Unified Events

The following topics describe how to use the Unified Events:

About the Unified Events

Unified Events provide you a single-screen view of multiple types (connection, intrusion, file, malware, and some security-related connection events) of firewall events. Events associated with each other are stacked together in the table to provide a unified view and more context about the security event. If you have an intrusion event on the Unified Events table, click the intrusion event to highlight the associated connection event. You can then correlate the connection event with the intrusion event to better understand and troubleshoot the 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. Unified events also has option to save the custom filters that you use often for specific needs, and then quickly load the saved filters. Also, you can make a tailored event viewer table by adding or removing columns, pin columns, or drag and re-order the columns.

The **Live View** option in the Unified Events table lets you see the firewall events in real time and monitor the activity on your network. For example, if you are a firewall administrator, viewing event updates in real time after you make a policy change can help you to ensure that the policy changes are correctly enforced on your network.

Requirements and Prerequisites for the Unified Events

Model Support

Any.

Supported Domains

Any.

User Roles

- Admin
- Security Analyst

Working 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, see 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, see 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 indicates 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, see View Live Events 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, see Event Investigation Using Web-Based Resources.
Open multiple unified events windows	• You can display different views of the unified events table using multiple browser tabs or windows. • Each new tab or window has the characteristics of the most recently modified tab/window. • To make any open tab/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 used 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

Configure time range in unified events to view firewall events for a specific period. 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.

Important 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**.

  Tip
  Click **Now** to quickly set the current time as the **End time**.

- If you want to configure a sliding default time window of the length you specify, click **Sliding Time Range**.

  The appliance displays all the events generated from a specific start time; for example, 1 hour ago, to the present. As you refresh event views, the time window slides so that you always see events from the last hour.

Step 4 Click **Apply**.

View Live Events in Unified Events

Configure the unified events to display firewall events in real time without manually refreshing the event viewer. In the **Live View** mode, the event logs appear in real time as the security event occurs in your network which helps you to better troubleshoot the issues.

Procedure

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

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

Step 2 To see live event updates, click **Go Live**.

New events get populated at the top of the event table. The time range section displays a timer to inform you for how long the unified events table is live.

Note

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

- By default, the **Go Live** feature in FMC considers traffic data from the last 30 seconds, which is shorter than the 120 seconds required for UDP connections to be processed into unified events. This may result in incomplete event logging for UDP traffic.
- To improve visibility, configure logging at the beginning of the connection for UDP traffic.

What to do next

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

Filters in Unified Events

The unified events table initially displays multiple types of firewall events from the past hour. You can filter the default view of unified events for a more granular contextual picture of activity on your network. Filters support exclusion as well as inclusion filter criteria.

Filters help you to provide quick access to critical information. For example, if you are a firewall administrator and you want to allow or deny specific application access to some users, you can set user search criteria to scan through the firewall logs. The event viewer displays event logs that match the search criteria.

Procedure

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

Step 2 Enter the filter criteria:

- To manually enter the filter criteria, type the exact criteria in the search text field, or select the criteria from the drop-down list. Then, provide the filter criteria value. While typing in the values, you are prompted with suggestions in the drop-down list whenever possible.
- Click the dots in a cell for an event in the table 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 important information about wildcards and search behavior, see Event Searches.
- Include operators (such as <, >, !, and so on) 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.

Unified Events Column Descriptions

Values in some fields depend on the event type. Field correspondences for the default fields are as follows:

Unified Events Field Name	Connection or Security Intelligence Event Field Name	Intrusion Event Field Name	File Event Field Name	Malware Event Field Name
Time	First Packet See note below.	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

Click the column picker ( ) icon to see all event fields and their correspondences.

For field descriptions, see the following topics:

- Connection and Security Intelligence Event Fields
- Intrusion Event Fields
- File and Malware Event Fields

See also A Note About Initiator/Responder, Source/Destination, and Sender/Receiver Fields.

Note Even if you have not enabled logging at the beginning of the connection, the system has and uses this value as the time field in the unified events table. To determine whether a connection event was logged at the beginning and end of the connection, expand the event's row to view details. If both ends of the connection were logged, you see a **Last Packet** field.

History for Unified Events

Feature	Minimum FMC	Minimum FTD	Details
Unified events table	7.0	Any	View and work in a single table with multiple event types: Connection (including Security Intelligence), intrusion, file, and malware. New/modified screens: New page under **Analysis** > **Unified Events**. Supported platforms: FMC