

# Custom Tables

The following topics describe how to use custom tables:


- Introduction to Custom Tables, on page 1
- Predefined Custom Tables, on page 1
- User-Defined Custom Tables, on page 6
- Searching Custom Tables, on page 8


# Introduction to Custom Tables

As the Firepower System collects information about your network, the Firepower Management Center stores it in a series of database tables. When you use a workflow to view the resulting information, the Firepower Management Center pulls the data from one of these tables. For example, the columns on each page of the Network Applications by Count workflow are taken from the fields in the Applications table.

If you determine that your analysis of the activity on your network would be enhanced by combining fields from different tables, you can create a custom table. For example, you could combine the host criticality information from the predefined Host Attributes table with the fields from the predefined Connection Data table and then examine connection data in a new context.

Note that you can create custom workflows for either predefined or custom tables.

# Predefined Custom Tables

Custom tables contain fields from two or more predefined tables. The Firepower System is delivered with a number of system-defined custom tables, but you can create additional custom tables that contain only information that matches your specific needs.

For example, the Firepower System is delivered with system-defined custom tables that correlate intrusion event data with host data, so you can search for events that impact critical systems and view the results of that search in one workflow.

In a multidomain deployment, the predefined custom tables belong to the Global domain and cannot be modified in lower domains.

The following table describes the custom tables provided with the system.

*Table 1: System-Defined Custom Tables*

| Table | Description |
|---|---|
| Hosts with Servers | Includes fields from the Hosts and Servers tables, providing you with information about the detected applications running on your network, as well as basic operating system information about the hosts running those applications. |
| Intrusion Events with Destination Criticality | Includes fields from the Intrusion Events table and the Hosts table, providing you with information on the intrusion events, as well as the host criticality of the destination host involved in each intrusion event.<br>You can use this table to search for intrusion events involving destination hosts with high host criticality. |
| Intrusion Events with Source Criticality | Includes fields from the Intrusion Events table and the Hosts table, providing you with information on the intrusion events and the host criticality of the source host involved in each intrusion event.<br>You can use this table to search for intrusion events involving source hosts with high host criticality. |

# Possible Table Combinations

When you create a custom table, you can combine fields from predefined tables that have related data. The following table lists the predefined tables you can combine to create a new custom table. Keep in mind that you can create a custom table that combines fields from more than two predefined custom tables.

*Table 2: Custom Table Combinations*

| You can combine fields from... | With fields from... |
|---|---|
| Applications | • Correlation Events<br>• Intrusion Events<br>• Connection Summary Data<br>• Host Attributes<br>• Application Details<br>• Discovery Events<br>• Connection Events<br>• Hosts<br>• Servers<br>• White List Events |

| You can combine fields from... | With fields from... |
|---|---|
| Correlation Events | • Applications<br>• Host Attributes<br>• Hosts |
| Intrusion Events | • Applications<br>• Host Attributes<br>• Hosts<br>• Servers |
| Connection Summary Data | • Applications<br>• Host Attributes<br>• Hosts<br>• Servers |
| Host Indications of Compromise | • Applications<br>• Application Details<br>• Captured Files<br>• Connection Events<br>• Connection Summary Data<br>• Correlation Events<br>• Discovery Events<br>• Host Attributes<br>• Hosts<br>• Intrusion Events<br>• Security Intelligence Events<br>• Servers<br>• White List Events |

| You can combine fields from... | With fields from... |
|---|---|
| Host Attributes | • Applications<br>• Correlation Events<br>• Intrusion Events<br>• Connection Summary Data<br>• Application Details<br>• Discovery Events<br>• Connection Events<br>• Hosts<br>• Servers<br>• White List Events |
| Application Details | • Applications<br>• Host Attributes<br>• Hosts |
| Discovery Events | • Applications<br>• Host Attributes<br>• Hosts |
| Connection Events | • Applications<br>• Host Attributes<br>• Hosts<br>• Servers |
| Security Intelligence Events | • Applications<br>• Host Attributes<br>• Hosts<br>• Servers |

| You can combine fields from... | With fields from... |
|---|---|
| Hosts | • Applications<br>• Correlation Events<br>• Intrusion Events<br>• Connection Summary Data<br>• Host Attributes<br>• Application Details<br>• Discovery Events<br>• Connection Events<br>• Servers<br>• White List Events |
| Servers | • Applications<br>• Intrusion Events<br>• Connection Summary Data<br>• Host Attributes<br>• Connection Events<br>• Hosts |
| White List Events | • Applications<br>• Host Attributes<br>• Hosts |

Sometimes a field in one table maps to more than one field in another table. For example, the predefined **Intrusion Events with Destination Criticality** custom table combines fields from the Intrusion Events table and the Hosts table. Each event in the Intrusion Events table has two IP addresses associated with it—a source IP address and a destination IP address. However, the "events" in the Hosts table each represent a single host IP address (hosts may have multiple IP addresses). Therefore, when you create a custom table based on the Intrusion Events table and the Hosts table, you must choose whether the data you display from the Hosts table applies to the host source IP address or the host destination IP address in the Intrusion Events table.

When you create a new custom table, a default workflow that displays all the columns in the table is automatically created. Also, just as with predefined tables, you can search custom tables for data that you want to use in your network analysis. You can also generate reports based on custom tables, as you can with predefined tables.

# User-Defined Custom Tables

**Tip** Instead of creating a new custom table, you can export a custom table from another Firepower Management Center, then import it onto your Firepower Management Center.

To create a custom table, decide which predefined tables delivered with the Firepower System contain the fields you want to include in your custom table. You can then choose which fields you want to include and, if necessary, configure field mappings for any common fields.

**Tip** Data involving the Hosts table allows you to view data associated with all IP addresses from one host, rather than one specific IP address.

For example, consider a custom table that combines fields from the Correlation Events table and the Hosts table. You can use this custom table to get detailed information about the hosts involved in violations of any of your correlation policies. Note that you must decide whether to display data from the Hosts table that matches the source IP address or the destination IP address in the Correlation Events table.

If you view the table view of events for this custom table, it displays correlation events, one per row. You can configure the custom table to include the following information:

- the date and time the event was generated
- the name of the correlation policy that was violated
- the name of the rule that triggered the violation
- the IP address associated with the source, or initiating, host involved in the correlation event
- the source host's NetBIOS name
- the operating system and version the source host is running
- the source host criticality

**Tip** You could create a similar custom table that displays the same information for destination, or responding, hosts.

# Creating a Custom Table

**Procedure**

**Step 1** Choose **Analysis** > **Custom** > **Custom Tables**.

**Step 2** Click **Create Custom Table**.

**Step 3** In the **Name** field, enter a name for the custom table.

**Example:**

For example, you might enter `Correlation Events with Host Information (Src IP)`.

**Step 4** From the **Tables** drop-down list, choose **Correlation Events**.

**Step 5** Under **Fields**, choose**Time** and click **Add** to add the date and time when a correlation event was generated.

**Step 6** Repeat step 5 to add the **Policy** and **Rule** fields.

**Tip** You can use Ctrl or Shift while clicking to choose multiple fields. You can also click and drag to choose multiple adjacent values. However, if you want to specify the order the fields appear in the table view of events associated with the table, add the fields one at a time.

**Step 7** From the **Tables** drop-down list, choose **Hosts**.

**Step 8** Add the **IP Address**, **NetBIOS Name**, **OS Name**, **OS Version**, and **Host Criticality** fields to the custom table.

**Step 9** Under **Common Fields**, next to **Correlation Events**, choose **Source IP**.

Your custom table is configured to display the host information you chose in step 8 for the source, or initiating, hosts involved in correlation events.

**Tip** You can create a custom table that displays detailed host information for the destination, or responding, hosts involved in a correlation event by following this procedure but choosing **Destination IP** instead of **Source IP**.

**Step 10** Click **Save**.

# Modifying a Custom Table

In a multidomain deployment, the system displays custom tables created in the current domain, which you can edit. It also displays custom tables created in ancestor domains, which you cannot edit. To view and edit custom tables in a lower domain, switch to that domain.

**Procedure**

**Step 1** Choose **Analysis** > **Custom** > **Custom Tables**.

**Step 2** Click **Edit** ( ) next to the table you want to edit.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 3** Optionally, remove fields from the table by clicking **Delete** ( ) next to the fields you want to remove.

**Note** If you delete fields currently in use in reports, the system will prompt you to confirm that you want to remove the sections using those fields from those reports.

**Step 4** Make other changes as needed.

**Step 5** Click **Save**.

# Deleting a Custom Table

In a multidomain deployment, the system displays custom tables created in the current domain, which you can delete. It also displays custom tables created in ancestor domains, which you cannot delete. To delete custom tables in a lower domain, switch to that domain.

**Procedure**

**Step 1** Choose **Analysis** > **Custom** > **Custom Tables**.

**Step 2** Click **Delete** ( ) next to the custom table you want to delete.

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

# Viewing a Workflow Based on a Custom Table

When you create a custom table, the system automatically creates a default workflow for it. The first page of this workflow displays a table view of events. If you include intrusion events in your custom table, the second page of the workflow is the packet view. Otherwise, the second page of the workflow is a hosts page. You can also create your own custom workflows based on your custom table.

**Tip** If you create a custom workflow based on a custom table, you can specify it as the default workflow for that table.

You can use the same techniques to view events in your custom table that you use for event views based on predefined tables.

In a multidomain deployment, the system displays custom tables created in the current domain, which you can edit. It also displays custom tables created in ancestor domains, which you cannot edit. To view and edit custom tables in a lower domain, switch to that domain.

**Procedure**

**Step 1** Choose **Analysis** > **Custom** > **Custom Tables**.

**Step 2** Click **View** ( ) next to the custom table related to the workflow you want to see.

# Searching Custom Tables

In a multidomain deployment, the system displays custom tables created in the current domain, which you can edit. It also displays custom tables created in ancestor domains, which you cannot edit. To view and edit custom tables in a lower domain, switch to that domain.

### Procedure

**Step 1** Choose **Analysis** > **Custom** > **Custom Tables**.

**Step 2** Click **View** ( ) next to the custom table you want to search.

**Tip** To use a different workflow, including a custom workflow, click **(switch workflow)** next the workflow title.

**Step 3** Click **Search**.

**Tip** To search the database for a different kind of event or data, choose it from the table drop-down list.

**Step 4** Enter your search criteria in the appropriate fields.

If you enter criteria for multiple fields, the search returns only the records that match search criteria specified for all fields.

**Tip** Click **Object** ( ) next to a search field to use an object as a search criterion.

**Step 5** Optionally, if you plan to save the search, you can check the **Private** check box to save the search as private so only you can access it. Otherwise, leave the check box clear to save the search for all users.

**Tip** If you want to use the search as a data restriction for a custom user role, you **must** save it as a private search.

**Step 6** Optionally, you can save the search to be used again in the future. You have the following options:

- Click **Save** to save the search criteria. The search is visible only to your account if you checked the **Private** check box.
- Click **Save As New** to save a new search or assign a name to a search you created by altering a previously-saved search. The search is saved and visible only to your account if you checked the **Private** check box.

**Step 7** Click **Search** to start the search.

Your search results appear in the default workflow for the custom table, constrained by the current time range (if applicable).