

Custom Tables

The following topics describe how to use custom tables:

- Custom tables, on page 1
- Predefined custom tables, on page 1
- User-defined custom tables, on page 5
- Search custom tables, on page 7
- History for custom tables, on page 9

Custom tables

A custom table is a user-defined database table that combines fields from different predefined tables to enhance analysis of network activity.

The Firewall Management Center collects data about your network and stores it in a series of database tables. When you use a workflow to view specific information, the Firewall Management Center retrieves the data from one of these tables.For example, the **Network Applications by Count** workflow displays columns that are sourced from 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.

Predefined custom tables

A predefined custom table is a system-delivered custom table that

- contains fields from two or more predefined tables
- correlates data across different table types for specific workflow needs, and
- provides a foundation for creating additional user-defined custom tables.

For example, Firewall Management Center includes predefined custom tables that correlate intrusion event data with host data. This enables you to search for events that impact critical systems and view the results in one workflow.

This table describes the custom tables provided in Firewall Management Center.

Table 1: Predefined 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.

You can create additional custom tables that contain only information that matches your specific needs. In a multidomain deployment, the predefined custom tables belong to the global domain. You cannot modify these tables in lower domains.

Possible table combinations

When you create a custom table, you can combine fields from predefined tables that have related data. This 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 • Intrusion Events • Connection Summary Data • Host Attributes • Application Details • Discovery Events • Hosts • Servers • Allow List Events
Correlation Events	• Applications • Host Attributes • Hosts
Intrusion Events	• Applications • Host Attributes • Hosts • Servers

You can combine fields from...	With fields from...
Connection Summary Data	• Applications • Host Attributes • Hosts • Servers
HostIndications of Compromise	• Applications • Application Details • Captured Files • Connection Summary Data • Correlation Events • Discovery Events • Host Attributes • Hosts • Intrusion Events • Security Intelligence Events • Servers • Allow List Events
Host Attributes	• Applications • Correlation Events • Intrusion Events • Connection Summary Data • Application Details • Discovery Events • Hosts • Servers • Allow List Events
Application Details	• Applications • Host Attributes • Hosts

You can combine fields from...	With fields from...
Discovery Events	• Applications • Host Attributes • Hosts
Security Intelligence Events	• Applications • Host Attributes • Hosts • Servers
Hosts	• Applications • Correlation Events • Intrusion Events • Connection Summary Data • Host Attributes • Application Details • Discovery Events • Servers • Allow List Events
Servers	• Applications • Intrusion Events • Connection Summary Data • Host Attributes • Hosts
Allow List Events	• Applications • Host Attributes • Hosts

Sometimes a field in one table maps to more than one field in another 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

A user-defined custom table is a table that you create or import to combine selected fields from multiple predefined tables to create customized data views. It lets you view related data from different tables in a single context, such as host details associated with specific events.

To create a custom table, first decide which predefined tables contain the fields you want to include. You can then select the desired fields and, if necessary, configure field mappings for any common fields.

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

Correlation events and hosts table combination

Consider a custom table that combines fields from the **Correlation Events** table and the **Hosts** table. This custom table enables you to get detailed information about the hosts involved in violations 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 for this custom table, it displays correlation events (one per row) and may include these 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, and
- the source host criticality.

Create a custom table

Create custom tables that contain only information that matches your specific needs. Custom tables allow you to combine information from multiple data sources to create comprehensive views of security events and associated host details.

Procedure

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

Step 2 Click **Create Custom Table**.

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

Step 4 From the **Tables** drop-down list, choose a predefined table that has related data.

Step 5 From **Fields** drop-down list, choose the fields that contain data for your specific needs.

You can combine fields from multiple predefined tables that have related data. After completing Step 5, select another predefined table that contains the required data and repeat the selection process as needed.

Note To select multiple fields at once, use **Ctrl**, **command**, or **Shift** key while selecting fields. You can also click and drag to select multiple adjacent fields. If you want to specify the order in which fields appear in the table view, add them one at a time.

Step 6 After selecting all required fields, click **Add** to add them to the table.

Step 7 Click **Save**.

Modify a custom table

Modify a custom table to update its structure, remove unnecessary fields, or change table properties to better meet your reporting needs.

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** > **Advanced** > **Custom Tables**.

Step 2 Click the **Edit** ( ) icon next to the custom table you want to modify.

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 a field that is currently in use in a report, the Firewall Management Center will prompt you to confirm whether you want to remove any sections from the report that are using this field.

Step 4 Make other changes as needed.

Step 5 Click **Save**.

Delete a custom table

Delete custom tables that are no longer needed from the current domain.

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** > **Advanced** > **Custom Tables**.

Step 2 Click the **Delete** ( ) icon 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.

View a workflow based on a custom table

View workflows to examine events in custom tables and access table views, packet views, or hosts pages depending on your custom table configuration.

When you create a custom table, Firewall Management Center 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.

Note 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 method 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** > **Advanced** > **Custom Tables**.

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

Search custom tables

Search for specific data within custom tables to locate relevant records based on your search criteria.

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** > **Advanced** > **Custom Tables**.

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

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

Step 3 Click **Search**.

Note 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.

Note 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.

Note 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).

History for custom tables

This table provides a chronological history of Custom Tables feature updates and improvements, enabling you to track feature availability and requirements across different Firewall Management Center versions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Support for connection events in custom tables was removed	6.6	Any	You can no longer create custom tables that include connection events. If you upgraded to version 6.6: Existing tables with connection events will be listed as deprecated and will show no data, and you cannot export or edit them. Existing reports, custom workflows, and dashboards may include deprecated tables; you may want to review these. Modified screens: **Analysis** > **Advanced** > **Custom Tables** and the page for adding or editing custom tables.