Using Health Monitoring

The health monitor provides numerous tests for determining the health of an appliance from the Defense Center. 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. You can create one health policy for every appliance in your system, customize a health policy for the specific appliance where you plan to apply it, or use the default health policy. You can also import a health policy exported from another Defense Center.

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 blacklisting 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. Optionally, you can also configure email, SNMP, or syslog alerting in response to health events.

On the Defense Center, you can view health status information for the entire system or for a particular 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.

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

See the following sections for more information:

- Understanding Health Monitoring, page 68-1
- Configuring Health Policies, page 68-6
- Using the Health Monitor Blacklist, page 68-34
- Configuring Health Monitor Alerts, page 68-37
- Using the Health Monitor, page 68-39
- Using Appliance Health Monitors, page 68-41
- Working with Health Events, page 68-46

Understanding Health Monitoring

License: Any
You can use the health monitor to check the status of critical functionality across your FireSIGHT System deployment. Monitor the health of your entire FireSIGHT System through the Defense Center by applying health policies to each of the managed devices and collecting the resulting health data at the Defense Center. Pie charts and status tables on the Health Monitor page visually represent the health status for monitored appliances, so you can check status at a glance, then drill down into status details if needed.

You can use the health monitor to access health status information for the entire system or for a particular appliance. The Health Monitor page provides a visual summary of the status of all appliances on your system. Individual appliance health monitors let you drill down into health details for a specific appliance.

You can also view health events in the standard FireSIGHT System table view. From an individual appliance’s health monitor, you can open a table view of occurrences of a specific event, or you can retrieve all the health events for that appliance. You can also search for specific health events. 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.

Because health monitoring is an administrative activity, only users with administrator user role privileges can access system health data. For more information on assigning user privileges, see Modifying User Privileges and Options, page 61-56.

Note: Except for the Defense Center, FireSIGHT System devices do not have health monitoring policies applied to them by default. Managed devices report hardware status automatically via the Hardware Alarms health module; if you want to use other modules to monitor a managed device, you must apply...
Understanding Health Monitoring

A health policy is a collection of health module settings you apply to an appliance to define the criteria that the Defense Center uses when checking the health of the appliance. The health monitor tracks a variety of health indicators to ensure that your FireSIGHT System hardware and software are working correctly.

When you create health policies, you choose which tests to run to determine appliance health. You can also apply the default health policy to any appliance.

Understanding Health Policies

**License:** Any

A *health policy* is a collection of health module settings you apply to an appliance to define the criteria that the Defense Center uses when checking the health of the appliance. The health monitor tracks a variety of health indicators to ensure that your FireSIGHT System hardware and software are working correctly.

When you create health policies, you choose which tests to run to determine appliance health. You can also apply the default health policy to any appliance.

Understanding Health Modules

**License:** Any

*Health modules*, also sometimes referred to as *health tests*, are scripts that test for the criteria you specify in a health policy. The available health modules are described in the following table.

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Malware Protection</td>
<td>This module alerts if the Defense Center cannot contact the Collective Security Intelligence Cloud, either to retrieve file disposition information for files detected in network traffic or to submit files for dynamic analysis, or if an excessive number of files are detected in network traffic, based on the file policy configuration. Connections via the FireAMP Private Cloud also generate alerts if the private cloud cannot connect to the public Cisco cloud. This module runs on all Defense Centers except the DC500, which does not support advanced malware protection.</td>
</tr>
<tr>
<td>Appliance Heartbeat</td>
<td>This module determines if an appliance heartbeat is being heard from the appliance and alerts based on the appliance heartbeat status.</td>
</tr>
<tr>
<td>Automatic Application Bypass Status</td>
<td>This module determines if an appliance has been bypassed because it did not respond within the number of seconds set in the bypass threshold, and alerts when a bypass occurs.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>This module checks that the CPU on the appliance is not overloaded and alerts when CPU usage exceeds the percentages configured for the module. This module is not available for health policies applied to 3D9900 devices.</td>
</tr>
</tbody>
</table>
### Table 68-1 Health Modules (continued)

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Reset</td>
<td>This module checks for network cards which have restarted due to hardware failure and alerts when a reset occurs.</td>
</tr>
<tr>
<td>Disk Status</td>
<td>This module examines performance of the hard disk, and malware storage pack (if installed) on the appliance. It alerts when the hard disks and RAID controller (if installed) are in danger of failing, or if the malware storage pack is not detected after installation or inauthentic.</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>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.</td>
</tr>
<tr>
<td>FireAMP Status Monitor</td>
<td>The module alerts if the Defense Center cannot connect to the Cisco cloud after an initial successful connection, if you deregister a cloud connection using the FireAMP portal, or if your private cloud is unable to communicate with the public Cisco cloud. This module only runs on Defense Centers.</td>
</tr>
<tr>
<td>FireSIGHT Host License Limit</td>
<td>This module determines if sufficient FireSIGHT host licenses remain and alerts based on the warning level configured for the module. This module only runs on Defense Centers.</td>
</tr>
<tr>
<td>Hardware Alarms</td>
<td>This module determines if hardware needs to be replaced on a Series 3 or 3D9900 device and alerts based on the hardware status. The module also reports on the status of hardware-related daemons and on the status of clustered appliances. For more information on the details reported for these devices, see Interpreting Hardware Alert Details for 3D9900 Devices, page 68-49 and Interpreting Hardware Alert Details for Series 3 Devices, page 68-51.</td>
</tr>
<tr>
<td>Health Monitor Process</td>
<td>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 Defense Center exceeds the Warning or Critical limits. This module only runs on Defense Centers.</td>
</tr>
<tr>
<td>Inline Link Mismatch Alarms</td>
<td>This module monitors the ports associated with inline sets and alerts if the two interfaces of an inline pair negotiate different speeds.</td>
</tr>
<tr>
<td>Intrusion Event Rate</td>
<td>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 Event Rate is zero, the intrusion process may be down or the managed device may not be sending events. Select Analysis &gt; Intrusions &gt; Events to check if events are being received from the device.</td>
</tr>
<tr>
<td>Interface Status</td>
<td>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.</td>
</tr>
<tr>
<td>License Monitor</td>
<td>This module determines if sufficient licenses for Control, Protection, URL Filtering, Malware, and VPN remain. It also alerts when devices in a stack have mismatched license sets. It alerts based on a warning level automatically configured for the module. You cannot change the configuration of this module. This module only runs on Defense Centers.</td>
</tr>
<tr>
<td>Link State Propagation</td>
<td>This module determines when a link in a paired inline set fails and triggers the link state propagation mode.</td>
</tr>
</tbody>
</table>
### Understanding Health Monitoring

**Memory Usage**
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.

**Power Supply**
This module determines if power supplies on the device require replacement and alerts based on the power supply status.

This module runs on these Defense Centers: DC1500, DC2000, DC3500, DC4000.

This module runs on these devices: 3D3500, 3D4500, 3D6500, 3D9900, and Series 3.

**Process Status**
This module determines if processes on the appliance exit or terminate outside of the process manager. If a process is deliberately exited outside of the process manager, the module status changes to Warning and the health event message indicates which process exited, until the module runs again and the process has restarted. If a process terminates abnormally or crashes outside of the process manager, the module status changes to Critical and the health event message indicates the terminated process, until the module runs again and the process has restarted.

**Reconfiguring Detection**
This module determines if detection capabilities persist after a failed policy apply on a registered managed device. If detection capabilities appear un-operational after a policy apply fails, the module generates health alerts until detection capabilities are reestablished.

**RRD Server Process**
This module determines if the round robin data server that stores time series data is running properly and alerts based on the number of recent RRD server restarts.

This module only runs on Defense Centers.

**Security Intelligence**
This module alerts in a variety of situations involving Security Intelligence filtering, including feed update, feed corruption, and memory issues.

This module runs on all Defense Centers except the DC500, which does not support Security Intelligence filtering.

**Time Series Data Monitor**
This module tracks the presence of corrupt files in the directory where time series data (such as compliance event counts) are stored and alerts when files are flagged as corrupt and removed.

This module only runs on Defense Centers.

**Time Synchronization Status**
This module tracks the synchronization of a device clock that obtains time using NTP with the clock on the NTP server and alerts if the difference in the clocks is more than ten seconds.

**URL Filtering Monitor**
This module tracks communication between the Defense Center and the Cisco cloud, where the system obtains its URL filtering (category and reputation) data for commonly visited URLs. The module alerts if the Defense Center fails to successfully communicate with or retrieve an update from the cloud.

This module also tracks communications between the Defense Center and any managed devices where you have enabled URL filtering. The module alerts if the Defense Center cannot push URL filtering data to those devices.

This module only runs on all Defense Centers except the DC500, which does not support URL filtering.

**User Agent Status Monitor**
This module alerts when heartbeats are not detected for any User Agents connected to the Defense Center.

This module only runs on Defense Centers.

**VPN Status**
This module alerts when the system detects that the VPN feature is not functioning.

This module only runs on Defense Centers.

### Table 68-1 Health Modules (continued)

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Usage</td>
<td>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.</td>
</tr>
<tr>
<td>Power Supply</td>
<td>This module determines if power supplies on the device require replacement and alerts based on the power supply status.</td>
</tr>
<tr>
<td></td>
<td>This module runs on these Defense Centers: DC1500, DC2000, DC3500, DC4000.</td>
</tr>
<tr>
<td></td>
<td>This module runs on these devices: 3D3500, 3D4500, 3D6500, 3D9900, and Series 3.</td>
</tr>
<tr>
<td>Process Status</td>
<td>This module determines if processes on the appliance exit or terminate outside of the process manager.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Reconfiguring Detection</td>
<td>This module determines if detection capabilities persist after a failed policy apply on a registered managed device.</td>
</tr>
<tr>
<td></td>
<td>If detection capabilities appear un-operational after a policy apply fails, the module generates health alerts until detection capabilities are reestablished.</td>
</tr>
<tr>
<td>RRD Server Process</td>
<td>This module determines if the round robin data server that stores time series data is running properly and alerts based on the number of recent RRD server restarts.</td>
</tr>
<tr>
<td></td>
<td>This module only runs on Defense Centers.</td>
</tr>
<tr>
<td>Security Intelligence</td>
<td>This module alerts in a variety of situations involving Security Intelligence filtering, including feed update, feed corruption, and memory issues.</td>
</tr>
<tr>
<td></td>
<td>This module runs on all Defense Centers except the DC500, which does not support Security Intelligence filtering.</td>
</tr>
<tr>
<td>Time Series Data Monitor</td>
<td>This module tracks the presence of corrupt files in the directory where time series data (such as compliance event counts) are stored and alerts when files are flagged as corrupt and removed.</td>
</tr>
<tr>
<td></td>
<td>This module only runs on Defense Centers.</td>
</tr>
<tr>
<td>Time Synchronization Status</td>
<td>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.</td>
</tr>
<tr>
<td>URL Filtering Monitor</td>
<td>This module tracks communication between the Defense Center and the Cisco cloud, where the system obtains its URL filtering (category and reputation) data for commonly visited URLs. The module alerts if the Defense Center fails to successfully communicate with or retrieve an update from the cloud.</td>
</tr>
<tr>
<td></td>
<td>This module also tracks communications between the Defense Center and any managed devices where you have enabled URL filtering. The module alerts if the Defense Center cannot push URL filtering data to those devices.</td>
</tr>
<tr>
<td></td>
<td>This module only runs on all Defense Centers except the DC500, which does not support URL filtering.</td>
</tr>
<tr>
<td>User Agent Status Monitor</td>
<td>This module alerts when heartbeats are not detected for any User Agents connected to the Defense Center.</td>
</tr>
<tr>
<td></td>
<td>This module only runs on Defense Centers.</td>
</tr>
<tr>
<td>VPN Status</td>
<td>This module alerts when the system detects that the VPN feature is not functioning.</td>
</tr>
<tr>
<td></td>
<td>This module only runs on Defense Centers.</td>
</tr>
</tbody>
</table>
Understanding Health Monitoring Configuration

**License:** Any

There are several steps to setting up health monitoring on your FireSIGHT System, as indicated in the following procedure:

---

**Step 1** Create health policies for your appliances.

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

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

For more information on setting up health policies, see Configuring Health Policies, page 68-6.

**Step 2** Apply a health policy to each appliance where you want to track health status. For information on the default health policy available for immediate application, see Understanding the Default Health Policy, page 68-7.

**Step 3** Optionally, configure health monitor alerts.

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.

For more information on setting up health monitor alerts, see Configuring Health Monitor Alerts, page 68-37.

---

After you set up health monitoring on your system, you can view the health status at any time on the Health Monitor page or the Health Events table view. For more information about viewing system health data, see the following topics:

- Using the Health Monitor, page 68-39
- Using Appliance Health Monitors, page 68-41
- Working with Health Events, page 68-46

Configuring Health Policies

**License:** Any

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. For more information on the health modules you can configure in a health policy, see Understanding Health Monitoring, page 68-1.

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. You can also import a health policy exported from another Defense Center.

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.
For more information on the default health policy, which is applied to the Defense Center automatically, see *Understanding the Default Health Policy*, page 68-7.

For more information, see the following topics:
- *Understanding the Default Health Policy*, page 68-7
- *Creating Health Policies*, page 68-8
- *Applying Health Policies*, page 68-28
- *Editing Health Policies*, page 68-29
- *Comparing Health Policies*, page 68-31
- *Deleting Health Policies*, page 68-33

**Understanding the Default Health Policy**

*License:* Any

The Defense Center health monitor includes a default health policy to make it easier for you to quickly implement health monitoring for your appliances. The default health policy is automatically applied to the Defense Center. You cannot edit the default health policy, but you can copy it to create custom policies based on its configuration. For more information, see *Creating Health Policies*, page 68-8.

To also monitor device health, you can push health policies to your managed devices.

---

**Note**

You cannot apply a health policy to Cisco NGIPS for Blue Coat X-Series.

In the default health policy, most of the health modules available on the running platform are automatically enabled. The following table details the modules activated in the default policy for Defense Centers and managed devices.

**Table 68-2**  
*Default Active Health Modules*

<table>
<thead>
<tr>
<th>Module</th>
<th>Defense Center</th>
<th>Managed Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Malware Protection</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Appliance Heartbeat</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Automatic Application Bypass</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Card Reset</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Disk Status</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>FireAMP Status Monitor</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>FireSIGHT Host License Limit</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Hardware Alarm</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Health Monitor Process</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Inline Link Mismatch Alarms</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Interface Status</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>
Creating Health Policies

License: Any

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 select 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.

Tip

Instead of creating a new policy, you can export a health policy from another Defense Center and then import it onto your Defense Center. You can then edit the imported policy to suit your needs before you apply it. For more information, see Importing and Exporting Configurations, page A-1.

To create a health policy:

Access: Admin/Maint

Step 1 Select Health > Health Policy.

The Health Policy page appears.

Step 2 Click Create Policy.

The Create Health Policy page appears.

Step 3 Select 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.
Configuring Health Policies

Step 5 Enter a description for the policy.

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

The Health Policy Configuration page appears, including a list of the modules.

Step 7 Configure settings on each module you want to use to test the health status of your appliances, as described in the following sections:

- Configuring Policy Run Time Intervals, page 68-10
- Configuring Advanced Malware Protection Monitoring, page 68-10
- Configuring Appliance Heartbeat Monitoring, page 68-11
- Configuring Automatic Application Bypass Monitoring, page 68-12
- Configuring CPU Usage Monitoring, page 68-12
- Configuring Card Reset Monitoring, page 68-13
- Configuring Disk Status Monitoring, page 68-13
- Configuring Disk Usage Monitoring, page 68-14
- Configuring FireAMP Status Monitoring, page 68-15
- Configuring FireSIGHT Host Usage Monitoring, page 68-16
- Configuring Hardware Alarm Monitoring, page 68-16
- Configuring Health Status Monitoring, page 68-17
- Configuring Inline Link Mismatch Alarm Monitoring, page 68-18
- Configuring Interface Status Monitoring, page 68-18
- Configuring Intrusion Event Rate Monitoring, page 68-19
- Understanding License Monitoring, page 68-20
- Configuring Link State Propagation Monitoring, page 68-20
- Configuring Memory Usage Monitoring, page 68-21
- Configuring Power Supply Monitoring, page 68-22
- Configuring Process Status Monitoring, page 68-22
- Configuring Reconfiguring Detection Monitoring, page 68-23
- Configuring RRD Server Process Monitoring, page 68-24
- Configuring Security Intelligence Monitoring, page 68-24
- Configuring Time Series Data Monitoring, page 68-25
- Configuring Time Synchronization Monitoring, page 68-26
- Configuring URL Filtering Monitoring, page 68-26
- Configuring User Agent Status Monitoring, page 68-27
- Configuring VPN Status Monitoring, page 68-27

**Note**

Make sure you enable each module that you want to run to test the health status on each Health Policy Configuration page as you configure the settings. Disabled modules do not produce health status feedback, even if the policy that contains the module has been applied to an appliance.

Step 8 Click **Save Policy and Exit** to save the policy.
You must apply the policy to each appliance for it to take effect. For more information on applying health policies, see Applying Health Policies, page 68-28.

### Configuring Policy Run Time Intervals

**License:** Any

You can control how often health tests run by modifying the Policy Run Time Interval for the health policy. The maximum run time interval you can set is 99999 minutes.

⚠️ **Caution**

Do not set a run interval of less than five minutes.

**To configure a policy run time interval:**

**Access:** Admin/Maint

**Step 1**

On the Health Policy Configuration page, select Policy Run Time Interval.

The Health Policy Configuration — Policy Run Time Interval page appears.

**Step 2**

In the Run Interval (mins) field, enter the time in minutes that you want to elapse between automatic repetitions of the test.

**Step 3**

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, select 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.

You must apply the health policy to the appropriate appliances if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

### Configuring Advanced Malware Protection Monitoring

**License:** Malware

This module tracks the state and stability of the Defense Center’s ability to query the Cisco cloud and detect files in network traffic. If the system detects that your connection with the cloud is interrupted, the encryption keys used for the connection are invalid, or the number of files detected in a time frame is excessive, the status classification for this module changes to Warning and the module generates a health alert. Note that if you are using a FireAMP Private Cloud and it is unable to communicate with the public Cisco cloud, the private cloud itself generates an alert; for more information, see the FireAMP Private Cloud Administration Portal User Guide.

⚠️ **Note**

If your Defense Center loses connectivity to the Internet, the system may take up to 30 minutes to generate an Advanced Malware Protection health alert.
To configure Advanced Malware Protection health module settings:

Access: Admin/Maint

Step 1
In the Health Policy Configuration page, select Advanced Malware Protection.
The Health Policy Configuration — Advanced Malware Protection page appears.

Step 2
Select On for the Enabled option to enable use of the module for health status testing.

Step 3
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, select 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.

You must apply the health policy to the appropriate appliances if you want your settings to take effect.
See Applying Health Policies, page 68-28 for more information.

Configuring Appliance Heartbeat Monitoring

License: Any

The Defense Center receives heartbeats from its managed devices once every two minutes or every 200 events, whichever comes first, as an indicator that the device is running and communicating properly with the Defense Center. Use the Appliance Heartbeat health status module to track whether the Defense Center receives heartbeats from managed appliances. If the Defense Center does not detect a heartbeat from a device, the status classification for this module changes to Critical. That status data feeds into the health monitor.

To configure Appliance Heartbeat health module settings:

Access: Admin/Maint

Step 1
In the Health Policy Configuration page, select Appliance Heartbeat.
The Health Policy Configuration — Appliance Heartbeat page appears.

Step 2
Select On for the Enabled option to enable use of the module for health status testing.

Step 3
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, select 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.

You must apply the health policy to the appropriate appliances if you want your settings to take effect.
See Applying Health Policies, page 68-28 for more information.
Configuring Automatic Application Bypass Monitoring

License: Any

Use this module to detect when a managed device is bypassed because it did not respond within the number of seconds configured as the bypass threshold. If a bypass occurs, this module generates an alert. That status data feeds into the health monitor.

For more information on automatic application bypass, see Automatic Application Bypass, page 4-54.

To configure automatic application bypass monitoring status:

Access: Admin/Maint

Step 1 In the Health Policy Configuration page, select Automatic Application Bypass Status.

The Health Policy Configuration — Automatic Application Bypass Status page appears.

Step 2 Select On for the Enabled option to enable use of the module for health status testing.

Step 3 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, select 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.

You must apply the health policy to the appropriate managed device if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

Configuring CPU Usage Monitoring

License: Any

Supported Devices: Any except 3D9900

Supported Defense Centers: Any

Excessive CPU usage may indicate that you need to upgrade your hardware or that there are processes that are not functioning correctly. Use the CPU Usage health status module to set CPU usage limits.

If the CPU usage on the monitored appliance exceeds the Warning limit, the status classification for that module changes to Warning. If the CPU usage on the monitored appliance exceeds the Critical limit, the status classification for that module changes to Critical. That status data feeds into the health monitor.

The maximum percentage you can set for either limit is 100 percent, and the Critical limit must be higher than the Warning limit.

To configure CPU usage limits:

Access: Admin/Maint

Step 1 On the Health Policy Configuration page, select CPU Usage.

The Health Policy Configuration — CPU Usage page appears.

Step 2 Select On for the Enabled option to enable use of the module for health status testing.
### Configuring Health Policies

**Step 3**
In the **Critical Threshold %** field, enter the percentage of CPU usage that should trigger a critical health status.

**Step 4**
In the **Warning Threshold %** field, enter the percentage of CPU usage that should trigger a warning health status.

**Step 5**
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, select 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.

You must apply the health policy to the appropriate appliances if you want your settings to take effect. See **Applying Health Policies**, page 68-28 for more information.

---

### Configuring Card Reset Monitoring

**License:** Any

Use the card reset monitoring health status module to track when the network card restarts because of hardware failure. If a reset occurs, this module generates an alert. That status data feeds into the health monitor.

**To configure card reset monitoring:**

**Access:** Admin/Maint

**Step 1**
In the Health Policy Configuration page, select **Card Reset**.

The Health Policy Configuration — Card Reset Monitoring page appears.

**Step 2**
Select **On** for the **Enabled** option to enable use of the module for health status testing.

**Step 3**
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, select 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.

You must apply the health policy to the appropriate Defense Center if you want your settings to take effect. See **Applying Health Policies**, page 68-28 for more information.

---

### Configuring Disk Status Monitoring

**License:** Any
Configuring Health Policies

Use the Disk Status health module to monitor the current status of your appliance’s hard disk, and malware storage pack if installed. 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.

To configure Disk Status health module settings:
Access: Admin/Maint

Step 1
On the Health Policy Configuration page, click Disk Status.
The Health Policy Configuration — Disk Status page appears.

Step 2
Select On for the Enabled option to enable use of the module for health status testing.

Step 3
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, select 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.

You must apply the health policy to the appropriate devices if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

Configuring Disk Usage Monitoring

License: Any

Without sufficient disk space, an appliance cannot run. The health monitor can identify low disk space conditions on your appliance’s hard drive and malware storage pack before space runs out. The health monitor can also alert when hard drive file draining occurs too frequently. Use the Disk Usage health status module to monitor disk usage for the / and /volume partitions on the appliance and track draining frequency.

Note
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.

If the overall disk usage on the monitored appliance exceeds the Warning limit, the status classification for that module changes to Warning. If the overall disk usage on the monitored appliance exceeds the Critical limit, the status classification for that module changes to Critical. The maximum percentage you can set for either limit is 100 percent, and the Critical limit must be higher than the Warning limit.

If the system deletes unprocessed events, the status classification for that module changes to Warning. If the system drains files in any disk usage category too frequently based on module thresholds, or if disk usage for files not in a monitored disk usage category grows too large based on module thresholds, the status classification for that module changes to Critical. For more information on disk usage categories, see Understanding the Disk Usage Widget, page 55-26.

To configure Disk Usage health module settings:
Access: Admin/Maint
Configuring Health Policies

**Step 1**
On the Health Policy Configuration page, select **Disk Usage**.
The Health Policy Configuration — Disk Usage page appears.

**Step 2**
Select **On** for the **Enabled** option to enable use of the module for health status testing.

**Step 3**
In the **Critical Threshold %** field, enter the percentage of disk usage that should trigger a critical health status.

**Step 4**
In the **Warning Threshold %** field, enter the percentage of disk usage that should trigger a warning health status.

**Step 5**
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, select 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.

You must apply the health policy to the appropriate appliances if you want your settings to take effect. See **Applying Health Policies**, page 68-28 for more information.

---

**Configuring FireAMP Status Monitoring**

**License:** Any
Use the FireAMP Status Monitor module to alert you in the following situations:
- the Defense Center cannot connect to the Cisco cloud after an initial successful connection
- you deregister a cloud connection using the FireAMP portal
- your FireAMP Private Cloud is unable to communicate with the public Cisco cloud

In these cases, the module status changes to Critical and provides the cloud name associated with the failed connection. For information on configuring a cloud connection, see **Working with Cloud Connections for FireAMP**, page 37-24.

To configure FireAMP Status Monitor module settings:
- **Access:** Admin/Maint

**Step 1**
In the Health Policy Configuration page, select **FireAMP Status Monitor**.
The Health Policy Configuration — FireAMP Status Monitor page appears.

**Step 2**
Select **On** for the **Enabled** option to enable use of the module for FireAMP status monitoring.

**Step 3**
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, select 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.
You must apply the health policy to the Defense Center if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

Configuring FireSIGHT Host Usage Monitoring

License: FireSIGHT

Use the FireSIGHT Host License Limit health status module to set FireSIGHT Host amount warning limits. If the number of remaining FireSIGHT Hosts on the monitored device falls below the Warning Hosts limit, the status classification for that module changes to Warning. If the number of remaining FireSIGHT Hosts on the monitored device falls below the Critical Hosts limit, the status classification for that module changes to Critical. That status data feeds into the health monitor.

The maximum number of hosts you can set for either limit is 1000, and the Critical host limit number must be lower than the Warning limit.

To configure FireSIGHT Host License Limit health module settings:

Access: Admin/Maint

Step 1 In the Health Policy Configuration page, select FireSIGHT Host License Limit.

The Health Policy Configuration — FireSIGHT Host License Limit page appears.

Step 2 Select On for the Enabled option to enable use of the module for health status testing.

Step 3 In the Critical number Hosts field, enter the remaining number of available hosts that should trigger a critical health status.

Step 4 In the Warning number Hosts field, enter the remaining number of available hosts that should trigger a warning health status.

Step 5 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, select 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.

You must apply the health policy to the appropriate devices if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

Configuring Hardware Alarm Monitoring

License: Any

Supported Devices: Series 3, 3D9900

Use the Hardware Alarms health status module to detect hardware failure on a Series 3 or 3D9900 device. If the Hardware Alarms module finds a hardware component that has failed or clustered devices that are not communicating with each other, the status classification for that module changes to Critical. That status data feeds into the health monitor.
For more information on the hardware status conditions that can cause hardware alerts on 3D9900 devices, see Interpreting Hardware Alert Details for 3D9900 Devices, page 68-49.

**To configure Hardware Alarm health module settings:**

**Access:** Admin/Maint

**Step 1**
In the Health Policy Configuration page, select **Hardware Alarms**.

The Health Policy Configuration — Hardware Alarm Monitor page appears.

**Step 2**
Select **On** for the **Enabled** option to enable use of the module for health status testing.

**Step 3**
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, select 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.

You must apply the health policy to the appropriate devices if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

---

**Configuring Health Status Monitoring**

**License:** Any

Use the Health Monitor Process module to monitor the health of the health monitor on a Defense Center by generating alerts when too many minutes elapse between health events received from monitored appliances.

For example, if a Defense Center (myrtle.example.com) monitors a device (dogwood.example.com), you apply a health policy with the Health Monitor Process module enabled to myrtle.example.com. The Health Monitor Process module then reports events that indicate how many minutes have elapsed since the last event was received from dogwood.example.com.

You can configure the elapsed duration between events, in minutes, that causes an alert to be generated. If the wait exceeds the number of minutes configured in the Warning Minutes since last event limit, the status classification for that module changes to Warning. If the wait exceeds the Critical Minutes since last event limit, the status classification for that module changes to Critical. That status data feeds into the health monitor.

The maximum number of minutes you can set for either limit is 144, and the Critical limit must be higher than the Warning limit. The minimum number of minutes is 5.

**To configure Health Monitor Process module settings:**

**Access:** Admin/Maint

**Step 1**
In the Health Policy Configuration page, select **Health Monitor Process**.

The Health Policy Configuration — Health Monitor Process page appears.

**Step 2**
Select **On** for the **Enabled** option to enable use of the module for health status testing.
Step 3  In the **Critical Minutes since last event** field, enter the maximum number of minutes to wait between events, before triggering a critical health status.

Step 4  In the **Warning Minutes since last event** field, enter the maximum number of minutes to wait between events, before triggering a warning health status.

Step 5  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, select 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.

You must apply the health policy to the Defense Center for your settings to take effect. See **Applying Health Policies**, page 68-28 for more information.

### Configuring Inline Link Mismatch Alarm Monitoring

**License:** Any

Use the Inline Link Mismatch Alarm health status module to track when the interfaces on either side of an inline set negotiate different connection speeds. If different negotiated speeds are detected, this module generates an alert.

**To configure inline link mismatch monitoring:**

**Access:** Admin/Maint

---

**Step 1**  In the Health Policy Configuration page, select **Inline Link Mismatch Alarms**.

The Health Policy Configuration — Inline Link Mismatch Alarms page appears.

**Step 2**  Select **On** for the **Enabled** option to enable use of the module for health status testing.

**Step 3**  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, select 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.

You must apply the health policy to the appropriate Defense Center if you want your settings to take effect. See **Applying Health Policies**, page 68-28 for more information.

---

### Configuring Interface Status Monitoring

**License:** FireSIGHT

Use the Interface Status health status module to detect whether a device receives traffic. If the Interface Status module determines that a device does not receive traffic, the status classification for that module changes to Critical. That status data feeds into the health monitor.
Interfaces labeled DataPlaneInterface{x}, where \( x \) is a numerical value, are internal ASA interfaces (not user-defined) and involve packet flow within the system.

To configure Interface Status health module settings:

Access: Admin/Maint

Step 1
In the Health Policy Configuration page, select Interface Status.
The Health Policy Configuration — Interface Status page appears.

Step 2
Select On for the Enabled option to enable use of the module for health status testing.

Step 3
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, select 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.

You must apply the health policy to the appropriate devices if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

Configuring Intrusion Event Rate Monitoring

License: Protection

Use the Intrusion Event Rate health status module to set limits for the number of packets per second that trigger a change in the health status. If the event rate on the monitored device exceeds the number of events per second configured in the Events per second (Warning) limit, the status classification for that module changes to Warning. If the event rate exceeds the number of events per second configured in the Events per second (Critical) limit, the status classification for that module changes to Critical. That status data feeds into the health monitor.

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.

To configure Intrusion Event Rate Monitor health module settings:

Access: Admin/Maint

Step 1
On the Health Policy Configuration page, select Intrusion Event Rate.
The Health Policy Configuration — Intrusion Event Rate page appears.
**Step 2** Select **On** for the **Enabled** option to enable use of the module for health status testing.

**Step 3** In the **Events per second (Critical)** field, enter the number of events per second that should trigger a critical health status.

**Step 4** In the **Events per second (Warning)** field, enter the number of events per second that should trigger a warning health status.

**Step 5** 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, select 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.

You must apply the health policy to the appropriate devices if you want your settings to take effect. See **Applying Health Policies, page 68-28** for more information.

---

**Understanding License Monitoring**

**License**: Any

Use the License Monitoring health status module to determine if sufficient licenses remain for Control, Protection, URL Filtering, Malware, and VPN. This module alerts if the number of remaining licenses is low or insufficient.

This module also alerts if the system detects that devices in a stacked configuration have mismatched license sets (stacked devices must have identical sets of licenses).

The License Monitoring module is automatically configured. Because you cannot change or disable this module, it does not appear on the Health Policy Configuration page.

**Configuring Link State Propagation Monitoring**

**License**: Any

Use the Link State Propagation health status module to detect the link state propagation status on an inline pair. 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.

**To configure Link State Propagation health module settings:**

**Access**: Admin/Maint

**Step 1** On the Health Policy Configuration page, select **Link State Propagation**.

The Health Policy Configuration — Link State Propagation monitor page appears.

**Step 2** Select **On** for the **Enabled** option to enable use of the module for health status testing.

**Step 3** 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, select 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.

You must apply the health policy to the appropriate devices if you want your settings to take effect. See **Applying Health Policies, page 68-28** for more information.

---

### Configuring Memory Usage Monitoring

**License:** Any

Use the Memory Usage health status module to set memory usage limits. The module calculates free memory by considering free memory, cached memory, and swap memory. If the memory usage on the monitored appliance exceeds the Warning limit, the status classification for that module changes to Warning. If the memory usage on the monitored appliance exceeds the Critical limit, the status classification for that module changes to Critical. That status data feeds into the health monitor.

For appliances with more than 4GB of memory, the preset alert thresholds are based on a formula that accounts for proportions of available memory likely to cause system problems.

**Note**

On <4GB appliances, because the interval between Warning and Critical thresholds may be very narrow, Cisco recommends that you manually set the **Warning Threshold %** value to 50. This will further ensure that you receive memory alerts for your appliance in time to address the issue.

The maximum percentage you can set for either limit is 100 percent, and the Critical limit must be higher than the Warning limit.

**Note**

If you apply an access control policy with many FireSIGHT features enabled (such as security intelligence, file capture, intrusion policies with many rules, or URL filtering), some lower-end ASA FirePOWER devices may generate intermittent memory usage warnings, as the device’s memory allocation is being used to the fullest extent possible.

**To configure Memory Usage health module settings:**

**Access:** Admin/Maint

---

**Step 1**

On the Health Policy Configuration page, select **Memory Usage**.

The Health Policy Configuration — Memory Usage page appears.

**Step 2**

Select **On** for the **Enabled** option to enable use of the module for health status testing.

**Step 3**

In the **Critical Threshold %** field, enter the percentage of memory usage that should trigger a critical health status.

**Step 4**

In the **Warning Threshold %** field, enter the percentage of memory usage that should trigger a warning health status.

**Step 5**

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**.

---
Configuring Health Policies

To temporarily save your changes to this module and switch to another module’s settings to modify, select 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.

You must apply the health policy to the appropriate appliances if you want your settings to take effect. See **Applying Health Policies**, page 68-28 for more information.

## Configuring Power Supply Monitoring

**License:** Any  
**Supported Devices:** 3D3500, 3D4500, 3D6500, 3D9900, Series 3  
**Supported Defense Centers:** DC1500, DC2000, DC3500, DC4000

Use the Power Supply health status module to detect a power supply failure on any of the supported platforms. If the module finds a power supply that has no power, the status classification for that module changes to No Power. If the module cannot detect the presence of the power supply, the status changes to Critical Error. That status data feeds into the health monitor. You can expand the Power Supply item on the Alert Detail list in the health monitor to see specific status items for each power supply.

**To configure Power Supply health module settings:**

**Access:** Admin/Maint

**Step 1**  
In the Health Policy Configuration page, select **Power Supply**.

The Health Policy Configuration — Power Supply page appears.

**Step 2**  
Select **On** for the **Enabled** option to enable use of the module for health status testing.

**Step 3**  
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, select 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.

You must apply the health policy to the appropriate devices if you want your settings to take effect. See **Applying Health Policies**, page 68-28 for more information.

## Configuring Process Status Monitoring

**License:** Any

Use the Process Status health module to monitor for processes running on the appliance that exit or terminate outside of the process manager. The response of the Process Status module to a process ending depends on how the process ends:

- If the process terminates inside the process manager, the module does not report any health events.
- 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.

**To configure Process Status health module settings:**

**Access:** Admin/Maint

---

**Step 1**
In the Health Policy Configuration page, select Process Status.

The Health Policy Configuration — Process Status page appears.

**Step 2**
Select On for the Enabled option to enable use of the module for health status testing.

**Step 3**
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, select 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.

You must apply the health policy to the appropriate appliances if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

---

**Configuring Reconfiguring Detection Monitoring**

**License:** Any

Use the Reconfiguring Detection Monitor module to determine the status of detection capabilities after applying a policy to your managed devices. If a policy apply fails and detection ceases functionality, the module generates an alert in Health Events.

**To configure time series data monitoring settings:**

**Access:** Admin/Maint

---

**Step 1**
In the Health Policy Configuration page, select Reconfiguring Detection.

The Health Policy Configuration — Reconfiguring Detection page appears.

**Step 2**
Select On for the Enabled option to enable use of the module for health alerts.

**Step 3**
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, select 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.

You must apply the health policy to the appropriate devices if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.
Configuring RRD Server Process Monitoring

License: Any

Use the RRD Server Process module to see if the RRD server that stores time series data is working 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.

To configure RRD server process monitoring settings:
Access: Admin/Maint

Step 1
In the Health Policy Configuration page, select RRD Server Process.
The Health Policy Configuration — RRD Server Process page appears.

Step 2
Select On for the Enabled option to enable use of the module for health status testing.

Step 3
In the Critical Number of restarts field, enter the number of consecutive detected RRD server resets that should trigger a critical health status.

Step 4
In the Warning Number of restarts field, enter the number of consecutive detected RRD server resets that should trigger a warning health status.

Step 5
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, select 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.

You must apply the health policy to the appropriate devices if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

Configuring Security Intelligence Monitoring

License: Protection

Supported Defense Centers: Any except DC500

Use the Security Intelligence module to warn you in a variety of situations involving Security Intelligence filtering. The module alerts if Security Intelligence is in use and:

- the Defense Center cannot update a feed, or if feed data is corrupt or contains no recognizable IP addresses
- a managed device had a problem receiving updated Security Intelligence data from the Defense Center
- a managed device cannot load all of the Security Intelligence data provided to it by the Defense Center, due to memory issues
If a Security Intelligence memory warning appears in the health monitor, you can reapply the affected device’s access control policy to increase the memory allocated to Security Intelligence; see Applying an Access Control Policy, page 12-15.

For more information on Security Intelligence filtering, see Blacklisting Using Security Intelligence IP Address Reputation, page 13-1 and Working with Security Intelligence Lists and Feeds, page 3-4.

To configure Security Intelligence module settings:
   Access: Admin/Maint

**Step 1**  
In the Health Policy Configuration page, select Security Intelligence.

The Health Policy Configuration — Security Intelligence page appears.

**Step 2**  
Select On for the Enabled option to enable use of the module for Security Intelligence monitoring.

**Step 3**  
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, select 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.

You must apply the health policy to the appropriate devices if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

### Configuring Time Series Data Monitoring

**License:** Any

Use the Time Series Data Monitor module to monitor the status of time series data (such as lists of compliance events) that your system has stored. This module scans your time series data storage directory for corrupt files. If the module finds corrupted data, it enters a Warning status and reports the names of all affected files.

To configure time series data monitoring settings:
   Access: Admin/Maint

**Step 1**  
In the Health Policy Configuration page, select Time Series Data Monitor.

The Health Policy Configuration — Time Series Data Monitor page appears.

**Step 2**  
Select On for the Enabled option to enable use of the module for health status testing.

**Step 3**  
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, select 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.
You must apply the health policy to the appropriate devices if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

### Configuring Time Synchronization Monitoring

**License:** Any

Use the Time Synchronization Status module to detect when the time on a managed device that uses NTP to obtain time from an NTP server differs by 10 seconds or more from the time on the server.

**To configure time synchronization monitoring settings:**

**Access:** Admin/Maint

**Step 1**

In the Health Policy Configuration page, select **Time Synchronization Status**.

The Health Policy Configuration — Time Synchronization Status page appears.

**Step 2**

Select **On** for the **Enabled** option to enable use of the module for health status testing.

**Step 3**

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, select 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.

You must apply the health policy to the appropriate devices if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

### Configuring URL Filtering Monitoring

**License:** URL Filtering

**Supported Defense Centers:** Any except DC500

Use the URL Filtering Monitor module to track communications between the Defense Center and the Cisco cloud, where the system obtains its URL filtering (category and reputation) data for commonly visited URLs. If the Defense Center fails to successfully communicate with or retrieve an update from the cloud, the status classification for that module changes to Critical.

In a high availability configuration, only the primary Defense Center communicates with the URL filtering cloud; all data from this module refers only to that primary appliance.

The URL Filtering Monitor module also tracks communications between the Defense Center and any managed devices where you have enabled URL filtering. If the Defense Center is successfully communicating with the cloud, the module status changes to Warning if the Defense Center cannot push new URL filtering data to its managed devices.

**To configure URL Filtering Monitor health module settings:**

**Access:** Admin/Maint
Chapter 68      Using Health Monitoring

Configuring Health Policies

Step 1 In the Health Policy Configuration page, select URL Filtering Monitor.
The Health Policy Configuration — URL Filtering Monitor page appears.

Step 2 Select On for the Enabled option to enable use of the module for health status testing.

Step 3 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, select 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.

You must apply the health policy to the Defense Center if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

Configuring User Agent Status Monitoring

License: FireSIGHT

You can use the User Agent Status Monitor health module to monitor the heartbeat of agents connected to a Defense Center. If you enable the module in an applied health policy, the module generates a health alert if the Defense Center does not detect a heartbeat for any agent configured on the Defense Center.

To configure User Agent Status Monitor health module settings:

Access: Admin/Maint

Step 1 In the Health Policy Configuration page, select User Agent Status Monitor.
The Health Policy Configuration — User Agent Status Monitor page appears.

Step 2 Select On for the Enabled option to enable use of the module for health status testing.

Step 3 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, select 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.

You must apply the health policy to the Defense Center if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

Configuring VPN Status Monitoring

License: VPN

Supported Defense Centers: Any except Series 2
Use the VPN Status health module to monitor the current status of your configured Gateway VPN tunnels; information for each individual tunnel is displayed. This module generates a Critical (red) health alert when any of your VPN tunnels is not working.

To configure VPN Status health module settings:

Access: Admin/Maint

Step 1

On the Health Policy Configuration page, click VPN Status.
The Health Policy Configuration — VPN Status page appears.

Step 2

Select On for the Enabled option to enable use of the module for health status testing.

Step 3

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, select 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.

You must apply the health policy to the appropriate devices if you want your settings to take effect. See Applying Health Policies, page 68-28 for more information.

### Applying Health Policies

**License:** Any

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 Defense 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.

**Note**

Custom health policies created on Defense Centers in a high availability pair will be replicated between both appliances. However, changes to default health policies are not replicated; each appliance uses the local default health policy configured for that appliance.

To apply a health policy:

Access: Admin/Maint

Step 1

Select Health > Health Policy.
The Health Policy page appears.
Step 2 Click the apply icon (✓) next to the policy you want to apply.
The Health Policy Apply page appears.

Tip The status icon (✓) next to the Health Policy column indicates the current health status for the appliance.

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

Step 4 Click Apply to apply the policy to the selected appliances.
The Health Policy page appears, with a message indicating if the application of the policy was successful. Monitoring of the appliance starts as soon as the policy is successfully applied.

Editing Health Policies

License: Any

You can modify a health policy by enabling or disabling modules or by changing module settings. If you modify a policy that is already applied to an appliance, the changes do not take effect until you reapply the policy.

Applicable health models for various appliances are listed in the following table.

<table>
<thead>
<tr>
<th>Module</th>
<th>Applicable Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Malware Protection</td>
<td>Defense Centers, except DC500</td>
</tr>
<tr>
<td>Appliance Heartbeat</td>
<td>Defense Center</td>
</tr>
<tr>
<td>Automatic Application Bypass Status</td>
<td>Any managed device</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>Any except 3D9900</td>
</tr>
<tr>
<td>Card Reset</td>
<td>Any managed device</td>
</tr>
<tr>
<td>Disk Status</td>
<td>Any</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>Any</td>
</tr>
<tr>
<td>FireAMP Status Monitor</td>
<td>Defense Center</td>
</tr>
<tr>
<td>FireSIGHT Host License Limit</td>
<td>Defense Center</td>
</tr>
<tr>
<td>Hardware Alarms</td>
<td>Series 3, 3D9900</td>
</tr>
<tr>
<td>Health Monitor Process</td>
<td>Defense Center</td>
</tr>
<tr>
<td>Inline Link Mismatch Alarms</td>
<td>Any managed device</td>
</tr>
<tr>
<td>Interface Status</td>
<td>Any managed device</td>
</tr>
<tr>
<td>Intrusion Event Rate</td>
<td>Managed devices with Protection</td>
</tr>
<tr>
<td>License Monitor</td>
<td>Defense Center</td>
</tr>
<tr>
<td>Link State Propagation</td>
<td>Managed devices with Protection</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>Any</td>
</tr>
</tbody>
</table>
Table 68-3  Health Modules Applicable to Appliances (continued)

<table>
<thead>
<tr>
<th>Module</th>
<th>Applicable Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply</td>
<td>Defense Centers: DC1500, DC2000, DC3500, DC4000 Devices: 3D3500, 3D4500, 3D6500, 3D9900, Series 3</td>
</tr>
<tr>
<td>Process Status</td>
<td>Any</td>
</tr>
<tr>
<td>Reconfiguring Detection</td>
<td>Any</td>
</tr>
<tr>
<td>RRD Server Process</td>
<td>Defense Center</td>
</tr>
<tr>
<td>Security Intelligence</td>
<td>Defense Center, except DC500</td>
</tr>
<tr>
<td>Time Series Data Monitor</td>
<td>Defense Center</td>
</tr>
<tr>
<td>Time Synchronization Status</td>
<td>Any</td>
</tr>
<tr>
<td>URL Filtering Monitor</td>
<td>Defense Centers, except DC500</td>
</tr>
<tr>
<td>User Agent Status Monitor</td>
<td>Defense Center</td>
</tr>
<tr>
<td>VPN Status</td>
<td>Defense Center</td>
</tr>
</tbody>
</table>

To edit a health policy:

Access: Admin/Maint

---

**Step 1** Select Health > Health Policy.

The Health Policy page appears.

**Step 2** Click the edit icon (🛠️) next to the policy you want to modify.

The Health Policy Configuration page appears, with the Policy Run Time Interval settings selected.

**Step 3** Modify settings as needed, as described in the following sections:

- Configuring Policy Run Time Intervals, page 68-10
- Configuring Advanced Malware Protection Monitoring, page 68-10
- Configuring Appliance Heartbeat Monitoring, page 68-11
- Configuring Automatic Application Bypass Monitoring, page 68-12
- Configuring CPU Usage Monitoring, page 68-12
- Configuring Card Reset Monitoring, page 68-13
- Configuring Disk Status Monitoring, page 68-13
- Configuring Disk Usage Monitoring, page 68-14
- Configuring FireAMP Status Monitoring, page 68-15
- Configuring FireSIGHT Host Usage Monitoring, page 68-16
- Configuring Hardware Alarm Monitoring, page 68-16
- Configuring Health Status Monitoring, page 68-17
- Configuring Inline Link Mismatch Alarm Monitoring, page 68-18
- Configuring Interface Status Monitoring
- Configuring Intrusion Event Rate Monitoring, page 68-19
Comparing Health Policies

License: Any

To review policy changes for compliance with your organization’s standards or to optimize health monitoring performance, you can examine the differences between two health policies. You can compare any two health policies or two revisions of the same health policy, for the health policies you can access. To quickly compare your active health policy to another, you can select the Running Configuration option. Optionally, after you compare, you can then generate a PDF report to record the differences between the two policies or policy revisions.

There are two tools you can use to compare health policies or health policy revisions:

- The comparison view displays only the differences between two health policies or health policy revisions in a side-by-side format; the name of each policy or policy revision appears in the title bar on the left and right sides of the comparison view. You can use this to view and navigate both policy revisions on the web interface, with their differences highlighted.

- The comparison report creates a record of only the differences between two health policies or health policy revisions in a format similar to the health policy report, but in PDF format. You can use this to save, copy, print and share your policy comparisons for further examination.

For more information on understanding and using the health policy comparison tools, see: 

Step 4 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, select 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 5 Reapply the policy to the appropriate appliances as described in Applying Health Policies, page 68-28.
Using the Health Policy Comparison View

License: Any

The comparison view displays both health policies or policy revisions in a side-by-side format, with each policy or policy revision identified by name in the title bar on the left and right sides of the comparison view. The time of last modification and the last user to modify are displayed to the right of the policy name. Note that the Health Policy page displays the time a policy was last modified in local time, but the health policy report lists the time modified in UTC.

Differences between the two health policies or policy revisions are highlighted:

- Blue indicates that the highlighted setting is different in the two policies or policy revisions, and the difference is noted in red text.
- Green indicates that the highlighted setting appears in one policy or policy revision but not the other.

You can perform any of the actions in the following table.

<table>
<thead>
<tr>
<th>To...</th>
<th>You can...</th>
</tr>
</thead>
<tbody>
<tr>
<td>navigate individually through changes</td>
<td>click Previous or Next above the title bar. The double-arrow icon ( ) centered between the left and right sides moves, and the Difference number adjusts to identify which difference you are viewing.</td>
</tr>
<tr>
<td>generate a new health policy comparison view</td>
<td>click New Comparison. The Select Comparison window appears. See Using the Health Policy Comparison Report for more information.</td>
</tr>
<tr>
<td>generate a health policy comparison report</td>
<td>click Comparison Report. The health policy comparison report creates a PDF containing information identical to the comparison view.</td>
</tr>
</tbody>
</table>

Using the Health Policy Comparison Report

License: Any

A health policy comparison report is a record of all differences between two health policies or two revisions of the same health policy identified by the health policy comparison view, presented as a PDF. You can use this report to further examine the differences between two health policy configurations and to save and disseminate your findings.

You can generate a health policy comparison report from the comparison view for any health policies to which you have access. Remember to commit any potential changes before you generate a health policy report; only committed changes appear in the report.

Depending on your configuration, a health policy comparison report can contain one or more sections. Each section uses the same format and provides the same level of detail. Note that the Value A and Value B columns represent the policies or policy revisions you configured in the comparison view.
Tip
You can use a similar procedure to compare SSL, network analysis, intrusion, file, system, or access control policies.

To compare two health policies or two revisions of the same policy:

Access: Admin/Maint

Step 1
Select Health > Health Policy.
The Health Policy page appears.

Step 2
Click Compare Policies.
The Select Comparison window appears.

Step 3
From the Compare Against drop-down list, select the type of comparison you want to make:
- To compare two different policies, select Other Policy.
- To compare two revisions of the same policy, select Other Revision.
- To compare another policy to the currently active policy, select Running Configuration.
Remember to commit any changes before you generate a health policy report; only committed changes appear in the report.

Step 4
Depending on the comparison type you selected, you have the following choices:
- If you are comparing two different policies, select the policies you want to compare from the Policy A and Policy B drop-down lists.
- If you are comparing two revisions of the same policy, select the policy from the Policy drop-down list, then select the revisions you want to compare from the Revision A and Revision B drop-down lists.
- If you are comparing the running configuration to another policy, select the second policy from the Policy B drop-down list.

Step 5
Click OK to display the health policy comparison view.
The comparison view appears.

Step 6
Click Comparison Report to generate the health policy comparison report.
The health policy report appears. Depending on your browser settings, the report may appear in a pop-up window, or you may be prompted to save the report to your computer.

Deleting Health Policies

License: Any

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; see Enabling and Disabling Alert Responses, page 43-8.
Using the Health Monitor Blacklist

License: Any

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 Defense Center.

You can use the health monitor blacklist feature 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 Defense 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 blacklist, the events that were generated during the blacklisting continue to show a status of disabled.

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

At times it may be more practical to just blacklist an individual health monitoring module on an appliance. For example, when you run out of FireSIGHT host licenses on an appliance, you can blacklist the FireSIGHT Host License Limit status messages.

Note that on the main Health Monitor page you can distinguish between appliances that are blacklisted if you expand to view the list of appliances with a particular status by clicking the arrow in that status row. For more information on expanding that view, see Using the Health Monitor, page 68-39.

A blacklist icon (tiği) and a notation are visible after you expand the view for a blacklisted or partially blacklisted appliance.
Note

On a Defense Center, Health Monitor blacklist settings are local configuration settings. Therefore, if you blacklist a device, then delete it and later re-register it with the Defense Center, the blacklist settings remain persistent. The newly re-registered device remains blacklisted.

For more information, see:
- Blacklisting Health Policies or Appliances, page 68-35
- Blacklisting an Appliance, page 68-36
- Blacklisting a Health Policy Module, page 68-36

Blacklisting Health Policies or Appliances

License: Any

If you want to set health events to disabled for all appliances with a particular health policy, you can blacklist the policy. If you need to disable the results of a group of appliances’ health monitoring, you can blacklist the group of appliances. After the blacklist settings take effect, the appliance shows as disabled in the Health Monitor Appliance Module Summary and Device Management page. Health events for the appliance have a status of disabled.

Note that if your Defense Center is in a high availability configuration, you can blacklist a managed device on one high availability peer and not the other. You can also blacklist the high availability peer to cause it to mark events generated by it and the devices from which it receives health events as disabled. Defense Centers in a high availability pair have the option to completely or partially blacklist their peer.

To blacklist an entire health policy or group of appliances:

Access: Admin/Maint

Step 1

Select Health > Blacklist.

The Blacklist page appears.

Step 2

Use the drop-down list on the right to sort the list by group, policy, or model. (Groups on a Defense Center are managed devices.)

Note that appliances with some, but not all, health modules blacklisted will appear as (Partially Blacklisted). If you edit their blacklist status on the main blacklist page, you can either blacklist all modules on those appliances or remove all blacklisting. For information on blacklisting individual health modules on an appliance, see Blacklisting a Health Policy Module, page 68-36.

Tip

The status icon next to the Health Policy column (icons) indicates the current health status for the appliance. The status icon next to the System Policy column (icons) indicates the communication status between the Defense Center and the device.

Step 3

You have two options:

- To blacklist all appliances in a group, model, or policy category, select the category, then click Blacklist Selected Devices.
- To clear blacklisting from all appliances in a group, model, or policy category, select the category, then click Clear Blacklist on Selected Devices.
The page refreshes, now indicating the new blacklist state of the appliances.

---

**Blacklisting an Appliance**

**License:** Any

If you need to set the events and health status for an individual appliance to disabled, you can blacklist the appliance. After the blacklist 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.

**To blacklist an individual appliance:**

**Access:** Admin/Maint

---

**Step 1**  
Select Health > Blacklist.  
The Blacklist page appears.

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

**Step 3**  
You have two options:

- To blacklist all appliances in a group, model, or policy category, select the category, then click Blacklist Selected Devices.
- To clear blacklisting from all appliances in a group, model, or policy category, select the category, then click Clear Blacklist on Selected Devices.

The page refreshes and indicates the new blacklist state of the appliances. Click **Edit** and see **Blacklisting a Health Policy Module**, page 68-36 to blacklist individual health policy modules.

---

**Blacklisting a Health Policy Module**

**License:** Any

You can blacklist 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.

When any part of a module is blacklisted, the line for that module appears in boldface type in the Defense Center web interface.

**Tip**  
After the blacklist settings take effect, the appliance shows as **Partially Blacklisted** or **All Modules Blacklisted** on the Blacklist page and in the Appliance Health Monitor Module Status Summary, but only in expanded views on the main Appliance Status Summary page. Make sure that you keep track of individually blacklisted 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.

**To blacklist an individual health policy module:**

**Access:** Admin/Maint
Configuring Health Monitor Alerts

License: Any

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.

For more information, see the following topics:

- Creating Health Monitor Alerts, page 68-37
- Interpreting Health Monitor Alerts, page 68-38
- Editing Health Monitor Alerts, page 68-39
- Deleting Health Monitor Alerts, page 68-39

Creating Health Monitor Alerts

License: Any

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.

Note that 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.

To create health monitor alerts:

Access: Admin

Step 1 Select Health > Health Monitor Alerts.

The Health Monitor Alerts page appears.
Step 2  Type a name for the health alert in the **Health Alert Name** field.

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

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

Tip  To select multiple modules, press Shift + Ctrl and click the module names.

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

Tip  Click **Alerts** to open the Alerts page. For more information on creating alerts, see Working with Alert Responses, page 43-2.

Step 6  Optionally, in the **Threshold Timeout** field, type the number of minutes that should elapse before each threshold period ends and the threshold count resets. The default value is 5 minutes.

Note that 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, such that if the threshold timeout is 8 minutes and the policy run time interval is 5 minutes, there will be a 10-minute interval (5 x 2) between reported events.

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

A message appears, indicating if the alert configuration was successfully saved. The Active Health Alerts list now includes the alert you created.

---

### Interpreting Health Monitor Alerts

**License:** Any

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.

For more information on health alert severity levels, see the following table.

<table>
<thead>
<tr>
<th><strong>Severity</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>The health test results met the criteria to trigger a Critical alert status.</td>
</tr>
<tr>
<td>Warning</td>
<td>The health test results met the criteria to trigger a Warning alert status.</td>
</tr>
<tr>
<td>Normal</td>
<td>The health test results met the criteria to trigger a Normal alert status.</td>
</tr>
<tr>
<td>Error</td>
<td>The health test did not run.</td>
</tr>
<tr>
<td>Recovered</td>
<td>The health test results met the criteria to return to a normal alert status, following a Critical or Warning alert status.</td>
</tr>
</tbody>
</table>

For more information on health modules, see Understanding Health Modules, page 68-3.
Editing Health Monitor Alerts

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

To edit health monitor alerts:
Access: Admin

Step 1  Select Health > Health Monitor Alerts.
The Health Monitor Alerts page appears.
Step 2  Select the alert you want to modify in the Active Health Alerts list.
Step 3  Click Load to load the configured settings for the selected alert.
Step 4  Modify settings as needed. For more information, see Creating Health Monitor Alerts, page 68-37.
Step 5  Click Save to save the modified health alert.
A message appears, indicating if the alert configuration was successfully saved.

Deleting Health Monitor Alerts

License: Any
You can delete existing health monitor alerts.

Note Deleting a health monitor alert does not delete the associated alert response. You must disable or delete the underlying alert response to ensure that alerting does not continue. For more information, see Enabling and Disabling Alert Responses, page 43-8 and Deleting an Alert Response, page 43-8.

To delete health monitor alerts:
Access: Admin

Step 1  Select Health > Health Monitor Alerts.
The Health Monitor Alerts page appears.
Step 2  Select the alert you want to delete in the Active Health Alerts list.
Step 3  Click Delete.
A message appears, indicating if the alert configuration was successfully deleted.

Using the Health Monitor

License: Any
The Health Monitor page provides the compiled health status for all devices managed by the Defense Center, plus the Defense Center. The Status table provides a count of the managed appliances for this Defense Center by overall health status. The pie chart supplies another view of the health status breakdown, indicating the percentage of appliances currently in each health status category.

**To use the health monitor:**

**Access:** Admin/Maint/Any Security Analyst

---

**Step 1**

Click **Health > Health Monitor**.

The Health Monitor page appears.

**Step 2**

Select the appropriate status in the Status column of the table or the appropriate portion of the pie chart to the list appliances with that status.

---

**Tip**

If the arrow in the row for a status level points down, the appliance list for that status shows in the lower table. If the arrow points right, the appliance list is hidden.

The following topics provide details on the tasks you can perform from the Health Monitor page:

- Interpreting Health Monitor Status, page 68-40
- Using Appliance Health Monitors, page 68-41
- Configuring Health Policies, page 68-6
- Configuring Health Monitor Alerts, page 68-37

---

### Interpreting Health Monitor Status

**License:** Any

Available status categories, by severity, include Error, Critical, Warning, Normal, Recovered, and Disabled, as described in the following table.

**Table 68-6 Health Status Indicator**

<table>
<thead>
<tr>
<th>Status Level</th>
<th>Status Icon</th>
<th>Status Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>🕵️‍♀️</td>
<td>White</td>
<td>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.</td>
</tr>
<tr>
<td>Critical</td>
<td>🚨</td>
<td>Red</td>
<td>Indicates that the critical limits have been exceeded for at least one health module on the appliance and the problem has not been corrected.</td>
</tr>
<tr>
<td>Warning</td>
<td>🔄</td>
<td>Yellow</td>
<td>Indicates that warning limits have been exceeded for at least one health module on the appliance and the problem has not been corrected.</td>
</tr>
<tr>
<td>Normal</td>
<td>🟢</td>
<td>Green</td>
<td>Indicates that all health modules on the appliance are running within the limits configured in the health policy applied to the appliance.</td>
</tr>
</tbody>
</table>
Using Appliance Health Monitors

License: Any

The Appliance health monitor provides a detailed view of the health status of an appliance.

Note: Your session normally logs you out after 1 hour of inactivity (or another configured interval). If you plan to passively monitor the health monitor for long periods of time, consider exempting some users from session timeout, or changing the system timeout settings. For more information, see Managing User Login Settings, page 61-49 and Configuring User Interface Settings, page 63-29.

To view the status summary for a specific appliance:

Access: Admin/Maint/Any Security Analyst

<table>
<thead>
<tr>
<th>Status Level</th>
<th>Status Icon</th>
<th>Status Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovered</td>
<td>🟢</td>
<td>Green</td>
<td>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.</td>
</tr>
<tr>
<td>Disabled</td>
<td>📡</td>
<td>Blue</td>
<td>Indicates that an appliance is disabled or blacklisted, that the appliance does not have a health policy applied to it, or that the appliance is currently unreachable.</td>
</tr>
</tbody>
</table>

For more information, see the following sections:
- Understanding Health Modules, page 68-3
- Interpreting Health Monitor Status, page 68-40
- Viewing Alerts by Status, page 68-42
- Running All Modules for an Appliance, page 68-42
- Running a Specific Health Module, page 68-43
- Generating Health Module Alert Graphs, page 68-44
Viewing Alerts by Status

License: Any
You can show or hide categories of alerts by status.

To show alerts by status:
Access: Admin/Maint/Any Security Analyst

Step 1
Click the status icon or the color segment in the pie chart that corresponds to the health status of the alerts you want to view. The alerts for that category appear in the Alert Detail list.

To hide alerts by status:
Access: Admin/Maint/Any Security Analyst

Step 1
Click the status icon or the color segment in the pie chart that corresponds to the health status of the alerts you want to view. The alerts in the Alert Detail list for that category disappear.

Running All Modules for an Appliance

License: Any
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.

To run all health modules for the appliance:
Access: Admin/Maint/Any Security Analyst

Step 1
Select Health > Health Monitor.
The Health Monitor page appears.

Step 2
To expand the appliance list to show appliances with a particular status, click the arrow in that status row.

Tip
If the arrow in the row for a status level points down, the appliance list for that status shows in the lower table. If the arrow points right, the appliance list is hidden.

Step 3
In the Appliance column of the appliance list, click the name of the appliance for which you want to view details.
The Health Monitor Appliance page appears.
Step 4  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

**License:** Any

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.

**To run a specific health module:**

**Access:** Admin/Maint/Any Security Analyst

---

**Step 1**  Select Health > Health Monitor.

The Health Monitor page appears.

**Step 2**  To expand the appliance list to show appliances with a particular status, click the arrow in that status row.

**Tip**  If the arrow in the row for a status level points down, the appliance list for that status shows in the lower table. If the arrow points right, the appliance list is hidden.

**Step 3**  In the Appliance column of the appliance list, click the name of the appliance for which you want to view details.

The Health Monitor Appliance page appears.

**Step 4**  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.

The Alert Detail list expands to list the health alerts for the selected appliance for that status category.

**Step 5**  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

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

To generate a health module alert graph:
Access: Admin/Maint/Any Security Analyst

Step 1
Select Health > Health Monitor.
The Health Monitor page appears.

Step 2
To expand the appliance list to show appliances with a particular status, click the arrow in that status row.

Tip
If the arrow in the row for a status level points down, the appliance list for that status shows in the lower table. If the arrow points right, the appliance list is hidden.

Step 3
In the Appliance column of the appliance list, click the name of the appliance for which you want to view details.
The Health Monitor Appliance page appears.

Step 4
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.
The Alert Detail list expands to list the health alerts for the selected appliance for that status category.

Step 5
In the Alert Detail row for the alert for which you want to view a list of events, click Graph.
A graph appears, showing the status of the event over time. The Alert Detail section below the graph lists all health alerts for the selected appliance.

Tip
If no events appear, you may need to adjust the time range. See Setting Event Time Constraints, page 58-23 for more information.

Using the Health Monitor to Troubleshoot

License: Any
In some cases, if you have a problem with your appliance, Support may ask you to generate troubleshooting files to help them diagnose the problem. You can select any of the options listed in the following table to customize the troubleshooting data that the health monitor reports.

Table 68-7 Selectable Troubleshoot Options

<table>
<thead>
<tr>
<th>This option...</th>
<th>Reports...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snort Performance and Configuration</td>
<td>data and configuration settings related to Snort on the appliance</td>
</tr>
<tr>
<td>Hardware Performance and Logs</td>
<td>data and logs related to the performance of the appliance hardware</td>
</tr>
</tbody>
</table>
Using Appliance Health Monitors

Note that some options overlap in terms of the data they report, but the troubleshooting files will not contain redundant copies, regardless of what options you select.

For more information, see the following sections:

- Generating Appliance Troubleshooting Files, page 68-45
- Downloading Troubleshooting Files, page 68-46

### Generating Appliance Troubleshooting Files

**License:** Any

Use the following procedure to generate customized troubleshooting files that you can send to Support.

**Note**

You **cannot** use the primary Defense Center in a high availability configuration to generate troubleshooting files for the secondary Defense Center, or visa versa. You must generate troubleshooting files for a Defense Center from its own web interface.

**To generate troubleshooting files:**

**Access:** Admin/Maint/Any Security Analyst

**Step 1**

Select **Health > Health Monitor.**

The Health Monitor page appears.

**Step 2**

To expand the appliance list to show appliances with a particular status, click the arrow in that status row.

**Tip**

If the arrow in the row for a status level points down, the appliance list for that status shows in the lower table. If the arrow points right, the appliance list is hidden.

**Step 3**

In the **Appliance** column of the appliance list, click the name of the appliance for which you want to view details.

The Health Monitor Appliance page appears.
Step 4  Click **Generate Troubleshooting Files**.

The Troubleshooting Options pop-up window appears.

Step 5  Select **All Data** to generate all possible troubleshooting data, or select individual check boxes to customize your report. For more information, see the Selectable Troubleshoot Options table.

Step 6  Click **OK**.

The Defense Center generates the troubleshooting files. You can monitor the file generation process in the task queue (**System > Monitoring > Task Status**).

Step 7  Continue with the procedure in the next section, **Downloading Troubleshooting Files**.

---

**Downloading Troubleshooting Files**

**License:** Any

Use the following procedure to download copies of your generated troubleshooting files.

**To download troubleshooting files:**

**Access:** Admin/Maint/Any Security Analyst

---

Step 1  Select **System > Monitoring > Task Status**.

The Task Status page appears.

Step 2  Find the task that corresponds to the troubleshooting files you generated.

Step 3  After the appliance generates the troubleshooting files and the task status changes to **Completed**, click **Click to retrieve generated files**.

Step 4  Follow your browser’s prompts to download the files.

The files are downloaded in a single **.tar.gz** file.

Step 5  Follow the directions from Support to send the troubleshooting files to Cisco.

---

**Working with Health Events**

**License:** Any

The Defense Center provides fully customizable event views that 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 easily access other information that may be related to the events you are investigating.

Many functions that you can perform on the health event view pages are constant across all event view pages. See **Understanding Health Event Views, page 68-47** for more information about these common procedures.

From the **Health > Health Events** menu option, you can view health events and can search for specific events.

See the following sections for more information about viewing events:

- **Understanding Health Event Views, page 68-47** describes the types of events that FireSIGHT generates.
• **Viewing Health Events**, page 68-47 describes how to access and use the Event View page.
• **Searching for Health Events**, page 68-53 describes how to search for specific events using the Event Search page.

### Understanding Health Event Views

**License:** Any

The Defense Center health monitor logs health events, which you can see on the Health Event View page. If you understand what conditions each health module tests for, you can more effectively configure alerting for health events. For more information on the different types of health modules that generate health events, see **Understanding Health Modules**, page 68-3.

For more information about viewing and searching for health events, see the following sections:

• **Viewing Health Events**, page 68-47
• **Understanding the Health Events Table**, page 68-52
• **Searching for Health Events**, page 68-53

### Viewing Health Events

**License:** Any

You can view the appliance health data collected by your health monitor in several ways.

For more information, see the following topics:

• **Viewing All Health Events**, page 68-47
• **Viewing Health Events by Module and Appliance**, page 68-48
• **Working with the Health Events Table View**, page 68-49
• **Interpreting Hardware Alert Details for 3D9900 Devices**, page 68-49
• **Interpreting Hardware Alert Details for Series 3 Devices**, page 68-51

### Viewing All Health Events

**License:** Any

The Table View of Health Events page provides a list of all health events on the selected appliance. For a description of the health modules that generated the events that you may see on this page, see **Understanding Health Modules**, page 68-3.

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

**To view all health events on all managed appliances:**

**Access:** Admin/Maint/Any Security Analyst

---

**Step 1**
Select **Health > Health Events**.

The Events page appears, containing all health events.
Chapter 68  Using Health Monitoring

Working with Health Events

Note
If no events appear, you may need to adjust the time range. See Setting Event Time Constraints, page 58-23 for more information.

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. For more information, see Setting Event Time Constraints, page 58-23.

Viewing Health Events by Module and Appliance

License: Any
You can query for events generated by a specific health module on a specific appliance.

To view the health events for a specific module:
Access: Admin/Maint/Any Security Analyst

Step 1
Select Health > Health Monitor.
The Health Monitor page appears.

Step 2
To expand the appliance list to show appliances with a particular status, click the arrow in that status row.

Tip
If the arrow in the row for a status level points down, the appliance list for that status shows in the lower table. If the arrow points right, the appliance list is hidden.

Step 3
In the Appliance column of the appliance list, click the name of the appliance for which you want to view details.
The Health Monitor Appliance page appears.

Step 4
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.
The Alert Detail list expands to list the health alerts for the selected appliance for that status category.

Step 5
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 query results for a query with the name of the appliance and the name of the selected health alert module as constraints.

If no events appear, you may need to adjust the time range. See Setting Event Time Constraints, page 58-23 for more information.

Step 6
If you want to view all health events for the selected appliance, expand Search Constraints and click the Module Name constraint to remove it.
## Working with the Health Events Table View

**License:** Any

The following table describes each action you can perform from the Event View page.

<table>
<thead>
<tr>
<th>To...</th>
<th>You can...</th>
</tr>
</thead>
<tbody>
<tr>
<td>learn more about the contents of the columns that appear in the Health event view</td>
<td>find more information in Understanding the Health Events Table, page 68-52.</td>
</tr>
<tr>
<td>modify the time and date range for events listed in the Health table view</td>
<td>find more information in Setting Event Time Constraints, page 58-23. 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.</td>
</tr>
<tr>
<td>sort the events that appear, change what columns display in the table of events, or constrain the events that appear</td>
<td>find more information in Sorting Drill-Down Workflow Pages, page 58-34.</td>
</tr>
<tr>
<td>delete health events</td>
<td>select 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.</td>
</tr>
<tr>
<td>navigate through event view pages</td>
<td>find more information in Navigating to Other Pages in the Workflow, page 58-35.</td>
</tr>
<tr>
<td>navigate to other event tables to view associated events</td>
<td>find more information in Navigating Between Workflows, page 58-36.</td>
</tr>
<tr>
<td>bookmark the current page so that you can quickly return to it</td>
<td>click Bookmark This Page, provide a name for the bookmark and click Save. See Using Bookmarks, page 58-37 for more information.</td>
</tr>
<tr>
<td>navigate to the bookmark management page</td>
<td>click View Bookmarks from any event view. See Using Bookmarks, page 58-37 for more information.</td>
</tr>
<tr>
<td>select another health events workflow</td>
<td>click (switch workflow). See Selecting Workflows, page 58-16 for more information.</td>
</tr>
<tr>
<td>view the details associated with a single health event</td>
<td>click the down arrow link on the left side of the event.</td>
</tr>
<tr>
<td>view event details for multiple health events</td>
<td>select the check box next to the rows that correspond with the events you want to view details for and then click View.</td>
</tr>
<tr>
<td>view event details for all events in the view</td>
<td>click View All.</td>
</tr>
<tr>
<td>view all events of a particular status</td>
<td>click the status icon in the Status column for an event with that status.</td>
</tr>
</tbody>
</table>

## Interpreting Hardware Alert Details for 3D9900 Devices

**License:** Any
For 3D9900 device models, hardware alarms generate in response to the events described in the following table. The triggering condition can be found in the message detail for the alert.

### Table 68-9  Conditions Monitored for 3D9900 Devices

<table>
<thead>
<tr>
<th>Condition Monitored</th>
<th>Causes of Yellow or Red Error Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFE card presence</td>
<td>If NFE hardware is detected that is not valid for the appliance, health status for the Hardware Alarms module changes to red and the message details include a reference to the NFE card presence.</td>
</tr>
</tbody>
</table>
| NFE temperature           | If NFE temperature exceeds 95 degrees Celsius, health status for the Hardware Alarms module changes to yellow and the message details include a reference to the NFE temperature.  
                          | If NFE temperature exceeds 99 degrees Celsius, health status for the Hardware Alarms module changes to red and the message details include a reference to the NFE temperature.       |
| NFE Platform daemon       | If the NFE Platform daemon goes down, health status for the Hardware Alarms module changes to red and the message details include a reference to the daemon.                      |
| NFE Message daemon        | If the NFE Message daemon goes down, health status for the Hardware Alarms module changes to red and the message details include a reference to the daemon.                       |
| NFE TCAM daemon           | If the NFE TCAM daemon goes down, health status for the Hardware Alarms module changes to red and the message details include a reference to the daemon.                      |
| LBIM presence             | If the Load Balancing Interface Module (LBIM) switch assembly is not present or not communicating, health status for the Hardware Alarms module changes to red and the message details include a reference to the LBIM presence. |
| Scmd daemon               | If the Scmd daemon goes down, health status for the Hardware Alarms module changes to red and the message details include a reference to the daemon.                         |
| Psls daemon               | If the Psls daemon goes down, health status for the Hardware Alarms module changes to red and the message details include a reference to the daemon.                      |
| Ftwo daemon               | If the Ftwo daemon goes down, health status for the Hardware Alarms module changes to red and the message details include a reference to the daemon.                      |
| Rulesd (host rules) daemon| If the Rulesd daemon goes down, health status for the Hardware Alarms module changes to yellow and the message details include a reference to the daemon.                |
| nfm_ipfragd (host frag) daemon | If the nfm_ipfragd daemon goes down, health status for the Hardware Alarms module changes to red and the message details include a reference to the daemon.                  |
Interpreting Hardware Alert Details for Series 3 Devices

For Series 3 devices, hardware alarms generate in response to the events described in the following table. The triggering condition appears in the message detail for the alert.

Table 68-10 Conditions Monitored for Series 3 Devices

<table>
<thead>
<tr>
<th>Condition Monitored</th>
<th>Causes of Yellow or Red Error Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster status</td>
<td>If clustered devices are no longer communicating with each other (due, for example, to a cabling problem), the Hardware Alarms module changes to red.</td>
</tr>
<tr>
<td>ftwo daemon status</td>
<td>If the ftwo daemon goes down, health status for the Hardware Alarms module changes to red and message details include a reference to the daemon.</td>
</tr>
<tr>
<td>NFE cards detected</td>
<td>Indicates the number of NFE cards detected on the system. If this value does not match the appliance’s expected NFE count, the Hardware Alarms module changes to red.</td>
</tr>
<tr>
<td>NFE hardware status</td>
<td>If one or more NFE cards are not communicating, the Hardware Alarms module changes to red and the applicable card appears in the message details.</td>
</tr>
<tr>
<td>NFE heartbeat</td>
<td>If the system detects no NFE heartbeat, the Hardware Alarms module changes to red and message details include a reference to the relevant card(s).</td>
</tr>
<tr>
<td>NFE internal link status</td>
<td>If the link between the NMSB and NFE card(s) goes down, the Hardware Alarms module changes to red and message details include a reference to the relevant ports.</td>
</tr>
<tr>
<td>NFE Message daemon</td>
<td>If the NFE Message daemon goes down, health status for the Hardware Alarms module changes to red and the message details include a reference to the daemon (and, if applicable, the NFE card number).</td>
</tr>
<tr>
<td>NFE temperature</td>
<td>If NFE temperature exceeds 97 degrees Celsius, health status for the Hardware Alarms module changes to yellow and message details include a reference to the NFE temperature (and, if applicable, the NFE card number). If NFE temperature exceeds 102 degrees Celsius, health status for the Hardware Alarms module changes to red and message details include a reference to the NFE temperature. (and, if applicable, the NFE card number).</td>
</tr>
<tr>
<td>NFE temperature status</td>
<td>Indicates the current temperature status of the given NFE card. The Hardware Alarms module indicates green for OK, yellow for Warning, and red for Critical (and, if applicable, the NFE card number).</td>
</tr>
<tr>
<td>NFE TCAM daemon</td>
<td>If the NFE TCAM daemon goes down, health status for the Hardware Alarms module changes to red and message details include a reference to the daemon (and, if applicable, the NFE card number).</td>
</tr>
<tr>
<td>nfm_ipfragd (host frag) daemon</td>
<td>If the nfm_ipfragd daemon goes down, health status for the Hardware Alarms module changes to red and message details include a reference to the daemon (and, if applicable, the NFE card number).</td>
</tr>
</tbody>
</table>
The fields in the health events table are described in the following table.

**Table 68-11 Health Event Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Name</td>
<td>The name of the health module that generated the event. For a list of health modules, see the Health Modules table.</td>
</tr>
<tr>
<td>Time</td>
<td>The timestamp for the health event.</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td>Value</td>
<td>The value (number of units) of the result obtained by the health test that generated the event. For example, if the Defense 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.</td>
</tr>
</tbody>
</table>
To display the table view of health events:

**Access:** Admin/Maint/Any Security Analyst

**Step 1**

Select **Health > Health Events**.

The table view appears. For information on working with health events, see Working with Health Events, page 68-46.

---

**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**.

---

### Searching for Health Events

**License:** Any

You can search for specific health events. You may want to create searches customized for your network environment, then save them to reuse later. The following table describes the search criteria you can use.

<table>
<thead>
<tr>
<th>Search Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module Name</td>
<td>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.</td>
</tr>
<tr>
<td>Value</td>
<td>Specify the value (number of units) of the result obtained by the health test for the events you want to view. For example, if you specify a value of 15 and type CPU in the Units field, you retrieve events where the appliance CPU was running at 15% utilization at the time the test ran.</td>
</tr>
<tr>
<td>Description</td>
<td>Specify the description of the events you want to view. For example, you could enter Unable to Execute to view any health events where a process was unable to execute. You can use an asterisk (*) in this field to create wildcard searches.</td>
</tr>
</tbody>
</table>
To search for health events:

Access: Admin/Maint/Any Security Analyst

Step 1
Select Analysis > Search.

The Search page appears.

Step 2
Select Health Events from the table drop-down list.

The page updates with the appropriate constraints.

Step 3
Enter your search criteria in the appropriate fields, as described in the Health Event Search Criteria table.

If you enter multiple criteria, the search returns only the records that match all the criteria.

Step 4
Optionally, if you plan to save the search, you can select the Private check box to save the search as private so only you can access it. Otherwise, leave the check box clear to save the search for all users.

Tip
If you want to use the search as a data restriction for a custom user role, you must save it as a private search.

Step 5
Optionally, you can save the search to be used again in the future. You have to following options:

- Click Save to save the search criteria.
  
  For a new search, a dialog box appears prompting for the name of the search; enter a unique search name and click Save. If you save new criteria for a previously-existing search, no prompt appears. The search is saved (and visible only to your account if you selected Private) so you can run it at a later time.

- Click Save as New to save a new search or assign a name to a search you created by altering a previously-save search.

### Table 68-12 Health Event Search Criteria

<table>
<thead>
<tr>
<th>Search Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Units</td>
<td>Specify the units descriptor for the result obtained by the health test for the events you want to view. You can use an asterisk (*) in this field to create wildcard searches. For example, if you type % in the Units field, you retrieve all events for the Disk Usage modules, because the Disk Usage module has a “%” label in the Units field (and no additional text). However, if you type *% in the Units field, you retrieve all events for any modules that contain text followed by a “%” sign in the Units field.</td>
</tr>
<tr>
<td>Status</td>
<td>Specify the status for the health events that you want to view. Valid status levels are Critical, Warning, Normal, Error, and Disabled. For example, type Critical to retrieve all health events that indicate a critical status.</td>
</tr>
<tr>
<td>Device</td>
<td>Type the device name or IP address, or a device group, stack, or cluster name to restrict the search to health events generated by one or more specific devices. For detailed information on how the FireSIGHT System treats the device field in searches, see Specifying Devices in Searches, page 60-7.</td>
</tr>
</tbody>
</table>

For more information on searching, including information on special search syntax as well as saving and loading searches, see Performing and Saving Searches, page 60-1.
A dialog box appears prompting for the name of the search; enter a unique search name and click **Save**. The search is saved (and visible only to your account if you selected **Private**) so that you can run it at a later time.

**Step 6**  
Click **Search** to start the search.

Your search results appear in the default health events workflow, constrained by the current time range. To use a different workflow, including a custom workflow, click **(switch workflow)**. For information on specifying a different default workflow, see Configuring Event View Settings, page 71-3.