排除XDR设备见解和Umbrella集成故障

目录

简介

本文档介绍配置集成并排除XDR设备见解和Cisco Umbrella集成故障的步骤。

先决条件

要求

Cisco建议您了解这些主题。

- XDR
- Umbrella
- 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。

Umbrella可自动发现针对当前威胁而转移的攻击者基础设施，并在恶意请求到达组织的网络或终端之前主动阻止它们。通过集成，您可以更早地阻止恶意软件感染，更快地识别已受感染的设备，并防止数据泄露。这种集成可全面了解所有位置和用户的Internet活动，并允许您通过两键式响应采取行动，快速阻止域。支持多个Umbrella功能并通过Umbrella平台中生成的API密钥进行链接。

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。

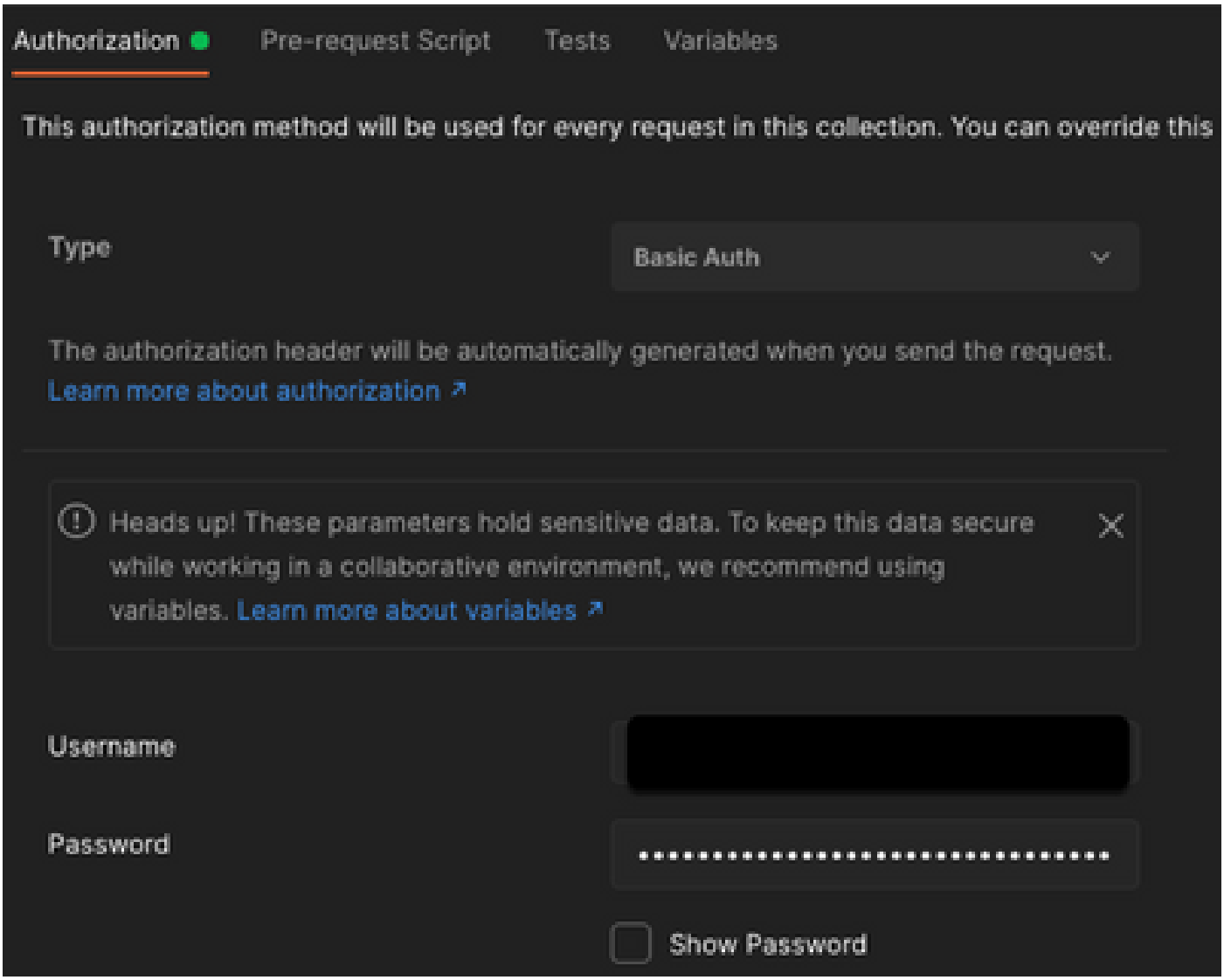
故障排除

为了解决XDR和Umbrella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Umbrella进行连接测试

步骤1:如图所示，您可以选择Basic Authas作为授权方法。

> 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。



第二步：通过此API调用，可以获取Roaming计算机（默认页面限制为100个条目）。

```
https://management.api.umbrella.com/v1/organizations/
```

```
/roamingcomputers
```

第三步：响应第一个调用，返回对象总数。可以使用限制和页面参数获取下一页。

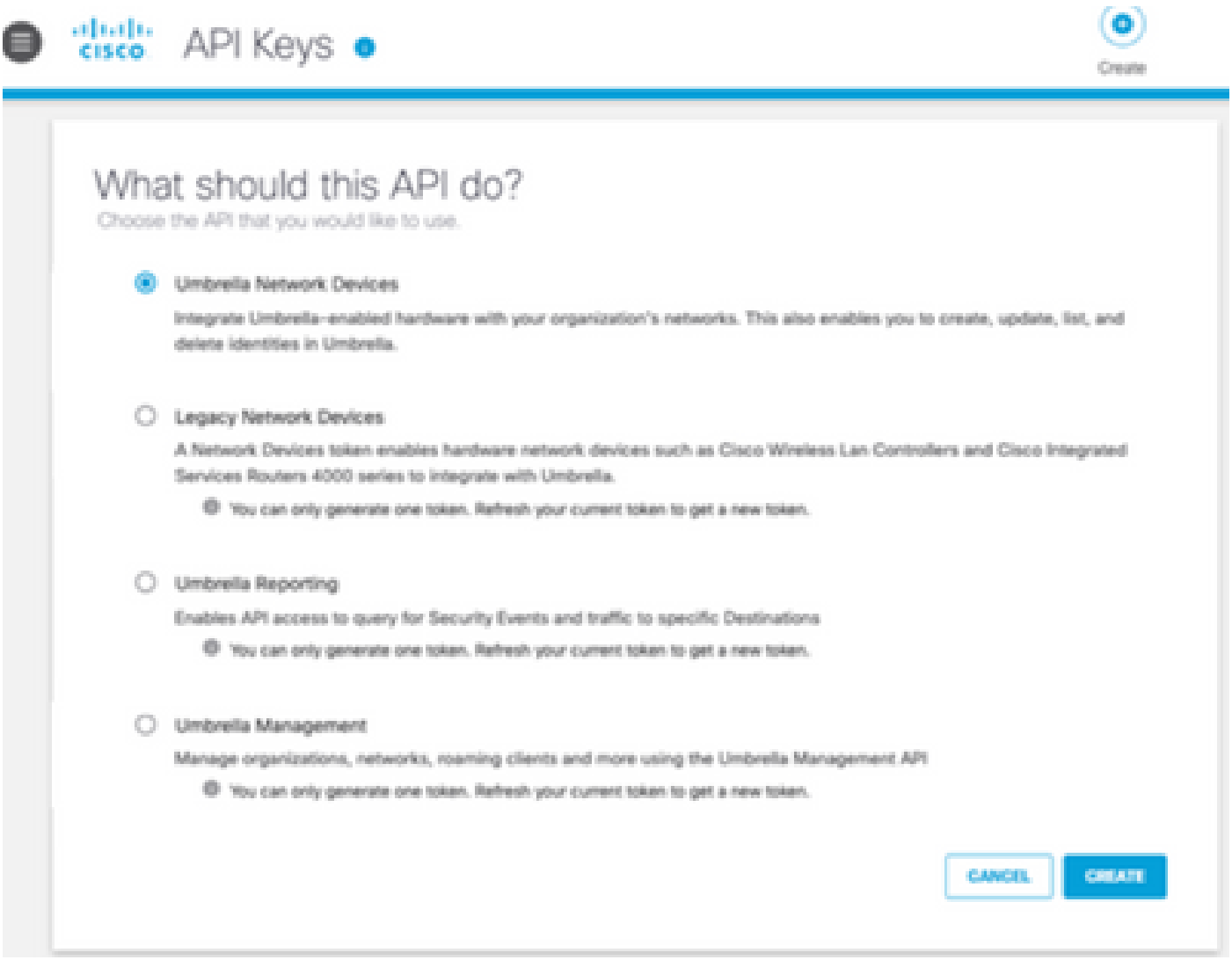
```
https://management.api.umbrella.com/v1/organizations/
```

```
/roamingcomputers?limit=5&page=2
```

错误的密钥

XDR Device Insights使用的密钥与XDR的密钥不同，因此需要验证并确认配置为Umbrella API密钥的密钥是否正确，如图所示。

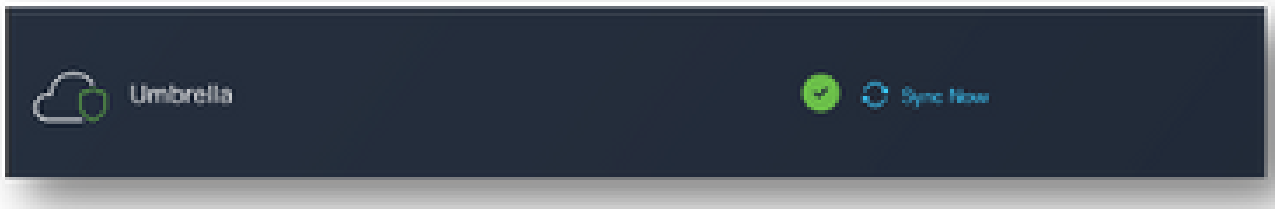
- Umbrella网络设备：用于了解DNS策略的API
- Umbrella Management：用于学习终端的API



验证

一旦将Umbrella添加为XDR设备洞察的源，您就可以看到成功的REST API连接状态。

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



如果Device Insights和Umbrella集成问题仍然存在，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）。