

Dépannage de XDR Device Insights et de l'intégration Umbrella

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

Introduction

Ce document décrit les étapes pour configurer l'intégration et dépanner l'intégration XDR Device Insights et Cisco Umbrella.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes .

- XDR
- Umbrella
- Connaissances de base des API
- Outil API Postman

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et matériel suivantes :

- 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. 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.

Umbrella détecte automatiquement l'infrastructure de l'attaquant préparée pour les menaces actuelles et bloque de manière proactive les requêtes malveillantes avant qu'elles n'atteignent le réseau ou les terminaux d'une entreprise. Grâce à l'intégration, vous pouvez arrêter plus tôt les infections par des programmes malveillants, identifier plus rapidement les périphériques déjà infectés et empêcher l'exfiltration des données. L'intégration offre une visibilité complète de l'activité Internet sur tous les sites et utilisateurs et vous permet d'agir en deux clics pour bloquer rapidement les domaines. Plusieurs fonctions Umbrella sont

prises en charge et liées via des clés API générées dans la plate-forme Umbrella.

Si vous souhaitez en savoir plus sur la configuration, consultez les détails du module d'intégration.

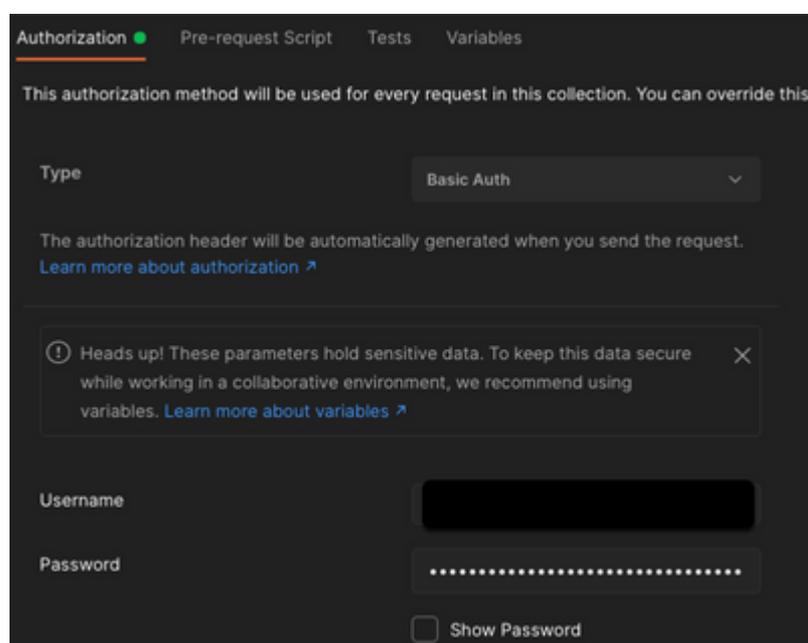
Dépannage

Afin de dépanner les problèmes courants avec l'intégration XDR et Umbrella, vous pouvez vérifier la connectivité et les performances de l'API.

Test de connectivité avec XDR Device Insights et Umbrella

Étape 1. Vous pouvez sélectionner **Basic Auth** comme méthode d'autorisation, comme illustré dans l'image.

Remarque : Postman n'est pas un outil développé par Cisco. Si vous avez une question sur la fonctionnalité de l'outil Postman, veuillez contacter le support de Postman.



Étape 2. Vous pouvez obtenir **les ordinateurs itinérants**, avec cet appel d'API (la limite de page par défaut est de 100 entrées).

`https://management.api.umbrella.com/v1/organizations/`

`/roamingcomputers`

Étape 3. En réponse au premier appel, le nombre total d'objets est renvoyé. Vous pouvez utiliser les paramètres de limite et de page pour obtenir les pages suivantes.

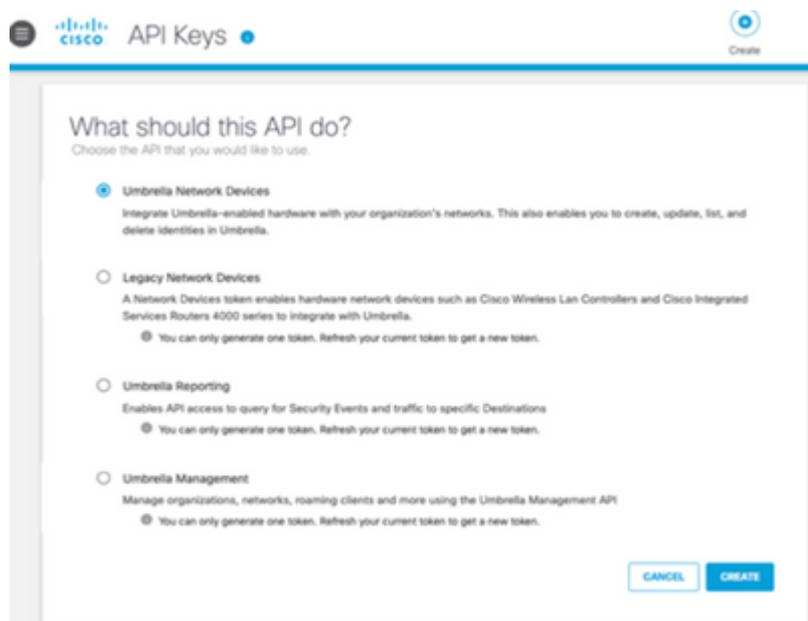
<https://management.api.umbrella.com/v1/organizations/>

[/roamingcomputers?limit=5&page=2](https://management.api.umbrella.com/v1/organizations/roamingcomputers?limit=5&page=2)

Clé incorrecte

XDR Device Insights n'utilise pas les mêmes clés que XDR. Vous devez donc vérifier et confirmer que les clés configurées comme clés d'API Umbrella sont correctes, comme illustré dans l'image.

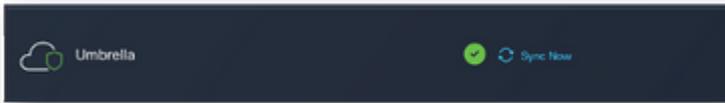
- Périphériques réseau parapluie : API utilisée pour connaître les politiques DNS
- Gestion globale : API utilisée pour apprendre les terminaux



Vérifier

Une fois qu'Umbrella est ajouté comme source à XDR Device Insights, vous pouvez voir un état de connexion **REST API** réussi.

- Vous pouvez voir la connexion de l'**API REST** avec un état vert
- Cliquez sur **SYNC NOW** pour déclencher la synchronisation complète initiale, comme indiqué dans l'image



Si le problème persiste avec l'intégration Device Insights et Umbrella, collectez les journaux HAR à partir du navigateur et contactez le support TAC afin d'effectuer une analyse plus approfondie.

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.