

Solución de problemas de Device Insights e integración de Intune

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Troubleshoot](#)

[Prueba de conectividad con Device Insights e InTune](#)

[El token de acceso está vacío, compruebe el módulo de configuración de Intune](#)

[Valor de ID secreto](#)

[Verificación](#)

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.

- SecureX
- 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.

- SecureX 1.103

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

SecureX 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 SecureX, se enriquecen los detalles del terminal disponibles en SecureX 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 SecureX.

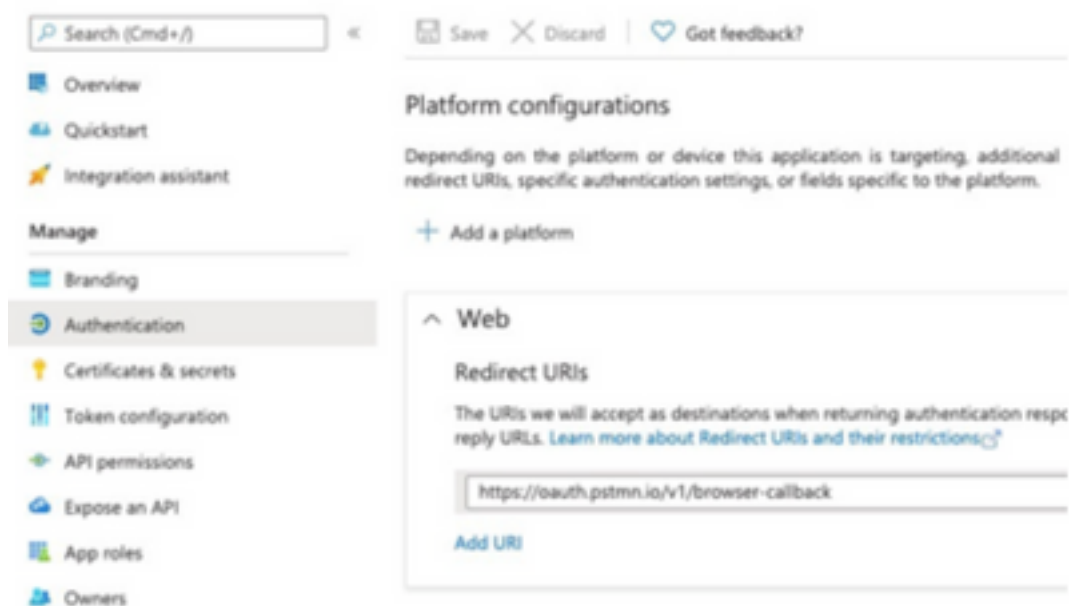
Si desea obtener más información sobre la configuración, revise dónde están los detalles del módulo de integración.

Troubleshoot

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

Prueba de conectividad con 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 redirección, 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 API de Graph

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

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

Microsoft Graph environment

VARIABLE

INITIAL VALUE

ClientID

ClientSecret

TenantID

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

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

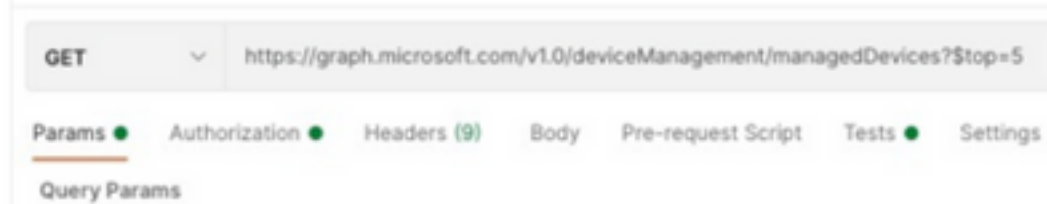
- La primera llamada que se ejecutará es **Get App-Only Access Token**. Si se utilizaron las **credenciales de la aplicación** y el **ID de arrendatario** correctos, esta llamada llena el entorno con el token de acceso a la aplicación. Una vez hecho esto, las llamadas API reales se pueden ejecutar como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

MS Graph PosaaS LAB / Intune / **Get App-Only Access Token**



- 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)

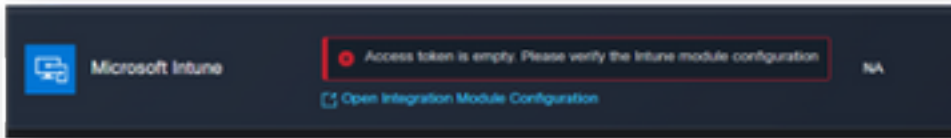
<https://graph.microsoft.com/v1.0/deviceManagement/managedDevices>



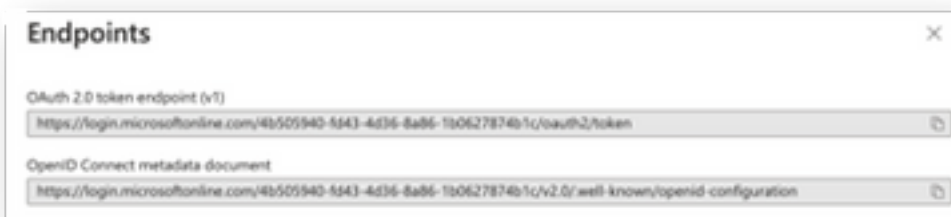
El token de acceso está vacío, compruebe el módulo de configuración de Intune

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 mostrados 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 SecureX Device Insights, y este valor solo se muestra temporalmente.

Verificación

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

- Puede ver la conexión API REST con un estado verde.
- Pulse en Sincronizar ahora para activar la sincronización completa inicial, como se muestra en la imagen.



En caso de que el problema persista con la integración de Device Insights e Intune, consulte este [artículo](#) para recopilar 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).