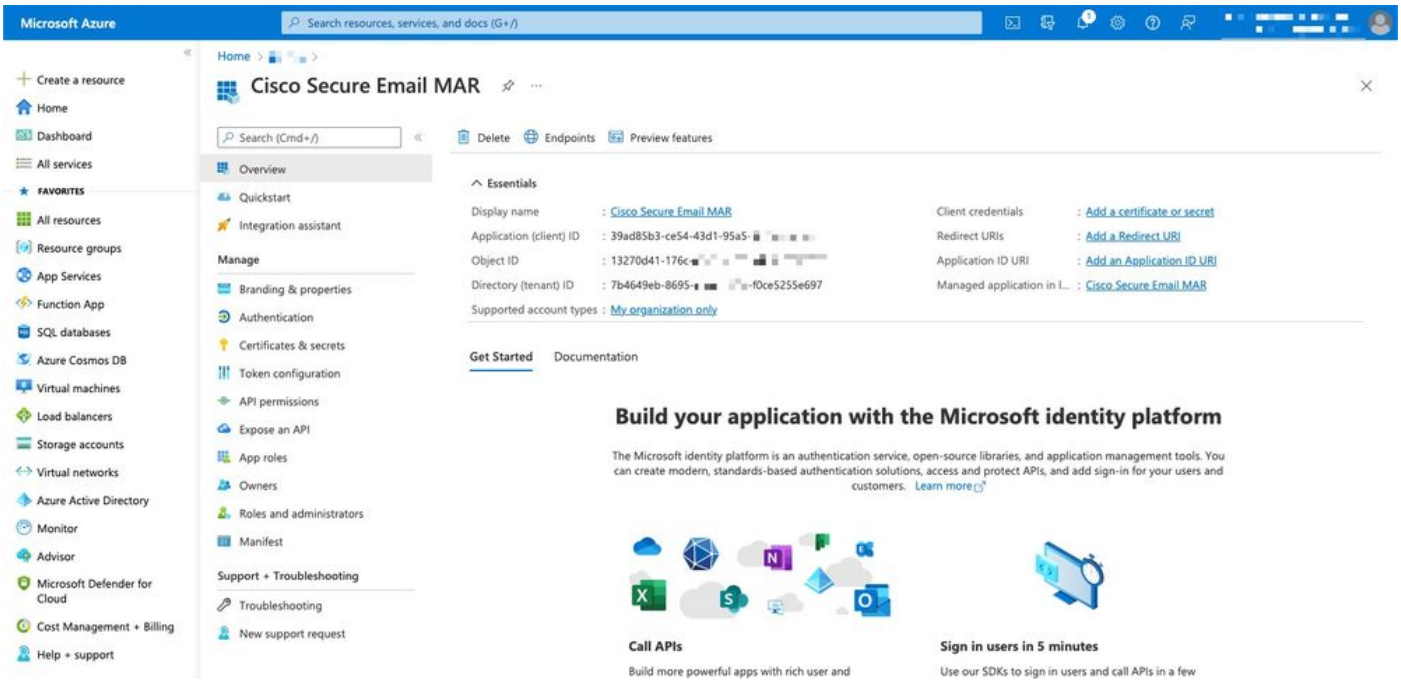
Aanmelden bij uw Microsoft Outlook-portal
1. Klik op **actieve map** in de **tijd** (afbeelding 2)

2. Klik op **App-registraties**
3. Klik op **+ nieuwe registratie**
4. Op de pagina "Een aanvraag registreren":
    a. Naam: **Cisco Secure Email MAR** (of de naam van uw keuze)
    b. Ondersteunde rekeningtypen: **alleen rekeningen in deze organisatiefolder (accountnaam)**
    c. Redirect URI: (Optioneel)
    [Opmerking: U kunt dit leeg laten of zich vrij voelen om https://www.cisco.com/sign-on te gebruiken voor invullen.]
    d. Klik onder op de pagina op **Registreren**



Afbeelding 2: Microsoft karwei Portal

Na voltooiing van de bovengenoemde stappen zult u uw aanvraag indienen:



Afbeelding 3: Microsoft Laura's Active Directory-toepassingspagina

Certificaten en geheimen

Als u AsyncOS 14.0 of nieuwer gebruikt, adviseert Cisco om uw buren app te configureren om een clientgeheim te gebruiken. In uw toepassingsvenster kunt u in de opties beheren:

1. Selecteer **Certificaten en geheimen**

2. In het gedeelte ***Clientgeheimen*** klikt u op **+ Nieuw clientgeheim**

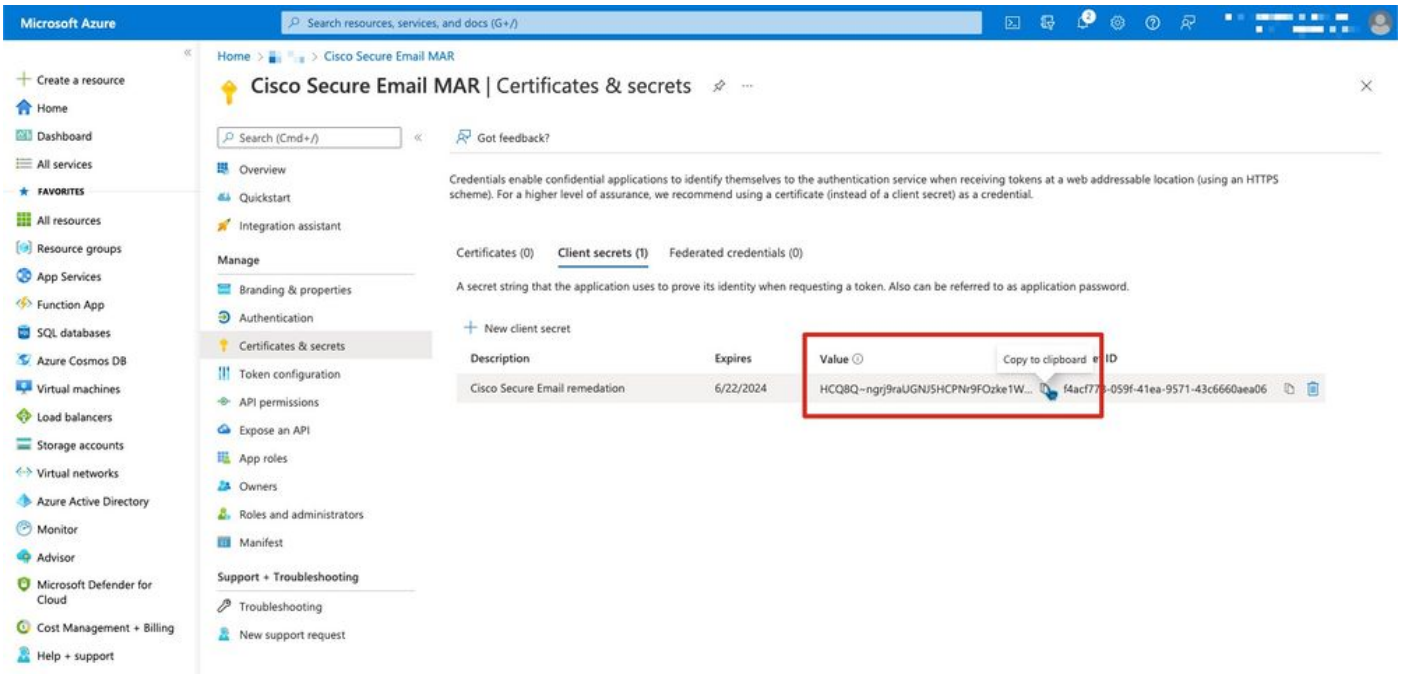
3. Voeg een beschrijving toe om te helpen identificeren waar dit clientgeheim voor is, bijvoorbeeld "Cisco beveiligde e-mailherstel"

4. Selecteer een verloopperiode

5. Klik op **Toevoegen**

6. Klik rechts van de waarde op het pictogram **Kopie naar klembord** en klik op het pictogram

7. Sla deze waarde op in de opmerkingen en let daarbij op als "Clientgeheim"



Afbeelding 4: Microsoft karwei creëert een cliënt geheim voorbeeld

> **Opmerking:** Als je je actieve Microsoft karwei sessie verlaat, zal de waarde van het clientgeheim dat je net gegenereerd hebt, de waarde *** weghalen. Als u de waarde niet registreert en beschermt voordat deze eindigt, moet u het clientgeheim opnieuw maken om de duidelijke tekstuitvoer te zien.

Optioneel - Als u uw lokale toepassing niet met een clientgeheim configureren, dient u uw eigen app te configureren om uw certificaat te gebruiken. In uw toepassingsvenster kunt u in de opties beheren:

1. Selecteer **Certificaten en geheimen**
2. Klik op **Uploadcertificaat**
3. Selecteer het CRT-bestand (zoals eerder gemaakt)
4. Klik op **Toevoegen**

API-toegangsrechten

Opmerking: Met ingang van AsyncOS 13.0 voor e-mailbeveiliging, zijn de API-toegangsrechten voor Microsoft landbouw expliciet aan Cisco Secure Email Communication vereist veranderd van het gebruik van Microsoft Exchange in Microsoft Graph. Als u al MAR hebt ingesteld en u uw

bestaande Cisco Secure Email Gateway naar AsyncOS 13.0 opwaart, kunt u simpelweg de nieuwe API-toegangsrechten bijwerken of toevoegen. (Als u een oudere versie van AsyncOS, 11.x of 12.x draait, raadpleeg dan Bijlage B voordat u doorgaat.)

In uw toepassingsvenster kunt u in de opties beheren:

1. Selecteer **API-toegangsrechten**
2. Klik op **+ Voeg een toestemming toe**
3. Microsoft **Graph** selecteren
4. Selecteer de volgende rechten op ***toepassingsrechten***: Mail > "Mail.Read" (Lezen in alle postvakjes)Mail > "Mail.ReadWrite" (Lezen en schrijven in alle postvakjes)Mail > "Mail.Verzend" (Verzend mail als elke gebruiker)Map > "Directory.Read.All" (Read folder data) [*Optioneel: Schakel deze optie in als u LDAP-connector/LDAP-synchronisatie gebruikt. Zo niet, dan is dit niet vereist.]
5. *Optioneel:* U zult zien dat Microsoft Graph per default is ingeschakeld voor de "User.Read"-rechten; U kunt dit als ingesteld achterlaten of op **Lezen** klikken en op **Verwijderen met toestemming** klikken om dit uit uw API-rechten te verwijderen die aan uw toepassing zijn gekoppeld.
6. Klik op **Add permissies** (of **Update permissies**, als Microsoft Graph al in de lijst stond)
7. Klik tot slot op **Grant Admin toestemming voor...** om er zeker van te zijn dat uw nieuwe toestemming op de toepassing wordt toegepast
8. Er verschijnt een pop-up in het deelvenster met de volgende vragen:
   "*Wilt u toestemming geven voor de gevraagde toestemming voor alle rekeningen in <burernaam>? Dit vult elke bestaande admin-toestemming bij die deze toepassing al moet aanpassen aan wat hieronder is weergegeven.*"

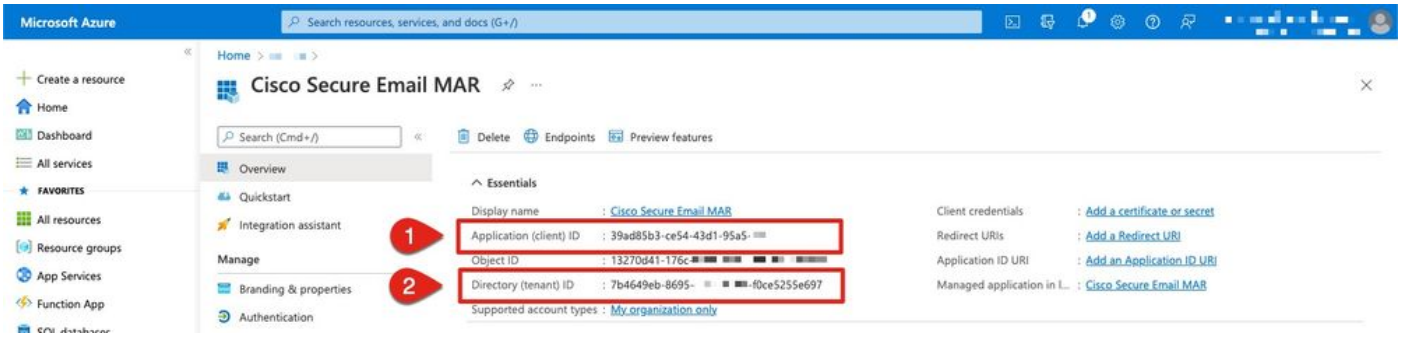
   Klik op **Ja**

Op dit punt, zou u een groen succesbericht moeten zien en het "Admin Consent" zuinigoed display Granted.

Uw client-id verkrijgen

In uw toepassingsvenster kunt u in de opties beheren:

1. Klik op **Overzicht**
2. Klik met de muis rechts van uw applicatie (client) en klik op het pictogram **Kopie naar klembord**
3. Sla deze waarde in de opmerkingen op als een "client-ID"
4. Klik rechts van uw directory (huurder) ID en klik op het pictogram **Kopie naar klembord**
5. Sla deze waarde in de opmerkingen op als een "Tanner-ID"



Afbeelding 5: Microsoft karwei... Bijvoorbeeld client-ID, huurID

Uw Cisco beveiligde e-mailgateway/cloudgateway configureren

Nu dient u de volgende waarden te hebben voorbereid en opgeslagen in uw opmerkingen:

- **Clientid**
- **AanbiedingsID**
- **Clientgeheim**

Optioneel: als u geen clientgeheim gebruikt:

- **Thumbprint**
- **De privé-toets (PEM-bestand)**

U bent klaar om de gedefinieerde waarden uit uw opmerkingen te gebruiken en de accountinstellingen te configureren in de Cisco Secure Email Gateway.

Accountprofiel maken

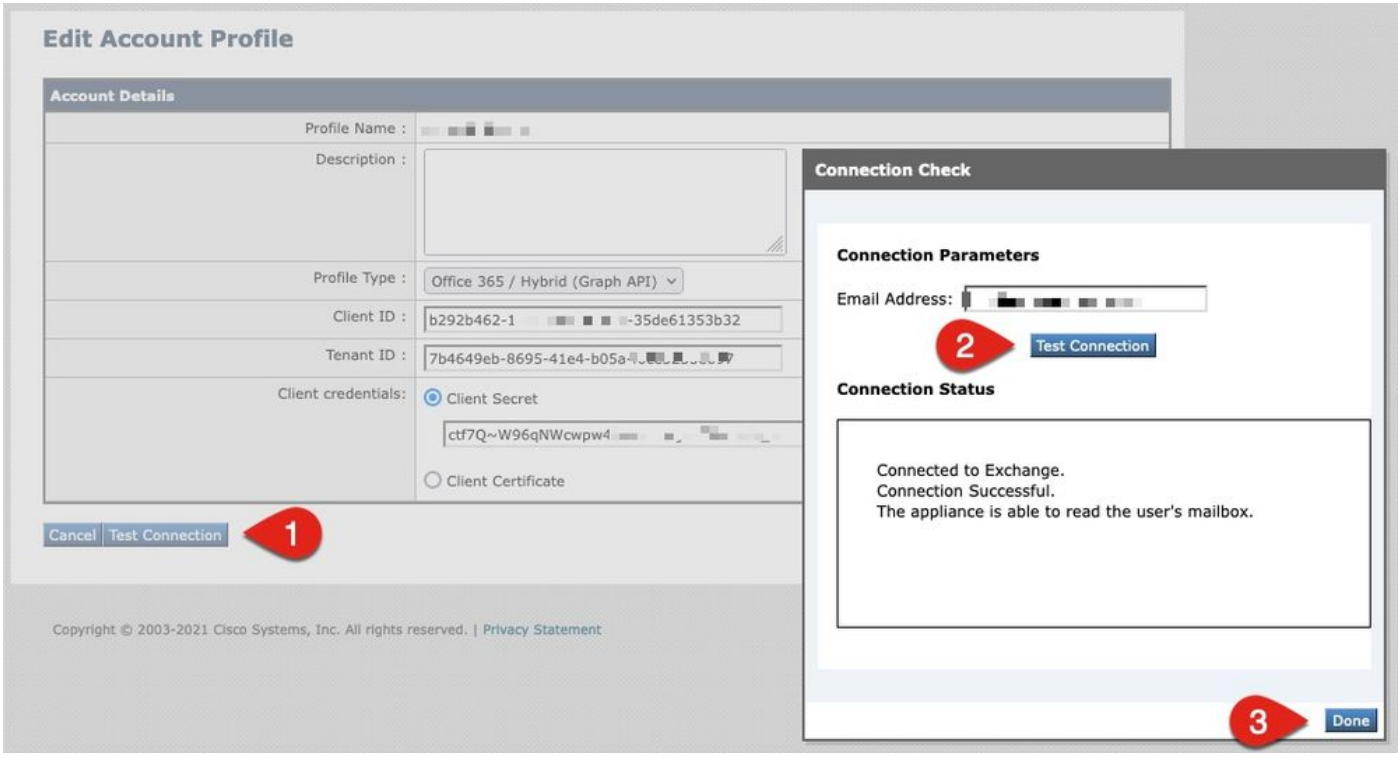
1. Inloggen op uw poort
2. Navigeren in naar **systeembeheer > accountinstellingen** Opmerking: Als u een versie uitvoert vóór AsyncOS 13.x, zal dit **Systeembeheer > Instellingen postvak** zijn
3. Klik op **Inschakelen**
4. Klik op het aanvinkvakje voor Account-instellingen inschakelen en klik op **Indienen**
5. Klik op **Accountprofiel maken**
6. Geef een profielnaam en beschrijving (iets dat uw account uniek zal beschrijven als u meerdere domeinen hebt)
7. Aangezien u een Microsoft 365-verbinding definieert, laat u het profieltype als **Office 365/Hybrid (Graph API) achter**
8. Voer uw **client-id in**
9. Voer uw **huurders-id in**
10. Voor Clientreferenties een van de volgende dingen doen, zoals u in Kuurtijd hebt ingesteld: Klik op **Clientgeheim** en plakken in het geconfigureerde clientgeheim, of...Klik op **Clientcertificaat** en voer uw Thumbprint in en specificeer ook uw PEM door op "Kies

bestand" te klikken
11. Klik op **Submit (Verzenden)**
12. Klik op **Commit Veranderingen** in de rechterbovenhoek van de UI
13. Voer opmerkingen in en vul de configuratiewijzigingen in door op **Commit Changes** te klikken

Controleer de verbinding

De volgende stap is alleen om de API-verbinding te controleren van uw Cisco Secure Email Gateway naar Microsoft Outlook:

1. Klik vanuit dezelfde pagina met accountdetails op **Test Connection**
2. Voer een geldig e-mailadres in voor het domein dat in uw Microsoft 365-account wordt beheerd
3. Klik op **Test Connection**
4. U dient een succesbericht te ontvangen (afbeelding 6)
5. Klik op **Gereed** om te voltooien



Afbeelding 6: Controleer accountprofiel/verbindingsvoorbeeld

6. Klik in het gedeelte *Domain mapping* op **Domain mapping**

7. Voer in uw domeinnaam(en) in die aan de Microsoft 365-account zijn gekoppeld, u hebt zojuist de API-verbinding gevalideerd voor

Het volgende is een lijst van geldige domeinformaten die kunnen worden gebruikt om een profiel van de Brievenbus in kaart te brengen:

- Het domein kan het speciale sleutelwoord "ALL" zijn om alle domeinen aan te passen om een standaard domein mapping te maken.

- Domeinnamen zoals 'voorbeeld.com' - Overeenkomst elk adres met dit domein.

- Partiële domeinnamen zoals '@.partiële.voorbeeld.com' - Overeenkomsten met elk adres dat eindigt met dit domein

- Meervoudige domeinen kunnen worden ingevoerd door gebruik te maken van een komma-gescheiden lijst met domeinen.

8. Klik op **Indienen**

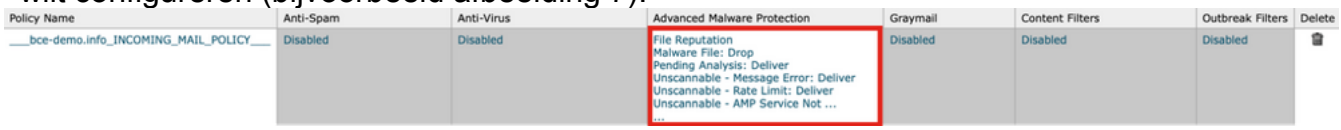
9. Klik op **Commit Veranderingen** in de rechterbovenhoek van de UI

10. Voer in een willekeurige opmerking opmerkingen in en vul de configuratiewijzigingen in door op **Commit Changes** te klikken

Auto Remediation (MAR) van postbus inschakelen voor geavanceerde Malware Protection in Mail Policy

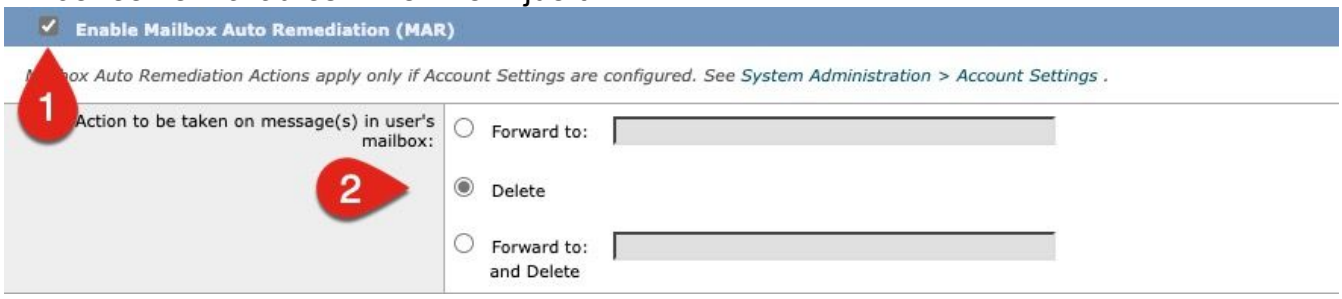
Voltooi deze stap om MAR in de configuratie van het AMP voor het postbeleid in te schakelen.

1. Navigeren in op **e-mailbeleid > Inkomend postbeleid**
2. Klik op de instellingen in de kolom Advanced Malware Protection voor de beleidsnaam die u wilt configureren (bijvoorbeeld afbeelding 7):



Afbeelding 7: MAR (inkomend postbeleid) inschakelen

3. Naar de onderkant van de pagina bladeren
4. Klik op het selectieteken voor automatische revisie van postbus inschakelen (MAR)
5. Selecteer een van de volgende acties die u voor de MAR wilt uitvoeren (bijvoorbeeld afbeelding 8): Verzenden naar: <*Voer een e-mailadres in*>VerwijderenVerzenden naar: <*voer een e-mailadres in*> en Verwijdert



Afbeelding 8: MAR-configuratiemodel voor AMP inschakelen

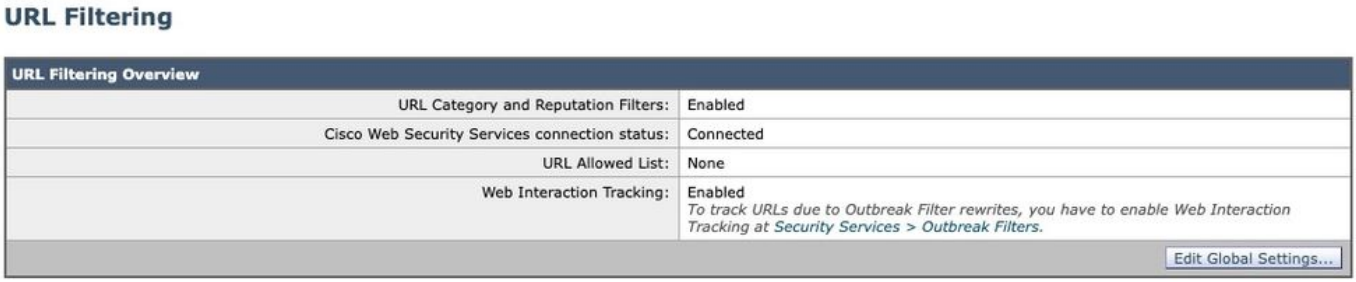
6. Klik op **Submit (Verzenden)**
7. Klik op **Commit Veranderingen** in de rechterbovenhoek van de UI
8. Voer opmerkingen in en vul de configuratiewijzigingen in door op **Commit Changes** te klikken

Auto-revitatie van postvakjes (MAR) inschakelen voor URL-filtering

Vanaf AsyncOS 14.2 voor Cisco Secure Email Cloud Gateway bevat URL-filtering nu URL met retrospectieve herziening en URL-correctie.

1. Navigeren in naar **security services > URL-filtering**
2. Als u nog geen URL-filtering hebt ingesteld, klikt u op **Inschakelen**
3. Klik op het selectieteken voor "URL-categorie en -herstellingfilters inschakelen"
4. De *geavanceerde instellingen* met de standaardinstellingen
5. Klik op Submit (Verzenden)

Uw URL-filtering moet op de volgende manieren vergelijkbaar zijn:



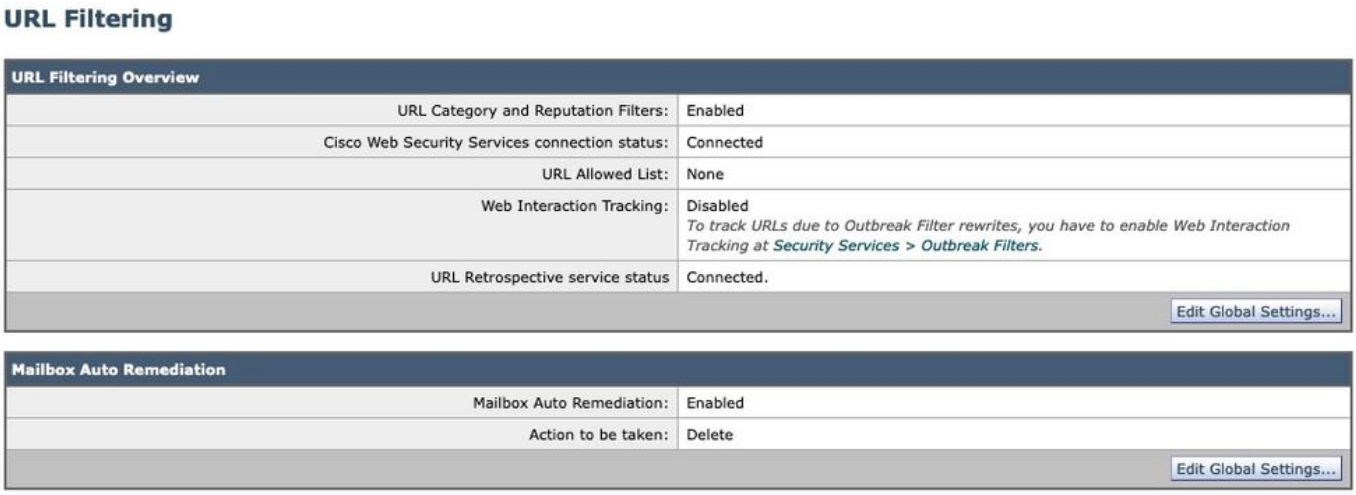
Afbeelding 9: URL-filtering van post-enabled-voorbeeld

Als u URL Retrospectie met URL-filtering wilt zien, voert u het volgende uit of hebt u een ondersteuningscase geopend voor Cisco om dit uit te voeren:

```
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
```

Nadat u dit hebt voltooid, verfrist u uw UI op de URL-filtering en u wilt nu een soortgelijke bewerking zien als de volgende:



Afbeelding 10: URL-filtering (AsyncOS 14.2 voor Cisco beveiligde e-mail cloudgateway)

URL protection is nu gereed om corrigerende maatregelen uit te voeren wanneer een vonnis de score verandert. Zie Bescherming tegen kwaadaardige of ongewenste URL's voor meer informatie in de gebruikersgids voor AsyncOS 14.2 voor Cisco Secure Email Cloud Gateway.

Configuratie voltooid.

Op dit moment is Cisco Secure Email klaar om opkomende bedreigingen voortdurend te evalueren wanneer nieuwe informatie beschikbaar wordt en u op de hoogte te stellen van

bestanden die bedreigd worden nadat ze uw netwerk zijn ingevoerd.

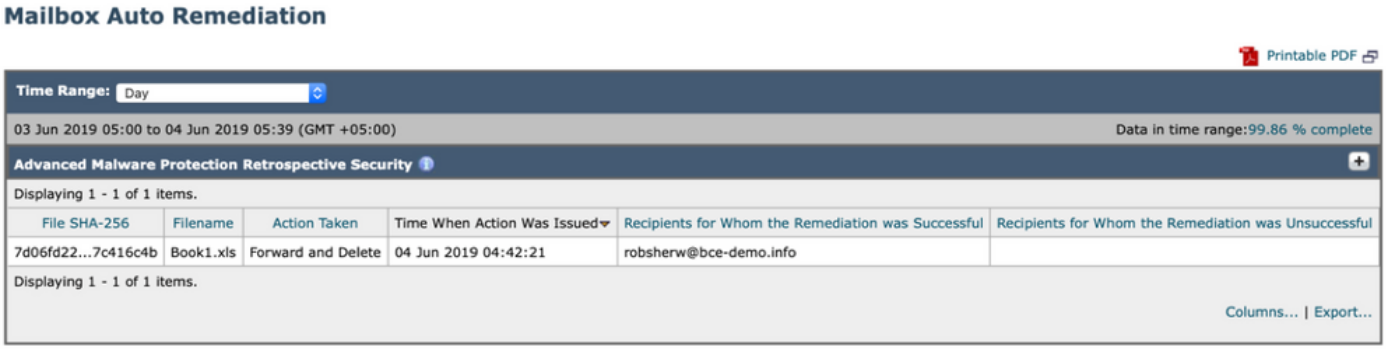
Wanneer een retrospectief oordeel uit Bestandsanalyse (Cisco Secure Malware Analytics) wordt geproduceerd, wordt een info-bericht naar de E-mailsecurity beheerder (indien geconfigureerd) verzonden. Voorbeeld:

```
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             : [redacted]
   To               : [redacted]
   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[redacted]
Timestamp: 04 Jun 2019 04:40:36 +0500
```

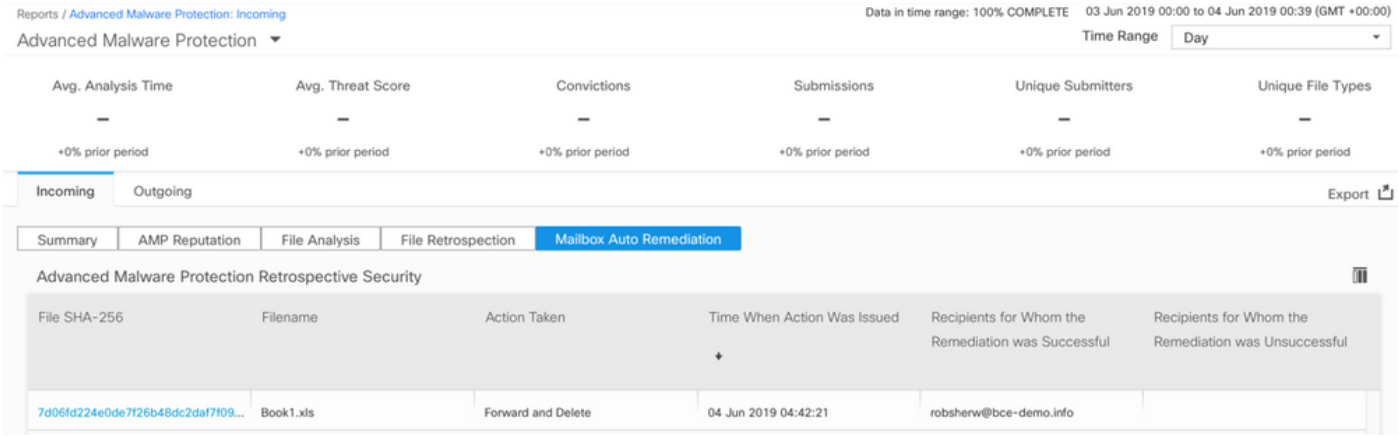
Auto-revisie van de postbus wordt zo ingesteld als wordt geconfigureerd voor het postbeleid.

Voorbeelden van Auto Remediation van postbus

Rapportage van elke SHA256 die is bijgewerkt, vindt plaats in het Auto Remediation-rapport van de postbus dat beschikbaar is in zowel de Cisco Secure Email Gateway als Cisco Secure Email Manager en Web Manager.



Afbeelding 11: (Legacy UI) rapport over automatische correctie van postbus



Afbeelding 12: (NG UI) rapport over automatische correctie van postbus

Vastlegging postbus voor automatische revisie

Auto Remediation van de postbus heeft een individueel logboek, "mar". De logs van de Auto Remediation van de brievenbus zullen alle communicatieactiviteit tussen uw Cisco Secure Email Gateway en Microsoft karwei, Microsoft 365 bevatten.

Een voorbeeld van de mar logt:

```
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.
```

Probleemoplossing voor Cisco Secure E-gateway

Als de resultaten voor de connectiviteitsstatus test niet succesvol zijn, kunt u de registratie van de applicatie die vanuit Microsoft karwei AD is uitgevoerd, bekijken.

Stel uw MAR-logbestanden vanuit Cisco Secure Email Gateway in op het 'overtrekken'-niveau en test de verbinding opnieuw.

Voor onsuccesvolle verbindingen kunnen logboeken vergelijkbaar zijn met:

```
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
```

Bevestig de Application ID, Directory ID (hetzelfde als de Tenant ID) of andere bijbehorende identificatiecodes uit het logbestand met uw toepassing in de Koude AD. Als u niet zeker weet wat de waarden zijn, verwijder de toepassing dan van de Klantenservice en begin opnieuw.

Voor een goede verbinding zouden logbestanden vergelijkbaar moeten zijn met:

```
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.
```

Probleemoplossing:

> **Opmerking**: Cisco TAC en Cisco Support hebben geen recht op problemen aan de klant-kant van probleemoplossing met Microsoft Exchange, Microsoft Messenger AD of Office 365.

Voor klantzijdeproblemen met Microsoft Outlook AD moet u Microsoft Support inschakelen. Zie de

optie "Help + ondersteuning" van uw Microsoft karton. U kunt mogelijk rechtstreeks ondersteuningsverzoeken vanuit het dashboard openen voor Microsoft Support.

Bijlage A

Opmerking: dit is ALLEEN vereist als u het clientgeheim NIET gebruikt voor het opzetten van uw eigen applicatie.

Bouwen aan een openbaar en particulier certificaat en een sleutelpark

Tip: Laat de uitvoer lokaal opgeslagen zijn voor *$base64Value*, *$base64Thumbprint* en *$keyid*, zoals ze later in de configuratiestappen vereist zullen zijn. Zorg dat u de .crt en de bijbehorende .pem van het certificaat in een beschikbare, lokale map op uw computer hebt.

Opmerking: Als u al een certificaat (x509-indeling/standaard) en een privétoets hebt, slaat u deze sectie over. Verzeker u ervan dat u zowel CRT- als PEM-bestanden hebt, aangezien u ze in de volgende secties nodig hebt!

Certificaat: Unix/Linux (met openssl)

Te creëren waarden:

- **Thumbprint**
- **Openbaar certificaat (CRT-bestand)**
- **Private Key (PEM-bestand)**

Administrateurs die Unix/Linux/OS X gebruiken, voor het doel en de uitvoering van het meegeleverde script, zijn ervan uitgegaan dat u OpenSSL geïnstalleerd hebt.

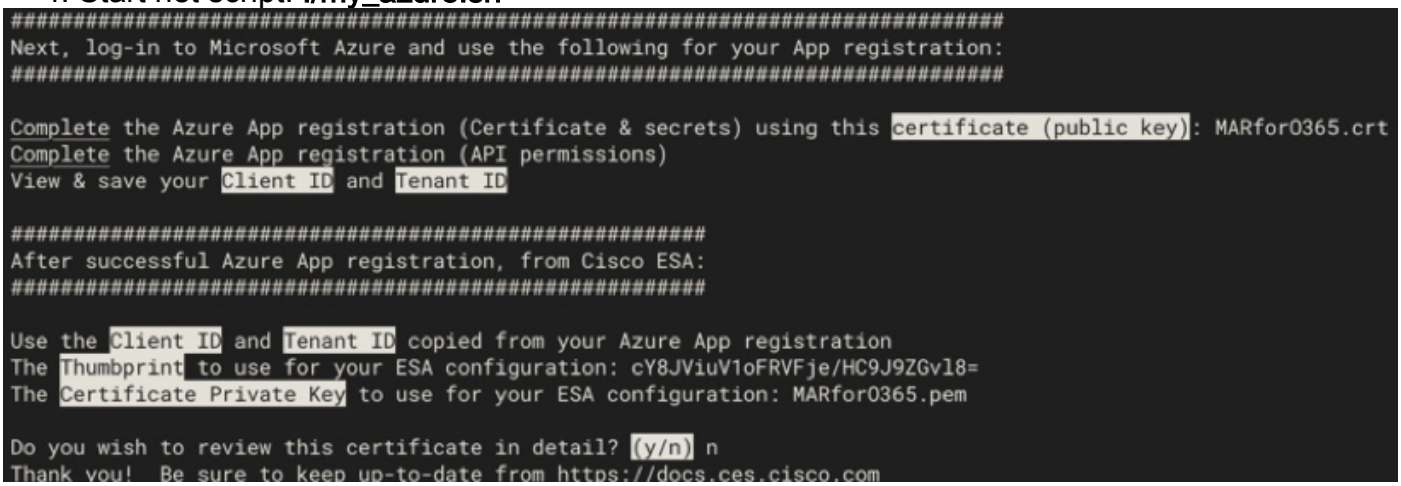
Opmerking: Start de opdrachten 'welke openssl' en 'openssl versie' om de installatie van OpenSSL te controleren. Installeer OpenSSL als deze niet aanwezig is!

Zie het volgende document voor assistentie: KRKER AD Configuration Script voor Cisco Secure E-mail

Van uw host (UNIX/Linux/OS X):

1. Vanaf een eindtoepassing, teksteditor (of hoe u het ook leuk vindt om een shell script te maken), maakt een script door het volgende te kopiëren: https://raw.githubusercontent.com/robsherw/my_azure/master/my_azure.sh

2. Het script plakken
3. Zorg ervoor dat je het script uitvoerbaar maakt. Start de volgende opdracht: **chmod u+x my_azure.sh**
4. Start het script: **./my_azure.sh**



Afbeelding 13: schermuitvoer van my_azure.sh

Zoals u in Afbeelding 2 ziet, bouwt het script en roept het **Public Certificate (CER-bestand)** uit dat nodig is voor de Appregistratie. Het script roept ook de ***Thumbprint*** en ***certificaatparticuliere sleutel (PEM-bestand)*** u gebruikt in het gedeelte Cisco Secure E-mail configureren.

U heeft de benodigde waarden om onze aanvraag in Microsoft Messenger te registreren!

[Naar de volgende sectie! Ga verder naar "Registreer een app voor gebruik met Cisco Secure Email"

Certificaat: Windows (met PowerShell)

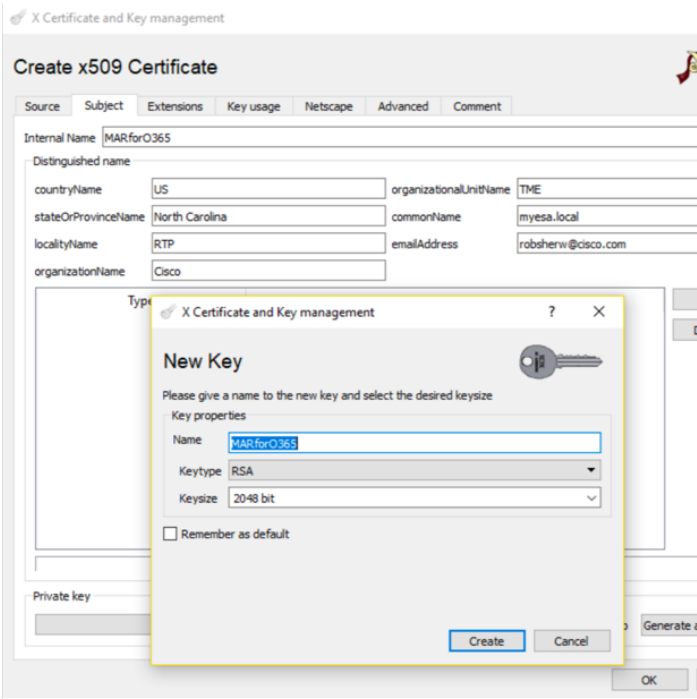
Voor beheerders die Windows gebruiken, zult u een toepassing moeten gebruiken of de kennis moeten hebben om een zelf-ondertekend certificaat te creëren. Dit certificaat wordt gebruikt voor het maken van de Microsoft karwei-toepassing en de bijbehorende API-communicatie.

Te creëren waarden:
- **Thumbprint**
- **Openbaar certificaat (CRT-bestand)**
- **Private Key (PEM-bestand)**

Ons voorbeeld voor dit document om een zelf-ondertekend certificaat te creëren gebruikt XCA (https://hohnstaedt.de/xca/, https://sourceforge.net/projects/xca/).

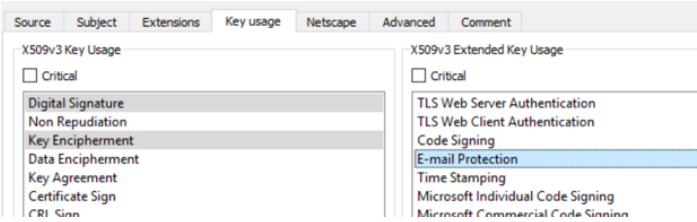
Opmerking: XCA kan worden gedownload voor Mac, Linux of Windows.

1. Maak een database voor uw certificaat en sleutels:
    a. Selecteer **Bestand** in de werkbalk
    b. Selecteer **Nieuwe database**
    c. Maak een wachtwoord voor uw database (u hebt het in latere stappen nodig, dus onthoud het!)
2. Klik op het tabblad Certificaten en klik vervolgens op **Nieuw certificaat**
3. Klik op het tabblad Onderwerp en vul het volgende in:
    a. Interne naam
    b. countryName
    c. staatorProvinceName
    d. plaatselijke naam
    e. organisatieNaam
    f. organisatorische eenheidnaam (OU)
    g. gewone naam (GN)
    h. e-mailadres
4. Klik op **Generate a New Key.**
5. Controleer bij de pop-up de verstrekte informatie (naar wens wijzigen):
    a. Name
    b. Keytype: RSA
    c. Keysize: 2048-bits
    d. Klik op Maken
    e. Bevestig de "Sucessated the RSA private key "Name" pop-up door op **OK** te klikken



Afbeelding 14: XCA gebruiken (stappen 3-5)

6. Klik op het tabblad Key use en selecteer de volgende opties:
    a. Gebruik onder X509v3-toets: **Digitale handtekeningen, toetsuitbreiding**
    b. Onder X509v3 uitgebreid gebruik van de sleutel: **E-mailbeveiliging**

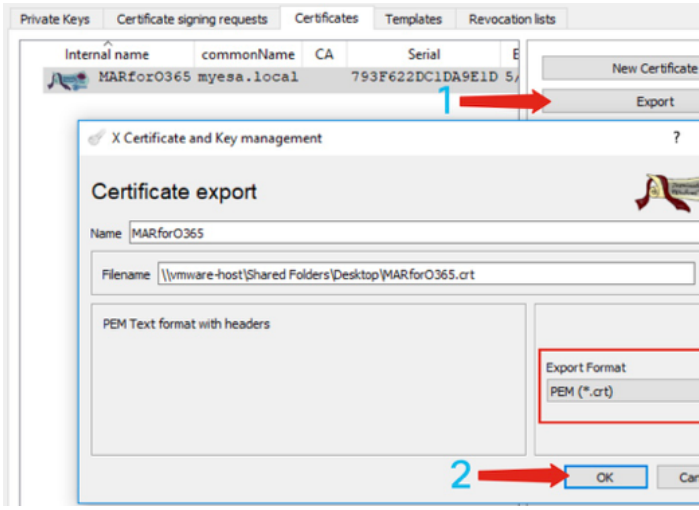


Afbeelding 15: Gebruik van XCA (stap 6)

7. Klik op **OK** om wijzigingen in uw certificaat toe te passen
8. Bevestig de "Sucessated the Certificate '*Name*" pop-up door op **OK** te klikken

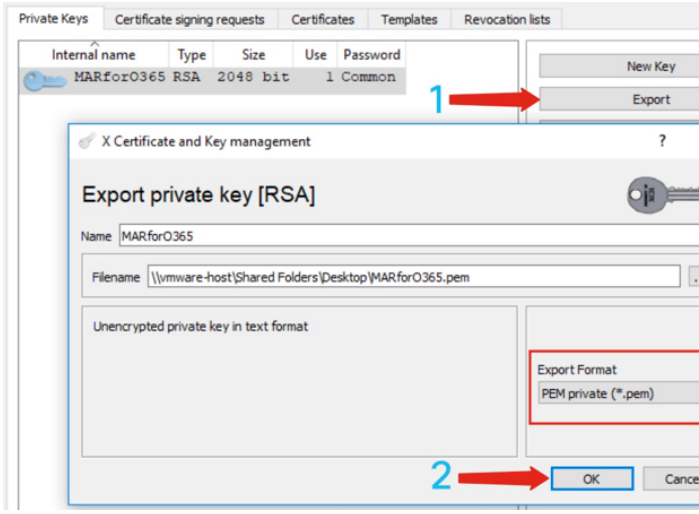
Daarna wilt u zowel het **openbare certificaat (CER-bestand)** als de ***certificaatparticuliere sleutel (PEM-bestand)*** exporteren voor gebruik in de opdrachten PowerShell naast elkaar en voor gebruik in de configureren Cisco beveiligde e-mailstappen:

1. Klik op de interne naam van uw nieuwe certificaat en selecteer deze naam.
2. Klik op **Exporteren**
    a. Stel de opgeslagen map in voor gemakkelijke toegang (indien gewenst wijzigen)
    b. Zorg ervoor dat het uitvoerformaat is ingesteld op **PEM (.crt)**
    c. Klik op **OK**



Afbeelding 16: Gebruik van XCA (export CRT) (stappen 1-2)

3. Klik op het tabblad **Private** Keys
4. Klik op de interne naam van uw nieuwe certificaat en benadruk deze.
5. Klik op **Exporteren**
    a. Stel de opgeslagen map in voor gemakkelijke toegang (indien gewenst wijzigen)
    b. Zorg ervoor dat het uitvoerformaat is ingesteld op **PEM Private (.pem)**
    c. Klik op **OK**
6. Afsluiten XCA



Afbeelding 17: Gebruik van XCA (export PEM) (stappen 3-5)

Tot slot neemt u uw gemaakte certificaat in en extraheert u de **Thumbprint**, die nodig is voor het configureren van Cisco Secure Email.

1. Gebruik Windows PowerShell om het volgende te doen:

```
$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. Zo haalt u waarden voor de volgende stappen op, slaat u op een bestand of kopieert u het klembord:

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

Opmerking: “c:\Users\joe\Desktop..." is de locatie op uw pc waarop u de uitvoer opslaat.

De verwachte uitvoer bij het uitvoeren van de opdracht PowerShell moet gelijk zijn aan het volgende:

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

Zoals u ziet, roept de opdracht PowerShell de *base64Thumbprint uit*, de **Thumbprint** die nodig is voor de configuratie van Cisco Secure Email Gateway.

U hebt ook het maken van het **openbare certificaat (CER-bestand)** voltooid dat nodig is voor de **aanmelding** van de App. En u hebt de ***Private Key (PEM-bestand)*** gemaakt**,** die u in de sectie Cisco Secure E-mail configureren zult gebruiken.

U hebt de benodigde waarden om uw aanvraag in Microsoft Messenger te registreren!

[Ga naar "Registreer een apps voor gebruik met Cisco Secure Email"

Bijlage B

Opmerking: dit is ALLEEN vereist als u AsyncOS 11.x of 12.x voor e-mail op uw gateway draait.

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

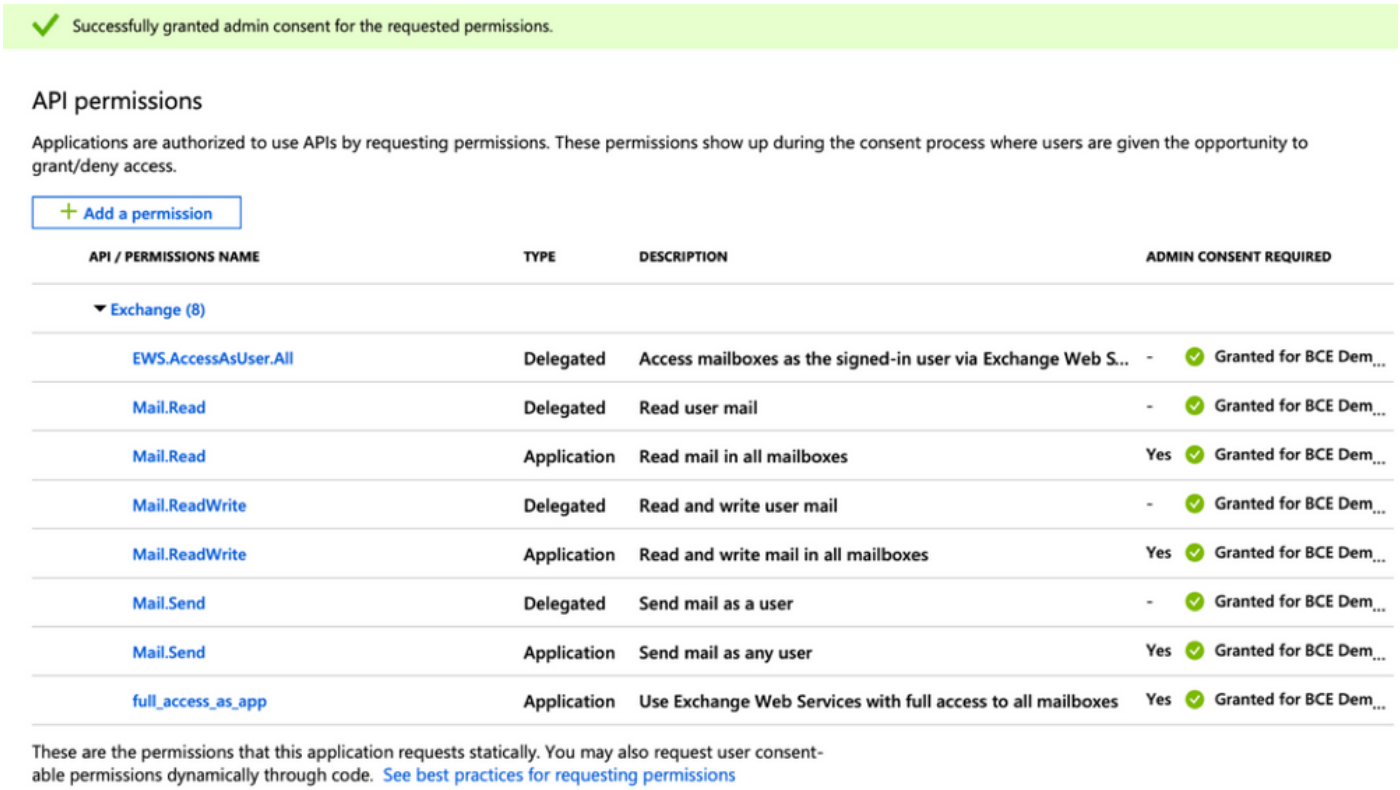
In uw toepassingsvenster, in de opties beheren...

1. Selecteer **API-toegangsrechten**
2. Klik op **+ Voeg een toestemming toe**

3. Scrolt naar **Ondersteunde API**'s en selecteer **Exchange**
4. Selecteer de volgende machtigingen op Gedelegeerde machtigingen: EWS > "EWS.AccessAsUser.All" (Access-mailboxen als de ingesloten gebruiker via Exchange Web Services)Mail > "Mail.Read" (Lezen van gebruikersmail)Mail > "Mail.ReadWrite" (Lees en schrijf gebruikersmail)Mail > "Mail.Verzend" (Verzend mail als gebruiker)
5. Naar boven in het deelvenster bladeren...
6. Selecteer de volgende rechten op toepassingsrechten: "full_access_as_app" (Gebruik Exchange Web Services met volledige toegang tot alle postboxen)Mail > "Mail.Read" (Lezen van gebruikersmail)Mail > "Mail.ReadWrite" (Lees en schrijf gebruikersmail)Mail > "Mail.Verzend" (Verzend mail als gebruiker)
7. *Optioneel:* U zult zien dat Microsoft Graph per default is ingeschakeld voor de "User.Read"-rechten; U kunt dit als ingesteld achterlaten of op **Lezen** klikken en op **Verwijderen met toestemming** klikken om dit uit uw API-rechten te verwijderen die aan uw toepassing zijn gekoppeld.
8. Klik op **Add permissies** (of **Update permissies**, als Microsoft Graph al in de lijst stond)
9. Klik tot slot op **Grant Admin toestemming voor...** om er zeker van te zijn dat uw nieuwe toestemming op de toepassing wordt toegepast
10. Er verschijnt een pop-up in het deelvenster met de volgende vragen:
    "*Wilt u toestemming geven voor de gevraagde toestemming voor alle rekeningen in <burernaam>? Dit vult elke bestaande admin-toestemming bij die deze toepassing al moet aanpassen aan wat hieronder is weergegeven.*"

    Klik op **Ja**

Op dit punt dient u een groen succesbericht te zien en de kolom "Admin Consent" (Vereiste instemming) te tonen, vergelijkbaar met de weergave:



Afbeelding 18: Microsoft Ken App registratie (API-permissies vereist)

[Ga naar "Registreer een apps voor gebruik met Cisco Secure Email"

Gerelateerde informatie

- Cisco e-mail security applicatie - productondersteuning
- Cisco e-mail security applicatie - release Notes
- Cisco e-mail security applicatie - eindgebruikershandleiding