Microsoft Azure(Microsoft 365)API用のCisco Secure Email Account Settingsの設定方法

内容

はじめに

- メールボックスの自動修復のプロセスフロー

前提条件

Cisco Secure Emailで使用するAzureアプリを登録する

- アプリケーション登録
- 証明書とシークレット
- APIアクセス許可
- クライアントIDとテナントIDの取得

Cisco Secure Email Gateway/クラウドゲートウェイの設定

- アカウントプロファイルの作成
- 接続の確認
- メールポリシーで高度なマルウェア防御のためのメールボックス自動修復(MAR)を有効にする
- URLフィルタリングのメールボックス自動修復(MAR)を有効にする

メールボックス自動修復レポートの例

メールボックス自動修復ログ

Cisco Secure Email Gatewayのトラブルシューティング

Azure ADのトラブルシューティング

付録 A

- 公開および秘密の証明書と鍵のペアの構築
  - 証明書：Unix/Linux（openssl を使用）
  - 証明書： Windows（PowerShellを使用）

付録 B

- API権限(AsyncOS 11.x、12.x)

関連情報

はじめに

このドキュメントでは、Microsoft Azure(Azure Active Directory)に新しいアプリケーションを登録して、必要なクライアントID、テナントID、クライアント資格情報を生成し、Cisco Secure Email Gatewayまたはクラウドゲートウェイのアカウント設定を構成する手順を順を追って説明します。メール管理者がCisco Secure Email and Web ManagerまたはCisco Secure Gateway/Cloud Gatewayで高度なマルウェア防御(AMP)またはURLフィルタリング用のメールボックス自動修復(MAR)を設定する場合、またはメッセージトラッキングからの修復アクションを利用する場合、アカウント設定および関連するアカウントプロファイルの設定が必要です。

メールボックスの自動修復のプロセスフロー

電子メールまたはURLの添付ファイルは、ユーザーのメールボックスに到達した後でも、いつでも悪意のあるファイルとしてマークされる可能性があります。Cisco Secure Email上のAMP（Cisco Secureマルウェア分析を使用）は、新しい情報が出現したときにこの開発を特定し、レトロスペクティブアラートをCisco Secure Emailにプッシュします。Cisco Talosは、AsyncOS 14.2 for Cisco Secure Email Cloud Gatewayの時点でURL分析と同じ機能を提供します。 組織でMicrosoft 365を使用してメールボックスを管理している場合は、Cisco Secure Emailを設定して、これらの脅威の判定が変更されたときに、ユーザのメールボックス内のメッセージに対して自動修復処理を実行できます。

Cisco Secure Emailは、Microsoft Azure Active Directoryと安全かつ直接通信し、Microsoft 365メールボックスにアクセスできるようにします。 たとえば、添付ファイルを含む電子メールがゲートウェイで処理され、AMPによってスキャンされる場合、ファイルのレピュテーションのために添付ファイル(SHA256)がAMPに提供されます。 AMPの評価はClean（手順5、図1）としてマーク付けされ、その後受信者のMicrosoft 365メールボックスに配信されます。 その後、AMPの評価がMaliciousに変更され、Cisco Malware Analyticsは、その特定のSHA256を処理した任意のゲートウェイにレトロスペクティブ判定更新（ステップ8、図1）を送信します。ゲートウェイがMalicious（設定されている場合）のレトロスペクティブ判定更新を受信すると、ゲートウェイは、メールボックス自動修復(MAR)アクションの1つを実行します。

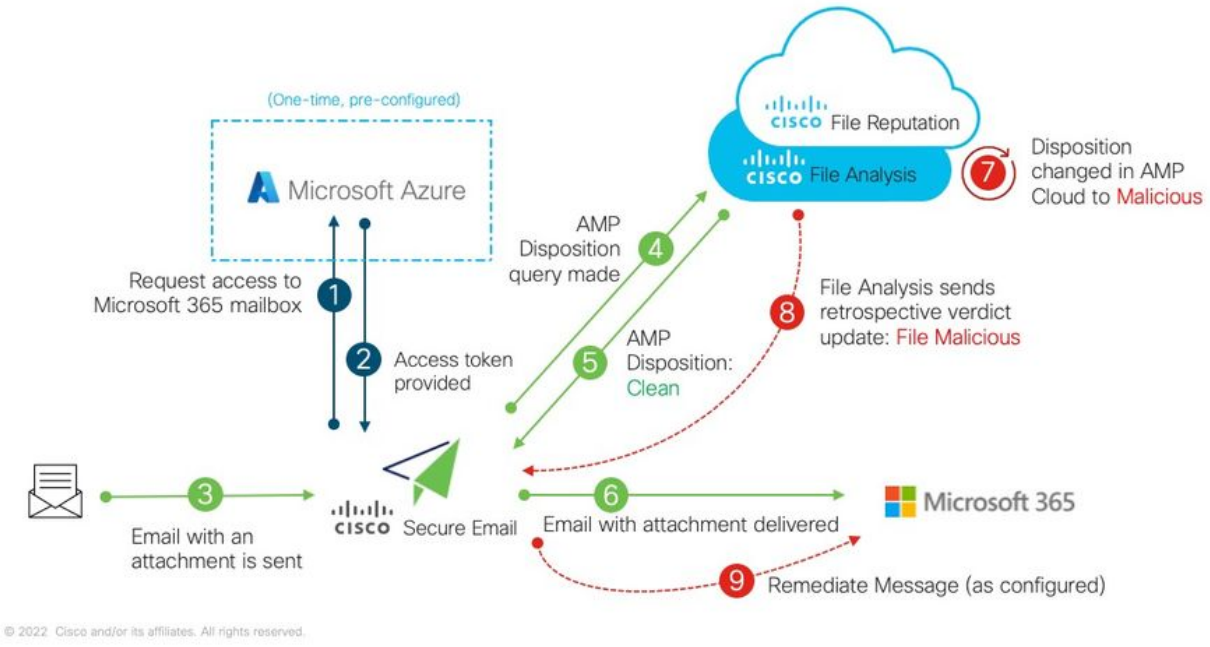


図1: Cisco Secure Emailの3月（AMP用）

このガイドでは、メールボックス自動修復のためだけにMicrosoft 365を使用してCisco Secure Emailを設定する方法について説明します。 ゲートウェイでのAMP（ファイルレピュテーションとファイル分析）やURLフィルタリングは、事前に設定しておく必要があります。 ファイルレピュテーションとファイル分析の詳細については、導入したAsyncOSのバージョンに対応するユーザガイドを参照してください。

前提条件

1. Microsoft 365アカウントサブスクリプション（Microsoft 365アカウントサブスクリプションに、Enterprise E3またはEnterprise E5アカウントなどのExchangeへのアクセスが含まれていることを確認してください）。

2. Microsoft Azure管理者アカウントとhttp://portal.azure.comへのアクセス

3. Microsoft 365とMicrosoft Azure ADアカウントは両方ともアクティブな「user@domain.com」電子メールアドレスに正しく関連付けられており、その電子メールアドレスを使用して電子メールを送受信できます。

Microsoft Azure ADへのCisco Secure Email Gateway API通信を設定するために、次の値を作成します。

- クライアント ID
- テナントID
- クライアントシークレット

注: AsyncOS 14.0以降では、アカウント設定により、Microsoft Azureアプリ登録の作成時にクライアントシークレットを使用した構成が可能です。これは簡単で推奨される方法です。

オプション：クライアントシークレットを使用しない場合は、次のものを作成し、準備しておく必要があります。

- 拇印
- 秘密鍵（PEMファイル）

拇印と秘密キーの作成については、このガイドの付録で説明します。

1. アクティブなパブリック（またはプライベート）証明書(CER)と証明書の署名に使用される秘密キー(PEM)、またはパブリック証明書(CER)を作成する機能と、証明書の署名に使用される秘密キー(PEM)を保存する機能。この作業を管理者の好みに基づいて行うには、次の2つの方法があります。
    1. 証明書：Unix/Linux/OS X（OpenSSLを使用）
    2. 証明書： Windows （PowerShellを使用）

2. Windows PowerShellへのアクセス（通常はWindowsホストまたはサーバから管理、またはUnix/Linux経由でターミナルアプリケーションにアクセス）

これらの必須値を設定するには、このドキュメントで説明する手順を実行する必要があります。

Cisco Secure Emailで使用するAzureアプリを登録する

アプリケーション登録

Microsoft Azureポータルにログインします

1. Azure Active Directoryをクリックします（図2）

2. App registrationsをクリックします。

3. + New registrationをクリックします。

4. 「アプリケーションの登録」ページで、次の操作を行います。

a.名前：Cisco Secure Email MAR（または任意の名前）
b.サポートされているアカウントタイプ：この組織ディレクトリのアカウントのみ（アカウント名）
c.リダイレクトURI:（オプション）

[注：空欄のままにするか、https://www.cisco.com/sign-onを使用して情報を入力してください]
d.ページの下部で、Registerをクリックします。

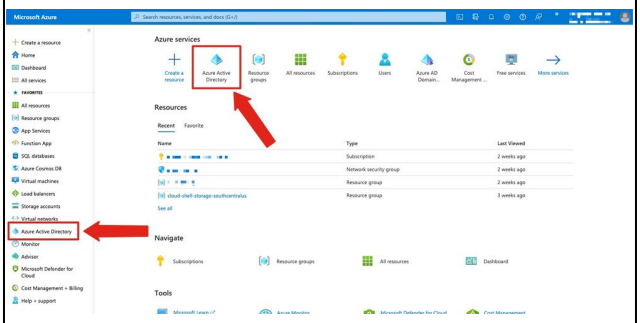


図2: Microsoft Azureポータルの例

上記の手順が完了すると、アプリケーションが表示されます。

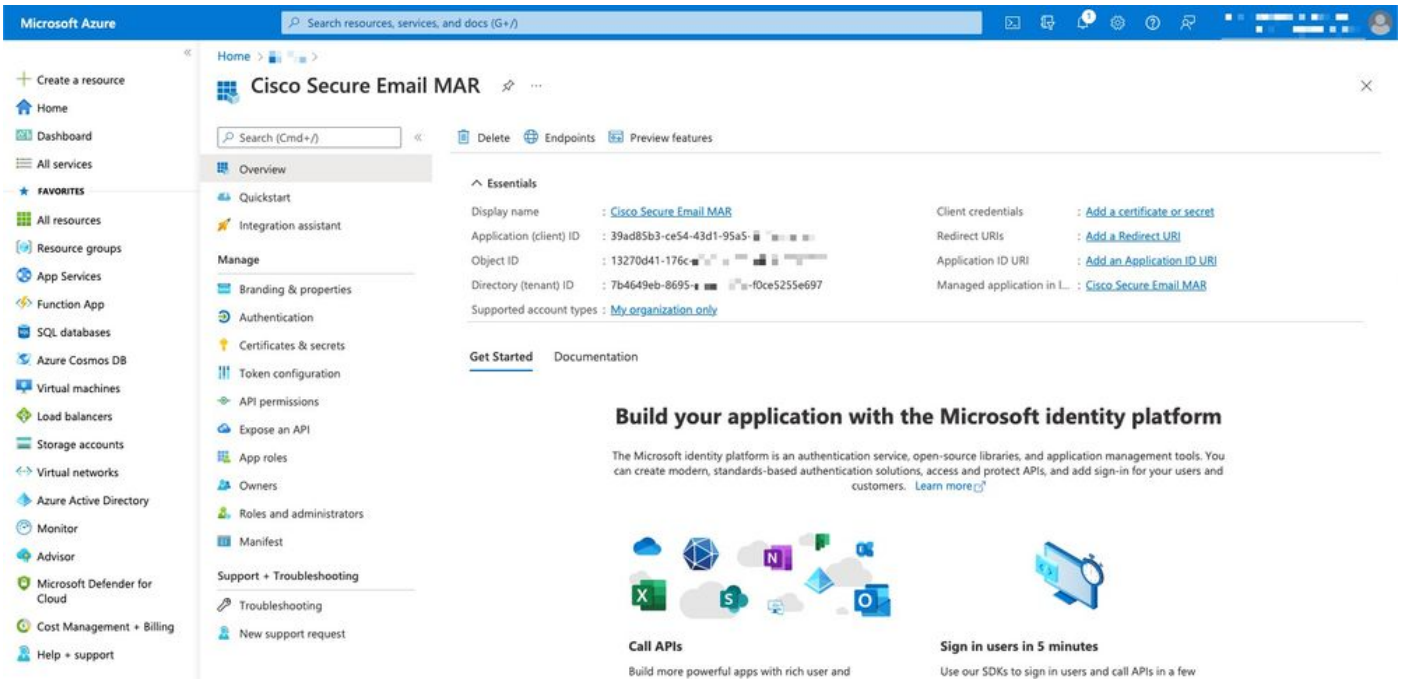


図3: Microsoft Azure Active Directoryアプリケーションページ

証明書とシークレット

AsyncOS 14.0以降を実行している場合は、クライアントシークレットを使用するようにAzureアプリを構成することをお勧めします。 アプリケーション・ペインの[管理オプション]で、次の操作を行います。

1. 証明書とシークレットを選択します

2. [クライアントシークレット]セクションで、[+新しいクライアントシークレット]をクリックします

3. クライアントシークレットの目的を識別するのに役立つ説明を追加します（例：「Cisco Secure Email remediation」）。

4. 有効期限を選択します

5. Addをクリックします。

6. 生成された値の右側にマウスを置き、Copy to Clipboardアイコンをクリックします

7. この値をメモに保存し、「Client secret」としてメモします。

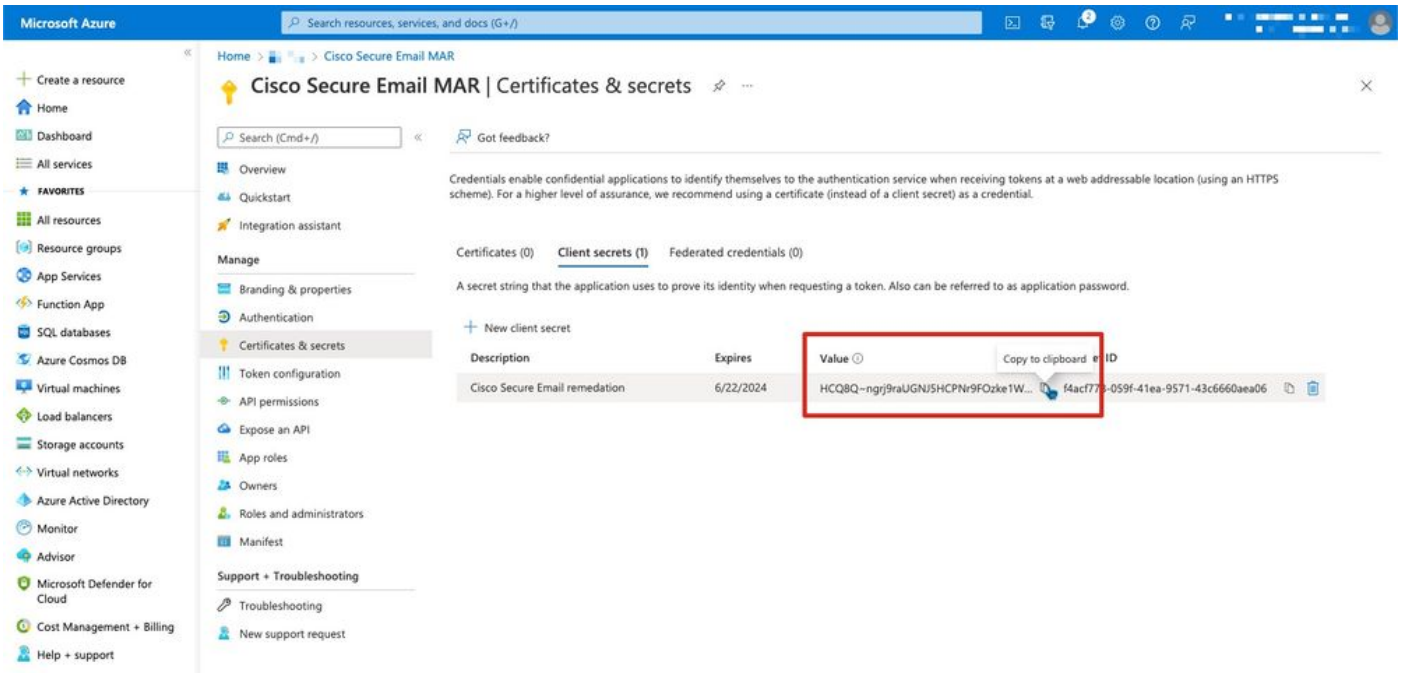


図4: Microsoft Azureのクライアントシークレットの作成の例

注：アクティブなMicrosoft Azureセッションを終了すると、生成したクライアントシークレットの値によって値が***き出されます。 終了する前に値を記録して保護しない場合は、クリアテキストの出力を確認するために、クライアントシークレットを再作成する必要があります。

オプション：クライアントシークレットを使用してAzureアプリケーションを構成しない場合は、証明書を使用するようにAzureアプリを構成してください。 アプリケーション・ペインの[管理オプション]で、次の操作を行います。

1. 証明書とシークレットの選択
2. Upload certificateをクリックします。
3. CRTファイルを選択します（以前に作成したファイルと同様）。
4. [Add] をクリックします。

APIアクセス許可

注：AsyncOS 13.0 for Email Security以降では、Microsoft AzureからCisco Secure Email Communicationに必要なAPI権限が、Microsoft ExchangeからMicrosoft Graphに変更されました。 MARをすでに設定していて、既存のCisco Secure Email GatewayをAsyncOS 13.0にアップグレードする場合は、新しいAPI権限を更新または追加するだけで済みます。 (古いバージョンのAsyncOS（11.xまたは12.x）を実行している場合は、続行する前に「付録B」を参照してください)。

アプリケーション・ペインの[管理オプション]で、次の操作を行います。

1. APIアクセス許可の選択
2. +権限の追加をクリックします
3. Microsoft Graphを選択します
4. アプリケーション権限に対して次の権限を選択します。
    1. Mail > "Mail.Read"（すべてのメールボックスのメールを読む）
    2. Mail > "Mail.ReadWrite"（すべてのメールボックスのメールの読み書き）
    3. Mail >「Mail.Send」（任意のユーザとしてメールを送信）
    4. Directory > "Directory.Read.All"（ディレクトリデータを読み取る）[*オプション：LDAPコネクタ/LDAP同期を使用している場合は、有効にします。 そうでない場合、これは必要ありません。]
5. オプション：デフォルトでMicrosoft Graphの「User.Read」権限が有効になっていることが表示されます。この権限は設定したままにしておくか、または「Read」をクリックして「Remove permission」をクリックし、アプリケーションに関連付けられているAPI権限から削除します。
6. 権限の追加(Microsoft Graphがすでにリストされている場合は、権限の更新)をクリックします
7. 最後に、Grant admin consent for...をクリックして、新しい権限がアプリケーションに適用されていることを確認します
8. 次の内容を確認するポップアップウィンドウが表示されます。

    '<Azure Name>のすべてのアカウントに対して、要求されたアクセス許可の同意を付与しますか？これにより、このアプリケーションがすでに持っている既存の管理者の同意レコードが、以下にリストされているものと一致する必要があります。」

    Yesをクリックします。

この時点で、成功を示すメッセージが緑色で表示され、「Admin Consent Required」列に「Granted」と表示されます。

クライアントIDとテナントIDの取得

アプリケーション・ペインの[管理オプション]で、次の操作を行います。

1. Overviewをクリックします
2. アプリケーション（クライアント）IDの右側にマウスを置き、Copy to Clipboardアイコンをクリックします
3. この値をメモに保存し、「Client ID」としてメモします。
4. ディレクトリ（テナント）IDの右側にマウスを置き、「クリップボードにコピー」アイコンをクリックします
5. この値をメモに保存し、「テナントID」としてメモします。

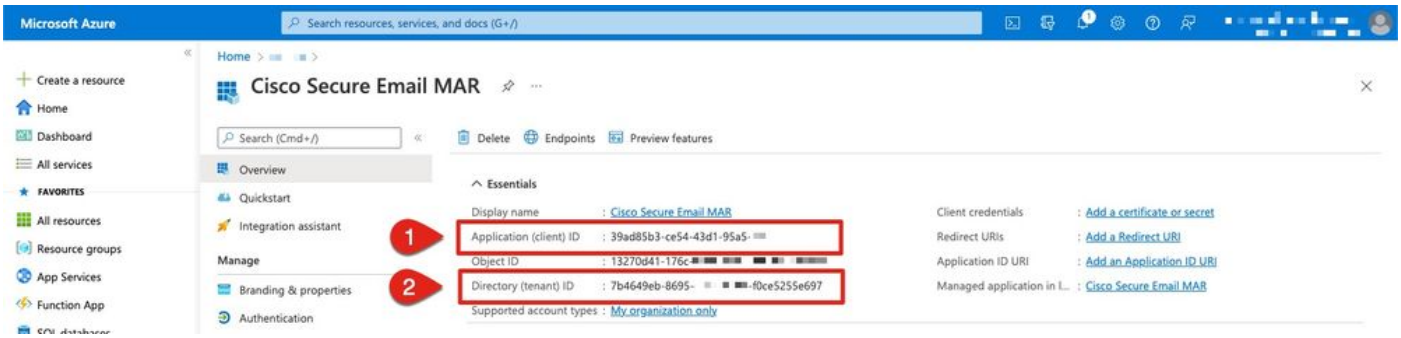


図5: Microsoft Azure...クライアントID、テナントIDの例

Cisco Secure Email Gateway/クラウドゲートウェイの設定

この時点で、次の値を準備してノートに保存する必要があります。

- クライアント ID
- テナントID
- クライアントシークレット

クライアントシークレットを使用していない場合は、オプションです。

- 拇印
- 秘密鍵（PEMファイル）

これで、ノートで作成した値を使用して、Cisco Secure Email Gatewayでアカウント設定を構成する準備が整いました。

アカウントプロファイルの作成

1. ゲートウェイにログインします
2. System Administration > Account Settingsの順に移動します。
    - 注：AsyncOS 13.x以前のバージョンを実行している場合は、System Administration > Mailbox Settingsになります。
3. Enableをクリックします。
4. [アカウント設定を有効にする]チェックボックスをオンにし、[送信]をクリックします
5. Create Account Profileをクリックします。
6. プロファイル名と説明を入力します（複数のドメインがある場合は、アカウントを一意に説明します）。
7. Microsoft 365接続を定義するときは、プロファイルタイプをOffice 365 / ハイブリッド(Graph API)のままにします
8. クライアントIDを入力します。

9. テナントIDを入力します
10. Azureで構成したクライアントクレデンシャルの場合は、次のいずれかを実行します。
    1. Client Secretをクリックし、設定したクライアントシークレットを貼り付けます。
    2. Client Certificateをクリックし、拇印を入力します。また、「Choose File」をクリックしてPEMを指定します。
11. [Submit] をクリックします。
12. UIの右上にあるCommit Changesをクリックします
13. コメントを入力し、Commit Changesをクリックして設定の変更を完了します。

接続の確認

次の手順は、Cisco Secure Email GatewayからMicrosoft AzureへのAPI接続を確認することだけです。

1. 同じAccount Detailsページで、Test Connectionをクリックします。
2. Microsoft 365アカウントで管理されているドメインの有効な電子メールアドレスを入力してください
3. Test Connectionをクリックします。
4. 成功メッセージが表示されます（図6）
5. 完了するにはDoneをクリックします

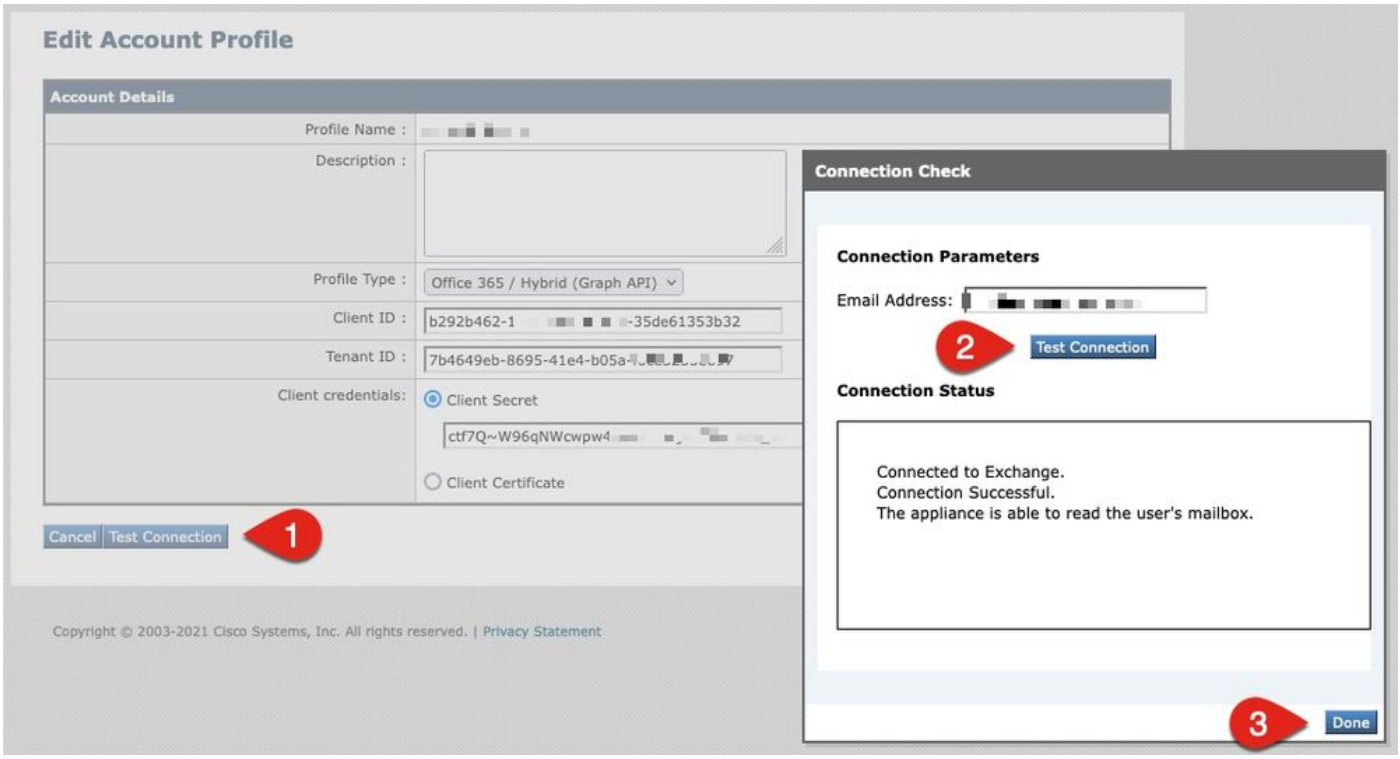


図6：アカウントプロファイル/接続チェックの例

6. [ドメインマッピング]セクションで、[ドメインマッピングの作成]をクリックします

7. API接続を検証したMicrosoft 365アカウントに関連付けられているドメイン名を入力します

メールボックスプロファイルのマッピングに使用できる有効なドメイン形式のリストを次に示します。

– ドメインには、デフォルトのドメインマッピングを作成するためにすべてのドメインに一致する特別なキーワード「ALL」を指定できます。

- 「example.com」などのドメイン名：このドメインのアドレスに一致します。

- '@.partial.example.com'などの部分的なドメイン名 – このドメインで終わるアドレスに一致します

– ドメインのコンマ区切りリストを使用して、複数のドメインを入力できます。

8. 「送信」をクリックします。

9. UIの右上にあるCommit Changesをクリックします

10. コメントを入力し、Commit Changesをクリックして設定の変更を完了します。

メールポリシーで高度なマルウェア防御のためのメールボックス自動修復(MAR)を有効にする

メールポリシーのAMP設定でMARを有効にするには、次の手順を実行します。

1. Mail Policies > Incoming Mail Policiesの順に移動します。
2. 設定するポリシー名のAdvanced Malware Protection列の設定をクリックします（図7など）。

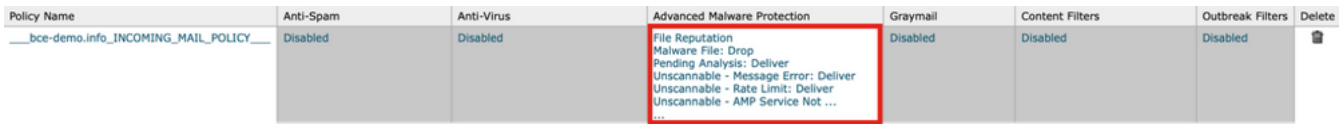


図7: MAR（受信メールポリシー）を有効にする

3. ページの一番下までスクロールします
4. メールボックスの自動修復を有効にする(MAR)チェックボックスをクリックします。
5. MARに対して実行するアクションを次から1つ選択します（図8など）。
   - 転送先： <電子メールアドレスを入力>
   - [削除（Delete）]
   - 転送先：<電子メールアドレスを入力>および削除

図8:AMPのMARを有効にする設定例

6. [Submit] をクリックします。
7. UIの右上にあるCommit Changesをクリックします
8. コメントを入力し、Commit Changesをクリックして設定の変更を完了します。

URLフィルタリングのメールボックス自動修復(MAR)を有効にする

AsyncOS 14.2 for Cisco Secure Email Cloud Gatewayから、URLフィルタリングにURLレトロスペクティブ判定およびURL修復が含まれるようになりました。

1. Security Services > URL Filteringの順に移動します。
2. URLフィルタリングが設定されていない場合は、Enableをクリックします。
3. 「Enable URL Category and Reputation Filters」チェックボックスをクリックします。
4. デフォルト設定の詳細設定
5. [Submit] をクリックします。

URLフィルタリングは次のようになります。

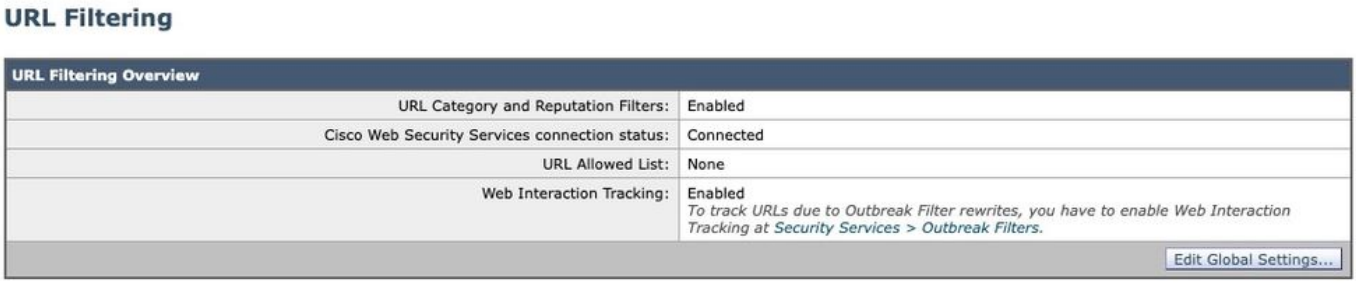


図9：イネーブル後のURLフィルタリングの例

URLフィルタリングを組み込んだURLレトロスペクションを表示するには、次の手順を実行するか、シスコが実行するサポートケースをオープンします。

<#root>

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
```

完了したら、URL FilteringページのUIを更新すると、次のような画面が表示されます。

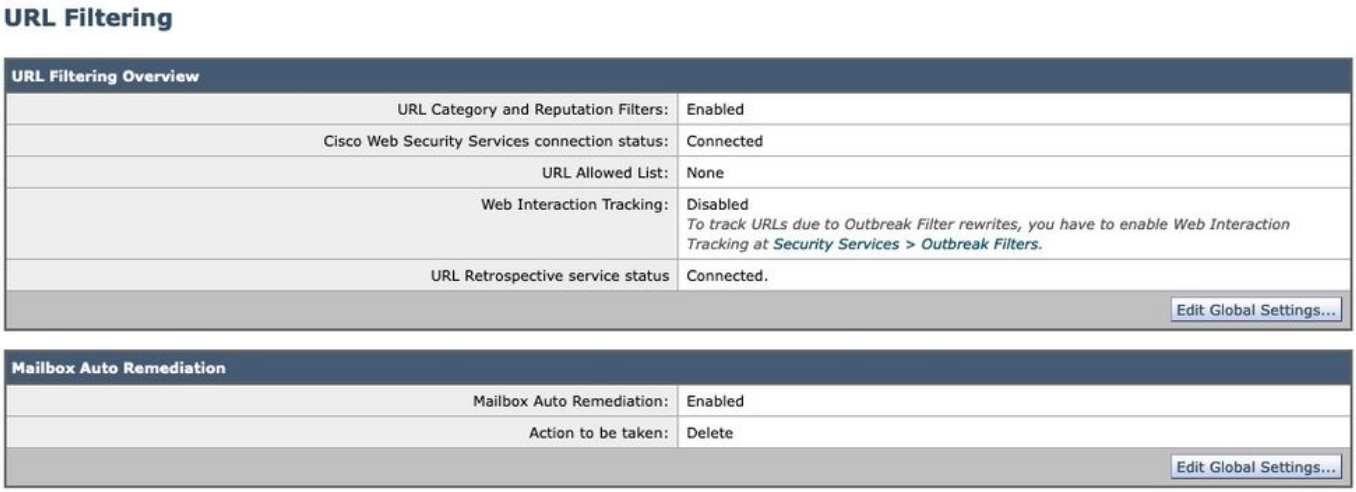


図10:URLフィルタリング（Cisco Secure Email Cloud Gateway向けAsyncOS 14.2）

URL保護は、判定のスコアが変更されたときに修復措置を実行する準備が整いました。 詳細については、『AsyncOS 14.2 for Cisco Secure Email Cloud Gatewayユーザガイド』の「悪意のあるURLまたは望ましくないURLからの保護」を参照してください。

設定が完了しました。

現時点では、Cisco Secure Emailは、新しい情報が入手可能になったときに新たな脅威を継続的に評価し、ネットワークに侵入した後に脅威と判定されたファイルについて通知する準備が整っています。

ファイル分析(Cisco Secure Malware Analytics)からレトロスペクティブ判定が生成されると、情報メッセージがEメールセキュリティ管理者（設定されている場合）に送信されます。 以下に例を挙げます。

```
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
```

メールボックス自動修復は、メールポリシーに対して設定されている場合は、設定されているとおりに実行されます。

メールボックス自動修復レポートの例

修復されたSHA256のレポートは、Cisco Secure Email GatewayとCisco Secure Email and Web Managerの両方で利用可能なメールボックス自動修復レポートに含まれます。

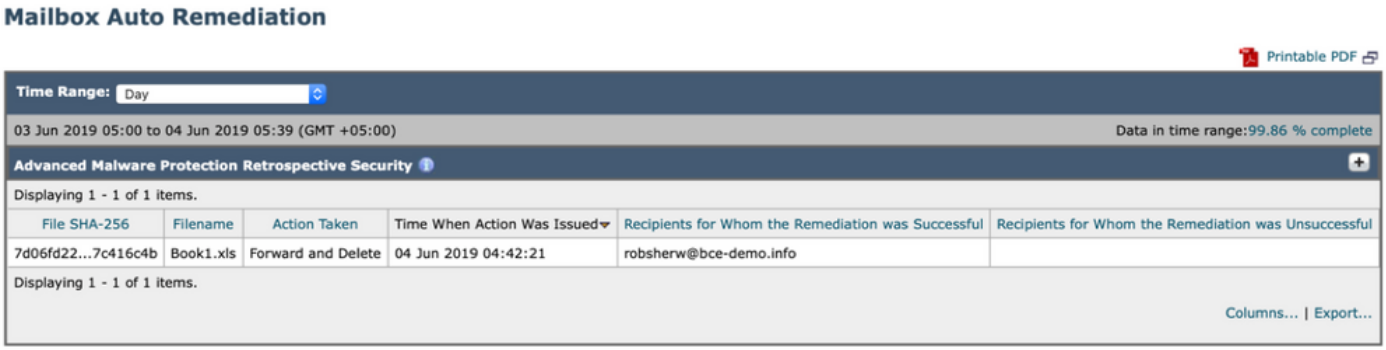


図11: (レガシーUI) メールボックス自動修復レポート

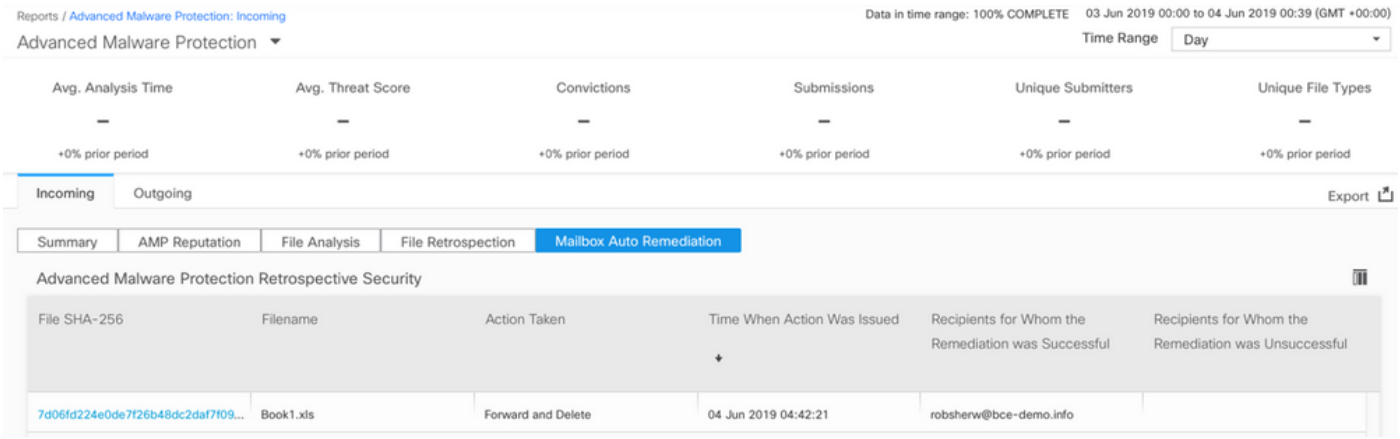


図12:(NG UI)メールボックス自動修復レポート

メールボックス自動修復ログ

メールボックス自動修復には、個別のログ「mar」があります。 メールボックス自動修復ログには、Cisco Secure Email GatewayとMicrosoft Azure(Microsoft 365)間のすべての通信アクティビティが含まれます。

marログの例を次に示します。

```
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:de4dd03acda
Fri May 31 04:41:55 2019 Info: Message containing attachment(s) for which verdict update was(were) avai
Tue Jun  4 04:42:20 2019 Info: Trying to perform the configured action on MID:348938 SHA256:7d06fd224e0
Tue Jun  4 04:42:21 2019 Info: Message containing attachment(s) for which verdict update was(were) avai
```

Cisco Secure Email Gatewayのトラブルシューティング

接続状態テストの結果が正常に表示されない場合は、Microsoft Azure ADから実行されたアプリケーション登録を確認してください。

Cisco Secure Email Gatewayから、MARログを「trace」レベルに設定し、接続を再テストします。

接続に失敗すると、次のような口グが表示されます。

```
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 '445
 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 '4
 Trace ID: 4afd14f4-ca97-4b15-bba4-e9be19f30d00
 Correlation ID: f38e3388-729b-4068-b013-a08a5492f190
 Timestamp: 2017-03-30 20:08:50Z
```

Azure ADのアプリケーションで、アプリケーションID、ディレクトリID（テナントIDと同じ）、またはその他の関連するIDを口グから確認してください。値がわからない場合は、Azure ADポータルからアプリケーションを削除し、やり直してください。

正常に接続するには、次のような口グが必要です。

```
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
```

Azure ADのトラブルシューティング

注:Cisco TACおよびシスコサポートは、Microsoft Exchange、Microsoft Azure AD、またはOffice 365を使用してお客様の問題をトラブルシューティングすることはできません。

Microsoft Azure ADに関するお客様側の問題については、Microsoftサポートにご連絡ください。 Microsoft Azure Dashboardの[ヘルプ+サポート]オプションを参照してください。 ダッシュボードからMicrosoftサポートへの直接サポート要求を開くことができます。

付録 A

注：これは、Azureアプリケーションのセットアップにクライアントシークレットを使用していない場合にのみ必要です。

公開および秘密の証明書と鍵のペアの構築

ヒント: $base64Value、$base64Thumbprint、および$keyidに対する出力はローカルに保存しておいてください。これらは設定手順で後から必要になります。 証明書の.crtおよび関連.pemは、コンピュータ上の使用可能なローカルフォルダに保存してください。

注：証明書（x509形式/標準）と秘密キーをすでに持っている場合は、このセクションをスキップしてください。 以降のセクションで必要になるため、CRTファイルとPEMファイルの両方があることを確認してください。

証明書：Unix/Linux（openssl を使用）

作成する値：
●拇印 ●公開証明書（CRTファイル） ●秘密キー（PEMファイル）

Unix/Linux/OS Xを使用する管理者は、提供されたスクリプトの目的と実行のために、OpenSSLがインストールされていることを前提としています。

注:OpenSSLのインストールを確認するには、コマンド「which openssl」および「openssl version」を実行します。OpenSSLがない場合はインストールします。

サポートについては、次のドキュメントを参照してください。Cisco Secure Email用のAzure AD構成スクリプト

ホストから(UNIX/Linux/OS X):

1. ターミナルアプリケーションのテキストエディタで(シェルスクリプトを作成するのは簡単ですが)、https://raw.githubusercontent.com/robsherw/my_azure/master/my_azure.shをコピーしてスクリプトを作成します。
2. スクリプトの貼り付け
3. 必ずスクリプトを実行可能にしてください。次のコマンドを実行します。chmod u+x my_azure.sh
4. 次のスクリプトを実行します。./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): MARfor0365.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: MARfor0365.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
```

図13: my_azure.shの画面出力

図2に示すように、スクリプトはAzureアプリの登録に必要な公開証明書(CERファイル)を構築し、呼び出します。また、「Cisco Secure Emailの設定」セクションで使用するThumbprintandCertificate Private Key(PEMファイル)も呼び出します。

microsoft Azureにアプリケーションを登録するために必要な値があります!

[次のセクションをスキップ! 「Cisco Secure Emailで使用するAzureアプリを登録する」に進んでください]

証明書： Windows （ PowerShellを使用 ）

Windowsを使用している管理者は、アプリケーションを使用するか、自己署名証明書を作成するための知識が必要です。 この証明書は、Microsoft Azureアプリケーションを作成し、API通信を関連付けるために使用されます。

作成する値：
●拇印 ●公開証明書（CRTファイル） ●秘密キー（PEMファイル）

このドキュメントで自己署名証明書を作成する例では、XCA(https://hohnstaedt.de/xca/、https://sourceforge.net/projects/xca/)を使用します。

注:XCAは、Mac、Linux、またはWindows用としてダウンロードできます。

---

1. 証明書とキーのデータベースを作成します。 a.ツールバーからFileを選択します b. New Databaseを選択します。 c.データベースのパスワードを作成します （後の手順で必要になるので、覚えておいてください）。 2. [証明書]タブをクリックし、[新しい証明書]をクリックします	

3. 「件名」タブをクリックし、次の項目を入力します。

a.内部名

b. countryName

c. stateOrProvinceName

d.地域名

e. organizationName（組織名）

f. organizationalUnitName(OU)

g. commonName（CN；共通名）

チ。電子メールアドレス

4. Generate a New Keyをクリックします。

5. ポップアップで、表示された情報を確認します

（必要に応じて変更します）。

イ。名称

b.キータイプ：RSA

c.キーサイズ：2048ビット

d. 「作成」をクリックします。

e. OKをクリックして、「Successfully created the RSA private key 'Name' 」ポップアップを確認します。

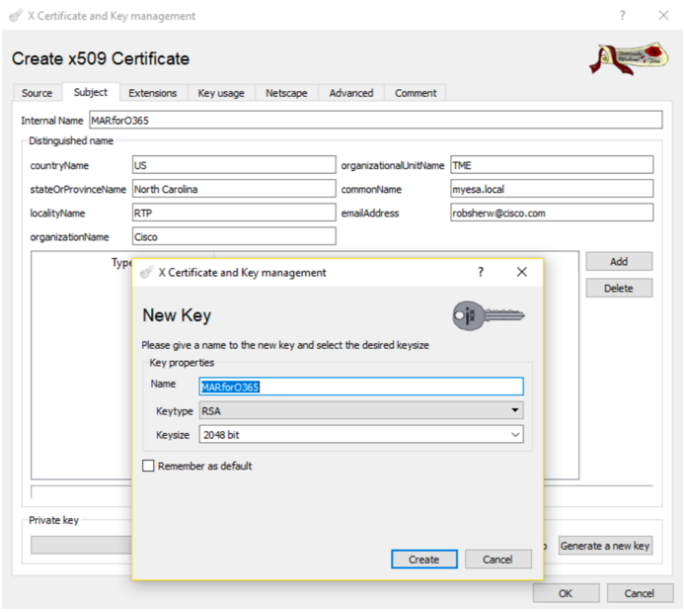


図14:XCAの使用（ステップ3 ～ 5）

6. [キー使用法]タブをクリックし、次の項目を選択します。

a. X509v3でのキー使用法：

デジタル署名、キーの暗号化

b. X509v3での拡張キー使用法：

電子メールの保護

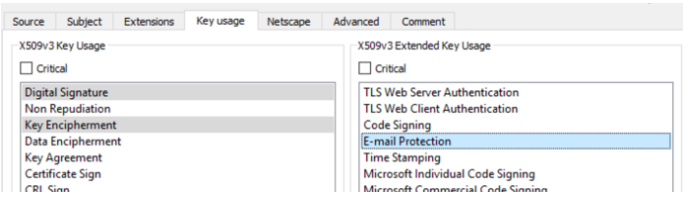
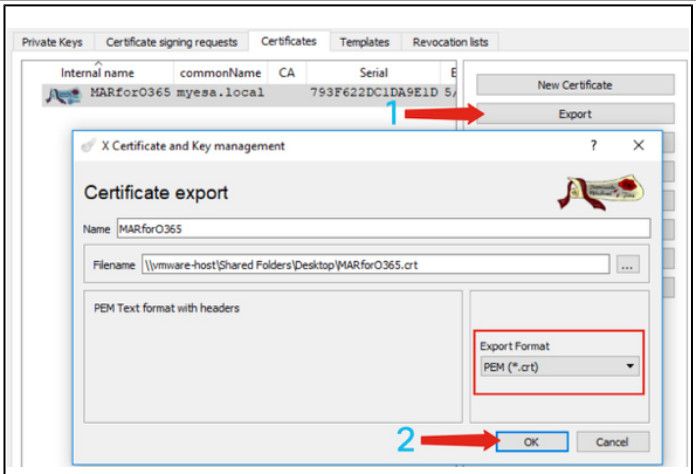
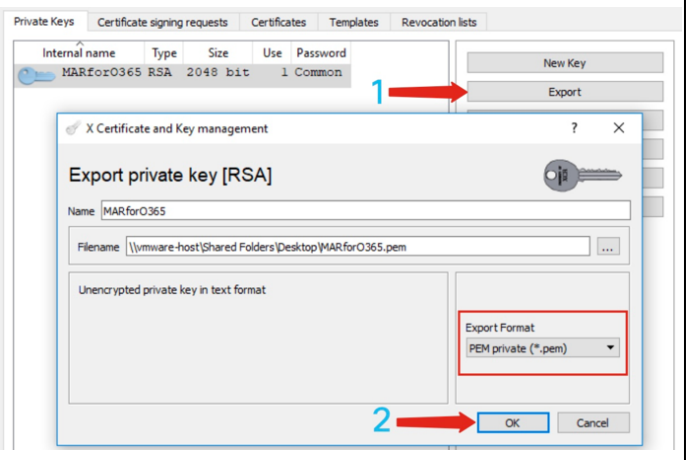


図15:XCAの使用（ステップ6）

7. OKをクリックして、証明書に変更を適用します 8. 「Successfully created the certificate 'Name'」というポップアップが表示されたら、「OK	

次に、公開証明書（CERファイル）と証明書秘密キー（PEMファイル）の両方を、次のPowerShellコマンドでの使用と、「Cisco Secure Emailの設定」の手順での使用のためにエクスポートします。

1. をクリックし、新しく作成した証明書の内部名を強調表示します。 2. 「エクスポート」をクリックします a.アクセスしやすいように保存ディレクトリを設定します（必要に応じて変更） b.エクスポート形式がPEM(.crt)に設定されていることを確認します。 c. OKをクリックします	 図16:XCAの使用（エクスポートCRT）（ステップ1 ～ 2）
3. Private Keysタブをクリックします 4. をクリックし、新しく作成した証明書の内部名を強調表示します。 5. 「エクスポート」をクリックします a.アクセスしやすいように保存ディレクトリを設定します（必要に応じて変更） b.エクスポートフォーマットがPEM private(.pem)に設定されていることを確認します。 c. OKをクリックします 6. XCAを終了して閉じます	 図17:XCAの使用（エクスポートPEM）（ステップ3 ～ 5）

最後に、作成した証明書を取得し、Cisco Secure Emailの設定に必要な拇印を抽出します。

1. Windows PowerShellを使用して、次の操作を実行します。

```
$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
```

2. 次の手順の値を取得するには、ファイルに保存するか、クリップボードにコピーします。

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

注: 「c:\Users\joe\Desktop...」は、出力を保存するPC上の場所です。

PowerShellコマンドを実行すると、次のような出力が表示されます。

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

上記のように、PowerShellコマンドはbase64Thumbprintを呼び出します。これは、Cisco Secure Email Gateway設定に必要なThumbprintです。

Azureアプリの登録に必要な公開証明書（CERファイル）の作成も完了しました。これで、「

Cisco Secure Emailの設定」セクションで使用する証明書秘密キー（PEMファイル）が作成されました。

Microsoft Azureにアプリケーションを登録するために必要な値があります！

[Cisco Secure Emailで使用するAzureアプリの登録に進んでください]

付録 B

注：これは、ゲートウェイでAsyncOS 11.xまたは12.x for Emailを実行している場合にのみ必要です。

API権限(AsyncOS 11.x、12.x)

アプリケーションペインの[管理オプション]で、

1. APIアクセス許可の選択
2. +権限の追加をクリックします
3. Supported legacy APIsまでスクロールダウンして、Exchangeを選択します。
4. 委任されたアクセス許可で次のアクセス許可を選択します。
    1. EWS > "EWS.AccessAsUser.All"（Exchange Webサービス経由でサインインしたユーザーとしてメールボックスにアクセスします）
    2. Mail >「Mail.Read」（ユーザメールを読む）
    3. Mail >「Mail.ReadWrite」（ユーザメールの読み書き）
    4. Mail >「Mail.Send」（ユーザとしてメールを送信）
5. ペインの上部までスクロールします…
6. アプリケーション権限に対する次の権限を選択します。
    1. 「full_access_as_app」（すべてのメールボックスにフルアクセスできるExchange Webサービスを使用）
    2. Mail >「Mail.Read」（ユーザメールを読む）
    3. Mail >「Mail.ReadWrite」（ユーザメールの読み書き）
    4. Mail >「Mail.Send」（ユーザとしてメールを送信）
7. オプション：デフォルトでMicrosoft Graphの「User.Read」権限が有効になっていることが表示されます。この権限は設定したままにしておくか、または「Read」をクリックして「Remove permission」をクリックし、アプリケーションに関連付けられているAPI権限から削除します。
8. 権限の追加(Microsoft Graphがすでにリストされている場合は、権限の更新)をクリックします
9. 最後に、Grant admin consent for...をクリックして、新しい権限がアプリケーションに適用されていることを確認します
10. 次の内容を確認するポップアップウィンドウが表示されます。

'<Azure Name>のすべてのアカウントに対して、要求されたアクセス許可の同意を付与しますか？これにより、このアプリケーションがすでに持っている既存の管理者の同意レコードが、以下にリストされているものと一致する必要があります。」

Yesをクリックします。

この時点で、成功を示すメッセージが緑色で表示され、次のように「Admin Consent Required」列に「Granted」と表示されます。

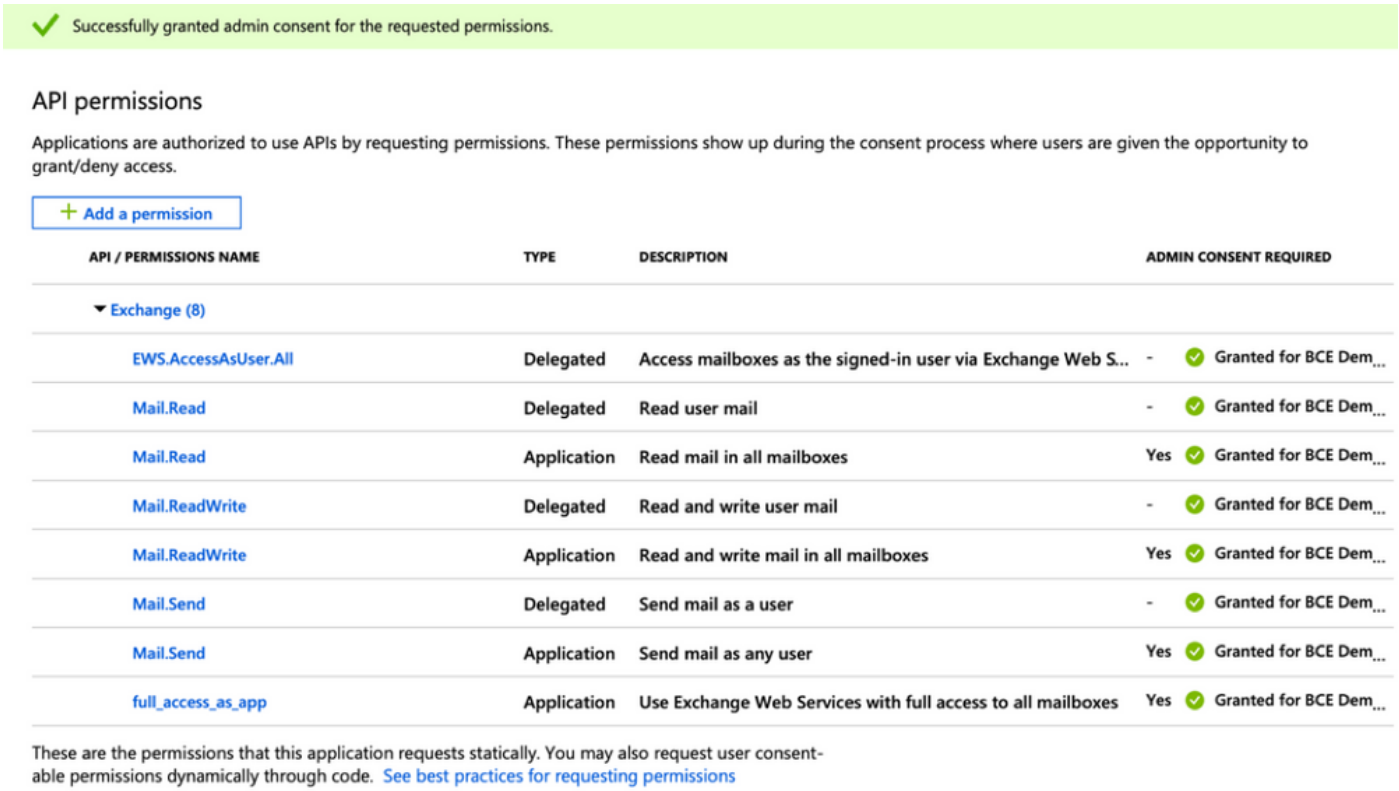


図18: Microsoft Azureアプリの登録（APIアクセス許可が必要）

[Cisco Secure Emailで使用するAzureアプリの登録に進んでください]

関連情報

- Cisco Eメールセキュリティアプライアンス – 製品サポート
- Cisco Eメールセキュリティアプライアンス – リリースノート
- Cisco Eメールセキュリティアプライアンス – エンドユーザガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。