如何為Microsoft Azure(Microsoft 365)API配置思科安全電子郵件帳戶設定

目錄

簡介

本文檔提供了分步操作步驟，用於在Microsoft Azure(Azure Active Directory)中註冊新應用程式以生成所需的客戶端ID、租戶ID和客戶端憑據，然後配置思科安全電子郵件網關或雲網關上的帳戶設定。當郵件管理員為高級惡意軟體防護(AMP)或URL過濾配置郵箱自動補救(MAR)或利用思科安全郵件和網路管理器或思科安全網關/雲網關上的郵件跟蹤中的補救操作時，需要配置帳戶設定和相關帳戶配置檔案。

郵箱自動修正流程

您的電子郵件或URL中的附件（檔案）在任何時候都可能被評定為惡意的，即使它到達使用者的郵箱之後也是如此。思科安全電子郵件上的AMP（通過思科安全惡意軟體分析）可以在出現新資訊時識別此發展，並向思科安全電子郵件推送追溯性警報。Cisco Talos提供的URL分析與AsyncOS 14.2 for Cisco Secure Email Cloud Gateway相同。 如果您的組織使用Microsoft 365管理郵箱，則可以配置Cisco Secure Email在使用者郵箱中的郵件在這些威脅判定發生更改時執行自動補救操作

。

思科安全電子郵件安全且直接與Microsoft Azure Active Directory通訊，以獲得對Microsoft 365郵箱的訪問許可權。 例如，如果包含附件的電子郵件通過您的網關處理並由AMP掃描，則檔案附件(SHA256)會提供給AMP以獲得檔案信譽。 AMP處置可以標籤為「Clean」（步驟5，圖1），然後傳遞給最終收件人的Microsoft 365郵箱。 稍後，AMP處置更改為惡意，思科惡意軟體分析會向處理該特定SHA256的任何網關傳送追溯判定更新（步驟8，圖1）。 一旦網關收到惡意的追溯判定更新（如果已配置），則網關將執行以下郵箱自動補救(MAR)操作之一：轉發、刪除或轉發和刪除。

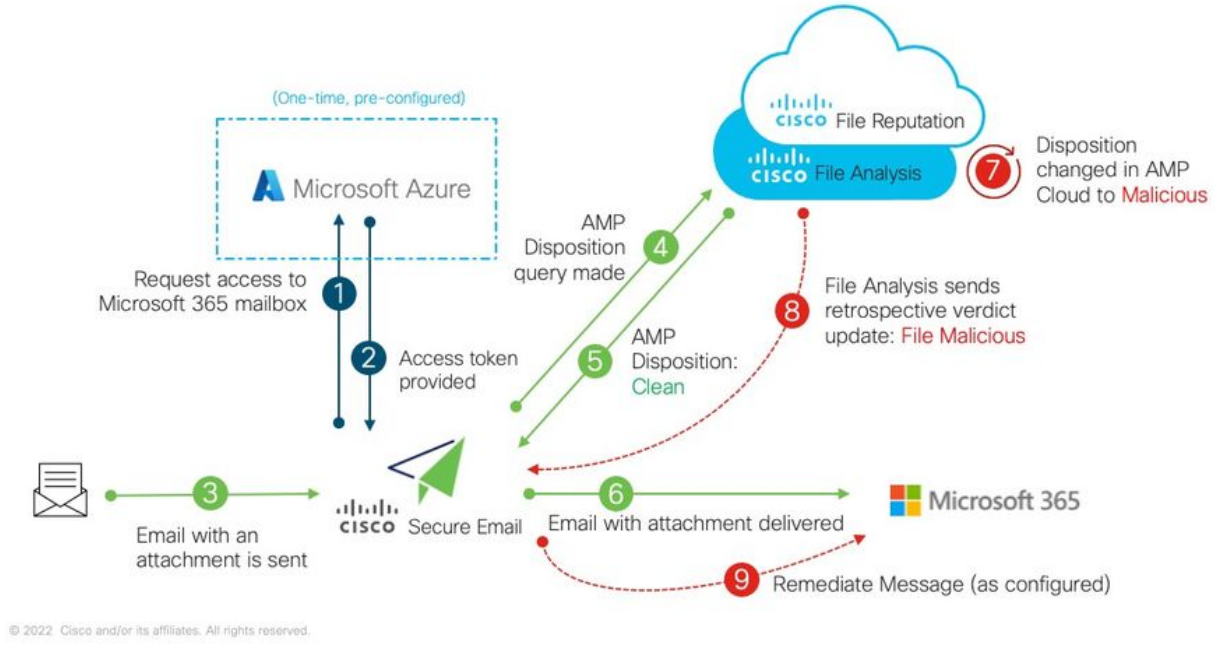

圖1:思科安全電子郵件上的MAR(AMP)

本指南介紹如何使用Microsoft 365配置Cisco Secure Email僅用於郵箱自動補救。 應已經配置網關上的AMP（檔案信譽和檔案分析）和/或URL過濾。 有關檔案信譽和檔案分析的更多詳細資訊，請參閱使用者手冊，瞭解您已部署的AsyncOS版本。

必要條件

1. Microsoft 365帳戶訂閱（請確保您的Microsoft 365帳戶訂閱包含對Exchange的訪問，例如企業E3或企業E5帳戶。 ）

2. Microsoft Azure管理員帳戶和對http://portal.azure.com的訪問

3. Microsoft 365和Microsoft Azure AD帳戶已正確繫結到有效的「user@domain.com」電子郵件地址，並且你可以通過該電子郵件地址傳送和接收電子郵件。

您將建立以下值，以配置與Microsoft Azure AD的思科安全電子郵件網關API通訊：

- **客戶端ID**

- **租戶ID**
- **客戶端密碼**

  附註： 從AsyncOS 14.0開始，**帳戶設定**允許在建立Microsoft Azure應用註冊時使用客戶端金鑰進行配置。這是比較容易和首選的方法。

可選 — 如果不使用客戶端密碼，則需要建立並做好準備：

- **指紋**
- **私鑰（PEM檔案）**

建立指紋和私鑰將在本指南的附錄中介紹：

1. 活動的公有（或私有）證書(CER)和用於簽署證書(PEM)的私密金鑰，或者能夠建立公共證書(CER)以及能夠儲存用於簽署證書的私密金鑰(PEM)。Cisco在本文檔中提供了兩種方法，以便根據您的管理偏好完成此操作： 證書：Unix/Linux/OS X（使用OpenSSL）證書 ：Windows（使用PowerShell）

2. 訪問Windows PowerShell（通常由Windows主機或伺服器管理），或通過Unix/Linux訪問終端應用程式

為了建立這些必需的值，您需要完成本文檔中提供的步驟。

註冊用於思科安全電子郵件的Azure應用

申請註冊

登入您的Microsoft Azure門戶
1.按一下**Azure Active Directory**（圖2）
2.按一下應用**註冊**
3.按一下**+新註冊**
4.在「註冊應用程式」頁面上：
a.名稱：**Cisco Secure Email MAR**（或您選擇的名稱）
b.支援的帳戶型別：**僅此組織目錄中的帳戶（帳戶名稱）**
c.重定向URI:（選用）
[附註：您可以將此欄位留空，或者隨意使用 https://www.cisco.com/sign-on進行填寫]
d.在頁面底部，按一下**Register**

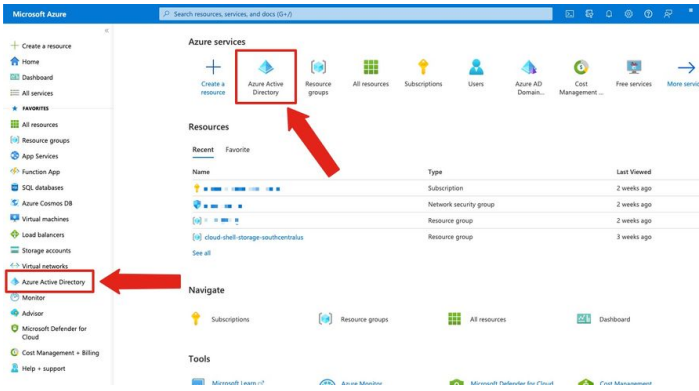

圖2:Microsoft Azure門戶示例

完成上述步驟後，系統將顯示您的應用程式：

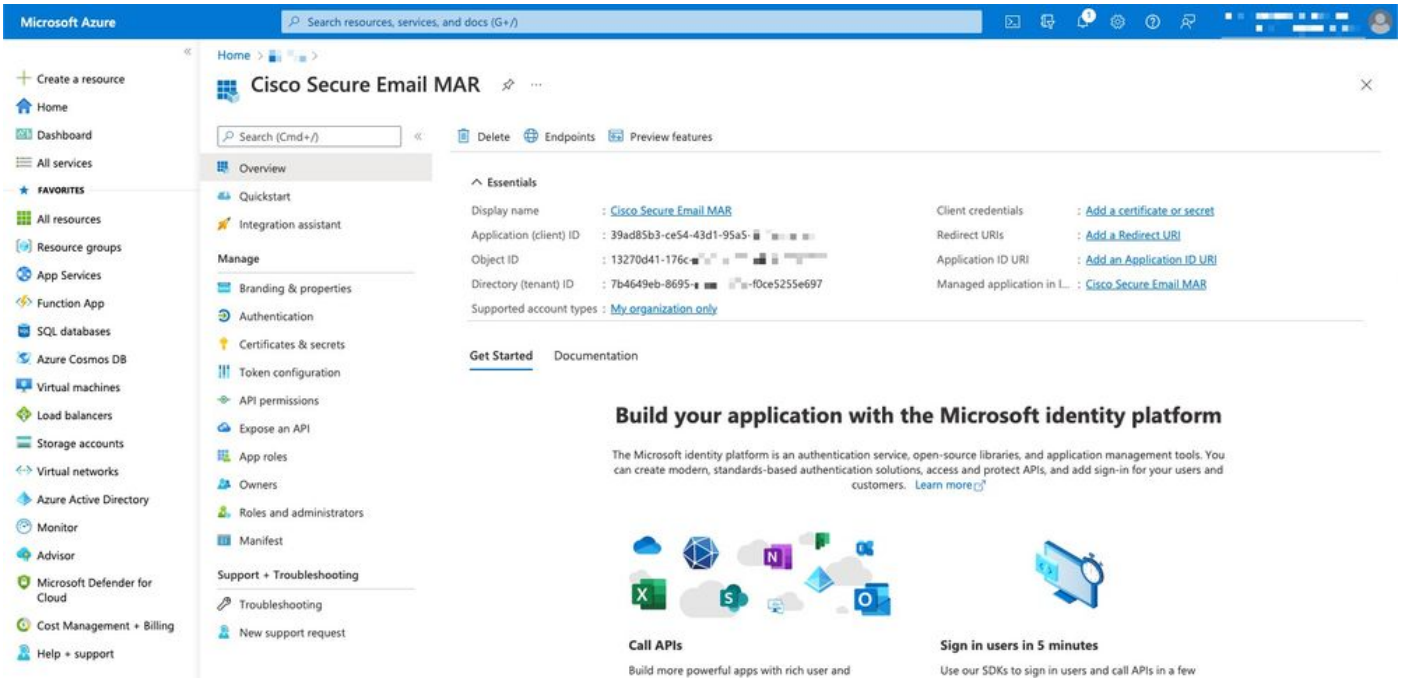

圖3:Microsoft Azure Active Directory應用程式頁

證書和機密

如果您正在運行AsyncOS 14.0或更高版本，思科建議配置Azure應用以使用客戶端密碼。 在應用程式窗格中，在管理選項中：

1.選擇**Certificates & secrets**

2.在***Client secrets***部分，按一下**+New client secret**

3.新增描述以幫助確定此客戶端金鑰的用途，例如「思科安全電子郵件補救」

4.選擇到期期間

5.按一下**Add**

6.將滑鼠懸停在生成的值的右側，然後按一下「複製到剪貼簿」(Copy to Clipboard)圖示

7.將此值儲存到您的備註中，請將此值記為「客戶端密碼」

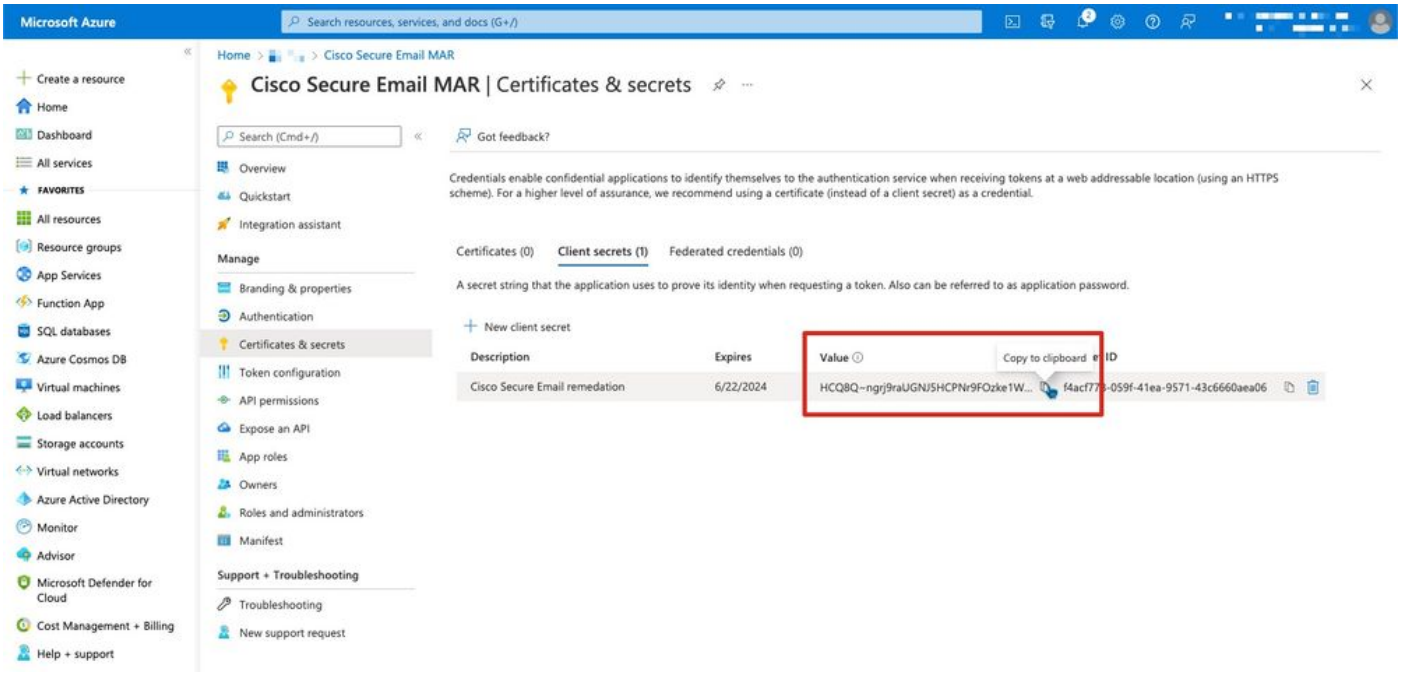

圖4:Microsoft Azure建立客戶端金鑰示例

附註：退出活動的Microsoft Azure會話後，您剛剛生成的客戶端金鑰值將***出該值。 如果在退出之前不記錄和保護該值，則需要重新建立客戶端加密才能看到明文輸出。

可選 — 如果未使用客戶端金鑰配置Azure應用程式，請將Azure應用配置為使用證書。 在應用程式窗格中，在管理選項中：

1. 選擇**Certificates & secrets**
2. 按一下**「Upload certificate」**
3. 選擇CRT檔案（如先前建立的）
4. 按一下**「Add」**

API許可權

附註：從AsyncOS 13.0 for Email Security開始，需要的Microsoft Azure到Cisco Secure Email通訊的API許可權已從使用Microsoft Exchange更改為Microsoft Graph。如果您已配置MAR，並且正在將現有的Cisco Secure Email網關升級到AsyncOS 13.0，則只需更新/新增新的API許可權即可。（如果您運行的是較舊版本的AsyncOS、11.x或12.x，請參閱附錄B，然後繼續。）

在應用程式窗格中，在管理選項中：

1. 選擇**API許可權**
2. 按一下**+「新增許可權」**
3. 選擇**Microsoft Graph**
4. 選擇以下對應用程式權***限的許可權***: 郵件>「Mail.Read」（讀取所有郵箱中的郵件）郵件>「Mail.ReadWrite」（在所有郵箱中讀取和寫入郵件）Mail >「Mail.Send」（以任何使用者身份傳送郵件）Directory > "Directory.Read.All"（讀取目錄資料）[*可選：如果使用LDAP聯結器

/LDAP同步，請啟用。 如果不是，則不需要此操作。]

5. *可選*:您將看到Microsoft Graph預設為「User.Read」許可權；您可以保持此配置不變，或者按一下**讀取**並按一下**刪除許可權**將其從與應用程式關聯的API許可權中刪除。
6. 按一下**Add permissions**(或者**Update permissions**（如果已列出Microsoft Graph）
7. 最後，按一下**Grant admin consent for..（授予管理員同意……）**確保將您的新許可權應用到應用程式
8. 窗格中將彈出一個問題：

"*是否要為<Azure名稱>中所有帳戶所請求的許可權授予同意許可權？這將更新此應用程式已經擁有的與下列內容匹配的任何現有管理員同意記錄。*」

按一下**Yes**

此時，您應該會看到綠色成功消息，並且「需要管理員同意」列顯示「已批准」。

獲取您的客戶端ID和租戶ID

在應用程式窗格中，在管理選項中：

1. 按一下**Overview**
2. 將滑鼠懸停在應用程式（客戶端）ID的右側，然後按一下**複製到剪貼簿圖**標
3. 將此值儲存到您的筆記，請將此記為「客戶端ID」
4. 將滑鼠懸停在目錄（租戶）ID右側，然後點選複製**到剪貼簿圖**標
5. 將此值儲存到您的筆記，請將此記為「租戶ID」

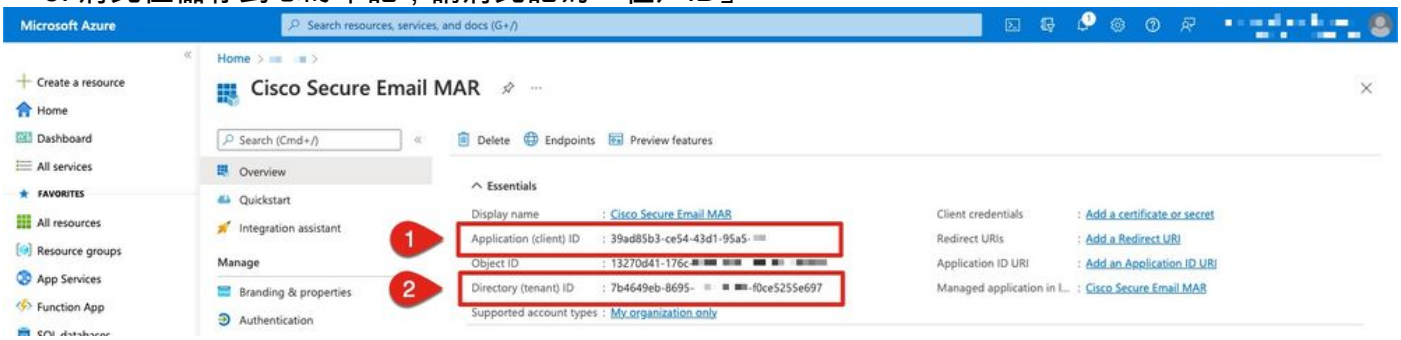

圖5:Microsoft Azure..客戶端ID、租戶ID示例

配置思科安全電子郵件網關/雲網關

此時，應準備以下值並將其儲存到您的備註中：

- **客戶端ID**
- **租戶ID**
- **客戶端密碼**

可選，如果未使用客戶端密碼：

- **指紋**
- **私鑰（PEM檔案）**

您已準備好使用您的筆記中建立的值，並在思科安全電子郵件網關上配置帳戶設定！

建立帳戶配置檔案

1. 登入到網關
2. 導航到**系統管理>帳戶設定** 附註：如果您運行的是AsyncOS 13.x之前的版本，則此版本將為System Administration > Mailbox Settings
3. 按一下**「Enable」**
4. 按一下「Enable Account Settings（啟用帳戶設定）」覈取方塊，然後按一下**「Submit（提交）」**
5. 按一下**Create Account Profile**
6. 提供配置檔名稱和說明（如果您有多個域，則可以唯一描述您的帳戶）
7. 在定義Microsoft 365連線時，請將配置檔案型別保留為**Office 365/混合(Graph API)**
8. 輸入您的**客戶端ID**
9. 輸入您**的租戶ID**
10. 對於客戶端憑據，請按照您在Azure中的配置執行下列操作之一： 按一下**Client Secret**並貼上到您配置的客戶端金鑰或……按一下**Client Certificate**，輸入您的指紋，還可以按一下「Choose File」提供PEM
11. 按一下**Submit**
12. 按一下UI右上角的**Commit Changes**
13. 輸入任何註釋，並通過點選提交更改完成**配置更改**

檢查連線

下一步只是驗證從思科安全電子郵件網關到Microsoft Azure的API連線：

1. 在相同的「帳戶詳細資訊」頁面中，按一下**測試連線**
2. 輸入在Microsoft 365帳戶中管理的域的有效電子郵件地址
3. 按一下**測試連線**
4. 您應該會收到成功訊息（圖6）
5. 按一下**完成**完成

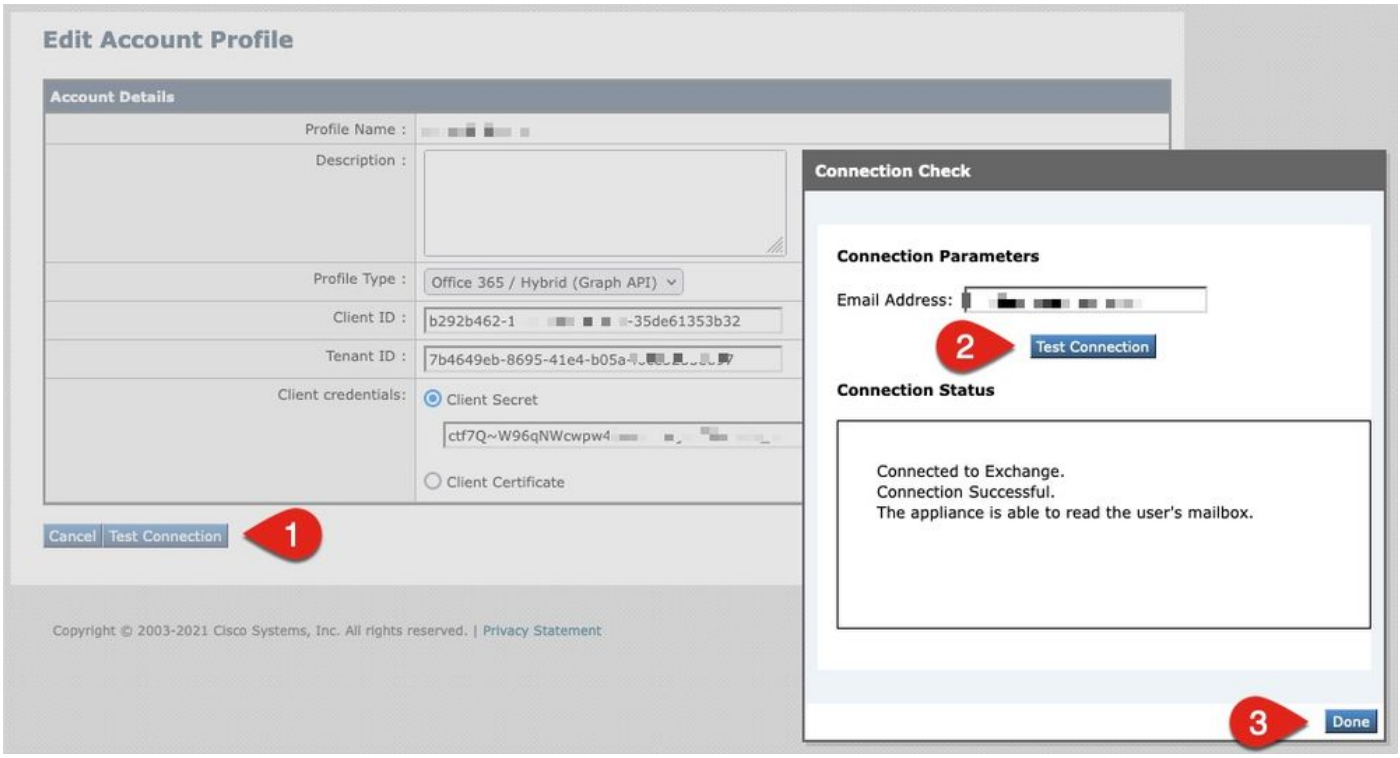

圖6:帳戶配置檔案/連線檢查示例

6.在*域對映*部分，按一下**建立域對映**

7.輸入與剛剛驗證的API連線的Microsoft 365帳戶關聯的域名

以下是可用於對映郵箱配置檔案的有效域格式清單：

— 域可以是特殊關鍵字「ALL」以匹配所有域，以便建立預設域對映。

— 域名，如「example.com」 — 匹配任何與此域匹配的地址。

— 部分域名，如「@.partial.example.com」 — 匹配任何以此域結尾的地址

— 可以使用逗號分隔的域清單輸入多個域。

8.按一下**提交**

9.按一下UI右上角的**Commit Changes**

10.輸入任何註釋，並通過按一下**Commit Changes**完成配置更改

啟用郵箱自動修正(MAR)，以便在郵件策略中進行高級惡意軟體防護

完成此步驟，在郵件策略的AMP配置中啟用MAR。

1. 導航到**Mail Policies > Incoming Mail Policies**
2. 點選要配置的策略名稱的「高級惡意軟體防護」列中的設定（例如，圖7）：

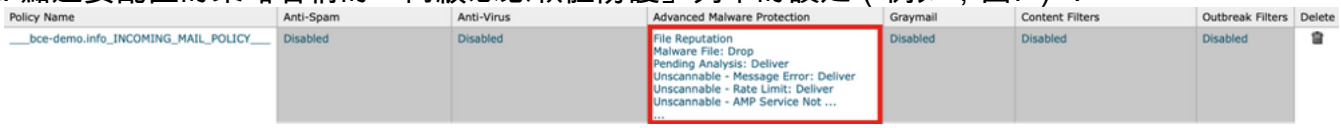

圖7:啟用MAR（傳入郵件策略）

3. 滾動到頁面底部
4. 按一下啟用郵箱自動補救(MAR)覈取方塊
5. 選擇您要為MAR採取的下列操作之一（例如，圖8）： 轉發至：<輸入*電子郵件地址*>刪除轉發至：<輸入*電子郵件地址*>並刪除

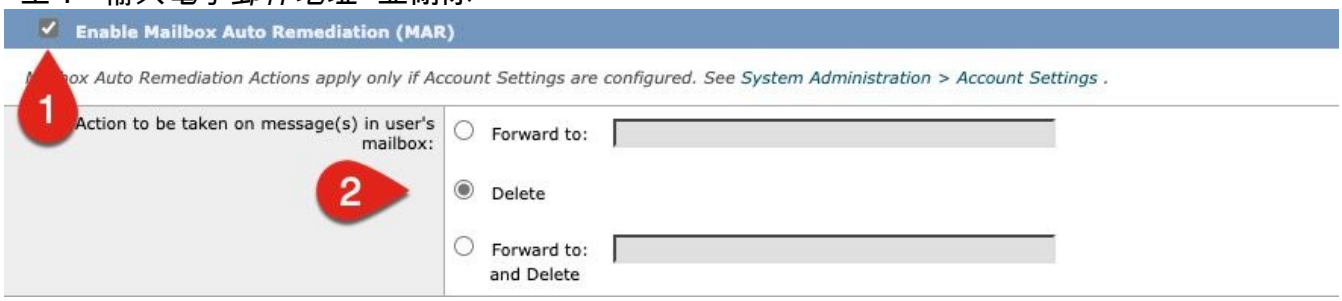

圖8:啟用AMP的MAR配置示例

6. 按一下**Submit**
7. 按一下UI右上角的**Commit Changes**
8. 輸入任何註釋，並通過點選提交更改完成**配置更改**

為URL過濾啟用郵箱自動修正(MAR)

從思科安全電子郵件雲網關的AsyncOS 14.2開始，URL過濾現在包括URL追溯判定和URL補救。

1. 導覽至**安全服務> URL篩選**
2. 如果您尚未配置URL過濾，請按一下**Enable**
3. 按一下「啟用URL類別和信譽過濾器」覈取方塊
4. 使用預設設定的*Advanced Settings*
5. 按一下**Submit**

您的URL過濾應類似於以下內容：

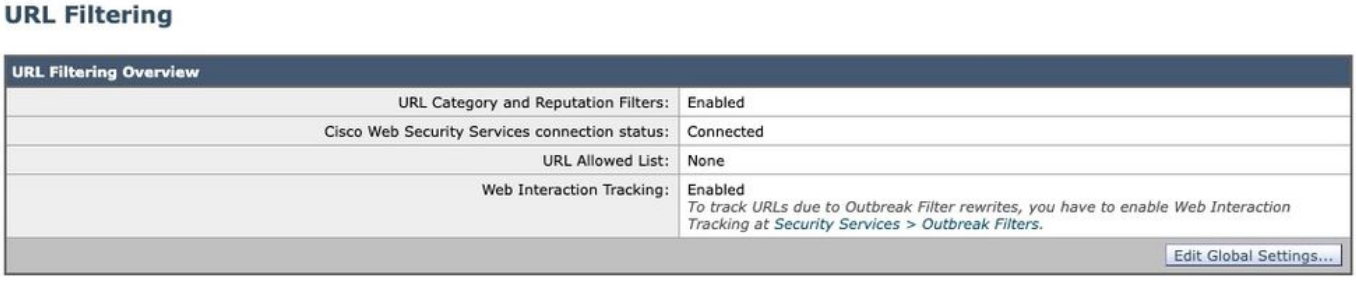

圖9:URL過濾啟用後示例

若要檢視具有內送URL篩選的URL追溯，請執行以下步驟，或開啟支援案例以供Cisco執行：

```
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
```

完成後，在「URL過濾」(URL Filtering)頁面刷新您的UI，您現在應該會看到類似以下的內容：

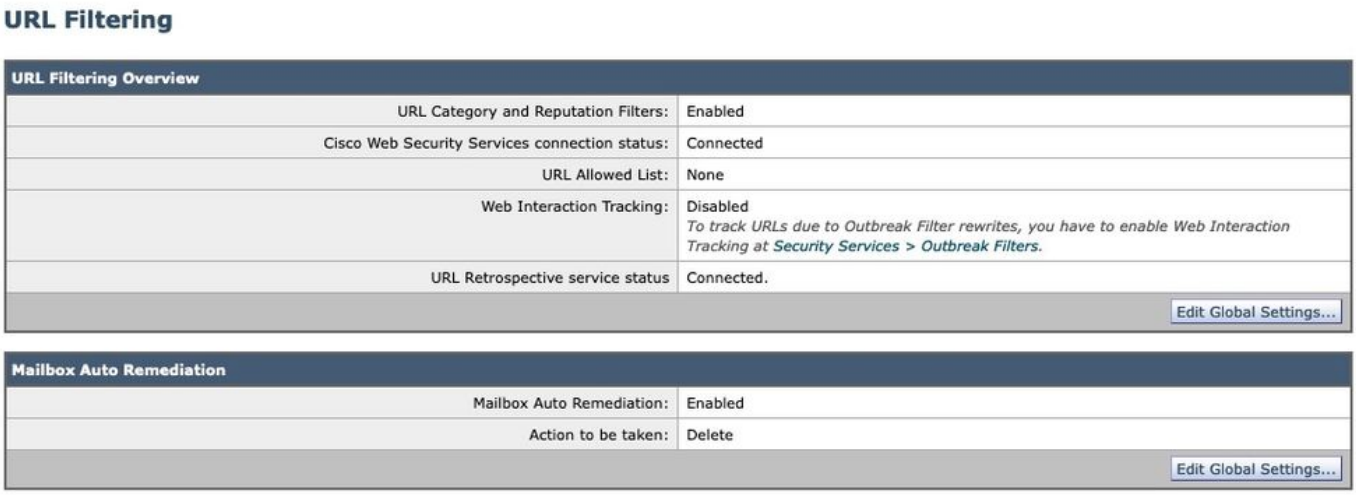

圖10:URL過濾（適用於思科安全電子郵件雲閘道的AsyncOS 14.2）

現在，URL保護已準備就緒，可在判定結果更改得分時執行補救措施。 有關詳細資訊，請參閱適用於Cisco Secure Email Cloud Gateway的AsyncOS 14.2使用手冊中的保護免受惡意或不想要的URL的侵害。

配置完成！

目前，思科安全電子郵件已準備就緒，可以在新資訊出現時持續評估新出現的威脅，並在檔案進入您的網路後通知您這些被確定為威脅的檔案。

當從檔案分析（思科安全惡意軟體分析）產生追溯性判定時，會向郵件安全管理員（如果已配置）傳送資訊消息。 範例：

```
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
```

如果根據郵件策略進行配置，則郵箱自動補救將採取已配置的方式。

郵箱自動修正報告示例

已修復的任何SHA256的報告將在思科安全郵件網關和思科安全郵件和網路管理器上可用的郵箱自動修復報告中提供。

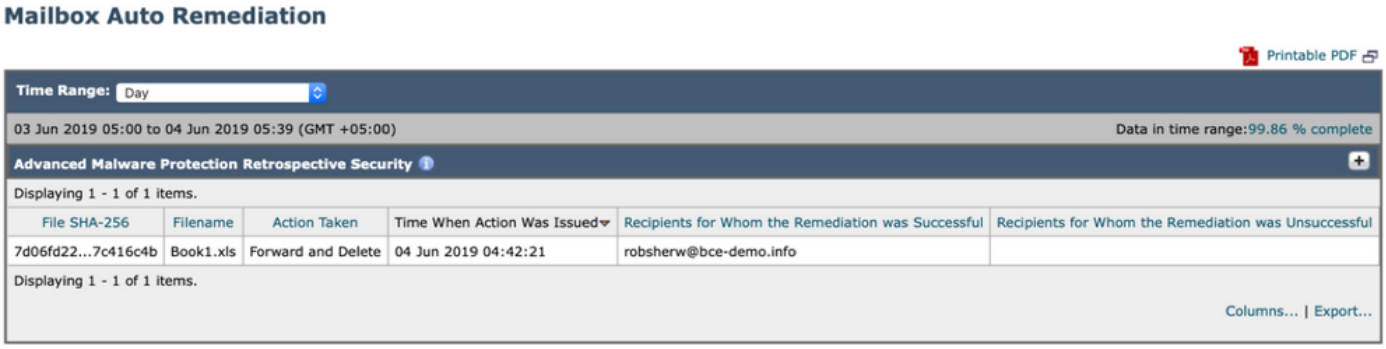

圖11:（舊版UI）郵箱自動修正報告

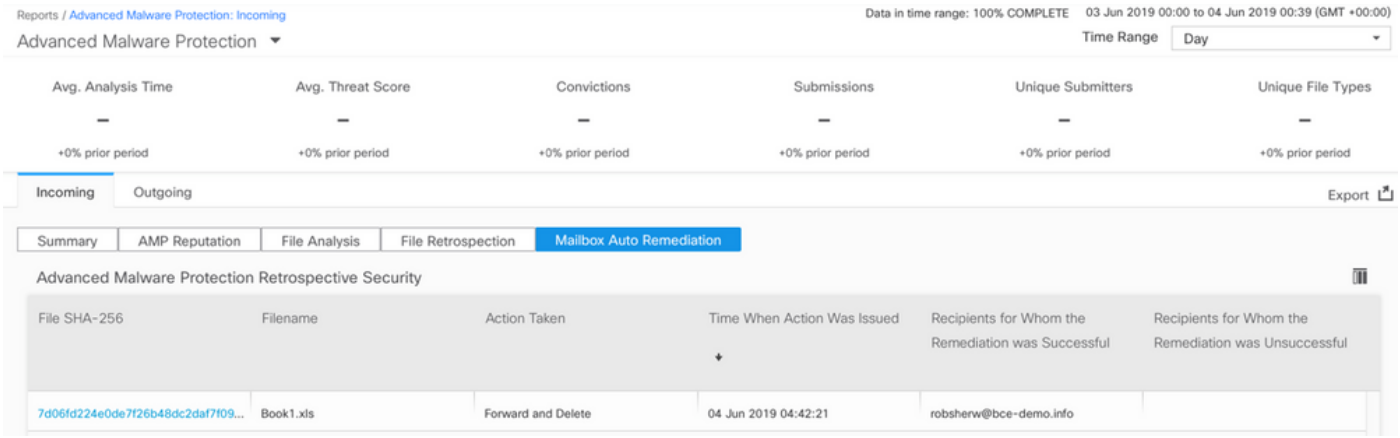

圖12:(NG UI)郵箱自動修正報告

郵箱自動修正日誌記錄

郵箱自動修正具有單獨的日誌「mar」。 郵箱自動修正日誌將包含您的思科安全電子郵件網關與Microsoft Azure、Microsoft 365之間的所有通訊活動。

標籤日誌示例：

```
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.
```

思科安全電子郵件網關故障排除

如果您沒有看到連線狀態測試的成功結果，則可能希望檢視從Microsoft Azure AD執行的應用程式註冊。

從思科安全電子郵件網關，將您的MAR日誌設定為「跟蹤」級別，然後重新測試連線。

對於不成功的連線，顯示的日誌可能類似於：

```
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
```

使用你的應用程式在Azure AD中確認日誌中的應用程式ID、目錄ID（與租戶ID相同）或其他關聯識別符號。如果你不確定這些值，請從Azure AD門戶刪除該應用程式並重新開始。

要成功連線，日誌應類似於：

```
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.
```

Azure AD故障排除

> **註**意：思科TAC和思科支援人員無權對Microsoft Exchange、Microsoft Azure AD或Office 365的客戶方問題進行故障排除。

對於Microsoft Azure AD的客戶方問題，您需要聯絡Microsoft支援部門。 請參閱Microsoft Azure儀表板中的「幫助+支援」選項。 您可以從控制面板向Microsoft支援部門提出直接支援請求。

附錄A

注意：僅當未使用客戶端金鑰設定Azure應用程式時，才需要此項。

建立公共和私人憑證與金鑰對

提示:請在本地儲存*$base64Value*、 *$base64Thumbprint*和*$keyid*的輸出，因為稍後在配置步驟中需要這些輸出。 請將證書的.crt和關聯的.pem放在電腦上的可用本地資料夾中。

附註：如果您已經擁有證書（x509格式/標準）和私鑰，請跳過此部分。 請確保您同時具有CRT和PEM檔案，因為您將在接下來的部分中需要它們！

證書：Unix/Linux（使用openssl）

要建立的值：
- 印
- **用憑證（CRT檔案）**
- **私密金鑰（PEM檔案）**

使用Unix/Linux/OS X的管理員為了執行提供的指令碼，假定您安裝了OpenSSL。

附註：執行命令「which openssl」和「openssl version」以驗證OpenSSL安裝。安裝OpenSSL（如果沒有）！

如需幫助，請參閱以下文檔：思科安全電子郵件的Azure AD配置指令碼

從主機(UNIX/Linux/OS X):

1. 從終端應用程式、文本編輯器（或者無論您如何輕鬆地建立shell指令碼）中，通過複製以下內容來建立指令碼
   ：https://raw.githubusercontent.com/robsherw/my_azure/master/my_azure.sh
2. 貼上指令碼

3. 請確保使指令碼可執行！運行以下命令： **chmod u+x my_azure.sh**
4. 運行指令碼：**./my_azure.sh**

```
################################################################################
Next, log-in to Microsoft Azure and use the following for your App registration:
################################################################################

Complete the Azure App registration (Certificate & secrets) using this certificate (public key): MARforO365.crt
Complete the Azure App registration (API permissions)
View & save your Client ID and Tenant ID

########################################################
After successful Azure App registration, from Cisco ESA:
########################################################

Use the Client ID and Tenant ID copied from your Azure App registration
The Thumbprint to use for your ESA configuration: cY8JViuV1oFRVFje/HC9J9ZGvl8=
The Certificate Private Key to use for your ESA configuration: MARforO365.pem

Do you wish to review this certificate in detail? (y/n) n
Thank you!  Be sure to keep up-to-date from https://docs.ces.cisco.com
```

圖13:my_azure.sh的螢幕輸出

如圖2所示，指令碼會生成並呼叫**Azure應用註冊所需的**公共證書（CER檔案）。指令碼還呼叫了***指紋***和***憑證私密金鑰（PEM檔案）***您將使用在配置思科安全電子郵件部分。

你擁有在Microsoft Azure中註冊我們的應用程式所需的值！

[跳過下一部分！ 請繼續操作「註冊Azure應用以用於Cisco Secure Email」]

證書：Windows（使用PowerShell）

對於使用Windows的管理員，您需要利用應用程式或具備建立自簽名證書的知識。 此證書用於建立Microsoft Azure應用程式並關聯API通訊。

要建立的值：
- **印**
- **用憑證（CRT檔案）**
- **私密金鑰（PEM檔案）**

本文建立自簽名證書的示例使用
XCA(https://hohnstaedt.de/xca/,https://sourceforge.net/projects/xca/)。

附註：可以為Mac、Linux或Windows下載XCA。

1.為證書和金鑰建立資料庫：

a.從工具欄中選擇**檔案**
b.選擇**新資料庫**
c.為您的資料庫建立口令
（在後續步驟中需要它，請記住它！）

2.按一下「證書」頁籤，然後按一下**新建證書**

3.按一下「主題」標籤並填寫以下內容：
a.內部名稱
b.國家/地區名稱
c.stateOrProvinceName
d.localityName
e.組織名稱
f. organizationalUnitName(OU)
g.一般名稱(CN)
h.電子郵件地址

4.按一下**生成新金鑰**

5.在彈出視窗中，驗證所提供的資訊（根據需要更改）：
a.名稱
b.Keytype:RSA
c.金鑰大小：2048位元
d.按一下建立
e.按一下「確定」以確認「已成功建立RSA私鑰『名稱』」彈出**框**

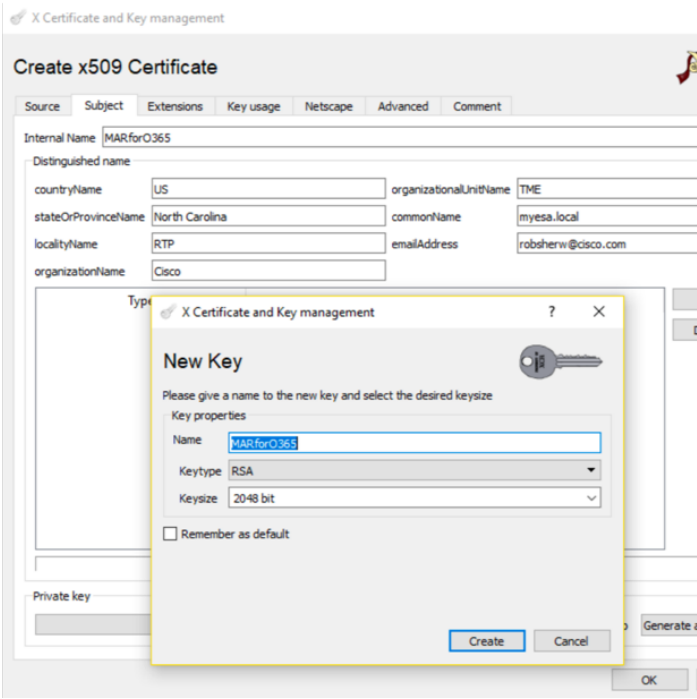

圖14:使用XCA（步驟3-5）

6.按一下「金鑰用法」頁籤，然後選擇以下內容：
a.在X509v3 Key Usage:
數位簽章、金鑰加密
b.在X509v3 Extended Key Usage:
電子郵件保護

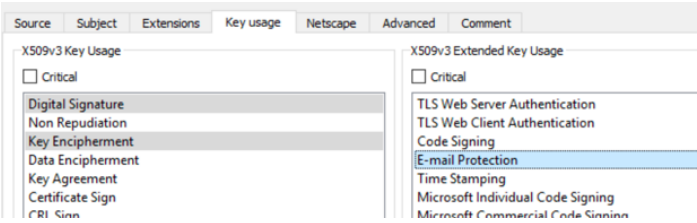

圖15:使用XCA（步驟6）

7.按一下**OK**將更改應用到您的證書
8.按一下「確定」以確認「*已成*功建立證書『名稱』」彈出窗**口**

接下來，您將要匯出**公共證書（CER檔案）**和***證書私鑰（PEM檔案）***，以便在PowerShell命令啟動時使用，並在配置Cisco安全電子郵件步驟中使用：

1.按一下並突出顯示新建立的證書的內部名稱。
2.按一下**匯出**
a.設定儲存目錄以便於訪問（根據需要更改）
b.確保匯出格式設定為**PEM(.crt)**
c.按一下**OK**

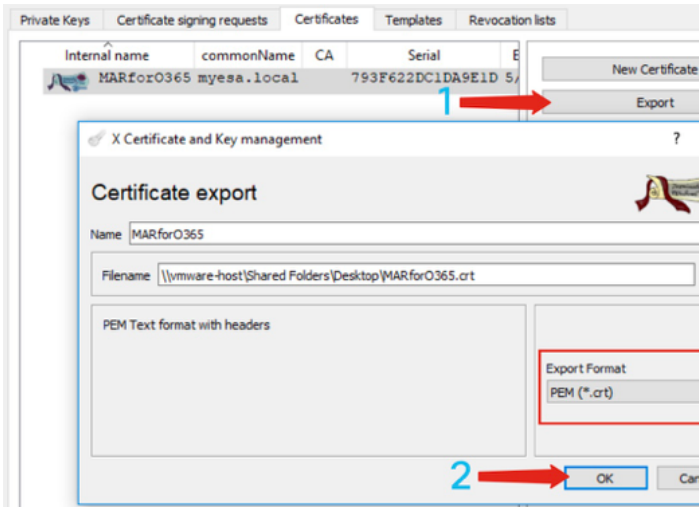

圖16:使用XCA（匯出CRT）（步驟1-2）

3.按一下**Private Keys(私鑰)選**項卡
4.按一下並突出顯示新建立的證書的內部名稱。
5.按一下**匯出**
   a.設定儲存目錄以便於訪問（根據需要更改）
   b.確保匯出格式設定為**PEM private(.pem)**
   c.按一下**OK**
6.退出並關閉XCA

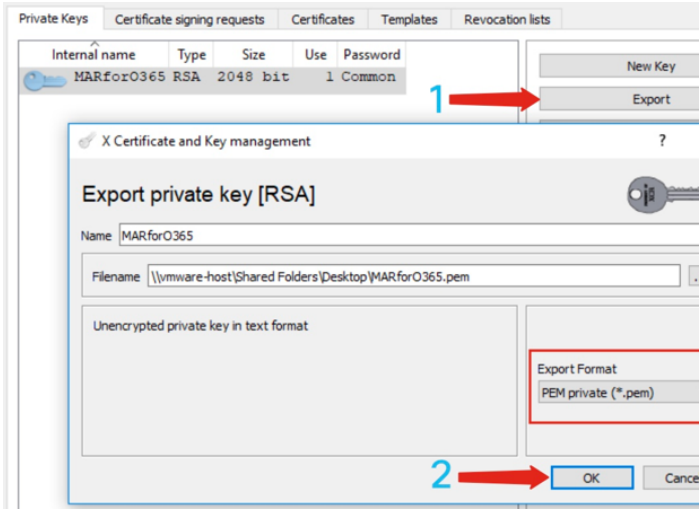

圖17:使用XCA（匯出PEM）（步驟3-5）

最後，您將獲取您建立的證書並提取**指紋**，這是配置Cisco安全電子郵件所必需的。

1. 使用Windows PowerShell，運行以下命令：

```
$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. 要獲取即將執行的步驟的值，請儲存到檔案或複製到剪貼簿：

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

```
$base64Thumbprint
```

附註：“c:\Users\joe\Desktop..." 是您在PC上儲存輸出的位置。

運行PowerShell命令時的預期輸出應類似於以下內容：

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

如您所見，PowerShell命令將呼叫*base64Thumbprint*，這是**思科安全電子郵件網關配置所需的Thumbprint**。

您還已完成建立**Azure應用註冊所需的**公共證書（CER檔案）。您已建立將在「配置Cisco Secure Email」部分使用的***證書私鑰（PEM檔案）***。

你擁有在Microsoft Azure中註冊應用程式所需的值！

[請繼續操作「註冊Azure應用以用於Cisco Secure Email」]

附錄B

注意：只有在網關上為郵件運行AsyncOS 11.x或12.x時，才需要執行此操作。

API許可權(AsyncOS 11.x、12.x)

在應用程式窗格中，在管理選項……

1. 選擇**API許可權**
2. 按一下**+「新增許可權」**
3. 向下滾動到**Supported legacy API**，然後選擇**Exchange**
4. 選擇以下對授權許可權的許可權： EWS > "EWS.AccessAsUser.All"（通過Exchange Web Services以登入使用者的身份訪問郵箱）Mail > "Mail.Read"（讀取使用者郵件）Mail > "Mail.ReadWrite"（讀取和寫入使用者郵件）Mail >「Mail.Send」（以使用者身份傳送郵件）
5. 滾動到窗格的頂部……
6. 選擇下列應用程式許可權許可權： "full_access_as_app"（使用具有對所有郵箱的完全訪問許可權的Exchange Web服務）Mail > "Mail.Read"（讀取使用者郵件）Mail > "Mail.ReadWrite"（讀取和寫入使用者郵件）Mail >「Mail.Send」（以使用者身份傳送郵件）
7. *可選*:您將看到Microsoft Graph預設為「User.Read」許可權；您可以保持此配置不變，或者按一下**讀取**並按一下**刪除許可權**將其從與應用程式關聯的API許可權中刪除。

8. 按一下**Add permissions**(或者**Update permissions**（如果已列出Microsoft Graph）
9. 最後，按一下**Grant admin consent for..（授予管理員同意……）**確保將您的新許可權應用到應用程式
10. 窗格中將彈出一個問題：

"是否要為<Azure名稱>中所有帳戶所請求的許可權授予同意許可權？這將更新此應用程式已經擁有的與下列內容匹配的任何現有管理員同意記錄。」

按一下**Yes**

此時，您應該會看到綠色成功消息，並且「需要管理員同意」列顯示「已授予」，與所示類似：

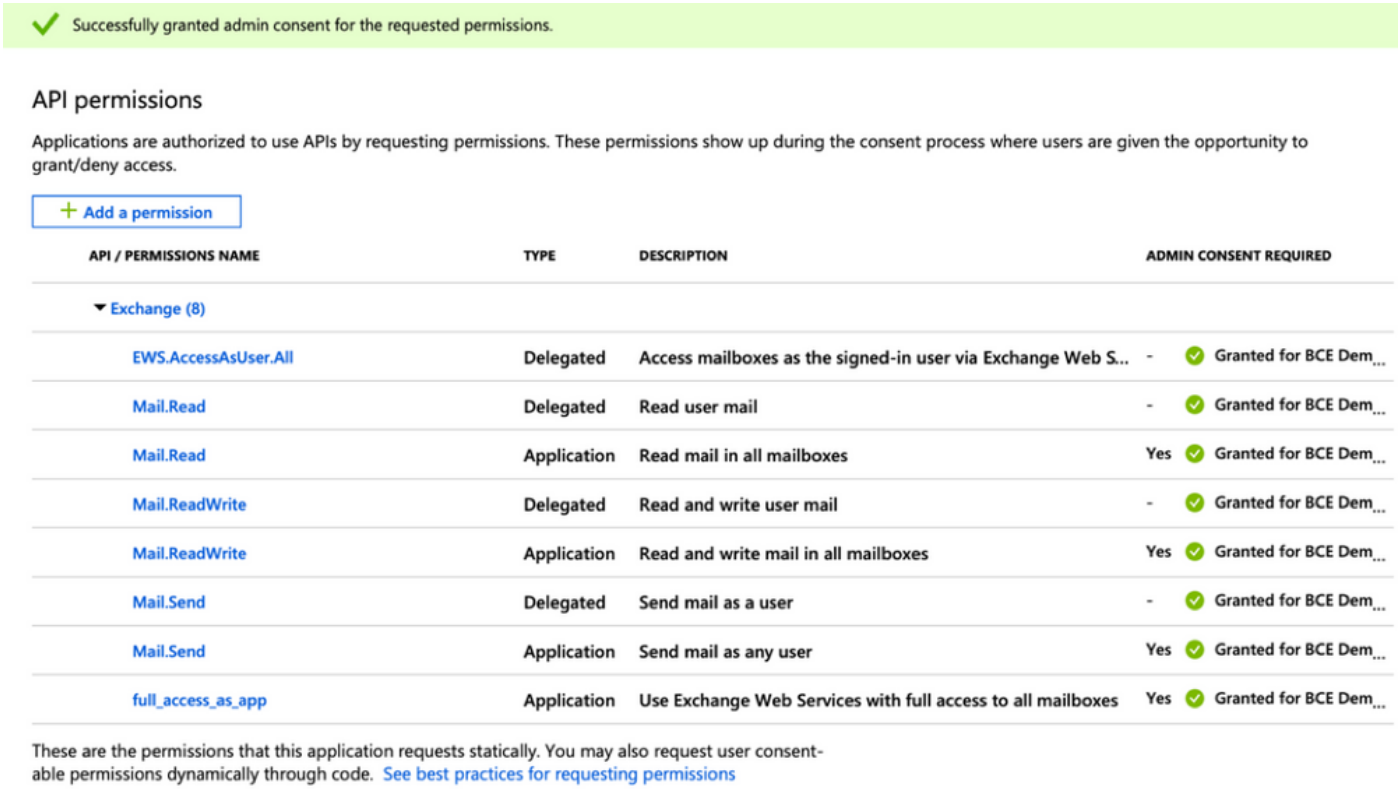

圖18:Microsoft Azure應用註冊（需要API許可權）

[請繼續操作「註冊Azure應用以用於Cisco Secure Email」]

相關資訊

- 思科電子郵件安全裝置 — 產品支援
- 思科電子郵件安全裝置 — 版本說明
- 思科郵件安全裝置 — 最終使用手冊