

# Fehlerbehebung: Einblicke in XDR-Geräte und orbitale Integration

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

## Einleitung

In diesem Dokument werden die Schritte zur Konfiguration der Integration und zur Fehlerbehebung bei Device Insights- und Orbital-Integration beschrieben.

## Voraussetzungen

### Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Weitere Informationen zur Konfiguration finden Sie unter [hier](#) Details zum Integrationsmodul.

## Hintergrundinformationen

XDR Device Insights bietet eine einheitliche Ansicht der Geräte in Ihrem Unternehmen und konsolidiert Bestände aus integrierten Datenquellen, z. B. Orbital.

## Fehlerbehebung

In diesem Abschnitt finden Sie die Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

### Konnektivität

- REST API-Anmeldeinformationen von Quellen können verwendet werden, um grundlegende Konnektivität mit Tools wie Postman zu testen.
- Sobald die Ergebnisse der Abfragen von den Orbital-Agenten ausgehen, werden die Daten im

Remote-Datenspeicher veröffentlicht.

- Überprüfen Sie, ob ein Remote-Datenspeicher für Geräteeinblicke erstellt wurde. Dies kann anhand der Kontoeinstellungen überprüft werden.
- Überprüfen Sie vom Remote Data Store details-Administrator, ob Device Insights-Tenant-ID und URL von Device Insights angezeigt werden. Status muss Authenticated sein.

The screenshot shows the 'Settings' page with a navigation menu including 'My Account', 'Users', 'Remote Data Stores', 'Organizations', and 'Notifications'. Under 'Remote Data Stores', there are two entries:

Name	ID	Address	Added By	Host	Status	Created
Trust Response Private Intelligence	20	...	Yeroldin Sanchez	private-intel.any.cisco.com	Authenticated	2022-07-28 14:02:11
DS12	243...	...	Yeroldin Sanchez	private-intel.any.cisco.com	Authenticated	2022-07-28 14:02:26

- Navigieren Sie zur Registerkarte Ergebnisse, um den von Device Insights erstellten Auftrag in einer Jobliste anzuzeigen.

The screenshot shows the 'Results' page with a table of job entries:

Name	Status	Created	Delivered	Interval	Results	Search Base	Type	Content	Creator	Remote Data Store	Score
Device Insights - test	...	2022-07-28 14:02:26	...	24 hours	...	...	Device Insights	Custom	Yeroldin Sanchez	...	...

- Navigieren Sie im XDR-Portal zu Administration, wählen Sie den API-Client aus, und stellen Sie sicher, dass Orbital ausgewählt ist, wie in den Bildern gezeigt.

The screenshot shows the 'SecureX Insights Test' API Client management interface. It displays the client name 'client-d5' and the user 'Yeroldin Sanchez'. There are 'View Client' and 'Delete Client' buttons. The interface also shows '25 per page' and '1-2 of 2' items.

The screenshot shows the 'Scopes' configuration dialog for the API Client. It lists several scopes with checkboxes:

- 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

Below the scopes, there are sections for 'Availability' (Organization), 'Approval Status' (Approved), and 'Description' (Device Insights Test). A 'Close' button is at the bottom right.

- Fehler "Keine Antwort vom Endpunkt, möglicherweise offline" - Dieser Fehler bedeutet, dass der Endpunkt deaktiviert ist oder keine Verbindung zur Orbital-Cloud hat. Weitere Informationen finden Sie im Dokument "[Required Server Addresses for Proper Cisco Secure Endpoint & Malware Analytics Operations](#)" (Erforderliche Serveradressen für ordnungsgemäße Vorgänge für sichere Endpunkte und Malware-Analysen), um sicherzustellen, dass IPs, Ports und URLs zulässig sind.

## Anzahl der Nichtübereinstimmungen

- Wenn die Geräteanzahl nicht übereinstimmt, wird dies erwartet, da Orbital seinen Bestand an Endgeräten, die > 90 Tage seit Version 1.14 liegen, nicht verwaltet. Dies umfasst alle Endgeräte, auf denen ein Orbital-Connector installiert ist, und nicht nur die aktiven Geräte im Bestand. Wenn die Device Insights-Funktion aktiviert ist, wird ein sich täglich wiederholender Auftrag erstellt, den alle Endpunkte ausführen müssen. Nachdem der Auftrag auf dem Endpunkt ausgeführt wurde und die resultierenden Geräteinformationen an Orbital zurückgesendet wurden, wird XDR über das Vorhandensein dieses Geräts von Orbital informiert. Wenn innerhalb von 90 Tagen kein Auftragsergebnis für dieses Gerät eingeht, wird der Orbitalendpunkt in den Geräteeinblicken aus dem Bestand gelöscht.
- Die orbitale Neuinstallation führt zu einer neuen GUID, die ein Duplikat in der Konsole verursachen kann.

## **Lizenz**

- Vergewissern Sie sich, dass die Secure Endpoint Console über die richtige Lizenz für den Zugriff auf Orbital verfügt.

## **Mac- und Linux-Geräte werden nicht angezeigt**

- MacOS- und Linux-Geräte aus Orbital-Quellen werden in XDR Device Insights noch nicht unterstützt.

Sollte das Problem weiterhin mit der Integration von XDR-Geräteinformationen und Orbitalssystemen bestehen, lesen Sie diesen [Artikel](#), um HAR-Protokolle vom Browser zu erfassen, und wenden Sie sich an den TAC-Support, um eine tiefere Analyse durchzuführen.

## **Zugehörige Informationen**

- [XDR-Referenzhandbuch](#)
- [Orbitale Fehlerbehebung](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.