XDRデバイスの洞察と包括的な統合のトラブルシューティング

内容

概要

このドキュメントでは、統合を設定し、XDR Device InsightsとCisco Umbrellaの統合をトラブルシューティングする手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- XDR
- Umbrella
- APIの基礎知識
- Postman APIツール

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- XDR

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

XDR Device Insightsは、組織内のデバイスの統合ビューを提供し、統合されたデータソースのインベントリを統合します。

Umbrellaは、現在の脅威に対してステージングされた攻撃者のインフラストラクチャを自動的に検出し、悪意のある要求が組織のネットワークまたはエンドポイントに到達する前に事前にブロックします。統合により、マルウェア感染を早期に阻止し、すでに感染しているデバイスを迅速に特定し、データの漏洩を防ぐことができます。この統合により、すべての場所とユーザにわたるインターネットアクティビティが完全に可視化され、2クリックで対応できるため、ドメインを迅速にブロックできます。複数のUmbrella関数がサポートされ、Umbrellaプラットフォームで生成されたAPIキーを介してリンクされます。

構成の詳細については、統合モジュールの詳細を参照してください。

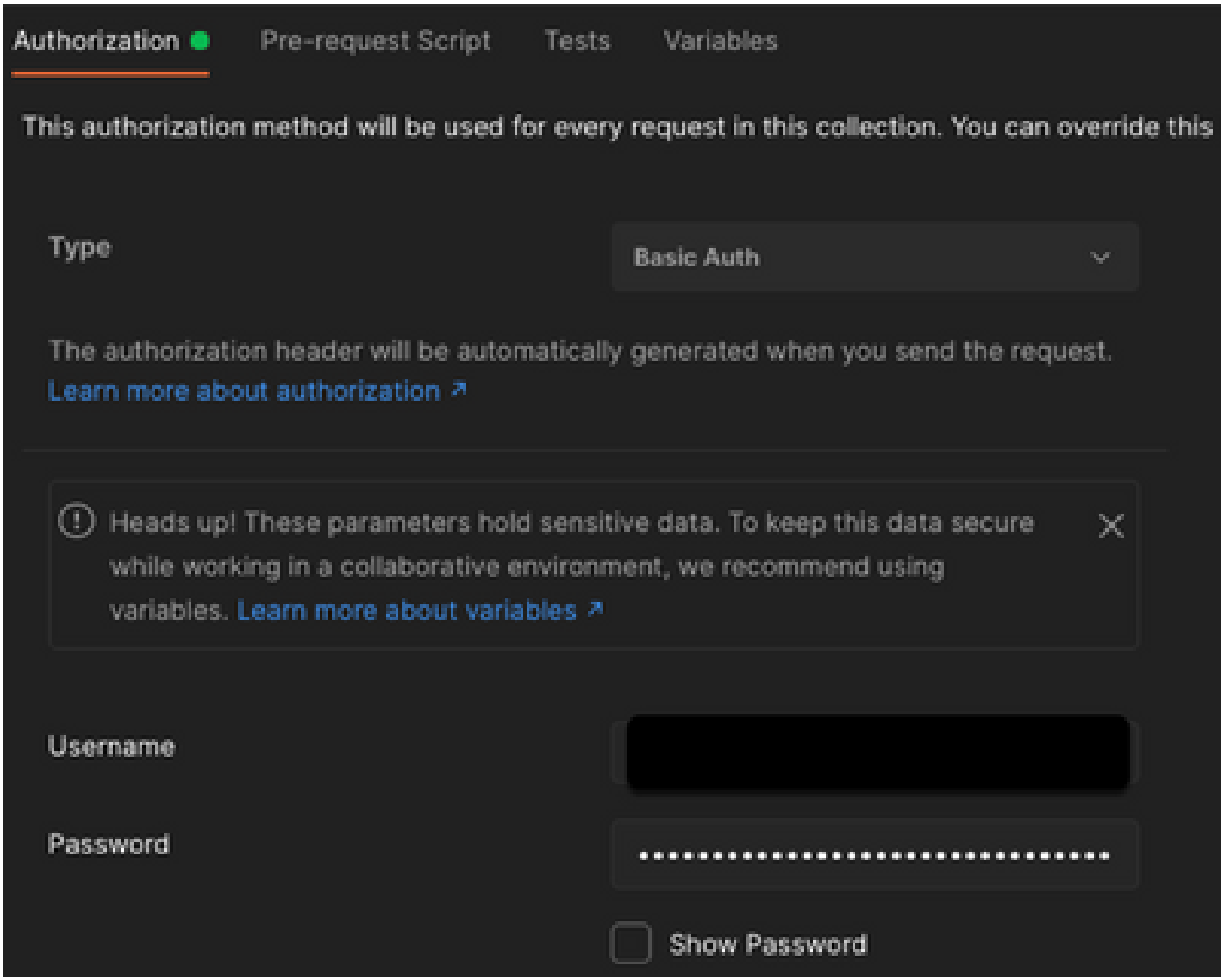
トラブルシュート

XDRとUmbrellaの統合に関する一般的な問題をトラブルシューティングするには、APIの接続とパフォーマンスを確認します。

XDR Device InsightsとUmbrellaによる接続テスト

ステップ 1：次の図に示すように、認可方式としてBasic認証を選択できます。

> 注:Postmanはシスコが開発したツールではありません。Postmanツールの機能について質問がある場合は、Postmanサポートにお問い合わせください。



ステップ 2：このAPI呼び出しを使用すると、theroaming computersを取得できます（デフォルトのページ制限は100エントリです）。

```
https://management.api.umbrella.com/v1/organizations/
```

```
    /roamingcomputers
```

ステップ 3：最初のコールに応答して、オブジェクトの総数が返されます。次のページを取得するには、limitパラメータとpageパラメータを使用できます。

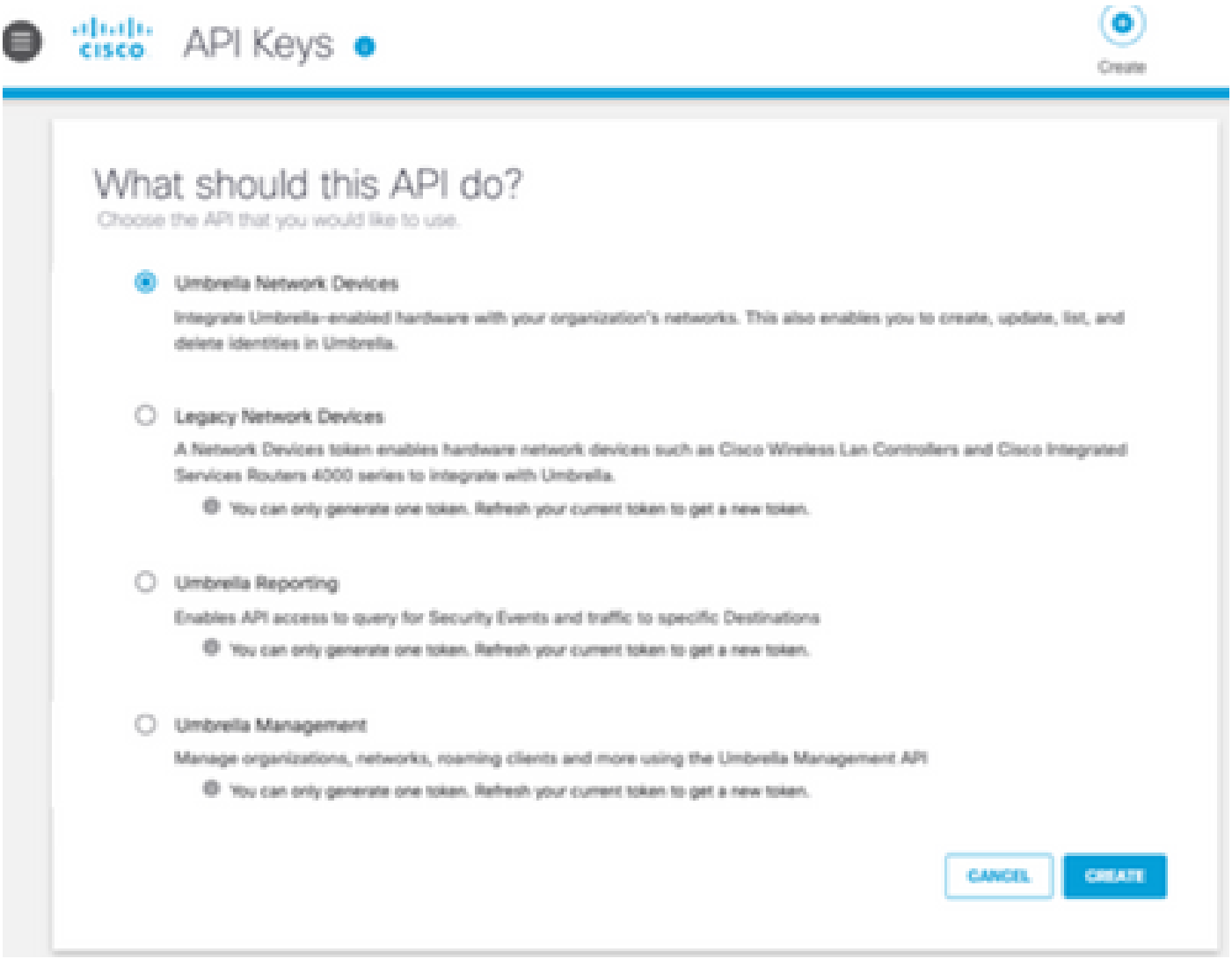
```
https://management.api.umbrella.com/v1/organizations/

        /roamingcomputers?limit=5&page=2
```

間違ったキー

XDR Device InsightsはXDRと同じキーを使用しないため、図に示すように、Umbrella APIキーとして設定されているキーが正しいことを確認する必要があります。

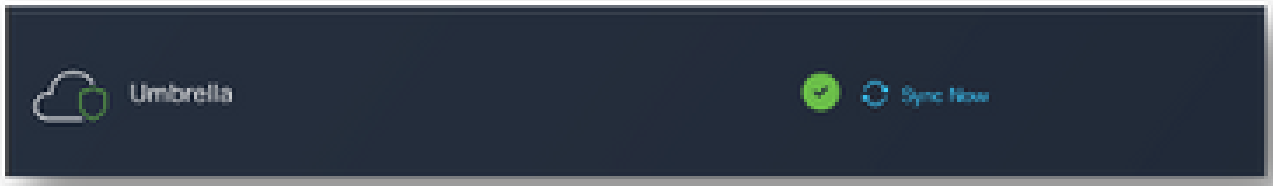
- 包括ネットワークデバイス：DNSポリシーを学習するために使用されるAPI
- Umbrella Management：エンドポイントの学習に使用されるAPI



確認

UmbrellaがXDR Device Insightsのソースとして追加されると、正常なREST API接続ステータスが表示されます。

- 緑色のステータスでREST API接続を確認できます
- 図に示すように、SYNC NOWをクリックして最初の完全同期をトリガーします



Device InsightsとUmbrellaの統合で問題が解決しない場合は、ブラウザからHARログを収集し、TACサポートに連絡して、詳細な分析を実行してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。