排除XDR和安全邮件设备（以前称为ESA）集成故障

目录

简介

本文档介绍执行基本分析的步骤以及如何对XDR和见解以及安全邮件设备集成模块进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- XDR
- 安全服务交换
- 安全电子邮件

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全服务交换
- XDR
- 软件版本13.0.0-392上的安全电子邮件C100V

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

思科安全邮件设备（以前称为邮件安全设备）提供高级威胁防护功能，通过端到端加密来更快地检测、阻止和修复威胁，防止数据丢失，并保护传输中的重要信息。配置完成后，安全邮件设备模块将提供与可观察项相关的详细信息。您可以：

- 查看邮件报告和邮件跟踪来自您组织中的多个设备的数据
- 识别、调查并修复在邮件报告和邮件跟踪中观察到的威胁
- 快速解决已确定的威胁，并针对已确定的威胁提供建议措施
- 记录威胁以保存调查，并在其他设备之间实现信息协作

集成安全邮件设备模块需要使用安全服务交换(SSE)。SSE允许安全邮件设备向Exchange注册，并且您提供访问已注册设备的明确权限。

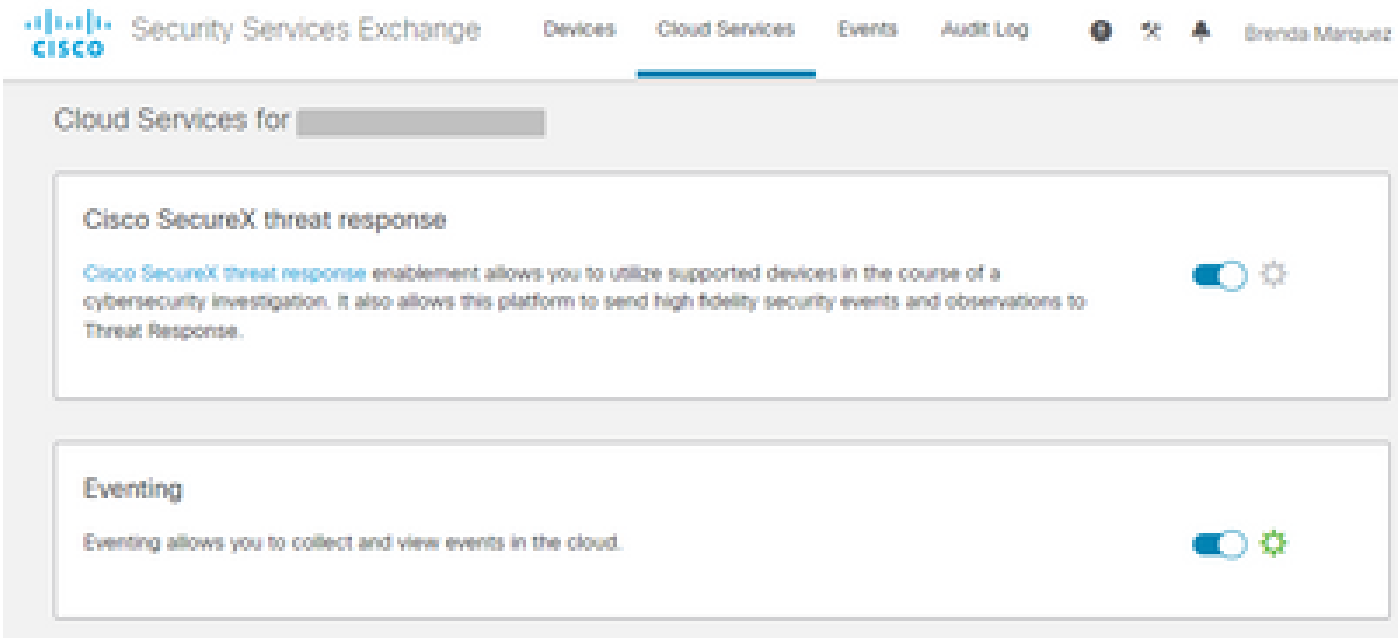
如果您想了解有关配置的更多信息，请查看，此文章介绍集成模块详情。

故障排除

为了排除XDR和安全邮件设备集成的常见问题，您可以验证这些步骤。

XDR和安全服务交换门户中未显示安全电子邮件设备

如果您的设备未显示在SSE门户中，请确保已在SSE门户中启用XDR威胁响应和事件服务，导航到云服务，然后启用服务，如下图所示：

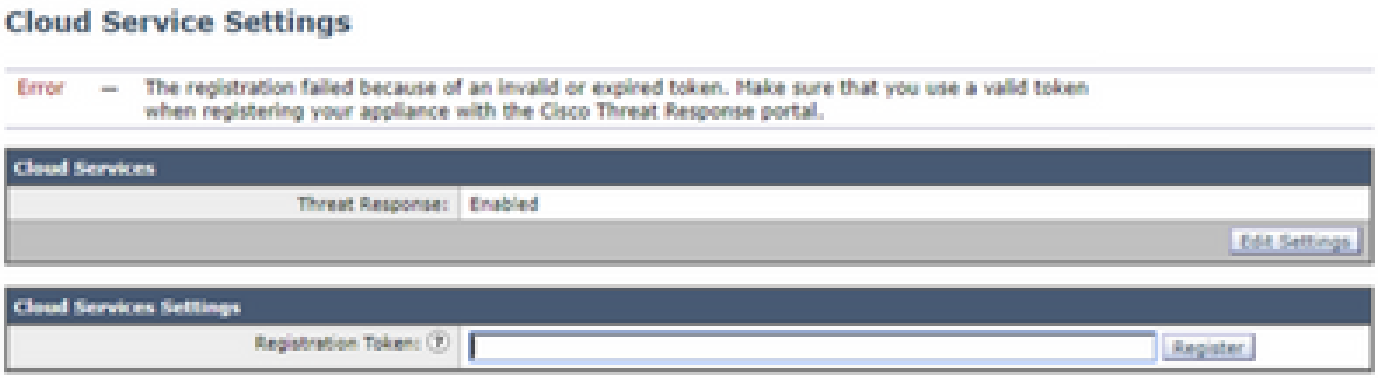


安全电子邮件不请求注册令牌

启用思科XDR/威胁响应服务后，请确保提交更改，否则，更改将不会应用于安全邮件中的“云服务”部分，请参阅下图。

注册失败，因为令牌无效或过期

如果看到错误消息："注册因无效或过期的令牌而失败。确保与安全邮件GUI中的Cisco XDR威胁响应门户""一起使用适用于您的设备的有效令牌，如下图所示：



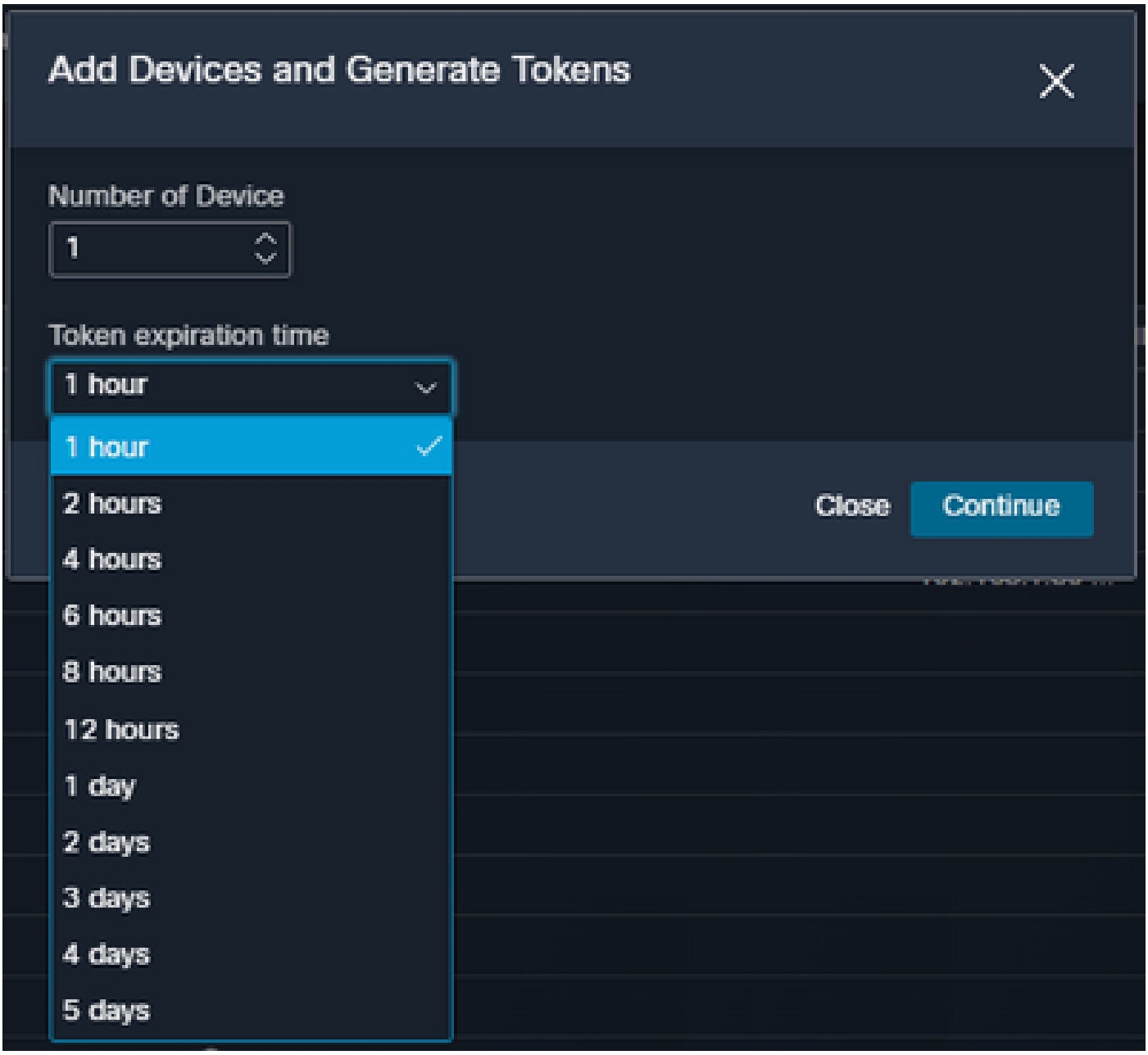
请确保从正确的云生成令牌：

如果您使用欧洲（欧盟）云安全邮件，请从https://admin.eu.sse.itd.cisco.com/生成令牌

如果使用美洲(NAM)云进行安全邮件，请从https://admin.sse.itd.cisco.com/生成令牌

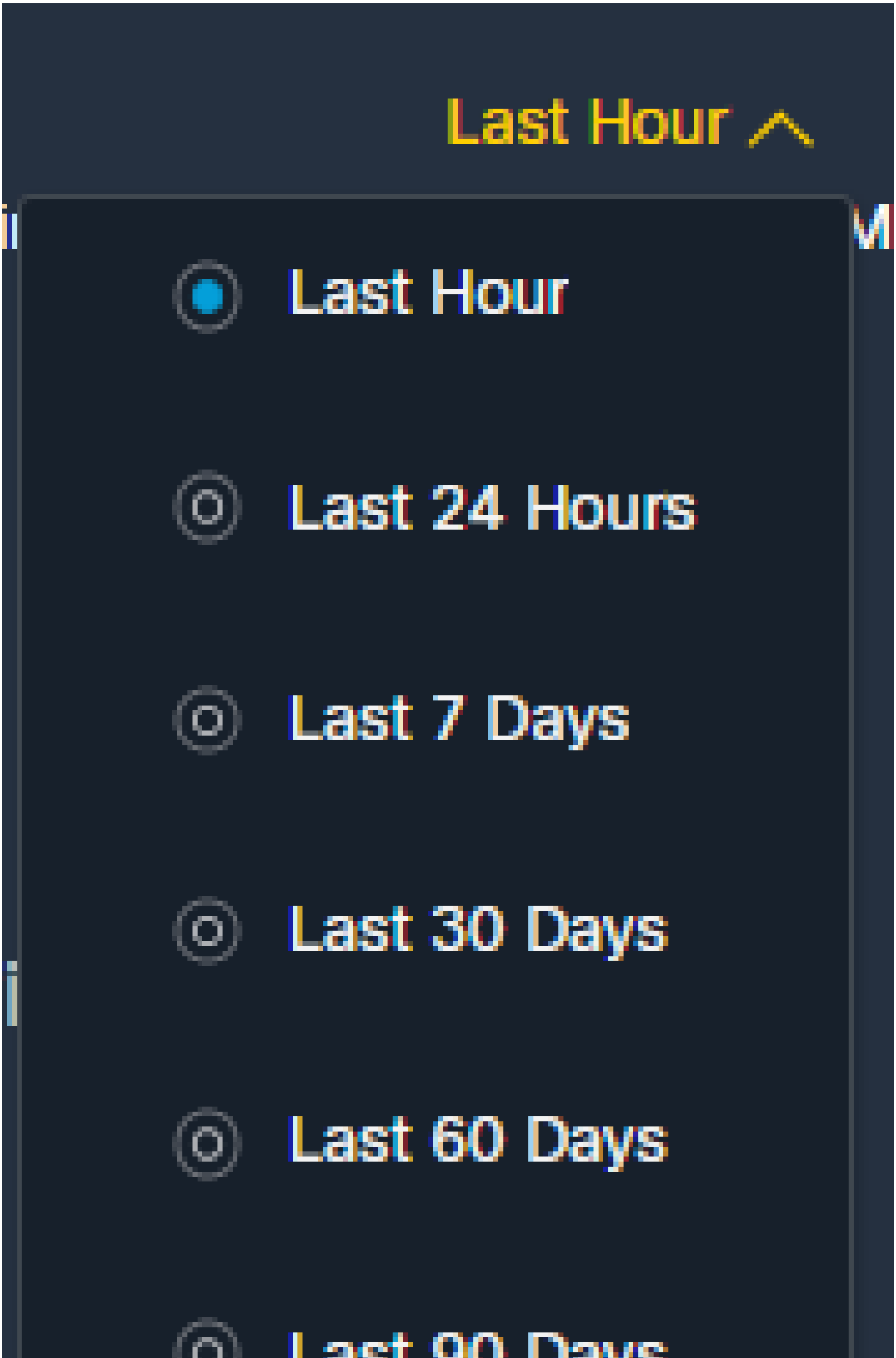
安全服务交换(SSE)门户：	NAM:https://admin.sse.itd.cisco.com/ 欧盟：https://admin.eu.sse.itd.cisco.com/
Cisco XDR门户	NAM:https://XDR.us.security.cisco.com/ 欧盟：https://XDR.eu.security.cisco.com/
安全邮件Cisco XDR/威胁响应服务器：	NAM:api-sse.cisco.com 欧盟：api.eu.sse.itd.cisco.com

此外，请记住，注册令牌有一个到期时间（选择最方便的时间及时完成集成），如图所示。



XDR控制面板不显示有关安全邮件模块的信息

您可以在可用磁贴中选择较宽的时间范围，从Last Hour到Last 90 Days，如下图所示。


Last Hour
Last Hour
Last 24 Hours
Last 7 Days
Last 30 Days
Last 60 Days

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）。