COMODO
Creating Trust Online®

cWatch

# Comodo

## cWatch Network

Software Version 2.23

# Quick Start Guide

Guide Version 2.23.021419

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

# cWatch Network – Quick Start Guide

cWatch Network is an advanced security intelligence and event management (SIEM) tool that features event log monitoring, powerful event querying, automatic assignment of incidents to personnel and more. The service allows managed security providers (MSPs) to provide comprehensive network monitoring services to their customers.

This tutorial briefly explains how to setup and start using cWatch Network.

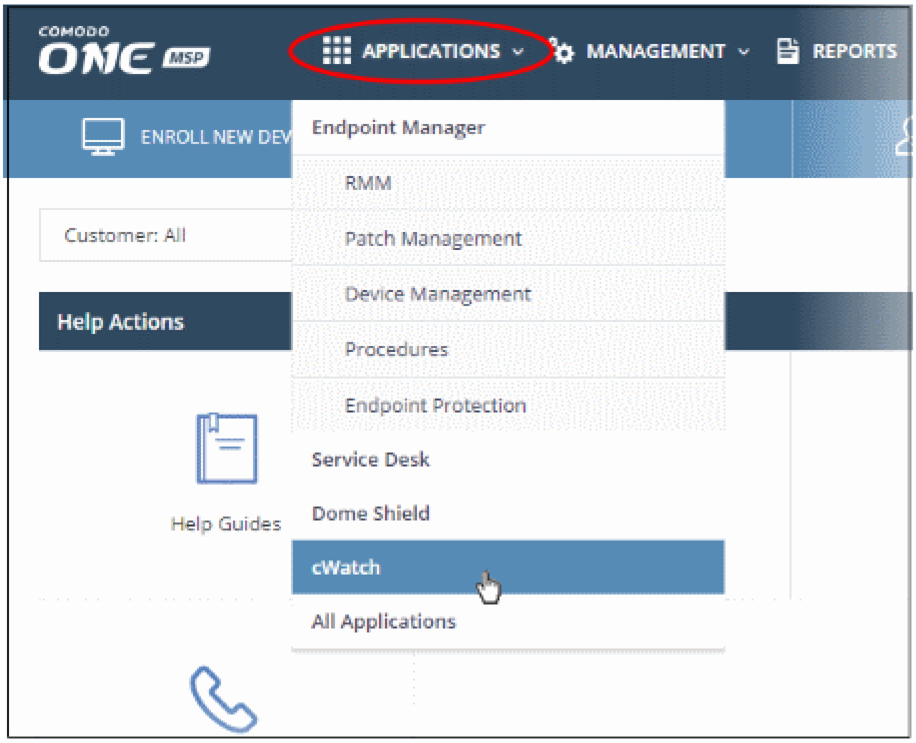
- **Step 1 – Login to cWatch Admin Console**
- **Step 2 – Add Customers and their Assets**
- **Step 3 – Deploy NXlog, Rsyslog and Network Monitoring Sensors**
- **Step 4 – Add Users**
- **Step 5 – Configure Event Queries**
- **Step 6 – Configure Correlation Rules**
- **Step 7 – Manage Incidents**
- **Step 8 – Generate Reports**

## Step 1 – Login to cWatch Admin Console

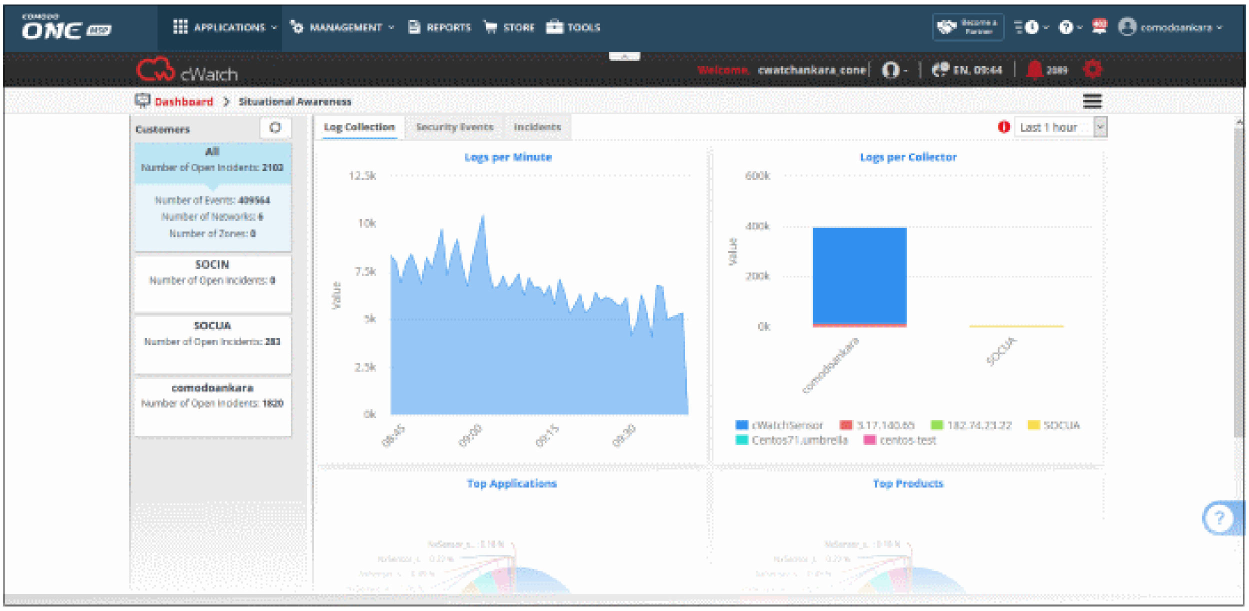
- You can login to cWatch after purchasing a license. You buy licenses in the Comodo One or ITarian MSP portal as follows:
  - Login to C1/ITarian
  - Click 'Store' in the top navigation
  - Scroll to the cWatch tile and click 'Free' to start the purchase process
  - **Click here** if you need more help with this

**Login to cWatch:**

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



The cWatch admin console will open at the dashboard:



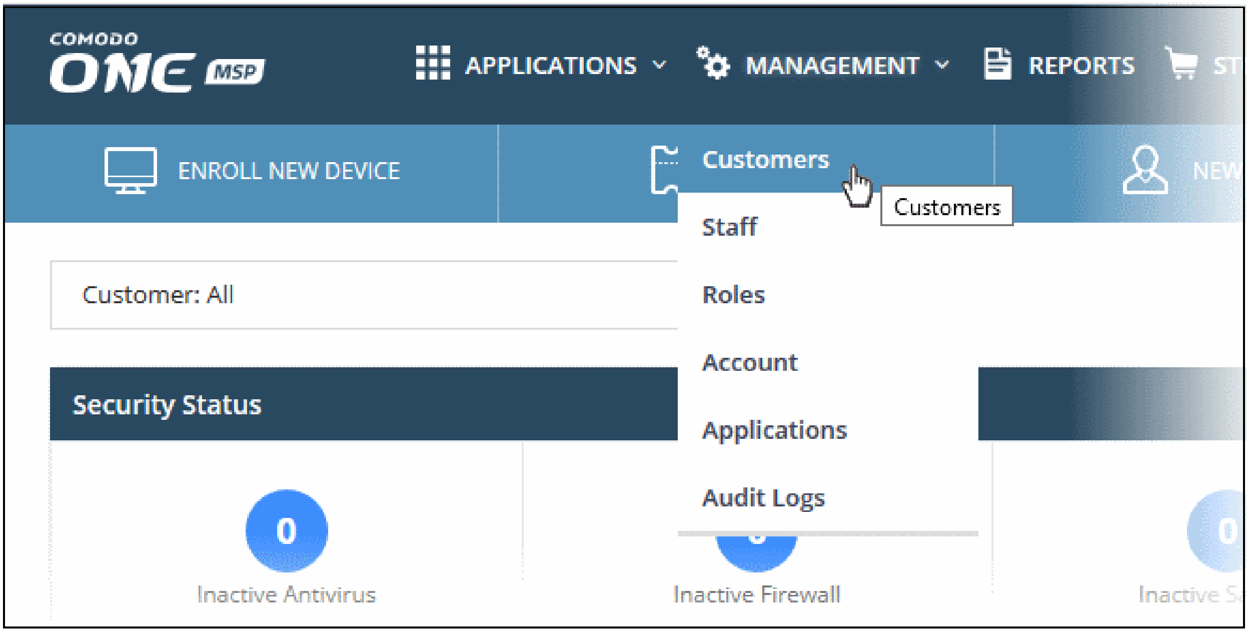
## Step 2 – Add Customers and their Assets

The next step is to add your customers and their assets to cWatch in order to monitor their networks. Customer assets are the networks, endpoints and web servers from which logs will be collected.

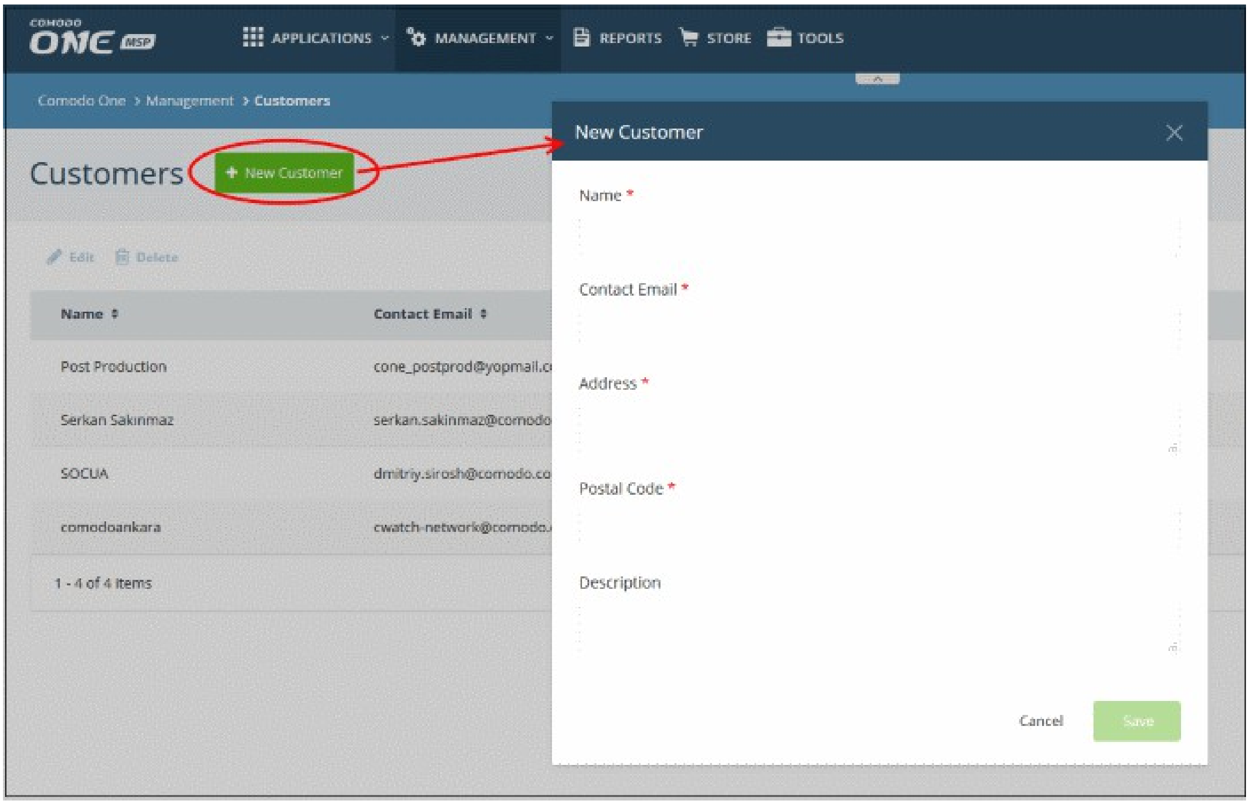
### Add a new customer

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

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



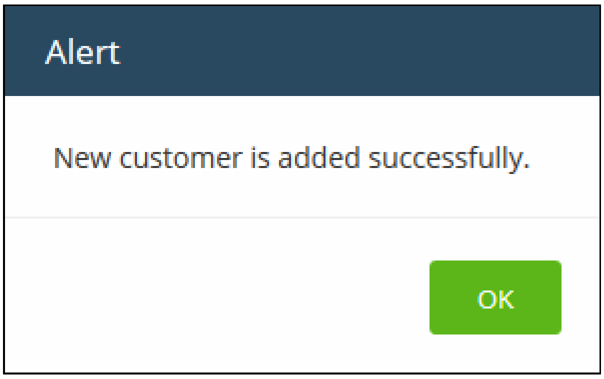
- Click the 'New Customer' button:



| Name | Contact Email |
|---|---|
| Post Production | cone_postprod@yopmail.c |
| Serkan Sakınmaz | serkan.sakinmaz@comodo |
| SOCUA | dmitriy.sirosh@comodo.co |
| comodoankara | cwatch-network@comodo. |

1 - 4 of 4 items

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



New customer is added successfully.

- Repeat the process to add more customers.

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

- Next, you need to:
  - Add customers' assets to cWatch Network for monitoring
- To open the cWatch interface, login to your **Comodo One** / **ITarian** MSP account, click 'Applications' then 'cWatch'
- The cWatch admin console will open at the dashboard:

**Add customer assets**

- 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.

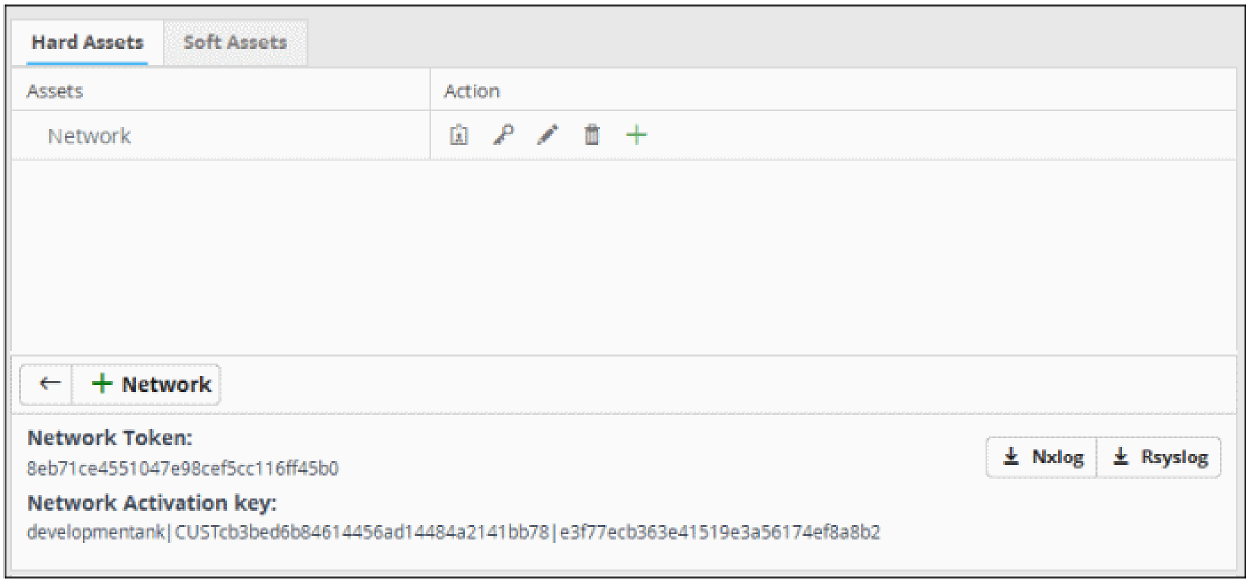
Customer details will be shown on the right.

- Click 'Manage' at the bottom:

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

- **Hard Assets –** Assets such as networks and zones to be monitored by entering their start and end IP addresses.
- **Soft Assets -** Assets such as services which are hosted on the network.

The hard assets tab contains a default customer network and token. You can use this to add endpoints or create a new network with another name.



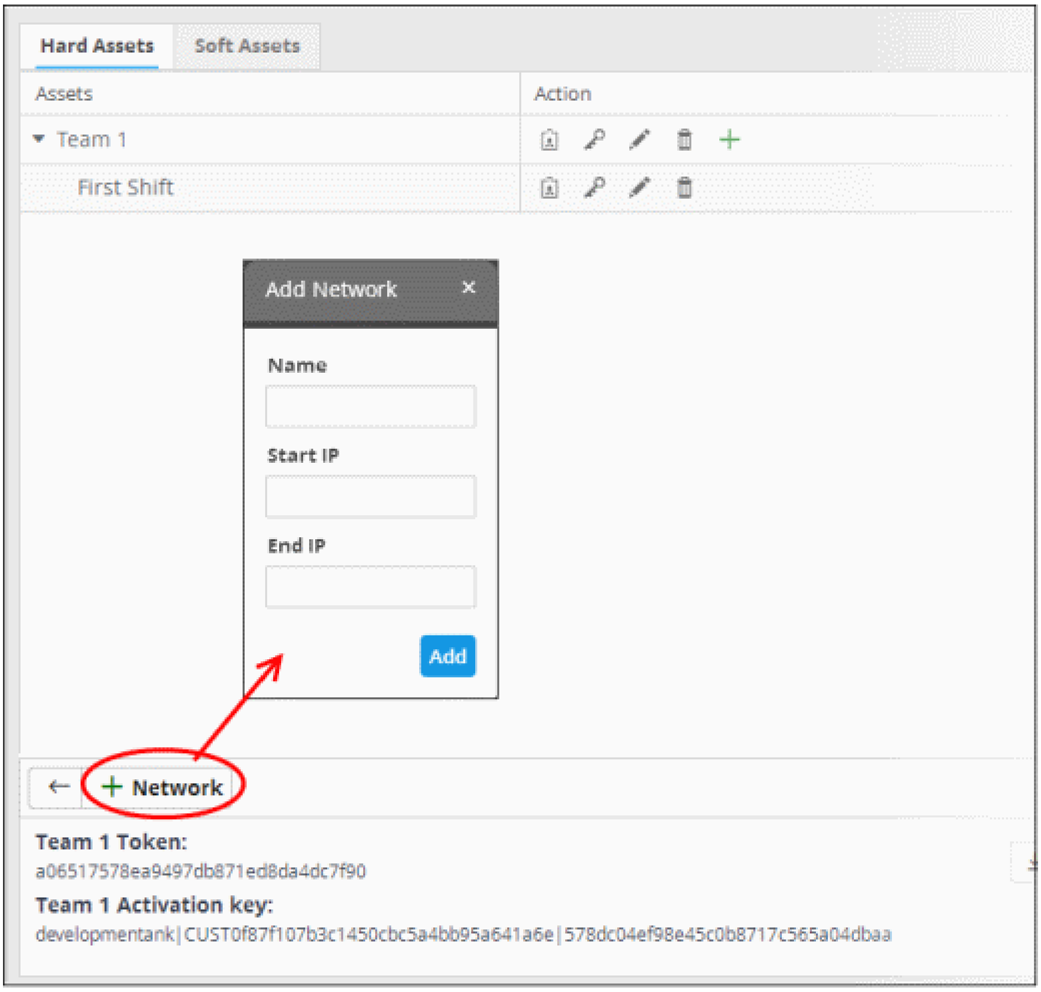
**Network Token:**
8eb71ce4551047e98cef5cc116ff45b0

**Network Activation key:**
developmentank|CUSTcb3bed6b84614456ad14484a2141bb78|e3f77ecb363e41519e3a56174ef8a8b2

| 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. |

### Add hard assets

- 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.



Team 1 Token:
a06517578ea9497db871ed8da4dc7f90

Team 1 Activation key:
developmentank|CUST0f87f107b3c1450cbc5a4bb95a641a6e|578dc04ef98e45c0b8717c565a04dbaa

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.

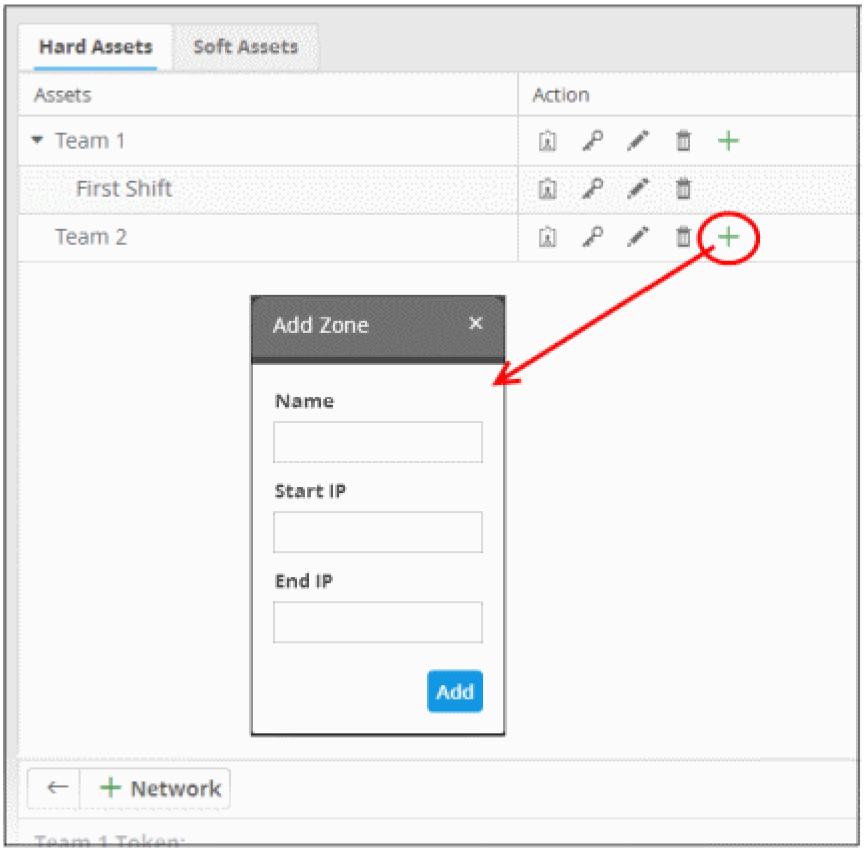
The network will be added and a unique authentication token and agent activation key will be generated for the network. Clicking the ▣ button in the new network row will display the token and the key at the bottom of the right pane.

- 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.

Now that you have added endpoints to be monitored in the Hard Assets area, the next step is to run the Nxlog and Rsyslog configuration files on endpoints with Nxlog and Rsyslog utilities. See **Step 3** for more details.

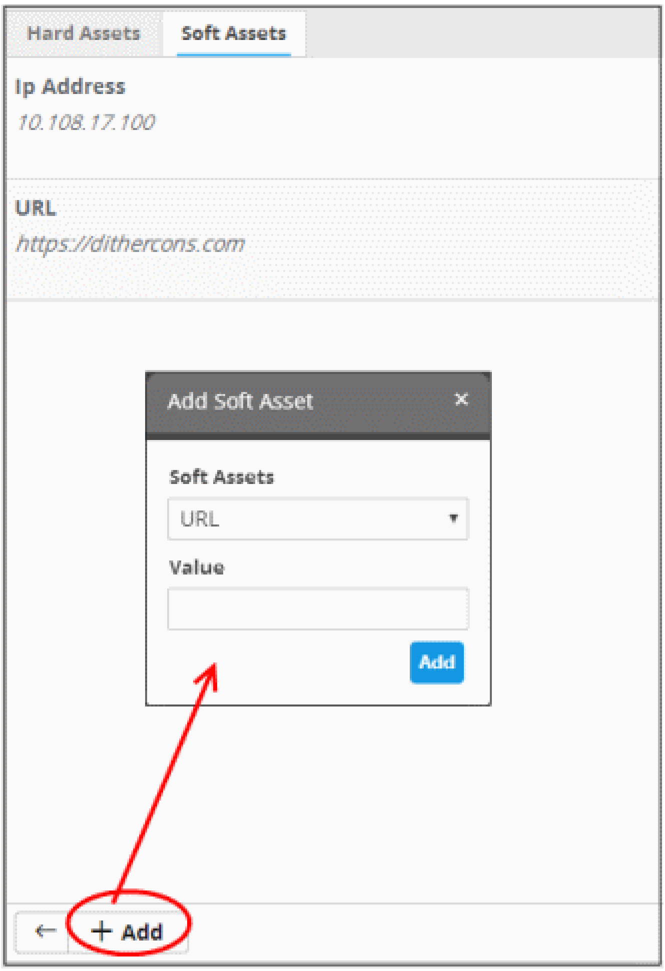
The 'Soft Assets' interface allows administrators to create and manage a list of important URLs, domains or IP addresses, which acts as a reference list for the operators/administrators/analysts. If items displayed in this screen are affected by an incident, the operator/administrator/analyst may decide to, for example, escalate the incident from high to critical.

**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 you wish to add from the left.

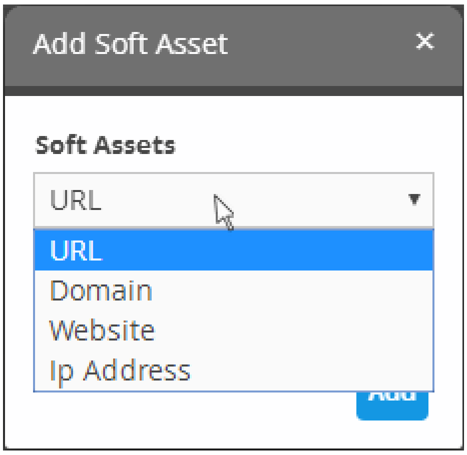
The Customer Details pane will open in the right.

- 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.

## Step 3 – Deploy Nxlog, Rsyslog and Network Monitoring Sensors

- After adding customers and their endpoints as explained in **Step 2**, you have to configure them to send logs to cWatch.
- cWatch features agent-less log collection from Windows/Linux endpoints via the NXLog and Rsyslog utilities
- NXLog (Windows) and Rsyslog (Linux) need to be configured to send logs to the cWatch Network server. **Click here** for more details about deploying script files.

You can also deploy Comodo sensors on the network to enlarge the scope of log collection. **Click here** for more details on this option.

Scripts can be configured and deployed in two ways:

- **Pre-configured script files** – The 'Hard Assets' area contains ready-made scripts pre-configured for a specific customer/network. This is the most convenient way to configure NXLog and RSYSLOG to send logs to cWatch.
- **Manually configure NXLOG and RSYSLOG scripts** - Download scripts for Rsyslog and NXLog and manually set network token, source product and so on. These scripts can be used to configure Rsyslog and NXLog utilities on Linux and Windows machines.

### Configure NXLog and Rsyslog using pre-configured script files

The following sections explain more about:

- **Configure the NXLOG Utility**
- **Configure the RSYSLOG Utility**

### Configure the NXLOG Utility

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**

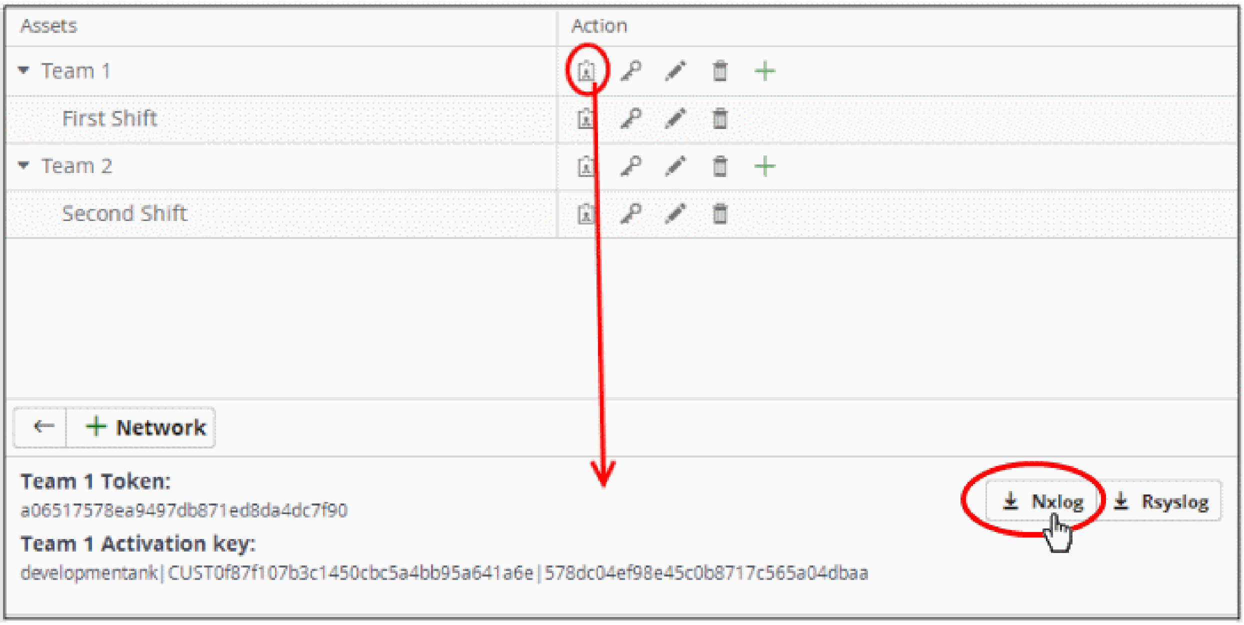
- Open the 'Asset Management' interface by clicking the 'Menu' button, then 'Assets' > 'Asset Management'.
- Select the customer from the left hand side pane.

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:



**Team 1 Token:**
a06517578ea9497db871ed8da4dc7f90

**Team 1 Activation key:**
developmentank|CUST0f87f107b3c1450cbc5a4bb95a641a6e|578dc04ef98e45c0b8717c565a04dbaa

- 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\webservers 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.

### Configuring 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**

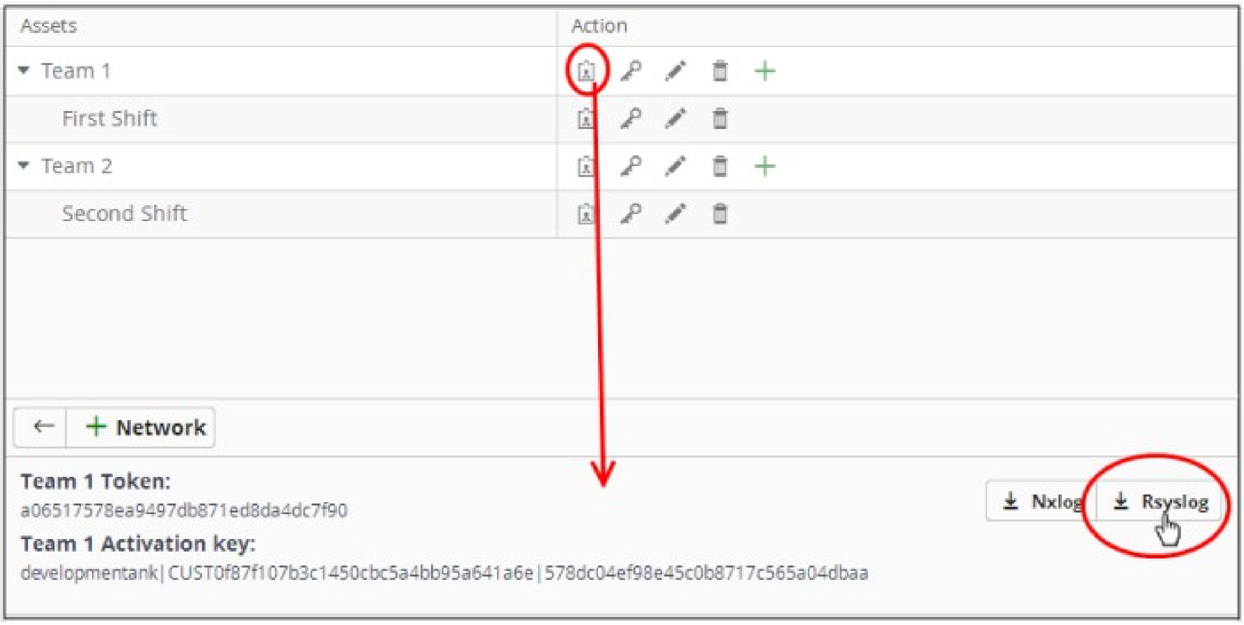
- Open the 'Asset Management' interface by clicking the 'Menu' button, then 'Assets' > 'Asset Management'.
- Select a customer from the left hand pane.

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 | |

**Team 1 Token:**
a06517578ea9497db871ed8da4dc7f90

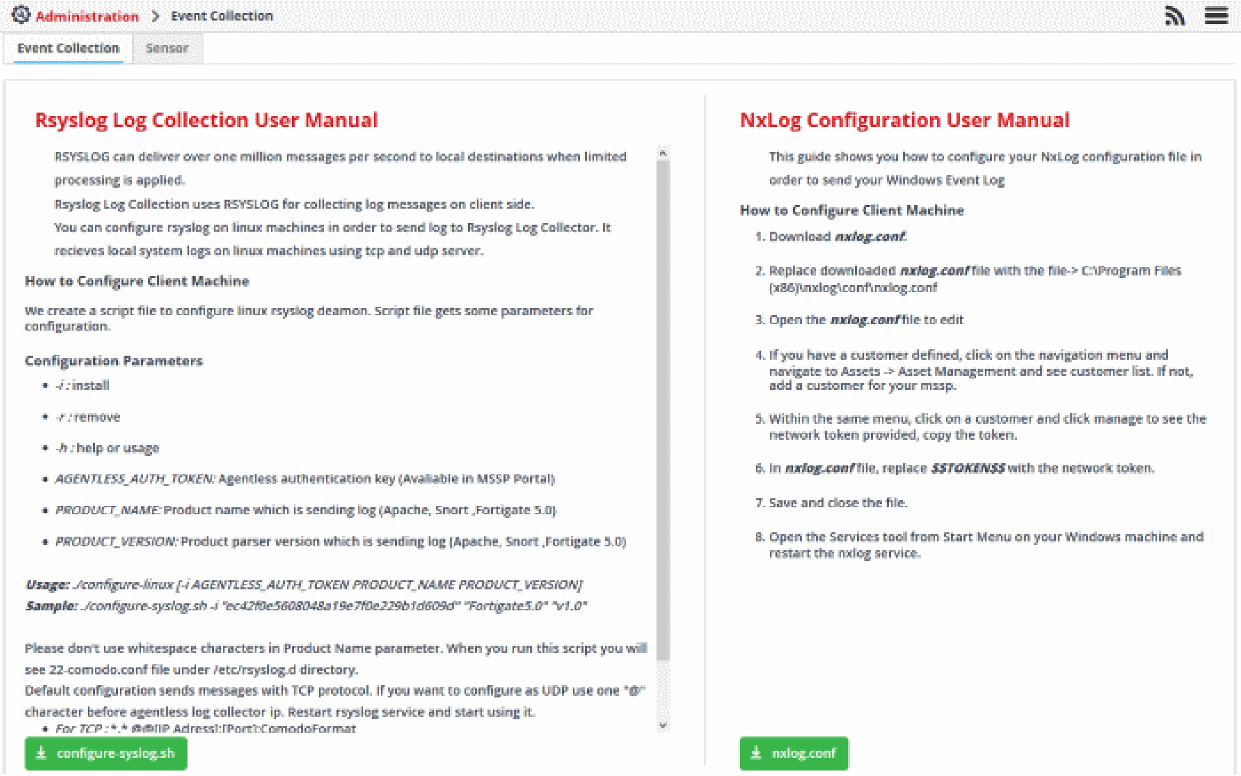
**Team 1 Activation key:**
developmentank|CUST0f87f107b3c1450cbc5a4bb95a641a6e|578dc04ef98e45c0b8717c565a04dbaa

- 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.

**Manually configure Nxlog and Rsyslog**

- Click the 'Menu' button from the top right, choose 'Administration' and then click 'Event Collection'



Rsyslog Log Collection User Manual

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 recieves 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 deamon. Script file gets some parameters for configuration.

Configuration Parameters

- *-i :* install
- *-r :* remove
- *-h :* help or usage
- *AGENTLESS_AUTH_TOKEN:* Agentless authentication key (Avaliable 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"*

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*

NxLog Configuration User Manual

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.

The 'Event Collection' page contains instructions about downloading the scripts, setting the parameters and configuring the RSYSLOG/NxLOG utilities using the scripts.

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 Log 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.

### Deploy Comodo Network Monitoring Sensors

In addition to agentless log collection, cWatch can also collect logs from sensors placed in your network. These sensors listen to network activity using span/tap technologies. Comodo staff will work with your team to deploy the sensors according to your specific requirements. Please contact your Comodo account manager for help to deploy sensors on your network.

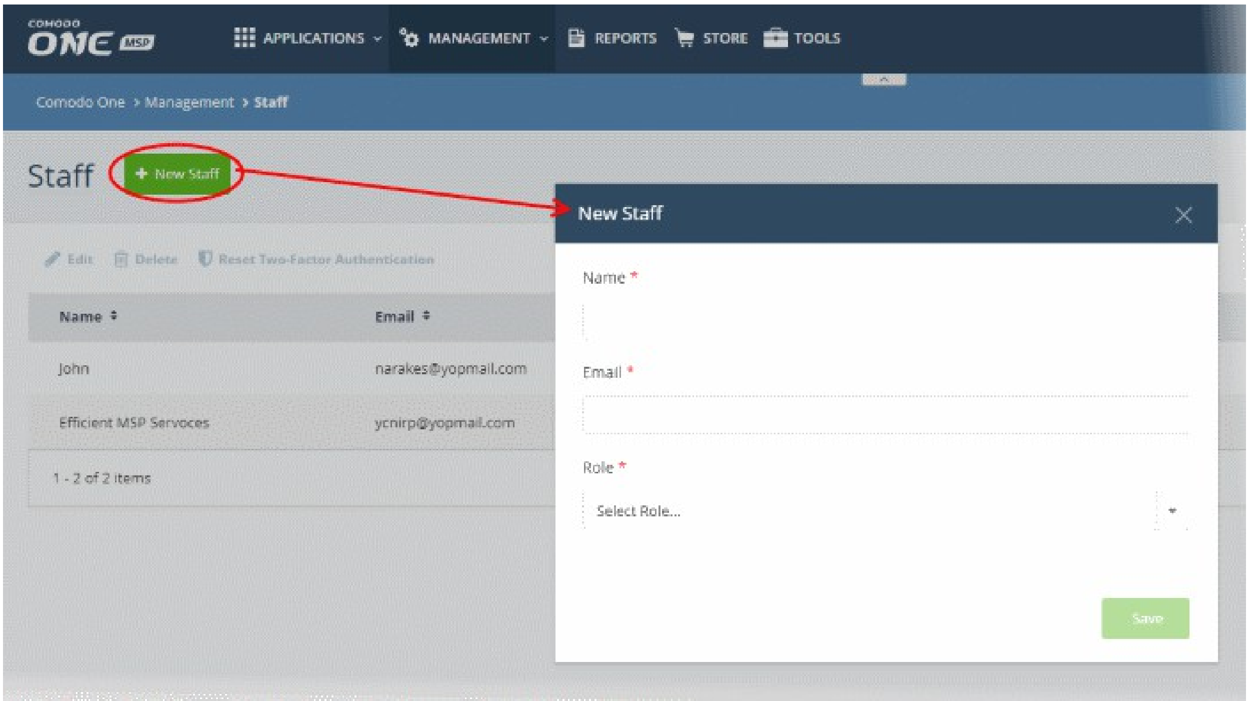
## Step 4 – Add Users

- Users are members of your staff assigned to a specific customer to address issues on their network.
- You create staff in the C1/ITarian interface. These staff then become available as 'Users' in cWatch.
- Users can only access the cWatch dashboards, events and incidents related to their assigned customers.
- 'Correlated Incidents' belonging to a customer are auto-routed to the user assigned to the customer.

### Add a user

You can add users (staff) from your **Comodo One** / **ITarian** MSP account:

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



| Name | Email |
|---|---|
| John | narakes@yopmail.com |
| Efficient MSP Servoces | ycnirp@yopmail.com |

- Click 'New Staff' at top-left

Complete the 'New Staff' form:

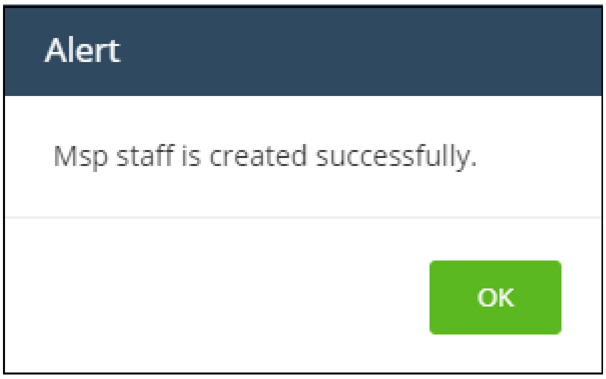
  - **Name -** The full name of the user (staff)
  - **Email -** The email address of the staff member. This also acts as their login username.
    - An account activation email is sent to this email address after you click 'Save'
    - Staff must click the link in the mail then create a password to activate their account.
    - Once their account is active, staff can login to C1 / ITarian at

https://one.comodo.com/app/msp/login / https://www.itarian.com/app/msp/login

- **Role** - Select appropriate privileges for the staff member. Note – make sure the role has permission to access the cWatch application. See **this page** if you need more help with ITarian roles.

- Click 'Save'

A confirmation message will appear:



Alert

Msp staff is created successfully.

Once the user activated their account they can access cWatch as follows

- Login to Comodo One/ITarian at **https://one.comodo.com/app/msp/login** / **https://www.itarian.com/app/msp/login**
- Click 'Applications' in the top-menu then select 'cWatch'

## Step 5 – Configure Event Queries

After configuring NXLog, Rsyslog and sensors as explained in **Step 3**, the logs will start to flow to cWatch.

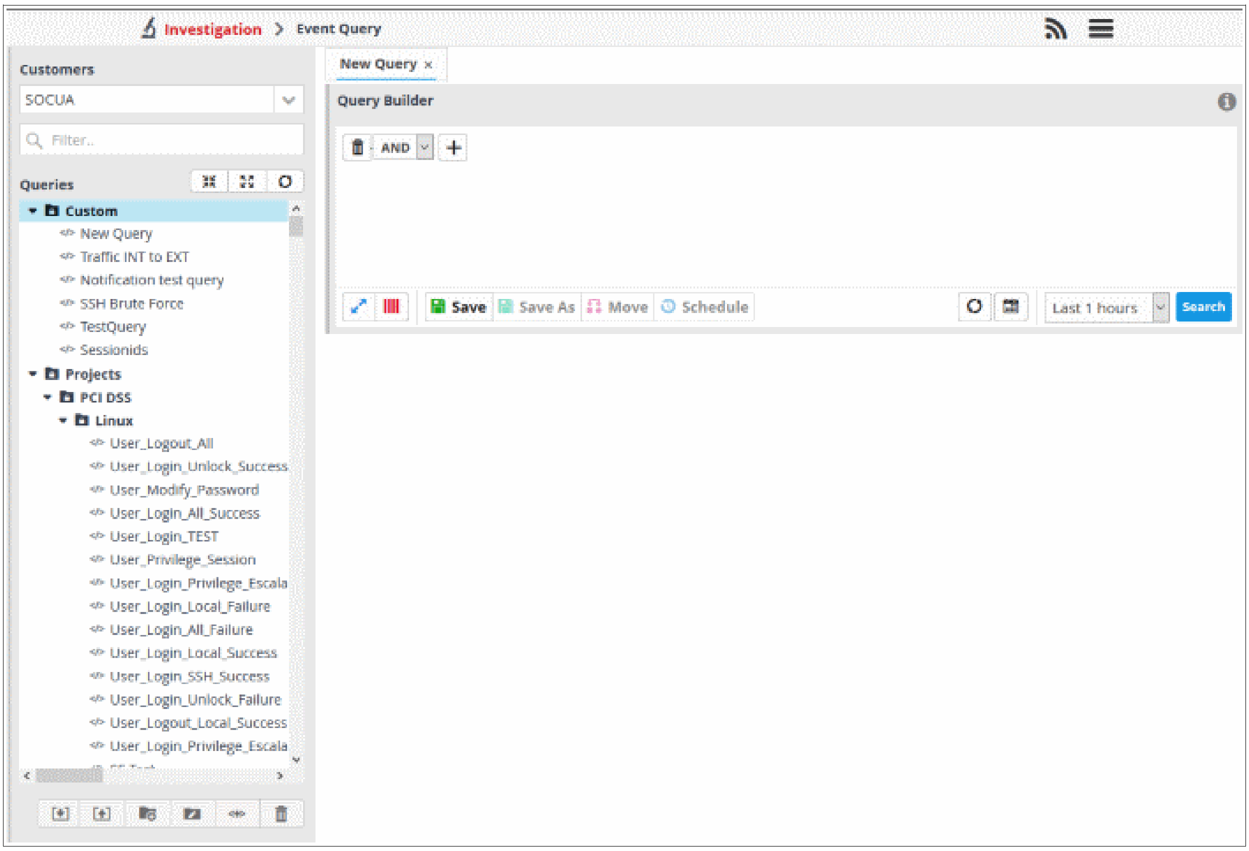
- The event query area lets you search for specific events using built-in queries or custom queries.
- You create your own conditions for each search. For example, for events during a specific period in specific customer networks.
- The results table shows all events which match the query conditions. 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 configure custom queries**

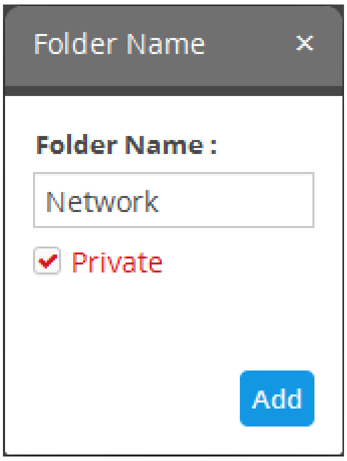
- Click the menu button at top-right > 'Investigation' > 'Event Query':
- Select the customer from the left pane under 'Customers' that you want to configure custom queries.



The 'New Query' tab contains a query builder which allows you to create a new query for a selected customer. Any queries you create will be added to 'Custom queries'.

The left side panel displays a list of predefined queries and custom queries for the selected customer. The predefined query folders are in blue and custom query folders are in black. Before creating a query, you have to create a folder under which the query should be saved.

- Click the folder button at the bottom on the left



Folder Name : Network

☑ Private

- Folder Name – Enter the name for the folder
- Private - If you select this, the folder will be accessible only to you. The folder will have a lock icon indicating it is a private folder. This option is available only while creating a top level folder.
- Click 'Add'

The folder will be saved and displayed on the left side. You can save an event query under this folder.

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. For full list of field groups and event fields, see '**Appendix 1 – Field Groups and Event Items Description**'.
- **Operator** - Controls the relationship between the field and the specified value. Examples include 'Equals to', 'Does not equal to', contains, 'does not contain' and so on.
- **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:

i. 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'**

ii. 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**

iii. 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:

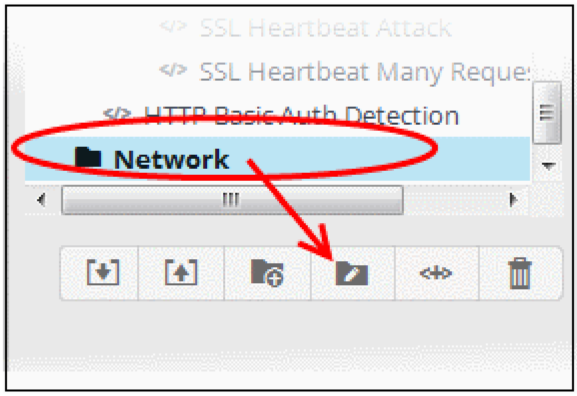
- To search for network connection events originating from an endpoint with the IP 10.100.100.100, and destined for an endpoint with the IP 10.100.100.120, build the filter statements with the AND operator as shown below:

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

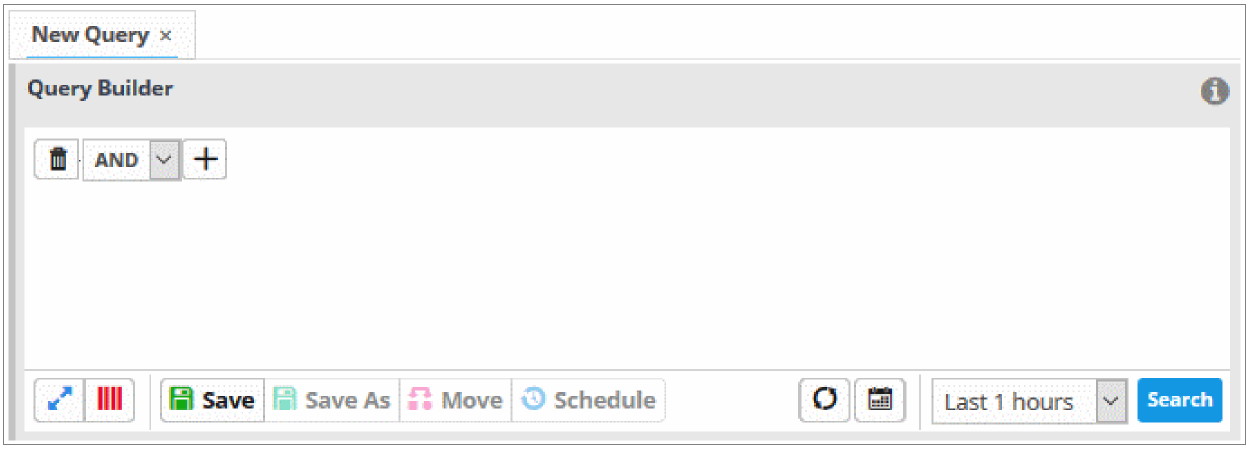
**AND**

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

- To create a new event query under the folder, select it and click the <+> button



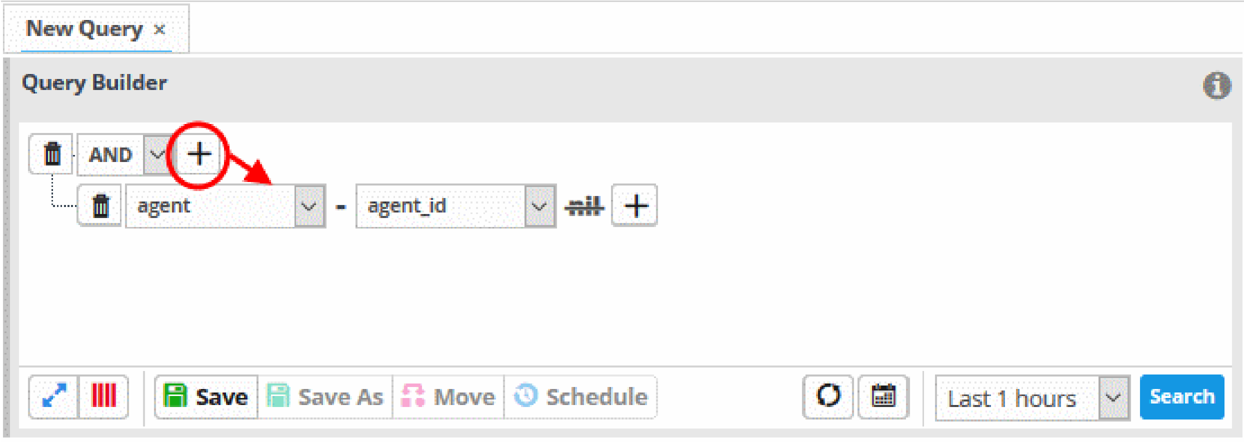
A 'New Query' tab will be added and displayed on the right.



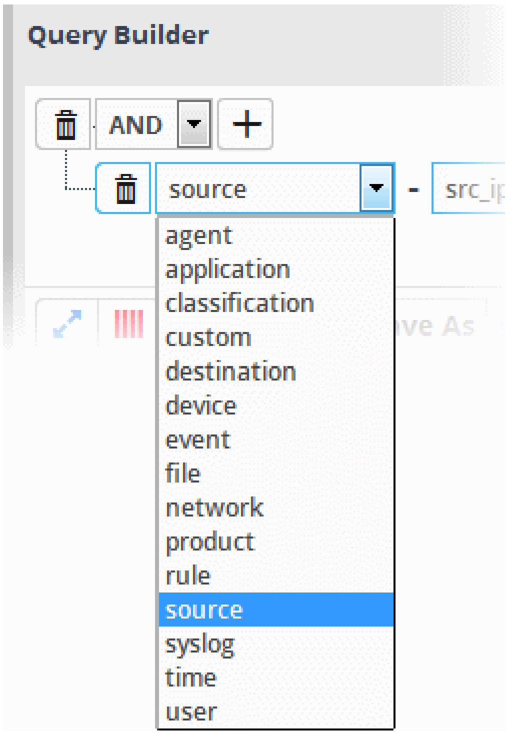
The next step is to add filters to the query.

- 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

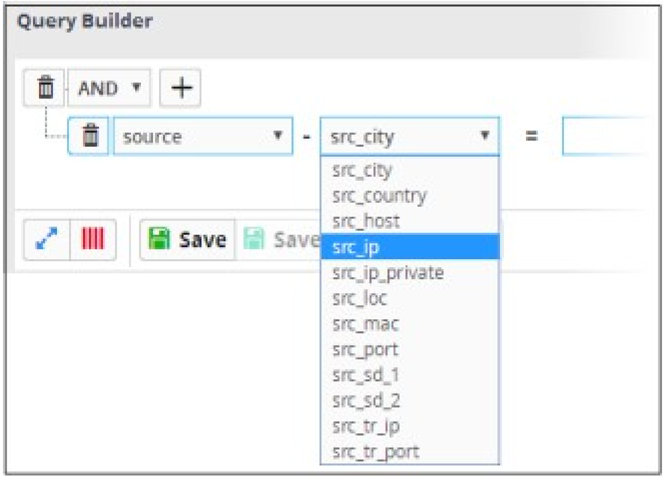
The 'Field Groups' drop-down and 'Fields' drop-down will appear. The 'Fields' drop-down will contain options relevant to the 'Field Group' chosen from the drop-down at the left.



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



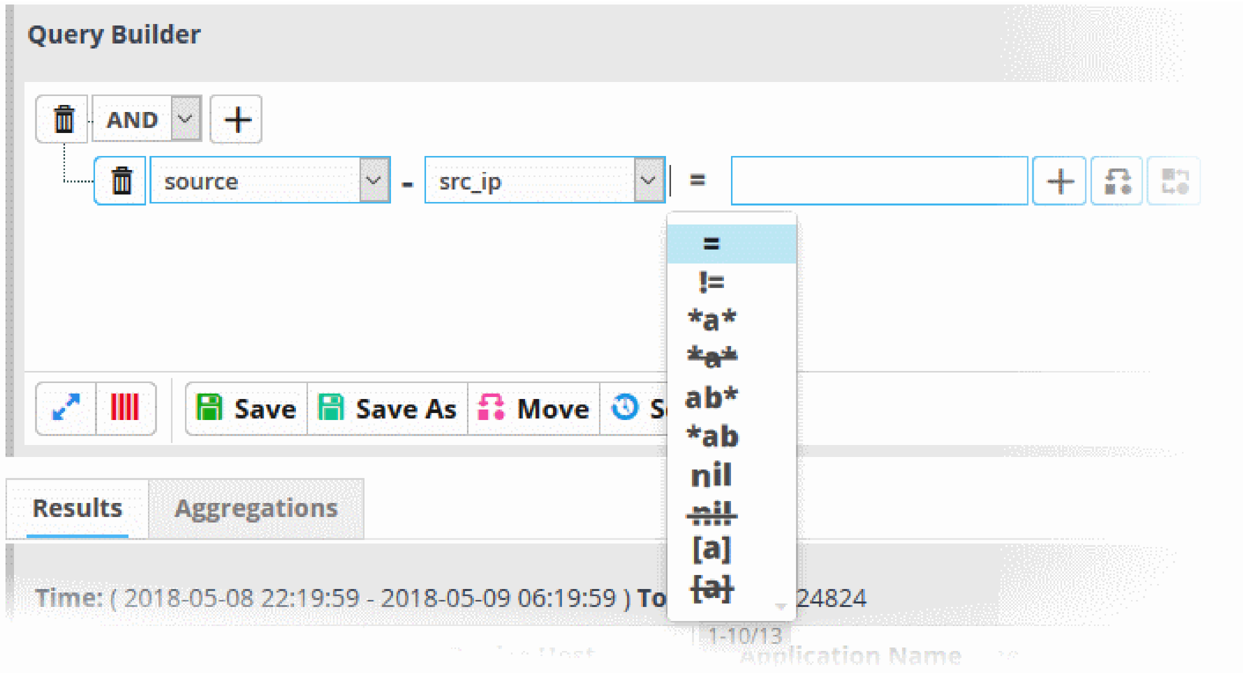
The next field will display the fields available for the selected field group.



**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.

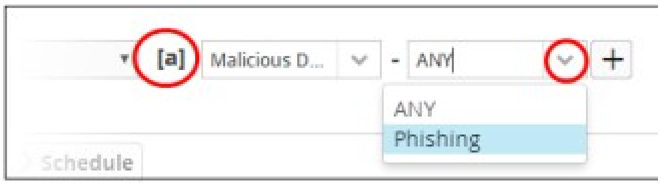
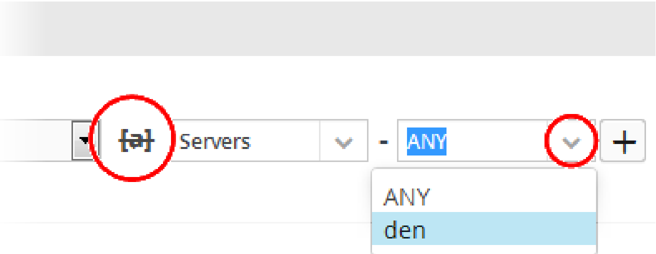
- To choose an operator, click the drop-down between the two fields:



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

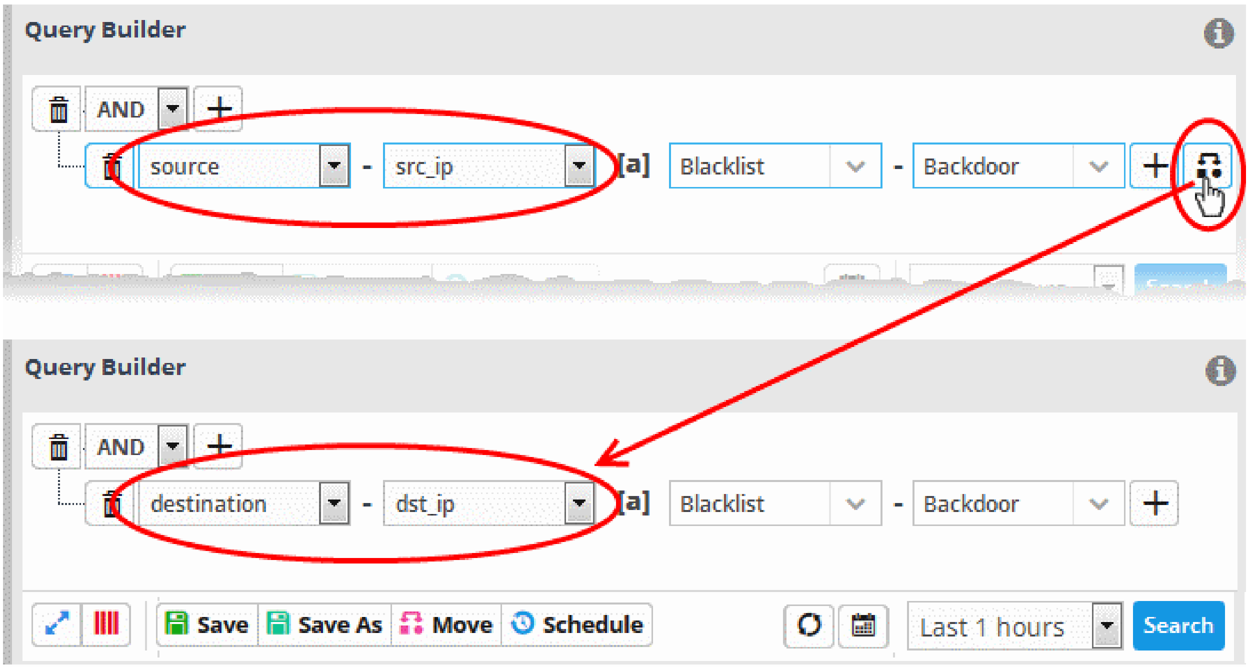
| Relation Operator | Description | Entering the value for the 'Field' |
|---|---|---|
| = | Equals to | • Events containing the same value will be identified by the query.<br>• Enter a value in the field to the right of the operator. |
| != | Does not equal to | • Events that do not contain the value will be identified by the query.<br>• Enter a value in the field to the right of the operator. |
| > | Greater than | • The query will identify events that contain values greater than the entered value.<br>• Enter a value in the field to the right of the operator.<br>• Applies only to fields with numerical values. For example, port numbers. |
| >= | Greater than or equal to | • The query will identify events that contain values equal to or greater than the entered value.<br>• Enter a value in the field to the right of the operator.<br>• Applies only to fields with numerical values. For example, port numbers. |
| < | Less than | • The query will identify events that contain values less than the entered value.<br>• Enter a value in the field to the right of the operator.<br>• Applies only to fields with numerical values. For example, port numbers. |
| <= | Less than or equal to | • 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.<br>• Applies only to fields with numerical values. For example, port numbers. |
| *a* | Contains | • The query will identify events that contain the entered value somewhere in the string.<br>• E.g - search for events with source IP addresses containing '123' anywhere in the address.<br>• Enter a value in the field to the right of the operator. |
| ~~*a*~~ | Does not contain | • The query will identify events that do not contain the entered value anywhere in the string.<br>• E.g - search for events which don't contain '123' anywhere in source IP address.<br>• Enter a value in the field to the right of the operator. |
| ab* | Starts with | • The query will identify events that begin with the entered value.<br>• E.g, - search for events with source IP addresses that start with '192'<br>• Enter a value in the field to the right of the operator. |
| *ab | Ends with | • The query will identify events that end with the entered value.<br>• E.g. - search for events with source IP addresses that end with '123'.<br>• Enter a value in the field to the right of the operator. |
| nil | Is Empty | • Search for events in which the selected field is empty (does not contain any value).<br>• E.g. - search for the events with no values in their source IP address fields, select 'Is Empty'. |
| ~~nil~~ | Is Not Empty | • Search for events in which the selected field is not empty (contains a value of some kind).<br>• 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 | Configure the filter statement to fetch values for the field from a pre-defined list containing specific values for the field type.<br>**Background**:<br>• Lists enable administrators to add and manage lists of values for different fields for use in queries and correlation rules.<br>• cWatch features three kinds of lists - Live Lists, Range List and IP Range.<br>• Lists can be created and the values updated manually.<br>• Live lists can be also be fetched from the output of |

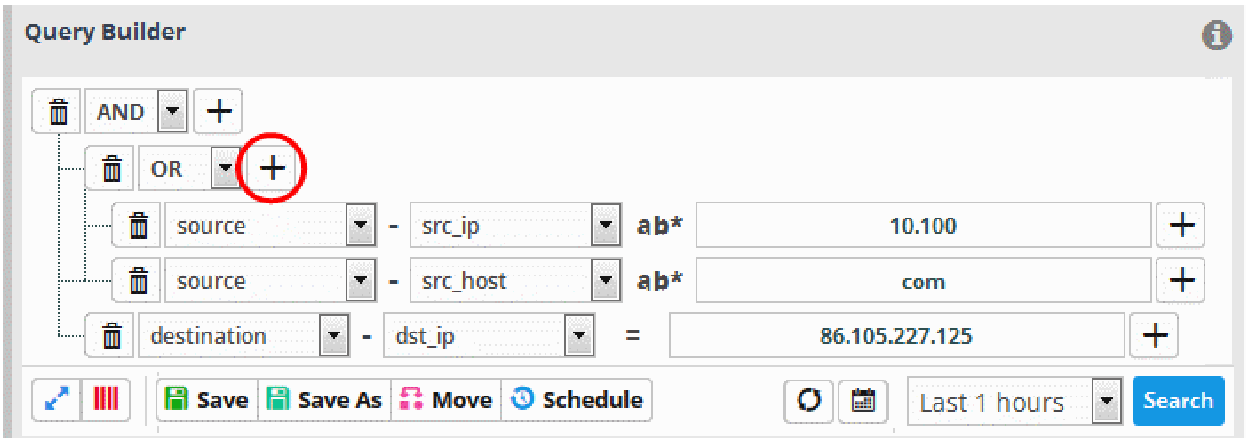
| | | |
|---|---|---|
| | | correlation rules.<br>- List updates will be immediately reflected in the queries and the rules in which they are used.<br>- See **Lists** for more details on list management.<br>On selecting **[a]** as the relation parameter, drop-down options will appear for the List and the List type:<br> <br>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'.<br>- Choose the List to be used in the query filter from the first drop-down.<br>- Choose the sub list that contains the set of values to be included in the query filter from the second drop-down.<br>All the values contained in the list will be included as values for the Field specified in the filter statement. |
| ~~[a]~~ | Not in List | Allows you to configure the filter statement to search for the events that do not contain specific values from a pre-defined list.<br>On selecting ~~[a]~~ as the relation parameter, drop-down options will appear for the List and the List type:<br> <br>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'.<br>- Choose the List to be used in the query filter from the first drop-down.<br>- Choose the sub list that contains the set of values to be input as exclusions to the query filter from the second drop-down.<br>The results will display all events that do not contain the values in the lists. |

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.

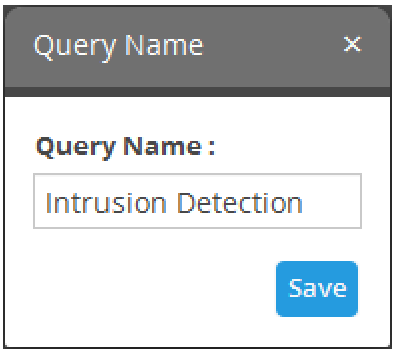


- To add a sub-filter statement, click the + button beside the filter and repeat the process.
- To set the relationship between each statement, use the drop-down menu.
- For example, the query below will return events whose source ends with 10.100 OR .com AND whose destination is 86.105.227.125



**Tip**: You can update and refine a query by adding more filters once you have seen the results.

- 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.



Query Name ×

Query Name :

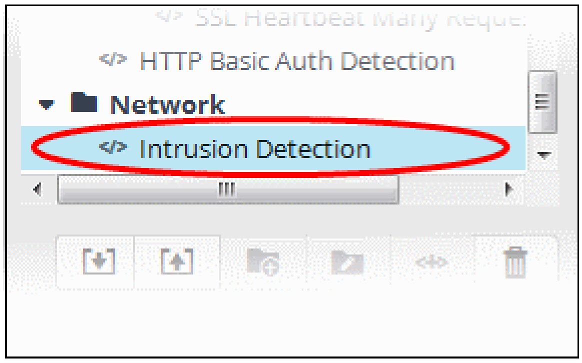
Intrusion Detection

Save

- 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.



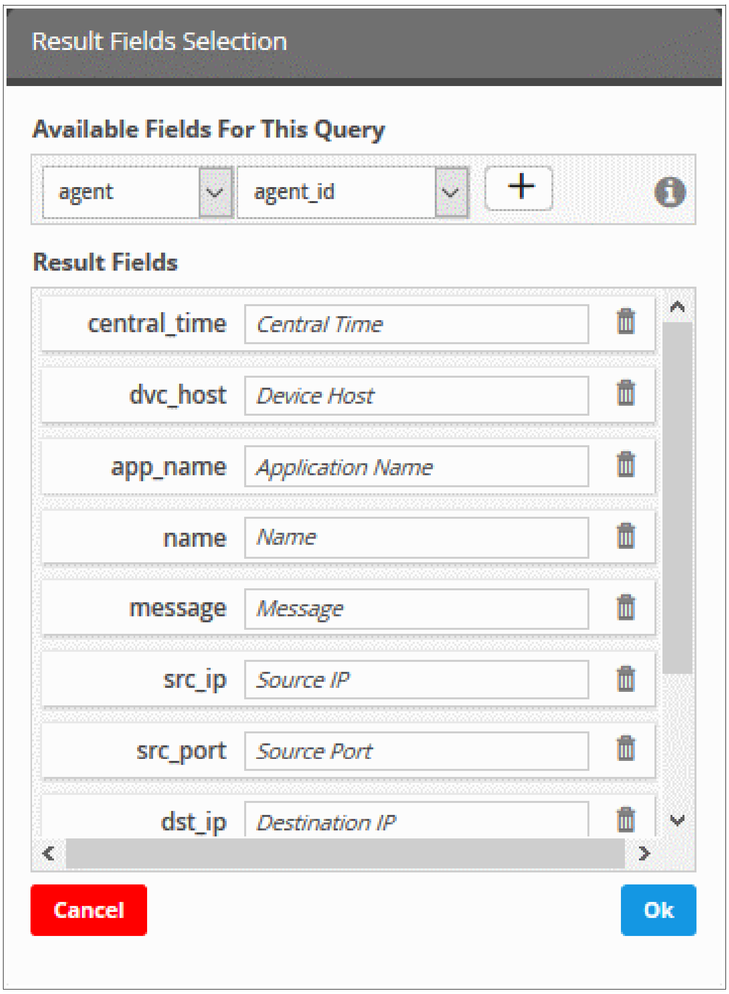
The next step is to run the event query. Before that, however, the 'Results' table must be checked and configured so that it is relevant to the event query. See '**Configure Results Table for a Query**' for more details.

### Configure the 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 side and click the |||| button from 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.



Result Fields Selection

Available Fields For This Query

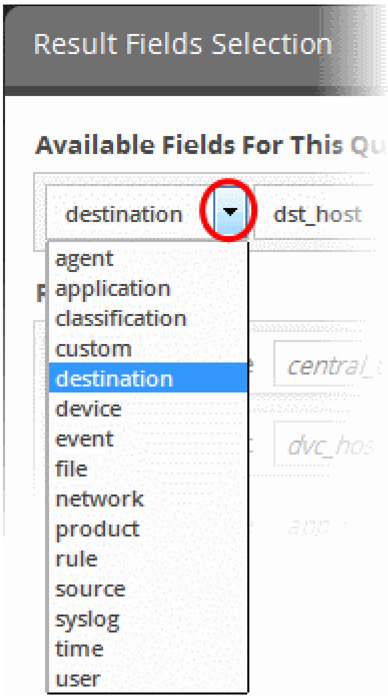
agent | agent_id

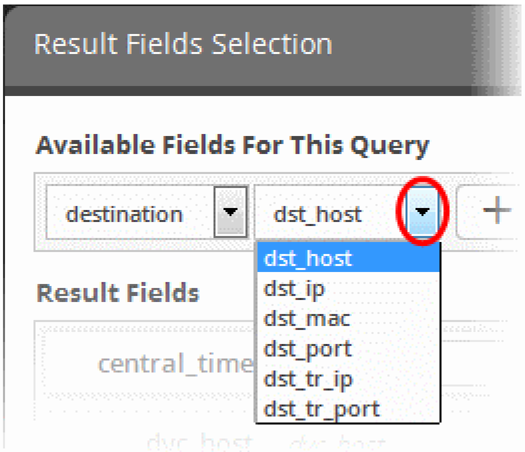
Result Fields

| | |
|---|---|
| central_time | Central Time |
| dvc_host | Device Host |
| app_name | Application Name |
| name | Name |
| message | Message |
| src_ip | Source IP |
| src_port | Source Port |
| dst_ip | Destination IP |

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.

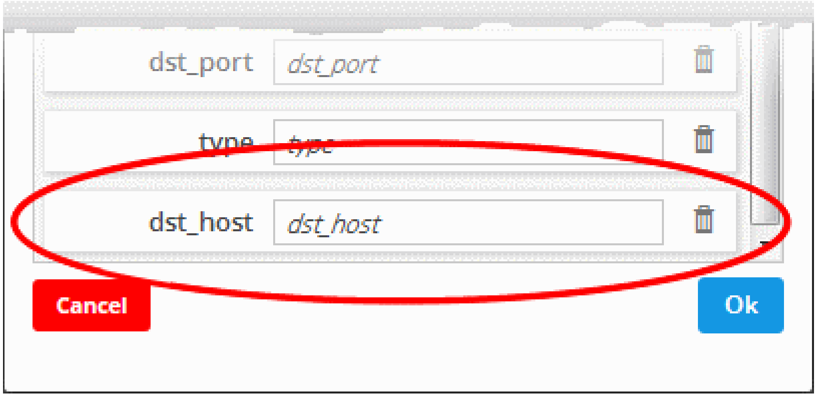




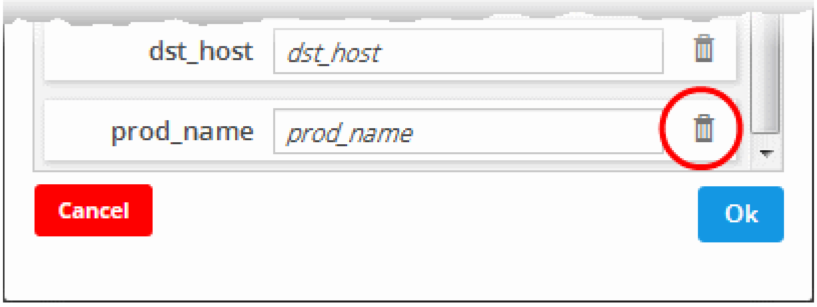
The next field will display the items available for the selected field group.

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

A new field will be added and you may provide a new label for the result field if required.



- Enter a name for the field if required, 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.



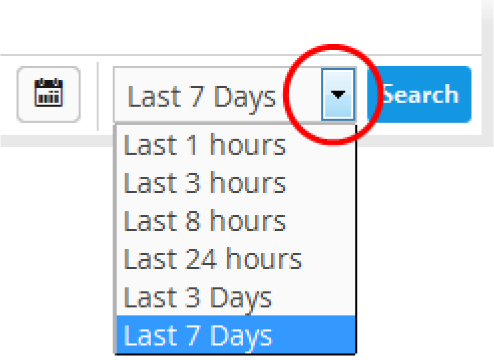
- Click the 'Ok' button

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

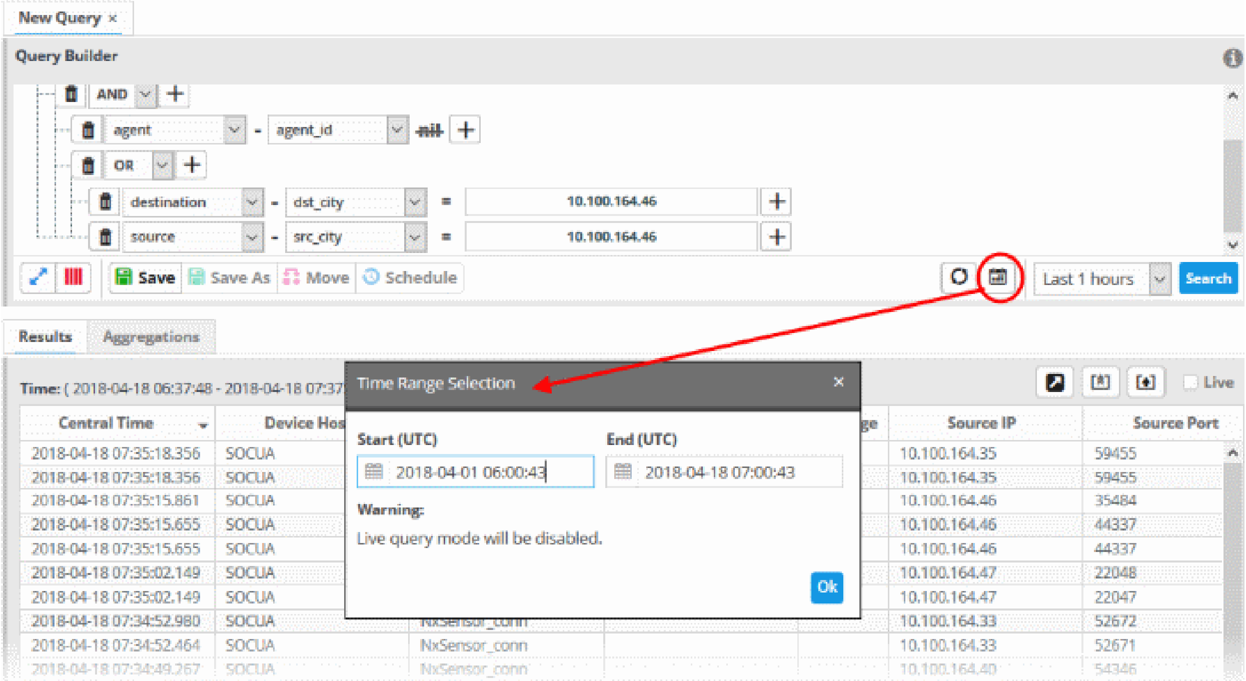
You can also refer to Comodo built-in event queries to have a better insight about configuring different types of queries.

Now that you have configured and saved an event query, the next step is to run it.

- 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'.



agent - agent_id ~~nil~~

OR

destination - dst_city = 10.100.164.46

source - src_city = 10.100.164.46

Time: ( 2018-04-18 06:37:48 - 2018-04-18 07:37

Start (UTC): 2018-04-01 06:00:43

End (UTC): 2018-04-18 07:00:43

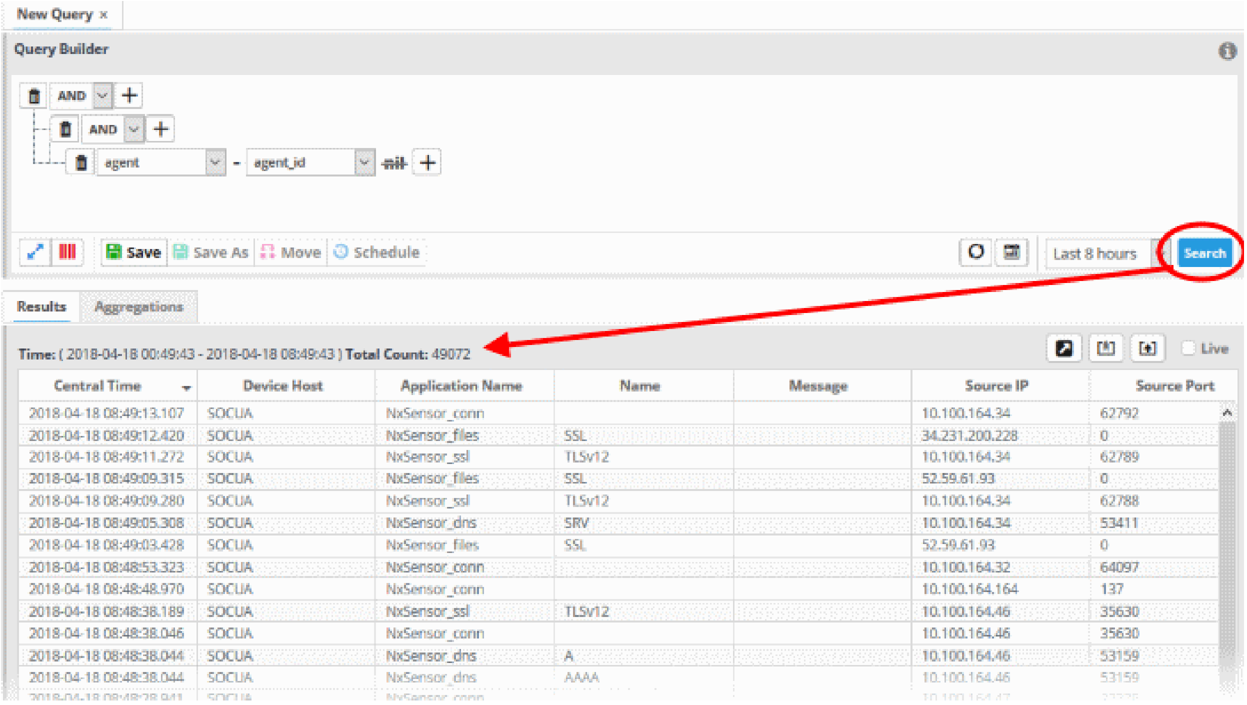
Warning:
Live query mode will be disabled.

| Central Time | Device Hos |  | Source IP | Source Port |
|---|---|---|---|---|
| 2018-04-18 07:35:18.356 | SOCUA |  | 10.100.164.35 | 59455 |
| 2018-04-18 07:35:18.356 | SOCUA |  | 10.100.164.35 | 59455 |
| 2018-04-18 07:35:15.861 | SOCUA |  | 10.100.164.46 | 35484 |
| 2018-04-18 07:35:15.655 | SOCUA |  | 10.100.164.46 | 44337 |
| 2018-04-18 07:35:15.655 | SOCUA |  | 10.100.164.46 | 44337 |
| 2018-04-18 07:35:02.149 | SOCUA |  | 10.100.164.47 | 22048 |
| 2018-04-18 07:35:02.149 | SOCUA |  | 10.100.164.47 | 22047 |
| 2018-04-18 07:34:52.980 | SOCUA | NxSensor_conn | 10.100.164.33 | 52672 |
| 2018-04-18 07:34:52.464 | SOCUA | NxSensor_conn | 10.100.164.33 | 52671 |
| 2018-04-18 07:34:49.267 | SOCUA | NxSensor_conn | 10.100.164.40 | 54346 |

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.



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 |
| 2018-04-18 08:48:28.941 | SOCUA | NxSensor_conn | | | 10.100.164.47 | [illegible] |

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**'.

For more details about event queries such as scheduling, viewing detailed results and aggregated results, managing a query folder and more see **Configuring Event Queries**.

**Tips:** You can configure other features in cWatch that will help to perform a tagged search, provide value from lists and populate events from correlation and aggregation rules:

- **Tagged Rule –** You can create rules to analyze events for criteria that you specify, then tag those events with labels of your choice. Matching events are then tagged and can be queried. See '**Managing Tagged Rules**' for more details.
- **Lists –** You can predefine values for fields, which then can be used as parameters in event queries and correlation rules. There are three types of lists, Live List, Range List and IP Range List in cWatch. See '**Lists**' for more details.
- **Correlation Rule –** A correlation rule can be configured from its Output Mappings section to generate a new event, which then can be queried. See '**Managing Correlation Rules**' for more details.
- **Aggregation Rule –** You can configure filters for two or more sub events that when the join condition is met, will create a new event. These aggregated events can be queried from the events query interface. See '**Managing Aggregation Rules**' for more details.

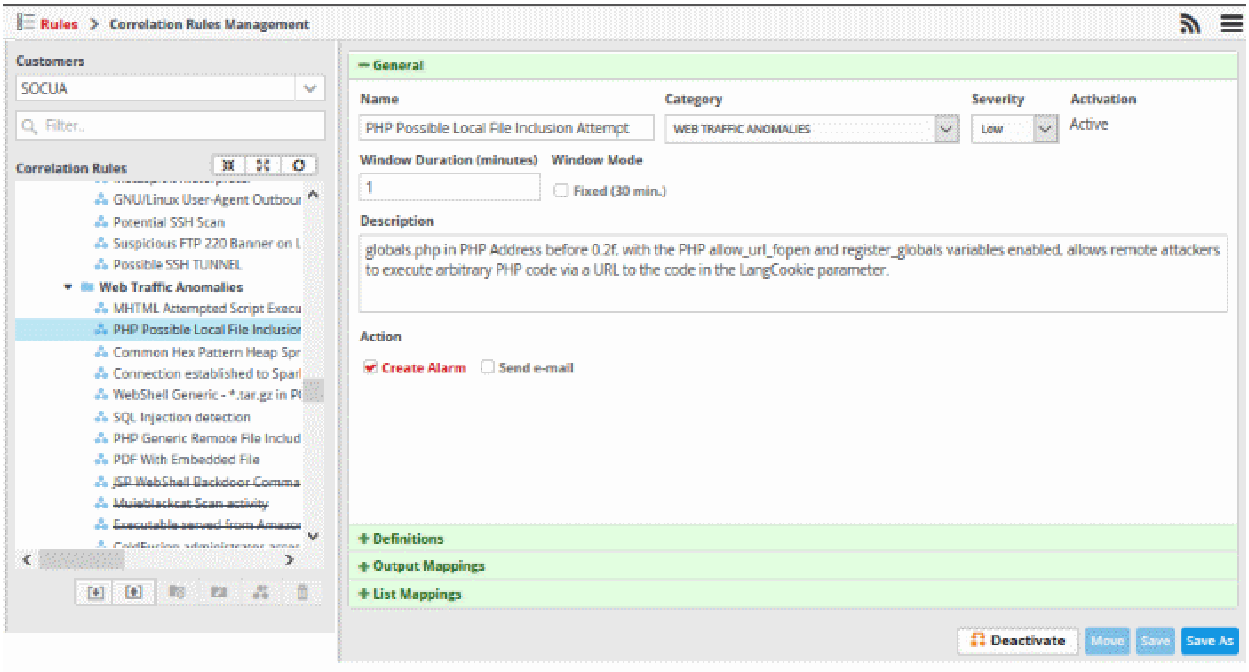
### Step 6 – Configure Correlation Rules

- The correlation rule area lets you create rules which monitor networks 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.

### To create a correlation rule

- Select a customer from the 'Customers' drop-down on the upper left:


Rules > Correlation Rules Management
Customers
Correlation Rules
GNU/Linux User-Agent Outbour
Potential SSH Scan
Suspicious FTP 220 Banner on L
Possible SSH TUNNEL
Web Traffic Anomalies
MHTML Attempted Script Execu
PHP Possible Local File Inclusior
Common Hex Pattern Heap Spr
Connection established to Spar
WebShell Generic - *.tar.gz in P
SQL Injection detection
PHP Generic Remote File Includ
PDF With Embedded File
~~JSP WebShell Backdoor Comma~~
~~Muieblackcat Scan activity~~
~~Executable served from Amazor~~
− General
+ Definitions
+ Output Mappings
+ List Mappings
Deactivate
Move
Save
Save As

Customers: SOCUA

Name: PHP Possible Local File Inclusion Attempt

Category: WEB TRAFFIC ANOMALIES

Severity: Low

Activation: Active

Window Duration (minutes): 1

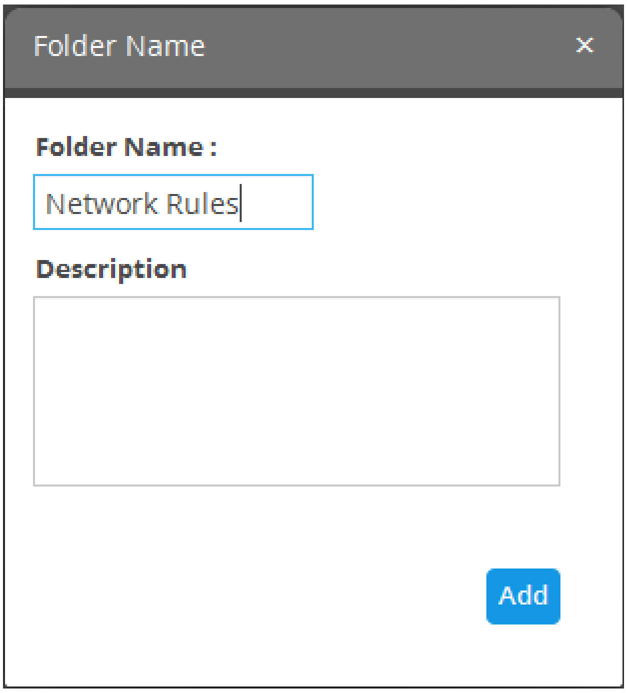
Window Mode: □ Fixed (30 min.)

Description: globals.php in PHP Address before 0.2f, with the PHP allow_url_fopen and register_globals variables enabled, allows remote attackers to execute arbitrary PHP code via a URL to the code in the LangCookie parameter.

Action: ☑ Create Alarm □ Send e-mail

A built-in correlation rule is selected by default, and its parameters shown on the right. The left-hand pane shows predefined and custom rules available for the selected customer. Before creating a correlation rule, you have to create a folder under which the rule should be saved.

- Select the appropriate rule category folder or create a new correlation rule folder under which you want to create a correlation rule.
- Click the folder button at the bottom on the left. The 'Folder Name' dialog will appear.



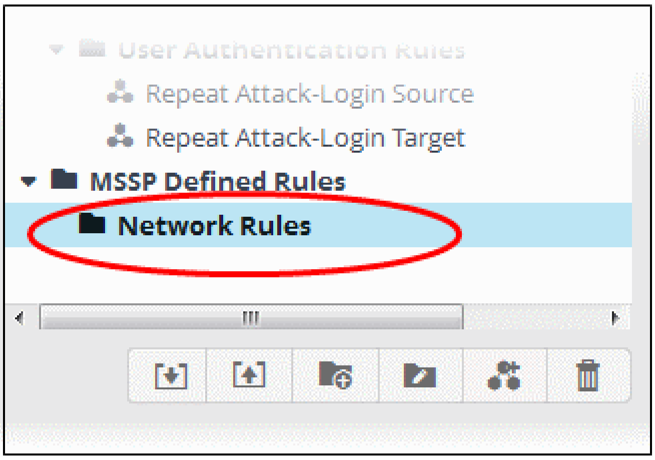
Folder Name : Network Rules

Description:

- Enter a name for the rules folder in the 'Folder Name' field

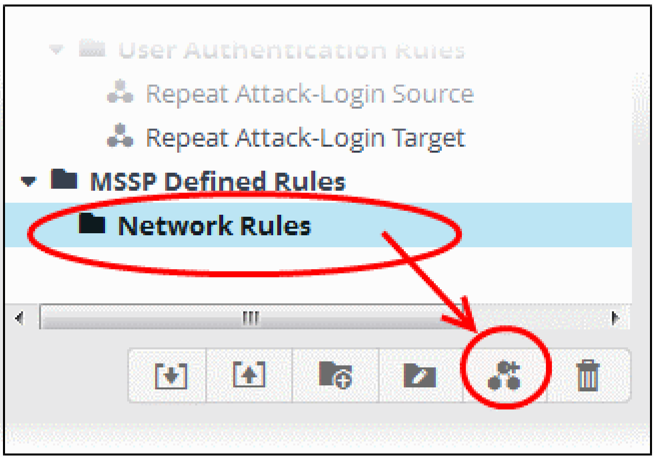
- Enter a description for the category of rules to be added to the new folder
- Click the 'Add' button

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

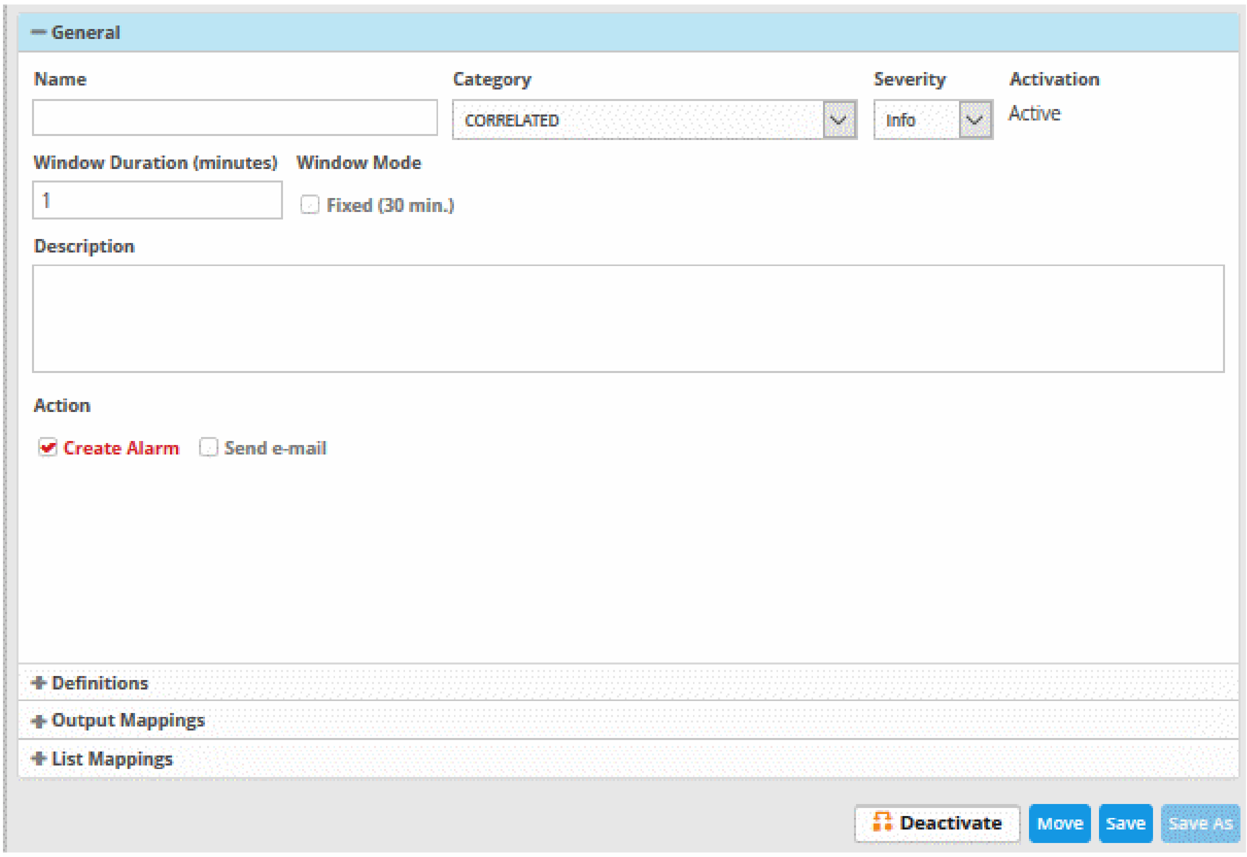

User Authentication Rules
Repeat Attack-Login Source
Repeat Attack-Login Target
MSSP Defined Rules
Network Rules

The relevant correlation rules can now be placed under the newly created folder.

- To create a correlation rule under a folder, select it and click the button.


User Authentication Rules
Repeat Attack-Login Source
Repeat Attack-Login Target
MSSP Defined Rules
Network Rules

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



− General

Name:

Category: CORRELATED

Severity: Info

Activation: Active

Window Duration (minutes): 1

Window Mode: □ Fixed (30 min.)

Description:

Action: ☑ Create Alarm □ Send e-mail

+ Definitions

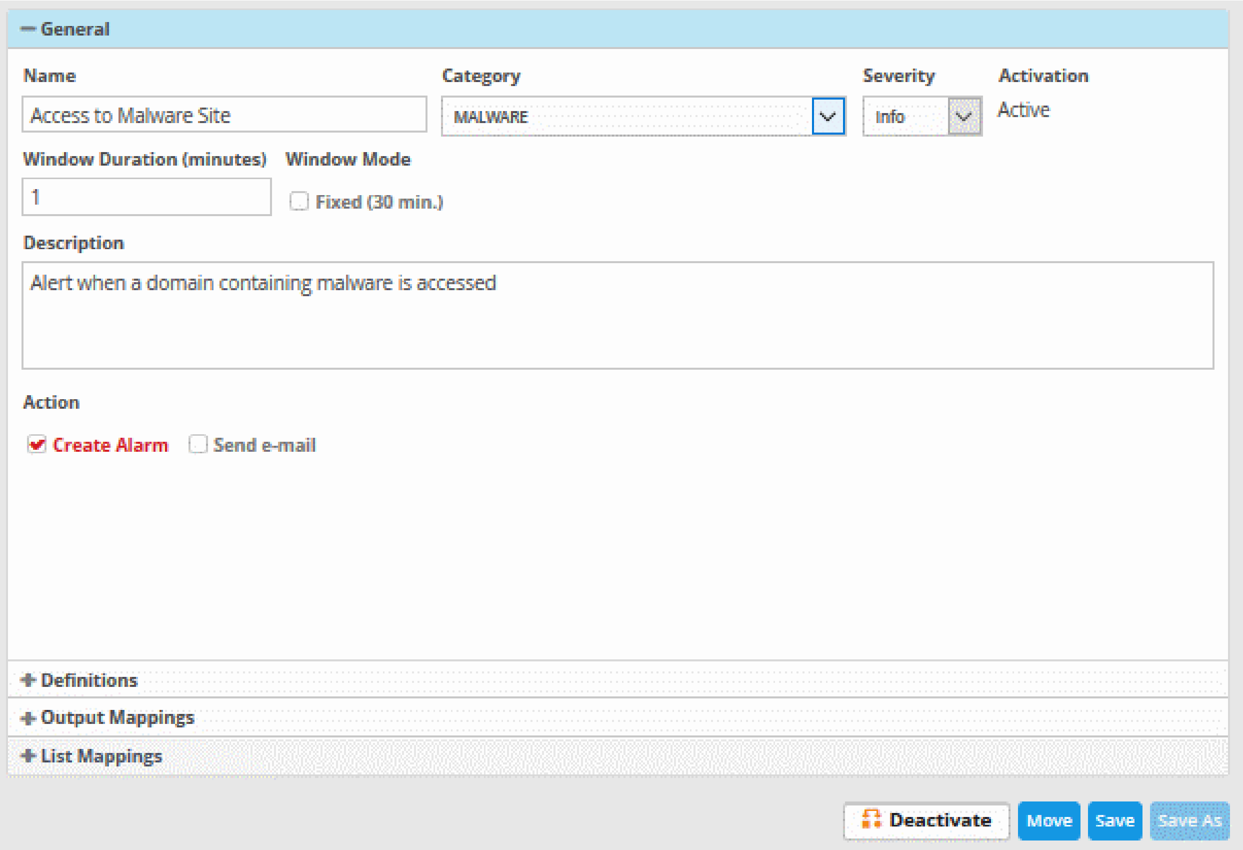
+ Output Mappings

+ List Mappings

- **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.



Name: Access to Malware Site

Category: MALWARE

Severity: Info

Activation: Active

Window Duration (minutes): 1

Window Mode: □ Fixed (30 min.)

Description: Alert when a domain containing malware is accessed

Action: ☑ Create Alarm □ Send e-mail

- **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

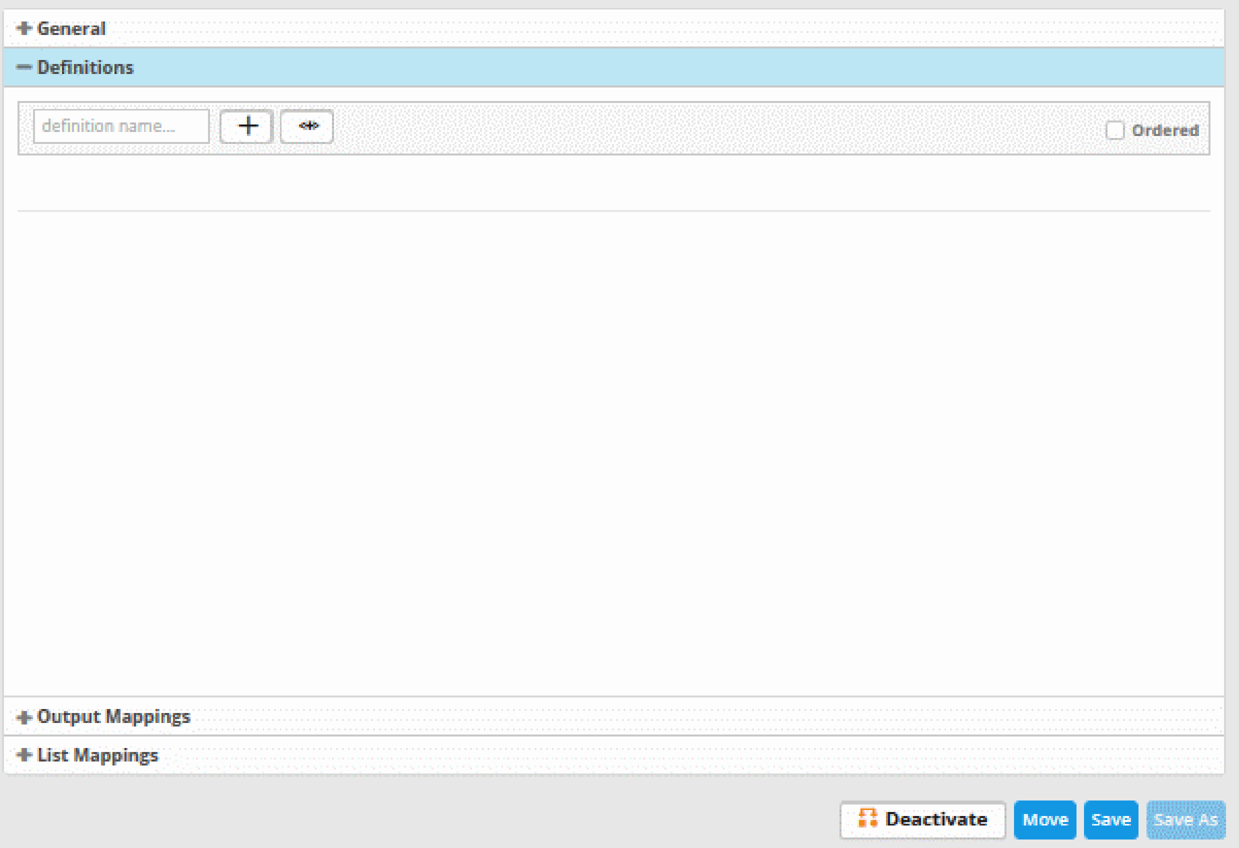
incident based on the rule.

- **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.

## 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.



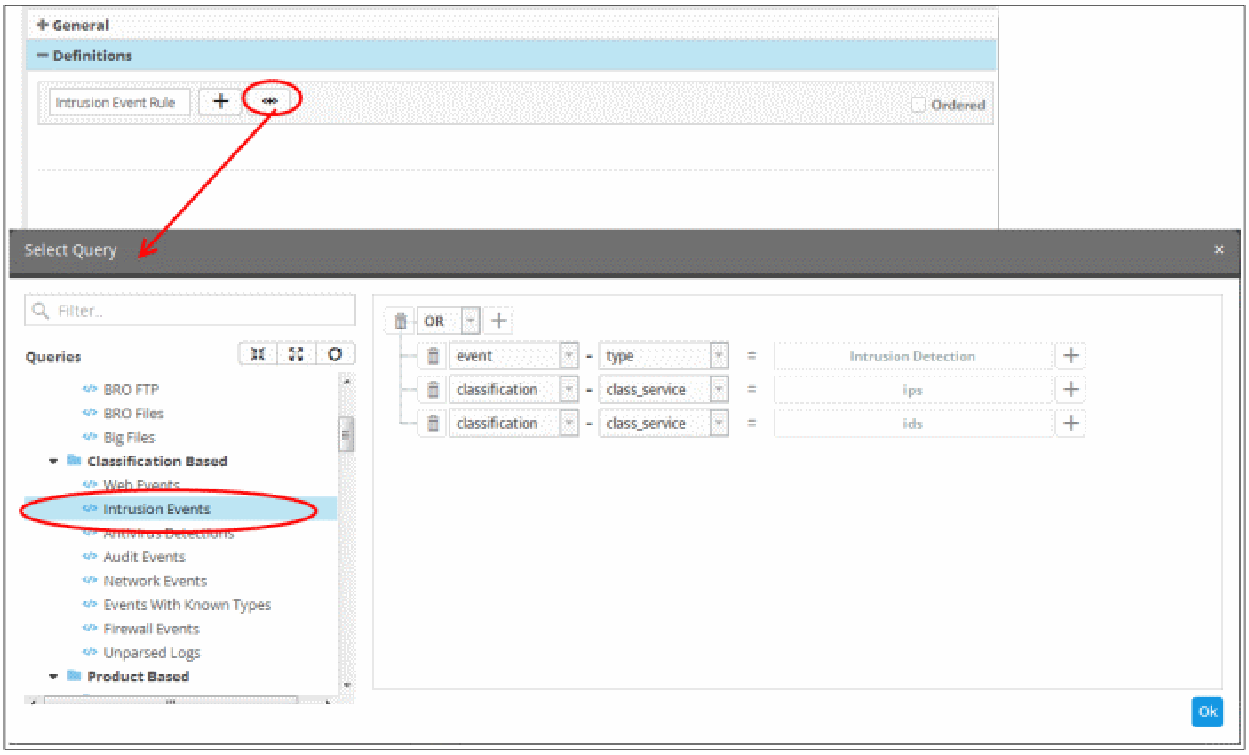
- To add a filter statement group as a rule definition, enter a name for the rule definition.

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.



+ General

− Definitions

Intrusion Event Rule

□ Ordered

Select Query

Filter..

Queries

- BRO FTP
- BRO Files
- Big Files
- Classification Based
  - Web Events
  - Intrusion Events
  - Antivirus Detections
  - Audit Events
  - Network Events
  - Events With Known Types
  - Firewall Events
  - Unparsed Logs
- Product Based

OR

| | | | | |
|---|---|---|---|---|
| event | - | type | = | Intrusion Detection |
| classification | - | class_service | = | ips |
| classification | - | class_service | = | ids |

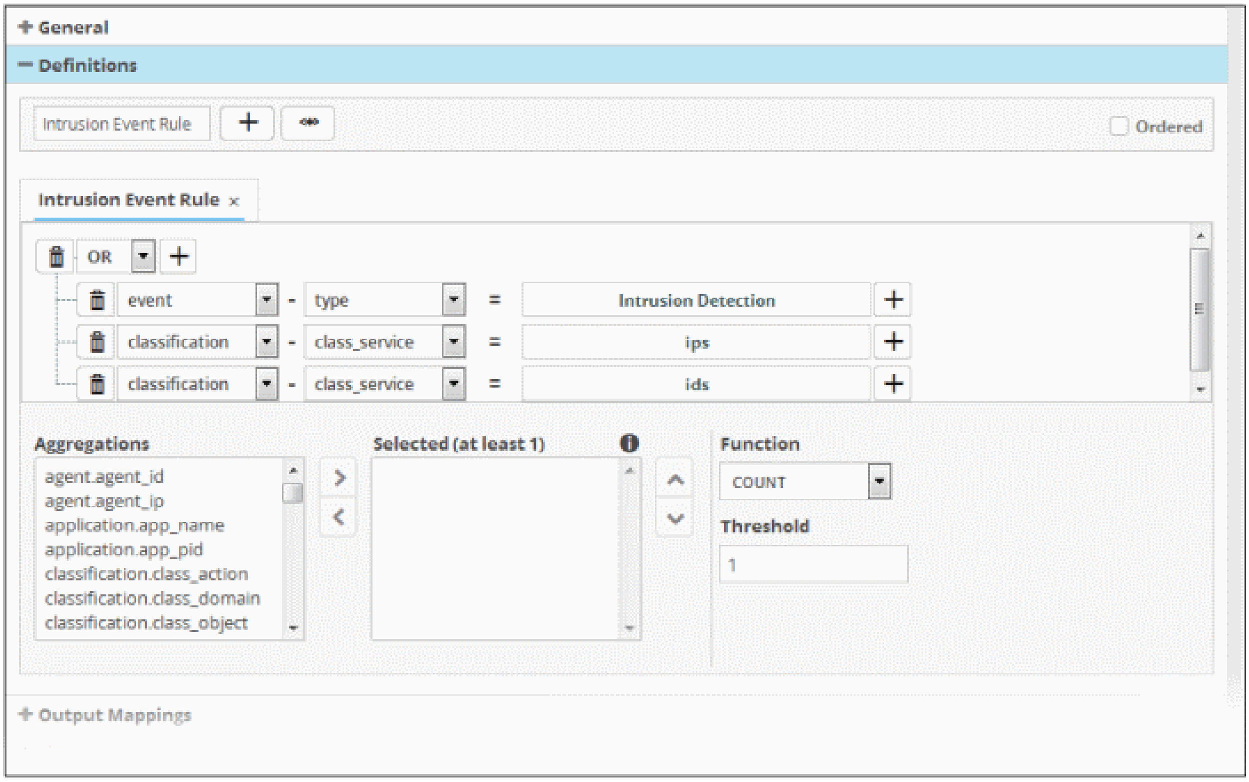
The 'Select Query' dialog will open with a list of pre-defined and custom event queries added for the customer in the left pane.

- 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 .



+ General

− Definitions

Intrusion Event Rule

□ Ordered

Intrusion Event Rule ×

OR

| | | | | |
|---|---|---|---|---|
| event | - | type | = | Intrusion Detection |
| classification | - | class_service | = | ips |
| classification | - | class_service | = | ids |

Aggregations

agent.agent_id
agent.agent_ip
application.app_name
application.app_pid
classification.class_action
classification.class_domain
classification.class_object

Selected (at least 1)

Function: COUNT

Threshold: 1

+ Output Mappings

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'. This is similar to building an event query. **Click here** to see the details.

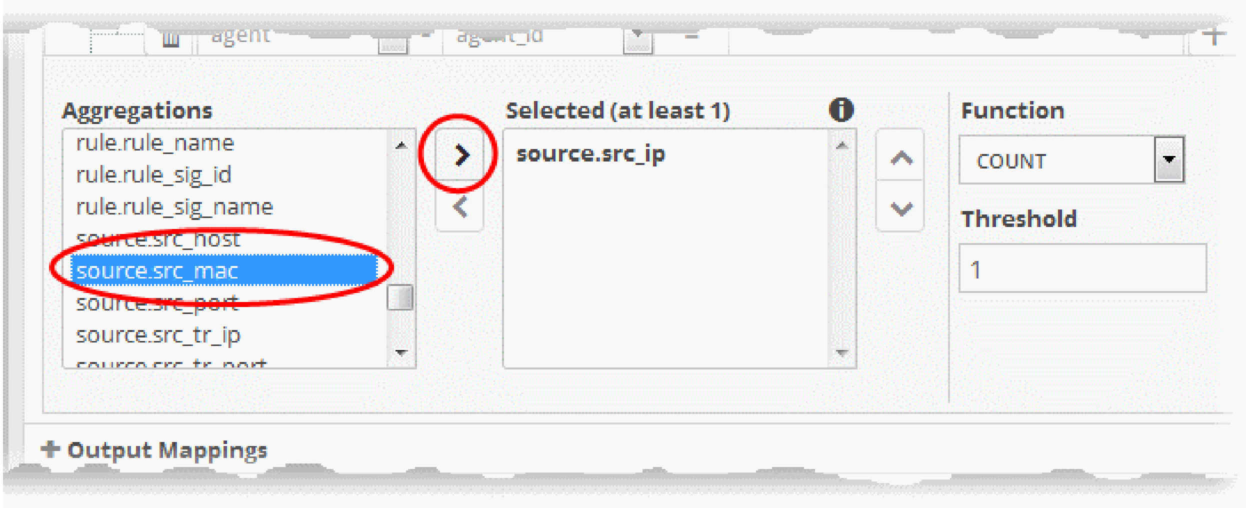
You can add multiple query definitions for a single rule and these are tied together.

- 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 and if any destination IP of the second tab matches the destination IP of the first tab, then an incident is created. Please note the number of selected aggregates should be equal for all the 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.

The next step is to select the field values based on which the events that meet the rule are to be aggregated to create the incident.. 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 from 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.



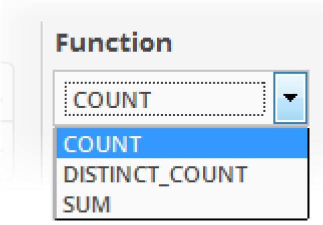
Selected (at least 1): source.src_ip

Function: COUNT

Threshold: 1

- 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 *(Optional)*

- 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.
- This is optional and for full details, see '**Manage Correlation Rules**'.

### List Mappings *(Optional)*

- 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.
- This is optional and for full details see '**Manage Correlation Rules**', '**Manage Live Lists**' and '**Manage Live List Content**'.
- You can also export and import correlation rules from one customer to another customer. See '**Manage Correlation Rules**' for more details.

### Step 7 – Manage Incidents

- cWatch will generate an 'Incident' when it identifies events which match a correlation rule.
- 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.

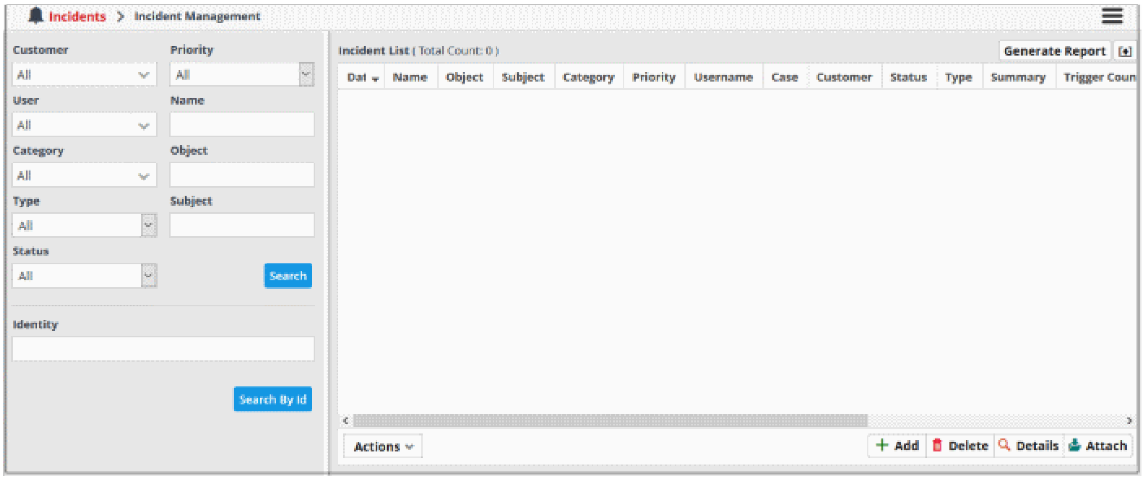
- The number of open incidents is shown beside the notification icon in the title bar.

## Manage Incidents

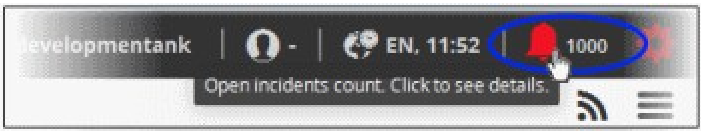
### To manage incidents

- Click the 'Menu' button > 'Incidents' > 'Incident Management'.
- The 'Incident Management' screen lists recent incidents along with details such as customer network, the user to whom it is assigned and so on.
- You can view incident details, reassign them to different users, close/re-open incidents and more.

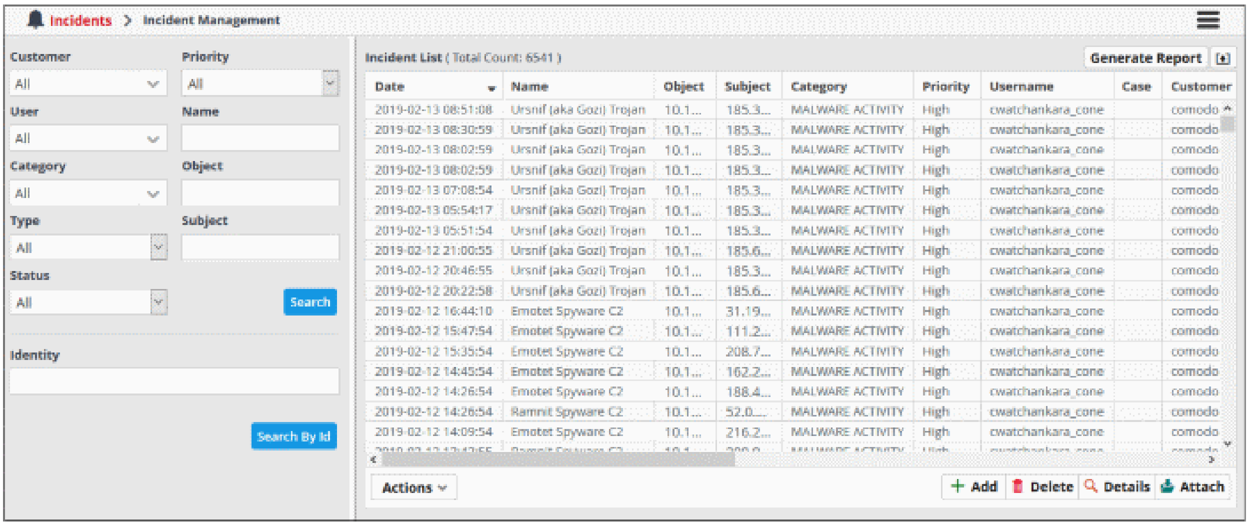
The 'Incident Management' screen:



- 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:



The example below shows all incidents from all customer networks.



Incident List ( Total Count: 6541 )

| Date | Name | Object | Subject | Category | Priority | Username | Case | Customer |
|---|---|---|---|---|---|---|---|---|
| 2019-02-13 08:51:08 | Ursnif (aka Gozi) Trojan | 10.1... | 185.3... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-13 08:30:59 | Ursnif (aka Gozi) Trojan | 10.1... | 185.3... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-13 08:02:59 | Ursnif (aka Gozi) Trojan | 10.1... | 185.3... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-13 08:02:59 | Ursnif (aka Gozi) Trojan | 10.1... | 185.3... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-13 07:08:54 | Ursnif (aka Gozi) Trojan | 10.1... | 185.3... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-13 05:54:17 | Ursnif (aka Gozi) Trojan | 10.1... | 185.3... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-13 05:51:54 | Ursnif (aka Gozi) Trojan | 10.1... | 185.3... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-12 21:00:55 | Ursnif (aka Gozi) Trojan | 10.1... | 185.6... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-12 20:46:55 | Ursnif (aka Gozi) Trojan | 10.1... | 185.3... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-12 20:22:58 | Ursnif (aka Gozi) Trojan | 10.1... | 185.6... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-12 16:44:10 | Emotet Spyware C2 | 10.1... | 31.19... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-12 15:47:54 | Emotet Spyware C2 | 10.1... | 111.2... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-12 15:35:54 | Emotet Spyware C2 | 10.1... | 208.7... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-12 14:45:54 | Emotet Spyware C2 | 10.1... | 162.2... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-12 14:26:54 | Emotet Spyware C2 | 10.1... | 188.4... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-12 14:26:54 | Ramnit Spyware C2 | 10.1... | 52.0.... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |
| 2019-02-12 14:09:54 | Emotet Spyware C2 | 10.1... | 216.2... | MALWARE ACTIVITY | High | cwatchankara_cone | | comodo |

From this interface you can:

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

See '**Managing Incidents**' for more details.

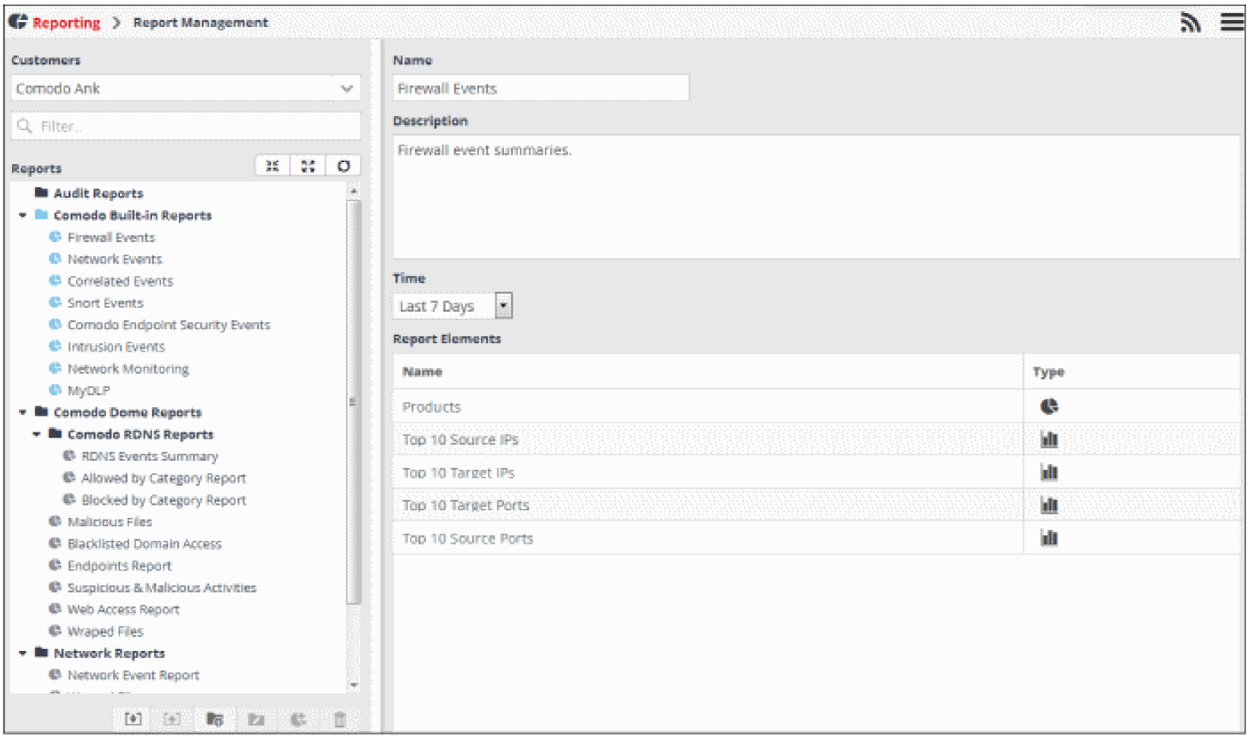
## Step 8 – Generate Reports

- 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 from from one hour up 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 generate reports

- To open the 'Report Management' interface:
  - Click the hamburger button at top-right
  - Select 'Reporting' then 'Report Management':

The 'Report Management' screen will open:



Reporting > Report Management

Customers: Comodo Ank

Filter..

Reports

- Audit Reports
- Comodo Built-in Reports
  - Firewall Events
  - Network Events
  - Correlated Events
  - Snort Events
  - Comodo Endpoint Security Events
  - Intrusion Events
  - Network Monitoring
  - MyDLP
- Comodo Dome Reports
  - Comodo RDNS Reports
    - RDNS Events Summary
    - Allowed by Category Report
    - Blocked by Category Report
  - Malicious Files
  - Blacklisted Domain Access
  - Endpoints Report
  - Suspicious & Malicious Activities
  - Web Access Report
  - Wraped Files
- Network Reports
  - Network Event Report

Name: Firewall Events

Description: Firewall event summaries.

Time: Last 7 Days

Report Elements

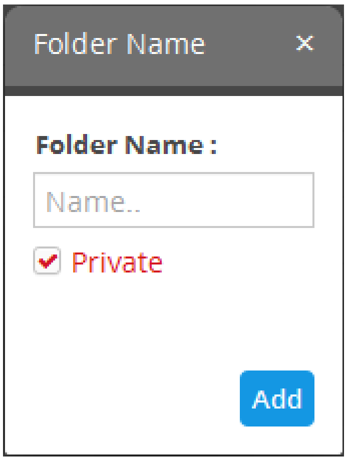
| Name | Type |
|---|---|
| Products | ◕ |
| Top 10 Source IPs | 📊 |
| Top 10 Target IPs | 📊 |
| Top 10 Target Ports | 📊 |
| Top 10 Source Ports | 📊 |

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.

### Generate reports for custom report queries

Before creating a custom report query, you have to create a report folder for the selected customer.

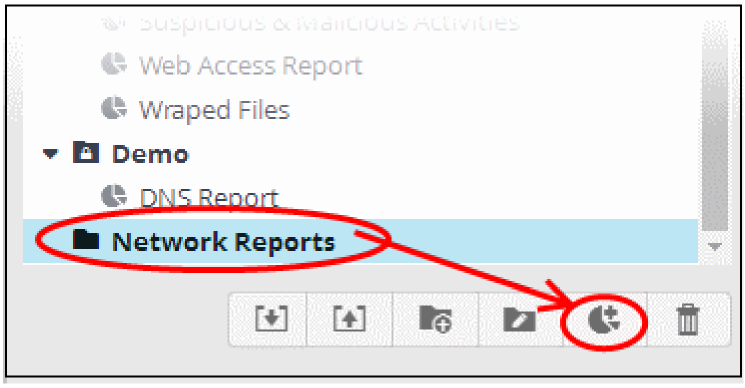
- Click the button at the bottom of the left pane. You can also create a new top level folder. The Folder Name dialog will appear.



- 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

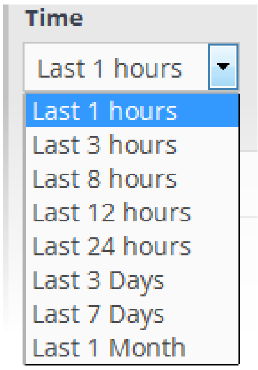
The newly created report folder will be listed. A lock icon will be displayed on the folder icon if the folder is created as a private folder.

- To create a report query, select the folder and click the button



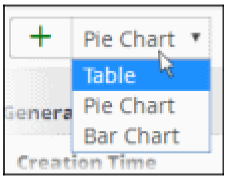
The configuration screen for creating the new report will be displayed in the right hand side panel.

- 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.

- Select the type of report element that should be added, from the drop-down at the bottom of the 'Report Elements' area.

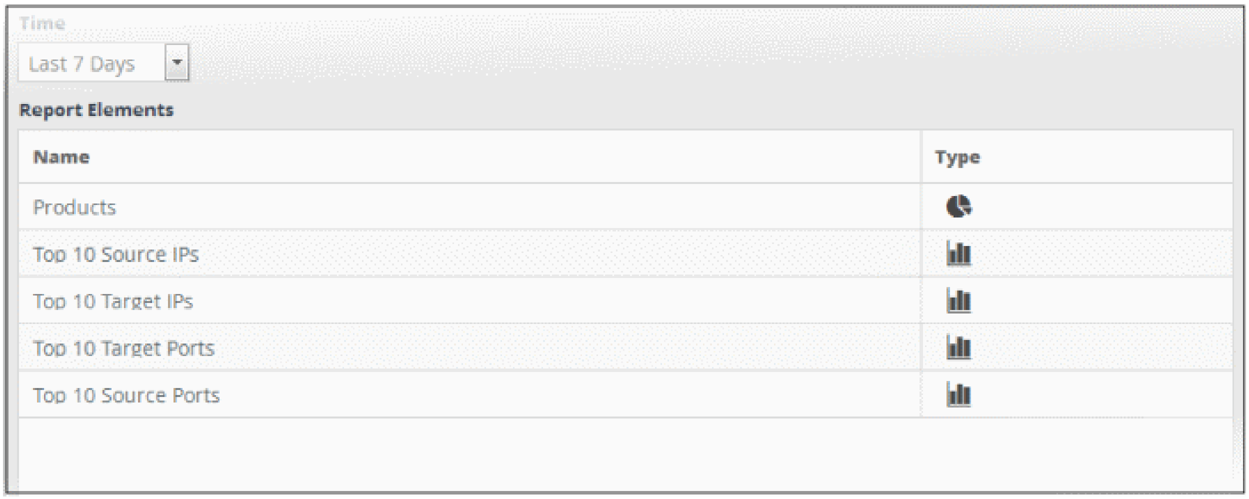


  - **Table -** A 'Table' report is configured by selecting an event query from the list of queries added for the customer. The report contain details of events that match the query in the selected time period.
  - **Pie Chart -** This report contains a pie-chart showing the statistical summary of the events that are aggregated based on parameters configured for the chart.
  - **Bar Chart -** This report contains a bar-chart showing the statistical summary of the events that are aggregated based on parameters configured for the chart.

- After selecting the type of report element, click the + button beside it.

The 'Add' screen for the selected report element will be displayed. The interface allows to select an existing query or create a new query. For more details about creating report element, see '**Managing Reports**'.

The configured report elements will be added to the list.



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 | 📊 |

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.

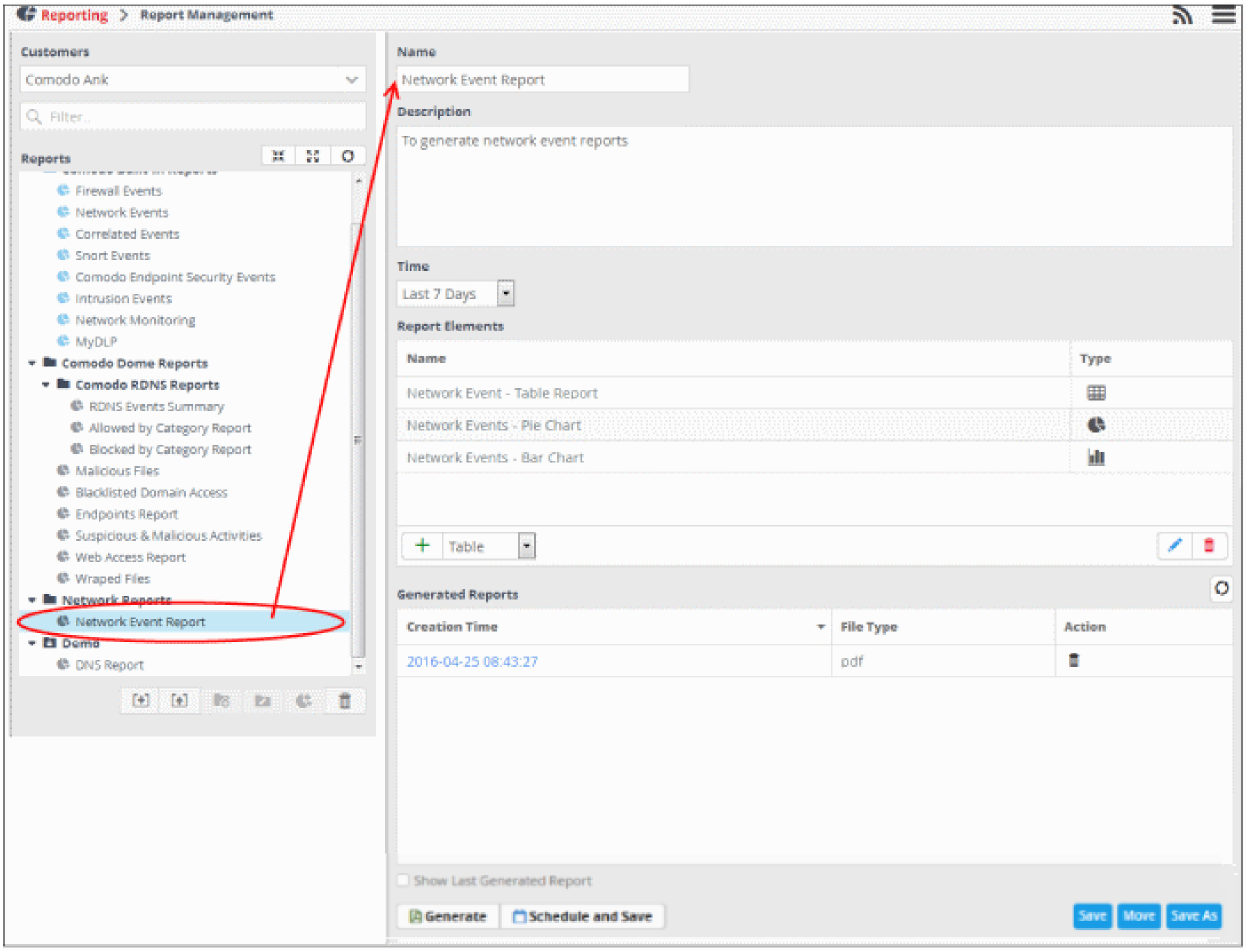
You can add as many report elements as required for a report.

- 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.

**To manually generate a report**

- 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.



Customers: Comodo Ank

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 | 🗑 |

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.

You can also schedule a report generation. For more details about generating reports, see '**Manage Reports**'.

# 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 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**