Cisco Eメールセキュリティにおける高度なマルウェア防御(AMP)のベストプラクティスガイド

内容

概要

Advanced Malware Protection(AMP)は、マルウェアの検出とブロック、継続的な分析、およびレトロスペクティブアラートを可能にする包括的なソリューションです。Cisco Eメールセキュリティ(ESA)でAMPを活用すると、高度なマルウェア防御に対する最もコスト効率の高い簡単なアプローチにより、攻撃前、攻撃中、攻撃後の一連の攻撃に対する優れた保護が可能になります。

このベストプラクティスドキュメントでは、次に示すように、Cisco Eメールセキュリティアプライアンス(ESA)のAMPの主な機能について説明します。

- **ファイルレピュテーション**:ESAを通過する各ファイルのフィンガープリントをキャプチャし、AMPのクラウドベースのインテリジェンスネットワークに送信してレピュテーション判定を行います。これらの結果から、悪意のあるファイルを自動的にブロックし、管理者定義のポリシーを適用できます。
- **ファイル分析**:ESAを通過する未知のファイルを分析する機能を提供します。安全性の高いサンドボックス環境により、AMPはファイルの動作に関する正確な詳細情報を取得し、そのデータを人間およびマシンの詳細な分析と組み合わせてファイルの脅威レベルを決定できます。この性質はAMPクラウドベースのインテリジェンスネットワークに取り込まれ、AMPクラウドデータセットを動的に更新および拡張して保護を強化するために使用されます。
- **Mailbox Auto Remediation(MAR)**:Microsoft Office 365およびExchange 2013/2016の場合、最初のインスペクション後に悪意のあるファイルが含まれた電子メールの削除を自動化します。これにより、管理者の作業時間が節約され、脅威の影響を抑えることができます。
- **Cisco AMP Unity**：組織がAMP with AMPサブスクリプションを含むAMP対応デバイスをAMP for Endpointsコンソールに登録できるようにする機能です。このような統合により、AMP for Endpointsコンソールがすでにエンドポイントに提供しているのと同じ方法でCisco Eメールセキュリティを確認して照会し、単一のユーザインターフェイスですべての脅威ベクトルにファイル伝搬データを関連付けることができます。
- **Cisco Threat Response**：シスコおよびサードパーティのソースからのセキュリティ関連情報を1つの直感的な調査および応答コンソールにまとめるオーケストレーションプラットフォー

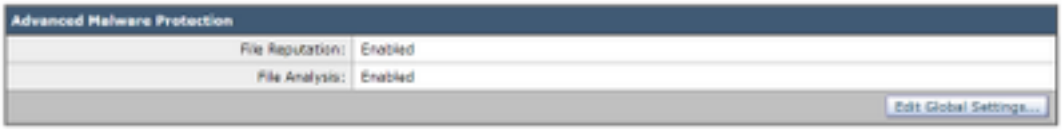
ムです。これは、イベントログと脅威インテリジェンスの統合フレームワークとして機能するモジュラ設計によって実現されます。モジュールにより、関係グラフを作成してデータの迅速な関連付けを可能にします。これにより、セキュリティチームは攻撃の明確なビューを取得し、効果的な対応を迅速に行うことができます。

機能キーの確認

- ESAで、[System Administration] > [Feature Keys]に移動します
- ファイルレピュテーションおよびファイル分析の機能キーを探し、ステータスがアクティブであることを確認します

高度なマルウェア防御(AMP)の有効化

- ESAで、[Security Services] > [Advanced Malware Protection - File Reputation and Analysis]に移動します
- [高度なマルウェア保護のグローバル設定]の[有効]ボタンをクリックします。



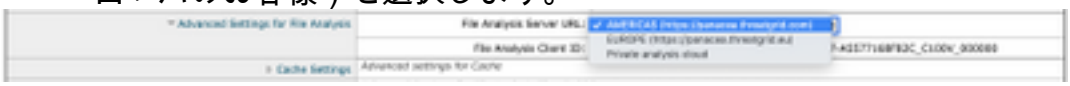
- 変更を保存します。

高度なマルウェア防御(AMP)グローバル設定のカスタマイズ

- AMPが有効になりました。[グローバル設定の編集]をクリックして、グローバル設定をカスタマイズします。
- ファイル拡張子の一覧は随時自動的に更新されるため、常にこの設定を参照し、すべてのファイル拡張子が選択され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の詳細設定を展開する
- File Reputation Serverのデフォルト選択はAMERICA(cloud-sa.amp.cisco.com)です
- ドロップダウンメニューをクリックし、最も近いファイルレピュテーションサーバを選択します（特にAPJCおよびヨーロッパのお客様）。

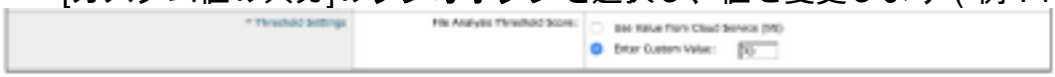
- ファイル分析の詳細設定を展開する
- File Analysis Server URLのデフォルト選択はAMERICAS(https://panacea.threatgrid.com)です
- ドロップダウンメニューをクリックし、最も近いファイルレピュテーションサーバ（特にヨーロッパのお客様）を選択します。



ファイル分析のしきい値設定

（オプション）ファイル分析スコアの上限しきい値を設定できます。しきい値設定に基づいてブロックされたファイルは、高度なマルウェア防御レポートの[着信マルウェア脅威ファイル(Incoming Malware Threat Files)]セクションに[カスタムしきい値(Custom Threshold)]として表示されます。

- AMPグローバル設定ページで、[Threshold Settings]を展開します。
- クラウドサービスのデフォルト値は95です。
- [カスタム値の入力]のラジオボタンを選択し、値を変更します（例：70）。

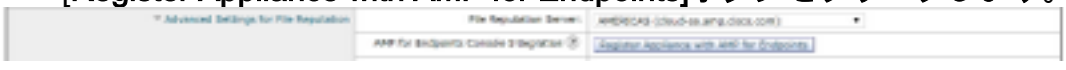


- [送信]をクリックし、[変更を確定]をクリックします

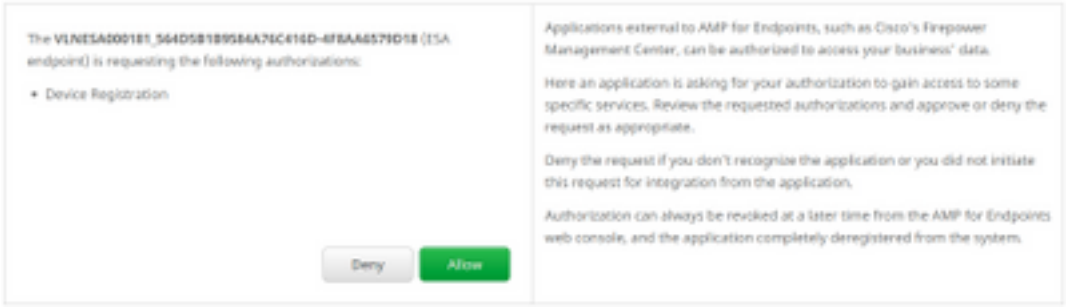
ESAとAMP for Endpointsコンソールの統合

（エンドポイント向けAMPの場合のみ）ユニファイドカスタムファイルブロックリスト（またはファイルAllowlist）は、AMP for Endpointsコンソールを使用して作成でき、ESAを含むセキュリティアーキテクチャ全体に格納戦略をシームレスに配布できます。

- AMPグローバル設定ページで、[ファイルレピュテーションの詳細設定]を展開します
- [Register Appliance with AMP for Endpoints]ボタンをクリックします。



- [OK]をクリックして、AMP for Endpointsコンソールサイトにリダイレクトし、登録を完了します。
- ユーザクレデンシャルを使用してAMP for Endpointsコンソールにログインします
- [Allow authorization the ESA registration:



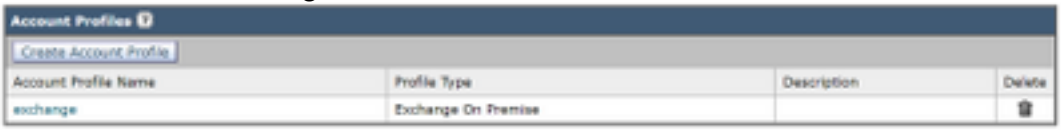
- AMP for Endpointsコンソールは、ページを自動的にESAにピボットします。
- 登録ステータスが[SUCCESS]と表示されていることを確認します。

- [Submit]をクリックし、[Commit your changes]をクリックします

メールボックス自動修復(MAR)の有効化

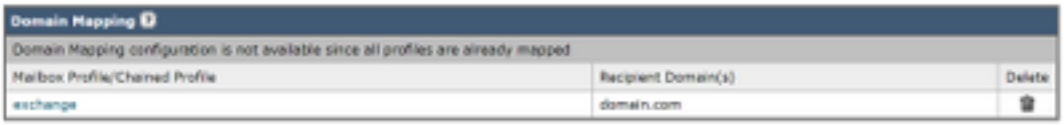
O365メールボックスまたはMicrosoft Exchange 2013/2016のメールボックス自動修復(MAR)機能を使用すると、ファイルレピュテーションの判定がClean/UnknownからMaliciousに変更されたときにアクションを実行できます。

- [システム管理] > [アカウント設定]に移動します
- [アカウントプロファイル]で[アカウントプロファイルの作成]をクリックし、Office 365またはMicrosoft Exchangeのメールボックスを使用してAPI接続プロファイルを作成します。



- [Submit]をクリックし、[Commit your changes]をクリックします

- （オプション）チェーンプロファイルはプロファイルの集合であり、チェーンされたプロファイルにアクセスするアカウントが展開の異なるテナント間に存在する場合にのみ設定します。
- [ドメインマッピングの作成]ボタンをクリックして、アカウントプロファイルを受信者ドメインにマッピングします。推奨される設定を次に示します。



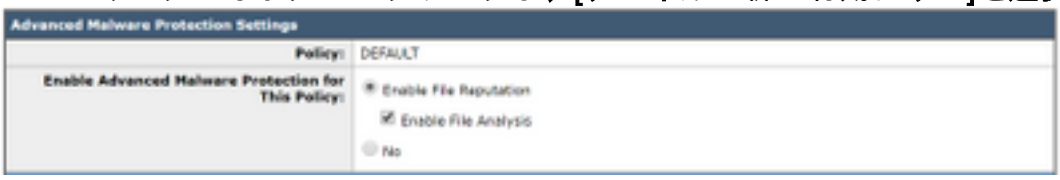
- [Submit]をクリックし、[Commit your changes]をクリックします

メールポリシーの高度なマルウェア防御(AMP)の設定

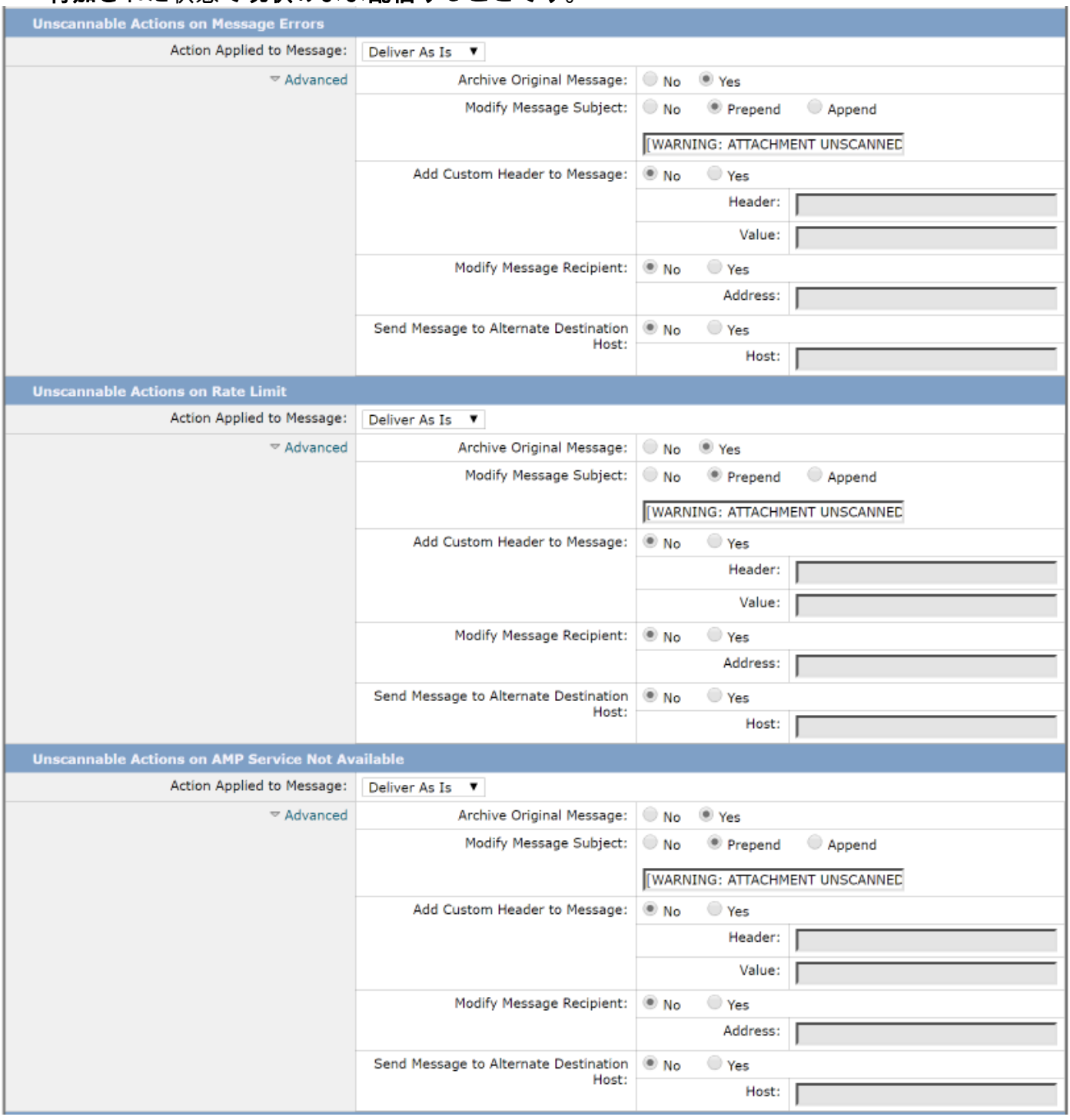
AMPとMARがグローバルに設定されたら、サービスをメールポリシーに対して有効にできます。

- [メールポリシー(Mail Policies)] > [着信メールポリシー(Incoming Mail Policies)]に移動します
- 受信メールポリシーの高度なマルウェア保護の設定をカスタマイズするには、カスタマイズするポリシーの[高度なマルウェア保護]の下の青いリンクをクリックします。

- このベストプラクティスのドキュメントでは、[ファイルレピュテーションを有効にする]の横にあるラジオボタンをクリックし、**[ファイル分析を有効にする]を選択します。**

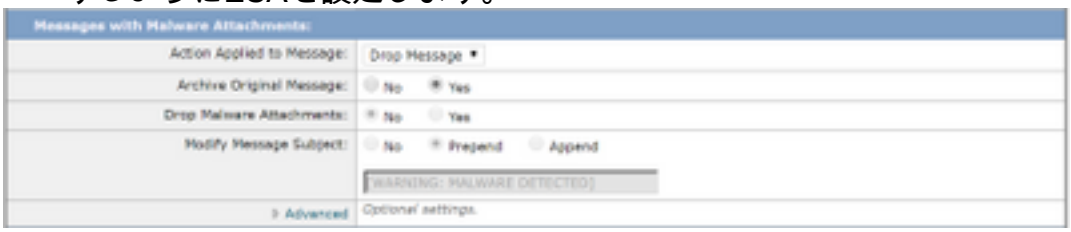


- AMPの結果をメッセージに**するXヘッダーを含めることをお勧めします。**
- 次の3つのセクションでは、メッセージエラー、レート制限、またはAMPサービスが使用できない場合に、添付ファイルがスキャン不能と見なされる場合にESAが実行する必要があるアクションを選択できます。推奨されるアクションは、メッセージの件名に**警告テキストが付加された状態で現状のまま配信することです。**

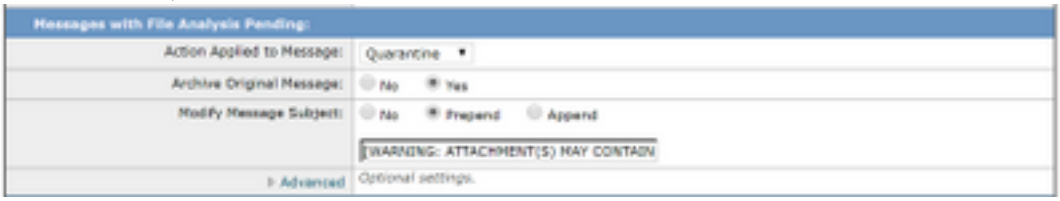


- 次のセクションでは、添付ファイルが悪意があると考えられる場合にメッセージをドロップ

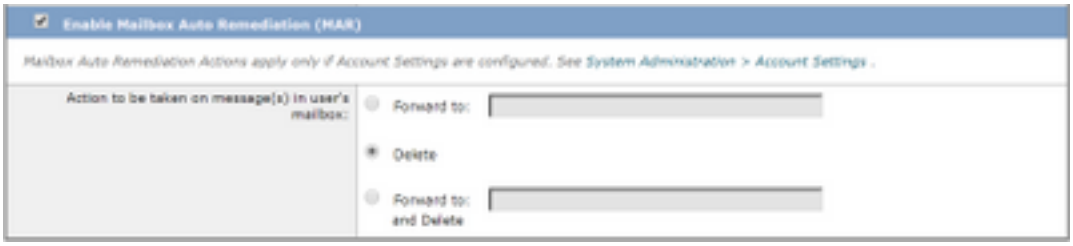
するようにESAを設定します。



- ファイル分析のために添付ファイルが送信された場合は、メッセージを検疫することをお勧めします。



- （受信メールポリシーのみ）脅威の判定が悪意に対して変化した場合に、エンドユーザに配信されるメッセージに対して実行される修復アクションを構成します。推奨される設定を次に示します。

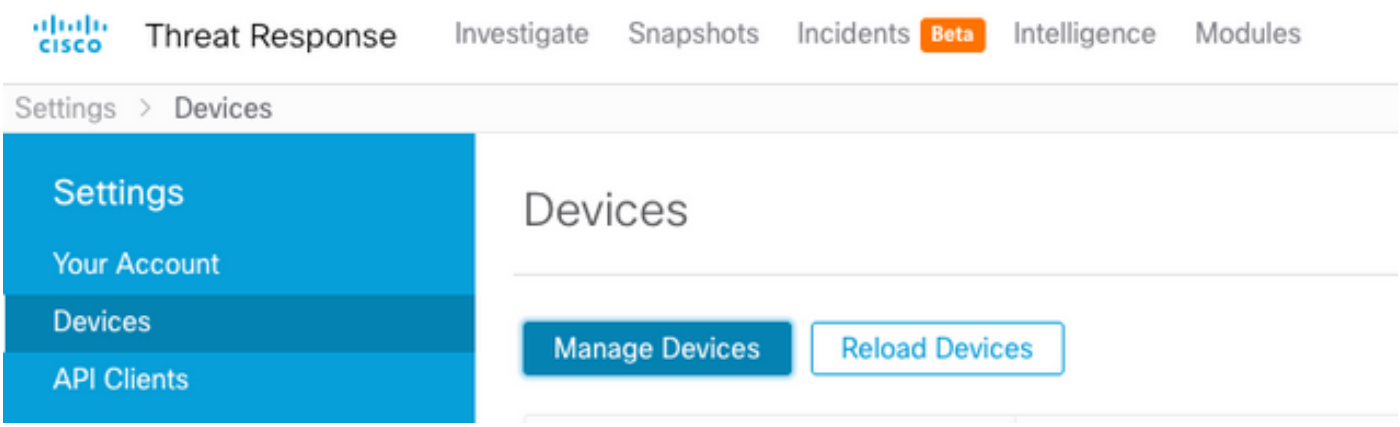


- [Submit]をクリックし、[Commit your changes]をクリックします

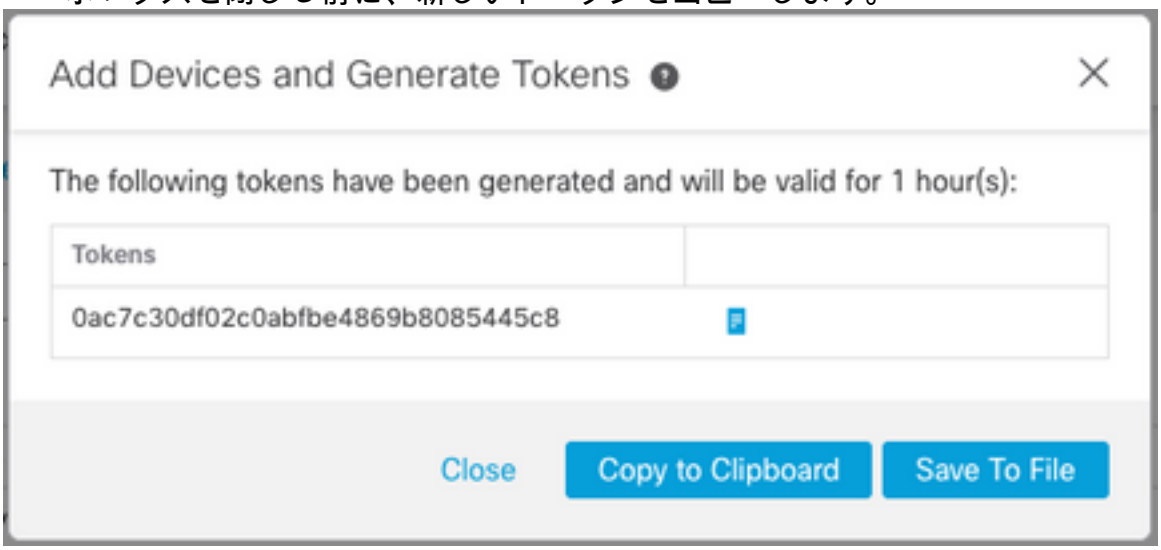
SMAとCisco Threat Response(CTR)の統合

SMA Eメールモジュールを統合するには、CTR経由でセキュリティサービス交換(SSE)を使用する必要があります。SSEを使用すると、SMAをExchangeに登録でき、登録されたデバイスにアクセスするためのCisco Threat Responseの明示的な権限を付与できます。このプロセスでは、SMAをリンクする準備ができたときに生成されるトークンを介してSSEにリンクします。

- CTRポータル(https://visibility.amp.cisco.com)で、ユーザクレデンシャルを使用してログインします。
- CTRはモジュールを使用して、ESAを含む他のシスコセキュリティ製品と統合します。[モジュール]タブをクリックします。
- [Devices]を選択し、[Manage Devices]をクリックします。



- CTRはページをSSEにピボットします。
- +アイコンをクリックして、新しいトークンを生成し、[続行]をクリックします。
- ボックスを閉じる前に、新しいトークンをコピーします。

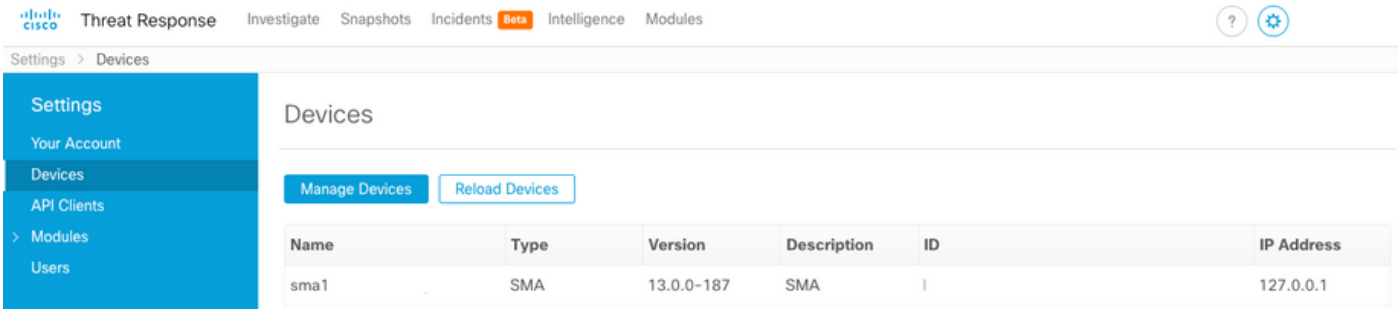


- SMAで、[Management Appliances]タブ> [**Network**] > [**Cloud Service Settings**]に移動します
- [Edit Setting]をクリックし、[Threat Response]オプションが[**Enable**]であることを確認します。
- Threat Response Server(THREAT)のURLは**AMERICAS(api-sse.cisco.com)で、ヨーロッパのお客様の場合は、ドロップダウンメニューをクリックし、EUROPE(api.eu.sse.itd.cisco.com)を選択します。**

- [**Submit**]をクリックし、[**Commit** your changes]をクリックします
- Cloud Services Settingにトークンキー（CTRポータルから生成したキー）を貼り付け、[Register]をクリックします。

- 登録プロセスが完了するまでに時間がかかります。数分後にこのページに戻り、ステータスを再度確認してください。
- [CTR] > [Modules] > [Device] に戻り、[Reload Device] ボタンをクリックしてSMAがリストに

表示されることを確認します。



結論

このドキュメントでは、Eメールセキュリティアプライアンス(ESA)でのCisco Advanced Malware Protection(AMP)のデフォルト設定またはベストプラクティス設定について説明します。これらの設定のほとんどは、着信および発信の電子メールポリシーの両方で使用でき、設定とフィルタリングは両方向で推奨されます。