Fehlerbehebung: Einblicke in XDR-Geräte und sichere Endgeräte-Integration

Inhalt

Einleitung

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

Hintergrundinformationen

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

Mit XDR Device Insights werden die Informationen aus allen Quellen konsolidiert und in Device Insights innerhalb von XDR angezeigt. So können Sie alle Geräteinformationen ganzheitlich betrachten und Geräte aus Ihrem Datenquellenportfolio effizienter untersuchen.

Nach der Aktivierung können Inventar- und Gerätedaten automatisch aus den in XDR integrierten Modulen abgerufen werden. Wenn Sie also bereits über Module verfügen, die in XDR integriert sind, müssen Sie sie nicht löschen oder neu hinzufügen, um diese Funktionalität zu erhalten.

Weitere Informationen zur Konfiguration finden Sie in den Cisco XDR-Konfigurationsmodulen.

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Secure Endpoint-Modul hinzufügen

- Der Benutzer, der das Modul aktiviert, benötigt Administratorrechte, um die Produkte zu integrieren.

Hinweis: Wenn Sie eine neue Quelle integrieren, müssen Sie entweder manuell eine Synchronisierung durchführen oder auf die automatische Synchronisierung warten, bevor Geräte angezeigt werden, die in den Bestand aufgenommen werden.

Konnektivität überprüfen

Um API-Verbindungen zuzulassen, stellen Sie sicher, dass der nächste FQDN in Ihrer Umgebung zugelassen ist.

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

User Postman zum Testen der Konnektivität

https://<Regionaler AMP API-FQDN>/v1/computers

https://< AMP-API, regionaler FQDN>/v1/computers/< Connector-GUID>

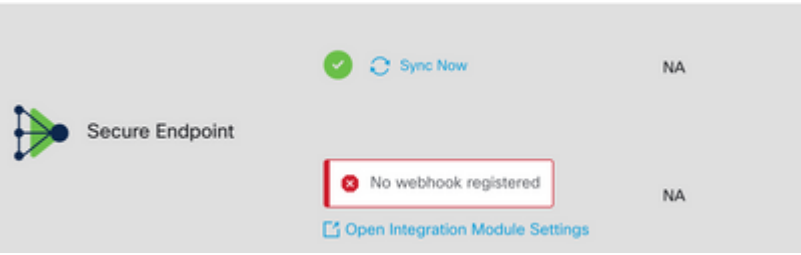
Hinweis: Secure Endpoint verwendet die grundlegende Authentifizierung als Autorisierungsmethode.

Nichtübereinstimmung der Gerätenummer

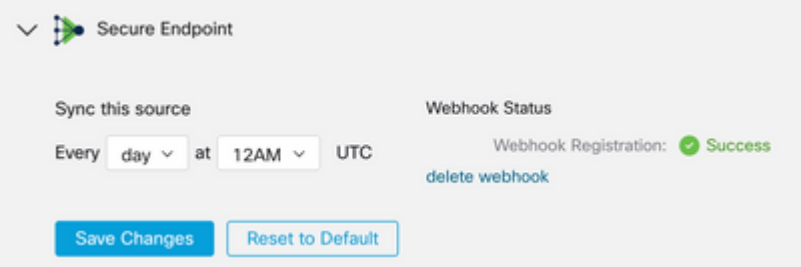
- Device Insights speichert die Informationen der letzten 90 Tage, Secure Endpoint dagegen die Informationen der letzten 30 Tage. Wenn bei der Anzahl der Geräte eine Diskrepanz festgestellt wird, stellen Sie sicher, dass der zuletzt angezeigte Computer nicht länger als 90 Tage in Anspruch nimmt.

- Vergewissern Sie sich, dass die Secure Endpoint-Konsole nicht über doppelte Anschlüsse verfügt, die die Ungleichheit auf beiden Konsolen verursachen.

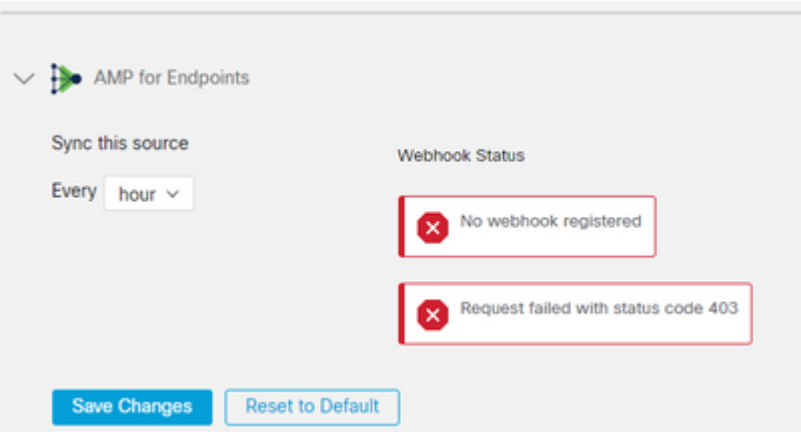
Szenario 1. Kein Webhook registriert



Navigieren Sie zu Source Setting, und klicken Sie dann auf die Schaltfläche Webhook registrieren. Sobald die Anforderung ausgeführt wurde, wird der Webhook-Status angezeigt, wie im Bild gezeigt.



Szenario 2. HTTP-Fehler.



400 - Ungültige Anfrage

401 - Nicht autorisiert

403 - Verboten

404 - Methode nicht zulässig

Überprüfen Sie bei HTTP-Fehlern die konfigurierten API-Anmeldeinformationen, und stellen Sie sicher, dass die gesammelten Informationen mit den Informationen übereinstimmen, die in die Modulkonfiguration von XDR eingefügt wurden.

Browser-Probleme

Wenn in Device Insights falsche Daten angezeigt werden, testen Sie dies in einem anderen Browser oder einem privaten Fenster, um den falschen oder veralteten Browser-Cache zu verwerfen.

Probleme mit mehreren Organisationen

Das Secure Endpoint-Integrationsmodul verwendet die Schaltfläche Enable. Aus diesem Grund kann Secure Endpoint jetzt nur mit einer Secure Endpoint-Konsole verknüpft werden, Sie können jedoch mehrere Secure Endpoint-Module unter einem XDR verknüpft haben, wenn Sie der Administrator für diese Unternehmen sind. Mit anderen Worten: Wenn Sie in mehreren sicheren Endpunkt-Organisationen als Administrator arbeiten, können Sie alle über das API-Modul unter einem XDR-Dashboard verknüpfen lassen. Vergewissern Sie sich, dass die Secure Endpoint-Konsole nicht bereits in eine andere XDR-Organisation integriert ist.

Im XDR-Portal können mehrere Instanzen von sicheren Endpunkten integriert sein, während sichere Endpunkte nur in eine einzige XDR-Instanz integriert werden können.

HAR-Protokolle

Falls das Problem weiterhin mit den Geräteinformationen und der Integration von sicheren Endpunkten auftritt, lesen Sie HAR-Protokolle von der XDR-Konsole sammeln, um zu erfahren, wie Sie HAR-Protokolle vom Browser sammeln können. Wenden Sie sich an den TAC-Support, um eine tiefere Analyse durchzuführen.

Zugehörige Informationen

- XDR-Anmeldung (Dokumentation)
- 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.