

COMODO
Creating Trust Online®



Comodo cWatch Network

Software Version 2.23

Administrator Guide

Guide Version 2.23.010820

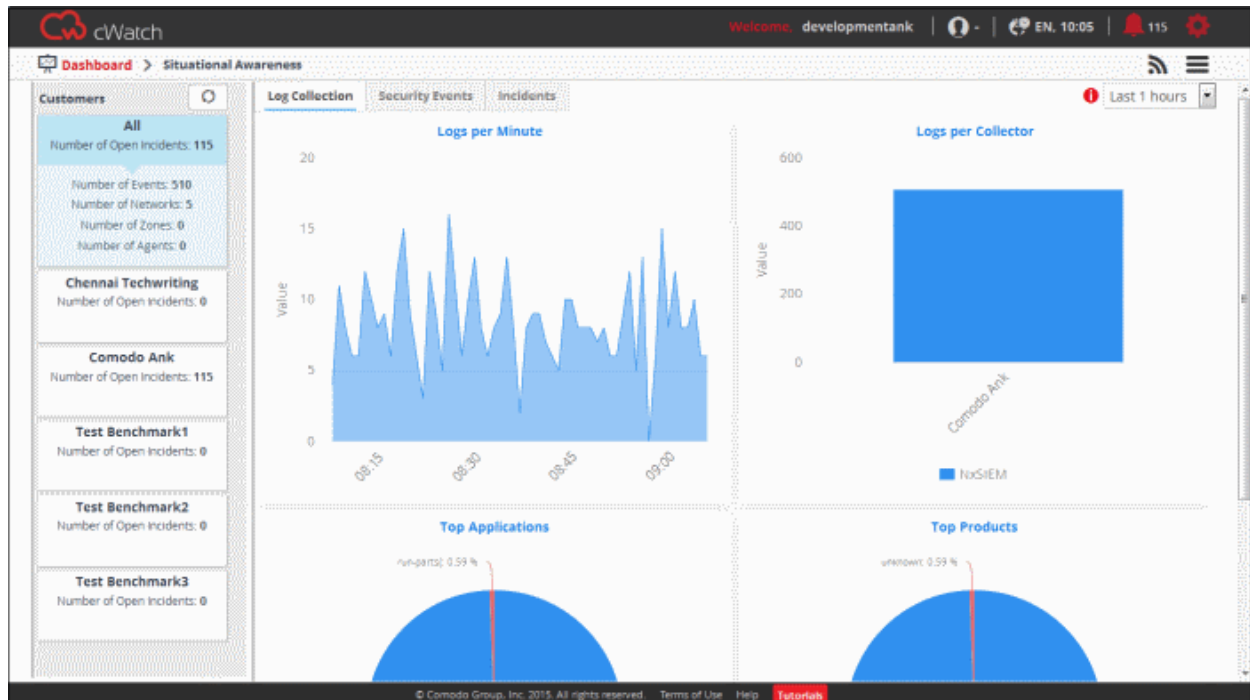
Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction to Comodo cWatch Network.....	3
1.1 Purchase a License	5
1.2 Log-in to the Admin Console.....	9
1.3 The Main Interface	10
2 The Dashboard.....	14
3 Customer Asset Management.....	24
3.1 Add Customers.....	25
3.2 Add Assets for Monitoring.....	28
3.2.1 Hard Assets.....	29
3.2.2 Soft Assets.....	34
3.3 Configure Nxlog and Rsyslog to Send Logs to cWatch Network Server.....	37
3.4 Edit Customers.....	39
4 Query Management.....	42
4.1 Configure Event Queries.....	42
4.2 Long Term Analysis.....	78
4.3 Configure Custom Dashboards.....	85
4.4 Event Field Selection Settings.....	102
5 Manage Rules.....	105
5.1 Manage Correlation Rules.....	106
5.2 Manage Tagged Rules.....	131
5.3 Manage Aggregation Rules.....	141
6 Incidents	166
6.1 Manage Incidents.....	167
6.2 Incident Category Management.....	176
6.3 Category Action Management.....	181
7 Lists.....	184
7.1 Manage Live Lists.....	185
7.2 Manage Live List Content.....	196
7.3 Manage Range List Content.....	201
7.4 Manage IP Range List Content.....	204
7.5 Manage Multiple Column List Content.....	207
8 Manage Reports	212
9 Administration	235
9.1 Event Collection.....	236
9.2 Phantom Settings.....	237
9.3 Manage Users.....	241
9.4 View License and Subscription Details	244
Appendix 1 - Field Groups and Event Items Description.....	246
Appendix 2 - cWatch Supported Logs.....	250
About Comodo Security Solutions	253

1 Introduction to Comodo cWatch Network

Comodo cWatch Network is a security intelligence and event management product (SIEM) built exclusively for MSPs to help them grow their business. cWatch Network features advanced event log monitoring, built-in reporting, multiple pre-set queries, a powerful custom-query interface, automatic assignment of incidents to personnel, customizable dashboards and real-time alerts. cWatch Network's multi-tenancy architecture enables MSPs to manage their customers from a single deployment and benefit from "big data" scalability as their log sizes increase.



Features

- Real-time event monitoring and processing
- Long-term log retention, archiving and backup
- Multiple 'Ready-to-go' queries to address typical use-cases
- Powerful query creation interface for custom queries
- Configurable custom dashboards
- Custom report generation and report scheduling
- Incident management
- Per-customer policy creation and management
- Immediate alerts and incident delegation
- 'Live Lists' of event parameters for use in queries and correlation rules
- Rapid search over huge volumes of data

Guide Structure

This guide is intended to take you through the configuration and use of cWatch Network and is broken down into the following main sections.

- **Introduction to Comodo cWatch Network**

- **Purchase a License**
- **Log-in to the Administrative Console**
- **The Main Interface**
- **The Dashboard**
- **Customer Asset Management**
 - **Add Customers**
 - **Add Assets for Monitoring**
 - **Configure Nxlog and Rsyslog to Send Logs to cWatch Network Server**
 - **Edit Customers**
- **Query Management**
 - **Configure Event Queries**
 - **Long Term Analysis**
 - **Configure Custom Dashboards**
 - **Event Field Selection Settings**
- **Managing Rules**
 - **Manage Correlation Rules**
 - **Manage Tagged Rules**
 - **Manage Aggregation Rules**
- **Incidents**
 - **Manage Incidents**
 - **Incident Category Management**
 - **Category Action Management**
- **Lists**
 - **Manage Live Lists**
 - **Manage Live List Content**
 - **Manage Range List Content**
 - **Manage IP Range List Content**
 - **Manage Multiple Column List Content**
- **Manage Reports**
- **Administration**
 - **Event Collection**
 - **Phantom Settings**
 - **Manage Users**
 - **View License and Subscription Details**
- **Appendix 1 - Field Groups and Event Items Description**
- **Appendix 2 – cWatch Supported Logs**

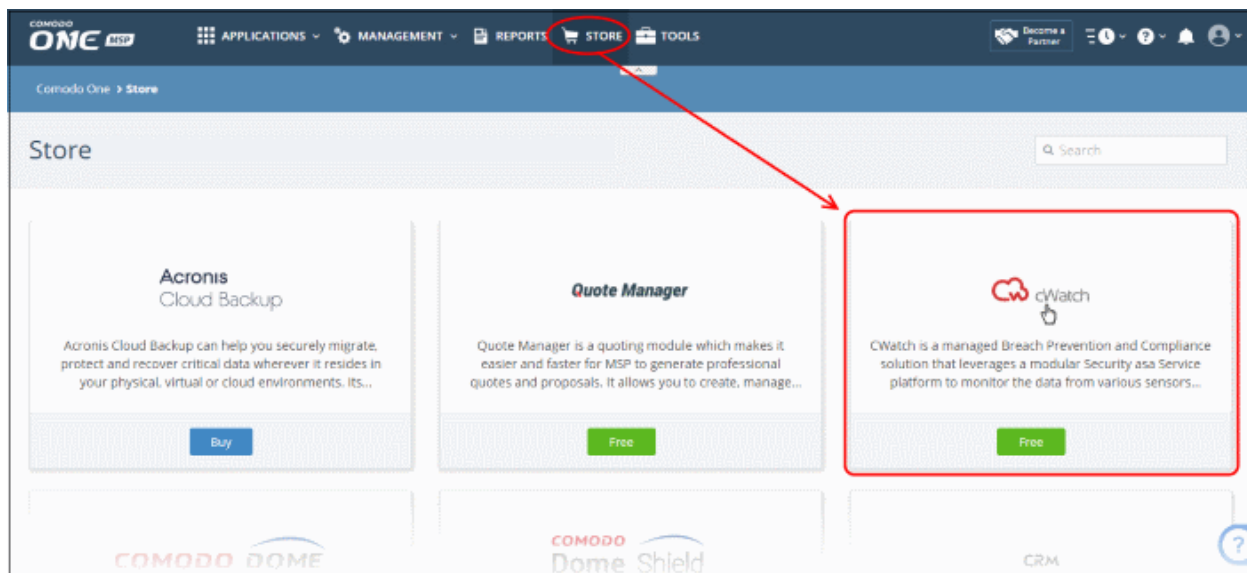
1.1 Purchase a License

To purchase a license:

- There are three ways you can subscribe for cWatch – via a Comodo One account, Comodo Dragon and via an ITarian account
 - [Click here](#) to learn how to subscribe for a Comodo One account
 - [Click here](#) to learn how to subscribe for a Comodo Dragon account.
 - [Click here](#) to learn how to subscribe for an ITarian account

cWatch purchasing is the same for both Comodo One, Comodo Dragon and ITarian. The following tutorial explains how to subscribe via Comodo One.

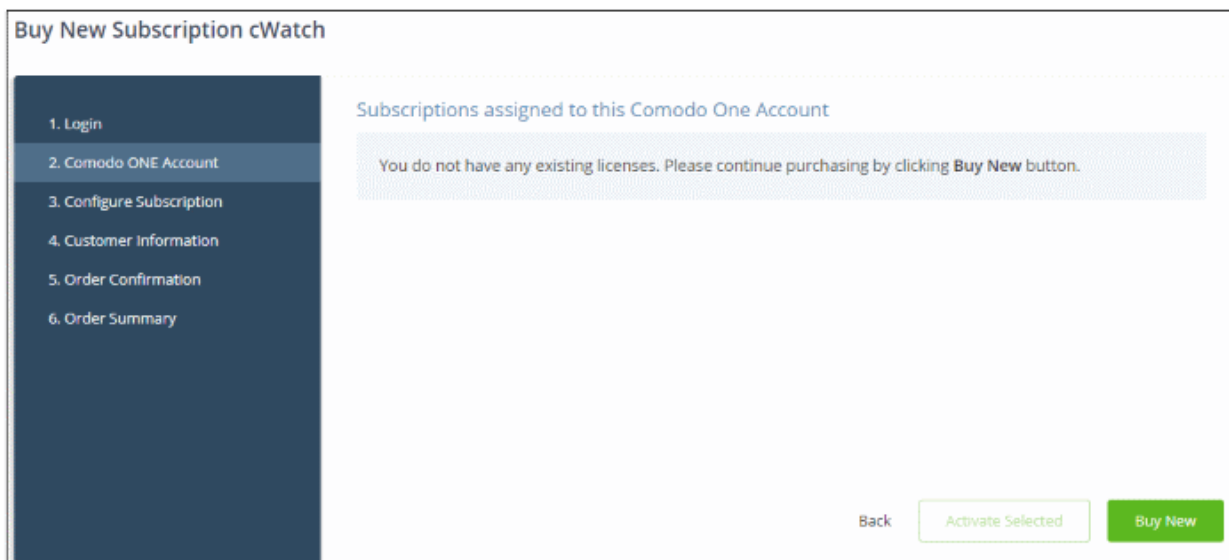
- Login to your **Comodo One / Comodo Dragon / ITarian** account
- Click 'Store' on the menu bar
- Click the cWatch tile to see product details and pricing:



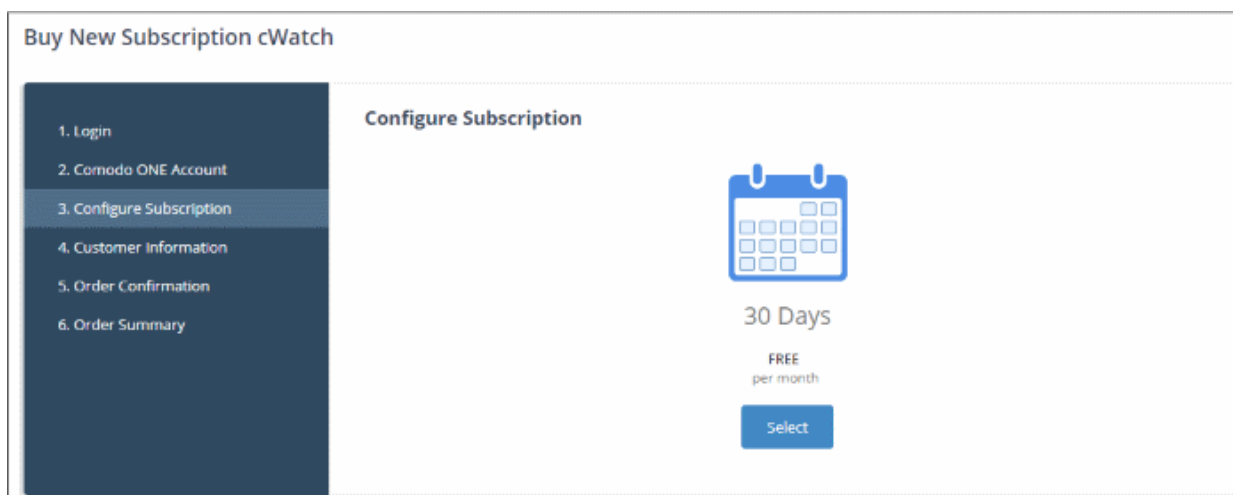
- Click the 'Free' button to open the purchase page:

The screenshot shows the 'Buy New Subscription cWatch' page. On the left, a sidebar lists the steps: 1. Login, 2. Comodo ONE Account, 3. Configure Subscription, 4. Customer Information, 5. Order Confirmation, 6. Order Summary. The main content area has a 'Login' section with a 'Login *' label, a text input field containing 'newcwatchcne@yopmail.com', and a 'Password *' label with an empty text input field. A 'Forgot Password' link is located below the password field. A green 'Login' button is at the bottom right.

- Enter your C1 account password and click 'Login'



- Click 'Buy New'



- Click 'Select'

Buy New Subscription cWatch

1. Login
2. Comodo ONE Account
3. Configure Subscription
4. Customer Information
5. Order Confirmation
6. Order Summary

Customer Information

Company Name

Company Website Phone Number *

Street Address * Street Address 2

City * Country *

State or Province Postal Code *

Billing Information
 The same as Contact Information

Terms and Conditions
 I have read and agree the [End User License/Service Agreement](#).

Back Next >

- Your company name is auto-filled. Edit it if required and provide website and company address details.
- Read and agree to the end-user license/service agreement.
- Click 'Next' to proceed to order confirmation

Buy New Subscription cWatch

1. Login
2. Comodo ONE Account
3. Configure Subscription
4. Customer Information
5. Order Confirmation
6. Order Summary

Order Confirmation


PRODUCT	LICENSE PERIOD	FULL PRICE
cWatch Core For Comodo One FREE 30 days (500 mb/day log volume)	30 days	\$0.00
TOTAL		\$0.00

Back Next >

- Click 'Next' to submit your order. The order summary page is shown afterwards:

Buy New Subscription cWatch

- 1. Login
- 2. Comodo ONE Account
- 3. Configure Subscription
- 4. Customer Information
- 5. Order Confirmation
- 6. Order Summary**

 Congratulations! Your order is completed.

Order #37859163-4

Comodo Security Solutions, Inc.
1255 Broad Street
Clifton, NJ 07013
United States

chennaiwatchsiem
9th Main Road 9th Main Road
Chennai
IN

Subscription Details

PRODUCT NAME	LICENSE KEY
cWatch Core For Comodo One FREE 30 days (500 mb/day log volume)	XXXXXXXXXX-XXXX-XXXX-XXXX-XXXXXX


INVOICE NUMBER	37859163-14	SUBSCRIPTION ID	0585FDC176
----------------	-------------	-----------------	------------

Order Details

Order Number	37859163-4
Order Date	2019-02-06
Order Total	\$0.00
Subscription Expires On	2019-03-09

Product Details

Number of Units	
Unit Price	\$0.00

Print 

- Click 'Finish'

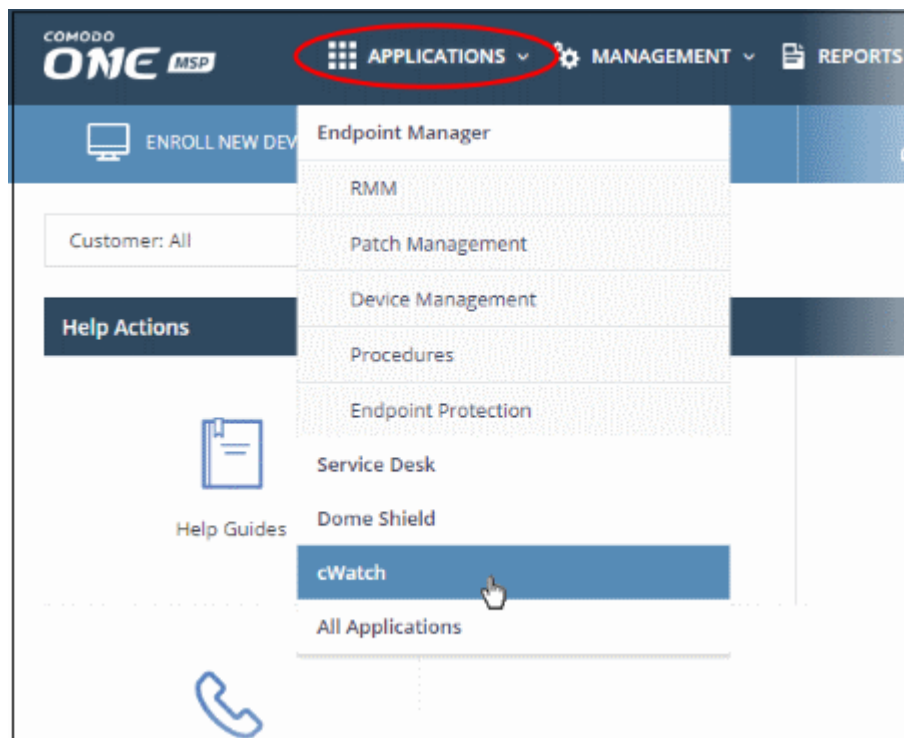
After the purchase is complete, cWatch will appear in the 'Applications' interface.

1.2 Log-in to the Admin Console

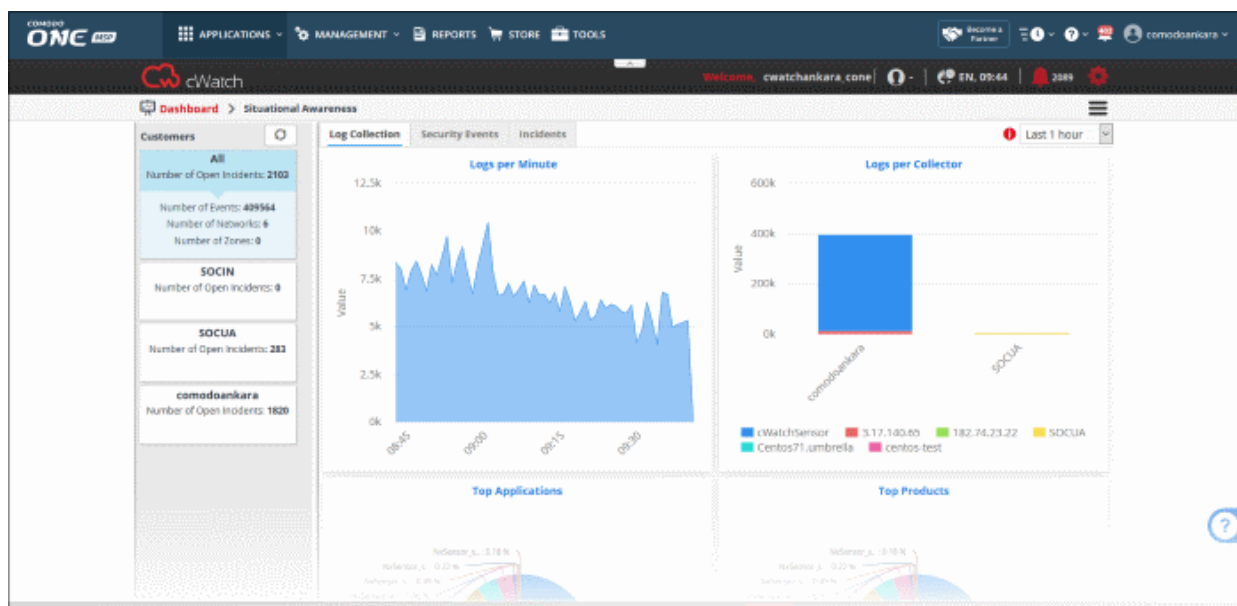
You can open the cWatch Network admin interface after logging-in to your Comodo One / Comodo Dragon / ITarian account.

Access the cWatch Network admin console:

- Login to your **Comodo One / Comodo Dragon / ITarian** account
- Click 'Applications' then 'cWatch'

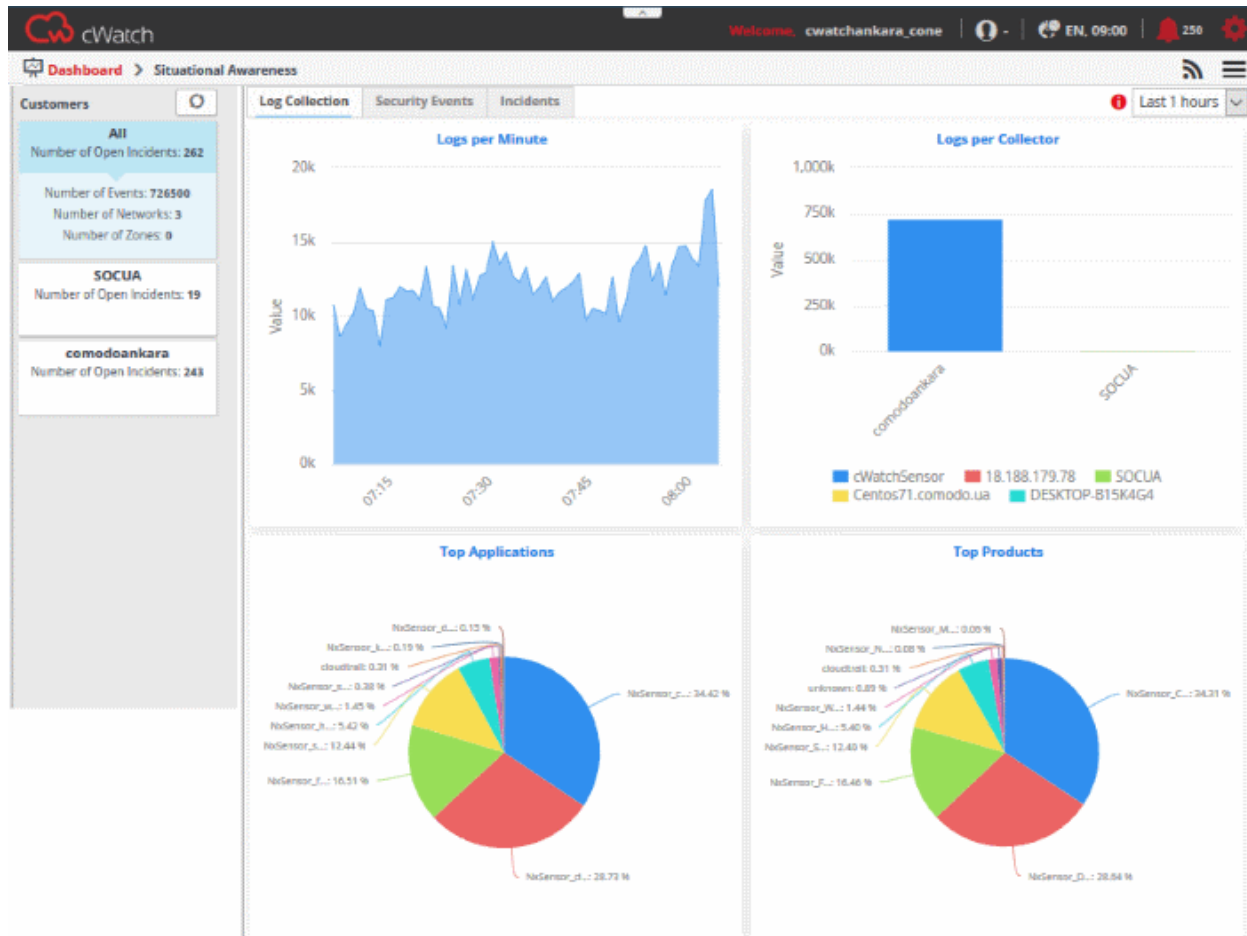


The cWatch admin console will open at the dashboard:





1.3 The Main Interface

The admin console is the nerve center of cWatch, allowing you to enroll networks/endpoints, create log collection policies and more. The dashboard contains at-a-glance statistics about your protected network.



- The title bar shows your username, region, language and the number of alerts you have. The options icon on the right lets you change profile settings and password.


Title Bar Controls - Descriptions	
	The username of the currently logged-in admin
	The name of the selected default customer. See ' Change Region and Default Customer ' for more details.
	The location, language and time zone settings as per the currently logged-in admin.
	The number of incidents detected. Click on the notification icon to open the incident management interface. The interface shows a list of incidents from all customers and lets you reassign them. See Incidents for more details.

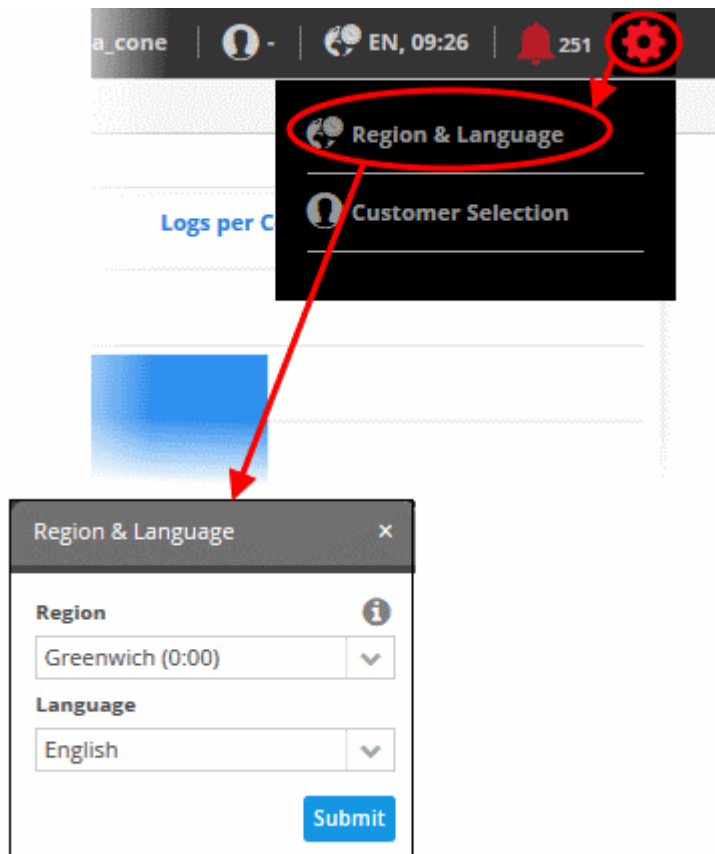
	<p>Allows the currently logged-in administrator to edit their location, language and set default customer. See 'Change Region and Default Customer' for more details.</p>
	<p>Navigational Menu button - Clicking this button allows administrators to navigate to the required main functional areas of the console: Dashboard, Assets, Investigation, Rules, Incidents, Live Lists, Reporting and Administration.</p>

Main Functional Areas

- **Dashboard** -A graphical summary of all events, top detected applications, attack sources, firewall event sources and more. See '**The Dashboard**' for more details.
- **Assets** - Add and manage networks for the customers, configure Nxlog and syslog servers and more. See '**Customer Asset Management**' for more details.
- **Investigation** - Create event queries and view the results in pie charts, bar charts and spider charts. See '**Query Management**' for more details.
- **Rules** - Create rules to analyze logs and provide alerts for certain conditions. See '**Managing Rules**' for more details.
- **Incidents** - Manage correlated and default incidents, assign/reassign incidents to users and more. See '**Incidents**' for more details.
- **Lists** - Create values that can be inserted into form fields when creating event queries and correlation rules. For a example, a list might be used to populate the suggestions in a drop-down menu. See **Lists** for more details.
- **Reporting** - Generate customer specific reports. Reports are available for different kinds of events such as login failures and successes, suspicious login attempts and more. See '**Managing Reports**' for more details.
- **Administration** – Download log collection utilities in order to deploy them on Windows and Linux servers. See '**Administration**' for more details.

Change Region and Default Customer

- Click the user setting button  and choose 'Region & Language' from the drop-down.



The 'Region and Language' dialog will appear.

- Choose the region and time zone to be followed from the 'Region' drop-down.
- Choose the language in which the cWatch Network web console is to be displayed from the 'Language' drop-down.
- Click the 'Submit' button.


A confirmation message will displayed.

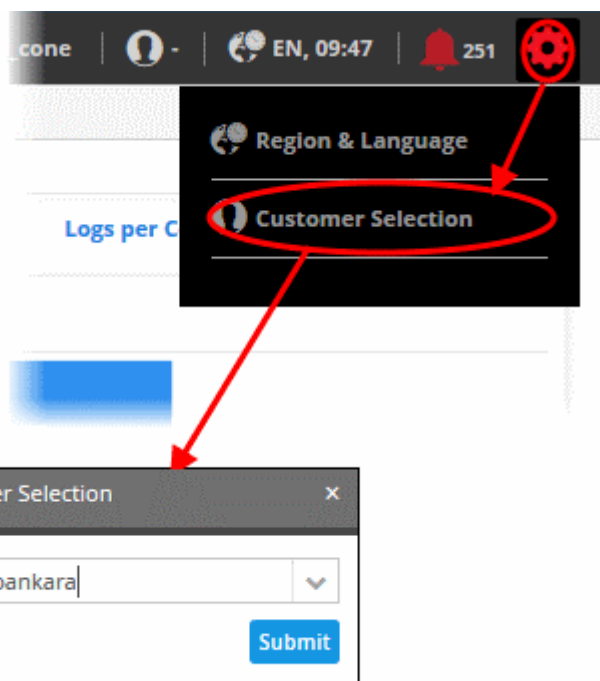
Region And Language changed successfully. Please login to portal again.

The settings will be changed and will take effect from your next login.

Customer Selection

- After logging in, by default, the dashboard will show statistics for all customers.
- You can configure cWatch to display statistics for a particular customer throughout the logged-in session. For example, if you navigate to different screens and return to dashboard, the statistics for the selected customer will be shown.
- Note – This setting is valid only for the session.

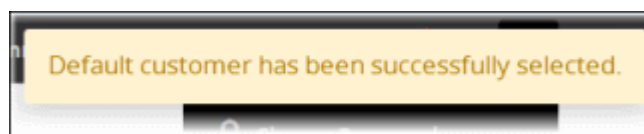
- Click the user setting button  and choose 'Customer Selection' from the drop-down.



The 'Customer Selection' dialog will appear.

- Choose the customer the drop-down.
- Click the 'Submit' button.

A confirmation message will displayed.



Support

At the bottom of the interface, clicking the 'Help' and 'Tutorials', opens the respective support pages.

- Help - Opens Comodo cWatch Network online help guide at <https://help.comodo.com>
- Tutorials - Opens the tutorials page that contains instructions and videos for some important tasks.

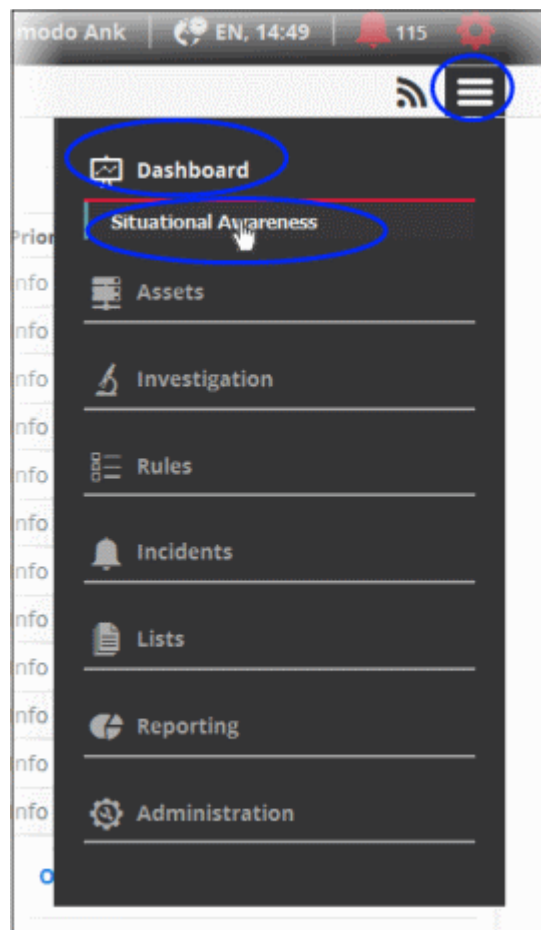
2 The Dashboard

- The dashboard shows a summary of collected logs, events and incidents detected on customer networks over a selected period of time. This allows admins to more effectively track customer progress, diagnose potential issues and to make informed decisions should corrective actions need to be taken.
- The default view shows details collected for all enrolled customers. You view statistics for a particular customer by clicking 'Settings' > 'Customer Selection'. You can also filter statistics by customer by choosing a customer on the left.

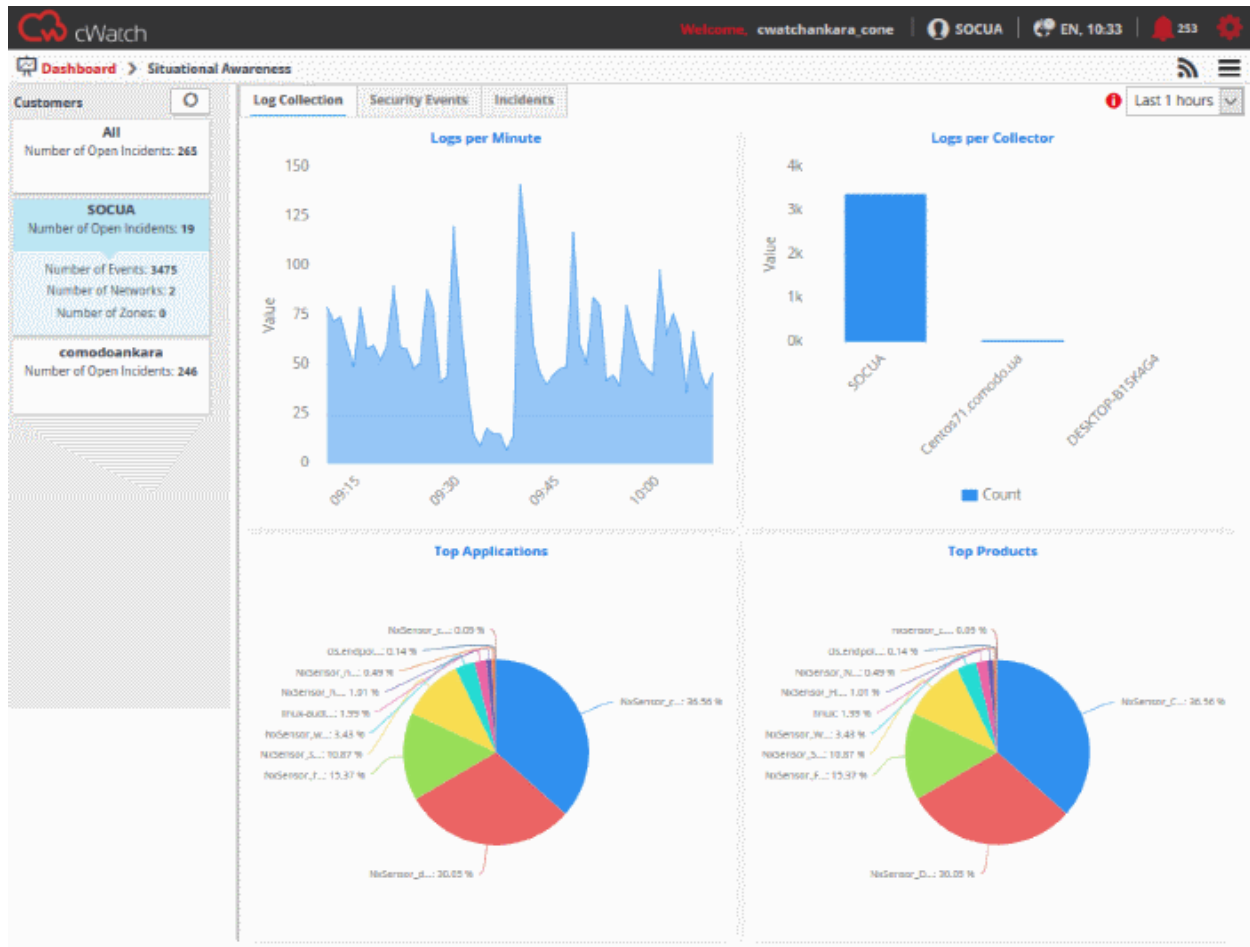
The 'Situational Awareness' dashboard contains three tabs, 'Log Collection', 'Security Events' and 'Incidents'.

- **Log Collection** - Displays graphical summaries of logs collected from different networks.
- **Security Events** - The 'Security Events' tab provides critical information such as top 10 attack sources, top 10 attack destinations, top 10 firewall event sources and number of firewall events happened per minute.
- **Incidents** - The 'Incidents' tab provides details such as incident list, top 10 alerts, open incidents and unassigned incidents.

The 'Situational Awareness' dashboard is shown by default whenever you log-in to cWatch. You can reach the interface at any time by clicking 'Menu' > 'Dashboard' > 'Situational Awareness':



By default, the statistics for all customers will be displayed after logging-in.



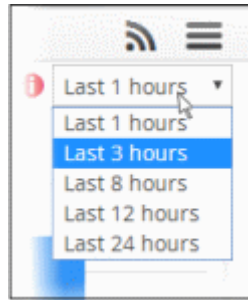
Selecting Customer and Time Period

The left hand menu displays a list of all enrolled customers along with details such as the number of events, number of open incidents, number of networks, number of zones and number of agents for each customer. The top item in the list displays a consolidated summary of details from all the customers.



- To view the charts with details from all the customers on the dashboard, select 'All' from the list
- To view the charts pertaining to a selected customer on the dashboard, select the customer from the list
- To update the list of customers and number of events, click the refresh button at the top

The drop-down at top left allows you to choose the time period for which the statistics should be displayed. You can choose from the past hour up to the past 24 hours.



Tip: You can also create custom dashboards to show data tailored to your requirements. Custom dashboards let you view complex queries in easy-to-understand charts. This allows you to effectively track, monitor and analyze customer activity. See '[Configuring Custom Dashboards](#)' for more details.

Following sections explain more on:

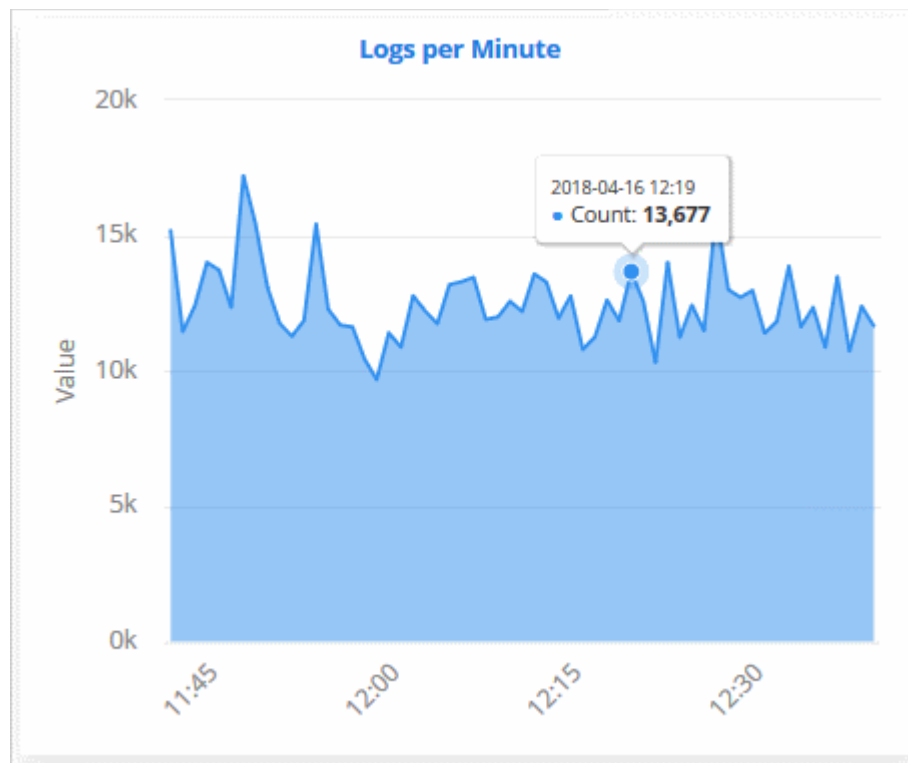
- [Log Collection Charts](#)
- [Security Events Charts](#)
- [Incidents Charts](#)

Log Collection Charts

The 'Log Collection' tab displays statistics of logs collected from the selected customer networks as four charts, 'Logs per Minute', 'Logs per Collector', 'Top Applications' and 'Top Products'. Comodo cWatch Network gathers logs from various systems, tools and devices so that the data may be searched, correlated and used to create reports.

Logs per Minute

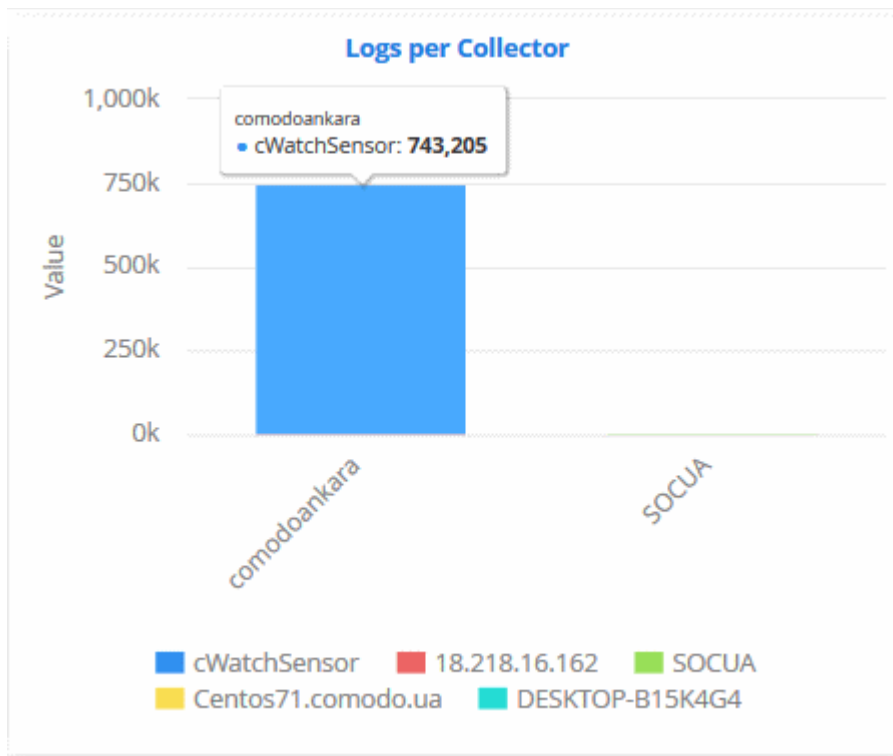
The chart shows the number of logs collected from various sources in selected customer network at different time points.



Placing the mouse cursor on the graph shows the exact number of logs collected at that time point as a tool tip.

Logs per Collector

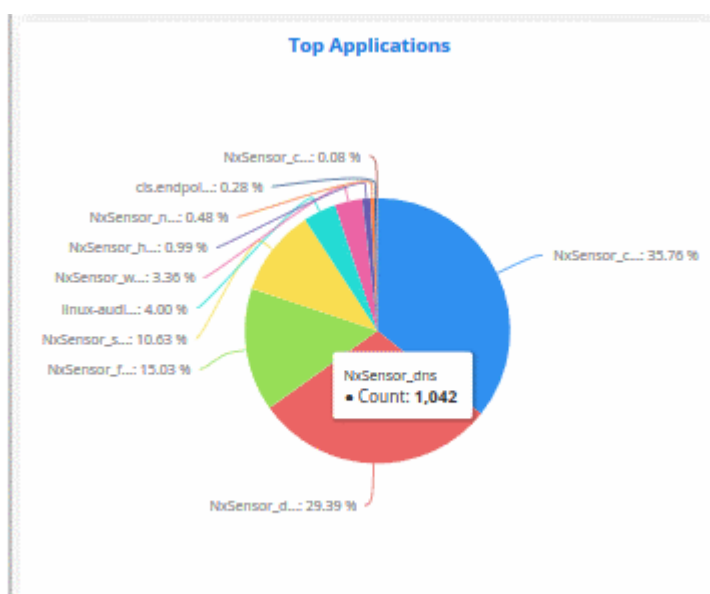
The 'Logs per Collector' chart shows the number of log entries collected from different agents/networks pertaining to the selected customer's networks.



Placing the mouse cursor on a bar shows the exact number of the log entries collected from the respective agent as a tool tip.

Top Applications

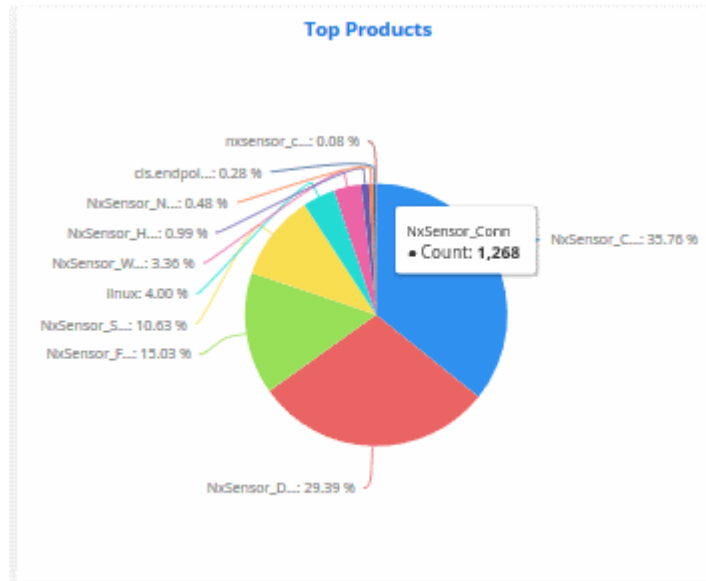
The 'Top Applications' pie-chart shows the percentage breakup of number of log entries received from events generated by various applications running in the customer's network.



Placing the mouse cursor on a sector shows the exact number of the log entries collected from the respective application as a tool tip.

Top Products

The 'Top Products' pie-chart shows the percentage breakup of number of log entries of events generated by network appliances and firewalls connected to the customer's network.



Placing the mouse cursor on a sector shows the exact number of the log entries collected from the respective product, as a tool tip.

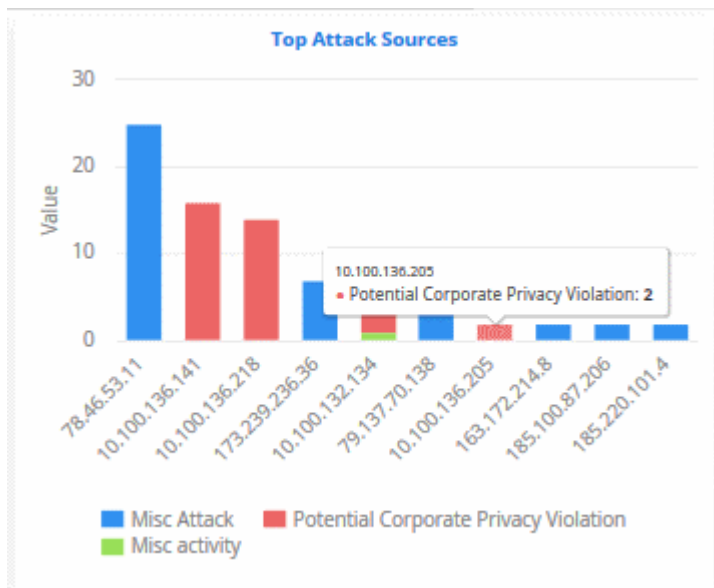
Security Events

The 'Security Events' tab in the dashboard displays summaries of events detected from the customer networks as four graphs, 'Top Attack Sources', 'Top Attack Destinations', 'Top Firewall Event Sources' and 'Firewall Events Per Minute'. Comodo cWatch Network gathers logs from various systems, tools and devices so that the data may be searched, correlated and used to create these reports. The data is then analyzed automatically and graphs are displayed accordingly.

Top Attack Sources

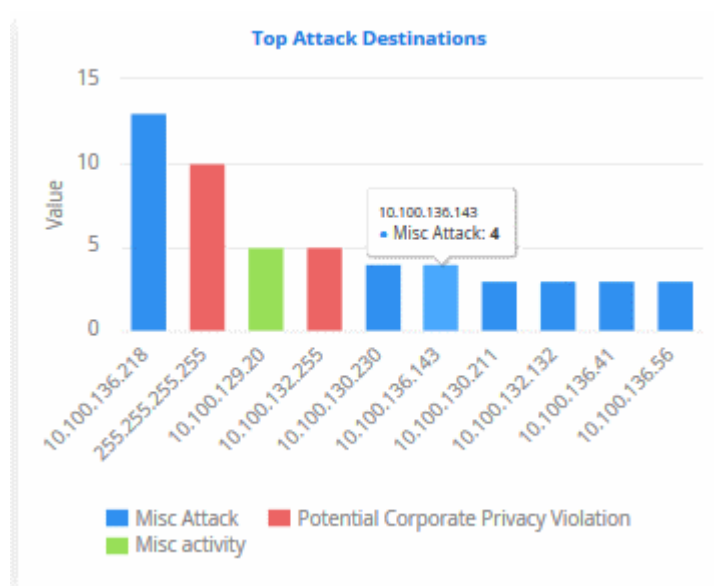
The addresses from which most attacks originated, and the type of attack.

- Addresses are shown on the X-axis. Quantity of attacks are shown on the Y-axis. Attack types are color-coded and listed in the legend below the chart.
- Place your mouse cursor over an event to view attack details.
- You can hide/view a bar by clicking its name in the legend. The colored box beside an event name will be black if the bar graph for it is hidden.



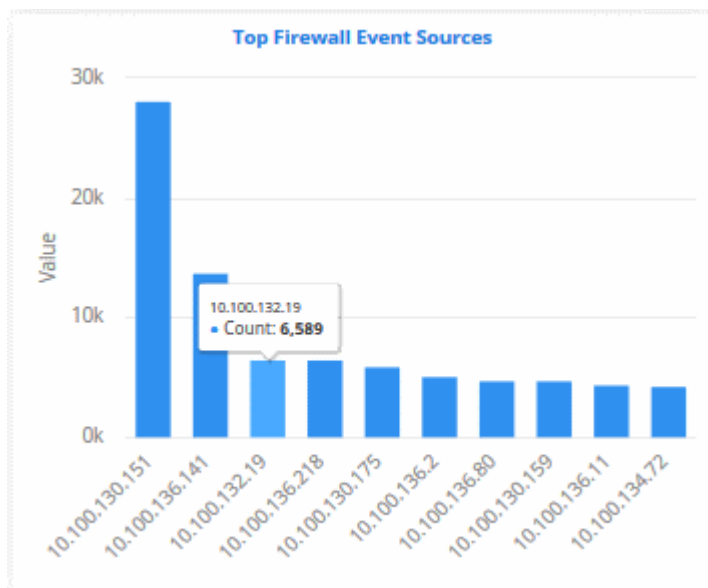
Top Attack Destinations

- The systems that are most affected by the attacks
- Addresses are shown on the X axis. Quantity of attacks are shown on the Y axis.
- Place your mouse cursor over an event to view attack details. The colored box beside the event name will be black if the bar graph for it is hidden.



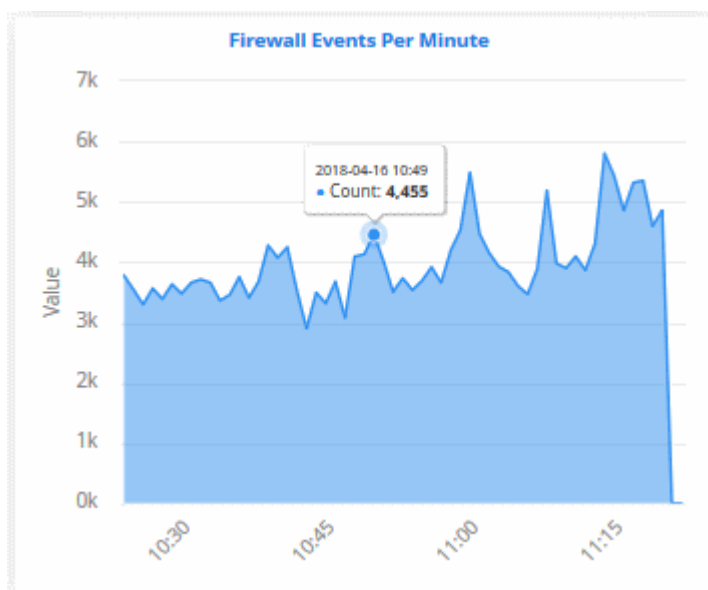
Top Firewall Event Sources

- The endpoints that are most affected by firewall attacks.
- IP addresses of systems from where the firewall events originated are shown on the X axis. Quantity of attack events are shown on the Y axis.
- Place your mouse cursor over an event to view attack details. The colored box beside the event name will be black if the bar graph for it is hidden.



Firewall Events Per Minute

- The bar graph provides occurrence of firewall events per minute.
- For example, admins can get the time when the greatest number of firewall events occurs for a customer or if no events are coming from a customer, it may indicate malfunctioning communications with the agent or issue with log forwarding.
- Place your mouse cursor on a point in the graph to see more event details.



Incidents

- cWatch generates alerts based on rules that defined in the 'Correlation Rules Management' interface
- These alerts are automatically assigned as incidents to the user responsible for the customer. See '[Administration](#)' for more about assigning admins to customers.
- Alerts that are assigned to users are called 'Incidents'. Incidents that are not closed are called 'Open Incidents'.
- Alerts that are not assigned are called 'Unassigned Incidents'.
- You can also add incidents manually in the '[Incidents](#)' screen and assign them to users.
- See '[Managing Incidents](#)' to learn more about incidents.

Log Collection
Security Events
Incidents

Incident List (Total Count: 270)

Date	Name	Object	Subject	Category	Priority	Username
2018-04-16 10:42:32	Blacklisted Communication EXT to INT	104...	10.10...	UNUSUAL NETWORK TRAFFIC	Medium	cwatchankara_c
2018-04-16 10:20:40	DNS Query to a *.top domain	10.1...	10.10...	DNS REQUEST ANOMALIES	Medium	cwatchankara_c
2018-04-16 10:20:40	DNS Query to a *.top domain	10.1...	192.1...	DNS REQUEST ANOMALIES	Medium	cwatchankara_c
2018-04-16 09:18:31	Blacklisted Communication EXT to INT	185...	10.10...	UNUSUAL NETWORK TRAFFIC	Medium	cwatchankara_c
2018-04-16 07:45:33	SCAN Behavioral on Unusual Ports	10.1...	10.10...	UNUSUAL NETWORK TRAFFIC	High	cwatchankara_c
2018-04-16 07:27:33	Blacklisted Communication INT to EXT	10.1...	162.2...	UNUSUAL NETWORK TRAFFIC	Medium	cwatchankara_c
2018-04-16 07:06:31	False Auth SSH Conn	10.1...	10.10...	AUTHENTICATION ANOMALIES	High	cwatchankara_c
2018-04-16 06:45:32	eMule KAD Network Connection Request	10.1...	157.5...	UNUSUAL NETWORK TRAFFIC	Medium	cwatchankara_c
2018-04-16 06:45:31	P2P Application(s) Activity	10.1...		UNUSUAL NETWORK TRAFFIC	Medium	cwatchankara_c
2018-04-16 05:54:32	CHAT Related Events	10.1...	64.23...	UNUSUAL NETWORK TRAFFIC	Info	cwatchankara_c
2018-04-16 05:24:32	Win.Trojan.Generic-6454615-0	10.1...	8.8.8.8	MALWARE ACTIVITY	High	cwatchankara_c

Top 10 Alerts

Alert Category	Percentage
New NvIDS	30.27 %
P2P Octosh	10.81 %
Potential	14.05 %
SCAN Behav	9.73 %
DNS Query	8.65 %
eMule KAD	7.03 %
P2P Applic	6.49 %
DYNAMIC DN	5.41 %
Possible T	3.78 %
Blackliste	3.78 %

Open Incidents

User	LOW	MEDIUM	HIGH	INFO	CRITICAL
cwatchankara_cone	~10	~10	~10	~10	~10
Unassigned	0	0	0	0	~50

Incident List

The 'Incident List' table at the top displays a list of events with details like name, description and so on.

Incident List (Total Count: 270)

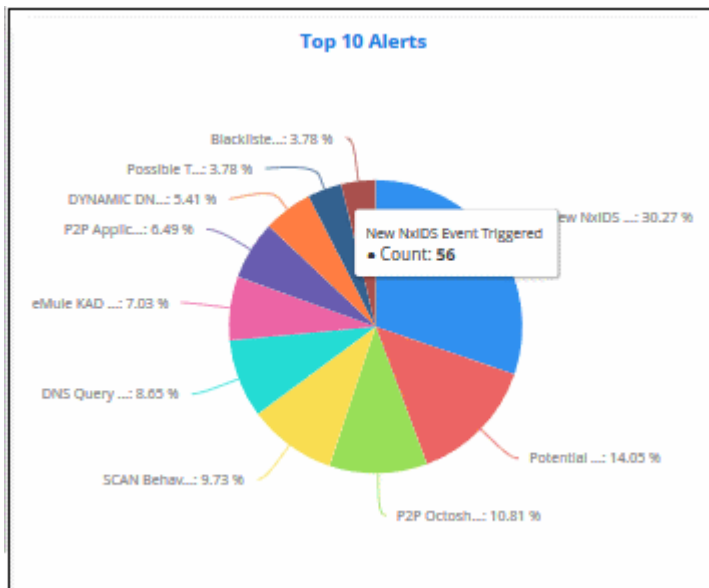
Date	Name	Object	Subject	Category	Priority	Username
2018-04-16 10:42:32	Blacklisted Communication EXT to INT	104...	10.10...	UNUSUAL NETWORK TRAFFIC	Medium	cwatchankara_c
2018-04-16 10:20:40	DNS Query to a *.top domain	10.1...	10.10...	DNS REQUEST ANOMALIES	Medium	cwatchankara_c
2018-04-16 10:20:40	DNS Query to a *.top domain	10.1...	192.1...	DNS REQUEST ANOMALIES	Medium	cwatchankara_c
2018-04-16 09:18:31	Blacklisted Communication EXT to INT	185...	10.10...	UNUSUAL NETWORK TRAFFIC	Medium	cwatchankara_c
2018-04-16 07:45:33	SCAN Behavioral on Unusual Ports	10.1...	10.10...	UNUSUAL NETWORK TRAFFIC	High	cwatchankara_c
2018-04-16 07:27:33	Blacklisted Communication INT to EXT	10.1...	162.2...	UNUSUAL NETWORK TRAFFIC	Medium	cwatchankara_c
2018-04-16 07:06:31	False Auth SSH Conn	10.1...	10.10...	AUTHENTICATION ANOMALIES	High	cwatchankara_c
2018-04-16 06:45:32	eMule KAD Network Connection Request	10.1...	157.5...	UNUSUAL NETWORK TRAFFIC	Medium	cwatchankara_c
2018-04-16 06:45:31	P2P Application(s) Activity	10.1...		UNUSUAL NETWORK TRAFFIC	Medium	cwatchankara_c
2018-04-16 05:54:32	CHAT Related Events	10.1...	64.23...	UNUSUAL NETWORK TRAFFIC	Info	cwatchankara_c
2018-04-16 05:24:32	Win.Trojan.Generic-6454615-0	10.1...	8.8.8.8	MALWARE ACTIVITY	High	cwatchankara_c

Incident List - Table of Column Descriptions	
Column Header	Description
Date	Date and time of the incident
Name	The rule that captured the event
Object	The source IP of the assets
Subject	The destination IP of the host
Category	The incident type. For example, 'Malware activity' or 'Unusual network Traffic'
Customer	Name of the affected customer
Username	The administrator to whom the incident is assigned
Priority	The severity of the event. Event priority can be specified in the 'Rule Creation' screen and in the 'Add Incident' screen.
Status	Shows whether the incident is 'Open', 'In-Progress', 'False Positive' or 'Closed'.
Type	Whether the event was automatically or manually generated. Automatic events are called 'Correlated'. Manual events are called 'Default'.
Summary	A short description of the incident. This description is provided when creating or editing the rule.
Trigger Count	The number of times the incident has occurred
Last Trigger Date	Time and date that the rule was most recently breached.
Identity	Internal id of the incident.
Report	Whether the report for the selected incident is generated or not

You can sort the column items alphabetically/ascending or descending by clicking on the column header.

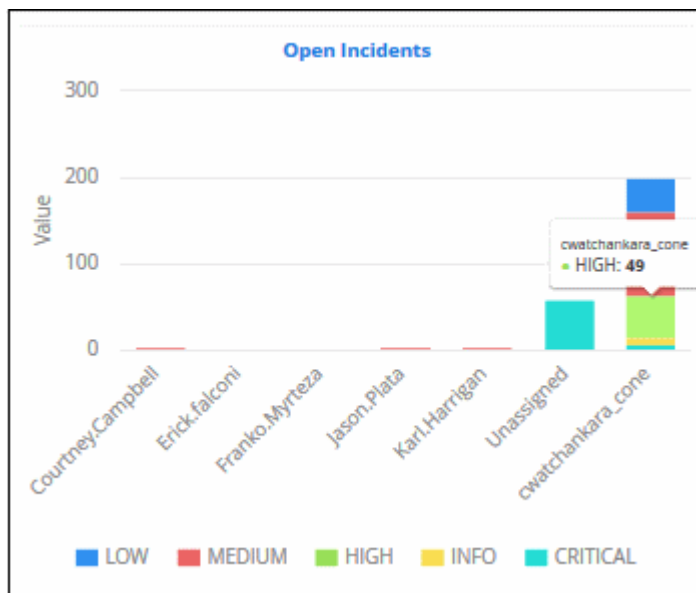
Top 10 Alerts

- Shows the 10 rules which generated the most alerts
- Place your mouse cursor over a chart slice to view more details.



Open Incidents

- Shows unresolved incidents by assignee.
- Assignees are shown on the X axis. Quantity of attacks are shown on the Y axis.
- Place your mouse cursor over a bar to view the number of incidents, the severity of the incident and the user assigned.
- You can hide/view a graph bar by clicking the legend items
- The colored box beside the priority will be black if the bar graph for it is hidden. Click on it again to display the bar graph.

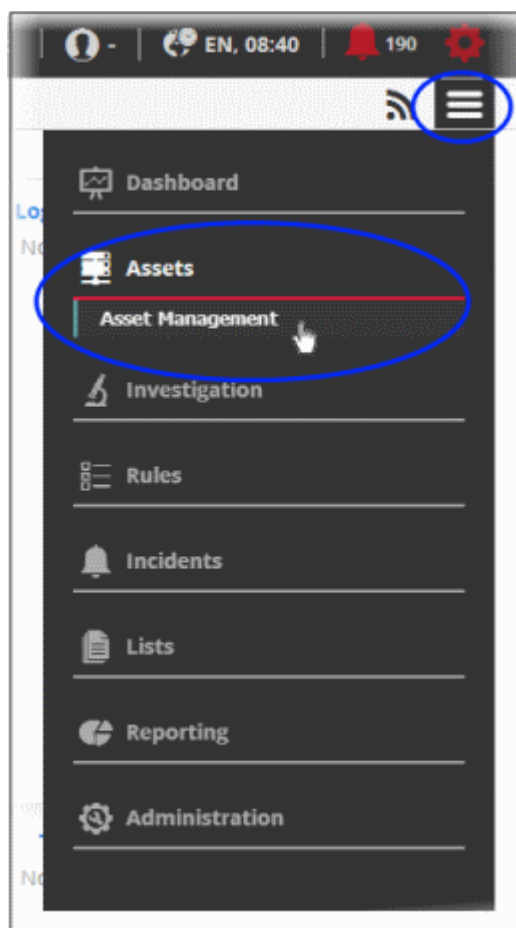


3 Customer Asset Management

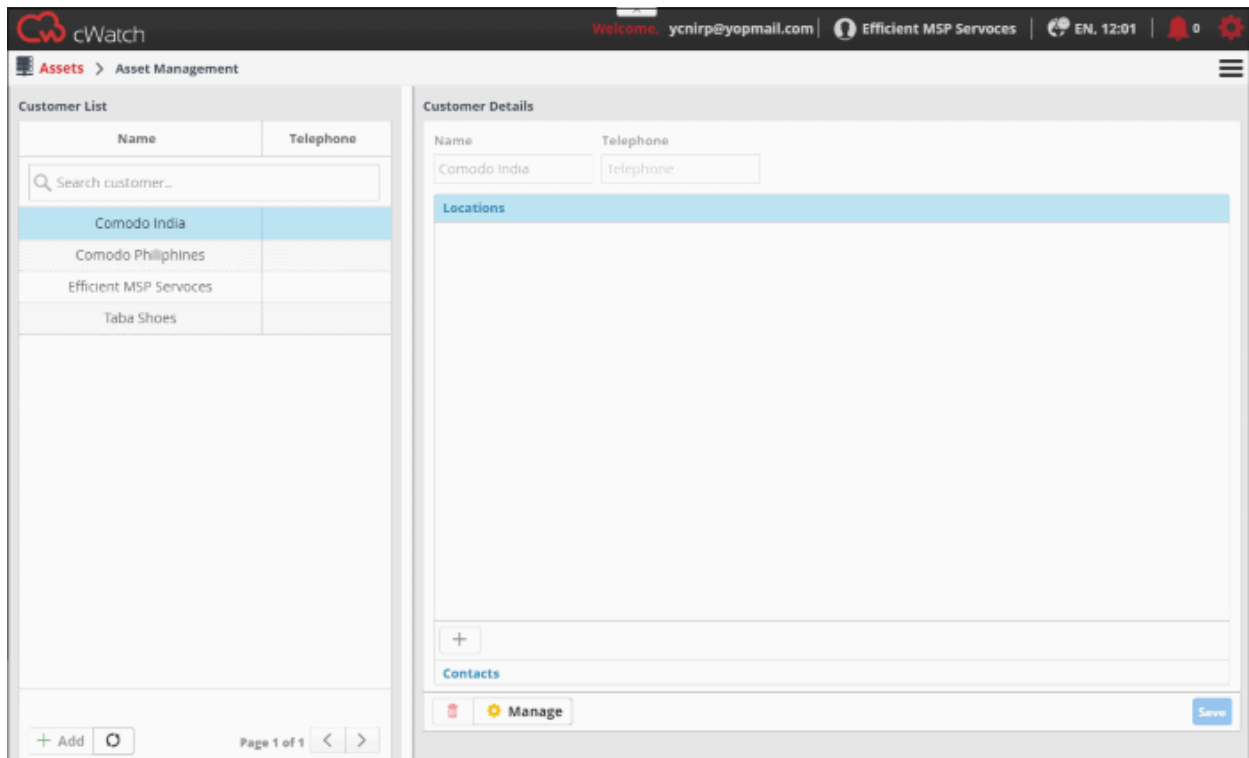
The asset management area lets you manage customer endpoints and networks.

To open the 'Asset Management' interface:

- Click the 'Menu' button at top-right
- Choose 'Assets' and click 'Asset Management'.



The 'Asset Management' interface lists customers on the left and customer details on the right:



The following sections explain how to manage customers, customer assets and configure customer network to send logs to cWatch.

- **Add New Customers**
- **Add Assets for Monitoring**
- **Configure Nxlog and Rsyslog to Send Logs to cWatch Network Server**
- **Edit Customers**

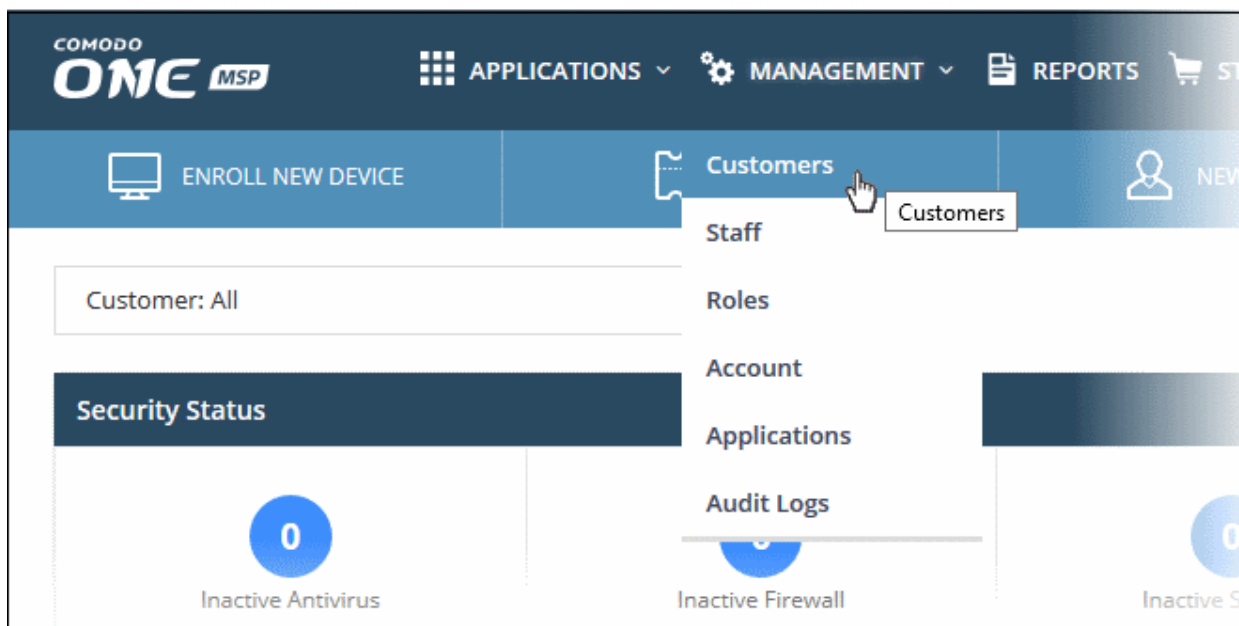
3.1 Add Customers

- To monitor customer networks, you first need to add a customer then provide details of their networks and other assets.
- Once a customer is added, a 'Network Activation Key' and 'Token' will be generated for them.
- This token, which is configured in the log config file, is used by cWatch to identify the web-server or network.
 - See '**Configure NxLog and Rsyslog to Send Logs to cWatch Network Server**' for more details.

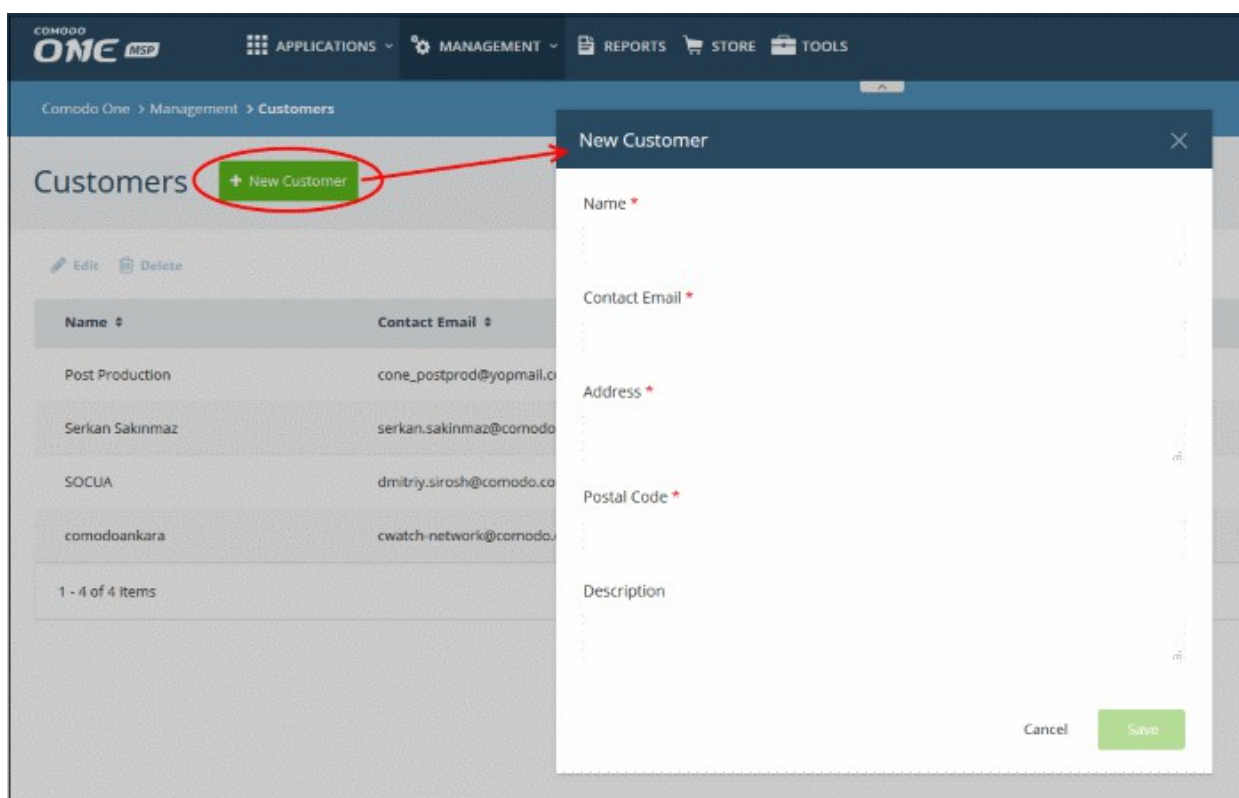
Add a new customer

Customers added to your Comodo One / Comodo Dragon / ITarian account are automatically added to cWatch.

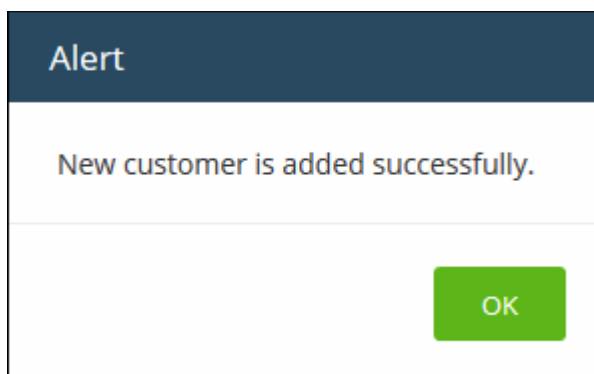
- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** MSP account
- Click 'Management' then 'Customers'



- Click the 'New Customer' button:

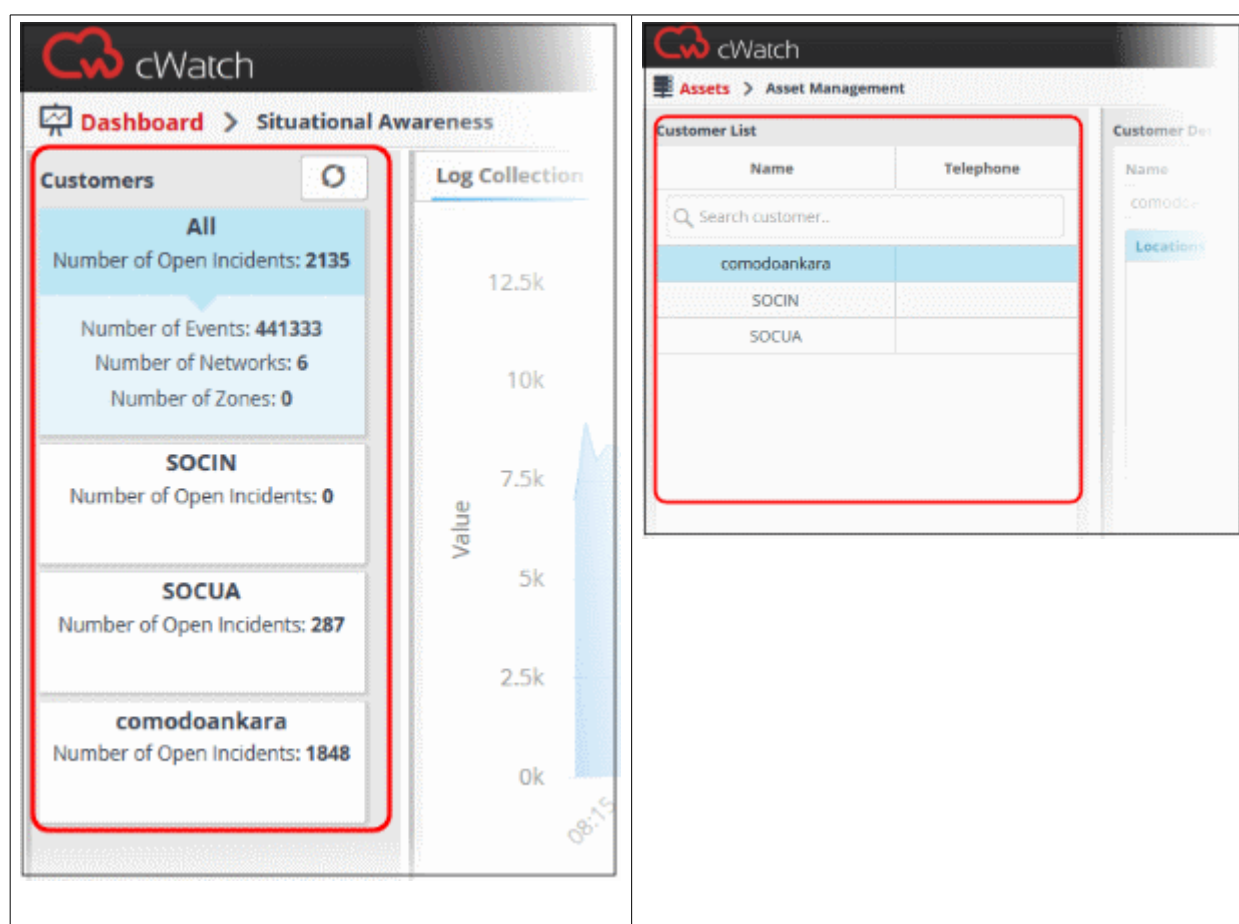


- Complete each field on the form then click 'Save' to add the customer.
- Click 'OK' in the confirmation dialog:



- Repeat the process to add more customers.

In the cWatch interface, you can view the customers in the dashboard and asset management screens.



- The next step is to:
 - Add assets to cWatch Network for monitoring
 - Download Nxlog and Rsyslog config files to deploy on networks

See '[Add Assets for Monitoring](#)' and '[Configure Nxlog and Rsyslog to Send Logs to cWatch Network Server](#)' for more details.

3.2 Add Assets for Monitoring

You need to add customer assets to cWatch Network in order to collect logs and monitor events. Administrators should enroll the web-servers, endpoints and software assets (such as services) that they wish to monitor.

To add assets for a customer

- Open the 'Asset Management' interface by clicking the 'Menu' button, then 'Assets' > 'Asset Management'.
- Select the customer whose assets are to be added, from the left hand side pane.

The Customer Details pane will open in the right.

- Click 'Manage' at the bottom left of the right pane

Customer Details

Name: Chennai Techwriting Telephone: 9445175813

Locations

USA
New Jersey

+ Add Location

Contacts

Manage (gear icon)

Save

Hard Assets | Soft Assets

Assets	Action
Team 1	🔍 ✎ 🗑️ +

← + Network

Team 1 Token:
a06517578ea9497db871ed8da4dc7f90

Team 1 Activation key:
developmentank|CUST0f87f107b3c1450cbc5a4bb95a641a6e|578dc04ef98e45c0b8717c565a04dbaa

↓ Nxlog ↓ Rsyslog

The interface for adding customer's assets will open. It contains two tabs:

- **Hard Assets** - Allows you to add networks and zones to be monitored by entering their start and end IP addresses. See **Hard Assets** for more details.
- **Soft Assets** - Allows you to add soft assets like services hosted from the network by specifying their URL, website and so on. See **Soft Assets** for more details.

3.2.1 Hard Assets

The 'Hard Assets' interface allows you to add and manage networks for enrolled customers. You can add several networks for each customer by specifying their start and end addresses. Each network can be divided into zones depending on organizational requirements.

For each network or zone defined for a customer:

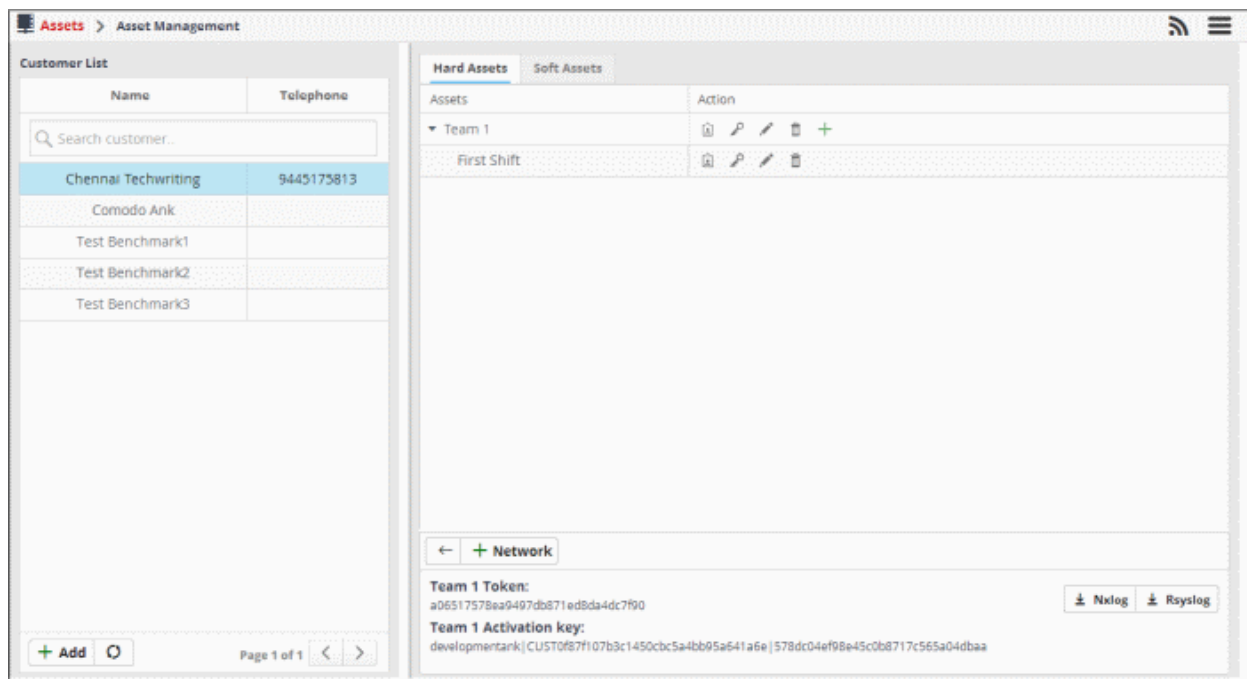
- A unique authentication token is generated. The authentication token can be used as 'AGENTLESS_AUTH_TOKEN' parameter on the configuration script that can be run on Linux and Windows endpoints with RSYSLOG and NXLOG utilities, for agent less log collection from them. See '**Configure Nxlog and Rsyslog to Send Logs to cWatch Network Server**' for more details.

To open the Hard Assets interface for a customer





- Open the 'Asset Management' interface by clicking the 'Menu' button, then 'Assets' > 'Asset Management'.
- Select the customer whose assets are to be added, from the left hand side pane.

The Customer Details pane will open in the right.

- Click 'Manage' at the bottom left of the right pane and choose the 'Hard Assets' tab.



The list of networks/zones added for the selected customer is displayed in the right hand side pane with action buttons. The network token and the activation key for the selected network are displayed in the lower right pane.

Hard Assets: Action - Controls	
	Clicking this icon displays the authentication token and download buttons for the pre-configured RSYSLOG and NXLOG configuration script files for the network/zone in the lower right pane.
	Allows you to reset the authentication token for the network/zone and generate new one. Once the token is changed, the old token becomes invalid. The cWatch Network server will not be able to collect logs from RSYSLOG and NXLOG utilities at endpoints with configuration script file containing the old token.
	Allows you to edit the name and IP address range of the network or the zone.
	Allows you to delete the network or zone. Deleting a network also deletes the zones

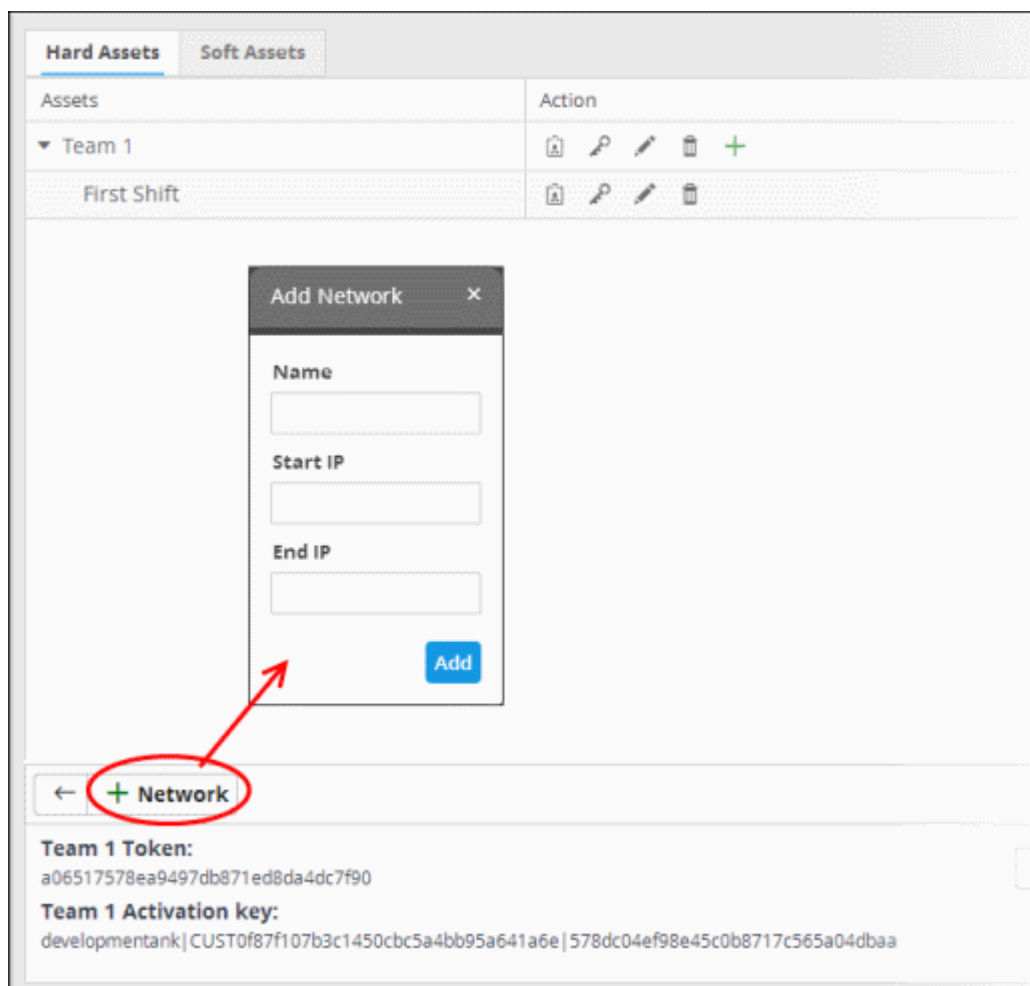
	configured under it.
+	Allows you to add a zone to the network.

The Hard Assets interface allows you to:

- **Add a new Networks and Zones**
- **Edit a network or zone**
- **Delete a network or zone**
- **Get the authentication token and activation key for a network or zone**

To add hard assets for a customer

- Select the customer from the left in the 'Asset Management' interface and click the 'Mange' button on the right pane.
- Click the 'Hard Assets' tab
- Click the 'Network' button at the bottom of the right pane.



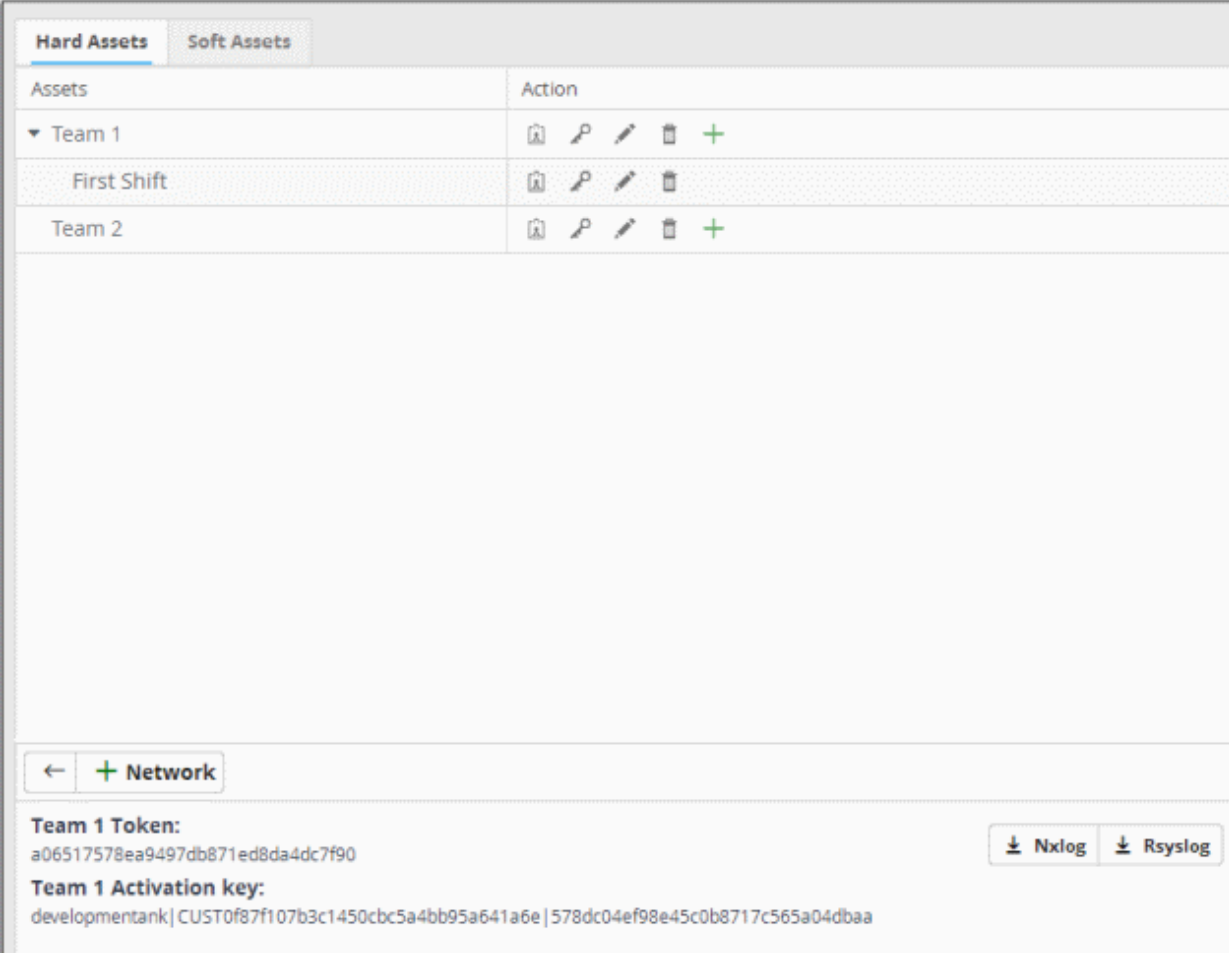
The 'Add Network' dialog will appear.

- **Name** - Enter the name of the network in the field.
- **Start IP** - Enter the start IP address if a range of endpoints are to be added. If a single endpoint is to be added, enter its IP address in both the 'Start IP' and 'End IP' fields.
- **End IP** - Enter the end IP address if a range of endpoints are to be added. If a single endpoint is to be















added, enter its IP address in both the 'Start IP' and 'End IP' fields.

- Click the 'Add' button.

The network will be added and a unique authentication token and agent activation key will be generated for the network. Clicking the  button in the new network row will display the token and the key at the bottom of the right pane.



The screenshot shows the 'Hard Assets' tab in the Comodo cWatch Network Administrator interface. It displays a table of assets and a detailed view for 'Team 1'.

Assets	Action
Team 1	    
First Shift	   
Team 2	    

Below the table, there is a '+ Network' button. The detailed view for 'Team 1' shows the following information:

- Team 1 Token:** a06517578ea9497db871ed8da4dc7f90
- Team 1 Activation key:** developmentank | CUST0f87f107b3c1450cbc5a4bb95a641a6e | 578dc04ef98e45c0b8717c565a04dbaa

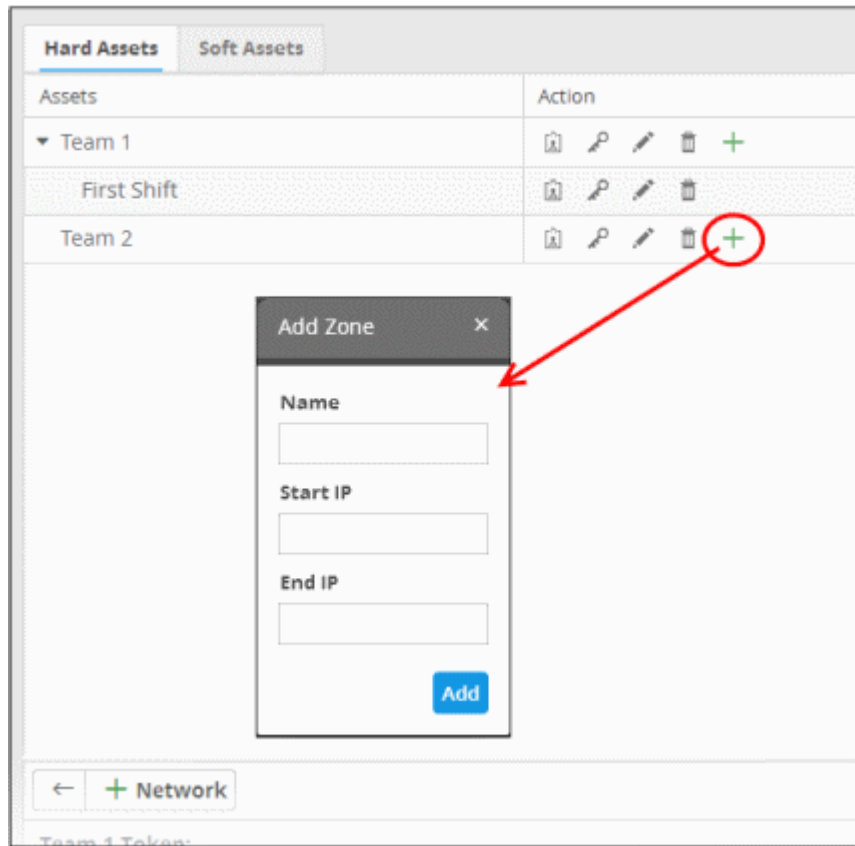
There are also buttons for 'Nxlog' and 'Rsyslog' in the bottom right corner of the detailed view.

- Repeat the process to add more networks.


To add a zone to a network

- Click the  button in the row of the network.


The 'Add Zone' dialog will appear.



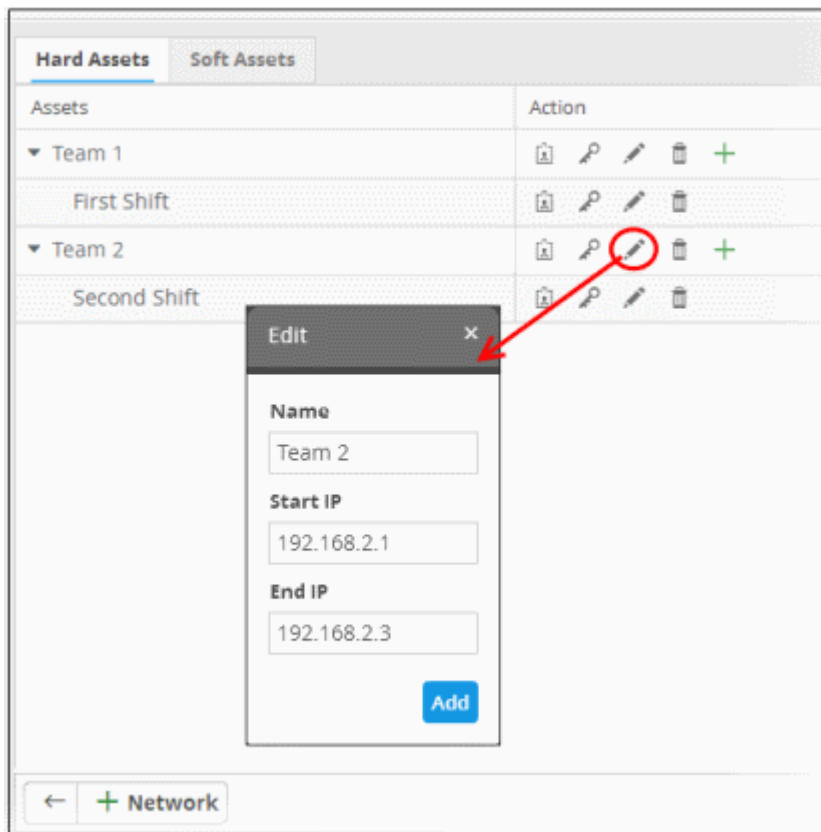
- **Name** - Enter the name of the zone in the field.
- **Start IP** - Enter the start IP address if a range of endpoints are to be added for the zone. If a single endpoint is to be added, enter its IP address in both the 'Start IP' and 'End IP' fields.
- **End IP** - Enter the end IP address if a range of endpoints are to be added for the zone. If a single endpoint is to be added, enter its IP address in both the 'Start IP' and 'End IP' fields.
- Click the 'Add' button.

The Zone will be added to the network and a unique authentication token will be generated for the zone. Clicking the  button in the row of the new zone will display the token and the key at the bottom of the right pane.

To edit a network or a zone

- Click the  button in the row of the network or the zone.

The 'Edit' dialog will appear. The dialog is similar to **Add Network or Add Zone** dialog.

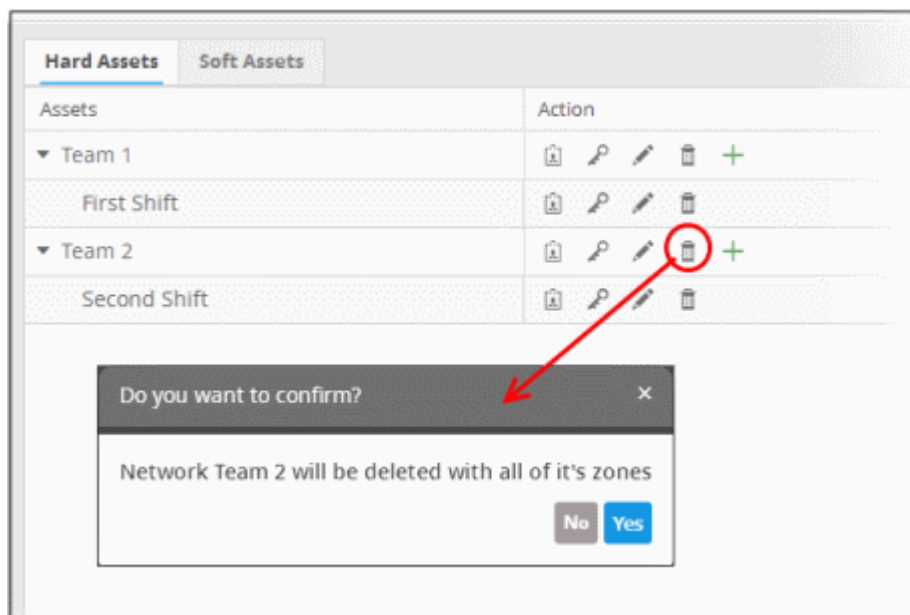


- Edit the details as required and click the 'Add' button.

To delete a network or zone

- Click the  button in the row of the network or the zone.

A confirmation dialog will appear.

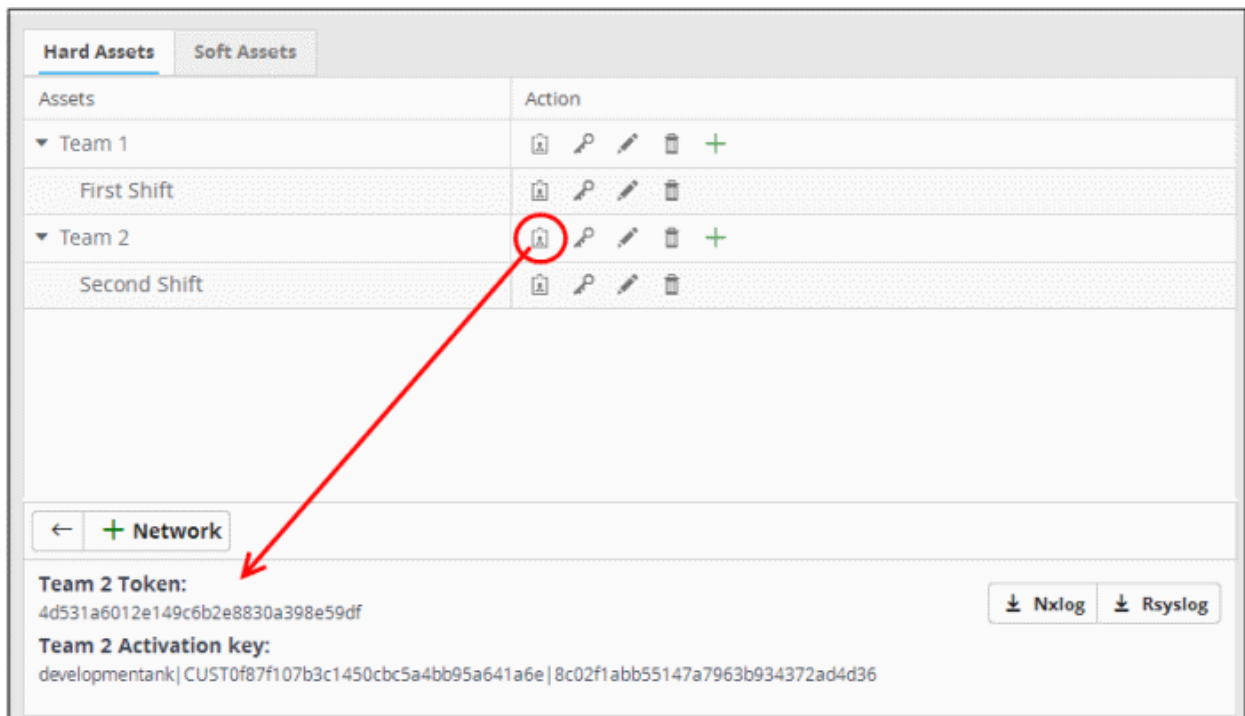


- Click 'Yes' to remove the network or the zone. Please note that if a network is removed, the zones under it will also be removed.

To get the authentication token, activation key and the configuration script files for a network or a zone

- Click the  button in the row of the network or zone.

The authentication token and the agent activation key for the item will be displayed at the bottom of the screen.



- **Authentication token** - The authentication token can be used as 'AGENTLESS_AUTH_TOKEN' parameter on the configuration script that can be run on Linux and Windows endpoints with RSYSLOG and NXLOG utilities, for agent less log collection from them. See '[Configure Nxlog and Rsyslog to Send Logs to cWatch Network Server](#)' for more details.
- **Configuration Script Download Buttons** - The configuration files can be directly run on endpoints with RSYSLOG and NXLOG utilities respectively without any re-configuration, for them to send logs to cWatch Network server. See '[Configure Nxlog and Rsyslog servers to send logs to NxNetwork server](#)' for more details.

3.2.2 Soft Assets

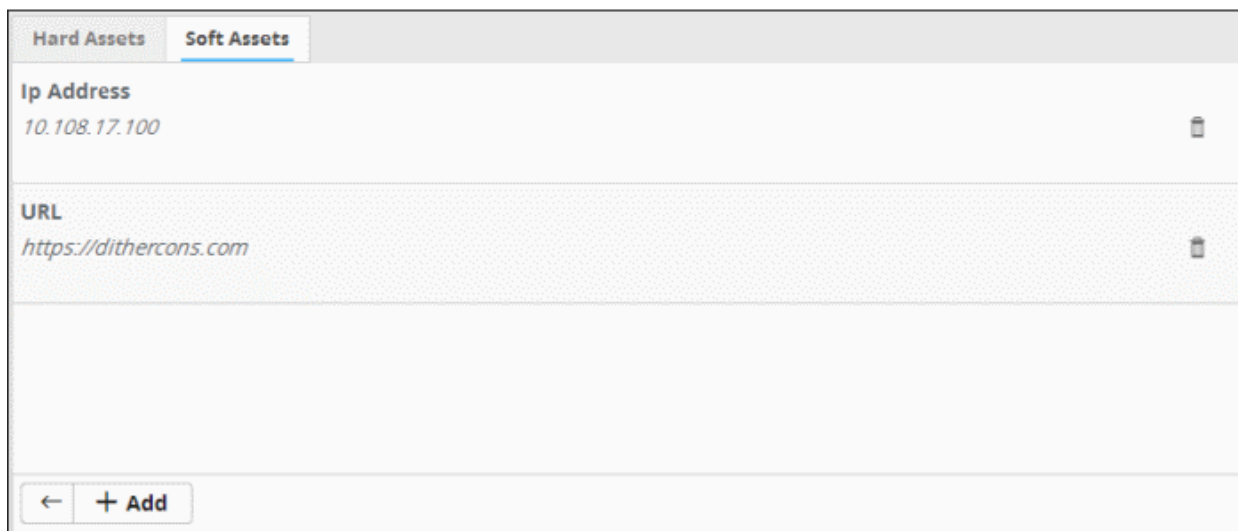
- The 'Soft Assets' interface allows you to create and manage a list of important URLs, domains or IP addresses. The list acts as a reference for operators/administrators/analysts.
- For example, admins can clearly see if an incident has affected one of their important addresses and take appropriate actions.

To open the Soft Assets interface for a customer

- Open the 'Asset Management' interface by clicking the 'Menu' button, then 'Assets' > 'Asset Management'.
- Select the customer whose assets are to be added, from the left hand side pane.

The Customer Details pane will open in the right.

- Click 'Manage' at the bottom left of the right pane and choose the 'Soft Assets' tab.



The list of soft assets added for the customer will be displayed. The Hard Assets interface allows you to:

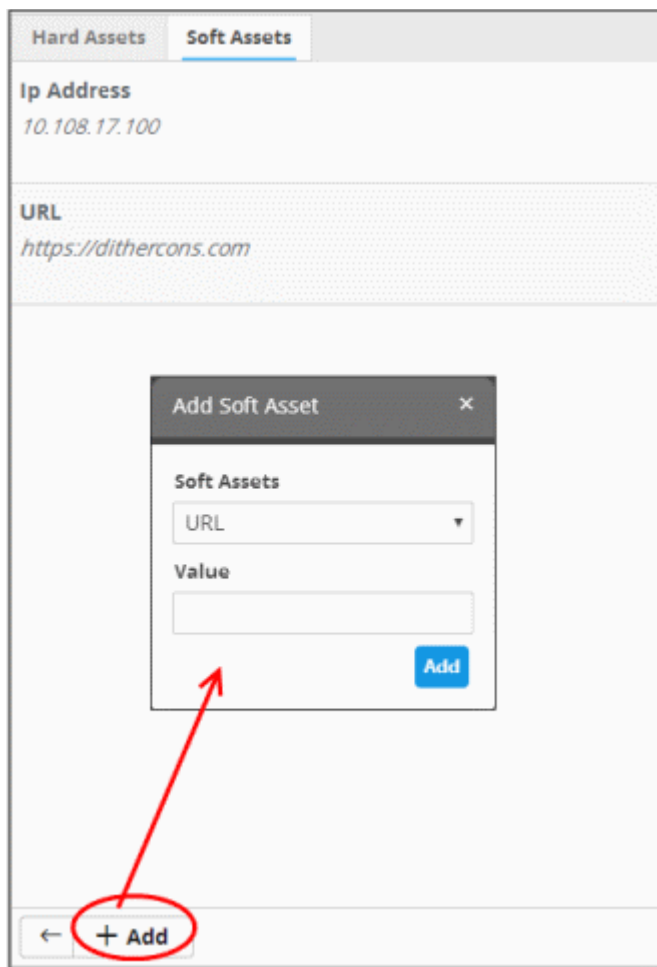
- **Add new Soft Assets**
- **Remove Soft Assets**

To add soft assets for a customer

- Open the 'Asset Management' interface by clicking the 'Menu' button, then 'Assets' > 'Asset Management'.
- Select the customer whose assets are to be added, from the left hand side pane.

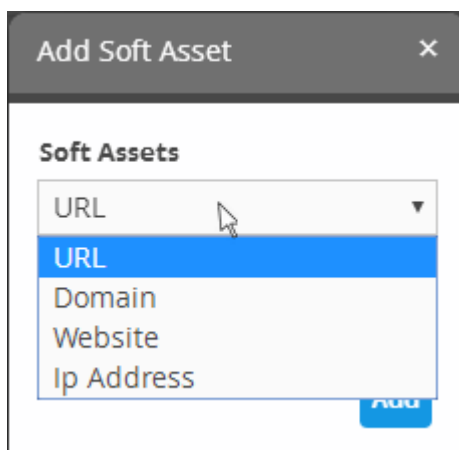
The Customer Details pane will open in the right.

- Click 'Manage' at the bottom left of the right pane and choose the 'Soft Assets' tab.
- Click the 'Add' button from the bottom of the right pane.



The 'Add Soft Asset' dialog will be displayed.

- Choose the type of soft asset that you want to add from the 'Soft Assets' drop-down.



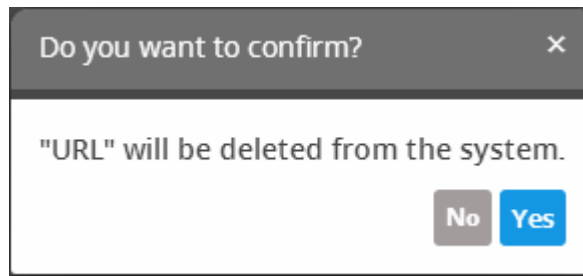
- Enter the value for the selected soft asset in the 'Value' field.
- Click the 'Add' button.

The Soft Asset will be added to the list for the customer.

To remove a soft asset

- Click the  button in the row of the asset.

A confirmation dialog will appear.



- Click 'Yes' to remove the item.

3.3 Configure Nxlog and Rsyslog to Send Logs to cWatch Network Server

- CWatch features agent-less log collection from Windows/Linux endpoints connected to customers' networks.
- This is achieved through the Nxlog and Rsyslog utilities. The NXLOG utility (for Windows) and the RSYSLOG utility (for Linux) need to be configured to send logs to the cWatch Network server.

Comodo cWatch Network provides ready-made configuration script files for each customer's /network/zone which can be downloaded from the respective 'Customer Details' page. Once connected, the cWatch Network will be able to receive and store logs from the customer's endpoints and web-servers.

The following sections explain more about:

- [Configure the NXLOG Utility](#)
- [Configure the RSYSLOG Utility](#)


Configure the NXLOG Utility

Administrators can download a specific customer's NXLOG configuration file from the administrative console and use this to configure the NXLOG utility installed on Windows endpoints and web-servers connected to the customer's network. Please make sure NXLOG utility is installed on the machine which is to be configured to send logs to cWatch.

To download the NXLOG Configuration File

- Open the 'Asset Management' interface by clicking the 'Menu' button, then 'Assets' > 'Asset Management'.
- Select the customer from the left hand side pane.

The 'Customer Details' pane will open at the right.

- Click 'Manage' at the bottom left of the right pane and choose the 'Hard Assets' tab.
- Choose the network/zone you wish to configure from the right hand side pane and click the  button in the row of the network/zone.

The authentication token, the authentication key and the download buttons for the NXLOG and RSYSLOG configuration script files for the selected network/zone will be displayed at the bottom of the right pane.

- Click the NXLOG configuration file download button as shown in the screenshot below and save the file:



- Replace the NXLOG configuration file at the location C:\Program Files (x86)\nxlog\conf\nxlog.conf or C:\Program Files\nxlog\conf\nxlog.conf in the endpoints\webserver with the downloaded configuration file.

All settings in the configuration file including network token for the selected network/zone are pre-configured and will instruct the NXLOG utility to send logs to the cWatch Network server. cWatch will receive and store the logs under the respective customer/network for monitoring and incident reporting.


Configure RSYSLOG Utility

- You can download a pre-configured RSYSLOG config script from the admin console. Each script is generated for a specific customer/network.
- The script will configure RSYSLOG utilities installed on Linux machines to send logs to the cWatch Network.
 - Please make sure the RSYSLOG utility is installed on the target machine.

To download the RSYSLOG Configuration File



















- Open the 'Asset Management' interface by clicking the 'Menu' button, then 'Assets' > 'Asset Management'.
- Select a customer from the left hand pane.

The 'Customer Details' pane will open at the right.

- Click 'Manage' at the bottom left of the right pane and choose the 'Hard Assets' tab.
- Choose the network/zone whose endpoints are to be configured, from the right hand side pane and click the  button in the row of the network/zone.

The authentication token, the authentication key and the download buttons for the NXLOG and RSYSLOG configuration script files for the selected network/zone will be displayed at the bottom of the right pane.



- Click the RSYSLOG configuration file download button as shown below and save the file.

Assets	Action
▼ Team 1	    
First Shift	   
▼ Team 2	    
Second Shift	   

← + Network

Team 1 Token:
a06517578ea9497db871ed8da4dc7f90

Team 1 Activation key:
developmentank|CUST0f87f107b3c1450cbc5a4bb95a641a6e|578dc04ef98e45c0b8717c565a04dbaa

 Nxlog  Rsyslog

- Run the script file on all required endpoints.

The script will configure the RSYSLOG utility to send logs to cWatch Network. cWatch will receive and store the logs under the respective customer/network for monitoring and incident reporting.

Alternatively, you can download the script file for configuring the RSYSLOG utility from 'Administration' > 'Event Collection' interface, manually enter the parameters for the customer network to be monitored and run the script at the endpoints. See **Event Collection** for more details.

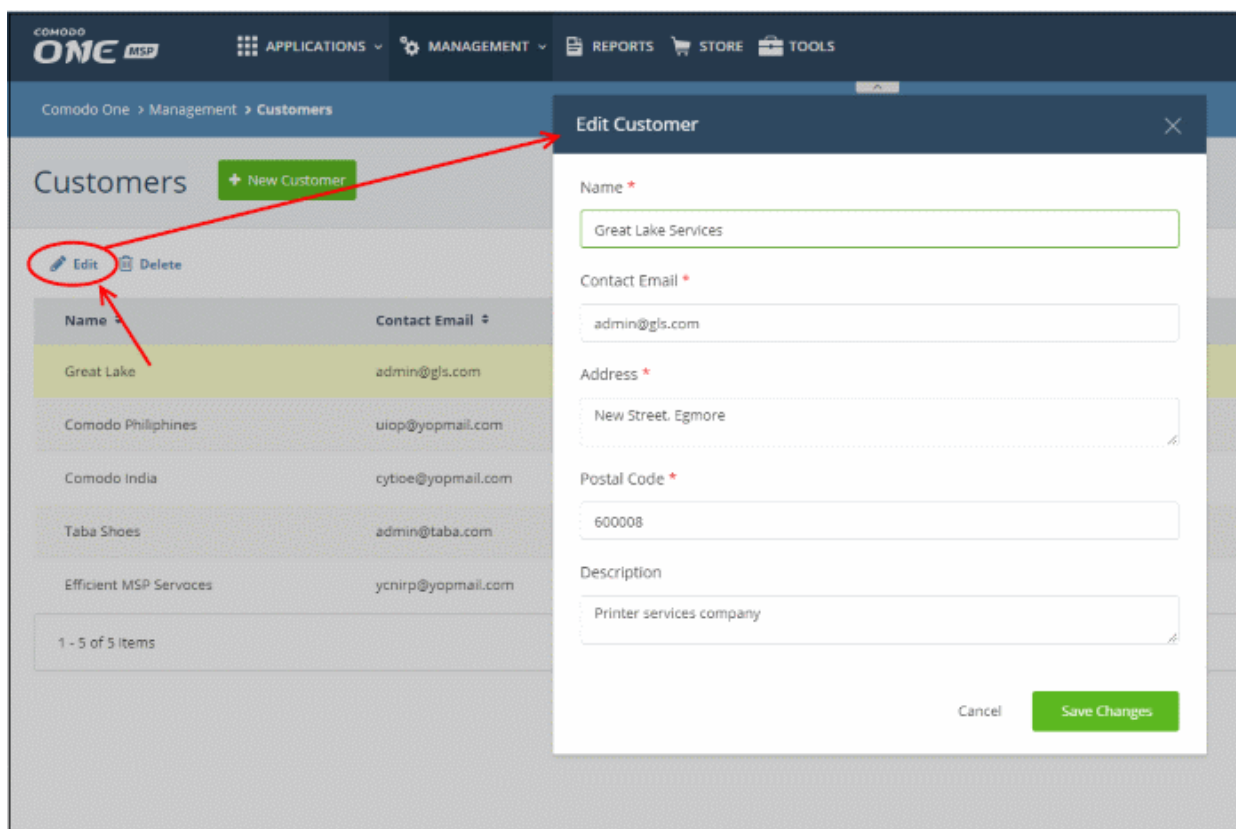
- In addition to event log collection, cWatch Network is capable of collecting log information from Comodo Network Monitoring Sensors.
- These sensors listen on the customer's network using span/tap technologies.
- Sensor deployment is customized according to a customers network topology. Please contact Comodo to arrange sensor deployment.

3.4 Edit Customers

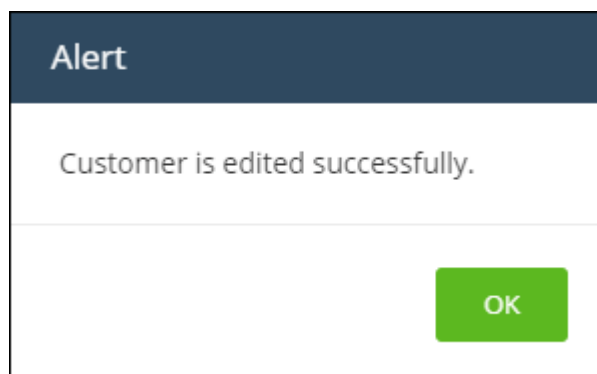
You can edit the name, address and location of a customer. You can also remove customers if required.

Edit a customer's details

- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** MSP account
- Click 'Management' > 'Customers'
- Select the customer and click 'Edit' at the top



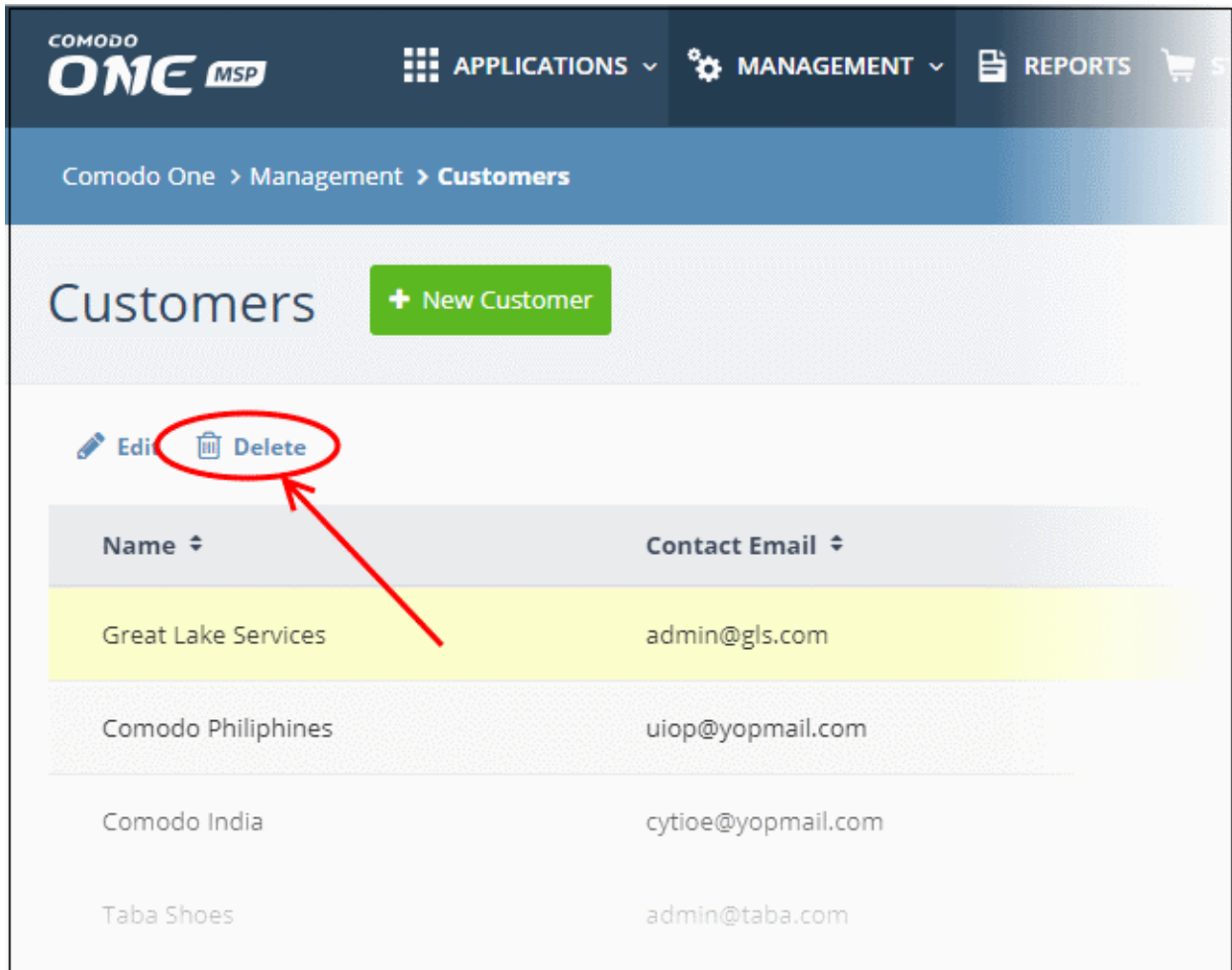
- Update the 'Edit Customer' form and click 'Save Changes'!
- Click 'OK' in the confirmation dialog.



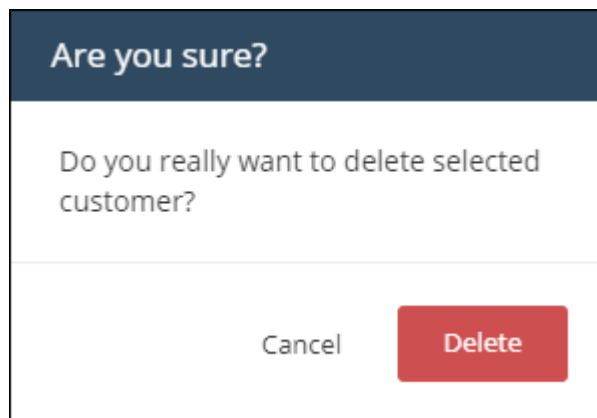
The changes done here will be updated in the cWatch interface also.

To delete a customer

- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** MSP account
- Click 'Management' > 'Customers'
- Select the customer and click 'Delete' at the top



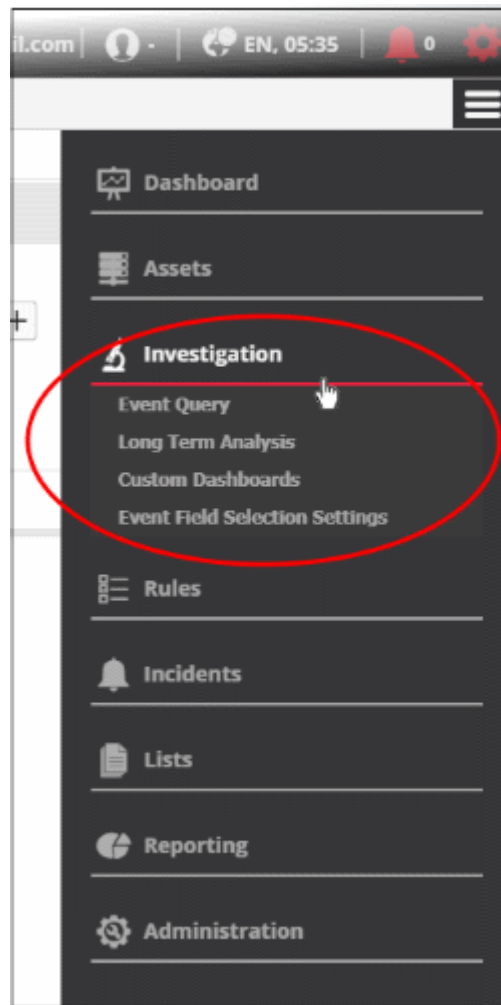
- Click 'Delete' in the confirmation dialog:



If a customer is removed, all the hard and soft assets added for the customer will also be removed and the customers networks will not be monitored.

4 Query Management

- You can query the log database to search for specific events on customer networks.
- The 'Investigation' feature lets you build granular queries, construct correlation rules and create custom dashboards.
- Comodo cWatch Network ships with a set of predefined queries for each customer and also allows you to create custom queries.



See the following sections for more details:

- [Configure Event Queries](#)
- [Long Term Analysis](#)
- [Configure Custom Dashboards](#)
- [Event Field Selection Settings](#)

4.1 Configure Event Queries

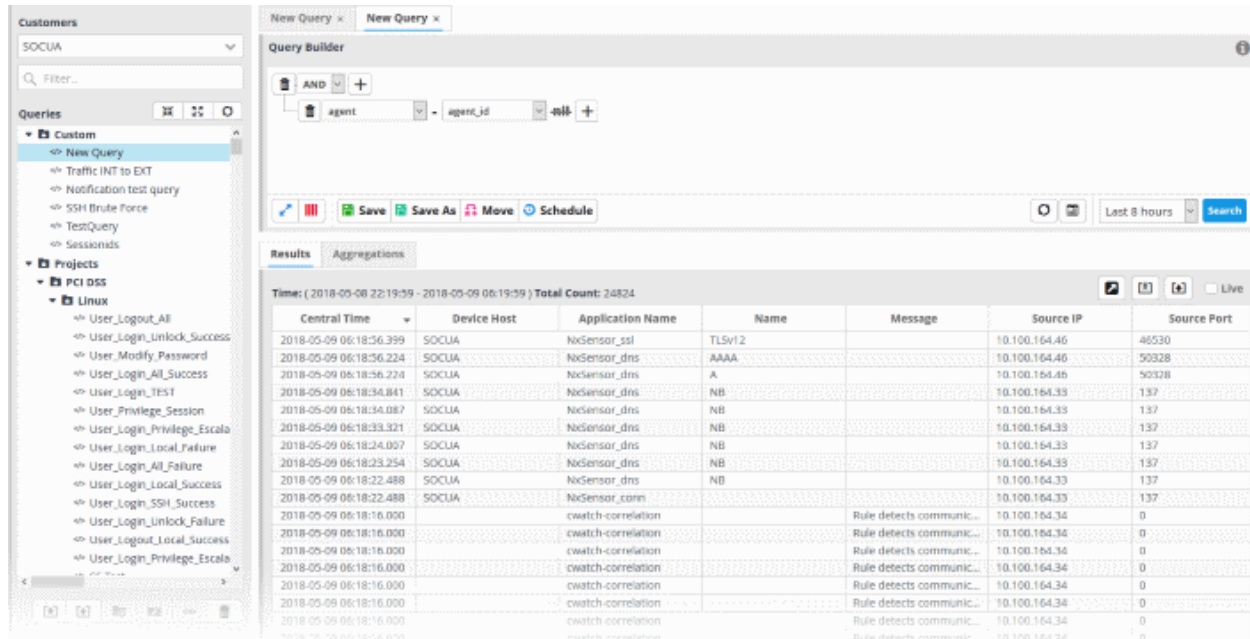
- The event query area lets you search for specific events using built-in queries or custom queries.
- You create your own conditions for each search. For example, for events during a specific period in specific customer networks.
- The results table shows all events which match the query conditions. The table also lets you run a look-up on external IPs involved in the event.

Once created, an event query can also be used for:

- Custom dashboards which show the query results as charts. See '**Configure Custom Dashboard**' for more details.
- Correlation rules which identify harmful events/incidents and assign them to customer admins for attention. See **Manage Rules** for more details.







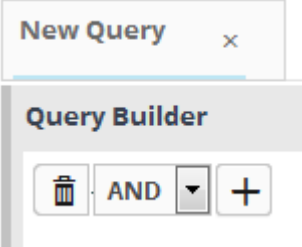










To open the event query interface:

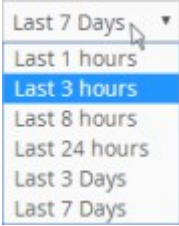

- Click the menu button at top-right > 'Investigation' > 'Event Query':



- The left-hand panel shows predefined and custom queries for the selected customer.
- The main panel shows the parameters of the selected query and its output.
- The 'New Query' tab contains a query builder. This allows you to create granular, customer queries for the selected customer. Any queries you create will be added to 'Custom queries'.
- Click 'Search' to run the query.

Event Query Interface - Table of controls	
<p>Customers</p> <p>Comodo Ank</p> <ul style="list-style-type: none"> Chennai Techwriting Comodo Ank Milkyway inc. Test Benchmark1 Test Benchmark2 Test Benchmark3 	<p>Select the customer on whose behalf you want to run the query.</p>
<p>Filter..</p>	<p>Search for a particular query. Enter the name of the query fully or partially and click on the search icon or press 'Enter'. The queries matching the entered text will be listed. To view the full list of queries again, clear the search field and press 'Enter'</p>
<p>[Expand] [Collapse] [Refresh]</p>	<p>Expand or collapse the list of queries. To collapse, click the first button and to expand it, click the second button. Click the refresh button at the end to instantly update the query list.</p>

	Add a new 'Queries' folder to the panel on the left
	Edit the name of a 'Queries' folder
	Add new event query under a selected folder
	Delete selected query folders or event queries
	Import saved queries
	Export queries
	<p>Add conditions for a query. The options available from the drop-down are:</p> <ul style="list-style-type: none"> • AND • OR • NOT <ul style="list-style-type: none"> • Click the  button to add a condition for a query. • Click the  button to delete a condition
	Expand or collapse the upper pane to view the complete list of conditions in the query.
	Configure the 'Results' table for the query displayed in the upper pane.
	Save a newly created or edited event query.
	Save the query under a different filename or to a different folder.
	Save and move your query to another folder.
	Configure alerts and email notifications based on the quantity of events detected by the query within a specified period. See explanation under ' Configure duration based alerts ' for more details.
	Refresh displayed data.
	<p>Run a query for time-period.</p> <p>You can set the start end dates to search for events matching the conditions defined in the query and click the 'Search' button in the 'Advanced Search' dialog that appears on clicking this button to view the list of events. Please note the event query created for searching events in the specific period in the past using this option, cannot be saved.</p>

	<p>Choose the time period from which events are fetched. Periods range from 1 hour to 7 days.</p>
	<p>Run a the search operation.</p>

The interface allows administrators to:

- **Manage query folders**
- **Add and Manage event queries**
- **Configure results table for a query**
- **Configure duration based alerts**
- **Run event queries**
- **View Results Table**
- **Perform IP Lookup of External IP Addresses from results using IPVOID**
- **Perform Lookup of IP Address/Domains from results using Virus Total**
- **Add Field values to Live Lists from results**
- **View Aggregated results**
- **Update and Refine Queries from results**
- **Export queries**
- **Import queries**
- **Export query results to CSV file**


Manage a Query Folder

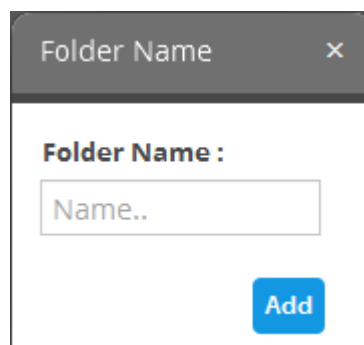
Query folders contain collections of event queries. Every new query must be placed in a query folder.

Creating a query folder

- Choose the customer from the 'Customers' drop-down at the top of the left panel.

Predefined queries added for a customer are displayed in a tree structure in the 'Queries' pane.

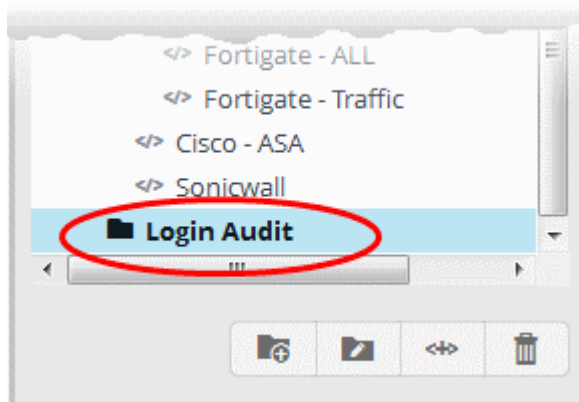
- Choose the parent folder to create a new sub-folder and click the  button. The Folder Name dialog will appear.



The dialog box is titled "Folder Name" and has a close button (X) in the top right corner. It contains a label "Folder Name:" followed by a text input field with the placeholder text "Name..". At the bottom right of the dialog is a blue "Add" button.


- Enter the name for the folder and click the 'Add' button

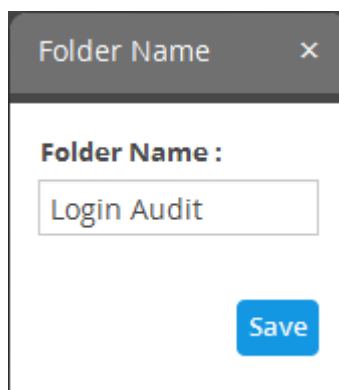
The folder will be saved and displayed on the left side.



The relevant event queries can now be placed under the newly created folder. See ['Manage an Event Query'](#) for more details.

Editing a query folder

- To edit the name of a query folder, select it and click the  button

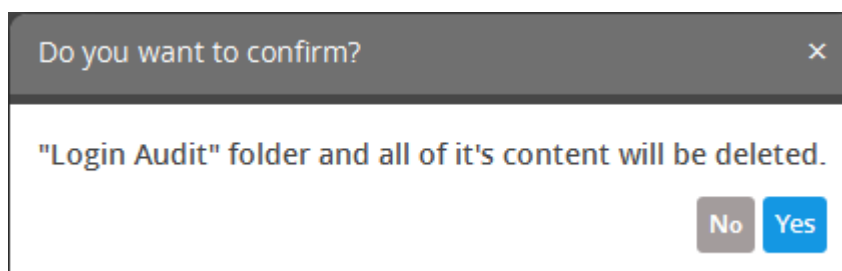


- Edit the name as required and click the 'Save' button

Deleting a query folder

- To delete a query folder, select it and click the  button

A confirmation dialog will appear.



- Click 'Yes' in the In the confirmation dialog. Please note all event queries in the folder will also be deleted.

Add and Manage Event Queries

Event queries can be created in two ways:

- **Create a new event query by defining conditions**
- **Create a new query using an existing query as a template**

Create a new event query

An event query is built with a set of filter statements that are connected by Boolean operators, 'AND', 'OR' or 'NOT'. Each filter contains the following components.

'Field Group' + 'Field' + 'Operator' + 'Value'

- **Field Group** - The group to which the 'Field' specified as the filter parameter belongs.
- **Field** - The field in the event log entry by which you want to filter results. For example, if you choose 'Agent' field group, you can select 'agent_id' or 'agent_ip' as an event field. See '**Appendix 1 - Field Groups and Event Items Description**' for a full list of field groups and event fields.
- **Operator** - Controls the relationship between the field and the specified value. Examples include 'Equals to', 'Does not equal to', 'contains', 'does not contain' etc.
- **Value** - The value for the field. Values can be entered manually or fetched from a pre-defined list which is managed in the 'Live List Management' interface. For example, if you choose a source IP (src_ip) as the field to be searched from network events, you can manually enter the IP address of the source of the connection request or choose a Live List containing a list of specified source IP addresses.

When the query is run, events will be fetched from the database and checked against the filter statements one by one.

Examples:

- To search for network connection events originating from an endpoint with IP address 10.100.100.100, build the filter statement as shown below:
'Source' + 'src_ip' + '=' + '10.100.100.100'
- To search for network connection events originating from a set of endpoints whose IP addresses start with 10.100.100.xxx, build the filter statement as shown below:
'Source' + 'src_ip' + 'AB*' + '10.100.100'
- To search for network connection events originating from a set of endpoints whose IP addresses are defined in the 'Live List type' named 'Internal' under the 'Live List' named 'IP Blacklist', build the filter statement as shown below:

'Source' + 'src_ip' + '[a]' + 'IP Blacklist' + 'Internal'

You can create more complex queries by adding more filter statements and linking them using 'AND', 'OR', or 'NOT'. For example:

- To search for network connection events originating from an endpoint with the IP 10.100.100.100, and destined for an endpoint with the IP 10.100.100.120, build the filter statements with the AND operator as shown below:


'Source' + 'src_ip' + '=' + '10.100.100.100'

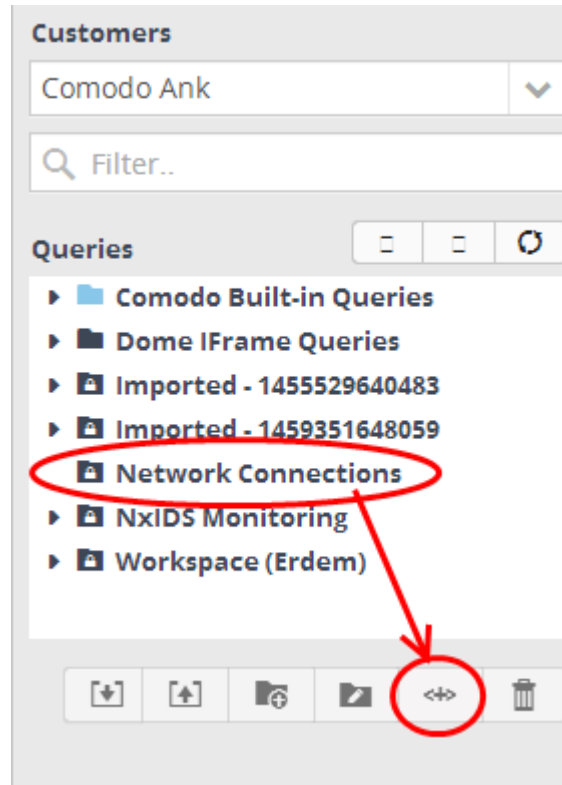
AND

'Destination' + 'dst_ip' + '=' + '10.100.100.120'

To add a new event query for a customer

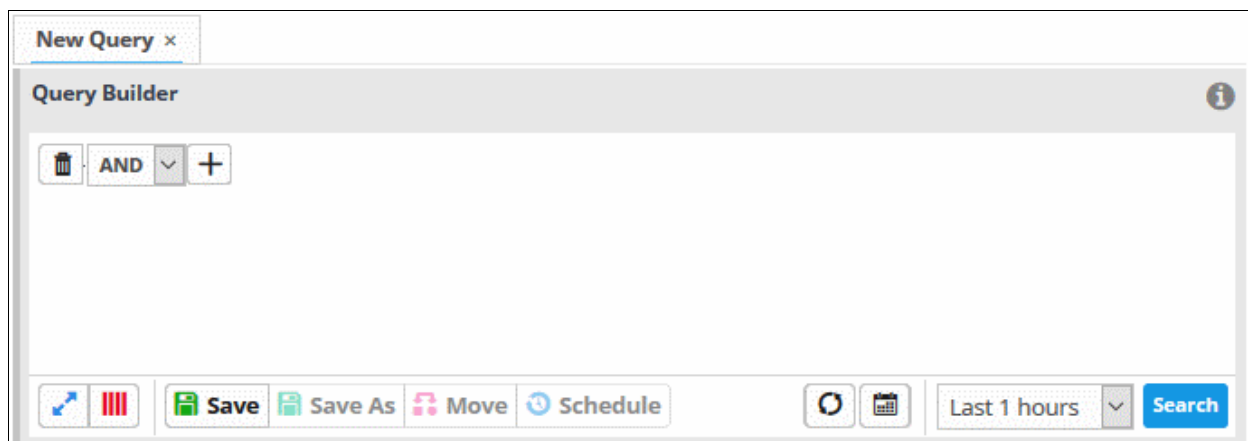
- Select the customer from the 'Customers' drop-down at the top of the left hand panel.

- Select the appropriate folder or **create a new query folder** under which you want to create an event query. Alternatively, you can also select a folder while saving a query.
- Click the  button.



A 'New Query' tab will be displayed.

Tip: You can also create a new query by selecting a customer then clicking the 'New Query' tab. You can save the created query by selecting an appropriate folder from the left side panel.

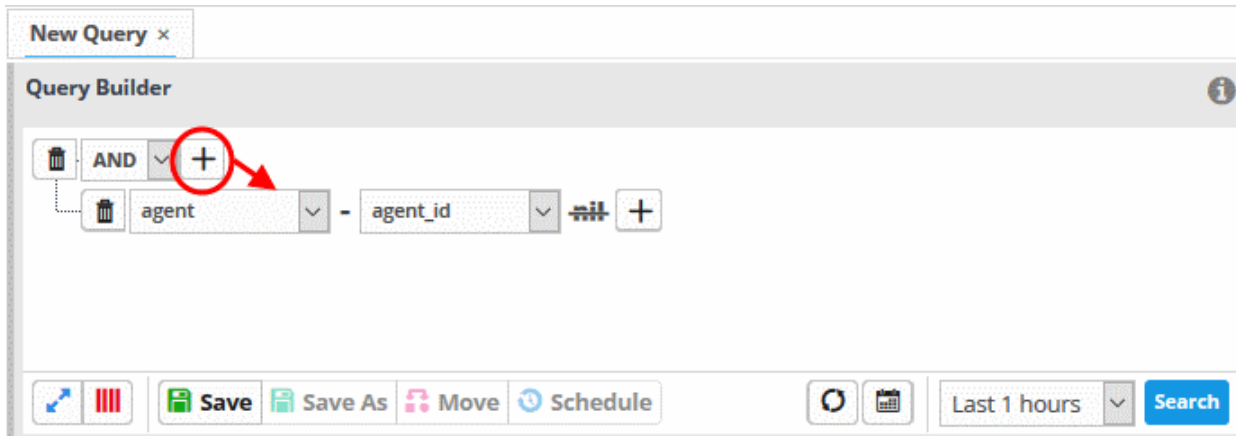


The next step is to add filters to the query.

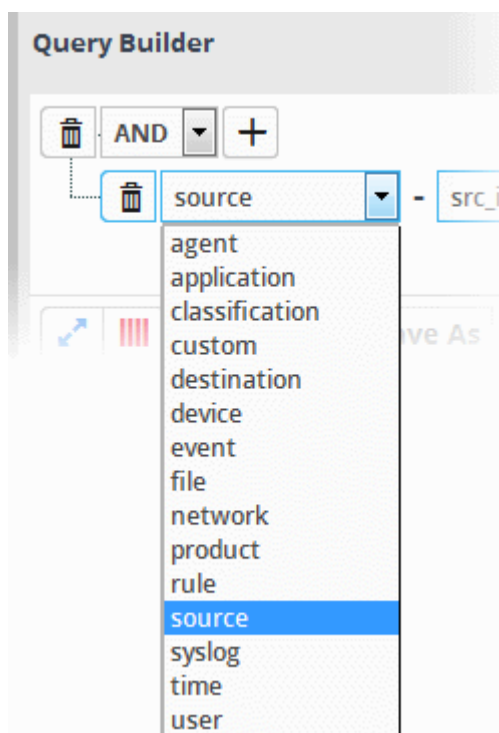
- Choose the operator for the query filter statement from the drop-down in the 'Query Builder' pane. The options available are:
 - AND
 - OR

- NOT
- Click the  button to add a filter

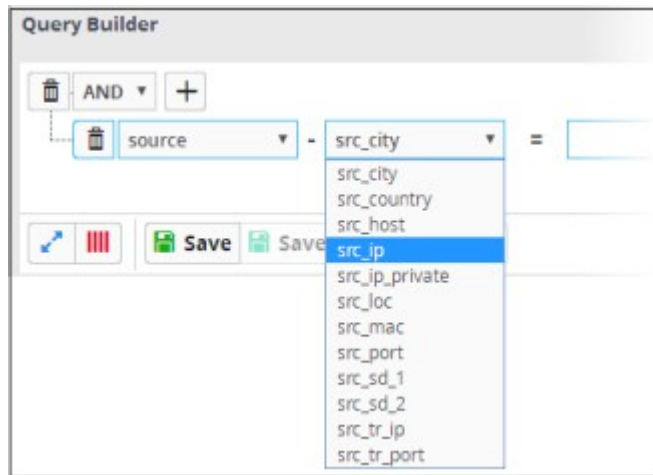
The 'Field Groups' drop-down and 'Fields' drop-down will appear. The 'Fields' drop-down will contain options relevant to the 'Field Group' chosen from the drop-down at the left.



- Choose the field group you wish to add to the filter from the 'Field Groups' drop-down.



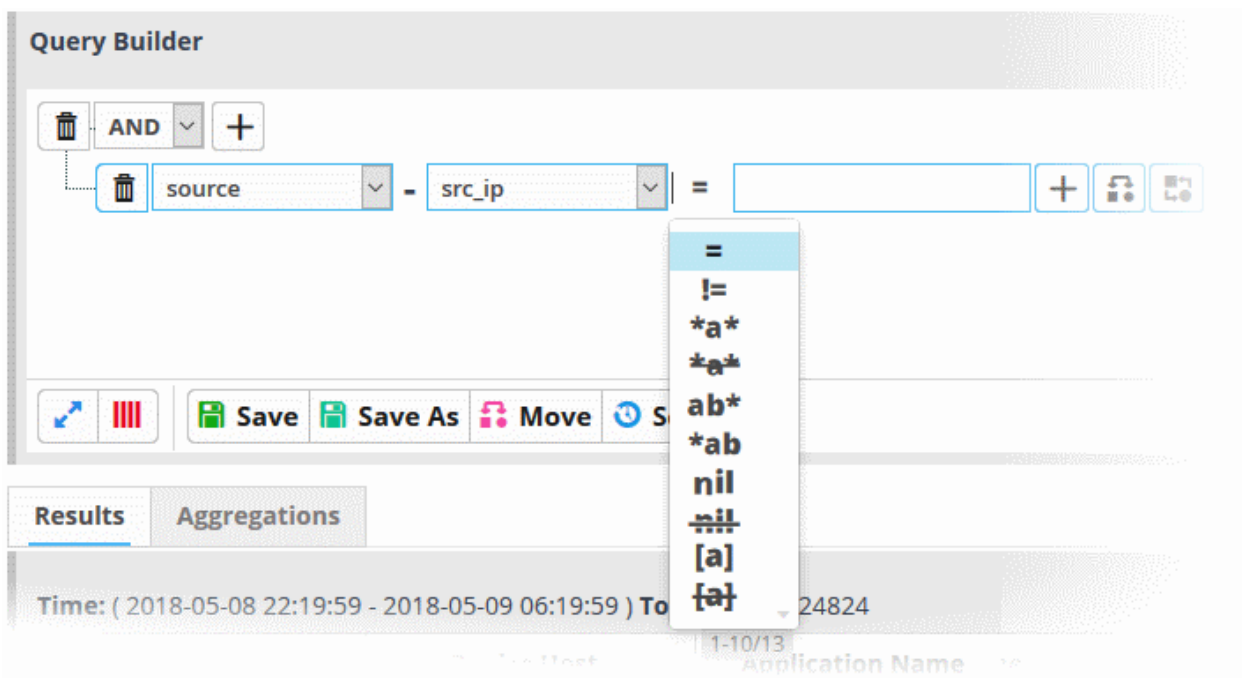
The next field will display the fields available for the selected field group.



Tip: Descriptions of each Field Group and the Field items under them are available in [Appendix 1 - Field Groups and Event Items Description](#).

The next step is to choose the relationship operator between the two fields.

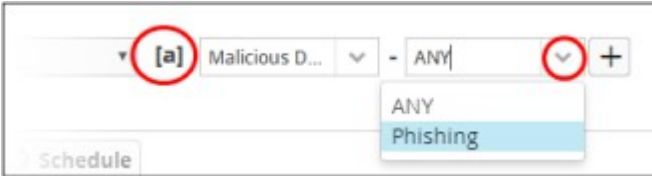
- To choose an operator, click the drop-down between the two fields:

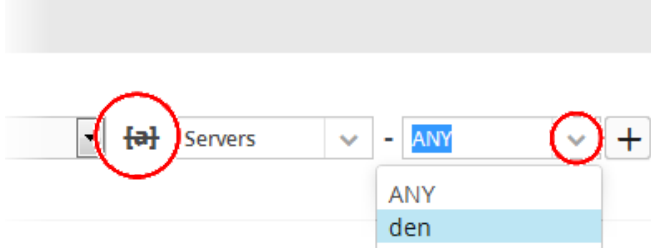


The types operators depends on the field chosen. The following table explains the various operator symbols:

Relation Operator	Description	Entering the value for the 'Field'
=	Equals to	<ul style="list-style-type: none"> Events containing the same value will be identified by the query. Enter a value in the field to the right of the operator.
!=	Does not equal to	<ul style="list-style-type: none"> Events that do not contain the value will be identified by the query.

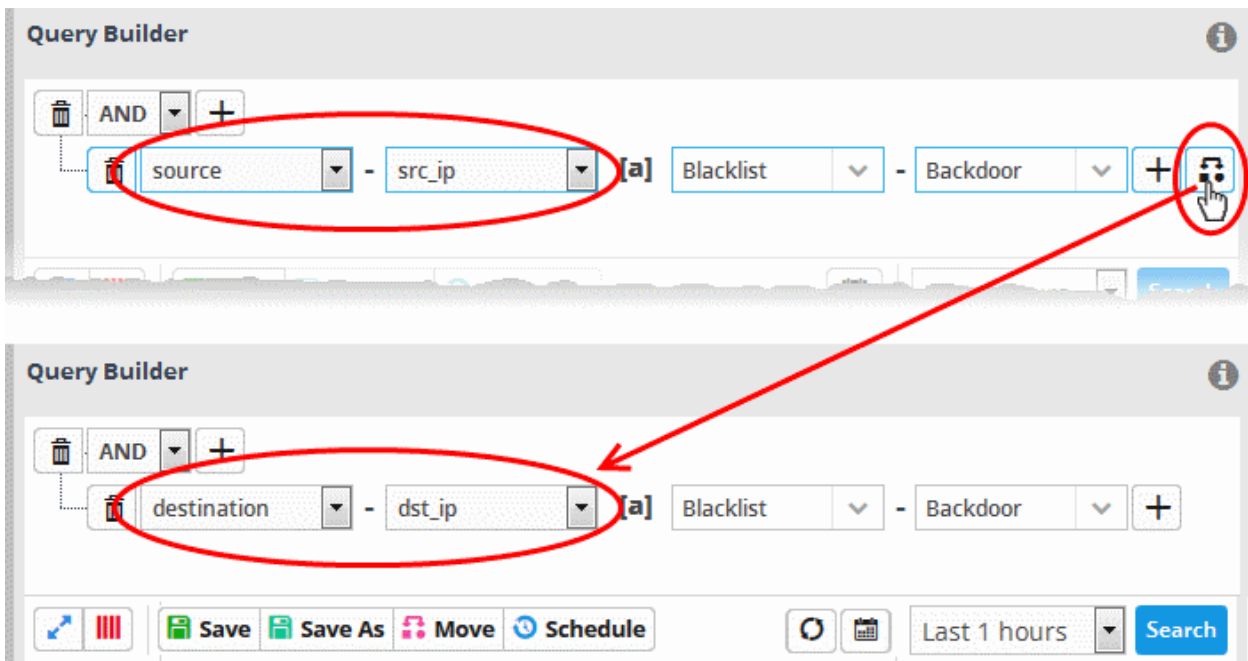
		<ul style="list-style-type: none"> Enter a value in the field to the right of the operator.
>	Greater than	<ul style="list-style-type: none"> The query will identify events that contain values greater than the entered value. Enter a value in the field to the right of the operator. <ul style="list-style-type: none"> Applies only to fields with numerical values. For example, port numbers.
>=	Greater than or equal to	<ul style="list-style-type: none"> The query will identify events that contain values equal to or greater than the entered value. Enter a value in the field to the right of the operator. <ul style="list-style-type: none"> Applies only to fields with numerical values. For example, port numbers.
<	Less than	<ul style="list-style-type: none"> The query will identify events that contain values less than the entered value. Enter a value in the field to the right of the operator. <ul style="list-style-type: none"> Applies only to fields with numerical values. For example, port numbers.
<=	Less than or equal to	<ul style="list-style-type: none"> The query will identify events that contain values equal to or lower than the entered value. Enter a value in the field to the right of the operator. <ul style="list-style-type: none"> Applies only to fields with numerical values. For example, port numbers.
a	Contains	<ul style="list-style-type: none"> The query will identify events that contain the entered value somewhere in the string. <ul style="list-style-type: none"> E.g - search for events with source IP addresses containing '123' anywhere in the address. Enter a value in the field to the right of the operator.
a	Does not contain	<ul style="list-style-type: none"> The query will identify events that do not contain the entered value anywhere in the string. <ul style="list-style-type: none"> E.g - search for events which don't contain '123' anywhere in source IP address. Enter a value in the field to the right of the operator.
ab*	Starts with	<ul style="list-style-type: none"> The query will identify events that begin with the entered value. <ul style="list-style-type: none"> E.g, - search for events with source IP addresses that start with '192' Enter a value in the field to the right of the operator.
*ab	Ends with	<ul style="list-style-type: none"> The query will identify events that end with the entered value. <ul style="list-style-type: none"> E.g. - search for events with source IP addresses that end with '123'. Enter a value in the field to the right of the operator.
nil	Is Empty	<ul style="list-style-type: none"> Search for events in which the selected field is

		<p>empty (does not contain any value).</p> <ul style="list-style-type: none"> E.g. - search for the events with no values in their source IP address fields, select 'Is Empty'.
≠	Is Not Empty	<ul style="list-style-type: none"> Search for events in which the selected field is not empty (contains a value of some kind). E.g - to search for the events with some IP addresses values in their source IP address fields, select 'Is Not Empty'.
[a]	Is in List	<p>Configure the filter statement to fetch values for the field from a pre-defined list containing specific values for the field type.</p> <p>Background:</p> <ul style="list-style-type: none"> Lists enable administrators to add and manage lists of values for different fields for use in queries and correlation rules. cWatch features three kinds of lists - Live Lists, Range List and IP Range. Lists can be created and the values updated manually. Live lists can be also be fetched from the output of correlation rules. List updates will be immediately reflected in the queries and the rules in which they are used. See Lists for more details on list management. <p>On selecting [a] as the relation parameter, drop-down options will appear for the List and the List type:</p>  <p>The first drop-down shows the Lists that contain values for the selected query field. The second drop-down shows the List Types within the selected 'List'.</p> <ul style="list-style-type: none"> Choose the List to be used in the query filter from the first drop-down. Choose the sub list that contains the set of values to be included in the query filter from the second drop-down. <p>All the values contained in the list will be included as values for the Field specified in the filter statement.</p>
{a}	Not in List	<p>Allows you to configure the filter statement to search for the events that do not contain specific values from a pre-defined list.</p>

		<p>On selecting [a] as the relation parameter, drop-down options will appear for the List and the List type:</p>  <p>The first drop-down shows the Lists that contain values for the selected query field. The second drop-down shows the List Types within the selected 'List'.</p> <ul style="list-style-type: none"> • Choose the List to be used in the query filter from the first drop-down. • Choose the sub list that contains the set of values to be input as exclusions to the query filter from the second drop-down. <p>The results will display all events that do not contain the values in the lists.</p>
--	--	--

If you are adding values for source parameters like source IP address, source port, source MAC etc., but wish to reverse the parameter, click the switch icon **[a]** that appears to the right of the statement. The field group and the field selected will automatically switch from source to destination or vice-versa.

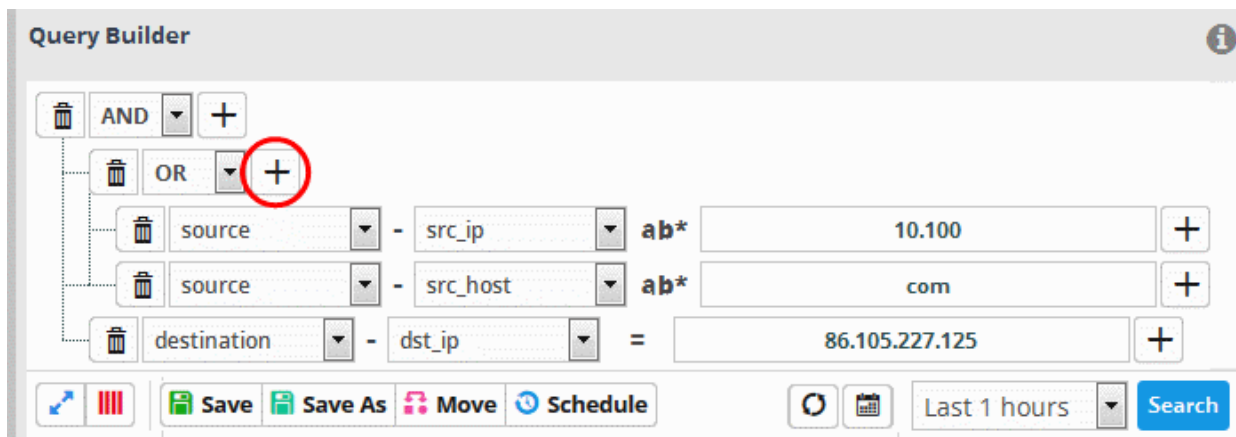
- For example, if you are specifying a live list containing values of source IPs for the source IP field, but want to change them to destination IPs, you can click the switch button.





The top screenshot shows the Query Builder interface with a query: **source** - **src_ip** **[a]** **Blacklist** - **Backdoor**. The **[a]** icon and the **source** field are circled in red.

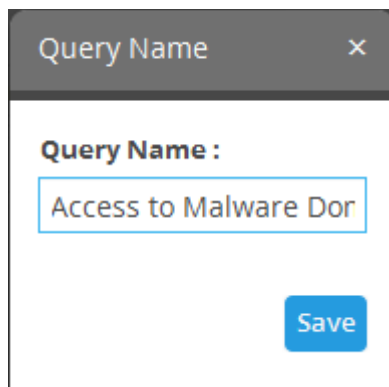
The bottom screenshot shows the Query Builder interface with a query: **destination** - **dst_ip** **[a]** **Blacklist** - **Backdoor**. The **[a]** icon and the **destination** field are circled in red. A red arrow points from the **[a]** icon in the top screenshot to the **[a]** icon in the bottom screenshot.

- To add a sub-filter statement, click the **+** button beside the filter and repeat the process.
- To set the relationship between each statement, use the drop-down menu.
- For example, the query below will return events whose source ends with 10.100 OR .com AND whose destination is 86.105.227.125



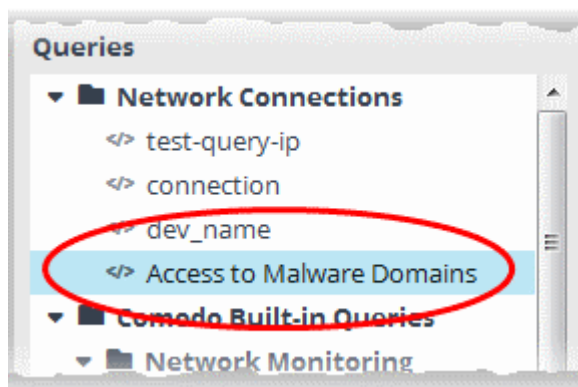
Tip: You can update and refine a query by adding more filters once you have seen the results. See [Updating a Query](#) for more details.

- To add more filter statements to the query, click the  button and repeat the process.
- To delete a filter, click the  button beside it.
- Click the 'Save' button in the 'Query Builder' screen.



- Enter the name of the query in the 'Query Name' field and click the 'Save' button.
- The 'Event Query' will be saved under the selected folder and displayed.

Note: If you didn't select a folder in the first step you will be asked to do so when saving the query.



The next step is to run the event query. Before that, however, the 'Results' table must be checked and configured so that it is relevant to the event query. See '[Configure Results Table for a Query](#)' and '[Event Field Selection Settings](#)' for more details.

Creating a new query using an existing query as a template

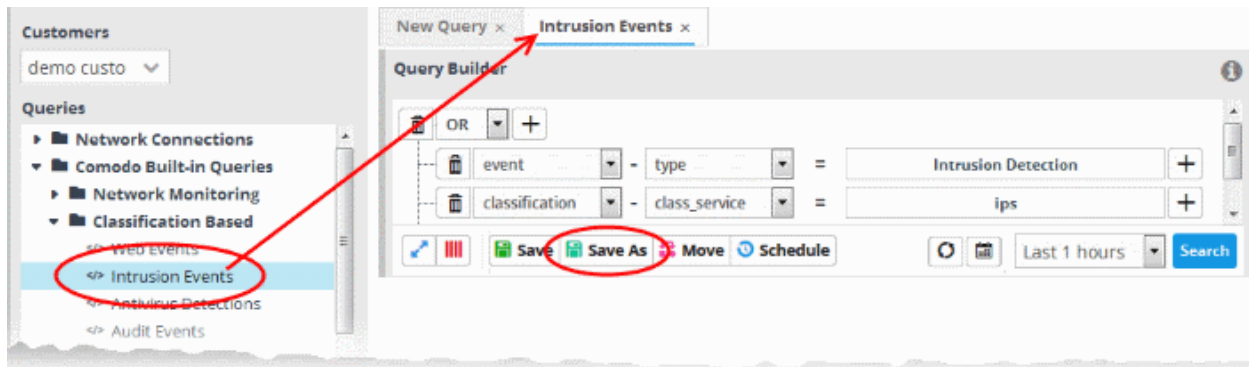
You can select a pre-defined query and modify its parameters to create a new query.

To create a query from an existing query

- Select the customer from the 'Customers' drop-down at the top of the left hand panel.
- Select the query from the list of queries in the left panel.

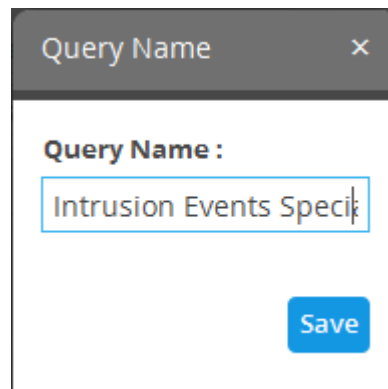
The query will be expanded under a new tab in the right side panel.

- Add or remove the query filter statements and/or edit the parameters in the existing filter statements. The process is same as creating a new condition as explained [above](#).



- Select the folder in which the new query is to be saved.
- Click 'Save as' from the 'Query Builder' pane.

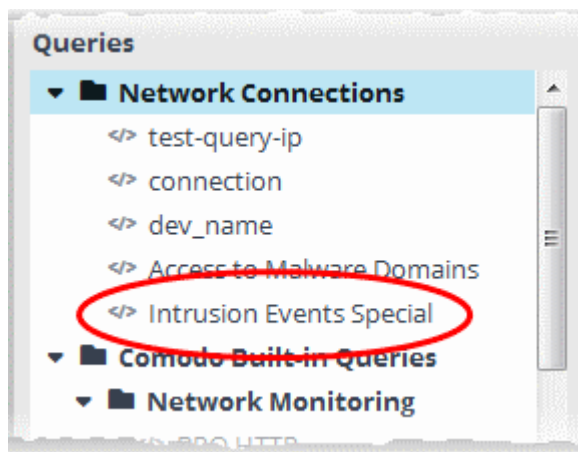
The 'Query Name' dialog will appear.



- Enter a new name for the query and click 'Save'.

The 'Event Query' will be saved and displayed under the selected folder.

The next step is to run the event query but before that the 'Results' table must be checked and configured so that it is relevant to the event query. See '[Configure Results Table for a Query](#)' for more details.

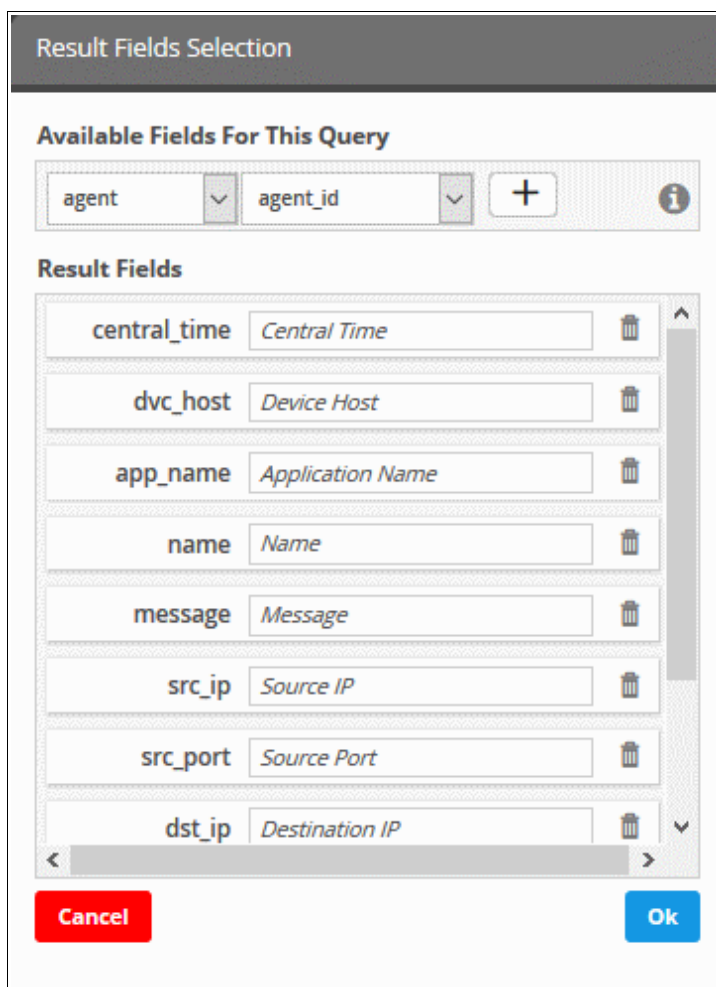


Configure Results Table for a Query

In order to display the event fields relevant to a specific query, the 'Results' table must first be configured.

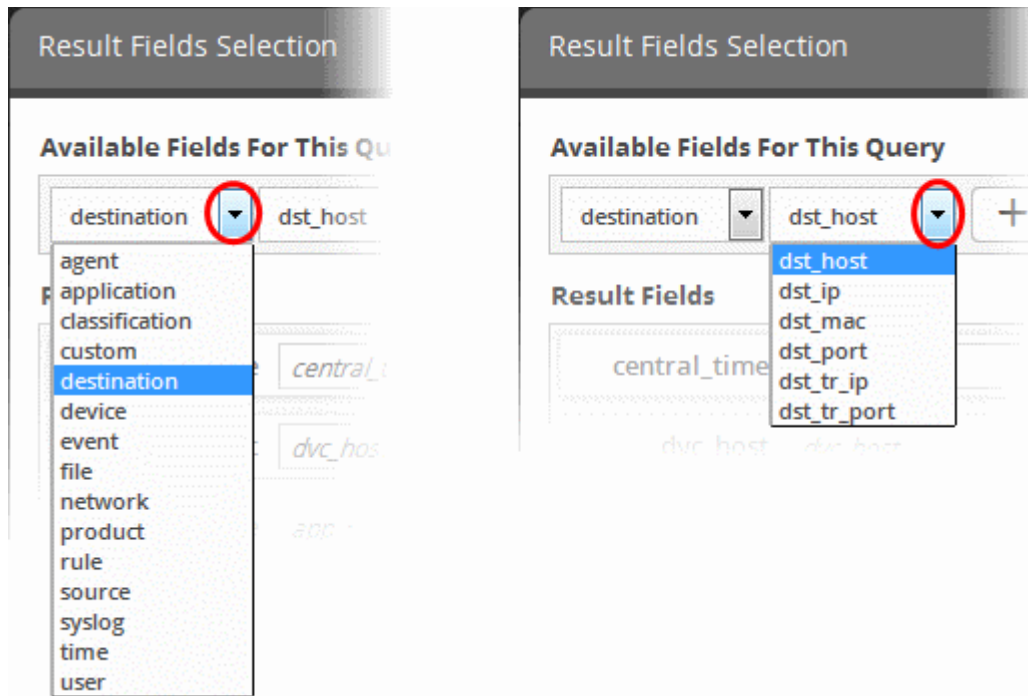
- By default, cWatch ships with ten event field columns in the results table.
- You can add more event field columns here.
- Select an event query from the left and click the  button in the 'Query Builder' pane. Note – The event field columns added to the results are valid for this search only. Go to 'Investigation' > **Event Field Selection Settings** to configure fields that are valid for all query searches.

The 'Result Fields Selection' dialog will be displayed.




The same 'Field Groups' and 'Fields' used for in the 'Query Builder' will be available for inclusion in the results table. By default a set of 'Result Fields' relevant to the query will be displayed.

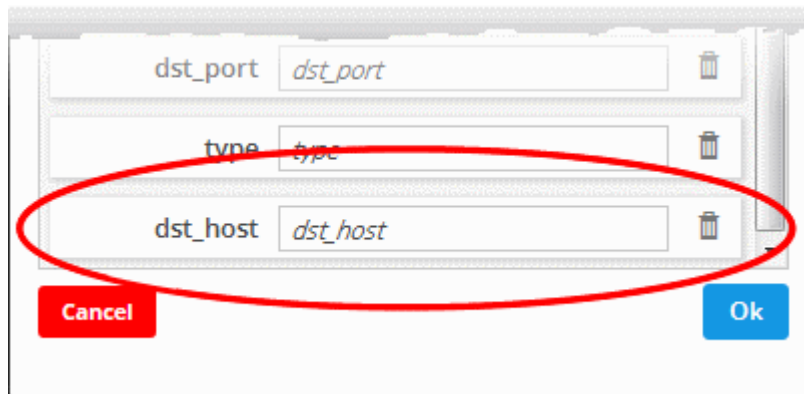
- To add new 'Result Fields', click the 'Field Groups' combo box and select the field group.




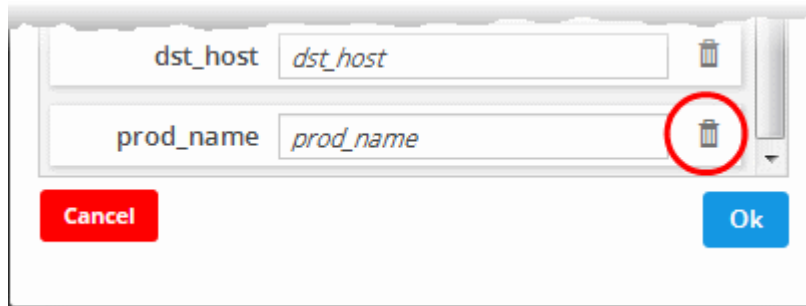
The next field will display the items available for the selected field group.

- Select the required field from the drop-down and click the  button.

A new field will be added and you have to provide a new label for the result field.



- Enter a name for the field, by which the field should be displayed in the 'Results' screen.
- Repeat the process to add more fields and click 'OK'
- To remove irrelevant fields, click the trash can icon  beside it.




- Click the 'Ok' button
- Click the 'Cancel' button to revert the changes you made.
- Click the 'Save' button in the 'Query Builder' screen to save your changes.

'Event Queries' can also be used to populate charts in a custom dashboard. See '[Configuring Custom Dashboard](#)' for more details.

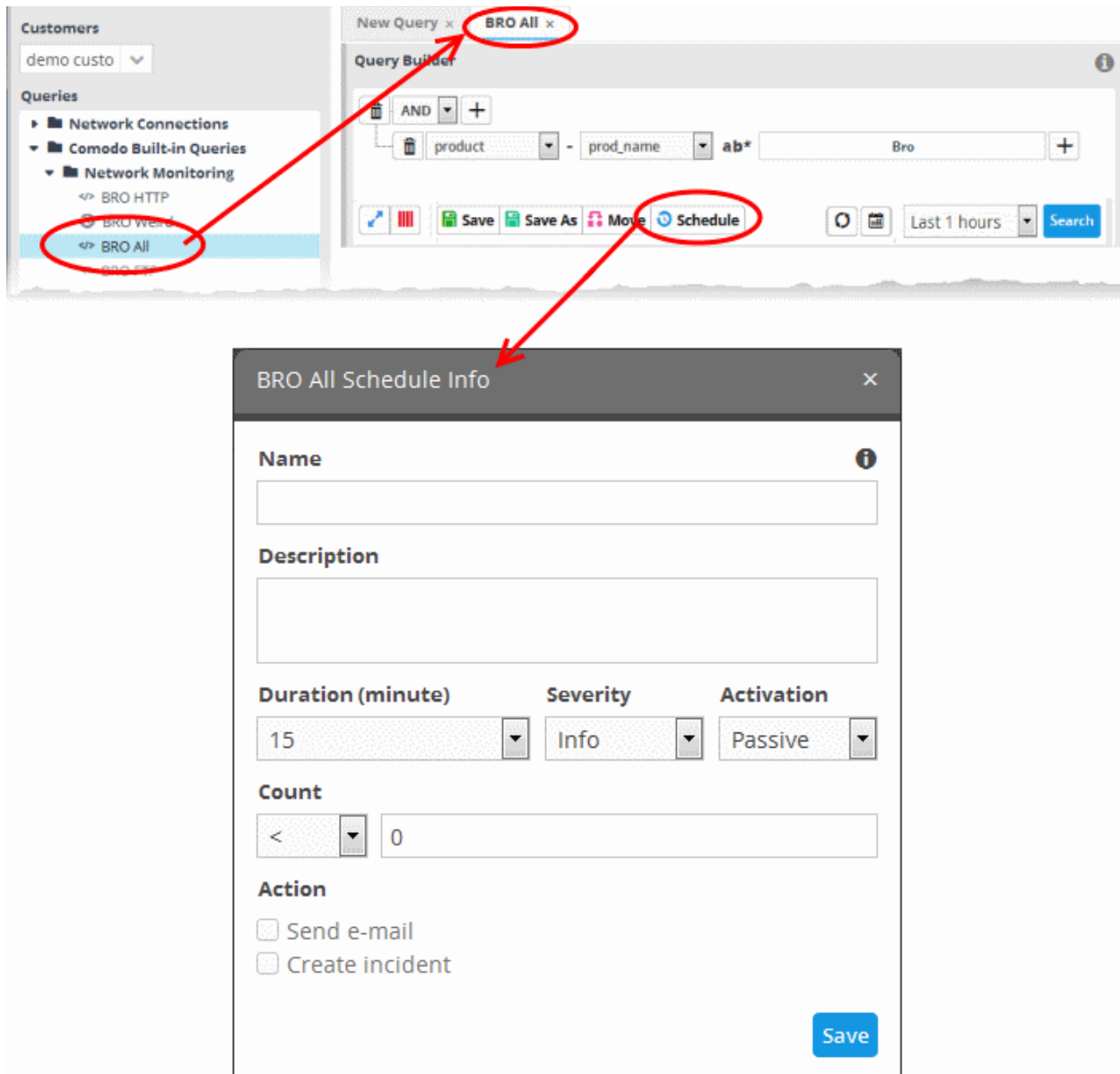
Configure Duration Based Alerts

- cWatch Network dynamically monitors customer networks for events based on user-defined queries.
- You can create queries to generate alerts if the number of events exceeds or falls below a certain threshold in a certain time-period.
- Examples. You can request alerts if the number of events matching a query exceeds 1000 in 10 minutes, or if no events are detected for a query for 15 minutes.
- Alerts can be configured to send notification emails to the admin and/or generate an 'Incident'. The incident can be auto-assigned to a user. See [Managing Incidents](#), for more details on this.

To schedule a query to generate alerts

- Select a saved event query from the left side and click the 'Schedule' button  from the 'Query Builder' pane.

The 'Schedule Info' dialog will be displayed for the selected query.



- **Name** - Enter a name to identify the schedule
- **Description** - Enter a short description for the schedule
- **Duration** - Enter the time period specified for monitoring the number of events matching the query, in minutes.
- **Severity** - Select the severity level for the alert to be generated by the schedule
- **Activation** - Specify whether the schedule is to be activated or not from the drop-down. You can switch the activation state of a schedule at any time from the 'Schedule Info' dialog.
- **Count** - Set the threshold for the number of events.
 - > - Will generate an alert if the number of events detected in the specified 'duration' exceeds the value in the text field.
 - < - Will generate an alert if the number of events detected in the specified 'duration' is lower than the value in the text field
 - To generate an alert if no events are detected within the specified duration, choose less than and enter 'zero' ('<' and '0')
- **Action** - Choose how cWatch should react if the alert's conditions are triggered.
 - Send e-mail - cWatch sends a notification email to the administrator if the conditions are met
 - Create Incident - An incident is created and assigned to a user to investigate. See **Managing Incidents** for more details.

- Click 'Save' in the Schedule Info dialog to save the schedule.

The event query will be added with a schedule.

- To edit a schedule of a query or switch the schedule between 'active' and 'inactive' states, select the query from the list at the left, click the 'Schedule' button, change the values in the 'Schedule Info' dialog and click 'Save'.

Run an Event Query

Saved event queries can be run at anytime to obtain a list of matching events within a chosen period of time. The results can be viewed in two ways:

1. As a results table with columns selected as explained **above**.

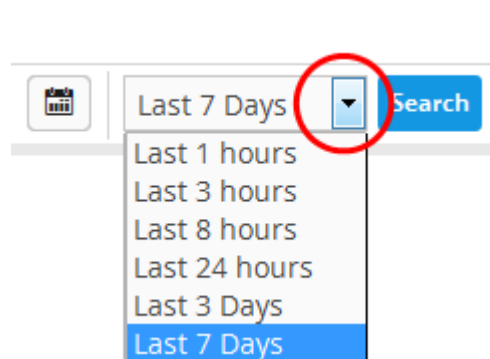
You can view the full details of any event in its 'Details Pane' containing values for all the fields in the log entry. The details pane also lets you add values of live lists for use in new event queries and rules. You can also run look-ups of IP addresses and domains involved in the event. More explanations are available under '**View Results Table**'.

2. As aggregated results.

Identified events are grouped based on selected event field(s) and the resultant event groups ranked based on the aggregation function. More explanations are available under '**View Aggregated Results**'.

To run an event query

- Select an event query from the left.
- Select the period for which you want to run the query.
 - View recent events - Select a period from the drop-down at the bottom right of the 'Query Builder' pane and click 'Search'. Options range from the past hour to the past 7 days.



- View events over specific dates - Click the calendar button, enter the start and end dates and click 'Search'.

The 'Results' are displayed in the lower pane.

- Select the 'Live' check box to search streaming data for the event query.

Note: The 'Live' option is not available for searches with specific start and end dates.

The lower pane has two tabs:

- **Results** - The 'Results' tab displays log entries that match the query with the selected event fields as column headers (explained above). Click an event to view its details. More details on the 'Results Table' are available under **'View Results Table'**.
- **Aggregations** - The Aggregations tab allows you to group identified events and view aggregation results. More details on aggregations are available under **'View Aggregated Results'**.

View Results Table

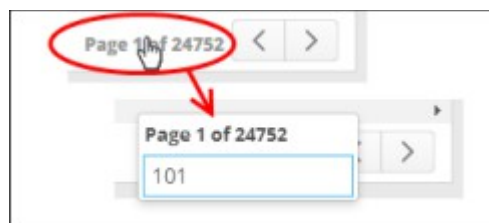
After running a query, the 'Results' tab is opened by default in the lower pane. You can click the 'Results' tab to view the results table if you are currently viewing the aggregation results.

The 'Results' tab contains a table of event log records that match the event query. The event fields form the table columns. Events can be created in the Query Builder pane. See '[Configure results table for a query](#)' and '[Event Field Selection Settings](#)' for more details.

Central Time	Device Host	Application Name	Name	Message	Source IP	Source Port
2018-04-18 09:34:34.948	SOCUA	NxSensor_ssl	TLsv12		10.100.164.34	62968
2018-04-18 09:34:34.224	SOCUA	NxSensor_ssl	TLsv12		10.100.164.34	62967
2018-04-18 09:34:29.739	SOCUA	NxSensor_conn			10.100.164.33	52378
2018-04-18 09:33:52.156	SOCUA	NxSensor_ssl	TLsv12		10.100.164.46	35722
2018-04-18 09:33:52.015	SOCUA	NxSensor_conn			10.100.164.46	35722
2018-04-18 09:33:51.950	SOCUA	NxSensor_dns	A		10.100.164.46	56511
2018-04-18 09:33:51.950	SOCUA	NxSensor_dns	AAAA		10.100.164.46	56511
2018-04-18 09:33:50.454	Centos71	linux-audit	SYSCALL	audit(1524044030.454:...		0
2018-04-18 09:33:50.454	Centos71	linux-audit	SYSCALL	audit(1524044030.454:...		0
2018-04-18 09:33:50.454	Centos71	linux-audit	PROCTITLE	audit(1524044030.454:...		0
2018-04-18 09:33:50.454	Centos71	linux-audit	SYSCALL	audit(1524044030.454:...		0
2018-04-18 09:33:50.454	Centos71	linux-audit	PROCTITLE	audit(1524044030.454:...		0
2018-04-18 09:33:50.454	Centos71	linux-audit	PROCTITLE	audit(1524044030.454:...		0
2018-04-18 09:33:50.221	SOCUA	NxSensor_conn			10.100.164.33	52374
2018-04-18 09:33:50.140	SOCUA	NxSensor_conn			10.100.164.47	27858
2018-04-18 09:33:50.140	SOCUA	NxSensor_conn			10.100.164.47	27857
2018-04-18 09:33:49.721	SOCUA	NxSensor_conn			10.100.164.33	52373
2018-04-18 09:33:45.881	SOCUA	NxSensor_weird	dns_unmatched_msg		10.100.164.51	5353
2018-04-18 09:33:45.881	SOCUA	NxSensor_weird	dns_unmatched_msg		fe80::fee4:288fe1b03...	5353
2018-04-18 09:33:43.002	SOCUA	NxSensor_weird	dns_unmatched_msg		10.100.164.47	137

Each page in the 'Results' table displays 20 entries. You can navigate to successive pages using the left and right arrows at the bottom-right.

- Open a specific page - Click the page number at bottom-right then enter the page number you require:



- You can view complete details of an event log entry in the results table. You can use values from the results as additional statements in your query to further refine the search.
- You can also perform IP and domain look-ups and feed these values into live lists for use in other queries and correlation rules.
- To view fields you selected earlier, click ' Selected Result Fields'

The screenshot displays the 'Results' tab with a table of events. The table has columns for Central Time, Device Host, Application Name, and a fourth column. The 'Details' tab is active, showing fields like agent_time, Application Name, bytes_in, bytes_out, Central Time, customer_id, Destination IP, Destination Port, Device Host, duration, event_id, It_1, Name, prod_name, prod_vendor, rcvd_pkt, session_id, Source IP, Source Port, trans_proto, and Type.

Central Time	Device Host	Application Name	
2018-04-18 09:46:36.335	SOCUA	NxSensor_dns	SRV
2018-04-18 09:46:35.207	SOCUA	NxSensor_ssl	TLSv12
2018-04-18 09:46:34.532	SOCUA	NxSensor_ssl	TLSv12
2018-04-18 09:46:34.072	SOCUA	NxSensor_ssl	TLSv12
2018-04-18 09:46:33.910	SOCUA	NxSensor_ssl	TLSv12
2018-04-18 09:46:33.032	SOCUA	NxSensor_ssl	TLSv12
2018-04-18 09:46:32.997	SOCUA	NxSensor_conn	
2018-04-18 09:46:31.110	SOCUA	NxSensor_conn	
2018-04-18 09:46:30.609	SOCUA	NxSensor_conn	
2018-04-18 09:46:30.364	SOCUA	NxSensor_conn	
2018-04-18 09:46:30.364	SOCUA	NxSensor_conn	
2018-04-18 09:46:22.852	SOCUA	NxSensor_conn	
2018-04-18 09:46:20.584	SOCUA	NxSensor_conn	
2018-04-18 09:46:11.797	SOCUA	NxSensor_ssl	TLSv12
2018-04-18 09:46:11.743	SOCUA	NxSensor_conn	
2018-04-18 09:46:11.743	SOCUA	NxSensor_dns	A
2018-04-18 09:46:00.662	SOCUA	NxSensor_dns	NB
2018-04-18 09:45:59.911	SOCUA	NxSensor_dns	NB
2018-04-18 09:45:59.602	SOCUA	NxSensor_dns	NB
2018-04-18 09:45:59.161	SOCUA	NxSensor_conn	

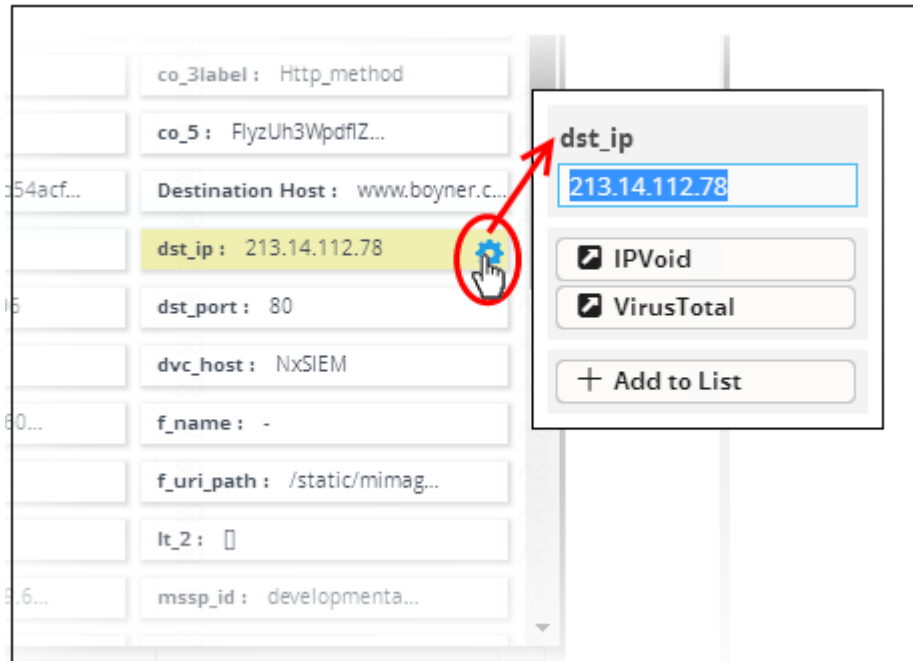
- View event details - Click the result row then the 'Details' tab.
- View second-level filtered results - Click and select the fields you want to view then click the 'Filter' tab.
- View all collected endpoint messages and activities - Click the 'Raw Log' tab.

The screenshot displays the 'Results' tab with a table of events. The table has columns for Central Time, Device Host, Application Name, and a fourth column. The 'Raw Log' tab is active, showing fields like 1524052716.625814, CekKylusOUidRgECd, 10.100.164.46, 36018, 35.169.33.2, 443, TLSv12, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, sensor.mssp.comodo.com, and T.

Central Time	Device Host	Application Name	
2018-04-18 11:58:45.703	SOCUA	NxSensor_conn	
2018-04-18 11:58:36.625	SOCUA	NxSensor_ssl	TLSv12
2018-04-18 11:58:36.485	SOCUA	NxSensor_conn	
2018-04-18 11:58:36.421	SOCUA	NxSensor_dns	AAAA
2018-04-18 11:58:36.421	SOCUA	NxSensor_conn	
2018-04-18 11:58:36.421	SOCUA	NxSensor_dns	A
2018-04-18 11:58:34.885	SOCUA	NxSensor_conn	
2018-04-18 11:58:34.884	SOCUA	NxSensor_conn	

External IP addresses and domain names are highlighted in yellow.

- Clicking on a field adds the field with its value as a filter statement to the query, enabling you to refine your search for events that contain the same value in the respective field and/or to create a new query. See explanation under **Update and Refine Queries from results** for more details.
- If you click the gear icon that appears when you hover your mouse over a field you will see a context sensitive menu:



From the context sensitive menu, you can:

- **Perform IP lookup of external IP addresses using IPVOID**
- **Perform IP Address/Domain lookup using Virus Total**
- **Add the value to a Live List**

Performing IP Lookup of External IP Addresses using IPVOID

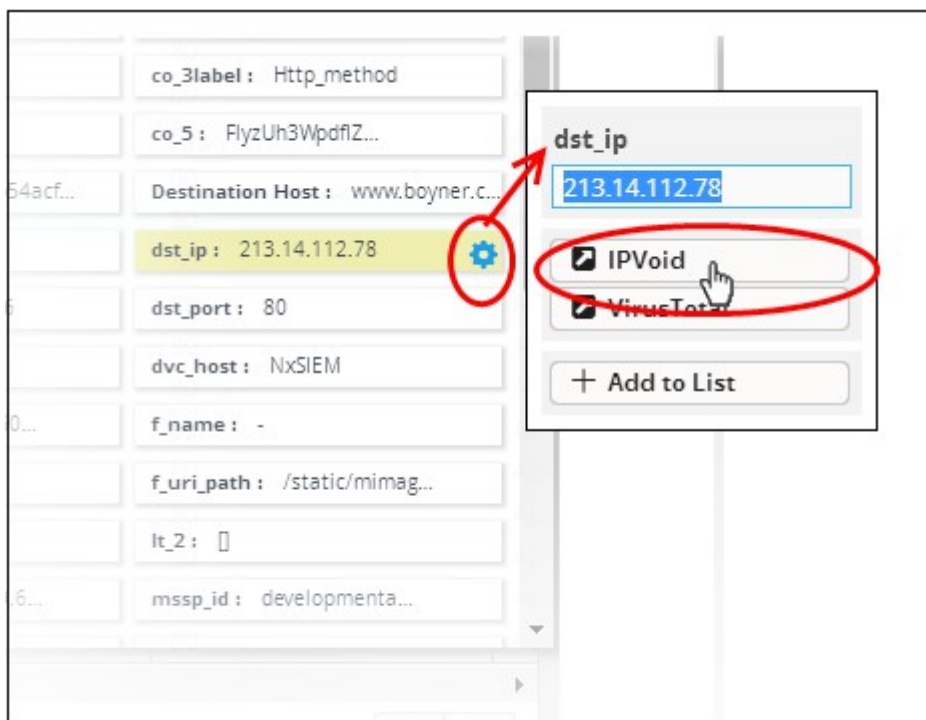
You can view the scan report containing IP address information and IP Blacklist Report for any external IP address detected in an event. The 'Details' pane of an event query result displays the detected external IP address field in yellow, which acts as a shortcut to perform the IP Look up through IPVOID website.

To perform IP Look up of External IP address

- Click on the event involving connection to an external network or host from the results table to open its 'Details' pane.

The fields containing external IP address(es) are highlighted in yellow as shown in the example below.

- Hover the mouse cursor over the field and click on the gear icon that appears at the right.
- Click on the 'IPVoid' option.



You will be taken to the IP Void webpage containing the scan results of the IP address.

An example is shown below.

IP Void

[Home](#)
[Scan IP Address](#)
[Statistics](#)
[FAQs](#)
[Contacts](#)

213.14.112.78 Scan Report

[Permalink](#) |
 [Email a Friend](#) |
 [Print this Page](#)

Update Report

IP Address Information

Analysis Date	2 months ago
Blacklist Status	POSSIBLY SAFE 0/39
IP Address	213.14.112.78 (Websites Lookup)
Reverse DNS	host-213-14-112-78.reverse.superonline.net
ASN	AS34984
ASN Owner	Turkcell Superonline İletisim Hizmetleri AS
ISP	Deksarnet Telekomunikasyon A.S.
Continent	Europe
Country Code	(TR) Turkey
Latitude / Longitude	41.0136 / 28.955
City	Unknown
Region	Unknown

IP Blacklist Report

Engine	Status
TornevallNET	✔ More details →
BlockList_de	✔ More details →
MyWOT	✔ More details →
SpamRATS	✔ More details →
DNSBL_AbuseCH	✔ More details →

Performing IP Address/Domain Lookup using Virus Total

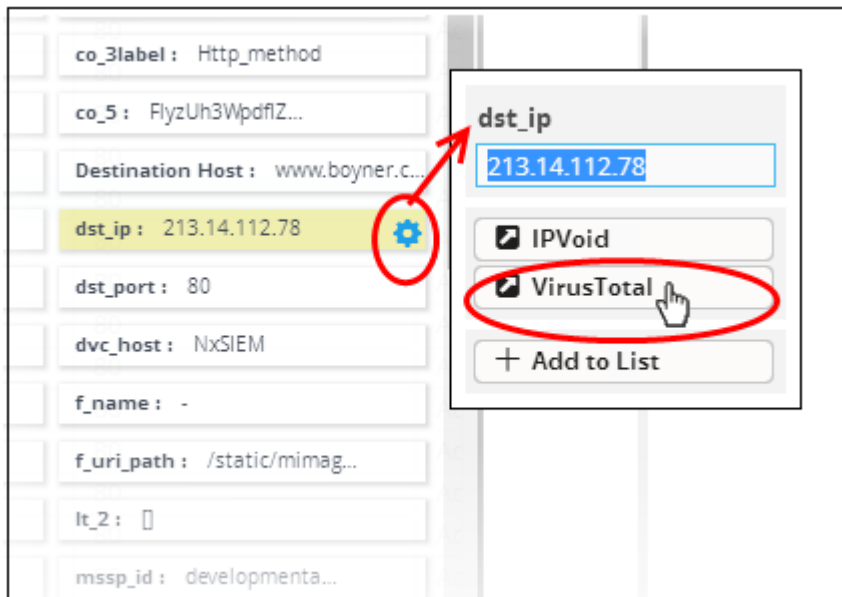
You can view the IP address information/Domain information for external IP addresses/domains detected in an event from the 'Virus Total' website. The 'Details' pane of an event query result displays the fields containing external IP address/domain names field in yellow, which acts as a shortcut to perform the look up.

To perform IP/Domain Look up using Virus Total

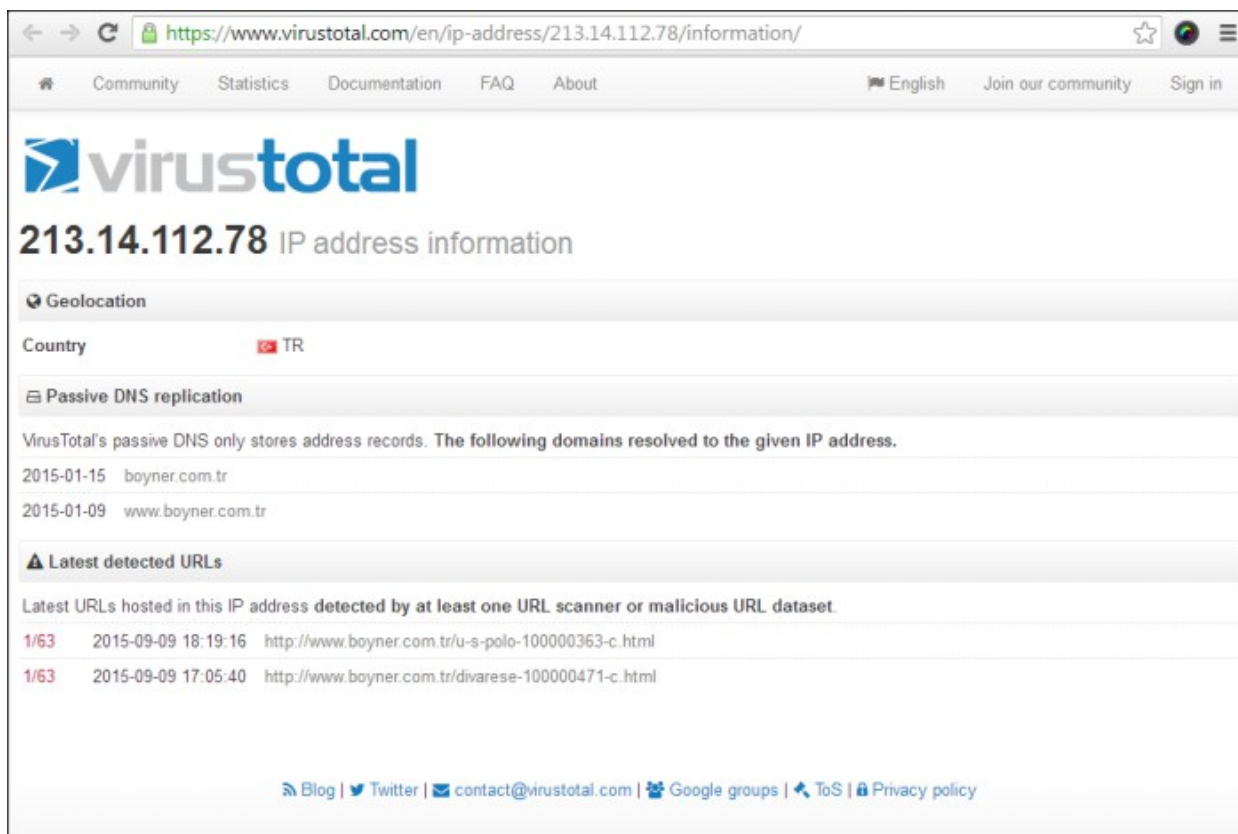
- Click on the event involving connection to an external network or host from the results table to open its 'Details' pane.

The fields containing external IP address/Domain name are highlighted in yellow as shown in the example below.

- Hover the mouse cursor over the field and click on the gear icon that appears at the right.
- Click on the 'Virus Total' option.



You will be taken to the Virus Total web page which contains information about the IP address/domain. An example is shown below.



Adding Field values to Live Lists from Results

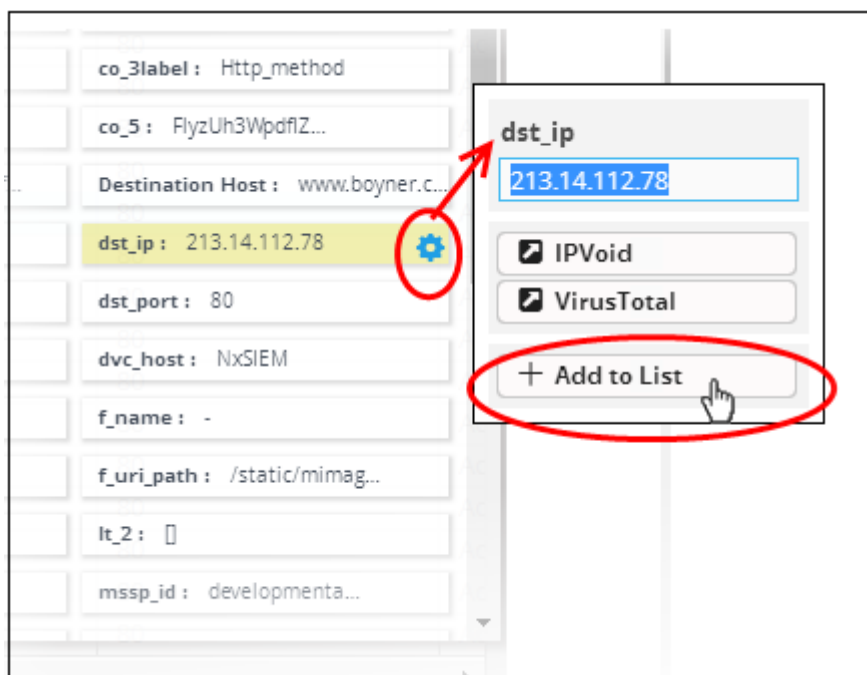
You can add values for certain fields detected in an event to Live Lists defined in cWatch Network, for use in other queries and correlation rules.

Background Note on Live Lists:

- Live lists let you add values for fields used in queries and correlation rules.
- Live lists can be updated manually or configured to fetch values by a correlation rule.
- List updates will be immediately reflected in the queries and the rules in which they are used.
- See **Live Lists** for more details on live list management.

To add a field value from an event to a live list:

- Click an event on the results table to open its 'Details' pane.
- Hover the mouse cursor over the field containing the value to be added to a list and click on the gear icon that appears at the right:



- Click on the 'Add to List' option.

The 'List Content Add' dialog will appear. The 'Value' field in the dialog is pre-populated with the chosen value.

List Content Add
×

Value

List Management

Due Date **Customer**

Permanent

- Select the 'Live List' and the list type to which the value is to be added, from the respective drop-downs under 'List Management'.
- Enter the date till which the value is valid in the 'Due Date' field. You can click the calendar icon at the left of

the field and choose the date. On the specified date, the value will be automatically removed from the list. If you want the value to be permanently valid, select the 'Permanent' checkbox.

- Select the customer to which the value is applicable from the 'Customer' drop-down.
- Click 'Submit'.

The value will be added to the respective 'List Type' and all the queries and correlation rules in which the list is deployed, will be updated immediately.

View Aggregated Results

- The 'Aggregations' tab lets you group responses from an event query.
- Events can be grouped based on values of selected fields to form event groups.
- Event groups can then be ranked based on the aggregation function selected and results can be viewed in ascending or descending order.

To view the aggregation of events

- Click the 'Aggregations' tab in the lower right pane of the 'Event Query' interface

The screenshot displays the 'Query Builder' interface. At the top, there are two tabs: 'New Query' and 'User_Modify_Password'. Below the tabs is the 'Query Builder' section, which includes a logical operator dropdown set to 'AND', a plus sign to add more conditions, and a single condition: 'agent' (with a dropdown arrow) followed by a minus sign and 'agent_id' (with a dropdown arrow), and a plus sign to add more conditions. Below the query builder is a toolbar with icons for 'Save', 'Save As', 'Move', and 'Schedule', along with a 'Last 8 hours' time range selector and a 'Search' button.

Below the query builder is the 'Results' section, which has two tabs: 'Results' and 'Aggregations'. The 'Aggregations' tab is active. It contains the 'Event Fields' section with 'agent' and 'agent_id' selected in dropdown menus, and a plus sign to add more fields. Below this is a list of event fields with up and down arrows for sorting and a trash icon for removal. The 'Aggregation Function' is set to 'Count'. The 'Order By' is set to 'Descending' and the 'Limit' is set to '500'. A 'Submit' button is located at the bottom left of the 'Aggregations' tab.

Aggregating events involves four steps:

- **Step 1 - Select the event field(s) on which events are to be grouped**
- **Step 2 - Select the aggregation function**
- **Step 3 - Select the order of ranking based on how you want to see the aggregation results**

- **Step 4 - Set the limit for number of results to be displayed**


Step 1 - Select the event field(s) by which events should be grouped

The first step is to choose the event fields by which the events should be grouped. Event groups will be formed so that each event group will have events with same value for the selected field. If you select more than one field, the combinations of values in the selected fields will be taken into account for grouping.

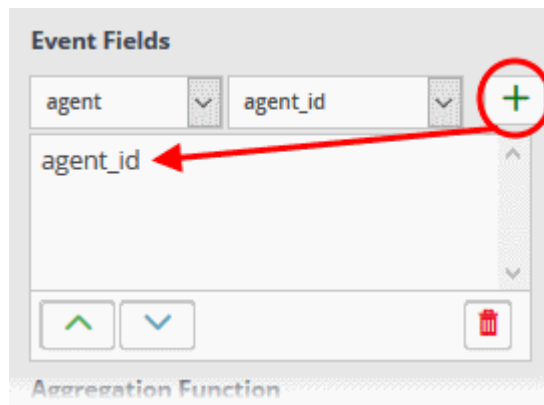
To select the event field(s) for grouping

- Choose the 'Field Group' from the first drop-down under 'Event Fields'

The next drop-down will be populated with the fields belonging the chosen group

- Choose the 'Field' from the second drop-down and click the  button.

The field will be added to the list below 'Event Fields'



- Repeat the process to add more fields for grouping.
- You can re-position fields by selecting them then clicking the up/down arrow buttons at bottom-left

Step 2 - Select the aggregation function

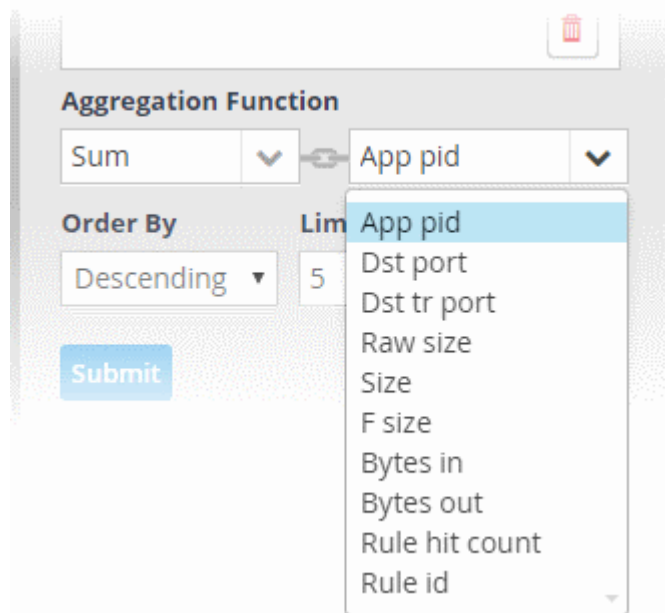
The event groups formed based on the fields chosen in the first step are ranked based on the function chosen from the 'Aggregation Function' drop-down. The available options are:

- **Count** - The event groups are ranked based on the number of events in each group.
 - For example, if you choose Source IP as 'Field', then the group which contains the most events on a particular source IP will have the top rank. The group containing the least events is ranked lowest.
 - You can further control how the data is displayed by modifying the 'Order By' and 'Limit' parameters.
- **Sum** - The event groups are ranked based on sum of values in another field that contains numerical value.
 - If you choose 'Sum', you need to select another field that contains a numerical value, like 'Bytes in/out'.
 - Event groups are ranked based on the sum of the values in the chosen numerical field from all the events in that group.
 - For example, if we choose 'Bytes-in' as numerical value, then the system adds up the values in the 'Bytes-in' field of all events in the group and ranks the group accordingly. This will tell you which source IP has the most incoming traffic.
 - The event group with the highest SUM in the 'Bytes-in' field is ranked top and vice-versa.
- **Average** - Similar to above.
 - Event groups are ranked based on the average values of the chosen numerical field from all the events in that group.
 - For example, the average of values of 'Bytes_in' field of events in the group, if we take the same example as above
- **Minimum** - Similar to above. The event groups are ranked based on the minimum of the values of chosen numerical field from all the events in that group.

- **Maximum** - Similar to above. The event groups are ranked based on the maximum of the values of chosen numerical field from all the events in that group.

To set the aggregation function

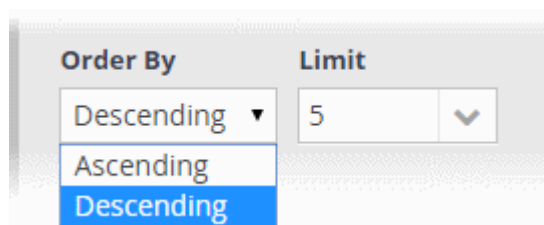
- Choose the function from the 'Aggregation Function' drop-down.
- If you choose 'Sum', 'Average', 'Maximum' or 'Minimum', then you should choose an item which is it useful to measure.
 - For example, 'Bytes-in' can be measured and is suitable for the Sum, Average, Max and Min functions.
 - On the other hand, there would be little value in applying these functions to destination port numbers.



Step 3 - Select the order of ranking based on how you want to see the aggregation results

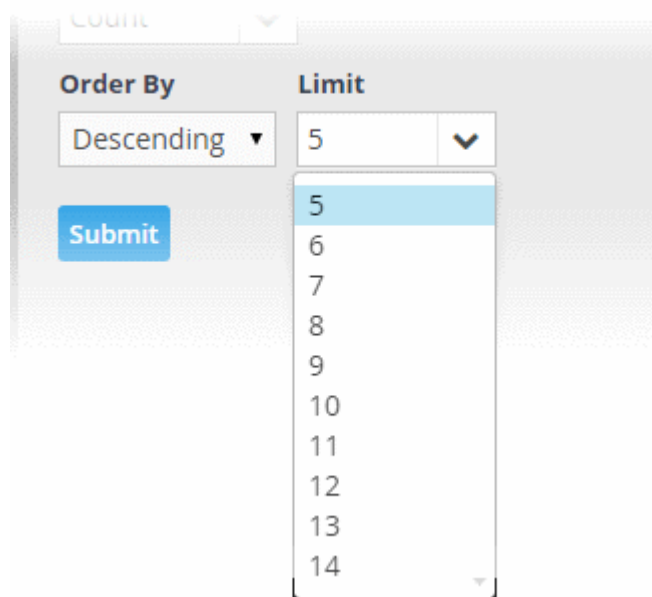
You can choose how event groups should be ranked from the 'Order By' drop-down. The available options are:

- **Ascending** - The group with the lowest rank will be top of the list. A limit of 5 will show the 5 groups with the lowest ranks.
- **Descending** - The group with the highest rank will be top of the list.. A limit of 5 will show the 5 groups with the highest ranks.



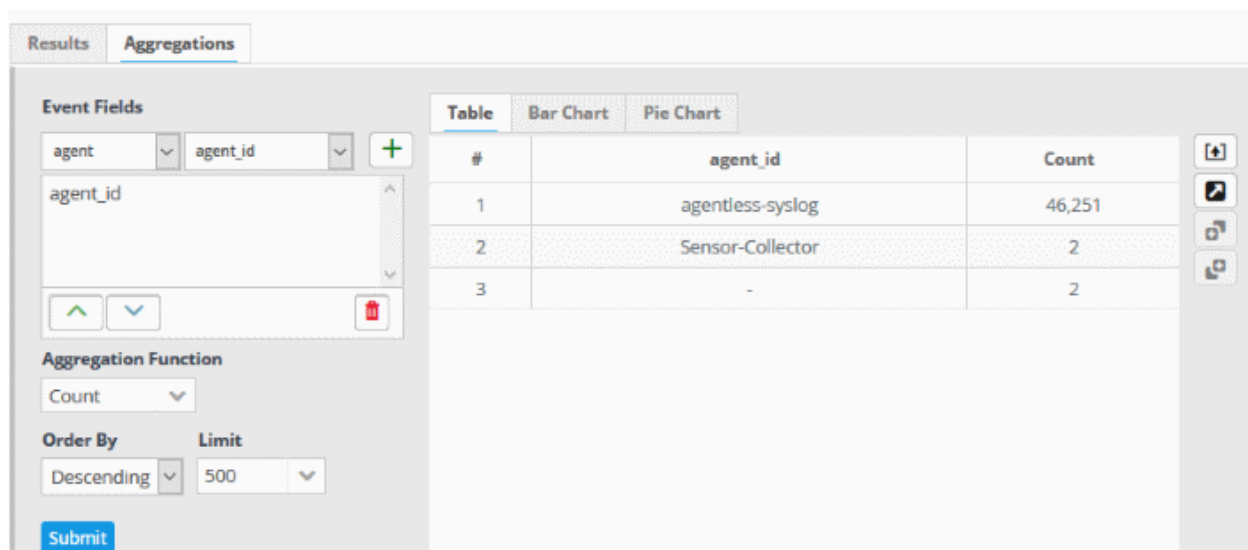
Step 4 - Set the limit for number of results to be displayed

The last step is to set a limit for the number of event groups to be displayed as aggregation results in ascending or descending order as chosen in the previous step.



- To set the limit, choose/enter the number of results to be displayed, in the 'Limit' drop-down combo box.
- Click 'Submit'.

The results will be displayed in the Aggregation Results pane at the right.




Updating an Event Query

Event queries can be updated and refined at any time from the 'Event Query' Interface. For example, you may wish to add new filters or to remove filters that offer little value.

To update a query

- Select the customer from the 'Customers' drop-down at the top of the left hand side panel.
- Choose the query to be updated, from the 'Queries' list at the left.

The query with its filter statements will be displayed in a new tab at the right panel

- To delete a filter , click the  button beside it.
- To add a new filter, follow the **process explained** in **Creating a New Event Query**.

To refine the query by adding a new filter(s) from the results

- Run the query as explained in the section **Run an Event Query**.

The results will be displayed in the lower pane in the 'Results' tab.

Query Builder

agent - agent_id

Save Save As Move Schedule Last 8 hours **Search**

Results Aggregations

Time: (2018-04-18 00:49:43 - 2018-04-18 08:49:43) Total Count: 49072

Central Time	Device Host	Application Name	Name	Message	Source IP	Source Port
2018-04-18 08:49:13.107	SOCUA	NxSensor_conn			10.100.164.34	62792
2018-04-18 08:49:12.420	SOCUA	NxSensor_files	SSL		34.231.200.228	0
2018-04-18 08:49:11.272	SOCUA	NxSensor_ssl	TLSv12		10.100.164.34	62789
2018-04-18 08:49:09.315	SOCUA	NxSensor_files	SSL		52.59.61.93	0
2018-04-18 08:49:09.280	SOCUA	NxSensor_ssl	TLSv12		10.100.164.34	62788
2018-04-18 08:49:05.308	SOCUA	NxSensor_dns	SRV		10.100.164.34	53411
2018-04-18 08:49:03.428	SOCUA	NxSensor_files	SSL		52.59.61.93	0
2018-04-18 08:48:53.323	SOCUA	NxSensor_conn			10.100.164.32	64097
2018-04-18 08:48:48.970	SOCUA	NxSensor_conn			10.100.164.164	137
2018-04-18 08:48:38.189	SOCUA	NxSensor_ssl	TLSv12		10.100.164.46	35630
2018-04-18 08:48:38.046	SOCUA	NxSensor_conn			10.100.164.46	35630
2018-04-18 08:48:38.044	SOCUA	NxSensor_dns	A		10.100.164.46	53159
2018-04-18 08:48:38.044	SOCUA	NxSensor_dns	AAAA		10.100.164.46	53159

- Click on the result, to view its details, from which new filters are to be added to the query.

Results Aggregations

Time: (2018-04-18 01:48:54 - 2018-04-18 09:48:54) Total Count: 45993

Central Time	Device Host	Application Name	Name
2018-04-18 09:46:36.335	SOCUA	NxSensor_dns	SRV
2018-04-18 09:46:34.207	SOCUA	NxSensor_ssl	TLSv12
2018-04-18 09:46:34.532	SOCUA	NxSensor_ssl	TLSv12
2018-04-18 09:46:34.072	SOCUA	NxSensor_ssl	TLSv12
2018-04-18 09:46:33.910	SOCUA	NxSensor_ssl	TLSv12
2018-04-18 09:46:33.032	SOCUA	NxSensor_ssl	TLSv12
2018-04-18 09:46:32.997	SOCUA	NxSensor_conn	
2018-04-18 09:46:31.110	SOCUA	NxSensor_conn	
2018-04-18 09:46:30.609	SOCUA	NxSensor_conn	
2018-04-18 09:46:30.364	SOCUA	NxSensor_conn	
2018-04-18 09:46:30.364	SOCUA	NxSensor_conn	
2018-04-18 09:46:22.852	SOCUA	NxSensor_conn	
2018-04-18 09:46:20.584	SOCUA	NxSensor_conn	
2018-04-18 09:46:11.797	SOCUA	NxSensor_ssl	TLSv12
2018-04-18 09:46:11.743	SOCUA	NxSensor_conn	
2018-04-18 09:46:11.743	SOCUA	NxSensor_dns	A
2018-04-18 09:46:00.662	SOCUA	NxSensor_dns	NB
2018-04-18 09:45:59.911	SOCUA	NxSensor_dns	NB
2018-04-18 09:45:59.602	SOCUA	NxSensor_dns	NB
2018-04-18 09:45:59.161	SOCUA	NxSensor_conn	

Selected Result Fields Details Filter Raw Log

agent_time: 2018-04-18 09:46:36.335
Application Name: NxSensor_dns

bytes_in: 0
bytes_out: 0

Central Time: 2018-04-18 09:46:36.335
customer_id: CUST0937a06...

Destination IP: 10.255.81.2
Destination Port: 53

Device Host: SOCUA
duration: 0

event_id: rpfyMgRZg...
it_1: AssetList

Name: SRV
prod_name: NxSensor_Dns

prod.vendor: Comodo
rcvd_pkt: 0

session_id: CBKvphKyAN...
Source IP: 10.100.164.34

Source Port: 53650
trans_proto: udp

Type: Access

Page 1 of 2300

The 'Selected Results Fields' pane will appear for the event log entry, with values for all the fields.

- Click one or more fields from the 'Selected Results Fields' tab

The screenshot illustrates the process of creating a new query with filters. It shows a table of results, a detailed view of a selected event, a query builder interface, and a 'New Query' window. Red annotations highlight the 'Filter (10)' tab, the 'prod_name' field in the details view, and the 'Save' and 'New Query' buttons in the query builder.

Central Time	Device Host	Application Name
2018-04-18 11:58:45.703	SOCUA	NxSensor_conn
2018-04-18 11:58:36.625	SOCUA	NxSensor_ssl
2018-04-18 11:58:36.485	SOCUA	NxSensor_conn
2018-04-18 11:58:36.421	SOCUA	NxSensor_dns
2018-04-18 11:58:36.421	SOCUA	NxSensor_conn
2018-04-18 11:58:36.421	SOCUA	NxSensor_dns
2018-04-18 11:58:34.885	SOCUA	NxSensor_conn
2018-04-18 11:58:34.884	SOCUA	NxSensor_conn
2018-04-18 11:58:24.082	SOCUA	NxSensor_conn
2018-04-18 11:58:23.582	SOCUA	NxSensor_conn
2018-04-18 11:58:05.695	SOCUA	NxSensor_conn
2018-04-18 11:58:04.481	SOCUA	NxSensor_weird
2018-04-18 11:57:54.875	SOCUA	NxSensor_conn



Selected Result Fields | **Details** | **Filter (10)** | **Raw Log**

Selected Result Fields | **Details** | **Filter (10)** | **Raw Log**

Query Builder

New Query x | **User_Modify_Password** x | **New Query** x

These fields will be added to the 'Filter' tab

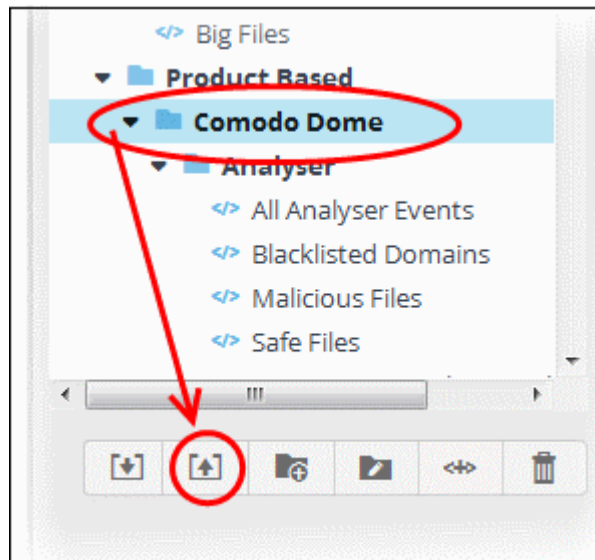
- To save the query with the new filter, click .
- To create a new query with the existing and newly added filters, leaving the existing query unchanged, select the category folder from the left click  and save the new query with a new name.
- You can select the specific time period to create a query or save to the current query.
- See '**View Results Table**' for more details on 'Raw Logs'

Export Event Queries

- You can save event queries in order to use them for other customers.
- You can export a query folder or a particular query.
 - Please note - exported event queries can only be imported to their respective sections. For example, event queries exported from the reports section can only be used in the report section. Also, the values in the filter items in the exported events for tagged and list events will be set to default values.

To export a query or query folder

- Select the customer from the 'Customers' drop-down at the top of the left hand side panel.
- Choose the query or query folder to be exported, from the 'Queries' list at the left.
- Click the 'Export' button at the bottom



The file with extension 'nxm' will be downloaded to the default download location.

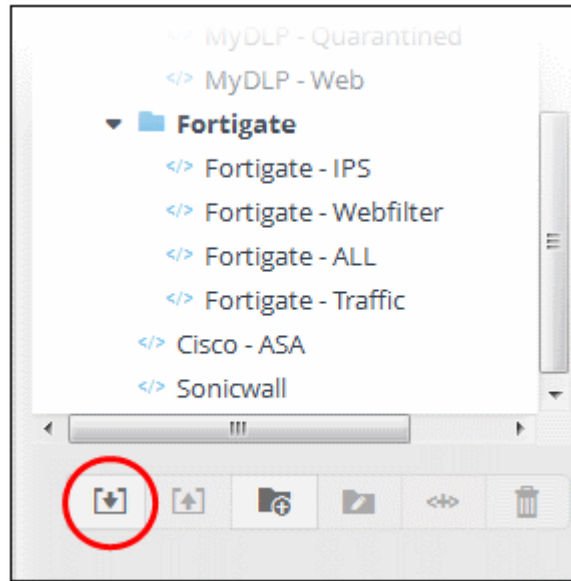
The saved query can be imported for use another customer account.

Import Event Queries

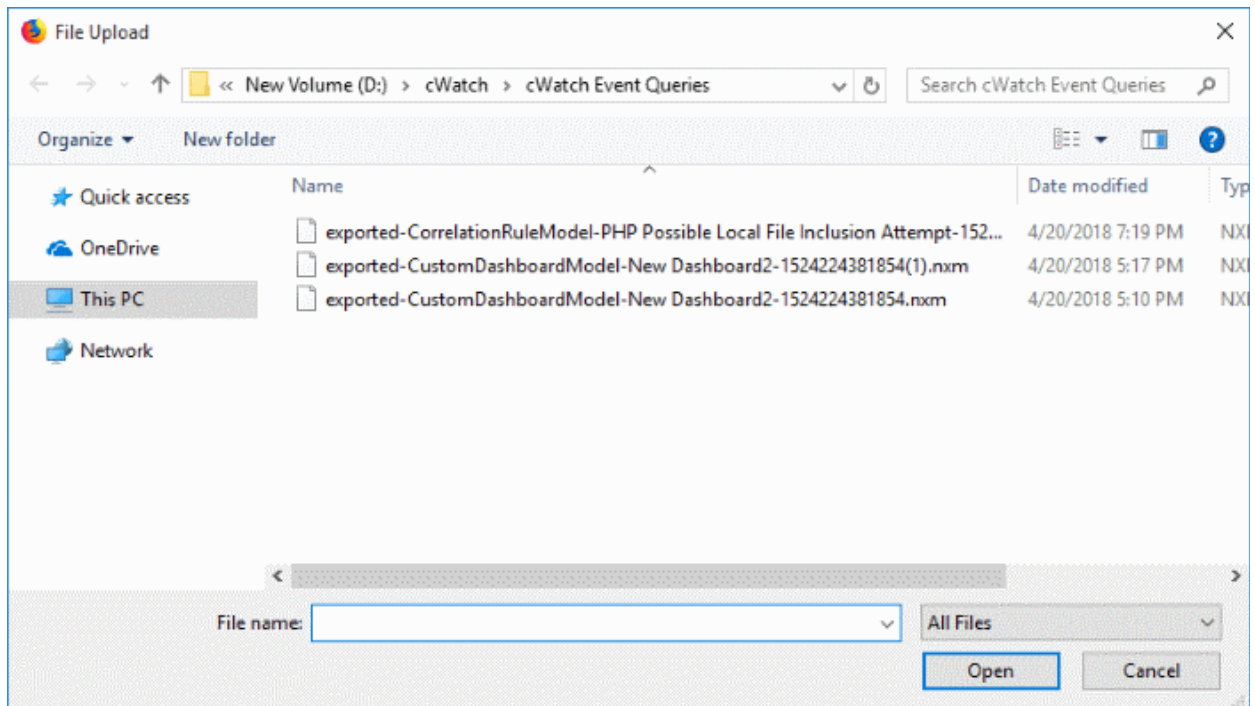
- You can import saved event queries to use them for other customers.
- Imported queries can be used as is or altered to suit the requirements of the customer.
 - Please note - exported event queries can only be imported to their respective sections. For example, event queries exported from the reports section can only be used in the report section. Also, the values in the filter items in the exported events for tagged and list events will be set to default values.

Import a query or query folder

- Select the customer from the 'Customers' drop-down at the top of the left hand side panel for which you want to import the saved queries
- Click the 'Import' button at the bottom

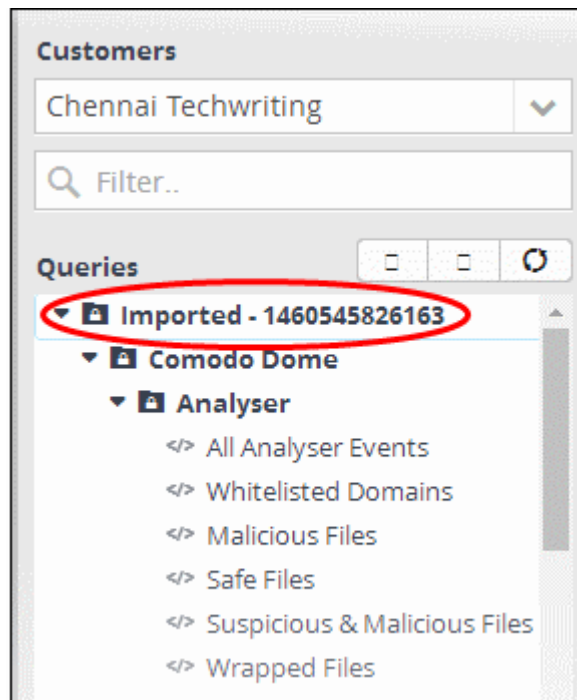


- Navigate to the location where the event query file is saved.



- Select the file and click 'Open'

The event query or event query folder will imported and will be listed under 'Imported' folder.



You can **run the queries** as it is or **alter** according to your requirement.

Exporting Query Results to a CSV file

Administrators can save the query results by exporting it as a CSV file for future use. Please note the query results available in the opened page will only be exported.

Export a query result

- Select the customer from the 'Customers' drop-down at the top of the left hand side panel.
- Choose the query whose results to be exported, from the 'Queries' list at the left.

The Query with its filter statements will be displayed in a new tab at the right panel

- Run the query as explained in the section **Run an Event Query**.

The Results will be displayed in the lower pane under the 'Results' tab.

Results		Aggregations			
time	Source IP	Source Port	Name	Target Port	Me
2016-04-12 13:15:39.973	54.239.22.240	0	HTTP	0	1460456135
2016-04-12 13:15:39.861	104.20.87.108	0	HTTP	0	1460456135
2016-04-12 13:15:39.839	10.0.33.57	0	HTTP	0	1460456135
2016-04-12 13:15:39.823	10.100.130.217	34694	GET	80	1460456135
2016-04-12 13:15:39.812	213.14.112.66	0	SSL	0	1460456135
2016-04-12 13:15:39.773	10.100.136.151	43020		443	Invalid vers
2016-04-12 13:15:39.756	10.100.130.253	56101	GET	80	1460456135
2016-04-12 13:15:39.755	10.100.136.151	57233		443	Invalid vers
2016-04-12 13:15:39.730	213.14.112.78	0	HTTP	0	1460456135
2016-04-12 13:15:39.725	91.235.64.155	0	HTTP	0	1460456135
2016-04-12 13:15:39.719	213.14.112.78	0	HTTP	0	1460456135
2016-04-12 13:15:39.699	10.100.136.151	41554		443	Invalid vers
2016-04-12 13:15:39.698	10.100.130.253	56039	GET	80	1460456135
2016-04-12 13:15:39.697	10.100.130.253	56078	GET	80	1460456135

- Click the 'Export' button above the results table header

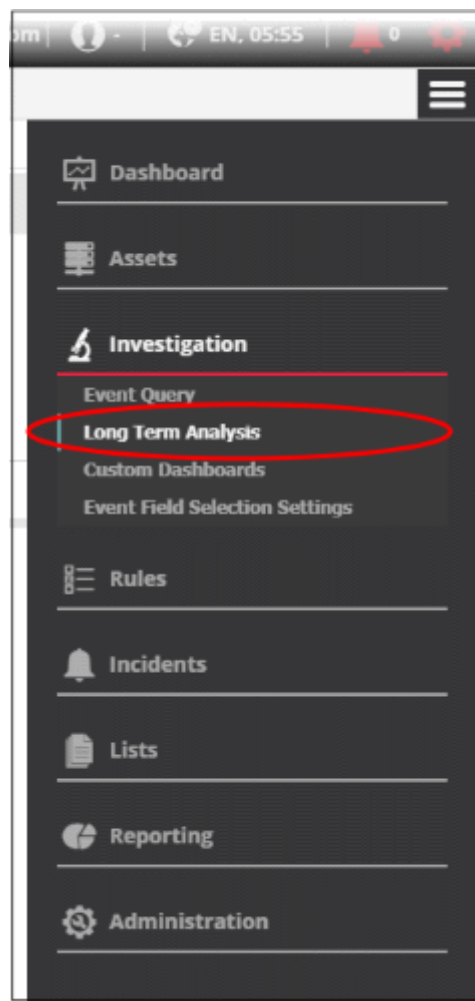
Results		Aggregations			
Time: (2016-04-06 11:53:31 - 2016-04-13 11:53:31) Total Count: 12979187					
time	Source IP	Source Port	Name	Target Port	Export
2016-04-12 13:15:39.973	54.239.22.240	0	HTTP	0	1460456135
2016-04-12 13:15:39.861	104.20.87.108	0	HTTP	0	1460456135
2016-04-12 13:15:39.839	10.0.33.57	0	HTTP	0	1460456135

The file will be downloaded to the default download folder.

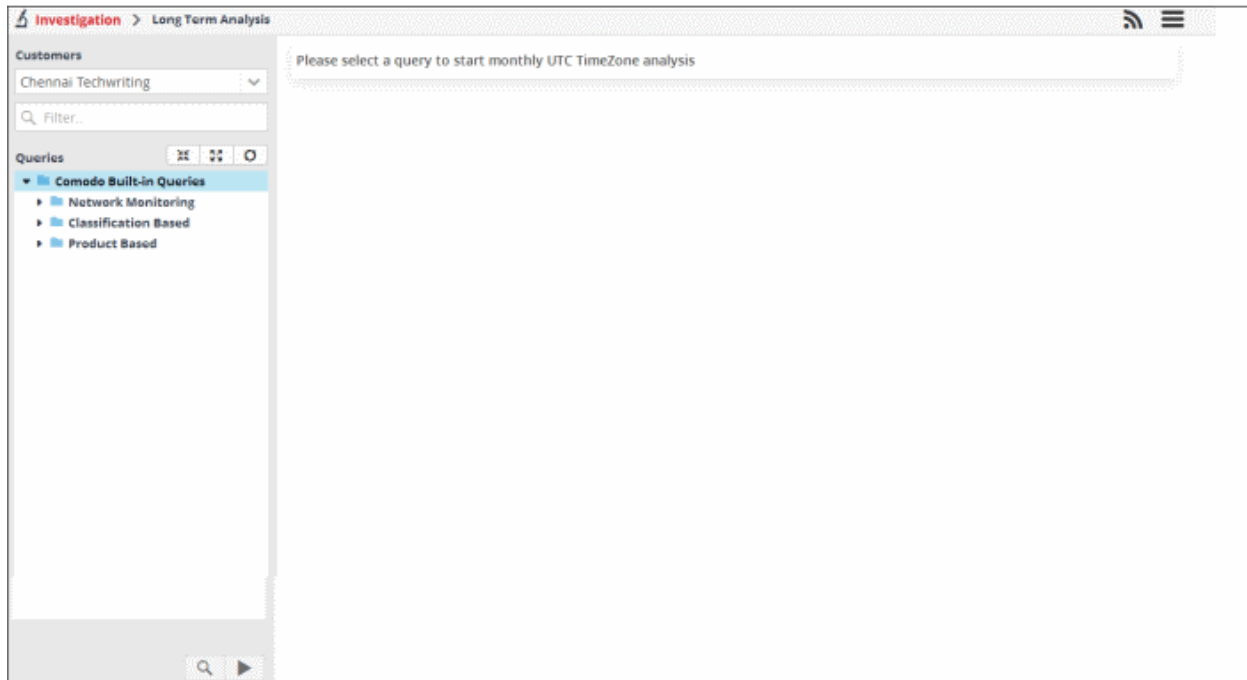
4.2 Long Term Analysis

Results for event queries (see '**Configure Event Queries**') are available for a maximum of seven days. To analyze results older than seven days you need to use the 'Long Term Analysis' interface. Results are available for up to four weeks in the past.

- Click the 'Menu' button > 'Investigation' > 'Long Term Analysis'.



The 'Long Term Analysis' screen will open:



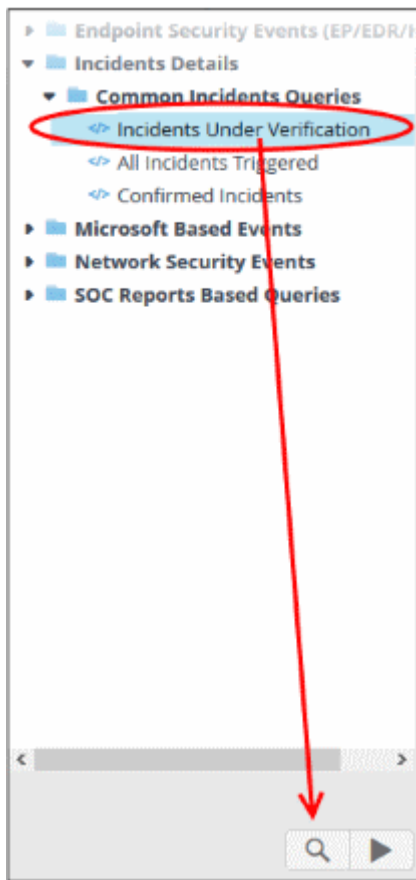
The default customer that was **configured** under the settings is shown in the left pane. A list of predefined and custom queries for the customer is shown under 'Queries'. The main panel will be blank and after pressing the play button at the bottom, will show the monthly results for the selected query.

Correlation Rules Management - Table of controls	
	The 'Customers' drop-down allows you to select the customer for which you want to analyze the long term query results.
	Allows you to search for a particular query. Enter the name of the query fully or partially and click on the search icon or press 'Enter'. Queries matching the entered text will be listed. To view the full list of queries again, clear the search field and press 'Enter'
	Expand, collapse or refresh the list of queries. Click the refresh button at the end to instantly update the query list.
	Allows you to preview the parameters of a selected query.
	Click this button to start the search for the selected query.

To preview the parameters of a query

- Select a customer from the 'Customers' drop-down at the top of the left hand panel.
- Select the query for which you want to preview the parameters

- Click the search icon at the bottom of the left menu



The preview of the selected query will be displayed.

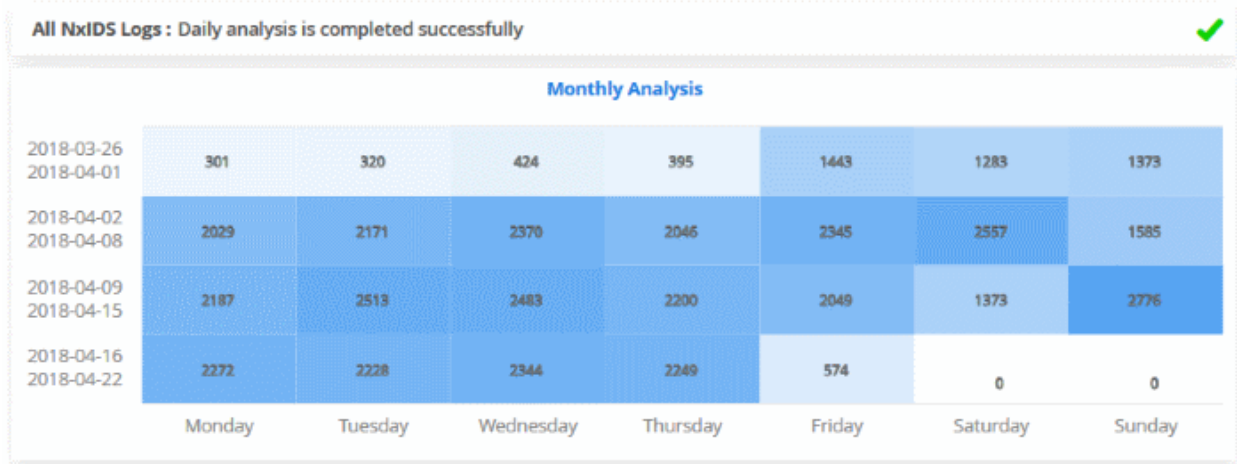


Please note that you cannot edit or update the query from this screen. Click 'X' to close the dialog.

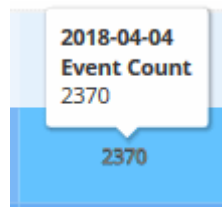
To search for monthly query results

- Select the customer from the 'Customers' drop-down at the top of the left hand panel.
- Select the query for which you want to view the monthly results
- Click the play button at the bottom of the left menu

The monthly analysis for the selected query will be displayed.



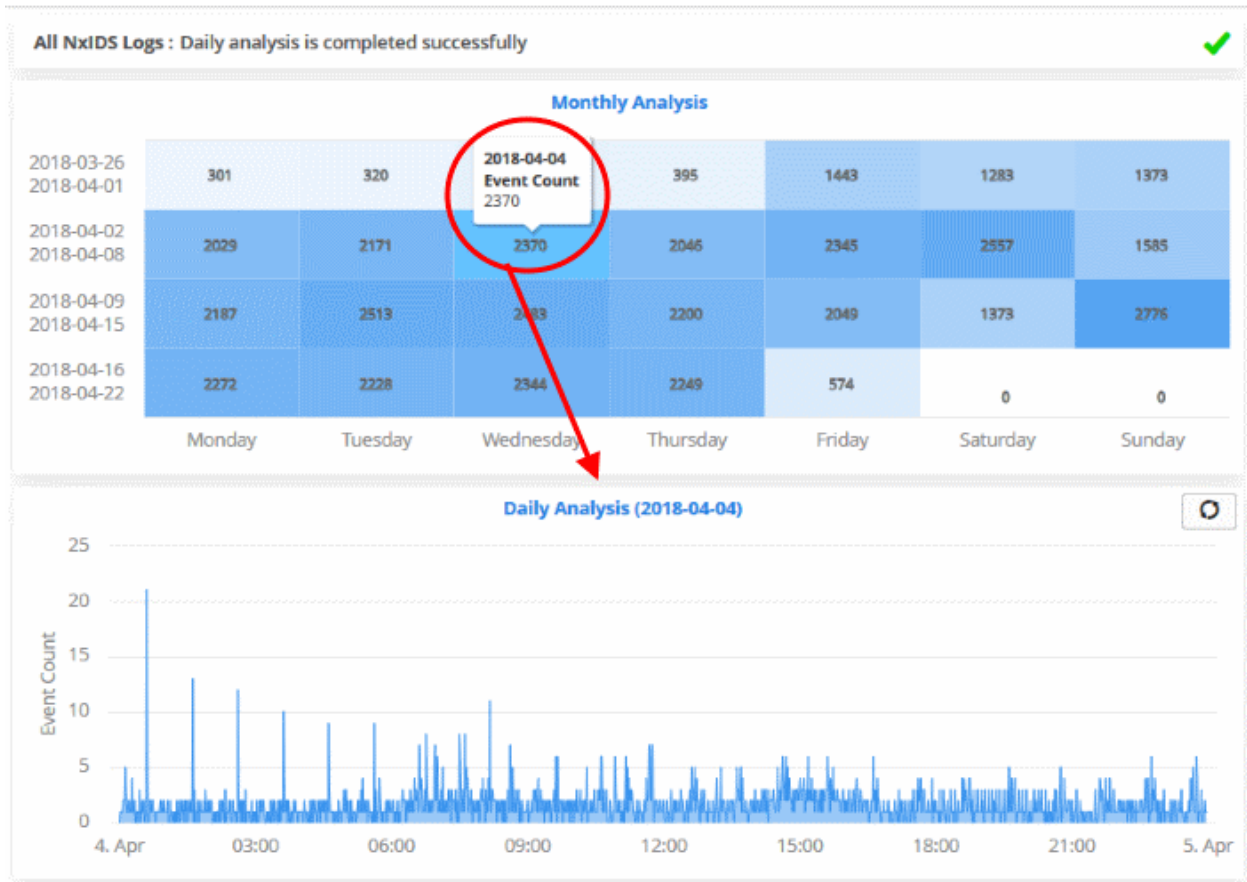
- The data will be shown as a heat map, displaying the number of events for the past four weeks.
- Place your mouse cursor over an event count to view the date it occurred and the number of events.



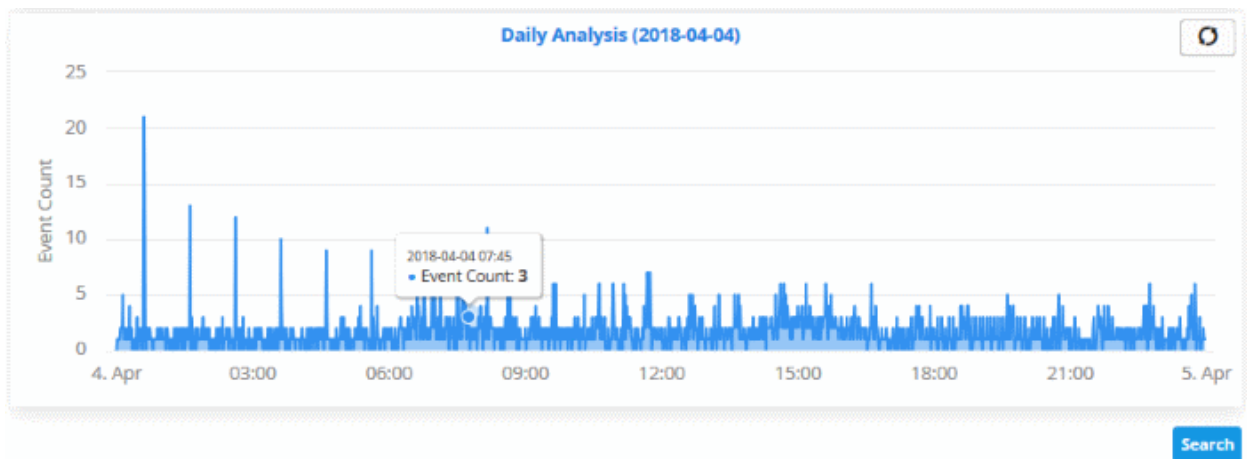
To search query results for a selected day of the week

- Click on a day of the week to view the results for the selected query

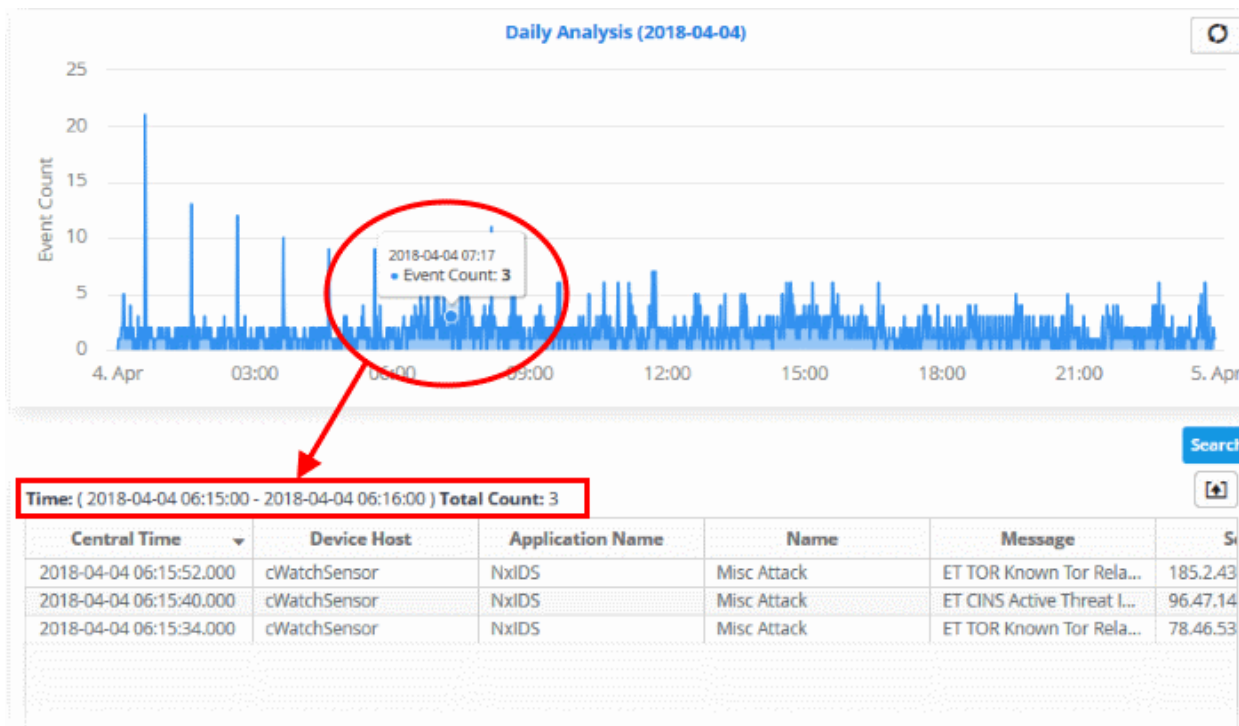
The daily analysis graph details will be displayed below the monthly analysis table.



- The number of events is displayed on the 'X' axis
- The time of the events is shown on the 'Y' axis
- Place your mouse cursor on a particular point to view the number of events at that time.



- Click on a particular time to view more details in a table below the graph.



The table displays details of events that happened during the selected period. See **'View Results Table'** in **'Configuring Event Queries'** for more information on event details.

- To view the full event results table for a particular day, click the day from the table. The 'Daily Analysis' for that particular day will be displayed.



- Click the 'Search' button.

The event results table for the selected date will be displayed:

Time: (2018-04-04 06:15:00 - 2018-04-04 06:16:00) Total Count: 3

Central Time	Device Host	Application Name	Name	Message	Source IP
2018-04-04 06:15:52.000	cWatchSensor	NxIDS	Misc Attack	ET TOR Known Tor Rela...	185.2.43
2018-04-04 06:15:40.000	cWatchSensor	NxIDS	Misc Attack	ET CINS Active Threat I...	96.47.14
2018-04-04 06:15:34.000	cWatchSensor	NxIDS	Misc Attack	ET TOR Known Tor Rela...	78.46.53

Please note that only last 1000 events for the selected date will be displayed even if the number of events exceeds that number. If the results for a query exceeds 1000, it means that the query is not properly configured and should be reconfigured.

- Clicking on an event will display its details.

Time: (2018-04-04 06:15:00 - 2018-04-04 06:16:00) Total Count: 3

Central Time	Device Host	Application Name	Name	Message	Source IP
2018-04-04 06:15:52.000	cWatchSensor	NxIDS	Misc Attack	ET TOR Known Tor Rela...	185.2.43
2018-04-04 06:15:40.000	cWatchSensor	NxIDS	Misc Attack	ET CINS Active Threat I...	96.47.14
2018-04-04 06:15:34.000	cWatchSensor	NxIDS	Misc Attack	ET TOR Known Tor Rela...	78.46.53

Details Filter

Application Name: NxIDS	Central Time: 2018-04-04 06:15:52.000
Destination IP: 10.100.130.242	Destination Port: 43291
Device Host: cWatchSensor	Message: ET TOR Know...
Name: Misc Attack	Source IP: 185.2.43.87
Source Port: 443	Type: Intrusion Dete...

See **'View Results Table'** in **'Configuring Event Queries'** for more information about event details.

To export a long term query result to a CSV file

- Click the 'Export' button above the results table header

Time: (2018-04-04 06:15:00 - 2018-04-04 06:16:00) Total Count: 3

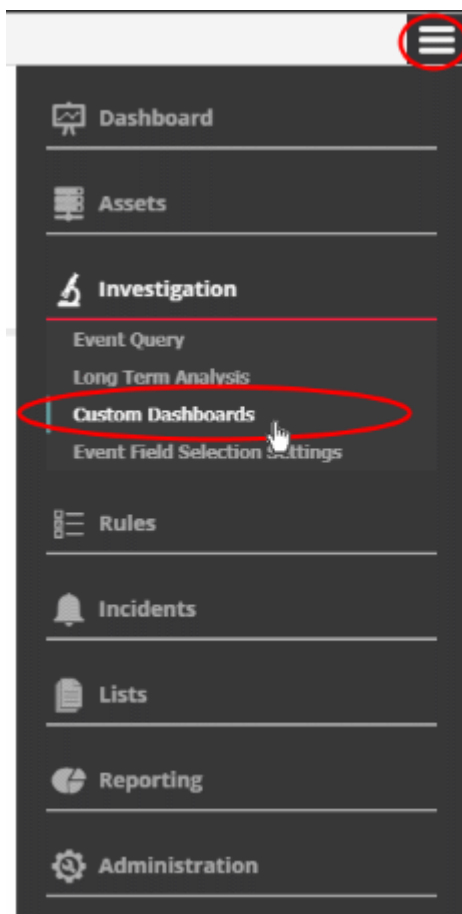
Central Time	Device Host	Application Name	Name	Message	Source IP
2018-04-04 06:15:52.000	cWatchSensor	NxIDS	Misc Attack	ET TOR Known Tor Rela...	185.2.43
2018-04-04 06:15:40.000	cWatchSensor	NxIDS	Misc Attack	ET CINS Active Threat I...	96.47.14
2018-04-04 06:15:34.000	cWatchSensor	NxIDS	Misc Attack	ET TOR Known Tor Rela...	78.46.53

Export

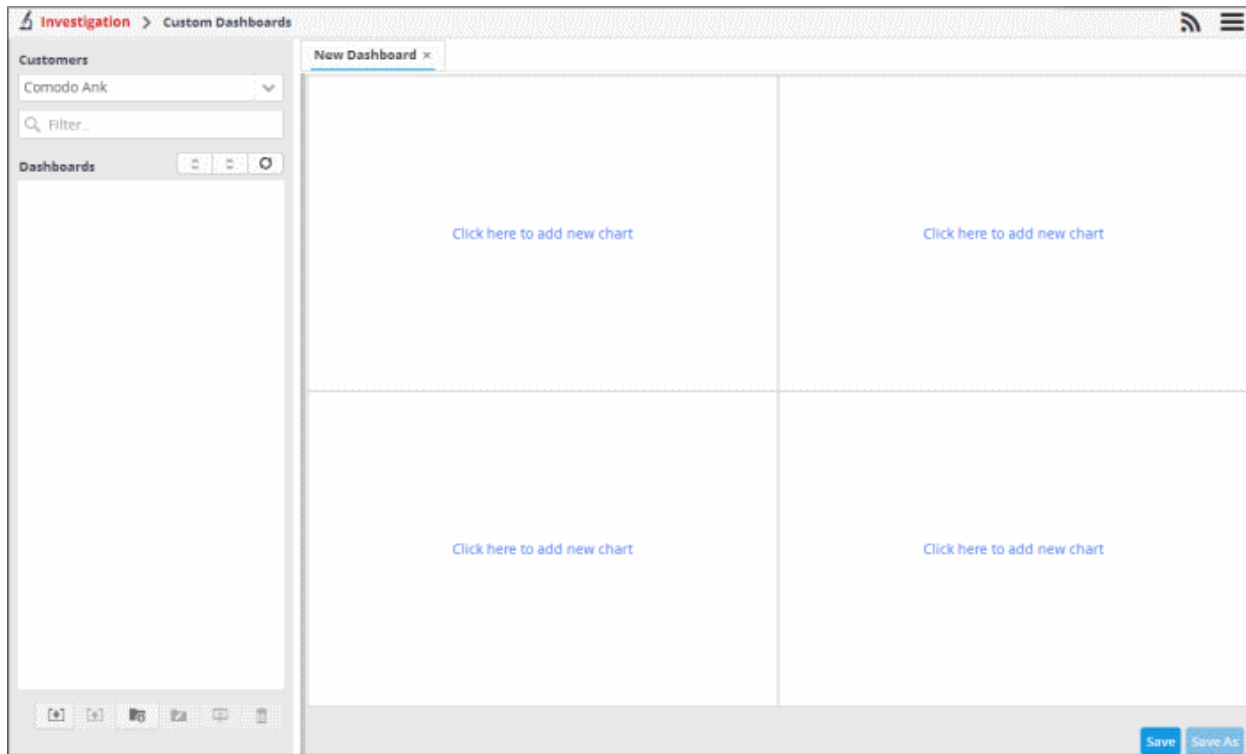
The file will be downloaded to the default download folder.

4.3 Configure Custom Dashboards

- The custom dashboards area lets you view query results as charts. This allows you to see data from often complex queries in an easily digested format. See '[Configure Event Queries](#)' if you need to learn how to create queries.
 - Click the 'Menu' button at top-right
 - Choose 'Investigation'
 - Click 'Custom Dashboards':






The custom dashboards area is initially a blank palette, awaiting your first custom dashboard:



- The left-hand panel shows custom queries for each customer. Select a customer and a query to view the custom dashboard for that query on the right.
- Each dashboard can contain four charts per query.

Custom Dashboards Interface - Table of controls

<p>Customers</p> <p>Comodo Ank</p> <p>Chennai Techwriting</p> <p>Comodo Ank</p> <p>Milkyway Inc.</p> <p>Test Benchmark1</p> <p>Test Benchmark2</p> <p>Test Benchmark3</p>	<p>Select the customer for whom you want to query events and/or add custom queries.</p>
<p>Filter..</p>	<p>Allows you to search for a particular query. Enter the name of the query fully or partially and click on the search icon or press 'Enter'. The queries matching the entered text will be listed. To view the full list of queries again, clear the search field and press 'Enter'.</p>
<p>[Expand] [Collapse] [Refresh]</p>	<p>Allows you to expand or collapse the list of queries. To collapse, click the first button and to expand it, click the second button. Click the refresh button at the end to instantly update the query list.</p>
<p>[Import]</p>	<p>Allows you to import saved queries to configure and view as custom dashboard</p>
<p>[Export]</p>	<p>Allows you to export queries</p>
<p>[Add Folder]</p>	<p>Allows you to add a new 'Dashboards' folder to the left side panel</p>

	Allows to edit the name of a 'Dashboards' folder
	Allows you to add a new dashboard by selecting an event query added for the selected customer.
	Allows to delete selected dashboards folders or dashboards.


The interface allows administrators to:

- **Manage dashboard folder**
- **Configure a custom dashboard**
- **Create an event query for specific events from the Dashboard**
- **Edit a dashboard tile**
- **Delete a dashboard tile**
- **Import queries to custom dashboard**
- **Export queries from custom dashboard**

Managing Dashboard Folders

You can create and manage dashboard folders to accommodate the custom dashboards of specific type and to display them as tree structure.

To create a new Dashboard Folder

- Select the parent folder under which you wish to create a new folder
- Click the  button at the bottom of the screen.

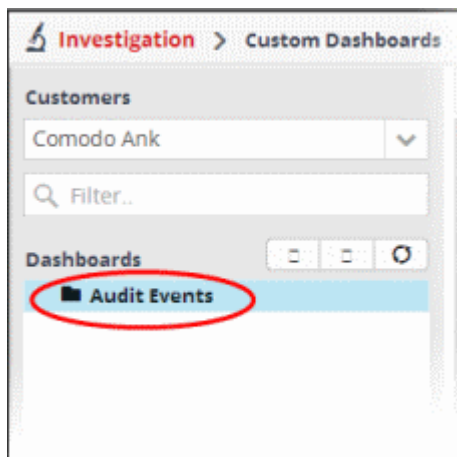
Folder Name
×

Folder Name :

Private

- Enter a name for the folder
- Private - This option will be available for first level folders. If selected, the folder will be accessible only for the user who created it and the administrator. Other users will not be able to access the folder.
- Click the 'Add' button

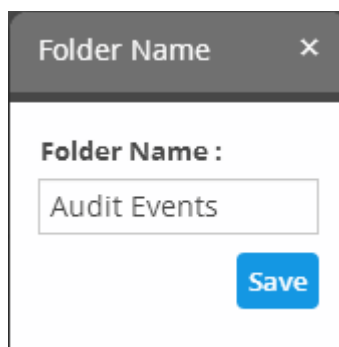
The folder will be saved and displayed on the left side. For private folders, a lock icon will be displayed over the folder.



You can add new dashboards under the folder.

To edit the name of a dashboard folder

- Select the folder and click the  button at the bottom

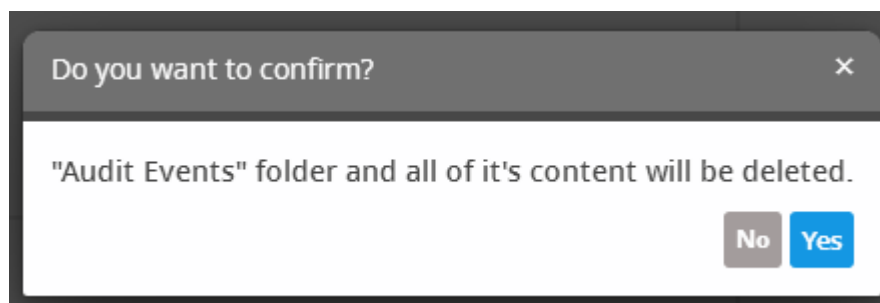


- Edit the name as required and click the 'Save' button

To delete a custom dashboard folder

- Select the folder and click the  button at the bottom.

A confirmation dialog will appear.



- Click 'Yes' to confirm the deletion.

Configuring Custom Dashboards

- You can add any number of custom dashboards for a customer for different event queries.

- If required, you can create new queries specifically for custom dashboards and save them, from the Custom Dashboard > Add dialog. You can also add existing queries.
- See **Manage an Event Query** in **Configuring Event Queries**, for a tutorial on creating new queries

Each dashboard can display up to four charts. Each chart is constructed from the following parameters.

'Name' + 'Selected or Created Event Query' + 'Group By' + 'Aggregation Function' + 'Order By' + 'Limit'

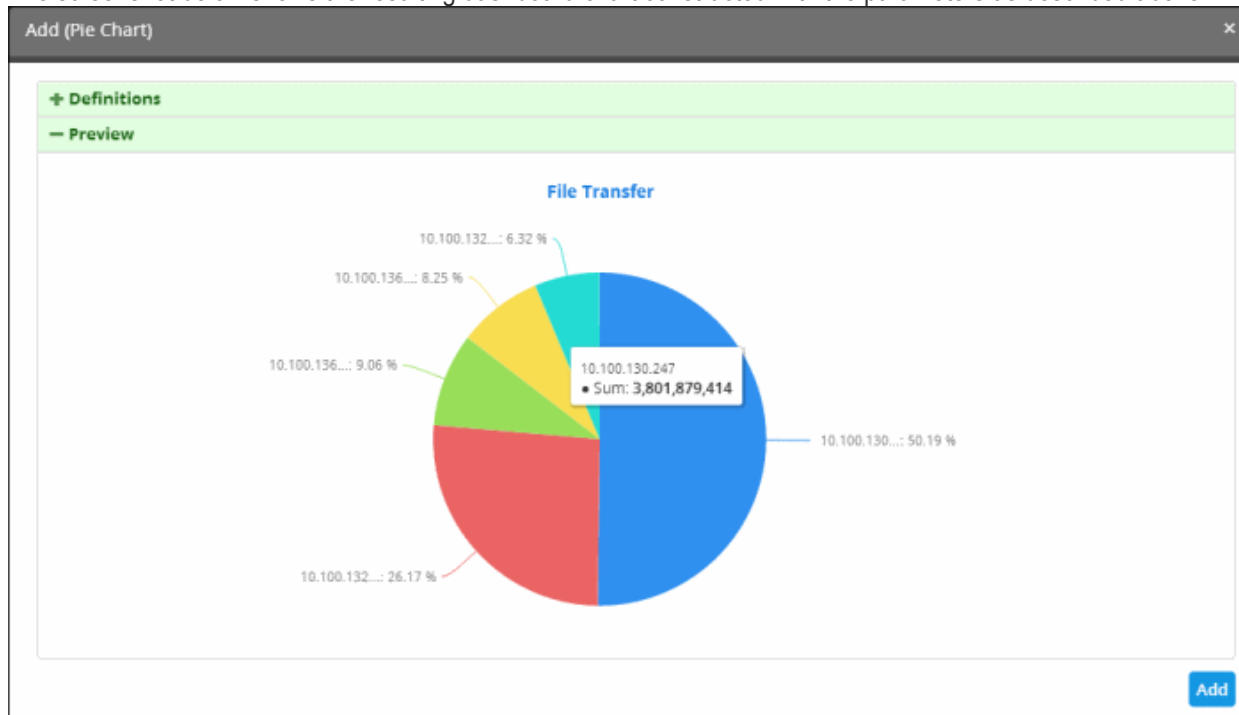
- Name - A name to identify the chart.
- Selected or created Event Query - The query whose results are to be displayed in the chart. The query can be selected from the list of queries, added from the selected customer or a new query can be created from the 'Add' chart dialog. The events that are detected based on the query for the last one hour will be displayed in the charts.
- Group By - The field, based on whose values, the events identified by the query are to be grouped and shown in the chart. Event groups will be formed so that each event group will have events with same value for the selected field.
- Aggregation Function - The event groups formed based on the fields chosen in the 'Group by' option, are ranked based chosen 'Aggregation Function'. The event groups are indicated in the charts in ascending or descending order as chosen in the 'Order by' setting. The available options are:
 - Count - Event groups are ranked based on the number of events in each group.
 - For example, if you choose Source IP as 'Field' then the group which contains the most events on a particular source IP will have the top rank and the group containing the lowest number of events is ranked lowest.
 - You can further control how the data is displayed by modifying the 'Order By' and 'Limit' parameters.
 - Sum - The event groups are ranked based on sum of values in another field that contains numerical value.
 - If you choose 'Sum', you need to select another field that contains a numerical value, like 'bytes in'/'bytes out'.
 - The event groups are ranked based on the sum of the values in the chosen numerical field from all the events in that group.
 - For example, if we choose 'Bytes-in' as numerical value, then the system adds up the values in the 'Bytes-in' field of all the events in a group and ranks the group accordingly. The event group having the sum of values in the 'Bytes-in' field as maximum is ranked top and vice-versa.
 - Average - Similar to above. Event groups are ranked based on the average of the values of the chosen numerical field from all the events in that group. (e.g. the average of values of 'Bytes_in' field of events in the group, if we take the same example as above)
 - Maximum - Similar to above. The event groups are ranked based on the maximum of the values of chosen numerical field from all the events in that group.
 - Minimum - Similar to above. The event groups are ranked based on the minimum of the values of chosen numerical field from all the events in that group.
- Order By - You can choose the order in which the event groups are to be indicated in the chart, based on their ranking. The available options are:
 - Ascending - The group with the lowest rank will be top of the list. A limit of 5 will show the 5 groups with the lowest ranks.
 - Descending - The group with the highest rank will be top of the list.. A limit of 5 will show the 5 groups with the highest ranks.
- Limit - The number of event groups to be displayed in the chart

For example, If you want to view the identify of the source IPs of top 5 endpoints that are involved in large file transfers and hence consume large bandwidth resource, you can:


- Create and save a query for identifying file transfer events

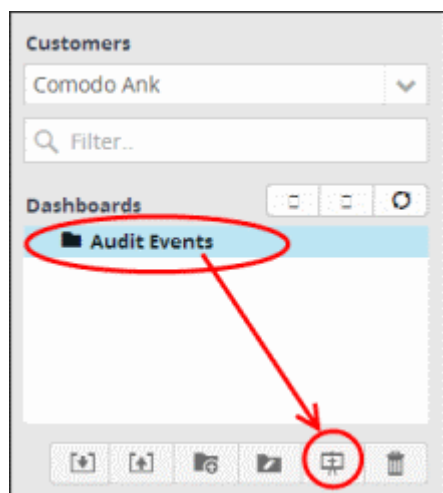
- Construct a chart by selecting the query
- Group the events by Source IPs
- Aggregate the event groups by the sum of 'Bytes-out'
- Set the chart to display top 5 groups in descending order

The screenshot below shows the resulting dashboard chart constructed with the parameters as described above:



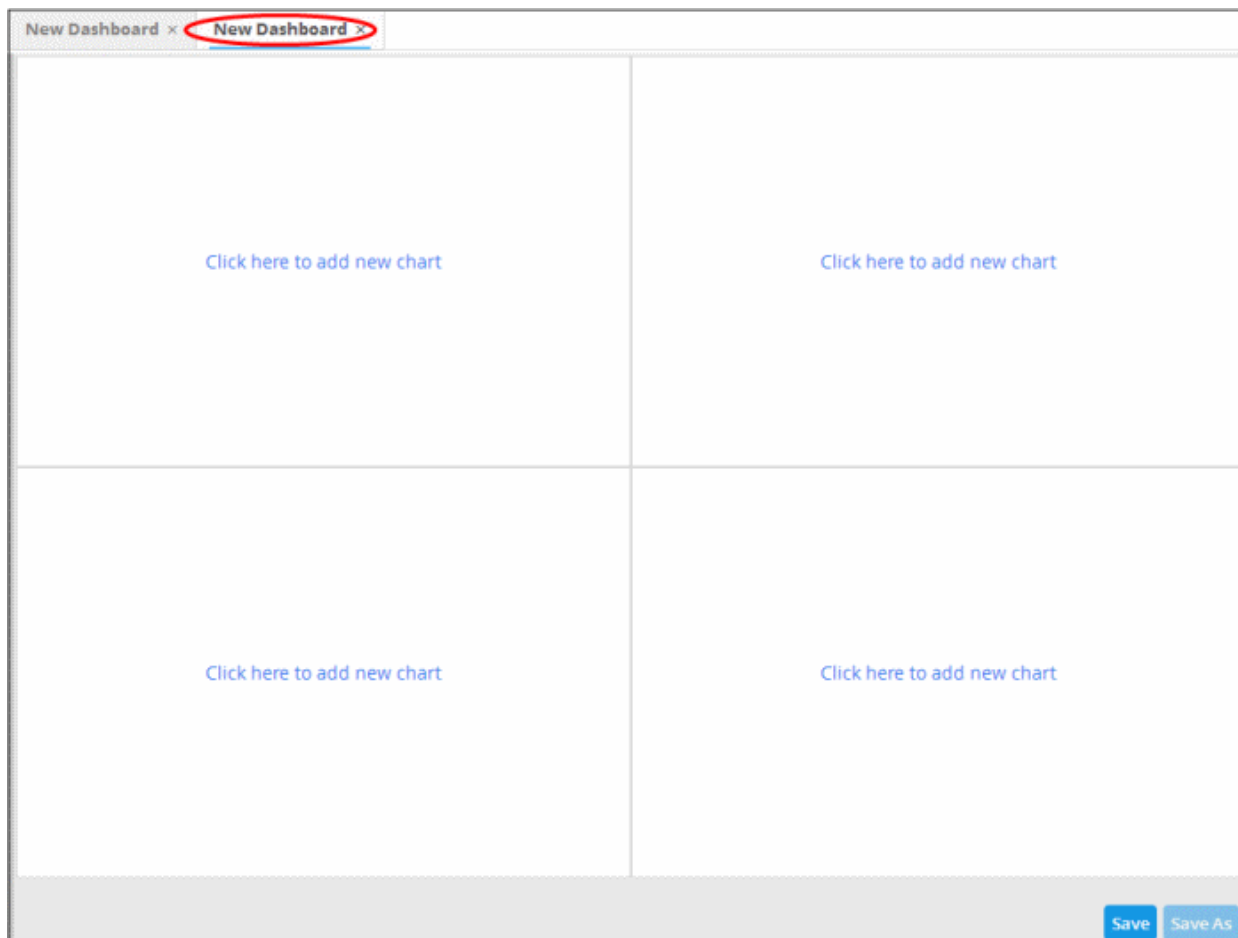
To create a new dashboard

- Select the customer from the 'Customers' drop-down at the top of the left hand side panel.
- Select the appropriate folder or **create a new dashboard folder** under which you want to create a new dashboard. Alternatively, you can also select a folder while saving a dashboard.
- Click the  button.



A 'New Dashboard' tab will be displayed.

Tip: You can also use the 'New Dashboard' tab that is displayed as the first tab on selecting a customer, to create a new dashboard. You can save the created dashboard by selecting an appropriate folder from the left side panel.



The new dashboard contains four tiles to display four charts.

- Click the 'Click here to add new chart' link on a tile.

The option to select the graph type to show the query results will be displayed.




The available options are:




- Pie Chart
- Bar Chart
- Spider Chart

- Time Chart
- Stacked Bar Chart
- Choose a graph type from the options


The 'Add' screen will be displayed for configuring the results to be shown in the chart.


The interface allows you to enter a name for the chart and select from event queries that were pre-configured for the customer's network or create a new query. You can select the event query for which the chart is to be displayed, from the list by clicking the  button.

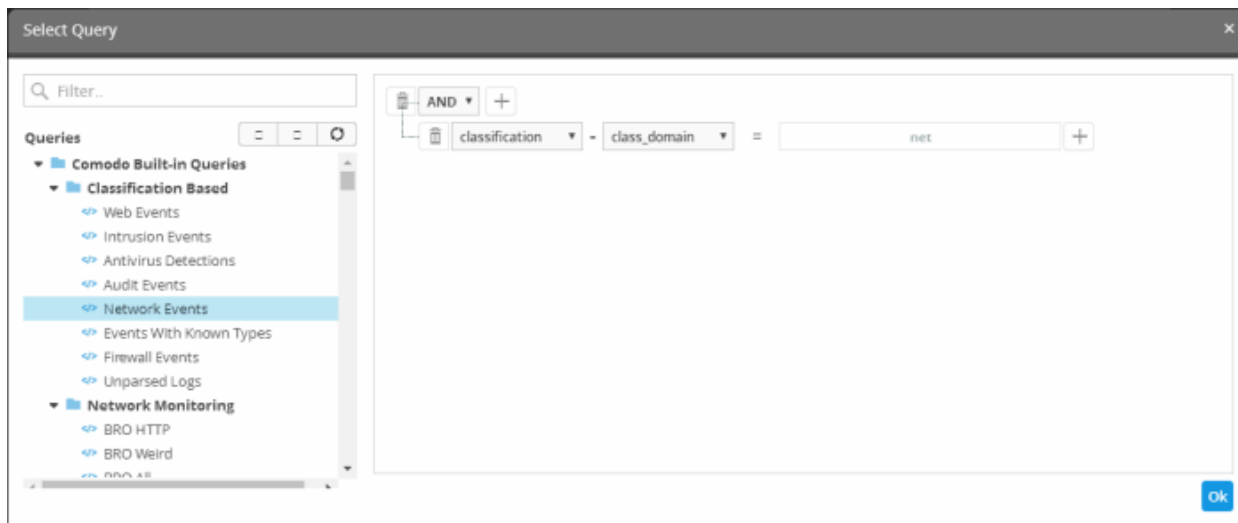
- Create a new query for the custom dashboard - Click the  button then follow the procedure **explained** in '**Configure Event Queries**'.

Add Chart - Form Parameters	
Parameter	Description
Name	Enter an appropriate name for the dashboard tile
	<ul style="list-style-type: none"> • Displays the list of predefined and custom event queries added for the selected customer. • Select the event query for which the results are to be displayed in the chart.
	<ul style="list-style-type: none"> • Allows you to configure the 'Results' table for the new query. • See 'Configure results table for a query' for more details.
	Allows you to configure a new event query
Group By	<ul style="list-style-type: none"> • The drop-down displays the fields, configured as event query results table column headers for the selected or created event query. • See 'Configure results table for a query' for more details.

	<ul style="list-style-type: none"> Choose the field by which events identified by the query should be grouped and shown in the chart. If you select 'Stacked Bar Chart', another 'Group By' field, 'Group By -2', will be available to further refine the grouping.
Aggregation Function	<p>Allows you to choose the aggregation operation to be applied for ranking the event groups and show them in ascending or descending order, in the chart. The options available are:</p> <ul style="list-style-type: none"> Count - The event groups are ranked based on the number of events in each group. <ul style="list-style-type: none"> For example, if you choose Source IP as 'Field' then the group which contains the most events on a particular source IP will have the top rank and the group containing the lowest number of events is ranked lowest. You can further control how the data is displayed by modifying the 'Order By' and 'Limit' parameters. Sum - The event groups are ranked based on sum of values in another field that contains numerical value. <ul style="list-style-type: none"> If you choose 'Sum', you need to select another field that contains a numerical value, like bytes in/out. The event groups are ranked based on the sum of the values in the chosen numerical field from all the events in that group. For example, if we choose 'Bytes-in' as numerical value, then the system adds up the values in the 'Bytes-in' field of all the events in a group and ranks the group accordingly. This will tell you which source IP has the most incoming traffic. The event group with the highest SUM in the 'Bytes-in' field is ranked top and vice-versa. Average - Similar to above. Event groups are ranked based on the average of the values of the chosen numerical field from all the events in that group. (e.g. the average of values of 'Bytes_in' field of events in the group, if we take the same example as above). Maximum - Similar to above. The event groups are ranked based on the maximum of the values of chosen numerical field from all the events in that group. Minimum - Similar to above. The event groups are ranked based on the minimum of the values of chosen numerical field from all the events in that group.
Order By	<p>Allows you to choose the order in which the event groups are to be indicated in the chart, based on their ranking. The available options are:</p> <ul style="list-style-type: none"> Ascending - The group with the lowest rank will be top of the list. A limit of 5 will show the 5 groups with the lowest ranks. Descending - The group with the highest rank will be top of the list. A limit of 5 will show the 5 groups with the highest ranks.
Limit	Maximum number of events to be shown in the chart
Preview	View the chart before adding it to the tile
Add	Commit the chart to the dashboard.

- To create a new query, click the  button. The procedure is same as **explained** in the section '**Configuring Event Queries**'.

- To select a predefined query, click the  button.

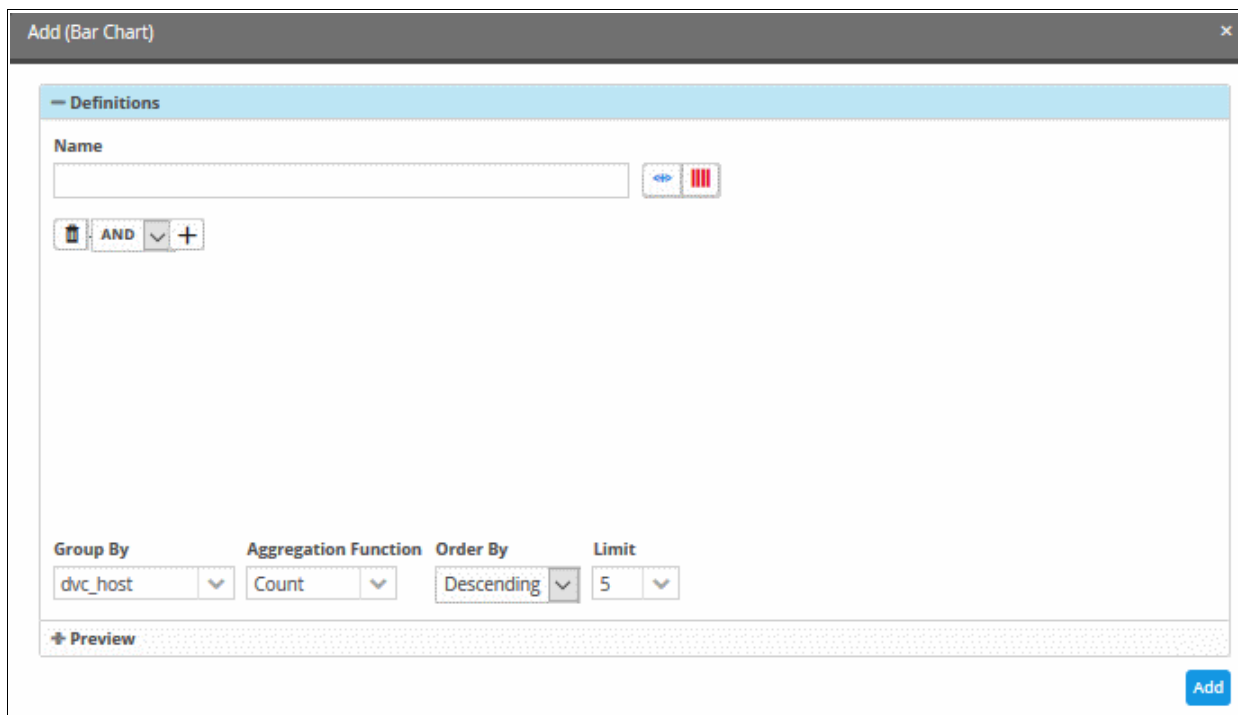


- Select the predefined query from the left.

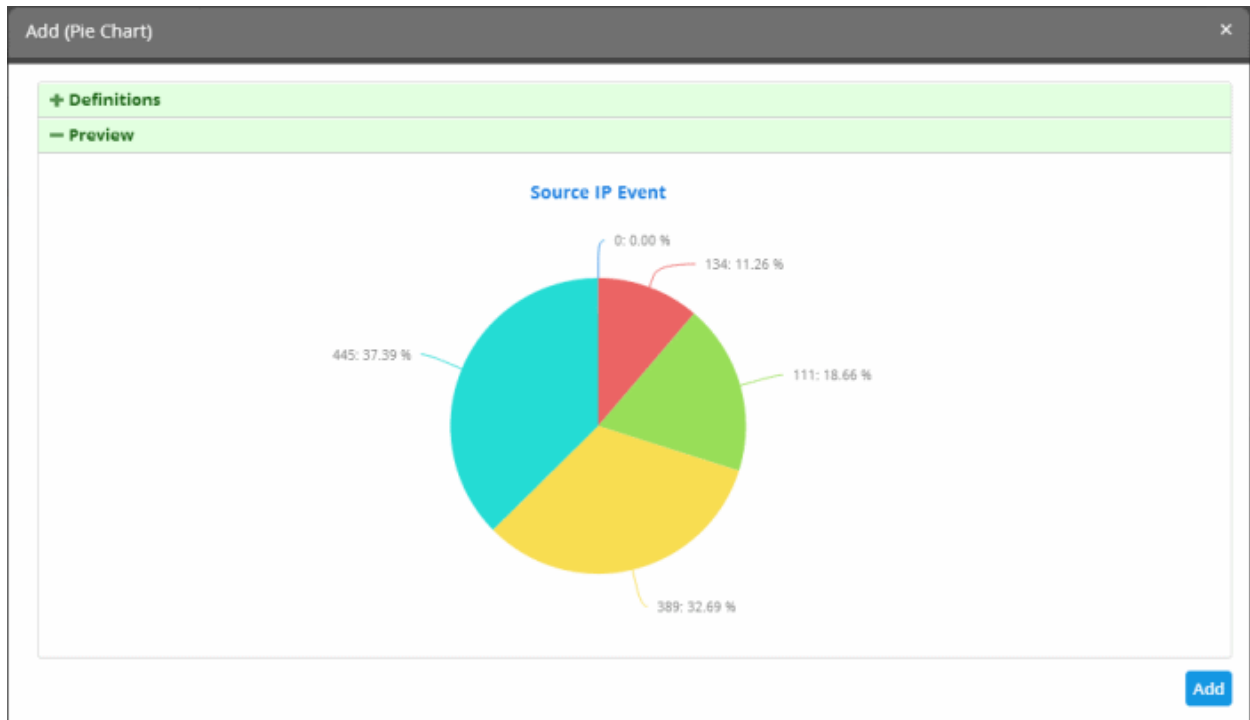
The query filter(s) will be displayed on the right. If required you can add more conditions for the selected query. The procedure is the same as explained in '[Configuring Event Queries](#)'.

- Click 'OK'

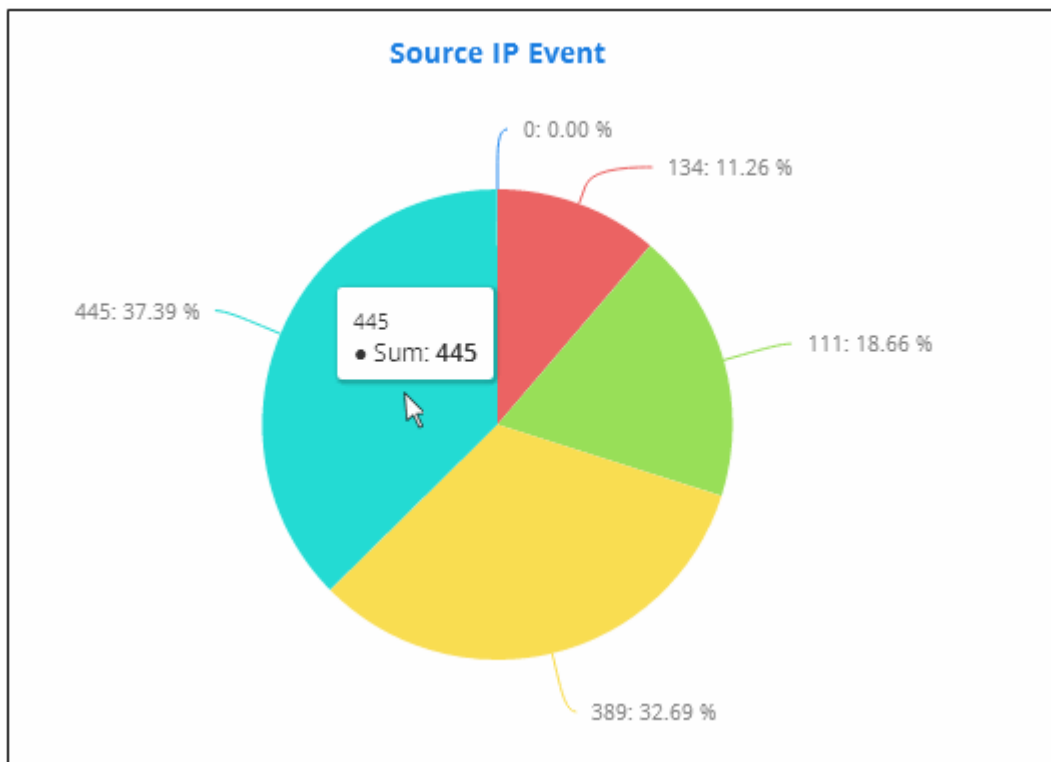
The query will be added and displayed in the 'Add' chart.



- Enter or select the parameters for 'Group By', 'Aggregation Function', 'Order By' and 'Limit' fields as explained in the above table
- Click the 'Preview' tab to check the chart before adding it to the dashboard tile.

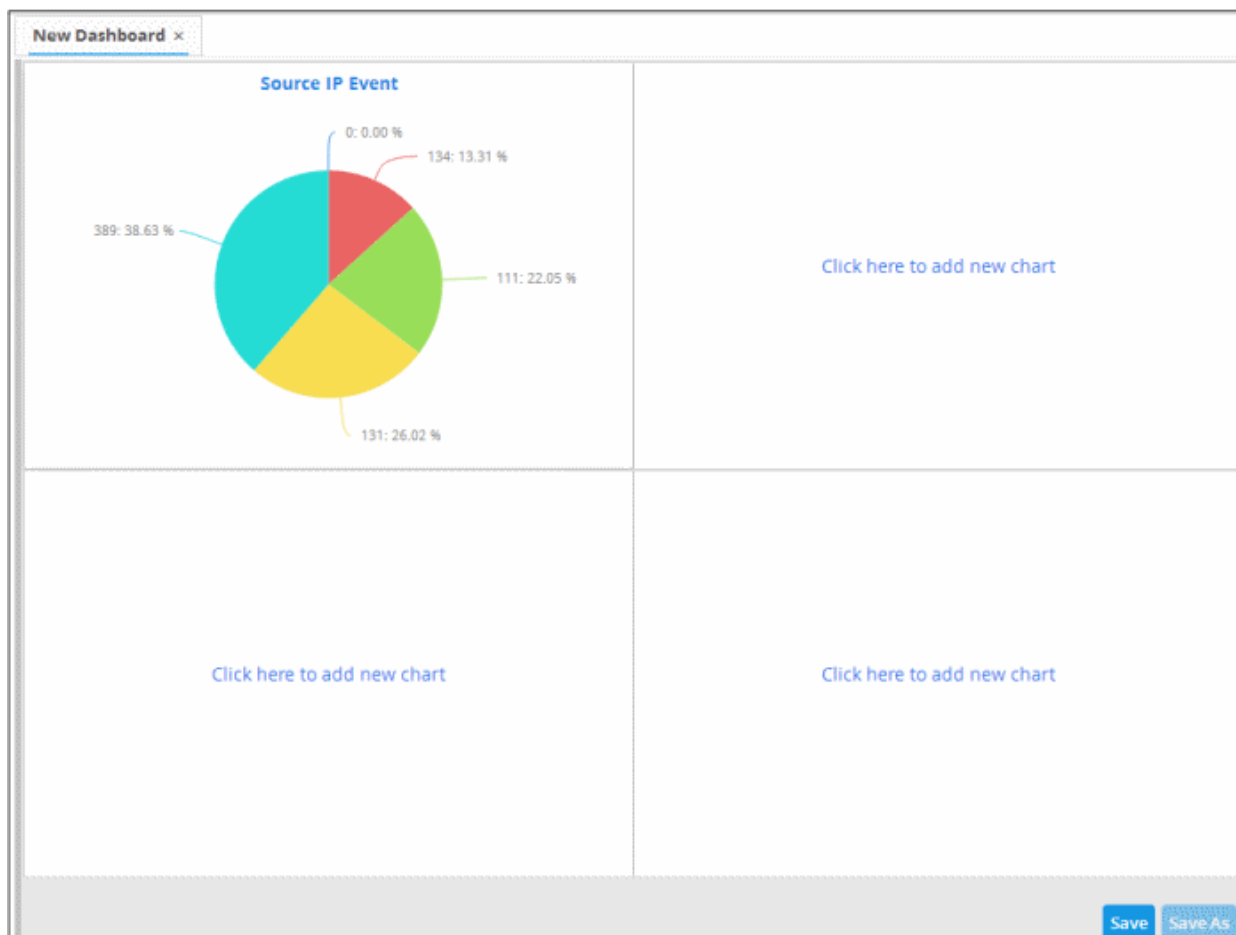


Placing the mouse cursor over a section will display the details of that particular event query.

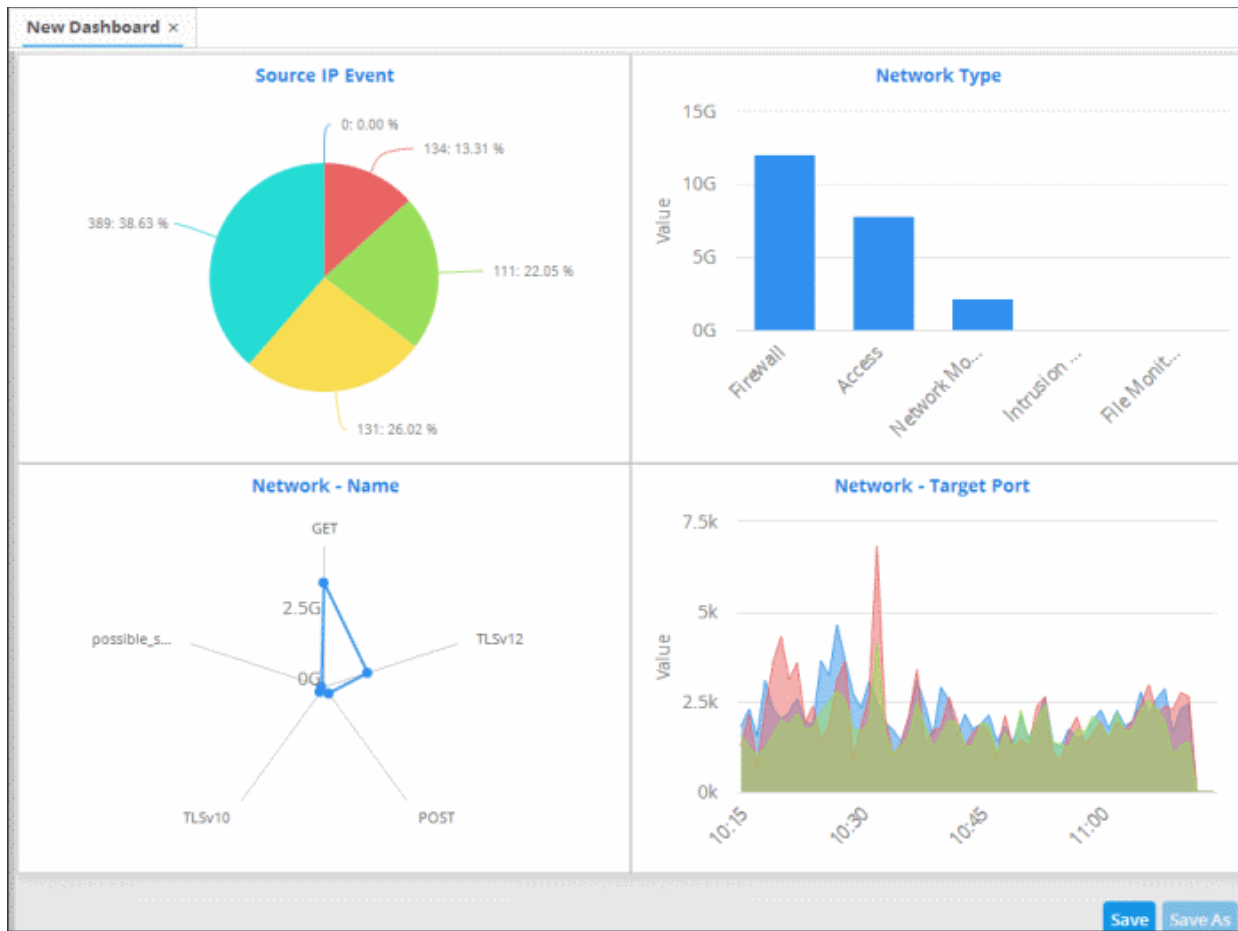


- Click the 'Add' button

The configured tile will be added to the dashboard.



- Repeat the process to add more number of tiles to the dashboard as explained **above**.



- Click the 'Save' button.

The 'Save' dialog will appear.

Save ×

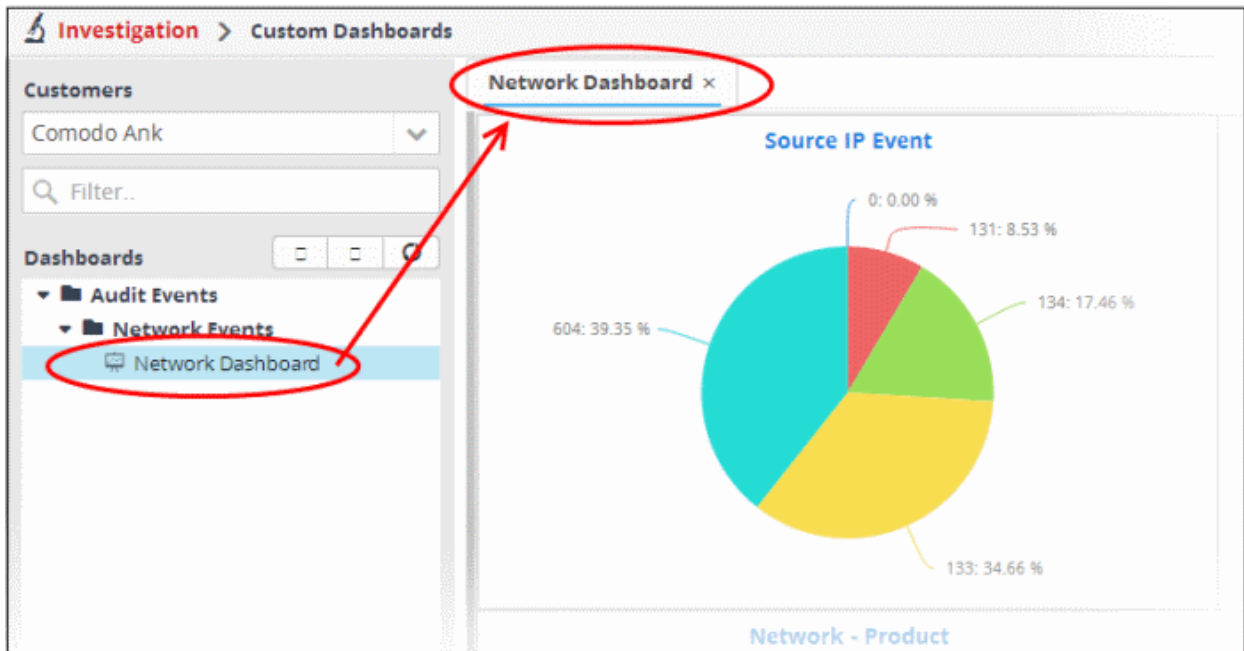
Name :

Refresh Interval :
 ▼

Save

- Enter the name for the dashboard in the 'Name' field
- Select the period at which the event query results chart should be updated from the 'Refresh Interval' drop-down. The options range from 30 seconds to 5 minutes.
- Click the 'Save' button

The dashboard will be saved and its name will be displayed on the tab and under the folder it was saved.



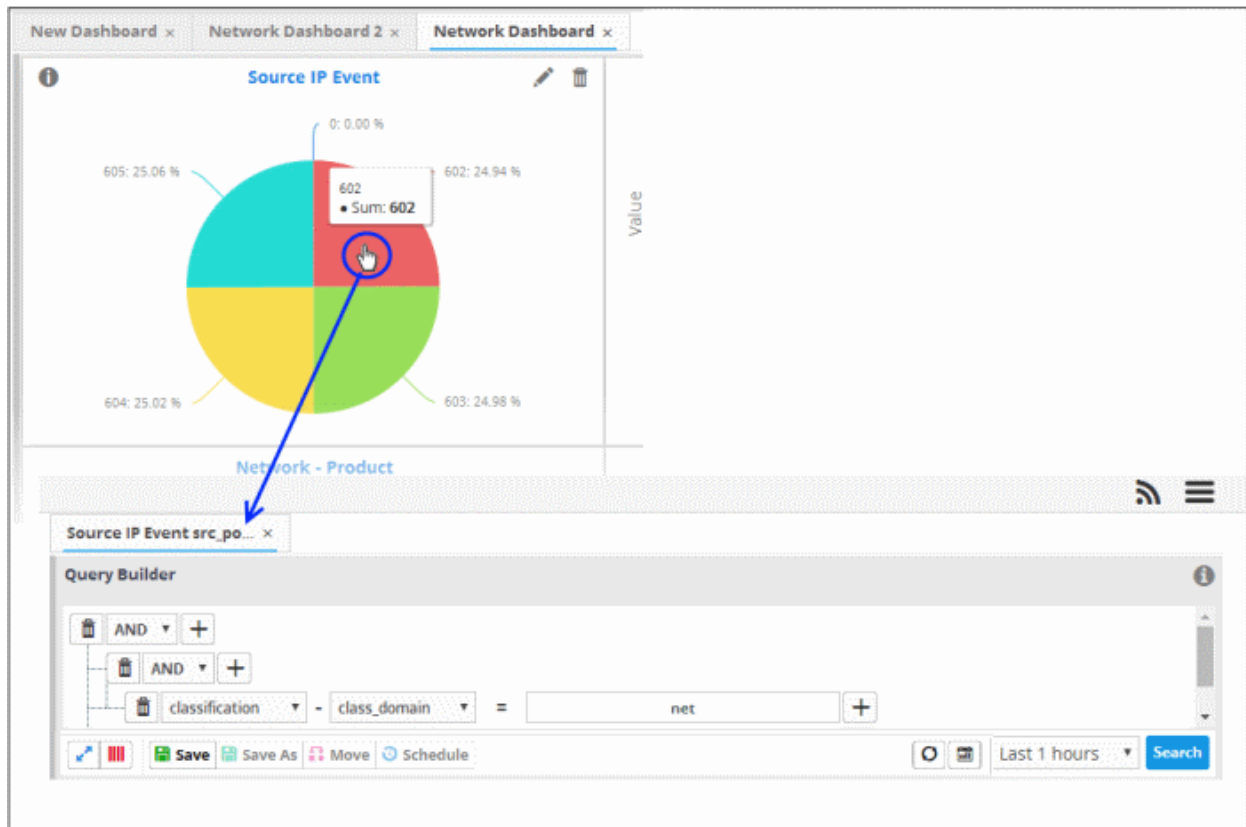
The 'Save As' button allows you to save the dashboard with the same parameters and with a different name. You can then edit the dashboard according to your requirement. You can add as many custom dashboards for various event queries configured for a customer by repeating the same process.

Create an Event Query for Specific Events from the Dashboard Chart

You can create new event queries for the customer to view the filtered results from the dashboard tiles.

To create a new query

- Click on the portion of the chart that indicates the events for which a new query is to be built



The query builder will open for the customer, with all the query parameters pre-configured for the specific event type indicated in the chart.

- If you want to change the parameters, directly edit on the 'Query Builder' interface.
- To view the results of the query, click 'Search'. The results will be displayed as a table in the lower right pane.
- Choose the folder in which the query is to be saved, from the list of folders in the left hand side pane and click 'Save'

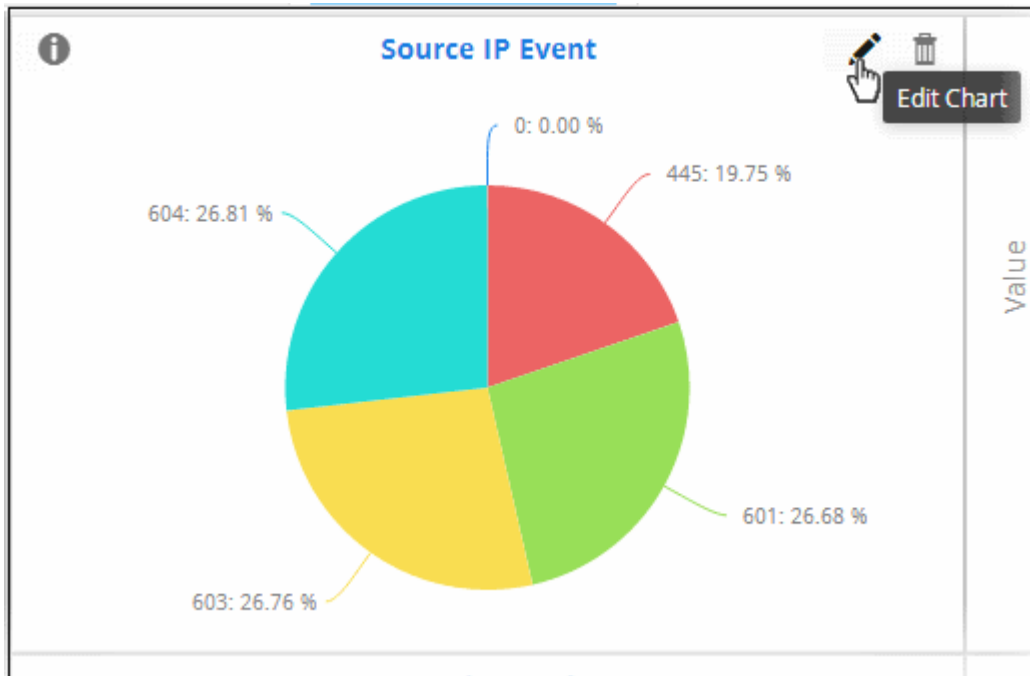
The Query will be saved. You can search for the events at anytime using the query.

Edit a Dashboard Tile

The custom dashboard tiles can be edited at anytime to change the query for which the results are displayed, the grouping and aggregation operation of the results and so on.

To edit a dashboard tile

- Place the mouse cursor over a tile to view the 'Edit', 'Delete' and 'Tool Tip' icons.



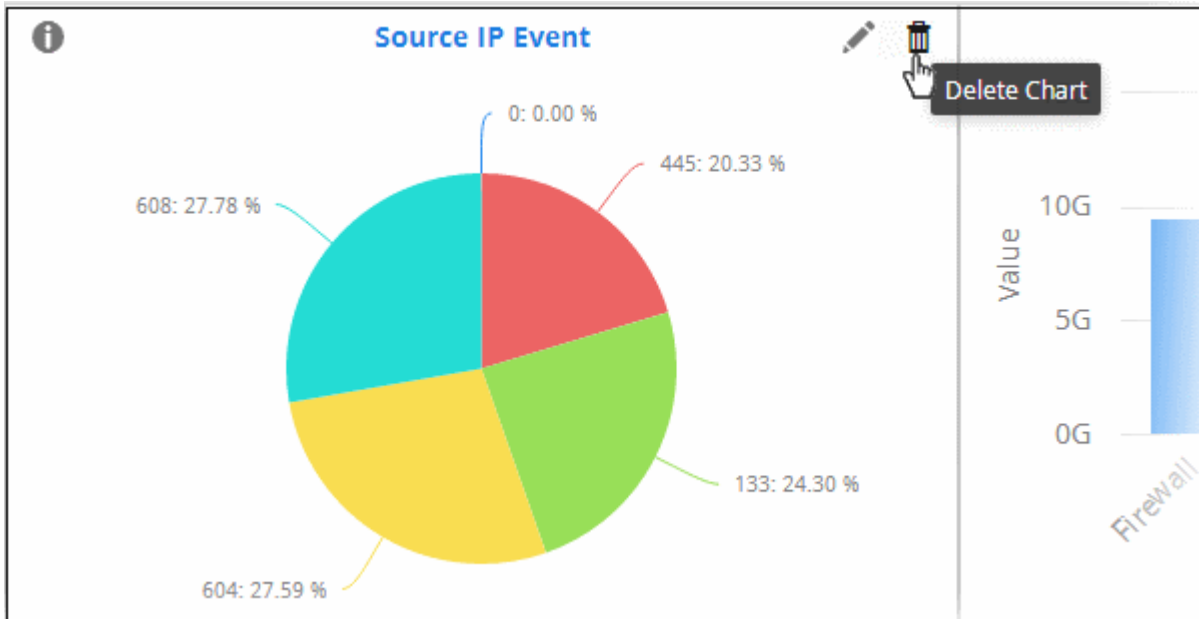
- Edit the chart details as required and click the 'Update' button

Delete a Custom Dashboard Tile

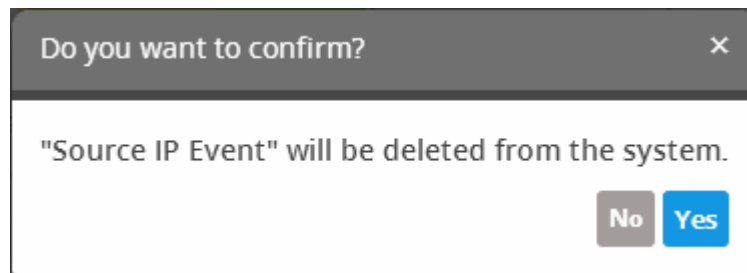
You can remove unwanted tiles from the dashboard, at anytime, and make room for new tiles to be added.

To delete a tile

- Place the mouse cursor over a tile to view the 'Edit', 'Delete' and 'Tool Tip' icons.



- Click 'Yes' to confirm the deletion.

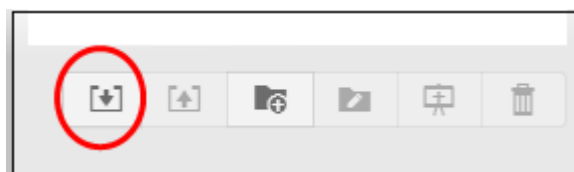


Import Event Queries to Custom Dashboard

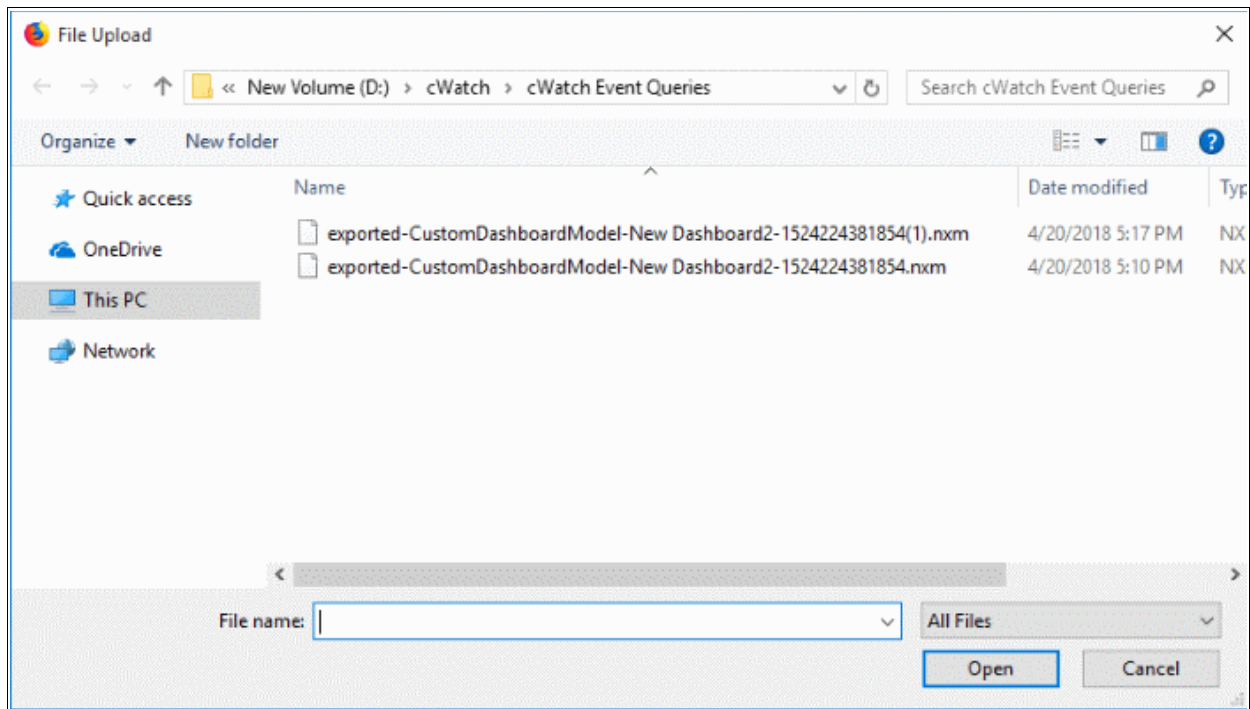
- You can import saved event queries to use them in a custom dashboard.
- Imported queries can be used as is or altered to suit the requirements of the customer. Please note - exported event queries can only be imported to their respective sections.
 - For example, event queries exported from the report section can only be used in the report section. Also, the values in the filter items in the exported events for tagged and list events will be set to default values.

To import a query or query folder

- Select the customer from the 'Customers' drop-down at the top of the left hand side panel for which you want to import the saved queries
- Click the 'Import' button at the bottom

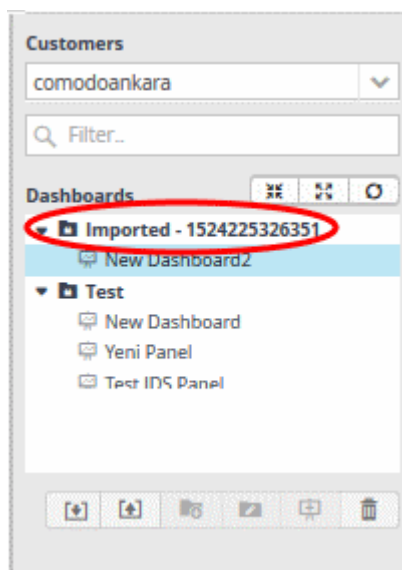


- Navigate to the location where the event query file is saved.



- Select the file and click 'Open'

The event query or event query folder will imported and will be listed under 'Imported' folder.



Select the query from the list and configure the custom dashboard as **explained** above.

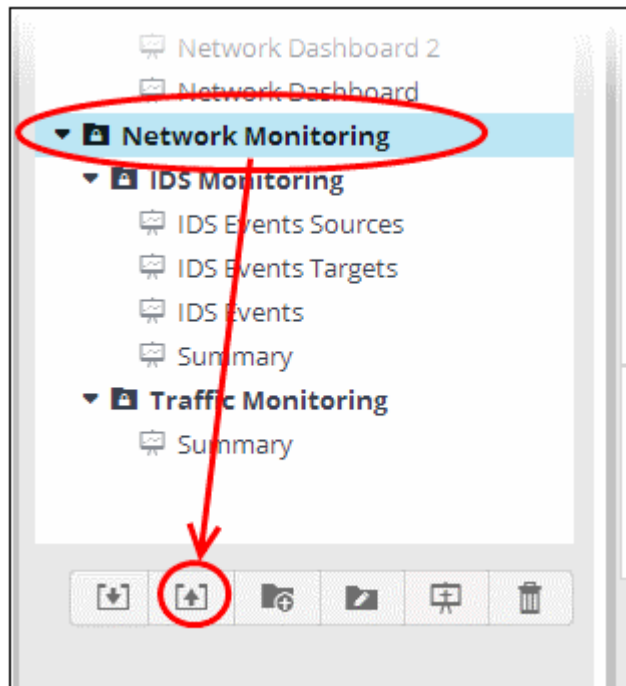
Export Event Queries from Custom Dashboard

- You can save event queries in order to use them for other customers.
- Imported queries can be used as is or altered to suit the requirements of the customer.
- You can export a query folder or a particular query. Please note - exported event queries can only be imported to their respective sections.
- For example, event queries exported from the report section can only be used in the report section. Also, the values in the filter items in the exported events for tagged and list events will be set to default values.

To export a query or query folder from the Custom Dashboard

- Select the customer from the 'Customers' drop-down at the top of the left hand side panel.

- Choose the query or query folder to be exported, from the 'Queries' list at the left.
- Click the 'Export' button at the bottom



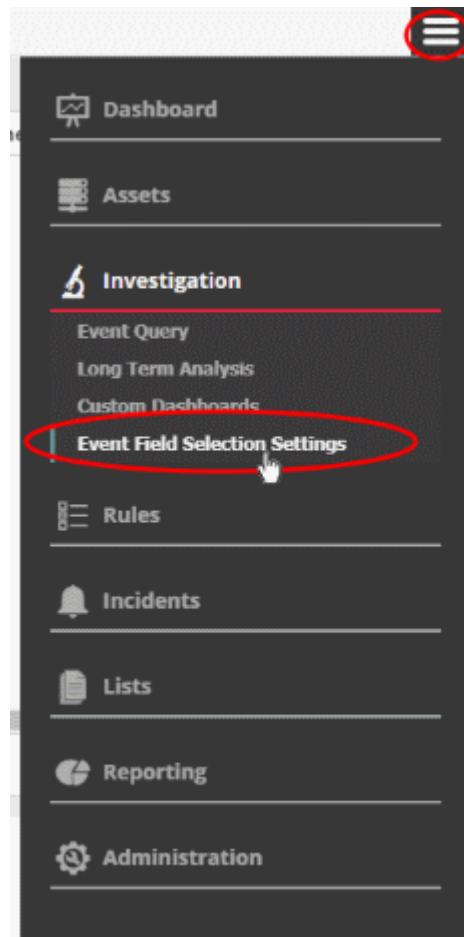
The file will be downloaded to your download folder. The saved query can be imported for use on another customer account.

4.4 Event Field Selection Settings

- The query results table should be configured appropriately to view the results of a query.
- cWatch ships with ten event field columns in the query results table
- This interface allows you to add event field columns to the results table that will be valid for all queries.
 - Alternatively, you can add event field columns on a one-off basis for a particular query. See '**Configure results table for a query**' for help with this.

Configure the query results table

- Click the hamburger icon > 'Investigation' > 'Event Field Selection Settings'



All default and custom event fields are shown:

Investigation > Event Field Selection Settings

Selection Fields Setting

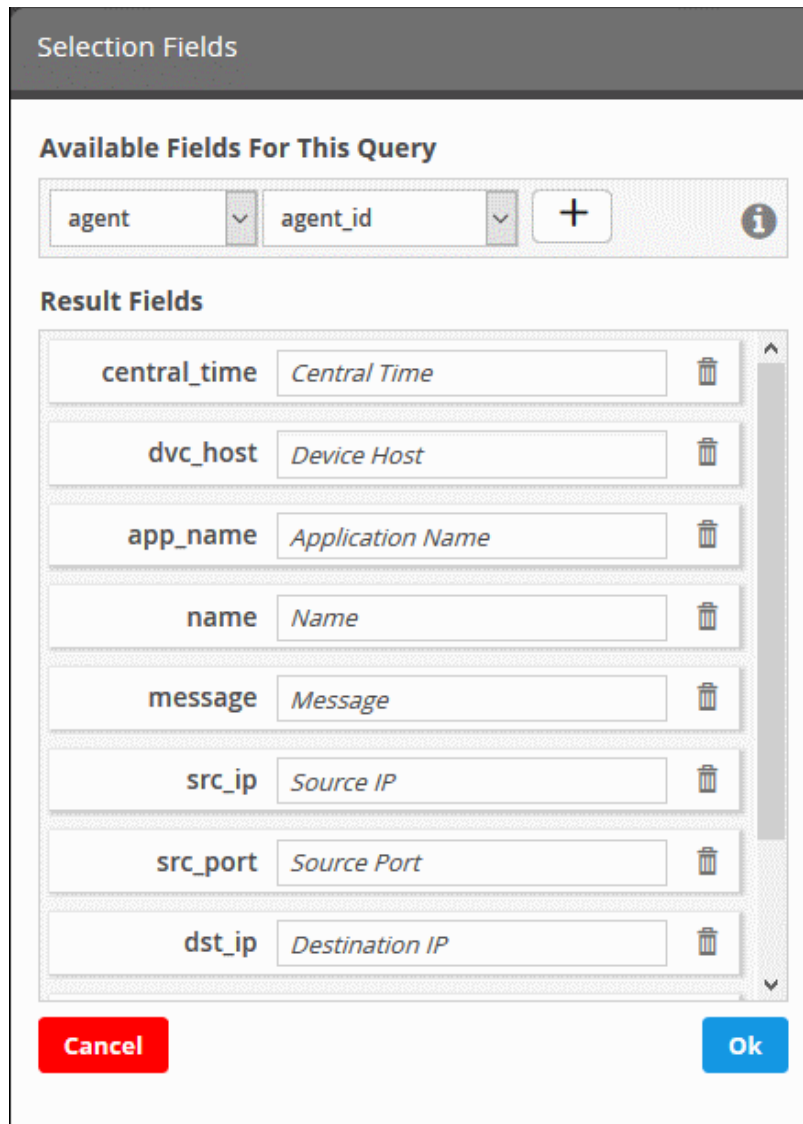
Selected Field Keys	Selected Field Values
central_time	Central Time
dvr_host	Device Host
app_name	Application Name
name	Name
message	Message
src_ip	Source IP
src_port	Source Port
dst_ip	Destination IP
dst_port	Destination Port
type	Type

[?](#) [Edit](#)

- Selected Field Values – The name of the event field group
- Selected Field Keys – The parameter selected for the event field

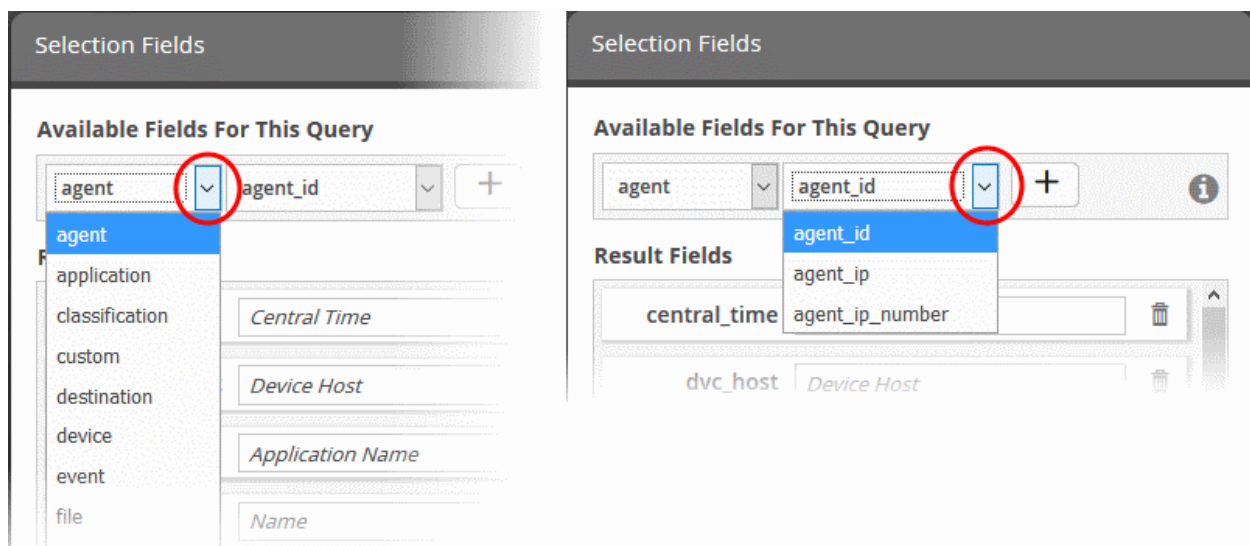
To add more event fields, click the 'Edit' button on the bottom-right

- The 'Selection Fields' dialog will open.




The default and added 'Result Fields' will be displayed.

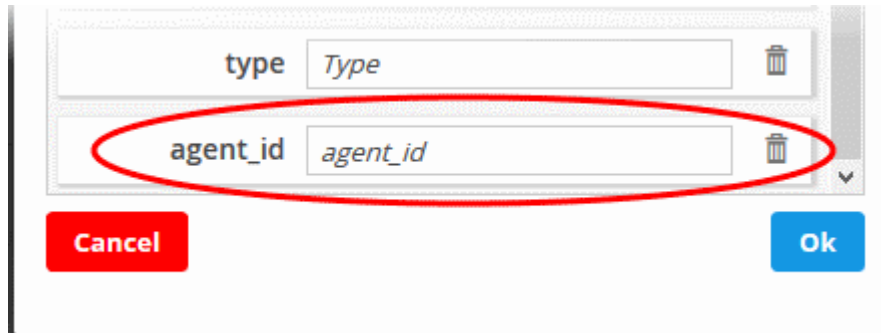
- To add new 'Result Fields', click the first combo box and select the event field group.




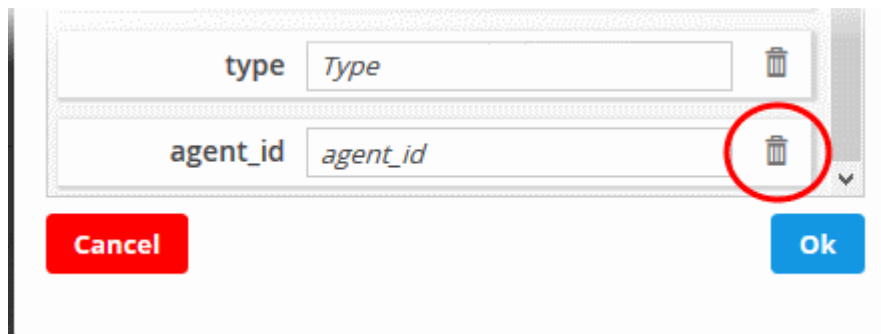
The next field will display the parameters available for the selected field group.

- Select the required field from the drop-down and click the  button.

A new results field will be added and you have to provide a new label for the result field.



- Enter a name for the field on the right side, by which the results field column should be displayed in the 'Results' screen. Note – Each event field group name should be unique.
- Repeat the process to add more fields and click 'OK'
- To remove irrelevant fields, click the trash can icon  beside it.

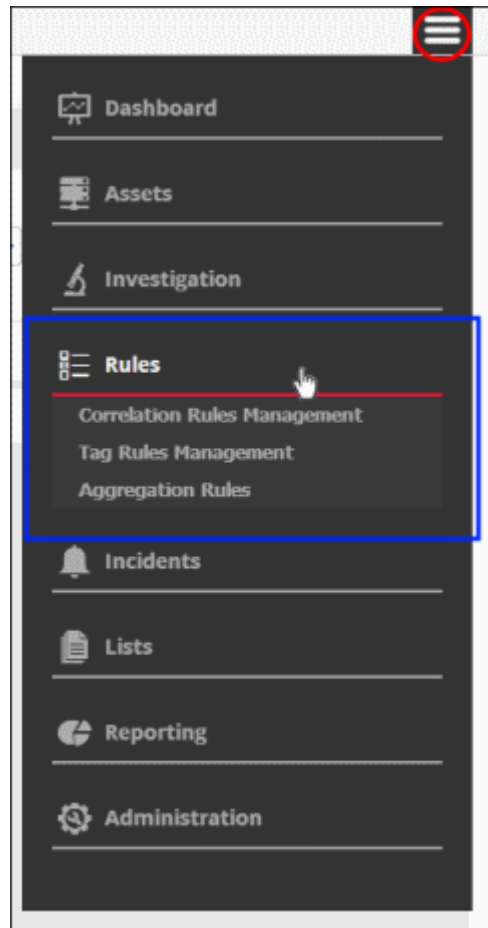


- Click the 'Cancel' button to revert the changes you made.
- Click the 'OK' button

See '[Configure Event Queries](#)' for more details.

5 Manage Rules

- cWatch monitoring rules identify events that may cause harm to customer networks and reports them to the admin console as 'Incidents'. For example, a firewall breach.
- Logs collected from customer networks are checked by the rules engine.
- Incidents created by rules are classified as 'Correlated Incidents' and automatically assigned to admins for further action. See '[Incidents](#)' for more information.
- This section also lets you tag events so you can search events more effectively.
- Aggregated rules let you configure multiple sub-events. When the conditions are met, a new event is created and can be queried in the 'Events Query' section.



See the following sections for more details:

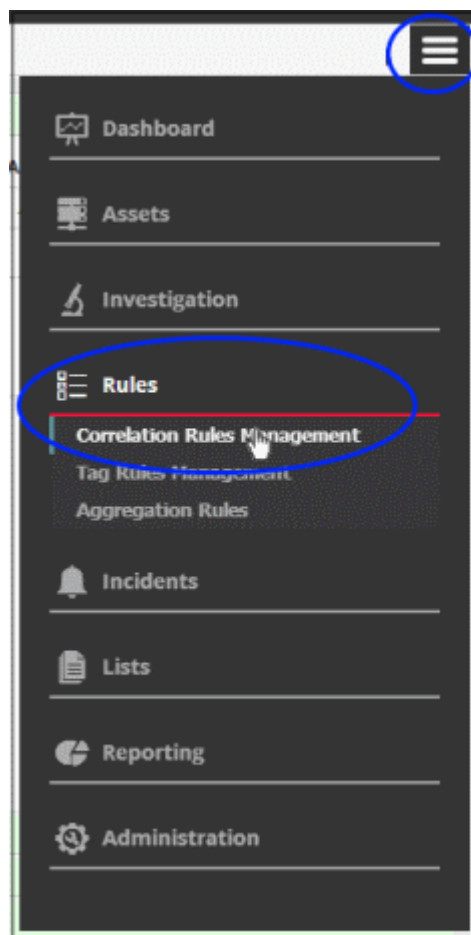
- [Manage Correlation Rules](#)
- [Manage Tagged Rules](#)
- [Manage Aggregation Rules](#)

5.1 Manage Correlation Rules

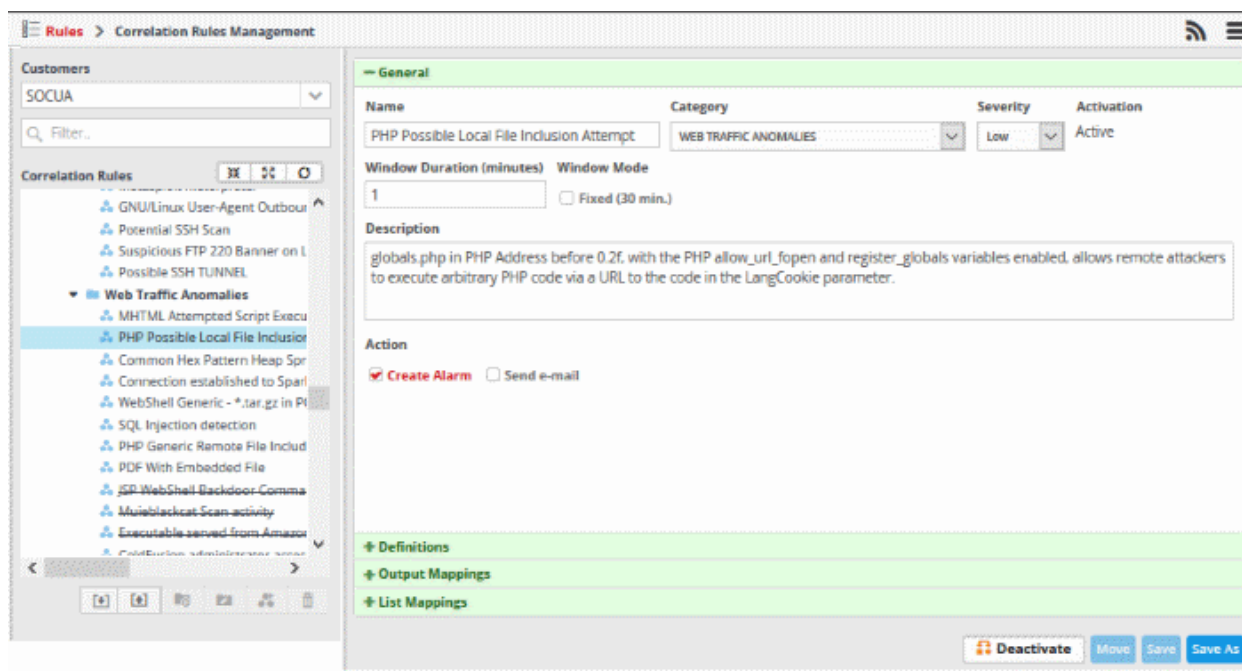
- Correlation rule management allows you to create rules which monitor the network for certain events.
- Events which match these rules are called 'Correlated Incidents'. These are automatically assigned to admins for further action.
- Correlation rules are created by defining query groups and aggregation parameters based on the event you want to capture. Each query group can be created by selecting saved 'Event Queries' and/or by adding new queries.
- The output from a correlation rule is also created as an event which can be queried from the 'Event Query' interface.
 - Each rule can be configured with 'Output Mappings' that define the fields shown in the 'Events Query' interface.
 - You can even configure a rule to just to create output events and not generate alerts.
- Also, selected field values of the outputs of a correlation rule can be used to update entries in live lists. Live lists contain values that can be used as parameters in a query or a rule.
- If a list is updated, the updated values are automatically reflected in the queries or rule which use the list.

See '**Live Lists**', for more details on managing Live Lists.

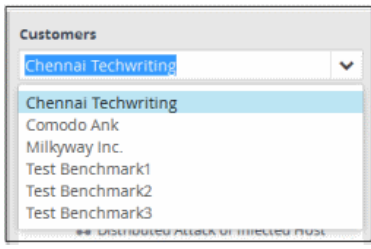








- Click the 'Menu' button > 'Rules' > 'Correlation Rules Management' to open the interface:



The 'Correlation Rules Management' interface will open:



The left-hand panel shows predefined correlation and custom rules for the selected customer. The right-hand panel show rule details and allows you to configure the rule. Rules are added to their respective folders based on their category.

Correlation Rules Management - Table of controls	
	The 'Customers' drop-down allows you to select the customer for which you want to manage correlation rules.
	Allows you to search for a particular correlation rule. Enter the name of the rule fully or partially and click on the search icon or press 'Enter'. The rules matching the entered text will be listed. To view the full list of rules again, clear the search field and press 'Enter'
	Allows you to expand or collapse the list of rules. To collapse, click the first button and to expand it, click the second button. Click the refresh button at the end to instantly update the rules list.
	Allows you to add a new category folder for adding the rules.
	Allows to edit the name and description of a 'Correlation Rules' folder
	Allows you to add new correlation rule under the chosen folder.
	Allows to delete rules folders or rules
	Allows you to import saved rules
	Allows you to export rules

The interface allows administrators to:

- **Manage rules folders**
- **Manage correlation rules**
- **Export correlation rules**
- **Import correlation rules**

Manage a Correlation Rules Folder

The correlation rules folder contains a collection of rules of specific category. Every new rule must be placed in a rules folder.

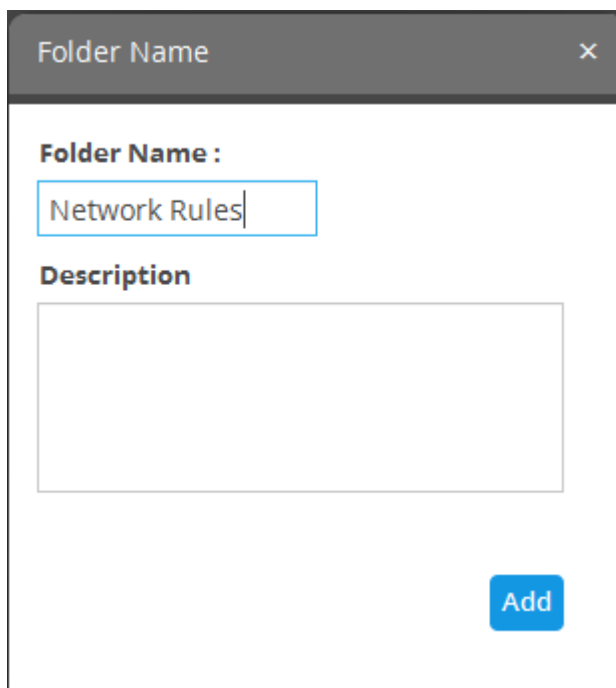
Creating a correlation rules folder

- Choose the customer from the 'Customers' drop-down at the top of the left panel.

The predefined and custom rules added for the customer is displayed as a folder tree structure in the 'Correlation

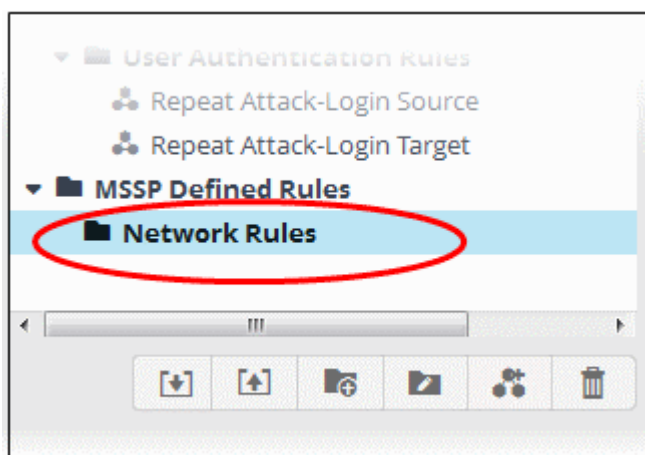
Rules' pane.

- Choose the parent folder to create a new sub-folder and click the  button.



- Enter a name for the rules folder in the 'Folder Name' field
- Enter a description for the category of rules to be added to the new folder
- Click the 'Add' button

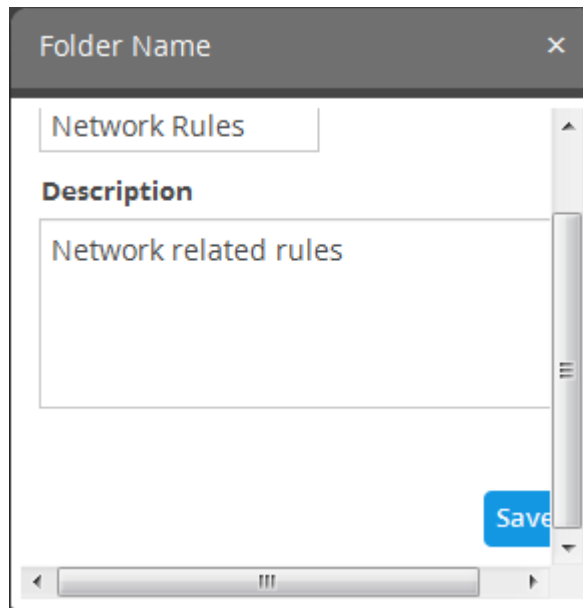
The folder will be saved and displayed on the left side.



The relevant correlation rules can now be placed under the newly created folder. See '[Manage a Correlation Rule](#)' section for more details.


Editing a correlation rules folder

- Select the folder and click the  button

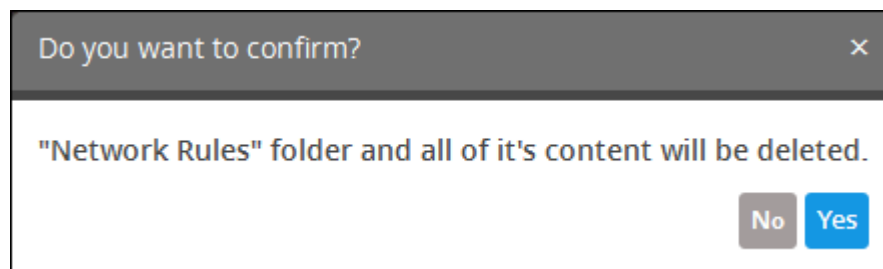


- Edit the details as required and click the 'Save' button

Deleting a correlation rules folder

- To delete a correlation rules folder, select it and click the  button.

A confirmation dialog will appear.




- Click 'Yes' in the In the confirmation dialog. Please note all the rules in the folder will also be deleted.

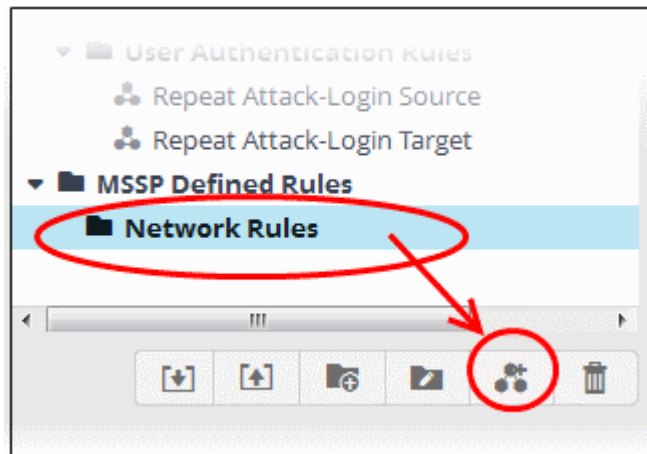
Configure a Correlation Rule

- Admins can create correlation rules in order to identify potentially harmful events. A event that meets the conditions of a rule will generate an 'Incident'.
- A rule is created by adding rule definitions with groups of filter statements and aggregation parameters for aggregating the events that are detected by the rule.
- Incidents will be assigned to the admin responsible for the customer.
- The detection of events based on a rule is also created as an event, that could be queried from the 'Event Query' interface.
- You can configure the values to be fetched for the fields for the output events generated by the rule every time.
- This allows you to further refine queries and rules based on output events. See [Output Mappings](#) for more details.

To create a correlation rule

- Select the customer from the 'Customers' drop-down on the left side.

- Select the appropriate rule category folder or **create a new correlation rule folder** under which you want to create a correlation rule.
- Click the  button



The configuration screen for creating the new rule will be displayed in the right hand side panel. It has four sections:

General

Name	Category	Severity	Activation
<input type="text"/>	CORRELATED	Info	Active

Window Duration (minutes) **Window Mode** Fixed (30 min.)

Description

Action

Create Alarm Send e-mail

Definitions

Output Mappings

List Mappings

Deactivate Move Save Save As

- **General** - Allows you to specify the name and description for the rule, category, select the severity level, window duration for rule, to set rule active or inactive and set whether or not to create an Incident when this rule is met.
- **Definitions** - Allows to define the queries for the rule and select aggregation parameters for grouping identified events and more.
- **Output Mappings** - Allows you to select the field values to be included in the output events generated based on the rule. The output events can be queried from the 'Event Query' interface (Optional).
- **List Mappings** - Allows you to map live lists to which the selected field values of the events detected by the

rule is to be updated (Optional).

General

- Click the 'General' Stripe to open the General Configuration area.

The screenshot shows the 'General' configuration tab for a rule. The rule name is 'Access to Malware Site', the category is 'MALWARE', and the severity is 'Info'. The activation status is 'Active'. The window duration is set to 1 minute, and the window mode is 'Fixed (30 min.)'. The description is 'Alert when a domain containing malware is accessed'. The action is set to 'Create Alarm'. At the bottom, there are buttons for 'Deactivate', 'Move', 'Save', and 'Save As'.

- **Name** - Enter a name for the rule
- **Category** - Select the type of rule. These options can be customized in the 'Incident Category Management' interface. The default categories are:
 - Authentication Anomalies
 - Anomalies in privileged user account activities
 - Anomalies specific to endpoint and backend
 - Check for known APS
 - Correlated
 - DNS Request Anomalies
 - Malware Activity
 - Malware
 - Manual
 - Scheduled Query
 - Unusual Network Traffic
 - Unpatched for Vulnerable Systems or applications
 - Web traffic anomalies
- **Severity** - Choose the severity level that will be assigned to the incident that matches the rule. The options available are:
 - Info
 - Low

- Medium
- High
- Critical
- **Window Duration (minutes)** - Enter the minimum duration (in minutes) for the event to be identified as an incident based on the rule.
- **Activation** - Choose whether you want the rule to be active or inactive from the drop-down
- **Description** - Enter an appropriate description for the rule. The description entered in this field will appear as the 'Summary' in the incident generated by the rule.
- **Create Alarm** - Configure whether or not an 'Incident' is to be created and an alert is to be sent to the administrator, when the rule is met. If selected, the rule creates an incident and an output event which can be queried from the 'Event Queries' interface. Else the rule creates only the output event and does not create an Incident.
- **Send e-mail** - Select this check-box if an email alert should be sent to the administrator when an incident is created. See **Adding Users** in 'Managing Users' for more details about configuring email address.

Definitions

Each rule is constructed with a set of filter condition statement groups to identify the events and generate alarms. The definitions stripe allows to define filter statement groups and aggregation parameters for the rule. You can add filter statement groups by selecting saved queries and/or by manually defining them.

- Click the 'Definitions' stripe, to open the 'Definitions' area.


The screenshot shows the 'Definitions' section of the Comodo cWatch Network Administrator interface. The 'Definitions' stripe is expanded, revealing a text input field for 'definition name...', a '+' button, a double-headed arrow button, and an 'Ordered' checkbox. Below the input field is a large empty area for defining filter statement groups. At the bottom of the interface, there are buttons for 'Deactivate', 'Move', 'Save', and 'Save As'.

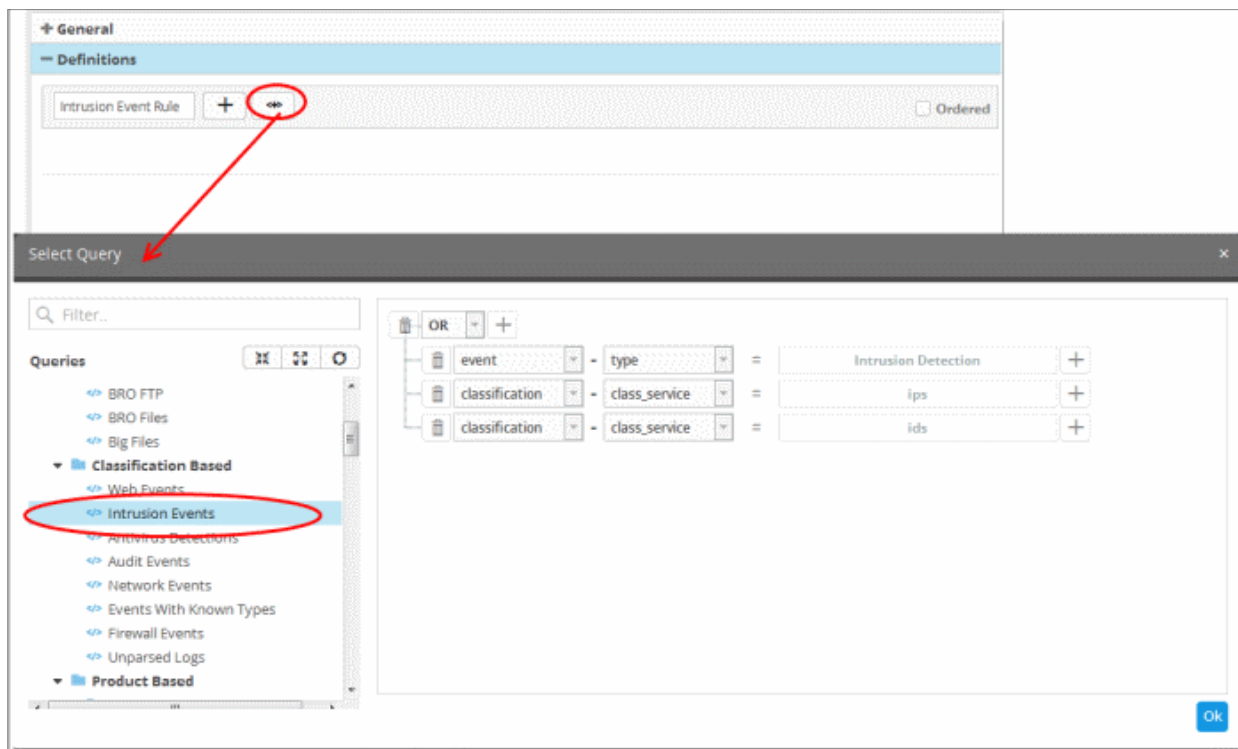
- To add a filter statement group as a rule definition, enter a name for the rule definition.

The next step is to add the filter condition statement groups to the definition. This can be done in two ways:

- **Select an Event Query and import the filter statement from it**
- **Manually define filter statements for the group**

Selecting an Event Query and import filter statements:

- Click the  button after entering a name for the rule definition.



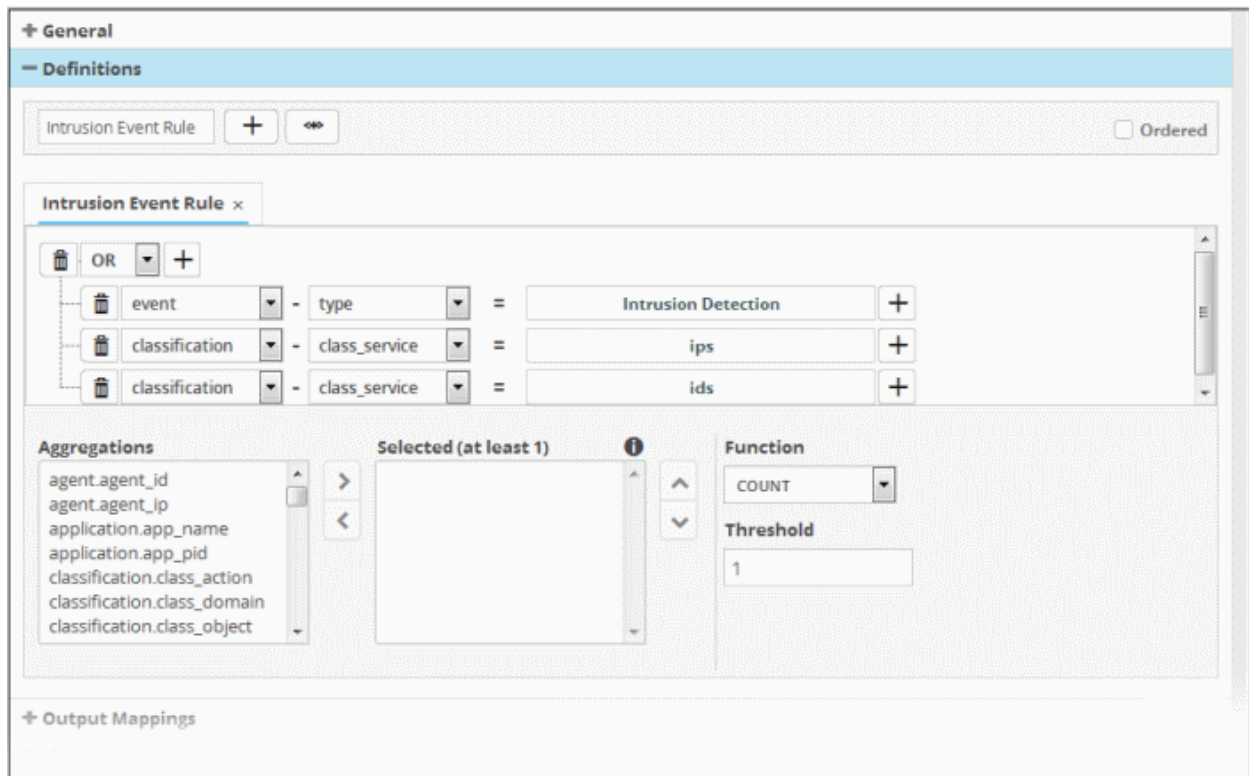
The 'Select Query' dialog will open with a list of pre-defined and custom event queries added for the customer in the left pane.

- Choose the query from the left pane.

The filter statements in the query will be displayed in the right pane.

- Click 'OK' to import the filter statements.


The rule definition will be added with the group of filter statements from the query .



You can edit the group by adding new statement(s), changing fields/values and/or removing existing statements. For more details on construction of the filter statements, see '[Manually defining filter statements for the group](#)' given below.

- Repeat the process to add more definitions from event queries.

Manually defining filter statements for the group

- Click the  button after entering a name for the rule definition.

A tab to add the query fields for the definition will open.

Each rule definition is built with a set of filter statements that are connected with Boolean operators like 'AND', 'OR' or 'NOT'. Each filter statement contains the following components.

'Field Group' + 'Field' + 'Operator' + 'Value'

- **Field Group** - The group to which the field specified as the filter parameter belongs.
- **Field** - The field in the event log entry by which you want to filter results
- **Operator** - Controls the relationship between the field and the specified value. Examples include 'Equals to', 'Does not equal to', 'contains', 'does not contain' etc.
- **Value** - The value for the field. Values can be entered manually or fetched from a pre-defined list which is managed in the 'List Management' interface. For example, if you choose a source IP (src_ip) as the field to be searched from network events, you can manually enter the IP address of the source of the connection request or choose a List containing a list of specified source IP addresses. Refer to the section [Lists](#) for more details on pre-defined lists.

Examples:

- To filter network connection events originated from an endpoint with IP address 10.100.100.100, build the filter statement as shown below:

'Source' + 'src_ip' + '=' + '10.100.100.100'

- ii. To filter network connection events originated from a set of endpoint whose IP addresses start with 10.100.100.xxx, build the filter statement as shown below:

'Source' + 'src_ip' + 'AB*' + '10.100.100'

- iii. To filter network connection events originated from a set of endpoint whose IP addresses are defined in the 'Live List type' named 'Internal' under the 'Live List' named 'IP Blacklist' build the filter statement as shown below:

'Source' + 'src_ip' + '[a]' + 'IP Blacklist' + 'Internal'

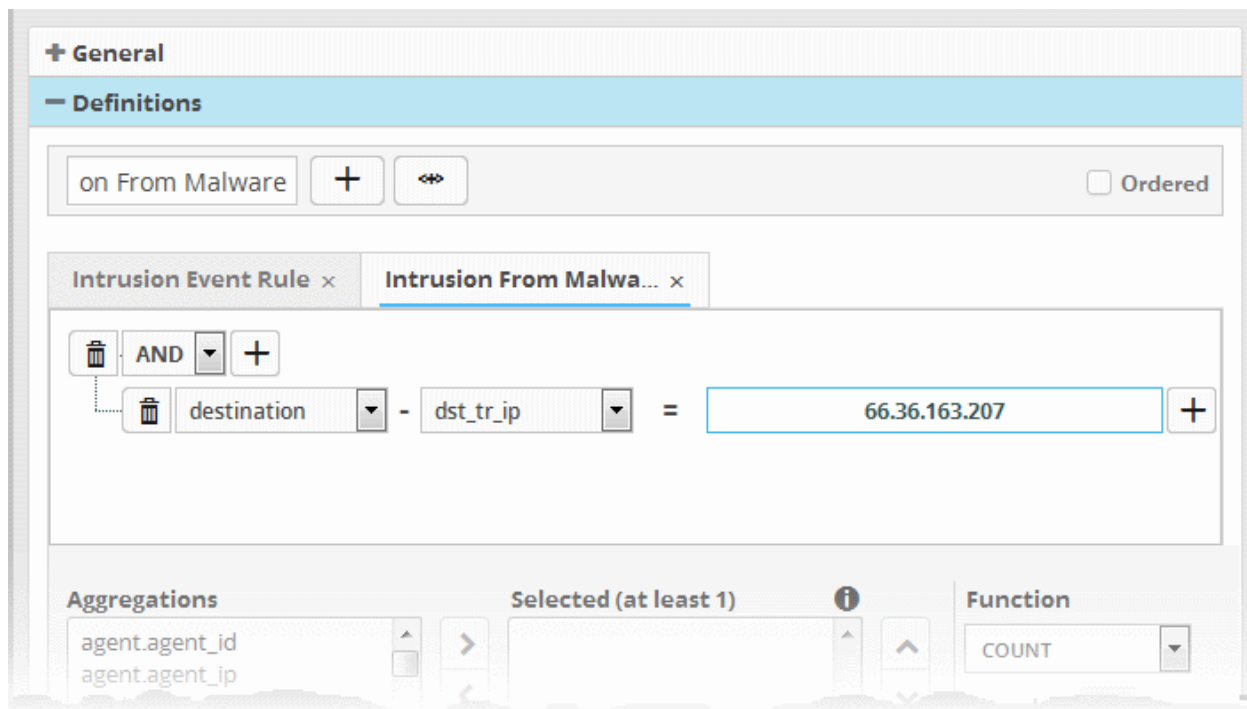
You can create more complex queries by adding more filter statements and linking them using 'AND', 'OR', or 'NOT'. For example:

- To filter network connection events originated from an endpoint with IP address 10.100.100.100, and destined to another endpoint with IP address 10.100.100.120, build the filter statements with an AND combination as shown below:


'Source' + 'src_ip' + '=' + '10.100.100.100'

AND

'Destination' + 'dst_ip' + '=' + '10.100.100.120'



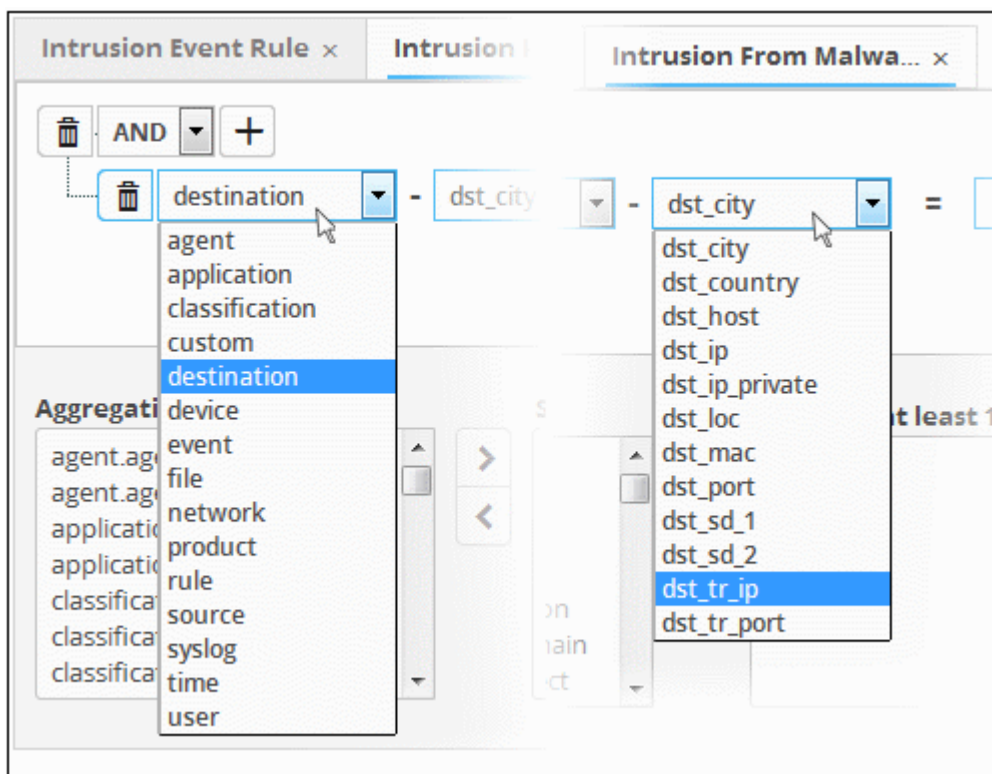
Manually add a filter statement group

- Choose the combination condition for the query(ies) to be defined from the drop-down at the top left. The options available are:
 - AND
 - OR
 - NOT
- Click the  button beside the drop-down to add a query filter.

The 'Field Groups' drop-down and 'Fields' drop-down will appear. The 'Fields' drop-down will contain options relevant to the 'Field Group' chosen from the drop-down at the left.

- Choose the field group you wish to add to the filter from the 'Field Groups' drop-down.

The next field will display the fields available for the selected field group.

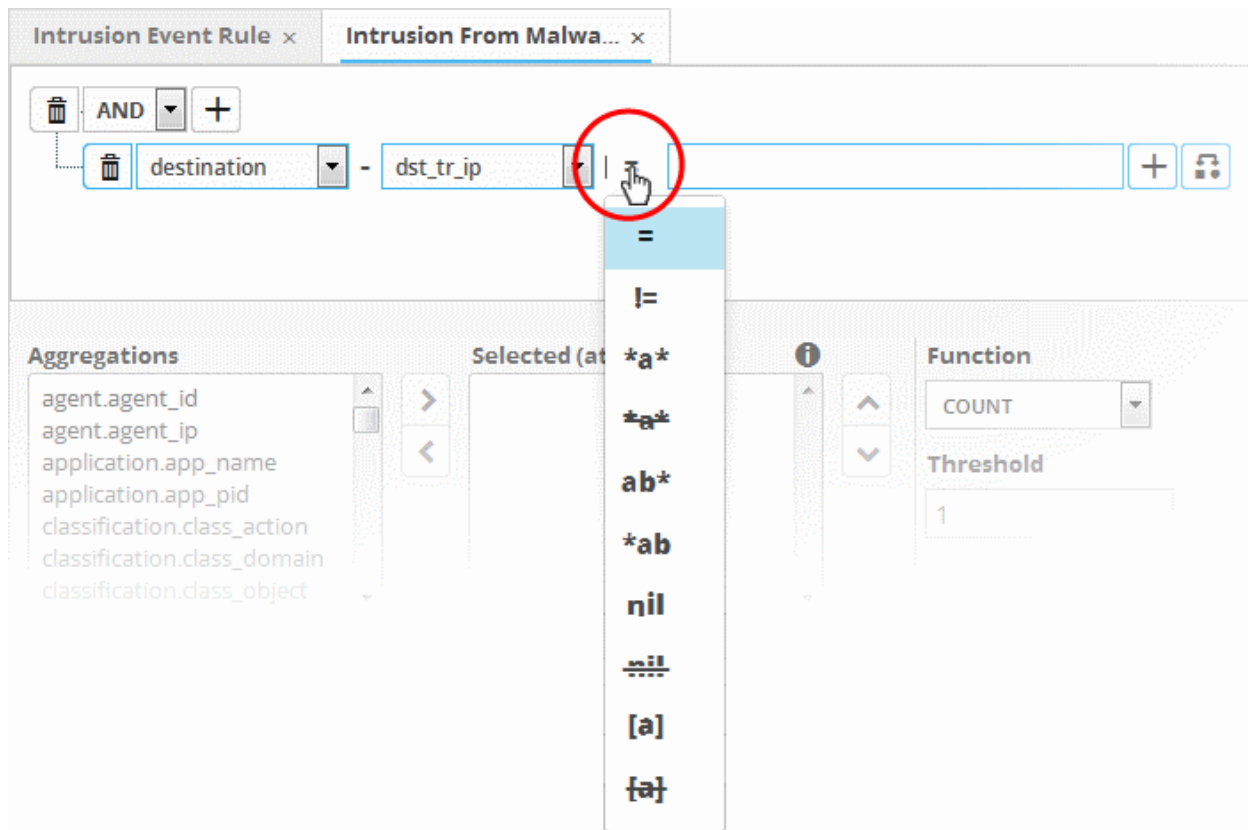


- Choose the field from the second drop-down.

Tip: The descriptions of the field groups and the field items under each of them, are available in [Appendix 1 - Field Groups and Event Items Description](#).

The next step is to choose the relation between the field chosen and the value to be entered in the next field.


- To choose the relation, click on the relation symbol at the right of the 'Field' drop-down.

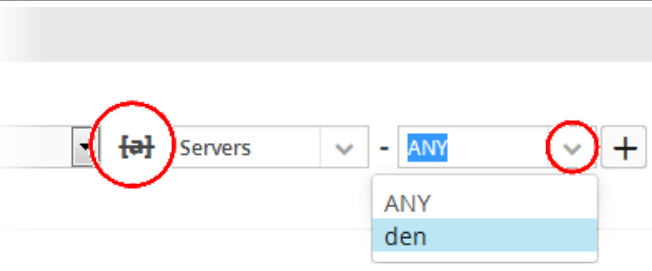



The types operators depends on the field chosen. The following table explains the various operator symbols:

Relation Operator	Description	Entering the value for the 'Field'
=	Equals to	<ul style="list-style-type: none"> Manually enter a value in the field to the right of the operator. Events containing the same value will be identified by the filter.
!=	Does not equal to	<ul style="list-style-type: none"> Manually enter a value in the field to the right of the operator. Events that do not contain the value will be identified by the filter.
>	Greater than	<ul style="list-style-type: none"> Applicable only for fields with numerical values, for example, port numbers. Manually enter a value in the field to the right of the operator. <ul style="list-style-type: none"> The filter will identify events that contain values greater than the entered value.
>=	Greater than or equal to	<ul style="list-style-type: none"> Applicable only for fields with numerical values, for example, port numbers. Manually enter a value in the field to the right of the operator. <ul style="list-style-type: none"> The filter will identify events that contain values equal to or greater than the entered value.
<	Less than	<ul style="list-style-type: none"> Applicable only for fields with numerical values, for example, port numbers.

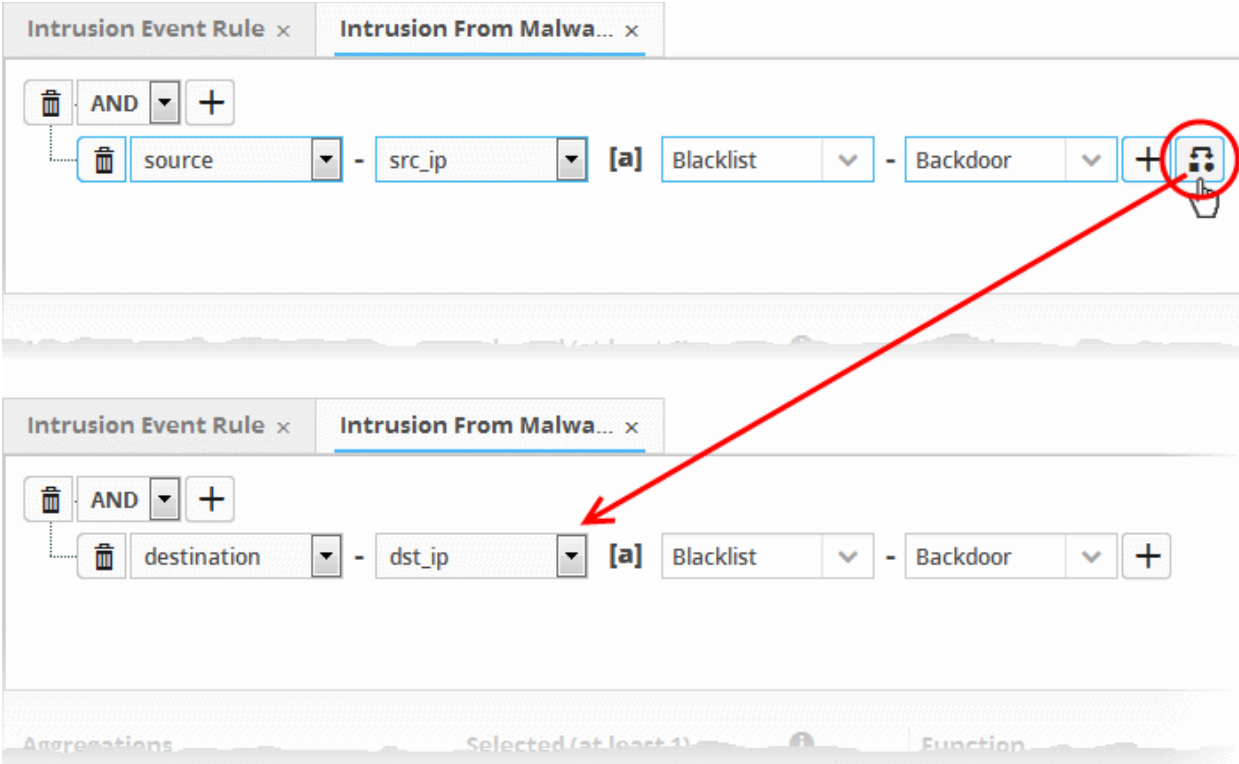
		<ul style="list-style-type: none"> Manually enter a value in the field to the right of the operator. The filter will identify events that contain values less than the entered value.
<=	Less than or equal to	<ul style="list-style-type: none"> Applies only to fields with numerical values. For example, port numbers. Manually enter a value in the field to the right of the operator. The filter will identify events that contain values equal to or lower than the entered value.
a	Contains	<ul style="list-style-type: none"> Manually enter a value in the field to the right of the operator. The filter will identify events that contain the entered value somewhere in the string. For example, to search for events with source IP addresses containing 123 anywhere in the address, enter '123'.
a	Does not contain	<ul style="list-style-type: none"> Manually enter a value in the field to the right of the operator. The filter will identify events that do not contain the entered value anywhere in the string. For example, to search for events with source IP addresses that do not contain 123 anywhere in the address, enter '123'.
ab*	Starts with	<ul style="list-style-type: none"> Manually enter a value in the field to the right of the operator. The filter will identify events that begin with the entered value. For example, to search for events with source IP addresses starting with 192, enter '192'.
*ab	Ends with	<ul style="list-style-type: none"> Manually enter a value in the field to the right of the operator. The filter will identify events that end with the entered value. For example, to search for events with source IP addresses that end with 123, enter '123'.
nil	Is Empty	<ul style="list-style-type: none"> Searches for events in which the selected field is empty (does not contain any value). For example, to search for the events with no values in their source IP address fields, select 'Is Empty'.
<u>nil</u>	Is Not Empty	<ul style="list-style-type: none"> Searches for events in which the selected field is not empty (contains a value of some kind). For example, to search for the events with some IP addresses values in their source IP address fields, select 'Is Not Empty'.


<p>[a]</p>	<p>Is in List</p>	<p>Allows you to configure the filter statement to fetch values for the field from a pre-defined list containing specific values for the field type.</p> <p>Background:</p> <ul style="list-style-type: none"> • Lists enable administrators to add and manage lists of values for different fields for use in queries and correlation rules. • cWatch features three kinds of Lists which are Live Lists, Range List and IP Range. • Lists can be created and the values can be updated manually. • Live Lists can be also be configured to be fetched from outputs of correlation rules. • The updates in a list will be immediately reflected in the queries and the rules in which it is used, relieving the administrator from the burden of updating queries and rules for change in values to be queried. • For more details on Lists management, see Lists. <p>On selecting [a] as the relation parameter, drop-down options will appear for the List and the List type:</p>  <p>The first drop-down shows the Lists that contain values for the selected query field. The second drop-down shows the List Types within the selected 'List'.</p> <ul style="list-style-type: none"> • Choose the List to be used in the query filter from the first drop-down. • Choose the sub list that contains the set of values to be included in the query filter from the second drop-down. <p>All the values contained in the list will be included as values for the Field specified in the filter statement.</p>
<p>{a}</p>	<p>Not in List</p>	<p>Allows you to configure the filter statement to search for the events that do not contain specific values from a pre-defined list .</p> <p>On selecting {a} as the relation parameter, drop-down options will appear for the List and the List type:</p>


		 <p>The first drop-down shows the Lists that contain values for the selected query field. The second drop-down shows the List Types within the selected 'List'.</p> <ul style="list-style-type: none"> • Choose the List to be used in the query filter from the first drop-down. • Choose the sub list that contains the set of values to be input as exclusions to the query filter from the second drop-down. <p>The results will display all events that do not contain the values in the lists.</p>
--	--	--

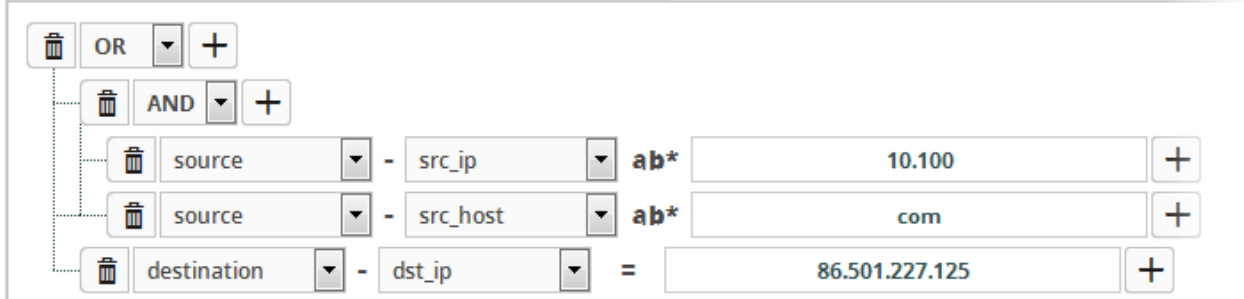
If you are adding values for source parameters like source IP address, source port, source MAC etc., but wish to reverse the parameter, click the switch icon  that appears to the right of the statement. The field group and the field selected will automatically switch from source to destination or vice-versa.

For example, if you are specifying a live list containing values of source IPs for the source IP field, but want to change them to destination IPs, you can click the switch button.








- To add more number of query filters under the same combination chosen in the first step, click the  button beside the same combination and repeat the process.

- To add a sub-filter statement, click the  button beside the filter and repeat the process.
- To set the relationship between each statement, use the drop-down menu.
- For example, the statements below will return events whose source ends with 10.100 OR .com AND whose destination is 86.105.227.125




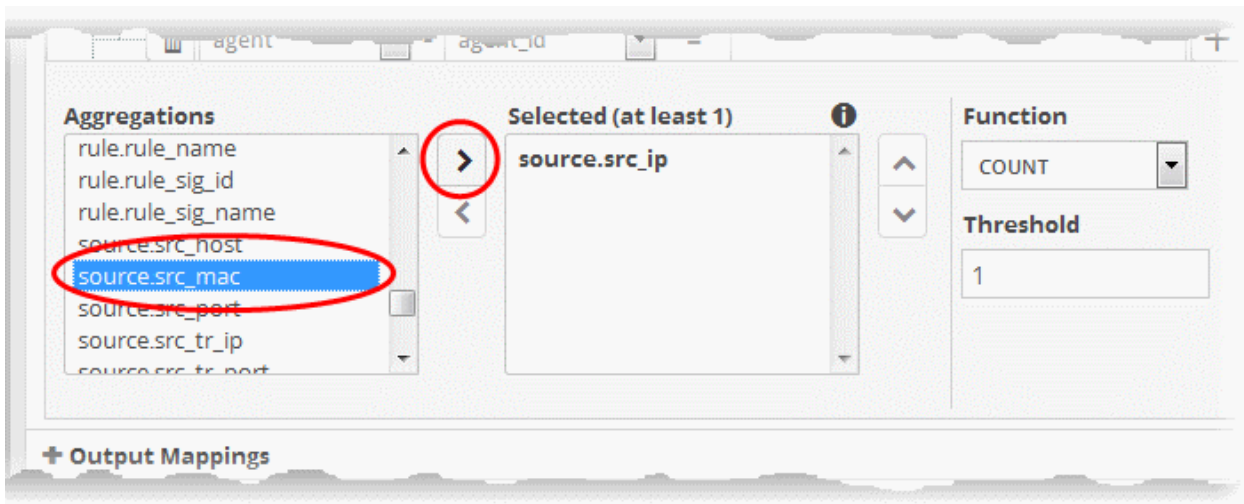
The screenshot shows a filter configuration interface with the following structure:

- Top level: **OR** (dropdown) 
- Second level: **AND** (dropdown) 
- Third level (under AND):
 - source (dropdown) - src_ip (dropdown) **ab*** [10.100] 
 - source (dropdown) - src_host (dropdown) **ab*** [com] 
- Fourth level (under OR):
 - destination (dropdown) - dst_ip (dropdown) = [86.501.227.125] 

- To delete a filter , click the  button beside it.




You can add multiple query definitions for a single rule and these are tied together.

- To add a new definition, enter the name of the new definition and add the filter statements as explained above.
- If you want the rules engine to process the definitions of the rule in order, select the 'Ordered' check-box.
 - For example, under the first tab you can create a rule that checks for a brute force attack on a destination IP and in the second tab you can create a rule for intrusion detection.
- The rules engine checks for brute force attack and intrusion events. If any destination IP in the second tab matches the destination IP in the first tab, then an incident is created. Note - the number of selected aggregates should be equal for all tabs in order to correctly define the fields in the **'Output Mappings'** section.
 - For example, if you select 4 aggregate fields in the first tab, then all other tabs for the rule should also have 4 aggregate fields.
- Incidents are logged and can be queried from the 'Event Query' interface.
 - For example, if you want the rule to search the source details from where the event occurred, then you have to select the appropriate event value in the 'Aggregations' box and move it to the 'Selected' box.
 - Select the required values from the 'Aggregation' box and move them to the 'Selected' box by clicking the  button.

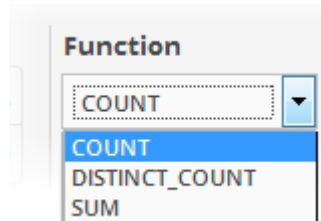


The screenshot shows the 'Aggregations' and 'Selected' interface with the following details:

- Aggregations:** rule.rule_name, rule.rule_sig_id, rule.rule_sig_name, source.src_host, **source.src_mac** (highlighted with a red oval), source.src_port, source.src_tr_ip, source.src_tr_port.
- Selected (at least 1):** source.src_ip (highlighted with a red circle).
- A red arrow points from the 'source.src_mac' field in the 'Aggregations' list to the right arrow button between the two lists.
- Function:** COUNT (dropdown).
- Threshold:** 1 (input field).
- + Output Mappings:** (button at the bottom).

- To remove a value added to the 'Selected' box by mistake, select it and click the  button.
- To reorder in the values in the 'Selected' box, select them one by one and click the  or  buttons.

The next step is to define the 'Aggregation Function' and 'Aggregation Threshold' for the defined query. The 'Function' drop-down has three options:



- **COUNT** - Select this if the incident is to be generated if the number of events that met the queries in the definition reach a certain number and enter the number in the Threshold field that appears on selecting this option.
- **DISTINCT_COUNT** - Choose this for the definition that checks for a range of events, for example, different source IPs to a single IP, choose the event items in the 'Distinct Field' combo boxes and enter the value in the 'Threshold' field.
- **SUM** - Choose this for the definition that checks for a numeric value, for example, number of bytes transferred or the rule hit count, select the event item in the 'Sum (Count)' field and enter the value in the 'Threshold' field.

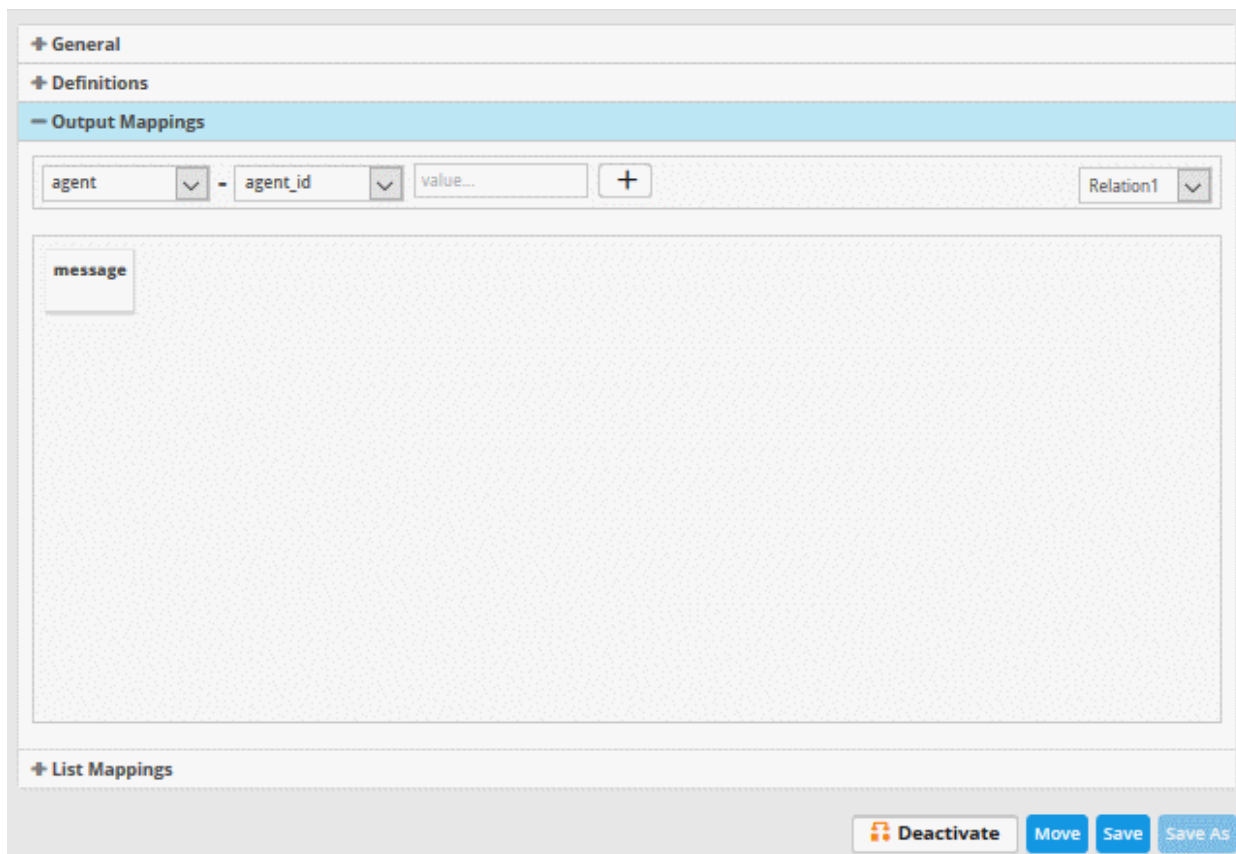
You can create any type of rules as required for your customers. For better insight into rules creation, please check out the built-in predefined rules on the left side of the 'Correlation Rules Management' screen.

Output Mappings

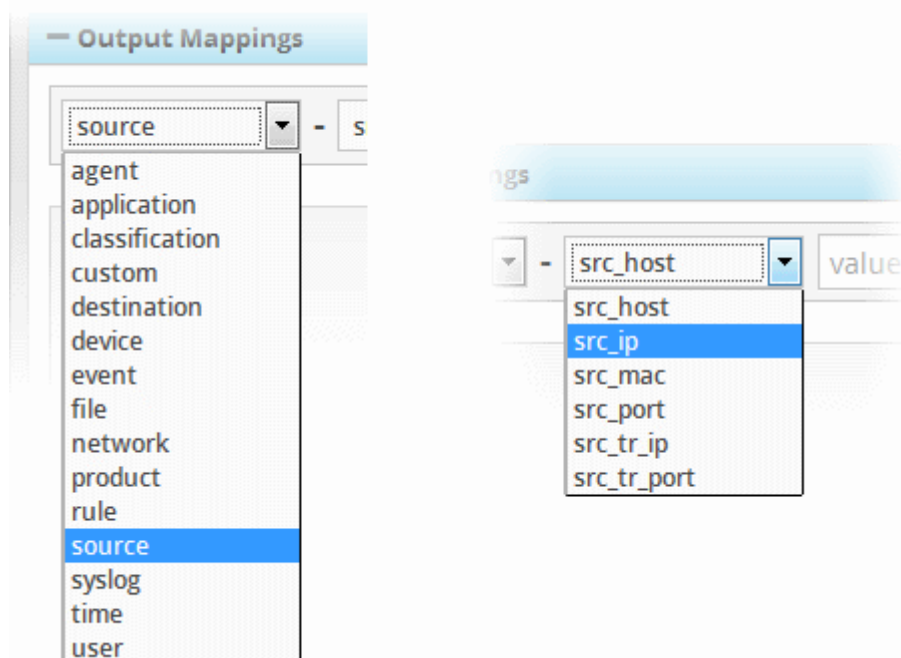
- In addition to generating an 'Incident', cWatch Network generates a new event as output event every time events are detected as per a correlation rule.
- The output event can be queried from the 'Event Query' interface and its details can be used to generate further event queries for the customer.
- The 'Output Mappings' area allows you to define the values to be fetched for selected fields of the output event from the respective input events detected by the rule.
- You can choose only values that are common to all the input events that generated an 'Incident' as per the rule.

To configure output mappings for the rule

- Click the 'Output Mappings' Stripe to open the 'Output Mappings' area.

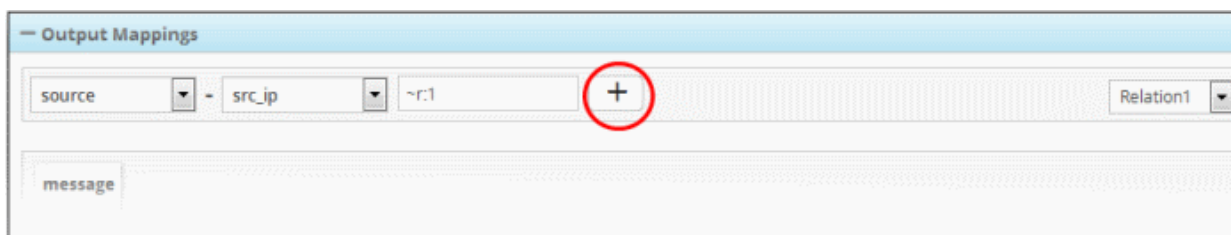


- Choose the Field to be configured for the output event by selecting the Field Group from the first drop-down and the field from the second drop-down.




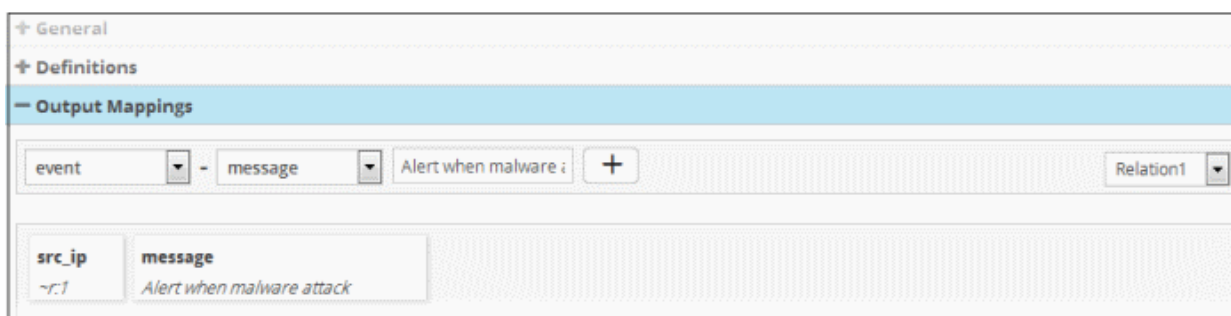
- In the 'Value' field, select the variable from the 'Relation' drop down at the far end that will fetch the value of the selected aggregate field in the 'Definitions' tab. The variable will be in the format ~r:1, ~r:2 and so on. For example selecting 'Relation1' from the drop down will auto fill ~r:1 in the value field. The variable '~r:1' will fetch the value of the first selected aggregate parameter, the variable '~r:2' will fetch the value of the second selected aggregate parameter and so on. If you enter some text, the field value will be static for that field for the new event generated on correlation.

- Click the  button to add the field value.



If you enter some text, the field value will be static for that field for the new event generated on correlation. For example, to enter a message for the 'Message' field, choose 'Event' > 'Message' from the drop-downs and enter the

message in the third field. Click the  button to add the field.



- Add more fields to fetch the values for, by repeating the same procedure.

List Mappings

- Each Live List managed from the 'Lists' > 'Live List Management' interface, is configured to contain a list of defined values of a specific field value.
- The live lists can be used to provide values for respective fields in event queries or in correlation rules relieving the administrator to enter several values for a single field one by one.
- Also, when a list is updated with addition of new values or removal of existing values, the query/rule in which it is used is automatically updated, hence the administrator need not modify the query/rule every time for changes in values.
- The values in a list can be populated in two ways:
 - Manual - The administrator can manually enter the values for the field in the respective list, from the 'Live List Content Management' interface, accessible by clicking 'Lists' > 'Live List Content Management' from the navigation menu.
 - Automatic - From the events detected by a correlation rule. The administrator can map a rule to Live Lists and configure the fields of the events from which the values are to be updated to the respective list.

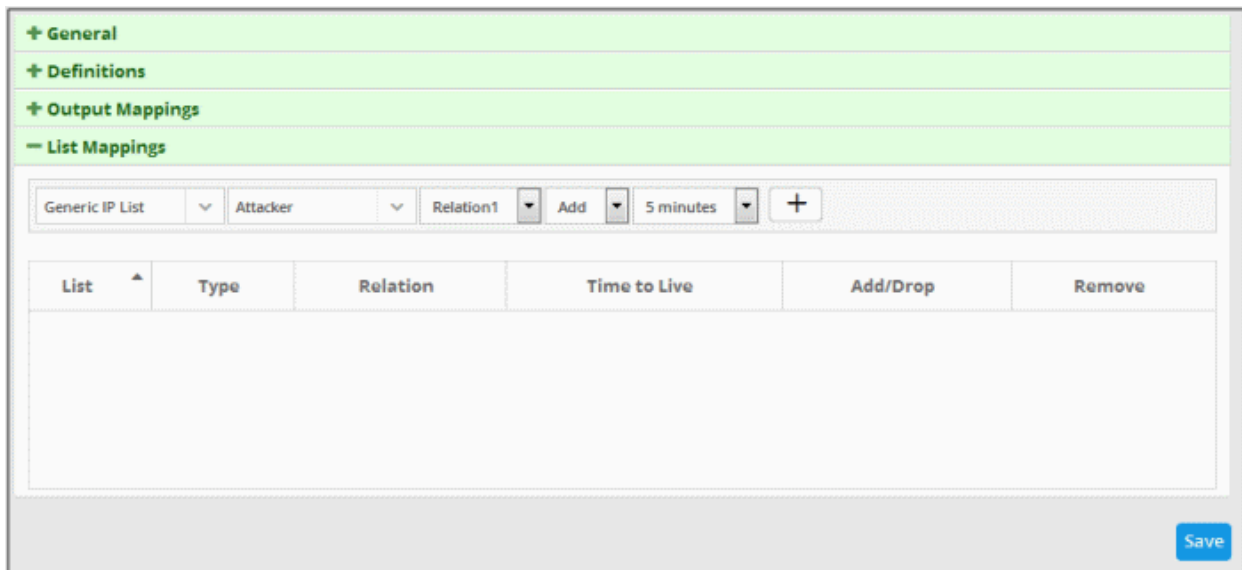
See '[Live Lists](#)', for more details on managing Live Lists.

- The 'List Mappings' area allows you to choose the Live Lists to which the selected field values of the events detected by the rule are to be automatically updated.
- As a prerequisite, you should have chosen the field values to be collected, as the aggregation parameters for the query defined in the rule.
- For example, if you want to collect the source IP addresses from the events identified by a rule that detects access to malware domains, in a live list that contain list of IP addresses of infected endpoints, you can map the respective live list to the rule and configure for the values of source IP address fields of the events to be fed to the list. The 'Source IP' field should have been set as a aggregation parameter in the query

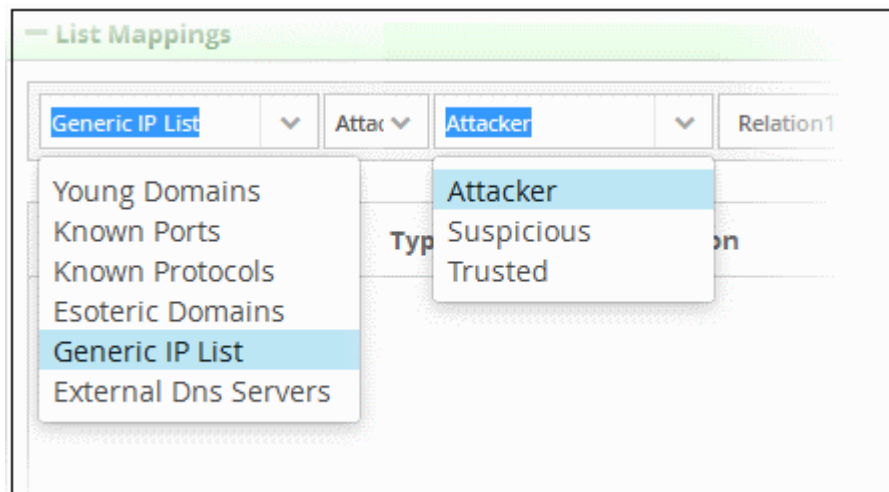
defined for the rule.

To map live lists to a rule

- Click the 'List Mappings' Stripe to open the 'List Mappings' area.



- Choose the list to be updated by selecting the 'List' from the first drop-down and the 'List Type' from the second drop-down.



More details on Lists and List Types are available in the chapter [Live Lists](#).

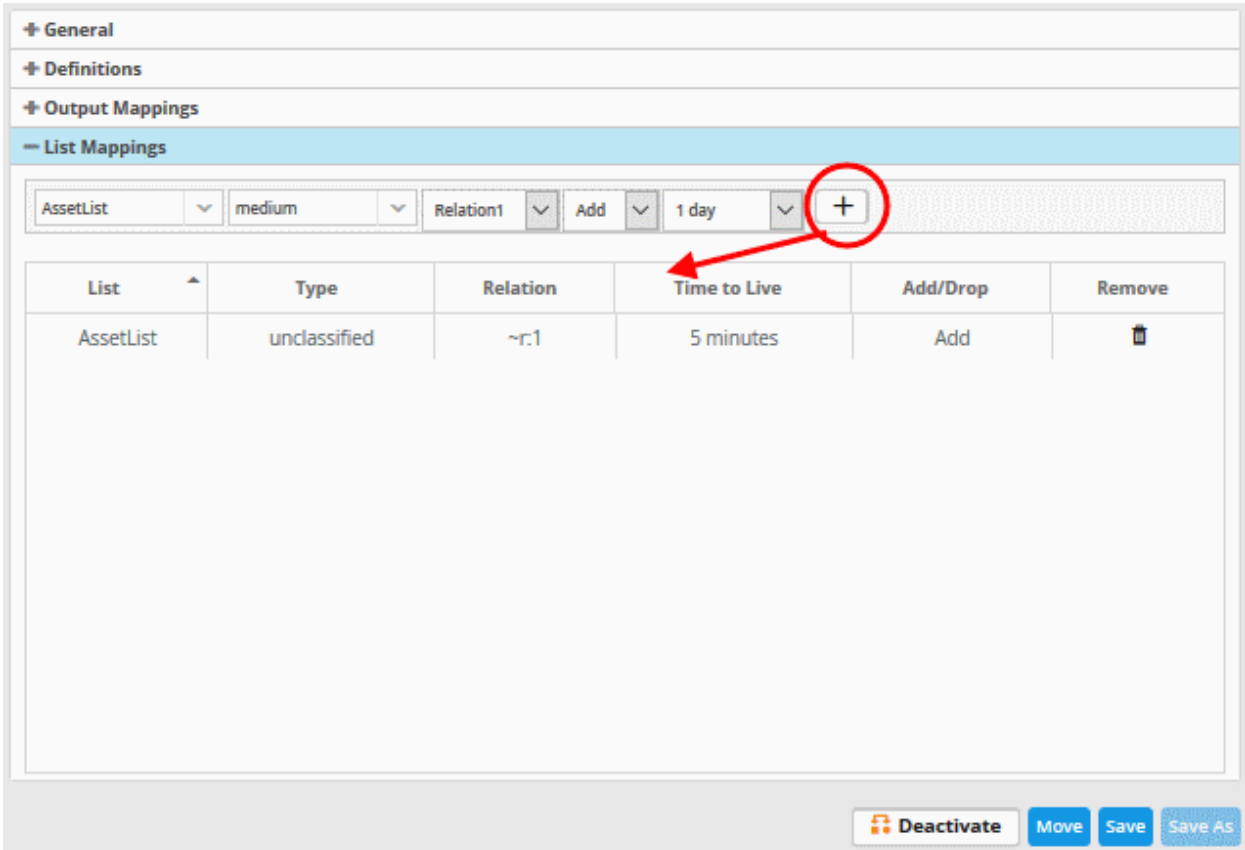
- In the 'Relation' field, select the variable that will fetch the value of the selected aggregate field from the 'Definitions' area. The variable will be in the format ~r:1, ~r:2 and so on. For example selecting 'Relation1' from the drop down will auto fill ~r:1' in the relation column. The variable '~r:1' will fetch the value of the first selected aggregate parameter, the variable '~r:2' will fetch the value of the second selected aggregate parameter and so on. Care should be taken that the field values contained in the specified list should be same as the aggregate parameter chosen by entering the relation parameter.


For example, If the list contains Source IPs, and if the 'source.src_ip' is chosen as first aggregate parameter for the rule, then for collecting the source IPs from the events identified by the rule, select 'Relation1'.

- Select 'Add' if the output is to be populated in the Live List Content interface. Select 'Drop' to remove the output from the Live List Content interface. For example, if the output value of an IP is 87.250.255.234 and if this value exists in the live list contents, then this will be removed from the content list.
- Choose the validity period for the value in the live list from the Time To Live (TTL) drop-down that appears next. The options available are from '5 minutes' to 'No Limit'. On lapse of the TTL period, the value fetched


to the list by the rule will be automatically deleted.

- Click the  button to add the list mapping.



List	Type	Relation	Time to Live	Add/Drop	Remove
AssetList	unclassified	~r.1	5 minutes	Add	

- Repeat the process to add more number of list mappings to the rule to fetch values from different fields for different live lists.

To remove a list mapping entry added by mistake or that is no longer needed, click the  icon under the 'Action' column for that mapping entry.

- Click the 'Save' button, to save your rule for the customer.
- Click the 'Save As' button, to create a new correlation rule
- Click the 'Deactivate' button, to disable the rule
- Click the 'Move' button, to change the folder of the current rule

The rules engine checks the events from the logs and if it matches the rule, generates an alert and creates an incident created. Also a new event is generated which will have the selected field values selected in the 'Output Mappings' area. If there are more than one query definition tabs are added for a rule, please make sure the number of selected aggregates is equal for all the tabs in order to correctly define the fields in the '**Output Mappings**' section. For example, in the '**Definitions**' section if you select 4 aggregate fields in the first tab, then all other tabs for the rule should also have 4 aggregate fields.

Editing a correlation rule

Correlation rules can be edited at anytime to change the name, query definitions, output mappings and list mappings.

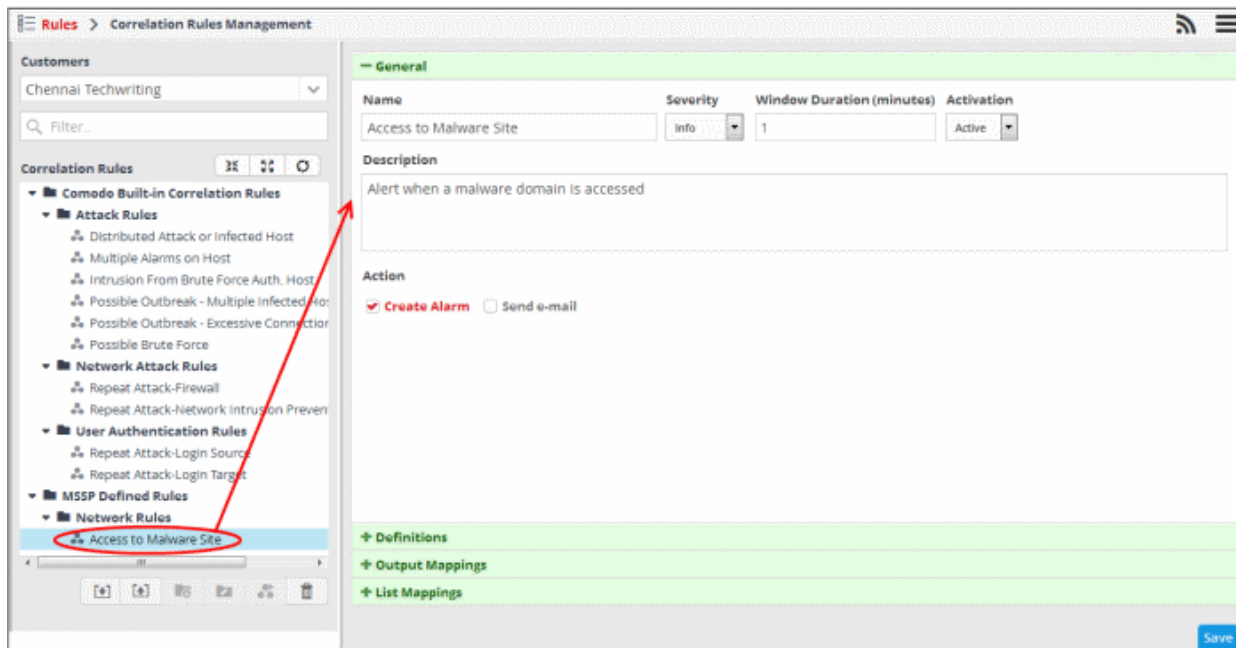
To edit a rule

- Choose the customer from the 'Customers' drop-down at the top of the left panel.

The predefined and custom rules added for the customer is displayed as a folder tree structure in the 'Correlation Rules' pane.


- Choose the rule to be edited.

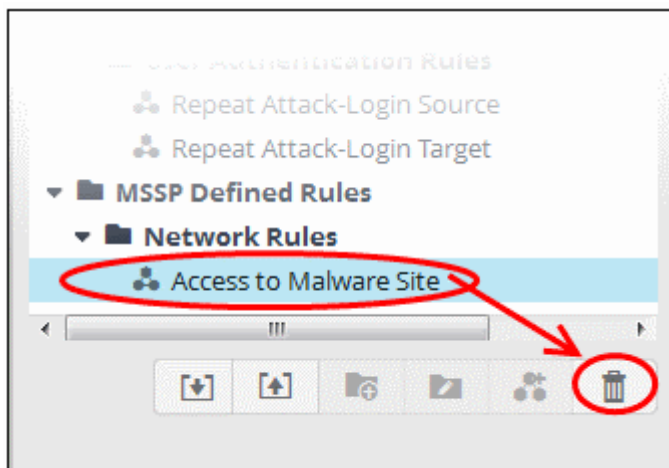
The configuration panel for the rule is displayed at the right.



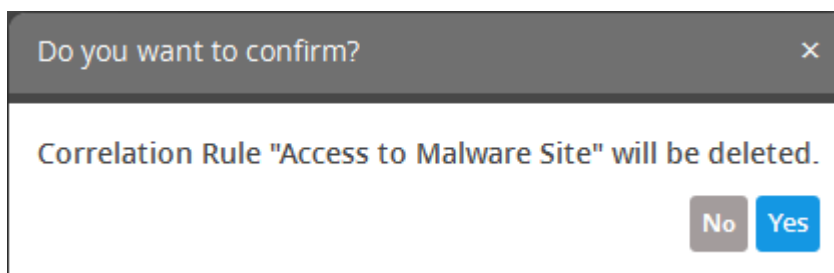
- Edit the rule as required. The procedure is same as adding a correlation rule. See [creating a correlation rule](#) for more details.
- Click the 'Save' button to save your changes.

Deleting a correlation rule

- To delete a correlation rule, select it and click the  button



A confirmation dialog will appear.



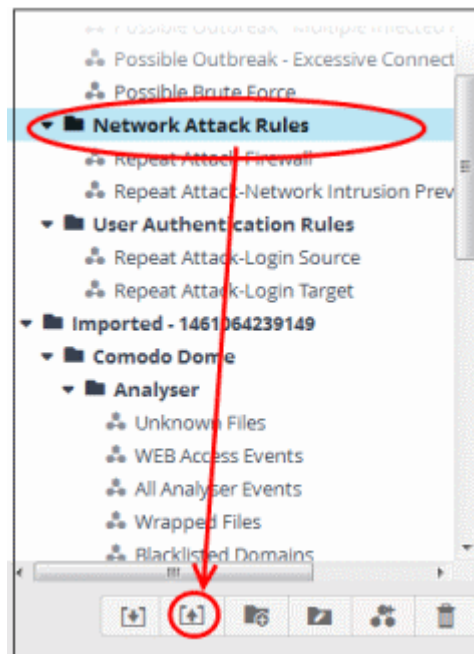
- Click 'Yes' in the confirmation dialog to remove the rule.

Exporting Correlation Rules

- cWatch Network allows administrators to save correlation rules, which are defined from event queries, in order to use them for other customers.
- The imported queries or rules can be used as is or altered to suit the requirements of the customer. You can export a rule folder or a particular rule.
- Please note - exported event queries can only be imported to their respective sections.
- For example, event queries exported from the reports section can only be used in the report section. Also the values in the filter items in the exported events for tagged and list events will be set to default values.

To export a rule or rule folder

- Select the customer from the 'Customers' drop-down at the top of the left hand side panel.
- Choose the rule or rule folder to be exported, from the 'Rules' list at the left.
- Click the 'Export' button at the bottom



For some browsers, the file with extension 'nxm' will be downloaded to the default download folder.

The saved rule(s) can be imported for use with another customer account.

Importing Correlation Rules

Administrators can import saved correlation rules to use them for other customers.

The imported rules can be used as is or altered to suit the requirements of the customer.

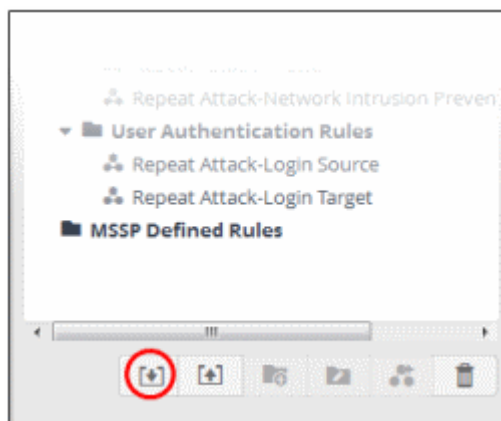
Please note - exported event queries can only be imported to their respective sections.

For example, event queries exported from the reports section can only be used in the report section. Also the values in the filter items in the exported events for tagged and list events will be set to default values.

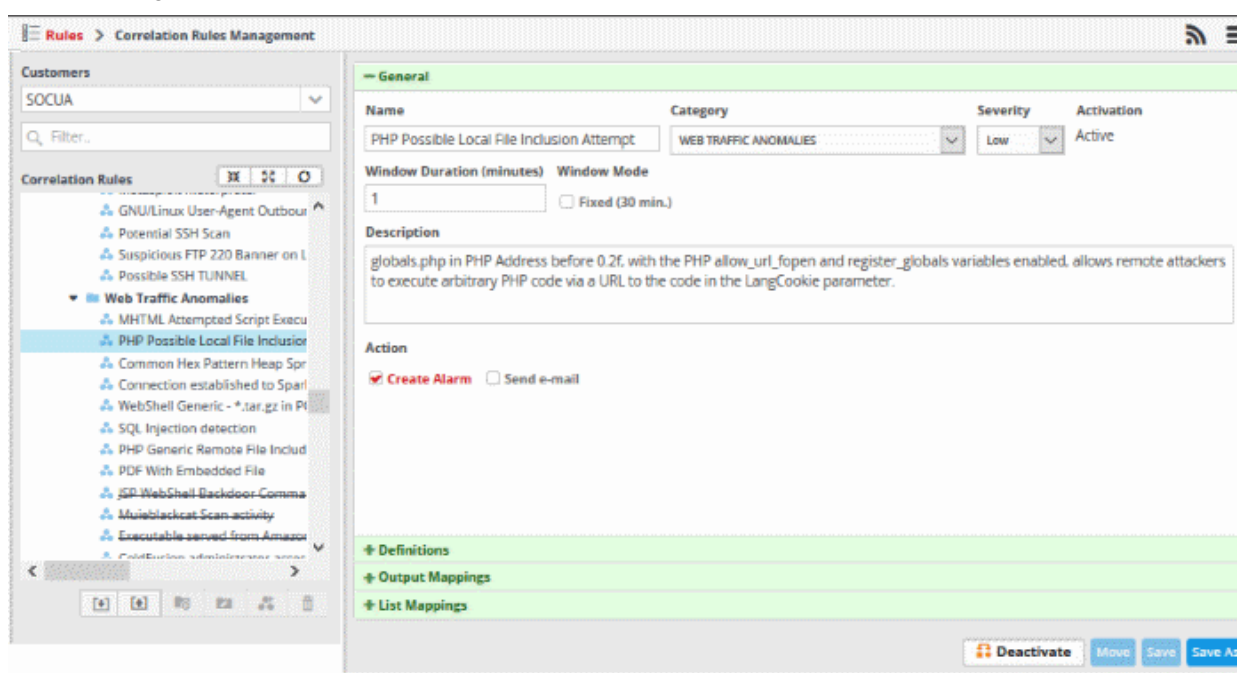
To import a query or query folder

- Select the customer from the 'Customers' drop-down at the top of the left hand side panel for which you want to import the saved queries

- Click the 'Import' button at the bottom

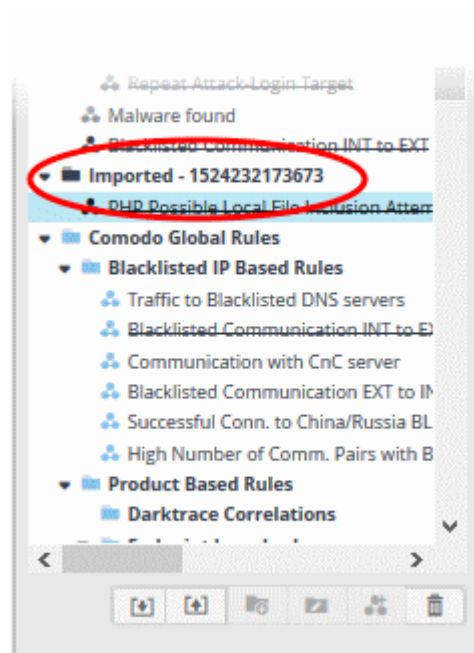


- Navigate to the location where the rules file is saved.



- Select the file and click 'Open'

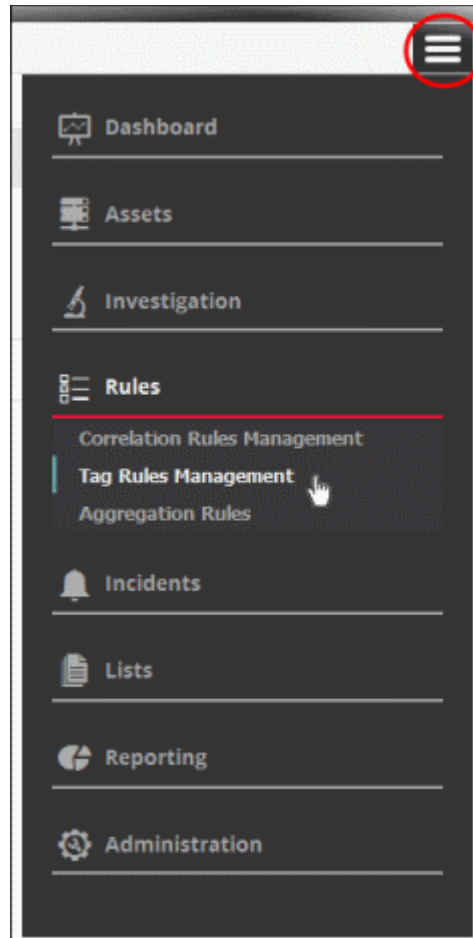
The rule or rules folder will imported and will be listed under 'Imported' folder.



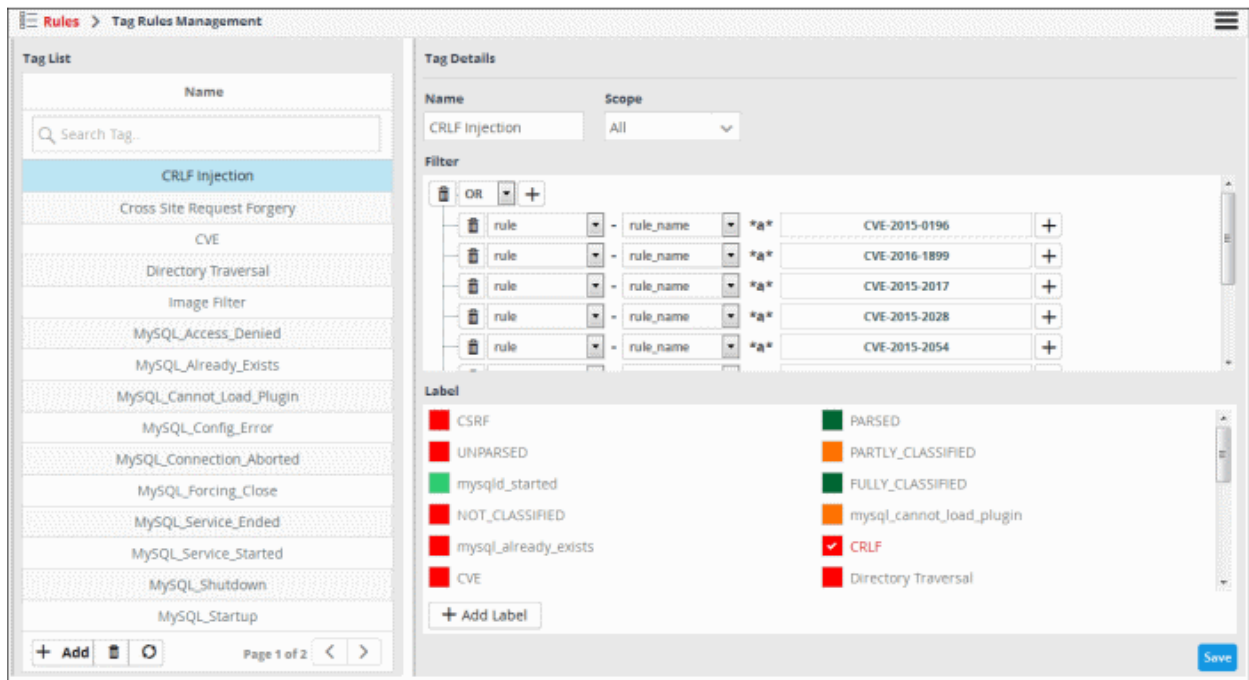
You can use the rules as it is or alter according to your requirement. Please note you can also import saved event queries and configure the mandatory settings, that is, 'General' and 'Definitions'.

5.2 Manage Tagged Rules

- The 'Tagged Rules' interface lets you create rules to monitor network activity for specific events. You can tag those events with labels of your choice.
- If a matching event is found in the streaming logs then it is tagged with your label.
- Tagged events can be queried from the **'Event Query'** page in the **Investigation** section.
- Tagged rules can be applied to customers by their assigned administrators.
- Click the 'Menu' button > 'Rules' > 'Tag Rules Management' to open the tag-rules management interface:



The 'Tag Rules Management' interface will open



The left-panel shows existing tag rules. The main panel shows the parameters of the selected tag rule. You can configure the rule from here.

Tag Rules Management Interface - Table of controls	
	Search for a particular tag rule. Enter the name of the rule fully or partially and click the search icon. The rules matching the entered text will be listed. To view the full list of rules again, clear the search field and press 'Enter'
	Allows you to add a new tag rule
	Allows you to delete selected tag rules
	The refresh button allows to instantly update the rules list
	Allows you to add a new name for the tag
	Allows to select customers to whom the tag rule will be applied
	Allows you to configure filter parameters for a tag rule
	Allows you to add new labels for tag rules
	Allows you to save the configured tag rule

The interface allows administrators to:

- **Manage a tag rule**
- **Create a new label**

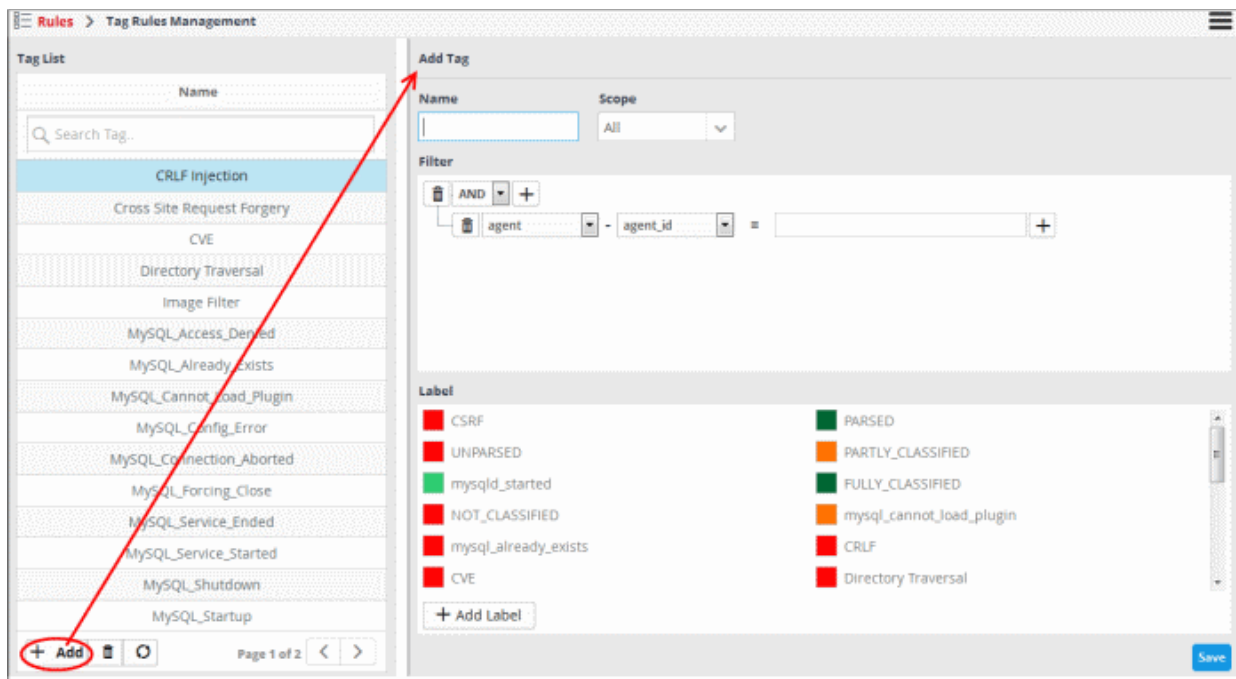
Manage a Tag Rule

From the Tag Rules Management interface, you can create a new tag rule, edit it and delete if no longer required.

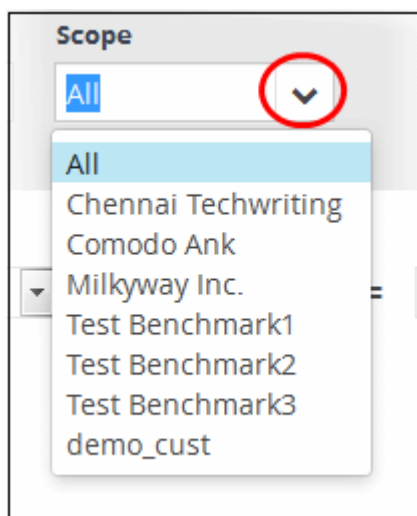
To create a new tag rule and apply it for a customer

- Click the 'Add' button at the bottom of the left pane

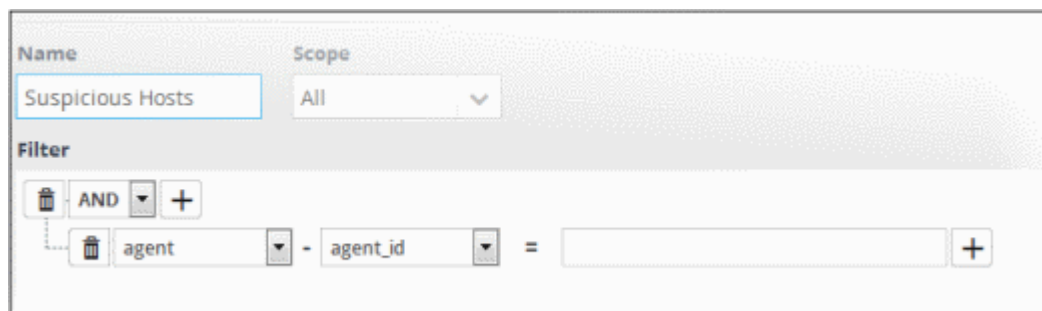
The 'Add Tag' screen will be displayed on the right side.



- Enter a new name for the tag rule in the 'Name' field
- Select the customer to whom the rule will be applied from the 'Scope' drop-down. Please note that you can apply the rule for all customers or any one customer. If you want to apply it to two or more customers, create a similar tag rule and apply it for each customer.



The next step is to add filters for the tag rule. By default, the 'AND' operator, 'agent' field group and 'agent_id' field will be displayed under the 'Filter' section.



The process of adding filters is same as explained in '[Configure Event Queries](#)'. [Click here](#) to view the details

about adding filters. An example of filters added to a tag rule is shown below:

Tag Details

Name: MySQL_Forcing_Close Scope: All

Filter

AND +

- product = MySQL_Error +
- event - message *a* Forcing close +

Label

- CSRF
- UNPARSED
- mysqlid_started
- NOT_CLASSIFIED
- PARSED
- PARTLY_CLASSIFIED
- FULLY_CLASSIFIED
- mysql_cannot_load_plugin

After adding filters for a tag rule, the next step is to label it.

- Select a label from the 'Label' section. If you haven't yet created a label you can add one by clicking the 'Add Label' button. See '[Create a New Label](#)' for more help with this.

Tag Details

Name: Suspicious Hosts Scope: All

Filter

AND +

- source = 198.1.2.100 +

Label

- PARSED
- Test Malware
- FULLY_CLASSIFIED
- Network Event
- LogsFromAnkara
- MALWARE
- UNPARSED
- PARTLY_CLASSIFIED
- NOT_CLASSIFIED
- HTTP
- suspicious_hosts

+ Add Label

Save

- Click the 'Save' button.

The tag rule will be saved and listed on the left. The rules will be checked every 15 minutes by cWatch and the events will be updated accordingly.

Now that a tagged rule is created, you can search for event queries that match the tagged rules.

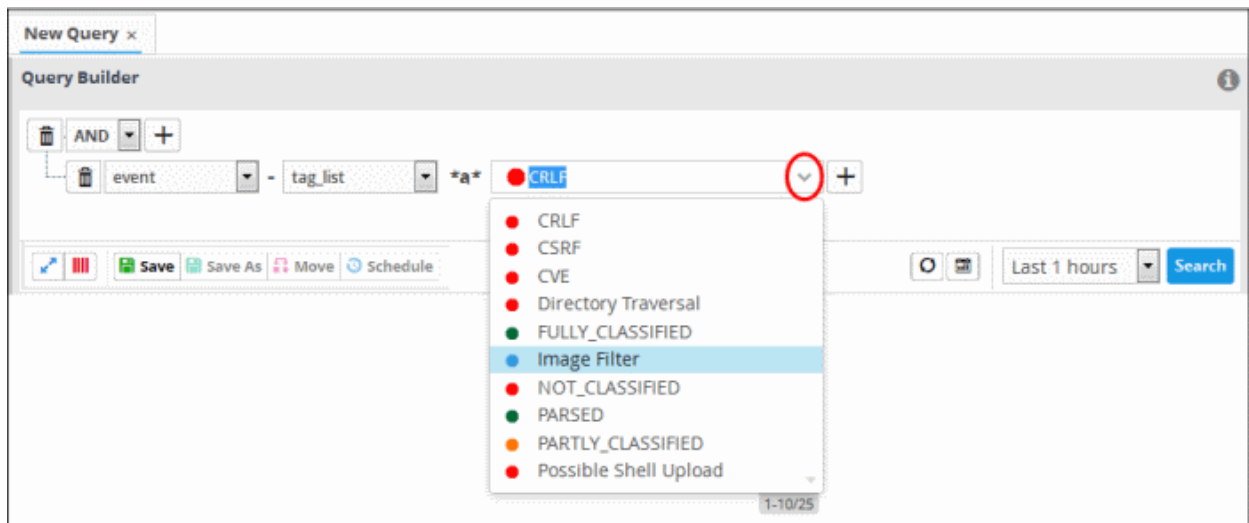
- To do that, click the menu button, then 'Investigation' > 'Event Query'.

See '[Configuring Event Queries](#)', for details about query building.

A 'New Query' builder interface will be displayed. An example of query building for searching events that matches tag rules is shown below:



The value field drop-down will display all the tag rule labels added for the customer.



- Select the tag rule label from the list, select the search period from the 'Last...' drop-down and click the 'Search' button.

The query results that matches the tag rule conditions will be displayed:

Central Time	Device Host	Application Name	Name	tag_list	Message
2018-04-23 10:30:36.818	SOCUA	NxSensor_notice	Query: wpad	PARTLY_CLASSL... PARSED	DNS::Not_p53
2018-04-23 10:30:36.818	SOCUA	NxSensor_notice	Query: wpad	PARTLY_CLASSL... PARSED	DNS::Not_p53
2018-04-23 10:30:28.505	SOCUA	NxSensor_files	HTTP	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:28.482	SOCUA	NxSensor_files	HTTP	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:28.357	SOCUA	NxSensor_files	HTTP	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:28.338	SOCUA	NxSensor_files	HTTP	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:27.999	SOCUA	NxSensor_files	SSL	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:27.999	SOCUA	NxSensor_files	SSL	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:27.943	SOCUA	NxSensor_ssl	TLsv12	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:27.872	SOCUA	NxSensor_conn		PARTLY_CLASSL... PARSED	
2018-04-23 10:30:27.872	SOCUA	NxSensor_dns	A	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:27.848	SOCUA	NxSensor_dns	A	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:27.848	SOCUA	NxSensor_conn		PARTLY_CLASSL... PARSED	
2018-04-23 10:30:27.780	SOCUA	NxSensor_http	GET	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:27.662	SOCUA	NxSensor_files	HTTP	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:20.078	SOCUA	NxSensor_files	SSL	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:19.830	SOCUA	NxSensor_dns	AAAA	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:19.830	SOCUA	NxSensor_conn		PARTLY_CLASSL... PARSED	
2018-04-23 10:30:19.612	SOCUA	NxSensor_dns	A	PARTLY_CLASSL... PARSED	
2018-04-23 10:30:12.782	Centos71	linux-audit	SYSCALL	PARTLY_CLASSL... PARSED	audit(1524479412.782:...

- You can also view the tag associated with the event by clicking on an event log.

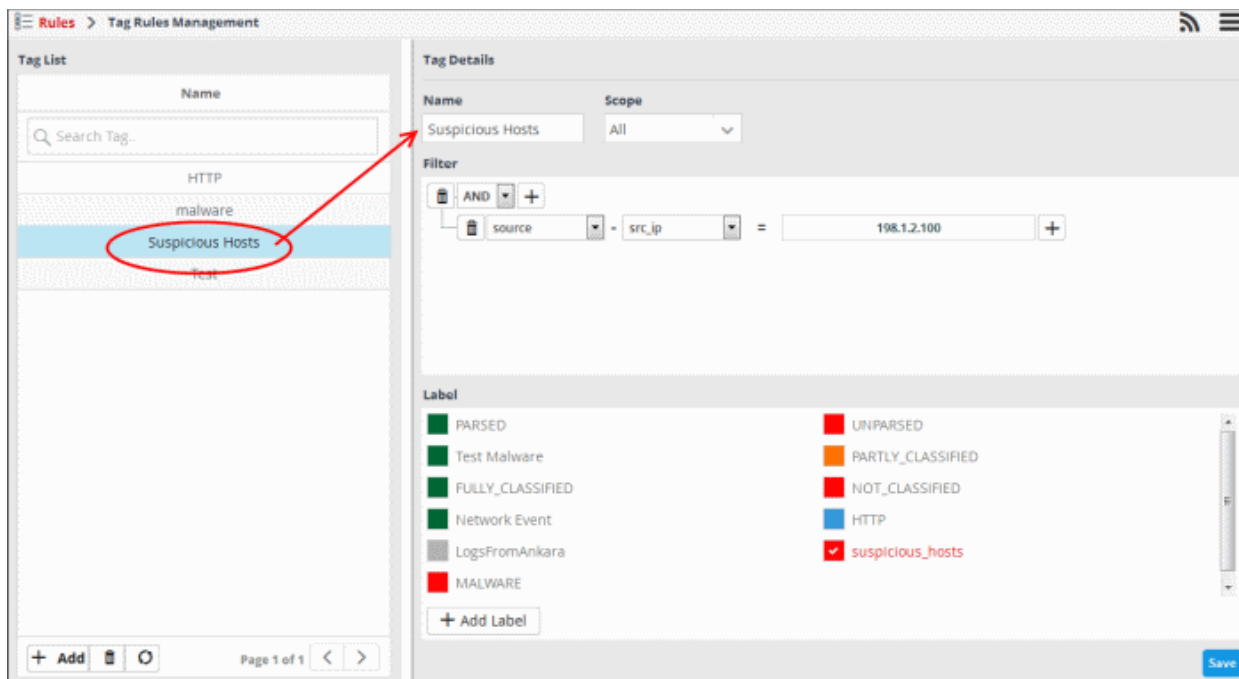
The screenshot shows the 'Results' tab with a table of events. One event is highlighted with a red circle. A red arrow points from this event to a 'Selected Result Fields' dialog box. The dialog box displays the following information:

- Application Name: NxSensor_files
- Central Time: 2018-04-23 10:30:27.999
- Destination IP: 10.100.164.34
- Destination Port: 0
- Device Host: SOCUA
- Name: SSL
- Source IP: 54.231.131.35
- Source Port: 0
- tag_list: PARTLY_CLASSL...
- Type: Access

Multiple 'tag_list' labels in the details dialog indicates that the event satisfies more than one tag rule. You can save the query and use the same for incident creation. See '[Configuring Event Queries](#)', '[Managing Correlation Rules](#)' and '[Managing Incidents](#)' for details about query building and configuring correlation rules in order to create incidents.

To edit a tag rule

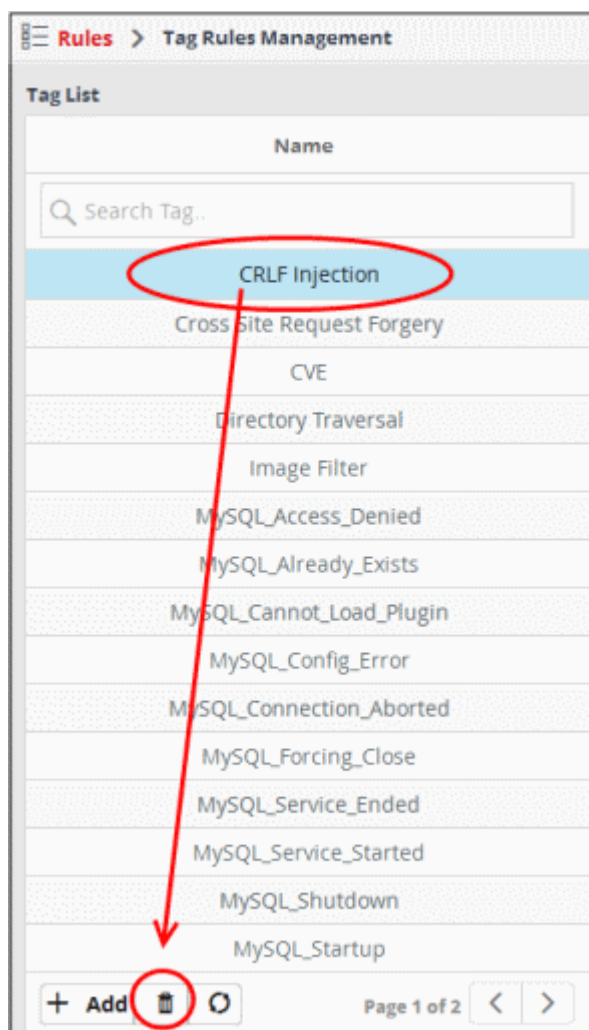
- Select the tag rule from the left menu



- To change the name, edit it directly in the 'Name' field
- To change the customer, select it from the 'Scope' drop-down. Please note that you can apply the rule for all the customers or any one customer. If you want to apply it to two or more customers, create a similar tag rule and apply it for each customer.
- If required, modify the filters as explained above.
- Change the label for the rule from the 'Label' section.
- Click the 'Save' button. The rules will be checked every 15 minutes by cWatch and the events will be updated accordingly.

To delete a tag rule

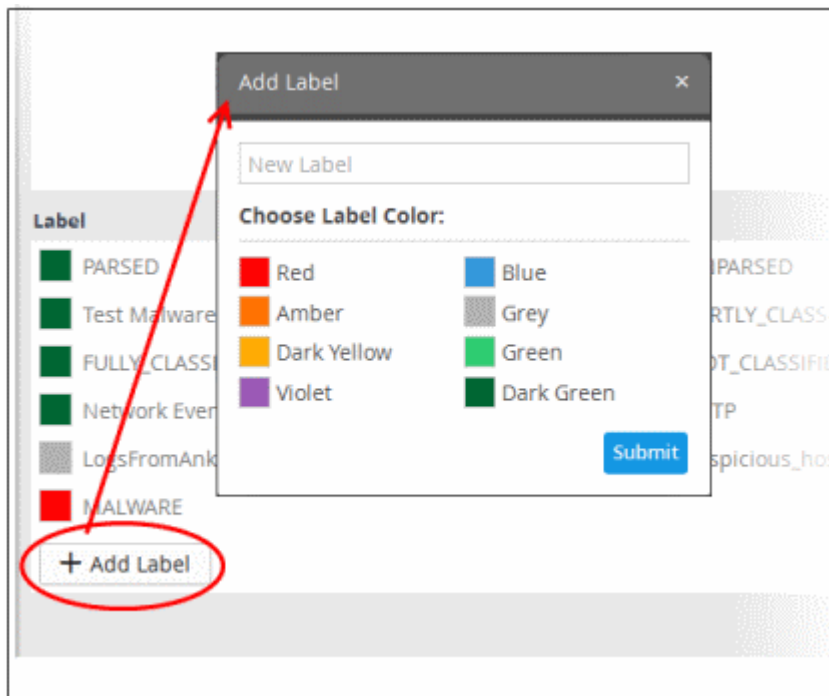
- Select the tag rule and click the trash can icon at the bottom



The selected tag rule will be removed from the list. Please note that the label associated with the rule will also be removed only in future events.

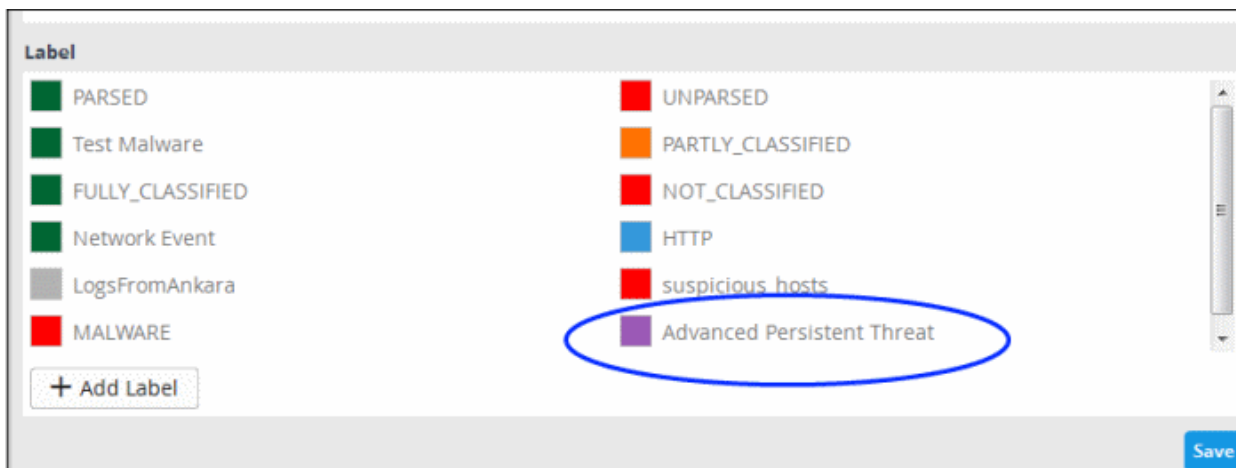
Create a New Label

- Click the 'Add Label' button at the bottom of the 'Label' section.



- Enter a name for the label in the 'New Label' field
- Select the color that should be displayed for the label in the event details dialog.
- Click the 'Submit' button

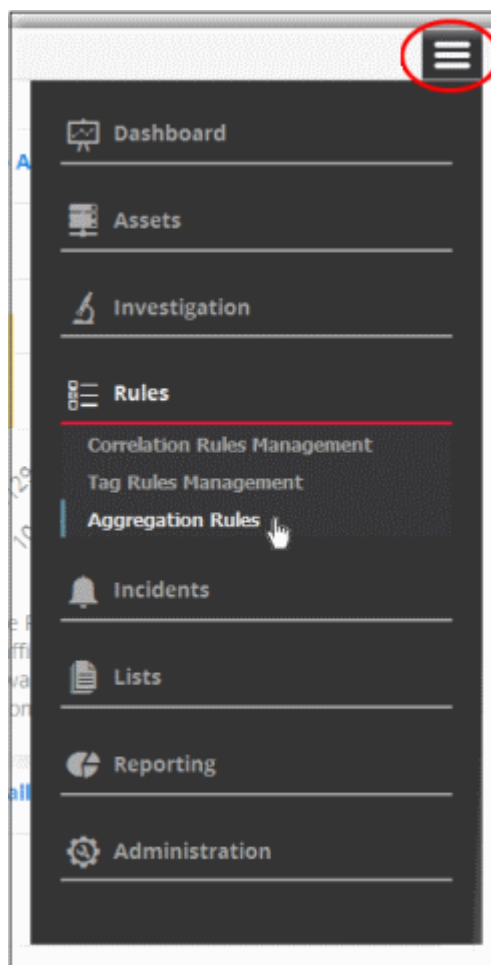
The new label will be added and displayed.



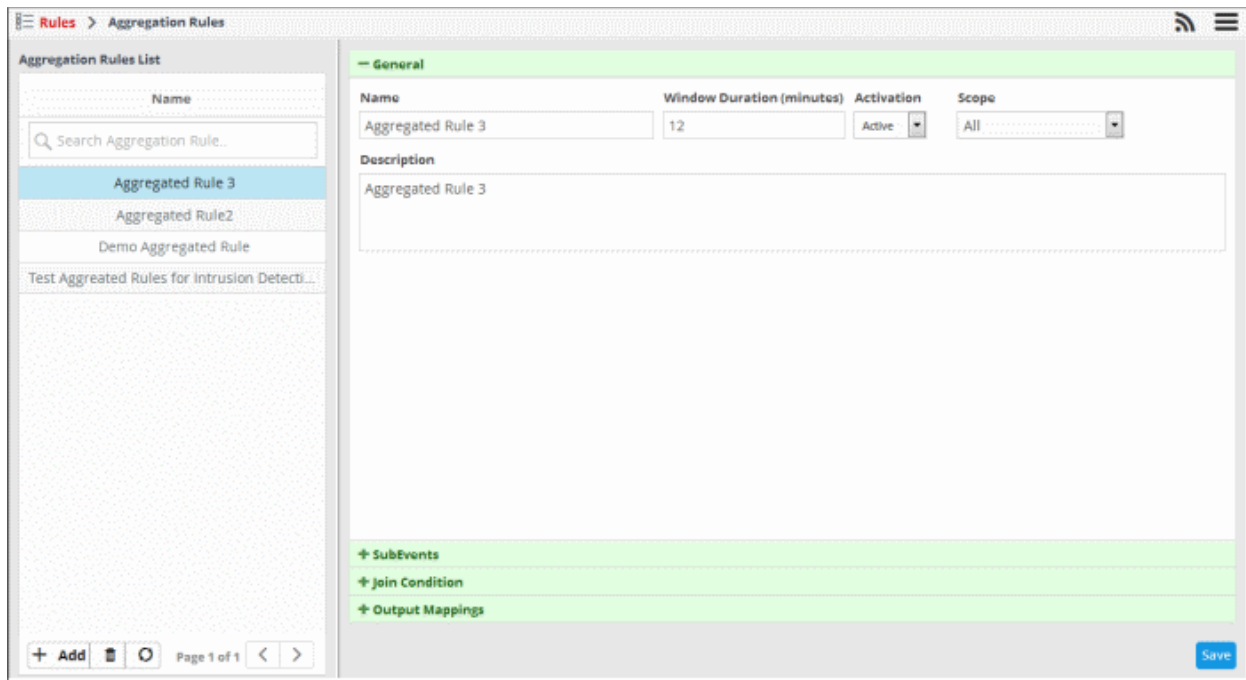
The newly added label can be used for a tag rule.

5.3 Manage Aggregation Rules


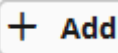


- The 'Aggregation Rules' interface allows you to log new events by configuring filters for sub-events and conditions that, when met, will create a new event.
- The aggregation rules filter lets you define highly granular event queries.
- For example, you can create an aggregation rule to generate a new event whenever a firewall event and access event for the same IP is detected. This event then can be queried from the **Event Query** page under **Investigation**.
- To open the 'Aggregation Rules' interface, click the 'Menu' button from the top right, choose 'Rules' and then click 'Aggregation Rules'.



The 'Aggregation Rules' interface will open:



The left hand panel shows configured aggregation rules. The right panel shows details of the rule chosen from the list and allows you to configure the rule.

Aggregation Rules Management Interface - Table of controls	
 Search Aggregation Rule..	Allows you to search for a particular aggregation rule. Enter the name of the rule fully or partially and click on the search icon or press 'Enter'. The rules matching the entered text will be listed. To view the full list of rules again, clear the search field and press 'Enter'.
	Allows you to add a new aggregation rule
	Allows you to delete selected aggregation rules
	The refresh button allows to instantly update the rules list.

The interface allows administrators to:

- **Create a new aggregation rule**
- **Edit an aggregation rule**
- **Delete an aggregation rule**

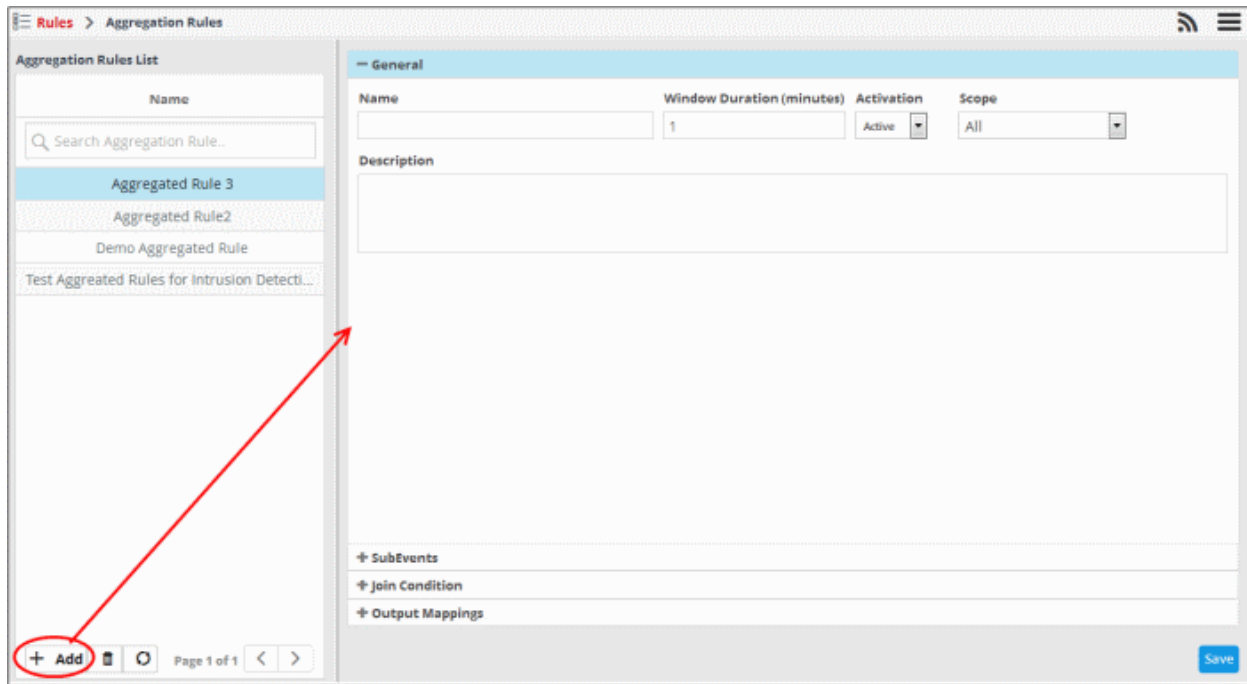
Create a New Aggregation Rule

You can create a new event from the output of configured sub-event queries and conditions.

To create a new aggregation rule

- Click the 'Add' button at the bottom of the left panel

The rule configuration screen will open on the right. It has four sections:



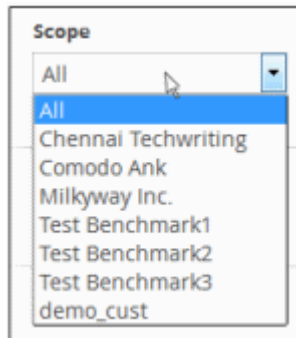
- **General** -
 - Specify a name and description for the rule.
 - Window duration (minutes) - The time span by which the join condition should be fulfilled
 - Activation - Enable or disable the rule
 - Scope - Select the customer to whom the rule should be applied.
- **Sub Events** - Allows you to define multiple event queries for the rule. The field values of the sub events will be used to check for conditions configured in 'Join Condition'.
- **Join Condition** - Allows you to configure field values that when matched in the sub events, a new event will be created per the output mappings. cWatch will check the field values of the sub events and if the join conditions are satisfied, then a new event will be generated.
- **Output Mappings** - Allows you to select the field values to be included in the output events generated if the join condition is true. The output events can be queried from the 'Event Query' interface.

General

- Click the 'General' stripe to open the general configuration area.

- **Name** - Enter a name for the rule
- **Window Duration (minutes)** - Enter the minimum duration (in minutes) for the join condition to be checked for the rule. For example, if you enter 5, the sub events join condition will be checked for every 5 minute cycle. If within the 5 minute window, say in the 1st minute, the join condition becomes true, an aggregated event is generated and the window is closed. The next cycle begins and so on.

- **Activation** - Choose whether you want the rule to be active or inactive from the drop-down
- **Scope** - Select the customer to whom the rule will be applied from the 'Scope' drop-down. Please note that you can apply the rule for all customers or any one customer. If you want to apply it to two or more customers, create a similar tag rule and apply it for each customer.

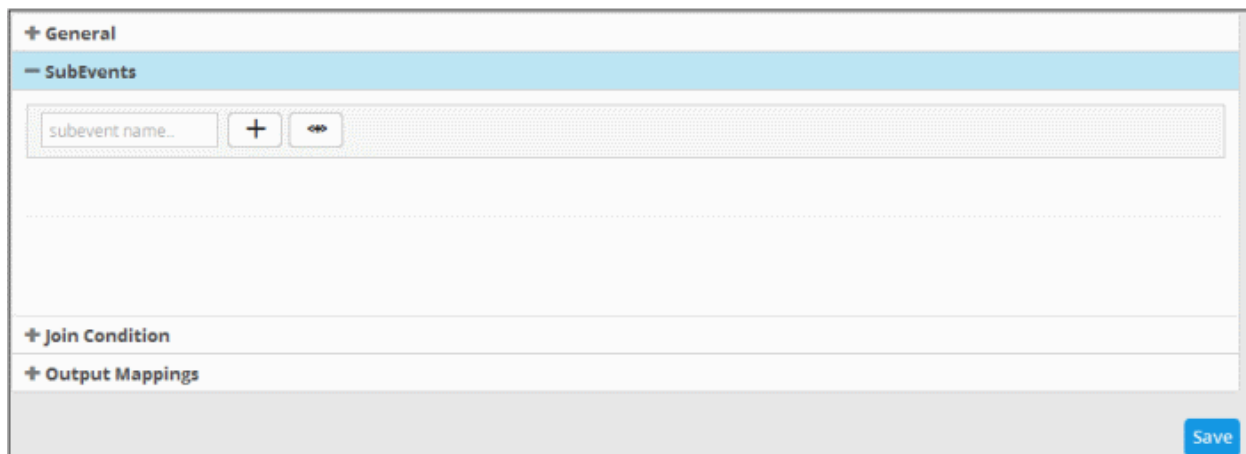


- **Description** - Enter an appropriate description for the rule.

Sub Events

Each sub event is constructed with a set of filter condition statement groups to identify the events. You can create multiple sub events for a rule. The 'Sub Events' stripe allows you to define filter statement groups for the rule. You can add filter statement groups by selecting saved queries and/or by manually defining them. Please note that you have to add at least two sub events to construct an aggregation rule.

- Click the 'Sub Events' stripe to open the 'Sub Events' area.




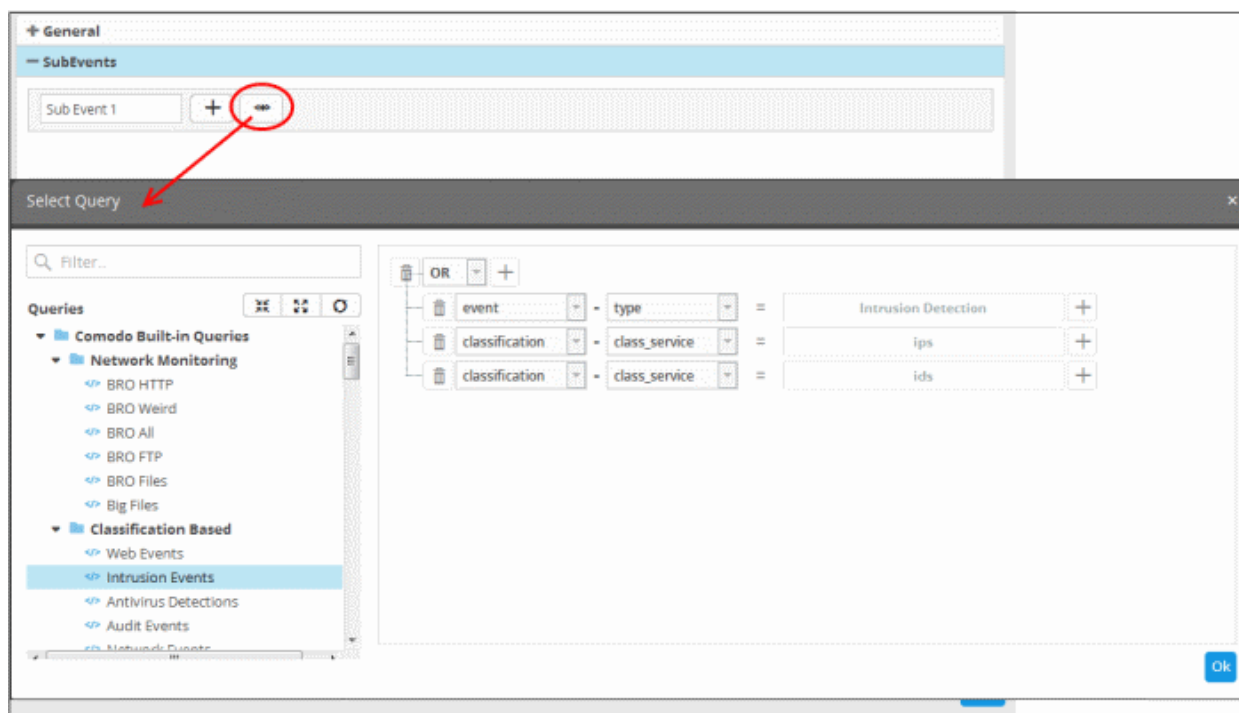
- To add a filter statement group for a sub event, enter a name for it in the 'Subevent name...' field

The next step is to add filter condition statement groups for the sub event. This can be done in two ways:

- **Select an Event Query and import the filter statement from it**
- **Manually define filter statements for the sub event**

Selecting an Event Query and import filter statements:

- Click the  button after entering a name for the sub event.



The 'Select Query' dialog will open with a list of pre-defined and custom event queries added for the customer in the left pane.

- Choose the query from the left pane.

The filter statements in the query will be displayed in the right pane.


- Click 'OK' to import the filter statements.

The sub event will be added with the group of filter statements from the query.

You can edit the group by adding new statement(s), changing fields/values and/or removing existing statements. See **'Manually defining filter statements for the group'** given below, for more details on the construction of filter statements.

- Repeat the process to add more definitions from event queries. Please note that you have to add at least two sub events to construct an aggregation rule.

Manually Define Filter Statements for the Sub Event

- Click the  button after entering a name for the sub event.

A tab to add the query fields for the definition will open.

Each rule definition is built with a set of filter statements that are connected with Boolean operators like 'AND', 'OR' or 'NOT'. Each filter statement contains the following components.

'Field Group' + 'Field' + 'Operator' + 'Value'

- **Field Group** - The group to which the field specified as the filter parameter belongs.
- **Field** - The field in the event log entry by which you want to filter results
- **Operator** - Controls the relationship between the field and the specified value. Examples include 'Equals to', 'Does not equal to', 'contains', 'does not contain' etc.
- **Value** - The value for the field. Values can be entered manually or fetched from a pre-defined list which is managed in the 'List Management' interface.
 - For example, if you choose a source IP (src_ip) as the field to be searched from network events, you can manually enter the IP address of the source of the connection request or choose a list containing a list of specified source IP addresses. See **Lists** for more details on pre-defined lists.

Examples:

- To filter network connection events originated from an endpoint with IP address 10.100.100.100, build the

filter statement as shown below:

'Source' + 'src_ip' + '=' + '10.100.100.100'

- ii. To filter network connection events originated from a set of endpoint whose IP addresses start with 10.100.100.xxx, build the filter statement as shown below:

'Source' + 'src_ip' + 'AB*' + '10.100.100'

- iii. To filter network connection events originated from a set of endpoint whose IP addresses are defined in the 'Live List type' named 'Internal' under the 'Live List' named 'IP Blacklist' build the filter statement as shown below:

'Source' + 'src_ip' + '[a]' + 'IP Blacklist' + 'Internal'

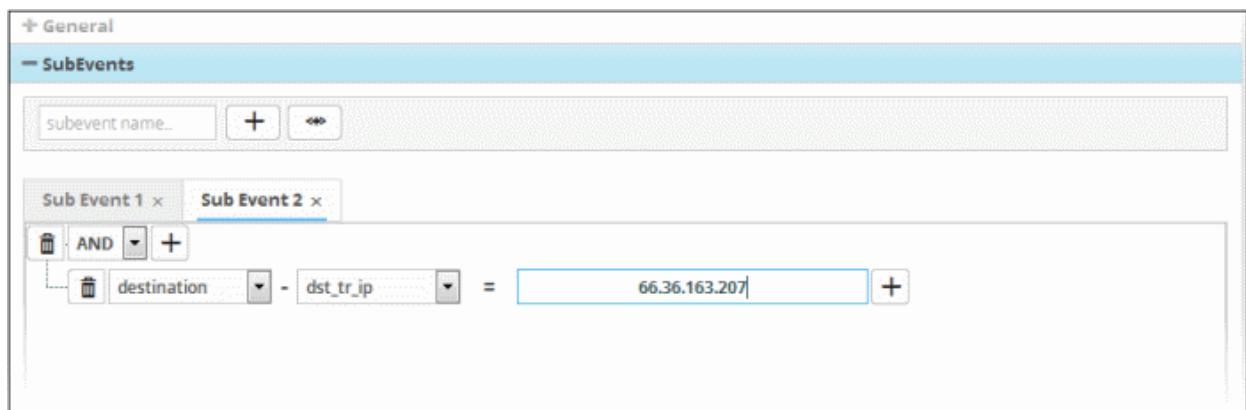
You can create more complex queries by adding more filter statements and linking them using 'AND', 'OR', or 'NOT'. For example:

- To filter network connection events originated from an endpoint with IP address 10.100.100.100, and destined to another endpoint with IP address 10.100.100.120, build the filter statements with an AND combination as shown below:


'Source' + 'src_ip' + '=' + '10.100.100.100'

AND

'Destination' + 'dst_ip' + '=' + '10.100.100.120'



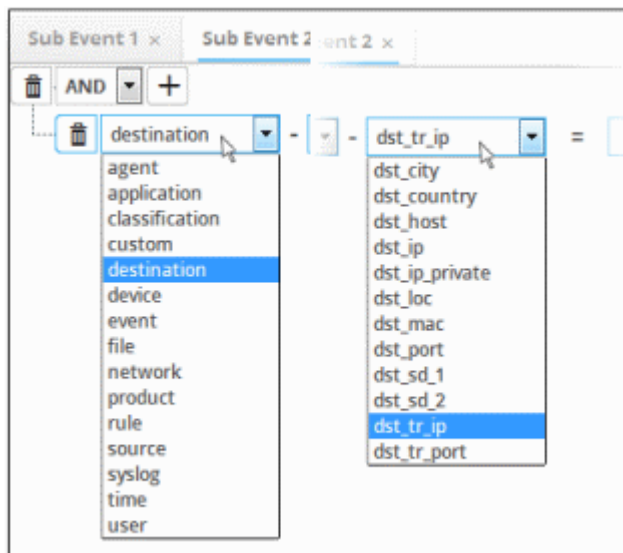
To manually add a filter statement group

- Choose the combination condition for the query(ies) to be defined from the drop-down at the top left. The options available are:
 - AND
 - OR
 - NOT
- Click the  button beside the drop-down to add a query filter.

The 'Field Groups' drop-down and 'Fields' drop-down will appear. The 'Fields' drop-down will contain options relevant to the 'Field Group' chosen from the drop-down at the left.

- Choose the field group you wish to add to the filter from the 'Field Groups' drop-down.

The next field will display the fields available for the selected field group.

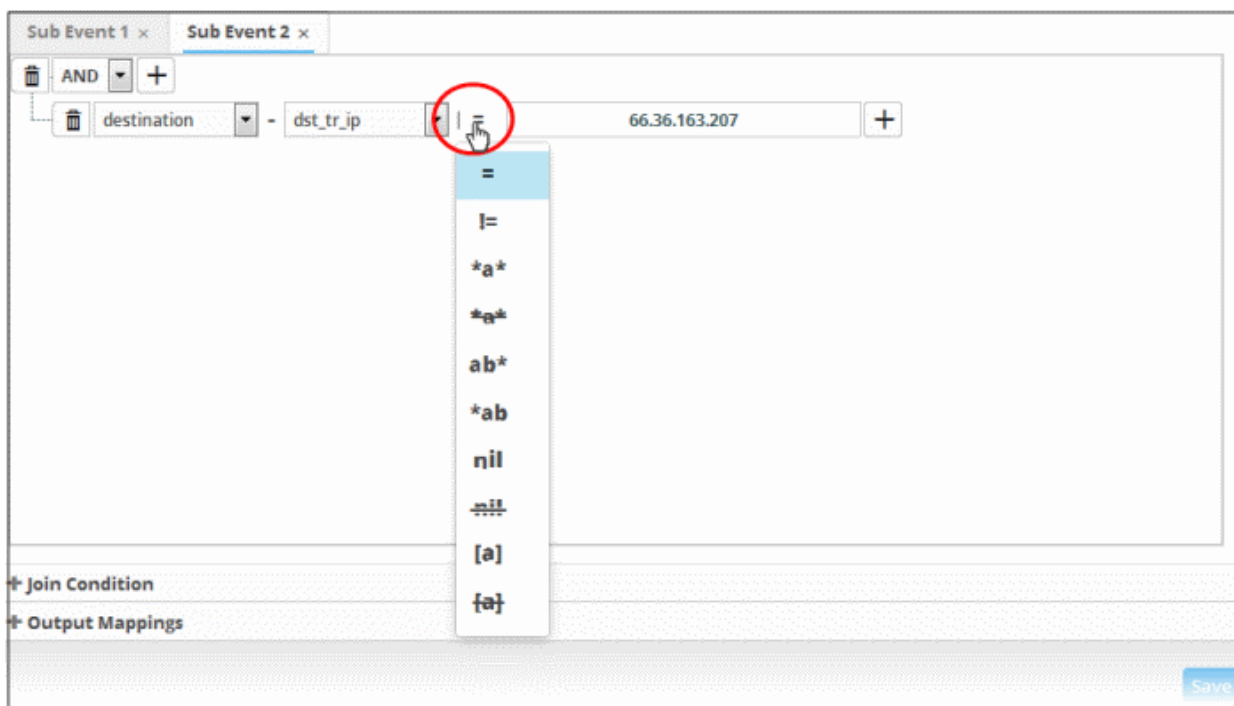


- Choose the field from the second drop-down.

Tip: The descriptions of the field groups and the field items under each of them, are available in [Appendix 1 - Field Groups and Event Items Description](#).

The next step is to choose the relationship between the field chosen and the value to be entered in the next field.


- To choose the relation, click on the relation symbol at the right of the 'Field' drop-down.

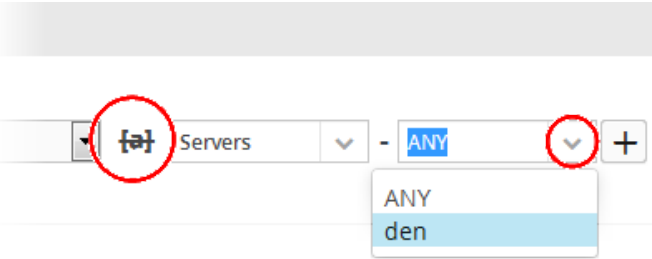



The types operators depends on the field chosen. The following table explains the various operator symbols:

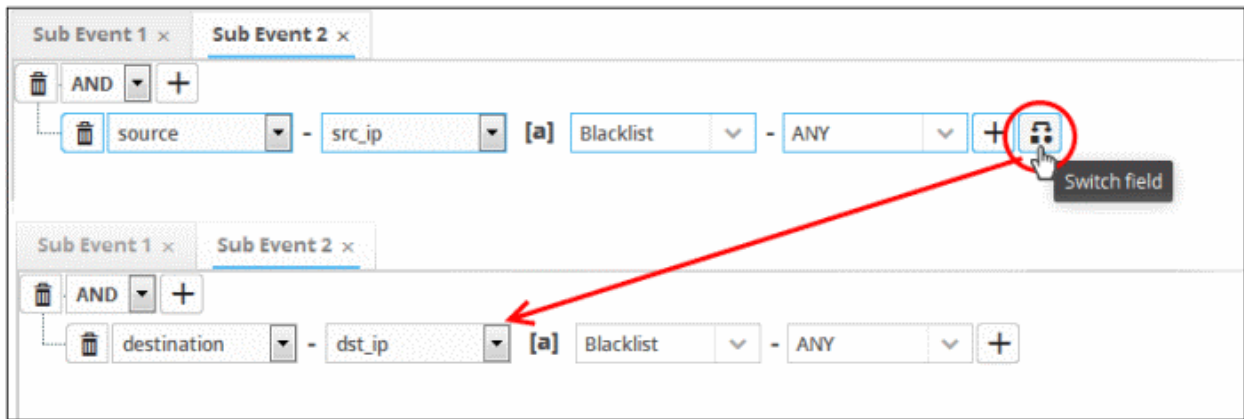
Relation Operator	Description	Entering the value for the 'Field'
=	Equals to	<ul style="list-style-type: none"> • Manually enter a value in the field to the right of the operator. • Events containing the same value will be identified by the filter.

!=	Does not equal to	<ul style="list-style-type: none"> Manually enter a value in the field to the right of the operator. Events that do not contain the value will be identified by the filter.
>	Greater than	<ul style="list-style-type: none"> Applicable only for fields with numerical values, for example, port numbers. Manually enter a value in the field to the right of the operator. <ul style="list-style-type: none"> The filter will identify events that contain values greater than the entered value.
>=	Greater than or equal to	<ul style="list-style-type: none"> Applicable only for fields with numerical values, for example, port numbers. Manually enter a value in the field to the right of the operator. <ul style="list-style-type: none"> The filter will identify events that contain values equal to or greater than the entered value.
<	Less than	<ul style="list-style-type: none"> Applicable only for fields with numerical values, for example, port numbers. Manually enter a value in the field to the right of the operator. <ul style="list-style-type: none"> The filter will identify events that contain values less than the entered value.
<=	Less than or equal to	<ul style="list-style-type: none"> Applicable only for fields with numerical values, for example, port numbers. Manually enter a value in the field to the right of the operator. <ul style="list-style-type: none"> The filter will identify events that contain values equal to or lower than the entered value.
a	Contains	<ul style="list-style-type: none"> Manually enter a value in the field to the right of the operator. The filter will identify events that contain the entered value somewhere in the string. <ul style="list-style-type: none"> For example, to search for events with source IP addresses containing 123 anywhere in the address, enter '123'.
a	Does not contain	<ul style="list-style-type: none"> Manually enter a value in the field to the right of the operator. The filter will identify events that do not contain the entered value anywhere in the string. <ul style="list-style-type: none"> For example, to search for events with source IP addresses that do not contain 123 anywhere in the address, enter '123'.
ab*	Starts with	<ul style="list-style-type: none"> Manually enter a value in the field to the right of the operator. The filter will identify events that begin with the

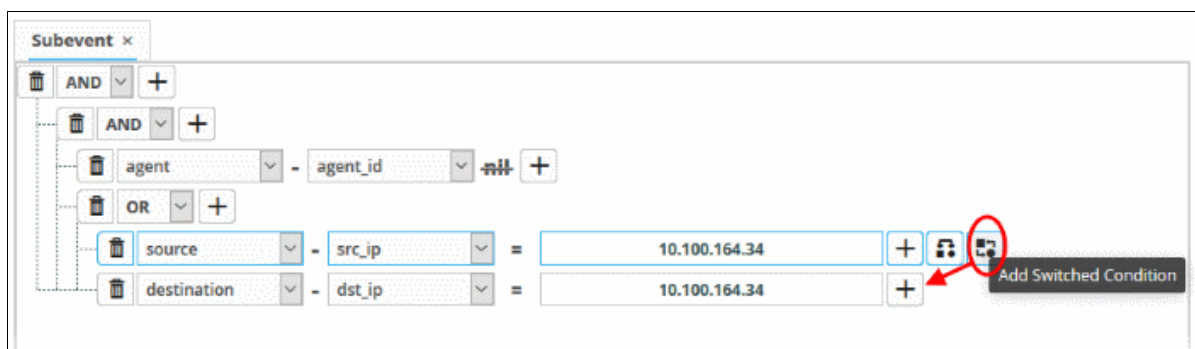
		<p>entered value.</p> <ul style="list-style-type: none"> For example, to search for events with source IP addresses starting with 192, enter '192'.
*ab	Ends with	<ul style="list-style-type: none"> Manually enter a value in the field to the right of the operator. The filter will identify events that end with the entered value. For example, to search for events with source IP addresses that end with 123, enter '123'.
nil	Is Empty	<ul style="list-style-type: none"> Searches for events in which the selected field is empty (does not contain any value). For example, to search for the events with no values in their source IP address fields, select 'Is Empty'.
!nil	Is Not Empty	<ul style="list-style-type: none"> Searches for events in which the selected field is not empty (contains a value of some kind). For example, to search for the events with some IP addresses values in their source IP address fields, select 'Is Not Empty'.
[a]	Is in List	<p>Allows you to configure the filter statement to fetch values for the field from a pre-defined list containing specific values for the field type.</p> <p>Background:</p> <ul style="list-style-type: none"> Lists enable administrators to add and manage lists of values for different fields for use in queries and correlation rules. cWatch features three kinds of Lists, Live Lists, Range List and IP Range. Lists can be created and the values can be updated manually. Live Lists can be also be configured to be fetched from outputs of correlation rules. The updates in a list will be immediately reflected in the queries and the rules in which it is used, relieving the administrator from the burden of updating queries and rules for change in values to be queried. For more details on Lists management, see Lists. <p>On selecting [a] as the relation parameter, drop-down options will appear for the list and the list type:</p>  <p>The screenshot shows a filter configuration interface. It includes a dropdown menu for the relation parameter, which is currently set to [a]. Below this, there is a dropdown menu for the list name, currently set to 'IP Blacklist'. To the right of the list name dropdown is another dropdown menu for the list type, currently set to 'ANY'. A red circle highlights the [a] dropdown, and another red circle highlights the list type dropdown. A dropdown menu is open below the list type dropdown, showing three options: 'ANY', 'External', and 'Internal', with 'Internal' selected.</p>



		<p>The first drop-down shows the lists that contain values for the selected query field. The second drop-down shows the list Types within the selected 'List'.</p> <ul style="list-style-type: none"> • Choose the list to be used in the query filter from the first drop-down. • Choose the sub list that contains the set of values to be included in the query filter from the second drop-down. <p>All the values contained in the list will be included as values for the field specified in the filter statement.</p>
<p>{a}</p>	<p>Not in List</p>	<p>Allows you to configure the filter statement to search for the events that do not contain specific values from a pre-defined list.</p> <p>On selecting {a} as the relation parameter, drop-down options will appear for the list and the list type:</p>  <p>The first drop-down shows the lists that contain values for the selected query field. The second drop-down shows the list Types within the selected 'List'.</p> <ul style="list-style-type: none"> • Choose the list to be used in the query filter from the first drop-down. • Choose the sub list that contains the set of values to be input as exclusions to the query filter from the second drop-down. <p>The results will display all events that do not contain the values in the lists.</p>

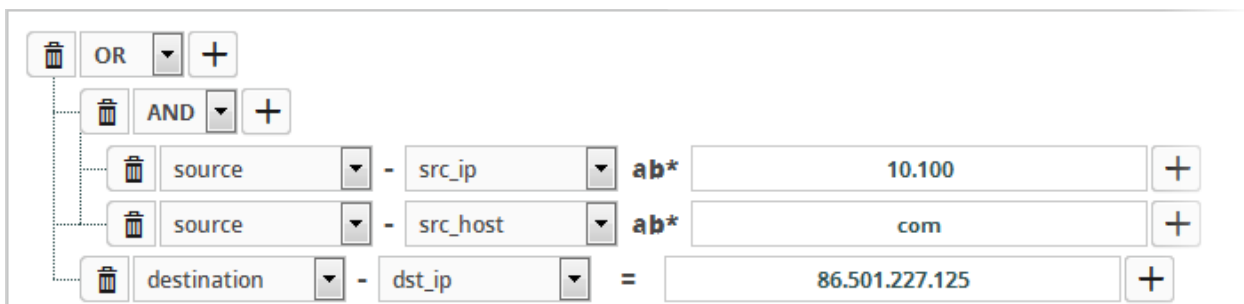
- If you are adding values for source parameters like source IP address, source port, source MAC etc., but wish to reverse the parameter, click the switch icon  that appears to the right of the statement.
- The field group and the field selected will automatically switch from source to destination or vice-versa.
- For example, if you are specifying a live list containing values of source IPs for the source IP field, but want to change them to destination IPs, you can click the switch button.



- Similarly to add the switched condition to the existing query, click 



- To add more query filters under the same combination chosen in the first step, click the  button beside the same combination and repeat the process.
- To add a sub-filter statement, click the  button beside the filter and repeat the process.
- To set the relationship between each statement, use the drop-down menu.
- For example, the statements below will return events whose source ends with 10.100 OR .com AND whose destination is 86.105.227.125



- To delete a filter, click the  button beside it.

You can add multiple query definitions for a single sub event and these are tied together.

The next step is to define sub events join condition that, when true, a new event will be generated per the output mappings configuration.

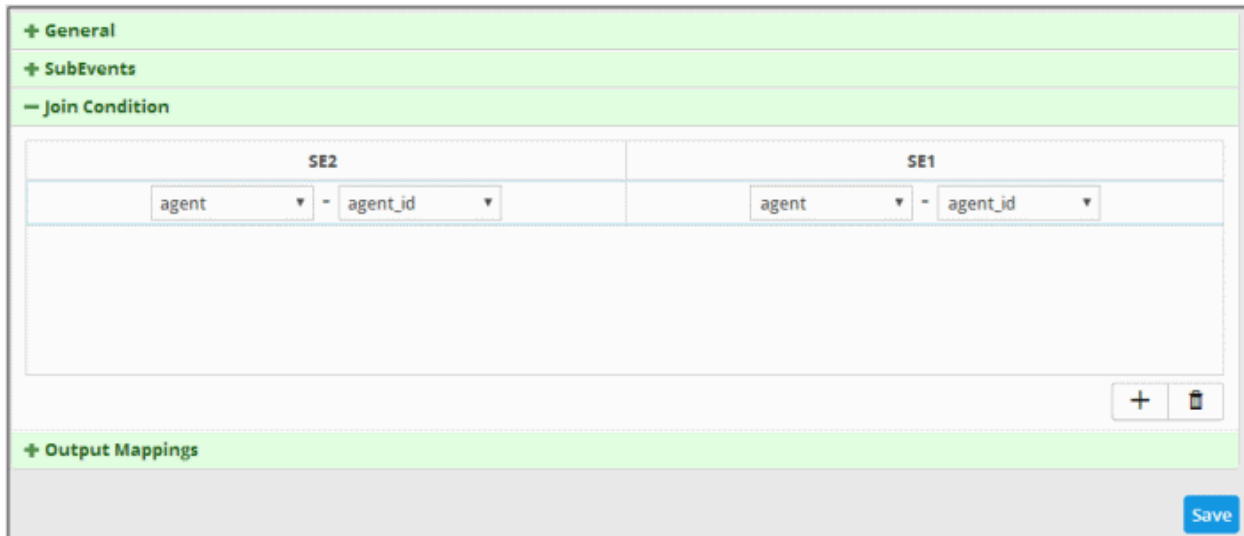
Join Condition

Please note that you have to add at least two sub events in order to define a join condition. This section allows you to configure field groups and fields that when those values are equal in the sub events, then a new aggregated event

will be generated as per the output mappings. For example if in the condition 'agent:agent_id' for sub event 1 is equal to 'agent:agent_id' for sub event 2 then the condition becomes true.

- Click the 'Join Condition' stripe to open the 'Join Condition' area.

The Join Condition screen will be displayed:

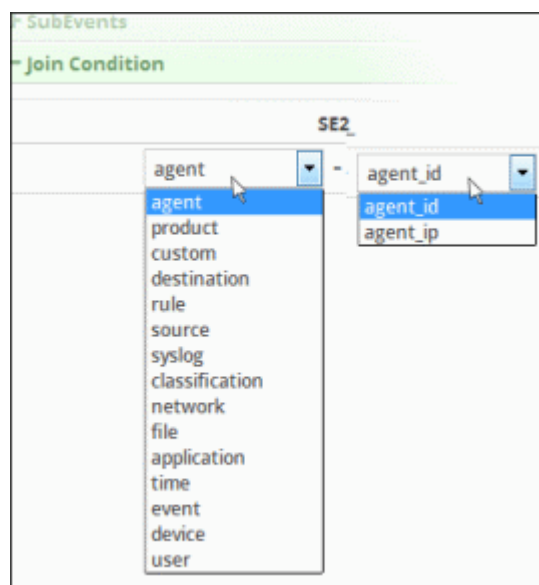


The number of columns displayed for 'Join Condition' depends on the number of sub events configured. For example, if you have configured three sub events, then the Join Condition will display field groups for three sub events allowing you to configure the condition. The above aggregated rule displays the Join Condition for two sub events and the selected values indicate that when the value of 'agent_id' is same for both the sub events then the condition becomes true. The column header displays the name of the sub events configured for the aggregated rule. When the condition become true, a new aggregated event will be logged and can be queried from the **Event Query** page under **Investigation**.

To configure a join condition


- Choose the field group you wish to add to the filter from the 'Field Groups' drop-down.

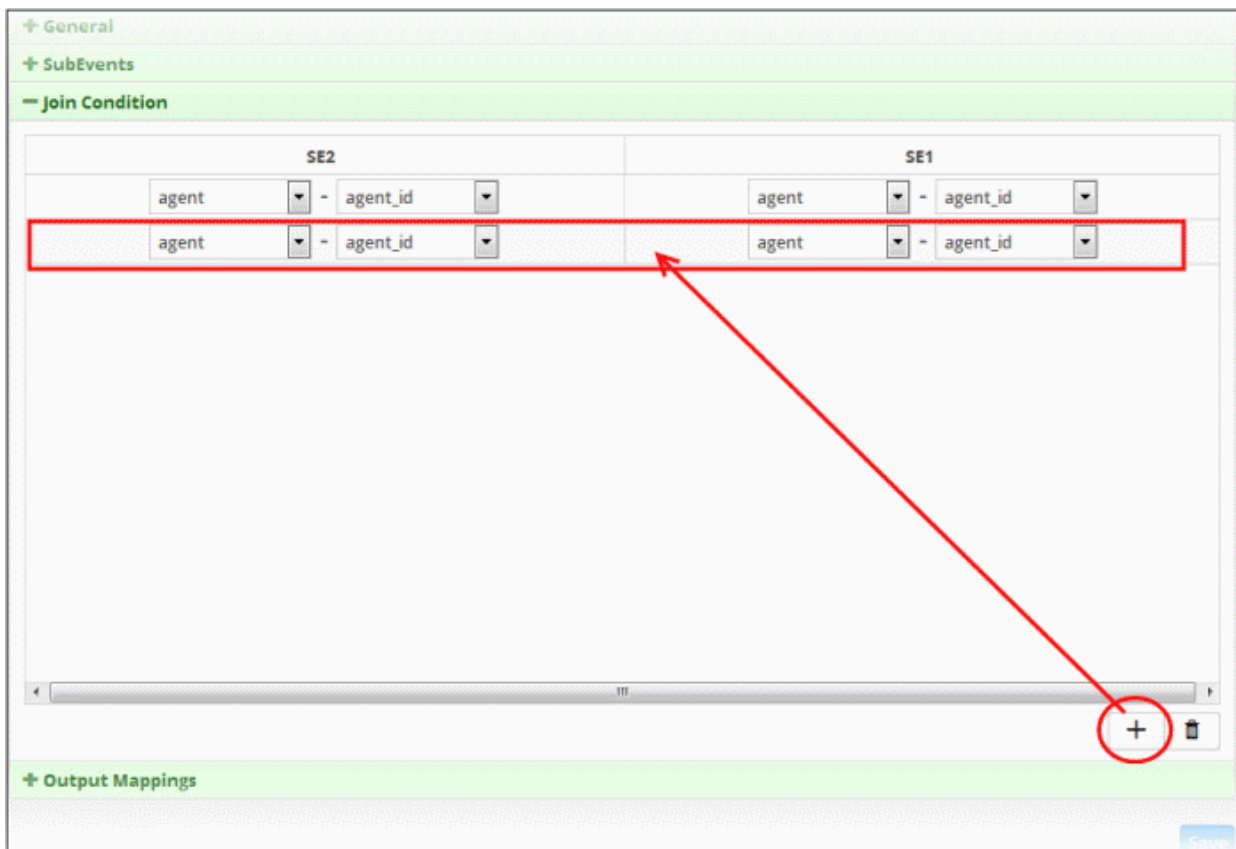
The next field will display the fields available for the selected field group.



- Choose the field from the second drop-down.

Tip: The descriptions of the Field Groups and the Field items under each of them, are available in **Appendix 1 - Field Groups and Event Items Description**.

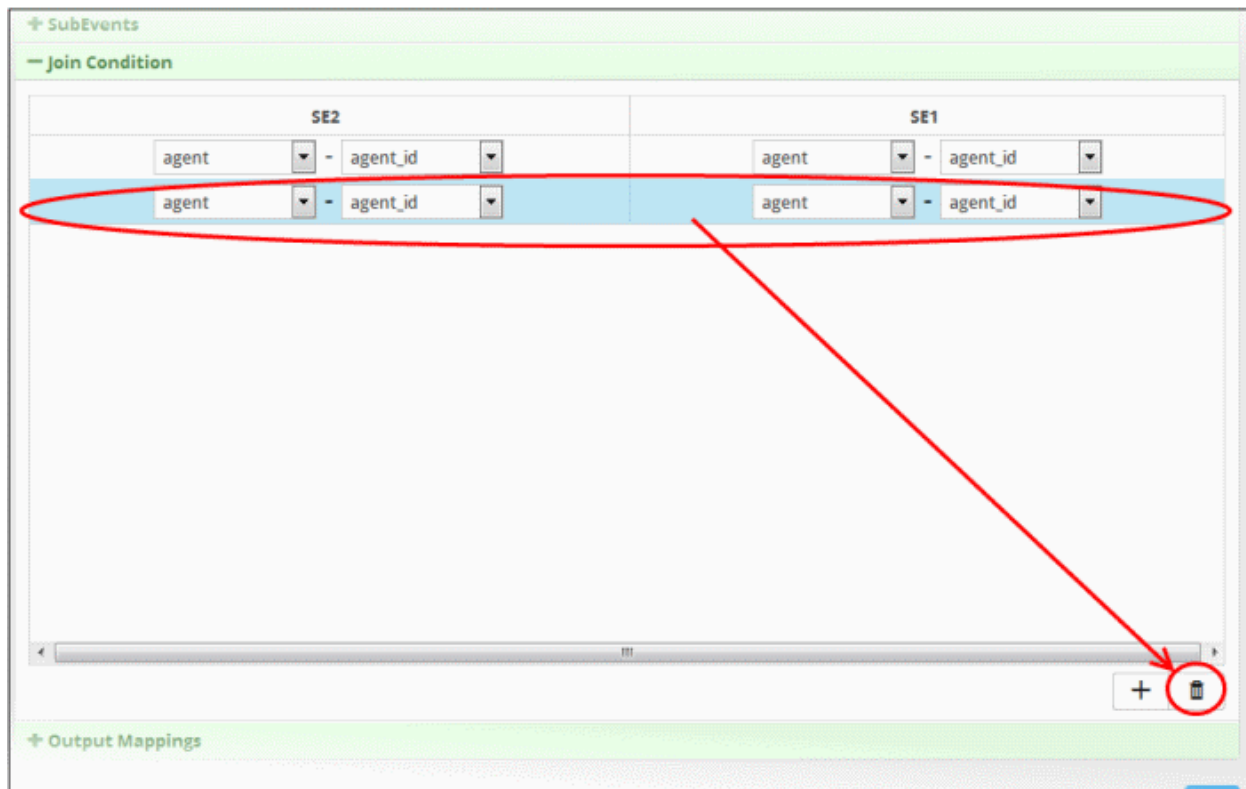
- Repeat the same process to select the field group and fields for the available sub event(s)
- To add more field groups and fields for the sub events, click the  button at the bottom of the screen. Another row to configure the field groups and fields for the sub events will be displayed.



- Repeat the same process explained above to select the field group and fields for the available sub event(s) for each row.

Please note that you can add multiple rows for a Join Condition. The values in the same row should be equal for the Join Condition to be true. For example, the value of row 1 of sub event 1 should be equal to value of row 1 of sub event 2. Similarly the value of row 2 of sub event 1 should be equal to value of row 2 of sub event 2 and so on.

- To remove a join condition row, select it and click the trash can icon at the bottom



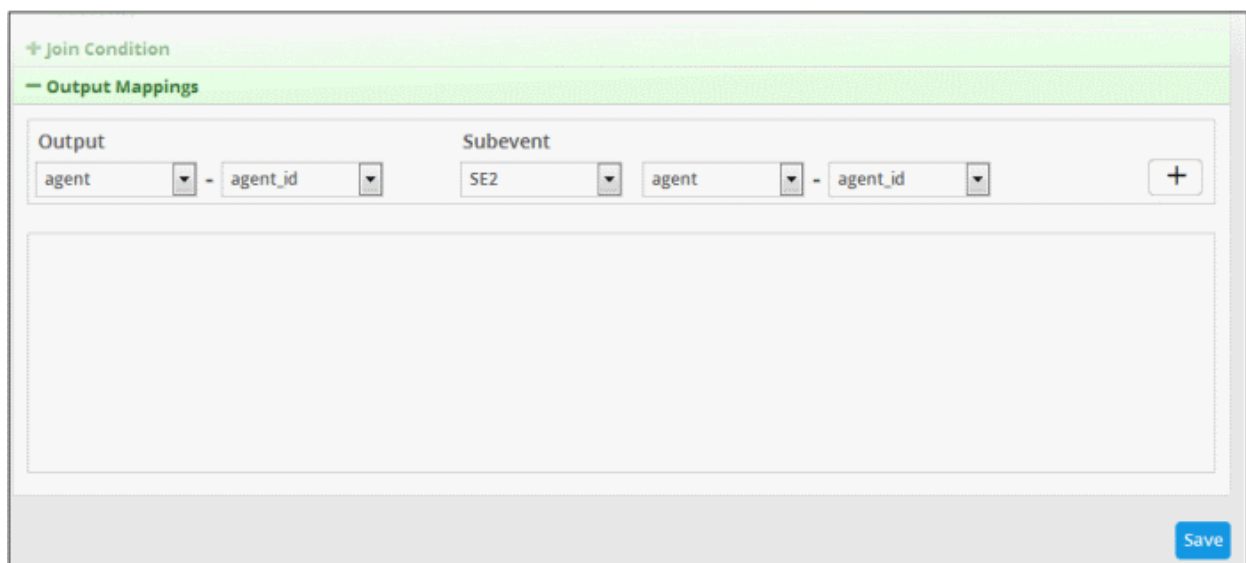
The row will be removed from the screen. After configuring the join condition for the sub events, the next step is to configure the fields that should be included in the aggregated events.

Output Mappings

The Output Mappings area allows you to configure the field values that should be displayed in the aggregated events that are generated whenever a join condition for sub events becomes true. Please note that the details screen of an aggregated event will display the configured output field values including default values. These default values may vary for different aggregated events.

- Click the 'Output Mappings' stripe to open the 'Output Mappings' area.

The 'Output Mappings' screen will be displayed:



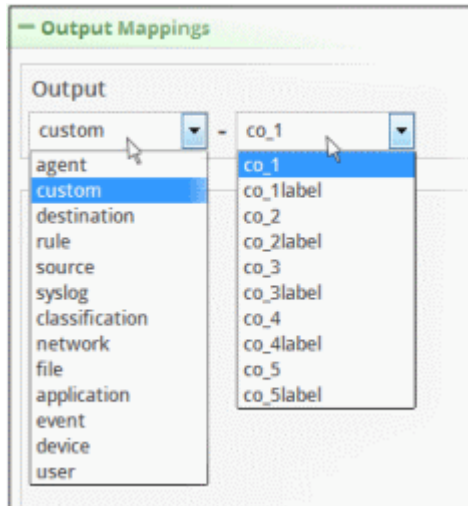
- **Output** - Allows you to configure the field that should be displayed on the details screens of an aggregated event

- **Subevent** - Allows you to select the value that should be displayed for the output field. The drop-down lists all the sub events added for the rule including 'Value' that allows to input a custom value.

To configure the output field

- Choose the field group from the 'Field Groups' drop-down from the 'Output' section

The next field will display the fields available for the selected field group.

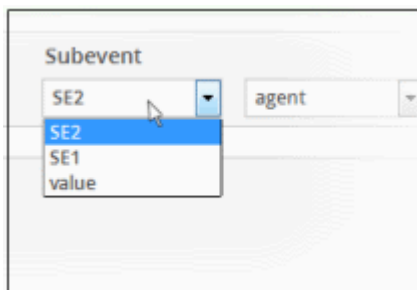


- Choose the field from the second drop-down.

Tip: The descriptions of the Field Groups and the Field items under each of them, are available in [Appendix 1 - Field Groups and Event Items Description](#).

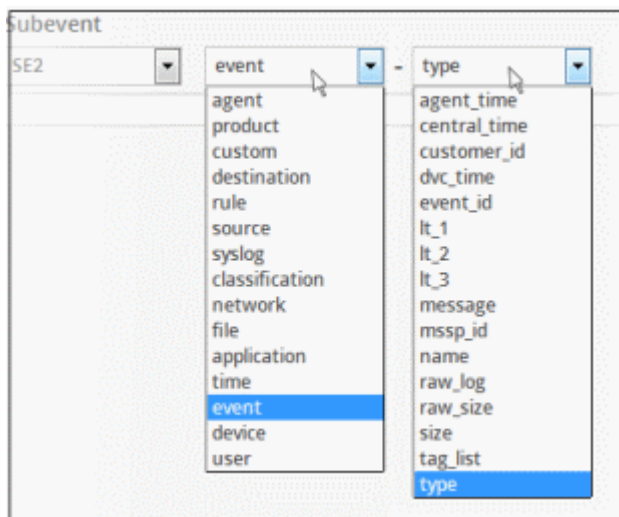
Next, you have to configure the sub event value that should be populated for the selected field under 'Output'

The first drop-down under the 'Subevent' section displays all the sub events available for the rule.




- Choose the sub event from the drop down. 'Value' allows you to input a custom value.
- Next, choose the field group from the 'Field Groups' drop-down

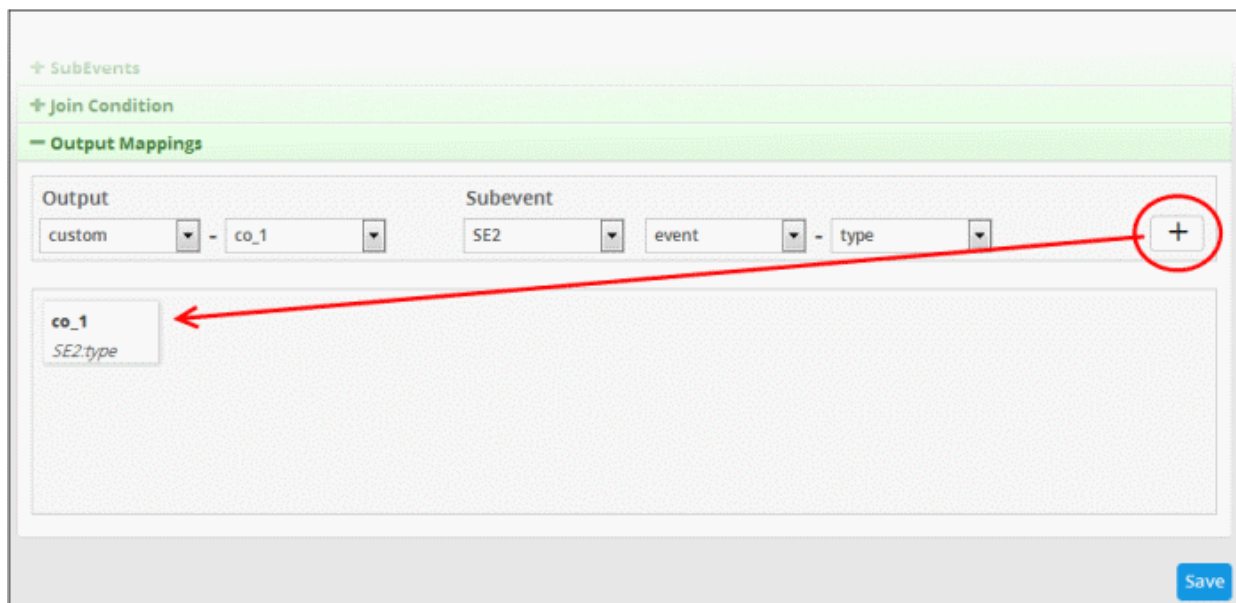
The next field will display the fields available for the selected field group.



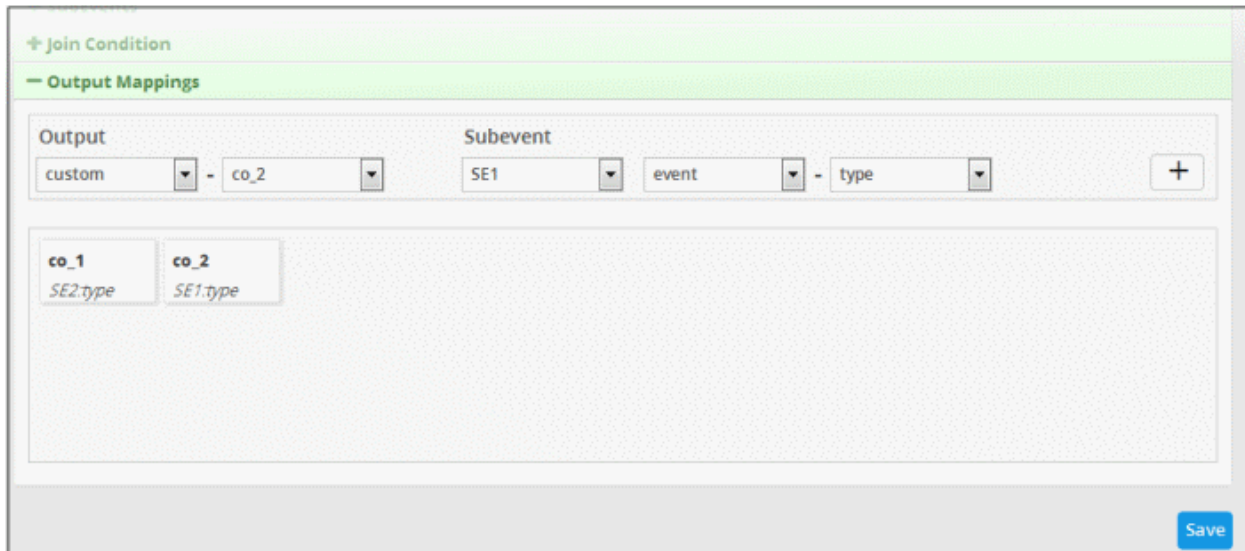
- Choose the field from the second drop-down.

Tip: The descriptions of the Field Groups and the Field items under each of them, are available in [Appendix 1 - Field Groups and Event Items Description](#).

- Click the  button on the right after selecting the output parameters.



The output field with the configured field value will be displayed below the configuration area. The following example shows the field output values added for sub event 1 and 2. You can add as many output fields as required for the aggregated event.



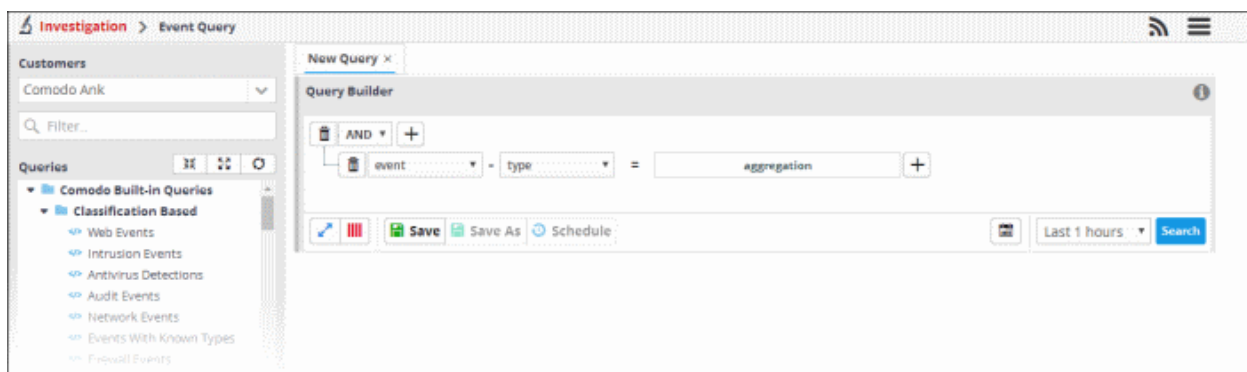
- To remove an output field, place the mouse cursor over an output configuration and click the 'x' mark.



- Click the 'Save' button.

The aggregation rule will be saved and when the join condition is triggered, an aggregation event will be generated and can be queried from the **Event Query** page under **Investigation**.

- To view an aggregated event that was triggered by an aggregation rule, click the menu button > 'Event Query' under 'Investigation'. Select the customer that was applied to the rule under 'Customers' on the left pane.



In the 'Query Builder', select 'event' from the 'Field Groups' drop-down and 'type' from the 'Fields' drop-down. Select '=' operator and enter 'aggregated' in the text field. Select the search period from the 'Last...' drop down and click the 'Search' button.

The search results for the aggregated event query will open.

Query Builder

AND +

source - src_ip = 105.140.126.2 +

Save Save As Move Schedule Last 3 hours Search

Results Aggregations

Event Fields

destination dst_ip +

dst_ip

Aggregation Function

Count


Order By Limit

Descending 500

Submit


Table Bar Chart Pie Chart

#	dst_ip	Count
31	198.58.106.243	36
32	211.159.235.58	32
33	172.217.1.238	31
34	96.6.45.26	30
35	91.189.88.152	30
36	96.6.45.83	28
37	8.253.231.254	28
38	8.252.36.126	28
39	23.202.233.152	27
40	173.194.167.170	26
41	128.122.109.46	25
42	23.57.36.67	20
43	172.217.2.238	20
44	85.236.43.108	18

- Click the export  button on the right of the table to generate a .csv file of the results.

Opening exported-New Query-aggregation-1524484026310.csv

You have chosen to open:

 **exported-New Query-aggregation-1524484026310.csv**
which is: OpenOffice.org XML 1.0 Spreadsheet
from: <https://cwatchankara.cone.mssp.comodo.com>

What should Firefox do with this file?

Open with: OpenOffice Calc (default)

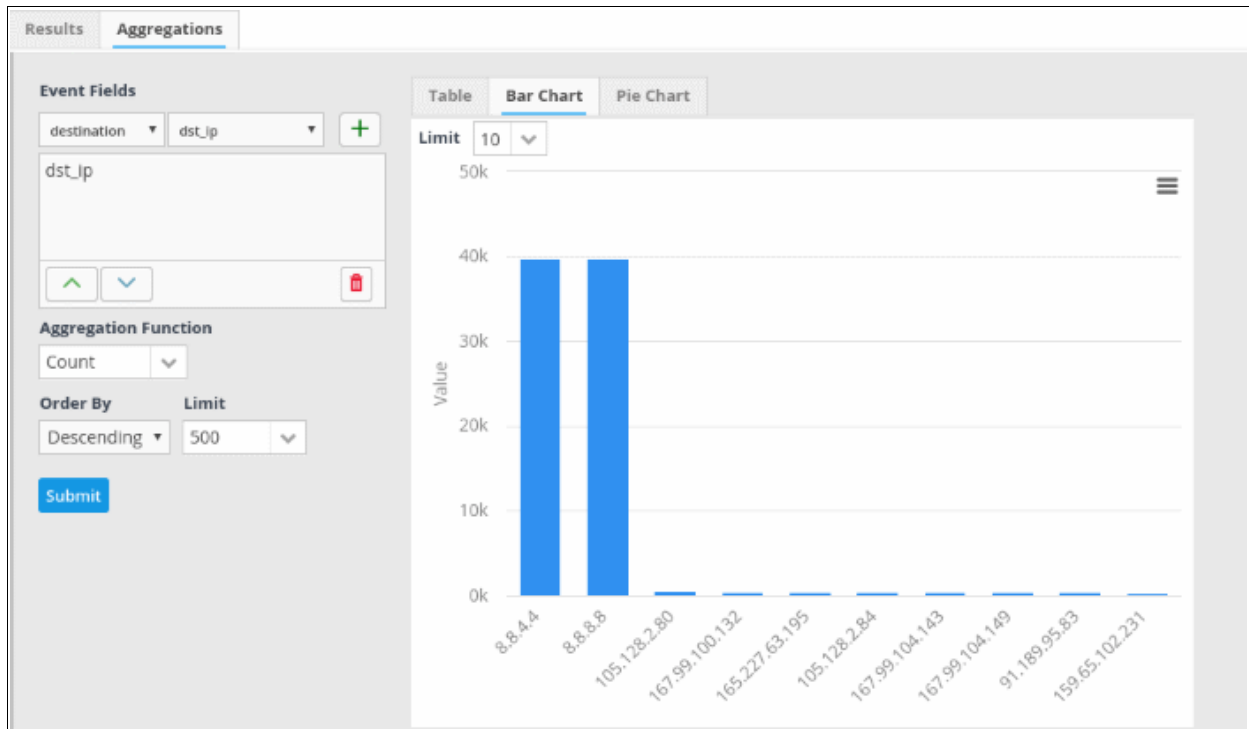
Save File

Do this automatically for files like this from now on.

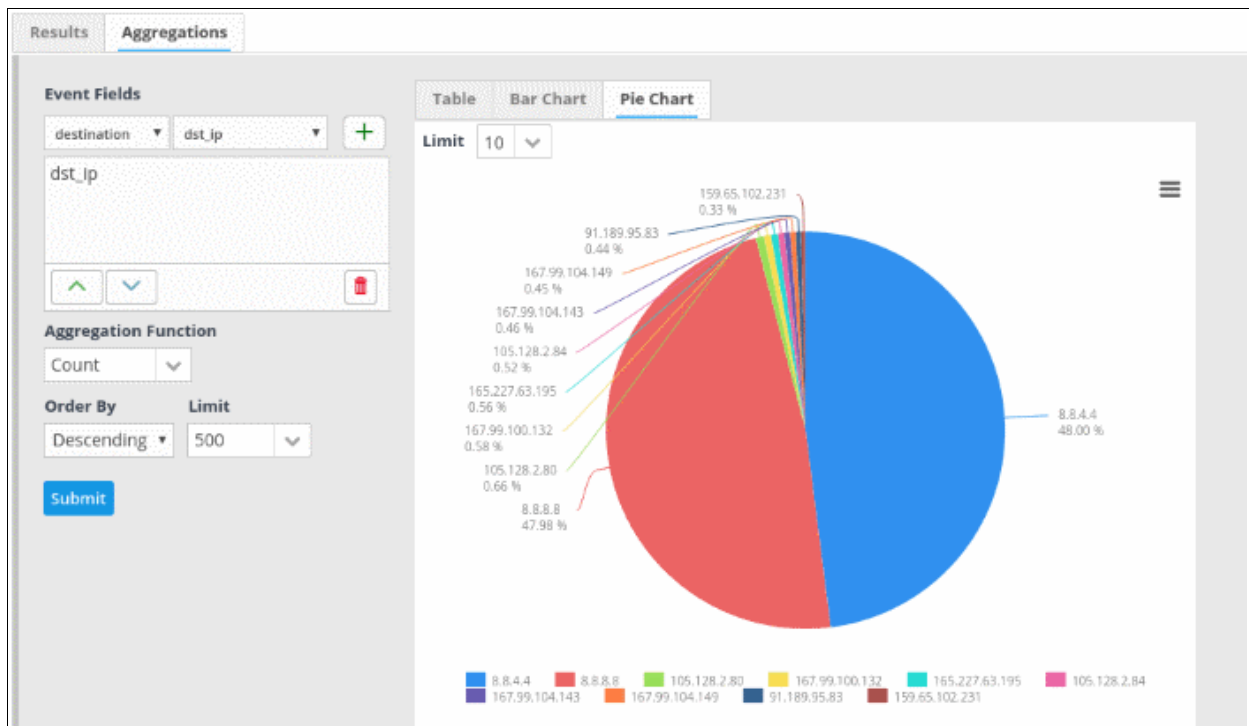
OK Cancel

You can also view the graphical representation of the number of events from source ip to destination ip.

- Click the 'Bar Chart' tab to view the bar chart representation of the aggregated events.




- Click the 'Pie Chart' tab to view the pie chart representation of the aggregated events.




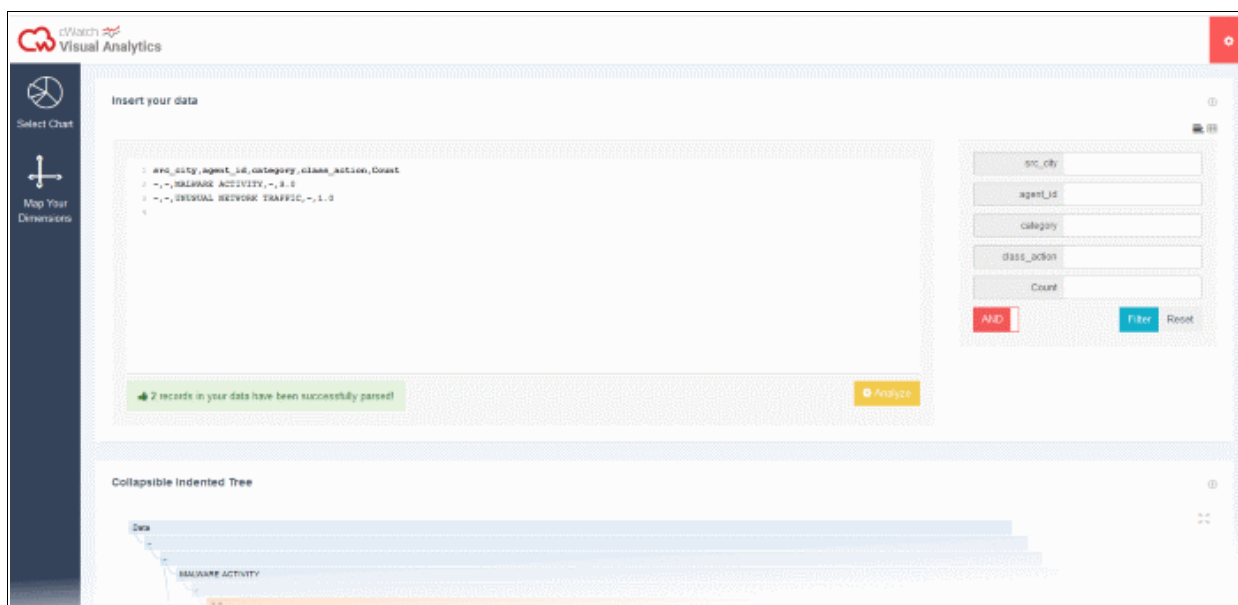
To re-arrange the event fields,

- Select the field you want to re-position

- Click the up/down  arrow button on the bottom left of the 'Event Fields' pane.

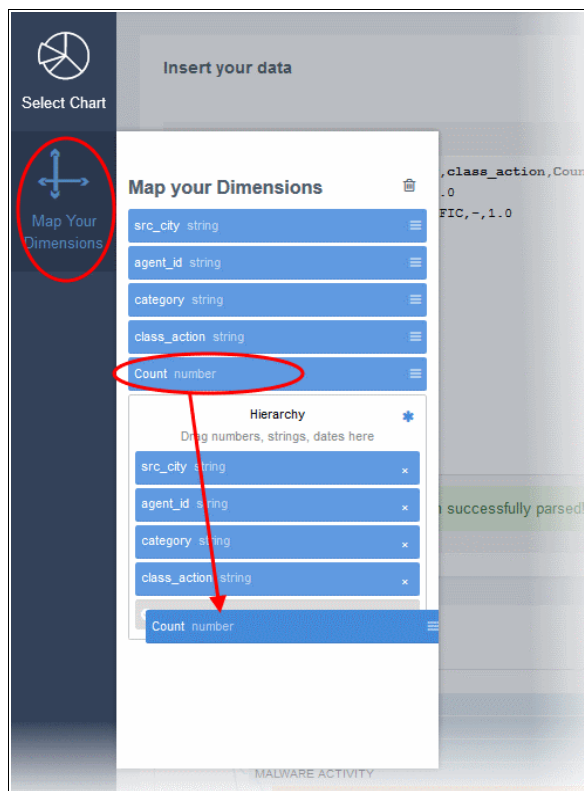
cWatch Analytics

- You can view more graphical representations of the aggregated results using cWatch Analytics.
- This interface helps you view a unique filtered chart by entering the specific values in the field as desired from event query.
- You can view the both the combination of fields or either of the fields entered in the right hand side filter to view the desired chart by clicking Boolean operators AND/OR present below the aggregated fields
- To view more graphical representations of the aggregated results, click the 'Go to cWatch Analytics'  button

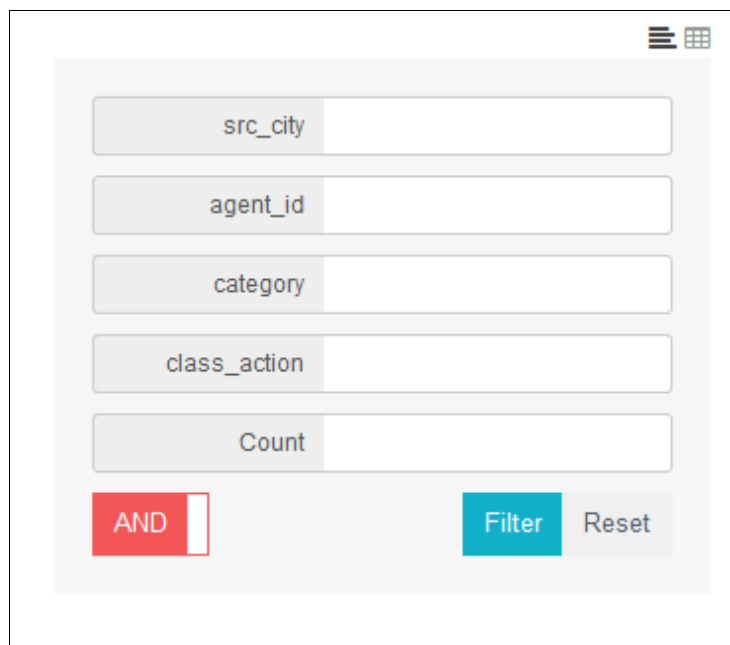



The analytical result for fields chosen in aggregated results will open. The parsed analysis results will also be displayed in this interface.

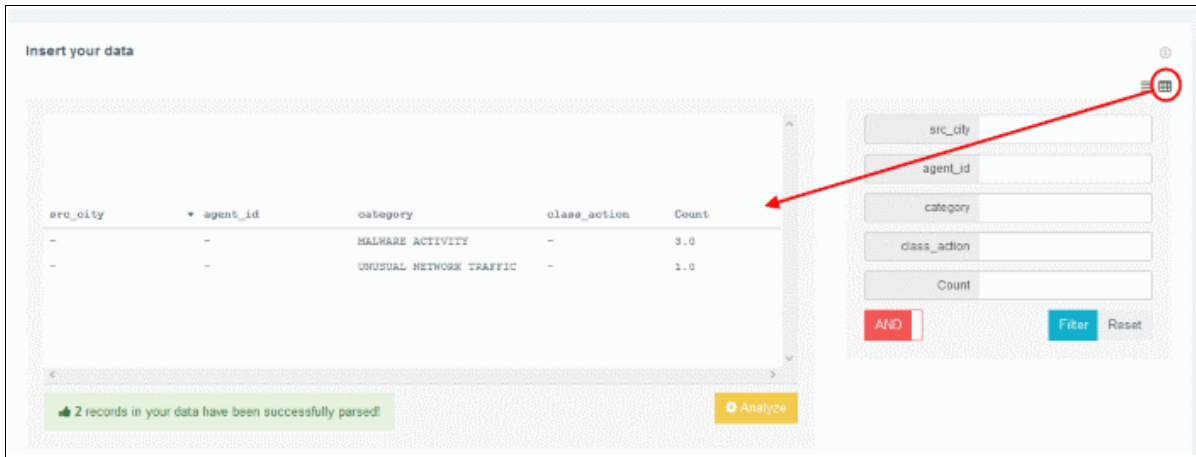
- To view this result in various types of charts, map the aggregated result fields, by clicking 'Map Your Dimensions' window on the left panel.




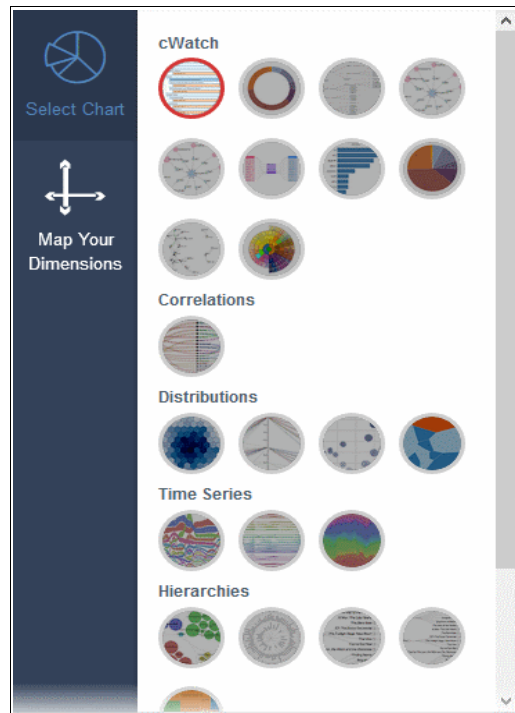
- Select the field you want to map and then drag and drop the parameter to the 'Hierarchy' below in the order you want it to be represented in the chart
- To view specific events in a graph, enter the fields displayed on the right of the interface and click 'Filter' to view the graph.





- Click 'Reset', to view all events of aggregated results
- To view data input in text format, click 



- To view data input in table format, click 
- Click the 'Select Chart' window to view the various types of charts that appropriately fits your event data inputs



- To add a particular event from the aggregated result to the current query, click 
- To add a particular event from the aggregated result as a new query, click 

Clicking on an aggregated event will open details with configured and default output values.

Results | Aggregations

Time: (2018-04-11 09:07:56 - 2018-04-11 12:07:56) Total Count: 20

Central Time	Device Host	Agent
2018-04-11 12:07:33.881	NxSensor	NxSensor
2018-04-11 12:07:33.810	NxSensor2	NxSensor2
2018-04-11 12:07:32.663	NxSensor2	NxSensor2
2018-04-11 12:07:30.103	NxSensor	NxSensor
2018-04-11 12:07:20.197	NxSensor	NxSensor
2018-04-11 12:07:20.162	NxSensor2	NxSensor2
2018-04-11 12:07:20.162	NxSensor2	NxSensor2
2018-04-11 12:07:20.162	NxSensor2	NxSensor2
2018-04-11 12:07:20.162	NxSensor2	NxSensor2
2018-04-11 12:07:18.438	NxSensor	NxSensor
2018-04-11 12:07:18.438	NxSensor	NxSensor
2018-04-11 12:07:18.438	NxSensor	NxSensor
2018-04-11 12:07:18.404	NxSensor2	NxSensor2
2018-04-11 12:07:18.404	NxSensor2	NxSensor2
2018-04-11 12:07:18.404	NxSensor2	NxSensor2
2018-04-11 12:07:18.404	NxSensor2	NxSensor2
2018-04-11 12:07:18.402	NxSensor	NxSensor
2018-04-11 12:07:18.402	NxSensor	NxSensor
2018-04-11 12:07:18.402	NxSensor	NxSensor
2018-04-11 12:07:18.402	NxSensor	NxSensor

Selected Result Fields | **Details** | Filter | Raw Log

agent_ip: NxSensor	agent_ip_number: -1
agent_time: 2018-04-11 12:07:20.197	app_pid: 0
Application Name: NxSensor_conn	app_proto: dris
base_score: 0	bytes_in: 77
bytes_out: 37	Central Time: 2018-04-11 12:07:20.197
class_action: connect	class_domain: net
class_object: flow	class_status: success
co_2: SF	co_2label: conn_state
co_3: Dd	co_3label: conn_history
customer_id: CUST6dcfe4e...	Destination IP: 8.8.8.8
dst_city: Mountain View	Destination Port: 53
dst_country: United States	Device Host: NxSensor
dst_ip_number: 134744072	dst_ip_private: false
dst_ip_version: 4	dst_loc: 37.3845,-122.0...
dst_sd_1: California	dst_tr_ip_number: -1
dst_tr_port: 0	duration: 0
dvc_ip_number: -1	dvc_time: 2018-04-11 12:07:20.197
dvc_tr_ip_number: -1	event_id: SDCpa2kGT_G...
f_size: 0	facility: 23
kafka_partition: 0	It_1: AssetRangeList
It_2: src_ip/AssetRa...	It_3: src_ip/AssetRa...
mssp_id: samsung_cone	

The following screenshot shows the output fields and values that were configured for an aggregated rule in the details screen of the aggregated event that the rule triggered. The 'event type' that were configured for sub event 1 and sub event 2 are Firewall and Access respectively.

General
+ SubEvents
+ Join Condition
- Output Mappings

Output: custom - co_1 - SE2

co_1: SE2.type
co_2: SE1.type

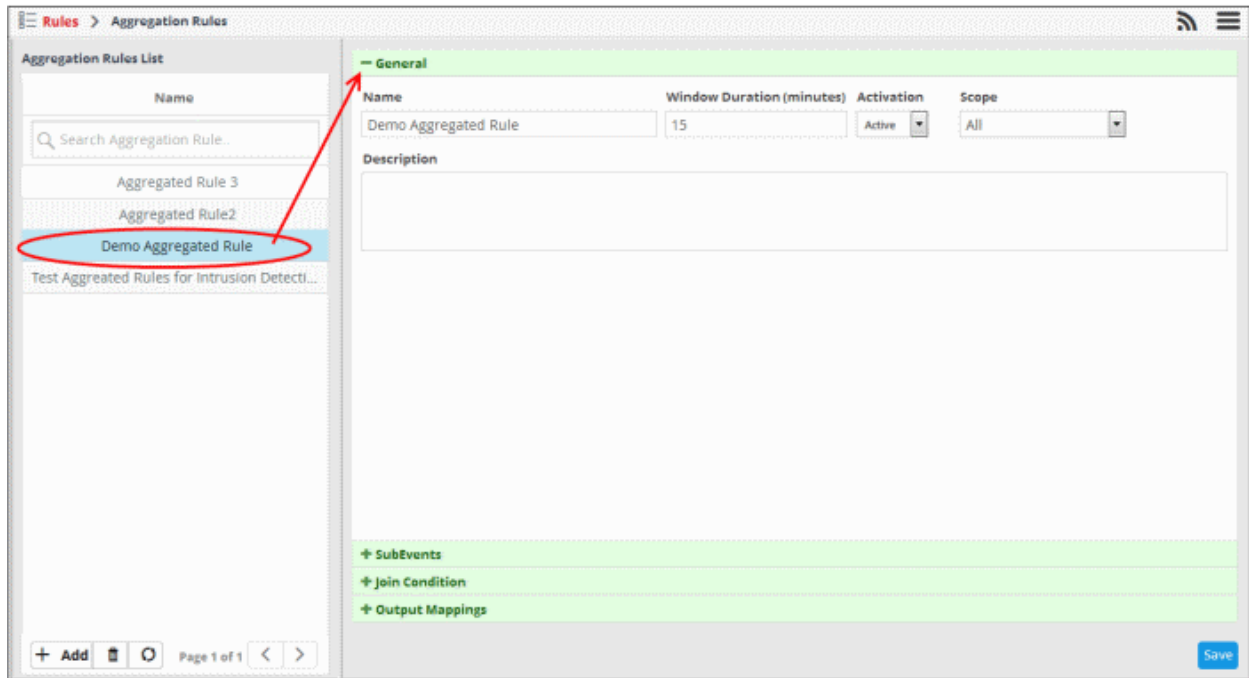
Details

agent_time: 2016-04-29 06:...	app_pid: 0	bytes_in: 0
bytes_out: 0	central_time: 2016-04-29 06:...	co_1: Access
co_2: Firewall	customer_id: CUST52b54...	dst_ip_private: false
dst_port: 0	dst_tr_port: 0	dvc_time: 2016-04-29 06:...
event_id: b0f992b-d0ea...	f_size: 0	facility: 0
It_1: []	It_2: []	It_3: []
mssp_id: developmenta...	name: Demo Aggrega...	partition_time: 0
pass_days: 16920	pass_hours: 406083	pass_minutes: 24365034
pass_months: 0	pass_years: 0	priority: 0
prod_name: Misp	prod_vendor: Comodo	raw_size: 0
rule_hit_count: 0	rule_id: 0	rule_sig_id: 0
security: 0	size: 0	src_ip_private: false
src_port: 0	src_tr_port: 0	type: aggregated

You can save the aggregated events and use it for correlation rules in order to create incidents. See '[Query Management](#)', '[Managing Correlation Rules](#)' and '[Managing Incidents](#)' for more details.

Edit an Aggregation Rule

- Select the aggregation rule that you want to edit from the list.

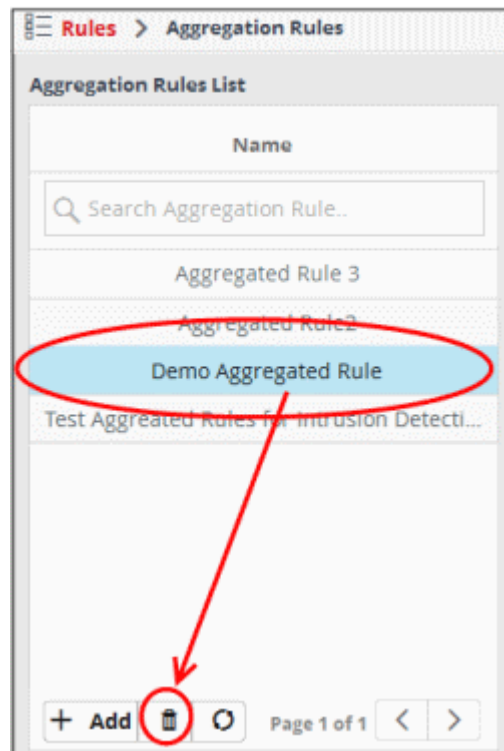


- **General** - Edit the name of the rule directly in the name field. Modify the other parameters as required. The process is similar to adding a new rule. [Click here](#) for more details about configuring the general section.
- **Sub Events** - Click 'SubEvents' to open the sub events configuration area. Modify or remove the sub events as required. The process is similar to configuring new sub events. [Click here](#) for more details about configuring sub events.
- **Join Condition** - Click 'Join Condition' to open the join condition configuration area. You can modify or remove join conditions as required. The process is similar to configuring new join conditions. [Click here](#) for more details about configuring sub events.
- **Output Mappings** - Click 'Output Mappings' to open the output mappings configuration area. You can edit existing current outputs, remove or add new outputs. The process is similar to configuring new output mappings. [Click here](#) for more details about configuring output mappings.
- Click the 'Save' button for the changes to take effect.

Please note that aggregated events triggered by aggregated rules prior to their modifications will not be affected.

Delete an Aggregation Rule

- Select the aggregation rule that you want to remove from the list.



The rule will be removed from the list. Please note that the aggregated events triggered by aggregated rules prior to their removal will not be affected.

6 Incidents

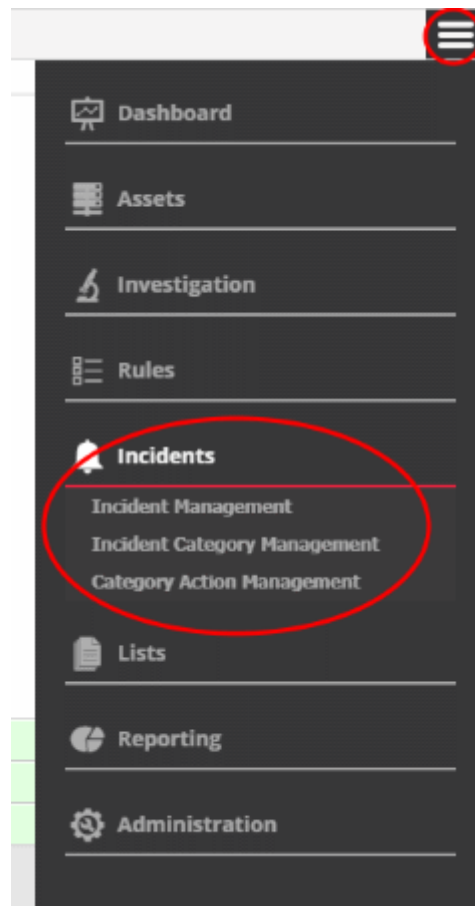
- cWatch will generate an 'Incident' when it identifies events which match a correlation rule. Correlation rules are defined per-customer and can be configured in the '**Rules**' section.
- Incidents are assigned to the user who is handling/supporting the customer.
- An incident remains open until the user closes it.
- Admins can manually add incidents and assign them to users if certain tasks are required on a customer network.
- The number of open incidents is shown beside the notification icon in the title bar.



The 'Incidents' menu allows users to manage incidents.

To open the incidents interface:

- Click the menu button at top-right and choose 'Incidents':

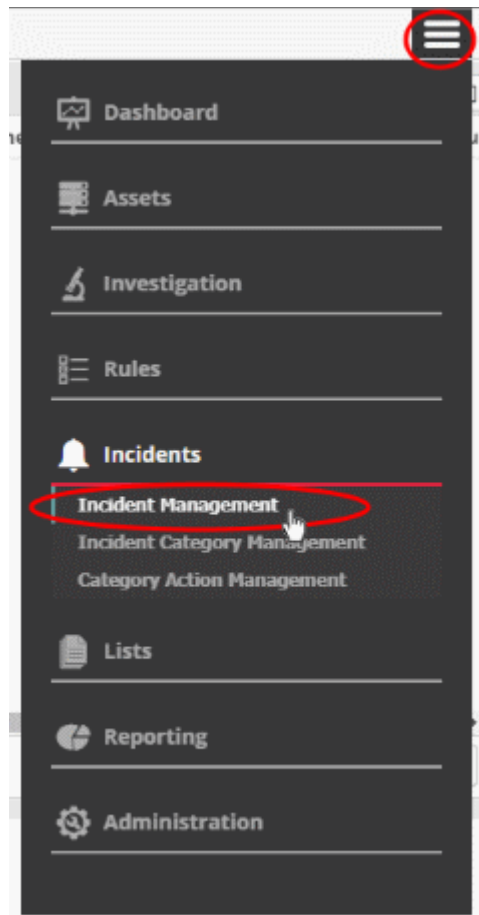


See the following sections for more details:

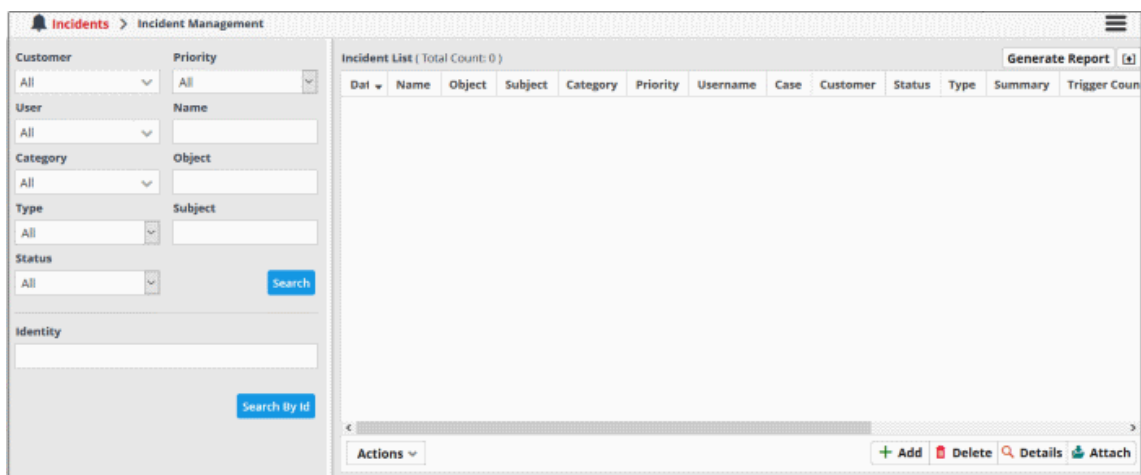
- [Manage Incidents](#)
- [Incident Category Management](#)
- [Category Action Management](#)

6.1 Manage Incidents

- Click the 'Menu' button > 'Incidents' > 'Incident Management'.
- This area lists recent incidents along with details such as customer network, the object affected, the user to whom it is assigned and more.
- The actions menu lets you close/re-open incidents, assign them to different users and change incident status.



The 'Incident Management' screen:



- Use the drop-down menus on the left to filter incidents. Click 'Search' to execute the query. You can combine filters to run more granular searches.
- You can also click the notification icon on the title bar to open this screen:



Incident List - Table of Column Descriptions	
Column Header	Description
Date	Time the incident was detected or added.
Name	<ul style="list-style-type: none"> For incidents added by correlation rules - The 'Name' column displays the name of the rule based on which the incident was detected. For manually added incidents - The 'Name' column displays the name as entered during its creation.
Object	The resource on which the incident occurred. For example, an endpoint.
Subject	The source of the incident. For example, a user or process that accessed the resource.
Category	The type of the incident
Priority	<ul style="list-style-type: none"> For incidents added by correlation rules - The 'Priority' column shows the severity level of the incident. This is set by the rule that detected the incident. For manually added events - The 'Priority' field shows the severity level entered by the person who created the ticket.
Username	The name of the admin to whom the incident is assigned.
Customer	The name of the customer on whose network the incident was detected.
Status	<p>The current standing of the incident. The possible values are:</p> <ul style="list-style-type: none"> Open In-Progress False-Positive Closed
Type	<p>Whether the incident was added manually or by a correlation rule. The possible values are:</p> <ul style="list-style-type: none"> Default - Incident was added manually Correlated - Incident was added by a correlation rule
Summary	<p>For incidents added by correlation rules - The 'Summary' column displays a short description of the it as defined in the rule based on which the it was detected.</p> <p>For manually added events - The 'Summary' field displays the short description of it as entered during its creation.</p>
Trigger Count	Number of times the incident occurred
Last Trigger Date	Date and time the incident last occurred
Identity	The incident identification number that was auto-generated by cWatch
Report	<p>Indicates whether a report has been generated for the incident. The possible values are:</p> <ul style="list-style-type: none"> Waiting request to generate report In progress Ready
TheHive	TheHive is a security incident response platform. Contact your Comodo account manager to access this.

- Click any column header to sort the table in order of the items in the column.

Following sections explain on:

- **View incident details**
- **Add and assign incidents to users**
- **Edit and Reassign an incident**
- **Delete an incident**

View incident details

- Select an incident and click the 'Details' button at the bottom.
- The details pane contains comprehensive information about the incident. This includes the name of the rule that triggered the alert, category of the incident, name of the customer, type of rule and more.
- The pane also lets you view other events detected by the same rule on other endpoints in the network.

Incident List (Total Count: 6515) Generate Report [↑]

Date	Name	Object	Subject	Category	Priority
2019-02-08 07:27:55	Ursnif (aka Gozi) Trojan	10.100.136....	8.8.8.8	MALWARE ACTIVITY	High
2019-02-08 07:27:54	Ursnif (aka Gozi) Trojan	10.100.136....	10.100.136.13	MALWARE ACTIVITY	High
2019-02-07 11:12:54	New NxiDS Event Triggered	2013495	ET TROJAN DN...	UNCATEGORIZED	Critical
2019-02-07 09:37:54	NanoCore RAT C2	10.100.132....	104.200.23.95	MALWARE ACTIVITY	High
2019-02-07 06:31:54	CHAT Related Events	10.100.130.41	74.125.133.125	UNUSUAL NETWORK TRAFFIC	Info
2019-02-06 15:42:55	Emotet Spyware C2	10.100.136.25	46.235.9.35	MALWARE ACTIVITY	High
2019-02-06 13:49:53	NanoCore RAT C2	10.100.132....	185.64.189.110	MALWARE ACTIVITY	High
2019-02-06 13:46:54	NanoCore RAT C2	10.100.132....	185.64.189.110	MALWARE ACTIVITY	High
2019-02-06 13:42:54	NanoCore RAT C2	10.100.132....	185.64.189.110	MALWARE ACTIVITY	High
2019-02-06 13:10:54	NanoCore RAT C2	10.100.132....	185.64.189.110	MALWARE ACTIVITY	High
2019-02-06 12:57:54	NanoCore RAT C2	10.100.130....	185.64.189.110	MALWARE ACTIVITY	High
2019-02-06 12:34:55	Potential Scan or Infection	10.100.134.74	10.100.129.20	UNUSUAL NETWORK TRAFFIC	Info
2019-02-06 12:30:54	NanoCore RAT C2	10.100.130.45	185.64.189.110	MALWARE ACTIVITY	High
2019-02-06 12:23:54	NanoCore RAT C2	10.100.134.71	185.64.189.110	MALWARE ACTIVITY	High
2019-02-06 11:45:54	NanoCore RAT C2	10.100.132.89	185.64.189.110	MALWARE ACTIVITY	High
2019-02-06 11:44:54	NanoCore RAT C2	10.100.132....	185.64.189.110	MALWARE ACTIVITY	High
2019-02-06 11:42:53	NanoCore RAT C2	10.100.136....	185.64.189.110	MALWARE ACTIVITY	High

Actions ▾ + Add [🗑️] Delete [🔍] Details [📎] Attach

The pane opens at the 'Summary' page

Incident Details

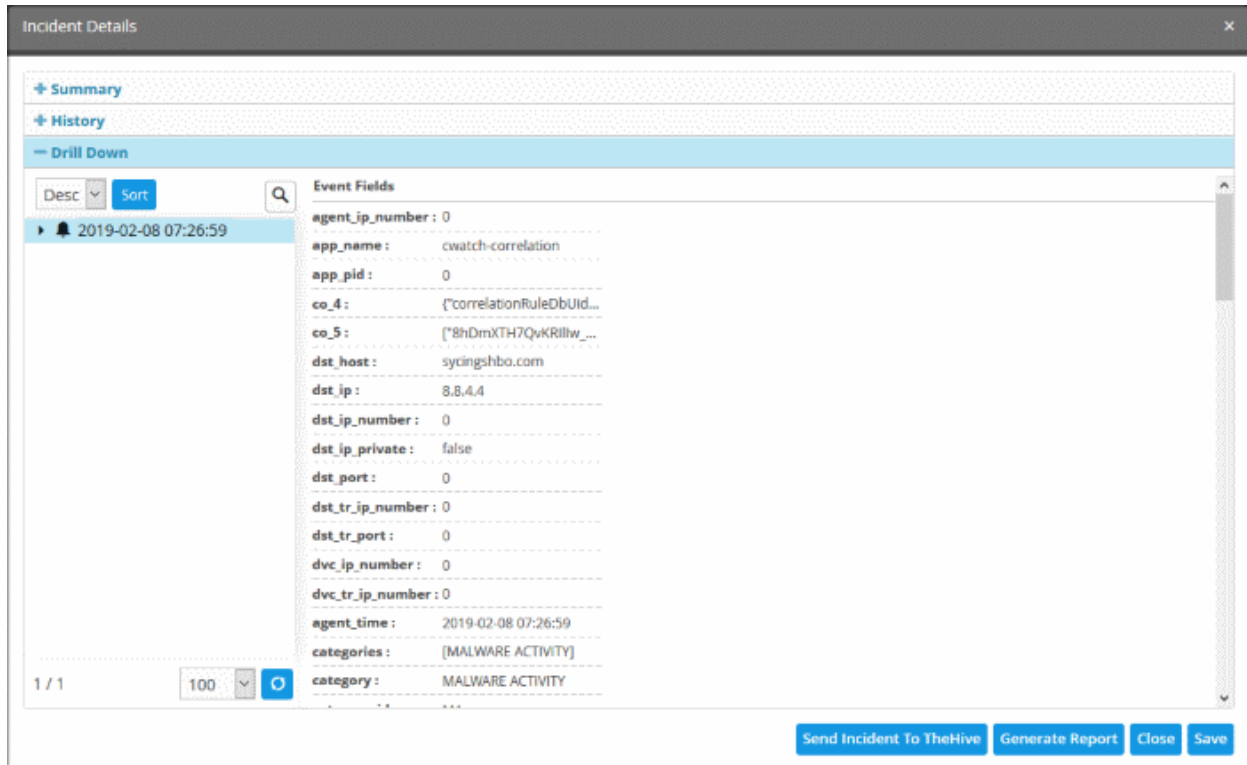
Summary	
Name:	Ursnif (aka Gozi) Trojan
Date:	2019-02-08 07:27:55
Customer:	comodoankara
Priority:	High
Object:	10.100.136.135
Last Trigger Date:	2019-02-08 07:27:55
Summary:	Ursnif (aka Gozi) Trojan was detected in the network.
Type:	Correl...
Category:	MALWARE ACTIVITY
Assignee:	cwatchankara
Status:	Open
Subject:	8.8.4.4
Trigger Count:	1

[History](#)
[Drill Down](#)

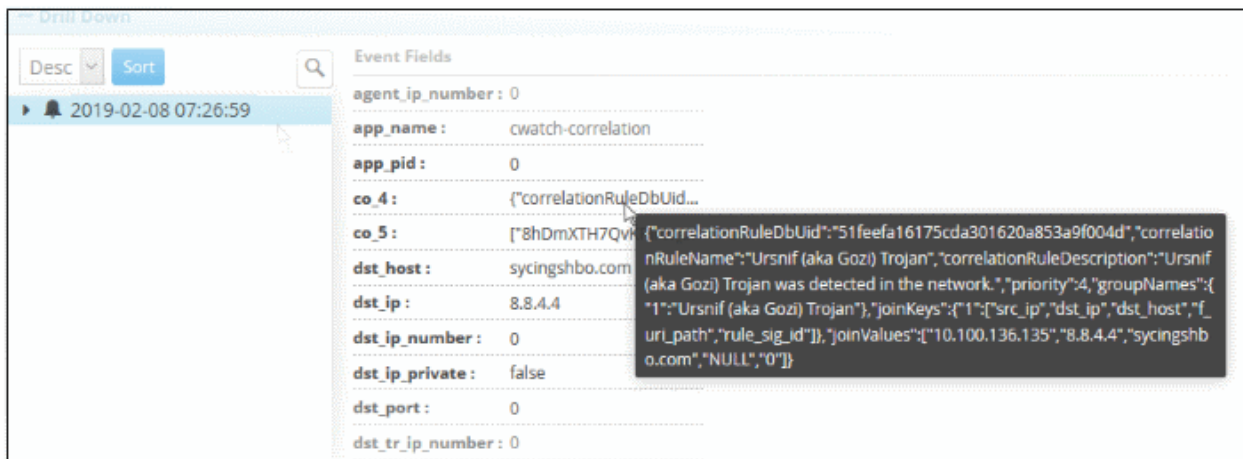
[Send Incident To TheHive](#)
[Generate Report](#)
[Close](#)
[Save](#)

The summary page provides details of the incident such as its name, date and time it was recorded and more.

- History – You can view the stages of the incident management, for example, closed with reason as False-Positive, in-progress and so on.
- Use the 'Drill Down' report to view all devices affected by the incident:



- Place your mouse cursor over an item to view full details as a tool tip.



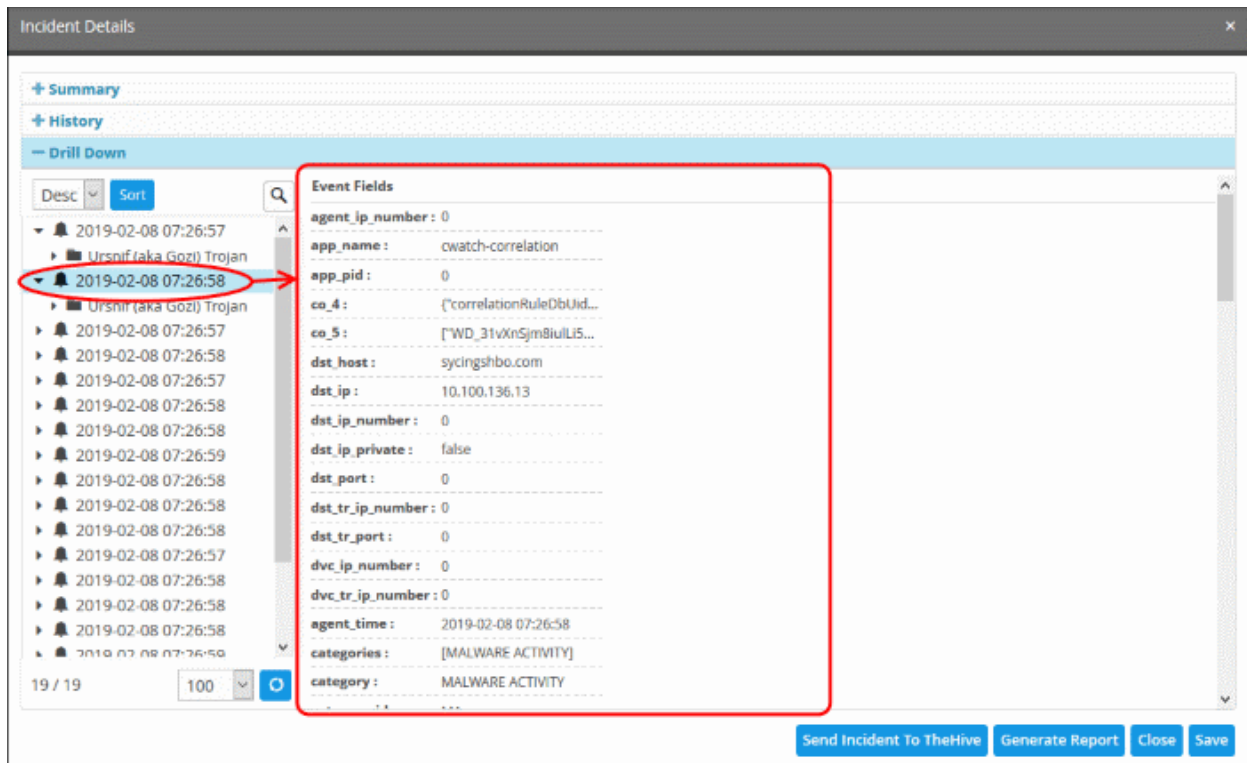
The 'Event Fields' pane on the right shows all event fields in the incident.

See **'Output Mappings'** under **'Configuring a Correlation Rule'** in **Managing Rules** for more details.

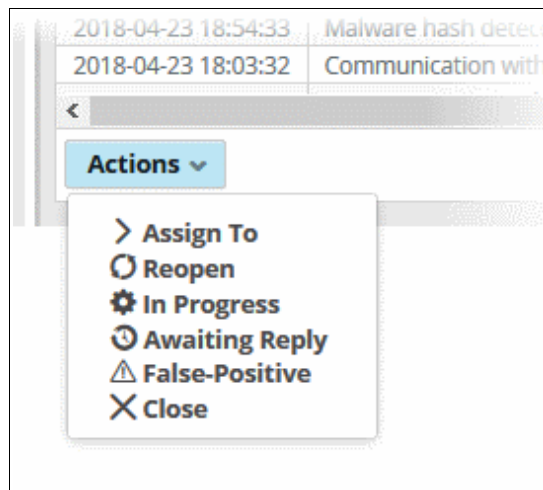
The 'Drill Down' pane lets you view other incidents identified by the same rule.

- To view the events, expand the folder structure under drill-down and select the time point.

The field values of the respective event detected at the time point will be displayed at the right.

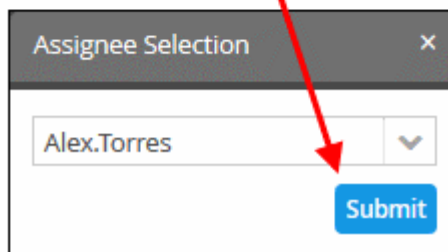
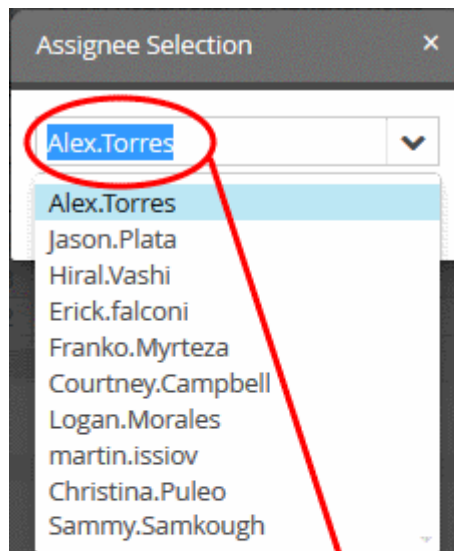


- Send Incidents to TheHive – TheHive is a security incident response platform. Contact your Comodo account manager to access this.
- Generate Report – Click to generate an incident report. Click 'View Report' to view the output.
- Close – Click this to close the ticket. Enter details for closing the ticket and click 'Save'. The incident details will be archived.
- The 'Actions' drop down lists various activities you can perform on the incident:

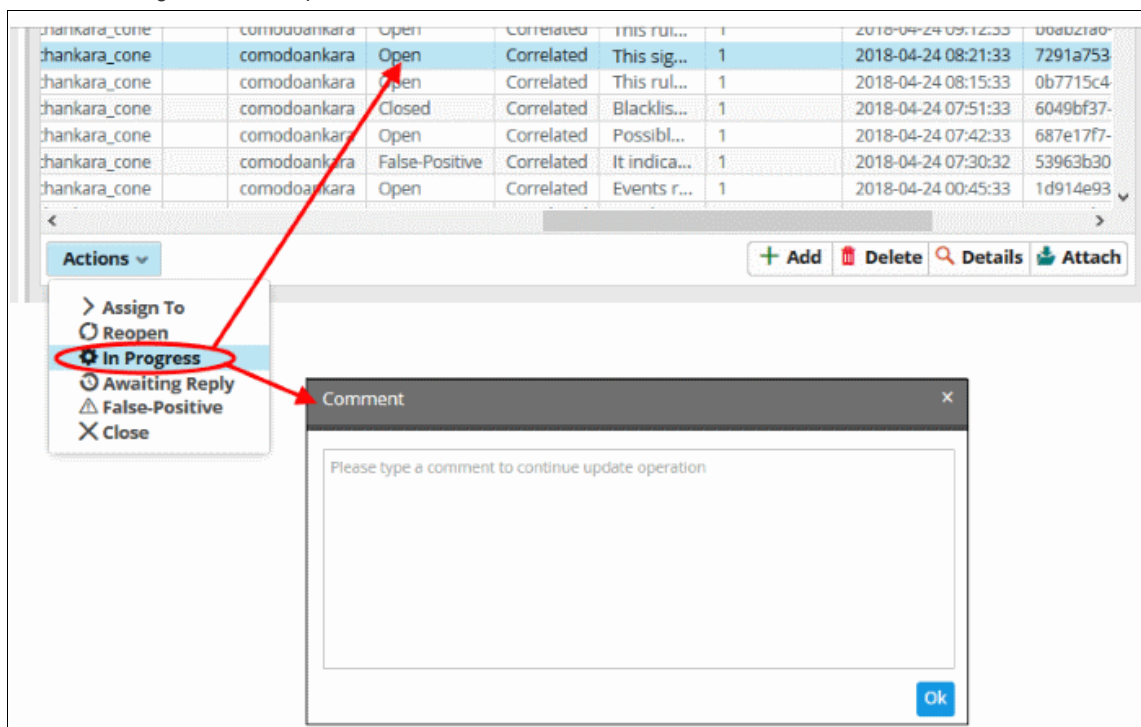


Actions:

- **Assign To** - The incident is assigned to one of the administrators



- **Reopen** - The status of the closed ticket will change to re open
- **In Progress** - Change the status of the incident to 'In Progress'. Enter a comment to explain the status change in the field provided.



- **Awaiting Reply** - Select an open incident that requires response from the user and click 'Awaiting Reply'. Enter a comment about the incident and click 'OK'
- **False-Positive** - Select the malware free incidents and select the 'False Positive' from the 'Action' drop down

- **Close** - Select 'Close' after the incident is resolved

Manually Add an Incident

In addition to the incidents reported by correlation rules, admins can manually add incidents and assign them to specific users.

To add and assign an incident

- Click the 'Add' button at the bottom of the screen.

The 'Add Incident' dialog will open.

- **Name** - Enter a name for the incident.
- **Category** - Select the classification of the incident from drop down
- **Object** - Enter the value you want to assign. For example: Source IP address
- **Subject** - Enter the value you want to assign. For example: if you have assigned source IP address to the object, you can enter the destination IP address to check for the events occurring between the two end points specified
- **Customer** - Choose the customer from the drop-down for whom you want to add the incident.
- **Assignee** - Select the user to whom the incident should be assigned
- **Priority** - Select the severity level of the incident from the drop-down. The options available are 'Info', 'Low', 'Medium', 'High' and 'Critical'.
- **Status** - Select the status of the incident from the drop-down. The options available are - Open, In

Progress, False-Positive and Closed.

- **Description** - Enter an appropriate description for the incident
- Click the 'Save' button
- Admins can identify incidents based on the name, object and subject of the incident.
- If the values above match an existing incident, then the incident will add to the count of the existing incident. If the values are new, then a new incident is created.

The incident will be added and displayed in the 'Incident List'. Please note that incidents added manually will be classified as 'Default'.

Delete an Incident

Administrator can delete incidents that are no longer required from the list.

To delete incidents

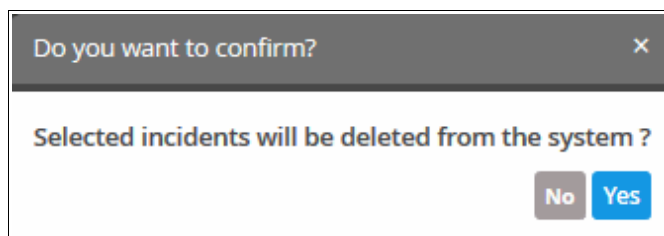
- Select the incident(s) from the list and click the 'Delete' button at the bottom

Incident List (Total Count: 1401) Generate Report [↑]

Date	Name	Object	Subject	Category	Priority	Userna
2018-04-22 14:39:32	P2P Application(s) Activity	10.1...		UNUSUAL NETWORK TRAFFIC	Medium	cwab
2018-04-21 13:27:34	New NxlDS Event Triggered	2009...	ET P2...	UNCATEGORIZED	Critical	
2018-04-21 13:27:34	P2P Application(s) Activity	10.1...		UNUSUAL NETWORK TRAFFIC	Medium	cwab
2018-04-20 15:33:33	DNS Query for Suspicious domains	10.1...	8.26...	DNS REQUEST ANOMALIES	Medium	cwab
2018-04-20 15:33:33	DNS Query for Suspicious domains	10.1...	8.26...	DNS REQUEST ANOMALIES	Medium	cwab
2018-04-20 15:26:38	SquirtDanger	10.1...	192.1...	MALWARE ACTIVITY	High	cwab
2018-04-20 15:26:38	SquirtDanger	10.1...	10.10...	MALWARE ACTIVITY	High	cwab
2018-04-20 15:21:18	eMule KAD Network Connection Request	10.1...	65.55...	UNUSUAL NETWORK TRAFFIC	Medium	cwab
2018-04-20 15:17:28	Zezin botnet activity	10.1...	5.101...	MALWARE ACTIVITY	High	cwab
2018-04-20 15:14:45	Emotet activity detection	10.1...	160.1...	MALWARE ACTIVITY	High	cwab
2018-04-20 15:14:45	Zezin botnet activity	10.1...	10.10...	MALWARE ACTIVITY	High	cwab
2018-04-20 12:42:32	Spamhaus Drop Events Inbound	10.1...	91.20...	UNUSUAL NETWORK TRAFFIC	Medium	cwab
2018-04-20 12:00:32	eMule KAD Network Connection Request	10.1...	111.2...	UNUSUAL NETWORK TRAFFIC	Medium	cwab
2018-04-20 12:00:32	P2P Application(s) Activity	10.1...		UNUSUAL NETWORK TRAFFIC	Medium	cwab
2018-04-20 10:33:33	Ransomware Tracker Reported	10.1...	103.2...	MALWARE ACTIVITY	High	cwab
2018-04-20 10:33:33	CnC Server	10.1...	103.2...	MALWARE ACTIVITY	High	cwab
2018-04-20 10:00:33	DNS Query to a *.top domain	10.1...	10.10...	DNS REQUEST ANOMALIES	Medium	cwab

Actions ▾ + Add Delete Details Attach

A confirmation dialog will be displayed before you want to delete the incident.



- Click 'Yes' to confirm removal of the incident from the list.

6.2 Incident Category Management

- Incident categories let you classify events based on their impact on the endpoint or network.
- You can assign colors to identify each category.
- There are predefined, default categories for managing essential incidents.
- You can add and edit categories as required.

Category Name	Auto Assigned Users	Manual Assigned Users	Color
AUTHENTICATION ANOMALIES	<input type="checkbox"/>	<input type="checkbox"/>	Black
ANOMALIES IN PRIVILEGED USER ACC...	<input type="checkbox"/>	<input type="checkbox"/>	Black
ANOMALIES SPECIFIC TO ENDPOINT & ...	<input type="checkbox"/>	<input type="checkbox"/>	Black
CHECK FOR KNOWN APT'S	<input type="checkbox"/>	<input type="checkbox"/>	Black
CORRELATED	<input type="checkbox"/>	<input type="checkbox"/>	Red
DNS REQUEST ANOMALIES	<input type="checkbox"/>	<input type="checkbox"/>	Black
MALWARE ACTIVITY	<input type="checkbox"/>	<input type="checkbox"/>	Black
MALWARE	<input type="checkbox"/>	<input type="checkbox"/>	Amber
MANUAL	<input type="checkbox"/>	<input type="checkbox"/>	Black
SCHEDULED QUERY	<input type="checkbox"/>	<input type="checkbox"/>	Black
UNUSUAL NETWORK TRAFFIC	<input type="checkbox"/>	<input type="checkbox"/>	Black
UNPATCHED OR VULNERABLE SYSTEM...	<input type="checkbox"/>	<input type="checkbox"/>	Black
WEB TRAFFIC ANOMALIES	<input type="checkbox"/>	<input type="checkbox"/>	Black

- The default incident categories are:
 - Authentication Anomalies
 - Anomalies in privileged user account activities
 - Anomalies specific to endpoint and backend
 - Check for known APS
 - Correlated
 - DNS Request Anomalies
 - Malware Activity
 - Malware
 - Manual
 - Scheduled Query
 - Unusual Network Traffic
 - Unpatched for Vulnerable Systems or applications
 - Web traffic anomalies

Incident Category Management List - Table of Column Descriptions	
Column Header	Description
Category Name	Label of the category.
Auto Assigned User	The user who is assigned to deal with incidents which belong to this category.

	<table border="1"> <thead> <tr> <th colspan="2">User</th> </tr> <tr> <th>Name</th> <th>Auto Assigned Users</th> </tr> </thead> <tbody> <tr> <td>yuriy.lazarenko@comodo.com</td> <td><input type="checkbox"/></td> </tr> <tr> <td>yuriy.konstantinovskiy@comodo.com</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Jason.Plata</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	User		Name	Auto Assigned Users	yuriy.lazarenko@comodo.com	<input type="checkbox"/>	yuriy.konstantinovskiy@comodo.com	<input type="checkbox"/>	Jason.Plata	<input type="checkbox"/>					
User																
Name	Auto Assigned Users															
yuriy.lazarenko@comodo.com	<input type="checkbox"/>															
yuriy.konstantinovskiy@comodo.com	<input type="checkbox"/>															
Jason.Plata	<input type="checkbox"/>															
Manual Assigned Users	<p>Users assigned when the category was created or edited.</p> <table border="1"> <thead> <tr> <th colspan="3">User</th> </tr> <tr> <th>Name</th> <th>Auto Assigned Users</th> <th>Manual Assigned Users</th> </tr> </thead> <tbody> <tr> <td>yuriy.lazarenko@comodo.com</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>yuriy.konstantinovskiy@comodo.com</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Jason.Plata</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	User			Name	Auto Assigned Users	Manual Assigned Users	yuriy.lazarenko@comodo.com	<input type="checkbox"/>	<input type="checkbox"/>	yuriy.konstantinovskiy@comodo.com	<input type="checkbox"/>	<input type="checkbox"/>	Jason.Plata	<input type="checkbox"/>	<input type="checkbox"/>
User																
Name	Auto Assigned Users	Manual Assigned Users														
yuriy.lazarenko@comodo.com	<input type="checkbox"/>	<input type="checkbox"/>														
yuriy.konstantinovskiy@comodo.com	<input type="checkbox"/>	<input type="checkbox"/>														
Jason.Plata	<input type="checkbox"/>	<input type="checkbox"/>														
Color	Represents the category type															

Note:

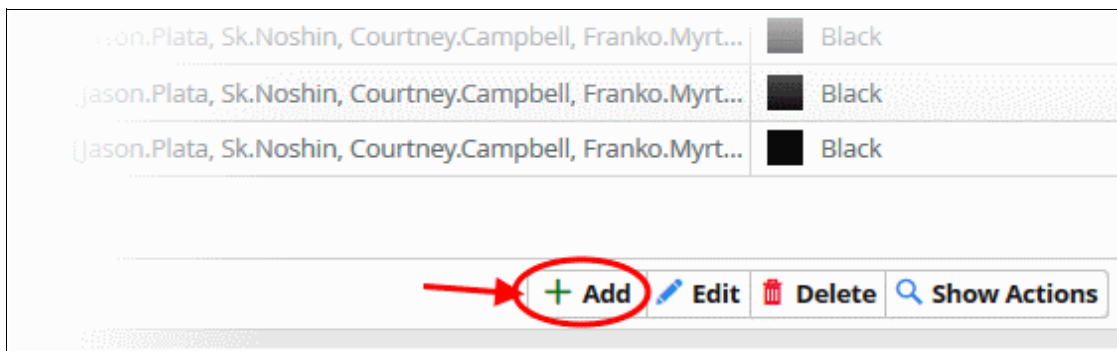
- Users take action on incidents.
- When an incident is created, it is automatically assigned to a user who is present in the 'Auto Assigned Users' list.
- You can reassign an incident to a user who is on the 'Manually Assigned Users' list. If the list is empty, you cannot assign the incident manually to a user.
- To add users to the existing list available see '**Managing Users**'

Add a Incident Category

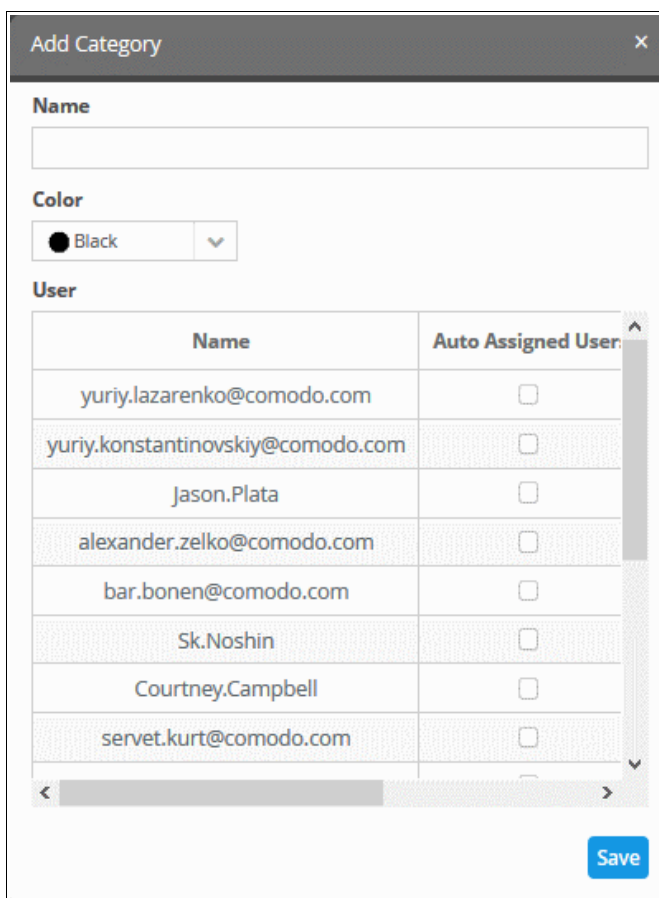
- To monitor and manage the types of incidents detected based on the correlation rules
- Once a category is added, the incidents will be grouped to the specified category based on the correlation results
- Based on the severity/priority the incident category is either auto-assigned or manually assigned to users for performing required action.

To add a new category

- Click the 'Add' button on the bottom right of the interface



The 'Add Category' dialog will open



- Enter a name to identify the detected incident type
- Select a color code from the 'Color' drop down, to indicate the category
- Select the user to whom you want the incident alerts to be sent.
 - You can choose to assign users automatically or manually by selecting the options 'Auto-Assigned User' or 'Manual Assigned Users' columns against the user
- Click 'Save' to create an incident category

Edit the incident category

You can edit the created incident category for reassigning users or changing category names.

To edit a category

- Click the 'Edit' button on the bottom right of the interface

AUTHENTICATION ANOMALIES	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...	Black
ANOMALIES IN PRIVILEGED USER ACCO...	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...	Black
ANOMALIES SPECIFIC TO ENDPOINT & ...	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...	Black
CHECK FOR KNOWN APT'S	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...	Black
MALWARE ACTIVITY	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...	Black
MALWARE	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...	Amber
SCHEDULED QUERY	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...	Black
UNUSUAL NETWORK TRAFFIC	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...	Black
UNPATCHED OR VULNERABLE SYSTEMS...	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...	Black
WEB TRAFFIC ANOMALIES	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...	Black

+ Add **Edit** Delete Show Actions

The 'Update Category' dialog will open

Update Category ✕

Name

ANOMALIES IN PRIVILEGED USER ACCOUNT ACTIVITY

Color

● Black ▾

User

Name	Auto Assigned User
yuriy.lazarenko@comodo.com	<input type="checkbox"/>
yuriy.konstantinovskiy@comodo.com	<input type="checkbox"/>
Jason.Plata	<input type="checkbox"/>
alexander.zelko@comodo.com	<input type="checkbox"/>
bar.bonen@comodo.com	<input type="checkbox"/>
Sk.Noshin	<input type="checkbox"/>
Courtney.Campbell	<input type="checkbox"/>
servet.kurt@comodo.com	<input type="checkbox"/>

Save

- Modify the fields as required and click 'Save' to update an incident category

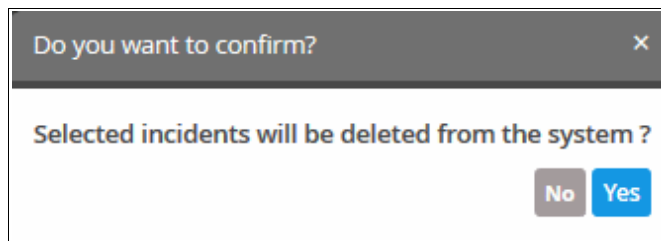
To Remove a Category

- Click 'Delete' on the bottom right

CORRELATED	[servet.kurt@comodo.com, operator]	[servet.kurt@comodo.com, operator]	Black
MANUAL	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
DNS REQUEST ANOMALIES	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
AUTHENTICATION ANOMALIES	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
ANOMALIES IN PRIVILEGED USER ACCO...	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
ANOMALIES SPECIFIC TO ENDPOINT & ...	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
CHECK FOR KNOWN APT'S	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
MALWARE ACTIVITY	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
MALWARE	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Amber
SCHEDULED QUERY	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
UNUSUAL NETWORK TRAFFIC	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
UNPATCHED OR VULNERABLE SYSTEMS...	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
WEB TRAFFIC ANOMALIES	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black

+ Add Edit Delete Show Actions

A confirmation dialog will be shown as follows:



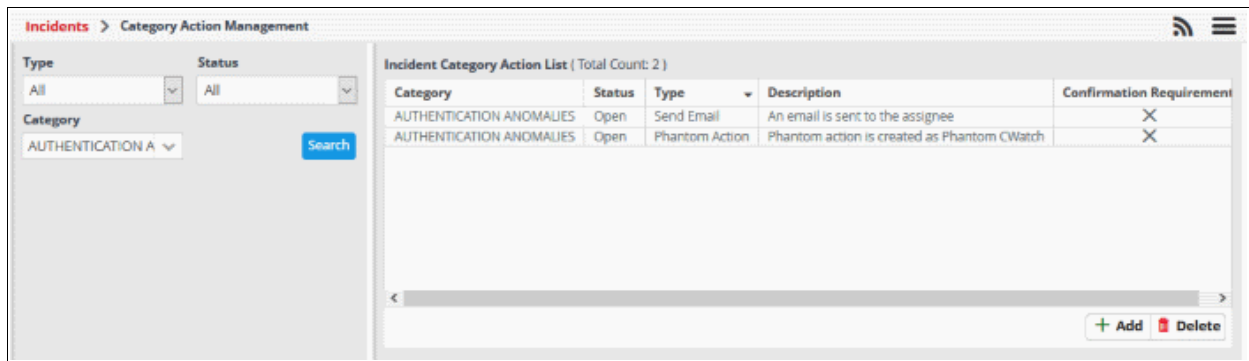
- Click 'Yes' to confirm removal of the incident category from the list.
- To view and manage the actions performed on an incident category, select a category and click 'Show Actions' on the bottom right

The 'Category Action Management' screen will open

Category Name	Auto Assigned Users	Manual Assigned Users	Color
AUTHENTICATION ANOMALIES	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
ANOMALIES IN PRIVILEGED USER ACCO...	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
ANOMALIES SPECIFIC TO ENDPOINT & ...	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
TEST CATEGORY	[yuriy.lazarenko@comodo.com]	[yuriy.lazarenko@comodo.com]	Black
CHECK FOR KNOWN APT'S	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
CORRELATED	[servet.kurt@comodo.com, operator]	[servet.kurt@comodo.com, operator]	Red
DNS REQUEST ANOMALIES	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
MALWARE ACTIVITY	[cwatchankara_cone]	[servet.kurt@comodo.com]	Black
MALWARE ACTIVITY	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
MALWARE	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Amber
MANUAL	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
SCHEDULED QUERY	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
UNUSUAL NETWORK TRAFFIC	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
UNPATCHED OR VULNERABLE SYSTEMS...	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black
WEB TRAFFIC ANOMALIES	[cwatchankara_cone]	[Jason.Plata, Sk.Noshin, Courtney.Campbell, Franko.Myrt...]	Black

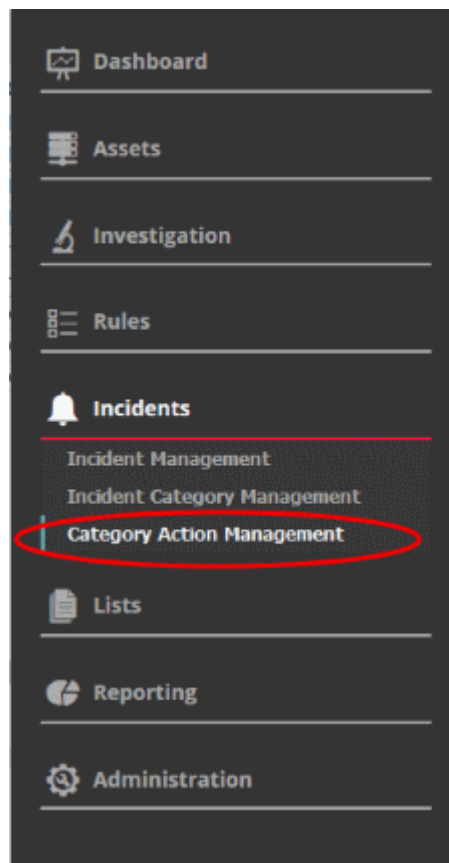
+ Add Edit Delete Show Actions

The 'Category' will be selected by default and the right hand panel will show the list of incidents that belong to the specified category.

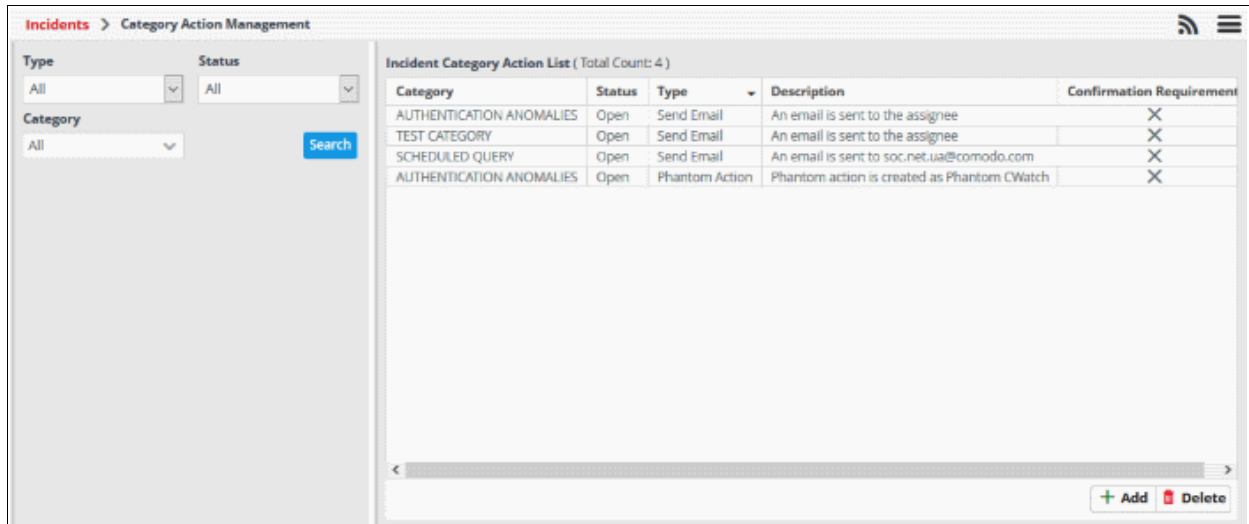


6.3 Category Action Management

- Click the 'Menu' button > 'Incidents' > 'Incident Management'.
- The category action area lets you manage the actions performed on a class of incidents.
 - You can also open this area from by selecting a category in the 'Incident Category Management' screen
- You can manually create and remove actions for incidents
- To open the interface:
 - Click the 'Menu' button > 'Incidents' > 'Incident Management'.



The 'Incident Category Action List' screen will open:

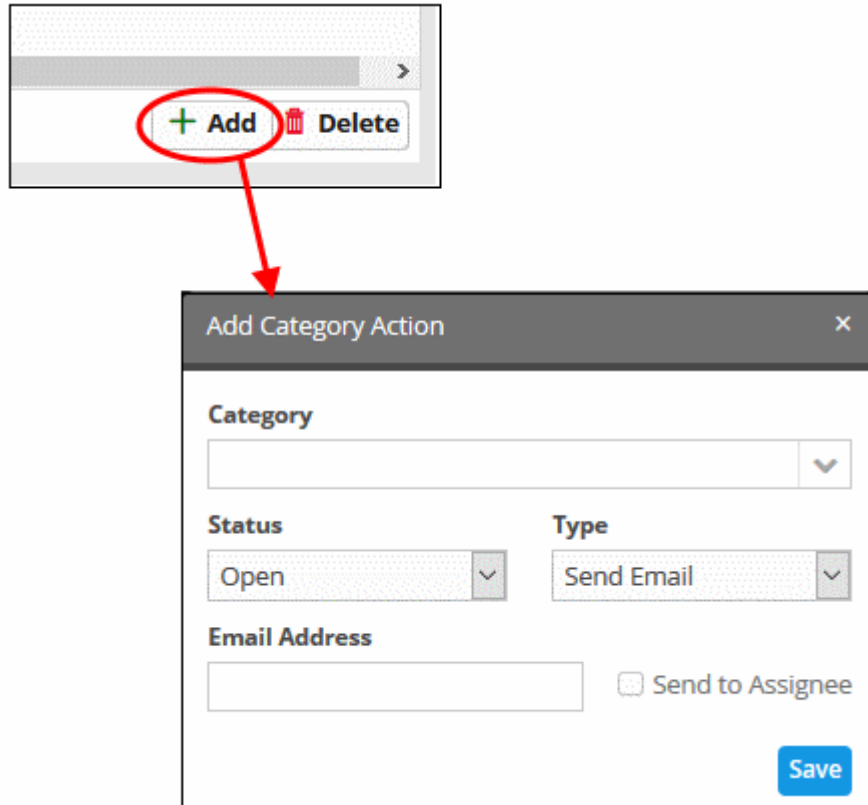


- You can filter the action list by selecting 'Type' and 'Status' of the incident
- The left hand side panel of the interface displays a list of filters to specify a particular group of incidents
- Specify values from the 'Type', 'Status' and 'Category' drop-down, and then click 'Search'

Custom Dashboards Interface - Table of controls	
Category	The incident type. For example, 'Malware activity' or 'Unusual network Traffic'
Status	Shows whether the incident is 'Open', 'In-Progress', 'False Positive' or 'Closed'.
Type	Whether the event was automatically or manually generated. Automatic events are called 'Correlated'. Manual events are called 'Default'.
Description	Specifies the current status of action in a line
Confirmation	Confirmation required to perform the action

Add a Category Action

- Click 'Add' at the bottom-right of the interface:



The 'Add Category Action' dialog will open. Users can now follow up and close their category of incidents with the actions assigned to them

- Select the category name to which you want to add an action
- Choose the status of your incident category from the 'Status' drop-down list
- Select the type of action you want to take from the 'Type' drop down
- Enter the email address of the user in the 'Email Address' field
- Select 'Send to Assignee' option if you want to send emails to the user assigned in the category management interface
- Click 'Save' to add the action to the list

Delete an Incident Action List

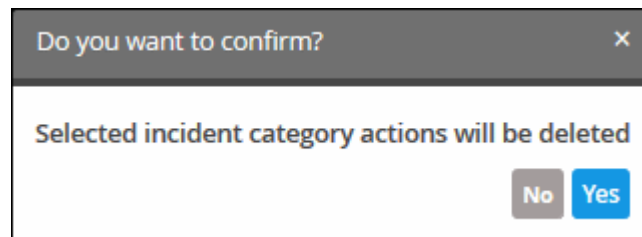
- Select the incident that you want to deleted and click the 'Delete' button on the bottom right

Incident Category Action List (Total Count: 9)

Category	Status	Type	Description	Confir
AUTHENTICATION ANOMALIES	Open	Send Email	An email is sent to the assignee	
TEST CATEGORY	Open	Send Email	An email is sent to the assignee	
CHECK FOR KNOWN APT'S	Open	Send Email	An email is sent to the assignee	
MANUAL	Open	Send Email	An email is sent to the assignee	
SCHEDULED QUERY	Open	Send Email	An email is sent to soc.net.ua@comodo.com	
AUTHENTICATION ANOMALIES	Open	Phantom Action	Phantom action is created as Phantom CWatch	
TEST CATEGORY	Open	Delete from List	Object field is deleted from the AssetList list	
AUTHENTICATION ANOMALIES	Closed	Add to List	Object field is added to the Miners list	
ANOMALIES IN PRIVILEGED USER ACCOUNT ACTIVITY	Open	Add to List	Object field is added to the AssetList list	

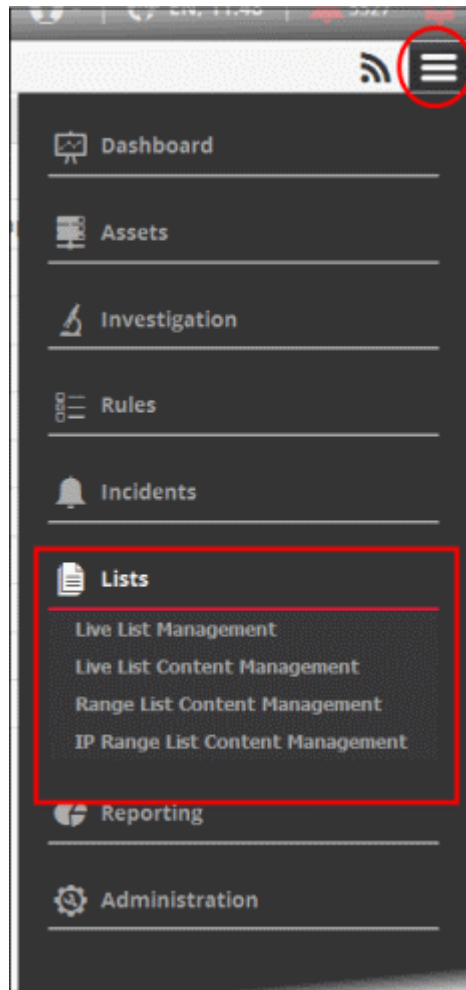
+ Add Delete

A confirmation dialog will be displayed before you want to delete the incident.



7 Lists

- A list is a set of field values which can be used as parameters in event queries and correlation rules. cWatch features three type of lists, 'Live Lists', 'Range Lists' and 'IP Range Lists'.
 - 'Live Lists' specify a single value.
 - 'Range Lists' specify a range of values (e.g. port numbers).
 - 'IP Range Lists' specify a range of IPs.
- Any updates to a list are dynamically reflected in all queries and rules in which they are used.
- Lists are created by first specifying the event field then populating it with values.
- Live lists can be populated by entering values manually or by configuring correlation rules to feed values automatically from events. See **List Mappings** in '**Managing Correlation Rules**' for more details.
- Values for range lists and IP range lists have to be entered manually.



See the following sections for more details:

- [Manage Live Lists](#)
- [Manage Live List Content](#)
- [Manage Range List Content](#)
- [Manage IP Range List Content](#)
- [Manage Multiple Column List Content](#)

7.1 Manage Live Lists

- The 'Live List Management' interface lets you create and manage 'Live Lists', 'Range List' and 'IP Range List'.
- A single list can have several 'Types', where different sets of values for the same field are used in different queries and correlation rules.
 - For example, you can create a live list called 'IP Blacklist'. The list could have two 'types' - 'Internal' (blacklisted IPs of internal hosts) and 'External' (blacklisted IPs of external hosts).
 - The two types can be used separately in queries and rules.
- You can also define the validity period of a value.

Please note that the number of lists that can be active at a time depends upon your subscription.

Note: The live list management interface only allows you to create and manage lists for various fields. The values for the fields can be manually added from the respective 'List Content Management' interface. See [Managing Live List Content](#), [Managing Range List Content](#) and [Managing IP Range List Content](#) for more details.

- To open the 'Live List Management' interface, click the 'Menu' button from the top right, choose 'Lists' options and then click 'Live List Management'.

The screenshot shows the 'Live List Management' interface with a table titled 'Live List Summary'. The table has five columns: Name, Type, Content Types, Field, and Active. Below the table are buttons for '+ Live List', '+ Range List', '+ IP Range List', '+ MCL', 'Change', and 'Show'.

Name	Type	Content Types	Field	Active
AssetList	Live List	unclassified, low, medium, high, critical	agent_ip, dst_ip, dst_tr_ip,...	✓
AssetList1	Live List	High, low	pass_days, th_handled, p...	✓
AssetRangeList	IP Range List	unclassified, low, medium, high, critical	agent_ip, dst_ip, dst_tr_ip,...	✓
Blacklist Ips	Live List	External Ips, Internal Ips	agent_id, app_name	✓
Hash	MCL	MD5, SHA256	f_md5, f_sha256	✓
Miners	Live List	IP	dst_ip	✓
Petya	Live List	MD5, SHA1, SHA256	f_sha1, f_sha256, f_md5	✓
Petya IOC	Live List	IP, domain name, mailid	src_ip, src_host, dst_ip, ds...	✓
Root DNS Servers	IP Range List	IP Adressess	dst_ip	✓
WannaCry	Live List	MD5	f_md5	✓
WannaCry List	Live List	MD5, SHA256	f_sha256, f_md5	✓
dridex_c2	Live List	IP	dst_ip	✓
mininghosts	Live List	IP	dst_ip	✓

The interface shows all existing live, range and IP lists. You can add new lists, enable or disable lists, and view list values.

Please use the following links to learn more about:

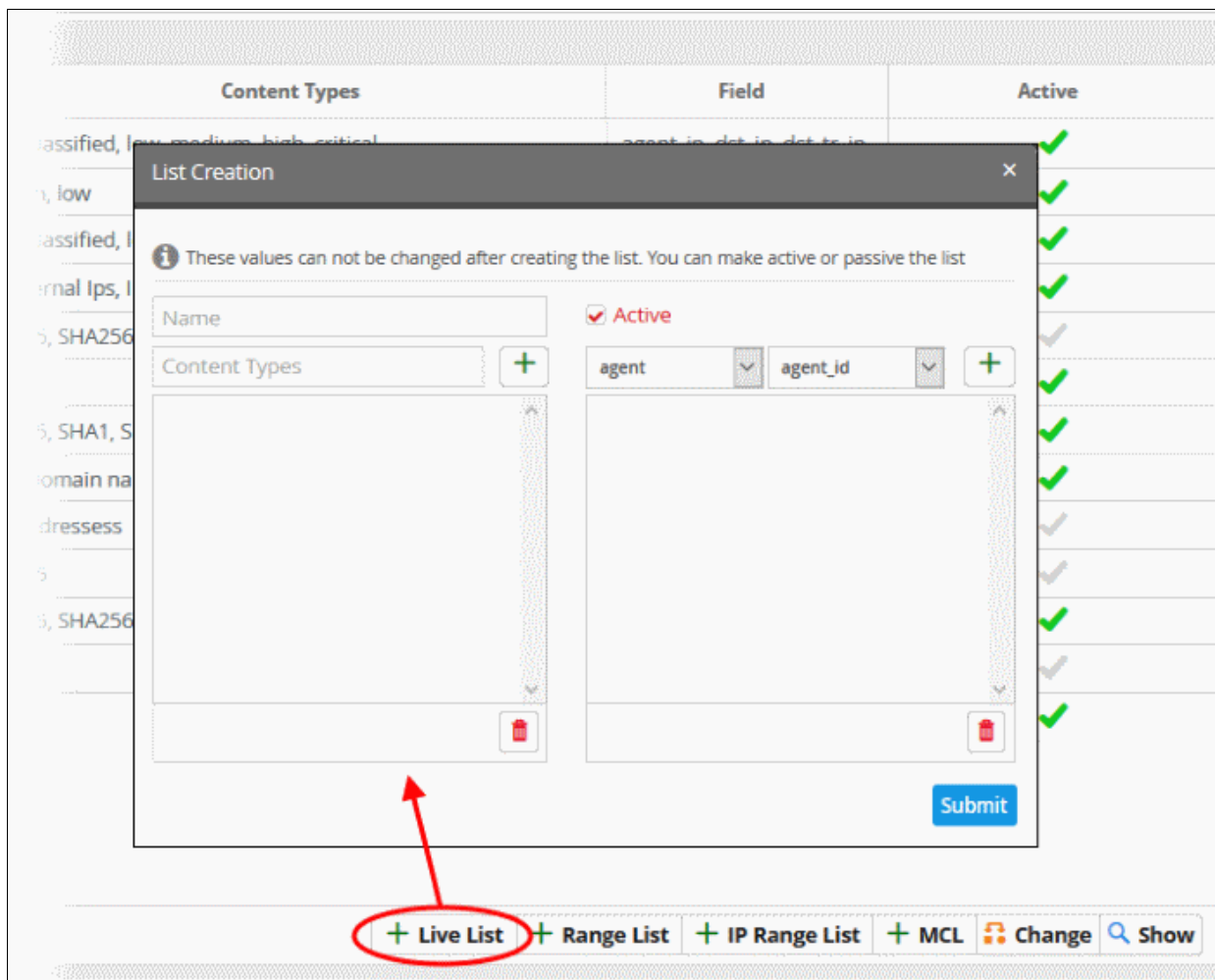
- [Create new Live Lists](#)
- [Create new Range Lists](#)
- [Create new IP Range Lists](#)
- [Change activation state of lists](#)
- [View the values entered for a list](#)
- [Create the Multiple Column Lists](#)

Create new Live Lists


A new live list can be created by specifying a name, adding types and defining the field for which the values are to be populated. The values for the field can be specified only from the 'Live List Content Management' interface. Explanations on adding values to the list types are available in [Managing Live List Content](#).

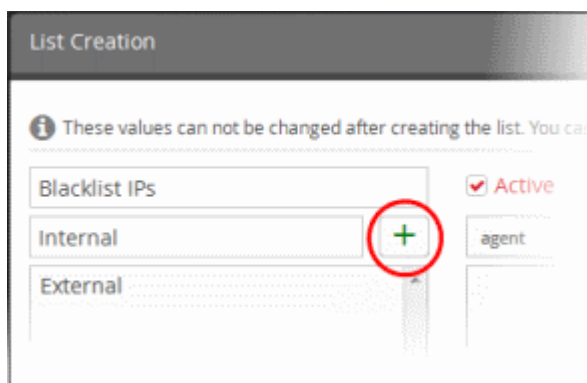
To create a new list


- Click the 'Live List' button at the bottom right of the 'Live List Management' interface.




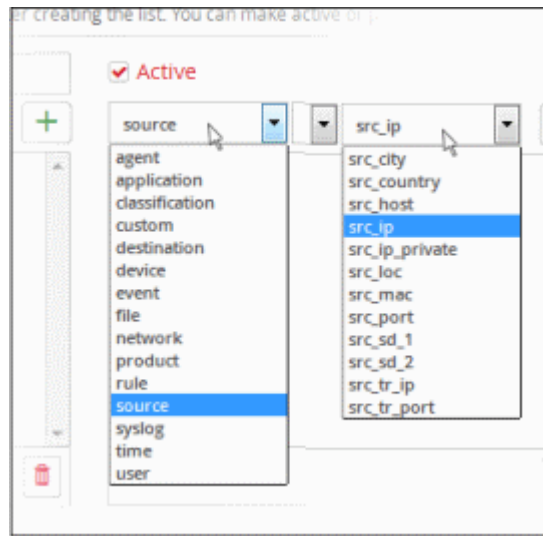
The 'List Creation' dialog will open.

- Enter a name for the live list in the 'Name' field.
- Add a name for a list type to be created in the 'Content Type' text box and click the  button. For example, you can enter 'Internal' or 'External', for which you can define IP addresses in the live list content page.




- Repeat the process to add more types for the live list.
- To remove a type, select the type from the list and click the  icon.
- Specify the field for which the values are to be populated in the list by selecting the 'Field Group' then

choose the field from the respective drop-downs and click the  button. Please note that for live lists, the full list of 'Field Group' will be available for selection.



The field will be added to the list of fields in the right pane.

- Repeat the process if you want to add more fields.
- To remove a field added by mistake, select the field from the list and click the  icon .
- Leave the 'Active' checkbox selected if you want the list to be active on creation. If you want to turn the list active at a later time, clear this checkbox.
- Click the 'Submit' button.

Caution: The name, types and field values once configured for a list cannot be changed or removed later. Please re-check these details before clicking 'Submit'.

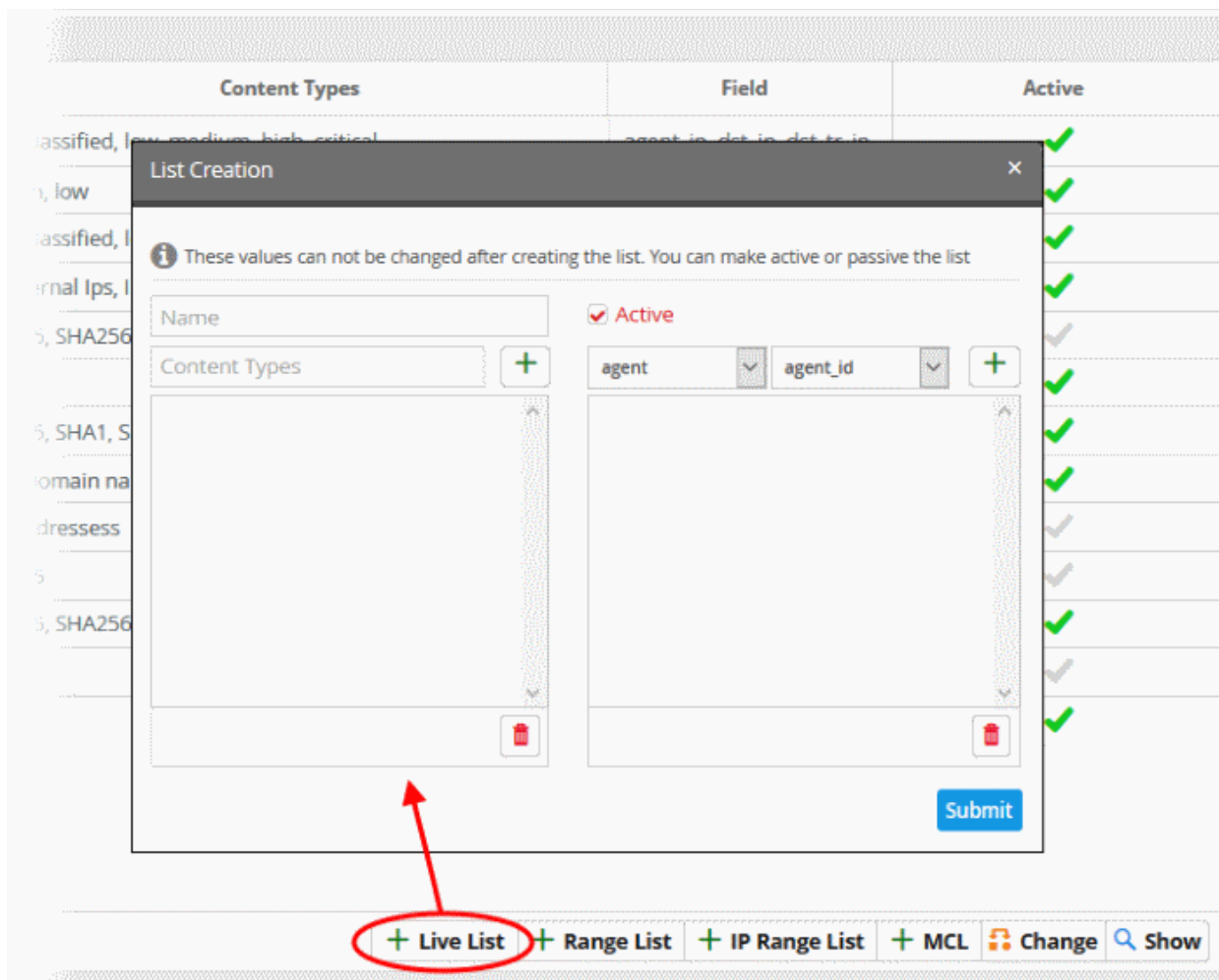
The list will be added to cWatch. The next step is to manage the values for the list. See [Managing Live List Content](#) for more details.

Create new Range Lists


- A new range list can be created by specifying a name, adding types and defining the field for which the values are to be populated.
- The values for the field can be specified only from the 'Range List Content Management' interface.
- Explanations on adding values to the range list types are available in [Managing Range List Content..](#)

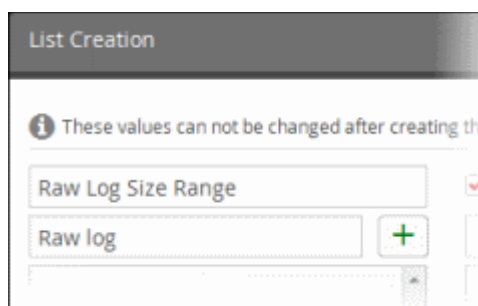
To create a new range list



- Click the 'Range List' button at the bottom right of the 'Live List Management' interface.



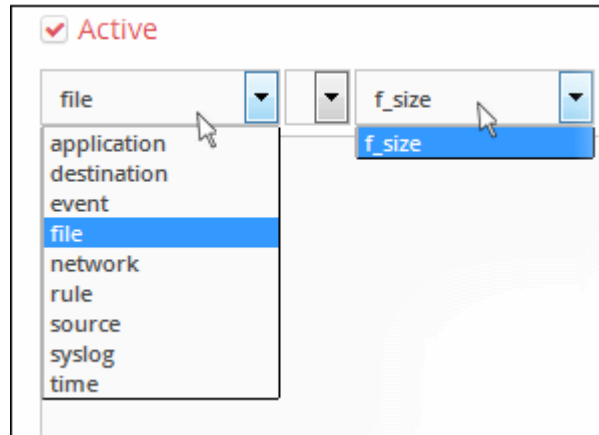
The 'List Creation' dialog will appear.

- Enter a label for the range list in the 'Name' field.
- Add a name for the range list type in the 'Type' box. Click  to save the type.




- Repeat the process to add more types for the range list.
- To remove a type, select the type from the list and click the trash can icon .
- Specify the field for which the values are to be populated in the list by selecting the field group then choose the field from the respective drop-downs and click the  button.
 - Please note that for range lists, only appropriate 'Field Groups' will be available.

- That is, the fields available for a field group can be configured for a range.
- For example, if you choose 'File' field group, then the field available for this is 'f_size' for which you can provide a minimum and maximum size.



The field will be added to the list of fields in the right pane.

- Repeat the process if you want to add more fields.
- To remove a field, select it from the list and click the  icon .
- Leave the 'Active' checkbox selected if you want the range list to be active on creation. If you want to turn the range list active at a later time, clear this checkbox.
- Click the 'Submit' button.

Caution: The name, types and field values once configured for a range list cannot be changed or removed later. Please re-check these details before clicking 'Submit'.

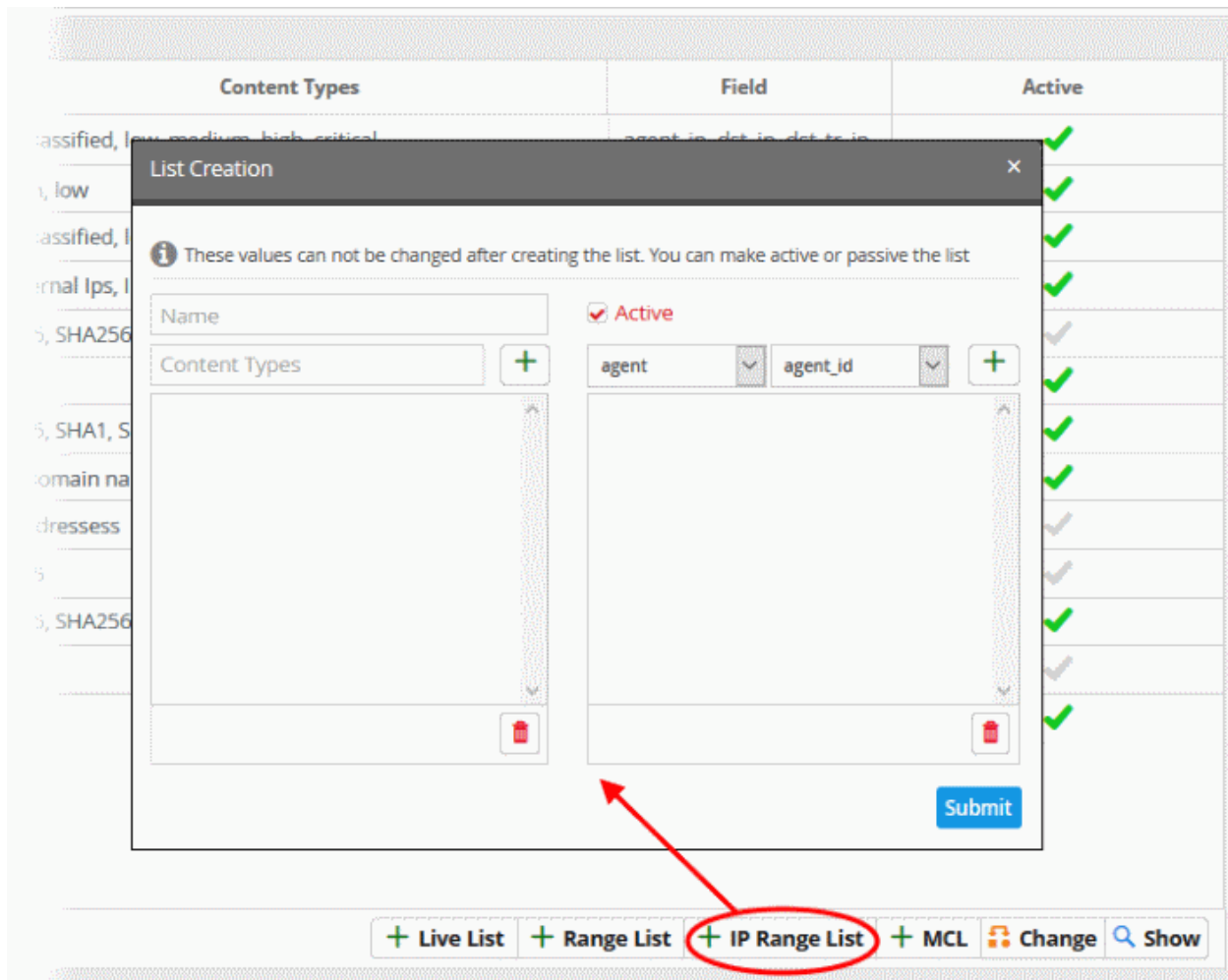
The range list will be added to cWatch. The next step is to manage the values for the range list. See [Managing Range List Content](#) for more details.

Creating new IP Range Lists


A new IP range list can be created by specifying a name, adding types and defining the field for which the values are to be populated. The values for the field can be specified only from the 'IP Range List Content Management' interface. Explanations on adding values to the IP range list types are available [Managing IP Range List Content](#).

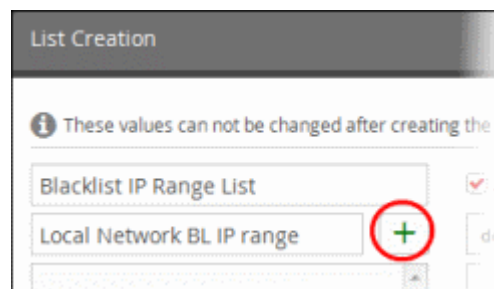
To create a new IP range list



- Click the 'IP Range List' button at the bottom right of the 'Live List Management' interface.



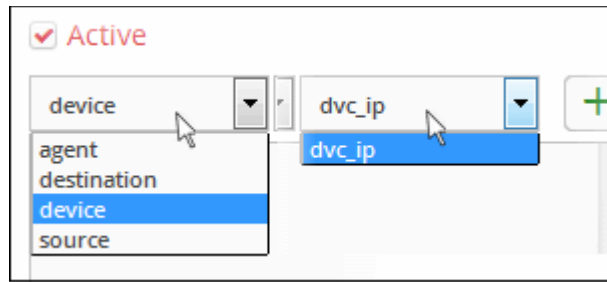
The 'List Creation' dialog will appear.

- Enter a name for the IP range list in the 'Name' field.
- Add a name for the IP range list type to be created in the Type text box and click the  button. For example, you can enter 'Local Network BL IP range' or 'External Network BL IP range', for which you can define the local IP network range in the IP range list content interface.




- Repeat the process to add more types for the IP range list.
- To remove a type, select the type from the list and click the  trash icon.
- Specify the field for which the values are to be populated in the list by selecting the 'Field Group' then choose the field from the respective drop-downs and click the  button. Please note that for IP range

lists, only appropriate 'Field Groups' will be available. That is, the fields available for a field group can be configured for an IP range. For example, if you choose 'Agent' field group, then the field available for this is 'agent_ip' for which you can provide a start and end IP range.



The field will be added to the list of fields in the right pane.

- Repeat the process if you want to add more fields.
- To remove a field, select the field from the list and click the  trash can icon.
- Leave the 'Active' checkbox selected if you want the IP range list to be active on creation. If you want to turn the IP range list active at a later time, clear this checkbox.
- Click the 'Submit' button.


Caution: The name, types and field values once configured for an IP range list cannot be changed or removed later. Please re-check these details before clicking 'Submit'.

The IP Range List will be added to cWatch. The next step is to manage the values for the range list. See [Managing IP Range List Content](#) for more details.

Changing activation state of lists

Lists can be switched between active and inactive states at any time. The inactive lists do not feed the values to the event queries and the correlation rules in which they are used.

To change the active/inactive state of a list

- Choose the list from the 'Live List Summary' interface and click the 'Change'  **Change** button at the bottom right.

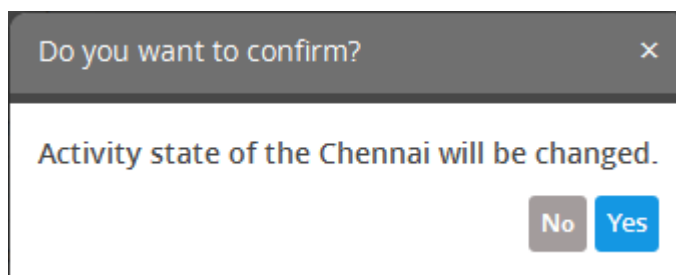
Lists > Live List Management

Live List Summary

Name	Type	Content Types	Field	Active
AssetList	Live List	unclassified, low, medium, high, critical	agent_ip, dst_ip, dst_tr_ip...	✓
AssetList1	Live List	High, low	pass_days, th_handled, th...	✓
AssetRangeList	IP Range List	unclassified, low, medium, high, critical	agent_ip, dst_ip, dst_tr_ip...	✓
Blacklist Ips	Live List	External ips, Internal ips	agent_id, app_name	✓
Hash	MCL	MD5, SHA256	f_md5, f_sha256	✓
Miners	Live List	IP	dst_ip	✓
Petya	Live List	MD5, SHA1, SHA256	f_sha1, f_sha256, f_md5	✓
Petya IOC	Live List	IP, domain name, mailid	src_ip, src_host, dst_ip, ds...	✓
Root DNS Servers	IP Range List	IP Adressess	dst_ip	✓
WannaCry	Live List	MD5	f_md5	✓
WannaCry List	Live List	MD5, SHA256	f_sha256, f_md5	✓
dridex_c2	Live List	IP	dst_ip	✓
mininghosts	Live List	IP	dst_ip	✓

+ Live List + Range List + IP Range List + MCL **Change** Show

A confirmation dialog will open.



- Click 'Yes' to confirm the change.

The change in the state of the list will be indicated under the 'Active' column in the 'Live List Summary' interface.

Viewing the values entered for a list

Administrators can view and edit values for all list types.

- Choose the list from the 'Live List Summary' interface and click the 'Show'  button at the bottom right.

Name	Type	Content Types	Field	Active
AssetList	Live List	unclassified, low, medium, high, critical	agent_ip, dst_ip, dst_tr_ip,...	✓
AssetList1	Live List	High, low	pass_days, th_handled, p...	✓
AssetRangeList	IP Range List	unclassified, low, medium, high, critical	agent_ip, dst_ip, dst_tr_ip,...	✓
Blacklist Ips	Live List	External Ips, Internal Ips	agent_id, app_name	✓
Hash	MCL	MD5, SHA256	f_md5, f_sha256	✓
Miners	Live List	IP	dst_ip	✓
Petya	Live List	MD5, SHA1, SHA256	f_sha1, f_sha256, f_md5	✓
Petya IOC	Live List	IP, domain name, mailid	src_ip, src_host, dst_ip, ip...	✓
Root DNS Servers	IP Range List	IP Adressess	dst_ip	✓
WannaCry	Live List	MD5	f_md5	✓
WannaCry List	Live List	MD5, SHA256	f_sha256, f_md5	✓
dridex_c2	Live List	IP	dst_ip	✓
mininghosts	Live List	IP	dst_ip	✓

[+ Live List](#)
[+ Range List](#)
[+ IP Range List](#)
[+ MCL](#)
[Change](#)
[Show](#)

The respective 'List Content Management' interface will open with a list of values added to the list.

Range Start	Range End	List	Type	Customer	Due Date	Last Update Time
80	7000	Chennai	Domain Na...	All	2037-01-01 02:00:00	2016-04-25 16:33:34

[+ Add](#)
[Edit](#)
[Delete](#)

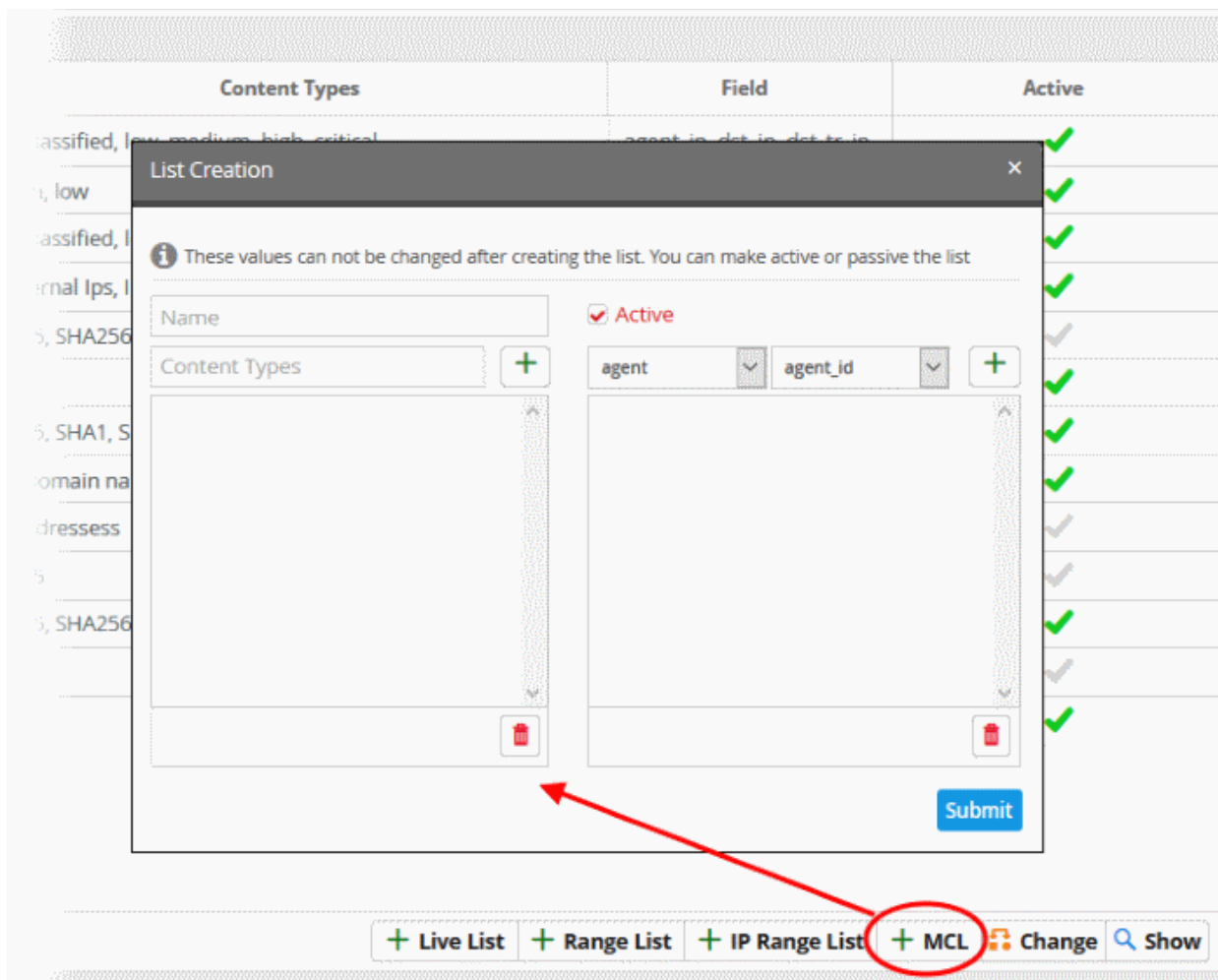
See [Managing Live List Content](#), [Managing Range List Content](#) and [Managing IP Range List Content](#), for more details on adding new values and editing existing values.

Create New Multiple Column Lists


- A new Multiple Column List (MCL) can be created by specifying a name, adding types and defining the field for which the values are populated.
- You can view more than one range of IPs using this interface.
- For example, If you want to track two lists of IPs in a incident, you can add IPs that spread virus as one list and IPs that are infected as another list in the MCL interface
- The values for the field can be specified from the 'Live List Content Management' interface.
- Explanations on adding values to the list types are available in [Managing Multiple Column Lists](#).

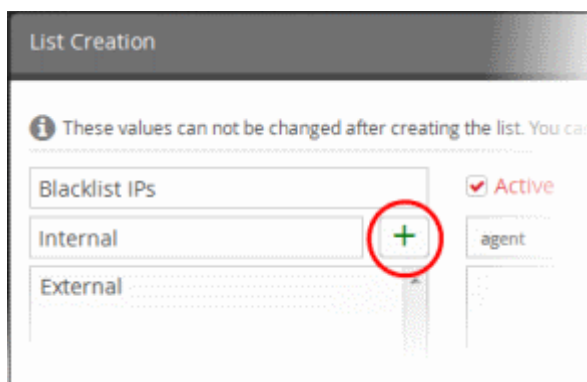
To create a new list



- Click the 'MCL' button at the bottom right of the 'Live List Management' interface.

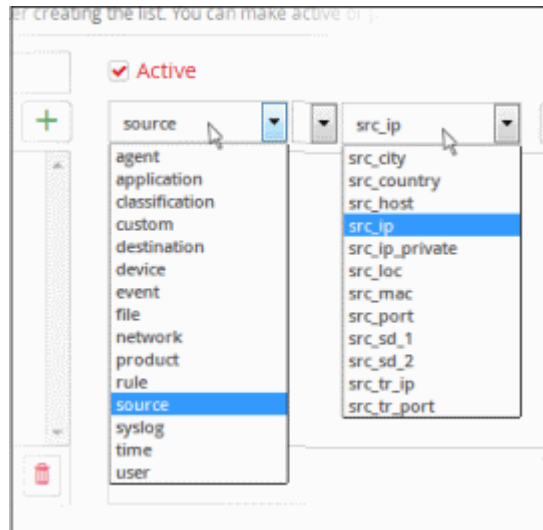


The 'List Creation' dialog will open.


- Enter a name for the MCL list in the 'Name' field.
- Add a name for a list type to be created in the 'Content Type' text box and click the  button. For example, you can enter 'Internal' or 'External', for which you can define IP addresses in the MCL list content page.



- Repeat the process to add more types for the live list.
- To remove a type, select the type from the list and click the  icon.
- Specify the field for which the values are to be populated in the list by selecting the 'Field Group' then choose the field from the respective drop-downs and click the  button. Please note that for live lists, the full list of 'Field Group' will be available for selection.



The field will be added to the list of fields in the right pane.

- Repeat the process if you want to add more fields.
- To remove a field added by mistake, select the field from the list and click the  icon .
- Leave the 'Active' checkbox selected if you want the list to be active on creation. If you want to turn the list active at a later time, clear this checkbox.
- Click the 'Submit' button.

Caution: The name, types and field values once configured for a list cannot be changed or removed later. Please re-check these details before clicking 'Submit'.

The list will be added to cWatch. The next step is to manage the values for the list. You can manage these MCL lists only by clicking 'Show' button. See [Create the Multiple Column Lists](#) for more details.

7.2 Manage Live List Content

The values for a live list can be populated in two ways:

- Manually added to the list.
- Fed from a correlation rule. Rules that identify specific events can be configured to feed values to a live list from those events. See [List Mappings](#) in [Managing Correlation Rules](#).

This section explains how to manually add values to lists and manage existing values. The 'Live List Content Management' interface allows you to view values added to all or selected lists, manually add new values, edit existing values and remove values from a list.

To open the 'Live List Content Management' interface,

- Click the 'Menu' button from the top right, choose 'Lists' and then click 'Live List Content Management'.

The screenshot shows the 'Live List Content Management' interface. At the top, there are filters for Customer (All), List (AssetList), Type (All), and a search box. Below the filters is a table titled 'List Contents' with the following columns: Value, List, Type, Customer, Due Date, and Last Update Time. The table contains 20 rows of data, all with 'AssetList' as the List and 'comodoankara' as the Customer. The Due Date for most items is '2018-05-17 06:35:43', while one item has a Due Date of '2037-01-01 00:00:00'. The Last Update Time for all items is '2017-05-17 06:36:10'. At the bottom right of the table, there are buttons for '+ Add', 'Import', 'Export', 'Edit', and 'Delete'.

By default, the live 'List Contents' table shows the values added to all the live lists. You can filter the table to view the values added to a specific list using the filter options from the top.

Live List Contents Table - Column Descriptions	
Column Header	Description
Value	Displays the value added to a list.
List	Displays the live list to which the value belongs.
Type	Displays the type of the live list, to which the value belongs.
Customer	Displays the customer to which the value is applicable.
Due Date	Indicates date and time till which the value is valid in the list. On lapse of the due date, the value will be automatically removed from the list.
Last Update Time	Date and time the live list was last updated.

Sorting and Filtering Options:

- Clicking on any of the table header sorts the items in alphabetical/ascending/descending order
- To filter values for a specific customer, choose the customer from the 'Customer' drop-down and click 'Search'.
- To view values that belong to a specific live list, choose the list from the 'List' drop-down and click 'Search'.
- To view values that belong to a specific live list type, select the list from the 'List' drop-down, then choose the type from the 'Type' drop-down and click 'Search'.

The interface allows you to:

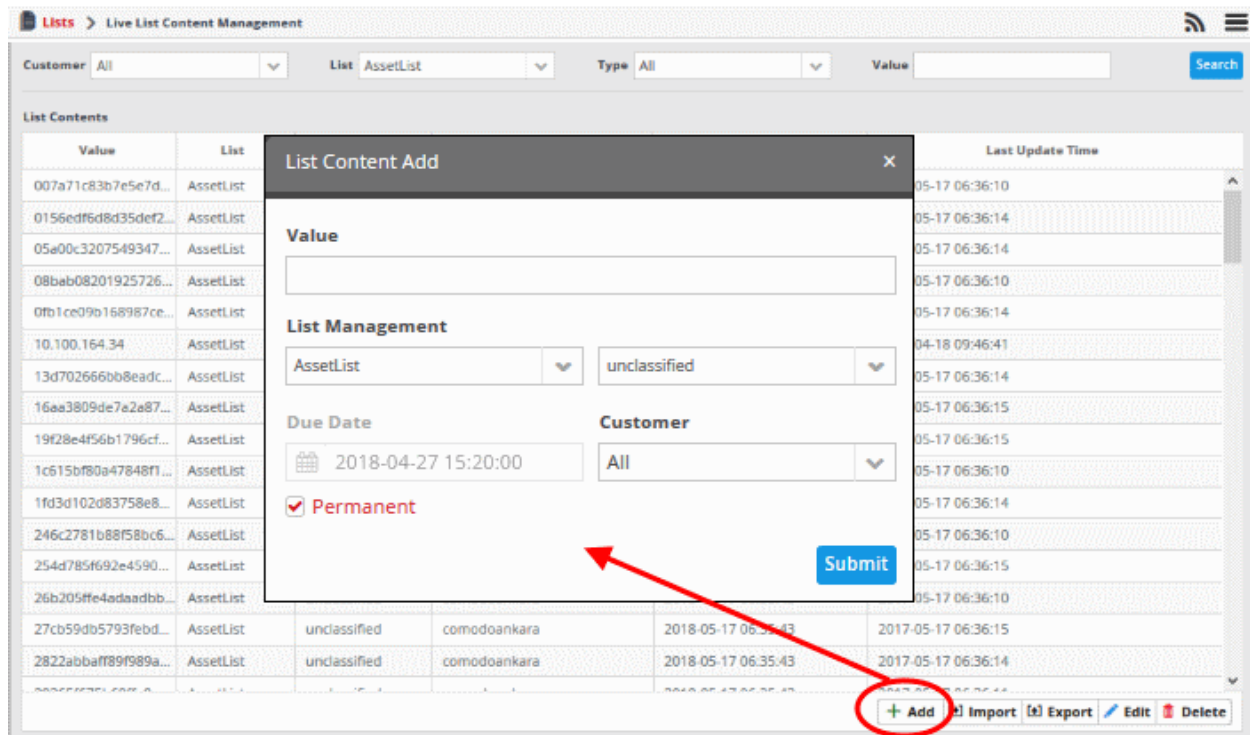
- **Manually add values to live lists**
- **Import values to a live lists**
- **Export values to a live lists**

- **Edit existing values in a list**
- **Remove values from a list**

To manually enter a value to a list

- Click the 'Add' button at the bottom right of the 'Live List Content Management' interface.

The 'List Content Add' dialog will appear.



- Select the live list and the list type to which the value is to be added, from the respective drop-downs under 'List Management'. See '**Creating new live list**' in '**Managing Live Lists**' for more details.
- Enter the value for the field defined for the live list in the 'Value' field.
- Enter the date till which the value is valid in the 'Due Date' field.
 - Click the calendar icon at the left of the field and choose the date.
 - On the specified date, the value will be automatically removed from the list. Select the 'Permanent' option if you want the value to be valid forever.
- Select the customer to which the value should apply from the 'Customer' drop-down.
- Click 'Submit'.

The value will be added to the selected list type.

- Repeat the process for adding more values to the list.

You can click 'Upload File' management

To Import values to a live list

- Click the 'Menu' button at top right > choose 'Lists'
- Click 'Live List Content Management'
- Select the list to which you want to import values then click the 'Import' button

007a71c83b7e5e7d...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:10
0156edf6d8d35def2...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:14
05a00c3207549347...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:14
08bab08201925726...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:10
0fb1ce09b168987ce...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:14
10.100.164.34	AssetList	unclassified	All	2037-01-01 00:00:00	2018-04-18 09:46:41
13d702666bb8eadc...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:14
16aa3809de7a2a87...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:15
19f28e4f56b1796c7...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:15
1c615b8f0a47848f1...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:10
1fd3d102d83758e8...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:14
246c2781b88f58bc6...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:10
254d785f692e45906...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:15
26b205ffe4adaadb...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:10
27cb59db5793fcbd...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:15
2822abba99f989a...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:14
...

+ Add [i] Import [E] Export [P] Edit [X] Delete

The 'Import List Content' screen will open:

Import List Content
✕

Select File to Upload

List Management

AssetList
▼

unclassified
▼

Due Date

📅
2018-04-27 11:09:00

Customer

All
▼

- 'Due Date' - Date at which the list values will expire and will no longer be active.
- Select the customer for whom you want to import live list values
- Click 'Import' to upload the file

Please note that you can upload only one list in a file.

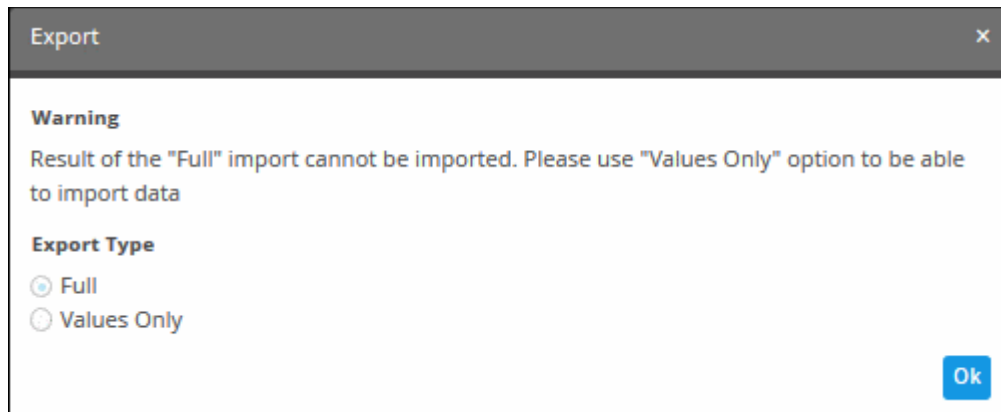
To Export values to a live list

- Select the live list and then click 'Export' button

007a71c83b7e5e7d...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:10
0156edf6d8d35def2...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:14
05a00c3207549347...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:14
08bab08201925726...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:10
0fb1ce09b168987ce...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:14
10.100.164.34	AssetList	unclassified	All	2037-01-01 00:00:00	2018-04-18 09:46:41
13d702666bb8eadc...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:14
16aa3809de7a2a87...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:15
19f28e4f56b1796cf7...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:15
1c615bf80a47848f1...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:10
1fd3d102d83758e8...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:14
246c2781b88f58bc6...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:10
254d785f692e45906...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:15
26b205ffe4adaadb...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:10
27cb59db5793fcbd...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:15
2822abbaff89f989a...	AssetList	unclassified	comodoankara	2018-05-17 06:35:43	2017-05-17 06:36:14
...

+ Add Import Export Edit Delete

- The 'Export' screen will open.




The 'Export' screen will open. Since all imported lists cannot be exported in a single attempt, you need to choose to

- Select 'Values Only' option to enable export
- Click 'OK' to upload the file

Please note that you can upload only one list in a file.

To edit an existing value in a list

- Select the live list and choose the type from the 'List' and 'Type' drop-downs respectively at the top of the 'Live List Content Management' interface and click 'Search', to view only the values added to the required 'Live List'/'Type'.
- Select the value and click the 'Edit' button  at the bottom right of the interface.

The 'List Content Edit' dialog will appear for the chosen value. The dialog is similar to the 'List Content Add' dialog. See [above](#) for more details.

- Edit the details as required and click 'Submit'.

The value will be edited and will take immediate effect on the event queries and correlation rules in which the live list is used.

To remove a value from a list

- Select the live list from the 'Live List Content' interface
- Select the value and click the 'Delete' button  at the bottom right of the interface.

A confirmation dialog will appear.

- Click 'Yes' to confirm the removal.

The list will be updated with the removal of the value. The change will take effect immediately in event queries and correlation rules which use the list.

7.3 Manage Range List Content

- The values of a range list can be populated manually in the 'Range List Content Management' interface.
- See [create new range list](#) and [Live List Management](#) for more help around this topic

To open the 'Range List Content Management' interface:

- Click 'Menu' on the top-right
- Choose 'Lists' > 'Range List Content Management'

Range Start	Range End	List	Type	Customer	Due Date	Last Update Time
200	1000	Raw Log S...	Raw log	All	2016-05-31 10:42:46	2016-05-05 09:43:38
80	7000	Chennai	Domain Na...	All	2037-01-01 02:00:00	2016-04-25 16:33:34

By default, the range list contents table shows values added to all range lists. You can filter the table to view values added to a specific list using the filter options at the top.

Range List Contents Table - Column Descriptions	
Column Header	Description
Range Start	Displays the start value for the range
Range End	Displays the end value for the range
List	Displays the range list to which the value belongs.
Type	Displays the type of the range list, to which the value belongs.
Customer	Displays the customer to which the value is applicable.
Due Date	Indicates date and time till which the value is valid in the list. On lapse of the due date, the value will be automatically removed from the list.
Last Update Time	Date and time the range list was last updated.

Sorting and Filtering Options:

- Clicking on any of the table header sorts the items in alphabetical/ascending/descending order
- To filter values for a specific customer choose the customer from the 'Customer' drop-down and click 'Search'.
- To view values belonging to a specific range list, choose the list from the 'List' drop-down and click 'Search'.
- To view values belonging to a specific range list type, select the type from the 'List' drop-down, then choose the type from the 'Type' drop-down and click 'Search'.

The interface allows you to:

- **Manually add values to range lists**
- **Edit existing values in a range list**
- **Remove values from a range list**

To manually enter a value to a range list

- Click the 'Add' button at the bottom right of the 'Range List Content Management' interface.


The 'List Content Add' dialog will appear.

- Select the 'Range List' and the list type to which the value is to be added, from the respective drop-downs under 'List Management'. See '**Creating new range list**' in '**Managing Live Lists**' for details about creating new range lists'
- Enter the values for the field defined for the range list in the 'Range Start' and 'Range End' fields. Please note that IP range value is not allowed here.
- Enter the date till which the value is valid in the 'Due Date' field. You can click the calendar icon at the left of the field and choose the date. On the specified date, the value will be automatically removed from the list. If you want the value to be permanently valid, select the 'Permanent' checkbox.
- Select the customer to which the value is applicable from the 'Customer' drop-down.
- Click 'Submit'.

The value will be added to the selected list type.

- Repeat the process for adding more values to the list.

To edit an existing value in a range list


- Select the range list and choose the type from the 'List' and 'Type' drop-downs respectively at the top of the 'Range List Content Management' interface and click 'Search', to view only the values added to the required range list/type.
- Select the value and click the 'Edit' button  at the bottom right of the interface.

The 'List Content Edit' dialog will appear for the chosen value. The dialog is similar to the 'List Content Add' dialog. See **above** for more details.

- Edit the details as required and click 'Submit'.

The change will take immediate effect in event queries and rules which use the list.

To remove a value from a range list

- Select the range list and choose the type from the 'List' and 'Type' drop-downs respectively at the top of the 'Range List Content Management' interface and click 'Search', to view only the values added to the required range list/type.
- Select the value and click the 'Delete' button  at the bottom right of the interface.

A confirmation dialog will appear.

- Click 'Yes' to confirm the removal.

The list will be updated to remove the value and will take effect immediately on the event queries and correlation rules in which the range list is used.

7.4 Manage IP Range List Content

The values for an IP Range List that was **created** in 'Live List Management' interface can be populated manually from the 'IP Range List Content Management' interface.

To open the 'IP Range List Content Management' interface,

- Click the 'Menu' button from the top right, choose 'Lists' and then click 'IP Range List Content Management'.

Range Start	Range End	List	Type	Customer	Due Date	Last Update Time
192.162.1.1	192.162.1.25	Blacklist L...	Local Networ...	All	2016-05-31 12:45:44	2016-05-05 11:47:14
192.160.2.1	192.160.2.25	Trichy	IP range list	All	2016-05-31 11:47:31	2016-05-05 11:48:31

By default, the 'IP Range List Contents' table shows the values added to all the range lists. You can filter the table to view the values added to a specific list using the filter options from the top.

Range List Contents Table - Column Descriptions	
Column Header	Description
Range Start	The first IP in the range
Range End	The last IP in the range
List	The IP range list to which the value belongs.
Type	The type of IP range list to which the value belongs.
Customer	The customer to whom the value applies.
Due Date	Date and time which the value is valid until. After the due date, the value will be automatically removed from the list.
Last Update Time	Date and time the IP range list was last updated.

Sorting and Filtering Options:

- Clicking on any of the table header sorts the items in alphabetical/ascending/descending order
- To filter values for a specific customer select the customer from the 'Customer' drop-down and click 'Search'.
- To view values belonging to a specific IP Range List, select the list from the 'List' drop-down and click 'Search'.
- To view values belonging to a specific IP range list type, select the type from the 'List' drop-down, then choose the type from the 'Type' drop-down and click 'Search'.

The interface allows you to:

- **Manually add values to IP range lists**
- **Edit existing values in an IP range list**
- **Remove values from a IP range list**

To manually enter a value to an IP range list

- Click the 'Add' button at the bottom right of the 'IP Range List Content Management' interface.


The 'List Content Add dialog' will appear.

- Select the IP range list and the list type to which the value is to be added, from the respective drop-downs under 'List Management'. See **'Creating new range list'** in **'Managing Live Lists'** for details about creating new range lists'
- Enter the values for the field defined for the IP range list in the 'Range Start' and 'Range End' fields. Please note that only IP range value is allowed here.
- Enter the date till which the value is valid in the 'Due Date' field.
 - You can click the calendar icon at the left of the field and choose the date. On the specified date, the value will be automatically removed from the list.
 - If you want the value to be permanently valid, select the 'Permanent' option.
- Select the customer to which the value is applicable from the 'Customer' drop-down.
- Click 'Submit'.

The value will be added to the selected list type.

- Repeat the process for adding more values to the list.

To edit an existing value in an IP range list


- Select the IP range list and choose the type from the 'List' and 'Type' drop-downs respectively at the top of the 'IP Range List Content Management' interface and click 'Search', to view only the values added to the required IP range list/type.
- Select the value and click the 'Edit' button  at the bottom right of the interface.

The 'List Content Edit' dialog will appear for the chosen value. The dialog is similar to the 'List Content Add' dialog. See **above** for more details.

- Edit the details as required and click 'Submit'.

The value will be edited and will take immediate effect on the event queries and correlation rules in which the IP range list is used.

To remove a value from a range list

- Select the range list and choose the type from the 'List' and 'Type' drop-downs respectively at the top of the 'Range List Content Management' interface and click 'Search', to view only the values added to the required IP range list/type.
- Select the value and click the 'Delete' button  at the bottom right of the interface.

A confirmation dialog will open.

- Click 'Yes' to confirm the removal.

The list will be updated for the removal of the value and take effect immediately on the event queries and correlation rules in which the IP range list is used.

7.5 Manage Multiple Column List Content

The values of a multiple column list (MCL) can be populated in two ways:

- Manually added to the list.
- Fed from a correlation rule. See **List Mappings** in **Managing Correlation Rules**.

This section explains how to manually add values to lists and manage existing values. The 'Multiple Column List Content Management' interface lets you view values under more than one column.

For example:

- If you want to check for attacks that originate from one set of IPs and target another set of IPs
 - You can create an MCL list with the two sets of IP as separate columns.
 - You can then manage the list from the 'Multiple Column List Content Management' interface by adding/updating/deleting IPs

OR

- To check for incidents that originate from assets belonging to specific departments, create an MCL list by adding columns for the assets of each department.

To open the 'Multiple Column List Content Management' interface,

- Select an MCL list from the 'Live List Management' interface and then click 'show'

Live List Summary

Name	Type	Content Types	Field	Active
AssetList	Live List	unclassified, low, medium, high, critical	agent_ip, dst_ip, dst_tr_ip...	✓
AssetList1	Live List	High, low	pass_days, th_handled, p...	✓
AssetRangeList	IP Range List	unclassified, low, medium, high, critical	agent_ip, dst_ip, dst_tr_ip...	✓
Blacklist Ips	Live List	External Ips, Internal Ips	agent_id, app_name	✓
Hash	MCL	MD5, SHA256	f_md5, f_sha256	✓
Miners	Live List	IP	dst_ip	✓
Petya	Live List	MD5, SHA1, SHA256	f_sha1, f_sha256, f_md5	✓
Petya IOC	Live List	IP, domain name, mailid	src_ip, src_host, dst_ip, ds...	✓
Root DNS Servers	IP Range List	IP Adressess	dst_ip	✓
WannaCry	Live List	MD5	f_md5	✓
WannaCry List	Live List	MD5, SHA256	f_sha256, f_md5	✓
dridex_c2	Live List	IP	dst_ip	✓
mininghosts	Live List	IP	dst_ip	✓

[+ Live List](#)
[+ Range List](#)
[+ IP Range List](#)
[+ MCL](#)
[Change](#)
[Show](#)

The content management list will open:

Multiple Column List Content Management

List Contents

agent_id	th_handled	base_score	prod_name	f_md5	List	Type	Customer	Due Date	Last Update Time
10.100.26.15	abc	52	cwatch	152	MCL lists	Asset Lists	All	2037-01-01 00:...	2018-05-02 04:24:30
10.120.25.100	lpo	test	cwatch	001	MCL lists	Asset Lists	All	2037-01-01 00:...	2018-05-02 04:25:58
01	low	123	cwatch network	aer	MCL lists	Asset Lists	All	2037-01-01 00:...	2018-05-02 01:57:11

[+ Add](#)
[Edit](#)
[Delete](#)

Multiple Column List Content Table - Column Descriptions	
Column Header	Description
agent_id	Agent id of the log collector
th_handled	Status of the threat handled
base_score	Score that indicates the severity of the incident
prod_name	Name of the product
Lists	Name of list that contains values, for example: in this case, the values belong to MCL lists
Type	Values are specified based on content classification. For example: if you want to enter field values like 'agent_ip', then you can enter the content as 'IP address'
Customer	The customer for whom the live lists are created
Due Date	Date and time which the value is valid until. After the due date, the value will be automatically removed from the list.
Last Update Time	Date and time the live list was last updated.

Sorting and Filtering Options:

- Click on any table header to sort items in alphabetical/ascending/descending order
- To filter values for a specific customer, choose the customer from the 'Customer' drop-down and click 'Search'.
- To view values that belong to a specific live list, choose the list from the 'List' drop-down and click 'Search'.
- To view values that belong to a specific live list type, select the list from the 'List' drop-down, then choose the type from the 'Type' drop-down and click 'Search'.

The interface allows you to:

- **Manually add values to MCL lists**
- **Edit existing values in an MCL list**
- **Remove values from a MCL list**

To manually enter a value to a MCL list

- Click the 'Add' button at the bottom right of the 'Multiple Column List Content Management' interface.

The 'List Content Add' dialog will appear.

The screenshot shows a 'List Content Add' dialog box with the following fields and controls:

- agent_id**: Text input field.
- th_handled**: Text input field.
- base_score**: Text input field.
- prod_name**: Text input field.
- f_md5**: Text input field.
- List Management**: Two dropdown menus, one for 'MCL lists' and one for 'Asset Lists'.
- Due Date**: A date and time picker showing '2018-05-02 12:24:00'.
- Customer**: A dropdown menu showing 'All'.
- Permanent**: A checked checkbox.
- Submit**: A blue button.
- Toolbar**: A row of buttons: '+ Add' (circled in red), 'Edit', and 'Delete'.


- Select the MCL list and the list type to which the value is to be added, from the respective drop-downs under 'List Management' interface. See '**Create the Multiple Column Lists**' in '**Managing Live Lists**' for details about creating new range lists'
- Enter the values for the field defined for the MCL list in the 'agent_id', 'th_handled', 'base_score', 'prod_name' fields.
- Enter the date till which the value is valid in the 'Due Date' field.
 - You can click the calendar icon at the left of the field and choose the date. On the specified date, the value will be automatically removed from the list.
 - If you want the value to be permanently valid, select the 'Permanent' option.
- Select the customer to which the value is applicable from the 'Customer' drop-down.
- Click 'Submit'.

The value will be added to the selected list type.

- Repeat the process for adding more values to the list.

To edit a value in an MCL list

- Click the hamburger icon > 'Live Lists'
- Select an MCL list from the 'Live List' interface and click 'Show' at the bottom right. The 'Multiple Column List Contents Management' interface will open.
- Choose 'Customer' and 'Type' from their respective drop downs.
- Click 'Search' to view the values added to the list

- Select the required list from the 'List Contents' section and click . The 'List Content Edit' dialog will open

List Content Edit×

agent_id	th_handled
<input type="text" value="10.100.26.15"/>	<input type="text" value="Malware"/>
base_score	prod_name
<input type="text" value="52"/>	<input type="text" value="cwatch"/>
f_md5	
<input type="text" value="152"/>	
List Management	
<input type="text" value="MCL lists"/> ▼	<input type="text" value="Asset Lists"/> ▼
Due Date	Customer
<input type="text" value="2018-05-02 12:01:00"/>	<input type="text" value="All"/> ▼
<input checked="" type="checkbox"/> Permanent	
<input type="button" value="Submit"/>	


- Modify the required details and click 'Submit'

The dialog is similar to the 'List Content Add' dialog. See [here](#) for more details.

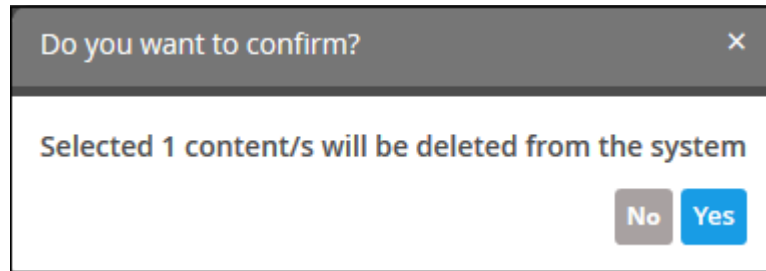
The value will be edited and will take immediate effect on the event queries and correlation rules in which the IP range list is used.

To Remove a value from a MCL list

- Click the hamburger icon > 'Live Lists'
- Select an MCL list from the 'Live List' interface and click 'Show' at the bottom right. The 'Multiple Column List Contents Management' interface will open.
- Choose 'Customer' and 'Type' from their respective drop downs and click 'Search'. The values added to the required MCL list/type will be listed.

- Select the required list from the 'List Contents' section and click . The 'List Content Edit' dialog will open

A confirmation dialog will open.



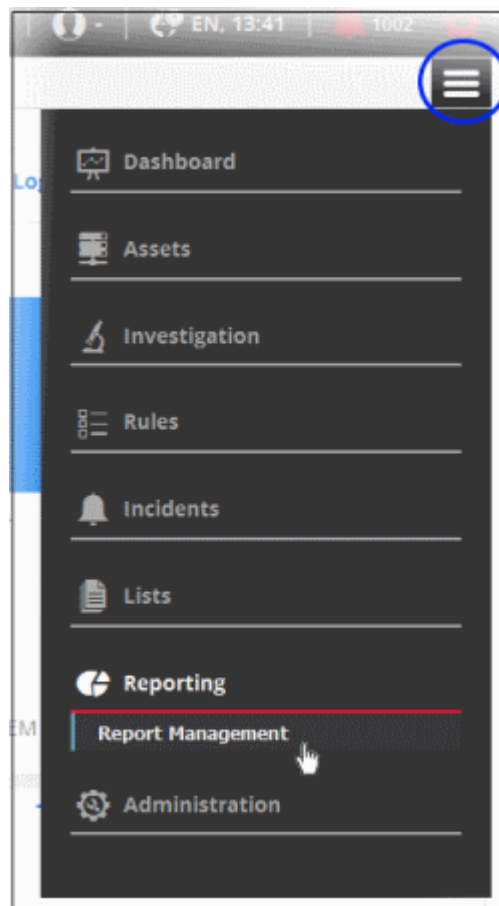
- Click 'Yes' to confirm the removal.

The value will be removed from the list. The change will take effect immediately on event queries and correlation rules which use the list.

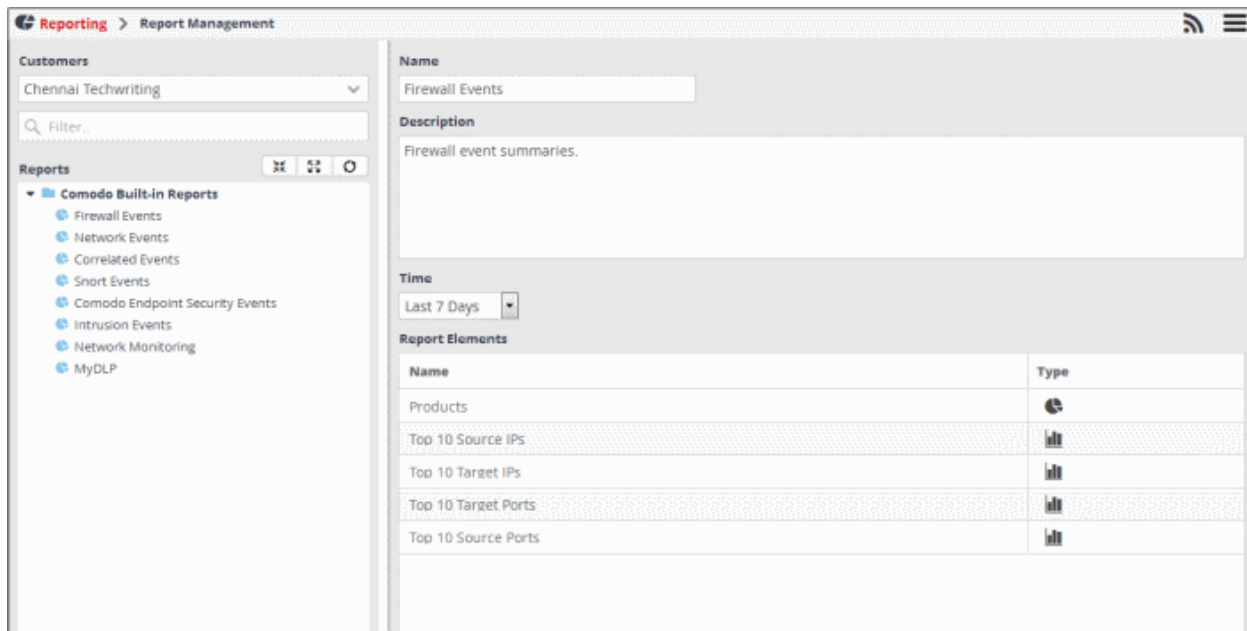
Please note that you cannot create more than 3 MCL lists in the 'Live List Management' interface

8 Manage Reports

- cWatch Network can generate event reports covering a wide range of security and productivity criteria. You can create reports on a per-customer basis.
- You can create reports for intervals from one hour to one month in the past. You can show data as tables, pie charts or bar charts.
- Data for reports is fetched from event query results. You can use pre-defined queries or custom queries. See '[Query Management](#)' for more help with this.
- To open the report interface:
 - Click the hamburger button at top right
 - Select 'Reporting' then 'Report Management':



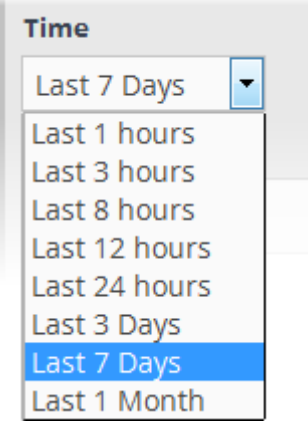
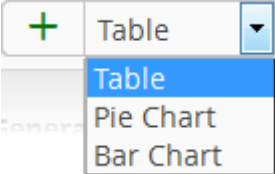






The 'Report Management' screen will open:

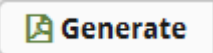
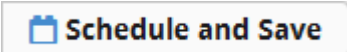


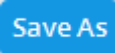


The left-hand panel shows a list of predefined reports (those in blue) and custom queries added for the selected customer. The right hand panel shows the configuration area for report generation.

Report Management Interface - Table of Controls and Fields

	<p>The 'Customers' drop-down allows you to select the customer for which you want to create or view the report(s).</p>
	<p>Expand, collapse or refresh the list of reports. To collapse, click the first button and to expand it, click the second button. Click the refresh button at the end to instantly update the rules list.</p>
	<p>Import saved report types</p>
	<p>Export reports.</p>
	<p>Add a new report category folder to the left side panel.</p>
	<p>Edit the name of a folder</p>
	<p>Add a new report type under a folder</p>
	<p>Delete selected report category folders or report types from the left hand side pane.</p>

Report Management Interface - Table of Controls and Fields	
Name	Displays the name of the report chosen from the left hand side pane. Allows you to enter the name for the report, when creating a new report.
Description	Displays a brief description of the report chosen from the left hand pane. Allows you to enter a brief description the for the report when creating a new report.
	Allows you to select the time period for report generation. Options ranges from the last hour to the entire previous month.
Report Elements	Displays a list of the contents in the report with details such as name, the event query based on which the data is populated and the type of report component (table, pie or bar chart).
	Add a report element to the selected report and choose the type of chart for the report.
	The last report can be moved to the first position
	The report can be moved to the above row
	The report can be moved to the below row
	The first report can be moved to the last position
	Edit a report element.
	Delete a report element from the list.
Generated Reports	Displays the list of reports generated so far for the selected customer, and allows you to download any report as a .pdf file.
Show Last Generated Report	Will display the most recently created report.

Report Management Interface - Table of Controls and Fields	
	Instantly generate a report according to your selected criteria.
	Automatically generate recurring reports according to a schedule of your choice.
	Save a configured report.
	Save and move your report to another folder
	Select a location in which to save the report.

The following sections explain how to:

- [Manage Report Folders](#)
- [Add and Configure Reports](#)
- [Generate a Report](#)
- [Schedule a Report](#)
- [Download/View Reports](#)
- [Edit Report Settings](#)
- [Manage Reports](#)
- [Export Event Reports](#)
- [Import Event Reports](#)


Manage Reports Folder

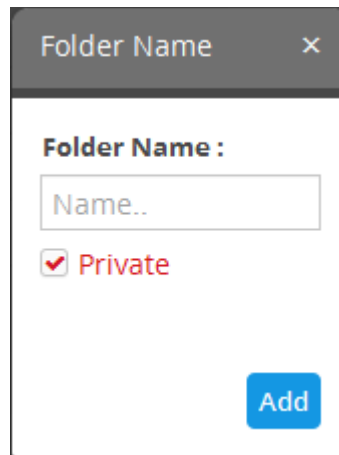
Each report folder contains a collection of reports belonging to a specific category. Every new report must be placed in a category folder.

Creating a report group folder

- Choose a customer from the 'Customers' drop-down at the top of the left panel.

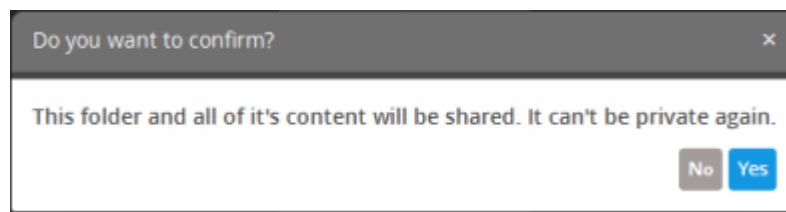
A list of predefined reports added for the customer is displayed as a tree structure in the 'Reports' pane.

- If you want to create a sub-folder, select a parent folder and click the  button. You can also create a new top level folder. The Folder Name dialog will appear.



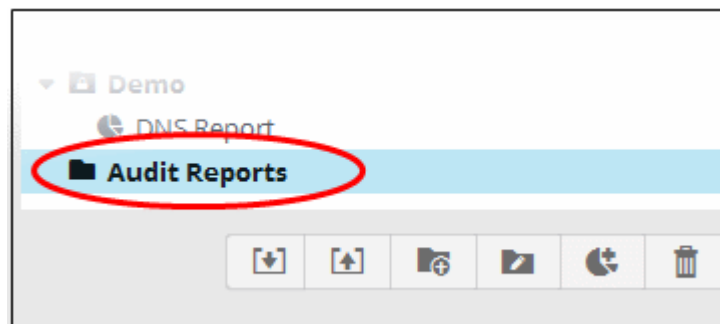
- Enter a name for the new folder in the 'Folder Name' field
- Select 'Private' if you want the folder accessible only to you. Note - this option is only available when creating a top level folder.
- Click the 'Add' button

If you did not select 'Private', a confirmation dialog will be displayed:




- Click 'Yes' to confirm

The newly created report folder will be listed. A lock icon will be displayed on the folder icon if the folder is created as a private folder.



The relevant reports can now be placed under the newly created folder. See '[Adding and Configuring a Report](#)' for more details.

Editing a reports group folder


- To edit the name of a reports group folder, select it and click the  button.

The 'Folder Name' dialog will appear.

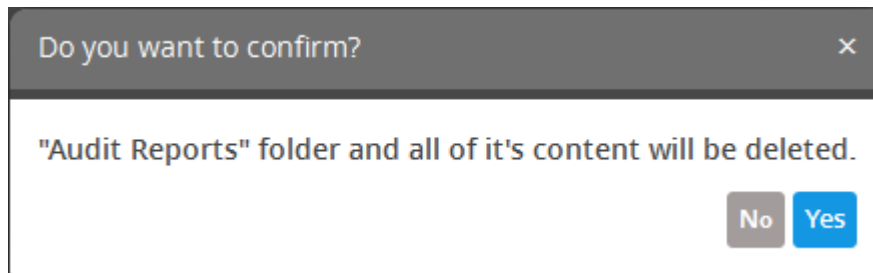
- Edit the name as required and click the 'Save' button

Please note you cannot edit built-in folder names.

Deleting a reports group folder

- To delete a reports group folder, select it and click the  button.

A confirmation dialog will appear.



- Click 'Yes' in the In the confirmation dialog. Please note all reports contained in the folder will also be deleted.


Add and Configure Reports

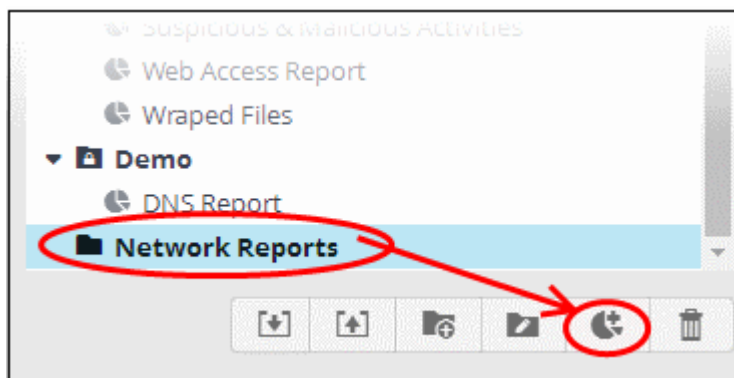
- cWatch Network ships with a set of pre-defined reports for common requests. These are listed in the 'Comodo Built-in Reports' folder in the left hand panel.
- Admins can also configure custom reports on demand for any customer.

Add a new report for a customer

- Choose a customer from the 'Customers' drop-down at the top of the left panel.

A list of predefined reports added for the customer is displayed as a tree structure in the 'Reports' pane.

- Select the appropriate folder or **create a new folder** in which you want to create a report.
- Click the  button.



The configuration screen for creating the new report will be displayed in the right hand side panel.

Name






Description

Firewall event summaries.




Time

Last 7 Days ▼


Report Elements

Name	Type
Products	
Top 10 Source IPs	
Top 10 Target IPs	
Top 10 Target Ports	
Top 10 Source Ports	

+ Table ▼

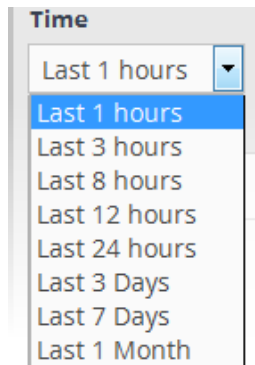




Generated Reports ○

Creation Time	File Type	Action
2018-05-02 12:58:26	pdf	

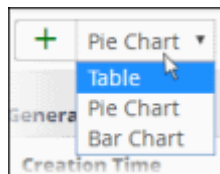
Show Last Generated Report

- Enter a name for the report in the 'Name' field
- Enter an appropriate description for the report in the 'Description' text box
- Select the period for which events are to be included from the 'Time' drop-down. Options range from the previous hour to the entire previous month.



The next step is to add the component tables/charts to be included in the report. The events for populating the tables/charts are fetched from the query results. Refer to the section '[Query Management](#)' for more details about configuring event queries.

- Select the type of report element that should be added, from the drop-down at the bottom of the 'Report Elements' area.




The options available are:

- **Table** - Table showing events that match the query selected. See [explanation on adding a table](#) given below for more details.
- **Pie Chart** - Pie-chart showing events aggregated by the parameters configured for the chart. See [explanation on adding a pie chart](#) given below for more details.
- **Bar chart** - Bar-chart showing events aggregated by the parameters configured for the chart. See [adding a bar chart](#) explanation given below for more details.

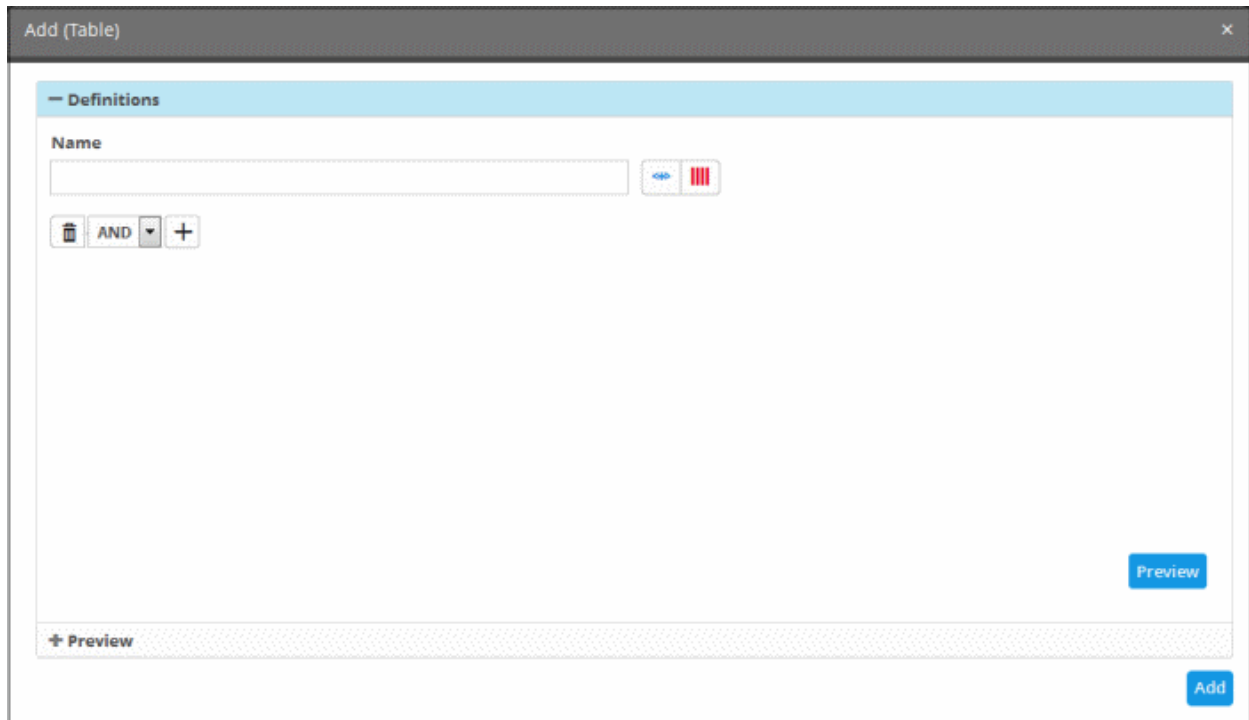
'Table' type Report Element



A 'Table' report is configured by selecting an event query from the list of queries added for the customer. The report will contain details of events that match the query in the selected time period.

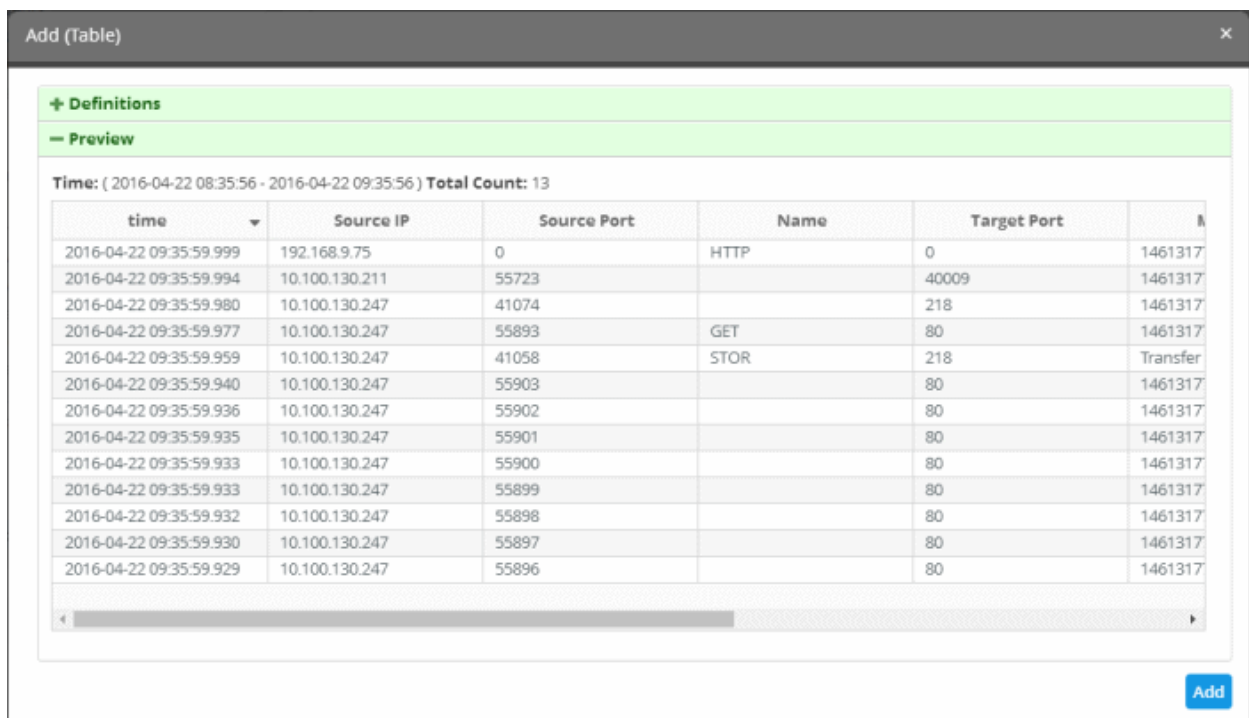
Add a Table type report

- Select 'Table' from the drop-down and click the  button beside it.

The 'Add (Table)' screen allows you to configure the event query:



- Enter a name for the report element in the 'Name' field.
- Select the event query you want to use by clicking the  button. This table is the same as **configured in the event queries**. To create a new query for generating a report, click the  button. The procedure is same as **explained in 'Configuring Event Queries'**.
- Click the 'Preview' button to view the result



- Click the 'Add' button.

The report element will be added to the report.

Time	
Last 1 Month ▾	
Report Elements	
Name	Type
Network Event - Table Report	

'Pie Chart' and 'Bar Chart' Reports

Chart type reports can be configured by specifying the following parameters:

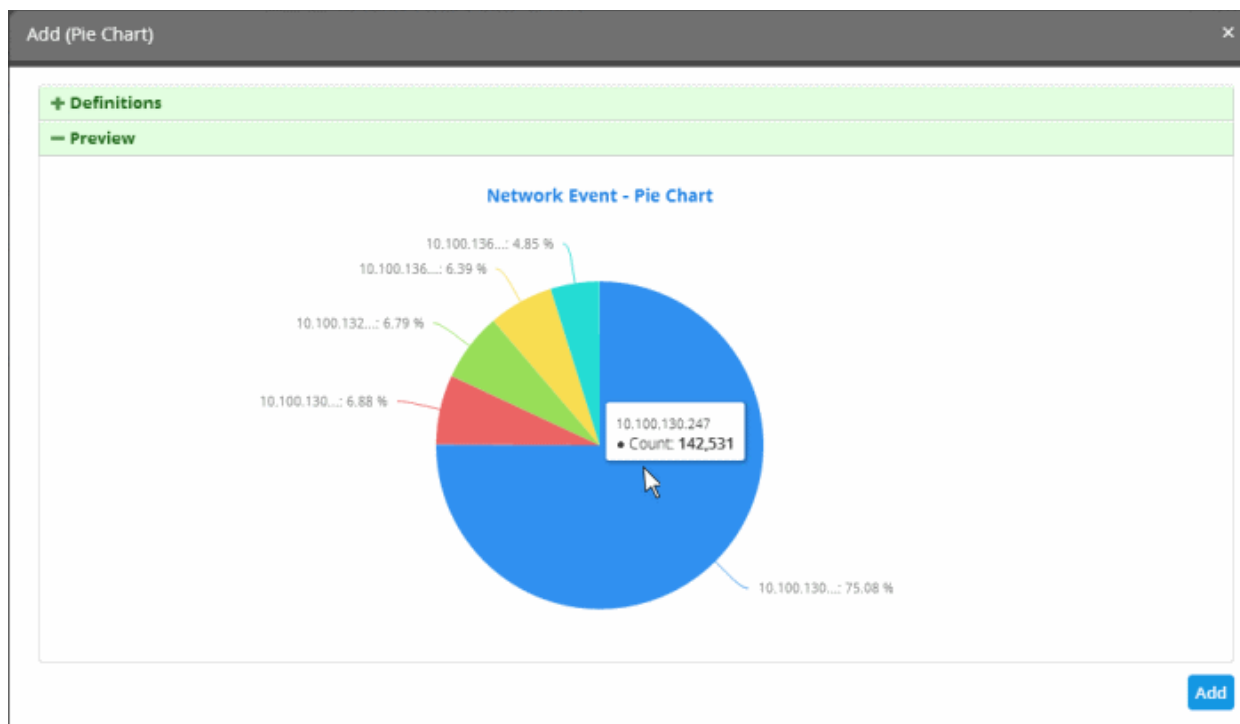
'Event Query' + 'Group By' + 'Aggregation Function' + 'Order By' + 'Limit'

- Event Query - The query whose results are to be displayed in the chart. The query can be selected from a list added for the selected customer.
- Group By - The parameter by which events identified in the query are displayed in the chart. For example, you can group events by 'Source IP'. Event groups will be formed so that each event group will have events with same value for the selected field.
- Aggregation Function - How the event groups should be ranked in the chart. Available options are:
 - *Count* - Event groups are ranked based on the number of events in each group. For example, if you choose Source IP as 'Field' then the group which contains the most events on a particular source IP will have the top rank and the group containing the lowest number of events is ranked lowest. You can further control how the data is displayed by modifying the 'Order By' and 'Limit' parameters.
 - *Sum* - Event groups are ranked based on the sum of values in another field that contains a numerical value. If you choose 'Sum', you need to select another field that contains a numerical value, like bytes in/out. The event groups are ranked based on the sum of the values in the chosen numerical field from all the events in that group. For example, if we choose 'Bytes-in' as numerical value, then the system adds up the values in the 'Bytes-in' field of all the events in a group and ranks the group accordingly. This will tell you which source IP has the most incoming traffic. The event group with the highest SUM in the 'Bytes-in' field is ranked top and vice-versa.
 - *Average* - Similar to above. Event groups are ranked based on the average of the values of the chosen numerical field from all the events in that group. (e.g. the average of values of 'Bytes_in' field of events in the group, if we take the same example as above)
 - *Minimum* - Similar to above. The event groups are ranked based on the minimum of the values of chosen numerical field from all the events in that group.
 - *Maximum* - Similar to above. The event groups are ranked based on the maximum of the values of chosen numerical field from all the events in that group.
- Order By - Choose whether results are shown in ascending or descending order. Available options are:
 - Ascending - The group with the lowest rank will be top of the list. A limit of 5 will show the 5 groups with the lowest ranks.
 - Descending - The group with the highest rank will be top of the list.. A limit of 5 will show the 5 groups with the highest ranks.
- Limit - The number of event groups to be displayed in the chart

Example:

The following screenshot shows the preview of resulting pie chart from the following configuration parameters:

'Network Events' + 'Source IP' + 'Count' + 'Descending' + '5'

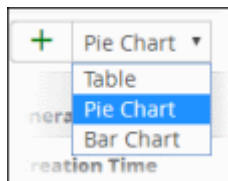


The following sections explain on:




- **Adding a pie chart**
- **Adding a bar chart**

To add a Pie Chart type report

- Select 'Pie Chart' from the drop-down and click the  button beside it



The 'Add (Table)' screen will be displayed for configuring the event query whose report is to be shown as pie chart.

Add (Pie Chart) - Form Parameters	
Parameter	Description
Name	Enter an appropriate name for the report element
	Displays the list of predefined and custom event queries added for the selected customer. Select the event query for which the results are to be displayed in the chart.
	Allows you to configure the 'Results' table for the new query. See ' Configure results table for a query ' for more details.
	Allows you to configure a new event query
Group By	The drop-down displays the fields, configured as event query results table column headers for the selected event query. See ' Configure results table for a query ' for more details. Select the field based on whose values, the events identified by the query are to be grouped and shown in the chart.
Aggregation Function	Allows you to choose the aggregation operation to be applied for ranking the event groups and show them in ascending or descending order, in the chart. The options available are: <ul style="list-style-type: none"> Count - The event groups are ranked based on the number of events in each group. For example, if you choose Source IP as 'Field' then the group which contains the most events on a particular source IP will have the top rank and the group containing the lowest number of events is ranked lowest. You can further control how the data is displayed by modifying the 'Order By' and 'Limit' parameters. Sum - The event groups are ranked based on sum of values in another field that contains numerical value. If you choose 'Sum', you need to select another field that contains a numerical value, like bytes in/out. The event groups are ranked based on the sum of the values in the chosen numerical field from all the events in that

	<p>group. For example, if we choose 'Bytes-in' as numerical value, then the system adds up the values in the 'Bytes-in' field of all the events in a group and ranks the group accordingly. This will tell you which source IP has the most incoming traffic. The event group with the highest SUM in the 'Bytes-in' field is ranked top and vice-versa.</p> <ul style="list-style-type: none"> • Average - Similar to above. Event groups are ranked based on the average of the values of the chosen numerical field from all the events in that group. (e.g. the average of values of 'Bytes_in' field of events in the group, if we take the same example as above) • Minimum - Similar to above. The event groups are ranked based on the minimum of the values of chosen numerical field from all the events in that group. • Maximum - Similar to above. The event groups are ranked based on the maximum of the values of chosen numerical field from all the events in that group.
Order By	<p>Allows you to choose the order in which the event groups are to be indicated in the chart, based on their ranking. The available options are:</p> <ul style="list-style-type: none"> • Ascending - The group with the lowest rank will be top of the list. A limit of 5 will show the 5 groups with the lowest ranks. • Descending - The group with the highest rank will be top of the list.. A limit of 5 will show the 5 groups with the highest ranks.
Limit	Enter the number of events to be displayed for the chart
Preview	This button allows to preview the chart before adding it to the report.
Add	Click this button to add the chart to the report

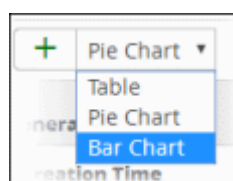
- Enter the parameters for the chart as shown in the table above and click the 'Preview' button to check the chart before adding it to the report.
- Click the 'Add' button

The configured report element will be added to the list.



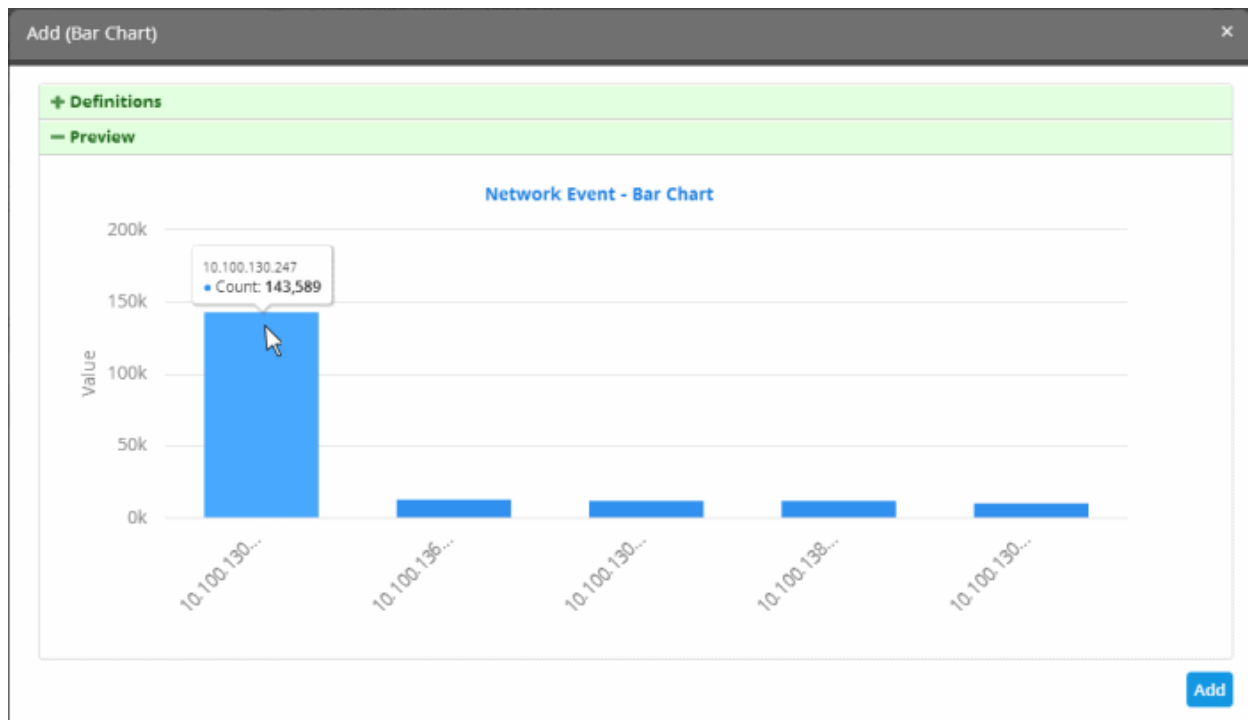
To add 'Bar Chart' type report element

- Select 'Bar Chart' from the drop-down and click the  button beside it.



The procedure is same as **adding a pie chart report element** explained above.

- Enter the parameters for the chart as shown in the table above and click the 'Preview' button to check the chart before adding it to the report.



- Click the 'Add' button

The configured report element will be added to the list.

Time	
Last 1 Month ▾	
Report Elements	
Name	Type
Network Event - Table Report	
Network Events - Pie Chart	
Network Event - Bar Chart	

The 'Report Elements' area displays the list of report components added to the report.

- **Name** - Displays the name of the report element
- **Type** - Indicates the type of report element, whether table, pie or bar chart.

You can add as many report elements as required for a report.

- Click the 'Save' button to save all the report elements.
- You can save the report to another folder by selecting it and then clicking the 'Save As' button.

Now that you have configured a report, you can **generate the report** and/or **schedule the report generation**.

Generate a Report

After configuring a report, you can generate it manually or specify the **automatic generation of the report** according to a schedule of your choice.

To manually generate a report

- Choose the customer from the 'Customers' drop-down at the top of the left panel.

A list of predefined and custom reports added for the customer is displayed as a tree structure in the 'Reports' pane.

- Select the report from the list.

The details of the report with the list of report elements will be displayed in the configuration area at the right.

The 'Generated Reports' area displays a list of reports generated manually or as per the schedule created for the report.

- **Creation Time** - The date and time the report was generated.
- **File Type** - Currently only PDF format is available for reports. Future releases will support RTF files also.
- **Action** - Allows to delete the generated report.
- To generate the report instantly, click the 'Generate' button.

The report generation will be started and on completion, it will be added to the list under 'Generated Reports' and its time stamp will be added to the 'Creation Time' column.

- To download the report, clicking the time stamp under the 'Creation Time' column.
- To view the report instantly select the 'Show Last Generated Report' check box.

See '[Download / View a Report](#)' for more details about how to download and /or view a report.

Schedule a Report

You can automate the process of report generation according to a schedule of your choice. If required, you can cancel a schedule later on.

To schedule a report generation

- Choose the customer from the 'Customers' drop-down at the top of the left panel.

A list of predefined and custom reports added for the customer is displayed as a tree structure in the 'Reports' pane.

- Select the report from the list.

The details of the report with the list of report elements will be displayed in the configuration area at the right.

- Click the 'Schedule' button at the bottom of the 'Generated Reports' area.

The 'Schedule Report' dialog will be displayed.

If the report is already scheduled, the 'Unschedule and Save' button will be in enabled status. You can remove the schedule by clicking the 'Unschedule and Save' button.

- To schedule report generation, select the parameters from the 'Date' and 'Occurs' fields
 - Date - Allows to select the start date and time of report generation

- Select the start date from the calendar

- Select the start time from the timing section
- To configure the frequency of report generation from the start date, select the parameter from the 'Occurs' field. The options available are:
 - Hourly
 - Daily
 - Weekly
 - Monthly
- Click the 'Schedule and Save' button after selecting the start date and frequency of report generation

A confirmation message will be displayed at the top right side of the screen. The reports will be automatically generated as per the schedule for the period selected under 'Time' drop-down and added to the list under 'Generated Reports' and represented by time stamps under the 'Creation Time' column. You can download required report(s) by clicking the respective time stamp.

Download / View Reports

The 'Generated Reports' area in the 'Report Management' interface allows you to download and / or view any generated report.

To download / view a report

- Choose the customer from the 'Customers' drop-down at the top of the left panel.

A list of predefined and custom reports added for the customer is displayed as a tree structure in the 'Reports' pane.

- Select the report from the list.

The details of the report with the list of report elements will be displayed in the configuration area at the right.

The screenshot displays the 'Reporting > Report Management' interface. On the left, the 'Customers' dropdown is set to 'Comodo Ank'. Below it, the 'Reports' tree structure is visible, with 'Network Event Report' selected and circled in red. A red arrow points from this selection to the main configuration area on the right.

The main configuration area shows the following details for the 'Network Event Report':

- Name:** Network Event Report
- Description:** To generate network event reports
- Time:** Last 7 Days
- Report Elements:**

Name	Type
Network Event - Table Report	
Network Events - Pie Chart	
Network Events - Bar Chart	
- Generated Reports:**

Creation Time	File Type	Action
2016-04-25 08:43:27	pdf	

At the bottom of the configuration area, there are buttons for 'Generate', 'Schedule and Save', 'Save', 'Move', and 'Save As'. A checkbox for 'Show Last Generated Report' is also present.

The 'Generated Reports' area displays a list of reports generated manually or as per the schedule created for the report.

- Click the time stamp in the 'Creation Time' column to download the report as a .pdf.
- 'Show Last Generated Report' - view the most recently created report.

The report will be displayed in the 'Last Generated Report' area, below 'Generated Reports' area.

Edit Report Settings

You can change the name, description, report elements and their configuration at any time from the Report management interface.

To edit a report

- Choose the customer from the 'Customers' drop-down at the top of the left panel.

A list of predefined and custom reports added for the customer is displayed as a tree structure in the 'Reports' pane.

- Select the report from the list.

The details of the report with the list of report elements will be displayed in the configuration area at the right.

The screenshot displays the 'Report Management' interface. On the left, the 'Reports' pane shows a tree structure. The 'Network Reports' folder is expanded, and 'Network Event Report' is selected and circled in red. A red arrow points from this selection to the configuration area on the right. The configuration area shows the following details:

- Name:** Network Event Report
- Description:** To generate network event reports
- Time:** Last 7 Days
- Report Elements:**

Name	Type
Network Event - Table Report	
Network Events - Pie Chart	
Network Events - Bar Chart	
- Generated Reports:**

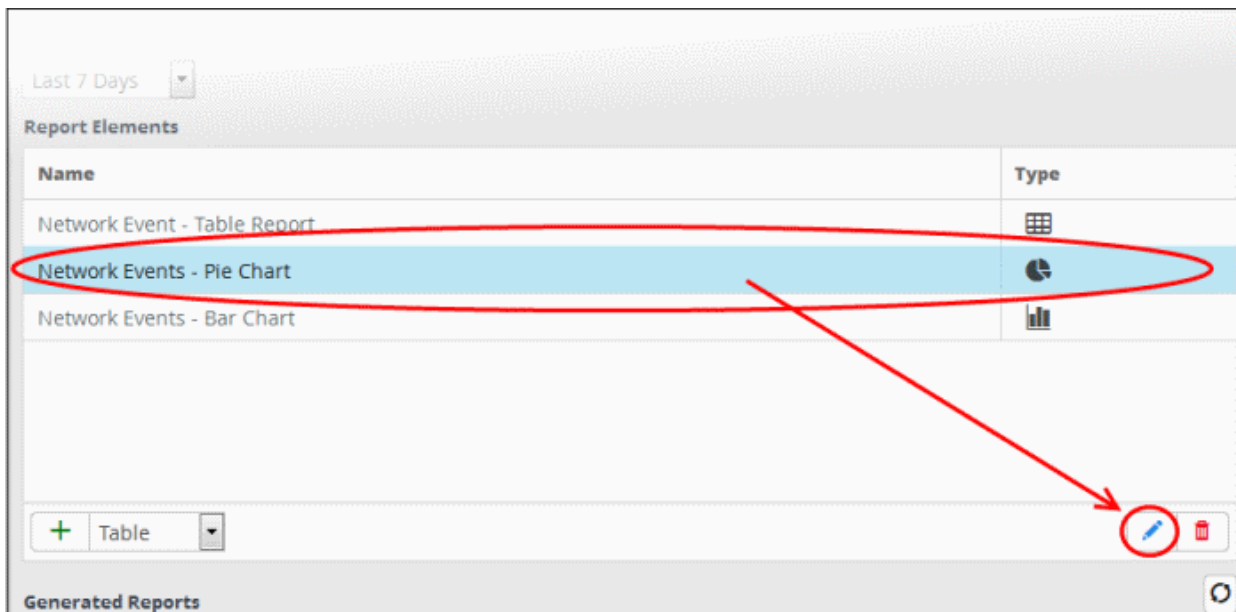
Creation Time	File Type	Action
2016-04-25 08:43:27	pdf	

At the bottom of the configuration area, there are buttons for 'Generate', 'Schedule and Save', 'Save', 'More', and 'Save As'.

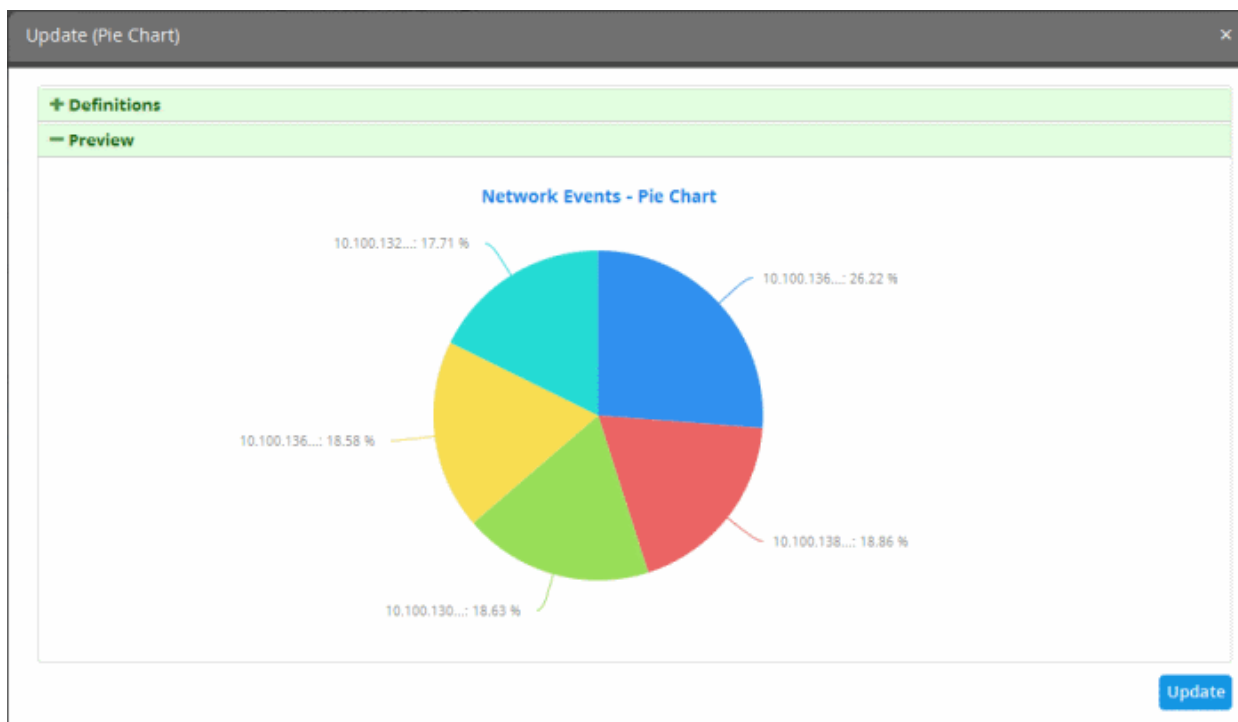
- Edit the name and description as required and click the 'Save' button at the bottom.

To edit the details of a report element

- Select the report element from the list that you want to edit and click the edit button at the bottom.



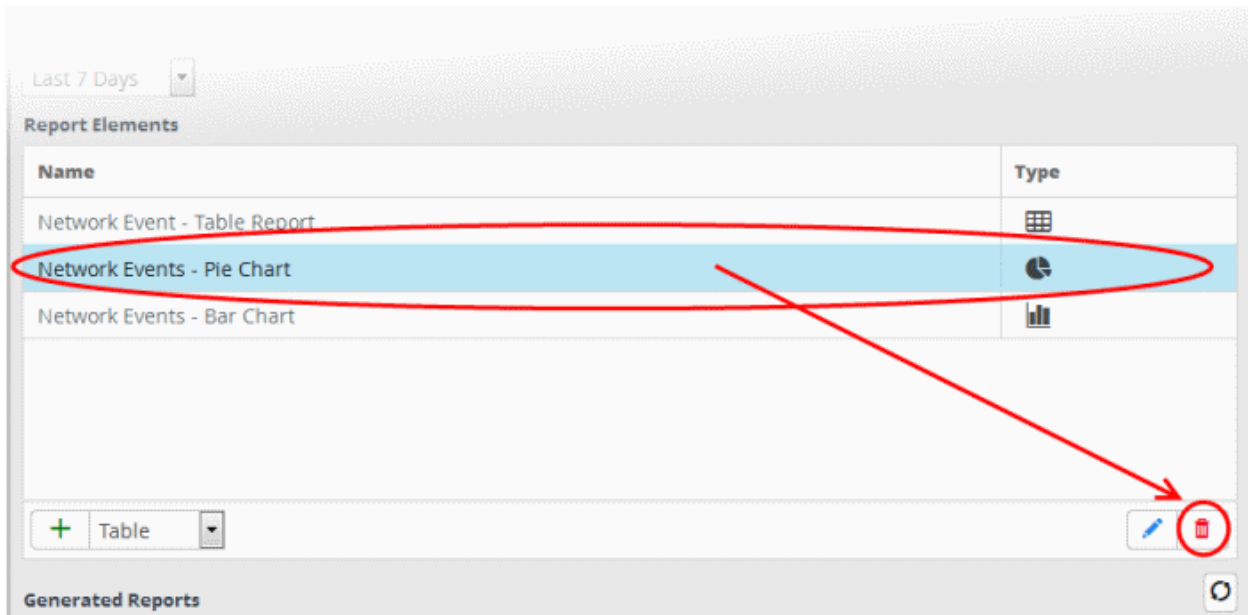
The 'Update' screen for the selected report element will be displayed.



- Edit the details of the report element as required. The procedure is similar to **adding a report element** as explained above.
- Click the 'Update' button.
- Click the 'Save' button at the bottom.

To delete a report element

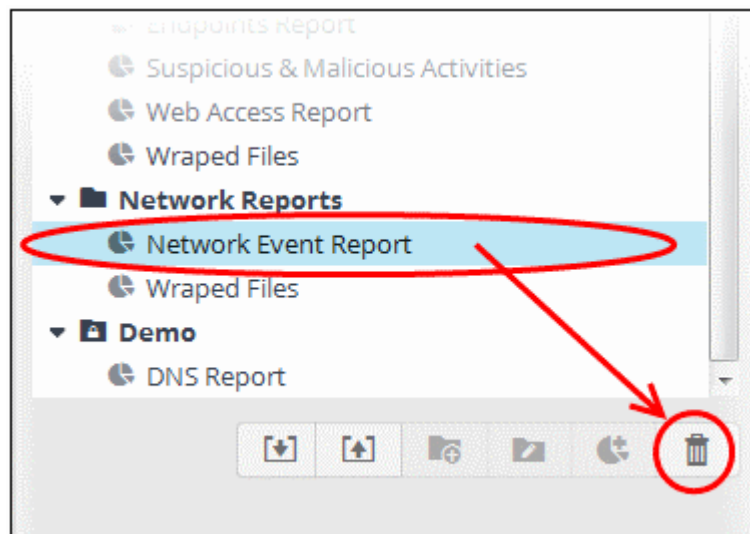
- Select the report the element and click the delete button at the bottom



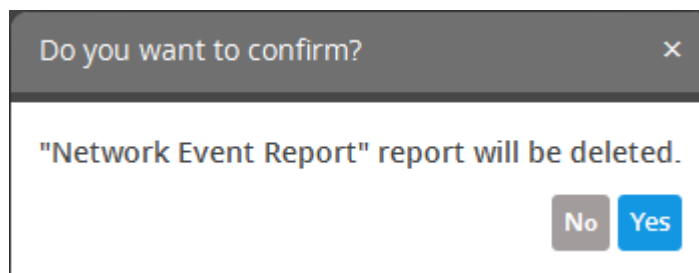
The report element will be deleted.

To delete a report

- Select the report on the left side and click the delete button at the bottom.



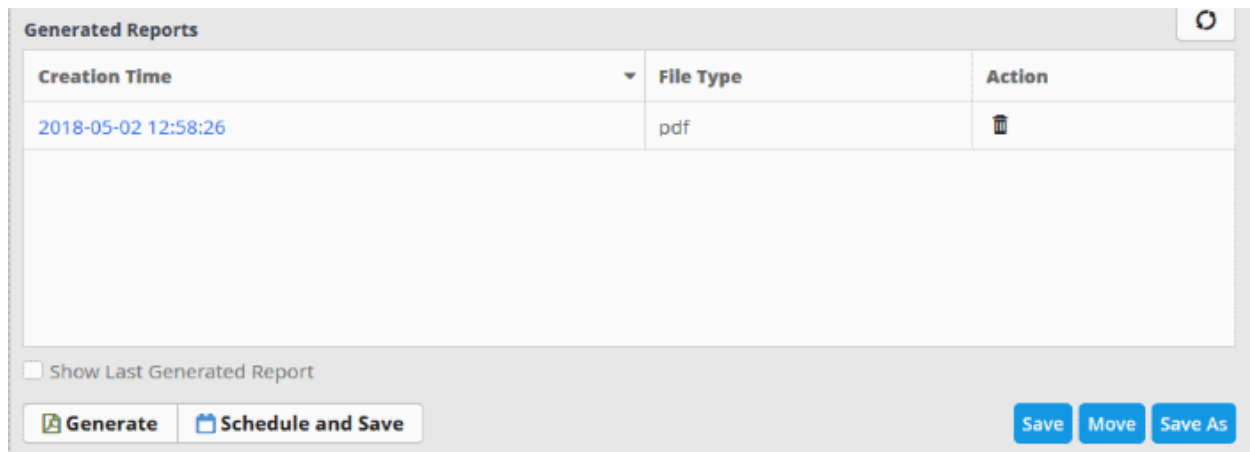
In the confirmation dialog, click the 'Yes' button to remove the report.



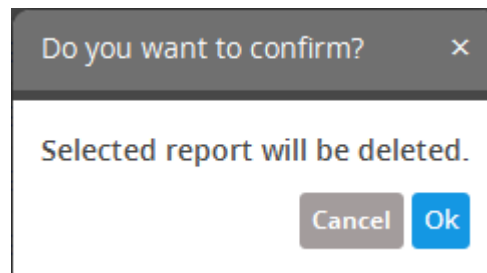
The report and all the report elements under it will be deleted.

Manage Reports

The 'Generated Reports' area displays a list of reports for the report selected on the left.



- To sort the report list according to date, click anywhere on the 'Creation Time' column header.
- To refresh the list, click the button on the right.
- Enable 'Show Last Generated Report' to view the most recently generated report. To close the report, clear the selection.
- To delete a report, click the trash can icon in the 'Action' column



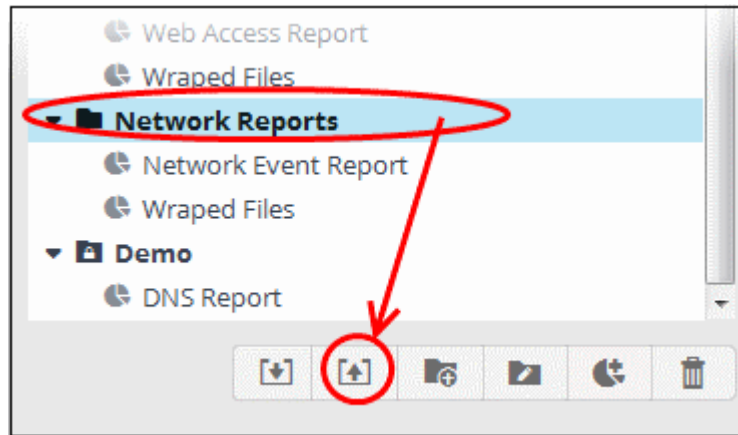
- Click 'Ok' to confirm the deletion of the report.

Export Event Reports

- cWatch Network allows you to save report queries in order to use them for other customers.
- Imported queries can be used 'as is' or altered to suit the requirements of the customer.
- You can export a query folder or a particular query. Please note - exported event queries can only be imported to their respective sections.
- For example, event queries exported from the reports section can only be used in the report section. Also the values in the filter items in the exported events for tagged and list events will be set to default values.

To export a report query or report folder

- Select a customer from the 'Customers' drop-down at the top of the left panel.
- Choose the report or report folder to be exported from the 'Reports' list on the left.
- Click the 'Export' button at the bottom



The 'Opening exported' dialog will open.

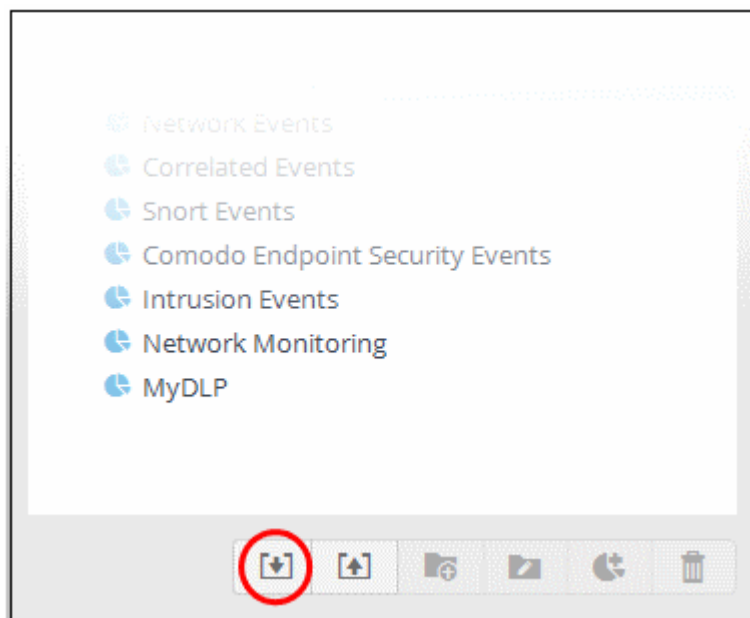
- This varies by browser. For some browsers, the file with extension 'nxm' will be automatically downloaded to the default download location.
- The saved query can be imported for use with another customer account.

Import Event Reports

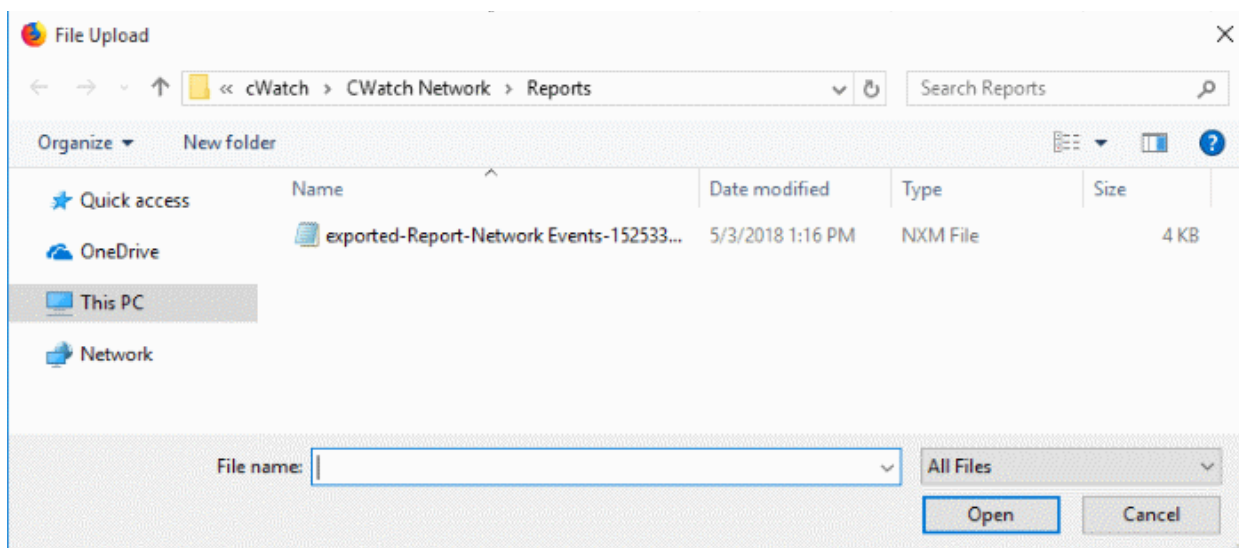
Administrators can import saved report queries for use with other customers. Imported queries can be used 'as is' or altered to suit the requirements of the customer. Please note that only exported queries from the report section should be imported for use here.

To import a query or query folder

- Select the customer from the 'Customers' drop-down (top of the left panel) for which you want to import the saved queries
- Click 'Import' at the bottom

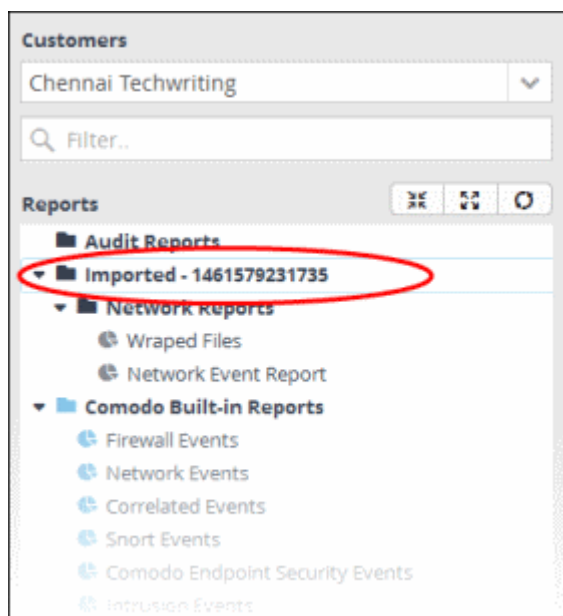


- Navigate to the location where the report query file is saved.



- Select the file and click 'Open'

The report or report folder will be imported and will be listed under 'Imported' folder.



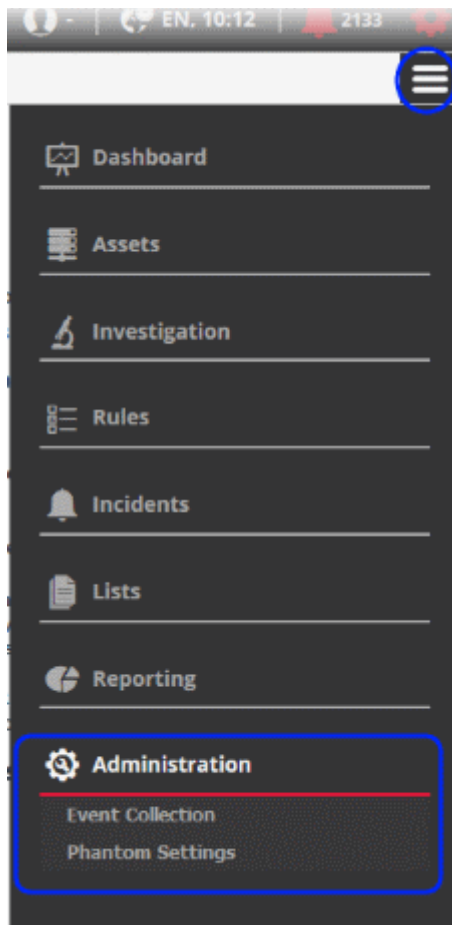
You can generate report as it is or **alter** according to your requirement.

9 Administration

The 'Administration' interface explains how to configure Syslog, Nxlog and network sensors. The section also explains how to add users and view license details from your Comodo One / Comodo Dragon /ITarian account.

The administration menu entry is only visible to people with admin privileges.

- Click the menu button at top-right and choose 'Administration':



See the following for more details:

- [Event Collection](#)
- [Phantom Settings](#)
- [Manage Users](#)
- [View License and Subscription Details](#)

9.1 Event Collection

- cWatch Network features agent-less log collection from Windows/Linux endpoints using the Nxlog and Rsyslog utilities.
- The NXLOG utility (for Windows) and the RSYSLOG utility (for Linux) need to be configured to send logs to the cWatch Network server.
- cWatch also provides pre-configured scripts for Nxlog and Rsyslog which will automatically send logs to cWatch.

Scripts can be configured and deployed in two ways:

- **Pre-configured script files** - The administrator can download ready-made configuration script files with all parameters pre-configured for a specific customer/network from the 'Hard Assets' interface. This is the most convenient way of configuring NXLOG and RSYSLOG utilities at the endpoints to send logs to the cWatch network server. See [Configuring Nxlog and Rsyslog to Send Logs to cWatch Network Server](#) for more detailed explanations about downloading the script files and deploying them.
- **Manually configure RSYSLOG/NXLOG scripts** - Administrators can download configuration scripts for RSYSLOG and NxLOG and manually set the parameters such as network authentication token, name of product from which the logs are to be collected and so on. These scripts can be used to configure RSYSLOG and NxLOG utilities at Linux and Windows based endpoints to send logs to the cWatch network server.

To download the manual configuration script for RSYSLOG and NxLOG

- Click the 'Menu' button from the top right, choose 'Administration' and then click 'Event Collection'

The screenshot shows the 'Administration > Event Collection' page. It features two main sections for user manuals:

- Rsyslog Log Collection User Manual:**
 - Text: "RSYSLOG can deliver over one million messages per second to local destinations when limited processing is applied. Rsyslog Log Collection uses RSYSLOG for collecting log messages on client side. You can configure rsyslog on linux machines in order to send log to Rsyslog Log Collector. It receives local system logs on linux machines using tcp and udp server."
 - How to Configure Client Machine:** "We create a script file to configure linux rsyslog daemon. Script file gets some parameters for configuration."
 - Configuration Parameters:**
 - i : install
 - r : remove
 - h : help or usage
 - AGENTLESS_AUTH_TOKEN: Agentless authentication key (Available in MSSP Portal)
 - PRODUCT_NAME: Product name which is sending log (Apache, Snort ,Fortigate 5.0)
 - PRODUCT_VERSION: Product parser version which is sending log (Apache, Snort ,Fortigate 5.0)
 - Usage:** `./configure-linux [-i AGENTLESS_AUTH_TOKEN PRODUCT_NAME PRODUCT_VERSION]`
 - Sample:** `./configure-syslog.sh -i "ec42f0e5608048a19e7f0e229b1d609d" "Fortigate5.0" "v1.0"`
 - Note: "Please don't use whitespace characters in Product Name parameter. When you run this script you will see 22-comodo.conf file under /etc/rsyslog.d directory. Default configuration sends messages with TCP protocol. If you want to configure as UDP use one '@' character before agentless log collector ip. Restart rsyslog service and start using it."
 - For TCP: `*.* @IP Adress:Port:ComodoFormat`
 - Download button: `configure.syslog.sh`
- NxLog Configuration User Manual:**
 - Text: "This guide shows you how to configure your NxLog configuration file in order to send your Windows Event Log"
 - How to Configure Client Machine:**
 1. Download `nxlog.conf`.
 2. Replace downloaded `nxlog.conf` file with the file -> C:\Program Files (x86)\nxlog\conf\nxlog.conf
 3. Open the `nxlog.conf` file to edit
 4. If you have a customer defined, click on the navigation menu and navigate to Assets -> Asset Management and see customer list. If not, add a customer for your mssp.
 5. Within the same menu, click on a customer and click manage to see the network token provided, copy the token.
 6. In `nxlog.conf` file, replace `$$TOKEN$$` with the network token.
 7. Save and close the file.
 8. Open the Services tool from Start Menu on your Windows machine and restart the nxlog service.
 - Download button: `nxlog.conf`

The 'Event Collection' page contains instructions about downloading the scripts, setting the parameters and configuring the RSYSLOG/NxLOG utilities using the scripts.

In addition to event collection, cWatch Network is capable of collecting log information from Comodo Network Monitoring Sensors. These sensors listens on the customer's network using span/tap technologies and can be configured according to customer requirements. The deployment of sensors has to planned according to customers network topology and can be done in coordination with Comodo. Please contact your account manager at Comodo for the deployment of sensors on your network.

9.2 Phantom Settings

- Phantom is a security operations platform that helps customers streamline workflows to improve efficiency and precision. The Phantom settings area lets you integrate cWatch with your Phantom account. cWatch can then pass cWatch incidents and event information to Phantom.

To open the 'Phantom Settings' interface

- Click the 'Hamburger' icon > 'Administration' > 'Phantom Settings'

Name	Authentication Token	Server	Severity	Sensitivity	Tags	Expire In Hours
Sample Phan...	ZYrAqDjexk2Bj3acmPDj5MY5HH4sq2egkUAU...	https://52.41....	Low	White	cWatch, in...	36
Phantom CW...	ZYrAqDjexk2Bj3acmPDj5MY5HH4sq2egkUAU...	https://52.41....	Medium	Amber	CWatch, l...	24

Phantom Settings - Table of Column Descriptions

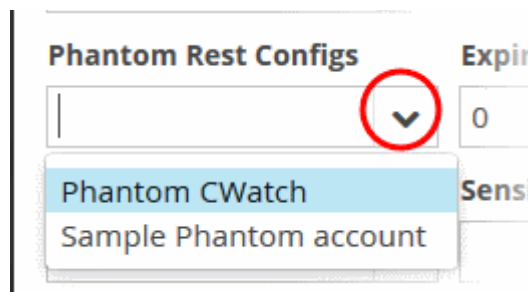
Column Header	Description
Name	Name of your phantom account
Authentication Token	Unique key generated to authenticate your Phantom account to cWatch
Server	Enter phantom server details
Severity	Select the severity level of incidents that are being pushed to phantom account <ul style="list-style-type: none"> Low Medium High Dynamic
Sensitivity	Color coded indicator for the incident. You configure the sensitivity in the ' Incident Category Management ' interface
Tags	Enter keywords which describe the Phantom account's purpose
Expires in hours	The length of time remaining on the current session.

To assign 'Phantom Action', to an incident:

- Click the 'Hamburger' icon > Incidents > Category Action Management
- Click 'Add'

The 'Add Category Action' dialog will open

- Select the incident status from the 'Status' drop-down
- Select 'Phantom Action' from the 'Type' drop-down
- Choose the phantom account you want your incident to be pushed to from the 'Phantom Rest Configs' drop-down



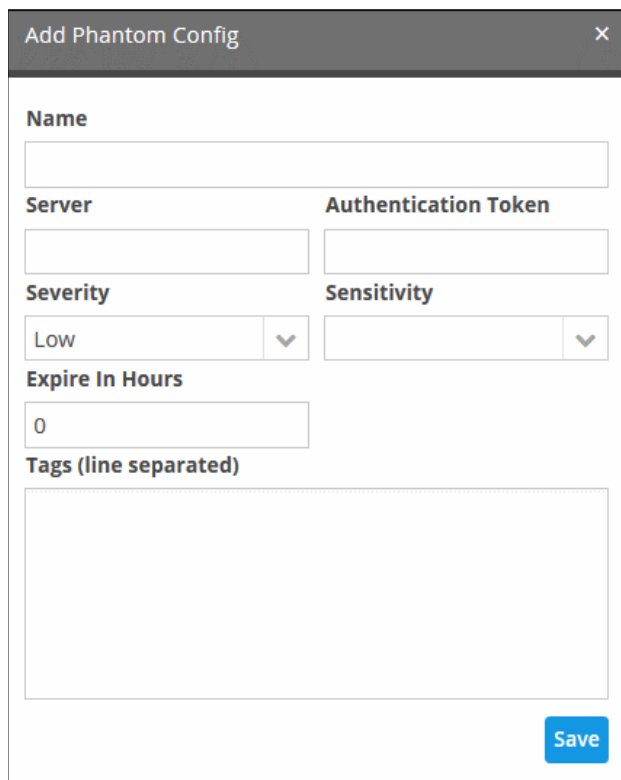
The phantom settings configured will populate based on the account you select. See [Category Action Management](#) for more details

The 'Phantom Settings' screen will open. Please see below links to learn more:

- [Add phantom account](#)
- [Edit phantom account](#)
- [Delete phantom account](#)

Add phantom account

- Click the 'Hamburger' icon > 'Administration' > 'Phantom Settings'
- Click 'Add' on the bottom right of the interface. The 'Add Phantom Config' interface will open



Add Phantom Config [X]

Name

Server **Authentication Token**

Severity **Sensitivity**

Expire In Hours

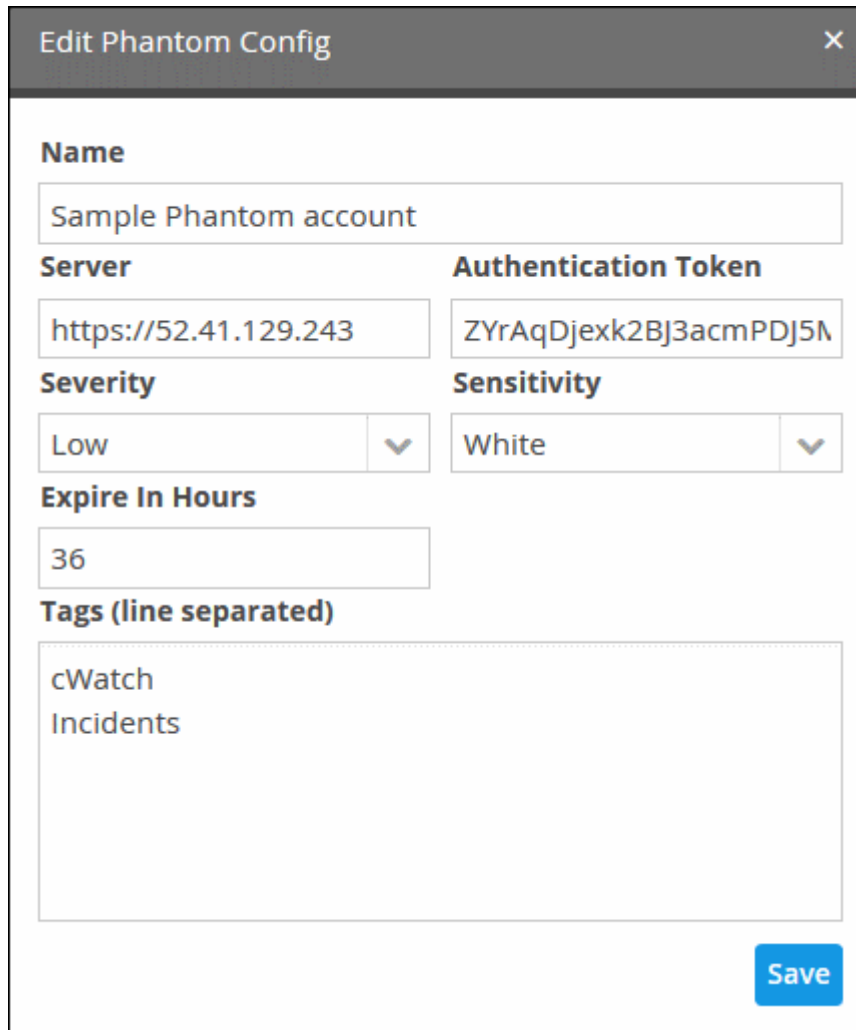
Tags (line separated)

Save

- Enter the required fields and click 'Save'
- The Phantom account will be added and you can view the details listed in the 'Phantom Settings' interface
- If you want to add a phantom action for an incident, select 'Phantom action' in actions field. See **Category Action Management** for more details.

Edit phantom account

- Click the 'Hamburger' icon > 'Administration' > 'Phantom Settings'
- Select the phantom account that you want to edit and click the 'Edit' button on the bottom right of the interface. The 'Edit Phantom Config' interface will open



Edit Phantom Config [X]

Name
Sample Phantom account

Server **Authentication Token**
https://52.41.129.243 ZYrAqDjexk2BJ3acmPDJ5M

Severity **Sensitivity**
Low [v] White [v]

Expire In Hours
36

Tags (line separated)
cWatch
Incidents

Save

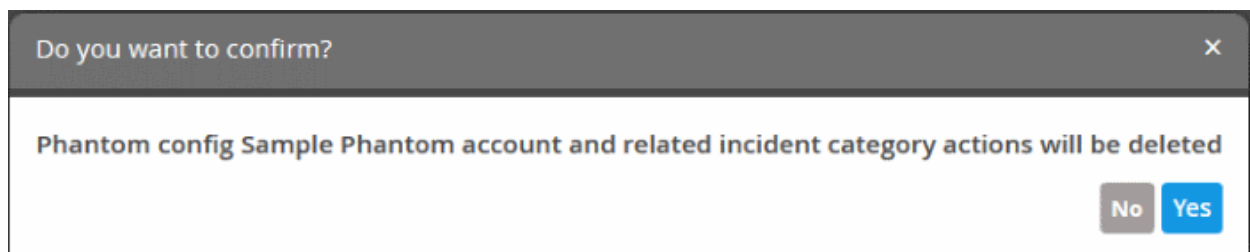
- Modify the required fields and click 'Save'

The modified account will be saved

Delete phantom account

- Click the 'Hamburger' icon > 'Administration' > 'Phantom Settings'
- Select the phantom account that you want to delete and click the 'Delete' button on the bottom right of the interface.

A confirmation dialog will open



Do you want to confirm? [X]

Phantom config Sample Phantom account and related incident category actions will be deleted

No **Yes**

- Click 'Yes' to remove the phantom account

Please note that the incident that are integrated with the account will also be removed.

9.3 Manage Users

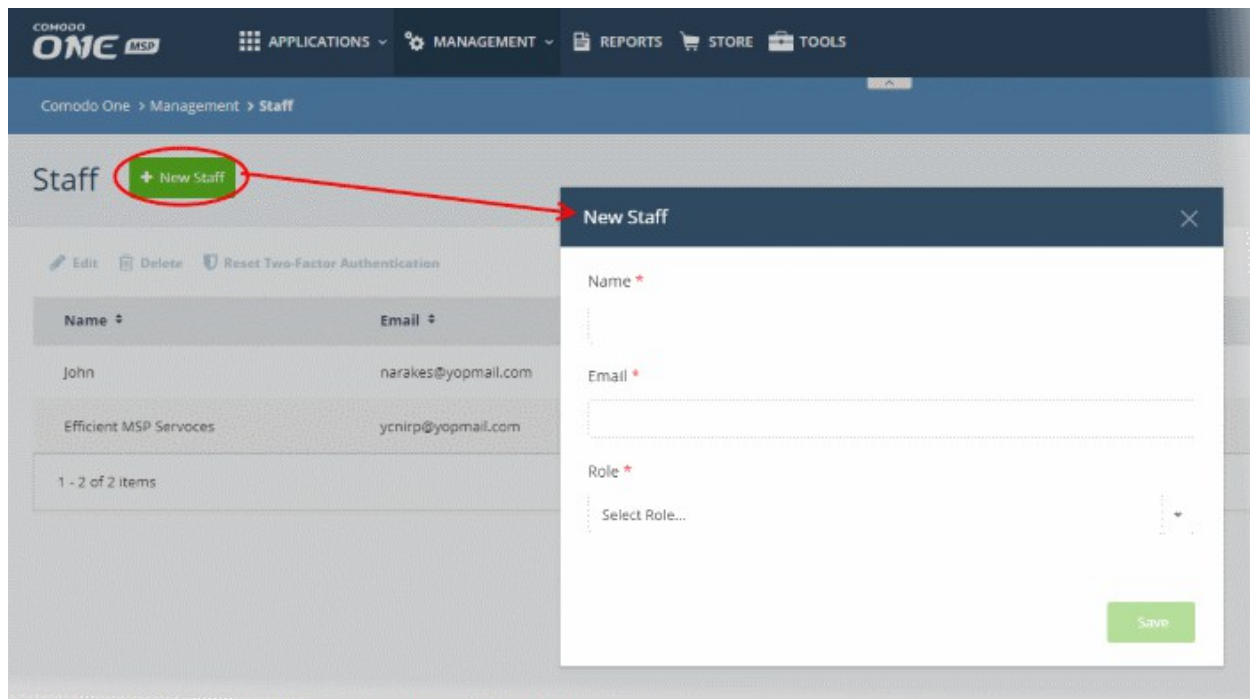
- Users are assigned to customers to address incidents and malicious events on customer networks.
- Users can only access the dashboards, events and incidents related to the customers assigned to them.
- 'Correlated Incidents' belonging to a customer are auto-routed to the user assigned to the customer. See **'Manage Incidents'** for more details.
- Add users (Staff) from your **Comodo One / Comodo Dragon / ITarian** MSP account

The following sections explain more about:

- **Adding users**
- **Editing user details**
- **Removing users**

Add a user

- Login to your **Comodo One / Comodo Dragon / ITarian** MSP account
- Click 'Management' then 'Staff'

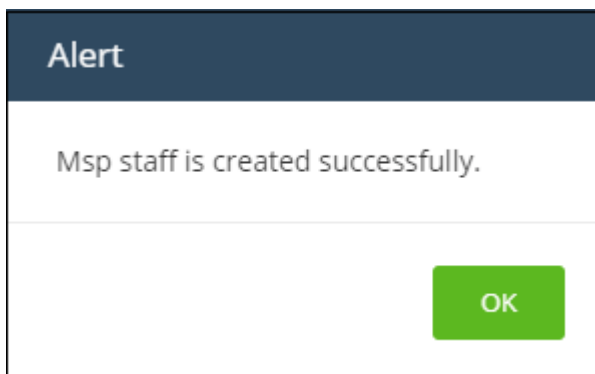


- Click 'New Staff' at top-left

Complete the 'New Staff' form:

- Name – The full name of the user (staff)
- Email – The email address of the staff member. This also acts as the staff member's username.
 - The account activation email is sent to this email address
 - Staff must click the activation link in the mail then create a password
 - The staff can login to Comodo One / Comodo Dragon / ITarian after completing the step above.
- Role – Select appropriate privileges for the staff. Note – Make sure the role has permission to access the cWatch application. See help page to know more how to manage roles in **C1 / Comodo Dragon / ITarian**
- Click 'Save'

A confirmation message will appear:

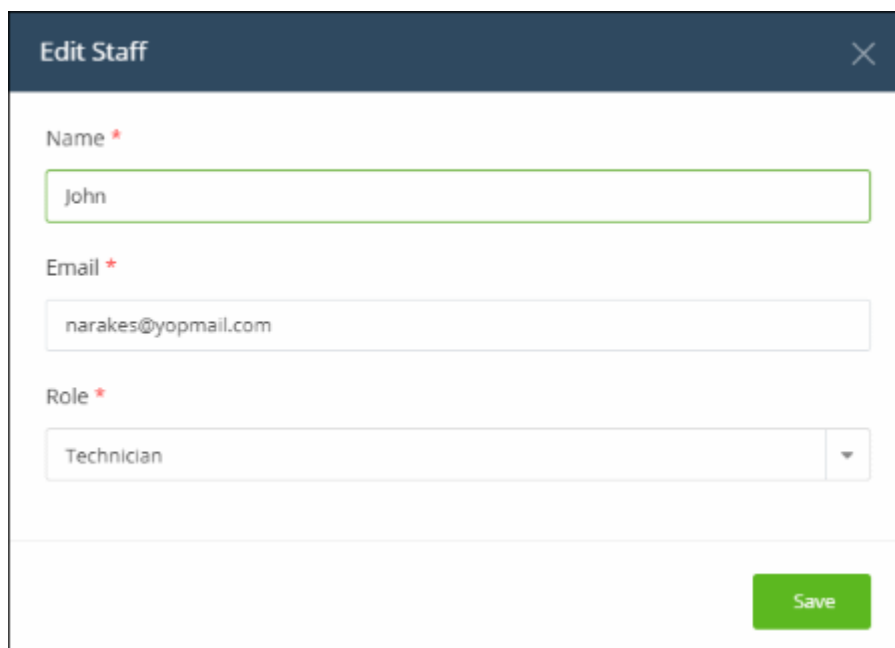


Once the user has validated his / her account from the activation email, he / she can login to their **Comodo One / Comodo Dragon / ITarian** account.

- To access cWatch, click 'Applications' then 'cWatch'

To edit the details of a user

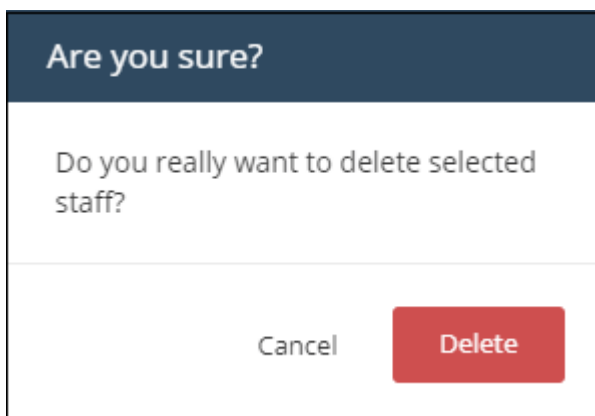
- Login to your **Comodo One / Comodo Dragon / ITarian** MSP account
- Click 'Management' > 'Staff'
- Select the user and click 'Edit' at the top-left

A dialog box titled "Edit Staff" with a close button (X) in the top right corner. It contains three input fields: "Name *" with the value "John", "Email *" with the value "narakes@yopmail.com", and "Role *" with a dropdown menu showing "Technician". A green "Save" button is located at the bottom right.

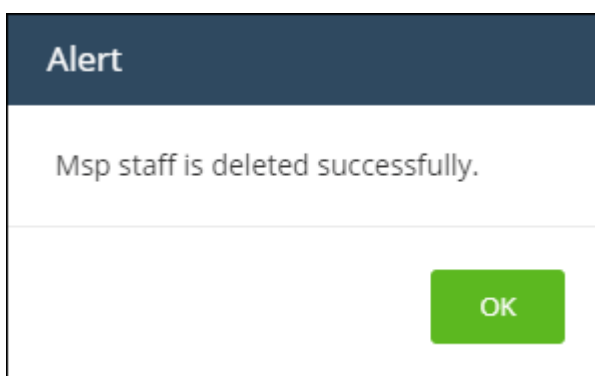
- Update staff details as required and click 'Save'. Please note the email address field cannot be edited.
- Click 'OK' in the confirmation dialog.

To remove a user

- Login to your **Comodo One / Comodo Dragon / ITarian** MSP account
- Click 'Management' > 'Staff'
- Select the user and click 'Delete' at the top-left



- Click 'Delete'



- Click 'OK' in the confirmation dialog.

9.4 View License and Subscription Details

- You can view your cWatch license details in your Comodo One / Comodo Dragon / ITarian MSP account
- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** MSP account
- Click 'Management' > 'Applications'

The 'Applications' screen shows all products that you have added to your account:

Comodo One > Management > Applications

Applications

Endpoint Manager

Dome Shield

Dome Secure Web Gateway

Dome Firewall Central Manager

cWatch

Subscriptions | Usage | Billing | Settings

Subscription List + Add New Subscription

ID:	ITSM Subscription Basic Edition For Comodo ONE	FREE	ACTIVE	Details
01e16c26b4	Unlimited	TRIAL		
	Start Date: 08/14/2017	30 days		

Comodo License Account Username	Date
ycnwp@yopmail.com	08/14/2017
Module Name	Period

- Click the 'cWatch' tile, then the 'Subscriptions' tab

Comodo One > Management > Applications

Applications

Endpoint Manager

Dome Shield

Dome Secure Web Gateway

Dome Firewall Central Manager

cWatch

Subscriptions | Usage | Billing | Settings

Subscription List

ID:	cWatch Core For Comodo One FREE 30 days (500 mb/day log volume)	FREE	ACTIVE	Details
e46f72595f		TRIAL		
	Start Date: 02/06/2019	30 days		

Comodo License Account Username	Date
ycnwp@yopmail.com	02/06/2019
Module Name	Period
cWatch	30 days
Product Name	Number of Users
cWatch Core For Comodo One FREE 30 days (500 mb/day log volume)	Price
Status	\$0.00
ACTIVE	Total Price
Subscription ID	\$0.00
e46f72595f	Payment Type
License Key	FREE
df930ef9-10d4-477c-971e-aea9cef4dc7a	

Each license is shown on a separate row. The following information is available for each license:

Subscription List

- Shows all your licenses for cWatch. Each license row contains basic information such as license name, type, duration, start date and mb/day log volume..
- Click a row to view more details about the license.

Details

- Comodo License Account Username - The email ID associated with the account for which the license was originally purchased.
- Module Name - The name of the application.
- Product Name - Indicates the name, duration and user/node allowances covered by the license.
- Status - Whether the license is active or not.
- Subscription ID - The identification number provided for the subscription.
- License Key - License key of the subscribed product.
- Date - The date of subscription.
- Period - The license validity period.
- Price – The base price of the product.
- Total Price – The total price paid for the product. This depends on the number of users, log volume per day and validity period.
- Payment Type - Indicates how payment was made for the product.

Appendix 1 - Field Groups and Event Items Description

S.No	Field Groups	Description	Event Items	Description
1	agent	Log collector	agent_id	ID of collector
			agent_ip	IP address of collector
2	application	Application information contained in events	app_name	Application Name
			app_pid	Application Process ID
3	classification	Event classification fields	class_action	Type of action attempted as part of the event
			class_domain	Environment or domain of the event
			class_object	Type of object that is targeted or affected by the event
			class_service	Service involved in event
			class_status	Status of the event action identified by the action field
			class_subject	Type of object that started the event action identified by the action field
4	custom	Custom field labels and their values	co_1	Custom Value 1
			co_1label	Custom Label 1
			co_2	Custom Value 2
			co_2label	Custom Label 2
			co_3	Custom Value 3
			co_3label	Custom Label 3
			co_4	Custom Value 4
			co_4label	Custom Label 4
			co_5	Custom Value 5
			co_5label	Custom Label 5
5	destination	Event target device	dst_city	Depending on country, it's either city or state of target device
			dst_country	Country Name of target device
			dst_host	Host name of target device
			dst_ip	IP Address of target device
			dst_ip_private	To show whether this target IP is

				private or not
			dst_ip_loc	Latitude and Longitude coordinates of target device
			dst_mac	MAC Address of target device
			dst_port	Port that is targeted
			dst_sd_1	If country has state, it's the state of target device's country(ex: USA/Kentucky)
			dst_sd_2	Subdivision of state of target device's country
			dst_tr_ip	Translated IP Address of target device
			dst_tr_port	Translated Port
6	device	Device where logs are produced on	dvc_host	Host name of device
			dvc_ip	IP Address of device
7	event	General event fields	agent_time	The time (in milliseconds) that raw log is processed on collector
			central_time	The time (in milliseconds) that raw log is transformed to an event
			customer_id	identifier for the customer of mssp
			dvc_time	The time (in milliseconds) that log is seen on device
			event_id	Unique id of the event
			lt_1	Indicates list name event
			lt_2	Indicates list event field group and list name event
			lt_3	Indicates list event field group and list name and list type event
			message	Message of the event
			mssp_id	identifier for mssp
			name	Name of the event
			raw_log	The log text seen on device
			raw_size	Received log size in bytes encoded in UTF-8
			size	Normalized event size in bytes encoded in UTF-8
			tag_list	Event tags separated with pipe character ()
			type	Type of the event
8	file	File information contained in	f_name	File name

		events		
			f_size	File size
			f_type	File type
			f_uri_path	File uri path
			f_url	File url
			f_md5	MD5 hash value of the file
			f_sha1	SHA1 hash value of the file
			f_sha256	SHA256 hash value of the file
9	network	Network-related information contained in events	app_proto	Application protocol used in event
			bytes_in	Bytes received
			bytes_out	Bytes sent
			int_in	Interface in
			int_out	Out interface
			session_id	Session id
			trans_proto	Transport protocol used in event
10	product	Product that produces raw logs that will be converted to events	prod_name	Name of the product
			prod_vendor	Vendor of the product
			prod_version	Version of the product
11	rule	Rule (firewall, ips, antivirus rule etc.) information contained in events	rule_hit_count	Represents how many hits occurred for the rule
			rule_id	ID of the rule
			rule_info	Extra information related to the rule
			rule_name	Name of the rule
			rule_sig_id	ID of the signature related to rule
			rule_sig_name	Name of the signature related to rule
12	source	Event source device	src_city	Depending on country, it's either city or state of source device
			src_country	Country of source device
			src_host	Host name of source device
			src_ip	IP Address of source device
			src_ip_private	To show whether this source IP is private or not
			src_loc	Latitude and Longitude coordinates of source device
			src_mac	MAC Address of source device

			src_port	Event source port
			src_sd_1	If country has state, it's the state of source device's country(ex: USA/Kentucky)
			src_sd_2	Subdivision of state of source device's country
			src_tr_ip	Translated IP Address of source device
			src_tr_port	Source Port
13	syslog	Syslog information	facility	Syslog facility field
			priority	Syslog priority field
			severity	Syslog severity field
14	time	Time-related information (calculated based on agent_time)	partition_time	Represents collection time of log in terms of day (calculated based on agent time)
			pass_days	Represents how many days have passed since January 1, 1970 UTC
			pass_hours	Represents how many hours have passed since January 1, 1970 UTC
			pass_minutes	Represents how many minutes have passed since January 1, 1970 UTC
			pass_months	Represents how many months have passed since January 1, 1970 UTC
			pass_years	Represents how many years have passed since January 1, 1970 UTC
15	user	User information contained in events	usr_domain	Domain of the user
			usr_name	Name of the user
			usr_uid	UID of the user
			target_domain	Tageted User's Domain
			target_name	Tageted User's Name
			target_uid	Tageted User's Unique Id

Appendix 2 - cWatch Supported Logs

The following table provides the details of logs that cWatch supports and fetches the data to populate Events fields according to event queries.

S.No.	Log Name	Vendor Name	Log Type
1	Mysql	Oracle	Database
2	Oracle	Oracle	Database
3	Active Directory	Unknown	Audit
4	Windows-Linux Audit	Comodo Audit Parser	Audit
5	Comodo UTM	Comodo	Audit
6	Juniper	Juniper Networks	Firewall
7	IPtables	Linux	Firewall
8	Sonicwall	SonicWALL	Firewall
9	Cisco-fw	CISCO	Firewall
10	Squid	Squid	Proxy
11	Apache	Apache	Application
12	Comodo Endpoint Security	Comodo	Content Security
13	MyDLP	Comodo	Data Protection
14	Snort	CISCO	Intrusion Detection
15	Tipping Point	HP	Intrusion Detection
16	Web Inspector	Comodo	Malware
17	VPN	Open VPN	Access
18	DHCP	Linux	Access
19	Fortigate	Fortinet	Firewall
20	Comodo DPI	Comodo	Access
21	Comodo DPI Bro	Comodo	Access
22	Snmp Trap Logs	Snmp	Audit
23	Fortigate 5.0	Fortinet	Firewall
24	Sophos Ulogd	Sophos	Firewall
25	Bro_HTTP	BRO	Access
26	Bro_FTP	BRO	Access
27	Bro_Weird	BRO	Network Monitoring

28	Bro_Files	BRO	Access
29	Bro_Conn	BRO	Firewall
30	Bro_Dpd	BRO	Access
31	Bro_Smtp	BRO	Access
32	Bro_Dns	BRO	Access
33	Windows Audit	Windows	Audit
34	Alarms	Comodo Alarm Producer	Audit
35	Cef	Common Event Format	Access
36	Bro_Ssl	BRO	Network Monitoring
37	Bro_Irc	BRO	Network Monitoring
38	Bro_Dhcp	BRO	Network Monitoring
39	Suricata	OISF	Intrusion Detection
40	NxIDS	Comodo	Intrusion Detection
41	NxSensor_HTTP	Comodo	Access
42	NxSensor_FTP	Comodo	Access
43	NxSensor_Files	Comodo	Access
44	NxSensor_Conn	Comodo	Firewall
45	NxSensor_Dpd	Comodo	Access
46	NxSensor_Smtp	Comodo	Access
47	NxSensor_Dns	Comodo	Access
48	NxSensor_Ssl	Comodo	Network Monitoring
49	NxSensor_Irc	Comodo	Network Monitoring
50	NxSensor_Dhcp	Comodo	Network Monitoring
51	NxSensor_Weird	Comodo	Network Monitoring
52	analyser	Comodo	Audit
53	dome-eapi	Comodo	Audit
54	dome-vs	Comodo	Audit
55	linux	Comodo	Audit
56	JUNOS SYS	Juniper	Firewall
57	comodo-rdns	Comodo	Network Monitoring
58	dome-cni	Comodo	Audit
59	Bro_Tunnel	BRO	Network Monitoring

60	Bro_Software	BRO	Network Monitoring
61	Bro_Pe	BRO	Network Monitoring
62	Bro_SSH	BRO	Network Monitoring
63	Bro_MySQL	BRO	Network Monitoring
64	Bro_Notice	BRO	Network Monitoring
65	Bro_Fls	BRO	Network Monitoring
66	NxSensor_Tunnel	Comodo	Network Monitoring
67	NxSensor_Software	Comodo	Network Monitoring
68	NxSensor_Pe	Comodo	Network Monitoring
69	NxSensor_SSH	Comodo	Network Monitoring
70	NxSensor_MySQL	Comodo	Network Monitoring
71	NxSensor_Notice	Comodo	Network Monitoring
72	NxSensor_Fls	Comodo	Network Monitoring
73	modsecurity	Comodo	ModSecurity Audit
74	Bro_Syslog	Comodo	Network Monitoring
75	NxSensor_Syslog	Comodo	Network Monitoring
76	cpanelaccess	CPanel Inc	Audit
77	cpanellogin	CPanel Inc	Audit
78	Panos	Palo Alto Inc.	Firewall
79	MySQL_Slow_Queries	Oracle	Database
80	Apache-Error	Apache	Application
81	MySQL_Error	Oracle	Database
82	NxSensor_Fvs	Comodo	File Monitoring
83	Cwatch Endpoint	Comodo	Application
84	modsecurity-java	Comodo	Audit
85	Internal Events	Comodo Internal Event Producer	Audit
86	DbCollector	Comodo Db Collector	Audit

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit [comodo.com](https://www.comodo.com) or our [blog](#). You can also follow us on [Twitter](#) (@ComodoDesktop) or [LinkedIn](#).

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: EnterpriseSolutions@Comodo.com