

Solución de problemas de XDR Device Insights y Secure Endpoint Integration

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

Introducción

Este documento describe los pasos para configurar la integración y resolver problemas de Device Insights y la integración de Secure Endpoint.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

XDR Device Insights proporciona una vista unificada de los dispositivos de su organización y consolida inventarios a partir de fuentes de datos integradas, como los terminales seguros.

Con XDR Device Insights, la información de todas las fuentes se consolida y se muestra en la información de dispositivos dentro de XDR, de una manera más sencilla para ver toda la información de su dispositivo de manera holística e investigar los dispositivos en su cartera de fuentes de datos de manera más eficiente.

Una vez activada, la información de dispositivos está lista para extraer automáticamente datos de inventario y de dispositivos de los módulos que ha integrado con XDR. Por lo tanto, si ya dispone de módulos integrados con XDR, no es necesario eliminarlos ni volver a agregarlos para disponer de esta funcionalidad.

Si desea obtener más información sobre la configuración, consulte los [módulos de configuración XDR de Cisco](#) para obtener más información.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Agregar el módulo de terminales seguros

- El usuario que habilita el módulo necesita tener derechos de administrador para integrar los productos.

Nota: Si integra un nuevo origen, debe sincronizar manualmente o esperar a que se realice la sincronización automática antes de ver los dispositivos que se registran en el inventario.

Verificar la conectividad

Para permitir conexiones API, asegúrese de que el siguiente FQDN esté permitido en su entorno.

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

El usuario Postman probará la conectividad

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

https://< FQDN regional de la API AMP>/v1/computers/< GUID del conector>

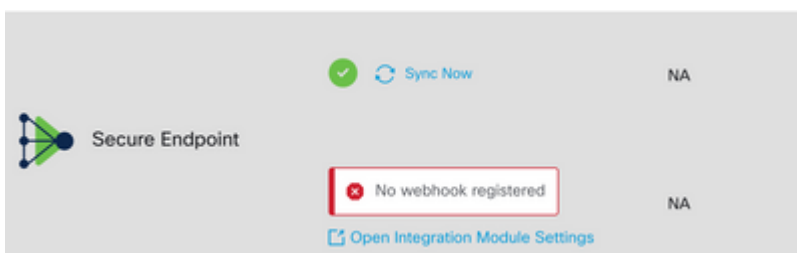


Nota: Secure Endpoint utiliza Basic Auth como método de autorización.

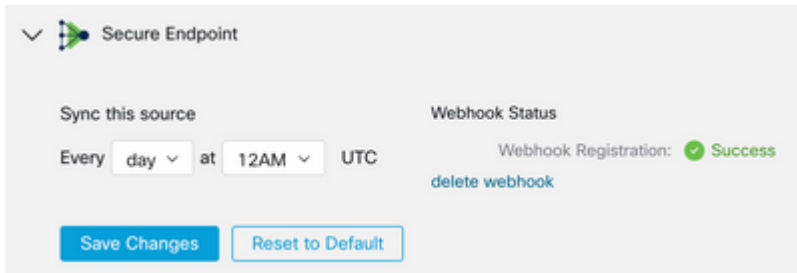
Discordancia de número de dispositivos

- Device Insights almacena la información de los últimos 90 días; sin embargo, Secure Endpoint almacena la información de los últimos 30 días. Si se encuentra una discordancia en el número de dispositivos, verifique que la última vista de los equipos involucrados no tenga más de 90 días.
- Verifique que la consola de Secure Endpoint no tenga conectores duplicados que provoquen la discordancia en ambas consolas.

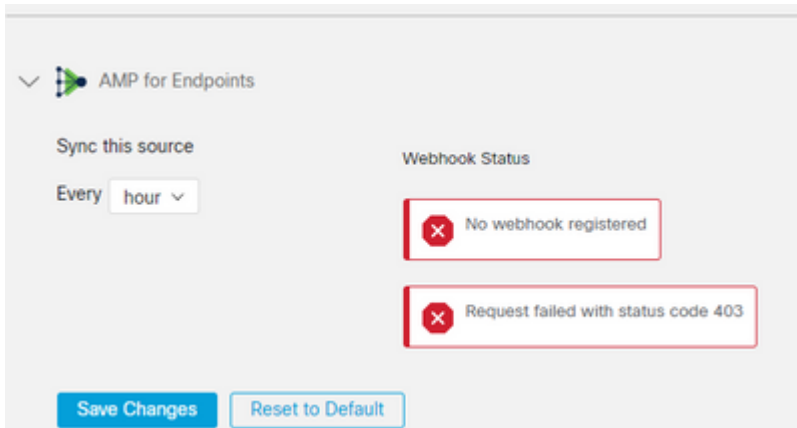
Escenario 1. Ningún webhook registrado



Vaya a Source Setting (Parámetro de origen) y haga clic en el botón Register Webhook (Registrar Webhook). Una vez realizada la solicitud, el estado de Webhook se muestra como se muestra en la imagen.



Situación hipotética 2. Errores HTTP.



400 - Solicitud incorrecta

401 - No autorizado

403 - Prohibido

404 - Método no permitido

Para los errores HTTP, revise las credenciales de API configuradas y asegúrese de que la información recopilada coincida con la información pegada en la configuración del módulo en XDR.

Problemas relacionados con el navegador

Cuando se muestran datos incorrectos en Device Insights, realice una prueba en un navegador diferente o en una ventana privada para descartar la caché del navegador incorrecta u obsoleta.

Problemas de multiorganización

El módulo de integración de terminales seguros utiliza el botón Activar. Debido a esto, Secure Endpoint solo se puede vincular a una consola de Secure Endpoint ahora, pero puede tener varios módulos de Secure Endpoint vinculados bajo un XDR si es el administrador de esas organizaciones. En otras palabras, si es administrador en varias organizaciones de terminales seguros, puede tener todos los enlaces a través del módulo API en un panel XDR. Compruebe que la consola de Secure Endpoint no esté integrada en otra organización XDR.

El portal XDR puede tener integradas varias instancias de terminales seguros, pero los terminales seguros solo se pueden integrar en una instancia XDR.

Registros HAR

En caso de que el problema persista con Device Insights y la integración de terminales seguros, consulte

[Recopilar registros HAR de la consola XDR](#) para obtener información sobre cómo recopilar registros HAR del navegador y ponerse en contacto con el soporte del TAC para realizar un análisis más profundo.

Información Relacionada

- [Inicio de sesión XDR \(documentación\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).