

Monitor Events Using Unified Event Viewer on FMC GUI

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Explore](#)

[Example of the Unified Event Page](#)

[Review Events](#)

[Personalize Columns](#)

[Save Column Set](#)

[Event Search](#)

[Save Search](#)

[Time Window](#)

[Go Live](#)

[Download Events as Comma-separated Values \(CSV\)](#)

[Related Information](#)

Introduction

This document describes the use of Unified Event Viewer on a graphical user interface (GUI) on Firewall Management Center (FMC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Access to FMC with Admin or Security Analyst privileges
- FMC with version equal or higher than v7.0

Components Used

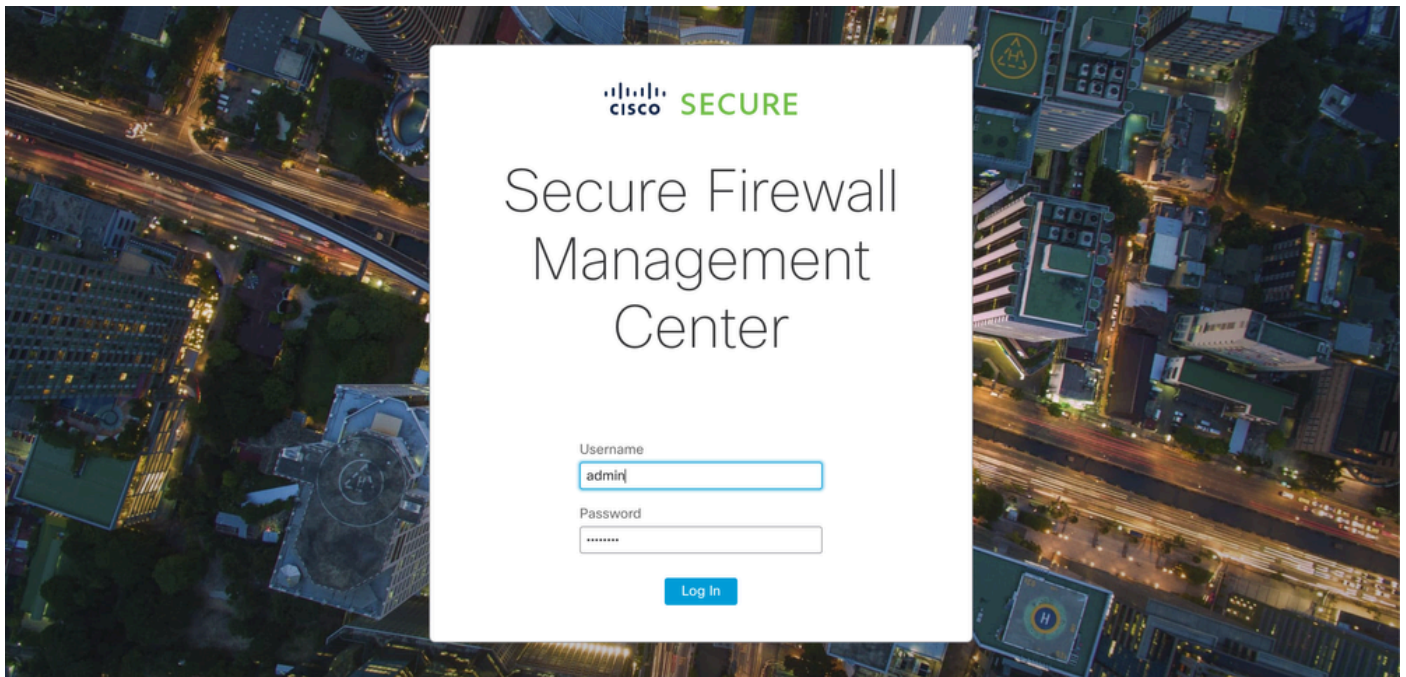
The information in this document is based on these software and hardware versions:

- Secure Firewall Management Center for VMware v7.2.5

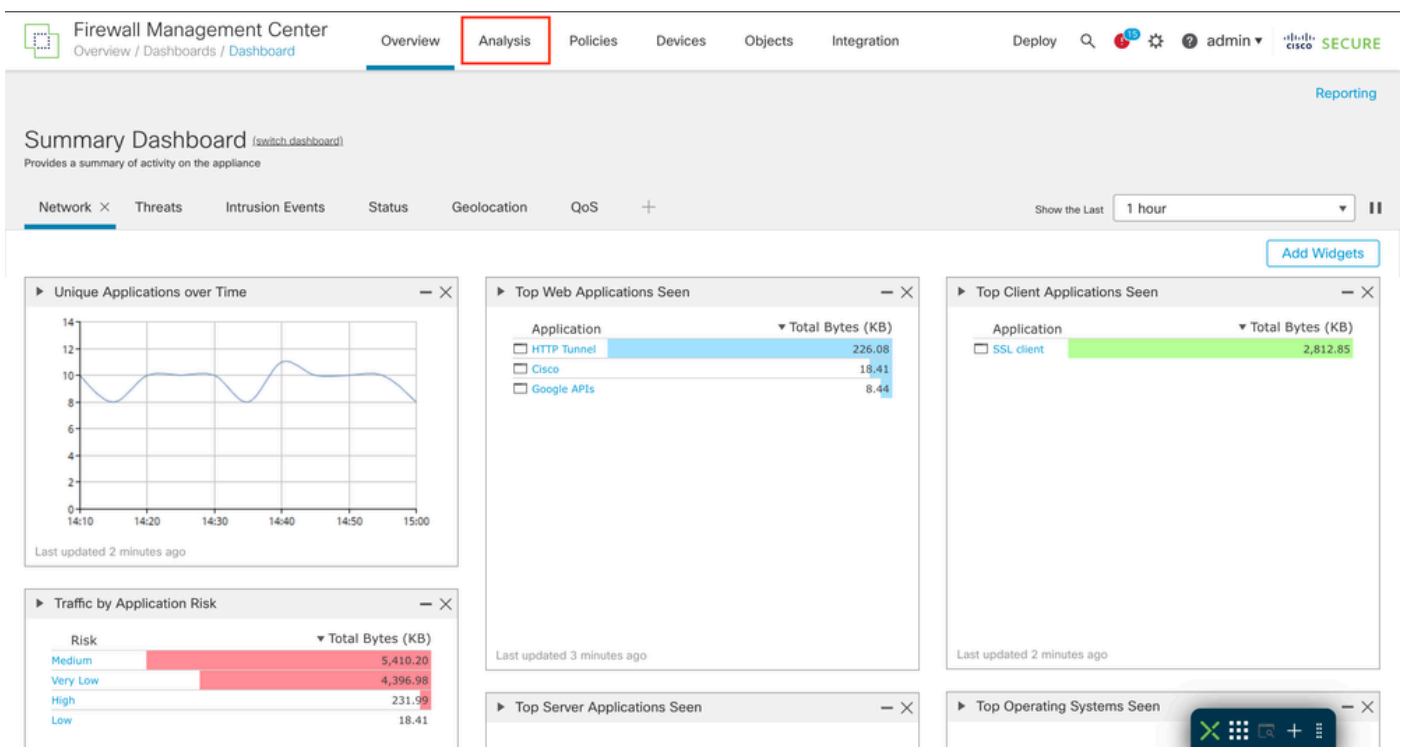
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Explore

Step 1. Log into the FMC GUI.



Step 2. Navigate to the **Analysis** tab.



Step 3. From the drop-down menu, click on **Unified Events**.

Firewall Management Center
Overview / Dashboards / Dashboard

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? admin 🔒 cisco SECURE

Summary Dashboard (switch dashboard)
Provides a summary of activity on the appliance

Network Threats Intrusion Events Status

Unique Applications over Time
Last updated 2 minutes ago

Traffic by Application Risk

Context Explorer

- Unified Events

Connections

- Events
- Security-Related Events

Intrusions

- Events
- Reviewed Events

Files

- Malware Events
- File Events
- Captured Files
- Network File Trajectory

Hosts

- Network Map
- Hosts
- Indications of Compromise
- Applications
- Application Details
- Servers
- Host Attributes
- Discovery Events
- Vulnerabilities
- Third-Party Vulnerabilities

Users

- Indications of Compromise
- Active Sessions
- Users
- User Activity

Correlation

- Correlation Events
- Allow List Events
- Allow List Violations
- Status

Advanced

- Custom Workflows
- Custom Tables
- Geolocation
- URL
- Whois
- Contextual Cross-launch
- Search

Reporting

Total Bytes (KB)
2,812.85

Add Widgets

Example of the Unified Event Page

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? admin 🔒 cisco SECURE

Select...

Showing 10,000 events (of 10,000) of tens of thousands

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
> 2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
> 2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
> 2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
> 2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
> 2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
> 2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
> 2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
> 2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
> 2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
> 2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
> 2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
> 2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
> 2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
> 2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
> 2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
> 2023-10-04 16:11:28	Connection	Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
> 2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
> 2023-10-04 16:11:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

Review Events

Step 1. Click on the > icon.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | 🔒 cisco SECURE

Q Select... Refresh

Showing 10,000 events (of 10,000) of tens of thousands 2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
2023-10-04 16:11:28	Connection	Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
2023-10-04 16:11:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

Step 2. The detailed information of the event is shown.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | 🔒 cisco SECURE

Q Select... Refresh

Showing 10,000 events (of 10,000) of tens of thousands 2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow

Event Type: Connection

Time: 2023-10-04 16:11:29

Last Packet: 2023-10-04 16:11:39

Action: Allow

Source IP: 10.18.19.111

Source User: Not Found

Destination IP: 10.1.8.107

Ingress Security Zone: inside

Egress Security Zone: outside

Source Port / ICMP Type: 55046 / udp

Destination Port / ICMP Code: 53 (domain) / udp

Client Application: DNS

Business Relevance: Very High

DNS Query: cloud-sa.amp.cisco.com

DNS Response: No Error

DNS Record Type: A

Intrusion Events: 0

Files: 0

Access Control Policy: t

Access Control Rule: allow

Network Analysis Policy: Balanced Security and Connectivity

Prefilter Policy: allow

QoS Policy: test

Domain: Global

Ingress Virtual Router: Global

Egress Virtual Router: Global

Initiator Packets: 2

Responder Packets: 0

QoS-Dropped Initiator Packets: 0

QoS-Dropped Responder Packets: 0

Initiator Bytes: 164

Responder Bytes: 0

QoS-Dropped Initiator Bytes: 0

QoS-Dropped Responder Bytes: 0

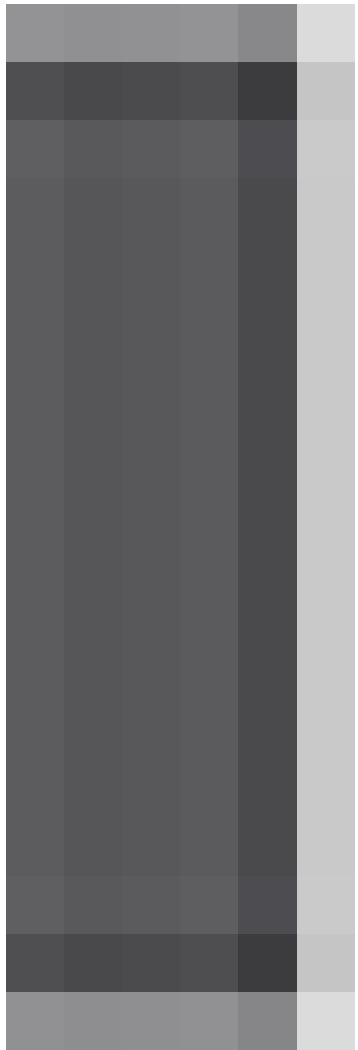
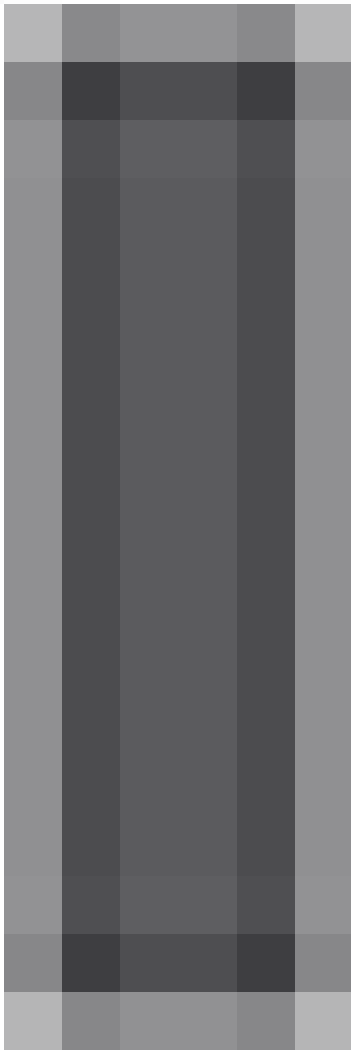
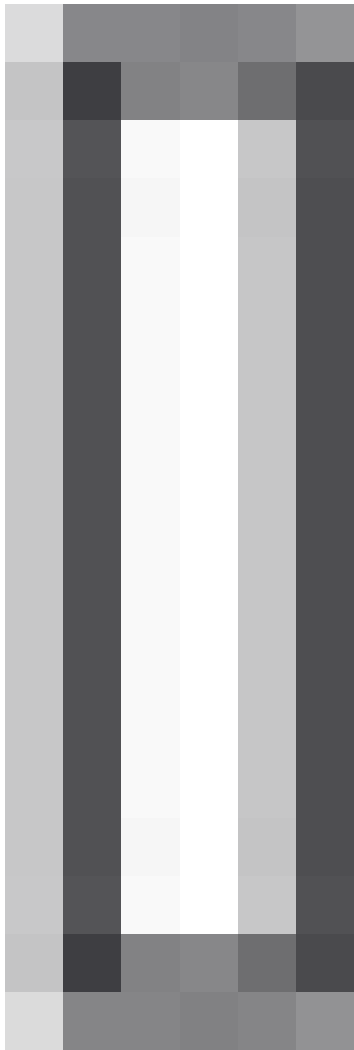
Detection Type: AppID

NAT Source IP: 10.88.243.43

2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow

Personalize Columns

Step 1. Click on the icon



Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

Showing 10,000 events (of 10,000) of tens of thousands

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
2023-10-04 16:11:28	Connection	Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
2023-10-04 16:11:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

Step 2. Select the event fields that you want on the table.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

Showing 10,000 events (of 10,000) of tens of thousands

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Ap
		Allow		10.18.19.111	10.1.8.107	55046 / udp	53 (domain) / udp	
		Allow		10.18.19.105	10.1.20.51	44563 / udp	53 (domain) / udp	
		Allow		10.18.19.166	142.250.72.202	53436 / tcp	443 (https) / tcp	
		Allow		10.18.19.166	142.250.72.202	53437 / tcp	443 (https) / tcp	
		Allow		10.18.19.105	10.27.20.51	57541 / udp	53 (domain) / udp	
		Allow		10.18.19.105	10.1.20.51	42318 / udp	53 (domain) / udp	
		Allow		10.18.19.110	10.1.9.38	38758 / udp	53 (domain) / udp	
		Allow		10.18.19.110	10.1.8.101	53922 / udp	53 (domain) / udp	
		Allow		10.18.19.105	10.27.20.51	52776 / udp	53 (domain) / udp	
		Allow		10.18.19.32	208.67.220.220	39366 / udp	53 (domain) / udp	
		Allow		10.18.19.111	10.1.8.101	47616 / udp	53 (domain) / udp	
		Allow		10.18.19.41	208.67.220.220	54037 / udp	53 (domain) / udp	
		Allow		10.18.19.230	173.37.87.157	60602 / udp	53 (domain) / udp	
		Allow		10.18.19.230	173.37.87.157	59309 / udp	53 (domain) / udp	
		Allow		10.18.19.111	10.1.8.101	39941 / udp	53 (domain) / udp	

Saved Column Sets

Select...

Filter columns

Select none | Select default

- Event Type
- Action
- Reason
- Source IP
- Destination IP
- Source Port / ICMP Type
- Destination Port / ICMP Code

Revert | 11 selected | Apply

















Step 3. (Optional) Search for the field to make navigation easier.

Saved Column Sets

Select...

Source

Select 14 filtered | Select default

<input checked="" type="checkbox"/>	Source IP	    
<input checked="" type="checkbox"/>	Source Port / ICMP Type	    
<input type="checkbox"/>	NAT Source IP	 
<input type="checkbox"/>	NAT Source Port	 
<input type="checkbox"/>	NetFlow Source Autonomous System	 

Revert 7 selected Apply

















Step 4. Click on an event field to disable or enable.

Saved Column Sets

Select...

Source

Select 14 filtered | Select default

<input checked="" type="checkbox"/>	Source IP	    
<input type="checkbox"/>	Source Port / ICMP Type	    
<input type="checkbox"/>	NAT Source IP	 
<input type="checkbox"/>	NAT Source Port	 
<input type="checkbox"/>	NetFlow Source Autonomous System	 

Revert 6 selected Apply

Step 5. Click on **Apply**.

Saved Column Sets

Select...

Filter columns

Select none | Select default

Event Type

Action

Destination Port / ICMP Code

Source IP

Device

Revert

6 selected

Apply

Step 6. (Optional) You can reposition the columns by dragging each one to a different location.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | SECURE

Showing 10,000 events (of 10,000) of tens of thousands

2023-10-05 12:02:15 EDT → 2023-10-05 13:02:15 EDT 1h

Time	Event Type	Action	Destination Port / ICMP Code	Source IP	Device	Access Control Rule
2023-10-05 13:02:15	Connection	Allow	53 (domain) / udp	10.18.1	GW	allow
2023-10-05 13:02:15	Connection	Allow	53 (domain) / udp	10.18.19.110	GW	allow
2023-10-05 13:02:15	Connection	Allow	443 (https) / tcp	10.18.19.230	GW	allow
2023-10-05 13:02:15	Connection	Allow	53 (domain) / udp	10.18.19.32	GW	allow
2023-10-05 13:02:14	Connection	Allow	53 (domain) / udp	10.18.19.105	GW	allow
2023-10-05 13:02:14	Connection	Allow	53 (domain) / udp	10.18.19.111	GW	allow
2023-10-05 13:02:14	Connection	Allow	53 (domain) / udp	10.18.19.111	GW	allow
2023-10-05 13:02:14	Connection	Allow	443 (https) / tcp	10.18.19.230	GW	allow
2023-10-05 13:02:14	Connection	Allow	53 (domain) / udp	10.18.19.105	GW	allow
2023-10-05 13:02:14	Connection	Allow	443 (https) / tcp	10.18.19.230	GW	allow
2023-10-05 13:02:14	Connection	Allow	443 (https) / tcp	10.18.19.230	GW	allow
2023-10-05 13:02:14	Connection	Allow	443 (https) / tcp	10.18.19.166	GW	allow
2023-10-05 13:02:13	Connection	Allow	53 (domain) / udp	10.18.19.110	GW	allow
2023-10-05 13:02:13	Connection	Allow	53 (domain) / udp	10.18.19.230	GW	allow
2023-10-05 13:02:13	Connection	Allow	443 (https) / tcp	10.18.19.166	GW	allow
2023-10-05 13:02:13	Connection	Allow	443 (https) / tcp	10.18.19.166	GW	allow

Save Column Set

Step 1. Click on **Saved Column Sets**.

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'Integration', 'Deploy', and 'admin'. The main content area displays a table of events with columns: Time, Event Type, Action, Reason, Source IP, Destination IP, Source Port / ICMP Type, Destination Port / ICMP Code, and Web Ac. A dropdown menu titled 'Saved Column Sets' is open, showing a 'Select...' option. Below the dropdown is a 'Filter columns' search bar and a list of columns with checkboxes: Event Type, Action, Reason, Source IP, Destination IP, Source Port / ICMP Type, and Destination Port / ICMP Code. The 'Apply' button is highlighted.

Step 2. Click on **Create column set from current selection**.

The screenshot shows the same Firewall Management Center interface. The 'Saved Column Sets' dropdown menu is open, showing 'Rule match' and 'Saved Column Set 1' options. The 'Create column set from current selection' option is highlighted with a red box. The table below shows columns: Time, Event Type, Action, Destination IP, Destination Port / ICMP Code, Device, Source IP, Source Port / ICMP Type, and Access Control Rule. The 'Apply' button is highlighted.

Step 3. (Optional) Change the name of column set.

Saved Column Sets

Select...

2 saved column sets

Rule match ✓

Time Event Type Action Reason Source IP Destination IP S

Saved Column Set 1

Time Event Type Action Reason Source IP Destination IP S

+ Create column set from current selection

NetFlow Source Autonomous System ↔️ 🗑️

NetFlow Source Prefix ↔️ 🗑️

Revert 6 selected Apply

Step 4. You can edit an existing set by clicking on the ellipsis (...).

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin 🔒 cisco SECURE

Showing 10,000 events (of 10,000) of tens of thousands

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Destination IP	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
ow			10.1.8.107	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
ow			10.1.20.51	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
ow			142.250.72.202	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
ow			142.250.72.202	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
ow			10.27.20.51	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
ow			10.1.20.51	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
ow			10.1.9.38	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
ow			10.1.8.101	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
ow			10.27.20.51	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
ow			208.67.220.220	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
ow			10.1.8.101	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
ow			208.67.220.220	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
ow			173.37.87.157	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
ow			173.37.87.157	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
ow			10.1.8.101	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow

Saved Column Sets

Rule match

2 saved column sets

Rule match

Time Event Type Action Reason Source IP Destination IP S

Saved Column Set 1

Time Event Type Action Reason Source IP Destination IP S

+ Create column set from current selection

Rename

Delete

Overwrite

Source IP

Destination IP

Source Port / ICMP Type

Destination Port / ICMP Code

Revert 11 selected Apply

Event Search

Step 1. To begin searching for specific events click on **Select**.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? admin | cisco SECURE

Q Select... Refresh

Showing 10,000 events (🔗 10,000) of tens of thousands

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
2023-10-04 16:11:27	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

Step 2. Select the field where you want to apply the filter.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? admin | cisco SECURE

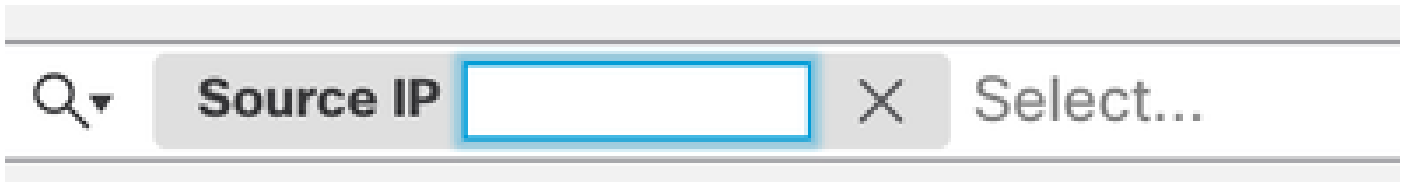
Q source Refresh

📄 NAT Source IP
📄 NAT Source Port
📄 NetFlow Source Autonomous System
📄 NetFlow Source Prefix
📄 NetFlow Source ToS
📄 Source Continent
📄 Source Country
📄 Source Device
📄 Source Host Criticality
📄 Source IP

ds

Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
🟢 Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
🟢 Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
🟢 Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
🟢 Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
🟢 Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

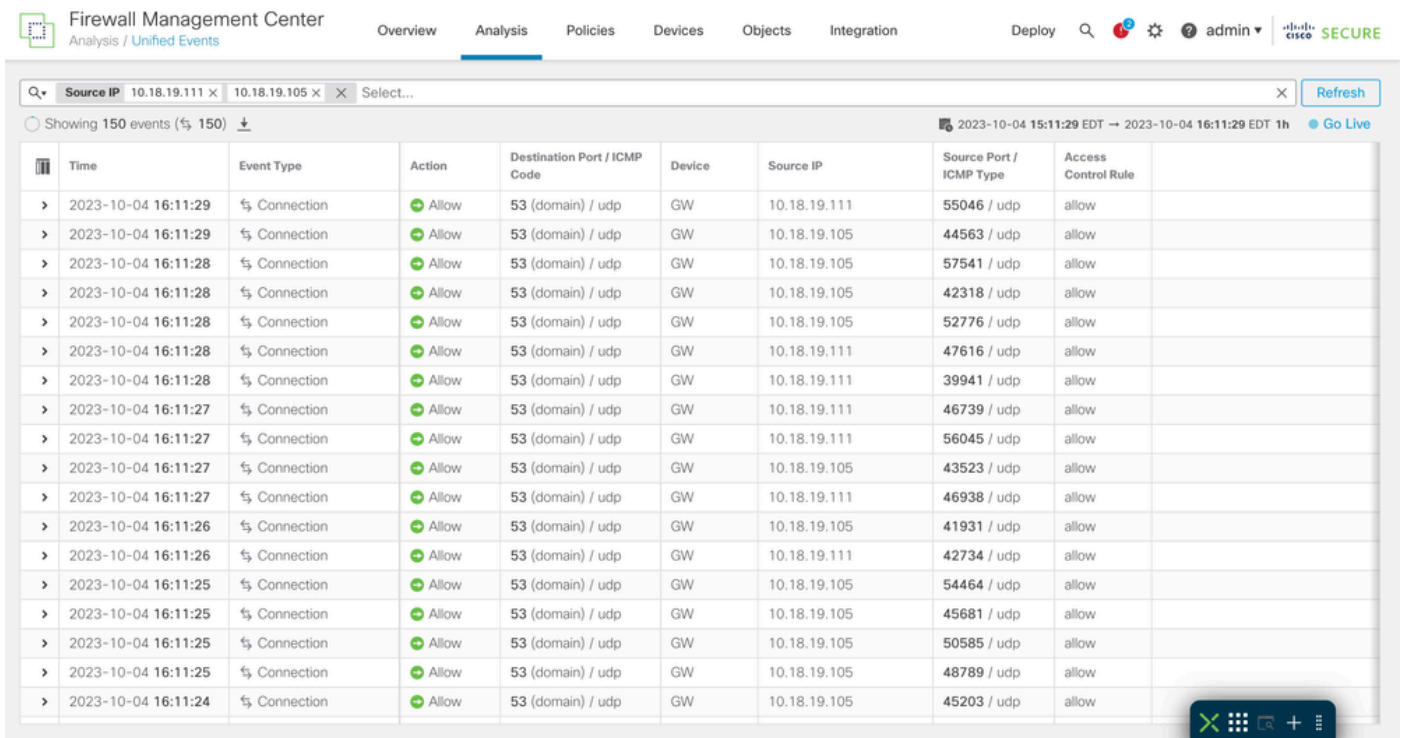
Step 3. Write the values to use as filter.



Step 4. Click on **Apply**, to configure the filter.



Step 5. (Optional) You can add multiple values to each filter.



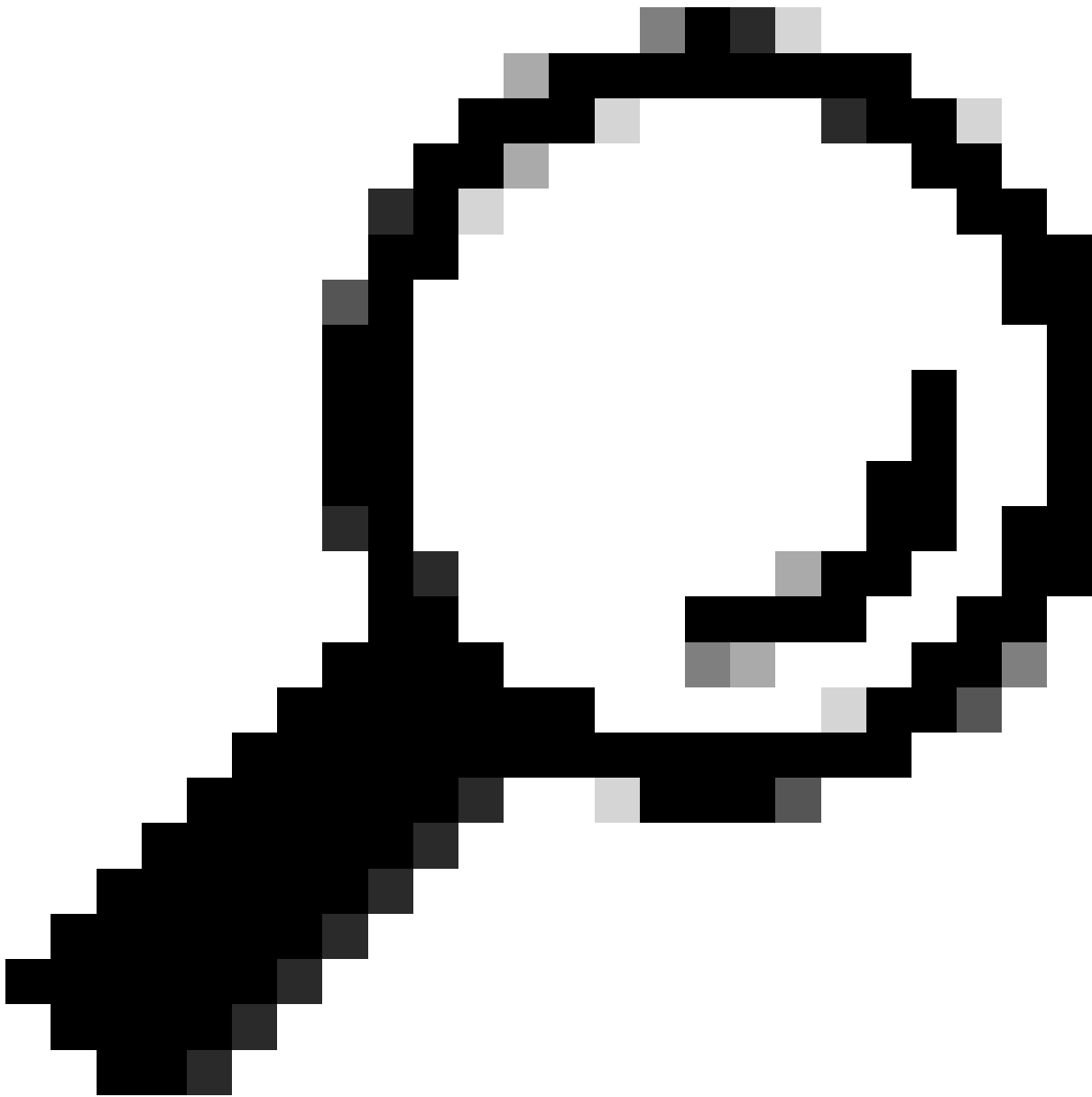
Step 6. (Optional) Add as many filters as you need.

Source IP 10.18.19.111 x 10.18.19.105 x Destination Port / ICMP Code 8910 x Select... Refresh

Showing all 106 events (🔍 106) ⌵ 2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:01	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50786 / tcp	allow
2023-10-04 16:10:51	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45442 / tcp	allow
2023-10-04 16:10:11	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50784 / tcp	allow
2023-10-04 16:10:01	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45440 / tcp	allow
2023-10-04 16:09:21	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50782 / tcp	allow
2023-10-04 16:09:11	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45438 / tcp	allow
2023-10-04 16:08:31	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50780 / tcp	allow
2023-10-04 16:08:21	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45436 / tcp	allow
2023-10-04 16:07:41	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50778 / tcp	allow
2023-10-04 16:07:31	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45434 / tcp	allow
2023-10-04 16:06:51	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50776 / tcp	allow
2023-10-04 16:06:41	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45432 / tcp	allow
2023-10-04 16:06:01	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50774 / tcp	allow
2023-10-04 16:05:51	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45430 / tcp	allow
2023-10-04 16:05:11	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50772 / tcp	allow
2023-10-04 16:05:01	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45428 / tcp	allow
2023-10-04 16:04:21	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50770 / tcp	allow
2023-10-04 16:04:11	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45426 / tcp	allow





Tip: You can use operators (>,<,!, and so on) while writing the values.

Save Search

It is possible to save searches so you can reuse the filters you have created.

Step 1. Click on the magnifying glass icon.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

Source IP 10.18.19.111 x 10.18.19.105 x Destination Port / ICMP Code 8910 x Select... Refresh

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Device Source IP Source Port / ICMP Type Access Control Rule

1 Filter Condition
Action = !Allow

1 saved search

Find saved search

Saved search 1

10.18.19.111/10.18.19.105 | 8910

+ Save search

Time Window

It is easier to narrow relevant events, based on a specific time, by modifying the time window.

Step 1. To modify the window frame of events, click on date range.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

Select... Refresh

Showing 10,000 events (of 10,000) of tens of thousands

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
2023-10-04 16:11:28	Connection	Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
2023-10-04 16:11:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

Step 2. Select the range of time in the pop-up window.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? admin | **SECURE**

Q Select... Refresh

Showing 8,317 events (🔗 8,317) of tens of thousands ⌵ 2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h **Go Live**

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
2023-10-04 16:11:27	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

Fixed Time Range Sliding Time Range

Show the last
6 hours

Select last: 5 minutes, 1 hour, 6 hours, 1 day, 2 weeks, 1 month

Apply

Go Live

You can enable the Go Live feature to show events in real time. The events appear as they are generated.

To enable, click on **Go Live**.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? admin | **SECURE**

Q Select... Refresh

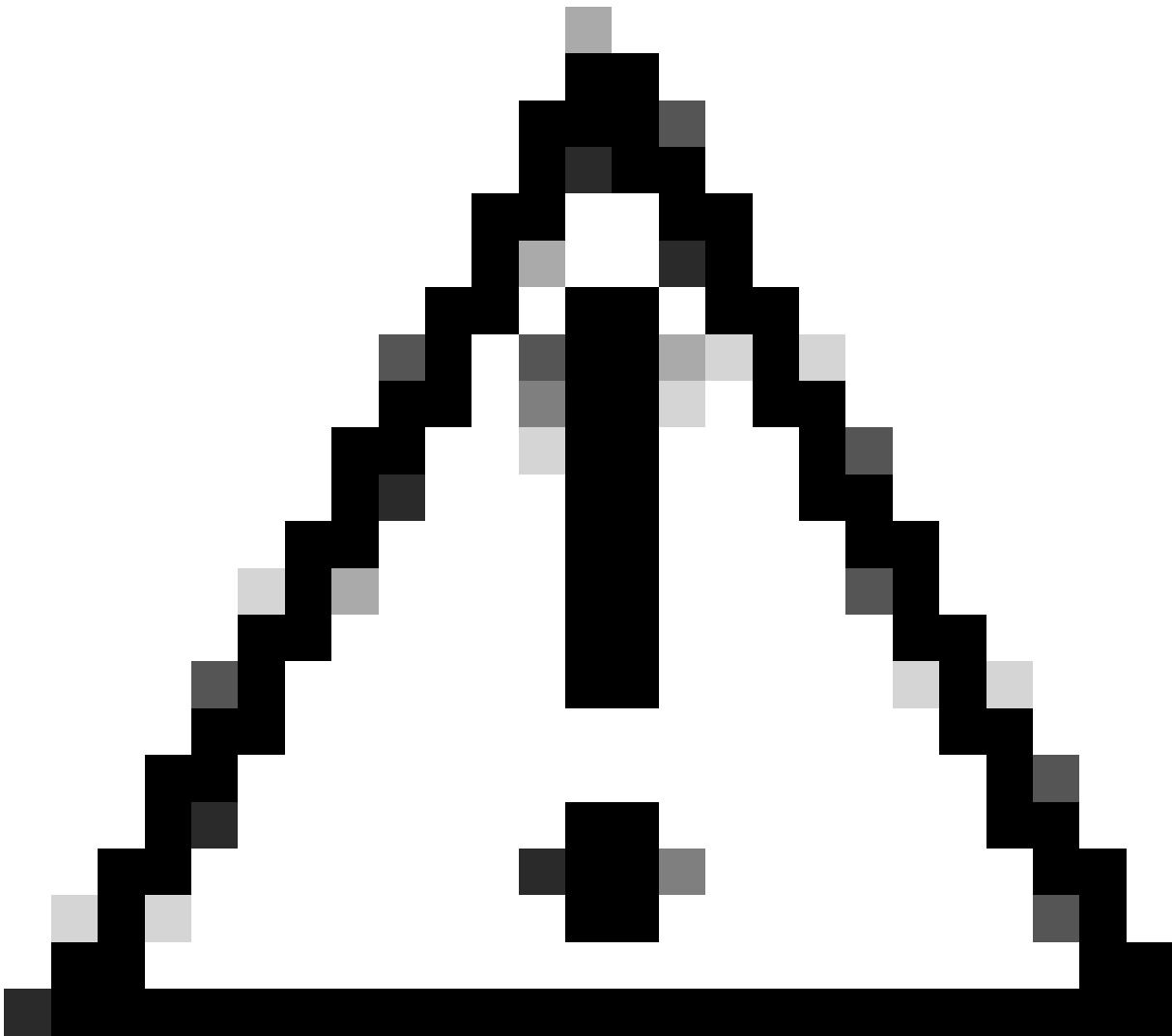
Showing 10,000 events (🔗 10,000) of tens of thousands ⌵ 2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h **Go Live**

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
2023-10-04 16:11:27	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

Go Live

Once it is enabled, it displays the word **Live**.

🕒 2023-10-05 21:55:25 EDT → 2023-10-05 21:56:04 EDT 39s **Live**



Caution: When Live is enabled it is not possible to modify the time window. In order to modify the time window, first disable Live option by clicking on it again.

Download Events as Comma-separated Values (CSV)

Step 1. Click on the download icon to generate a file containing the events currently showing on the page.

Showing all 144 events (🔍 144) ↓ 2023-10-05 12:58:42 EDT → 2023-10-05 13:58:42 EDT 1h [Go Live](#)

Time	Event Type	Action	Destination Port / ICMP Code	Source IP	Device	Access Control Rule
2023-10-05 13:58:04	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:57:54	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:57:14	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:57:04	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:56:24	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:56:14	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:55:34	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:55:24	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:54:44	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:54:34	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:53:54	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:53:44	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:53:04	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:52:54	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:52:14	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:52:04	🔗 Connection	🟢 Allow	8910 / tcp	10.18.19.105	GW	allow

Step 2. Select the download folder, name and click on **Save**.

Save As: ↓

Tags:

Navigation: < > [Grid] [List] Desktop ↓ ^ Search

Yesterday

- unifiedevents

Format: ↓

Step 3. Verify the CSV file.

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

Related Information

- [Working with the Unified Event Viewer](#)
- [Cisco Secure Firewall - Unified Events Viewer: Tips & Tricks](#)
- [Cisco Technical Support & Downloads](#)