メールボックスのメッセージの自動修復

この章は、次の項で構成されています。

概要

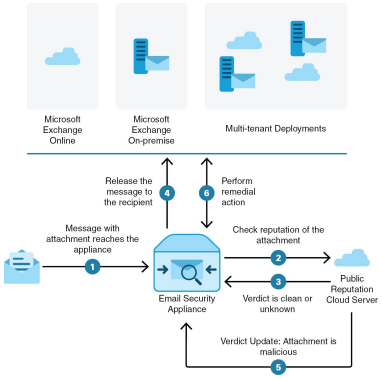
ファイルは常に、ユーザのメールボックスに達した後であっても、悪意のあるファイルに変化する可能性があります。AMP は、新しい情報が発生する際にこの変化を識別し、アプライアンスにレトロスペクティブアラートを送信することができます。脅威判定が変更されたときにユーザのメールボックス内のメッセージに対して自動修復アクションを実行するようにアプライアンスを設定できます。たとえば、添付ファイルに対する判定が「正常」から「悪意がある」に変更されたときには受信者のメールボックスからメッセージを削除するようにアプライアンスを設定することができます。

アプライアンスは、次のメールボックス展開のメッセージに対して自動修復アクションを実行できます。

- Microsoft Exchange Online：Microsoft Office 365 でホストされたメールボックス
- Microsoft Exchange オンプレミス：ローカルの Microsoft Exchange サーバ
- ハイブリッド/マルチテナント構成：Microsoft Exchange Online 展開および Microsoft Exchange オンプレミス展開で設定されたメールボックスの組み合わせ

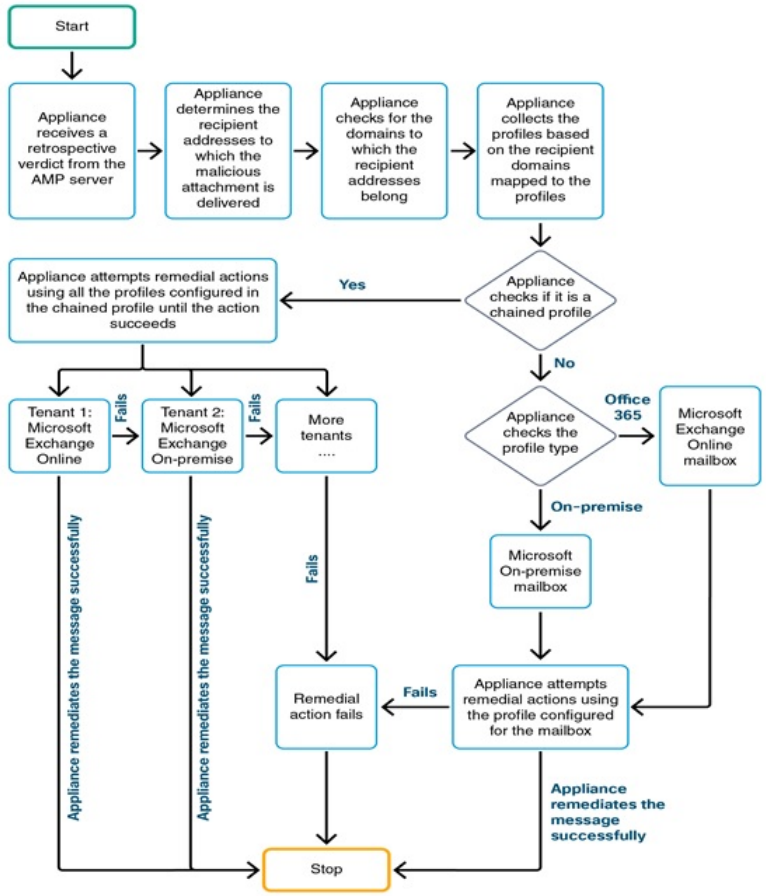
ワークフロー

図 *1:* メールボックス自動修復ワークフロー



1. 添付ファイル付きメッセージがアプライアンスに到達します。
2. アプライアンスは、添付ファイルのレピュテーションを評価する AMP サーバーを照会します。
3. AMP サーバーは、判定をアプライアンスに送信します。判定は、[正常（clean）] または [不明（unknown）] です。
4. アプライアンスは、受信者へメッセージをリリースします。
5. 一定期間後に、アプライアンスは、AMPサーバーから判定の更新を受け取ります。新しい判定は、[悪意のある（malicious）] です。
6. アプライアンスは、受信者のメールボックスに存在する（悪意のある添付ファイルを含む）メッセージに対し、設定された修復アクションを実行します。

アプライアンスによる自動修復アクションの実行の仕組み



1. アプライアンスは AMP サーバーからレトロスペクティブ判定を受信するとメールボックス修復プロセスを開始します。添付ファイル付きメッセージがアプライアンスに到達します。
2. アプライアンスは、悪意のあるメッセージが配信された電子メール アドレスを特定します。
3. アプライアンスは、電子メール アドレスが属する受信者ドメインを識別します。
4. その受信者ドメインに基づいて、アプライアンスはドメインにマッピングされているアカウント プロファイルを収集します。

   アカウント プロファイルは、アプライアンスがメールボックスに接続して自動修復アクションを実行するために使用するメールボックス設定を定義します。メールボックスから

メッセージを正常に修復するには、アカウントプロファイルを作成して受信者ドメインにマッピングする必要があります。

5. アプライアンスは、ドメインにマッピングされたプロファイルをチェックします。
   - （ハイブリッドまたはマルチテナント展開のみ）連結プロファイルの場合、アプライアンスは連結プロファイル内のすべてのアカウントプロファイルを使用して修復アクションを実行しようとします。

     連結プロファイルとは、複数のアカウントプロファイルを組み合わせたものです。複数の展開にメールボックスが存在するハイブリッドまたはマルチテナント展開の場合は、展開内のメールボックスが定義されているすべてのプロファイルを組み合わせた連結プロファイルを作成する必要があります。アプライアンスは、アカウント プロファイルが連結プロファイルに追加された順序に基づいて、修復アクションの実行を試みます。
   - 連結プロファイルでない場合、アプライアンスはプロファイル タイプが Microsoft Exchange Online プロファイルか Microsoft Exchange オンプレミス プロファイルかを確認します。
6. アプライアンスは、識別されたプロファイルを使用して修復アクションを実行し、メッセージを修復します。

（注） メールボックスの修復は、さまざまな理由で失敗することがあります。詳細については、メールボックス修復のトラブルシューティング （22 ページ）を参照してください。

目次

メールボックス内のメッセージに対する修復アクションの実行

修復アクションは、次のメールボックス展開のメッセージに対して実行できます。

- Microsoft Exchange Online（Office 365）： Microsoft Exchange Online メールボックスのメッセージに対する自動修復アクションの実行 （5 ページ）

- Microsoft Exchange オンプレミス： Microsoft Exchange オンプレミス メールボックスのメッセージに対する自動修復アクションの実行 （7 ページ）
- ハイブリッド/マルチテナント展開： ハイブリッド展開のメールボックスのメッセージに対する自動修復アクションの実行 （8 ページ）

Microsoft Exchange Online メールボックスのメッセージに対する自動修復アクションの実行

組織でメールボックスの管理に Microsoft Exchange Online を使用している場合、脅威判定が変更されたときにユーザーのメールボックス内のメッセージに対して自動修復アクションを実行するようにアプライアンスを設定できます。たとえば、添付ファイルに対する判定が「正常」から「悪意がある」に変更されたときには受信者のメールボックスからメッセージを削除するようにアプライアンスを設定することができます。

目次

Microsoft Exchange Online メールボックスのメッセージに対する修復アクションの設定方法

	操作内容	詳細
ステップ 1	前提条件を確認します。	Microsoft Exchange Online メールボックスのメッセージ修復の前提条件 （11 ページ）
ステップ 2	Azure AD（Azure 管理ポータル）上のアプリケーションとして、E メールセキュリティ アプライアンスを登録します。	Azure AD 上のアプリケーションとしてのアプライアンスの登録 （13 ページ）
ステップ 3：	アプライアンスでアカウント設定を有効にします。	アプライアンスでメールボックスの修復機能を有効にします。 Cisco E メール セキュリティ アプライアンスでのアカウント設定の有効化 （15 ページ）

	操作内容	詳細
ステップ 4：	アプライアンスで [Office 365/ハイブリッド（Graph API）（Office 365/Hybrid (Graph API)）] タイプのアカウントプロファイルを作成します。	ユーザー メールボックスの Office 365 プロファイルを作成し、アプライアンスでメールボックスの設定を定義します。 手順を開始する前に、次の点を確認してください。 • .pem 形式の証明書の秘密キーを取得します。「セキュアな通信の証明書」を参照してください。 • 次のパラメータの値です。 • Azure 管理ポータルで登録したアプリケーションのクライアント ID とテナント ID。 • 「Azure AD 上のアプリケーションとしてのアプライアンスの登録」のステップ 9 を参照してください。 • 証明書サムプリント（$base64Thumbprint）。「Azure AD 上のアプリケーションとしてのアプライアンスの登録」のステップ 8 を参照してください。 アカウントプロファイルの作成 （16 ページ）を参照してください。
ステップ 5	受信者ドメインを追加し、ドメインを Office 365 プロファイルにマッピングします。	受信者メールボックスが属するドメインを追加し、ドメインを Office 365 アカウントプロファイルにマッピングします。 アカウント プロファイルへのドメインのマッピング （18 ページ）を参照してください。
ステップ 6	（自動修復の場合のみ）脅威の判定が「悪意がある」に変更された時点でエンドユーザーに送信されるメッセージに修復アクションを実行するようにアプライアンスを設定します。	メールボックスにあるメッセージに対する自動修復アクションの設定 （19 ページ）

Microsoft Exchange オンプレミス メールボックスのメッセージに対する自動修復アクションの実行

Exchange オンプレミス サーバー上のメールボックスからメッセージを修復するようにアプライアンスを設定できます。アプライアンスは、偽装権限があるユーザーアカウントを使用して Exchange オンプレミス メールボックスにアクセスし、メッセージに対して修復アクションを実行します。偽装権限があるこのユーザーアカウントは、アプライアンスが接続してメッセージを修復する必要があるメール交換サーバーで作成する必要があります。

（注） シスコは、Microsoft Exchange 2013 および 2016 でのみ自動メールボックス修復を検証しました。

目次

Microsoft Exchange オンプレミス メールボックスのメッセージに対する修復アクションの設定方法

	操作内容	詳細
ステップ 1	前提条件を確認します。	オンプレミス アカウントのメッセージ修復の前提条件 （12 ページ）
ステップ 2	アプライアンスでアカウント設定を有効にします。	アプライアンスでメールボックスの自動修復を有効にします。 Cisco E メール セキュリティ アプライアンスでのアカウント設定の有効化 （15 ページ）

	操作内容	詳細
ステップ 3：	アプライアンスで [オンプレミス（On-Premise）] タイプのアカウント プロファイルを作成します。	ユーザー メールボックスのオンプレミス プロファイルを作成し、アプライアンスでメールボックスの設定を定義します。 手順を開始する前に、次の点を確認してください。 • 偽装ユーザ アカウントの詳細 • ローカル メール交換サーバのホスト名 アカウント プロファイルの作成 （16ページ）。
ステップ 4	受信者ドメインを追加し、ドメインをオンプレミス アカウント プロファイルにマッピングします。	受信者メールボックスが属するドメインを追加し、ドメインをオンプレミス アカウント プロファイルにマッピングします。 アカウント プロファイルへのドメインのマッピング （18 ページ）を参照してください。
ステップ 5	脅威の判定が「悪意がある」に変更された時点でエンド ユーザーに送信されるメッセージに対して修復アクションを実行するようにアプライアンスを設定します。	メールボックスにあるメッセージに対する自動修復アクションの設定 （19 ページ）

ハイブリッド展開のメールボックスのメッセージに対する自動修復アクションの実行

単一のアプライアンスでハイブリッド Exchange 展開または複数の Exchange テナントからメッセージを修復するように設定できます。たとえば、組織がメールボックスを Microsoft Exchange オンプレミスから Microsoft Exchange Online に移行中の場合、移行が完了するまでは、Microsoft Exchange Online と Microsoft Exchange オンプレミスにメールボックスが展開されることになります。

異なる展開で設定された複数のメールボックスからメッセージを自動的に修復するには、連結プロファイルを作成します。連結プロファイルは、ハイブリッドまたはマルチテナント展開のすべてのアカウント プロファイルを統合します。プロファイルが連結プロファイルに追加される順序によって、アプライアンスがメッセージを修復するためにプロファイルを確認する優先順位が定義されます。

アプライアンスは AMP サーバーからレトロスペクティブ判定を受信すると、連結プロファイルで定義されている優先順に連結プロファイル内の各プロファイルを使用して修復アクションの実行を試みます。

目次

ハイブリッド展開のメールボックスのメッセージに対する修復アクションの実行方法

	操作内容	詳細
ステップ 1	前提条件を確認します。	ハイブリッドまたはマルチテナント展開で、Microsoft Exchange Online および Microsoft Exchange オンプレミスのメールボックスに対して自動修復アクションを実行するためのすべての前提条件が満たされていることを確認します。 前提条件 （11 ページ）を参照してください。
ステップ 2	Azure AD（Azure 管理ポータル）上のアプリケーションとして、E メールセキュリティ アプライアンスを登録します。	Azure AD 上のアプリケーションとしてのアプライアンスの登録 （13 ページ）
ステップ 3：	アプライアンスでアカウント設定を有効にします。	アプライアンスでメールボックスの修復機能を有効にします。 Cisco E メール セキュリティ アプライアンスでのアカウント設定の有効化 （15 ページ）を参照してください。

	操作内容	詳細
ステップ 4	ハイブリッド/マルチテナント展開内の全メールボックスのアカウント プロファイルを作成します。	ユーザー メールボックスのアカウント プロファイルを作成し、アプライアンスでメールボックスの設定を定義します。 手順を開始する前に、次の点を確認してください。 • .pem 形式の証明書の秘密キーを取得します。「セキュアな通信の証明書」を参照してください。 • 次のパラメータの値です。 • Azure 管理ポータルで登録したアプリケーションのクライアント ID とテナント ID。 • 「Azure AD 上のアプリケーションとしてのアプライアンスの登録」のステップ 9 を参照してください。 • 証明書サムプリント（$base64Thumbprint）。「Azure AD 上のアプリケーションとしてのアプライアンスの登録」のステップ 8 を参照してください。 • 偽装ユーザ アカウントの詳細 • ローカル メール交換サーバのホスト名 アカウント プロファイルの作成 （16 ページ）を参照してください。
ステップ 5	連結プロファイルを作成します。	連結プロファイルを作成し、ハイブリッド/マルチテナント展開のすべてのプロファイルを追加します。 連結プロファイルの作成 （18 ページ）を参照してください。

	操作内容	詳細
ステップ 6	受信者のドメインを追加して連結プロファイルにマッピングします。	受信者のメールボックスが属するドメインを追加し、そのドメインを連結プロファイルにマッピングします。 アカウント プロファイルへのドメインのマッピング （18 ページ）を参照してください。
ステップ 7	脅威の判定が「悪意がある」に変更された時点でエンド ユーザーに送信されるメッセージに対して修復アクションを実行するようにアプライアンスを設定します。	メールボックスにあるメッセージに対する自動修復アクションの設定 （19 ページ）

Cisco E メール セキュリティ アプライアンスでのメールボックス自動修復の設定

前提条件

Microsoft Exchange Online メールボックスのメッセージ修復の前提条件

ファイル レピュテーション サービスとファイル分析サービスの機能キー

次の内容について確認してください。

- ファイル レピュテーション サービスおよびファイル分析サービスの機能キーをお使いのアプライアンスに追加していること。
- アプライアンスでのファイル レピュテーションと分析機能が有効になっている。ファイル レピュテーション フィルタリングとファイル分析 を参照してください。

Office 365 アカウント

Azure ADに、アプライアンスを登録する必要がある次のアカウントがあることを確認します。

- Office 365 のビジネス アカウント
- Office 365 のビジネス アカウントに関連付けられた Azure AD サブスクリプション

詳細については、Office 365 のシステム管理者にお問い合わせください。

セキュアな通信の証明書

Office 365 サービスとアプライアンス間の通信をセキュリティで保護するには、自己署名証明書を作成する、または信頼されたCAから証明書を取得する方法のいずれかで証明書を設定する必要があります。

次のものが必要です。

- .crt または .p12 形式の公開キー。emailAddress に Office 365 の管理者の電子メール アドレスが設定されていること（<admin_username>@<domain>.com）。
- キーサイズが少なくとも 2048 ビットで、関連付けられた .pem 形式の秘密キー。

詳細については、https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/211404-How-to-configure-Azure-AD-and-Office-365.htmlを参照してください。

（注） パスフレーズを含む秘密キーはこのリリースではサポートされません。

オンプレミス アカウントのメッセージ修復の前提条件

- ファイル レピュテーション サービスとファイル分析サービスの機能キー （12 ページ）
- （任意）Microsoft Exchange Web サービス（EWS）証明書のインポート （13 ページ）
- 偽装ロールへのユーザの追加 （13 ページ）

ファイル レピュテーション サービスとファイル分析サービスの機能キー

次の内容について確認してください。

- ファイル レピュテーション サービスおよびファイル分析サービスの機能キーをお使いのアプライアンスに追加していること。

- アプライアンスでのファイル レピュテーションと分析機能が有効になっている。ファイル レピュテーション フィルタリングとファイル分析 を参照してください。

（任意）Microsoft Exchange Web サービス（EWS）証明書のインポート

EWS サービス用に Microsoft Exchange オンプレミス サーバーで自己署名証明書を使用している場合は、Microsoft Exchange オンプレミス サーバーから E メール セキュリティ アプライアンスに証明書をインポートする必要があります。証明書をインポートするには、証明書のインポート を参照してください。

偽装ロールへのユーザの追加

アプライアンスは偽装権限があるユーザー アカウントを使用して、Microsoft Exchange オンプレミスのメールボックスにアクセスします。メール交換管理者は、ローカル交換サーバーで偽装権限があるユーザー アカウントを作成する必要があります。アプライアンスはこのユーザー アカウントを使用して、メールボックスからメッセージを修復します。

手順

ステップ 1 偽装権限を割り当てる必要があるユーザー アカウントを作成します。このユーザー アカウントは、アプライアンスがメッセージの修復を目的にメールボックスにアクセスして操作するために使用されます。

ステップ 2 管理者クレデンシャルを使用して、Microsoft Exchange コントロール パネル インターフェイスにログインします。

ステップ 3 [権限（Permissions）] -> [管理者ロール（Admin Roles）] に移動します。

ステップ 4 ロールを作成し、そのロールに「ApplicationImpersonation」権限を割り当てます。

ステップ 5 この新しいロールのメンバーとして、偽装権限を割り当てる必要があるユーザ アカウントを追加します。

Azure AD 上のアプリケーションとしてのアプライアンスの登録

Office 365 サービスは、ユーザーのメールボックスへのセキュアなアクセスを提供する Azure Active Directory（Azure AD）を使用します。Office 365 のメールボックスにアプライアンスがアクセスするには、Azure AD でアプライアンスを登録しなければなりません。Azure AD でアプライアンスを登録するために実行する必要がある手順の概要を次に示します。詳細な手順については、Microsoft のマニュアルを参照してください（https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app）。

はじめる前に

Microsoft Exchange Online メールボックスのメッセージ修復の前提条件 （11 ページ）で説明されている作業を行います。

手順

ステップ 1 Office 365 のビジネスアカウントの資格情報を使用して Azure 管理ポータルにログインします。

ステップ 2 Office 365 のサブスクリプションにリンクされているディレクトリに新しいアプリケーションを追加します。

ステップ 3 [アプリケーションの登録（App Registrations）] > [新規登録（New Registration）] に移動して、新しいアプリケーションを追加します。

ステップ 4 新しいアプリケーションを追加している間に、次のことを確認します。

- アプリケーション名、およびアプリケーションがサポートする必要があるアカウントタイプを指定します。
- （任意）アプリケーション タイプとして [Web] を選択し、ユーザーがサインインしてアプライアンスを使用できる URL を指定します。

ステップ 5 アプリケーションに必要な権限を割り当てます。ナビゲーション ウィンドウで[API権限（API permissions）] をクリックし、[権限の追加（Add a permission）] をクリックします。

ステップ 6 [Microsoft Graph] > [アプリケーション権限（Application permissions）] を選択し、次の権限を割り当てます。

- Mail.Read：すべてのメールボックスのメールを読み取ります。
- Mail. ReadWrite：すべてのメールボックスのメールの読み取りと書き込みを行います。
- Mail.Send：任意のユーザとしてメールを送信します。

ステップ 7 組織内のすべてのアカウントで必要なすべての権限に対して管理者の同意を付与します。

ステップ 8 パブリックキー証明書からのキー資格情報によりアプリケーションマニフェストを更新して、Office 365 サービスとアプライアンス間の通信を保護します。次の操作を行ってください。

a) Windows PowerShell プロンプトを使用して、公開キー証明書の `$base64Thumbprint`、`$base64Value`、および `$keyid` の値を取得します。次の例を参照してください。Windows PowerShell プロンプトから公開キー証明書を含むディレクトリに移動し、次を実行します。

例：

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import(".\mycer.cer")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)
$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)
$keyid = [System.Guid]::NewGuid().ToString()
```

上記のコマンドを実行した後、次のコマンドを実行して、その値を抽出します。

```
$keyid
$base64Value
$base64Thumbprint
```

b) 登録済みアプリケーション ペインの左ペインにある [マニフェスト（manifest）] をクリックして、アプリケーションのマニフェストを開きます。

c) マニフェスト テキスト エディタを使用して、空の KeyCredentials プロパティを次の JSON で置き換えます。

例：

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint_from_step_1",
"keyId": "$keyid_from_step1",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value_from_step1"
}
],
```

例：

上記の JSON スニペットでは、`$base64Thumbprint`、`$base64Value`、および `$keyid` の値が、手順 a で取得した値で置き換えられていることを確認します。各値は 1 行で入力する必要があります。

ステップ 9 アプライアンスを Azure AD に登録した後、Azure 管理ポータルで、登録したアプリケーションの [概要（Overview）] ペインにある次の詳細を書き留めてください。

- クライアント ID
- テナント ID テナント ID は、このページに記載されているすべての URL で使用できる一意の値です。たとえば、このページに記載されている次のような URL です。
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/federationmetadata/2007-06/federationmetadata.xml
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/wsfed
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/saml2

この例では、テナント ID は abcd1234-bcdd-469d-8545-a0662708cbc3 です。

次のタスク

Cisco E メール セキュリティ アプライアンスでのアカウント設定の有効化 （15 ページ）

Cisco E メール セキュリティ アプライアンスでのアカウント設定の有効化

はじめる前に

次の内容について確認してください。

- アプライアンスでのファイル レピュテーションと分析機能が有効になっている。ファイル レピュテーション フィルタリングとファイル分析 を参照してください。

手順

ステップ 1 アプライアンスへのログイン

ステップ 2 [システム管理（System Administration）] > [アカウントの設定（Account Settings）] をクリックします。

ステップ 3 **[有効（Enable）]** をクリックします。

ステップ 4 [アカウント設定の有効化（Enable Account Settings）] を選択します。

ステップ 5 （任意）アプライアンスがメッセージを修復するためにメールボックスへの接続を試行する最大回数を入力します。許容値は 1 ～ 5 の整数です。

ステップ 6 （任意）ハイブリッド メール交換サーバーへの接続がタイムアウトする前にアプライアンスが待機する秒数を入力します。許容値は 15 ～ 90 の整数です。

ステップ 7 （任意）ローカル メール交換サーバーへの接続がタイムアウトする前にアプライアンスが待機する秒数を入力します。許容値は 15 ～ 90 の整数です。

ステップ 8 変更を送信し、保存します。

次のタスク

アカウント プロファイルの作成 （16 ページ）

アカウント プロファイルの作成

アカウントプロファイルは、メールボックス内のメッセージの脅威判定が「悪意のある」に変わったときに、アプライアンスがメールボックスに接続して修復アクションを実行するために必要なメールボックス パラメータを定義します。

各プロファイルのクレデンシャルは、1 つのテナントに関連しています。複数のテナント間で修復を実行する場合は、テナントごとにプロファイルを設定し、チェーンプロファイルを使用してそれらを連結する必要があります。ただし、マルチテナント展開でロードバランサを使用している場合は、1 つのプロファイルを設定し、ロード バランサのホスト名を使用してプロファイルを作成することができます。

はじめる前に

次の内容について確認してください。

- 有効化されたアカウント設定。Cisco E メール セキュリティ アプライアンスでのアカウント設定の有効化 （15 ページ）を参照してください。
- Microsoft Exchange Online サーバまたは Microsoft Exchange オンプレミス サーバの有効な電子メール アドレス。
- Microsoft Exchange Online アカウントまたは Microsoft Exchange オンプレミス アカウントを設定するために必要なパラメータ。

手順

ステップ 1 アプライアンスへのログイン

ステップ 2 [システム管理（System Administration）] > [アカウントの設定（Account Settings）] をクリックします。

ステップ 3 [アカウントプロファイルの作成（Create Account Profile）] をクリックします。

ステップ 4 プロファイルの名前および説明を入力します。

ステップ 5 メールボックスの展開に基づいてプロファイル タイプを選択します。

- [Office 365/ハイブリッド（Graph API）（Office 365/Hybrid (Graph API)）]：Microsoft Exchange Online 上に展開されたメールボックスを設定し、Azure 管理ポータルに登録したアプリケーションのクライアント ID とテナント ID を入力するには、このタイプを選択します。
  - Azure 管理ポータルで登録したアプリケーションのクライアント ID とテナント ID。
  - 証明書のサムプリント（$base64Thumbprint の値）。
  - 証明書の秘密キーをアップロードします。[ファイルの選択（Choose File）] をクリックして、.pem ファイルを選択します。
- [Exchangeオンプレミス（Exchange On-premise）]：Microsoft Exchange オンプレミスで展開されたメールボックスを設定し、次の詳細情報を入力する場合に選択します。
  - 偽装権限を持つユーザアカウントのユーザ名とパスワードを入力します。詳細については、偽装ロールへのユーザの追加 （13 ページ）を参照してください。
  - Microsoft Exchange オンプレミス サーバのホスト名を入力します。

    （注） マルチテナント展開でロード バランサを使用する場合は、ロード バランサのホスト名を設定する必要があります。

ステップ 6 アプライアンスが Microsoft Exchange Online サーバーまたは Microsoft Exchange オンプレミス サーバーに接続できるかどうかを確認します。

a) [テスト接続（Test Connection）] をクリックします。
b) 電子メール アドレスを入力します。これは、Microsoft Exchange Online または Microsoft Exchange オンプレミスの有効な電子メール アドレスである必要があります。
c) [テスト接続（Test Connection）] をクリックします。
アプライアンスがメールボックス サーバーに接続できるかどうかを示すステータスが表示されます。
d) 4. [完了（Done）] をクリックします。エラーのトラブルシューティングについては、メールボックス修復のトラブルシューティング （22 ページ）を参照してください。

ステップ 7 変更を送信し、保存します。

次のタスク

- 連結プロファイルの作成 （18 ページ）
- アカウント プロファイルへのドメインのマッピング （18 ページ）

連結プロファイルの作成

このタスクは、ハイブリッド展開またはマルチテナント展開のメールボックスにあるメッセージを修復する場合にのみ必須です。

はじめる前に

少なくとも1つのアカウントプロファイルがアプライアンスに追加されていることを確認してください。

手順

ステップ 1 アプライアンスへのログイン

ステップ 2 [システム管理（System Administration）] > [アカウントの設定（Account Settings）] をクリックします。

ステップ 3 [連結プロファイルの作成（Create Chained Profile）] をクリックします。

ステップ 4 連結プロファイルの名前および説明を入力します。

ステップ 5 連結プロファイルに追加するアカウント プロファイルをドロップダウン メニューから選択します。さらにプロファイルを追加するには、[アカウントプロファイルの追加（Add Account Profile）] をクリックします。

（注）
- アプライアンスがメッセージを修復するためにプロファイルを確認する優先順にプロファイルを追加する必要があります。
- アプライアンスには、一度に最大 5 つの連結プロファイルを作成できます。
- 連結プロファイルごとに最大10個のアカウントプロファイルを追加できます。

ステップ 6 変更を送信し、保存します。

次のタスク

アカウント プロファイルへのドメインのマッピング （18 ページ）

アカウント プロファイルへのドメインのマッピング

受信者のメールボックスが属するドメインを定義する必要があります。次に、アプライアンスがメールボックス内のメッセージを修復する際に使用するアカウントプロファイルにドメインをマッピングします。

（注）
- ドメインマッピングを編集して、プロファイルにマッピングされた既存のドメインに新しいドメインを追加することができます。
- ドメインマッピングはプロファイルに固有です。あるプロファイルにマップされたドメインは、別のプロファイルにマップできません。

はじめる前に

少なくとも1つのアカウントプロファイルがアプライアンスに追加されていることを確認してください。

手順

ステップ1 アプライアンスへのログイン

ステップ2 [システム管理（System Administration）] > [アカウントの設定（Account Settings）] をクリックします。

ステップ3 [ドメインマッピングの作成（Create Domain Mapping）] をクリックします。

ステップ4 ドメイン名をカンマで区切って入力します。すべてのドメインにプロファイルをマッピングする場合は、「ALL」という文字列を入力します。

ステップ5 ドメインにマッピングするプロファイルを選択します。また、連結プロファイルをドメインにマッピングすることもできます。

ステップ6 変更を送信し、保存します。

次のタスク

メールボックスにあるメッセージに対する自動修復アクションの設定 （19 ページ）

メールボックスにあるメッセージに対する自動修復アクションの設定

はじめる前に

Cisco Secure Email クラウドゲートウェイでメールボックスの修復機能が有効になっており、アカウントの設定が完了していることを確認します。Cisco E メール セキュリティ アプライアンスでのアカウント設定の有効化 （15 ページ）を参照してください。

手順

ステップ1 [設定（Configuration）] > [メール設定（Mail Configuration）] > [インバウンド（Inbound）] > [受信ポリシー（Incoming Policies）] を選択します。

ステップ2 編集するポリシーの横にあるドロップダウン矢印をクリックします。

ステップ 3 [AMP] 列の横にある [編集（Edit）] アイコンをクリックします。

ステップ 4 [メールボックス自動修復の有効化（Enable Mailbox Auto Remediation）] チェックボックスを選択します。

ステップ 5 脅威の判定が悪意に変更されたときにエンドユーザに配信されたメッセージ基づいて実行するアクションを指定します。要件に応じて、次のいずれかの修復アクションを選択します。

- [電子メールアドレスに転送（Forward to an email address）]。指定したユーザ（たとえば、電子メール管理者など）に悪意のある添付ファイルを転送する場合は、このオプションを選択します。
- メッセージを削除します。悪意のある添付ファイルをエンドユーザのメールボックスから完全に削除する場合は、このオプションを選択します。
- [指定した電子メール アドレスに転送してメッセージを削除（Forward to an email address and delete the message）]。指定したユーザ（たとえば、電子メール管理者など）に悪意のある添付ファイルを転送して、悪意のある添付ファイルをエンドユーザのメールボックスから完全に削除する場合は、このオプションを選択します。

ステップ 6 変更を送信します。

次のタスク

関連項目

- メールボックス修復結果のモニタリング （20 ページ）
- メッセージ トラッキングでのメールボックス修復の詳細の表示 （22 ページ）
- メールボックス修復のトラブルシューティング （22 ページ）

AsyncOS 13.0 以降のリリースへのアップグレード

以前の AsyncOS バージョンで定義されたメールボックスの設定は、アップグレード中にシームレスに移行されます。このメールボックスは、「Default」というプロファイル名で作成されて「すべて」のドメインにマッピングされます。このプロファイルは、アップグレード後に必要に応じて編集できます。アプリケーションが Azure Active Directory の Microsoft Graph API にアクセスして、Microsoft Exchange Online メールボックスからメッセージを自動修復できることを確認します。詳細については、Azure AD 上のアプリケーションとしてのアプライアンスの登録 （13 ページ）を参照してください。

メールボックス修復結果のモニタリング

[メールボックスの自動修復レポート（Mailbox Auto Remediation report）]ページを使用して（[モニタ（Monitor）] > [メールボックスの自動修復（Mailbox Auto Remediation）]）、メールボックス修復結果の詳細を表示できます。このレポートを使用して次の詳細を表示します。

- メッセージに対してとられる修復のアクション
- SHA-256 ハッシュに関連付けられているファイル名

- メールボックス修復が成功または失敗した受信者について定義されているプロファイル名の一覧
- 修復が失敗した理由
- ドメインにマッピングされたプロファイルがない

[修復が失敗した受信者（Recipients for whom remediation was unsuccessful）] フィールドは、次のシナリオで更新されます。

- 添付ファイルを含むメッセージをメールボックスで使用できない。たとえば、エンドユーザがメッセージを削除した。
- 無効なメールボックス：受信者が有効な Microsoft Exchange Online ユーザーまたは Microsoft Exchange オンプレミス ユーザーではないか、アプライアンスに設定された Microsoft Exchange Online または Microsoft Exchange オンプレミスのドメイン アカウントに属していない。
- 添付ファイルを含むメッセージをメールボックスで使用できない。たとえば、エンドユーザーがメッセージを削除した。
- 認証エラー：Microsoft Exchange オンプレミスのメールボックスに接続するためにアプライアンスで指定されたユーザー アカウントが正しくない。
- 接続エラー：アプライアンスが修復アクションを実行しようとしたときに、アプライアンスと Microsoft Exchange Online または Microsoft Exchange オンプレミス サービスとの間に接続の問題が発生した。
- 権限に関するエラー：
  - Microsoft Exchange オンプレミス アカウントの場合、Microsoft Exchange オンプレミスのメールボックスに接続するためにアプライアンスで指定されたユーザーアカウントに偽装ロールが割り当てられていない。
  - Microsoft Exchange Online アカウントの場合、Office 365 アプリケーションに、受信者のメールボックスにアクセスするために必要な権限がない。
- ドメインにプロファイルがマッピングされていない：受信者ドメインにマッピングされたプロファイルがない。
- メールボックスがアクセス不能または無効：
  - メールボックスへのアクセスに使用されるアカウント プロファイルのプロファイル タイプが正しくない。
  - 受信者が有効な Microsoft Exchange Online ユーザまたは Microsoft Exchange オンプレミス ユーザではない。
  - 受信者が、アプライアンスに設定された Microsoft Exchange Online または Microsoft Exchange オンプレミスのドメイン アカウントに属していない。

メッセージ トラッキングに関連メッセージを表示するには、SHA-256 ハッシュをクリックします。

メッセージ トラッキングでのメールボックス修復の詳細の表示

メッセージ トラッキングでメールボックス修復の詳細を表示するには、

- メッセージ トラッキングが有効になっている必要があります。メッセージ トラッキング を参照してください
- メールボックス修復アクション（[メールポリシー（Mail Policies）]>[受信メールポリシー（Incoming Mail Policies）] > [高度なマルウェア防御（Advanced Malware Protection）] > [メールボックス自動修復の有効化（Enable Mailbox Auto Remediation）]）を設定する必要があります。メールボックスにあるメッセージに対する自動修復アクションの設定 （19 ページ）を参照してください。

表示されるデータの詳細については、メッセージ トラッキングの詳細 を参照してください。

メールボックス修復のトラブルシューティング

接続エラー

問題

[アカウントの設定（Account Settings）] ページ（[システム管理（System Administration）] > **[アカウントの設定（Account Settings）]**）でアプライアンスと受信者メールボックスとの接続を確認しようとすると、エラー メッセージ「接続に失敗しました（Connection Unsuccessful）」が表示されます。

解決方法

サーバからの応答に応じて、次のいずれかを実行します。

エラー メッセージ	理由とソリューション
`The SMTP address has no mailbox associated with it`	関連付けられたメール ドメインに属していない電子メール アドレスを入力しました。 有効な電子メール アドレスを入力して、接続を再度確認します。

エラー メッセージ	理由とソリューション
The mailbox cannot be accessed using this profile or the required permissions may be missing	以下を確認します。 • ユーザー メールボックスにアクセスするために必要な権限があります。Micrsoft Exchange Online アカウントには Microsoft Graph API でのみアクセスでき、Microsoft Exchange オンプレミス アカウントには偽装権限を持つユーザ アカウントを使用してアクセスできます。 • 誤ったプロファイル タイプを選択しました。[アカウントプロファイルの編集（Edit Account Profile）] ページでプロファイルの詳細を変更し、接続を再度確認します。
Access is denied. Check credentials and try again	Microsoft Azure に設定された Office 365 アプリケーションに、Microsoft Exchange Online メールボックスにアクセスするために必要な権限がありません。
Application with identifier '<*client_id*>' was not found in the directory <*tenant_id*>	無効なクライアント ID を入力しました。 [アカウントプロファイル（Account Profile）] ページでクライアント ID を変更し、接続を再度確認します。
No service namespace named '<*tenant_id*>' was found in the data store.	無効なテナント ID を入力しました。 [アカウントプロファイル（Account Profile）] ページでテナント ID を変更し、接続を再度確認します。
Error validating credentials. Credential validation failed	無効な証明書サムプリントを入力しました。 [アカウントプロファイル（Account Profile）] ページで証明書サムプリントを変更し、接続を再度確認します。
Error validating credentials. Client assertion contains an invalid signature.	誤った証明書サムプリントを入力したか、または無効なあるいは誤った証明書秘密キーをアップロードしました。 以下を確認します。 • 正しいサムプリントを入力しました。 • 正しい証明書の秘密キーをアップロードしました。 • 証明書の秘密キーは有効期限が切れていません。 • アプライアンスの時間帯は、証明書の秘密キーの時間帯と一致します。
要求されたユーザ <電子メール アドレス> が無効です	入力された電子メール アドレスが、アカウント プロファイルのプロファイル タイプと一致しません。有効な電子メールアドレスを入力するか、[アカウントプロファイル（Account Profile）] ページでアカウント プロファイルを変更して、接続を再度確認します。

エラー メッセージ	理由とソリューション
`Failed to verify exchange server('<host name>') certificate. If self-signed certificate is used on exchange server install its custom CA certificate`	• Microsoft Exchange オンプレミス サーバで、無効な CA または自己署名証明書を入力しました。証明書を検証してから、接続を再度確認します。 （注） 使用している証明書が、プロファイルで指定されたホスト名に対応していることを確認します。たとえば、プロファイル設定で Exchange Server の IP アドレスを指定した場合に証明書がホスト名に基づいていると、接続は失敗します。 • Microsoft Exchange オンプレミス サーバーからアプライアンスに自己署名証明書がインポートされていません。詳細については、証明書のインポートを参照してください。
`Invalid username or password entered for exchange server ('<email address>')`	Microsoft Exchange オンプレミスのメールボックスに接続するために使用される偽装ユーザ アカウントの無効なユーザ名またはパスワードを入力しました。
`The account does not have permission to impersonate the requested user`	Microsoft Exchange オンプレミスのメールボックスに接続するために使用されるユーザ アカウントは、偽装ロールのメンバーではありません（偽装権限を持っていません）。
`Please check host <hostname> is valid exchange server address.`	Microsoft Exchange オンプレミス サーバの誤ったホスト名を入力しました。[アカウントプロファイル（Account Profile）] ページでホスト名を変更し、接続を再度確認します。

ログの表示

メールボックスの修復情報は、次のログに書き込まれます。

- メール ログ（mail_logs）。メールボックスの修復プロセスの開始時刻は、このログに転記されます。情報：
  - メールボックスの修復プロセスの開始時刻は、このログに転記されます。
  - 修復が失敗した理由。
  - 修復が成功および失敗した受信者の数。
- メールボックスの自動修復ログ（mar）。修復状態、実行された操作、エラーに関連する情報などがこのログに転記されます。

アラート

アラート：検出されたアプライアンス と Microsoft Exchange サービスとの間の接続の問題

問題

アプライアンス と Microsoft Exchange Online サービスまたは Microsoft Exchange オンプレミス サービスの間に接続の問題があり、設定された修復アクションをアプライアンスが実行できないことを示す情報レベルのアラートを受け取ります。

ソリューション

次の手順を実行します。

- アプライアンス と Microsoft Exchange Online サービスまたは Microsoft Exchange オンプレミスサービスとの通信を妨げている可能性があるネットワークの問題を確認します。

  アプライアンスのネットワーク設定を確認します。ネットワーク設定値の変更を参照してください。

- アプリケーションに Azure Active Directory 上の Microsoft Graph API へのアクセス権があることを確認します。
- Exchange オンプレミスのメールボックスへのアクセスに使用されるユーザ アカウントに偽装権限があることを確認します。
- 対応するプロファイルに設定されているパラメータが有効であることを確認し、接続をテストします。
- ファイアウォールの問題を確認します。ファイアウォール情報を参照してください。
- Microsoft Exchange Online サービスまたは Microsoft Exchange オンプレミス サービスが動作しているかどうかを確認します。

設定された是正措置が実行されない

問題

AMP サーバからレトロスペクティブ アラートを受信した後、設定済みの修復アクションが Exchange Online および Exchange オンプレミスのメールボックスにある悪意のあるメッセージに対して実行されません。

ソリューション

次の手順を実行します。

- アプライアンスと Exchange Online サービスおよび Exchange オンプレミス サービスの接続をテストします。アカウント プロファイルの作成 （16 ページ）を参照してください。
- 「アプライアンスとExchange Onlineサービスおよびオンプレミスサービス間の接続の問題が検出されました。（Connectivity Issues Between Appliance and Exchange online and Exchange on-premise Services Detected.）」というアラートを受信しているかどうかを確認します。アラート （25 ページ） を参照してください。

設定された是正措置が実行されない

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。