

Dépannage de XDR Device Insights et de l'intégration orbitale

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 Device Insights et Orbital.

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.

Si vous souhaitez en savoir plus sur la configuration, consultez [ici](#) les détails du module d'intégration.

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 qu'Orbital.

Dépannage

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

Connectivité

- Les identifiants des sources de l'API REST peuvent être utilisés pour tester la connectivité de base à l'aide d'outils tels que Postman.
- Une fois que les résultats des requêtes commencent à provenir d'agents orbitaux, les données sont publiées dans Remote Datastore.
- Vérifiez si un data store distant a été créé pour Device Insights, cela peut être vérifié à partir des

paramètres du compte.

- À partir de l'administrateur des détails du magasin de données distant, vérifiez que l'ID du client Device Insights et l'URL de Device Insights s'affichent, l'état doit être Authenticated.



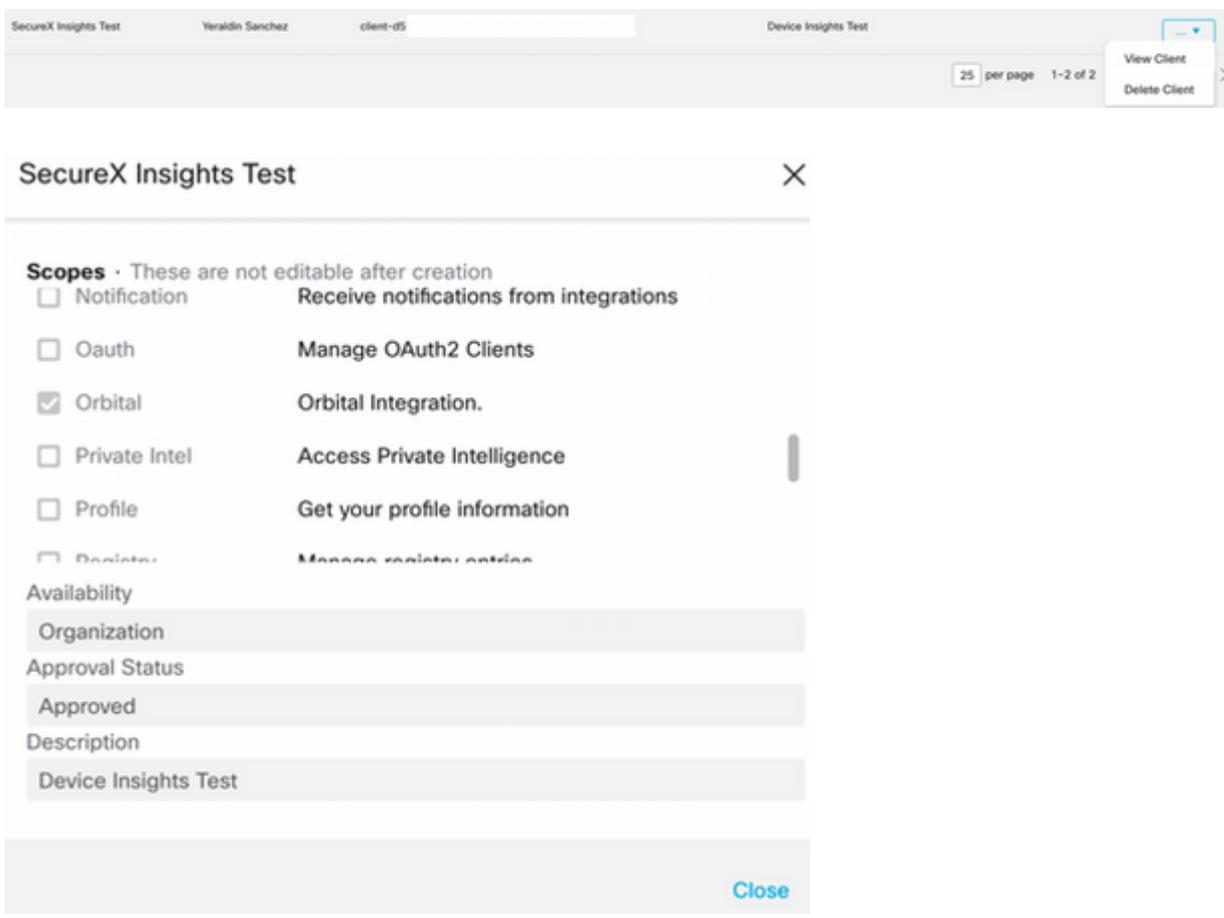
Name	ID	Address	Added By	Host	Status	Backend
Trust Response Private Intelligence	254...	4...	2023-07-28 14:02:11	Yeraklin Sanchez	private-intel.splunk.com	Authenticated
API2	242...	3...	2023-07-28 14:02:28	Yeraklin Sanchez	insights-api.us.securex.com	Authenticated

- Accédez à l'onglet Résultats afin de voir dans une liste de travaux le travail créé par Device Insights



Name	Status	Created	Substatus	Interval	Results	Search Base	Type	Created	Creator	Remote Data Store	Score
SecureX Insights Test	1	2023-07-28 14:07:48	0	24 Hours	0	0	Device Insights	Custom	Yeraklin Sanchez		

- À partir du portail XDR, accédez à Administration, sélectionnez le client API et assurez-vous qu'Orbital est sélectionné, comme indiqué dans les images.



SecureX Insights Test Yeraklin Sanchez client-d5 Device Insights Test

25 per page 1-2 of 2 View Client Delete Client

SecureX Insights Test

Scopes · These are not editable after creation

- Notification Receive notifications from integrations
- Oauth Manage OAuth2 Clients
- Orbital Orbital Integration.
- Private Intel Access Private Intelligence
- Profile Get your profile information
- Register Manage register entries

Availability

Organization

Approval Status

Approved

Description

Device Insights Test

Close

- Erreur « No response from endpoint, it may be offline » - Cette erreur signifie que le terminal est désactivé ou qu'il n'a pas de connectivité avec le cloud Orbital. Consultez le document [Required Server Addresses for Appropriate Cisco Secure Endpoint & Malware Analytics Operations](#) pour vous assurer que les adresses IP, les ports et les URL sont autorisés.

Nombre de discordances

- Si le nombre d'appareils ne correspond pas, cela est attendu car Orbital ne conserve pas son inventaire des terminaux qui sont plus de 90 jours depuis la version 1.14, cela inclut tous les terminaux sur lesquels un connecteur Orbital est installé à tout moment, et pas seulement les terminaux actifs dans son inventaire. Lorsque la fonction d'analyse des périphériques est active, elle crée une tâche

quotidienne récurrente que tous les terminaux doivent effectuer. Une fois que la tâche est exécutée sur le terminal et que les informations sur le périphérique résultant sont renvoyées à Orbital, XDR est averti de l'existence de ce périphérique par Orbital. Si aucun résultat de tâche n'est reçu pour cet appareil dans les 90 jours, le terminal Orbital est supprimé de l'inventaire dans les aperçus d'appareils.

- La réinstallation orbitale entraîne la création d'un nouveau GUID qui peut entraîner un doublon dans la console.

Licence

- Vérifiez que la console Secure Endpoint dispose de la licence appropriée pour accéder à Orbital.

Périphériques Mac et Linux non affichés

- Les appareils MacOS et Linux provenant d'Orbital ne sont pas encore pris en charge dans XDR Device Insights.

Si le problème persiste avec l'intégration XDR Device Insights et Orbital, veuillez consulter cet [article](#) pour collecter les journaux HAR à partir du navigateur et contacter le support TAC afin d'effectuer une analyse plus approfondie.

Informations connexes

- [Guide de référence XDR](#)
- [Dépannage orbital](#)
- [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.