組織とユーザの管理

この章では、Threat Grid で組織とユーザを管理する方法について説明します。説明する項目は次のとおりです。

はじめに

Threat Grid は、デフォルトの組織と管理者ユーザを使用して Threat Grid アプライアンスにインストールされます。セットアップとネットワーク設定が完了したら、ユーザがログインして分析用のマルウェアサンプルの送信を開始できるように、追加の組織とユーザアカウントを作成できます。

組織の構成によっては、組織、ユーザ、管理者を追加する際に複数のユーザやチーム間での計画と調整が必要になる場合があります。

新しい組織の作成

ユーザは常に特定の組織と関係しています。ユーザを追加する前に、まず組織を作成して、その組織にユーザを追加できるようにする必要があります。

重要 一度作成された組織をインターフェイスから削除することはできないため、このタスクは慎重に計画する必要があります。

ステップ 1 管理者として Threat Grid Portal にログインします。

ステップ 2 [**Administration**] メニューをクリックし、[**Manage Organization**] を選択します。[Organizations] ページが開き、アプライアンスで設定されているすべての組織が表示されます。

ステップ 3 ページの右上隅にある [**New organization**] をクリックして、[New Organization] ダイアログを開きます。

ステップ 4 以下の項目に入力します。

- [**Name**]：組織の名前を入力します（現在、名前にサイズ制限はありません）。
- [**Industry**]：[**Industry**] ドロップダウンリストからビジネスのタイプを選択します。該当する業界がリストにない場合は、[**Unknown**] に設定したままにし、Threat Grid サポート（support@threatgrid.com）に連絡してオプションの追加を依頼してください。
- [**ATS ID**]：高度な脅威サービス ID を入力します。

ステップ 5 [**送信 (Submit)**] をクリックします。新しい組織が作成され、[Organizations] リストに表示されます。

ステップ 6 新しく作成した組織を編集し、次の情報を入力します。

- [**Options**]：必要に応じて入力します。
- [**Rate Limit**]：デフォルトのユーザ送信レート制限を設定します。

  API レート制限は、ライセンス契約の条件に基づいて Threat Grid アプライアンス全体に適用されます。この制限は、API 送信のみに適用され、手動でのサンプル送信には適用されません。ライセンスのレート制限は、組織に適用されます。

  また、オンラインヘルプの「Using Threat Grid」で説明されているように、個々のユーザにサンプル送信レートを設定することもできます（ナビゲーションバーで **[Help] > [Using Threat Grid Online Help]** をクリックします）。

  レート制限は、暦日ではなく、24 時間単位の時間枠に基づきます。送信レートの上限に達すると、次の API 送信で、429 エラーと、再試行までの待機時間を示すメッセージが返されます。

組織が作成されると、管理者または組織の管理者がその組織を管理できます（オンラインヘルプの「Managing Organizations」を参照してください）。

ユーザの管理

ユーザの追加方法など、ユーザアカウントの作成と管理に関する手順とマニュアルについては、Threat Grid Portal UI のオンラインヘルプを参照してください。

ナビゲーションバーで、**[Help] > [Using Threat Grid Online help] > [Managing Threat Grid Users]** をクリックします。

（注） ユーザは、API のみで削除でき、サンプルを送信していない場合にのみ削除できます。

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デバイスを統合するためのデバイスユーザアカウントの管理については、「新しいデバイスユーザアカウントの有効化」を参照してください。

新しいデバイスユーザアカウントの有効化

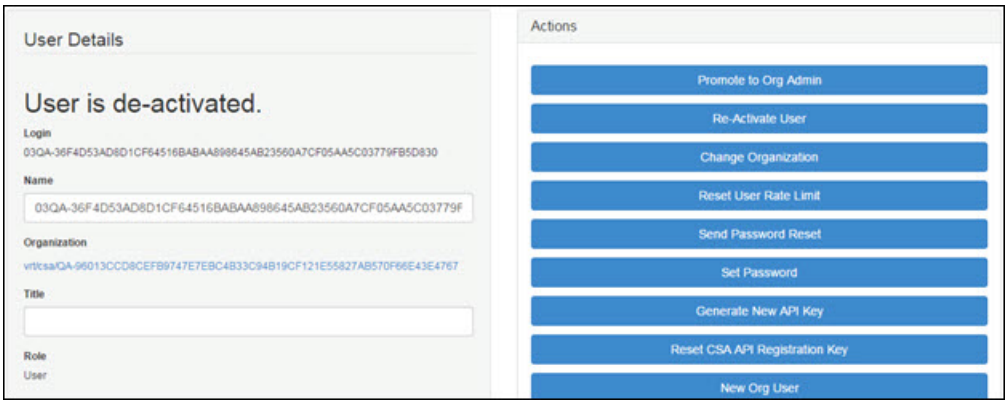
Cisco E メール セキュリティ アプライアンス、Web セキュリティアプライアンス、または他の Cisco Sandbox API 統合が Threat Grid アプライアンスに接続して登録されると、新しい Threat Grid ユーザアカウントが自動的に作成されます。ユーザアカウントの初期ステータスは、非アクティブになっています。デバイスユーザアカウントは、分析用のマルウェアサンプルの送信に使用する前に、Threat Grid アプライアンス管理者が手動でアクティブにする必要があります。

ステップ 1 管理者として Threat Grid ポータルにログインします。

ステップ 2 [**Administration**] メニューをクリックし、[**Manage Users**] を選択します。

ステップ 3 デバイスのユーザアカウントを見つけて、[**User Details**] ページを開きます。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。

図 *1* : ユーザの詳細



ステップ 4 [ユーザの再アクティブ化（Re-Activate User）] をクリックします。

ステップ 5 確認ダイアログで、[**Re-Activate User**] をクリックしてアクションを確定します。

確定後、統合するアプライアンスまたはデバイスが Threat Grid アプライアンスと通信できるようになります。