

Custom Workflows

The following topics describe how to use custom workflows:

- Custom workflows, on page 1
- Saved custom workflows, on page 1
- How custom workflows work, on page 2
- How to access custom workflows, on page 5

Custom workflows

Custom workflows are workflows you create to meet your specific needs when the predefined or Cisco-provided workflows do not meet your requirements.

Custom workflow features

- When creating a custom workflow, you select the event type or database table that the workflow will use as its basis.

  The Firewall Management Center allows you to base a custom workflow on a custom table.

- You can include drill-down pages, table views, and host or packet views in custom workflows to visualize and analyze data.
- If your event evaluation process changes, you can edit custom workflows to accommodate new requirements.

Note You can set a custom workflow as the default workflow for any event type.

Saved custom workflows

In addition to predefined workflows, which cannot be modified, the Firewall Management Center includes several saved custom workflows. Each of these workflows is based on a custom table and can be modified.

In a multidomain deployment, these saved workflows belong to the global domain and cannot be modified in lower domains.

Table 1: Saved custom workflows

Workflow name	Description
Events by Priority and Classification	This workflow lists events and their type in order of event priority, along with a count showing how many times each event has occurred. This workflow is based on the Intrusion Events custom table.
Hosts with Servers Default Workflow	You can use this workflow to quickly view the basic information in the Hosts with Servers custom table. This workflow is based on the Hosts with Servers custom table.
Server and Host Details	You can use this workflow to determine what servers are most frequently used on your network and which hosts are running those servers. This workflow is based on the Hosts with Servers custom table.

How custom workflows work

If the predefined and Cisco-provided custom workflows do not meet your needs, you can create custom workflows.



Note Instead of creating a new custom workflow, you can export a custom workflow from another appliance and then import it onto your appliance. You can then edit the imported workflow to suit your needs.

Summary

The key components in the process of creating a custom workflow are:

- Source table: Provides data foundation for the workflow.
- Drill-down pages: Display detailed data with customizable columns and sorting.
- Table view pages: Provide a standard table display without customizable properties.
- Final page: Automatically added based on selected table type.

Workflow

The custom workflow creation process involves these stages:

1. Initiate workflow creation and configure basic settings:
   - Select a table to be the source of the workflow.
   - Enter a workflow name.
   - Add drill-down pages and table view pages to the workflow.
2. Configure the page properties for each drill-down page in these ways:

- Provide a name that appears at the top of the page in the web interface.
- Specify the default sort order as ascending or descending.
- You can include up to five columns on each page.

Note

- Add at least one drill-down page or a table view of events to each custom workflow.
- If you selected **Vulnerabilities** as the table type, then add **IP Address** as a table column, the **IP Address** column does not appear when you view vulnerabilities using your custom workflow. It appears only when you use the search feature to limit the workflow to a specific IP address or block of addresses.

3. Add table view pages. You can add table view pages anywhere in the sequence of workflow pages. They do not support editable properties such as page name, sort order, or user-definable columns.
4. The Firewall Management Center automatically adds a final page based on the selected table type, as described in this table. This final page is added by default when you create the workflow.

Table 2: Custom workflow final pages

Event/Asset Type	Final Page
Discovery events	Hosts
Vulnerabilities	Vulnerability detail
Third-party vulnerabilities	Hosts
Users	Users
Indications of compromise	Hosts or users
Intrusion events	Packets

The system does not add a final page for custom workflows based on other kinds of events (for example, audit log or malware events).

Custom workflows based on connection data are similar to other workflows, except you can include drill-down pages containing connection summary data, connection data graph pages, drill-down pages with data for individual connections, and table view pages.

Create custom workflows based on non-connection data

Custom workflows based on non-connection data allow you to organize and analyze security information in a structured format that suits your specific monitoring and analysis needs.

Before you begin

You must have **Admin** or **Security Analyst** privileges to create a custom workflow based on non-connection data.

Procedure

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

Step 2 Click **Create Custom Workflow**.

Step 3 Enter a name for the workflow in the **Name** field.

Step 4 Enter a **Description**. This is optional.

Step 5 Choose the table you want to include from the **Table** drop-down list.

Step 6 To add one or more drill-down pages to the workflow, complete these steps:

a) Click **Add Page**.

b) Enter a name for the page in the **Page Name** field.

c) Under **Column 1**, set the preferred sort priority and select a table column to display as the left-most column.

Example:

To create a page showing the destination ports that are targeted, and to sort the page by count, choose **2** from the **Sort Priority** drop-down list and **Destination Port/ICMP Code** from the **Field** drop-down list.

d) Continue choosing fields and set their sort priority until you have specified all the fields to appear on the page.

Step 7 To add a table view page to the workflow, click **Add Table View**.

You cannot customize or configure table views.

Step 8 Click **Save**.

Create custom connection data workflows

Create custom workflows based on connection data to visualize and analyze network connection information through various graph types and data views.

Custom connection data workflows let you add connection data graph pages, drill-down pages, and table view pages. You can add any number of each page type to the workflow in any order. Each connection data graph page includes one graph: a line, bar, or pie chart. You can include more than one dataset on line and bar graphs.

Before you begin

You must have **Admin** privileges to create a custom workflow based on connection data.

Procedure

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

Step 2 Click **Create Custom Workflow**.

Step 3 Enter a name for the workflow in the **Name** field.

Step 4 Enter a **Description**. This is optional.

Step 5 From the **Table** drop-down list, choose **Connection Events**.

Step 6 To add one or more drill-down pages to the workflow, complete these steps:

a) Click **Add Page** to add a drill-down page that contains data on individual connections.

Alternatively, click **Add Summary Page** to add a drill-down page that contains connection summary data.

b) Enter a name for the page in the **Page Name** field.

c) Under **Column 1**, set the preferred sort priority and select a table column to display as the left-most column.

d) Continue choosing fields and set their sort priority until you have specified all the fields to appear on the page.

Example:

To create a page showing the amount of traffic transmitted over your monitored network and to sort the page by the responders that transmitted the most traffic, choose **1** from the **Sort Priority** drop-down list and **Responder Bytes** from the **Field** drop-down list.

Step 7 To add one or more graph pages to the workflow, complete these steps:

a) Click **Add Graph**.

b) Enter a name for the page in the **Graph Name** field.

c) Choose the type of graph you want to include on the page.

d) Specify what kind of data you want to graph by choosing the x-axis and y-axis of the graph.

On a pie chart, the x-axis represents the independent variable and the y-axis represents the dependent variable.

e) Choose the datasets you want to include on the graph.

Note that pie charts can include only one data set.

Step 8 To add a table view of connection data, click **Add Table View**.

You cannot customize or configure table views.

Step 9 Click **Save**.

How to access custom workflows

The method you use to view a workflow depends on whether the workflow is based on one of the predefined event tables or on a custom table.

- If your custom workflow is based on a predefined event table, access it in the same way that you would access a workflow that ships with the appliance. For example, to access a custom workflow based on the **Hosts** table, choose **Analysis** > **Hosts heading** > **Hosts**.
- If your workflow is based on a custom table, choose **Analysis** > **Advanced** > **Custom Tables** to access it.

If your event evaluation process changes, you can edit custom workflows to meet your new needs.

Note

- You cannot edit any of the predefined workflows.
- You can set a custom workflow as the default workflow for any event type.

View custom workflows based on predefined tables

View and manage custom workflows that utilize predefined tables in Firewall Management Center.

Before you begin

You must have **Admin**, **Maintenance User**, or **Security Analyst** user privileges to view a custom workflow.

Procedure

Step 1 Choose the appropriate menu path and option for the table on which you based your custom workflow, as described in the Workflow selection.

Step 2 To switch workflows, click **(switch workflow)** next to the current workflow title and choose a different workflow.

Step 3 If no events appear and the workflow can be constrained by time, adjust the time range as needed to display relevant events. For more information, refer to Event time constraints.

View custom workflows based on custom tables

View custom workflows that are based on custom tables. These workflows provide insights into custom data analysis and security event monitoring.

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

Before you begin

You must have **Admin** or **Security Analyst** privileges to view a custom workflow that is based on custom tables.

Procedure

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

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

Step 3 To switch workflows, click **(switch workflow)** next to the current workflow title and choose a different workflow, including custom workflows.

Step 4 If no events appear and the workflow can be constrained by time, adjust the time range as needed to display relevant events. For more information, refer to Event time constraints.

Edit custom workflows

Edit custom workflows to modify existing workflow configurations and adapt them to changing security requirements.

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

Before you begin

You must have **Admin** or **Security Analyst** privileges to edit a custom workflow.

Procedure

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

Step 2 Click **Edit** ( ) next to the workflow that 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 Edit the workflow as needed.

Step 4 Click **Save**.