

XDR Device InsightsとMicrosoft Intuneの統合の トラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

概要

このドキュメントでは、統合を構成し、Device InsightsとIntuneの統合のトラブルシューティングを行う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
- Microsoft Intune
- 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。

Microsoft IntuneはEnterprise Mobility Manager (EMM)で、Mobile Device Manager (MDM)またはUnified Endpoint Manager (UEM)とも呼ばれます。Microsoft IntuneをXDRと統合すると、XDR Device Insightsで利用できるエンドポイントの詳細と、インシデントの調査時に利用できるエンドポイントデータが強化されます。Microsoft Intune統合を構成する場合は、Azureポータルから情報を収集し、XDRにMicrosoft Intune統合モジュールを追加する必要があります。

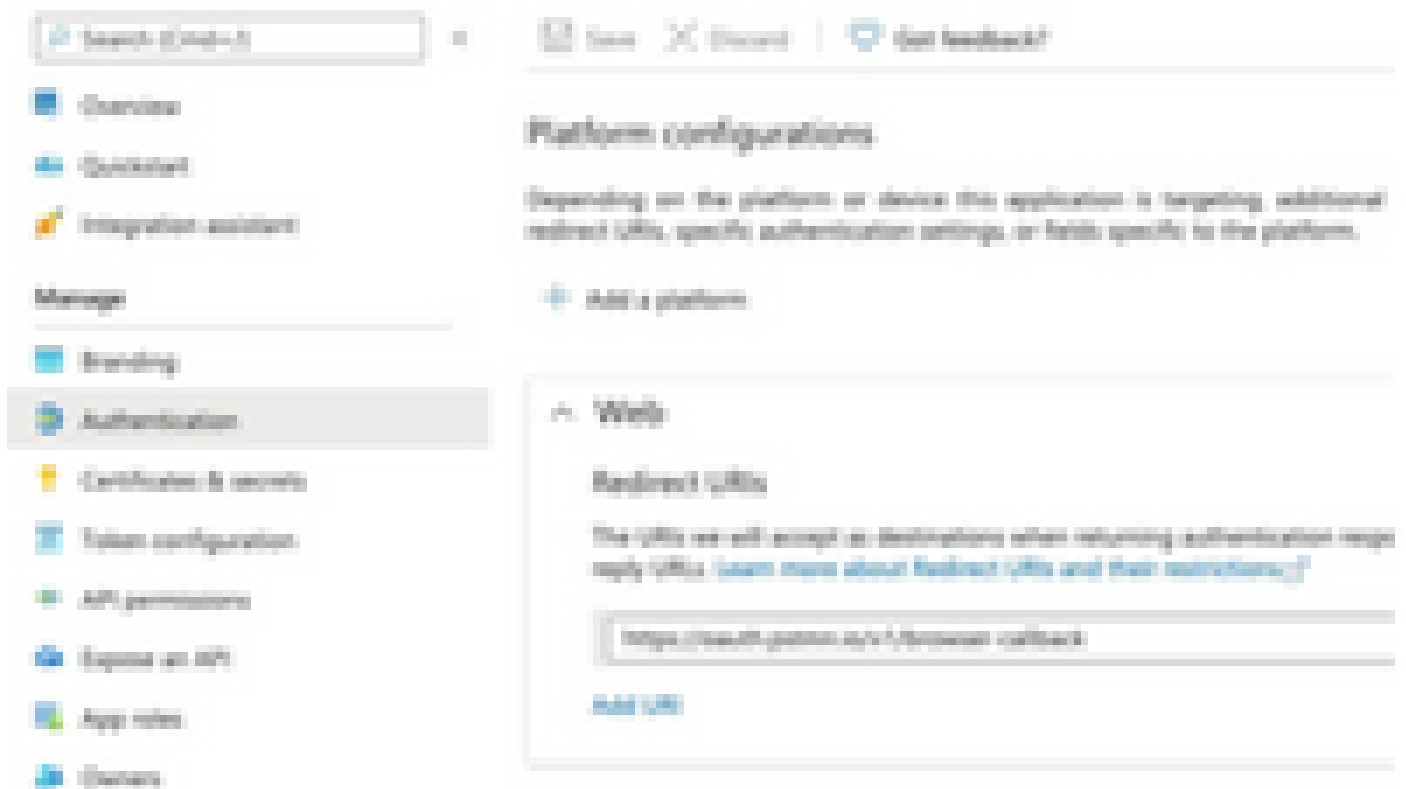
構成の詳細については、統合モジュールの詳細を参照してください。

トラブルシューティング

XDRとIntune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Intuneによる接続テスト

- Graph APIのPostman Azureアプリの構成については、[ここ](#)を参照してください
- ハイレベル管理者は、たとえばリダイレクトURIを定義する必要があります。



- APIアクセス許可は、Device Insightsアプリと同じままにすることができます
- グラフAPIコレクションのフォークは、[ここ](#)で作成できます

API / Permissions name	Type	Description
Microsoft Graph (2)		
DeviceManagementManaged	Application	Read Microsoft Intune devices
User.Read	Delegated	Sign in and read user profile

- フォークに付属する環境では、アプリケーション/テナントごとにこれらの値を調整する必要があります

Microsoft Graph environment

VARIABLE	INITIAL VALUE
----------	---------------

ClientID

ClientSecret

TenantID

- Postmanツールを使用すると、接続をテストしながら、より視覚的な出力を得ることができます。

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。

- 最初に実行されるコールはGet App-Only Access Tokenです。適切なAppクレデンシャルとテナントIDを使用した場合、このコールはアプリケーションアクセストークンで環境を作成します。完了すると、図に示すように実際のAPIコールを実行できます

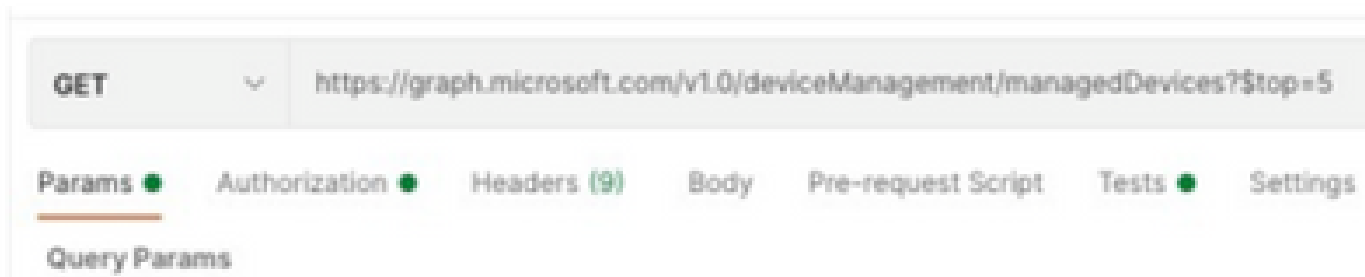
MS Graph PosaaS LAB / Intune / Get App-Only Access Token

POST	▼	https://login.microsoftonline.com/{{TenantID}}/oauth2/v2.0/token
------	---	--

- このAPI呼び出しを使用して、図に示すようにIntuneエンドポイントを取得できます(必要に

応じて、このグラフAPIのページネーションに関する [ドキュメント](#)を確認してください)

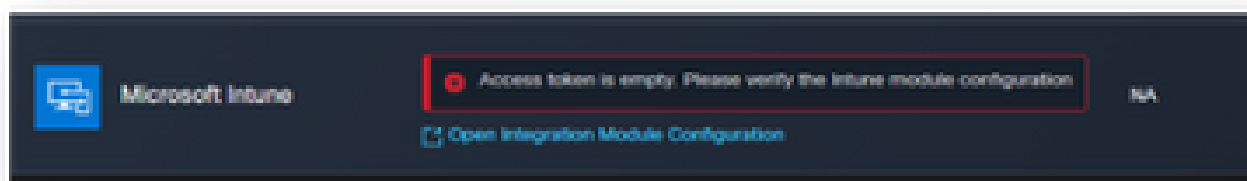
<https://graph.microsoft.com/v1.0/deviceManagement/managedDevices>



アクセストークンが空です。Intune構成モジュールを確認してください

Access Token is emptyは、次の図に示すようにOAuthエラーです。

- 通常はAzure UIのバグが原因
- 組織のトークンエンドポイントである必要があります



- 両方の場所で、エンドポイント、統合アプリ、およびApp Registrations > Endpointsのルートを確認できます。
- 図に示すように、Azure統合アプリからエンドポイントをOAuthエンドポイントの汎用の非固有URLとして表示できます



シークレットID値

Secret Valueではなく、Secret IDをコピーしたことを確認します（値はAPIキーで、Secret ID自体はAzure自体の内部インデックスであり、役に立ちません）。XDR Device Insightsの値を使用する必要があります。この値は一時的にのみ表示されます。

確認

Intune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を押して最初の完全同期をトリガーします。



XDR Device InsightsとIntune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、より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。