Troubleshoot XDR Device Insights and DUO Integration

Contents

Introduction

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

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics.

- XDR
- DUO
- 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.

Duo secures your workforce and takes access security beyond the corporate network perimeter to protect your data at every authentication attempt, from any device, anywhere. With Duo, you can confirm your identities in a snap, monitor the health of managed and unmanaged devices, set adaptive security policies tailored for your business, secure remote access without a device agent, and provide secure, user-friendly Single Sign-On quickly and easily.

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

Troubleshoot

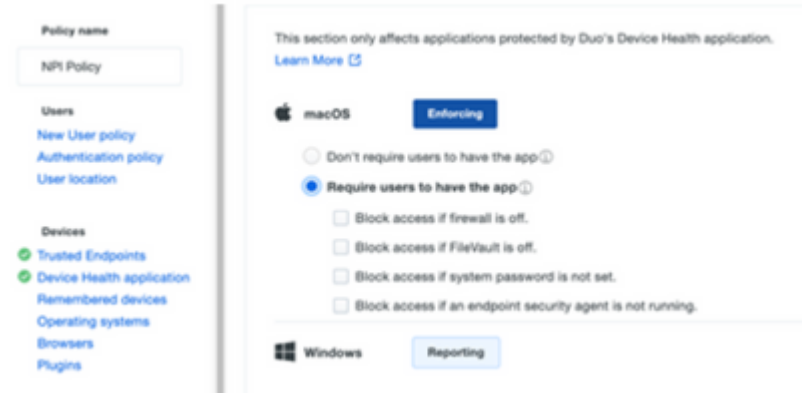
In order to troubleshoot common issues with the XDR and DUO integration, you can verify the connectivity and performance of the API.

Review the License Level

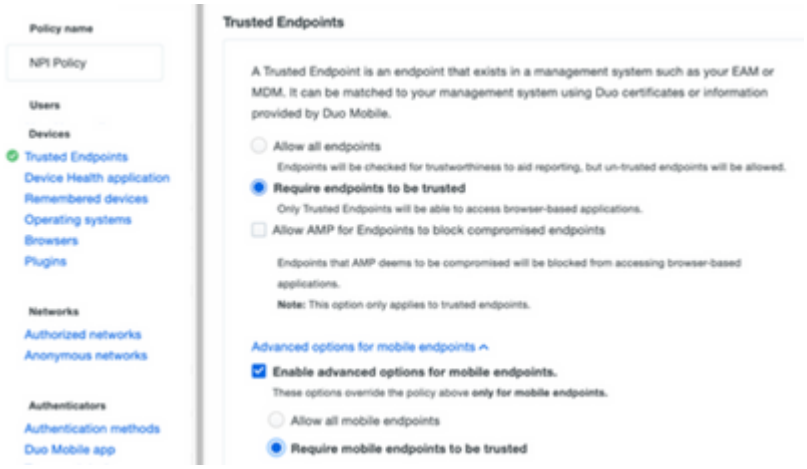
- Check license in **Duo Admin Panel**
- Duo Licensed for Duo Access, Duo Beyond (or any newer high-end license, MFA only or Free does not apply), as shown in the image

No data from Duo

- Verify you use **Duo Health Agent** data in **Auth Policy**, as shown in the image



- Verify you use **Trusted Endpoint** in **Auth Policy**, as shown in the image



Connectivity test with XDR Device Insights and DUO

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.

- Error code 40301 â€œ**Access Forbidden**â€ means you do not have the right level of license, as shown in the image

- You can select **No Auth** as an authorization method
- You can use this API call in order to get a list of the devices (API returns the maximum supported number of entries per page), and you can find documentation about DUO API pagination

```
https://<DUO admin API FQDN>/admin/v1/endpoints
```

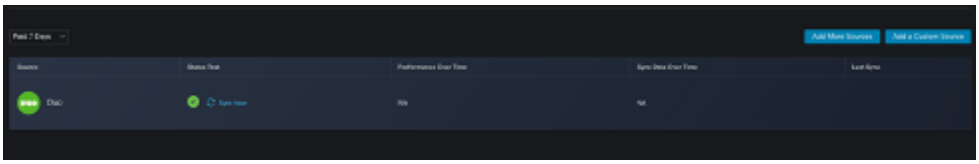
- In response to the first call, the total number of objects is returned (offset and limit parameters can be used to get the next pages), as shown in the image

```
https://<DUO admin API FQDN>/admin/v1/endpoints?limit=5&offset=5
```

Verify

Once DUO 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 DUO integration,please collect HAR logs from the browser and contact TAC support in order to perform a deeper analysis.