

Dashboards

The following topics describe how to use dashboards:

- Dashboards, on page 1
- Best practices for dashboard usage, on page 2
- Dashboard widgets, on page 2
- Widget availability by appliance, user role, and domain, on page 3
- Predefined dashboard widgets, on page 4
- Manage dashboards, on page 17

Dashboards

A dashboard is a customizable monitoring interface that provides at-a-glance views of the current system status, including data about events collected and generated by the firewall deployment. This interface also shows information on the status and overall health of the appliances in your deployment, and

The information that the dashboard provides depends on how you license, configure, and deploy the system.

Dashboard components and features

Firewall Management Center includes several predefined dashboards that you can use as-is or modify to suit your needs. By default, if your user role has dashboard access, your home page is the predefined **Summary Dashboard**. You can configure a different default home page or change the default dashboard to another predefined or custom dashboard.

Dashboard components include:

- Tabs: Each dashboard uses tabs to organize and display widgets grouped by related information. Tabs help you navigate different aspects of system monitoring within the same dashboard.
- Widgets: Small, self-contained components within tabs that provide insights into specific system aspects. For example, the predefined **Appliance Information** widget displays the appliance name, model, and currently running software version. Widgets display data constrained by the dashboard's time range, which you can adjust from as short as the last hour to as long as the last year.

The **Summary Dashboard** includes tabs for key features such as Encrypted Visibility Engine and Zero Trust Network Access, among others. For more information about these dashboards, see *Cisco Secure Firewall Management Center Device Configuration Guide*.

User role requirements for accessing Dashboards

Access to dashboards depends on your user role. Roles with dashboard access include:

- **Administrator**
- **Maintenance User**
- **Security Analyst**
- **Security Analyst (Read Only)**
- Custom roles with the **Dashboards** permission

If your role does not have dashboard access, your default home page will be relevant to your role. For example, a **Discovery Admin** sees the **Network Discovery** page instead of a dashboard.

Best practices for dashboard usage

Consider the following best practices and guidelines for accessing and using dashboards in Firewall Management Center.

- Use dashboards to monitor your network with customizable views and detailed information. For a quick, visual summary of your monitored network, use **Context Explorer**.
- Create custom dashboards based on predefined ones. These custom dashboards can be shared with others, or kept private. When creating or modifying dashboards, use predefined dashboards as a base to maintain consistency, and ease of use.
- If you have **Administrator** access, you can view or edit private dashboards created by other users.
- Some drill-down pages and event tables include a dashboard toolbar link that opens a relevant predefined dashboard. Deleting a predefined dashboard or tab disables these toolbar links.
- In multidomain environments, dashboards from ancestor domains are not accessible. Create copies of higher-level dashboards if needed.
- To view the correlated device metrics on the dashboard, ensure that you have enabled the REST API (**System** (⚙) > **Configuration** > **REST API Preferences**).

Dashboard widgets

Widgets are modular dashboard components that display data such as events, operations, or general information, organized in a three-column layout.

The dashboard widgets that you can view depend on:

- the type of appliance you are using,
- your user role, and
- your current domain in a multidomain deployment.

In addition, each dashboard has a set of preferences that determines its behavior.

You can minimize and maximize widgets, add and remove widgets from tabs, as well as rearrange the widgets on a tab.

Note For widgets that display event counts over a time range, the total number of events may not reflect the number of events for which detailed data is available in the tables on pages under the **Analysis** menu. This occurs because Firewall Management Center sometimes prunes older event details to manage disk space usage. To minimize the occurrence of event detail pruning, you can fine-tune event logging to log only those events most important to your deployment.

Widget availability by appliance, user role, and domain

The dashboard widgets that you can view depend on the type of appliance you are using, your user role, and your current domain (in a multidomain deployment).

Under these conditions, a widget becomes unavailable for you:

- Widget is invalid because you are using the wrong type of appliance.
- You are not authorized to view the widget because your user account does not have the necessary privileges.

  For example, the **Appliance Status** widget is available only to users with **Administrator**, **Maintenance User**, **Security Analyst**, or **Security Analyst (Read Only)** account privileges.

Although you cannot add an unauthorized or invalid widget to a dashboard, an imported dashboard may contain unauthorized or invalid widgets. For example, such widgets can be present if the imported dashboard:

- was created by a user with different access privileges, or
- belongs to an ancestor domain.

Unavailable widgets are disabled and display error messages that indicate why you cannot view them. Individual widgets also display error messages when those widgets have timed out or are otherwise experiencing problems.

Note You can delete or minimize unauthorized and invalid widgets, as well as widgets that display no data, keeping in mind that modifying a widget on a shared dashboard modifies it for all users of the appliance.

In a multidomain deployment, if you do not see a widget that you expect to see, switch to the Global domain. Refer to Switch domains on Secure Firewall Management Center.

Dashboard widget availability by user role

This table lists the user account privileges required to view each widget. Only user accounts with Administrator, Maintenance User, Security Analyst, or Security Analyst (Read Only) access can use dashboards.

Users with custom roles may have access to any combination of widgets, or none at all, as their user roles permit.

Table 1: User roles and dashboard widget availability

Widget	Administrator	Maintenance User	Security Analyst	Security Analyst (Read Only)
Appliance Information	yes	yes	yes	yes
Appliance Status	yes	yes	yes	no
Correlation Events	yes	no	yes	yes
Current Interface Status	yes	yes	yes	yes
Current Sessions	yes	no	no	no
Custom Analysis	yes	no	yes	yes
Disk Usage	yes	yes	yes	yes
Interface Traffic	yes	yes	yes	yes
Intrusion Events	yes	no	yes	yes
Network Compliance	yes	no	yes	yes
Product Licensing	yes	yes	no	no
Product Updates	yes	yes	no	no
RSS Feed	yes	yes	yes	yes
System Load	yes	yes	yes	yes
System Time	yes	yes	yes	yes
Allow List Events	yes	no	yes	yes

Predefined dashboard widgets

Predefined dashboard widgets are system-delivered, ready-to-use widgets that

- provide at-a-glance views of current system status and operational data
- display information about events that the system collects and generates
- display the status and overall health of the appliances in your deployment, and
- can be further customized through preferences that control display options and update frequency.

Widget categories

Predefined widgets are grouped into these categories based on the type of information they present:

- **Analysis & Reporting** widgets display data about the events collected and generated by the system.

- **Miscellaneous** widgets display neither event data nor operations data. Currently, the only widget in this category displays an RSS feed.
- **Operations** widgets display information about the status and overall health of the system.

Some widgets may not be visible to you, depending on appliance type, your user role, or domain restrictions.

The Allow list events widget

The **Allow List Events** widget shows the average events per second by priority, over the dashboard time range.

You can configure the widget to display allow list events of different priorities by modifying the widget preferences. In the widget preferences, you can:

- Check one or more **Priorities** check boxes to display separate graphs for events of specific priorities, including events that do not have a priority.
- Check the **Show All** check box to display an additional graph for all allow list events, regardless of priority.
- Choose **Linear** (incremental) or **Logarithmic** (factor of ten) scale from the **Vertical Scale** drop-down list.
- Specify how often the widget updates.

You can click a graph to view allow list events of a specific priority, or click the **All** graph to view all allow list events. In either case, the events are constrained by the dashboard time range; accessing allow list events via the dashboard changes the events (or global) time window for the Firewall Management Center.

The appliance information widget

The Appliance Information widget provides a snapshot of the appliance. It appears by default on the Status tabs of the **Detailed Dashboard** and the **Summary Dashboard**.

The widget provides:

- The name, IPv4 address, IPv6 address, and model of the appliance.
- The versions of the system software, operating system, Snort, rule update, rule pack, module pack, vulnerability database (VDB), and geolocation update installed on the appliances with dashboards, except for Firewall Management Center Virtual.
- For managed appliances, the name and status of the communications link with the managing appliance.
- For Firewall Management Centers in a high availability pair, the name, model, and system software and operating system versions of the peer Firewall Management Center, as well as how recently the Firewall Management Centers made contact.

You can configure the widget to display more or less information by modifying the widget preferences to display a simple or an advanced view; the preferences also control how often the widget updates.

Appliance status widget

The Appliance Status widget indicates the health of the appliance and of any appliances it is managing. Note that because the Firewall Management Center does not automatically apply a health policy to managed devices, you must manually apply a health policy to devices or their status appears as **Disabled**. This widget appears by default on the **Status** tabs of the **Detailed Dashboard** and the **Summary Dashboard**.

You can configure the widget to display appliance status as a pie chart or in a table by modifying the widget preferences.

The preferences also control how often the widget updates.

Click a section on the pie chart or one of the numbers on the appliance status table to go to the health monitoring page and view the compiled health status of the appliance and of any appliances it is managing.

The correlation events widget

The Correlation Events widget shows the average number of correlation events per second, by priority, over the dashboard time range. It appears by default on the Correlation tab of the Detailed Dashboard.

You can configure the widget to display correlation events of different priorities by modifying the widget preferences, as well as to choose a linear (incremental) or logarithmic (factor of ten) scale.

Check one or more **Priorities** check boxes to display separate graphs for events of specific priorities, including events that do not have a priority. Choose **Show All** to display an additional graph for all correlation events, regardless of priority. The preferences also control how often the widget updates.

Click a graph to view correlation events of a specific priority, or click the **All** graph to view all correlation events. In either case, the events are constrained by the dashboard time range; accessing correlation events via the dashboard changes the events (or global) time window for the appliance.

Current interface status widget

The Current Interface Status widget shows the status of all interfaces on the appliance, enabled or unused. On the Firewall Management Center, you can display the management (`eth0`, `eth1`, and so on) interfaces. On a managed device, you can choose to show only sensing (`s1p1` and so on) interfaces or both management and sensing interfaces. Interfaces are grouped by type: management, inline, passive, switched, routed, and unused.

For each interface, the widget provides:

- the name of the interface
- the link state of the interface
- the link mode (for example, 100Mb full duplex, or 10Mb half duplex) of the interface
- the type of interface, that is, copper or fiber
- the amount of data received (Rx) and transmitted (Tx) by the interface

The color of the ball representing link state indicates the current status, as follows:

- green: link is up and at full speed
- yellow: link is up but not at full speed
- red: link is not up

- gray: link is administratively disabled
- blue: link state information is not available (for example, ASA)

The widget preferences control how often the widget updates.

Current sessions widget

The **Current Sessions** widget shows which users are currently logged into the appliance, the IP address associated with the machine where the session originated, and the last time each user accessed a page on the appliance (based on the local time for the appliance). The user that represents you, that is, the user currently viewing the widget, is marked with a **User icon** and rendered in bold type. Sessions are pruned from this widget's data within one hour of logoff or inactivity. This widget appears by default on the Status tabs of the **Detailed Dashboard** and the **Summary Dashboard**.

On the **Current Sessions** widget, you can:

- Click any user name to manage user accounts on the **User Management** page.
- Click the **Host icon** or **Compromised Host icon** next to any IP address to view the host profile for the associated machine.
- Click any IP address or access time to view the audit log constrained by that IP address and by the time that the user associated with that IP address logged on to the web interface.

The widget preferences control how often the widget updates.

The custom analysis widget

The **Custom Analysis** widget is a highly customizable widget that allows you to display detailed information on the events collected and generated by the system.

The widget is delivered with multiple presets that provide quick access to information about your deployment. The predefined dashboards make extensive use of these presets. You can use these presets or create a custom configuration. At a minimum, a custom configuration specifies the data you are interested in (table and field), and an aggregation method for that data. You can also set other display-related preferences, including whether you want to show events as relative occurrences (bar graph) or over time (line graph).

The widget displays the last time it updated, based on local time. The widget updates with a frequency that depends on the dashboard time range. For example, if you set the dashboard time range to an hour, the widget updates every five minutes. On the other hand, if you set the dashboard time range to a year, the widget updates once a week. To determine when the dashboard will update next, hover your pointer over the **Last updated** notice in the bottom left corner of the widget.



Note A red-shaded Custom Analysis widget indicates that its use is harming system performance. If the widget continues to stay red over time, remove the widget. You can also disable all Custom Analysis widgets from the Dashboard settings in your system configuration (**System** (⚙) > **Configuration** > **Dashboard**)

Displaying relative occurrences of events (bar graphs)

For bar graphs in the Custom Analysis widget, the colored bars in the widget background show the relative number of occurrences of each event. Read the bars from right to left.

The **Direction icon** indicates and controls the sort order of the display. A downward-pointing icon indicates descending order; an upward-pointing icon indicates ascending order. To change the sort order, click the icon.

Next to each event, the widget can display one of three icons to indicate any changes from the most recent results:

- The new event icon **Add** (+) signifies that the event is new to the results.
- The **Up Arrow icon** indicates that the event has moved up in the standings since the last time the widget updated. A number indicating how many places the event has moved up appears next to the icon.
- The **Down Arrow icon** indicates that the event has moved down in the standings since the last time the widget updated. A number indicating how many places the event has moved down appears next to the icon.

Displaying events over time (line graphs)

If you want information on events or other collected data over time, you can configure the Custom Analysis widget to display a line graph, such as one that displays the total number of intrusion events generated in your deployment over time.

Limitations to the custom analysis widget

A Custom Analysis widget may indicate that you are unauthorized to view the data that is configured to display. For example, Maintenance Users are not authorized to view discovery events. As another example, the widget does not display information related to unlicensed features. However, you (and any other users who share the dashboard) can modify the widget preferences to display data that you can see, or even delete the widget. If you want to make sure that this does not happen, save the dashboard as private.

When viewing user data, the system displays only authoritative users.

When viewing URL category information, the system does not display uncategorized URLs.

When viewing intrusion events aggregated by **Count**, the count includes reviewed events for intrusion events; if you view the count in tables on pages under the Analysis menus, the count will not include reviewed events.



Note In a multidomain deployment, the system builds a separate network map for each leaf domain. As a result, a leaf domain can contain an IP address that is unique within its network, but identical to an IP address in another leaf domain. When you view Custom Analysis widgets in an ancestor domain, multiple instances of that repeated IP address can be displayed. At first glance, they might appear to be duplicate entries. However, if you drill down to the host profile information for each IP address, the system shows that they belong to different leaf domains.

How to create dashboard widgets for a device

Any widgets that show events from devices can be configured to use a filter that limits the display of events for a given device or a set of devices.

1. Create and save a search: Go to **Analysis** > **Search** and enter the search parameters to match the specific device names.

Note You must provide exact text match as there is no drop-down listing the deployed device names.

2. Go to **Overview** > **Dashboards heading** > **Dashboard**, then click **Add Widgets** to create a **Custom Analysis** widget.
3. Return to **Overview** > **Dashboards heading** > **Dashboard** and modify the new widget to customize with the scope of search.

Example: configuration of custom analysis widget

You can configure the Custom Analysis widget to display a list of recent intrusion events by configuring the widget to display data from the **Intrusion Events** table. Choosing the **Classification** field and aggregating this data by **Count** displays the number of events that were generated for each type.

On the other hand, aggregating by **Unique Events** displays the number of unique intrusion events of each type (for example, how many detections of network trojans, potential violations of corporate policy, attempted denial-of-service attacks, and so on).

You can further customize the widget using a saved search, either one of the predefined searches delivered with your appliance or a custom search that you created. For example, constraining the first example (intrusion events using the **Classification** field, aggregated by **Count**) using the **Dropped Events** search displays the number of intrusion events that were dropped for each type.

Related Topics

Modify dashboard time settings, on page 22

Custom analysis widget preferences

This table describes the preferences you can set in the Custom Analysis widget.

Different preferences appear depending on how you configure the widget. For example, a different set of preferences appears if you configure the widget to show relative occurrences of events (a bar graph) vs a graph over time (a line graph). Some preferences, such as **Filter**, only appear if you choose a specific table from which to display data.

Table 2: Custom analysis widget preferences

Preference	Details
Title	If you do not specify a title for the widget, the system uses the configured event type as the title.
Preset	Custom Analysis presets provide quick access to information about your deployment. The predefined dashboards make extensive use of these presets. You can use these presets or you can create a custom configuration.
Table (required)	The table of events or assets that contains the data the widget displays.
Field (required)	The specific field of the event type you want to display. To show data over time (line graphs), choose **Time**. To show relative occurrences of events (bar graphs), choose another option.

Preference	Details
Aggregate (required)	The aggregation method configures how the widget groups the data it displays. For most event types, the default option is **Count**.
Filter	You can use application filters to constrain data from the Application Statistics and Intrusion Event Statistics by Application tables.
Search	You can use a saved search to constrain the data that the widget displays. You do not have to specify a search, although some presets use predefined searches. Only you can access searches that you have saved as private. If you configure the widget on a shared dashboard and constrain its events using a private search, the widget resets to not using the search when another user logs in. This affects your view of the widget as well. If you want to make sure that this does not happen, save the dashboard as private. Only fields that constrain connection summaries can constrain Custom Analysis dashboard widgets based on connection events. Saved searches with invalid search constraints do not appear under search. If you constrain a Custom Analysis widget using a saved search, then edit the search, the widget does not reflect your changes until the next time it updates.
Show	Choose whether you want to display the most (**Top**) or the least (**Bottom**) frequently occurring events.
Results	Choose the number of result rows to display.
Show Movers	Choose whether you want to display the icons that indicate changes from the most recent results.
Time Zone	Choose the time zone you want to use to display results.
Color	You can change the color of the bars in the widget's bar graph.

Related Topics

Configure widget preferences, on page 20

View associated events from the custom analysis widget

From a Custom Analysis widget, you can invoke an event view (workflow) that provides detailed information about the events displayed in the widget. The events appear in the default workflow for that event type, constrained by the dashboard time range. This also changes the appropriate time window on the Firewall Management Center, depending on how many time windows you configured and on the event type.

For example:

- If you configure multiple time windows, then access health events from a Custom Analysis widget, the events appear in the default health events workflow, and the health monitoring time window changes to the dashboard time range.
- If you configure a single time window and then access any type of event from the Custom Analysis widget, the events appear in the default workflow for that event type, and the global time window changes to the dashboard time range.

Procedure

Step 1 View the dashboard you want to modify. For more information on viewing dashboard, refer to View dashboards, on page 24.

Step 2 Choose one of the following options:

- On any custom analysis widget, click **View** ( ) in the lower right corner of the widget to view all associated events, constrained by the widget preferences.
- On a custom analysis widget showing relative occurrences of events (bar graph), click any event to view associated events constrained by the widget preferences, as well as by that event.

Disk usage widget categories and features

The disk usage widget displays the percentage of space used on the hard drive, organized by disk usage categories. It also shows the usage and capacity of each partition of the appliance's hard drive. The disk usage widget displays the same information for the malware storage pack if installed in the device, or if the Firewall Management Center manages a device containing a malware storage pack. This widget appears by default on the Status tabs of the Default Dashboard and the Summary Dashboard.

The **By Category** stacked bar displays each disk usage category as a proportion of the total available disk space used. The table describes the available categories.

Table 3: Disk usage categories

Disk Usage Category	Description
Events	All events logged by the system
Files	All files stored by the system
Backups	All backup files
Updates	All files related to updates, such as rule updates and system updates
Other	System troubleshooting files and other miscellaneous files
Free	Free space remaining on the appliance

Hover your pointer over a disk usage category in the stacked bar to view the percentage of available disk space used by that category, the actual storage space on the disk, and the total disk space available for that category. If your device has a malware storage pack, the Files category shows the space on the malware storage pack.

You can configure the widget to display only the **By Category** stacked bar, or you can show the stacked bar plus the admin (`/`), `/Volume`, and `/boot` partition usage, as well as the `/var/storage` partition if the malware storage pack is installed, by modifying the widget preferences.

Use widget preferences to control how often the widget updates and whether it displays current disk usage or collected disk usage statistics over the dashboard time range.

The interface traffic widget

The Interface Traffic widget shows the rate of traffic received (Rx) and transmitted (Tx) on the appliance's management interface. The widget does not appear by default on any of the predefined dashboards.

The widget preferences control how often the widget updates.

This widget displays the input and output rates from Snort. Note that the traffic rates in the **Interface** dashboard (**System** (⚙) > **Health** > **Monitor** page) may differ, as those values are collected from Lina.

Devices with Malware Defense licenses enabled periodically attempt to connect to the AMP cloud even if you have not configured dynamic analysis. Because of this, these devices show transmitted traffic; this is expected behavior.

The intrusion events widget

The **Intrusion Events** widget shows the intrusion events that occurred over the dashboard time range, organized by priority. This includes statistics on intrusion events with dropped packets and different impacts. This widget appears by default on the **Intrusion Events** tab of the **Summary Dashboard**.

Widget preferences

In the widget preferences, you can choose:

- **Event Flags** to display separate graphs for events with dropped packets, would have dropped packets, or specific impacts. Choose **All** to display an additional graph for all intrusion events, regardless of impact or rule state.

  For explanations of the icons, see Intrusion Events. The arrow (if any) that appears above the impact level numbers describes the inline result and is defined as follows:

  Table 4: Inline Result Field Contents in Workflow and Table Views

This Icon	Indicates
	The system dropped the packet that triggered the rule.
	IPS would have dropped the packet if you enabled the **Drop when Inline** intrusion policy option (in an inline deployment), or if a Drop and Generate rule generated the event while the system was pruning.
	IPS may have transmitted or delivered the packet to the destination, but the connection that contained this packet is now blocked.
No icon (blank)	The triggered rule was not set to Drop and Generate Events

  In a passive deployment, the system does not drop packets, including when an inline interface is in tap mode, regardless of the rule state or the inline drop behavior of the intrusion policy.

- **Show** to specify **Average Events Per Second** (EPS) or **Total Events**.
- **Vertical Scale** to specify **Linear** (incremental) or **Logarithmic** (factor of ten) scale.
- How often the widget updates.

Widget actions

On the widget, you can:

- Click a graph corresponding to dropped packets, to would have dropped packets, or to a specific impact to view intrusion events of that type.
- Click the graph corresponding to dropped events to view dropped events.
- Click the graph corresponding to would have dropped events to view would have dropped events.
- Click the **All** graph to view all intrusion events.

The resulting event view is constrained by the dashboard time range; accessing intrusion events via the dashboard changes the events (or global) time window for the appliance. Note that packets in a passive deployment are not dropped, regardless of intrusion rule state or the inline drop behavior of the intrusion policy.

Network compliance widget

The Network Compliance widget summarizes your hosts' compliance with the allow lists you configured. By default, the widget displays a pie chart that shows the number of hosts that are compliant, non-compliant, and that have not been evaluated, for all compliance allow lists in active correlation policies. This widget appears by default on the Correlation tab of the Detailed Dashboard.

You can configure the widget to display network compliance either for all allow lists or for a specific allow list by modifying the widget preferences.

If you choose to display network compliance for all allow lists, the widget considers a host to be non-compliant if it is not compliant with any allow list in an active correlation policy.

The preferences control how often the widget updates. You can check the **Show Not Evaluated** box to hide events which have not been evaluated.

You can also use the widget preferences to specify which of these three different styles you want to use to display network compliance:

- The **Network Compliance** style (the default) displays a pie chart that shows the number of hosts that are compliant, non-compliant, and that have not been evaluated. You can click the pie chart to view the host violation count, which lists the hosts that violate at least one allow list.
- The **Network Compliance over Time (%)** style displays a stacked area graph showing the relative proportion of hosts that are compliant, non-compliant, and that have not yet been evaluated, over the dashboard time range.
- The **Network Compliance over Time** style displays a line graph that shows the number of hosts that are compliant, non-compliant, and that have not yet been evaluated, over the dashboard time range.

The product licensing widget

The Product Licensing widget shows the device and feature licenses currently installed on the Firewall Management Center. It also indicates the number of items licensed and the number of remaining licensed items allowed. It does not appear by default on any of the predefined dashboards.

The top section of the widget displays all device and feature licenses installed on the Firewall Management Center, including temporary licenses, while the Expiring Licenses section displays only temporary and expired licenses.

The bars in the widget background show the percentage of each type of license that is being used; you should read the bars from right to left. Expired licenses are marked with a strikethrough.

You can configure the widget to display either the features that are currently licensed, or all the features that you can license, by modifying the widget preferences. The preferences also control how often the widget updates.

You can click any of the license types to go to the License page of the local configuration and add or delete feature licenses.

Product updates widget

The Product Updates widget provides you with a summary of the software currently installed on the appliance as well as information on updates that you have downloaded, but not yet installed. This widget appears by default on the Status tabs of the **Detailed Dashboard** and the **Summary Dashboard**.

Because the widget uses scheduled tasks to determine the latest version, it displays `Unknown` until you configure a scheduled task to download, push or install updates.

You can configure the widget to hide the latest versions by modifying the widget preferences. The preferences also control how often the widget updates.

The widget also provides you with links to pages where you can update the software. You can:

- Manually update an appliance by clicking the current version.
- Create a scheduled task to download an update by clicking the latest version.

RSS feed widget

The RSS Feed widget adds an RSS feed to a dashboard. By default, the widget shows a feed of Cisco security news. It appears by default on the Status tabs of the Detailed Dashboard and the Summary Dashboard.

You can also configure the widget to display a preconfigured feed of company news, the Snort.org blog, or the Cisco Threat Research blog, or you can create a custom connection to any other RSS feed by specifying its URL in the widget preferences. The Firewall Management Center can display encrypted RSS feeds only if they use trusted server certificates signed by a certificate authority (CA) that the Firewall Management Center recognizes. If you configure the RSS Feed widget to display an encrypted RSS feed that uses a CA the Firewall Management Center does not recognize, or that uses a self-signed certificate, the verification fails and the widget does not display the feed.

Feeds update every 24 hours (although you can manually update the feed), and the widget displays the last time the feed was updated based on the local time of the appliance. Keep in mind that the appliance must have access to the web site (for the two preconfigured feeds) or to any custom feed you configure.

When you configure the widget, you can also choose how many stories from the feed you want to show in the widget, as well as whether you want to show descriptions of the stories along with the headlines; keep in mind that not all RSS feeds use descriptions.

On the RSS Feed widget, you can:

- Click one of the stories in the feed to view the story.

- Click the **more** link to go to the feed's web site.
- Click **Refresh** ( ) to manually update the feed.

The shadow traffic widget

The Shadow Traffic Widget provides information about network traffic that bypasses the intended visibility or access control measures of threat defense devices. Various techniques can be used to create shadow traffic and this widget displays the number of connections and other details for these techniques.

Evasive VPN

Evasive VPN is network traffic that circumvents network restrictions and firewall rules by using techniques such as traffic masking or protocol obfuscation, making VPN traffic appear similar to regular web traffic.

This widget displays the total number of evasive VPN connections, along with the process or application name identified by the Encrypted Visibility Engine (EVE) for each connection. To view detailed connection events for a specific EVE process or application, click the **EVE Process Name** or **Application** name at the bottom of the widget. This action opens the **Connection Events** window, where all connections associated with the selected **EVE Process Name** or **Application** name and classified as **Evasive VPN** traffic are filtered and displayed.

Recommended action: To block evasive VPN traffic, create or update an access control rule to block traffic to the identified EVE processes or application.

Encrypted DNS

Encrypted DNS traffic refers to DNS queries that are secured using advanced encryption protocols, making it difficult for traditional DNS filtering systems and firewalls to inspect or block them.

This widget displays the total number of encrypted DNS connections and highlights the top responder IP addresses, identified from known resolver lists. To view detailed connection events for a specific responder IP address, click the **Responder IP** address at the bottom of the widget. This action opens the **Connection Events** window, where all connections associated with the selected **Responder IP** address and classified as **Encrypted DNS** traffic are filtered and displayed.

Recommended action: To block encrypted DNS traffic, create or update an access control rule to block traffic to the identified responder IP addresses.

Domain fronting

Domain fronting is a traffic concealment technique that conceals the actual destination of encrypted traffic by advertising a widely trusted front domain during the TLS handshake (using the SNI field), while the HTTP Host header inside the encrypted session specifies a different backend service hosted by the same provider. This technique can bypass basic domain-based filtering and requires advanced traffic inspection for reliable detection.

This widget displays the total number of connections and highlights the top server names that are identified as domain fronting URLs. To view detailed connection events for a specific server, click the **Server Name** at the bottom of the widget. This action opens the **Connection Events** window, where all connections associated with the selected server name and classified as **Domain Fronting** traffic are filtered and displayed.

Note Domain fronting is detected only when decryption is enabled.

Recommended action: To block domain fronting traffic, create or update an access control rule to block traffic to the identified server URLs. You can also block domain fronting traffic by creating a custom detector to match a set of related server URLs, and then add a rule to block the custom application.

Multihop proxies

A multihop proxy is a traffic routing mechanism that routes internet traffic through multiple intermediary servers before reaching the final destination, adding additional layers of obfuscation and privacy.

This widget displays the total number of multihop proxy connections and highlights the top responder IP addresses, identified from known resolver lists. To view detailed connection events for a specific responder IP address, click the **Responder IP** address at the bottom of the widget. This action opens the **Connection Events** window, where all connections associated with the selected **Responder IP** address and classified as **Multihop Proxy** traffic are filtered and displayed.

Recommended action: To block multihop proxy traffic, create or update an access control rule to block traffic to the identified responder IP addresses.

Fake TLS

Fake TLS is a TLS evasion technique that attempts to evade basic domain-based filtering by presenting a trusted domain name during a TLS/HTTPS session, while actually connecting to infrastructure not legitimately associated with that domain. Also, parts of the TLS handshake, such as cipher suite lists and extensions, can be faked or modified to appear legitimate, and may include unusual or unregistered cipher suites.

This widget displays the total number of fake TLS traffic connections and highlights the top responder IP addresses, identified from known resolver lists. To view detailed connection events for a specific responder IP address, click the **Responder IP** address at the bottom of the widget. This action opens the **Connection Events** window, where all connections associated with the selected **Responder IP** address and classified as **Fake TLS** traffic are filtered and displayed.

Note Fake TLS traffic is detected only when EVE is enabled.

Recommended action: To block fake TLS traffic, create or update an access control rule to block traffic to the identified responder IP addresses.

The system load widget

The System Load widget shows the CPU usage (for each CPU), memory (RAM) usage, and system load (also called the load average, measured by the number of processes waiting to execute) on the appliance, both currently and over the dashboard time range. It appears by default on the Status tabs of the Detailed Dashboard and the Summary Dashboard.

You can configure the widget to show or hide the load average by modifying the widget preferences. The preferences also control how often the widget updates.

System time widget

The **System Time** widget shows the local system time, uptime, and boot time for the appliance. It appears by default on the Status tabs of the **Detailed Dashboard** and the **Summary Dashboard**.

You can configure the widget to hide the boot time by modifying the widget preferences. The preferences also control how often the widget synchronizes with the appliance's clock.

Manage dashboards

Manage dashboards to customize your monitoring interface by creating, deleting, and modifying dashboards and their widgets to meet your specific operational requirements.

Procedure

Step 1 Choose **Overview** > **Dashboards** > **Management**, and then manage your dashboards:

- Create Dashboards: Create a custom dashboard; refer to Create custom dashboards, on page 20.
- Delete Dashboards: To delete a dashboard, click **Delete** ( ) next to the dashboard you want to delete. If you delete your default dashboard, you must define a new default or the appliance prompts you to choose a dashboard every time you attempt to view a dashboard.
- Edit Options: Edit custom dashboard options; refer to Edit dashboard options, on page 21.
- Modify Time Constraints: Modify the time display or pause/unpause the dashboard as described in Modify dashboard time settings, on page 22.

Step 2 To modify a single dashboard, choose **Overview** > **Dashboards heading** > **Dashboard**, and then go to the dashboard you want to modify.

Step 3 Add, delete, or rename dashboard tabs.

- For more information about adding a dashboard tab, refer to Add a dashboard, on page 18.
- For more information about renaming a dashboard tab, refer to Rename a dashboard, on page 23.
- To delete a dashboard tab, click **Close** ( ).

Note You cannot change the order of dashboards.

Step 4 Manage dashboard widgets:

- Add Widgets: Add widgets to a dashboard; refer to Adding widgets to a dashboard, on page 18.
- Configure Preferences: Configure widget preferences; refer to Configure widget preferences, on page 20.
- Customize Display: Customize the widget display; refer to Customize the widget display, on page 19.
- View Events: View associated events from the Custom Analysis Widget; refer to View associated events from the custom analysis widget, on page 10.

Note Every configuration of the Custom Analysis widget in the Cisco predefined dashboards corresponds to a system preset for that widget. If you change or delete one of these widgets, you can restore it by creating a new Custom Analysis widget based on the appropriate preset.

Add a dashboard

Add a dashboard to customize your security monitoring interface and organize relevant data displays for your specific operational needs.

Use this procedure when you need to create a new dashboard to group related monitoring widgets and data visualizations for your security environment.

Procedure

Step 1 View the dashboard you want to modify; see View dashboards, on page 24.

Step 2 Click **Add** (+).

Step 3 Enter a name.

Step 4 Click **OK**.

The new dashboard is created and becomes available in your dashboard list for configuration and use.

Adding widgets to a dashboard

Add widgets to dashboard tabs to customize your monitoring and analysis capabilities. You can add up to 15 widgets per tab to create personalized views of system data and metrics.

Each tab can display one or more widgets in a three-column layout. When adding a widget to a dashboard, you choose the tab to which you want to add the widget. The system automatically adds it to the column with the fewest widgets. If all columns have an equal number of widgets, Firewall Management Center adds the new widget to the left-most column. You can add a maximum of 15 widgets to a dashboard tab.

Tip After you add widgets, you can move them to any location on the tab. You cannot, however, move widgets from tab to tab.

The dashboard widgets you see depend on your appliance type, your user role, and your current domain (in a multidomain deployment). If you have fewer permissions than the dashboard creator, you may not be able to use all of the widgets on the dashboard. Firewall Management Center displays unauthorized widgets as disabled.

Procedure

Step 1 View the dashboard where you want to add a widget. For instructions, refer to View dashboards, on page 24.

Step 2 Click the tab where you want to add the widget.

Step 3 Click **Add Widgets**. You can view the widgets in each category by clicking on the category name, or you can view all widgets by clicking **All Categories**.

Step 4 Click **Add** next to the widgets you want to add. The **Add Widgets** page shows how many widgets of each type are on the tab, including the one you want to add.

To add multiple widgets of the same type, click **Add** again.

Step 5 When you are finished adding widgets, click **Done** to return to the dashboard.

What to do next

- If you added a **Custom Analysis** widget, configure the widget preferences. For more information, refer to Configure widget preferences, on page 20.

Related Topics

Widget availability by appliance, user role, and domain, on page 3

Customize the widget display

Customize widget display to optimize dashboard layout and focus on relevant information. You can minimize and maximize widgets, as well as rearrange the widgets on a tab.

Procedure

Step 1 View a dashboard. For more information, refer to View dashboards, on page 24.

Step 2 Customize the widget display:

- To rearrange a widget on a tab, click the title bar of the widget you want to move, then drag it to its new location.

Note You cannot move widgets from tab to tab. If you want a widget to appear on a different tab, you must delete it from the existing tab and add it to the new tab.

- To minimize or maximize a widget on the dashboard, click **Minimize** ( ) or **Maximize** ( ) in a widget's title bar.
- To delete a widget if you no longer want to view it on a tab, click **Close** ( ) in the title bar of the widget.

Configure widget preferences

Configure widget preferences to customize the behavior and functionality of individual widgets according to your specific requirements.

Procedure

Step 1 On the title bar of the widget whose preferences you want to change, click **Show Preferences** ( ).

Step 2 Make changes as needed.

Step 3 On the widget title bar, click **Hide Preferences** ( ) to hide the preferences section.

Create custom dashboards

Custom dashboards allow you to organize and display specific data visualizations that meet your monitoring requirements and provide tailored views of your network security information.

Create new dashboards to customize your monitoring environment. Alternatively, you can export dashboards from other appliances and import them to save time. You can then edit the imported dashboard to suit your needs.

Procedure

Step 1 Choose **Overview** > **Dashboards** > **Management**.

Step 2 Click **Create Dashboard**.

Step 3 Modify the custom dashboard options as described in Custom dashboard options, on page 20.

Step 4 Click **Save**.

Custom dashboard options

This table describes options you can use when creating or editing custom dashboards.

Table 5: Custom dashboard options

Option	Description
Copy Dashboard	When you create a custom dashboard, you can choose to base it on any existing dashboard, whether user-created or system-defined. This option makes a copy of the preexisting dashboard, which you can modify to suit your needs. Optionally, you can create a blank new dashboard by choosing **None**. This option is available only when you create a new dashboard. In a multidomain deployment, you can copy any non-private dashboards from ancestor domains.
Name	A unique name for the custom dashboard.

Option	Description
Description	A brief description of the custom dashboard.
Change Tabs Every	Specifies (in minutes) how often the dashboard should cycle through its tabs. Unless you pause the dashboard or your dashboard has only one tab, this setting advances your view to the next tab at the interval you specify. To disable tab cycling, enter `0` in the **Change Tabs Every** field.
Refresh Page Every	Determines how often the entire dashboard page automatically refreshes. Refreshing the entire dashboard allows you to see any preference or layout changes that were made to a shared dashboard by another user, or that you made to a private dashboard on another computer, since the last time the dashboard refreshed. A frequent refresh can be useful, for example, in a networks operations center (NOC) where a dashboard is displayed at all times. If you make changes to the dashboard at a local computer, the dashboard in the NOC automatically refreshes at the interval you specify, and no manual refresh is required. This refresh does not update the data, and you do not need to refresh the entire dashboard to see data updates; individual widgets update according to their preferences. This value must be greater than the **Change Tabs Every** setting. Unless you pause the dashboard, this setting will refresh the entire dashboard at the interval you specify. To disable the periodic page refresh, enter `0` in the **Refresh Page Every** field. **Note** This setting is separate from the update interval available on many individual widgets; although refreshing the dashboard page resets the update interval on individual widgets, widgets will update according to their individual preferences even if you disable the **Refresh Page Every** setting.
Save As Private	Determines whether the custom dashboard can be viewed and modified by all users of the appliance or is associated with your user account and reserved solely for your own use. Keep in mind that any user with dashboard access, regardless of role, can modify shared dashboards. If you want to make sure that only you can modify a particular dashboard, save it as private.

Edit dashboard options

Edit dashboard options to modify the configuration and settings of an existing dashboard to better meet your monitoring and analysis requirements.

Procedure

Step 1 View the dashboard you want to edit. For more information, refer to View dashboards, on page 24.

Step 2 Click **Edit** ( ).

Step 3 Change the options as described in Custom dashboard options, on page 20.

Step 4 Click **Save**.

Modify dashboard time settings

You can change the time range to reflect a period as short as the last hour (the default) or as long as the last year. When you change the time range, the widgets that can be constrained by time automatically update to reflect the new time range.

The maximum number of data points in any graph is 300, and the time setting determines how much time is summarized within each data point. This is the number of data points, and the time span covered, in the dashboards for each time range:

- 1 hour = 12 data points, 5 minutes each
- 6 hours = 72 data points, 5 minutes each
- 1 day = 288 data points, 5 minutes each
- 1 week = 300 data points, 33.6 minutes each
- 2 weeks = 300 data points, 67.2 minutes each
- 30 days = 300 data points, 144 minutes each
- 90 days = 300 data points, 432 minutes each
- 180 days = 300 data points, 864 minutes each
- 1 year = 300 data points, 1752 minutes each

Note that not all widgets can be constrained by time. For example, the dashboard time range has no effect on the Appliance Information widget, which provides information that includes the appliance name, model, and current version of the software. For more information about pre-defined tables that cannot be constrained by time, refer to Time constraints in dashboard tables, on page 23.

Keep in mind that for enterprise deployments of the Secure Firewall System, changing the time range to a long period may not be useful for widgets like the Custom Analysis widget, depending on how often newer events replace older events.

You can also pause a dashboard, which allows you to examine the data provided by the widgets without the display changing and interrupting your analysis. Pausing a dashboard has these effects:

- Individual widgets stop updating, regardless of any **Update Every** widget preference.
- Dashboard tabs stop cycling, regardless of the **Cycle Tabs Every** setting in the dashboard properties.
- Dashboard pages stop refreshing, regardless of the **Refresh Page Every** setting in the dashboard properties.
- Changing the time range has no effect.

When you are finished with your analysis, you can unpause the dashboard. Unpausing the dashboard causes all appropriate widgets on the page to update to reflect the current time range. In addition, dashboard tabs resume cycling and the dashboard page resumes refreshing according to the settings you specified in the dashboard properties.

If you experience connectivity problems or other issues that interrupt the flow of system information to the dashboard, the dashboard automatically pauses and an error notice appears until the problem is resolved.

Note Your session normally logs you out after 1 hour of inactivity (or another configured interval), regardless of whether the dashboard is paused. If you plan to passively monitor the dashboard for long periods of time, consider exempting some users from session timeout, or changing the system timeout settings.

Follow these steps to modify dashboard time settings:

Procedure

Step 1 View the dashboard where you want to add a widget; refer to View dashboards, on page 24.

Step 2 Optionally, to change the dashboard time range, choose a time range from the **Show the Last** drop-down list.

Step 3 Optionally, pause or unpause the dashboard on the time range control, using **Pause** ( ) or **Play** ( ).

Time constraints in dashboard tables

In Firewall Management Center, information about your network is collected and stored in structured data tables. When you view network information through a dashboard widget, Firewall Management Center retrieves the relevant data from these tables.

Tables can be classified into these categories based on ability to constrain by time:

- Tables that are event-based, such as **Connection Events** or **User Activity**, include a time column and can be constrained by event time, allowing you to filter data based on specific time ranges.
- Tables that are state-based, such as **Hosts**, do not have an associated event time and therefore cannot be constrained by time filters. These tables represent the current or recent state of the system rather than discrete events.

Consider this distinction while you are customizing your dashboard and analyzing network events. Ensure that you apply time-based filtering only when it is supported by the displayed data.

Rename a dashboard

Change the name of an existing dashboard to improve clarity or organizational structure.

Procedure

Step 1 View the dashboard you want to modify. For more information on viewing dashboard, refer to View dashboards, on page 24.

Step 2 Click the dashboard title you want to rename.

Step 3 Enter a new name.

Step 4 Click **OK**.

View dashboards

View dashboards to monitor and analyze data relevant to your appliance configuration and performance.

By default, the home page for your appliance displays the default dashboard. If you do not have a default dashboard defined, the home page shows the **Dashboard Management** page, where you can choose a dashboard to view.

Procedure

At any time, you can do one of the following:

- To view the default dashboard for your appliance, choose **Overview** > **Dashboards heading** > **Dashboard**.
- To view a specific dashboard, choose **Overview** > **Dashboards heading** > **Dashboard**, and choose the dashboard from the menu.
- To view all available dashboards, choose **Overview** > **Dashboards** > **Management**. You can then choose **View** () next to an individual dashboard to view it.