

Risoluzione dei problemi relativi a XDR Device Insights e all'integrazione orbitale

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

Introduzione

In questo documento viene descritto come configurare l'integrazione e la risoluzione dei problemi relativi a Device Insights e all'integrazione orbitale.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Per ulteriori informazioni sulla configurazione, consultare il [qui](#) i dettagli del modulo di integrazione.

Premesse

XDR Device Insights fornisce una vista unificata dei dispositivi dell'organizzazione e consolida gli inventari da origini dati integrate, come Orbital.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Connettività

- Le credenziali API REST delle origini possono essere utilizzate per verificare la connettività di base utilizzando strumenti come Postman.
- Quando i risultati delle query iniziano a provenire dagli agenti orbitali, i dati vengono pubblicati nell'archivio dati remoto.

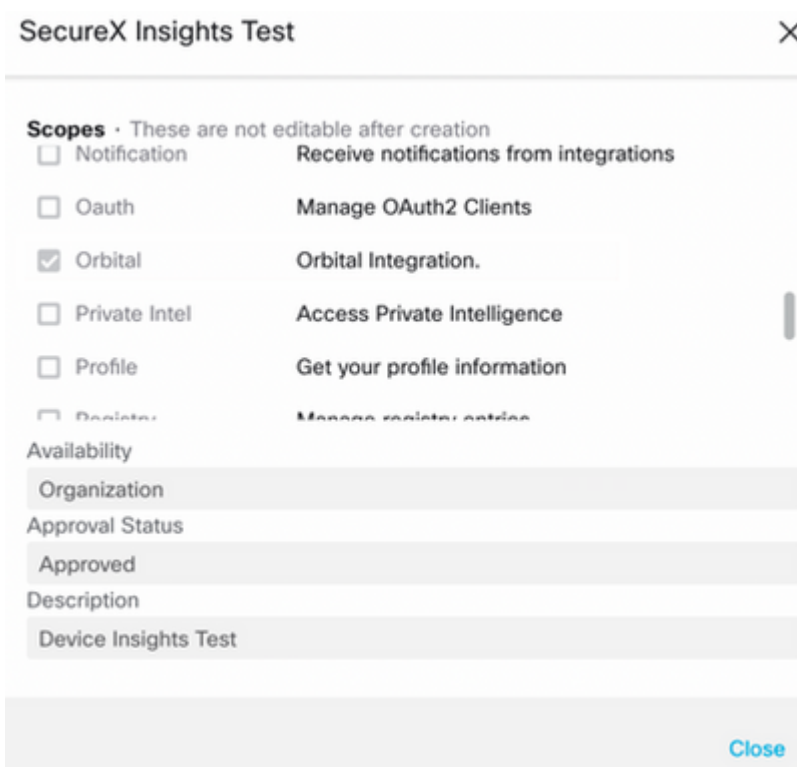
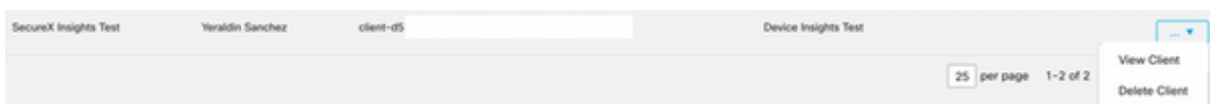
- Verificare se è stato creato un archivio dati remoto per Device Insights. È possibile verificare questa condizione dalle impostazioni dell'account.
- Dall'amministratore dei dettagli dell'archivio dati remoto, verificare che siano visualizzati l'ID tenant di Device Insights e l'URL di Device Insights. Lo stato deve essere Autenticato.



- Passare alla scheda Risultati per visualizzare in un elenco di processi il processo creato da Device Insights



- Dal portale XDR, passare ad Amministrazione, selezionare il client API e assicurarsi che sia selezionato Orbital, come mostrato nelle immagini.



- Errore "Nessuna risposta dall'endpoint, potrebbe essere offline" - Questo errore indica che l'endpoint è disattivato o non ha connettività con il cloud orbitale. Per verificare che gli IP, le porte e gli URL siano consentiti, consultare il documento [Required Server Addresses for Corper Cisco Secure Endpoint & Malware Analytics Operations](#).

Conteggio non corrispondente

- Se il numero di dispositivi non corrisponde, è previsto che Orbital non mantenga il proprio inventario di endpoint > 90 giorni dalla versione 1.14, ma includa tutti gli endpoint in cui è stato installato un

connettore orbitale in qualsiasi momento e non solo quelli attivi nel proprio inventario. Quando la funzionalità Device Insights è attiva, crea un processo giornaliero ricorrente per tutti gli endpoint da eseguire. Dopo l'esecuzione del processo sull'endpoint e l'invio delle informazioni risultanti a Orbital, XDR riceve una notifica dell'esistenza del dispositivo da Orbital. Se non si riceve alcun risultato di processo per il dispositivo entro 90 giorni, l'endpoint orbitale viene eliminato dall'inventario in device insights.

- La reinstallazione orbitale genera un nuovo GUID che può causare un duplicato nella console.

Licenza

- Verificare che Secure Endpoint Console disponga della licenza appropriata per accedere a Orbital.

Dispositivi Mac e Linux non visualizzati

- I dispositivi MacOS e Linux da origine orbitale non sono ancora supportati in XDR Device Insights.

Se il problema persiste con XDR Device Insights e l'integrazione orbitale, consultare questo [articolo](#) per raccogliere i log HAR dal browser e contattare il supporto TAC per eseguire un'analisi più approfondita.

Informazioni correlate

- [Guida di riferimento XDR](#)
- [Risoluzione dei problemi orbitali](#)
- [Documentazione e supporto tecnico](#) © Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).