FTD Dashboard

About the FTD Dashboard

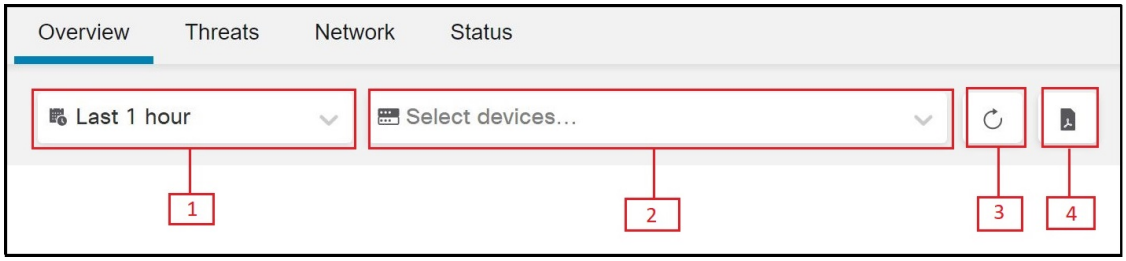
The FTD dashboard provides you an at-a-glance view of the status, including events data collected and generated by all CDO-managed threat defense devices.

You can use this dashboard to view collective information that is related to the device status and the overall health of the devices in your deployment. The information that the FTD dashboard provides depends on how you license, configure, and deploy the devices in your system. Although, the FTD dashboard displays data for all CDO-managed threat defense devices, 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 CDO users who have access to a CDO 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.

Figure 1: FTD Dashboard



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.

View the FTD Dashboard

From the CDO menu, choose **Analytics** > **FTD 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, Application and Users, and Status tab.

The following table lists the widgets available under each tab:

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
Network	• Network Activity • Event Activity • Access Control Actions • Top Access Control Policies • Top Access Control Rules • Top Devices • Top Users

Name of the Tab	Available Widgets
Status	• Unhealthy Devices • Top Loaded Devices

The FTD Dashboard Widgets

The FTD dashboard displays predefined widgets that can provide you with at-a-glance views of the current system status. These views include:

- Data about the events collected and generated by threat defense devices managed FMC.
- Information about the status and the overall health of the devices in your deployment.

The Top Intrusion Rules Widget

The **Top Intrusion Rules** widget displays counts of the intrusion events that have occurred over the specified time range and are organized by priority. These counts include statistics on intrusion events with dropped packets and different impacts. The generated list is scrollable.

The 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.

The Top Intrusion Targets Widget

The **Top Intrusion Targets** widget displays counts of intrusion events for the top target host IP addresses (targeted in the connections causing those events) on your monitored network.

The 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.

The 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.

The 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.

The Malware Events by Disposition Widget

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

The Network Activity Widget

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

The 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.

The 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.

The Top Access Control Policies Widget

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

The Top Access Control Rules Widget

The **Top Access Control Rules** widget displays the top five counts of the access control rules that are used for each event. These counts can be sorted by bytes or events.

The Top Devices Widget

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

The Top Users Widget

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

The Unhealthy Devices Widget

The **Unhealthy Devices** widget displays the current compiled health status for CDO-managed threat defense devices.

The Top Loaded Devices Widget

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

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. Following is 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