## FMC System Monitoring

### Dashboard Widget Availability by User Role

The following 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.

| Widget | Administrator | Maintenance User | Security Analyst | Security Analyst (RO) |
| --- | --- | --- | --- | --- |
| 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 |
| White List Events | yes | no | yes | yes |
|  | | | | |

## Monitoring Traffic and System Dashboards

|  |  |
| --- | --- |
| **Step 1** | Select predefined time ranges, such as the last hour or week, or define a custom time range with specific start and end times, to control the data shown in the dashboard graphs and tables.  Traffic-related dashboards include the following types of display:   * Top 5 bar graphs—these are shown in the **Network Overview** dashboard, and in the per-item summary dashboards you see if you click on an item in a dashboard table. You can toggle the information between a count of **Transactions** or **Data Usage** (total bytes sent and received). You can also toggle the display to show all transactions, allowed transactions, or denied transactions. Click the **View More** link to see the table associated with the graph. * Tables—Tables show items of a particular type (for example, applications or web categories) with that item's total transactions, allowed transactions, blocked transactions, data usage, and bytes sent and received. You can toggle the numbers between raw **Values** and **Percentages**, and show the top 10, 100, or 1000 entries. If the item is a link, click it to see a summary dashboard with more detailed information. |
| **Step 2** | Click the **Dashboard** links in the table of contents to see dashboards for the following data:   * **Network Overview**—Shows summary information about the traffic in the network, including the access rules (policies) matched, users initiating traffic, applications used in connections, intrusion threats (signatures) matched, web categories for URLs accessed, and the most frequent destinations for connections. * **Users**—Shows the top users of your network. You must configure identity policies to see user information. You might see the following special entities:   + **Failed Authentication**—the user was prompted to authenticate, but failed to enter a valid username/password pair within the maximum number of allowed attempts. Failure to authenticate does not itself prevent the user from accessing the network, but you can write an access rule to limit network access for these users.   + **Guest**—Guest users are like Failed Authentication users, except that your identity rule is configured to call these users Guest. Guest users were prompted to authenticate and failed to do so within the maximum number of attempts.   + **No Authentication Required**—the user was not prompted to authentication, because the user's connections matched identity rules that specified no authentication.   + **Unknown**—there is no user mapping for the IP address, and there is no record of failed authentication yet. Typically, this means that no HTTP traffic has yet been seen from that address. * **Applications**—Shows the top applications, such as HTTP, that are being used in the network. The information is available only for connections that are inspected. Connections are inspected if they match an “allow” rule, or a block rule that uses criteria other than zone, address, and port. Thus, application information is not available if the connection is trusted or blocked prior to hitting any rule that requires inspection. * **Web Categories**—shows the top categories of web sites, such as Gambling or Educational Institutions that are being used in the network based on the categorization of web sites visited. You must have at least one access control rule that uses URL category as a traffic matching criteria to get this information. The information will be available for traffic that matches the rule, or for traffic that has to be inspected to determine if it matches the rule. You will not see category (or reputation) information for connections that match rules that come before the first web-category access control rule. * **Policies**—Shows the top access rules matched by network traffic. * **Ingress Zones**—shows the top security zones through which traffic is entering the device. * **Egress Zones**—shows the top security zones through which traffic is exiting the device. * **Destinations**—Shows the top destinations for network traffic. * **Attackers**—Shows the top attackers, which are the source of connections that trigger intrusion events. You must configure intrusion policies on access rules to see this information. * **Targets**—Shows the top targets of intrusion events, which are the victims of an attack. You must configure intrusion policies on access rules to see this information. * **Threats**—Shows the top intrusion rules that have been triggered. You must configure intrusion policies on access rules to see this information. * **File Logs**—shows the top file types seen in network traffic. You must configure file policies on access rules to see this information. * **System**— Shows an overall system view, including a display of interfaces and their status (mouse over an interface to see its IP addresses), overall average system throughput (in 5 minute buckets for up to one hour, and one hour buckets for longer periods), and summary information on system events, CPU usage, memory usage, and disk usage. You can restrict the throughput graph to show a specific interface rather than all interfaces. Interface-related statistics such as throughput does not include sub-interfaces.  Health Modules Because health monitoring is an administrative activity, only users with administrator user role privileges can access system health data.   * [Health Modules](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Health_Monitoring.html#ID-2227-00000049) * [Configuring Health Monitoring](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Health_Monitoring.html#ID-2227-000001a9)   Health Modules  *Health modules,* or *health tests,* test for the criteria you specify in a health policy.   | Module | Appliances | Description | | --- | --- | --- | | AMP for Endpoints Status | Management Center | The module alerts if the Firepower Management Center cannot connect to the AMP cloud or Cisco AMP Private Cloud (AMPv) after an initial successful connection, or if AMPv cannot contact the AMP cloud. It also alerts if you deregister an AMP cloud connection using the AMP for Endpoints management console. | | AMP for Firepower Status  (AMP for Networks Status) | Management Center | This module alerts if:   * The Firepower Management Center cannot contact the AMP cloud, a Cisco AMP Private Cloud (AMPv), the AMP Threat Grid cloud, an AMP Threat Grid on-premises appliance, or AMPv cannot contact the AMP cloud. * The encryption keys used for the connection are invalid. * A device cannot contact the AMP Threat Grid cloud or an AMP Threat Grid on-premises appliance to submit files for dynamic analysis. * An excessive number of files are detected in network traffic based on the file policy configuration.   If your Firepower Management Center loses connectivity to the Internet, the system may take up to 30 minutes to generate an AMP for Firepower Status health alert. | | Appliance Heartbeat | Any | This module determines if an appliance heartbeat is being heard from the appliance and alerts based on the appliance heartbeat status. | | CPU Usage | Any | This module checks that the CPU on the appliance is not overloaded and alerts when CPU usage exceeds the percentages configured for the module. | | Card Reset | Any | This module checks for network cards which have restarted due to hardware failure and alerts when a reset occurs. | | Disk Status | Any | This module examines performance of the hard disk, and malware storage pack (if installed) on the appliance. This module generates a Warning (yellow) health alert when the hard disk and RAID controller (if installed) are in danger of failing, or if an additional hard drive is installed that is not a malware storage pack. This module generates an Alert (red) health alert when an installed malware storage pack cannot be detected. | | Disk Usage | Any | This module compares disk usage on the appliance’s hard drive and malware storage pack to the limits configured for the module and alerts when usage exceeds the percentages configured for the module. This module also alerts when the system excessively deletes files in monitored disk usage categories, or when disk usage excluding those categories reaches excessive levels, based on module thresholds. Use the Disk Usage health status module to monitor disk usage for the /and /volume partitions on the appliance and track draining frequency. Although the disk usage module lists the /boot partition as a monitored partition, the size of the partition is static so the module does not alert on the boot partition. | | FireSIGHT Host Limit | Management Center | This module determines if the number of hosts the Firepower Management Center can monitor is approaching the limit and alerts based on the warning level configured for the module. For more information, see [Firepower System Host Limit](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Introduction_to_Network_Discovery.html#ID-2240-00000246). | | Health Monitor Process | Any | This module monitors the status of the health monitor itself and alerts if the number of minutes since the last health event received by the Firepower Management Center exceeds the Warning or Critical limits. | | Intrusion and File Event Rate | Any managed device | This module compares the number of intrusion events per second to the limits configured for this module and alerts if the limits are exceeded. If the Intrusion and File Event Rate is zero, the intrusion process may be down or the managed device may not be sending events. Select**Analysis** > **Intrusions** > **Events** to check if events are being received from the device.  Typically, the event rate for a network segment averages 20 events per second. For a network segment with this average rate, Events per second (Critical) should be set to 50 and Events per second (Warning) should be set to 30. To determine limits for your system, find the Events/Sec value on the Statistics page for your device (**System** > **Monitoring** > **Statistics**), then calculate the limits using these formulas:   * Events per second (Critical) = Events/Sec \* 2.5 * Events per second (Warning) = Events/Sec \* 1.5   The maximum number of events you can set for either limit is 999, and the Critical limit must be higher than the Warning limit. | | Local Malware Analysis | Any | This module alerts if a device is configured for local malware analysis and fails to download local malware analysis engine signature updates from the AMP cloud. | | Memory Usage | Any | This module compares memory usage on the appliance to the limits configured for the module and alerts when usage exceeds the levels configured for the module.  For appliances with more than 4GB of memory, the preset alert thresholds are based on a formula that accounts for proportions of available memory likely to cause system problems. On >4GB appliances, because the interval between Warning and Critical thresholds may be very narrow, Cisco recommends that you manually set the **Warning Threshold %** value to 50. This will further ensure that you receive memory alerts for your appliance in time to address the issue.  Complex access control policies and rules can command significant resources and negatively affect performance. Some lower-end ASA devices with FirePOWER Services Software may generate intermittent memory usage warnings, as the device’s memory allocation is being used to the fullest extent possible. | | Process Status | Any | This module determines if processes on the appliance exit or terminate outside of the process manager. If a process is deliberately exited outside of the process manager, the module status changes to Warning and the health event message indicates which process exited, until the module runs again and the process has restarted. If a process terminates abnormally or crashes outside of the process manager, the module status changes to Critical and the health event message indicates the terminated process, until the module runs again and the process has restarted. | | Reconfiguring Detection | Any managed device | This module alerts if a device reconfiguration has failed. | | Security Intelligence | Management Center | This module alerts if Security Intelligence is in use and:   * The Firepower Management Center cannot update a feed, or feed data is corrupt or contains no recognizable IP addresses. * A managed device had a problem receiving updated Security Intelligence data from the Firepower Management Center. * A managed device cannot load all of the Security Intelligence data provided to it by the Firepower Management Center due to memory issues; see [Troubleshooting Memory Use](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01011110.html#id_66824). | | Time Series Data Monitor | Management Center | This module tracks the presence of corrupt files in the directory where time series data (such as correlation event counts) are stored and alerts when files are flagged as corrupt and removed. | | Time Synchronization Status | Any | This module tracks the synchronization of a device clock that obtains time using NTP with the clock on the NTP server and alerts if the difference in the clocks is more than ten seconds. | | URL Filtering Monitor | Management Centers | This module tracks communications between the Firepower Management Center and its managed devices, as well as with Cisco Collective Security Intelligence (CSI), where the system obtains threat intelligence for commonly visited URLs. The module alerts if the Firepower Management Center fails to successfully communicate with or retrieve an update from Cisco CSI.  This module also alerts if the Firepower Management Center cannot push URL data to your managed devices. | | User Agent Status Monitor | Management Center | This module alerts when heartbeats are not detected for any User Agents connected to the Firepower Management Center. | | VPN Status | Management Center | This module alerts when one or more VPN tunnels between Firepower System devices are down. | | **Table 1 Health Modules** | | | |

## Health Event Views

The Health Event View page allows you to view health events logged by the health monitor on the Firepower Management Center logs health events. The fully customizable event views allow you to quickly and easily analyze the health status events gathered by the health monitor. You can search event data to easily access other information that may be related to the events you are investigating. If you understand what conditions each health module tests for, you can more effectively configure alerting for health events.

You can perform many of the standard event view functions on the health event view pages.

* [Viewing Health Events](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Health_Monitoring.html#ID-2227-000007cf)
* [Viewing Health Events by Module and Appliance](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Health_Monitoring.html#ID-2227-000007f4)
* [Viewing the Health Events Table](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Health_Monitoring.html#ID-2227-0000081d)
* [Hardware Alert Details for 7000 and 8000 Series Devices](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Health_Monitoring.html#ID-2227-0000085d)
* [The Health Events Table](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Health_Monitoring.html#ID-2227-000008dd)

System Statistics

The following topics describe how to monitor the Firepower System:

* [System Statistics](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Monitoring_the_System.html#concept_406648C061224A5C8C1F06FCB389752B)
* [System Messages](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Monitoring_the_System.html#concept_B2F107B9BAD246BB91A032E472F8FD9D)
* [Managing System Messages](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Monitoring_the_System.html#task_FEB0C1566983423EB3A68D35217C0D57)

The Statistics page in the Firepower System web interface lists the current status of general appliance staistics, including disk usage and system processes, Data Correlator statistics, and intrusion event information.

You view system statistics on the Firepower Management Center

* [System Statistics Availability by Appliance](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Monitoring_the_System.html#reference_2D25F81DDF6346088EAB309419798211)
* [The Host Statistics Section](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Monitoring_the_System.html#ID-2257-0000005c)
* [The Disk Usage Section](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Monitoring_the_System.html#reference_2D5566A5417745E58317A4AD0DE3EA49)
* [The Processes Section](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Monitoring_the_System.html#reference_91757A8256AB48F0939FBDDE79FE1160)
* [The SFDataCorrelator Process Statistics Section](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Monitoring_the_System.html#ID-2257-0000034a)
* [The Intrusion Event Information Section](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Monitoring_the_System.html#ID-2257-00000391)
* [Viewing System Statistics](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Monitoring_the_System.html#ID-2257-00000028)