排除XDR设备见解和安全终端集成故障

目录

简介

本文档介绍配置集成以及对Device Insights和安全终端集成进行故障排除的步骤。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

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（如安全终端）的资产。

有了XDR设备洞察，来自所有来源的信息将进行整合，并在XDR内的设备洞察中显示，其方式更简单，以便从整体上查看所有设备信息，更有效地调查整个数据源产品组合中的设备。

激活后，设备洞察已准备好从与XDR集成的模块中自动提取资产和设备数据。因此，如果您已有与XDR集成的模块，则无需删除或重新添加这些模块即可实现此功能。

如果您想了解有关配置的更多信息，请查看Cisco XDR配置模块了解详细信息。

故障排除

本部分提供的信息可用于对配置进行故障排除。

添加安全终端模块

- 启用模块的用户需要具有管理员权限才能集成产品。

注意：如果集成了新源，则需要在看到报告到资产的任何设备之前手动同步或等待自动同步。

检验连通性

为了允许API连接，请确保您的环境中允许下一个FQDN。

- api.amp.cisco.com
- api.apjc.amp.cisco.com
- api.eu.am p.cisco.com

用户Postman以测试连通性

https://<AMP API区域FQDN>/v1/computers

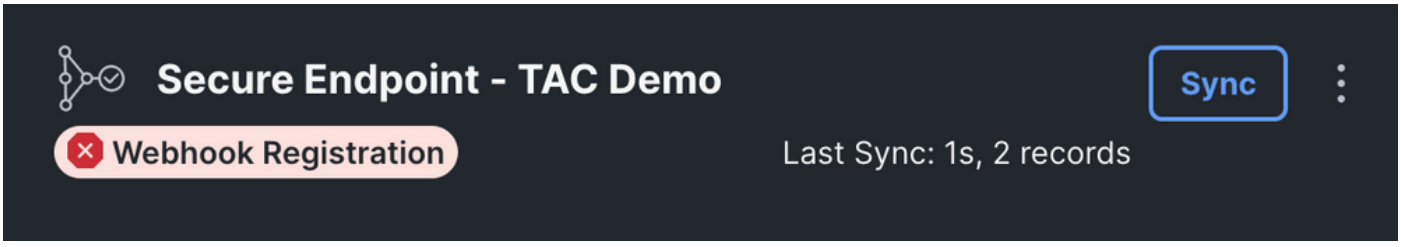
https://< AMP API regional FQDN>/v1/computers/<连接器GUID>

注意：安全终端使用基本身份验证作为授权方法。

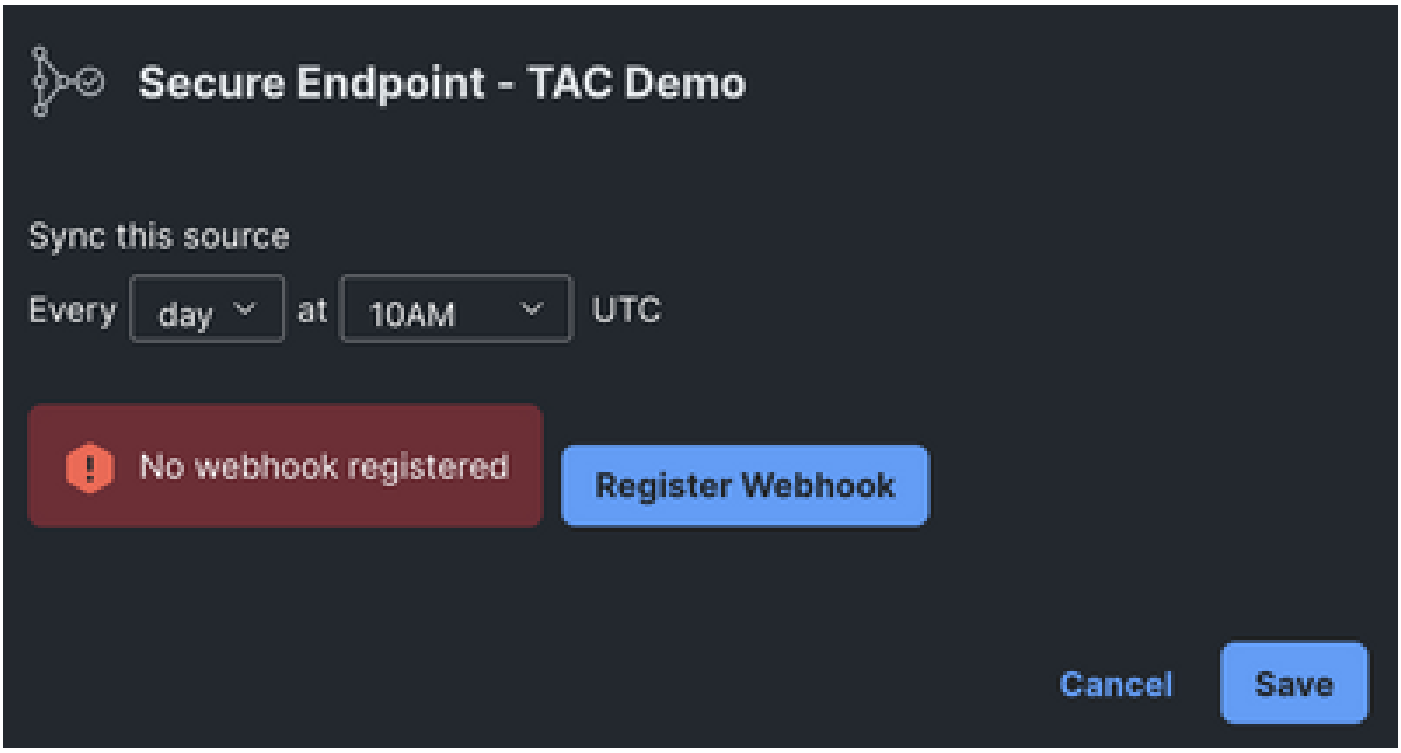
设备编号不匹配

- Device Insights存储最近90天的信息，但是，安全终端会存储30天的信息。如果在设备数量上发现不匹配，请验证最后一次发现的涉及的计算机不超过90天。
- 验证安全终端控制台没有导致两个控制台上不匹配的重复连接器。

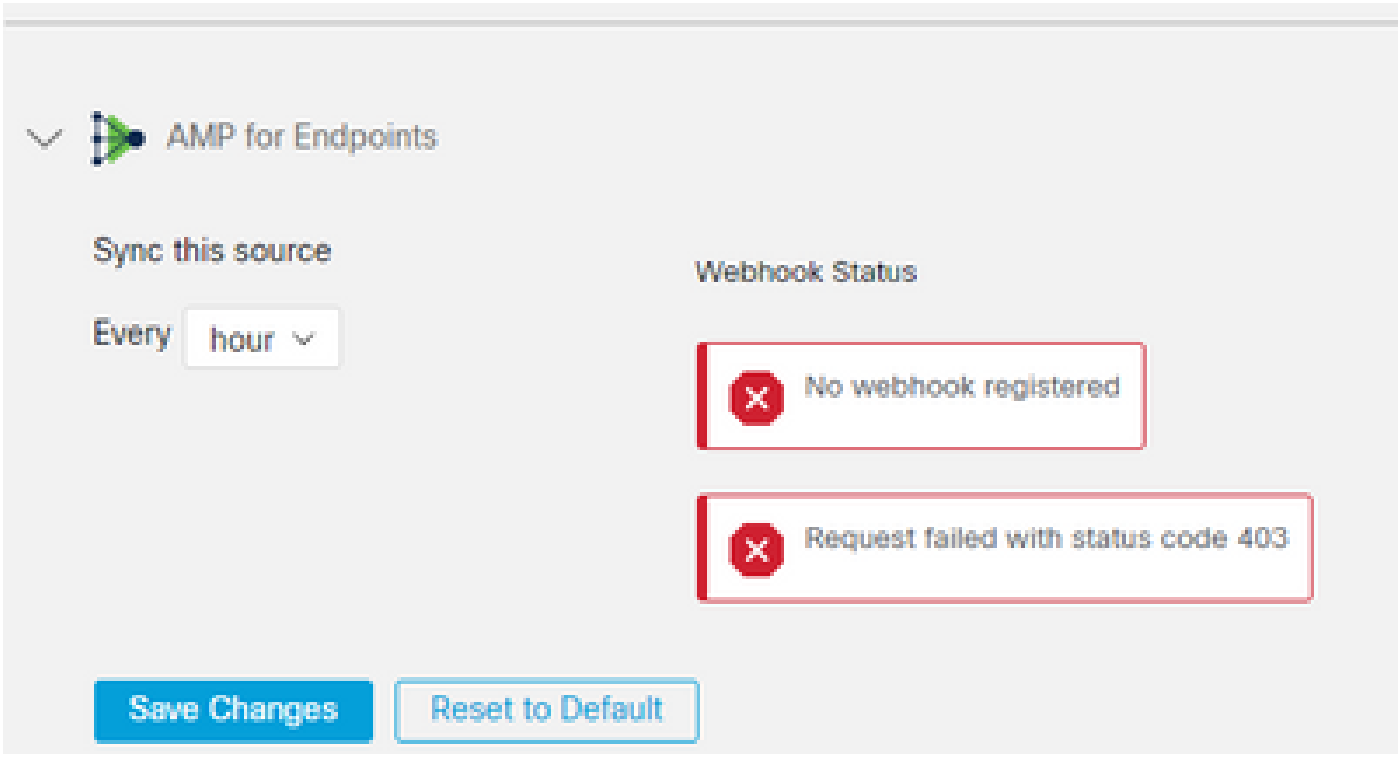
场景 1.无Webhook注册



导航到Source Setting（源设置），然后点击Register Webhook（注册Webhook）按钮，执行请求后，Webhook状态将显示如图所示。



场景 2：HTTP错误。



400 — 请求错误

401 — 未授权

403 — 禁止的

404 — 不允许使用方法

对于HTTP错误，请查看配置的API凭证，并确保收集的信息与粘贴在XDR上的模块配置上的信息匹配。

浏览器问题

当Device Insights中显示错误数据时，请在不同的浏览器或专用窗口中进行测试，以丢弃错误或过时的浏览器缓存。

多组织问题

安全终端集成模块使用Enable按钮。因此，安全终端现在只能链接到一个安全终端控制台，但如果您是这些组织的管理员，则仍可以在一个XDR下链接多个安全终端模块。换句话说，如果您是多个安全终端组织中的管理员，您可以让所有管理员通过一个XDR控制面板下的API模块进行链接。确认安全终端控制台尚未集成到另一个XDR组织，

XDR门户可以集成多个安全终端实例，但安全终端只能集成到一个XDR实例中。

HAR日志

如果设备见解和安全终端集成问题仍然存在，请参阅从XDR控制台收集HAR日志，了解如何从浏览器收集HAR日志，并联系TAC支持以执行更深入的分析。

相关信息

- XDR登录（文档）
- 技术支持和文档 - Cisco Systems

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）。

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）。