EclecticIQ Intelligence at the core

Intelligence Hunting Response

EclecticIQ Endpoint Response Community Edition Product Guide

Version 3.5.1

May 2022

Table of contents

Getting started 5

- Intended Audience 5
- Architecture 5

Configuring the EclecticIQ Endpoint Response Server 6

- Configure VirusTotal 6
- Set up alert aggregation 7
- Specify data retention settings 8

Managing users 10

- Configure single sign-on (SSO) authentication 10
- Add users and assign roles 12
- Deactivate users 13
- Update user profiles 15
- View user activity 16
- Reset user passwords 17

Configuring the client 19

- Edit the osquery.flags file 19
- Client configuration options 20

Understanding filters 28

- Types of filters 28
- Adding Filters 28
  - Examples 30
  - Tables that support filters 30

Using Queries 32

- Query structure 32
- Query workflow 33
- Types of queries 33
- Scheduled queries 34
- Query packs 35
  - Manage existing packs 35

Define a new pack 35

Predefined queries 36

Manage defined queries 36

Define a custom query 37

Live queries 38

Understanding Rules 39

Managing alerts 41

Reviewing alerts 41

Closing alerts 43

Using carves 44

Getting started

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

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

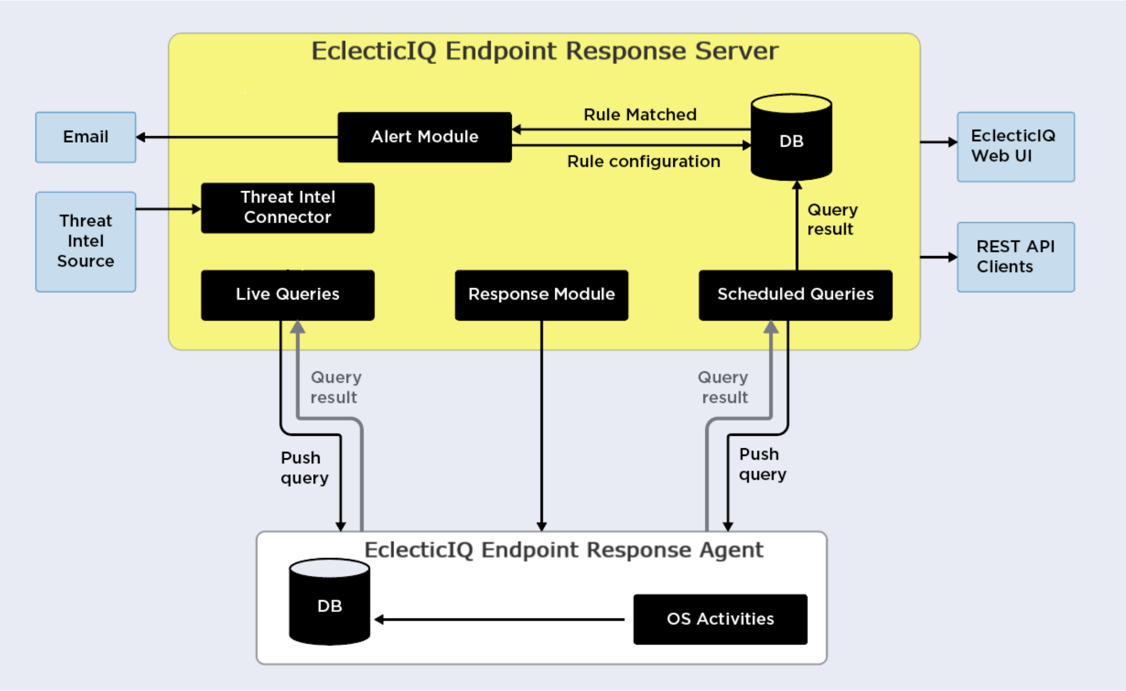
- The server receives, processes, and stores the data sent by the clients.
- The client is installed on each node and monitors all activity on the node.

Intended Audience

This document provides information on how to use the EclecticIQ Endpoint Response server and client.

Architecture

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



Configuring the EclecticIQ Endpoint Response Server

After the EclecticIQ Endpoint Response server is provisioned, the default and seeded configuration comes into play. If needed, you can customize the various configuration settings defined for the server.

Configure VirusTotal

The Virus Total database is a collection of multiple anti-virus (AV) engines. The EclecticIQ Endpoint Response server matches collected file hashes against the VirusTotal database. You can specify the matching criteria based on which alerts are generated using the following:

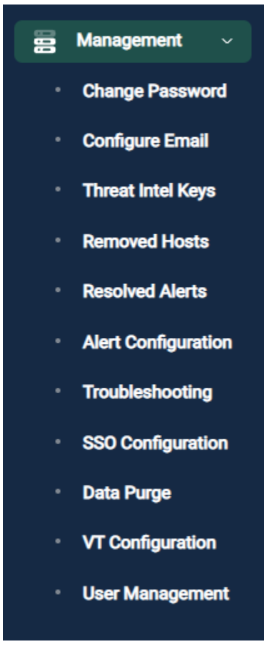
- Minimum Matching AV Count : Specifies the minimum number of AV engines to match to provide a positive match on a file hash.
- VT Scan Retention Period: Indicates the duration in days after which a file hash value is refreshed.
- AV engines list: Select the AV engines from the list to specify the engines with which to match file hashes.

An alert is generated when one of the following conditions is met:

- The file hash matches the specified AV engine count.
- Any one of the selected AV engines provides a positive match.

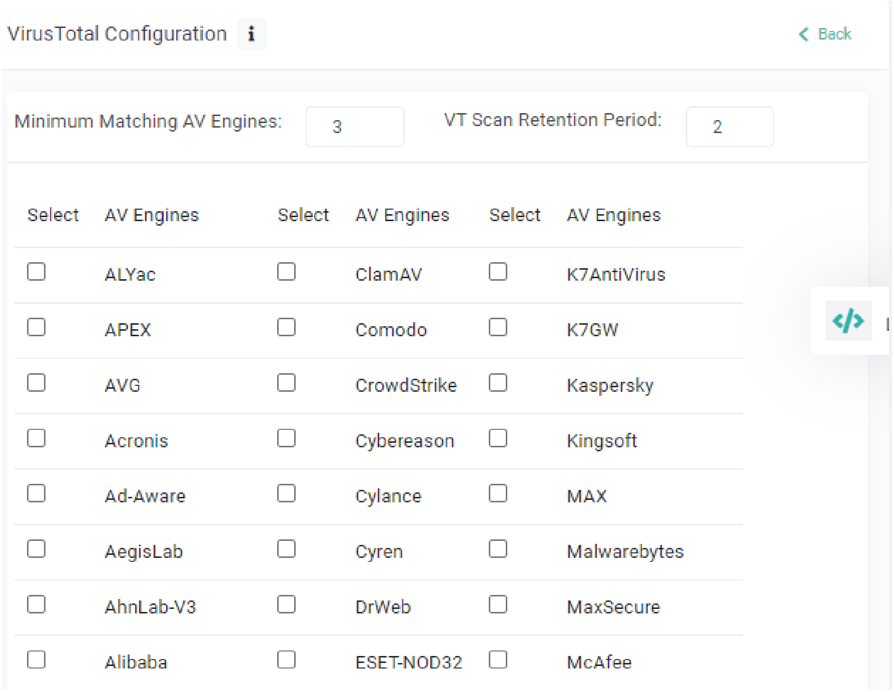
Complete the following steps to configure VirusTotal settings:

1. Access the web interface for the server.



2. Navigate to Management > VT Configuration.
3. Specify the values for the Minimum Matching AV Count and VT Scan Retention Period fields.

4. From the list, select the AV engines with which to match file hashes.



VirusTotal Configuration

Minimum Matching AV Engines: 3 VT Scan Retention Period: 2

Select	AV Engines	Select	AV Engines	Select	AV Engines
□	ALYac	□	ClamAV	□	K7AntiVirus
□	APEX	□	Comodo	□	K7GW
□	AVG	□	CrowdStrike	□	Kaspersky
□	Acronis	□	Cybereason	□	Kingsoft
□	Ad-Aware	□	Cylance	□	MAX
□	AegisLab	□	Cyren	□	Malwarebytes
□	AhnLab-V3	□	DrWeb	□	MaxSecure
□	Alibaba	□	ESET-NOD32	□	McAfee

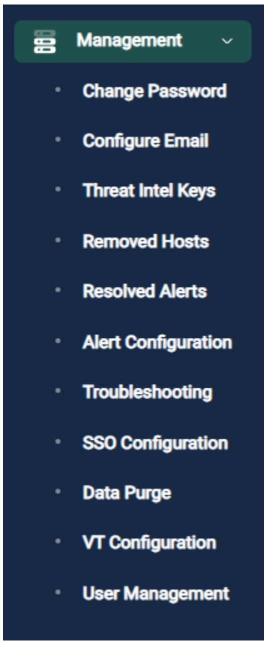
Set up alert aggregation

Using EclecticIQ Endpoint Response you can define rules that match notable activity on the endpoint and generate corresponding alerts. The defined rules are designed to indicate potentially suspicious or malicious behavior. However, on occasion a rule may match benign activity and generate an alert repeatedly. EclecticIQ Endpoint Response server can aggregate (or Deduplicate) the alerts generated based on a rule from an endpoint. For alert aggregation or grouping, you can specify the time window (in seconds) in which to aggregate alerts.

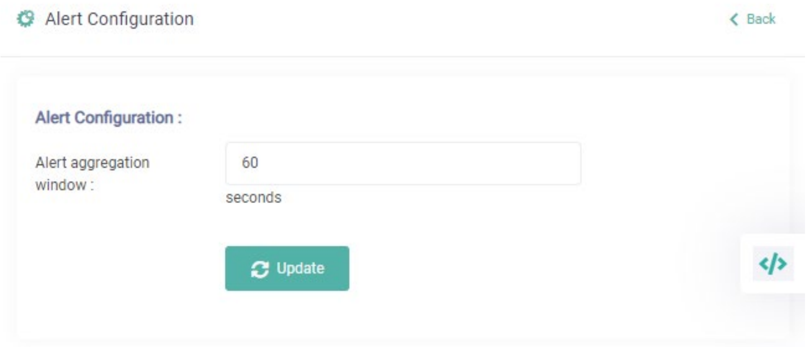
Complete the following steps to configure alert aggregation settings:

1. Access the web interface for the server.

2. Navigate to Management > Alert Configuration.



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



Alert Configuration :

Alert aggregation window : 60 seconds

4. Click Update.

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 hosts is purged.

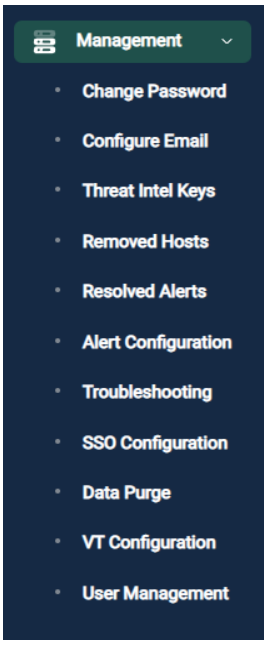
If needed, you can edit the default value and specify how long data is retained in your setup.

Note: Extended data retention periods can impact your sizing needs. Ensure you evaluate sizing requirements before configuring extended data retention periods.

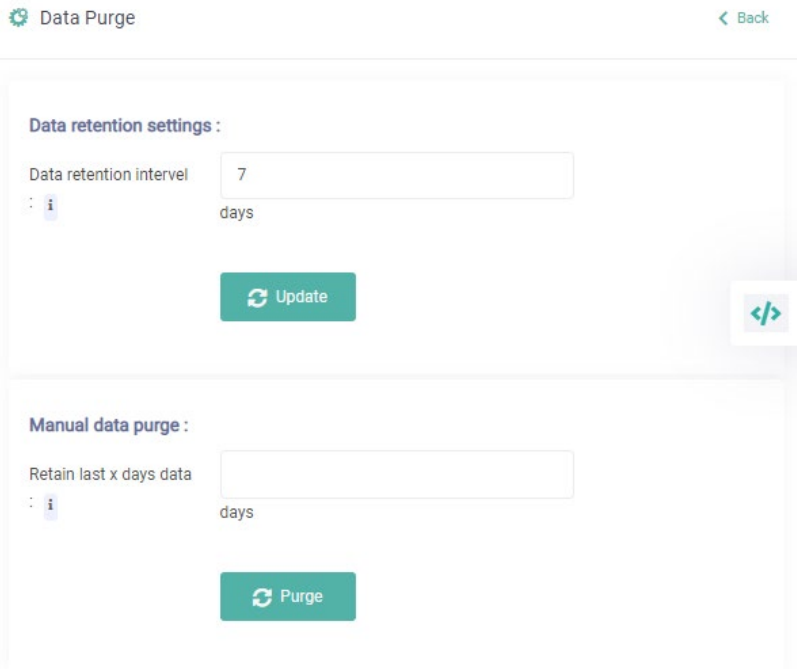
Complete the following steps to specify data retention setting for your setup:

1. Access the web interface for the server.

2. Navigate to Management > Data Purge.



3. Under Data retention settings, specify the number of days for which to retain data in the database.



Data Purge

Data retention settings :

Data retention intervel : 7 days

Manual data purge :

Retain last x days data : days

4. Click Update.

Managing users

As an administrator, you can control and manage the 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 user password

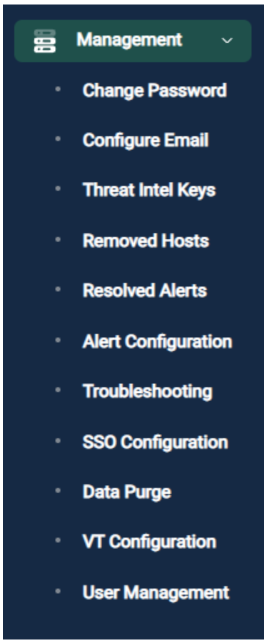
Configure single sign-on (SSO) authentication

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 providing integration with the following identity providers.

- OKTA
- Ping Identity
- Azure
- One Login

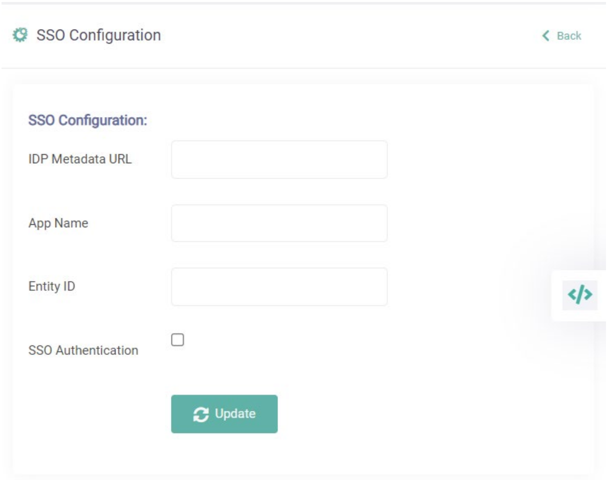
Perform these steps to configure SSO.

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



3. On the SSO configuration page, 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.



SSO Configuration

SSO Configuration:

IDP Metadata URL

App Name

Entity ID

SSO Authentication □

7. Click Update to save your changes.

Add users and assign roles

Starting with the 3.5.1 release, 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.

Here are the tasks an analyst can perform:

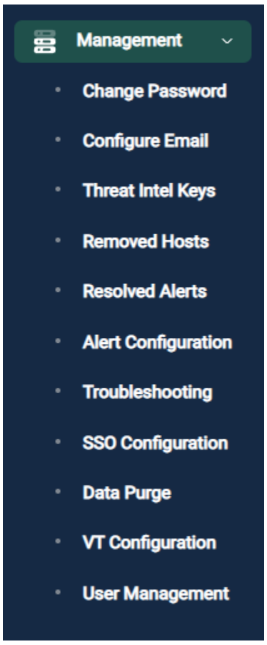
- Browse hosts and review host information, such as properties, activity, policies, and configuration
- Download client installers
- Browse, investigate, and resolve alerts
- Run live queries
- Review rules and threat intel licenses
- Upload YARA signatures
- Perform search, hunt, and carve operations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

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

Perform these steps to add users.

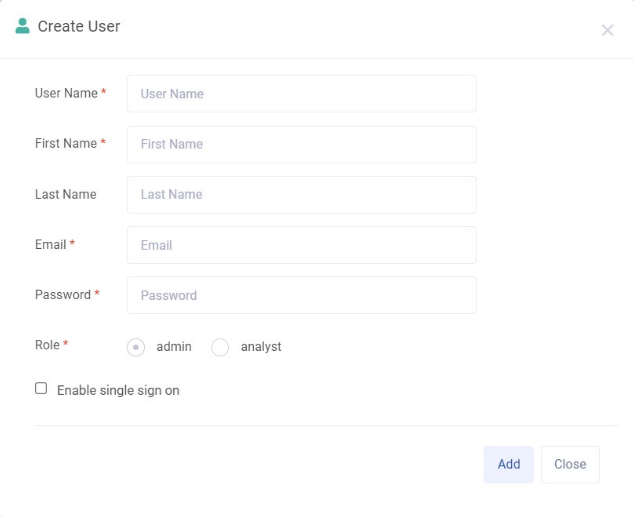
1. Access the web interface for the server.

2. Navigate to Management > User Management.



3. On the User Management page, 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.

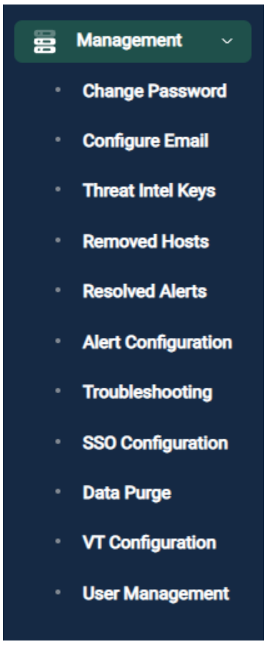
   You are returned the User Management page where a message box indicates if the user is successfully added.

Deactivate users

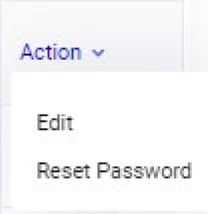
When using EclecticIQ Endpoint Response, you can deactivate a user account to prevent the user from accessing the EclecticIQ Endpoint Response server.

Perform these steps to deactivate a user account.

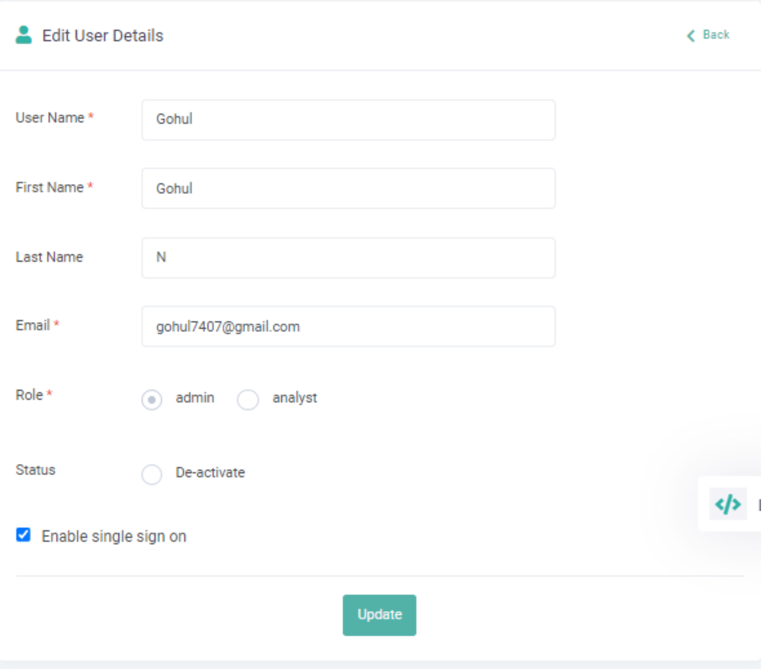
1. Access the web interface for the server.
2. Navigate to Management > User Management.



3. On the User Management page, click the Action drop-down list for the user to deactivate.



4. Select Edit.
5. On the Edit User details page, select De-activate for the Status field.



Edit User Details

Back

User Name *	Gohul
First Name *	Gohul
Last Name	N
Email *	gohul7407@gmail.com
Role *	● admin ○ analyst
Status	○ De-activate

☑ Enable single sign on

Update

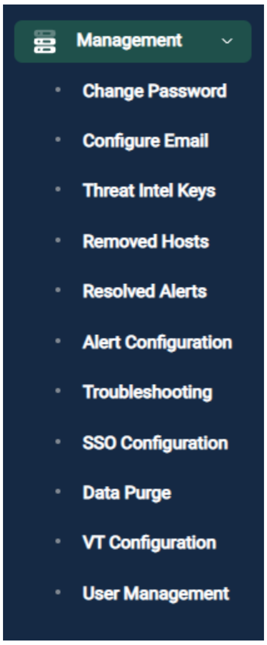
6. Click Update.
The associated user account is deactivated.

Update user profiles

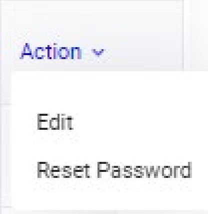
If needed, you can edit details for an existing user account.

Perform these steps to update a user account.

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

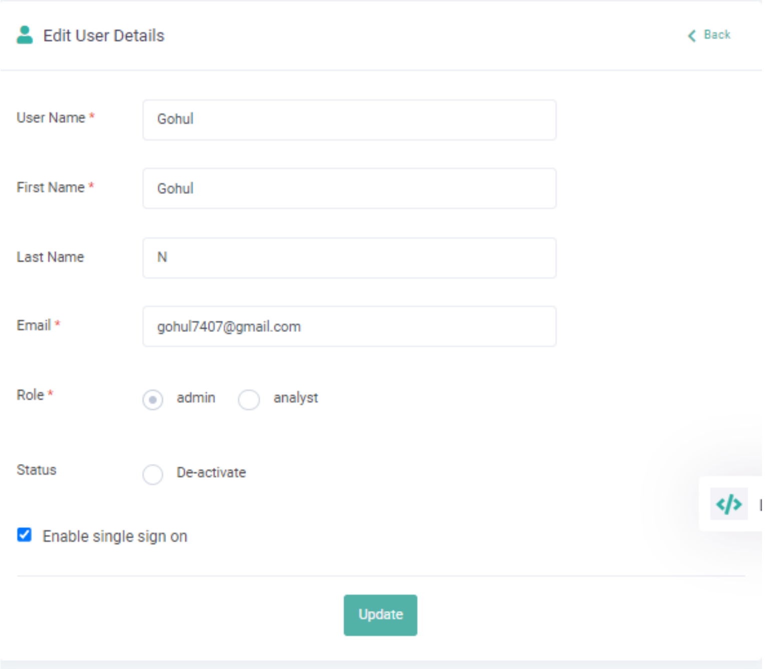


3. On the User Management page, click the Action drop-down list for the user.



4. Select Edit.

5. On the Edit User details page, update the needed details.



Edit User Details

< Back

User Name * Gohul

First Name * Gohul

Last Name N

Email * gohul7407@gmail.com

Role * ● admin ○ analyst

Status ○ De-activate

☑ Enable single sign on

Update

6. Click Update.

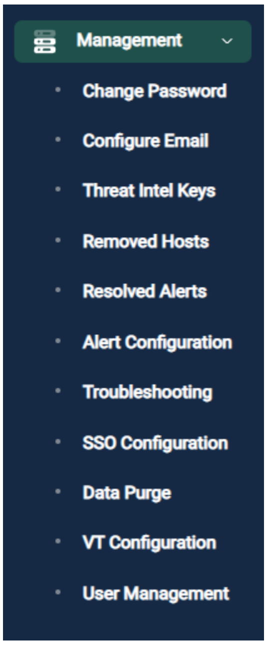
   The associated user account is updated.

View user activity

EclecticIQ Endpoint Response can track activities for each authorized user.

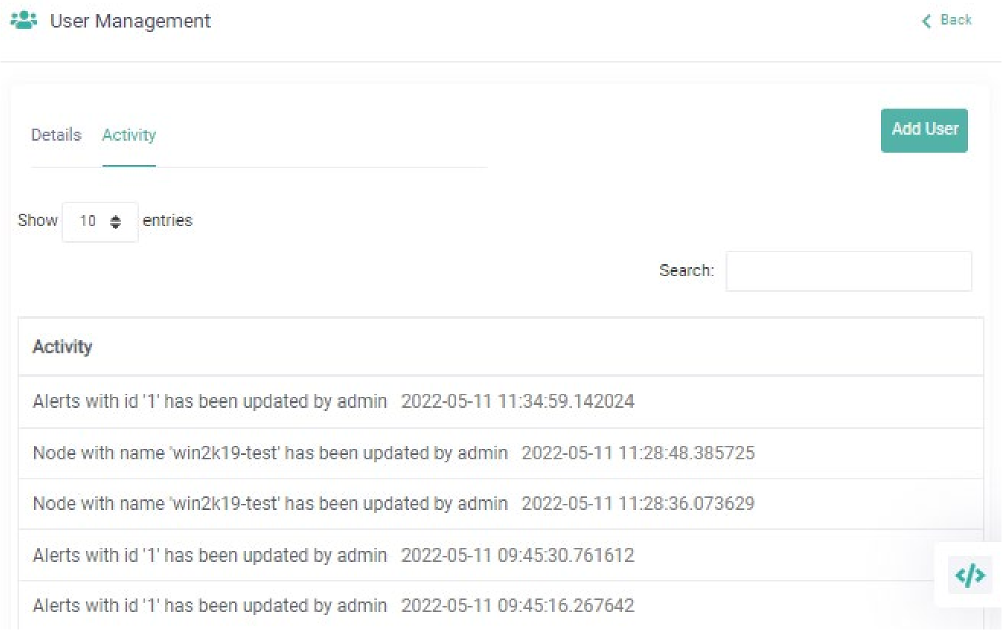
To view recent user activity, perform these steps.

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



3. Switch to the Activity tab.

4. Review the recent user activity.



Activity
Alerts with id '1' has been updated by admin 2022-05-11 11:34:59.142024
Node with name 'win2k19-test' has been updated by admin 2022-05-11 11:28:48.385725
Node with name 'win2k19-test' has been updated by admin 2022-05-11 11:28:36.073629
Alerts with id '1' has been updated by admin 2022-05-11 09:45:30.761612
Alerts with id '1' has been updated by admin 2022-05-11 09:45:16.267642

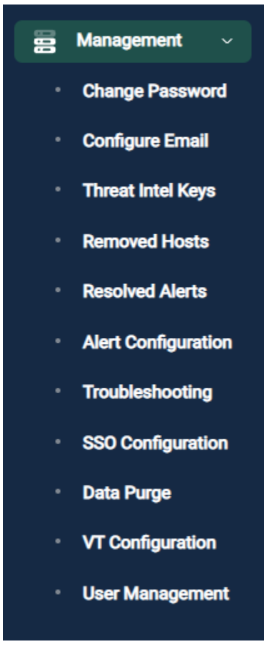
5. Optionally, use the Search field to identify changes made by a specific user or to a specific endpoint.

Reset user passwords

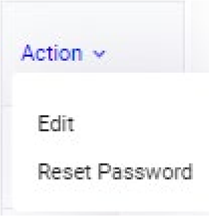
You can reset the password for a user.

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

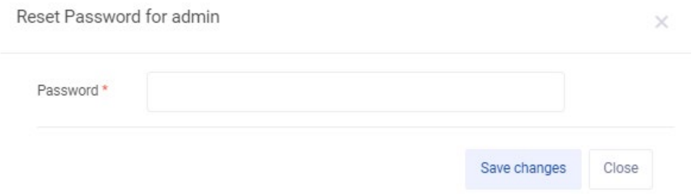
1. Access the web interface for the server.
2. Navigate to Management > User Management.



3. On the User Management page, click the Action drop-down list for the user.



4. Select Reset Password.
5. 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.

6. Save your changes.

Configuring the client

After the EclecticIQ Endpoint Response client is provisioned, the default and seeded configuration comes into play. If needed, you can customize the various configuration settings defined for the EclecticIQ Endpoint Response client.

The topics detailed in this section assume Windows x64 as the client operating system because the EclecticIQ Endpoint Response platform provides maximum number of configuration options for Windows x64-based clients. Similar steps can be used for clients based on other supported operating systems.

To customize the configuration settings, you can modify the following:

- osquery.flags file
- Client configuration options

Edit the osquery.flags file

The osquery.flags file includes all the parameters needed for osquery initialization and functioning. By default, this file is stored in the *C:\Program Files\plgx_osquery* folder.

Although this file contains all the flags supported by osquery, in this section, we will discuss only the key flags that are relevant for the EclecticIQ Endpoint Response platform.

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 endpoint agent. These configured values are passed to the endpoint agent during client provisioning through the osquery.flags file.

Flag	***Description***
extensions_autoload=C:\Program Files\plgx_osquery\extensions.load	Informs the osquery agent to load an extension during osquery initialization. The extensions.load contains the location to the EclecticIQ Endpoint Response Extension file. We recommended that you DO NOT change this flag.

extensions_interval=10
extensions_timeout=90
extensions_require=plgx_win_extension
allow_unsafe
	Control the extension loading behavior of the osquery agent. We recommended that you DO NOT change this flag.

disable_watchdog=true
watchdog_level=-1
	EclecticIQ Endpoint Response Extension is a real-time event monitor on the endpoint. Real time monitoring can be voluminous and query paths to the tables where those events are recorded could surpass the default

Flag	***Description***
	performance constraints imposed by osquery on its child processes and threads. It is therefore recommended to turn off those constraints for better stability.

events_max=1500
events_expiry=3600
	Manage the history of real time events recorded on the endpoint. By default, up to 2500 events are recorded and when the count is hit, all the events that are older than 3600 seconds are purged from the local database. Altering these values can cause performance impact on queries.

config_tls_refresh=300	Controls the refresh interval for agent configuration. Any changes to the agent configuration are picked by the agent after this interval.

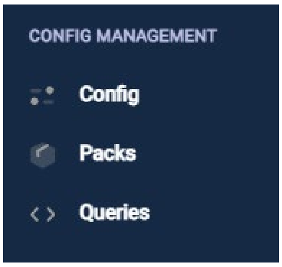
Client configuration options

The EclecticIQ Endpoint Response configuration options are global in nature and are applied to all clients. For the Linux and macOS operating systems, EclecticIQ Endpoint Response is shipped a *Default* seeded configuration. For the Windows clients, two seeded configurations are available: *Default* and *Deep*. As the name suggests, the *Deep* configuration is designed for more aggressive data collection from endpoints than the *Default* configuration.

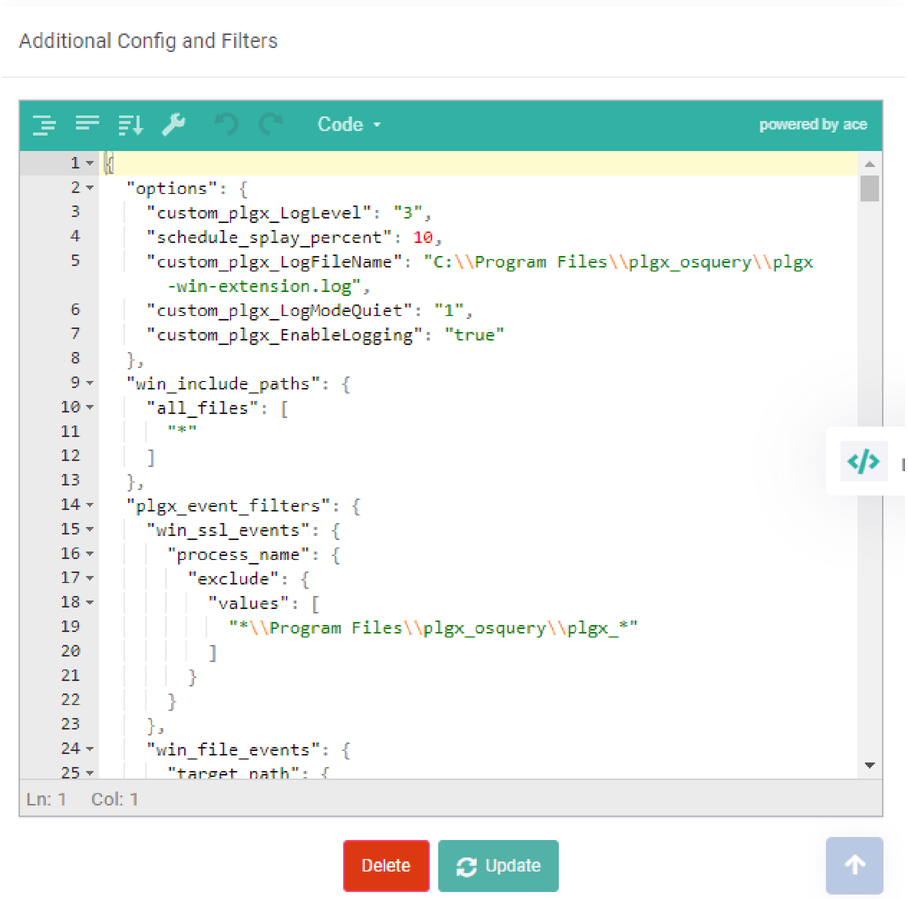
If needed, you can create additional custom configurations (up to a maximum of 5) based on your needs. Once created, you can assign the configuration easily to a specific client based on the host name or to multiple clients based on the operating system.

Perform these steps to view or edit this configuration.

1. Access the web interface for the server.
2. Navigate to CONFIG MANAGEMENT > Config.



3. Scroll on the Config page to review the options listed at the end of the page.



```
{
  "options": {
    "custom_plgx_LogLevel": "3",
    "schedule_splay_percent": 10,
    "custom_plgx_LogFileName": "C:\\Program Files\\plgx_osquery\\plgx
      -win-extension.log",
    "custom_plgx_LogModeQuiet": "1",
    "custom_plgx_EnableLogging": "true"
  },
  "win_include_paths": {
    "all_files": [
      "*"
    ]
  },
  "plgx_event_filters": {
    "win_ssl_events": {
      "process_name": {
        "exclude": {
          "values": [
            "*\\Program Files\\plgx_osquery\\plgx_*"
          ]
        }
      }
    },
    "win_file_events": {
      "target_path": {
```

4. Edit the option values, as needed, and click Update.

Note that the options and values are both case sensitive. Here are the option descriptions.

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)
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	No (Windows only)

Option	*Description*	*Possible values*	*Present in Default config*
		EclecticIQ Endpoint Response agent (from the Hosts page on the server UI by selecting the host and clicking Action > Restart Agent) to ensure the changes take effect.	
custom_plgx_ DnsPorts	If custom_plgx_ EnableDns is set to true, you can specify ten 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 host and clicking Action > Restart Agent) to ensure the changes take effect.	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 host and clicking Action > Restart Agent) to ensure the changes take effect.	No (Windows only)
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_	• 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 host and clicking Action > Restart Agent) to ensure the	No (Windows only)

Option	***Description***	***Possible values***	***Present in Default config***
	EnableShallowSSL at a time.	changes take effect.	
custom_plgx_ EnableHttp	Specifies whether to enable o disable HTTP 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 host 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 Files\\plgx_osquery\\plgx-agent.log.	Yes (Windows only)
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)
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)
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)

Option	***Description***	***Possible values***	***Present in Default config***
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)
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 whe the memory threshold is breached for an endpoint (specified by the custom_plgx MemoryLimitHigh options. • When set to true, the endpoint is restarted. • 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.	• true • false By default, set to false.	No (Windows only)
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 enabl again when memory range is within acceptable limit.	• true • false By default, set to true.	No (Windows only)
custom_plgx_ MemoryLimit High	This flag defines the maximum memory usage for a client exceeding which triggers the Memory watcher functionality	By default, this is set to 150 MB and can be set to a maximum value of 350 MB.	No (Windows only)

Option	*Description*	*Possible values*	*Present in Default config*
	This option comes into play only when the custom_plgx_EnableWatcher option is set to true.		
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)
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, and macOS)
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_ EnableAmsiStrea m 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 malware. The scanned bytes are base64 encoded and reported in the file write events.	• true • false By default, set to false.	No (Windows, only)

Option	***Description***	***Possible values***	***Present in Default config***
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 ignor Image Load events.	• true • false By default, set to true.	No (Windows, only)

Understanding filters

By default, the EclecticIQ Endpoint Response client is designed to capture system events in real-time for a variety of system activities. Also, it makes the telemetry available through a flexible SQL syntax.

Any system, even when idle, generates a high volume of events. Streaming these events from an endpoint to the server at regular intervals using scheduled queries, despite compressing data, can cause a burden on the network and server storage. A lot of the system activity is benign or irrelevant for incident reporting and results in a large volume of data.

By default, the data captured for endpoints is based on multiple seeded filters already defined in the osquery configuration file. These seeded filters reduce the volume of data you need to review to search for incidents of interest. Also, this reduces the burden on network and server resources. These filters are derived from the high fidelity sysmon filters built by SwiftOnSecurity. 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.

Types of filters

Using filters, you can configure the EclecticIQ Endpoint Response client 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 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 file is not captured.
    - When multiple include filters are defined for an event type, an OR condition is used across filters to match the events.

Adding Filters

Filters operate on the tables and are defined in the osquery configuration file. Use JSON syntax to define filters. Place all filters within the plgx_event_filters tag in the osquery configuration file.

Here is the syntax used to define a filter.

```
“plgx_event_filters”: {
       “table name1”: {
```

```
      “column name1” : {
            “filter type” : {
                  “values”:[
                        “value 1”,
                        “value 2”
                        ]
                        }
                  },
      “column name2” : {
            “filter type” : {
                  “values”:[
                        “value 3”,
                        “value 4”
                        ]
                      }
               }
            },
“table name2”: {
      “column name3” : {
            “filter type” : {
                  “values”:[
                        “value 5”,
                        “value 6”
                        ]
                  }
         },
      “column name2” : {
            “filter type” : {
                  “values”:[
                        “value 7”,
                        “value 8”
                        ]
                  }
            }
      }
}
```

In the syntax:

- table name1 and table name2 - Represent the name of the table for which to define filters. You must include the table names in quotes (“”). You can apply filters only on a selected set of tables. For more information, see *Tables that support filters.*
- column name1, column name2, and so on - Indicate the name of the column within the table on which to filter information. You must include the column names in quotes (“”). You can define filters on selected columns in a set of tables. For more information, see *Tables that support filters.*
- filter type - Specifies the filter type. Possible values are include and exclude. You must specify the values in quotes (“”).

- value 1, value 2 and so on - List 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 quotes (“”). Specified values are case insensitive. You can also use regular expressions in the values.
    - * – Represents one or more characters
    - ? – Represents a single character

Examples

Here are a few examples of exclude filters.

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

Here are a few examples of include filters.

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

Tables that support filters

Event filtering is supported on following tables (and fields or columns).

Table Name	***Supported Columns***
win_process_events	cmdline, path, and parent_path
win_registry_events	target_name
win_socket_events	process_name, remote_port, and remote_address

Table Name	***Supported Columns***
win_file_events	target_path and process_name
win_remote_thread_events	src_path, target_path, and function_name
win_dns_events	domain_name
win_dns_response_events	domain_name
win_ssl_events	process_name

Using Queries

A query is a request for data or information from a database table or combination of tables. After the EclecticIQ Endpoint Response client is provisioned, seeded queries are run on the managed endpoints and the fetched data is stored in the database on the EclecticIQ Endpoint Response server. This data stored in various tables and can be viewed or searched. You can review, push, and manage queries from the UI or by using APIs. This topic describes how to manage queries using the UI.

Query structure

All queries that are defined in the EclecticIQ Endpoint Response framework are sent to the EclecticIQ Endpoint Response agent using JSON syntax.

Here is format used to define queries.

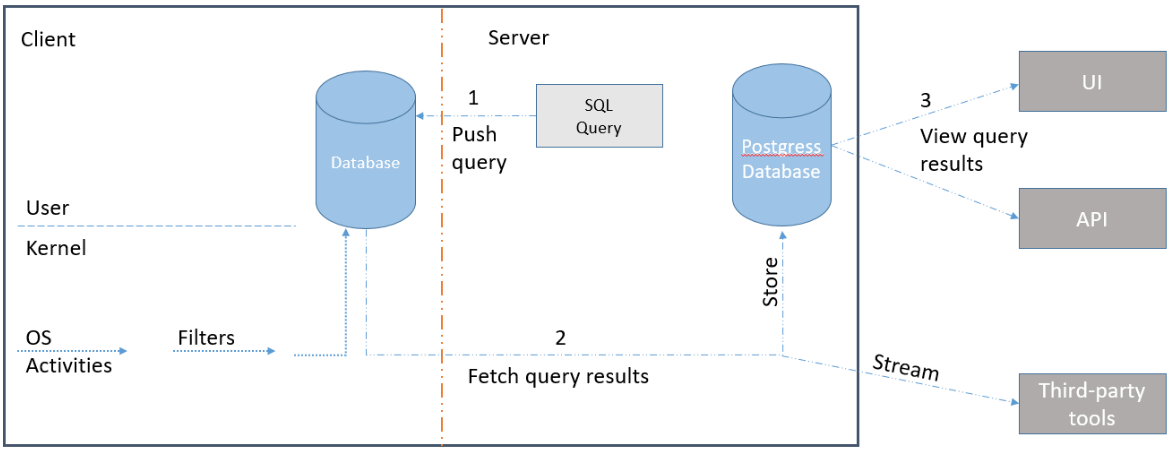
```
"table name": {
         "query": "select * from table  where column='value';",
         "interval": number of seconds,
         "platform": "operating system",
         "version": "x.x.x",
         "description": "this describes the query",
         "value": "Process Events",
         "removed": false
       },
```

Here is an example.

```
"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
       },
```

Query workflow

The following diagram depicts the high-level query workflow.



1. Query is pushed to the relevant nodes at the next configuration refresh interval.
2. Typically, queries (and packs) are applied using tags that are identifiers to help you logically group hosts. You can define tags using the Tag page and assign created tags to nodes using the Hosts page.
3. Query result is sent from the client database to the server database.
4. Query results can be viewed on the UI or by using APIs. Steps 1, 2, and 3 apply to scheduled queries, query packs, and queries. Step 2 is not performed for Live queries.

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. See *Configuring the client* for more information.

Types of queries

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, predefined queries are run to pull relevant information for each node.
Query packs	A pack is a collection of queries. It allows you to logically group queries into categories. Once defined, you can run all queries included in a pack simultaneously.
Queries	A query is an individual request for data from a table or collection of tables. Define an individual query, as needed, to fetch data for nodes.

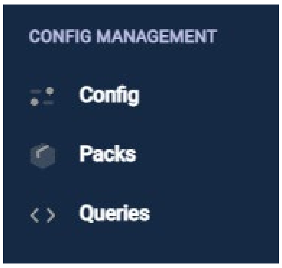
Type	*Description*
Live Queries	A Live Query is suitable to meet your immediate and infrequent needs. It gives you a current snapshot of the nodes.

Scheduled queries

These out-of-box queries run frequently (as defined for the query) to fetch data from the nodes and require no configuration.

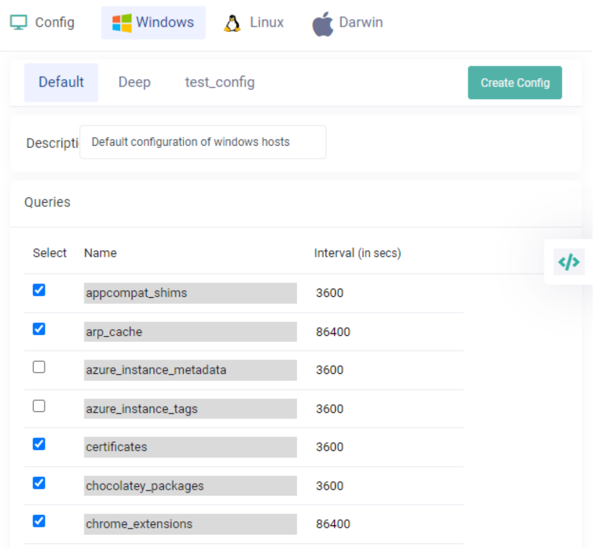
Perform these steps to view or edit scheduled queries:

1. Access the web interface for the server.
2. Navigate to CONFIG MANAGEMENT > Config.



The page lists the predefined queries available for Windows, Linux, and macOS.

3. Select an operating system, such as Windows.
4. Review the predefined queries applied on the Windows endpoints.



Descripti Default configuration of windows hosts

Select	Name	Interval (in secs)
☑	appcompat_shims	3600
☑	arp_cache	86400
□	azure_instance_metadata	3600
□	azure_instance_tags	3600
☑	certificates	3600
☑	chocolatey_packages	3600
☑	chrome_extensions	86400

5. Deselect a query to remove it from the applied client configuration.
6. 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.
7. Click Update to save your changes.

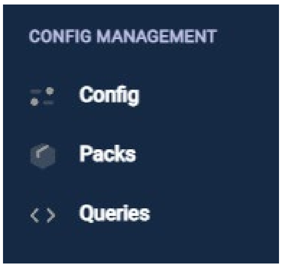
Query packs

By default, few packs are included with your EclecticIQ Endpoint Response configuration. You can add more packs, as needed, to meet your requirements.

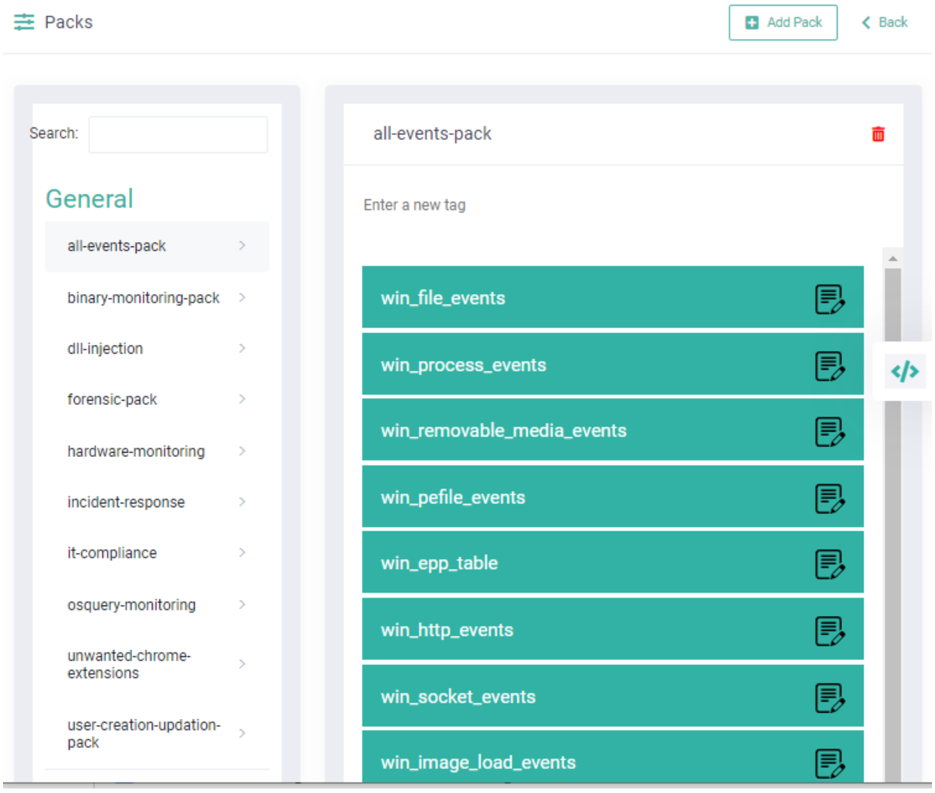
Manage existing packs

Perform these steps to view and edit existing packs:

1. Access the web interface for the server.
2. Navigate to CONFIG MANAGEMENT > Pack.



3. Review the available packs.
4. Click a pack name to see the included queries.



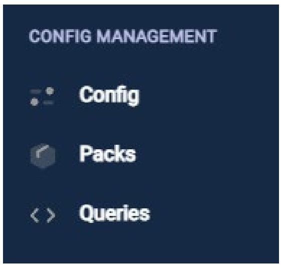
5. To apply a pack, specify the tag associated with the relevant nodes. All queries in the pack are applied to the associated nodes at the next config refresh interval.

Define a new pack

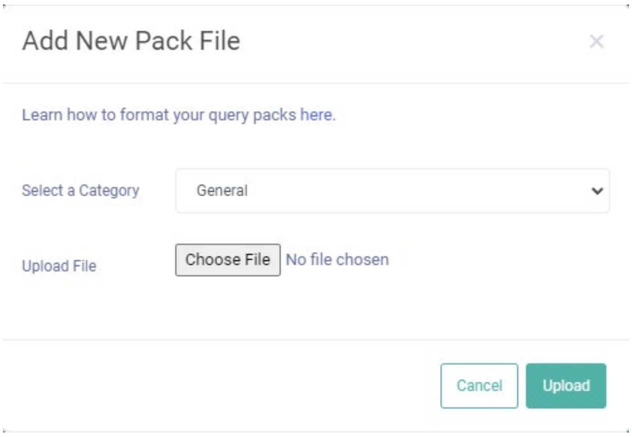
Perform these steps to add a new query pack.

1. Access the web interface for the server.

2. Navigate to CONFIG MANAGEMENT > Pack.



3. Click Add Pack. The Add New Pack File dialog is displayed.


Add New Pack File

Learn how to format your query packs here.

Select a Category: General

Upload File: Choose File No file chosen

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.

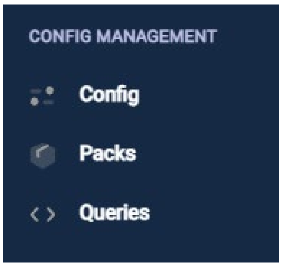
Predefined queries

By default, multiple predefined queries are included with your EclecticIQ Endpoint Response configuration. These are defined but not assigned to any nodes by default.

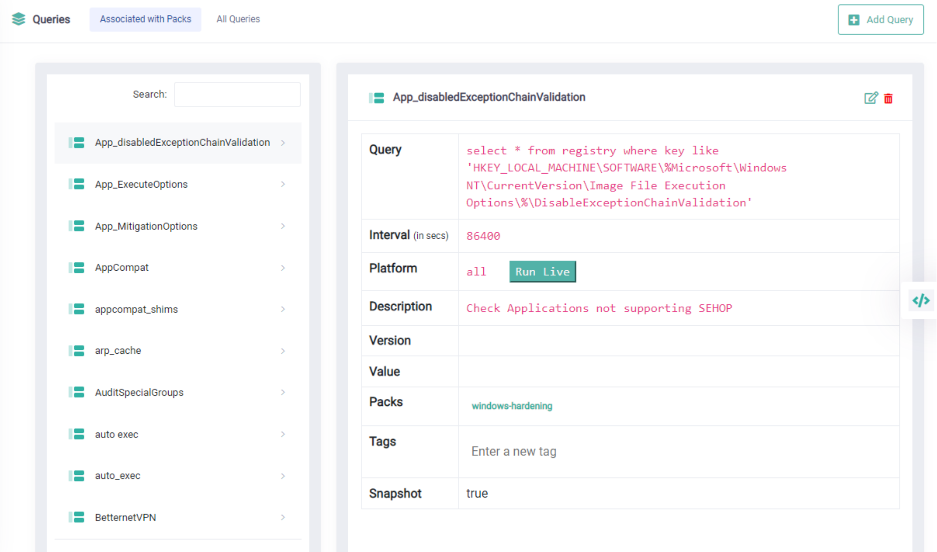
Manage defined queries

Perform these steps to view or run a predefined query.

1. Access the web interface for the server.
2. Navigate to CONFIG MANAGEMENT > Queries.



3. Click a query to review its details.



App_disabledExceptionChainValidation

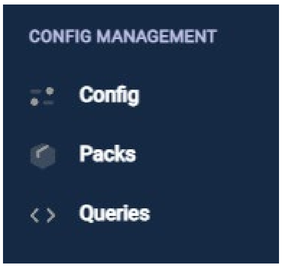
Query	select * from registry where key like 'HKEY_LOCAL_MACHINE\SOFTWARE\%Microsoft\Windows NT\CurrentVersion\Image File Execution Options\%\DisableExceptionChainValidation'
Interval (in secs)	86400
Platform	all
Description	Check Applications not supporting SEHOP
Version	
Value	
Packs	windows-hardening
Tags	Enter a new tag
Snapshot	true

4. Click Run Live for a query to run it immediately. For more information, see Live queries.
5. Specify the nodes on which to run the query by adding relevant tags.

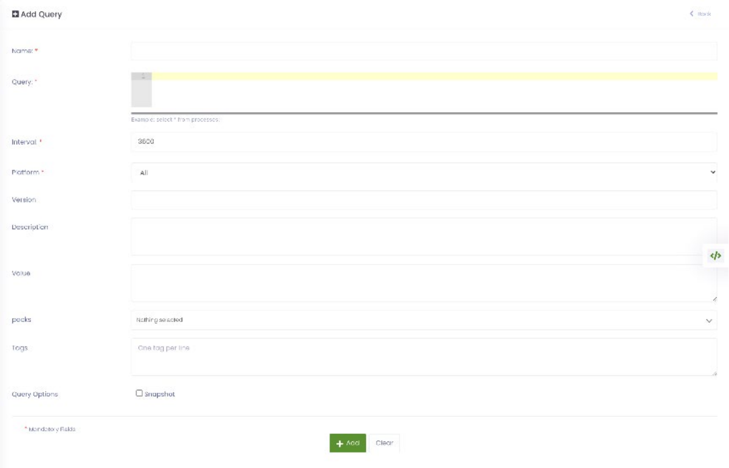
Define a custom query

Perform these steps to add a new query:

1. Access the web interface for the server.
2. Navigate to CONFIG MANAGEMENT > Queries.



3. On the Queries page, click Add Query. The Add Query page is displayed.



Name: *	
Query: *	
	Example: select * from processes;
Interval *	3600
Platform *	All
Version	
Description	
Value	
packs	Nothing selected
Tags	One tag per line
Query Options	□ Snapshot

* Mandatory Fields

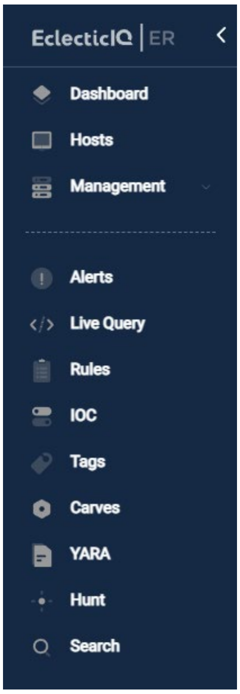
4. Enter the query details, such as name, query, interval, platform, and version.
5. Optionally, select a pack from the Packs list to associate the query with a pack.

6. Optionally, assign tags to the query to run on associated nodes.
7. Click Add to save the query.

Live queries

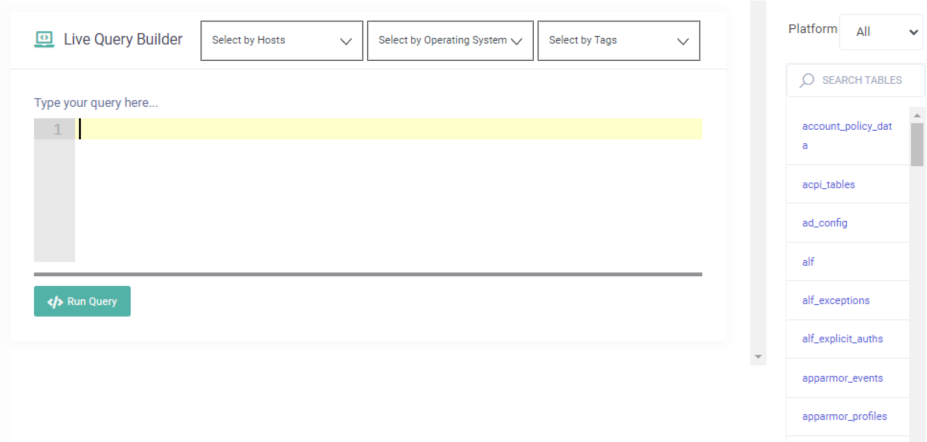
When you run a Live query, the data is fetched and displayed to you immediately. If needed, you can save the data in an Excel or CSV file. Perform these steps to define and run a live query:

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



The Live Query Builder page is displayed.

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



4. Select the operating system, hosts, or tags to specify the nodes on which to run the query.
5. Click Run Query. The query results are displayed.
6. Click Excel or CSV to save the data in Excel or CSV format, respectively.

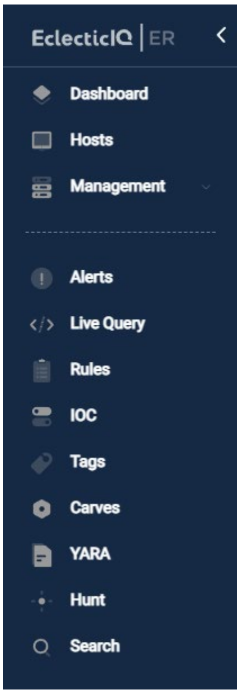
Understanding Rules

Rules, in the EclecticIQ Endpoint Response framework, 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.

EclecticIQ Endpoint Response provides a set of predefined rules (available only in the Enterprise Edition of the EclecticIQ Endpoint Response) that can serve as a starting point to detect some of the malicious behavior. EclecticIQ Endpoint Response provides a seeded repository of rules in Sigma format that you can use as a starting point. These rules have been developed based on MITRE attack vector framework. Navigate to https://github.com/polylogyx/DetectionRules to review the seeded rules.

You can define rules using the web interface. Perform these steps to view or edit rules:

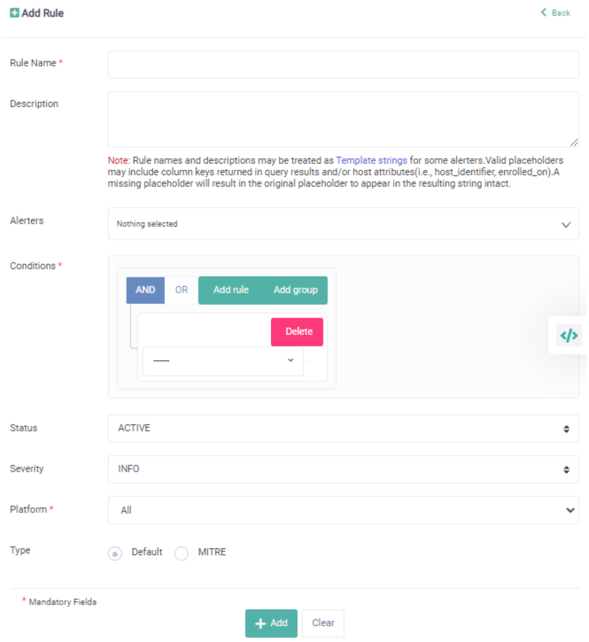
1. Access the web interface for the server.
2. Navigate to Rules.



The Rules page is displayed.

3. Select a rule in the list to review its details in the right pane.
4. Click Edit Rule for a rule to modify it. Click Update when done.

5. Click Add Rule to open the Add Rule page to define a new rule. Click Add when done.



Add Rule

Rule Name *

Description

Note: Rule names and descriptions may be treated as Template strings for some alerters.Valid placeholders may include column keys returned in query results and/or host attributes(i.e., host_identifier, enrolled_on).A missing placeholder will result in the original placeholder to appear in the resulting string intact.

Alerters: Nothing selected

Conditions *

Status: ACTIVE

Severity: INFO

Platform *: All

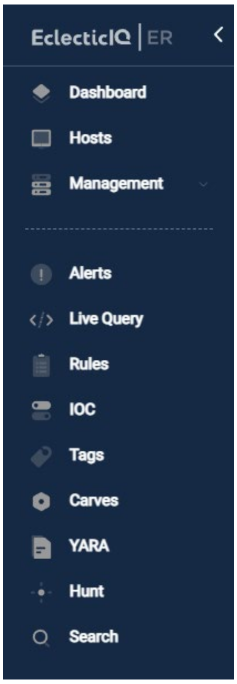
Type: ● Default ○ MITRE

* Mandatory Fields

Managing 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 Threat Intel feed.

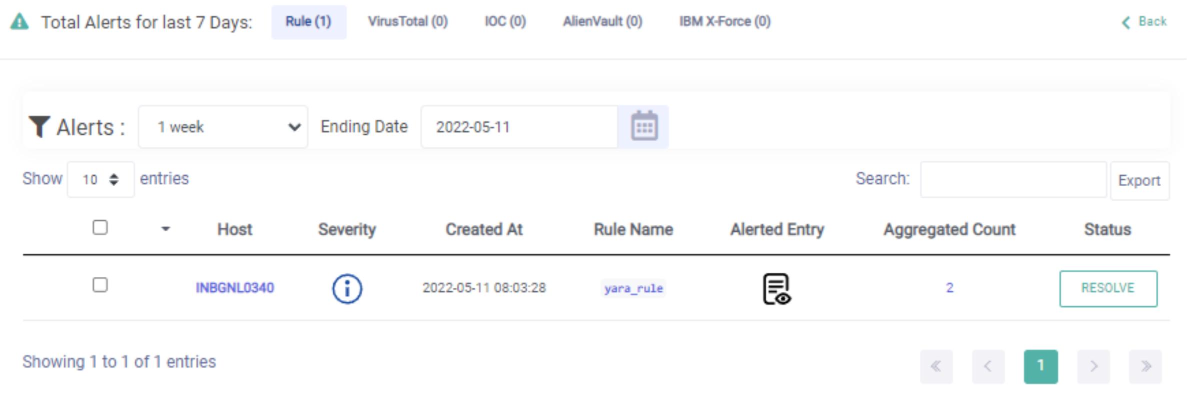
The Alerts page is the central console that allows you to manage and review alerts. Click Alerts to view the Alerts page.



Reviewing alerts

Click the AlientVault OTX, IBM X-Force, Rule, and VirusTotal tabs on the page to review the alerts based on the source generating the alerts.

For example, when you click the Rule tab only the alerts generated based on predefined rules matching event data are displayed.



Alerts : 1 week Ending Date 2022-05-11

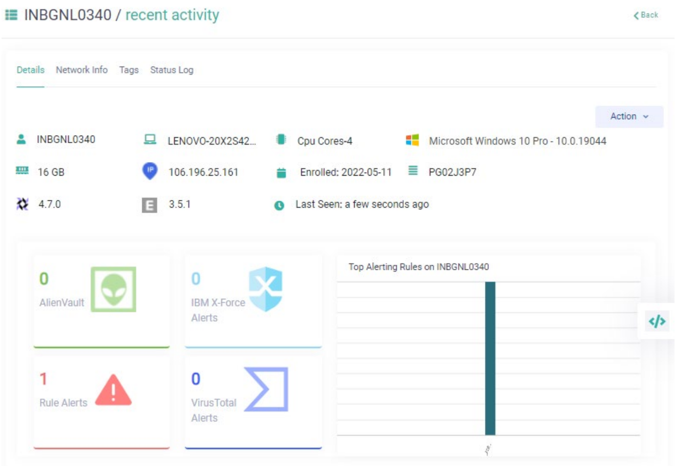
Show 10 entries Search: Export

□		Host	Severity	Created At	Rule Name	Alerted Entry	Aggregated Count	Status
□		INBGNL0340	ⓘ	2022-05-11 08:03:28	yara_rule		2	RESOLVE

Showing 1 to 1 of 1 entries

Perform these steps to review alert information:

1. Click the node name to view endpoint details.



INBGNL0340 / recent activity

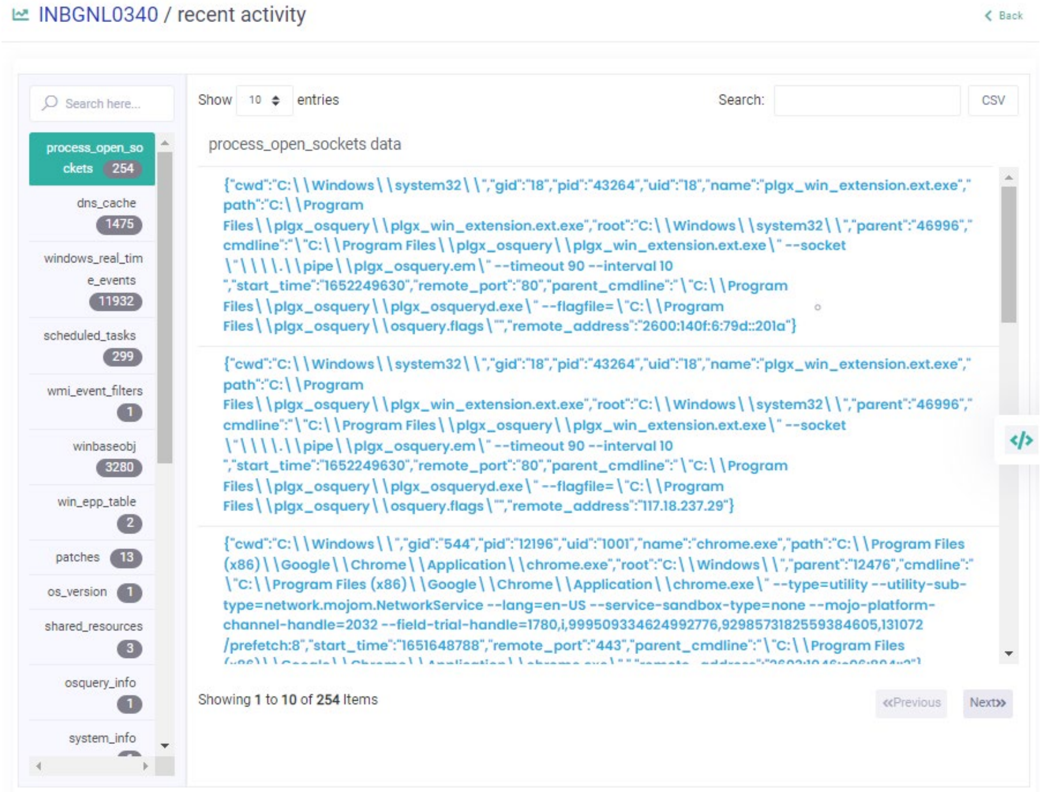
INBGNL0340 LENOVO-20X2S42... Cpu Cores-4 Microsoft Windows 10 Pro - 10.0.19044

16 GB 106.196.25.161 Enrolled: 2022-05-11 PG02J3P7

4.7.0 3.5.1 Last Seen: a few seconds ago

2. Click the recent activity link to open the recent activity page.

   On this page, you can run various queries to view node-specific information. Click the recent activity link for the node to review details.



INBGNL0340 / recent activity

process_open_sockets data

```
{"cwd":"C:\\Windows\\system32\\","gid":"18","pid":"43264","uid":"18","name":"plgx_win_extension.ext.exe","path":"C:\\Program Files\\plgx_osquery\\plgx_win_extension.ext.exe","root":"C:\\Windows\\system32\\","parent":"46996","cmdline":"\"C:\\Program Files\\plgx_osquery\\plgx_win_extension.ext.exe\" --socket \"\\\\.\\pipe\\plgx_osquery.em\" --timeout 90 --interval 10 ","start_time":"1652249630","remote_port":"80","parent_cmdline":"\"C:\\Program Files\\plgx_osquery\\plgx_osqueryd.exe\" --flagfile=\"C:\\Program Files\\plgx_osquery\\osquery.flags\"","remote_address":"2600:140f:6:79d::201a"}

{"cwd":"C:\\Windows\\system32\\","gid":"18","pid":"43264","uid":"18","name":"plgx_win_extension.ext.exe","path":"C:\\Program Files\\plgx_osquery\\plgx_win_extension.ext.exe","root":"C:\\Windows\\system32\\","parent":"46996","cmdline":"\"C:\\Program Files\\plgx_osquery\\plgx_win_extension.ext.exe\" --socket \"\\\\.\\pipe\\plgx_osquery.em\" --timeout 90 --interval 10 ","start_time":"1652249630","remote_port":"80","parent_cmdline":"\"C:\\Program Files\\plgx_osquery\\plgx_osqueryd.exe\" --flagfile=\"C:\\Program Files\\plgx_osquery\\osquery.flags\"","remote_address":"117.18.237.29"}

{"cwd":"C:\\Windows\\","gid":"544","pid":"12196","uid":"1001","name":"chrome.exe","path":"C:\\Program Files (x86)\\Google\\Chrome\\Application\\chrome.exe","root":"C:\\Windows\\","parent":"12476","cmdline":"\"C:\\Program Files (x86)\\Google\\Chrome\\Application\\chrome.exe\" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2032 --field-trial-handle=1780,i,9995093346249927776,9298573182559384605,131072 /prefetch:8","start_time":"1651648788","remote_port":"443","parent_cmdline":"\"C:\\Program Files
```

Showing 1 to 10 of 254 Items

3. Review the severity information. For rule-based alerts severity values are none, info, warning, and critical. For alerts based on the Threat Intel data, severity values are low, medium, and high.
4. Click Intel Data for an alert to view the source data based on which the alert was generated.
5. Click Alerted Entry for an alert to view the event associated with the alert.
6. Optionally, use the Search field to filter alerts based on a criterion.

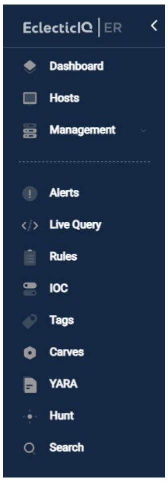
Note: The EclecticIQ Endpoint Response Enterprise Edition offers additional alert management features. When using the Enterprise Edition, you can review the event timeline for your enterprise to understand the traffic trend. You can also deep dive or investigate an alert to determine the actions you might need to take.

Closing alerts

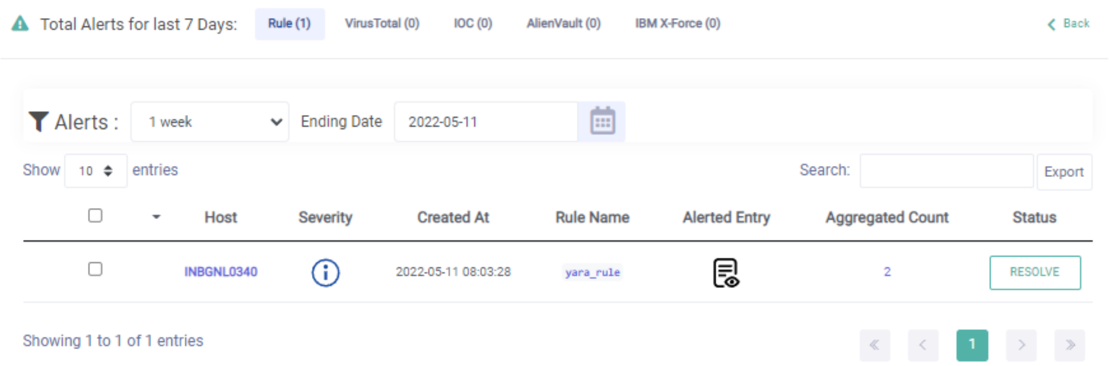
After you have processed an alert, close it to remove it from the Alerts page.

Perform these steps to close an alert:

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



3. On the Alerts page, click Resolve for an alert.



Alerts : 1 week Ending Date 2022-05-11

Show 10 entries

Search: Export

□		Host	Severity	Created At	Rule Name	Alerted Entry	Aggregated Count	Status
□		INBGNL0340	ⓘ	2022-05-11 08:03:28	yara_rule		2	RESOLVE

Showing 1 to 1 of 1 entries

A message box is displayed.

4. Select an option in the message box to provide the user verdict.
5. Click Submit.

The alert is resolved and removed from the Alerts page.

Resolved

Alert has been successfully resolved

Using carves

For investigative purposes, you can fetch any file from the managed endpoints to the EclecticIQ Endpoint Response server. You can fetch files by using Live queries. You can fetch a single file or batch of files based on specified criteria.

On the EclecticIQ Endpoint Response server, each crave file is stored in archive (.TAR) format.

Perform these steps to acquire files.

1. Run a Live query.
2. On the Live Query Builder page, specify the query.

   - To fetch a single file from an endpoint, use the following 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.

   - To fetch one or more files that meet a specified criterion, use the following 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 and type indicates the file type. You can use other file properties, as needed, to fetch the files.

3. Navigate to the Carves to open the Carves page.
4. Review the acquired files.
5. Click a file name to download the file.