Probleemoplossing voor Device Insights en Secure Endpoint-integratie

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Achtergrondinformatie](#)
[Problemen oplossen](#)
[Voeg de beveiligde endpointmodule toe](#)
[Controleer de connectiviteit](#)
[Mismatch in nummer van apparaat](#)
[Problemen met browser](#)
[Problemen met Multi-org](#)
[HAR-logs](#)
[Gerelateerde informatie](#)

Inleiding

In dit document worden de stappen beschreven om de integratie te configureren en de integratie van Apparaatinzichten en Secure Endpoint probleemoplossing uit te voeren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

SecureX Device Insights biedt een uniforme weergave van de apparaten in uw organisatie en consolideert inventarissen uit geïntegreerde gegevensbronnen, zoals Secure Endpoint.

Met Device Insights wordt de informatie uit alle bronnen geconsolideerd en weergegeven in apparaatinzichten binnen SecureX, op een eenvoudiger manier om al uw apparaatinformatie holistisch te bekijken en apparaten in uw portfolio van gegevensbronnen efficiënter te onderzoeken.

Na activering is apparaatinzichten klaar om automatisch inventaris- en apparaatgegevens uit de modules te halen die u met SecureX hebt geïntegreerd. Dus als u al modules hebt die zijn geïntegreerd met SecureX, hoeft u deze niet te verwijderen of opnieuw toe te voegen om deze functionaliteit te hebben.

Als u meer wilt weten over de configuratie, raadpleegt u de Cisco SecureX-configuratiemodules voor meer informatie.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Voeg de beveiligde endpointmodule toe

- De gebruiker die de module inschakelt, moet beheerdersrechten hebben om de producten te integreren.

  Opmerking: Als u nieuwe bron integreert, moet u of handmatig synchroniseren of wachten op auto-synchronisatie te gebeuren voordat u apparaten ziet die in te inventariseren.

Controleer de connectiviteit

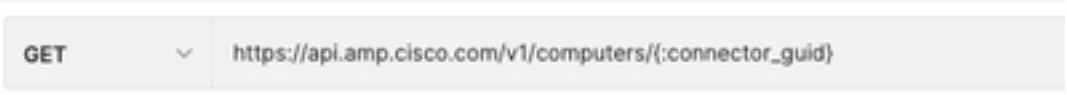
Om API-verbindingen toe te staan, moet u ervoor zorgen dat de volgende FQDN op uw omgeving is toegestaan.

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

Gebruiker Postman om connectiviteit te testen

https://<AMP API voor regionale FQDN>/v1/computers

https://< AMP API regionale FQDN>/v1/computers/<-connector GUID>



Opmerking: Secure Endpoint gebruikt basisautorisatie als een autorisatiemethode.

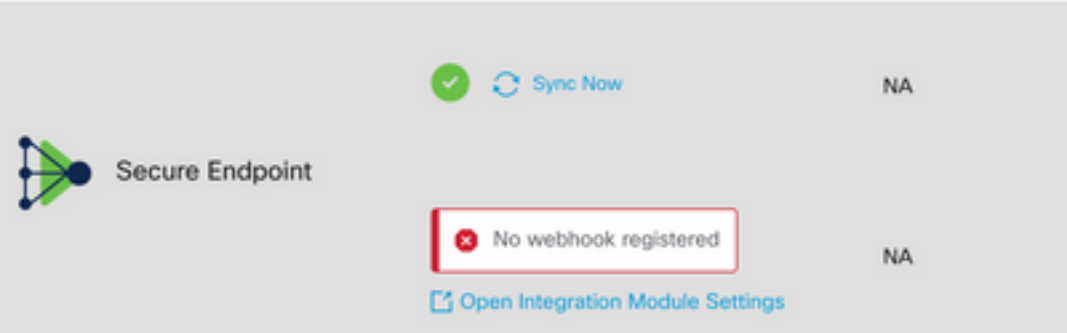
Mismatch in nummer van apparaat

- Device Insights slaat de informatie van de laatste 90 dagen op, maar Secure Endpoint slaat de informatie vanaf 30 dagen op. Als er een mismatch wordt gevonden op het aantal

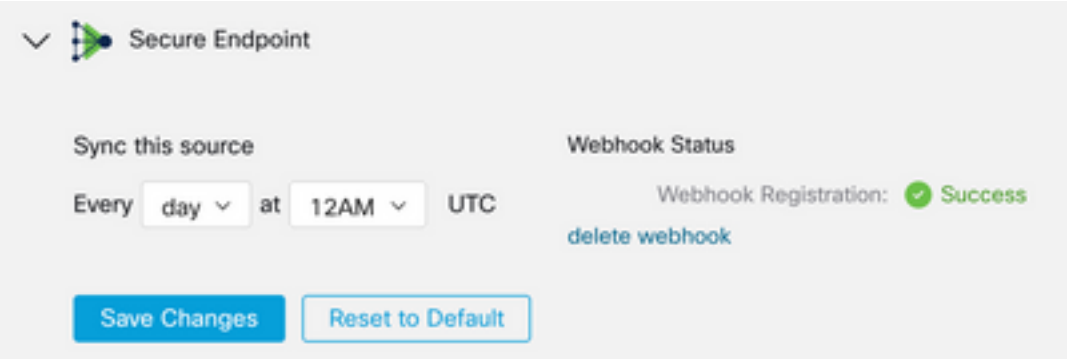
apparaten, controleert u of de laatst geziene van de betrokken computers niet meer dan 90 dagen heeft.

- Controleer of de Secure Endpoint-console geen dubbele connectors heeft die de mismatch op beide consoles veroorzaken.

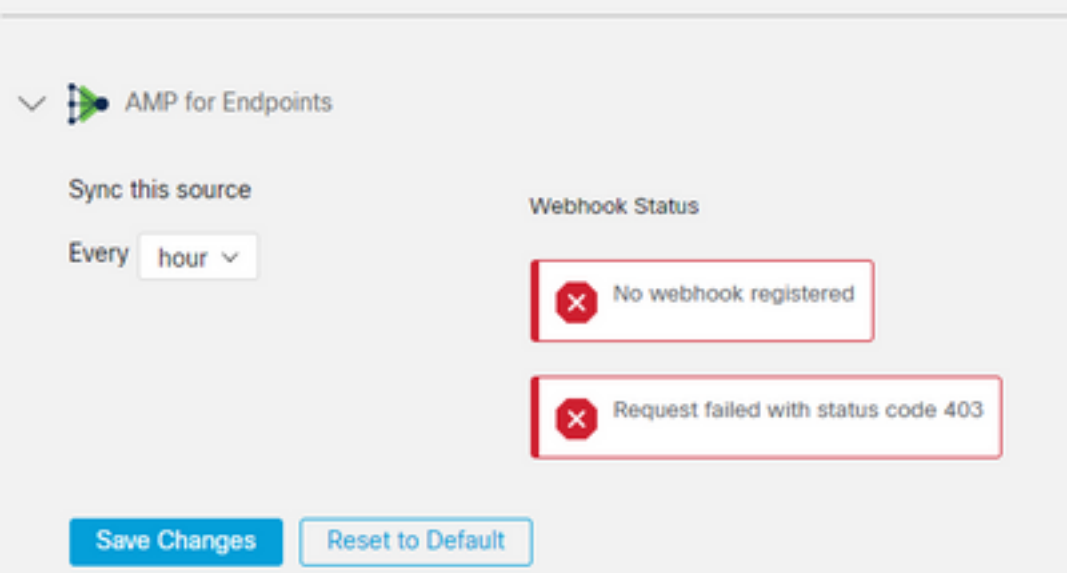
Scenario 1. Geen Webhook geregistreerd



Navigeer naar broninstelling en klik op de knop Webhook registreren, zodra het verzoek wordt uitgevoerd, de status van Webhook weergegeven zoals in de afbeelding.



Scenario 2. HTTP-fouten.



400 - Slecht verzoek

401 - Niet geautoriseerd

403 - Forbiden

404 - Methode niet toegestaan

Voor HTTP-fouten controleert u de geconfigureerde API-referenties en zorgt u ervoor dat de verzamelde informatie overeenkomt met de informatie die op de moduleconfiguratie op SecureX is geplakt.

Problemen met browser

Wanneer verkeerde gegevens worden weergegeven in Device Insights, test je in een andere browser of een privévenster om verkeerde of verouderde browsercache te verwijderen.

Problemen met Multi-org

Secure Endpoint-integratiemodule gebruikt de knop Enable. Om die reden kan Secure Endpoint nu slechts aan één Secure Endpoint console worden gekoppeld, maar u kunt nog steeds meerdere Secure Endpoint modules hebben die onder één SecureX zijn gekoppeld als u de Admin voor die organisaties bent. Met andere woorden als u Admin bent in meerdere Secure Endpoint organisaties kunt u al die verbonden via API-module onder één SecureX-dashboard hebben. Controleer dat de Secure Endpoint console nog niet is geïntegreerd in een andere SecureX-organisatie.

SecureX-portal kan meerdere Secure Endpoint-instanties hebben geïntegreerd, maar Secure Endpoint kan slechts in één SecureX-instantie worden geïntegreerd.

HAR-logs

Als het probleem blijft bestaan met de integratie van Device Insights en Secure Endpoint, raadpleeg dan HAR Logs van SecureX Console voor het verzamelen van HAR-logbestanden van de browser en neem contact op met TAC-ondersteuning om een diepere analyse uit te voeren.

Gerelateerde informatie

- SecureX-aanmelding (documentatie)
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.