

Unified Events

- Unified events, on page 1
- Requirements for using unified events, on page 1
- Work with unified events, on page 2
- Set a time range in unified events, on page 4
- Enable live event monitoring in unified events, on page 5
- Filters in unified events, on page 6
- Unified events column details, on page 7

Unified events

Unified Events is a firewall event monitoring feature in Firewall Management Center that:

- Provides a single-screen view of various firewall event types, including connection, intrusion, file, malware, and security-related connection events.
- Stacks related events together in the table to provide more context about the security incident.
- Correlates associated events so that you can better understand and troubleshoot network issues without toggling between multiple event viewers.

The **Unified Events** table is highly customizable. You can create and apply custom filters to fine-tune the information displayed on the event viewer. You can save custom filters for specific needs that you use often, and quickly load these saved filters. You can customize the event table by adding, removing, pinning, or reordering columns.

Requirements for using unified events

Before using **Unified Events** in the Firewall Management Center, ensure you meet these requirements.

- You must configure the necessary policies and enable logging settings on your devices to generate security events and display them on the **Unified Events** page.

Work with unified events

View and work with various firewall event types in a single table without needing to switch between multiple event viewers.

Use this view to:

- Look for relationships between events of different types in the unified view.
- See the effects of policy changes in real time.

Before you begin

You must have Admin or Security Analyst privileges to perform this task.

Procedure

Step 1 Choose **Analysis** > **Unified Events**.

Step 2 Choose the time range (fixed or sliding).

For more information, refer to Set a time range in unified events, on page 4.

Step 3 If you are storing events remotely on a Secure Network Analytics appliance and you have good reason to change the data source, choose a data source.

See important information at Work in the Secure Firewall Management Center with Connection Events Stored on a Secure Network Analytics Appliance.

Step 4 You can filter the vast list of firewall events that the unified events table initially displays for a more granular contextual picture of events in your network.

For more information, refer to Filters in unified events, on page 6.

Step 5 Choose more options:

To do this ...	Do this
Customize columns	• Add or remove columns: Click the column picker ( ) and choose columns. Values in some fields depend on the event type. The following icons that appear next to each field indicate the event type correspondence: • Connection event ( ) • Security-related connection event ( ) • Intrusion event ( ) • File event ( ) • Malware event ( ) Click the event icon next to the column set filtering options to filter the list of event fields according to the selected event type. **Note** Including many columns may degrade performance. You can view data for hidden columns by expanding an event row to view event details. • Reorder columns: Drag and drop the column heading. • Pin (freeze) columns to the left or right side of the table so they do not scroll: • Drag a column all the way to either left or right side of the table or drag and drop a column heading into the pinned area. • To unpin a column, drag the column out of the pinned area. • Resize columns. • Revert columns to the default setting. Data is always sorted by time, with the most recent events on top.
Identify related events	Click a row to highlight other events that are related to this event. If needed, filter the events to display a small enough set of events. **Note** The initiator of a connection is not necessarily the same as the sender of a malware file. Search for the file or malware event associated with a connection event by filtering the unified events table with the **Source or Destination IP** filter.

To do this ...	Do this
View event details	Click the > (Expand) icon at the left end of the row. Event details do not include the field which has no data to display. **Tip** Alternatively, double-click on an event row to view the **Event Details** pane. When the **Event Details** pane is open, click on any event row in the table to load the details of that event.
View events in real time	Click **Go Live**. For more information, refer to Enable live event monitoring in unified events, on page 5. If events stream too quickly, enter filter criteria.
Cross-launch to external resources	Click the ellipsis (⋮) in a table cell to see the options available for that cell value, if any. For more information, refer to Event investigation using web-based resources.
Open multiple unified events windows	• Open unified events table in multiple browser tabs or windows to view different filtered data simultaneously. • Each new tab or window has the characteristics of the most recently modified tab or window. • To make any open tab or window as the template, make a minor change to it. • The system processes queries on multiple tabs sequentially. • Depending on the view (complex queries, or viewing in live view mode when the incoming event rate is high, for example), you may experience slower performance if more than 4 tabs are open simultaneously.
Bookmark or share query results	Bookmark or copy-paste the URL in the browser window. • The URL retrieves different events later if it uses the sliding time range. • The URL does not capture column visibility, size and order, and real-time streaming settings.

Set a time range in unified events

Set a time range in unified events to view firewall events for a specific period and control which events are displayed in the table.

When you change the time range, the unified events table automatically refreshes to reflect your changes. The time range that you select does not apply to other tables in the event viewer. For example, a time range that you select when viewing connection events does not apply to the unified events table and vice versa.

Note If your time window extends back beyond the retention period for connection events, look for Security-Related Connection events in the tables under **Analysis** > **Connections** > **Security Intelligence Events** .

Procedure

Step 1 Choose **Analysis** > **Unified Events**.

By default, the unified events table displays events from the past hour.

Step 2 Click the current time range.

Step 3 Choose one of the following:

- If you want to see events for a fixed time range, click **Fixed Time Range** and choose the **Start time** and **End time**.

  To set the current time as the **End time**, click **Now**.

- If you want a sliding default time window (such as last one hour), select **Sliding Time Range** and specify the desired length.

  The table displays all the events generated from a specific start time—for example, the past hour—relative to the present. Refreshing the view ensures the window always displays events from the most recent hour of activity.

Step 4 Click **Apply**.

Enable live event monitoring in unified events

Configure **Unified Events** to display firewall events in real time, eliminating the need for manual refreshes.

When live view mode is active, the event logs appear in real time as the security event occurs in your network. This enables you to identify and resolve security incidents quickly.

Procedure

Step 1 Choose **Analysis** > **Unified Events**.

By default, the **Unified Events** table displays historical events from the past hour.

Step 2 Click **Go Live** to start real-time viewing of new events.

New events are displayed at the top of the events table. The time range section includes a timer that indicates the length of time live view has been active.

Note
When using the **Go Live** feature, this limitation applies for the UDP traffic:

- By default, the **Go Live** feature in Firewall Management Center considers traffic data from the last 30 seconds, which is shorter than the 120 seconds required for UDP connections to be processed to include in **Unified Events** table. This may cause UDP events to appear incomplete in the **Unified Events** table.
- Configure logging at the beginning of the connection for UDP traffic to improve visibility.

What to do next

To exit the live view mode, click **Live**.

Filters in unified events

The **Unified Events** table displays firewall events from the past hour. Use these steps to filter and narrow the view for more granular analysis of your network traffic.

Filters help you quickly access critical information. For example, if you want to monitor application access for specific users, you can apply search criteria to isolate relevant firewall logs. The event viewer displays only the entries that match your criteria.

You can use both inclusion and exclusion criteria to refine your search results effectively.

Procedure

Step 1 Choose **Analysis** > **Unified Events**.

Step 2 Enter the filter criteria:

- To manually enter the filter criteria:
  1. **a.** Enter filter criteria in the search field, or select a filter from the drop-down list.
  2. **b.** Enter the value for the selected filter criteria. Suggestions will appear in the drop-down list as you type.
- To pick the filter criteria from the table, click the dots in a cell and choose an option to include or exclude that value from your filter criteria.

  Tip
  - Use the **`Ctrl+click`** (Windows) or **`Command-click`** (Mac) key to quickly add an inclusion filter criteria.
  - Use the **`Alt+click`** (Windows) or **`Option-click`** (Mac) key to quickly add an exclusion filter criteria.
- Refine your filter criteria. For information about wildcards and search behavior, see Event searches.
- Include operators (such as <, >, !) in the value field, preceding the value. For example, enter **`!Allow`** in the **Action** field to find all events with an action other than Allow.

Step 3 Perform the search.

Tip
You can use the **Ctrl+Enter** (Windows) or **Command-Enter** (Mac) key command to initiate a search.

Events in the unified events table are not aggregated when the displayed columns all hold identical values. Every event matching your filter criteria is listed individually.

The unified events table displays filtered results based on your criteria, showing only the events that match your inclusion and exclusion filters for more targeted analysis.

Unified events column details

Values in some field on the **Unified Events** page depend on the event type. See this table for values by event type for the default fields.

To see all event fields and their correspondences, use the column picker ( ) icon.

Unified events field	Connection or security-related connection event field	Intrusion event field	File event field	Malware event field
Time	First Packet	Time	Time	Time
Event Type	--	--	--	--
Action	Action	Inline Result	Action	Action
Reason	Reason	Reason	(Not applicable)	(Not applicable)
Source IP	Initiator IP	Source IP	Sending IP	Sending IP
Destination IP	Responder IP	Destination IP	Receiving IP	Receiving IP
Source Port/ICMP Type	Source Port	Source Port	Sending Port	Sending Port
Destination Port/ ICMP Type	Destination Port	Destination Port	Receiving Port	Receiving Port
Web Application	Web Application	Web Application	Web Application	Web Application
Rule	Access Control Rule	Access Control Rule	(Not applicable)	(Not applicable)
Policy	Access Control Policy	Intrusion Policy	File Policy	File Policy
Device	Device	Device	Device	Device

For more information about the event fields, refer to:

- Connection and Security Intelligence Event Fields
- Intrusion event fields
- File and malware event fields

See also: Initiator and responder, source and destination, and sender and receiver fields.



Note Even if logging is not enabled at the beginning of a connection, the system has and uses this value as the **Time** field in the unified events table. To check if a connection event was logged at the beginning and end of the connection, expand the event row for details. If both ends of the connection were logged, you will see a **Last Packet** field.