Troubleshoot XDR Device Insights and Secure Endpoint Integration

Contents

Introduction

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

Background Information

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

With XDR Device Insights, the information from all the sources is consolidated, and displayed in device insights within XDR, in a simpler way to view all your device information holistically and investigate devices across your portfolio of data sources more efficiently.

Once activated, device insights are ready to automatically pull inventory and device data from the modules you have integrated with XDR. So if you already have modules integrated with XDR, there is no need to delete or re-add them to have this functionality.

If you want to know more about the configuration, please review the Cisco XDR Configuration Modules for details.

Troubleshoot

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

Add the Secure Endpoint Module

- The user that enables the Module needs to have Admin rights to integrate the products.

Note: If you integrate a new source you need to either manually sync up or wait for auto-sync to happen before you see any devices that report into inventory.

Verify Connectivity

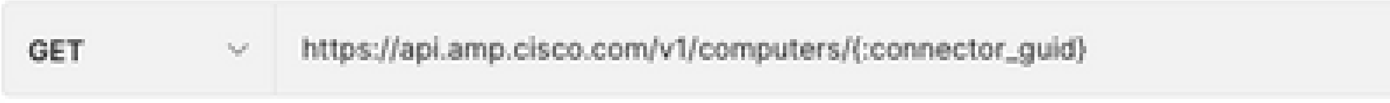
In order to allow API connections, make sure the next FQDN are allowed on your environment.

- api.amp.cisco.com
- api.apjc.amp.cisco.com
- api.eu.amp.cisco.com

User Postman to test connectivity

https://<AMP API regional FQDN>/v1/computers

https://< AMP API regional FQDN>/v1/computers/< connector GUID>



GET

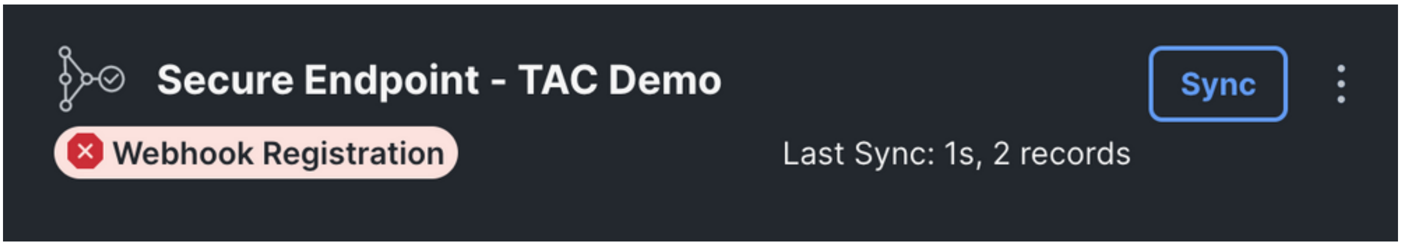
https://api.amp.cisco.com/v1/computers/{:connector_guid}

Note: Secure Endpoint uses Basic Auth as an authorization method.

Devices Number Mismatch

- Device Insights stores the information from the last 90 days, however, Secure Endpoint stores the information from 30 days. If a mismatch is found on the number of devices, verify the last seen of the involved computers does not have more than 90 days.
- Verify the Secure Endpoint console does not have duplicate connectors that cause the mismatch on both consoles.

Scenario 1. No Webhook registration

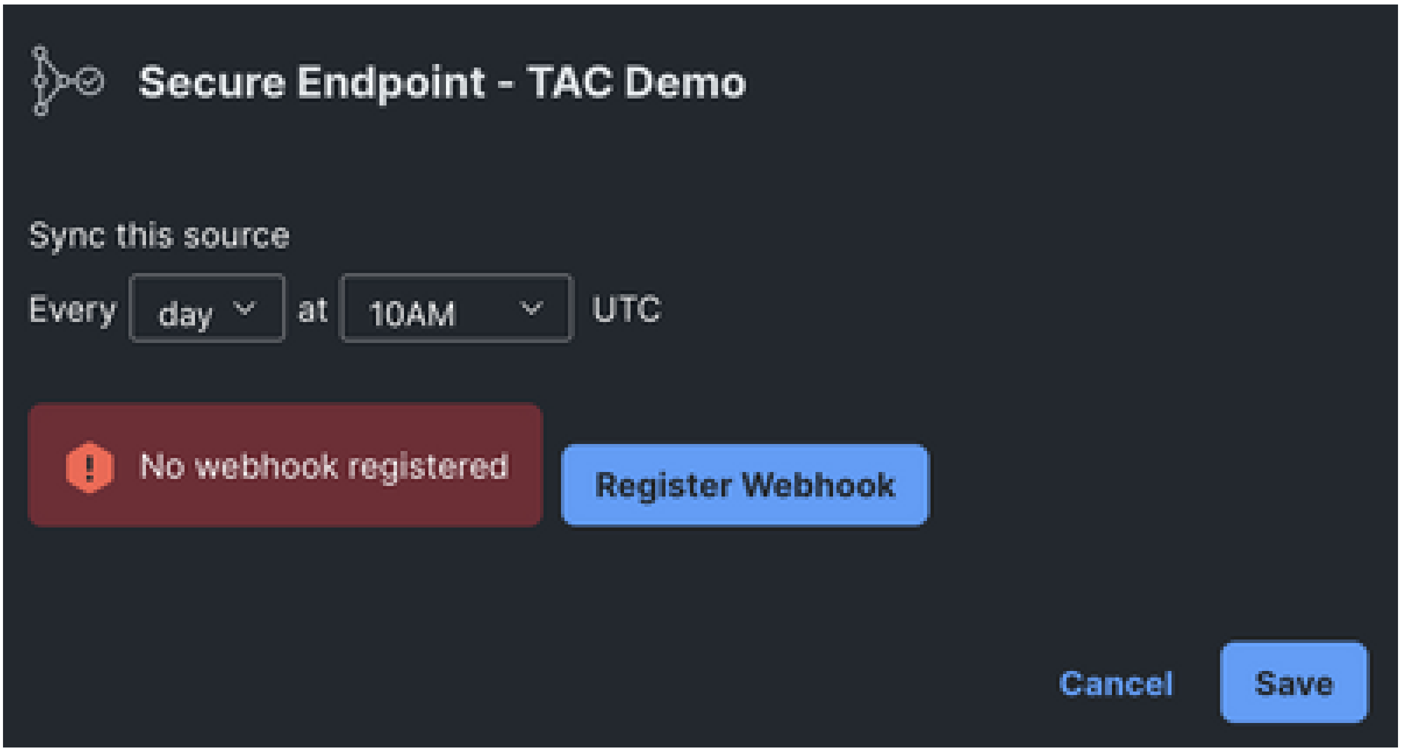


Secure Endpoint - TAC Demo

✕ Webhook Registration

Last Sync: 1s, 2 records

Navigate to Source Setting, then click on Register Webhook button, once the request is performed, the Webhook status displayed as shown in the image.



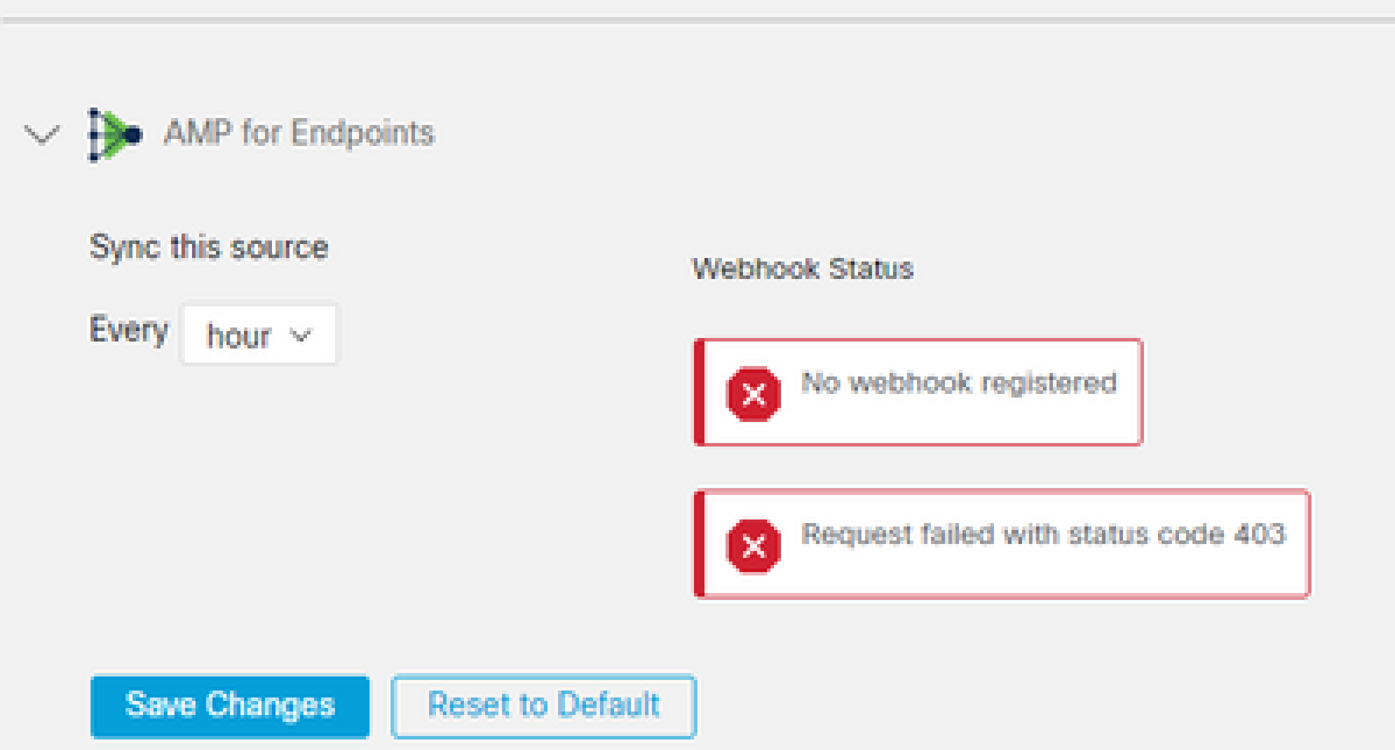
Secure Endpoint - TAC Demo

Sync this source

Every day at 10AM UTC

No webhook registered

Scenario 2. HTTP errors.



AMP for Endpoints

Sync this source

Every hour

Webhook Status

No webhook registered

Request failed with status code 403

400 - Bad request

401 - Unauthorized

403 - Forbidden

404 - Method not allowed

For HTTP errors, review the API credentials configured, and make sure that the information gathered matches the information pasted on the module configuration on XDR.

Browser Issues

When wrong data is displayed in Device Insights, test in a different browser or a private window to discard the wrong or outdated browser cache.

Multi-org Issues

Secure Endpoint integration module uses the Enable button. Due to that, Secure Endpoint can only be linked to one Secure Endpoint console now, but you can still have multiple Secure Endpoint modules linked under one XDR if you are the Admin for those organizations. In other words, if you are an Admin in multiple Secure Endpoint organizations you can have all of those linked via the API module under one XDR dashboard. Verify that the Secure Endpoint console is not already integrated into another XDR organization,

XDR portal can have integrated multiple Secure Endpoint instances, but Secure Endpoint can only be integrated into one XDR instance.

HAR logs

In case the issue persists with the Device Insights and Secure Endpoint integration,please see Collect HAR Logs from XDR Console for how to collect HAR logs from the browser and contact TAC support in order to perform a deeper analysis.

Related Information

- XDR Login (Documentation)
- Technical Support & Documentation - Cisco Systems