

Probleemoplossing voor XDR-apparaatzichten en Microsoft Intune-integratie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

Inleiding

In dit document worden de stappen beschreven om de integratie te configureren en de integratie van Device Insights en Intune op te lossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan.

- XDR
- Microsoft Intune
- Basiskennis van API's™s
- Postman API-tool

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies.

- XDR

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

XDR Device Insights biedt een uniforme weergave van de apparaten in uw organisatie en consolideert inventarissen uit geïntegreerde gegevensbronnen.

Microsoft Intune is een Enterprise Mobility Manager (EMM), ook bekend als Mobile Device Manager (MDM) of Unified Endpoint Manager (UEM). Wanneer u Microsoft Intune met XDR integreert, verkrijgt het de endpointdetails die beschikbaar zijn in XDR Device Insights en de endpointgegevens die beschikbaar zijn wanneer u incidenten onderzoekt. Wanneer u Microsoft Intune-integratie configureert, moet u enige informatie verzamelen via uw Azure-portal en vervolgens de Microsoft Intune-integratiemodule in XDR toevoegen.

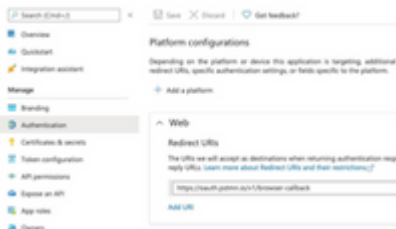
Wilt u meer weten over de configuratie, bekijk dan de details van de integratiemodule.

Problemen oplossen

Om gemeenschappelijke problemen met de integratie van XDR en Intune op te lossen, kunt u de connectiviteit en de prestaties van de API verifiëren.

Connectiviteitstest met XDR Device Insights en Intune

- Postman Azure App-configuratie voor Graph API is [hier](#) gedocumenteerd
- Op hoog niveau moet de beheerder bijvoorbeeld omleiding-URI's definiëren



- API-rechten kunnen hetzelfde blijven als in de Device Insights-app
- Fork for Graph API-verzameling kan [hier](#) worden gemaakt

API / Permissions name	Type	Description
Microsoft Graph (2)		
DeviceManagementManagement	Application	Read Microsoft Intune devices
User Read	Delegated	Sign in and read user profile

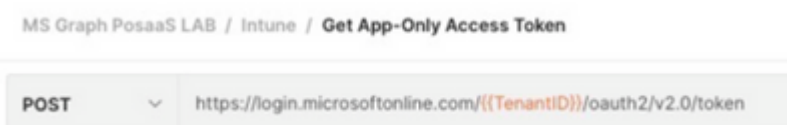
- De omgeving die bij de vork komt, moet deze waarden per app/huurder laten aanpassen

Microsoft Graph environment	
VARIABLE	INITIAL VALUE
ClientID	
ClientSecret	
TenantID	

- U kunt Postman Tool gebruiken om een meer visuele output te hebben terwijl u de connectiviteit test.

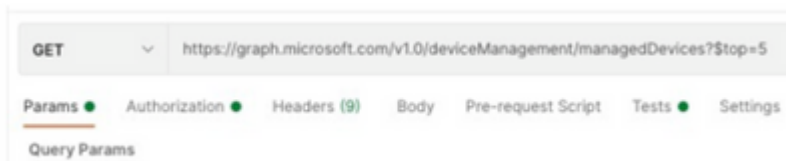
Opmerking: Postman is geen door Cisco ontwikkeld programma. Als u een vraag hebt over de functionaliteit van Postman tool, neem dan contact op met Postman support.

- De eerste oproep die wordt uitgevoerd is **Get App-Only Access Token**. Als de juiste **App-referenties** en **huurder-ID** werden gebruikt, wordt de omgeving door deze oproep bevolkt met het app-toegangsteken. Als dit is gebeurd, kunnen feitelijke API-oproepen worden uitgevoerd zoals in de afbeelding.



- U kunt deze API-aanroep gebruiken om Intune-endpoints te verkrijgen, zoals in de afbeelding wordt getoond (indien nodig, bekijk dit Graph API-[paginatiedocument](#))

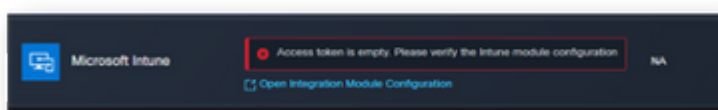
https://graph.microsoft.com/v1.0/deviceManagement/managedDevices



Access Token is leeg. Controleer de Intune-configuratiemodule

Access Token is leeg als er een OAuth-fout optreedt, zoals in de afbeelding.

- Meestal veroorzaakt door een Azure UI-bug
- Het moet het token-eindpunt zijn voor de Org.



- U kunt beide locaties proberen om de Endpoints, de **geïntegreerde app** en de wortel van **App-registraties > Endpoints** te zien
- U kunt Endpoints bekijken vanuit uw Azure geïntegreerde App die wordt getoond als generieke, niet-specifieke URL's voor de OAuth Endpoints, zoals in de afbeelding



Waarde geheime id

Controleer of u de **geheime ID** hebt gekopieerd, niet de **geheime waarde** (de waarde is de API-sleutel en de geheime ID zelf is een interne index voor Azure zelf en het helpt niet). U moet de waarde gebruiken in XDR Device Insights en deze waarde wordt alleen tijdelijk weergegeven.

Verifiëren

Zodra Intune wordt toegevoegd als een bron aan XDR Device Insights, kunt u een succesvolle **REST API** verbindingstatus zien.

- U kunt de **REST API** verbinding met een groene status zien.
- Druk op **SYNC NOW** om de eerste volledige sync te activeren, zoals in het beeld wordt getoond.



Als het probleem blijft bestaan met de integratie van XDR Device Insights en Intune, verzamel dan HAR-logbestanden van de browser en neem contact op met TAC-ondersteuning om een diepere analyse uit te voeren.

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.