Monitoraggio degli eventi tramite il Visualizzatore eventi unificato sull'interfaccia utente di FMC

Sommario

Introduzione

In questo documento viene descritto l'utilizzo del Visualizzatore eventi unificato su un'interfaccia utente grafica (GUI) in Firewall Management Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso a FMC con privilegi di amministratore o analista della sicurezza
- FMC con versione uguale o superiore a v7.0

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure Firewall Management Center per VMware v7.2.5

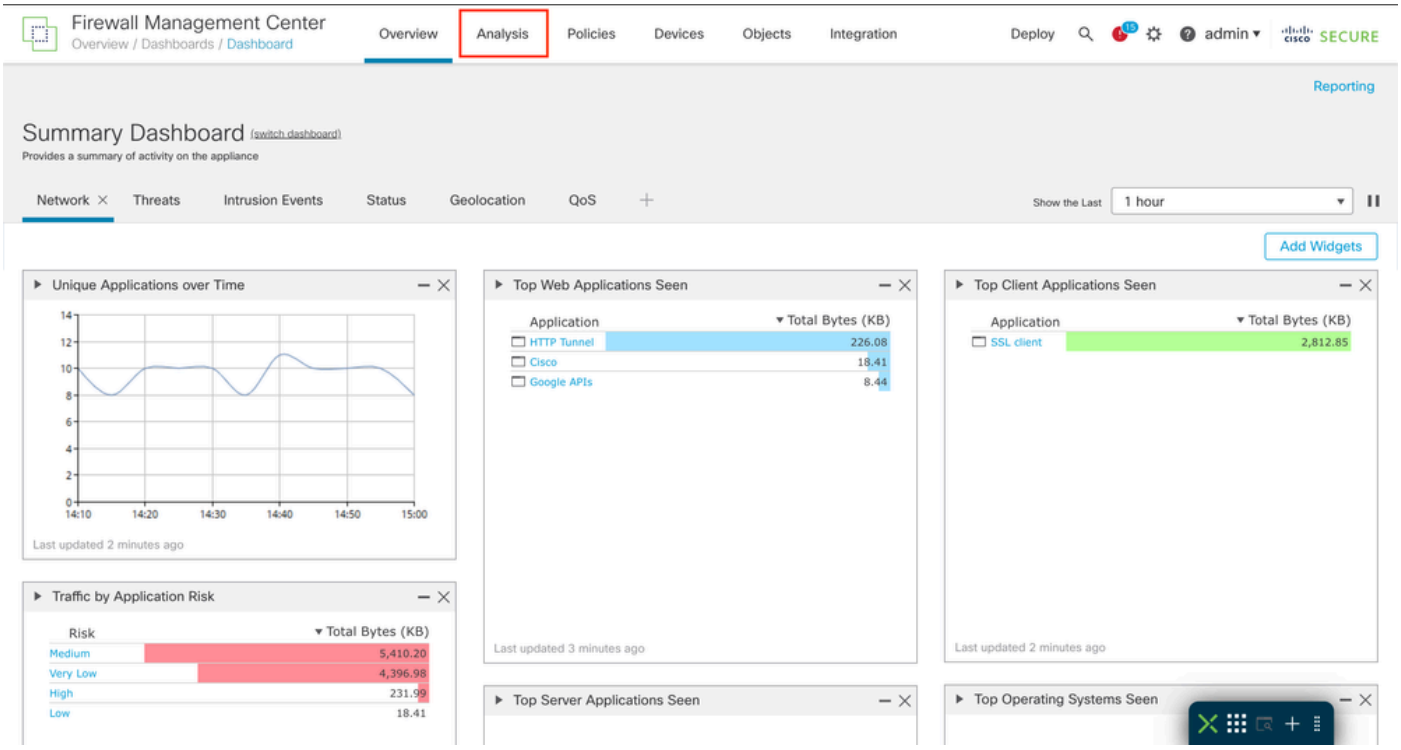
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

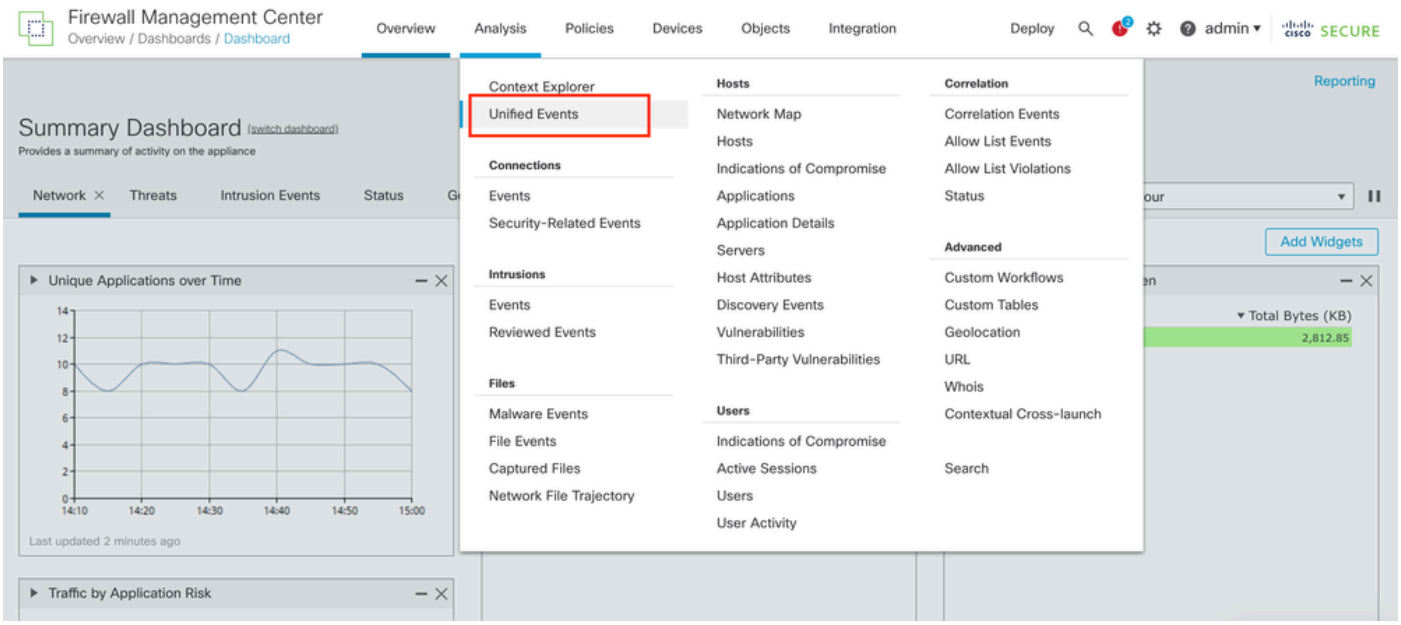
Esplora

Passaggio 1. Accedere all'interfaccia utente di FMC.

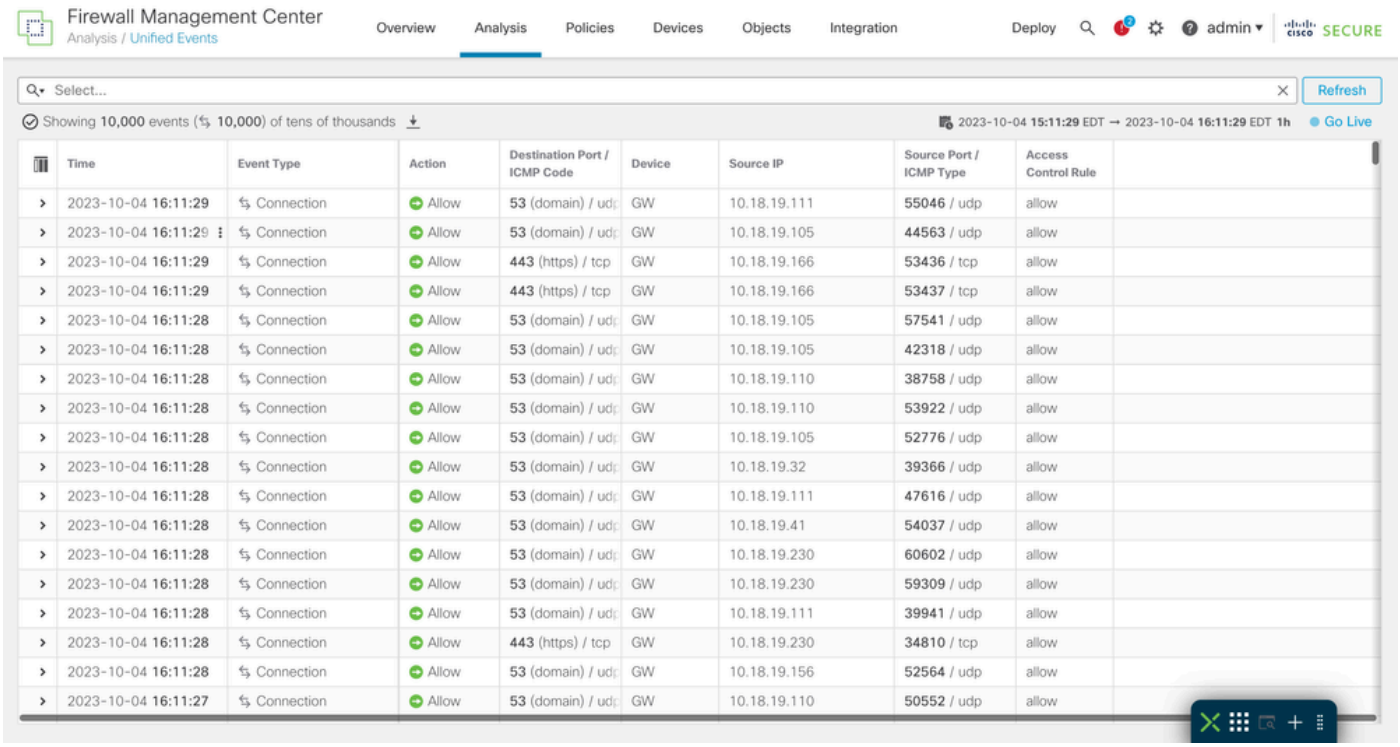
Passaggio 2. Passare alla scheda Analisi.



Passaggio 3. Dal menu a discesa, fare clic su Unified Events (Eventi unificati).

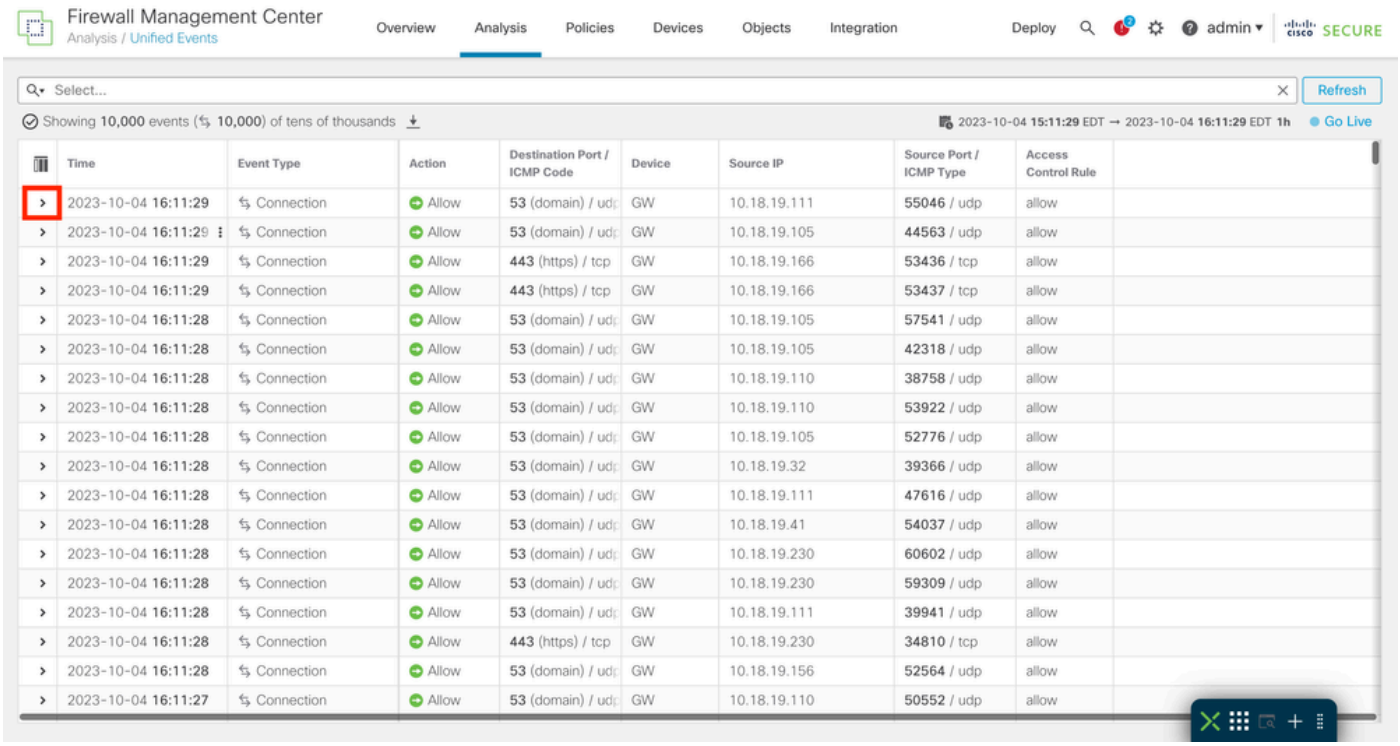


Esempio di pagina evento unificato

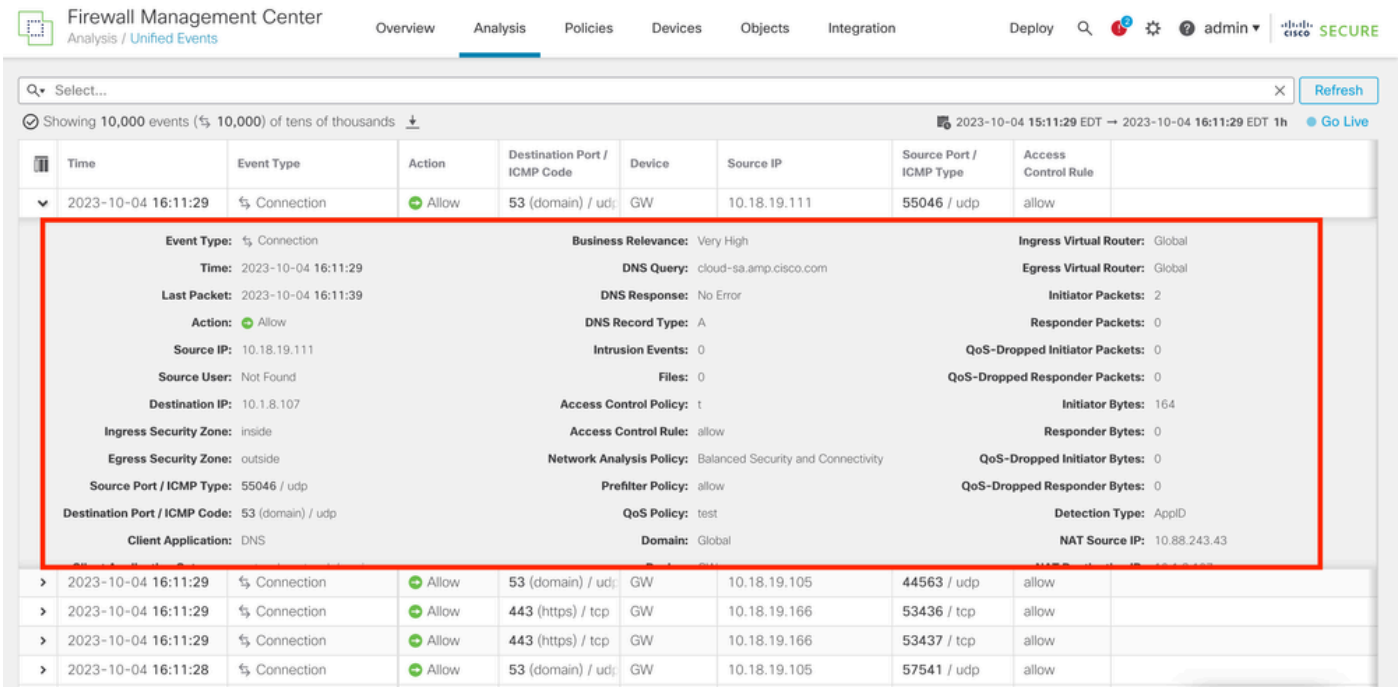


Eventi di revisione

Passaggio 1. Fare clic sull'icona >.

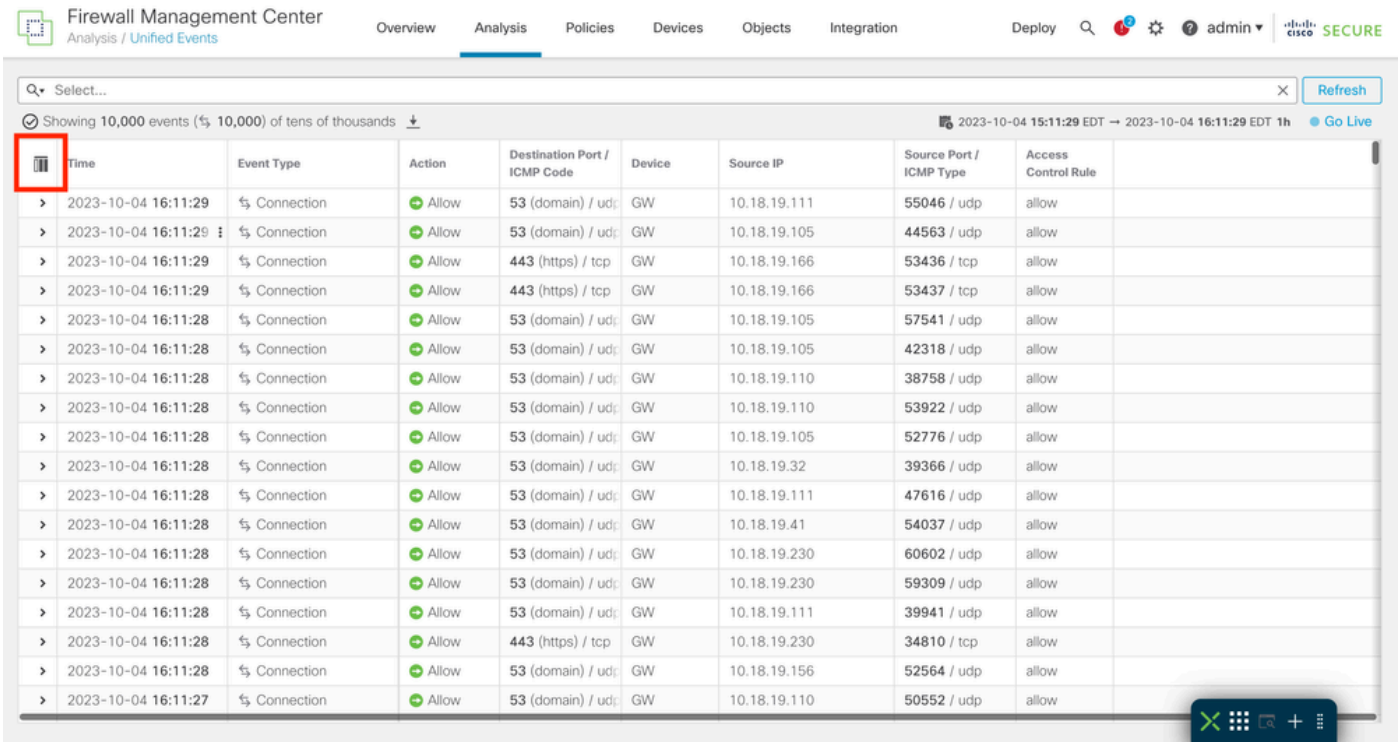


Passaggio 2. Vengono visualizzate informazioni dettagliate sull'evento.

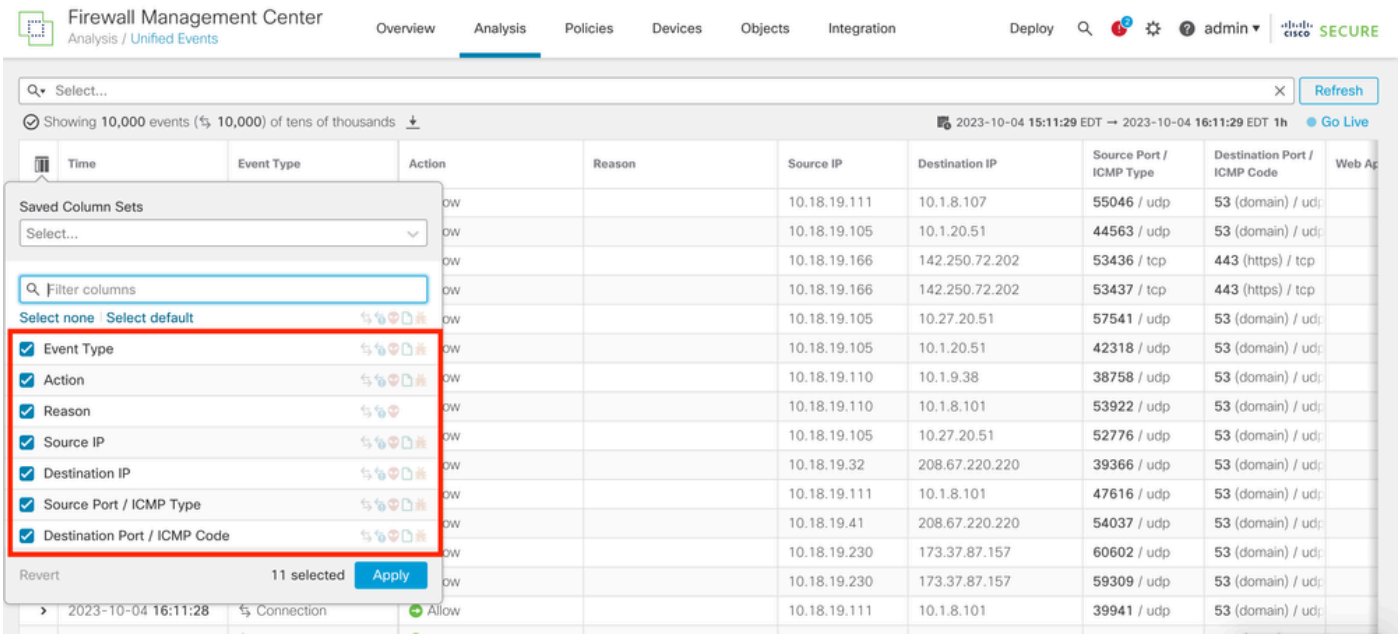


Personalizza colonne

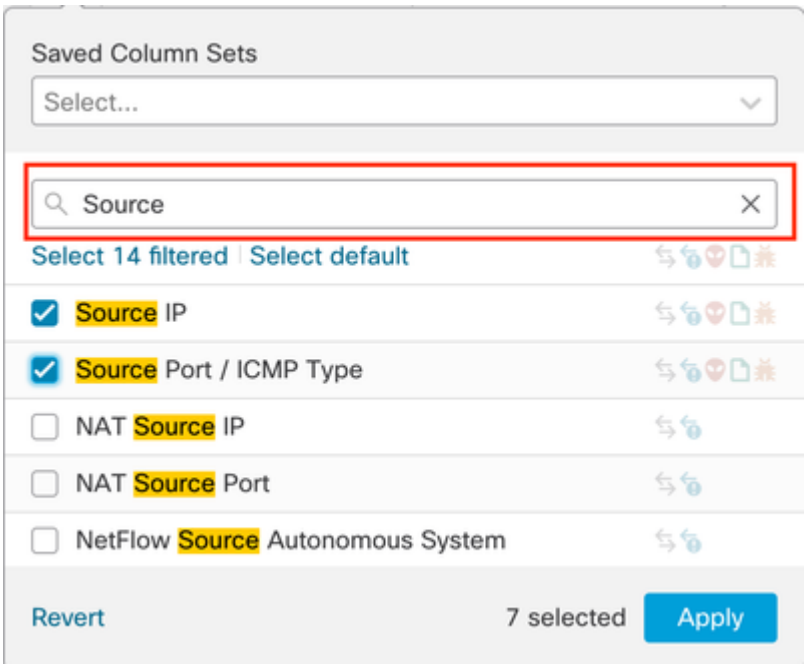
Passaggio 1. Fare clic sull'icona .



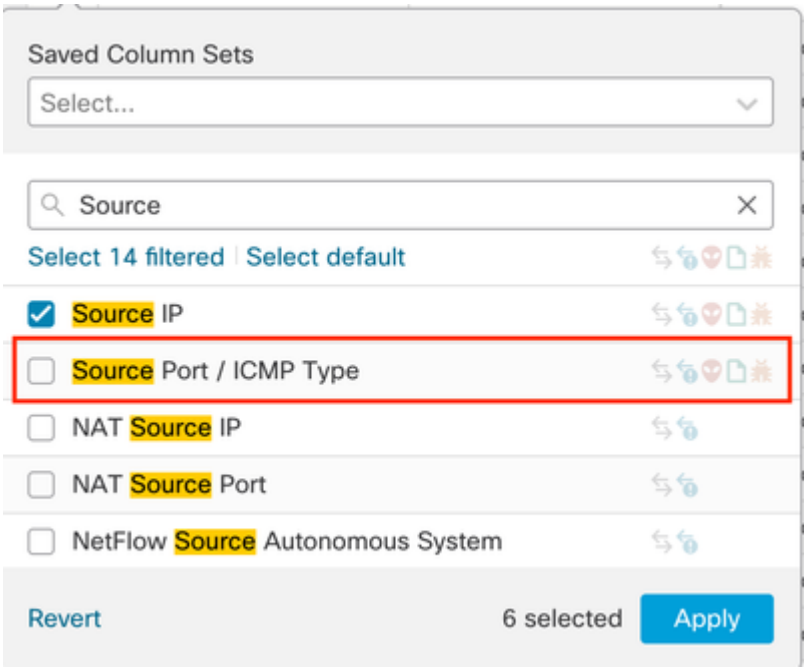
Passaggio 2. Selezionare i campi evento che si desidera visualizzare nella tabella.



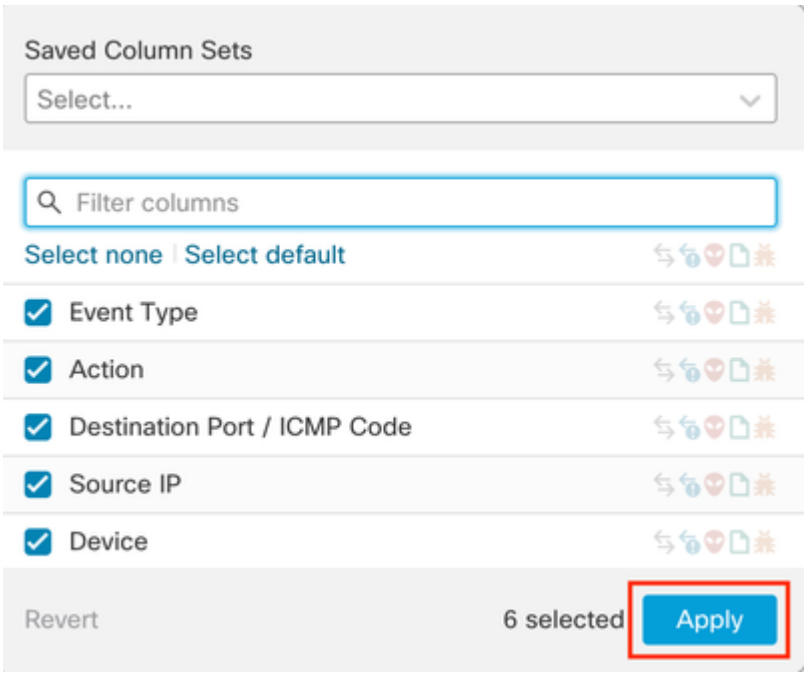
Passaggio 3. (Facoltativo) Cercare il campo per semplificare la navigazione.



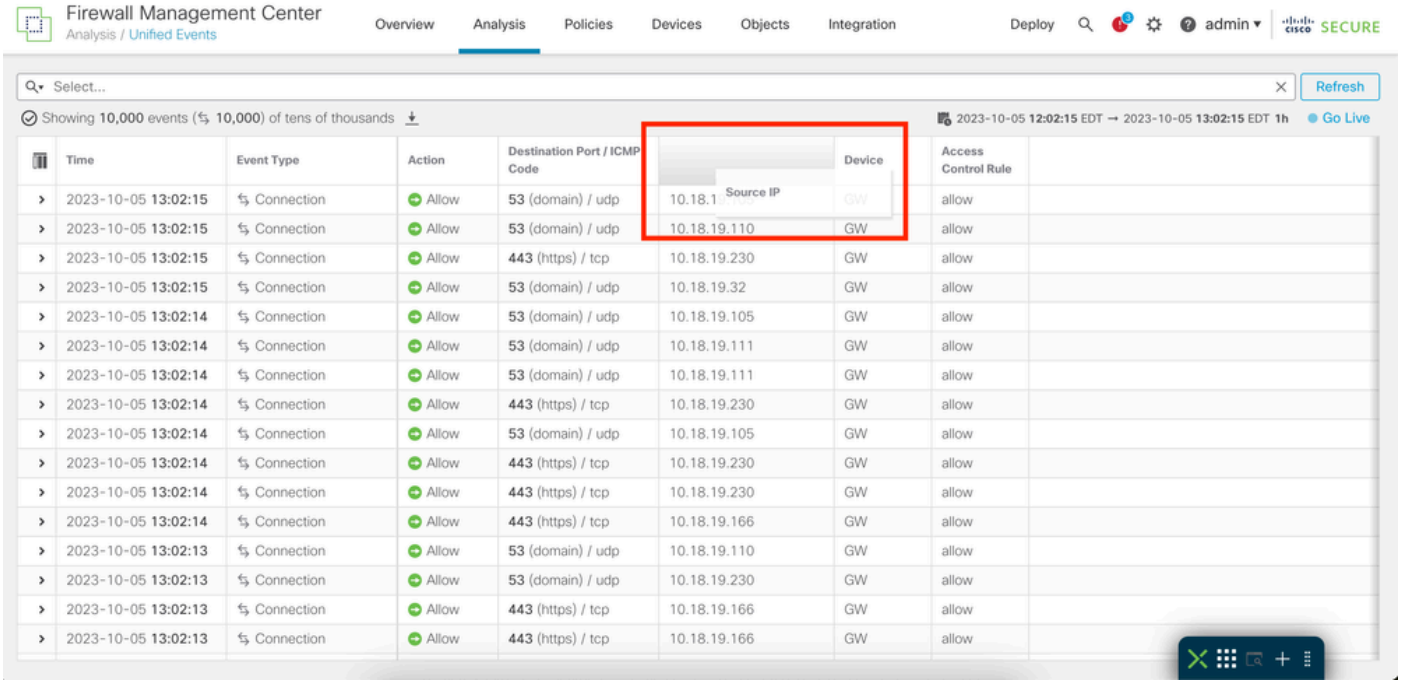
Passaggio 4. Fare clic su un campo evento per disabilitarlo o abilitarlo.



Passaggio 5. Fare clic su Apply (Applica).

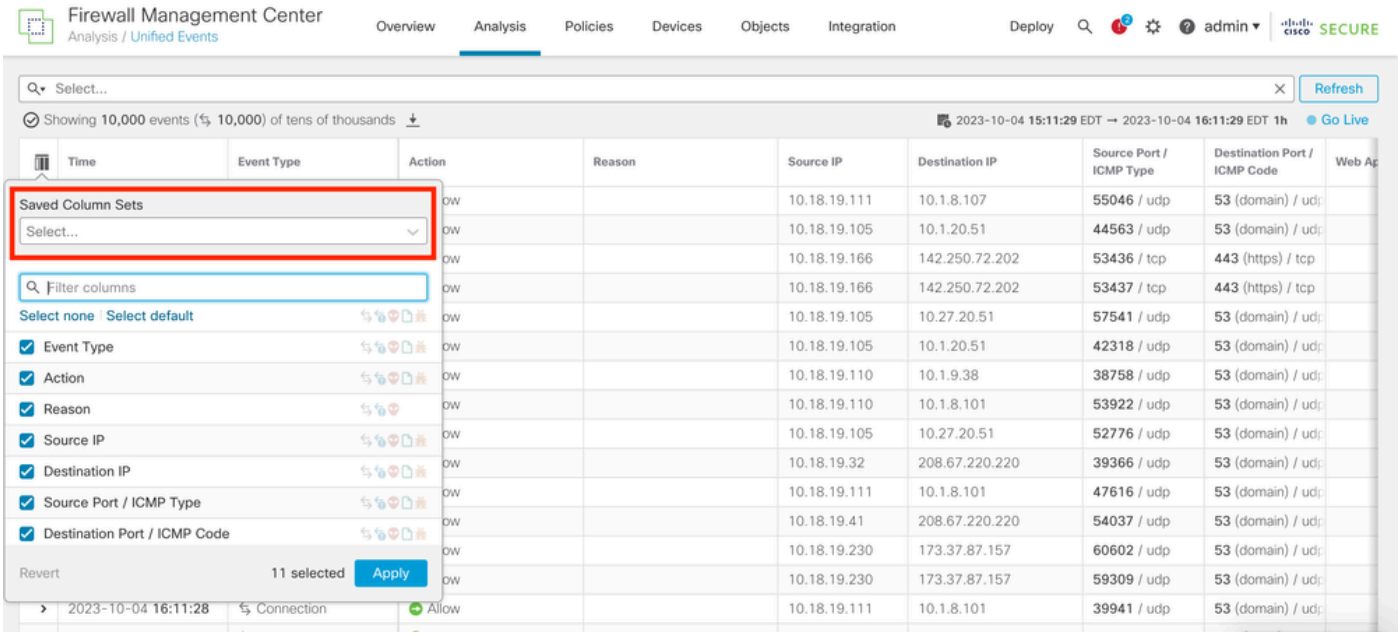


Passaggio 6. (Facoltativo) È possibile riposizionare le colonne trascinandole in una posizione diversa.

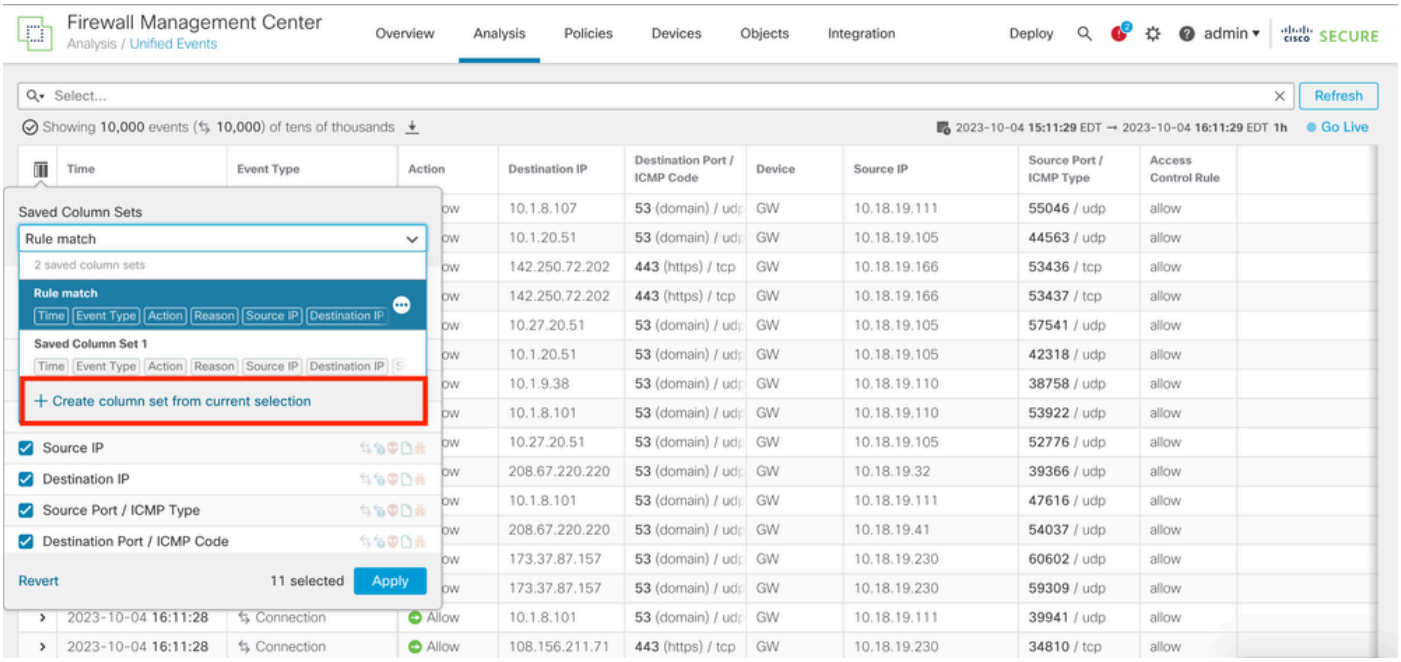


Salva set di colonne

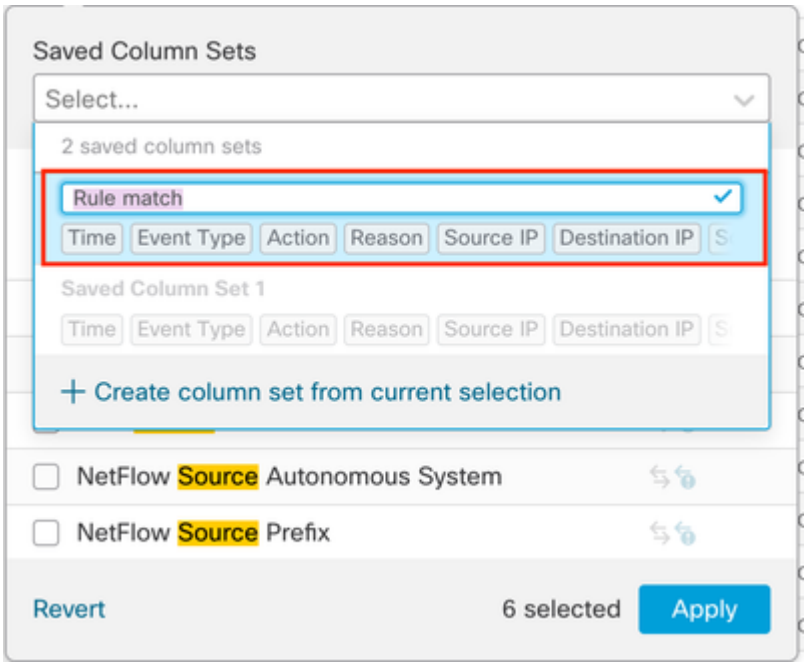
Passaggio 1. Fare clic su Serie di colonne salvate.



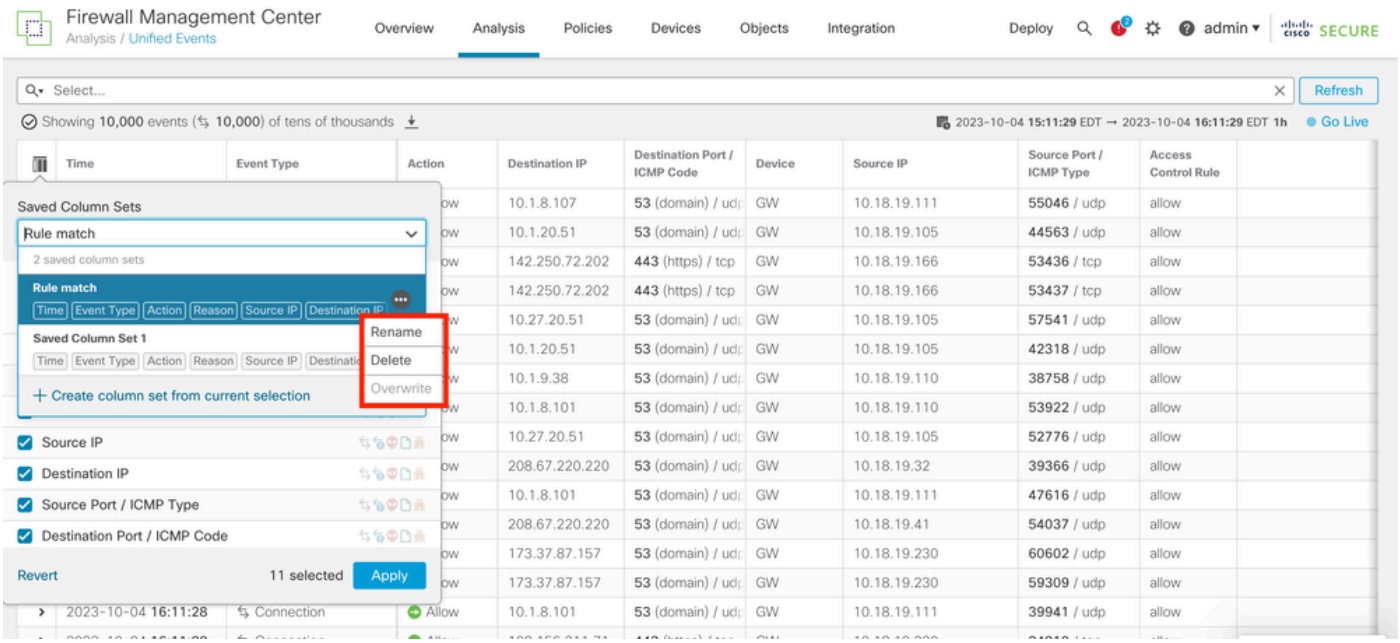
Passaggio 2. Fare clic su Crea serie di colonne dalla selezione corrente.



Passaggio 3. (Facoltativo) Modificare il nome della serie di colonne.

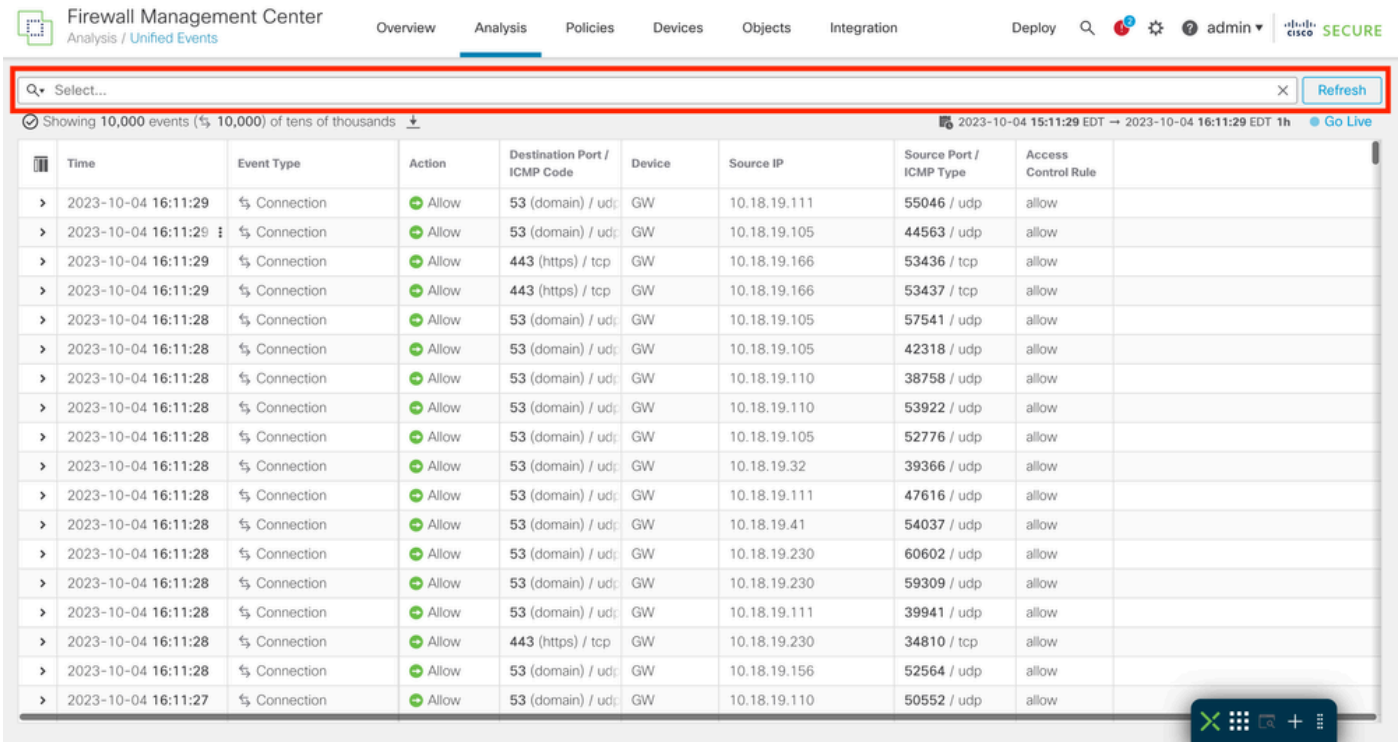


Passaggio 4. È possibile modificare un insieme esistente facendo clic sui puntini di sospensione (...).

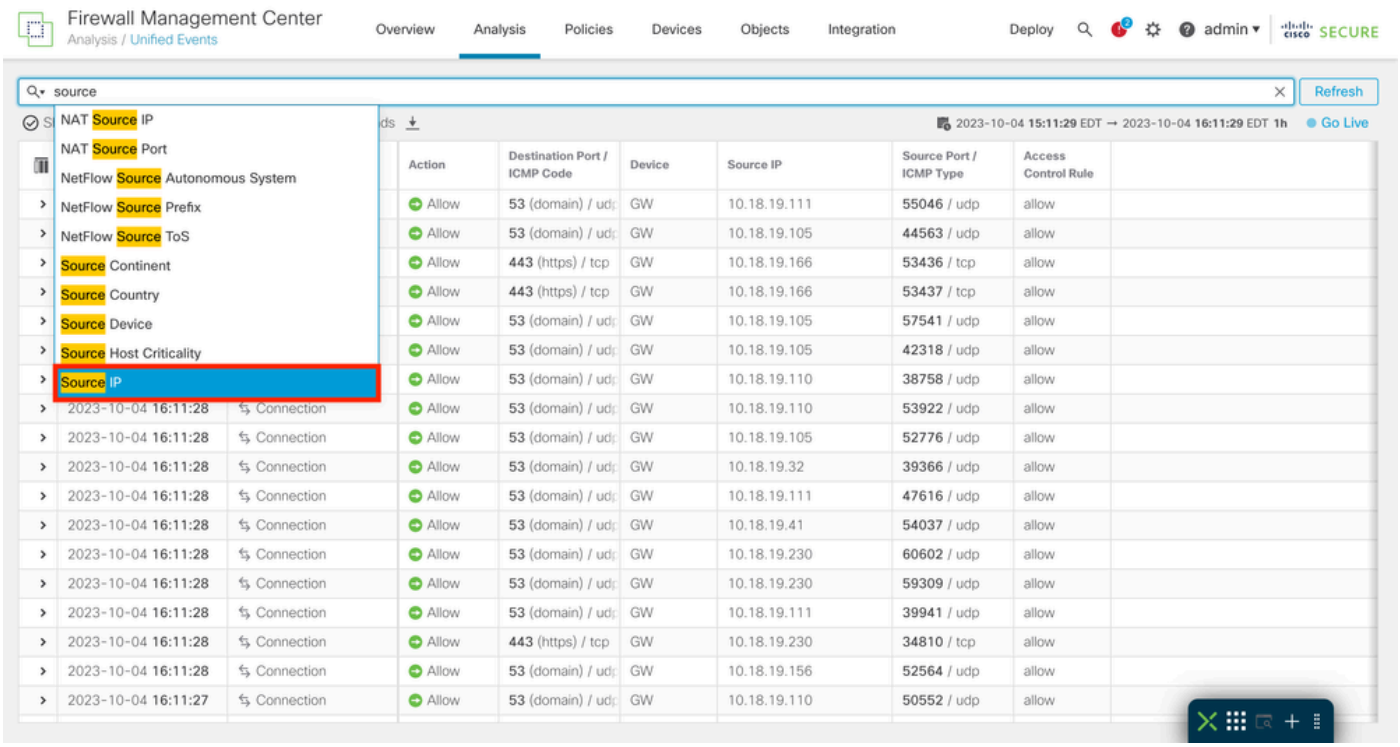


Ricerca eventi

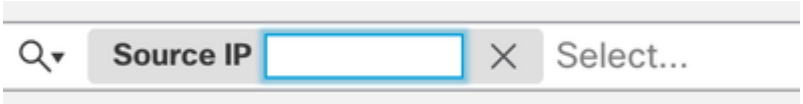
Passaggio 1. Per iniziare la ricerca di eventi specifici, fare clic su Seleziona.



Passaggio 2. Selezionare il campo in cui si desidera applicare il filtro.

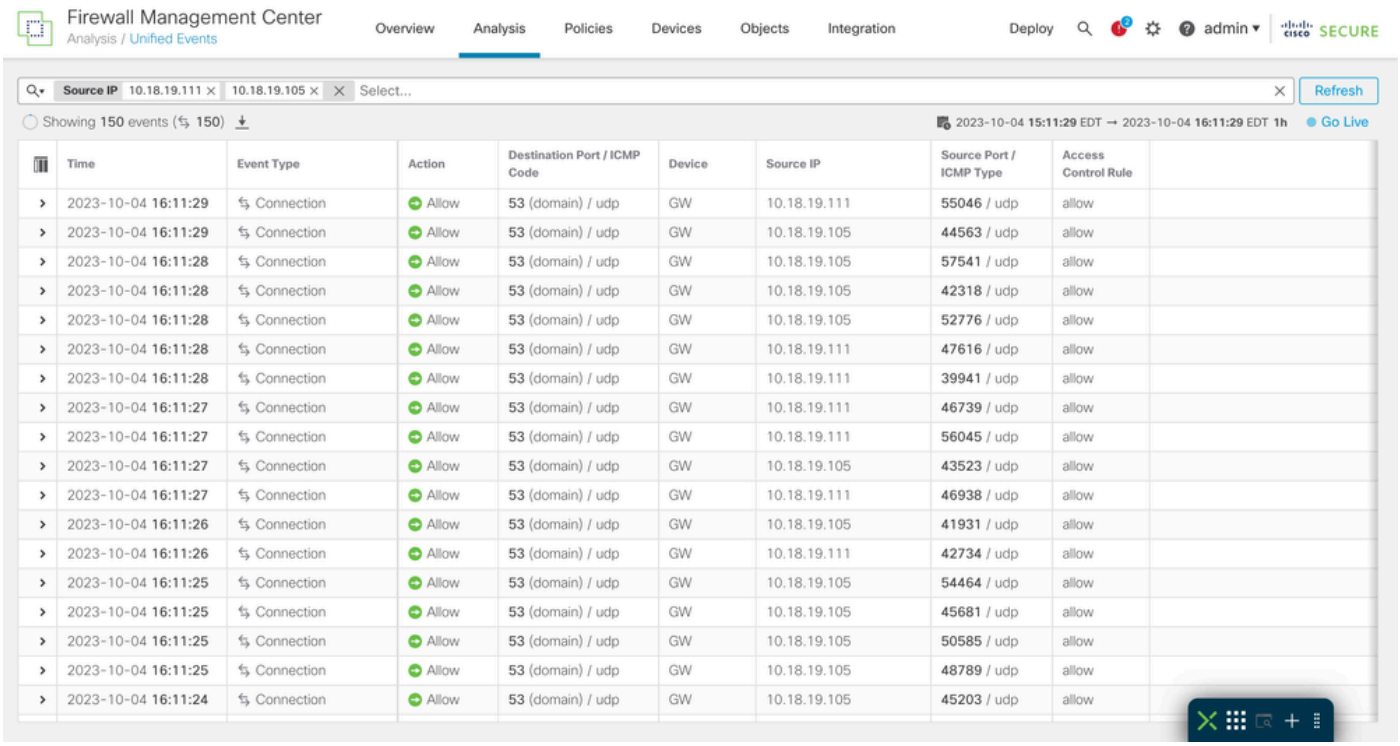


Passaggio 3. Scrivere i valori da utilizzare come filtro.

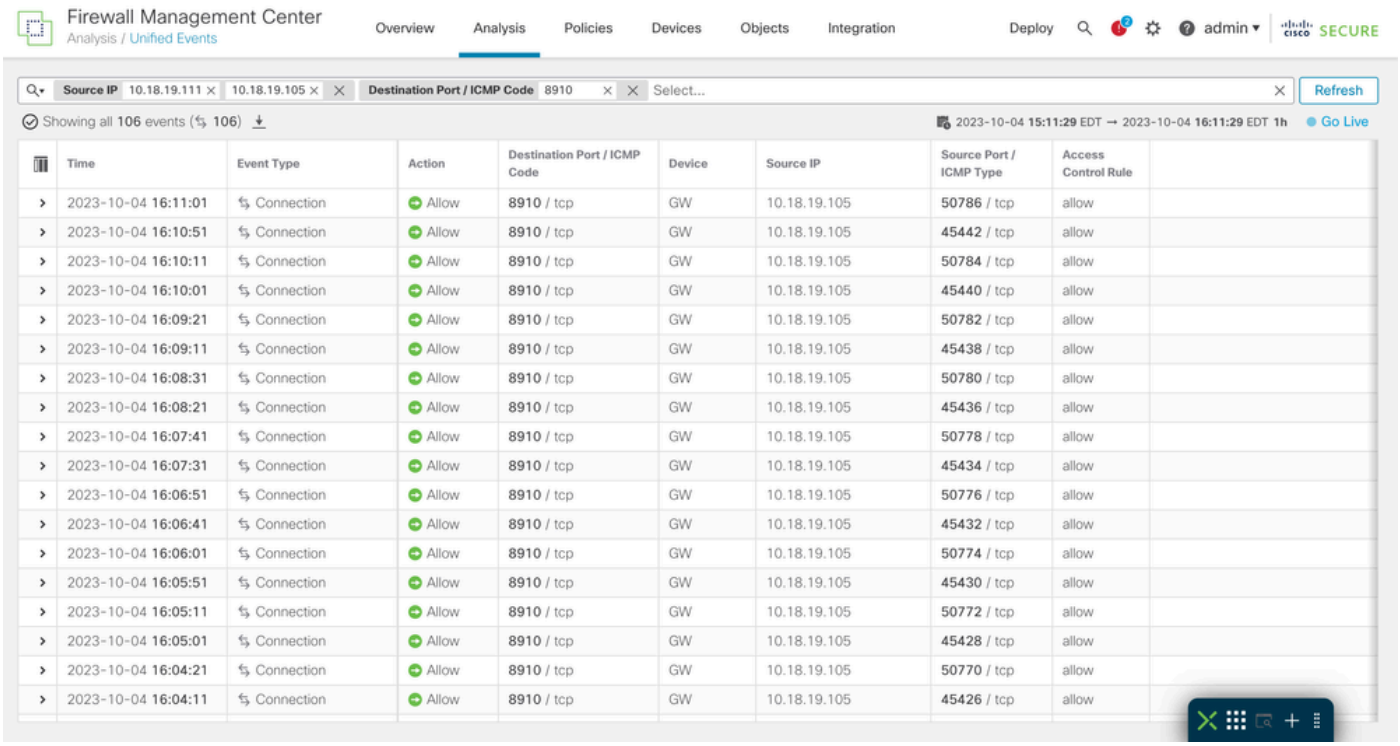


Passaggio 4. Fare clic su Apply (Applica) per configurare il filtro.

Passaggio 5. (Facoltativo) È possibile aggiungere più valori a ogni filtro.



Passaggio 6. (Facoltativo) Aggiungere tutti i filtri necessari.

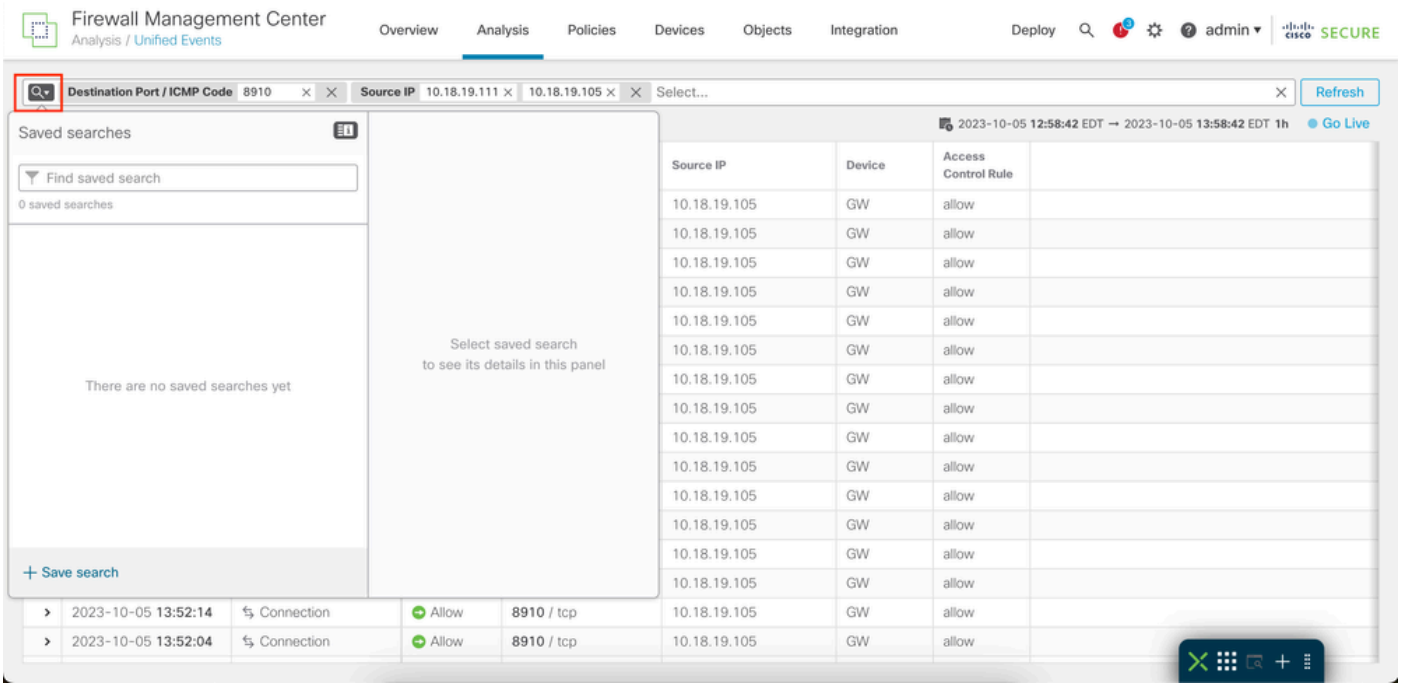


Suggerimento: È possibile utilizzare gli operatori (>,<, ! e così via) durante la scrittura dei valori.

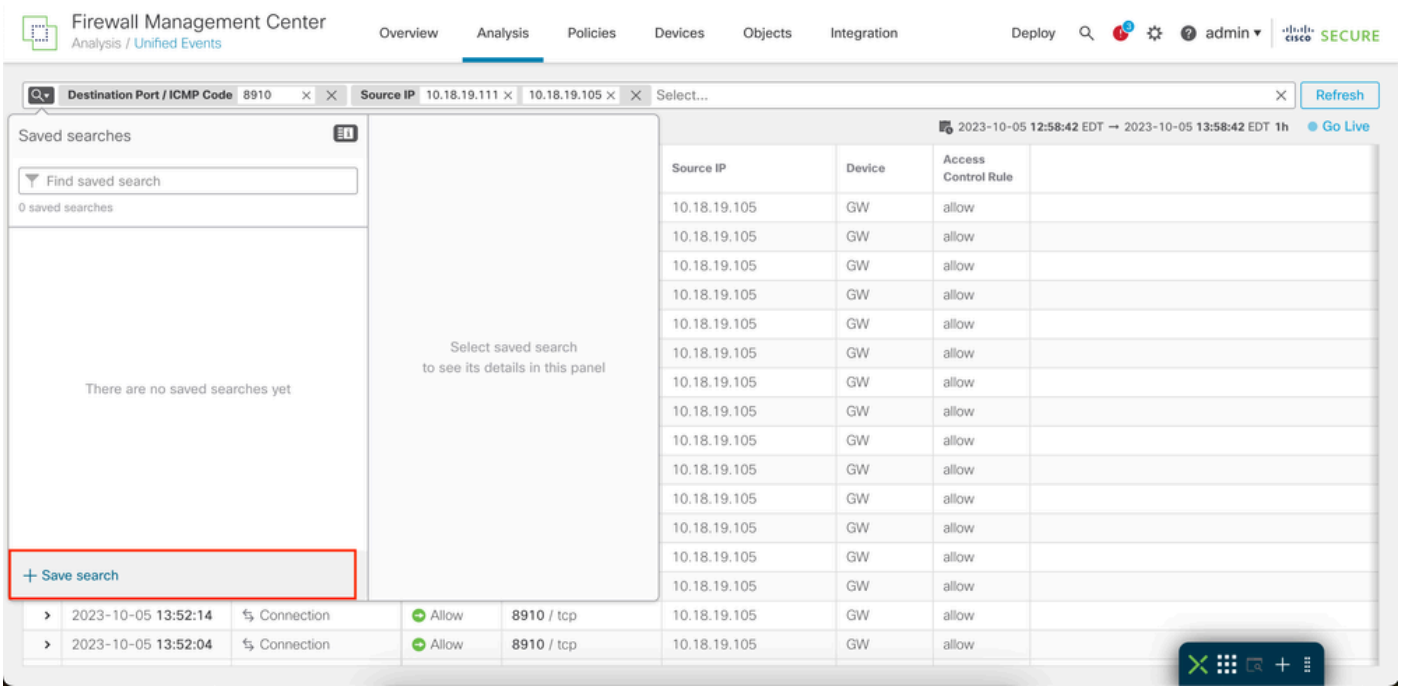
Salva ricerca

È possibile salvare le ricerche in modo da poter riutilizzare i filtri creati.

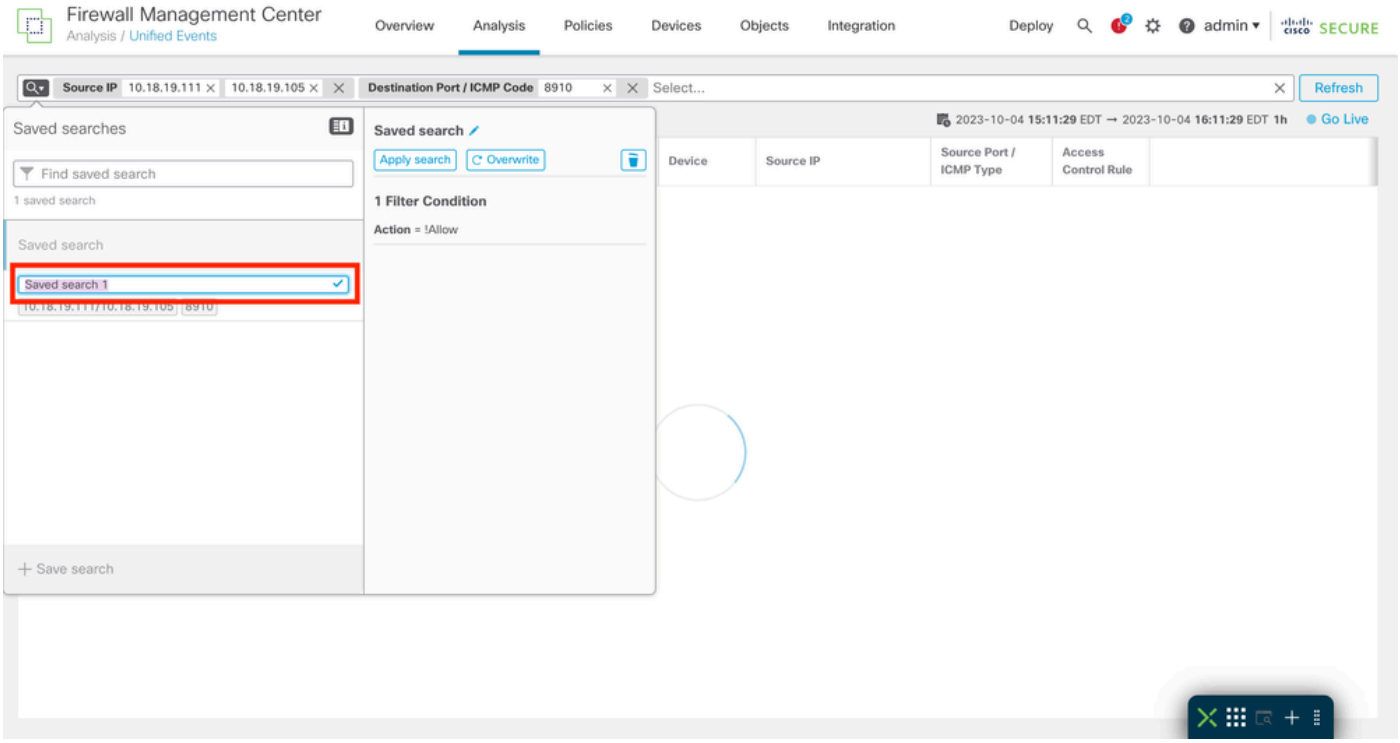
Passaggio 1. Fare clic sull'icona della lente di ingrandimento.



Passaggio 2. Fare clic su Salva ricerca.



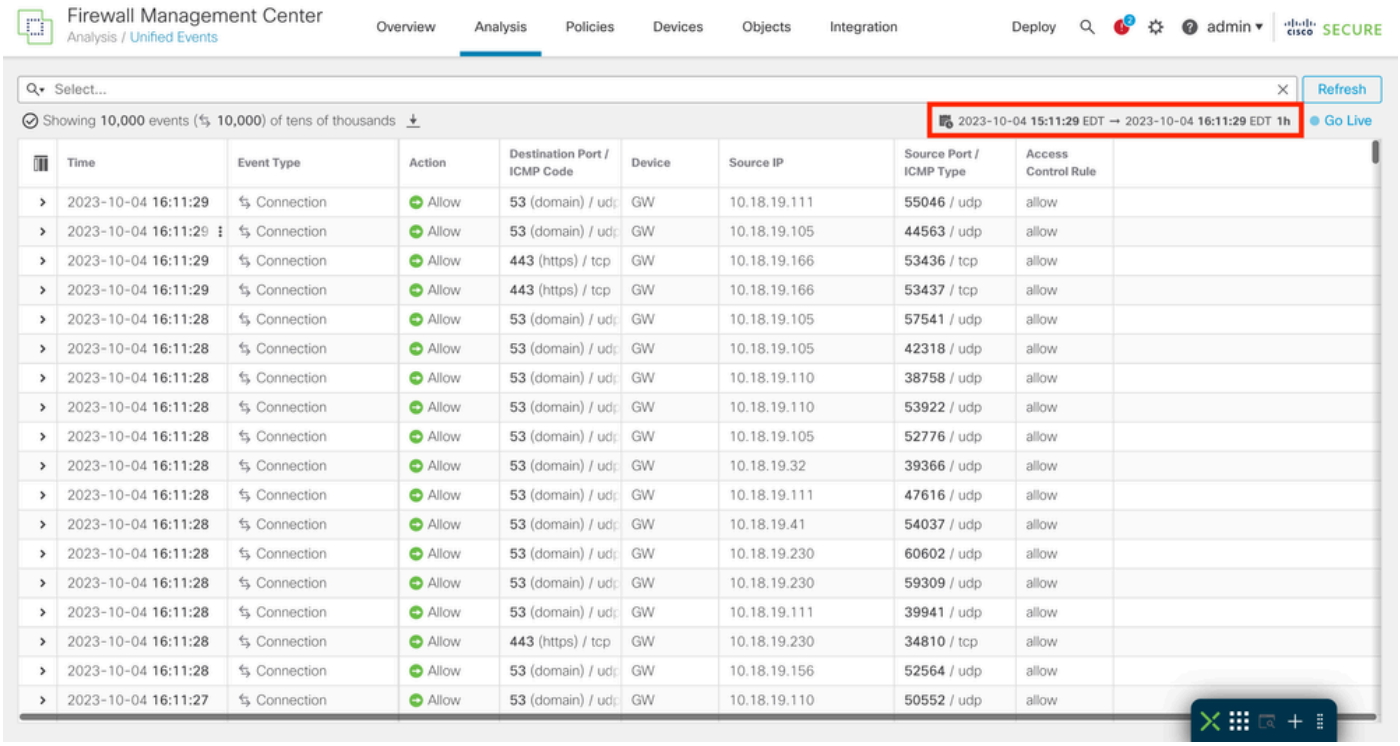
Passaggio 3. (Facoltativo) Modificare il nome della ricerca.



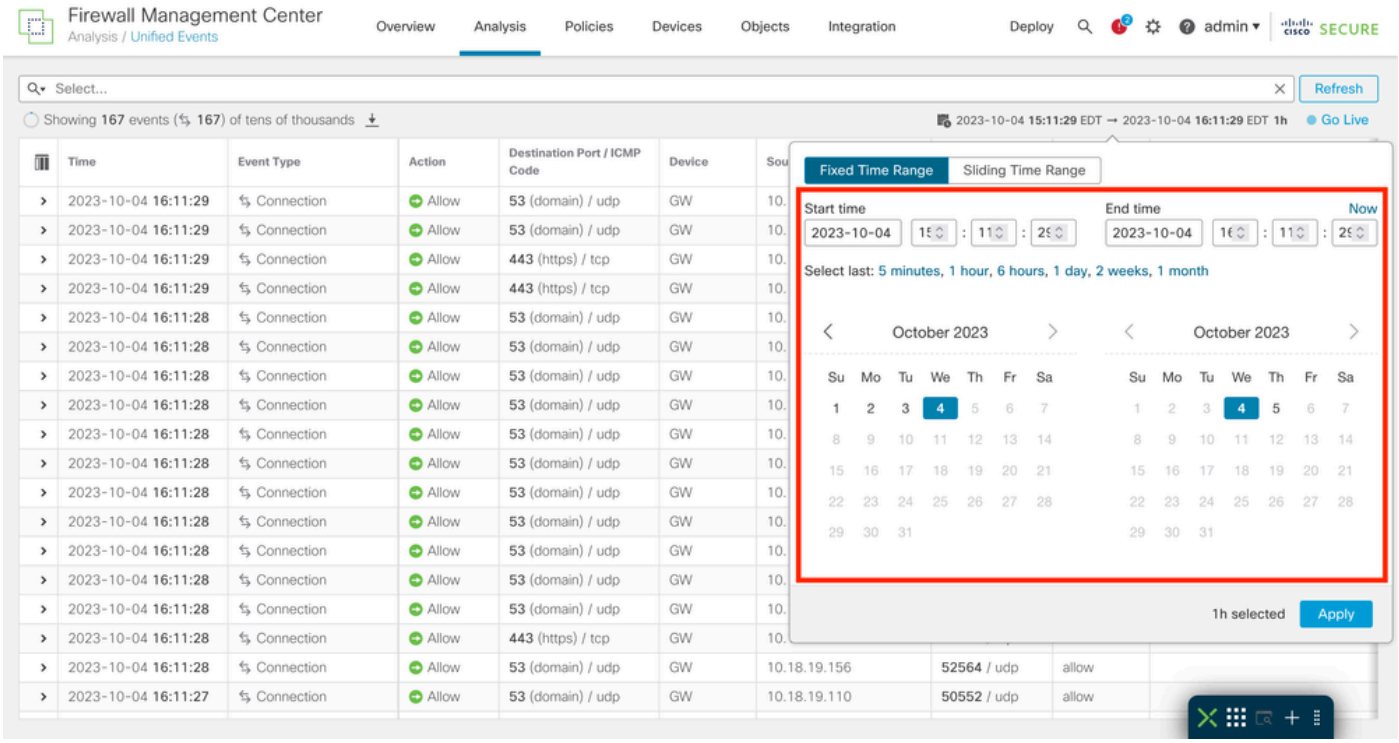
Finestra temporale

È più semplice restringere gli eventi rilevanti in base a un tempo specifico modificando la finestra temporale.

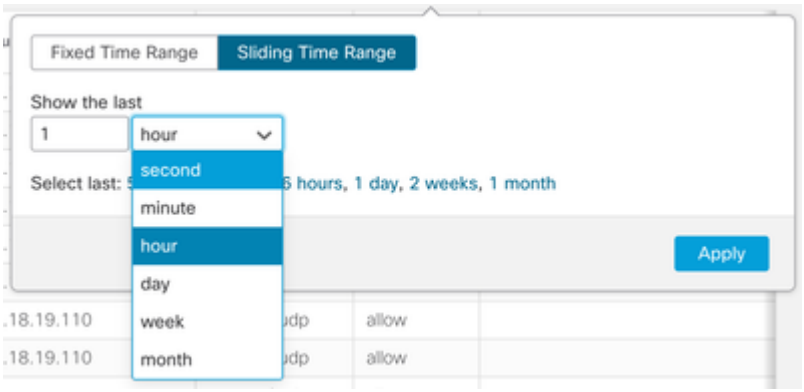
Passaggio 1. Per modificare il frame della finestra degli eventi, fare clic su un intervallo di date.



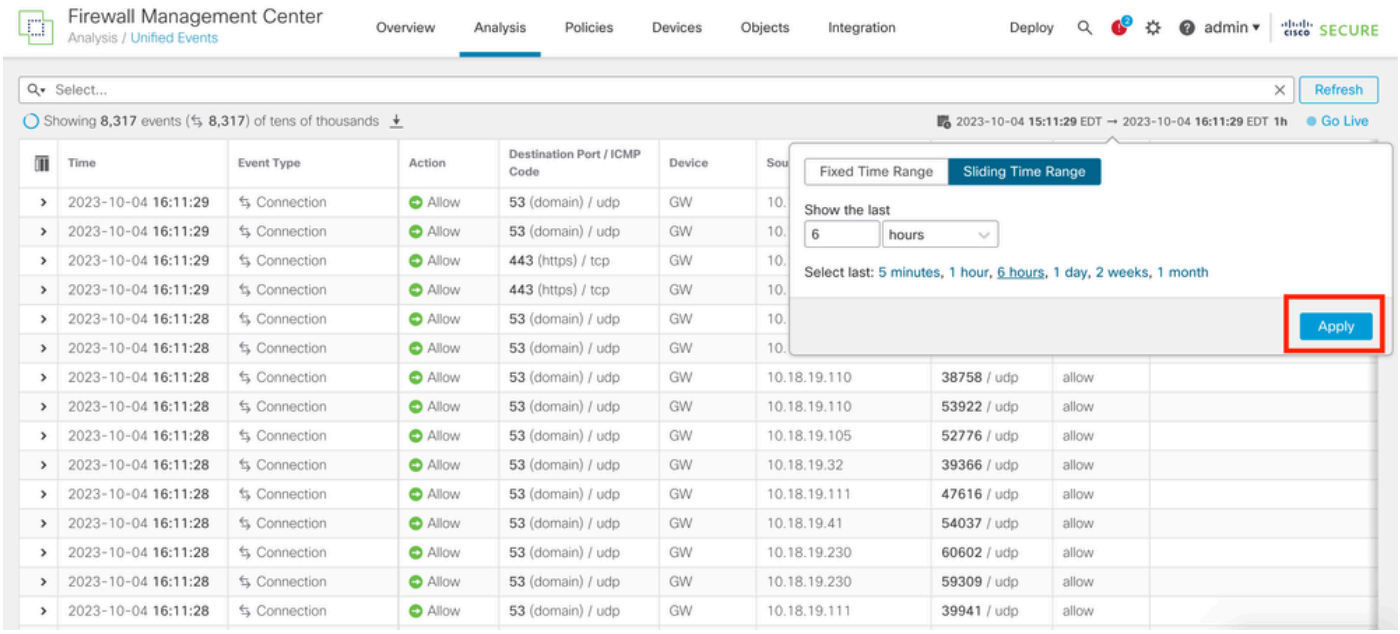
Passaggio 2. Selezionare l'intervallo di tempo nella finestra popup.



Passaggio 3. (Facoltativo) Utilizzare Intervallo di tempo scorrevole per visualizzare gli eventi da un'ora specifica all'ora corrente.



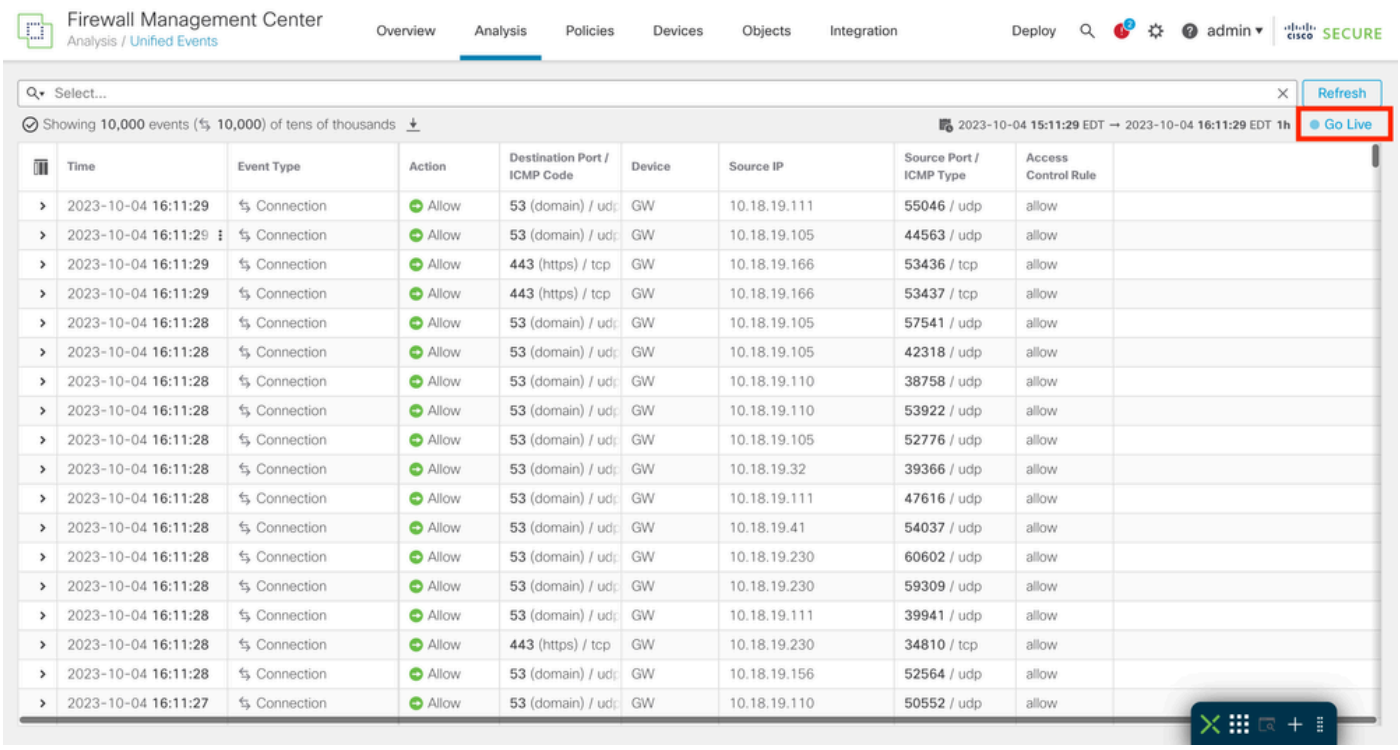
Passaggio 4. Fare clic su Apply per filtrare gli eventi nell'intervallo di tempo configurato.



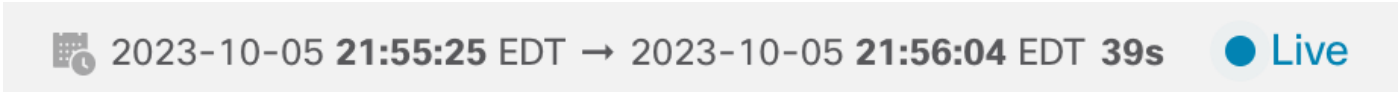
Vai in diretta

È possibile attivare la funzione Go Live per visualizzare gli eventi in tempo reale. Gli eventi vengono visualizzati nel momento in cui vengono generati.

Per abilitarla, fai clic su Go Live.



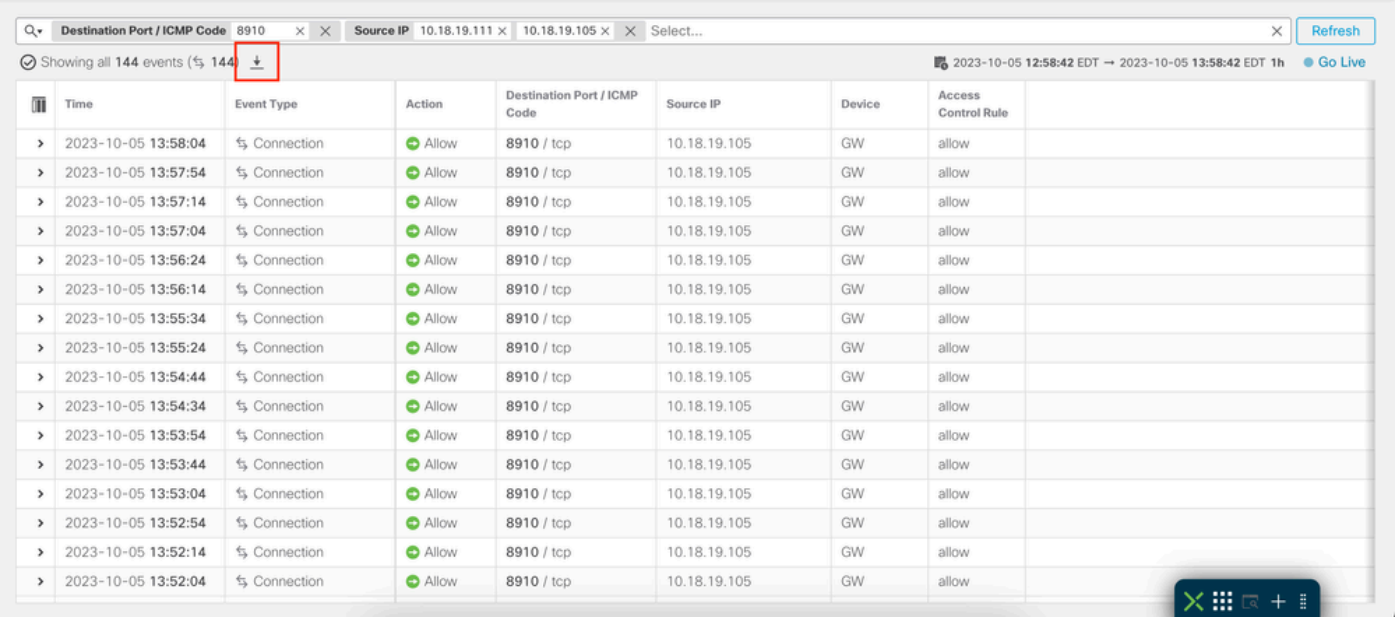
Una volta attivata, viene visualizzata la parola Live.



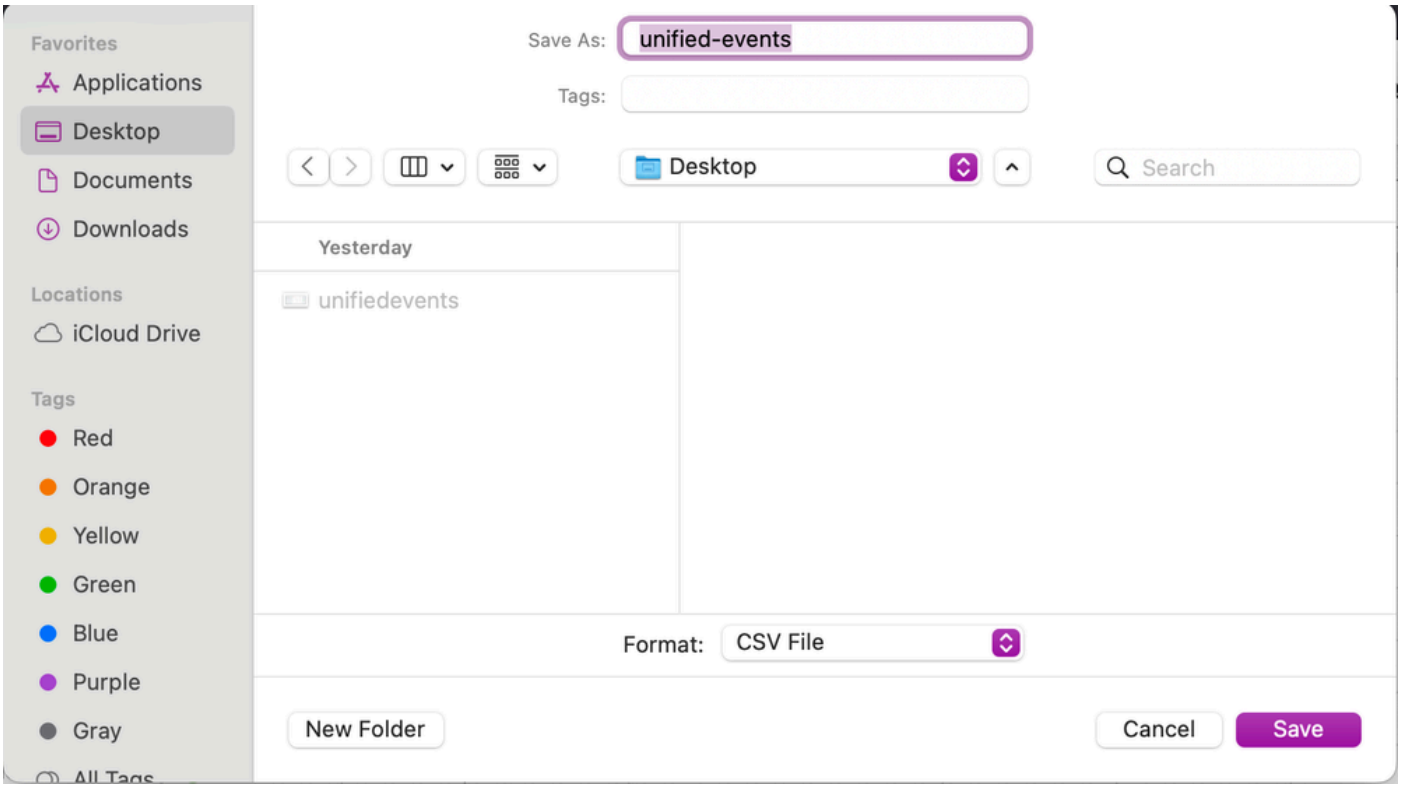
⚠ Attenzione: Quando Live è abilitato, non è possibile modificare la finestra temporale. Per modificare la finestra temporale, disattivate prima l'opzione Dal vivo facendovi nuovamente clic sopra.

Scarica eventi come Valori delimitati da virgole (CSV)

Passaggio 1. Fare clic sull'icona di download per generare un file contenente gli eventi attualmente visualizzati nella pagina.



2. Selezionare la cartella di download, il nome e fare clic su Save (Salva).



Passaggio 3. Verificare il file CSV.

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

Informazioni correlate

- Utilizzo del Visualizzatore eventi unificato
- Cisco Secure Firewall - Visualizzatore eventi unificato: Suggerimenti
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).