# Comodo

## Next Generation Security Information and Event Management

Software Version 1.4

# Administrator Guide

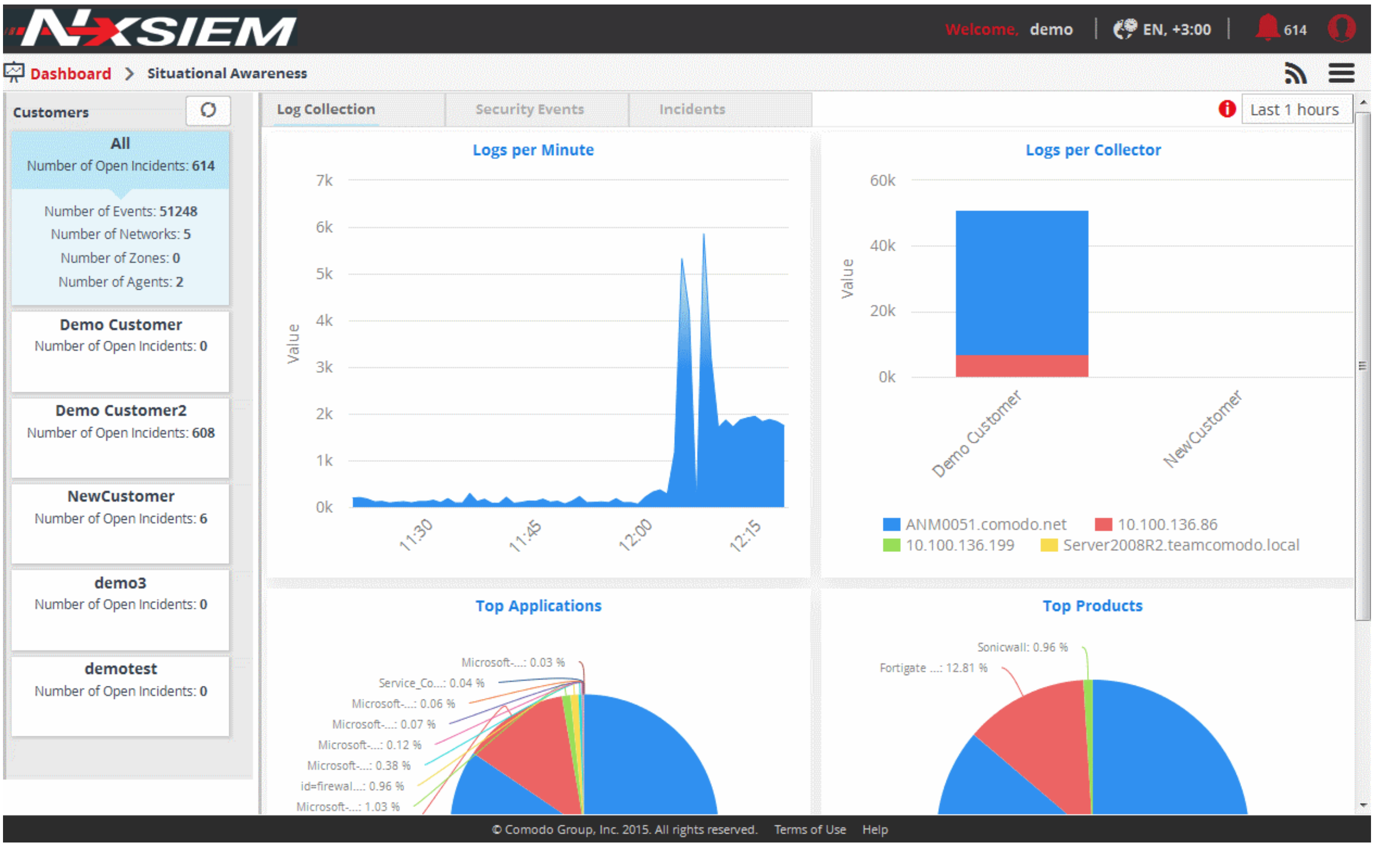
Guide Version 1.4.101915

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

# Table of Contents

# 1 Introduction to Comodo NxSIEM

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



All
Number of Open Incidents: 614
Number of Events: 51248
Number of Networks: 5
Number of Zones: 0
Number of Agents: 2

Demo Customer
Number of Open Incidents: 0

Demo Customer2
Number of Open Incidents: 608

NewCustomer
Number of Open Incidents: 6

demo3
Number of Open Incidents: 0

demotest
Number of Open Incidents: 0

### Features

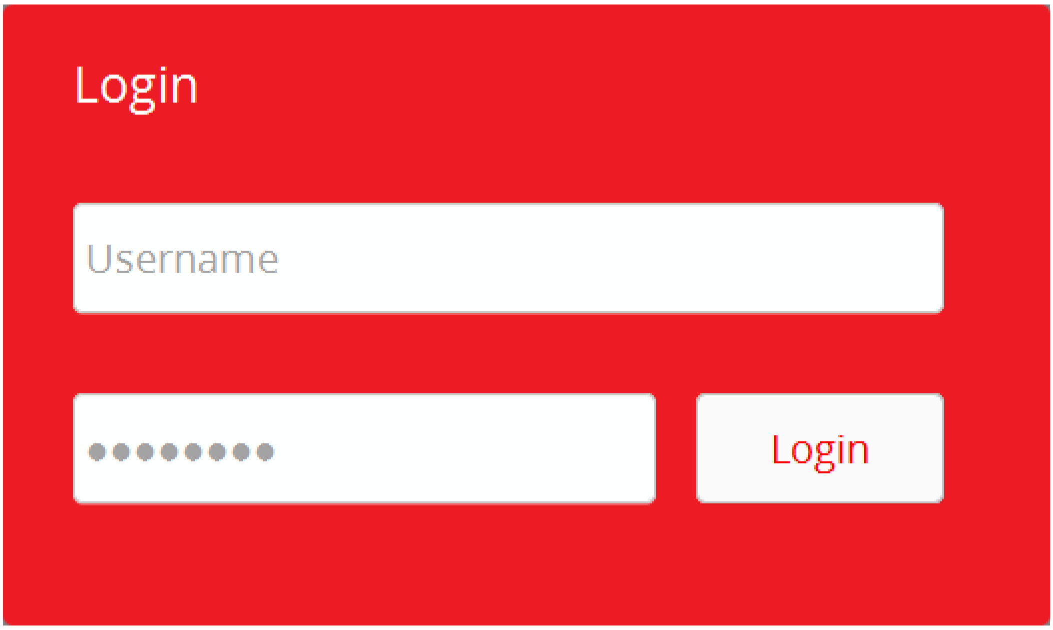
- Real-time event monitoring and processing
- Long-term log retention, archiving and backup
- Multiple 'Ready-to-go' queries to address typical use-cases
- Powerful query creation interface for custom queries
- Configurable custom dashboards
- Custom report generation and report scheduling
- Incident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

### Guide Structure

This guide is intended to take you through the configuration and use of Comodo Managed Security Service Provider Platform and is broken down into the following main sections.

## 1.1 Logging-in to the Administrative Console

Comodo NxSIEM service is a offered as a web based application, its administrative interface can be accessed using any browser. Enter the URL of Comodo NxSIEM that was provided at the time of subscription to the service.

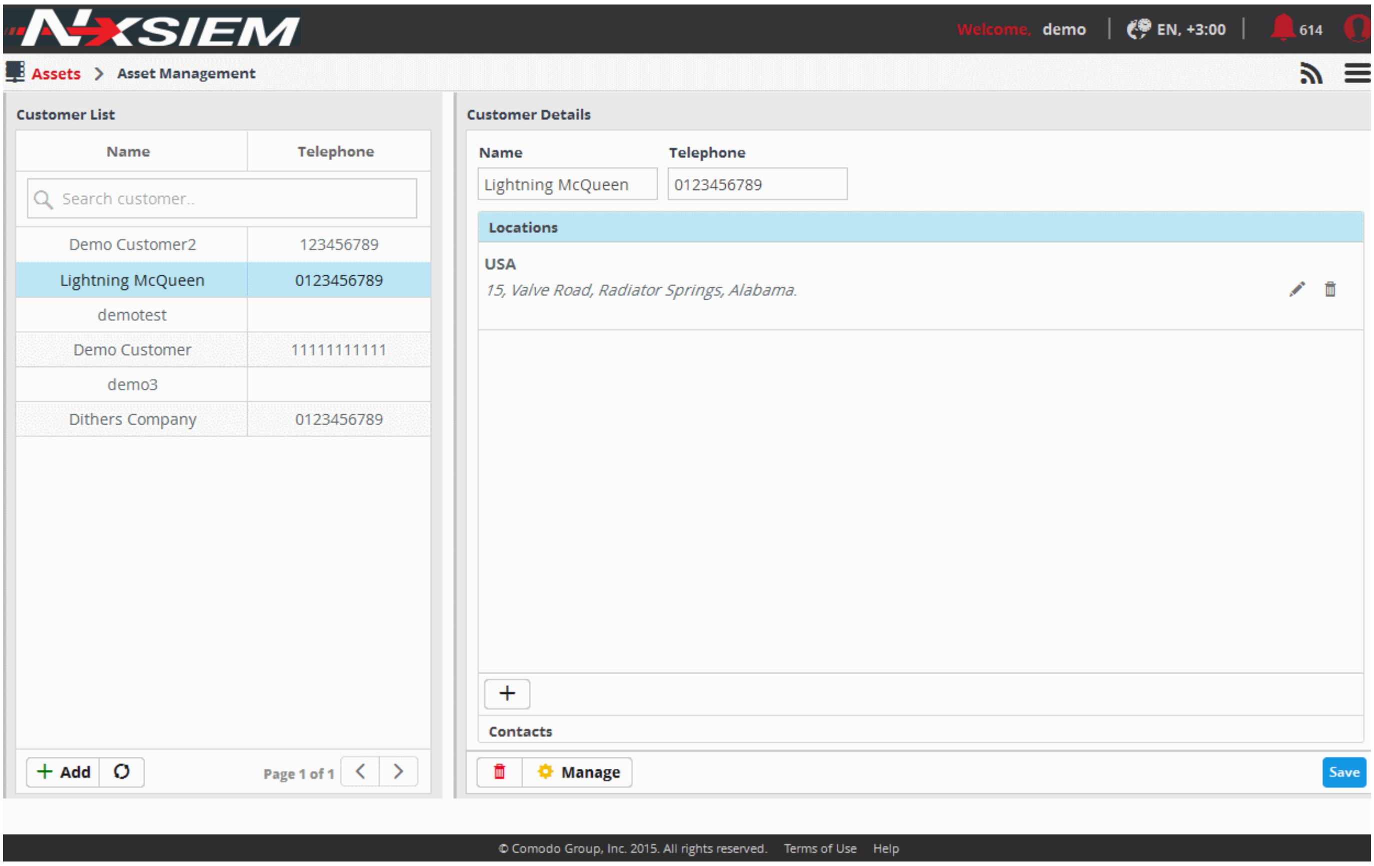


- Enter the username and password in the respective fields and click 'Login'.

> **Tip**: After the first login you can change the sub-domain name in the URL at anytime from the License and Subscription interface. Refer to the section **Viewing License and Subscription Details and Configuring NxSIEM Platform URL** for more details.

# 2 The Main Interface

The Administrative Console is the nerve center of Comodo NxSIEM, allowing administrators to add customers, enroll networks and endpoints, create polices for collecting different kinds of logs and more.


NXSIEM
Welcome, demo
EN, +3:00
614
Assets > Asset Management
Add
Page 1 of 1
Manage
Save
© Comodo Group, Inc. 2015. All rights reserved. Terms of Use Help

Customer List

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

Customer Details

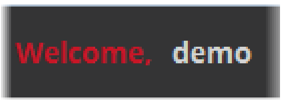
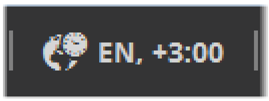
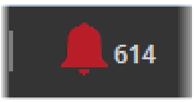
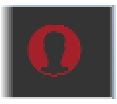
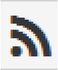
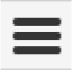
Name: Lightning McQueen
Telephone: 0123456789

Locations

USA
*15, Valve Road, Radiator Springs, Alabama.*

Contacts

Once logged-in, the title bar displays the administrator's 'Usename', region and language, the number of incidents, and options to change the administrator's profile settings and password. The main configuration area is displayed depending on the option chosen from the drop-down, that appears on clicking the menu button at the top right. The following table explains the elements in the title bar.

| Title Bar Controls - Descriptions | |
|---|---|
|  | Displays the username of the currently logged-in administrator |
|  | Displays the location, language and time zone settings as per the currently logged-in administrator. |
|  | Displays the number of incidents detected. Clicking on the notification icon opens the Incident Management interface that allows the administrator to view the list of incidents from all the customers, assign them to respective administrative users, create cases and assign them to administrative users. Refer to the section **Incidents and Cases** for more details. |
|  | Allows the currently logged-in administrator to edit their location and language, change their login password and logout of the console. Refer to the following section '**Changing Password and Language Settings**' for more details. |
|  | Operational Feeds button - Clicking this button displays the batch operations that were completed and currently running, for example, customer creation and so on. |
|  | Navigational Menu button - Clicking this button allows administrators to navigate to the required main functional areas of the console: Dashboard, Assets, Agents, Investigation, Rules, Incidents, Live Lists, Reporting and Administration. |

**Main Functional Areas**

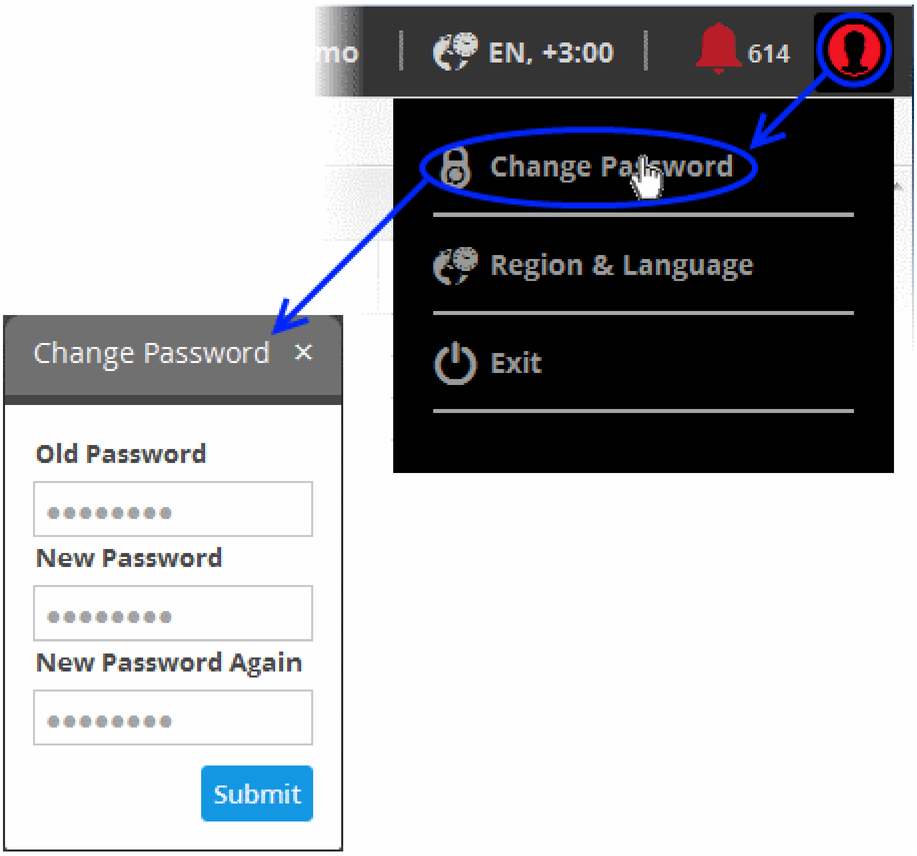
- **Dashboard** - Allows the administrator to view graphical summary of all occurred events, top detected applications, most active agents, attack sources, firewall event sources and more. Refer to the section '**The Dashboard**' for more details.
- **Assets** - Allows the administrator to add new customers, manage existing customers, add and manage networks for the customers, configuring Nxlog and syslog servers and more. Refer to the section '**Customer Asset Management**' for more details.
- **Agents** - Allows the administrator to download MSSP agent for Windows and Linux, manage the agents that are installed on systems, create polices for the purpose of collecting various kinds of logs from devices, systems and more. Refer to the section '**Log Collection Agents and Policies**' for more details.
- **Investigation** - Allows administrators to create event queries and view the results from event queries in pie charts, bar charts and spider charts. Refer to the section '**Query Management**' for more details.
- **Rules** - Allows the administrator to create rules for analyzing the processed logs and to provide alerts for certain conditions. Refer to the section '**Managing Rules**' for more details.
- **Incidents** - Allows the administrator to manage incidents, both Correlated Incidents and Default Incidents, assign/reassign incidents to users, create groups of incidents as cases and assign to users and more. Refer to the section '**Incidents and Cases**' for more details.
- **Lists** - Allows the administrator to create lists of values for fields like sources, destinations, networks, that can be used in creating event queries and correlation rules. Refer to the section **Live Lists** for more details.
- **Reporting** - Allows the administrator to generate customer specific reports. The reports are available for different kinds of events such as login failures and successes, suspicious login attempts and more. Refer to the section '**Managing Reports**' for more details.
- **Administration** - Allows administrators to view a summary of logs collected from different customers, add and manage administrative users and assign them to specific customer(s), view license and subscription details and set the sub-domain name for configuring Access URL for the administrative interface . Refer to the section '**Administration**' for more details.

## Changing Password and Language Settings

The administrator can change their location and language settings and login password by clicking the user icon displayed at the right end of the title bar.

**To change the password**

- Click the button and choose 'Change Password' from the drop-down.



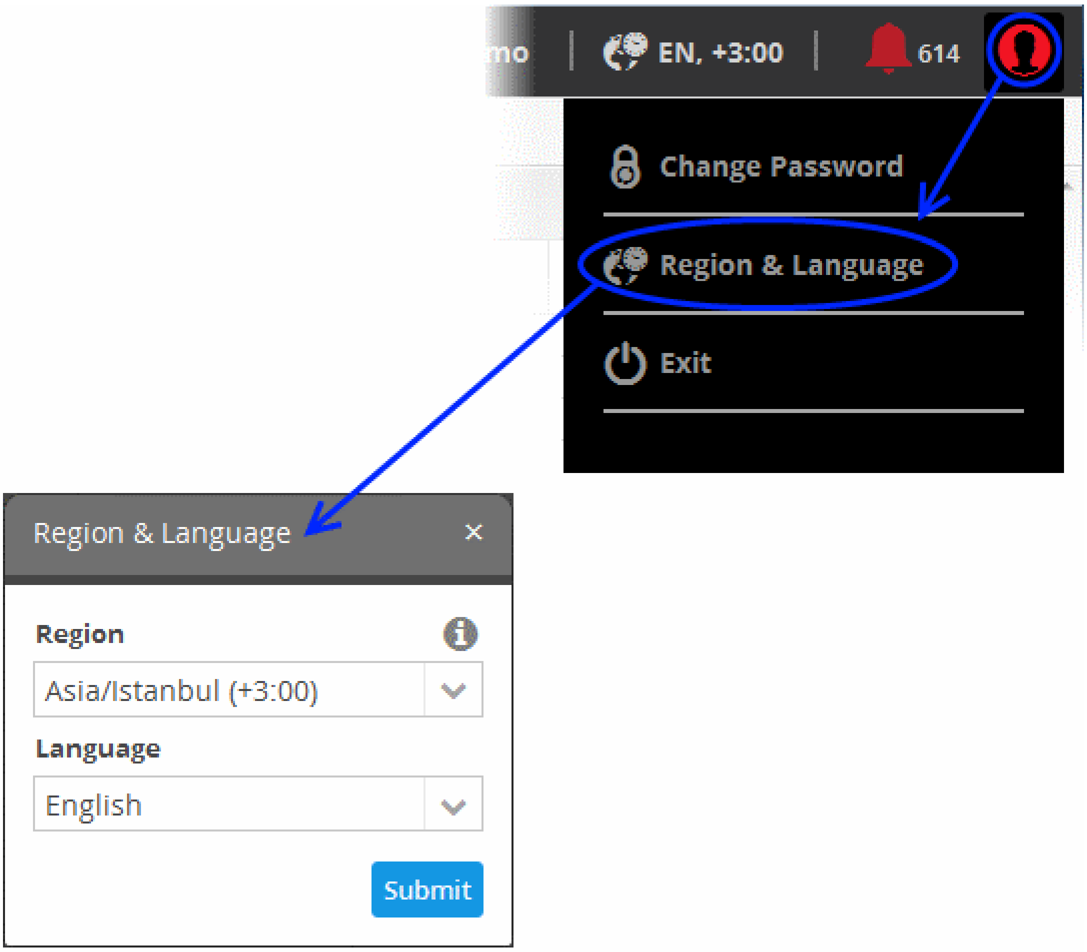
The 'Change Password' dialog will appear.

- Enter your current password in the 'Old Password' field
- Enter your new password in the 'New Password' field and confirm it in the next field.
- Click the 'Submit' button.

Use the new password next time you login to the NxSIEM platform.

**To change the Region and Language Settings**

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



Region: Asia/Istanbul (+3:00)

Language: English

The 'Region and Language' dialog will appear.

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

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

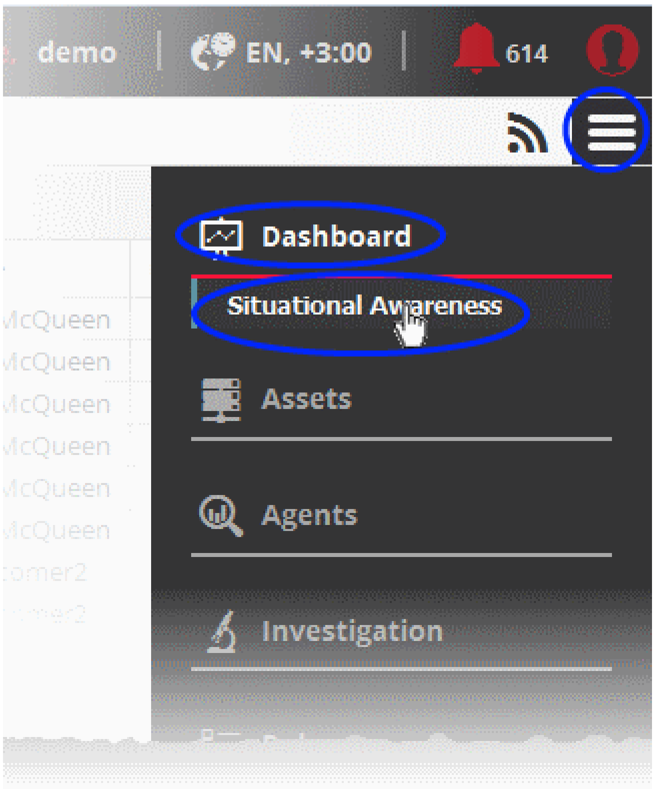
# 3 The Dashboard

The dashboard provides a snapshot summary of collected logs, events and incidents that were detected from customer networks for a selected period of time. This allows administrators to more effectively track customer progress, diagnose potential issues and to make informed decisions should corrective actions need to be taken. The default view shows the details collected for all enrolled customers. The administrator can filter the statistics for specific customer by selecting the customer from the left and for time periods ranging from last one hour  to previous 24 hours by selecting the period from the drop-down at the top right.

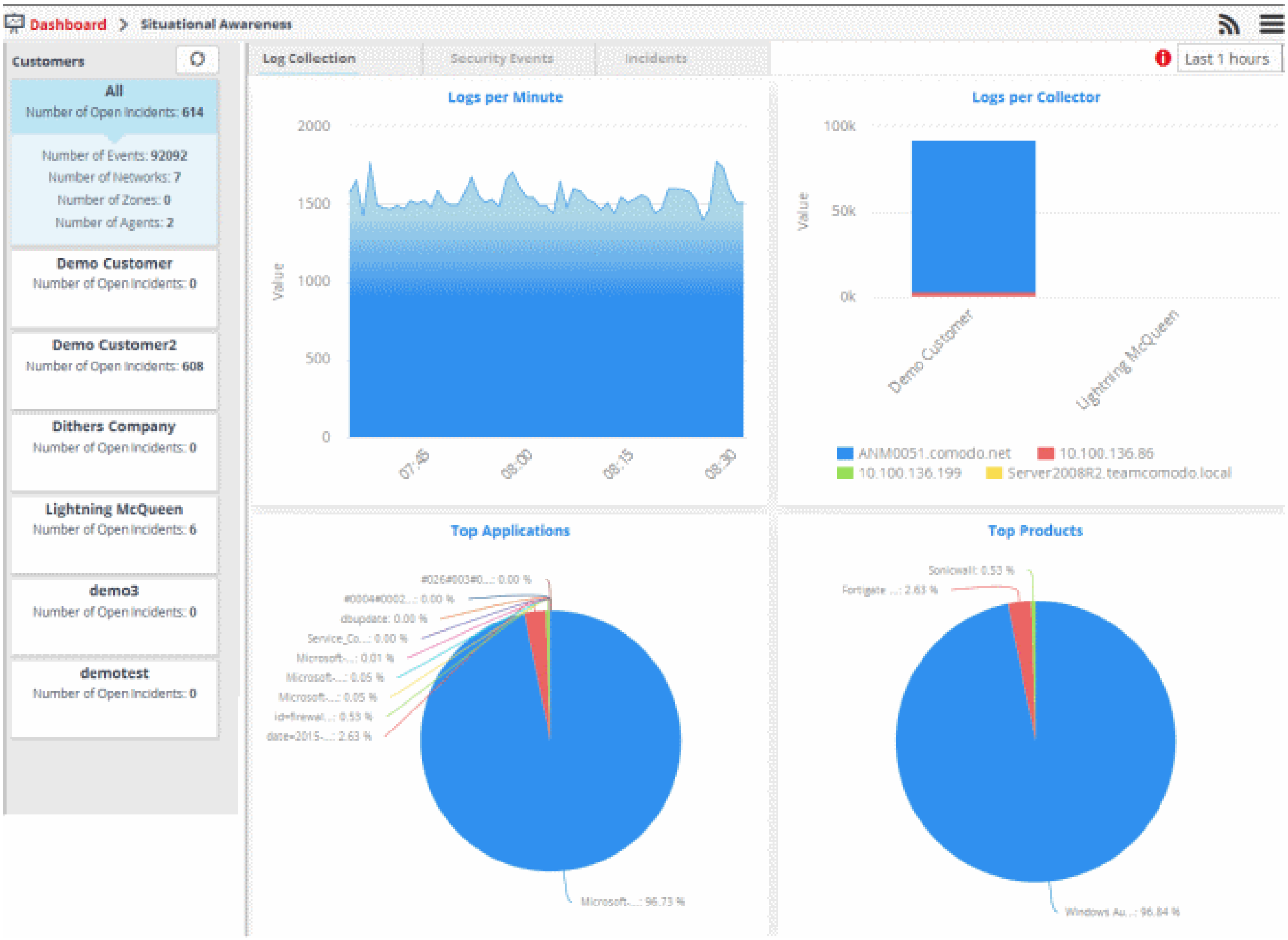
The 'Situational Awareness' dashboard contains three tabs, 'Log Collection', 'Security Events' and 'Incidents'.

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

The 'Situational Awareness' Dashboard is displayed by default whenever you log-in to NxSIEM. To switch to the Dashboard interface from any other interface, click the 'Menu' button, choose 'Dashboard' from the options and click 'Situational Awareness'.



By default, the statistics for all customers will be displayed.



All
Number of Open Incidents: 614

Number of Events: 92092
Number of Networks: 7
Number of Zones: 0
Number of Agents: 2

Demo Customer
Number of Open Incidents: 0

Demo Customer2
Number of Open Incidents: 608

Dithers Company
Number of Open Incidents: 0

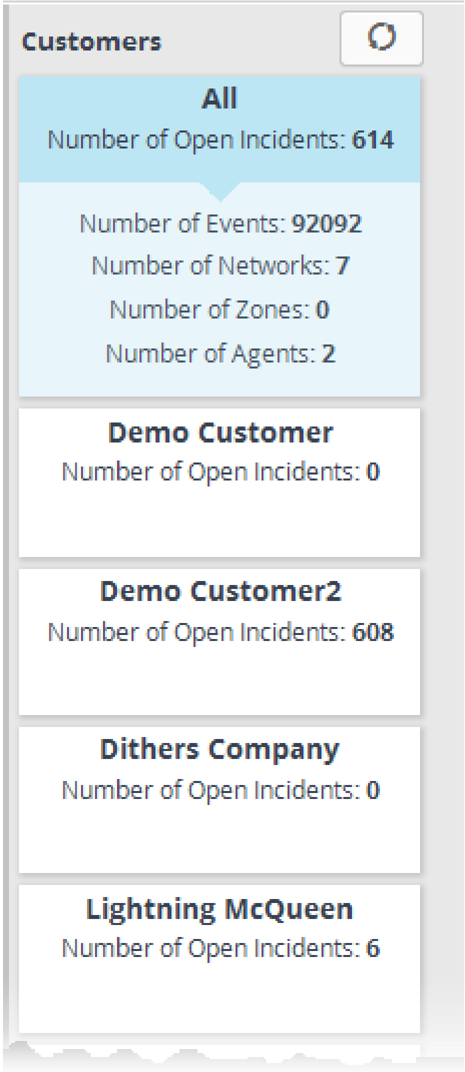
Lightning McQueen
Number of Open Incidents: 6

demo3
Number of Open Incidents: 0

demotest
Number of Open Incidents: 0

## Selecting Customer and Time Period

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



Customers

**All**
Number of Open Incidents: **614**

Number of Events: **92092**
Number of Networks: **7**
Number of Zones: **0**
Number of Agents: **2**

**Demo Customer**
Number of Open Incidents: **0**

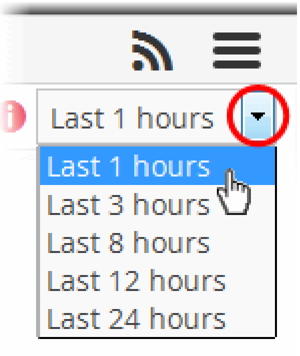
**Demo Customer2**
Number of Open Incidents: **608**

**Dithers Company**
Number of Open Incidents: **0**

**Lightning McQueen**
Number of Open Incidents: **6**

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

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



The dashboard will display the graphs for the selected customer with the details collected within the selected period.

**Tip**: In addition to the 'Situation Awareness' dashboard that displays the statistics of pre-defined parameters, the administrator can create custom dashboards specific to the customers, to display the results of event queries, as pie-charts, bar-charts and/or spider charts. The custom dashboards enable the administrator to view important details from often complex queries in an easily digested chart format and to effectively track, monitor and analyze the activities of their customers. Refer to the section '**Configuring Custom Dashboards**' for more details.

Following sections explain more on:

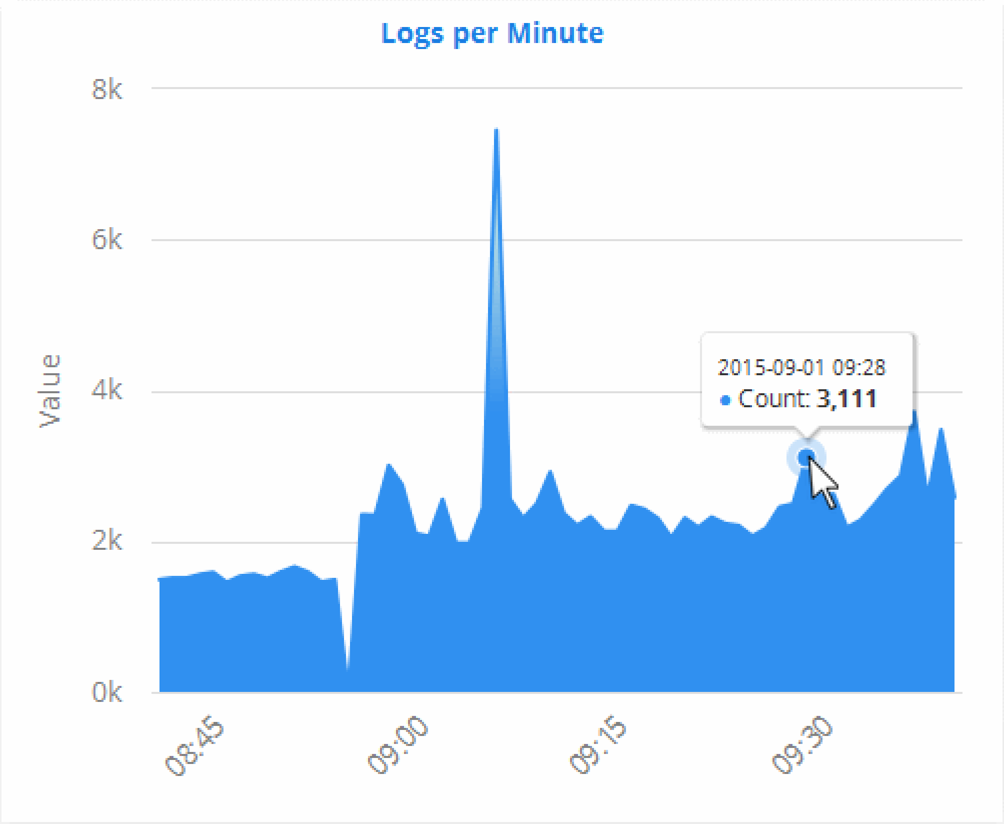
- **Log Collection Charts**
- **Security Events Charts**
- **Incidents Charts**

## Log Collection Charts

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

### Logs per Minute

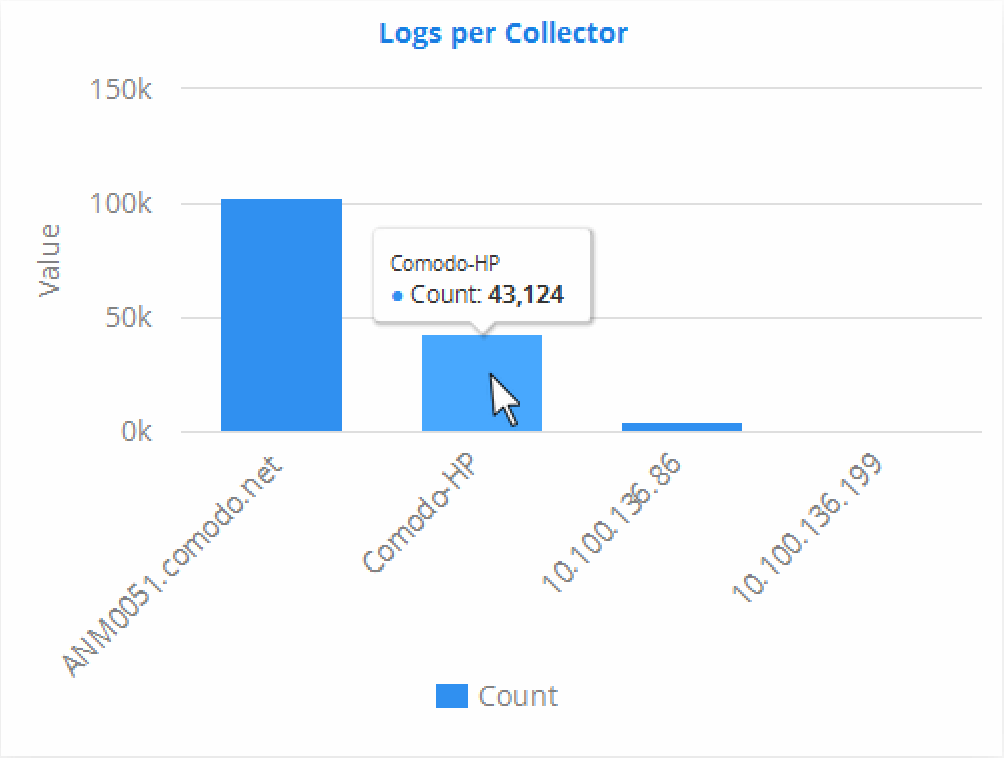
The chart shows the number of logs collected from various sources in selected customer network at different time points.



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

### Logs per Collector

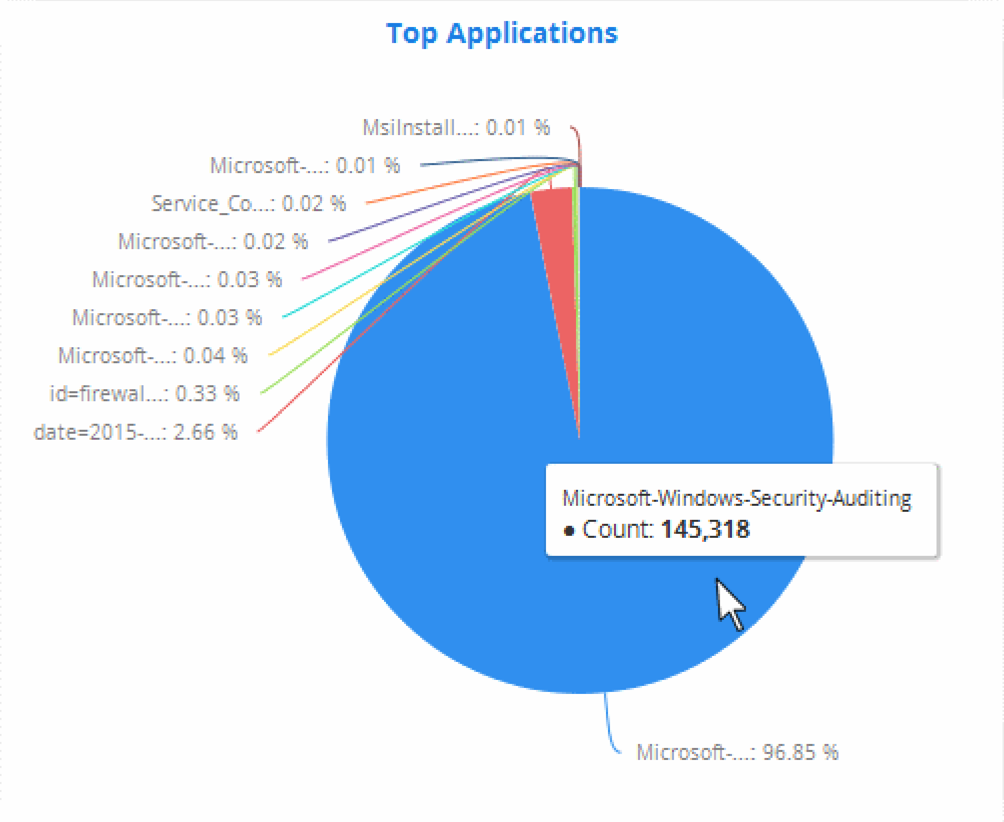
The 'Logs per Collector' chart shows the number of log entries collected from different agents/networks pertaining to the selected customer's networks.



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

**Top Applications**

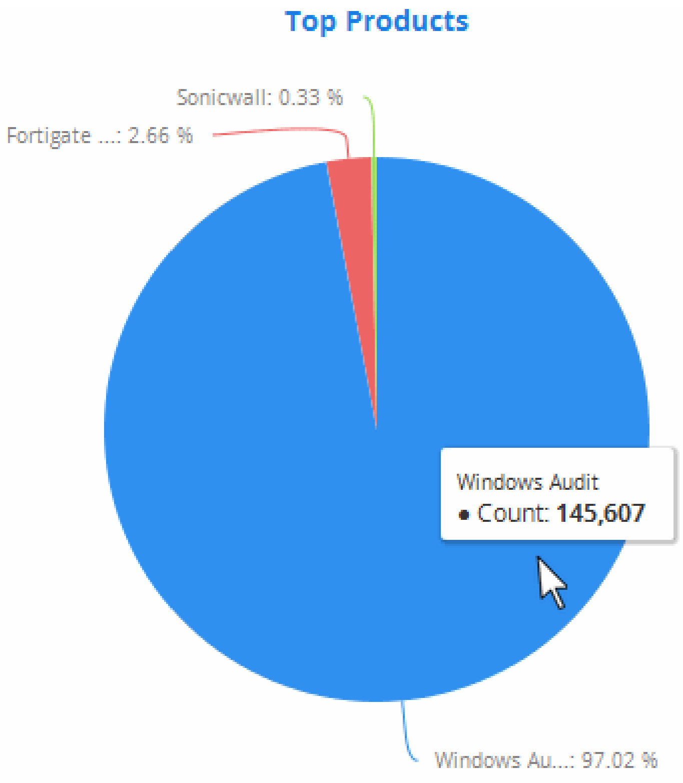
The 'Top Applications' pie-chart shows the percentage breakup of number of log entries received from events generated by various applications running in the customer's network.



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

**Top Products**

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



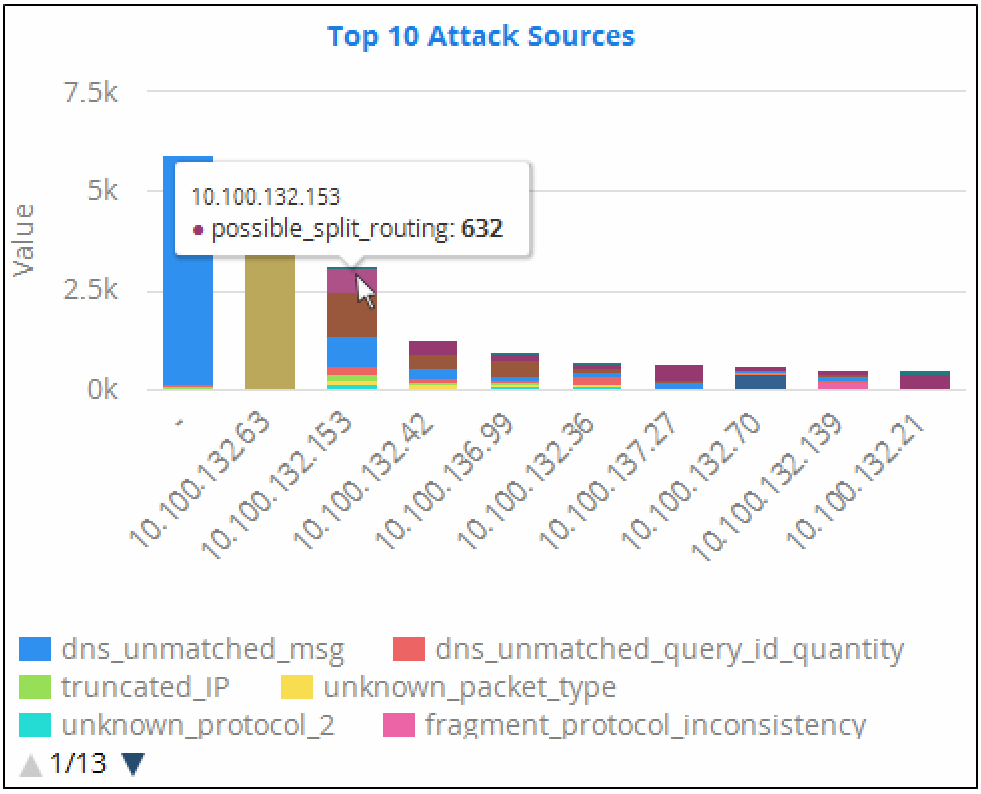
Placing the mouse cursor on a sector shows the exact number of the log entries collected from the respective product, as a tool tip.

## Security Events

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

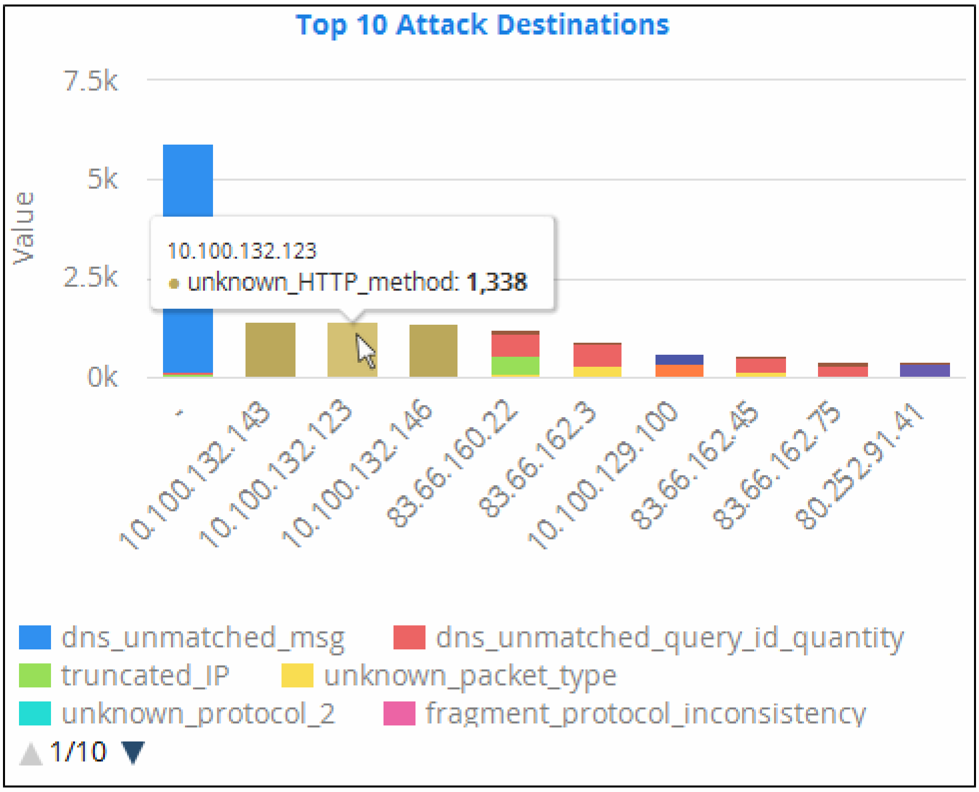
### Top 10 Attack Sources

The bar graph displays the top attack events, from where the events originated and the type of attack events. The IP addresses of the systems from where the attacks came are displayed on the X-axis. Placing the mouse cursor over an event will display its details such as the event name and the number of times the attack event is generated from the source. The value in the Y-axis displays the number of attack events. You can hide/view a graph bar by clicking on the respective event name at the bottom. View all the attack event names by using the triangle buttons below it.



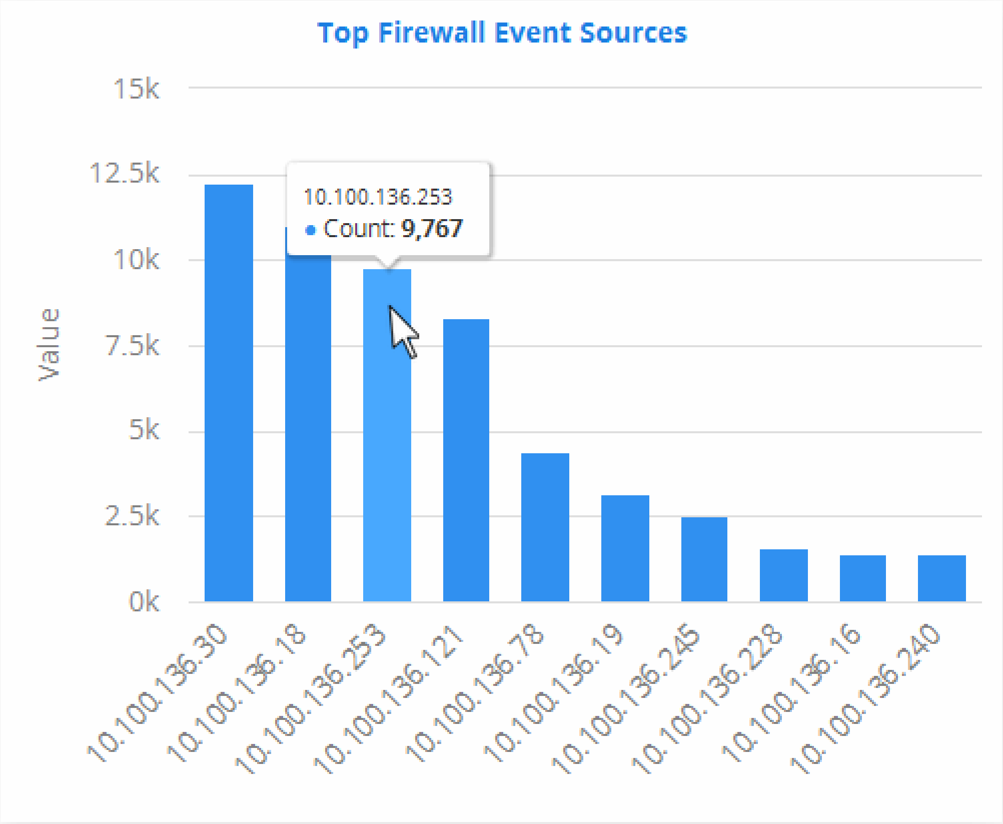
### Top Attack Destinations

The bar graph displays the top attack events, the type of attacks and the affected systems. The IP addresses of the systems that were attacked are displayed on the X-axis. Placing the mouse cursor over an event will display its details such as the event name and the number of times the system was attacked. The value in the Y-axis displays the number of attack events. At the bottom of the graph, the attack event names with color coding are displayed. You can hide/view a graph bar by clicking on the respective event name at the bottom. View all the attack event names by using the triangle buttons below it.



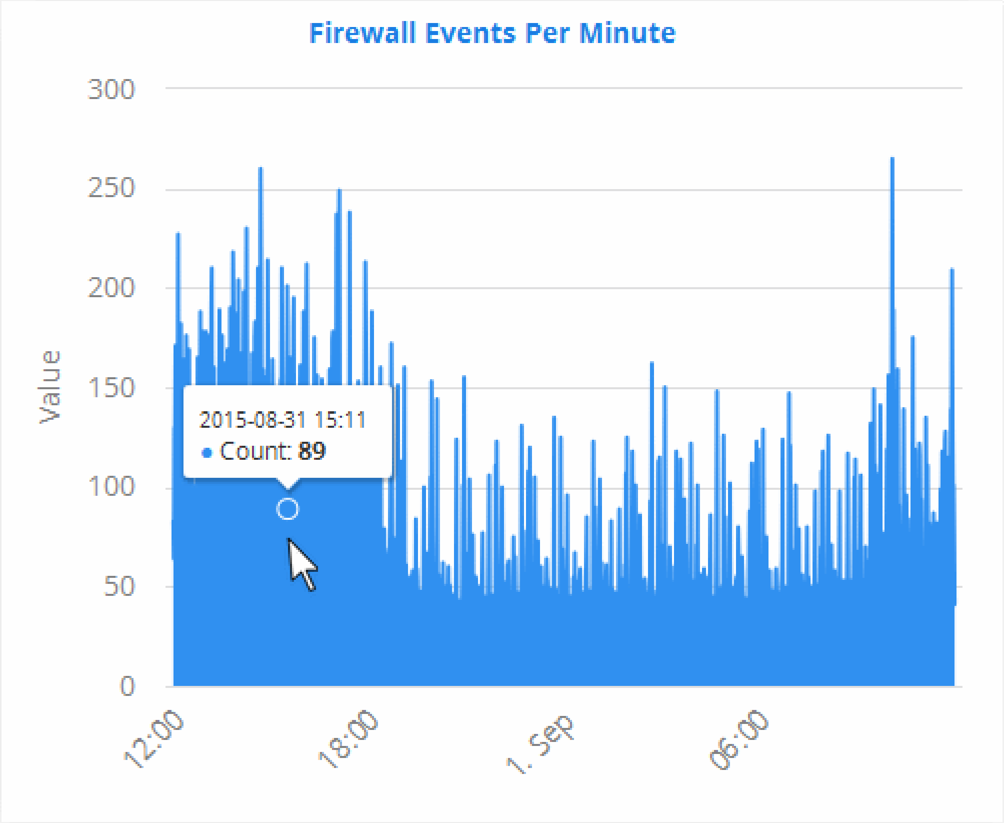
### Top Firewall Event Sources

The bar graph displays the occurrence details of top 10 firewall events, for example, a block event, that occurred on the endpoints. The IP addresses of the systems from where the firewall events originated are displayed on the X-axis and the number of times the events occurred is displayed on the Y-axis.  Placing the mouse cursor over an event source will display the number of times the event occurred on the system.



### Firewall Events Per Minute

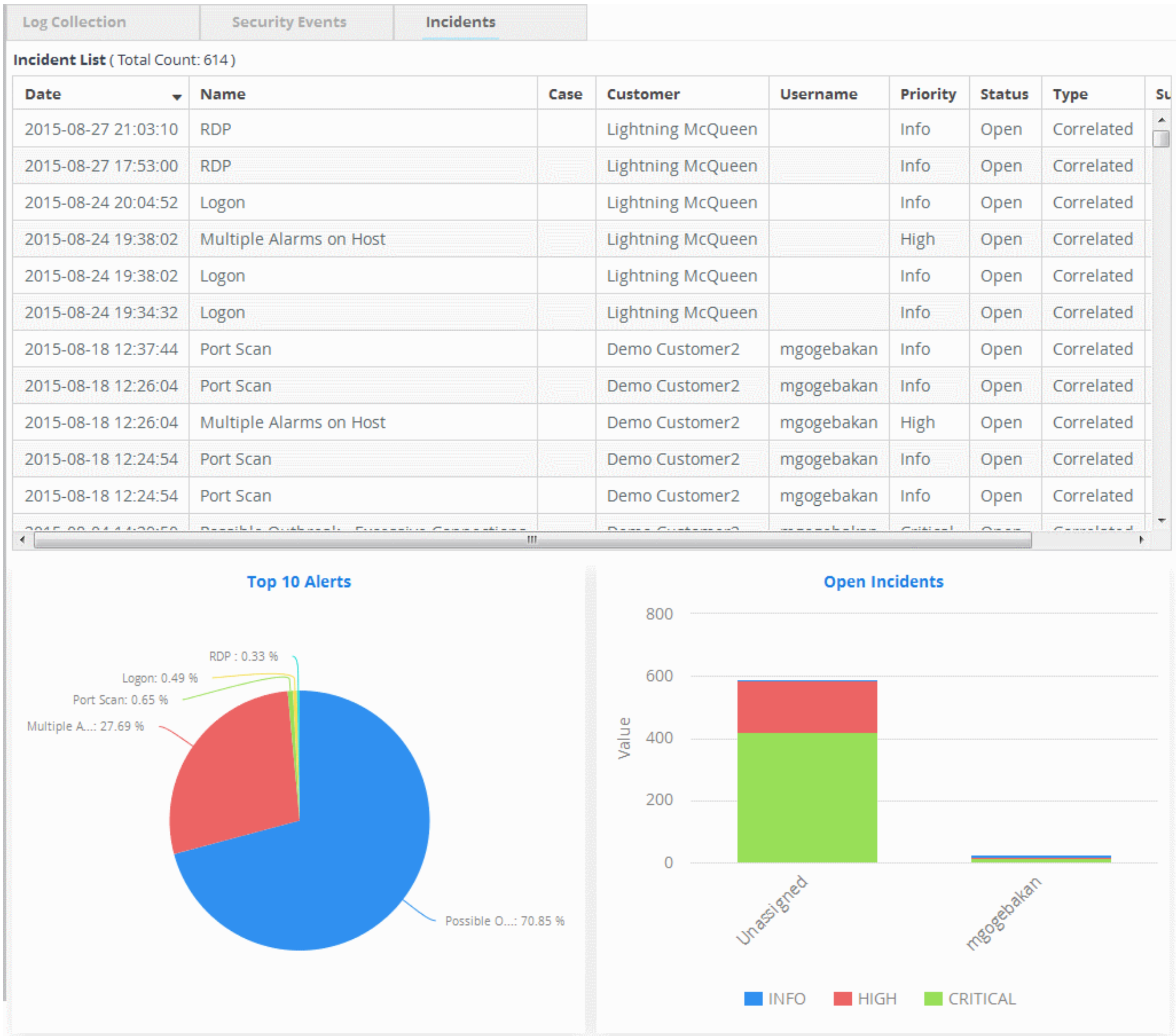
The bar graph provides occurrence details of firewall events on a per minute basis for better analysis. For example, administrators can get the time when the greatest number of firewall events occurs for a customer or if no events are coming from a customer, it may indicate malfunctioning communications with the agent or issue with log forwarding. Placing the mouse cursor over the graph will display the day, date, time and the number of times the event occurred.



## Incidents

Comodo NxSIEM generates alerts based on rules that are defined in Rule Creation & Activation  interface and these alerts are automatically assigned as incidents to administrative users enrolled for the respective customers to take necessary actions. Refer to the section '**Administration**' to know about assigning users to customers. When the alerts are assigned to users, they are called 'Incidents' and incidents that are not closed are called 'Open Incidents'. Alerts that are not assigned are called 'Unassigned Incidents'. You can also add incidents manually in the '**Incidents**' screen and assign them to users. These are classified as 'Default' and incidents that are detected automatically via alerts are called 'Correlated'. Refer to the section '**Managing Incidents**' to know how to add incidents manually, view assigned alerts, edit and close the incidents.

- Click the 'Incidents' tab after selecting a customer from the left side.

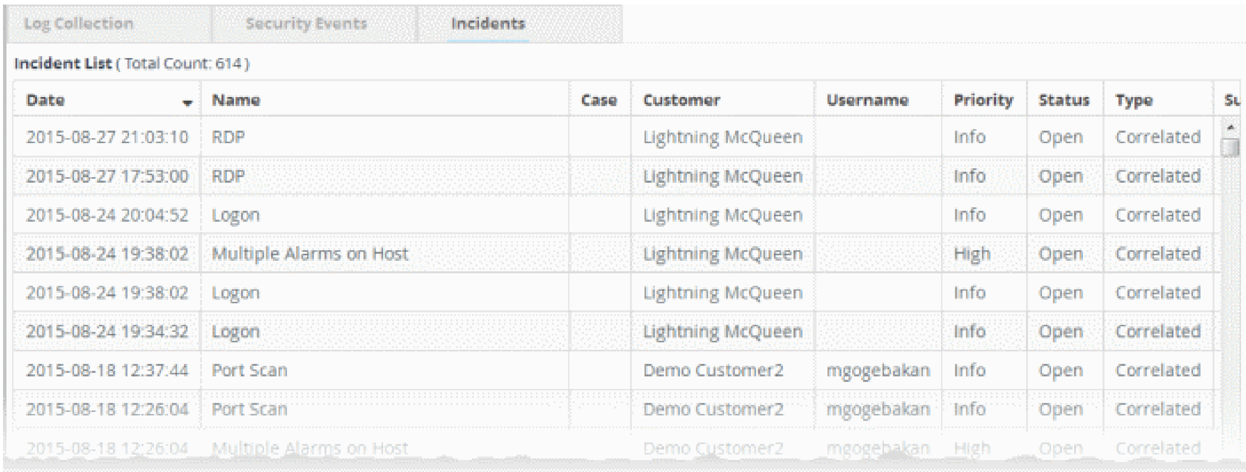


**Incident List** ( Total Count: 614 )

| Date | Name | Case | Customer | Username | Priority | Status | Type | Su |
|---|---|---|---|---|---|---|---|---|
| 2015-08-27 21:03:10 | RDP | | Lightning McQueen | | Info | Open | Correlated | |
| 2015-08-27 17:53:00 | RDP | | Lightning McQueen | | Info | Open | Correlated | |
| 2015-08-24 20:04:52 | Logon | | Lightning McQueen | | Info | Open | Correlated | |
| 2015-08-24 19:38:02 | Multiple Alarms on Host | | Lightning McQueen | | High | Open | Correlated | |
| 2015-08-24 19:38:02 | Logon | | Lightning McQueen | | Info | Open | Correlated | |
| 2015-08-24 19:34:32 | Logon | | Lightning McQueen | | Info | Open | Correlated | |
| 2015-08-18 12:37:44 | Port Scan | | Demo Customer2 | mgogebakan | Info | Open | Correlated | |
| 2015-08-18 12:26:04 | Port Scan | | Demo Customer2 | mgogebakan | Info | Open | Correlated | |
| 2015-08-18 12:26:04 | Multiple Alarms on Host | | Demo Customer2 | mgogebakan | High | Open | Correlated | |
| 2015-08-18 12:24:54 | Port Scan | | Demo Customer2 | mgogebakan | Info | Open | Correlated | |
| 2015-08-18 12:24:54 | Port Scan | | Demo Customer2 | mgogebakan | Info | Open | Correlated | |
| 2015-08-04 14:20:50 | Possible Outbreak - Excessive Connections | | Demo Customer2 | mgogebakan | Critical | Open | Correlated | |

## Incident List

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


Log Collection
Security Events
Incidents

**Incident List** ( Total Count: 614 )

| Date | Name | Case | Customer | Username | Priority | Status | Type | Su |
|---|---|---|---|---|---|---|---|---|
| 2015-08-27 21:03:10 | RDP | | Lightning McQueen | | Info | Open | Correlated | |
| 2015-08-27 17:53:00 | RDP | | Lightning McQueen | | Info | Open | Correlated | |
| 2015-08-24 20:04:52 | Logon | | Lightning McQueen | | Info | Open | Correlated | |
| 2015-08-24 19:38:02 | Multiple Alarms on Host | | Lightning McQueen | | High | Open | Correlated | |
| 2015-08-24 19:38:02 | Logon | | Lightning McQueen | | Info | Open | Correlated | |
| 2015-08-24 19:34:32 | Logon | | Lightning McQueen | | Info | Open | Correlated | |
| 2015-08-18 12:37:44 | Port Scan | | Demo Customer2 | mgogebakan | Info | Open | Correlated | |
| 2015-08-18 12:26:04 | Port Scan | | Demo Customer2 | mgogebakan | Info | Open | Correlated | |
| 2015-08-18 12:26:04 | Multiple Alarms on Host | | Demo Customer2 | mgogebakan | High | Open | Correlated | |

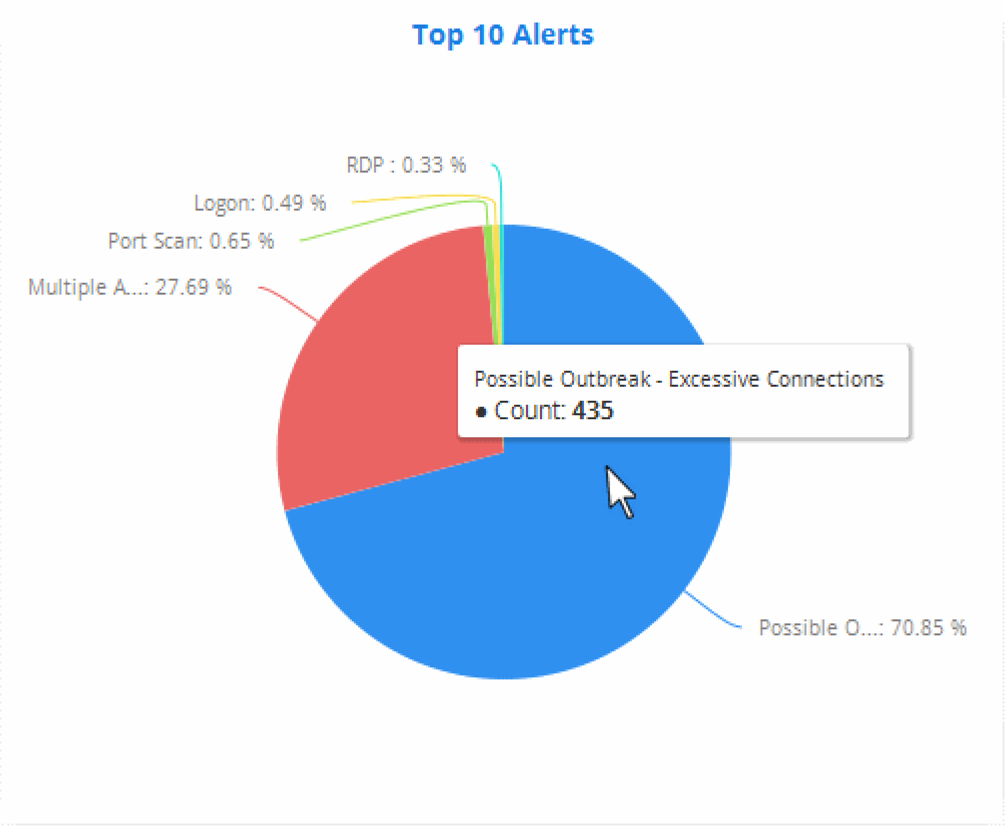
| Incident List - Table of Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Date | Indicates the precise date and time of the incident. |

| | |
|---|---|
| Name | Displays the name of rule  based on which the incident was detected or added. |
| Case | Displays the case to which the incident is integrated and assigned to the administrative user.. |
| Customer | The name of the customer |
| Username | Displays the username of the administrator to whom the incident is assigned. |
| Priority | Displays the option chosen in the 'Severity' drop-down of 'Rule Creation' screen and in the 'Priority' drop-down of 'Add Incident' screen. |
| Status | Displays whether the status of the incident is 'Open, In-Progress, False Positive or Closed' |
| Type | Indicates whether the incident is assigned automatically via alerts or added manually. Incidents assigned automatically are 'Correlated' type and those that are added manually are called 'Default' |
| Summary | Displays the a short description of the incident based on the description provided for the rule. |

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

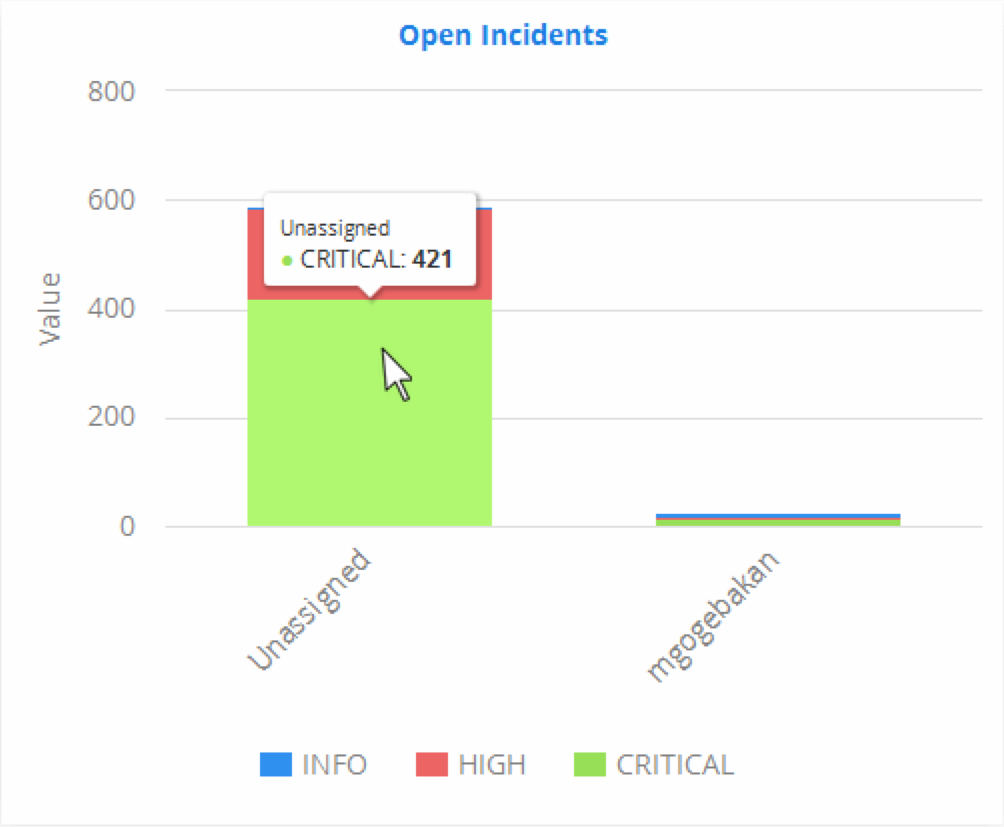
**Top 10 Alerts**

The pie chart displays the percentage breakup of rules based on which  top 10 number of alerts were generated. Placing the mouse cursor over a sector displays the description of the rule and number of alerts generated for that rule.



**Open Incidents**

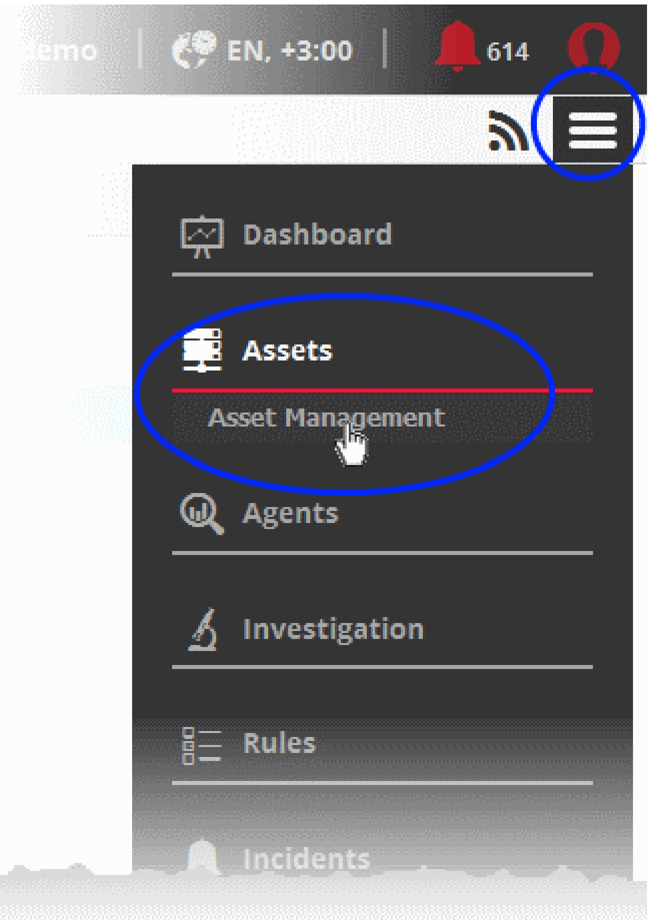
The bar graph displays the numbers of incidents assigned  to different administrative users and unassigned incidents. The X-axis displays the user details to whom the incidents are assigned and the Y-axis displays the number of incidents. Placing the mouse cursor over a graph bar will display the number of incidents, the severity of the incident and to which the user they are assigned.



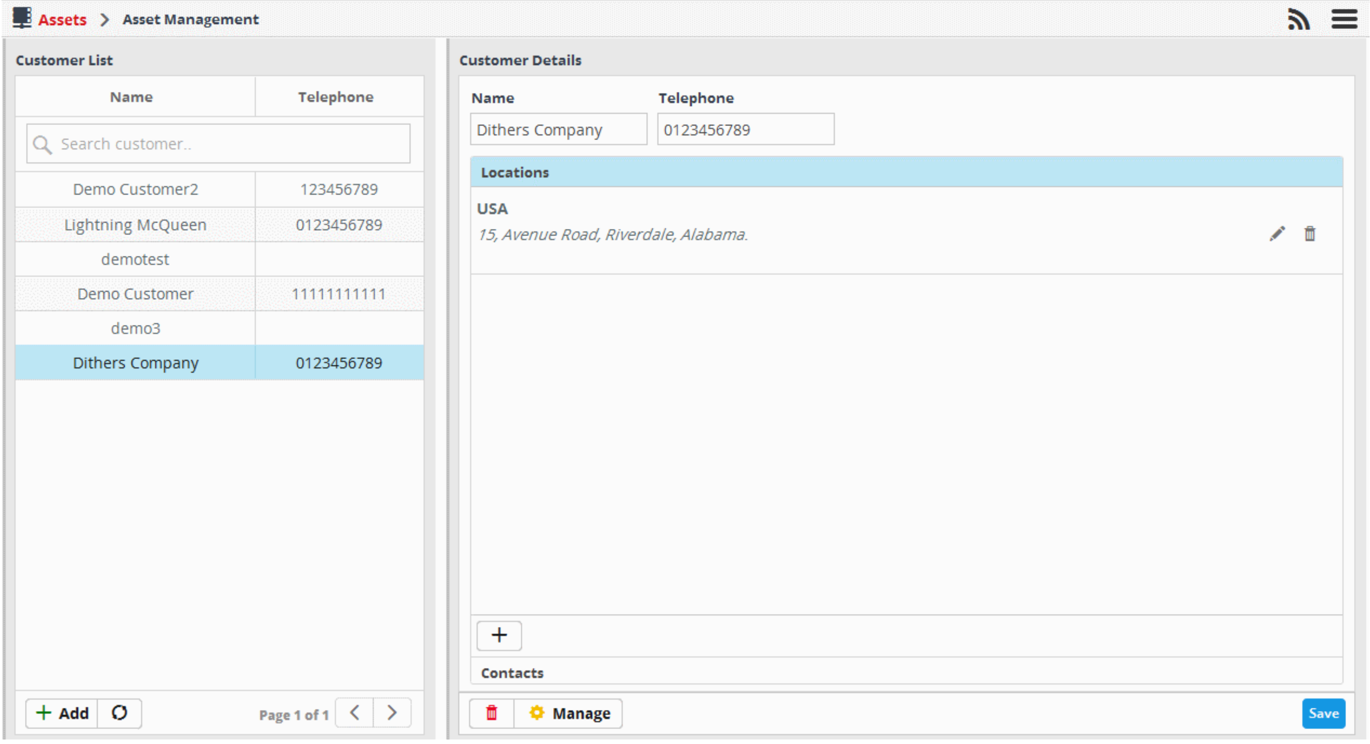
# 4 Customer Asset Management

The administrator can add and manage customers whose networks and endpoints are to be monitored and managed, though the 'Asset management' interface.

To open the 'Asset Management' interface, click the 'Menu' button at the top right, choose 'Assets' and click 'Asset Management'.



The 'Asset Management' interface displays the list of the customers on the left hand side pane and the details of the selected customer on the right hand side pane.



Customer List

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

Customer Details

Name: Dithers Company
Telephone: 0123456789

Locations

USA
*15, Avenue Road, Riverdale, Alabama.*

The following sections explain on managing customers and their assets and configuring for customer networks for sending logs to NxSIEM server.

- Adding new customers
- Adding Customer's Assets for Monitoring

- **Downloading and Installing NxSIEM Agent on customers' endpoints for log collection**
- **Downloading and Installing Nxlog and Rsyslog configuration files for fetching logs from Nxlog and Rsyslog servers in customers' networks**
- **Editing Customers**

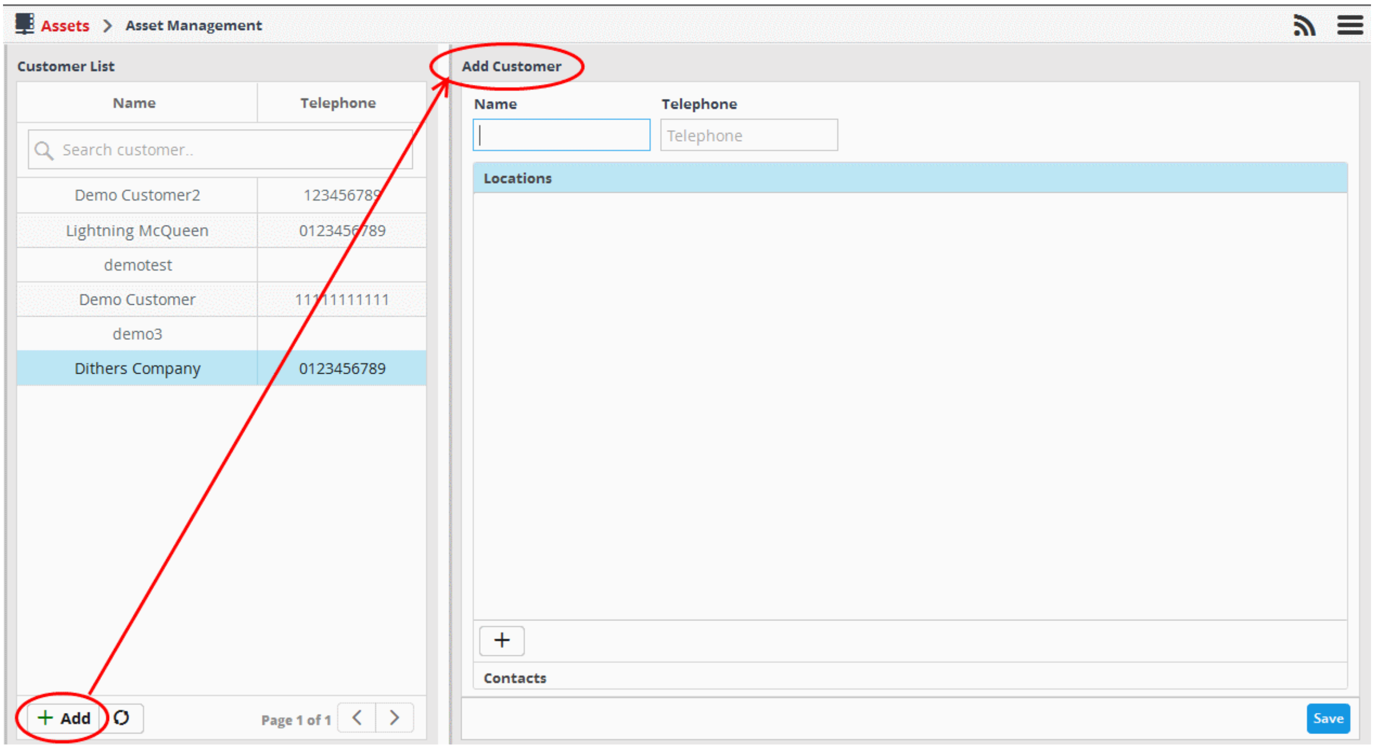
## 4.1 Adding Customers

In order to monitor the endpoints in customer networks and collect logs from them, the customer needs to be added to NxSIEM with the details of their networks and other assets. Once a customer is added, a 'Network Activation Key' will be automatically generated. The key should be used to activate the agents installed on the customer's endpoints. Refer to the section '**Downloading and Installing the NxSIEM Agent**' for more details.

**To add a new customer**

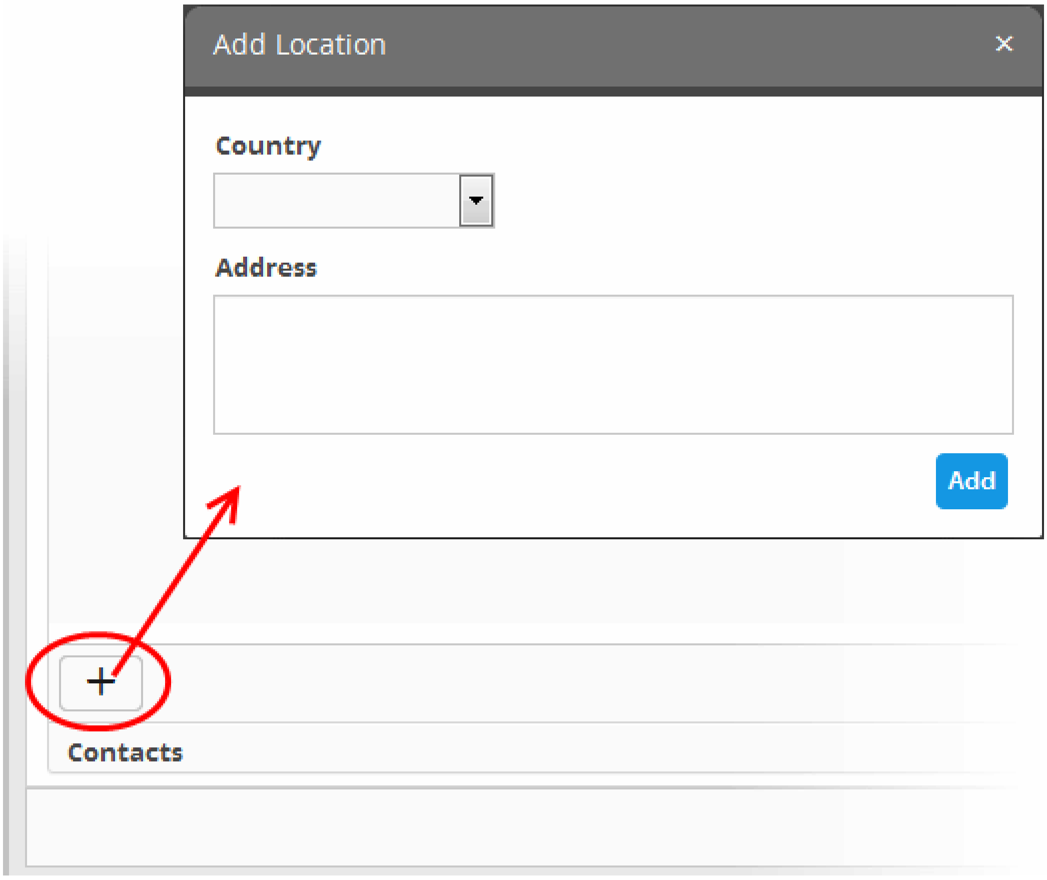
- Open the 'Asset Management' interface by clicking the 'Menu' button, then 'Assets' > 'Asset Management'.
- Click the 'Add' button at the bottom of the 'Customer List' pane on the left.

The 'Add Customer' screen will be displayed on the right hand side pane.



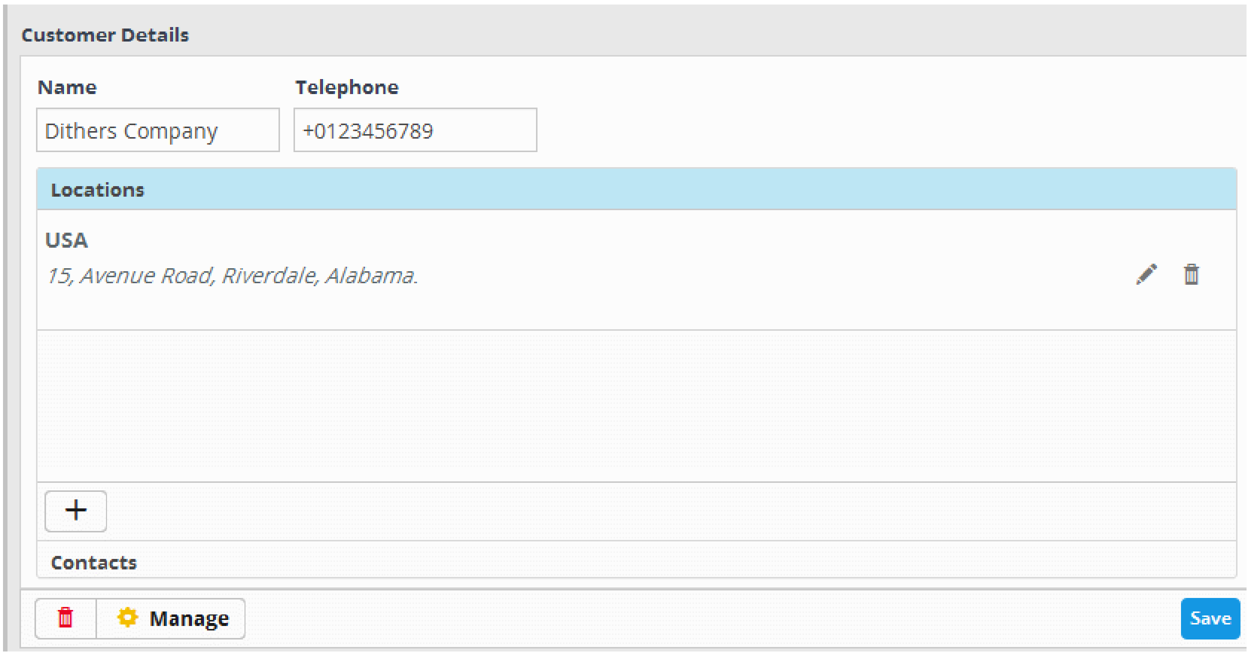
| Name | Telephone |
|---|---|
| Demo Customer2 | 123456789 |
| Lightning McQueen | 0123456789 |
| demotest | |
| Demo Customer | 11111111111 |
| demo3 | |
| Dithers Company | 0123456789 |

- Enter the name of customer in the 'Name' field.
- Enter their contact number in the 'Telephone' field.
- To add the location of the customer, click the 'Location' stripe and click the + button at the bottom.



- Select the country in which the company is located, from the 'Country' drop-down
- Enter the address of the company in the 'Address' field.
- Click the 'Add' button.

The location will be added and displayed in the screen.

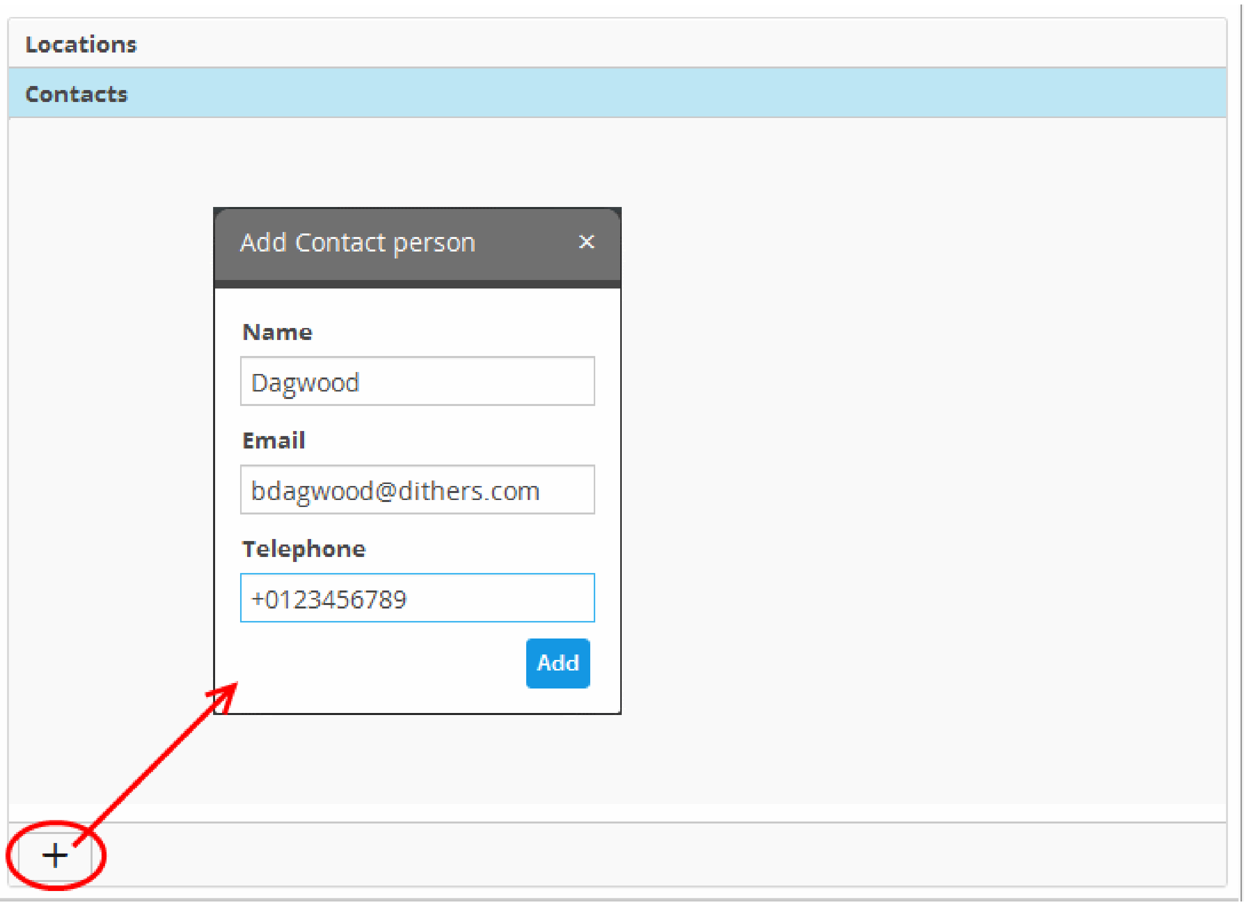


| Name | Telephone |
|---|---|
| Dithers Company | +0123456789 |

USA
*15, Avenue Road, Riverdale, Alabama.*

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

- To add the contact details of the customer, click the 'Contacts' stripe and click the + button at the bottom..



Locations

Contacts

Add Contact person ×

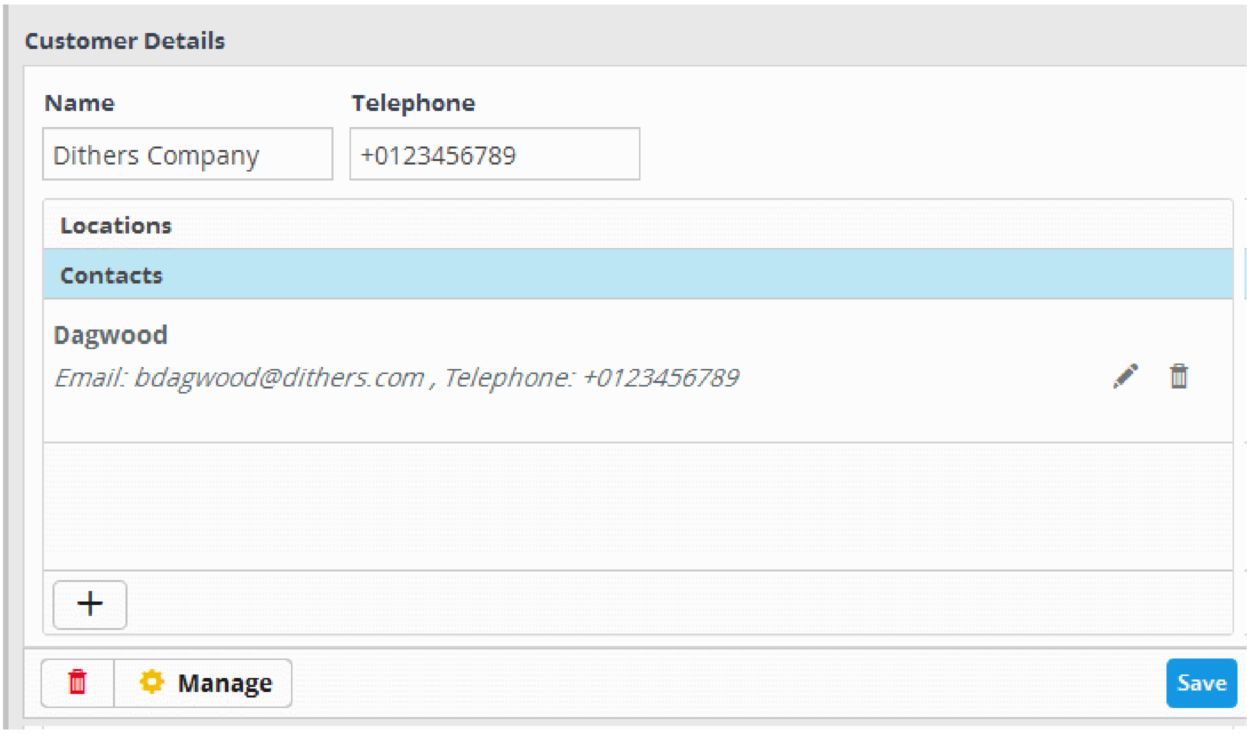
Name: Dagwood

Email: bdagwood@dithers.com

Telephone: +0123456789

- Enter the Name, Email address and Phone number of the contact person in the 'Add Contact person' dialog and click 'Add'.

The contact will be added.



Customer Details

Name: Dithers Company

Telephone: +0123456789

Locations

Contacts

Dagwood

*Email: bdagwood@dithers.com , Telephone: +0123456789*

- Repeat the process to add more contact persons.
- Click the 'Save' button.

The customer will be added. The next step is to add assets and import endpoints to NxSIEM for monitoring. Refer to the sections '**Adding Assets for Monitoring**' and '**Downloading and Installing the NxSIEM Agent on Endpoints**' for more details.

## 4.2 Adding Assets for Monitoring

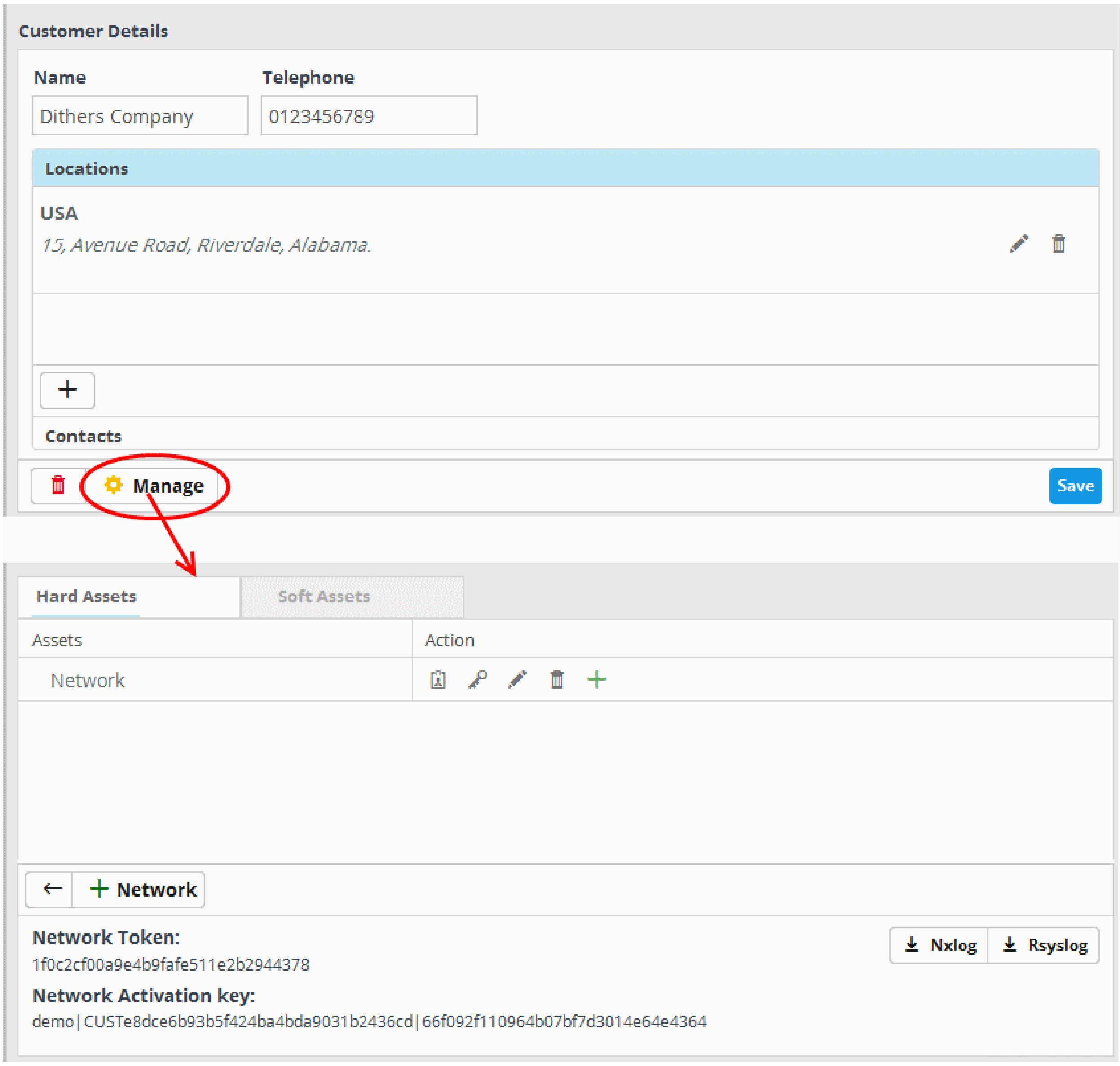
In order to collect logs and monitor events on customer networks, administrators need to add the customer's network assets to NxSIEM. Administrators should enroll the endpoints and software assets (such as services) that they wish to monitor.

**To add assets for a customer**

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

The Customer Details pane will open in the right.

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



Customer Details

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

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

## 4.2.1 Hard Assets

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

For each network or the zone defined for a customer:

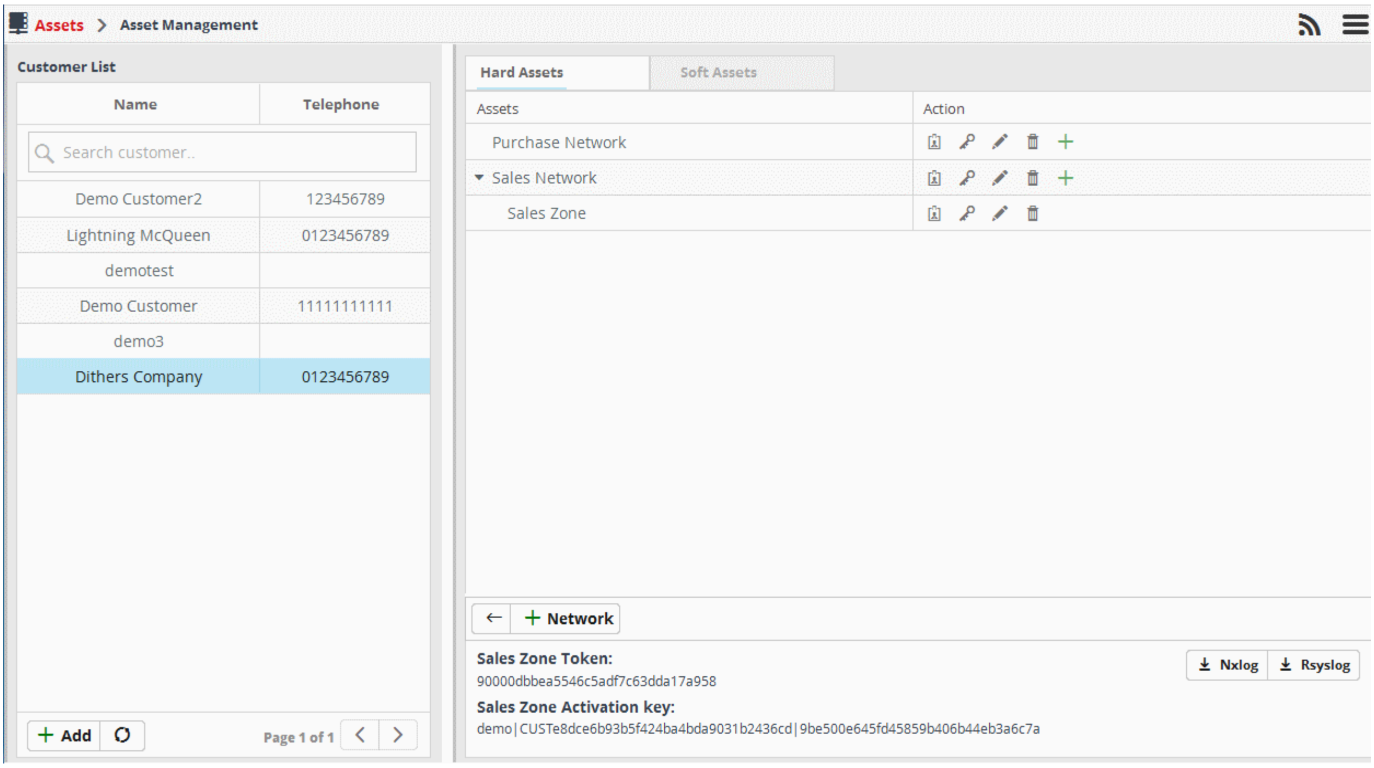
- A unique activation key is generated. The activation key is used to activate the log collection agent installed on Windows and Linux endpoints in the network/zone, for connection to the NxSIEM server and to send logs from them. Refer to the section **Downloading and Installing NxSIEM Agent on Endpoints** for more details.
- A unique authentication token is generated. The authentication token can be used as '*AGENTLESS_AUTH_TOKEN*' parameter on the configuration script that can be run on Linux endpoints with RSYSLOG utility, for agent less log collection from them. Refer to the section **Agentless Log Collection** for more details.
- Configuration files for RSYSLOG and NXLOG utilities are generated. The configuration files can be directly run on endpoints with RSYSLOG and NXLOG utilities respectively without any re-configuration, for them to send logs to NXSIEM server. Refer to the section **Configuring Nxlog and Rsyslog servers to send logs to NxSIEM server** for more details.

**To open the Hard Assets interface for a customer**

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

The Customer Details pane will open in the right.

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



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

| Assets | Action |
|---|---|
| Purchase Network | |
| Sales Network | |
| Sales Zone | |

**Sales Zone Token:**
90000dbbea5546c5adf7c63dda17a958

**Sales Zone Activation key:**
demo|CUSTe8dce6b93b5f424ba4bda9031b2436cd|9be500e645fd45859b406b44eb3a6c7a

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

| Hard Assets: Action - Controls | |
|---|---|
| 📋 | Clicking this icon displays the authentication token, agent activation key 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 NxSIEM server will not be able to collect logs |

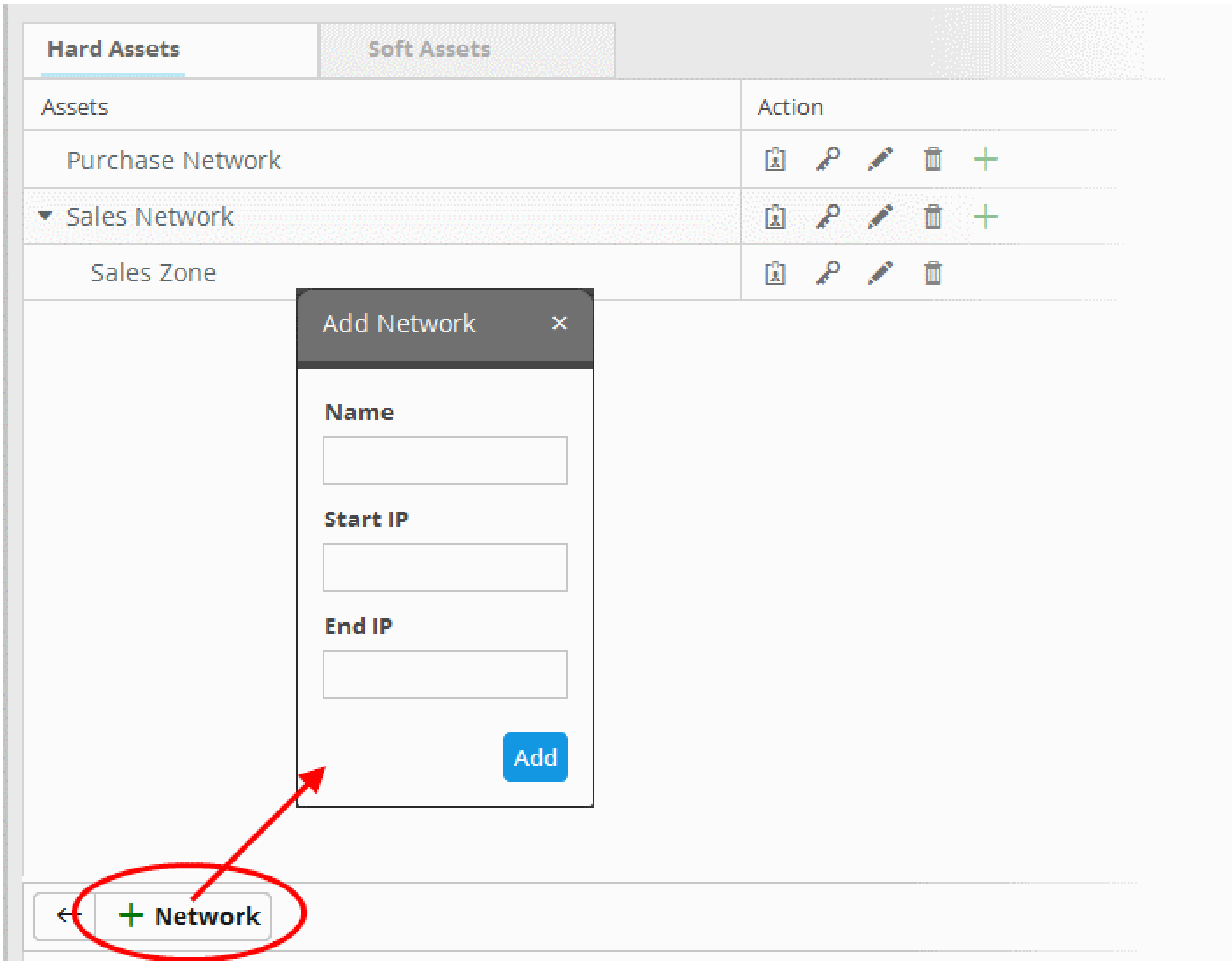
| | |
|---|---|
| | from RSYSLOG utility at endpoints with configuration script file containing the old token. |
| ✎ | Allows you to edit the name and IP address range of the network or the zone. |
| 🗑 | Allows you to delete the network or zone. Deleting a network also deletes the zones configured under it. |
| + | Allows you to add a zone to the network. |

The Hard Assets interface allows you to:

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

**To add hard assets for a customer**

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



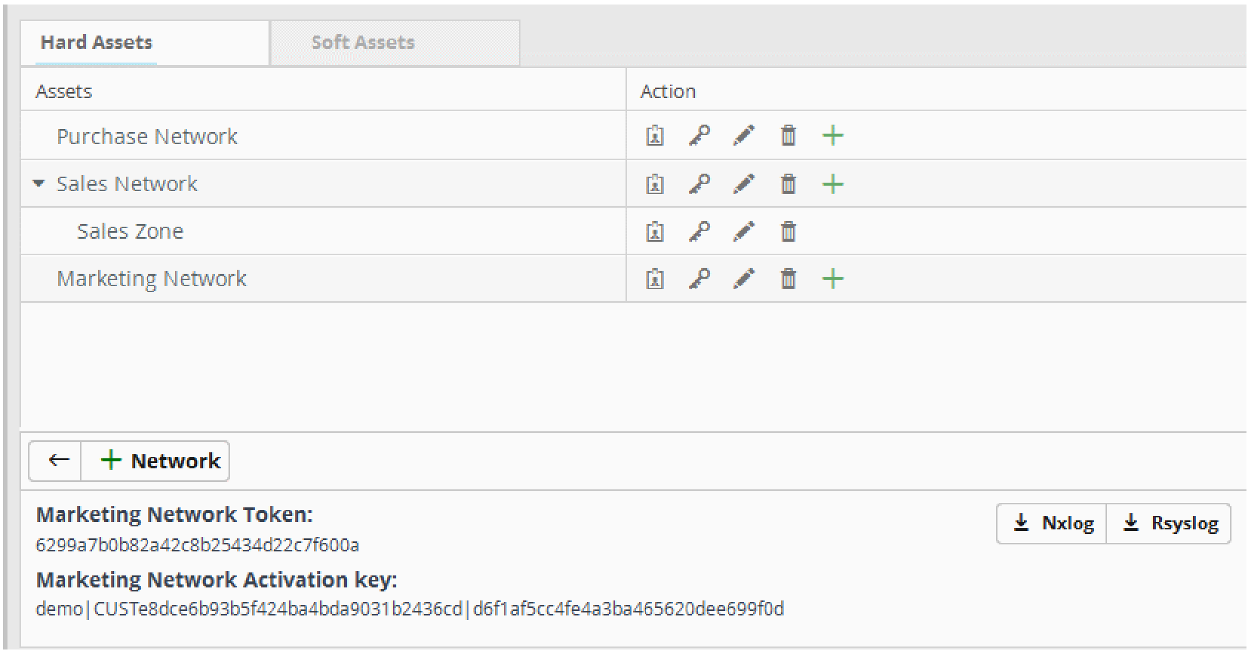
The 'Add Network' dialog will appear.

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

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

- Click the 'Add' button.

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



| Assets | Action |
|---|---|
| Purchase Network | |
| Sales Network | |
| Sales Zone | |
| Marketing Network | |

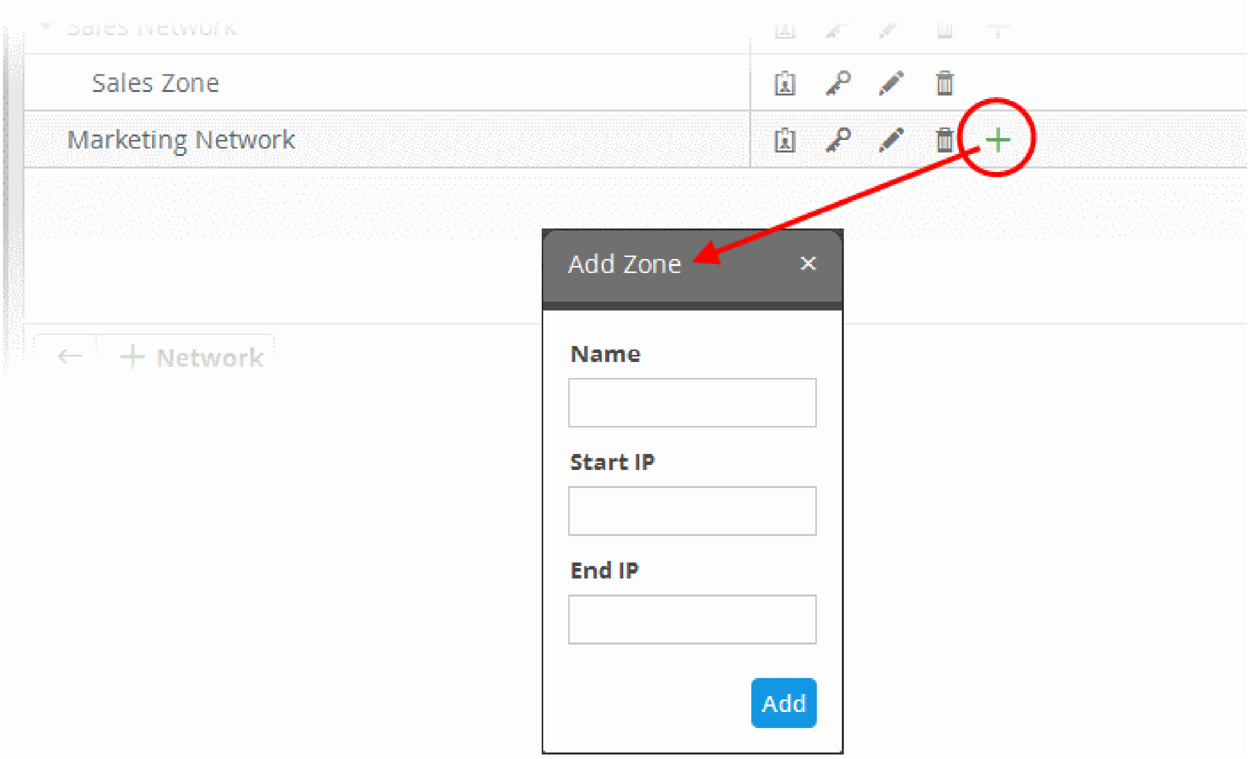
**Marketing Network Token:**
6299a7b0b82a42c8b25434d22c7f600a

**Marketing Network Activation key:**
demo|CUSTe8dce6b93b5f424ba4bda9031b2436cd|d6f1af5cc4fe4a3ba465620dee699f0d

- Repeat the process to add more networks.

**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.

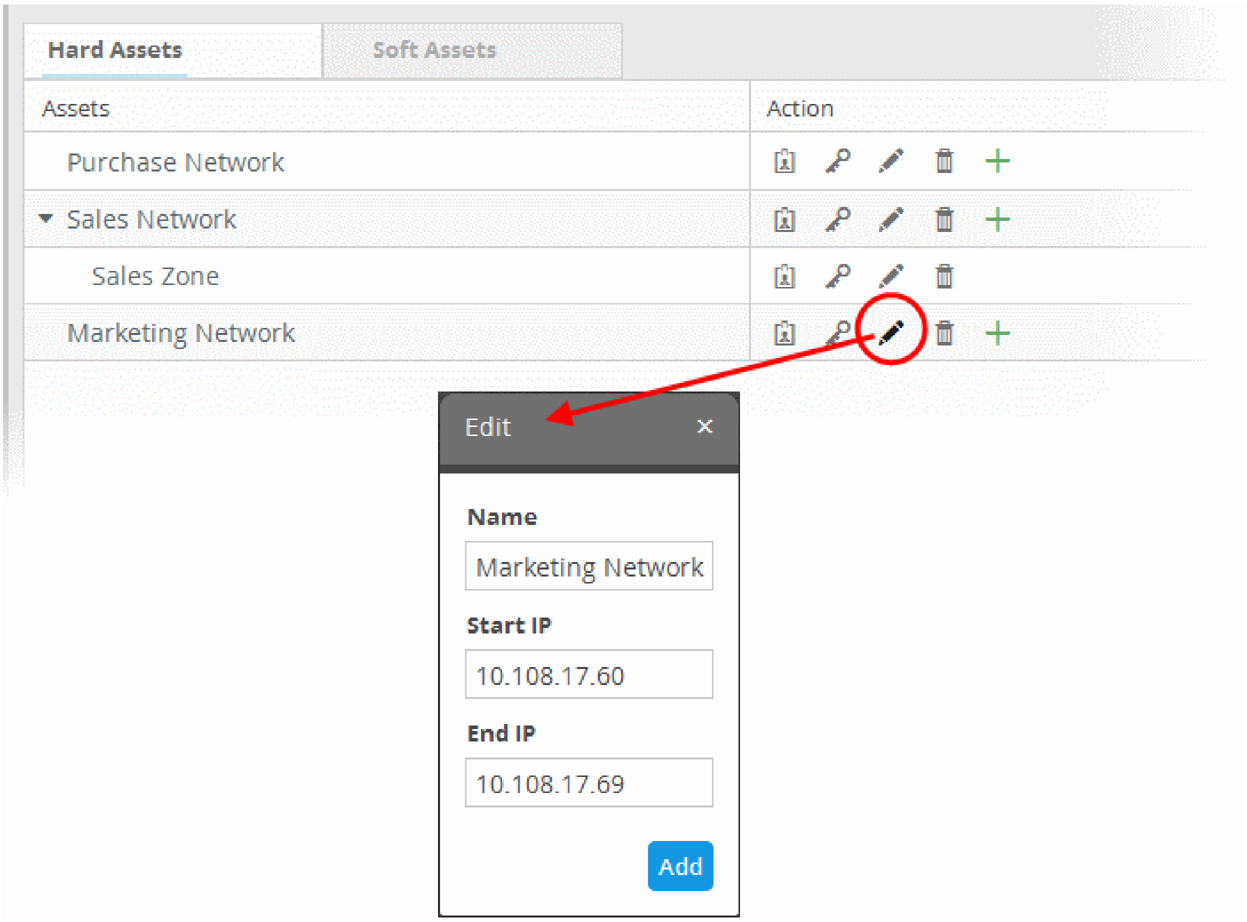
  - **End IP -** Enter the end IP address if a range of endpoints are to be added for the zone. If a single endpoint is to be added, enter its IP address in both the 'Start IP' and 'End IP' fields.
- Click the 'Add' button.

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

**To edit a network or a zone**

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

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



Name: Marketing Network

Start IP: 10.108.17.60

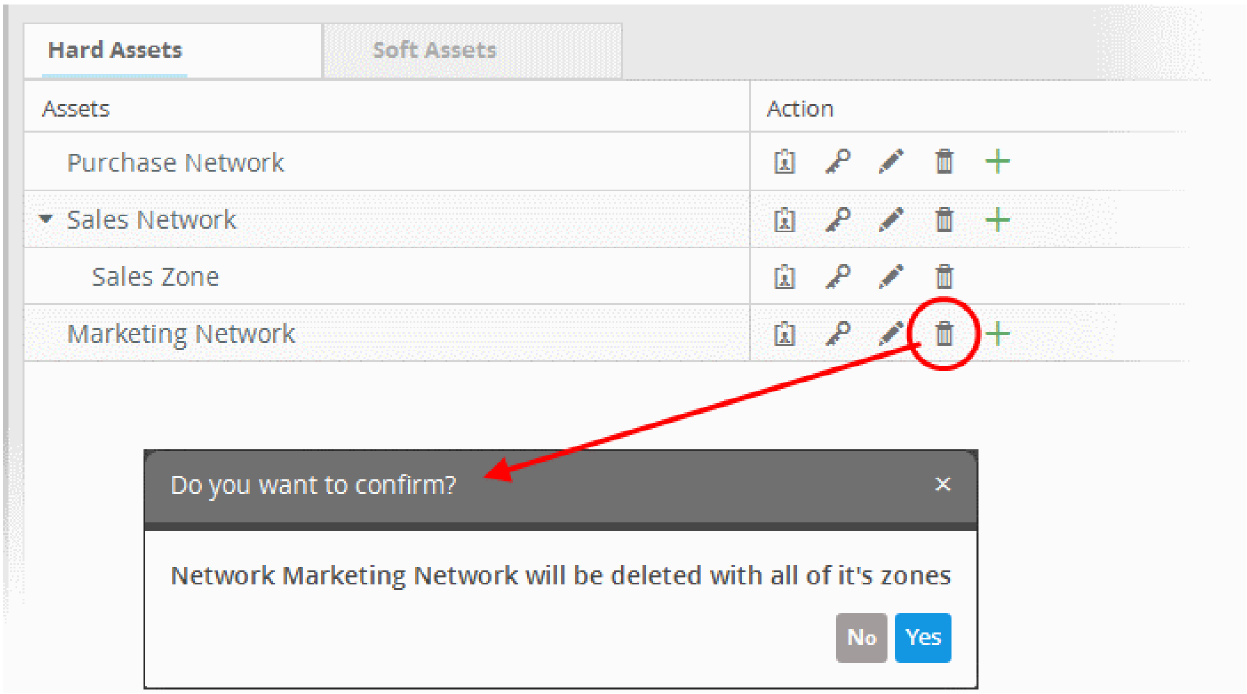
End IP: 10.108.17.69

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

**To delete a network or zone**

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

A confirmation dialog will appear.



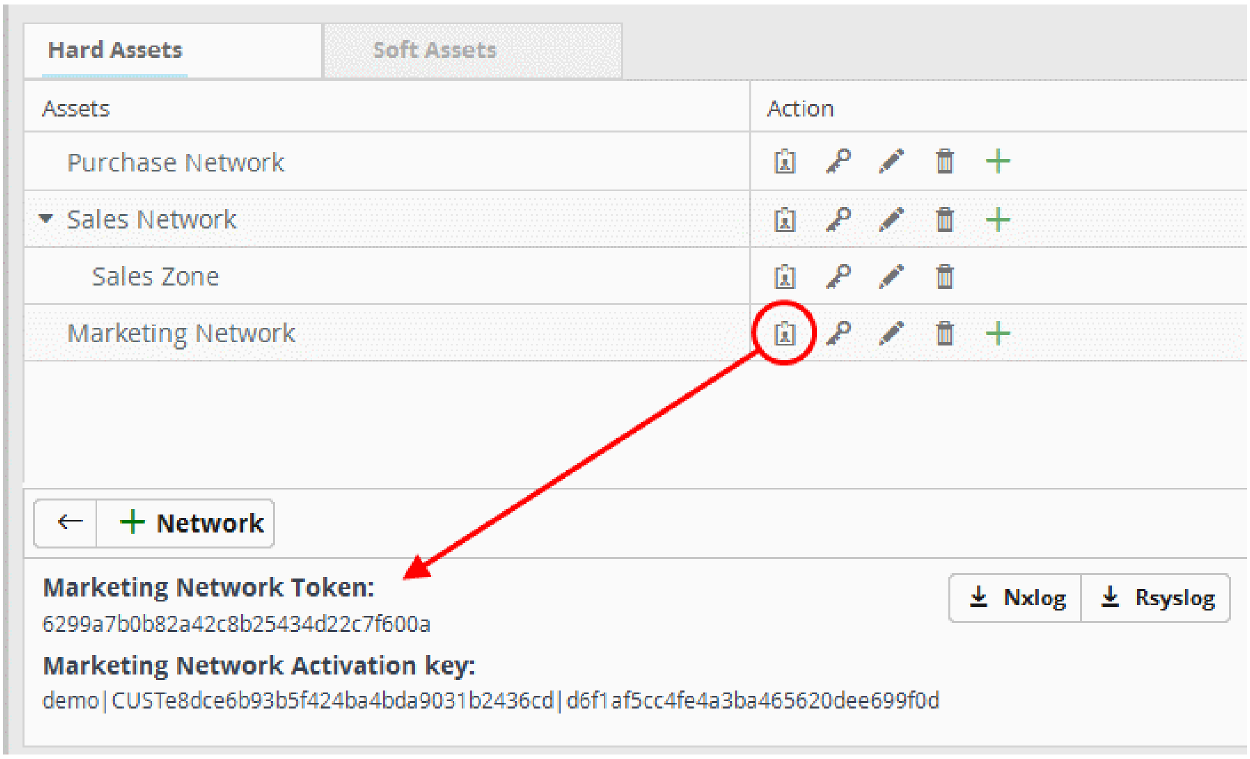
Network Marketing Network will be deleted with all of it's zones

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

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

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

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



**Marketing Network Token:**
6299a7b0b82a42c8b25434d22c7f600a

**Marketing Network Activation key:**
demo|CUSTe8dce6b93b5f424ba4bda9031b2436cd|d6f1af5cc4fe4a3ba465620dee699f0d

- **Authentication token -** The authentication token can be used as 'AGENTLESS_AUTH_TOKEN' parameter on the configuration script that can be run on Linux endpoints with RSYSLOG utility, for agent less log collection from them. Refer to the section **Agentless Log Collection** for more details.
- **Activation key -** The activation key is used to activate the log collection agent installed on Windows and Linux endpoints in the network/zone, for connection to the NxSIEM server and to send logs from them. Refer to the section

**Downloading and Installing NxSIEM Agent on Endpoints** for more details.

- **Configuration Script Download Buttons** - The configuration files can be directly run on endpoints with RSYSLOG and NXLOG utilities respectively without any re-configuration, for them to send logs to NXSIEM server. Refer to the section **Configuring Nxlog and Rsyslog servers to send logs to NxSIEM server** for more details.

### 4.2.2 Soft Assets

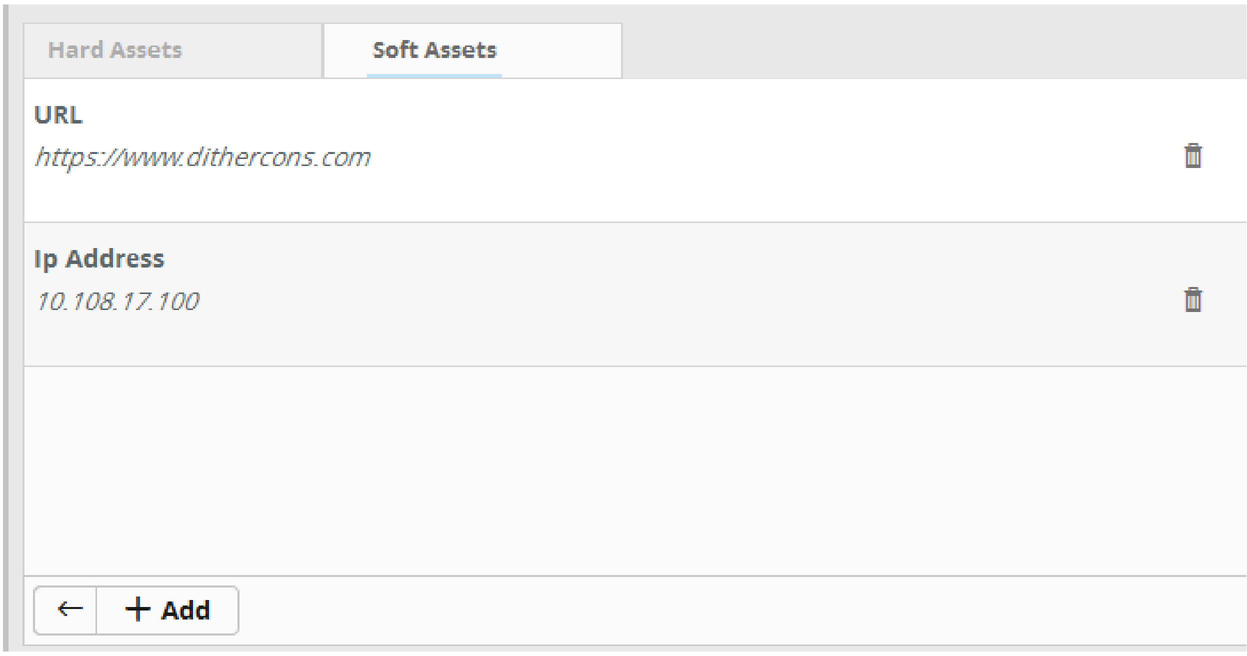
The 'Soft Assets' interface allows administrators to add and manage the services hosted from the customer networks and to create a list of important URLs, domains or IP addresses, which acts as a reference list for the operators/administrators/analysts. Suppose if any of the items displayed in this screen is affected by an incident, the operator/administrator/analyst may decide to act upon it, say for example escalate the incident from high to critical or choose any other action as required.

**To open the Soft Assets interface for a customer**

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

The Customer Details pane will open in the right.

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



URL
https://www.dithercons.com

Ip Address
10.108.17.100

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

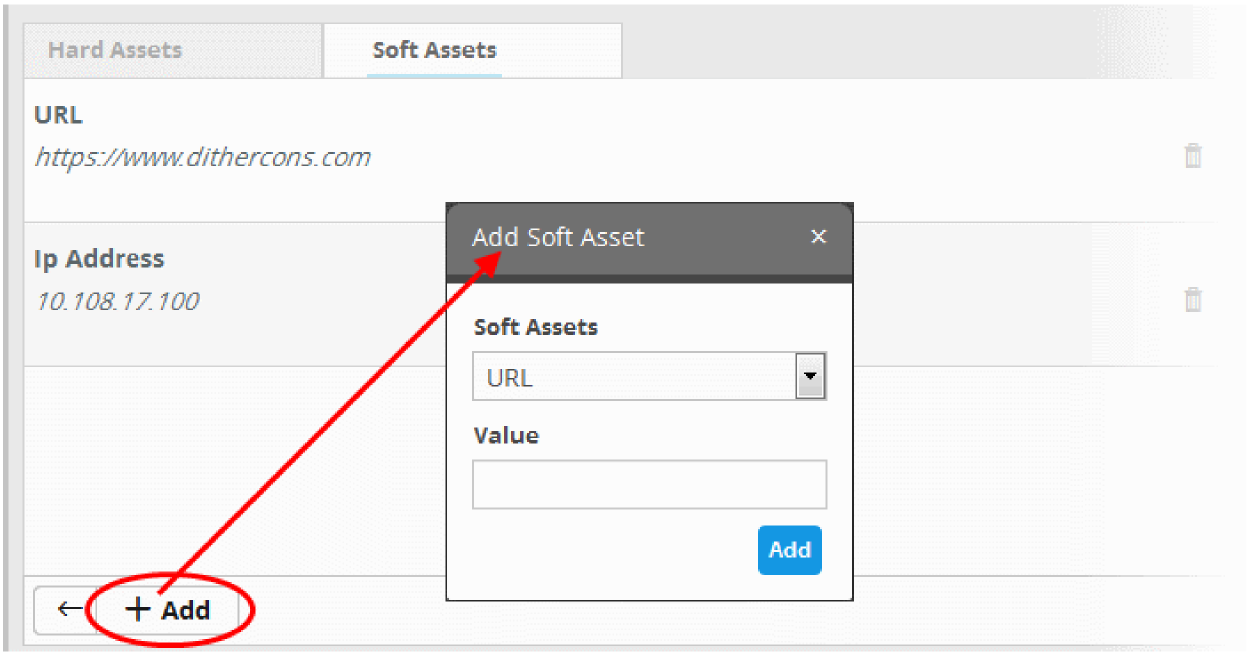
- **Add new Soft Assets**
- **Remove Soft Assets**

**To add soft assets for a customer**

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

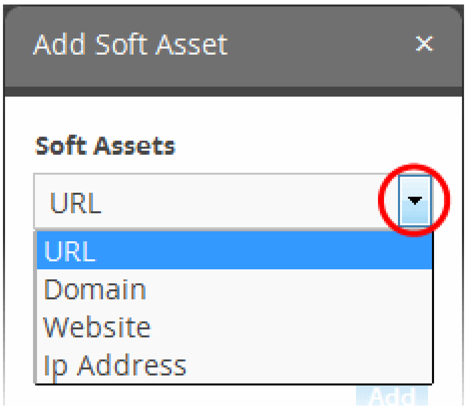
The Customer Details pane will open in the right.

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



The 'Add Soft Asset' dialog will be displayed.

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



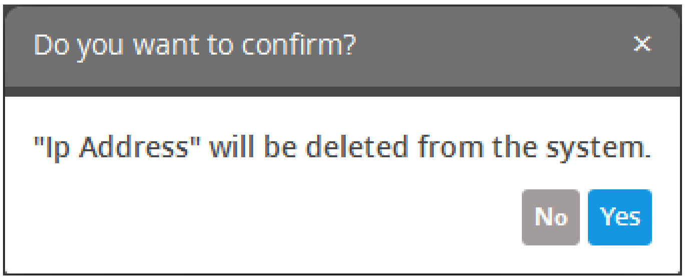
- Enter the value for the selected soft asset in the 'Value' field.
- Click the 'Add' button.

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

**To remove a soft asset**

- Click the 🗑 button in the row of the asset.

A confirmation dialog will appear.



Do you want to confirm?

"Ip Address" will be deleted from the system.

- Click 'Yes' to remove the item.

## 4.3 Downloading and Installing the NxSIEM Agent on Endpoints

There are two methods administrators can use to collect logs from endpoints connected to customer networks:

- Collection Agent - A Log Collection Agent installed on Windows and Linux endpoints forwards the logs to the NxSIEM server
- Agent less Collection - On target endpoints, administrators use our pre-defined scripts to configure RSYSLOG or NXLOG utilities to send the logs to the NxSIEM server

This section explains the installation of the collection agent on endpoints. The agent setup file for Windows and Linux endpoints can be downloaded from the NxSIEM administrative console. For each network and zone added, NxSIEM generates a unique agent activation key which has to be used for configuring the agent to connect to the server. Refer to the **explanation of getting the activation key for a network or zone** in the previous section, **Hard Assets**, for more details.

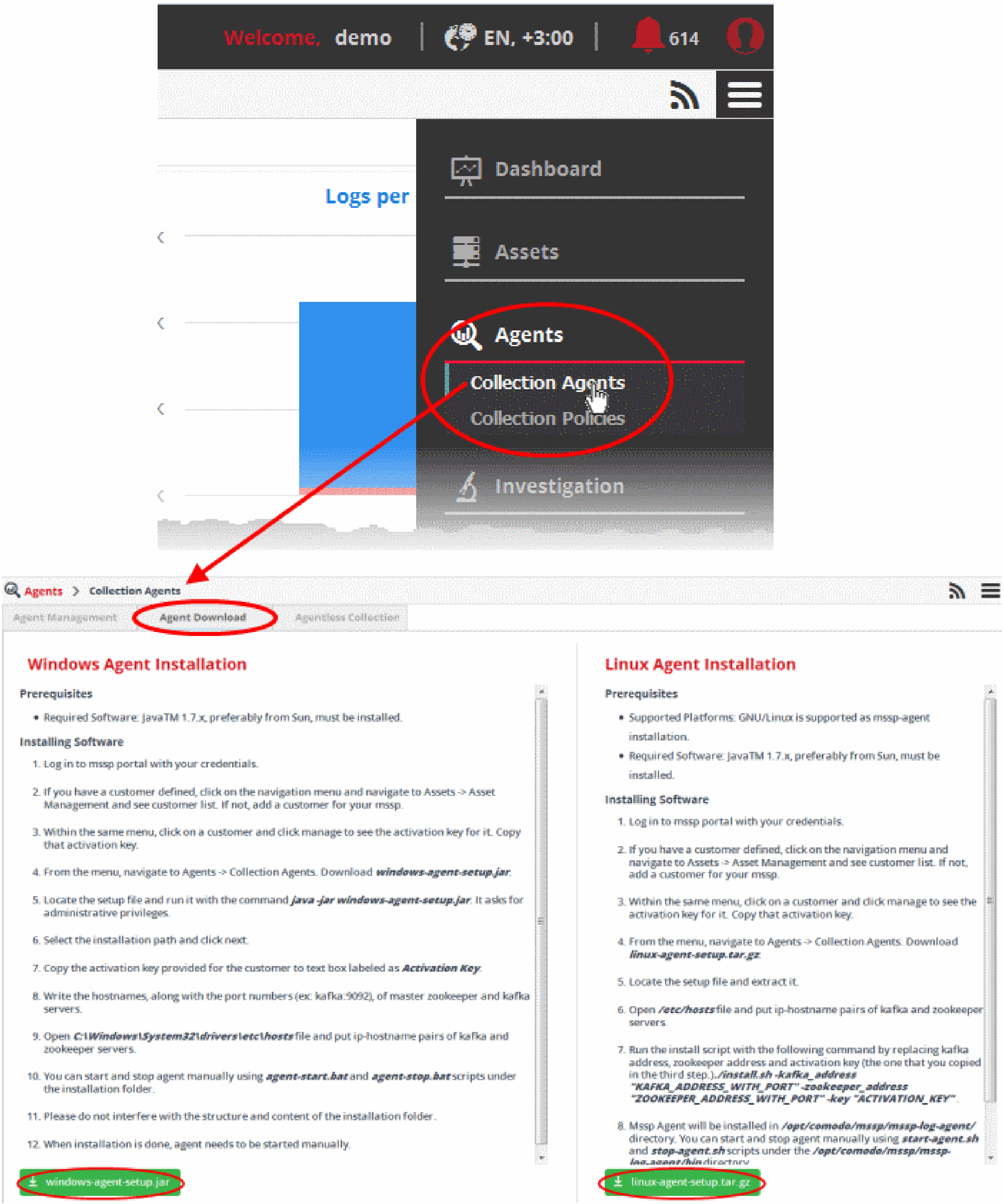
The next sections in this guide cover:

- **Downloading the Agent Setup file**
- **Installation on Windows Endpoints**
- **Installation on Linux Endpoints**

### Downloading the Setup Files

The agent setup files for Windows and Linux can be downloaded from the 'Agent Download' tab:

- 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.

**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

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.

## Installation on Windows Endpoints

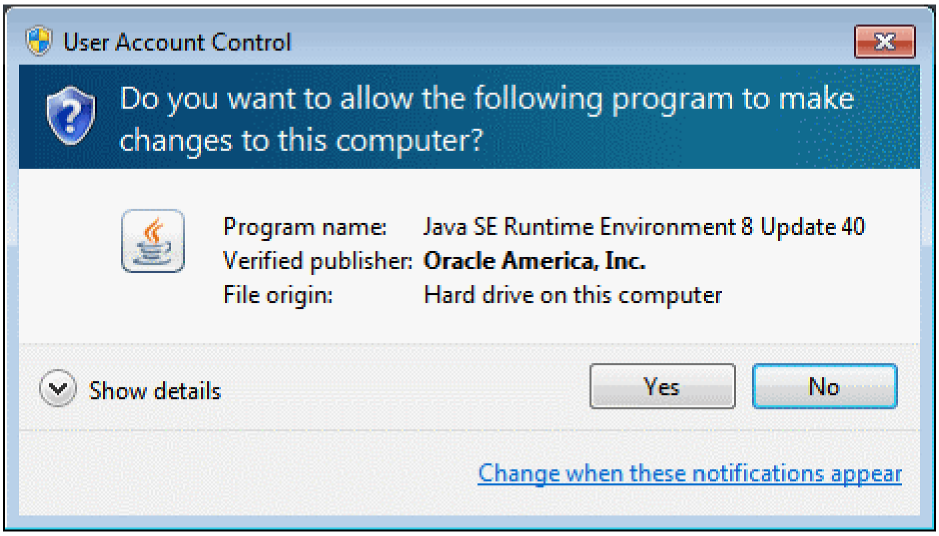
**Prerequisites for a Windows agent installation:**

- Software: Java 1.7 or higher preferably downloaded from Sun website.

Tip: 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. Refer to the **explanation of getting the activation key for a network or zone** in the previous section **Hard Assets** for more details.

**To install the Agent and enroll the endpoint**

- Navigate to the location where the 'Windows-agent-setup' file is saved at the endpoint and double click on it.

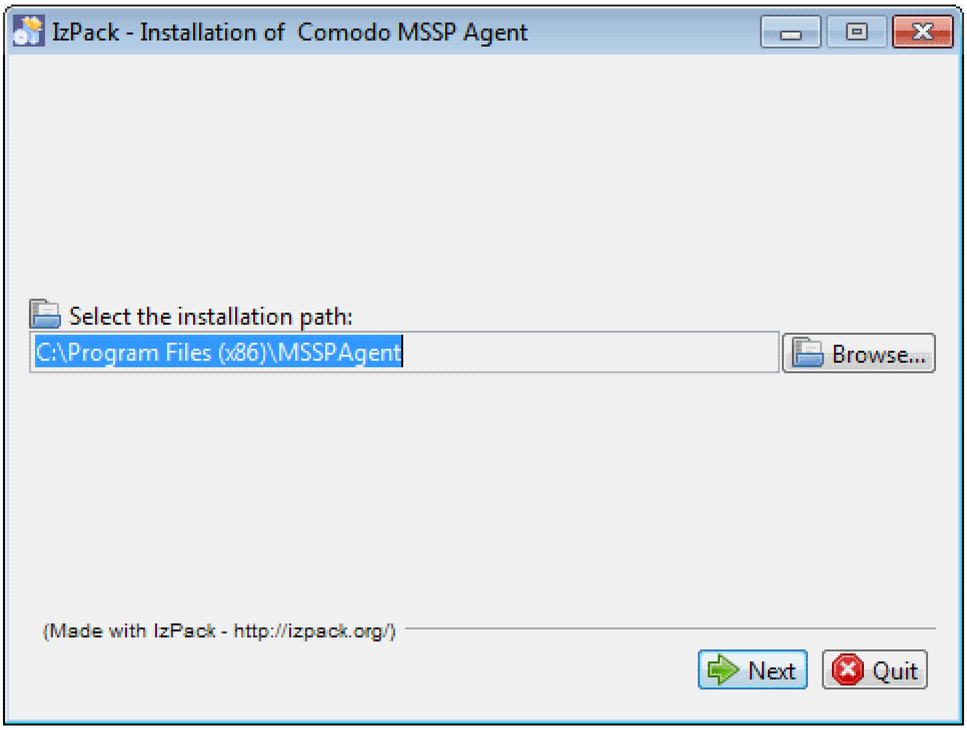


User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Java SE Runtime Environment 8 Update 40
Verified publisher: Oracle America, Inc.
File origin: Hard drive on this computer

- Click 'Yes' to continue the agent installation

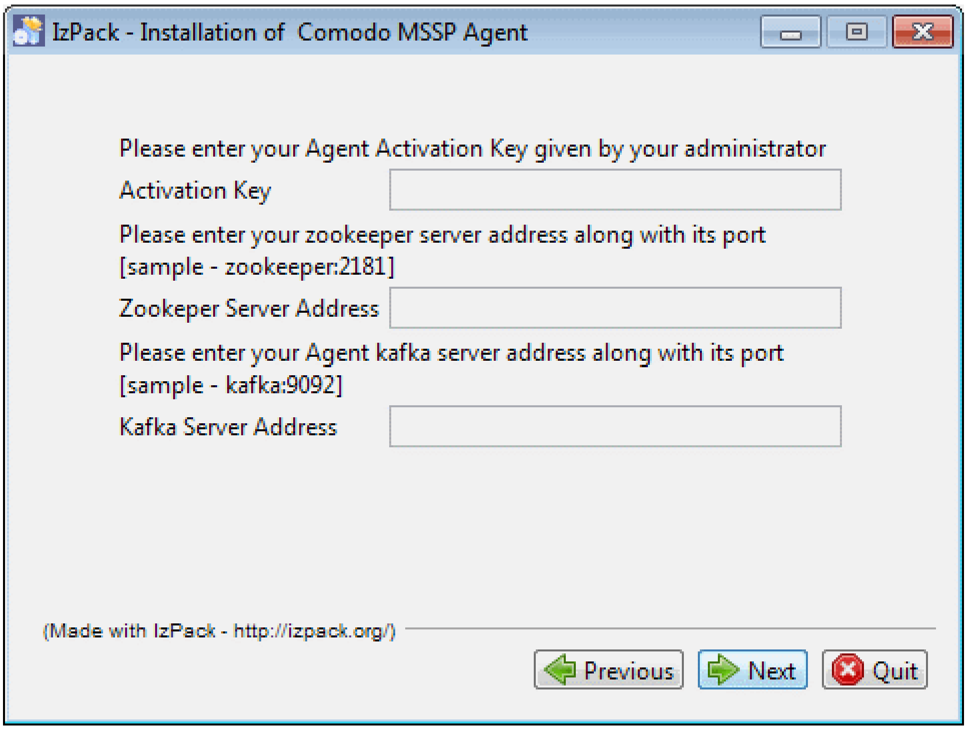


IzPack - Installation of Comodo MSSP Agent

Select the installation path:
C:\Program Files (x86)\MSSPAgent

(Made with IzPack - http://izpack.org/)

- By default the collection agent is installed at C:\Program Files\MSSP Agent. If you want to install the agent in a location other than the default, click 'Browse' to choose a different location.
- Click 'Next'


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]

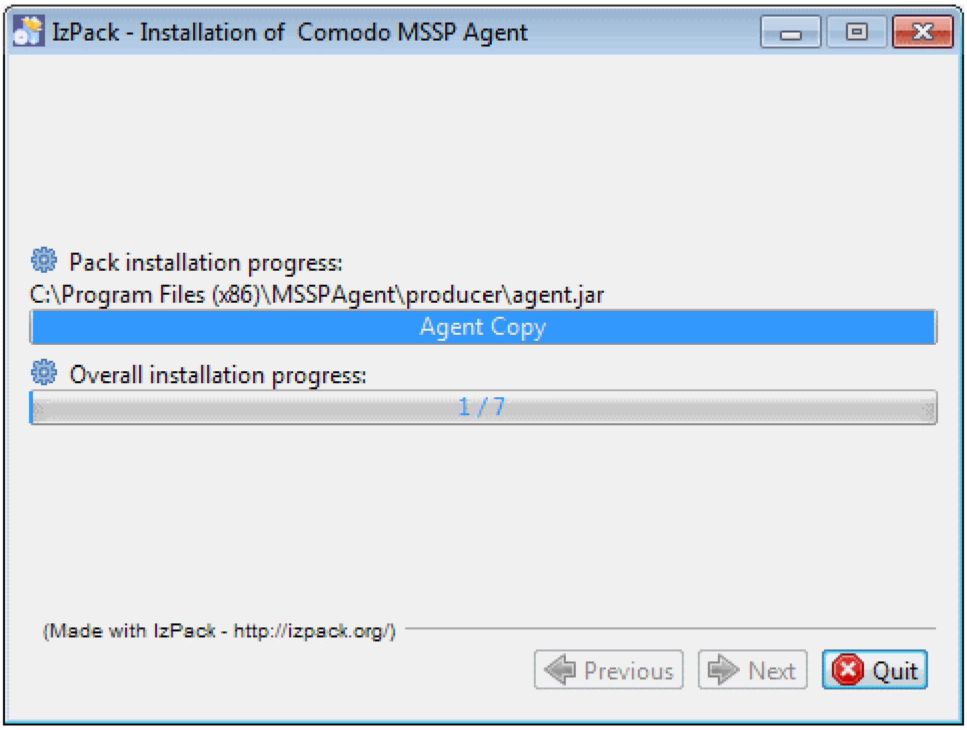
Kafka Server Address

(Made with IzPack - http://izpack.org/)

- **Activation Key** - Copy and paste the activation key that was generated for the customer network or zone for which you want to enroll the endpoint.
- **Zookeeper Server Address** - Enter the Zookeeper server address, including the port number.
- **Kafka Server Address** - Enter the Kafka server address, including the port number.

- Click 'Next'

The installation progress will be displayed...


IzPack - Installation of Comodo MSSP Agent

Pack installation progress:

C:\Program Files (x86)\MSSPAgent\producer\agent.jar

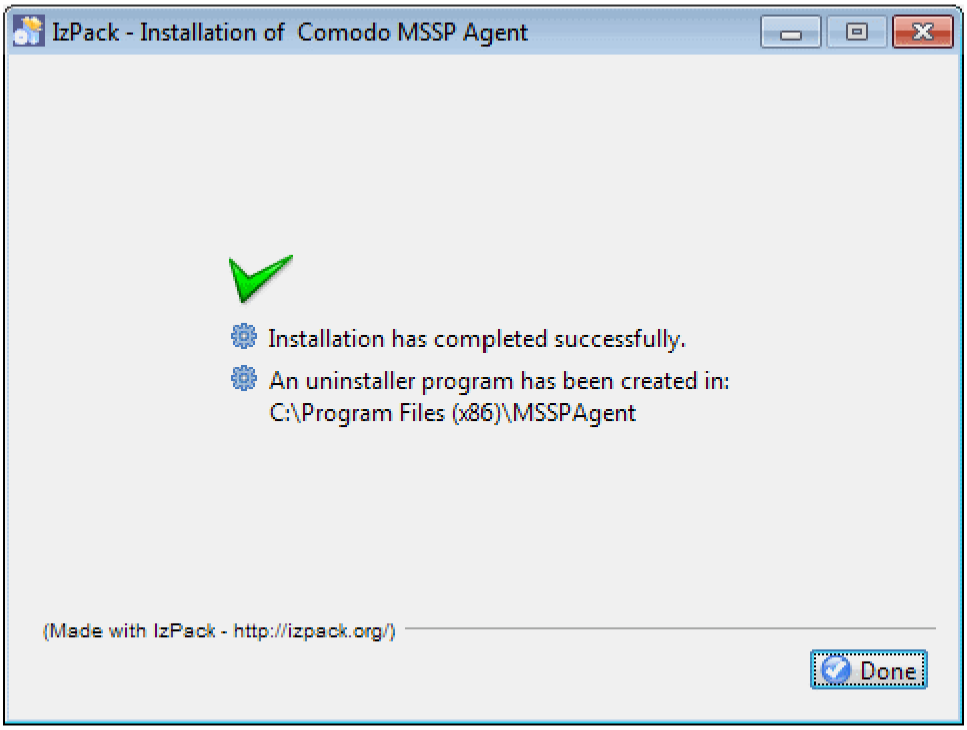
Agent Copy

Overall installation progress:

1 / 7

(Made with IzPack - http://izpack.org/)

….and on completion, the success dialog will be displayed.



Installation has completed successfully.

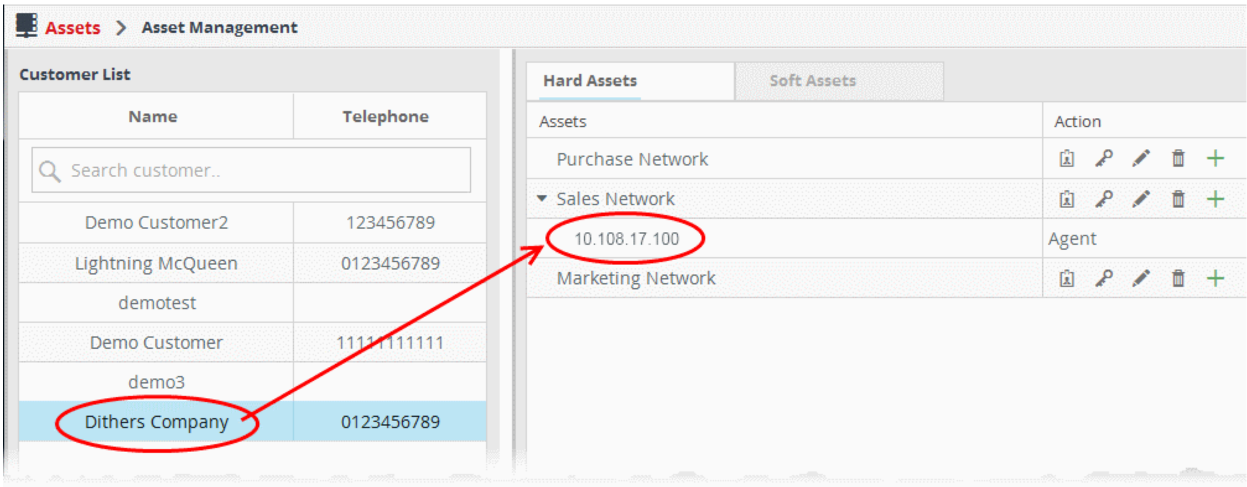
An uninstaller program has been created in:
C:\Program Files (x86)\MSSPAgent

(Made with IzPack - http://izpack.org/)

Now that the agent is installed, the next step is to add the host names of Zookeeper and Kafka servers.

- Open C:\Windows\System32\drivers\etc\hosts file and add IP-Hostname pairs of Zookeeper and Kafka servers.
- Save the hosts file.

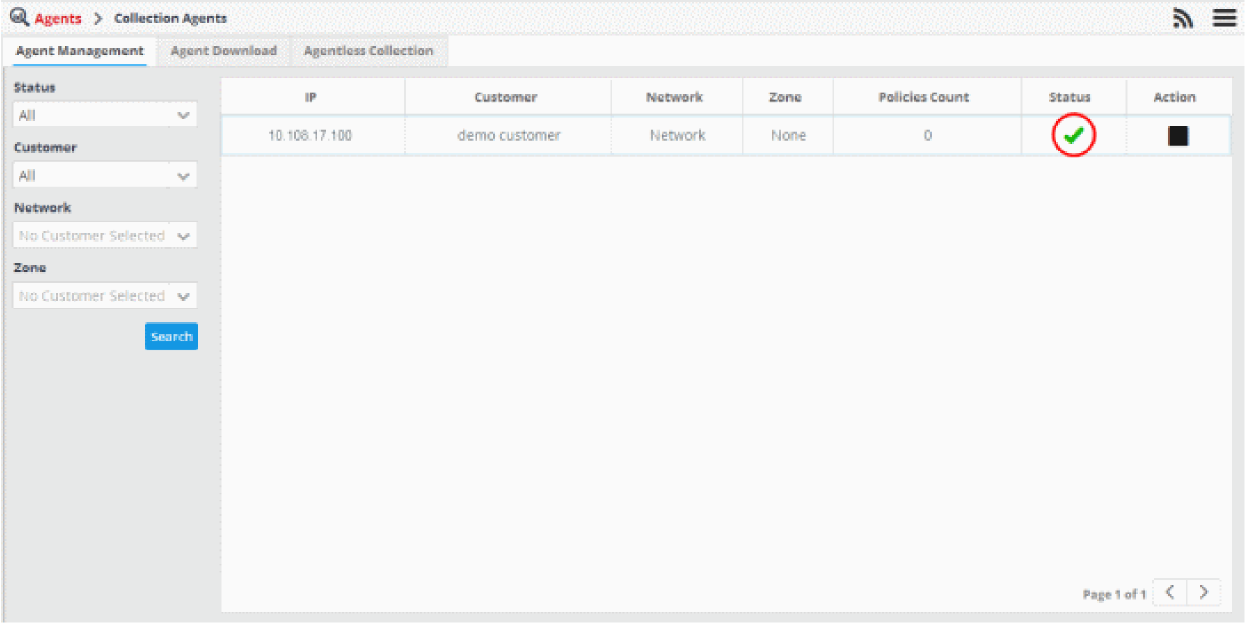
The agent will establish connection with NxSIEM server and the endpoint will be listed for the customer under the respective network/zone.



| Name | Telephone |
|---|---|
| Demo Customer2 | 123456789 |
| Lightning McQueen | 0123456789 |
| demotest | |
| Demo Customer | 1111111111 |
| demo3 | |
| Dithers Company | 0123456789 |

| Assets | Action |
|---|---|
| Purchase Network | |
| Sales Network | |
| 10.108.17.100 | Agent |
| Marketing Network | |

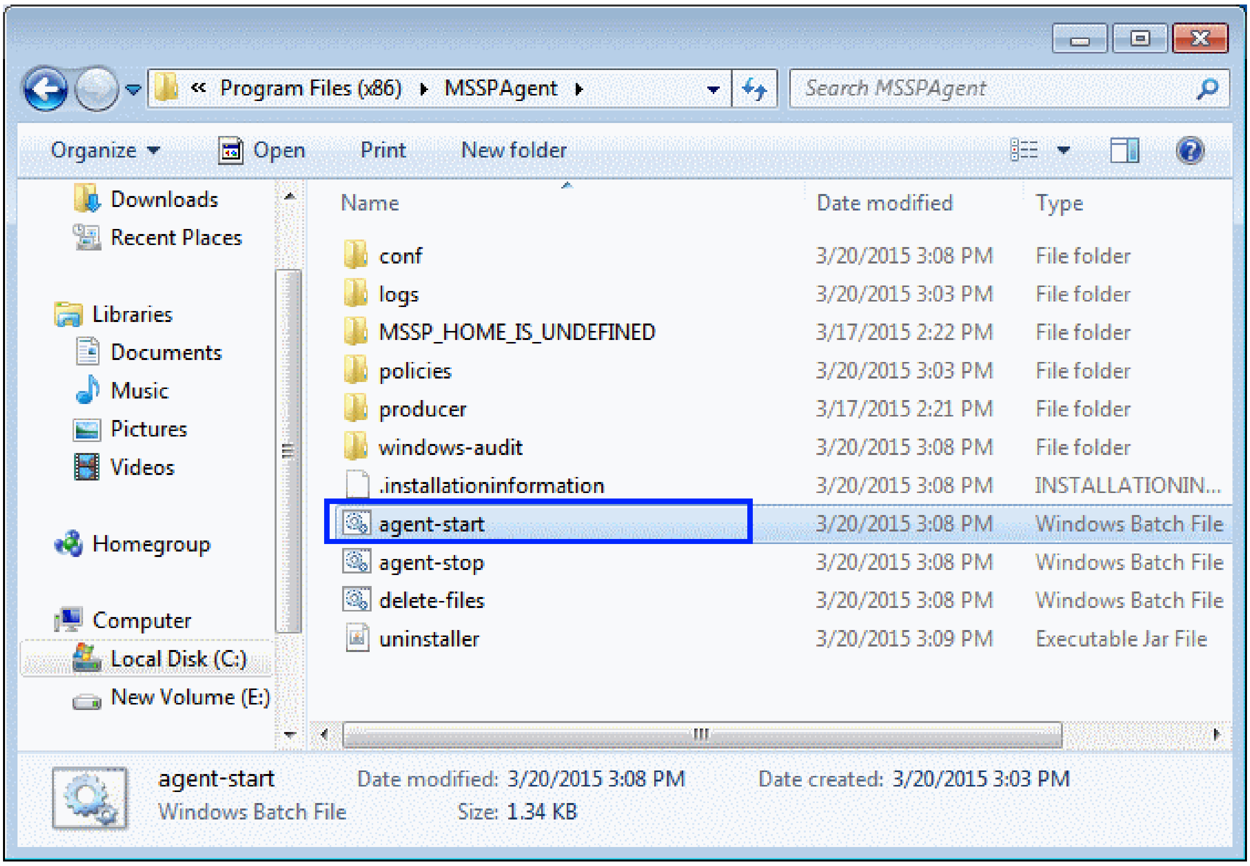
To check whether the agent is running, click the 'Menu' button, navigate to 'Agent' > 'Collection Agents' > 'Agent Management' tab.



| IP | Customer | Network | Zone | Policies Count | Status | Action |
|---|---|---|---|---|---|---|
| 10.108.17.100 | demo customer | Network | None | 0 | ✓ | ■ |

The green tick mark under the 'Status' column indicates the agent is running and connected to NxSIEM server.

If an agent is not running on an endpoint end for any reason, you can start it by navigating to the 'MSSPAgent' folder, right-clicking on the 'agent-start' file and selecting 'Run as administrator' from the context sensitive menu.



| Name | Date modified | Type |
|---|---|---|
| conf | 3/20/2015 3:08 PM | File folder |
| logs | 3/20/2015 3:03 PM | File folder |
| MSSP_HOME_IS_UNDEFINED | 3/17/2015 2:22 PM | File folder |
| policies | 3/20/2015 3:03 PM | File folder |
| producer | 3/17/2015 2:21 PM | File folder |
| windows-audit | 3/20/2015 3:08 PM | File folder |
| .installationinformation | 3/20/2015 3:08 PM | INSTALLATIONIN... |
| agent-start | 3/20/2015 3:08 PM | Windows Batch File |
| agent-stop | 3/20/2015 3:08 PM | Windows Batch File |
| delete-files | 3/20/2015 3:08 PM | Windows Batch File |
| uninstaller | 3/20/2015 3:09 PM | Executable Jar File |

agent-start Date modified: 3/20/2015 3:08 PM Date created: 3/20/2015 3:03 PM
Windows Batch File Size: 1.34 KB

## Installation on Linux Endpoints

**Prerequisites for a Linux agent installation**:

- Software: Java TM 1.7 or higher preferably downloaded from Sun website.

**Tip**: 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. Refer to the **explanation of getting the activation key for a network or zone** in the previous section **Hard Assets** for more details.

**To install the Agent and enroll the endpoint**

- 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-agent*** 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 a connection to the NxSIEM server and the endpoint will be listed for the customer under the respective network/zone.

- To stop the agent, run the command ***stop-agent.sh*** under ***/opt/comodo/mssp/mssp-log-agent /bin*** directory

## 4.4 Configuring Nxlog and Rsyslog to Send Logs to NxSIEM Server

Comodo NxSIEM features agent-less log collection from Windows/Linux endpoints connected to customers' networks, through the use of Nxlog and Rsyslog utilities. This is useful for customers who do not wish to install agents on their endpoints. The NXLOG utility (Windows endpoints) and the RSYSLOG utility (Linux endpoints) need to be configured to send logs to the NxSIEM server.

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

The following sections explain more about:

- **Configuring the NXLOG Utility**
- **Configuring the RSYSLOG Utility**

### Configuring the NXLOG Utility

Administrators can download a specific customer's NXLOG configuration file from the administrative console and use this to configure the NXLOG utilities installed on Windows endpoints connected to the customer's network.

**To download the NXLOG Configuration File**

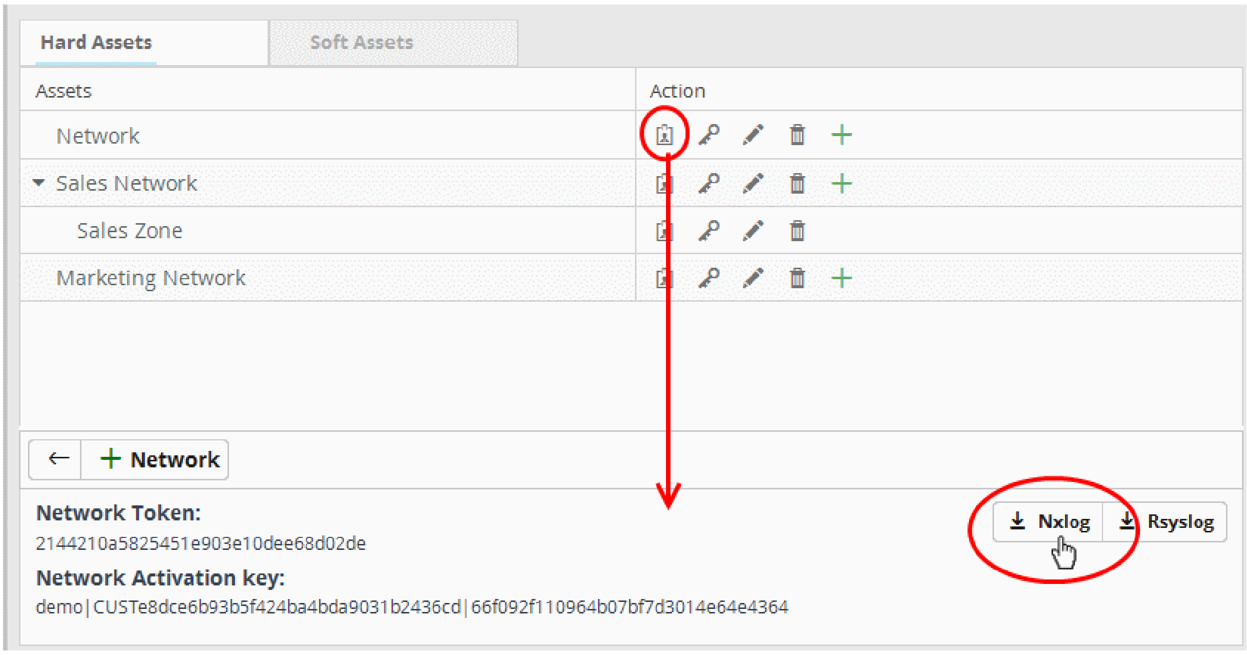
- Open the 'Asset Management' interface by clicking the 'Menu' button, then 'Assets' > 'Asset Management'.
- Select the customer from the left hand side pane.

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:



Network Token:
2144210a5825451e903e10dee68d02de

Network Activation key:
demo|CUSTe8dce6b93b5f424ba4bda9031b2436cd|66f092f110964b07bf7d3014e64e4364

- 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.

## Configuring RSYSLOG Utility

Administrators can download a pre-configured RSYSLOG configuration script, generated specifically for each customer/network, from the administrative console. This script will configure RSYSLOG utilities installed on Linux endpoints in customer networks to send logs to the NxSIEM server.

**To download the RSYSLOG Configuration File**

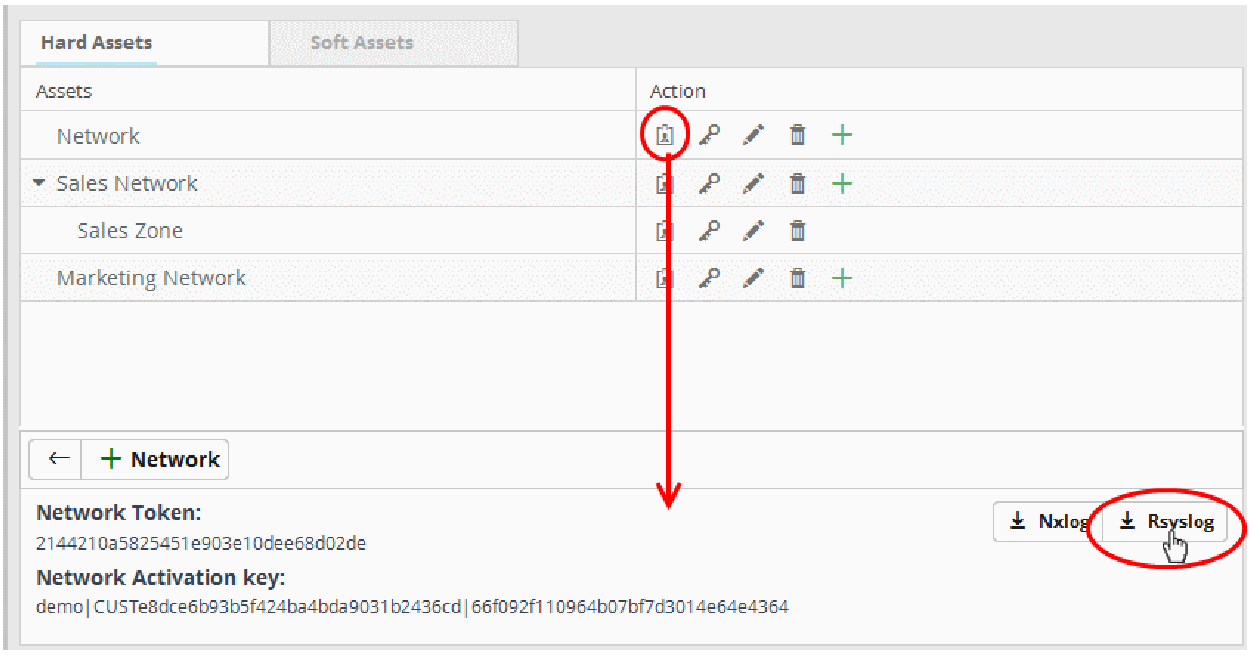
- Open the 'Asset Management' interface by clicking the 'Menu' button, then 'Assets' > 'Asset Management'.
- Select a customer from the left hand pane.

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.



**Network Token:**
2144210a5825451e903e10dee68d02de

**Network Activation key:**
demo|CUSTe8dce6b93b5f424ba4bda9031b2436cd|66f092f110964b07bf7d3014e64e4364

- 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 the script file for configuring the RSYSLOG utility 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 section **Agentless Log Collection** for more details.

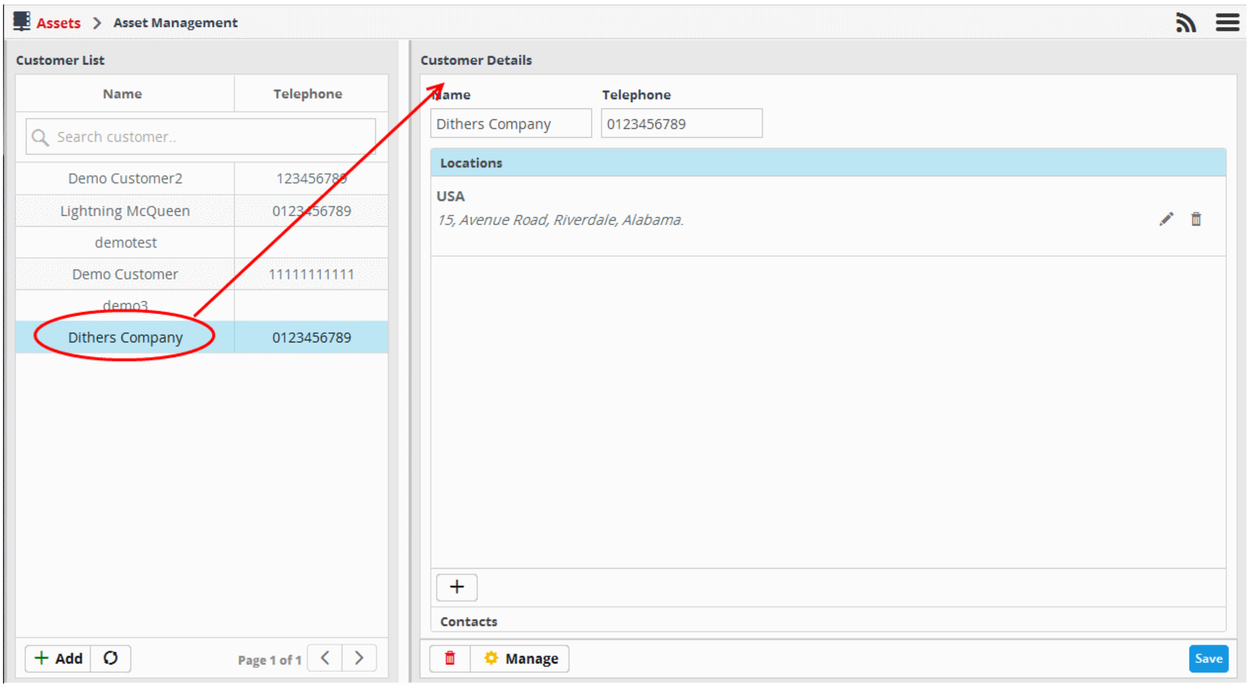
## 4.5 Editing Customers

Administrators can edit the details of a customer such as name of the company, its address and location. If required, the customer can also be removed from NxSIEM.

**To edit a customer's details**

- 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.



Customer List

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

Customer Details

Name: Dithers Company

Telephone: 0123456789

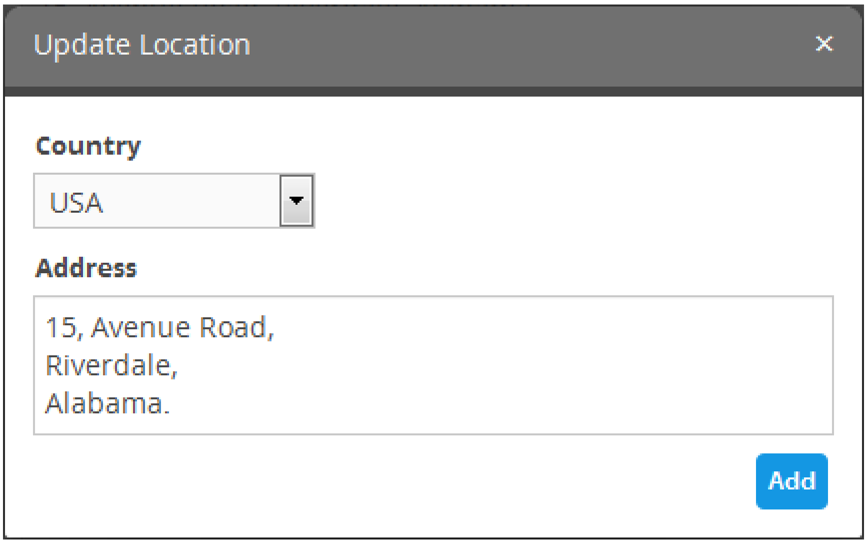
Locations

USA
*15, Avenue Road, Riverdale, Alabama.*

- To edit the company name and telephone number, click in the respective fields, edit the details and click the 'Save' button.
- To edit the location details, click the 'Location' stripe.

A list of locations added for the customer will be displayed.

- To edit a location, click the ✎ button beside it. The Update Location dialog will open.



Update Location

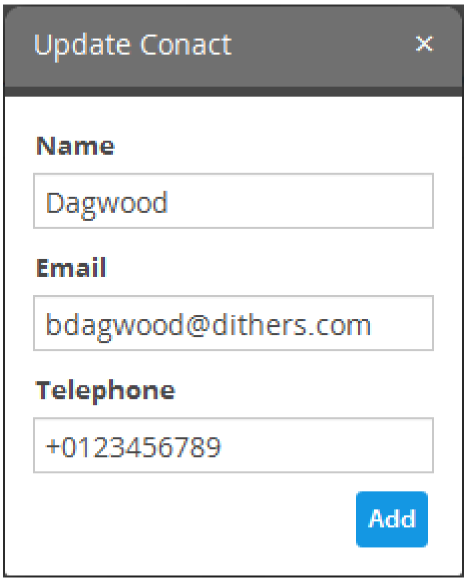
Country: USA

Address:
15, Avenue Road,
Riverdale,
Alabama.

  - Edit the details as required and click the 'Add' button and then the 'Save' button at the bottom of the interface.
  - To remove a location for the customer, click the 🗑 button and then click the 'Save' button at the bottom of the interface.
- To edit the contact details of a customer, click the 'Contacts' stripe.

A list of contacts added for the customer will be displayed.

- To edit a contact, click the ✎ button beside it. The 'Update Contact' dialog will open.



Update Conact

Name: Dagwood

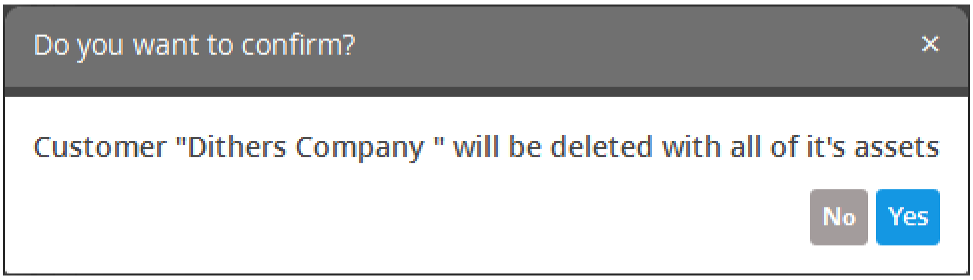
Email: bdagwood@dithers.com

Telephone: +0123456789

- Edit the details as required and click the 'Add' button and then the 'Save' button at the bottom of the interface.
- To remove a contact for the customer, click the 🗑 button and then click the 'Save' button at the bottom of the interface.

- To remove a customer, click the 🗑 button beside the 'Manage' button at the bottom.

A confirmation dialog will appear.



Do you want to confirm?

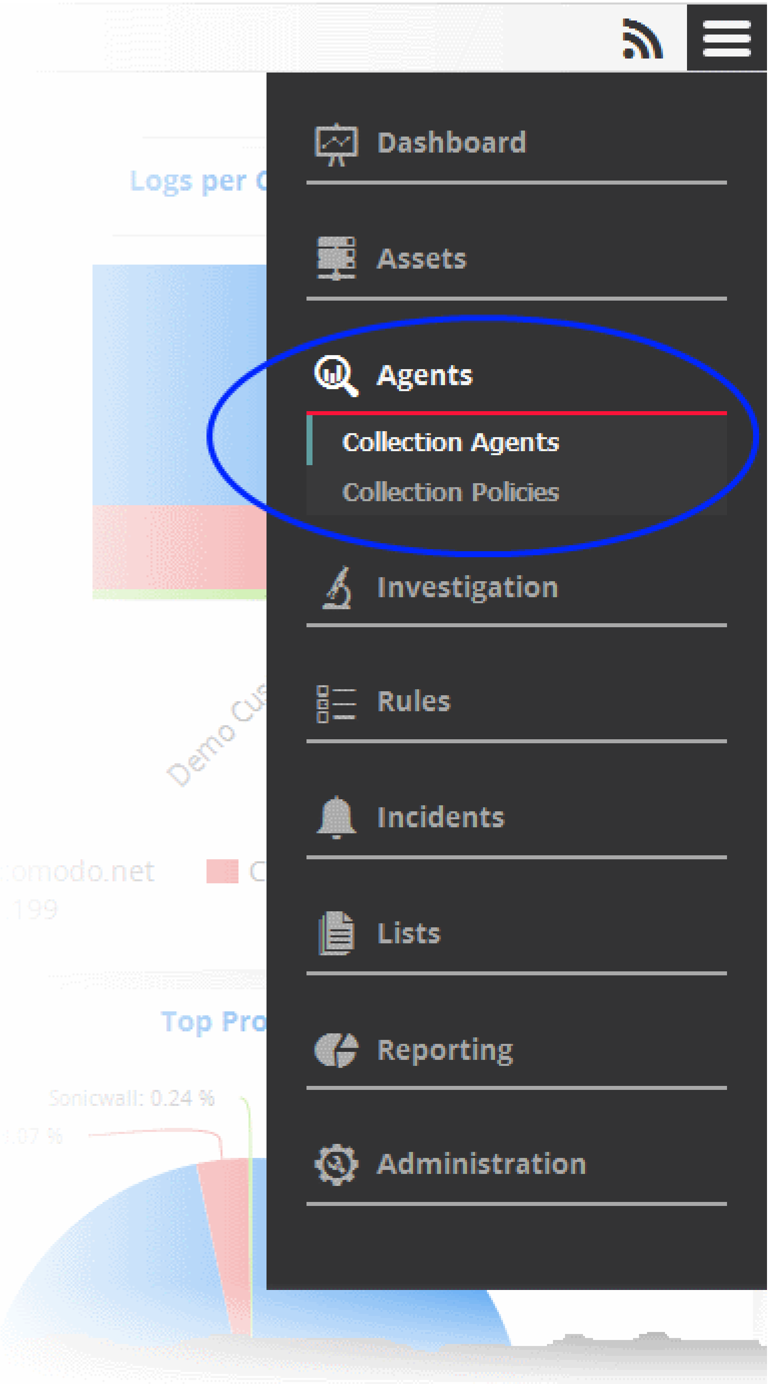
Customer "Dithers Company " will be deleted with all of it's assets

- Click 'Yes' to remove the customer.

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

# 5 Log Collection Agents and Policies

Comodo NxSIEM is capable of collecting logs in two ways - by deploying agents or by using NXLOG/RYSLOG software utilities (agent-less collection). You can download the agents, configure polices to collect logs and more from the 'Agents' menu.



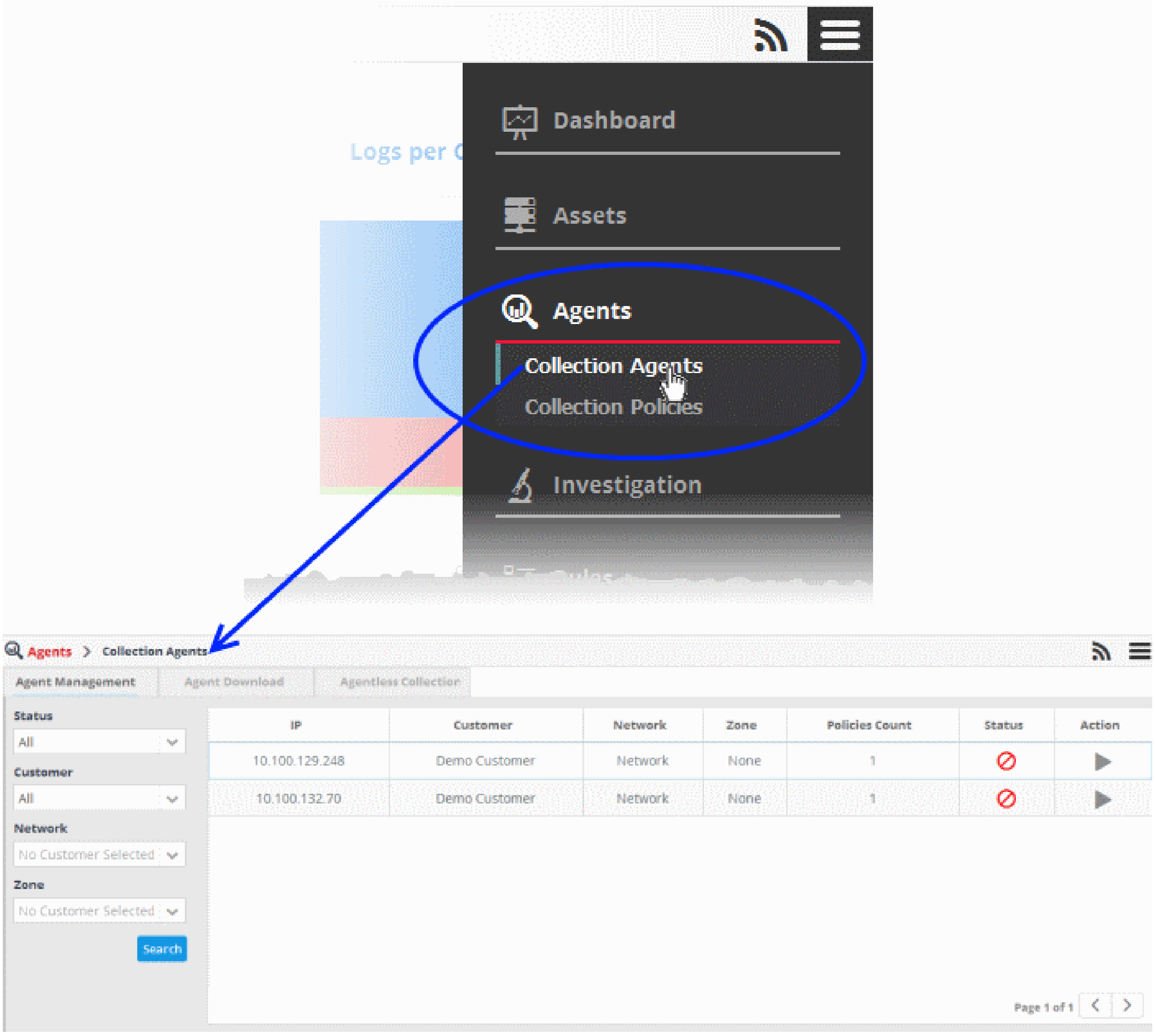
Refer to the following sections for more details:

- Collection Agents
- Log Collection Policies

## 5.1 Collection Agents

The 'Collection Agents' interface allows administrators to download NxSIEM agents for Windows and Linux endpoints, manage agents and configure RSYSLOG software utility for agent-less log collection.

To open the 'Collection Agents' interface, click the 'Navigational Menu' button from the top right, choose 'Agents' and then click 'Collection Agents'.



Status: All

Customer: All

Network: No Customer Selected

Zone: No Customer Selected

| IP | Customer | Network | Zone | Policies Count | Status | Action |
|---|---|---|---|---|---|---|
| 10.100.129.248 | Demo Customer | Network | None | 1 | ⊘ | ▶ |
| 10.100.132.70 | Demo Customer | Network | None | 1 | ⊘ | ▶ |

The 'Collection Agents' interface has three tabs:

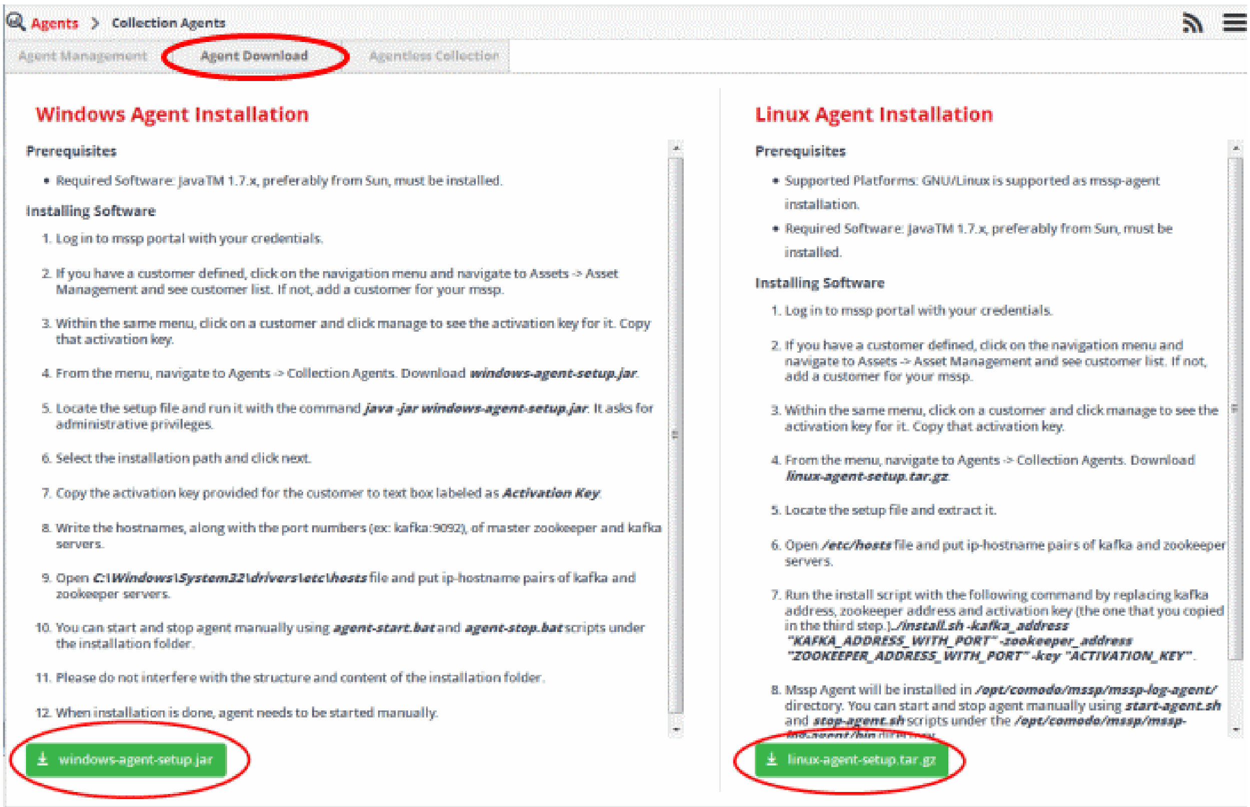
- **Agent Management** - Displays all customer endpoints that have log collection agents installed. Also allows the administrator to manually start and stop agents as required. Refer to the section **Managing Agents** for more details.
- **Agent Download** - Enables administrators to download the log collection agent installation files for Windows and Linux endpoints. Refer to the section **Downloading NxSIEM Agents for Windows and Linux Endpoints** for more details.
- **Agentless Collection** - Enables administrators to download configuration scripts for the Linux RSYSLOG utility. This will allow you to collect logs from Linux endpoints without installing the collection agent. Refer to the section **Agentless Log Collection** for more details.

## 5.1.1 Downloading NxSIEM Agents for Windows and Linux Endpoints

Comodo NxSIEM uses agents deployed on endpoints to collect logs for monitoring and analysis. After installation, each agent needs to be activated using the activation key specific for the customer's network.

**To download the agent setup file**

- Click the 'Navigational Menu' button from the top right, then choose 'Agents' > 'Collection Agents'
- Click the 'Agent Download' tab:



**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.

**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.

The 'Agent Download' page contains instructions for installing the agent on Windows and Linux endpoints and allows you to download the agent installation files. Read the instructions fully.

- Click the 'windows-agent-setup.jar' or 'linux-agent-setup.gz' button to download the respective agent.

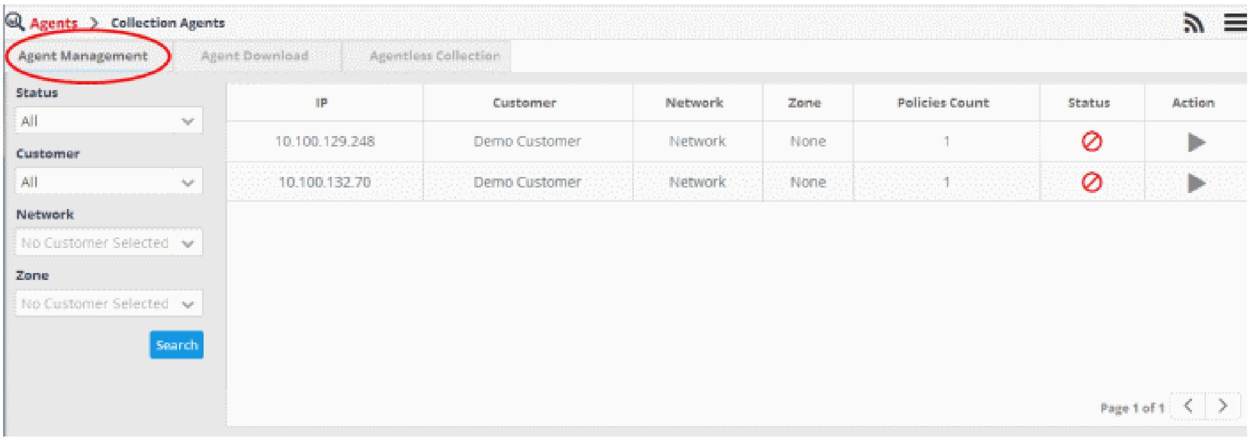
After downloading the agent setup file, transfer it to the endpoint that you want to import into NxSIEM and monitor and install the agent. For more details on installing the agent, refer to the section **Downloading and Installing the NxSIEM Agent on Endpoints**.

### 5.1.2 Managing Agents

The 'Agent Management' interface allows administrators to view all customer endpoints that have the log collection agent installed, allow with details such as network and zone, the number of **collection policies** deployed on the agents and more. The administrator can also manually start/stop the agent at the required endpoints.

**To access the agent management interface**

- Click the 'Navigational Menu' button from the top right and choose 'Agents' from the options and then click 'Collection Agents'
- Click the 'Agent Management' tab:



Status: All

Customer: All

Network: No Customer Selected

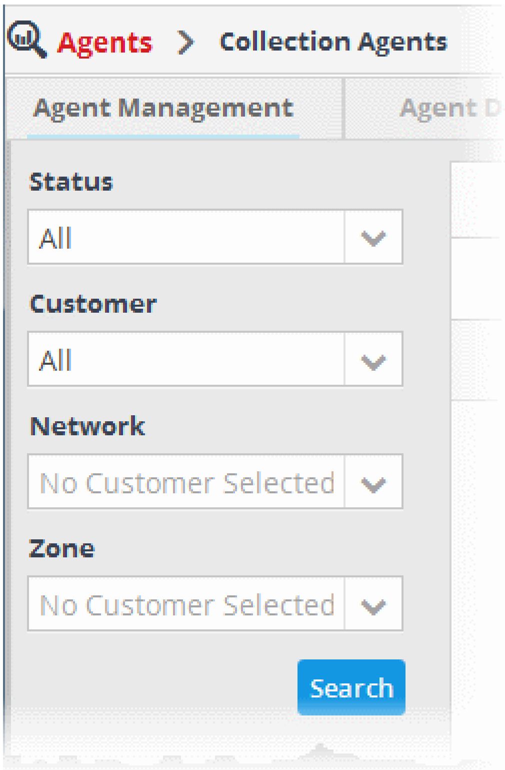
Zone: No Customer Selected

| IP | Customer | Network | Zone | Policies Count | Status | Action |
|---|---|---|---|---|---|---|
| 10.100.129.248 | Demo Customer | Network | None | 1 | ⊘ | ▶ |
| 10.100.132.70 | Demo Customer | Network | None | 1 | ⊘ | ▶ |

| Agent Management - Table of Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| IP | The IP address of the endpoint that is enrolled. |
| Customer | The name of the customer to which the enrolled endpoint is linked. |
| Network | The name of the network to which the endpoint is added. Refer to the section '**Hard Assets**' for more details on adding networks/zones. |
| Zone | The name of the zone to which the endpoint is added. Refer to the section '**Hard Assets**' for more details on adding networks/zones. |
| Policies Count | The number of log collection policies in effect on the agent. Refer to the section '**Log Collection Policies**' for more details on deploying policies to agents. |
| Status | Indicates whether the agent is running or stopped. |
| Action | Allows administrators to stop or start the agent. |

**Filter Options**

The filter options on the left allow you to display endpoints according customer, network, running status and more.

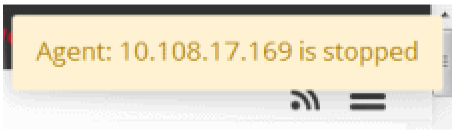


- **Status** - Allows you to filter the list depending on the current running status of the agents. The options available are:
  - All - Displays all the endpoints
  - Up - Displays the endpoints whose agents are running
  - Down - Displays the endpoints whose agents are stopped
- **Customer** - Allows you to filter the list depending on the customers. You can further refine the list by choosing the network/zone added for the customer.
- **Network** - Allows you to filter the list by choosing the network pertaining to the selected customer.
- **Zone** - Allows you to filter the list by choosing the zone formed in the chosen network.
- Click 'Search' after selecting the filter parameters to filter the list.

**To stop an agent**

- Click the ⏸ button in the row of the agent, under the 'Action' column to stop an agent.

The agent stopped message will be displayed:



Agent: 10.108.17.169 is stopped

**To restart an agent**

- Click the ▶ button in the row of the agent,  under the 'Action' column.

## 5.1.3 Agentless Log Collection

As an alternative to installing an agent, logs can be collected from endpoints by configuring the Nxlog (Windows) and Rsyslog (Linux) utilities on target endpoints.

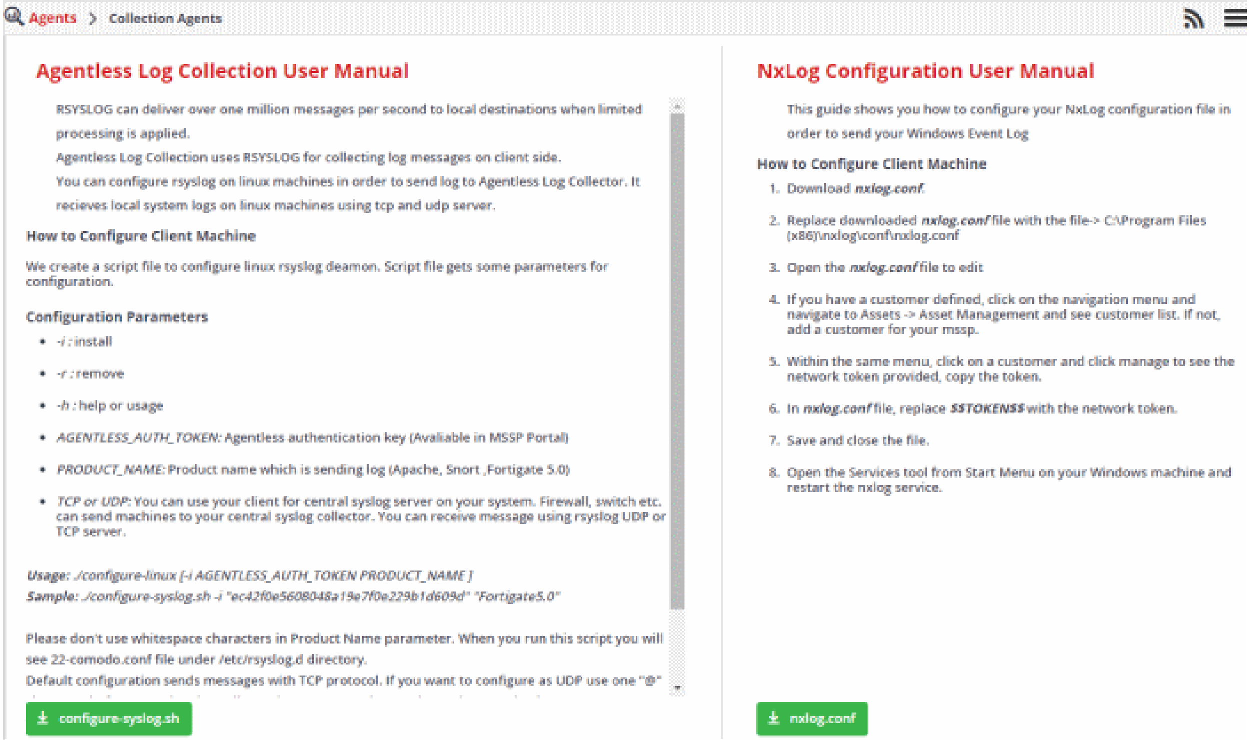
The NxSIEM console contains customer-specific configuration scripts for both utilities which will automatically configure the utilities to send logs to NxSIEM.

Scripts can be configured and deployed in two ways:

- **Pre-configured script files** - The administrator can download ready-made configuration script files with all parameters pre-configured for a specific customer/network from the 'Hard Assets' interface. This is the most convenient way of configuring NXLOG and RSYSLOG utilities at the endpoints to send logs to the NXSIEM server. Refer to the section **Configuring Nxlog and Rsyslog to Send Logs to NxSIEM Server** for more detailed explanations on downloading the script files and deploying them.
- **Manually configure RSYSLOG/NXLOG scripts** -  Administrators can download configuration scripts for RSYSLOG and NxLOG and manually set the  parameters such as network authentication token, name of product from which the logs are to be collected and so on. These scripts can be used to configure RSYSLOG and NxLOG utilities at Linux and Windows based endpoints to send logs to the NXSIEM server.

**To download the manual configuration script for RSYSLOG and NxLOG**

- Click the 'Menu' button from the top right, choose 'Agents' and then click 'Collection Agents'
- Click the 'Agentless Collection' tab.



**Agentless Log Collection User Manual**

RSYSLOG can deliver over one million messages per second to local destinations when limited processing is applied.

Agentless Log Collection uses RSYSLOG for collecting log messages on client side.

You can configure rsyslog on linux machines in order to send log to Agentless 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)
- *TCP or UDP:* You can use your client for central syslog server on your system. Firewall, switch etc. can send machines to your central syslog collector. You can receive message using rsyslog UDP or TCP server.

***Usage:*** *./configure-linux [-i AGENTLESS_AUTH_TOKEN PRODUCT_NAME ]*
***Sample:*** *./configure-syslog.sh -i "ec42f0e5608048a19e7f0e229b1d609d" "Fortigate5.0"*

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 "@"

**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 'Agentless Collection' page contains instructions on downloading the scripts, setting the parameters and configuring the RSYSLOG/NxLOG utilities using the scripts.

## 5.2 Log Collection Policies

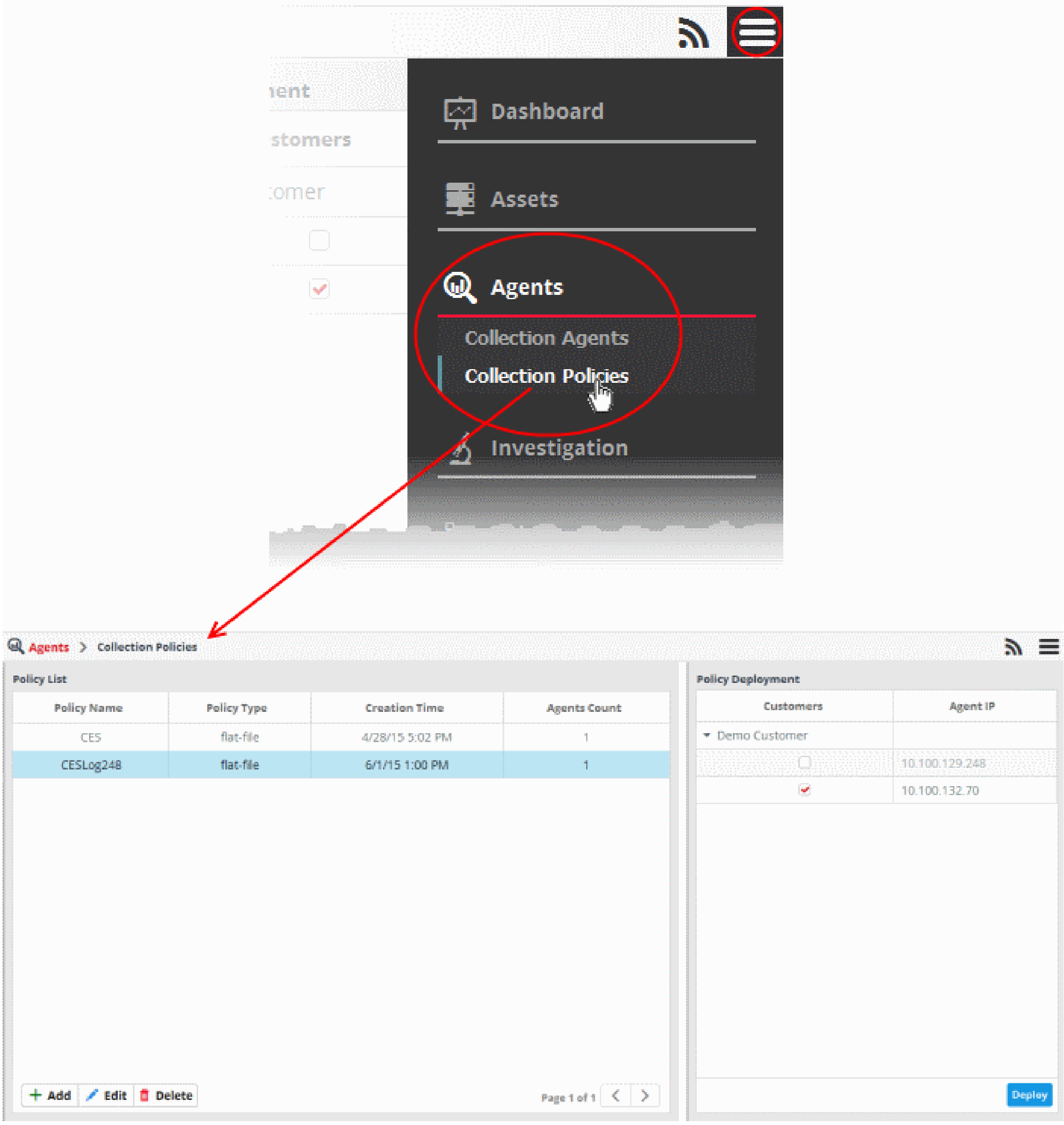
Collection policies allow administrators to define events for which logs should be collected, the sources from which logs are collected and so on. These can then be deployed to control the behavior of agents on managed customer endpoints. These logs are used to generate incidents, can be queried and used to generate comprehensive event reports. Refer to the sections '**Configuring Event Queries**' and '**Report Generation**' for more details.

Four types of collection policies are available in NxSIEM:

- **Audit Policy** - Agents collect the audit events from the host machine. This policy type does not require any additional configuration.
- **Flat File Policy** - This policy type allows administrators to configure agents to track and send specific files from the agent's host machine.
- **Remote Collection Policy** - This policy type allows administrators to configure agent installed on one machine to track a log file from another machine.
- **Syslog Policy** - This policy type allows administrators to configure the agent to collect Syslog entries from a specific port

Log collection policies can be configured and deployed from the 'Collection Policies' interface.

To open the 'Collection Policies' screen, click the 'Navigational Menu' button from the top right and choose 'Agents' from the options and then click 'Collection Policies'.



Policy List

| Policy Name | Policy Type | Creation Time | Agents Count |
|---|---|---|---|
| CES | flat-file | 4/28/15 5:02 PM | 1 |
| CESLog248 | flat-file | 6/1/15 1:00 PM | 1 |

Policy Deployment

| Customers | Agent IP |
|---|---|
| ▾ Demo Customer | |
| □ | 10.100.129.248 |
| ☑ | 10.100.132.70 |

The 'Policy List' section on the left side displays a list of policies available for deployment.

| Policy List - Table of Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Policy Name | The name of the log collection policy as assigned during its creation |
| Policy Type | Indicates the type of the policy, that defines the events for which the log is collected and the log collection source. |
| Creation Time | The date and time at which the policy was created |
| Agents Count | The number of agents onto which the policy is deployed. |

The 'Policy Deployment' pane on the right displays a list of all customer endpoints which have the agent installed, and allows administrators to deploy the policy selected on the left to the selected endpoints.

| Policy Deployment - Table of Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Customers | The name of the customer. Below each customer, the check boxes indicate the deployment state of the policy selected from the left hand side pane on the corresponding endpoint shown in the Agent IP column. The check boxes can be used to deploy or remove the selected policy to the endpoints. Refer to the section '**Deploy a policy**' for more details. |
| Agent IP | The IP addresses of the systems in which the agents are installed |

Following sections contain descriptions of different types of policies, and explain on creating and deploying policies to selected agents:

- **Audit Policy**
- **Flat File Policy**
- **Remote Log Collection Policy**
- **Syslog Policy**
- **Configuring Log Collection Policies**

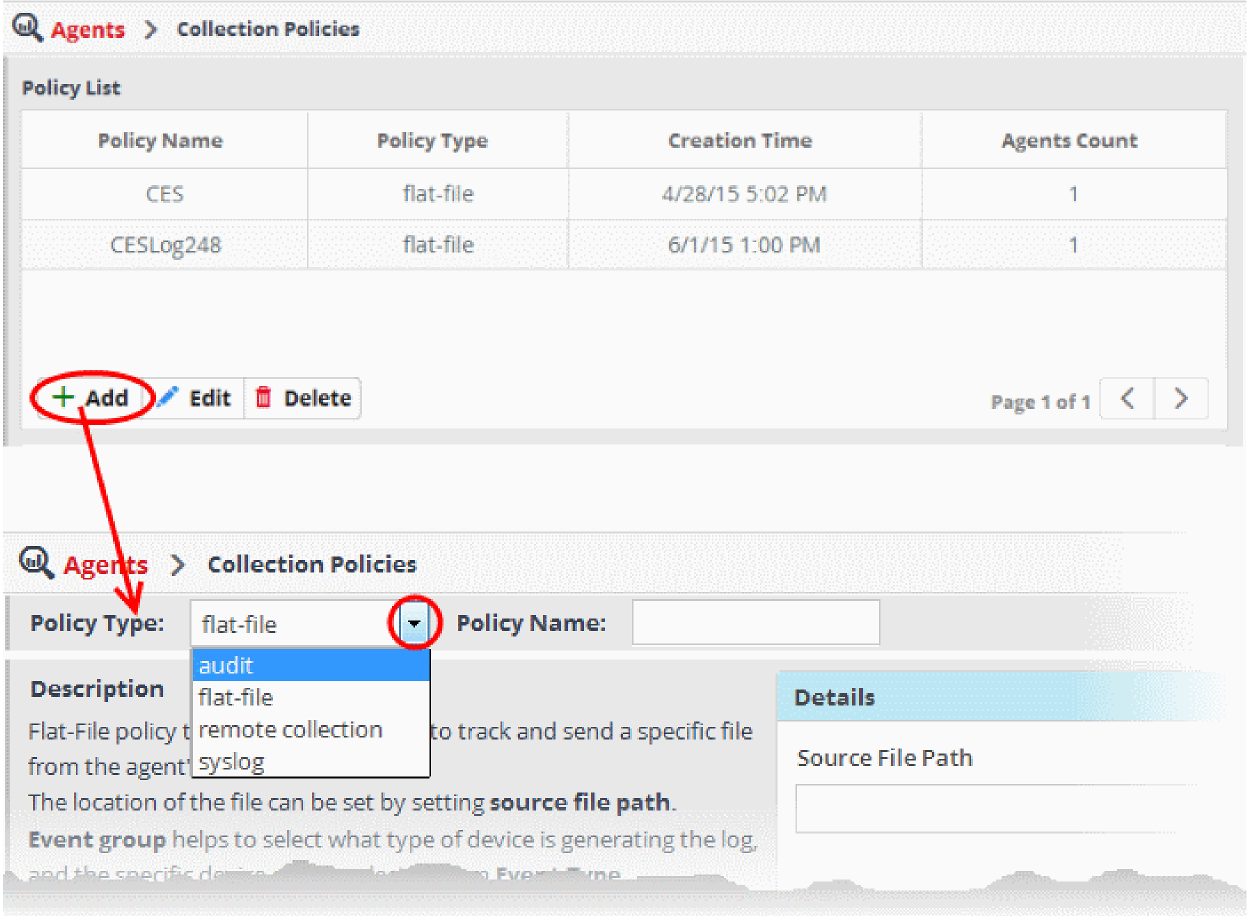
### 5.2.1 Audit Events Policy

The 'Audit Event' policy type allows administrators to collect logs from audit events at the endpoints. The audit event logs are available by default in Windows and Linux systems and this type of policy does not require any additional configuration. The administrator can create a schedule to collects logs and define a blackout period during which the agent will not collect logs. The newly created policy can then be deployed onto the agents installed in the customer's endpoints. Refer to the section '**Configuring Log Collection Policies**' for more details.

To create an audit policy

- Open the Collection Policies interface by clicking the 'Navigational Menu' button from the top right, choosing 'Agents' from the options and then clicking 'Collection Policies'.
- Click the 'Add' button at the bottom of the 'Collection Policies' screen at the left.

The configuration screen for creating a new policy will be displayed.



Agents > Collection Policies

Policy List

| Policy Name | Policy Type | Creation Time | Agents Count |
|---|---|---|---|
| CES | flat-file | 4/28/15 5:02 PM | 1 |
| CESLog248 | flat-file | 6/1/15 1:00 PM | 1 |

Agents > Collection Policies

Policy Type: flat-file Policy Name:

Description

Flat-File policy t... to track and send a specific file from the agent'...

The location of the file can be set by setting **source file path**.

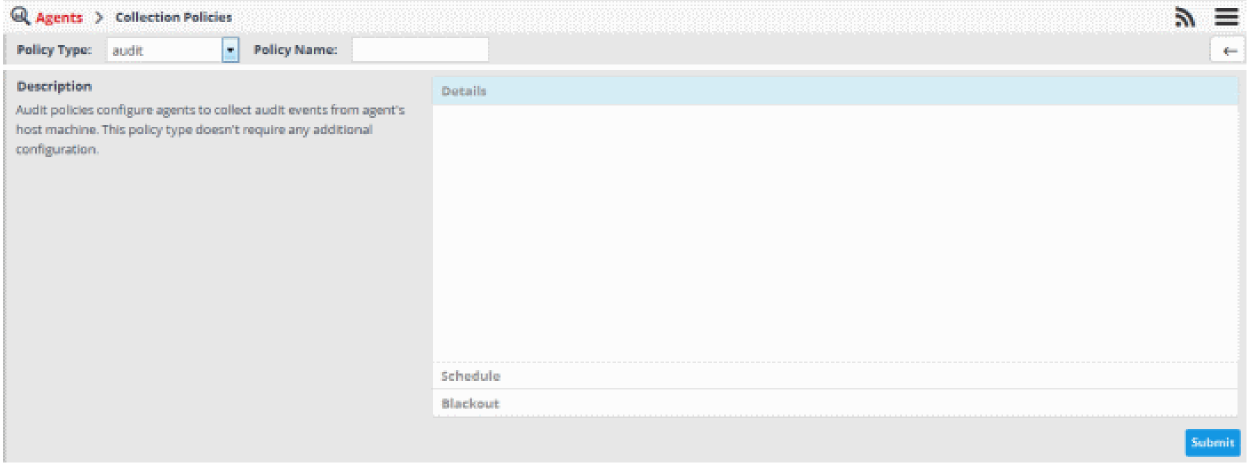
**Event group** helps to select what type of device is generating the log, and the specific de...

Details

Source File Path

- Choose 'Audit' from the 'Policy Type' drop-down.

The configuration screen for Audit Policy will be displayed.



Agents > Collection Policies

Policy Type: audit Policy Name:

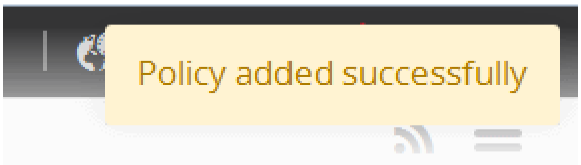
Description

Audit policies configure agents to collect audit events from agent's host machine. This policy type doesn't require any additional configuration.

- Enter a name for the new policy in the 'Policy Name' field at the top.

The Audit policy does not require any additional configuration as it instructs the agent to collect logs from audit events and is to be always ON. Hence the configuration area at the right is disabled for this policy type.

- Click the 'Submit' button to save your changes.



Policy added successfully

The policy will be added to NxSIEM and will be available for deployment to endpoints. Refer to the section '**Configuring Log Collection Policies**' for more details on deploying the newly created policy onto customer's endpoints.

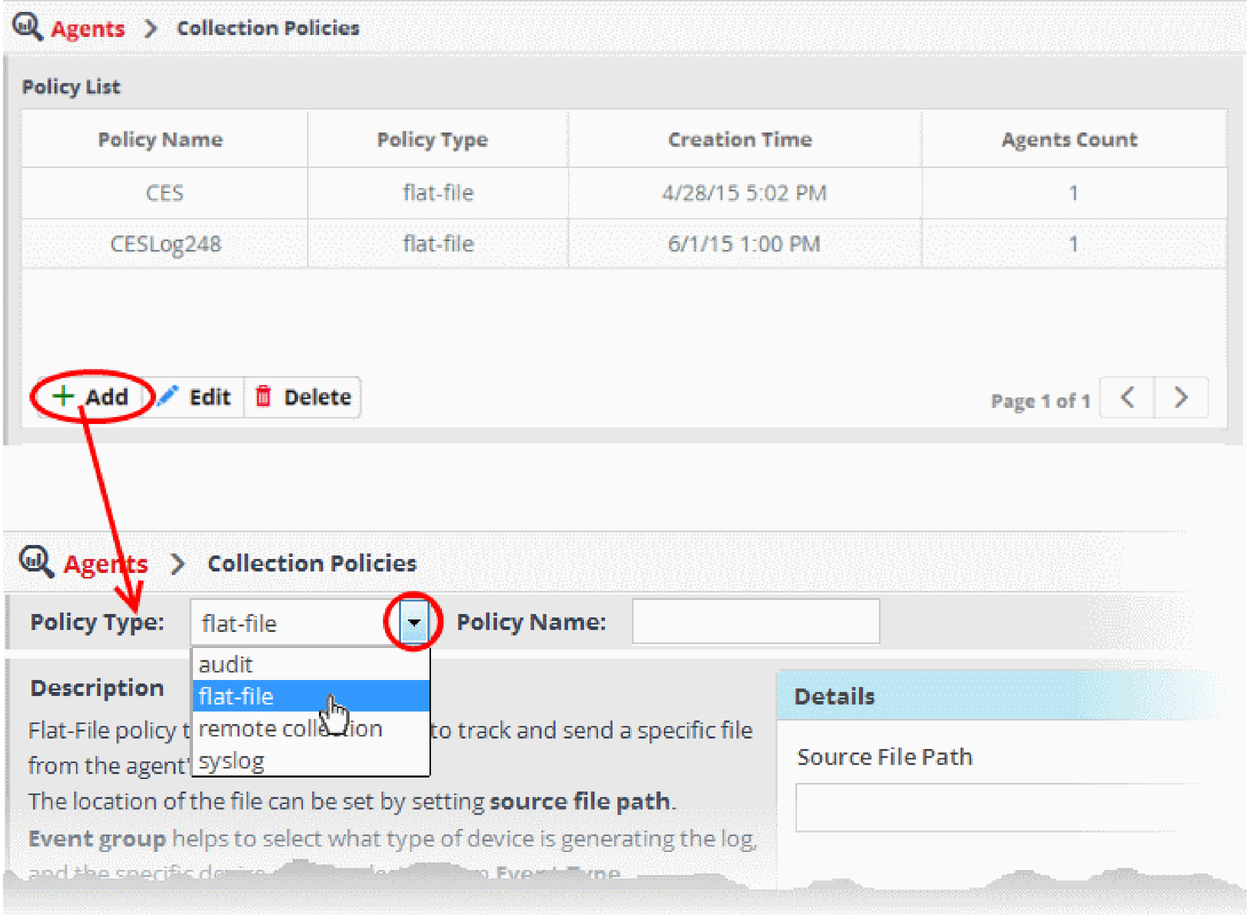
## 5.2.2 Flat File Policy

The 'Flat-File' policy type allows administrators to configure the agents to track and collect a specific log file from the endpoint at which it is installed. The administrator can define the path of the file in the 'Details' section, create a schedule to collect the file and define a blackout period during which the agent will not collect logs. The newly created policy can then be deployed onto required agents.

**To create a flat file policy**

- Open the Collection Policies interface by clicking the 'Navigational Menu' button from the top right, choosing 'Agents' from the options and then clicking 'Collection Policies'.
- Click the 'Add' button at the bottom of the 'Collection Policies' screen at the left.

The configuration screen for creating a new policy will be displayed.



| Policy Name | Policy Type | Creation Time | Agents Count |
|---|---|---|---|
| CES | flat-file | 4/28/15 5:02 PM | 1 |
| CESLog248 | flat-file | 6/1/15 1:00 PM | 1 |

Policy Type: flat-file

Policy Name:

Flat-File policy t to track and send a specific file from the agent'

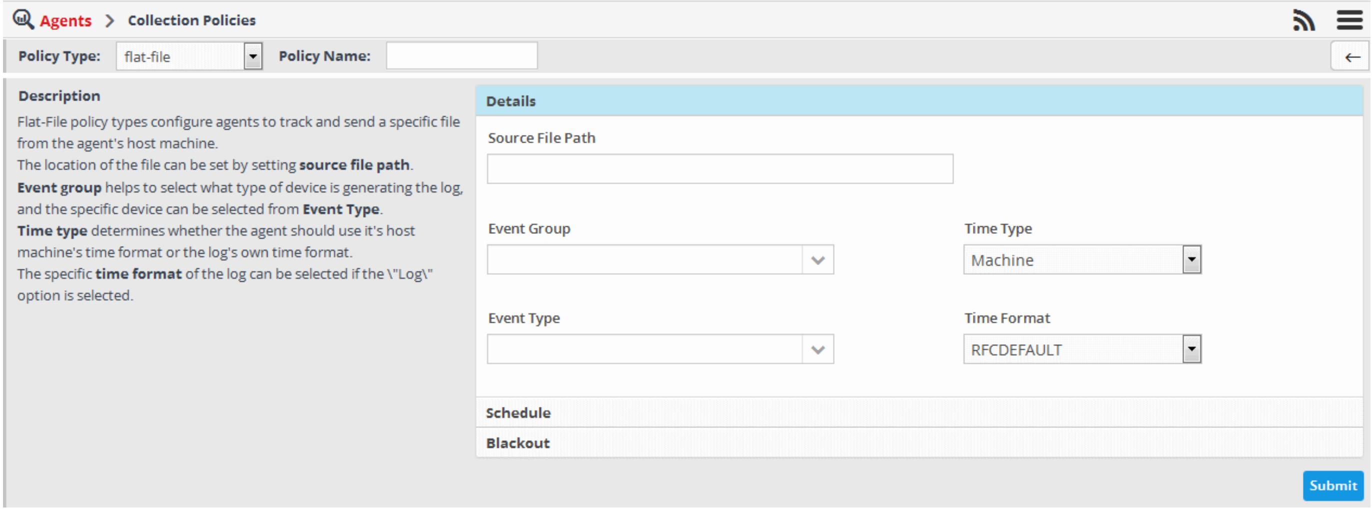
The location of the file can be set by setting **source file path**.

**Event group** helps to select what type of device is generating the log,

Source File Path:

By default, the screen to create a Flat-File policy type will be displayed.

- To return to flat-file policy type from a different configuration screen, choose 'flat-file' from the 'Policy Type' drop-down.



Policy Type: flat-file
Policy Name:

**Description**

Flat-File policy types configure agents to track and send a specific file from the agent's host machine.
The location of the file can be set by setting **source file path**.
**Event group** helps to select what type of device is generating the log, and the specific device can be selected from **Event Type**.
**Time type** determines whether the agent should use it's host machine's time format or the log's own time format.
The specific **time format** of the log can be selected if the \"Log\" option is selected.

**Details**

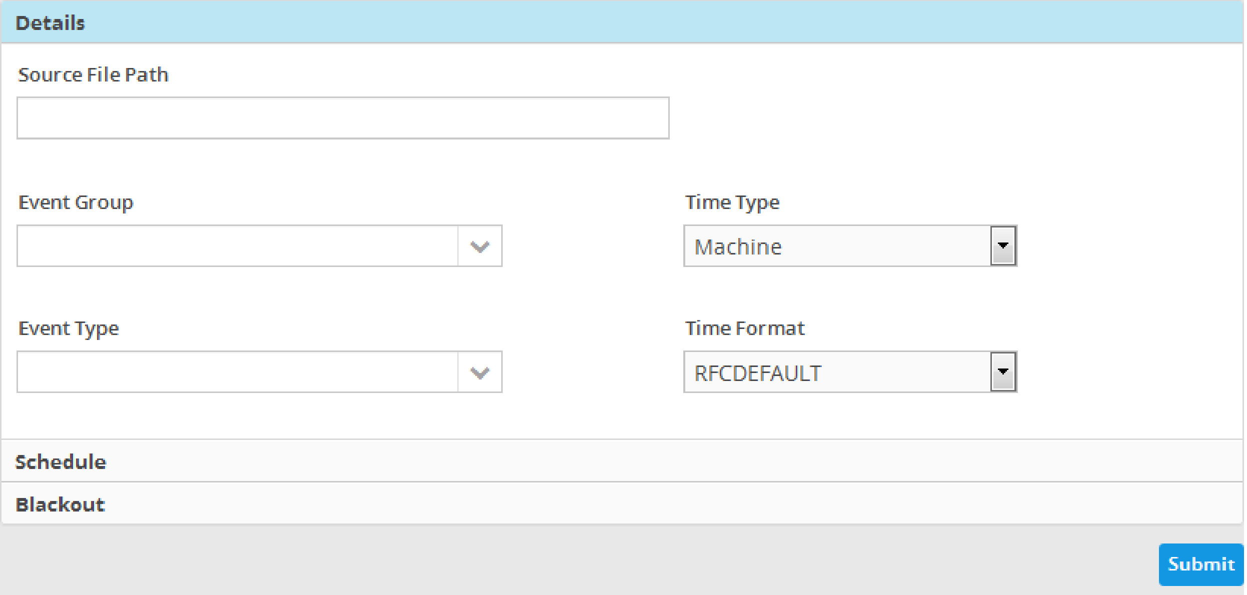
Source File Path:
Event Group:
Time Type: Machine
Event Type:
Time Format: RFCDEFAULT

- Enter a name for the new policy in the 'Policy Name' field

Next you need to configure the details defining the source of log collection, schedule and blackout period of log collection.

**To configure the details for the new policy**

- Click the 'Details' stripe



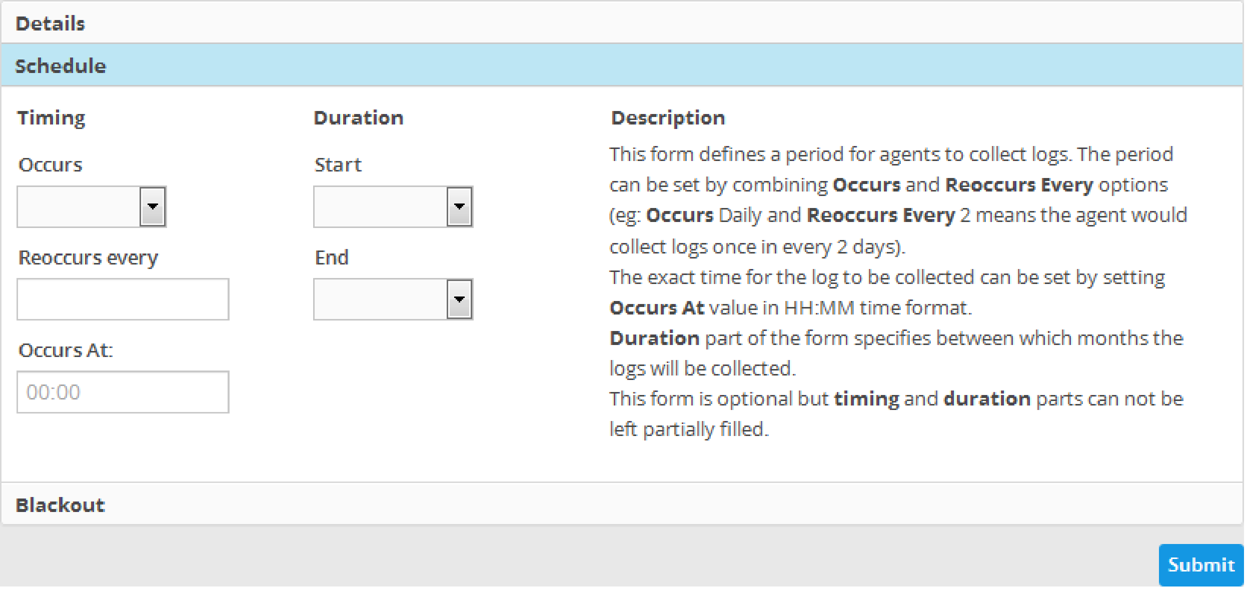
**Details**

Source File Path:
Event Group:
Time Type: Machine
Event Type:
Time Format: RFCDEFAULT

- Source File Patch - Enter the location of the log file in the endpoint that the agent should collect and forward to NxSIEM server
- Event Group: Select the 'Event Group' for which the log should be collected. The options available are:
  - Firewall and UTM
  - Application
  - Endpoint Security
  - Data Protection
  - Network Intrusion Detection & Protection
  - Network Monitoring
- Event Type - Choose the product for which the logs are to be collected, based on the chosen event group.
- Time Type - Select the time stamp that the agent should use for the logs, whether to use host machine's time stamp or the log's own time stamp
- Time Format - Select the time format to be used, from the drop-down.

**To create a schedule**

- Click the 'Schedule' stripe



**Description**

This form defines a period for agents to collect logs. The period can be set by combining **Occurs** and **Reoccurs Every** options (eg: **Occurs** Daily and **Reoccurs Every** 2 means the agent would collect logs once in every 2 days).
The exact time for the log to be collected can be set by setting **Occurs At** value in HH:MM time format.
**Duration** part of the form specifies between which months the logs will be collected.
This form is optional but **timing** and **duration** parts can not be left partially filled.

The 'Timing' section allows you to define the period for log collection.

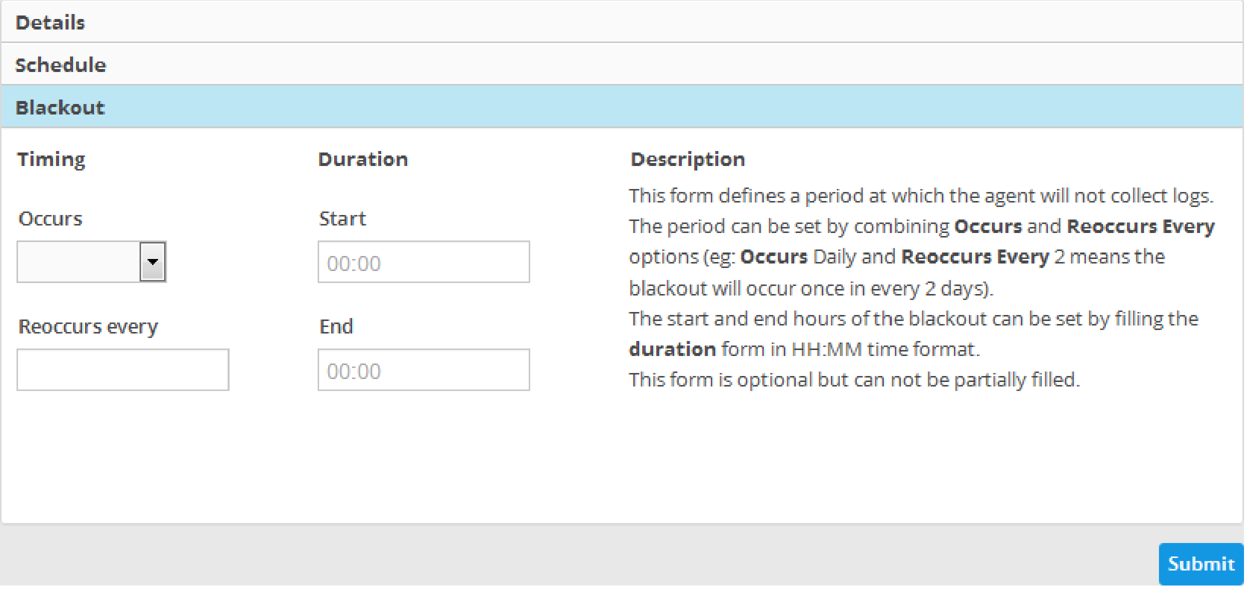
- **Occurs** - Select the period for log collection from the drop-down. The options available are:
  - Hourly
  - Daily
  - Weekdays
  - Weekend
  - Weekly
  - Monthly
- **Reoccurs every** - Enter the frequency for log collection at the chosen days. For example, if you select 'Daily' and enter 2, then the agent will collect the logs once in every 2 days
- **Occurs At** - Enter the exact time at which the log should be collected

The 'Duration' section allows you to define the start and end months for the period of log collection.

- **Start -** Select the start month from the drop-down
- **End -** Select the end month from the drop-down

**To configure a blackout period**

- Click the 'Blackout' stripe



**Description**

This form defines a period at which the agent will not collect logs. The period can be set by combining **Occurs** and **Reoccurs Every** options (eg: **Occurs** Daily and **Reoccurs Every** 2 means the blackout will occur once in every 2 days).
The start and end hours of the blackout can be set by filling the **duration** form in HH:MM time format.
This form is optional but can not be partially filled.

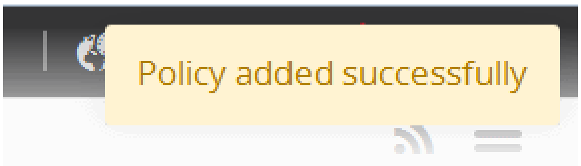
The 'Timing' section allows you to define the blackout period.

- **Occurs -** Select the period for blackout from the drop-down. The options available are:
  - Daily
  - Weekdays
  - Weekend
  - Weekly
  - Monthly
- **Reoccurs every -** Enter the frequency for blackout period. For example, if you choose daily and enter 2, then the blackout will occur once in every 2 days

The 'Duration' section allows you to define the start and end time for blackout duration within the chosen period.

- **Start -** Enter the start time for the blackout duration
- **End -** Enter the end time for the blackout duration

- Click the 'Submit' button to save your changes.



Policy added successfully

The policy will be added to NxSIEM and will be available for deployment to endpoints. Refer to the section '**Configuring Log Collection Policies**' for more details on deploying the newly created policy onto customer's endpoints.

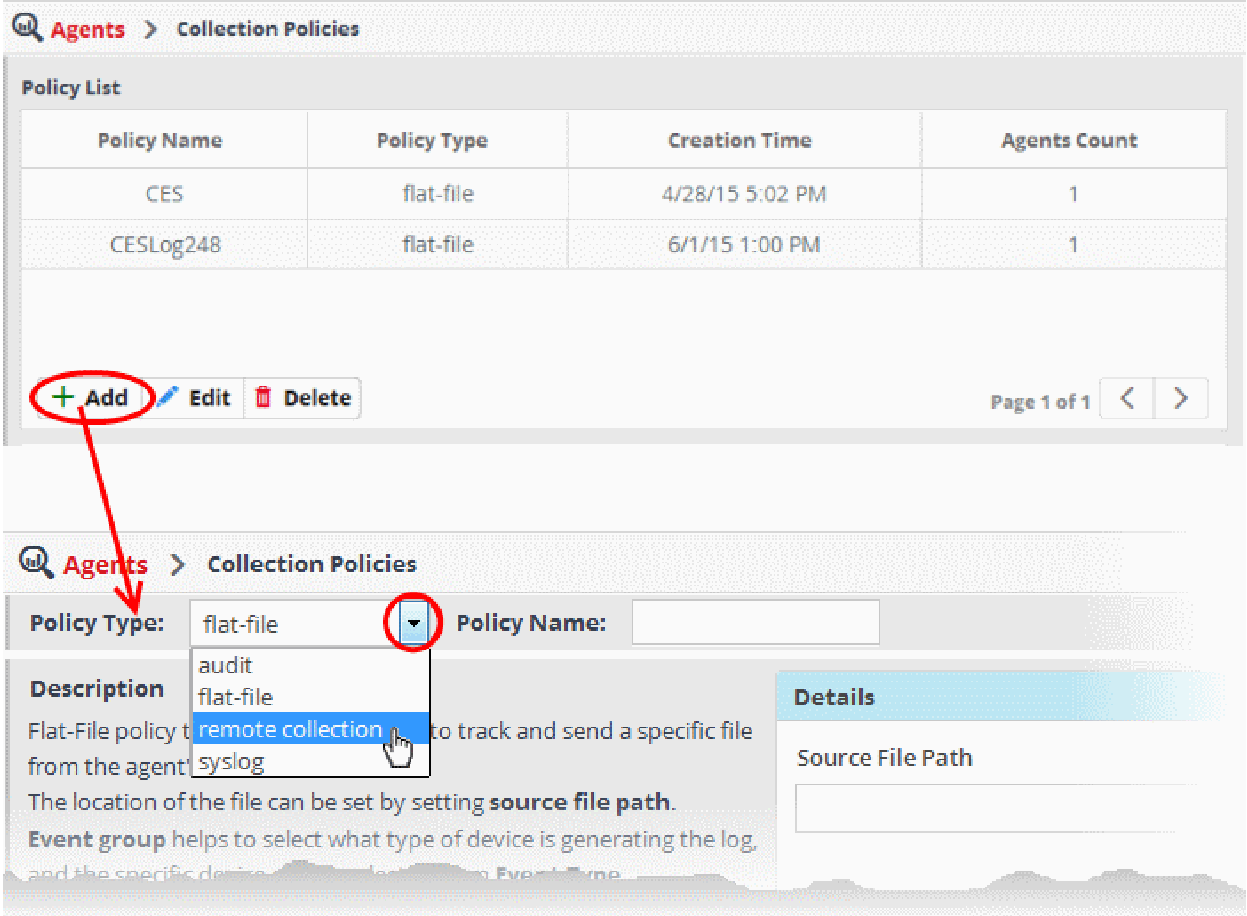
### 5.2.3 Remote Log Collection Policy

The 'Remote Collection' policy is similar to the '**Flat-File**' policy except this is configured to collect logs from an endpoint with no agent installed, using agent installed on another endpoint. Additional information required for this policy includes IP or domain address of the endpoint from which the logs are to be collected, username and password to access the log and connection protocol. The administrator can create a schedule to collects the logs.

**To create a remote log collection policy**

- Open the Collection Policies interface by clicking the 'Navigational Menu' button from the top right, choosing 'Agents' from the options and then clicking 'Collection Policies'.
- Click the 'Add' button at the bottom of the 'Collection Policies' screen at the left.

The configuration screen for creating a new policy will be displayed.



Policy List

| Policy Name | Policy Type | Creation Time | Agents Count |
|---|---|---|---|
| CES | flat-file | 4/28/15 5:02 PM | 1 |
| CESLog248 | flat-file | 6/1/15 1:00 PM | 1 |

Policy Type: flat-file Policy Name:

**Description**

Flat-File policy t ... to track and send a specific file from the agent'

The location of the file can be set by setting **source file path**.

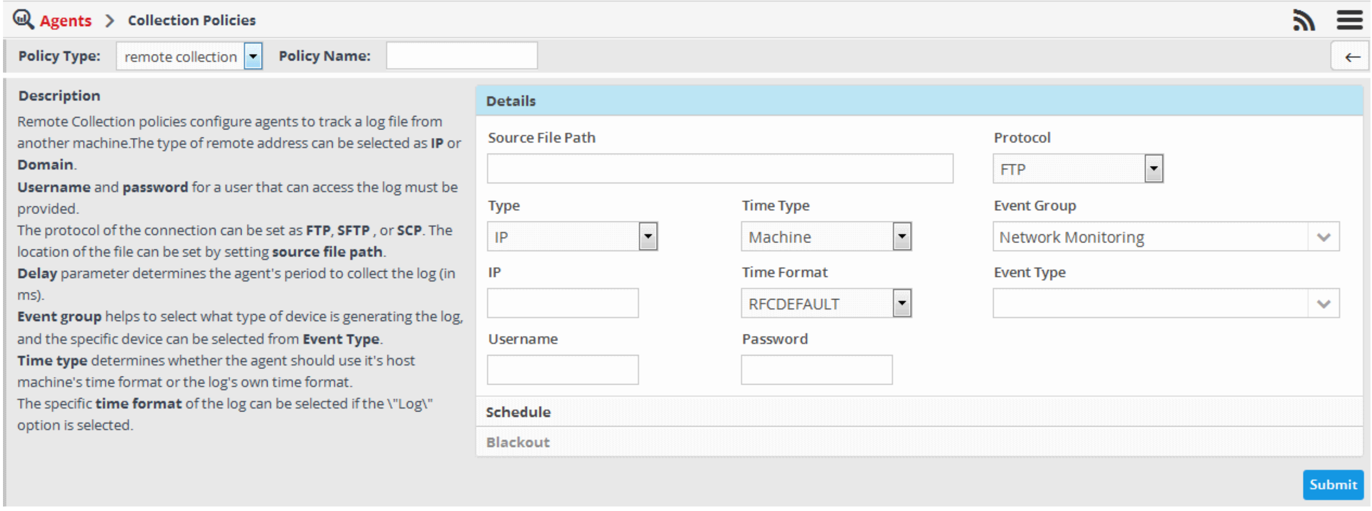
**Event group** helps to select what type of device is generating the log,

**Details**

Source File Path

- Choose 'remote collection' from the 'Policy Type' drop-down.

The configuration screen for remote collection policy will be displayed.



Policy Type: remote collection Policy Name:

**Description**

Remote Collection policies configure agents to track a log file from another machine.The type of remote address can be selected as **IP** or **Domain**.

**Username** and **password** for a user that can access the log must be provided.

The protocol of the connection can be set as **FTP**, **SFTP** , or **SCP**. The location of the file can be set by setting **source file path**.

**Delay** parameter determines the agent's period to collect the log (in ms).

**Event group** helps to select what type of device is generating the log, and the specific device can be selected from **Event Type**.

**Time type** determines whether the agent should use it's host machine's time format or the log's own time format.

The specific **time format** of the log can be selected if the \"Log\" option is selected.

**Details**

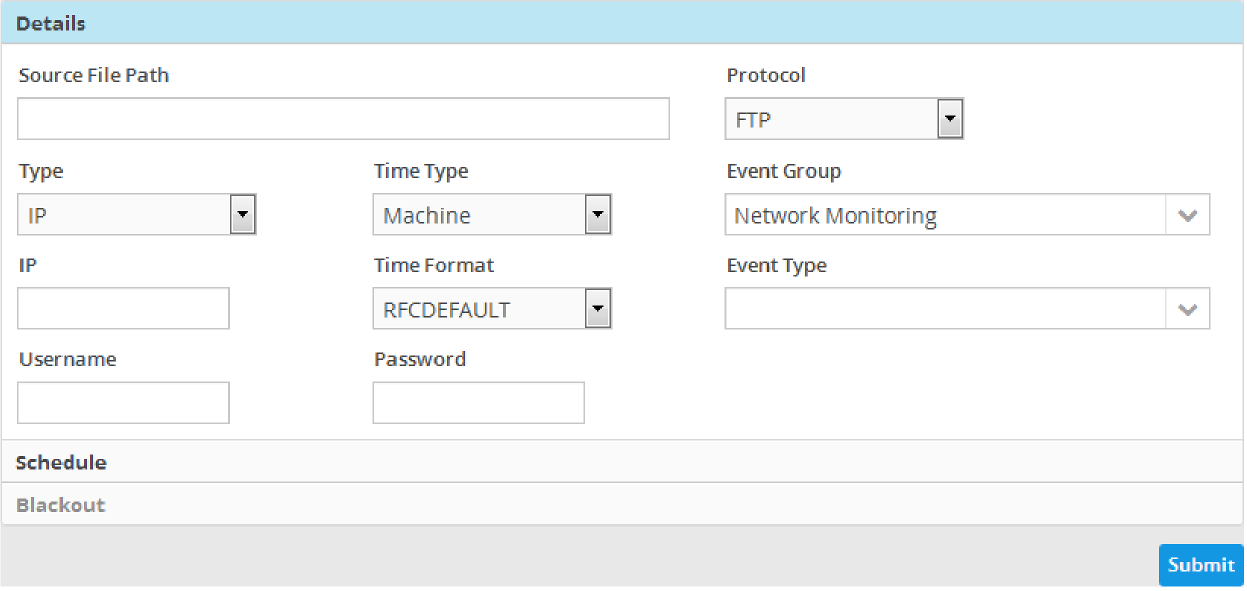
| | | |
|---|---|---|
| Source File Path: | | Protocol: FTP |
| Type: IP | Time Type: Machine | Event Group: Network Monitoring |
| IP: | Time Format: RFCDEFAULT | Event Type: |
| Username: | Password: | |

- Enter a name for the new policy in the 'Policy Name' field

Next you need to configure the details defining the source of log collection and the schedule for log collection.

**To configure the details for the new policy**

- Click the 'Details' stripe



Details

Source File Path:

Protocol: FTP

Type: IP

Time Type: Machine

Event Group: Network Monitoring

IP:

Time Format: RFCDEFAULT

Event Type:

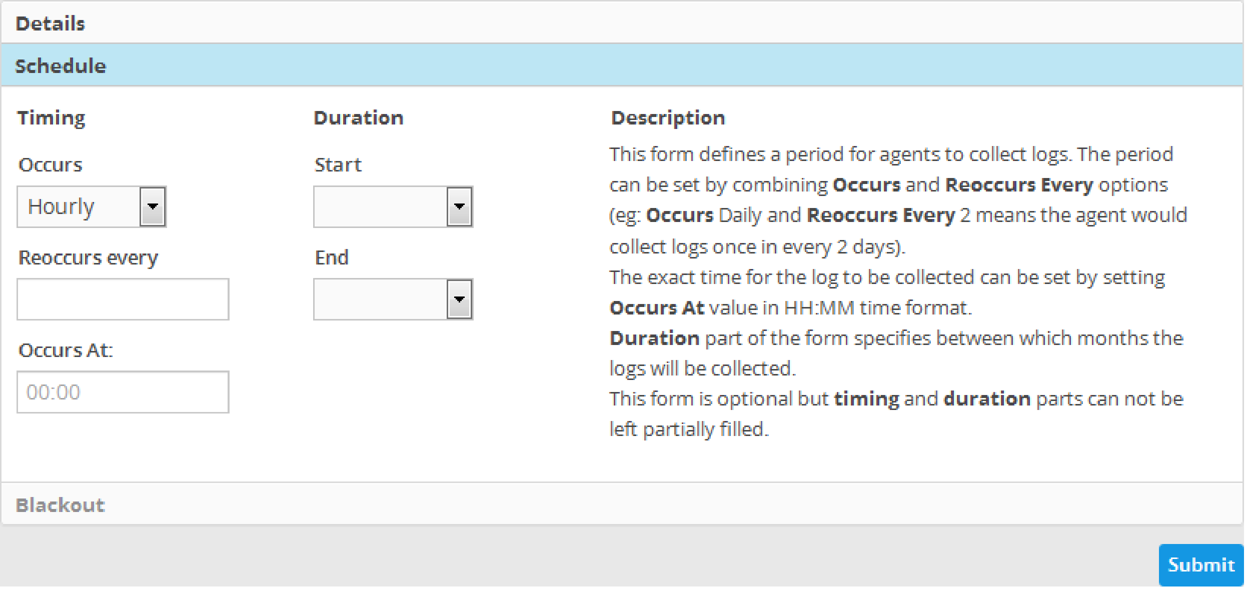
Username:

Password:

- **Source File Patch** - Enter the location of the log file in the remote endpoint that the agent from another endpoint should collect and forward to NxSIEM server.
- **Type -** Select the type of address to be entered for the remote endpoint. The options available are 'IP' and 'Domain'. Enter the address of the remote endpoint as per the chosen type in the field that appears below the 'Type' field.
- **Time Type** - Select the time stamp that the agent should use for the logs, whether to use host machine's time stamp or the log's own time stamp
- **Time Format -** Select the time format to be used, from the drop-down.
- **Time Type -** Select the time stamp that the agent should use for the logs. The optiion avawhether host machine's time stamp or the log's own time stamp.
- **Username -** Enter the username of an administrative account for the agent to log-in to the remote endpoint, in order to access the log files.
- **Password -** Enter the password for the administrative account.
- **Protocol -** Select the type of protocol to be used for the agent to connect to the remote endpoint to collect the logs.
- **Event Group** - Select the 'Event Group' for which the log should be collected. The options available are:
  - Firewall and UTM
  - Application
  - Endpoint Security
  - Data Protection
  - Network Intrusion Detection & Protection
  - Network Monitoring
- **Event Type** - Choose the product for which the logs are to be collected, based on the chosen event group.

**To create a schedule**

- Click the 'Schedule' stripe



**Description**

This form defines a period for agents to collect logs. The period can be set by combining **Occurs** and **Reoccurs Every** options (eg: **Occurs** Daily and **Reoccurs Every** 2 means the agent would collect logs once in every 2 days).
The exact time for the log to be collected can be set by setting **Occurs At** value in HH:MM time format.
**Duration** part of the form specifies between which months the logs will be collected.
This form is optional but **timing** and **duration** parts can not be left partially filled.

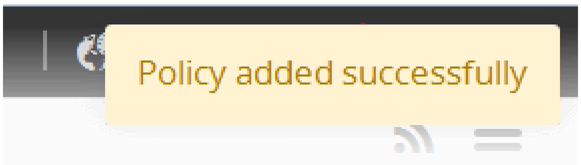
The 'Timing' section allows you to define the period for log collection.

- **Occurs** - Select the period for log collection from the drop-down. The options available are:
  - Hourly
  - Daily
  - Weekdays
  - Weekend
  - Weekly
  - Monthly
- **Reoccurs every** - Enter the frequency for log collection at 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 log should be collected

The 'Duration' section allows you to define the start and end months for the period of log collection.

- **Start -** Select the start month from the drop-down
- **End -** Select the end month from the drop-down

- Click the 'Submit' button to save your changes.



Policy added successfully

The policy will be added to NxSIEM and will be available for deployment to endpoints. Refer to the section '**Configuring Log Collection Policies**' for more details on deploying the newly created policy onto customer's endpoints.

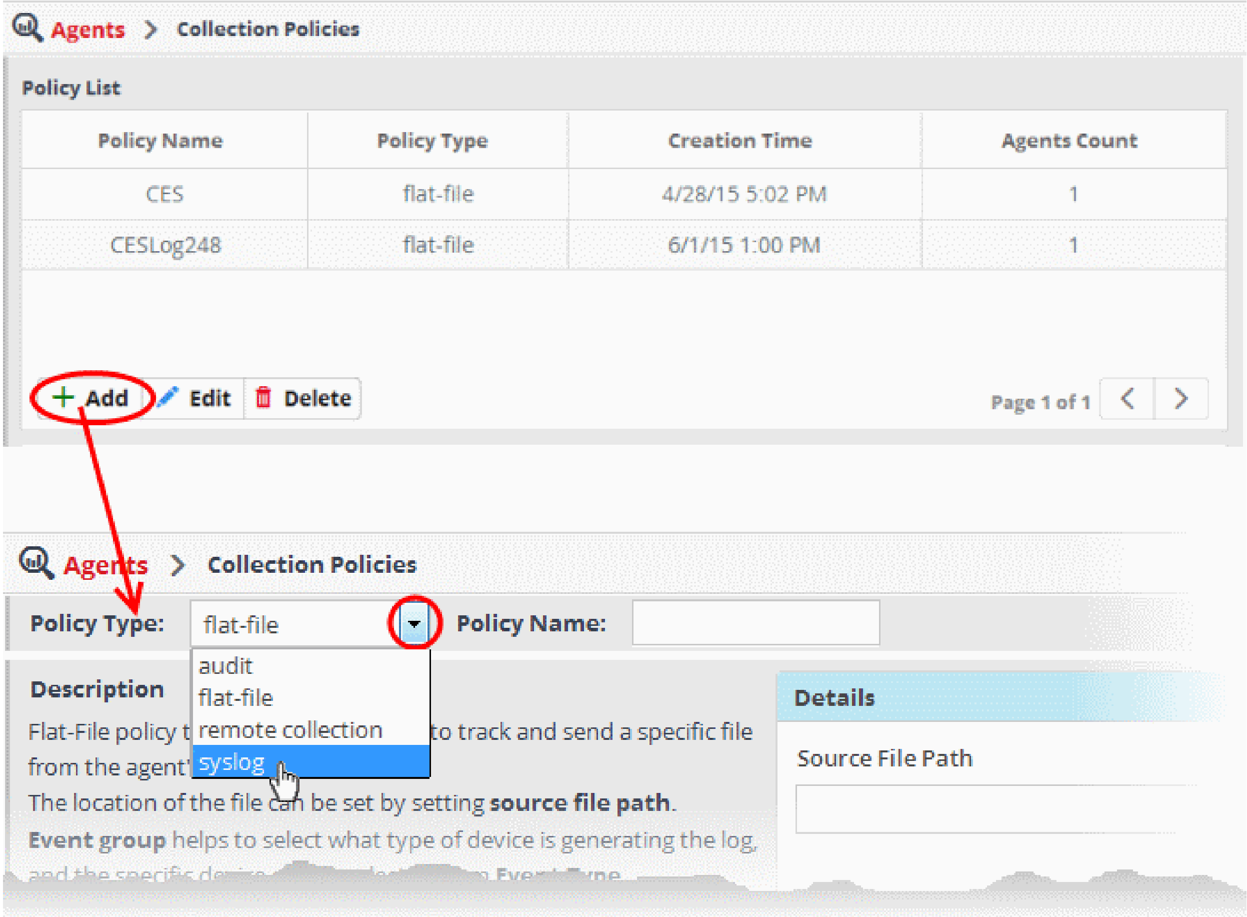
### 5.2.4 Syslog Policy

The 'Syslog' policy allows administrators to configure the agent installed on one endpoint to listen to a specified port of remote endpoints with no agent installed, in order to collect the logs from them, for example from a Syslog server, Linux servers and Windows servers that use syslog protocol in order to collect the logs. Please note that these systems must be configured to send logs from syslog to the endpoint on which the agent is installed. Multiple remote endpoints can be added for a single policy and each endpoint can be configured to provide log pertaining to specific events. No schedule and blackout options are available for this type of policy.

**To create a syslog policy**

- Open the Collection Policies interface by clicking the 'Navigational Menu' button from the top right, choosing 'Agents' from the options and then clicking 'Collection Policies'.
- Click the 'Add' button at the bottom of the 'Collection Policies' screen at the left.

The configuration screen for creating a new policy will be displayed.



| Policy Name | Policy Type | Creation Time | Agents Count |
|---|---|---|---|
| CES | flat-file | 4/28/15 5:02 PM | 1 |
| CESLog248 | flat-file | 6/1/15 1:00 PM | 1 |

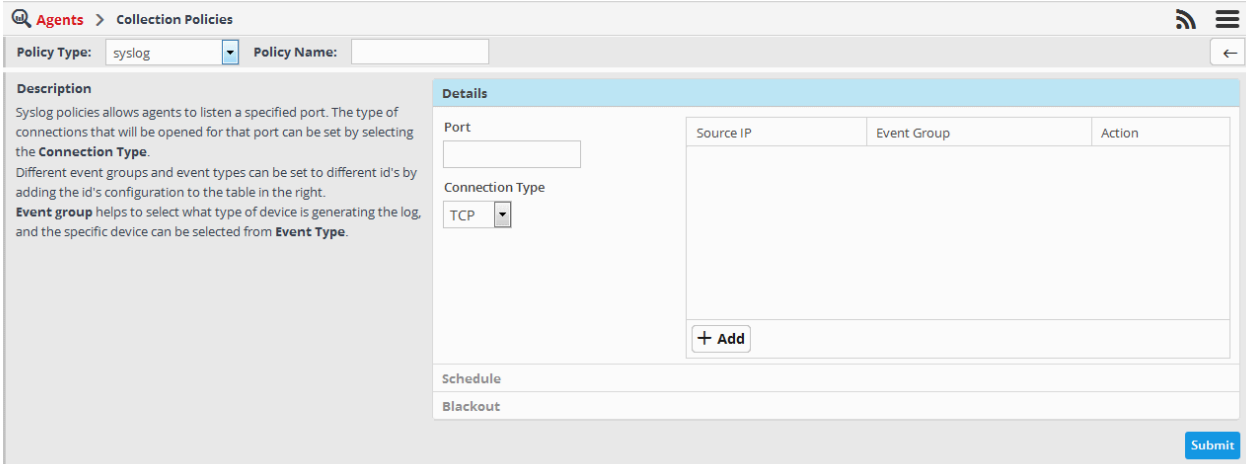
Policy Type: flat-file

Description

Flat-File policy t to track and send a specific file from the agent' The location of the file can be set by setting **source file path**. **Event group** helps to select what type of device is generating the log,

- Choose 'syslog' from the 'Policy Type' drop-down.

The configuration screen for syslog policy will be displayed.



Policy Type: syslog

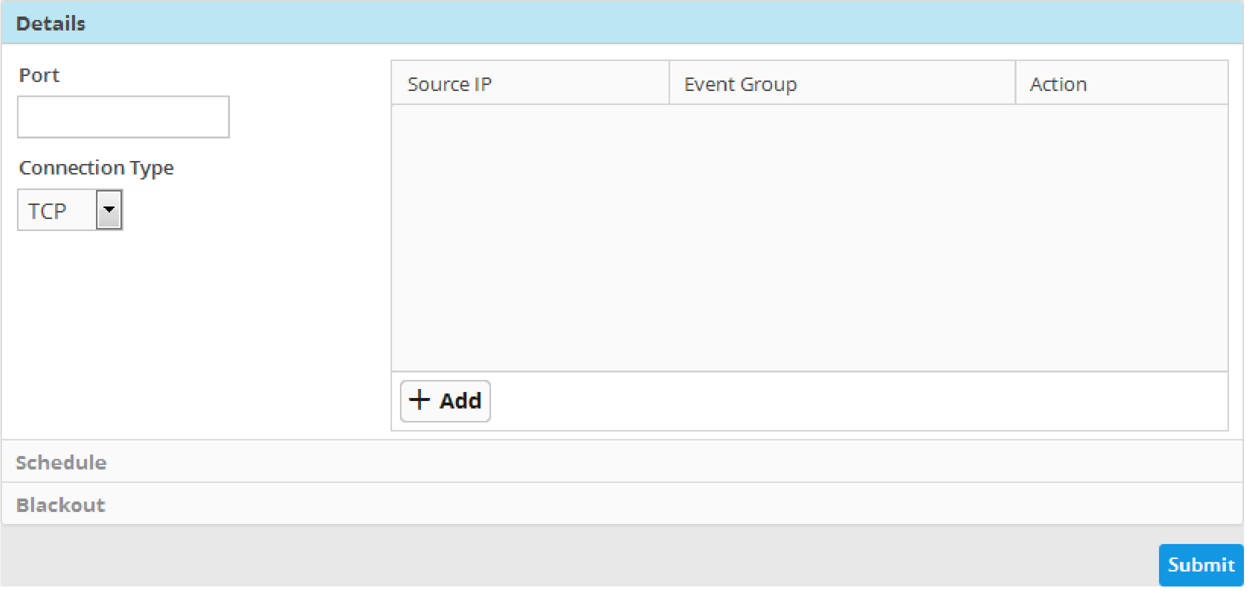
Connection Type: TCP

Description

Syslog policies allows agents to listen a specified port. The type of connections that will be opened for that port can be set by selecting the **Connection Type**.
Different event groups and event types can be set to different id's by adding the id's configuration to the table in the right.
**Event group** helps to select what type of device is generating the log, and the specific device can be selected from **Event Type**.

- Enter a name for the new policy in the 'Policy Name' field

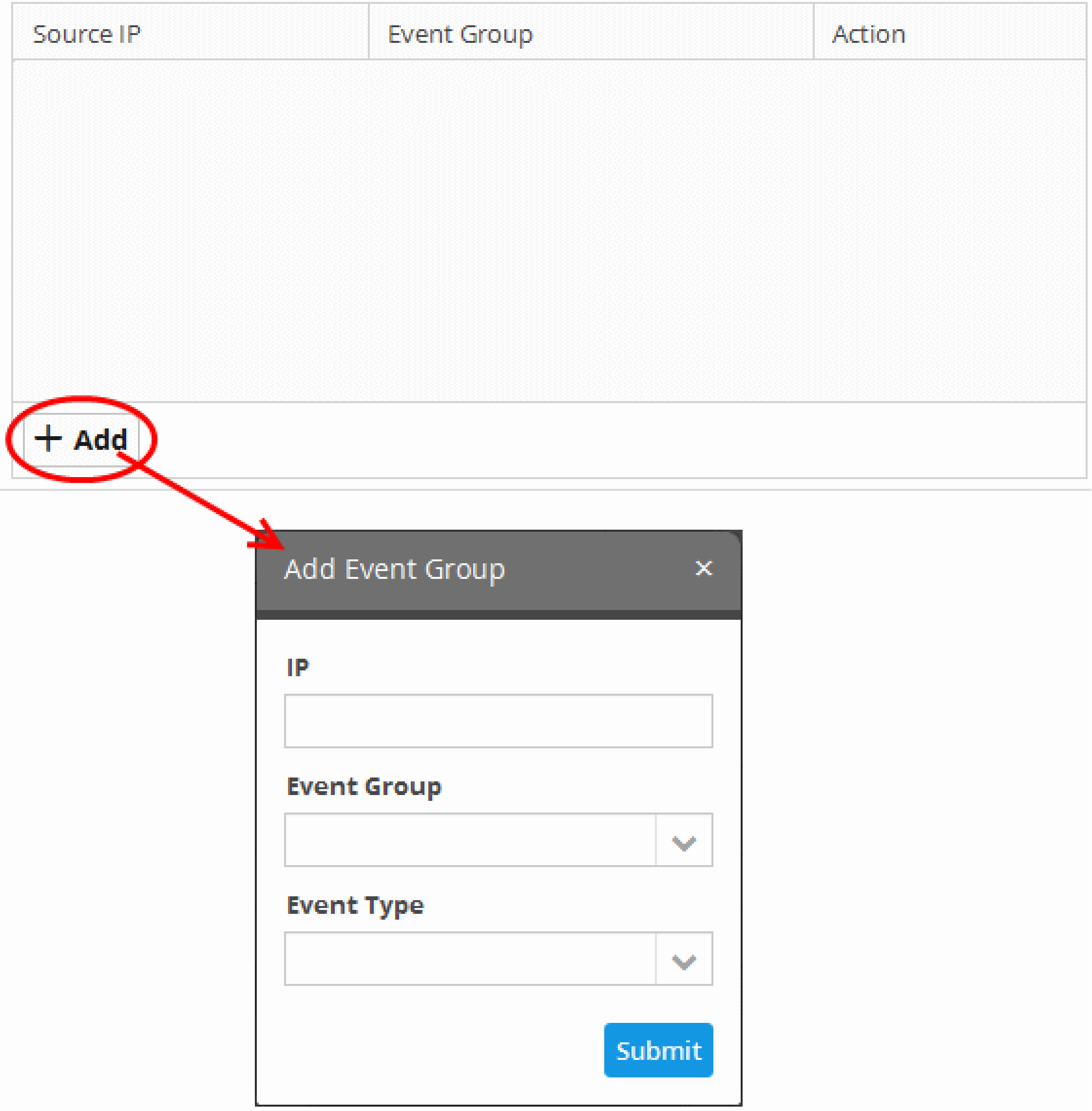
Next you need to configure the details defining the source of log collection.



- **Port** - Specify the port number which will be used by the agent in one endpoint to connect to the remote endpoint(s).
- **Connection Type** - Select the type of connection protocol to be used for the agent to connect to the remote endpoint to collect the logs from the drop-down. The options available are TCP, UDP and BOTH.

**Note**: The port number and the connection type should match with the syslog connection configuration made at the remote endpoints.

- Click the 'Add' button at the bottom end of the list of remote endpoints. to add the endpoints from which the logs should be fetched.

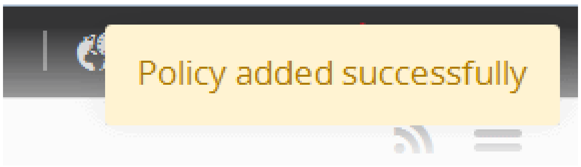


- **IP** - Enter the IP address of the remote endpoint.
- **Event Group** - Select the 'Event Group' for which the log should be collected. The options available are:
  - Firewall and UTM
  - Application
  - Endpoint Security
  - Data Protection
  - Network Intrusion Detection & Protection
  - Network Monitoring
- **Event Type** - Choose the product for which the logs are to be collected, based on the chosen event group.

- Click the 'Submit' button in the 'Add Event Group' dialog.

The remote endpoint will be added to the policy.

- Repeat the process to add more number of remote endpoints.
- Click the 'Submit' button to save your changes.

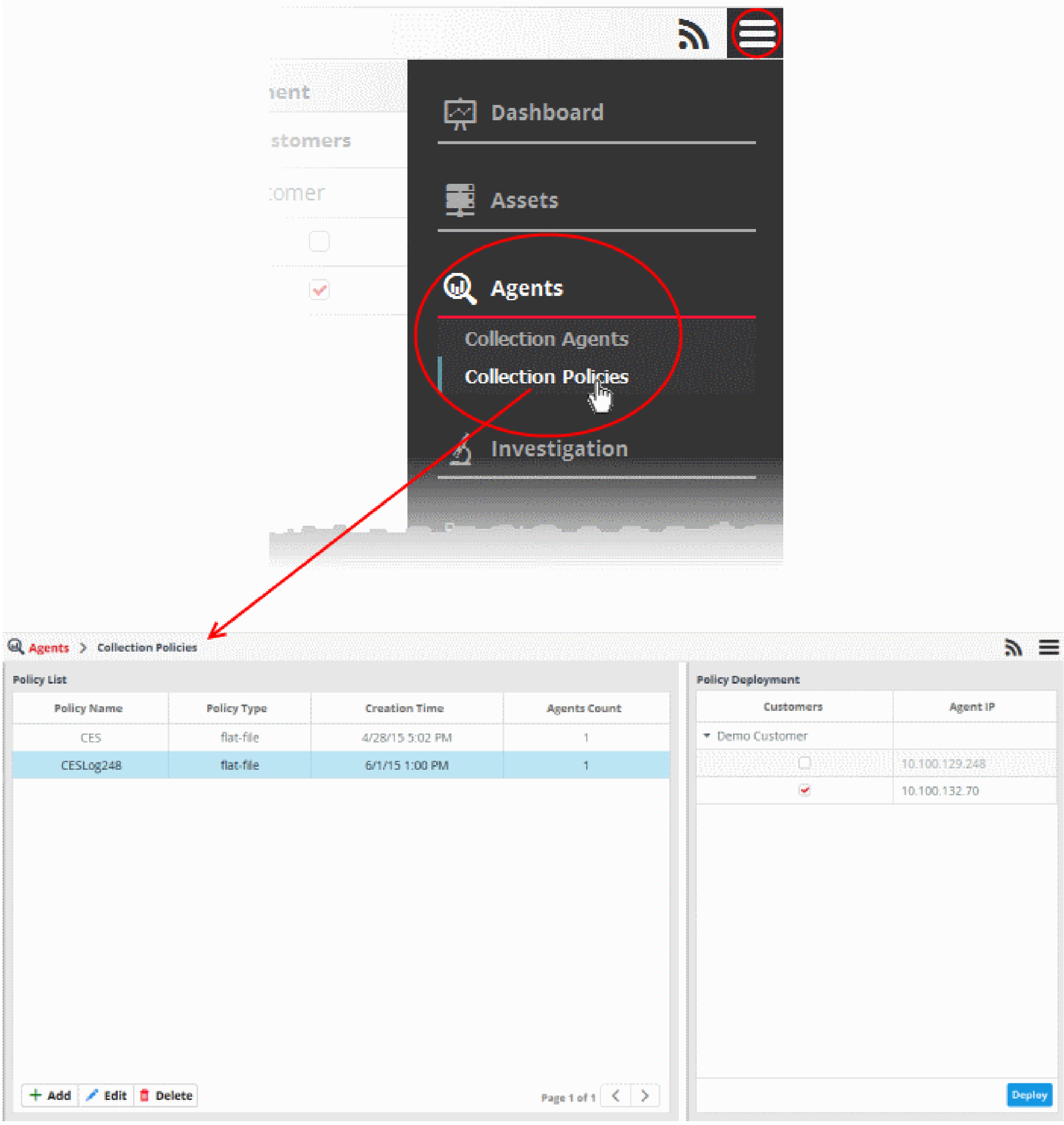

Policy added successfully

The policy will be added to NxSIEM and will be available for deployment to endpoints. Refer to the section '**Configuring Log Collection Policies**' for more details on deploying the newly created policy onto customer's endpoints.

## 5.2.5 Configuring Log Collection Policies

The Collection Policies interface displays the list of policies added to NxSIEM and allows the administrator to deploy them to the agents installed on endpoints in customers' networks as required.

To open the 'Collection Policies' screen, click the 'Menu' button from the top right , choose 'Agents' and then click 'Collection Policies'.



| Policy Name | Policy Type | Creation Time | Agents Count |
|---|---|---|---|
| CES | flat-file | 4/28/15 5:02 PM | 1 |
| CESLog248 | flat-file | 6/1/15 1:00 PM | 1 |

| Customers | Agent IP |
|---|---|
| ▾ Demo Customer | |
| □ | 10.100.129.248 |
| ☑ | 10.100.132.70 |

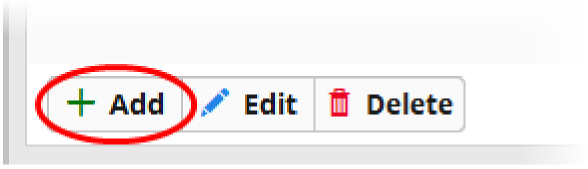
The interface allows the administrator to:

- **Add a new poliicies**
- **Edit a policy**
- **Delete a policy**

- Deploy a policy
- View policy deployment status

**To add a new policy**

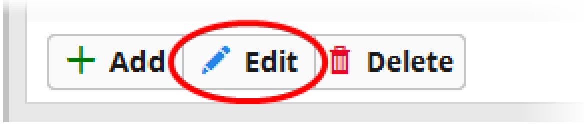
- Click the 'Add' button on the bottom of the screen.



Refer to the sections '**Audit Events Policy**', '**Flat File Policy**', '**Remote Log Collection Policy**' and '**Syslog Policy**' for details on adding different types of policies.

**To edit a policy**

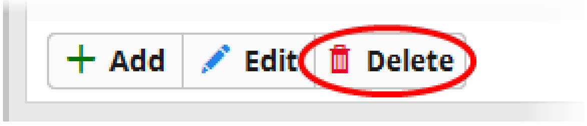
- Select the policy from the list that you want to edit and click the 'Edit' button at the bottom of the screen.



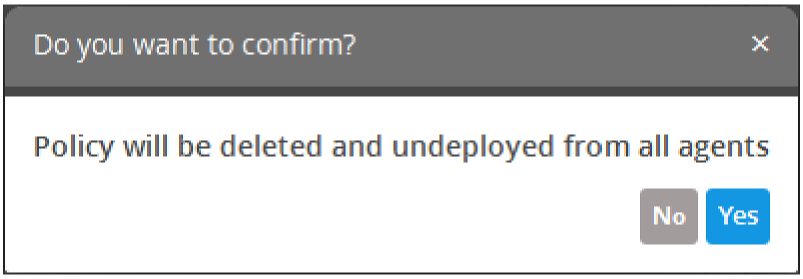
The configuration interface of the selected policy type will be displayed. Edit the details as required. The editing procedure is similar to adding a new policy process. Refer to the sections '**Audit Events Policy**', '**Flat File Policy**', '**Remote Log Collection Policy**' and '**Syslog Policy**' for more details.

**To delete a policy**

- Select the policy from the list that you want to remove and click the 'Delete' button at the bottom of the screen.



A confirmation dialog will appear.

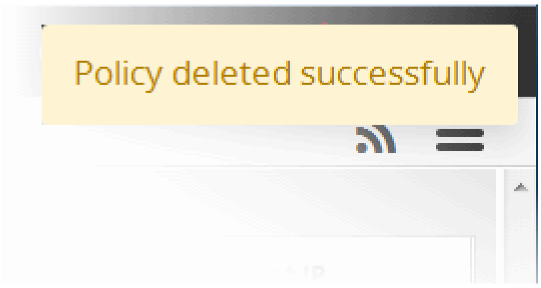


Do you want to confirm?

Policy will be deleted and undeployed from all agents

- Click 'Yes' to remove the policy.

If a policy is deleted it will be automatically removed from all the agents on which it was deployed.



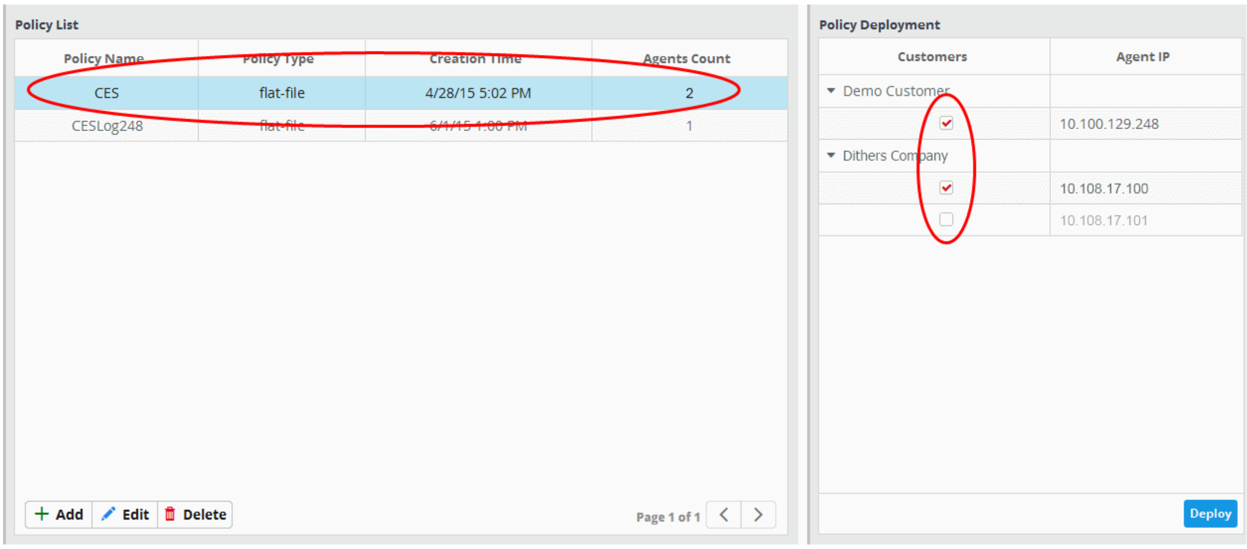
Policy deleted successfully

**To deploy a policy to an agent**

- Select the policy from the 'Policy List' pane at the right of the Collection Policies interface

The Policy Deployment pane at the right displays the list of all endpoints from all the customers. The endpoints on which the policy is already applied, are indicated with tick mark in the checkboxes beside them under each customer.

- To deploy the selected policy to a new endpoint, select the checkbox beside it under the respective customer name.
- To remove the policy from the endpoints de-select the checkboxes beside them under the respective customer name



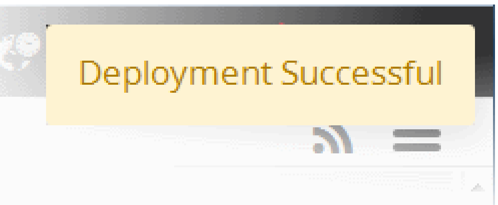
Policy List

| Policy Name | Policy Type | Creation Time | Agents Count |
|---|---|---|---|
| CES | flat-file | 4/28/15 5:02 PM | 2 |
| CESLog248 | flat-file | 6/1/15 1:00 PM | 1 |

Policy Deployment

| Customers | Agent IP |
|---|---|
| Demo Customer | |
| ☑ | 10.100.129.248 |
| Dithers Company | |
| ☑ | 10.108.17.100 |
| □ | 10.108.17.101 |

- Click the 'Deploy' button.

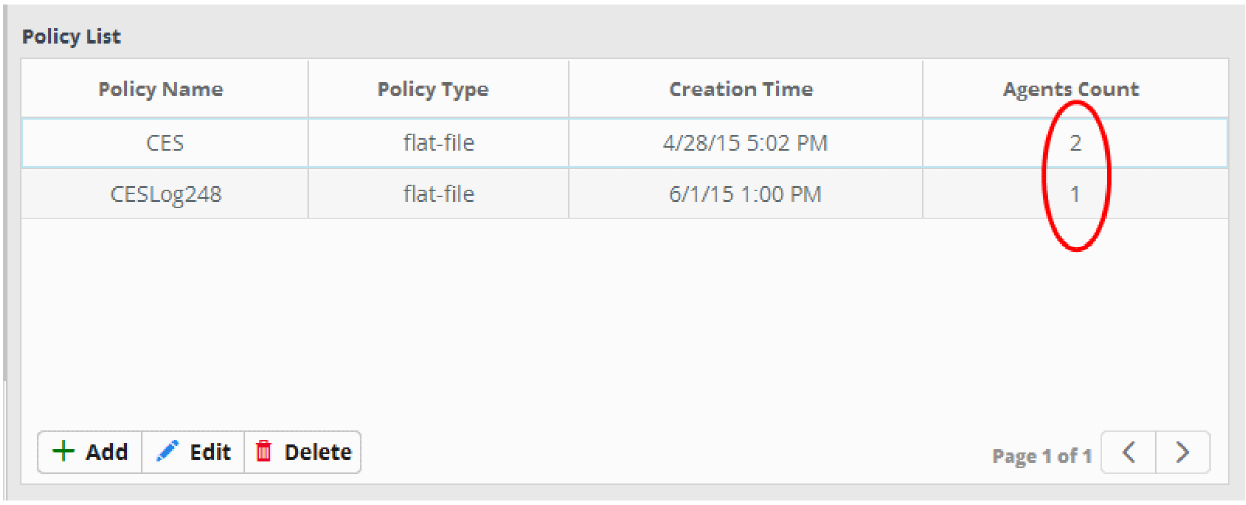


Deployment Successful

The 'Agents Count' column will also be updated and the number of agents on which the policy is deployed.

**To view policy deployment status**

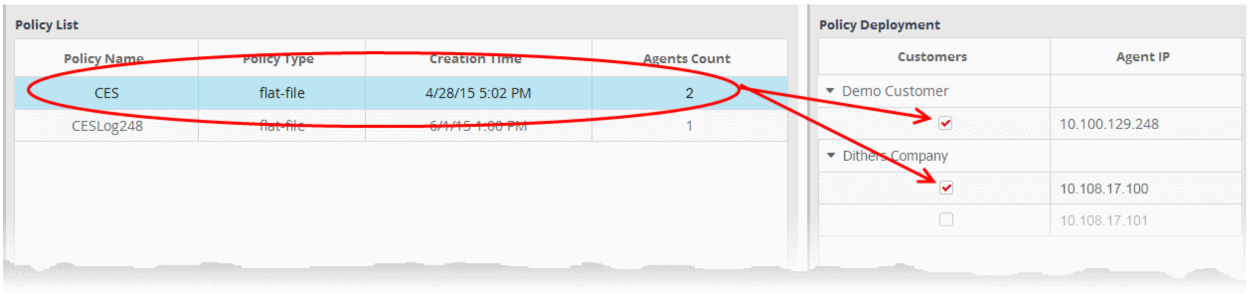
The 'Agent Count' column in the 'Policy List' section displays the number of systems onto which the policies are deployed.



Policy List

| Policy Name | Policy Type | Creation Time | Agents Count |
|---|---|---|---|
| CES | flat-file | 4/28/15 5:02 PM | 2 |
| CESLog248 | flat-file | 6/1/15 1:00 PM | 1 |

- Click on a policy to view the systems onto which they are deployed.



Policy List

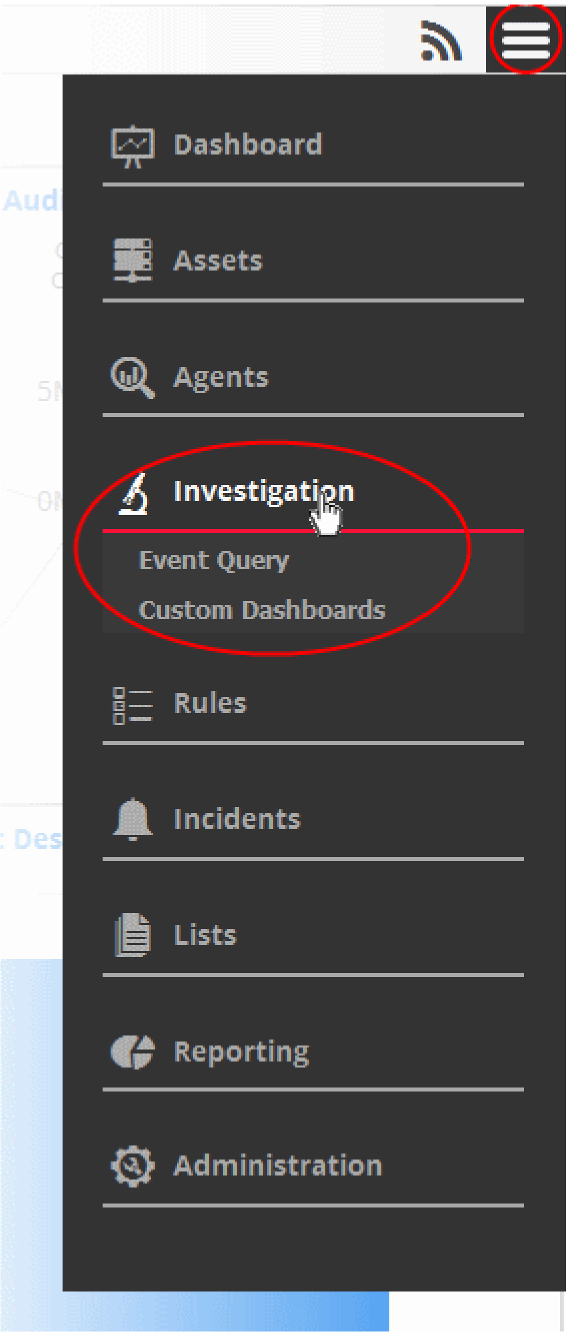
| Policy Name | Policy Type | Creation Time | Agents Count |
|---|---|---|---|
| CES | flat-file | 4/28/15 5:02 PM | 2 |
| CESLog248 | flat-file | 6/1/15 1:00 PM | 1 |

Policy Deployment

| Customers | Agent IP |
|---|---|
| ▾ Demo Customer | |
| ☑ | 10.100.129.248 |
| ▾ Dithers Company | |
| ☑ | 10.108.17.100 |
| □ | 10.108.17.101 |

# 6 Query Management

The administrator can query the logs database to search for logs corresponding to specific events from specific customers. The 'Investigation' feature allows the administrators to build queries for searching specific logs, for constructing correlation rules for identifying incidents and to create custom dashboards which display the resulting data as graphical charts. Comodo NxSIEM ships with a set of predefined queries for each customer and also allows you to add custom queries for customers according to your requirements.



Refer to the following sections for more details:

- Configuring Event Queries
- Configuring Custom Dashboards

## 6.1 Configuring Event Queries

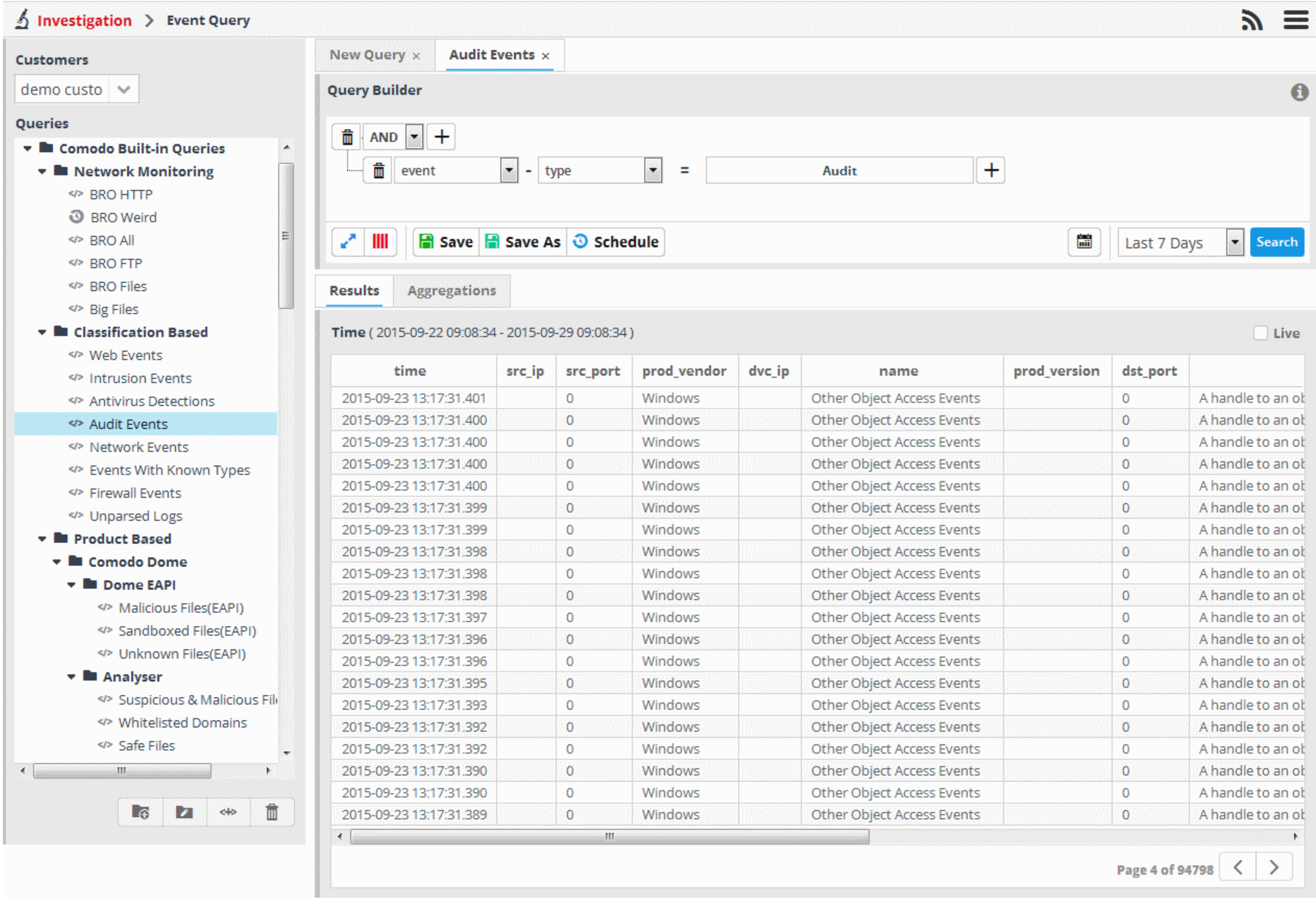
The 'Event Query' interface allows administrators to search for specific events using built-in queries. The administrator can also add custom 'Event Queries' according to specific requirements. You have to create conditions for a search and configure the results table accordingly to display the search results. Queries can be made to search for events that occurred during a specific time period in the selected customer's networks. The results table displays events which match the query with the fields specified for the results table as columns. The results table even allows you to perform an IP look up of external IP addresses involved in the event.

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

- Constructing custom dashboards which display query results as graphical charts. Refer to the section '**Configuring Custom Dashboard**' 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 section **Managing Rules** for more details.

To open the 'Event Query' interface, click the 'Menu' button at top right, choose 'Investigation' then 'Event Query'.

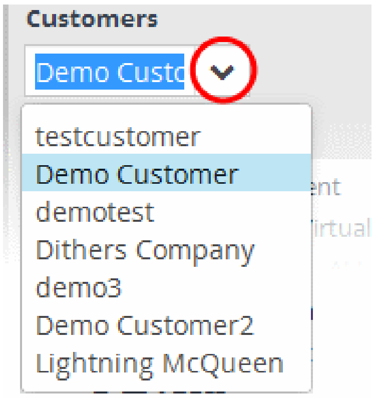


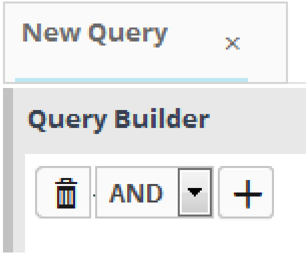
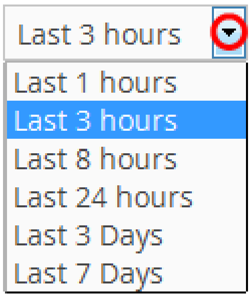
**Time** ( 2015-09-22 09:08:34 - 2015-09-29 09:08:34 )

| time | src_ip | src_port | prod_vendor | dvc_ip | name | prod_version | dst_port | |
|---|---|---|---|---|---|---|---|---|
| 2015-09-23 13:17:31.401 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.400 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.400 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.400 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.400 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.399 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.399 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.398 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.398 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.398 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.397 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.396 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.396 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.395 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.393 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.392 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.392 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.390 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.390 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |
| 2015-09-23 13:17:31.389 | | 0 | Windows | | Other Object Access Events | | 0 | A handle to an ob |

The left hand panel displays a list of predefined queries and custom queries for the selected customer. The main panel displays the parameters of the selected query and the output of the query in the lower pane. Click 'Search' to run the query.

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

| Event Query Interface - Table of controls | |
|---|---|
|  | The 'Customers' drop-down allows you to select the customer for which you want to query events and/or add custom queries. |
| | Allows you to add a new 'Queries' folder to the left side panel |
| | Allows you to edit the name of a 'Queries' folder |

| | |
|---|---|
| ⊕ | Allows you to a add new event query under a selected query folder |
| 🗑 | Allows you to delete selected query folders or event queries |
|  New Query ×<br>Query Builder<br>🗑 AND ▾ + | Allows you to add conditions for a query. The options available from the drop-down are:<br>• AND<br>• OR<br>• NOT<br>• Click the + button to add a condition for a query.<br>• Click the 🗑 button to delete a condition |
| ⤢ | Allows you to expand or collapse the upper pane to view the complete list of conditions in the query. |
| ▥ | Allows you to configure the 'Results' table for the query displayed in the upper pane. |
| Save | Allows you to save a newly created or edited event query, configured from the upper pane. |
| Save As | Allows you to save a copy of the query to a different folder or a new query created using an existing query as a template, with a different name. |
| Schedule | Allows you to configure alerts and email notifications based on the quantity of events detected by the query within a specified period. Refer to the explanation under 'Configure duration based alerts' for more details. |
| 📅 | Allows you to run a query search for a specific period in the past.<br>You can set the start end dates to search for events matching the conditions defined in the query and click the 'Search' button in the 'Advanced Search' dialog that appears on clicking this button to view the list of events. Please note the event query created for searching events in the specific period in the past using this option, cannot be saved. |
|  Last 3 hours ▾<br>Last 1 hours<br>Last 3 hours<br>Last 8 hours<br>Last 24 hours<br>Last 3 Days<br>Last 7 Days | Allows you choose the time period from which events are fetched. Periods range from 1 hour to 7 days. |
| Search | Allows you to run a search operation based on the configured query. |

The interface allows administrators to:

- Manage query folders
- Add and Manage event queries
- Configure results table for a query
- Configure duration based alerts
- Run event queries

- View Results Table
- Perform IP Lookup of External IP Addresses from results using IPVOID
- Perform Lookup of IP Address/Domains from results using Virus Total
- Add Field values to Live Lists from results
- View Aggregated results
- Update and Refine Queries from results

## Manage a Query Folder

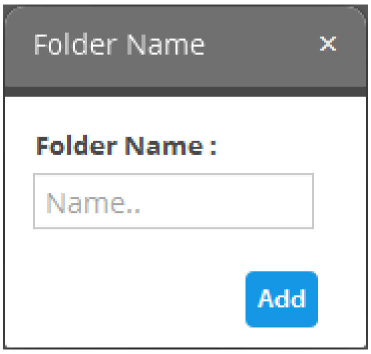
Query folders contain collections of event queries. Every new query must be placed in a query folder.

**Creating a query folder**

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

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

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



Folder Name ×

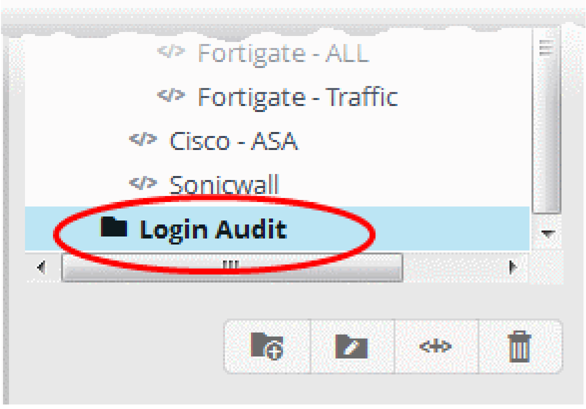
Folder Name :

Name..

Add

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

The folder will be saved and displayed on the left side



Fortigate - ALL

Fortigate - Traffic

Cisco - ASA

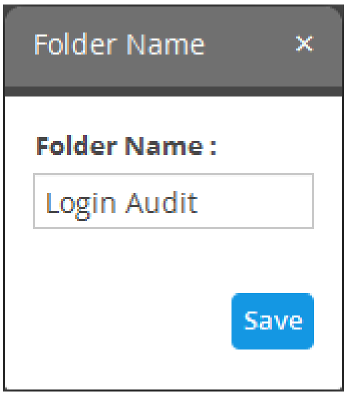
Sonicwall

Login Audit

The relevant event queries can now be placed under the newly created folder. Refer to '**Manage an Event Query**' for more details.

**Editing a query folder**

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



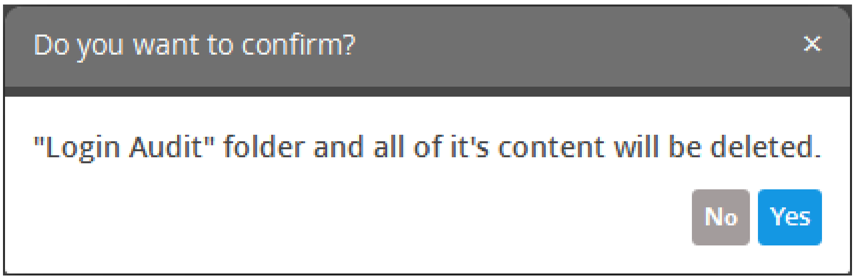
Folder Name : Login Audit

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

**Deleting a query folder**

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

A confirmation dialog will appear.



"Login Audit" folder and all of it's content will be deleted.

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

## Manage an Event Query

Event queries can be created in two ways:

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

### Creating a new event query

An 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 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 originated from an endpoint with IP address 10.100.100.100, build the filter statement as shown below:

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

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

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

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

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

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

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

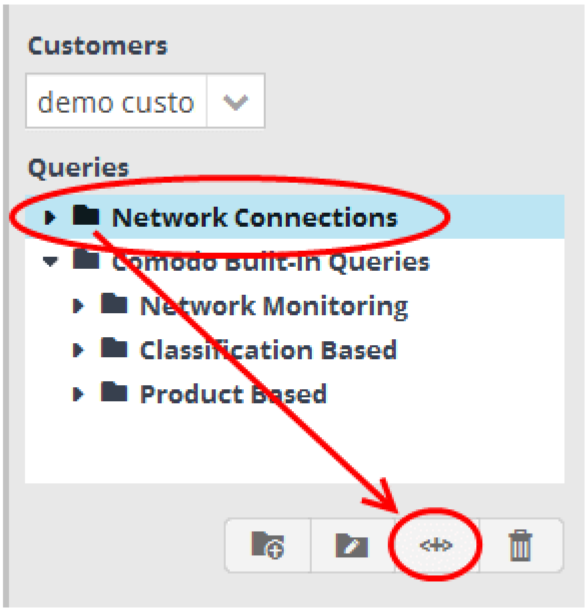
**'Source' + 'src_ip' + '=' + '10.100.100.100'**

**AND**

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

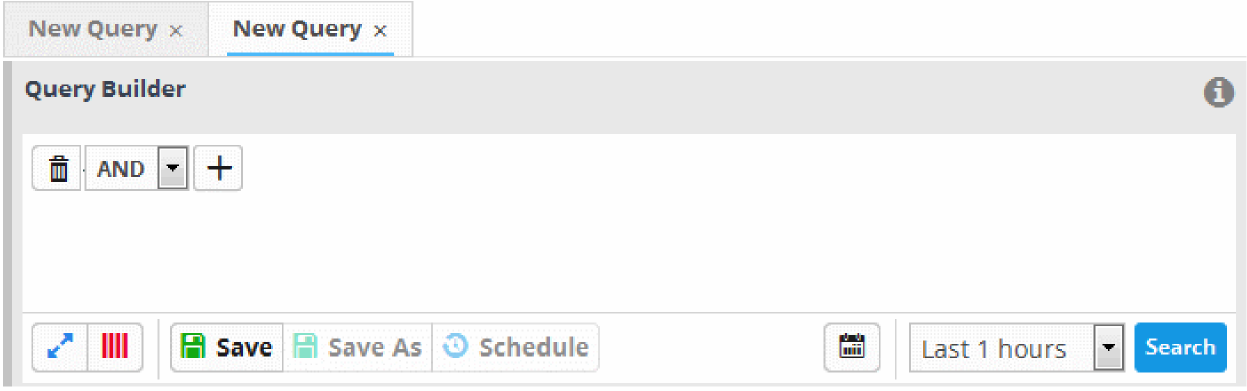
**To add a new event query for a customer**

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



A 'New Query' tab will be displayed.

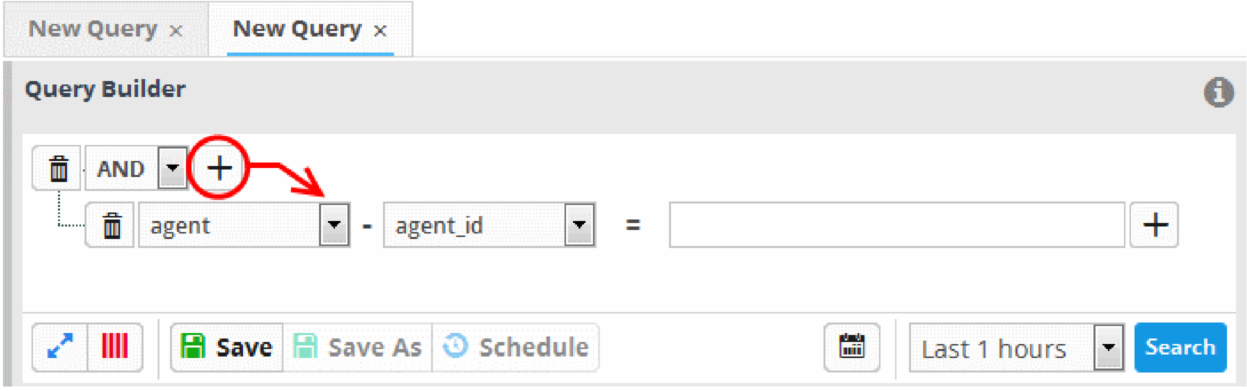
**Tip**: You can also use the 'New Query' tab that is displayed as the first tab on selecting a customer, to create a new query. You can save the created query by selecting an appropriate folder from the left side panel.



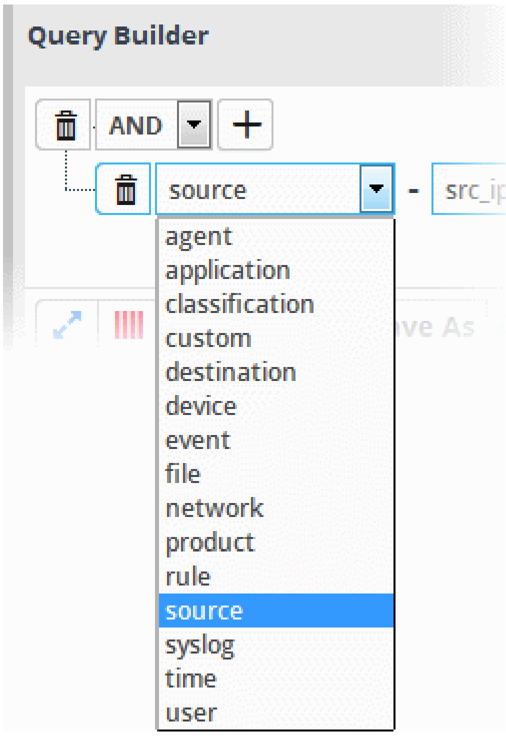
The next step is to add the filters for the query.

- 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

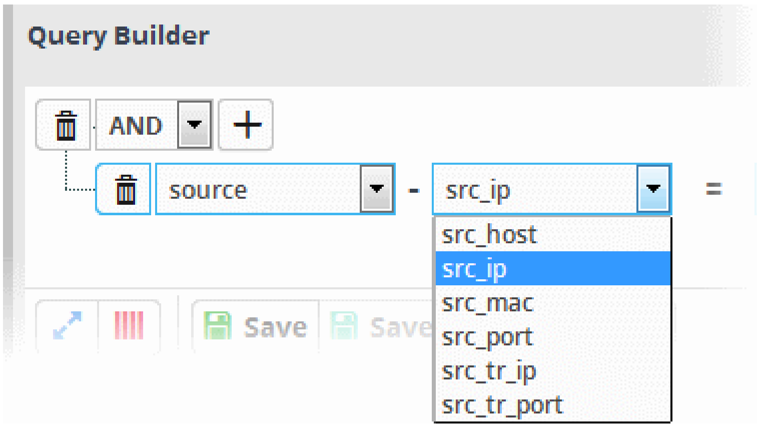
The 'Field Groups' drop-down and 'Fields' drop-down will appear. The 'Fields' drop-down will contain options relevant to the 'Field Group' chosen from the drop-down at the left.



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



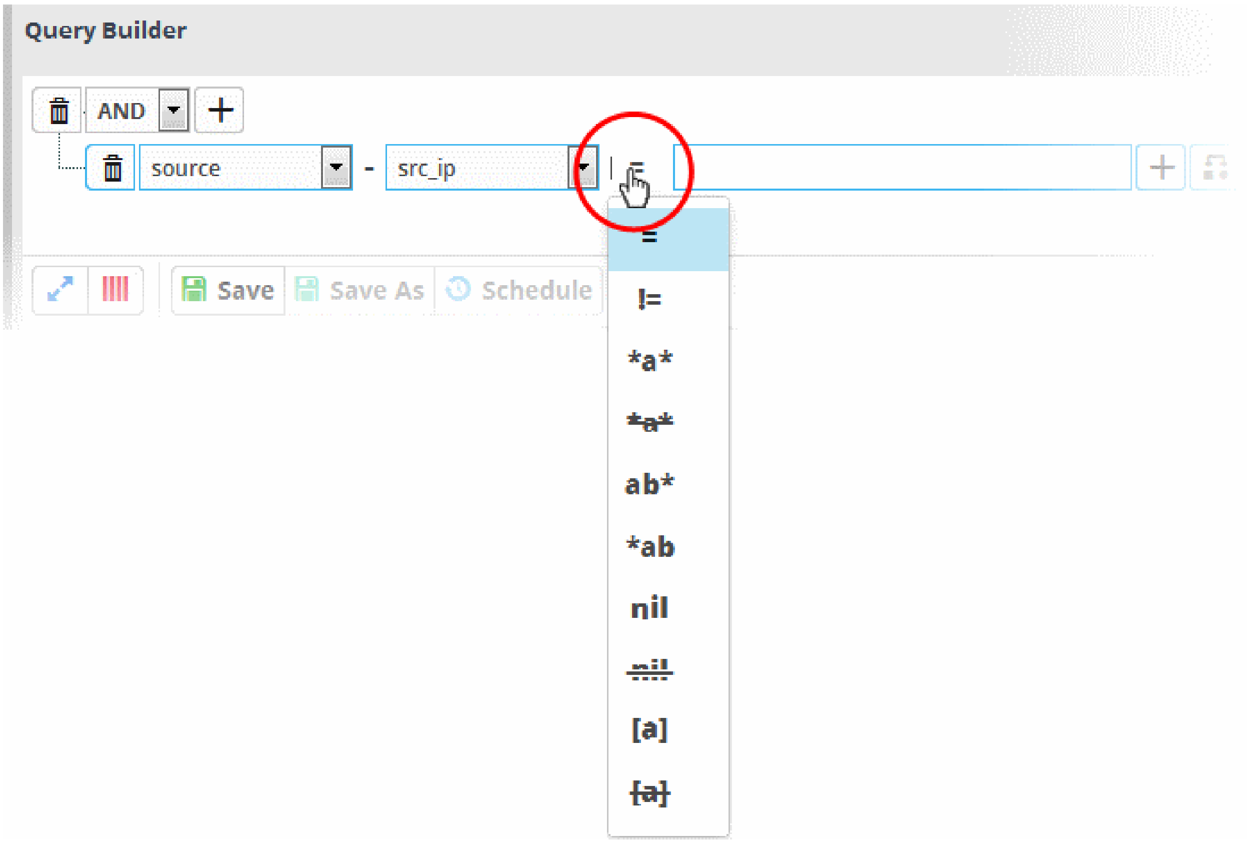
The next field will display the fields available for the selected field group.



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

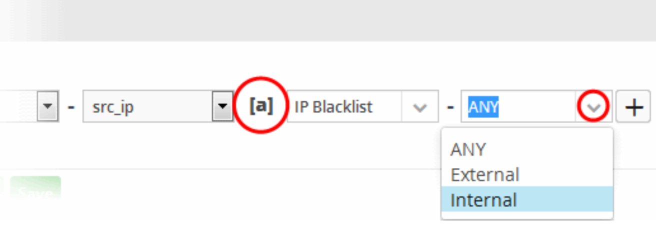
The next step is to choose the relationship operator between the two fields.

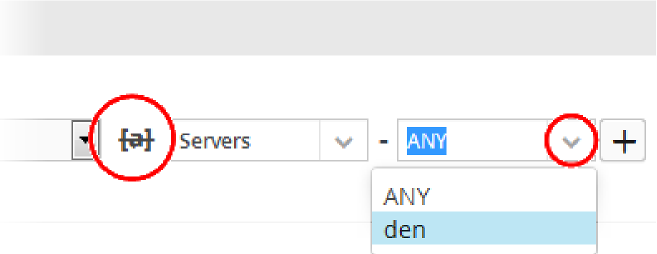
- To choose an operator, click the drop-down between the two fields:



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

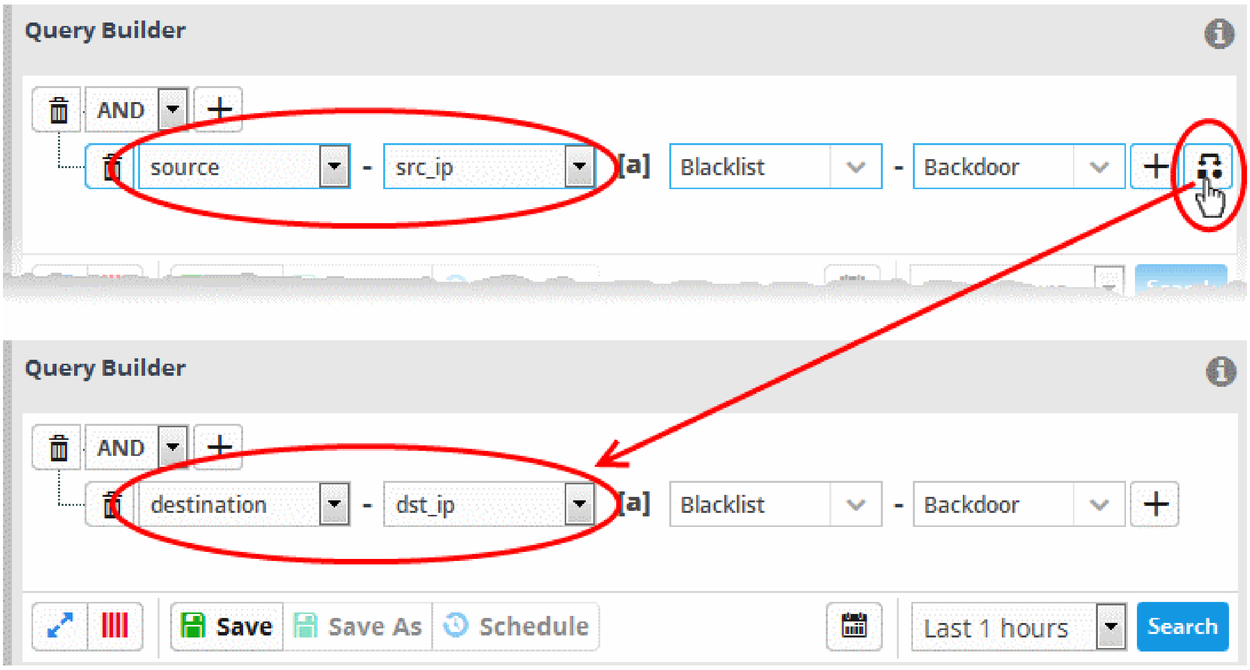
| Relation Operator | Description | Entering the value for the 'Field' |
|---|---|---|
| = | Equals to | Manually enter a value in the field to the right of the operator. Events containing the same value will be identified by the query. |
| != | Does not equal to | Manually enter a value in the field 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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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).<br>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).<br>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.<br>**Background**:<br>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 section **Live Lists**.<br>On selecting **[a]** as the relation parameter, drop-down options will appear for the List and the List type:<br> src_ip<br>[a]<br>IP Blacklist<br>ANY<br>+<br>ANY<br>External<br>Internal<br>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'.<br>• Choose the Live 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 live list .<br>On selecting ~~[a]~~ as the relation parameter, drop-down options will appear for the List and the List type:<br><br>~~[a]~~ Servers - ANY<br>ANY<br>den<br>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'.<br>- Choose the Live 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 live 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.



Query Builder

AND

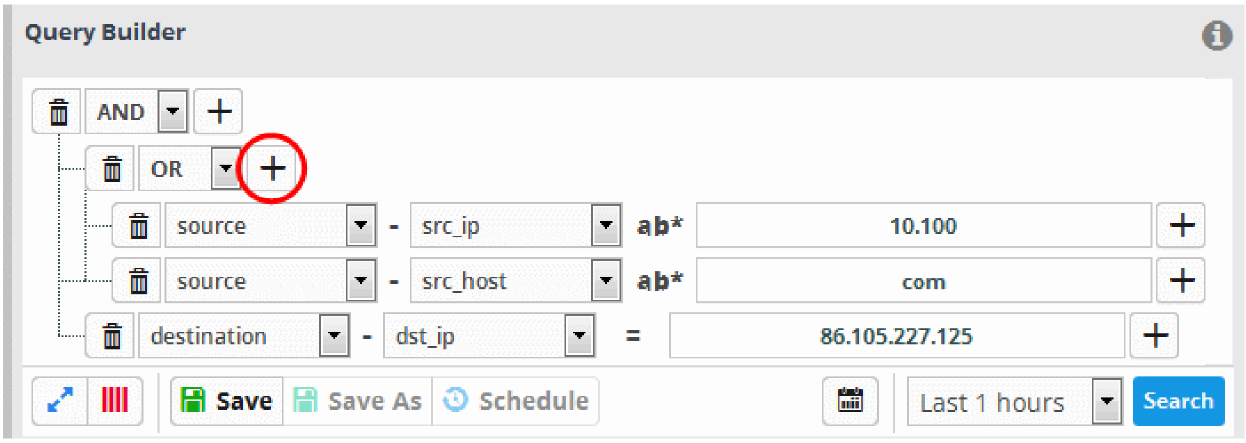
source - src_ip [a] Blacklist - Backdoor

Query Builder

AND

destination - dst_ip [a] Blacklist - Backdoor

- 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



Query Builder

AND

OR

source - src_ip ab* 10.100

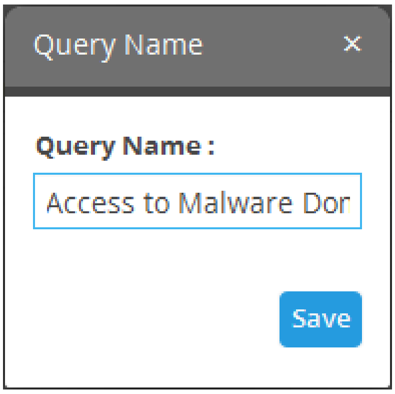
source - src_host ab* com

destination - dst_ip = 86.105.227.125

Last 1 hours

**Tip**: You can update and refine a query by adding more filters once you have seen the results. Refer to the section **Updating a Query** for more details.

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



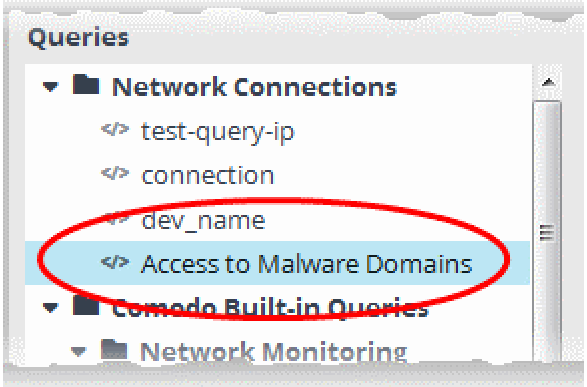
Query Name

Query Name : Access to Malware Dor

- 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. Refer to '**Configure Results Table for a Query**' for more details.

**Creating a new query using an existing query as a template**

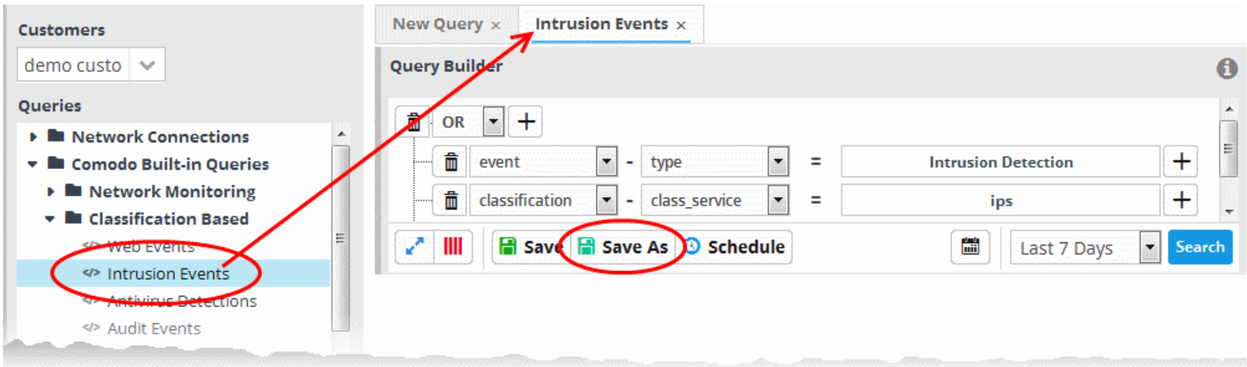
You can select a pre-defined query and modify its parameters to create a new query.

**To create a query from an existing query**

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

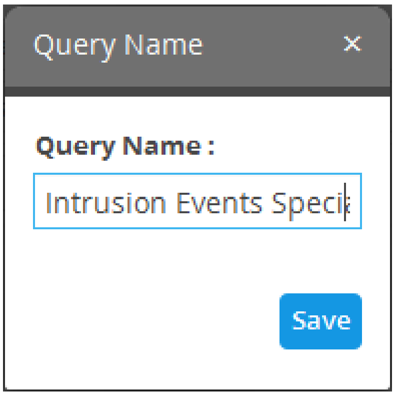
The query will be expanded under a new tab in the right side panel.

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



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

The Query Name dialog will appear.

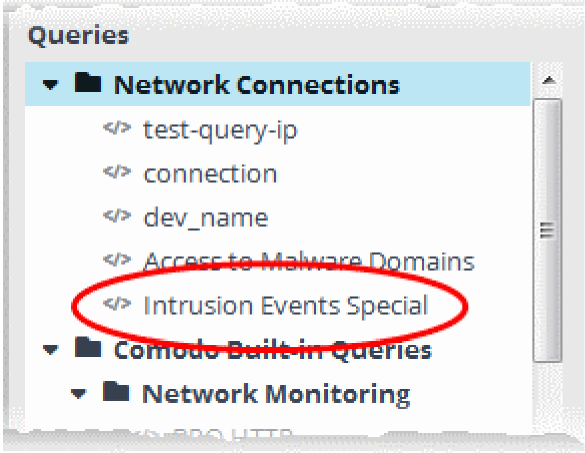


Query Name : Intrusion Events Speci

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

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

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

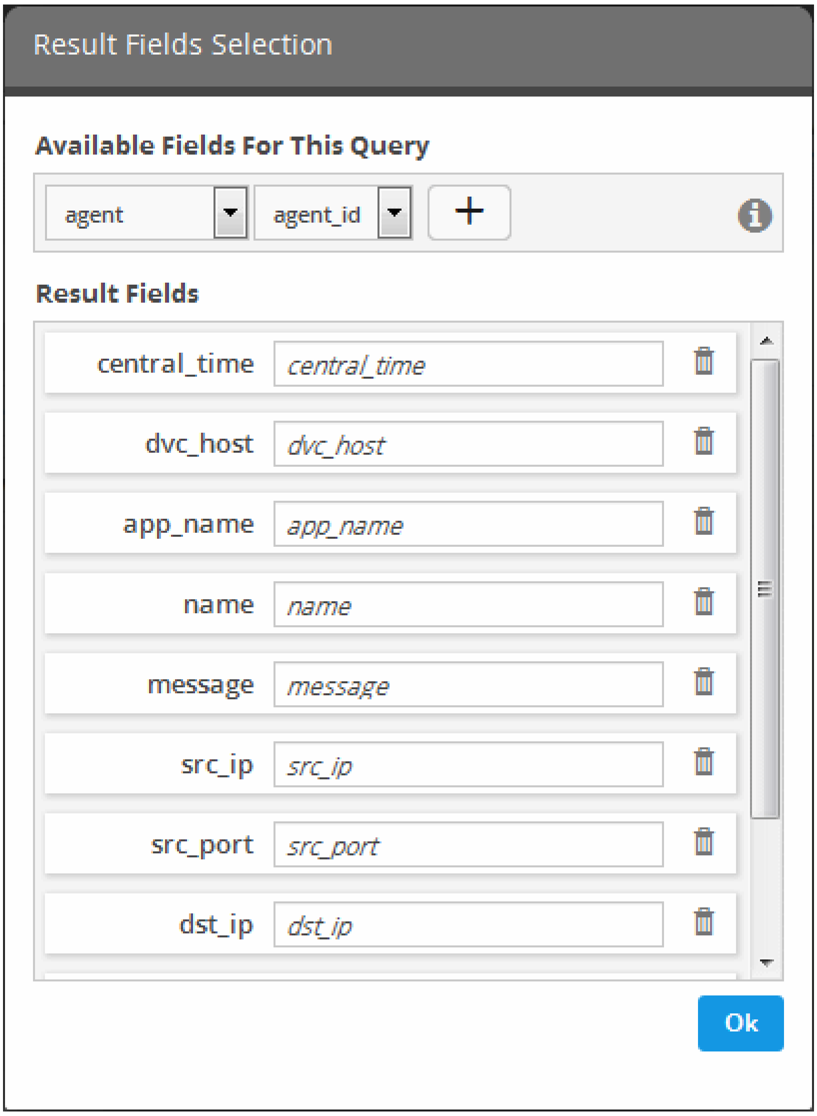


## Configure Results Table for a Query

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

- Select an event query from the left side and click the |||| button from the 'Query Builder' pane.

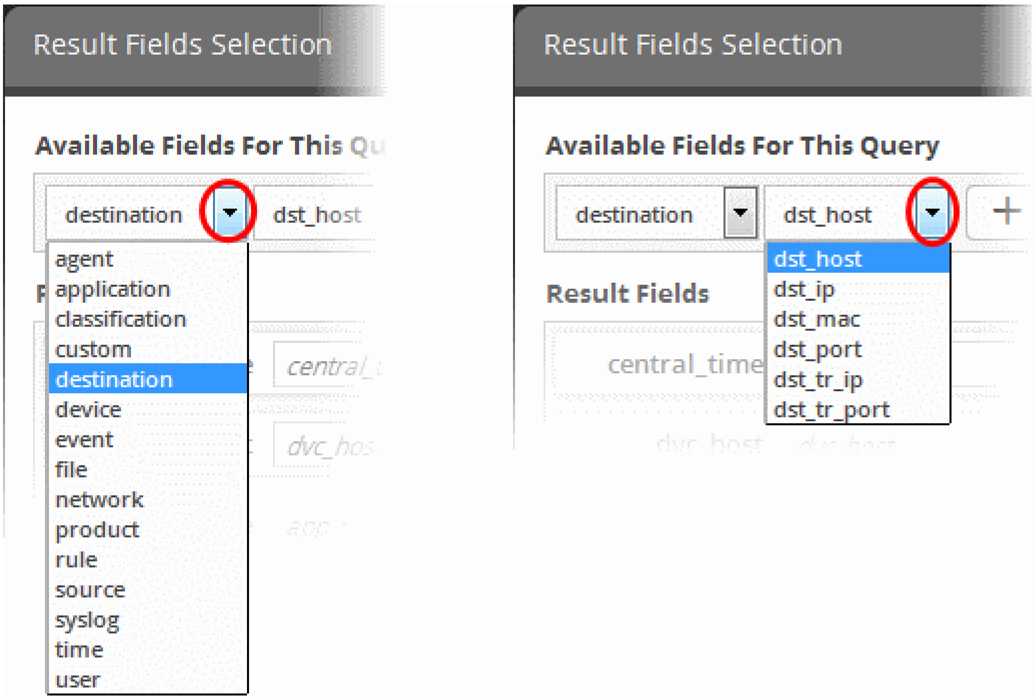
The 'Result Fields Selection' dialog will be displayed.



| | |
|---|---|
| central_time | central_time |
| dvc_host | dvc_host |
| app_name | app_name |
| name | name |
| message | message |
| src_ip | src_ip |
| src_port | src_port |
| dst_ip | dst_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.

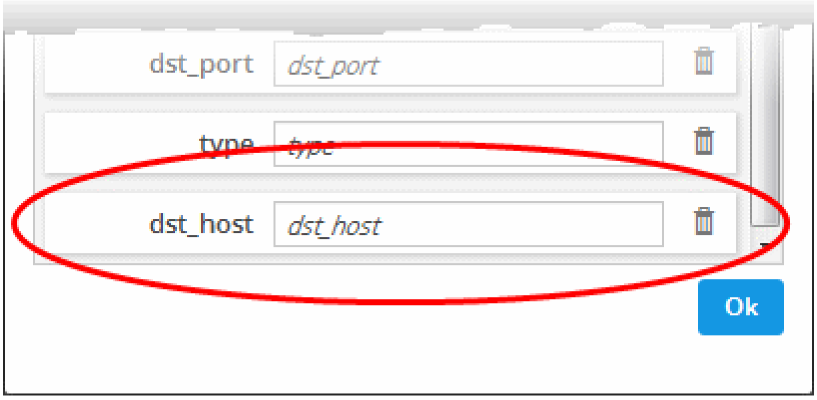
- To add new 'Result Fields', click the 'Field Groups' combo box and select the field group.



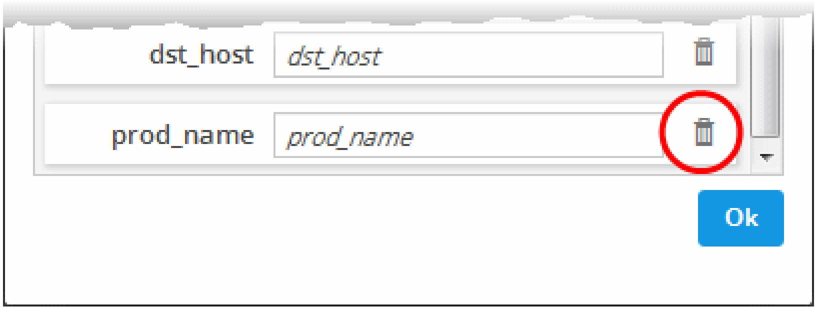
The next field will display the items available for the selected field group.

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

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



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



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

'Event Queries' can also be used to populate charts in a custom dashboard. Refer to the section '**Configuring Custom Dashboard**' for more details.

## Configure Duration Based Alerts

NxSIEM dynamically monitors customer networks for events based on used-defined queries. Administrators can configure queries to generate alerts if the number of events exceeds or falls below a certain threshold in a certain time-period.

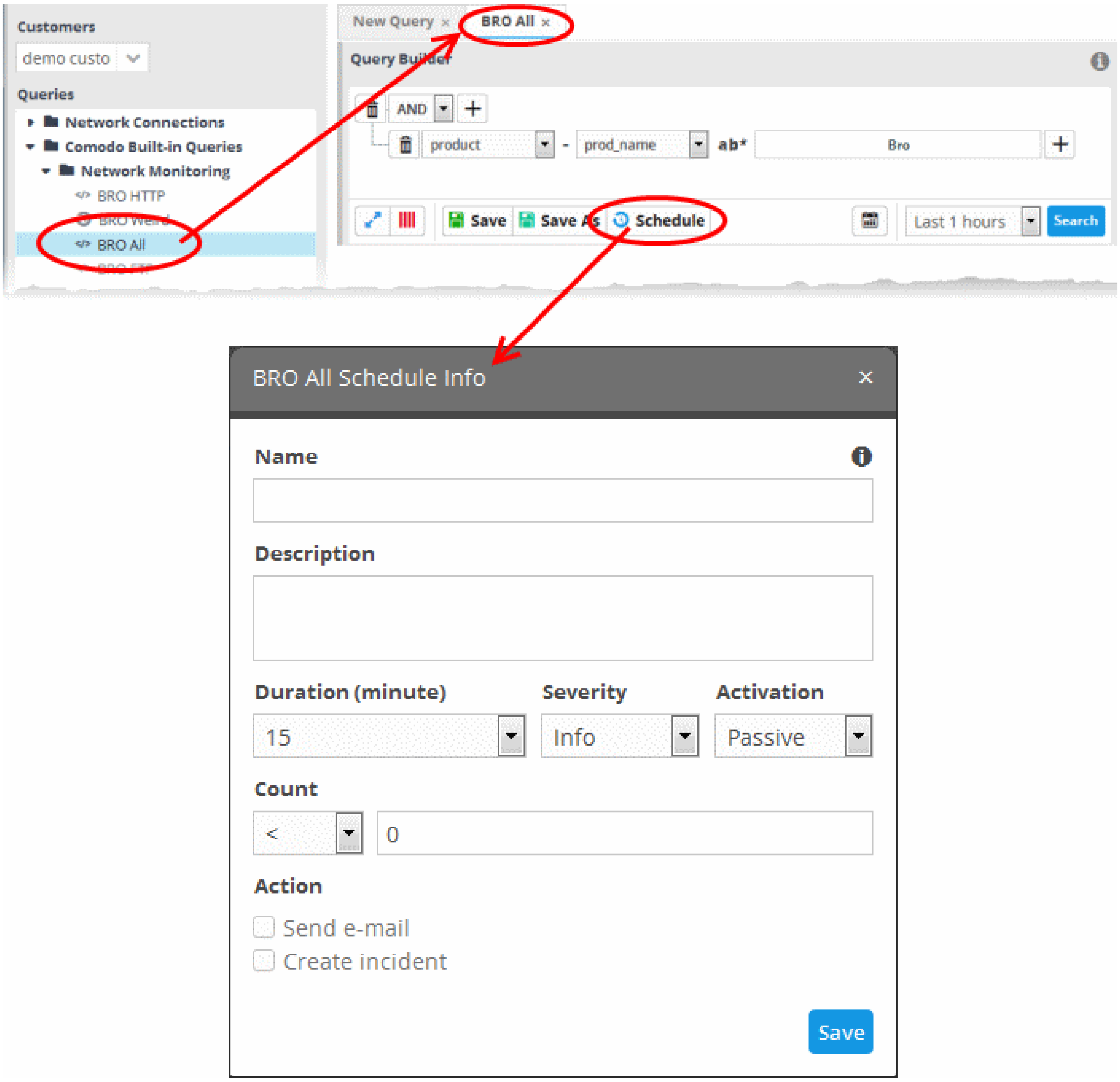
Examples - administrators can request alerts if the number of events matching a query exceeds 1000 in 10 minutes, or if no events are detected for a query for 15 minutes.

Alerts can be configured to send notification emails to the administrator and/or set to generate an 'Incident' which is assigned to a user. For more details on Incidents, refer to the section **Managing Incidents**.

**To schedule a query to generate alerts**

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

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



BRO All Schedule Info

Name

Description

Duration (minute): 15

Severity: Info

Activation: Passive

Count: < 0

Action

□ Send e-mail

□ Create incident

Save

- **Name** - Enter a name to identify the schedule

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

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

The event query added with a schedule.

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

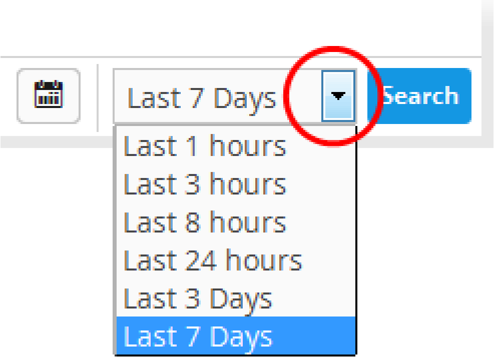
## Run an Event Query

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

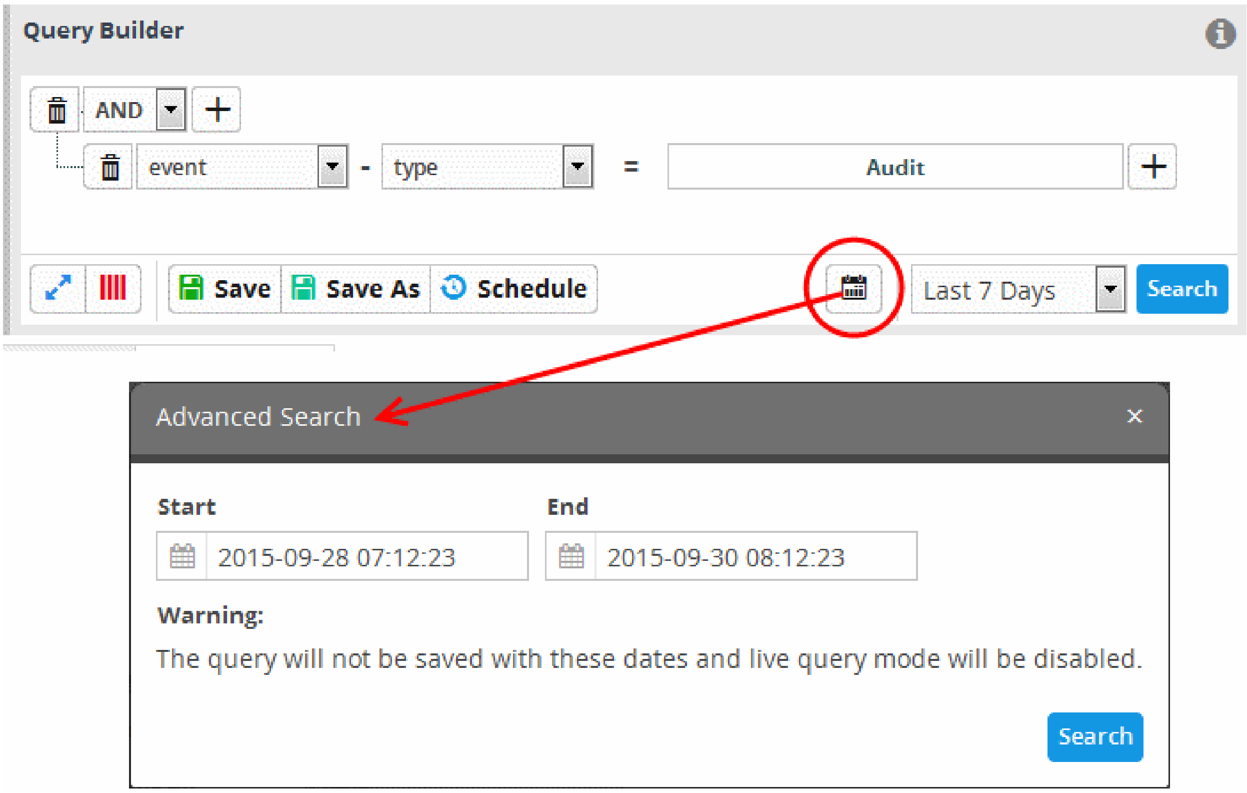
- As a results table with columns selected as explained **above**. You can view the full details of any event in its 'Details Pane' containing values for all the fields in the log entry. The Details pane also allows you to add values of selected fields to Live Lists for use in new event queries and correlation rules. You can also run look-ups of IP addresses and domains involved in the event.  More explanations are available under '**View Results Table**'.
- As aggregations of results, with identified events grouped based on selected event field(s) and the resultant event groups ranked based on specified aggregation function. More explanations are available under **View Aggregated Results**.

**To run an event query**

- Select an event query from the left.
- Select the period for which you want to run the query.
  - 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'.



event - type = Audit

Start: 2015-09-28 07:12:23

End: 2015-09-30 08:12:23

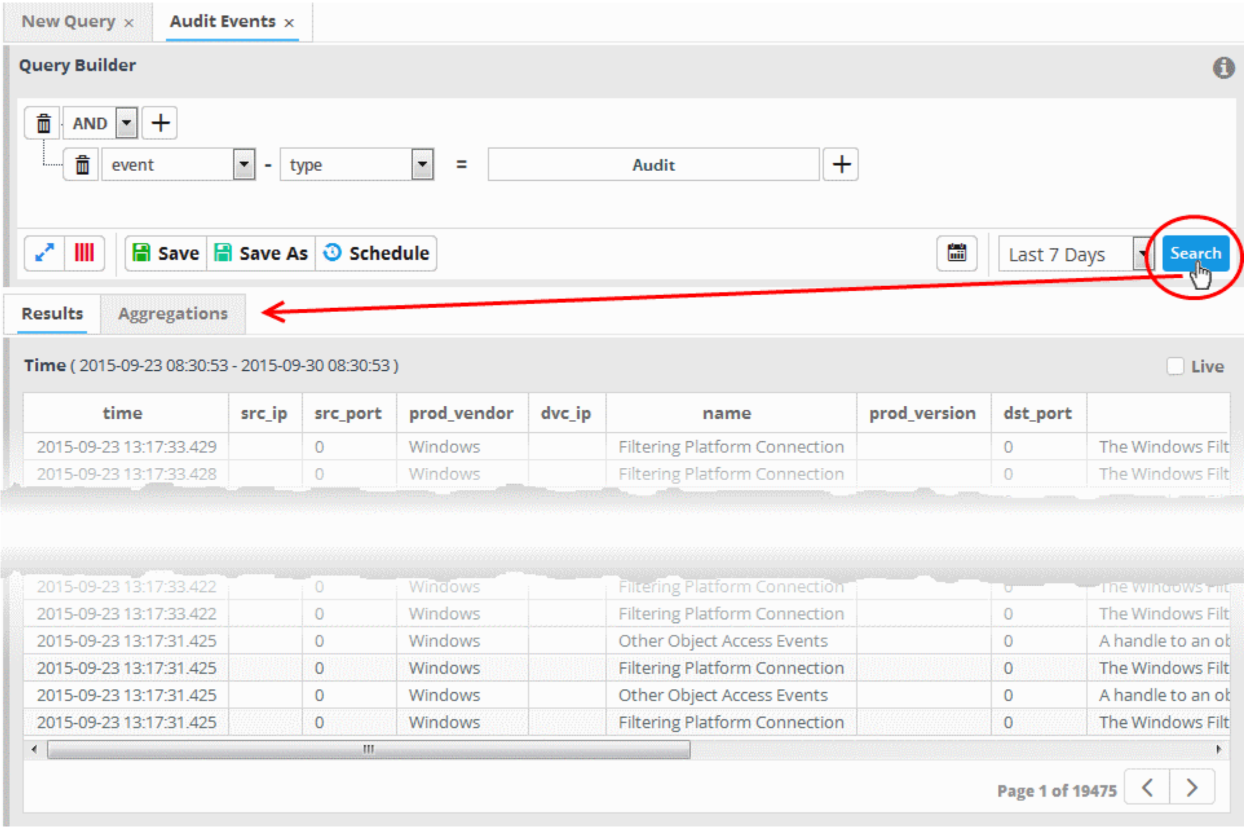
Warning:

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

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 will not be available for advanced searches with specific start and end dates.



event - type = Audit

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 | |
|---|---|---|---|---|---|---|---|---|
| 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 |

The lower pane has two tabs:

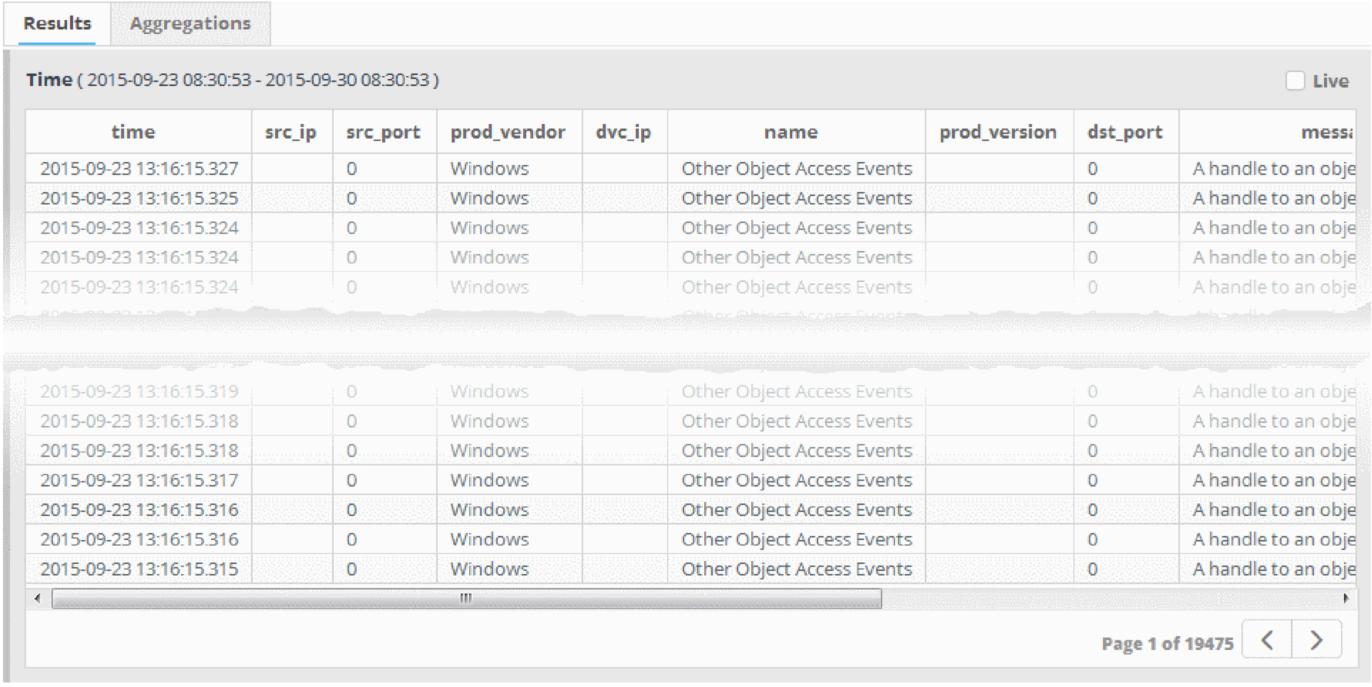
- **Results** - The 'Results' tab displays log entries that match the query with the selected event fields as column headers (explained above). Clicking on an event allows you  to view its details. More details on the 'Results Table' are available under '**View Results Table**'.

- **Aggregations** - The Aggregations tab allows you to group identified events and view aggregation results. More details on aggregations are available under '**View Aggregated Results**'.

## View Results Table

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

The 'Results' tab contains a table of event log records that match the event query. The event fields form the table columns. Events can be created in the Query Builder pane. Refer to the explanation of  '**Configure results table for a query**' for more details.

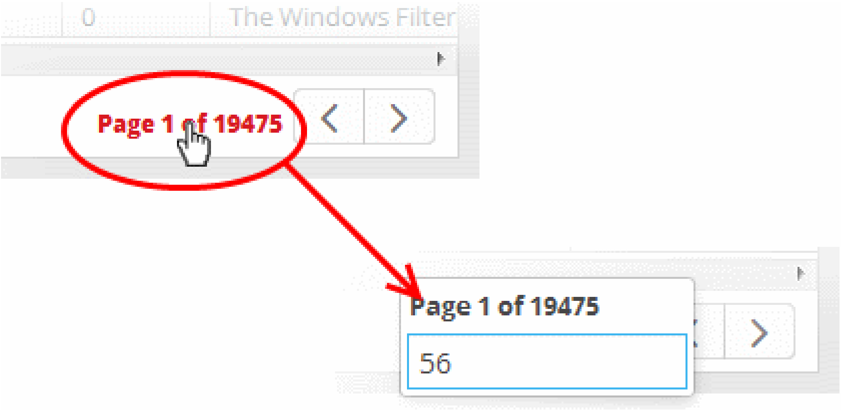


Time ( 2015-09-23 08:30:53 - 2015-09-30 08:30:53 )

| time | src_ip | src_port | prod_vendor | dvc_ip | name | prod_version | dst_port | messa |
|---|---|---|---|---|---|---|---|---|
| 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 |

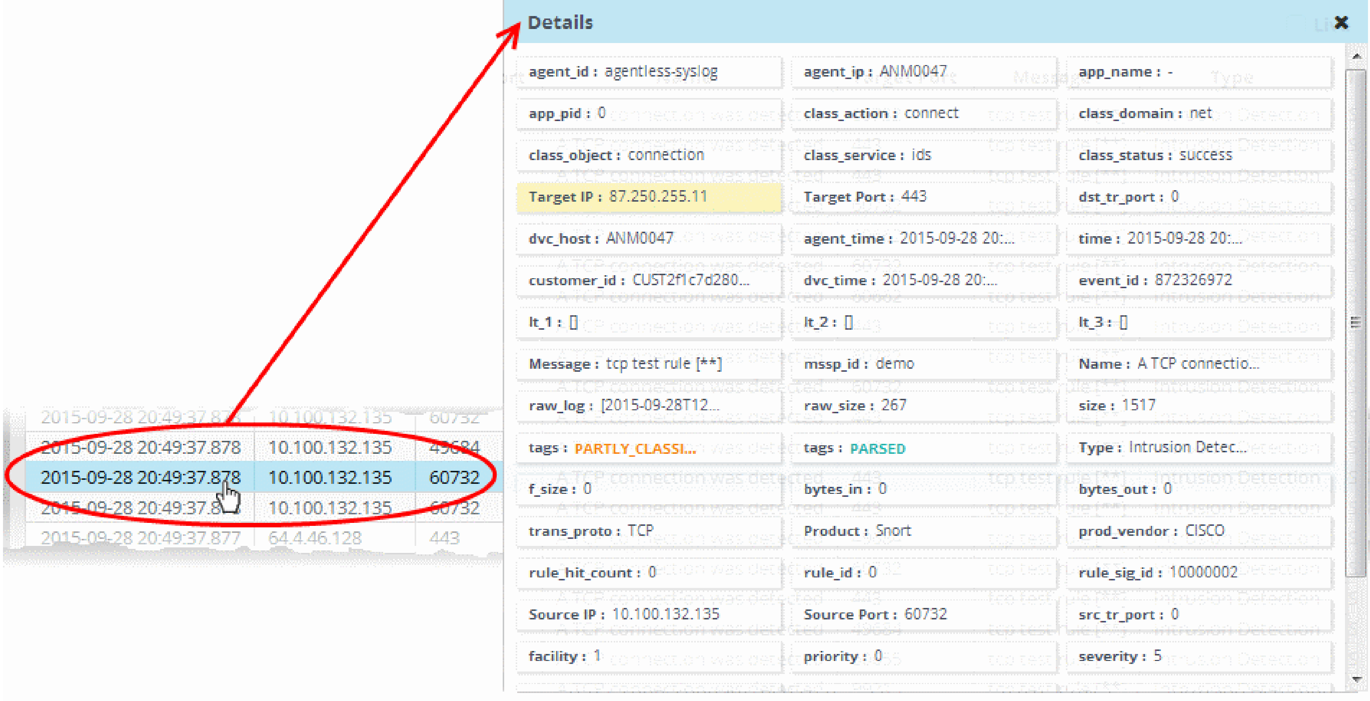
Page 1 of 19475

Each page in the 'Results' table displays 20 entries. You can navigate to successive pages using the left and right arrows at the bottom-right. To open a specific page, click the page number at bottom-right then enter the page number in the text box:



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.



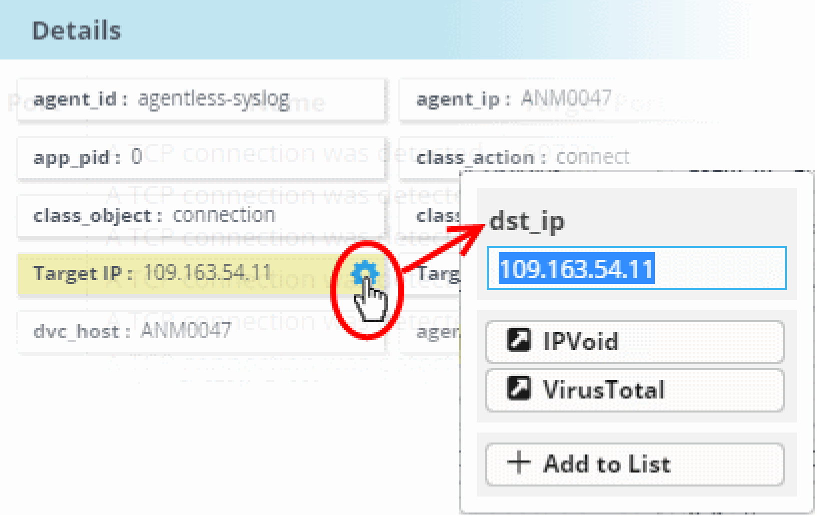
| | | |
|---|---|---|
| 2015-09-28 20:49:37.878 | 10.100.132.135 | 60732 |
| 2015-09-28 20:49:37.878 | 10.100.132.135 | 49684 |
| 2015-09-28 20:49:37.878 | 10.100.132.135 | 60732 |
| 2015-09-28 20:49:37.8 | 10.100.132.135 | 60732 |
| 2015-09-28 20:49:37.877 | 64.4.46.128 | 443 |

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. Refer to the explanation under **Update and Refine Queries from results** for more details.
- If you click the gear icon that appears when you hover your mouse over a field you will see a context sensitive menu:



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

From the context sensitive menu, you can:

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

## Performing IP Lookup of External IP Addresses using IPVOID

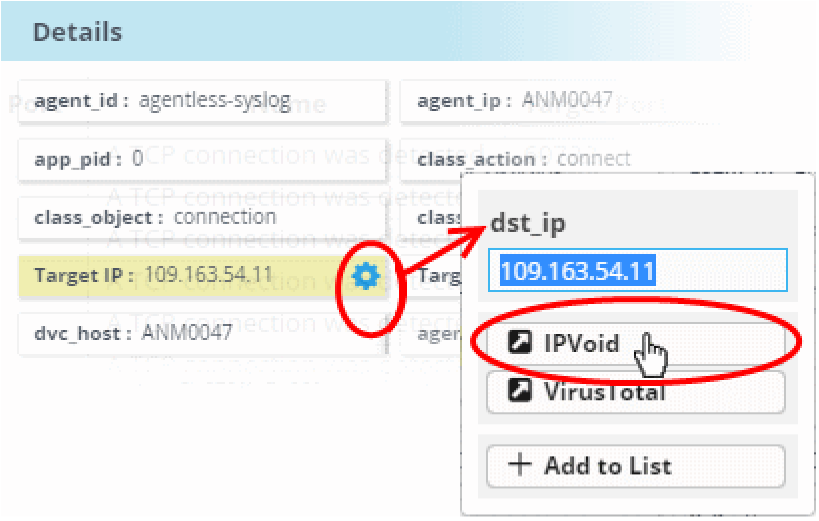
You can view the scan report containing IP address information and IP Blacklist Report for any external IP address detected in an event. The 'Details' pane of an event query result displays the detected external IP address field in yellow, which acts as a shortcut to perform the IP Look up through IPVOID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

**To perform IP Look up of External IP address**

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

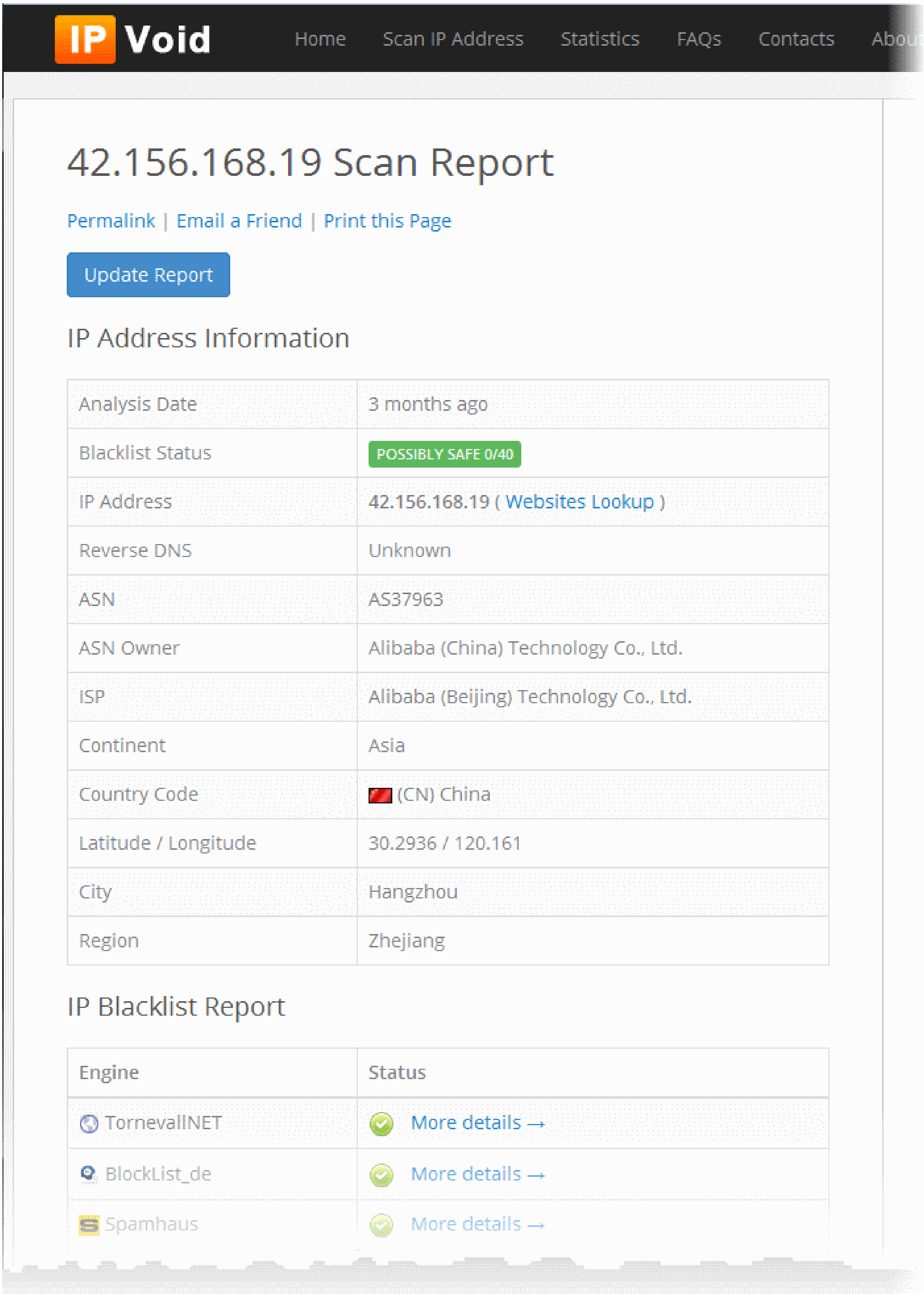
The fields containing external IP address(es) are highlighted in yellow as shown in the example below.

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



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

An example is shown below.



42.156.168.19 Scan Report

Permalink | Email a Friend | Print this Page

Update Report

IP Address Information

| | |
|---|---|
| Analysis Date | 3 months ago |
| Blacklist Status | POSSIBLY SAFE 0/40 |
| IP Address | 42.156.168.19 ( Websites Lookup ) |
| Reverse DNS | Unknown |
| ASN | AS37963 |
| ASN Owner | Alibaba (China) Technology Co., Ltd. |
| ISP | Alibaba (Beijing) Technology Co., Ltd. |
| Continent | Asia |
| Country Code | (CN) China |
| Latitude / Longitude | 30.2936 / 120.161 |
| City | Hangzhou |
| Region | Zhejiang |

IP Blacklist Report

| Engine | Status |
|---|---|
| TornevallNET | ✓ More details → |
| BlockList_de | ✓ More details → |
| Spamhaus | ✓ More details → |

## Performing IP Address/Domain Lookup using Virus Total

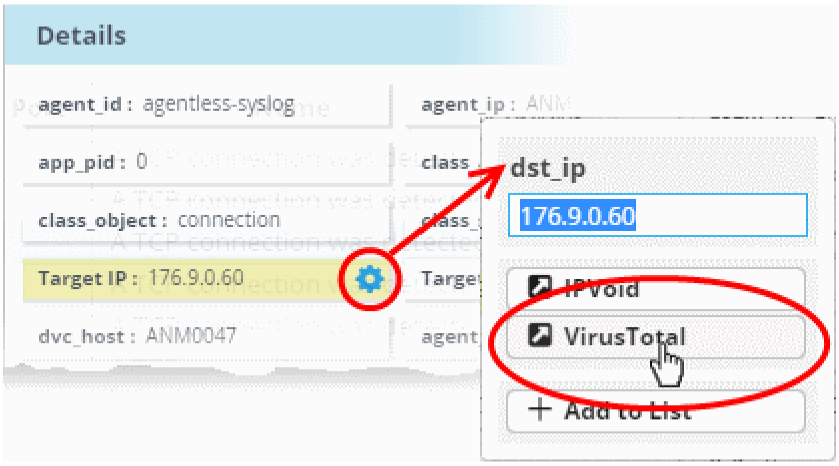
You can view the IP address information/Domain information for external IP addresses/domains detected in an event from the 'Virus Total' website. The 'Details' pane of an event query result displays the fields containing external IP address/domain names field in yellow, which acts as a shortcut to perform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

**To perform IP/Domain Look up using Virus Total**

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

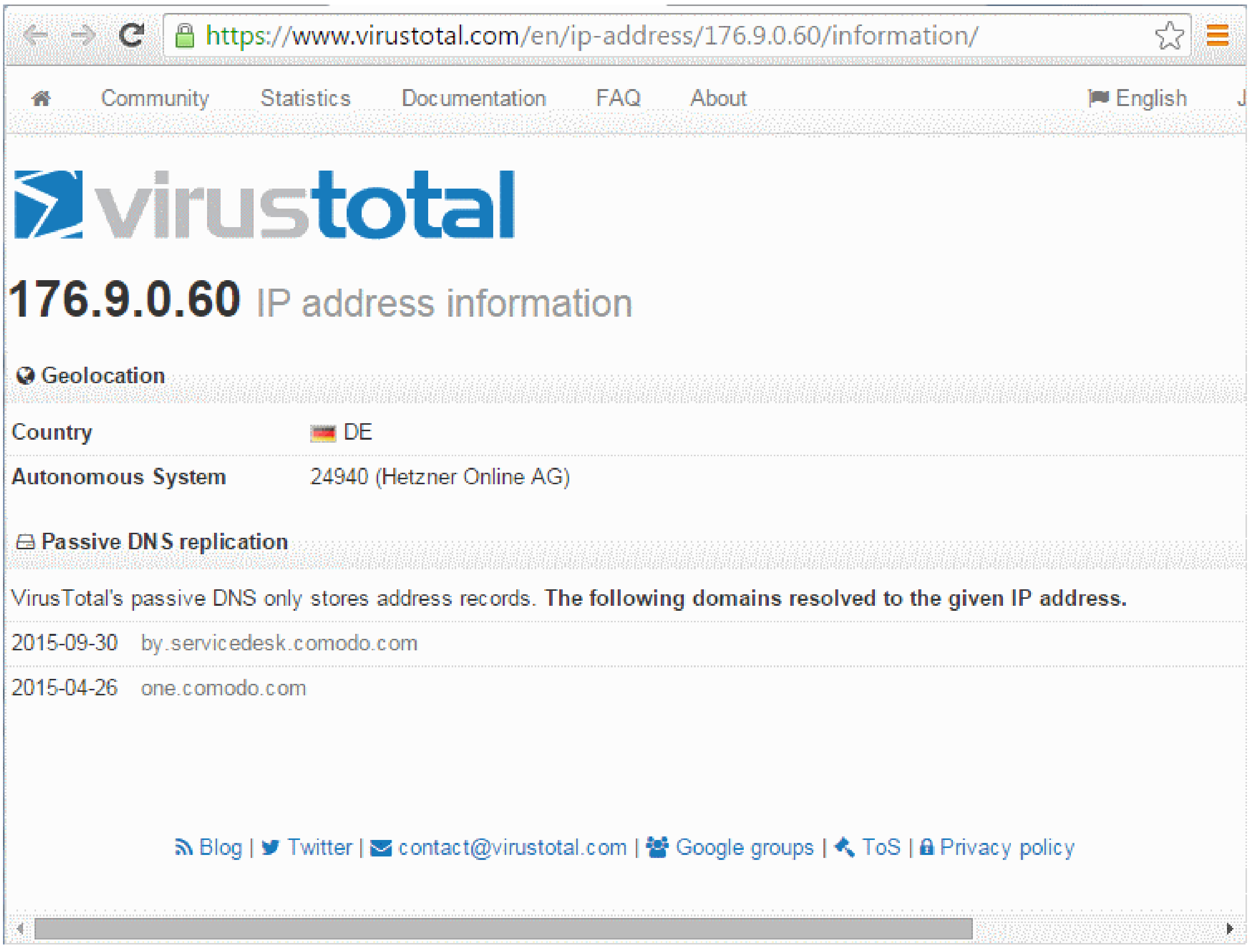
The fields containing external IP address/Domain name are highlighted in yellow as shown in the example below.

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



You will be taken to the Virus Total web page which contains information about the IP address/domain.

An example is shown below.


https://www.virustotal.com/en/ip-address/176.9.0.60/information/
Community
Statistics
Documentation
FAQ
About
English
virustotal
Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy

176.9.0.60 IP address information

Geolocation

| | |
|---|---|
| Country | DE |
| Autonomous System | 24940 (Hetzner Online AG) |

Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

| | |
|---|---|
| 2015-09-30 | by.servicedesk.comodo.com |
| 2015-04-26 | one.comodo.com |

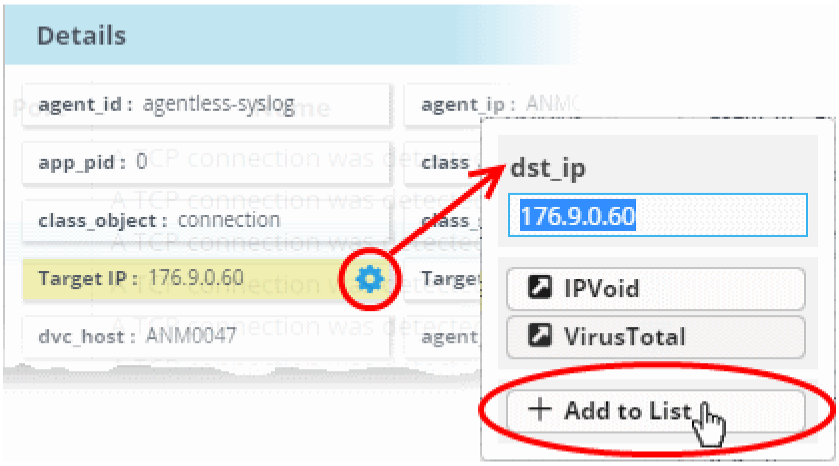
## Adding Field values to Live Lists from Results

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

**Background Note on Live Lists**: Live Lists enable administrators to add lists of values for fields used in queries and correlation rules. Lists can be updated manually or configured to fetch values by a correlation rule. List updates will be immediately reflected in the queries and the rules in which it is used, relieving the administrator of the burden of updating them manually. For more details on Live List management, refer to **Live Lists**.

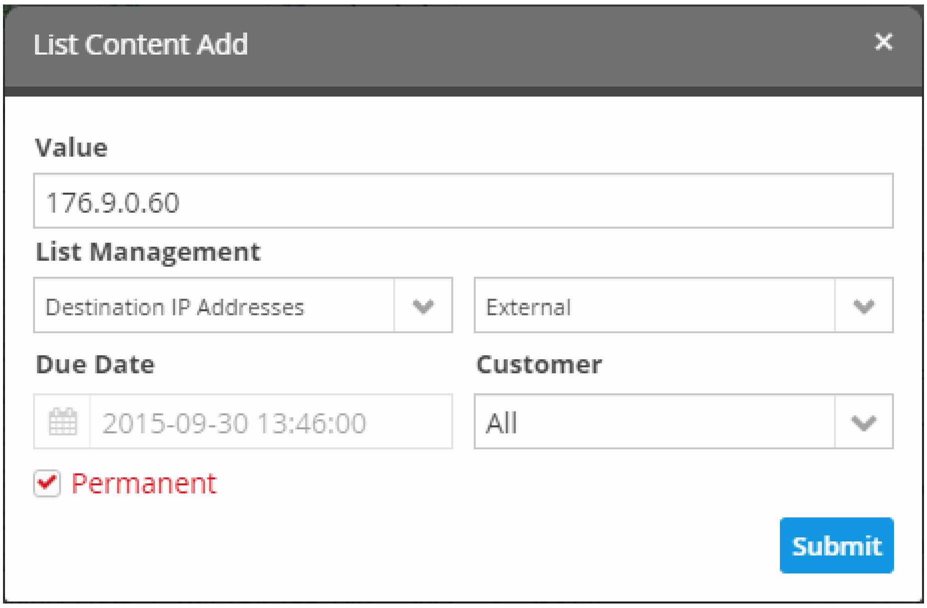
To add a field value from an event to a live list:

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



- Click on the 'Add to List' option.

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


List Content Add ×

Value: 176.9.0.60

List Management: Destination IP Addresses | External

Due Date: 2015-09-30 13:46:00

Customer: All

☑ Permanent

- Select the Live List and the list type to which the value is to be added, from the respective drop-downs under 'List Management'.
- Enter the date till which the value is valid in the Due Date field. You can click the calendar icon at the left of the field and choose the date. On the specified date, the value will be automatically removed from the list. If you want the value to be permanently valid, select the 'Permanent' checkbox.
- Select the customer to which the value is applicable from the 'Customer' drop-down.
- Click 'Submit'.

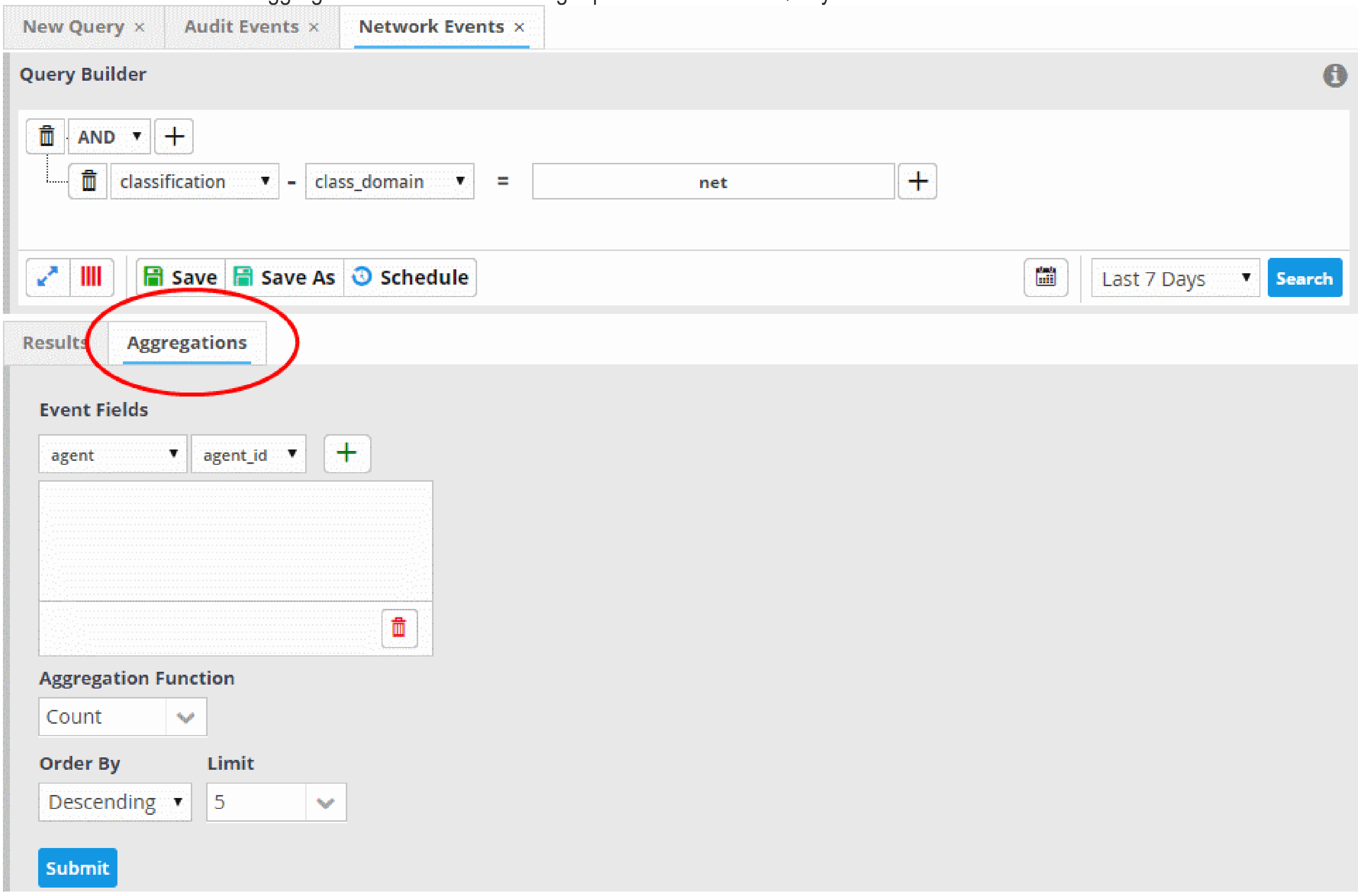
The value will be added to the respective List Type and all the queries and correlation rules in which the list is deployed, will be updated immediately.

## View Aggregated Results

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

**To view the aggregation of events**

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



Aggregating events involves four steps:

- Step 1 - Select the event field(s) on which events are to be grouped
- Step 2 - Select the aggregation function
- Step 3 - Select the order of ranking based on how you want to see the aggregation results
- Step 4 - Set the limit for number of results to be displayed

**Step 1 - Select the event field(s) on which events are to be grouped**

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

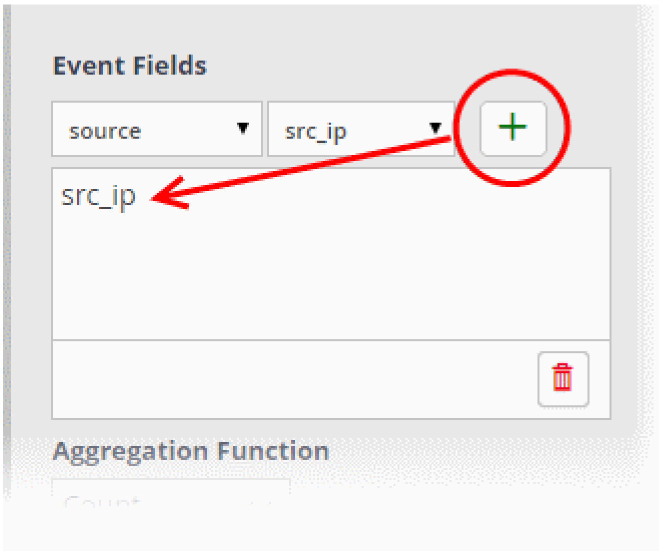
To select the event field(s) for grouping

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

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

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

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



- Repeat the process to add more fields for grouping.

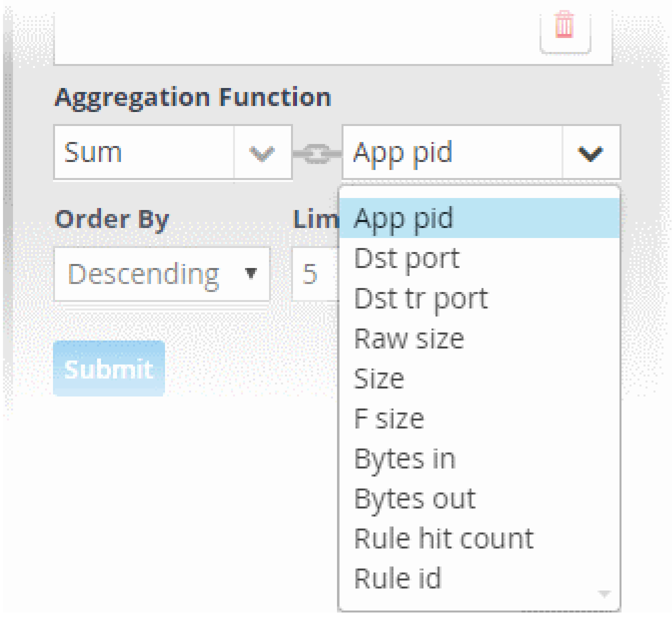
**Step 2 - Select the aggregation function**

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

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

**To set the aggregation function**

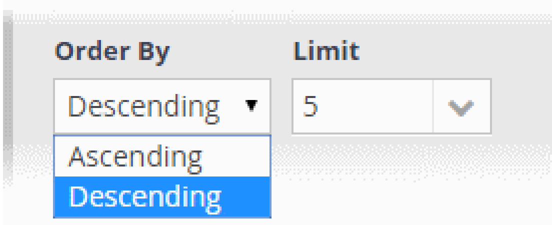
- Choose the function from the 'Aggregation Function' drop-down.
- If you choose 'Sum', 'Average', 'Maximum' or 'Minimum', then you should choose an item which is it useful to measure. For example, 'Bytes-in' can be measured and is suitable for the Sum, Average, Max and Min functions. On the other hand,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



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

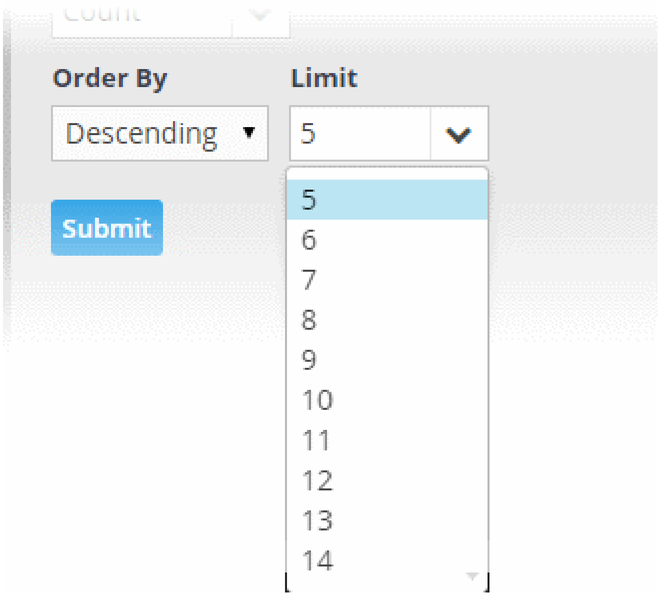
You can choose how event groups should be ranked from the 'Order By' drop-down. The available options are:

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



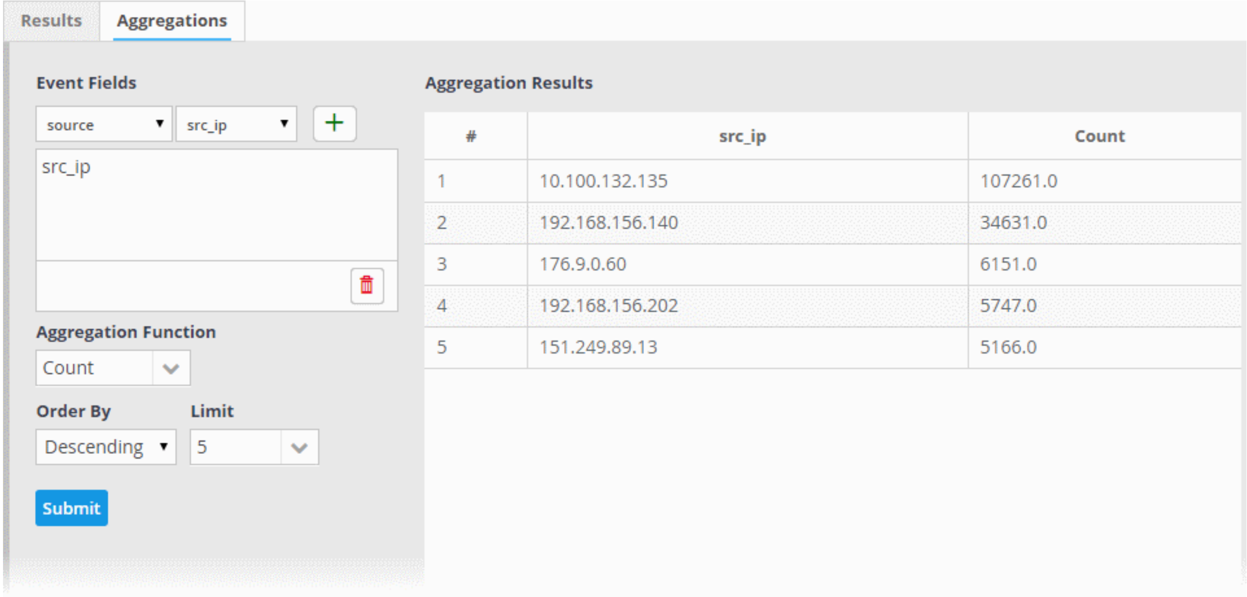
**Step 4 - Set the limit for number of results to be displayed**

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



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

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



Aggregation Results

| # | src_ip | Count |
|---|---|---|
| 1 | 10.100.132.135 | 107261.0 |
| 2 | 192.168.156.140 | 34631.0 |
| 3 | 176.9.0.60 | 6151.0 |
| 4 | 192.168.156.202 | 5747.0 |
| 5 | 151.249.89.13 | 5166.0 |

## Updating an Event Query

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

**To update a query**

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

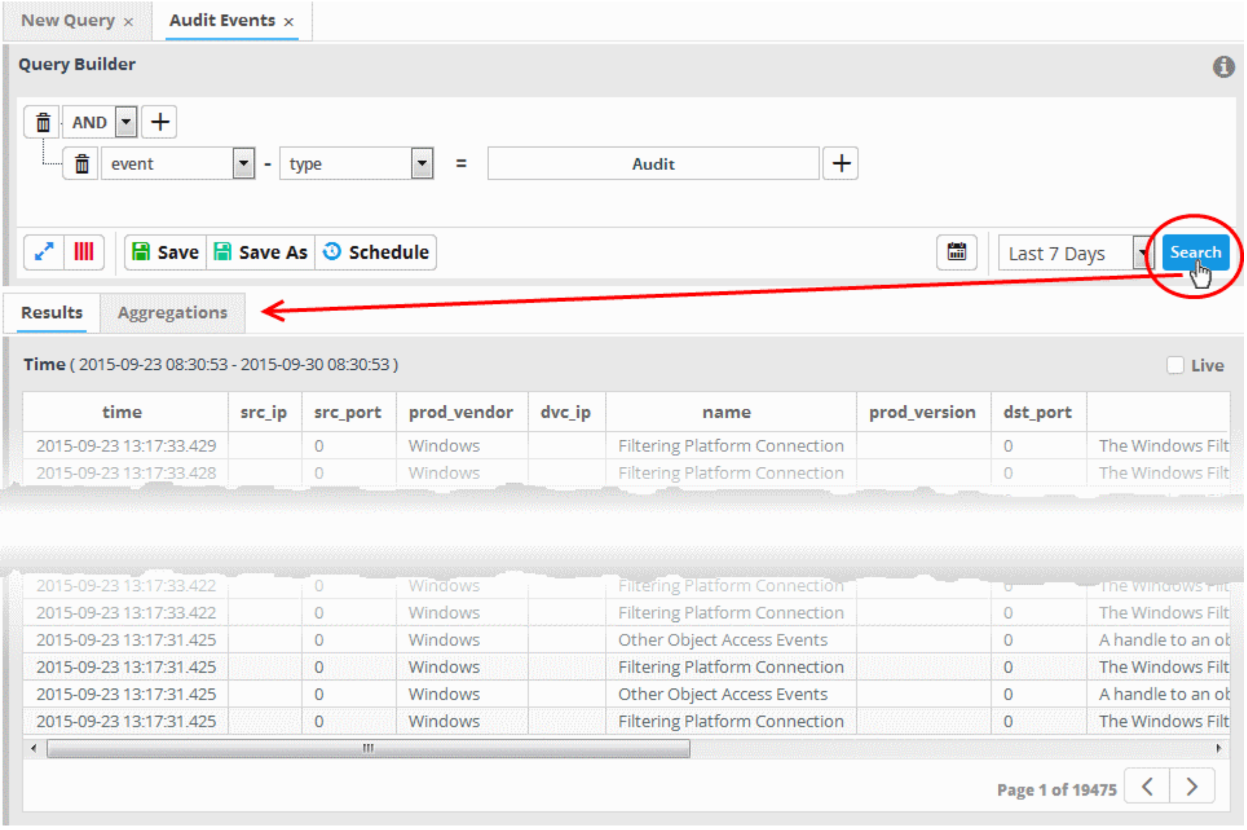
The Query with its filter statements will be displayed in a new tab at the right panel

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

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

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

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

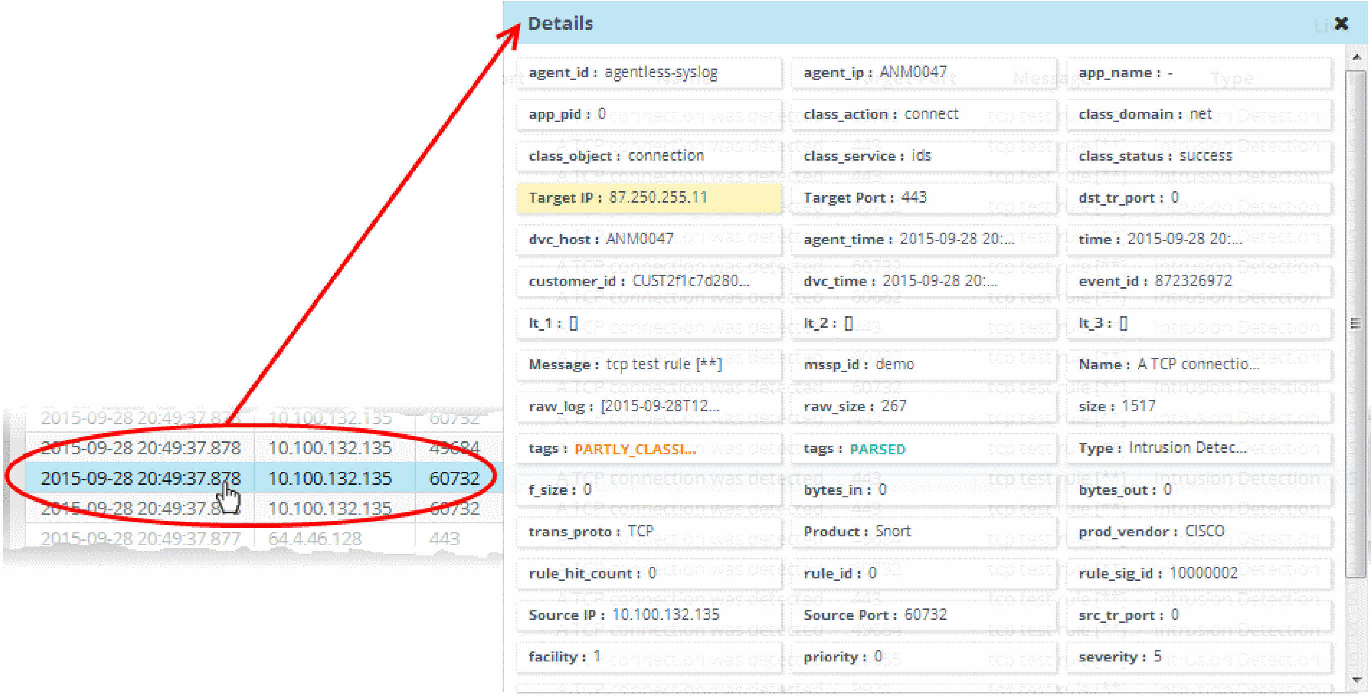


**Time** ( 2015-09-23 08:30:53 - 2015-09-30 08:30:53 )

| time | src_ip | src_port | prod_vendor | dvc_ip | name | prod_version | dst_port | |
|---|---|---|---|---|---|---|---|---|
| 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

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



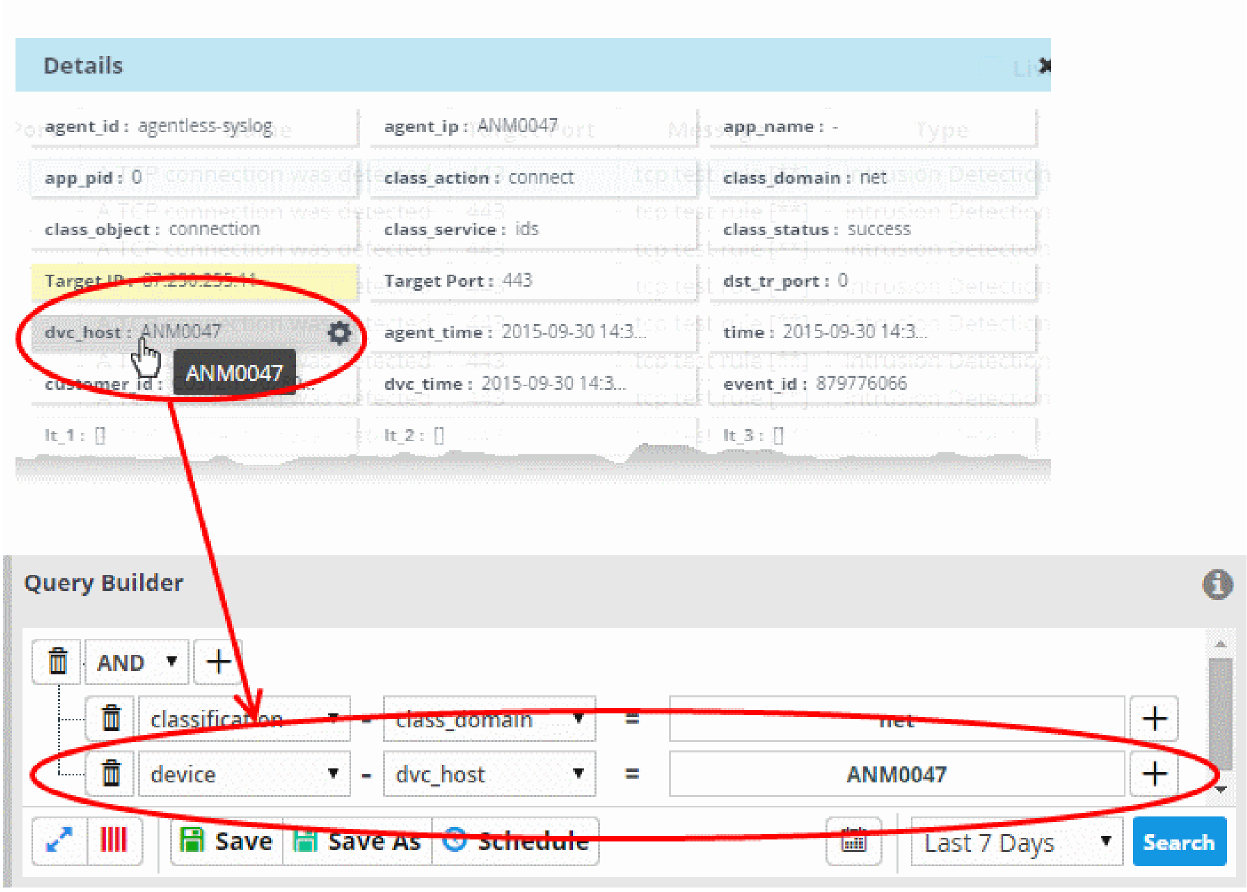
| | | |
|---|---|---|
| 2015-09-28 20:49:37.878 | 10.100.132.135 | 60732 |
| 2015-09-28 20:49:37.878 | 10.100.132.135 | 49684 |
| 2015-09-28 20:49:37.878 | 10.100.132.135 | 60732 |
| 2015-09-28 20:49:37.8.. | 10.100.132.135 | 60732 |
| 2015-09-28 20:49:37.877 | 64.4.46.128 | 443 |

**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 |

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

- Click on the field, to be added as a filter with its value as shown in the result, to the query.



**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 : 87.230.255.11 | Target Port : 443 | dst_tr_port : 0 |
| dvc_host : ANM0047 | agent_time : 2015-09-30 14:3... | time : 2015-09-30 14:3... |
| customer_id : | dvc_time : 2015-09-30 14:3... | event_id : 879776066 |
| lt_1 : [] | lt_2 : [] | lt_3 : [] |

**Query Builder**

AND
- classification - class_domain = net
- device - dvc_host = ANM0047

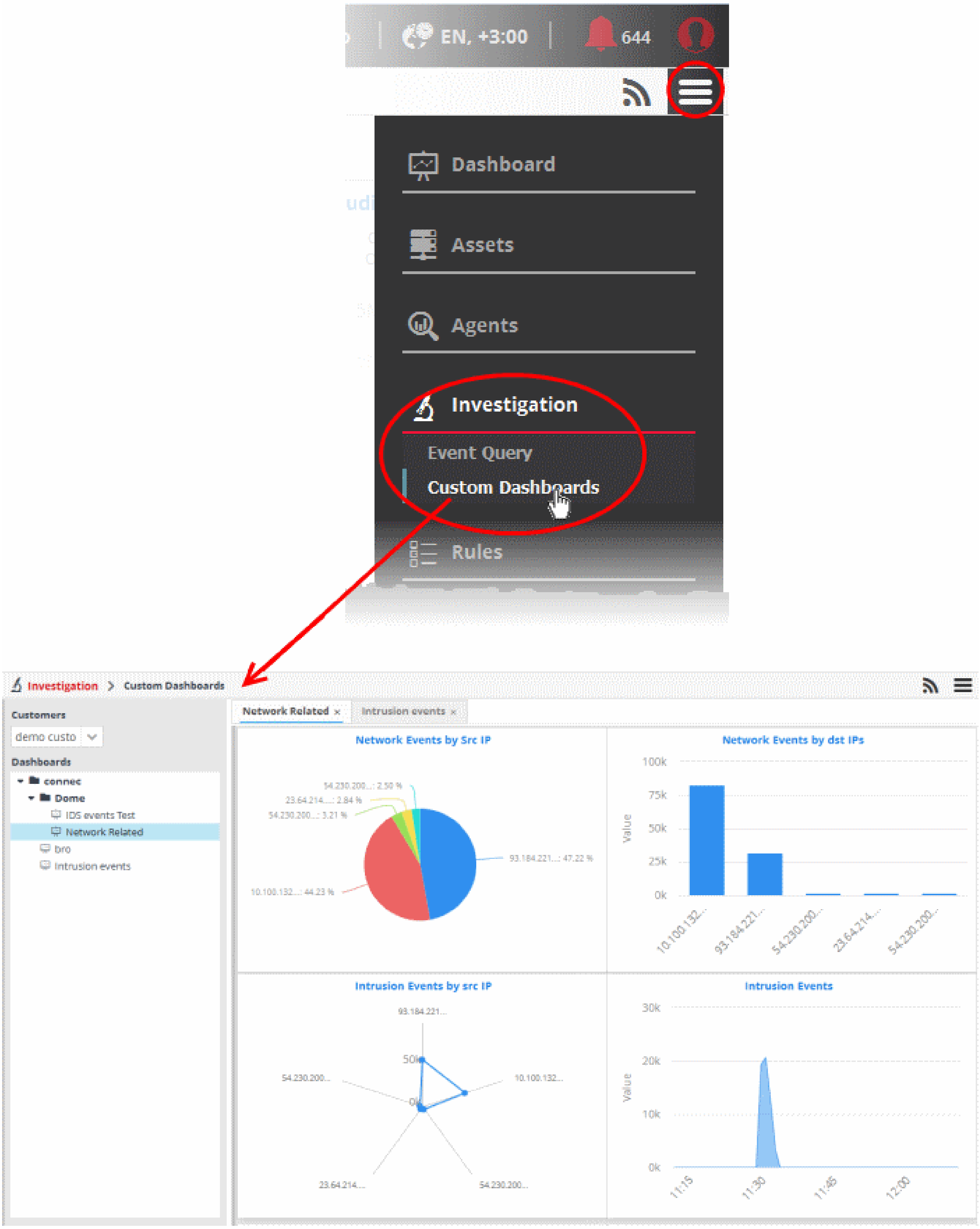
A new filter will be added with the parameter contained in the field chosen from the 'Details' pane

- To save the query with the new filter, click 'Save'.
- To create a new query with the existing and newly added filters, leaving the existing query unchanged, select the category folder from the left click 'Save as' and save the new query with a new name.

## 6.2 Configuring Custom Dashboards

The 'Custom Dashboards' interface allows administrators to view 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, administrators can more effectively track, monitor and analyze the activities of their customers. Refer to the section '**Configuring Event Queries**' to know more about event queries.

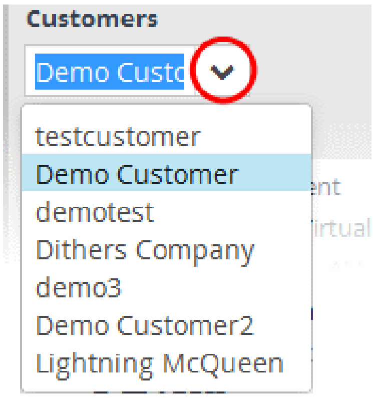
To open the 'Custom Dashboards' interface, click the 'Menu' button from the top right, choose 'Investigation' and then click 'Custom Dashboards'.



The left hand side panel of the interface displays a list of predefined queries and custom queries added for the selected customer under respective folders. The right hand side panel displays the custom dashboards generated for the queries selected from the LHS pane under respective tabs.

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

Each dashboard tab can displays four charts for the selected query.

| Custom Dashboards Interface - Table of controls | |
|---|---|
| <br>Customers<br>Demo Custo<br>testcustomer<br>Demo Customer<br>demotest<br>Dithers Company<br>demo3<br>Demo Customer2<br>Lightning McQueen | The 'Customers' drop-down allows you to select the customer for which you want to query events and/or add custom queries. |
| | Allows you to add a new 'Dashboards' folder to the left side panel |
| | Allows to edit the name of a 'Dashboards' folder |
| | Allows you to a add a new dashboard by selecting an event query added for the selected customer. |
| | Allows to delete selected dashboards folders or dashboards. |

The interface allows administrators to:

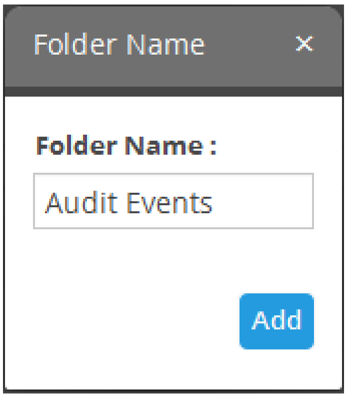
- Manage Dashboard folder
- Configure a custom dashboard
- Create an event query for specific events from the Dashboard
- Edit a dashboard tile
- Delete a dashboard tile

## Managing Dashboard Folders

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

**To create a new Dashboard Folder**

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

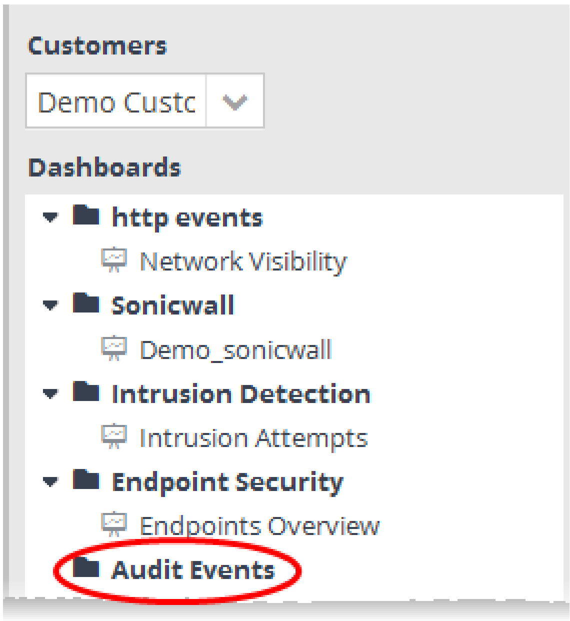


Folder Name ×

Folder Name : Audit Events

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

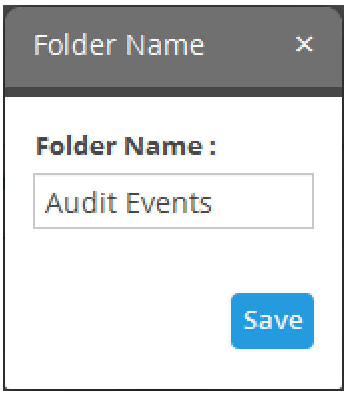
The folder will be saved and displayed on the left side



You can add new dashboards under the folder.

**To edit the name of a dashboard folder**

- Select the folder and click the button at the bottom



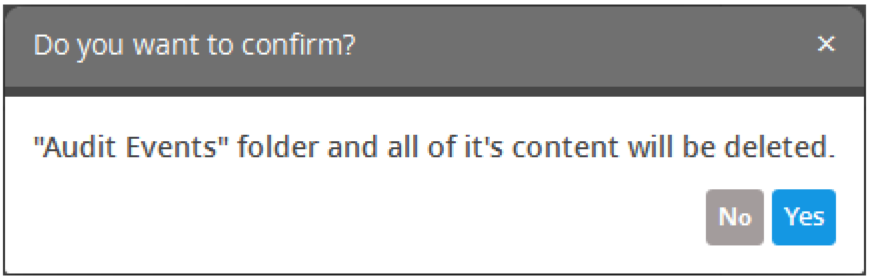
Folder Name : Audit Events

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

**To delete a custom dashboard folder**

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

The confirmation dialog will appear.



"Audit Events" folder and all of it's content will be deleted.

- Click 'Yes' to confirm the deletion.

## Configuring Custom Dashboards

You can add any number of custom dashboards for a customer for different event queries. If required, you can create new queries specifically for custom dashboards and save them, from the Event Query interface. For a tutorial on creating new queries, refer to the explanation of **Manage an Event Query** in the section **Configuring Event Queries**.

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

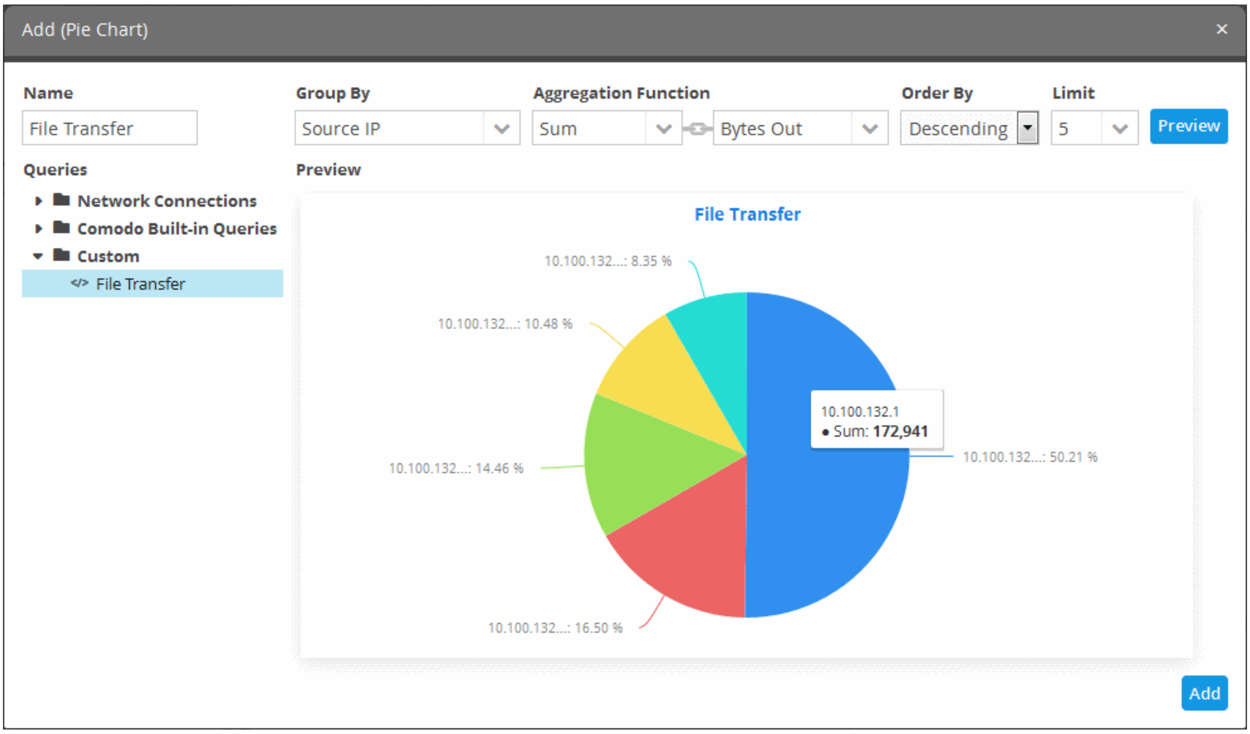
'Name' +'Selected Event Query' + 'Group By' + 'Aggregation Function' + 'Order By' + 'Limit'

- 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. The events that are detected based on the query for the last one hour will be displayed in the charts.
- Group By - The field, based on whose values, the events identified by the query are to be grouped and shown in the chart. Event groups will be formed so that each event group will have events with same value for the selected field.
- Aggregation Function - The event groups formed based on the fields chosen in the 'Group by' option, are ranked based chosen 'Aggregation Function'. The event groups are indicated in the charts in ascending or descending order as chosen in the 'Order by' setting. The available options are:
  - Count - 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 view the 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

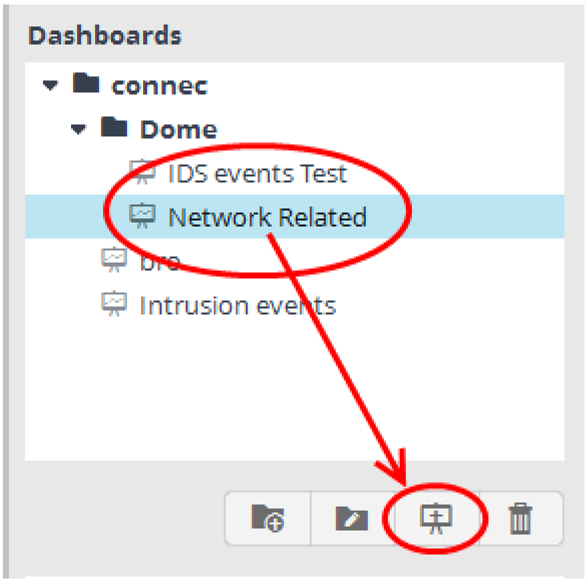
Aggregation Function: Sum — Bytes Out

Order By: Descending

Limit: 5

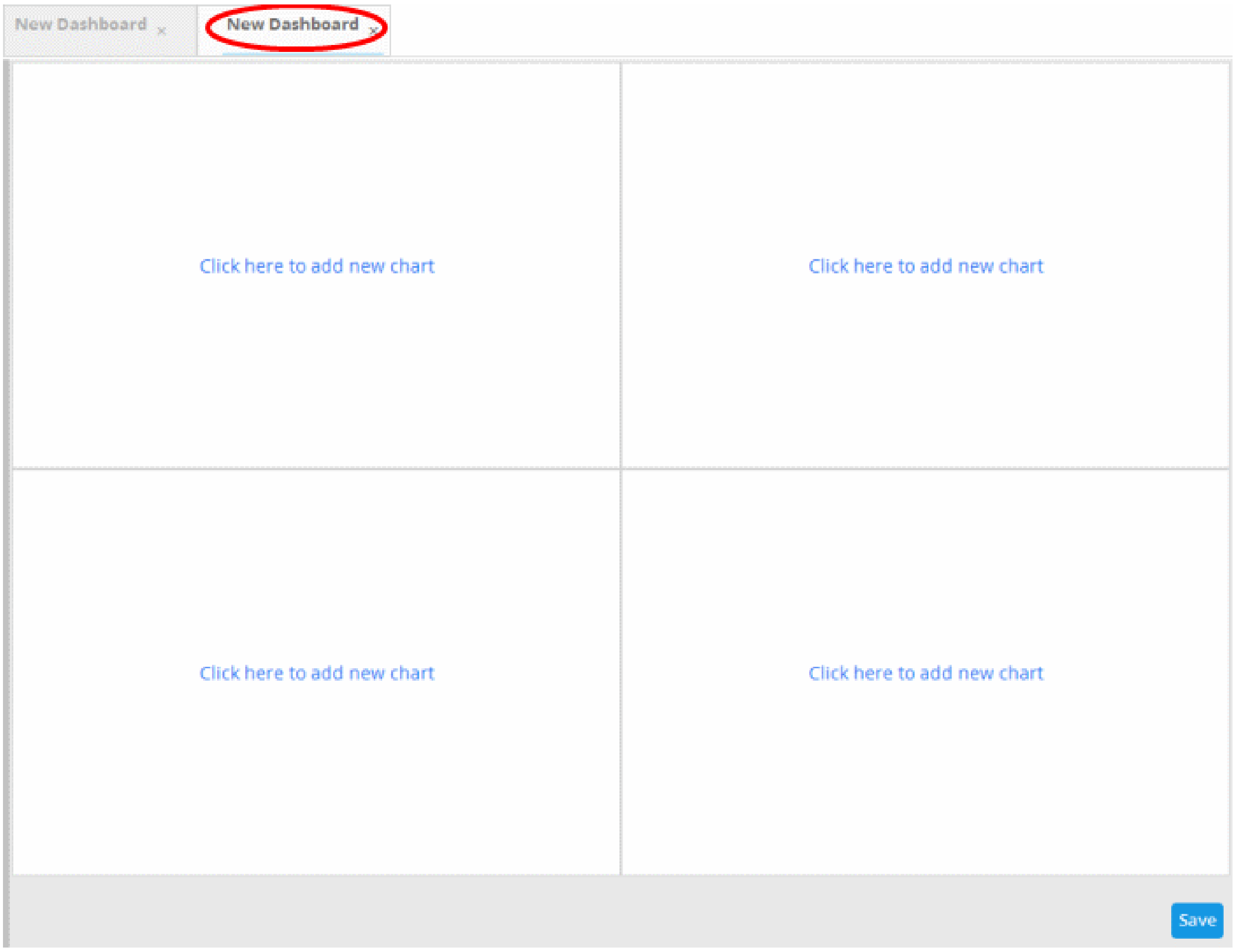
**To create a new dashboard**

- 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.

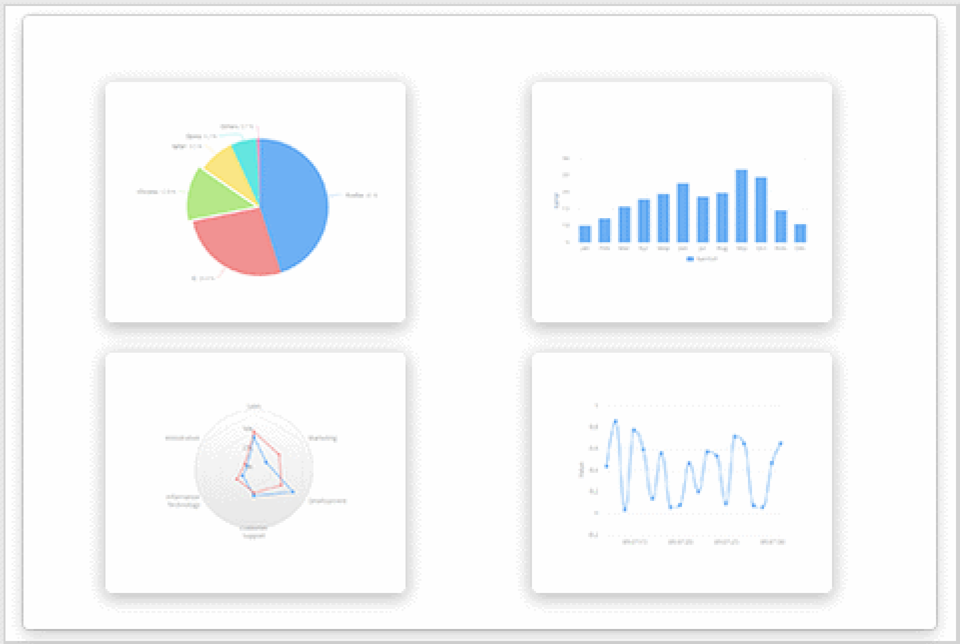
**Tip**: You can also use the 'New Dashboard' tab that is displayed as the first tab on selecting a customer, to create a new dashboard. You can save the created dashboard by selecting an appropriate folder from the left side panel.


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.

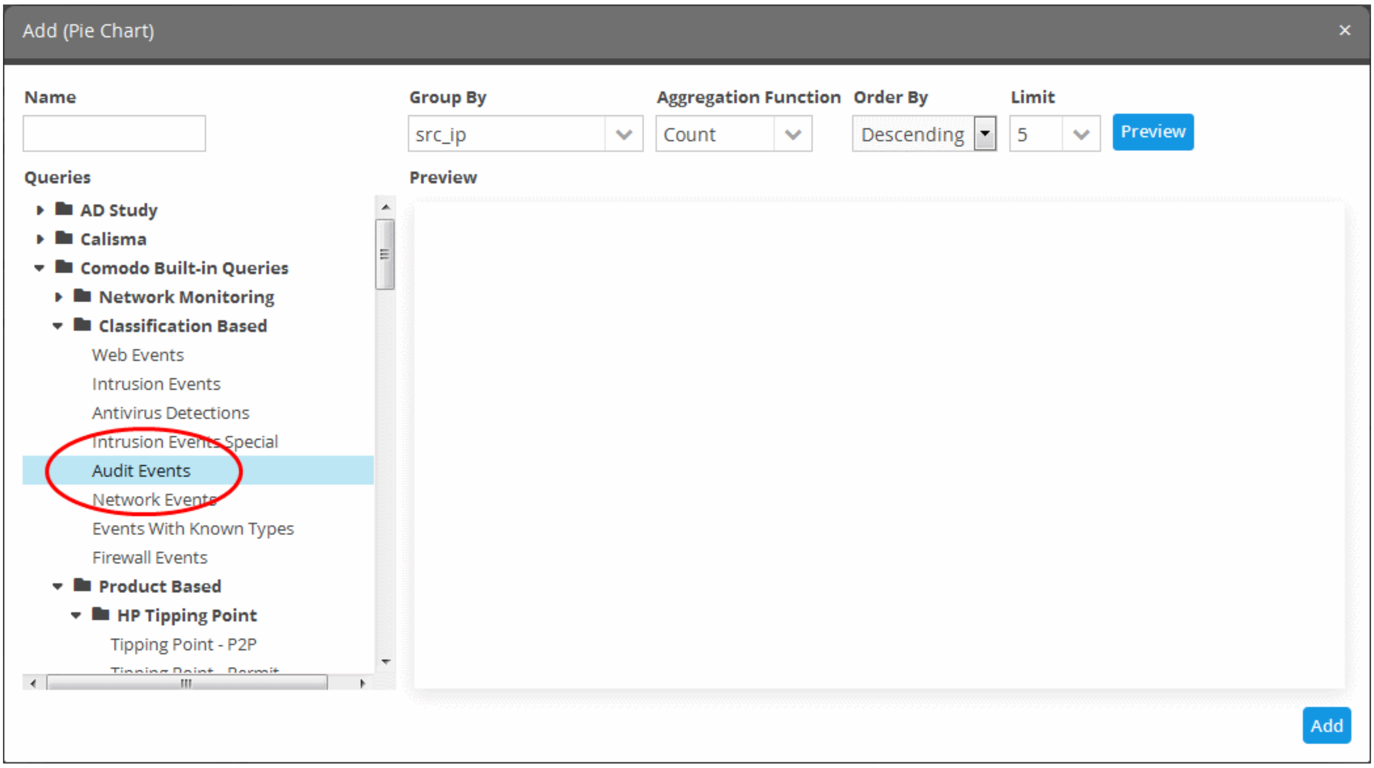


The available options are:

- 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.

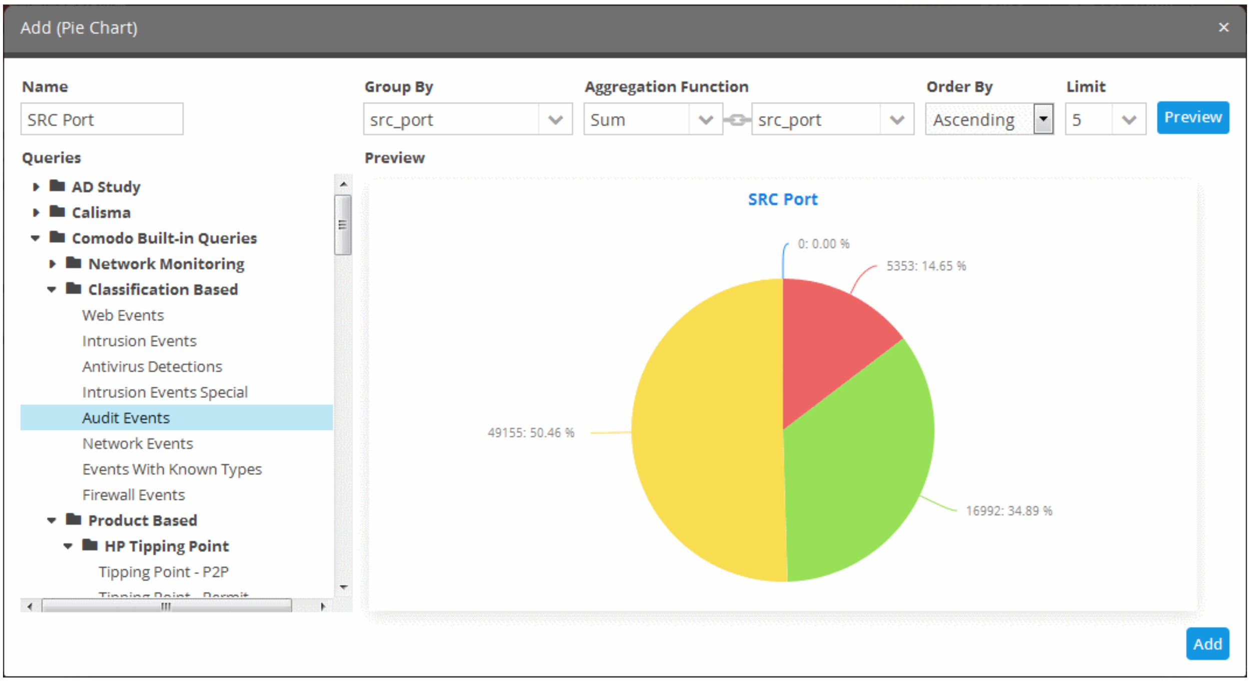


The left hand side pane allows you to enter a name for the chart and displays the list of event queries that were pre-configured for the customer's network. You can select the event query for which the chart is to be displayed, from the list. The right hand side pane displays options for configuring the chart and a preview pane.

| Add Chart - Form Parameters | |
|---|---|
| **Parameter** | **Description** |
| Name | Enter an appropriate name for the dashboard tile |
| Queries | Displays the list of predefined and custom event queries added for the selected customer. Select the event query for which the results are to be displayed in the chart. |
| Group By | The drop-down displays the fields, configured as event query results table column headers for the selected event query. Refer to '**Configure results table for a query**' for more details.<br>Choose the Field based on whose values, the events identified by the query are to be grouped and shown in the chart. |
| Aggregation Function | Allows you to choose the aggregation operation to be applied for ranking the event groups and show them in ascending or descending order, in the chart. The options available are:<br>• 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.<br>• Sum - The event groups are ranked based on sum of values in another field that contains numerical value. If you choose 'Sum', you need to select another field that contains a numerical value, like bytes in/out. The event groups are ranked based on the sum of the values in the chosen numerical field from all the events in that group. For example, if we |

| | |
|---|---|
| | choose 'Bytes-in' as numerical value, then the system adds up the values in the 'Bytes-in' field of all the events in a group and ranks the group accordingly. This will tell you which source IP has the most incoming traffic. The event group with the highest SUM in the 'Bytes-in' field is ranked top and vice-versa.<br>• 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).<br>• 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.<br>• 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 | Allows you to choose the order in which the event groups are to be indicated in the chart, based on their ranking. The available options are:<br>• **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.<br>• **Descending** - The group with the highest rank will be top of the list. A limit of 5 will show the 5 groups with the highest ranks. |
| Limit | Enter the number of events to be displayed for the chart |
| Preview | This button allows to preview the chart before adding it to the tile |
| Add | Click this button to add the chart to the dashboard tile |

- Enter the parameters for the chart as shown in the table above and click the 'Preview' button to check the chart before adding it to the dashboard tile



Add (Pie Chart)

Name: SRC Port

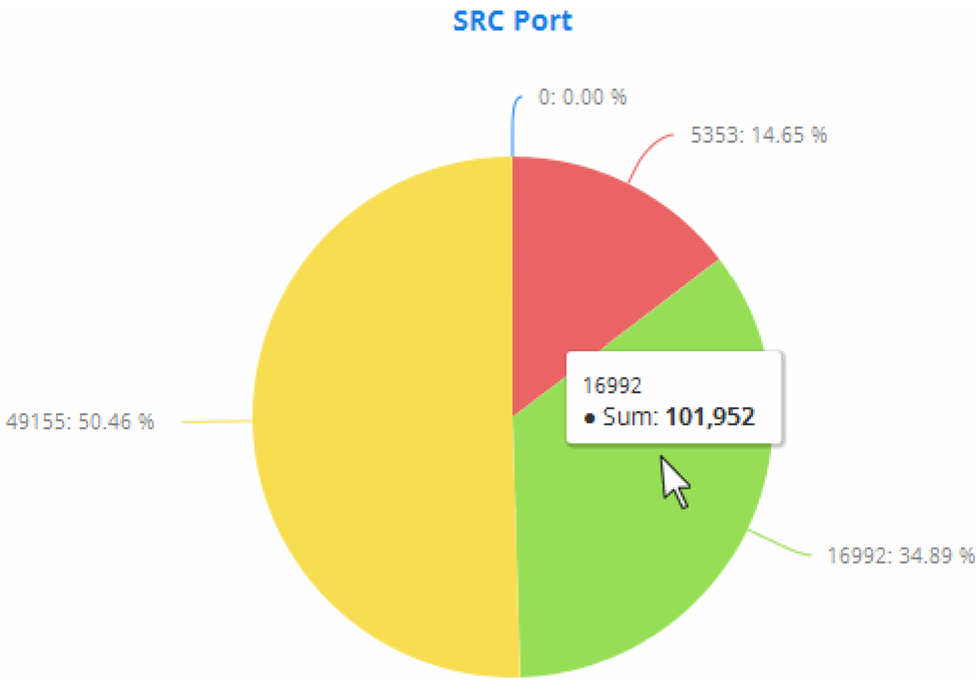
Group By: src_port

Aggregation Function: Sum src_port

Order By: Ascending

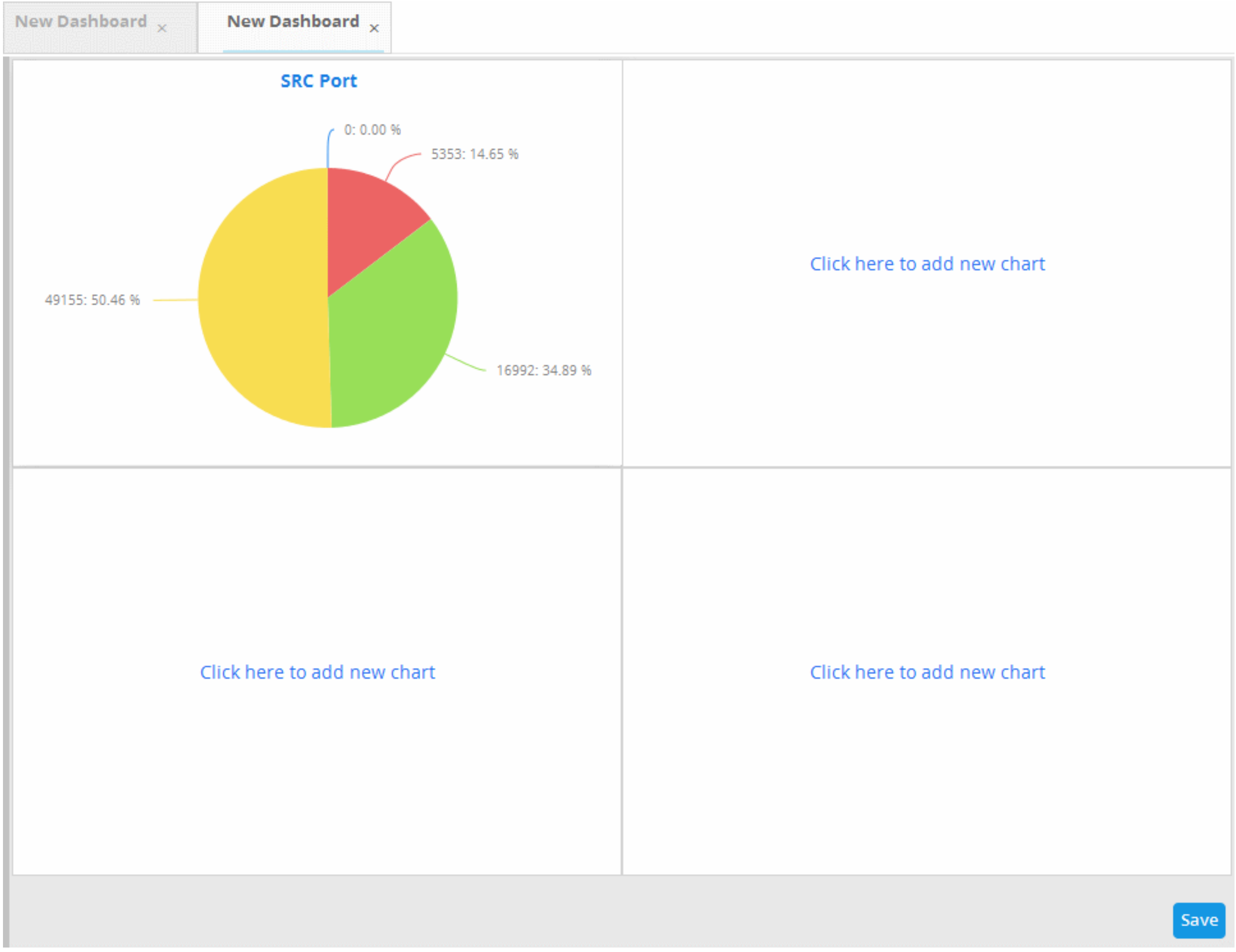
Limit: 5

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

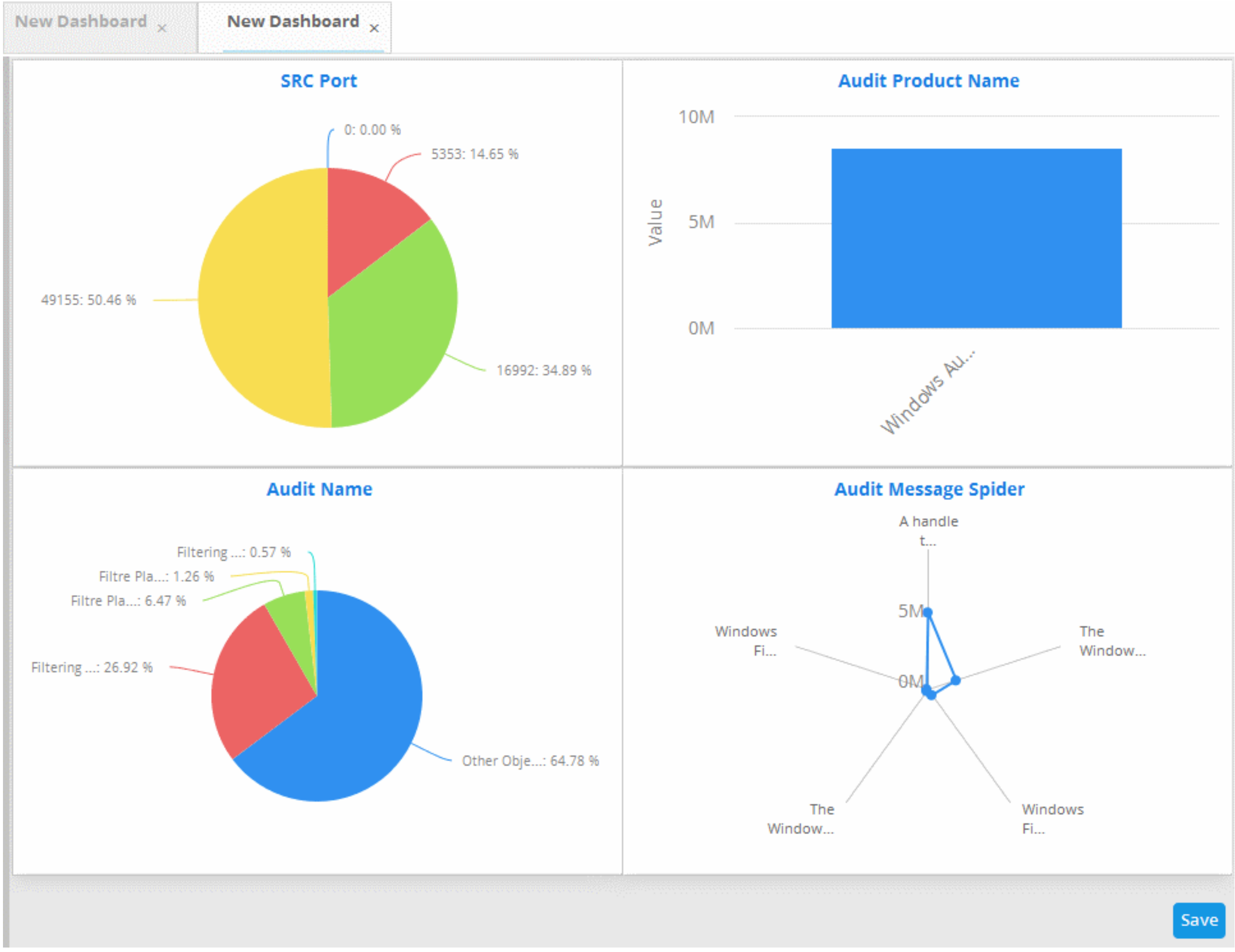


- Click the 'Add' button

The configured tile will be added to the dashboard.

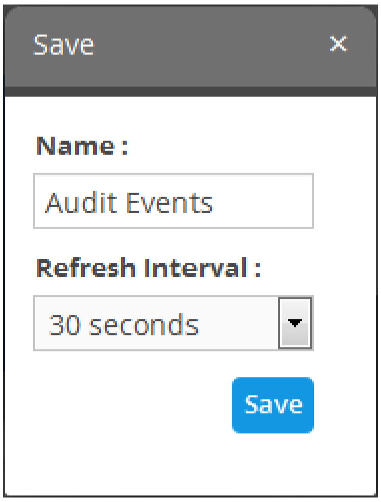


- Repeat the process to add more number of tiles to the dashboard as explained **above**.



- Click the 'Save' button.

The 'Save' dialog will appear.

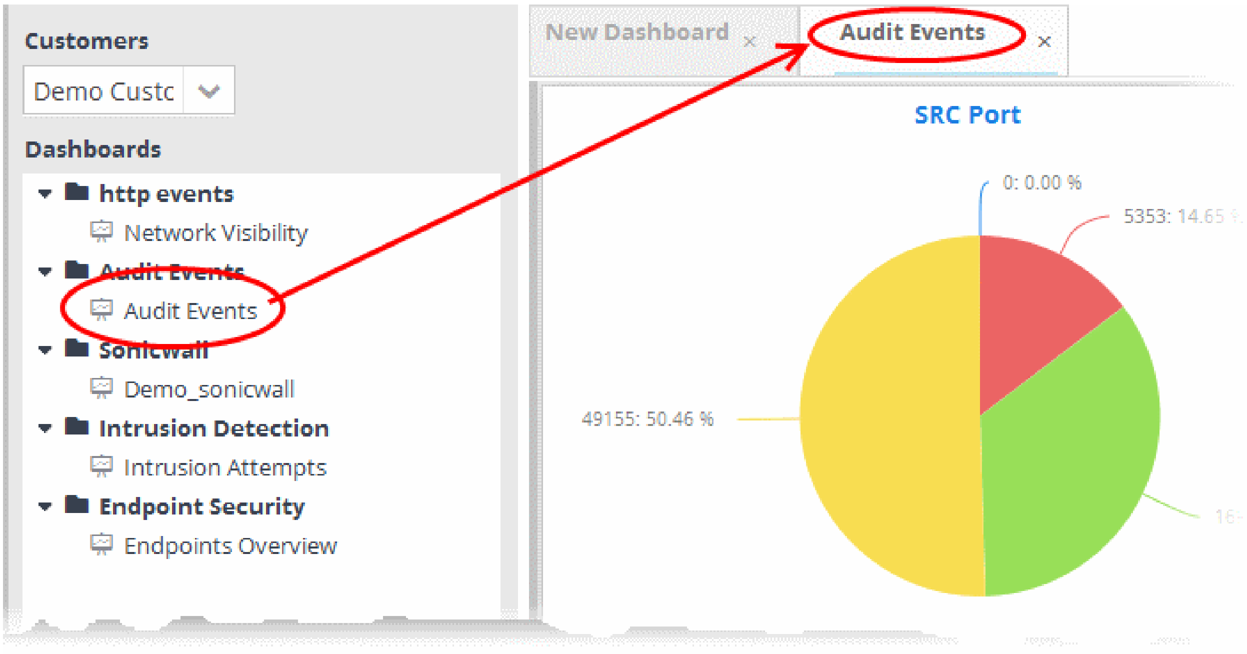


Name : Audit Events

Refresh Interval : 30 seconds

- 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.



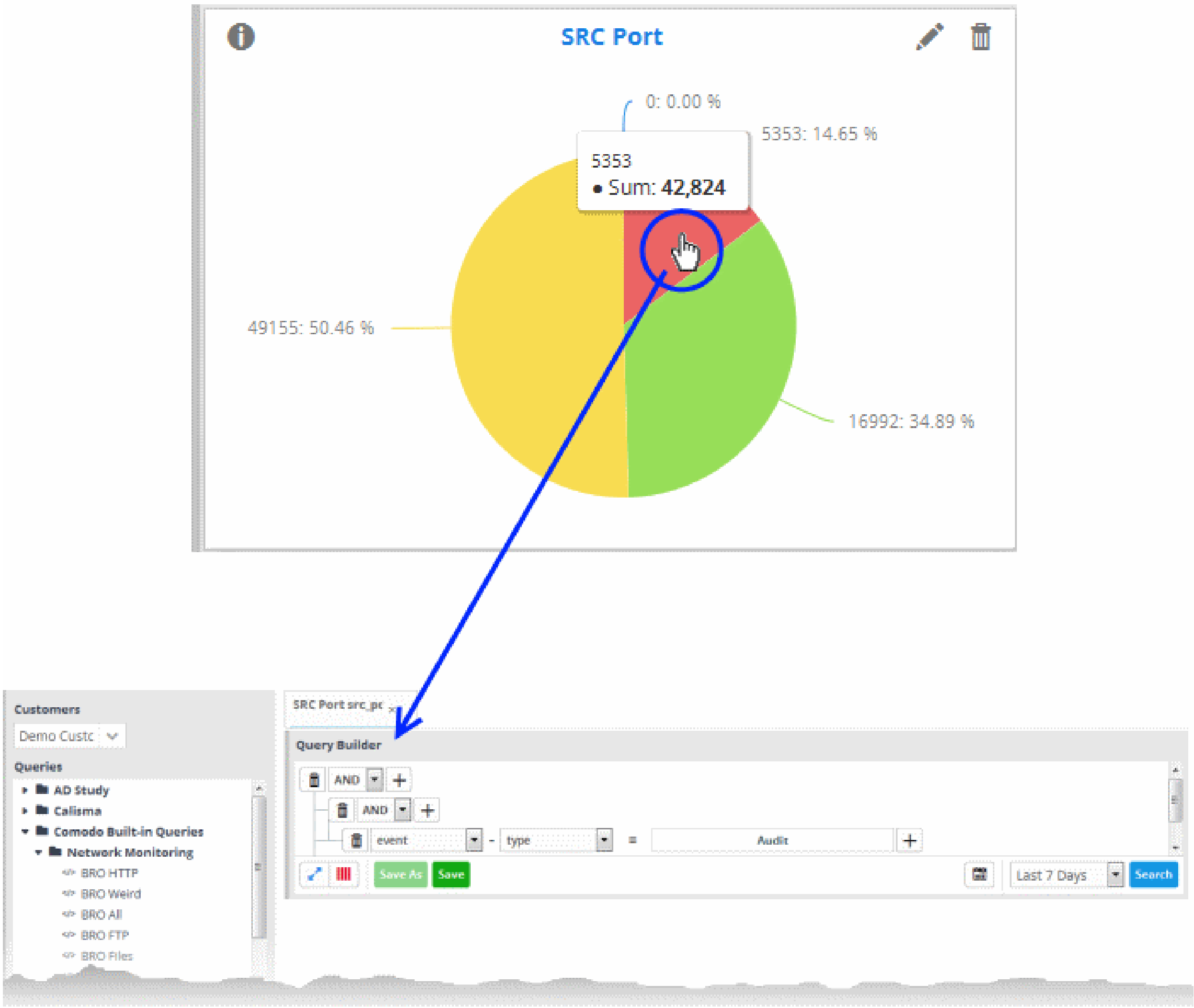
You can add as many custom dashboards for various event queries configured for a customer by repeating the same process.

## Creating an Event Query for Specific Events from the Dashboard Chart

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

**To create a new query**

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



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

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

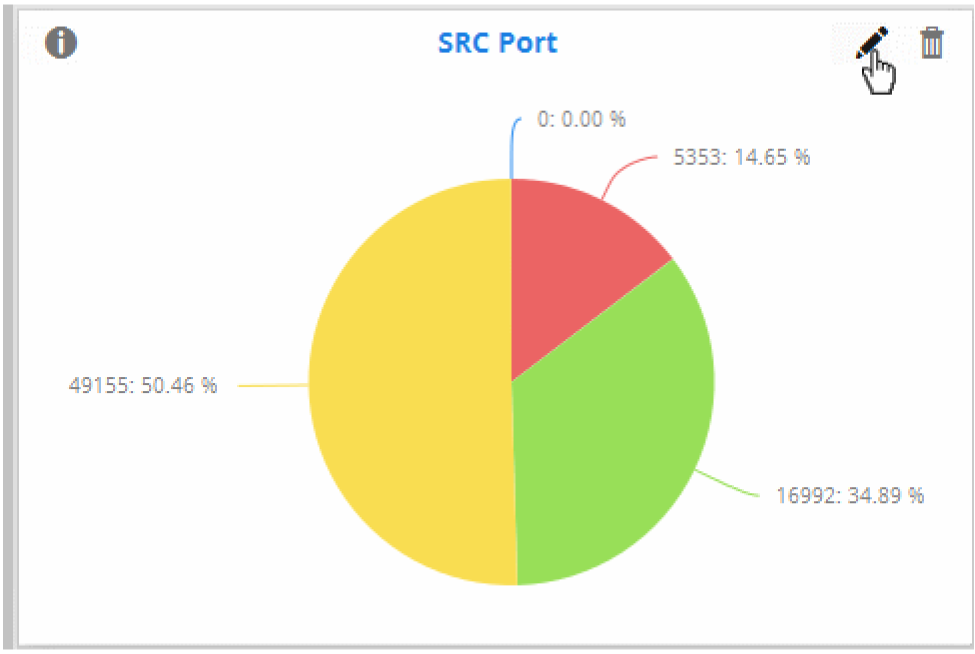
The Query will be saved. You can search for the events at anytime using the query.

## Editing a Dashboard Tile

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

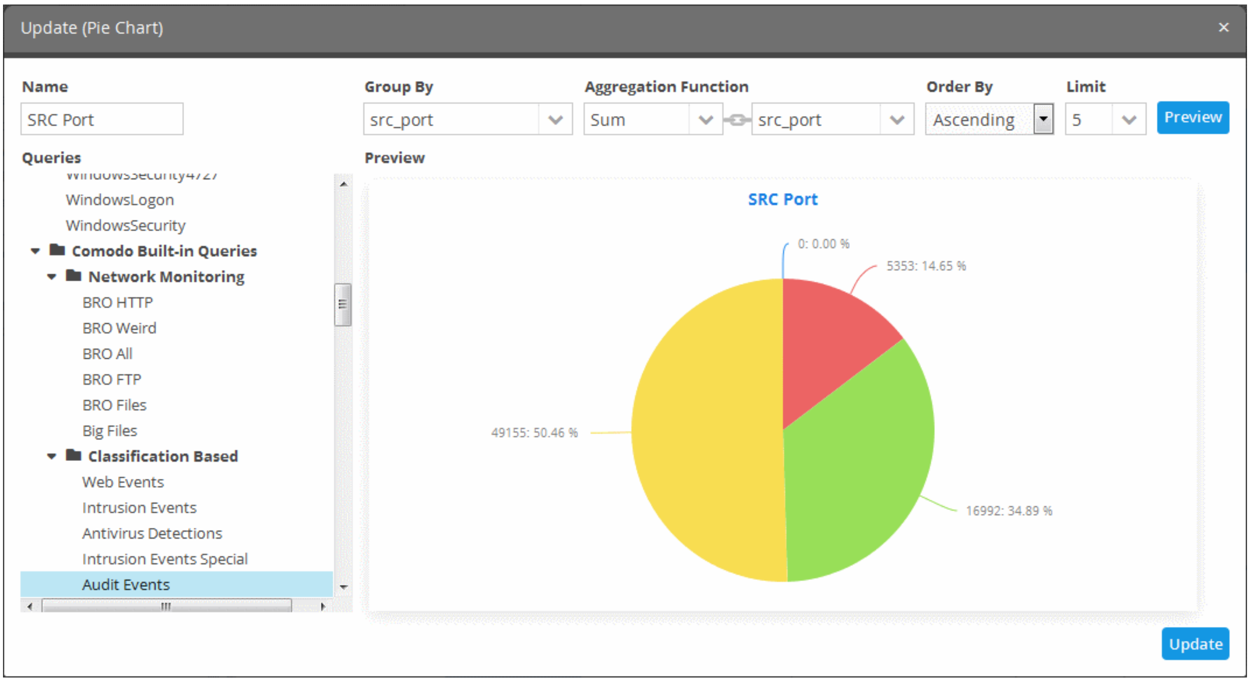
**To edit a dashboard tile**

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



- Click the 'Edit' icon

The 'Update' screen will appear.



Name: SRC Port
Group By: src_port
Aggregation Function: Sum src_port
Order By: Ascending
Limit: 5

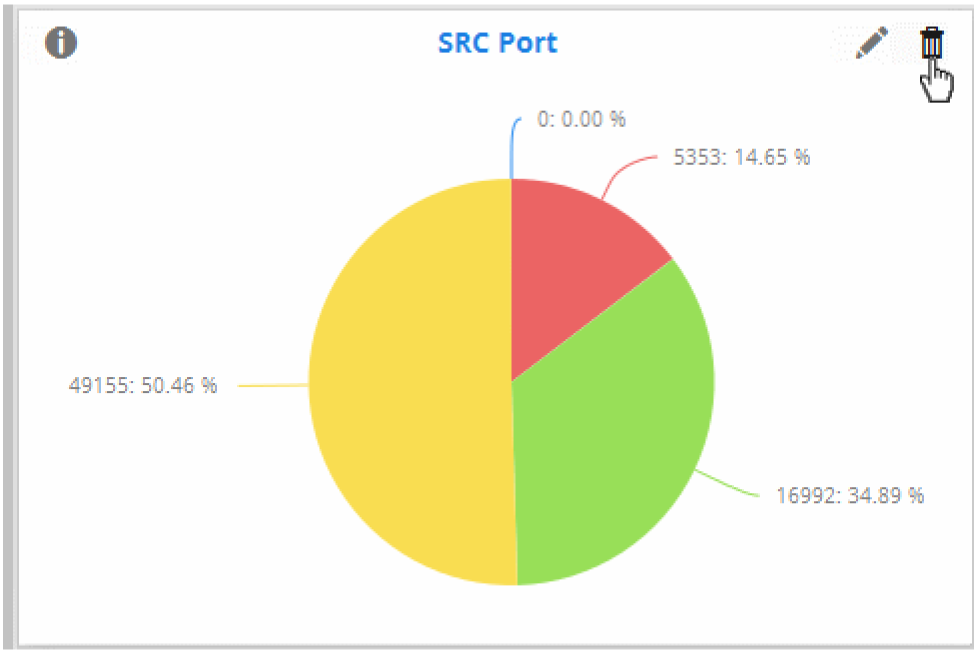
- Edit the chart details as required and click the 'Update' button

## Deleting a Custom Dashboard Tile

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

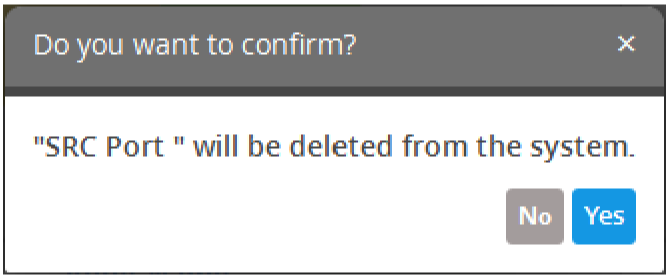
**To delete a tile**

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



- Click the trash can icon.

The confirmation dialog will appear.


Do you want to confirm?

"SRC Port " will be deleted from the system.

- Click 'Yes' to confirm the deletion.

# 7 Managing Rules

NxSIEM identifies events that may cause harm to customer networks (for example, a firewall breach) based on monitoring rules and alerts them as 'Incidents'. The logs collected from the customer networks are checked by the rules engine. If any data matches a configured rule then NxSIEM will immediately generate an alert and create an 'Incident'. Incidents created by rules are classified as 'Correlated Incidents' and automatically assigned to administrative users for their perusal and remedial action. Refer to the section '**Incidents and Cases**' and '**Administration**' for more information.

Rules are created by defining query groups and aggregation parameters based on which the identified events are to be aggregated in the results. Each query group can be created by selecting saved 'Event Queries' and/or by adding new queries.

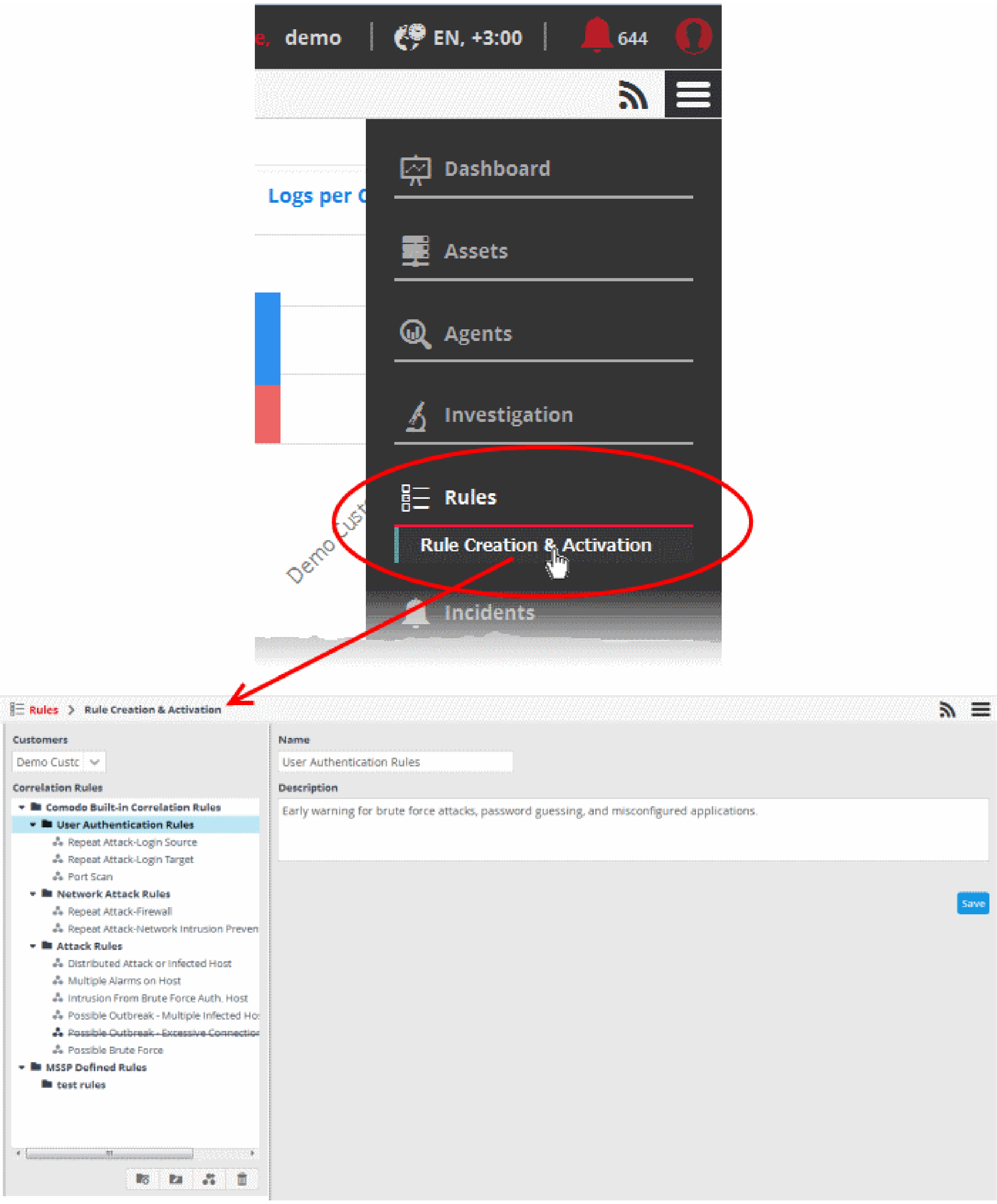
The output from a correlation rule is also created as an event and can be queried from the 'Event Query' interface. Each rule can be configured with 'Output Mappings' that define the fields to be displayed in the result events in the 'Events Query' interface. You can even configure a rule to just to create output events on identifying the events that match the rule and not to create alerts.

Also, selected field values of the outputs of a correlation rule can be used to update entries in Live Lists. Live Lists are configured to contain lists of field values that can be used as query parameters in a query or a rule. If a list is updated, the updated values are automatically reflected in the queries or rule in which the list is used. For more details on managing Live Lists, refer to the section **Live Lists**.

Comodo NxSIEM adds a set of predefined correlation rules under respective category folder for each newly created customer.

The 'Rules Activation and Creation interface' allows the administrator to create and manage the correlation rules for each customer.

To open the 'Rules Activation and Creation' interface interface, click the 'Menu' button from the top right, choose 'Rules' and then click 'Rules Activation and Creation'.



Customers: Demo Custc

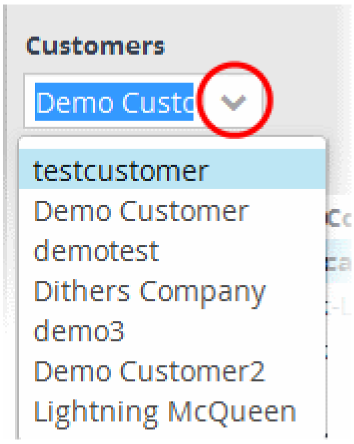
Correlation Rules

- Comodo Built-in Correlation Rules
  - User Authentication Rules
    - Repeat Attack-Login Source
    - Repeat Attack-Login Target
    - Port Scan
  - 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 Connectior~~
    - Possible Brute Force
- MSSP Defined Rules
  - test rules

Name: User Authentication Rules

Description: Early warning for brute force attacks, password guessing, and misconfigured applications.

The left hand side panel displays a list of predefined correlation rules and the custom rules added for the selected customer. The right hand side panel displays the details of the rule chosen from the list and allows the administrator to configure the rule. The rules are added to their respective folders based on their category.

| Rule Correlation and Activation - Table of controls | |
|---|---|
|  Customers<br>Demo Custo<br>testcustomer<br>Demo Customer<br>demotest<br>Dithers Company<br>demo3<br>Demo Customer2<br>Lightning McQueen | The 'Customers' drop-down allows you to select the customer for which you want to manage correlation rules. |
| 📁 | Allows you to add a new category folder for adding the rules. |
| ✎ | Allows to edit the name and description of a 'Rules' folder |
| ⁂ | Allows you to a add new correlation rule under the chosen folder. |
| 🗑 | Allows to delete rules folders or rules |

The interface allows administrators to:

- Manage rules folders
- Manage correlation rules

## Manage a Correlation Rules Folder

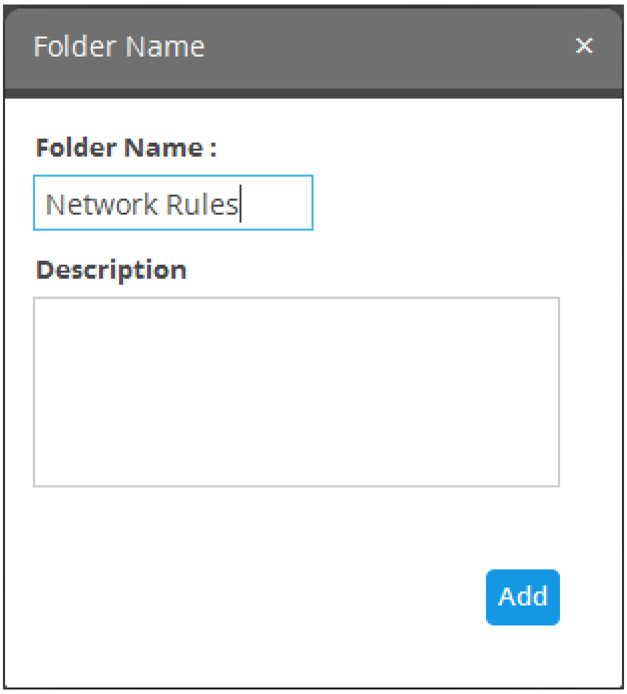
The correlation rules folder contains a collection of rules of specific category. Every new rule must be placed in a rules folder.

### Creating a correlation rules folder

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

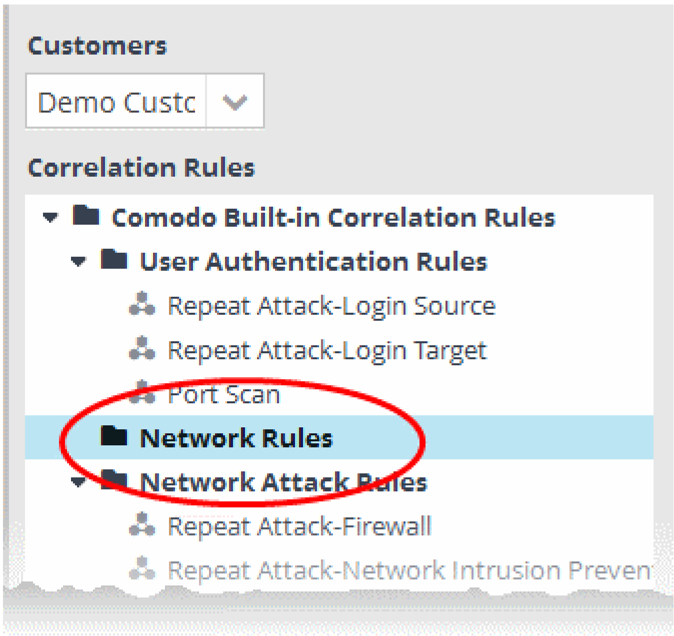
The predefined and custom rules added for the customer is displayed as a folder tree structure in the 'Correlation Rules' pane.

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



- 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

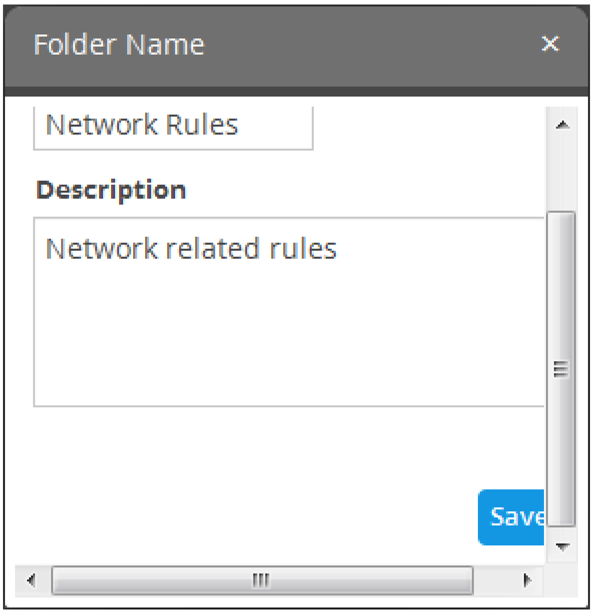
The folder will be saved and displayed on the left side.


Customers
Demo Custc
Correlation Rules
Comodo Built-in Correlation Rules
User Authentication Rules
Repeat Attack-Login Source
Repeat Attack-Login Target
Port Scan
Network Rules
Network Attack Rules
Repeat Attack-Firewall
Repeat Attack-Network Intrusion Preven

The relevant correlation rules can now be placed under the newly created folder. Refer to the '**Manage a Correlation Rule**' section for more details.

**Editing a correlation rules folder**

- Select the folder and click the ✎ button



Folder Name

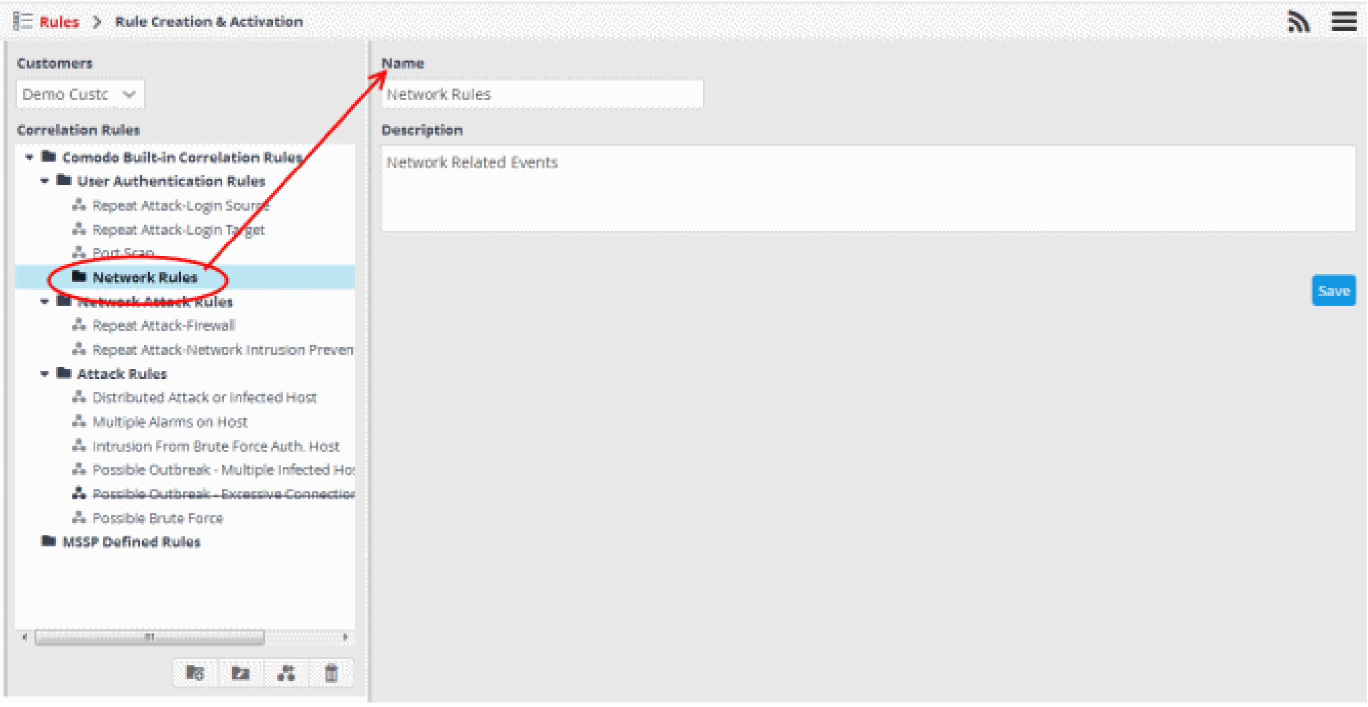
Network Rules

Description

Network related rules

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

Alternatively, click on the folder, edit the details on the right side and click the 'Save' button.



Customers

Demo Custc

Correlation Rules

- Comodo Built-in Correlation Rules
  - User Authentication Rules
    - Repeat Attack-Login Source
    - Repeat Attack-Login Target
    - Port Scan
    - Network Rules
  - 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 Hos
    - Possible Outbreak - Excessive Connectior
    - Possible Brute Force
- MSSP Defined Rules

Name

Network Rules

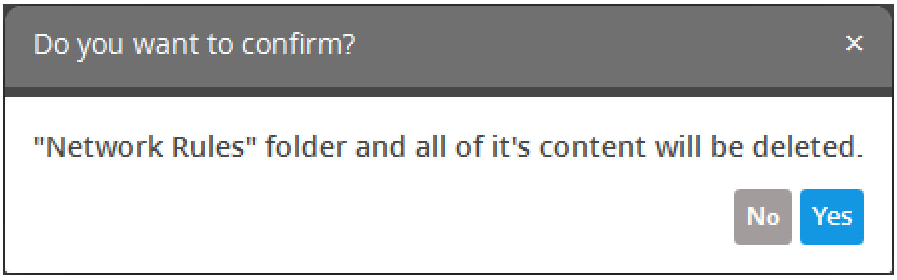
Description

Network Related Events

### Deleting a correlation rules folder

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

A confirmation dialog will appear.



Do you want to confirm?

"Network Rules" folder and all of it's content will be deleted.

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

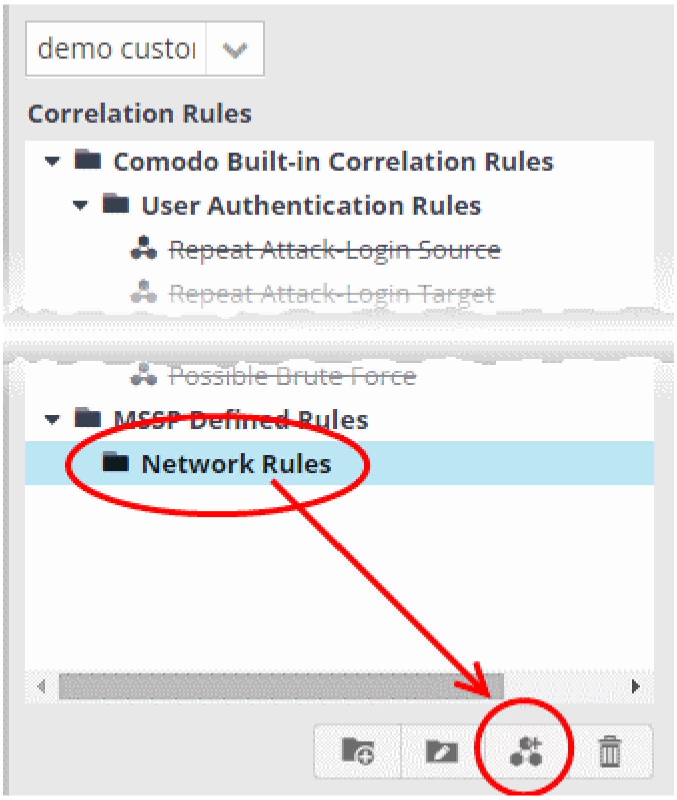
## Configuring a Correlation Rule

The administrator can create correlation rules similar to a query, in order to identify events that might be harmful to the endpoint or the network and to generate an 'Incident'. The identified incidents are automatically addressed to the users allotted for the respective customer for remedial action. A rule is created by adding rule definitions with groups of filter statements and aggregation parameters for aggregating the events that are detected by the rule.

The detection of events based on a rule is also created as an event, that could be queried from the 'Event Query' interface. You can configure the values to be fetched for the fields for the output events generated by the rule every time. This enables the administrator to generate further refined new queries and rules based on output events of a rule. Refer to the explanation of **Output Mappings** for more details.

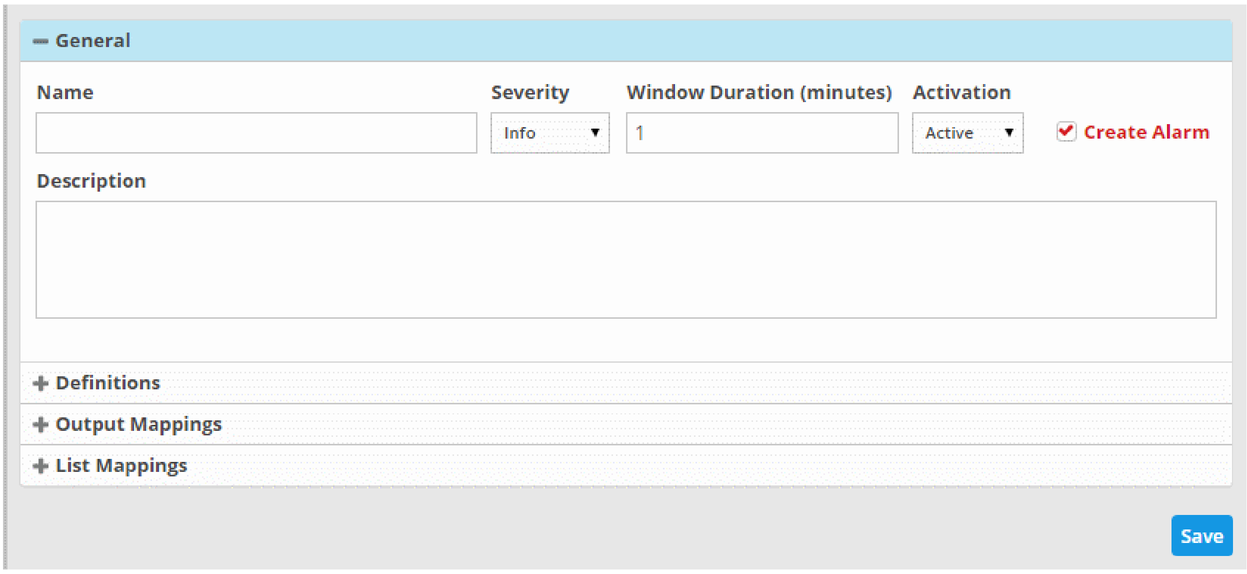
**To create a correlation rule**

- Select the customer from the 'Customers' drop-down on the left side.
- Select the appropriate rule category folder or **create a new correlation rule folder** under which you want to create a correlation rule.
- Click the button



demo custo
Correlation Rules
Comodo Built-in Correlation Rules
User Authentication Rules
~~Repeat Attack-Login Source~~
~~Repeat Attack-Login Target~~
~~Possible Brute Force~~
~~MSSP Defined Rules~~
Network Rules

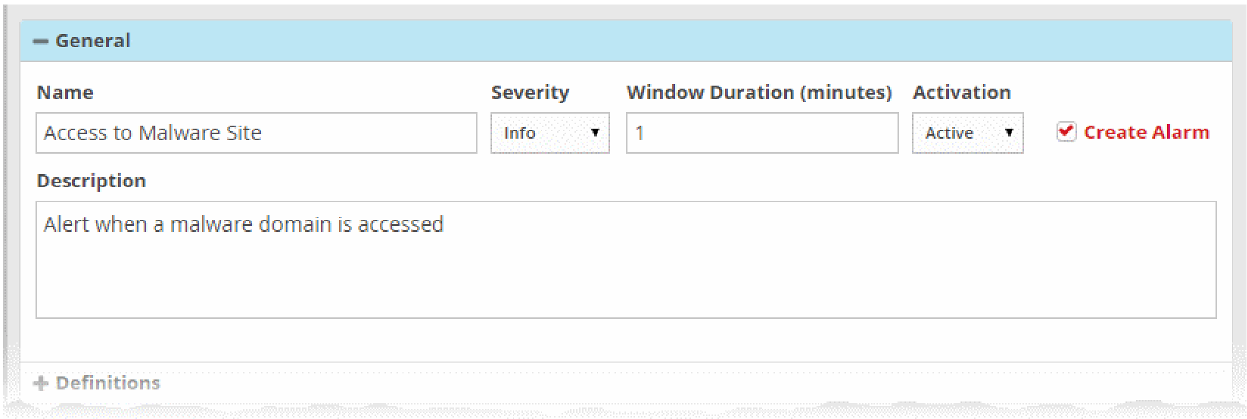
The configuration screen for creating the new rule will be displayed in the right hand side panel. It has four sections:



- **General** - 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).

## General

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



− General

Name: Access to Malware Site

Severity: Info

Window Duration (minutes): 1

Activation: Active

☑ Create Alarm

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. 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
- **Create Alarm** - Configure whether or not an 'Incident' is to be created and an alert is to be sent to the administrator,

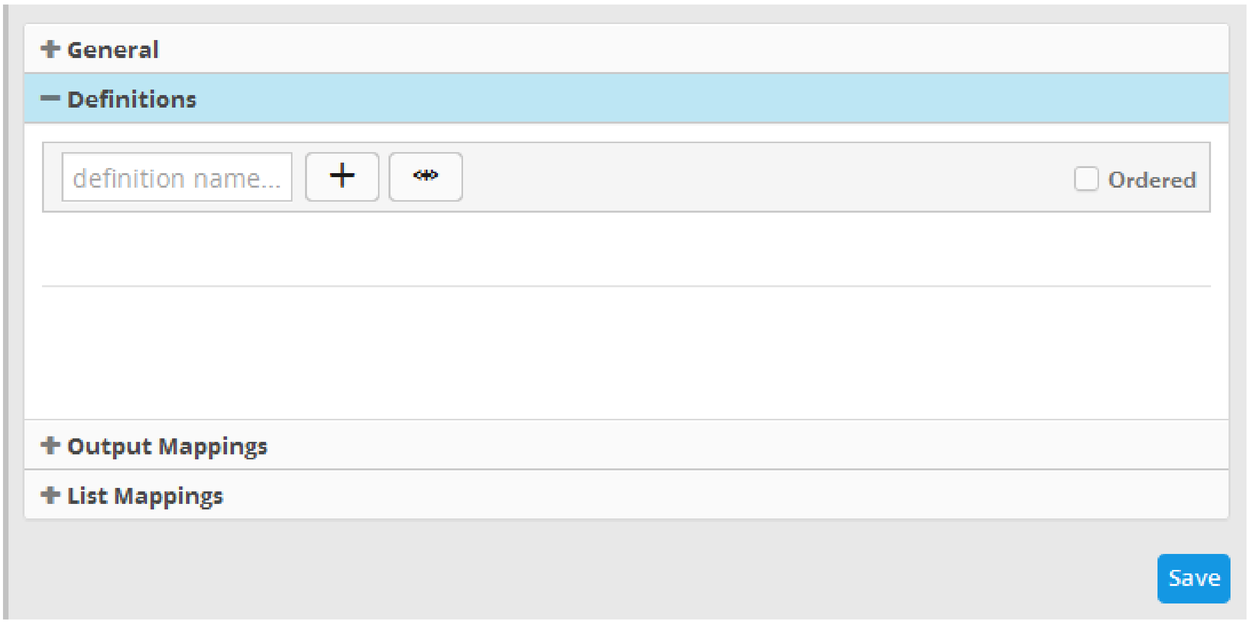
when the rule is met. If selected, the rule creates an incident and an output event which can be queried from the 'Event Queries' interface. Else the rule creates only the output event and does not an Incident.

- **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.



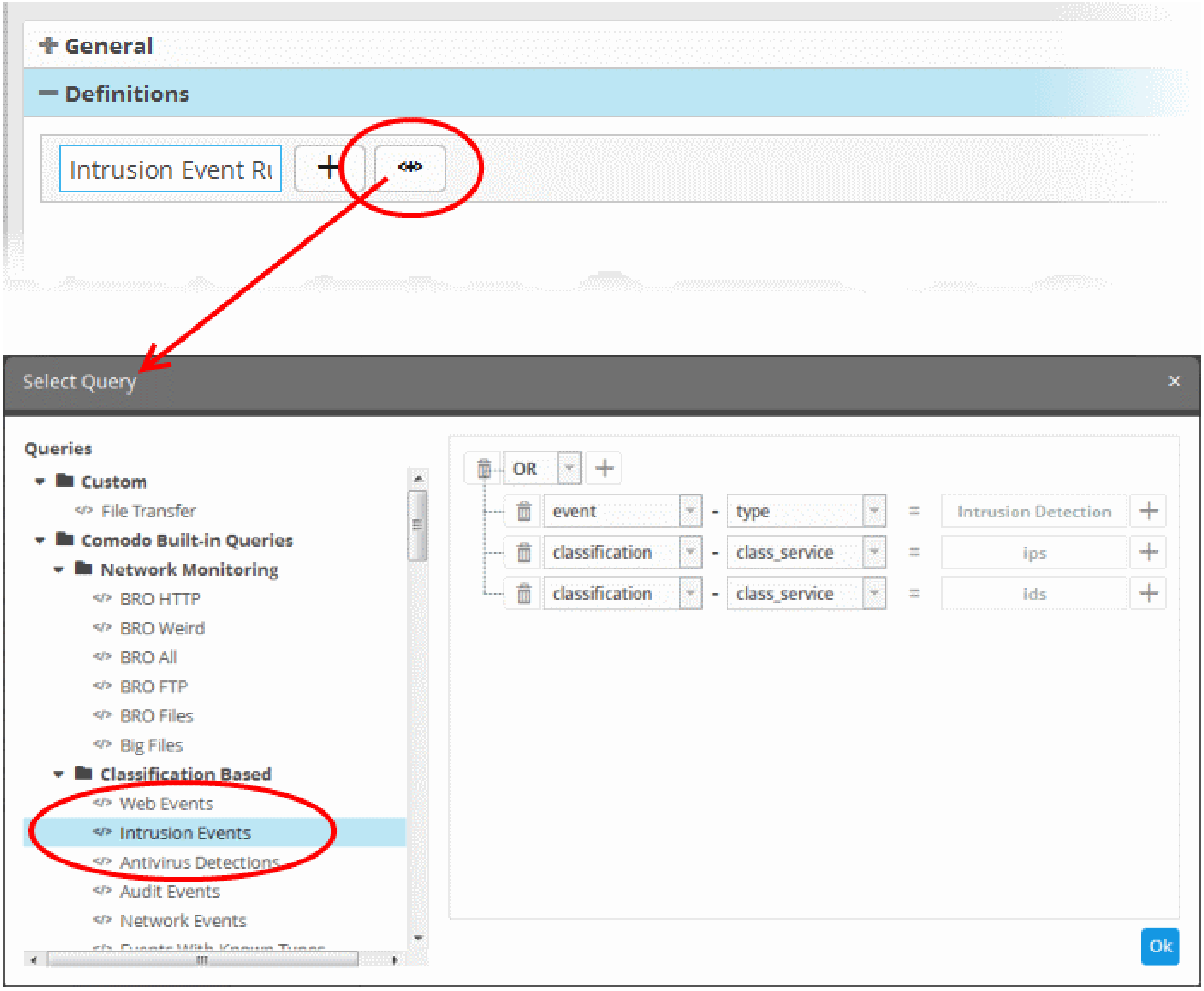
- To add a filter statement group as a rule definition, enter a name for the rule definition.

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.



OR

event - type = Intrusion Detection

classification - class_service = ips

classification - class_service = ids

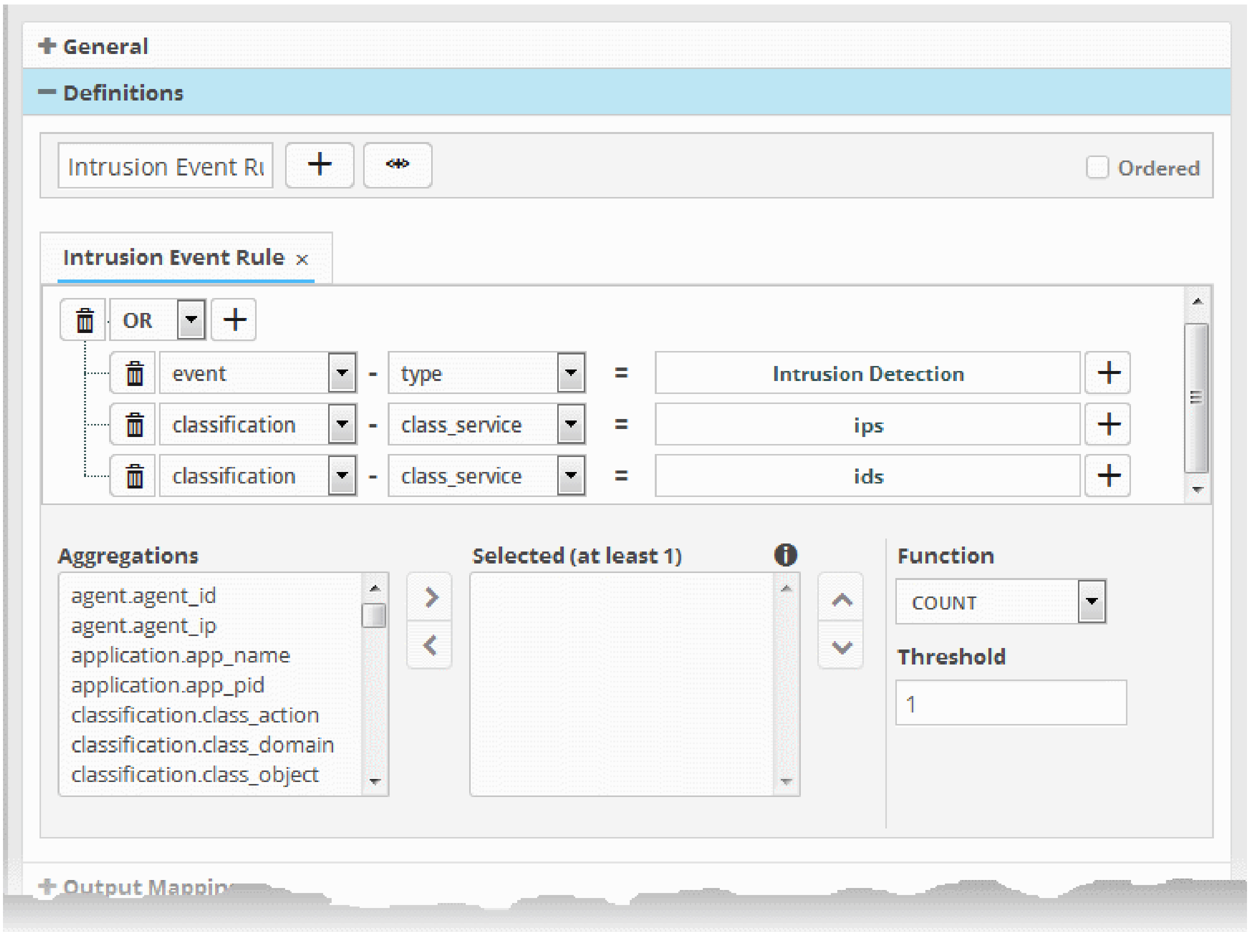
The 'Select Query' dialog will open with a list o pre-defined and custom event queries added for the customer in the left pane.

- 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 .



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 query fields for the definition will open.

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

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

- **Field Group** - The group to which the field specified as the filter parameter belongs.
- **Field** - The field in the event log entry by which you want to filter results
- **Operator** - Controls the relationship between the field and the specified value. Examples include 'Equals to', 'Does not equal to', contains, 'does not contain' etc.
- **Value** - The value for the field. Values can be entered manually or fetched from a pre-defined list which is managed in the '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. Refer to the section **Live Lists** for more details on pre-defined lists.

Examples:

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

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

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

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

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

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

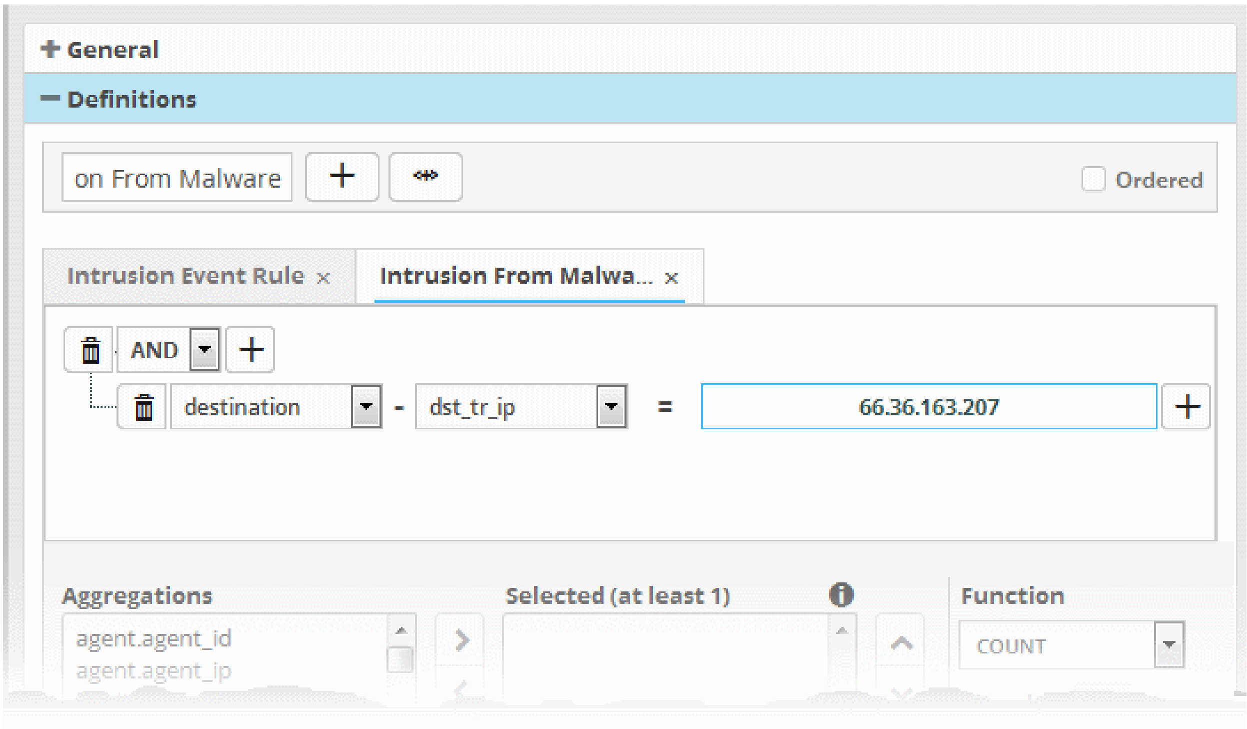
You can create more complex queries by adding more filter statements and linking them using 'AND', 'OR', or 'NOT'. For example:

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

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

**AND**

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



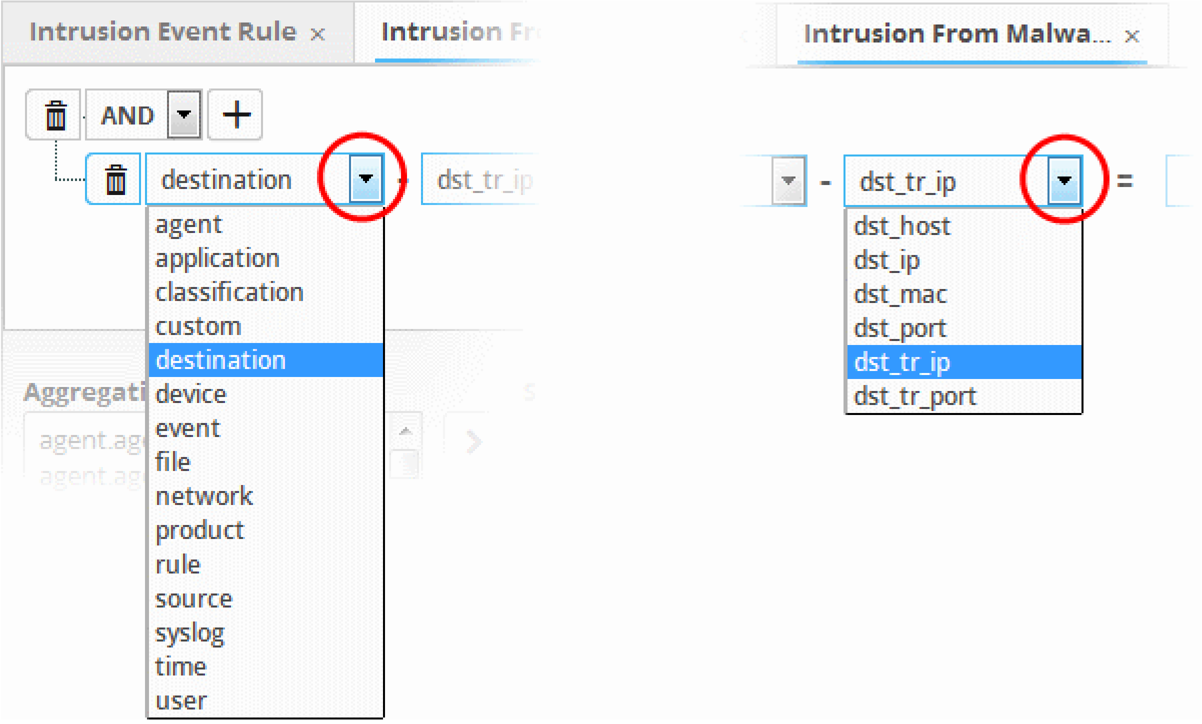
**To manually add a filter statement group**

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

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

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

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

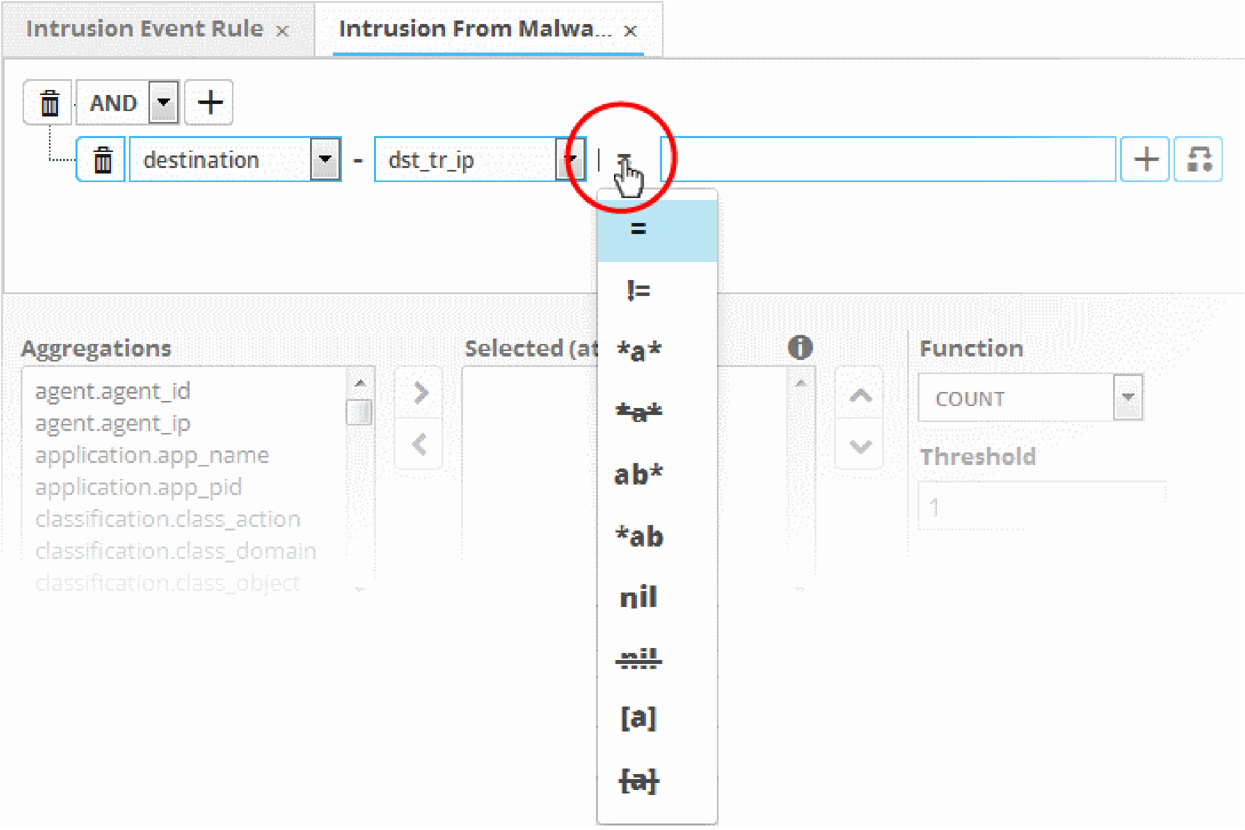


- Choose the field from the second drop-down.

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

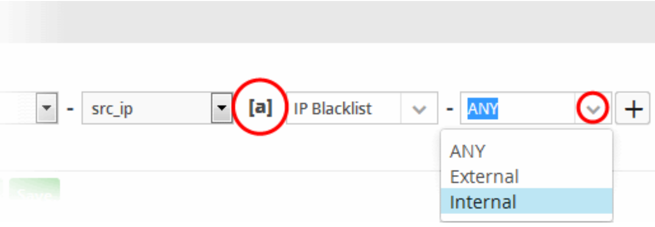
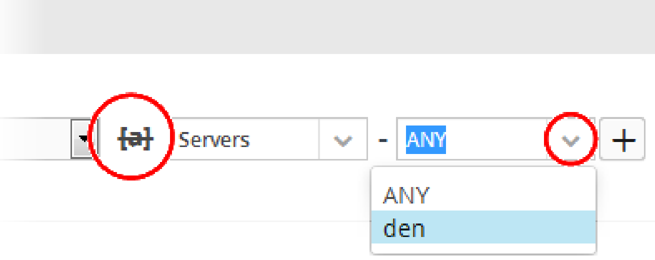
The next step is to choose the relation between the field chosen and the value to be entered in the next field.

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



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

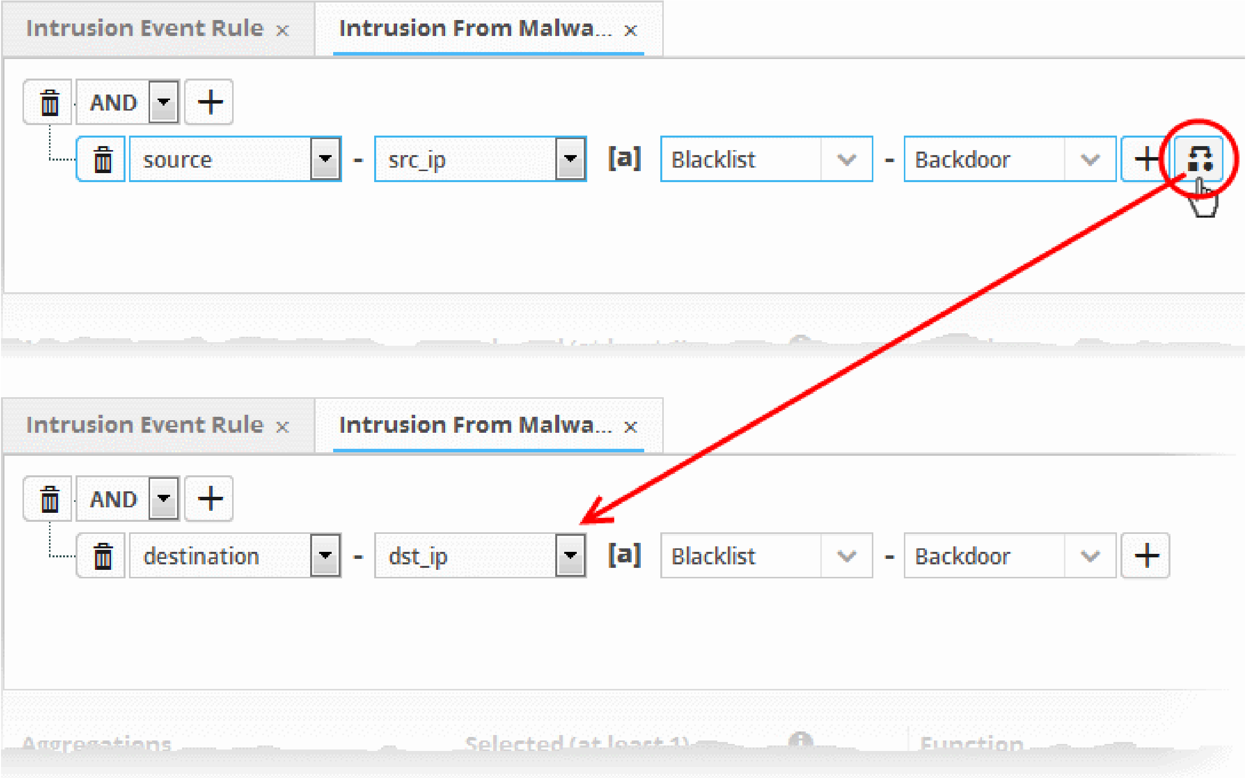
| Relation Operator | Description | Entering the value for the 'Field' |
|---|---|---|
| = | Equals to | Manually enter a value in the field to the right of the operator. Events containing the same value will be identified by the filter. |
| != | Does not equal to | Manually enter a value in the field to the right of the operator. Events that do not contain the value will be identified by the filter. |
| > | Greater than | Applicable only for fields with numerical values, for example, port numbers.<br>Manually enter a value in the field to the right of the operator. The filter 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.<br>Manually enter a value in the field to the right of the operator. The filter 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.<br>Manually enter a value in the field to the right of the operator. The filter will identify events that contain values less than the entered value. |
| <= | Less than or equal to | Applicable only for fields with numerical values, for example, port numbers.<br>Manually enter a value in the field to the right of the operator. The filter will identify events that contain values equal to or lower than the entered value. |
| *a* | Contains | Manually enter a value in the field to the right of the operator. The filter will identify events that *contain* the entered value somewhere in the string.<br>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 filter will identify events that *do not contain* the entered value anywhere in the string.<br>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 filter will identify events that *begin* with the entered value.<br>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 filter will identify events that *end* with the entered value.<br>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).<br>For example, to search for the events with no values in their source IP address fields, select 'Is Empty'. |

<table>
<tr><td>~~nil~~</td><td>Is Not Empty</td><td>Searches for events in which the selected field is not empty (contains a value of some kind).<br>For example, to search for the events with some IP addresses values in their source IP address fields, select 'Is Not Empty'.</td></tr>
<tr><td>[a]</td><td>Is in List</td><td>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.<br><span style="color:red"><b>Background</b></span>:<br>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 section Live Lists.<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 Live Lists that contain values for the selected query field. The second drop-down shows the List Types within the selected 'Live List'.<br>• Choose the Live 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.</td></tr>
<tr><td>~~{a}~~</td><td>Not in List</td><td>Allows you to configure the filter statement to search for the events that do not contain specific values from a pre-defined live 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 Live Lists that contain values for the selected query field. The second drop-down shows the List Types within the selected 'Live List'.</td></tr>
</table>

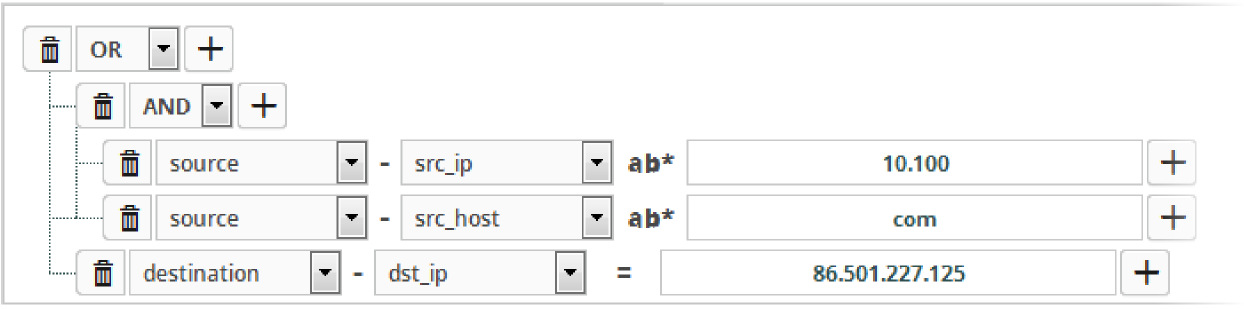
| | | |
|---|---|---|
| | | • Choose the Live List to be used in the query filter from the first drop-down.<br>• Choose the sub list that contains the set of values to be input as exclusions to the query filter from the second drop-down.<br>The results will display all events that do not contain the values in the live 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.


Intrusion Event Rule ×
Intrusion From Malwa... ×
AND +
source - src_ip [a] Blacklist - Backdoor +
Intrusion Event Rule ×
Intrusion From Malwa... ×
AND +
destination - dst_ip [a] Blacklist - Backdoor +
Aggregations
Selected (at least 1)
Function

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


OR +
AND +
source - src_ip ab* 10.100 +
source - src_host ab* com +
destination - dst_ip = 86.501.227.125 +

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

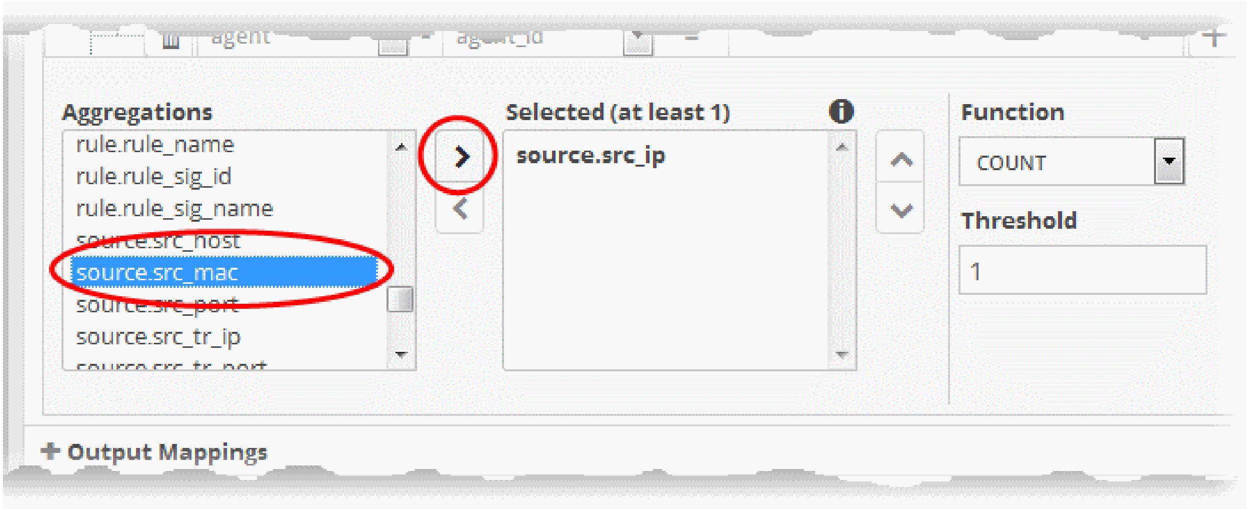
You can add multiple query definitions for a single rule and these are tied together.

- To add a new definition, enter the name of the new definition and add the filter statements as explained above.
- If you want the rules engine to process the definitions of the rule in order, select the 'Ordered' checkbox.

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.



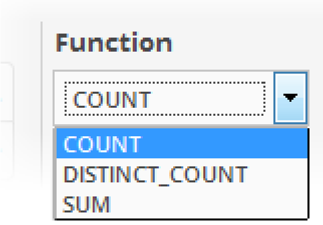
Selected (at least 1): source.src_ip

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 'Rule Creation & Activation' screen.

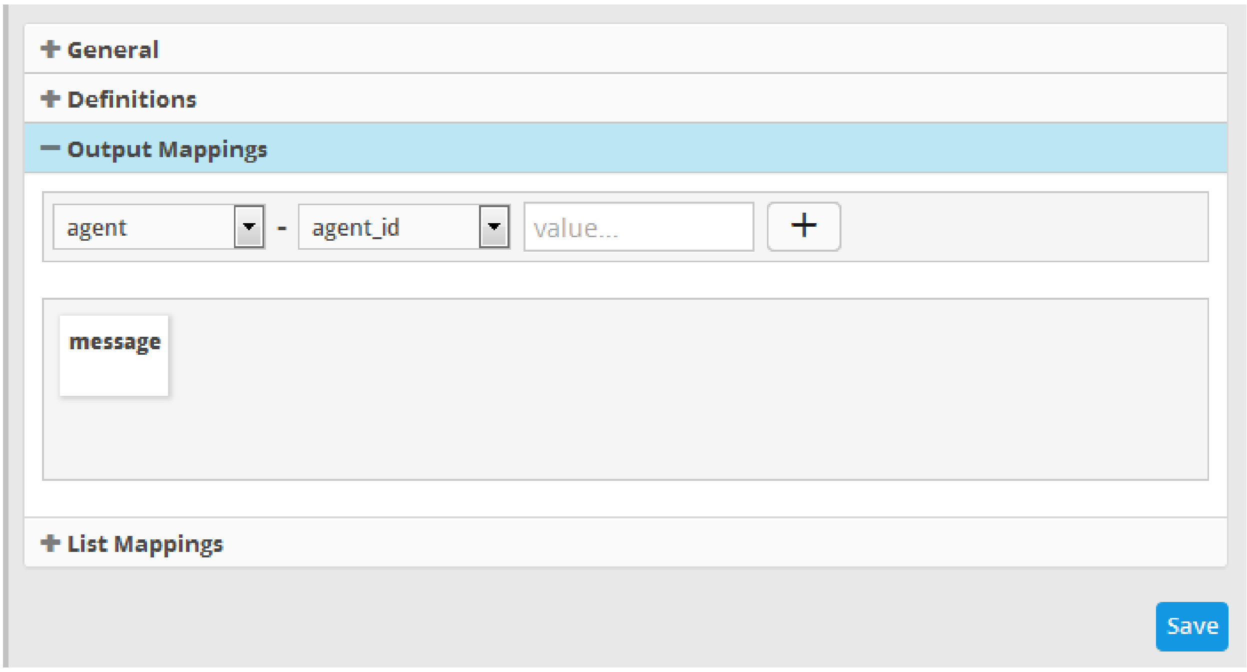
## Output Mappings

In addition to generating an 'Incident', NxSIEM generates a new event as output event every time when events are detected as per a correlation rule. The output event can be queried from the 'Event Query' interface and its details can be used to generate further event queries for the customer.

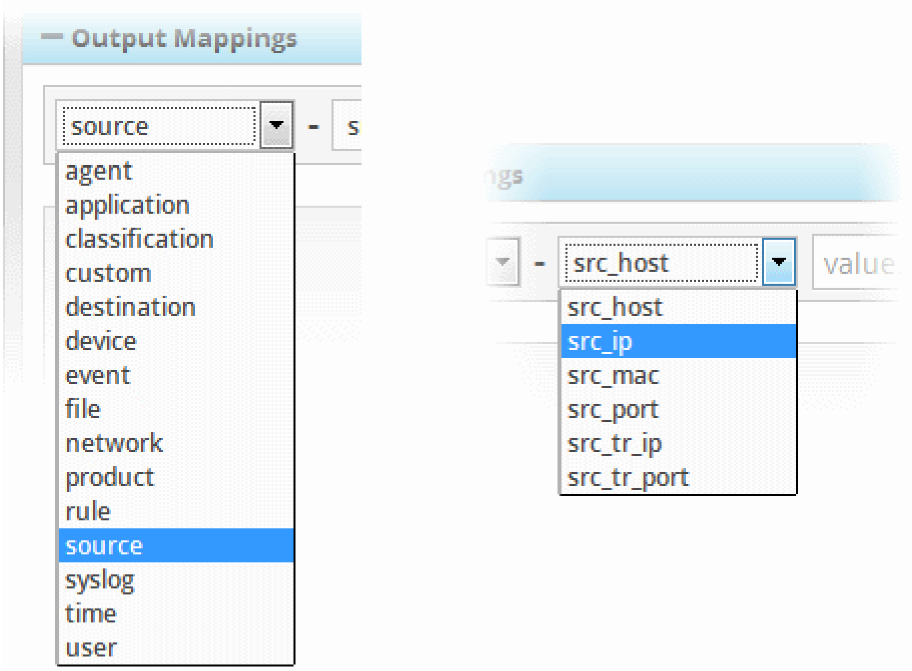
The 'Output Mappings' area allows you to define the values to be fetched for selected fields of the output event from the respective input events detected by the rule. You can choose only values that are common to all the input events that generated an 'Incident' as per the rule.

**To configure output mappings for the rule**

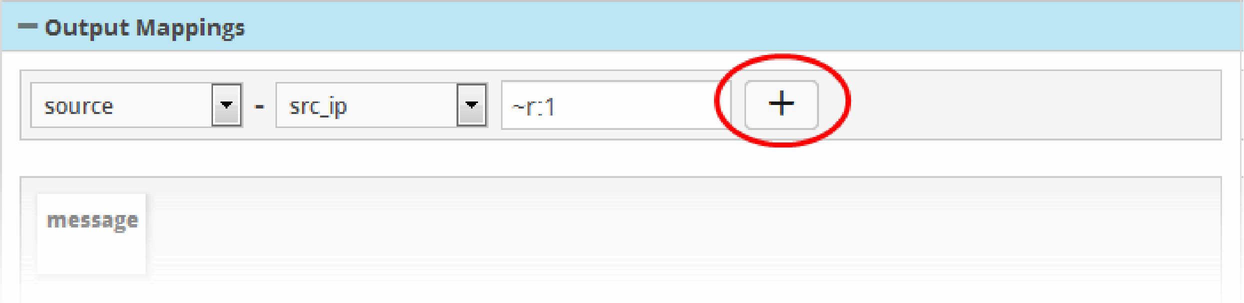
- Click the 'Output Mappings' Stripe to open the 'Output Mappings' area.



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

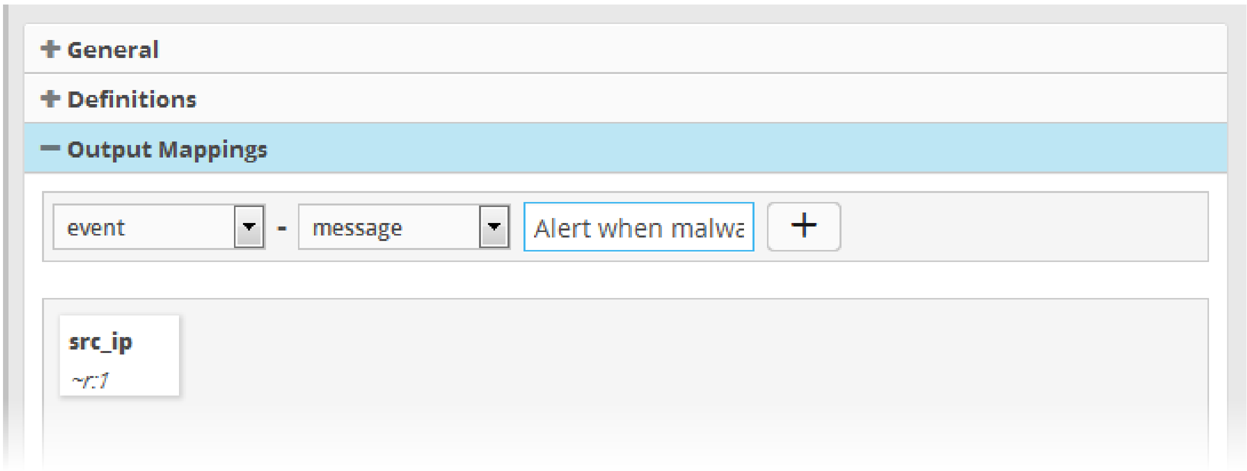


- In the 'Value' field, enter the variable that will fetch the value of the selected aggregate field in the 'Definitions' tab. The variable should be in the format ~r:1, ~r:2 and so on. The variable '~r:1' will fetch the value of the first selected aggregate parameter, the variable '~r:2' will fetch the value of the second selected aggregate parameter and so on. If you enter some text, the field value will be static for that field for the new event generated on correlation.
- Click the + button to add the field value.



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

Click the ' + button to add the field.



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

## List Mappings

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

- Manual - The administrator can manually enter the values for the field in the respective list, from the 'Live List Content Management' interface, accessible by clicking 'Lists' > 'Live List Content Management' from the navigation menu.
- Automatic - From the events detected by a correlation rule. The administrator can map a rule to Live Lists and configure the fields of the events from which the values are to be updated to the respective list.

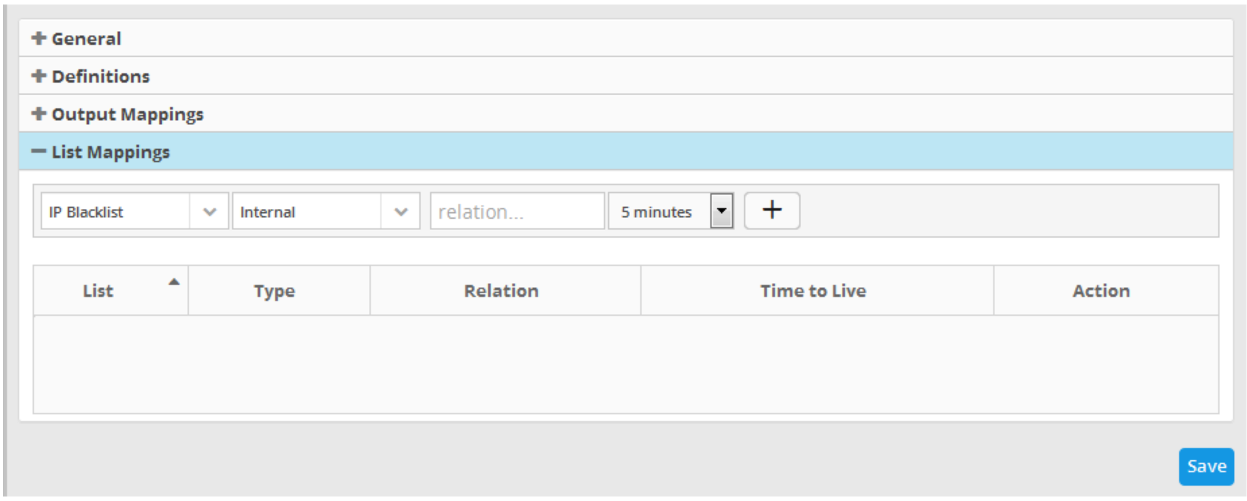
For more details on managing Live Lists, refer to the chapter **Live Lists**.

The 'List Mappings' area allows you to choose the Live Lists to which the selected field values of the events detected by the rule are to be automatically updated. As a prerequisite, you should have chosen the field values to be collected, as the aggregation parameters for the query defined in the rule.

For example, if you want to collect the source IP addresses from the events identified by a rule that detects access to malware domains, in a live list that contain list of IP addresses of infected endpoints, you can map the respective live list to the rule and configure for the values of source IP address fields of the events to be fed to the list. The 'Source IP' field field should have been set as a aggregation parameter in the query defined for the rule.

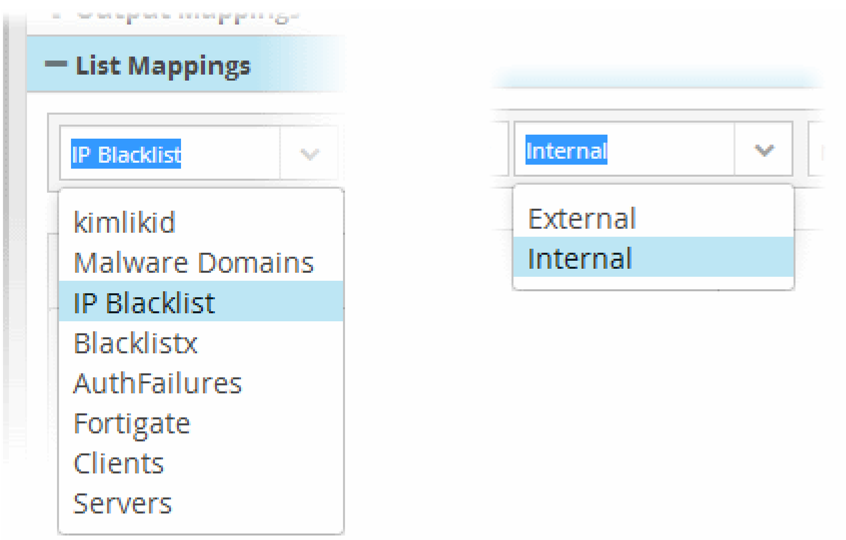
**To map live lists to a rule**

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



| List | Type | Relation | Time to Live | Action |
|---|---|---|---|---|

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



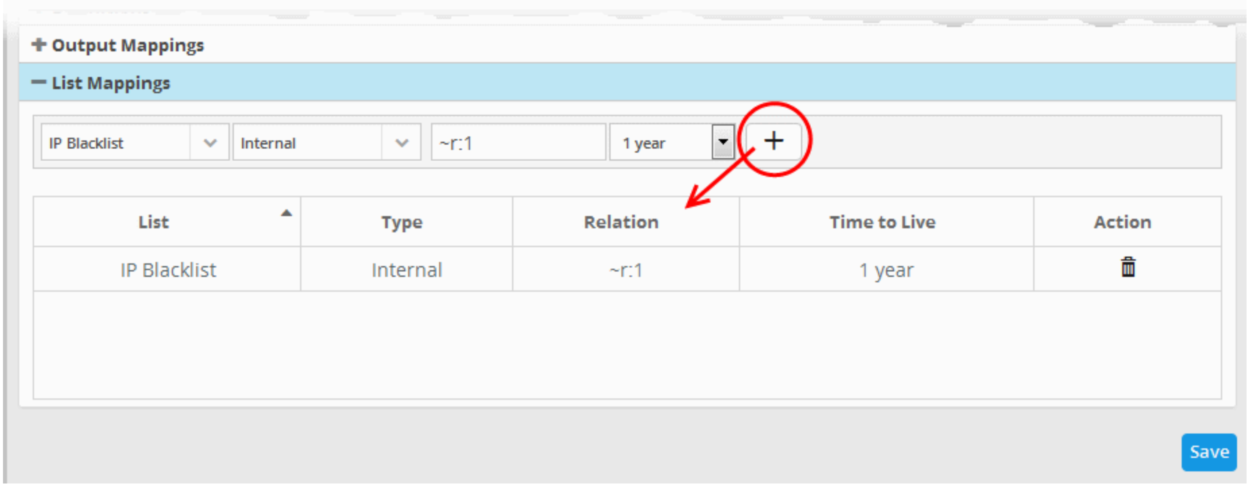
More details on Lists and List Types are available in the chapter **Live Lists**.

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

  For example, If the list contains Source IPs, and if the 'source.src_ip' is chosen as first aggregate parameter for the rule, then for collecting the source IPs from the events identified by the rule, enter ~r:1.

- Choose the validity period for the value in the live list from the Time To Live (TTL) drop-down that appears next. The options available are from '5 minutes' to 'No Limit'. On lapse of the TTL period, the value fetched to the list by the rule will be automatically deleted.

- Click the + button to add the list mapping.



| List | Type | Relation | Time to Live | Action |
|---|---|---|---|---|
| IP Blacklist | Internal | ~r:1 | 1 year | 🗑 |

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

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

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

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

### Editing a correlation rule

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

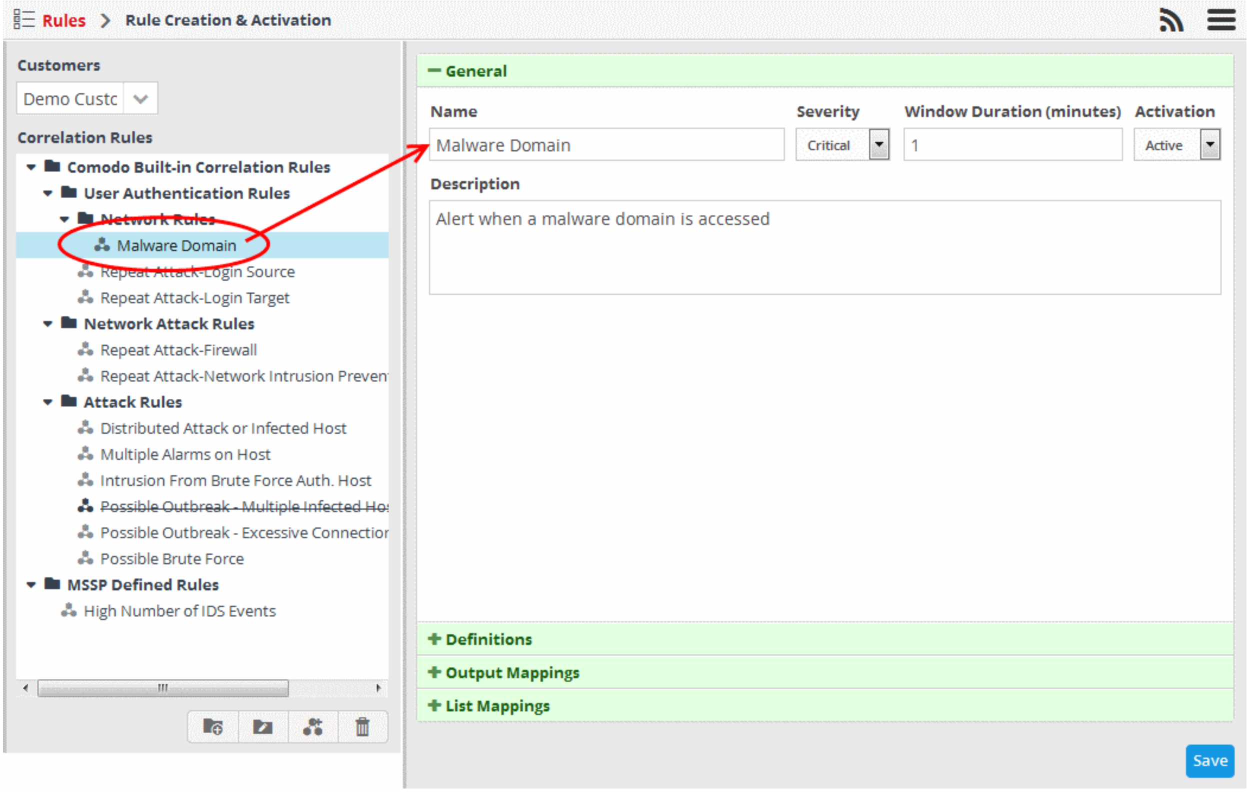
**To edit a rule**

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

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

- Choose the rule to be edited.

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

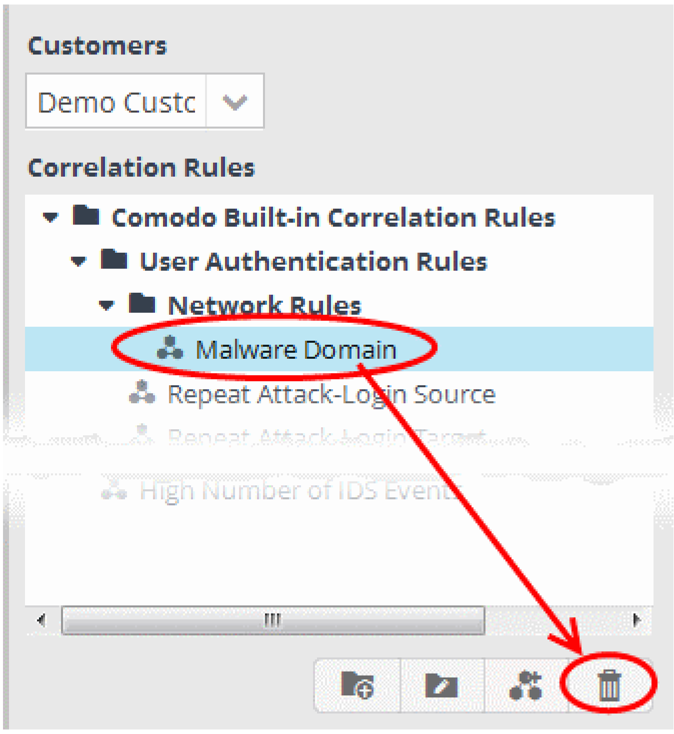

Rules
Rule Creation & Activation
Customers
Demo Custc
Correlation Rules
Comodo Built-in Correlation Rules
User Authentication Rules
Network Rules
Malware Domain
Repeat Attack-Login Source
Repeat Attack-Login Target
Network Attack Rules
Repeat Attack-Firewall
Repeat Attack-Network Intrusion Preven
Attack Rules
Distributed Attack or Infected Host
Multiple Alarms on Host
Intrusion From Brute Force Auth. Host
Possible Outbreak - Multiple Infected Ho
Possible Outbreak - Excessive Connectior
Possible Brute Force
MSSP Defined Rules
High Number of IDS Events
− General
+ Definitions
+ Output Mappings
+ List Mappings
Save

Name: Malware Domain
Severity: Critical
Window Duration (minutes): 1
Activation: Active
Description: Alert when a malware domain is accessed

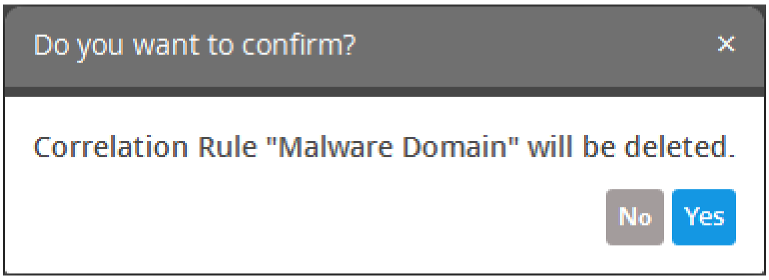
- Edit the rule as required. The procedure is same as adding a correlation rule. Refer to the **creating a correlation rule** section for more details.
- Click the 'Save' button to save your changes.

### Deleting a correlation rule

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


Customers
Demo Custc
Correlation Rules
Comodo Built-in Correlation Rules
User Authentication Rules
Network Rules
Malware Domain
Repeat Attack-Login Source
Repeat Attack-Login Target
High Number of IDS Events

A confirmation dialog will appear.



Do you want to confirm?

Correlation Rule "Malware Domain" will be deleted.

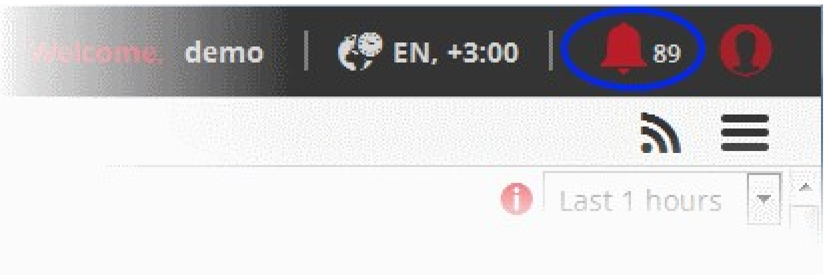
- Click 'Yes' in the confirmation dialog to remove the rule.

# 8 Incidents and Cases

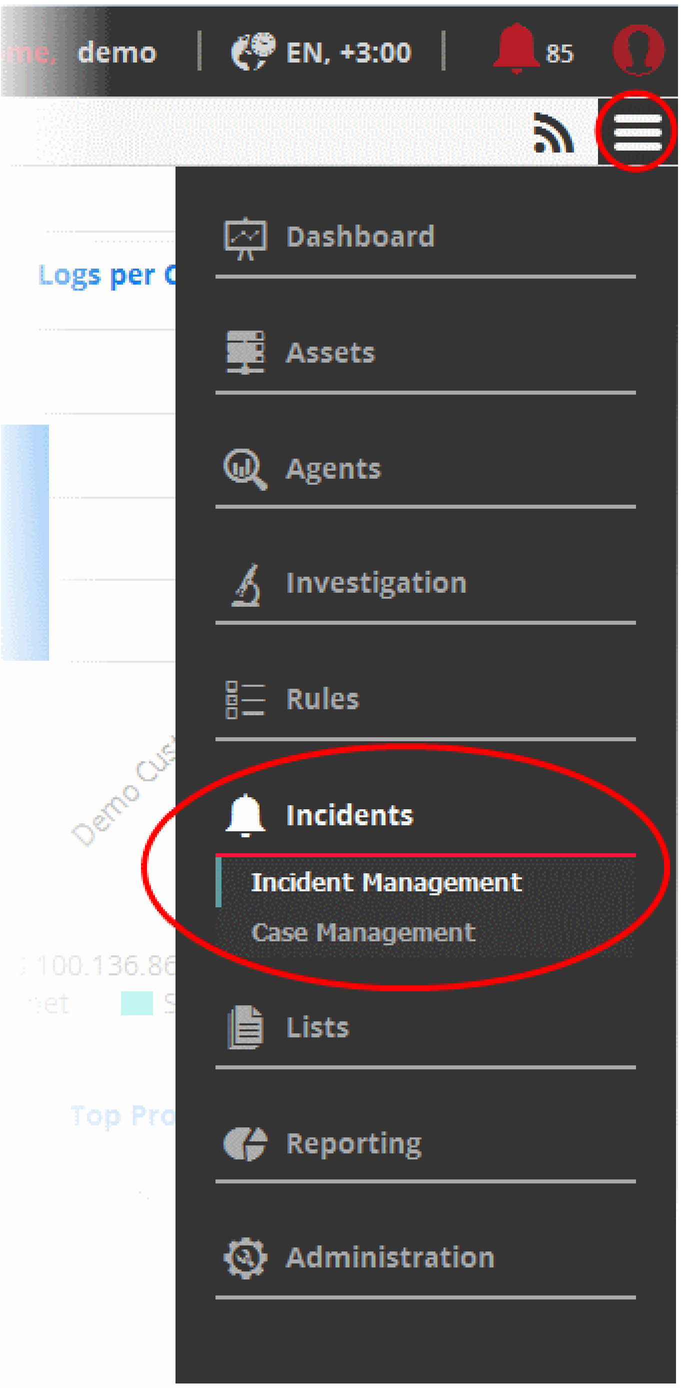
NxSIEM generates alerts when it identifies events which match correlation rules that have been defined for each customer in the **Rule Creation & Activation** interface. These alerts are automatically assigned as 'Incidents' to the 'users' allotted to the respective customer. Each 'Incident' has a status of 'Open' until it is closed by a user once the issue related to the event has been resolved. Administrators can also manually add incidents and assign them to users if certain actions are required on customer networks.

A series of incidents on the same network which are assigned to the same user, can be grouped together as a 'Case'. The case can then be assigned to a user for collective investigation.

The number of open incidents is dynamically displayed beside the notification icon in the title bar of the administration console.



The 'Incidents' menu allows the user to manage incidents and cases. To open the 'Incidents' menu, click the menu button at top right and choose 'Incidents':



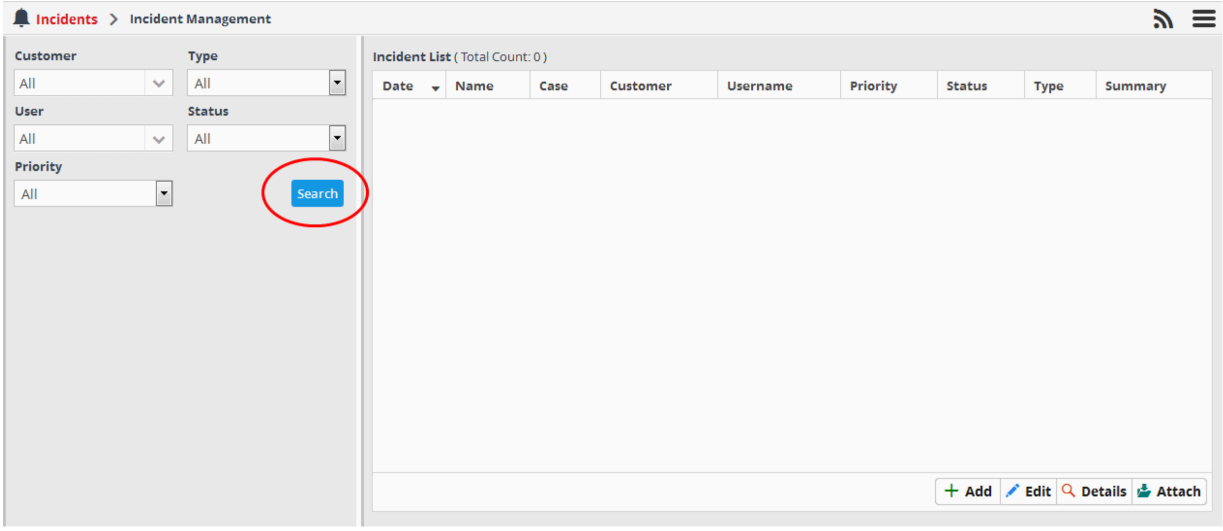
The following sections explain more about:

- Managing Incidents
- Managing Cases

## 8.1 Managing Incidents

The 'Incident Management' interface displays a list of incidents along with details such as customer network, the user to whom it is assigned and so on. Administrators can view incident details, reassign them to different users, add incidents to a case, close/re-open incidents and more.

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



Incidents > Incident Management

Customer
All
Type
All
User
All
Status
All
Priority
All

Search

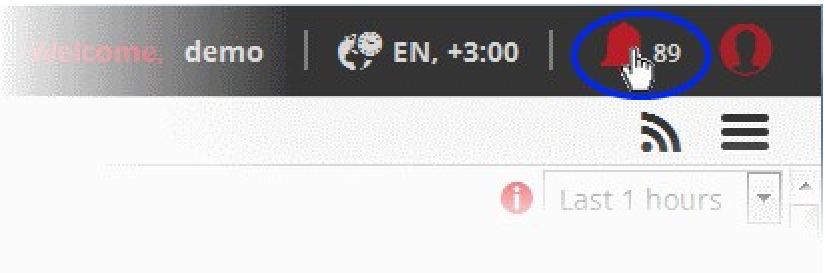
Incident List ( Total Count: 0 )

| Date | Name | Case | Customer | Username | Priority | Status | Type | Summary |
|---|---|---|---|---|---|---|---|---|

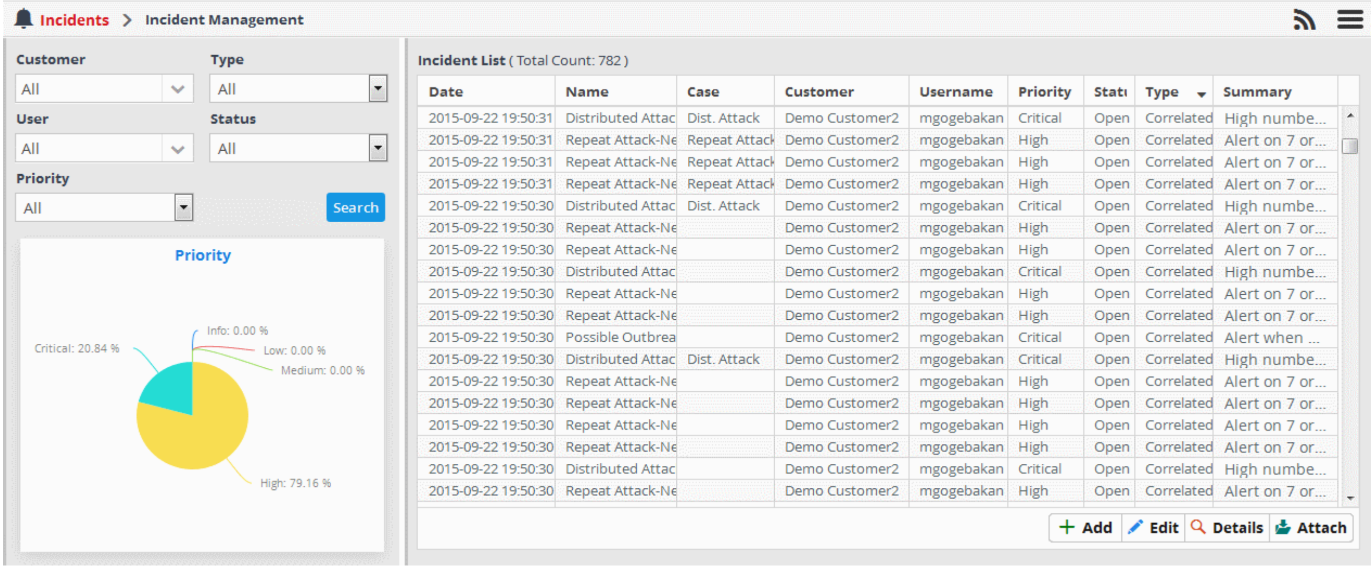
The panel on the left allows you to filter which incidents are displayed.

- 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.



Incidents > Incident Management

Customer
All
Type
All
User
All
Status
All
Priority
All

Search

Incident List ( Total Count: 782 )

| Date | Name | Case | Customer | Username | Priority | Statı | 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.

| Incident List - Table of Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Date | Displays the precise date and time at which the incident was detected or added. |
| Name | For incidents added by correlation rules - The 'Name' column displays the name of the rule based on which the incident was detected.<br>For manually added incidents - The 'Name' column displays the name as entered during its creation. |
| Case | Displays the name of the case to which the incident is attached. A case is a collection of incidents assigned to a user for collective investigation and countermeasure. Refer to the section **Managing Cases** for more details. |
| Customer | Indicates the customer on whose network the incident was detected. |
| Username | Indicates the user to whom the incident is assigned for investigation. |
| Priority | For incidents added by correlation rules - The 'Priority' column displays the severity level of the incident, as configured for the rule based on which the incident was detected.<br>For manually added events - The 'Priority' field displays their severity level as entered during creation. |
| Status | Displays the status of the incident on whether it is attended or yet to be attended. The possible values are:<br>• Open;<br>• In-Progress;<br>• False-Positive;<br>• Closed. |
| Type | Indicates whether the incident is added manually or by a correlation rule. The possible values are:<br>• Default - Incident is added manually<br>• Correlated - Incident is added based on a correlation rule. |
| Summary | For incidents added by correlation rules - The 'Summary' column displays a short description of the it as defined in the rule based on which the it was detected.<br>For manually added events - The 'Summary' field displays the short description of it as entered during its creation. |

## Sorting Options:

- Clicking on any column header sorts the items in alphabetical order of entries in that column.

Following sections explain on:

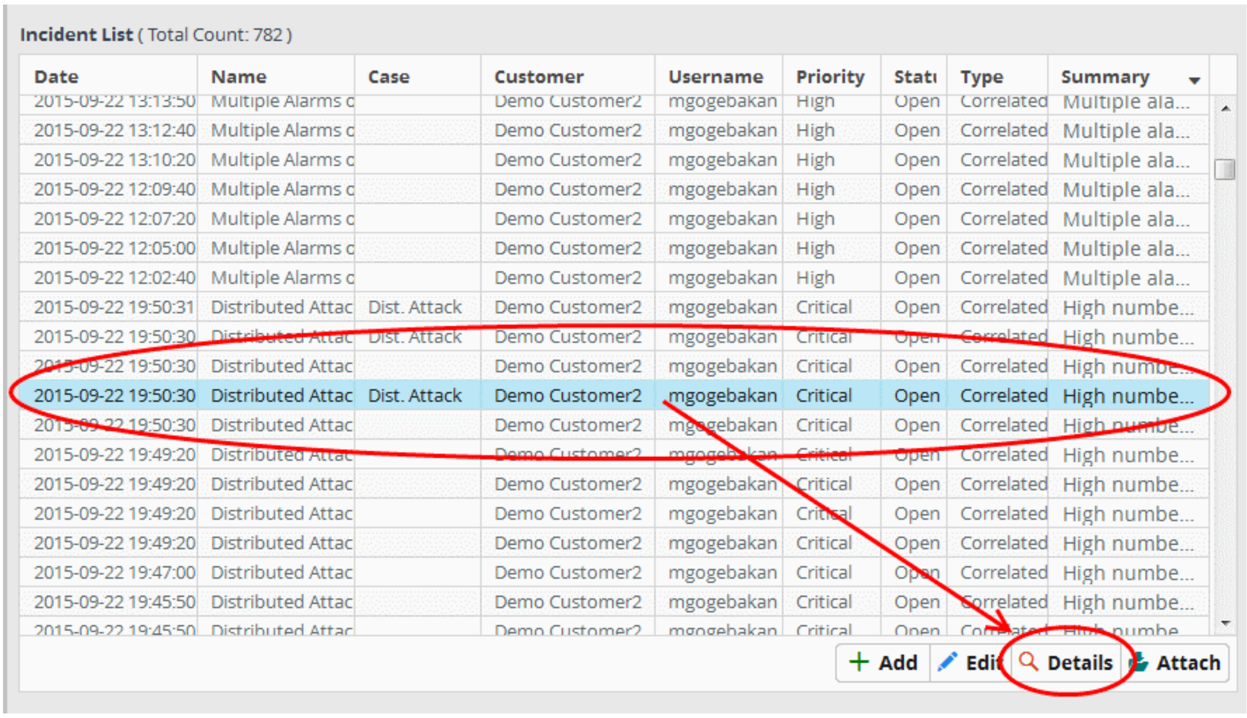
- **Viewing the details of incidents**
- **Adding and assigning incidents to users**
- **Editing and Reassigning an incident**
- **Adding incidents to cases**

## Viewing the details of incidents

The administrator can view the complete details including  of an incident from the 'Incident Details' pane. The 'Incident Details' pane 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.

**To view the details of an incident**

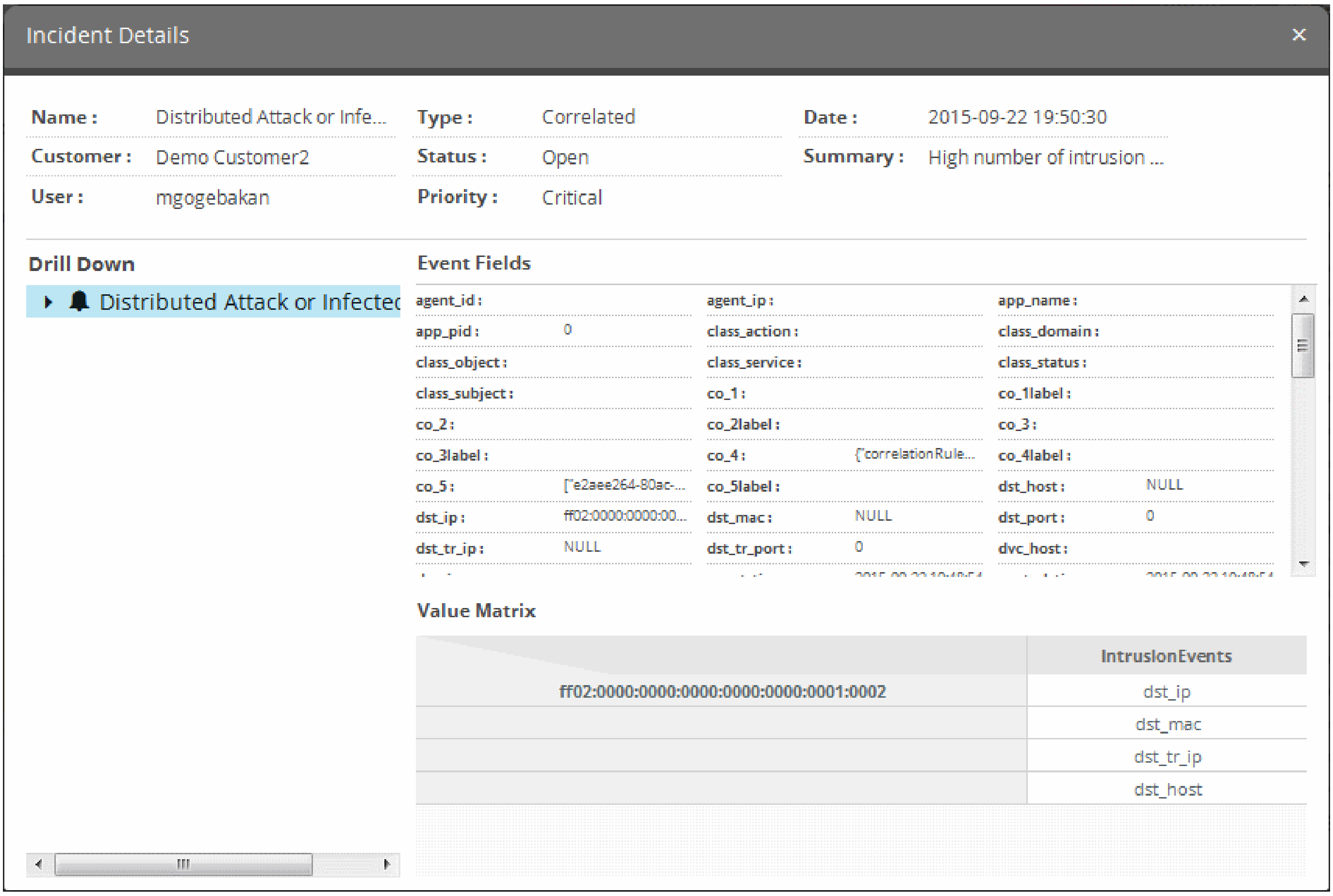
- Select an incident that you want to view the details and click the 'Details' button at the bottom



**Incident List** ( Total Count: 782 )

| Date | Name | Case | Customer | Username | Priority | Statu | Type | Summary |
|---|---|---|---|---|---|---|---|---|
| 2015-09-22 13:13:50 | Multiple Alarms c | | Demo Customer2 | mgogebakan | High | Open | Correlated | Multiple ala... |
| 2015-09-22 13:12:40 | Multiple Alarms c | | Demo Customer2 | mgogebakan | High | Open | Correlated | Multiple ala... |
| 2015-09-22 13:10:20 | Multiple Alarms c | | Demo Customer2 | mgogebakan | High | Open | Correlated | Multiple ala... |
| 2015-09-22 12:09:40 | Multiple Alarms c | | Demo Customer2 | mgogebakan | High | Open | Correlated | Multiple ala... |
| 2015-09-22 12:07:20 | Multiple Alarms c | | Demo Customer2 | mgogebakan | High | Open | Correlated | Multiple ala... |
| 2015-09-22 12:05:00 | Multiple Alarms c | | Demo Customer2 | mgogebakan | High | Open | Correlated | Multiple ala... |
| 2015-09-22 12:02:40 | Multiple Alarms c | | Demo Customer2 | mgogebakan | High | Open | Correlated | Multiple ala... |
| 2015-09-22 19:50:31 | Distributed Attac | Dist. Attack | Demo Customer2 | mgogebakan | Critical | Open | Correlated | High numbe... |
| 2015-09-22 19:50:30 | Distributed Attac | Dist. Attack | Demo Customer2 | mgogebakan | Critical | Open | Correlated | High numbe... |
| 2015-09-22 19:50:30 | Distributed Attac | | Demo Customer2 | mgogebakan | Critical | Open | Correlated | High numbe... |
| 2015-09-22 19:50:30 | Distributed Attac | Dist. Attack | Demo Customer2 | mgogebakan | Critical | Open | Correlated | High numbe... |
| 2015-09-22 19:50:30 | Distributed Attac | | Demo Customer2 | mgogebakan | Critical | Open | Correlated | High numbe... |
| 2015-09-22 19:49:20 | Distributed Attac | | Demo Customer2 | mgogebakan | Critical | Open | Correlated | High numbe... |
| 2015-09-22 19:49:20 | Distributed Attac | | Demo Customer2 | mgogebakan | Critical | Open | Correlated | High numbe... |
| 2015-09-22 19:49:20 | Distributed Attac | | Demo Customer2 | mgogebakan | Critical | Open | Correlated | High numbe... |
| 2015-09-22 19:49:20 | Distributed Attac | | Demo Customer2 | mgogebakan | Critical | Open | Correlated | High numbe... |
| 2015-09-22 19:47:00 | Distributed Attac | | Demo Customer2 | mgogebakan | Critical | Open | Correlated | High numbe... |
| 2015-09-22 19:45:50 | Distributed Attac | | Demo Customer2 | mgogebakan | Critical | Open | Correlated | High numbe... |
| 2015-09-22 19:45:50 | Distributed Attac | | Demo Customer2 | mgogebakan | Critical | Open | Correlated | High numbe... |

The 'Incident Details' pane for the selected incident will be displayed. It provides complete information about the incident such as the name of the rule that triggered the alert, name of the customer, type of incident and more. 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

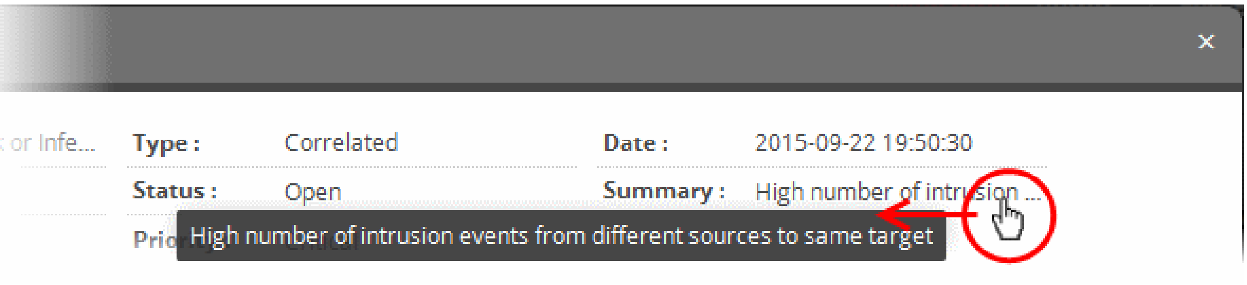
**Event Fields**

| | | | | | |
|---|---|---|---|---|---|
| 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

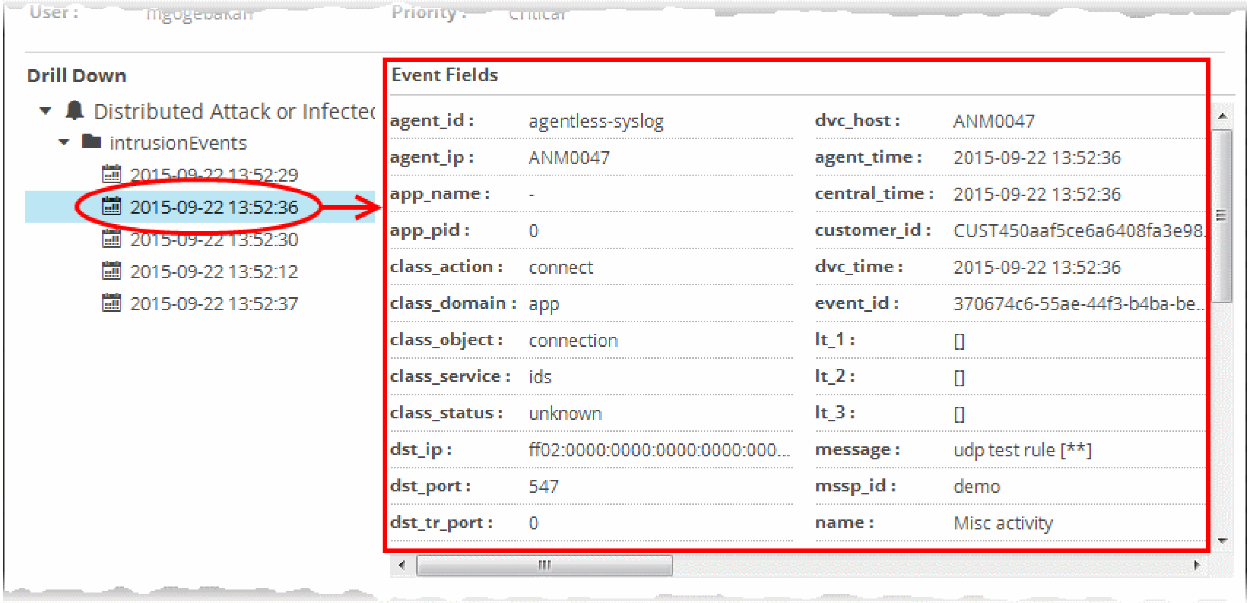
High number of intrusion events from different sources to same target

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. Refer to the explanation of '**Output Mappings**' under '**Configuring a Correlation Rule**' in the section **Managing Rules** for more details.

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.



User : mgogebakan Priority : Critical

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 |

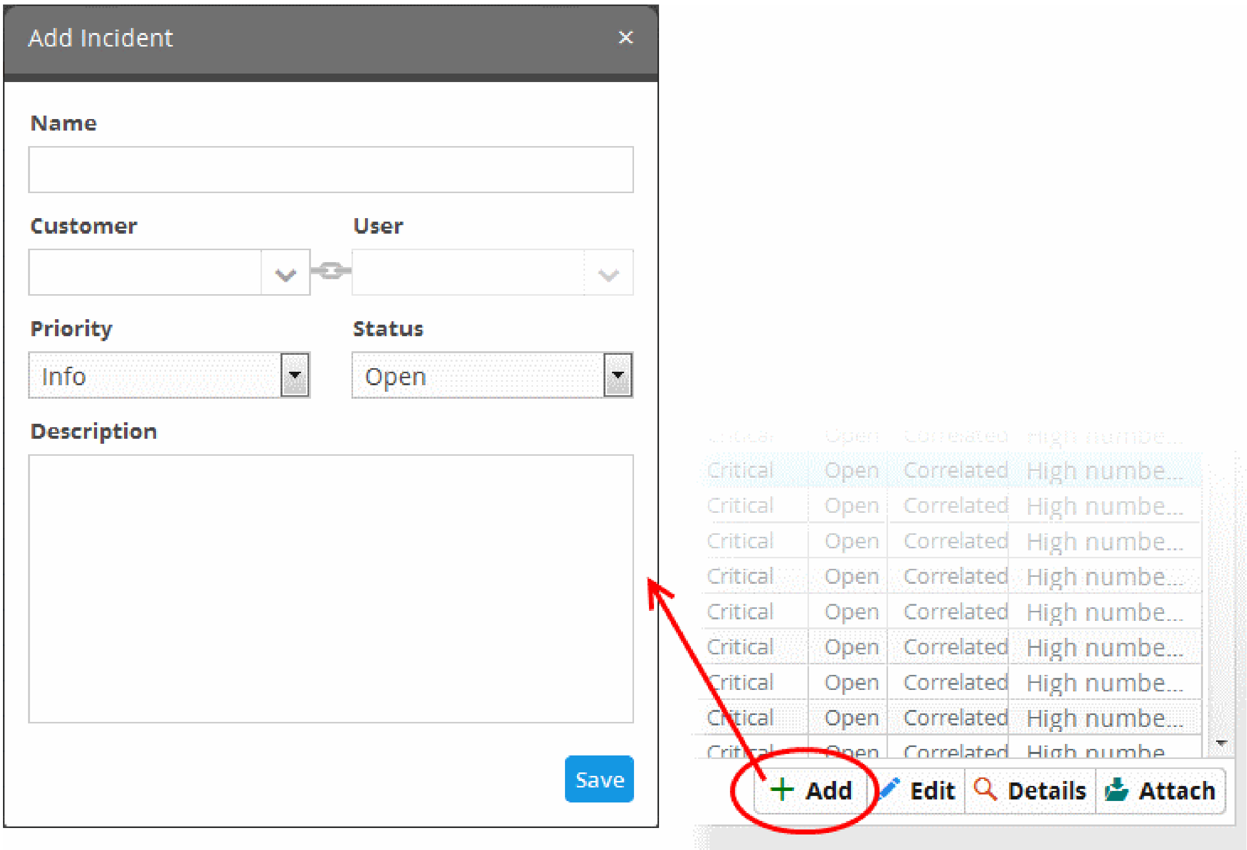
## Manually Adding an Incident

In addition to the incidents reported by the correlation rules, the administrator can manually add an incidents in order to assign specific jobs to the user allotted to a customer. The manually added incidents can also be attached to a case for combined investigation and action by the user.

**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

|  |  |  |  |
|---|---|---|---|
| Critical | Open | Correlated | High numbe... |
| Critical | Open | Correlated | High numbe... |
| Critical | Open | Correlated | High numbe... |
| Critical | Open | Correlated | High numbe... |
| Critical | Open | Correlated | High numbe... |
| Critical | Open | Correlated | High numbe... |
| Critical | Open | Correlated | High numbe... |
| Critical | Open | Correlated | High numbe... |

- **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

The incident will be added and displayed in the 'Incident List' and will be available for attachment to a case. Please note that incidents added manually will be classified as 'Default'.

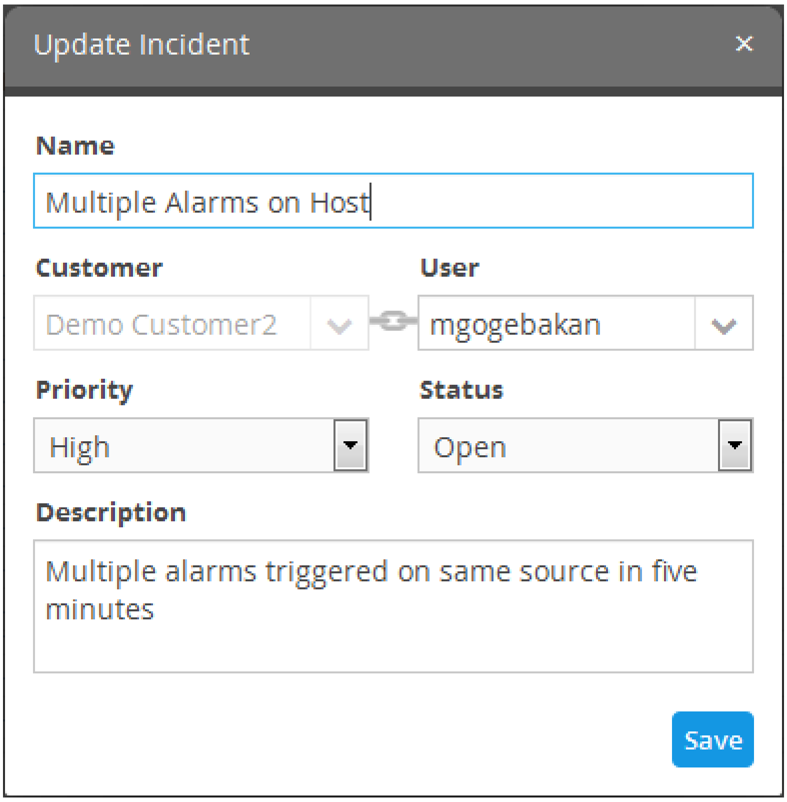
## Editing and Reassigning an Incident

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.

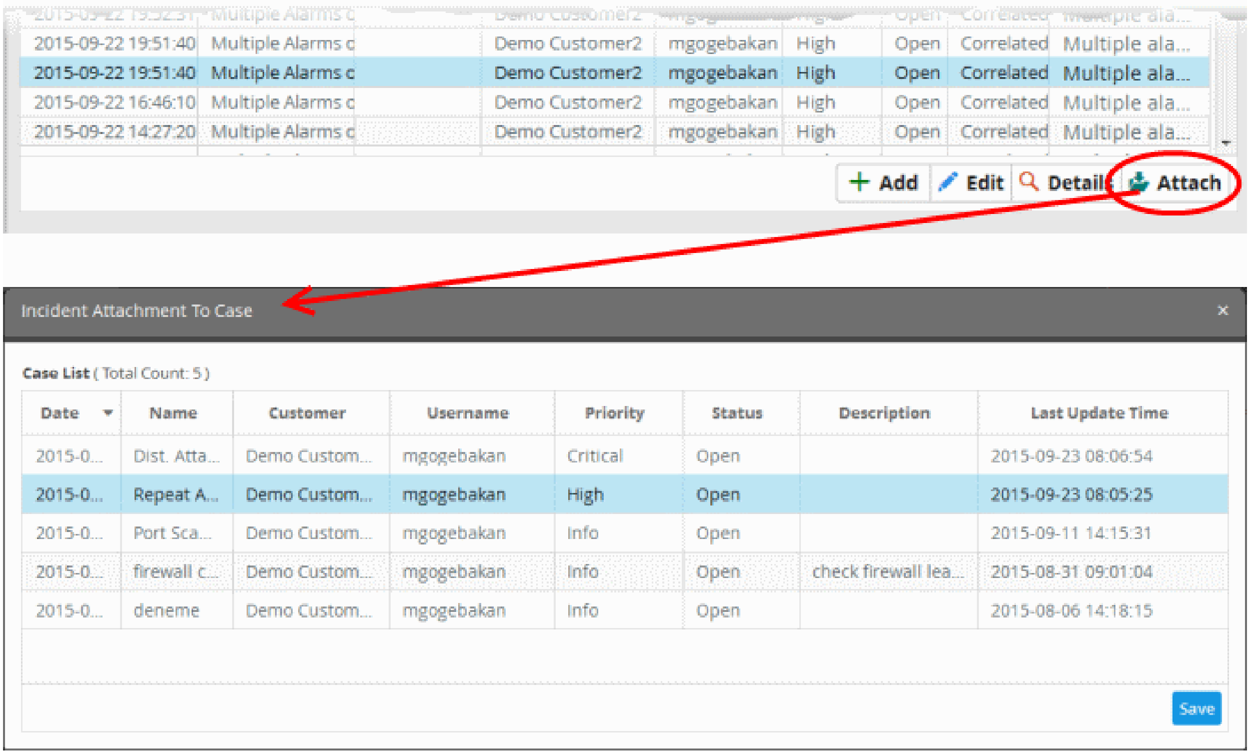
## Adding Incidents to Cases

A 'Case' is a collection of mutually related or a series of incidents for collective investigation and remedial action by the user to whom it is assigned. The administrator can create a case and assign to a same user, from the 'Case  Management' interface and attach incidents to cases from the 'Incident Management' interface. For more details on creation and management of cases, refer to the section **Managing Cases**.

**To attach an incident to a case**

- 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 add to case and click the 'Attach' button.

The 'Incident Attachment to Case' pane will open with a list of cases assigned to the same user to whom the selected incident is assigned.



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2015-09-22 19:52:31 | Multiple Alarms c | Demo Customer2 | mgogebakan | High | Open | Correlated | Multiple ala... |
| 2015-09-22 19:51:40 | Multiple Alarms c | Demo Customer2 | mgogebakan | High | Open | Correlated | Multiple ala... |
| 2015-09-22 19:51:40 | Multiple Alarms c | Demo Customer2 | mgogebakan | High | Open | Correlated | Multiple ala... |
| 2015-09-22 16:46:10 | Multiple Alarms c | Demo Customer2 | mgogebakan | High | Open | Correlated | Multiple ala... |
| 2015-09-22 14:27:20 | Multiple Alarms c | Demo Customer2 | mgogebakan | High | Open | Correlated | Multiple ala... |

Incident Attachment To Case

**Case List** ( Total Count: 5 )

| Date | Name | Customer | Username | Priority | Status | Description | Last Update Time |
|---|---|---|---|---|---|---|---|
| 2015-0... | Dist. Atta... | Demo Custom... | mgogebakan | Critical | Open | | 2015-09-23 08:06:54 |
| 2015-0... | Repeat A... | Demo Custom... | mgogebakan | High | Open | | 2015-09-23 08:05:25 |
| 2015-0... | Port Sca... | Demo Custom... | mgogebakan | Info | Open | | 2015-09-11 14:15:31 |
| 2015-0... | firewall c... | Demo Custom... | mgogebakan | Info | Open | check firewall lea... | 2015-08-31 09:01:04 |
| 2015-0... | deneme | Demo Custom... | mgogebakan | Info | Open | | 2015-08-06 14:18:15 |

- Select the case to which the incident needs to be added
- Click 'Save'.

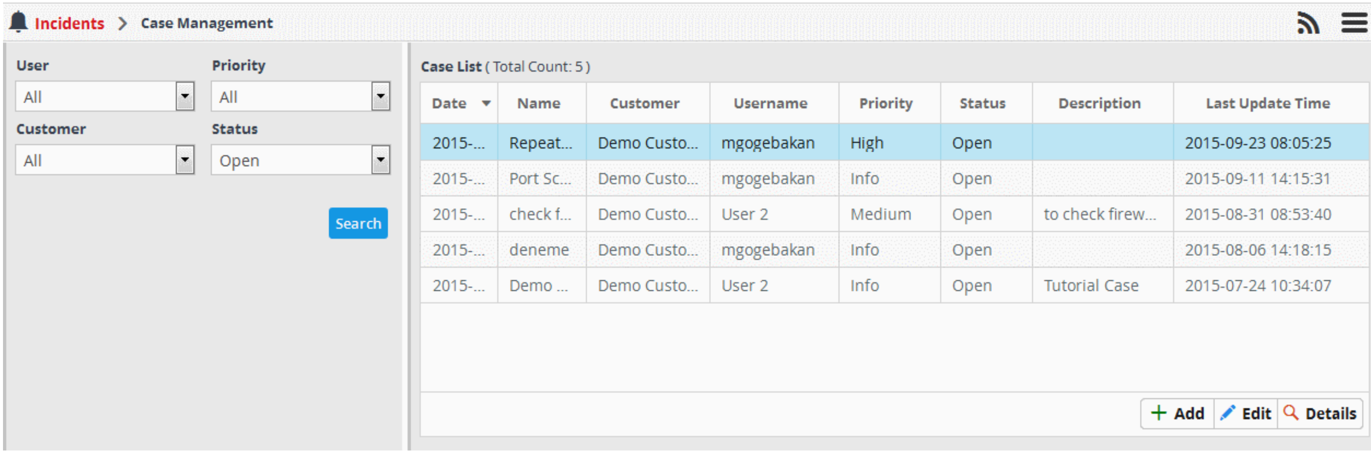
The incident will be added to the case.

## 8.2 Managing Cases

NxSIEM allows the administrator 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 example, if an intruder executes Brute Force attack and access a network and tries to identify the vulnerable endpoints in the network by performing a port scan, the brute force attack is added as an incident and port scans at different endpoints are added as separate incidents in NxSIEM, if appropriate correlation rules are deployed for the customer. These incidents can be combined as a case and assigned to the user allotted for the customer for a collective remedial action.

The Case Management interface allows the administrator to create and manage cases. To open the 'Case Management' interface, click the 'Menu' button from the top right, choose 'Incidents' and then click 'Case Management'.



User All
Priority All
Customer All
Status Open

**Case List** ( Total Count: 5 )

| Date | Name | Customer | Username | Priority | Status | Description | Last Update Time |
|---|---|---|---|---|---|---|---|
| 2015-... | Repeat... | Demo Custo... | mgogebakan | High | Open | | 2015-09-23 08:05:25 |
| 2015-... | Port Sc... | Demo Custo... | mgogebakan | Info | Open | | 2015-09-11 14:15:31 |
| 2015-... | check f... | Demo Custo... | User 2 | Medium | Open | to check firew... | 2015-08-31 08:53:40 |
| 2015-... | deneme | Demo Custo... | mgogebakan | Info | Open | | 2015-08-06 14:18:15 |
| 2015-... | Demo ... | Demo Custo... | User 2 | Info | Open | Tutorial Case | 2015-07-24 10:34:07 |

The Left side panel contains the options for selecting the cases to be displayed in the right panel using the filter options. The right side panel displays the list of cases with their details as a table.

- To view all incidents without filtering, select 'All' in all the filter option drop-downs and click 'Search'.
- To view the cases created for a specific customer, assigned to a specific user, of specific, status and/or priority, select the option(s) from the respective drop-downs and click 'Search'.

| Case List - Table of Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Date | Displays the precise date and time at which the case was created. |
| Name | Displays the name of the case. |
| Customer | Indicates the customer for whom the case was created. |
| Username | Indicates the user allotted to the customer, to whom the case is assigned for investigation. |
| Priority | Indicates the severity level of the case as set by the administrator. |
| Status | Displays the status of the case on whether it is attended or yet to be attended. The possible values are:<br>• Open;<br>• In-Progress;<br>• False-Positive;<br>• Closed. |
| Description | A short description of the case as entered by the administrator. |
| Last Update Time | Displays the date and time at which the case was last updated by adding or removing incidents, adding notes etc. |

### Sorting Options:

- Clicking on any column header sorts the items in alphabetical order of entries in that column.

The following sections explain on:

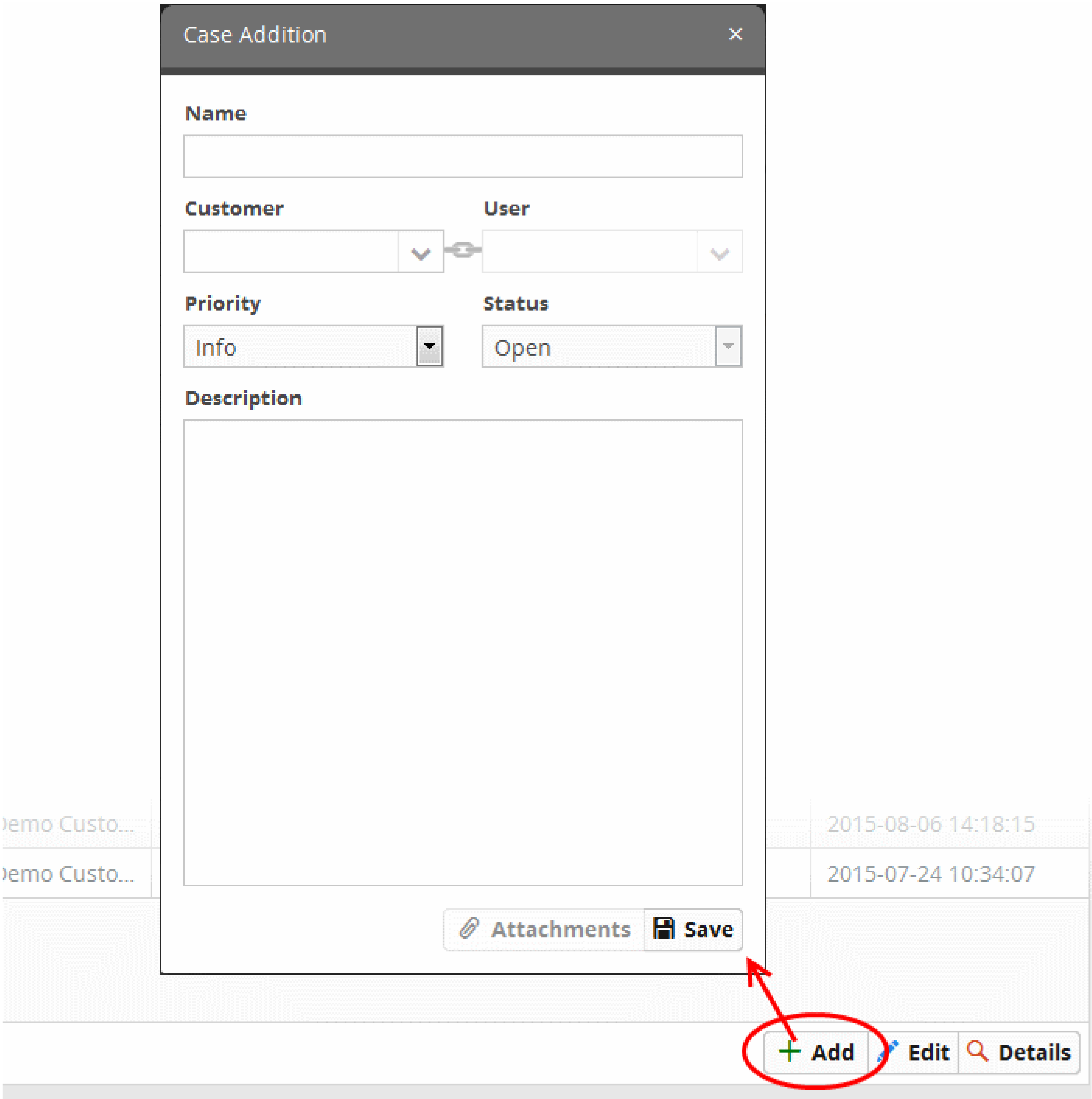
- **Creating cases**
- **Viewing details and updating the cases**
- **Editing cases**

## Creating Cases

The administrator can create cases and assign to specific users from the case Management interface. The incidents can be attached to the case only from the 'Incident Management' interface.

**To add a case**

- Click the 'Add' button at the bottom right of the 'Case Management' interface



The 'Case Addition' dialog will appear.

- **Name** - Enter a name for the case.
- **Customer** - Choose the customer from the drop-down for whom you want to add the case.
- **User** - The drop-down will display the users assigned to the selected customer. Choose the user to whom the case is to be assigned. Refer to the section '**Administration**' for details about assigning users to customers.
- **Priority** - Select the severity level of the case from the drop-down. The options available are 'Info', 'Low', 'Medium', 'High' and 'Critical'.
- **Description** - Enter an appropriate description for the case.

- Click the 'Save' button

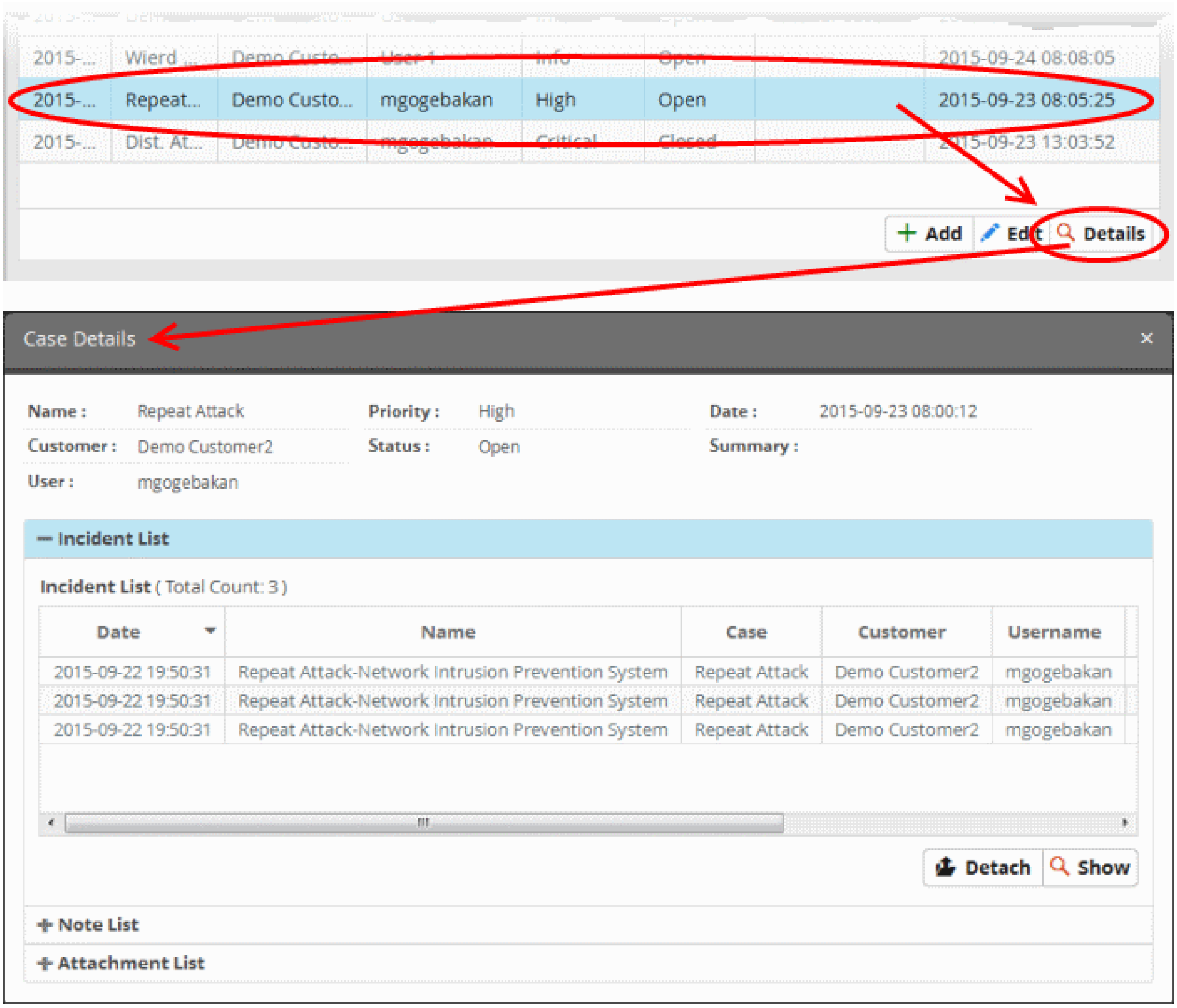
The Case will be added. The next step is to add incidents to it. For a tutorial on attaching incidents to the case, refer to the explanation of **Adding Incidents to Cases** in the previous section **Managing Incidents**.

## Viewing Details and Updating the Cases

The 'Case Details' pane allows the administrator to view and manage incidents attached to the case, view the details of the incidents, update the case on actions taken, like exchanging comment and notes with the user and add attachments that may aid in attending to the incidents.

### To view the details of a case

- Use the filter options at the left to view the list of cases pertaining to a specific customer, assigned to a specific user, specific type, status and/or priority level .
- Choose the case from the 'Case List' at the right and click the 'Details' button.



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2015-... | Wierd ... | Demo Custo... | User 1 | Info | Open | | 2015-09-24 08:08:05 |
| 2015-... | Repeat... | Demo Custo... | mgogebakan | High | Open | | 2015-09-23 08:05:25 |
| 2015-... | Dist. At... | Demo Custo... | mgogebakan | Critical | Closed | | 2015-09-23 13:03:52 |

Case Details

| | | | | | |
|---|---|---|---|---|---|
| Name : | Repeat Attack | Priority : | High | Date : | 2015-09-23 08:00:12 |
| Customer : | Demo Customer2 | Status : | Open | Summary : | |
| User : | mgogebakan | | | | |

— Incident List

Incident List ( Total Count: 3 )

| Date | Name | Case | Customer | Username |
|---|---|---|---|---|
| 2015-09-22 19:50:31 | Repeat Attack-Network Intrusion Prevention System | Repeat Attack | Demo Customer2 | mgogebakan |
| 2015-09-22 19:50:31 | Repeat Attack-Network Intrusion Prevention System | Repeat Attack | Demo Customer2 | mgogebakan |
| 2015-09-22 19:50:31 | Repeat Attack-Network Intrusion Prevention System | Repeat Attack | Demo Customer2 | mgogebakan |

The upper portion displays the general details like name of the case, priority, customer, status, user to whom the case is assigned and so on. The lower portion contains three stripes that allow you to:

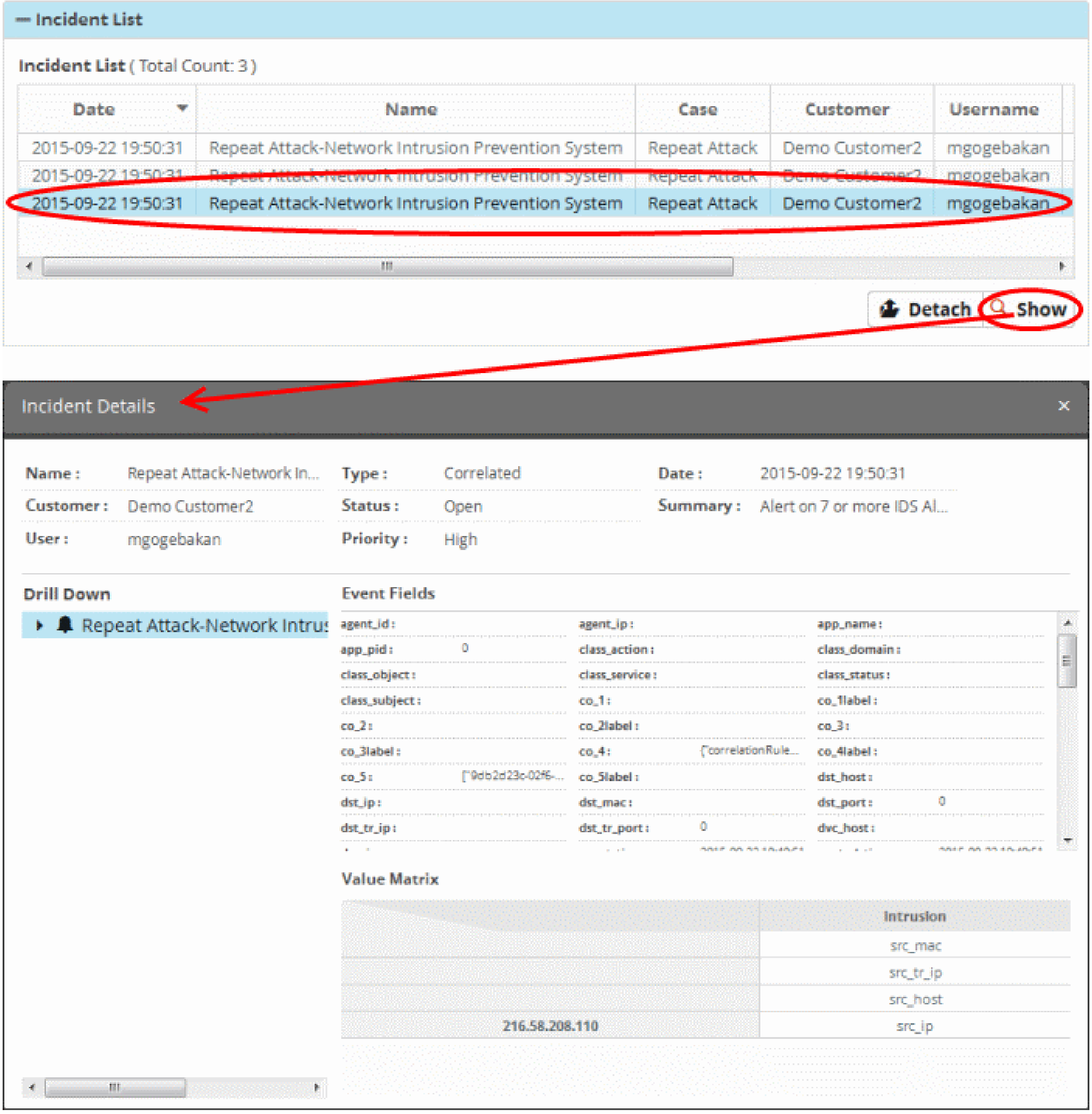
- **Incident List** - View and manage list of incidents attached to the case and view details on individual incidents
- **Note List** - View and add notes to the case
- **Attachment List** - View and share files that may be useful to investigate and take remedial measures for the incidents

### To view and manage incidents

- Click the 'Incident List' stripe to open the 'Incident List' pane.

The 'Incident List' displays the list of incidents attached to the list with their details, as a table, similar to the 'Incident List' in the Incident Management interface. Refer to **Incident List - Table of Column Descriptions** in the section **Managing Incidents** for explanations of the details displayed.

- To view the full details of an incident, select the incident and click 'Show'.



Incident List ( Total Count: 3 )

| Date | Name | Case | Customer | Username |
|---|---|---|---|---|
| 2015-09-22 19:50:31 | Repeat Attack-Network Intrusion Prevention System | Repeat Attack | Demo Customer2 | mgogebakan |
| 2015-09-22 19:50:31 | Repeat Attack-Network Intrusion Prevention System | Repeat Attack | Demo Customer2 | mgogebakan |
| 2015-09-22 19:50:31 | Repeat Attack-Network Intrusion Prevention System | Repeat Attack | Demo Customer2 | mgogebakan |

Incident Details

| | | | | | |
|---|---|---|---|---|---|
| Name : | Repeat Attack-Network In... | Type : | Correlated | Date : | 2015-09-22 19:50:31 |
| Customer : | Demo Customer2 | Status : | Open | Summary : | Alert on 7 or more IDS Al... |
| User : | mgogebakan | Priority : | High | | |

Drill Down

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 : | ["9db2d23c-02f6-... | co_5label : | | dst_host : | |
| dst_ip : | | dst_mac : | | dst_port : | 0 |
| dst_tr_ip : | | dst_tr_port : | 0 | dvc_host : | |

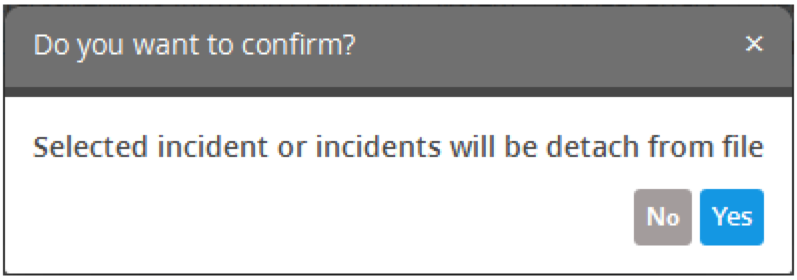
Value Matrix

| | Intrusion |
|---|---|
| | src_mac |
| | src_tr_ip |
| | src_host |
| 216.58.208.110 | src_ip |

The 'Incident Details' pane for the selected incident will be displayed. Refer to the explanation of **Viewing the details of incidents** in the section **Managing Incidents** for more information on the details displayed in this pane.

- To remove an attended/closed incident or incident added by mistake, from the case, select the case and click the 'Detach' button Detach .

A confirmation dialog will appear.



Do you want to confirm?

Selected incident or incidents will be detach from file

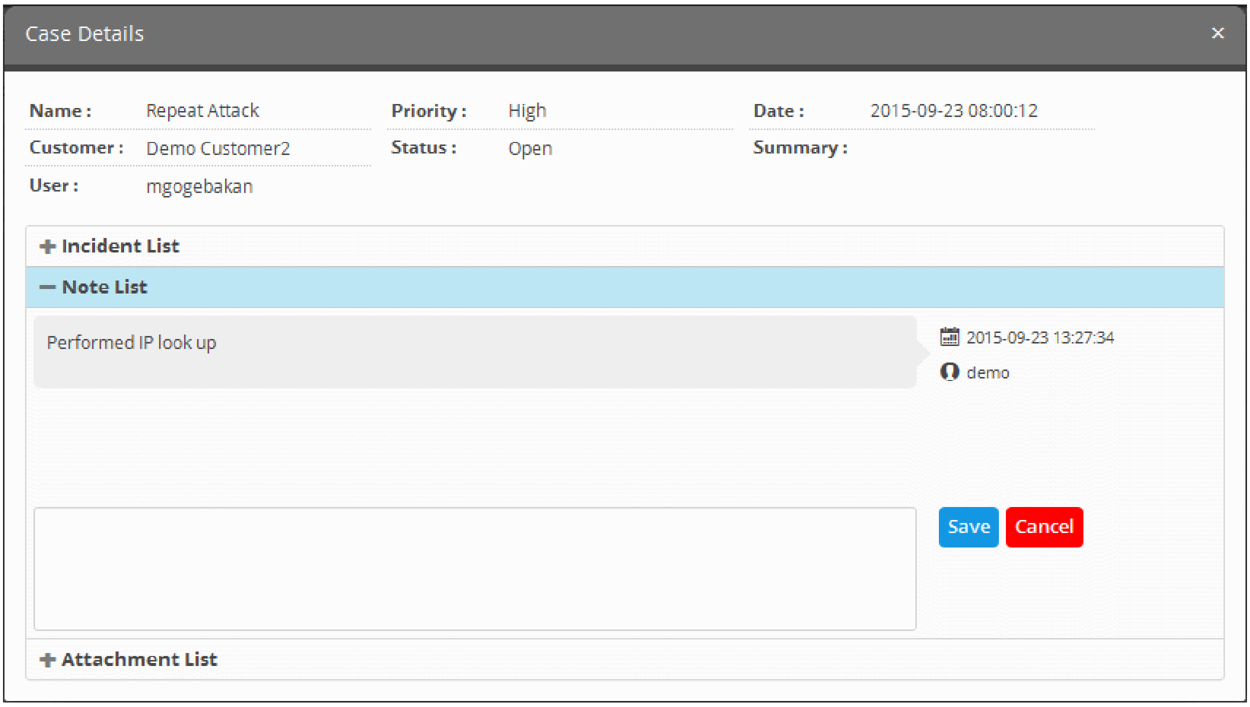
- Click 'Yes' to remove the incident from the case.

**To view and add notes to the case**

- Click the 'Note List' stripe to open the 'Note List' pane.

The 'Notes List' displays the list of comments and notes entered by the administrator and user that attends the case. You can add your comments to the case, through this pane.

- To view the full details of an incident, select the incident and click 'Show'.



Name : Repeat Attack
Customer : Demo Customer2
User : mgogebakan
Priority : High
Status : Open
Date : 2015-09-23 08:00:12
Summary :

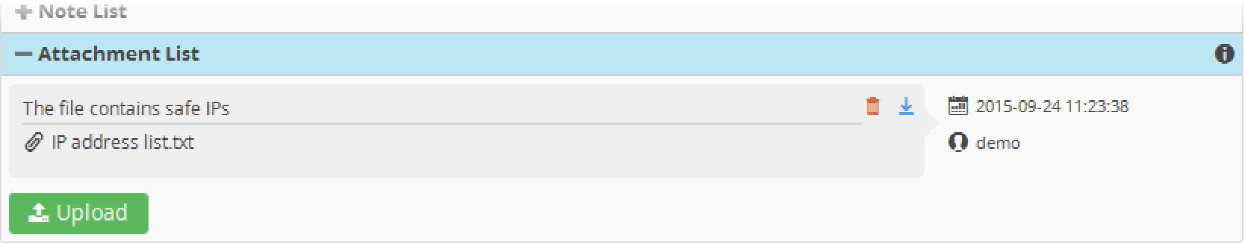
Performed IP look up
2015-09-23 13:27:34
demo

- To add a new note/comment, enter the text in the text box at the bottom and click 'Save'.

**To share files for use in attending the case**

- Click the 'Attachment List' stripe to open the 'Attachment List' pane.

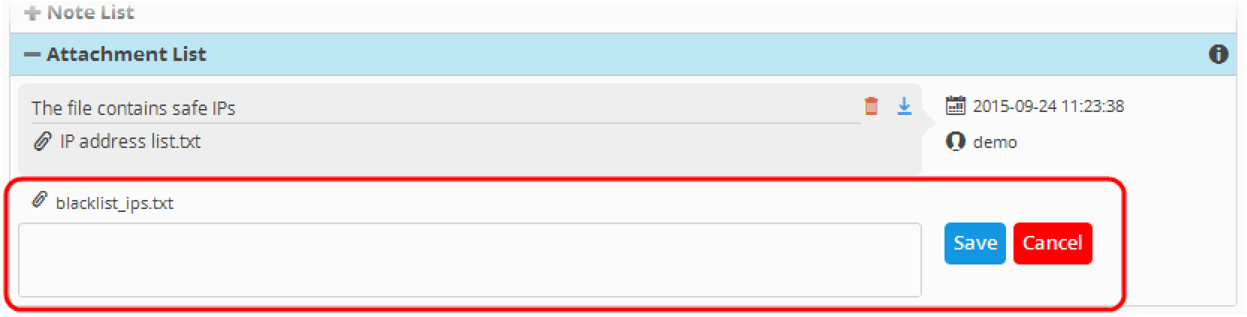
The pane displays the list of files that were shared in regard to the case, with comments entered for them.



The file contains safe IPs
IP address list.txt
2015-09-24 11:23:38
demo

- To upload a file to the case
  - Click 'Upload', navigate to the file to be uploaded in the 'File Upload' dialog and click 'Open'.

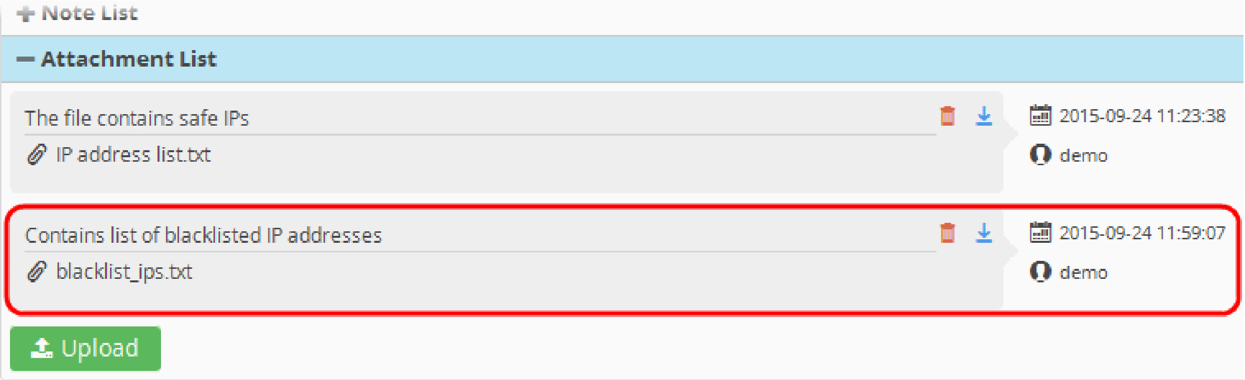
  The file will be added for uploading and a text box will be displayed for entering the description of the file.



The file contains safe IPs
IP address list.txt
2015-09-24 11:23:38
demo
blacklist_ips.txt

- Enter a description for the file in the text box and click 'Save'.

The file will be uploaded and added t the list. The user attending the case can download and use the file.



+ Note List

− Attachment List

The file contains safe IPs
IP address list.txt
2015-09-24 11:23:38
demo

Contains list of blacklisted IP addresses
blacklist_ips.txt
2015-09-24 11:59:07
demo

- To download a file, click the download icon beside the file to be downloaded and save the file.
- To remove a file from the case, click the thrash can icon beside the file.

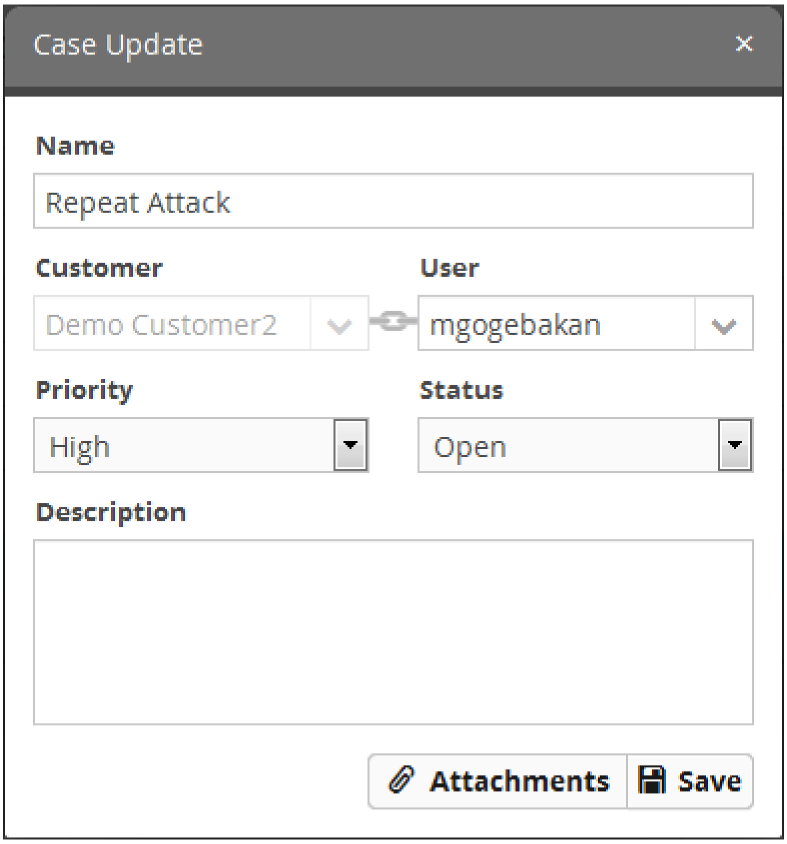
## Editing Cases

You can change the status, edit the name and severity level of a case at any time. You can also reassign the case to a different individual if required. Also you will be able to view the incidents attached to the case and update the case while editing the case. For example, if you are re-assigning a case to a new user, you can add a note on that to the case.

**To edit a case**

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

The 'Case Update' dialog will appear.



Case Update

Name: Repeat Attack

Customer: Demo Customer2

User: mgogebakan

Priority: High

Status: Open

Description:

- Edit the details like Name, priority, status as required.
- To reassign the case to a new user, 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.
- To view the list of incidents and update the case, click the 'Attachments' button.

The 'Case Details' pane will appear. For more details on managing the case from this pane, refer to the explanation of **Viewing Details and Updating the Cases**.

# 9 Live Lists

Live Lists allows administrators to create and manage lists of defined values for fields which can be used as parameters in event queries and correlation rules. For example, a list can be created with the IP addresses of malicious domains which could be used for the 'Destination Translated IP' (dst_tr_ip) field of a query designed to identify events involving access to malware domains.

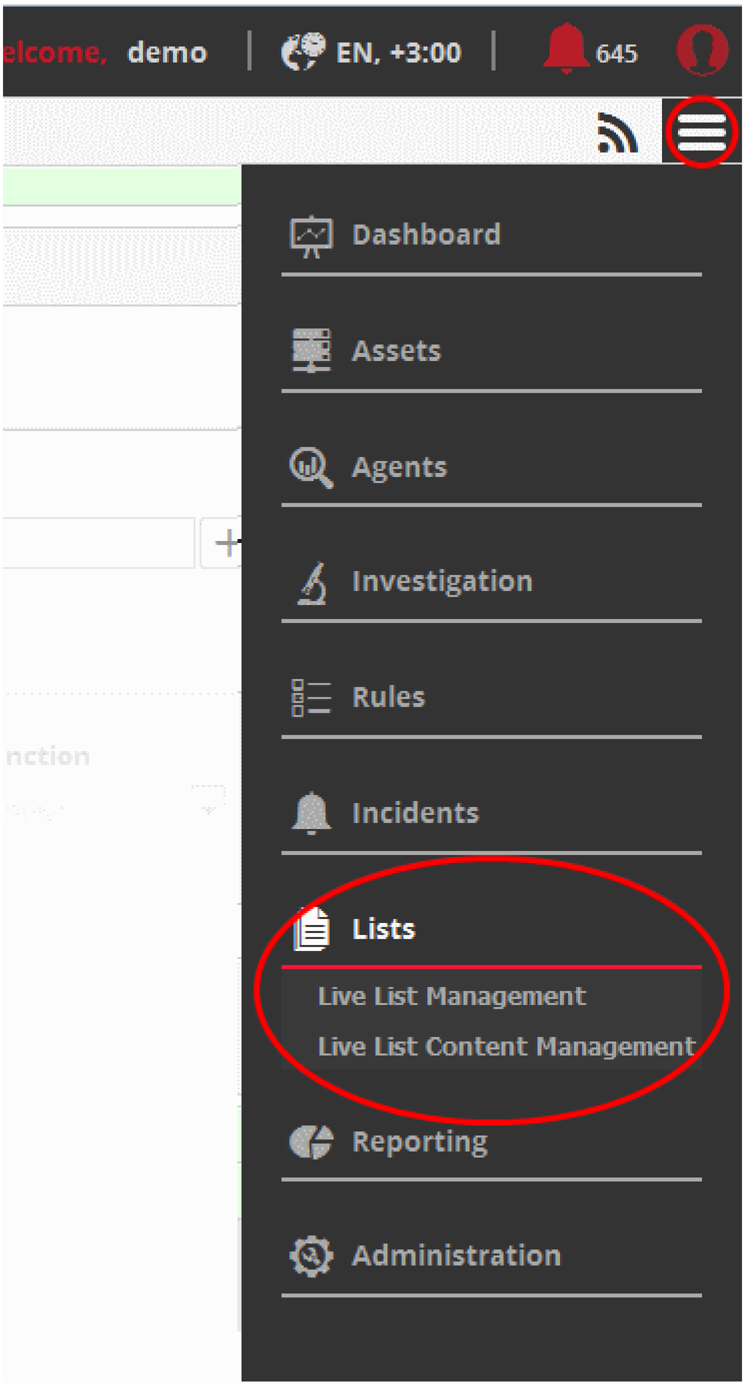
Any updates to a live list are dynamically reflected in all queries and rules in which it is used.

Live lists are created by first specifying the event field then populating it with values. Values can be populated in two ways:

- Values can be manually entered
- Correlation rules can be configured to feed values from events to a live list

Each Live List can be defined with several list types, each type containing a set of values. For example, you can create a Live List called 'IP Blacklist' which contains two types, 'Internal' (IP addresses of infected internal hosts) and 'External' (IP addresses of external malware hosts). These two lists can be used separately if required.

To open the 'Live List' interface, click the menu button at top right and choose 'Lists':



Refer to the following sections for more details:

- Managing Live Lists
- Managing Live List Content

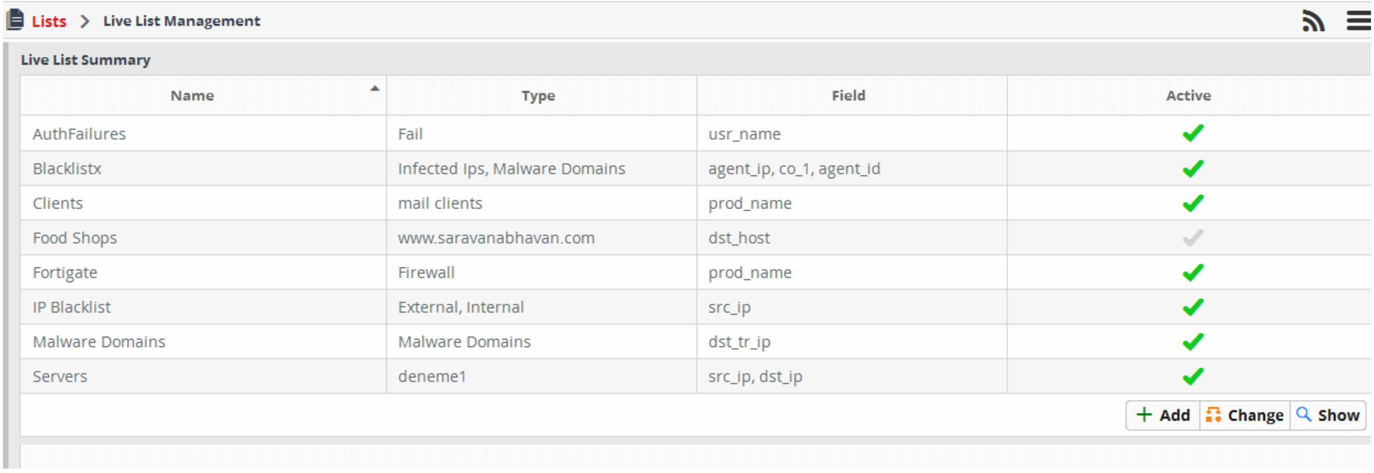
## 9.1 Managing Live Lists

The 'Live List Management' interface allows administrators to create and manage Live Lists and their types for different customers. Each 'Live List' can be configured for a single field type and a single live list can be made to have several 'Types' for defining different sets of values for the same field for use in different 'Event Queries' and 'Correlation Rules'. You can also define the time period for which a value entered in the list is valid.

For example, you can create a Live List 'IP Blacklist' with two types, 'Internal' ( containing IP addresses of infected internal hosts in a network) and 'External' ( containing IP addresses of external malware hosting domains). These two list types can be used separately as appropriate to different types of queries and rules.

**Note**: The Live List Management interface allows you to only create and manage lists for various fields. The values for the fields can be manually added from the Live List Content Management interface. Refer to the section **Managing Live List Content**.

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



| Name | Type | Field | Active |
|---|---|---|---|
| AuthFailures | Fail | usr_name | ✓ |
| Blacklistx | Infected Ips, Malware Domains | agent_ip, co_1, agent_id | ✓ |
| Clients | mail clients | prod_name | ✓ |
| Food Shops | www.saravanabhavan.com | dst_host | ✓ |
| Fortigate | Firewall | prod_name | ✓ |
| IP Blacklist | External, Internal | src_ip | ✓ |
| Malware Domains | Malware Domains | dst_tr_ip | ✓ |
| Servers | deneme1 | src_ip, dst_ip | ✓ |

The interface displays a list of Live Lists added to NxSIEM with their details and controls for adding a new list, switching a list between active and inactive states and viewing the values added to a list.

| Live List Summary Table - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Name | Displays the name of the live list |
| Type | Displays the types available for the live list |
| Field | Displays the event log entry field for which the list contains the values. |
| Active | Indicates whether the list is active or not. |

Following sections explain on:

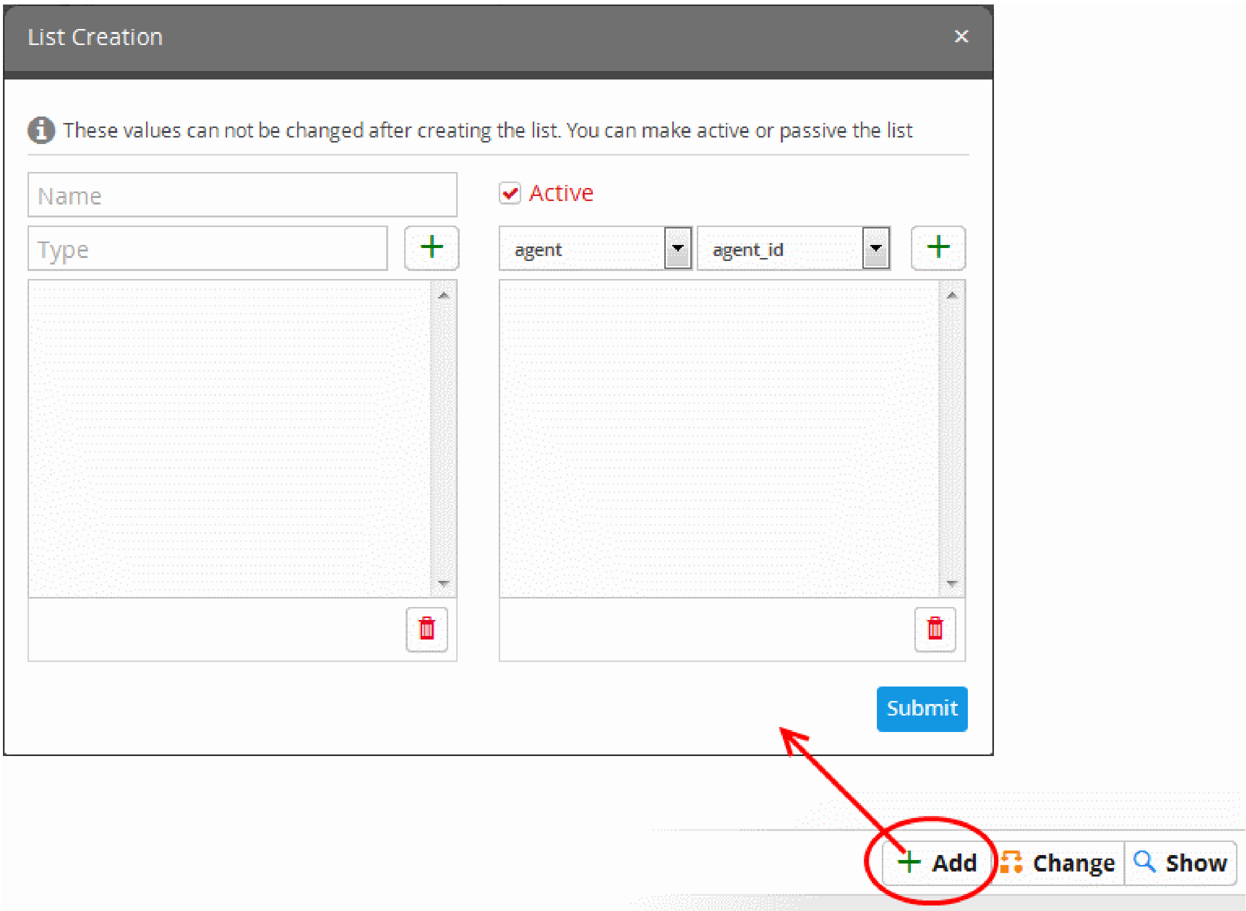
- **Creating new lists**
- **Changing activation state of lists**
- **Viewing the values entered for a list**

## Creating new lists

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

**To create a new list**

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

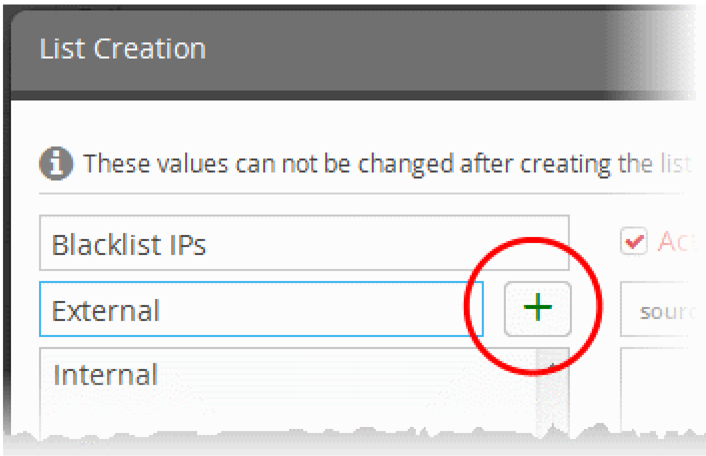


List Creation
×
These values can not be changed after creating the list. You can make active or passive the list
Name
☑ Active
Type
+
agent
agent_id
+
Submit
+ Add
Change
Show

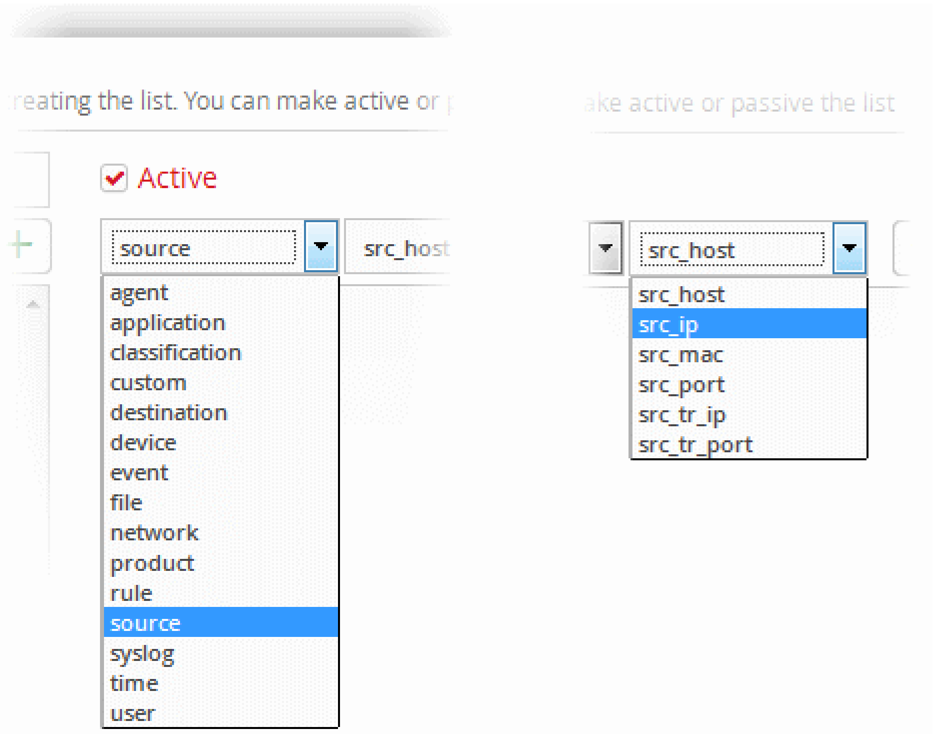
The 'List Creation' dialog will appear.

- Enter a name for the live list in the 'Name' field.
- Add a name for a list type to be create in the Type text box and click the + button.

The Type will be added to the list of types in the left pane.



- Repeat the process to add more types for the types.
- To remove a type added by mistake, select the type from the list and click the thrash can icon 🗑.
- Specify the field for which the values are to be populated in the list by selecting the 'Field Group' and choosing the Field from the respective drop-downs above the left pane.



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

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

**Caution**: The name, types and filed values once configured for a list cannot be changed or removed later. Please re-check these details before clicking 'Submit'.

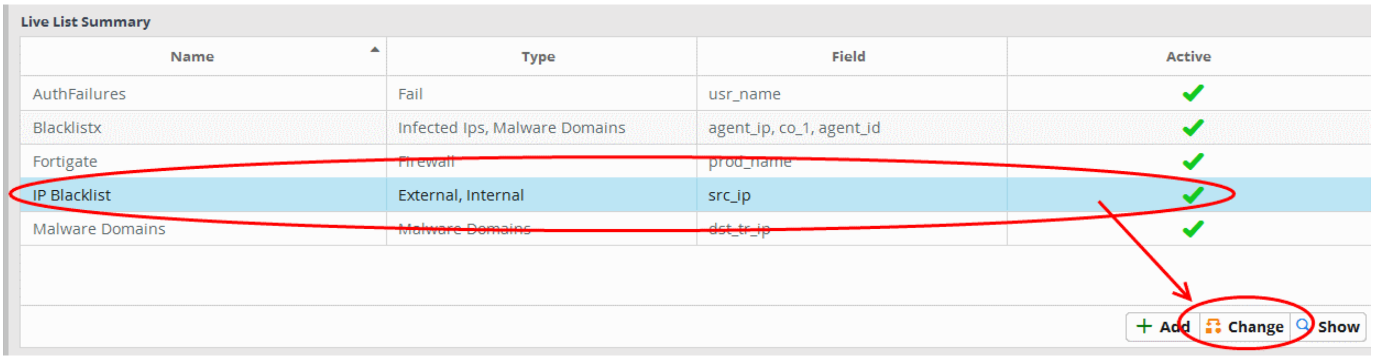
The List will be added to NxSIEM. The next step is to manage the values for the list. Refer to the section **Managing Live List Content** for more details.

## Changing  Activation State of Lists

The Live Lists can be switched between active and inactive states at any time. The inactive lists do not feed the values to the event queries and the correlation rules in which they are used.

**To change the active/inactive state of a list**

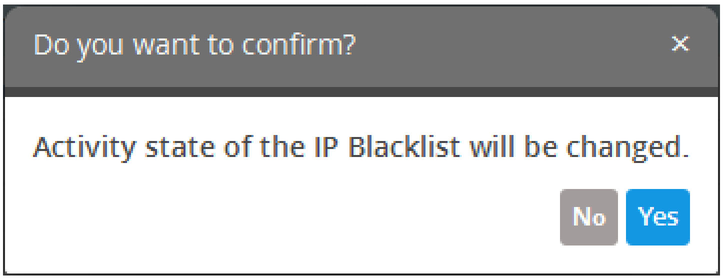
- Choose the list from the 'Live List Summary' interface and click the 'Change' button Change at the bottom right.



Live List Summary

| Name | Type | Field | Active |
|---|---|---|---|
| AuthFailures | Fail | usr_name | ✓ |
| Blacklistx | Infected Ips, Malware Domains | agent_ip, co_1, agent_id | ✓ |
| Fortigate | Firewall | prod_name | ✓ |
| IP Blacklist | External, Internal | src_ip | ✓ |
| Malware Domains | Malware Domains | dst_tr_ip | ✓ |

A confirmation dialog will appear.



Do you want to confirm?

Activity state of the IP Blacklist will be changed.

- Click 'Yes' to confirm the change.

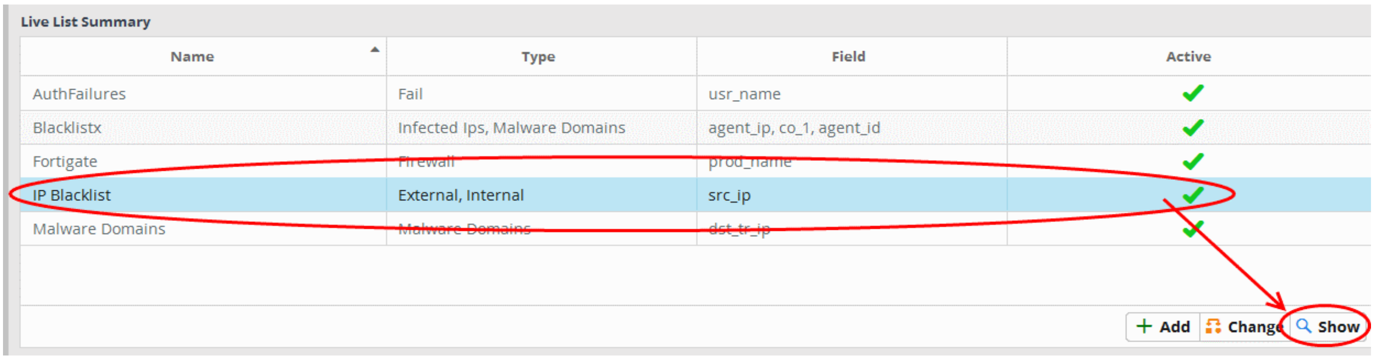
The change in the state of the list will be indicated under the 'Active' column in the 'Live List Summary' interface.

### Viewing the Values Entered for a List

The administrator can view the values for all types, added for a live list and can edit them.

**To view the values in a list**

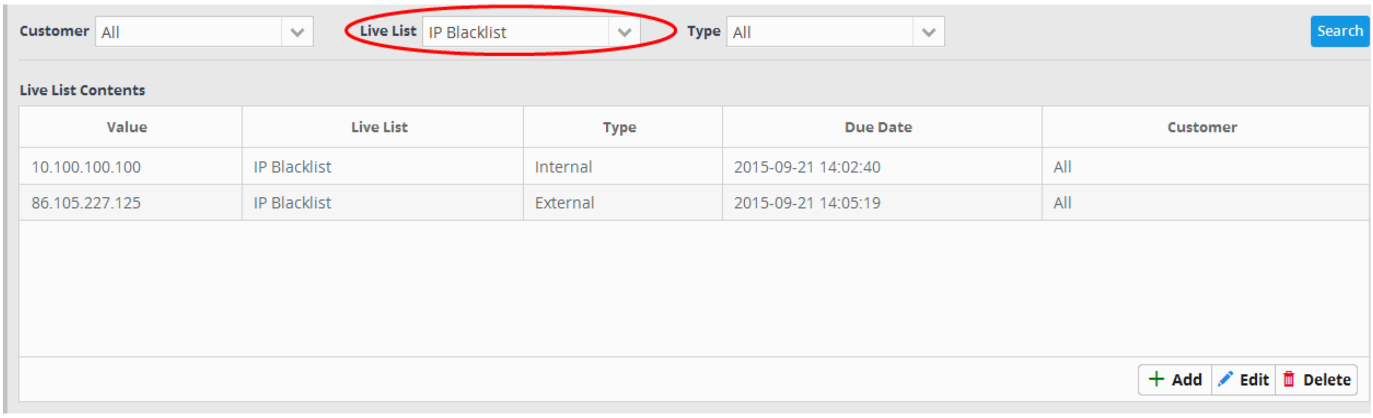
- Choose the list from the 'Live List Summary' interface and click the 'Show' button Show at the bottom right.



Live List Summary

| Name | Type | Field | Active |
|---|---|---|---|
| AuthFailures | Fail | usr_name | ✓ |
| Blacklistx | Infected Ips, Malware Domains | agent_ip, co_1, agent_id | ✓ |
| Fortigate | Firewall | prod_name | ✓ |
| IP Blacklist | External, Internal | src_ip | ✓ |
| Malware Domains | Malware Domains | dst_tr_ip | ✓ |

The 'Live List Content Management' interface will open with a list of values added to the list.



Customer: All | Live List: IP Blacklist | Type: All

Live List Contents

| Value | Live List | Type | Due Date | Customer |
|---|---|---|---|---|
| 10.100.100.100 | IP Blacklist | Internal | 2015-09-21 14:02:40 | All |
| 86.105.227.125 | IP Blacklist | External | 2015-09-21 14:05:19 | All |

For more details on adding new values and editing existing values, refer to the following section Managing Live List Content.

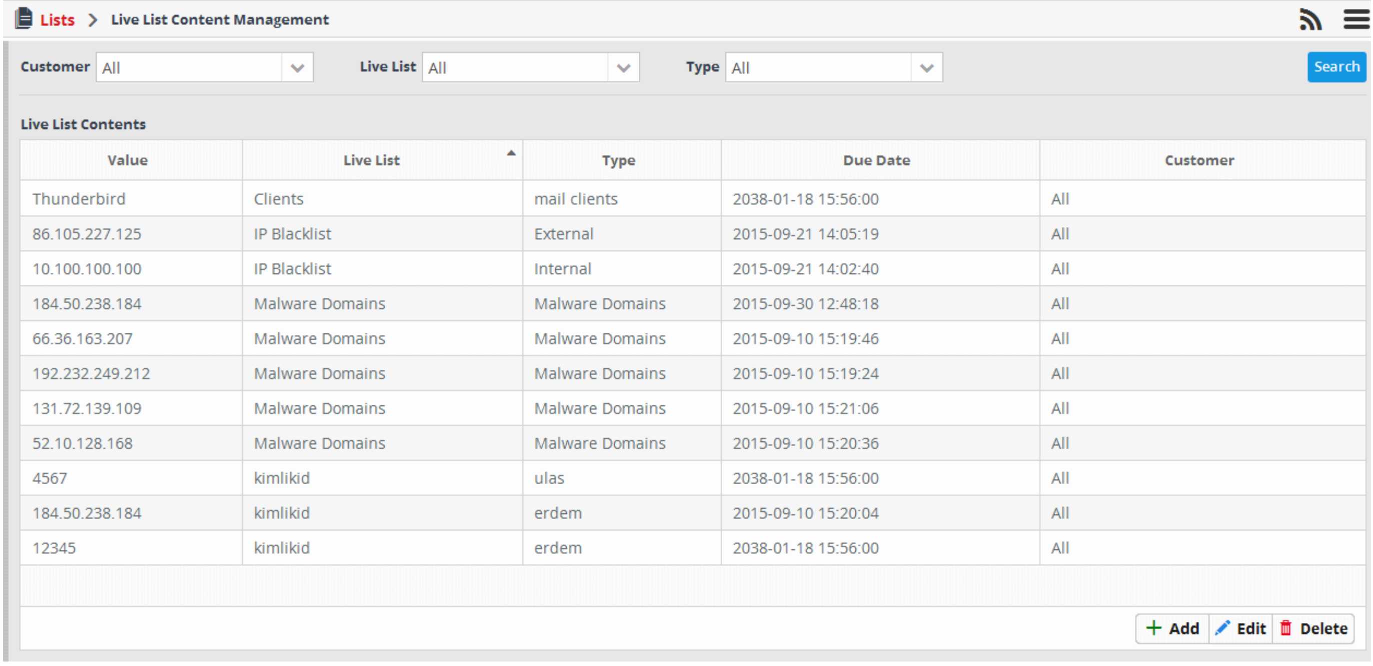
## 9.2 Managing Live List Content

The values for a Live List can be populated in two ways:

- The values can be manually entered to the list.
- Correlation rules that are used for identifying events based on certain criteria and to generate incidents, can be configured to feed the values from the events identified by it, to the live lists. Refer to the explanation of **List Mappings** in the section **Managing Rules**.

This section explains on manually adding values to lists and managing existing values. The 'Live List Content Management' interface allows the administrator to view the values added to all or selected lists, manually add new values, edit existing values and remove values from a list.

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



| Value | Live List | Type | Due Date | Customer |
|---|---|---|---|---|
| Thunderbird | Clients | mail clients | 2038-01-18 15:56:00 | All |
| 86.105.227.125 | IP Blacklist | External | 2015-09-21 14:05:19 | All |
| 10.100.100.100 | IP Blacklist | Internal | 2015-09-21 14:02:40 | All |
| 184.50.238.184 | Malware Domains | Malware Domains | 2015-09-30 12:48:18 | All |
| 66.36.163.207 | Malware Domains | Malware Domains | 2015-09-10 15:19:46 | All |
| 192.232.249.212 | Malware Domains | Malware Domains | 2015-09-10 15:19:24 | All |
| 131.72.139.109 | Malware Domains | Malware Domains | 2015-09-10 15:21:06 | All |
| 52.10.128.168 | Malware Domains | Malware Domains | 2015-09-10 15:20:36 | All |
| 4567 | kimlikid | ulas | 2038-01-18 15:56:00 | All |
| 184.50.238.184 | kimlikid | erdem | 2015-09-10 15:20:04 | All |
| 12345 | kimlikid | erdem | 2038-01-18 15:56:00 | All |

By default, the Live List Contents table shows the values added to all the lists. You can filter the table to view the values added to a specific list using the filter options from the top.

| Live List Contents Table - Column Descriptions | |
|---|---|
| **Column Header** | **Description** |
| Value | Displays the value added to a list. |
| Live List | Displays the Live List to which the value belongs. |
| Type | Displays the type of the Live List, to which the value belongs. |
| Due Date | Indicates date and time till which the value is valid in the list. On lapse of the due date, the value will be automatically removed from the list. |
| Customer | Displays the customer to which the value is applicable. |

## Sorting and Filtering Options:

- Clicking on any of 'Value', 'Live List' and 'Type' table header sorts the items in alphabetical order of entries in that column.
- To filter the values for a specific customer choose the customer from the 'Customer' drop-down and click 'Search'.
- To view the values belonging to a specific Live List, choose the list from the 'Live List' drop-down and click 'Search'.
- To view the values belonging to a specific Live List Type, select the list from the 'Live List' drop-down, then choose the type from the 'Type' drop-down and click 'Search'.

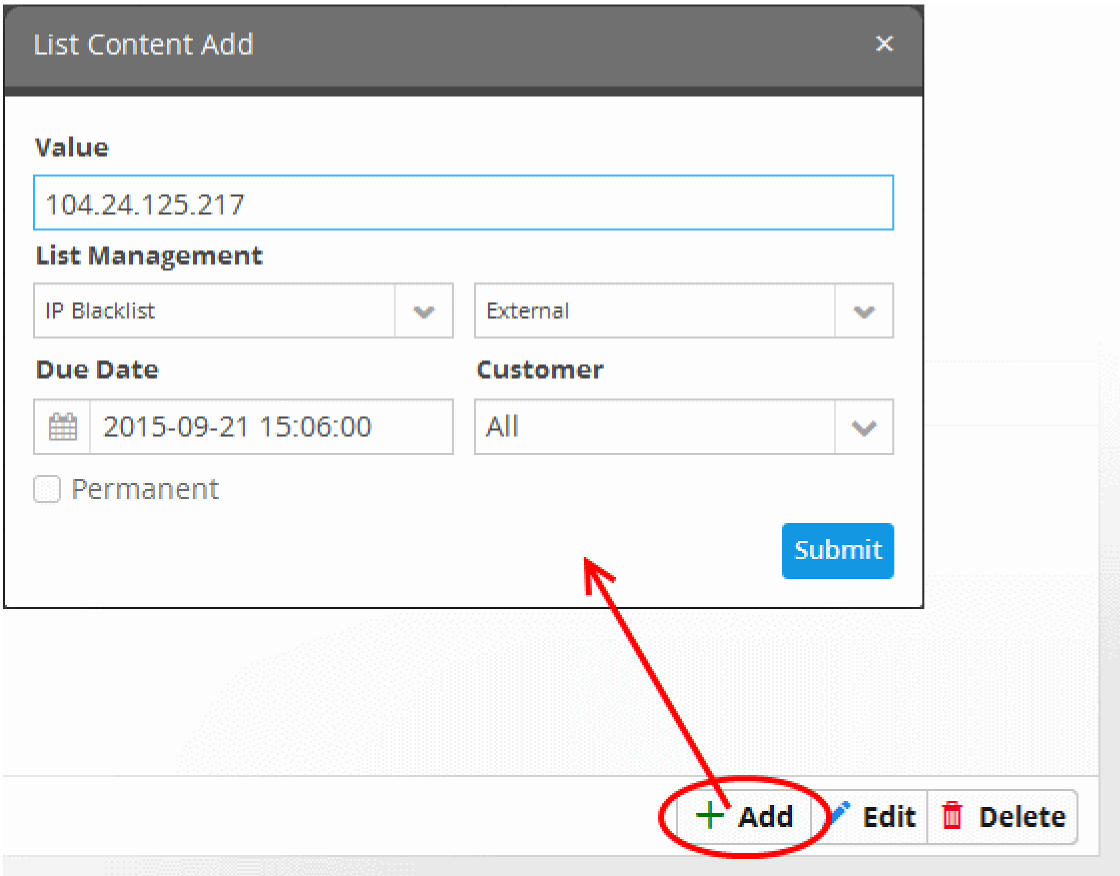
The interface allows you to:

- **Manually add values to live lists**
- **Edit existing values in a list**
- **Remove values from a list**

### To manually enter a value to a list

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

The List Content Add dialog will appear.



- Select the Live List and the list type to which the value is to be added, from the respective drop-downs under 'List Management'.
- Enter the value for the field defined for the Live List in the 'Value' field.
- Enter the date till which the value is valid in the Due Date field. You can click the calendar icon at the left of the field and choose the date. On the specified date, the value will be automatically removed from the list. If you want the value to be permanently valid, select the Permanent checkbox.
- Select the customer to which the value is applicable from the Customer drop-down.
- Click 'Submit'.

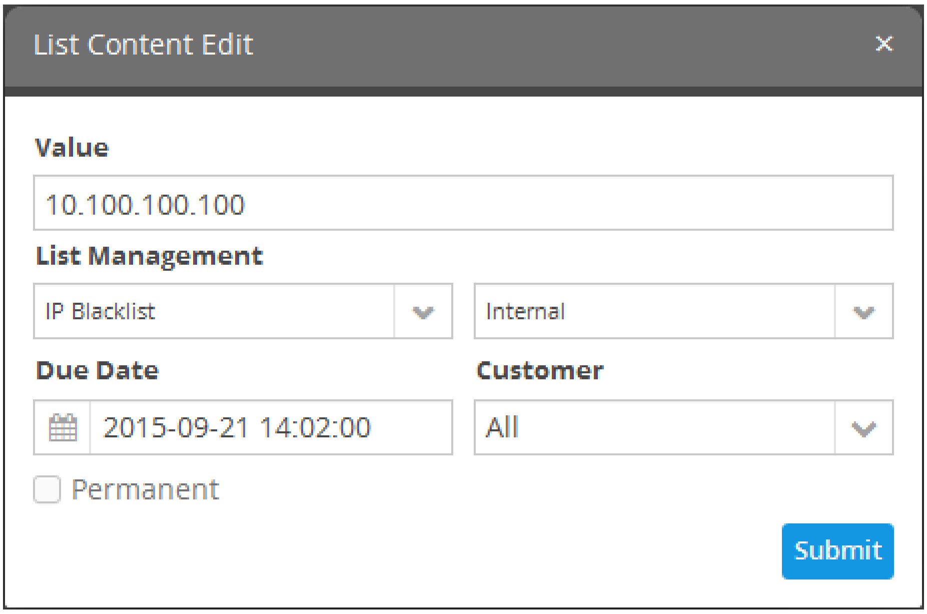
The value will be added to the selected list type.

- Repeat the process for adding more values to the list.

**To edit an existing value in a list**

- Select the Live List and choose the type from the 'Live List' and 'Type' drop-downs at the top of the Live List Content Management interface and click 'Search', to view only the values added to the required Live List/Type.
- Select the value and click the 'Edit' button Edit at the bottom right of the interface.

The List Content Edit dialog will appear for the chosen value. The dialog is similar to the List Content Add dialog. Refer to the section **above** for more details.



List Content Edit ×

Value: 10.100.100.100

List Management: IP Blacklist | Internal

Due Date: 2015-09-21 14:02:00

Customer: All

□ Permanent

Submit

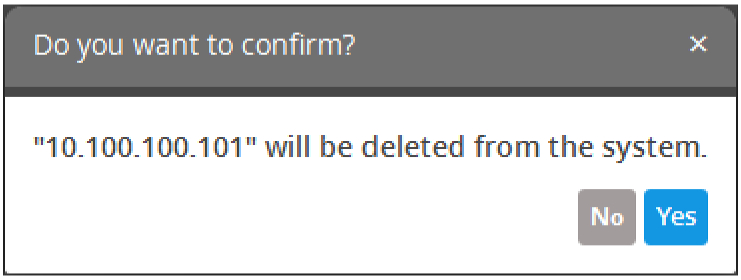
- Edit the details as required and click 'Submit'.

The value will be edited and will take immediate effect on the Event Queries and Correlation Rules in which the Live List has been used.

**To remove a value from a list**

- Select the Live List and choose the type from the 'Live List' and 'Type' drop-downs at the top of the Live List Content Management interface and click 'Search', to view only the values added to the required Live List/Type.
- Select the value and click the 'Delete' button **Delete** at the bottom right of the interface.

A confirmation dialog will appear.



Do you want to confirm? ×

"10.100.100.101" will be deleted from the system.

No | Yes

- Click Yes to confirm the removal.

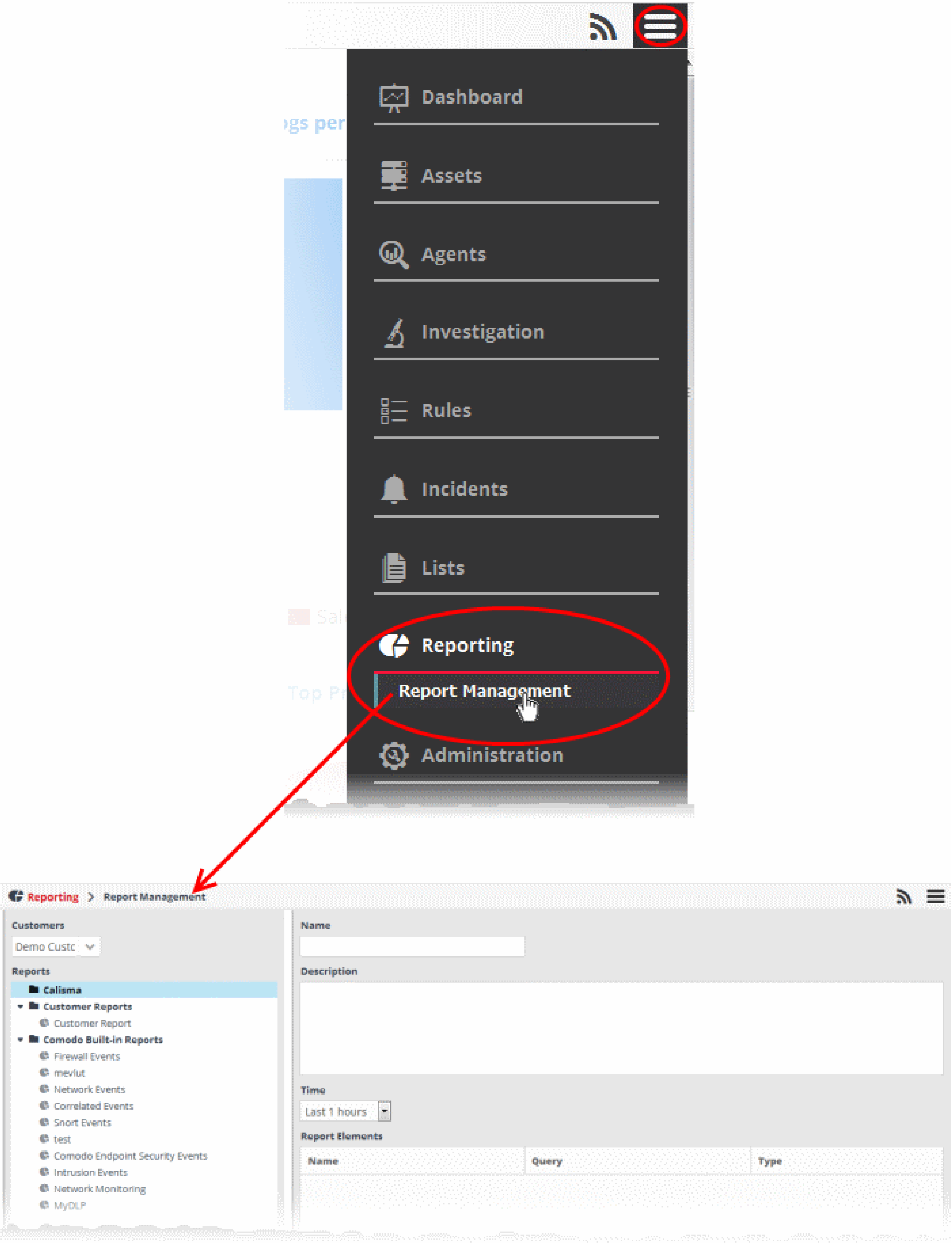
The list will be updated for the removal of the value and take effect immediately on the Event Queries and Correlation Rules in which the Live List has been used.

# 10 Managing Reports

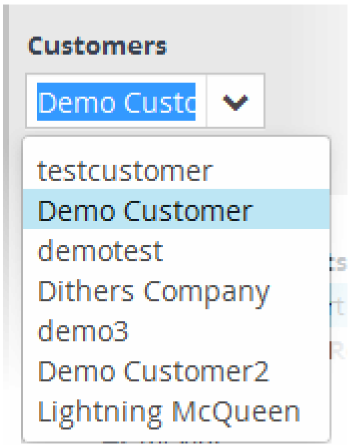
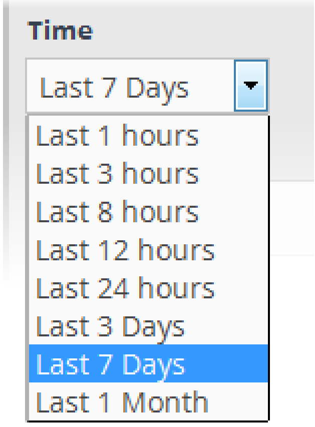
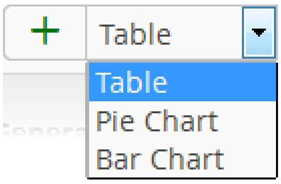
Comodo NxSIEM is capable of generating detailed event reports covering a wide range of security and productivity criteria. Reports can be generated for periods ranging from one hour to one month and configured to be displayed as tables, pie charts and bar charts. The data for the reports are fetched from the event query results. You can use both pre-defined queries and custom queries added for a customer or event create new custom queries to generate reports as required. Refer to the section '**Query Management**' for more details about configuring event queries.

The Report Management interface allows the administrator to configure and generate reports for selected customers.

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

| Report Management Interface - Table of Controls and Fields | |
|---|---|
|   Customers<br>Demo Custo<br>testcustomer<br>Demo Customer<br>demotest<br>Dithers Company<br>demo3<br>Demo Customer2<br>Lightning McQueen | The 'Customers' drop-down allows you to select the customer for which you want to create or view the report(s). |
| 📁 | Allows you to add a new report category folder to the left side panel |
| ✎ | Allows to edit the name of a selected report category folder |
| ◔ | Allows you to add a new report type under a selected category folder |
| 🗑 | Allows to delete selected report category folders or report type from the left hand side pane. |
| **Name** | Displays the name of the report chosen from the left hand side pane. Allows you to enter the name for the report, when creating a new report. |
| **Description** | Displays a brief description about the report chosen from the left hand side pane. Allows you to enter a brief description the for the report, when creating a new report. |
|   Time<br>Last 7 Days<br>Last 1 hours<br>Last 3 hours<br>Last 8 hours<br>Last 12 hours<br>Last 24 hours<br>Last 3 Days<br>Last 7 Days<br>Last 1 Month | Allows you to select the time period for report generation. Options ranges from the last hour to the entire previous month. |
| **Report Elements** | Displays the list of contents in the report with details like their name, the event query based on which the data is populated in the report component and the type of the report component, like table, pie or bar chart. |
|  | Allows you to add a report element to the selected report and choose the type of chart for the report element. |

| Report Management Interface - Table of Controls and Fields | |
|---|---|
| ✎ | Allows to edit a report element. |
| 🗑 | Allows to delete a report element from the list. |
| **Generated Reports** | Displays the list of reports generated so far for the selected customer and allows you to download any report as a .pdf file. |
| **Show Last Generated Report** | On selecting this option, the last generated report for the customer is displayed. |
| Generate | Allows you to instantly generate the selected report. |
| Schedule | Allows you to specify the automatic generation of the selected reports according to a schedule of your choice |
| Save | Allows to save a configured report. |

Following sections explain on:

- **Managing Reports Folders**
- **Adding and Configuring Reports**
- **Generating a Report**
- **Scheduling Report generation**
- **Downloading/Viewing Report**
- **Editing Report Settings**
- **Managing generated Reports**

## Manage a Reports Category Folder

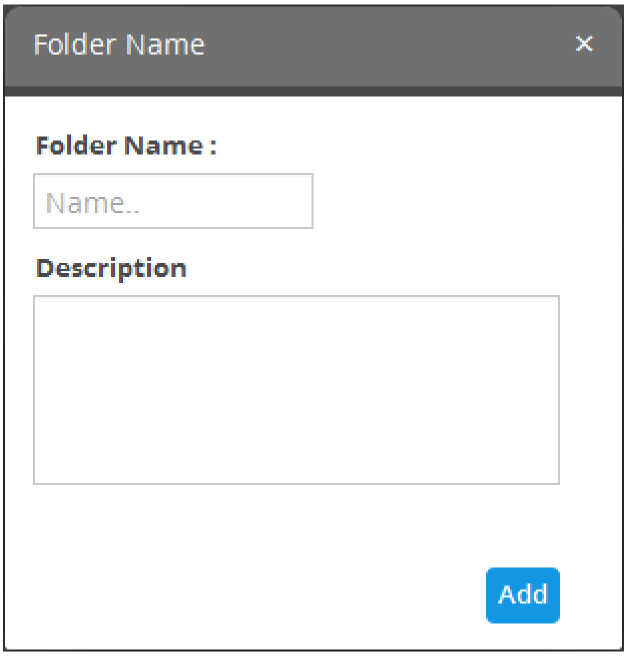
Each report folder contains a collection of reports of a specific category. Every new report configured, must always be placed in a category folder.

**Creating a reports group folder**

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

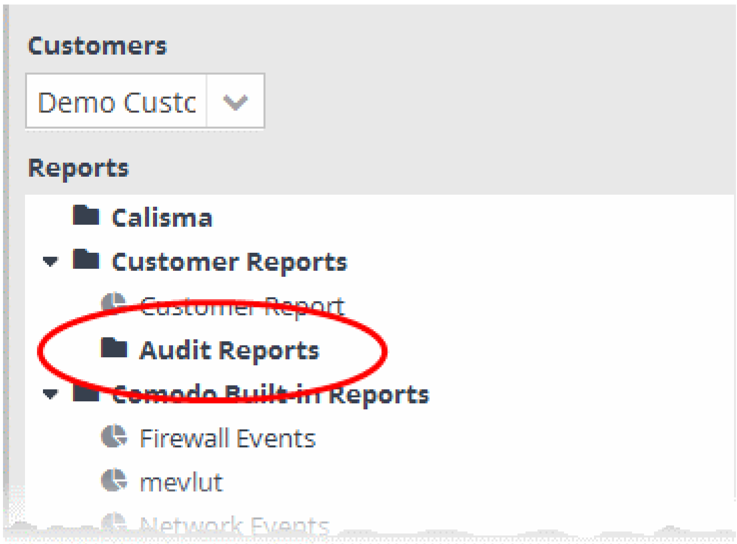
A list of predefined reports added for the customer is displayed as a tree structure in the 'Reports' pane.

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



- Enter a name for the new folder in the 'Folder Name' field
- Enter a description for the folder
- Click the 'Add' button

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



The relevant reports can now be placed under the newly created folder. Refer to the '**Adding and Configuring a Report**' for more details.

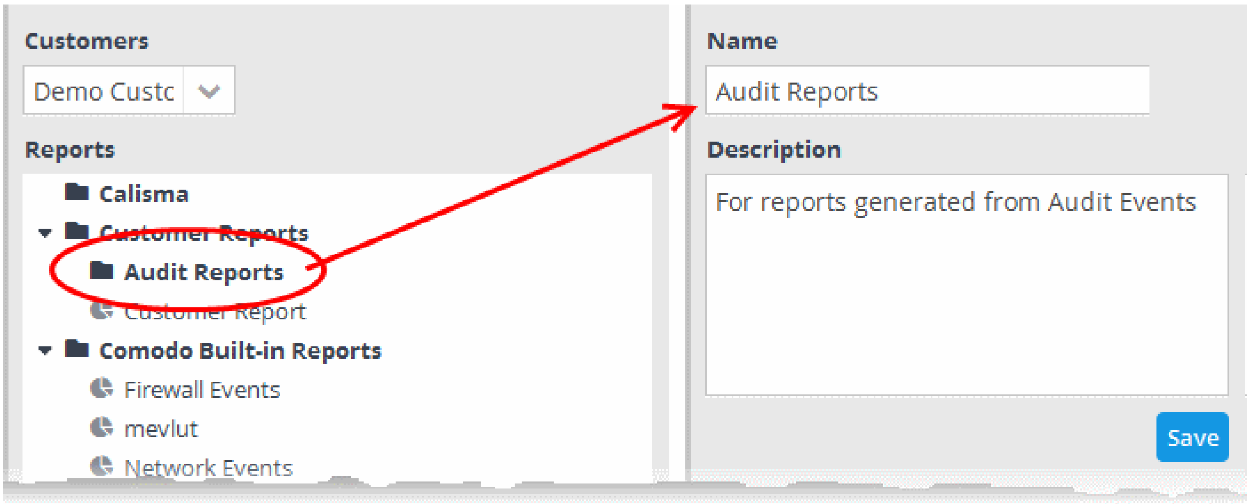
**Editing a reports group folder**

- To edit the name of a reports group folder, select it and click the ✎ button.

The 'Folder Name' dialog will appear.

- Edit the name and/or the description as as required and click the 'Save' button

Alternatively, click on the folder, edit the details on the right side and click the 'Save' button.



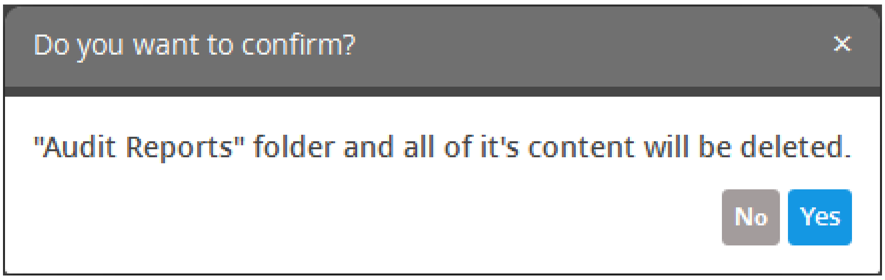
Name: Audit Reports

Description: For reports generated from Audit Events

**Deleting a reports group folder**

- To delete a reports group folder, select it and click the 🗑 button.

A confirmation dialog will appear.


Do you want to confirm?

"Audit Reports" folder and all of it's content will be deleted.

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

## Add and Configure a Report

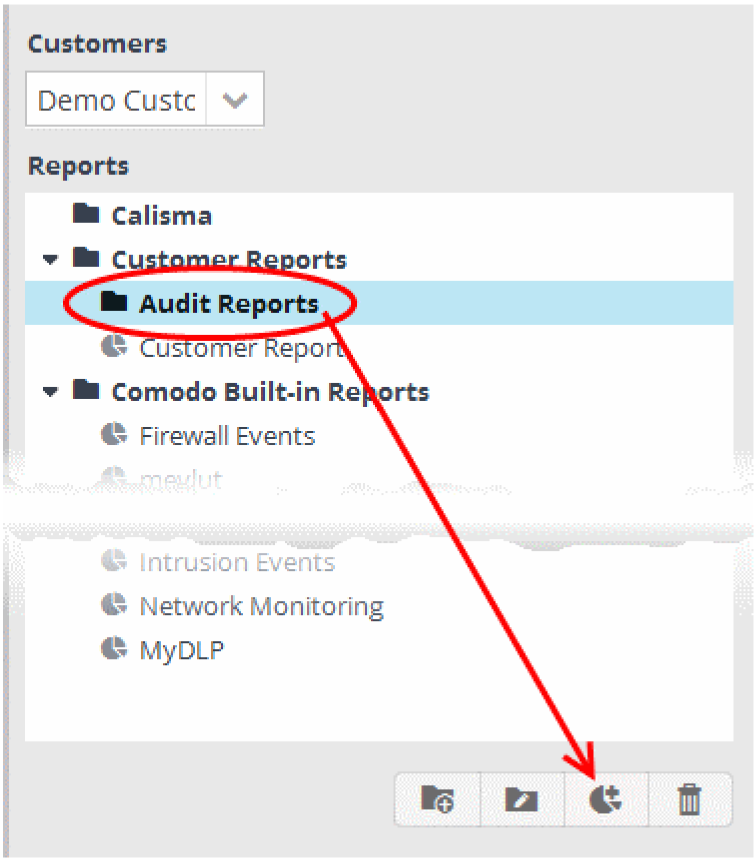
Comodo NxSIEM ships with a set of pre-defined reports which are listed under the 'Comodo Built-in Reports' folder in the left hand side panel of the 'Report Management' interface. The interface also allows the administrator to configure custom reports for various categories of events for selected customer and save them under the respective category folder. The reports can be generated at anytime as and when required for the customer.

**To add a new report for a customer**

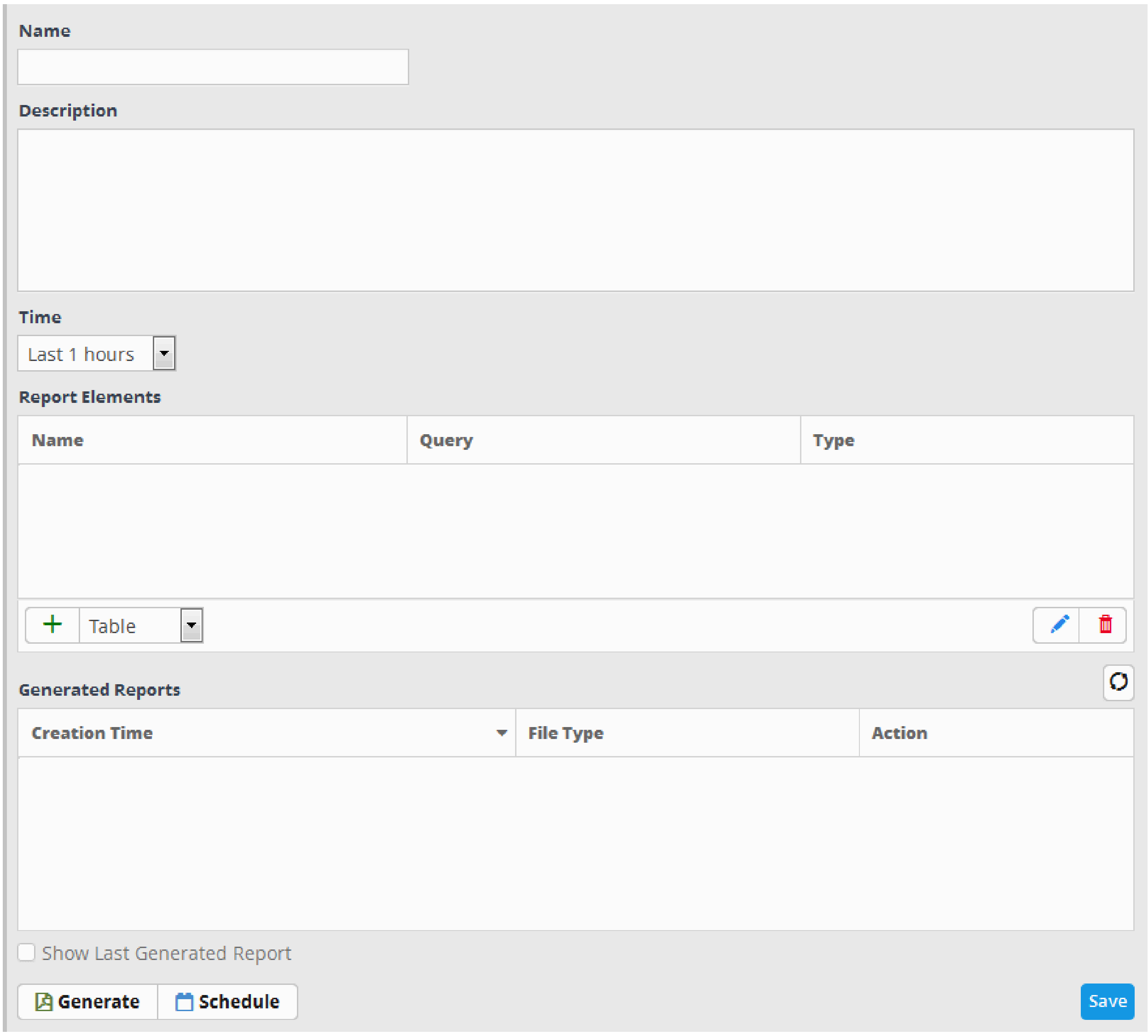
- Choose the customer from the 'Customers' drop-down at the top of the left panel.

A list of predefined reports added for the customer is displayed as a tree structure in the 'Reports' pane.

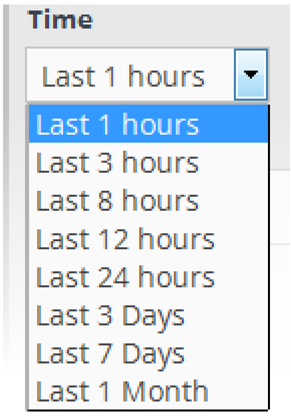
- Select the appropriate folder or **create a new folder** under which you want to create a report.
- Click the button.



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



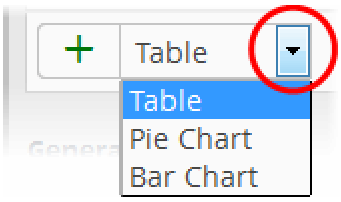
- Enter a name for the report in the 'Name' field
- Enter an appropriate description for the report in the 'Description' text box
- Select the period for which the events are to be included in the report, from the 'Time' drop-down



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. Refer to the section '**Query Management**' for more details about configuring event queries.

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



The options available are:

- **Table** - 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.

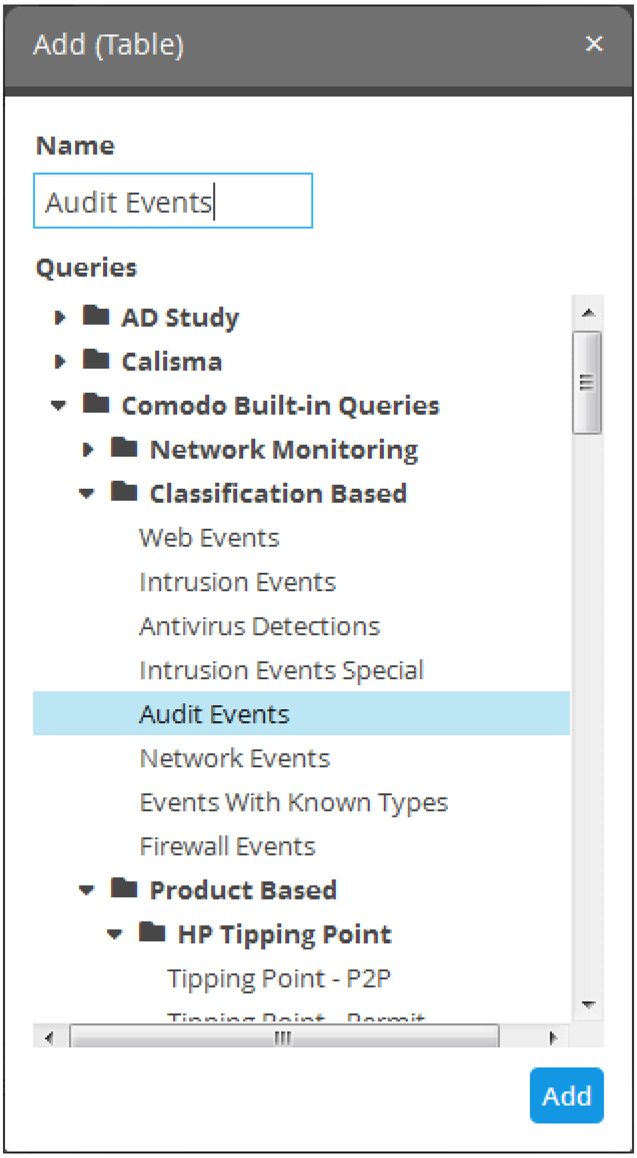
### 'Table' type Report Element

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

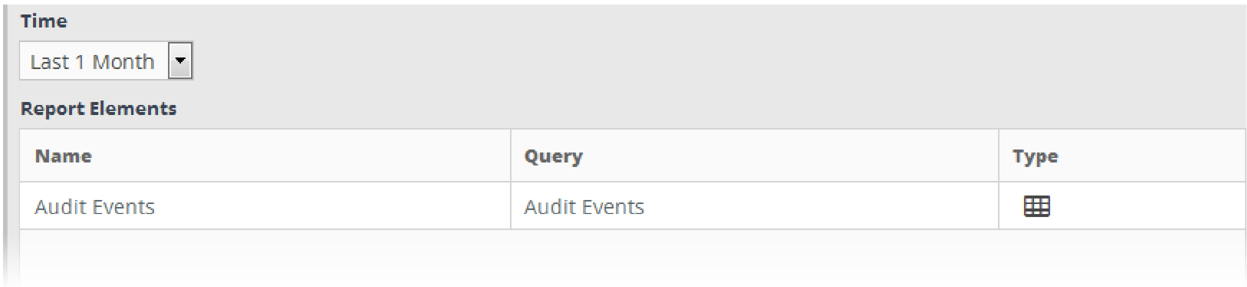
Audit Events

Queries

- AD Study
- Calisma
- Comodo Built-in Queries
  - Network Monitoring
  - Classification Based
    - Web Events
    - Intrusion Events
    - Antivirus Detections
    - Intrusion Events Special
    - Audit Events
    - Network Events
    - Events With Known Types
    - Firewall Events
  - Product Based
    - HP Tipping Point
      - Tipping Point - P2P
      - Tipping Point - Permit

- 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. This table is the same as **configured in the event queries**.
- 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 reports can be configured by specifying the following parameters:

**'Event Query' + 'Group By' + 'Aggregation Function' + 'Order By' + 'Limit'**

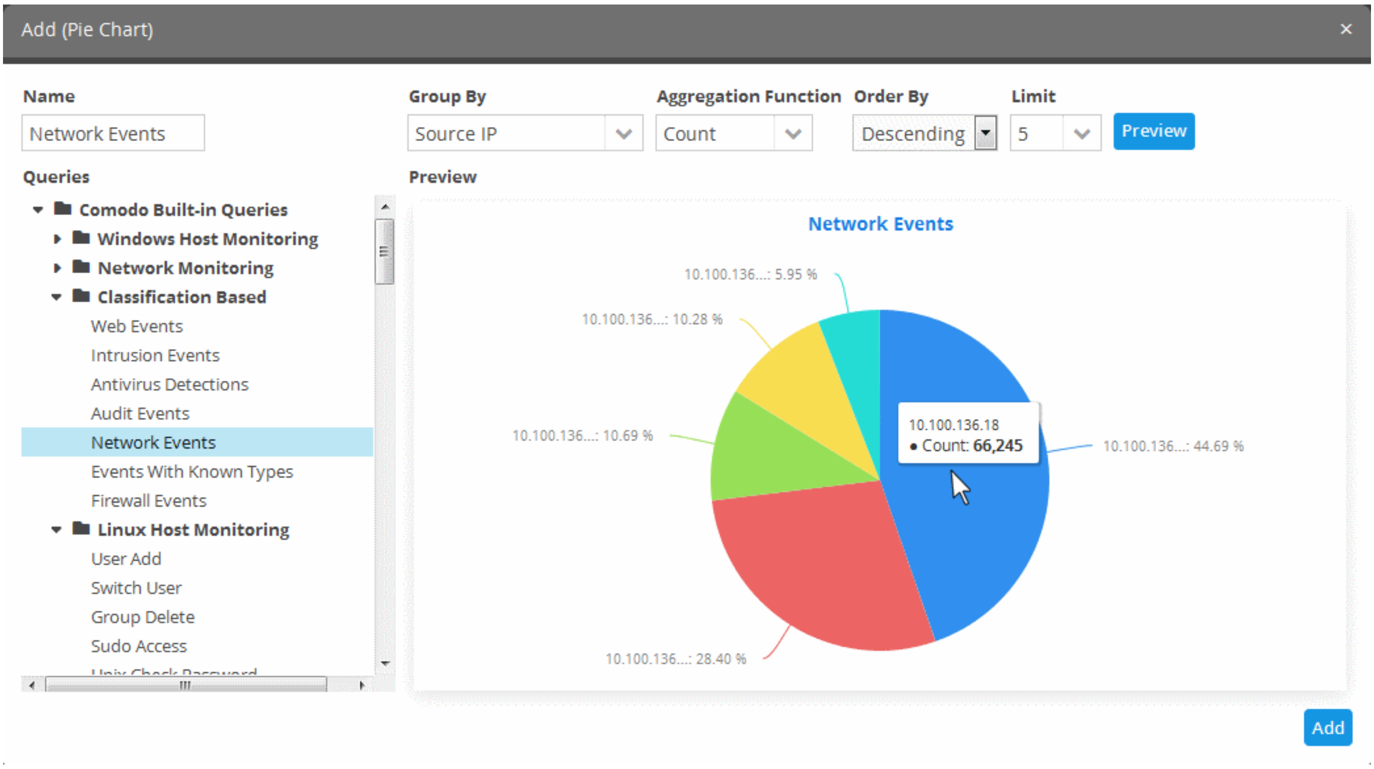
- Event Query - The query whose results are to be displayed in the chart. The query can be selected from the list of queries, added fro the selected customer. The events that are detected based on the query for the last one hour will be displayed in the charts.

- Group By - The field, based on whose values, the events identified by the query are to be grouped and shown in the chart. Event groups will be formed so that each event group will have events with same value for the selected field.
- Aggregation Function - The event groups formed based on the fields chosen in the 'Group by' option, are ranked based chosen 'Aggregation Function'. The event groups are indicated in the charts in ascending or descending order as chosen in the 'Order by' setting. The available options are:
  - Count - The event groups are ranked based on the number of events in each group. For example, if you choose Source IP as 'Field' then the group which contains the most events on a particular source IP will have the top rank and the group containing the lowest number of events is ranked lowest. You can further control how the data is displayed by modifying the 'Order By' and 'Limit' parameters.
  - Sum - The event groups are ranked based on sum of values in another field that contains numerical value. If you choose 'Sum', you need to select another field that contains a numerical value, like bytes in/out. The event groups are ranked based on the sum of the values in the chosen numerical field from all the events in that group. For example, if we choose 'Bytes-in' as numerical value, then the system adds up the values in the 'Bytes-in' field of all the events in a group and ranks the group accordingly. This will tell you which source IP has the most incoming traffic. The event group with the highest SUM in the 'Bytes-in' field is ranked top and vice-versa.
  - Average - Similar to above. Event groups are ranked based on the average of the values of the chosen numerical field from all the events in that group. (e.g. the average of values of 'Bytes_in' field of events in the group, if we take the same example as above)
  - Minimum - Similar to above. The event groups are ranked based on the minimum of the values of chosen numerical field from all the events in that group.
  - Maximum - Similar to above. The event groups are ranked based on the maximum of the values of chosen numerical field from all the events in that group.
- Order By - 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

Example:

The following screenshot shows the preview of resulting pie chart from the following configuration parameters:

'Network Events' + 'Source IP' + 'Count' + 'Descending' + '5'



Add (Pie Chart)

Name: Network Events

Group By: Source IP

Aggregation Function: Count

Order By: Descending

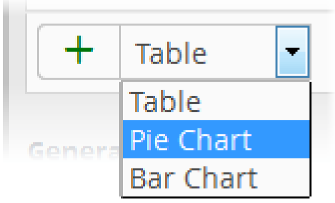
Limit: 5

The following sections explain on:

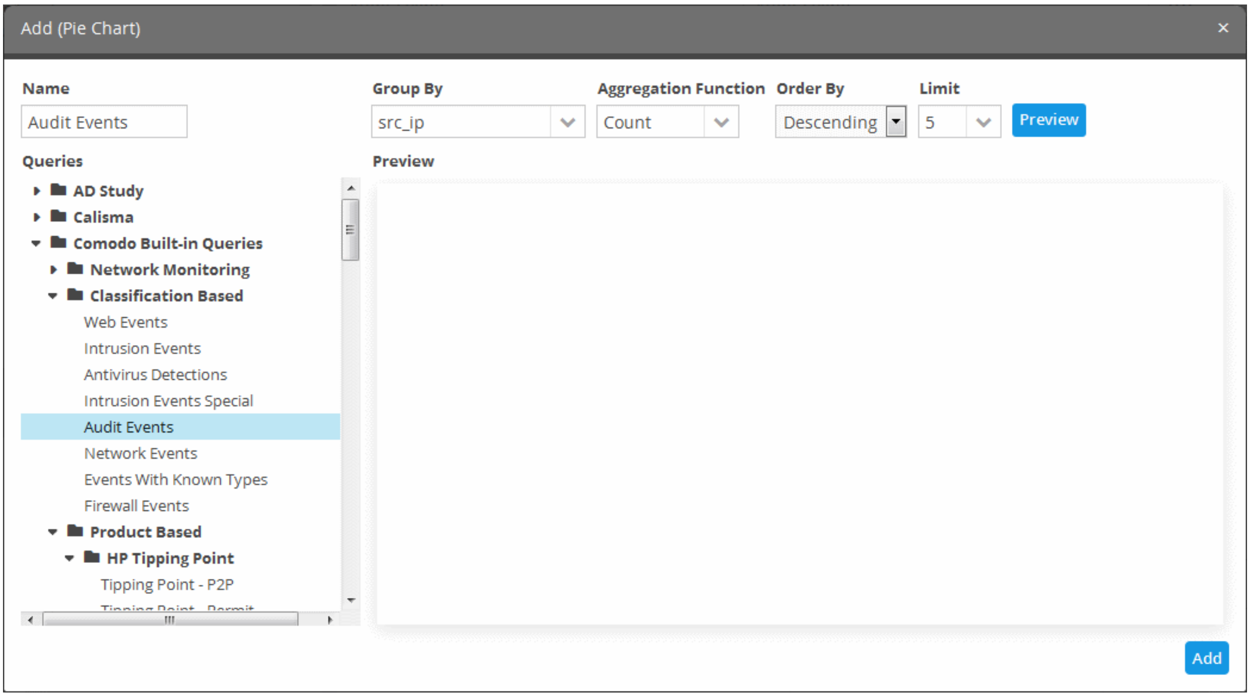
- Adding a pie chart
- Adding a bar chart

**To add a Pie Chart type report**

- Select 'Pie Chart' from the drop-down and click the + button beside it



The 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

Queries

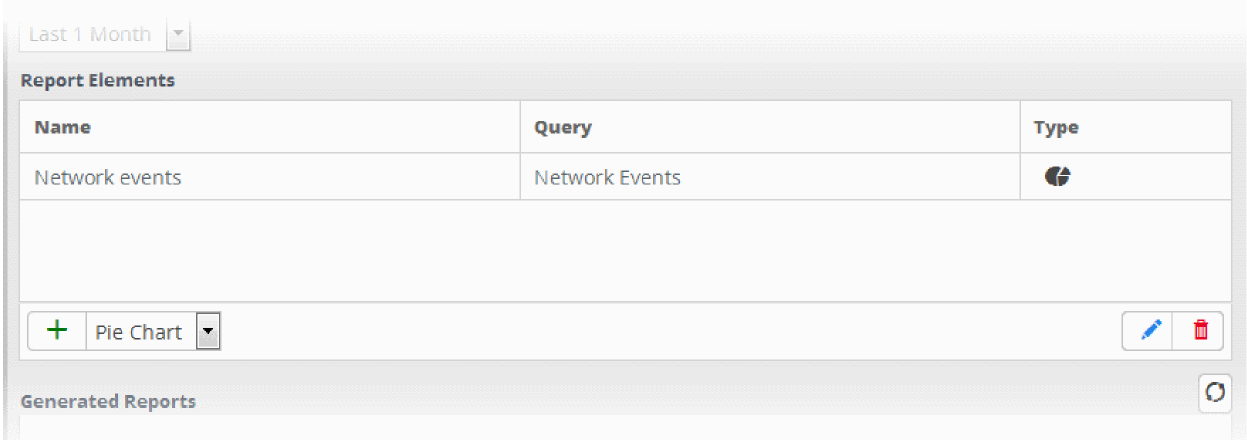
- AD Study
- Calisma
- Comodo Built-in Queries
  - Network Monitoring
  - Classification Based
    - Web Events
    - Intrusion Events
    - Antivirus Detections
    - Intrusion Events Special
    - Audit Events
    - Network Events
    - Events With Known Types
    - Firewall Events
  - Product Based
    - HP Tipping Point
      - Tipping Point - P2P
      - Tipping Point - Permit

| Add (Pie Chart) - Form Parameters | |
|---|---|
| **Parameter** | **Description** |
| Name | Enter an appropriate name for the report element |
| Queries | Displays the list of predefined and custom event queries added for the selected customer. Select the event query for which the results are to be displayed in the chart. |
| Group By | The drop-down displays the fields, configured as event query results table column headers for the selected event query. Refer to '**Configure results table for a query**' for more details.<br>Choose the Field based on whose values, the events identified by the query are to be grouped and shown in the chart. |
| Aggregation Function | Allows you to choose the aggregation operation to be applied for ranking the event groups and show them in ascending or descending order, in the chart. The options available are:<br>• 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.<br>• Sum - The event groups are ranked based on sum of values in another field that contains numerical value. If you choose 'Sum', you need to select another field that contains a numerical value, like bytes in/out. The event groups are ranked based on the sum of the values in the chosen numerical field from all the events in that group. For example, if we choose 'Bytes-in' as numerical value, then the system adds up the values in the 'Bytes-in' field of all the events in a group and ranks the group accordingly. This will tell you which source IP has the most incoming traffic. The event group with the highest SUM in the 'Bytes-in' field is ranked top and vice-versa.<br>• 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)<br>• Minimum - Similar to above. The event groups are ranked based on the minimum of the values of chosen numerical field from all the events in that group. |

| | |
|---|---|
| | - Maximum - Similar to above. The event groups are ranked based on the maximum of the values of chosen numerical field from all the events in that group. |
| Order By | Allows you to choose the order in which the event groups are to be indicated in the chart, based on their ranking. The available options are:<br>- 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.<br>- Descending - The group with the highest rank will be top of the list.. A limit of 5 will show the 5 groups with the highest ranks. |
| Limit | Enter the number of events to be displayed for the chart |
| Preview | This button allows to preview the chart before adding it to the report. |
| Add | Click this button to add the chart to the report |

- Enter the parameters for the chart as shown in the table above and click the 'Preview' button to check the chart before adding it to the report.
- Click the 'Add' button

The configured report element will be added to the list.

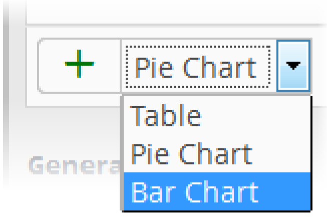


Report Elements

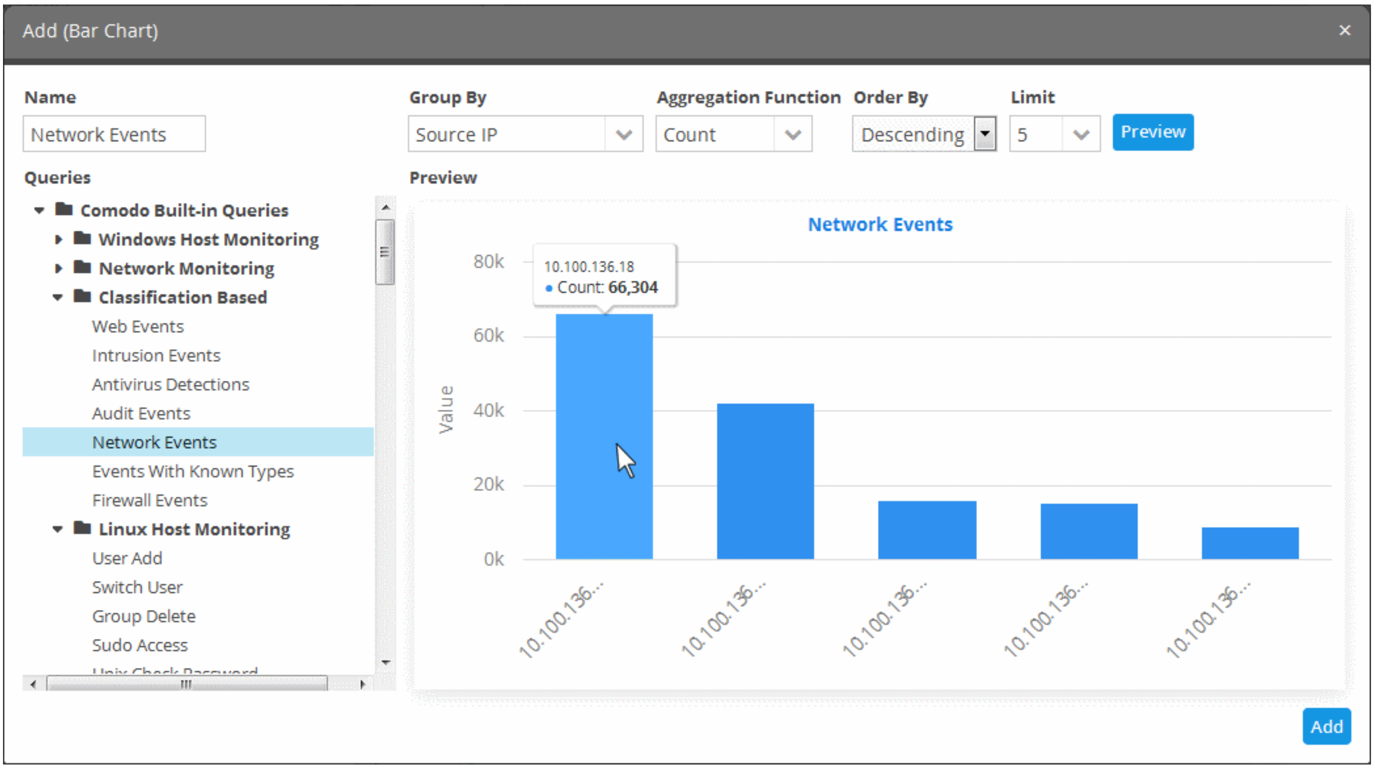
| Name | Query | Type |
|---|---|---|
| Network events | Network Events | ◕ |

**To add 'Bar Chart' type report element**

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



The procedure is same as **adding a pie chart report element** explained above.



Add (Bar Chart)

Name: Network Events

Group By: Source IP

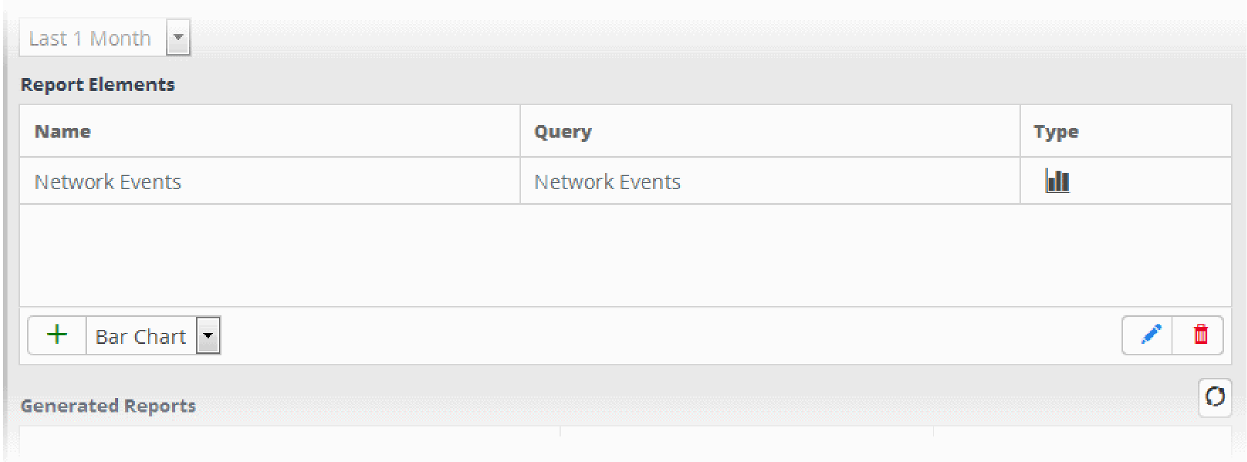
Aggregation Function: Count

Order By: Descending

Limit: 5

- Click the 'Add' button

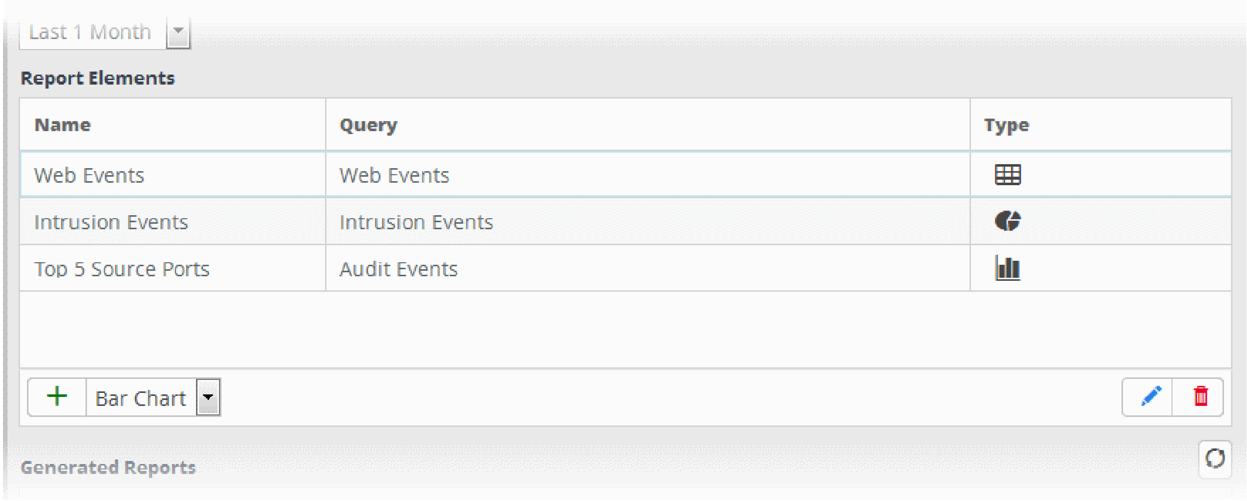
The configured report element will be added to the list.



Report Elements

| Name | Query | Type |
|---|---|---|
| Network Events | Network Events | 📊 |

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 | 📊 |

Generated Reports

- **Name** - Displays the name of the report element
- **Query** - Displays the name of the event query that was used to configure 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.

Now that you have configured a report, you can **generate the report** and/or **schedule the report generation**.

## Generate a Report

After configuring a report, you can generate it manually or specify the **automatic generation of the report** according to a schedule of your choice.

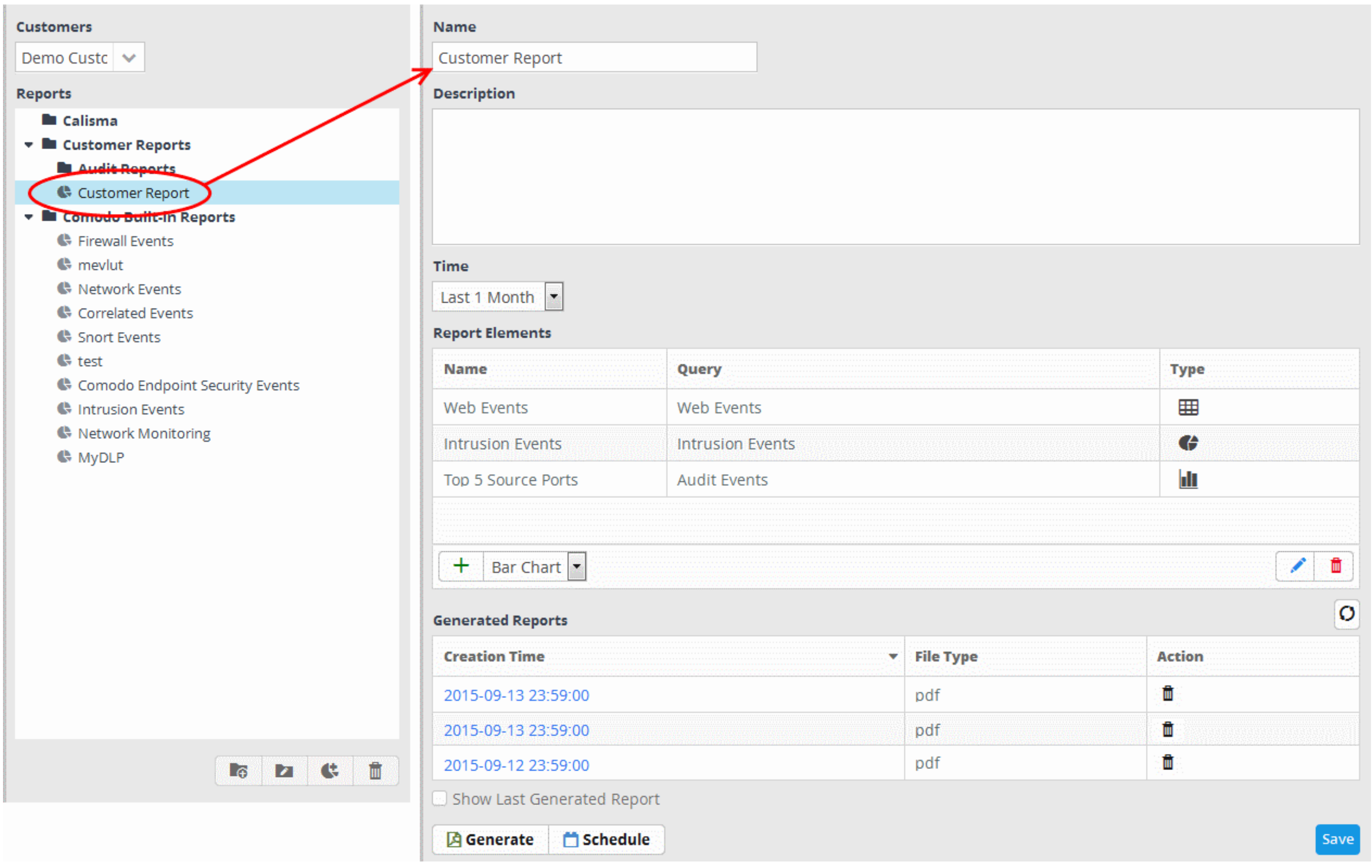
### To manually generate a report

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

A list of predefined and custom reports added for the customer is displayed as a tree structure in the 'Reports' pane.

- Select the report from the list.

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



Customers: Demo Custc

Reports

- Calisma
- Customer Reports
  - Audit Reports
  - Customer Report
- Comodo Built-in Reports
  - Firewall Events
  - mevlut
  - Network Events
  - Correlated Events
  - Snort Events
  - test
  - Comodo Endpoint Security Events
  - Intrusion Events
  - Network Monitoring
  - MyDLP

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

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.

Refer to the section '**Download / View a Report**' for more details about how to download and /or view a report.

## Schedule a Report Generation

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

### To schedule a report generation

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

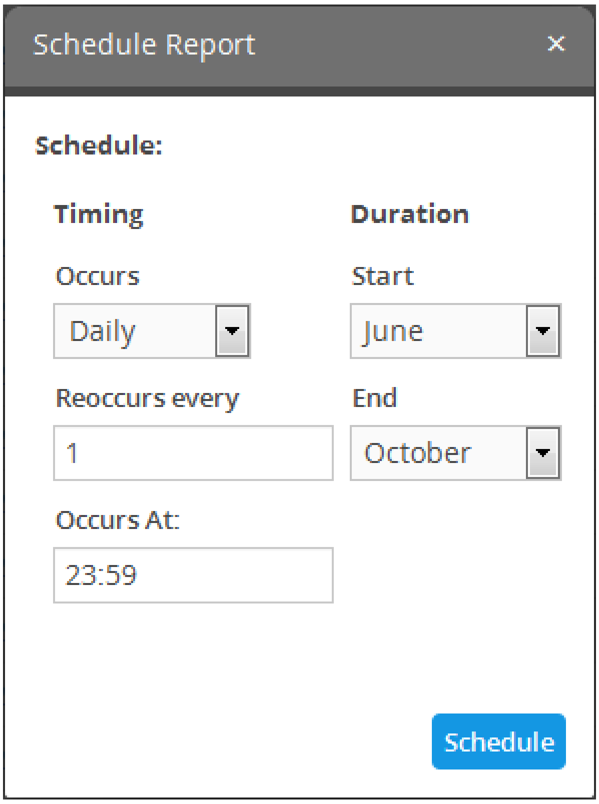
A list of predefined and custom reports added for the customer is displayed as a tree structure in the 'Reports' pane.

- Select the report from the list.

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

- Click the 'Schedule' button at the bottom of the 'Generated Reports' area.

The 'Schedule Report' dialog will be displayed.



Schedule Report

Schedule:

Timing

Occurs: Daily

Reoccurs every: 1

Occurs At: 23:59

Duration

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. The options available are:
  - Hourly
  - Daily
  - Weekdays
  - Weekend
  - Weekly
  - Monthly
- **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.

## Download / View a Report

The 'Generated Reports' area in the 'Report Management' interface allows you to download and / or view any generated report.

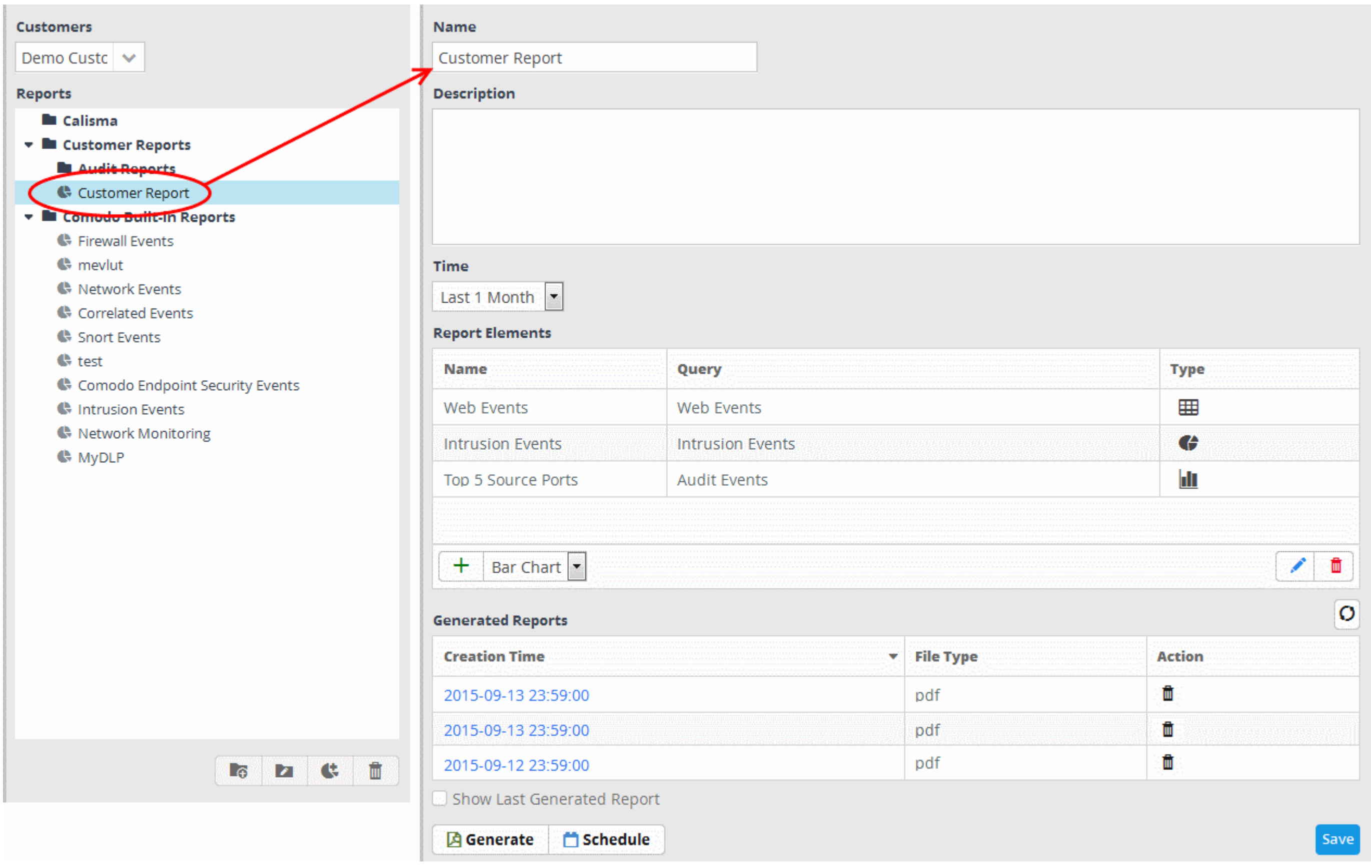
### To download / view a report

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

A list of predefined and custom reports added for the customer is displayed as a tree structure in the 'Reports' pane.

- Select the report from the list.

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



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 | ▮ |

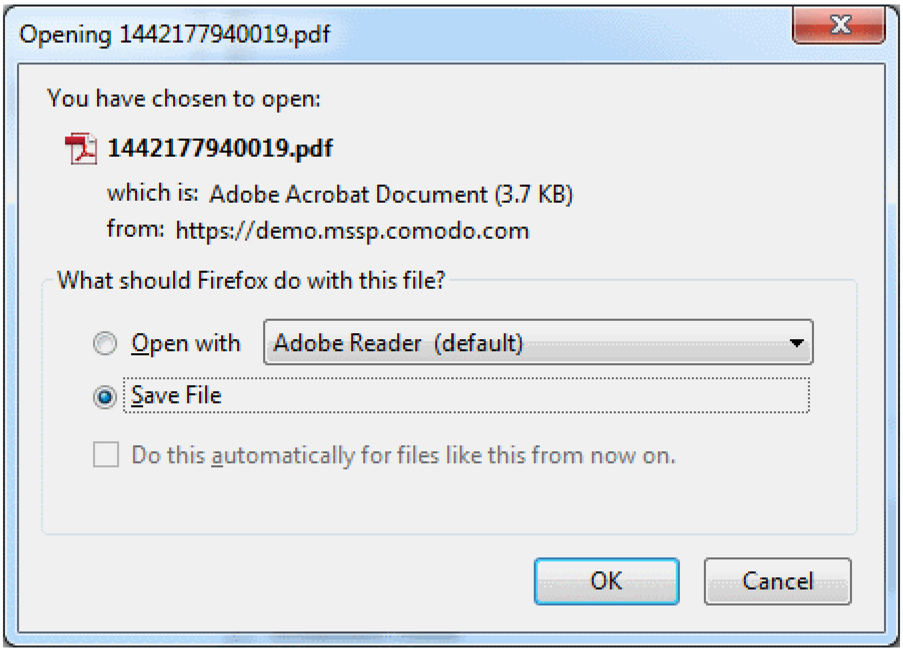
Generated Reports

| 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

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

- To download a report, click on the time stamp link of it under the 'Creation Time' column.



Opening 1442177940019.pdf

You have chosen to open:

1442177940019.pdf

which is: Adobe Acrobat Document (3.7 KB)

from: https://demo.mssp.comodo.com

What should Firefox do with this file?

○ Open with Adobe Reader (default)

● Save File

□ Do this automatically for files like this from now on.

You can download the report in .pdf format.

- To view the last generated report instantly, select the 'Show Last Generated Report' check box.

The report will be displayed in the 'Last Generated Report' area, below 'Generated Reports' area.

## Edit Report Settings

You can change the name, description, report elements and their configuration at any time from the Report management interface.

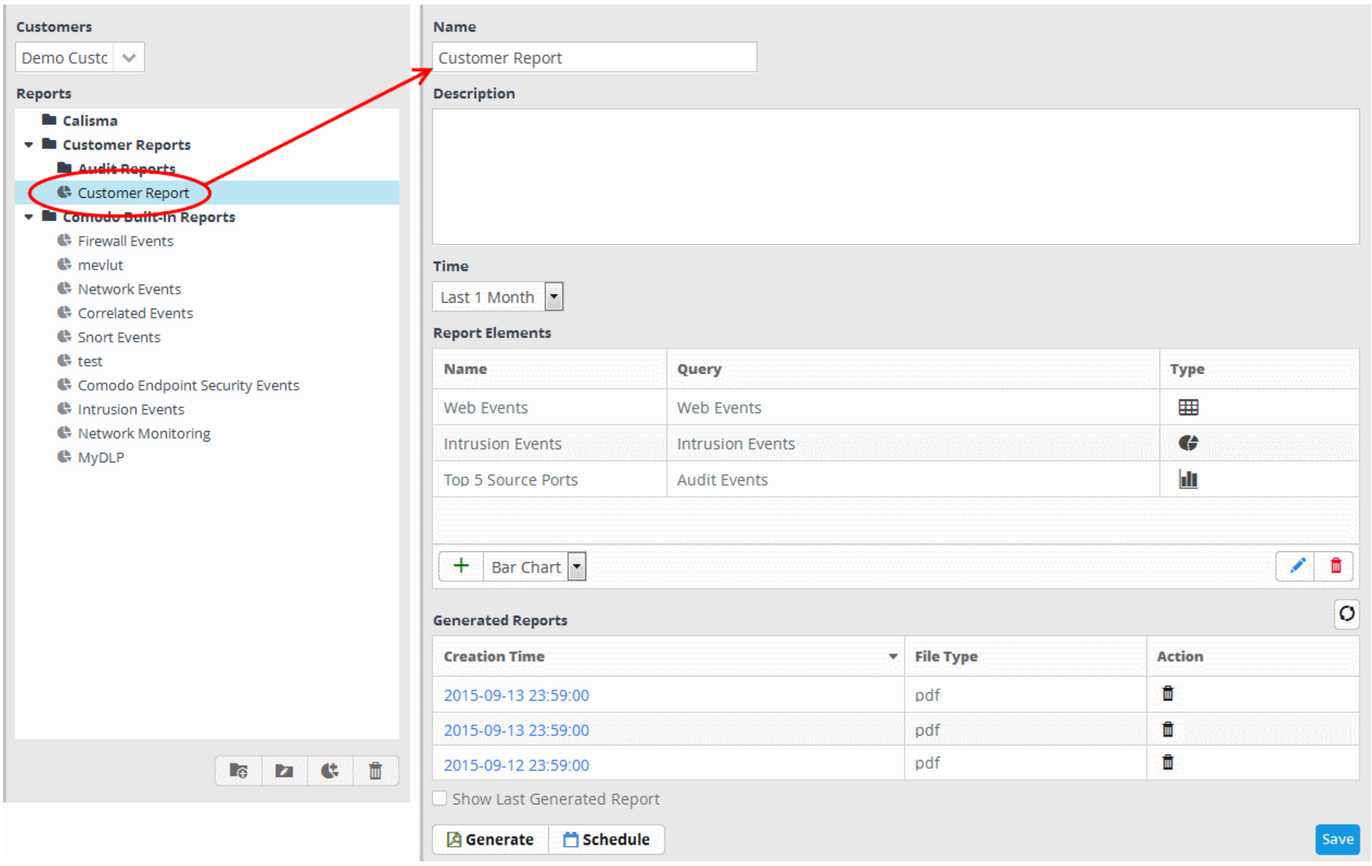
### To edit a report

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

A list of predefined and custom reports added for the customer is displayed as a tree structure in the 'Reports' pane.

- Select the report from the list.

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



Customers

Demo Custc

Reports

- Calisma
- Customer Reports
  - Audit Reports
  - Customer Report
- Comodo Built-in Reports
  - Firewall Events
  - mevlut
  - Network Events
  - Correlated Events
  - Snort Events
  - test
  - Comodo Endpoint Security Events
  - Intrusion Events
  - Network Monitoring
  - MyDLP

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 | 📊 |

+ Bar Chart

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 | 🗑 |

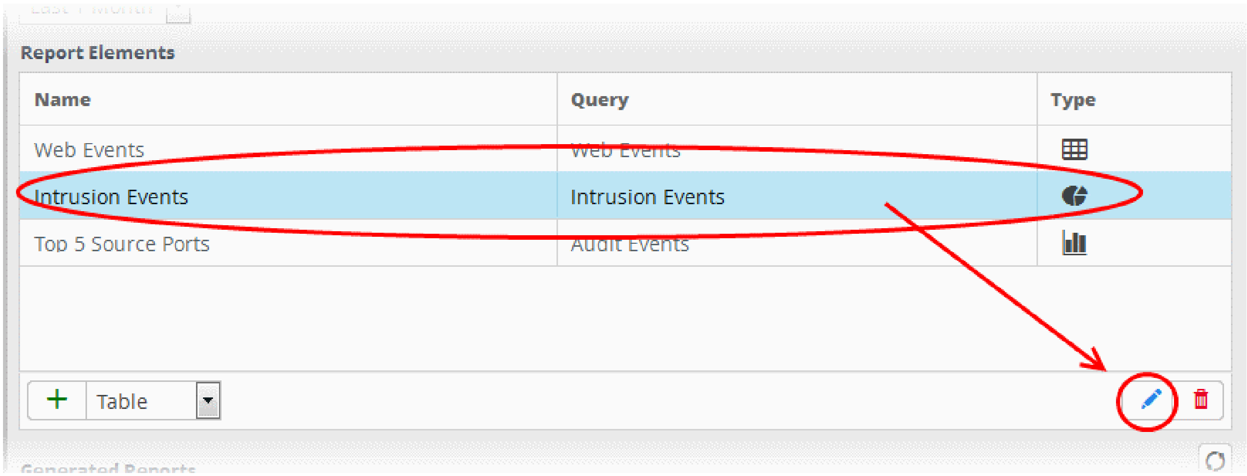
□ Show Last Generated Report

Generate | Schedule | Save

- Edit the name and description as required and click the 'Save' button at the bottom.

### To edit the details of a report element

- Select the report element from the list that you want to edit and click the edit button at the bottom.



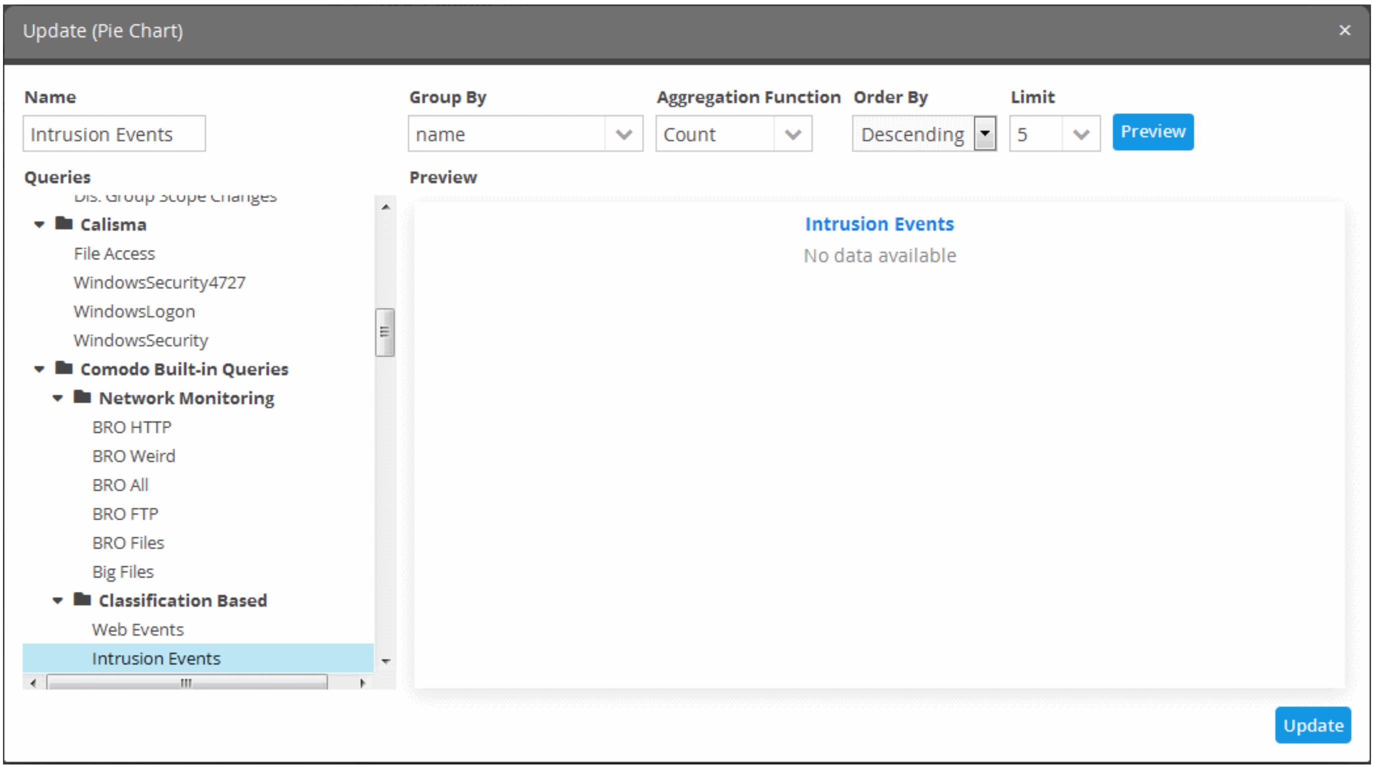
Report Elements

| Name | Query | Type |
|---|---|---|
| Web Events | Web Events | ▦ |
| Intrusion Events | Intrusion Events | ◕ |
| Top 5 Source Ports | Audit Events | 📊 |

+ Table

Generated Reports

The 'Update' screen for the selected report element will be displayed.



Update (Pie Chart)

Name: Intrusion Events

Group By: name

Aggregation Function: Count

Order By: Descending

Limit: 5

Queries

- Dis. Group Scope Changes
- Calisma
  - File Access
  - WindowsSecurity4727
  - WindowsLogon
  - WindowsSecurity
- Comodo Built-in Queries
  - Network Monitoring
    - BRO HTTP
    - BRO Weird
    - BRO All
    - BRO FTP
    - BRO Files
    - Big Files
  - Classification Based
    - Web Events
    - Intrusion Events

Preview

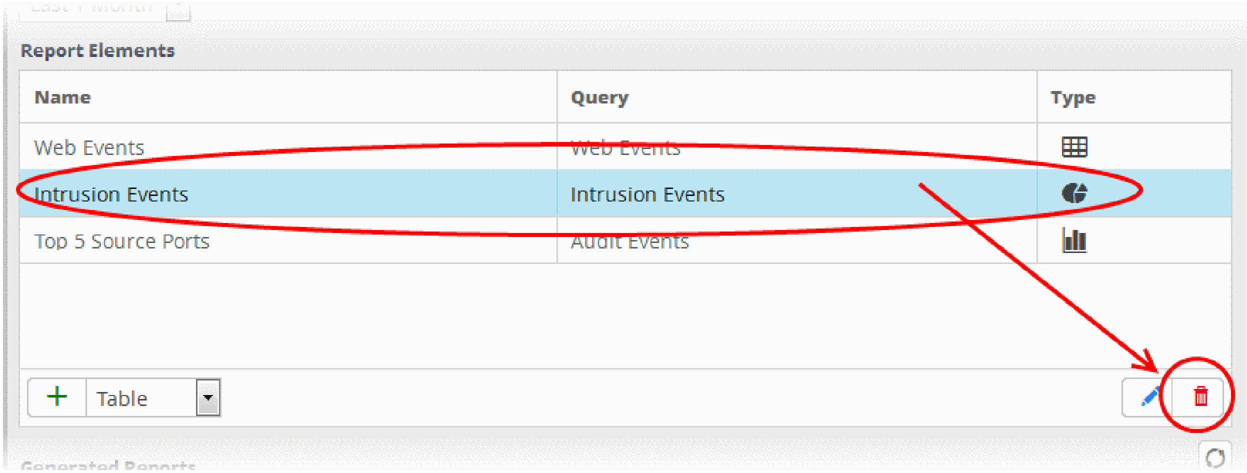
Intrusion Events

No data available

- Edit the details of the report element as required. The procedure is similar to **adding a report element** as explained above.
- Click the 'Update' button.
- Click the 'Save' button at the bottom.

**To delete a report element**

- Select the report the element and click the delete button at the bottom



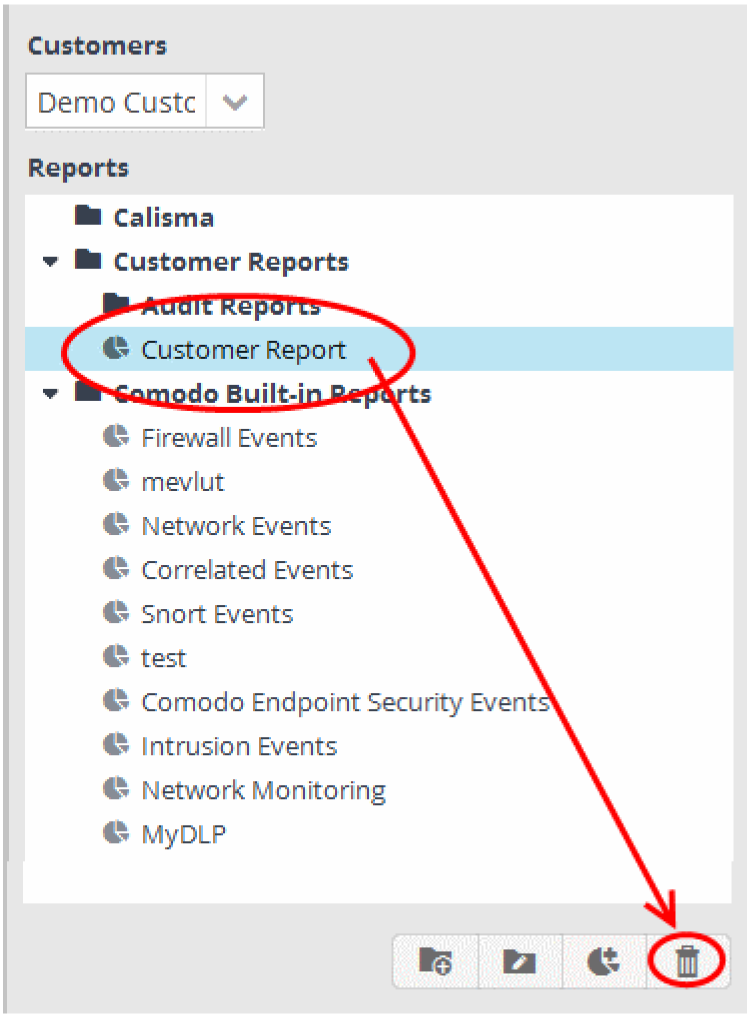
Report Elements

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

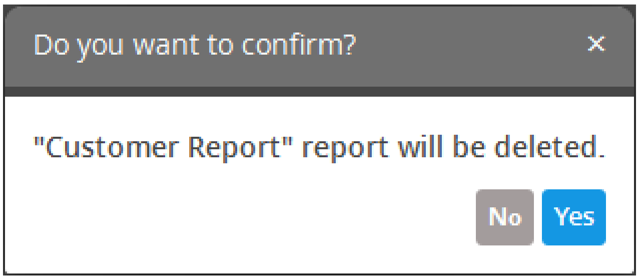
The report element will be deleted.

**To delete a report**

- Select the report on the left side and click the delete button at the bottom.



In the confirmation dialog, click the 'Yes' button to remove the report.

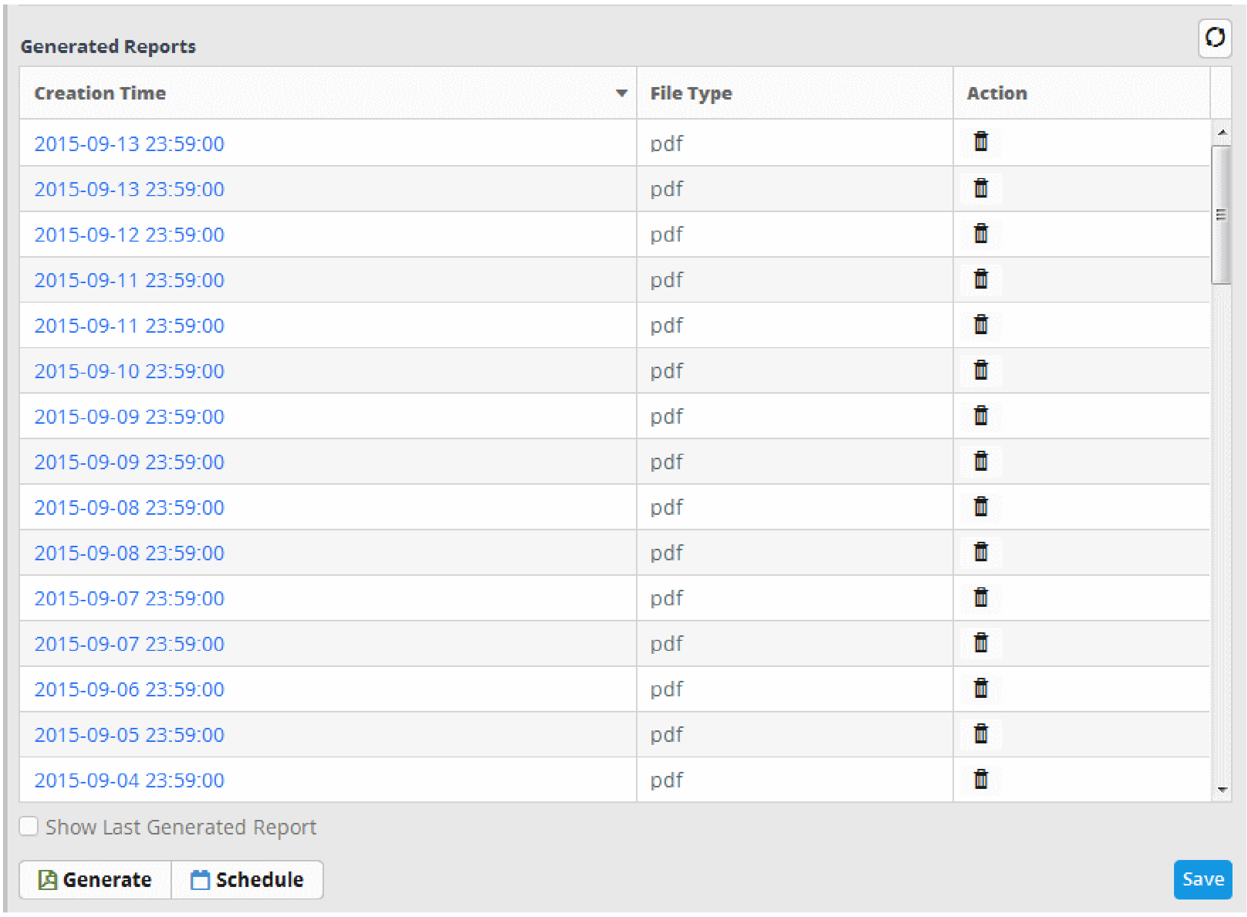

Do you want to confirm?

"Customer Report" report will be deleted.

The report and all the report elements under it will be deleted.

### Manage Generated Reports

The 'Generated Reports' area in the Report Management interface displays a list of manually generated and scheduled report files for the report selected from the left.



Generated Reports

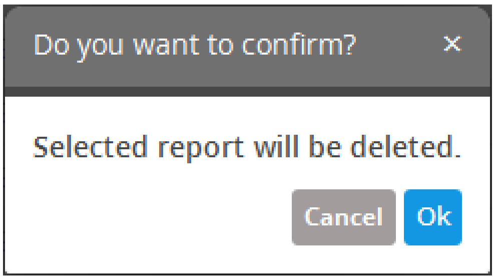
| Creation Time | File Type | Action |
|---|---|---|
| 2015-09-13 23:59:00 | pdf | 🗑 |
| 2015-09-13 23:59:00 | pdf | 🗑 |
| 2015-09-12 23:59:00 | pdf | 🗑 |
| 2015-09-11 23:59:00 | pdf | 🗑 |
| 2015-09-11 23:59:00 | pdf | 🗑 |
| 2015-09-10 23:59:00 | pdf | 🗑 |
| 2015-09-09 23:59:00 | pdf | 🗑 |
| 2015-09-09 23:59:00 | pdf | 🗑 |
| 2015-09-08 23:59:00 | pdf | 🗑 |
| 2015-09-08 23:59:00 | pdf | 🗑 |
| 2015-09-07 23:59:00 | pdf | 🗑 |
| 2015-09-07 23:59:00 | pdf | 🗑 |
| 2015-09-06 23:59:00 | pdf | 🗑 |
| 2015-09-05 23:59:00 | pdf | 🗑 |
| 2015-09-04 23:59:00 | pdf | 🗑 |

□ Show Last Generated Report

- To sort the generated report list according to the date from latest to earliest and vice versa, click anywhere on the 'Creation Time' column header.
- To refresh the list of generated reports, click the button ⟳ on the right.
- To view the report that was generated last, select the 'Show Last Generated Report' check box

The report will be displayed below the section.

- To close the report, deselect the 'Show Last Generated Report' check box
- To delete a report file, click the thrash can icon 🗑 under the 'Action' column



Do you want to confirm?

Selected report will be deleted.

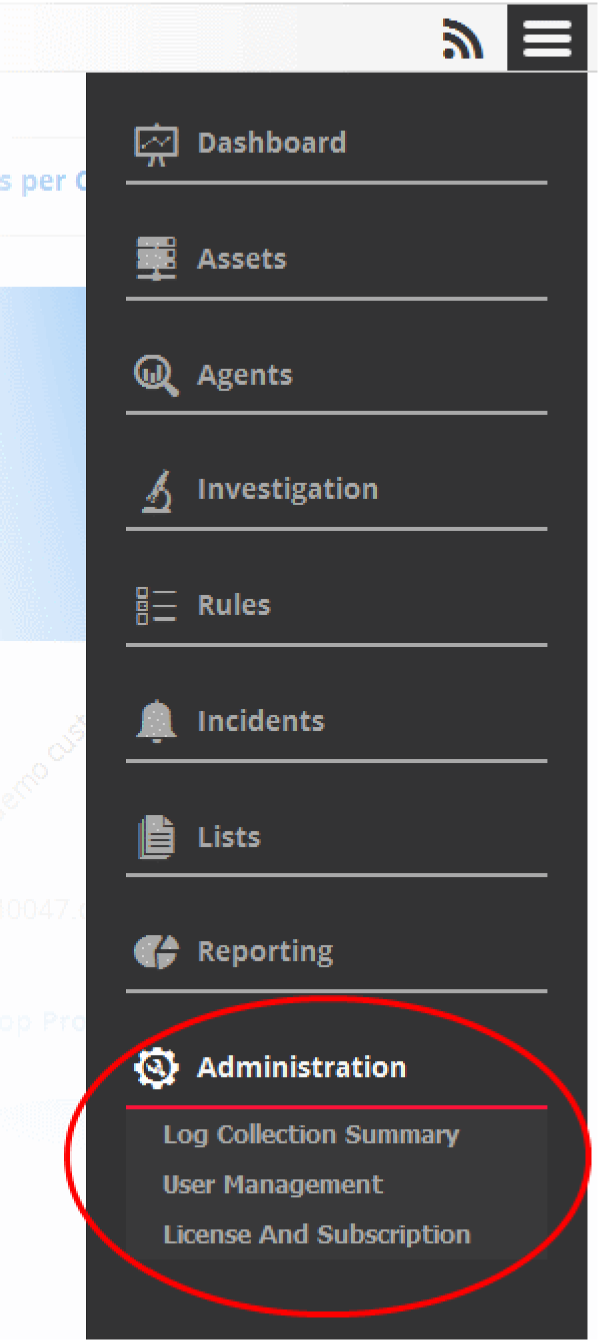
- Click the 'Ok' button to confirm the deletion of the report.

# 11 Administration

The 'Administration' interface allows administrators to view log collection summaries, manage administrative users assigned to particular customer(s) and view license and subscription details and configure the sub-domain name for the NxSIEM URL.

The 'Administration' tab will only be visible to persons with administrative privileges, and not to regular 'users'.

To open the 'Administration' interface, click the menu button at top right and choose 'Administration':



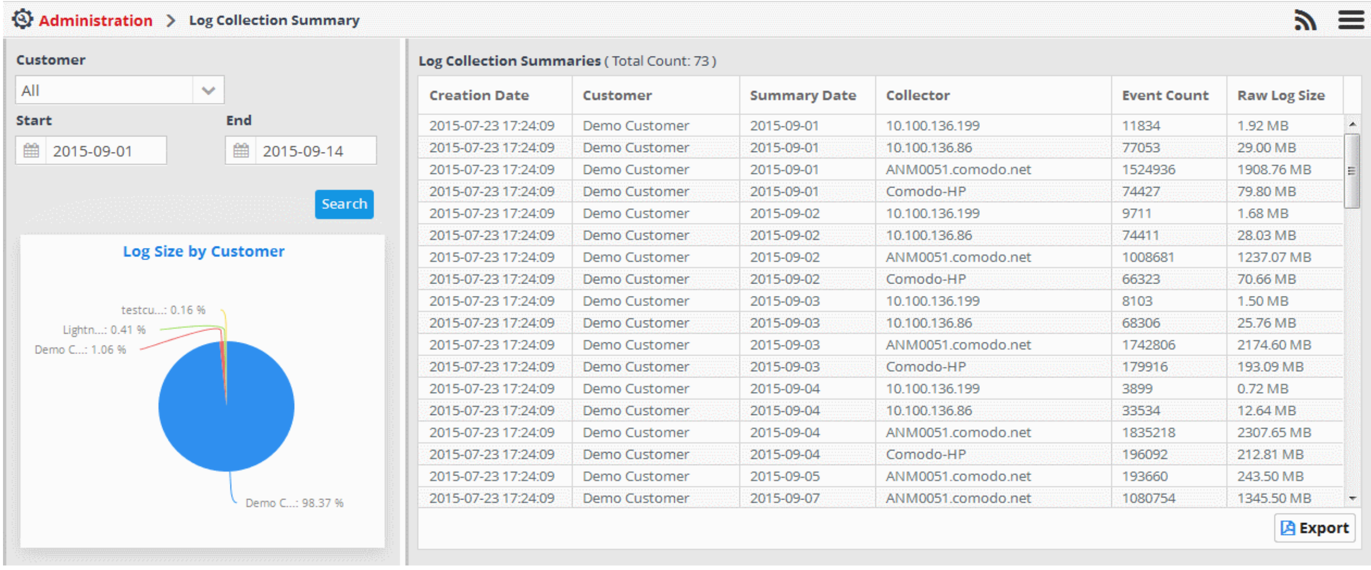
Refer to the following sections for more details:

- Viewing Log Collection Summaries
- Managing Users
- Viewing License and Subscription Details and Configuring NxSIEM platform URL

## 11.1 Viewing Log Collection Summaries

Log collection summaries provide an insight into event logs collected from agents and endpoints on customer networks. Administrators can view a history of log collection and can export the summaries to .pdf for offline analysis.

To open the 'Log Collection Summary' interface, click the 'Navigational Menu' button at top right, choose 'Administration' from the options and then click 'Log Collection Summary'.



Customer: All

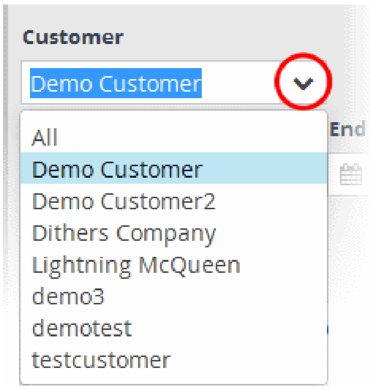
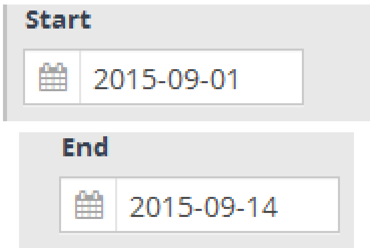
Start: 2015-09-01

End: 2015-09-14

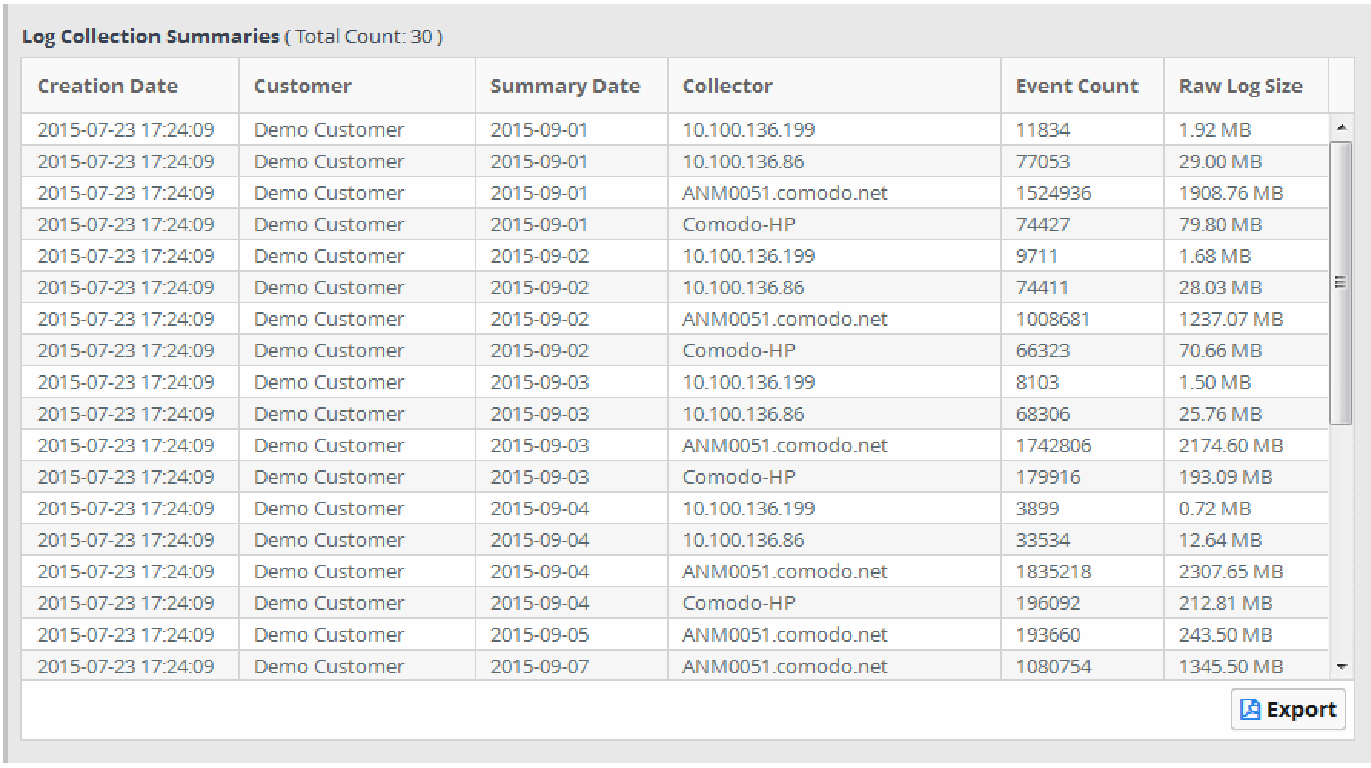
**Log Collection Summaries** ( Total Count: 73 )

| Creation Date | Customer | Summary Date | Collector | Event Count | Raw Log Size |
|---|---|---|---|---|---|
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-01 | 10.100.136.199 | 11834 | 1.92 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-01 | 10.100.136.86 | 77053 | 29.00 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-01 | ANM0051.comodo.net | 1524936 | 1908.76 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-01 | Comodo-HP | 74427 | 79.80 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-02 | 10.100.136.199 | 9711 | 1.68 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-02 | 10.100.136.86 | 74411 | 28.03 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-02 | ANM0051.comodo.net | 1008681 | 1237.07 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-02 | Comodo-HP | 66323 | 70.66 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-03 | 10.100.136.199 | 8103 | 1.50 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-03 | 10.100.136.86 | 68306 | 25.76 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-03 | ANM0051.comodo.net | 1742806 | 2174.60 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-03 | Comodo-HP | 179916 | 193.09 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-04 | 10.100.136.199 | 3899 | 0.72 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-04 | 10.100.136.86 | 33534 | 12.64 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-04 | ANM0051.comodo.net | 1835218 | 2307.65 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-04 | Comodo-HP | 196092 | 212.81 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-05 | ANM0051.comodo.net | 193660 | 243.50 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-07 | ANM0051.comodo.net | 1080754 | 1345.50 MB |

The upper pane in the left side panel allows you to select the customer and the time period for which the log collection summaries are to be viewed. The lower pane in the left panel displays a pie chart that shows the breakup of sizes of log files collected from each agent/endpoint in the selected customer's networks.

| Log Collection Summary Interface - Table of controls | |
|---|---|
|  Customer<br>Demo Customer<br>End<br>All<br>Demo Customer<br>Demo Customer2<br>Dithers Company<br>Lightning McQueen<br>demo3<br>demotest<br>testcustomer | The 'Customers' drop-down allows you to select the customer for which you want to view the log collection summary. |
| <br>Start: 2015-09-01<br>End: 2015-09-14 | The 'Start' and 'End' fields allow you to define the period for which you want to view the log collection summaries for the selected customer. Use the calendar icons in the respective fields to specify the start and end dates. |
| Search | Allows to search the logs collected from the customer within the specified time period. The details of the log collection are displayed in the 'Log Collection Summaries' table at the right. |
| Export | Allows you to save the log collection summary table to a .pdf file and save it for future analysis. |

The 'Log Collection Summaries' pane in the right hand side displays the summary of logs collected at each day from each agent/endpoint of the selected customer's networks, within the specified period.

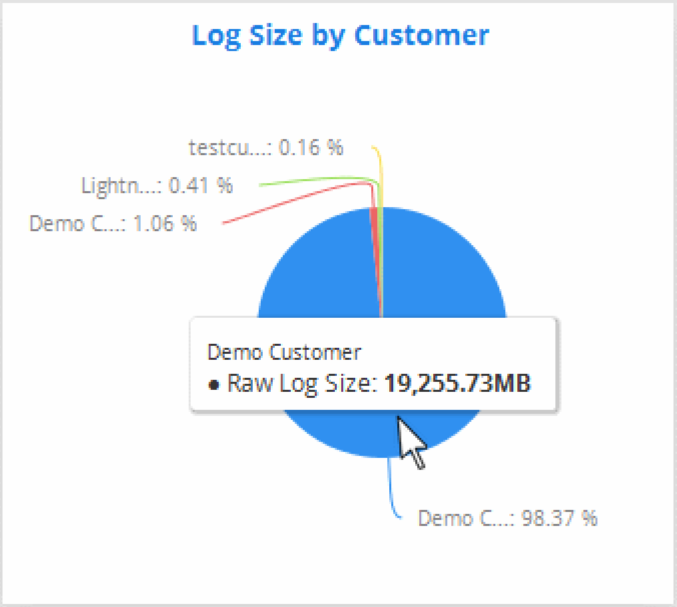


**Log Collection Summaries** ( Total Count: 30 )

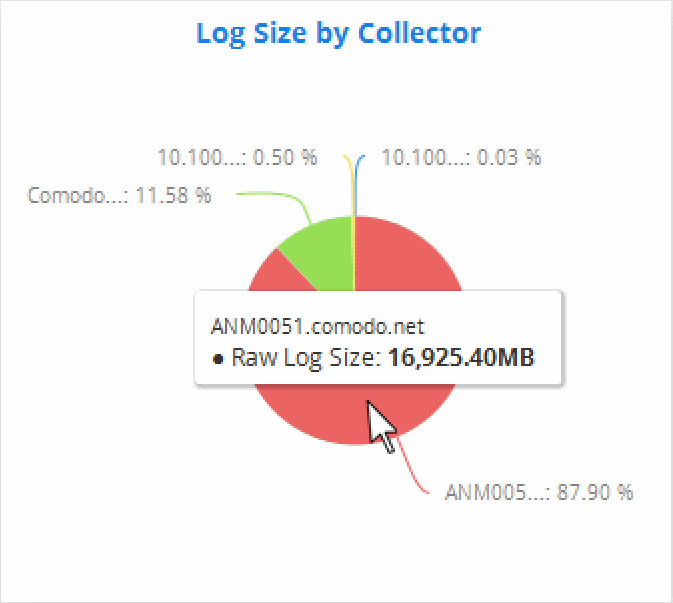
| Creation Date | Customer | Summary Date | Collector | Event Count | Raw Log Size |
|---|---|---|---|---|---|
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-01 | 10.100.136.199 | 11834 | 1.92 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-01 | 10.100.136.86 | 77053 | 29.00 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-01 | ANM0051.comodo.net | 1524936 | 1908.76 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-01 | Comodo-HP | 74427 | 79.80 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-02 | 10.100.136.199 | 9711 | 1.68 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-02 | 10.100.136.86 | 74411 | 28.03 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-02 | ANM0051.comodo.net | 1008681 | 1237.07 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-02 | Comodo-HP | 66323 | 70.66 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-03 | 10.100.136.199 | 8103 | 1.50 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-03 | 10.100.136.86 | 68306 | 25.76 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-03 | ANM0051.comodo.net | 1742806 | 2174.60 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-03 | Comodo-HP | 179916 | 193.09 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-04 | 10.100.136.199 | 3899 | 0.72 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-04 | 10.100.136.86 | 33534 | 12.64 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-04 | ANM0051.comodo.net | 1835218 | 2307.65 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-04 | Comodo-HP | 196092 | 212.81 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-05 | ANM0051.comodo.net | 193660 | 243.50 MB |
| 2015-07-23 17:24:09 | Demo Customer | 2015-09-07 | ANM0051.comodo.net | 1080754 | 1345.50 MB |

| Log Collection Summary Interface - Table of controls | |
|---|---|
| **Column Header** | **Description** |
| Creation Date | Displays the date at which the customer was added to NxSIEM. |
| Customer | Displays the name of the customer. |
| Summary Date | Displays the log collection date for which the summary is displayed in the row. |
| Collector | Displays the agent/endpoint from which the logs are collected |
| Event Count | Displays the number of events for which the logs are collected on that day from that agent/endpoint. |
| Raw Log Size | Displays the total size of log file collected from that agent/endpoint on that day. |

- To view the log collection summary for all customers, choose 'All' from the 'Customer' drop-down, specify the start and end dates for the log collection period and click 'Search'. The details of the logs collected will be displayed at the right panel. The pie chart at the lower left panel will display a breakdown of sizes of log files collected from each customer network. Placing the mouse cursor on the chart displays the total size of log files from the specific customer.



- To view the log collection summary for a specific customer, choose the customer from the 'Customer' drop-down, specify the start and end dates for the log collection period and click 'Search'. The details of the logs collected will be displayed at the right panel. The pie chart at the lower left panel will display a breakdown of sizes of log files collected from each agent/endpoint in the customer networks. Placing the mouse cursor on the chart displays the total size of log files from the specific agent/endpoint.



- To save the displayed Log Summaries table as a .pdf file, click the 'Export' button.

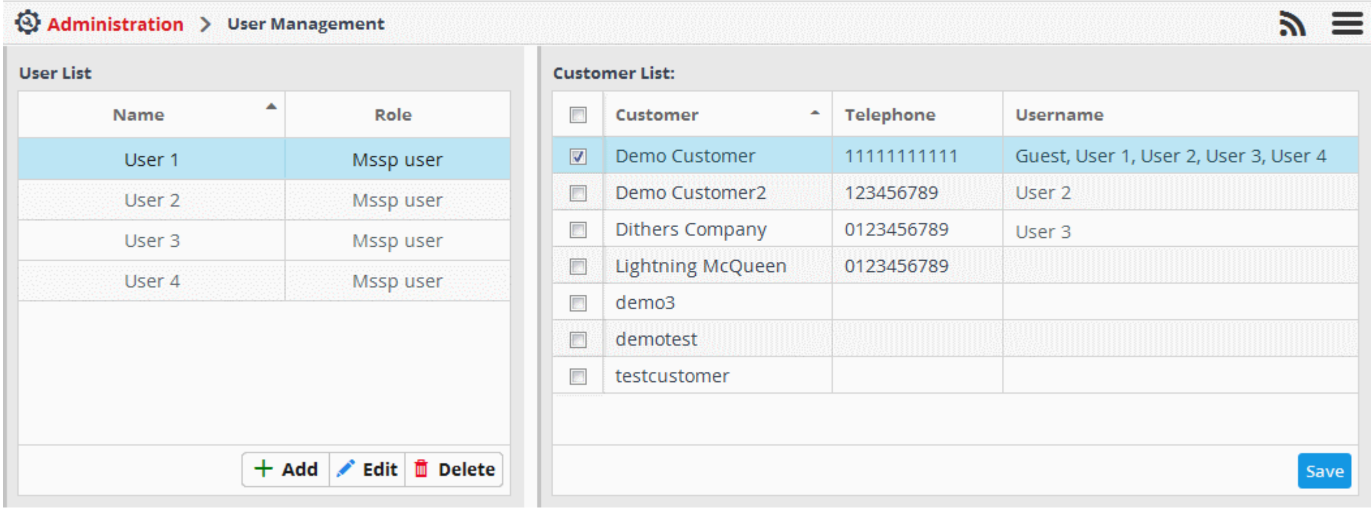
The .pdf file will be displayed in a new browser tab, which enables you to print or save the file.

## 11.2 Managing Users

The administrator can add and manage users that can be assigned to the customers to address the incidents, cases and malicious events arising from their respective customer's networks. These technician users can access and view and manage only the dashboards, events and incidents pertaining to the customers assigned to them. The 'Correlated Incidents' and 'Cases' that are detected for customers will be automatically assigned to users enrolled for the respective customers on a random basis. Refer to the section '**Managing Incidents**' for more details.

The User Management interface allows the administrator to add users, assign them to customers and manage them.

To open the 'User Management' interface, click the 'Navigational Menu' button from the top right, choose 'Administration' from the options and then click 'User Management'.



User List

| Name | Role |
|---|---|
| User 1 | Mssp user |
| User 2 | Mssp user |
| User 3 | Mssp user |
| User 4 | Mssp user |

Customer List:

| □ | Customer | Telephone | Username |
|---|---|---|---|
| ☑ | Demo Customer | 11111111111 | Guest, User 1, User 2, User 3, User 4 |
| □ | Demo Customer2 | 123456789 | User 2 |
| □ | Dithers Company | 0123456789 | User 3 |
| □ | Lightning McQueen | 0123456789 | |
| □ | demo3 | | |
| □ | demotest | | |
| □ | testcustomer | | |

The 'User List' pane at the left displays a list of existing users and their roles. The 'Customer List' panel at the right displays the list of enrolled customers and the users assigned to them respectively. Refer to the section '**Adding Customers**' to know about adding customers to the NxSIEM.

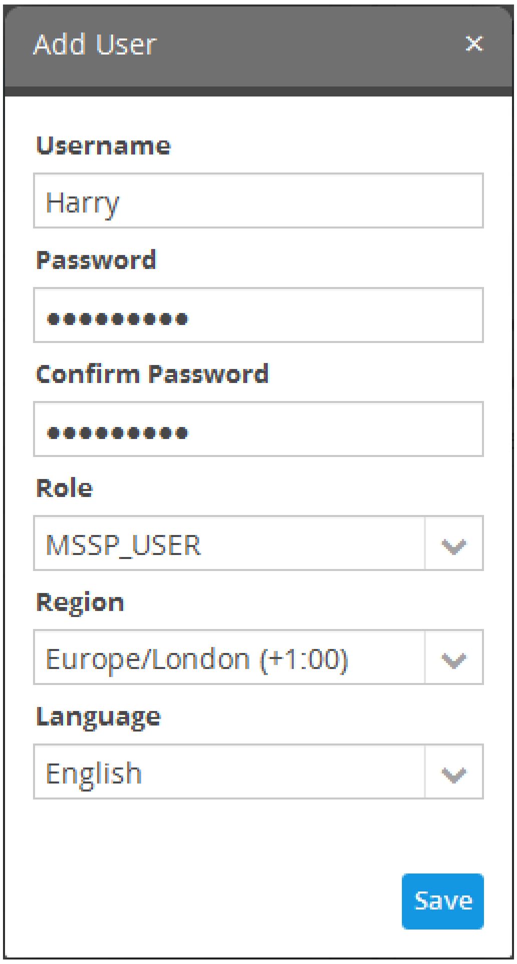
Following sections explain on:

- **Adding users**
- **Assigning a user to customer(s)**
- **Edit user details**
- **Remove a user**
- **Reassign/remove customer access for a user**

**To add a user**

- Click the 'Add' button + Add at the bottom of the User List pane at the left.

The 'Add User' dialog will appear.



Username

Harry

Password

●●●●●●●●●

Confirm Password

●●●●●●●●●

Role

MSSP_USER

Region

Europe/London (+1:00)

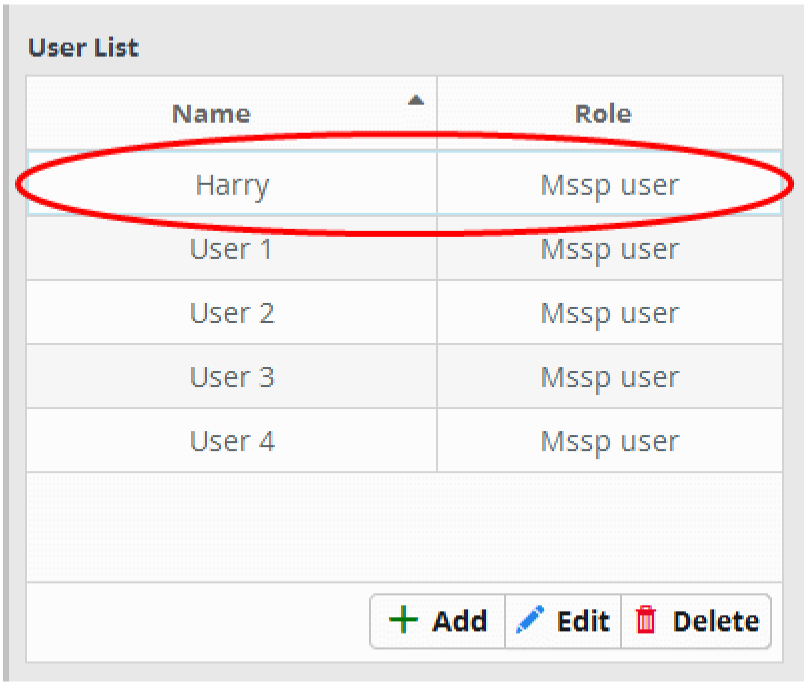
Language

English

- **Username** - Enter the username for the user.
- **Password** - Enter the password for the user to login to NxSIEM. The password should be of at least 8 characters in length, should contain at least one uppercase, one lowercase and one numeral.
- **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, from the drop-down.
- **Language** - Choose the language in which the NxSIEM web console is to be displayed to the user from the drop-down.

- Click the 'Save' button.

The user will be added and displayed under 'User List'.

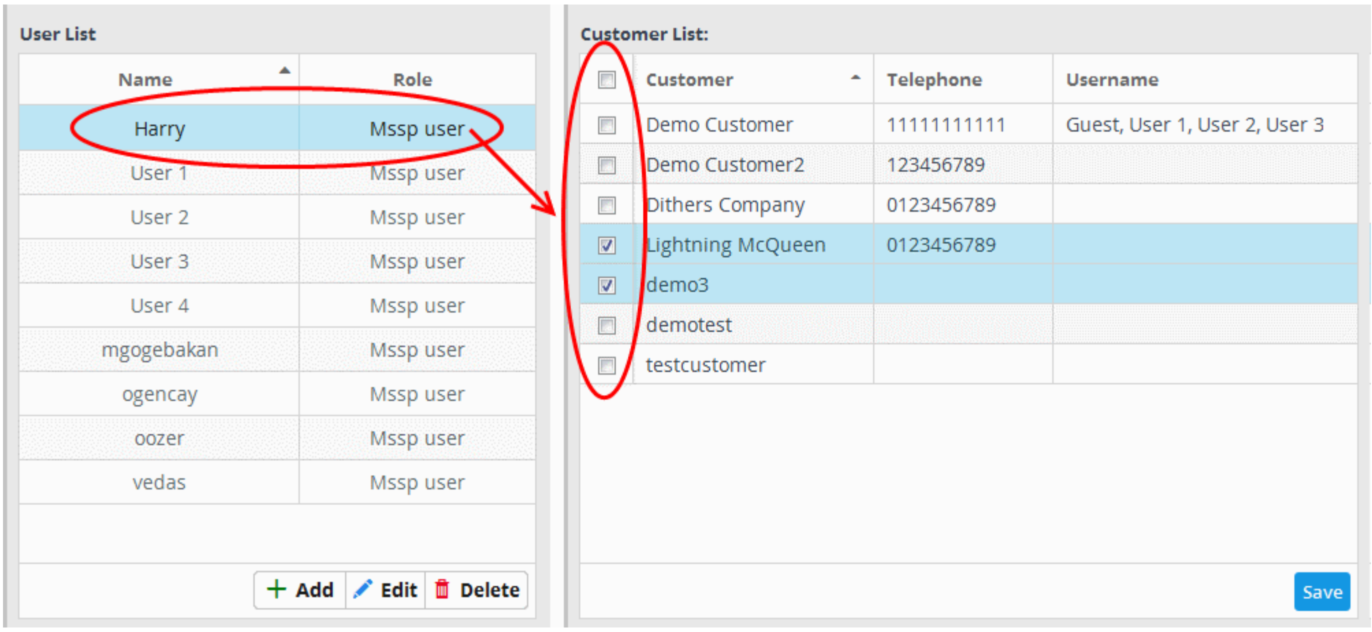


User List

| Name | Role |
|---|---|
| Harry | Mssp user |
| User 1 | Mssp user |
| User 2 | Mssp user |
| User 3 | Mssp user |
| User 4 | Mssp user |

**To assign a user to customer(s)**

- Choose the user to be assigned to customer(s) from the 'User List' at the left.
- Select the customer(s) to whom the user is to be assigned from the Customer List at the right side



User List

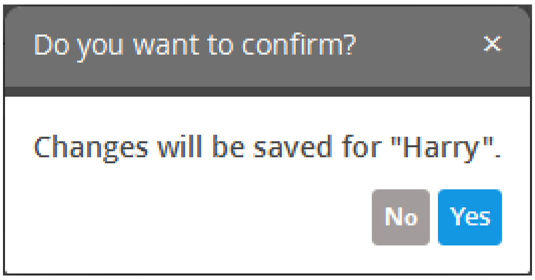
| Name | Role |
|---|---|
| Harry | Mssp user |
| User 1 | Mssp user |
| User 2 | Mssp user |
| User 3 | Mssp user |
| User 4 | Mssp user |
| mgogebakan | Mssp user |
| ogencay | Mssp user |
| oozer | Mssp user |
| vedas | Mssp user |

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.

A confirmation dialog will appear.



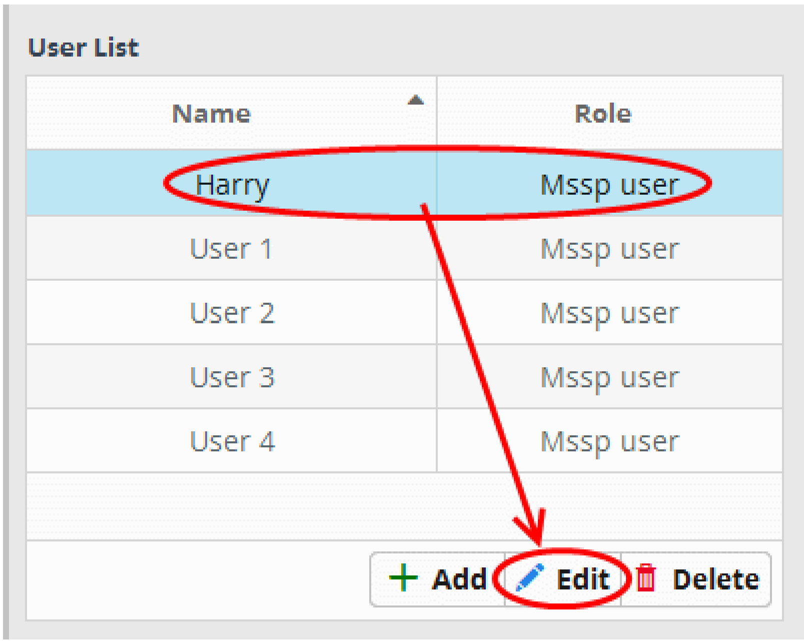
Do you want to confirm?

Changes will be saved for "Harry".

- Click 'Yes' to confirm the assignment.

**To edit the details of a user**

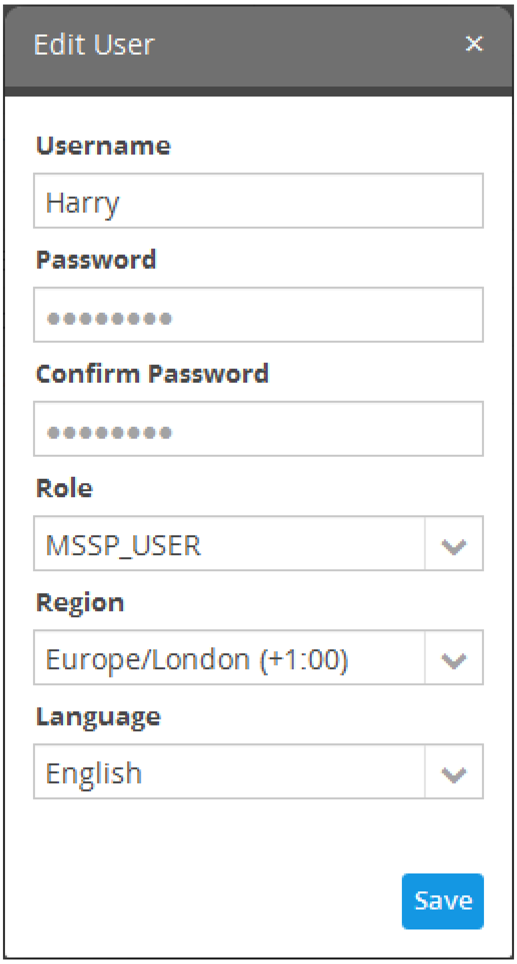
- Choose the user whose details are to be changed and click the 'Edit' button from the bottom of the User List pane at the right.



User List

| Name | Role |
|---|---|
| Harry | Mssp user |
| User 1 | Mssp user |
| User 2 | Mssp user |
| User 3 | Mssp user |
| User 4 | Mssp user |

The 'Edit User' screen will be displayed.



Edit User

Username: Harry

Password: ••••••••

Confirm Password: ••••••••

Role: MSSP_USER

Region: Europe/London (+1:00)

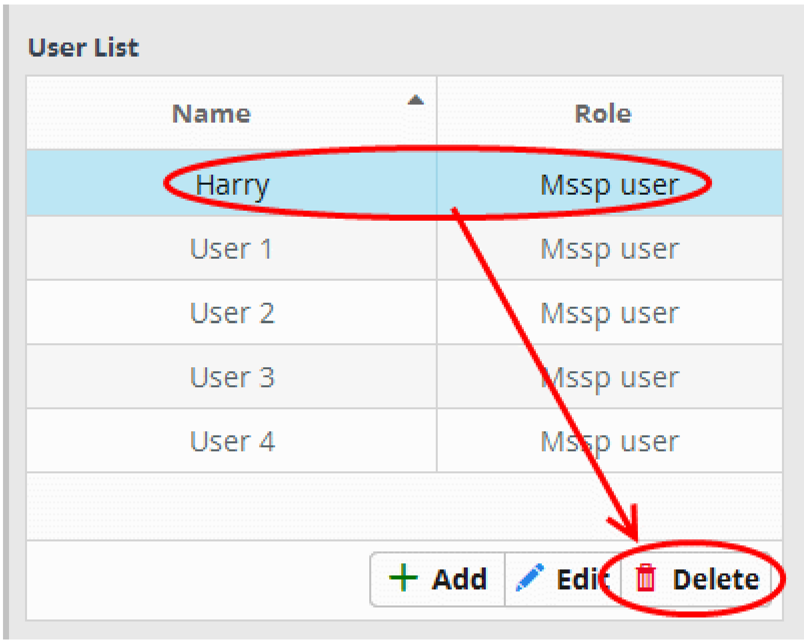
Language: English

The 'Edit User' dialog is similar to 'Add User' dialog. Refer to the section explaining **adding a new user** above for the descriptions of the fields available in this dialog.

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

**To remove a user**

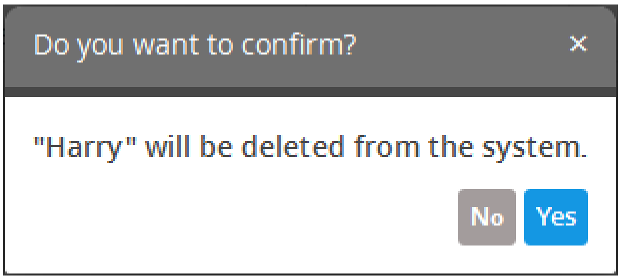
- Choose the user to be removed and click the 'Delete' button from the bottom of the 'User List' pane at the right.



User List

| Name | Role |
|---|---|
| Harry | Mssp user |
| User 1 | Mssp user |
| User 2 | Mssp user |
| User 3 | Mssp user |
| User 4 | Mssp user |

A confirmation dialog will appear.



Do you want to confirm?

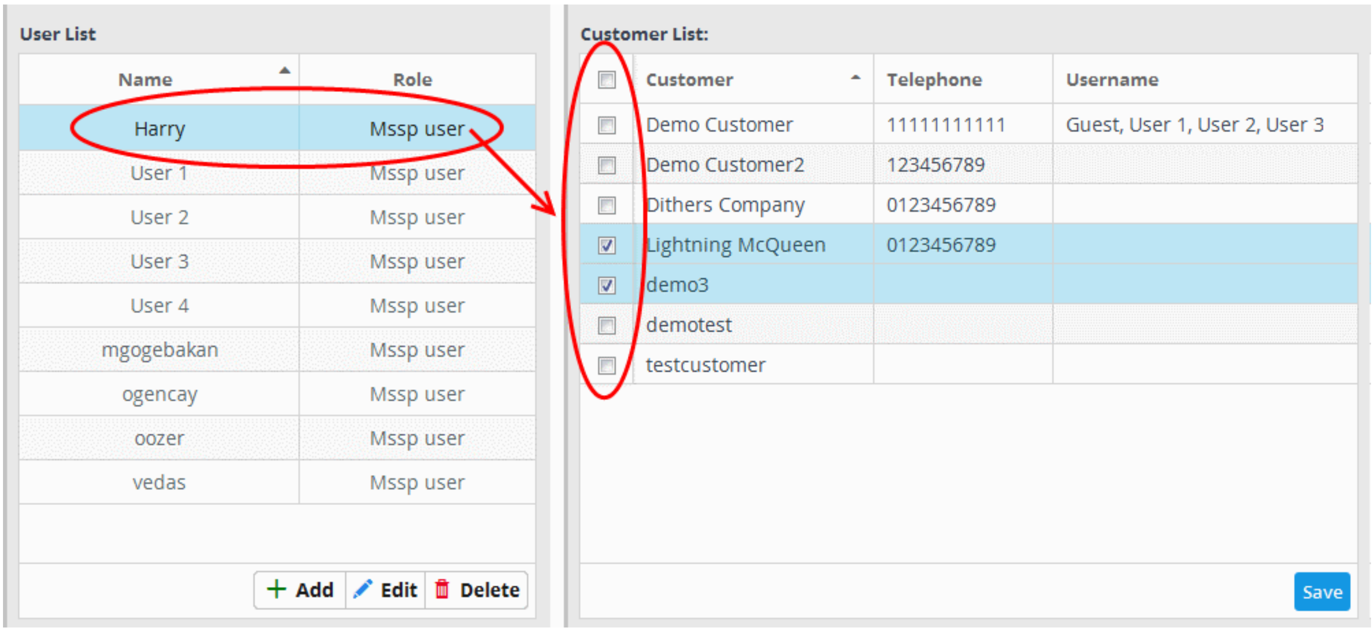
"Harry" will be deleted from the system.

- Click 'Yes' to confirm the removal.

**To reassign user to customer(s)**

- Choose the user to be reassigned to a new customer(s) or removed from a customer, from the 'User List' at the left.

The customers to whom the user is currently assigned will be indicated with their checkboxes selected, in the 'Customer List' at the right.



User List

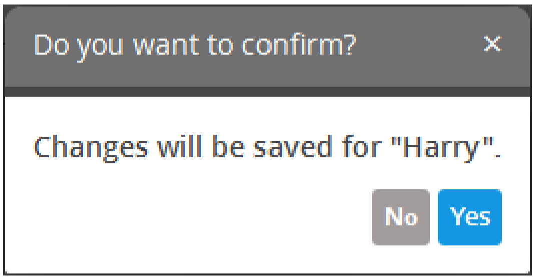
| Name | Role |
|---|---|
| Harry | Mssp user |
| User 1 | Mssp user |
| User 2 | Mssp user |
| User 3 | Mssp user |
| User 4 | Mssp user |
| mgogebakan | Mssp user |
| ogencay | Mssp user |
| oozer | Mssp user |
| vedas | Mssp user |

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 | | |

- To assign the user to new customer(s), select the new customer(s) from the 'Customer List' at the right side
- To remove access to a customer from the user, deselect the customer.

A confirmation dialog will appear.



Do you want to confirm?

Changes will be saved for "Harry".

- Click 'Yes' to confirm the re-assignment.

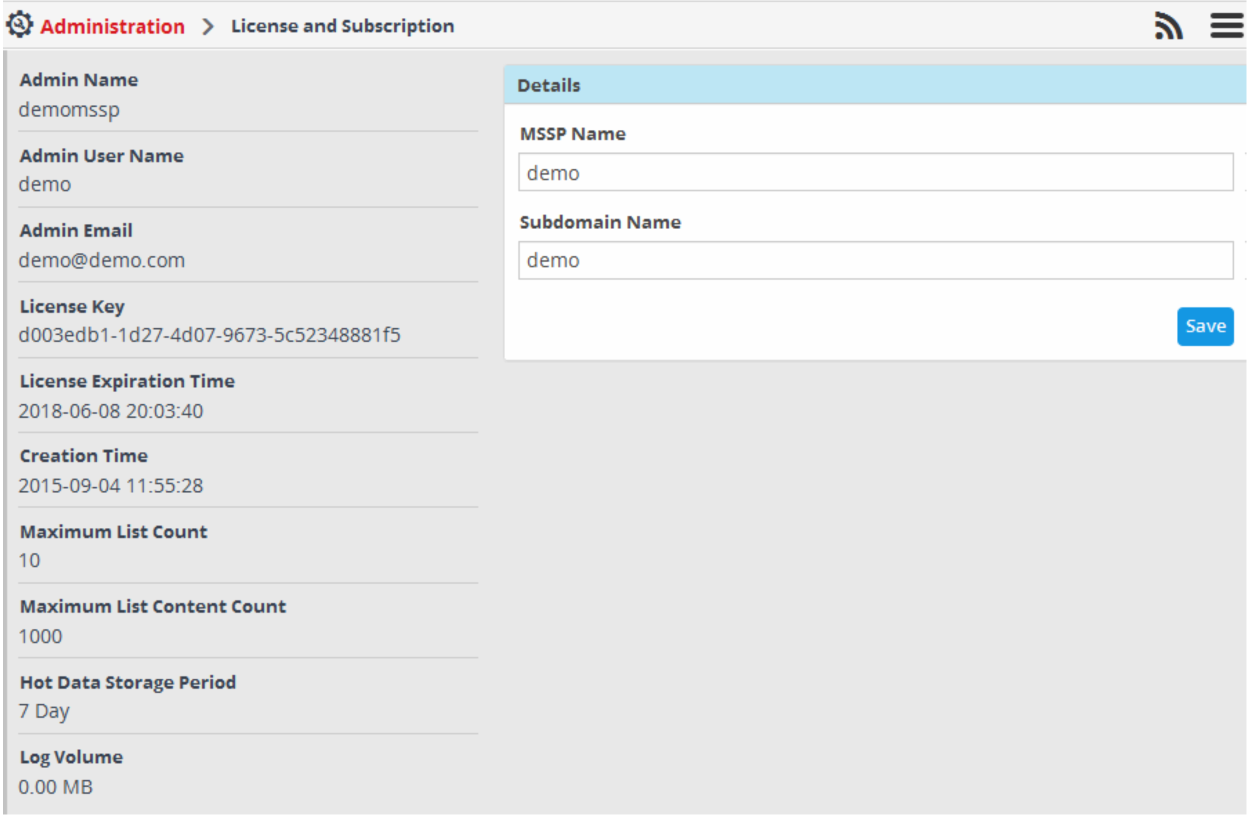
## 11.3 Viewing License and Subscription Details and Configuring NxSIEM Platform URL

The License and Subscription interface displays the license details like license key, validity and so on and the limits set for Live Lists, log data storage period and so on. If the administrator wants to extend these limits, they can contact Comodo and request for them.

The interface also allows the administrator to change their MSSP service provider name and set the sub-domain name.

- You can set your desired service provider name for example, your company name as MSSP Name, so that the reports generated by NxSIEM will have your company name in their titles.
- You can set your desired sub-domain name, so that the access URL for your MSSP service will be set to https://<your subdomain name>.mssp.comodo.com/ui/start. All your administrators and users can login to your NxSIEM administrative console using this URL.

To open the 'License and Subscription' interface, click the 'Menu' button from the top right, choose 'Administration' and then click 'License and Subscription'.



Admin Name
demomssp

Admin User Name
demo

Admin Email
demo@demo.com

License Key
d003edb1-1d27-4d07-9673-5c52348881f5

License Expiration Time
2018-06-08 20:03:40

Creation Time
2015-09-04 11:55:28

Maximum List Count
10

Maximum List Content Count
1000

Hot Data Storage Period
7 Day

Log Volume
0.00 MB

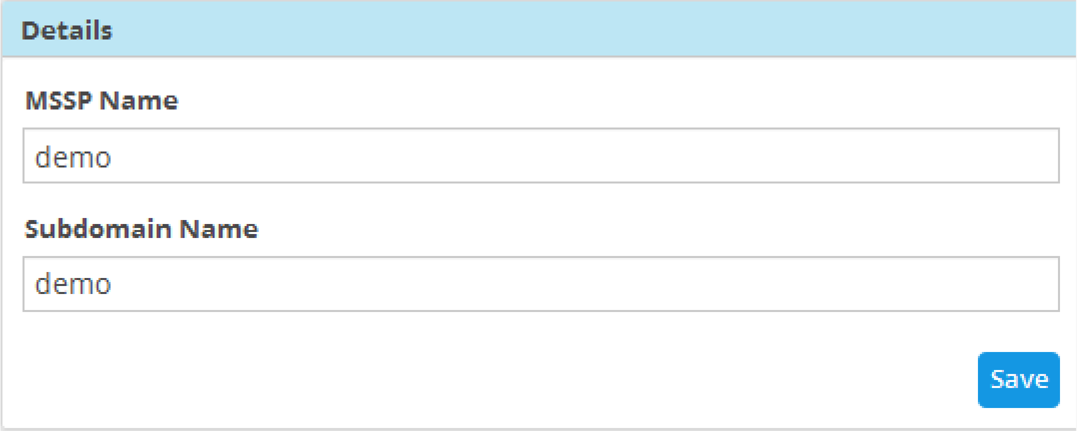
Details

MSSP Name: demo

Subdomain Name: demo

The subscription details, license information and the limits set for the Live List count, data retention period and maximum log storage space covered by the license are displayed at the left. If you want to increase the limits, you can contact Comodo and place a request.

The 'Details' pane at the top right allows you to change your MSSP name and sub-domain name.



Details

MSSP Name: demo

Subdomain Name: demo

- To change the MSSP service provider name, directly edit the name in the 'MSSP Name' field.
- To change the sub-domain name in the NxSIEM platform URL, directly enter the new sub-domain in the 'Subdomain Name' field.
- Click Save for your changes to take effect.

From the next login the administrators and the users should use the URL with the new sub-domain name to access the NxSIEM administrative console. The URL is of the form 'https://<new subdomain name>.mssp.comodo.com/ui/start.

# Appendix 1 - Field Groups and Event Items Description

| S.No | Field Groups | Description | Event Items | Description |
|---|---|---|---|---|
| 1 | agent | Log collector | agent_id | ID of collector |
| | | | agent_ip | IP address of collector |
| 2 | application | Application information contained in events | app_name | Application Name |
| | | | app_pid | Application Process ID |
| 3 | classification | Event classification fields | class_action | Type of action attempted as part of the event |
| | | | class_domain | Environment or domain of the event |
| | | | class_object | Type of object that is targeted or affected by the event |
| | | | class_service | Service involved in event |
| | | | class_status | Status of the event action identified by the action field |
| | | | class_subject | Type of object that started the event action identified by the action field |
| 4 | custom | Custom field labels and their values | co_1 | Custom Value 1 |
| | | | co_1label | Custom Label 1 |
| | | | co_2 | Custom Value 2 |
| | | | co_2label | Custom Label 2 |
| | | | co_3 | Custom Value 3 |
| | | | co_3label | Custom Label 3 |
| | | | co_4 | Custom Value 4 |
| | | | co_4label | Custom Label 4 |
| | | | co_5 | Custom Value 5 |
| | | | co_5label | Custom Label 5 |
| 5 | destination | Event target device | dst_host | Host name of target device |
| | | | dst_ip | IP Address of target device |
| | | | dst_mac | MAC Address of target device |
| | | | dst_port | Port that is targeted |
| | | | dst_tr_ip | Translated IP Address of target device |
| | | | dst_tr_port | Translated Port |

| | | | | |
|---|---|---|---|---|
| 6 | device | Device where logs are produced on | dvc_host | Host name of device |
| | | | dvc_ip | IP Address of device |
| 7 | event | General event fields | agent_time | The time (in miliseconds) that raw log is processed on collector |
| | | | central_time | The time (in miliseconds) that rae log is transformed to an event |
| | | | dvc_time | The time (in miliseconds) that log is seen on device |
| | | | event_id | Unique id of the event |
| | | | message | Message of the event |
| | | | name | Name of the event |
| | | | raw_log | The log text seen on device |
| | | | tags | Event tags seperated with pipe character (\|) |
| | | | type | Type of the event |
| | | | customer_id | identifier for the customer of mssp |
| | | | mssp_id | identifier for mssp |
| | | | raw_size | Received log size in bytes encoded in UTF-8 |
| | | | size | Normalized event size in bytes encoded in UTF-8 |
| 8 | file | File information contained in events | f_name | File name |
| | | | f_size | File size |
| | | | f_type | File type |
| | | | f_uri_path | File uri path |
| | | | f_url | File url |
| | | | f_md5 | MD5 hash value of the file |
| | | | f_sha1 | SHA1 hash value of the file |
| | | | f_sha256 | SHA256 hash value of the file |
| 9 | network | Network-related information contained in events | app_proto | Application protocol used in event |
| | | | bytes_in | Bytes received |
| | | | bytes_out | Bytes sent |
| | | | int_in | Interface in |
| | | | int_out | Out interface |
| | | | session_id | Session id |
| | | | trans_proto | Transport protocol used in event |
| 10 | product | Product that produces raw logs | prod_name | Name of the product |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | that will be converted to events |  |  |
|  |  |  | prod_vendor | Vendor of the product |
|  |  |  | prod_version | Version of the product |
| 11 | rule | Rule (firewall, ips, antivirus rule etc.) information contained in events | rule_hit_count | Represents how many hits occurred for the rule |
|  |  |  | rule_id | ID of the rule |
|  |  |  | rule_info | Extra information related to the rule |
|  |  |  | rule_name | Name of the rule |
|  |  |  | rule_sig_id | ID of the signature related to rule |
|  |  |  | rule_sig_name | Name of the signature related to rule |
| 12 | source | Event source device | src_host | Host name of source device |
|  |  |  | src_ip | IP Address of source device |
|  |  |  | src_mac | MAC Address of source device |
|  |  |  | src_port | Event source port |
|  |  |  | src_tr_ip | Translated IP Address of source device |
|  |  |  | src_tr_port | Source Port |
| 13 | syslog | Syslog information | facility | Syslog facility field |
|  |  |  | priority | Syslog priority field |
|  |  |  | severity | Syslog severity field |
| 14 | time | Time-related information<br>(calculated based on agent_time) | pass_days | Represents how many days have passed since January 1, 1970 UTC |
|  |  |  | pass_hours | Represents how many hours have passed since January 1, 1970 UTC |
|  |  |  | pass_minutes | Represents how many minutes have passed since January 1, 1970 UTC |
|  |  |  | pass_months | Represents how many months have passed since January 1, 1970 UTC |
|  |  |  | pass_years | Represents how many years have passed since January 1, 1970 UTC |
| 15 | user | User information contained in events | usr_domain | Domain of the user |
|  |  |  | usr_name | Name of the user |
|  |  |  | usr_uid | UID of the user |
|  |  |  | target_domain | Tageted User's Domain |
|  |  |  | target_name | Tageted User's Name |
|  |  |  | target_uid | Tageted User's Unique Id |

# Appendix 2 - Configuring Endpoints to Forward Logs to NxSIEM server

You can configure endpoints in customer networks to forward logs to NxSIEM in several ways. There are two broad methods of log collection:

- **Using The Log Collection Agent**
- **Agentless Log Collection**

## Using NxSIEM Agent

### Agent Installation and Configuration

You can download the log collection agent from the NxSIEM interface, install on each endpoint and activate it using the unique key generated for the customer network/zone. Refer to the section **Downloading and Installing the NxSIEM Agent on Endpoints** for detailed explanation.

### Remote Log Collection

An agent installed on one endpoint in a network can be configured via a 'Remote Log Collection Policy' to acquire logs from another endpoint in which log collection is not installed. For more details on Log Collection Policies and their deployment to selected agents, refer to the section **Log Collection Policies**. For a tutorial on configuring a Remote Log Collection Policy, refer to the section **Remote Log Collection Policy**.

## Agentless Log Collection

Agentless log collection involves configuring RSYSLOG and NXLOG utilities installed on Linux and Windows endpoints respectively. Configuration scripts for both RSYSLOG and NXLOG can be downloaded from the NxSIEM interface then run on endpoints to automatically forward logs to the NxSIEM server.

### Using Ready Made Script Files

NxSIEM generates ready-made configuration script files with all parameters pre-configured for each enrolled customer/network. You can download the configuration script/file from the administrative console and deploy onto endpoints. This is the most convenient way of configuring NXLOG (Windows endpoints) and RSYSLOG (Linux endpoints) to send logs to the NXSIEM server. Refer to the section **Configuring Nxlog and Rsyslog to Send Logs to NxSIEM Server** for more detailed explanations on downloading the script files and deploying them.

### Using manually Configurable Script File

NxSIEM allows you to download a configuration script for RSYSLOG which lets you manually set parameters such as network authentication token, name of product from which the logs are to be collected and so on. This script can be used to configure RSYSLOG utilities at Linux based endpoints to send logs to the NXSIEM server. For more details on downloading and configuring the script, refer to the section **Agentless Log Collection**.

# 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.**