

Health Monitoring

The following topics describe how to use health monitoring in the Firepower System:

- Requirements and Prerequisites for Health Monitoring, on page 1
- About Health Monitoring, on page 1
- Health Policies, on page 13
- Device Exclusion in Health Monitoring, on page 16
- Health Monitor Alerts, on page 19
- About the Health Monitor, on page 21
- Health Event Views, on page 30
- History for Health Monitoring, on page 34

Requirements and Prerequisites for Health Monitoring

Model support

Any

Supported domains

Any

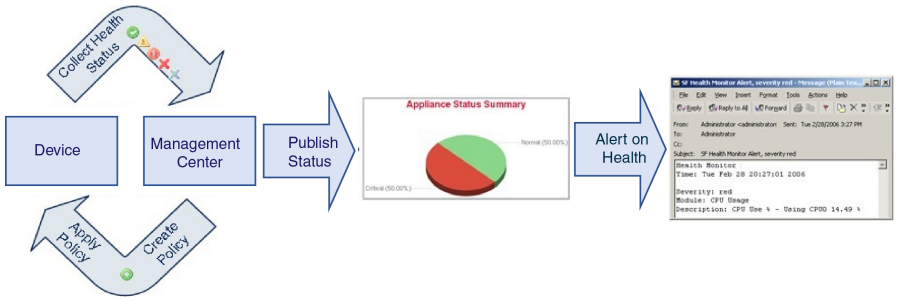
User roles

Admin

Maintenance User

About Health Monitoring

The health monitor on the Firepower Management Center tracks a variety of health indicators to ensure that the hardware and software in the Firepower System are working correctly. You can use the health monitor to check the status of critical functionality across your Firepower System deployment.



You can use the health monitor to create a collection of tests, referred to as a *health policy*, and apply the health policy to one or more appliances. The tests, referred to as *health modules*, are scripts that test for criteria you specify. You can modify a health policy by enabling or disabling tests or by changing test settings, and you can delete health policies that you no longer need. You can also suppress messages from selected appliances by excluding them.

The tests in a health policy run automatically at the interval you configure. You can also run all tests, or a specific test, on demand. The health monitor collects health events based on the test conditions configured.

Note All appliances automatically report their hardware status via the Hardware Alarms health module. The Firepower Management Center also automatically reports status using the modules configured in the default health policy. Some health modules, such as the Appliance Heartbeat module, run on the Firepower Management Center and report the status of the Firepower Management Center's managed devices. Some health modules do not provide managed device status unless you apply a health policy configured with those modules to a device.

You can use the health monitor to access health status information for the entire system, for a particular appliance, or, in a multidomain deployment, a particular domain. Pie charts and status tables on the Health Monitor page provide a visual summary of the status of all appliances on your network, including the Firepower Management Center. Individual appliance health monitors let you drill down into health details for a specific appliance.

Fully customizable event views allow you to quickly and easily analyze the health status events gathered by the health monitor. These event views allow you to search and view event data and to access other information that may be related to the events you are investigating. For example, if you want to see all the occurrences of CPU usage with a certain percentage, you can search for the CPU usage module and enter the percentage value.

You can also configure email, SNMP, or syslog alerting in response to health events. A *health alert* is an association between a standard alert and a health status level. For example, if you need to make sure an appliance never fails due to hardware overload, you can set up an email alert. You can then create a health alert that triggers that email alert whenever CPU, disk, or memory usage reaches the Warning level you configure in the health policy applied to that appliance. You can set alerting thresholds to minimize the number of repeating alerts you receive.

Note The health monitoring can take 5-6 minutes from the occurrence of the health event to generate a health alert.

You can also generate troubleshooting files for an appliance if you are asked to do so by Support.

Because health monitoring is an administrative activity, only users with administrator user role privileges can access system health data.

High Availability Pair

In a high-availability deployment running Version 6.7 or higher, the active creates a health monitor page that uses REST APIs to show detailed metric-based information. The standby creates the health monitor page that shows the alert information and provide a visual summary of the status of all appliances on your network using pie charts and status tables. The standby does not display the metric-based information.

Health Modules

Health modules, or *health tests,* test for the criteria you specify in a health policy.

Table 1: Health Modules

Module	Platforms	Description
Advanced Snort Statistics	FMC	This module monitors Snort statistics related to packet performance, flow counters, and flow events.
AMP Connection Status	FTD	The module alerts if the device cannot connect to the AMP cloud or Cisco AMP Private Cloud after an initial successful connection, or if the private cloud cannot contact the public AMP cloud. Disabled by default.
AMP for Endpoints Status	FMC	The module alerts if the FMC cannot connect to the AMP cloud or Cisco AMP Private Cloud after an initial successful connection, or if the private cloud cannot contact the public 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)	FMC	This module alerts if: • The FMC cannot contact the AMP cloud (public or private) or the Cisco Threat Grid public cloud or on-premises appliance, or the AMP private cloud cannot contact the public AMP cloud. • The encryption keys used for the connection are invalid. • A device cannot contact the Cisco Threat Grid cloud or an Cisco 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 FMC loses connectivity to the Internet, the system may take up to 30 minutes to generate a health alert.
AMP Threat Grid Status	FTD	The module alerts if the device cannot connect to the AMP Threat Grid cloud after an initial successful connection.
Appliance Heartbeat	Any	This module determines if an appliance heartbeat is being heard from the appliance and alerts based on the appliance heartbeat status.

Module	Platforms	Description
ASP Drop	FMC	This module monitors the connections dropped by the data plane accelerated security path.
Backlog Status	FMC	This module alerts if the backlog of event data awaiting transmission from the device to the FMC has grown continuously for more than 30 minutes. To reduce the backlog, evaluate your bandwidth and consider logging fewer events.
Card Reset	Any	This module checks for network cards which have restarted due to hardware failure and alerts when a reset occurs.
Chassis Status Firepower Threat Defense	Firepower 1000 series Firepower 2100 series	This module monitors chassis parameters such as fan speed and chassis temperature, and enables you to set a warning threshold and critical threshold for temperature. The **Critical Chassis Temperature (Celsius)** default value is `85`. The **Warning Chassis Temperature (Celsius)** default value is `75`.
Classic License Monitor	FMC	This module determines if sufficient Classic licenses remain. It alerts based on a warning level automatically configured for the module. You cannot change the configuration of this module.
Cluster/Failover Status	FTD	This module monitors the status of device clusters. The module alerts if: • A new primary unit is elected to a cluster. • A new secondary unit joins a cluster. • A primary or secondary unit leaves a cluster.
Configuration Database	FMC	This module checks the size of the configuration database and alerts when the size exceeds the values (in gigabytes) configured for the module.
Configuration Memory Allocation	Any managed device	This module alerts if the size of your deployed configurations puts a device at risk of running out of memory. The alert shows you how much memory your configurations require, and by how much this exceeds the available memory. If this happens, re-evaluate your configurations. Most often you can reduce the number or complexity of access control rules or intrusion policies. **Snort Memory Allocation** • *Total Snort Memory* indicates the memory allotted for the Snort 2 instances running on the FTD device. • *Available Memory* indicates the memory allotted by the system for a Snort 2 instance. Note that this value is not just the difference between the *Total Snort Memory* and the combined memory reserved for other modules. This value is derived after few other computations and then divided by the number of Snort 2 processes. A negative *Available Memory* value indicates that Snort 2 instance does not have enough memory for the deployed configuration. For support, contact Cisco Technical Assistance Center (TAC).

Module	Platforms	Description
Connection Statistics	FTD	This module monitors the connection statistics and NAT translation counts.
CPU Usage (per core)	FTD	This module checks that the CPU usage on all of the cores is not overloaded and alerts when CPU usage exceeds the percentages configured for the module. The **Warning Threshold %** default value is `80`. The **Critical Threshold %** default value is `90`.
CPU Usage Data Plane	FTD	This module checks that the average CPU usage of all data plane processes on the device is not overloaded and alerts when CPU usage exceeds the percentages configured for the module. The **Warning Threshold %** default value is `80`. The **Critical Threshold %** default value is `90`.
CPU Usage Snort	FTD	This module checks that the average CPU usage of the Snort processes on the device is not overloaded and alerts when CPU usage exceeds the percentages configured for the module. The **Warning Threshold %** default value is `80`. The **Critical Threshold %** default value is `90`.
CPU Usage System	FTD	This module checks that the average CPU usage of all system processes on the device is not overloaded and alerts when CPU usage exceeds the percentages configured for the module. The **Warning Threshold %** default value is `80`. The **Critical Threshold %** default value is `90`.
Critical Process Statistics	FTD	This module monitors the state of critical processes, their resource consumption, and the restart counts.
Deployed Configuration Statistics	FTD	This module monitors statistics about the deployed configuration, such as the number of ACEs and IPS rules.
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.

Module	Platforms	Description
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. See Disk Usage and Drain of Events Health Monitor Alerts for information about troubleshooting scenarios for Disk Usage alerts. 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. **Attention** If you receive alerts for high unmanaged disk usage for the partition `/volume` even though the usage is below the critical or warning threshold specified in the health policy, this could indicate that there are files which need to be deleted manually from the system. Contact TAC if you receive these alerts.
Event Stream Status	FMC	This module monitors connections to third-party client applications that use the Event Streamer on the FMC.
File System Integrity Check	FMC	This module performs a file system integrity check and runs if the system has CC mode or UCAPL mode enabled, or if the system runs an image signed with a DEV key. This module is enabled by default.
Flow Offload	Firepower 4100 series Firepower 9300	This module monitors hardware flow offload statistics for a managed device.
FMC Access Configuration Changes	FMC	This module monitors access configuration changes made on the FMC directly using the **configure network management-data-interface** command.
FMC HA Status	FMC	This module monitors and alerts on the high availability status of the FMC. If you have not established FMC high availability, the HA Status is `Not in HA`. **Note** This module replaces the HA Status module, which previously provided HA status for the FMC. In Version 7.0, we added HA status for managed devices.
Hardware Alarms	FTD hardware	This module determines if hardware needs to be replaced on a physical managed device and alerts based on the hardware status. The module also reports on the status of hardware-related daemons.
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 FMC exceeds the Warning or Critical limits.
Hit Count	FMC	This module tracks the number of times a particular rule is hit on the access control policy. Disabled by default.

Module	Platforms	Description
Host Limit	FMC	This module determines if the number of hosts the FMC 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.
Inline Link Mismatch Alarms	Any managed device except ASA FirePOWER	This module monitors the ports associated with inline sets and alerts if the two interfaces of an inline pair negotiate different speeds.
Interface Status	Any	This module determines if the device currently collects traffic and alerts based on the traffic status of physical interfaces and aggregate interfaces. For physical interfaces, the information includes interface name, link state, and bandwidth. For aggregate interfaces, the information includes interface name, number of active links, and total aggregate bandwidth. **Note** This module also monitors the HA standby device traffic flow. Though it is known that the standby device would not be receiving any traffic, yet, the FMC alerts that the interface is not receiving any traffic. The same alerting principle is applied when traffic is not received by some of the subinterfaces on a port channel. If you use the **show interface** CLI command to know the interface statistics of your device, the input and output rates in the CLI command result can be different from the traffic rates that appear in this interface module. This module displays the traffic rates according to the values from Snort performance monitoring. Sampling intervals of snort performance monitoring and the FTD interface statistics are different. This difference in sampling interval results in different throughput values in the FMC GUI and in the FTD **show interface** CLI command result. For ASA FirePOWER, interfaces labeled DataPlaneInterfacex, where x is a numerical value, are internal interfaces (not user-defined) and involve packet flow within the system.
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.

Module	Platforms	Description
ISE Connection Status Monitor	FMC	This module monitors the status of the server connections between the Cisco Identity Services Engine (ISE) and the FMC. ISE provides additional user data, device type data, device location data, SGTs (Security Group Tags), and SXP (Security Exchange Protocol) services.
Link State Propagation	ASA 5500-X series and ISA 3000 with FTD	This module determines when a link in a paired inline set fails and triggers the link state propagation mode. If a link state propagates to the pair, the status classification for that module changes to Critical and the state reads: `Module Link State Propagation: ethx_ethy is Triggered` where `x` and `y` are the paired interface numbers.
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 4 GB of memory, the preset alert thresholds are based on a formula that accounts for proportions of available memory likely to cause system problems. On >4 GB 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. See Memory Usage Thresholds for Health Monitor Alerts for additional information about how thresholds are calculated. Beginning with Version 6.6.0, the minimum required RAM for FMCv upgrades to Version 6.6.0+ is 28 GB, and the recommended RAM for FMCv deployments is 32 GB. We recommend you do not decrease the default settings: 32 GB RAM for most FMCv instances, 64 GB for the FMCv 300 (VMware only). **Attention** A critical alert is generated by the health monitor when insufficient RAM is allocated to an FMCv deployment. 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.
Memory Usage Data Plane	FTD	This module checks the percentage of allocated memory used by the Data Plane processes and alerts when memory usage exceeds the percentages configured for the module. The **Warning Threshold %** default value is `80`. The **Critical Threshold %** default value is `90`.
Memory Usage Snort	FTD	This module checks the percentage of allocated memory used by the Snort process and alerts when memory usage exceeds the percentages configured for the module. The **Warning Threshold %** default value is `80`. The **Critical Threshold %** default value is `90`.

Module	Platforms	Description
MySQL Status	FMC	This module monitors the status of the MySQL database, including the database size, number of active connections, and memory use. Disabled by default.
NTP Status FTD	FTD	This module monitors the NTP clock synchronisation status of the managed device. Disabled by default.
Platform Faults	Firepower 1000 series Firepower 2100 series	On Firepower 2100 and Firepower 1000 series devices, a fault is a mutable object that is managed by the FMC. Each fault represents a failure in the device instance or an alarm threshold that has been raised. During the lifecycle of a fault, it can change from one state or severity to another. Each fault includes information about the operational state of the affected object at the time the fault was raised. If the fault is transitional and the failure is resolved, then the object transitions to a functional state. For more information, see the *Cisco Firepower 1000/2100 FXOS Faults and Error Messages Guide*.
Power Supply	FMC hardware	This module determines if power supplies on the device require replacement and alerts based on the power supply status.
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.
RabbitMQ Status	FMC	This module monitors the status of the RabbitMQ.
Realm	Any managed device	Enables you to set a warning threshold for realm or user mismatches, which are: • User mismatch: A user is reported to the Firepower Management Center without being downloaded. A typical reason for a user mismatch is that the user belongs to a group you have excluded from being downloaded to the Firepower Management Center. Review the information discussed in Realm Fields. • Realm mismatch: A user logs into a domain that corresponds to a realm not known to the Firepower Management Center. For more information, see Detect Realm or User Mismatches.
Reconfiguring Detection	Any managed device	This module alerts if a device reconfiguration has failed.
Routing Statistics	FMC	This module monitors the current state of routing table.

Module	Platforms	Description
RRD Server Process	FMC	This module determines if the round robin data server that stores time series data is running properly. The module will alert If the RRD server has restarted since the last time it updated; it will enter Critical or Warning status if the number of consecutive updates with an RRD server restart reaches the numbers specified in the module configuration.
Security Intelligence	FMC	This module alerts if Security Intelligence is in use and the FMC cannot update a feed, or feed data is corrupt or contains no recognizable IP addresses. See also the Threat Data Updates on Devices module
Smart License Monitor	FMC	This module alerts if: • There is a communication error between the Smart Licensing Agent (Smart Agent) and the Smart Software Manager. • The Product Instance Registration Token has expired. • The Smart License usage is out of compliance. • The Smart License authorization or evaluation mode has expired.
Snort Identity Memory Usage	FTD	Enables you to set a warning threshold for Snort identity processing and alerts when memory usage exceeds the level configured for the module. The **Critical Threshold %** default value is `80`. This health module specifically keeps track of the total space used for the user identity information in Snort. It displays the current memory usage details, the total number of user-to-IP bindings, and user-group mapping details. Snort records these details in a file. If the memory usage file is not available, the Health Alert for this module displays *Waiting for data*. This could happen during a Snort restart due to a new install or a major update, switch from Snort2 to Snort3 or back, or major policy deployment. Depending on the health monitoring cycle, and when the file is available, the warning disappears, and the health monitor displays the details for this module with its status turned Green.
Snort Statistics	FTD	This module monitors the Snort statistics for events, flows, and packets.
SSE Connection Status	Any managed device	The module alerts if the device cannot connect to the SSE cloud after an initial successful connection. Disabled by default.
Sybase Status	FMC	This module monitors the status of the Sybase database on the FMC, including the database size, number of active connections, and memory use.

Module	Platforms	Description
Threat Data Updates on Devices	Any	Certain intelligence data and configurations that devices use to detect threats are updated on the FMC from the cloud every 30 minutes. This module alerts you if this information has not been updated on the devices within the time period you have specified. Monitored updates include: • Local URL category and reputation data • Security Intelligence URL lists and feeds, including global Block and Do Not Block lists and URLs from Threat Intelligence Director • Security Intelligence network lists and feeds (IP addresses), including global Block and Do Not Block lists and IP addresses from Threat Intelligence Director • Security Intelligence DNS lists and feeds, including global Block and Do Not Block lists and domains from Threat Intelligence Director • Local malware analysis signatures (from ClamAV) • SHA lists from Threat Intelligence Director, as listed on the **Objects > Object Management > Security Intelligence > Network Lists and Feeds** page • Dynamic analysis settings configured on the **AMP > Dynamic Analysis Connections** page • Threat Configuration settings related to expiration of cached URLs, including the Cached URLs Expire setting on the **System > Integration > Cloud Services** page. (Updates to the URL cache are not monitored by this module.) • Communication issues with the Cisco cloud for sending events. See the **Cisco Cloud** box on the **System > Integration > Cloud Services** page. **Note** Threat Intelligence Director updates are included only if TID is configured on your system and you have feeds. By default, this module sends a warning after 1 hour and a critical alert after 24 hours. If this module indicates failure on the FMC or on any devices, verify that the FMC can reach the devices. For low-memory devices that show failure of the URL category and reputation data type, see Troubleshooting Memory Use.
Firepower Threat Defense HA Status	FTD	This module monitors and alerts on the high availability status of the device and provides a health alert for a split brain scenario. If you have not established high availability, the HA Status is `Not in HA`.

Module	Platforms	Description
Time Series Data Monitor	FMC	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.
Unresolved Groups Monitor	FMC	Monitors unresolved groups used in policies.
URL Filtering Monitor	FMC	This module alerts if the FMC fails to: • Register with the Cisco cloud. • Download URL threat data updates from the Cisco cloud. • Complete URL lookups. You can configure time thresholds for these alerts. See also the Threat Data Updates on Devices module.
VPN Statistics	FMC	This module monitors Site to Site and RA VPN tunnels between Firepower devices.
VPN Status	FMC	This module alerts when one or more VPN tunnels between Firepower devices are down. This module tracks: • Site-to-site VPN for FTD **Attention** Site-to-site VPN tunnels created with Virtual Tunnel Interfaces (VTIs) do not generate health alerts when the tunnel goes down. If you experience packet loss over a VPN with VTIs, check your VPN configuration. • Remote access VPN for FTD
xTLS Counters	Any	This module monitors xTLS/SSL flows, memory and cache effectiveness. Disabled by default.

Configuring Health Monitoring

Procedure

Step 1 Determine which health modules you want to monitor as discussed in Health Modules, on page 3.

You can set up specific policies for each kind of appliance you have in your Firepower System, enabling only the appropriate tests for that appliance.

Tip
To quickly enable health monitoring without customizing the monitoring behavior, you can apply the default policy provided for that purpose.

Step 2 Apply a health policy to each appliance where you want to track health status as discussed in Creating Health Policies, on page 14.

Step 3 (Optional.) Configure health monitor alerts as discussed in Creating Health Monitor Alerts, on page 19.

You can set up email, syslog, or SNMP alerts that trigger when the health status level reaches a particular severity level for specific health modules.

Health Policies

A health policy contains configured health test criteria for several modules. You can control which health modules run against each of your appliances and configure the specific limits used in the tests run by each module.

When you configure a health policy, you decide whether to enable each health module for that policy. You also select the criteria that control which health status each enabled module reports each time it assesses the health of a process.

You can create one health policy that can be applied to every appliance in your system, customize each health policy to the specific appliance where you plan to apply it, or use the default health policy provided for you. In a multidomain deployment, administrators in ancestor domains can apply health policies to devices in descendant domains, which descendant domains can use or replace with customized local policies.

Default Health Policy

The Firepower Management Center setup process creates and applies an initial health policy, in which most—but not all—available health modules are enabled. The system also applies this initial policy to devices added to the Firepower Management Center.

This *initial* health policy is based on a *default* health policy, which you can neither view nor edit, but which you can copy when you create a custom health policy.

Upgrades and the Default Health Policy

When you upgrade the FMC, any new health modules are added to all health policies, including the initial health policy, default health policy, and any other custom health policies. Usually, new health modules are added in an enabled state.

Note For a new health module to begin monitoring and alerting, reapply health policies after upgrade.

Creating Health Policies

If you want to customize a health policy to use with your appliances, you can create a new policy. The settings in the policy initially populate with the settings from the health policy you choose as a basis for the new policy. You can enable or disable modules within the policy and change the alerting criteria for each module as needed.

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain. Administrators in ancestor domains can apply health policies to devices in descendant domains, which descendant domains can use or replace with customized local policies.

Procedure

Step 1 Choose **System** > **Health** > **Policy** .

Step 2 Click **New Policy**.

Step 3 Choose the existing policy that you want to use as the basis for the new policy from the **Copy Policy** drop-down list**.**

Step 4 Enter a name for the policy.

Step 5 Enter a description for the policy.

Step 6 Choose **Save** to save the policy information.

Step 7 Choose the module you want to use.

Step 8 Choose **On** for the **Enabled** option to enable use of the module for health status testing.

Step 9 Where appropriate, set the **Critical** and **Warning** criteria.

Step 10 Configure any additional settings for the module. Repeat steps 7-10 for each module.

Step 11 You have three choices:

- To save your changes to this module and return to the Health Policy page, click **Save Policy and Exit**.
- To return to the Health Policy page without saving any of your settings for this module, click **Cancel**.
- To temporarily save your changes to this module and switch to another module's settings to modify, choose the other module from the list at the left of the page. If you click **Save Policy and Exit** when you are done, all changes you made will be saved; if you click **Cancel**, you discard all changes.

What to do next

- Apply the health policy to each appliance as described in Applying Health Policies, on page 14. This applies your changes and updates the policy status for all affected policies.

Applying Health Policies

When you apply a health policy to an appliance, the health tests for all the modules you enabled in the policy automatically monitor the health of the processes and hardware on the appliance. Health tests then continue to run at the intervals you configured in the policy, collecting health data for the appliance and forwarding that data to the Firepower Management Center.

If you enable a module in a health policy and then apply the policy to an appliance that does not require that health test, the health monitor reports the status for that health module as disabled.

If you apply a policy with all modules disabled to an appliance, it removes all applied health policies from the appliance so no health policy is applied.

When you apply a different policy to an appliance that already has a policy applied, expect some latency in the display of new data based on the newly applied tests.

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain. Administrators in ancestor domains can apply health policies to devices in descendant domains, which descendant domains can use or replace with customized local policies.

Procedure

Step 1 Choose **System** > **Health** > **Policy** .

Step 2 Click the **Apply** ( ) next to the policy you want to apply.

Tip

The **Status** ( ) next to the Health Policy column indicates the current health status for the appliance.

Step 3 Choose the appliances where you want to apply the health policy.

Step 4 Click **Apply** to apply the policy to the appliances you chose.

What to do next

- Optionally, monitor the task status; see Viewing Task Messages.

  Monitoring of the appliance starts as soon as the policy is successfully applied.

Editing Health Policies

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain. Administrators in ancestor domains can apply health policies to devices in descendant domains, which descendant domains can use or replace with customized local policies.

Procedure

Step 1 Choose **System** > **Health** > **Policy** .

Step 2 Click **Edit** ( ) next to the policy you want to modify.

Step 3 Edit the **Policy Name** or **Policy Description** fields as desired.

Step 4 Click the health module you want to modify.

Step 5 Modify settings as described in Health Modules, on page 3.

Step 6 You have three options:

- To save your changes to this module and return to the Health Policy page, click **Save Policy and Exit**.
- To return to the Health Policy page without saving any of your settings for this module, click **Cancel**.
- To temporarily save your changes to this module and switch to another module's settings to modify, choose the other module from the list at the left of the page. If you click **Save Policy and Exit** when you are done, all changes you made will be saved; if you click **Cancel**, you discard all changes.

Step 7 Apply the health policy to your appliance as described in Applying Health Policies, on page 14.

Apply the health policy to each appliance where you want to track health status. When you apply the health policy to an appliance, all the modules you enabled in the policy monitor the health of the processes and hardware on the appliance, and forwards that data to the FMC.

What to do next

- Reapply the health policy as described in Applying Health Policies, on page 14. This applies your changes and updates the policy status for all affected policies.

Deleting Health Policies

You can delete health policies that you no longer need. If you delete a policy that is still applied to an appliance, the policy settings remain in effect until you apply a different policy. In addition, if you delete a health policy that is applied to a device, any health monitoring alerts in effect for the device remain active until you disable the underlying associated alert response.

In a multidomain deployment, you can only delete health policies created in the current domain.

Tip To stop health monitoring for an appliance, create a health policy with all modules disabled and apply it to the appliance.

Procedure

Step 1 Choose **System** > **Health** > **Policy** .

Step 2 Click **Delete** ( ) next to the policy you want to delete.
A message appears, indicating if the deletion was successful.

Device Exclusion in Health Monitoring

In the course of normal network maintenance, you disable appliances or make them temporarily unavailable. Because those outages are deliberate, you do not want the health status from those appliances to affect the summary health status on your Firepower Management Center.

You can use the health monitor excludefeature to disable health monitoring status reporting on an appliance or module. For example, if you know that a segment of your network will be unavailable, you can temporarily disable health monitoring for a managed device on that segment to prevent the health status on the Firepower Management Center from displaying a warning or critical state because of the lapsed connection to the device.

When you disable health monitoring status, health events are still generated, but they have a disabled status and do not affect the health status for the health monitor. If you remove the appliance or module from the excluded list, the events that were generated during the exclusion continue to show a status of disabled.

To temporarily disable health events from an appliance, go to the exclusion configuration page and add an appliance to the exclude list. After the setting takes effect, the system no longer includes the excluded appliance when calculating the overall health status. The Health Monitor Appliance Status Summary lists the appliance as disabled.

You can also disable an individual health module. For example, when you reach the host limit on a Firepower Management Center, you can disable Host Limit status messages.

Note that on the main Health Monitor page you can distinguish between appliances that are excluded if you expand to view the list of appliances with a particular status by clicking the arrow in that status row.

An **Exclude** ( ) icon and a notation are visible after you expand the view for a excluded or partially excluded appliance.

Note On a Firepower Management Center, Health Monitor exclusion settings are local configuration settings. Therefore, if you exclude a device, then delete it and later re-register it with the Firepower Management Center, the exclusion settings remain persistent. The newly re-registered device remains excluded.

In a multidomain deployment, administrators in ancestor domains can exclude an appliance or health module in descendant domains. However, administrators in the descendant domains can override the ancestor configuration and clear the exclusion for devices in their domain.

Excluding Appliances

You can exclude appliances individually or by group, model, or associated health policy.

If you need to set the events and health status for an individual appliance to disabled, you can exclude the appliance. After the exclusion settings take effect, the appliance shows as disabled in the Health Monitor Appliance Module Summary, and health events for the appliance have a status of disabled.

In a multidomain deployment, excluding an appliance in an ancestor domain excludes it for all descendant domains. Descendant domains can override this inherited configuration and clear the exclusion. You can only exclude the Firepower Management Center at the Global level.

Procedure

Step 1 Choose **System** > **Health** > **Exclude**.

Step 2 Use the drop-down list on the right to sort the list by group, model, or by health policy.

Tip

The status icon next to the Health Policy column **Status** ( ) indicates the current health status for the appliance. The status icon next to the System Policy column **Status** ( ) indicates the communication status between the Firepower Management Center and the device.

Step 3 You have two choices:

- To exclude all appliances in a group, model, or policy category, check the check box for the category, then click **Exclude Selected Devices**.
- To clear excluding from all appliances in a group, model, or policy category, check the check box for the category, then click **Clear Exclude on Selected Devices**.

What to do next

To exclude individual health policy module on appliances, see Excluding Health Policy Modules, on page 18.

Excluding Health Policy Modules

You can exclude individual health policy modules on appliances. You may want to do this to prevent events from the module from changing the status for the appliance to warning or critical.

After the exclusion settings take effect, the appliance shows as **Partially Excluded** or **All Modules Excluded** on the Exclude page and in the Appliance Health Monitor Module Status Summary, but only in expanded views on the main Appliance Status Summary page.

Tip Make sure that you keep track of individually excluded modules so you can reactivate them when you need them. You may miss necessary warning or critical messages if you accidentally leave a module disabled.

In a multidomain deployment, administrators in ancestor domains can exclude health modules in descendant domains. However, administrators in descendant domains can override this ancestor configuration and clear the excluding for policies applied in their domains. You can only exclude Firepower Management Center health modules at the Global level.

Procedure

Step 1 Choose **System** > **Health** > **Exclude**.

Step 2 Click **Edit** ( ) next to the appliance you want to modify.

Step 3 Check the check boxes next to the health policy modules you want to exclude. Certain modules are applicable to specific devices only; for more information, see Health Modules, on page 3.

Step 4 Click **OK**.

Step 5 In the device exclusion main page, click **Apply**.

Health Monitor Alerts

You can set up alerts to notify you through email, through SNMP, or through the system log when the status changes for the modules in a health policy. You can associate an existing alert response with health event levels to trigger and alert when health events of a particular level occur.

For example, if you are concerned that your appliances may run out of hard disk space, you can automatically send an email to a system administrator when the remaining disk space reaches the warning level. If the hard drive continues to fill, you can send a second email when the hard drive reaches the critical level.

In a multidomain deployment, you can view and modify health monitor alerts created in the current domain only.

Health Monitor Alert Information

The alerts generated by the health monitor contain the following information:

- Severity, which indicates the severity level of the alert.
- Module, which specifies the health module whose test results triggered the alert.
- Description, which includes the health test results that triggered the alert.

The table below describes these severity levels.

Table 2: Alert Severities

Severity	Description
Critical	The health test results met the criteria to trigger a Critical alert status.
Warning	The health test results met the criteria to trigger a Warning alert status.
Normal	The health test results met the criteria to trigger a Normal alert status.
Error	The health test did not run.
Recovered	The health test results met the criteria to return to a normal alert status, following a Critical or Warning alert status.

Creating Health Monitor Alerts

You must be an Admin user to perform this procedure.

When you create a health monitor alert, you create an association between a severity level, a health module, and an alert response. You can use an existing alert or configure a new one specifically to report on system health. When the severity level occurs for the selected module, the alert triggers.

If you create or update a threshold in a way that duplicates an existing threshold, you are notified of the conflict. When duplicate thresholds exist, the health monitor uses the threshold that generates the fewest alerts and ignores the others. The timeout value for the threshold must be between 5 and 4,294,967,295 minutes.

In a multidomain deployment, you can view and modify health monitor alerts created in the current domain only.

Before you begin

- Configure an alert response that governs the Firepower Management Center's communication with the SNMP, syslog, or email server where you send the health alert; see Firepower Management Center Alert Responses.

Procedure

Step 1 Choose **System** > **Health** > **Monitor Alerts**.

Step 2 Enter a name for the health alert in the **Health Alert Name** field.

Step 3 From the **Severity** list, choose the severity level you want to use to trigger the alert.

Step 4 From the **Module** list, choose the health policy modules for which you want the alert to apply.

Step 5 From the **Alert** list, choose the alert response that you want to trigger when the specified severity level is reached.

Step 6 Optionally, in the **Threshold Timeout** field, enter the number of minutes that should elapse before each threshold period ends and the threshold count resets.

Even if the policy run time interval value is less than the threshold timeout value, the interval between two reported health events from a given module is always greater. For example, if you change the threshold timeout to 8 minutes and the policy run time interval is 5 minutes, there is a 10-minute interval (5 x 2) between reported events.

Step 7 Click **Save** to save the health alert.

Editing Health Monitor Alerts

You must be an Admin user to perform this procedure.

You can edit existing health monitor alerts to change the severity level, health module, or alert response associated with the health monitor alert.

In a multidomain deployment, you can view and modify health monitor alerts created in the current domain only.

Procedure

Step 1 Choose **System** > **Health** > **Monitor Alerts**.

Step 2 Choose the alert you want to modify from the **Active Health Alerts** list.

Step 3 Click **Load** to load the configured settings for the alert you chose.

Step 4 Modify settings as needed.

Step 5 Click **Save** to save the modified health alert.

A message indicates if the alert configuration was successfully saved.

Deleting Health Monitor Alerts

In a multidomain deployment, you can view and modify health monitor alerts created in the current domain only.

Procedure

Step 1 Choose **System** > **Health** > **Monitor Alerts**.

Step 2 Choose the active health alerts you want to delete, then click **Delete**.

What to do next

- Disable or delete the underlying alert response to ensure that alerting does not continue; see Firepower Management Center Alert Responses.

About the Health Monitor

You must be an Admin, Maintenance, or Security Analyst user to perform this procedure.

The health monitor provides the compiled health status for all devices managed by the Firepower Management Center, plus the Firepower Management Center itself. The health monitor is composed of:

- The Health Status summary page — Provides you with an at-a-glance view of the health of the Firepower Management Center and all of the devices that the FMC manages. Devices are listed individually, or grouped according to their geolocation, high availability, or cluster status where applicable.
  - View the health summary of the FMC and any device when you hover on the hexagon that represents the device health.
  - The dot to the left of a device indicates its health:
    - Green — No alarms.
    - Orange — At least one health warning.
    - Red — At least one critical health alarm.
- The Monitoring navigation pane — Allows you to navigate the device hierarchy. You can view health monitors for individual devices from the navigation pane.

In a multidomain deployment, the health monitor in an ancestor domain displays data from all descendant domains. In the descendant domains, it displays data from the current domain only.

Procedure

Step 1 Choose **System** > **Health** > **Monitor**.

Step 2 View the status of the FMC and its managed devices in the **Health Status** landing page.

a) Hover your pointer over a hexagon to view the health summary of a device. The popup window shows a truncated summary of the top five health alerts. Click on the popup to open a detailed view of the health alert summary.

b) In the device list, click **Expand** ( ) and **Collapse** ( ) to expand and collapse the list of health alerts for a device.

When you expand the row, all of the health alerts are listed, including the status, title, and details.

Note
Health alerts are sorted by their severity level.

Step 3 Use the Monitoring navigation pane to access device-specific health monitors. When you use the Monitoring navigation pane:

a) In the device list, click **Expand** ( ) and **Collapse** ( ) to expand and collapse the list of managed devices.

When you expand the row, all of the devices are listed.

b) Click on a device to view a device-specific health monitor.

What to do next

- See Device Health Monitors, on page 25 for information about the compiled health status and metrics for any device managed by the Firepower Management Center.
- See Using the FMC Health Monitor, on page 22 for information about the health status of the Firepower Management Center.

To return to the Health Status landing page at any time, click **Home**.

Using the FMC Health Monitor

You must be an Admin, Maintenance, or Security Analyst user to perform this procedure.

The FMC monitor provides a detailed view of the health status of the Firepower Management Center. The health monitor is composed of:

- High Availability (if configured) — The High Availability (HA) panel displays the current HA status, including the status of the Active and Standby units, the last sync time, and overall device health.
- Event Rate — The Event Rate panel shows the maximum event rate as a base line as well as the overall event rate received by the FMC.

- Event Capacity — The Event Capacity panel shows the current consumption by event categories, including the retention time of events, the current vs. maximum event capacity, and a capacity overflow mechanism where you are alerted when events are stored beyond the configured maximum capacity of the FMC.
- Process Health — The Process Health panel has an at-a-glace view of the critical processes as well as a tab that lets you see state of all processed, including the CPU and memory usage for each process.
- CPU — The CPU panel lets you toggle between the average CPU usage (default) and the CPU usage of all cores.
- Memory — The Memory panel shows the overall memory usage on the FMC.
- Interface — The Interface panel shows avaerage input and output rate of all interfaces.
- Disk Usage — The Disk Usage panel shows the use of entire disk, and the use of the critical partitions where FMC data is stored.

Tip Your session normally logs you out after 1 hour of inactivity (or another configured interval). If you plan to passively monitor health status for long periods of time, consider exempting some users from session timeout, or changing the system timeout settings. See Add an Internal User and Configure Session Timeouts for more information.

Procedure

Step 1 Choose **System** > **Health** > **Monitor**.

Step 2 Use the **Monitoring** navigation pane to access the FMC and device-specific health monitors.

- A standalone FMC is shown as a single node; a high-availability FMC is shown as a pair of nodes.
- The health monitor is available to both the active and standby FMC in an HA pair.

Step 3 Explore the FMC dashboard.

The FMC dashboard includes a summary view of the HA state of the FMC (if configured), as well as at-a-glance views of FMC processes and device metrics such as CPU, memory, and disk usage.

Running All Modules for an Appliance

You must be an Admin, Maintenance, or Security Analyst user to perform this procedure.

Health module tests run automatically at the policy run time interval you configure when you create a health policy. However, you can also run all health module tests on demand to collect up-to-date health information for the appliance.

In a multidomain deployment, you can run health module tests for appliances in the current domain and in any descendant domains.

Procedure

Step 1 View the health monitor for the appliance.

Step 2 Click **Run All Modules**. The status bar indicates the progress of the tests, then the Health Monitor Appliance page refreshes.

Note
When you manually run health modules, the first refresh that automatically occurs may not reflect the data from the manually run tests. If the value has not changed for a module that you just ran manually, wait a few seconds, then refresh the page by clicking the device name. You can also wait for the page to refresh again automatically.

Running a Specific Health Module

You must be an Admin, Maintenance, or Security Analyst user to perform this procedure.

Health module tests run automatically at the policy run time interval you configure when you create a health policy. However, you can also run a health module test on demand to collect up-to-date health information for that module.

In a multidomain deployment, you can run health module tests for appliances in the current domain and in any descendant domains.

Procedure

Step 1 View the health monitor for the appliance.

Step 2 In the **Module Status Summary** graph, click the color for the health alert status category you want to view.

Step 3 In the **Alert Detail** row for the alert for which you want to view a list of events, click **Run**.

The status bar indicates the progress of the test, then the Health Monitor Appliance page refreshes.

Note
When you manually run health modules, the first refresh that automatically occurs may not reflect the data from the manually run tests. If the value has not changed for a module that you just manually ran, wait a few seconds, then refresh the page by clicking the device name. You can also wait for the page to refresh automatically again.

Generating Health Module Alert Graphs

You must be an Admin, Maintenance, or Security Analyst user to perform this procedure.

You can graph the results over a period of time of a particular health test for a specific appliance.

Procedure

Step 1 View the health monitor for the appliance.

Step 2 In the **Module Status Summary** graph of the Health Monitor Appliance page, click the color for the health alert status category you want to view.

Step 3 In the **Alert Detail** row for the alert for which you want to view a list of events, click **Graph**.

Tip
If no events appear, you may need to adjust the time range.

Device Health Monitors

The device health monitor provides the compiled health status for any device managed by the Firepower Management Center. The device health monitor collects health metrics for Firepower devices in order to predict and repond to system events. The device health monitor is comprised of the following components:

- System Details — Displays information about the managed device, including the installed Firepower version and other deployment details.
- Troubleshooting & Links — Provides convenient links to frequently used troubleshooting topics and procedures.
- Health alerts — A health alert monitor provides an at-a-glance view of the health of the device.
- Time range — An adjustable time window to constrain the information that appears in the various device metrics windows.
- Device metrics — An array of key Firepower device health metrics catagorized across predefined dashboards, including:
  - CPU — CPU utilization, including the CPU usage by process and by physical cores.
  - Memory — Device memory utilization, including data plane and Snort memory usage.
  - Interfaces — Interface status and aggregate traffic statistics.
  - Connections — Connection statistics and NAT translation counts.
  - Snort — Statistics related to the Snort process.
  - Disk Usage — Device disk usage, including the disk size and disk utilization per partition.
  - Critical Processes — Statistics related to managed processes, including process restarts and other select health monitors such as CPU and memory utilization.

Viewing System Details and Troubleshooting

You must be an Admin, Maintenance, or Security Analyst user to perform this procedure.

The System Details section provides a general system information for a selected device. You can also launch troubleshooting tasks for that device.

Procedure

Step 1 Choose **System** > **Health** > **Monitor**.

Use the Monitoring navigation pane to access device-specific health monitors.

Step 2 In the device list, click **Expand** ( ) and **Collapse** ( ) to expand and collapse the list of managed devices.

Step 3 Click on a device to view a device-specific health monitor.

Step 4 Click the link for **View System & Troubleshoot Details …**

This panel is collapsed by default. Clicking on the link expands the collapsed section to see **System Details** and **Troubleshooting & Links** for the device. The system details include:

- **Version:** The Firepower software version.
- **Model:** The device model.
- **Mode:** The firewall mode. The Firepower Threat Defense device supports two firewall modes for regular firewall interfaces: Routed mode and Transparent mode.
- **VDB:** The Cisco vulnerability database (VDB) version.
- **SRU:** The intrusion rule set version.
- **Snort:** The Snort version.

Step 5 You have the following troubleshoot choices:

- Generate troubleshooting files; see Producing Troubleshooting Files for Specific System Functions
- Generate and download advanced troubleshooting files; see Downloading Advanced Troubleshooting Files.
- Create and modify health policies; see Creating Health Policies, on page 14.
- Create and modify health monitor alerts; see Creating Health Monitor Alerts, on page 19.

Viewing the Device Health Monitor

You must be an Admin, Maintenance, or Security Analyst user to perform this procedure.

The device health monitor provides a detailed view of the health status of a Firepower device. The device health monitor compiles device metrics and provides health status and trends of the device in an array of dashboards.

Procedure

Step 1 Choose **System** > **Health** > **Monitor**.

Use the Monitoring navigation pane to access device-specific health monitors.

Step 2 In the device list, click **Expand** ( ) and **Collapse** ( ) to expand and collapse the list of managed devices.

Step 3 View the **Health Alerts** for the device in the alert notification at the top of page, directly to the right of the device name.

Hover your pointer over the **Health Alerts** to view the health summary of the device. The popup window shows a truncated summary of the top five health alerts. Click on the popup to open a detailed view of the health alert summary.

Step 4 You can configure the time range from the drop-down in the upper-right corner. The time range can reflect a period as short as the last hour (the default) or as long as two weeks. Select **Custom** from the drop-down to configure a custom start and end date.

Click the refresh icon to set auto refresh to 5 minutes or to toggle off auto refresh.

Step 5 Click on deployment icon for a deployment overlay on the trend graph, with respect to the selected time range.

The deployment icon indicates the number of deployments during the selected time-range. A vertical band indicates the deployment start and end time. In the case of multiple deployments, multiple bands/lines will appear. Click on the icon on top of the dotted line to view the deployment details.

Step 6 The device monitor reports health and performance metrics in several predefined dashboards by default. The metrics dashboards include:

- Overview — Highlights key metrics from the other predefined dashboards, including CPU, memory, interfaces, connection statistics; plus disk usage and critical process information.
- CPU — CPU utilization, including the CPU usage by process and by physical cores.
- Memory — Device memory utilization, including data plane and Snort memory usage.
- Interfaces — Interface status and aggregate traffic statistics.
- Connections — Connection statistics and NAT translation counts.
- Snort — Statistics related to the Snort process.

You can navigate through the various metrics dashboards by clicking on the labels. See Cisco Secure Firewall Threat Defense Health Metrics for a comprehensive list of the supported device metrics.

Step 7 Click the plus sign (+) in the upper right corner of the device monitor to create a custom correlation dashboard by building your own variable set from the available metric groups; see Correlating Device Metrics, on page 27.

Correlating Device Metrics

You must be an Admin, Maintenance, or Security Analyst user to perform this procedure.

The device health monitor includes an array of key Firepower device metrics that serve to predict and respond to system events. The health of any Firepower device can be determined by these reported metrics.

The device monitor reports these metrics in several predefined dashboards by default. These dashboards include:

- Overview — Highlights key metrics from the other predefined dashboards, including CPU, memory, interfaces, connection statistics; plus disk usage and critical process information.
- CPU — CPU utilization, including the CPU usage by process and by physical cores.
- Memory — Device memory utilization, including data plane and Snort memory usage.
- Interfaces — Interface status and aggregate traffic statistics.
- Connections — Connection statistics and NAT translation counts.
- Snort — Statistics related to the Snort process.
- ASP Drops — Statistics related to the Accelerated Security Path (ASP) performance and behavior.

You can add custom dashboards to correlate metrics that are interrelated. Select from predefined correlation groups, such as CPU and Snort; or create a custom correlation dashboard by building your own variable set from the available metric groups. See Cisco Secure Firewall Threat Defense Health Metrics for a comprehensive list of the supported device metrics.

Before you begin

To view and correlate the time series data (device metrics) in the health monitor dashboard, enable REST API (**Settings** > **Configuration** > **REST API Preferences**).

Note Correlating device metrics is available only for FTD 6.7 and later versions. Hence, for FTD versions earlier than 6.7, the health monitor dashboard does not display these metrics even if you enable REST API.

Procedure

Step 1 Choose **System** > **Health** > **Monitor**.

Use the Monitoring navigation pane to access device-specific health monitors.

Step 2 In the device list, click **Expand** ( ) and **Collapse** ( ) to expand and collapse the list of managed devices.

Step 3 Click the plus sign (+) in the upper right corner of the device monitor to add a new dashboard.

Step 4 From the **Select Correlation Group** drop-down, choose a predefined correlation group or or create a custom group.

Step 5 To create a dashboard from a predefined correlation group, select the group and click **Add**.

- CPU - Data Plane
- CPU - Snort
- CPU - Others
- Memory - Data Plane
- Packet drops

Step 6 To create a custom correlation dashboard:

a) Choose **Custom**.

b) Optionally, enter a unique name in the **Dashboard Name** field or accept the default.

c) Next, select a group from the **Select Metric Group** drop-down, then select corresponding metrics from the **Select Metrics** drop-down.

See Cisco Secure Firewall Threat Defense Health Metrics for a comprehensive list of the supported device metrics.

Step 7 Click **Add Metrics** to add and select metrics from another group.

Step 8 To remove an individual metric, click the **x** on the right side of the item. Click the delete icon (a trash can) to remove the entire group.

Step 9 Click **Add** to complete the workflow and add the dashboard to the health monitor.

Step 10 You can **Edit** or **Delete** custom correlation dashboards.

Health Monitor Status Categories

Available status categories are listed by severity in the table below.

Table 3: Health Status Indicator

Status Level	Status Icon	Status Color in Pie Chart	Description
Error	**Error** ( )	Black	Indicates that at least one health monitoring module has failed on the appliance and has not been successfully re-run since the failure occurred. Contact your technical support representative to obtain an update to the health monitoring module.
Critical	**Critical** ( )	Red	Indicates that the critical limits have been exceeded for at least one health module on the appliance and the problem has not been corrected.
Warning	**Warning** ( )	Yellow	Indicates that warning limits have been exceeded for at least one health module on the appliance and the problem has not been corrected. This status also indicates a transitionary state, where the required data is temporarily unavailable or could not be processed because of changes in the device configuration. Depending on the monitoring cycle, this transitionary state is auto-corrected.
Normal	**Normal** ( )	Green	Indicates that all health modules on the appliance are running within the limits configured in the health policy applied to the appliance.
Recovered	**Recovered** ( )	Green	Indicates that all health modules on the appliance are running within the limits configured in the health policy applied to the appliance, including modules that were in a Critical or Warning state.

Status Level	Status Icon	Status Color in Pie Chart	Description
Disabled	**Disabled** (⊘)	Blue	Indicates that an appliance is disabled or excluded, that the appliance does not have a health policy applied to it, or that the appliance is currently unreachable.

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

You must be an Admin, Maintenance, or Security Analyst user to perform this procedure.

The Table View of Health Events page provides a list of all health events on the specified appliance.

When you access health events from the Health Monitor page on your Firepower Management Center, you retrieve all health events for all managed appliances.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.



Tip You can bookmark this view to allow you to return to the page in the health events workflow containing the Health Events table of events. The bookmarked view retrieves events within the time range you are currently viewing, but you can then modify the time range to update the table with more recent information if needed.

Procedure

Choose **System** > **Health** > **Events**.

Tip
If you are using a custom workflow that does not include the table view of health events, click **(switch workflow)**. On the Select Workflow page, click **Health Events**.

Note
If no events appear, you may need to adjust the time range.

Viewing Health Events by Module and Appliance

Procedure

Step 1 View the health monitor for the appliance; see Viewing the Device Health Monitor, on page 26.

Step 2 In the **Module Status Summary** graph, click the color for the event status category you want to view.

The Alert Detail list toggles the display to show or hide events.

Step 3 In the **Alert Detail** row for the alert for which you want to view a list of events, click **Events**.

The Health Events page appears, containing results for a query with the name of the appliance and the name of the specified health alert module as constraints. If no events appear, you may need to adjust the time range.

Step 4 If you want to view all health events for the specified appliance, expand **Search Constraints**, and click the **Module Name** constraint to remove it.

Viewing the Health Events Table

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

Procedure

Step 1 Choose **System** > **Health** > **Events**.

Step 2 You have the following choices:

- Bookmark — To bookmark the current page so that you can quickly return to it, click **Bookmark This Page**, provide a name for the bookmark, and click **Save**.
- Change Workflow — To choose another health events workflow, click **(switch workflow)**.
- Delete Events — To delete health events, check the check box next to the events you want to delete, and click **Delete**. To delete all the events in the current constrained view, click **Delete All**, then confirm you want to delete all the events.
- Generate Reports — Generate a report based on data in the table view — click **Report Designer**.
- Modify — Modify the time and date range for events listed in the Health table view. Note that events that were generated outside the appliance's configured time window (whether global or event-specific) may appear in an event view if you constrain the event view by time. This may occur even if you configured a sliding time window for the appliance.
- Navigate — Navigate through event view pages.
- Navigate Bookmark — To navigate to the bookmark management page, click **View Bookmarks** from any event view.
- Navigate Other — Navigate to other event tables to view associated events.
- Sort — Sort the events that appear, change what columns display in the table of events, or constrain the events that appear
- View All — To view event details for all events in the view, click **View All**.

- View Details — To view the details associated with a single health event, click the down arrow link on the left side of the event.
- View Multiple — To view event details for multiple health events, choose the check box next to the rows that correspond with the events you want to view details for and then click **View**.
- View Status — To view all events of a particular status, click status in the Status column for an event with that status.

The Health Events Table

The Health Monitor modules you choose to enable in your health policy run various tests to determine appliance health status. When the health status meets criteria that you specify, a health event is generated.

The table below describes the fields that can be viewed and searched in the health events table.

Table 4: Health Event Fields

Field	Description
Module Name	Specify the name of the module which generated the health events you want to view. For example, to view events that measure CPU performance, type `CPU`. The search should retrieve applicable CPU Usage and CPU temperature events.
Test Name (Search only)	The name of the health module that generated the event.
Time (Search only)	The timestamp for the health event.
Description	The description of the health module that generated the event. For example, health events generated when a process was unable to execute are labeled `Unable to Execute`.
Value	The value (number of units) of the result obtained by the health test that generated the event. For example, if the Firepower Management Center generates a health event whenever a device it is monitoring is using 80 percent or more of its CPU resources, the value could be a number from 80 to 100.
Units	The units descriptor for the result. You can use the asterisk (*) to create wildcard searches. For example, if the Firepower Management Center generates a health event when a device it is monitoring is using 80 percent or more of its CPU resources, the units descriptor is a percentage sign (%).
Status	The status (Critical, Yellow, Green, or Disabled) reported for the appliance.
Domain	For health events reported by managed devices, the domain of the device that reported the health event. For health events reported by the Firepower Management Center, `Global`. This field is only present in a multidomain deployment.

Field	Description
Device	The appliance where the health event was reported.

History for Health Monitoring

Feature	Version	Details
New health modules	7.0.0	We added the following health modules: • AMP Connection Status: Monitors AMP cloud connectivity from the FTD. • AMP Threat Grid Status: Monitors AMP Threat Grid cloud connectivity from the FTD. • ASP Drop: Monitors the connections dropped by the data plane accelerated security path. • Advanced Snort Statistics: Monitors Snort statistics related to packet performance, flow counters, and flow events. • Event Stream Status: Monitors connections to third-party client applications that use the Event Streamer. • FMC Access Configuration Changes: Monitors access configuration changes made directly on the FMC. • FMC HA Status: Monitors the active and standby FMC and the sync status between the devices. Replaces the HA Status module. • FTD HA Status: Monitors the active and standby FTD HA pair and the sync status between the devices. • File System Integrity Check: Performs a file system integrity check if the system has CC mode or UCAPL mode enabled. • Flow Offload: Monitors hardware flow offload statistics on the Firepower 9300 and 4100 platforms. • Hit Count: Monitors the number of times a particular rule is hit on the access control policy. • MySQL Status: Monitors the status of the MySQL database. • NTP Status FTD: Monitors the NTP clock synchronisation status of the managed device. • RabbitMQ Status: Monitors the status of the RabbitMQ messaging broker. • Routing Statistics: Monitors both IPv4 and IPv6 route information from the FTD. • SSE Connection Status: Monitors SSE cloud connectivity from the FTD. • Sybase Status: Monitors the status of the Sybase database. • Unresolved Groups Monitor: Monitors the unresolved groups used in access control policies. • VPN Statistics: Monitors site-to-site and remote access VPN tunnel statistics. • xTLS Counters: Monitors xTLS/SSL flows, memory and cache effectiveness.

Feature	Version	Details

Health monitor enhancements	7.0.0	The health monitor adds the following enhancements:
		• Enhanced FMC dashboard with summary views of:
		  • High Availability
		  • Event Rate & Capacity
		  • Process Health
		  • CPU thresholds
		  • Memory
		  • Interface rates
		  • Disk Usage
		• Enhanced FTD dashboard:
		  • Health alert for split brain scenario
		  • Additional health metrics available from new Health Modules

New health modules	6.7.0	The CPU Usage module is no longer used. Instead, see the following modules for CPU usage: • CPU Usage (per core): Monitors the CPU usage on all of the cores. • CPU Usage Data Plane: Monitors the average CPU usage of all data plane processes on the device. • CPU Usage Snort: Monitors the average CPU usage of the Snort processes on the device. • CPU Usage System: Monitors the average CPU usage of all system processes on the device. The following modules were added to track statistics: • Connection Statistics: Monitors the connection statistics and NAT translation counts. • Critical Process Statistics: Monitors the state of critical processes, their resource consumption, and the restart counts. • Deployed Configuration Statistics: Monitors statistics about the deployed configuration, such as the number of ACEs and IPS rules. • Snort Statistics: Monitors the Snort statistics for events, flows, and packets. The following modules were added to track memory usage: • Memory Usage Data Plane: Monitors the percentage of allocated memory used by the Data Plane processes. • Memory Usage Snort: Monitors the percentage of allocated memory used by the Snort process.

Feature	Version	Details
Health monitor enhancements	6.7.0	The health monitor adds the following enhancements: • Health Status summary page that provides an at-a-glance view of the health of the Firepower Management Center and all of the devices that the FMC manages. • The Monitoring navigation pane allows you to navigate the device hierarchy. • Managed devices are listed individually, or grouped according to their geolocation, high availability, or cluster status where applicable. • You can view health monitors for individual devices from the navigation pane. • Custom dashboards to correlate interrelated metrics. Select from predefined correlation groups, such as CPU and Snort; or create a custom correlation dashboard by building your own variable set from the available metric groups.
Functionality moved to the Threat Data Updates on Devices module	6.7.0	The Local Malware Analysis module is no longer used. Instead, see the Threat Data Updates on Devices module for this information. Some information formerly provided by the Security Intelligence module and the URL Filtering Module is now provided by the Threat Data Updates on Devices module.
New health module: Configuration Memory Allocation	7.0.0 6.6.3	Version 6.6.3 improves device memory management and introduces a new health module: Configuration Memory Allocation. This module alerts when the size of your deployed configurations puts a device at risk of running out of memory. The alert shows you how much memory your configurations require, and by how much this exceeds the available memory. If this happens, re-evaluate your configurations. Most often you can reduce the number or complexity of access control rules or intrusion policies.
URL Filtering Monitor improvements	6.5.0	The URL Filtering Monitor module now alerts if the FMC fails to register to the Cisco cloud.
URL Filtering Monitor improvements	6.4.0	You can now configure time thresholds for URL Filtering Monitor alerts.
New health module: Threat Data Updates on Devices	6.3.0	A new module, **Threat Data Updates on Devices**, was added. This module alerts you if certain intelligence data and configurations that devices use to detect threats has not been updated on the devices within the time period you specify.