在FMC GUI上使用統一事件檢視器監控事件

目錄

簡介

本文檔介紹如何在防火牆管理中心(FMC)的圖形使用者介面(GUI)上使用統一事件檢視器。

必要條件

需求

思科建議您瞭解以下主題：

- 使用管理員或安全分析師許可權訪問FMC
- FMC的版本等於或高於v7.0

採用元件

本文中的資訊係根據以下軟體和硬體版本：

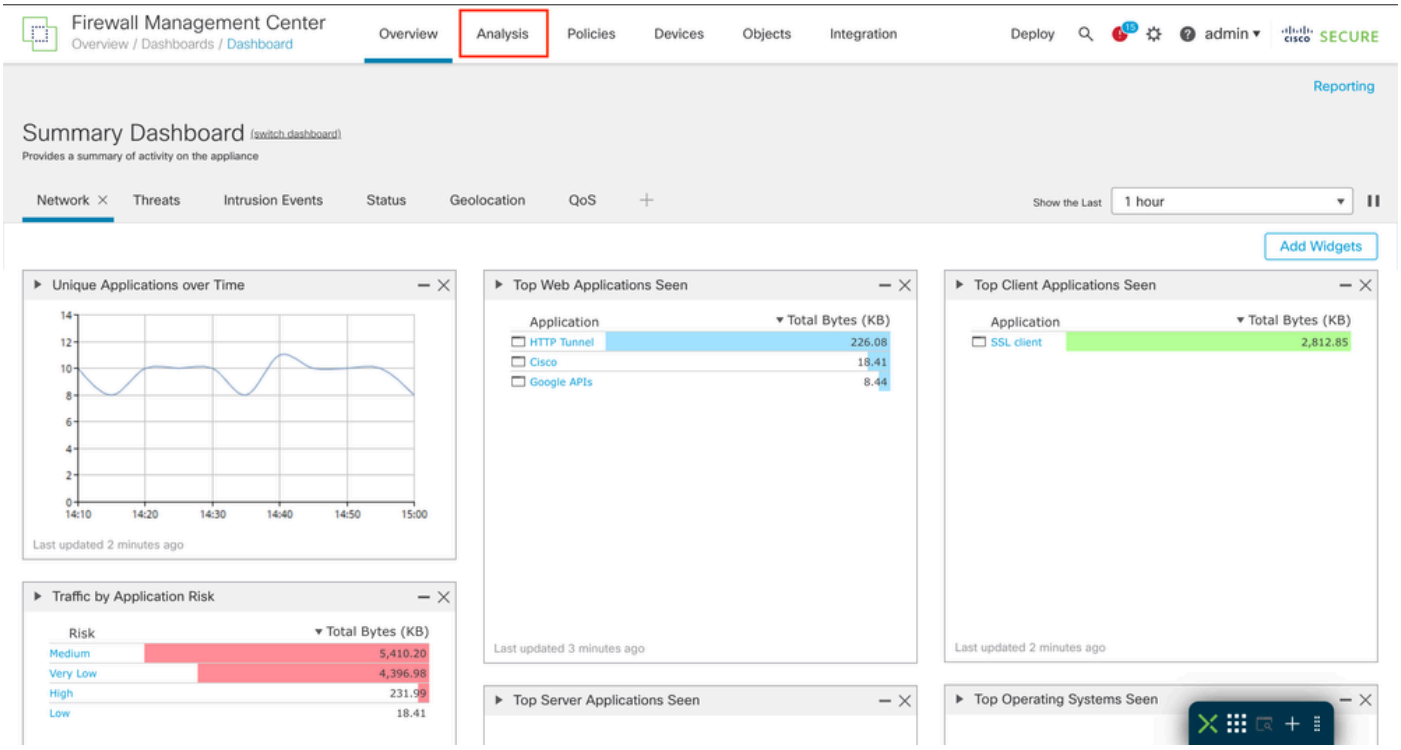
- 適用於VMware v7.2.5的安全防火牆管理中心

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。

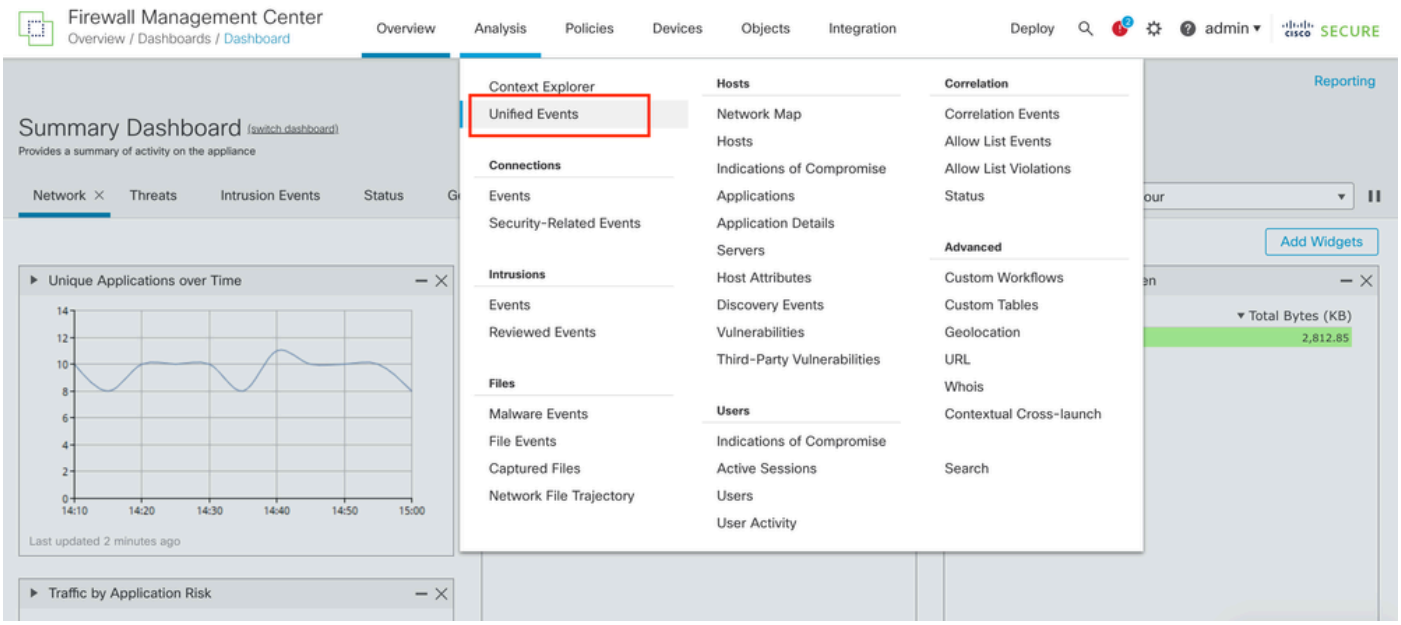
探索

步驟1.登入FMC GUI。

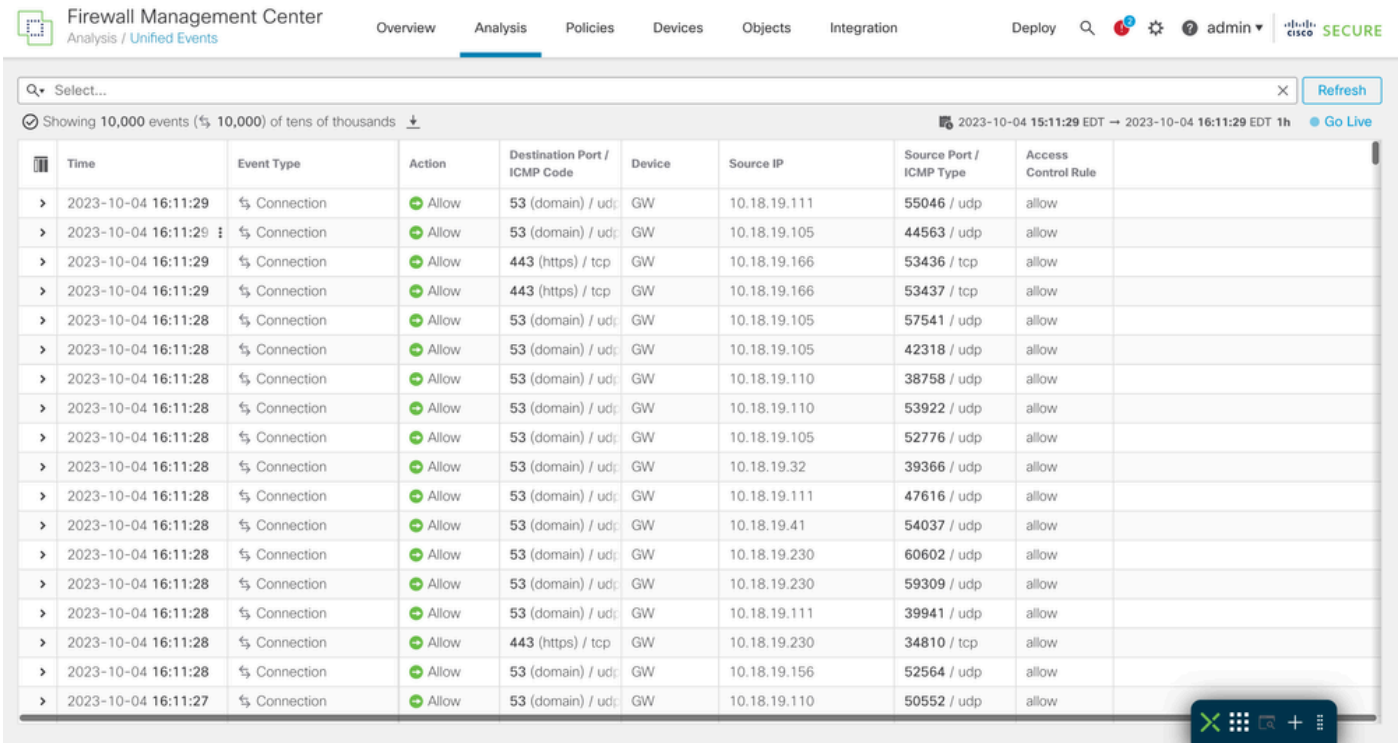
步驟2.定位至Analysis標籤。



步驟3.從下拉選單中，按一下Unified Events。

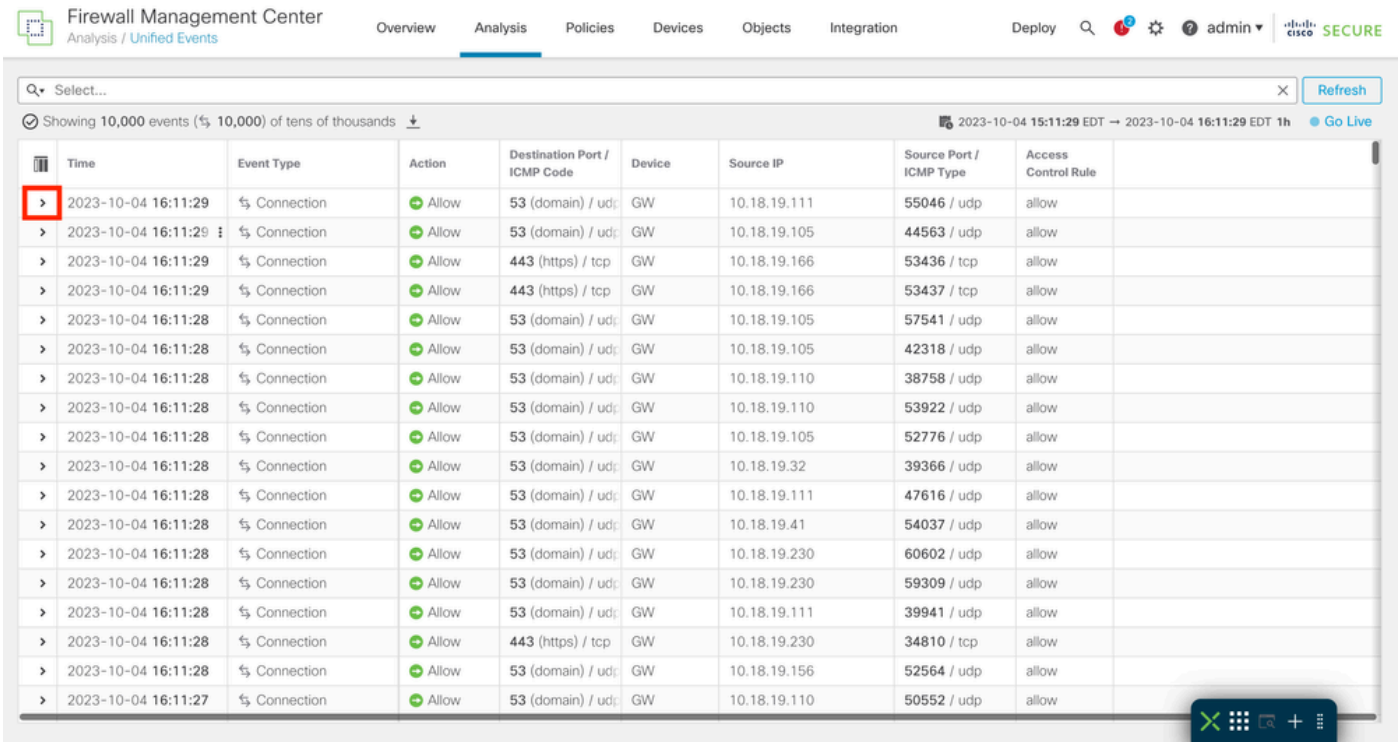


統一事件頁面示例

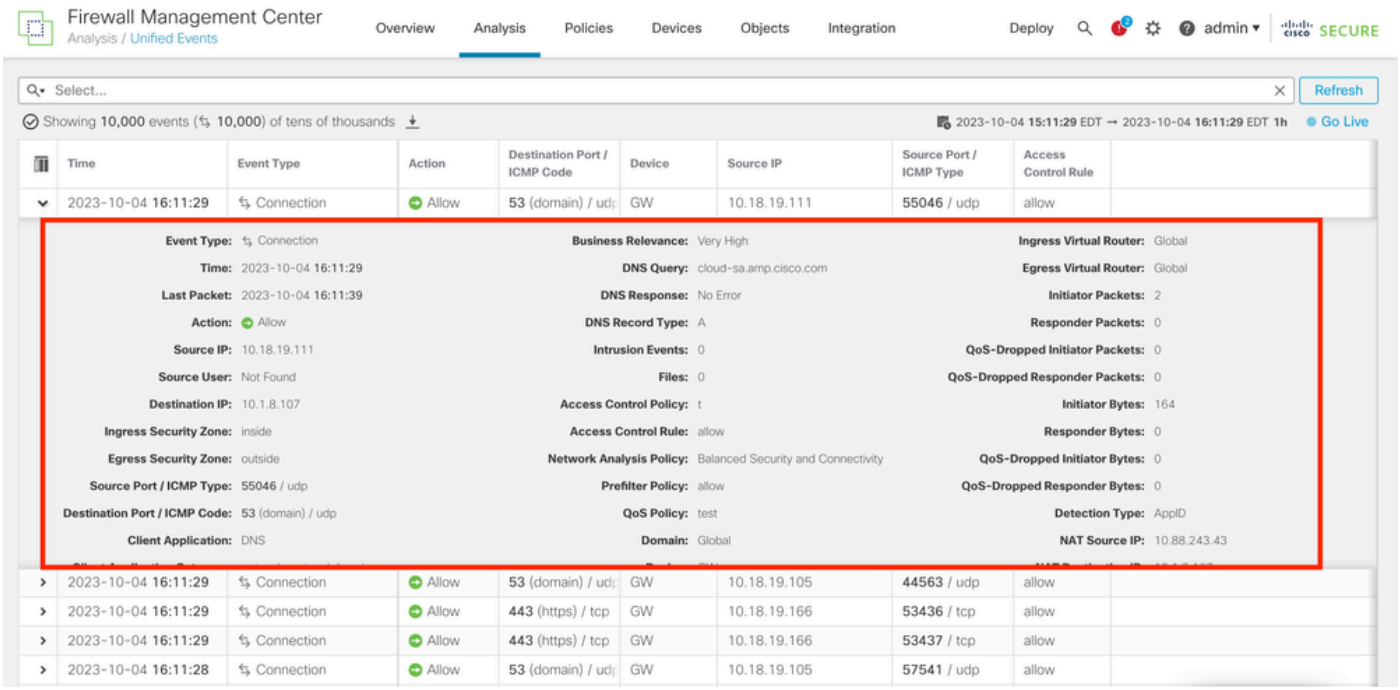


審閱事件

步驟1。按一下> 圖示。

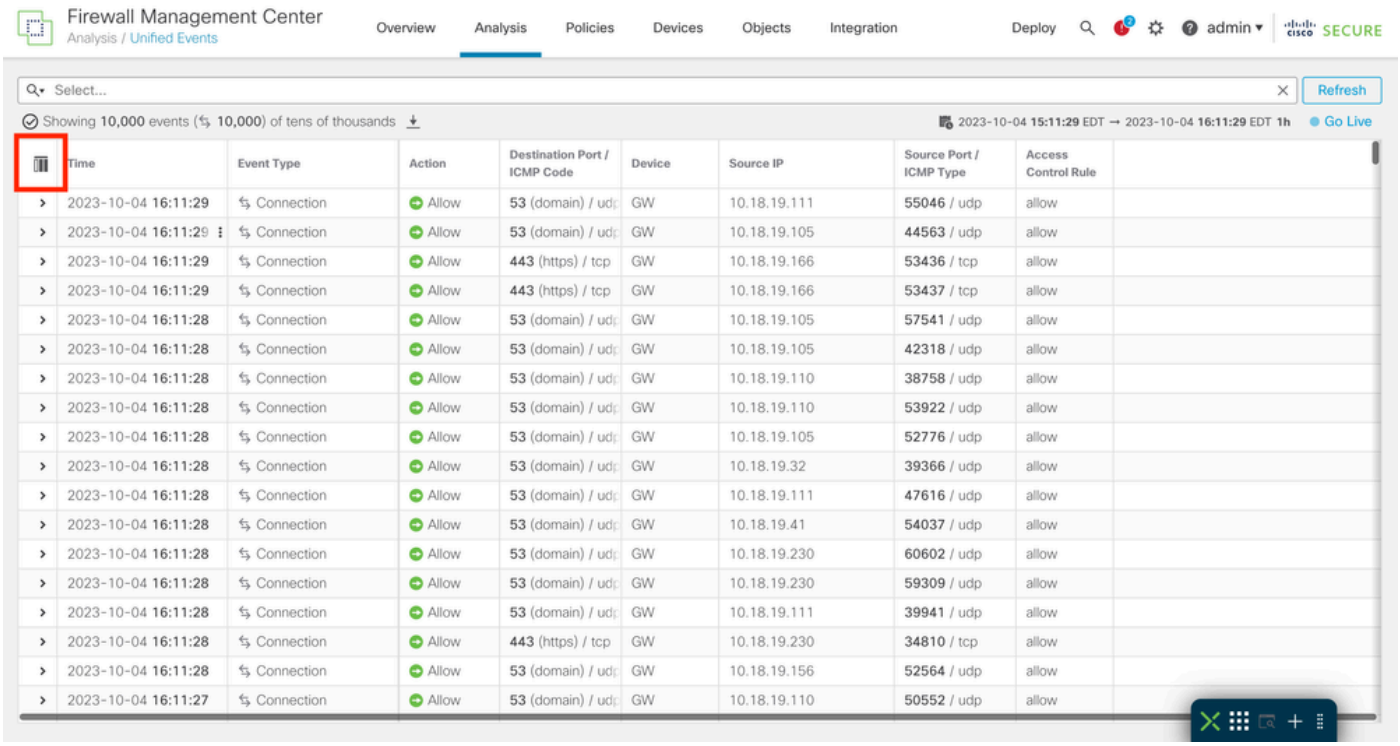


步驟2.顯示事件的詳細資訊。

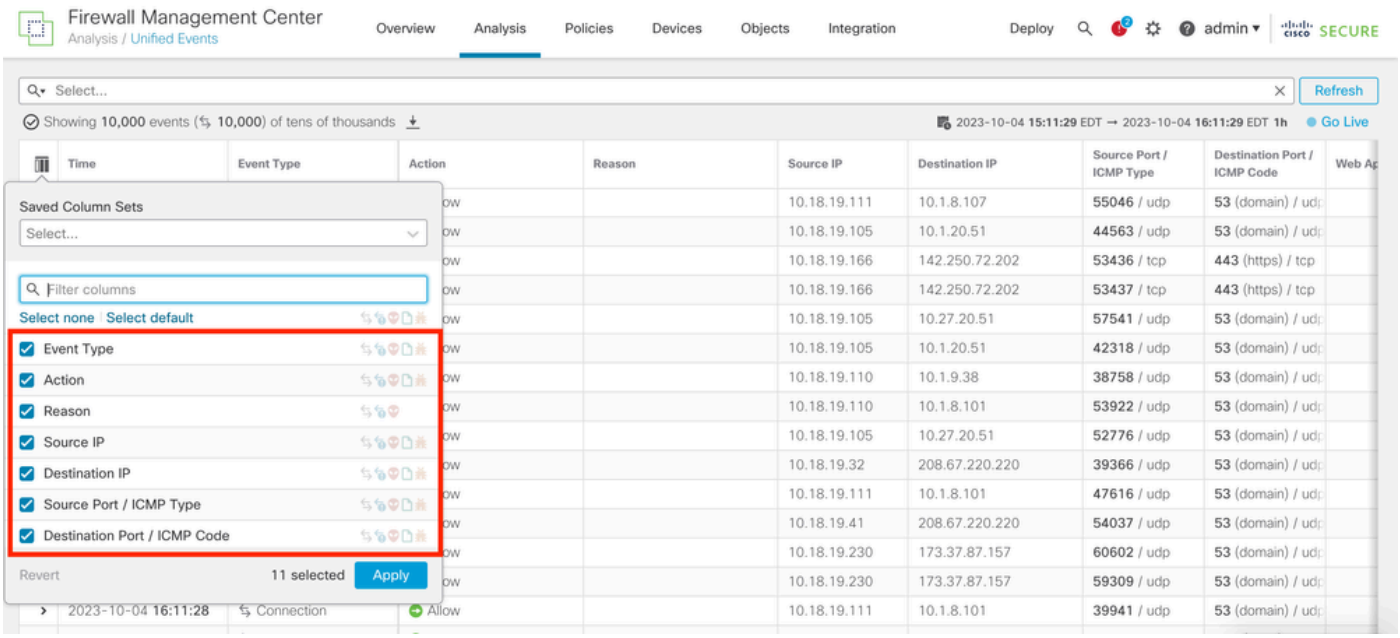


個人化列

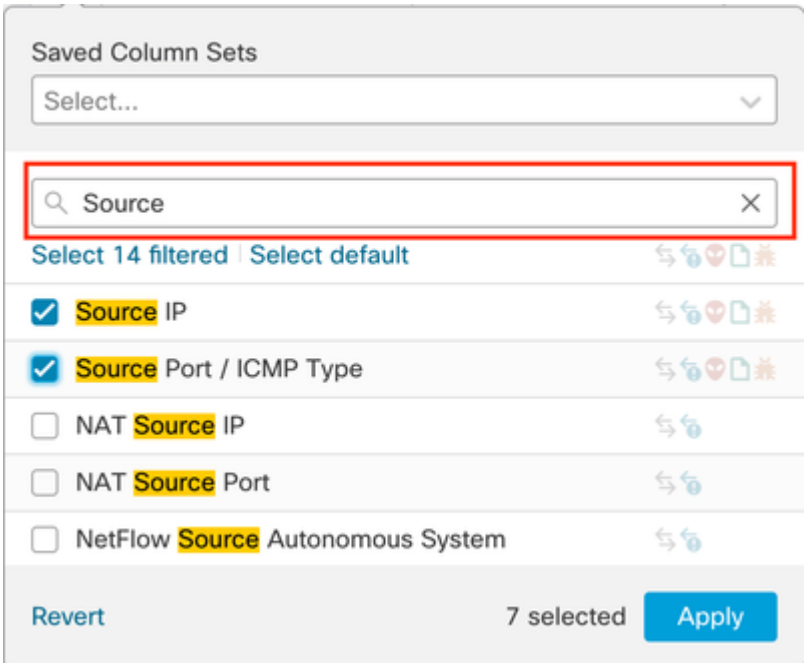
步驟1.按一下圖示  .



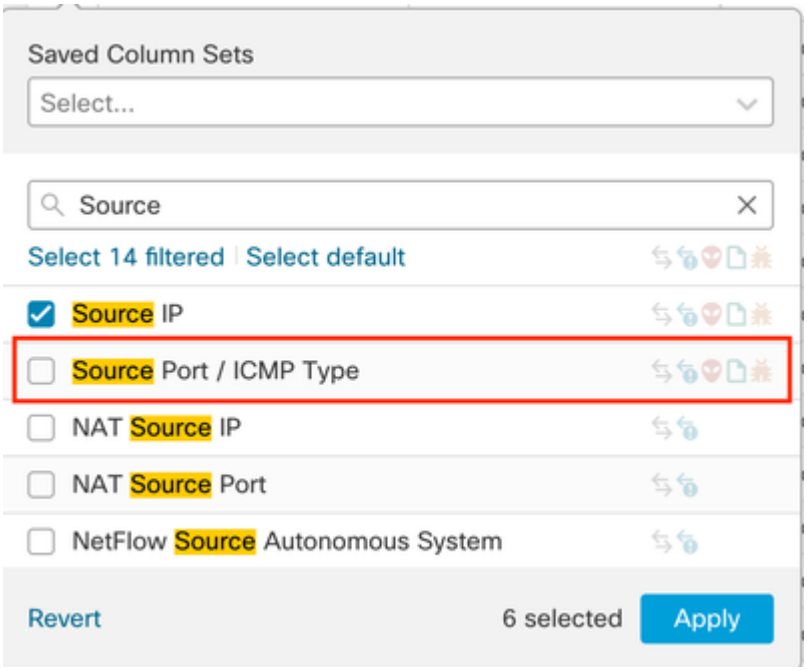
步驟2.選擇您要在表上的事件欄位。



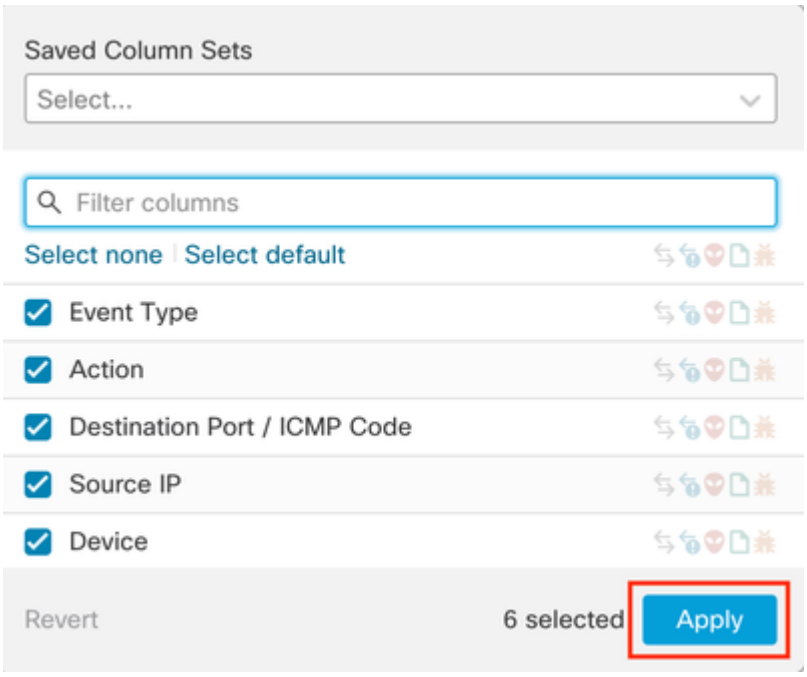
步驟3.（可選）搜尋欄位以簡化導覽。



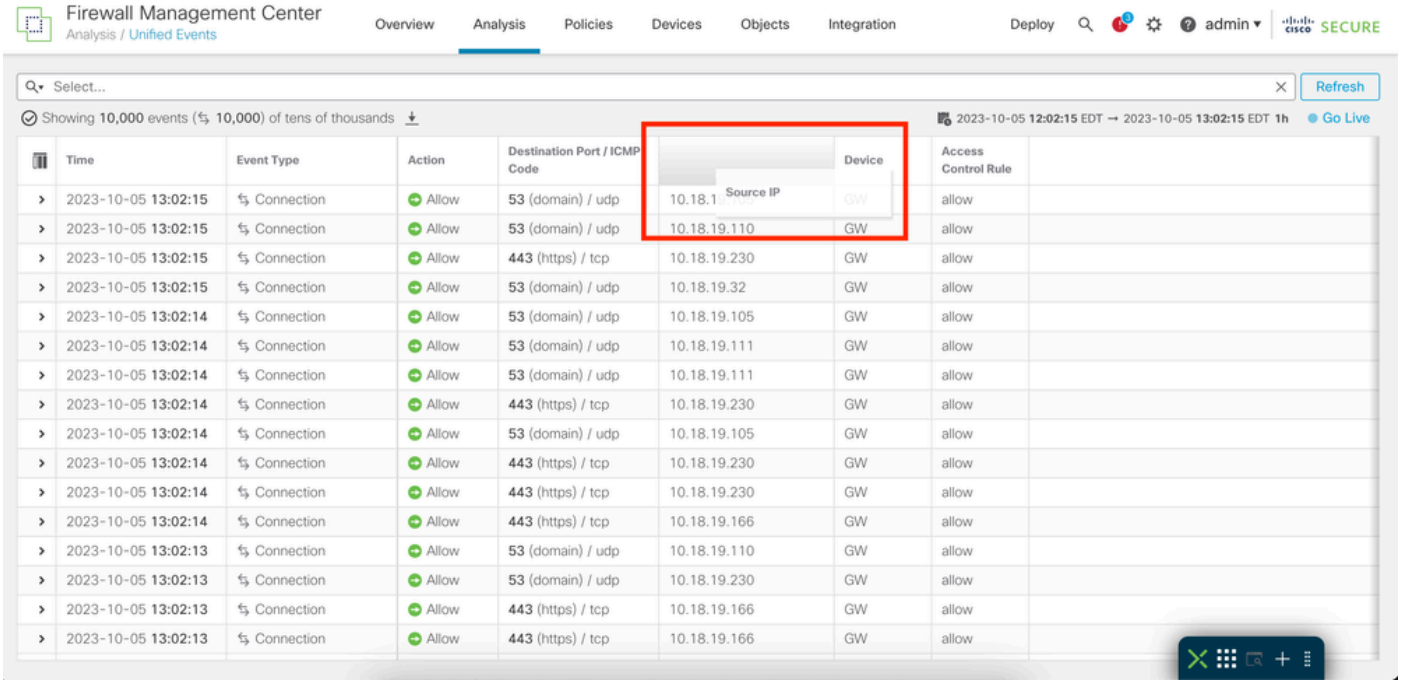
步驟4.按一下事件欄位以禁用或啟用。



步驟5.按一下Apply。

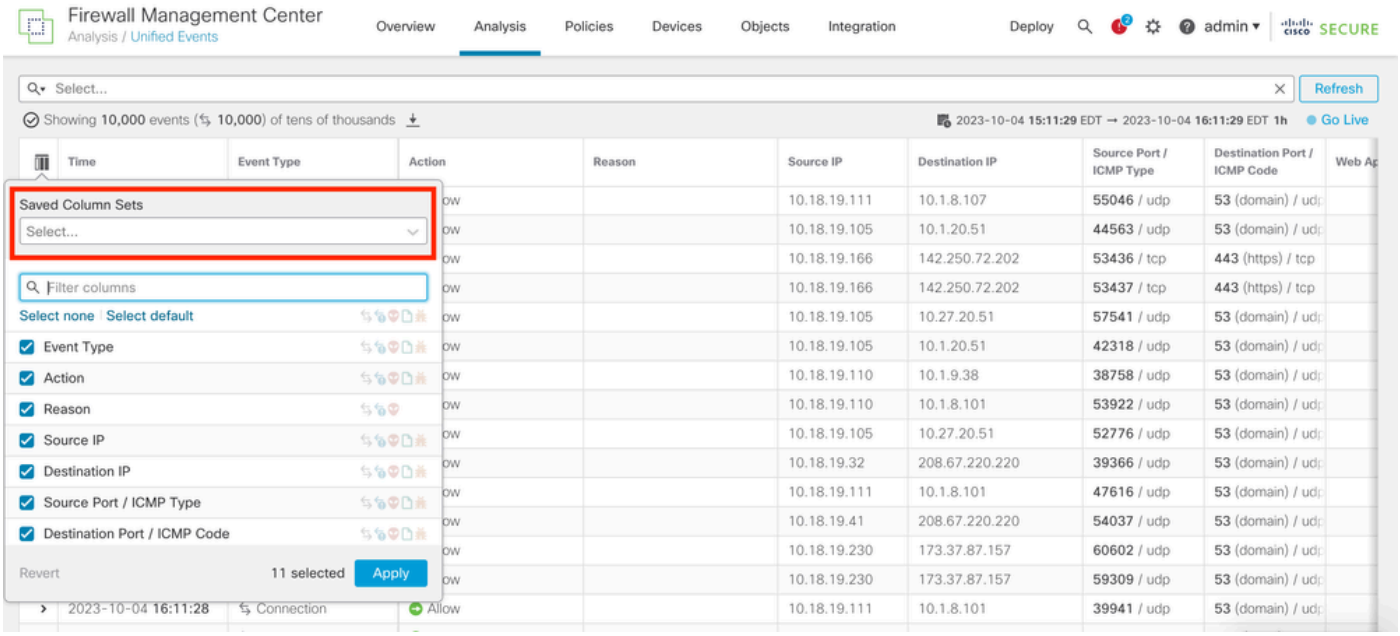


步驟6.（可選）您可以將每個列拖動到不同的位置，以重新定位列。

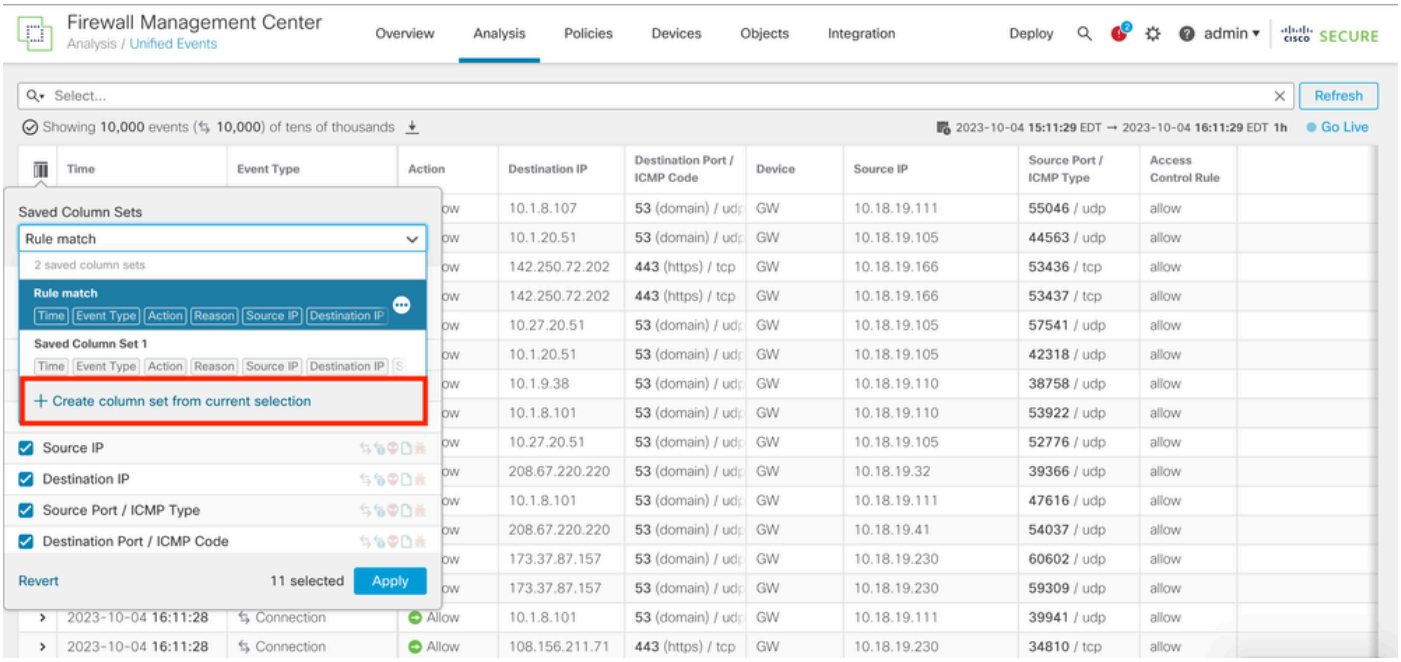


儲存列集

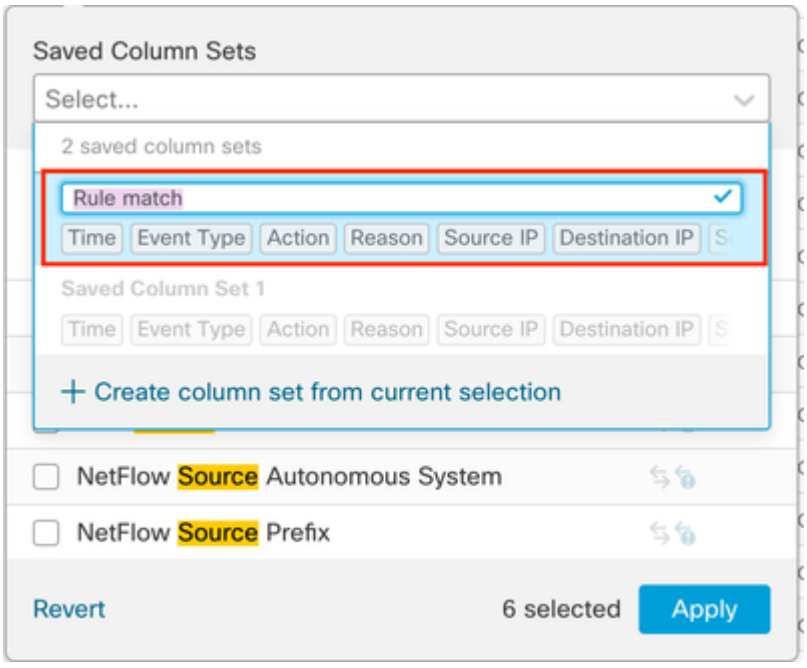
步驟1.按一下Saved Column Sets。



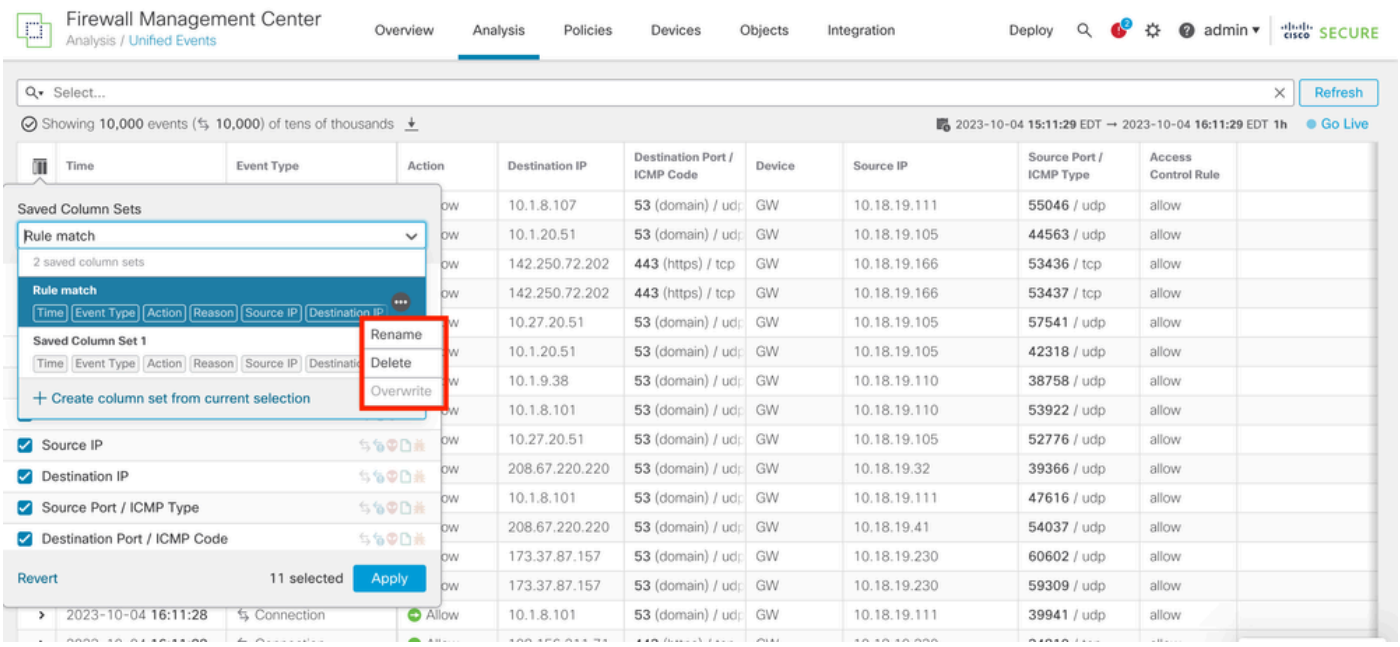
步驟2.按一下Create column set from current selection。



步驟3.（可選）更改列集的名稱。

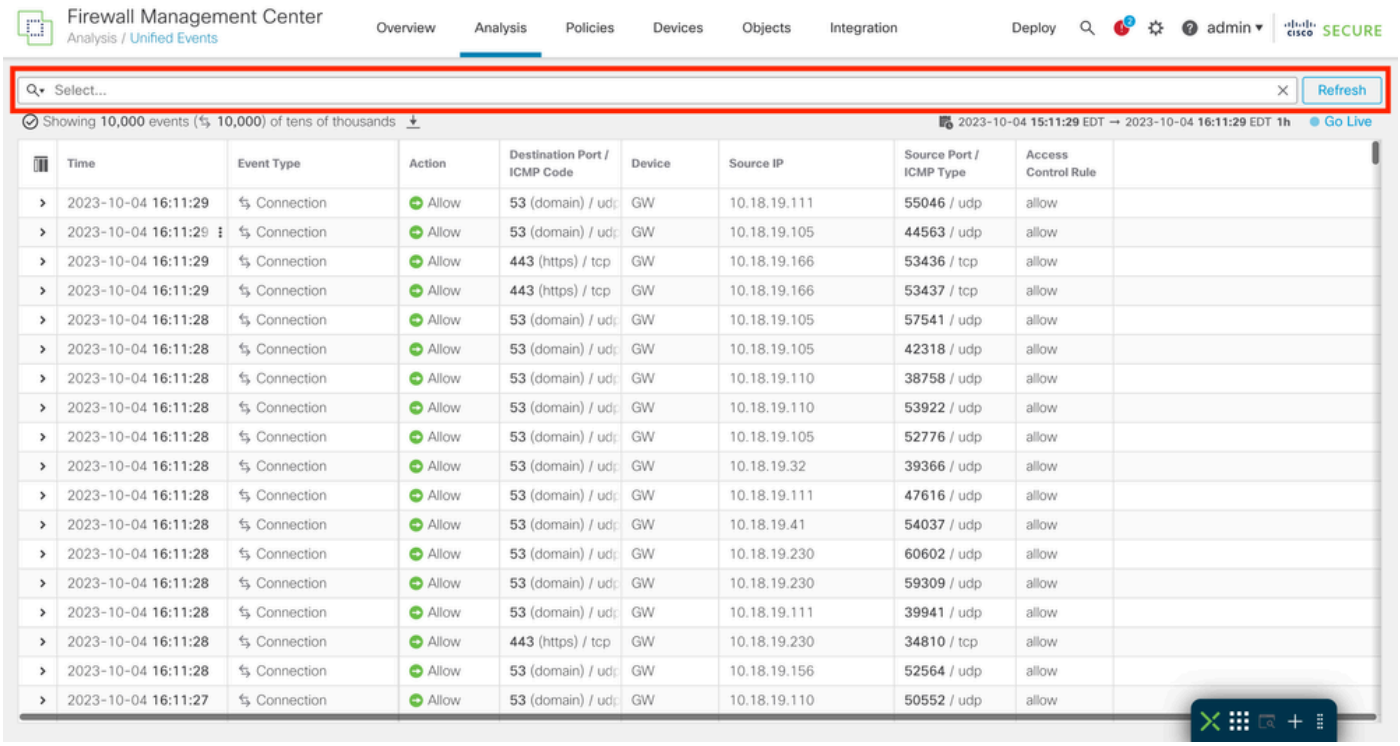


步驟4.按一下省略號(...)可以編輯現有集。

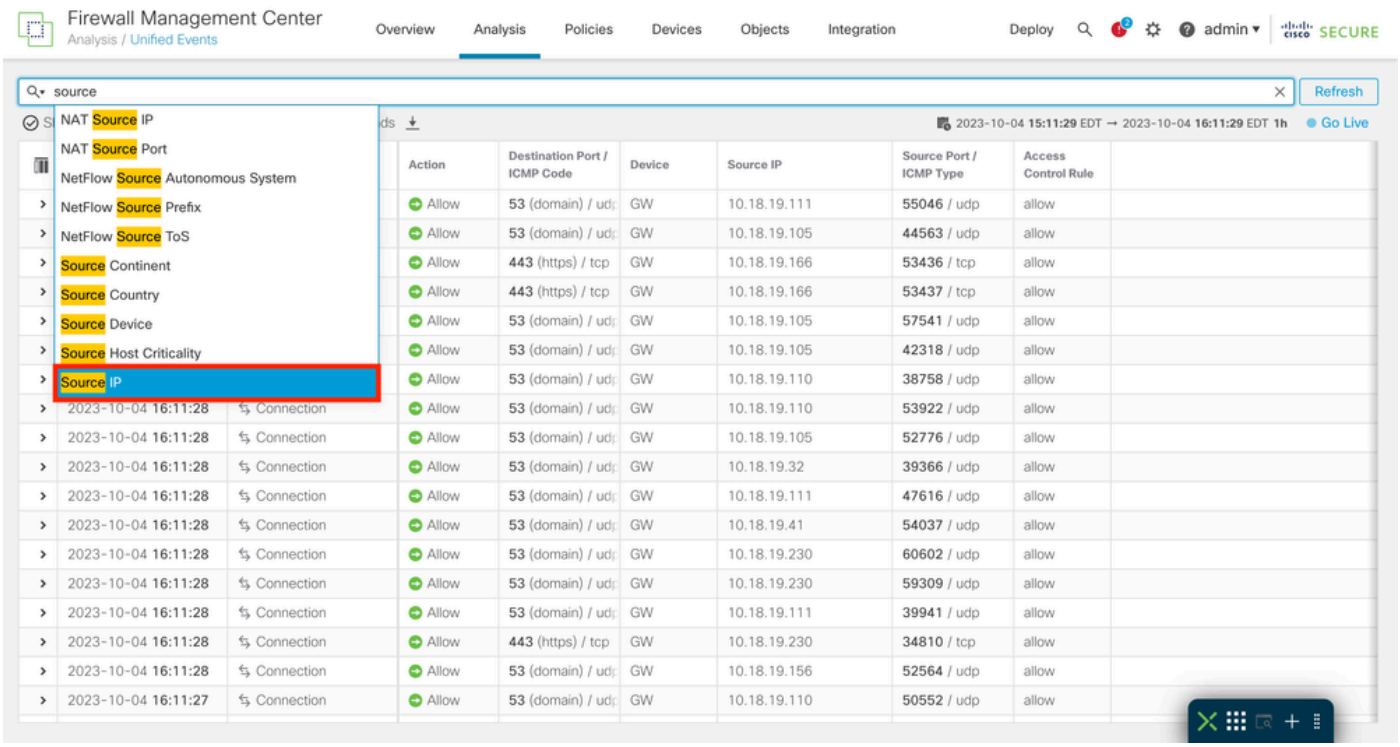


事件搜尋

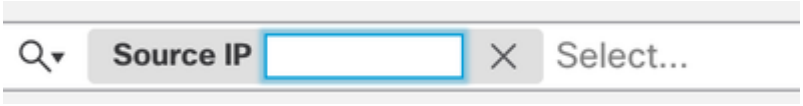
步驟1。若要開始搜尋特定事件，請按一下「Select」。



步驟2.選擇要應用篩選器的欄位。

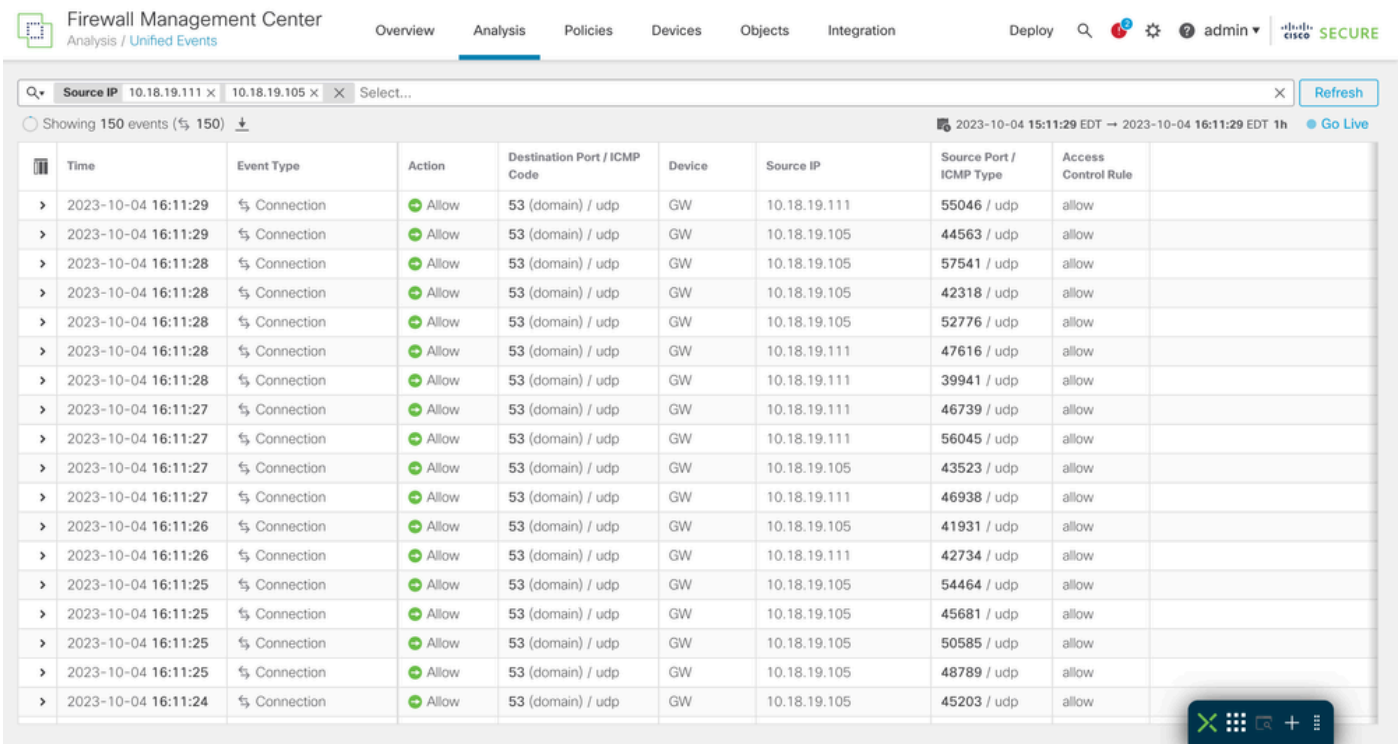


步驟3.寫入要用作篩選器的值。

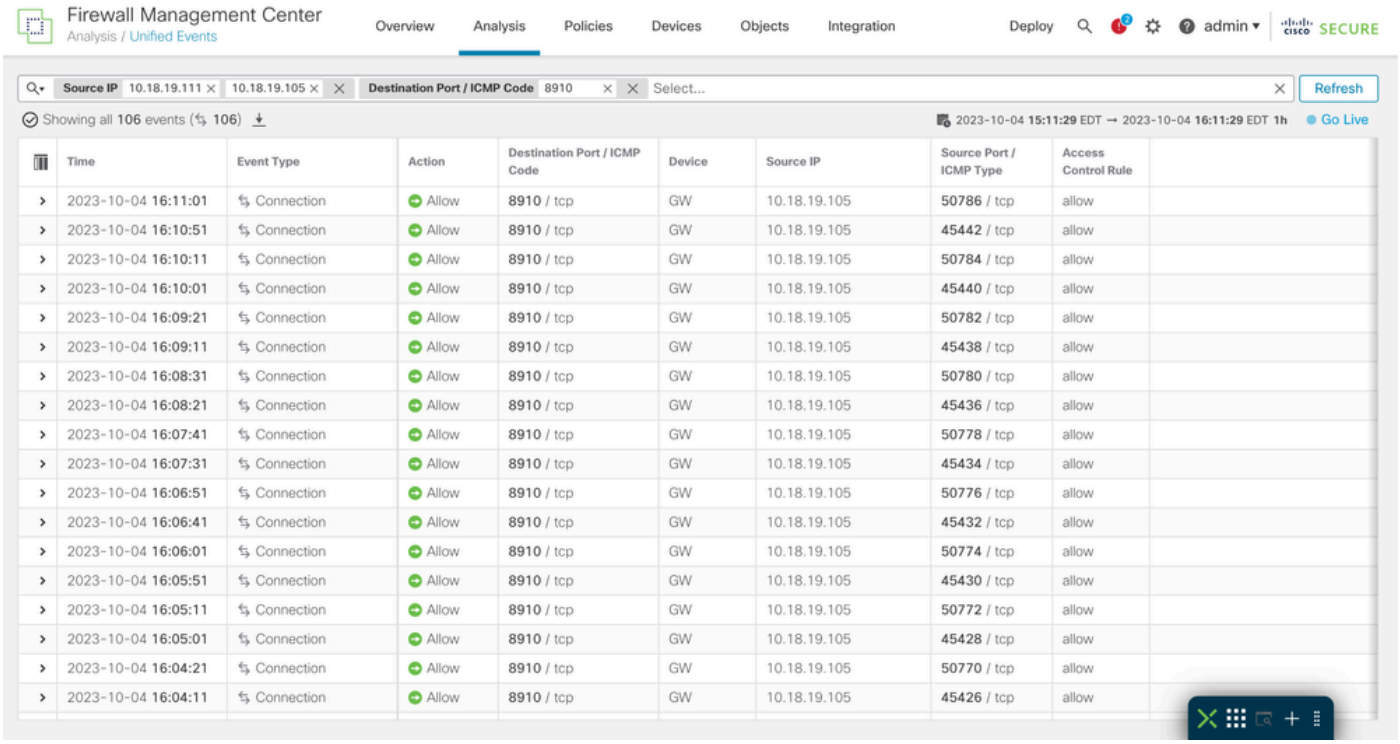


步驟4.按一下Apply以設定篩選條件。

步驟5.（可選）可以向每個篩選器新增多個值。



步驟6.（可選）根據需要新增多個篩選條件。

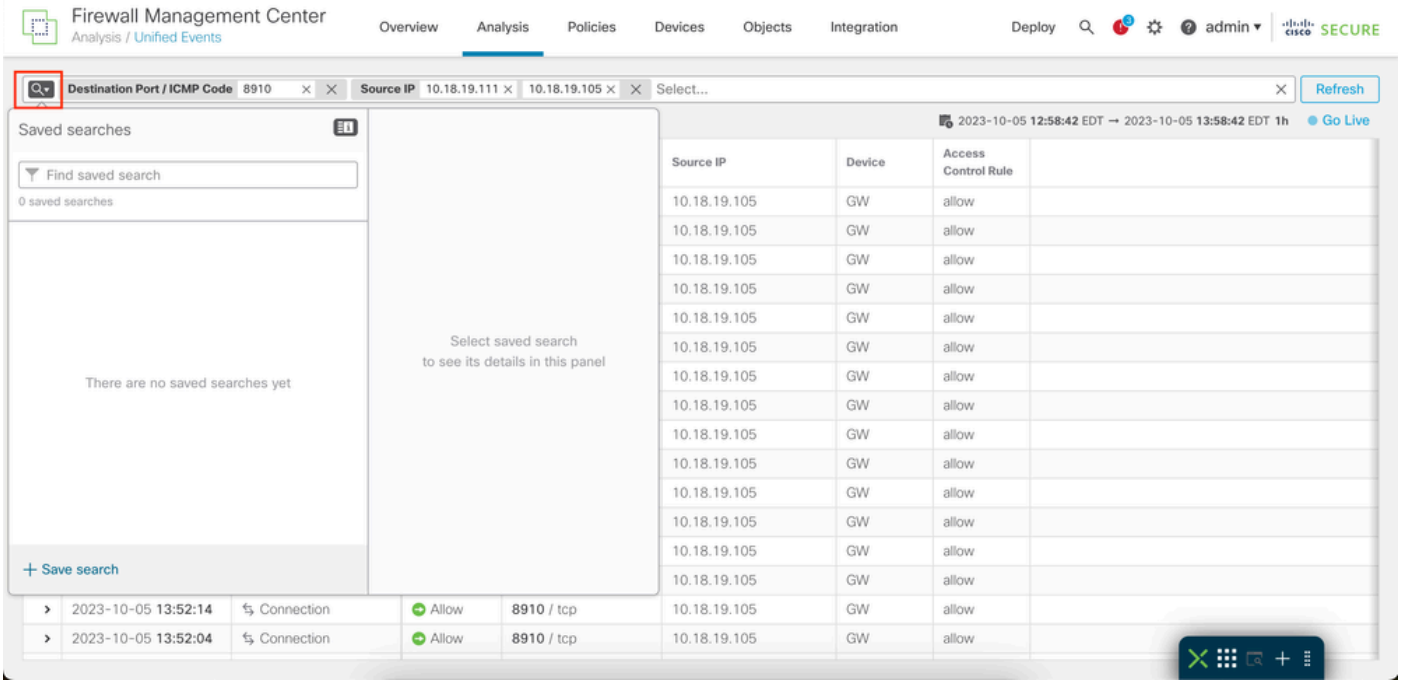


提示：編寫值時可以使用運算子（>、<、 ！等）。

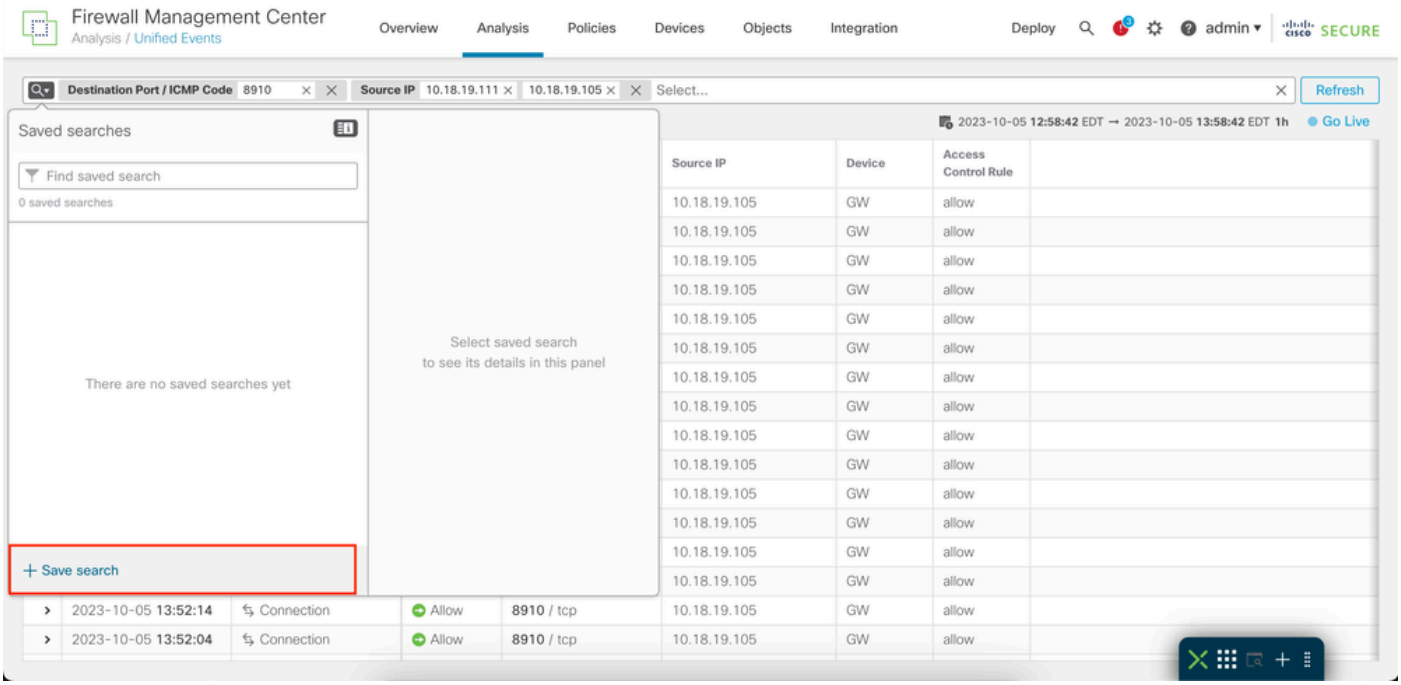
儲存搜尋

可以儲存搜尋，以便您可以重複使用已建立的過濾器。

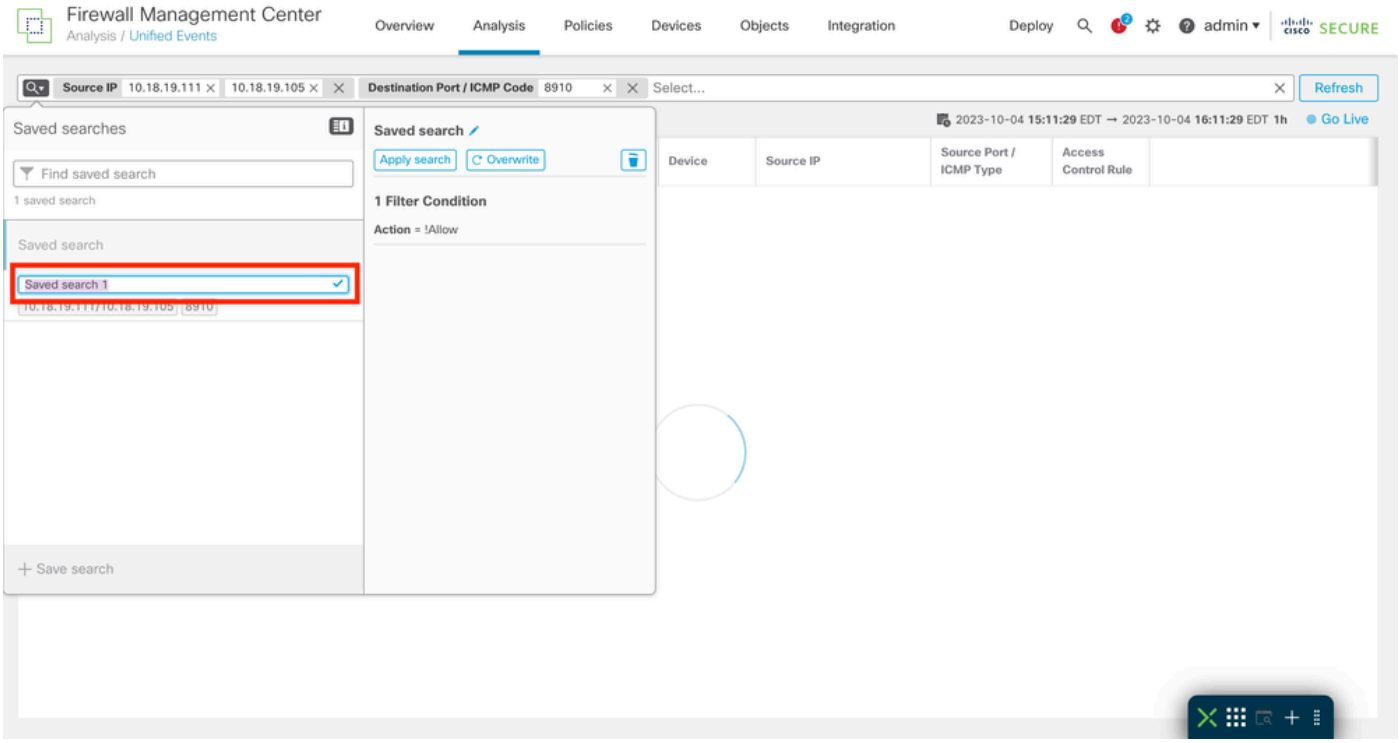
步驟1.按一下放大鏡圖示。



步驟2.按一下Save Search。



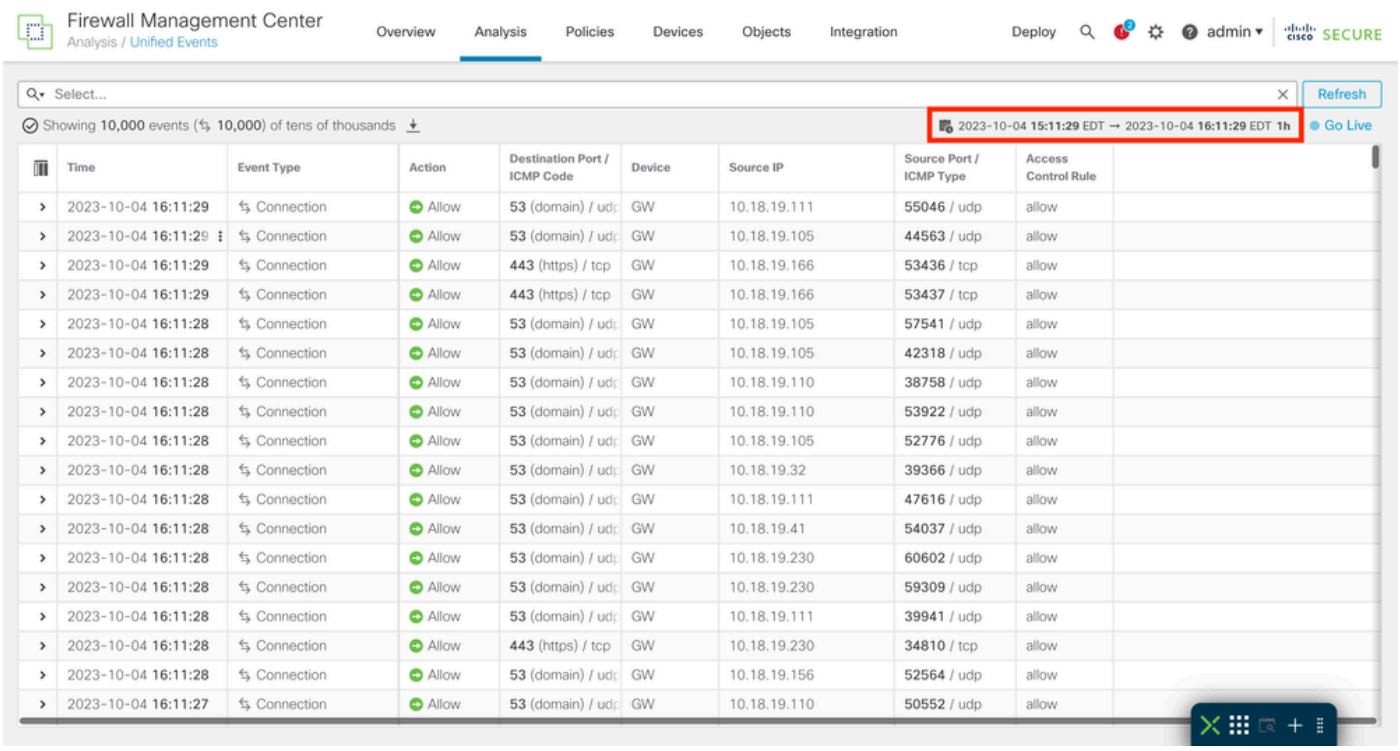
步驟3.（可選）更改搜尋的名稱。



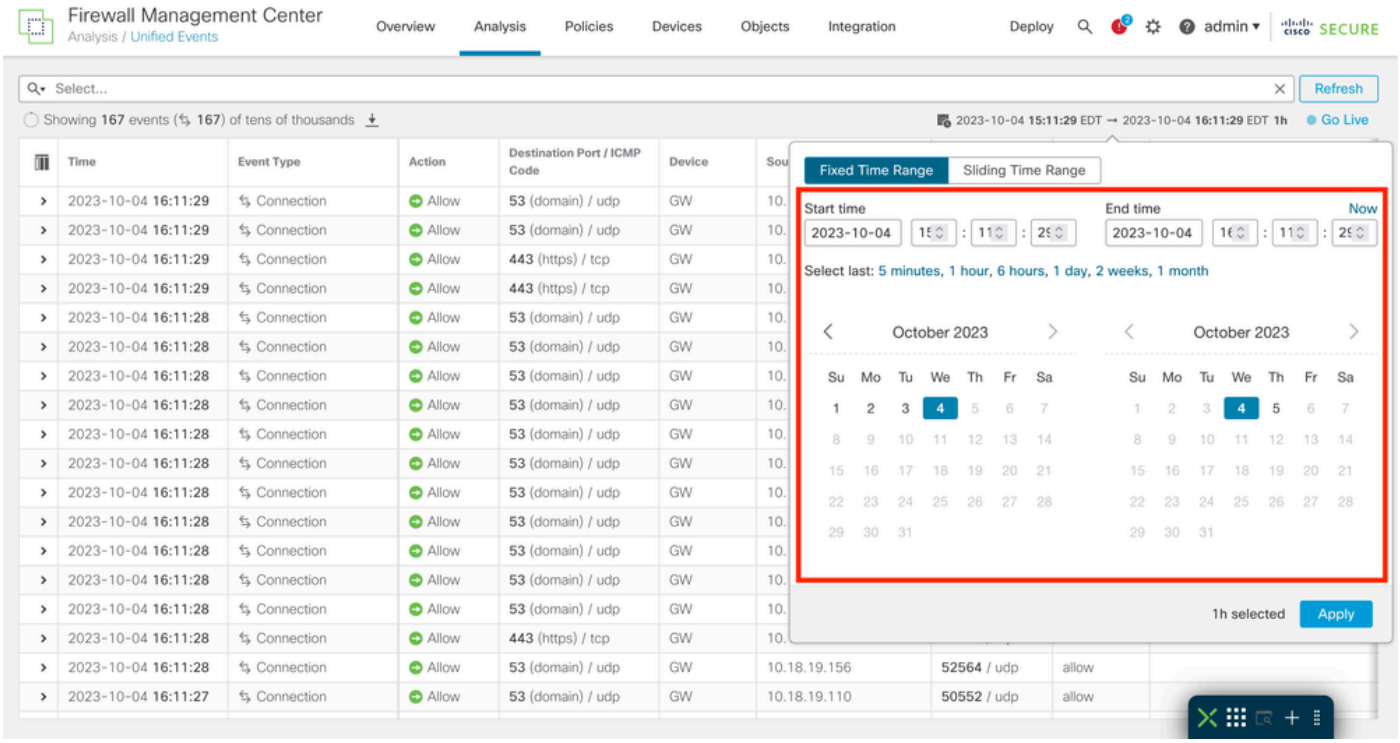
時間段

通過修改時間視窗，可以更容易地根據特定時間縮小相關事件的範圍。

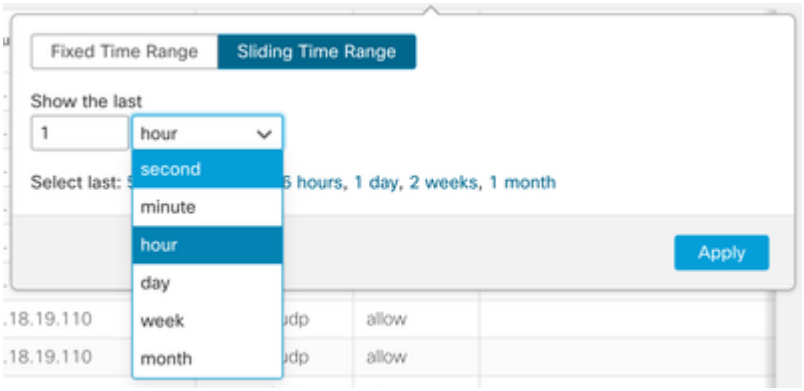
步驟1。若要修改事件的視窗框架，請按一下日期範圍。



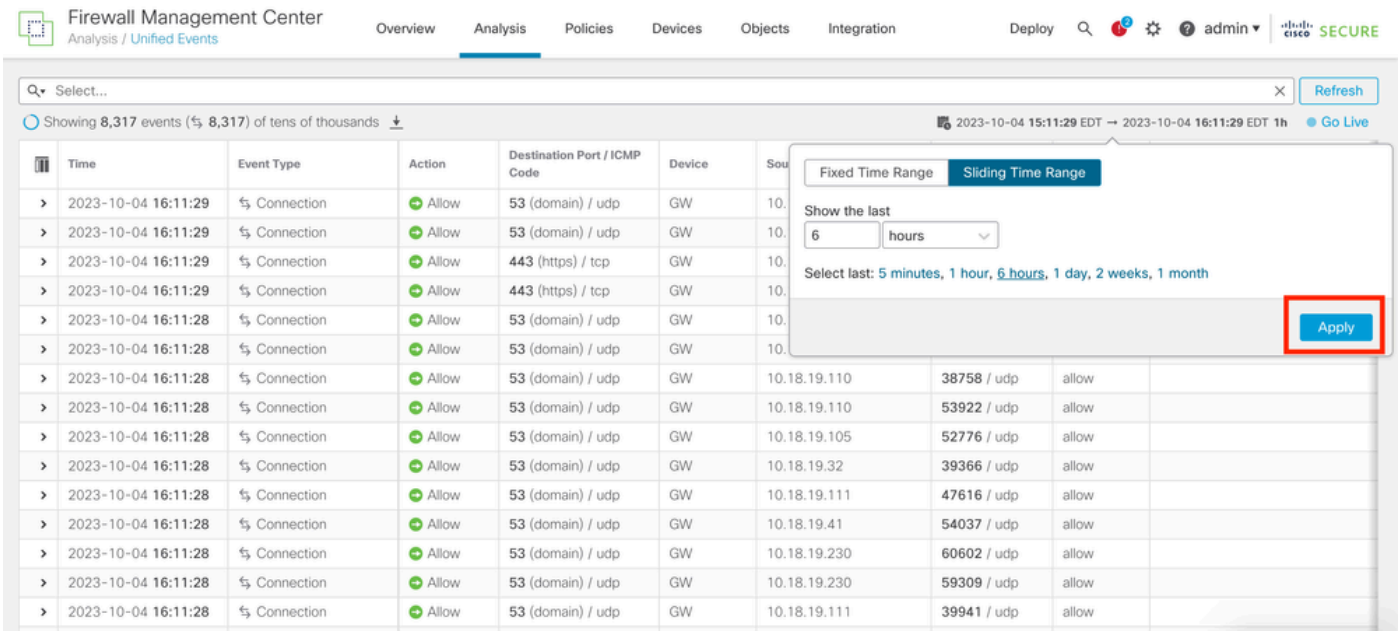
步驟2.在彈出視窗中選擇時間範圍。



步驟3.（可選）使用滑動時間範圍顯示從特定時間到當前時間的事件。



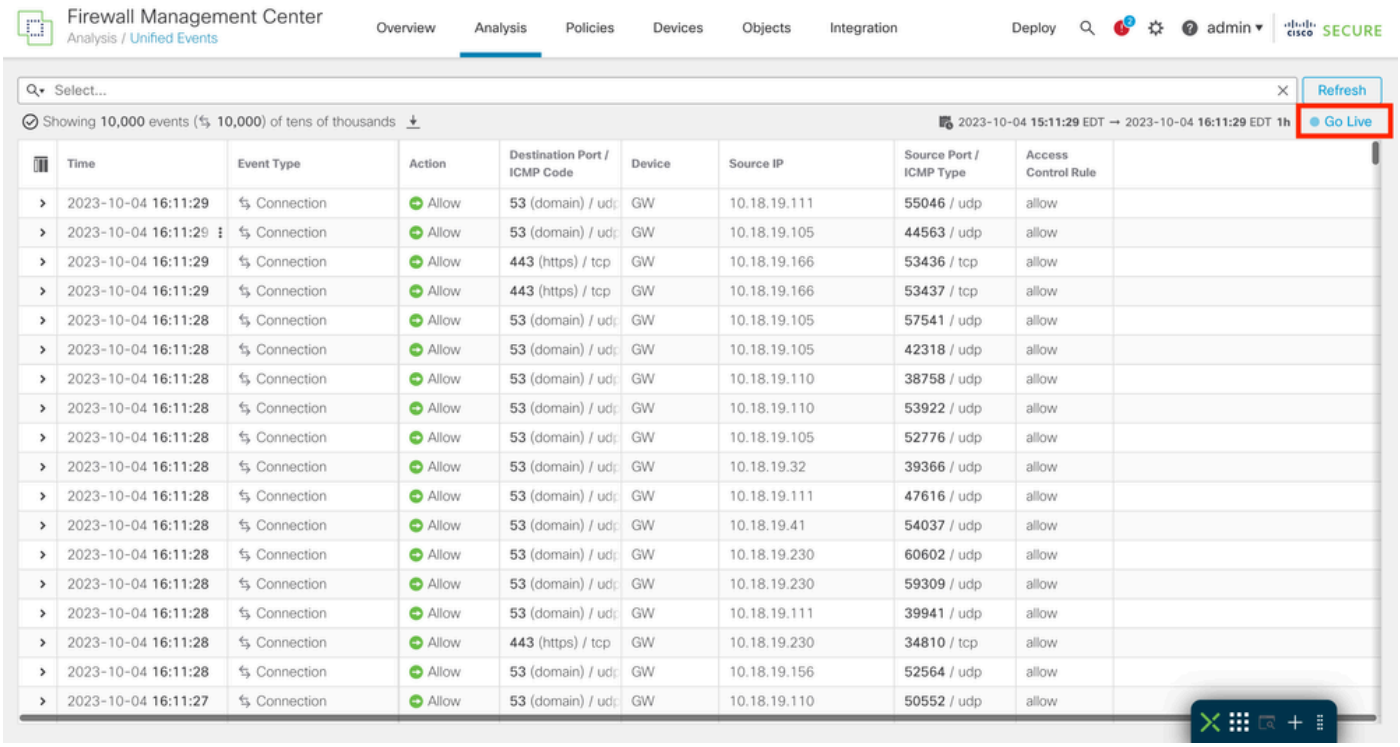
步驟4.按一下Apply以過濾所設定時間範圍的事件。



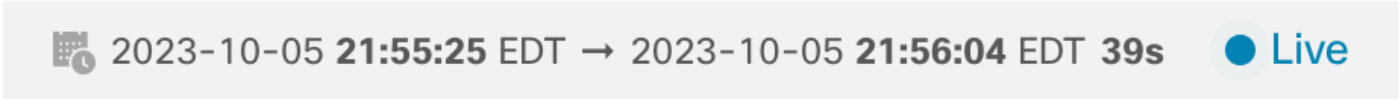
啟用

您可以啟用「啟用」功能以即時顯示事件。事件在生成時顯示。

要啟用，請按一下啟用。



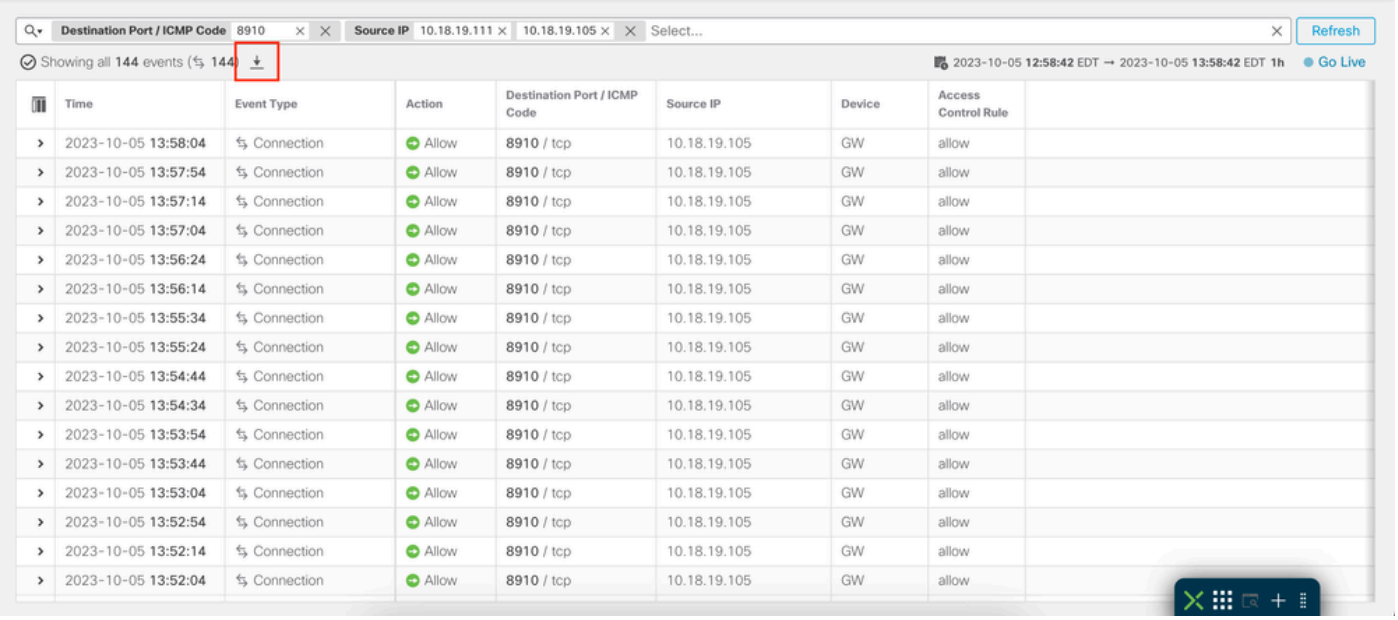
啟用後，它會顯示Live一詞。



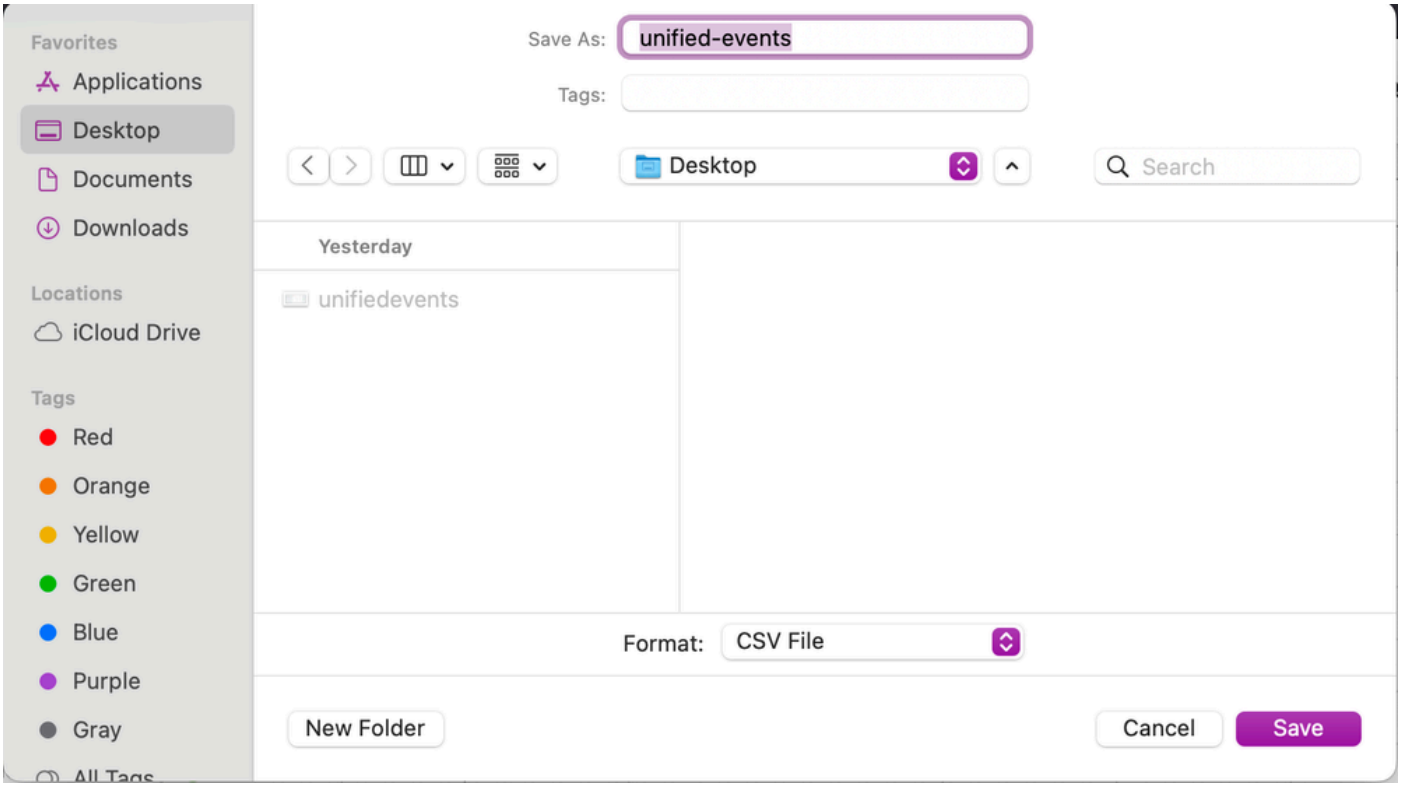
注意：啟用Live後，無法修改時間視窗。要修改時間視窗，請先再次按一下以禁用「即時」選項。

將事件下載為 逗號分隔值(CSV)

步驟1.按一下下載圖示以生成包含當前顯示在頁面上的事件的檔案。



步驟2.選擇下載資料夾和名稱，然後按一下Save。



步驟3.驗證CSV檔案。

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	37412 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	54766 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.166	54279 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	55185 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	46312 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	36785 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	57394 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	57395 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	38278 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44865 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	58387 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	49873 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	51060 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	34103 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.31	60020 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	43410 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47406 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	43359 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	43336 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	42658 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52923 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	46485 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.201	52178 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55864 / udp	allow

相關資訊

- 使用統一事件檢視器
- 思科安全防火牆 — 統一事件檢視器：提示與訣竅
- 思科技術支援與下載

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）。

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）。

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）。