

FTD Dashboard

This chapter provides information about the FTD dashboard and describes the predefined widgets that offer an overview of your system.

- FTD dashboard, on page 1
- View the FTD dashboard, on page 2
- FTD dashboard widgets, on page 3
- Modify time settings for the FTD dashboard, on page 6

FTD dashboard

The FTD dashboard is a monitoring interface that

- provides an at-a-glance view of the status and events data collected by all Security Cloud Control-managed Firewall Threat Defense devices
- displays collective information related to device status and overall health of devices in your deployment, and
- uses tabs with predefined widgets that provide insights into different aspects of the system.

FTD dashboard capabilities

The information that the FTD dashboard provides depends on how you license, configure, and deploy the devices in your system. The FTD dashboard displays data for all Security Cloud Control-managed Firewall Threat Defense devices, but you can choose to filter device-based data. You can also choose the time range to display for specific time range.

This dashboard uses tabs to display predefined widgets: small, self-contained components that provide insights into different aspects of the system. For example, the Network Activity widget shows you event graphs that display information about all connection, malware, and intrusion events. The widgets in the dashboard are predefined and cannot be customized. This dashboard is visible to all Security Cloud Control users who have access to a Security Cloud Control tenant.

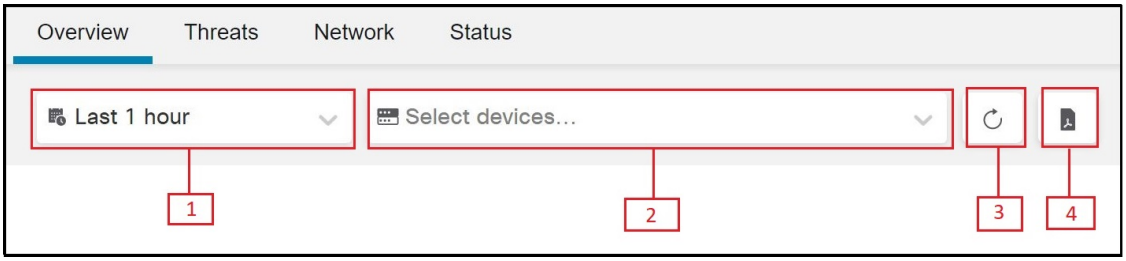
- The dashboard does not displays any event statistics for historic events.
- Since the aggregation service batch processes the events to aggregate every five minutes, you can expect a five-minute latency between the time the events are aggregated to the time the statistics are displayed.

The dashboard provides these control options:

Table 1: FTD dashboard controls

Number	Description
1	Allows you to change the time range to reflect a period as short as the last hour or as long as the last year. When you change the time range, the widgets automatically update the events data to reflect the new time range.
2	Allows you to filter the events data based on selected devices. If no devices are selected, the widgets display all available events data.
3	Reinitiates the events data query
4	Displays the events data in a PDF output format. You can choose to download or save a copy of this PDF on your local machine.

Figure 1: FTD dashboard



View the FTD dashboard

From the Security Cloud Control menu, choose **Insights & Reports** > **Firewall Threat Defense** > **Dashboard** to view the **FTD Dashboard**.

By default, the home page for your tenant displays the **Overview** tab.

The dashboard includes widgets that are listed under each tab: Threat, Network, Applications, and Status tab.

Table 2: FTD dashboard tabs and widgets

Name of the Tab	Available Widgets
Overview	All available widgets
Threat	• Top Intrusion Rules • Top Intrusion Attackers • Top Intrusion Targets • Top Malware Signatures • Top Malware Senders • Top Malware Receivers • Malware Events by Disposition

Name of the Tab	Available Widgets
Network	• Network Activity • Event Activity • Access Control Actions • Top Access Control Policies • Top Access Control Rules • Top Devices • Top Users • Top Users by Blocked Connections
Status	• Top Devices with Health Alerts • Top Loaded Devices
Applications	• Top Web Applications • Top Client Applications • Blocked Web Applications

FTD dashboard widgets

FTD dashboard widgets are predefined display components that

- provide at-a-glance views of current system status
- display data about events collected and generated by Firewall Threat Defense devices managed FMC, and
- show information about the status and overall health of the devices in your deployment.

Top intrusion rules widget

A Top Intrusion Rules Widget is a dashboard widget that displays counts of the intrusion events that have occurred over the specified time range and are organized by priority, includes statistics on intrusion events with dropped packets and different impacts, and provides a scrollable generated list.

Top intrusion attackers widget

The **Top Intrusion Attackers** widget displays counts of intrusion events for the top attacking host IP addresses (causing those events) on your monitored network.

Top intrusion targets widget

A Top Intrusion Targets widget is a dashboard component that displays counts of intrusion events for the top target host IP addresses (targeted in the connections causing those events) on your monitored network.

Top malware signatures widget

The **Top Malware Signatures** widget displays counts of the top malware signatures detected in the network traffic for top file-sending host IP addresses.

Top malware senders widget

The **Top Malware Senders** widget displays counts of the top malware threats that are detected in the network traffic for top file-sending host IP addresses.

Top malware receivers widget

The **Top Malware Receivers** widget displays counts of the top malware threats that are detected in the network traffic for all top file-receiving host IP addresses.

Malware events by disposition widget

The **Malware Events by Disposition** widget is a display component that shows counts of all disposition of malware events that are generated when the managed device detects a file containing malware.

Network activity widget

The **Network Activity** widget displays all ingress and egress data rate that is based on information from the connection events.

Event activity widget

The **Event Activity** widget displays counts of events that have occurred in the last hour and the total number of each event type that is available in the database.

Access Control Actions Widget

The **Access Control Actions** widget displays counts of events that are logged based on the allowed or blocked access control actions for each event. If you hover on the pie chart, you can view the percentage of the allowed and blocked actions.

Top access control policies widget

The **Top Access Control Policies** widget displays counts of top access control policies generating events.

Top access control rules widget

The **Top Access Control Rules** widget is a dashboard component that

- displays the top five counts of the access control rules that are used for each event
- provides sorting capabilities by bytes or events, and
- helps monitor network security policy effectiveness.

Top devices widget

The **Top Devices** widget displays counts of events per devices. These count can be sorted by bytes or events.

Top users widget

The **Top Users** widget is a network monitoring display that

- displays a list of users on your monitored network that are associated with the highest intrusion event counts
- draws data primarily from the intrusion detection (IDS) User Statistics and Intrusion Events tables, and
- displays authoritative user data.

Top users by blocked connections widget

A **Top Users by Blocked Connections** widget is a network monitoring tool that displays users who have the highest number of blocked connection events associated with them in your monitored network.

Top devices with health alerts widget

The **Top Devices with Health Alerts** widget displays the current compiled health status for Security Cloud Control-managed Firewall Threat Defense devices.

Top loaded devices widget

The **Top Loaded Devices** widget displays a list of Secure Firewall Threat Defense devices along with the CPU usage information.

Top web applications widget

A Top Web Applications widget is a network monitoring interface element that displays the web applications that are associated with the highest number of connection events in your monitored network and allows you to sort this list based on bytes or event count.

Top client applications widget

The **Top Client Applications** widget displays the most used client applications in your monitored network. You can sort this list based on bytes or event count.

Top blocked web applications widget

A **Top Blocked Web Applications** widget is a network monitoring display that shows the top web applications that are associated with blocked connection events and the count of blocked connection events in your monitored network.

Modify time settings for the FTD dashboard

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. These are the number of data points, and the time span covered, in the FTD dashboard 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