



Monitoring the System

The following topics describe how to monitor the Firepower System:

- [About System Statistics, on page 1](#)
- [System Messages, on page 9](#)
- [Managing System Messages, on page 12](#)

About System Statistics

You can view system statistics for the Firepower Management Center and 7000 & 8000 Series devices.

The Statistics page lists the current status of general appliance statistics, including disk usage and system processes, Data Correlator statistics (FMC only), and intrusion event information (FMC only).

The Host Statistics Section

The following table describes the host statistics listed on the Statistics page.

Table 1: Host Statistics

Category	Description
Time	The current time on the system.
Uptime	The number of days (if applicable), hours, and minutes since the system was last started.
Memory Usage	The percentage of system memory that is being used.
Load Average	The average number of processes in the CPU queue for the past 1 minute, 5 minutes, and 15 minutes.
Disk Usage	The percentage of the disk that is being used. Click the arrow to view more detailed host statistics.
Processes	A summary of the processes running on the system.

The Disk Usage Section

The Disk Usage section of the Statistics page provides a quick synopsis of disk usage, both by category and by partition status. If you have a malware storage pack installed on a device, you can also check its partition status. You can monitor this page from time to time to ensure that enough disk space is available for system processes and the database.



Tip You can also use the Disk Usage health monitor on the Firepower Management Center to monitor disk usage and alert on low disk space conditions.

The Processes Section

The Processes section of the Statistics page allows you to see the processes that are currently running on an appliance. It provides general process information and specific information for each running process. You can use the Firepower Management Center's web interface to view the process status for any managed device.

Note that there are two different types of processes that run on an appliance: daemons and executable files. Daemons always run, and executable files are run when required.

Process Status Fields

When you expand the Processes section of the Statistics page, you can also view the following:

Cpu(s)

Lists the following CPU usage information:

- user process usage percentage
- system process usage percentage
- nice usage percentage (CPU usage of processes that have a negative nice value, indicating a higher priority). Nice values indicate the scheduled priority for system processes and can range between -20 (highest priority) and 19 (lowest priority).
- idle usage percentage

Mem

Lists the following memory usage information:

- total number of kilobytes in memory
- total number of used kilobytes in memory
- total number of free kilobytes in memory
- total number of buffered kilobytes in memory

Swap

Lists the following swap usage information:

- total number of kilobytes in swap
- total number of used kilobytes in swap
- total number of free kilobytes in swap
- total number of cached kilobytes in swap

The following table describes each column that appears in the Processes section.

Table 2: Process List Columns

Column	Description
Pid	The process ID number
Username	The name of the user or group running the process
Pri	The process priority
Nice	The <i>nice</i> value, which is a value that indicates the scheduling priority of a process. Values range between -20 (highest priority) and 19 (lowest priority)
Size	The memory size used by the process (in kilobytes unless the value is followed by <i>m</i> , which indicates megabytes)
Res	The amount of resident paging files in memory (in kilobytes unless the value is followed by <i>m</i> , which indicates megabytes)
State	The process state: <ul style="list-style-type: none"> • D — process is in uninterruptible sleep (usually Input/Output) • N — process has a positive nice value • R — process is runnable (on queue to run) • S — process is in sleep mode • T — process is being traced or stopped • W — process is paging • X — process is dead • Z — process is defunct • < — process has a negative nice value
Time	The amount of time (in hours:minutes:seconds) that the process has been running
Cpu	The percentage of CPU that the process is using
Command	The executable name of the process

Related Topics

[System Daemons](#), on page 4

[Executables and System Utilities](#), on page 5

System Daemons

Daemons continually run on an appliance. They ensure that services are available and spawn processes when required. The following table lists daemons that you may see on the Process Status page and provides a brief description of their functionality.



Note The table below is not an exhaustive list of all processes that may run on an appliance.

Table 3: System Daemons

Daemon	Description
crond	Manages the execution of scheduled commands (cron jobs)
dhclient	Manages dynamic host IP addressing
fpcollect	Manages the collection of client and server fingerprints
httpd	Manages the HTTP (Apache web server) process
httpsd	Manages the HTTPS (Apache web server with SSL) service, and checks for working SSL certificate authentication; runs in the background to provide secure web access to the appliance
keventd	Manages Linux kernel event notification messages
klogd	Manages the interception and logging of Linux kernel messages
kswapd	Manages Linux kernel swap memory
kupdated	Manages the Linux kernel update process, which performs disk synchronization
mysqld	Manages database processes
ntpd	Manages the Network Time Protocol (NTP) process
pm	Manages all Firepower System processes, starts required processes, restarts any process that unexpectedly
reportd	Manages reports
safe_mysqld	Manages safe mode operation of the database; restarts the database daemon if an error occurs; logs runtime information to a file
SFDataCorrelator	Manages data transmission
sfstreamer (FMC only)	Manages connections to third-party client applications that use the Event Streamer
sfmgr	Provides the RPC service for remotely managing and configuring an appliance using an SSH connection to the appliance
SFRemediateD (FMC only)	Manages remediation responses

Daemon	Description
sftimeserviced (FMC only)	Forwards time synchronization messages to managed devices
sfmbservice	Provides access to the sfmb message broker process running on a remote appliance, using a connection to the appliance. Currently used only by health monitoring to send health events from a managed device to a Firepower Management Center.
sftroughd	Listens for connections on incoming sockets and then invokes the correct executable (Cisco message broker, sfmb) to handle the request
sftunnel	Provides the secure communication channel for all processes requiring communication with the appliance
sshd	Manages the Secure Shell (SSH) process; runs in the background to provide SSH access to the appliance
syslogd	Manages the system logging (syslog) process

Executables and System Utilities

There are a number of executables on the system that run when executed by other processes or through user action. The following table describes the executables that you may see on the Process Status page.

Table 4: System Executables and Utilities

Executable	Description
awk	Utility that executes programs written in the <code>awk</code> programming language
bash	GNU Bourne-Again Shell
cat	Utility that reads files and writes content to standard output
chown	Utility that changes user and group file permissions
chsh	Utility that changes the default login shell
SFDataCorrelator (FMC only)	Analyzes binary files created by the system to generate events, connection data, and network maps
cp	Utility that copies files
df	Utility that lists the amount of free space on the appliance
echo	Utility that writes content to standard output
egrep	Utility that searches files and folders for specified input; supports extended set of regular expressions not supported in standard <code>grep</code>
find	Utility that recursively searches directories for specified input
grep	Utility that searches files and directories for specified input
halt	Utility that stops the server

Executable	Description
httpsdctl	Handles secure Apache Web processes
hwclock	Utility that allows access to the hardware clock
ifconfig	Indicates the network configuration executable. Ensures that the MAC address stays constant
iptables	Handles access restriction based on changes made to the Access Configuration page.
iptables-restore	Handles iptables file restoration
iptables-save	Handles saved changes to the iptables
kill	Utility that can be used to end a session and process
killall	Utility that can be used to end all sessions and processes
ksh	Public domain version of the Korn shell
logger	Utility that provides a way to access the syslog daemon from the command line
md5sum	Utility that prints checksums and block counts for specified files
mv	Utility that moves (renames) files
myisamchk	Indicates database table checking and repairing
mysql	Indicates a database process; multiple instances may appear
openssl	Indicates authentication certificate creation
perl	Indicates a perl process
ps	Utility that writes process information to standard output
sed	Utility used to edit one or more text files
sfheartbeat	Identifies a heartbeat broadcast, indicating that the appliance is active; heartbeat used to maintain contact between a device and Firepower Management Center
sfmb	Indicates a message broker process; handles communication between Firepower Management Centers and device.
sh	Public domain version of the Korn shell
shutdown	Utility that shuts down the appliance
sleep	Utility that suspends a process for a specified number of seconds
smtpclient	Mail client that handles email transmission when email event notification functionality is enabled

Executable	Description
snmptrap	Forwards SNMP trap data to the SNMP trap server specified when SNMP notification functionality is enabled
snort	Indicates that Snort is running
ssh	Indicates a Secure Shell (SSH) connection to the appliance
sudo	Indicates a sudo process, which allows users other than admin to run executables
top	<p>Utility that displays information about the top CPU processes</p> <p>Note The CPU usage output of this utility is a split up of different types of usages of the CPU core. You must add both user and system processes usage to know the actual total CPU usage.</p> <p>For example, if the output of top command is: %Cpu(s): 76.6 us, 22.1 sy, 0.0 ni, 0.0 id, 0.0 wa, 0.0 hi, 1.3 si, 0.0 st</p> <p>Here, 76.6% of CPU time are used by user processes, 22.1% of CPU time is used by system(kernel) processes. The total CPU usage is 98.7%.</p> <p>Thus, the CPU usage reported in this utility appear to be different from the Health Monitor dashboard. In addition, this utility uses a three seconds interval to calculate the CPU usage. Whereas, the management center health monitor uses one-second intervals.</p>
touch	Utility that can be used to change the access and modification times of specified files
vim	Utility used to edit text files
wc	Utility that performs line, word, and byte counts on specified files

Related Topics

[Configure an Access List](#)

The SFDataCorrelator Process Statistics Section

On a Firepower Management Center, you can view statistics about the Data Correlator and network discovery processes for the current day. As the managed devices perform data acquisition, decoding, and analysis, the network discovery process correlates the data with the fingerprint and vulnerability databases, then produces binary files that are processed by the Data Correlator running on the Firepower Management Center. The Data Correlator analyzes the information from the binary files, generates events, and creates network maps.

The statistics that appear for network discovery and the Data Correlator are averages for the current day, using statistics gathered between 12:00 AM and 11:59 PM for each device.

The following table describes the statistics displayed for the Data Correlator process.

Table 5: Data Correlator Process Statistics

Category	Description
Events/Sec	Number of discovery events that the Data Correlator receives and processes per second
Connections/Sec	Number of connections that the Data Correlator receives and processes per second
CPU Usage — User (%)	Average percentage of CPU time spent on user processes for the current day
CPU Usage — System (%)	Average percentage of CPU time spent on system processes for the current day
VmSize (KB)	Average size of memory allocated to the Data Correlator for the current day, in kilobytes
VmRSS (KB)	Average amount of memory used by the Data Correlator for the current day, in kilobytes

The Intrusion Event Information Section

On both the Firepower Management Center and managed devices, you can view summary information about intrusion events on the Statistics page. This information includes the date and time of the last intrusion event, the total number of events that have occurred in the past hour and the past day, and the total number of events in the database.



Note The information in the Intrusion Event Information section of the Statistics page is based on intrusion events stored on the managed device rather than those sent to the Firepower Management Center. No intrusion event information is listed on this page if the managed device cannot (or is configured not to) store intrusion events locally.

The following table describes the statistics displayed in the Intrusion Event Information section of the Statistics page.

Table 6: Intrusion Event Information

Statistic	Description
Last Alert Was	The date and time that the last event occurred
Total Events Last Hour	The total number of events that occurred in the past hour
Total Events Last Day	The total number of events that occurred in the past twenty-four hours
Total Events in Database	The total number of events in the events database

Viewing System Statistics

On the Firepower Management Center, the web interface displays statistics for the FMC and any devices it manages. On 7000 and 8000 Series devices, the system displays statistics for that device only.

Before you begin

You must be an Admin or Maintenance user and be in the Global domain to view system statistics.




Procedure

-
- | | |
|---------------|--|
| Step 1 | Choose System > Monitoring > Statistics . |
| Step 2 | (FMC only) Choose a device from the Select Device(s) list, and click Select Devices . |
| Step 3 | View available statistics. |
| Step 4 | In the Disk Usage section, you can: <ul style="list-style-type: none">• Hover your pointer over a disk usage category in the By Category stacked bar to view (in order):<ul style="list-style-type: none">• the percentage of available disk space used by that category• the actual storage space on the disk• the total disk space available for that category• Click the down arrow next to By Partition to expand it. If you have a malware storage pack installed, the <code>/var/storage</code> partition usage is displayed. |
| Step 5 | (Optional) Click the arrow next to Processes to view the information described in Process Status Fields, on page 2 . |
-

System Messages

When you need to track down problems occurring in the Firepower System, the Message Center is the place to start your investigation. This feature allows you to view the messages that the Firepower System continually generates about system activities and status.

To open the Message Center, click on the System Status icon, located to the immediate right of the Deploy button in the main menu. This icon can take one of the following forms, depending on the system status:

-  — Indicates one or more errors and any number of warnings are present on the system.
-  — Indicates one or more warnings and no errors are present on the system.
-  — Indicates no warnings or errors are present on the system.

If a number is displayed with the icon, it indicates the total current number of error or warning messages.

To close the Message Center, click anywhere outside of it within the Firepower System web interface.

In addition to the Message Center, the web interface displays pop-up notifications in immediate response to your activities and ongoing system activities. Some pop-up notifications automatically disappear after five seconds, while others are "sticky," meaning they display until you explicitly dismiss them by clicking **Dismiss** (✕). Click the **Dismiss** link at the top of the notifications list to dismiss all notifications at once.



Tip Hovering your cursor over a non-sticky pop-up notification causes it to be sticky.

The system determines which messages it displays to users in pop-up notifications and the Message Center based on their licenses, domains, and access roles.

Message Types

The Message Center displays messages reporting system activities and status organized into three different tabs:

Deployments

This tab displays current status related to configuration deployment for each appliance in your system, grouped by domain. The Firepower System reports the following deployment status values on this tab.

- **Running (Spinning)** — The configuration is in the process of deploying.
- **Success** — The configuration has successfully been deployed.
- **Warning** (⚠) — Warning deployment statuses contribute to the message count displayed with the **Warning System Status icon**.
- **Failure** — The configuration has failed to deploy; see [Out-of-Date Policies](#). Failed deployments contribute to the message count displayed with the **Error System Status icon**.

Health

This tab displays current health status information for each appliance in your system, grouped by domain. Health status is generated by health modules as described in [About Health Monitoring](#). The Firepower System reports the following health status values on this tab:

- **Warning** (⚠) — Indicates that warning limits have been exceeded for a health module on an appliance and the problem has not been corrected. The Health Monitoring page indicates these conditions with a **Yellow Triangle** (⚠). Warning statuses contribute to the message count displayed with the **Warning System Status icon**.
- **Critical** (❗) — Indicates that critical limits have been exceeded for a health module on an appliance and the problem has not been corrected. The Health Monitoring page indicates these conditions with a **Critical** (❗) icon. Critical statuses contribute to the message count displayed with the **Error System Status icon**.
- **Error** (✖) — Indicates that a health monitoring module has failed on an appliance and has not been successfully re-run since the failure occurred. The Health Monitoring page indicates these conditions with a **Error icon**. Error statuses contribute to the message count displayed with the **Error System Status icon**.

You can click on links in the Health tab to view related detailed information on the Health Monitoring page. If there are no current health status conditions, the Health tab displays no messages.

Tasks

In the Firepower System, you can perform certain tasks (such as configuration backups or update installation) that can require some time to complete. This tab displays the status of these long-running tasks, and can include tasks initiated by you or, if you have appropriate access, other users of the system. The tab presents messages in reverse chronological order based on the most recent update time for each message. Some task status messages include links to more detailed information about the task in question. The Firepower System reports the following task status values on this tab:

- **Waiting()** — Indicates a task that is waiting to run until another in-progress task is complete. This message type displays an updating progress bar.
- **Running** — Indicates a task that is in-progress. This message type displays an updating progress bar.
- **Retrying** — Indicates a task that is automatically retrying. Note that not all tasks are permitted to try again. This message type displays an updating progress bar.
- **Success** — Indicates a task that has completed successfully.
- **Failure** — Indicates a task that did not complete successfully. Failed tasks contribute to the message count displayed with the **Error System Status icon**.
- **Stopped or Suspended** — Indicates a task that was interrupted due to a system update. Stopped tasks cannot be resumed. After normal operations are restored, start the task again.
- **Skipped** — A process in progress prevented the task from starting. Try again to start the task.

New messages appear in this tab as new tasks are started. As tasks complete (status success, failure, or stopped), this tab continues to display messages with final status indicated until you remove them. Cisco recommends you remove messages to reduce clutter in the Tasks tab as well as the message database.

Message Management

From the Message Center you can:

- Configure pop-up notification behavior (choosing whether to display them).
- Display additional task status messages from the system database (if any are available that have not been removed).
- Remove individual task status messages. (This affects all users who can view the removed messages.)
- Remove task status messages in bulk. (This affects all users who can view the removed messages.)



Tip

Cisco recommends that you periodically remove accumulated task status messages from the Task tab to reduce clutter in the display as well the database. When the number of messages in the database approaches 100,000, the system automatically deletes task status messages that you have removed.

Managing System Messages

Procedure

Step 1 Click System Status to display the Message Center.

Step 2 You have the following choices:

- Click **Deployments** to view messages related to configuration deployments. See [Viewing Deployment Messages, on page 12](#). You must be an Admin user or have the **Deploy Configuration to Devices** permission to view these messages.
 - Click **Health** to view messages related to the health of your Firepower Management Center and the devices registered to it. See [Viewing Health Messages, on page 12](#). You must be an Admin user or have the **Health** permission to view these messages.
 - Click **Tasks** to view or manage messages related to long-running tasks. See [Viewing Task Messages, on page 13](#) or [Managing Task Messages, on page 13](#). Everyone can see their own tasks. To see the tasks of other users, you must be an Admin user or have the **View Other Users' Tasks** permission.
 - Click **Cog** (⚙) in the upper right corner of the Message Center to configure pop-up notification behavior. See [Configuring Notification Behavior, on page 14](#).
-

Viewing Deployment Messages

You must be an Admin user or have the **Deploy Configuration to Devices** permission to view these messages.

Procedure

Step 1 Click System Status to display the Message Center.

Step 2 Click **Deployments**.

Step 3 You have the following choices:

- Click **total** to view all current deployment statuses.
 - Click a status value to view only messages with that deployment status.
 - Hover your cursor over the time elapsed indicator for a message (for example, **1m 5s**) to view the elapsed time, and start and stop times for the deployment.
-

Related Topics

[Deploy Configuration Changes](#)

Viewing Health Messages

You must be an Admin user or have the **Health** permission to view these messages.

Procedure

- Step 1** Click System Status to display the Message Center.
- Step 2** Click **Health**.
- Step 3** You have the following choices:
- Click **total** to view all current health statuses.
 - Click on a status value to view only messages with that status.
 - Hover your cursor over the relative time indicator for a message (for example, **3 day(s) ago**) to view the time of the most recent update for that message.
 - To view detailed health status information for a particular message, click the message.
 - To view complete health status on the Health Monitoring page, click **Health Monitor**.
-

Related Topics

[About Health Monitoring](#)

Viewing Task Messages

Everyone can see their own tasks. To see the tasks of other users, you must be an Admin user or have the **View Other Users' Tasks** permission.

Procedure

- Step 1** Click System Status to display the Message Center.
- Step 2** Click **Tasks**.
- Step 3** You have the following choices:
- Click **total** to view all current task statuses.
 - Click a status value to view only messages for tasks with the that status.
- Note** Messages for stopped tasks appear only in the total list of task status messages. You cannot filter on stopped tasks.
- Hover your cursor over the relative time indicator for a message (e.g., **3 day(s) ago**) to view the time of the most recent update for that message.
 - Click any link within a message to view more information about the task.
 - If more task status messages are available for display, click **Fetch more messages** at the bottom of the message list to retrieve them.
-

Managing Task Messages

Everyone can see their own tasks. To see the tasks of other users, you must be an Admin user or have the **View Other Users' Tasks** permission.

Procedure

- Step 1** Click System Status to display the Message Center.
- Step 2** Click Tasks.
- Step 3** You have the following choices:
- If more task status messages are available for display, click on **Fetch more messages** at the bottom of the message list to retrieve them.
 - To remove a single message for a completed task (status stopped, success, or failure), click on **Remove** (✕) next to the message.
 - To remove all messages for all tasks that have completed (status stopped, success, or failure), filter the messages on **total** and click on **Remove all completed tasks**.
 - To remove all messages for all tasks that have completed successfully, filter the messages on **success**, and click on **Remove all successful tasks**.
 - To remove all messages for all tasks that have failed, filter the messages on **failure**, and click on **Remove all failed tasks**.
-

Configuring Notification Behavior



Note This setting affects all pop-up notifications and persists between login sessions.

Procedure

- Step 1** Click System Status to display the Message Center.
- Step 2** Click **Cog** (⚙) in the upper right corner of the Message Center.
- Step 3** To enable or disable pop-up notification display, click the **Show notifications** slider.
- Step 4** Click **Cog** (⚙) again to hide the slider.
- Step 5** Click System Status again to close the Message Center.
-