

Dépannage de XDR Device Insights et de l'intégration sécurisée des terminaux

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

Introduction

Ce document décrit les étapes à suivre pour configurer l'intégration et dépanner l'intégration de Device Insights et Secure Endpoint.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

XDR Device Insights fournit une vue unifiée des périphériques de votre entreprise et consolide les inventaires à partir de sources de données intégrées, telles que Secure Endpoint.

Grâce à XDR Device Insights, les informations provenant de toutes les sources sont consolidées et affichées dans les aperçus des périphériques au sein de XDR, d'une manière plus simple pour afficher toutes les informations de vos périphériques de manière holistique et examiner les périphériques à travers votre portefeuille de sources de données plus efficacement.

Une fois activés, les aperçus des périphériques sont prêts à extraire automatiquement l'inventaire et les données des périphériques des modules que vous avez intégrés à XDR. Ainsi, si vous avez déjà des modules intégrés avec XDR, il n'est pas nécessaire de les supprimer ou de les rajouter pour avoir cette fonctionnalité.

Si vous voulez en savoir plus sur la configuration, veuillez consulter les [modules de configuration Cisco XDR](#) pour plus de détails.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Ajout du module Secure Endpoint

- L'utilisateur qui active le module doit disposer de droits d'administrateur pour intégrer les produits.

Remarque : si vous intégrez une nouvelle source, vous devez soit synchroniser manuellement, soit attendre que la synchronisation automatique se produise avant de voir les périphériques qui se rapportent à l'inventaire.

Vérifier la connectivité

Afin d'autoriser les connexions d'API, assurez-vous que les noms de domaine complets suivants sont autorisés dans votre environnement.

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

User Postman pour tester la connectivité

`https://<FQDN régional de l'API AMP>/v1/computers`

`https://< FQDN régional de l'API AMP>/v1/computers/< GUID du connecteur>`

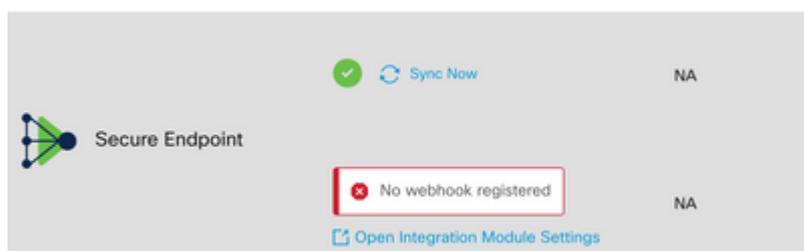


Remarque : Secure Endpoint utilise l'authentification de base comme méthode d'autorisation.

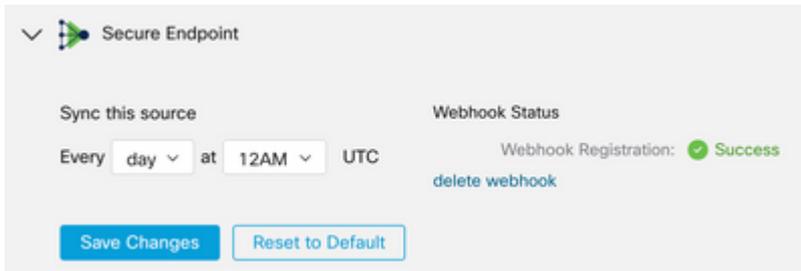
Non-concordance des numéros de périphériques

- Device Insights stocke les informations des 90 derniers jours, mais Secure Endpoint les stocke à partir de 30 jours. Si le nombre de périphériques ne correspond pas, vérifiez que le dernier ordinateur détecté ne dispose pas de plus de 90 jours.
- Vérifiez que la console Secure Endpoint ne comporte pas de connecteurs dupliqués à l'origine de la non-concordance sur les deux consoles.

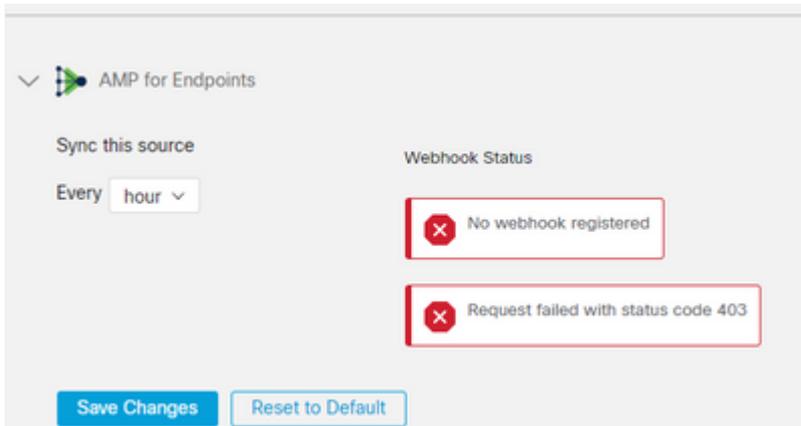
Scénario 1. Aucun Webhook enregistré



Accédez à Source Setting, puis cliquez sur le bouton Register Webhook. Une fois la demande effectuée, l'état Webhook s'affiche comme indiqué dans l'image.



Scénario 2. Erreurs HTTP.



400 - Demande incorrecte

401 - Non autorisé

403 - Interdit

404 - Méthode non autorisée

Pour les erreurs HTTP, vérifiez les informations d'identification de l'API configurées et assurez-vous que les informations collectées correspondent aux informations collées dans la configuration du module sur XDR.

Problèmes de navigateur

Lorsque des données incorrectes sont affichées dans Device Insights, effectuez un test dans un autre navigateur ou dans une fenêtre privée pour supprimer le cache du navigateur erroné ou obsolète.

Problèmes concernant plusieurs organisations

Le module d'intégration Secure Endpoint utilise le bouton Enable. Pour cette raison, Secure Endpoint ne peut désormais être lié qu'à une seule console Secure Endpoint, mais vous pouvez toujours avoir plusieurs modules Secure Endpoint liés sous un seul XDR si vous êtes l'administrateur de ces organisations. En d'autres termes, si vous êtes administrateur dans plusieurs organisations Secure Endpoint, vous pouvez lier toutes ces organisations via le module API sous un tableau de bord XDR. Vérifiez que la console Secure Endpoint n'est pas déjà intégrée à une autre organisation XDR,

Le portail XDR peut intégrer plusieurs instances Secure Endpoint, mais Secure Endpoint ne peut être intégré qu'à une seule instance XDR.

Journaux HAR

Si le problème persiste avec l'intégration de Device Insights et Secure Endpoint, consultez [Collecter les](#)

[journaux HAR à partir de la console XDR](#) pour savoir comment collecter les journaux HAR à partir du navigateur et contactez le support TAC afin d'effectuer une analyse plus approfondie.

Informations connexes

- [Connexion XDR \(documentation\)](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.