Troubleshoot XDR Device Insights and Microsoft Intune Integration

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Background Information](#)

Introduction

This document describes the steps to configure the integration and troubleshoot Device Insights and Intune integration.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics.

- XDR
- Microsoft Intune
- Basic knowledge of APIs
- Postman API tool

Components Used

The information in this document is based on these software and hardware versions.

- XDR

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

XDR Device Insights provides a unified view of the devices in your organization and consolidates inventories from integrated data sources.

Microsoft Intune is an Enterprise Mobility Manager (EMM), also known as a Mobile Device Manager (MDM) or a Unified Endpoint Manager (UEM). When you integrate Microsoft Intune with XDR, it enriches the endpoint details available in XDR Device Insights and the endpoint data available when you investigate incidents. When you configure Microsoft Intune integration, you need to gather some information from your Azure portal and then add the Microsoft Intune integration module in XDR.

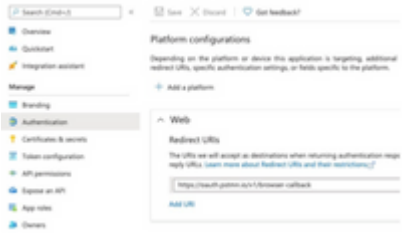
If you want to know more about the configuration, please review the integration module details.

Troubleshoot

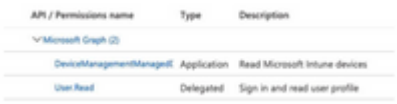
In order to troubleshoot common issues with the XDR and Intune integration, you can verify the connectivity and performance of the API.

Connectivity test with XDR Device Insights and Intune

- Postman Azure App configuration for Graph API is documented here
- At the high-level administrator needs to define Redirect URIs, for example



- API permissions can stay the same as in Device Insights App
- Fork for Graph API collection can be created here

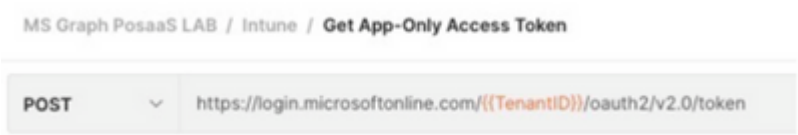


- The Environment that comes with the fork needs to have those values adjusted per App/Tenant

- You can use Postman Tool to have a more visual output while you test the connectivity.

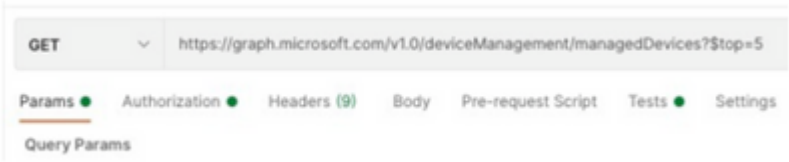
> **Note**: Postman is not a Cisco-developed tool. If you have a question about Postman tool functionality, please contact Postman support.

- The first call to be executed is **Get App-Only Access Token**. If the right **App credentials** and **tenant ID** were used, this call populates the environment with the app access token. Once it is done, actual API calls can be executed as shown in the image



- You can use this API call to get Intune endpoints, as shown in the image (if needed, review this Graph API pagination document)

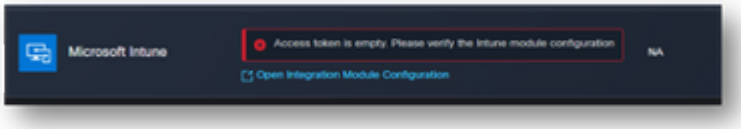
```
https://graph.microsoft.com/v1.0/deviceManagement/managedDevices
```



Access Token is empty, please verify the Intune configuration module

Access Token is empty is an OAuth error, as shown in the image.

- Usually caused by an Azure UI bug
- It must be the token endpoint for the Org



- You can try both locations to see the Endpoints, **Integrated App,** and the root of **App Registrations > Endpoints**
- You can view Endpoints from your Azure integrated App shown as generic, non-specific URLs for the OAuth Endpoints, as shown in the image

Secret ID value

Verify you copied the **Secret ID**, not the **Secret Value** (the Value is the API Key and the Secret ID itself is an internal index for Azure itself and it does not help). You need to use the Value in XDR Device Insights, and this value is only displayed temporarily.

Verify

Once Intune is added as a source to XDR Device Insights, you can see a successful **REST API** connection status.

- You can see the **REST API** connection with a green status.

- Press on **SYNC NOW** to trigger the initial full sync, as shown in the image.

In case the issue persists with the XDR Device Insights and Intune integration,please collect HAR logs from the browser and contact TAC support in order to perform a deeper analysis.