Comodo

Next Generation Security Information and Event Management

Software Version 1.4

Quick Start Guide

Guide Version 1.4.011817

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

1 Comodo NxSIEM Quick Start Guide

This tutorial explains how an administrators can setup Comodo NxSIEM.

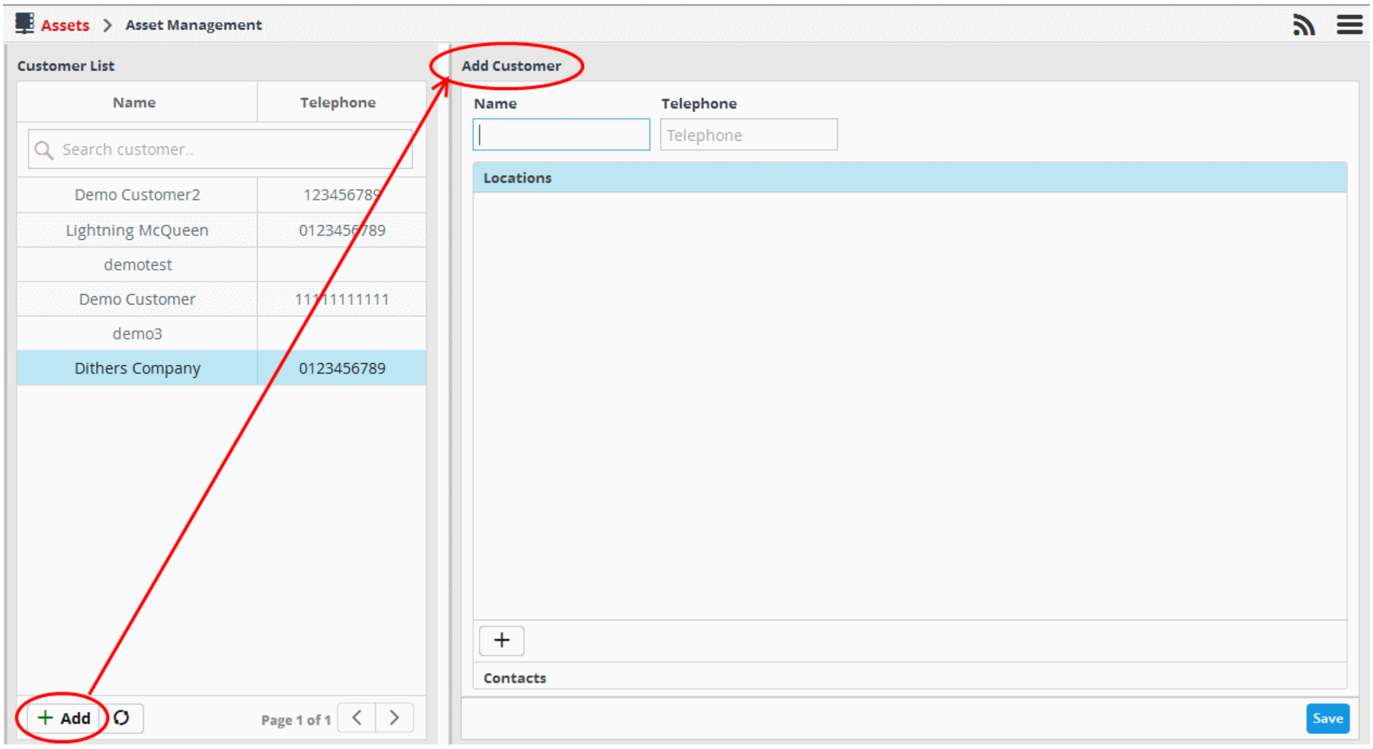
The guide will take you through the following processes - click on any link to go straight to that section as per your current requirements.

Step 1 - Enroll customers and assign users

The first step in configuring NxSIEM is to add customers and to assign admin users to these customers who can attend to incidents arising from their networks.

To add a customer

- Open the 'Asset Management' interface by clicking the 'Menu' button at the top right, then click 'Assets' > 'Asset Management'.
- Click the 'Add' button at the bottom of the 'Customer List' pane on the left. The 'Add Customer' screen will be displayed on the right:



Name	Telephone
Demo Customer2	123456789
Lightning McQueen	0123456789
demotest	
Demo Customer	11111111111
demo3	
Dithers Company	0123456789

Name	Telephone
	Telephone

- Enter the name of customer and their telephone number in the respective fields.
- To add the address details for the customer, select the 'Location' stripe then click the + button at the bottom.

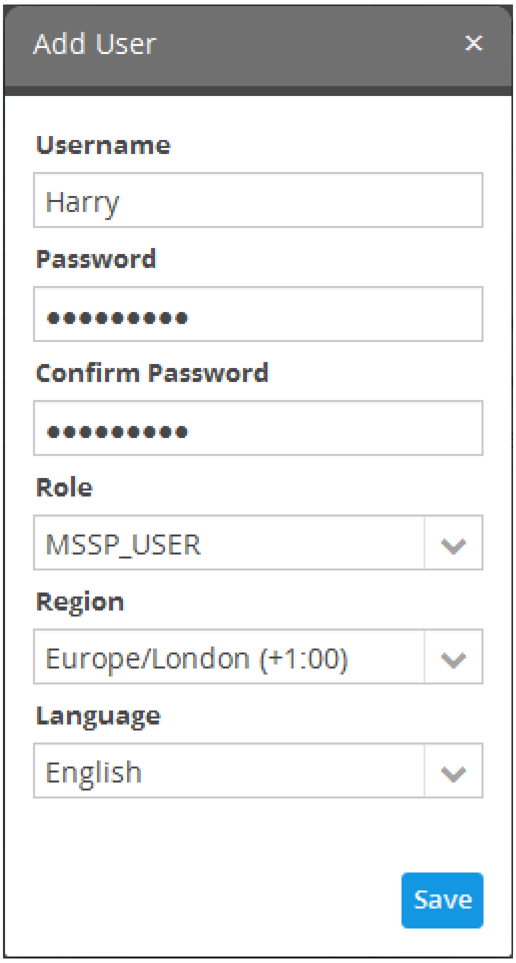
  - Repeat the process to add more locations for the customer.

- To add contact details for the customer, select the 'Contacts' stripe then click the + button at the bottom..
  - Enter the Name, Email address and Phone number of the contact person in the 'Add Contact person' dialog and click 'Add'.
  - Repeat the process to add more contact persons.
- Click the 'Save' when you are finished.

The customer will be added and you can repeat the process to add more customers.

To add and assign administrative users to attend customer networks

- Open the 'User Management' interface by clicking the 'Menu' button, then 'Administration' > 'User Management'.
- To add a new user, click the 'Add' button at the bottom of the 'User List' pane on the left. The 'Add User' dialog will appear.



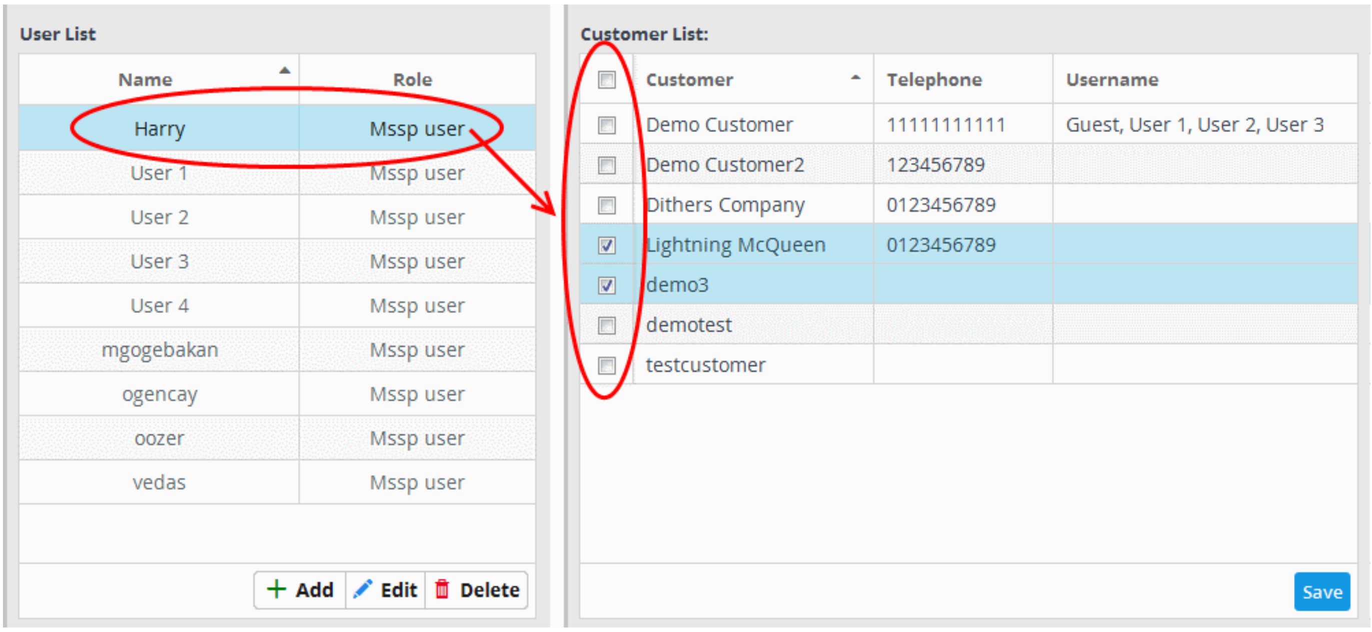
Username: Harry
Password: •••••••••
Confirm Password: •••••••••
Role: MSSP_USER
Region: Europe/London (+1:00)
Language: English

  - **Username and Password-** Enter a user-name and password for the user. Passwords should be at least 8 characters long and should contain at least one uppercase letter, one lowercase letter and one numeric character.
  - **Role -** Select the role to be assigned for the user. Currently only one role, 'MSSP_User' is available. More roles will be added in future releases.
  - **Region -** Choose the region and time zone to which the user belongs.
  - **Language -** Choose the language in which the NxSIEM web console is to be displayed to the user.

- Click the 'Save' button.

The user will be displayed in the 'User List'. You can repeat the process to add more users.

- To assign a user to a customer(s), first choose a user from the 'User List' on the left.
- Select the customer(s) to whom the user should be assigned from the 'Customer List' on the right:



User List

Name	Role
Harry	Mssp user
User 1	Mssp user
User 2	Mssp user
User 3	Mssp user
User 4	Mssp user
mgogebakan	Mssp user
ogencay	Mssp user
oozer	Mssp user
vedas	Mssp user

Customer List:

□	Customer	Telephone	Username
□	Demo Customer	11111111111	Guest, User 1, User 2, User 3
□	Demo Customer2	123456789	
□	Dithers Company	0123456789	
☑	Lightning McQueen	0123456789	
☑	demo3		
□	demotest		
□	testcustomer		

- Click the 'Save' button.

Step 2 - Add customer networks for monitoring

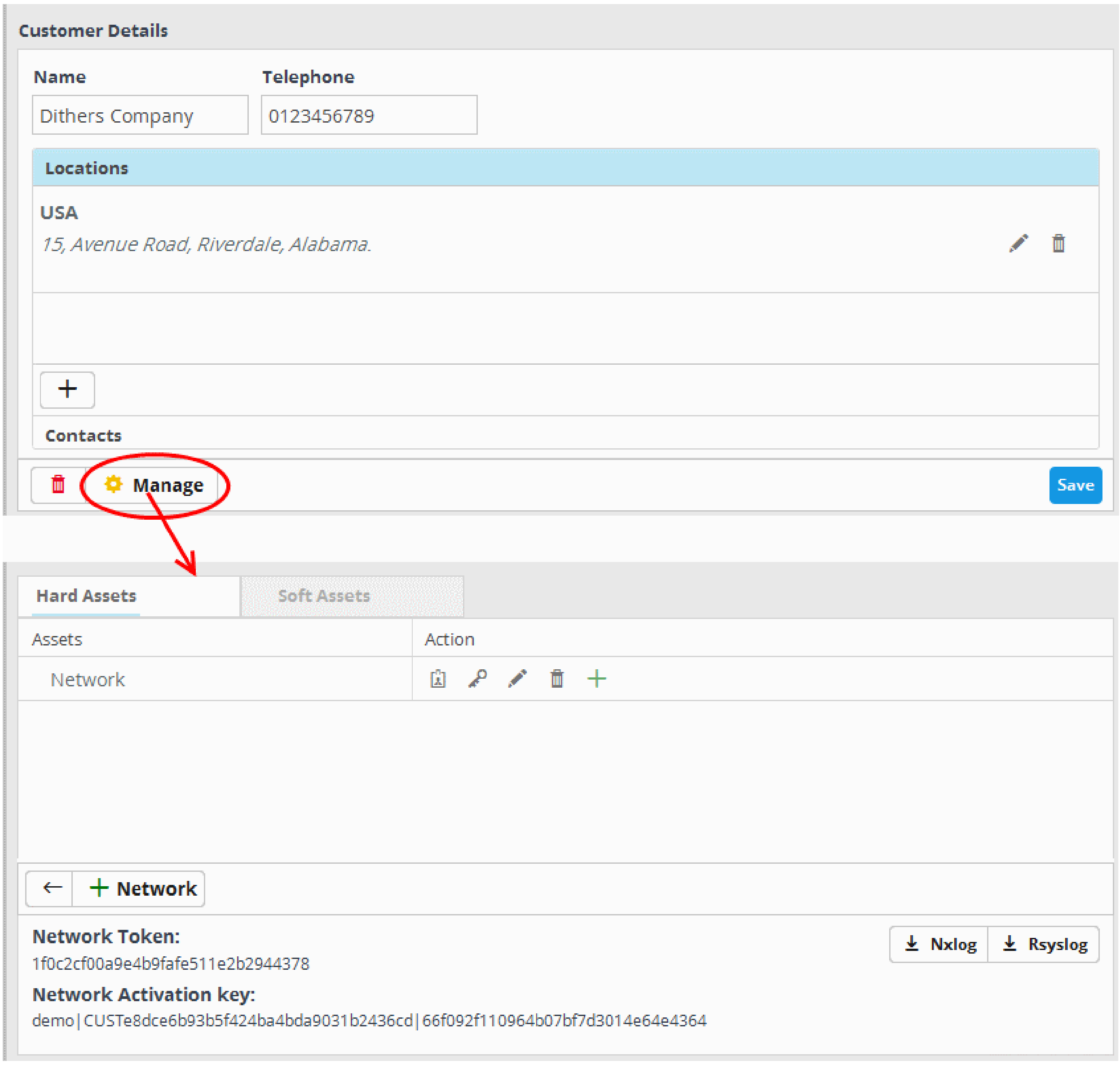
In order to collect logs and monitor events on customer networks, administrators need to add the customer's network assets to NxSIEM. Optionally, the administrator can also enroll the software assets (such as services) that they wish to monitor.

To add customer networks to NxSIEM

- 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

The Customer Details pane will open on the right.

- Click 'Manage' at the bottom left of the details pane:



Customer Details

Name: Dithers Company

Telephone: 0123456789

Locations

USA

15, Avenue Road, Riverdale, Alabama.

Contacts

Assets	Action
Network	

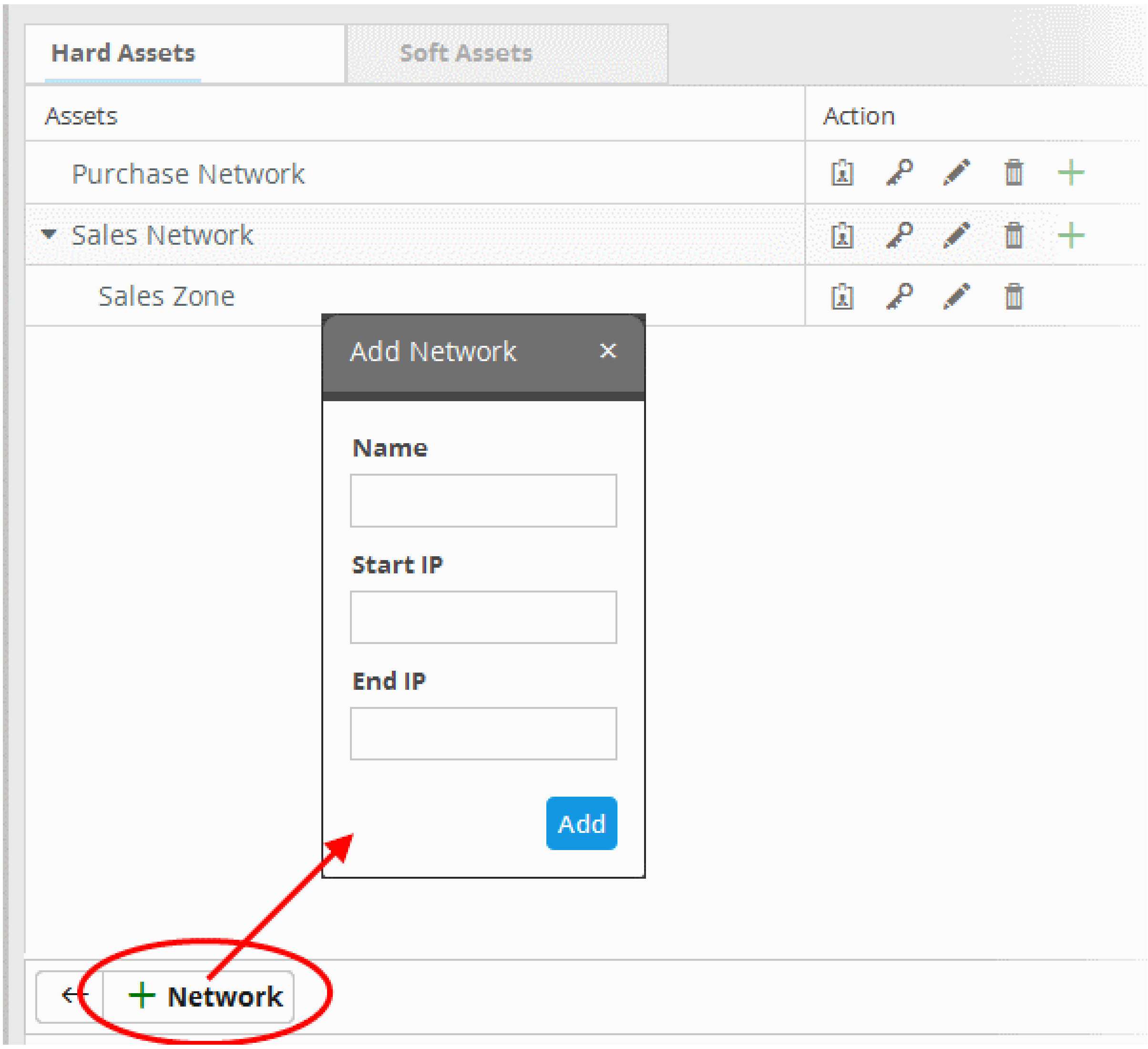
Network Token:
1f0c2cf00a9e4b9fafe511e2b2944378

Network Activation key:
demo|CUSTe8dce6b93b5f424ba4bda9031b2436cd|66f092f110964b07bf7d3014e64e4364

The interface to add 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. For each network,
  - A unique activation key is generated for the log collection agent installed on the endpoints and configure the agents to send logs to NxSIEM.
  - Configuration files for RSYSLOG and NXLOG utilities are generated for directly running on endpoints with RSYSLOG and NXLOG utilities respectively, for them to send logs to NXSIEM server.
- **Soft Assets** - Allows you to add soft assets like services hosted from the network by specifying their URL, website and so on. For details on adding soft assets, refer to the Administrative Guide at **https://help.comodo.com/topic-325-1-675-8367-Soft-Assets.html**.
- To add hard-assets:

- Click the 'Hard Assets' tab and then click the 'Network' button at the bottom of the right pane.

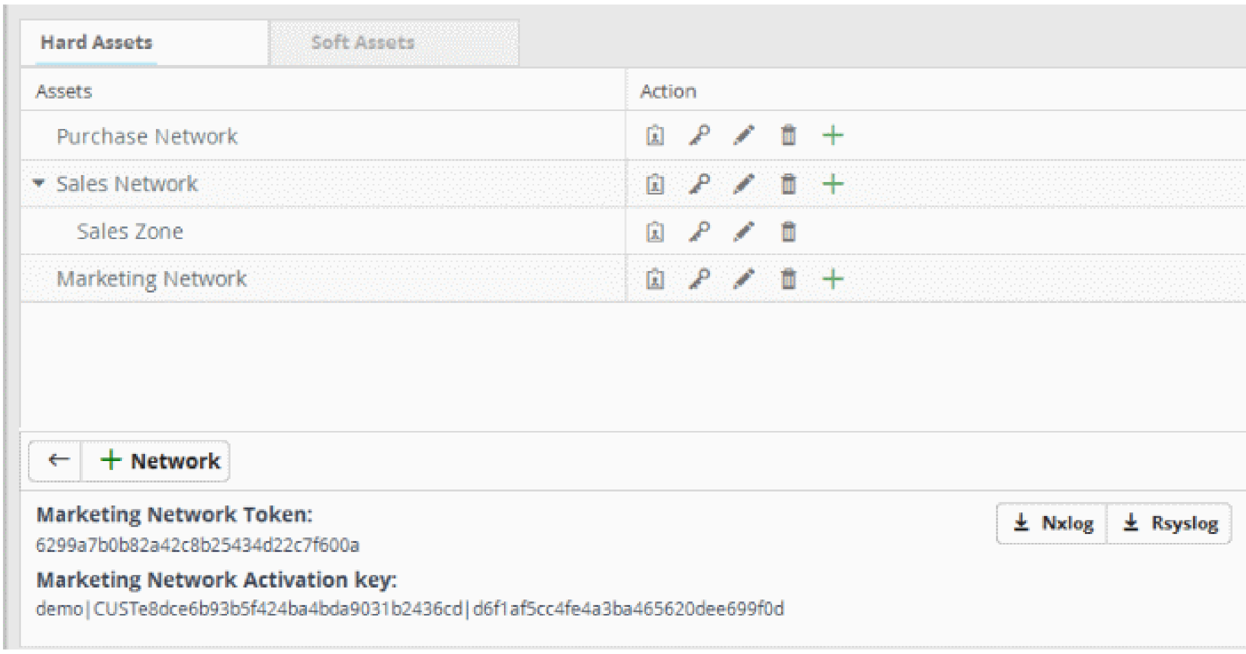


The 'Add Network' dialog will appear.

- **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.

- 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.



Assets	Action
Purchase Network	
Sales Network	
Sales Zone	
Marketing Network	

Marketing Network Token:
6299a7b0b82a42c8b25434d22c7f600a

Marketing Network Activation key:
demo|CUSTe8dce6b93b5f424ba4bda9031b2436cd|d6f1af5cc4fe4a3ba465620dee699f0d

- Repeat the process to add more networks.

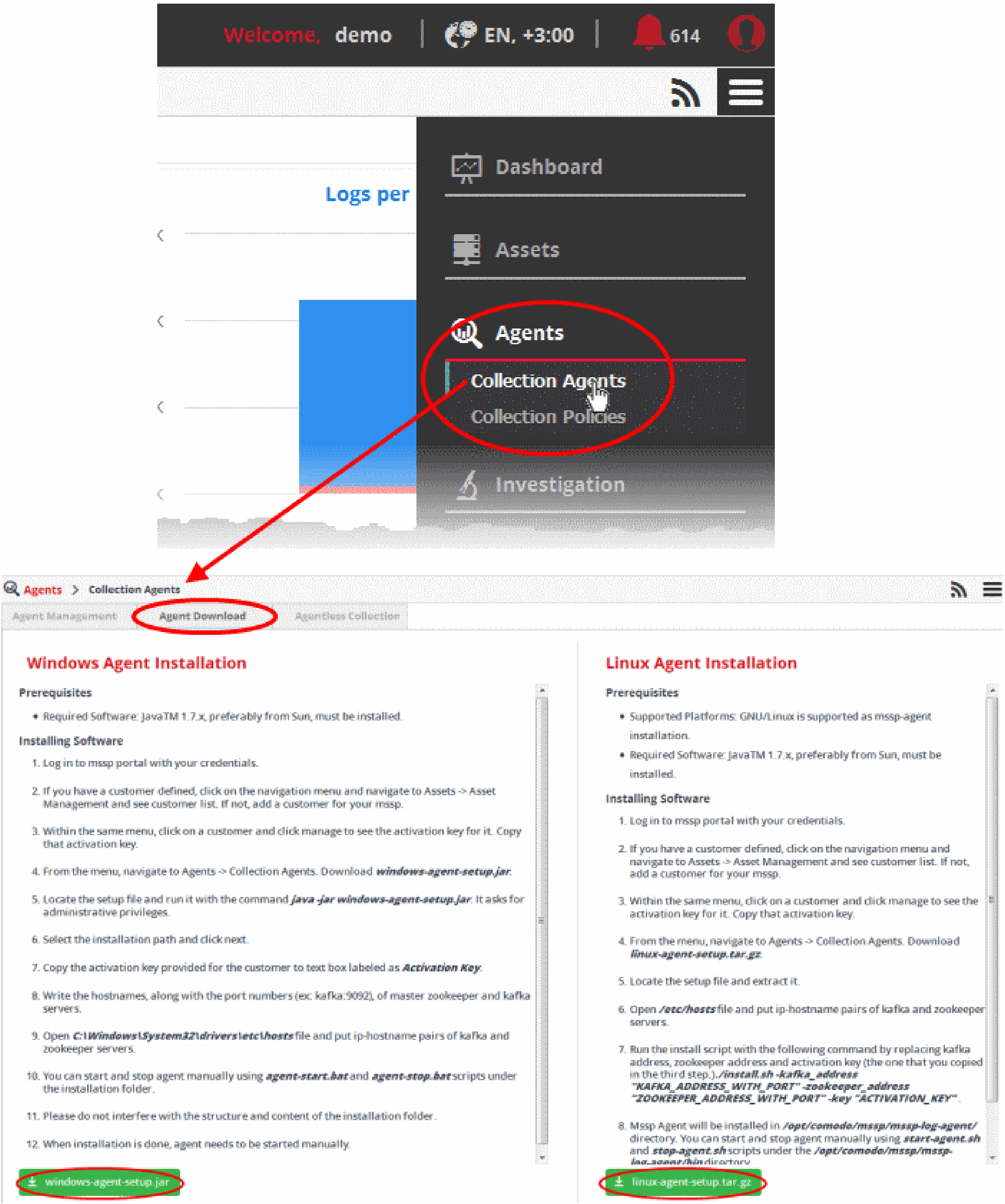
Step 3 - Configure customer endpoints to forward logs to NxSIEM

There are different methods available to configure log collection:

- **Collection Agent** - An agent installed on Windows and Linux endpoints forwards logs to the NxSIEM server. The agent setup file for Windows and Linux endpoints can be downloaded from the NxSIEM console. For each network and zone added, NxSIEM generates a unique agent activation key to authorize the agent to connect to the server.
- **Agent less Collection** - The admin console contains ready-made configuration script files for RSYSLOG and NXLOG utilities which have all parameters pre-configured for a specific customer/network. Once deployed to customer endpoints, these scripts automatically configure the RSYSLOG (Linux endpoints) and NXLOG (Windows endpoints) utilities to forward logs to the NxSIEM server.

To download, install and activate the collection agent

- Click the navigation button at top right then 'Agents' > 'Collection Agents' > 'Agent Download', as shown:



Windows Agent Installation

Prerequisites

- Required Software: JavaTM 1.7.x, preferably from Sun, must be installed.

Installing Software

1. Log in to mssp portal with your credentials.
2. 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.
3. Within the same menu, click on a customer and click manage to see the activation key for it. Copy that activation key.
4. From the menu, navigate to Agents -> Collection Agents. Download ***windows-agent-setup.jar***.
5. Locate the setup file and run it with the command ***java -jar windows-agent-setup.jar***. It asks for administrative privileges.
6. Select the installation path and click next.
7. Copy the activation key provided for the customer to text box labeled as ***Activation Key***.
8. Write the hostnames, along with the port numbers (ex: kafka:9092), of master zookeeper and kafka servers.
9. Open ***C:\Windows\System32\drivers\etc\hosts*** file and put ip-hostname pairs of kafka and zookeeper servers.
10. You can start and stop agent manually using ***agent-start.bat*** and ***agent-stop.bat*** scripts under the installation folder.
11. Please do not interfere with the structure and content of the installation folder.
12. When installation is done, agent needs to be started manually.

windows-agent-setup.jar

Linux Agent Installation

Prerequisites

- Supported Platforms: GNU/Linux is supported as mssp-agent installation.
- Required Software: JavaTM 1.7.x, preferably from Sun, must be installed.

Installing Software

1. Log in to mssp portal with your credentials.
2. 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.
3. Within the same menu, click on a customer and click manage to see the activation key for it. Copy that activation key.
4. From the menu, navigate to Agents -> Collection Agents. Download ***linux-agent-setup.tar.gz***.
5. Locate the setup file and extract it.
6. Open ***/etc/hosts*** file and put ip-hostname pairs of kafka and zookeeper servers.
7. Run the install script with the following command by replacing kafka address, zookeeper address and activation key (the one that you copied in the third step.).***/install.sh -kafka_address "KAFKA_ADDRESS_WITH_PORT" -zookeeper_address "ZOOKEEPER_ADDRESS_WITH_PORT" -key "ACTIVATION_KEY"***.
8. Mssp Agent will be installed in ***/opt/comodo/mssp/mssp-log-agent/*** directory. You can start and stop agent manually using ***start-agent.sh*** and ***stop-agent.sh*** scripts under the ***/opt/comodo/mssp/mssp-log-agent/bin*** directory

linux-agent-setup.tar.gz

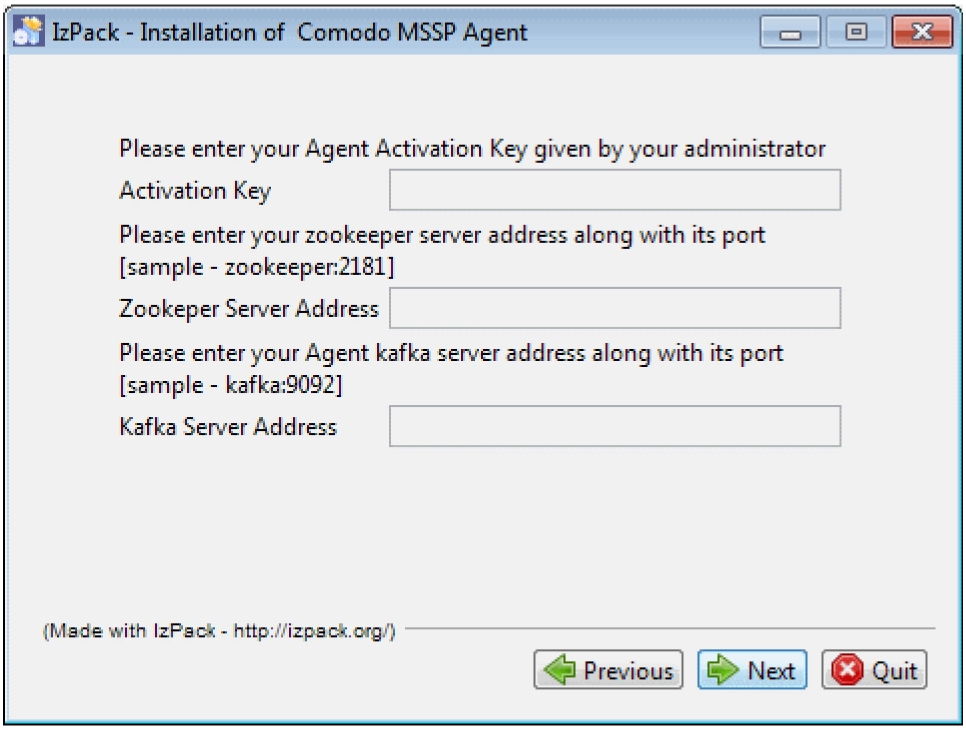
The 'Agent Download' page contains installation instructions and download links for Windows and Linux agents:

- Click the 'windows-agent-setup.jar' or 'linux-agent-setup.gz' button to download the respective agent.
- Transfer the setup files to required endpoints for installation.

Tip: The agent requires Java 1.7 or higher, pre-installed at the endpoint for its operation. Ensure you have Java at the endpoints before installing the agent. Also, ensure that the network to which the endpoint is connected is added to NxSIEM for the customer. Keep the Unique Agent Activation Key of the customer/network handy to authorize the agent to connect to NxSIEM server. The key can be obtained from the 'Asset Management' > 'Hard Assets' interface. Select the Customer > Network and click the 🗎 button in the row of the network. The 'Activation Key' is displayed at the bottom of the 'Hard Assets' pane.

For Windows Endpoints:

- Double click on the setup file and follow the installation wizard.



IzPack - Installation of Comodo MSSP Agent

Please enter your Agent Activation Key given by your administrator

Activation Key

Please enter your zookeeper server address along with its port [sample - zookeeper:2181]

Zookeper Server Address

Please enter your Agent kafka server address along with its port [sample - kafka:9092]

Kafka Server Address

- In the second step, enter the agent activation key, the Zookeeper and Kafka server addresses of the network, click 'Next' and continue the installation.
- On completion of the installation, manually start the agent by navigating to the folder 'C:\Program Files (x86)\MSSP Agent' and click on 'agent-start' file.

The agent will establish connection with NxSIEM server and start sending logs from the endpoint.

For Linux Endpoints:

- Navigate to the location on the endpoint where you saved 'linux-agent-setup.tar.gz' and extract it.
- Open /etc/hosts file, add the IP-Hostname pairs of Zookeeper and Kafka servers and save it.
- Run the installation file with the following command.

  /install.sh - <IP address of Kafka server:port number> -<IP address of Zookeeper server:port number> -<Activation key for the customer/network>

  The log collection agent will be installed at **/opt/comodo/mssp/mssp-log-agen**t directory.
- Start the agent manually by running the command start-agent.sh under **/opt/comodo/mssp/mssp-log-agent /bin** directory

The agent will establish connection with NxSIEM server and start sending logs from the endpoint. Optionally, you can configure log collection policies and deploy them as required to the agents. For detailed explanations on the policies and tutorials on configuring and deploying them, refer to the online help page at **https://help.comodo.com/topic-325-1-675-8372-Log-Collection-Policies.html**.

To deploy per-configured script files for agent-less log collection

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

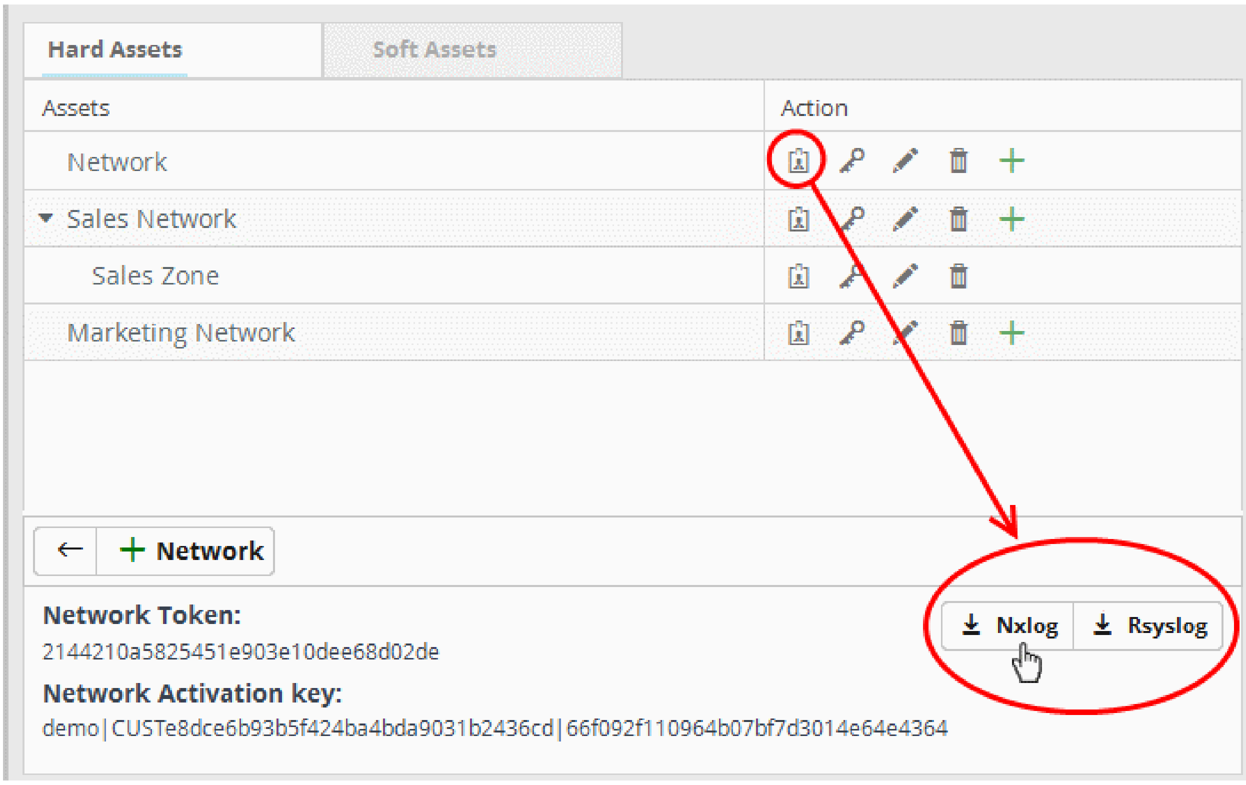
The 'Customer Details' pane will open at the right.

- 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 or the 'RSYSLOG Configuration File Download' button as required and save the file.



Assets	Action
Network	
Sales Network	
Sales Zone	
Marketing Network	

Network Token:
2144210a5825451e903e10dee68d02de

Network Activation key:
demo|CUSTe8dce6b93b5f424ba4bda9031b2436cd|66f092f110964b07bf7d3014e64e4364

To configure NXLOG on Windows Endpoints:

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

All settings in the configuration file are pre-configured and will instruct the NXLOG utility to send logs to the NxSIEM server. The NxSIEM server will receive and store the logs under the respective customer/network for monitoring and incident reporting.

To configure RSYSLOG on Linux Endpoints:

- Run the script file on all required endpoints.

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

Alternatively, you can download a manually configurable script files for NXLOG and RSYSLOG utilities from 'Agents' > 'Collection Agents' > 'Agentless Collection' interface, manually enter the parameters for the customer network to be monitored and run the script at the endpoints. Refer to the online help page at **https://help.comodo.com/topic-325-1-675-8396-Agentless-Log-Collection.html** for more details.

Step 4 - Generate event queries and view events

Once the endpoints at customer networks are configured, NxSIEM collects and saves them in its database. You can search for specific events by running event queries created for the customer. NxSIEM returns the list of event log entries with field values matching those in the query, as a table. The results table contains selected field names as column headers. You can view all the fields with their values for any event log entry from the results table and even use them for creating further queries, perform an IP/Domain lookup of external IP addresses/domains involved in the event and more.

NxSIEM ships with a set of pre-defined queries placed under respective category folders and allows you t create custom queries too. You can search the event log database using both pre-defined queries and custom queries.

The event queries can also be used for:

- Constructing custom dashboards which display query results as graphical charts. Refer to the online help page of the administrator guide at **https://help.comodo.com/topic-325-1-675-8386-Configuring-Custom-Dashboards.html** for more details.
- Constructing 'Correlation Rules' which identify harmful events/incidents on customer networks and assign them to customer administrators for attention. Refer to the next step '**Step 5 - Creating Correlating Rules to Monitor Networks for Harmful Incidents**' for more details.

Each event query is built with a set of filter statements that 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
- **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 source IP addresses. More details on Live Lists are available in the online help page at **https://help.comodo.com/topic-325-1-675-8897-Live-Lists.html**.

To view the Event Query interface

- Open the 'Event Query' interface by clicking the 'Menu' button at the top right, then clicking 'Investigation' > 'Event Query'.
- Select the customer from the left hand side pane.

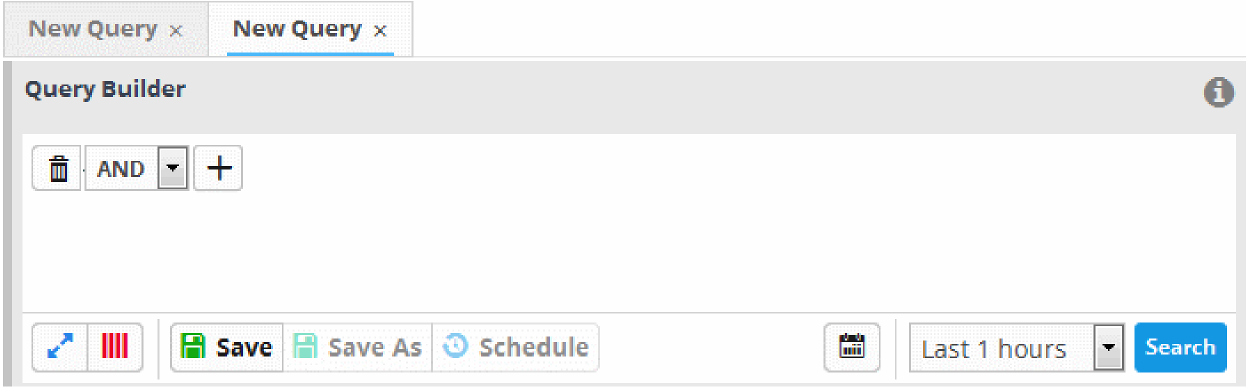
The interface displays the list of pre-defined queries pertaining to the customer in the left side panel.

To create a new custom query

- Select the appropriate query category folder under which you want to add a new query or create a new folder by clicking the button at the bottom of the list and select it.
- Click the button.

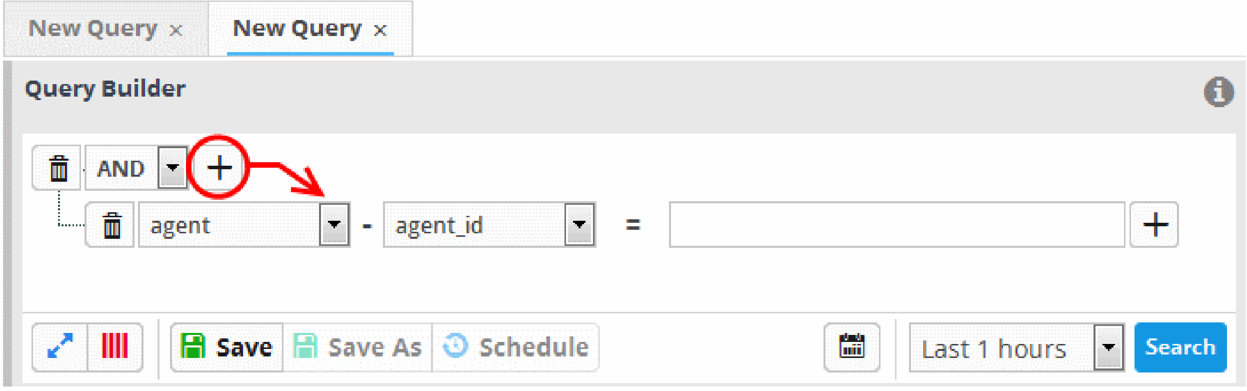
A 'New Query' tab will be displayed with its query builder pane below it.

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



The next step is to add the filters for the query.

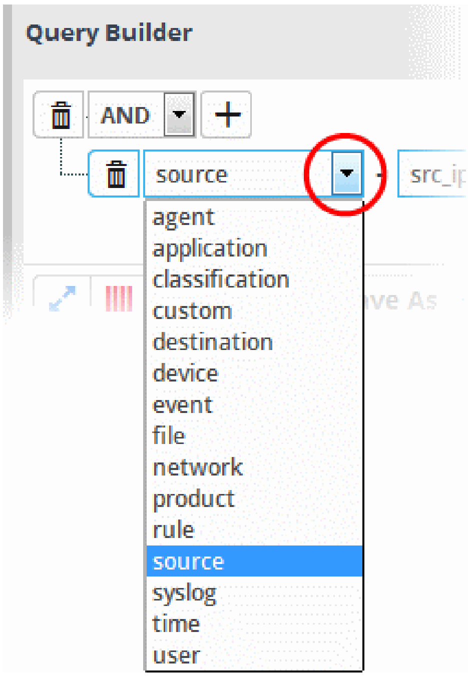
- Choose the combination condition for the query filter statements to be defined from the drop-down in the 'Query Builder' pane. The options available are:
    - AND
    - OR
    - NOT
- Click the + button to add a filter

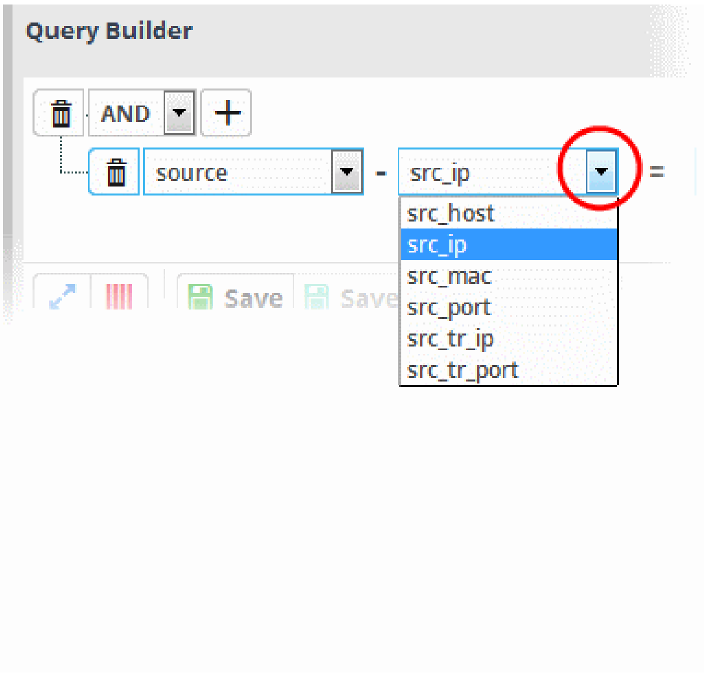


- Choose the field group you wish to add to the filter from the first drop-down.

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

- Select the field whose value is to be specified as search criteria from the second drop-down.

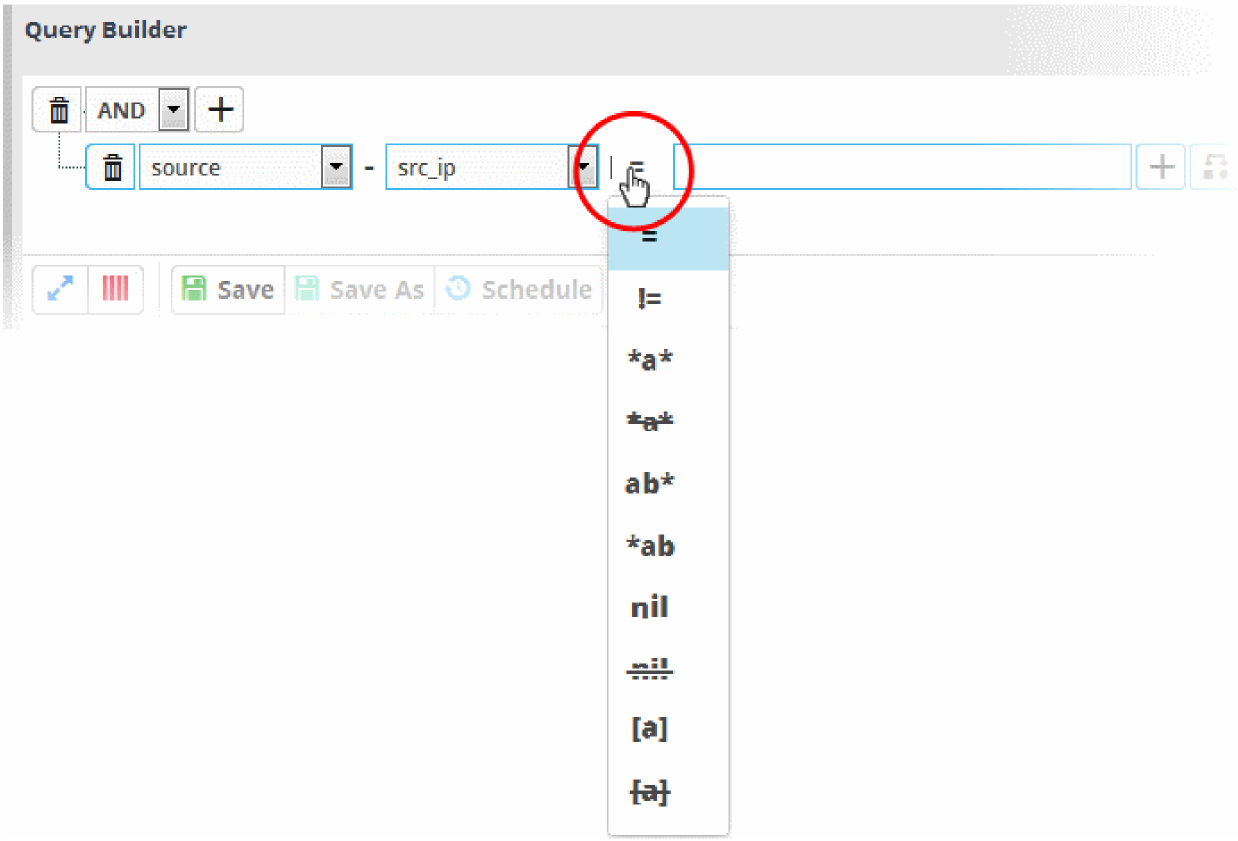




Tip: The descriptions of the Field Groups and the Field items under each of them, are available in the online help page at **https://help.comodo.com/topic-325-1-675-8452-Appendix-1--%E2%80%93-Field-Groups-and-Event-Items-Description.html**.

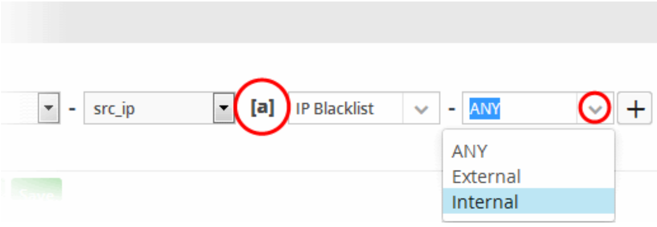
The next step is to choose the relationship operator between the field and the value specified.

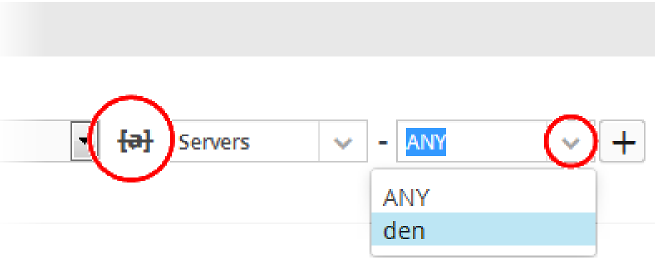
- To choose an operator, click the drop-down between the two fields:



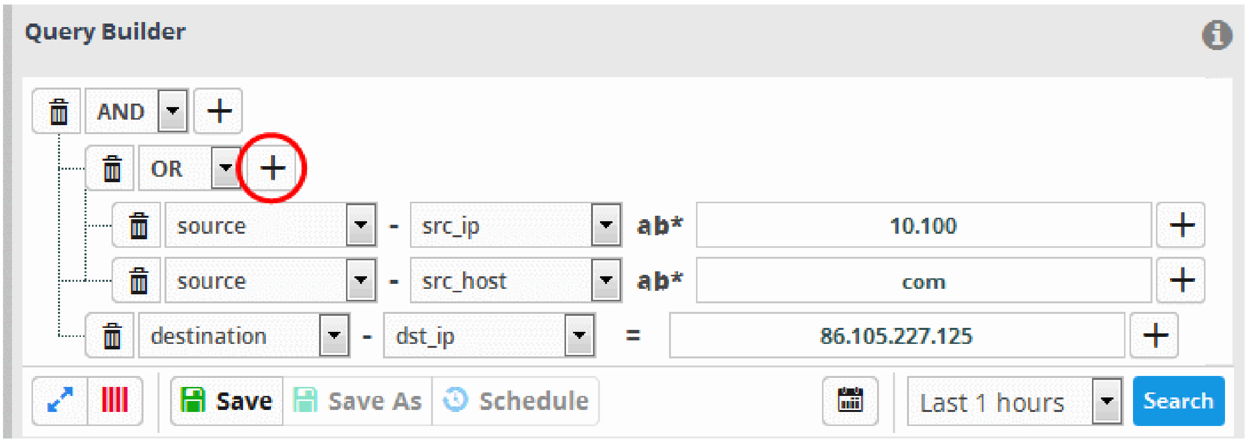
The operators depends on the field chosen. The following table explains the various operator symbols:

Relation Operator	Description	Entering the value for the 'Field'
=	Equals to	Manually enter a value in the field to the right of the operator. Events containing the same value will be identified by the query.
!=	Does not equal to	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 query.
>	Greater than	Applicable only for fields with numerical values, for example, port numbers. Manually enter a value in the field to the right of the operator. The query will identify events that contain values greater than the entered value.
>=	Greater than or equal to	Applicable only for fields with numerical values, for example, port numbers. Manually enter a value in the field to the right of the operator. The query will identify events that contain values equal to or greater than the entered value.
<	Less than	Applicable only for fields with numerical values, for example, port numbers. Manually enter a value in the field to the right of the operator. The query will identify events that contain values less than the entered value.
<=	Less than or equal to	Applicable only for fields with numerical values, for example, port numbers. Manually enter a value in the field to the right of the operator. The query will identify events that contain values equal to or lower than the entered value.
a	Contains	Manually enter a value in the field to the right of the operator. The query 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	Manually enter a value in the field to the right of the operator. The query 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	Manually enter a value in the field to the right of the operator. The query 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	Manually enter a value in the field to the right of the operator. The query 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	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	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	Allows you to configure the filter statement to fetch values for the field from a pre-defined live list containing specific values for the field type. **Background**: Live Lists enable administrators to add and manage lists of values for different fields for use in queries and correlation rules. Lists can be created and the values can be updated manually or 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 Live Lists management, refer to the online help page at **https://help.comodo.com/topic-325-1-675-8897-Live-Lists.html**. On selecting [a] as the relation parameter, drop-down options will appear for the List and the List type:  src_ip [a] IP Blacklist ANY ANY External Internal The first drop-down shows the Live Lists that contain values for the selected query field. The second drop-down shows the List Types within the selected 'Live List'. • Choose the Live 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. 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 live list . On selecting ~~[a]~~ as the relation parameter, drop-down options will appear for the List and the List type:

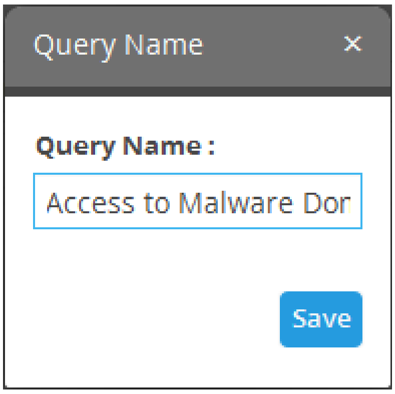
		 The first drop-down shows the Live Lists that contain values for the selected query field. The second drop-down shows the List Types within the selected 'Live List'. • Choose the Live List to be used in the query filter from the first drop-down. • Choose the sub list that contains the set of values to be input as exclusions to the query filter from the second drop-down. The results will display all events that do not contain the values in the live lists.

- 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



AND
OR
source - src_ip ab* 10.100
source - src_host ab* com
destination - dst_ip = 86.105.227.125
Last 1 hours

- 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.

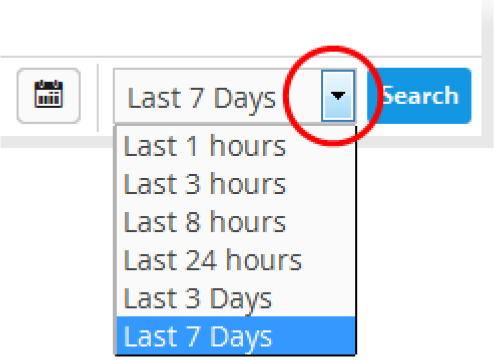


- Enter the name of the query in the 'Query Name' field and click the 'Save' button .

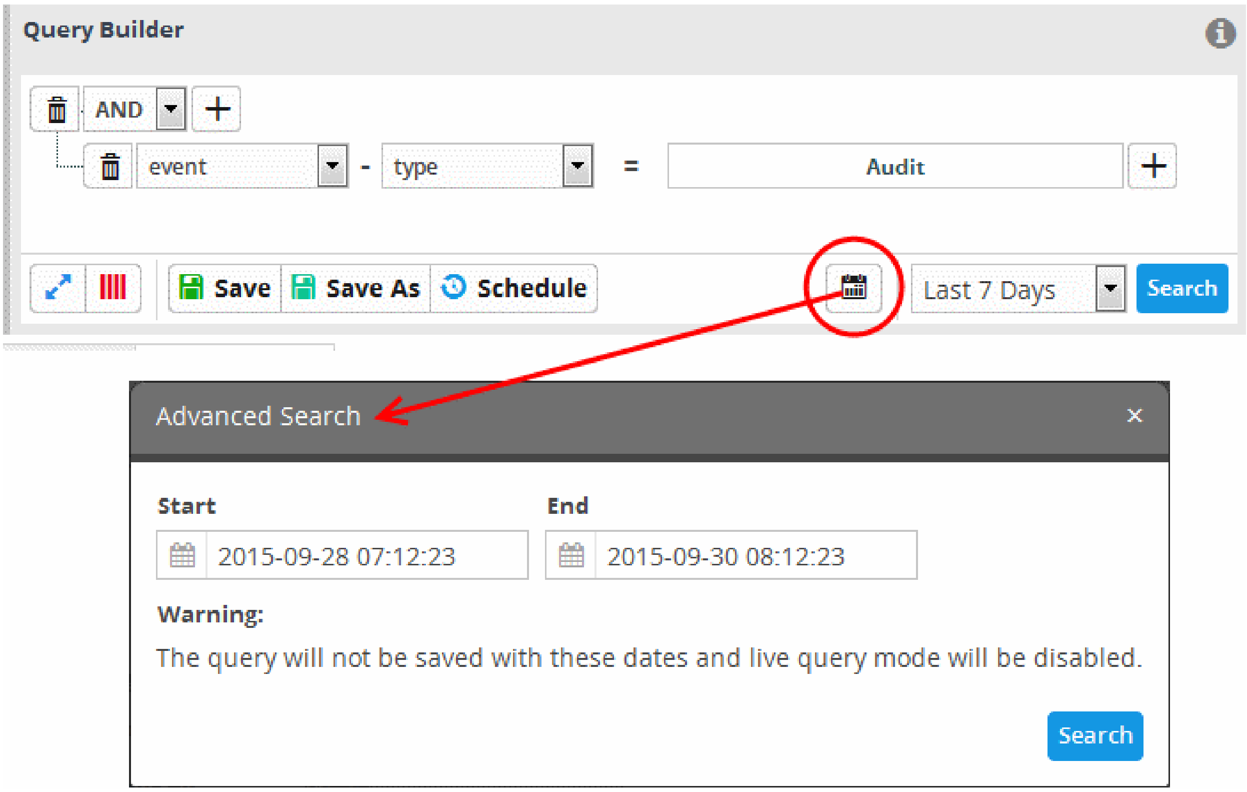
The next step is to run the event query.

To run an event query

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



  - To view events that occurred within specific dates, click the calendar button, enter the 'Start' and 'End' dates in the 'Advanced Search' dialog and click 'Search'.



Advanced Search

Start 2015-09-28 07:12:23

End 2015-09-30 08:12:23

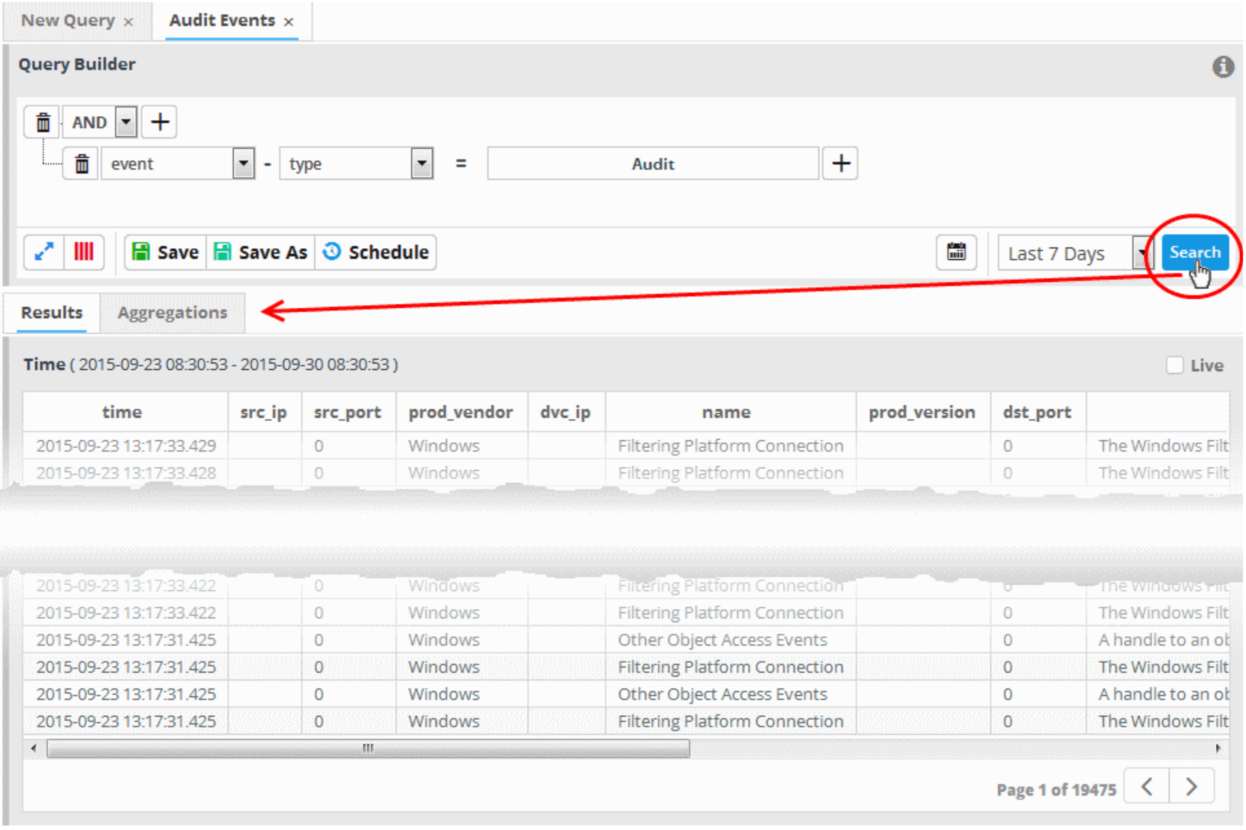
Warning:

The query will not be saved with these dates and live query mode will be disabled.

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

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

The 'Results' are displayed in the lower pane.



Time (2015-09-23 08:30:53 - 2015-09-30 08:30:53)

□ Live

time	src_ip	src_port	prod_vendor	dvc_ip	name	prod_version	dst_port	
2015-09-23 13:17:33.429		0	Windows		Filtering Platform Connection		0	The Windows Filt
2015-09-23 13:17:33.428		0	Windows		Filtering Platform Connection		0	The Windows Filt
2015-09-23 13:17:33.422		0	Windows		Filtering Platform Connection		0	The Windows Filt
2015-09-23 13:17:33.422		0	Windows		Filtering Platform Connection		0	The Windows Filt
2015-09-23 13:17:31.425		0	Windows		Other Object Access Events		0	A handle to an ob
2015-09-23 13:17:31.425		0	Windows		Filtering Platform Connection		0	The Windows Filt
2015-09-23 13:17:31.425		0	Windows		Other Object Access Events		0	A handle to an ob
2015-09-23 13:17:31.425		0	Windows		Filtering Platform Connection		0	The Windows Filt

Page 1 of 19475

The lower pane has two tabs:

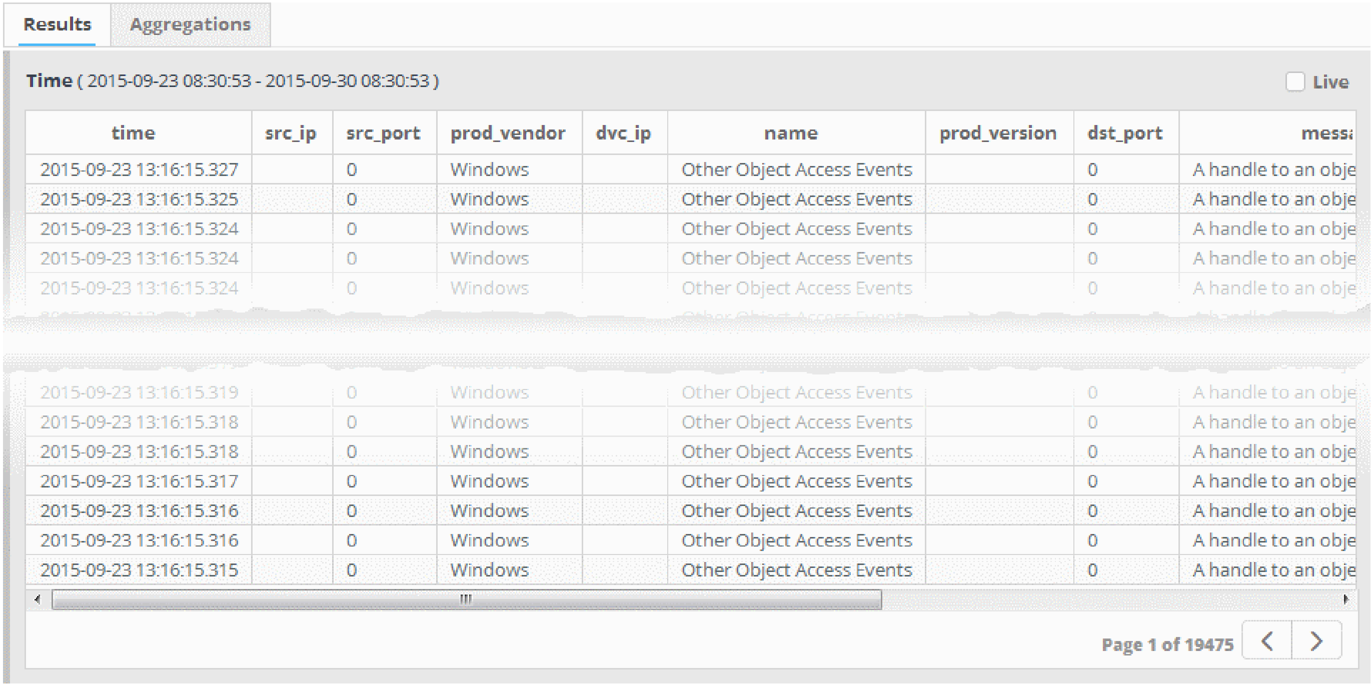
- **Results -** The 'Results' tab displays the list of log entries that match the query as a table, with relevant event fields as column headers. Clicking on an event allows you to view its details.
- **Aggregations -** The Aggregations tab allows you to group identified events and view aggregations of the identified events.

The rest of this section explains on viewing the results table. For detailed explanations and tutorials on viewing event aggregations, refer to the online help page of the administrator guide at **https://help.comodo.com/topic-325-1-675-8385-Configuring-Event-Queries.html**.

The Results Table

The 'Results' table shows list of event log records that match the event query, with event log entry fields, relevant to the query, as table headers.

Tip: The Query builder allows you to even customize the fields to be displayed as table headers in the table. For more details, refer to the explanation under '**Configure results table for a query** ' in the online help page **https://help.comodo.com/topic-325-1-675-8385-Configuring-Event-Queries.html** of the administrator guide.



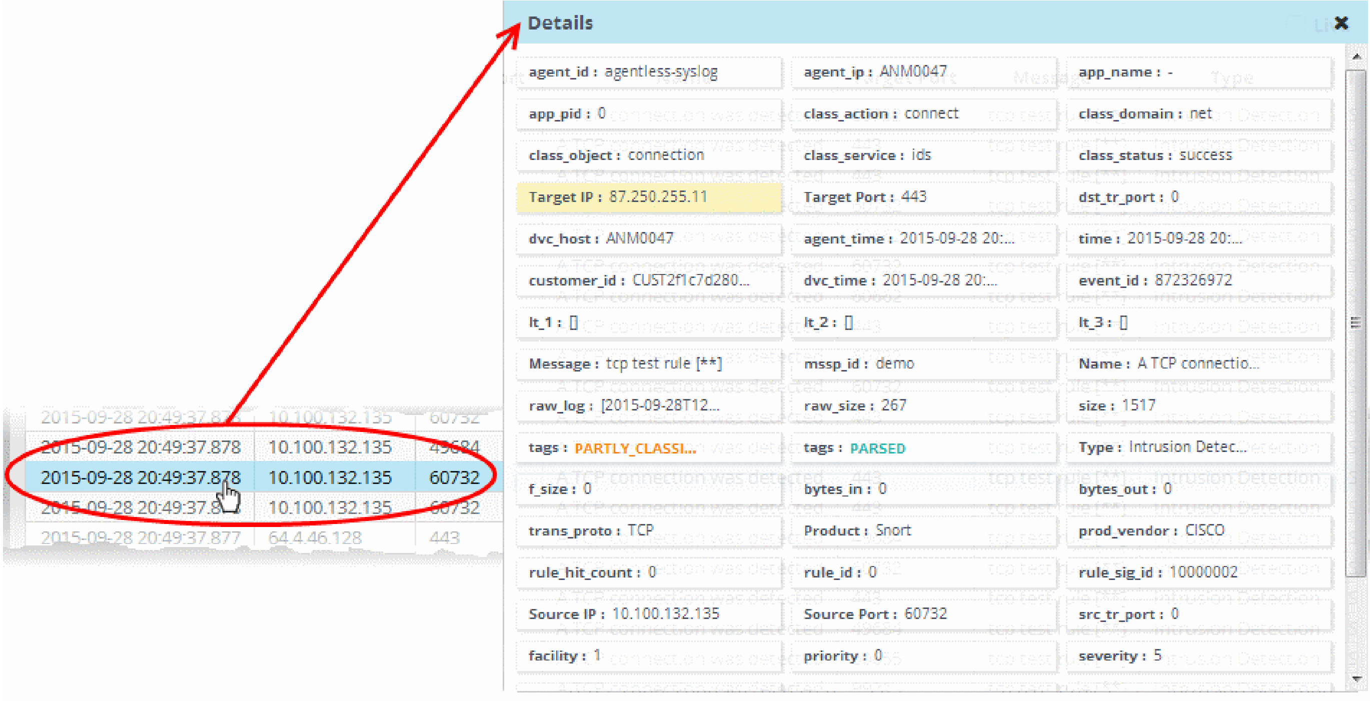
Time (2015-09-23 08:30:53 - 2015-09-30 08:30:53)

time	src_ip	src_port	prod_vendor	dvc_ip	name	prod_version	dst_port	mess
2015-09-23 13:16:15.327		0	Windows		Other Object Access Events		0	A handle to an obje
2015-09-23 13:16:15.325		0	Windows		Other Object Access Events		0	A handle to an obje
2015-09-23 13:16:15.324		0	Windows		Other Object Access Events		0	A handle to an obje
2015-09-23 13:16:15.324		0	Windows		Other Object Access Events		0	A handle to an obje
2015-09-23 13:16:15.324		0	Windows		Other Object Access Events		0	A handle to an obje
2015-09-23 13:16:15.319		0	Windows		Other Object Access Events		0	A handle to an obje
2015-09-23 13:16:15.318		0	Windows		Other Object Access Events		0	A handle to an obje
2015-09-23 13:16:15.318		0	Windows		Other Object Access Events		0	A handle to an obje
2015-09-23 13:16:15.317		0	Windows		Other Object Access Events		0	A handle to an obje
2015-09-23 13:16:15.316		0	Windows		Other Object Access Events		0	A handle to an obje
2015-09-23 13:16:15.316		0	Windows		Other Object Access Events		0	A handle to an obje
2015-09-23 13:16:15.315		0	Windows		Other Object Access Events		0	A handle to an obje

Page 1 of 19475

You can view complete details of an event log entry from the 'Results' table and use the values to add further filters statements to the query in order to refine the search. You can also perform IP and Domain lookups and feed these values to live lists for use in other queries and correlation rules.

- To view the details of an event, click on the result row.



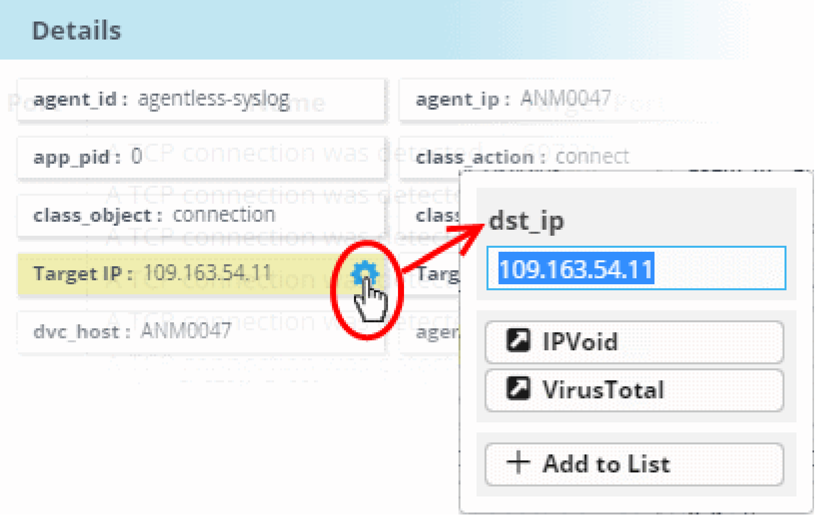
2015-09-28 20:49:37.87	10.100.132.135	60732
2015-09-28 20:49:37.878	10.100.132.135	49684
2015-09-28 20:49:37.878	10.100.132.135	60732
2015-09-28 20:49:37.8	10.100.132.135	60732
2015-09-28 20:49:37.877	64.4.46.128	443

Details

agent_id : agentless-syslog	agent_ip : ANM0047	app_name : -
app_pid : 0	class_action : connect	class_domain : net
class_object : connection	class_service : ids	class_status : success
Target IP : 87.250.255.11	Target Port : 443	dst_tr_port : 0
dvc_host : ANM0047	agent_time : 2015-09-28 20:...	time : 2015-09-28 20:...
customer_id : CUST2f1c7d280...	dvc_time : 2015-09-28 20:...	event_id : 872326972
lt_1 : []	lt_2 : []	lt_3 : []
Message : tcp test rule [**]	mssp_id : demo	Name : A TCP connectio...
raw_log : [2015-09-28T12...	raw_size : 267	size : 1517
tags : PARTLY_CLASSI...	tags : PARSED	Type : Intrusion Detec...
f_size : 0	bytes_in : 0	bytes_out : 0
trans_proto : TCP	Product : Snort	prod_vendor : CISCO
rule_hit_count : 0	rule_id : 0	rule_sig_id : 10000002
Source IP : 10.100.132.135	Source Port : 60732	src_tr_port : 0
facility : 1	priority : 0	severity : 5

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.
- Clicking the gear icon that appears at the right end on hovering the mouse cursor over a field opens a context sensitive menu, that allows you to:
    - Perform IP lookup of external IP addresses using IPVOID by clicking on the 'IPVoid' button.
    - Perform IP Address/Domain lookup using Virus Total by clicking on the 'VirusTotal' button.
    - Add the value to a Live List. Refer to the online help page at **https://help.comodo.com/topic-325-1-675-8897-Live-Lists.html** for more details on live lists.



Details

agent_id : agentless-syslog

agent_ip : ANM0047

app_pid : 0

class_action : connect

class_object : connection

Target IP : 109.163.54.11

dvc_host : ANM0047

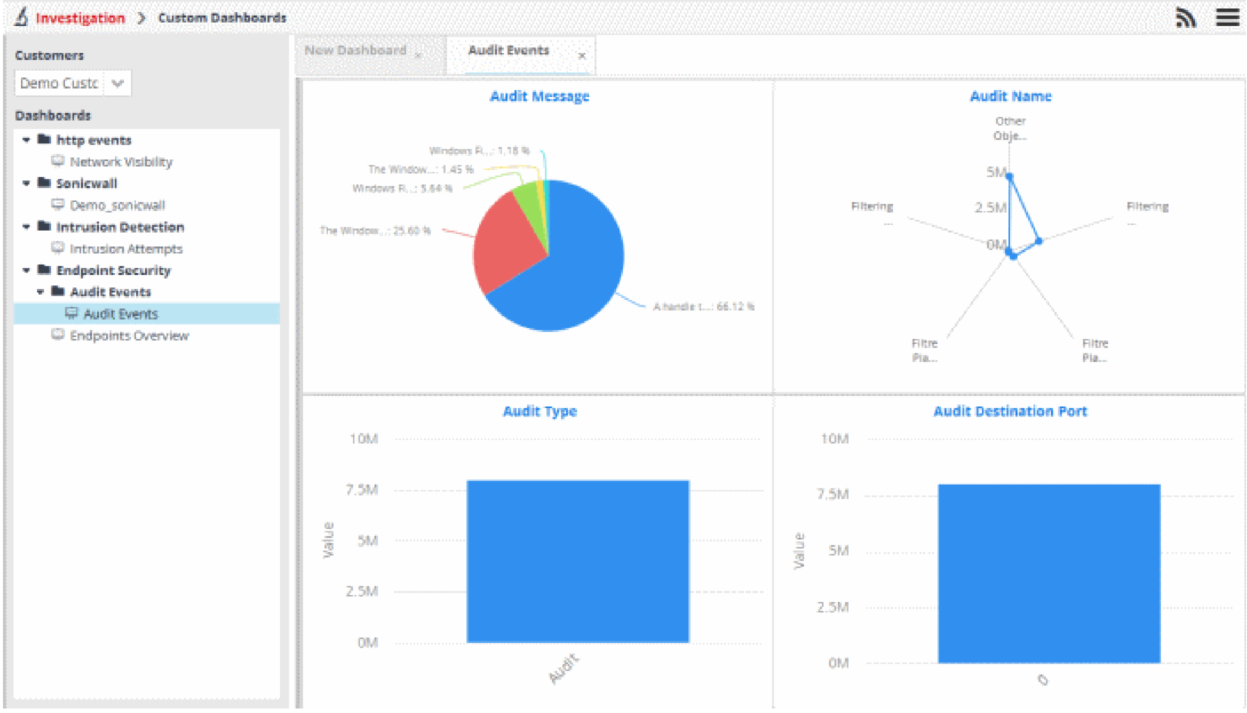
dst_ip

109.163.54.11

Step 5 - Create custom dashboards for customer networks

Custom Dashboards allow you to view dynamically updated results from event queries as pie charts, bar charts, time charts and spider charts. By viewing important data from often complex queries in an easily digested chart format, you can more effectively track, monitor and analyze the activities of your customers.

To open the 'Custom Dashboards' interface, click the 'Menu' button from the top right, choose 'Investigation' and then click 'Custom Dashboards'.



The left hand side panel displays a list of custom dashboards added for the customer under respective category folders. The right hand side panel displays the custom dashboards selected from the LHS pane under respective tabs. Each dashboard can display up to four charts.

By default, The first tab displays a 'New Dashboard' tab that allows you to create a new dashboard for the selected customer.

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 'Event Query' interface. Each dashboard can display up to four charts.

Each chart is constructed from the following parameters.

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

- **Name -** A name to identify the chart.
- **Selected Event Query -** The query whose results are to be displayed in the chart. The query can be selected from the list of queries, added fro the selected customer.
- **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 - 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'/'bytes out'. The event groups are ranked based on the sum of the values in the

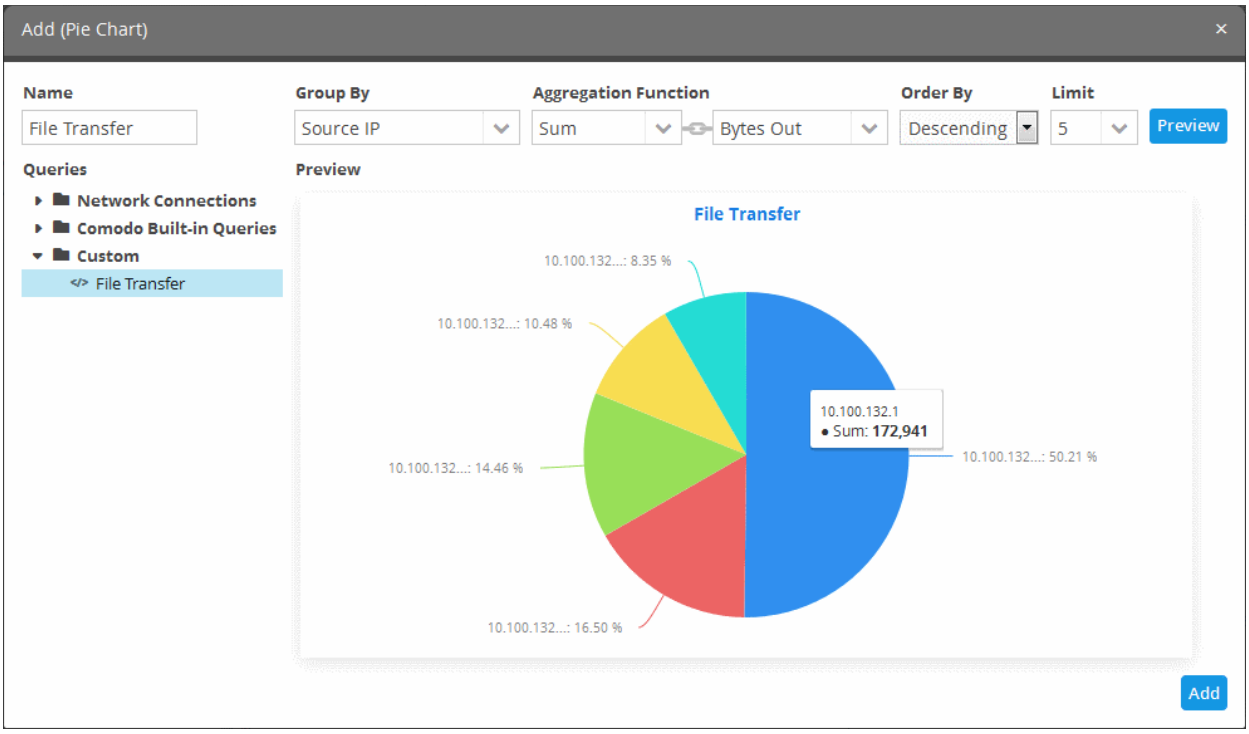
chosen numerical field from all the events in that group. For example, if we choose 'Bytes-in' as numerical value, then the system adds up the values in the 'Bytes-in' field of all the events in a group and ranks the group accordingly. The event group having the sum of values in the 'Bytes-in' field as maximum is ranked top and vise-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 identify 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:



Add (Pie Chart)

Name: File Transfer

Group By: Source IP

Aggregation Function: Sum, Bytes Out

Order By: Descending

Limit: 5

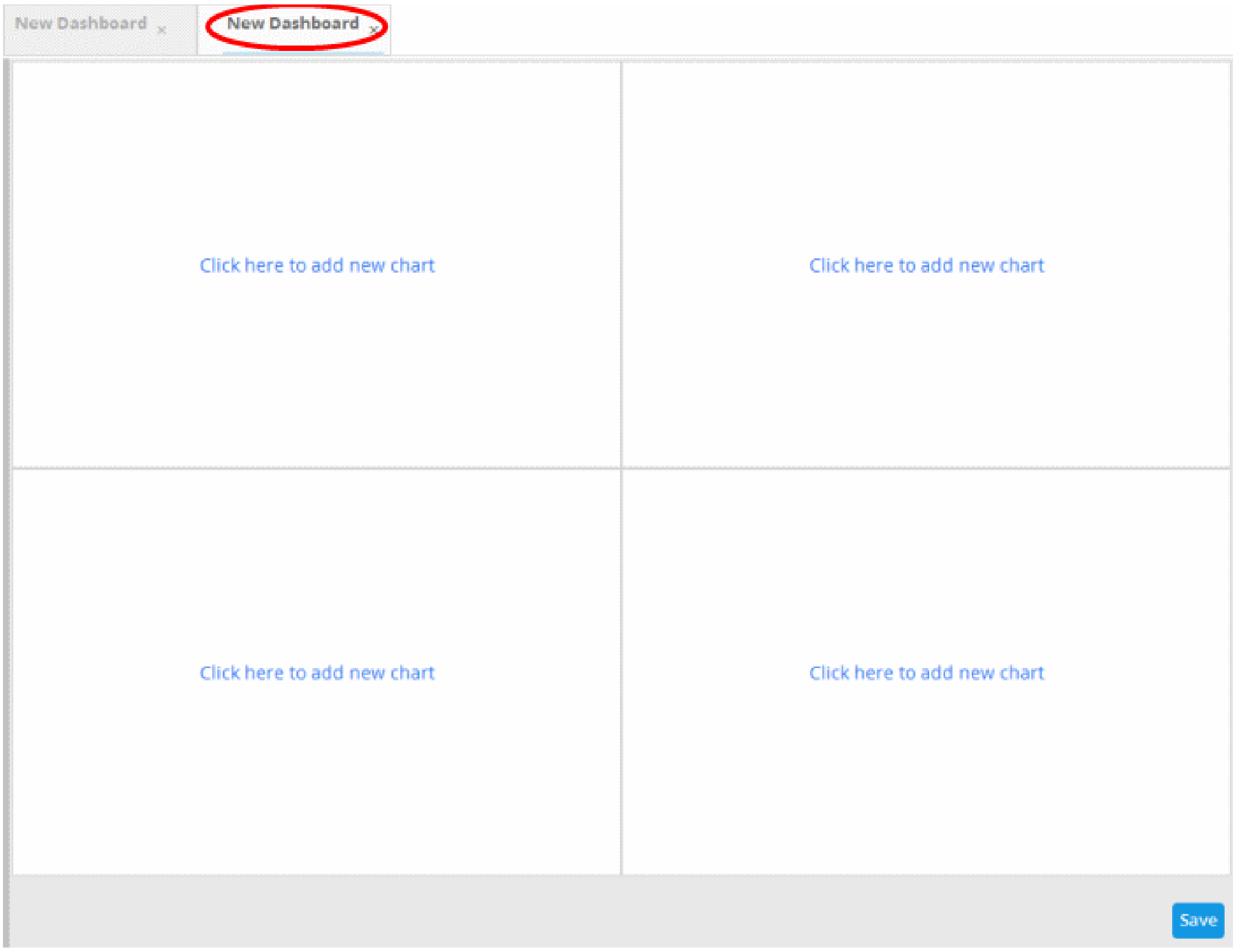
To create a new dashboard

- 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.

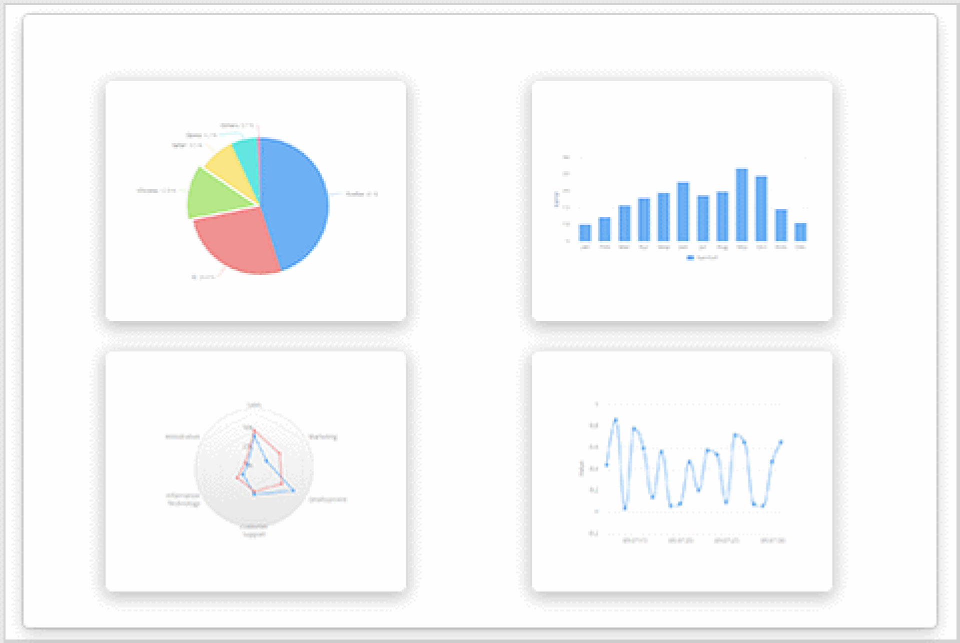
Tip: You can also use the 'New Dashboard' tab that is displayed as the first tab on selecting a customer, to create a new dashboard. You can save the created dashboard by selecting an appropriate folder from the left side panel.


New Dashboard
New Dashboard
Click here to add new chart
Click here to add new chart
Click here to add new chart
Click here to add new chart
Save

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.

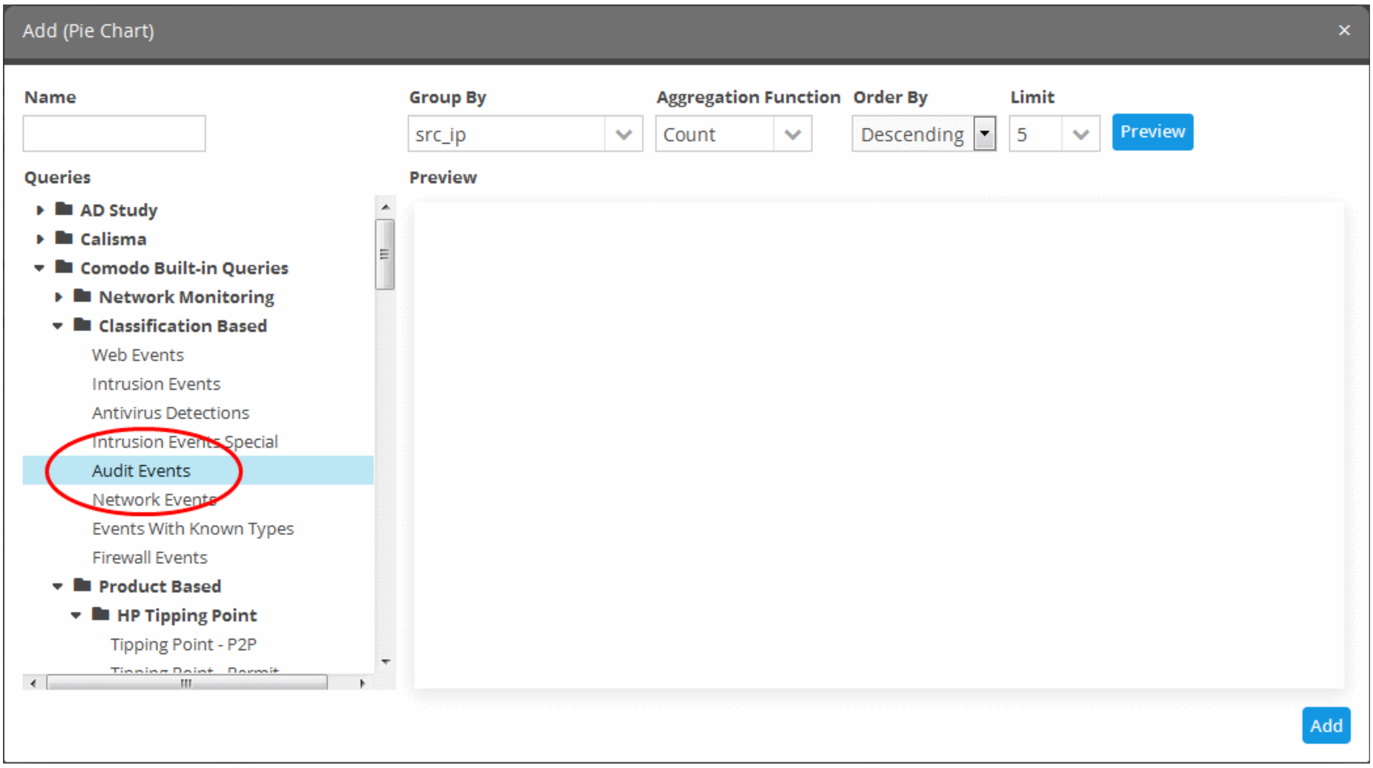


The available options are:

- Pie Chart
- Bar Chart
- Spider Chart
- Time Chart

- Click on a graph type from the options

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



Add (Pie Chart)

Name

Group By: src_ip

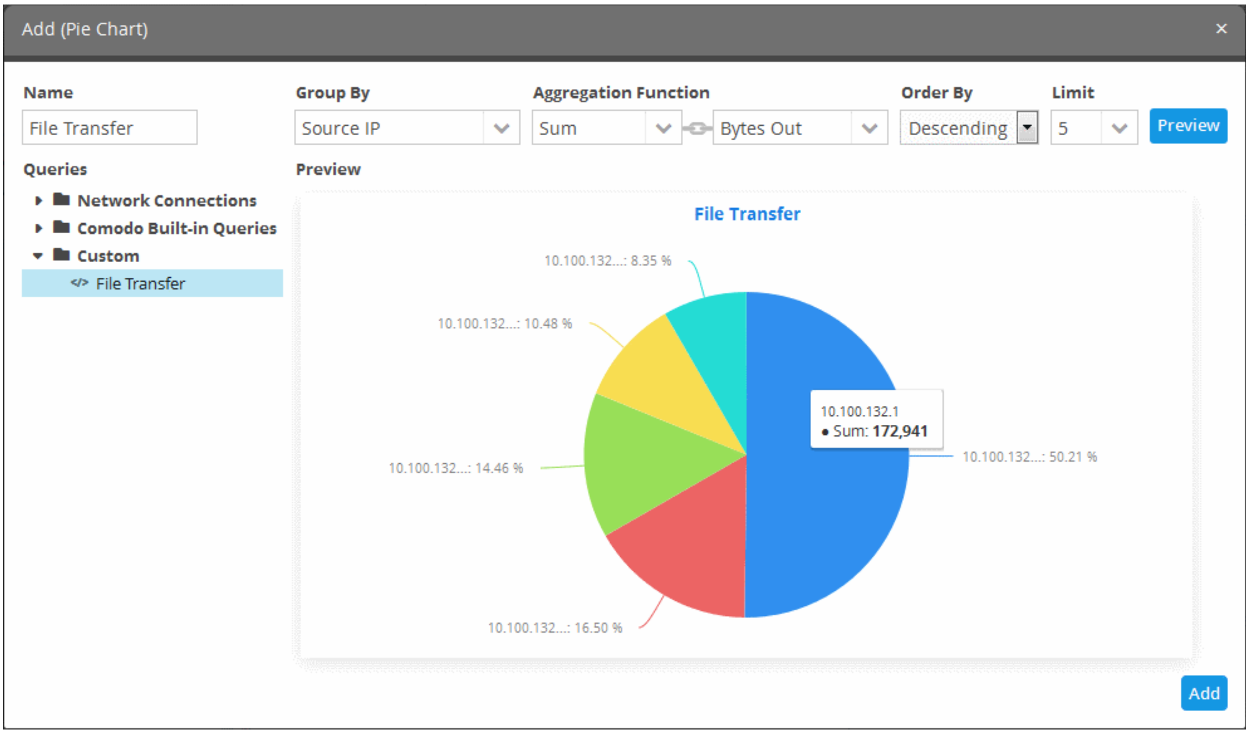
Aggregation Function: Count

Order By: Descending

Limit: 5

- Enter a name for the chart, in the 'Name' text field
- Choose the query whose results are to be populated in the report, from the 'Queries' list.
- Select 'Group By', 'Aggregation Function', 'Order by' and 'Limit' parameters as explained **above**.

- Click the 'Preview' button to check the chart before adding it to the dashboard tile



Add (Pie Chart)

Name: File Transfer

Group By: Source IP

Aggregation Function: Sum — Bytes Out

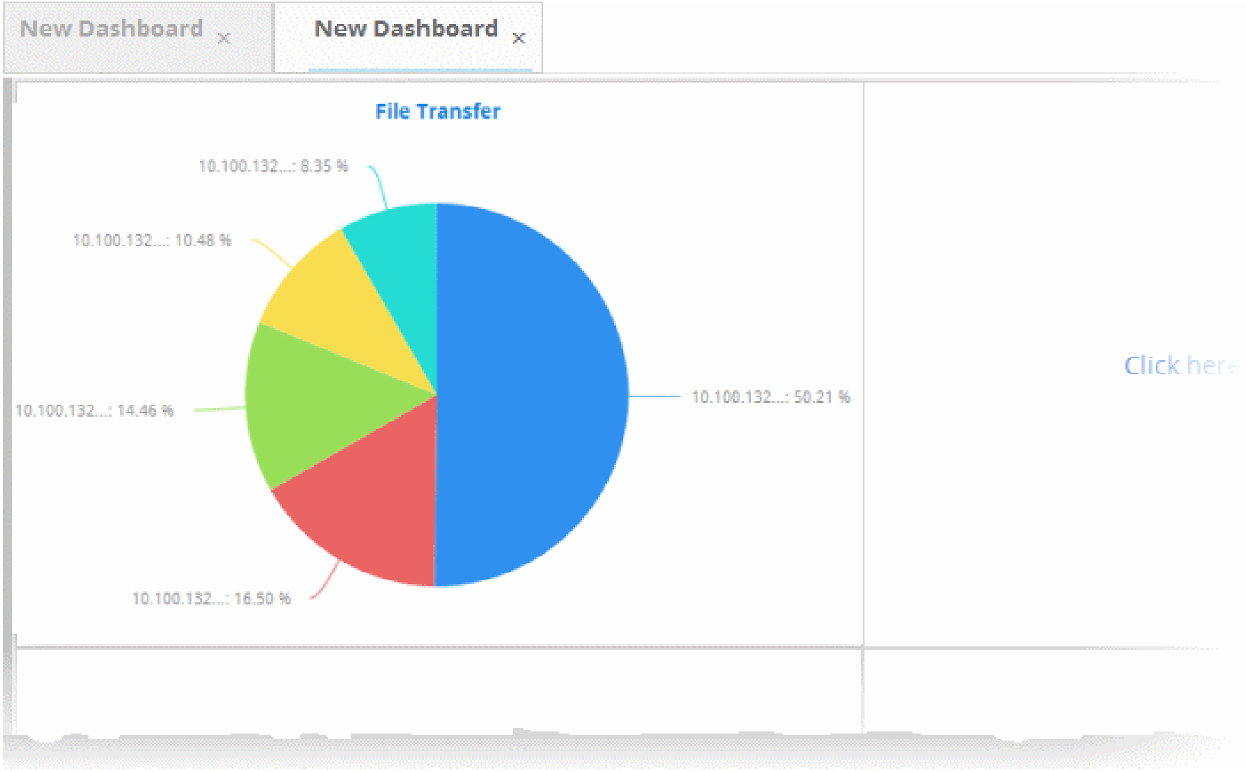
Order By: Descending

Limit: 5

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

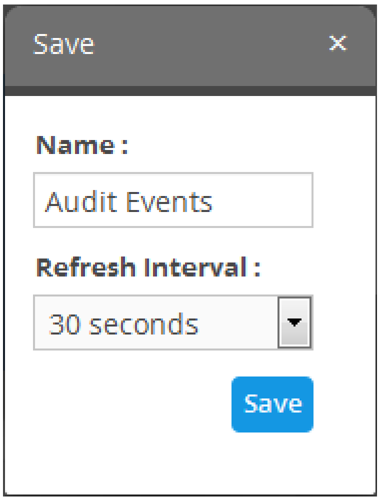
- Click the 'Add' button

The configured tile will be added to the dashboard.



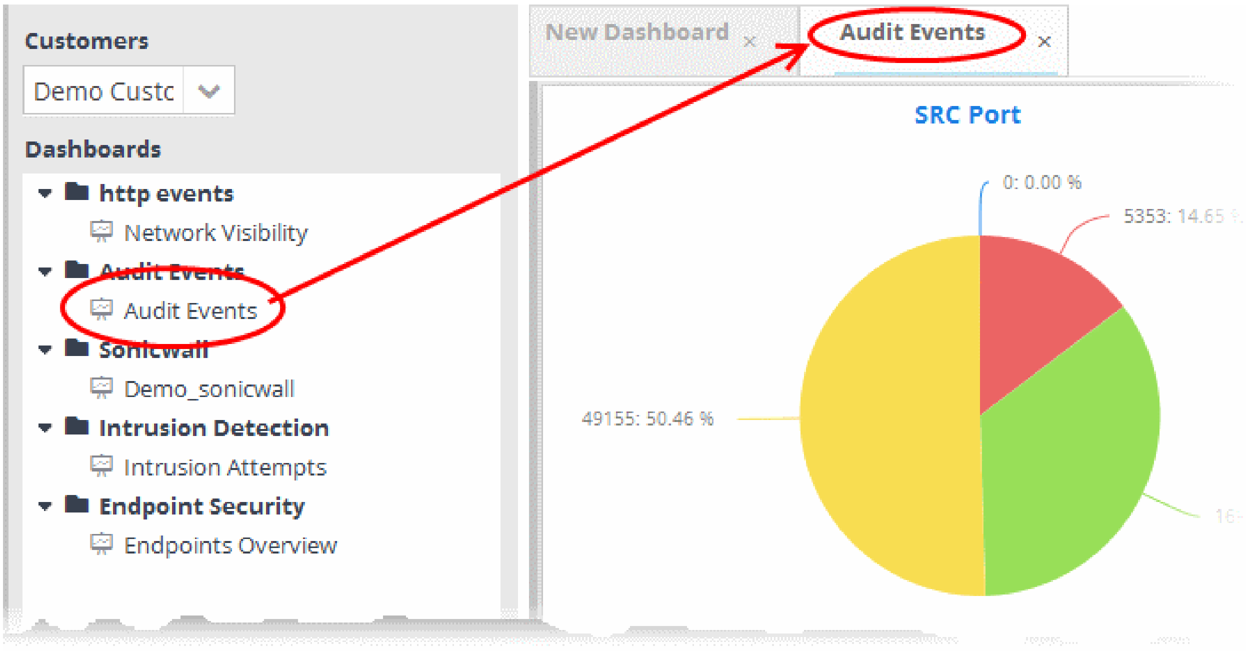
- Repeat the process to add more number of tiles to the dashboard as explained **above**.
- Click the 'Save' button.

The 'Save' dialog will appear.



- 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.



You can add as many custom dashboards for various event queries configured for a customer by repeating the same process.

Step 6 - Create correlating rules to monitor networks for incidents

NxSIEM monitors the logs received from enrolled customers networks, based on rules added for the customer and generates 'Incidents' on identifying events that match the conditions specified in the rules. The incidents are notified by alerts and automatically assigned to the users allotted to the respective customer for investigation and appropriate countermeasure.

NxSIEM ships with a set of pre-configured correlation rules for each customer. In addition, you can create and add custom rules for each customer. Following sections explain on:

- Managing Rules
- Viewing Incidents

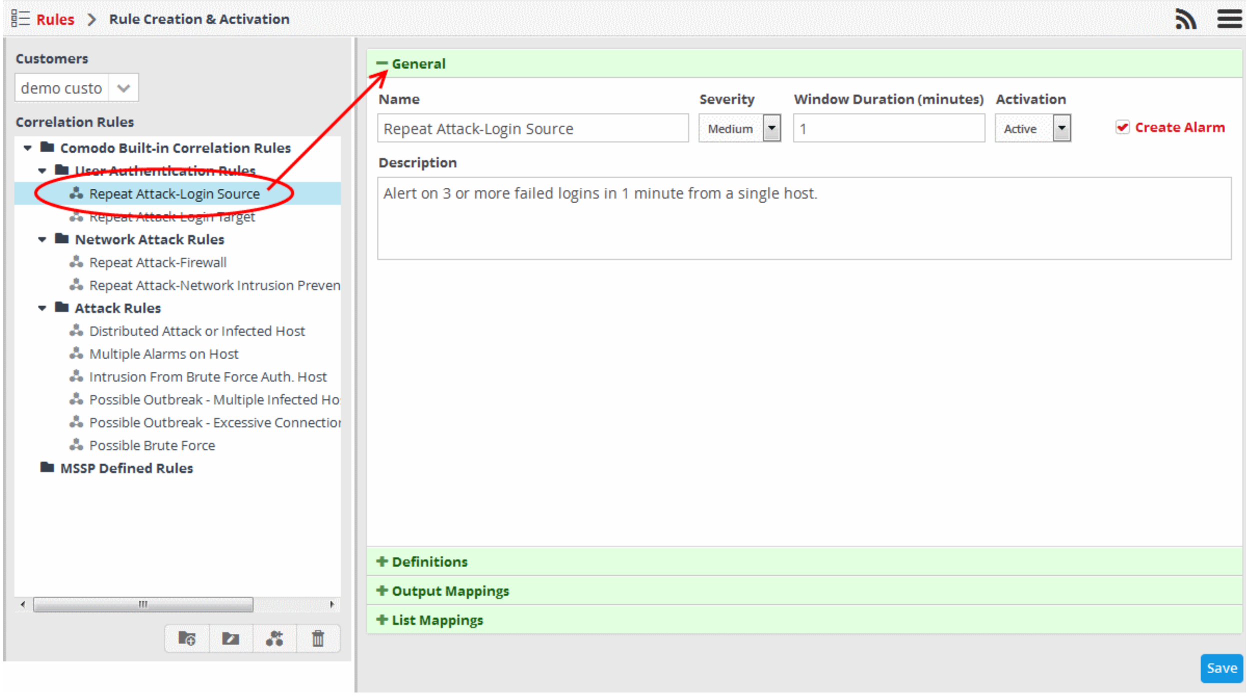
Managing Rules

Rules can be created by adding filter statement groups as conditions and specifying aggregation parameters. Optionally, you can configure how the output events are to be generated when the rule is met and to feed selected field values involved in events identified by the rule to Live Lists, for use in creating queries and other rules.

To view the 'Rule Creation and Activation' interface

- Click the 'Menu' button from the top right, choose 'Rules' and then click 'Rules Activation and Creation'.
- Choose the customer from the drop-down at the top left.

The 'Rule Creation and Activation' interface displays a list of pre-configured rules added for the customer under respective category folders in the left pane. Selecting a rule displays its details in the right pane.

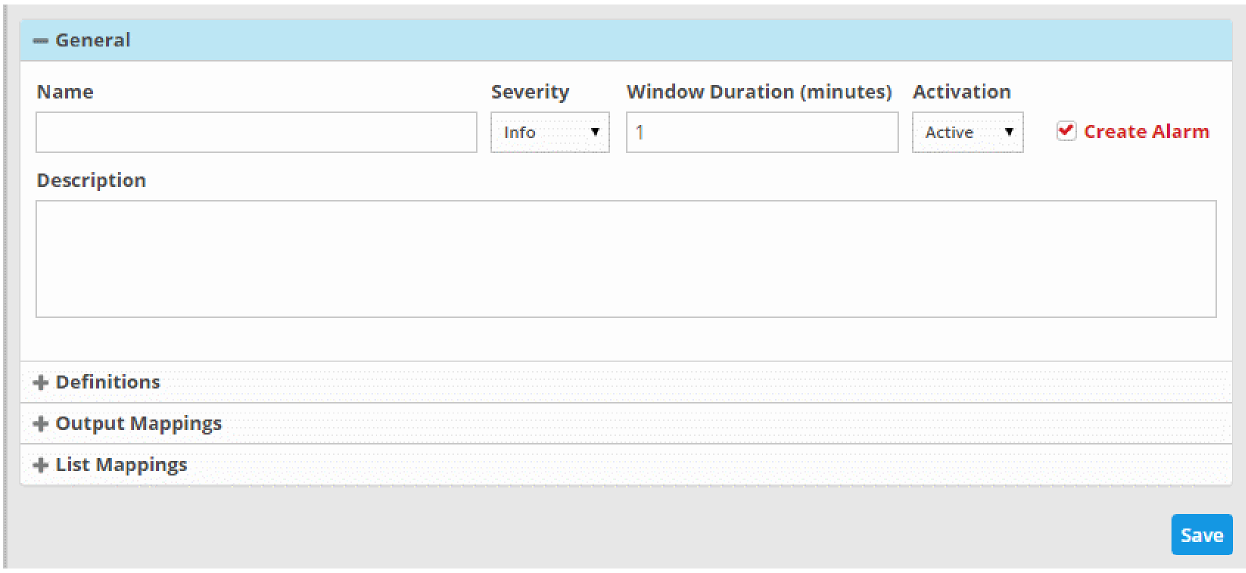

Rules > Rule Creation & Activation
Customers
demo custo
Correlation Rules
Comodo Built-in Correlation Rules
User Authentication Rules
Repeat Attack-Login Source
Repeat Attack-Login Target
Network Attack Rules
Repeat Attack-Firewall
Repeat Attack-Network Intrusion Preven
Attack Rules
Distributed Attack or Infected Host
Multiple Alarms on Host
Intrusion From Brute Force Auth. Host
Possible Outbreak - Multiple Infected Ho
Possible Outbreak - Excessive Connectio
Possible Brute Force
MSSP Defined Rules
General
Definitions
Output Mappings
List Mappings
Save

Name: Repeat Attack-Login Source
Severity: Medium
Window Duration (minutes): 1
Activation: Active
☑ Create Alarm
Description: Alert on 3 or more failed logins in 1 minute from a single host.

To create a 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:

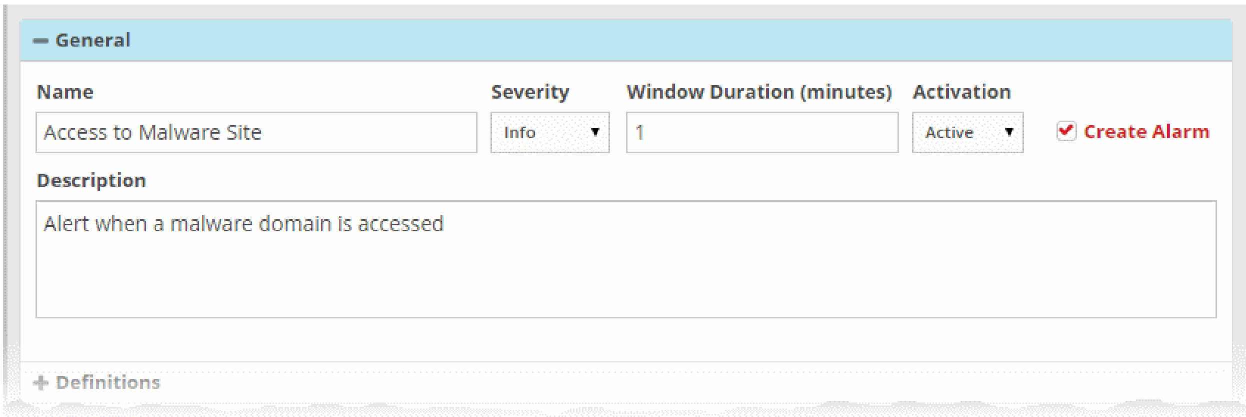


- **General -** Allows you to specify the name and description for the rule, select the severity level, window duration for rule, to set rule active or inactive and set whether or not to create an Incident when this rule is met.
- **Definitions -** Allows to define the queries for the rule and select 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).

The rest of this section explains on configuring General and Definitions sections for a rule. The 'Output Mappings' and 'List Mappings' are optional. For detailed explanations and tutorials on configuring those sections, refer to the online help page of the administrator guide at **https://help.comodo.com/topic-325-1-675-8387-Managing-Rules.html**.

General

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



Name: Access to Malware Site
Severity: Info
Window Duration (minutes): 1
Activation: Active
Description: Alert when a malware domain is accessed

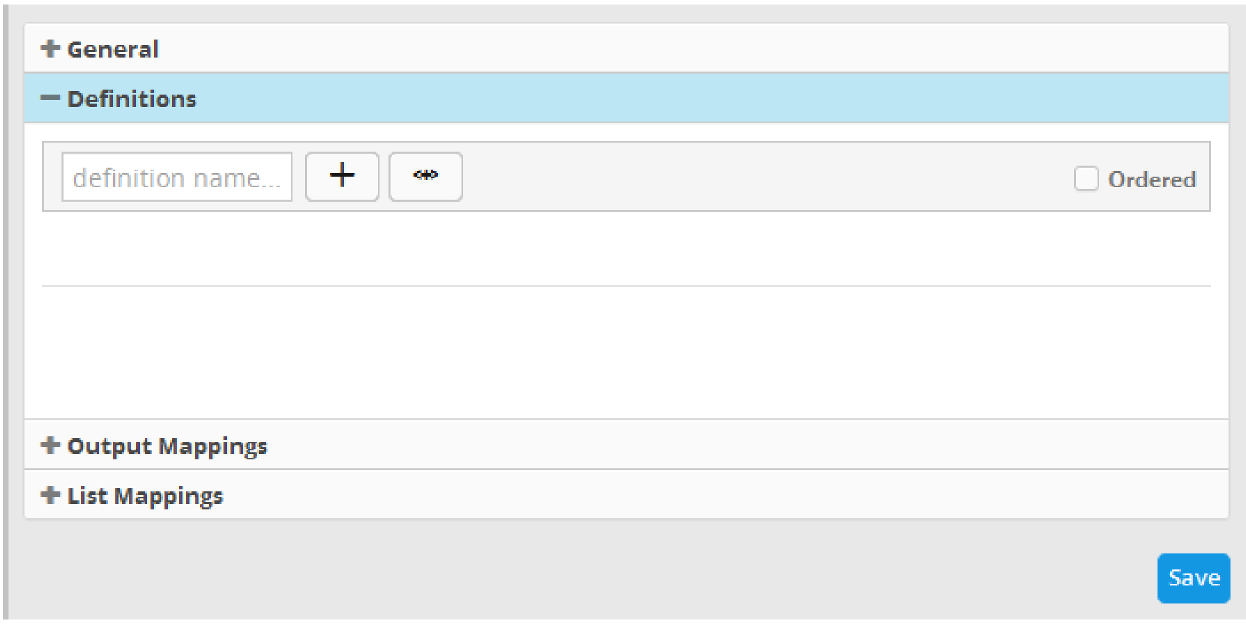
- **Name -** Enter a name for the rule
- **Severity -** Choose the severity level that will be assigned to the incident that matches the rule.
- **Window Duration (minutes) -** Enter the minimum duration (in minutes) for the event to be identified as an incident based on the rule.
- **Activation -** Choose whether you want the rule to be active or inactive from the drop-down

- **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 an Incident.
- **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.

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.



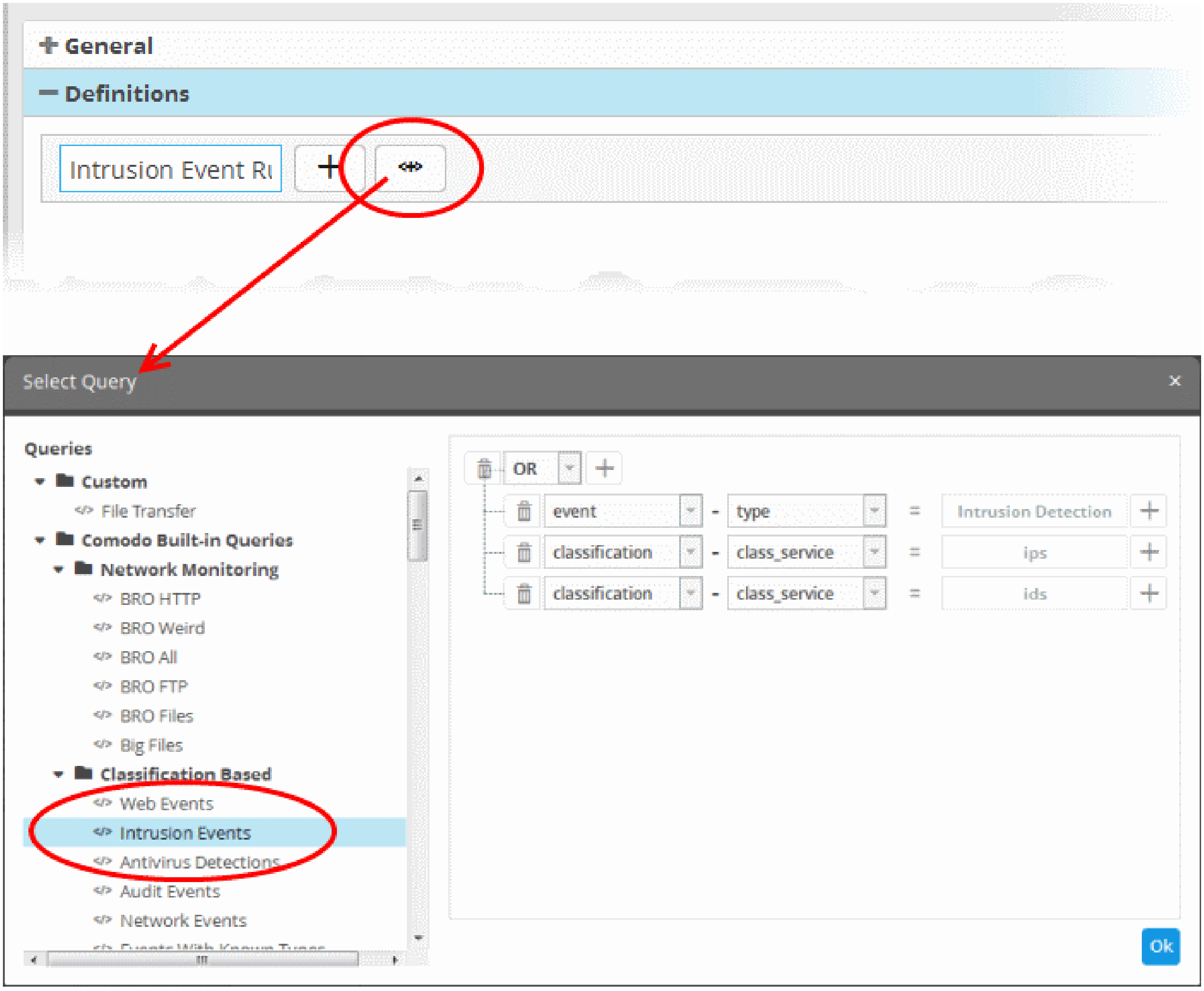
- To add a filter statement group as a rule definition, enter a name for the rule definition.

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.



event - type = Intrusion Detection

classification - class_service = ips

classification - class_service = ids

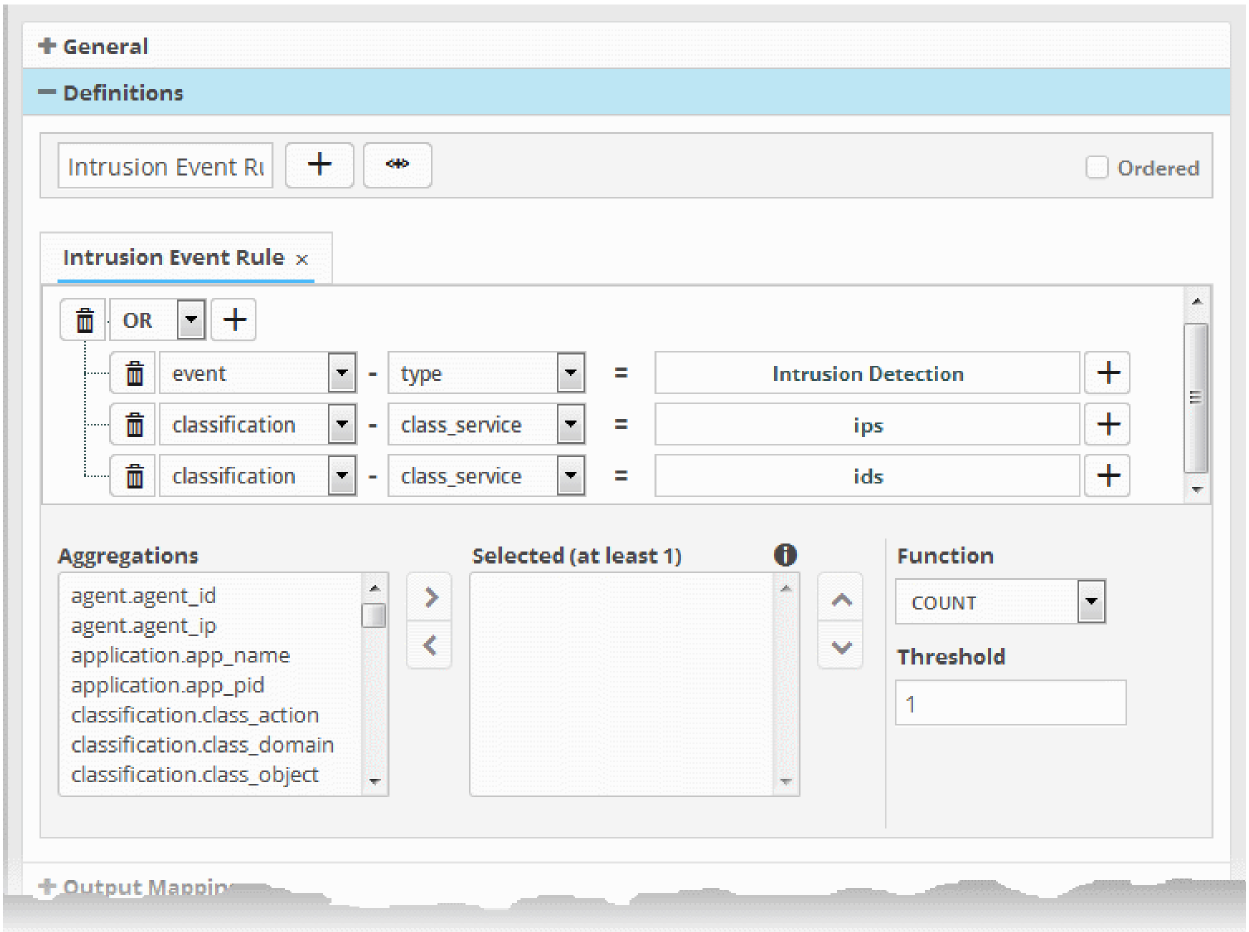
The 'Select Query' dialog will open with a list o pre-defined and custom event queries added for the customer in the left pane.

- 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 .



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

Function: COUNT

Threshold: 1

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, refer to the explanation of '**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.

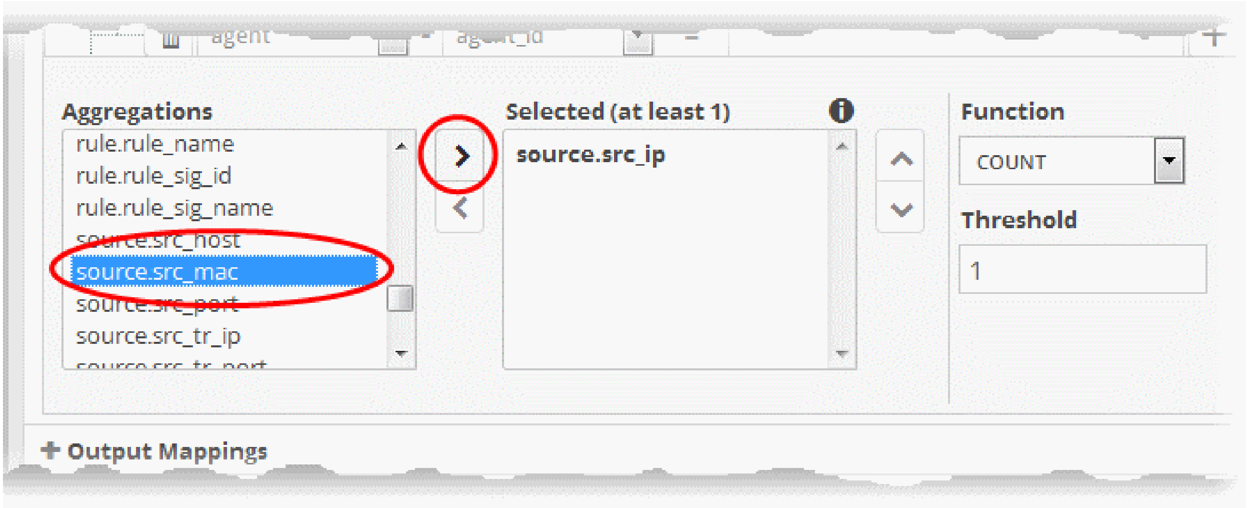
A tab to add the filter statements for the definition will open. Adding filter statements to the group is similar to that for an event query. Refer to the **explanation of adding filter statements under 'To create a new custom query'** for a tutorial on adding filter statement groups to the rule.

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' checkbox.

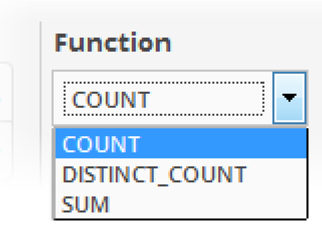
The next step is to select the field values based on which the events that meet the rule are to be aggregated to create the incident. For example if you want the rule to search the source details from where the event occurred, then you have to select the appropriate event value from the 'Aggregations' 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.



- 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.

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.

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 'Rule Creation & Activation' screen.

Tip: The 'Output Mappings' and 'List Mappings' are optional. For detailed explanations and tutorials on configuring those sections, refer to the online help page of the administrator guide at **https://help.comodo.com/topic-325-1-675-8387-Managing-Rules.html**.

- Click the 'Save' button to save your rule for the customer.

The rules engine checks the events from the logs and if it matches the rule, generates an alert and creates an incident.

Viewing Incidents

The list of incidents generated on identification of events that match the rules added for the customer can be viewed from the 'Incident Management' interface. You can also view the complete details of a selected incident and can re-assign it to a different user too.

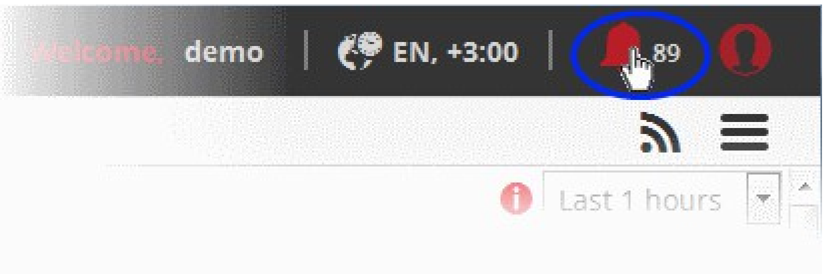
In addition to the incidents reported by the correlation rules, you can manually add incidents in order to assign specific jobs to the user allotted to a customer.

Tip: NxSIEM also allows you to group 'Incidents' that are mutually related or identified as series of events as a 'Case' and assign it to the user allotted for the customer. The user will be able to view the list of incidents to be attended together, take a consolidated remedial action and close the case. For more details refer to the online help page of the administrator guide at **https://help.comodo.com/topic-325-1-675-8388-Incidents-and-Cases.html**.

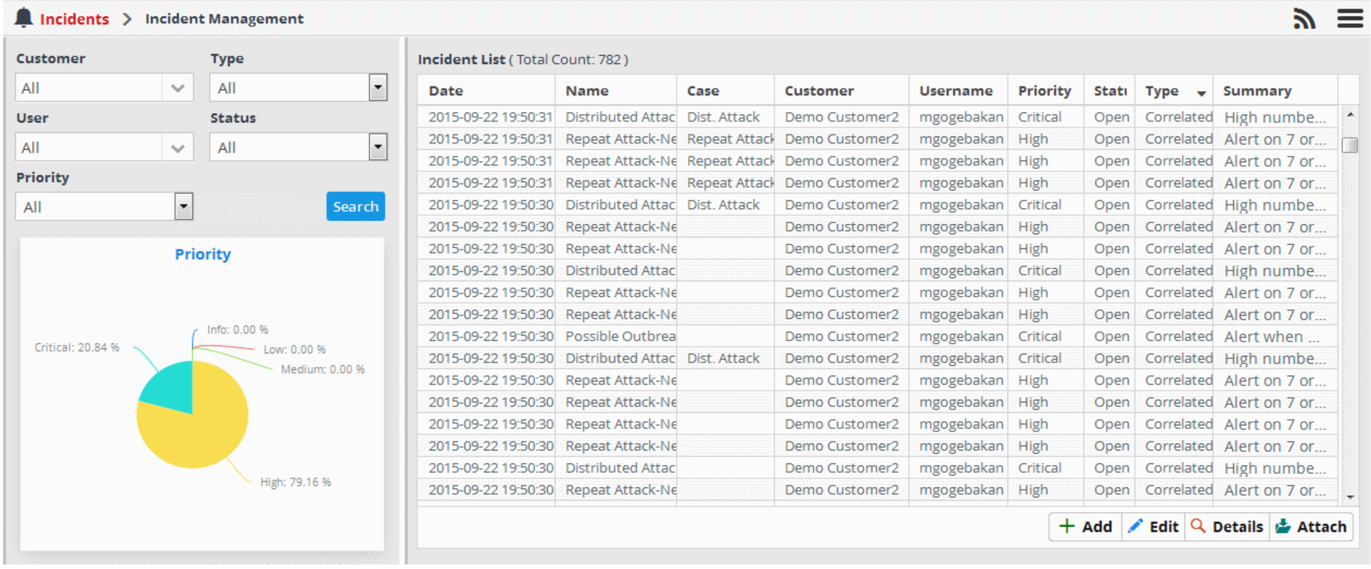
To view the list of incidents

- Click the 'Menu' button from the top right, choose 'Incidents' and then click 'Incident Management' to open the 'Incident Management' interface.
- Select the filter options from the left pane of the 'Incident Management' interface
  - To view all incidents without filtering, select 'All' in all the filter option drop-downs and click 'Search'.
  - To view incidents detected from specific customer networks, assigned to specific users, of specific type, status and/or priority, select the option(s) from the respective drop-downs and click 'Search'.

Tip: To view a list of all incidents on all customer networks in this interface, click the notification icon on the title bar:



The example below, shows all incidents from all customer networks.



Incident List (Total Count: 782)

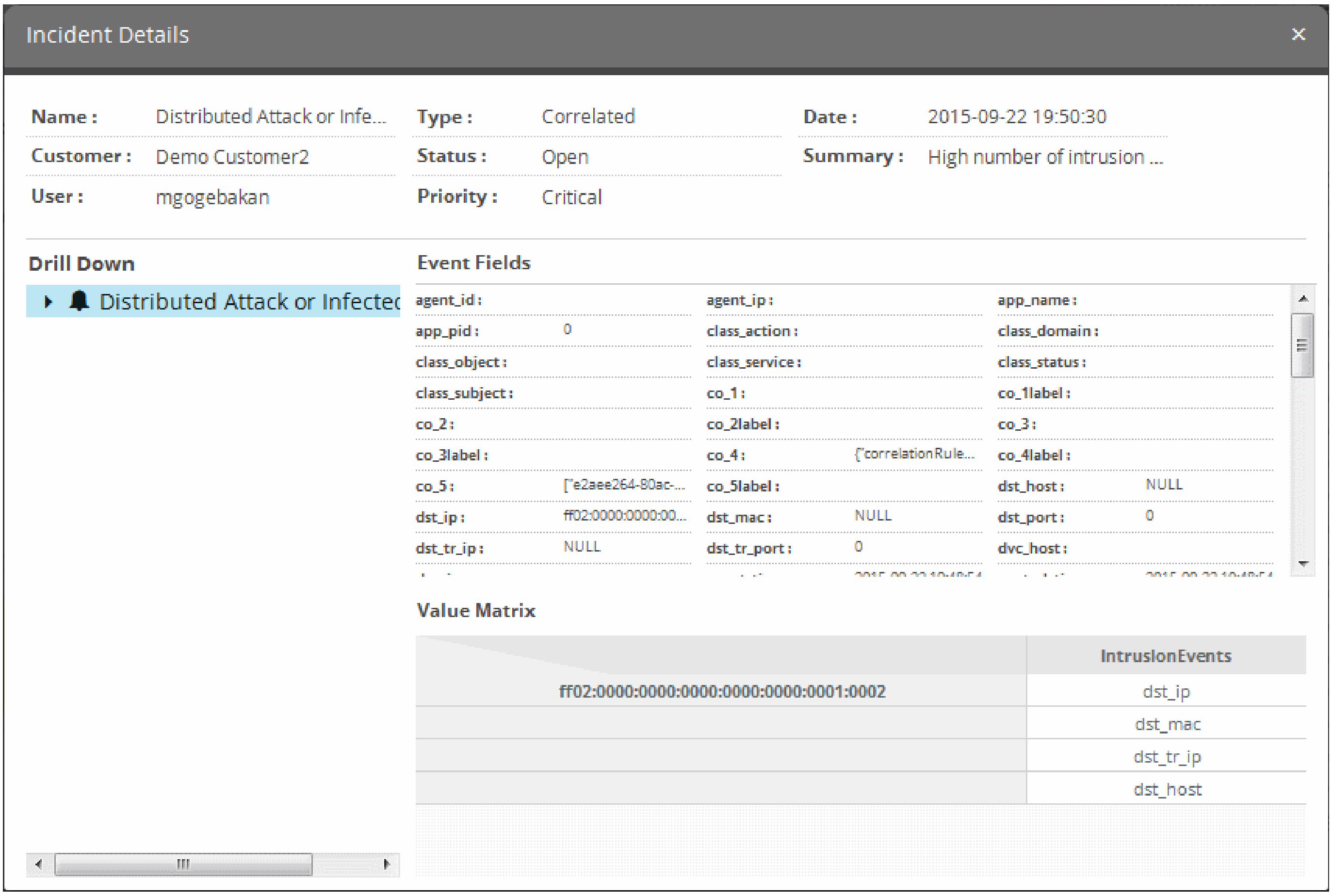
Date	Name	Case	Customer	Username	Priority	Statu	Type	Summary
2015-09-22 19:50:31	Distributed Attac	Dist. Attack	Demo Customer2	mgogebakan	Critical	Open	Correlated	High numbe...
2015-09-22 19:50:31	Repeat Attack-Ne	Repeat Attack	Demo Customer2	mgogebakan	High	Open	Correlated	Alert on 7 or...
2015-09-22 19:50:31	Repeat Attack-Ne	Repeat Attack	Demo Customer2	mgogebakan	High	Open	Correlated	Alert on 7 or...
2015-09-22 19:50:31	Repeat Attack-Ne	Repeat Attack	Demo Customer2	mgogebakan	High	Open	Correlated	Alert on 7 or...
2015-09-22 19:50:30	Distributed Attac	Dist. Attack	Demo Customer2	mgogebakan	Critical	Open	Correlated	High numbe...
2015-09-22 19:50:30	Repeat Attack-Ne		Demo Customer2	mgogebakan	High	Open	Correlated	Alert on 7 or...
2015-09-22 19:50:30	Repeat Attack-Ne		Demo Customer2	mgogebakan	High	Open	Correlated	Alert on 7 or...
2015-09-22 19:50:30	Distributed Attac		Demo Customer2	mgogebakan	Critical	Open	Correlated	High numbe...
2015-09-22 19:50:30	Repeat Attack-Ne		Demo Customer2	mgogebakan	High	Open	Correlated	Alert on 7 or...
2015-09-22 19:50:30	Repeat Attack-Ne		Demo Customer2	mgogebakan	High	Open	Correlated	Alert on 7 or...
2015-09-22 19:50:30	Possible Outbrea		Demo Customer2	mgogebakan	Critical	Open	Correlated	Alert when ...
2015-09-22 19:50:30	Distributed Attac	Dist. Attack	Demo Customer2	mgogebakan	Critical	Open	Correlated	High numbe...
2015-09-22 19:50:30	Repeat Attack-Ne		Demo Customer2	mgogebakan	High	Open	Correlated	Alert on 7 or...
2015-09-22 19:50:30	Repeat Attack-Ne		Demo Customer2	mgogebakan	High	Open	Correlated	Alert on 7 or...
2015-09-22 19:50:30	Repeat Attack-Ne		Demo Customer2	mgogebakan	High	Open	Correlated	Alert on 7 or...
2015-09-22 19:50:30	Repeat Attack-Ne		Demo Customer2	mgogebakan	High	Open	Correlated	Alert on 7 or...
2015-09-22 19:50:30	Distributed Attac		Demo Customer2	mgogebakan	Critical	Open	Correlated	High numbe...
2015-09-22 19:50:30	Repeat Attack-Ne		Demo Customer2	mgogebakan	High	Open	Correlated	Alert on 7 or...

The left panel displays a pie-chart showing a breakdown of incidents based on priority. Placing the mouse cursor over a sector displays the count of incidents and priority/severity level.

To view the details of an incident

- Select an incident that you want to view the details and click the 'Details' button at the bottom

The 'Incident Details' pane displays complete details such as the name of the rule that triggered the alert, name of the customer, type of incident and more, of the selected incident. It also allows the administrator to view the details of events detected by the same rule from other endpoints in the same customer network at different time points. Use the 'Drill Down' report to view all the devices affected by the incident.



Incident Details

Name :	Distributed Attack or Infe...	**Type :**	Correlated	**Date :**	2015-09-22 19:50:30
Customer :	Demo Customer2	**Status :**	Open	**Summary :**	High number of intrusion ...
User :	mgogebakan	**Priority :**	Critical		

Drill Down

Distributed Attack or Infected

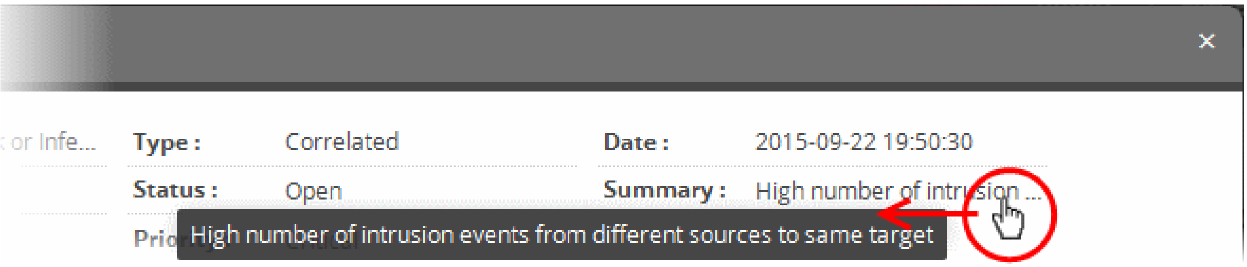
Event Fields

agent_id :		agent_ip :		app_name :	
app_pid :	0	class_action :		class_domain :	
class_object :		class_service :		class_status :	
class_subject :		co_1 :		co_1label :	
co_2 :		co_2label :		co_3 :	
co_3label :		co_4 :	{"correlationRule...	co_4label :	
co_5 :	["e2aee264-80ac-...	co_5label :		dst_host :	NULL
dst_ip :	ff02:0000:0000:00...	dst_mac :	NULL	dst_port :	0
dst_tr_ip :	NULL	dst_tr_port :	0	dvc_host :	

Value Matrix

	IntrusionEvents
ff02:0000:0000:0000:0000:0000:0001:0002	dst_ip
	dst_mac
	dst_tr_ip
	dst_host

The upper portion displays the details like name of the rule that triggered the incident, name of the customer, type of incident, date and time the incident was created and so on. Placing the mouse cursor over an item shows the full details as a tool tip.



or Infe...	**Type :**	Correlated	**Date :**	2015-09-22 19:50:30
	Status :	Open	**Summary :**	High number of intrusion ...
	Prio			

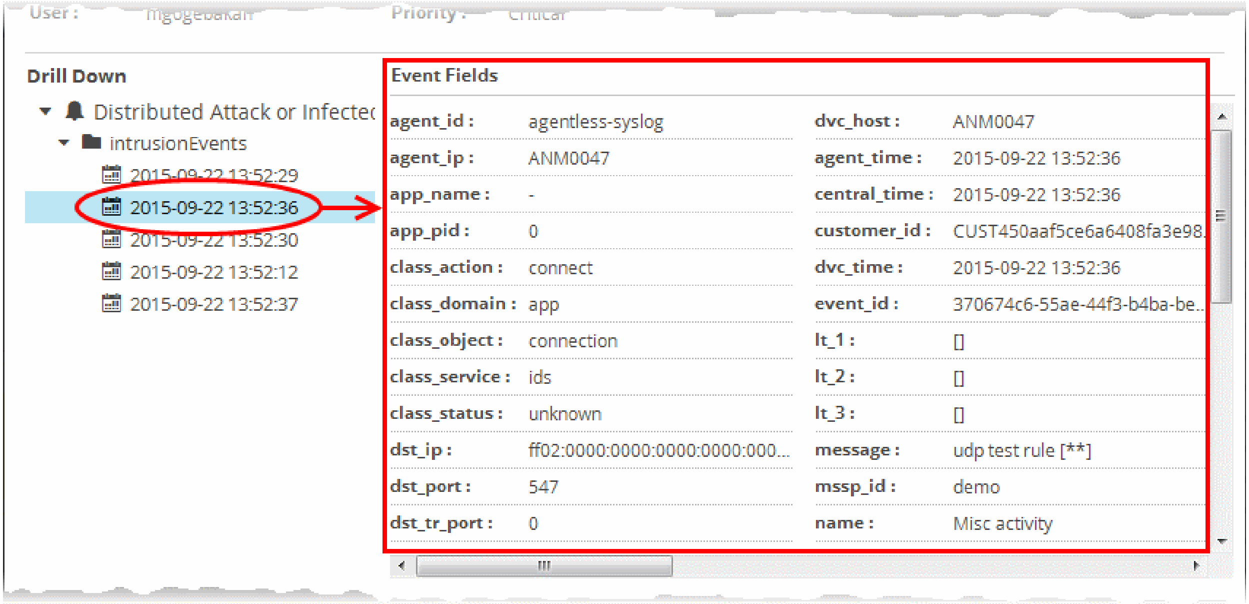
High number of intrusion events from different sources to same target

The 'Event Fields' pane at the right displays the values of all the fields of the event detected as the incident. The 'Value Matrix' pane at the bottom right displays the aggregation values fed by the rule from the detected event, in order to generate a new event indicating the event detection by it.

The 'Drill Down' pane at the left allows you to view the details of the 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.



Drill Down
- Distributed Attack or Infected
  - intrusionEvents
    - 2015-09-22 13:52:29
    - 2015-09-22 13:52:36
    - 2015-09-22 13:52:30
    - 2015-09-22 13:52:12
    - 2015-09-22 13:52:37

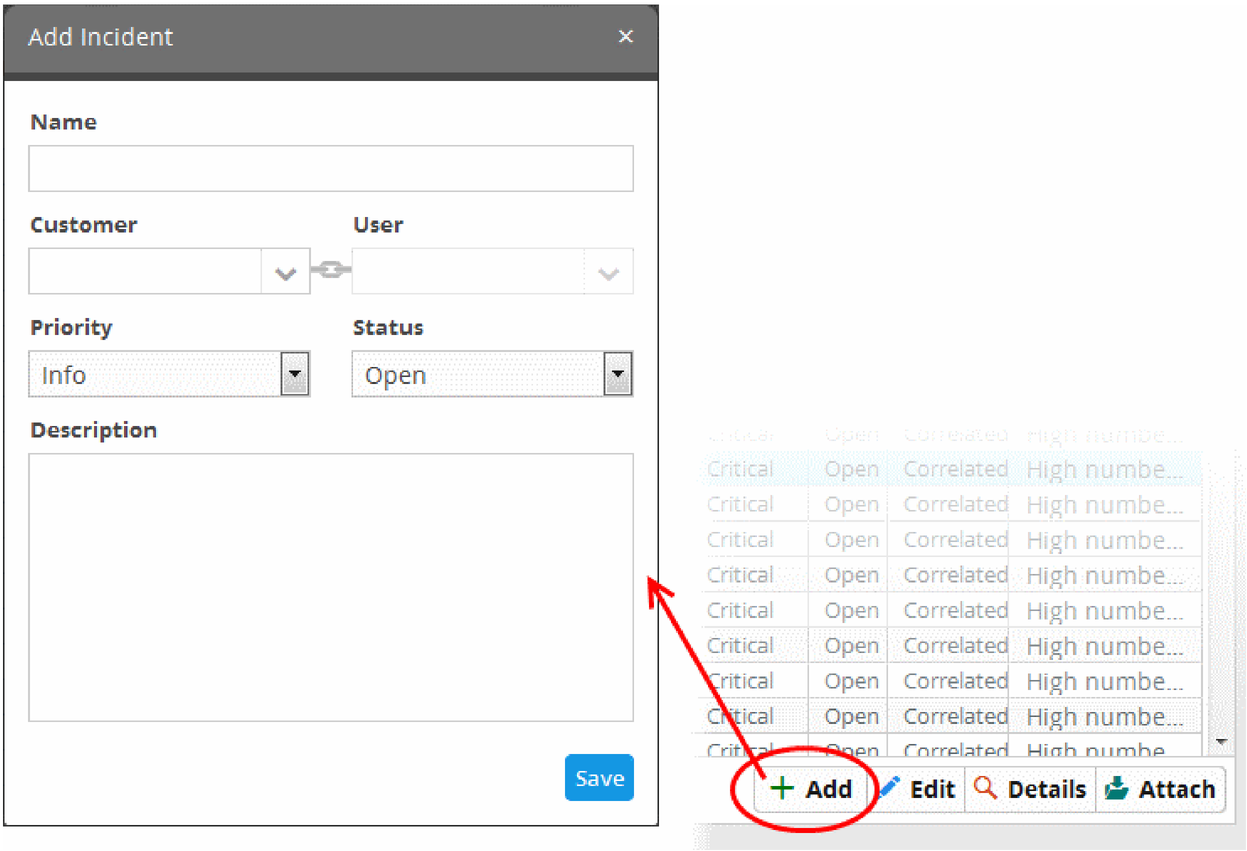
Event Fields

agent_id :	agentless-syslog	dvc_host :	ANM0047
agent_ip :	ANM0047	agent_time :	2015-09-22 13:52:36
app_name :	-	central_time :	2015-09-22 13:52:36
app_pid :	0	customer_id :	CUST450aaf5ce6a6408fa3e98
class_action :	connect	dvc_time :	2015-09-22 13:52:36
class_domain :	app	event_id :	370674c6-55ae-44f3-b4ba-be...
class_object :	connection	lt_1 :	[]
class_service :	ids	lt_2 :	[]
class_status :	unknown	lt_3 :	[]
dst_ip :	ff02:0000:0000:0000:0000:000...	message :	udp test rule [**]
dst_port :	547	mssp_id :	demo
dst_tr_port :	0	name :	Misc activity

To add and assign an incident

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

The 'Add Incident' dialog will open.



Add Incident

Name

Customer

User

Priority

Info

Status

Open

Description

- **Name** - Enter a name for the incident.
- **Customer** - Choose the customer from the drop-down for whom you want to add the incident.
- **User** - The drop-down will display the users assigned to the selected customer. Choose the user to whom the incident is to be assigned. Refer to the section '**Administration**' for details about assigning users to customers.

- **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

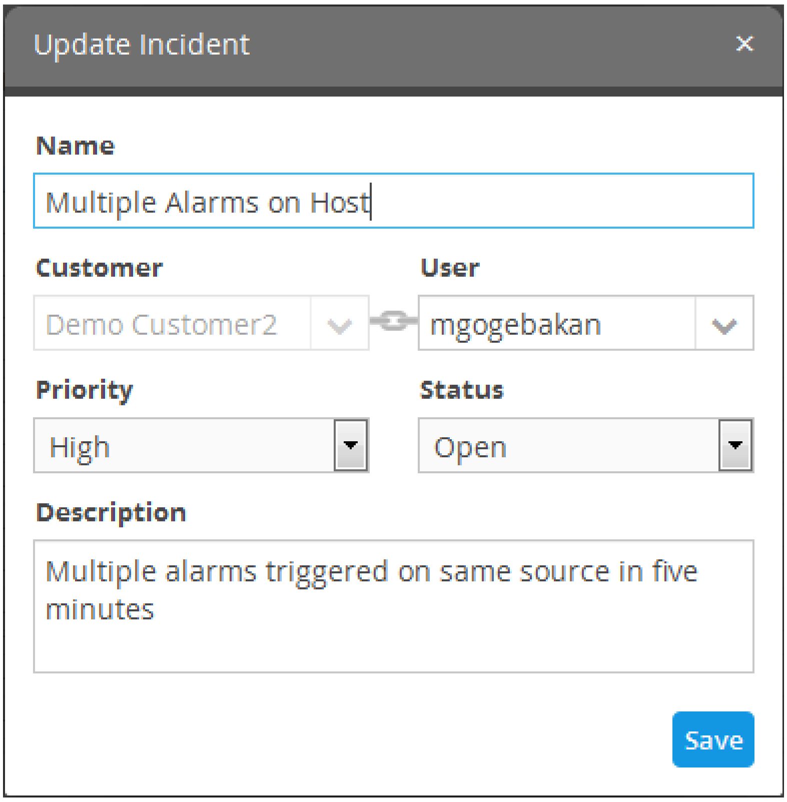
Editing and Reassigning an Incident

You can change the status, edit the name, severity level of an incident at any time. You can also reassign an incident to a different user if required.

To edit an incident

- Use the filter options at the left to view the list of incidents pertaining to a specific customer, assigned to a specific user, specific type, status and/or priority level .
- Select the incident that you want to edit from the list and click the 'Edit' button at the bottom.

The 'Update Incident' dialog will be displayed.



Update Incident

Name: Multiple Alarms on Host

Customer: Demo Customer2

User: mgogebakan

Priority: High

Status: Open

Description: Multiple alarms triggered on same source in five minutes

- Edit the details like Name, priority, status as required.
- To reassign the incident select the new user to whom the incident has to be assigned, from the User drop-down.

Note: The 'User' drop-down will display only the users that are added for the customer. Refer to the section '**Administration**' for details about assigning users to customers.

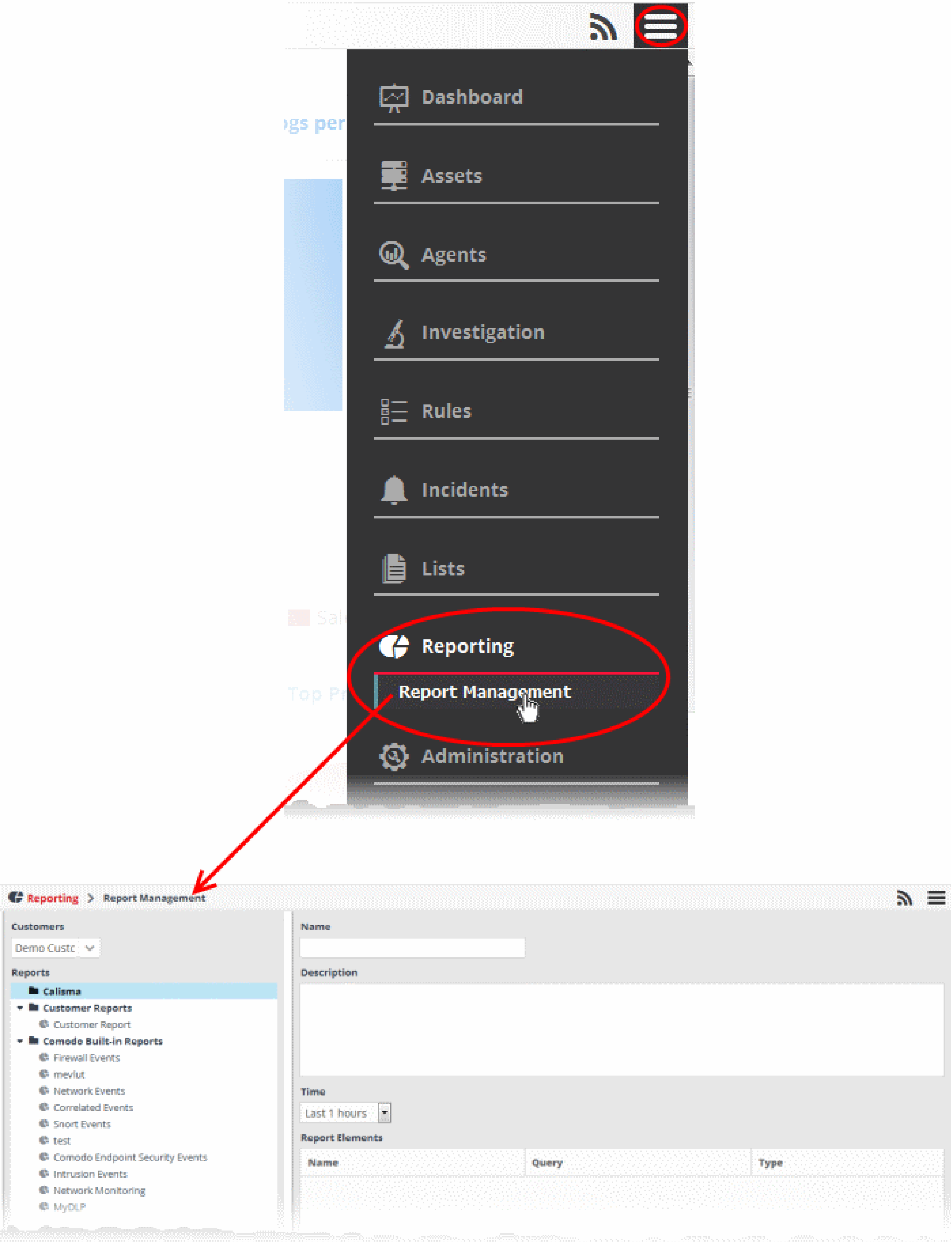
- Click the Save button for your changes to take effect.

Step 7 - Generate reports

NxSIEM allows you to configure and generate event reports covering a wide range of security and productivity criteria, by fetching data from the results of selected event queries. The reports can display details of events matching events queries added for a customer, as tables, pie charts and bar charts.

NxSIEM ships with a set of pre-configured report types under different category folders. You can configure custom reports too as required.

To open the Report Management interface, click the 'Menu' button from the top right, choose 'Reporting' and then click 'Report Management'.



The left hand side panel of the interface displays a list of predefined reports and custom queries added for the selected customer under respective category folders. The right hand side panel displays the configuration area for report generation.

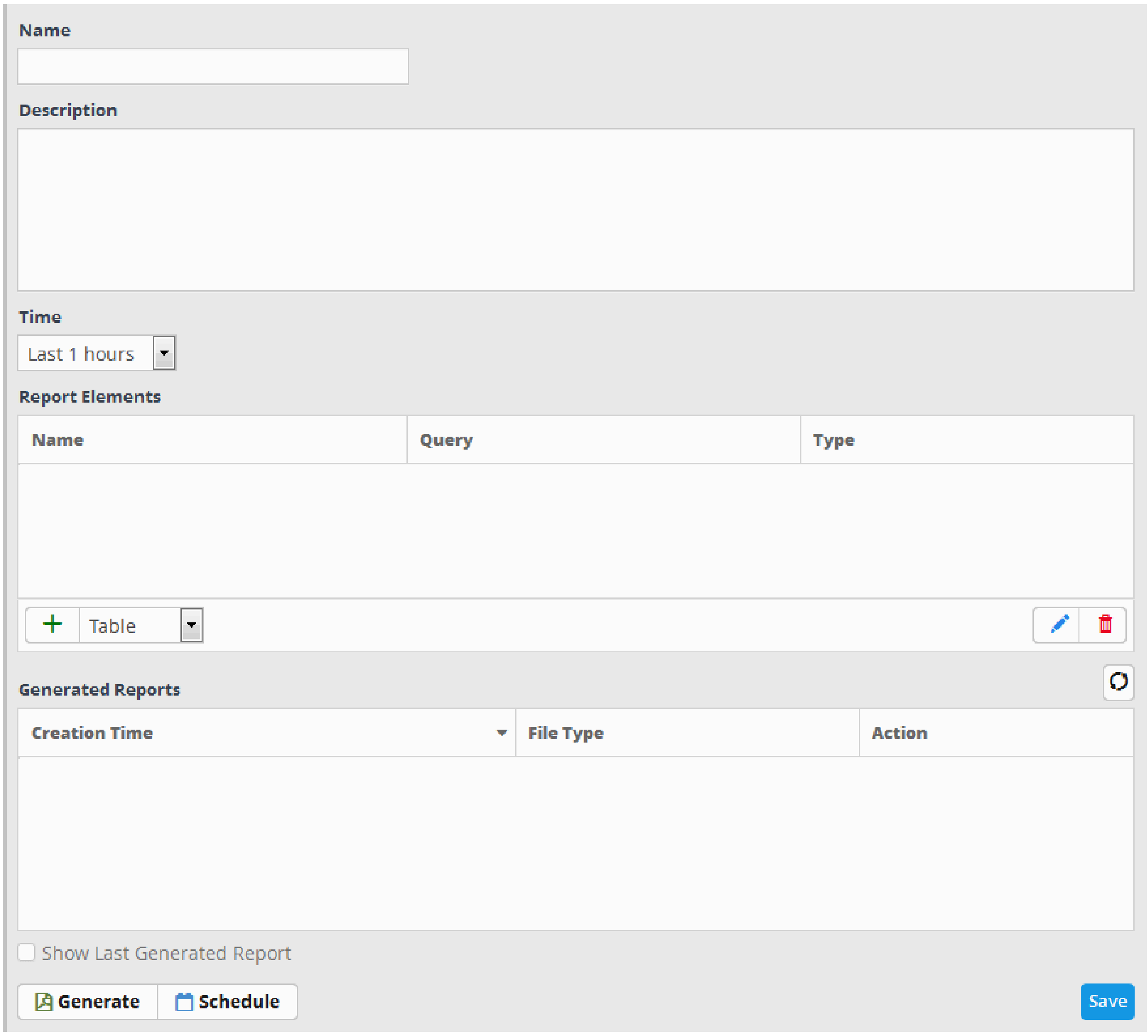
To configure a new report type for a customer

- Choose the 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 under 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. It has four areas:



Name

Description

Time: Last 1 hours

Report Elements

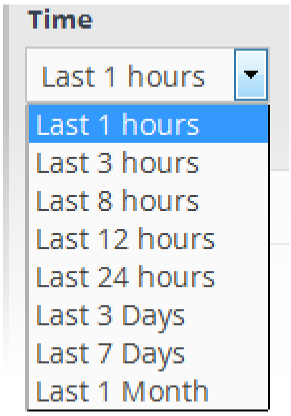
Name	Query	Type

Generated Reports

Creation Time	File Type	Action

□ Show Last Generated Report

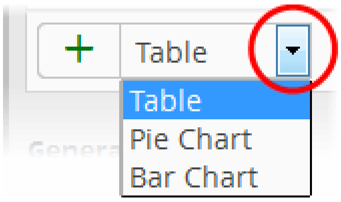
- Enter a name for the report in the 'Name' field
- Enter an appropriate description for the report in the 'Description' text box
- Select the period for which the events are to be included in the report, from the 'Time' drop-down



The period options range from last one hour to the entire previous month of the report generation time.

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.



The options available are:

- **Table** - The report component will contain the details of the events that match the query selected. Refer to the **explanation on adding a table** given below, for more details.
- **Pie Chart** - The report will contain a pie-chart showing the statistical summary of the events that are aggregated based on parameters configured for the chart. Refer to the **explanation on adding a pie chart** given below , for more details.
- **Bar chart** - The report will contain a bar-chart showing the statistical summary of the events that are aggregated based on parameters configured for the chart. Refer to the **explanation on adding a bar chart** given below , for more details.

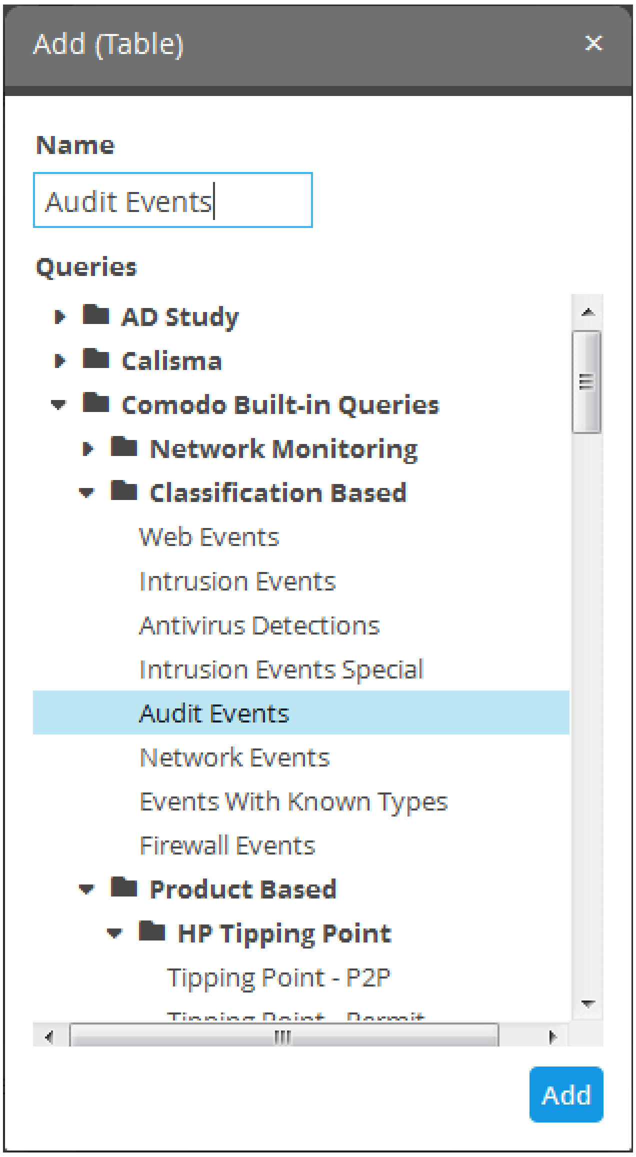
'Table' type Report Element

The Table Type report is configured just by selecting the event query from the list of queries added for the customer. The resultant report will contain all the details of the events that match the query, detected within the selected time period, displayed as a table.

To add a Table type report

- Select 'Table' from the drop-down and click the + button beside it.

The configuration dialog for adding a report table will appear with a list of all event queries configured for the customer.



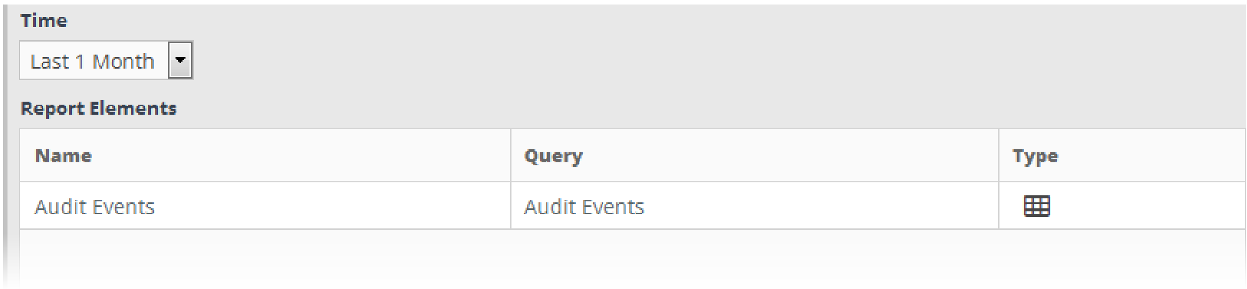
Add (Table)

Name: Audit Events

Queries

- Enter the name for the report element in the 'Name' field.
- Select the event query for which you want to generate a report in table format.
- Click the 'Add' button.

The report element will be added to the report.



Time: Last 1 Month

Report Elements

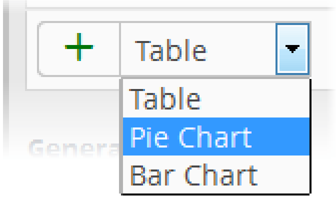
Name	Query	Type
Audit Events	Audit Events	▦

'Pie Chart' type and Bar Chart Type Report Elements

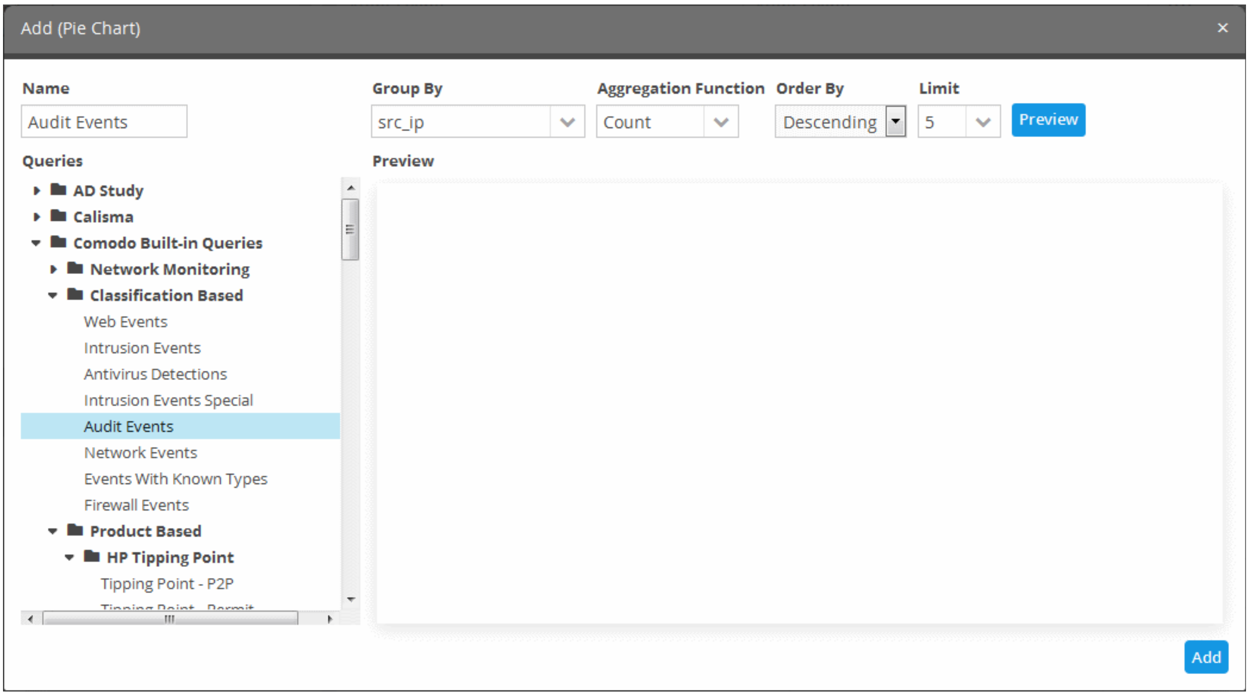
The chart type report is configured just by selecting the event query from the list of queries added for the customer. The resultant report will contain all the details of the events that match the query, detected within the selected time period, displayed as a pie-chart or a bar chart as chosen.

To add a Pie Chart type or Bar chart type report

- Select 'Pie Chart'/'Bar chart' as required. from the drop-down and click the + button beside it



The configuration dialog for adding a report pie chart will appear with a list of all event queries configured for the customer at the left.


Add (Pie Chart)

Name: Audit Events

Group By: src_ip

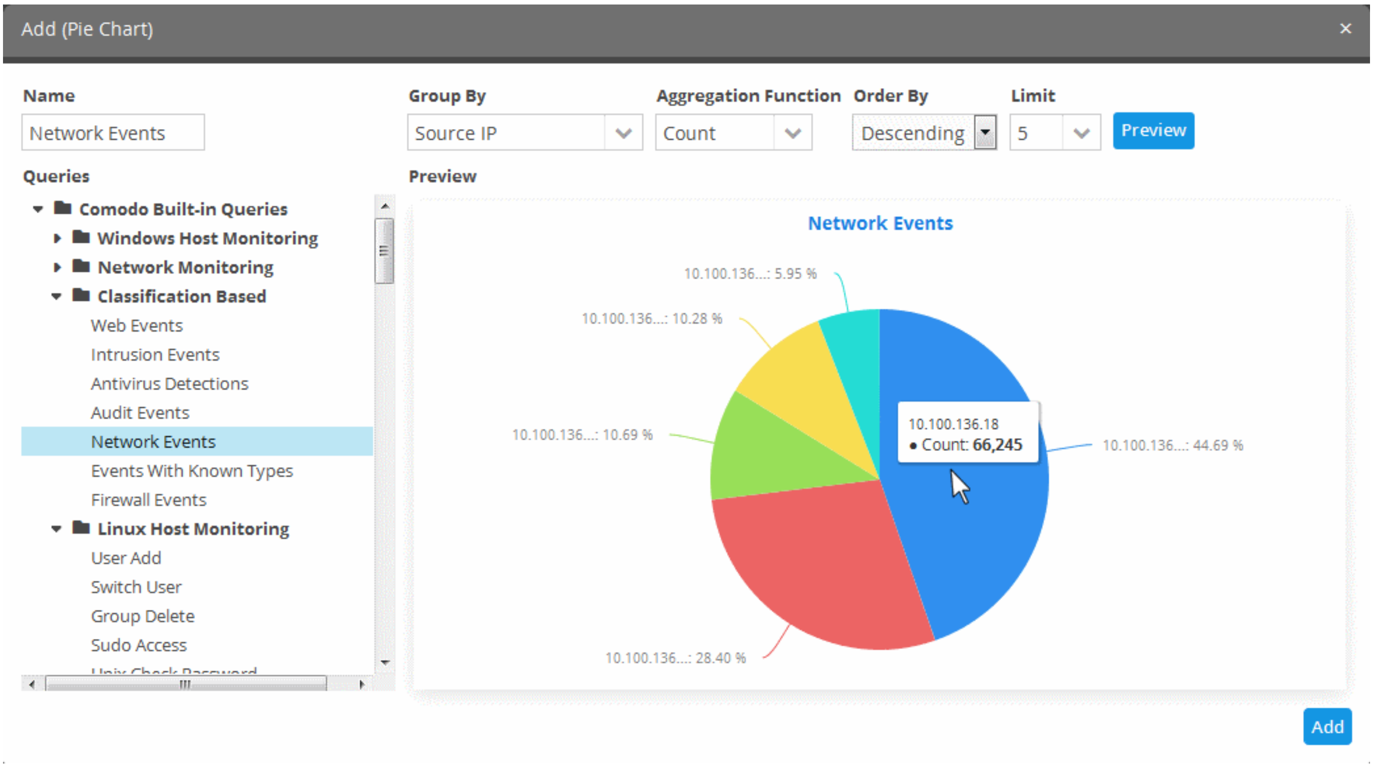
Aggregation Function: Count

Order By: Descending

Limit: 5

The configuration parameters for the report chart are similar to those for creating a dashboard chart in custom dashboard generation. Refer to the section explaining **Configuring Custom Dashboards** in the section **Step 5 - Creating Custom Dashboards for Customer Networks** for a detailed explanation of the parameters and a tutorial in configuring them.

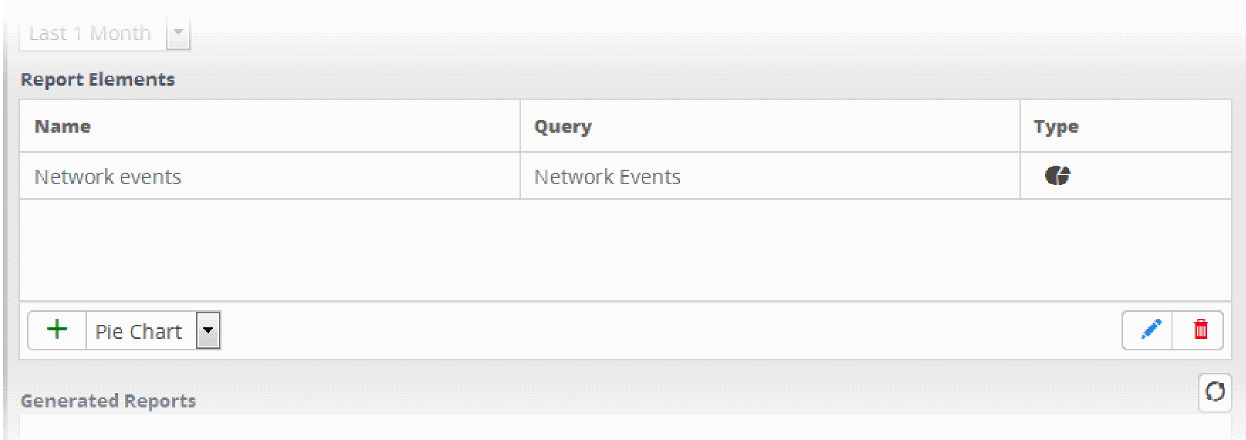
- Click the 'Preview' button to check the chart before adding it to the report.



Add (Pie Chart)

Name	Group By	Aggregation Function	Order By	Limit
Network Events	Source IP	Count	Descending	5

- Click the 'Add' button



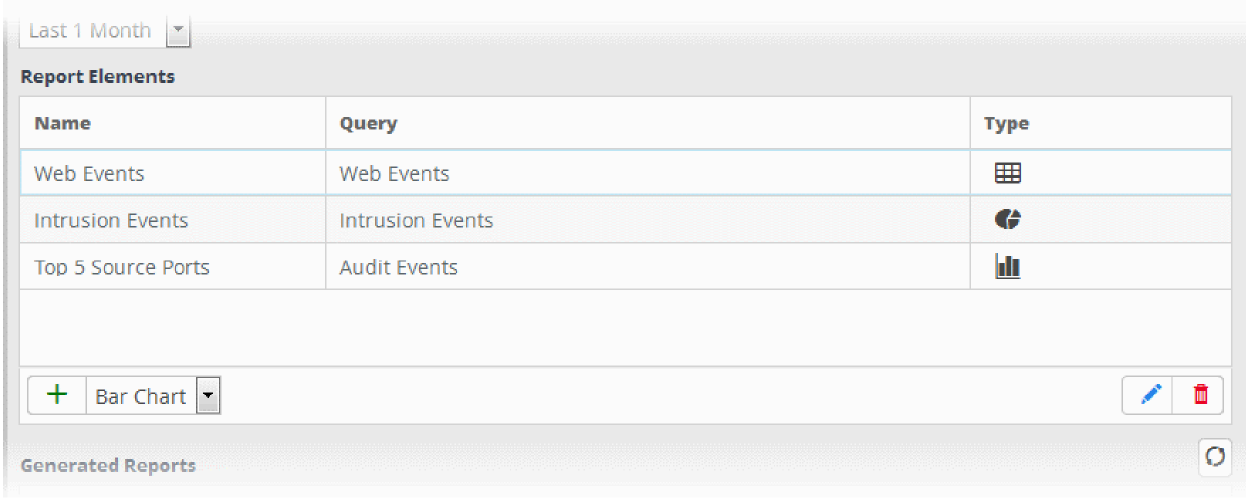
Last 1 Month

Report Elements

Name	Query	Type
Network events	Network Events	●

- Repeat the process to add more report elements to the report.

The 'Report Elements' area displays the list of report components added to the report.



Last 1 Month

Report Elements

Name	Query	Type
Web Events	Web Events	▦
Intrusion Events	Intrusion Events	◕
Top 5 Source Ports	Audit Events	▮

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

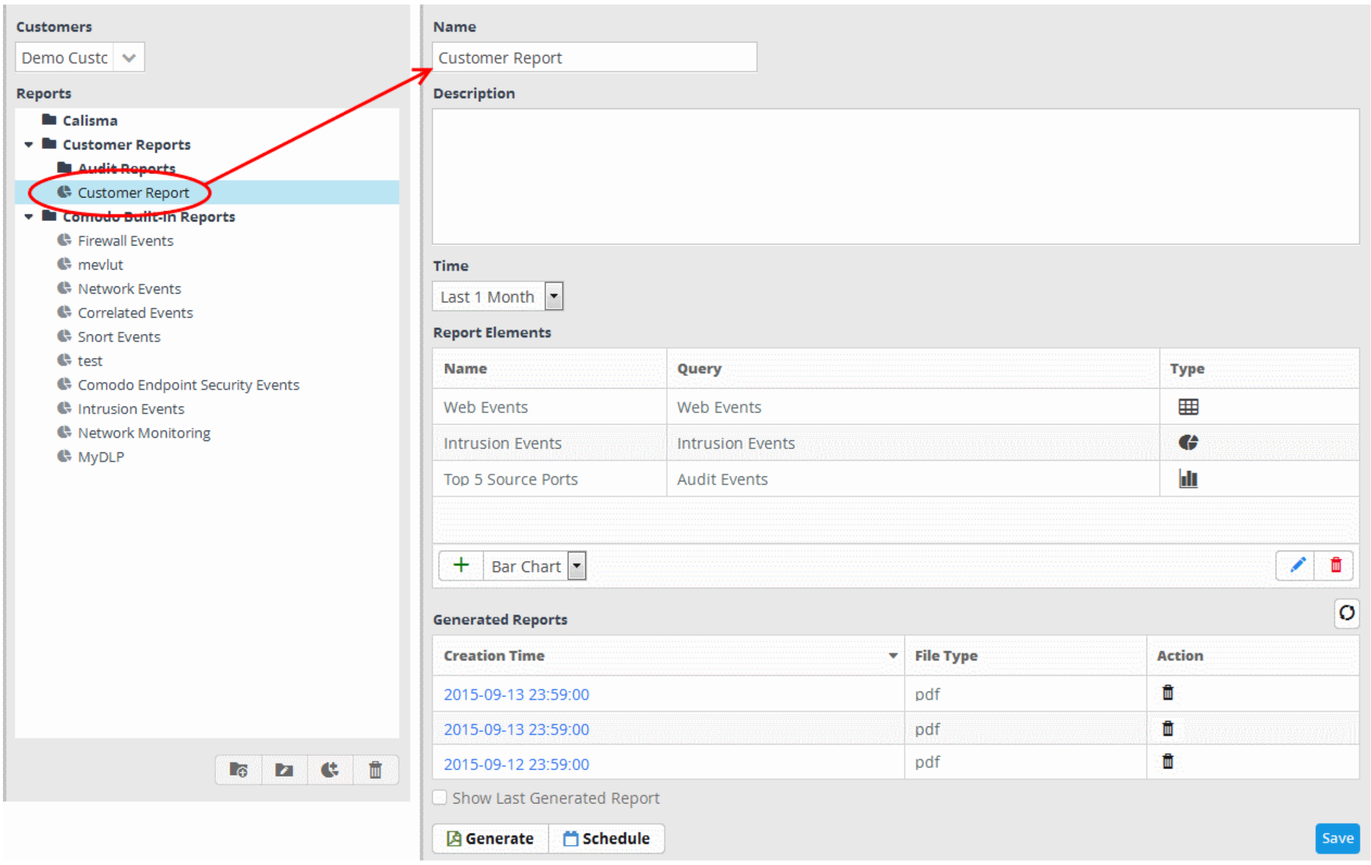
- Select the report from the list.

The details of the report with the list of report elements will be displayed in the configuration area at the right.

- 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.

The 'Generated Reports' area displays a list of reports generated manually or as per the schedule created for the report.



Name: Customer Report

Description:

Time: Last 1 Month

Report Elements

Name	Query	Type
Web Events	Web Events	▦
Intrusion Events	Intrusion Events	●
Top 5 Source Ports	Audit Events	📊

Generated Reports

Creation Time	File Type	Action
2015-09-13 23:59:00	pdf	🗑
2015-09-13 23:59:00	pdf	🗑
2015-09-12 23:59:00	pdf	🗑

□ Show Last Generated Report

- To download the report, click the time stamp under the 'Creation Time' column.
- To view the report instantly select the 'Show Last Generated Report' check box.

Schedule a Report Generation

You can automate the process of report generation according to a schedule of your choice.

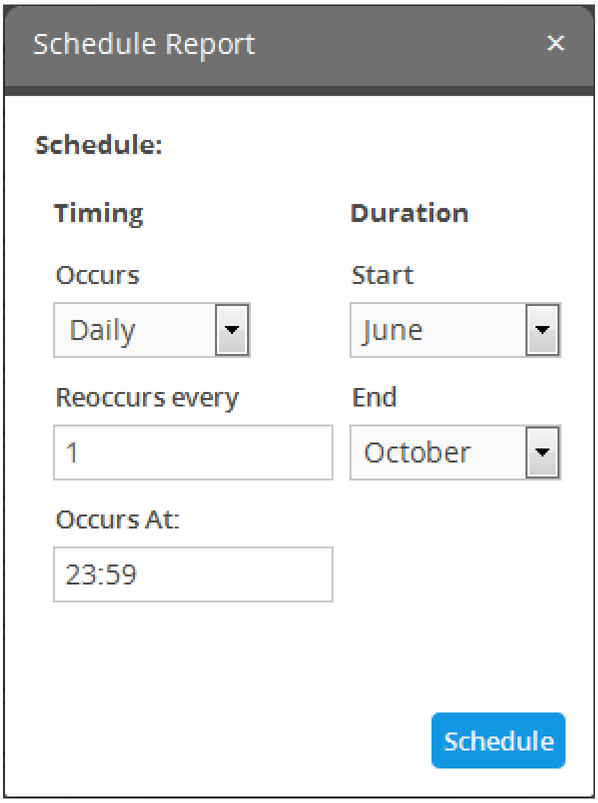
To schedule a report generation

- 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.



Occurs: Daily

Reoccurs every: 1

Occurs At: 23:59

Start: June

End: October

The 'Timing' section allows you to define the frequency for report generation.

- **Occurs -** Select the period for report generation from the drop-down.
- **Reoccurs every -** Enter the frequency for report generation as per the chosen days. For example, if you select 'Daily' and enter 2, then the agent will collect the logs once in every 2 days
- **Occurs At -** Enter the exact time at which the report is to be generated at the set days.

The 'Duration' section allows you to define the start and end days for the period of report generation.

  - **Start** - Select the start month from the drop-down
  - **End** - Select the end month from the drop-down
- Click the 'Schedule' button.

A confirmation message will be displayed at the top right side of the screen. The reports will be automatically generated as per the schedule 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.

About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ, 07013

United States

Email: **EnterpriseSolutions@Comodo.com**

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford
Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit **http://www.comodo.com.**