Device InsightsとSecure Endpoint Integration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、Device InsightsとSecure Endpoint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

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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、初期（デフォルト）設定の状態から起動しています。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

SecureX Device Insightsは、組織内のデバイスの統合ビューを提供し、Secure Endpointなどの統合データソースからのインベントリを統合します。

Device Insightsを使用すると、すべてのソースからの情報が統合され、SecureX内のDevice Insightsに表示されます。すべてのデバイス情報を包括的に表示し、データソースのポートフォリオ全体でデバイスをより効率的に調査する簡単な方法です。

有効化されると、Device Insightsは、SecureXと統合したモジュールからインベントリとデバイスデータを自動的に取得する準備が整います。そのため、SecureXと統合されたモジュールがすでに存在する場合は、この機能を使用するためにモジュールを削除したり再度追加したりする必要はありません。

設定の詳細については、『Cisco SecureXコンフィギュレーションモジュール』を参照してください。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

セキュアエンドポイントモジュールの追加

- モジュールを有効にするユーザには、製品を統合するための管理者権限が必要です。

  注：新しいソースを統合する場合は、手動で同期するか、自動同期が行われるのを待ってから、インベントリに報告するデバイスを確認する必要があります。

接続の確認

API接続を許可するには、使用している環境で次のFQDNが許可されていることを確認します。

- api.amp.cisco.com
- api.apjc.amp.cisco.com
- api.eu.am p.cisco.com

ユーザPostmanによる接続テスト

https://<AMP API地域FQDN>/v1/computers

https://< AMP API regional FQDN>/v1/computers/< connector GUID>

注：セキュアエンドポイントは、認可方式として基本認証を使用します。

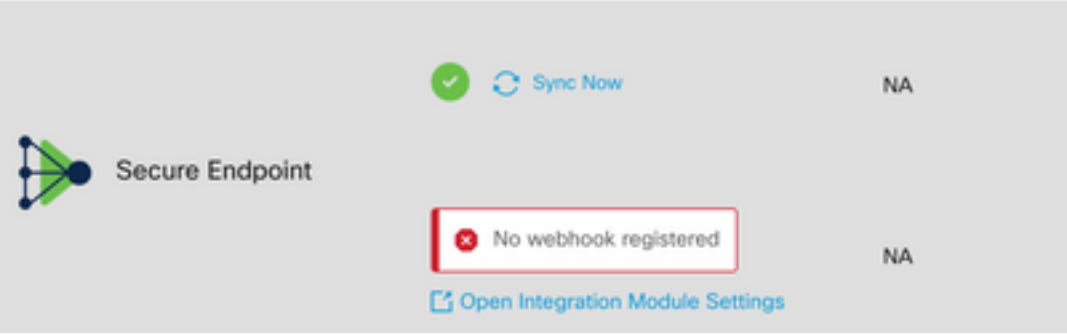
デバイス番号の不一致

- Device Insightsは過去90日間の情報を保存しますが、Secure Endpointは30日間の情報を保存します。デバイスの数に不一致が見つかった場合は、関連するコンピュータの最後に表示された日数が90日を超えていないことを確認します。

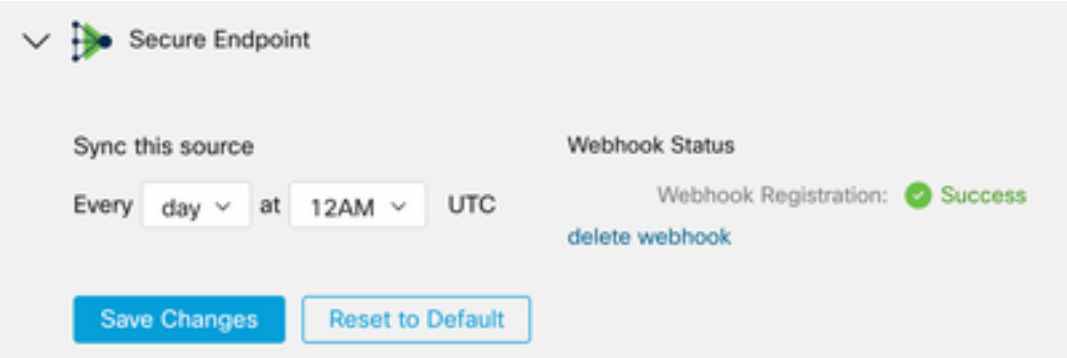
- セキュアエンドポイントコンソールに、両方のコンソールで不一致を引き起こす重複コネク

タがないことを確認します。

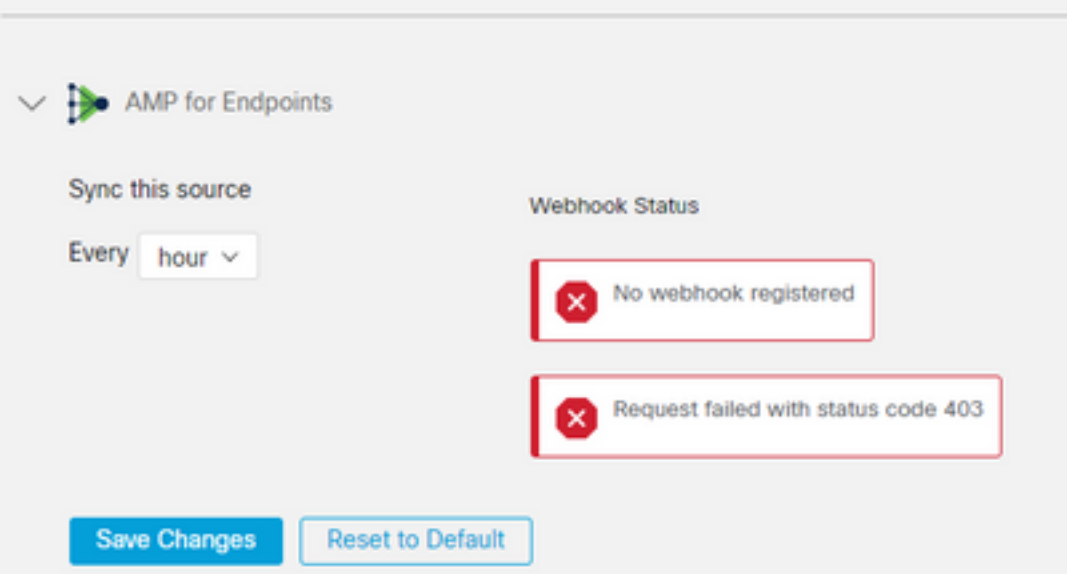
シナリオ1:Webhookが登録されていない



[Source Setting]に移動し、[Register Webhook]ボタンをクリックします。要求が実行されると、図に示すようにWebhookのステータスが表示されます。



シナリオ2:HTTPエラー



400 – 要求が正しくありません

401 – 不正

403 – フォービデン

404 – メソッドは許可されていません

HTTPエラーについては、設定されているAPIクレデンシャルを確認し、収集した情報が

SecureXのモジュール設定に貼り付けられた情報と一致することを確認します。

ブラウザの問題

Device Insightsに誤ったデータが表示された場合は、別のブラウザまたはプライベートウィンドウでテストして、誤ったブラウザキャッシュや古いブラウザキャッシュを破棄します。

複数組織の問題

Secure Endpoint統合モジュールでは、[Enable]ボタンを使用します。そのため、現在セキュアエンドポイントは1つのセキュアエンドポイントコンソールにのみリンクできますが、それらの組織の管理者であれば、1つのSecureXで複数のセキュアエンドポイントモジュールをリンクできます。つまり、複数のSecure Endpoint組織の管理者は、1つのSecureXダッシュボードのAPIモジュールを介してこれらすべてをリンクできます。セキュアエンドポイントコンソールが別のSecureX組織に統合されていないことを確認します。

SecureXポータルでは、複数のSecure Endpointインスタンスを統合できますが、Secure Endpointは1つのSecureXインスタンスにのみ統合できます。

HARログ

Device InsightsとSecure Endpointの統合で問題が解決しない場合は、「SecureXコンソールからHARログを収集する」でブラウザからHARログを収集する方法を確認し、TACサポートに連絡してさらに詳細な分析を行ってください。

関連情報

- SecureXログイン（ドキュメント）
- テクニカル サポートとドキュメント – Cisco Systems

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。