



ENDPOINT SECURITY

Host Management
MODULE USER GUIDE

FireEye and the FireEye logo are registered trademarks of FireEye, Inc. in the United States and other countries. All other trademarks are the property of their respective owners.

FireEye assumes no responsibility for any inaccuracies in this document. FireEye reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Copyright © 2020 FireEye, Inc. All rights reserved.

Endpoint Security Host Management Module

Software Release 1.2.1

Revision 1

FireEye Contact Information:

Website: www.fireeye.com

Technical Support: <https://csportal.fireeye.com>

Phone (US):

1.408.321.6300

1.877.FIREEYE

Contents

- PART I: MODULE OVERVIEW 4
 - HOST MANAGEMENT MODULE..... 4
 - PREREQUISITES 4
- PART II: CONFIGURING ENDPOINT HOST MANAGEMENT MODULE..... 4
 - ENABLING THE HOST MANAGEMENT MODULE..... 5
 - DISABLING THE HOST MANAGEMENT MODULE..... 5
 - CONFIGURING THE HOST MANAGEMENT MODULE INTERNAL SETTINGS 6
 - CONFIGURING THE HOST MANAGEMENT MODULE LOGGING SETTINGS..... 7
 - VIEWING THE HOST MANAGEMENT PAGE..... 8
- PART III: TECHNICAL SUPPORT 12

PART I: Module Overview

Host Management Module

The Host Management (formerly Agent Status) module allows you to view a broad range of data about your host endpoints running Endpoint Security Agent software.

After you install and enable the Host Management module, a Host Management page appears at the top of the Hosts menu. The Host Management page displays the current state of different agent components making it easier to see what engines are currently enabled on a given host. You can also use the Host Management page to create and manage filter sets for your agents.

You can use the Host Management Module Settings page to specify how often an agent's information is refreshed, indicate the length of time before an agent's information must be refreshed, determine the level at which information about your agents is logged, and specify the amount of time agent status records are kept before they are deleted.

Prerequisites

This general availability release of Endpoint Host Management is supported on **Endpoint Security 5.0.0** and higher.

Note: Host Management 1.2.1 **will NOT work** on Endpoint Security 4.9 or lower. This is not a supported scenario.

PART II: Configuring Endpoint Host Management Module

This section describes how to enable and disable the Host Management module and configure the polling interval, logging level, and aging setting for the Agent Status module. This section covers the following topics:

This section covers the following topics:

- Enabling the Host Management Module
- Disabling the Host Management Module
- Configuring the Host Management Module Interval Settings
- Configuring the Host Management Logging Settings

- Configuring the Host Management Module Aging Settings

Enabling the Host Management Module

You can enable the Host Management module from the Modules page in the Endpoint Security Web UI.

To enable the Host Management module:

1. Log in to the Endpoint Security Web UI as an administrator.
2. From the **Modules** menu, select **HX Module Administration** to access the **Modules** page.
3. On the **Modules** page, locate the **Host Management** module and perform one of the following actions:
 - In the **Enabled** column, toggle the switch to **ON** to enable the module.
 - Click the Actions icon () and select **Enable** to enable the module.

Disabling the Host Management Module

You can disable the Host Management module from the Modules page in the Endpoint Security Web UI.

To disable the Host Management module:

1. Log in to the Endpoint Security Web UI as an administrator.
2. From the **Modules** menu, select **HX Module Administration** to access the Modules page.
3. On the **Modules** page, locate the **Host Management** module and perform one of the following actions:
 - In the **Enabled** column, toggle the switch to **OFF** to disable the module.
 - Click the Actions icon () and select **Disable** to disable the module.

Configuring the Host Management Module Internal Settings

You can use the Endpoint Security Web UI to specify how frequently the recalculation process runs and when to process an agent's information.

The table below describes the interval settings for the Host Management module and includes the description, range and default value for each setting

Interval Setting	Description	Range	Default Value
Recalculate Interval	Specifies how frequently host record information is refreshed. This information is used to populate the Online Status field for the agent.	60 seconds to 600 seconds	120 seconds
Recalculate Records Older Than	The Host Management module only recalculates records that are older than the amount of time you specify here.	300 seconds to 600 seconds	600 seconds

To configure the interval settings for the Host Management module:

1. Log in to the Endpoint Security Web UI as an administrator.
2. From the **Modules** menu, select **HX Module Administration** to access the **Modules** page.
3. On the **Modules** page, click the **Actions** icon () for the Host Management module, and select **Configure** to access the **Host Management Module Settings** page.
4. On the Intervals tab, enter a number of seconds in the following fields:
 - a. **Recalculate Interval** – Specifies how often the recalculation process runs
 - b. **Recalculate Records Older Than** – Specifies the age limit for the host timestamp record. When an agent's record is older than the limit specified here, it is recalculated.
5. Click **Save Settings**.

Configuring the Host Management Module Logging Settings


You can use the Endpoint Security Web UI to configure the logging level (the type and amount of logging data) to determine the type of messages that are logged by the Agent Status module.

The table below lists the log levels and describes each logging level. Each log level includes the log messages from lower log levels. For example, Alert logs will also include Emergency log messages, Critical logs will also include Alert and *Emergency* log messages, and so on. Emergency is the lowest logging level and *Debug* is the highest logging level. The default logging level is *Debug*.

Logging Level	Description
Emergency	Logs system failure messages that identify total system failures on the host endpoint. These system failures usually cause the agent to stop functioning.
Alert	Logs messages that identify crucial conditions on the host endpoint that require immediate remediation, such as a corrupted system database.
Critical	Logs critical messages that identify serious conditions on the host endpoint, such as hard drive errors.
Error	Logs error messages that identify program errors on the host endpoint, such as when a file cannot be found.
Warning	Logs warning messages that identify non-critical and correctable errors on the host endpoint, such as a specified value that is too large.
Notice	Logs notification messages that identify minor problems on the host endpoint that do not inhibit regular agent function and for which defaults are used until the problem is resolved.
Info	Logs Informational messages about regular system processing.
Debug	Logs debugging messages. This logging level is normally used when debugging a program only. It includes all the types of logging messages.

To configure the Host Management module logging level:

1. Log in to the Endpoint Security Web UI as an administrator.

2. From the **Modules** menu, select **HX Module Administration** to access the Modules page.
3. On the **Modules** page, locate the **Host Management** module, click the Actions icon (), and select **Configure** to access the **Host Management Plugin Settings** page.
4. On the **Host Management Plugin Settings** page, click the **Logging** tab and select the logging level for the Host Management module. The table below describes each logging level. Notice the default logging level.
5. Click **Save Settings**.

Viewing the Host Management Page

You can view the Host Management page from either the Hosts menu or the Modules menu. The Host Management page provides information about the current status of your host endpoints. You can also use the Host Management page to view detailed information and Raw Sysinfo for a selected endpoint.

To view the Host Management page from the Hosts menu:

1. Log in to the Endpoint Security Web UI.
2. From the **Hosts** menu, select **Host Management** to access the **Host Management** page.

To view the Host Management page from the Modules menu:

1. Log in to the Endpoint Security Web UI.
2. From the **Modules** menu, select **Host Management** to access the **Host Management** page.

To view detailed information and Raw Sysinfo for a selected endpoint:

1. On the **Host Management** page, click the row containing the host endpoint about which you want to view details.

A Details pane appears showing the detailed information about the selected endpoint.

2. Click the **Raw Sysinfo** tab at the top of the Details pane to view the raw sysinfo data.
3. Click the **Close** icon to close the Details pane.

Viewing Module Information:

The Host Management grid will dynamically add columns to the grid as modules are enabled on your enterprise. Once an agent returns information for any module, the Host Management Grid will add columns for that module's version and status. These columns are not displayed by default, you will need to use the column selector to add them to your grid view.

The table below describes the information you can view on the Host Management page, and indicates which columns are displayed by default.

Column Name	Description	Displayed By Default
Endpoint Agent ID	The system-generated unique ID for the host endpoint.	No
Server Time	The clock time on the Endpoint Security Server.	No
Hostname	The hostname of the host endpoint.	Yes
Online Status	The current status of the agent on the host endpoint. Possible values are: All, Online, and Offline.	Yes
Operating System	The operating system used on the host endpoint.	Yes
Patch	The name or version number of the most recent patch installed on the operating system that is running on the host endpoint.	Yes
Build	The name or version number of the most recent build installed on the operating system that is running on the host endpoint.	Yes
Logged On User	The host user account running the agent.	Yes
Time Zone	The time zone where the host system is installed.	Yes
Last Check-in	The date and time when the agent last reported its online status.	Yes
Agent Version	The version of Agent software running on the host endpoint.	Yes
Containment Status	The containment state of the host endpoint.	Yes
Real Time	Indicates the status of real-time indicator detection on the host endpoint.	Yes
Content Version	The version of real-time incident detection running on the host endpoint	Yes
Real Time Content Update	The date and time when the real-time indicator detection content was last updated on the host endpoint.	No

Column Name	Description	Displayed By Default
Exploit Guard	Indicates the status of exploit guard on the host endpoint.	Yes
EXD Content Version	The version of exploit guard running on the host endpoint	Yes
EXD Engine Version	The version of exploit guard engine running on the host endpoint	No
Malware Guard	Indicates the status of MalwareGuard on the host endpoint.	Yes
Malware Guard Quarantine	Indicates the status of MalwareGuard quarantine on the host endpoint.	Yes
Malware Guard Model	The version of MalwareGuard running on the host endpoint.	Yes
Malware Guard Model Last Updated	The date and time when MalwareGuard was last updated on the host endpoint.	No
Maware Guard Engine Version	The version of MalwareGuard engine running on the host endpoint.	No
Malware Guard Core Engine Version	The version of MalwareGuard core engine running on the host endpoint.	No
Maware Protection	Indicates the status of malware protection on the host endpoint.	No
Signature and Heuristic Detection	Indicates the status of signature and heuristic detection on the host endpoint.	Yes
Sig and Heuristic Det Quarantine	Indicates the status of signature and heuristic detection quarantine on the host endpoint.	Yes
Signature and Heuristic Version	The version of signature and heuristic detection content on the host endpoint.	Yes
AV Content Last Updated	The date and time when the antivirus content was last updated on the host endpoint.	No
AV Engine Version	The version of antivirus engine running on the host endpoint.	No
Quarantine Actions	The status of the quarantine action taken on the host endpoint. Possible values are: Queued, Success, and Failed.	No
FIPS	Indicates the status of Federal Information Processing Standards (FIPS) on the host endpoint	No

Column Name	Description	Displayed By Default
ProRemSvcStatus	Indicates if the protection removal service is on or off.	No
kernelServicesStatus	The status of the Linux kernel services on the endpoint.	No
Machine Name	The machine name of the host endpoint.	No
Uptime	The number of seconds the host endpoint has been running.	No
Registered Org	The registered organization of the host endpoint.	No
Registered Owner	The registered owner of the host endpoint	No
Platform	The platform of the host endpoint. Possible values are: All, Win, OSX, and Linux.	No
vmGuest	Indicates if the host endpoint is on a virtual image. Possible values are Yes or No.	No
virtual	Indicates if the host endpoint is on a virtual image. Possible values are Yes or No.	No
GMT Offset	The GMT offset time of the host endpoint.	No
Domain	The network domain of the host system.	No
Primary IPv4 Address	The primary IPv4 address of the host endpoint.	No
Primary IP Address	The primary IP address of the host endpoint.	No
MAC	The MAC address of the host endpoint.	No
Total Storage (GB)	The amount of total storage on the host endpoint.	No
Available Storage (GB)	The amount of storage on the host endpoint that is still available to use.	No

PART III: Technical Support

For technical support, contact FireEye through the Support portal:

<https://csportal.fireeye.com>