排除XDR和安全電子郵件裝置（以前稱為ESA）整合故障

目錄

簡介

本文檔介紹執行基本分析的步驟以及如何對XDR和見解以及安全電子郵件裝置整合模組進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- XDR
- 安全服務交換
- 安全電子郵件

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 安全服務交換
- XDR
- 軟體版本13.0.0-392上的安全電子郵件C100V

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

思科安全郵件裝置（前身為郵件安全裝置）提供高級威脅防護功能，可更快地檢測、阻止和修復威脅，防止資料丟失，並通過端到端加密保護傳輸中的重要資訊。配置完成後，安全郵件裝置模組將提供與可觀察內容相關的詳細資訊。您可以：

- 檢視電子郵件報告和郵件跟蹤來自您組織中的多個裝置的資料
- 識別、調查和補救電子郵件報告和郵件跟蹤中觀察到的威脅
- 快速解決已確定的威脅，並針對已確定的威脅提供建議措施
- 記錄威脅以儲存調查，並在其他裝置之間啟用資訊合作

整合安全電子郵件裝置模組需要使用安全服務交換(SSE)。SSE允許安全電子郵件裝置在Exchange中註冊，並且您提供了訪問已註冊裝置的明確許可權。

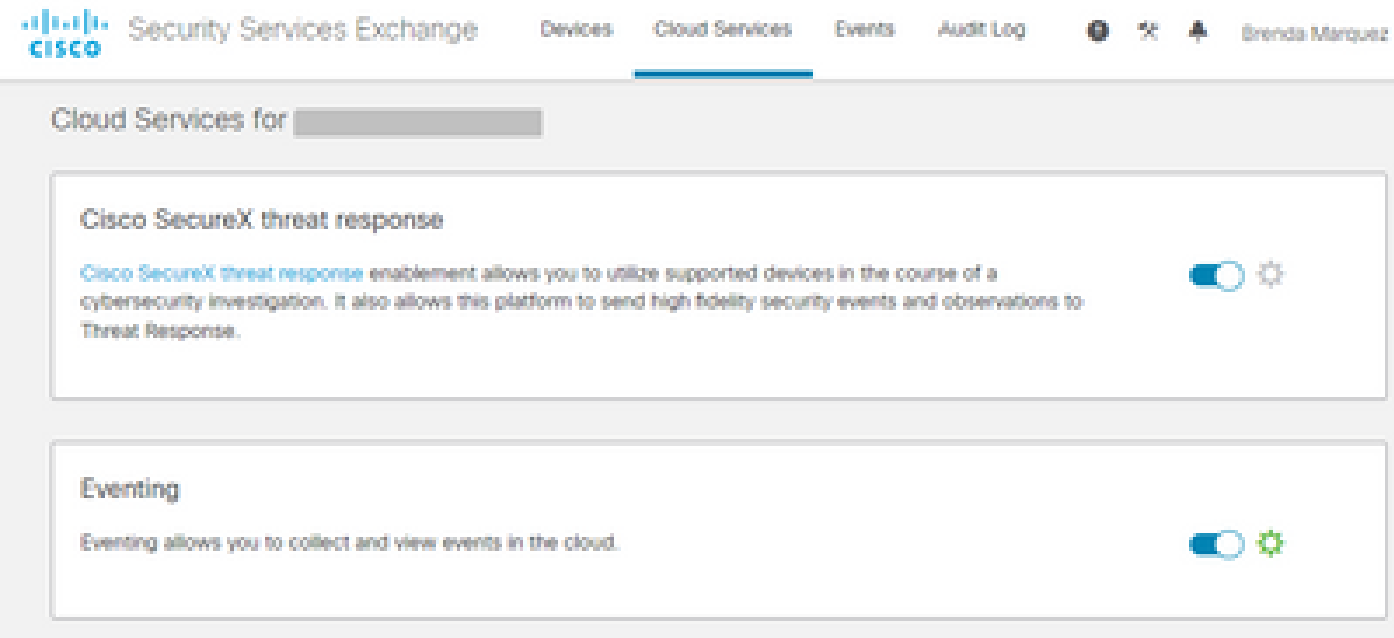
如果您想瞭解有關配置的更多資訊，請檢視，本文在此處提供整合模組詳情。

疑難排解

為了解決XDR和安全電子郵件裝置整合的常見問題，您可以驗證這些步驟。

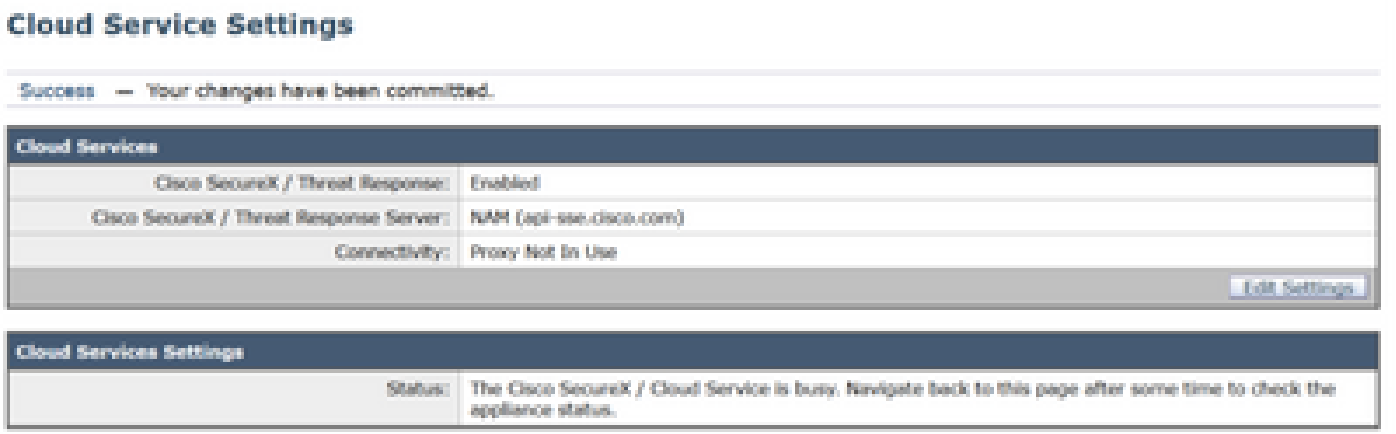
XDR或安全服務交換門戶中未顯示安全電子郵件裝置

如果您的裝置未顯示在SSE門戶中，請確保已在SSE門戶中啟用XDR威脅響應和事件服務，導航到Cloud Services，然後啟用這些服務，如下圖所示：



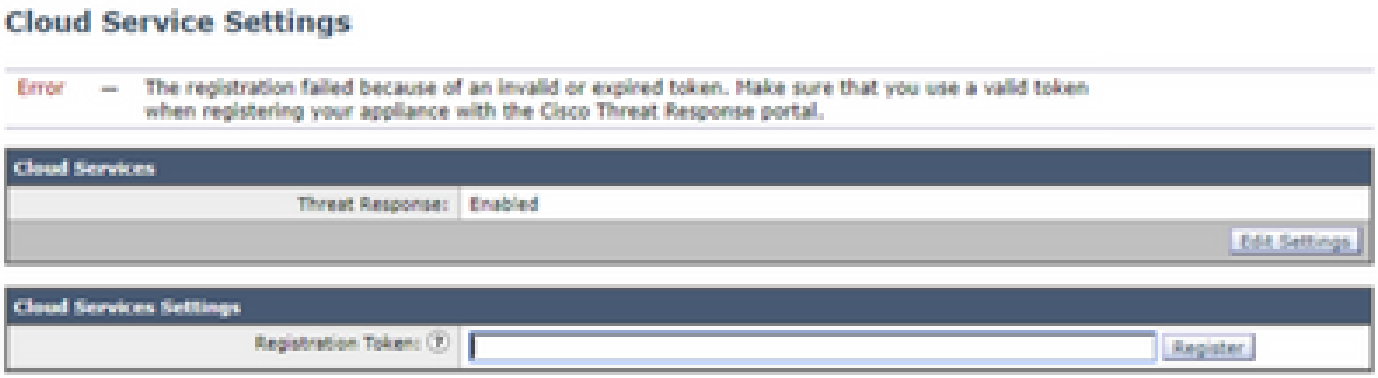
安全電子郵件不請求註冊令牌

請確保在啟用思科XDR/威脅響應服務後提交更改，否則這些更改將不會應用於安全郵件中的「雲服務」部分，請參閱下圖。



註冊失敗，因為令牌無效或已過期

如果您看到錯誤消息：「由於令牌無效或過期，註冊失敗。確保在安全電子郵件GUI中的Cisco XDR威脅響應門戶「」中，為裝置使用有效令牌，如下圖所示：



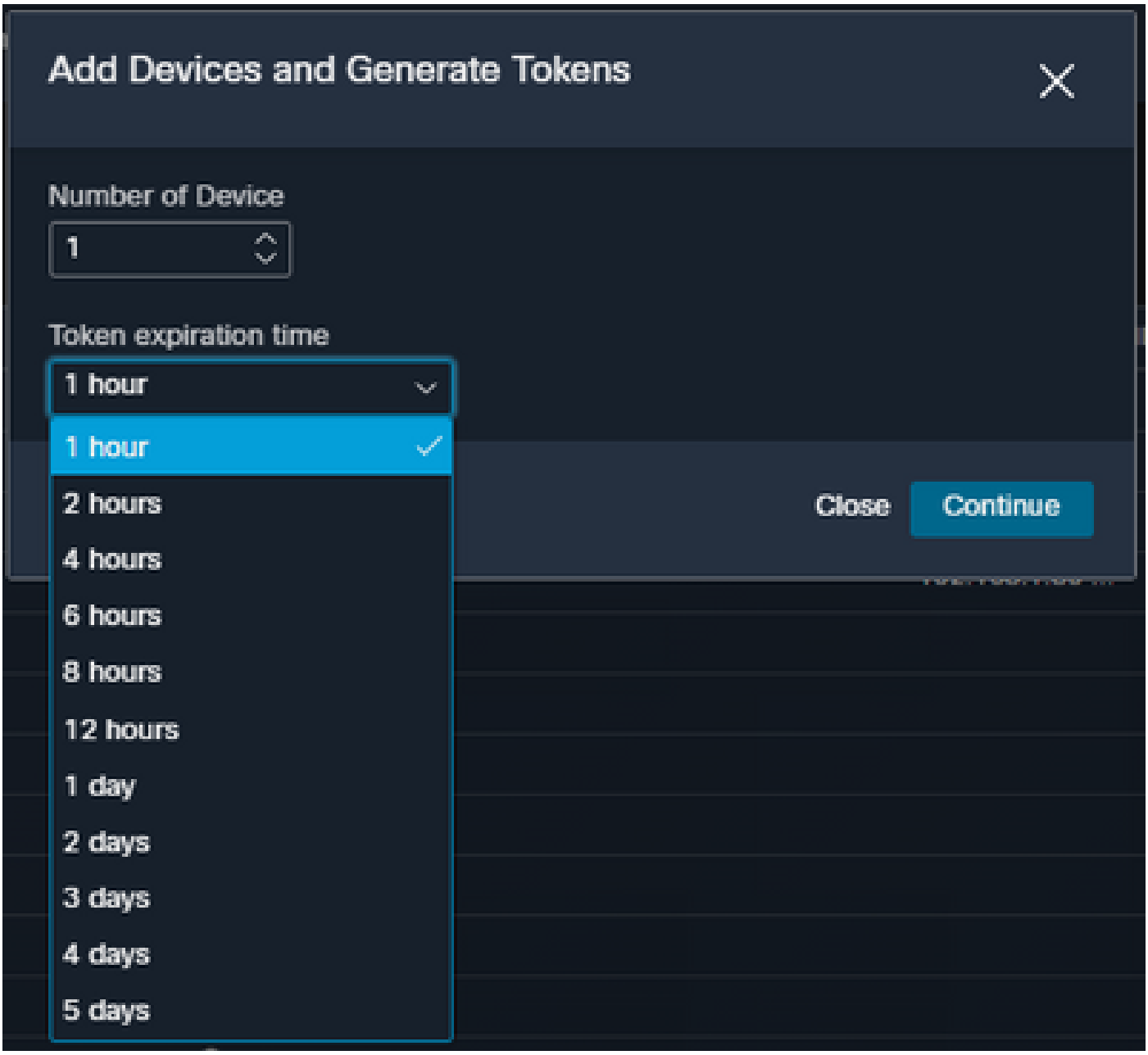
請確保從正確的雲生成令牌：

如果使用歐洲(EU)雲用於安全電子郵件，請從https://admin.eu.sse.itd.cisco.com/生成令牌

如果使用美洲(NAM)雲用於安全電子郵件，請從https://admin.sse.itd.cisco.com/生成令牌

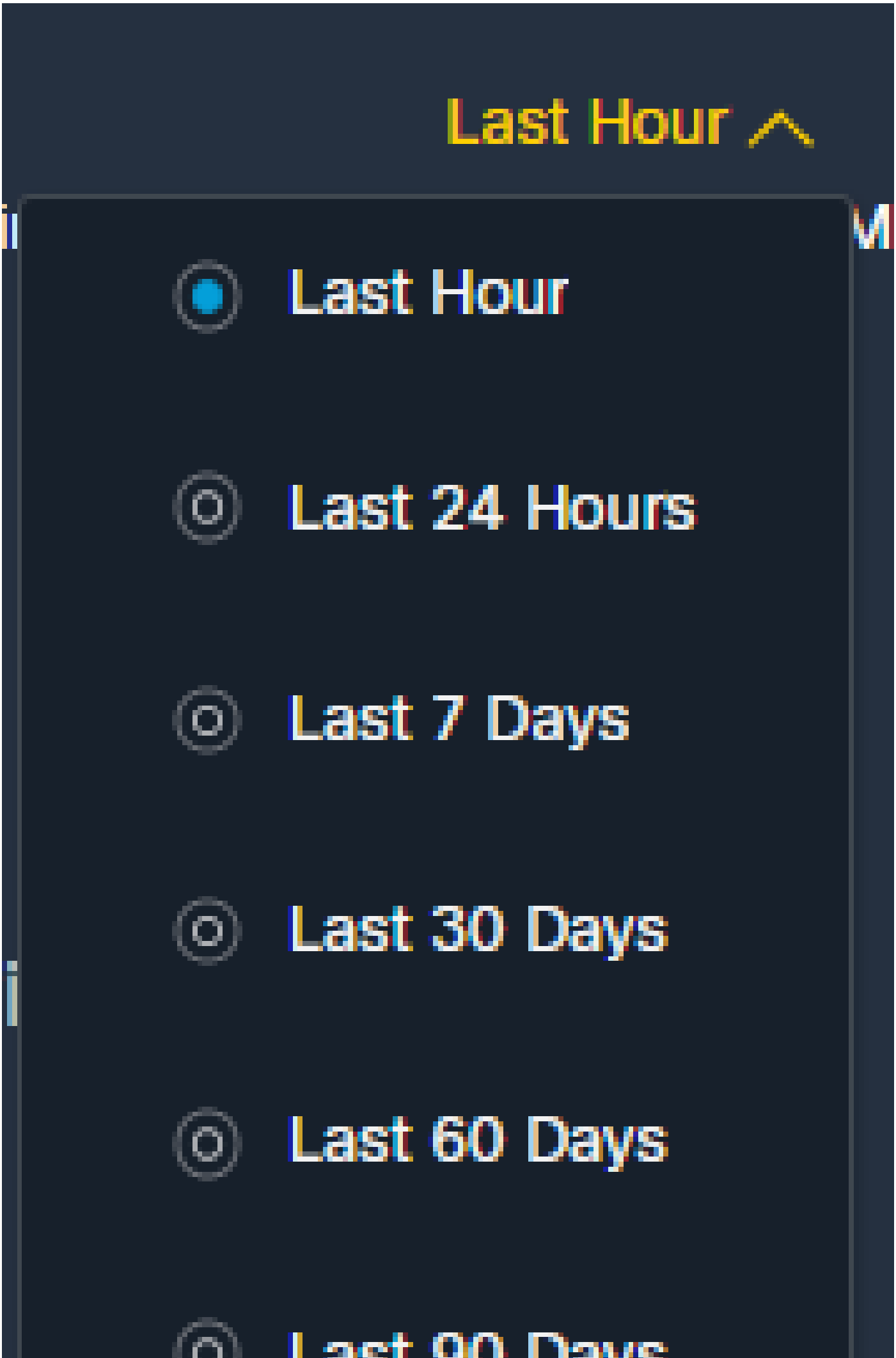
安全服務交換(SSE)門戶：	NAM:https://admin.sse.itd.cisco.com/ 歐盟：https://admin.eu.sse.itd.cisco.com/
Cisco XDR門戶	NAM:https://XDR.us.security.cisco.com/ 歐盟：https://XDR.eu.security.cisco.com/
安全電子郵件Cisco XDR/威脅響應伺服器：	NAM:api-sse.cisco.com 歐盟：api.eu.sse.itd.cisco.com

此外，請記住，註冊令牌有到期時間（選擇最方便的時間及時完成整合），如下圖所示。



XDR控制面板不顯示有關安全電子郵件模組的資訊

您可以在可用磁貼中選擇較寬的時間範圍，如下圖所示，從Last Hour到Last 90 Days。


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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。