# 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.

**Note**

- The Unified Events feature requires activation. If you have not yet activated this feature, contact your Cisco sales representative to enable it.

- The **Unified Events** page uses the Cisco Security Analytics and Logging data store as its event data source. You must have a valid Cisco Security Analytics and Logging subscription plan to view firewall events on the **Unified Events** page.

# 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**

The **Unified Events** page uses the Cisco Security Analytics and Logging data store as its event data source. You must have a valid Cisco Security Analytics and Logging subscription plan to view firewall events on the **Unified Events** page.

**Procedure**

| | |
|---|---|
| **Step 1** | Choose **Analysis** > **Unified Events**. |
| **Step 2** | Choose the time range (fixed or sliding). For more information, see . |
| **Step 3** | 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 . |
| **Step 4** | Choose more options: |

| To Do This ... | Do This |
|---|---|
| Customize columns | • Add or remove columns:<br><br>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:<br><br>   • Connection event (⇆)<br><br>   • Security-related connection event (👽)<br><br>   • Intrusion event (👽)<br><br>   • File event (📄)<br><br>   • Malware event (🐛)<br><br>Click the event icon next to the column set filtering options to filter the list of event fields according to the selected event type.<br><br>**Note**<br>Including many columns may degrade performance. You can view data for hidden columns by expanding an event row to view event details.<br><br>• Reorder columns:<br><br>Drag and drop the column heading.<br><br>• Pin (freeze) columns to the left or right side of the table so they do not scroll:<br><br>Drag a column all the way to either left or right side of the table.<br><br>Or, drag and drop a column heading into the pinned area.<br><br>To unpin a column, drag the column out of the pinned area.<br><br>• Resize columns.<br><br>• Revert columns to the default setting.<br><br>• Save column sets to quickly reload your customized view later. For more information, see Save a Column Set, on page 7 topic.<br><br>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.<br><br>If needed, filter the events to display a small enough set of events.<br><br>**Note**<br>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.<br><br>**Tip**<br>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. |
| Cross-launch to external resources | Click the ellipsis (⋮) in a table cell to see the options available for that cell value, if any.<br><br>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.<br><br>• Each new tab or window has the characteristics of the most recently modified tab/window.<br><br>• To make any open tab/window as the template, make a minor change to it.<br><br>• The system processes queries on multiple tabs sequentially.<br><br>• 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. |
| Save searches | Save custom searches as your favorites and quickly load them later. For more information, see Save a Search in Unified Events, on page 6. |
| Bookmark or share query results | Bookmark or copy-paste the URL in the browser window.<br><br>• The URL retrieves different events later if it used the sliding time range.<br><br>• 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.

| | |
|---|---|
| **Note** | If your selected time range goes beyond the event retention period allowed by your license, it will automatically adjust to fit within the retention period. |

**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**.

# 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.

- 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.

**What to do next**

To save a custom filter, see topic.

# Save a Search in Unified Events

Save custom searches as your favorites and quickly load them later. Note that this option is not available for the **Troubleshooting** table.

**Procedure**

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

**Step 2**   Click the **Events** tab.

**Step 3**   Establish a search criteria as described in the topic.

**Step 4**   Click the **Favourite Searches** ( ☆ ) icon on the search text box.

**Step 5**   Do one of the following:

- To save a new search, specify a search name and click **Save as new**.

• To overwrite a saved search, click **Edit** on the saved search that you want to overwrite, and click **Overwrite**.

**What to do next**

# Load a Saved Search in Unified Events

**Before you begin**

**Procedure**

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

**Step 2** Click the **Favourite Searches** ( ☆ ) icon on the search text box.

**Step 3** Click the saved search that you want to load.

# Save a Column Set

Save custom column sets as your favorites to load them later or quickly toggle between custom tables. Note that this option is not available for the **Troubleshooting** table.

**Procedure**

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

**Step 2** Click the column picker Icon (▥) and choose the set of columns that you want to save.

**Step 3** Click the **Favorite column sets** ( ☆ ) icon.

**Step 4** Do one of the following:

• To save a new column set, specify a column set name and click **Save as new**.

• To overwrite a favorite column set, click **Edit(⋮)** on the column set that you want to overwrite, and click **Overwrite**.

**What to do next**

To load a saved column set, see topic.

# Load a Saved Column Set

**Before you begin**

Save a favorite column set as described in the topic.

**Procedure**

| | |
|---|---|
| **Step 1** | Choose **Analysis** > **Unified Events**. |
| **Step 2** | Click the column picker icon (▥). |
| **Step 3** | Click the **Favorite column sets** ( ☆ ) . |
| **Step 4** | Click the column set that you want to load. |

# 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<br>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 |

| Unified Events Field Name | Connection or Security Intelligence Event Field Name | Intrusion Event Field Name | File Event Field Name | Malware Event Field Name |
|---|---|---|---|---|
| **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.

**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.