排除XDR设备见解和Microsoft Intune集成故障

目录

简介

本文档介绍配置集成以及对Device Insights和Intune集成进行故障排除的步骤。

先决条件

要求

Cisco建议您了解这些主题。

- XDR
- Microsoft Intune
- API基础知识
- Postman API工具

使用的组件

本文档中的信息基于以下软件和硬件版本。

- XDR

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

XDR Device Insights提供组织中设备的统一视图，并整合来自集成数据源的资产。

Microsoft Intune是企业移动管理器(EMM)，也称为移动设备管理器(MDM)或统一终端管理器(UEM)。将Microsoft Intune与XDR集成时，会丰富XDR设备见解中可用的终端详细信息以及调查事件时可用的终端数据。配置Microsoft Intune集成时，需要从Azure门户收集一些信息，然后在XDR中添加Microsoft Intune集成模块。

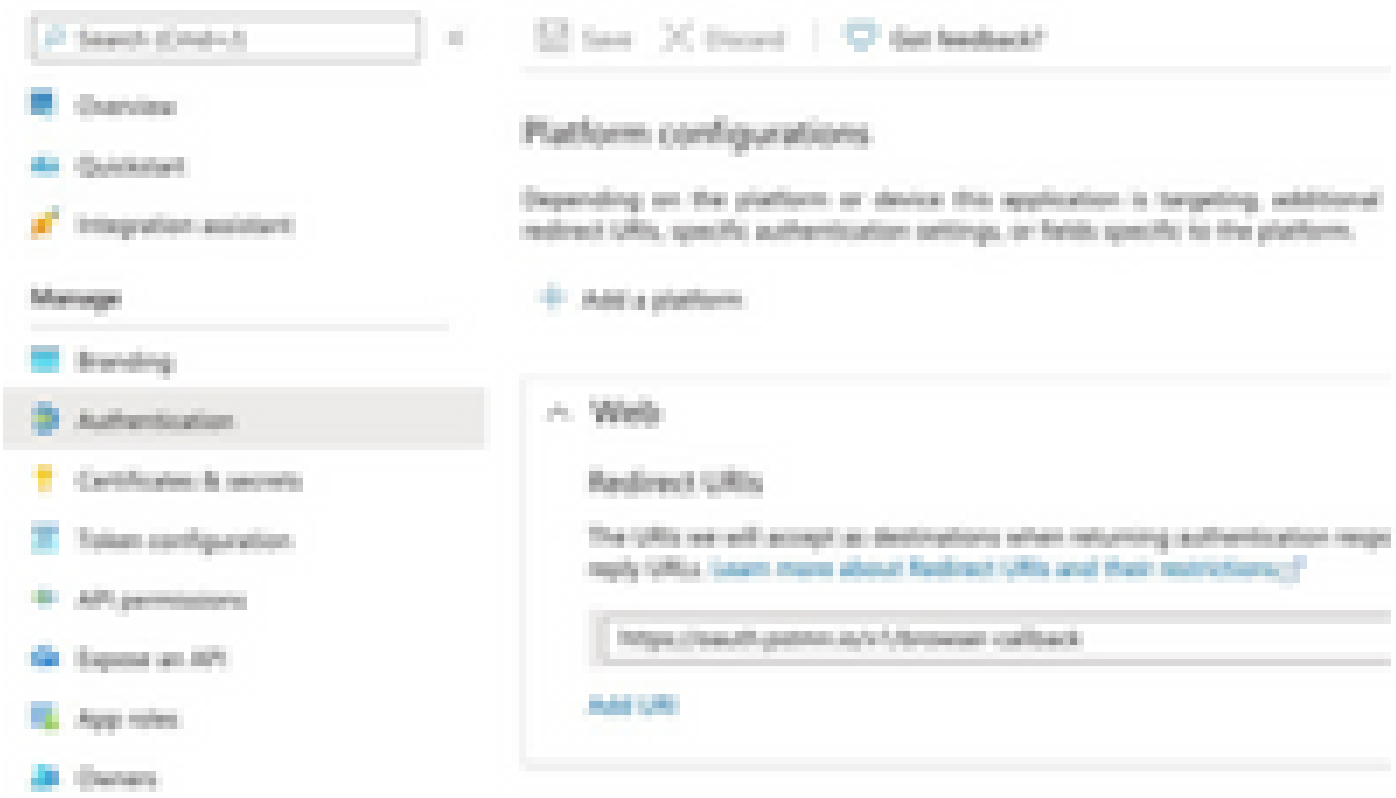
如果您想了解有关配置的更多信息，请查看集成模块详细信息。

故障排除

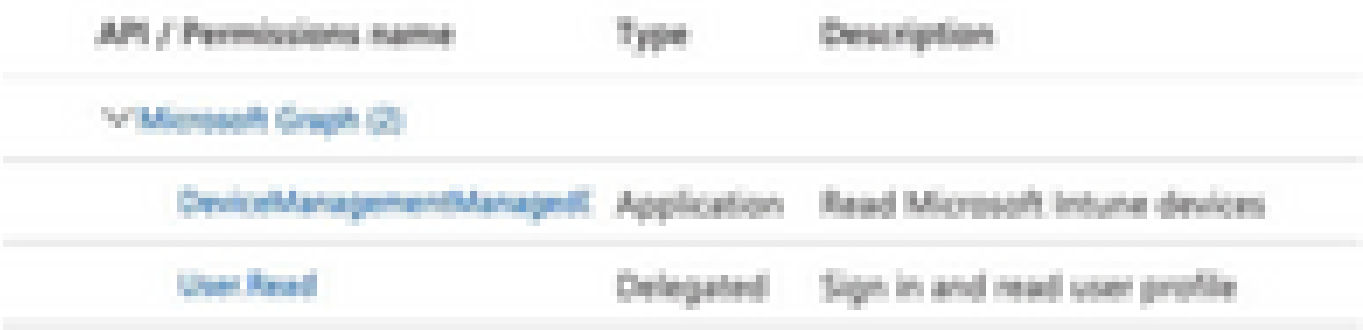
为了解决XDR和Intune集成的常见问题，您可以验证API的连接和性能。

使用XDR Device Insights和Intune进行连接测试

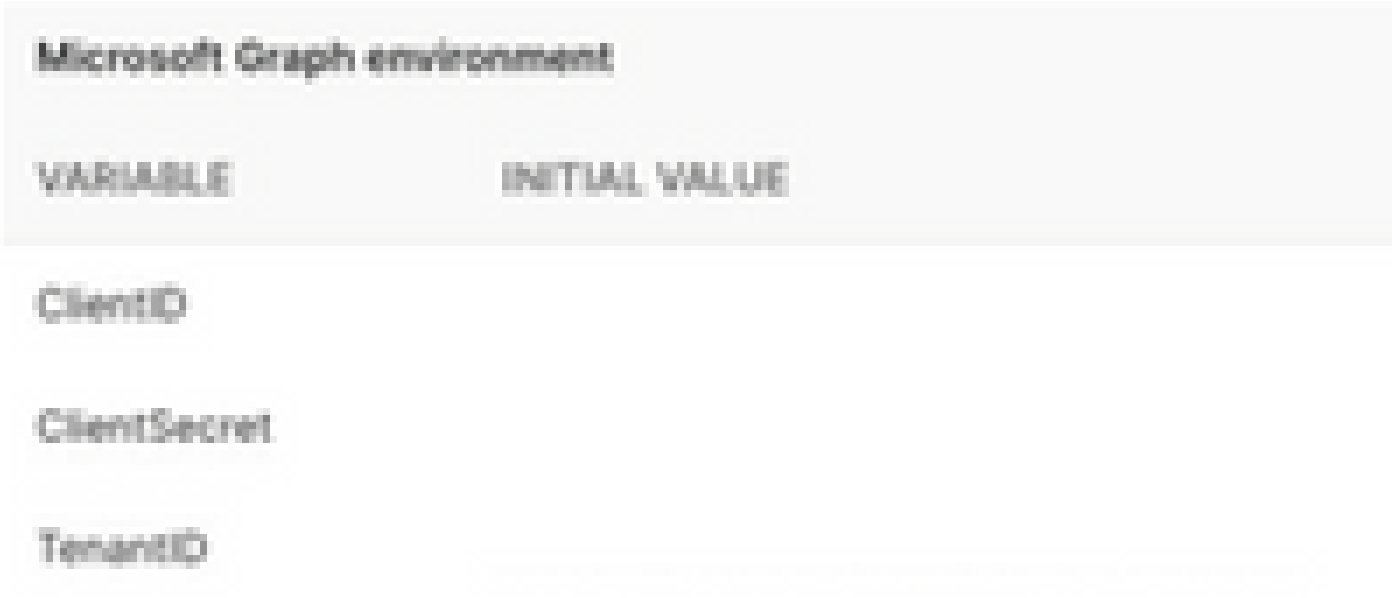
- Postman Azure App的图形API配置记录在此
- 例如，高级管理员需要定义重定向URI



- API权限可以与Device Insights App中的权限相同
- 可以在此处创建Fork for Graph API集合



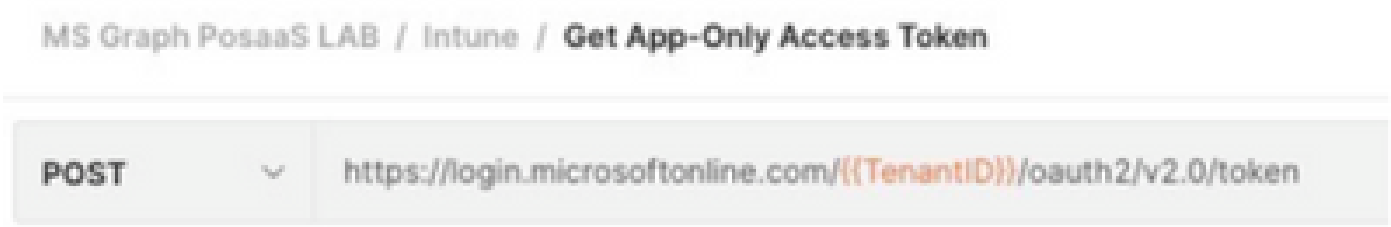
- 分叉附带的环境需要根据应用/租户调整这些值



- 测试连接时，您可以使用Postman工具获得更直观的输出。

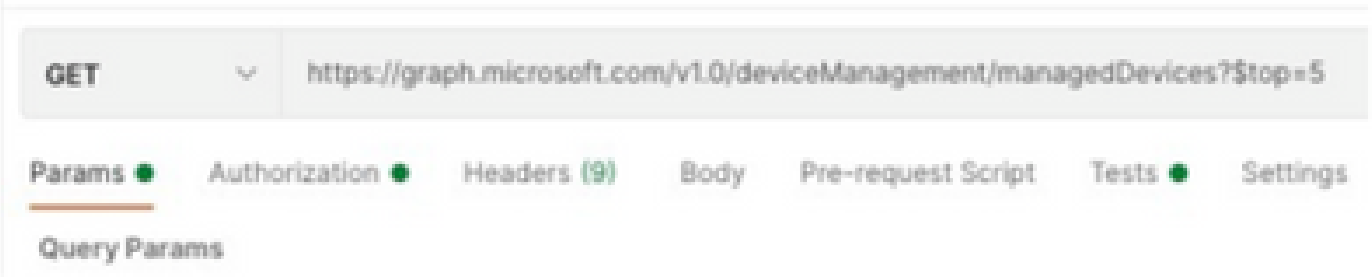
注:Postman不是思科开发的工具。如果您对Postman工具功能有任何疑问，请联系Postman支持。

- 要执行的第一个调用是获取仅应用访问令牌。如果使用正确的应用凭据和租户ID，此调用将使用应用访问令牌填充环境。完成后，即可执行实际的API调用，如图所示



- 您可以使用此API调用获取Intune终端，如图所示(如果需要，请查看此Graph API分页文档)

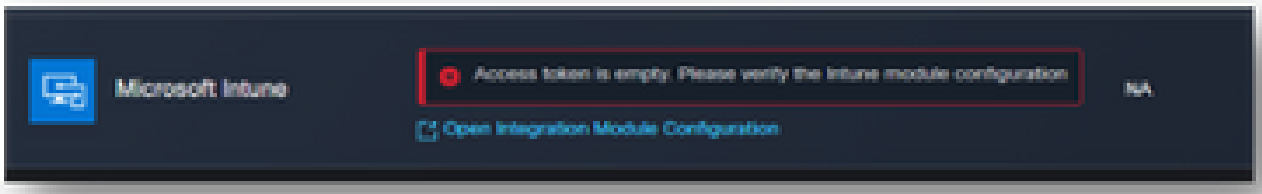
```
https://graph.microsoft.com/v1.0/deviceManagement/managedDevices
```



访问令牌为空，请验证Intune配置模块

Access Token is empty是一个OAuth错误，如图所示。

- 通常由Azure UI漏洞引起
- 它必须是组织的令牌终结点



- 您可以尝试两个位置查看终端、集成应用和应用注册>终端的根
- 您可以从Azure集成应用查看终端，这些终端显示为适用于OAuth终端的通用、非特定URL，如图所示

密钥ID值

验证您是否复制了Secret ID，而不是Secret Value（Value是API Key，Secret ID本身是Azure的内部索引，它不起作用）。您需要使用XDR设备见解中的值，并且此值仅临时显示。

验证

将Intune添加为XDR设备洞察的源后，您可以看到成功的REST API连接状态。

- 您可以看到REST API连接处于绿色状态。
- 按SYNC NOW以触发初始完全同步，如图所示。

如果XDR Device Insights和Intune集成仍然存在问题，请从浏览器收集HAR日志，并联系TAC支持以执行更深入的分析。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。