Microsoft Azure(Microsoft 365) API용 Cisco Secure Email 계정 설정을 구성하는 방법

목차

소개
사서함 자동 교정 프로세스 흐름
사전 요구 사항
Cisco Secure Email에 사용할 Azure 앱 등록
애플리케이션 등록
인증서 및 비밀
API 권한
클라이언트 ID 및 테넌트 ID 가져오기
Cisco Secure Email Gateway/Cloud Gateway 구성
계정 프로필 생성
연결 확인
메일 정책에서 AMP(Advanced Malware Protection)를 위한 MAR(Mailbox Auto Remediation) 활성화
URL 필터링을 위해 MAR(Mailbox Auto Remediation) 사용
사서함 자동 교정 보고서 예
사서함 자동 교정 로깅
Cisco Secure Email Gateway 트러블슈팅
Azure AD 문제 해결
부록 A
퍼블릭 및 프라이빗 인증서 및 키 쌍 구축
인증서: Unix/Linux(openssl 사용)
인증서: Windows(PowerShell 사용)
부록 B
API 권한(AsyncOS 11.x, 12.x)
관련 정보

소개

이 문서에서는 Microsoft Azure(Azure Active Directory)에 새 응용 프로그램을 등록하여 필요한 클라이언트 ID, 테넌트 ID 및 클라이언트 자격 증명을 생성한 다음 Cisco Secure Email Gateway 또는 클라우드 게이트웨이의 계정 설정에 대한 구성을 생성하기 위한 단계별 "방법"을 제공합니다. 메일 관리자가 AMP(Advanced Malware Protection) 또는 URL 필터링을 위해 MAR(Mailbox Auto Remediation)을 구성하거나 Cisco Secure Email and Web Manager 또는 Cisco Secure Gateway/Cloud Gateway의 Message Tracking에서 Remediate 작업을 사용하는 경우 계정 설정 및 관련 계정 프로필을 구성해야 합니다.

사서함 자동 교정 프로세스 흐름

이메일이나 URL의 첨부 파일(파일)은 사용자의 사서함에 도달한 후에도 언제든지 악성으로 평가될 수 있습니다. (Cisco Secure Malware Analytics를 통해) Cisco Secure Email의 AMP는 새로운 정보

가 등장함에 따라 이러한 개발을 식별하고 회귀적 알림을 Cisco Secure Email로 전달합니다. Cisco Talos는 AsyncOS 14.2 for Cisco Secure Email Cloud Gateway와 동일한 URL 분석을 제공합니다. 조직에서 Microsoft 365를 사용하여 사서함을 관리하는 경우 이러한 위협 판정이 변경될 때 사용자 사서함의 메시지에 대해 자동 교정 작업을 수행하도록 Cisco Secure Email을 구성할 수 있습니다.

Cisco Secure Email은 Microsoft Azure Active Directory에 안전하게 직접 통신하여 Microsoft 365 사서함에 액세스할 수 있습니다. 예를 들어, 첨부 파일이 있는 이메일이 게이트웨이를 통해 처리되고 AMP에서 스캔하는 경우 파일 평판을 위해 파일 첨부 파일(SHA256)이 AMP에 제공됩니다. AMP 성향이 Clean(5단계, 그림 1)으로 표시된 다음 최종 수신자의 Microsoft 365 사서함으로 배달됩니다. 나중에 AMP 성향이 Malware로 변경되고 Cisco Malware Analytics는 회귀적 판정 업데이트(8단계, 그림 1)를 해당 특정 SHA256을 처리한 *모든* 게이트웨이로 전송합니다. 게이트웨이가 악성(구성된 경우)의 회귀적 판정 업데이트를 수신하면 게이트웨이는 다음 사서함 자동 교정(MAR) 작업 중 하나를 수행합니다. 전달, 삭제 또는 전달과 삭제

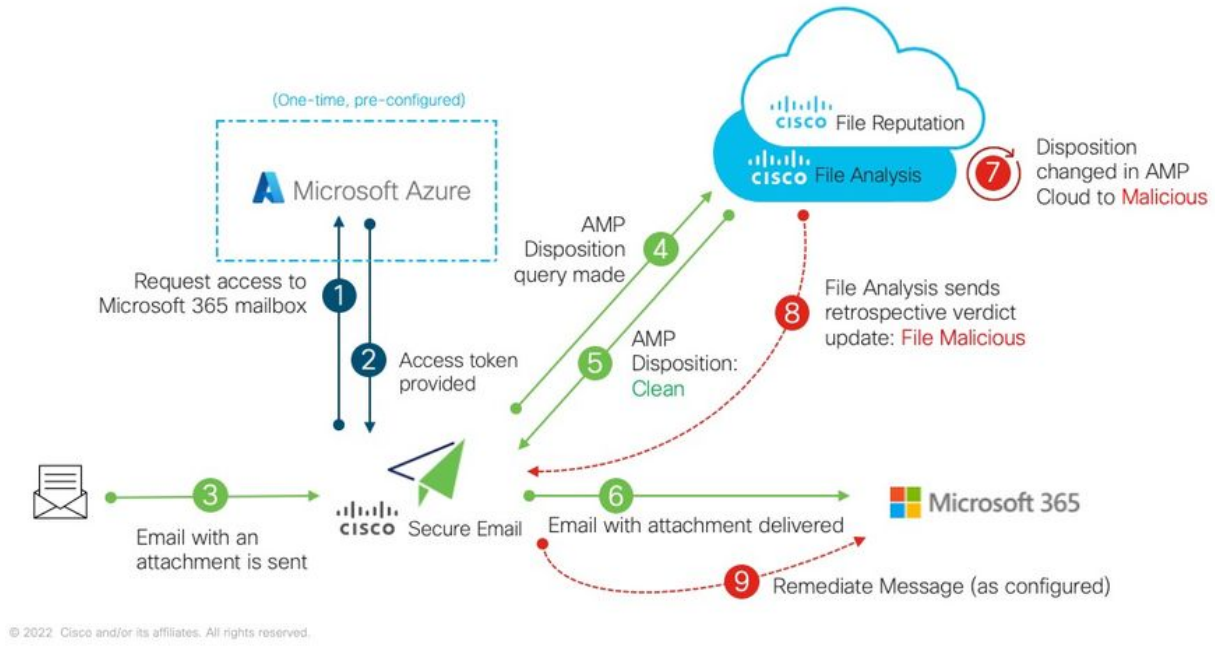

그림 1: Cisco Secure Email의 MAR(AMP용)

이 설명서는 사서함 자동 교정을 위한 Microsoft 365를 사용하여 Cisco Secure Email을 구성하는 방법에 대한 것입니다. 게이트웨이의 AMP(File Reputation and File Analysis) 및/또는 URL 필터링이 이미 구성되어 있어야 합니다. 파일 평판 및 파일 분석에 대한 자세한 내용은 구축한 AsyncOS 버전에 대한 사용 설명서를 참조하십시오.

사전 요구 사항

1. Microsoft 365 계정 구독(Microsoft 365 계정 구독에 Enterprise E3 또는 Enterprise E5 계정과 같은 Exchange에 대한 액세스가 포함되어 있는지 확인하십시오.)

2. Microsoft Azure 관리자 계정 및 http://portal.azure.com에 액세스

3. Microsoft 365와 Microsoft Azure AD 계정 모두 활성 "user@domain.com" 전자 메일 주소에 제대로 연결되어 있으며 해당 전자 메일 주소를 통해 전자 메일을 보내고 받을 수 있습니다.

Microsoft Azure AD에 대한 Cisco Secure Email Gateway API 통신을 구성하려면 다음 값을 만듭니다.

- **클라이언트 ID**
- **테넌트 ID**
- **클라이언트 암호**

  참고: AsyncOS 14.0부터 **계정 설정은** Microsoft Azure 앱 등록을 만들 때 클라이언트 암호를 사용하여 구성을 허용합니다. 이것이 더 쉽고 선호하는 방법입니다.

선택 사항 - 클라이언트 암호를 사용하지 않는 경우 다음을 생성하고 준비해야 합니다.

- **지문**
- **개인 키(PEM 파일)**

지문 및 개인 키를 생성하는 방법은 이 설명서의 부록에서 다룹니다.

1. 인증서(PEM)에 서명하는 데 사용되는 활성 공개(또는 개인) 인증서(CER) 및 개인 키(CER) 생성 기능 및 인증서(PEM)에 서명하는 데 사용되는 개인 키를 저장하는 기능. Cisco는 이 문서에서 관리 환경 설정에 따라 이 작업을 수행할 수 있는 두 가지 방법을 제공합니다. 인증서: Unix/Linux/OS X(OpenSSL 사용)인증서: Windows(PowerShell 사용)

2. Windows PowerShell에 대한 액세스(일반적으로 Windows 호스트 또는 서버에서 관리) 또는 Unix/Linux를 통해 터미널 애플리케이션에 대한 액세스

이러한 필수 값을 작성하려면 이 문서에 제공된 단계를 완료해야 합니다.

Cisco Secure Email에 사용할 Azure 앱 등록

애플리케이션 등록

Microsoft Azure 포털에 로그인
1. **Azure Active Directory**를 클릭합니다(그림 2).
2. **앱 등록**을 클릭합니다.
3. **+ New Registration(신규 등록)을 클릭합니다.**
4. "신청 등록" 페이지에서
   a. 이름: **Cisco Secure Email MAR**(또는 선택한 이름)
   b. 지원되는 계정 유형: **이 조직 디렉터리에 있는 계정만(계정 이름)**
   c. 리디렉션 URI: (선택 사항)
   [참고: 이 필드를 비워 두거나 https://www.cisco.com/sign-on을 채우기에 자유롭게 사용할 수 있습니다.]
   d. 페이지 하단에서 **등록**을 클릭합니다.

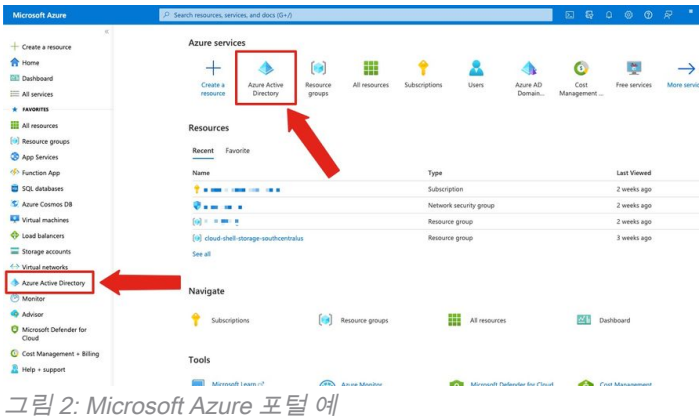

그림 2: Microsoft Azure 포털 예

위의 단계를 완료하면 다음과 같은 애플리케이션이 표시됩니다.

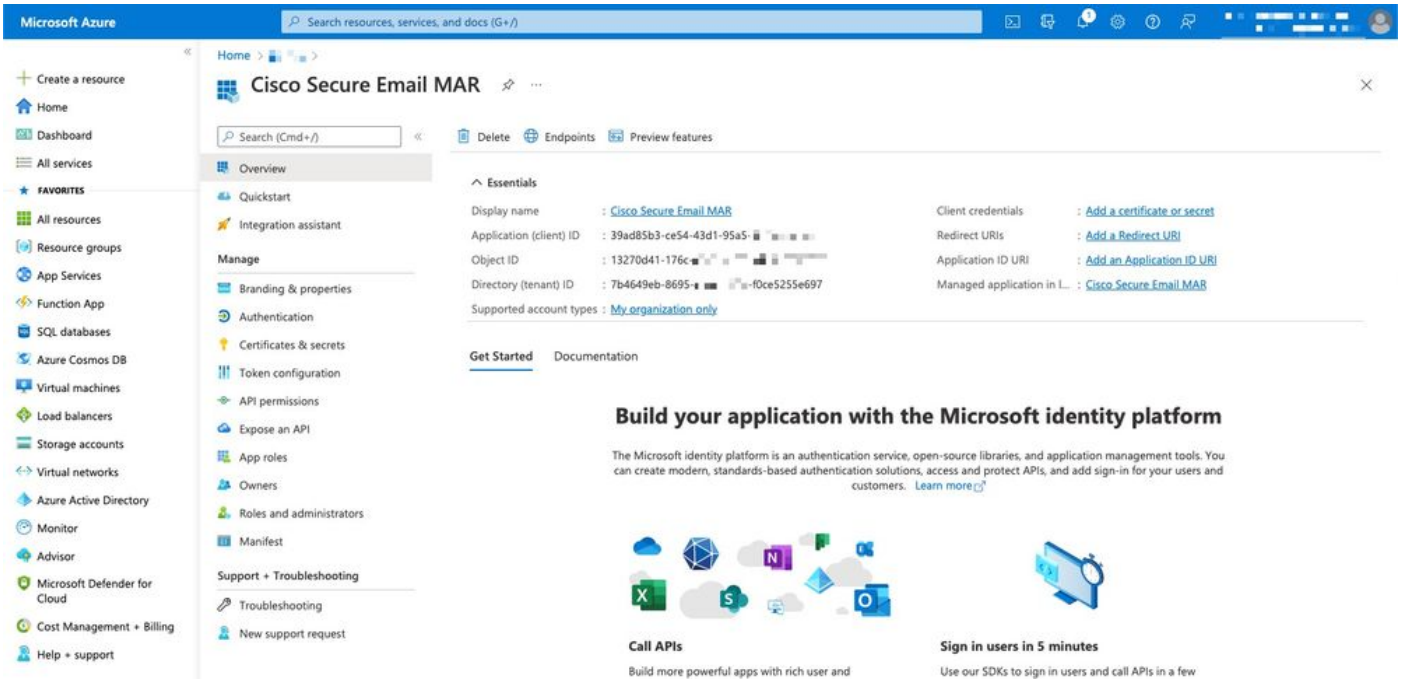

그림 3: Microsoft Azure Active Directory 응용 프로그램 페이지

인증서 및 비밀

AsyncOS 14.0 이상을 실행하는 경우 Cisco에서는 클라이언트 암호를 사용하도록 Azure 앱을 구성하는 것이 좋습니다. 응용 프로그램 창의 관리 옵션에서 다음을 수행합니다.

1. 인증서 **및 기밀**을 선택합니다.

2. Client Secrets(***클라이언트 보안***) 섹션에서 **+ New client secret(새 클라이언트 암호)를** 클릭합니다.

3. 설명을 추가하여 이 클라이언트 비밀의 목적(예: "Cisco Secure Email 교정"

4. 만기 기간을 선택합니다.

5. **추가**를 클릭합니다.

6. 생성된 값의 오른쪽에 마우스를 놓고 클립보드에 **복사** 아이콘을 클릭합니다.

7. 이 값을 노트에 저장하고 "클라이언트 암호"로 기록합니다.

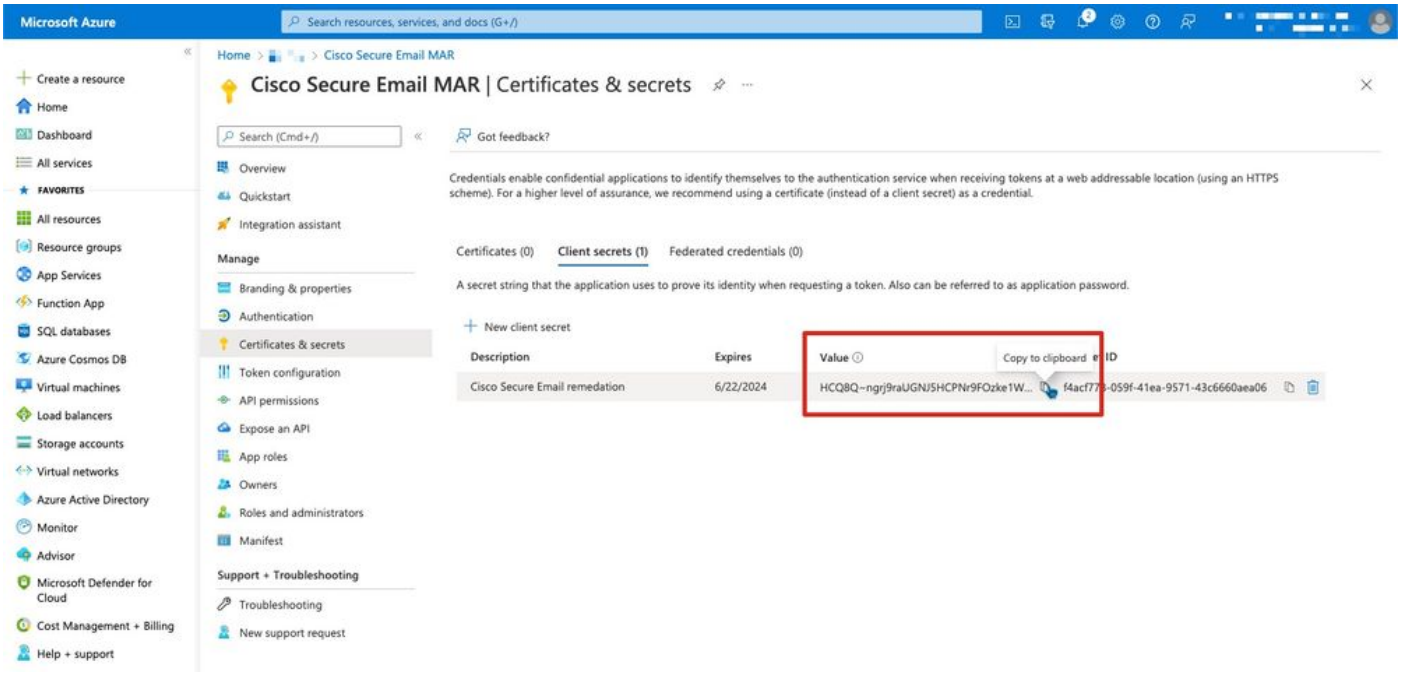

그림 4: Microsoft Azure 만들기 클라이언트 암호 예

참고: 활성 Microsoft Azure 세션을 종료하면 방금 생성한 클라이언트 암호 값이 ***에서 값을 제거합니다. 종료하기 전에 값을 기록하고 보호하지 않으면 일반 텍스트 출력을 보려면 클라이언트 암호를 다시 생성해야 합니다.

선택 사항 - 클라이언트 암호로 Azure 응용 프로그램을 구성하지 않는 경우 인증서를 사용하도록 Azure 앱을 구성하십시오. 응용 프로그램 창의 관리 옵션에서 다음을 수행합니다.

1. 인증서 **및 암호 선택**
2. Upload **certificate를 클릭합니다.**
3. CRT 파일(앞에서 생성한 대로) 선택
4. Add(추가)를 **클릭합니다.**

API 권한

참고: AsyncOS 13.0 for Email Security부터 Microsoft Azure에서 Cisco Secure Email 통신으로의 API 권한이 필요한 경우 Microsoft Exchange를 사용하는 것에서 Microsoft Graph로 변경되었습니다. 이미 MAR을 구성했으며 기존 Cisco Secure Email 게이트웨이를 AsyncOS 13.0으로 업그레이드하는 경우 새 API 권한을 업데이트/추가하면 됩니다. (이전 버전의 AsyncOS, 11.x 또는 12.x를 실행 중인 경우 계속하기 전에 부록 B를 참조하십시오.)

응용 프로그램 창의 관리 옵션에서 다음을 수행합니다.

1. **API 권한 선택**
2. **+ 권한 추가를 클릭합니다.**
3. **Microsoft Graph** 선택
4. 응용 프로그램 사용 권한에 대한 아래 사용 권한***을 선택하십시오***. Mail(메일) > "Mail.Read"(모

든 사서함에서 메일 읽기)Mail > "Mail.ReadWrite"(모든 사서함에서 메일 읽기 및 쓰기)Mail(메일) > "Mail.Send(메일 보내기)"(다른 사용자로 메일 보내기)디렉터리 > "Directory.Read.All"(디렉터리 데이터 읽기) [*선택 사항: LDAP 커넥터/LDAP 동기화를 사용하는 경우 를 활성화합니다. 그렇지 않은 경우 이는 필요하지 않습니다.]

5. *선택 사항:* Microsoft Graph는 기본적으로 "User.Read" 권한에 대해 활성화되어 있습니다. 이 항목을 구성된 상태로 두거나 **읽기**를 클릭하고 **제거 권한**을 클릭하여 응용 프로그램과 연결된 API 권한에서 제거할 수 있습니다.
6. **권한 추가**(또는 **Microsoft Graph**가 이미 나열된 경우 권한 업데이트)를 클릭합니다.
7. 마지막으로, **Grant admin consent for..(관리자 동의 권한 부여...)를** 클릭합니다. 새 사용 권한이 응용 프로그램에 적용되는지 확인합니다.
8. 다음과 같은 메시지가 표시되는 팝업 창이 나타납니다.

"*<Azure Name>의 모든 계정에 대해 요청된 권한에 동의하시겠습니까? 그러면 이 애플리케이션이 이미 아래 나열된 것과 일치해야 하는 기존 관리자 동의 레코드가 업데이트됩니다.*"

예를 클릭합니다.

이때 녹색 성공 메시지가 표시되고 "Admin Consent Required" 열에 Granted가 표시됩니다.

클라이언트 ID 및 테넌트 ID 가져오기

응용 프로그램 창의 관리 옵션에서 다음을 수행합니다.

1. Overview(**개요)를 클릭합니다.**
2. 응용 프로그램(클라이언트) ID의 오른쪽에 마우스를 놓고 클립보드에 **복사** 아이콘을 클릭합니다.
3. 이 값을 메모에 저장하고 "Client ID"로 기록합니다.
4. 디렉터리(테넌트) ID의 오른쪽으로 마우스를 가져간 후 **클립보드에 복사** 아이콘을 클릭합니다.
5. 이 값을 노트에 저장하고 "테넌트 ID"로 기록합니다.

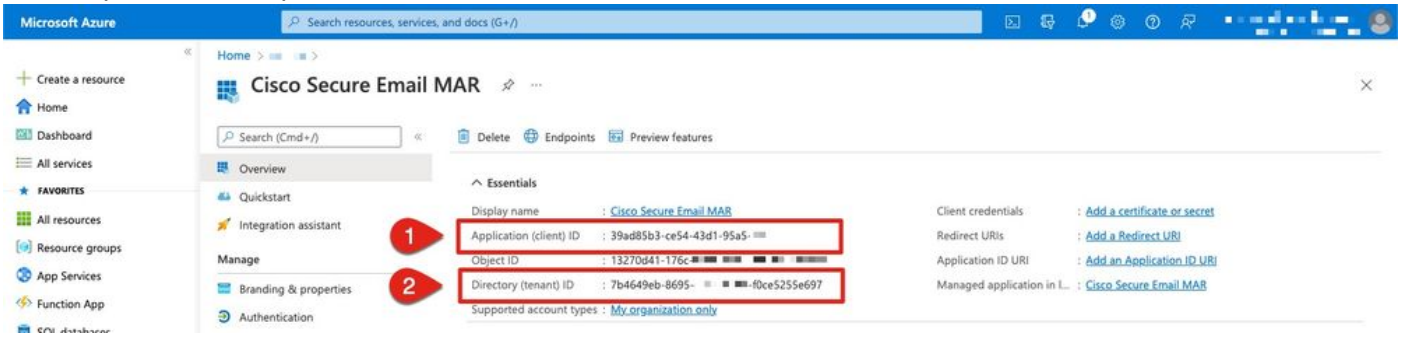

그림 5: Microsoft Azure... 클라이언트 ID, 테넌트 ID 예

Cisco Secure Email Gateway/Cloud Gateway 구성

이때 다음 값을 준비하여 메모에 저장해야 합니다.

- **클라이언트 ID**
- **테넌트 ID**
- **클라이언트 암호**

클라이언트 암호를 사용하지 않는 경우 선택 사항:

- **지문**
- **개인 키(PEM 파일)**

메모에서 생성한 값을 사용하고 Cisco Secure Email Gateway에서 계정 설정을 구성할 준비가 되었습니다!

계정 프로필 생성

1. 게이트웨이에 로그인
2. System Administration(**시스템 관리) > Account Settings(계정 설정)로 이동합니다.** 참고: AsyncOS 13.x 이전 버전을 실행하는 경우 System Administration(시스템 관리) **> Mailbox Settings(사서함 설정)가 됩니다.**
3. Enable(활성화)을 **클릭합니다.**
4. Enable Account Settings(계정 설정 활성화) 확인란을 클릭하고 Submit(제출)을 클릭합니다.
5. Create **Account Profile을 클릭합니다.**
6. 프로필 이름 및 설명(여러 도메인이 있는 경우 계정을 고유하게 설명하는 항목) 제공
7. Microsoft 365 연결을 정의할 때 프로파일 유형을 **Office 365/Hybrid(Graph API)**로 유지합니다.
8. 클라이언트 **ID 입력**
9. 테넌트 **ID 입력**
10. 클라이언트 자격 증명의 경우 Azure에서 구성한 대로 다음 중 하나를 수행합니다. Client **Secret(클라이언트** 암호)를 클릭하고 구성된 클라이언트 암호를 붙여넣거나..Client **Certificate(클라이언트 인증서**)를 클릭하고 Thumbprint(지문)를 입력하고 "Choose File(파일 선택)"을 클릭하여 PEM을 제공합니다.
11. **Submit(제출)을 클릭합니다.**
12. UI의 오른쪽 상단에서 Commit Changes를 클릭합니다.
13. 주석을 입력하고 Commit Changes(변경 사항 커밋)를 클릭하여 컨피그레이션 변경 사항**을 완료합니다.**

연결 확인

다음 단계는 Cisco Secure Email Gateway에서 Microsoft Azure로의 API 연결을 확인하는 것입니다.

1. 동일한 Account Details(계정 세부 정보) 페이지에서 **Test Connection(연결 테스트)을** 클릭합니다.
2. Microsoft 365 계정에서 관리되는 도메인의 유효한 전자 메일 주소를 입력하십시오.

3. Test **Connection(연결 테스트)을 클릭합니다.**
4. 성공 메시지를 받아야 합니다(그림 6).
5. Done(완료)을 클릭하여 완료합니다.

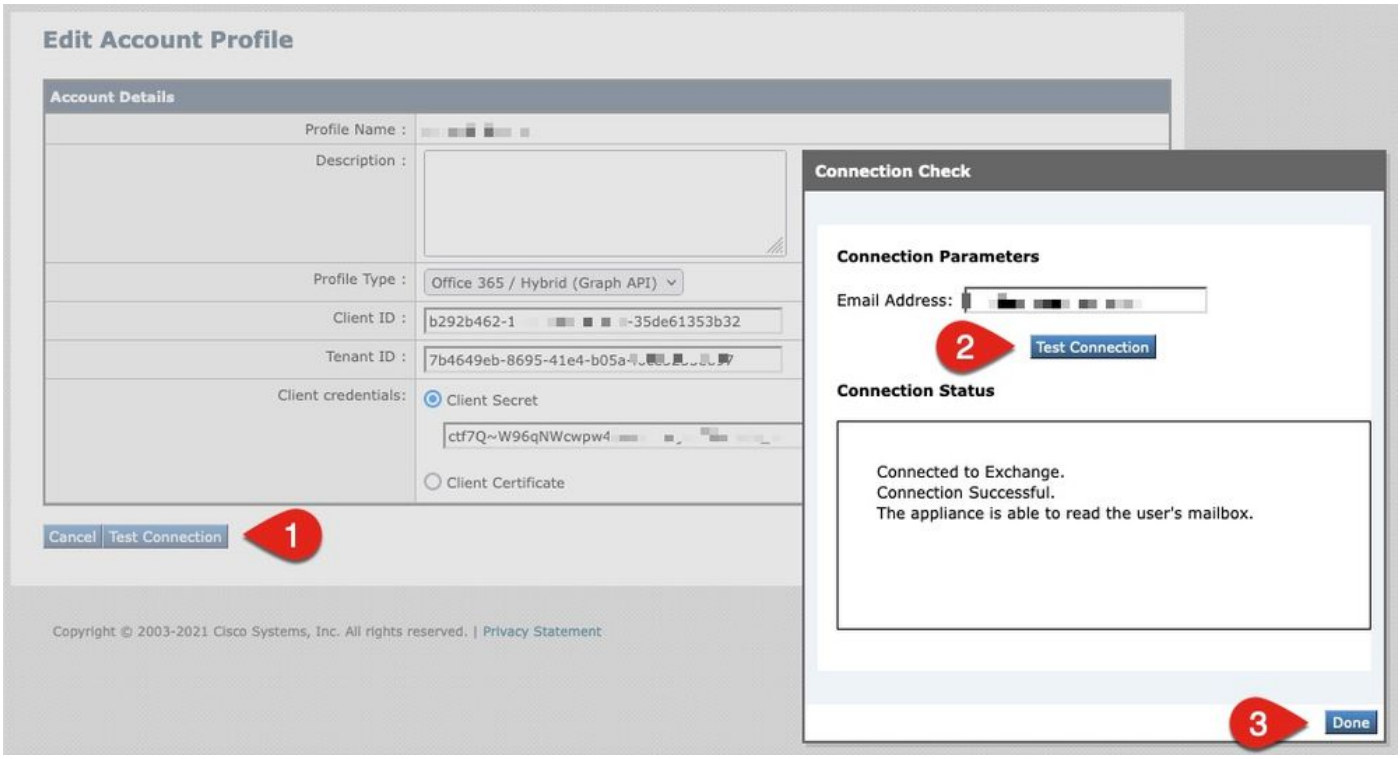

그림 6: 계정 프로필/연결 확인 예

6. *Domain Mapping(도메인 매핑)* 섹션에서 **Create Domain Mapping(도메인 매핑 생성)을** 클릭합니다.

7. API 연결을 검증한 Microsoft 365 계정과 연결된 도메인 이름을 입력합니다.

    다음은 사서함 프로필을 매핑하는 데 사용할 수 있는 유효한 도메인 형식의 목록입니다.

    - 기본 도메인 매핑을 생성하기 위해 모든 도메인을 확인하는 특수 키워드 'ALL'이 될 수 있습니다.

    - 도메인 이름(예: 'example.com') - 이 도메인의 모든 주소와 일치시킵니다.

    - 부분 도메인 이름(예: '@.partial.example.com') - 이 도메인으로 끝나는 모든 주소와 일치시킵니다.

    - 쉼표로 구분된 도메인 목록을 사용하여 여러 도메인을 입력할 수 있습니다.

8. 제출을 클릭합니다.

9. UI 오른쪽 상단에서 **Commit Changes(변경 사항 커밋)**를 클릭합니다.

10. 주석을 입력하고 **변경** 커밋(Commit Changes)을 눌러 구성 변경 사항을 **완료합니다.**

메일 정책에서 AMP(Advanced Malware Protection)를 위한 MAR(Mailbox Auto Remediation) 활성화

메일 정책에 대한 AMP 컨피그레이션에서 MAR을 활성화하려면 이 단계를 완료합니다.

1. Mail Policies(**메일 정책**) > **Incoming Mail Policies(수신 메일 정책)로 이동합니다.**
2. 구성할 정책 이름의 Advanced Malware Protection(Advanced Malware Protection) 열에서 설정을 클릭합니다(예: 그림 7).

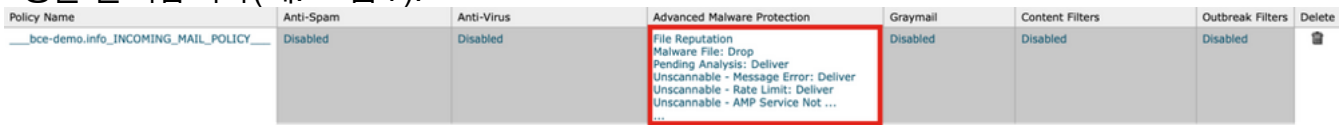

그림 7: MAR 사용(수신 메일 정책)

3. 페이지 아래쪽으로 스크롤합니다.
4. Enable Mailbox Auto Remediation (MAR)(사서함 자동 교정 사용(MAR)) 확인란을 클릭합니다.
5. MAR에 대해 수행할 다음 작업 중 하나를 선택합니다(예: 그림 8). 전달 대상: <*이메일 주소 입력*>삭제전달 대상: <*이메일 주소 입력*> 및 삭제

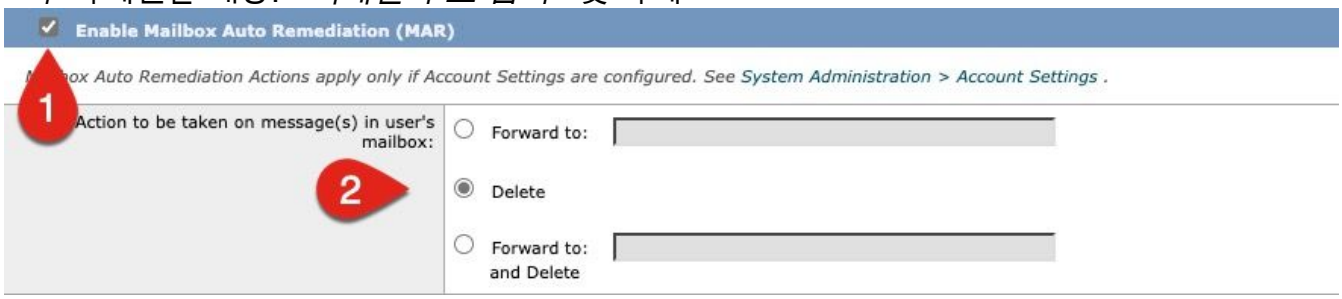

그림 8: AMP용 MAR 구성 예 사용

6. **Submit(제출)을 클릭합니다.**
7. UI의 오른쪽 상단에서 Commit Changes를 클릭합니다.
8. 주석을 입력하고 Commit Changes(변경 사항 커밋)를 클릭하여 컨피그레이션 변경 사항**을 완료합니다.**

URL 필터링을 위해 MAR(Mailbox Auto Remediation) 사용

AsyncOS 14.2 for Cisco Secure Email Cloud Gateway부터 URL 필터링에 URL 회귀적 판정 및 URL 리미디에이션이 포함됩니다.

1. Security **Services(보안 서비스) > URL Filtering(URL 필터링)으로 이동합니다.**
2. URL 필터링이 구성되지 않은 경우 Enable(활성화)을 클릭합니다
3. "Enable URL Category and Reputation Filters(URL 카테고리 및 평판 필터 활성화)"의 확인란

을 클릭합니다.

4. 기본 설정의 고급 설정
5. Submit(제출)을 클릭합니다.

URL 필터링은 다음과 비슷해야 합니다.

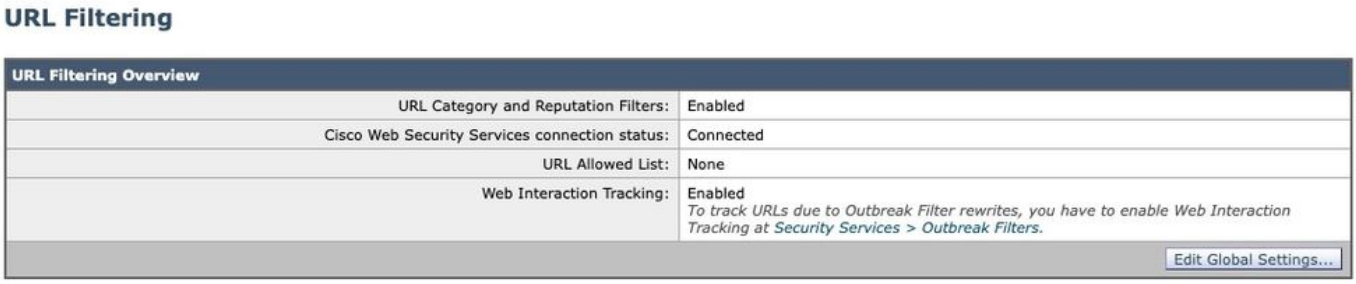

그림 9: URL 필터링 사후 활성화 예

URL 필터링을 통한 URL 회귀 분석을 보려면 다음을 수행하거나 Cisco에서 수행할 지원 케이스를 여십시오.

```
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
```

완료되면 URL Filtering(URL 필터링) 페이지에서 UI를 새로 고침합니다. 이제 다음과 유사한 내용이 표시됩니다.

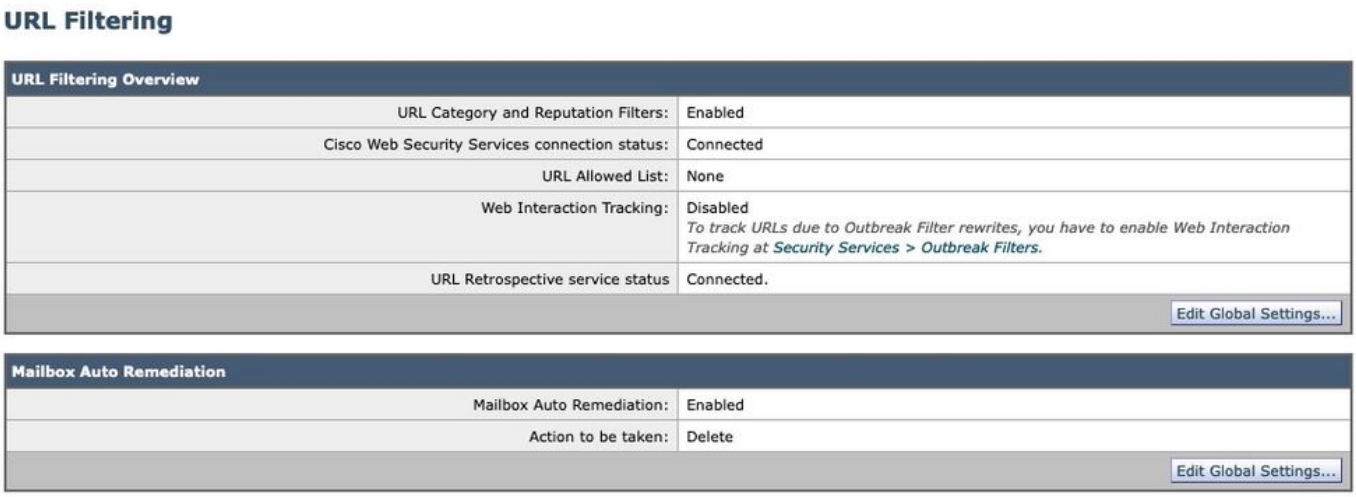

그림 10: URL 필터링(AsyncOS 14.2 for Cisco Secure Email Cloud Gateway)

이제 판정이 점수를 변경하면 URL 보호에서 교정 작업을 수행할 준비가 되었습니다. 자세한 내용은 AsyncOS 14.2 for Cisco Secure Email Cloud Gateway의 User Guide for AsyncOS 14.2에서 Protecting Against Malicious or 바람직하지 않은 URLs를 참조하십시오.

구성 완료!

현재 Cisco Secure Email은 새로운 정보가 제공됨에 따라 새로운 위협을 지속적으로 평가하고, 네트워크에 들어온 후 위협으로 확인된 파일에 대해 알려줍니다.

File Analysis(Cisco Secure Malware Analytics)에서 회귀적 판정을 생성하면 이메일 보안 관리자(구성된 경우)에게 정보 메시지가 전송됩니다. 예:

```
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
```

사서함 자동 교정은 메일 정책에 대해 구성된 경우 구성된 대로 수행됩니다.

사서함 자동 교정 보고서 예

수정된 SHA256에 대한 보고는 Cisco Secure Email Gateway 및 Cisco Secure Email and Web Manager에서 모두 사용할 수 있는 Mailbox Auto Remediation 보고서에 포함됩니다.

Mailbox Auto Remediation

Printable PDF

Time Range: Day

03 Jun 2019 05:00 to 04 Jun 2019 05:39 (GMT +05:00) — Data in time range:99.86 % complete

Advanced Malware Protection Retrospective Security

Displaying 1 - 1 of 1 items.

File SHA-256	Filename	Action Taken	Time When Action Was Issued	Recipients for Whom the Remediation was Successful	Recipients for Whom the Remediation was Unsuccessful
7d06fd22...7c416c4b	Book1.xls	Forward and Delete	04 Jun 2019 04:42:21	robsherw@bce-demo.info	

Displaying 1 - 1 of 1 items.

Columns... | Export...

그림 11: (레거시 UI) 사서함 자동 교정 보고서

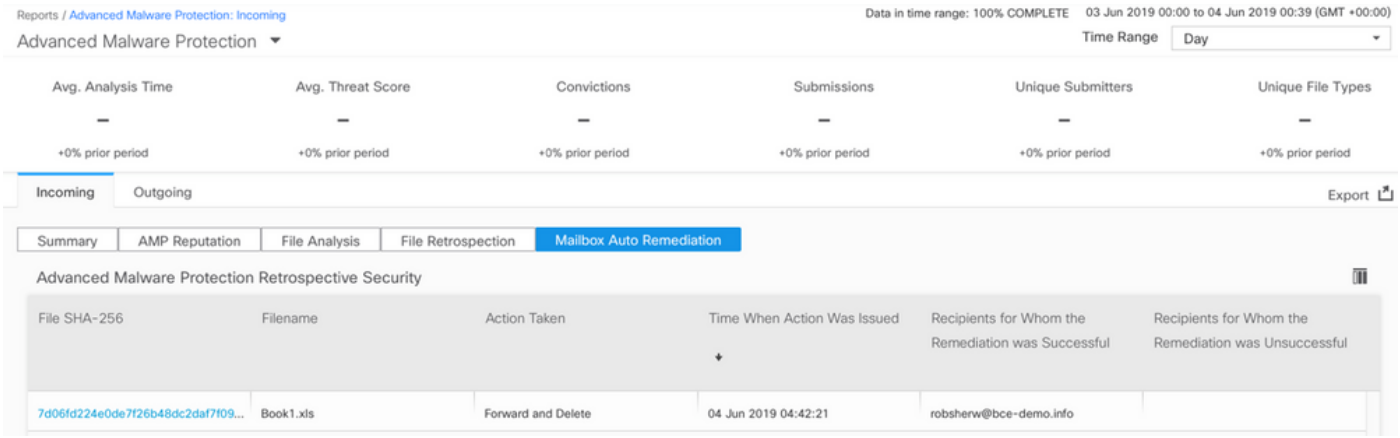

그림 12: (NG UI) 사서함 자동 교정 보고서

사서함 자동 교정 로깅

Mailbox Auto Remediation에는 개별 로그, "3월"이 있습니다. 사서함 자동 교정 로그에는 Cisco Secure Email 게이트웨이와 Microsoft Azure, Microsoft 365 간의 모든 통신 활동이 포함됩니다.

3월 로그의 예:

```
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.
```

Cisco Secure Email Gateway 트러블슈팅

연결 상태 테스트에 대한 성공적인 결과가 표시되지 않으면 Microsoft Azure AD에서 수행된 응용 프로그램 등록을 검토할 수 있습니다.

Cisco Secure Email 게이트웨이에서 MAR 로그를 '추적' 레벨로 설정하고 연결을 다시 테스트합니다.

실패한 연결의 경우 다음과 유사한 로그가 표시될 수 있습니다.

```
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
```

Azure AD에서 응용 프로그램과 함께 로그에서 응용 프로그램 ID, 디렉터리 ID(테넌트 ID와 동일) 또는 기타 연결된 식별자를 확인합니다. 값이 확실하지 않으면 Azure AD 포털에서 응용 프로그램을 삭제하고 다시 시작하십시오.

성공적으로 연결하려면 다음과 유사한 로그가 필요합니다.

```
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 문제 해결

> **참고**: Cisco TAC 및 Cisco Support는 Microsoft Exchange, Microsoft Azure AD 또는 Office 365와 관련된 고객 측 문제를 해결할 권한이 없습니다.

Microsoft Azure AD에 대한 고객 측 문제의 경우 Microsoft 지원에 문의해야 합니다. Microsoft Azure 대시보드에서 "도움말 + 지원" 옵션을 참조하십시오. 대시보드에서 Microsoft 지원에 대한 직접 지원 요청을 열 수 있습니다.

부록 A

참고: Azure 응용 프로그램을 설정하는 데 클라이언트 암호를 사용하지 않는 경우에만 필요합니다.

퍼블릭 및 프라이빗 인증서 및 키 쌍 구축

팁: *$base64Value, $base64Thumbprint 및 $keyid에 대한 출력을 로컬에 저장하도록 하십시오. 이 출력은 구성 단계의 뒷부분에 필요합니다.* 컴퓨터의 사용 가능한 로컬 폴더에 인증서의 .crt 및 관련 .pem을 지정하십시오.

참고: 인증서(x509 형식/표준)와 개인 키가 이미 있는 경우 이 섹션을 건너뜁니다. CRT 파일과 PEM 파일이 모두 있어야 합니다. 이 파일은 다음 섹션에 있어야 합니다!

인증서: Unix/Linux(openssl 사용)

생성할 값:
- **지문**
- **공용 인증서(CRT 파일)**
- **개인 키(PEM 파일)**

제공된 스크립트의 용도와 실행을 위해 Unix/Linux/OS X를 사용하는 관리자는 OpenSSL을 설치한 것으로 가정합니다.

참고: OpenSSL 설치를 확인하려면 'which openssl' 및 'openssl version' 명령을 실행합니다. OpenSSL이 없으면 설치합니다.

자세한 내용은 다음 문서를 참조하십시오. Cisco Secure Email용 Azure AD 구성 스크립트

호스트에서(UNIX/Linux/OS X):

1. 터미널 응용 프로그램의 텍스트 편집기(또는 셸 스크립트를 만드는 것이 편하지만) 다음 항목을 복사하여 스크립트를 만듭니다.
   https://raw.githubusercontent.com/robsherw/my_azure/master/my_azure.sh

2. 스크립트 붙여넣기
3. 스크립트를 실행 가능하게 만들어야 합니다! 다음 명령을 실행합니다. **chmod u+x my_azure.sh**
4. 스크립트 실행: **./my_azure.sh**

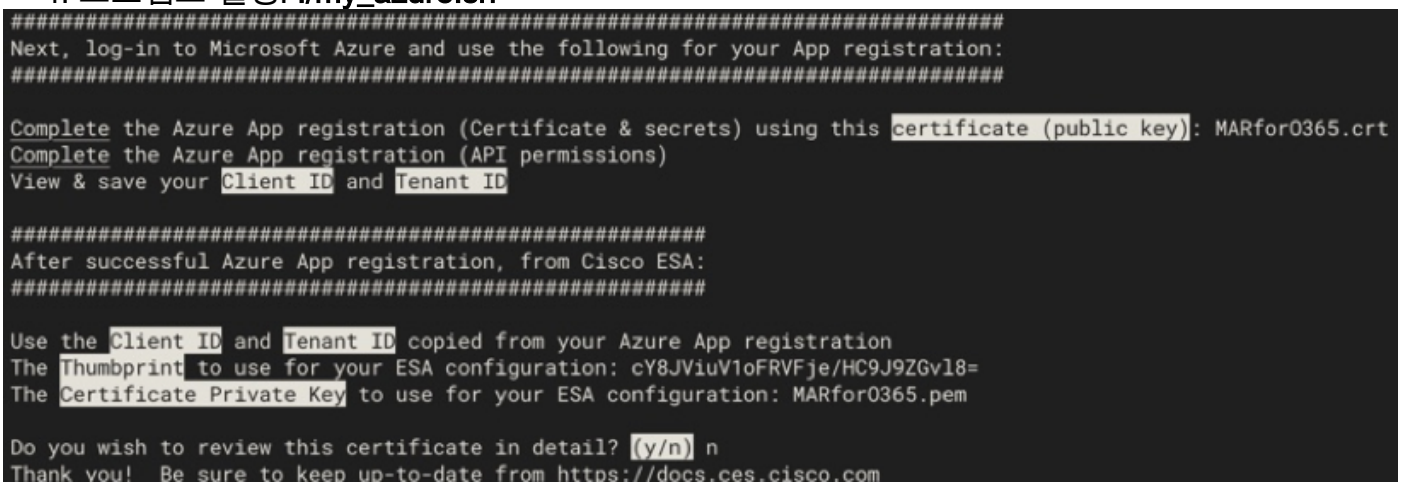

그림 13: my_azure.sh의 화면 출력

그림 2에서 볼 수 있듯이 스크립트는 Azure 앱 등록에 필요한 **공용 인증서(CER 파일)**를 빌드하고 호출합니다. 스크립트에서***지문***및***인증서 개인 키(PEM 파일)***Configuring Cisco Secure Email(Cisco 보안 이메일 구성) 섹션에서 을(를) 사용합니다.

Microsoft Azure에서 응용 프로그램을 등록하는 데 필요한 값이 있습니다.

[다음 섹션을 건너뜁니다! "Cisco Secure Email과 함께 사용할 Azure 앱 등록"으로 이동하십시오.]

인증서: Windows(PowerShell 사용)

Windows를 사용하는 관리자의 경우 애플리케이션을 활용하거나 자체 서명 인증서를 만드는 데 필요한 지식을 보유해야 합니다. 이 인증서는 Microsoft Azure 응용 프로그램을 만들고 API 통신을 연결하는 데 사용됩니다.

생성할 값:
- **지문**
- **공용 인증서(CRT 파일)**
- **개인 키(PEM 파일)**

자체 서명 인증서를 만드는 이 문서의 예는
XCA(https://hohnstaedt.de/xca/,https://sourceforge.net/projects/xca/)를 사용합니다.

참고: XCA는 Mac, Linux 또는 Windows용으로 다운로드할 수 있습니다.

1. 인증서 및 키에 대한 데이터베이스를 생성합니다.
   a. 도구 모음에서 파일 선택
   b. 새 **데이터베이스 선택**
   c. 데이터베이스의 비밀번호를 생성합니다.
   (나중에 수행해야 하므로 기억하십시오!)
2. Certificates(인증서) 탭을 클릭한 다음 New Certificate(**새 인증서**)를 클릭합니다.
3. 제목 탭을 클릭하고 다음을 입력합니다.
   a. 내부 이름
   b. 국가 이름
   c. 주/도 이름
   d. localityName
   e. 조직 이름
   f. OU(조직 구성 단위 이름)
   g. commonName(CN)
   h. 이메일 주소
4. Generate a **New Key(새 키 생성)를 클릭합니다.**
5. 팝업에서 제공된 정보를 확인합니다.
(필요에 따라 변경):
   a. 이름
   b. 키 유형: RSA
   c. 키 크기: 2048비트
   d. Create(생성)를 클릭합니다.
   e. **확인**을 클릭하여 "Successfully created the RSA private key 'Name'" 팝업 창을 승인합니다.

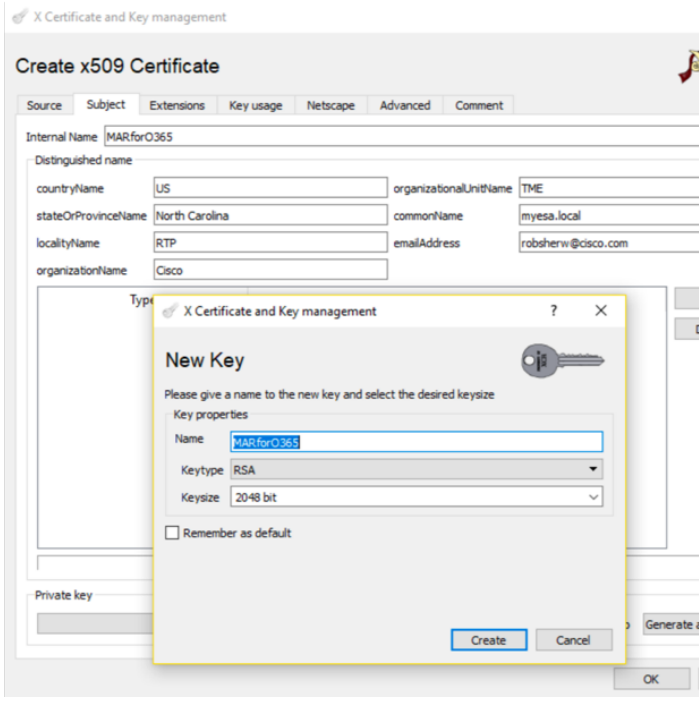

그림 14: XCA 사용(3~5단계)

6. 키 사용 탭을 클릭하고 다음을 선택합니다.
   a. X509v3 키 사용에서 다음을 수행합니다.
   디지털 서명, 키 암호화
   b. X509v3 확장 키 사용에서 다음을 수행합니다.
   이메일 보호

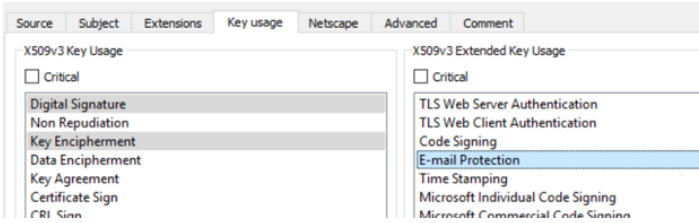

그림 15: XCA 사용(6단계)

7. **OK(확인)**를 클릭하여 인증서 변경 사항을 적용합니다.
8. "Successfully created the certificate '*Name*'" 팝업 창을 확인 **클릭**

그런 다음 PowerShell 명령에서 사용하고 Cisco Secure Email 구성 단계에서 사용할 **퍼블릭 인증서 (CER 파일)** 및 ***PEM 파일***을 모두 내보내려고 합니다.

1. 를 클릭하고 새로 만든 인증서의 Internal Name(내부

이름)을 강조 표시합니다.
2. 내보내기를 **클릭합니다.**
    a. 액세스 용이성을 위해 저장 디렉토리를 설정합니다(필요에 따라 변경).
    b. Export Format(내보내기 형식)이 PEM**(.crt)으로 설정되었는지 확인합니다.**
    c. **확인**을 클릭합니다.

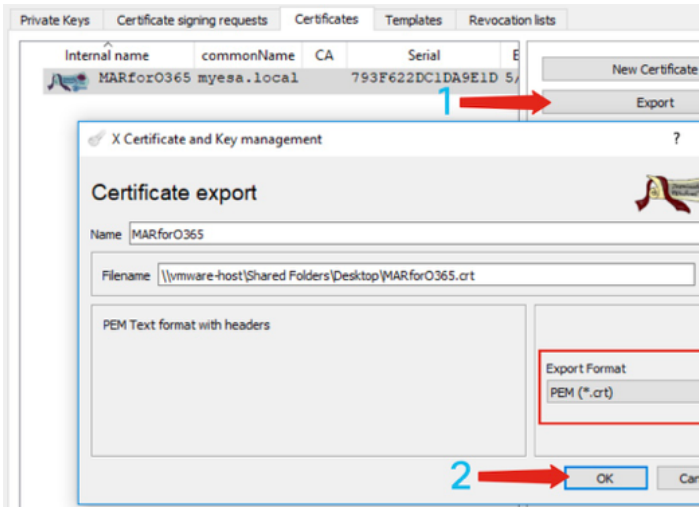

그림 16: XCA 사용(CRT 내보내기)(1-2단계)

3. **개인 키** 탭을 클릭합니다.
4. 를 클릭하고 새로 만든 인증서의 Internal Name(내부 이름)을 선택합니다.
5. 내보내기를 **클릭합니다.**
    a. 액세스 용이성을 위해 저장 디렉토리를 설정합니다(필요에 따라 변경).
    b. Export Format(내보내기 형식)이 PEM **private(.pem)으로 설정되었는지 확인합니다.**
    c. **확인**을 클릭합니다.
6. XCA를 종료하고 닫습니다.

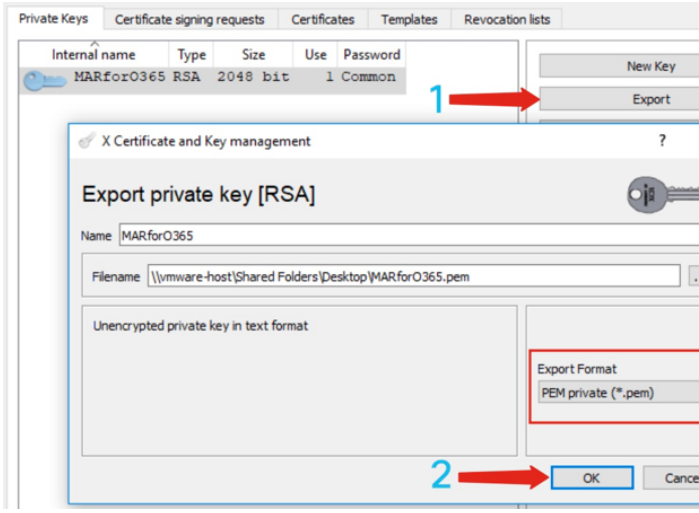

그림 17: XCA 사용(PEM 내보내기)(3~5단계)

마지막으로, 생성한 인증서를 가져가서 Cisco Secure Email 구성에 필요한 **지문**을 추출합니다.

1. Windows PowerShell을 사용하여 다음을 실행합니다.

```
$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. 다음 단계에 대한 값을 가져오려면 파일에 저장하거나 클립보드에 복사합니다.

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

```
$base64Thumbprint
```

참고: “c:\Users\joe\Desktop..." 출력을 저장할 PC의 위치입니다.

PowerShell 명령을 실행할 때의 예상 출력은 다음과 유사해야 합니다.

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

보시다시피 PowerShell 명령은 *base64Thumbprint를* 호출합니다. 이는 Cisco Secure Email 게이트웨이 구성에 필요한 지문입니다.

또한 Azure 앱 등록에 필요한 **공용 인증서(CER 파일)**를 만들었습니다. 그리고 Configuring Cisco Secure Email(Cisco 보안 이메일 구성) 섹션에서 사용할 ***Certificate Private Key(PEM 파일)***를 생성했습니다.

Microsoft Azure에서 응용 프로그램을 등록하는 데 필요한 값이 있습니다!

[Cisco Secure Email과 함께 사용할 Azure 앱 등록"으로 이동하십시오.]

부록 B

참고: 이 작업은 게이트웨이에서 AsyncOS 11.x 또는 12.x for Email을 실행하는 경우에만 필요합니다.

API 권한(AsyncOS 11.x, 12.x)

응용 프로그램 창의 관리 옵션에서

1. **API 권한 선택**
2. **+ 권한 추가를 클릭합니다.**
3. 아래로 스크롤하여 Supported **legacy APIs(지원되는 레거시 API**)로 이동하고 **Exchange**를 선택합니다.
4. 위임된 권한에 대해 아래 권한을 선택하십시오. EWS > "EWS.AccessAsUser.All"(Exchange Web Services를 통해 서명된 사용자로 사서함 액세스)Mail(메일) > "Mail.Read"(사용자 메일 읽기)Mail(메일) > "Mail.ReadWrite"(사용자 메일 읽기 및 쓰기)Mail(메일) > "Mail.Send(메일 보내기)"(메일로 메일 보내기)
5. 창 맨 위로 스크롤...
6. 응용 프로그램 사용 권한에 대해 아래 사용 권한을 선택하십시오. "full_access_as_app"(모든

사서함에 대한 전체 액세스 권한을 가진 Exchange 웹 서비스 사용)Mail(메일) > "Mail.Read"(사용자 메일 읽기)Mail(메일) > "Mail.ReadWrite"(사용자 메일 읽기 및 쓰기)Mail(메일) > "Mail.Send(메일 보내기)"(메일로 메일 보내기)

7. *선택 사항:* Microsoft Graph는 기본적으로 "User.Read" 권한에 대해 활성화되어 있습니다. 이 항목을 구성된 상태로 두거나 **읽기**를 클릭하고 **제거 권한**을 클릭하여 응용 프로그램과 연결된 API 권한에서 제거할 수 있습니다.
8. **권한 추가**(또는 **Microsoft Graph**가 이미 나열된 경우 권한 업데이트)를 클릭합니다.
9. 마지막으로, **Grant admin consent for..(관리자 동의 권한 부여...)를** 클릭합니다**.** 새 사용 권한이 응용 프로그램에 적용되는지 확인합니다.
10. 다음과 같은 메시지가 표시되는 팝업 창이 나타납니다.

"*<Azure Name>의 모든 계정에 대해 요청된 권한에 동의하시겠습니까? 그러면 이 애플리케이션이 이미 아래 나열된 것과 일치해야 하는 기존 관리자 동의 레코드가 업데이트됩니다.*"

예를 클릭합니다.

이 시점에서는 다음과 같이 녹색 성공 메시지가 표시되고 "Admin Consent Required(관리자 동의 필수)" 열에 Granted(부여됨)가 표시됩니다.

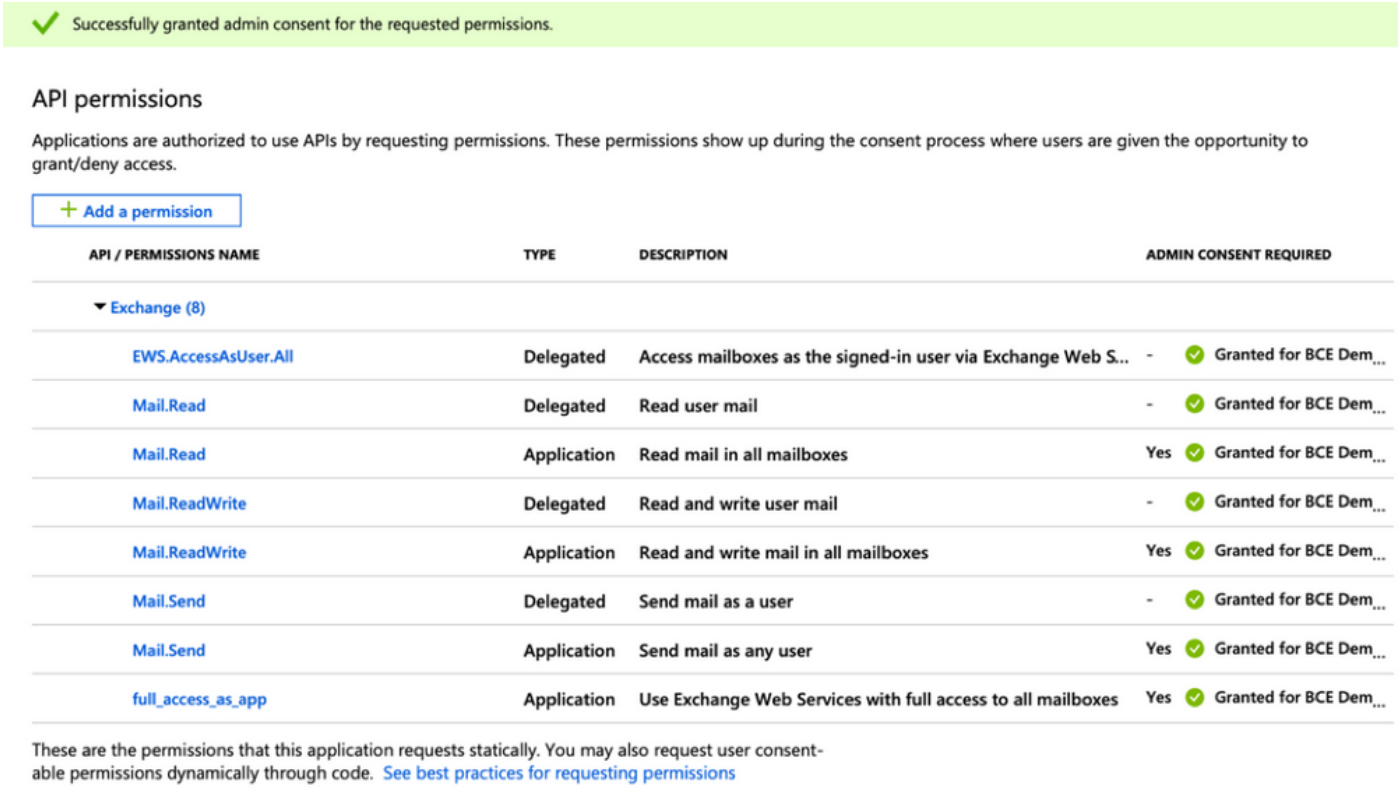

그림 18: Microsoft Azure 앱 등록(API 권한 필요)

[Cisco Secure Email과 함께 사용할 Azure 앱 등록"으로 이동하십시오.]

관련 정보

- Cisco Email Security Appliance - 제품 지원
- Cisco Email Security Appliance - 릴리스 정보
- Cisco Email Security Appliance - 최종 사용자 가이드