



**ENDPOINT SECURITY**  
**Endpoint Agent Console**  
**GA UPDATE RELEASE NOTES**  
**RELEASE 1.1.2**

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 © 2021 FireEye, Inc. All rights reserved.

Endpoint Security Agent Console Module

Software Release 1.1.2

Revision 1

**FireEye Contact Information:**

Website: [www.fireeye.com](http://www.fireeye.com)

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

**Phone (US):**

1.408.321.6300

1.877.FIREEYE

# Contents

- ANNOUNCEMENTS..... 4**
- FIREEYE CUSTOMER SECURITY BEST PRACTICES ..... 4**
- FEATURES ..... 5**
- INSTALLATION INSTRUCTIONS..... 5**
  
- BUG FIXES..... 7**
  
- KNOWN ISSUES..... 7**
  
- TECHNICAL SUPPORT..... 7**
  
- DOCUMENTATION..... 7**

# Announcements

Thank you for using this FireEye Product. This document provides an overview of the new features, resolved issues, and known issues in the FireEye Endpoint Security Agent Console 1.1.2 release.

## FireEye Customer Security Best Practices

Because our quality assurance process includes continuous security testing, FireEye recommends updating all FireEye products with the latest releases as soon as possible. As an overall strategy to reduce risk exposure, customers are also encouraged to follow best practices, which include:

- Always keep the product version up to date.
- Limit network access to the management interfaces of the appliance using firewalls or similar measures.
- Only issue accounts to trusted administrators.
- Use strong passwords.
- Monitor logs.
- Restrict physical access to the appliance to trusted administrators.

# Endpoint Agent Console

This release of Endpoint Agent Console is supported on **Endpoint Security 5.0.0** with **xAgent 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:** This release is supported on Windows platform only. It is not recommended to install Endpoint Agent Console release 1.1.2 on Endpoint Security Server 4.9.x with xAgent 31 or lower versions. This is not a supported scenario.

## Features

Endpoint Agent Console is an HX Innovation Architecture (IA) module designed to provide the end user with access to Endpoint Security Agent features through a local graphical user interface (GUI). This module provides insights into:

- Detected malware events
- Server scheduled scan(s) summary events
- Quarantined items
- Restore quarantined items
- Agent version information

For more details on usage of these feature see the Endpoint Security Agent Console module user guide.

## Installation Instructions

Endpoint Agent Console is an optional module available for **Endpoint Security 5.0.0** with **xAgent 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.

For more details on install and configuration see the Endpoint Security Agent Console module user guide, 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

**Note:** If you have non-Windows hosts, FireEye recommends that you exclude them from Endpoint Agent Console module install because the release 1.1.2 doesn't support mac OS and Linux platforms.

# Product Compatibility

This section describes the product compatibility for Endpoint Agent Console release 1.1.2

Agent Version	Endpoint Security Server Version	Operating System Requirements		
		Windows	macOS	Linux
32.0+	5.0+	Yes*	No	No

**Supported Windows operating systems:**

Windows 7, Windows 8, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019

\* Requires Windows 7 with .NET Framework 4.0 and above

## Bug Fixes

The following issues have been fixed in Endpoint Security Agent Console release 1.1.2.

- ENDPT-77594: Agent Console installation failure if PowerShell is disabled or not found on the target host.
- ENDPT-74249: A popup stating that *program is not responding for Agent Services* on some hosts during reboot only when running Agent Console.
- ENDPT-79361: Installation and upgrade failure workflow improvements.

## Known Issues

The following issues are known in Endpoint Security Agent Console release 1.1.2 and the relevant issue tracking numbers for each item are included in parentheses.

- New instance of Agent Console does not launch from Start Menu when xagtnotif GUI (Pause/Cancel Scan) is visible (ENDPT-63499). Work around is to close the xagtnotif window temporarily and launch Agent Console.
- Multiple detection events are displayed in Event Log page when Quarantine policy is disabled (ENDPT-51941). There is no functional impact, however Agent Console shows more than one entry in the current release.
- Quarantine notification can't be deleted on the HX UI if the user deletes a quarantined file on the agent (ENDPT-54621)

## Technical Support

For Technical Preview modules please send email to [EndpointTechPreview@fireeye.com](mailto:EndpointTechPreview@fireeye.com)

For General Availability modules, contact FireEye through the Support portal <https://csportal.fireeye.com>

## Documentation

Documentation for all FireEye products is available on the FireEye Documentation Portal (login required) <https://docs.fireeye.com>