# Solucionar Problemas do Device Insights XDR e da Integração do Microsoft Intune

### Contents

Introdução Pré-requisitos Requisitos Componentes Utilizados Informações de Apoio

# Introdução

Este documento descreve as etapas para configurar a integração e solucionar problemas do Device Insights e da integração do Intune.

# **Pré-requisitos**

#### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos.

- XDR
- Microsoft Intune
- Conhecimento básico de APIs
- ferramenta de API Postman

#### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware.

• XDR

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

O XDR Device Insights fornece uma visão unificada dos dispositivos em sua organização e consolida inventários de fontes de dados integradas.

O Microsoft Intune é um Enterprise Mobility Manager (EMM), também conhecido como Mobile Device Manager (MDM) ou Unified Endpoint Manager (UEM). Quando você integra o Microsoft Intune com o XDR, ele enriquece os detalhes de endpoint disponíveis no XDR Device Insights e os dados de endpoint disponíveis quando você investiga incidentes. Ao configurar a integração do Microsoft Intune, você precisa coletar algumas informações do portal do Azure e adicionar o módulo de integração do Microsoft Intune no XDR. Para saber mais sobre a configuração, consulte os detalhes do módulo de integração.

### Troubleshooting

Para solucionar problemas comuns com a integração do XDR e do Intune, você pode verificar a conectividade e o desempenho da API.

#### Teste de conectividade com o XDR Device Insights e o Intune

- A configuração do aplicativo Postman Azure para a API do Graph está documentada aqui
- No nível superior, o administrador precisa definir URIs de redirecionamento, por exemplo

P Search (Crub-)	«
Chenies	Platform configurations
f Integration assistant	Depending on the platform or device this application is targeting, adultional redirect URs, specific authentication settings, or fields specific to the platform.
Manage	+ Add a platform
Branding	
Advertisation	~ Web
Cartificates & secure	Redirect URIs
Token configuration	The URs we will accept as destinations when returning authentication respo
AP permissions	reply URLs. Users mere about Nethret URLs and their restrictions.;?
Copena an API	https://www.injution.injuti/informationalitank
App roles	AMP UNI
a Owners	

- As permissões de API podem ser as mesmas do aplicativo Device Insights
- A bifurcação da coleção de API do Graph pode ser criada aqui

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

• O ambiente que vem com a bifurcação precisa ter esses valores ajustados por aplicativo/usuário

Microsoft Graph env	ironment
VARIABLE	INITIAL VALUE
ClientID	
ClientSecret	
TenantiD	

• Você pode usar a ferramenta Postman para ter uma saída mais visual enquanto testa a conectividade.

**Observação**: Postman não é uma ferramenta desenvolvida pela Cisco. Se você tiver alguma dúvida sobre a funcionalidade da ferramenta Postman, entre em contato com o suporte do Postman.

• A primeira chamada a ser executada é **Obter Token de Acesso Somente de Aplicativo**. Se as **credenciais do aplicativo** e a **ID do locatário** corretas forem usadas, essa chamada preencherá o ambiente com o token de acesso do aplicativo. Depois de concluído, as chamadas de API reais podem ser executadas como mostrado na imagem

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

POST v https://login.microsoftonline.com/{{TenantID}}/oauth2/v2.0/token

• Você pode usar esta chamada à API para obter pontos de extremidade do Intune, como mostrado na imagem (se necessário, revise este <u>documento</u> de paginação da API do Graph)



#### O Token de Acesso está vazio, verifique o módulo de configuração do Intune

O Token de Acesso está vazio é um erro OAuth, como mostrado na imagem.

- Causado geralmente por um bug de interface do usuário do Azure
- Ele deve ser o endpoint de token para a Org

Microsoft Intune	Access token is empty. Please verify the Intune module configuration C Open Integration Module Configuration	**
_		_

- Você pode tentar os dois locais para ver os endpoints, o aplicativo integrado e a raiz de Registros de aplicativo > Endpoints
- Você pode exibir Pontos de Extremidade de seu Aplicativo integrado do Azure mostrado como URLs genéricas e não específicas para os Pontos de Extremidade OAuth, como mostrado na imagem

Endpoints	×
JAuth 2.0 token endpoint (v1)	
https://login.microsoftonline.com/organizations/oauth2/token	0
OpenID Connect metadata document	
https://login.microsoftonline.com/organizations/v2.0/ well-known/openid-configuration	0
Endpoints	×
Endpoints	×
Endpoints Ofwarh 2.0 tokan endpoint (v1)	×
Endpoints OAuth 2.0 tokan andpoint (v1) (https://fogin.microsoftonline.com/40505940-5443-4d)4-8a64-10062787401c(bavdh3/tokan	×
Endpoints OAuth 2.0 token endpoint (v1) https://togin.microsoftunline.com/40505540-6543-4d36-8a86-10062787401c/bauth2/token OpenID Connect metadata document	×

#### Valor da ID do segredo

Verifique se você copiou a **ID Secreta**, não o **Valor Secreto** (o Valor é a Chave de API e a própria ID Secreta é um índice interno do próprio Azure e não ajuda). Você precisa usar o valor no XDR Device Insights, e esse valor é exibido apenas temporariamente.

### Verificar

Depois que o Intune for adicionado como uma origem para o XDR Device Insights, você poderá ver um status de conexão **REST API** bem-sucedido.

- Você pode ver a conexão da **API REST** com um status verde.
- Pressione SYNC NOW para acionar a sincronização completa inicial, como mostrado na imagem.



Caso o problema persista com o XDR Device Insights e a integração do Intune, colete logs HAR do navegador e entre em contato com o suporte do TAC para executar uma análise mais profunda.

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.