SSL 証明書の管理

この章では、Threat Grid アプライアンスの SSL 証明書と、統合されたアプライアンスおよびデバイスの管理について説明します。説明する項目は次のとおりです。

SSL 証明書と Threat Grid アプライアンスの概要

Threat Grid アプライアンスを通過するネットワーク トラフィックは、SSL を使用してすべて暗号化されます。次の情報は、E メール セキュリティ アプライアンス（ESA）、Web セキュリティアプライアンス（WSA）、AMP for Endpoints プライベートクラウドといった統合先との Threat Grid アプライアンスの接続をサポートするように SSL 証明書を設定する手順の実行に役立ちます。

（注） SSL 証明書を管理する方法の詳細は、このガイドの説明範囲に含まれていません。

SSL を使用するインターフェイス

SSL を使用する Threat Grid アプライアンスには、次の 2 つのインターフェイスがあります。

- Threat Grid ポータルの UI と API、および統合先（ESA/WSA アプライアンス、AMP for Endpoints プライベートクラウド配置更新サービス）用の**クリーン**インターフェイス。
- OpAdmin ポータル用の**管理**インターフェイス。

サポートされている SSL/TLS バージョン

Threat Grid アプライアンスでは、次のバージョンの SSL/TLS がサポートされています。

- TLS v1.0：管理インターフェイスでは無効（v2.7 以降）
- TLS v3.0：管理インターフェイスでは無効（v2.7 以降）
- TLS v1.2

（注） TLS v1.0 と TLS v3.0 は、管理インターフェイスでは無効になっており（v2.7 以降）、メインアプリケーションでもデフォルトでは無効になっています。これらのプロトコルのいずれかが統合の互換性のために必要な場合は、TGSH から再有効化できます（メインアプリケーションに対してのみ）。

サポートされているお客様提供の CA 証明書

お客様提供の CA 証明書がサポートされており（v2.0.3 以降）、お客様独自の信頼できる証明書または CA 証明書をインポートすることができます。

自己署名デフォルト SSL 証明書

Threat Grid アプライアンスは、自己署名 SSL 証明書とキーのセットがインストールされて出荷されます。1 つのセットがクリーンインターフェイス用で、もう一つのセットが管理インターフェイス用です。管理者はこれらの SSL 証明書を置き換えることができます。

Threat Grid アプライアンスのデフォルト SSL 証明書のホスト名（共通名）は **pandem** で、10 年間有効です。設定時に別のホスト名が Threat Grid アプライアンスに割り当てられた場合、証明書内のホスト名と共通名は一致しなくなります。

証明書内のホスト名は、接続先の ESA アプライアンスや WSA アプライアンス、または他の統合先のシスコデバイスやサービスによって想定されるホスト名とも一致している必要があります。多くのクライアントアプリケーションは、証明書で使用される共通名がアプライアンスのホスト名と一致する SSL 証明書を必要とするためです。

インバウンド接続用の SSL証明書の設定

E メールセキュリティアプライアンス、Web セキュリティアプライアンス、AMP for Endpoints プライベートクラウドなどのシスコのセキュリティ製品は、Threat Grid アプライアンスと統合してサンプルを送信することができます。このような統合は Threat Grid アプライアンスから見ればインバウンド接続になります。

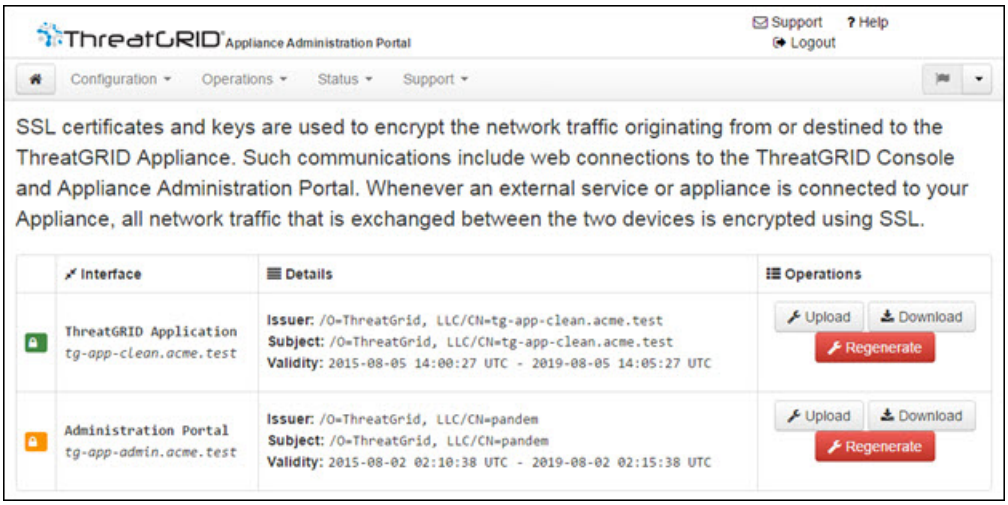
統合するアプライアンスまたは他のデバイスは、Threat Grid アプライアンスの SSL 証明書を信頼できる必要があります。まず、ホスト名が共通名と一致していることを確認する必要があります。一致していない場合は、再生成するか置き換える必要があります。その後、Threat Grid

アプライアンスからSSL証明書をエクスポートし、統合するアプライアンスまたはサービスにインポートする必要があります。

インバウンドSSL接続に使用されるThreat Gridアプライアンスの証明書は、[**SSL Certificate**]ページで設定されます。クリーンインターフェイスと管理インターフェイス用のSSL証明書は別々に設定することができます。

ステップ1 OpAdminポータルで、**[Configuration] > [SSL]** をクリックして、SSL証明書の設定ページを開きます。

図 *1 : SSL* 証明書の設定ページ



この例では、クリーンインターフェイス用の「**ThreatGRID Application**」と管理インターフェイス用の「**Administration Portal**」という2つのSSL証明書を取り上げます。

ステップ2 SSL証明書で使用されている共通名（緑色の南京錠アイコン）とホスト名が一致することを確認します。「SSL 証明書の共通名の検証」を参照してください。

SSL 証明書の共通名の検証

ホスト名は、Threat Gridアプライアンスの SSL証明書で使用される共通名と一致している必要があります。

[SSL Certificate]ページで、インターフェイス名の左側の列にある南京錠アイコンは、SSL証明書のステータスを示しています。

- **緑色**：インターフェイスのホスト名がSSL証明書で使用されている共通名と一致していることを示します。
- **黄色**：インターフェイスのホスト名がSSL証明書で使用されている共通名と一致していないことを示します。現在のホスト名を使用している証明書に置き換える必要があります（「SSL 証明書の置き換え」を参照）。

SSL 証明書の置き換え

通常、SSL 証明書は、証明書が期限切れになった、ホスト名が変更された、または他のシスコデバイスやサービスとの統合をサポートするためなど、さまざまな理由からいずれかの時点で置き換える必要があります。

Cisco E メールセキュリティアプライアンス、Web セキュリティアプライアンスなどの CSA シスコ統合デバイスでは、記載の共通名が Threat Grid アプライアンスのホスト名と一致する SSL 証明書が必要になる場合があります。デフォルトの SSL 証明書を、同じホスト名を使用して Threat Grid アプライアンスにアクセスする、新たに生成された証明書に置き換える必要があります。

Threat Grid アプライアンスを AMP for Endpoints プライベートクラウドと統合して、その配置更新サービスを使用する場合は、Threat Grid アプライアンスが接続を信頼できるように、AMP for Endpoints プライベートクラウド SSL 証明書をインストールする必要があります。

Threat Grid アプライアンスで SSL 証明書を交換するには、複数の方法があります。

- 共通名に現在のホスト名を使用するSSL 証明書の再作成します。
- SSL 証明書のダウンロードします。
- SSL 証明書のアップロードします。これは市販の SSL や企業向けの SSL の場合もあれば、OpenSSL を使用して作成したものである場合もあります。
- OpenSSL を使用した SSL 証明書の作成

SSL 証明書の再作成

ホスト名が証明書の共通名と一致しない場合は、[**SSL Certificate**] ページで SSL 証明書を再生成できます。

ステップ 1 OpAdmin ポータルで、 **[Configuration] > [SSL]** をクリックして [**SSL Certificate**] ページを開きます。

ステップ 2 [Operations] 列で、新しい証明書を必要とするインターフェイスのための [**Regenerate**] をクリックします。

新しい自己署名 SSL 証明書が Threat Grid アプライアンス上で生成されます。この証明書の [Common Name] フィールドでは、アプライアンスの現在のホスト名が使用されます。インターフェイス名の横にある [Common Name] 検証用の南京錠アイコンが緑色に変わります。

再生成された証明書（SSL 証明書のダウンロードファイル）を**ダウンロード**して、統合するアプライアンスにインストールできるようになりました。

SSL 証明書のダウンロード

Threat Grid アプライアンスの SSL 証明書を統合先のデバイスにダウンロードしてインストールし、Threat Grid アプライアンスからの接続をデバイスが信頼できるようにすることができます。

ステップ 1 OpAdmin ポータルで、**[Configuration] > [SSL]** をクリックして、SSL 証明書の設定ページを開きます。

ステップ 2 [Operations] 列で、インターフェイス証明書の [**Download**] をクリックします。SSL 証明書の **.cert** ファイルがダウンロードされます。

ステップ 3 ダウンロードした SSL 証明書（**.cert** ファイル）を、E メール セキュリティ アプライアンス、Web セキュリティアプライアンス、AMP For Endpoints プライベートクラウド、または他のシスコ製品に、製品マニュアルに従ってインストールします。

SSL 証明書のアップロード

組織で商用または企業向けの SSL 証明書をすでに運用している場合は、その証明書を使用して Threat Grid アプライアンス用の新しい SSL 証明書を生成し、統合先のデバイスに対して CA 証明書を使用することができます。

ステップ 1 OpAdmin ポータルで、 **[Configuration] > [SSL]** をクリックして [**SSL Certificate**] ページを開きます。

ステップ 2 [Operations] 列で、適切なインターフェイスの [**Upload**] をクリックします。

インターフェイス名の横にある [Common Name] 検証用の南京錠アイコンが緑色に変わります。

OpenSSL を使用した SSL 証明書の作成

オンプレミスの SSL 証明書インフラストラクチャが設置されていない場合、OpenSSL を使用して SSL 証明書を手動で生成し、Threat Grid アプライアンスにアップロードすることができます（「SSL 証明書のアップロード」を参照）。OpenSSL は、OpenSSL 証明書、キー、その他のファイルを作成および管理するための標準的なオープンソース SSL ツールです。

（注） OpenSSL はシスコ製品ではないため、テクニカルサポートは提供されません。OpenSSL の使用方法の詳細については、Web を検索することをお勧めします。シスコは、SSL 証明書を生成するための SSL ライブラリ *Cisco SSL* を提供しています。

ステップ 1 次のコマンドを実行して、新しい自己署名 SSL 証明書を生成します。

```
openssl req -x509 -days 3650 -newkey rsa:4096 -keyout tgapp.key -nodes -out
tgapp.cert -subj "/C=US/ST=New York/L=Brooklyn/O=Acme Co/CN=tgapp.acmeco.com"
```

openssl：OpenSSL

req：X.509 証明書署名要求（CSR）管理の使用を指定します。X.509 は、キーおよび証明書の管理に SSL と TLS が使用する公開キーインフラストラクチャの標準規格です。次の例では、このパラメータを使用して、新しい X.509 証明書を作成します。

-x509：証明書署名要求を生成せずに、自己署名証明書を作成するように req パラメータ X.509 を変更します。

-days 3650：このオプションは、証明書が有効と見なされる期間を設定します。この例では、10 年間に設定されています。

-newkey rsa: 4096：新しい証明書と新しいキーを同時に生成するように指定します。必要なキーが事前に作成されなかったため、証明書を使用して作成する必要があります。パラメータ「**rsa:4096**」は、4096 ビット長の RSA キーを作成することを示します。

-keyout：このパラメータは、作成中の秘密キーファイルが OpenSSl によって保存される場所を示します。

-nodes：このパラメータは、パスフレーズを使用して証明書を保護するためのオプションを OpenSSL がスキップする必要があることを示します。サーバの起動時に、アプライアンスは、ユーザの介入なしでファイルを読み取ることができる必要があります。パスフレーズで保護されている証明書の場合、サーバの再起動のたびにユーザがパスフレーズを入力する必要があります。

-out：このパラメータは、作成中の証明書が OpenSSL によって保存される場所を示します。

-subj（例）：

- **C=US**：国
- **ST=New York**：州
- **L=Brooklyn**：場所
- **O=Acme Co**：所有者の名前
- **CN=tgapp.acmeco.com**：Threat Grid アプライアンスの FQDN（完全修飾ドメイン名）を入力します。この名前には、Threat Grid アプライアンスのホスト名（この例では **tgapp**）と、関連するドメイン名（この例では **acmeco.com**）が含まれます。

  重要　Threat Grid アプライアンスのクリーンインターフェイスの FQDN と一致するように、少なくとも共通名を変更する必要があります。

ステップ 2　新しい SSL 証明書が生成されたら、**[SSL Certificate]** ページから Threat Grid アプライアンスに証明書をアップロードします（「SSL 証明書のアップロード」を参照）。E メール セキュリティ アプライアンスまたは Web セキュリティアプライアンスに証明書（**.cert** ファイルのみ）をアップロードする必要もあります。

アウトバウンド接続用の SSL 証明書の設定

Threat Grid アプライアンス（v2.0.3 以降）は、配置更新サービス用の Cisco AMP for Endpoints プライベートクラウドとの統合をサポートしています。この統合は、Threat Grid アプライアンスから見ればアウトバウンド接続になります。

DNS の設定

デフォルトで、DNS はダーティインターフェイスを使用します。AMP for Endpoints プライベートクラウドなど、統合先のアプライアンスまたはサービスのホスト名がダーティインターフェイスで解決できない（統合にクリーンインターフェイスが使用されるため）場合は、クリーンインターフェイスを使用する別の DNS サーバを OpAdmin で設定できます。

ステップ 1 OpAdmin で、**[Configuration] > [Network]** をクリックします。

ステップ 2 ダーティネットワークとクリーンネットワークの [**DNS**] フィールドに入力します。

ステップ 3 **[Save]** をクリックします。

CA 証明書の管理

OpAdmin ポータルの [**CA Certificate**] ページは、アウトバウンド SSL 接続用の CA 証明書信頼ストアを管理するために使用されます。この機能により、Threat Grid アプライアンスは、Cisco AMP For Endpoints プライベートクラウドを信頼して、悪意があると見なされた分析済みサンプルについて通知することができます。

ステップ 1 OpAdmin ポータルで、**[Configuration] > [CA Certificates]** をクリックします。

ステップ 2 次のインポートオプションのいずれかを選択します。

- サーバから証明書を取得するには、[**Import from Host**] を選択します。AMP for Endpoints プライベートクラウドの [**Host**] と [**Port**] に入力してから、[**Retrieve**] をクリックします。
- [**Import from Clipboard**] を選択し、クリップボードから PEM を貼り付けた後、[**Add Certificate**] をクリックします。

ステップ 3 **[インポート (Import)]** をクリックします。

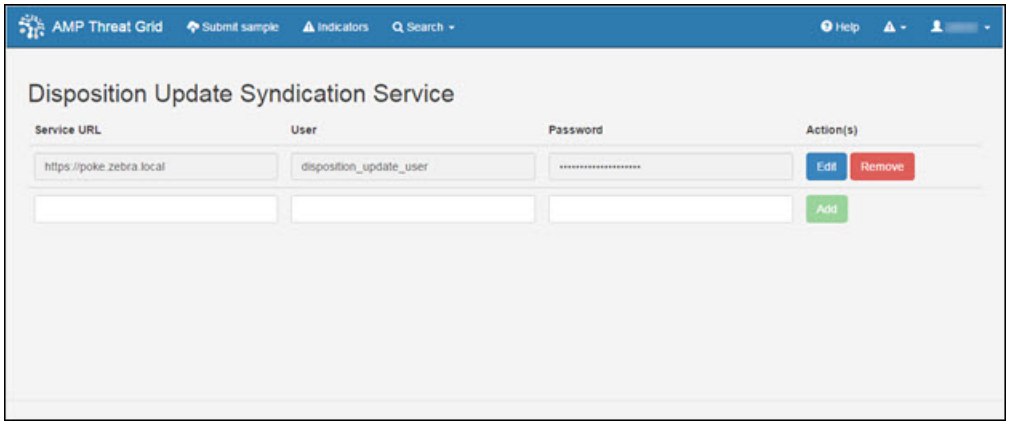
配置更新の配信サービスの管理

Threat Grid portal ユーザインターフェイスで、AMP for Endpoints プライベート クラウド アプライアンスの統合に向けて、配置更新の配信サービスを管理できます。URL は、[**Disposition Update Syndication Service**] ページで追加、編集、削除できます。

（注） AMP for Endpoints プライベート クラウド アプライアンスの統合に関する詳細については、「AMP for Endpoints プライベートクラウドを Threat Grid アプライアンスに接続する」を参照してください。

ステップ 1 Threat Grid ポータルで、ログイン名の横にあるナビゲーションバーのドロップダウンをクリックし、[**Manage FireAMP Integration**] を選択して、[**Disposition Update Syndication Service**] ページを開きます。

図 *2:* 配置更新の配信サービス



ステップ 2 次の情報を入力します。

- [**Service URL**]：AMP For Endpoints プライベートクラウドの URL。
- [**User**]：管理者ユーザ名。
- [**Password**]：AMP for Endpoints 設定ポータルによって提供されるパスワード。

ステップ 3 [**Config**] をクリックします。

ESA/WSA の Threat Grid アプライアンスへの接続

E メールセキュリティアプライアンス（ESA）、Web セキュリティアプライアンス（WSA）その他のアプライアンス、デバイス、サービスなどのシスコ製品は、SSL で暗号化された接続を

使用して Threat Grid アプライアンスと統合し、分析用のマルウェアサンプルを送信することができます。

ESA/WSA と Threat Grid アプライアンスの統合は、Cisco Sandbox API（CSA API）によって有効にされます。この統合は、多くの場合 CSA 統合と呼ばれます。

統合先の ESA/WSA は、分析用のサンプルを送信する前に、Threat Grid アプライアンスに登録する必要があります。統合先の ESA/WSA を Threat Grid アプライアンスに登録するには、まず ESA/WSA の管理者が、使用中のアプライアンスとネットワーク環境に適した SSL 証明書接続をセットアップする必要があります。

このセクションでは、Threat Grid アプライアンスと通信できるように ESA、WSA その他のシスコ製品を設定するために必要な手順について説明します。

ESA および WSA のマニュアル

ESA/WSA の製品マニュアルで、「Enabling and Configuring File Reputation and Analysis Services」の手順を参照してください。

（注） これらのマニュアルで、Threat Grid アプライアンスは、多くの場合「分析サービス」または「プライベートクラウドファイル分析サーバ」と呼ばれています。

- 『*Cisco Email Security Appliance User Guides*』
- 『*Cisco Web Security Appliance User Guides*』

ESA と WSA の統合プロセスの概要

このセクションでは、Threat Grid アプライアンスと E メール セキュリティ アプライアンス（ESA）、Web セキュリティアプライアンス（WSA）、その他の CSA 統合（インバウンド）間の接続を設定する手順の概要を示します。詳細については、「ESA/WSA の統合プロセスの手順」を参照してください。

SSL 証明書の設定

Threat Grid アプライアンスの SSL 証明書の SAN（サブジェクト代替名）または CN（共通名）は、ホスト名および ESA/WSA の想定と一致している必要があります。統合先の ESA/WSA との接続を成功させるには、統合先の ESA/WSA が Threat Grid アプライアンスの識別に使用するものと同じホスト名にする必要があります。

要件に応じて、Threat Grid アプライアンスで自己署名 SSL 証明書を再生成する必要があります。その際、[SAN/CN] フィールドには現在のホスト名が入力されます。この証明書を作業環境にダウンロードし、統合先の ESA/WSA にアップロードしてインストールできます。

あるいは、企業向けの SSL 証明書や市販の SSL 証明書（または手動で生成した証明書）をアップロードして、現在の Threat Grid アプライアンスの SSL 証明書と置き換えなければならない

こともあります。詳細な手順については、「インバウンド接続用の SSL証明書の設定」を参照してください。

接続の確認

SSL 証明書の設定が完了したら、次の手順として、ESA/WSA が Threat Grid アプライアンスと通信できることを確認します。

ESA/WSA は、ネットワーク経由で Threat Grid アプライアンスのクリーンインターフェイスに接続できる必要があります。製品マニュアルの手順に従って、Threat Grid アプライアンスと ESA/WSA が相互に通信できることを確認します（ESA/WSA の Threat Grid アプライアンスへの接続を参照）。

ESA/WSA ファイル分析設定の実行

ファイル分析セキュリティサービスを有効にし、詳細設定を実行します。

ESA/WSA の Threat Grid アプライアンスへの登録

製品マニュアルに従って設定された ESA/WSA は、自動的に Threat Grid アプライアンスに登録されます。接続先デバイスの登録時に、デバイス ID がログイン ID となる新しい Threat Grid ユーザが自動的に作成され、同じ ID に基づく名前を使用して新しい組織が作成されます。管理者は、新しいデバイスユーザアカウントをアクティブにする必要があります。

Threat Grid アプライアンスでの新しい ESA/WSA アカウントのアクティブ化

ESA/WSA または他の統合が Threat Grid アプライアンスに接続して登録されると、新しい Threat Grid ユーザアカウントが自動的に作成されます。ユーザアカウントの初期ステータスは、非アクティブになっています。Threat Grid アプライアンス管理者は、分析用のマルウェアサンプルの送信に使用する前に、デバイスユーザアカウントを手動でアクティブにする必要があります。

ESA/WSA の統合プロセスの手順

ESA/WSA 間の接続は、Threat Grid アプライアンスから見れば受信になります。この統合では CSA API を使用します。

（注） 実行する必要のあるタスクの詳細については、ESA および WSA 製品のマニュアルを参照してください。

ステップ 1 Threat Grid アプライアンスを通常どおりに（まだ統合されていない状態で）セットアップして設定します。更新を確認し、必要に応じてインストールします。

ステップ 2 ESA/WSA を通常どおりに（まだ統合されていない状態で）セットアップして設定します。

ステップ 3 Threat Grid アプライアンスの SSL 証明書 の SAN または CN は、現在のホスト名および ESA/WSA の想定と一致している必要があります。自己署名 SSL 証明書を展開する場合は、（Threat Grid アプリケーションのクリーンインターフェイスで）新しい SSL 証明書を生成し、必要に応じてデフォルトと置き換え、ダウンロードして ESA/WSA にインストールします（「SSL 証明書の置き換え」を参照）。

（注） Threat Grid アプライアンスのホスト名が SAN または CN になっている証明書を生成してください（Threat Grid アプライアンスのデフォルトの証明書は機能しません）。IP アドレスではなく、ホスト名を使用します。

ステップ 4 ESA/WSA が、ネットワークを介して Threat Grid アプライアンスのクリーンインターフェイスに接続できることを確認します。

ステップ 5 Threat Grid アプライアンスの統合に使用する ESA/WSA を設定します。詳細な手順については、ESA/WSA 製品のマニュアルを参照してください。次の手順は ESA に特有のものですが、現在最も一般的なタイプの統合です。

a) **[Security Services] > [File Reputation and Analysis]** をクリックします。
b) [Enable] をクリックします。
c) [Edit Global Settings] をクリックします。
d) [**File Analysis**] セクションでは、ファイル分析がデフォルトで有効になっています。この機能を有効にしない場合は、[**Enable File Analysis**] チェックボックスをオフにします。オフにしないと、次回のコミット後にファイル分析の機能キーがアクティブになります。分析のためにクラウドに送信するファイルタイプを選択します。
e) ESA または WSA の製品マニュアルに従い、必要に応じてファイル分析の [**Advanced Settings**] を設定します。

- [**File Analysis Server URL**]：プライベートクラウドを選択します。
- [**Server**]：オンプレミスの Cisco Threat Grid アプライアンスの URL。この値と証明書には、ホスト名（IP アドレスではない）を使用します。
- [**SSL Certificate**]：オンプレミスの Threat Grid アプライアンスで生成した自己署名証明書をアップロードします。最後にアップロードされた自己署名証明書が使用されます。最新の証明書より前にアップロードされた証明書にアクセスすることはできません。必要ならば、該当する証明書を再びアップロードします。

ステップ 6 変更を送信し、保存します。

ページの下部に表示される**ファイル分析クライアント ID** を確認します。この ID で、アクティブ化されるユーザを識別できます。

Threat Grid アプライアンスへの ESA/WSA の登録は、ファイル分析の設定を送信すると自動的に実行されます。

ステップ 7 Threat Grid アプライアンスで新しいデバイスのユーザアカウントをアクティブ化します。

a) 管理者として Threat Grid ポータルにログインします。
b) ログイン名の横にあるナビゲーションバーのドロップダウンメニューから、[**Manage Users**] を選択して Threat Grid [**Users**] ページを開きます。

c) デバイス ユーザ アカウントの [User Details] ページを開きます（探すために検索を使用する必要がある場合があります）。
d) ユーザの現在のステータスは、非アクティブになっています。[Re-Activate User] をクリックします。
e) 確認ダイアログで、[**Re-Activate**] をクリックしてアクションを確定します。

確定後、ESA/WSA その他の統合されるアプライアンスやデバイスが、Threat Grid アプライアンスとの接続を開始できるようになります。

AMP for Endpoints プライベートクラウドを Threat Grid アプライアンスに接続する

Threat Grid アプライアンスは、配置更新サービス用の AMP for Endpoints プライベートクラウドとの統合をアウトバウンド接続としてサポートします。

（注） 特に新しいアプライアンスを設定する場合は、Threat Grid アプライアンス配置更新サービスと AMP for Endpoints プライベートクラウドの統合の設定タスクを、指定された順序に従ってデバイスで実行する必要があります。すでにセットアップして設定されているアプライアンスを統合する場合は、順序はそれほど重要ではありません。

実行するタスクの詳細については、AMP for Endpoints プライベートクラウドのマニュアルを参照してください。

ステップ 1 Threat Grid アプライアンスを通常どおりに（まだ統合されていない状態で）セットアップして設定します。更新を確認し、必要に応じてインストールします。

ステップ 2 AMP for Endpoints プライベートクラウドを通常どおりに（まだ統合されていない状態で）セットアップして設定します。

ステップ 3 Threat Grid アプライアンスの OpAdmin ポータルで、必要に応じてデフォルトの証明書と置き換えるため、クリーンインターフェイスで SSL 証明書の再作成し、その証明書をダウンロードして AMP For Endpoints プライベート クラウド デバイスにインストールします。

AMP for Endpoints プライベート クラウドデバイスで統合を設定するために必要な次の情報を取得します。

- **ホスト名**：**[Configuration] > [Hostname]** をクリックし、ホスト名をメモします。
- **API キー**：Threat Grid ポータルの [**User Details**] ページから **API キー**をコピーします（ログイン名の横にあるドロップダウンをクリックし、[**Manage Users**] を選択して、統合ユーザアカウントに移動します）。

  （注） この手順を実行するには管理者ユーザでなければならないというわけではありません。Threat Grid アプライアンスで、この目的のために特別にユーザを作成することも可能です。

ステップ 4 Threat Grid アプライアンスとの統合に向けて、AMP for Endpoints プライベート クラウド デバイスを設定します。

a) **[Integrations] > [Threat Grid]** をクリックして、[**Connection to Threat Grid**] セクションに移動します。

b) 次のフィールドに入力します。

- [**Hostname**]：Threat Grid アプライアンスのホスト名を入力します（前の手順で取得）。
- [**API Key**]：統合に使用するアカウントの Threat Grid API キーを入力します（前の手順で取得）。
- [**SSL Certificate**]：Threat Grid アプライアンスの SSL 証明書ファイルを選択します。

c) [Save Configuration] をクリックします。

d) [Test Connection] をクリックします。

接続テストに成功したら、AMP for Endpoints プライベートクラウドで**再設定**を実行して変更を適用する必要があります。適用後、AMP が Threat Grid アプライアンスと通信できるようになり、Threat Grid にサンプルを送信することが可能になります。

ただし、配置更新サービスをセットアップするための残りの手順を実行して、配置結果を Threat Grid アプライアンスに伝達する必要があります。詳細については、AMP for Endpoints プライベートクラウドのユーザマニュアルを参照してください。

ステップ 5 OpAdmin ポータルで、配置更新の配信サービスをセットアップします。

a) 必要に応じて、DNS を設定します。「DNS の設定」を参照してください。

b) 統合先のデバイスを信頼できるように、AMP for Endpoints プライベートクラウド SSL 証明書を Threat Grid アプライアンスにダウンロードするかコピーして貼り付けます。「CA 証明書の管理」を参照してください。

c) 右上のメニューから、[**Manage FireAMP Integration**] を選択し、AMP 配置更新サービスの URL とログイン情報を指定します（「配置更新の配信サービスの管理」を参照してください）。

d) [**Config**] をクリックします。