EclecticIQ Intelligence at the core

Intelligence Hunting Response

Product name	EclecticIQ Endpoint Response Community Edition
Release version	3.5.1
Release date	May 11, 2022

TABLE OF CONTENTS

WHAT'S NEW

This release includes the following enhancements and features.

Role-based access

In this release, we have added two new roles:

- Administrator
- Analyst

As the name suggests, the administrator role has access to all features while the analyst role has access to limited features. Here are the tasks an analyst can perform:

- Browse hosts and review host information, such as properties, activity, policies, and configuration
- Download agent installers
- Browse, investigate, and resolve alerts
- Run live queries
- Review rules and threat intel licenses
- Upload YARA signatures
- Perform search, hunt, and carve operations

- Add notes to alerts (Any user assigned the Analyst role can add notes when reviewing alerts. Once added, these notes are visible to

all users.)

Single sign-on (SSO) support	Single sign-on (SSO) is an authentication method that allows you to use one set of credentials to login securely across various applications and websites. EclecticIQ Endpoint Response provides multi-user support by providing integration with the following identity providers. • OKTA • Ping Identity • Azure • One Login
Tags assignment during provisioning	When provisioning agents using the Client Provisioning Tool (CPT), you can assign tags or labels to the endpoints for improved categorization. These tags can be used later to define and assign specific policies for the categories. This feature is available for Windows, Linux, and macOS.
Network path monitoring	Starting with this release, you can monitor and track file and process activity for network paths. This feature is available only on the Windows operating system.
Granular control of network-related events	Starting with this release, you have higher control on network-related events and can choose to receive SSL (detailed or shallow), HTTP, and DNS events. This is possible due to the addition of the following parameters to the configuration: • custom_plgx_EnableDns • custom_plgx_EnableSSL • custom_plgx_EnableShallowSSL • custom_plgx_EnableHttp Refer to *EclecticIQ Endpoint Response Deployment Guide* for more information.
Activity metrics data	The Dashboard page on the web console for the EclecticIQ Endpoint Response server now includes the following new graphs. These graphs

offer valuable insight into the setup and help to take remedial actions, if needed.

- Hourly Client Incoming Data - Displays the volume of data (in bytes) received from all clients in the last four hours. Each point on the graph depicts data received within the hour.
- Hourly Client HTTP Requests Status - Displays the number of successful and failed requests received from the clients in the last four hours. Each point on the graph depicts requests received within the hour. Success indicates requests that were successfully received while failure represents requests that were not received successfully by the server or contained invalid information.
- Recent top 5 Hosts by Events - Lists the five hosts with the most events generated for the day (in UTC).
- Disk Usage - For a single or monolithic server, this graph depicts disk usage for the server. In a clustered setup, this graph depicts the disk usage for the server running the UI application.
- Requests Awaiting Processing - Displays the number of requests that are successfully received from the clients and are awaiting processing at the server.

Third-party component upgrade	In the 3.5.1 release, we have updated existing third-party libraries used by the EclecticIQ Endpoint Response server.
Scalability enhancements	This release includes multiple changes to improve product scalability. Refer to *EclecticIQ Endpoint Response Deployment Guide* for server scaling specifications and guidelines.

BUG FIXES

ER-531	Events for registry deletion (reg_delete) are missing from the win_registry_events table.
ER-1135	In some cases, the process GUID value is missing for some Windows defender events.

ER-1147	When running a basic load of 1000 connections per second on the Windows (2019, 2016 and 2012R2) operating system, CPU usage of 15-20% is observed.
ER-1148	During client installation, the installer copies files to the system32 folder before placing files in the Drivers folder.
ER-1149	When running a basic load of 1000 connections per second on the Windows operating system, some socket events for the endpoint are not logged by the EclecticIQ Endpoint Response client.
ER-1191, ER-1206, and ER-1207	Few security vulnerability issues were fixed for the Windows operating system.
ER-1254	If a filter for registry events is defined using the registry value, the filter does not work, and corresponding events are not generated. The filter works correctly if defined using the registry key.
ER-5064	A security vulnerability issue was fixed for the Linux operating system.

SUPPORTED BROWSERS

Here is the list of supported browsers.

- Chrome
- Firefox
- Safari
- Edge

For the best experience, we recommend that you use a resolution of 1366 x 768 or higher.

UPGRADE SUPPORT

Upgrade to the 3.5.1 version is supported only from EclecticIQ Endpoint Response Community Edition version 3.0.0 (release date May 20,2021).

SUPPORTED OPERATING SYSTEMS

The 3.5.1 release includes supports for the following operating systems.

Windows	32-bit		• Windows 7 SP1 (with this and this security update) • Windows 10
	64-bit		• Windows 2008 R2 SP1 (with this and this security update) • Windows 2012 • Windows 2012 R2 • Windows 2016 • Windows 2019 • Windows 7 SP1 (with this security update) • Windows 10 • Windows 11
Linux	64-bit	Amazon Linux	• 2 • 2018.03
		Centos	• 6.10 • 7.7.1908 (Core)
		Debian	• 8 (Jessie) • 10 (Buster)
		Kali	• 2021.1
		Linux Mint	• 20.1 (Ulyssa)
		Manjaro	• (21.0.3) GNOME
		MX Linux	• 19.4 • 21
		openSUSE	• 15-SP1 (with insserv-compat package installed) • 12-SP5
		Red Hat Enterprise Linux (RHEL)	• 6 • 8.0
		Ubuntu	• 14.04 LTS • 18.04 LTS

		• 20.04 LTS • 21.04 LTS
macOS	64-bit	• 10.15 (Catalina) • 11 (Big Sur) • 12 (Monterey)

KNOWN ISSUES

The 3.5.1 release includes the following known issues.

ID	*Affected platform*	*Description*
ER-526	Windows 10	On the Windows 10 operating system, running a query on the win_process_handles table may not give any results.
ER-906	Windows	Although a valid block rule is defined for the Windows operating system, copying files from USB flash drives, external hard disks and mobile phones to the local system is erroneously permitted.
ER-1137	Windows	In some cases, for performance reasons, MD5 or SHA256 values may not get reported in network path events.
ER-4404	Not applicable	After upgrading the EclecticIQ Endpoint Response server to the 3.5.1 version, any specified anti-virus engines with which to match the file hash (on the VirusTotal Configuration page) are not retained. **Workaround**: On the VirusTotal Configuration page, reselect the various anti-virus engines with which to match the file hash.
ER-4845	Windows	win_process_open events may be erroneously generated for System process (PID 4) even when appropriate exclude filters are applied.
ER-4937	Not applicable	The Sign In with Single Sign On (SSO) link on the login page or the EclecticIQ Endpoint Response server portal works for a user only after the user is added (on the User Management page) and SSO login is enabled for the user.

ER-4959	Windows	After you upgrade the EclecticIQ Endpoint Response server and client to the 3.5.1 version, events, if any, that were buffered based on the windows_events seeded query (in config) for hosts prior to upgrade are listed on the recent activity page for the host. This occurs because the windows_events query has been renamed to windows_real_time_events in the 3.5.1 release.
ER-5123	Windows	In some cases, the client memory keeps growing until the Maximum memory limit is reached and if the amsi scan option is enabled, events stop generating. **Workaround**: 1. Enable debug logging by setting the value of the custom_plgx_LogLevel option to 1 (in the client config). 2. Check agent logs for the string Amsi scan requested for: <byte_data> If byte_data is empty, the EclecticIQ Endpoint Response client was unable to read file bytes for amsi scanning. 3. Check the file write events for the relevant file name or process name. Note that for the event byte_stream field will be empty. 4. Check and update the file event filters in the client config with an appropriate exclude rule for the relevant file or process. 5. Apply the config and restart the EclecticIQ Endpoint Response client.
ER-5855	Not applicable	If you create a tag with special characters in its name, the tag is created, but the Page Not Found error is displayed when you try to view tag details.

CONTACT US

For enquiries and questions, you can contact support.