EclecticIQ Intelligence at the core

Intelligence Hunting Response

EclecticIQ Endpoint Response Community Edition Troubleshooting Guide

Version 3.5.1

May 2022

Table of contents

Getting started 5

Intended Audience 5

Troubleshooting server issues 6

Sign In with Single Sign On (SSO) link on the login page doesn't work 6

Unable to search for file paths 6

Defined filter is getting truncated on the client 6

Server UI is sluggish or stops responding, Hosts appear offline on the Hosts page 6

Browser times out when accessing the server UI 7

Existing agents are running fine but new agents are unable to connect to the server 8

Server showing very high RAM usage 8

Troubleshooting client installation issues 8

Invalid set of options provided 9

Invalid IP Address 9

No such host is known 9

Network Connectivity Check Error: Couldn't connect to server (Windows) 9

Downloading files from server failed (Windows only) 10

Invalid set of options provided 10

Failed to read server's public key from input file: <file name> 10

Error: Peer certificate cannot be authenticated with given CA certificates 10

Downloading files from server failed 10

Insufficient privileges. Need Administrator privileges to run the tool. 10

EclecticIQ Agent is already installed, please uninstall before proceeding. 11

Troubleshooting client uninstall issues 11

Invalid set of options provided. Either d or s should also be provided. (only for macOS and Windows) 11

Troubleshooting client upgrade issues 11

Error occurred in processing options 11

Troubleshooting other issues 12

Agent not responding and tasks from server UI fail 12

Live query results do not match events on Recent Activity page for an endpoint 12

Troubleshooting event-related issues 12
Events are not generated when absolute paths are used to define file and process filters for network paths 12
Monitoring system resources 12
Manually purge data 13
Running Diagnostics 13
Enabling agent debug logging 13
Restarting the server and endpoints 14
Restarting the complete server 14
Restarting a specific container on the server 14
Restarting services on an endpoint 15

Getting started

The EclecticIQ Endpoint Response platform is a sophisticated and flexible endpoint monitoring and response platform. It provides endpoint monitoring and visibility, threat detection, and incident response for Security Operating Centers (SOCs).

EclecticIQ Endpoint Response includes two primary components: server and client.

- The server receives, processes, and stores the data sent by the clients.
- The client is installed on each node and monitors all activity on the node.

Intended Audience

This document is intended to help diagnose and troubleshoot common issues you may face when using the EclecticIQ Endpoint Response server and client.

Troubleshooting server issues

Here are common errors encountered when working with the EclecticIQ Endpoint Response server.

Sign In with Single Sign On (SSO) link on the login page doesn't work

The Sign In with Single Sign On (SSO) link on the login page is enabled and works for a user only after the user is added and SSO login is enabled for the user.

Resolution: Configure SSO and add the relevant users. For more information, refer to the *EclecticIQ Endpoint Response Deployment Guide*.

Unable to search for file paths

On the EclecticIQ Endpoint Response server, when using the Search field in the Alerted Entry window (on the Alerts page), adding multiple backward slashes in the path does not yield any results. Similar behavior is observed when using the Search field in the View command window (on the Response Actions page).

Resolution: We recommend you use a single backward slash when searching for paths in the Alerted Entry or View Command window. For example, use *C:\Program Files\notepad.exe*.

Defined filter is getting truncated on the client

When creating, you can define a filter value longer that 260 characters on the server. However, the client retains only 259 characters and truncates the remainder.

Resolution: Ensure the length of each filter is not more than 260 characters.

Server UI is sluggish or stops responding, Hosts appear offline on the Hosts page

If the EclecticIQ Endpoint Response server is experiencing a high volume of requests, it may get sluggish or stop responding.

Resolution: Here are high-level steps to help you identify and resolve the issue.

1. Review the Requests Awaiting Processing graph on the Dashboard page of the server UI to ensure that requests are being processed timely and are not building up.
2. Check the CPU or RAM usage in your setup.
   Use the htop command line utility (on the Linux operating system) to interactively monitor the resources or processes in real-time. Using the htop command you can review available memory and processor cores, and which identify the process that are using the most system resources.

   In the htop output, check the Load Average value and ensure that it is not higher than 4.0 per core for an extended period. If the Load Average value is higher than 4.0, identify the processes hogging CPU usage in the htop output. Typically, these would be the Postgres or the Celery processes.

Review the log file (within the nginx container using the `docker logs <container ID>` command) to check the average time for the Celery process. The value should be under 10 seconds. If the value is more than 15 seconds, then you must take remedial actions, such as scale up your setup. Review the sizing guidelines in the *EclecticIQ Endpoint Response Deployment Guide* to ensure your setup is appropriate for your needs.

3. Review the filters defined in your setup.
   To optimize the configuration and reduce *noise*, identify known processes and trusted file and network activities in your setup and define corresponding filters. This will reduce the volume of received events, improve server and agent performance, and allow you to focus on malicious and suspicious activities. For more information, refer to the *Understanding Filters* section.

   Note: If you have access to a database UI client, such as PGADMIN, review the server dashboard and identify any queries that may be blocked. Contact EclecticIQ Endpoint Response support for further assistance.

4. Verify port 443 is open.
5. Verify that you are using the correct server URL.
6. Check disk usage and verify if sufficient space is available.

   ```
   df -h
   ```

7. Check the status of the various server containers.

   ```
   docker ps
   ```

8. Check if the containers up and running.
9. Verify the status of the nginx container.
10. Note the ID of the nginx container.
11. If the status of the nginx container is restarting, check the container log files.

    ```
    docker logs <container id>
    ```

    If the log contains a certificate-related error message, the possible cause could be a missing certificate. To resolve this issue, ensure certificate is available and then restart the nginx container. For more information, refer to the *EclecticIQ Endpoint Response Deployment Guide*.

12. If all containers are up and running, restart the nginx container.

    ```
    docker restart <container id>
    ```

Browser times out when accessing the server UI

If port 443 (used by the EclecticIQ Endpoint Response server) is not open, you may face issues accessing the server UI. Ensure TCP port 443 is open for inbound to the EclecticIQ Endpoint Response server.

Resolution: On the EclecticIQ Endpoint Response server, use the tcpdump utility (available on Ubuntu) to verify port connectivity. Tcpdump is a command line utility that allows you to capture and analyze network traffic going through your server.

1. SSH to the server and login with server root credentials.
2. Run the following command to verify if inbound traffic is reaching the server.

   ```
   tcpdump src port 443
   ```

tcpdump will begin capturing traffic and communication attempts with the server.

3. Run the following command from an endpoint to simulate traffic.

```
curl https://<server IP address or URL>
```

Ensure no firewall is blocking traffic between the endpoint and the server.
Here is the expected successful sample output.

```
https > 192.168.10.19.59704: Flags [R.], seq 0, ack 1, win 0, length 0
https > 192.168.10.19.59704: Flags [R.], seq 0, ack 1, win 0, length 0
9000 > 192.168.10.50.59986: Flags [R.], seq 0, ack 3377322019, win 0,
length 0
9000 > 192.168.10.50.59987: Flags [R.], seq 0, ack 2072158504, win 0,
length 0
```

Existing agents are running fine but new agents are unable to connect to the server

In some cases, you may be unable to provision new agents with a server, but existing provisioned agents work fine.

Resolution: Perform these high-level steps to identify the possible cause of the issue.

1. Check if the certificate is configured and available.

   For more information, refer to the EclecticIQ Endpoint Response Deployment Guide.

Note: If needed, you can regenerate the server certificate if there is a mismatch between the certificate on the server and application. Bear in mind that regenerating the certificate will require you to update the certificate for all existing agents.

2. Verify that the environment (.env) file (present in the installation location) is configured with relevant values for the parameters.

   For more information, refer to the *EclecticIQ Endpoint Response Deployment Guide*.

Server showing very high RAM usage

The EclecticIQ Endpoint Response server manages endpoint data at scale and to do so efficiently, it leverages Celery threads (version 4.1.1). Currently, Celery threads have a known issue (related to a memory leak) which can occur due to unpredictable reasons. While the root cause for this issue is being determined, if the server exhibits any unresponsiveness due to high RAM usage, use the following commands to restart the celery thread.

1. Open the maintenance port 5555 on the server.
2. Access the server (https://<IP address>:5555).
3. Log in with the default username and password.
4. Click on the celery worker.
5. From the drop-down list on the right, select Restart Pool.

Troubleshooting client installation issues

Here are common errors encountered when installing the EclecticIQ Endpoint Response client.

Invalid set of options provided

If you issue a command with incorrect flags with the -p option, the following error message is displayed.

Invalid set of options provided. Either of -i or -h is missing or incorrectly specified.

Resolution: Execute the command with correct flags.

Peer certificate cannot be authenticated with given CA certificates (Windows) Downloading files...Downloading files from server failed (Linux and macOS)

If you created the server certificate using the host name and issue a command to install using the IP address or vice versa, the following error message is displayed.

Peer certificate cannot be authenticated with given CA certificates (Windows)

Downloading files...Downloading files from server failed.(Linux and macOS).

Resolution: Execute the command with correct flags. If you created the server certificate using the IP address, then use the -i option for installation. Alternatively, if you created the server certificate using the host name, then use the -h option for installation.

Invalid IP Address

If you issue a command with incorrect server details, such as an invalid IP address, the following error message is displayed.

Invalid IP Address: <IP address>

Resolution: Execute the command with valid and accurate IP address.

No such host is known

If you issue a command with incorrect server details, such as invalid host name, the following error message is displayed.

No such host is known.

Resolution: Execute the command with correct server details.

Network Connectivity Check Error: Couldn't connect to server (Windows)

If you issue a command with incorrect server details, such as specify the IP address of the machine not running the EclecticIQ Endpoint Response server, the following error message is displayed.

Network Connectivity Check
Error: Couldn't connect to server.

Resolution: Execute the command with correct server details.

Downloading files from server failed (Windows only)

When using the -f option (force install without pre-install checks) if you issue a command with incorrect server details (unreachable or incorrect host name or IP address) the following error message is displayed.

Downloading files from server failed.

Resolution: Execute the command with the correct IP address or hostname using -i or -h option, respectively.

Invalid set of options provided

If you issue a command with incorrect options, such as without specifying the -k flag, the following error message is displayed.

Invalid set of options provided. -k is missing or incorrectly specified.

Resolution: Execute the command with the -k flag.

Failed to read server's public key from input file: <file name>

If you issue a command with an invalid certificate path, the following error message is displayed.

Failed to read server's public key from input file: <file name>.

Resolution: Execute the command with a valid certificate path.

Error: Peer certificate cannot be authenticated with given CA certificates

If you execute the command with an invalid certificate, the following error message is displayed.

Network Connectivity Check [Fail]
Error: Peer certificate cannot be authenticated with given CA certificates.

Resolution: Execute the command with a valid certificate.

Downloading files from server failed

If you execute the command with an incorrect certificate, the following error message is displayed.

Downloading files...Downloading files from server failed.

Resolution: Execute the command with a valid certificate.

Insufficient privileges. Need Administrator privileges to run the tool.

If you run a command without administrative privileges or relevant arguments, the following error message is displayed.

Insufficient privileges. Need Administrator privileges to run the tool.

Resolution: Execute the command with administrative privileges and needed arguments.

EclecticIQ Agent is already installed, please uninstall before proceeding.

If you try to install the endpoint agent when it is already installed, the following error message is displayed.

EclecticIQ Agent is already installed, please uninstall before proceeding.
Use plgx_cpt -u <d / s> option for uninstall

Resolution: Follow these steps to resolve the issue:

1. Use the CPT tool with -u option to uninstall the endpoint agent. For more information, see the *Uninstall the client* section in the *EclecticIQ Endpoint Response Deployment Guide*.
2. Execute the command to install the EclecticIQ Endpoint Response client with administrative rights and a valid certificate. For more information, see the *Installing the client* section in the *EclecticIQ Endpoint Response Deployment Guide*.

Troubleshooting client uninstall issues

Here are common errors encountered when upgrading the EclecticIQ Endpoint Response client.

Invalid set of options provided. Either d or s should also be provided. (only for macOS and Windows)

If you run a command without providing the relevant arguments with the -u flag, the following error message is displayed.

Invalid set of options provided. Either d or s should also be provided.

Resolution: Execute the uninstall command with the needed options.

Troubleshooting client upgrade issues

Here are common errors encountered when upgrading the EclecticIQ Endpoint Response client.

Error occurred in processing options

If you run a command without providing the relevant arguments with the -g flag, the following error message is displayed.

Error occurred in processing options.

Resolution: Execute the upgrade command with the needed options.

Troubleshooting other issues

Agent not responding and tasks from server UI fail

If CPU usage reaches 100% on an endpoint, the agent stops responding. Additionally, any tasks you may perform from the server UI may fail. For example, the live terminal may not display any results and may remain in processing state.

Resolution: Check CPU usage on the endpoint and identify processes hogging CPU.

Live query results do not match events on Recent Activity page for an endpoint

The EclecticIQ Endpoint Response agent pushes events to the server at regular intervals with 1024 events in each batch of query results. In cases where an endpoint is generating a high volume of events, there may be a lag before all events reach the server and you may find discrepancies between the Live query results and Recent Activity page for the endpoint.

Resolution: Execute a live query to view the most-recent data for the endpoint.

Troubleshooting event-related issues

Events are not generated when absolute paths are used to define file and process filters for network paths

On the Windows platform, events may not be generated if filters aren't defined correctly.

Resolution: When defining include or exclude filters for network paths (in the win_file_events section of the config), use an additional leading single slash in the target_path section. For example, to add a filter for *x.x.x.x**testfolder**testfile* specify *x.x.x.x**testfolder**testfile* in the target_path. Similarly, to define process filters in the win_process_events section, use the * character to prefix paths in the path section. For example, to define a filter for *x.x.x.x**testfolder**testfile.exe* specify **x.x.x.x**testfolder**testfile.exe* in the path.

Monitoring system resources

The EclecticIQ Endpoint Response server UI includes multiple dashboards to help you monitor system health and performance. Navigate to the Dashboard page of the server UI to review the available graphs and charts. These graphs and charts offer valuable insight into your operations and help you to take remedial actions, if needed.

- Platform Distribution - Displays the percentage and number of Windows, Linux, and macOS endpoints currently being managed by the server.
- Host Status - Indicates the percentage and number of hosts that are online and offline.
- 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.
- Top 5 Hosts by Alerts Generated - Lists the five hosts generating the highest number of alerts in your setup. Hover over a bar to know the alert count for the corresponding host.

- Top 5 Queries Generating Alerts - Lists the five queries generating the highest number of alerts in your setup. Hover over a bar to know the alert count for the corresponding query.
- Top 5 Rules Generating Alerts - Lists the five rules generating the highest number of alerts in your setup. Hover over a bar to know the alert count for the corresponding rule.
- Recent Top 5 Hosts by Events - Lists the five hosts with the most events generated for the day (in UTC).
- Hourly Client Data Volume - 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.
- Requests Awaiting Processing - Displays the number of requests that are successfully received from the clients and are awaiting processing at the server.

Manually purge data

By default, the EclecticIQ Endpoint Response database is purged every seven days. If needed, you can manually clean up the Postgres database.

Complete the following steps to purge the database:

1. Access the web interface for the server.
2. Navigate to Management > Data Purge.
3. Under Manual data purge, specify the number of days for which to retain data in the database.
4. Click Purge.

Running Diagnostics

Here are common diagnostic tools available to you when working with the EclecticIQ Endpoint Response server and client.

Enabling agent debug logging

By default, the logging level for endpoints is set to 3 to only log WARNING and ERROR events. In the event of a suspected issue or when troubleshooting problems, set the log level to DEBUG.

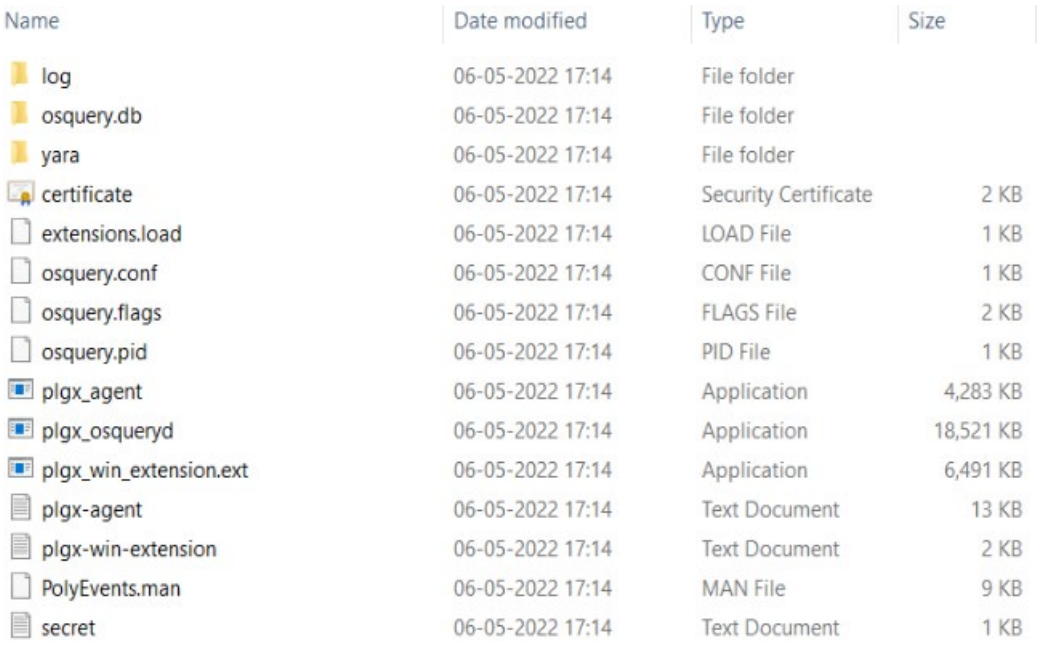
Complete the following steps to set the log level to DEBUG:

1. Log onto the EclecticIQ Endpoint Response server.
2. Navigate to the Config page.
3. Scroll to the Additional Config and Filters section and edit the value for the custom_plgx_LogLevel variable to 1.

On the endpoint, to review the:

- extension debug log, open the C:\Program Files\plgx_osquery\plgx-win-extension.log file.

- agent debug log, open the C:\Program Files\plgx_osquery\plgx-agent.log file.



Name	Date modified	Type	Size
log	06-05-2022 17:14	File folder	
osquery.db	06-05-2022 17:14	File folder	
yara	06-05-2022 17:14	File folder	
certificate	06-05-2022 17:14	Security Certificate	2 KB
extensions.load	06-05-2022 17:14	LOAD File	1 KB
osquery.conf	06-05-2022 17:14	CONF File	1 KB
osquery.flags	06-05-2022 17:14	FLAGS File	2 KB
osquery.pid	06-05-2022 17:14	PID File	1 KB
plgx_agent	06-05-2022 17:14	Application	4,283 KB
plgx_osqueryd	06-05-2022 17:14	Application	18,521 KB
plgx_win_extension.ext	06-05-2022 17:14	Application	6,491 KB
plgx-agent	06-05-2022 17:14	Text Document	13 KB
plgx-win-extension	06-05-2022 17:14	Text Document	2 KB
PolyEvents.man	06-05-2022 17:14	MAN File	9 KB
secret	06-05-2022 17:14	Text Document	1 KB

Restarting the server and endpoints

When needed, use the following information to restart the EclecticIQ Endpoint Response server and client.

Restarting the complete server

If for any reason you restart the EclecticIQ Endpoint Response server, perform these steps.

1. Login with the server root credentials.
2. Switch to the extracted zip folder.
3. Run the command.

```
docker-compose -p <project name> up -d
```

Note: Review the rabbitmq queues prior to restarting celery workers to ensure no data is lost.

Restarting a specific container on the server

Restarting the server restarts all micro services. If needed, you can restart a specific micro service for the EclecticIQ Endpoint Response server.

To restart a micro service, run the following command.

```
docker-compose -p <project name> up -d <container_id>
```

If you restart any container (except the nginx container), we recommend that you restart the nginx container using the above command.

Restarting services on an endpoint

Complete the following steps to restart services on an endpoint:

1. On the Windows endpoint, type services.msc in the Run dialog box and click OK.
2. Scroll and locate the EclecticIQ Agent Service entry.
3. Right click the service and click Restart.
4. Issue to following commands from a command window with administrative privileges to verify that other required services are up and running.

```
sc query vast
sc query vastnw
```