



ENDPOINT SECURITY

ENDPOINT AGENT CONSOLE v1.1.0

MODULE USER GUIDE

GENERAL AVAILABILITY RELEASE

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 Agent Console Module User Guide

Software Release 1.1.0

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	5
PREREQUISITES	5
PART II: INSTALLING ENDPOINT AGENT CONSOLE MODULE	5
DOWNLOADING THE INSTALLER PACKAGE	5
UPLOADING THE INSTALLER PACKAGE	6
INSTALLING THE ENDPOINT AGENT CONSOLE AGENT MODULE	6
PART III: UNINSTALLING ENDPOINT AGENT CONSOLE MODULE	7
UNINSTALLING THE ENDPOINT AGENT CONSOLE AGENT MODULE	7
PART IV: CONFIGURING ENDPOINT AGENT CONSOLE MODULE	8
ENABLING THE ENDPOINT AGENT CONSOLE MODULE	8
DISABLING THE ENDPOINT AGENT CONSOLE MODULE	9
CONFIGURING ENDPOINT AGENT CONSOLE SERVER CONFIGURATION	10
LOGGING	10
DATA AGING	10
CONFIGURATION API	11
GET ENDPOINT AGENT CONSOLE CONFIGURATION	11
UPDATE ENDPOINT AGENT CONSOLE CONFIGURATION	11
CONFIGURING ENDPOINT AGENT CONSOLE AGENT POLICY	12
EVENT LOG	12
QUARANTINE	13
PART V: USING THE ENDPOINT AGENT CONSOLE INTERFACE	13
QUARANTINE	13
RESTORED FILES	15
EVENT LOG	16
ABOUT	18
AGENT CONSOLE DASHBOARD	19
AGENT CONSOLE REST API	20
GET LOCAL QUARANTINE ACTIONS	20
GET LOCAL QUARANTINE ACTIONS, CSV FORMATTED	21
APPENDIX A: FREQUENTLY ASKED QUESTIONS	22

DEPENDENCIES / LIMITATIONS / KNOWN ISSUES..... 24

PART I: Module Overview

Endpoint Agent Console is an HX Innovation Architecture (IA) module designed to enable the end user to access Endpoint Agent features using a local graphical user interface (GUI). This module provides insights into the quarantined items, detected malware, server scheduled scan summary events and agent version information.

The data displayed in the Agent Console is collected from the endpoint agent locally. There is no server communication involved in displaying the data.

Prerequisites

This general availability release of Endpoint Agent Console is supported on **Endpoint Security 5.0.0** with **Endpoint Agent 32** running on **Windows 7 and above**. Endpoint Agent Console requires Microsoft .NET 4.0 and above on the endpoint to function. Please review Appendix A for dependencies, limitations and known issues for the current release.

Note: It is not recommended to install Endpoint Agent Console on Endpoint Security 4.9.x with Endpoint Agent 31 or lower. This is not a supported scenario.

PART II: Installing Endpoint Agent Console Module

Endpoint Agent Console is an optional module available for **Endpoint Security 5.0.0** with **Endpoint Agent 32**. It is installed using your Endpoint Security Web UI by downloading the module installer package (.cms file) from the FireEye Market and then uploading the module .cms file to your Endpoint Security Web UI. The module is disabled by default. Refer to *Part IV: Enabling the Endpoint Agent Console Module* for steps to enable the server module. After you have installed, the module appears on the Modules menu tab.

Downloading the Installer Package

To download the module installer package:

1. Log in to the Endpoint Security Web UI with your administrator credentials.
2. From the **Modules** menu, select **HX Module Administration** to access the **Modules** page.
3. On the **Modules** page, click **Find Modules** to access the FireEye Market. The FireEye Market opens in a new browser tab.
4. In the **Types** filter list on the FireEye Market, select **Endpoint Security Modules**.
5. In the Search Results, click the **Agent Console** module.
6. On the FireEye Market page for the **Agent Console** module, click **Download** to download the module .cms file to your local drive.

Be sure to note the navigation path to the directory where you downloaded the .cms file.

Uploading the Installer Package

To upload the Endpoint Agent Console module installer package to your Endpoint Security Web UI:

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 **Install Modules** to upload the module .cms file from your local drive to the Endpoint Security Console. The .cms file includes **server module** and an **agent module** of Endpoint Agent Console Module.
4. In the **Upload Module** dialog box, click **Select File**.
5. Navigate to the downloaded module .cms file, select the .cms file, and click **Open**.

The selected .cms file appears in the **Upload Module** dialog box.

6. In the **Upload Module** dialog box, click **Upload**.

A message at the top of the page tells you that module installation has been initiated.

After you have uploaded the Agent Console module successfully, the module appears in the list of modules on the Modules page.

NOTE: You may need to refresh the Endpoint Security Web UI before the new module appears on the Modules page.

Installing the Endpoint Agent Console Agent Module

The **Endpoint Agent Console** module consists of a **server module** and an **agent module**. The above section provided steps to upload the Endpoint Agent Console module to the HX server. To install the **agent module** on a given host set:

1. Log in to the Endpoint Security Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. On the **Policies** page, click the **Actions** icon (the gear icon) for the policy for the agent on which you want to activate Endpoint Agent Console, and select **Edit Policy**.
4. Click on the **Categories** button in the **Edit Policy** page and select **Endpoint Agent Console – <version number>** (e.g., Endpoint Agent Console – 1.0.0) and click **Apply**.
5. On the **Edit Policy** page, click **Save**.

The above steps will inform the endpoints (local systems) to download the agent module and install it during configuration update. Please review the [Configuring Endpoint Agent Console Agent Policy](#) section below to understand various policy options.

PART III: Uninstalling Endpoint Agent Console Module

To uninstall the Endpoint Agent Console module from your Endpoint Security Web UI:

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 **Endpoint Agent Console** module and click the Actions icon (the gear icon) and select *Uninstall* to uninstall the module. A confirmation window appears before uninstallation can proceed. Click **Uninstall** to start the uninstallation of the module.

A message at the top of the page tells you that module uninstallation succeeded.

The **Endpoint Agent Console** module consists of a **server module** and an **agent module**. Uninstalling the **Endpoint Agent Console** module removes Endpoint Agent Console policy settings from all policies and ensures that both **server module** and the **agent module** are removed from endpoints (local systems).

Uninstalling the Endpoint Agent Console Agent Module

The **Endpoint Agent Console** module consists of a **server module** and an **agent module**. The above section provided steps to uninstall the Endpoint Agent Console module completely from the HX server and managed FireEye endpoints. To remove only the **agent module** on a given host set:

6. Log in to the Endpoint Security Web UI as an administrator.
7. From the **Admin** menu, select **Policies** to access the **Policies** page.
8. On the **Policies** page, click the **Actions** icon (the gear icon) for the policy for the agent on which you want to remove the **Endpoint Agent Console**, and select **Edit Policy**.
9. Click on the **Categories** button in the **Edit Policy** page and unselect **Endpoint Agent Console – <version number>** (e.g., Endpoint Agent Console – 1.0.0) and click **Apply**.
10. On the **Edit Policy** page, click **Save**.

PART IV: Configuring Endpoint Agent Console Module

The Endpoint Agent Console module consists of a **server module** and an **agent module**. It is important to understand the following relationships between the server and agent modules:

- The **agent module** is installed and enabled on agents using the Endpoint Agent Console policy.
- Once the **server module** is enabled, disabling the **server module** will **disable** the **agent module** in **all the policies**.
- Uninstalling the **Endpoint Agent Console** module removes Endpoint Agent Console policy settings from all policies and ensures that both **server module** and the **agent module** are removed from endpoints (local systems).

Enabling the Endpoint Agent Console Module

You can perform these tasks from the Modules and Policies pages in the Endpoint Security Web UI.

Before proceeding, please review the [Configuring Endpoint Agent Console Agent Policy](#) section below. It is important to understand the implications of these settings before enabling Agent Console on endpoint agents.

To enable the Endpoint Agent Console server 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 **Endpoint Agent Console** module and click the **Actions** icon (the gear symbol) and select **Enable** to enable the module.

To enable the Endpoint Agent Console agent module:

1. Log in to the Endpoint Security Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. On the **Policies** page, click the **Actions** icon (the gear icon) for the policy for the agent on which you want to activate Endpoint Agent Console, and select **Edit Policy**.
4. In the **Configurations** area of the **Edit Policy** page, click **Endpoint Agent Console**.
5. Toggle the **Enable the Agent Console on the host** selector to **ON**.
6. If you are editing Agent Default Policy, leave all other settings at the default value. If you wish to make any adjustments, please review the [Configuring Endpoint Agent Console Agent Policy](#) section below first.
7. On the **Edit Policy** page, click **Save**.

Disabling the Endpoint Agent Console Module

To disable the server 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 **Endpoint Agent Console** module and click the **Actions** icon (the gear icon) and select **Disable** to disable the module.

Disabling the Endpoint Agent Console **server module** (once enabled) will disable the **agent module** in all the policies, causing it to be disabled on associated endpoints (local systems).

To disable the agent module:

1. Log in to the Endpoint Security Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. On the **Policies** page, click the **Actions** icon (the gear icon) for the policy for the agent on which you want to disable Endpoint Agent Console, and select **Edit Policy**.
4. In the **Configurations** area of the **Edit Policy** page, click **Endpoint Agent Console**.
5. Toggle the **Enable the Agent Console on the host** selector to **OFF**.
6. On the **Edit Policy** page, click **Save** button.

Configuring Endpoint Agent Console Server Configuration

This section describes the various configuration settings provided in the Endpoint Agent Console server configuration.

Logging

Logging settings allow the user to configure the log level for the Endpoint Agent Console server module as shown in Figure 1.

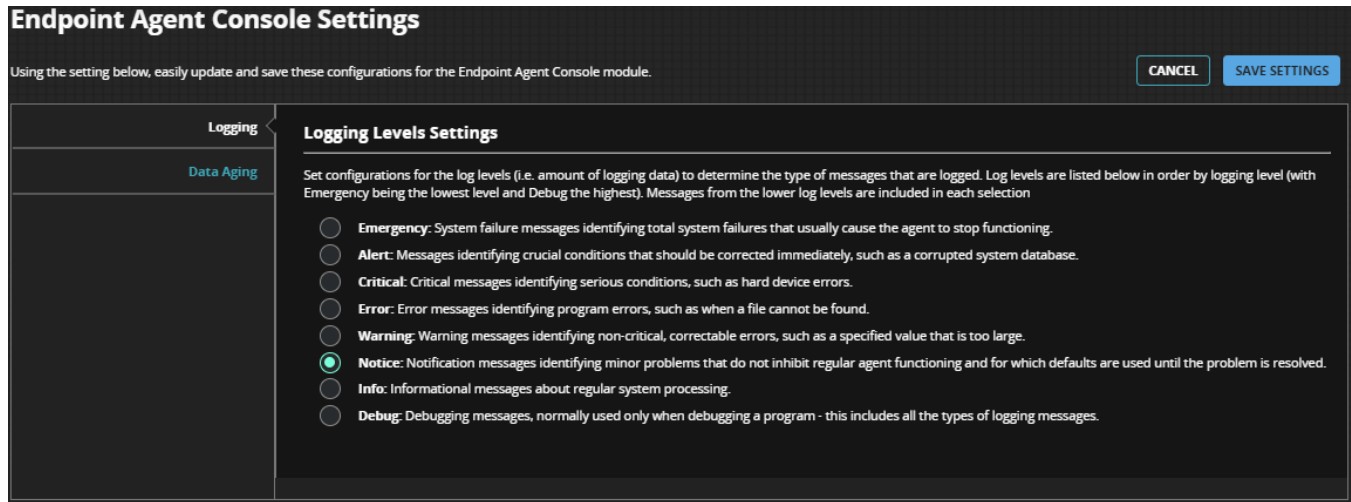


Figure 1 – Logging Settings

Data Aging

Data aging settings allow the user to configure the number of days that quarantine action records are saved on the server as shown in Figure 2. These records serve as audit records for the administrators to keep track of user actions.

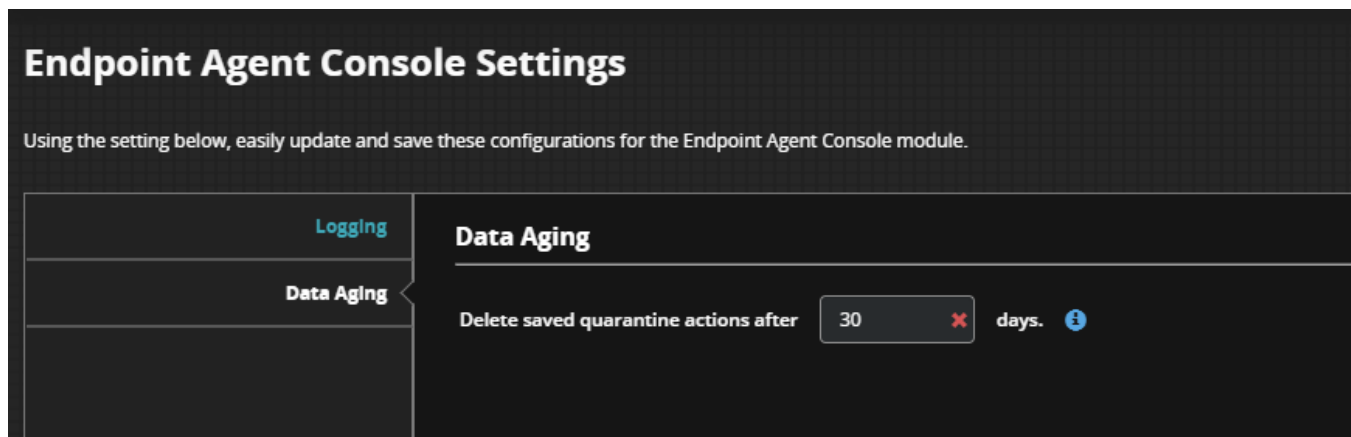


Figure 2 – Data Aging Settings

Configuration API

The configuration API is made available via the configuration endpoint of the Endpoint Security Server REST API. For complete details on how to interact with the Endpoint Security Server API, please refer to FireEye document *Endpoint Security REST API Guide Release 5.0*.

Get Endpoint Agent Console Configuration

Returns the current configuration for the Endpoint Agent Console module as a JSON result.

HTTP Verb	Route	Parameters
GET	hx/api/services/config/tree	?node_name=/config/agent-console

Response

Key	Notes
data	List of configuration properties. Each property has the following attributes: <ul style="list-style-type: none"> name – the name of the configuration property type – the shape of the value for this configuration property value – the current value of this configuration property default_value – the default value of this configuration property

The following is a list of configuration properties for the Endpoint Agent Console Module.

Property	Path	Type {Values}
Aging Interval	/config/agent-console/aging/database/monitor_interval	Int32 (number of seconds) Default = 1 hour
Aging Period	/config/agent-console/aging/database/period	Int32 (number of seconds) Default = 30 days
Logging Level	/config/agent-console/logging/level	String {'debug' 'info' 'warning' 'notice' 'error' 'critical' 'alert' 'emergency'}

Update Endpoint Agent Console Configuration

Updates a configuration property for the Endpoint Agent Console Module. See the list of configuration properties above.

HTTP Verb	Route	Parameters
PUT	hx/api/services/config/tree	?node_name={config path}

Query Headers

Content-Type	Application/json
---------------------	-------------------------

Query Body

List of configuration properties to be set, formatted as JSON. For example, the following request body will specify that the logging level be updated to a value of *Error*.

```
{
  "data": [
    {
      "default_value": "notice",
      "name": "/config/agent-console/logging/level",
      "type": "string",
      "value": "error"
    }
  ]
}
```

Configuring Endpoint Agent Console Agent Policy

This section describes the various configuration settings provided in the Endpoint Agent Console policy.

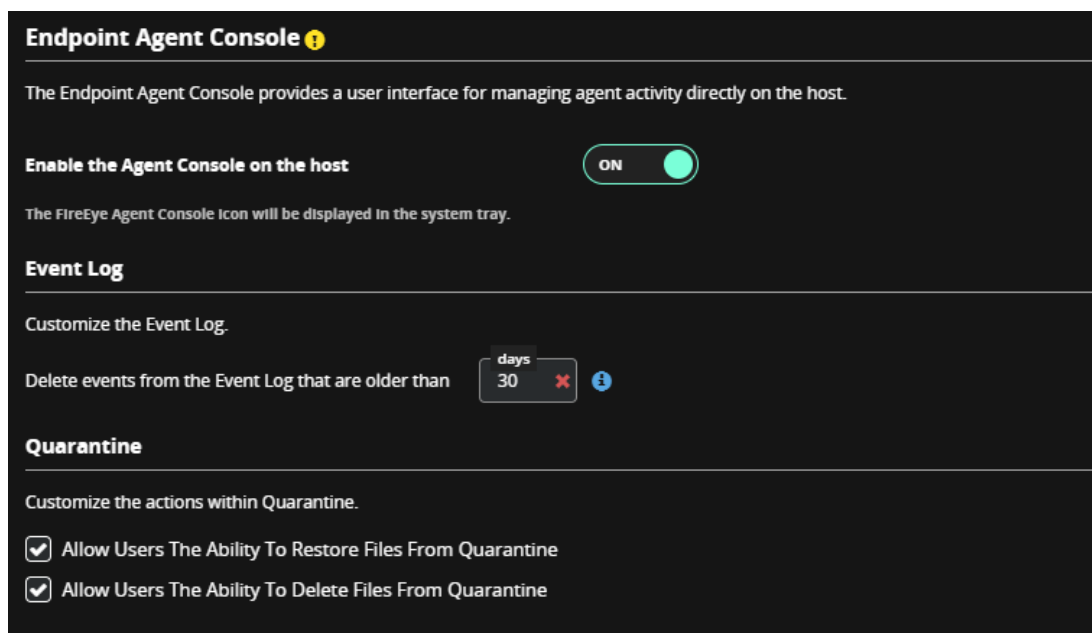


Figure 3 – Agent Console Policy on HX Server

In order to enable Endpoint Agent Console on a given host set, toggle the **Enable the Agent Console on the host** to **ON** and save the policy changes. Upon configuration update on the agent, a FireEye system tray icon will appear on the endpoint. Users can click directly on the icon or right-click the icon and select the appropriate menu item to bring up the Endpoint Agent Console graphical user interface (GUI).

Event Log

Event Log settings allows users to view and manage the events on the endpoint (local system). Default event retention value is as shown in Figure 3 and can be customized based on your needs (1 to 30 days). Events older than the given number of days are purged from the local data base on the agent and they will no longer be visible

using the Endpoint Agent Console. Further details on Event Log functionality are provided in *Part V: Using the Endpoint Agent Console Interface*. An event deleted from the Endpoint Agent Console GUI does not impact the events on the HX server.


Quarantine

Quarantine policy settings are provided to allow the endpoint user/admin (local host) to restore and delete quarantined files locally. These settings are intended for advanced users of the endpoint who understand the implications of restoring possible malware. Further details on Quarantine functionality are provided in *Part V: Using the Endpoint Agent Console Interface*.

PART V: Using the Endpoint Agent Console Interface

This section describes how to use the Endpoint Agent Console interface on the endpoint.

To access the Endpoint Agent Console interface via the system tray icon:

1. Login to the endpoint (workstation) using user credentials.
2. Locate the FireEye logo icon () in the system tray notification area.
3. Right click on the FireEye logo icon and select **Show Main Console**. Clicking the FireEye logo icon also brings up the **Main Console** of the application.

To access the Endpoint Agent Console interface via the start menu:

4. Login to the endpoint (workstation) using user credentials.
5. Click the start button.
6. Navigate to where all programs are displayed. This will vary depending on your operating system. Scroll to **FireEye Endpoint Security** and click on it. This will bring up the **Main Console** of the application.

The Endpoint Agent Console application has a left navigation pane and a display area on the right pane. Details of each item in the left pane and corresponding right pane content are explained below:

Quarantine

Upon launching the Main Console from the system tray, you will be presented with the screen shown in Figure 4 below.

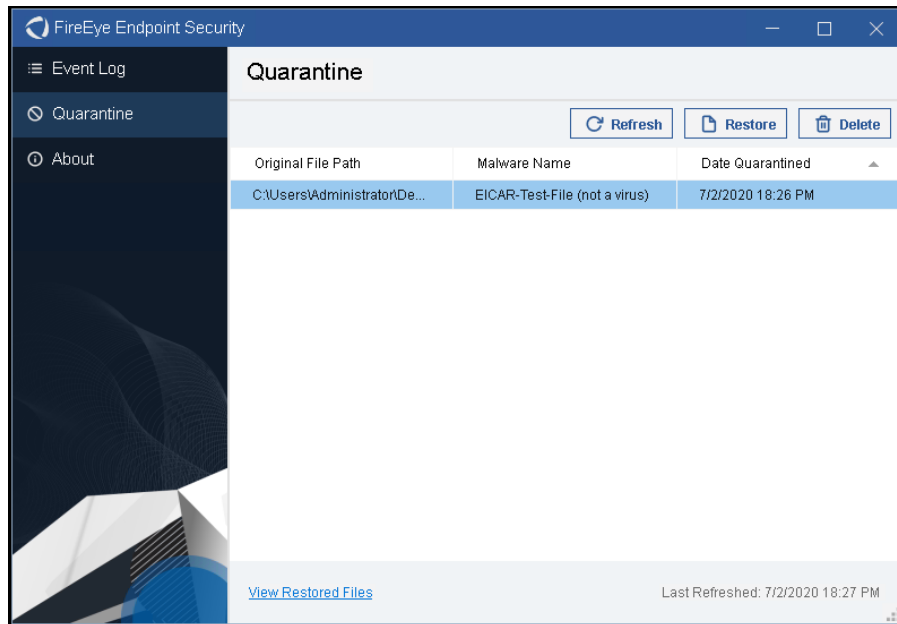


Figure 4 – Quarantine

Quarantine displays the list of quarantined files on the local system. **Restore** and **Delete** buttons are shown or hidden based on the Quarantine policy configuration options. The list of quarantined items can be refreshed by clicking the **Refresh** button. **Restore** and **Delete** actions can be done on a single item or multiple items by selecting them on the display grid.

Delete action will result in deleting a stored quarantined file from the local system permanently. Note that once the quarantined items are deleted, the HX server will not be able to acquire those files from the agent. Upon deletion of a quarantined item, an event will be sent to the HX server for auditing purposes.

Restore action will result in restoring a quarantined file to its original location. This will allow the file to be accessed by the end user. Caution should be exercised as this may lead to unintended consequences if the restored file is malware. Upon restoration of a quarantined file, an event will be sent to the HX server for auditing purposes. Restore action is only limited to the endpoint (local system) and does not affect other endpoints managed by the HX server. Once a quarantined file is restored, it will be added to a restored files list, so that it is not detected again. Further details on restored files is provided in the following section.

Restored files can be viewed by clicking **View Restored Files** at the bottom left corner of the Quarantine window as shown in Figure 5.



Figure 5 – View Restored Files

Following section provides more details about the restored files.

Restored Files

Restored Files displays a list of files restored from quarantine by users of the endpoint (local system) as shown in Figure 6.

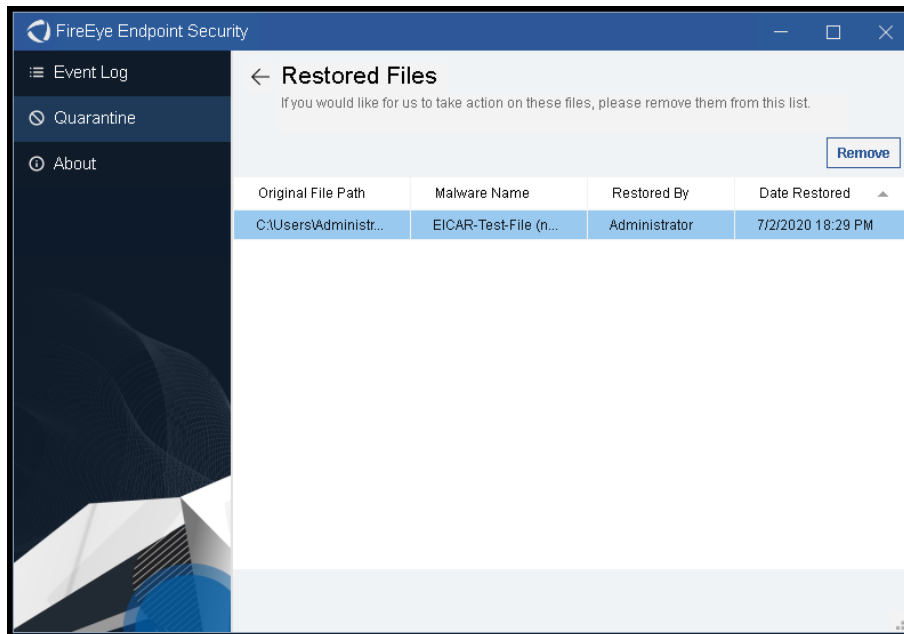


Figure 6 – Restored Files

Once a quarantined file is restored, the file details such as original file path and file hashes are maintained in the restored files list so that these files are no longer detected as malware. By clicking the **Remove** button, users can remove entries from the **Restored Files** list, thereby enabling the agent to again detect the file(s) as malicious. Removing a restored file from the list does not immediately cause the restored file to be detected. It will be detected when the file is accessed or modified subsequently either through real time scanning or an on-demand scan.

Note that restoring a file using the Endpoint Agent Console is only limited to endpoint (local system) and does not apply to any other endpoints managed by the HX server. Files in the **Restored Files** list can only be deleted using the Endpoint Agent Console and can't be overridden by the HX server. Hence caution should be exercised when enabling users to restore files on the endpoint.

Event Log

Event Log provides a list of events triggered on the endpoint (local system). These can be accessed by selecting **Event Log** on the left navigation pane as shown in Figure 7 below.

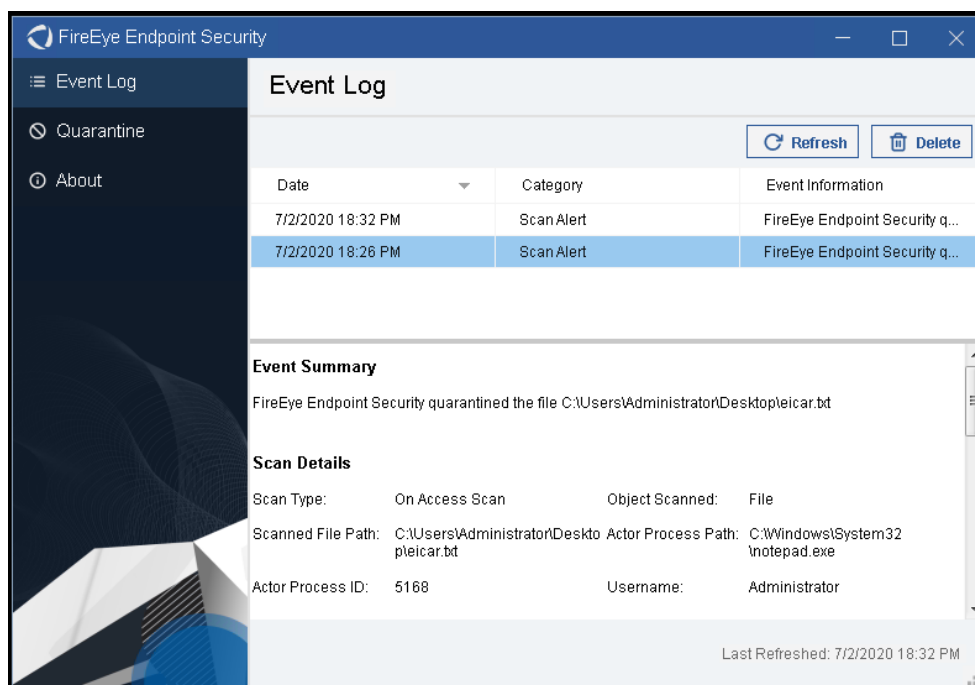


Figure 7 – Event Log

The list of events is locally maintained on the endpoint and do not interfere with events sent to the HX server. Clicking the **Refresh** button causes the content to be refreshed with new events, if any. Users can delete a single event or multiple events by selecting event(s) and clicking the **Delete** button. Deleting the events only deletes events from the endpoint (local system) and does not impact events sent to the HX server.

The current release of the Endpoint Agent Console module supports the following categories of events.

Category	Description
Scan Alert	Detection events from Malware Protection and Malware Guard
Scan Summary	Scan summary events of scheduled on demand scan.

Upon selection of any event, the bottom pane of the **Event Log** displays detailed meta data associated with the selected event. The meta data varies based on the category of the event as explained below.

Scan Alert Meta Data	Description
Scan Details	
Scan Type	Type of scan – On Access Scan, On Demand Scan
Object Scanned	Typically, a file object, but additional enhancements in scanners may result in the definition of new types
Scanned File Path	Path of scanned file
Actor Process Path	Path of the process that caused the file to be detected
Actor Process ID	Process identifier (PID)
Username	Username under which the event was detected
Action Details	
Actioned Object Type	Typically, a file object, but additional enhancements in scanners may result in the definition of new types
Actioned File Path	Path of file that was acted upon
System File	Indicates if the file was treated as a system file
File Size	File size
File Created	File creation time
File Modified	File modified time
File Last Accessed	Last accessed time
MD5/SHA1/SHA256 Hash	Different types of hashes
Requested Action	Action requested by policy
Applied Action	Action performed by scan engine
Result	Result of applied action
Engine Details	
Engine	Engine responsible for detection. It can be Antivirus or Malware Guard
Engine version	Engine version
Content Version	Content version at the time of detection
Malware Details	
Malware Type	Malware type as determined by engine
Malware Name	Malware name as determined by engine

Scan Summary Meta Data	Description
Scan Name	Scan name configured in HX server
Scan Type	Type of scan. Supported types are Quick scan, Full Scan, and Memory Scan
Number of Scanned Object(s)	Total number of scanned objects
Number of Infected Object(s)	Number of infected objects detected
Number of Actioned Object(s)	Number of objects acted upon by scanner
Start Time	Scan start time
End Time	Scan end time
Reboot Required	If any infected objects require reboot of the system to clean, this value will be set to True.

About

About provides version information of the installed FireEye Endpoint Agent as shown in Figure 8 below.

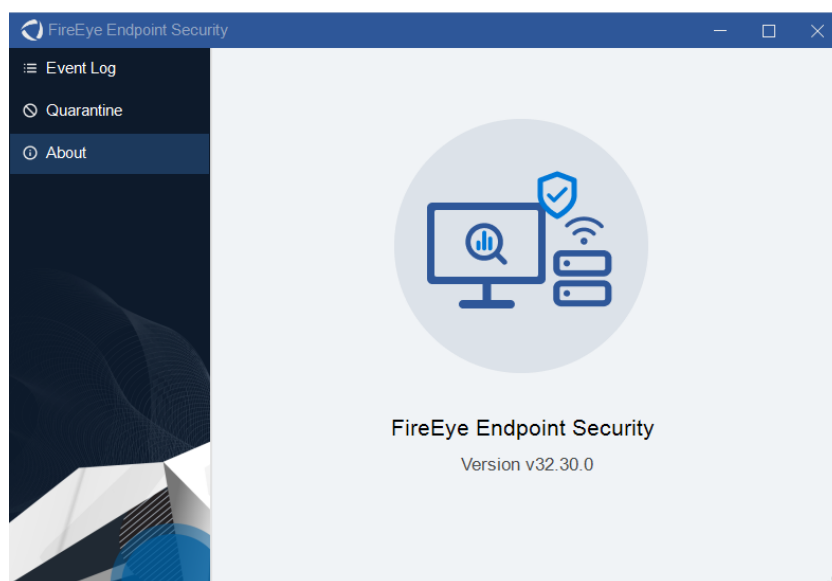


Figure 8 – About

About can be accessed by using the left navigation pane or by right clicking on the FireEye system tray icon and selecting **About**.

Agent Console Dashboard

The **Agent Console Dashboard** on the Endpoint Security Web UI displays user actions on the quarantined items as shown in in Figure 9. This page can be accessed by clicking on **HX Module Administration** under the **Modules** tab and then clicking on **Endpoint Agent Console**.

The screenshot shows the 'Endpoint Agent Console Dashboard' with a section titled 'Local Quarantine Actions'. It features a table with columns for Agent ID, Action, Object, Object Type, Threat, Hostname, User, Time, MD5, and SHA1. The table contains five rows of data, each representing a quarantine action performed on a file. The actions include 'delete' and 'restore' operations. At the bottom of the table, it indicates '5 record(s). Displaying 50 per page' and 'Showing page 1 of 1'.

Agent ID	Action	Object	Object Type	Threat	Hostname	User	Time	MD5	SHA1
rjH2xep6Hj1f1jg7e8B...	delete	C:\Users\qausen\Des...	file	EICAR-Test-File (not a ...	Win1019H1x64	qausen	2020-07-28T16:16:57.0...	44d88612fea8a8f36de82e1278abb02f	3395856ce81f2b7382dee72602f798b642f14140
rjH2xep6Hj1f1jg7e8B...	restore	C:\Users\qausen\Des...	file	EICAR-Test-File (not a ...	Win1019H1x64	qausen	2020-07-28T16:14:56.0...	44d88612fea8a8f36de82e1278abb02f	3395856ce81f2b7382dee72602f798b642f14140
rjH2xep6Hj1f1jg7e8B...	delete	C:\Users\qausen\Des...	file	EICAR-Test-File (not a ...	Win1019H1x64	qausen	2020-07-27T23:19:23.0...	44d88612fea8a8f36de82e1278abb02f	3395856ce81f2b7382dee72602f798b642f14140
rjH2xep6Hj1f1jg7e8B...	restore	C:\Users\qausen\Des...	file	EICAR-Test-File (not a ...	Win1019H1x64	qausen	2020-07-27T23:18:51.0...	44d88612fea8a8f36de82e1278abb02f	3395856ce81f2b7382dee72602f798b642f14140
rjH2xep6Hj1f1jg7e8B...	delete	C:\Users\qausen\Des...	file	EICAR-Test-File (not a ...	Win1019H1x64	qausen	2020-07-27T18:34:35.0...	44d88612fea8a8f36de82e1278abb02f	3395856ce81f2b7382dee72602f798b642f14140

Figure 9 – Endpoint Agent Console Dashboard

Agent Console REST API

The following API endpoints are provided by the Endpoint Agent Console module. These API endpoints center around the retrieval of events specific to the Endpoint Agent Console. To access other aspects that tie into Endpoint Security Server artifacts such as policies, refer to the FireEye document **Endpoint Security REST API Guide Release 5.0** for more details.

Endpoint	Purpose
/quarantine/actions	GET the record of quarantine actions performed via the Endpoint Agent Console
/quarantine/actions/export	GET the record of quarantine actions performed via the Endpoint Agent Console as CSV formatted data

Get Local Quarantine Actions

Returns record of quarantine actions from the Endpoint Agent Console database as a JSON result.

HTTP Verb	Route
GET	/hx/api/plugins/agent-console/v1/quarantine/actions

Query Parameters

Parameter	Notes
limit=<unsigned 32>	Limits the number of records returned. The default is 50.
offset=<unsigned 32>	Used for pagination. Returns the records starting at this offset. The default is 0.
sort=<text>	Sorts the results by the specified field and direction. Default is <code>id:ascending</code> . Valid Fields: <code>object</code> , <code>threat</code> , <code>hostname</code> , <code>user</code> , <code>time</code> Valid Directions: <code>ascending</code> , <code>descending</code>
filters=<filter list>	Specifies how to filter the records. The default is no filter. A filter is declared with the following keys and values: <pre>{ "operator": "eq", "field": "object_type", "arg": "file" }</pre> Where <code>field</code> may be any field belonging to a record, and <code>arg</code> is the value(s) to filter against. A complex filter can contain more than one filter as follows: <code>Filter=[{filter spec 1}, {filter spec 2}, ...]</code> Where the implied operation between filter specs is AND

Response

Key	Notes
total	Number of data rows available
data	List of rows, each as a key-value pair
offset	The offset requested
limit	The limit requested
filter	The filter requested
sort	The sort requested

Get Local Quarantine Actions, CSV Formatted

Returns record of quarantine actions from the Endpoint Agent Console database as a JSON result.

HTTP Verb	Route
GET	/hx/api/plugins/agent-console/v1/quarantine/actions/export

Query Parameters

Parameter	Notes
limit=<unsigned 32>	Limits the number of records returned. The default is 50.
offset=<unsigned 32>	Used for pagination. Returns the records starting at this offset. The default is 0.
sort=<text>	Sorts the results by the specified field and direction. Default is <code>id:ascending</code> . Valid Fields: <code>object, threat, hostname, user, time</code> Valid Directions: <code>ascending, descending</code>
filters=<filter list>	Specifies how to filter the records. The default is no filter. See section above for remaining details.
columns=<text>	A comma-separated list of record fields to include in the export. Default is all fields.

Response

The information that is returned is CSV formatted data. Each row of the CSV data is terminated by a newline. The first row is the column header row. Note that the column headers are representative of the text that is shown in the data grid. For example, field `agent_id` is returned as `Agent ID` because that is how it is represented in the Grid Area of the Web Interface.

APPENDIX A: Frequently Asked Questions

How to verify if the Agent Console installation succeeded?

Once the Endpoint Agent Console is installed and enabled, one can see a system tray icon with FireEye logo visible. Agent Console module reports its working status via agent info (aka system info on the HX) report as shown below.

```
"EndpointUIStatus": "running",
"EndpointUI": {
  "version": "1.1.0",
  "dotNetDependency": {
    "available": "1"
  }
}
```

If the `available` is "0" and the `EndpointUIStatus` shows as running, it means that the endpoint does not have .NET 4.0 or above for the Agent Console to display user interface. Installing .NET 4.0 will resolve this issue.

Are there any log files created during installation on the endpoint agents?

Endpoint Agent Console **agent module** creates log files under %TEMP% (Usually this is C:\Users\\AppData\Local\Temp), where <username> is the username of the logged in user. Depending on the scenario, the following files get created:

- endpoint_ui_install.log
- endpoint_ui_uninstall.log
- endpoint_ui_preupgrade.log
- endpoint_ui_upgrade.log

One can also refer to agent logs to find out if there are any installer messages related to plug-in installation.

Does the Agent Console generate any log file of its own?

In order to launch the Agent Console with logging enabled, it needs to be run with either `-l` or `-log` as a command line parameter. This needs to be followed by the log level. If no log level is passed in, the log level will be set to the lowest level (Error) by default. The log file is called `xagtui.log` and is also located under %TEMP% (Usually this is C:\Users\\AppData\Local\Temp)

The following are the log levels available to the Agent Console:

- **Error**: Used for program errors. If this log level is specified at the command line, only **Error** level messages will be logged.
- **Info**: Used for informational messages. If this log level is specified at the command line, only **Error** and **Info** level messages will be logged.
- **Debug**: Messages that contain information normally only of use when debugging a program. If this log level is specified at the command line, then all messages (**Error**, **Info**, and **Debug**) will be logged.

Is there a log on the HX appliance for the Agent Console server module?

You can find the log file under `/var/log/supervisor/agent-console-server_<version>_<unique_id>.log`

Since there is a dependency on .NET 4.0 on Windows platform, is there a way to know if Agent Console is running on all the deployed systems?

Agent Console plug-in reports the availability of .NET dependency in the agentinfo report. This can be verified using HX API for the given host.

What are the processes created when Agent Console is installed and enabled?

After successful installation following processes will be created.

- An instance of xagt.exe with *EndpointUI* in its command line. This is a container application to interact with agent services. This process runs under system account like any other agent instances.
- xagtui.exe, a GUI application, runs under each logged in user account.

I exited Agent Console using system tray exit menu option. How can I launch it again?

Agent Console can be launched by accessing shortcut from Windows Start Menu entry. If the agent console is already running (and hidden in system tray), launching it from start menu brings it to foreground.

Why do I see two FireEye icons sometimes? And does this lead to any functional issues?

You will see two icons (a) when there is a detection notification message, and (b) when there is a scheduled scan in progress and admin had enabled Pause/Cancel options to end user. This does not lead to any functional issues.

Why do I see error messages sometimes when Agent Console is in the foreground?

This can happen if a dependent service such as Malware Protection or remediation service is temporarily unavailable (content updates, etc.) During that time Agent Console will not be able to fetch data and hence it shows an error message. Please retry the operation in some time (few seconds) and things should work as expected.

Why do I see error message when I launch Agent Console using Start Menu shortcut?

Administrators can disable Agent Console module on host/hostsets. When disabled, Agent Console will not automatically launch during user logon sessions. If user attempts to launch it using Start Menu shortcut, it displays an error message.

I see multiple instances of xagtui.exe. Is this normal?

If the endpoint supports multiple user sessions, it is normal to see multiple instances of xagtui.exe. An instance of this application is launched for each user session.

What languages are supported in Agent Console?

Agent Console supports English, German, Italian, Portuguese/Brazilian, Japanese, Russian, Spanish, Korean, Chinese simplified, French, Polish, and Taiwan traditional.

Why does Malware Protection service get restarted when Agent Console module is uninstalled from the agent?

The Malware Protection component uses the Endpoint Agent Console components when available for sharing detection events and scan summary details. In order to properly unload and delete all the Endpoint Agent Console components, Malware Protection service is gracefully restarted.

Dependencies / Limitations / Known Issues

- This general availability release of Endpoint Agent Console is supported on Endpoint Security 5.0.0 with Endpoint Agent 32 running on Windows 7 and above only. Mac OS and Linux platforms are not supported as of this release.
- Features such as quarantine and restore require Malware Protection feature to be enabled on the endpoint.
- Users may see two FireEye system tray icons at times. This is as per the current design and does not cause any system performance overhead.
- Malware Protection service is restarted when Endpoint Agent Console is uninstalled. This is necessary to ensure clean uninstallation of Agent Console.
- Endpoint Agent Console requires Microsoft .NET 4.0 and above to run and display the user interface. Without this version of .NET, installation will succeed, but the Endpoint Agent Console system tray icon won't appear.

Refer to **Endpoint Agent Console Release Notes** for more details on known issues.