Troubleshoot XDR Device Insights and Orbital Integration

Contents

Introduction

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

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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.

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

Background Information

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

Troubleshoot

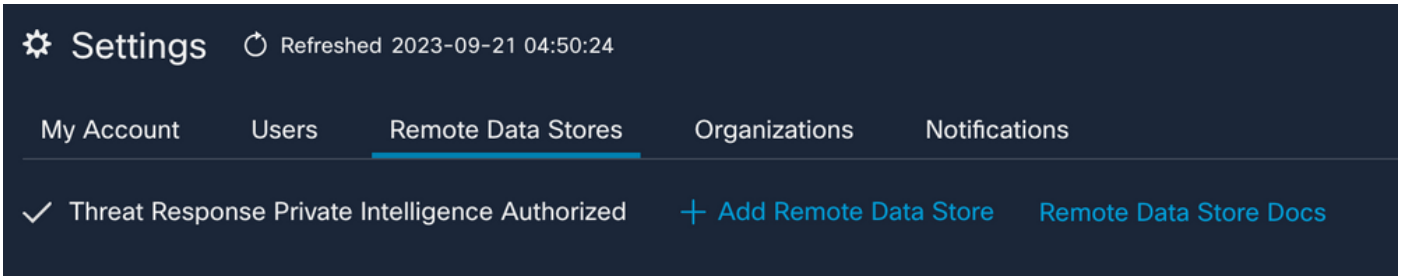
This section provides the information you can use to troubleshoot your configuration.

Connectivity

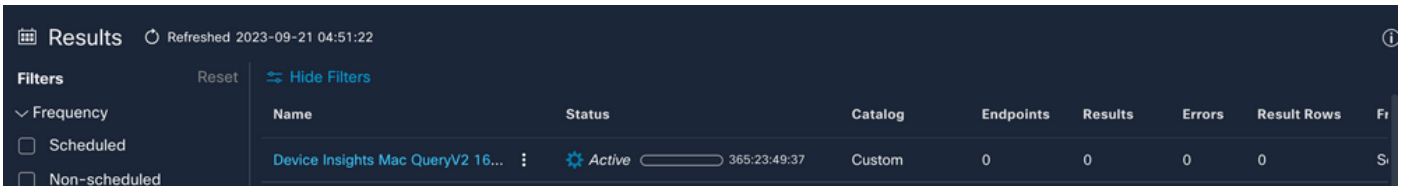
- REST API credentials of sources can be used to test basic connectivity using tools like Postman.
- Once results of queries start to come from Orbital agents data is published to Remote Datastore.
- Validate if a Remote Datastore has been created for Device Insights, this can be verified from account

settings.

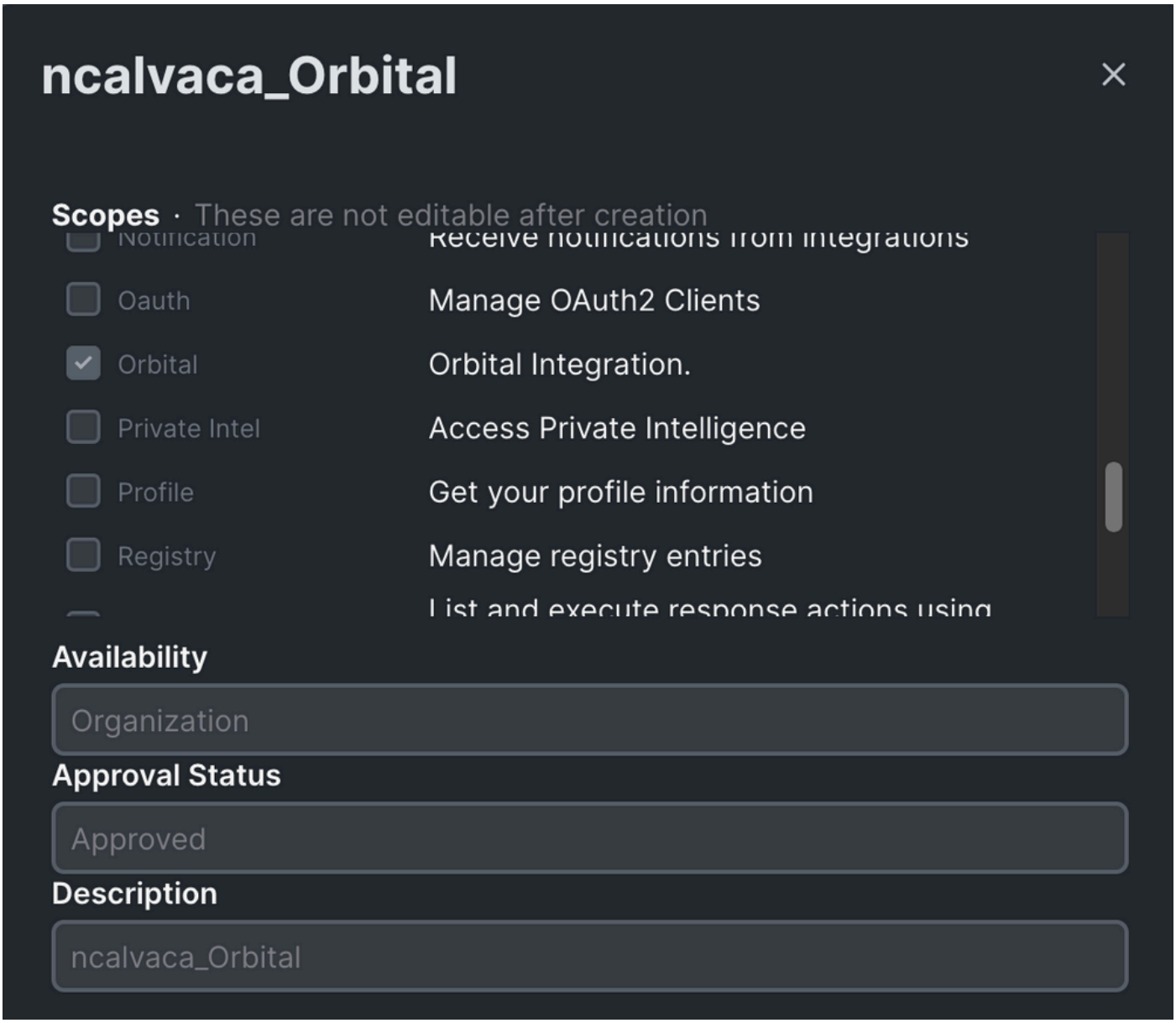
- From the Remote Data Store details administrator, verify that Device Insights tenant ID, and URL of Device Insights is displayed, Status must be Authenticated.



- Navigate to the Results tab in order to see in a Job list the Job created by Device Insights



- From the XDR portal, navigate to Administration, select the API Clients and make sure Orbital is selected:



- Error "No response from endpoint, it may be offline" - This error means that the endpoint is turned off or does not have connectivity with Orbital cloud, please refer to the Required Server Addresses for Proper Cisco Secure Endpoint & Malware Analytics Operations document to make sure the IPs, ports and URLs are allowed.

Mismatch count

- If the device count does not match, this is expected as Orbital does not maintain its inventory of endpoints that are > 90 days since version 1.14, it includes all endpoints that have had an Orbital connector installed at any time and not just the active ones in its inventory. When the device insights feature is active, it creates a recurring daily job for all endpoints to perform. After the job is run on the endpoint and the resulting device information is sent back to Orbital, XDR is notified about the existence of that device from Orbital. If no job result for that device is received within 90 days, the Orbital endpoint is purged from the inventory in device insights.
- Orbital reinstallation results in a new GUID which can cause a duplicate in the console.

License

- Verify that the Secure Endpoint Console has the proper license to access Orbital.

Mac and Linux devices not displayed

- MacOS & Linux devices from Orbital source are not supported in XDR Device Insights yet.

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

Related Information

- **XDR Reference Guide**
- **Orbital Troubleshooting**
- **Technical Support & Documentation - Cisco Systems**