EclecticIQ Intelligence at the core

Intelligence Hunting Response

EclecticIQ Endpoint Response Product Guide

Version 4.0.0

October 2022

Contents

Getting started

EclecticIQ Endpoint Response is a comprehensive and extensible endpoint security platform for detection, monitoring, response, device management, and other IT security needs. It includes prepopulated detection rules (only in the Enterprise Edition), both custom and community-driven, aligned with MITRE ATT&CK framework. The platform is fed by comprehensive data from individual endpoints. Additionally, an open and extensible API allows for easy integration with your existing security stack and workflow.

Use cases

Here are a few of the possible use cases with the EclecticIQ Endpoint Response platform.

- Compliance (PCI, HIPAA)
- Digital forensics
- Asset and inventory
- Vulnerability management
- Host intrusion detection
- Performance and operational troubleshooting

Components

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 endpoint and monitors all activity on the endpoint. The EclecticIQ Endpoint Response client is based on osquery.

Product variants

EclecticIQ Endpoint Response is available in two variants.

- Enterprise Edition
- Community Edition

While the Enterprise Edition provides all features, the Community Edition provides limited features. The following features are not available in the Community Edition.

- Predefined or default rule sets
- Comprehensive and detailed investigative abilities
- Trend abilities or time line graph (on the Alerts page)
- Response capabilities
- Ability to execute scripts using a live terminal
- Security center tab (on the endpoint details page) displaying status of security products
- Ability to restart agents from the server UI

About the product

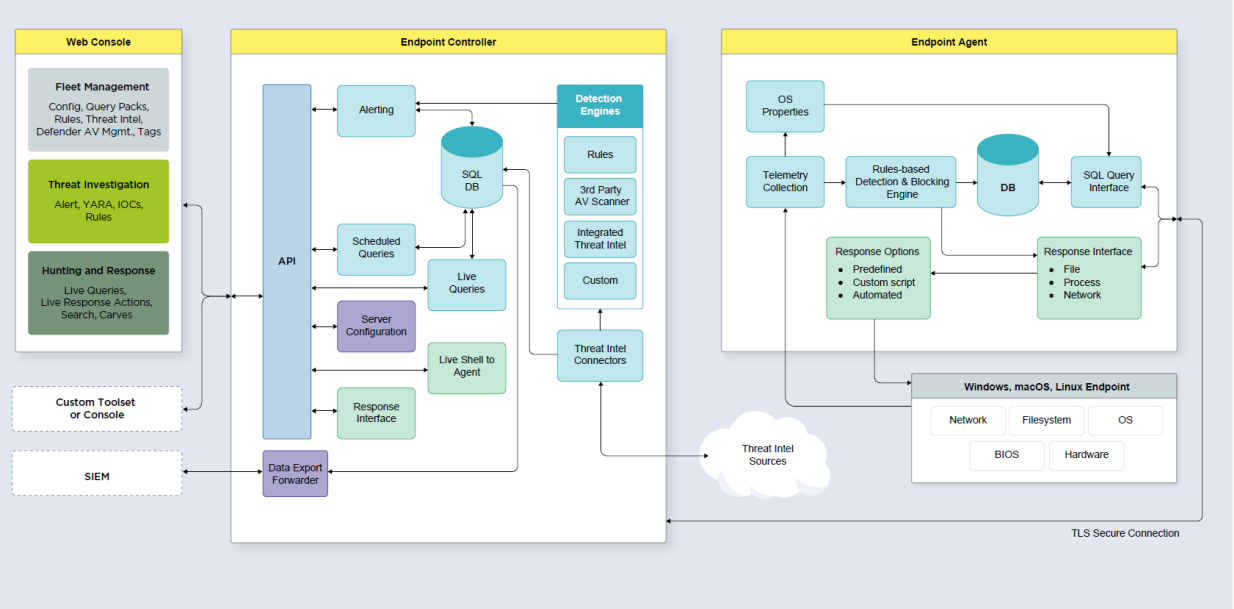
EclecticIQ Endpoint Response offers these capabilities.

Captures telemetry data from your endpoints.	The EclecticIQ Endpoint Response client captures a wide range of data and expands on the baseline osquery tables with custom extensions. EclecticIQ Endpoint Response extends the osquery agent on Microsoft Windows by adding visibility into real-time events. In effect, it

	leverages osquery capabilities and augments it further by using a proprietary extension that eliminates any visibility blind spots in the base osquery agent. The captured telemetry provides visibility to track file, process, users, registry, and network events for all endpoints in your environment.
Provides investigation and diagnostic features to help you deep dive into collected data (only in the Enterprise Edition).	Using the EclecticIQ Endpoint Response server, you can review data captured across your environment and configure specific rules to generate alerts. You can proactively perform hunts for knowns and unknowns in your environment and further investigate and diagnose, as needed. To efficiently triage incidents and activities, EclecticIQ Endpoint Response provides detailed contextual information for generated alerts.
Offers capability to respond to threats and possible attacks based on investigation (only in the Enterprise Edition).	The EclecticIQ Endpoint Response platform includes built-in and customizable response actions that work even during an active attack. Using response actions helps you to quickly isolate, diagnose, and rectify.

Architecture

Here is a high-level overview of the product architecture.



Note: Response-related features are available only in the Enterprise Edition and unavailable in the Community Edition.

How to use this guide?

This guide is divided into the following five sections:

- Getting started – Provides an overview of the product, its components and architecture, working, and features.
- Administration – Details the administrative tasks for the EclecticIQ Endpoint Response platform.

- Configuration – Describes the multiple methods available to configure the EclecticIQ Endpoint Response platform to ensure it captures relevant telemetry data for your needs and provides visibility into activities.
- Investigation – Explains the tools and methods available in the EclecticIQ Endpoint Response platform for investigation and diagnostics.
- Response – Details the type of actions you can take to response to possible threats in your environment (available only in the Enterprise Edition).

Intended audience

This document is intended for anyone who wants to use and maintain the EclecticIQ Endpoint Response platform. This guide is intended for customers using either edition (Enterprise Edition or Community Edition) of the EclecticIQ Endpoint Response platform.

Contact us

For enquiries and questions, you can contact support.

Administration

As an administrator, you can perform the following tasks to manage the EclecticIQ Endpoint Response platform.

- Manage users
- Manage tags
- Manage active hosts
- Manage removed hosts
- Specify data retention settings
- Define log level settings
- Download log files
- Purge data

Manage users

Only authorized users can login to the EclecticIQ Endpoint Response platform. After completing installation, you must add users and assign them roles to ensure they can perform relevant activities.

As an administrator, you can control users who have access to the EclecticIQ Endpoint Response server.

- Configure single sign-on (SSO) authentication
- Add users and assign roles
- Deactivate users
- Update user profile
- View user activity
- Reset passwords

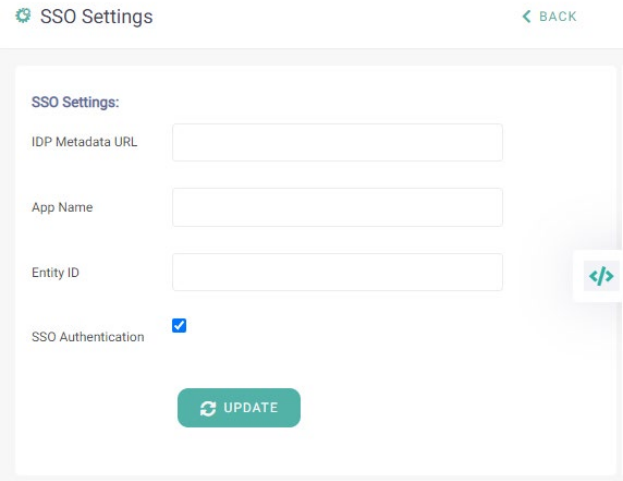
Configure single sign-on (SSO) authentication

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 integrating with various identity providers.

Perform these steps to configure SSO.

1. Access the web interface for the server.
2. Navigate to Settings > SSO Settings.

   The SSO Settings page is displayed.



3. Specify the URL for the identity provider.
4. Enter the application name.
5. Specify the entity ID.
6. Select the Enable option to activate SSO authentication.
7. Click Update to save your changes.

Understand roles

In the EclecticIQ Endpoint Response platform, two user roles are available: Administrator and Analyst.

As the name suggests, the administrator role has access to all features while the analyst role has access to limited features. A user assigned the analyst role can perform only the following tasks:

- Browse endpoints and review endpoint information, such as properties, recent activity, policies, and configuration
- Download client installers
- Browse, investigate (available only in the Enterprise Edition), and resolve alerts
- Execute live queries
- Review rules
- View configuration for threat intel sources
- Upload YARA signatures
- Perform search, hunt, and carve operations
- Add notes to alerts (a user assigned the Analyst role can add notes when reviewing alerts. Once added, these notes are visible to all users.) (available only in the Enterprise Edition)

Add users and assign roles

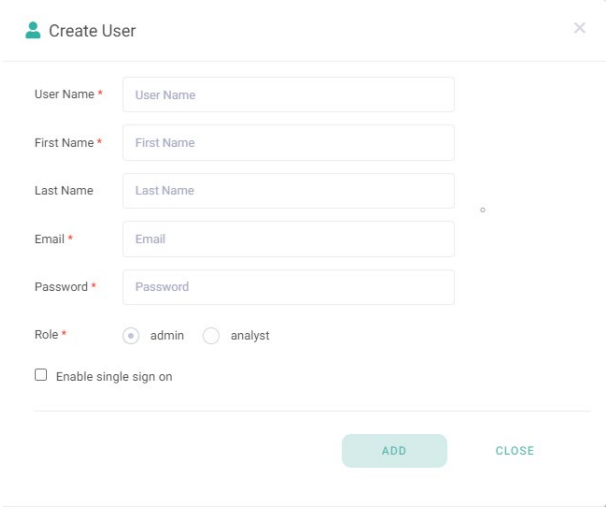
Perform these steps to add a user.

1. Access the web interface for the server.
2. Navigate to Settings > User Management.

   The Details tab is displayed.

3. Click Add User.

   The Create User dialog box is displayed.



4. Specify the user details, including the username, first name, and last name.
5. Enter the email ID.
6. Specify a password.
7. Assign a role to the user – Administrator or Analyst.
8. Select the Enable SSO Login to enable SSO authentication for the user.
9. Click Add.

   You are returned the User Management page where a message box indicates if the user is successfully added.

Deactivate users

When using EclecticIQ Endpoint Response, you can deactivate a user account to prevent the user from accessing the EclecticIQ Endpoint Response server.

Perform these steps to deactivate a user account.

1. Access the web interface for the server.
2. Navigate to Settings > User Management.

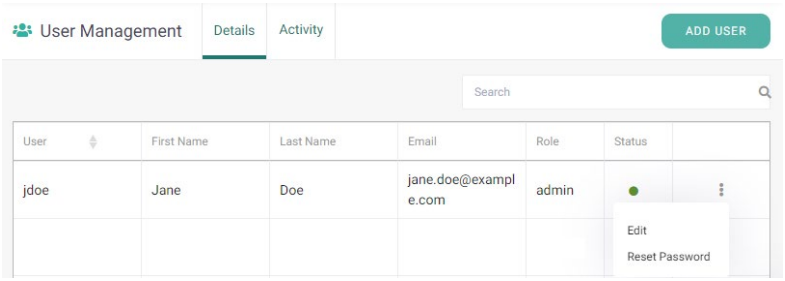
   The Details tab is displayed.

3. Use the Search field to locate a specific user.

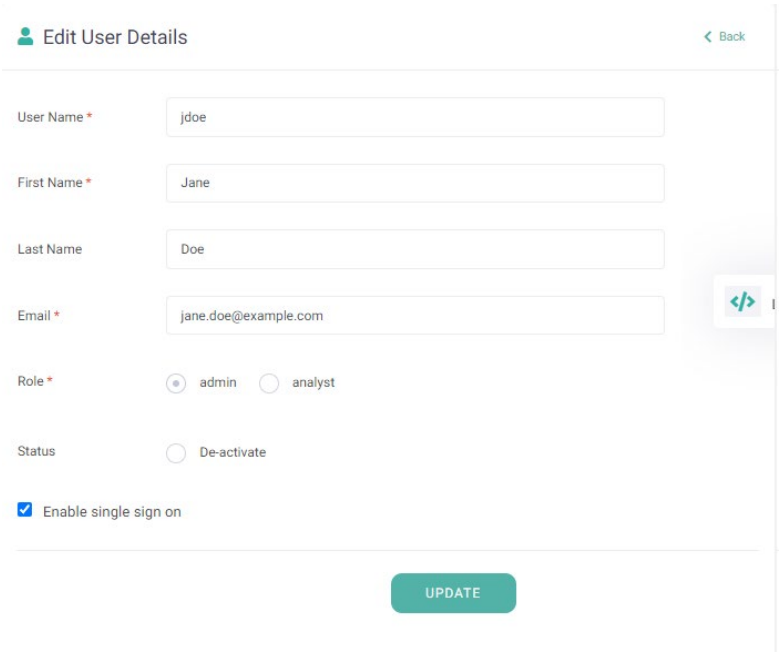
   You can find user details based on the user name, first name, last name, email, and role.

4. Click the Action drop-down list for the user to deactivate.

5. Select Edit.



6. On the Edit User details page, select De-activate for the Status field.



7. Click Update.

The associated user account is deactivated.

If needed, you can restore a deactivated host. For more information, see Manage removed hosts.

Update user profile

If needed, you can edit details for an existing user account.

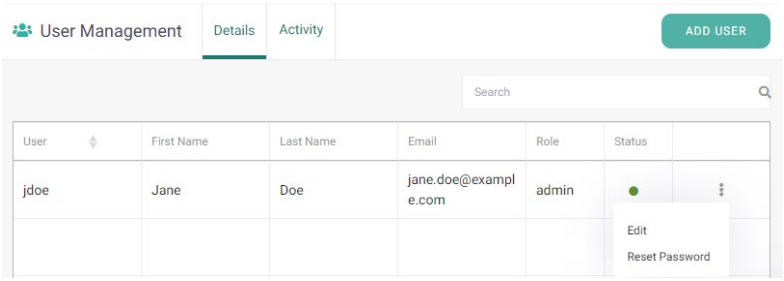
Perform these steps to update a user account.

1. Access the web interface for the server.
2. Navigate to Settings > User Management.

   The Details tab is displayed.
3. Use the Search field to locate a specific user.

   You can find user details based on the user name, first name, last name, email, and role.
4. Click the Action drop-down list for the user.

5. Select Edit.



6. On the Edit User details page, update the needed details.
7. Click Update.

The associated user account is updated.

Note: A logged in user can edit their first name and last name by selecting to the User Profile option on the web server.

View user activity

EclecticIQ Endpoint Response can track activities for each authorized user.

To view recent user activity, perform these steps.

1. Access the web interface for the server.
2. Navigate to Settings > User Management.

   The Details tab is displayed.
3. Switch to the Activity tab.
4. Review the recent user activity.
5. Optionally, use the Search field to identify changes made by a specific user or to a specific endpoint.

Reset passwords

You can reset the password for a user.

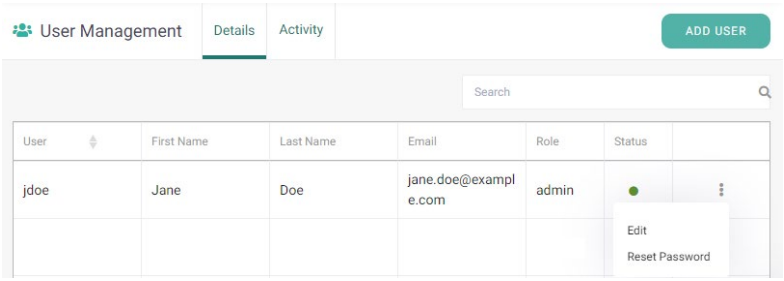
Perform these steps to reset the password for a user account.

1. Access the web interface for the server.
2. Navigate to Settings > User Management.

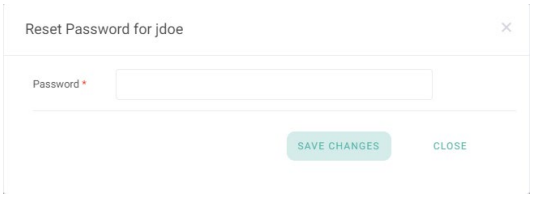
   The Details tab is displayed.
3. Use the Search field to locate a specific user.

   You can find user details based on the user name, first name, last name, email, and role.
4. Click the Action drop-down list for the user.

5. Select Reset Password.



6. In the Reset Password for <user> dialog box, specify the new password.



   Ensure the password is at least eight characters long and contains one uppercase letter, one lowercase letter, one digit, and one special character.

7. Click Save changes.

The password for the user account is reset.

Manage tags

A tag is a unique identifier that helps you logically group objects, such as endpoints, queries, and packs. You can define a tag, assign it to the relevant endpoints, and then assign the same tag to appropriate queries and packs to associate the queries and packs with that specific group of endpoints.

For example, to categorize endpoints based on the department, you can define tags, such as Sales, HR, Accounting, IT, Legal, and Finance. After you assign the ***Legal*** tag to all endpoints in the Legal department, you can assign the same tag to specific queries or packs that are relevant for the Legal group.

Alternatively, you can create tags to classify queries and packs and then assign those to relevant endpoints. For example, you can define and assign tags to categorize packs based on specific goals, such as DLL injection detection, IT compliance, or Vulnerability Management. You can then assign the same tags to endpoints on which to monitor these specific activities based on the goals.

As an administrator, you can manage the tags for your environment.

- Create and assign new tags
- Create new tags
- Assign existing tags
- Delete tags

Guidelines for tags

Review these guideline before creating tags.

- Define meaningful tags names.
- Use a combination of uppercase letters, lowercase letters, numbers, and special characters in tag names.
- Spaces and commas (,) are not allowed in tag names .
- Only the underscore (_), hyphen (-), @ (a sign) and period (.) special characters are allowed in tag names.

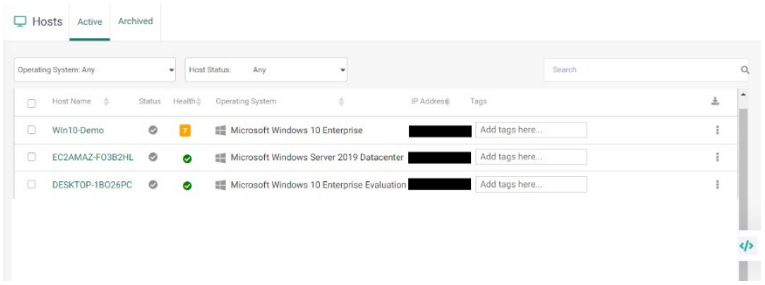
Create and assign new tags

In the EclecticIQ Endpoint Response platform, using the Hosts, Queries, and Packs pages you can create and assign a new tag to an endpoint, query, or pack.

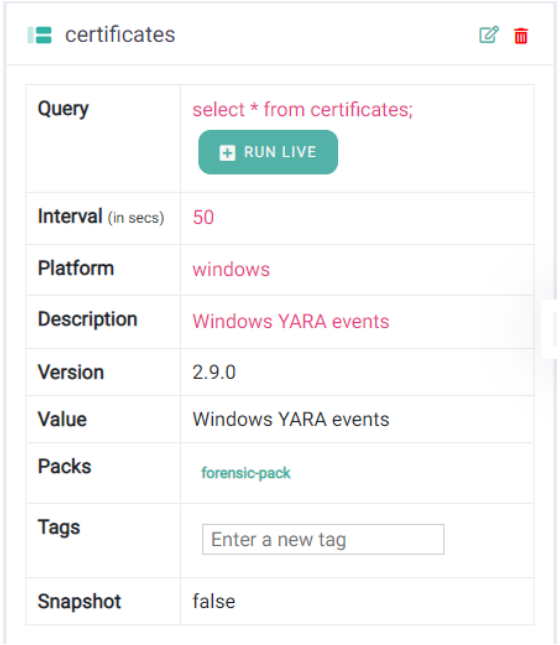
Perform these steps to define new tags using the Hosts, Queries, and Packs page.

1. Access the web interface for the server.
2. Navigate to Hosts, Host Configuration > Queries, or Host Configuration > Packs page.
3. Select the needed endpoint, query, or pack.
4. Create and assign the new tag to the object.

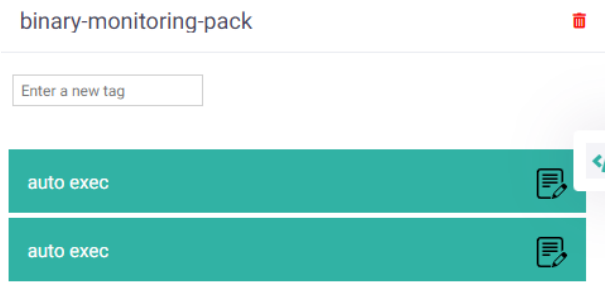
- On the Hosts page, specify the tag name in the Tags field in the Add tags here text box and click Enter.



- On the Queries page, specify the tag name in the Enter a new tag text box and click Enter.



- On the Packs page, specify the tag name in the Enter a new tag text box under the pack name and click Enter.



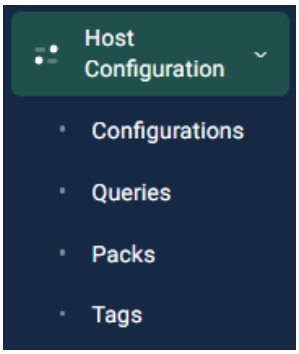
The new tag is assigned to the endpoint, query, or pack and is also listed on the Tags page. You can now assign this tag to additional endpoints, packs, and queries, as needed.

Create new tags

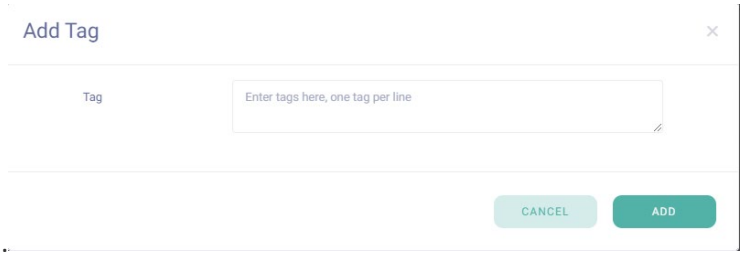
In the EclecticIQ Endpoint Response platform, you can create tags using the Tags page. When using the Tags page, the tag is only created and not assigned to any object. You must manually assign the tag to relevant endpoints, packs, and queries.

Perform these steps to define new tags using the Tags page.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Tags.



3. On the Tags page, click Add Tag.



The Add Tag window is displayed.

4. Specify the tag name and click Add.

   A success message box is displayed, and the new tag is listed on the Tags page.

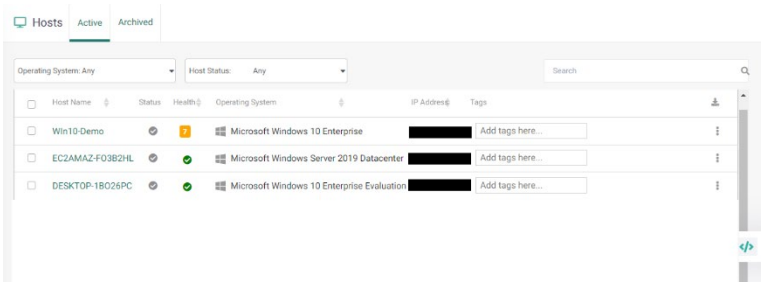
Assign existing tags

You can assign existing tags to endpoints, queries, and packs using the Hosts, Queries, and Packs page, respectively.

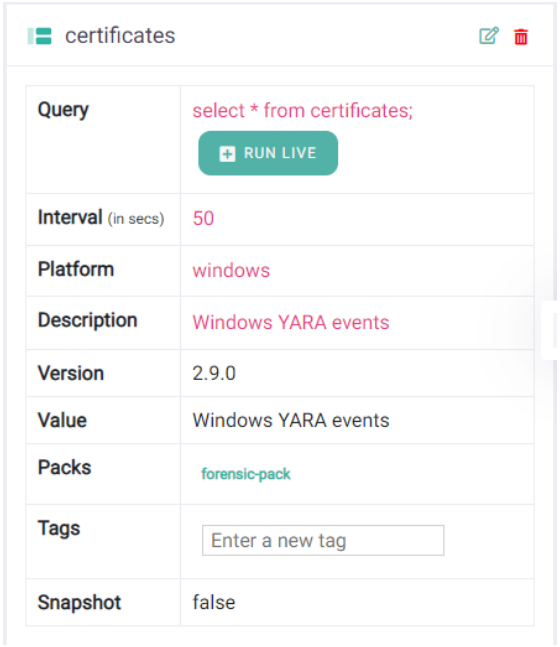
Perform these steps to assign existing tags using the Hosts, Queries, or Packs page.

1. Access the web interface for the server.
2. Navigate to Hosts, Host Configuration > Queries, or Host Configuration > Packs page.
3. Select the endpoint, query, or pack to which to assign the tag.
4. Specify the tag to assign to the endpoint, pack, or query.

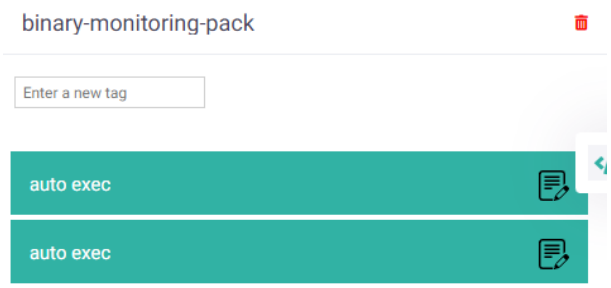
- On the Hosts page, specify the tag name in the Tags field in the Add tags here text box and click Enter.



- On the Queries page, specify the tag name in the Enter a new tag text box and click Enter.



- On the Packs page, specify the tag name in the Enter a new tag text box under the pack name and click Enter.

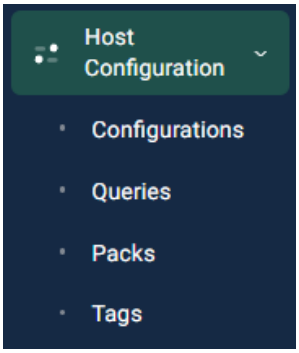


The existing tag is assigned to the endpoint, query, or pack. Be careful when typing the tag name, an error in spelling can result in creation and assignment of a new tag (based on the misspelling).

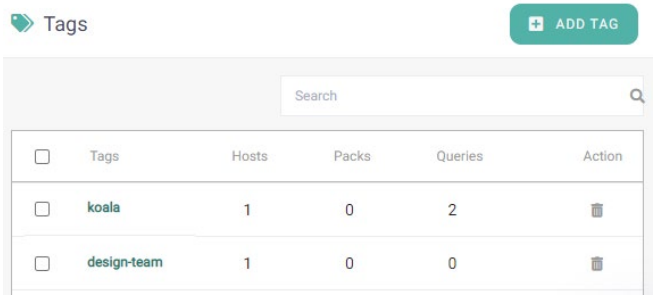
Delete tags

You can delete tags that are no longer relevant. Perform these steps to delete tags.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Tags.



3. On the Tags page, navigate to the tag you need to delete.
4. Optionally, find a specific tag using the Search field by specifying the tag name.
5. Click Delete for the tag.



A confirmation dialog prompts you to confirm the action.

6. Click OK.

   A success message box is displayed, and the tag is removed from the Tags page.

Manage active hosts

You can manage active hosts or endpoints using the Hosts page.

- View or assign config
- Assign tags
- Remove hosts

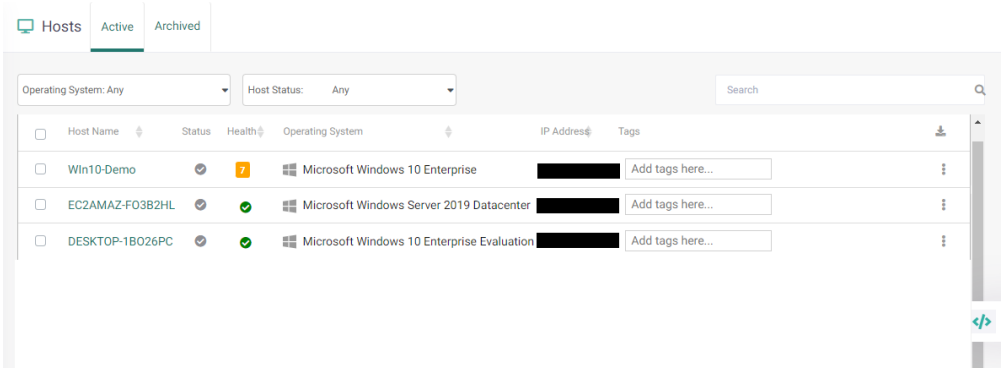
View or assign config

At a time, only one config can be assigned to an endpoint. You can choose to retain the default config for an endpoint or assign a new config based on your needs.

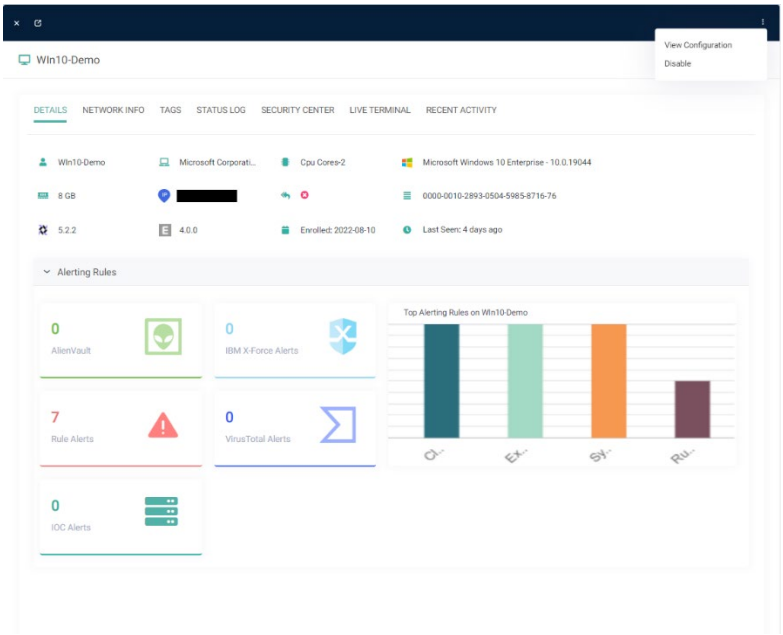
Perform these steps to manage the config for an endpoint.

1. Access the web interface for the server.
2. Click Hosts in the navigation pane.

   The Hosts page lists all managed endpoints.

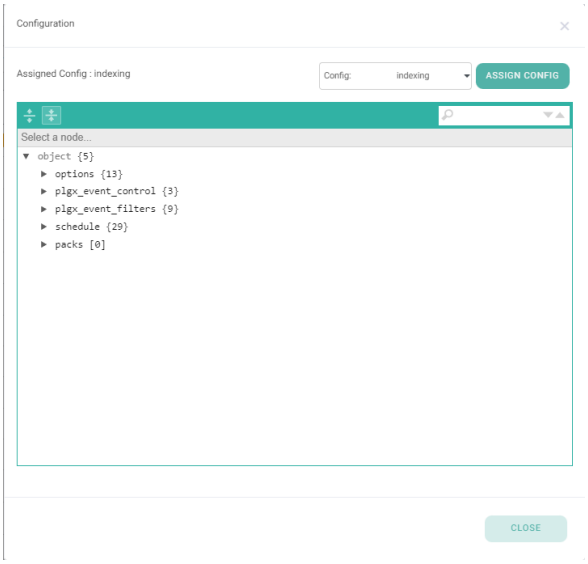


3. For an endpoint, click the ellipsis icon and select View Configuration.



   The Configuration window displays the name and details of the config assigned to the endpoint. The Assigned Config field denotes the current config assigned to the endpoint.
   Note: The Response Action status (visible in the graphic) is available only in the Enterprise Edition.

4. Review the details of the assigned config.



Use the expand and collapse buttons to view and hide config details, as needed.

5. To assign a new config to the endpoint, select the config from the drop down and click Assign config.

The selected config is assigned to the endpoint and a confirmation message is displayed.

6. Click OK in the message box.

Assign tags

You can create and assign new tags or assign existing tags to endpoints using the Hosts page. For more information on assigning tags to endpoints, see Manage tags.

Note: You can also assign tags to endpoints when provisioning the endpoints with the client using the EclecticIQ Endpoint Response Client Provisioning Tool (CPT). Use the -j option with the CPT tool to assign tags. For more information on the CPT options, see the *EclecticIQ Endpoint Response Deployment Guide*.

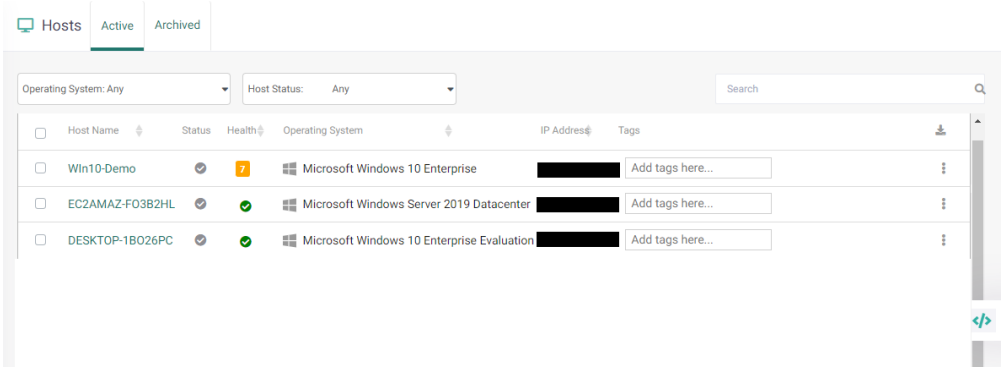
Remove hosts

If needed, you can remove a host or endpoint from the Hosts page.

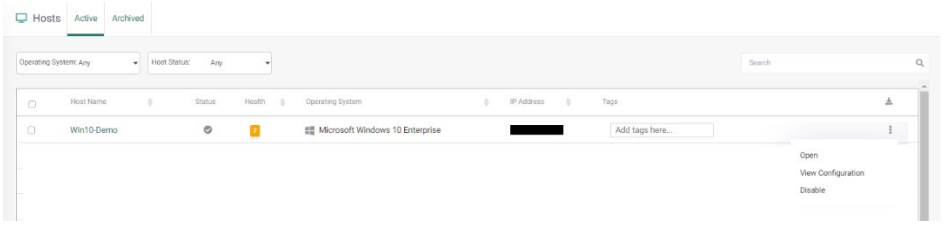
Perform these steps to remove an endpoint.

1. Access the web interface for the server.
2. Click Hosts in the navigation pane.

   The Active tab of the Hosts page lists all managed endpoints.



3. Select options from the Operating System and Host Status drop-down lists to view relevant endpoints.
4. Navigate to the row for the endpoint to delete.
5. For an endpoint, click the ellipsis icon and select Disable.



   A confirmation dialog is displayed.

6. Click Yes, Remove it to confirm.

   A message box is displayed, and the endpoint is removed from the Active page and moved to the Archived page.

Manage removed hosts

All hosts or endpoints removed from the Active page are displayed on the Archived page. Using this page, you can either permanently delete the endpoints or restore endpoints back to the Active page.

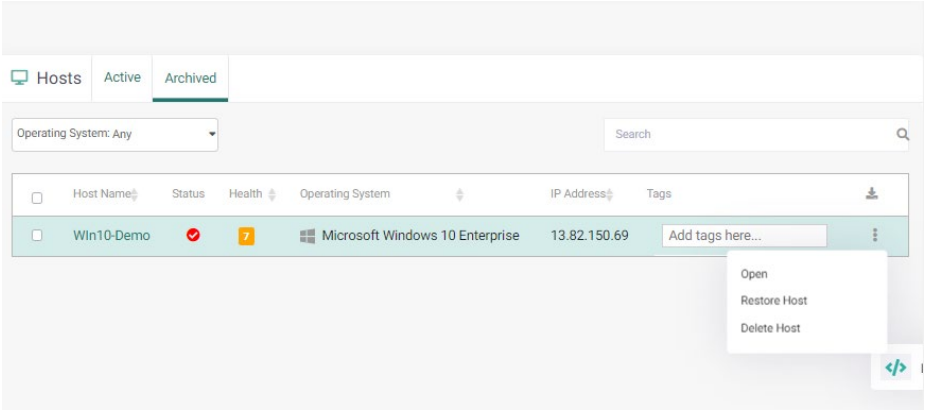
Delete hosts

Perform these steps to permanently delete archived endpoints.

1. Access the web interface for the server.
2. Navigate to Hosts > Archived.

   All endpoints removed from the Active page are listed on the Archived page.

3. For an endpoint, click the ellipsis icon and select Delete Host.



   A confirmation dialog is displayed.

4. Click OK in the dialog.

   A success message is displayed, and the endpoint is deleted.

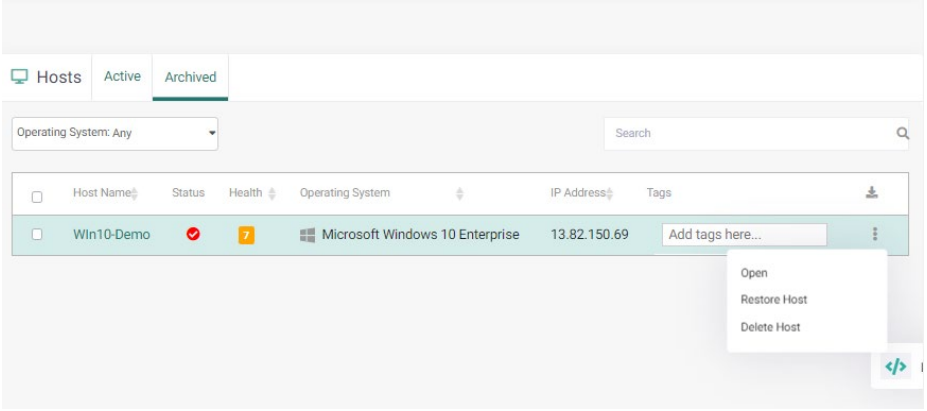
Restore hosts

Perform these steps to restore removed hosts or endpoints.

1. Access the web interface for the server.
2. Navigate to Hosts > Archived.

   All endpoints removed from the Active page are listed.

3. For an endpoint, click the ellipsis icon and select Restore Host.



   A confirmation dialog is displayed.

4. Click Yes, Restore it in the dialog.

   A success message is displayed, and the endpoint is restored.

Specify data retention settings

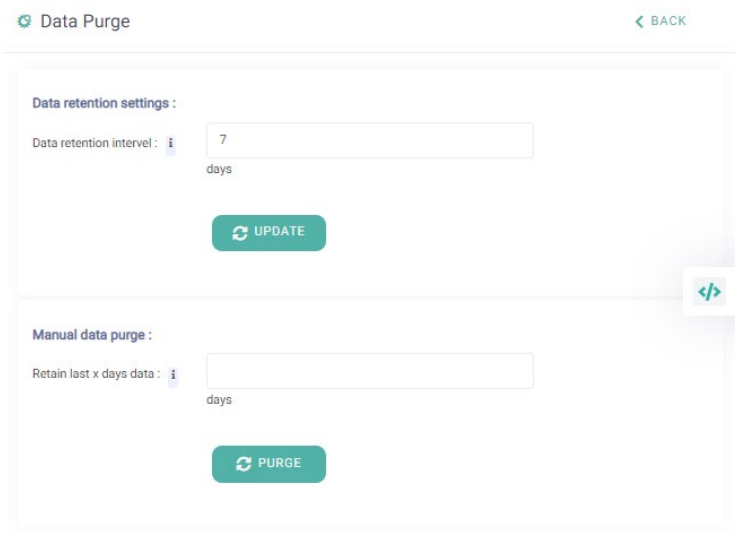
By default, the EclecticIQ Endpoint Response database is purged every seven days. All data for alerts, scheduled query results, status logs, and deleted endpoints is purged.

If needed, you can edit the default value and specify how long data is retained in your environment.

Note: Extending the data retention period can impact your sizing needs. Evaluate sizing requirements before configuring extended data retention periods.

Perform these steps to specify data retention setting for your environment.

1. Access the web interface for the server.
2. Navigate to Settings > Data Purge.
3. Under Data retention settings, specify the number of days for which to retain data in the database.



4. Click Update.

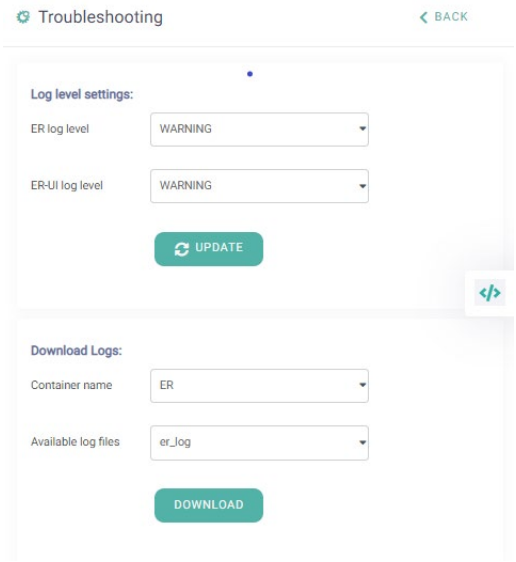
Define log level settings

By default, log level is set to Warning for the EclecticIQ Endpoint Response platform. If needed, you can change the log level setting based on your needs.

Perform these steps to specify log level settings.

1. Access the web interface for the server.
2. Navigate to Settings > Troubleshooting.

   The Troubleshooting page is displayed.



3. In the ER log level drop-down list, select a value to set the log level for the plgx-esp_plgx-esp micro service.

   This service of the EclecticIQ Endpoint Response server processes requests coming from the EclecticIQ Endpoint Response clients.

4. In the ER-UI log level drop-down list, select a value to set the log level for the plgx-esp_plgx-esp-ui micro service.

   This service of the EclecticIQ Endpoint Response server takes actions, such as modify properties of an endpoint.

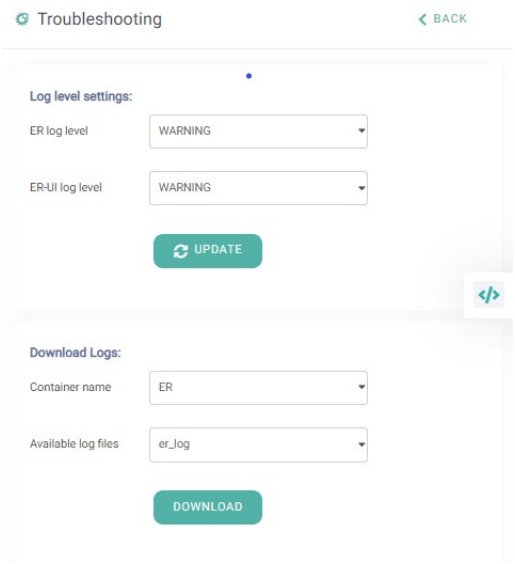
5. Click Update.

Download log files

The EclecticIQ Endpoint Response server saves log files that can be downloaded and examined for troubleshooting and diagnostic purposes.

Perform these steps to specify log level settings.

1. Access the web interface for the server.
2. Navigate to Settings > Troubleshooting.
3. The Troubleshooting page is displayed.



4. Select a value from the Container name drop-down list.

   You can download log files for the plgx-esp_plgx-esp and plgx-esp_plgx-esp-ui micro services of the EclecticIQ Endpoint Response server.

5. Select the file to download.

   The latest log file is named log. A new file is created when the size of the current log file reaches 10 MB. To ease identification, old log file names are suffixed with time and date.

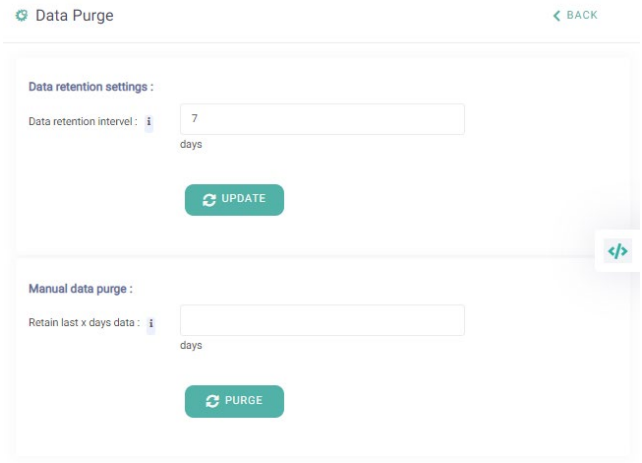
6. Click Download.

Purge data

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

Complete the following steps to purge the database:

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



4. Click Purge.

Regenerate server certificate

The server certificate created during initial installation is valid for 1 year. You must periodically check the certificate validity and regenerate the certificate prior to expiry.

Here are the steps you can perform to update the certificate.

1. Generate a new certificate on the server.
   a. Remove the certificate.crt file and private.key file from the eiq-er/nginx folder.
   b. Create a new certificate.

   ```
   .sh certificate-generate.sh <server IP/host name>
   ```

2. Copy the new certificate to the resources folder.

   ```
   cp nginx/certificate.crt resources/updated_certificate.crt
   ```

3. Perform one of the following steps.

For the Enterprise Edition	Update the certificate on the endpoints by creating needed Response Actions. a. Access the web interface for the server. b. Navigate to Response Action. c. The Send Response Action to Agent page is displayed. d. Switch to the Custom Action tab. e. Enter the script name. f. Select one of the following predefined scripts. ○ plgx_win7_agent_cert_update_3.5.0.ps1 (for Windows7 and Windows 2008 R2)

	○ plgx_win10_agent_cert_update_3.5.0.ps1 (for all versions except Windows7 and Windows 2008 R2) ○ plgx_win7-10_agent_cert_update_3.5.0.bat (for all Windows versions) ○ plgx_linux_agent_cert_update_3.5.0.sh ○ plgx_mac_agent_cert_update_3.5.0.sh Before running a seeded script, update the relevant information in script based on your needs. You must provide the IP address of the server and location of the new certificate. Review the time window after which the scheduled task is created (default is 2 minutes).
For the Community Edition	a. Download the certificate.crt from server. b. Copy the downloaded certificate.crt to C:\Program Files\plgx_osquery. c. Restart the plgx_agent service.

Exercise caution when updating the certificate. You must ensure the scheduled task is well-timed and reaches the agent before you the update the certificate for the server. In effect, to ensure uninterrupted communication the server certificate must be updated before the certificate on the endpoints is updated.

Note: If for some reason, the certificate on the agent is replaced before the server certificate is updated, the agent will be unable to communicate with the server. This will cause the host to appear as degraded or offline and can possibly result in data loss. To correct this, you must manually restart the service on the EclecticIQ Endpoint Response agent.

4. Update the certificate on server by restarting the plgx-esp_nginx micro service.

```
sudo docker-compose restart <container name or container ID>
```

Configuration

The EclecticIQ Endpoint Response platform is a powerful tool that offers multiple ways to configure it to capture relevant telemetry data for your needs. You must configure the platform judiciously to ensure you capture relevant data from the endpoints, create appropriate rules that and generate alerts to stay informed on activities of interest.

Agent configuration flags

After the EclecticIQ Endpoint Response client is provisioned, the default and seeded configuration comes into play. These configured values are passed to the endpoint agent during client provisioning through the osquery.flags file. The file includes various parameters needed for osquery initialization and functioning. By default, this file is stored in the:

- C:\Program Files\plgx_osquery folder for Windows
- /etc/plgx_osquery directory for Linux
- /usr/local/etc/plgx_osquery/osquery.flags for macOS (Enterprise Edition) and private/var/osquery.flags for macOS (Community Edition)

Although this file contains all the flags supported by osquery, in this section we will only review the key flags relevant for the EclecticIQ Endpoint Response platform. We recommend that you DO NOT change the default settings for any of the flags.

Note: If needed, you can update the parameters to configure the deployment environment to meet your specific needs. Note that modifying these values may significantly alter the performance of the EclecticIQ Endpoint Response agent. *If you choose to edit any flag in the osquery.flags file, you **must** stop the agent, make the changes to the flags file, and restart the agent to ensure the changes come into effect.*

Flags	***Description***	***Operating system***
disable_watchdog=false watchdog_level=0 watchdog_memory_limit=0 watchdog_utilization_limit=0 watchdog_delay=300	These flags help manage osquery daemon memory and CPU utilization and define performance limits. For more information on these flags, see this article.	All
config_plugin=filesystem (only for Enterprise Edition)	These flags control the configuration by identifying the filesystem as the config source and specifying the	All

config_plugin=tls (only for Community Edition) config_path=C:\program files\plgx_osquery\ osquery.conf (for Windows for Enterprise Edition) config_path=/etc/plgx_osquery/ osquery.conf(for Linux for Enterprise Edition) config_path=/usr/local/etc/plgx_osquery/ osquery.conf (for macOS for Enterprise Edition) config_path=/private/var/osquery (for macOS for Community Edition)	location of the EclecticIQ Endpoint Response config file. We recommend you DO NOT change these values.	
logger_plugin=tls	This flag allows you specify the type of logging. For more information, see this article.	All
windows_event_channels=Microsoft-Windows-Windows Defender /Operational,Security,microsoft-windows-P/operational events_max=1500 events_expiry=1800	These flags help manage events (on Windows only). These specify: • list of Windows event log channels to subscribe to • maximum number of events to store in the temporary storage • when to purge the storage Note that altering these values can cause a performance impact. For more information on these flags, see this article.	Windows only
enable_bpf_events=true (only for Enterprise Edition)	This flag specifies the source for socket and process events. True indicates that the source is BPF and false indicates that events source is auditd subsystem.	Linux only

Mechanisms available

The EclecticIQ Endpoint Response platform provides multiple methods to configure how to capture data for endpoints and specify what data to capture and what data to ignore. For the received endpoint data, you can also define rules and IOCs on the server to identify activities of interest.

Here are the tools available to you when using the EclecticIQ Endpoint Response platform.

- Queries
- Filters
- Rules
- YARA rule files
- Indicators of compromise

Queries

A query is a request for data from a database table or combination of tables that is executed on the endpoint running the EclecticIQ Endpoint Response agent.

The EclecticIQ Endpoint Response client is based on osquery that exposes the operating system as a high-performance relational database that can be queried. Using SQL queries, you can extract and review operating system data, such as running processes, loaded kernel modules, open network connections, browser plugins, hardware events, and file hashes. The EclecticIQ Endpoint Response client extends existing osquery features by adding real-time event collection.

You can review, push, and manage queries from the EclecticIQ Endpoint Response server UI or by using APIs. This topic describes how to manage queries using the UI. For more information on managing queries using APIs, refer to the *EclecticIQ Endpoint Response REST API Guide*.

Query types

Here are the types of queries you can use.

Type	***Description***
Scheduled queries	As the name suggests, scheduled queries run periodically to fetch the specified data for you. • After the EclecticIQ Endpoint Response client is provisioned and the connection to the EclecticIQ Endpoint Response server is established, few predefined queries (included in the config) are run to pull relevant information for each endpoint. For more information on how to view and manage seeded queries, see Edit an existing config. • In addition to the seeded queries, you can define custom queries based on your needs to fetch specific data from the endpoints. When created, you can run the individual query on one or more endpoints using tags. To run your custom query on one or more endpoints, associate a tag with the query and assign the same tag to relevant endpoints. For more information on how to create and manage queries, see Manage queries. • To run a set of multiple queries, you can group them into a pack, which is a collection of queries. Packs allow you to logically group queries into categories. Once defined, you can run all queries included in a pack simultaneously using tags. To run a pack on one or more endpoints, associate a tag with the pack and assign the same tag to relevant endpoints. For more information on how to create and manage packs, see Manage packs. The results of these SQL queries are stored in the PostgreSQL database on the EclecticIQ Endpoint Response server.
Live queries	A live query is suitable to meet your immediate and infrequent needs. It gives you a current snapshot of the endpoints. Data for live queries is transient; it is displayed on the UI but not stored in the database. For more information on how to run live queries, see Run live queries.

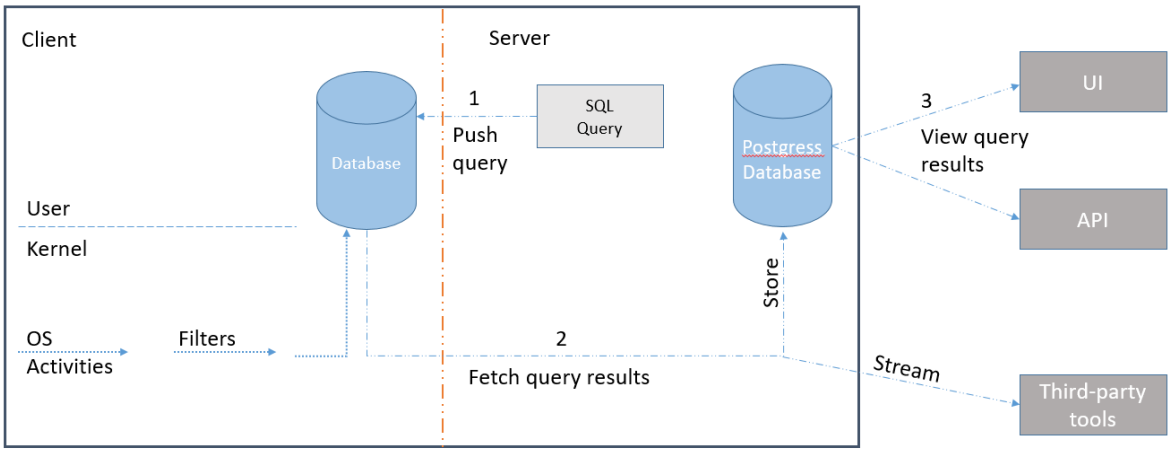
Query structure

All queries you define or use in the EclecticIQ Endpoint Response framework are defined using JSON syntax.

Query type	***Format***	***Example***
Schedule query	`"table name": { "query": "select * from table where column='value';", "interval": number of seconds, "platform": "operating system", "version": "x.x.x", "description": "describes the query", "value": "Process Events", "removed": false },`	`"win_process_events": { "query": "select * from win_process_events where action='PROC_CREATE';", "interval": 30, "platform": "windows", "version": "2.9.0", "description": "Windows Process Events", "value": "Process Events", "removed": false },`
Live query	`"select * from table where column='value';"`	`"select * from win_process_events where action='PROC_CREATE';"`

Query workflow

Here is a high-level query workflow in EclecticIQ Endpoint Response platform.



As the diagram depicts:

1. Query is pushed to the relevant endpoints at the next config update.
2. Query result is sent from the client database to the server database.
3. Query results can be viewed on the server or by using APIs.

- Steps 1, 2 and 3 apply to scheduled queries, query packs, and queries.
- Step 2 isn't performed for Live queries.

Note: The client database can store up to 2500 events. If it receives more events, events older than an hour are deleted. These values are configurable.

Filters

By default, the EclecticIQ Endpoint Response client captures system events in real-time for a multitude of system activities and makes the telemetry available through a flexible SQL syntax. Filters are available only for endpoints running the Windows operating system.

Any system, even when idle, generates a high volume of events. Streaming these events from the endpoint to the server at regular intervals using scheduled queries, despite compressing data, can cause a burden on the network and server storage. Although a lot of the system activity is benign or irrelevant for incident reporting, it still results in a large volume of data. This is where filters come into play and help capture only relevant data and reduce noise.

EclecticIQ Endpoint Response includes seeded filters to reduce the volume of data you need to review to search for incidents of interest. Also, these filters reduce the burden on network and server resources. For the most part, the data captured by the seeded filters will meet your needs. However, if needed, you can further tweak the data captured by defining additional filters.

Filter types

Using filters, you can configure the EclecticIQ Endpoint Response agent to capture only data relevant to you. You can choose to include relevant data and exclude non-meaningful data. In effect you can define two types of filters:

- Include filters to receive information about events matching the specified filtering criteria.
- Exclude filters to ignore information about events matching the specified filtering criteria.

Before you define filters, review the following guidelines:

- If no filter is defined for a table, all data for the table is captured.
- If you define an include filter for a table and column combination, all other data for that table and column combination is automatically excluded. Only the data matching the defined include filters is captured.
- If you define an exclude filter for a table and column combination, all other data for that table and column combination is automatically captured. Only the data matching the defined exclude filters is ignored.
- When the defined filters are processed:
    - *Exclude filters take precedence over include filters when rules conflict*. So, if an include and exclude filter match the same event, information for the activity is not captured.
    - When multiple include filters are defined for an event type, an OR condition is used across filters to match the events.

Filter examples

Here are examples of filters.

Filter type	***Example***

Exclude filter	`"win_process_events": {`
	`  "cmdline": {`
	`  "exclude" : {`
	`  "values":`
	`  [`
	`  "C:\\Windows\\system32\\DllHost.exe /Processid*",`
	`  "C:\\Windows\\system32\\SearchIndexer.exe /Embedding",`
	`  "C:\\windows\\system32\\wermgr.exe -queuereporting",`
	`  ]`
	`  }`
	`  }`
	`}`

Include filter	`"win_registry_events": {`
	`  "target_name": {`
	`  "include": {`
	`  "values":`
	`  [`
	`  "*CurrentVersion\\Run*",`
	`  "*Policies\\Explorer\\Run*",`
	`  "*Group Policy\\Scripts*",`
	`  "*Windows\\System\\Scripts*",`
	`  ]`
	`  }`
	`  }`
	`}`

Include and exclude filters	`"win_process_events": {`
	`  "cmdline": {`
	`  "exclude" : {`
	`  "values":`
	`  [`
	`  "C:\\Windows\\system32\\DllHost.exe /Processid*",`
	`  ]`
	`  }`
	`  "include": {`
	`  "values":`
	`  [`
	`  "C:\\Windows\\system32\\SearchIndexer.exe /Embedding",`
	`  "C:\\windows\\system32\\wermgr.exe -queuereporting",`
	`  ]`
	`  }`
	`  }`
	`}`

Rules

Rules, in the EclecticIQ Endpoint Response platform, offer a mechanism to deep dive into the data captured from the endpoints. You can narrow down and review selective data based on your area of interest. For example, you can define rules to detect potentially malicious system files. Alternatively, you can define rules to meet your compliance needs.

Based on your needs, you can define specific rules to monitor certain activities in your environment. After a rule is defined, rule matching occurs on the EclecticIQ Endpoint Response server based on the incoming endpoint data. An alert is generated if the rule matches incoming endpoint data.

For example, to track the Acrobat.exe file in the C:\Program Files (x86)\Adobe\Acrobat DC\Acrobat folder for any tampering or modification, you can define a rule to monitor file modification action for the Acrobat.exe file. After the rule is defined, an alert is generated if the Acrobat.exe file is changed. You can check the changes made to the file by reviewing the alert details.

For more information on reviewing and defining, see Manage rules.

YARA rule files

The EclecticIQ Endpoint Response platform provides YARA scan capabilities allowing you to scan endpoint artefacts, such as files on disk or memory of running processes based on YARA rules. Based on your requirements, you can manually define rules to specify characteristics for which to scan the endpoints in your environment. The rules can be configured as files (on the server) for the Windows, Linux, and macOS platforms. For more information, see Manage YARA files.

Indicators of compromise

Indicators of compromise (IOCs) allow you to monitor possible attacks or malicious activities in your environment. IOCs provide evidence that the security professionals and system administrators can analyse and use to detect intrusion attempts.

In the EclecticIQ Endpoint Response platform, you can provide IOCs, such as IPv4 addresses, domain names, and MD5 hashes, in JSON format that are compared with endpoint data. After an IOC is defined, matching occurs on the EclecticIQ Endpoint Response server based on the incoming endpoint data. If a provided IOC matches incoming data, an alert is generated.

For more information, see Configure IOCs.

Manage configs

As soon as an endpoint checks-in with the server (after agent installation), the default config is applied to the client based on the operating system of the endpoint. Along with configuration parameters and blocking rules, the applied config contains a list of predefined scheduled queries and filters that are applied on the endpoint.

At a time, only one config can be assigned to an endpoint. You can choose to retain the default applied config for an endpoint or assign a new config based on your needs. The default applied config is also editable and the changes to the config are picked up by the endpoints each time the config is updated.

- For Windows x64 systems, two types of built-in configs are available, Default (applied by default) and Deep. The Deep config is designed for more aggressive data collection from endpoints than the Default config.
  Note: Prior to using the Deep config, make sure that the server has sufficient resources to handle associated data.
- For the Linux and Darwin operating systems, only one Default config is available.

At any time, five configs can be defined for each operating system. Considering the Default and Deep configs are predefined for the Windows operating system, you can define three additional custom configs for the Windows operating system. For the Linux and Darwin operating systems, you can define four additional configs.

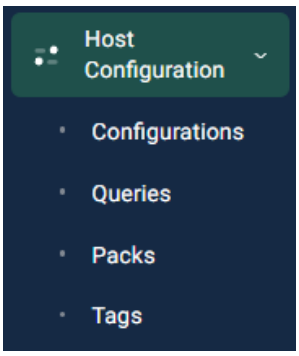
- Edit existing configs
- Create new configs
- Understand config parameters

Edit existing configs

If needed, you can edit an existing config to suit your requirements. We advise that you understand each parameter and use caution when editing the config. For more information on the options, see Understand config parameters.

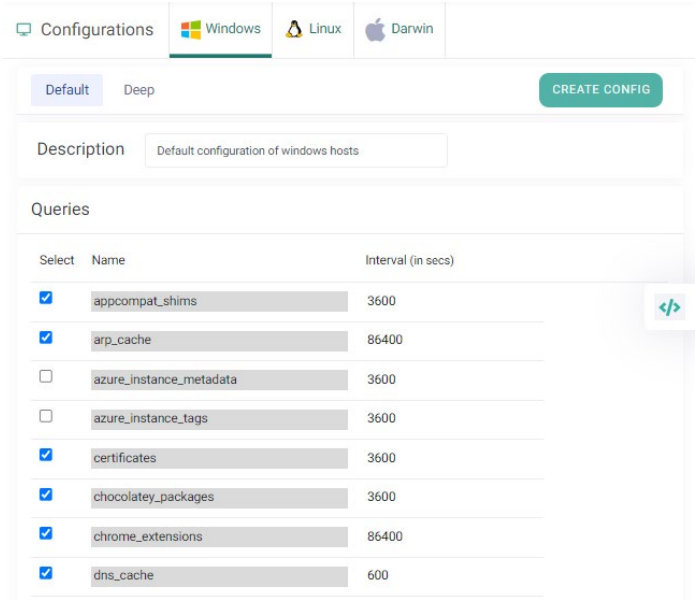
Perform these steps to edit an existing config.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Configurations.



   The Configurations page is displayed.

3. Select the platform for which to edit the config.
4. Select the config to edit (by clicking the appropriate tab).



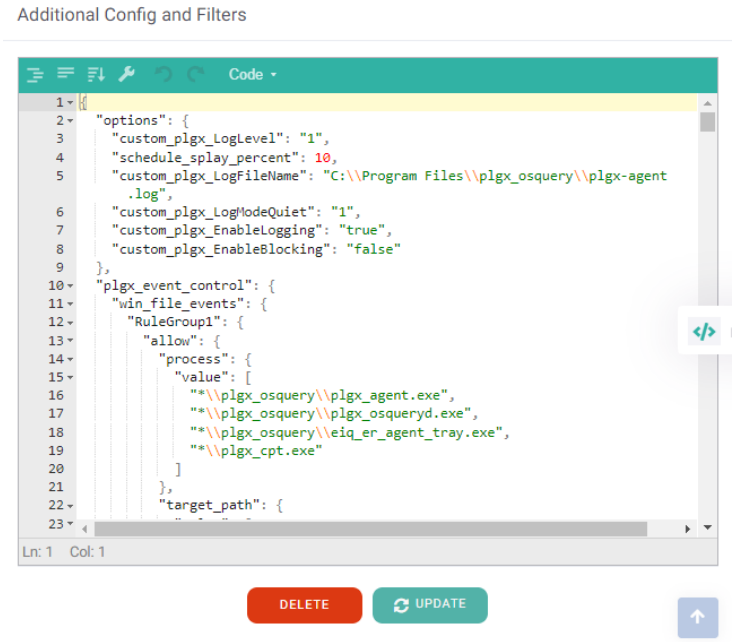
5. Review the predefined queries.

As part of the config, multiple pre-defined scheduled queries are applied on the endpoints. Each scheduled query is targeted to collect certain data and runs at a specified interval. The applied scheduled queries vary for each operating system.

6. Deselect a query to remove it from the config.
7. Optionally, modify the interval for a query to specify how often the query is run.

   The time duration (in seconds) specifies the duration after which the query is run on the client and query results are pushed to the server.

8. Scroll to the Additional Config and Filters section and review the predefined filters.



9. Optionally, edit defined filters, as needed.
10. Review and edit the option values, if needed.

    Note that the options and values are both case sensitive. For more information on the available options, see Understand config parameters.
    Note: If you change the custom_plgx_EnableHttp or custom_plgx_EnableDns option, you must restart the service on the agent for the changes to be applied.

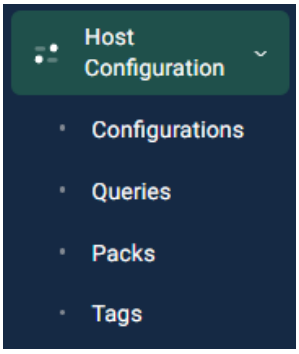
11. Click Update.

Create new configs

If needed, you can create additional custom configurations based on your needs.

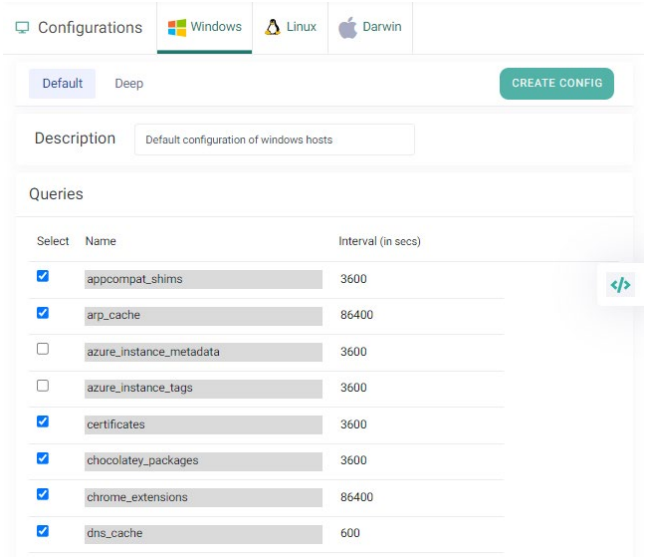
Perform these steps to create a new configuration.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Configurations.



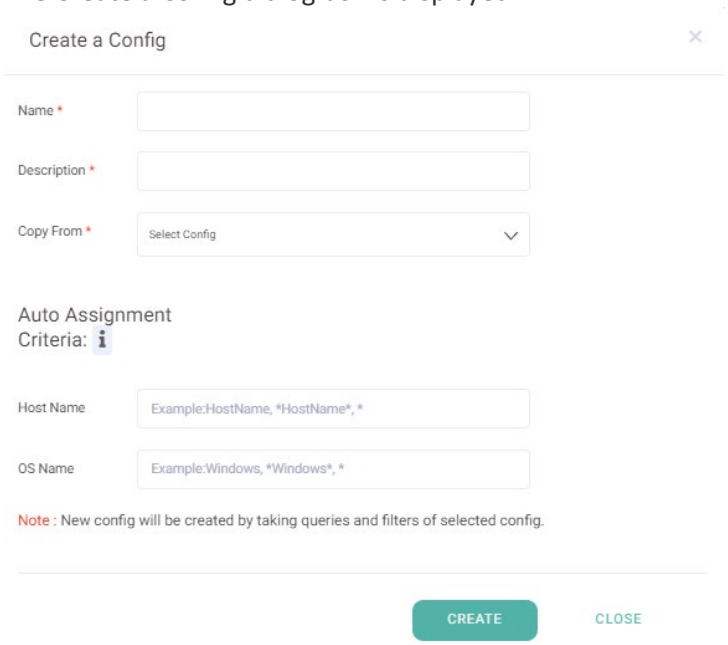
   The Configurations page is displayed.

3. Select the platform for which to create the config.



4. Click Create Config.

   The Create a Config dialog box is displayed.



5. Specify the config name and description.
6. Select an existing config in the Copy From drop down.

   The most efficient method to create a new config is to use an existing config as a base and make additional changes. All queries and filters of the selected config are added to the new config.

7. Optionally, specify the assignment criteria for the new config.

   You can assign the config to a specific endpoint based on its name or to multiple endpoints based on the operating system. Only the endpoints that are enrolled after a new config is created are automatically assigned the new config if they match the specified assignment criteria.

   Note: When an endpoint is enrolled in the EclecticIQ Endpoint Response server and two or more configs match the endpoint based on the auto assignment criteria defined for the configs, neither config is assigned to the endpoint and the server assigns the Default config to the endpoint.

8. Click Create.

   A success message is displayed.

9. Click OK.

   The new config is displayed on the Configurations page.

10. Make additional changes, as needed, to the config and click Update.

    For more information, see Edit existing configs.

Understand config parameters

Here are the parameters available in the config file. Note that not all parameters are available in the default config and that some parameters are specific to the Windows operating system.

Option	***Description***	***Possible values***	***Present in Default config***
custom_plgx_ LogLevel	Indicates the logging level for response actions.	• 0 (Trace) • 1 (Debug) • 2 (Info) • 3 (Warning) • 4 (Error) By default, set to 3 (Warning).	Yes (for Windows, Linux macOS for Enterprise Edition) Yes (for Windows only for Community Edition)
custom_plgx_ EnableDns	Specifies whether to report Domain Name Server (DNS) and DNS response events.	• true • false By default, set to false. If you change the value at runtime, restart the EclecticIQ Endpoint Response agent (from the Hosts page on the server UI by selecting the endpoint and clicking Action > Restart Agent) to ensure the changes take effect.	No (Windows only)
custom_plgx_ DnsPorts	If custom_plgx_ EnableDns is set to true, you can specify 10 port values (comma separated) for which to receive events.	By default, set to port 53. If you change the value at runtime, restart the EclecticIQ Endpoint Response agent (from the Hosts page on the server UI by selecting the endpoint and clicking Action > Restart Agent) to ensure the changes take effect.	No (Windows only)
custom_plgx_DiskIndexingRecordLimitHint	Specifies the maximum number of records to reindex in one attempt. This	By default, this is set to 10000.	No (Windows only)

Option	*Description*	*Possible values*	*Present in Default config*
	is a suggested value and is not binding.	We suggest you specify a value between 0 and 10000. Note that if you set a very high value, osquery may not report any rows (based on the system configuration).	
custom_plgx_DiskIndexingReindexTimeout	Allows you to specify (in seconds) when disk reindexing is performed.	By default, this is set to 0. A value of 0 or negative value indicates that the disk is indexed only once (and never again). Possible values are between -1 to +infinity. Note that if you set a very high value, osquery may not report any rows (based on the system configuration).	No (Windows only)
custom_plgx_DiskIndexingEnabled	Specifies whether to enable or disable search capabilities for Windows endpoints.	• true • false By default, set to false.	No (Windows only)
custom_plgx_EnableSSL	Specifies whether to enable or disable SSL cert events. You can enable only custom_plgx_EnableSSL or custom_plgx_EnableShallowSSL at a time.	• true • false By default, set to false. If you change the value at runtime, restart the EclecticIQ Endpoint Response agent (from the Hosts page on the server UI by selecting the endpoint	No (Windows only)

Option	*Description*	*Possible values*	*Present in Default config*
		and clicking Action > Restart Agent) to ensure the changes take effect.	
custom_plgx_ EnableShallow SSL	Specifies whether to enable or disable SSL cert events. Set this option to true to receive a subset of information received with the custom_plgx_ EnableSSL option. You can enable only custom_plgx_ EnableSSL or custom_plgx_ EnableShallowSSL at a time.	• true • false By default, set to false. If you change the value at runtime, restart the EclecticIQ Endpoint Response agent (from the Hosts page on the server UI by selecting the endpoint and clicking Action > Restart Agent) to ensure the changes take effect.	No (Windows only)
custom_plgx_ EnableHttp	Specifies whether to enable or disable HTTP events.	• true • false By default, set to false. If you change the value at runtime, restart the EclecticIQ Endpoint Respons agent (from the Hosts page on the server UI by selecting the endpoint and clicking Action > Restart Agent) to ensure the changes take effect.	No (Windows only)
schedule_splay_ percent	Specifies the percentage to splay the config times for scheduled queries.	By default, this is set to 10 and should not be changed.	Yes (for Windows, Linux, macOS)
custom_plgx_ LogFileName	Specifies the name and location of the log file.	By default, this is set to C:\\Program	Yes (Windows only)

Option	*Description*	*Possible values*	*Present in Default config*
		Files\\plgx_osquery\\plgx-agent.log.	
custom_plgx_ LogFileName Linux	This flag specifies name and location of log file on Linux endpoints.	By default, this is set to /usr/bin/plgx-agent.log.	Yes (Linux only for Enterprise Edition)
custom_plgx_ LogFileName Mac	This flag specifies name and location of log file on macOS endpoints.	By default, this is set to /usr/local/bin/plgx-agent.log.	Yes (macOS only for Enterprise Edition)
custom_plgx_ LogModeQuiet	Specifies whether the log messages are printed on console or not. Relevant only when running the client as a console application.	• 0 • 1 By default, this is set to 1. A value of 1 indicates that the agent will not print log messages on the CLI.	Yes (for Windows, Linux macOS for Enterprise Edition) Yes (for Windows only for Community Edition)
custom_plgx_ EnableLogging	Specifies whether to enable logging for the response actions on endpoints.	• true • false By default, set to true.	Yes (for Windows, Linux macOS for Enterprise Edition) Yes (for Windows only for Community Edition)
custom_plgx_ EventBufferSize	Specifies the maximum number of events that can be sent in a query result from a client to the server.	By default, set to 1024 events.	No (Windows only)
custom_plgx_ EnableAgent Restart	Specifies how to respond when the memory threshold is breached for an endpoint (specified by the custom_plgx_ MemoryLimitHigh options. • When set to true, the endpoint is restarted.	• true • false By default, set to false.	No (Windows only)

Option	*Description*	*Possible values*	*Present in Default config*
	• When set to false, event collection is suspended to the endpoint. This option comes into play only when the custom_plgx_EnableWatcher option is set to true.		
custom_plgx_ EnableWatcher	This flag enables Memory Watcher functionality of the client. This entails disabling client's memory intensive operations if its memory limit is breached, allowing client memory to recover and enable again when memory range is within acceptable limit.	• true • false By default, set to true.	No (Windows only)
custom_plgx_ MemoryLimitHigh	This flag defines the maximum memory usage for a client exceeding which triggers the Memory watcher functionality. This option comes into play only when the custom_plgx_EnableWatcher option is set to true.	By default, this is set to 150 MB and can be set to a maximum value of 350 MB.	No (Windows only)
custom_plgx_ MemoryLimitLow	This flag applies only if the maximum memory usage threshold of the client is exceeded and specific the memory usage threshold at which event collection is resumed. This option comes into play only when the custom_plgx_EnableWatcher option is set to true.	By default, this is set to 75 MB and can be set to a minimum value of 50 MB.	No (Windows only)

Option	*Description*	*Possible values*	*Present in Default config*
custom_plgx_ EnableExtension Monitor	Allows you to monitor if the osquery extension is loaded. When set to true, it restarts the osquery if extension is not loaded for any reason.	• true • false By default, set to true.	No (for Windows, Linux, an macOS for Enterprise Edition) No (for Windows only for Community Edition)
custom_plgx_ EnableResp Server	This option allows you to enable or disable the response feature.	By default, this is enabled.	No (for Windows, Linux, macOS for Enterprise Edition) Unavailable in the Community Edition
custom_plgx_ SaveCustom ResponseScript	Setting this flag will save the response command to a file on the target endpoint before executing it.	• true • false By default, set to false.	No (for Windows, Linux, macOS for Enterprise Edition) Unavailable in the Community Edition
custom_plgx_ EnableYara ProcessScan	Set this option to scan processes on launch against YARA signatures on the target Windows endpoint.	• true • false By default, set to false.	No (Windows only)
custom_plgx_ ResponseData LimitInMb	Specify the output size for the response of a custom script (run by using a response command).	By default, set to 2 MB.	No (for Windows, Linux, macOS for Enterprise Edition) Unavailable in the Community Edition

Option	*Description*	*Possible values*	*Present in Default config*
custom_plgx_ EnableAmsiStream EventData	Set this option to enable or disable AMSI scanning. When this option is enabled, every time a file is modified, the first 70 bytes of the file are scanned by the AMSI module for possible malware. The scanned bytes are base64 encoded and reported in the file write events.	• true • false By default, set to false.	No (Windows only)
custom_plgx_ EnableBlocking	Set this option to enable or disable defined rules to allow or block following operations: • Process execution • Process termination • File operations • Registry operations	• true • false By default, set to false.	No (Windows only)
custom_plgx_ EnableImageLoad	Allows you to receive or ignore Image Load events.	• true • false By default, set to true.	No (Windows only)

Manage queries and packs

The EclecticIQ Endpoint Response platform supports scheduled and live queries. For queries and packs, you can manage existing or define new using the EclecticIQ Endpoint Response server.

Query type	*Description*
Scheduled queries	Predefined queries included in the Default config Seeded queries that are included in the config run periodically on the endpoints to fetch data. For a query included in the config, you can View, edit, or run scheduled queries.
	Individual seeded or custom queries (not included in the config) Few predefined queries available in the EclecticIQ Endpoint Response platform are not assigned to any endpoints. You can choose to assign these queries to endpoints or define a new query based on your needs and assign those to endpoints. For seeded and custom queries, you can edit queries, assign tags to queries and packs, and delete queries.

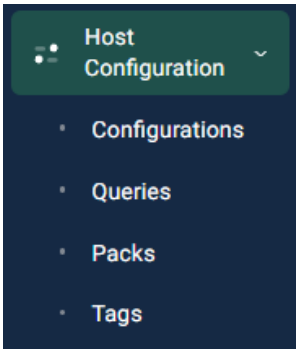
	Queries contained in packs EclecticIQ Endpoint Response includes multiple predefined packs that group relevant queries based on purpose. These predefined packs are not assigned to any endpoints by default. You can review the packs and contained queries and assign these to endpoints in your environment, as needed. For more information, see Manage packs.
Live queries	A live query is run on-demand and provides current snapshot of the endpoints. Live query results are only displayed on the UI after execution and are not stored in the database. For more information on how to execute live queries, see Run live queries.

View, edit, or run scheduled queries

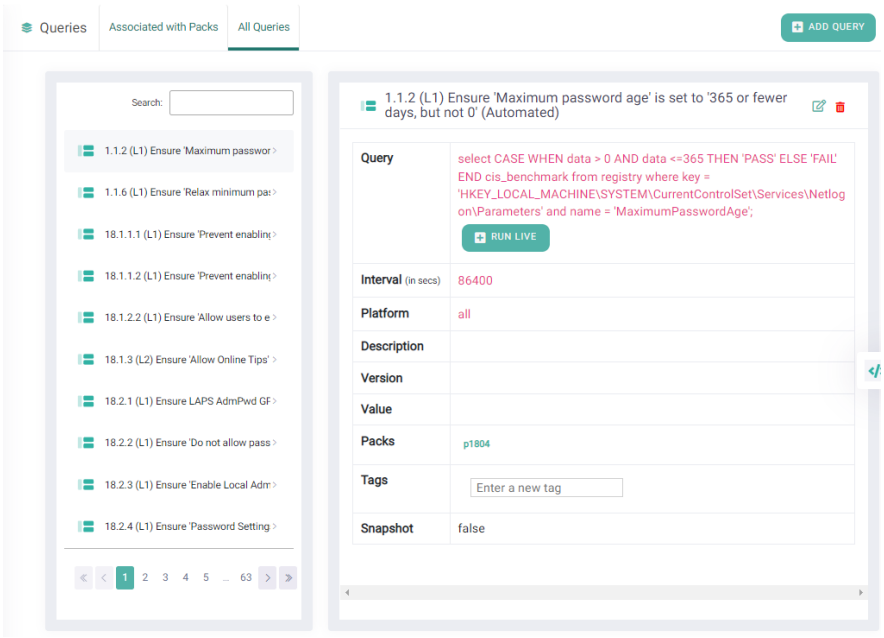
The default config includes a set of scheduled queries that capture process creation and network connections data from the endpoint.

Perform these steps to view or run a predefined query.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Queries.



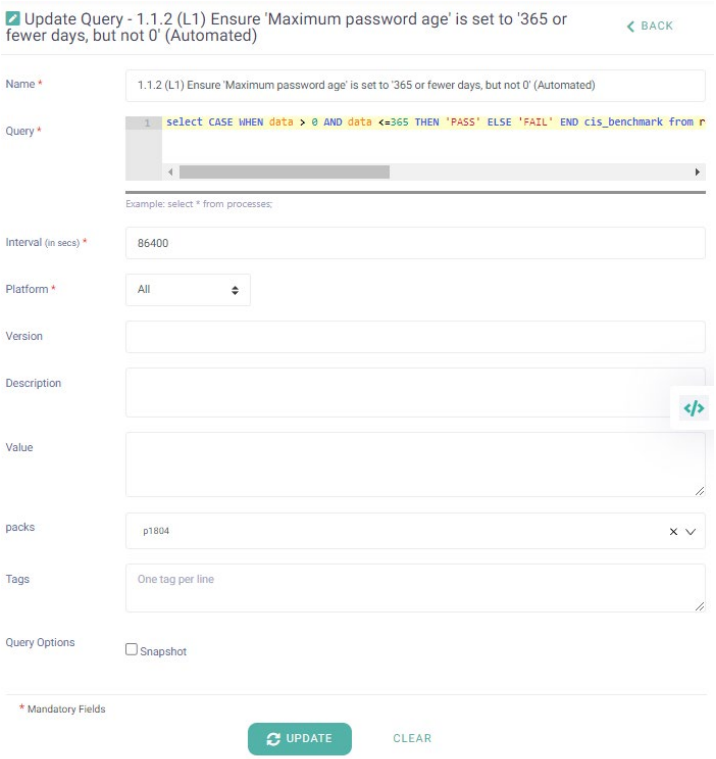
3. On the Queries page, switch to the All Queries tab.



4. Locate the query to view or edit by using the Search field.
5. Click a query in the left pane to review its details.

6. Edit the query, if needed.
    a. Click the edit icon in the right pane next for the query.

       The Update Query <query name> page is displayed.



    b. Make the needed changes.
    c. Click Update.

       A confirmation dialog prompts you to confirm the changes.

    d. Click Yes, Update.

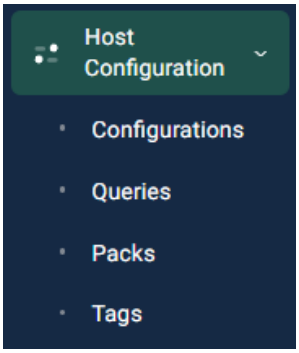
       A success message is displayed, and you are returned to the Queries page.
7. Optionally, click Run Live for the query to run it immediately.

   For more information, see Run live queries.
8. Optionally, assign the query to additional endpoints by adding tags.

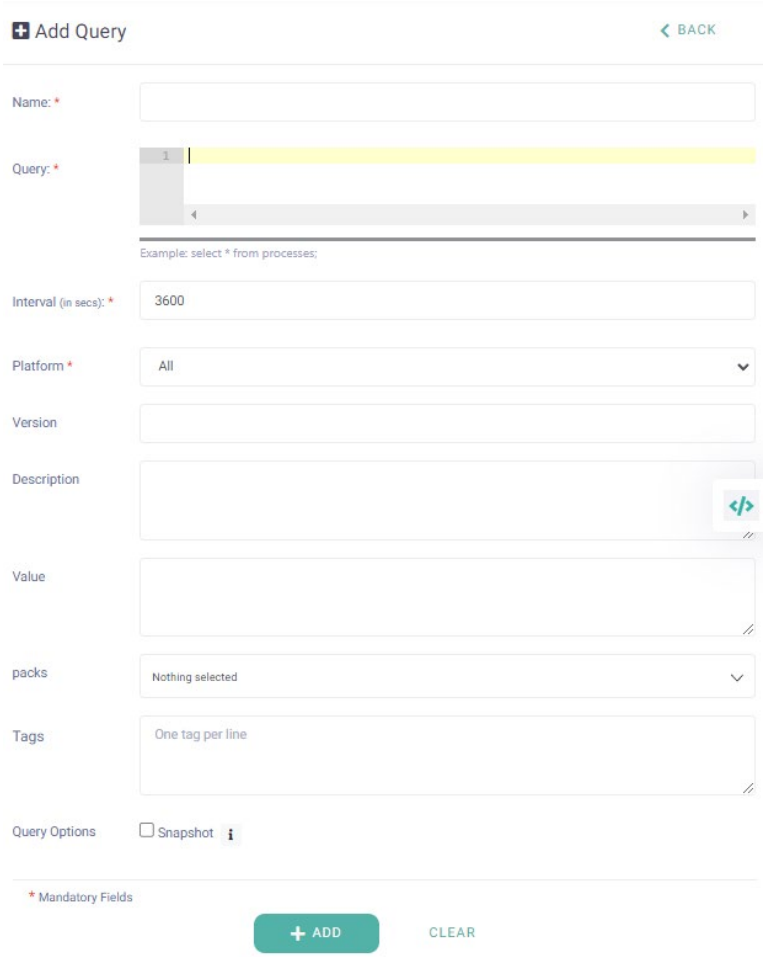
Define new queries

Perform these steps to create a new query.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Queries.



3. On the Queries page, click Add Query.



4. On the Add Query page, specify the query details, such as name, query, interval, and platform.

   Use caution when specifying query names. Make sure each query name is unique. If you erroneously provide the name of a seeded query (included in the config) for a new query, the existing seeded query will be overwritten.

5. Specify the query type.

By default, queries are differential and fetch only the delta since the last query run. This improves performance and optimizes database storage. To get complete query results instead of differential, select Snapshot in Query Options.
Note: To avoid performance degradation, we recommend that you exercise caution and selectively define snapshot queries. Do not define snapshot queries for data intensive tables, such as win_file_events and win_process_events.

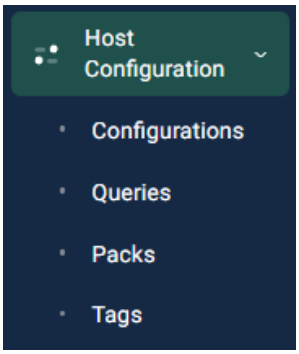
6. Click Add.

   A success message is displayed, and the query is added to the Queries page.

Edit queries

Perform these steps to edit a predefined query.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Queries.

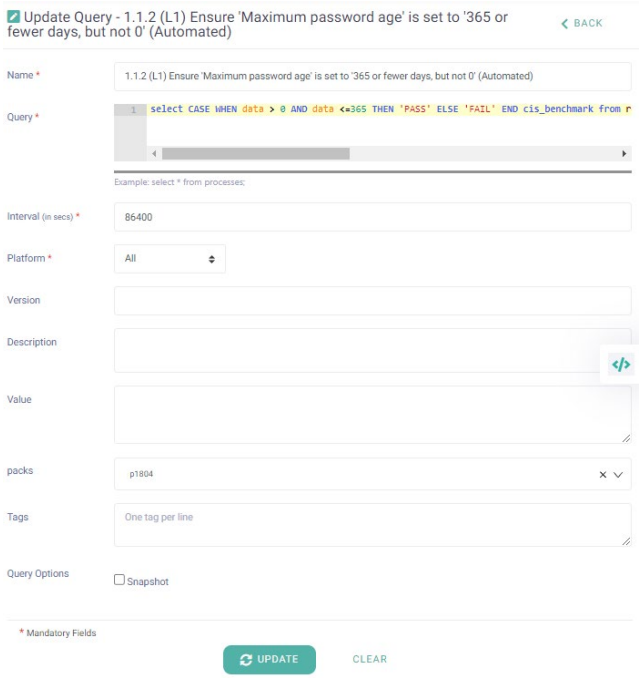


3. On the Queries page, select a tab to view corresponding queries.

   You can either view all queries or only queries assigned to packs.

4. In the left pane, select the query to edit.
5. Click the edit icon in the right pane next to the query name.

   The Update Query <query name> page is displayed.



6. Make the needed changes.
7. Click Update.

   A confirmation dialog prompts you to confirm the changes.

8. Click Yes, Update.

   A success message is displayed, and you are returned to the Queries page.

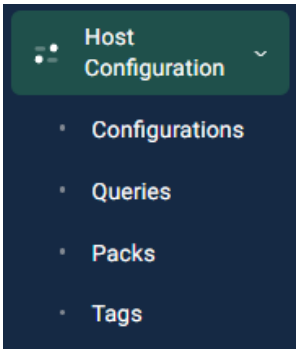
Assign tags to queries and packs

For more information on assigning tags to queries and packs, see Manage tags.

Delete queries

Perform these steps to edit a predefined query.

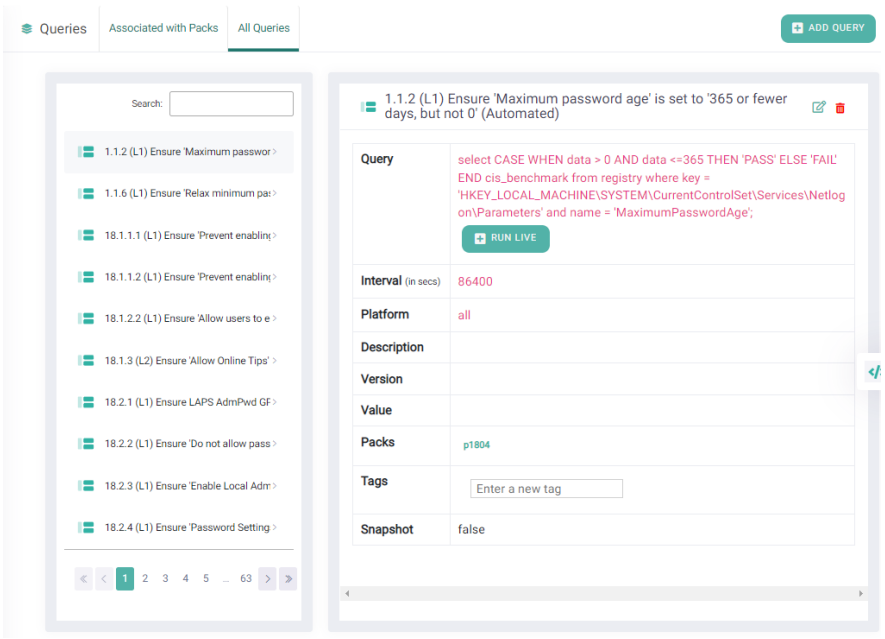
1. Access the web interface for the server.
2. Navigate to Host Configuration > Queries.



3. On the Queries page, select a tab to view corresponding queries.

   You can either view all queries or only queries assigned to packs.

4. In the left pane, select the query to delete.



5. Click the delete icon in the right pane next to the query name.

A confirmation dialog is displayed.

6. Click OK.

   A success message is displayed, and the query is removed from the Queries page.

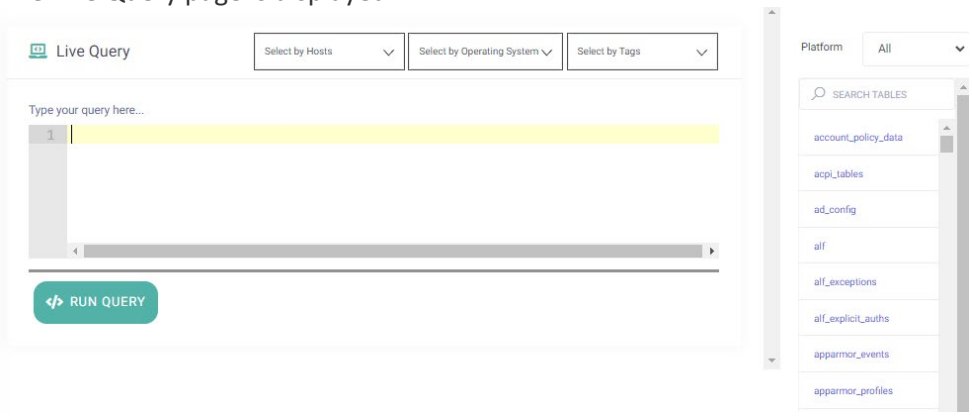
Run live queries

When you run a live query, the data is fetched and displayed to you immediately. If needed, you can save the data in an Excel or CSV file.

Perform these steps to define and run a live query.

1. Access the web interface for the server.
2. Navigate to Live Query.

   The Live Query page is displayed.



3. Specify the query to run in the Type your query here field.

   When building your query:
   - Refer to the tables list to correctly specify table and column names for each platform.
   - Ensure you create targeted queries using conditions and operators to fetch only relevant data. A vague or imprecise query may cause the server to hang if it fetches a very high volume of records.
   - Use the OFFSET and LIMIT clauses when creating a query that is likely to fetch a high volume of records. These clauses help control the fetch records. The LIMIT clause specifies the number of rows to return while the OFFSET clause is used to skip the specified number of records from the result. Here a few examples.

     ```
     select * from win_dns_events limit 100;
     select * from win_dns_events offset 100 limit 100;
     ```

4. Specify the endpoints on which to run the query.

   - To run the query on an endpoint, choose the endpoint from the Select Hosts drop-down list.
   - To run the query on a group of endpoints, select a tag from the Select by Tags drop-down list.
   - To run the query on endpoints running a specific operating system, choose a value from the Select by Operating System drop-down list.

5. Click Run Query.

   The query is executed, and the Status and Results tabs appear. The Status tab displays the status of the query: Pending, Failure, or Success.

6. After the query is run, switch to the Results tab to view the details.
7. Optionally, click Excel or CSV to save the data in Excel or CSV format, respectively.

Manage packs

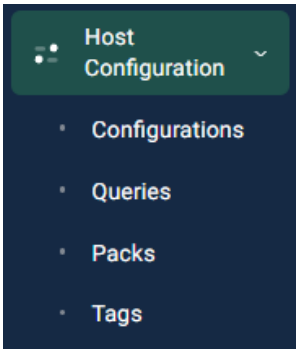
By default, multiple packs are included with your EclecticIQ Endpoint Response configuration. Although available, these packs are not assigned to endpoints in your environment. You can use existing packs or add more packs, as needed, to meet your requirements.

- View and assign packs to hosts
- Define a new pack
- Delete a pack

View and assign packs to hosts

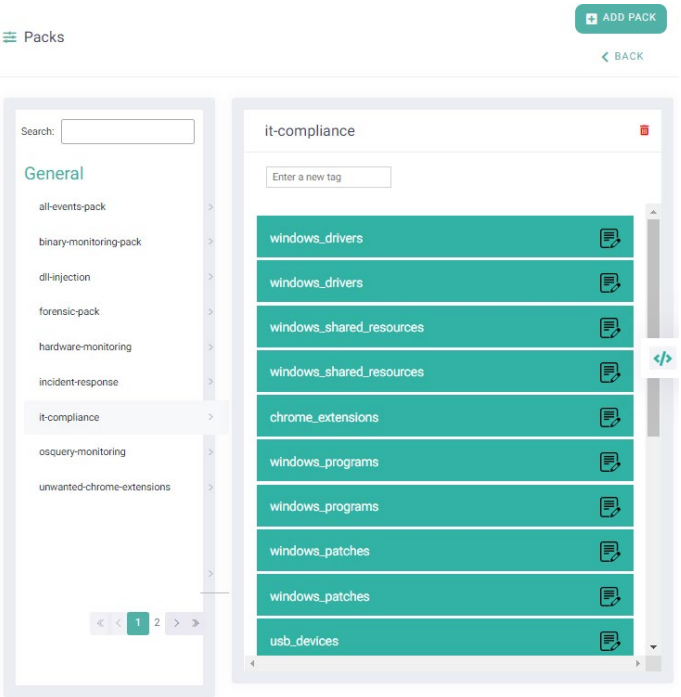
Perform these steps to view and edit packs.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Packs.



The Packs page is displayed.

3. Review the available packs (listed in the left pane).
4. Click a pack name to see the included queries.



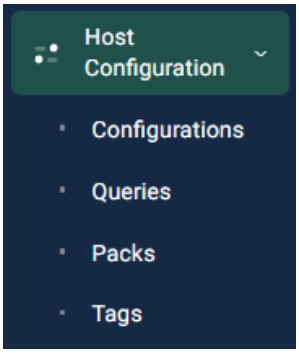
5. Optionally, to assign a pack to a group of endpoints, specify a tag.

   All queries in the pack are applied to the endpoints assigned the tag at the next config update.

Define new packs

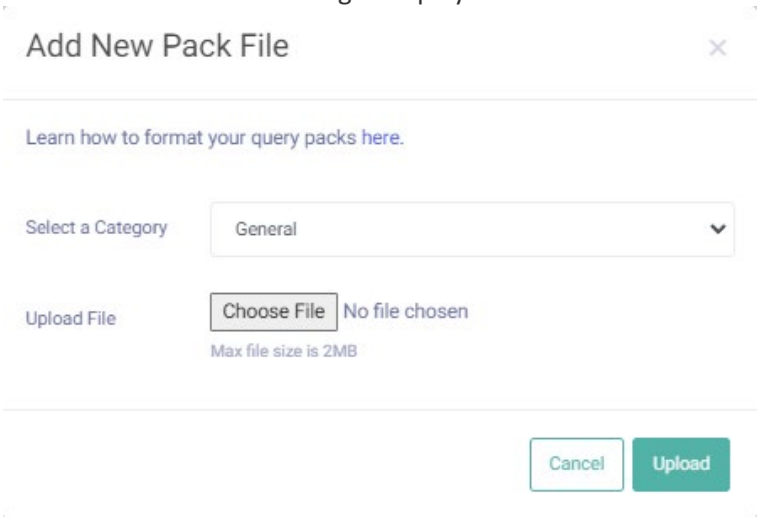
Perform these steps to add a new query pack.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Packs.



3. Click Add Pack.

   The Add New Pack File dialog is displayed.



4. Select a category from the list.
5. Click the Choose File button to specify the pack file.

   For more information on how to create a pack file, review this page.

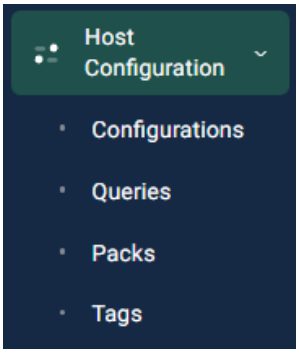
6. Click Upload to create the pack.

   A success message is displayed, and the pack is added.

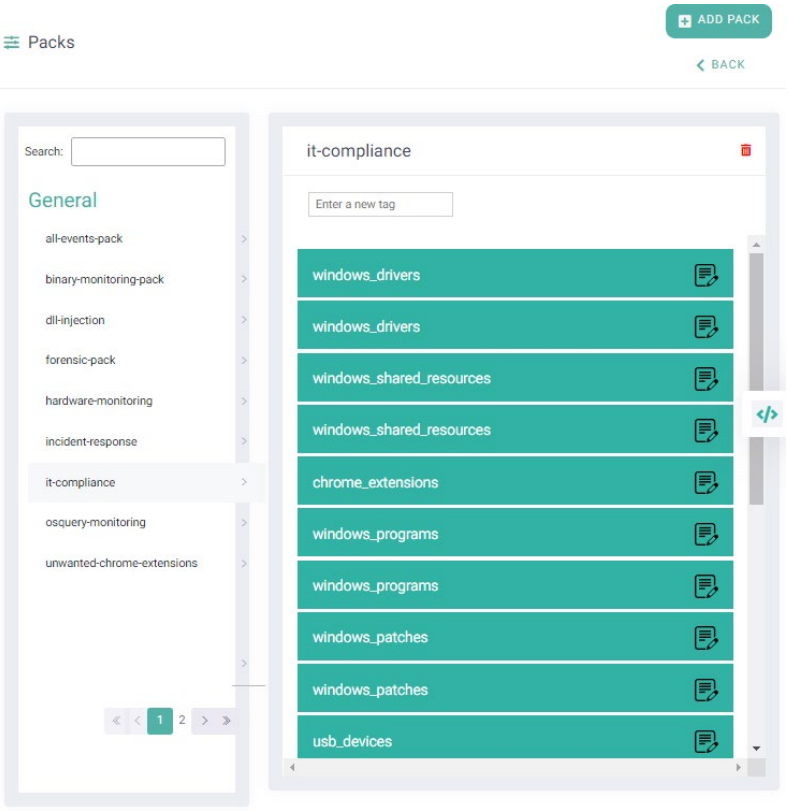
Delete packs

Perform these steps to delete a pack.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Packs.



3. Select the pack to delete in the left pane.



4. Click the delete icon in the right pane next to the pack name.

   A confirmation dialog is displayed.

5. Click OK.

   A success message is displayed, and the pack is removed from the Packs page.

Manage filters

The default config for the Windows operating system includes seeded filters to eliminate *white noise* from the real-time telemetry. You can define additional filters, as needed, based on your requirements. Filters are only available for endpoints running the Windows operating system and operate on selected tables and are defined in the osquery config file.

- Syntax for filters
- Config sections for filters
- Add a filter

Syntax for filters

Use the JSON syntax to define filters.

```
"plgx_event_filters": {
        "section name1": {
                "subsection name1" : {
                        "filter type" : {
                                "values":[
                                        "value 1",
                                        "value 2"
                                        ]
                                        }
                                },
                "subsection name2" : {
                        "filter type" : {
                                "values":[
                                        "value 3",
                                        "value 4"
                                        ]
                                    }
                           }
                        },
        "section name2": {
                "subsection name3" : {
                        "filter type" : {
                                "values":[
                                        "value 5",
                                        "value 6"
                                        ]
                                }
                   },
                "subsection name2" : {
                        "filter type" : {
                                "values":[
                                        "value 7",
                                        "value 8"
                                        ]
                                }
                        }
                }
        }
```

In the syntax:

- **section name** - Represents the name of the section (based on the EclecticIQ Endpoint Response table on the agent) under which to define filters. You must include the section names in double quotes (“”). For more information on valid section names, see Config sections for filters.
- **subsection name** - Indicates the name of the subsection (based on the column in the EclecticIQ Endpoint Response table on the agent) in the section for which to filter information. You must include the subsection names in double quotes (“”). For more information on valid subsection names (under each section), see Config sections for filters.
- **filter type** - Specifies the filter type. Possible values are include and exclude. You must include the values in double quotes (“”).
- **value** - Lists the values to match for the specified filter. Each entry represents a value that you want to store or ignore data for (based on the filter type). You must include the values in double quotes (“”). Specified values are case insensitive. You can also use following wild cards in the values where * represents one or more characters and ? represents a single character.

Config sections for filters

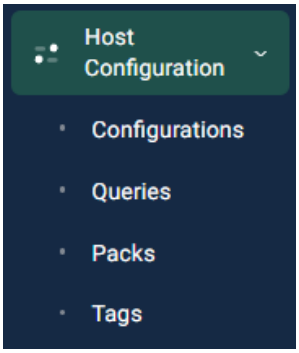
In the config, you can define filters under only specific sections (based on the EclecticIQ Endpoint Response table and columns on the agent that support event filters).

Section	***Subsection***	***Description***
win_proc_events	cmdline, path, parent_path	Section to include filters for process events.
win_registry_events	target_name, action, process_name	Section to include filters for registry events.
win_socket_events	process_name, remote_port, remote_address	Section to include filters for socket events.
win_file_events	target_path, process_name	Section to include filters for file events and named pipe events.
win_remote_thread_events	src_path, target_path	Section to include filters for remote thread events.
win_process_open _events	src_path, target_path, granted_access	Section to include filters for process open events.
win_dns_events	domain_name	Section to include filters for DNS request events.
win_dns_response _events	domain_name	Section to include filters for DNS response events.
win_image_load _events	image_path, issuer_name	Section to include filters for events generated for loaded images.
win_image_load_ process_map	image_path	Section to include filters for events generated for images loaded in a process.
win_ssl_events	process_name	Section to include filters for SSL events.

Add filters

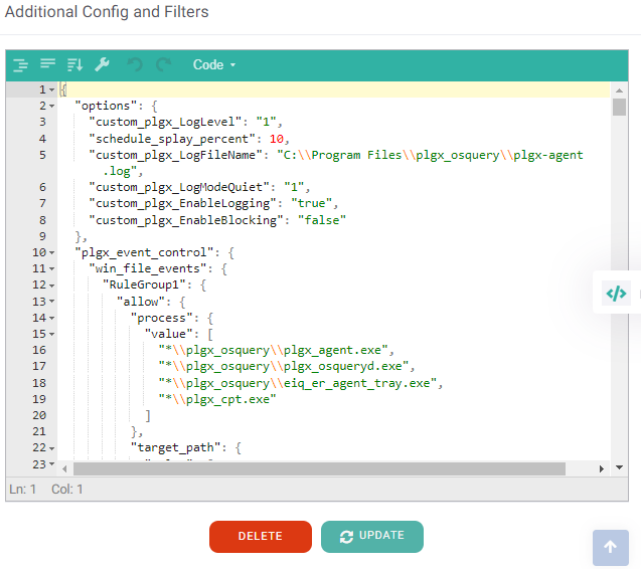
Perform these steps to edit an existing config to add a new filter.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Configurations.



   The Configurations page is displayed.

3. Select the platform for which to edit the config.
4. Select the config to edit (by clicking the appropriate tab).
5. Scroll to the Additional Config and Filters section.



6. Add the new filters.

   Ensure you follow the syntax for filters and place all filters within the plgx_event_filters tag. Also, make sure you create filters within the appropriate sections in the config. For more information, see Config sections for filters.

7. Click Update.

   A confirmation dialog is displayed.

8. Click Yes, Update.

   A success message box is displayed, and the config is updated.

9. Click OK.

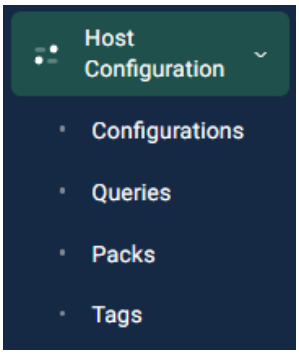
Set up named pipe monitoring

Starting with the 4.0.0 release, EclecticIQ Endpoint Response provides visibility for named pipe events (Windows only).

By default, this feature is disabled. To enable the feature, you must specify the pipe name to monitor in the config.

Perform these steps to configure event monitoring for a specific pipe.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Configurations.



   The Configurations page is displayed.

3. Select the Windows platform.

   This feature is available only on endpoints running the Windows 2012 R2, Windows 2016, Windows 2019, Windows 10 (x86 and x64), and Windows 11 operating systems.

4. Select the config to edit (by clicking the appropriate tab).
5. Scroll to the Additional Config and Filters section.
6. Navigate to the plgx_event_filters > win_file_events > target_path > include > values section.

7. Specify the pipe details.

   - Add “\\unknown drive\\<pipe name>” to monitor a specific named pipe
   - Add “\\unknown drive*” to monitor all named pipes

8. Click Update.

   The NAMED_PIPE_CREATE and NAMED_PIPE_DISCONNECT events are generated for pipe creation and pipe disconnect, respectively.

Manage rules

EclecticIQ Endpoint Response includes a set of predefined rules (available only in the Enterprise Edition) that can serve as a starting point to enable you to define additional custom rules specific to your needs. These seeded rules are developed based on MITRE attack vector framework and stored in Sigma format.

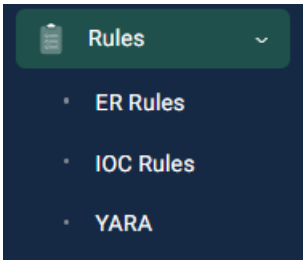
- View and edit existing rules
- Add new rules
- View alerts for a rule
- Deactivate rules

View and edit existing rules

Perform these steps to view or edit existing rules.

Note: No predefined or default rules are available in the Community Edition.

1. Access the web interface for the server.
2. Navigate to Rules > ER Rules.

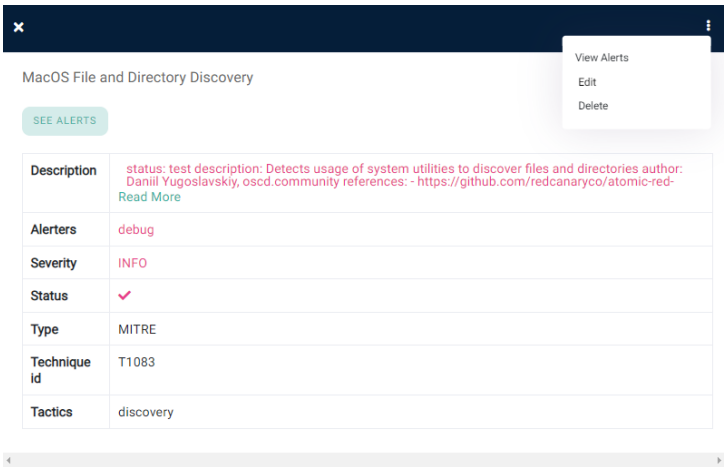


   The ER Rules page is displayed.

3. Click a row (associated with a rule).

   If needed, use the Search field to locate a specific rule by specifying its name.
   A pop-up page displays rule details.

4. Click the ellipsis icon and select Edit.



   The Update Rule page displays the rule details.

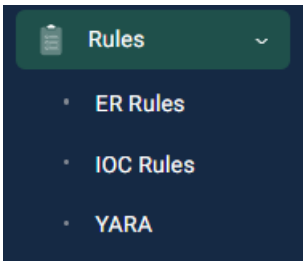
5. Click Update when done.

   A success message is displayed.

Add new rules

Perform these steps to add new rules.

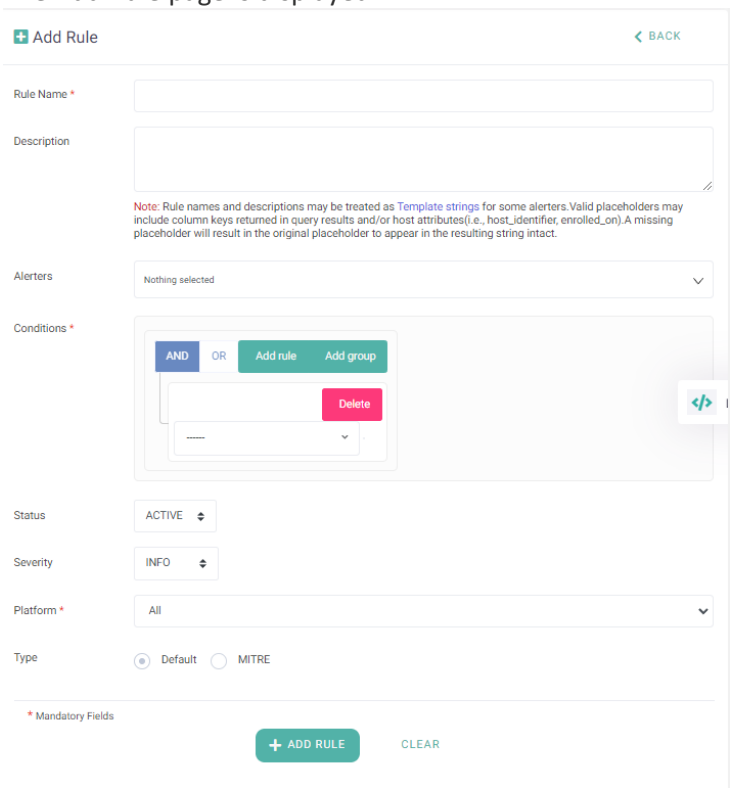
1. Access the web interface for the server.
2. Navigate to Rules > ER Rules.



   The ER Rules page is displayed.

3. Click Create Rule.

   The Add Rule page is displayed.



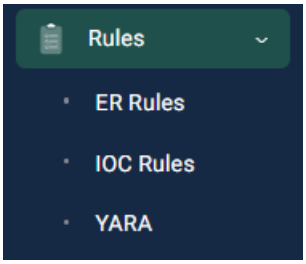
4. Specify the rule information, such as name, alerters, conditions, platform, severity, status, and type.
5. Click Add Rule.

   A success message is displayed, and the rule is added to the ER Rules page.

View alerts for a rule

Perform these steps to view alerts generated based on a specific rule.

1. Access the web interface for the server.
2. Navigate to Rules > ER Rules.

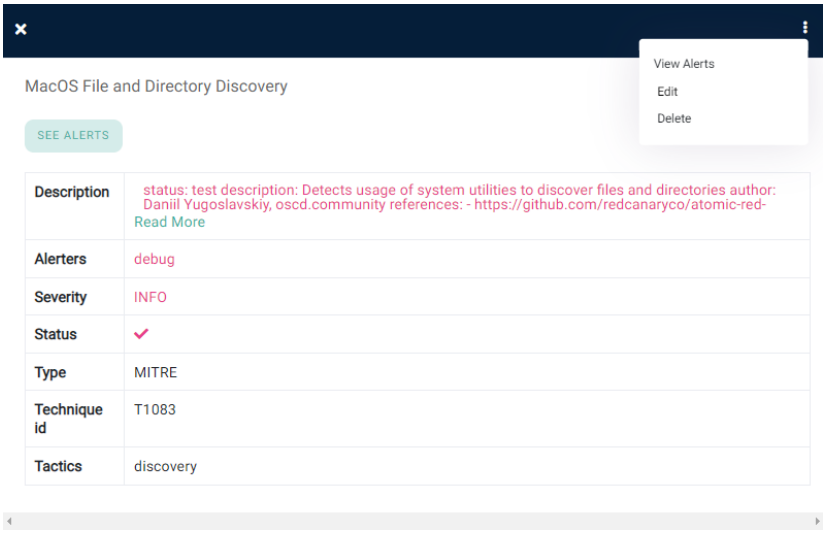


The ER Rules page is displayed.

3. Click a row (associated with a rule).

   A pop-up page displays rule details.

4. Click See Alerts or click the ellipsis icon and select View Alerts.



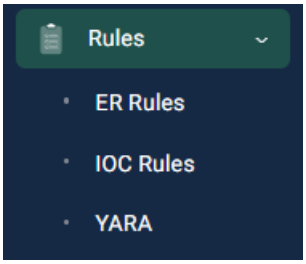
The Alerts page is displayed.

5. Review the listed alerts.
6. Optionally, click Export to export the alerts list to a CSV file.

Deactivate rules

Perform these steps to view or edit existing rules.

1. Perform these steps to deactivate existing rules.
2. Access the web interface for the server.
3. Navigate to Rules > ER Rules.

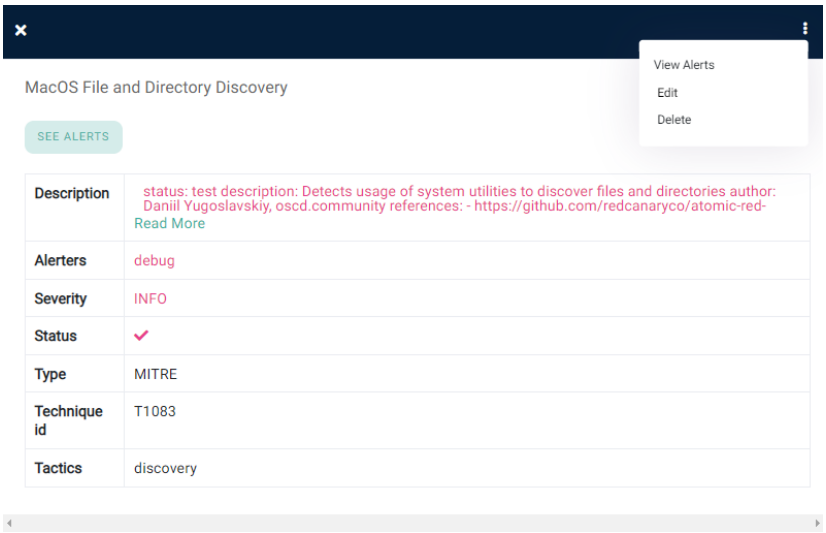


The ER Rules page is displayed.

4. If needed, use the Search field to locate a specific rule by specifying its name.
5. To view details for a rule, click the rule name.

   A pop-up page displays rule details.

6. Click the ellipsis icon and select Edit.



7. Set the value of the Status field to INACTIVE.
8. Click Update.

   A success message is displayed, and the rule is deactivated.

Configure YARA files

EclecticIQ Endpoint Response supports two types of YARA scans; automatic (based on the settings specified in config) and manual (by running a live query).

- Configure automatic YARA scans
- Run a manual YARA scan
- Define rules for alerts

Configure automatic YARA scans

You can configure automatic YARA scans for the:

- Windows, Linux, and macOS operating systems (in the Enterprise Edition)
- Windows only (in the Community Edition)

YARA scanning is supported only for file events on the Linux and macOS operating systems. On the Windows operating system, YARA scanning is supported for file and process events.

To set up automatic YARA scans, you need to perform the following tasks:

1. Upload YARA rules as files to specify characteristics to search for in the enterprise. For more information, see Manage YARA files.
2. Edit the config to include YARA options, namely yara and signatures. These options allow you to identify and group the YARA rules files you uploaded to the EclecticIQ Endpoint Response server. For more information, see Config options for file events.
3. Include paths in the file_paths entry to indicate where to search for the specified characteristics. Add a corresponding entry for each YARA group (specified in step 2) and specify the file paths in which to search for all the signatures associated with the group. Note that only specified file paths are considered for matching against the YARA signatures. For more information, see Config options for file events.
4. Specify needed config options to configure YARA scans for process events on the endpoints running the Windows operating system For more information, see Config options for process events (on Windows only).
5. Configure and set up automatic scans.

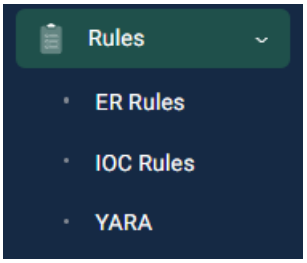
Manage YARA rule files

You can add, view, and delete YARA rule files for the Windows, Linux, and Darwin platforms (in the Enterprise Edition) and Windows only (in the Community Edition).

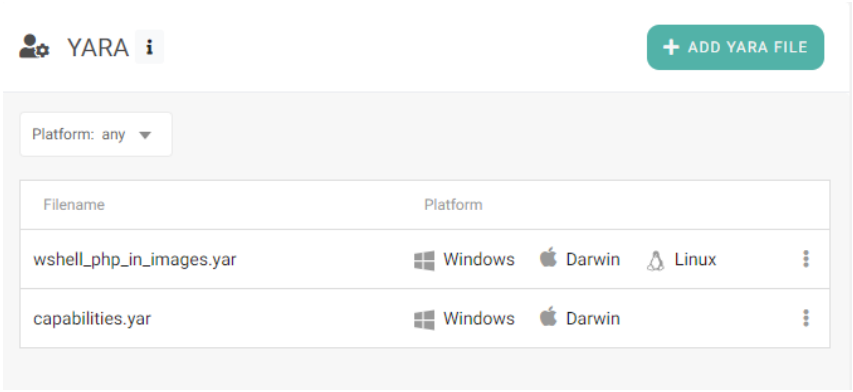
Add a YARA rule file

Perform these steps to add a new YARA rule file.

1. Access the web interface for the server.
2. Navigate to Rules > YARA.

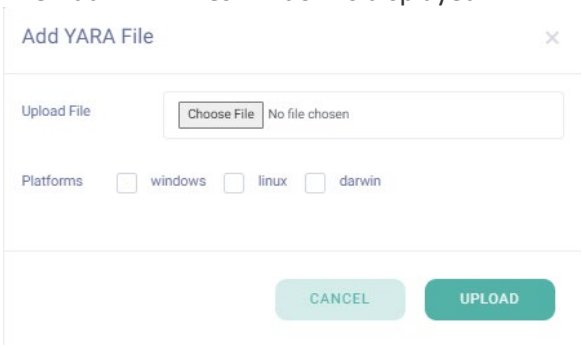


The YARA page is displayed.



3. Click Add YARA File.

   The Add YARA Files window is displayed.



4. Click Choose File and specify the location of the YARA rule file to upload.

   Note that wild cards are not supported in YARA signature file names.

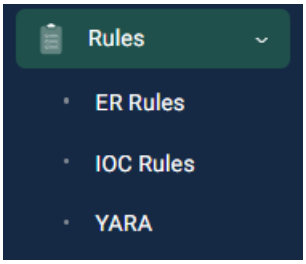
5. Select the platform for the YARA rule file.
6. Click Upload.

   The YARA file is uploaded, and you are returned to the YARA page.

View YARA rule files

Perform these steps to view an existing YARA file.

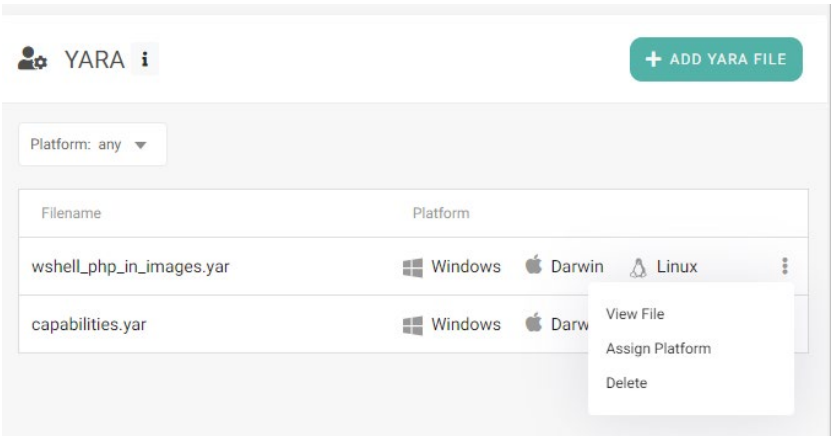
1. Access the web interface for the server.
2. Navigate to Rules > YARA.



   The YARA page is displayed.

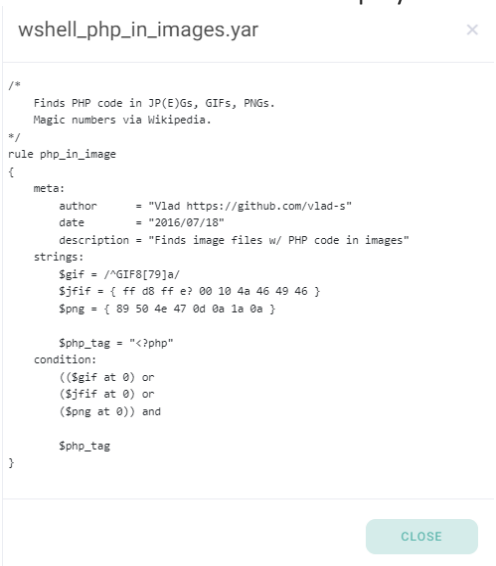
3. Optionally, select the platform for which to view YARA files.

4. Click the ellipsis icon for an entry.



5. Click View File.

   The YARA file contents are displayed.

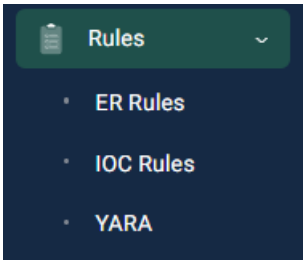


6. Click Close.

Update platform for YARA rule files

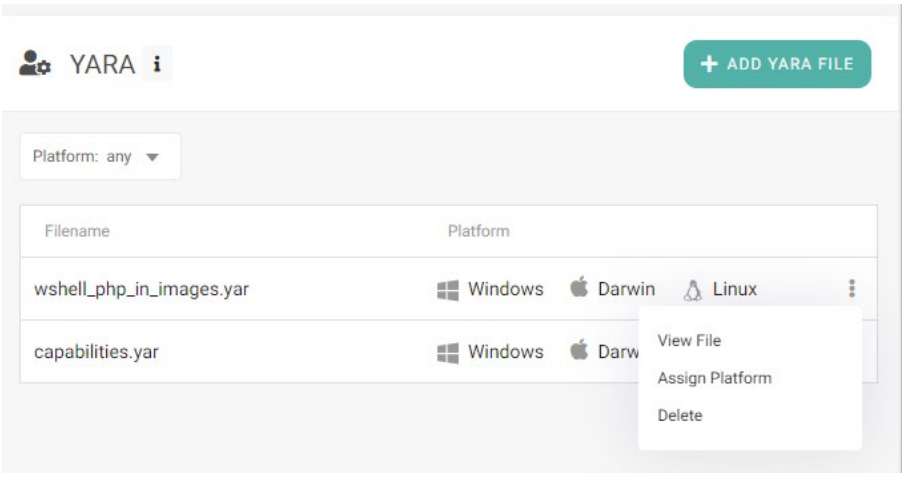
Perform these steps to edit or assign platform to an existing YARA file.

1. Access the web interface for the server.
2. Navigate to Rules > YARA.



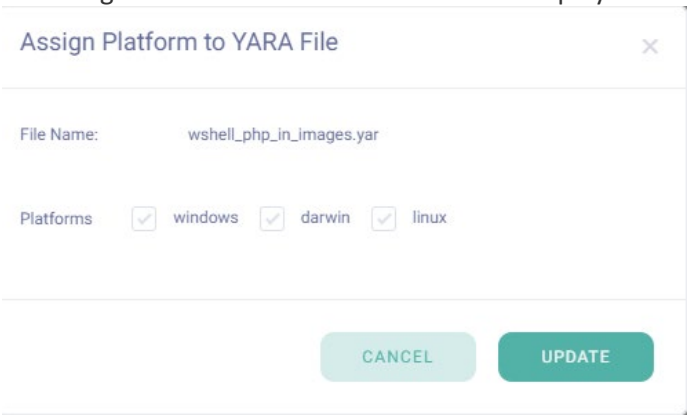
   The YARA page is displayed.

3. Click the ellipsis icon for an entry.



4. Click Assign Platform.

   The Assign Platform to YARA File window is displayed.



5. Select the platforms for the YARA rule file.

   Note: Available only for the Windows platform in the Community Edition.

6. Click Update.

   The platform details are updated for the YARA file.

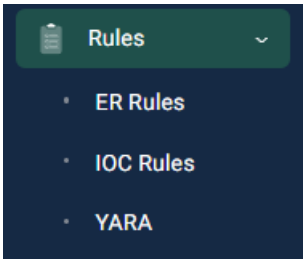
Delete YARA rule files

Deleting a YARA file from the EclecticIQ Endpoint Response UI only deletes it from the server.

To delete a YARA file from the agent, you must manually run a response action. For more information, see Create a response action.

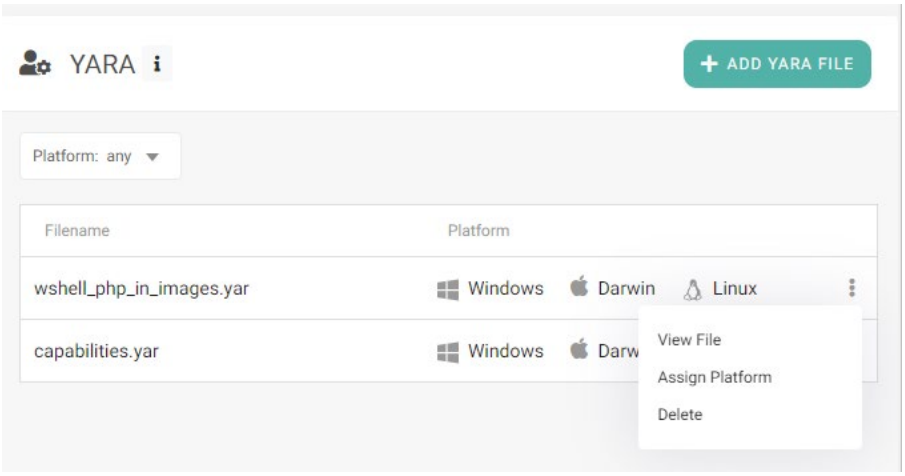
Perform these steps to delete an existing YARA file.

1. Access the web interface for the server.
2. Navigate to Rules > YARA.



The YARA page is displayed.

3. Select the platform for which to delete the YARA file.
4. Click the ellipsis icon for an entry.



5. Click Delete.

   A confirmation dialog box is displayed.

6. Click Yes, delete it.

A success message is displayed and the YARA file is removed from the YARA page.

Config options for file events

Here is syntax you must use when defining YARA settings in the config. The syntax is the same as for osquery.

Use the following syntax to specify the file events to match with YARA rules. Two options need to be added in the yara entry: file_paths and signatures along with the EclecticIQ Endpoint Response file_paths entry.

```
"yara": {
   "file_paths": {
       "test_files_1": [ "test_group1" ],
       "test_files_2": [ "test_group2" ]
       }
  "signatures": {
       "test_group1": [
         "C:\\Program Files\\plgx_osquery\\yara\\eicar.yar" ],
       "test_group2": [
         "C:\\Program Files\\plgx_osquery\\yara\\ExampleRule.yar" ]
       },

   },

   "file_paths": {
```

```
        "test_files_1": [ "C:\\Users\\Admin\\Downloads" ],
        "test_files_2": [ "C:\\Users\\Default" ]
    }
```

This config implies that all YARA signatures included in:

- test_group1 will be matched to any files created or modified in the folder C:\Users\Admin\Downloads
- test_group2 will be matched to any files created or modified in the folder C:\Users\Default

Config options for process events

While file events are scanned by default on the Windows platform, to scan process events you must set the custom_plgx_EnableYaraProcessScan parameter in the config to true.

1. Open the config for the Windows operating system.
2. Under options, add the custom_plgx_EnableYaraProcessScan parameter.
3. Set the value of the parameter to true.

   ```
   "options" :
   {
      "custom_plgx_EnableYaraProcessScan": "true"
   },
   ```

   Note that the options and values are both case sensitive. For more information on config parameters, see Understand config parameters.

4. Click Update.

Also, use the following syntax to specify the process events to match with YARA rule files (on Windows only). Two options need to be added in the yara entry: process_paths and signatures along with the EclecticIQ Endpoint Response process_paths entry.

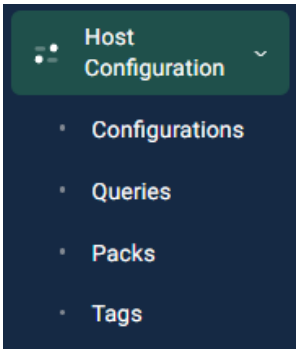
```
"yara": {
    "process_paths": {
      "test_files": [ "eicar_test_group" ]
    },

    "signatures": {
      "eicar_test_group": [
        "C:\\Program Files\\plgx_osquery\\yara\\eicar.yara"
      ]
    },
  },

  "process_paths": {
    "test_files": [ "C:\\mal_prog.exe" ]
  }
```

This config implies that all YARA signatures included in eicar_test_group will be matched with the C:\mal_prog.exe process.

Set up automatic scans

Perform these steps to set up automatic YARA scans.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Configurations.



   The Configurations page is displayed.

3. Select the platform for which to edit the config.
4. Select the config to edit (by clicking the appropriate tab).
5. Scroll to the Additional Config and Filters section.

6. Specify the file events to match with YARA rule files.

   For more information, see Config options for file events.

7. Specify the process events to match with YARA rule files(on Windows only).

   For more information, see Config options for process events.

8. Click Update.

Run a manual YARA scan

When configured, YARA scans are run automatically for each file modification (Windows, Linux, and macOS) or process launch event (Windows only). Alternatively, you can run an on-demand scan to query for a specific criterion.

To run a manual YARA scan, use the Live Query Builder. For more information on how to run live queries, see Run a live query.

Here are examples of queries you can run for manual or on demand YARA scans.

Windows	`select * from win_yara where target_path like 'c:\test\%' and sig_group= 'yara_eicar_test_group'`
	
	Note: If you are using sig_group for manual YARA scans, ensure you define the group composition in the config file. For more information, see Config options for file events and Config options for process events.
	
	`select * from win_yara where target_path like 'c:\test\%' and sigfile = 'C:\Program Files\plgx_osquery\yara\eicar.yara'`
	
	Note: In the query, you must specify the target_path and use the like operator for the Windows platform.

Linux and macOS	`select * from yara where path like '/home/%' and sigfile = '/usr/bin/yara/eicar.yara'`

Define rules for alerts

After YARA rules are configured and YARA files are added, they are pushed to the agents and the YARA scan is run. If the YARA scan finds a match for a defined YARA rule, the relevant tables are populated.

Scan type	***Platform***	***Table name***
Automatic YARA scans	Windows	win_yara_events
	Linux and macOS	yara_events
Manual YARA scans	Windows	win_yara
	Linux and macOS	yara

To generate alerts based on YARA scans, you must define rules in your environment for events in the respective tables for automatic and manual scans. When defining YARA-specific rules, you can:

- For Windows, use the windows_real_time_events table and set event ID to 14
- For Linux and macOS, use the yara_events table

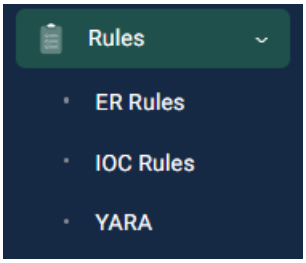
Add other specific conditions to the rule, as needed, based on your needs. For more information on defining rules, see Add new rules .

Configure IOCs

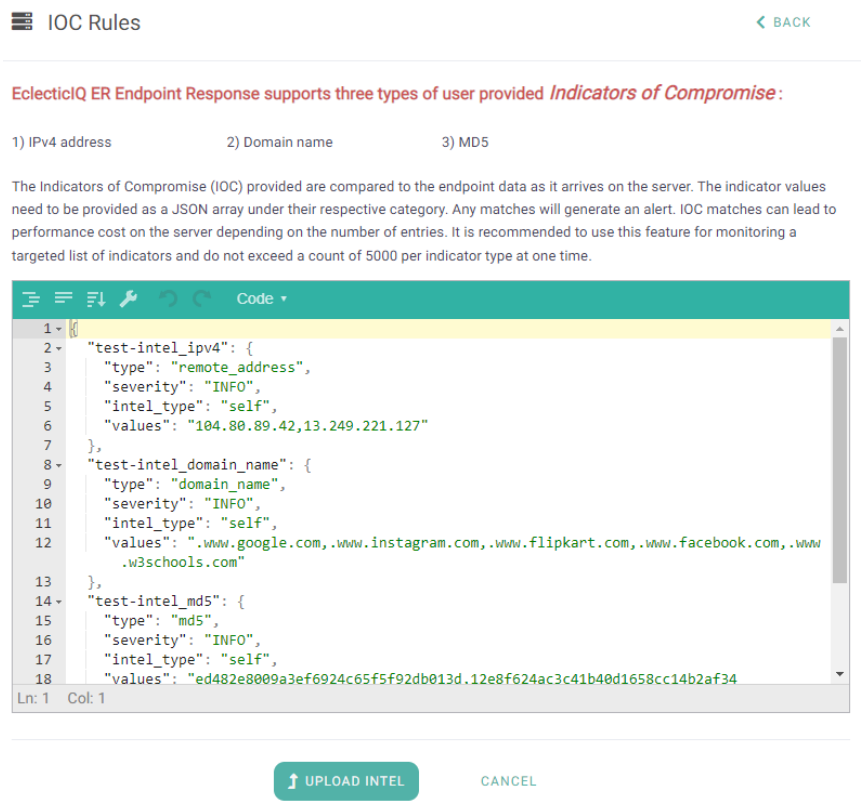
When defining IOCs, bear in mind that extensive IOC matching may lead to performance degradation on the server. We recommend that you use this feature to monitor specific and targeted indicators. To ensure performance is not compromised, we recommend you define 5000 or fewer indicators of each type.

Perform these steps to define IOCs.

1. Access the web interface for the server.
2. Navigate to Rules > IOC Rules.



The IOC Rules page is displayed.



3. Specify the details for the IOC.

   Here are a few examples.

```
"sample_test_ipv4": {
    "type": "remote_address",
    "severity": "INFO",
    "intel_type": "self",
    "values": "x.xx.x.xx,y.yy.y.yy"
  },
  "sample_test_intel_md5": {
```

```
    "type": "md5",
    "severity": "INFO",
    "intel_type": "self",
    "values": "xxxxxxxxxx,yyyyyyyyyyy"
}
```

4. Click Upload Intel.

Configure threat intelligence sources

The EclecticIQ Endpoint Response platform can integrate with the following external threat intelligence sources:

- VirusTotal
- IBM X-Force
- AlienVault

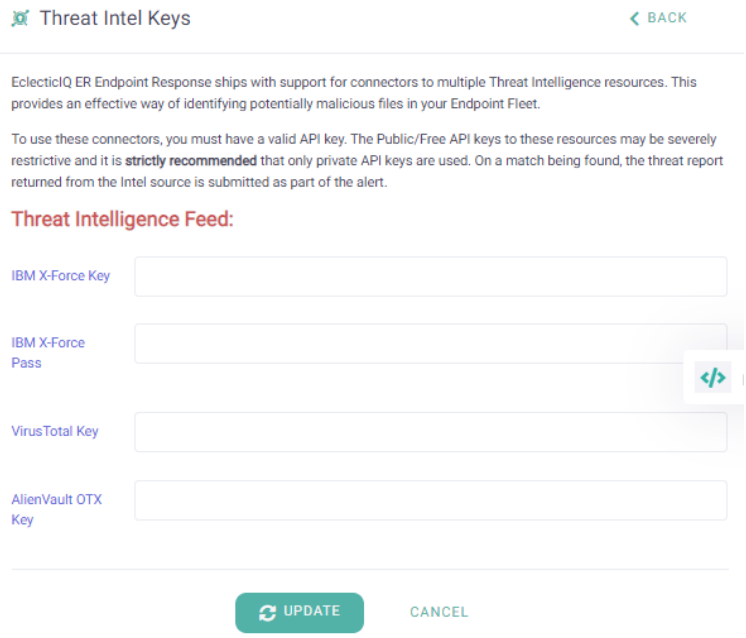
When configured, the EclecticIQ Endpoint Response platform performs automated reputation checks for all file hashes (MD5/SHA1/SHA256). Event data is matched to the feed from the configured threat intelligence sources every 24 hours.

Specify keys

Perform these steps to specify the keys to integrate with external threat intelligence sources.

1. Access the web interface for the server.
2. Navigate to Settings > Threat Intel Keys.

   The Threat Intel Keys page is displayed.



3. Specify the threat intelligence API keys.

   When integrating with IBM X-Force, ensure you specify both the key and pass.

4. Click Update.

   A confirmation dialog is displayed.

5. Click Yes, Update.

A success message is displayed after the keys are updated.

6. Click OK.

Note: To deactivate or remove a configured threat intel source, remove its key from the Threat Intel Keys page and click Update.

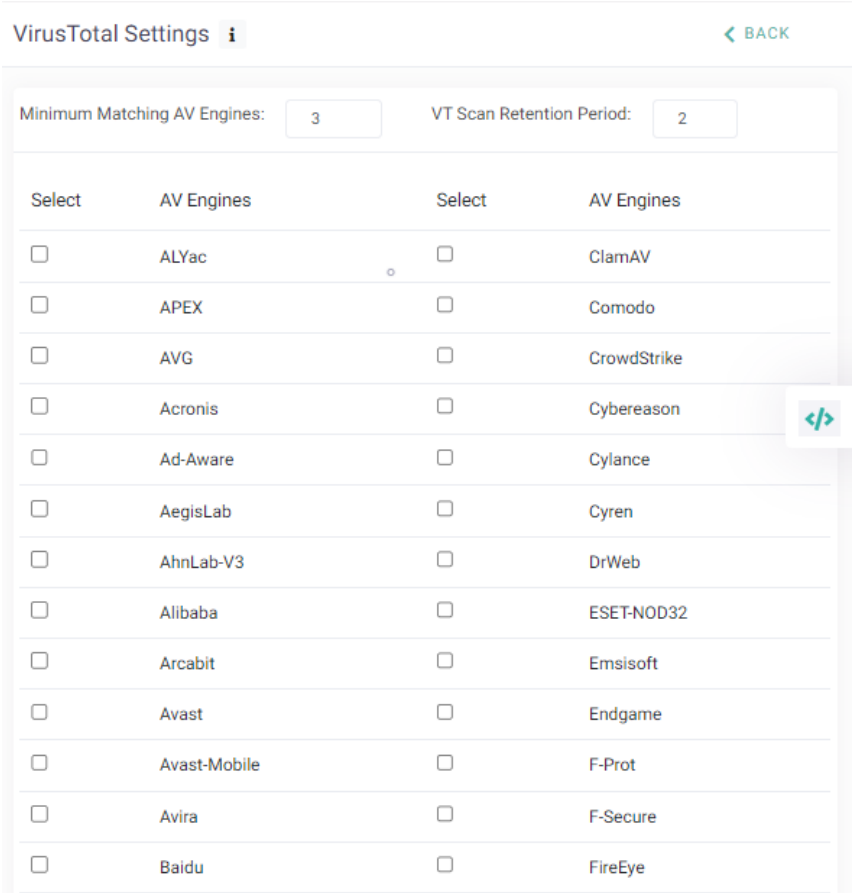
Configure VirusTotal

The VirusTotal database is a collection of multiple anti-virus (AV) engines. If integrated with VirusTotal, the EclecticIQ Endpoint Response server matches collected file hashes against the VirusTotal database.

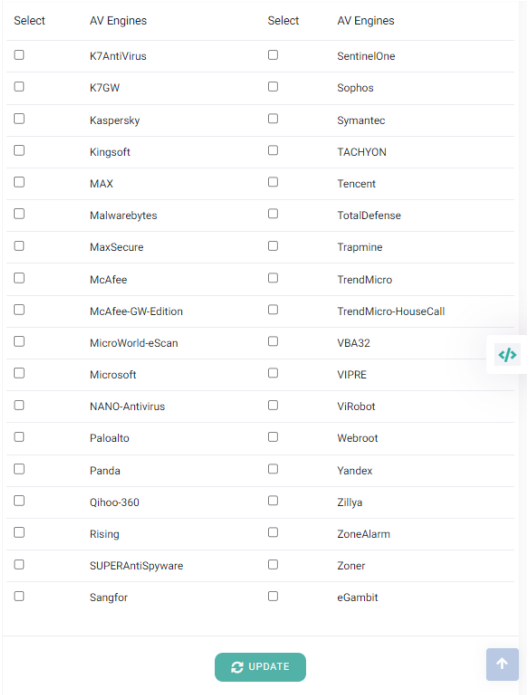
Complete the following steps to configure VirusTotal settings:

1. Access the web interface for the server.
2. Navigate to Settings > VT Settings.

   The VirusTotal Settings page is displayed.



3. Specify the values for the following fields.
   - Minimum Matching AV Count – This value comes into play if none of the selected AV engines provide a conclusive indication for a file hash. Then, the remainder of the AV engines (no selected on the page) are considered. This value specifies the number of non-selected AV engines that must indicate that a file is harmful before an alert is generated. An alert is generated only when the number of (non-selected) AV engines indicating that the hash is unsafe is higher than the value specified.
   - VT Scan Retention period – Indicates the duration (in days) after which a file hash value is refreshed.
4. From the list, select the AV engines with which to match file hashes.



   Even if one selected AV engine indicates that a file is harmful, an alert is generated.
5. Click Update.

   A confirmation dialog is displayed.
6. Click Yes, Update.

   A success message is displayed, and you are returned to the VirusTotal Configuration page.

Configure alerts

An alert indicates an important occurrence in the enterprise. An alert is generated when incoming event data matches a predefined rule or IOC, or when event data (for last 24 hours) matches the feed from the configured threat intelligence sources.

- Specify email details
- Set up alert aggregation

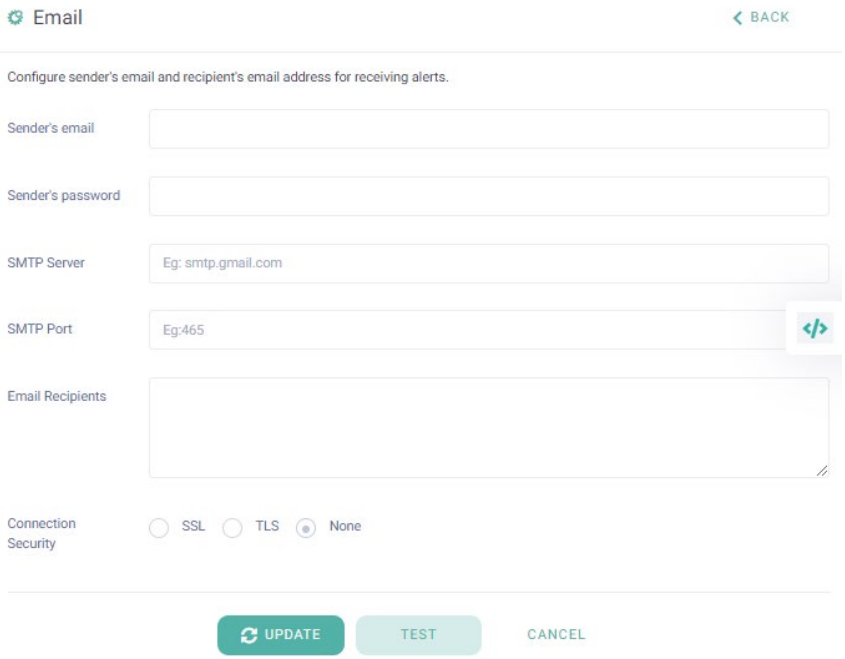
Specify email details

When an alert is generated, you can choose to get information for the alert through e-mail.

Perform these steps to specify email configuration to use for alerting through email.

1. Access the web interface for the server.
2. Navigate to Settings > Email.

   The Email page is displayed.



3. Specify the details, such as the email ID, password, SMTP port and address, recipients for the email, and connection type.
4. Click Test to verify the provided details work correctly.

   The Checking Email Credentials message box is displayed while the server verifies the provided information. A success message is displayed if the details are accurate.

5. Click Update to save the email settings.

Set up alert aggregation

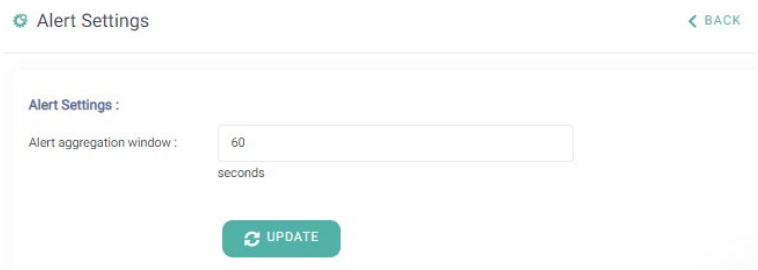
In some cases, an alert may be generated repeatedly based on the activities on an endpoint. EclecticIQ Endpoint Response server can aggregate alerts generated based on rules for an endpoint. Alerts generated based on IOCs and threat intel sources are not aggregated. This in effect removes duplicate alerts and allows you to focus on meaningful information.

For alert aggregation or grouping, you can specify the time window (in seconds) in which to aggregate alerts.

Perform these steps to configure alert aggregation settings.

1. Access the web interface for the server.
2. Navigate to Settings > Alert Settings.

   The Alert Settings page is displayed.



3. Specify a value for alert aggregation (in seconds).
4. Click Update.

Investigation

Using the EclecticIQ Endpoint Response server, you can review and monitor endpoint activity in your enterprise and drill down into details to investigate possible suspicious activities.

- View graphs and dashboards
- Examine host information
- Manage alerts
- Respond to alerts
- Define carves
- Searching for files and indicators

Alternatively, you can stream query results and alert data from the endpoints to backend systems for investigation, such as Splunk, ELK, and GrayLog by using an rSysLog container. For more information on configuring the rSysLog container, see the *EclecticIQ Endpoint Response Deployment Guide.*

EclecticIQ Endpoint Response also provides APIs that allow you to pull query results and alert data for investigation. For more information on available APIs, see the *EclecticIQ Endpoint Response REST API Guide*.

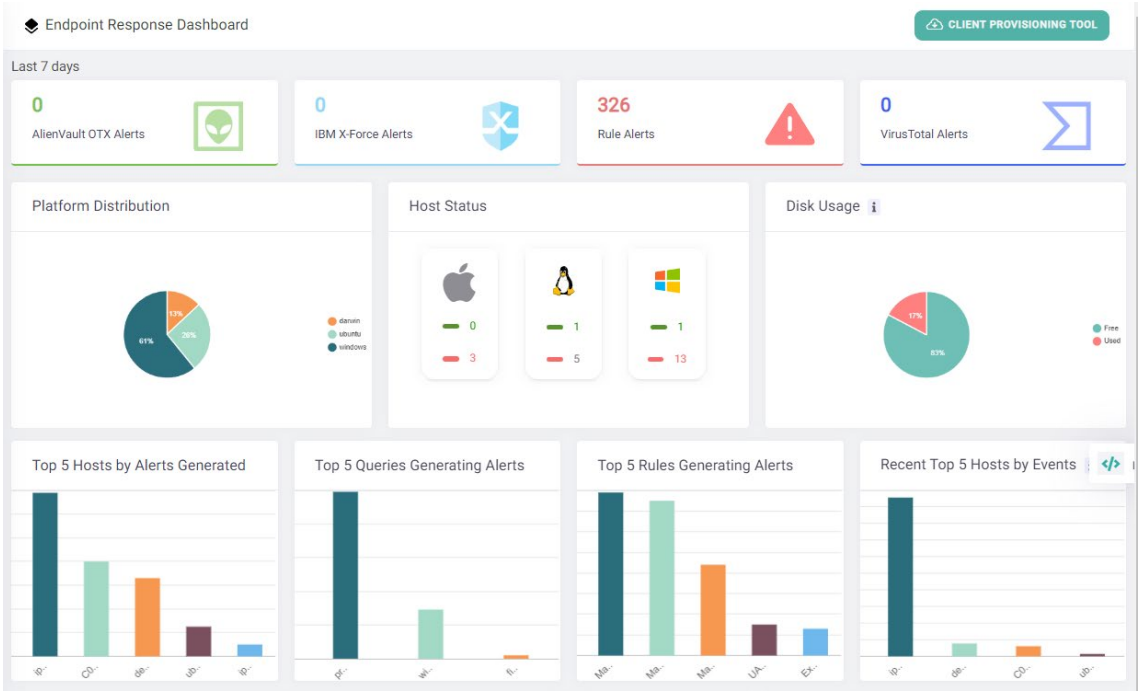
View graphs and dashboards

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

Perform these steps to view the available graphs and charts for your environment.

1. Access the web interface for the server.
2. Navigate to the Dashboard page.

   The Endpoint Response Dashboard page displays the available graphs and charts.



3. Review the alert information.

   The four tabs at the top of the page represent the alerts received based on the different rules. The Rule Alerts tab represents the alerts generated based on the EclecticIQ Endpoint Response rules. If configured, the AlienVault OTX, IBM X-Force, and VirusTotal tabs display alert count for generated alerts for each threat intel source.

4. Review the graphs and charts.

   - 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 endpoints that are online and offline.
   - Disk Usage - For a single or monolithic server, this graph depicts disk usage for the server. In a clustered environment, this graph depicts the disk usage for the server running the UI application.
   - Top 5 Hosts by Alerts Generated - Lists the five endpoints generating the highest number of alerts in your environment. Hover over a bar to know the alert count for the corresponding endpoint.
   - Top 5 Queries Generating Alerts - Lists the five queries generating the highest number of alerts in your environment. 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 environment. Hover over a bar to know the alert count for the corresponding rule.
   - Recent Top 5 Hosts by Events - Lists the five endpoints with the most events generated for the day (in UTC).
   - Hourly Client Data Volume - Displays the volume of data (in bytes) received from all endpoints 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 endpoints 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 endpoints and are awaiting processing at the server.

Examine host information

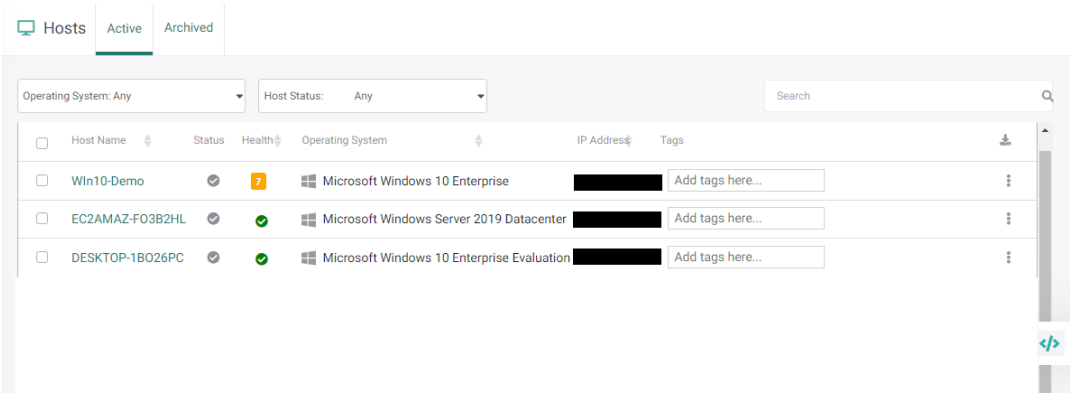
The Hosts page serves as a central console to monitor and manage endpoints.

Review hosts

Perform these steps to review host or endpoint information.

1. Access the web interface for the server.
2. Click Hosts in the navigation pane.

   The Active tab lists all endpoints managed by the EclecticIQ Endpoint Response server.



3. Review information for the endpoints.

Field	***Description***
Host Name	Displays the hots name.
Status	Indicates if the endpoint is online, offline, or degraded. • An online status indicates that the EclecticIQ Endpoint Response agent on the endpoint is running and communicating at regular intervals with the EclecticIQ Endpoint Response server. • An offline status indicates that the endpoint is down or disconnected and currently not communicating with the EclecticIQ Endpoint Response server. • A degraded status (available only in the Enterprise Edition) indicates that the EclecticIQ Endpoint Response agent on the endpoint is running and connected to the EclecticIQ Endpoint Response server, but only limited functionality is available on the EclecticIQ Endpoint Response server. This state typically occurs when the endpoint has either not communicated with the EclecticIQ Endpoint Response server for the last 5 minutes or when the Response Action status is disabled.
Health	Depicts the status of alerts received from the endpoint. A green circle with a check mark ( ) indicates that no unresolved alerts exist for the endpoint. An orange square with a number (66) indicates the number of unresolved alerts for the endpoint.
Operating system	Specifies the operating system running on the endpoint.
IP Address	Displays the IP address of the endpoint.
Tags	Lists the tags, if any, are assigned to the endpoint.

4. Select options in the Platform and Host Status drop-down lists to view online and offline endpoints for the selected operating system.
5. Optionally, enter a keyword in the Search field to find specific information.

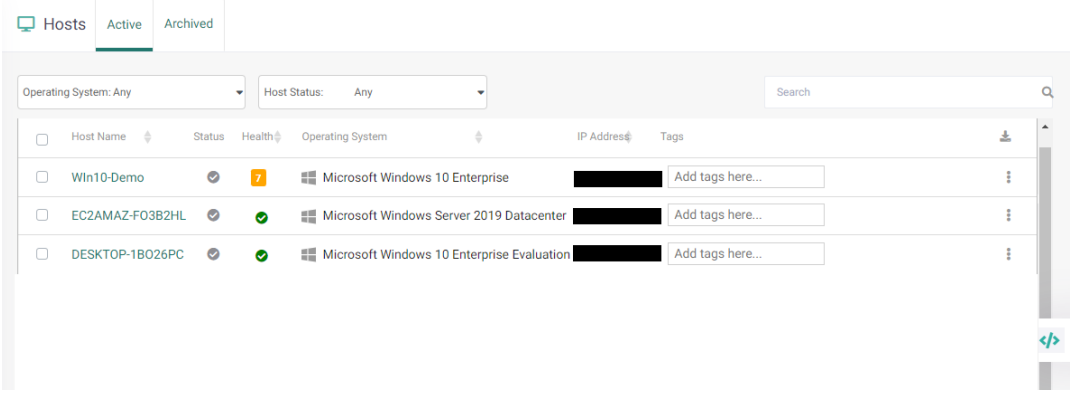
You can search based on host name, operating system, IP address, and tags.

View host health and activity

Perform these steps to review endpoint details and activities.

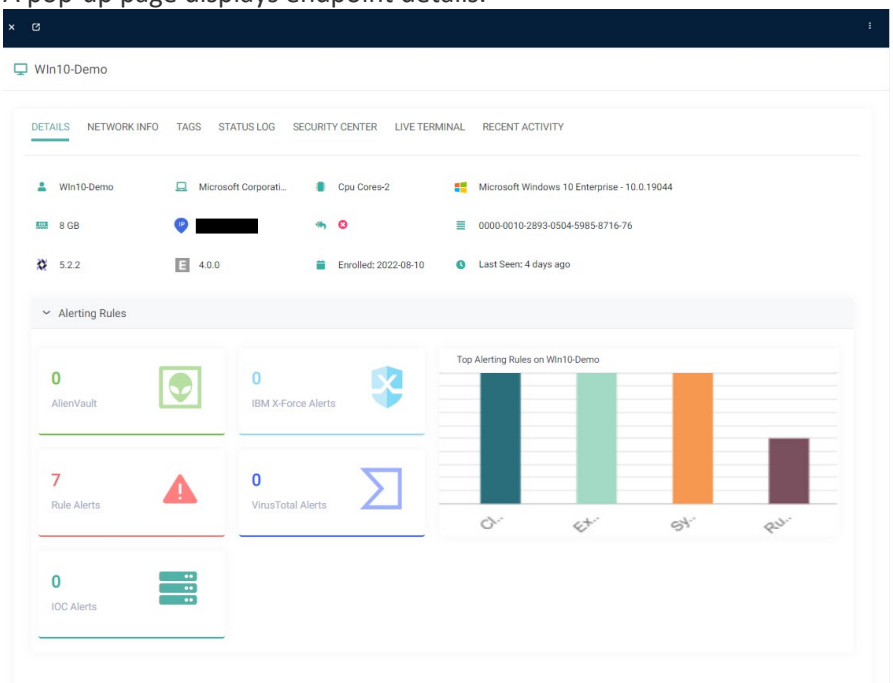
1. Access the web interface for the server.
2. Click Hosts in the navigation pane.

   The Active tab lists all managed endpoints.



3. Click a row to review endpoint details.

   A pop-up page displays endpoint details.



   Note: The Response Action status (visible in the graphic) is available only in the Enterprise Edition.

4. Review the tabs on the page.

Tab	***Description***
Details	Provides the following endpoint information. • Host name, host ID, and IP address • Serial number, make, and model details • CPU cores and memory information

	• Operating system, Osquery, and EclecticIQ Endpoint Response versions • Agent enrolment date, last seen time, and response action status • Top rules that have generated alerts on the endpoint • Alerts based on rules and threat intel sources
Network Info	Lists network-specific information for the endpoint.
Tags	Lists all tags, packs, and queries assigned to the endpoint.
Status Log	Selecting the Show Status Log option review entries from the osquery logs of the endpoint.
Security Center	For endpoints running Windows version 8 or higher, this tab displays the status of security and antivirus products. Using this tab you can also manage Windows Defender and review the Windows Defender action center logs. **Note**: This tab is not available in the Community Edition.
Live Terminal	Based on the operating system the endpoint is running, you can run batch, PowerShell, or shell scripts on the endpoint. This tab is available only if the Response Action status is active for the endpoint. For more information, see Execute scripts using a live terminal. **Note**: This tab is not available in the Community Edition.
Recent Activity	Lists the names of all queries run for the endpoint along with the count of events received from the endpoint for each query. Only queries assigned to endpoint are listed on the Recent Activity list. For details of the assigned queries, review the config (assigned to the endpoint) and the Tags tab (after clicking the endpoint on the Hosts page). You can click the query name in the left pane to view events received for the query in the right pane. Click an event in the right pane to review its details. Optionally, use the Search field to locate specific details. All column values can be searched but not column names. **Note**: For endpoints running the Windows operating system, an additional event filter is available when viewing events received windows_real_time_events query. Select a value from the list (on the top right) to view corresponding events. If needed, click CSV to download table data to a file for further analysis. **Note**: Starting with the 4.0.0 release, the EclecticIQ Endpoint Response server provides visibility into events that run within Docker containers. For process and socket events, the bpf_process_table and bpf_socket_table tables include the container_ID field. This field is populated only for events generated for containers. The feature is available only on the Linux platform for the following distributions: • Ubuntu 18, 20, and 22 • Debian 10 and 11 • RHEL 8 and 9 • Centos 8 • Fedora 33, 34, and 36 • OpenSUSE 12 and 15 • Amazon Linux 2

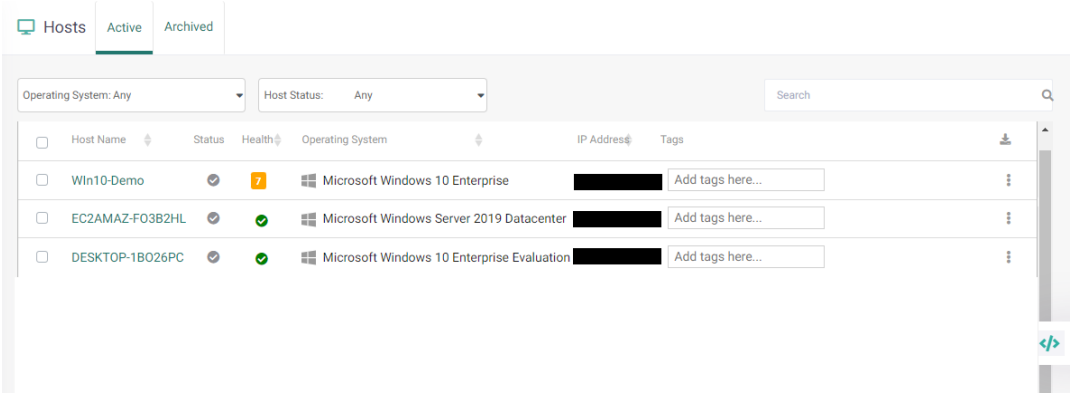
Export host details

You can export details for all endpoints in your environment for analysis.

Perform these steps to export endpoint details.

1. Access the web interface for the server.
2. Click Hosts in the navigation pane.

   The Active tab lists all managed endpoints.



3. Click the download icon (right corner of the table).

   Details for all endpoints are added to a CSV file.

Review agent service status on endpoint

Starting with the 4.0.0 release, the EclecticIQ Endpoint Response application icon is available in the system tray on Windows endpoints (only in the Enterprise Edition).

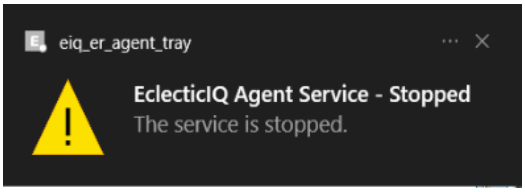
The icon () is available after installation and allows you to review application status and perform various tasks.

Note: To change the default EclecticIQ Endpoint Response icons, replace the three app tray files in the C:\program files\plgx_osquery\ folder and restart the tray application. The icon files included in the folder are: eiq_er_tray.ico (icon for agent stopped state), eiq_er_tray_svc_err.ico (icon for error state), and eiq_er_tray_svc_ok.ico (icon for normal state).

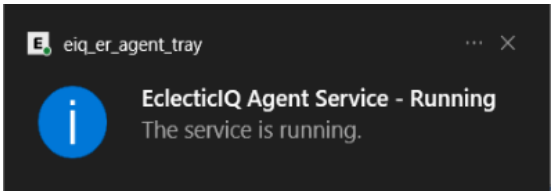
Perform these steps to check the status of the EclecticIQ Endpoint Response application from an endpoint.

1. Double-click the icon to review statistics for the EclecticIQ Endpoint Response agent.
2. Right-click the icon to view available menu options.
3. Optionally, start, stop, and restart the service (available only to users with Administrator role).

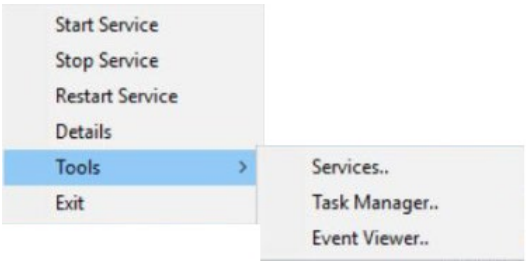
   - Click Stop Service to stop the agent service.



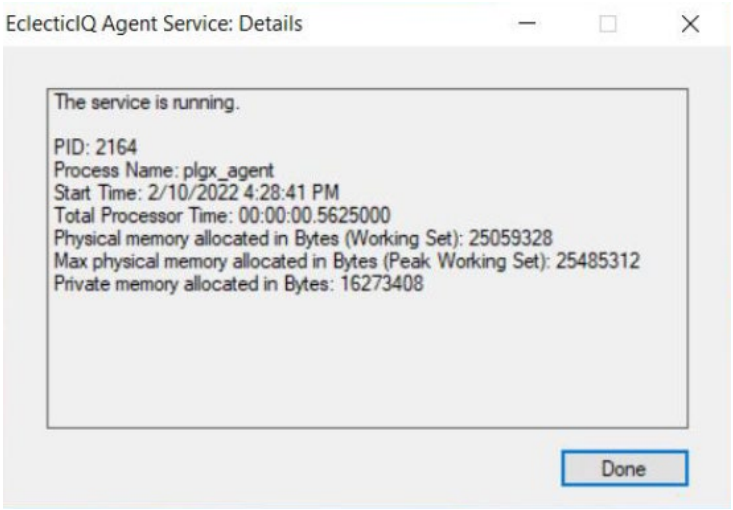
   - Click Restart Service to restart the agent service.



4. Access tools, such as the Task Manager, Event Viewer, and Services.



5. Review agent service details, including PID, process name, start time, and memory information.



6. Click Close.

Manage alerts

An alert indicates a notable occurrence in the enterprise. An alert is generated when incoming event data matches a predefined rule or IOC, or when event data (for last 24 hours) matches the threat intel feed.

Alerts allow you to monitor and track important events in your environment. Based on the alert severity and importance, you can take needed actions for an alert. You can choose to ignore it or act on it.

The Alerts page is the central console that allows you to manage and review alerts.

- Review generated alerts
- Examine an alert in detail
- Export alert details

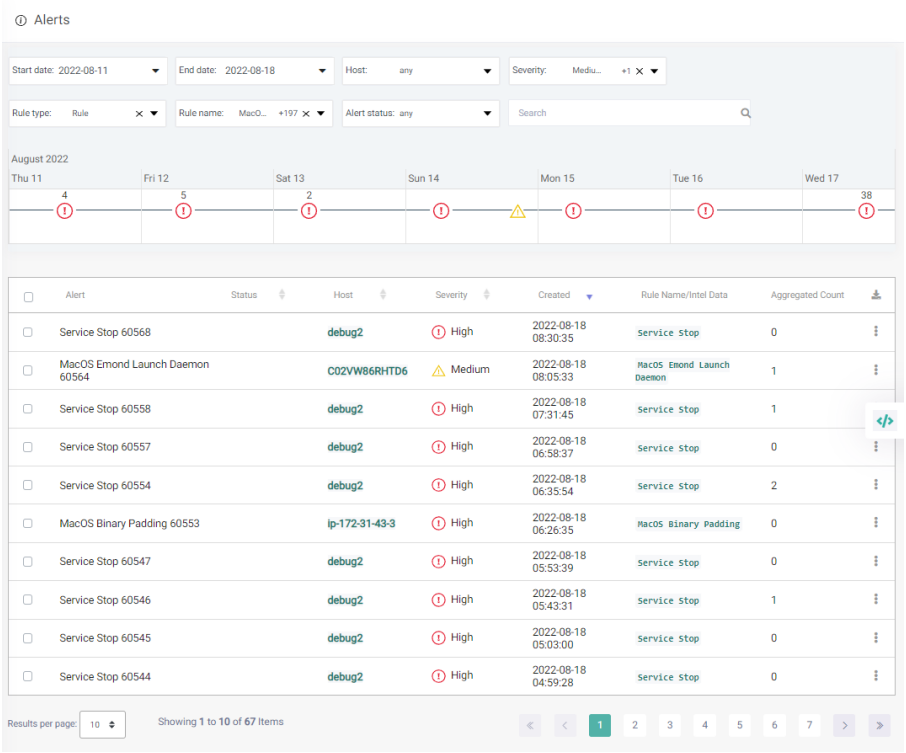
Review generated alerts

Perform these steps to view the generated alerts.

1. Access the web interface for the server.
2. Navigate to the Alerts page.

   By default, the Alerts page displays alert data for the last 7 days.

3. Select values from the Start date, End date, Host, Severity, Rule type, Rule name, and Alert status drop-down lists (on the top of the page) to filter and view relevant alerts.



   The alert timeline is updated based on the filters applied (available only in the Enterprise Edition).

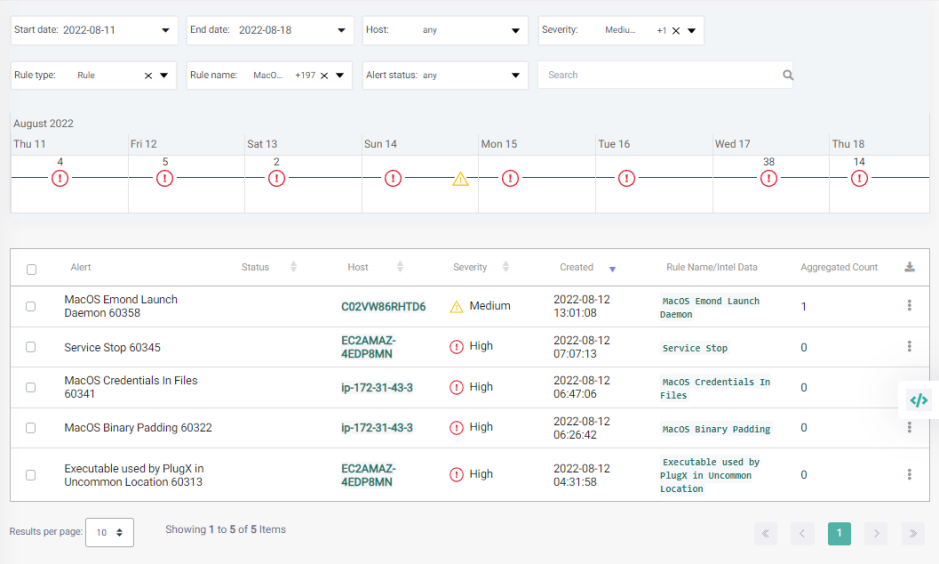
4. Optionally, enter a keyword in the Search field to find specific information.

You can search based on endpoint name, severity, rule name, or intel data. Note that you cannot search for alerts based on alert name.

5. Review the event timeline for your enterprise to understand the traffic trend.

   Each cluster on the timeline represents a collection of alerts. Hover over a cluster to see its details.
   Note: The alert timeline is unavailable in the Community Edition.

6. Click an event cluster to see the alerts contained in that cluster (available only in the Enterprise Edition).



7. Click an endpoint name to review its details.

   A pop-up page displays endpoint details. For more information on the fields on this page, see View host health and activity.

8. Review the severity information.

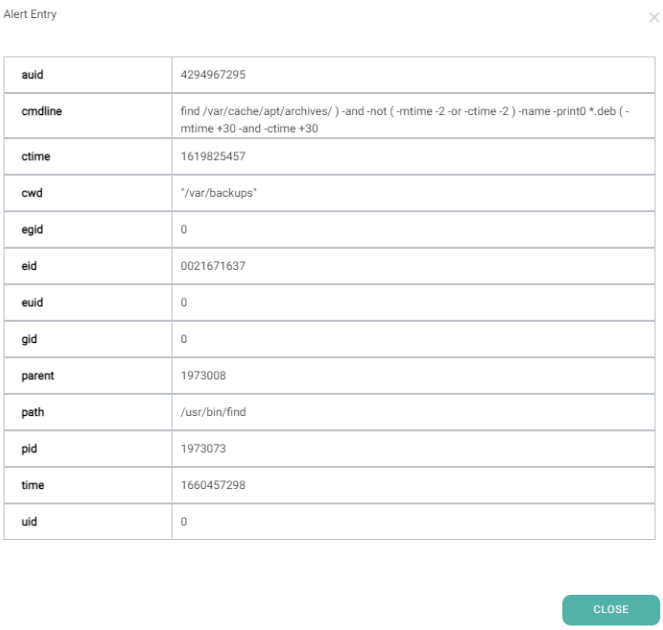
   For alerts, severity values are info, low, medium, high, and critical.

9. Click the rule name to view details of the rule based on which the alert was generated.

   A pop-up page displays rule details. For alerts generated based on IOCs and threat intel sources, the Rule Name field is blank.

10. Click the ellipsis icon for an alert and select View alert entry to view the events associated with the alert.

    The Alert Entry window is displayed. You can view event-related details, such as ID, parent, path, and time.



11. Click Close to return to the Alerts page.

Examine an alert in detail

When using the Enterprise Edition, you can deep dive or further investigate an alert to determine any actions you might need to take.

Note: Comprehensive investigation abilities for alerts are only available to the Enterprise Edition and unavailable in the Community Edition.

Perform these steps to investigate an alert.

1. Access the web interface for the server.
2. Navigate to the Alerts page.

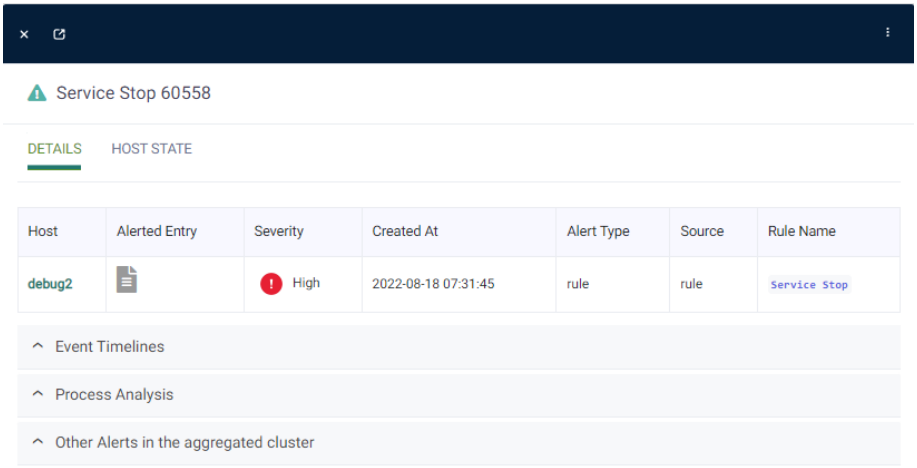
   By default, the Alerts page displays alert data for the last 7 days.

3. Select values from the Start date, End date, Host, Severity, Rule type, Rule name, and Alert status drop-down lists (on the top of the page) to filter and view relevant alerts.

   For rule-based alerts, the Rule Name field displays the rule that was matched for the generated alert. Click the rule name to view or update the predefined rule. For alerts generated based on IOCs and threat intel sources, the Rule Name and Aggregation fields are blank.

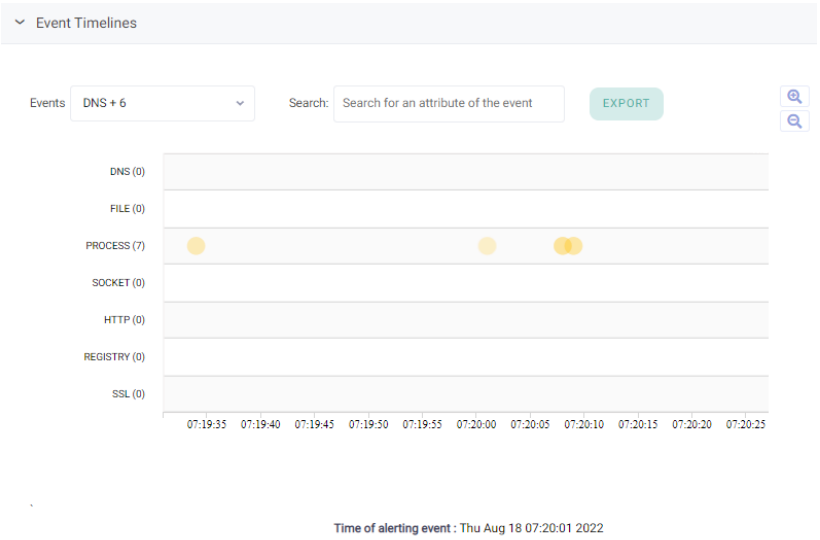
4. Click the ellipsis icon for an alert and select Open alert.

   A pop-up page displays alert details.



5. Review alert details.
    a. View alert-related details, such as endpoint, alerted entry, severity, alert type, source, and rule name.
    b. Click the endpoint name to view corresponding details.
    c. Click alerted entry to view event-related details, such as ID, parent, path, and time.
    d. Review alert details based on the alert source.
        - For rule-based alerts, the rule name field displays the rule that was matched for the generated alert. Click the rule name to view or update the predefined rule.
        - For alerts generated based on IOCs, the Rule Name field is not displayed.
        - For alerts generated based on threat intel sources, the click Intel Data to view details.
6. Review the event timeline and associated events.
    a. Expand the Event Timelines pane.

    This depicts the state of the endpoint around the time the event (associated with the alert) was generated. It provides a graphical view of events depicting event history for the endpoint.



    Each bubble on the timeline represents a cluster of aggregated events. The flashing bubble represents the event associated with the alert.

By default, the period for the event window is 30 seconds before and after the *event* is generated. Click the + button to zoom in and – button to zoom out.

b. Optionally, select the filters from the Events drop down to focus and review events of a specific type, such as DNS, File, Process, Socket, HTTP, PowerShell, SSL, and Registry.
c. Click a bubble on the timeline to view the details for all aggregated events in the Event info pane.
d. Click the down arrow for an event in the Event info pane to view details for the specific event.
e. If needed, you can use the Search field to locate a specific event.

   You can search for any column value for the events displayed in bubbles.

f. Optionally, click Export as Excel to download event information to an Excel file.

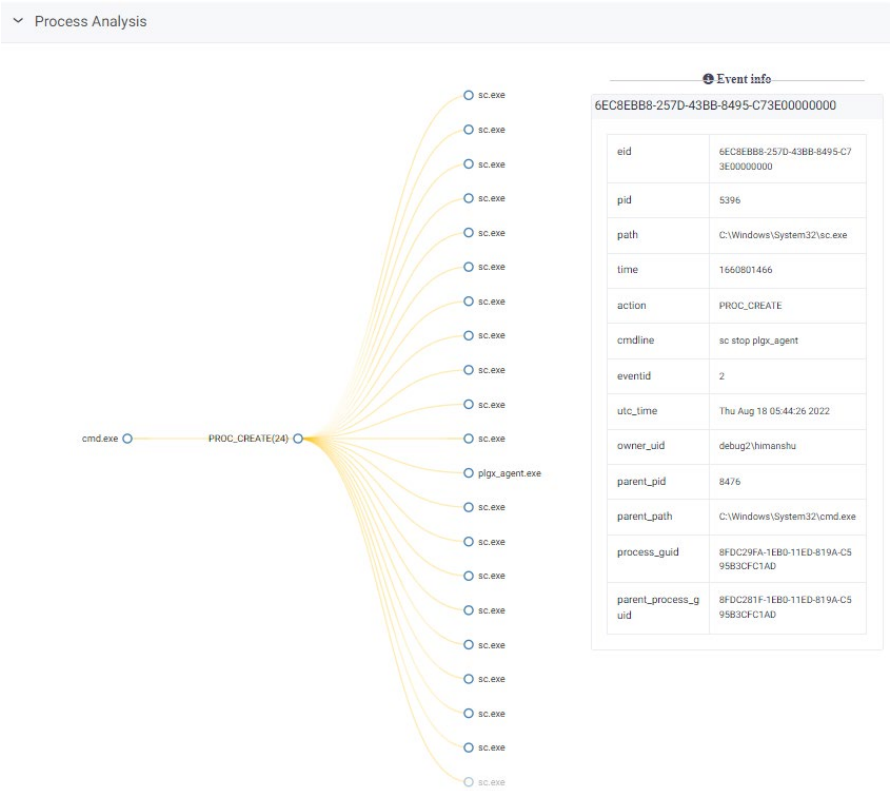
7. Review process details for the event.

   a. Expand the Process Analysis pane.

      This depicts the process hierarchy of the process associated with the alert and its activities. The flashing node represents the process associated with the alert. The process tree provides a graphical and convenient way to review process details.

      Note: The Process Analysis graph is available only for alerts generated for endpoints running the Windows operating system. The graph is displayed for alerts created on Windows event data for which the process_guid or parent_process_guid field is populated. The *Process analysis not applicable* message is displayed in the pane for alerts generated for endpoints running the Linux and macOS operating systems.

   b. Clicking on a node updates the tree and associated nodes to reflect the activities for the selected node.

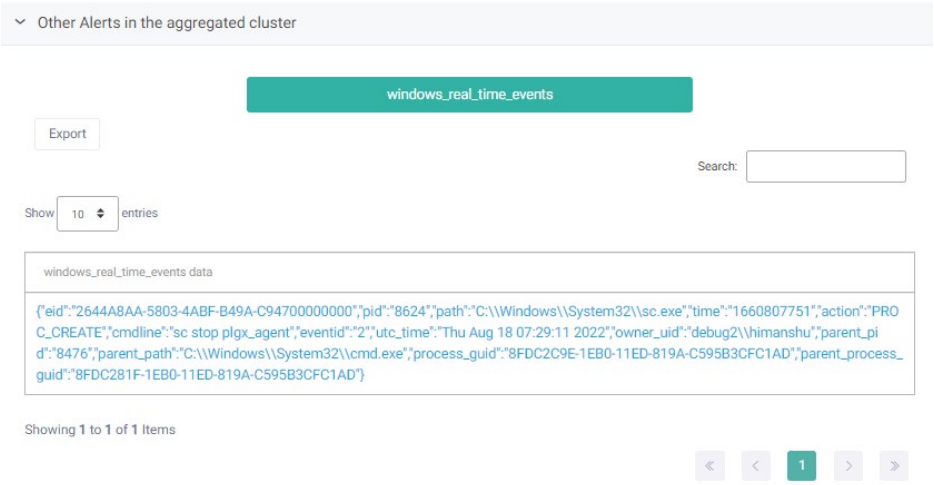


The details for the selected node are also displayed in the Event info pane.

c. Traverse the tree by clicking on the various nodes in the tree to explore the process hierarchy.

8. Review other alerts in the cluster (only available for rule-based alerts).

   a. Expand the Other Alerts in the aggregated cluster pane.



   The EclecticIQ Endpoint Response server aggregates alerts (and removes duplicates) based on rules for an endpoint. Alerts generated based on IOCs and threat intel sources are not aggregated.

   b. Click the event category.

      The list displays all events associated with the alerts aggregated to form the cluster.

   c. Click an alert entry to view associated event details, such as event ID, action, path, and GUID.
   d. Optionally, you can use the Search field to locate a specific event.
   e. Optionally, click Export to download a CSV file with event information.

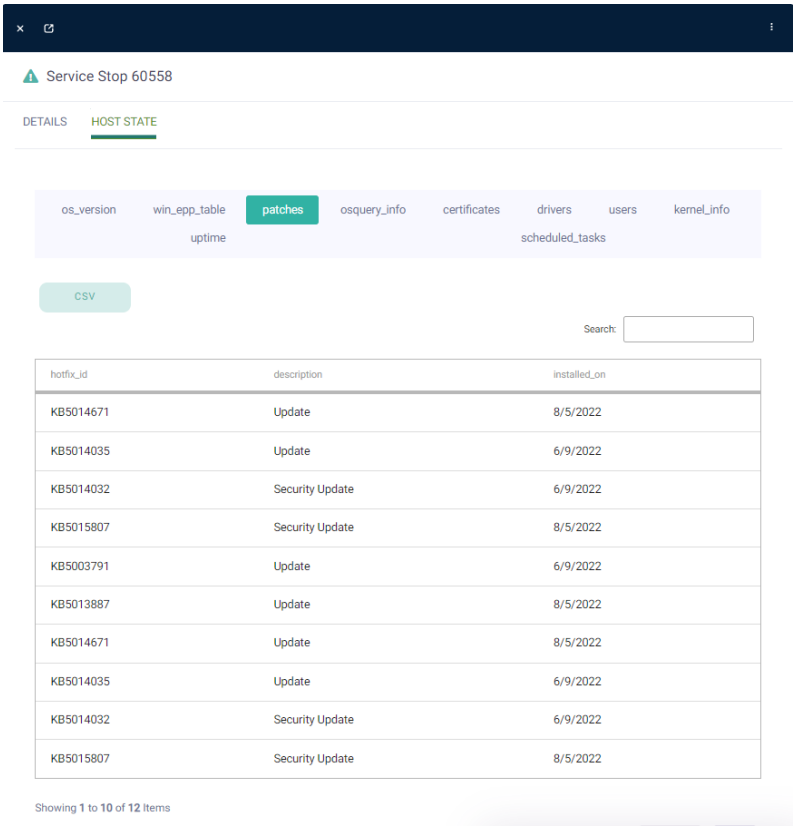
9. Click the Host State tab to view endpoint-related information.

   a. View details in the various tabs, such as scheduled tasks, uptime, drivers, operating system, certificates, and patches.

      The Host State tab includes multiple tabs where each tab corresponds to a seeded query that is run for the platform (associated with the endpoint). Each tab provides most recent information for the endpoint. Here are the tabs that are available for each operating system.

Windows	• os_version • kernel_info • startup_items • drivers • etc_hosts • osquery_info • wmi_cli_event_consumers • wmi_script_event_consumers • users • uptime • certificates • chrome_extensions

	• ie_extensions • scheduled_tasks • appcompat_shims • powershell_events_script_blocks
Linux	• etc_hosts • deb_packages • iptables • kernel_info • osquery_info • rpm_packages
macOS	• chrome_extensions • etc_hosts • homebrew_packages • osquery_info • startup_items



b. Optionally, for endpoint-specific information use the Search field available in the various tabs. The search works on all column values (but not on column names).

10. For further investigation, run a live query using the Live Query Builder to fetch immediate results for the endpoint. For more information on how to run live queries, see Run a live query.

Export alert details

You can export details (to a CSV file) for the alerts in your environment for further analysis.

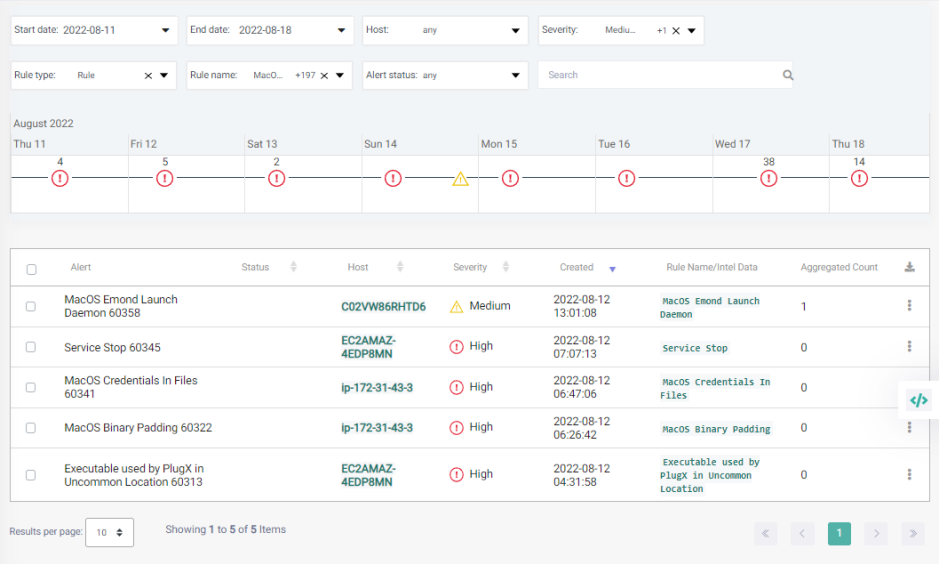
Perform these steps to export alert details.

1. Access the web interface for the server.
2. Click Alerts in the navigation pane.

   The Alerts page lists all managed endpoints.

3. Select values for the filters on the page to review corresponding alerts.

   Alerts matching the specified filters are displayed.



   Note: The alert timeline available only in the Enterprise Edition.

4. Click the Download icon .

   Details for all alerts are exported to a CSV file. Note that all the listed alerts are exported. So, the selected filters will determine the list of alerts that are exported.

Respond to alerts

After you review an alert and its details, you can take an appropriate action for the alert.

- Add notes
- Resolve alerts
- Reopen or unresolve an alert

Add notes

When using the Enterprise Edition, any user (with Administrator or Analyst role) can add notes when reviewing alerts. Notes allow you to include relevant diagnostic or forensic information for alerts. Once added, these notes are visible to all users.

Note: The ability to add notes in only available in the Enterprise Edition and is unavailable in the Community Edition.

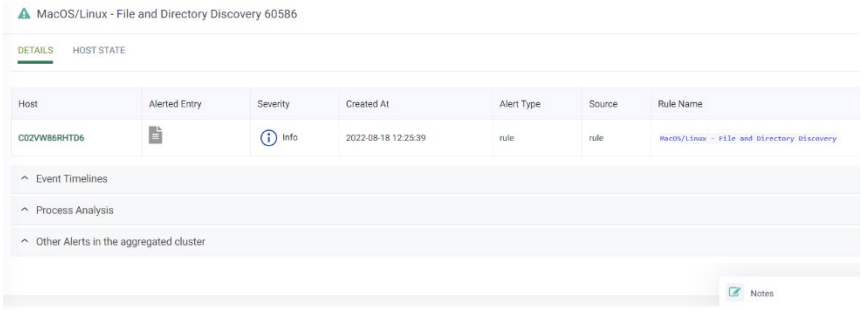
Perform these steps to add notes to an alert.

1. Access the web interface for the server.
2. Navigate to the Alerts page.

   By default, the Alerts page displays alert data for the last 7 days.

3. Select values from the Start date, End date, Host, Severity, Rule type, Rule name, and Alert status drop-down lists (on the top of the page) to filter and view relevant alerts.
4. Click the ellipsis icon for an alert and select Open alert.

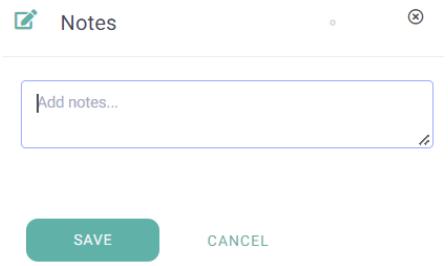
   A pop-up page displays alert details.



5. Click the note icon at the bottom right corner of the page.

   The Notes window is displayed.

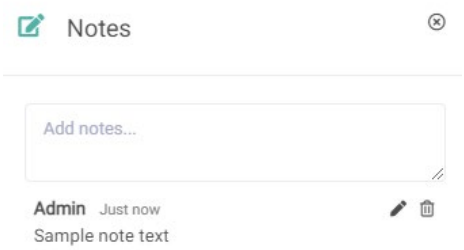
6. Type the note for the alert in the Add notes text field.



7. Click Save.

   The note is saved and displayed in the Notes window.

8. Optionally, edit or delete the note by clicking the Edit Note or Delete Note icon for the note.



9. Close the Notes window to return to the Alert Data page.

Resolve alerts

After you have reviewed an alert and taken needed actions, you can resolve the alert.

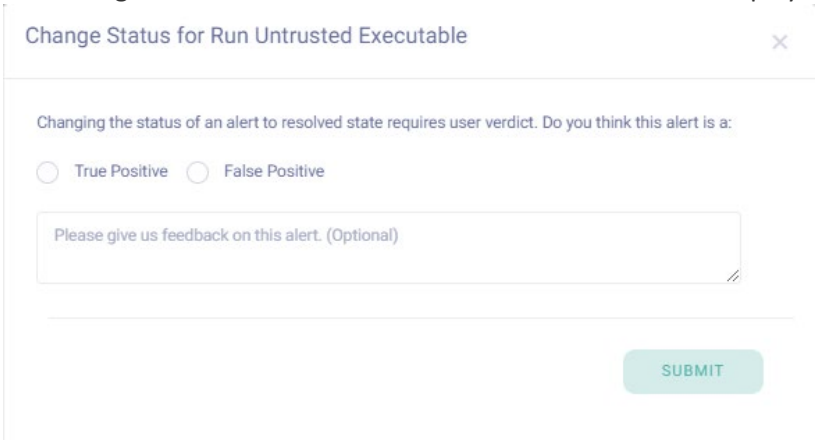
Perform these steps to resolve an alert.

1. Access the web interface for the server.
2. Navigate to the Alerts page.

   By default, the Alerts page displays alert data for the last 7 days.

3. Select values from the Start date, End date, Host, Severity, Rule type, Rule name, and Alert status drop-down lists (on the top of the page) to filter and view relevant alerts.
4. Click the ellipsis icon for an alert and select Resolve.

   The Change Status for Run Untrusted Executable window is displayed.



5. Provide a verdict for the alert.
6. Optionally, provide feedback for the alert.
7. Click Submit to return to the Alerts page.

   A success message box is displayed, and the alert is resolved.

Unresolve an alert

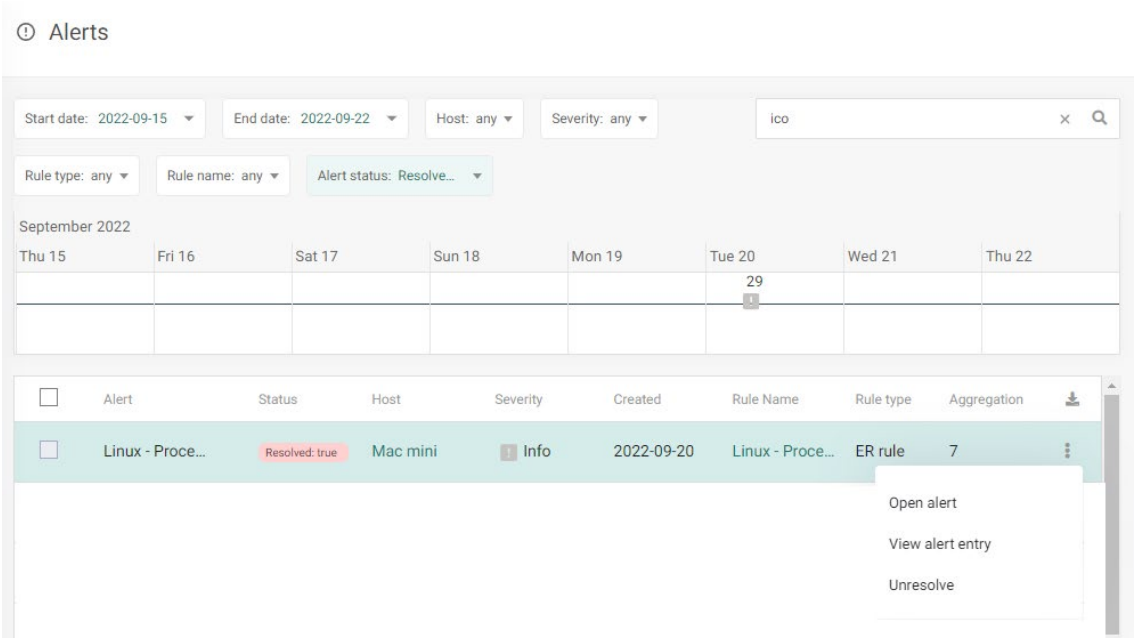
If you accidentally resolved an alert, you can unresolve the alert.

Perform these steps to unresolve an alert.

1. Access the web interface for the server.
2. Navigate to the Alerts page.

   By default, the Alerts page displays alert data for the last 7 days.

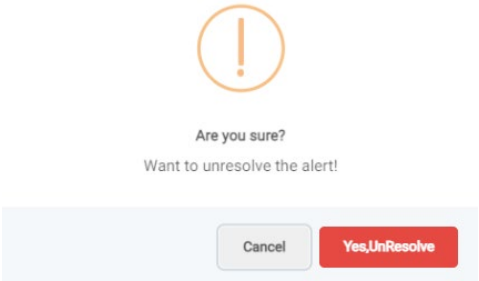
3. Select the Resolved values from Alert status drop-down list (on the top of the page) to view resolved alerts.



Note: The alert timeline is available only in the Enterprise Edition.

4. Click the ellipsis icon for a resolved alert and select Unresolve.

   A confirmation message box is displayed.



5. Click Yes, Unresolve.

   A success message box is displayed, and the alert is unresolved.

Define carves

File carving is a forensic technique that refers to extracting files from an endpoint. Using the EclecticIQ Endpoint Response framework, you can fetch one or more files from the managed endpoints to the server for investigation.

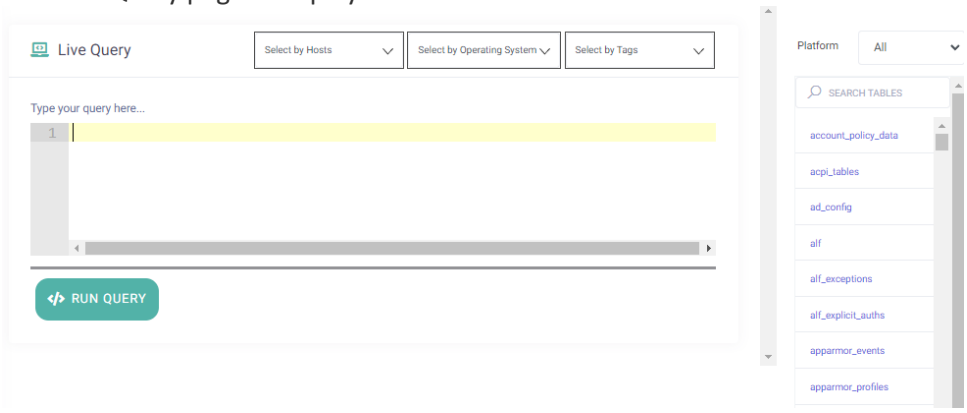
Note: No configuration is needed to use the Carves functionality. By default, the following parameters are included in the osquery.flags file.

- disable_carver=false
- carver_block_size=300000
- carver_start_endpoint=/start_uploads
- carver_continue_endpoint=/upload_blocks
- carver_disable_function=false

Perform these steps to acquire files.

1. Access the web interface for the server.
2. Navigate to Live Query.

   The Live Query page is displayed.



3. Specify the query to run in the Type your query here field.

To fetch a single file from an endpoint	Use this syntax to build your query.

	`select * from carves where path like '/file/path/%' and carve=1;` In the syntax, *</file/path/%>* represents the file path. You can use the % wildcard while specifying the path.
To fetch one or more files that meet the specified criteria	Use this syntax to build your query. `select carve(path) from file where directory like '/dir_path/%/Downloads/' and mode='0755' and type == 'regular';` In the syntax: • *</dir_path/%/Downloads/>* represents the directory path • mode represents the file permissions on UNIX • type indicates the file type. You can use other file properties, as needed, to fetch the files.

4. Specify the endpoints on which to run the query.
   - To run the query on an endpoint, choose the endpoint from the Select Hosts drop-down list.
   - To run the query on a group of endpoints, select a tag from the Select by Tags drop-down list.
   - To run the query on endpoints running a specific operating system, choose a value from the Select by Operating System drop-down list.
5. Click Run Query.
6. After the query is run, navigate to Carves.

   The Craves page lists the acquired files.
7. Check the status of the entry.
8. When completed, click the file name to download the retrieved files.

   The file is downloaded.

Searching for files and indicators

For investigative purposes, you can search all received endpoint data based on filters or specific indicators.

- Hunt for indicators
- Search endpoint data
- Search for files on endpoints

While hunt allows you to examine data based a single indicator type (with multiple possible values) at a time, you can use search to examine data based on a set of conditions.

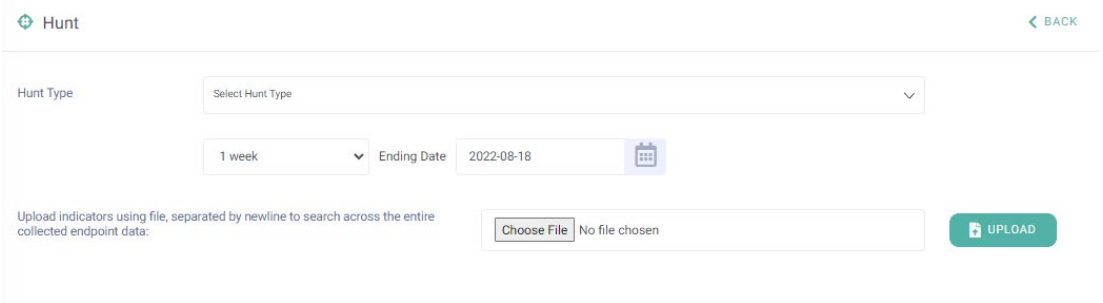
Hunt for indicators

Threat hunting is a technique that allows you to deep dive and search for possibly malicious files in your environment. These files may have evaded preliminary endpoint security tools to enter your network. The EclecticIQ Endpoint Response platform supports threat hunting and allows you to proactively search for any possible hidden threats in your environment.

Perform these steps to hunt in your environment.

1. Access the web interface for the server.
2. Navigate to Hunt.

   The Hunt page is displayed.



3. Specify the type of indicator to hunt for.

   The possible options are MD5, SHA256, domain name, and certificates.

4. Specify the data in which to search.

   c. Select the time window.

      You can search for the indicator in endpoint data across a day, week, or month.

   d. Select the end date.

      The selected date indicates the end of the day, week, or month in which to search endpoint data.

5. Specify the value to hunt for.

   e. Click Choose File.

      The Open dialog box is displayed.

   f. Select the file containing the indicators to search for.

      When specifying multiple indicators, ensure the values are separated by a new line.

6. Click Upload.

   After the hunt completes, the results are displayed. For each entry, host name, query name, and columns are displayed.

7. Review the entries and associated details.

Search endpoint data

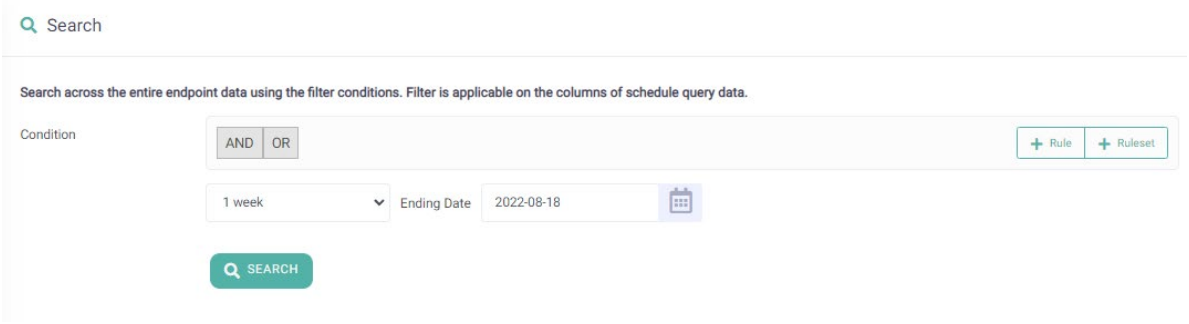
You can search for specific information across all received endpoint data by using conditions and filters. Using conditions will help you narrow down the fetched results.

Perform these steps to hunt in your environment.

1. Access the web interface for the server.

2. Navigate to Search.

   The Search page is displayed.



3. Select the condition: AND or OR.
4. Specify the type of indicator to search for.

   The possible values are:

   - md5
   - sha256
   - domain_name
   - ja3_md5
   - process_guid
   - parent_process_guid
   - target_path
   - target_name
   - process_name
   - remote_address

5. Select the operator for the indicator.

   The possible values are equals and contains.

6. Specify the value for the indicator.
7. If needed, add more rules and rulesets to specify the conditions and indicators.
8. Specify the data in which to search.

   g. Select the time window.

      You can search for the indicator in endpoint data across a day, week, or month.

   h. Select the end date.

      The selected date indicates the end of the day, week, or month in which to search endpoint data.

9. Click Search.

   After the search completes, the results are displayed. For each entry, host name, query name, and columns are displayed.

10. Review the entries and associated details.

Search for files on endpoints

Starting with the 4.0.0 release, you can search for specific files on managed endpoints. This feature is available on all supported Windows operating systems.

Before you can search for a file on endpoints, you must enable search capabilities by setting the custom_plgx_DiskIndexingEnabled option to true in the config. By default, this option is set to false. For more information, see Edit existing configs and Understand config parameters.

To perform the actual search for the file, you must run a live query. Here is an example of a live query you can run.

```
select * from win_disk_index where filename like '%test%'
```

For more information, see Run live queries.

Response

As an administrator, you can respond to threats and take actions when intrusions or attempted intrusions are detected.

Note: Response abilities are only available in the Enterprise Edition and are unavailable in the Community Edition.

Review these guidelines before you create any response action. To respond to threats, you can:

- Delete a file from an endpoint
- Terminate a process on an endpoint
- Push a firewall rule to contain or isolate an endpoint or limit its network access
- Block specific applications on an endpoint using a firewall rule
- Delete rules for an endpoint
- Execute commands using batch files and PowerShell scripts on endpoints running the Windows operating system or shell scripts on endpoints running the Linux and macOS operating systems
- Execute scripts on a specific using a live terminal and fetch immediate results on the UI
- Restart endpoints
- Define blocking rules

Before you begin

Consider the following guidelines before using response actions in your environment.

- Verify the response capabilities of the endpoint before initiating any response action. You can only send response actions to endpoints for which response capabilities are enabled. Perform these steps to verify Response Action status.

  i. Access the web interface for the server.
  j. Click Hosts in the navigation pane.

     The Active tab lists all endpoints.

  k. Click a row to review endpoint details.

     A pop-up page displays endpoint details.

  l. Review the Response action status on the Details tab.

     A green circle with a check mark (✅) indicates that response capabilities are enabled for the endpoint.
     A red circle with a cross (❌) indicates that response capabilities are disabled for the endpoint.

- When running scripts:
  - Because no human intervention is feasible on endpoints, execute scripts that **DO NOT** require user intervention. In effect, interactive mode scripts are not supported.
  - Prior to running a script, thoroughly test the script on a standalone system to ensure it works as designed.
  - If the script fails or does not return any output, DO NOT send another one until you diagnose and identify the cause of failure.
- Response actions are available on Windows, Linux, and macOS endpoints.

- You can send response actions to offline endpoints (if response capabilities are enabled for the endpoint).
- While being able to respond to threats is an effective feature, you must exercise caution if responding to an incident on scale. If not used properly and with care this feature may cause disruptions. EclecticIQ recommends that you must be judicious and prudent when running a script for a multitude of endpoints in your environment.
- If you intend to extensively use response actions to execute PowerShell scripts, we recommend that you edit to the config file (for Windows) to set the values of the custom_plgx_MemoryLimitHigh parameter to 200 and custom_plgx_MemoryLimitLow parameter to 100. For more information, see Understand config parameters.

Delete files

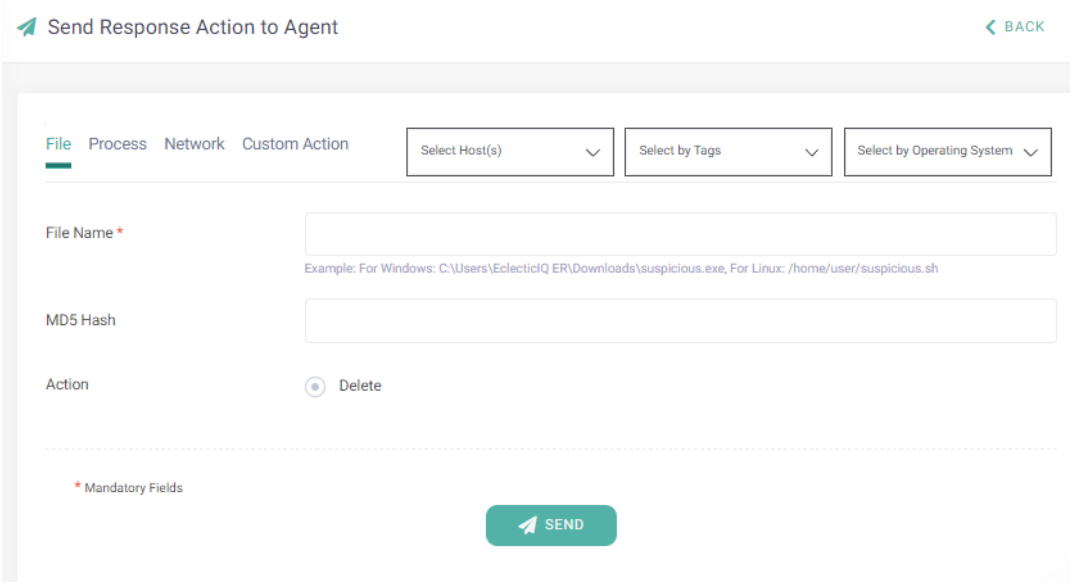
Perform these steps to delete a file.

1. Access the web interface for the server.
2. Navigate to Response Action.

   The Response Action page is displayed.

3. Click Create New Response Action.

   The Send Response Action to Agent page is displayed.



4. On the File tab, enter the complete file path in the File field.
5. Optionally, specify the MD5 hash value for the file.
6. Verify Delete is selected.
7. Specify the endpoints on which to send the response action.

   - To send the response action to an endpoint, choose the endpoint from the Select Hosts drop-down list.
   - To send the response action to a group of endpoints, select a tag from the Select by Tags drop-down list.
   - To send the response action to endpoints running a specific operating system, choose a value from the Select by Operating System drop-down list.

8. Click Send.

Terminate processes

Perform these steps to terminate a process.

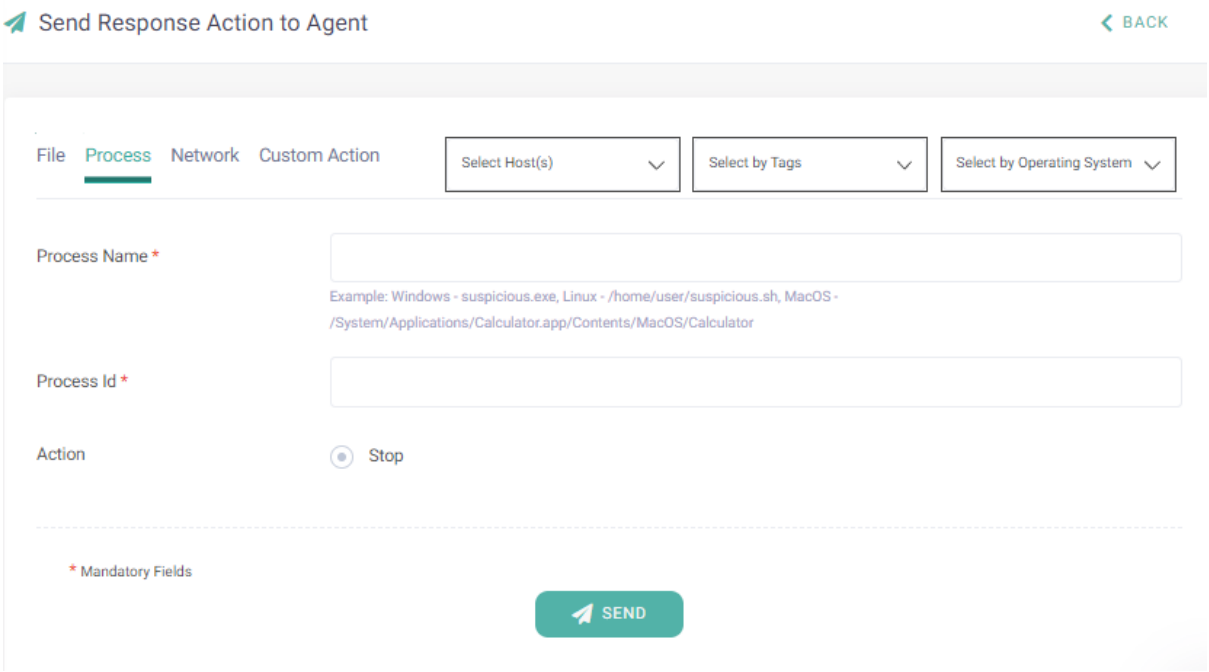
1. Access the web interface for the server.
2. Navigate to Response Action.

   The Response Action page is displayed.

3. Click Create New Response Action.

   The Send Response Action to Agent page is displayed.

4. Switch to the Process tab.



5. Enter the process name or path in the Process Name field.
6. Specify the process ID value for the process.
7. Verify Stop is selected.
8. Specify the endpoints on which to send the response action.

   - To send the response action to an endpoint, choose the endpoint from the Select Hosts drop-down list.
   - To send the response action to a group of endpoints, select a tag from the Select by Tags drop-down list.
   - To send the response action to endpoints running a specific operating system, choose a value from the Select by Operating System drop-down list.

9. Click Send.

Isolate endpoints or specific applications

You can isolate endpoints or specific applications only on endpoints that are running Windows operating systems.

Note: To prevent an agent from communicating with the server, create an Isolate response action, select Any for all options, and set Direction to OUT.

Perform these steps to isolate an endpoint.

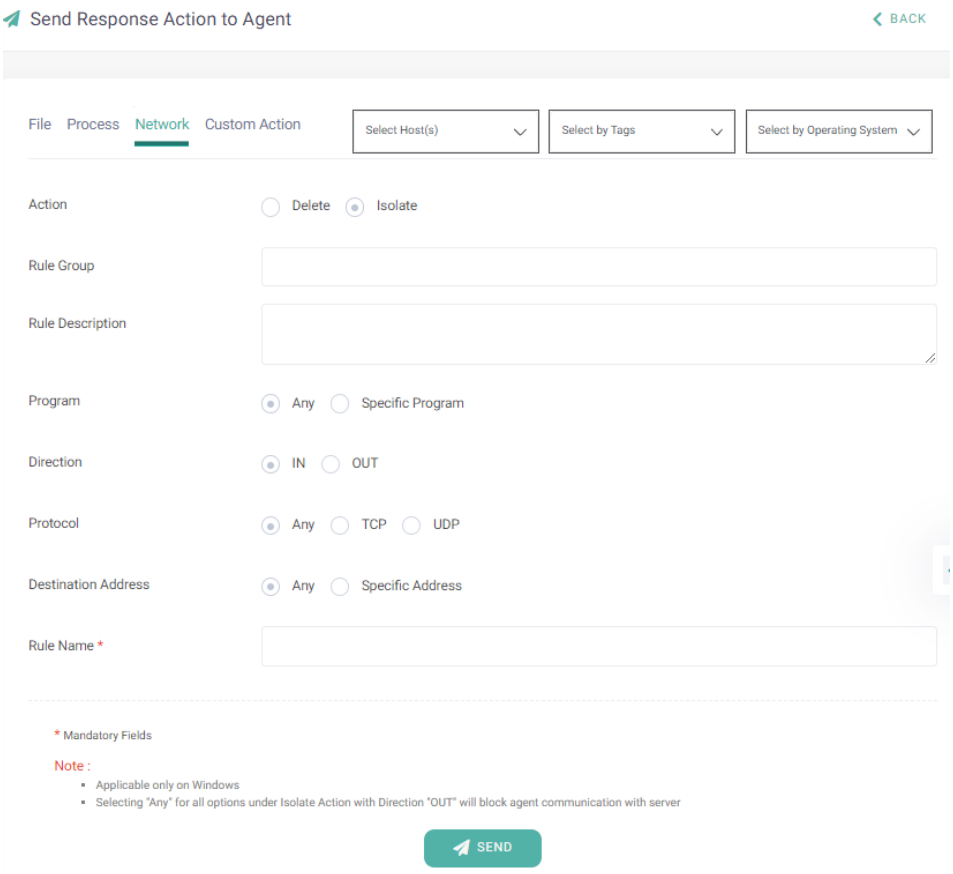
1. Access the web interface for the server.
2. Navigate to Response Action.

   The Response Action page is displayed.

3. Click Create New Response Action.

   The Send Response Action to Agent page is displayed.

4. Switch to the Network tab.
5. Select the Isolate option.



6. Specify the name of the network rule group.
7. Provide a description for the network rule.
8. Specify the program name to isolate.

   You can choose Any or Specific Program. When isolating a specific program, enter the absolute or relative path to the application.

9. Specify whether the rule is an inbound or outbound rule.
10. Specify the request protocol type to use.

You can choose Any, TCP, or UDP. For TCP and UDP, you must also provide values for the local and remote ports to use in the rule. You can choose to use any port, a specific port value, or a range of values (between 1 and 65535).

11. Specifies the destination address to use in the network rule to isolate.

    You can choose Any or Specific Address. For a specific address, you can enter a range or a value.

12. Specify the network rule name to create or update.
13. Specify the endpoints on which to send the response action.

- To send the response action to an endpoint, choose the endpoint from the Select Hosts drop-down list.
- To send the response action to a group of endpoints, select a tag from the Select by Tags drop-down list.
- To send the response action to endpoints running a specific operating system, choose a value from the Select by Operating System drop-down list.

14. Click Send.

Delete rules

You can delete rules (Windows firewall) on endpoints that are running Windows operating system. Perform these steps to delete a rule.

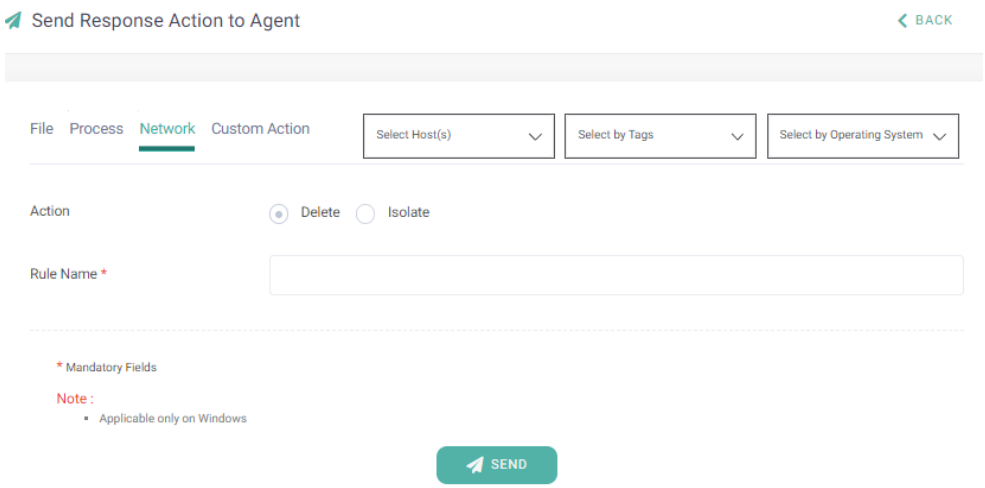
1. Access the web interface for the server.
2. Navigate to Response Action.

   The Response Action page is displayed.

3. Click Create New Response Action.

   The Send Response Action to Agent page is displayed.

4. Switch to the Network tab.
5. Select the Delete option.



6. Specify the name of the rule to delete.

7. Specify the endpoints on which to send the response action.
   - To send the response action to an endpoint, choose the endpoint from the Select Hosts drop-down list.
   - To send the response action to a group of endpoints, select a tag from the Select by Tags drop-down list.
   - To send the response action to endpoints running a specific operating system, choose a value from the Select by Operating System drop-down list.
8. Click Send.

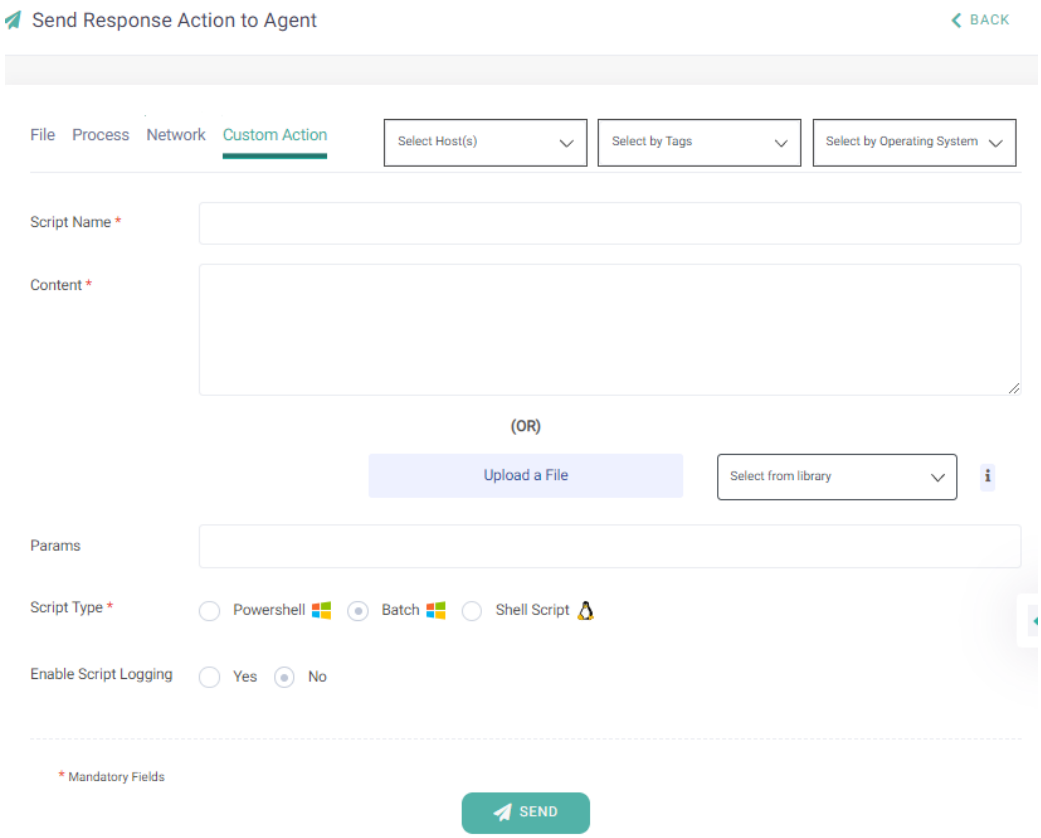
Execute custom scripts

Perform these steps to execute a custom script.

1. Access the web interface for the server.
2. Navigate to Response Action.

   The Response Action page is displayed.
3. Click Create New Response Action.

   The Send Response Action to Agent page is displayed.
4. Switch to the Custom Action tab.



5. Enter the script name.

6. Specify the content.

   - Enter the content for the script.
   - Click the Upload a File button to upload the script file.
   - Select a predefined script to run.

   When running a seeded script, update the relevant information in script based on your needs.

7. Optionally, specify any parameters for the script file to run.
8. Select the script type.

   You can choose to run .bat files and PowerShell scripts (on endpoint running the Windows operating system) or Shell scripts (on endpoints running Linux and macOS).

9. Specify whether to save the script file to the EclecticIQ Endpoint Response server database.
10. Specify the endpoints on which to send the response action.

    - To send the response action to an endpoint, choose the endpoint from the Select Hosts drop-down list.
    - To send the response action to a group of endpoints, select a tag from the Select by Tags drop-down list.
    - To send the response action to endpoints running a specific operating system, choose a value from the Select by Operating System drop-down list.

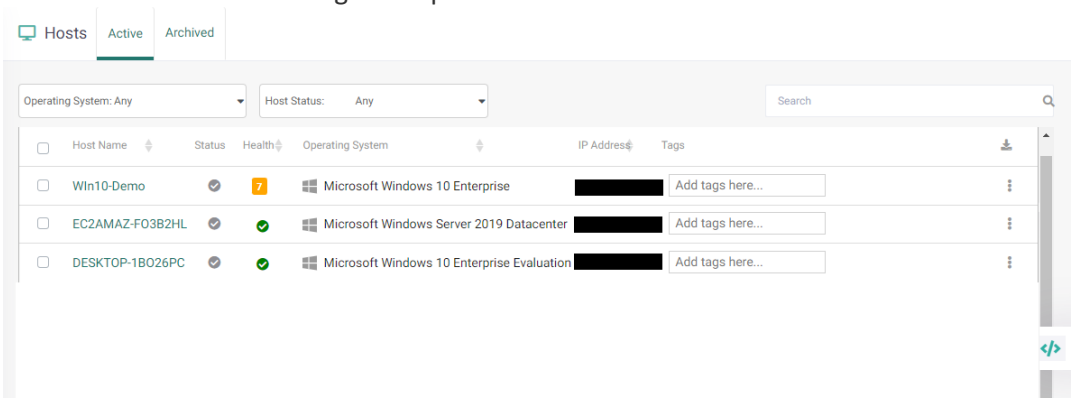
11. Click Send.

Execute scripts using a live terminal

Perform these steps to execute a script on a specific endpoint using a live terminal. The script is executed right away and corresponding results are displayed on the UI.

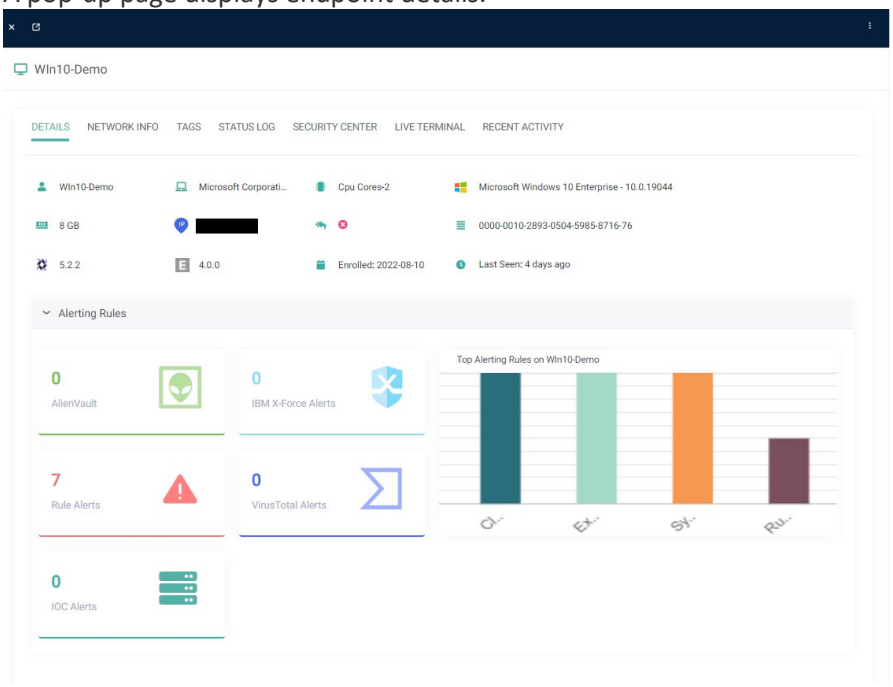
1. Access the web interface for the server.
2. Click Hosts in the navigation pane.

   The Active tab lists all managed endpoints.



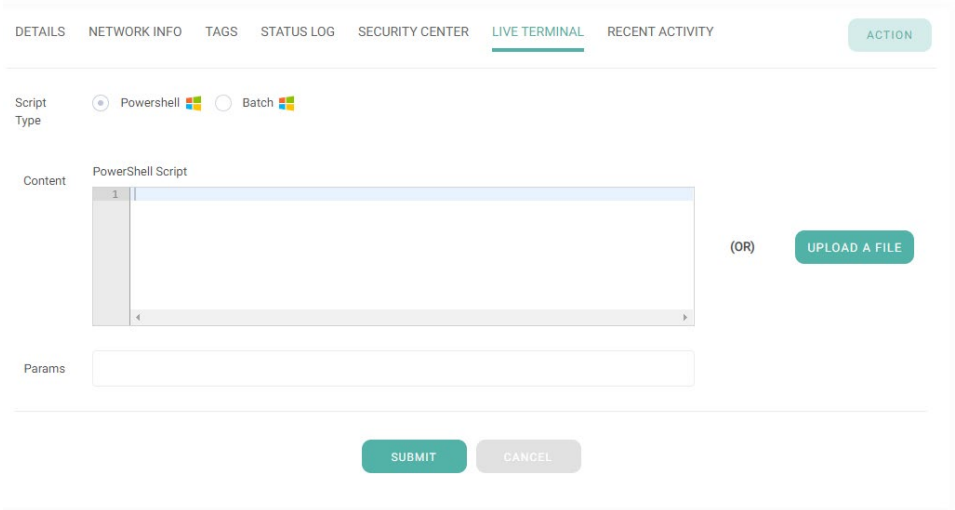
3. Click a row to review endpoint details.

   A pop-up page displays endpoint details.



4. Switch to the Live Terminal tab.

   The options available on the tab vary based on the operating system running on the endpoint. You can execute PowerShell and batch files on Windows endpoints and Shell scripts on Linux and macOS endpoints.



5. Specify the content.

   - Enter the content for the script.
   - Click the Upload a File button to upload the script file.

6. Click Submit.

   The script is executed on the endpoint and its output is displayed on the UI.

7. Review the script output.

Restart endpoints

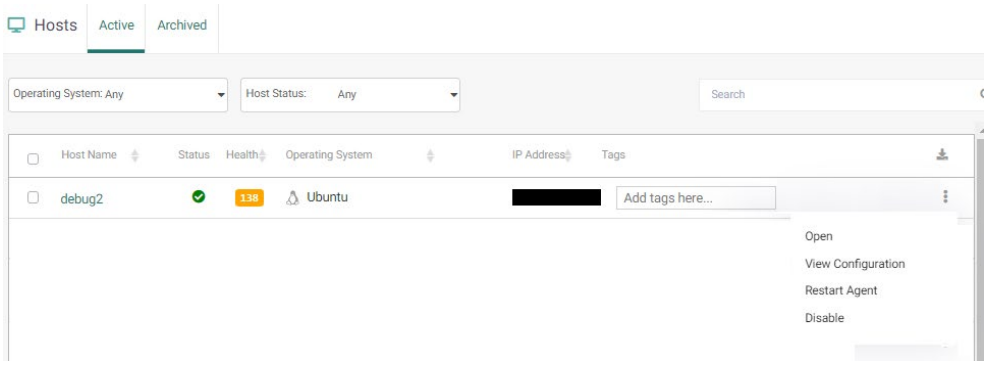
To troubleshoot and investigate issues, you can restart an endpoint, if needed. From the EclecticIQ Endpoint Response server, you can only restart online endpoints.

Perform these steps to restart an endpoint.

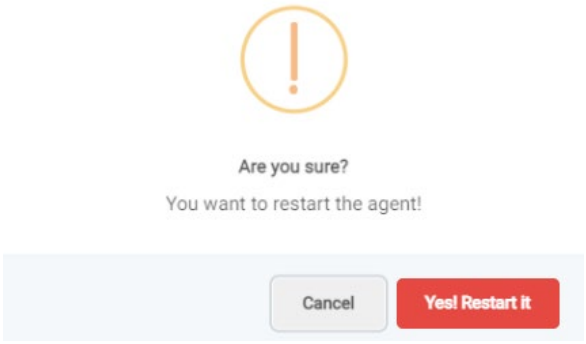
1. Access the web interface for the server.
2. Click Hosts in the navigation pane.

   The Active tab lists all managed endpoints.

3. For an endpoint, click the ellipsis icon and select Restart Agent.



   A confirmation dialog is displayed.



4. Click Yes, Restart it to confirm.

   A message box is displayed, and the agent is restarted.

Define blocking rules

By default, EclecticIQ Endpoint Response includes seeded blocking rules for self-protection for the Windows operating system. If needed, you can define custom blocking rules (on Windows only) to prevent malicious or unauthorized operations and processes and allow authorized file and process operations. You can define blocking rules for the following:

- File operations
- Registry operations
- Process launch
- Process termination

Exercise caution and judgment when choosing possible candidates (files or processes) for blocking rules. We recommend that you perform extensive testing of any defined rules before adding to your

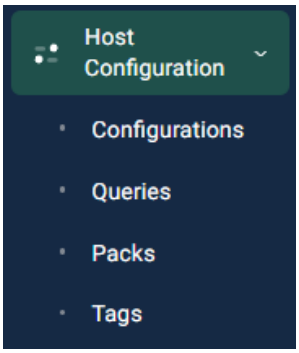
enterprise. If not defined prudently, blocking rules can cause extensive disruptions in your environment.

Additionally, when defining a blocking rule, ensure you create a targeted or specific rule. Defining vague or wide rules may result in inappropriate system behavior.

Configure blocking rules

To configure blocking rules you must set the custom_plgx_EnableBlocking parameter in the config to true.

1. Navigate to Host Configuration > Configurations.



   The Configurations page is displayed.

2. Ensure the Windows platform is selected.
3. Select the config to edit (by clicking the appropriate tab).
4. Scroll to the Additional Config and Filters section.
5. Under options, add the custom_plgx_EnableBlocking parameter.
6. Set the value of the parameter to true.

```
"options" :
{
   "custom_plgx_EnableBlocking": "true"
},
```

   Note that the options and values are both case sensitive. For more information on config parameters, see Understand config parameters.

7. Click Update.

Syntax for blocking rules

Use the JSON syntax to define blocking rules.

```
"plgx_event_control": {
   "section_name": {
      "RuleGroup1": {
        "rule type": {
          "subsection1": {
            "value": [
```

```
            "*\\path1\\*"
          ]
        },
        "subsection2": {
          "value": [
            "*\\path1\\abc.exe",
            "*\\path1\\xyz.exe"
          ]
        }
      },
      "rule type": {
        "subsection": {
          "values": [
            "*\\path1\\*"
          ]
        }
      }
    },
}
```

In the syntax:

- **section name** - Represents the name of the section (based on the EclecticIQ Endpoint Response table on the agent) under which to define the blocking rules. You must include the section names in double quotes (“”). For more information on valid section names, see Config sections for blocking rules.
- **RuleGroup1** - Denotes the rule group containers in which to include the blocking rules. You can define multiple rule groups. Each rule group can have a combination of allow and block subsections. Each rule group should be named RuleGroupn where n is a number that indicates the rule group’s position in the array. All rules defined across multiple rule groups within a section are applied in conjunction. You must include the rule group names in double quotes (“”).
- **allow** and **block** - Specify the type of rule. While the **block** section lists the blocking rules, the **allow** section lists any exceptions to the defined blocking rules. In other words, rules defined in the allow section are exceptions to the rules defined in corresponding block section within a rule group. You must include the allow and block keywords in double quotes (“”). Each allow and block section can include multiple conditions.
  If there are multiple allow or block rules, all rules within a allow or block sub group are applied in conjunction (a logical AND condition) during matching. If any rule group decides to block an operation, that rule group takes precedence, and the operation is blocked regardless of the outcome or decision of other rule groups. If none of the rule groups decide to block the operation, it is allowed.
- **subsection** - Indicates the name of the subsection (based on the column in the EclecticIQ Endpoint Response table on the agent) in the section under which to define block rules. You must include the subsection names in double quotes (“”). For more information on valid subsection names (under each section), see Config sections for blocking rules.
- **value** - Lists the values to match for the specified rule or exception. Each entry represents a value that you want to block or allow (based on whether it is included in the block or allow section). You must include the values in double quotes (“”). Specified values are case insensitive. You can also use wild cards in the values where * represents one or more characters and ? represents a single character.

Config sections for blocking rules

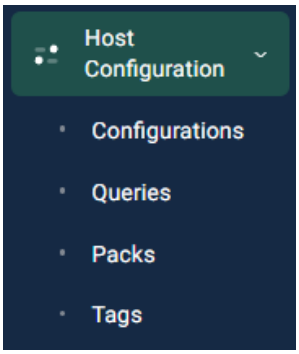
In the config, you can define blocking rules under only specific sections (based on the EclecticIQ Endpoint Response tables and columns).

Section	***Subsection***	***Description***
win_proc_events	process, cmdline, parent_process	Section to define blocking rules for process operations, such as launch and termination. For process launch operations, you can define blocking rules using: • Process name • Parent process name • Command line (with which process was launched) For process termination operations, you can define blocking rules using the process name.
win_registry_events	key_name, process	Section to define blocking rules for registry operations.
win_file_events	process, target_path	Section to define blocking rules for file operations.

Add blocking rules

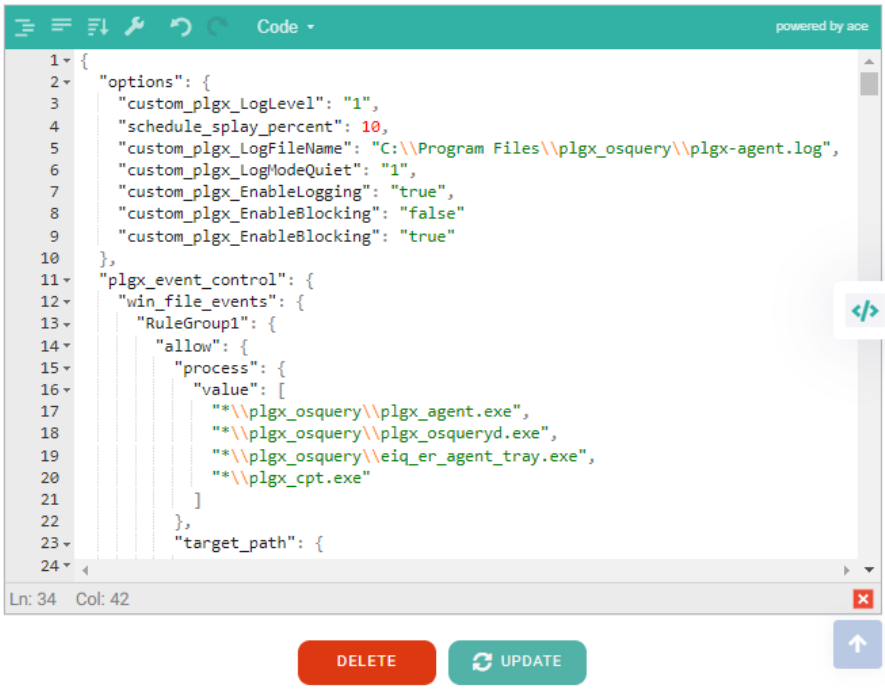
Perform these steps to edit an existing config to add a new blocking rule.

1. Access the web interface for the server.
2. Navigate to Host Configuration > Configurations.



   The Configurations page is displayed.

3. Ensure the Windows platform is selected.
4. Select the config to edit (by clicking the appropriate tab).
5. Scroll to the Additional Config and Filters section.
6. Navigate to the plgx_event_control tag and add the new blocking rules.



Note: In the graphic, the blocking rules specified in the plgx_event_control section are specific to the Enterprise Edition. Note that the rules will vary for the Community Edition.

Ensure you follow the syntax for blocking rules and place all rules within the plgx_event_control tag. Also, make sure you add rules within relevant sections in the config. For more information, see Config sections for blocking rules.

7. Click Update.

   A confirmation dialog is displayed.

8. Click Yes, Update.

   A success message box is displayed, and the config is updated.

9. Click OK.

Appendix A – EclecticIQ Endpoint Response tables

Windows tables

EclecticIQ Endpoint Response includes the following tables for Linux.

- win_file_events
- win_process_events
- win_remote_thread_events
- win_process_open_events
- win_removable_media_events
- win_image_load_events
- win_image_load_process_map
- win_http_events
- win_ssl_events
- win_socket_events
- win_dns_events
- win_dns_response_events
- win_registry_events
- win_yara_events
- win_logger_events
- win_file_timestomp_events
- win_pefile_events
- win_named_pipe_events
- win_network_stats
- win_process_perf
- win_msr
- win_services
- win_epp_table
- win_event_log_channels
- win_event_log_data
- win_yara
- win_process_handles
- win_hash
- win_suspicious_process_scan
- win_suspicious_process_dump
- win_programs
- win_mem_perf
- win_startup_items
- windows_events_table_optimized
- win_disk_index

win_file_events

Stores Windows file activity events.

Column	***Data type***
action	TEXT

eid	TEXT
target_path	TEXT
md5	TEXT
sha256	TEXT
hashed	BIGINT
uid	TEXT
time	BIGINT
utc_time	TEXT
pe_file	TEXT
pid	BIGINT
process_guid	TEXT
process_name	TEXT
amsi_is_malware	TEXT
byte_stream	TEXT
eventid	INTEGER

win_process_events

Stores Windows process creation and termination events.

Column	***Data type***
action	TEXT
eid	TEXT
pid	BIGINT
process_guid	TEXT
path	TEXT
cmdline	TEXT
parent_pid	BIGINT
parent_process_guid	TEXT
parent_path	TEXT
owner_uid	TEXT
time	BIGINT
utc_time	TEXT
eventid	INTEGER
sha256 (available only in the Community Edition)	TEXT

win_remote_thread_events

Stores Windows remote thread events.

Column	***Data type***
action	TEXT
eid	TEXT
src_pid	BIGINT
src_process_guid	TEXT
target_pid	BIGINT
target_process_guid	TEXT
src_path	TEXT
target_path	TEXT
function_name	TEXT

module_name	TEXT
owner_uid	TEXT
time	BIGINT
utc_time	TEXT
eventid	INTEGER

win_process_open_events

Stores Windows process open events.

Column	***Data type***
action	TEXT
eid	TEXT
src_pid	BIGINT
src_process_guid	TEXT
target_pid	BIGINT
target_process_guid	TEXT
src_path	TEXT
target_path	TEXT
granted_access	TEXT
granted_access_value	TEXT
owner_uid	TEXT
time	BIGINT
utc_time	TEXT
eventid	INTEGER

win_removable_media_events

Stores Windows removable media events.

Column	***Data type***
action	TEXT
eid	TEXT
uid	TEXT
pid	BIGINT
time	BIGINT
utc_time	TEXT
eventid	INTEGER

win_image_load_events

Stores Windows image load events.

Column	***Data type***
action	TEXT
eid	TEXT
pid	BIGINT
process_name	TEXT
process_guid	TEXT
md5	TEXT
uid	TEXT
image_path	TEXT
sign_info	TEXT

trust_info	TEXT
num_of_certs	BIGINT
cert_type	TEXT
version	TEXT
pubkey	TEXT
pubkey_length	TEXT
pubkey_signhash_algo	TEXT
issuer_name	TEXT
subject_name	TEXT
serial_number	TEXT
signature_algo	TEXT
subject_dn	TEXT
issuer_dn	TEXT
time	BIGINT
utc_time	TEXT
eventid	INTEGER

win_image_load_process_map

Stores Windows process map events.

Column	***Data type***
pid	BIGINT
process_guid	TEXT
process_name	TEXT
image_path	TEXT
image_size	TEXT
md5	TEXT
image_memory_mode	TEXT
image_base	TEXT
time	BIGINT
utc_time	TEXT
eventid	INTEGER

win_http_events

Stores Windows HTTP events.

Column	***Data type***
action	TEXT
event_type	TEXT
eid	TEXT
pid	BIGINT
process_guid	TEXT
process_name	TEXT
url	TEXT
remote_address	TEXT
remote_port	INTEGER
time	BIGINT
utc_time	TEXT
eventid	INTEGER

win_ssl_events

Stores SSL certificate events.

Column	***Data type***
event_type	TEXT
action	TEXT
eid	TEXT
subject_name	TEXT
issuer_name	TEXT
serial_number	TEXT
dns_names	TEXT
ja3_md5	TEXT
ja3s_md5	TEXT
pid	BIGINT
process_guid	TEXT
process_name	TEXT
remote_address	TEXT
remote_port	INTEGER
time	BIGINT
utc_time	TEXT
eventid	INTEGER

win_socket_events

Stores Windows socket events.

Column	***Data type***
event_type	TEXT
eid	TEXT
action	TEXT
pid	BIGINT
process_guid	TEXT
process_name	TEXT
family	TEXT
protocol	INTEGER
local_address	TEXT
remote_address	TEXT
local_port	INTEGER
remote_port	INTEGER
time	BIGINT
utc_time	TEXT
eventid	INTEGER

win_dns_events

Stores DNS events.

Column	***Data type***
action	TEXT
event_type	TEXT

eid	TEXT
domain_name	TEXT
request_type	INTEGER
request_class	INTEGER
pid	BIGINT
remote_address	TEXT
remote_port	INTEGER
time	BIGINT
utc_time	TEXT
eventid	INTEGER

win_dns_response_events

Stores DNS response events.

Column	***Data type***
action	TEXT
event_type	TEXT
eid	TEXT
domain_name	TEXT
request_type	INTEGER
request_class	INTEGER
resolved_ip	TEXT
pid	BIGINT
remote_address	TEXT
remote_port	INTEGER
time	BIGINT
utc_time	TEXT
eventid	INTEGER

win_registry_events

Stores Windows registry events.

Column	***Data type***
action	TEXT
eid	TEXT
pid	BIGINT
process_guid	TEXT
process_name	TEXT
target_name	TEXT
target_new_name	TEXT
value_type	TEXT
value_data	TEXT
owner_uid	TEXT
time	BIGINT
utc_time	TEXT
eventid	INTEGER

win_yara_events

Stores Windows YARA events.

Column	Data type
eid	TEXT
target_path	TEXT
category	TEXT
action	TEXT
matches	TEXT
md5	TEXT
time	BIGINT
utc_time	TEXT
count	INTEGER
eventid	INTEGER

win_logger_events

Stores agent logger events table.

Column	Data type
logger_name	TEXT
logger_watch_file	TEXT
log_entry	TEXT
eventid	INTEGER

win_file_timestomp_events

Stores Windows file timestomp events.

Column	Data type
action	TEXT
eid	TEXT
target_path	TEXT
old_timestamp	TEXT
new_timestamp	TEXT
md5	TEXT
hashed	BIGINT
uid	TEXT
time	BIGINT
utc_time	TEXT
pe_file	TEXT
pid	BIGINT
process_guid	TEXT
process_name	TEXT
eventid	INTEGER

win_pefile_events

Stores Windows PE file activity events.

Column	Data type
action	TEXT
eid	TEXT
target_path	TEXT
md5	INTEGER
hashed	BIGINT

uid	TEXT
pid	BIGINT
process_guid	TEXT
process_name	TEXT
time	BIGINT
utc_time	TEXT
eventid	INTEGER

win_named_pipe_events

Stores Windows named pipe events.

Column	***Data type***
action	TEXT
eid	TEXT
target_path	TEXT
uid	TEXT
time	BIGINT
utc_time	TEXT
pid	BIGINT
process_guid	TEXT
process_name	TEXT
eventid	INTEGER

win_network_stats

Stores network statistics values.

Column	***Data type***
process_id	BIGINT
tcp_connection_state	TEXT
remote_ip_address	TEXT
remote_port	BIGINT
local_ip_address	TEXT
local_port	BIGINT
incoming_bytes	BIGINT
outgoing_bytes	BIGINT

win_process_perf

Stores Windows process resource statistics.

Column	***Data type***
name	TEXT
pid	INTEGER
user_time	TEXT
privileged_time	TEXT
processor_time	TEXT
thread_count	INTEGER
working_set	TEXT
creating_process_id	TEXT
elapsed_time	TEXT
handle_count	INTEGER

io_data_bytes_per_sec	TEXT
io_read_bytes_per_sec	TEXT
io_read_ops_per_sec	TEXT
io_write_bytes_per_sec	TEXT
io_write_ops_per_sec	TEXT
non_paged_pool_bytes	TEXT
page_pool_bytes_peak	TEXT
priority_base	TEXT
private_bytes	TEXT
working_set_peak	TEXT

win_msr

Stores MSR register values.

Column	***Data type***
turbo_disabled	BIGINT
turbo_ratio_limt	BIGINT
platform_info	BIGINT
perf_status	BIGINT
perf_ctl	BIGINT
feature_control	BIGINT
rapl_power_limit	BIGINT
rapl_energy_status	BIGINT
rapl_power_units	BIGINT

win_services

Stores Windows services information.

Column	***Data type***
name	TEXT
service_type	TEXT
display_name	TEXT
status	TEXT
pid	INTEGER
start_type	TEXT
win32_exit_code	INTEGER
service_exit_code	INTEGER
path	TEXT
module_path	TEXT
description	TEXT
user_account	TEXT

win_epp_table

Stores Windows endpoint protection details.

Column	***Data type***
product_type	TEXT
product_name	TEXT
product_state	TEXT
product_signatures	TEXT

win_event_log_channels

Stores Windows event log channels information.

Column	***Data type***
source	TEXT

win_event_log_data

Stores Windows event log data.

Column	***Data type***
time	BIGINT
datetime	TEXT
source	TEXT
provider_name	TEXT
provider_guid	TEXT
eventid	INTEGER
task	INTEGER
level	INTEGER
keywords	BIGINT
data	TEXT
eid	TEXT

win_yara

Stores information for Windows on-demand YARA scans.

Column	***Data type***
target_path	TEXT
matches	TEXT
count	INTEGER
sig_group	TEXT
sigfile	TEXT

win_process_handles

Stores details for open handles in processes.

Column	***Data type***
pid	BIGINT
process_guid	TEXT
handle_type	TEXT
object_name	TEXT
access_mask	BIGINT

win_hash

Stores Windows hash information.

Column	***Data type***
path	TEXT
path_ex	TEXT
md5	TEXT
sha1	TEXT
sha256	TEXT

win_suspicious_process_scan

Stores information for suspicious processes.

Column	***Data type***
pid	BIGINT
process_name	TEXT
modules_scanned	BIGINT
modules_suspicious	BIGINT
modules_replaced	BIGINT
modules_detached	BIGINT
modules_hooked	BIGINT
modules_implanted	BIGINT
modules_skipped	BIGINT
modules_errors	BIGINT

win_suspicious_process_dump

Stores dumps for suspicious processes.

Column	***Data type***
pid	BIGINT
process_name	TEXT
process_dumps_location	TEXT

win_programs

Stores information for Windows programs.

Column	***Data type***
name	TEXT
version	TEXT
install_location	TEXT
install_source	TEXT
language	TEXT
publisher	TEXT
uninstall_string	TEXT
install_date	TEXT
identifying_number	TEXT

win_mem_perf

Stores system memory statistics.

Column	***Data type***
physical_memory_load	BIGINT
total_physical	BIGINT
available_physical	BIGINT
total_pagefile	BIGINT
available_pagefile	BIGINT
total_virtual	BIGINT
available_virtual	BIGINT
available_extended_memory	BIGINT

win_startup_items

Stores start-up items information.

Column	***Data type***
name	TEXT
path	TEXT
args	TEXT
type	TEXT
source	TEXT
status	TEXT
username	TEXT

windows_events_table_optimized

Stores Windows agent real-time events information. This table is a combination of multiple EclecticIQ Endpoint Response tables.

Column	***Data type***
data	TEXT

win_disk_index

Stores Windows disk index details.

Column	***Data type***
filename	TEXT
path	TEXT
flags	UNSIGNED_BIGINT
attribs	UNSIGNED_BIGINT

Linux tables

EclecticIQ Endpoint Response (Enterprise Edition) includes the following tables for Linux.

- bpf_process_table
- bpf_socket_table

bpf_process_table

Stores Linux container bpf process events.

Column	***Data type***
pid	BIGINT
parent	BIGINT
uid	BIGINT
gid	BIGINT
cid	INTEGER
syscall	TEXT
path	TEXT
cwd	TEXT
cmdline	TEXT
time	BIGINT
eid	INTEGER
container_id	TEXT

bpf_socket_table

Stores Linux container bpf socket events.

Column	***Data type***
pid	BIGINT
cid	INTEGER
path	TEXT
fd	TEXT
family	INTEGER
protocol	INTEGER
local_address	TEXT
remote_address	TEXT
local_port	INTEGER
remote_port	INTEGER
time	BIGINT
eid	INTEGER
container_id	TEXT

Appendix B – Event list

Here is a list of events for the EclecticIQ Endpoint Response server.

Event	***Associated actions***
WIN_FILE_EVENTS	FILE_CREATE
	FILE_DELETE
	FILE_WRITE
	FILE_RENAME
	FILE_DELETE_BY_DISP
WIN_PROCESS_EVENTS	PROC_CREATE
	PROC_TERMINATE
WIN_REMOTE_THREAD_EVENTS	REMOTE_THREAD_CREATE
WIN_PROCESS OPEN_EVENTS	PROC_OPEN
WIN_REMOVABLE_MEDIA_EVENTS	REMOVABLE_MEDIA_USB_MASS_STORAGE_DEVICE _ATTACHED
	REMOVABLE_MEDIA_CDROM_INSERTED
WIN_IMAGE_LOAD_EVENTS	IMAGE_LOAD_IN_MEMORY
WIN_HTTP_EVENTS	HTTP_REQUEST
WIN_SSL_EVENTS	TLS_CERT_RECEIVED
	SNI_EXTENSION (with shallow SSL)
WIN_SOCKET_EVENTS	SOCKET_CONNECT
	SOCKET_LISTEN
	SOCKET_ACCEPT
WIN_DNS_EVENTS	DNS_LOOKUP
WIN_DNS_RESPONSE_EVENTS	DNS_RESPONSE
WIN_REGISTRY_EVENTS	REG_CREATE
	REG_DELETE
	REG_RENAME
	REG_SETVALUE
WIN_YARA_EVENTS	PROC_CREATE
	FILE_WRITE
WIN_FILE_TIMESTOMP_EVENTS	FILE_TIMESTOMPED
WIN_PEFILE_EVENTS	FILE_CREATE
	FILE_RENAME
	FILE_DELETE
	FILE_WRITE
	FILE_DELETE_BY_DISP
WIN_NAMED_PIPE_EVENTS	NAMED_PIPE_CREATE
	NAMED_PIPE_DISCONNECT
WIN_EPP_TABLE	Not applicable
WIN_MSR	Not applicable
WIN_PROCESS_HANDLES	Not applicable
WIN_IMAGE_LOAD_PROCESS_MAP	Not applicable
WIN_LOGGER_EVENTS	Not applicable
WIN_DEFENDER_EVENTS	Not applicable
WIN_SUSPICIOUS_PROCESS_SCAN	Not applicable
WIN_SUSPICIOUS_PROCESS_DUMP	Not applicable
WIN_STARTUP_ITEMS	Not applicable
WIN_SERVICES	Not applicable
WIN_DISK_INDEX	Not applicable
WIN_EVENT_LOG_CHANNELS	Not applicable
WIN_EVENT_LOG_DATA	Not applicable
WIN_HASH	Not applicable
WIN_MEM_PERF	Not applicable

WIN_NETWORK_STATS	Not applicable
WIN_PROCESS_PERF	Not applicable
WIN_PROGRAMS	Not applicable
WINBASEOBJ	Not applicable
WINDOWS_CRASHES	Not applicable
WINDOWS_EVENTS	Not applicable
WINDOWS_OPTIONAL_FEATURES	Not applicable
WINDOWS_SECURITY_CENTER	Not applicable
WINDOWS_SECURITY_PRODUCTS	Not applicable