Troubleshoot XDR Device Insights and Umbrella Integration

Contents

Introduction

This document describes the steps to configure the integration and troubleshoot XDR Device Insights and Cisco Umbrella integration.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics.

- XDR
- Umbrella
- 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.

Umbrella automatically uncovers attacker infrastructure staged for current threats and proactively blocks malicious requests before they reach an organizationâ€™s network or endpoints. With integration, you can stop malware infections earlier, identify already-infected devices faster, and prevent data exfiltration. The integration provides complete visibility into Internet activity across all locations and users and allows you to take action with a two-click response to quickly block domains. Multiple Umbrella functions are supported and linked via API keys that have been generated in the Umbrella Platform.

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

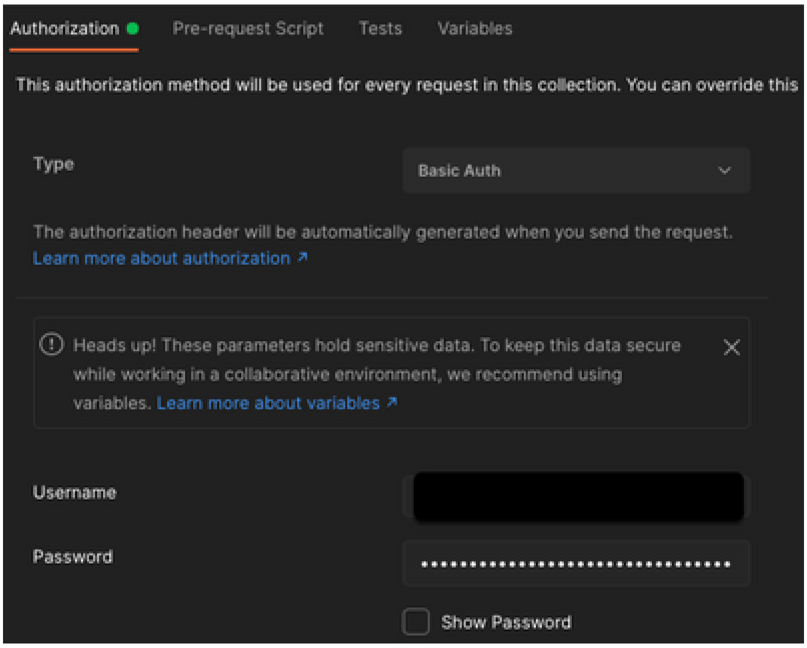
Troubleshoot

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

Connectivity test with XDR Device Insights and Umbrella

Step 1. You can select **Basic Auth**as an authorization method, as shown in the image.

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



This authorization method will be used for every request in this collection. You can override this

Type: Basic Auth

The authorization header will be automatically generated when you send the request.
Learn more about authorization ↗

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. Learn more about variables ↗

Username: [redacted]

Password: ••••••••••••••••••••••••••••••••

□ Show Password

Step 2. You can get the**roaming computers**, with this API call (the default page limit is 100 entries).

```
https://management.api.umbrella.com/v1/organizations/<OrgID>/roamingcomputers
```

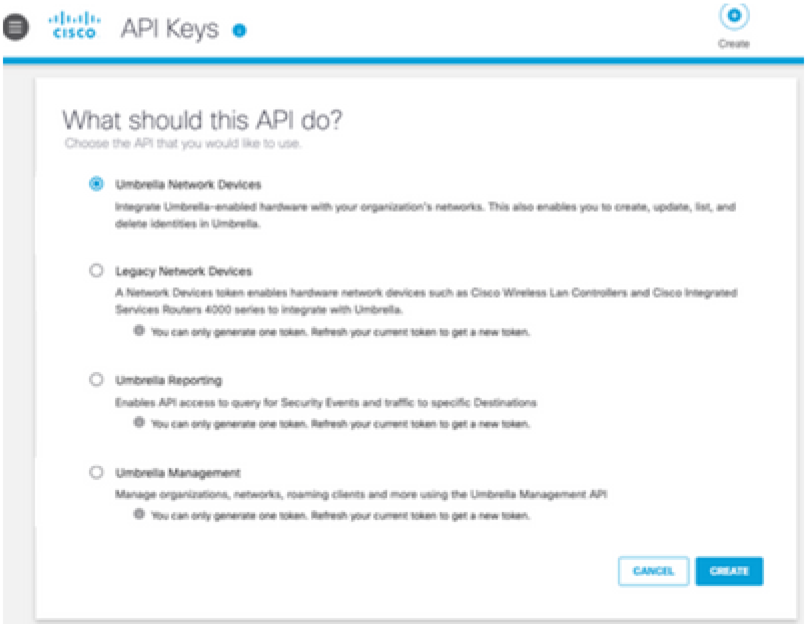
Step 3. In response to the first call, the total number of objects is returned. You can use limit and page parameters to get the next pages.

```
https://management.api.umbrella.com/v1/organizations/<OrgID>/roamingcomputers?limit=5&page=2
```

Wrong Key

XDR Device Insights does not use the same keys that XDR, then you need to verify and confirm the Keys configured as Umbrella API keys are correct, as shown in the image.

- Umbrella Network Devices: API used to learn what DNS policies
- Umbrella Management: API used to learn endpoints



What should this API do?

Choose the API that you would like to use.

● Umbrella Network Devices
Integrate Umbrella-enabled hardware with your organization's networks. This also enables you to create, update, list, and delete identities in Umbrella.

○ Legacy Network Devices
A Network Devices token enables hardware network devices such as Cisco Wireless Lan Controllers and Cisco Integrated Services Routers 4000 series to integrate with Umbrella.
You can only generate one token. Refresh your current token to get a new token.

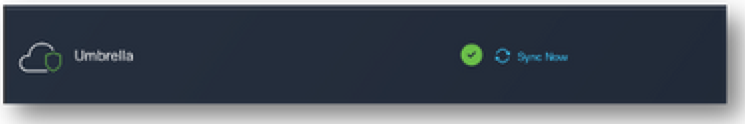
○ Umbrella Reporting
Enables API access to query for Security Events and traffic to specific Destinations
You can only generate one token. Refresh your current token to get a new token.

○ Umbrella Management
Manage organizations, networks, roaming clients and more using the Umbrella Management API
You can only generate one token. Refresh your current token to get a new token.

Verify

Once Umbrella 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
- Click on **SYNC NOW** to trigger the initial full sync, as shown in the image



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