組織およびユーザー

Cisco Secure Malware Analytics は、デフォルトの組織および管理者ユーザーを使用して Cisco Secure Malware Analytics 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、ユーザー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ーアカウントを作成できます。

組織の構成によっては、組織、ユーザー、管理者を追加する際に複数のユーザー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。この章では、Cisco Secure Malware Analytics で組織とユーザーを管理する方法について説明します。内容は次のとおりです。

新規組織の作成

ユーザーは常に特定の組織と関係しています。ユーザーを追加する前に、まず組織を作成して、その組織にユーザーを追加できるようにする必要があります。新しい組織を作成するには、管理者としてログインする必要があります。これは、Cisco Secure Malware Analytics ポータル UI の **[組織の管理（Managing Organizations）]** ページで実行します。

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。

手順

ステップ 1 Cisco Secure Malware Analytics ポータルに管理者としてログインします。

ステップ 2 **[管理（Administration）]** メニューをクリックし、**[組織の管理（Manage Organization）]** を選択します。**[組織（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。

組織およびユーザー

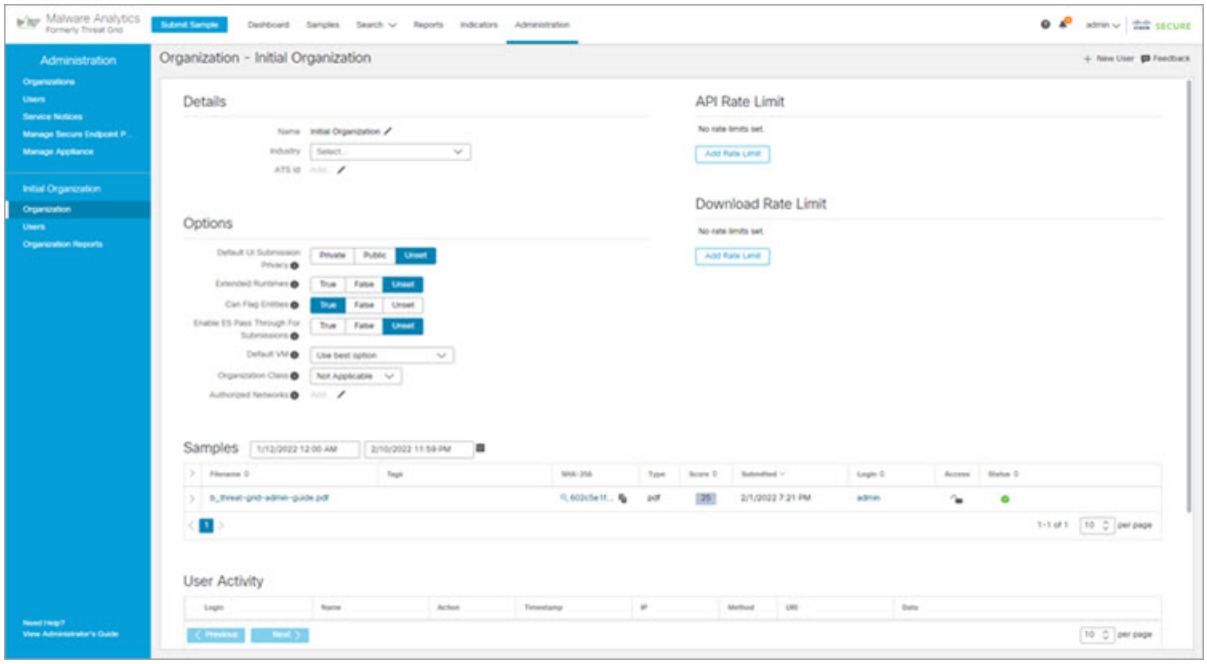
ステップ 3 ページの右上隅にある **[新しい組織（New organization）]** をクリックして、**[新しい組織（New organization）]** ダイアログを開きます。

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）。
- **業界（Industry）** - **[業界（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、Cisco Secure Malware Analytics サポート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。

図 *1*: デフォルトの初期組織の組織ページ



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ー送信レート制限を設定します。

  API レート制限は、ライセンス契約条件に基づいて Cisco Secure Malware Analytics 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。

  Cisco Secure Malware Analytics ポータルのオンラインヘルプに記載されているように、個々のユーザーにサンプル送信レートを設定することもできます。

  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れを管理できます。

ユーザーの管理

ユーザーの追加方法など、ユーザー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、Cisco Secure Malware Analytics 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、**[ヘルプ（Help）] > [Cisco Secure Malware Analytics オンライン ヘルプの使用（Using Secure Malware Analytics Online Help）] > [Cisco Secure Malware Analytics ユーザーの管理（Managing Secure Malware Analytics Users）]** をクリックします。

（注） ユーザーは、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 ユーザー アカウントの管理については、「新しいデバイスユーザーアカウントの有効化」を参照してください。

組織とユーザーの削除

組織とユーザーは、管理者ユーザーが Cisco Secure Malware Analytics API を使用して削除できます。組織は、ユーザーがいない場合にのみ削除できます。ユーザーが含まれている場合は、組織を削除する前にユーザーを削除する必要があります。ただし、サンプルを送信していない場合にのみユーザーを削除できます。

- 組織を削除するには、Cisco Secure Malware Analytics API（/api/v3/organizations/:org-id）と DELETE を使用します。
- ユーザーを削除するには、Cisco Secure Malware Analytics API（/api/v3/users/:user-id）と DELETE を使用します。

API エンドポイントの詳細については、Cisco Secure Malware Analytics ポータルのオンラインヘルプを参照してください。

新しいデバイスユーザーアカウントの有効化

Cisco Email Security アプライアンス、Web Security アプライアンス、または他の Cisco Sandbox API 統合が Cisco Secure Malware Analytics アプライアンスに接続して登録されると、新しい Cisco Secure Malware Analytics ユーザーアカウントが自動的に作成されます。ユーザー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。Cisco Secure Malware Analytics アプ

組織およびユーザー

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、デバイスユーザーアカウントを手動でアクティブにする必要があります。

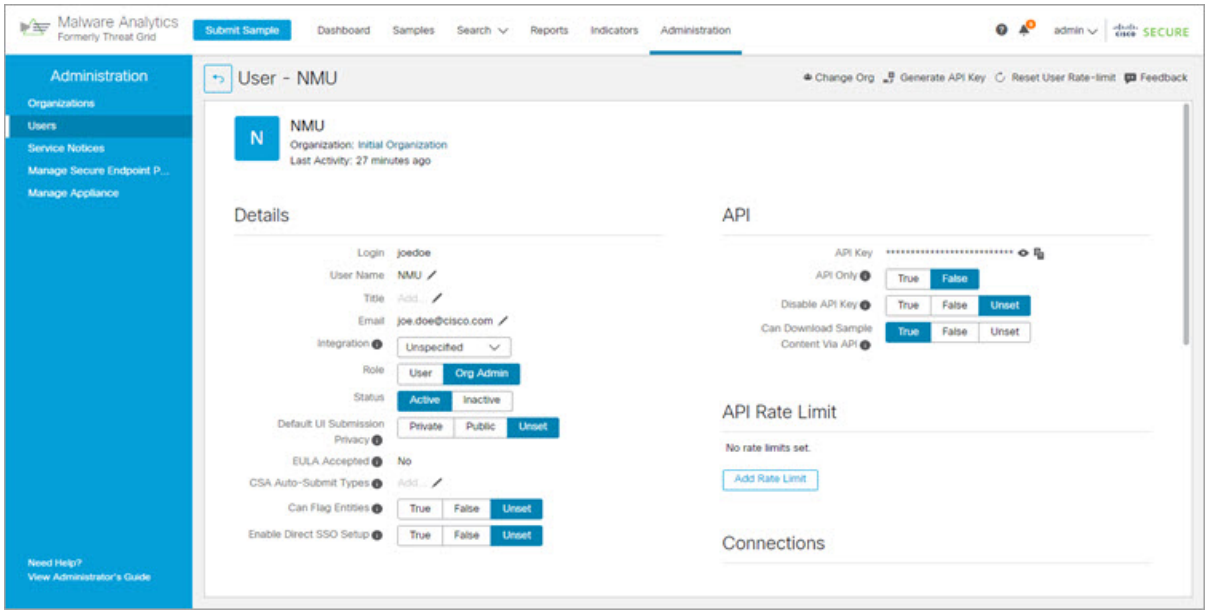
手順

ステップ 1 Cisco Secure Malware Analytics ポータル UI に管理者としてログインします。

ステップ 2 **[管理（Administration）]** メニューをクリックし、**[ユーザーの管理（Manage Users）]** を選択します。

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

図 *2:* ユーザの詳細



ユーザー ステータスは現在 **非アクティブ**です。

ステップ 4 [Activate] をクリックします。

ステップ 5 確認ダイアログで、アクションを確認します。

これで、統合するアプライアンスまたはデバイスが Cisco Secure Malware Analytics アプライアンスと通信できるようになります。

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。