メールボックスでのメッセージの修復

この章は、次の項で構成されています。

概要

電子メールゲートウェイは、ユーザメールボックスにすでに配信されている悪意のあるメッセージを修復する機能を提供します。電子メールゲートウェイを設定し、次の方法でメッセージを修復できます。

- AMP が電子メールゲートウェイにレトロスペクティブアラートを送信すると、メッセージを自動的に修復する
- メッセージ トラッキング フィルタを使用してメッセージを手動で検索して修正する。

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、電子メールゲートウェイ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電子メールゲートウェイを設定できます。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電子メールゲートウェイを設定することができます。

また、[メッセージトラッキング（Message Tracking）]ページを使用して、ユーザのメールボックスに配信されたメッセージを検索して修正することもできます。[メッセージトラッキング（Message Tracking）]ページは、メールボックスに配信されたすべてのメッセージを対象にし

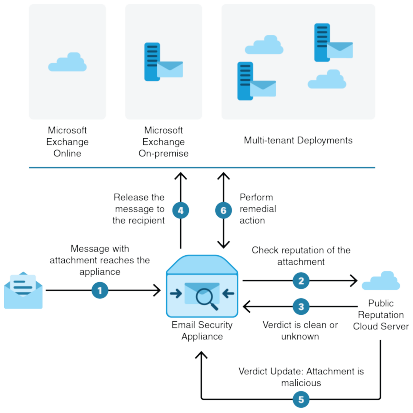
た検索を実行するための統合された場所です。検索結果から修復するメッセージを選択し、そのメッセージに対して実行するアクションを適用できます。

電子メールゲートウェイは、次のメールボックスに展開されたメッセージに対して修復アクション（手動または自動）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

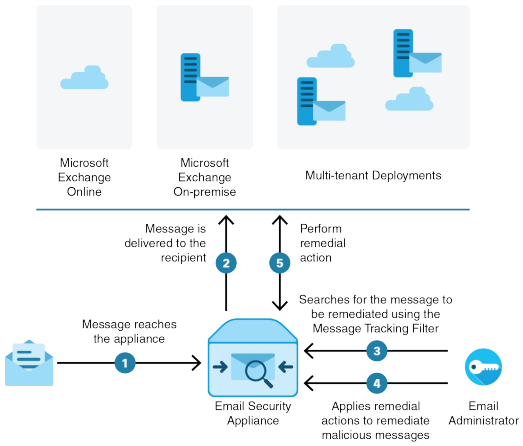
ワークフロー

メールボックス自動修復ワークフロー



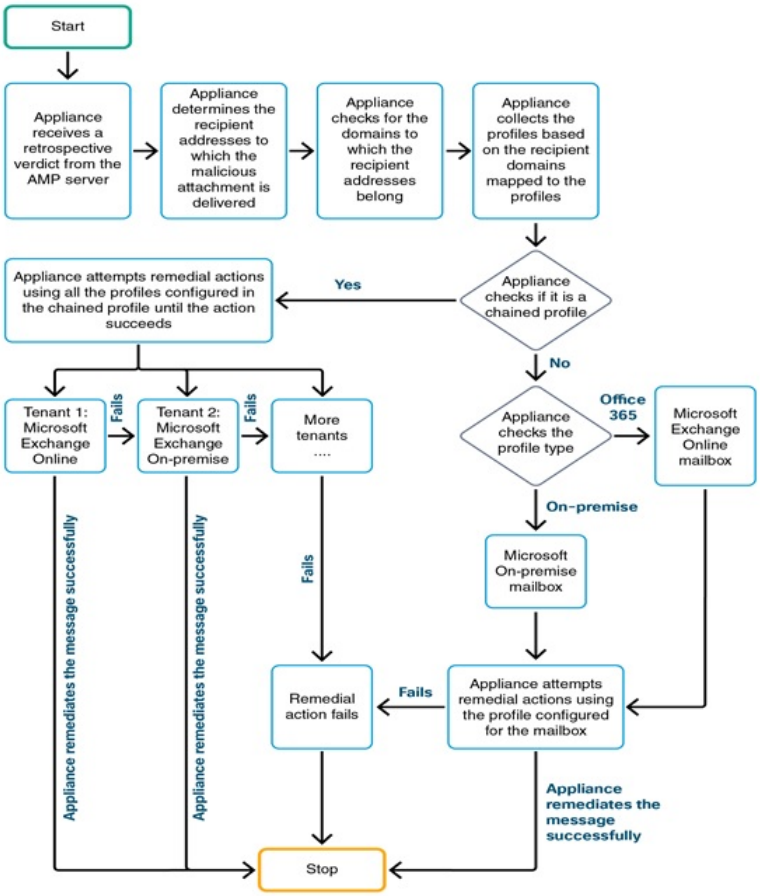
1. 添付ファイル付きメッセージが電子メールゲートウェイに到達します。
2. 電子メールゲートウェイは、添付ファイルのレピュテーションを評価するため、パブリック ファイル レピュテーション クラウド サーバにクエリを実行します。
3. パブリック ファイル レピュテーション クラウド サーバは、判定を電子メールゲートウェイに送信します。判定は、[正常（clean）] または [不明（unknown）] です。
4. 電子メールゲートウェイは、受信者へメッセージをリリースします。
5. 一定期間後に、電子メールゲートウェイはパブリック ファイル レピュテーション クラウド サーバから判定の更新を受け取ります。新しい判定は、[悪意のある（malicious）] です。
6. 電子メールゲートウェイは、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。

メッセージワークフローの検索と修復



1. メッセージが電子メールゲートウェイに到達します。
2. メッセージは受信者に配信されます。
3. 管理者はメッセージ トラッキング フィルタを使用して、受信者に配信されたメッセージを検索します。
4. ユーザは受信者のメールボックスから修正するメッセージを選択し、メッセージに修正アクションを適用します。
5. 電子メールゲートウェイは、受信者のメールボックスに存在するメッセージに対し、設定された修復アクションを実行します。

電子メールゲートウェイによる自動修復アクションの実行の仕組み



1. （メッセージを検索して修復する場合のみ）ユーザは、メッセージ トラッキング フィルタを使用して、ユーザメールボックスに配信されたメッセージを検索します。
2. （メッセージを検索して修復する場合のみ）：ユーザは修復するメッセージを選択し、そのメッセージに修復アクションを適用します。
3. （メッセージを自動修復する場合のみ）電子メールゲートウェイがパブリック ファイル レピュテーション クラウド サーバからレトロスペクティブな判定を受信すると、電子メールゲートウェイはメールボックスの修復プロセスを開始します。
4. （メッセージを自動修復する場合のみ）電子メールゲートウェイは、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。
5. 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。

6. その受信者ドメインに基づいて、電子メールゲートウェイ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。

7. 電子メールゲートウェイは、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、電子メールゲートウェイ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。電子メールゲートウェイは、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、電子メールゲートウェイ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。

8. 電子メールゲートウェイは、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 （27 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 メールボックス内のメッセージに対する修復アクションの実行 （6 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内のメッセージに対する修復アクションの実行 （9 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内のメッセージに対する修復アクションの実行 （11 ページ）

Microsoft Exchange Online 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

ユーザメールボックスのメッセージの修復を実行するように電子メールゲートウェイを設定できます。

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電子メールゲートウェイを設定できます。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電子メールゲートウェイを設定することができます。

ユーザメールボックスにすでに配信されているメッセージに対して、手動で修復アクションを実行できます。たとえば、着信メッセージをモニタする管理者は、メッセージ トラッキング フィルタを使用して、ユーザメールボックス内のメッセージに対して修復アクションを実行できます。

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 （15 ページ）

	操作内容	詳細
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、電子メールゲートウェイを登録します。	Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録 （17 ページ）
ステップ 3	電子メールゲートウェイでアカウント設定を有効にします。	電子メールゲートウェイでメールボックスの修復機能を有効にします。 電子メールゲートウェイでのアカウント設定の有効化 （19 ページ）

	操作内容	詳細
ステップ 4	電子メールゲートウェイで [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。	ユーザメールボックスの Office 365 プロファイルを作成し、電子メールゲートウェイ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。 • 次のパラメータの値 - 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電子メールゲートウェイの登録 （17 ページ） のステップ 9 を参照してください。 • クライアント証明書ベースの通信の場合は、次のパラメータの値を取得します。 • .pem 形式の証明書の秘密キー。「セキュアな通信の証明書」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電子メールゲートウェイの登録 （17 ページ） のステップ 8 を参照してください。 • クライアント シークレット ベースの通信の場合は、Azure 管理ポータルで作成したアプリケーションの生成されたクライアントシークレットの値を取得します。Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録 （17 ページ） 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 （20 ページ）を参照してください。

	操作内容	詳細
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 （23 ページ）を参照してください。
ステップ 6	（自動的にメッセージを修復する場合のみ）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、電子メールゲートウェイを設定します。	メールボックス内のメッセージに対する自動修復アクションの設定 （24 ページ）
ステップ 7	（メッセージを検索して修復する場合のみ）エンドユーザに送信されるメッセージに対して修復アクションを手動で実行するように電子メールゲートウェイを設定します。	メールボックス内のメッセージの検索と修復 （25 ページ）

MicrosoftExchangeオンプレミス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

Exchange オンプレミスサーバ上のメールボックスからメッセージを修復するように電子メールゲートウェイを設定できます。メッセージは、電子メールゲートウェイによって自動的に修復することも、ユーザがメッセージ トラッキング フィルタを使用して手動で修復することもできます。

電子メールゲートウェイは、偽装権限があるユーザ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アカウントは、電子メールゲートウェイ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で作成する必要があります。

（注） シスコでは、Microsoft Exchange 2013、2016 および 2019 でのみメールボックス自動修復機能を検証しました。

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 （16 ページ）
ステップ 2	電子メールゲートウェイでアカウント設定を有効にします。	電子メールゲートウェイでメールボックスの修復機能を有効にします。 電子メールゲートウェイでのアカウント設定の有効化 （19 ページ）
ステップ 3	電子メールゲートウェイで [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。	ユーザメールボックスのオンプレミスプロファイルを作成し、電子メールゲートウェイ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 （20 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 （23 ページ）を参照してください。
ステップ 5	（自動的にメッセージを修復する場合のみ）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、電子メールゲートウェイを設定します。	メールボックス内のメッセージに対する自動修復アクションの設定 （24 ページ）
ステップ 6	（メッセージの検索と修復のみ）オンプレミス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を設定します。	メールボックス内のメッセージの検索と修復 （25 ページ）

ハイブリッド展開の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

単一の電子メールゲートウェイでハイブリッド 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。メッセージは、電子メールゲートウェイによって自動的に修復することも、ユーザがメッセージ トラッキング フィルタを使用して手動で修復することもできます。

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、電子メールゲートウェイ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。

電子メールゲートウェイは AMP サーバ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。

ユーザメールボックスに配信されるメッセージを手動で検索して修正するには、メッセージ トラッキング フィルタを使用します。このフィルタを使用すると、修復するメッセージを選択して、修復アクションを設定し、メッセージに修復アクションを適用できます。

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 （15 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、電子メールゲートウェイを登録します。	Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録 （17 ページ）

	操作内容	詳細
ステップ 3	電子メールゲートウェイでアカウント設定を有効にします。	電子メールゲートウェイでメールボックスの修復機能を有効にします。 電子メールゲートウェイでのアカウント設定の有効化 （19 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。	ユーザメールボックスのアカウントプロファイルを作成し、電子メールゲートウェイ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。
		• 次のパラメータの値 - 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電子メールゲートウェイの登録 （17 ページ） のステップ 9 を参照してください。
		• クライアント証明書ベースの通信の場合は、次のパラメータの値を取得します。
		  • .pem 形式の証明書の秘密キー。「セキュアな通信の証明書」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電子メールゲートウェイの登録 （17 ページ） のステップ 8 を参照してください。
		• クライアント シークレット ベースの通信の場合は、Azure 管理ポータルで作成したアプリケーションの生成されたクライアントシークレットの値を取得します。Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録 （17 ページ） 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 （20 ページ） を参照してください。

	操作内容	詳細
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 （22 ページ）を参照してください。
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 （23 ページ）を参照してください。
ステップ 7	（自動的にメッセージを修復する場合のみ）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、電子メールゲートウェイを設定します。	メールボックス内のメッセージに対する自動修復アクションの設定 （24 ページ）
ステップ 8	（メッセージを検索して修復する場合のみ）メッセージに修復アクションを適用します。	メールボックス内のメッセージの検索と修復 （25 ページ）

電子メールゲートウェイでのメールボックス修復機能の設定

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

（注） 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は、ユーザメールボックス内のメッセージに対して検索および修復アクションを実行する際には必要ありません。

ユーザ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をメールボックス自動修復機能で設定するには、次の条件を満たしていることを確認してください。

- 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電子メールゲートウェイに追加していること。
- 電子メールゲートウェイ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）。

Office 365 アカウント

Azure AD に、電子メールゲートウェイ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。

セキュアな通信のクライアントシークレットまたは証明書

Office 365 サービスと電子メールゲートウェイ間の通信を保護するには、次のタスクのいずれかを実行する必要があります。

- Azure 管理ポータルで生成したアプリケーションのクライアントシークレットを生成します。

- 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します。

  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（<admin_username>@<domain>.com）が設定されていること。
  - 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。

（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。

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。

オンプレミス アカウントのメッセージ修復の前提条件

- （メールボックス自動修復の場合のみ） 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 （15 ページ）
- （任意）Microsoft Exchange Web サービス（EWS）証明書のインポート （16 ページ）
- 偽装ロールへのユーザの追加 （17 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

（注） 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は、ユーザメールボックス内のメッセージに対して検索および修復アクションを実行する際には必要ありません。

ユーザ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をメールボックス自動修復機能で設定するには、次の条件を満たしていることを確認してください。

- 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電子メールゲートウェイに追加していること。
- 電子メールゲートウェイ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）。

（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から電子メールゲートウェイ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

電子メールゲートウェイは偽装権限があるユーザ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で偽装権限があるユーザ アカウントを作成する必要があります。 電子メールゲートウェイはこのユーザ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アカウントを作成します。このユーザアカウントは、電子メールゲートウェイ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電子メールゲートウェイの登録

Office 365 サービスは、ユーザ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電子メールゲートウェイがアクセスするには、Azure AD で電子メールゲートウェイを登録しなければなりません。Azure AD で電子メールゲートウェイ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 （15 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、ユーザがサインインして電子メールゲートウェイを使用できる 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。
- Directory.Read.All：Azure Active Directory からユーザまたはグループ情報を読み取って、シスコ クラウド環境に設定されている LDAP サーバに保存します。

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 次のタスクのいずれかを実行して、Office 365 サービスと電子メールゲートウェイ間の通信を保護します。

- Azure 管理ポータルで生成したアプリケーションのクライアントシークレットを生成します。

  （注） クライアントシークレットの値は、Azure 管理ポータルへの後続のログイン時に表示されないため、必ずコピーしてください。

- 公開キー証明書のキークレデンシャルでアプリケーションマニフェストを更新します。次の操作を行ってください。

  1. 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
     ```

2. 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。
3. 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。

- Client 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

電子メールゲートウェイでのアカウント設定の有効化 （19 ページ）

電子メールゲートウェイ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。

- （メールボックスの自動修復でのみ必要）電子メールゲートウェイで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こと。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 電子メールゲートウェイにログインします。

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 （オプション）電子メールゲートウェイ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 （オプション）ハイブリッドメール交換サーバへの接続がタイムアウトする前に 電子メールゲートウェイ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 （オプション）ローカルメール交換サーバへの接続がタイムアウトする前に電子メールゲートウェイ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 （20 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、電子メールゲートウェイ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。 電子メールゲートウェイでのアカウント設定の有効化（19 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 電子メールゲートウェイにログインします。

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、次の詳細情報を入力する場合に選択します。
  - 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。
  - クライアントのクレデンシャルを検証するには、次のいずれかの方法を選択します。
    - [クライアントシークレット（Client Secret）]：Azure 管理ポータルで生成したアプリケーションのクライアントシークレットを入力する場合に選択します。
    - [クライアント証明書（Client Certificate）]：証明書のサムプリント（$base64Thumbprint の値）を入力し、[ファイルの選択（Choose File）] をクリックして、証明書の秘密キーを .pem 形式でアップロードする場合に選択します。
- [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 （17 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 電子メールゲートウェイが Microsoft Exchange Online サーバまたは Microsoft Exchange オンプレミスサーバ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。
電子メールゲートウェイがメールボックス サーバ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 （27 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 （22 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 （23 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電子メールゲートウェイ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 電子メールゲートウェイにログインします。

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）
- 電子メールゲートウェイ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。
- 電子メールゲートウェイには、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 （23 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、電子メールゲートウェイ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電子メールゲートウェイ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 電子メールゲートウェイにログインします。

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

- メールボックス内のメッセージに対する自動修復アクションの設定 （24 ページ）
- メールボックス内のメッセージの検索と修復 （25 ページ）

メールボックス内のメッセージに対する自動修復アクションの設定

（注） メールボックス自動修復機能で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を設定する場合は、次の手順を実行します。

はじめる前に

メールボックスの自動修復機能が有効になっており、アプライアンスでアカウントの設定が完了していることを確認します。電子メールゲートウェイでのアカウント設定の有効化 （19 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] を選択します。

ステップ 2 変更するメール ポリシーの [高度なマルウェア防御（Advanced Malware Protection）] カラム内のリンクをクリックします。

ステップ 3 [メールボックス自動修復の有効化（Enable Mailbox Auto Remediation）] を選択します。

ステップ 4 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 5 変更を送信し、保存します。

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 （26 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 （27 ページ）
- メールボックス修復のトラブルシューティング （27 ページ）

メールボックス内のメッセージの検索と修復

はじめる前に

- 電子メール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いること、およびアカウントの設定が完了していることを確認します。電子メールゲートウェイでのアカウント設定の有効化 （19 ページ）を参照してください。
- 電子メールゲートウェイでメッセージトラッキングを有効にします。メッセージトラッキングの有効化を参照してください。
- 中央集中型メッセージトラッキングサービスを使用している場合は、管理対象の電子メールゲートウェイで Trailblazer ポートと AsyncOS API HTTP ポートが有効になっていること、および Cisco Secure Email and Web Manager が Trailblazer ポートにアクセスできることを確認します。Trailblazer ポートが無効になっている場合は、 Cisco Secure Email and Web Manager が、管理対象の 電子メールゲートウェイの AsyncOS API HTTP ポートにアクセスできることを確認します。

（注） 次の手順は、 電子メールゲートウェイの新しい Web インターフェイスでのみ実行できます。

手順

ステップ 1 レガシー Web インターフェイスの [Eメールセキュリティアプライアンスの外観が新しくなりました。お試しください（Email Security Appliance is getting a new look. Try it!!）] リンクをクリックします。Web ベースのグラフィカル ユーザー インターフェイス（GUI）へのアクセスを参照してください。

ステップ 2 [Tracking] タブをクリックします。

ステップ 3 [メッセージ（Messages）] タブをクリックし、検索結果を絞り込みます。詳細については、新しい Web インターフェイスでの電子メール メッセージの検索を参照してください。

ステップ 4 修復するメッセージを選択します。一度に最大 1000 件のメッセージを選択できます。配信済みのメッセージのみを修復できます。

ステップ 5 [修復（Remediate）] をクリックします。

ステップ 6 次の詳細を入力します。

- 修正対象のバッチ名を入力します。
- 次の修復アクションのいずれかを選択します
  - メッセージを削除する。悪意のあるメッセージ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。
  - 1 つの電子メールアドレス、またはセミコロン（;）で区切った複数の電子メールアドレスに転送する。指定したユーザ（電子メール管理者など）に悪意のあるメッセージを転送する場合は、このオプションを選択します。

- 1 つの電子メールアドレス、またはセミコロン（;）で区切った複数の電子メールアドレスに転送してからメッセージを削除する。指定したユーザ（電子メール管理者など）に悪意のあるメッセージを転送した後に、そのメッセージ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 7 **[Apply]**をクリックします。

[適用（Apply）] をクリックすると、[メッセージトラッキング（Message Tracking）] ページの右下隅にある [修復レポートのステータス（Remediation Report Status）] ウィジェットを表示できます。このウィジェットを使用して修復レポートの生成ステータスを確認します。修復レポートの生成が完了したら、ウィジェットの [詳細の表示（View Details）] をクリックして修復レポートに移動し、修復結果を表示します。

（注） また、[レポート（Reports）]>[ユーザレポート（User Reports）]>[修復レポート（Remediation Report）] に移動し、[メールボックスの検索と修復（Mailbox Search And Remediate）] タブをクリックして、修復レポートを直接表示することもできます。

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 （26 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 （27 ページ）
- メールボックス修復のトラブルシューティング （27 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電子メールゲートウェイの登録 （17 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

[修復（Remediation）] レポートページを使用して、メールボックスの修復結果の詳細を表示できます。レポートを表示するには、次の手順を行います。

1. **レガシー Web インターフェイスの [Eメールセキュリティアプライアンスの外観が新しくなりました。**お試しください（Email Security Appliance is getting a new look. Try it!!）] リンクをクリックします。
2. [モニタリング（Monitoring）] タブをクリックします。
3. [レポート（Reports）] ドロップダウンメニューをクリックし、[修復レポート（Remediation Report）] を選択します。

このレポートを使用して次の詳細情報を表示します。

- [メールボックスの自動修復（Mailbox Auto Remediation）] と [メールボックスの検索と修復（Mailbox Search and Remediate）] を使用して修復が試行されたメッセージの合計数。
- 設定された修正アクションに対して正常に修復されたメッセージの数。
- 修復が失敗したメッセージの数。
- 修復が試行されたメッセージの詳細。

詳細については、[修復レポート（Remediation Report）] ページを参照してください。

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（Message Tracking）]ページの[メールボックスの検索と修復（Mailbox Search and Remediate）] を使用して、修復されたメッセージの詳細を表示できます。修復を開始する前に、[メッセージトラッキング（Message Tracking）] が有効になっていることを確認します。

（注） メールボックス自動修復機能を使用して修復が試みられたメッセージは、トラッキングの検索結果に含まれません。

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）] > [メールボックスの設定（Mailbox Settings）][アカウントの設定（Account Settings）]）で 電子メールゲートウェイ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 `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。
`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。

エラー メッセージ	理由とソリューション
`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。 • 電子メールゲートウェイの時間帯は、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。
`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から 電子メールゲートウェイ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。メールボックスの自動修復機能またはメールボックス検索と修復アクションに関する情報：
  - 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。
  - 修復ステータス
  - 修復が失敗した理由。
  - 修復が成功および失敗した受信者。
  - 検索および修復アクションが開始された送信元。
  - 検索および修復アクションを開始したユーザ。
  - メッセージに対して実行された修復アクション。
- 修復ログ。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 電子メールゲートウェイと Microsoft Exchange サービスとの間の接続の問題

問題

電子メールゲートウェイと 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電子メールゲートウェイ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。

- 電子メールゲートウェイと 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。

  電子メールゲートウェイ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。

または

ユーザは、[メッセージトラッキング（Message Tracking）] ページの [修復（Remediate）] オプションを使用してメッセージを手動で修復できません。

ソリューション

次の手順を実行します。

- 電子メールゲートウェイと 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 （20 ページ） を参照してください。
- （メールボックス自動修復の場合のみ）「電子メールゲートウェイと Exchange Online サービスおよびExchange 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 （30 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。