

Health

The following topics describe how to use health monitoring:

- Requirements and prerequisites for health monitoring, on page 1
- Health monitoring, on page 1
- Health policies, on page 14
- Device exclusion in health monitoring, on page 18
- Health monitor alerts, on page 22
- About the health monitor, on page 24
- Health event views, on page 31

Requirements and prerequisites for health monitoring

This reference provides the requirements and prerequisites needed to implement health monitoring functionality.

Model support

Any

Supported domains

Any

User roles

Admin

Maintenance User

Health monitoring

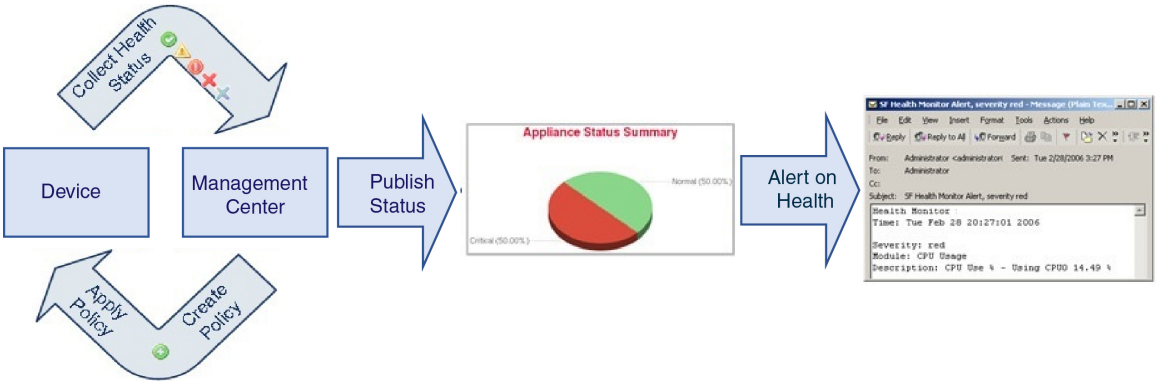
Health monitoring is a system capability that

- tracks various health indicators to ensure hardware and software are working correctly,
- checks the status of critical functionality across your deployment, and
- enables configuration of test frequency for alerting and time series data collection.

Health monitoring capabilities

Health monitoring includes two key capabilities: health status monitoring through health policies and health modules, and time series data collection for metrics analysis.

With time series data collection, you can configure how frequently metric data is collected for the device and its health modules. The device monitor reports these metrics in several predefined health monitor dashboards by default. This metric data is collected for analysis. Some alerts are generated from metric values when they cross the thresholds specified in the health policy.



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 the 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 health monitoring system run the tests in a health policy at the configured intervals. 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 Firewall 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 Firewall Management Center and report the status of the Firewall Management Center's managed devices. For the health modules to provide managed device status, you must deploy all health policies to the device.

You can use the health monitor to access health status information for the entire system and for a particular appliance. In a multi-domain deployment, you can view the health status summary for a device in the domain where the device is located.

A hexagon-shaped widget and status tables on the **Health Status** page provide a visual summary of the status of all appliances on your network, including the Firewall 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 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 want 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 an 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 the health alert.

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

Only users with administrator user role privileges can access system health data.

High availability pair

In a Firewall Management Center high availability deployment, the active peer creates a health monitor page that uses REST APIs to show detailed metric-based information. The standby peer 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 peer does not display the metric-based information.

Health modules

Describes health modules that monitor system conditions and provide alerts or metrics for managing device health and performance.

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

Health monitoring includes both health alerts or tests and metric or time series data collection. The two types of health modules are alert modules and metrics modules. Alerts modules (sometimes called *legacy* modules) monitor system infrastructure and report only the health status. When the conditions specified in the health policy for these monitored systems are met, these modules raise health alerts. Metrics modules (sometimes called *telegraf* modules) collect statistics (sometimes called *time series data*) that you can view on the health monitoring dashboard. Some alerts are also generated from metric values when they cross the thresholds specified in the health policy. You can create custom dashboards with your preferred health metrics, allowing you to monitor statistics or troubleshoot appliance health issues.

Table 1: Device Health Modules

Module	Type	Description
AMP Connection Status	Metrics	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 Threat Grid Connectivity	Metrics	The module alerts if the device cannot connect to the AMP Threat Grid cloud after an initial successful connection.
ASP Drop	Metrics	Monitors the connections dropped by the data plane accelerated security path.
Automatic Application Bypass	Alert	Monitors bypassed detection applications.

Module	Type	Description
Chassis Environment Status	Alert	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`.
Cluster/HA Failover Status	Alert	For threat defense clusters, alerts when a unit joins, leaves, or is elected primary.
Configuration Resource Utilization	Alert	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, reevaluate your configurations. You may be able to reduce the number or complexity of access control rules or intrusion policies.
Connection Statistics	Metrics	Monitors connection statistics and NAT translation counts. For standby Firewall Threat Defense devices in a high availability pair, this widget reflects only the statistics of connections replicated from the active device.
CPU Usage (per core)	Metrics	Alerts when CPU core use exceeds a configurable threshold.
Critical Process Statistics	Metrics	Monitors the state of critical processes, their resource consumption, and the restart counts.
CPU Usage Date Plane	Metrics	Alerts when data plane CPU use exceeds a configurable threshold.
Memory Usage Data Plane	Metrics	Alerts when data plane memory use exceeds a configurable threshold.
Deployed Configuration Statistics	Metrics	Monitors statistics about the deployed configuration, such as the number of ACEs and IPS rules.
Disk Status	Alert	Alerts if there is an issue with the hard disk or RAID controller. If this module alerts, contact Cisco TAC. This will prevent upgrade.
Disk Usage	Metrics	This module compares disk usage on the appliance's hard drive to the limits configured for the module and alerts when usage exceeds the thresholds 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. For more information, refer to 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` although the usage is below the critical or warning threshold specified in the health policy, this could indicate that there are files which must be deleted manually from the system. Contact TAC if you receive these alerts.

Module	Type	Description
File System Integrity Check	Alert	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.
Firewall Threat Defense HA	Alert	Alerts if a threat defense high availability pair is split brain.
Firewall Threat Defense Platform Faults	Alert	Monitors Secure Firewall 1000 /2100 /3100 platform faults and generate health alerts for the faults. A platform fault represents a failure in the Firewall Threat Defense instance or an alarm threshold that has been raised. During the lifecycle of a platform 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, refer to *Cisco Firepower 1000/2100 FXOS Faults and Error Messages Guide*.
Flow Offload Statistics	Metrics	Monitors hardware flow offload.
Hardware Alarms	Alert	This module determines if hardware needs to be replaced on a physical managed device and alerts based on the hardware status. It also reports on the status of hardware-related daemons.
Inline Link Mismatch Alarms	Alert	Alerts if inline pair interfaces negotiate different speeds.
Interface Status	Alert	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 high availability standby device traffic flow. Though it is known that the standby device would not be receiving any traffic yet, the Firewall Management Center 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. • This module displays the traffic rates according to the values from Lina. However, 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 the **Interface** widget. The sampling intervals of Lina and the Firewall Management Center interface statistics are different. Due to the difference in sampling interval, throughput values in the Firewall Management Center GUI can be different from the throughput values appears in the device CLI result. • Note that traffic rates in the **Interface Traffic Rate** widget (**Overview** > **Dashboards heading** > **Dashboard** page) can be different as it displays the input and output rates from Snort.

Module	Type	Description
Intrusion and File Event Rate	Alert	Alerts if intrusion events per second exceed a configurable threshold. We recommend a warning threshold of 1.5 times your average intrusion event rate, and a critical threshold of 2.5 times. For example, for an average event rate on network segment of 20 events per second, we recommend a warning value of 30 and a critical value of 50. The critical limit must be lower than 1000, and higher than the warning limit. Event rates for your devices are available on **System** (⚙) > **Monitoring** > **Statistics**. If the rate is zero, the Snort process may be down or the device may not be sending events.
Link State Propagation	Alert	For the ISA 3000, alerts when an interface in a inline set fails.
Memory Usage	Alert	Alerts when memory use exceeds configurable thresholds. 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, it is recommended 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. For more information, refer to Memory usage thresholds for health monitor alerts for additional information about how thresholds are calculated. Complex access control policies and rules can command significant resources and negatively affect performance.
Network Card Reset	Alert	Alerts when a network card restarts due to hardware failure.
NTP Statistics	Metrics	Monitors NTP synchronization status. Disabled by default.
Firewall Management Center Access Configuration Changes	Alert	Monitors configuration changes made on the Firewall Management Center directly using the **configure network management-data-interface** command. This module alerts when there is a conflict between the existing Firewall Management Center configuration and the out of band configuration changes made.
Process Status	Alert	Alerts when 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.
Routing Statistics	Metrics	Monitors the current state of routing table.
Snort 3 Statistics	Metrics	Collects Snort 3 statistics for events, flows, and packets.

Module	Type	Description
CPU Usage Snort	Metrics	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`.
Snort Identity Memory Usage	Alert	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 Snort 2 to Snort 3 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.
Memory Usage Snort	Metrics	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`.
Snort Reconfiguring Detection	Metrics	Alerts if a device reconfiguration has failed. This module detects reconfiguration failure for both Snort 2 and Snort 3 instances.
Snort Statistics	Metrics	Monitors Snort statistics for events, flows, and packets.
SSE Connection Status	Metrics	The module alerts if the device cannot connect to the security services exchange cloud after an initial successful connection. Disabled by default.
CPU Usage System	Metrics	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`.

Module	Type	Description
Threat Data Updates on Devices	Alert	Certain intelligence data and configurations that devices use to detect threats are updated on the Firewall Management Center 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 **Integration** > **Dynamic Attributes Connector** 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. Refer to **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 Firewall Management Center or on any devices, verify that the Firewall Management Center can reach the devices.
VPN Statistics	Metrics	Monitors site-to-site and remote access VPN tunnels between Firewall Threat Defense devices.
XTLS Counters	Metrics	Monitors XTLS/SSL flows, memory and cache effectiveness. Disabled by default.

Table 2: Management Center Health Modules

Module	Type	Description
Secure Endpoint Status	Alert	The module alerts if the Firewall Management Center 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 Secure Endpoint management console.
AMP for Firepower Status	Alert	Alerts if: • The Firewall Management Center cannot contact the AMP cloud (public or private) or the Secure Malware Analytics Cloud or 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 Secure Malware Analytics Cloud or Secure Malware Analytics 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 Firewall Management Center loses connectivity to the Internet, the system may take up to 30 minutes to generate a health alert.
Appliance Heartbeat	Alert	This module determines if an appliance heartbeat is being heard from the appliance and alerts based on the appliance heartbeat status.
CPU Usage (per core)	Metrics	This module checks that the CPU usage on all the cores is not overloaded and alerts when CPU usage exceeds the thresholds configured for the module. The **Warning Threshold %** default value is `80`. The **Critical Threshold %** default value is `90`.
Critical Process Statistics	Metrics	Monitors the state of critical processes, their resource consumption, and the restart counts.
Database Size	Alert	Alerts if the configuration database size is too big. If this module alerts, contact Cisco TAC. This will prevent upgrade.
Discovery Host Limit	Alert	This module determines if the number of hosts the Firewall Management Center can monitor is approaching the limit and alerts based on the warning level configured for the module. For more information, refer to Host limits.
Disk Status	Alert	This module examines the performance of the hard disk and storage pack (if installed) on the appliance. The disk status health module generates a critical alert (red) if either of the following conditions is detected: • One or more disks may have failed or are experiencing errors. • An installed storage pack cannot be detected or unrecognized. All other disk health conditions generate a warning alert (yellow). For further diagnosis of warning conditions, contact Cisco Technical Assistance Center.

Module	Type	Description
Disk Usage	Metrics	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 thresholds 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. Refer to 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` although the usage is below the critical or warning threshold specified in the health policy, this could indicate that there are files which must be deleted manually from the system. Contact TAC if you receive these alerts.
eStream Status	Alert	Monitors connections to third-party client applications that use the Event Streamer on the Firewall Management Center.
Event Backlog Status	Alert	Alerts if the backlog of event data awaiting transmission from the device to the Firewall Management Center has grown continuously for more than 30 minutes. To reduce the backlog, evaluate your bandwidth and consider logging fewer events.
Event Monitor	Metrics	This module monitors overall incoming event rate to Firewall Management Center.
File System Integrity Check	Alert	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.
Firewall Management Center HA Status	Alert	Monitors Firewall Management Center high availability. This module generates alerts if the HA pairs are not synchronized and if there is a discrepancy in the number of managed devices between the active and standby units.
Health Monitor Process	Alert	Monitors the health process itself, and alerts if there have been no health events in some number of minutes (configurable).
ISE Connection Monitor	Alert	This module monitors the status of the server connections between the Cisco Identity Services Engine (ISE) and the Firewall Management Center. ISE provides additional user data, device type data, device location data, SGTs (Security Group Tags), and SXP (Security Exchange Protocol) services.
License Monitor	Alert	This module monitors expiration of Classic licenses.
Local Malware Analysis	Alert	This module monitors ClamAV updates for Local Malware Analysis.

Module	Type	Description
Memory Usage	Alert	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, it is recommended 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. For additional information about how thresholds are calculated, refer to Memory usage thresholds for health monitor alerts. Beginning with Version 6.6.0, the minimum required RAM for Firewall Management Center Virtual upgrades to Version 6.6.0+ is 28 GB, and the recommended RAM for Firewall Management Center Virtual deployments is 32 GB. We recommend you do not decrease the default settings: 32 GB RAM for most Firewall Management Center Virtual instances, 64 GB for the Firewall Management Center Virtual 300 (VMware only). **Attention** A critical alert is generated by the health monitor when insufficient RAM is allocated to a Firewall Management Center Virtual deployment. Complex access control policies and rules can command significant resources and negatively affect performance.
MySQL Statistics	Metrics	Monitors the status of the MySQL database, including the database size, number of active connections, and memory use.
Process Status	Alert	Alerts when 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	Metrics	Monitors and collects RabbitMQ statistics.

Module	Type	Description
Realm	Alert	Allows you to set a warning threshold for realm or user mismatches, which are: • User mismatch: A user is reported to the Secure Firewall 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 Secure Firewall Management Center. Review the information discussed in *Cisco Secure Firewall Management Center Device Configuration Guide*. • Realm mismatch: A user logs into a domain that corresponds to a realm not known to the Firewall Management Center. For more information, *Cisco Secure Firewall Management Center Device Configuration Guide*. This module also displays health alerts when you try to download more users than the maximum number of downloaded users supported per realm. The maximum number of downloaded users for a single realm depends on your management center model. For more information, refer to *User Limit* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
RRD Server Process	Alert	Alerts if the round robin data (RRD) server that stores time series data has restarted since the last time it updated. You can configure additional warning and critical thresholds for consecutive restarts.
Security Intelligence	Alert	Alerts if Security Intelligence is in use and the Firewall Management Center cannot update a feed, or feed data is corrupt or contains no recognizable IP addresses. Refer to the Threat Data Updates on Devices module.
Smart License Monitor	Alert	Monitors Smart Licensing status and 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.
Sybase Statistics	Metrics	Monitors the status of the Sybase database, including the database size, number of active connections, and memory use.

Module	Type	Description
Threat Data Updates on Devices	Alert	Certain intelligence data and configurations that devices use to detect threats are updated on the Firewall Management Center 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 **Integration** > **Dynamic Attributes Connector** 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. Refer to 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 Firewall Management Center or on any devices, verify that the Firewall Management Center can reach the devices.
Time Series Data (RRD) Monitor	Alert	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	Alert	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.

Module	Type	Description
Unresolved Groups Monitor	Alert	Monitors Foreign Security Principals (FSPs) that are groups used in policies. Security principals are Active Directory objects, like authenticated user groups, to which security can be applied in access control policies. This module generates a warning alert for unresolved groups that exist but are not used in policies, and a critical alert for unresolved groups that are used in policies.
URL Filtering Monitor	Alert	Monitors connectivity with the Cisco cloud, which is required for downloading URL filtering data and doing URL filtering lookups.
VPN Tunnel Status	Alert	Alerts when VPN tunnels are down. Supported for both remote access and site-to-site VPN , with the exception of VTI site-to-site tunnels.

Configure health monitoring

Health monitoring enables proactive management of network appliances by tracking their operational status using customizable policies and alert mechanisms. You can configure specific monitoring policies for different appliance types, enabling only the relevant tests for each type.

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, 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 Create a health policy, on page 15.

Step 3 (Optional.) Configure health monitor alerts as discussed in Create a health monitor alert, on page 23.

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 is a configuration framework that

- enables you to define test criteria for monitoring the health of appliances,
- allows selective enabling of health modules and critical alert settings, and
- provides flexibility to apply, customize, or use default policies for each appliance.

Health policy configuration options

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.

Note When you register an appliance, the Firewall Management Center automatically assigns it the default health policy. To disassociate a health policy from an appliance, you must first associate a different health policy with it. An appliance must have at least one health policy assigned.

Default health policy

The Firewall 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 Firewall Management Center.

This initial health policy is based on a default health policy. You cannot view or edit the default health policy, but you can copy it when creating a custom health policy.

Upgrades and the default health policy

When you upgrade the Firewall Management Center, 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.

Create a health policy

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 edit the policy to specify your preferences, such as enable or disable modules within the policy, change the alerting criteria for each module as needed, and specify the run time intervals.

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Policy**.

Step 2 Click **Create Policy**.

Step 3 Enter a name for the policy.

Note that the following names are reserved for the default policies, and you cannot create a health policy using these names:

- Default Device Policy
- Default Health Policy

Step 4 Choose the existing policy that you want to use as the basis for the new policy from the **Base Policy** drop-down list.

Step 5 Enter a description for the policy.

Step 6 Choose **Save**.

What to do next

- Apply the health policy on devices as described in Apply a health policy, on page 16.
- Edit the policy to specify the module-level policy settings as described in Edit a health policy, on page 17.

Apply a health policy

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 Firewall 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. However, you must have at least one health policy assigned to an appliance.

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.

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Policy**.

Step 2 Click the **Deploy health policy** (📥) next to the policy you want to apply.

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

Note
An appliance must have at least one health policy assigned to it. To stop health monitoring for an appliance, create a health policy with all modules disabled and apply it to the appliance. To disassociate a health policy from an appliance, you must first associate a different health policy with it.

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

The health policy is successfully applied to the selected appliances, and monitoring begins automatically.

What to do next

- Optionally, monitor the task status; see View task messages.

  Monitoring of the appliance starts when the policy is successfully applied.

Edit a health policy

Edit a health policy when you need to adjust which modules are monitored, change critical or warning thresholds, or reassign policies to different devices.

Before you begin

- Ensure you have access to Firewall Management Center.
- Identify the health policy you need to modify.

Follow these steps to edit a health policy:

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Policy**.

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

Step 3 To edit the policy name and its description, click the **Edit** (✎) icon provided against the policy name.

Step 4 The **Health Modules** tab displays all the device modules and its attributes. Configure your health modules using the following actions:

- Click the toggle button that is provided against the module and its attributes—turn on () or turn off () to enable or disable testing of health status respectively.
- To execute a bulk enable or disable testing on the health modules, click the **Select All** toggle button

Note

- The modules and attributes are flagged with the supporting appliances—Firewall Threat Defense, Firewall Management Center, or both.
- You cannot choose to include or exclude the individual attributes of CPU and Memory modules.

For information on the modules, refer to Health modules, on page 3.

Step 5 Where appropriate, set the **Critical** and **Warning** threshold percentages.

Step 6 In the **Run Time Intervals** tab, enter the relevant values in the fields:

- **Health Module Run Interval**: The frequency for running the health modules. The minimum interval is 5 minutes.
- **Metric Collection Interval**: The frequency of collecting the time series data on the device and its health modules. The device monitor reports these metrics in several predefined health monitor dashboards by default. For detailed information on the dashboard, refer to View the device health monitor, on page 28. The metric data is collected for analysis and hence no alerting is associated with it.

Step 7 To view and modify the devices to which the policy is assigned, do the following:

a) Click **Policy Assignments & Deploy**.

b) From the **Available Devices** list, click the + icon next to the device to which you want to assign the health policy.

c) Click **Apply**.

Alternatively, you can apply the health policy to your appliance as described in Apply a health policy, on page 16

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 Firewall Management Center.

Step 8 Click **Save**.

Delete a health policy

You can delete health policies that you no longer need. However, an appliance must have at least one health policy assigned to it. 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.

Note 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 that you want to delete.

Step 3 Click **Delete health policy** to delete it.

Device exclusion in health monitoring

A device exclusion is a health monitoring configuration that

- prevents deliberate device or module outages from affecting the overall health summary,
- allows administrators to temporarily disable health monitoring for selected devices, Firewall Management Center where supported, or specific health modules, and
- ensures health events generated during exclusion are marked as disabled and do not affect health calculations.

Device exclusion behavior

In the course of normal network maintenance, you may disable managed devices or make them temporarily unavailable. In Firewall Management Center, you can also exclude Firewall Management Center health monitoring where applicable. Because those outages or expected conditions are deliberate, you may not want their health status to affect the overall health summary.

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 device or module from the excluded list, the events that were generated during the exclusion continue to show a status of disabled.

Note If all health modules or a device are added to the exclusion list, the device's health status will be set to disabled. This status refers only to health monitoring and should not be interpreted as the device being offline or disconnected.

You can also disable an individual health module. For example, when you reach the host limit on the Firewall Management Center, you can disable Host Limit status messages. Excluding health modules for individual interfaces is not supported on devices operating in transparent mode.

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

Note On Firewall 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 Firewall Management Center, the exclusion settings remain persistent. The newly re-registered device remains excluded.

Temporary device exclusion scenario

You can use the health monitor exclude feature to disable health monitoring status reporting for a device, Firewall Management Center where applicable, or specific health modules. 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 Firewall Management Center from displaying a warning or critical state because of the lapsed connection to the device.

To temporarily disable health events from a managed device, or from Firewall Management Center where supported, go to the exclusion configuration page and add the target to the exclusion list. After the setting takes effect, the system no longer considers the excluded device when calculating the overall health status. The Health Monitor Appliance Status Summary lists the device as disabled.

Exclude devices from health monitoring

Exclude devices from health monitoring to disable their events and health status when needed for maintenance or troubleshooting purposes.

You can exclude managed devices individually or by group, model, associated health policy, or other supported scope. In Firewall Management Center exclusion can also apply to Firewall Management Center where supported.

If you need to set the events and health status for an individual managed device to disabled, you can exclude the device from health monitoring. Where supported, you can also exclude Firewall Management Center health monitoring. After the exclusion settings take effect, the device shows as disabled in the Health Monitor Appliance Module Summary, and health events for the device have a status of disabled.

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Exclude**.

Step 2 Click **Add Device**.

Step 3 In the **Device Exclusion** dialog box, under **Available Devices**, click **Add** (⊕) against the device that you want to exclude from health monitoring.

Step 4 Click **Exclude**.

The selected device is displayed in the exclusion main page.

Step 5 To remove the device from the exclusion list, click **Delete** (🗑).

Step 6 Click **Apply**.

Exclude health policy modules on a device

Excluding health policy modules is useful when certain modules produce irrelevant or temporary health alerts, which you do not want to affect the overall device status. Exclusion settings indicate the number of modules excluded from health monitoring.

Note Excluding health modules for individual interfaces is not supported on devices operating in transparent mode.

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

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Exclude**.

Step 2 Click **Edit** (✎) next to the Firewall Threat Defense device you want to modify.

Step 3 In the **Exclude Health Modules** dialog box, by default, all the modules of the device are excluded from health monitoring.

Certain modules are applicable to a specific device only; for more information, refer to Health modules, on page 3.

Step 4 To choose modules to be excluded from health monitoring, click the **Enable Module Level Exclusion** link.

The **Exclude Health Modules** dialog box displays all the modules of the device. The modules that are not applicable for the associated health policies are disabled by default. To exclude a module, perform these steps:

a. Click the **Slider** () button next to the desired module.

b. To specify the duration of the exclusion for the selected modules, from the **Exclude Period** drop-down list, select the duration.

Step 5 Click **OK**.

Step 6 Click **Apply**.

Note
Interface exclusion differs from other module exclusions because you can exclude selected physical interfaces while still monitoring associated subinterfaces, depending on the UI options available in your version.

Exclude interface health monitoring

Use interface exclusion when you want to suppress health status updates for selected physical interfaces without suppressing health monitoring for the entire device. Interface exclusion is useful when interface state is expected during maintenance or when you want to focus on subinterface health instead of physical interface status.

When you configure interface exclusion, select the physical interfaces that you want to exclude from the list of available interfaces. Depending on the available UI options in your version, selecting a physical interface can also exclude its subinterfaces. If subinterface controls are available, you can continue monitoring subinterfaces while excluding only the physical interface.

Use this option to reduce unnecessary health alerts when traffic loss or interface state changes are expected on a physical interface.

Manage expired health monitor exclusions

When monitoring device or module health, some items may have temporary exclusions. Once these exclusion periods lapse, you need to decide whether to renew the exclusion or clear the device/module from exclusion so alerts resume.

Procedure

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

The **Warning** () icon is displayed against the device indicating the expiry of the duration of exclusion of the device or the modules from alerting.

Step 2 To renew the exclusion of the device, click **Edit** () next to the device. In the **Exclude Health Modules** dialog box, click the **Renew** link. The exclusion period of the device is extended with the current value.

Step 3 To clear the device from being excluded, click **Delete** ( ) next to the device, click **Remove the device from exclusion**, and then click **Apply**.

Step 4 To renew or clear the modules from exclusion, click **Edit** ( ) next to the device. In the **Exclude Health Modules** dialog box, click the **Enable Module Level Exclusion** link, and then click the **Renew** or **Clear** link against the modules. When you click **Renew**, the exclusion period is extended on the module with the current value.

Health monitor alerts

A health monitor alert is a notification mechanism that

- provides email, SNMP, or syslog notifications when module status changes occur,
- enables association of alert responses with health event levels to trigger notifications based on event severity, and
- allows customization to monitor specific system conditions such as disk space thresholds.

Disk space monitoring alert 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.

Health monitor alert information

The alerts generated by the health monitor contain specific information that helps identify issues and their severity.

Health monitor alerts include these attributes:

- Severity: Indicates the severity level of the alert.
- Module: Specifies the health module whose test results triggered the alert.
- Description: Includes the health test results that triggered the alert.

The table describes these severity levels.

Table 3: 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.

Severity	Description
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.

Create a health monitor alert

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.

Before you begin

- You must be an Admin user.
- Ensure that you have configured alert responses that govern the Firewall Management Center's communication with the SNMP, syslog, email server, or webhook where you send the health alert; For more information, refer to Configuring external alerts with alert responses.

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Monitor Alerts**.

Step 2 Click **Add**.

Step 3 In the **Add Health Alert** dialog box, enter a name for the health alert in the **Health Alert Name** field.

Step 4 From the **Severity** drop-down list, choose the severity level you want to use to trigger the alert.

Step 5 From the **Alert** drop-down list, choose the alert response that you want to trigger when the specified severity level is reached. If you have not yet configured the alert responses, click **Alerts** to visit the **Alerts** page and set them.

Step 6 From the **Health Modules** list, choose the health policy modules for which you want the alert to apply.

Step 7 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 8 Click **Save** to save the health alert.

Edit a health monitor alert

Administrators may need to update the alert parameters for health monitor alerts in order to adjust severity, change modules, or select different responses as requirements evolve.

Before you begin

You must be an Admin user to perform this task.

Follow these steps to edit health monitor alerts:

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Monitor Alerts**.

Step 2 Click the **Edit** (✎) icon that is provided against the required health alert that you want to modify.

Step 3 In the **Edit Health Alert** dialog box, from the **Alert** drop-down list, select the required alert entry, or click **Alerts** link to configure a new alert entry.

Step 4 Click **Save**.

Delete health monitor alerts

Health monitor alerts notify you about system events, issues, or warnings. You may need to delete outdated or irrelevant alerts to streamline monitoring.

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Monitor Alerts**.

Step 2 Click **Delete** (🗑) next to the health alert you want to delete.

Step 3 Click **Delete health alert** to delete it.

What to do next

Disable or delete the underlying alert response to ensure that alerting does not continue. For more information, refer to Configuring external alerts with alert responses.

About the health monitor

The health monitor provides the compiled health status for all devices managed by the Firewall Management Center, plus the Firewall Management Center itself.

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

The health monitor is composed of:

- The Health Status summary page — Provides you with an at-a-glance view of the health of the Firewall Management Center and all of the devices that the Firewall Management Center manages. In a multi-domain deployment, you can view the health status summary for a device in the domain where the device is located. Devices are listed individually, or grouped according to their geolocation, high availability, or cluster status where applicable.
  - View the health summary of the Firewall Management Center 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.

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Monitor**.

Step 2 View the status of the Firewall Management Center 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.

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.

c) In the health monitor, hover over a graph to view all metrics and their respective values at that specific point on the graph. Click on the graph to pin the metrics statistics box, allowing you to explore the metrics and their values in detail. To close the statistics box and move to another point on the graph, simply click the close button.

You have accessed the health monitor and can view the compiled health status for all managed devices. You can interact with the Health Status landing page and use the Monitoring navigation pane to access device-specific health information.

What to do next

- See Device health monitors, on page 26 for information about the compiled health status and metrics for any device managed by the Firewall Management Center.

Device health monitors

The device health monitor provides the compiled health status for any device managed by the Firewall Management Center. The device health monitor collects health metrics for Secure Firewall devices in order to predict and respond to system events.

The device health monitor is comprised of these components:

- System Details: Displays information about the managed device, including the installed Secure Firewall 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 firewall device health metrics categorized across predefined dashboards, including:
  - CPU: CPU utilization, including the CPU usage by process and by physical cores. The Firewall Threat Defense CPU core allocation dashboard shows core assignments for these categories:
    - **Data Plane**: Handles basic network functions, including core packet forwarding and network data processing.
    - **Snort**: Manages intrusion detection and deep packet inspection features.



Note Multi-threaded Snort processes are allocated across multiple Snort cores to improve device performance. The Snort core allocation shown in the **CPU** dashboard reflects the total number of Snort process threads assigned to Snort cores.

    - **System**: Includes all other system processes. While some processes may have dedicated CPU cores allocated, their usage is combined and displayed under the **System** category in the dashboard.

  - Memory: Device memory utilization, including data plane and Snort memory usage.
  - Interfaces: Interface status and aggregate traffic statistics.

- Connections: Connection statistics (such as elephant flows, active connections, peak connections, and so on) 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.

For a comprehensive list of the supported device metrics, refer to Cisco Secure Firewall Threat Defense Health Metrics.

View system details and troubleshoot devices

Use this task when you need to monitor device health or initiate troubleshooting procedures on specific devices through the management center.

Before you begin

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

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 Secure Firewall software version.
- **Model:** The device model.
- **Mode:** The firewall mode. The Firewall 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 these troubleshoot choices:

- Generate troubleshooting files; refer to Generate troubleshooting files for specific system functions
- Generate and download advanced troubleshooting files; refer to Download advanced troubleshooting files.
- Create and modify health policies; refer to Create a health policy, on page 15.

- Create and modify health monitor alerts; refer to Create a health monitor alert, on page 23.

View the device health monitor

The device health monitor compiles device metrics and displays health status and trends using an array of dashboards.

Before you begin

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

Follow these steps to view the device health monitor:

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 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 the **Show Deployment Info** ( ) icon for a deployment overlay on the trend graph, with respect to the selected time range.

The **Show Deployment Info** ( ) 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 can appear. Click the icon on top of the dotted line to view the deployment details.

Step 6 View 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 (such as elephant flows, active connections, peak connections, and so on) and NAT translation counts.
- Snort: Statistics related to the Snort process.
- ASP Drops: Statistics related to the Accelerated Security Path (ASP) performance and behavior.

Note

- Multi-threaded Snort processes are allocated across multiple Snort cores to improve device performance. Note that the Snort core allocation shown in the **CPU**dashboard reflects the total number of Snort process threads assigned to Snort cores.
- The **Process Health** widget in Firewall Management Center displays the CPU% usage for each process. The CPU% metric reflects usage relative to the number of cores in the Firewall Threat Defense device, where 100% corresponds to full utilization of one core. For example, on an 8-core device, 200% indicates two fully utilized cores, leaving six available for other processes. To monitor overall system CPU usage, use the **CPU** widget instead of the **Process Health** widget.

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

Step 7 Click the **Add New Dashboard**(+) to create a custom correlation dashboard by building your own variable set from the available metric groups.

For more information, refer to Correlating device metrics, on page 29.

Correlating device metrics

The device health monitor includes an array of key Firewall Threat Defense device metrics that serve to predict and respond to system events. The health of any Firewall Threat Defense 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 (such as elephant flows, active connections, peak connections, and so on) 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. For a comprehensive list of the supported device metrics, refer to Cisco Secure Firewall Threat Defense Health Metrics.

Before you begin

- To view and correlate the time series data (device metrics) in the health monitor dashboard, enable REST API (**System** (⚙) > **Configuration** > **REST API Preferences**).
- You must be an Admin, Maintenance, or Security Analyst user to perform this procedure.

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

Follow these steps to correlate device metrics:

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Monitor**. In the **Devices** list, click **Expand**(>) and **Collapse** (⌄) to expand and collapse the list of managed devices, and choose the device for which you want to modify the dashboard.

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

Step 2 Click the **Add Dashboard** (+) icon in the upper right corner of the device monitor to add a new dashboard.

Step 3 From the **Select Correlation Group** drop-down, choose a predefined correlation group or to create a custom group. To create a dashboard from a predefined correlation group, choose the group and click **Add**.

Step 4 To create a custom correlation dashboard:

a) Choose **Custom**.
b) Enter a unique name in the **Dashboard Name** field or accept the default.
c) Choose a group from the **Select Metric Group** drop-down, then select corresponding metrics from the **Select Metrics** drop-down.

For a comprehensive list of the supported device metrics, refer to Cisco Secure Firewall Threat Defense Health Metrics.

Step 5 Click **Add Metrics** to add and select metrics from another group, and to remove an individual metric, click the Remove ✕ icon on the right side of the item. Click the delete icon to remove the entire group. Click **Add** to add the dashboard to the health monitor.

Step 6 You can **Edit** or **Delete** custom correlation dashboards.

Health monitor status categories

The table summarizes the available health monitor status categories, their severity levels, icons, associated colors in pie charts, and descriptions.

Table 4: 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.
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

Health event views enable you to monitor health events logged by the health monitor in the Firewall Management Center. The views are fully customizable, allowing you to analyze health statuses efficiently and access related event data.

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.

View health events

Use this task when you need to monitor the health of your appliances and review any incidents or events recorded.

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

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.

Before you begin

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

Follow these steps to view health events:

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.

View health events by module and appliance

This task helps you efficiently monitor appliance health by filtering health events based on module status and viewing detailed alerts for specified events.

Procedure

Step 1 View the health monitor for the appliance; refer to View the device health monitor, on page 28.

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.

View the health events table

The Health Events Table provides actionable insight into system health and allows users to organize, modify, and respond to health events.

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.
- Search: Search for specific health events or health metrics recorded within your deployment. Customize your search query to analyze health events and other monitored data and save the search constraints for quick access. For more information, refer to Event searches.

Health event fields

The health monitor modules you enable in your health policy run tests to determine appliance health status. When the health status meets specified criteria, a health event is generated. The health event table includes fields that are searchable and viewable for monitoring appliance health.

Table 5: 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 Firewall 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 Firewall 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.
Device	The appliance where the health event was reported.