Solución de problemas de XDR Device Insights y Microsoft Intune Integration

Contenido

Introducción

Este documento describe los pasos para configurar la integración y resolver problemas de Device Insights e integración de Intune.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas.

- XDR
- Microsoft Intune
- Conocimiento básico de las API
- herramienta API Postman

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- XDR

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

XDR Device Insights proporciona una vista unificada de los dispositivos de su organización y consolida inventarios a partir de fuentes de datos integradas.

Microsoft Intune es un Enterprise Mobility Manager (EMM), también conocido como Mobile Device Manager (MDM) o Unified Endpoint Manager (UEM). Al integrar Microsoft Intune con XDR, se enriquecen los detalles del terminal disponibles en XDR Device Insights y los datos del terminal disponibles al investigar incidentes. Al configurar la integración de Microsoft Intune, debe recopilar información del portal de Azure y, a continuación, agregar el módulo de integración de Microsoft Intune en XDR.

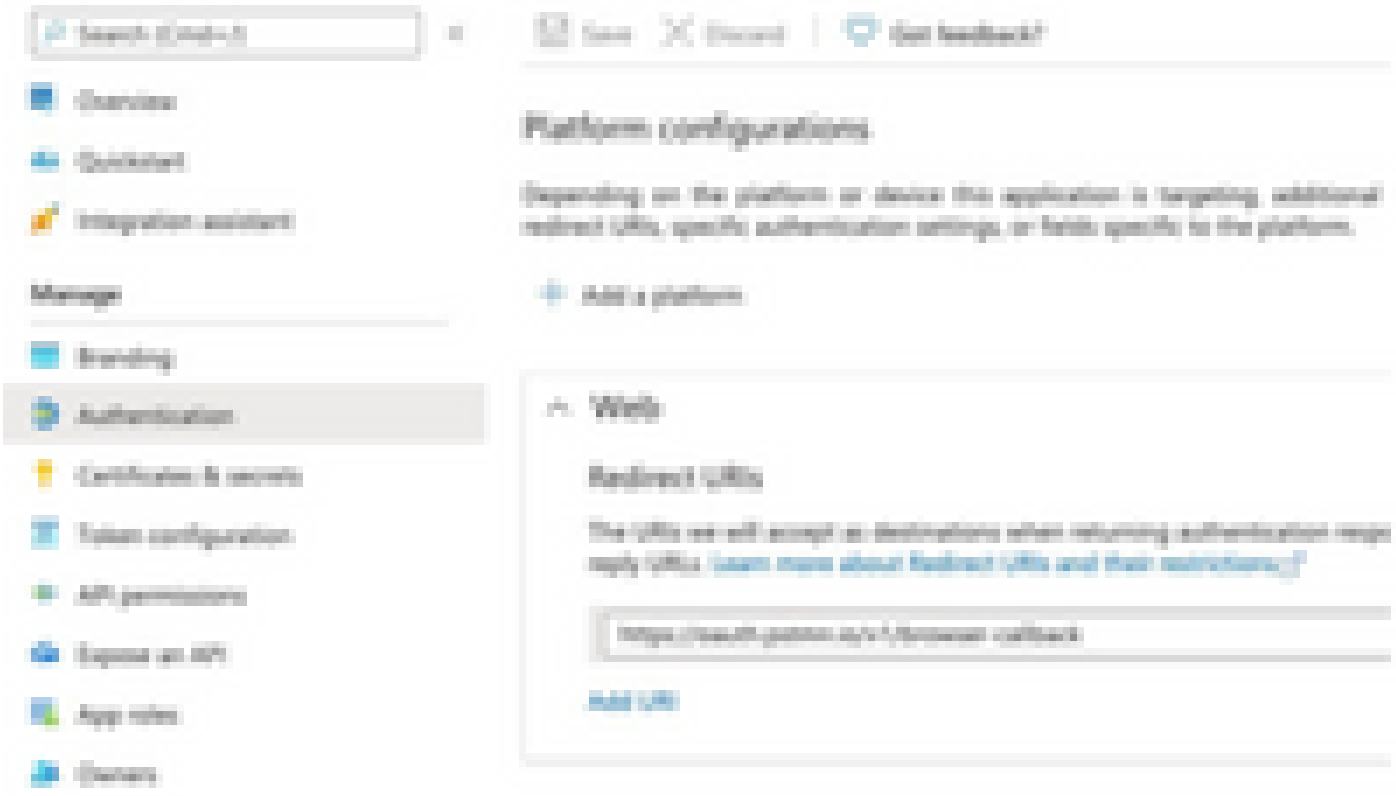
Si desea obtener más información sobre la configuración, revise los detalles del módulo de integración.

Troubleshoot

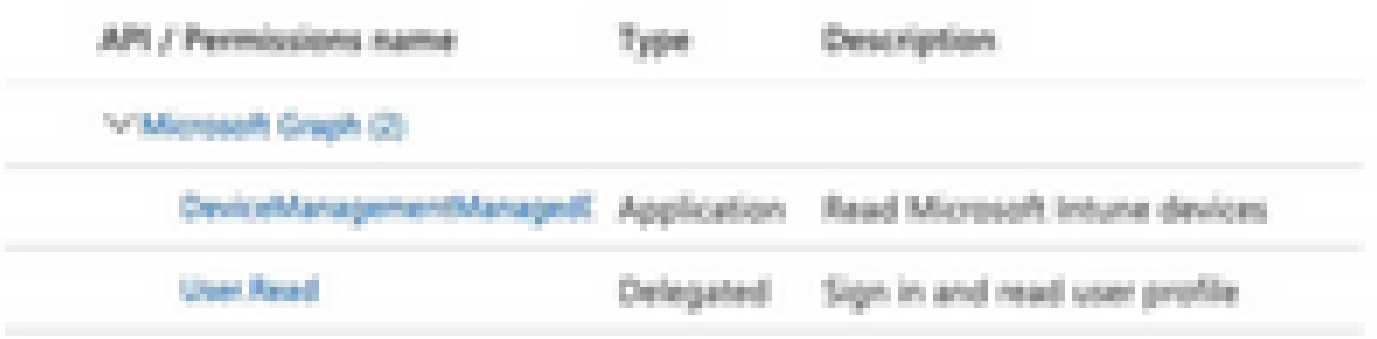
Para solucionar problemas comunes con la integración XDR e Intune, puede verificar la conectividad y el rendimiento de la API.

Prueba de conectividad con XDR Device Insights e Intune

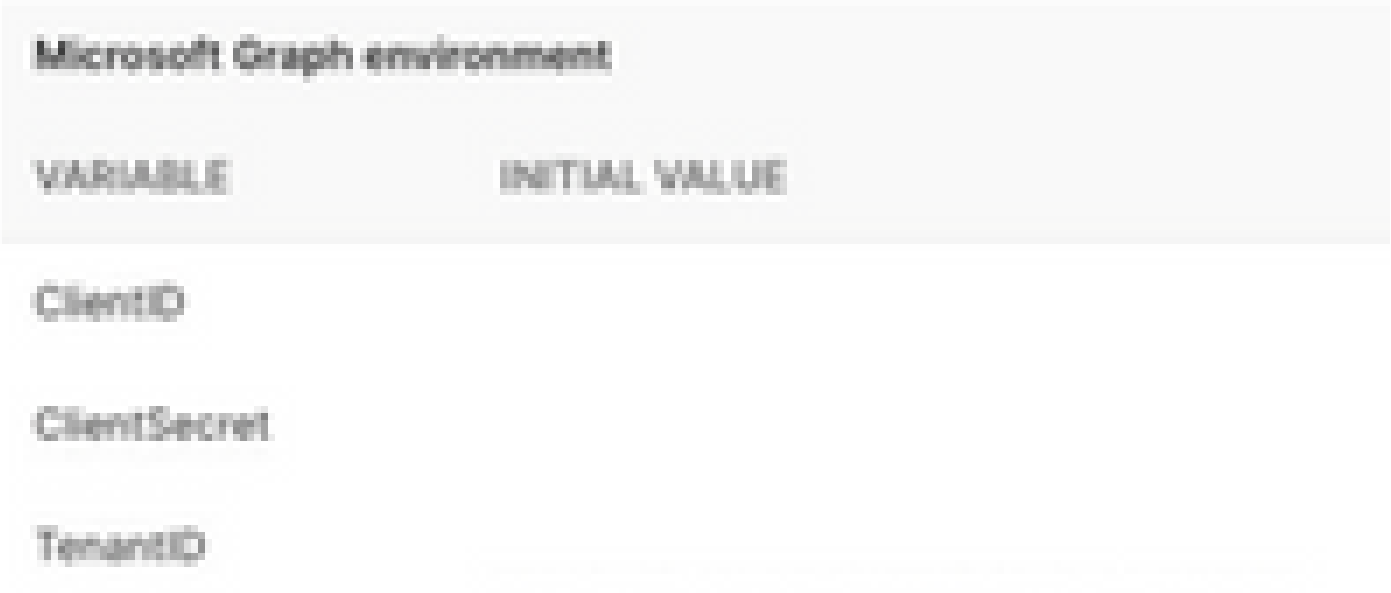
- La configuración de la aplicación Postman Azure para Graph API se documenta aquí
- En el administrador de alto nivel necesita definir URI de redireccionamiento, por ejemplo



- Los permisos de la API pueden ser los mismos que en la aplicación Device Insights
- Aquí se puede crear una bifurcación para la recopilación de API de Graph



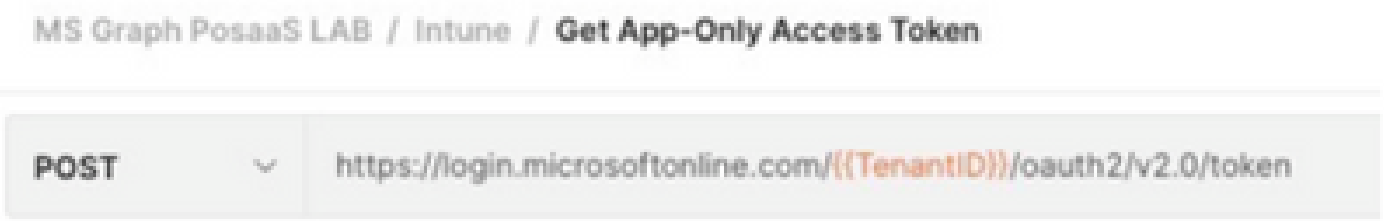
- El entorno que se incluye con la bifurcación debe tener esos valores ajustados por aplicación/arrendatario



- Puede utilizar la herramienta Postman para obtener una salida más visual mientras prueba la conectividad.

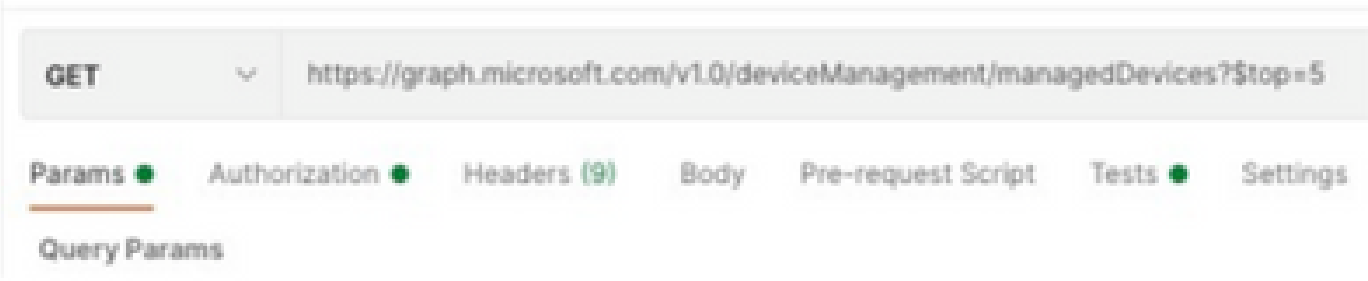
Nota: Postman no es una herramienta de Cisco. Si tiene alguna pregunta sobre la funcionalidad de la herramienta Postman, póngase en contacto con el servicio de asistencia de Postman.

- La primera llamada que se ejecutará es Get App-Only Access Token. Si se utilizaron las credenciales de la aplicación y el ID de arrendatario correctos, esta llamada rellena el entorno con el token de acceso a la aplicación. Una vez hecho esto, las llamadas API reales se pueden ejecutar como se muestra en la imagen



- Puede utilizar esta llamada de API para obtener los terminales de Intune, como se muestra en la imagen (si es necesario, revise este documento de paginación de la API de Graph)

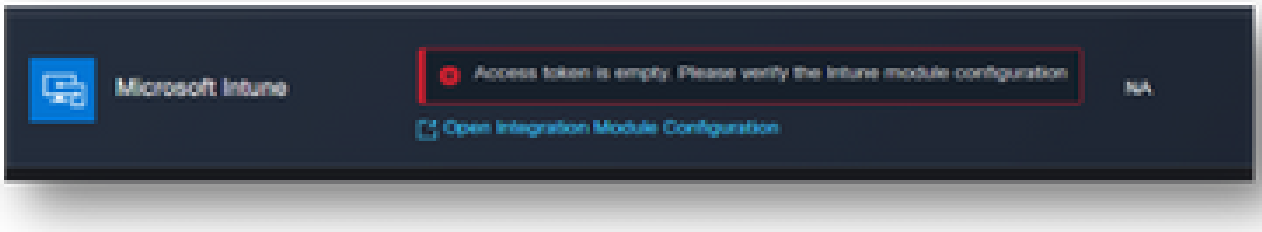
```
https://graph.microsoft.com/v1.0/deviceManagement/managedDevices
```



El token de acceso está vacío, compruebe el módulo de configuración de Intune

El token de acceso está vacío es un error de OAuth, como se muestra en la imagen.

- Generalmente causado por un error de interfaz de usuario de Azure
- Debe ser el punto final del token para la organización



- Puede probar ambas ubicaciones para ver los terminales, la aplicación integrada y la raíz de Registros de aplicaciones > Terminales

- Puede ver los extremos desde la aplicación integrada de Azure que se muestra como URL genéricas no específicas para los extremos de OAuth, como se muestra en la imagen

Valor de ID secreto

Verifique que copió el ID secreto, no el Valor secreto (el Valor es la Clave API y el ID secreto en sí es un índice interno para Azure y no ayuda). Debe utilizar el valor en XDR Device Insights, y este valor solo se muestra temporalmente.

Verificación

Una vez que Intune se agrega como fuente a XDR Device Insights, puede ver un estado de conexión API REST exitoso.

- Puede ver la conexión REST API con un estado verde.
- Presione en SYNC NOW para activar la sincronización completa inicial, como se muestra en la imagen.

En caso de que el problema persista con la integración de Intune y XDR Device Insights, recopile los registros HAR del navegador y póngase en contacto con el soporte del TAC para realizar un análisis más profundo.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).