SURELOG

User Guide

ANET USA INC.

Table of Contents

Preface

This guide explains how to use the SureLog platform software.

Intended Audience

The reader should have experience in system administration along with networking and information security. In addition, they should be comfortable in installing software on distributed enterprise servers and understand TCP/IP networking and remote logging. Familiarity with network protocols and standards is also highly recommended.

Technical Support

Customers requiring technical assistance can reach our support representatives through telephone or email:

E-mail Address:

Please send a detailed email to support@anetusa.net

Chapter 1: Introduction to SureLog

As Information Technology (IT) becomes the center of today‘s wired enterprise, organizations are under increasing pressure to implement best practices to better control growing security, risk, and compliance challenges. These challenges include internal and external threats, operational issues, intellectual property protection, privacy, and even regulatory mandates. Even though there has been a great emergence of network security centers and risk management groups to help remedy this situation, they have discovered that no one tool completely integrates security, risk, and compliance. As a result, numerous organizations are forced to bundle tools from multiple vendors to achieve their security and compliance goals. However, these techniques result in disparate silos of data that are costly and complex to manage. SureLog software attempts to resolve this issue for its customers.

For custom or non-supported data types, SureLog includes a universal parser to map anydata feed into a data store. Once the data is collected, full record fidelity is maintained to ensure the forensic and evidentiary capabilities of the data. From there, the data is encrypted -a best practice required by numerous regulations including PCI. Finally, the stored data is compressed at a rate of 15:1 to control storage costs. SureLog's correlation engine is unmatched in the industry because it correlates not just log data, but all other data types that are collected and parsed. SureLog also provides over 1,000 security and compliance metrics-based reports, letting users quickly gain visibility into infrastructure activities across lines of business, locations, and applications. These reports are viewable from a secure onscreen portal or they can exported into HTML, PDF, and various other formats.

Comprehensive Log Data Collection and Log Management

It is imperative that a true log management and analysis solution have the ability to collect log data across an enterprise regardless of its source. The solution must also be able to present the logs in a uniform and consistent manner, while managing the state and location for efficient access to the data. The SureLog solution was designed to address these needs along with the following:

- The ability to collect any type of log data regardless of source
- The ability to collect log data with or without installing an agent on the log source device, system or application
- The ability to "normalize" any type of log data for more effective reporting and analysis
- The ability to "scale-down" for small deployments and "scale-up" for extremely large environments
- An open architecture allowing direct and secure access to log data via third-party analysis and reporting tools
- A role-based security model providing user accountability and access control
- Automated archiving for secure long-term retention
- Wizard-based retrieval of any archived logs within seconds

Cross-Platform Log Collection

Today's IT operations require many technologies such as routers, firewalls, switches, file servers and applications. SureLog is designed to collect information from these tools through intelligent use of agent-less and agent-based techniques.

Windows Event Logs: Agent-less or Agent-based

Many Windows-based applications write their logs to an Application Event Log or a custom Event Log. SureLog has the ability to collect all types of Windows Event Logs with or without the use of an agent.

Introduction to Syslog Protocol

The management of Syslog messages is a valuable, but often overlooked aspect of network and business management. Within any enterprise, routers, servers, workstations, and other business applications are constantly collecting important error and status information. This data –extremely pertinent to business operations- resides in error logs, transaction logs, and event logs on each computer. SureLog uses its main messaging protocol, the Syslog Protocol, to aid with these data collecting activities.

Syslog is a simple, yet highly interoperable and well-established component of SureLog. As one of the oldest management protocols available, Syslog has proven to be a mainstay of network management and one of the best in existence. It has been operated in networks of various complexity levels and is a capability that is already built into many of the users' critical systems.

SNMP Trap Reception and Processing

Although the main messaging format of SureLog is in the "Syslog" format, SureLog can process SNMP traps as well. In fact, some sites will setup its servers to receive SNMP traps only and not necessarily use the system to process Syslog messages. SureLog does not require any SNMP MIBs to be compiled or installed. The trap receiver uses a heuristic algorithm to find textual conventions within a trap message and compose a readable and pertinent Syslog message. The native Syslog protocol encourages the creation of semantically correct messages, which is a feature that is often lacking in other SNMP trap receivers. SureLog has a unique capability to convert cryptic SNMP traps into a readable text and transparent relay of a message to the Syslog receiver. This furnishes a high degree of simplicity and sophistication when conducting such activities.

SureLog Server Features

High-Speed Message Reception: The SureLog Server is able to operate as the single Syslog and SNMP Trap receiver for all devices on a large enterprise network. SureLog can process more than 5,000 messages per second and can handle burst traffic of more than 25,000 messages. SureLog physically tracks and catalogs network devices without a maximum limit, while receiving messages from virtually an unlimited numbers of sources without tracking.

Automatic Aggregating, Correlation, and Reporting of Information: The SureLog Server provides a powerful correlation service. The features require minimal configuration and serve as building blocks for larger correlation strategies.

Large Scale Data Aggregation, Archiving, and Reporting Ability: The SureLog Server is designed to have high-data aggregation ability. It can collect in excess of 1 gigabyte worth of data each day, while saving this data for up to 500 days online and for more than 5,000 days offline in a compressed format. The archiving function includes MD5checksums and security codes on data items to support detailed forensics. Reports are also generated daily in Microsoft Excel format.

Large-Scale Data Searching Ability: One of the most important functions of the SureLog system is its search engine capability. SureLog employs a high-speed, real-time index system. This allows for quick searches throughout massive amounts of data. Users can search a terabyte of data for a particular keyword in less than one second.

Ergonomic Reception of SNMP Traps: SNMP traps are often faulted by users for being too cryptic and difficult to decipher. The SureLog system employs a heuristic method of formatting trap messages, assigning these messages with Syslog severity levels and facility codes (so that the received SNMP traps make sense in an operational standpoint). The SureLog system receives SNMP traps in various formats and versions and converts these traps into readable text for correlation.

Chapter 2: System Requirements

Supported Operating Systems

You can install SureLog on servers that run any of the following operating systems:

- Microsoft Windows Server from server 2008 to current
- Microsoft Windows Client from version 7 to current

Hardware Requirements

Minimum hardware requirements depend on Events Per Seconds (EPS) values. For a maximum EPS value of 250, a 2.3 GHz 8 Core or equivalent processor with 12 GM RAM and 50 GB hard disk drive space is recommended.

Chapter 3: First Time Users

Installing and Uninstalling SureLog

Download the setup file and begin the installation using Administrator rights on the respective machine. Follow the on-screen instructions as directed. Firewall and User Account Control (UAC) should be disabled before installing SureLog.

Uninstalling SureLog

Navigate to the Program folder in which SureLog has been installed. In most cases, the user can choose Start > All Program > SureLog. Select the option to uninstall SureLog and follow the on-screen instructions as directed.

Accessing the Web Client

Once the server has successfully started, follow the steps below to access SureLog.

1. Open a supported web browser window
2. Enter the URL address: https://<hostname>:8099 (where "<hostname>" is the name of the machine on which SureLog is running and 8099 is the default web server port)
3. Log into SureLog using the default username/password combination of **admin/anet**

Navigating Through SureLog

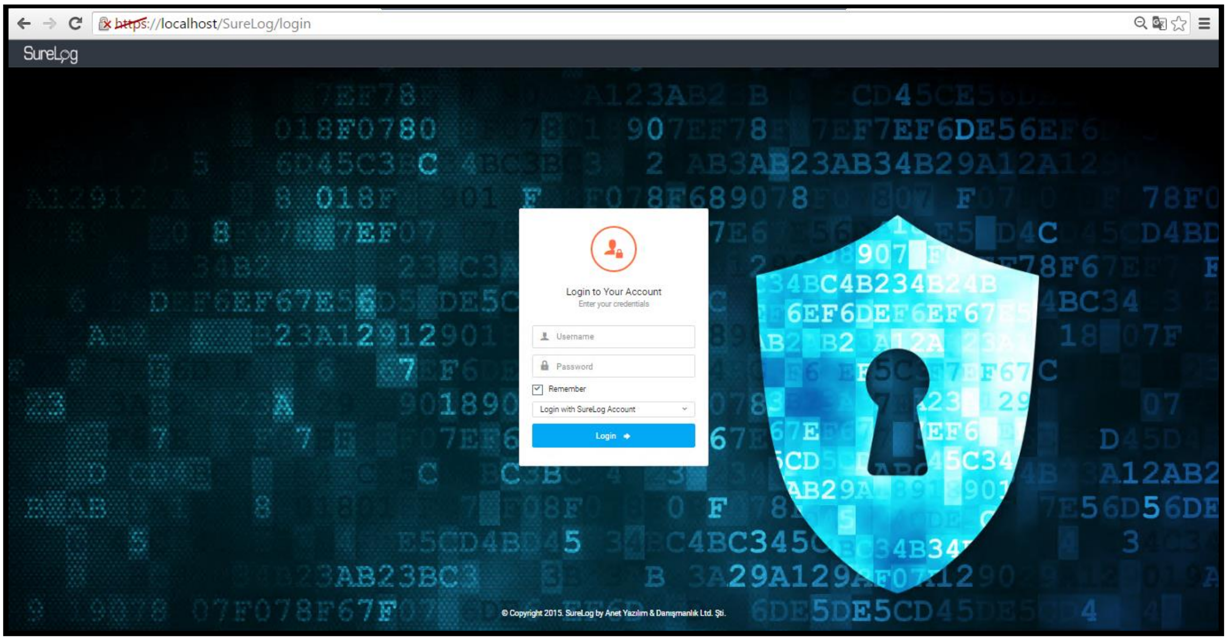
By default, once SureLog opens, the Dashboard is available. From this screen, you can navigate to various portals such as Reports, Search, Compliance, Correlation, Maps, User Management, Settings, and Help.

Login and Log out

When you open the Login URL from the browser for the first time, you are immediately prompted with the username and password screen. After entering the proper credentials, the user is logged into the tool.

Login Procedure:

- Open the SureLog login page using the login URL
- Enter the user name in the username field
- Enter the password in the password field
- Click Login


~~https~~://localhost/SureLog/login
SureLog
Login to Your Account
Enter your credentials
Username
Password
☑ Remember
Login with SureLog Account
Login
© Copyright 2015. SureLog by Anet Yazılım & Danışmanlık Ltd. Şti.

Logout Procedure:

- Click the Logout option available under the username menu at the top right corner of the screen
- The application closes and the SureLog Login screen is displayed
  Note: For security reasons, SureLog recommends that users always use the Logout option to terminate their SureLog session. By simply clicking Close or Exit, the other users may have still have access to the tool and thus, the ability to change information.

Chapter 4: Performance

One of the main advantages of SureLog is its performance. SureLog can reach speeds of 50,000 EPS with legacy HW. As previously stated, EPS is a measurement that is used to convey how fast a network generates data from its security devices such as firewalls, Intrusion Detection Systems (IDS), servers, and routers. It is also used to see how fast an SIEM product can correlate data from those types of devices. In addition, there are two EPS metrics definitions:

Normal or Sustained Events per second (NE): The NE metric represents the normal number of events usage time for a device or Log/Event Management scope.

Peak Events per second (PE): The PE metric represents the peak number of events usage time for a device or Log/Event Management scope. The PE represents abnormal activities on devices that create temporary peaks of EPS such as DoS, ports scanning, and mass SQL injections attempts. The PE metric is a bit more significant in this case because it determines real EPS requirements.

,

Minimum Requirements:

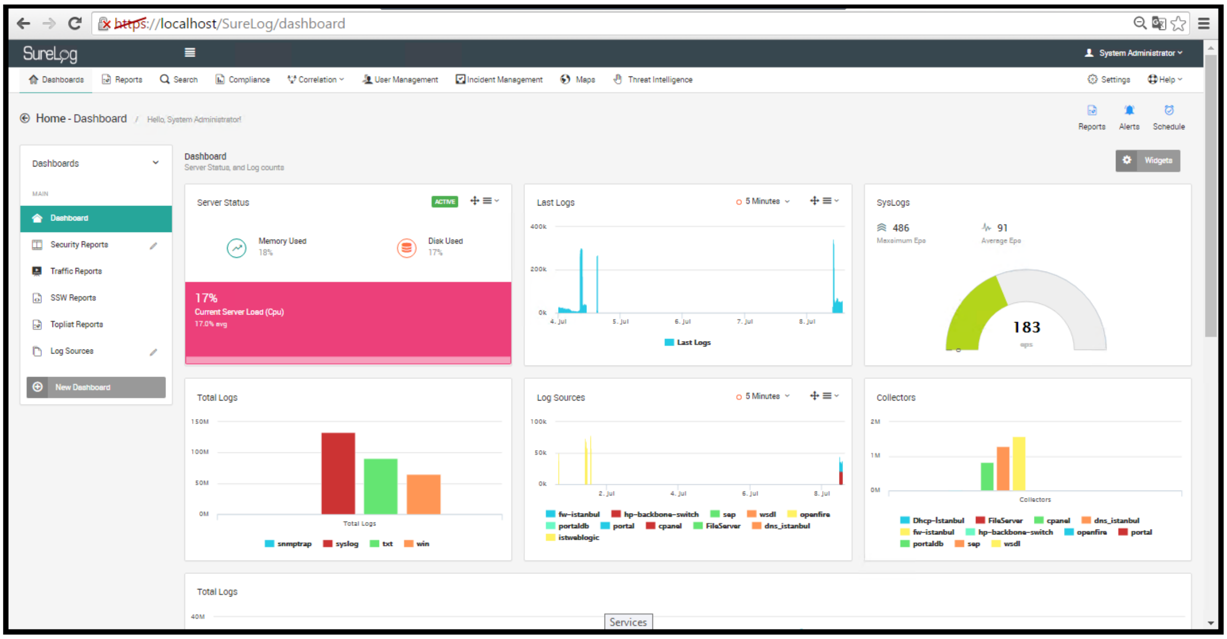
Max EPS	Requirements
250	**8 GB RAM, 8 core,** **RAID 10 10,000 RPM**
500	**12 GB RAM, 8 core,** **RAID 10 10,000 RPM**
1000	**24 GB RAM, 12 core,** **RAID 10 10,000 RPM**
2500	**48 GB RAM, 16 core, RAID 10 15,000 RPM**
5000	**64 GB RAM, 24 core,** **RAID 10 15,000 RPM**
10000	**96 GB RAM, 48 core,** **RAID 10 15,000 RPM**
15000	**128 GB RAM, 56 core ,** **RAID 10 15,000 RPM**

Why Fast EPS Performance Matters

The sooner threats and attacks to network security can be identified, the more effectively they can be contained. With the fastest EPS performance available, SureLog provides the tools and data necessary to properly monitor security incidents in real-time. With comprehensive incident reporting tools, users have instant answers to some of the most important questions like who was involved, which systems were affected and how the attack happened.

Chapter 5: Dashboards

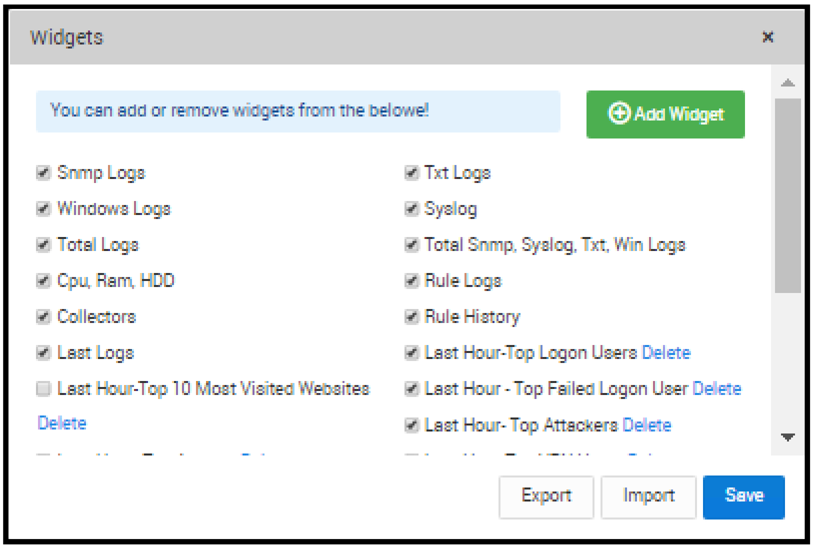
The SureLog application features dashboards on various security topics. Dashboards deliver monitoring and reporting metrics to track the state of security throughout the network. These are simple to configure and user friendly, while allowing users to read a summary of existing network infrastructure data using graphs and tables.



The following tasks can be accomplished in the Dashboard portal:

- Adding a Dashboard Panel
- Creating a New Dashboard
- Editing a Dashboard
- Deleting a Dashboard
- Selecting a Widget*

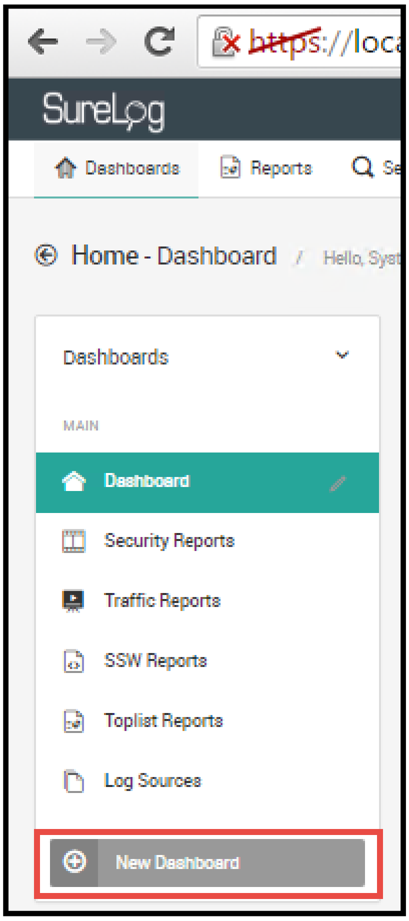
*Widgets: Use the Widgets button to add more Widgets to the Dashboard’s panel.



Widgets ×

You can add or remove widgets from the belowe!

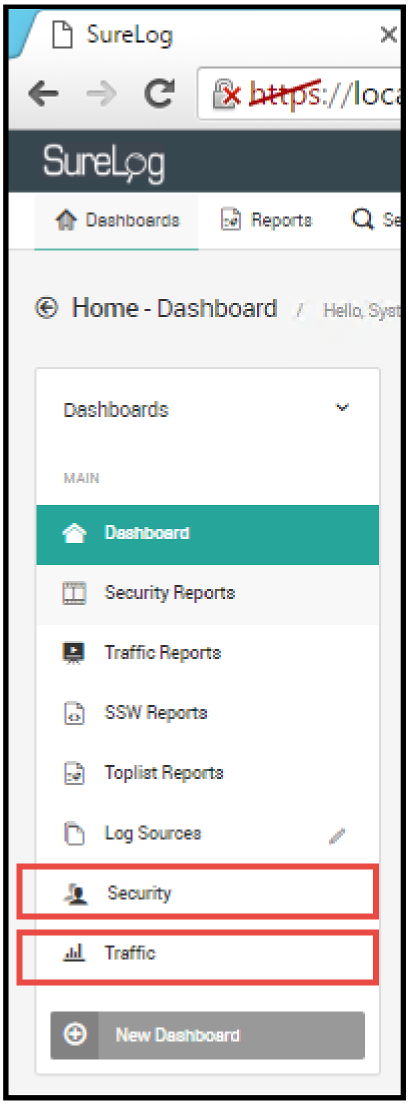
- ☑ Snmp Logs
- ☑ Windows Logs
- ☑ Total Logs
- ☑ Cpu, Ram, HDD
- ☑ Collectors
- ☑ Last Logs
- □ Last Hour-Top 10 Most Visited Websites Delete
- ☑ Txt Logs
- ☑ Syslog
- ☑ Total Snmp, Syslog, Txt, Win Logs
- ☑ Rule Logs
- ☑ Rule History
- ☑ Last Hour-Top Logon Users Delete
- ☑ Last Hour - Top Failed Logon User Delete
- ☑ Last Hour- Top Attackers Delete



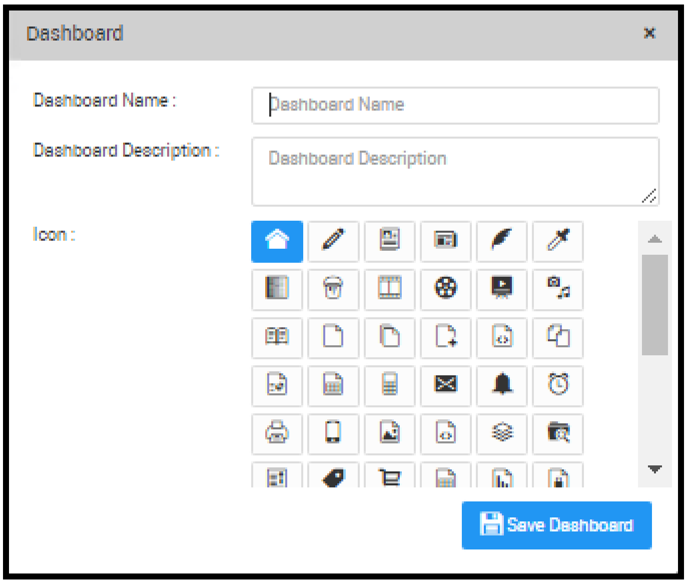
Home - Dashboard / Hello, Syst

*We can add more than one Dashboard Panels for each user such as Security and Traffic as shown in the figure below.

To create dashboard:



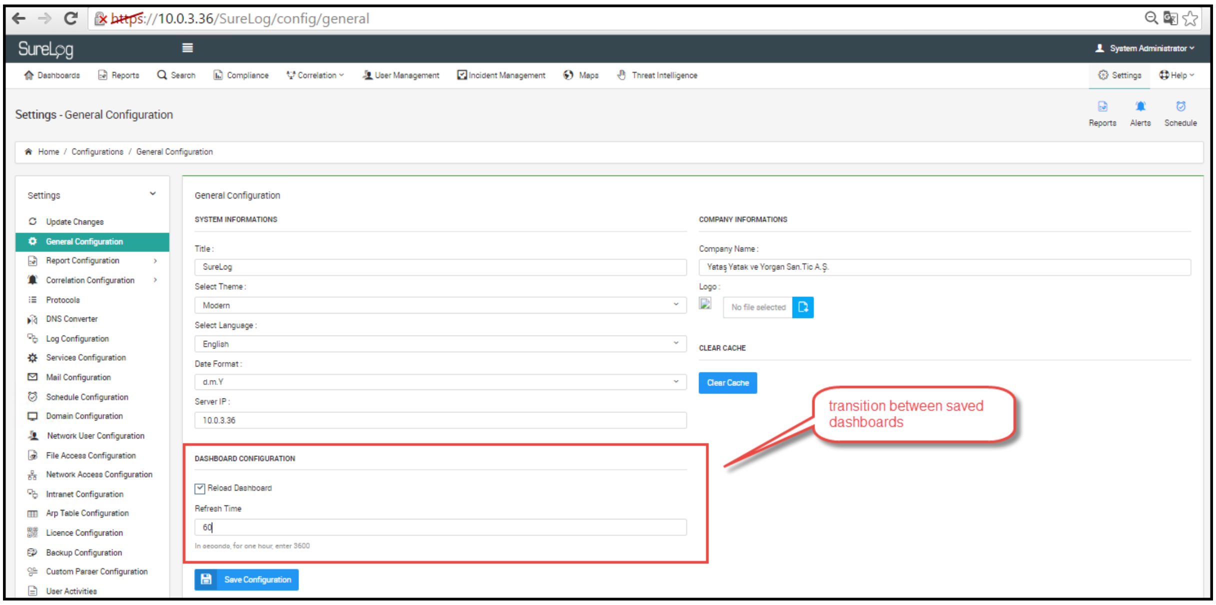
1. Click New Dashboard button
2. Enter a name for the dashboard, you can chose icon from the list.



3. Click Save Dashboard button to save the dashboard.

Transition Between Dashboard

You can transition between dashboards refresh value set 60 second as shown in the following figures:



Settings - General Configuration

General Configuration

SYSTEM INFORMATIONS

Title : SureLog

Select Theme : Modern

Select Language : English

Date Format : d.m.Y

Server IP : 10.0.3.36

COMPANY INFORMATIONS

Company Name : Yataş Yatak ve Yorgan San.Tic A.Ş.

Logo :

CLEAR CACHE

DASHBOARD CONFIGURATION

☑ Reload Dashboard

Refresh Time 60

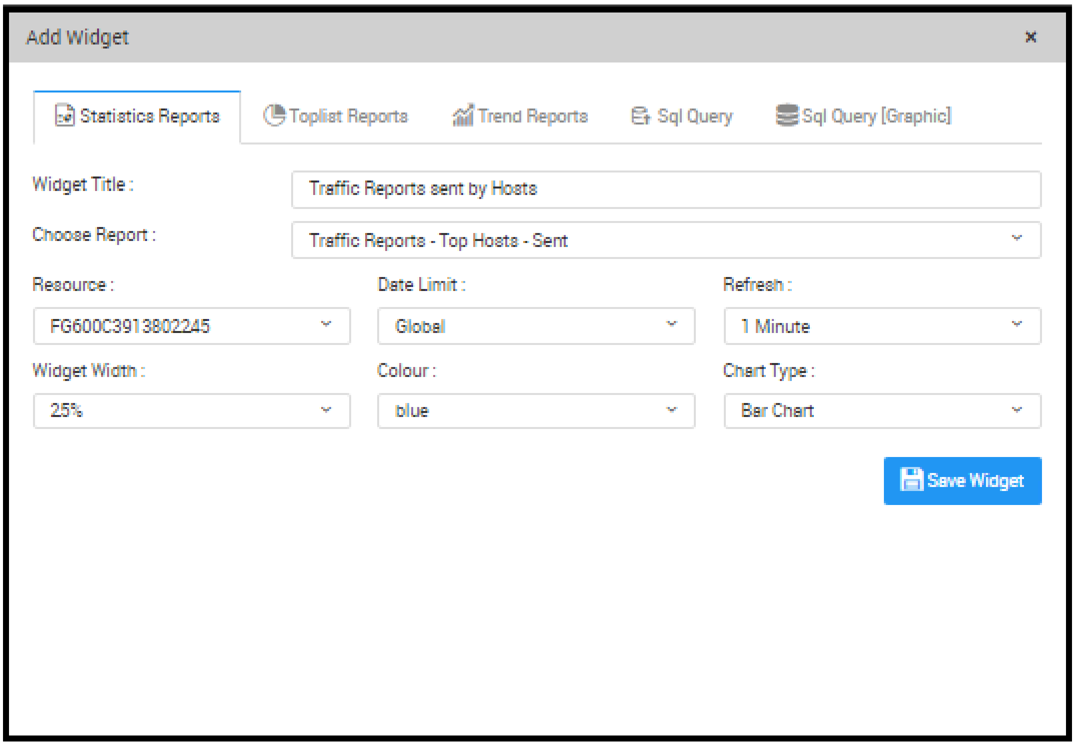
In seconds, for one hour, enter 3600

transition between saved dashboards

*The users can add Statistics Reports, Top lists Reports, Trend Reports, SQL Query and SQL Query(Graphic) as widget on Dashboard as shown in the following figures:

To add a Statistic Report on Dashboard

1. Select Dashboard
2. Select Widgets button
3. Select Add Widget button
4. Select Statistic Reports
5. Enter the following configurations into the appropriate fields:



Widget Title : Traffic Reports sent by Hosts

Choose Report : Traffic Reports - Top Hosts - Sent

Resource : FG600C3913802245

Date Limit : Global

Refresh : 1 Minute

Widget Width : 25%

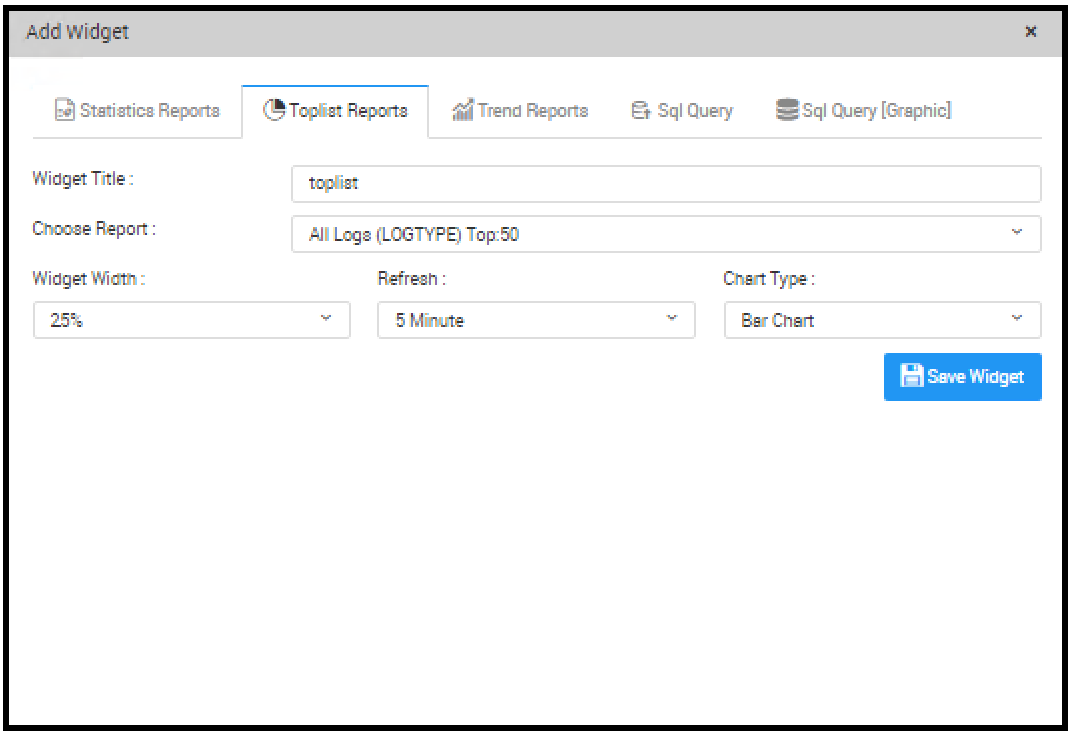
Colour : blue

Chart Type : Bar Chart

6. Click Save to save the configuration.

To add a Top list Report on Dashboard:

1. Select Dashboard
2. Select Widgets button
3. Select Add Widget button
4. Select Top list Reports
5. Enter the following configurations into the appropriate fields:



Widget Title : toplist

Choose Report : All Logs (LOGTYPE) Top:50

Widget Width : 25%

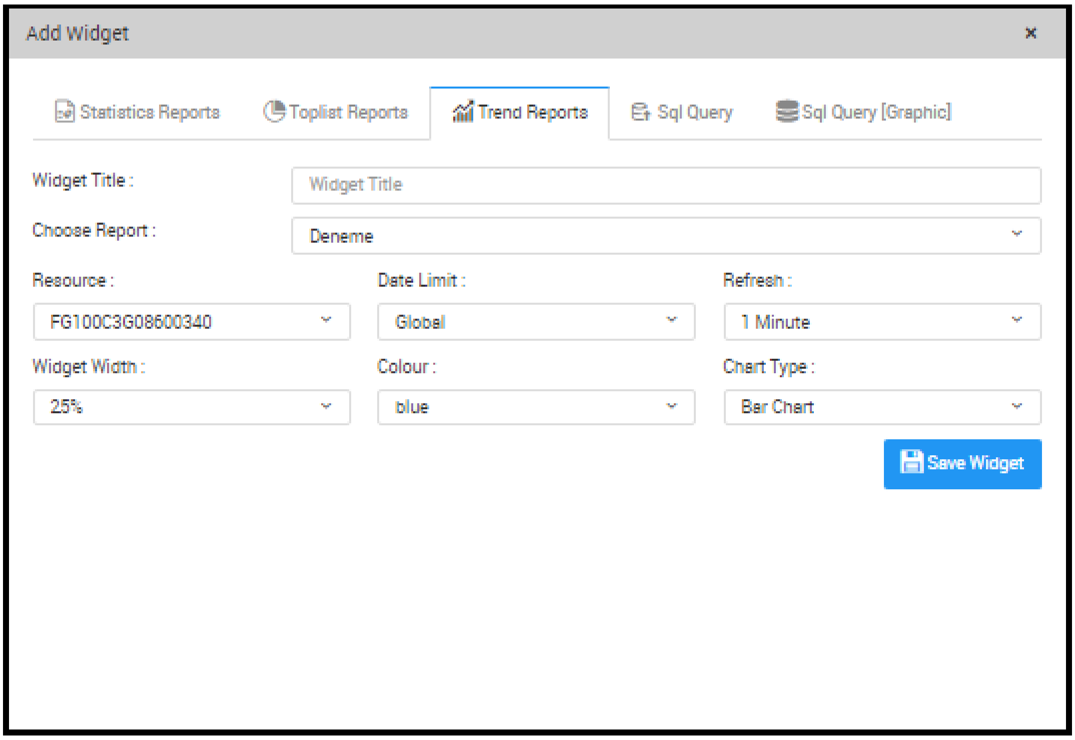
Refresh : 5 Minute

Chart Type : Bar Chart

6. Click Save to save the configuration.

To add a Trend Report on Dashboard:

1. Select Dashboard
2. Select Widgets button
3. Select Add Widget button
4. Select Trend Reports
5. Enter the following configurations into the appropriate fields:



Add Widget

Widget Title : Widget Title

Choose Report : Deneme

Resource : FG100C3G08600340

Date Limit : Global

Refresh : 1 Minute

Widget Width : 25%

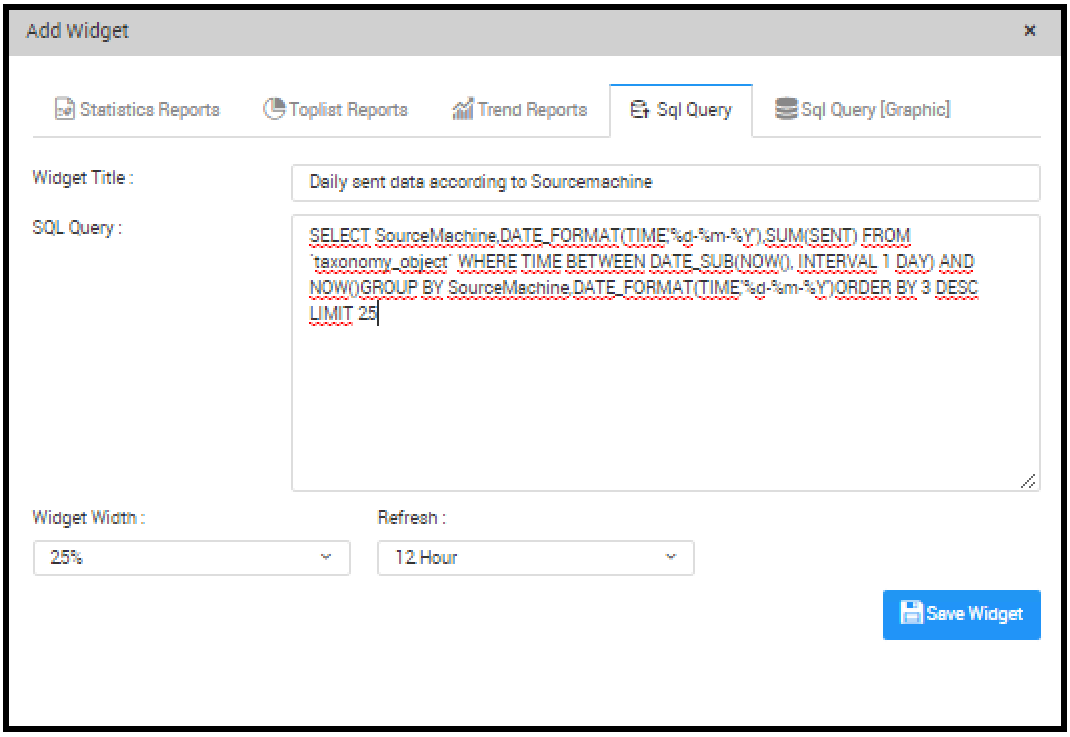
Colour : blue

Chart Type : Bar Chart

6. Click Save to save the configuration.

To add a SQL Query Report on Dashboard:

1. Select Dashboard
2. Select Widgets button
3. Select Add Widget button
4. Select SQL Query Reports
5. Enter the following configurations into the appropriate fields:



Widget Title : Daily sent data according to Sourcemachine

SQL Query :

```
SELECT SourceMachine,DATE_FORMAT(TIME,'%d-%m-%Y'),SUM(SENT) FROM
`taxonomy_object` WHERE TIME BETWEEN DATE_SUB(NOW(), INTERVAL 1 DAY) AND
NOW()GROUP BY SourceMachine,DATE_FORMAT(TIME,'%d-%m-%Y')ORDER BY 3 DESC
LIMIT 25
```

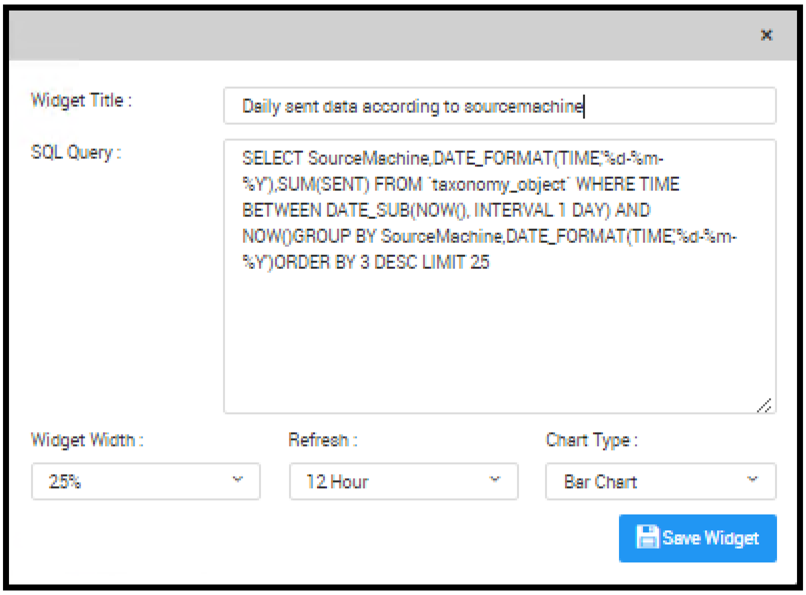
Widget Width : 25%

Refresh : 12 Hour

6. Click Save to save the configuration.

To add a SQL Query (Graphic) Report on Dashboard:

1. Select Dashboard
2. Select Widgets button
3. Select Add Widget button
4. Select SQL Query (Graphic) Reports
5. Enter the following configurations into the appropriate fields:



Widget Title : Daily sent data according to sourcemachine

SQL Query :

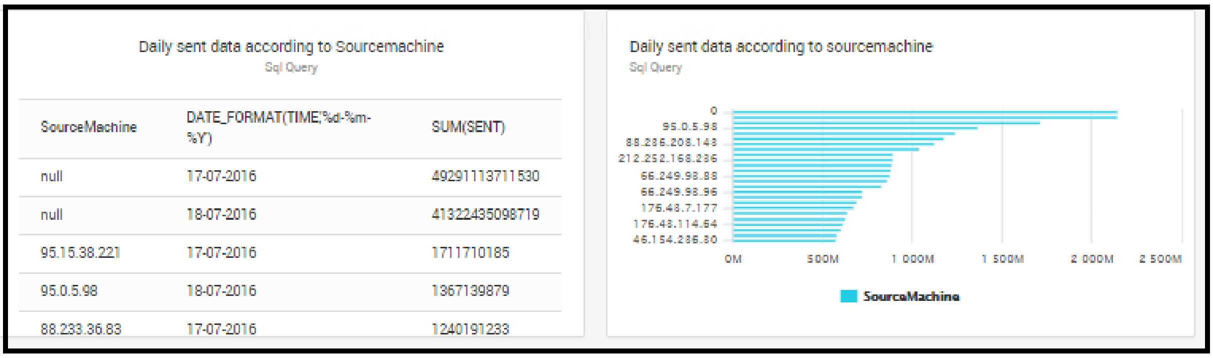
```
SELECT SourceMachine,DATE_FORMAT(TIME,'%d-%m-
%Y'),SUM(SENT) FROM `taxonomy_object` WHERE TIME
BETWEEN DATE_SUB(NOW(), INTERVAL 1 DAY) AND
NOW()GROUP BY SourceMachine,DATE_FORMAT(TIME,'%d-%m-
%Y')ORDER BY 3 DESC LIMIT 25
```

Widget Width : 25%

Refresh : 12 Hour

Chart Type : Bar Chart

6. Click Save to save the configuration.
   The widgets are shown below;



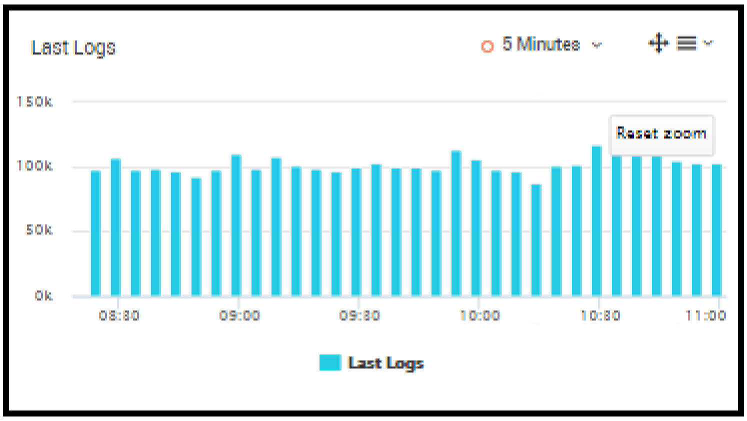
Daily sent data according to Sourcemachine
Sql Query

SourceMachine	DATE_FORMAT(TIME,'%d-%m-%Y')	SUM(SENT)
null	17-07-2016	49291113711530
null	18-07-2016	41322435098719
95.15.38.221	17-07-2016	1711710185
95.0.5.98	18-07-2016	1367139879
88.233.36.83	17-07-2016	1240191233

Daily sent data according to sourcemachine
Sql Query

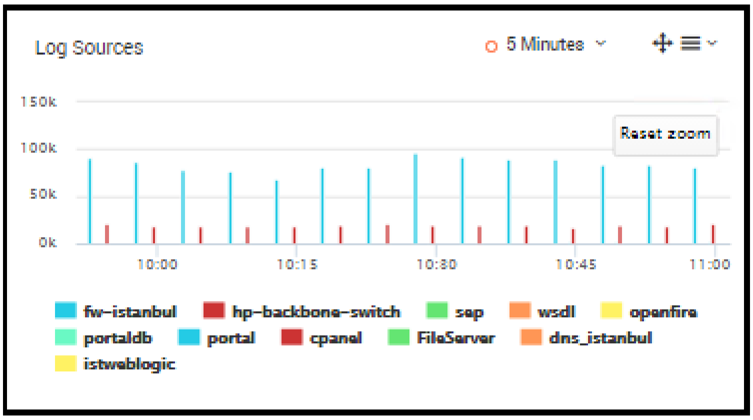
Last Logs

You can follow last log volume from dashboard;



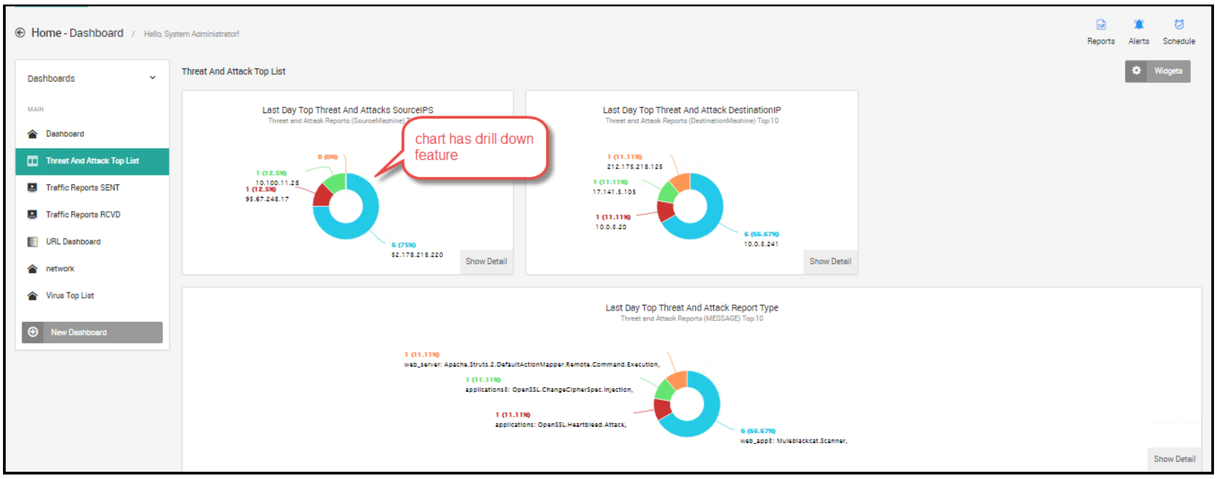
Log Sources

You can follow log sources from dashboard;



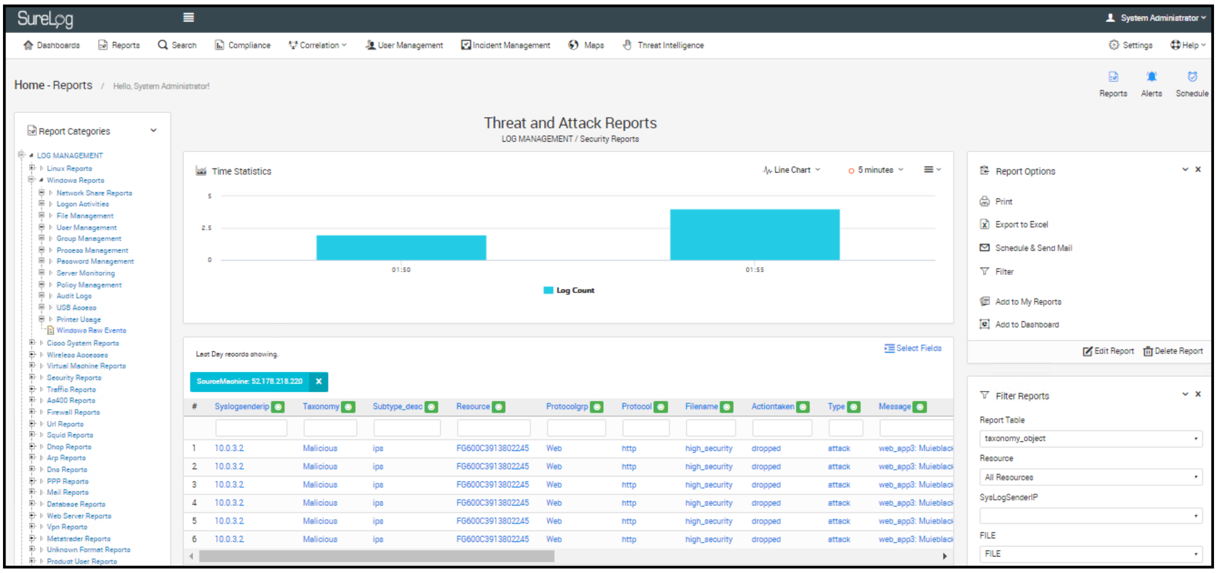
Drill –Down Feature

If you click on charts you move from one place to another, information to detailed data by focusing in on details. Each chart has this property.



Home - Dashboard / Hello, System Administrator!
Reports
Alerts
Schedule
Widgets
Dashboards
MAIN
Dashboard
Threat And Attack Top List
Traffic Reports SENT
Traffic Reports RCVD
URL Dashboard
network
Virus Top List
New Dashboard
Threat And Attack Top List
Last Day Top Threat And Attacks SourceIPS
Threat and Attack Reports (SourceMachine) Top:10
0 (0%)
1 (12.5%)
10.100.11.28
1 (12.5%)
95.67.248.17
6 (75%)
52.178.218.220
Show Detail
Last Day Top Threat And Attack DestinationIP
Threat and Attack Reports (DestinationMachine) Top:10
1 (11.11%)
212.175.218.125
1 (11.11%)
17.141.5.105
1 (11.11%)
10.0.3.20
6 (66.67%)
10.0.3.241
Show Detail
Last Day Top Threat And Attack Report Type
Threat and Attack Reports (MESSAGE) Top:10
1 (11.11%)
web_server: Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution,
1 (11.11%)
applications: OpenSSL.ChangeCipherSpec.Injection,
1 (11.11%)
applications: OpenSSL.Heartbleed.Attack,
6 (66.67%)
web_app3: Mulebleckcat.Scanner,
Show Detail

chart has drill down feature



Threat and Attack Reports
LOG MANAGEMENT / Security Reports

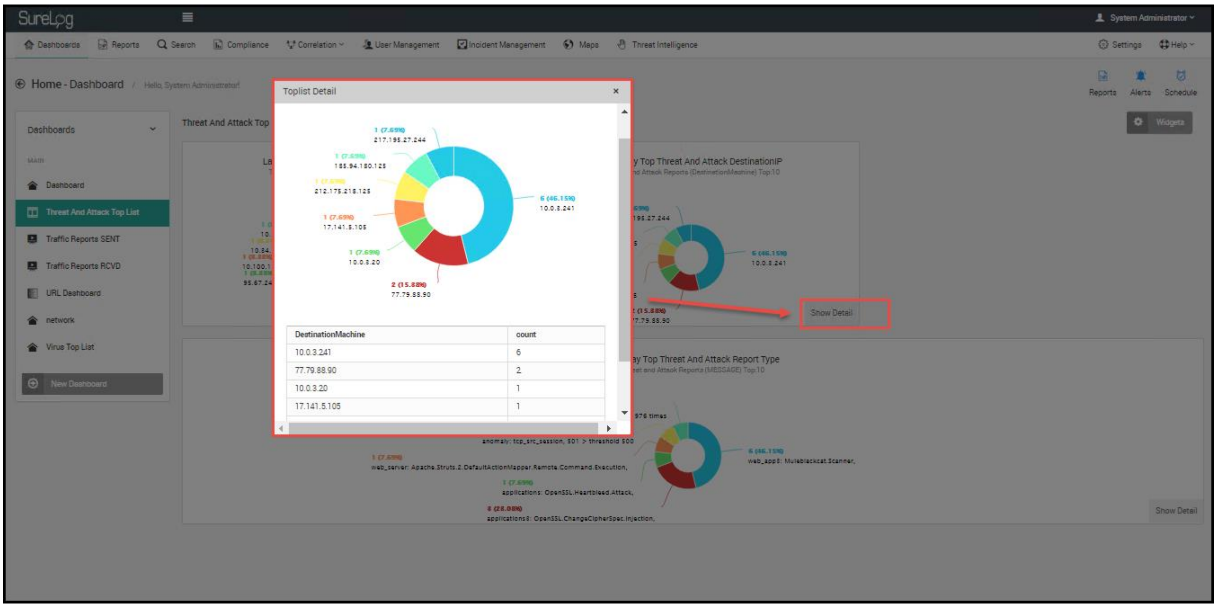
Last Day records showing.

SourceMachine: 52.178.218.220 ×

#	Syslogsenderip	Taxonomy	Subtype_desc	Resource	Protocolgrp	Protocol	Filename	Actiontaken	Type	Message
1	10.0.3.2	Malicious	ips	FG600C3913802245	Web	http	high_security	dropped	attack	web_app3: Muieblack
2	10.0.3.2	Malicious	ips	FG600C3913802245	Web	http	high_security	dropped	attack	web_app3: Muieblack
3	10.0.3.2	Malicious	ips	FG600C3913802245	Web	http	high_security	dropped	attack	web_app3: Muieblack
4	10.0.3.2	Malicious	ips	FG600C3913802245	Web	http	high_security	dropped	attack	web_app3: Muieblack
5	10.0.3.2	Malicious	ips	FG600C3913802245	Web	http	high_security	dropped	attack	web_app3: Muieblack
6	10.0.3.2	Malicious	ips	FG600C3913802245	Web	http	high_security	dropped	attack	web_app3: Muieblack

Report Table: taxonomy_object
Resource: All Resources
SysLogSenderIP:
FILE: FILE

Also you can find details by clicking the Show details shown below;



DestinationMachine	count
10.0.3.241	6
77.79.88.90	2
10.0.3.20	1
17.141.5.105	1

Adding a Dashboard Panel

SureLog provides users with the flexibility to instantly add a panel to the current dashboard layout. The dashboard layout is logically divided into Top and Bottom sections.

1. In the New Dashboard Widget panel, select any widget from list, drag and drop the selected panel into the Set Dashboard Layout section. The selected report/monitor is added to the dashboard panel.

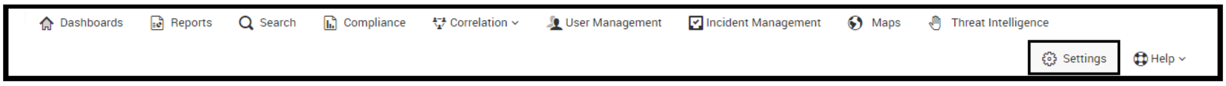
Customizing Dashboard View

To customize the panels available in the dashboard, users can do the following:

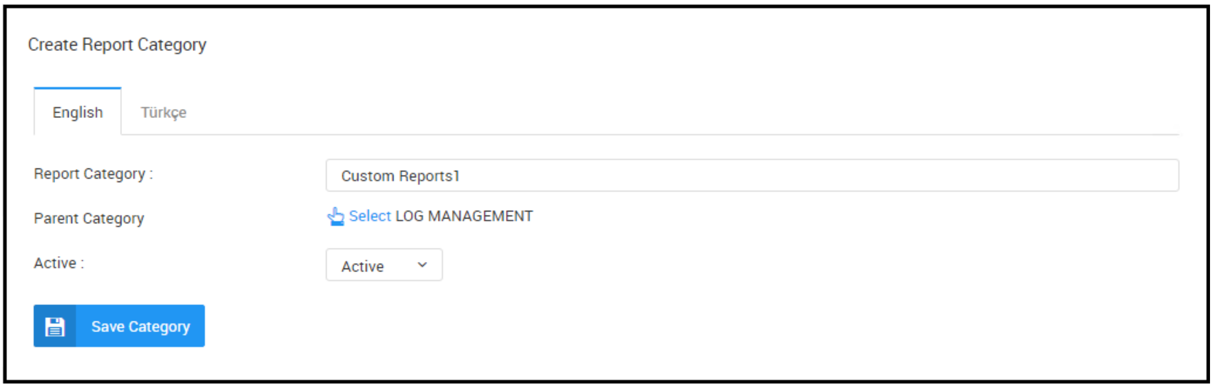
Creating report categories

To create a report category, the user can do the following:

1. Click on the Settings menu



2. Select Settings
3. Select Report Configuration
4. Select Report Categories
5. Click the Add Category button at the top right corner of the screen.
6. Enter the following configurations into the appropriate fields:
7. Click save button to save the changes.


Create Report Category

English Türkçe

Report Category : Custom Reports1

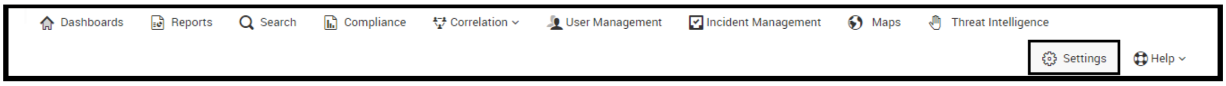
Parent Category Select LOG MANAGEMENT

Active : Active

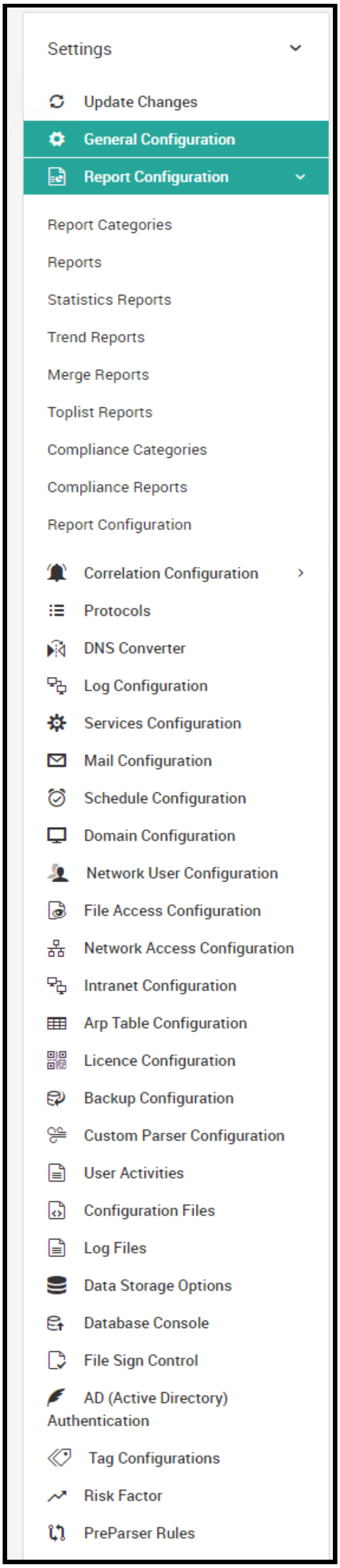
Creating custom reports

To create a custom report such as statistic report, the users can do the following:

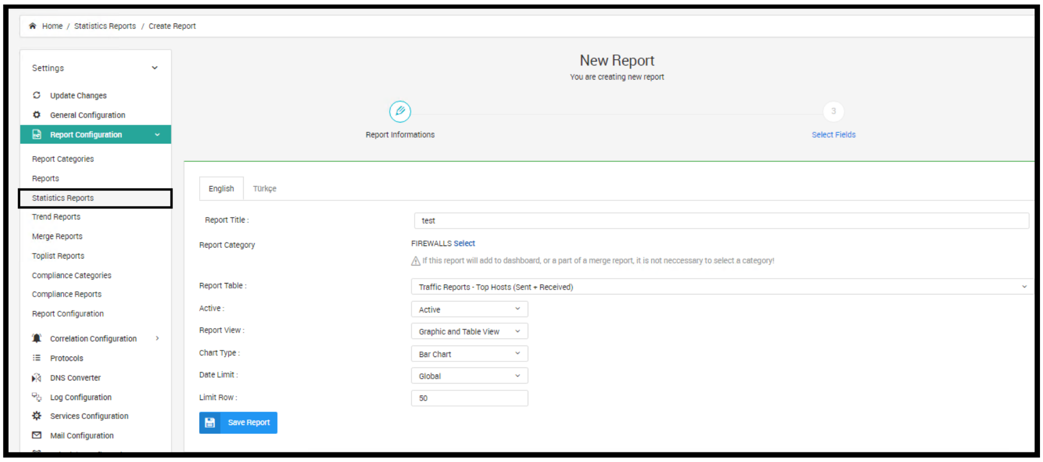
1. Click on the Settings menu



2. Select Statistics Reports from the Report Configuration tree based on the user’s requirement


Settings
Update Changes
General Configuration
Report Configuration
Report Categories
Reports
Statistics Reports
Trend Reports
Merge Reports
Toplist Reports
Compliance Categories
Compliance Reports
Report Configuration
Correlation Configuration
Protocols
DNS Converter
Log Configuration
Services Configuration
Mail Configuration
Schedule Configuration
Domain Configuration
Network User Configuration
File Access Configuration
Network Access Configuration
Intranet Configuration
Arp Table Configuration
Licence Configuration
Backup Configuration
Custom Parser Configuration
User Activities
Configuration Files
Log Files
Data Storage Options
Database Console
File Sign Control
AD (Active Directory) Authentication
Tag Configurations
Risk Factor
PreParser Rules

1. Select Settings
2. Select Report Configuration
3. Select Statistics Reports
4. Click the Create Report button at the top right corner of the screen.



New Report

You are creating new report

Report Title : test

Report Category FIREWALLS Select

⚠ If this report will add to dashboard, or a part of a merge report, it is not neccessary to select a category!

Report Table : Traffic Reports - Top Hosts (Sent + Received)

Active : Active

Report View : Graphic and Table View

Chart Type : Bar Chart

Date Limit : Global

Limit Row : 50

5. Enter the following configurations into the appropriate fields:
   Report Title: Title & name of the widget
   Report Category: The users can use their own report categories.
   Report Table: Select from the available statistics parameters:

Active: Enable/Disable

Report View: Select a report type as table, graphic, or both

Chart type: Select from various graphic chart type options such as bar, line, area, etc.

Date Limit: Select a time frame value. If global time is selected, the value will be adjusted to the system's global time which is configured within the reports module. Other options include:

- Last Hour
- Last Day
- Last Week
- Last Month
- Last Three Months
- Last Six Months
- Last Year

Limit Row: Limits the data and row number

6. Click the Save Report button
7. Select the Fields option to choose the fields that are displayed on the Dashboard or reports. (If uncertain, select all fields.)

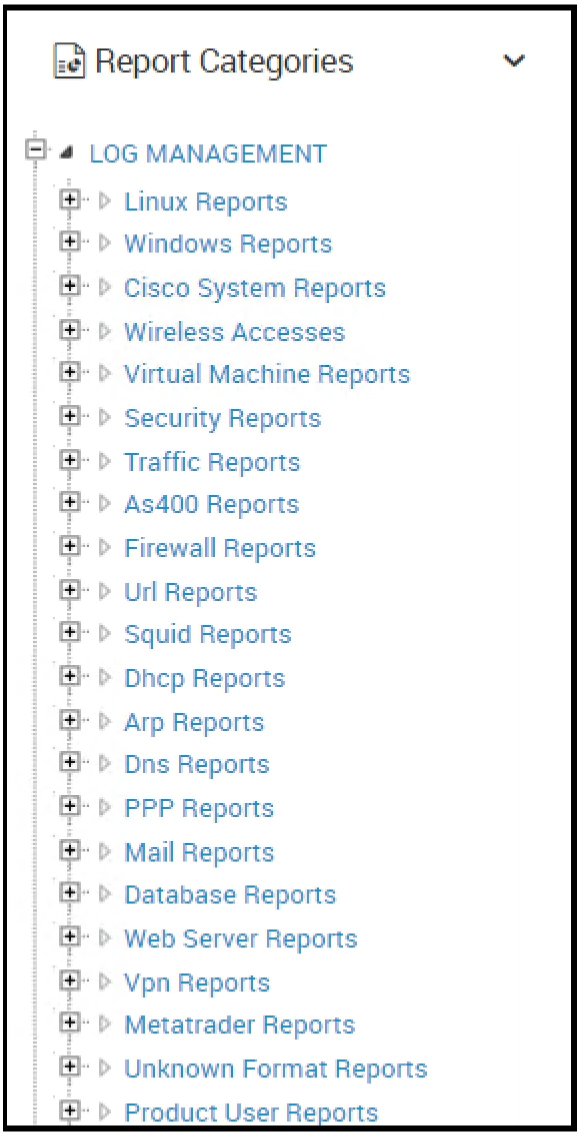
Chapter 6: Reports

Log Management

The Log Management module helps users manage and create report views on aggregated logs for all collected logs. The Diagnostics module, an extension of the product‘s reporting features, provides an in-depth evaluation with a narrow analysis scope. This module is aimed at identifying a specific condition or problem.

To access the Log Management section, click Reports, then Log Management.

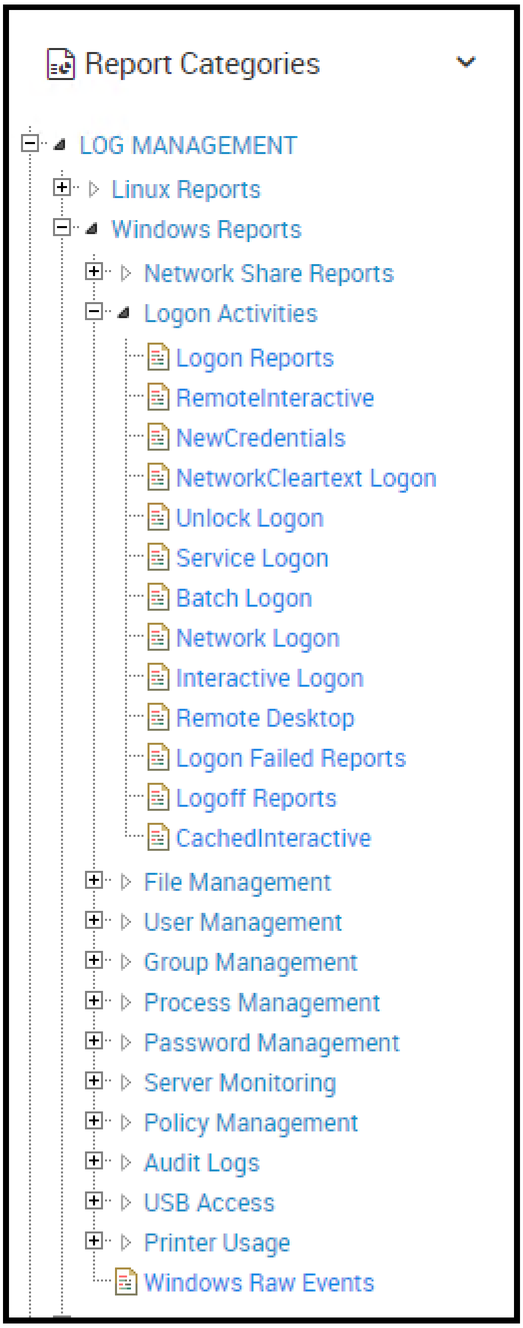
Log Management Report Categories:



Report Categories

- LOG MANAGEMENT
  - Linux Reports
  - Windows Reports
  - Cisco System Reports
  - Wireless Accesses
  - Virtual Machine Reports
  - Security Reports
  - Traffic Reports
  - As400 Reports
  - Firewall Reports
  - Url Reports
  - Squid Reports
  - Dhcp Reports
  - Arp Reports
  - Dns Reports
  - PPP Reports
  - Mail Reports
  - Database Reports
  - Web Server Reports
  - Vpn Reports
  - Metatrader Reports
  - Unknown Format Reports
  - Product User Reports

Each report has sub-reports:



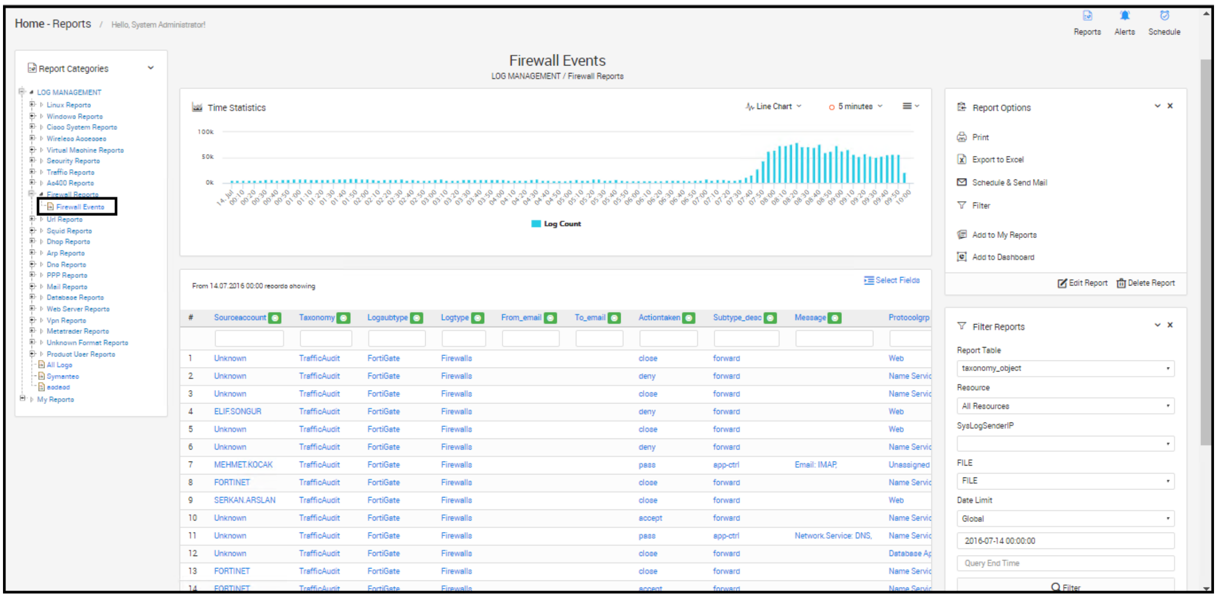
Report Categories

- LOG MANAGEMENT
  - Linux Reports
  - Windows Reports
    - Network Share Reports
    - Logon Activities
      - Logon Reports
      - RemoteInteractive
      - NewCredentials
      - NetworkCleartext Logon
      - Unlock Logon
      - Service Logon
      - Batch Logon
      - Network Logon
      - Interactive Logon
      - Remote Desktop
      - Logon Failed Reports
      - Logoff Reports
      - CachedInteractive
    - File Management
    - User Management
    - Group Management
    - Process Management
    - Password Management
    - Server Monitoring
    - Policy Management
    - Audit Logs
    - USB Access
    - Printer Usage
    - Windows Raw Events

In most cases, sub-reports have sub-categories:

To view cataloged logs:

1- Select a catalog from the left tree
2- Select a sub-catalog, if any, or click All Events (Here is Firewall Events)



From 14.07.2016 00:00 records showing

#	Sourceaccount	Taxonomy	Logsubtype	Logtype	From_email	To_email	Actiontaken	Subtype_desc	Message	Protocolgrp
1	Unknown	TrafficAudit	FortiGate	Firewalls			close	forward		Web
2	Unknown	TrafficAudit	FortiGate	Firewalls			deny	forward		Name Servic
3	Unknown	TrafficAudit	FortiGate	Firewalls			close	forward		Name Servic
4	ELIF.SONGUR	TrafficAudit	FortiGate	Firewalls			deny	forward		Web
5	Unknown	TrafficAudit	FortiGate	Firewalls			close	forward		Web
6	Unknown	TrafficAudit	FortiGate	Firewalls			deny	forward		Name Servic
7	MEHMET.KOCAK	TrafficAudit	FortiGate	Firewalls			pass	app-ctrl	Email: IMAP,	Unassigned
8	FORTINET	TrafficAudit	FortiGate	Firewalls			close	forward		Name Servic
9	SERKAN.ARSLAN	TrafficAudit	FortiGate	Firewalls			close	forward		Web
10	Unknown	TrafficAudit	FortiGate	Firewalls			accept	forward		Name Servic
11	Unknown	TrafficAudit	FortiGate	Firewalls			pass	app-ctrl	Network.Service: DNS,	Name Servic
12	Unknown	TrafficAudit	FortiGate	Firewalls			close	forward		Database Ap
13	FORTINET	TrafficAudit	FortiGate	Firewalls			close	forward		Name Servic
14	FORTINET	TrafficAudit	FortiGate	Firewalls			accept	forward		Name Servic

Report Table: taxonomy_object

Resource: All Resources

SysLogSenderIP:

FILE: FILE

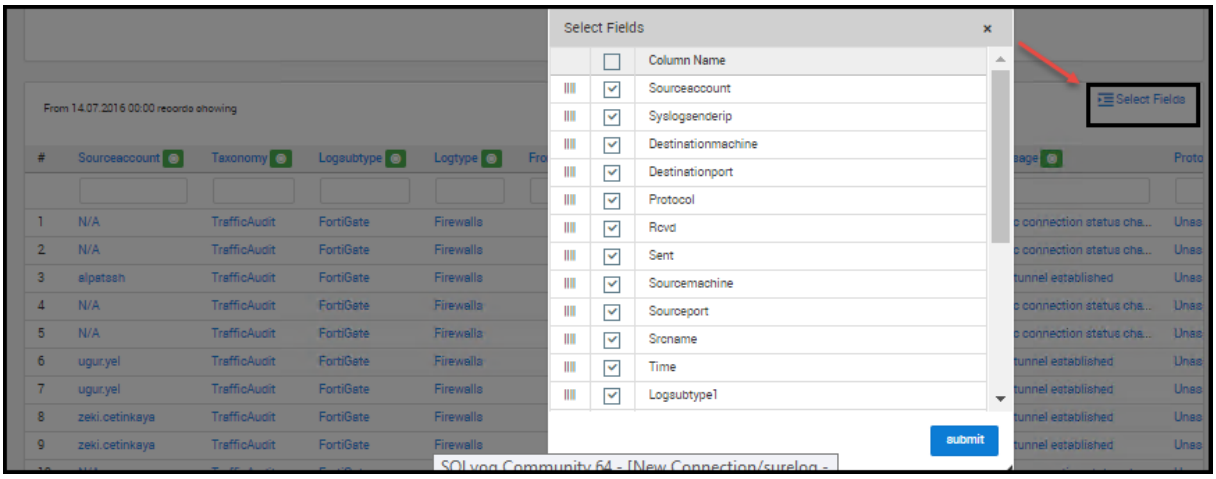
Date Limit: Global

2016-07-14 00:00:00

Query End Time

To configure catalog views:

1. On the right pane, To configure views or enable/disable columns, select Select Fields as shown in the following figure:



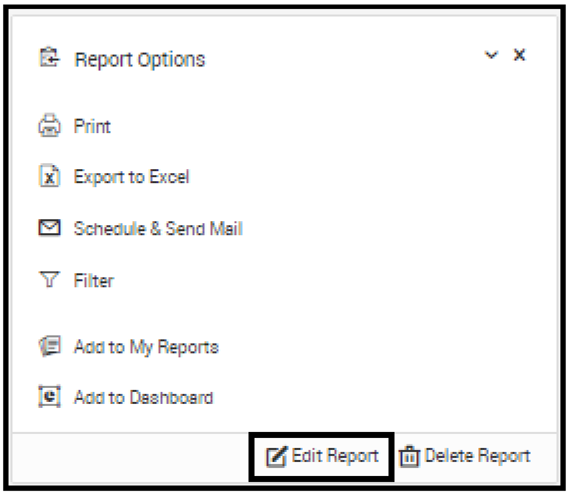
	Column Name
☑	Sourceaccount
☑	Syslogsenderip
☑	Destinationmachine
☑	Destinationport
☑	Protocol
☑	Rcvd
☑	Sent
☑	Sourcemachine
☑	Sourceport
☑	Srcname
☑	Time
☑	Logsubtype1

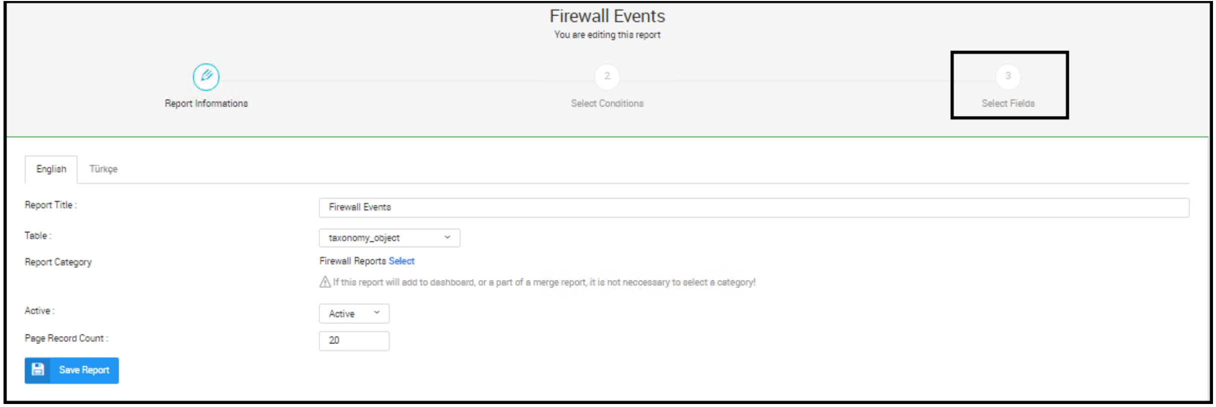
From 14.07.2016 00:00 records showing

#	Sourceaccount	Taxonomy	Logsubtype	Logtype	Fro	sage	Proto
1	N/A	TrafficAudit	FortiGate	Firewalls		c connection status cha...	Unas
2	N/A	TrafficAudit	FortiGate	Firewalls		c connection status cha...	Unas
3	alpatash	TrafficAudit	FortiGate	Firewalls		tunnel established	Unas
4	N/A	TrafficAudit	FortiGate	Firewalls		c connection status cha...	Unas
5	N/A	TrafficAudit	FortiGate	Firewalls		c connection status cha...	Unas
6	ugur.yel	TrafficAudit	FortiGate	Firewalls		tunnel established	Unas
7	ugur.yel	TrafficAudit	FortiGate	Firewalls		tunnel established	Unas
8	zeki.cetinkaya	TrafficAudit	FortiGate	Firewalls		tunnel established	Unas
9	zeki.cetinkaya	TrafficAudit	FortiGate	Firewalls		tunnel established	Unas

Select fields to be shown in Views and Reports:

1. To rename a column, enter the desired name into Column Description.
2. Edit report
3. Select field and write desired name to related field





Firewall Events

You are editing this report

Report Title : Firewall Events

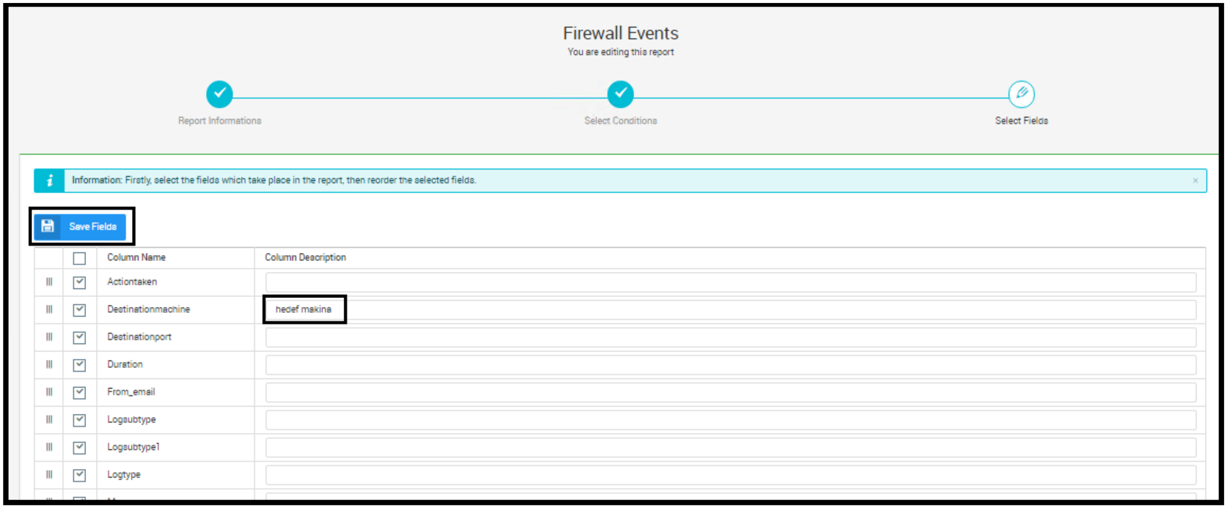
Table : taxonomy_object

Report Category Firewall Reports Select

⚠ If this report will add to dashboard, or a part of a merge report, it is not neccessary to select a category!

Active : Active

Page Record Count : 20



Firewall Events

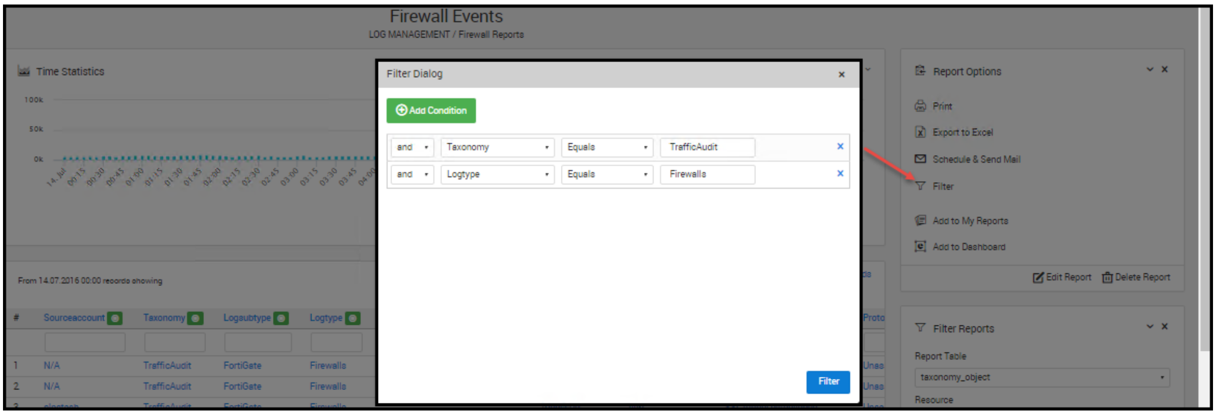
You are editing this report

Information: Firstly, select the fields which take place in the report, then reorder the selected fields.

	□	Column Name	Column Description
|||	☑	Actiontaken	
|||	☑	Destinationmachine	hedef makina
|||	☑	Destinationport	
|||	☑	Duration	
|||	☑	From_email	
|||	☑	Logsubtype	
|||	☑	Logsubtype1	
|||	☑	Logtype	

Steps to filter logs:

1. On the left panel,
2. Click Filter,
3. Add conditions to filter the logs



Firewall Events

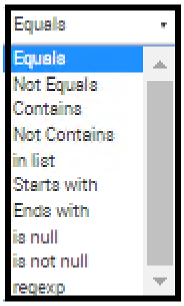
LOG MANAGEMENT / Firewall Reports

Filter Dialog

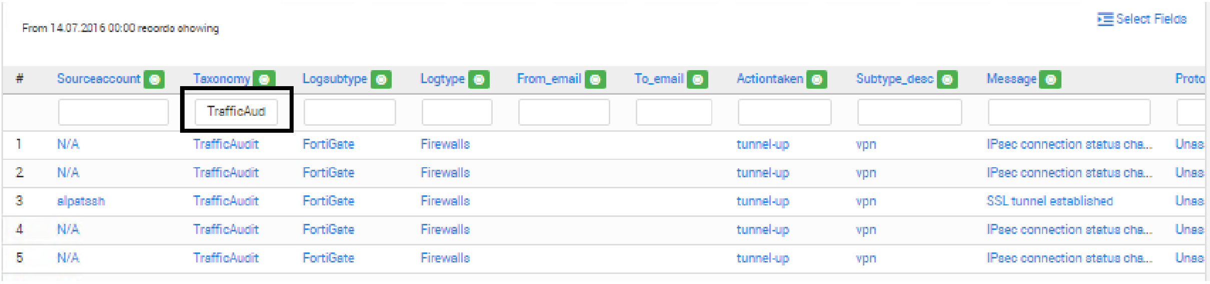
and	Taxonomy	Equals	TrafficAudit
and	Logtype	Equals	Firewalls

From 14.07.2016 00:00 records showing

4. Logic operators such as “AND” or “OR “can be used between columns (many operators can be used to filter the column’s value)



Also you can filter trough writing to selected blank area that shown below



From 14.07.2016 00:00 records showing

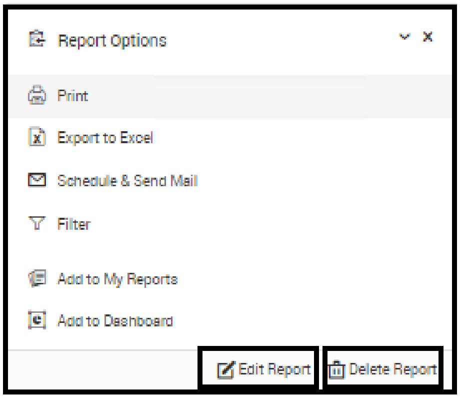
#	Sourceaccount	Taxonomy	Logsubtype	Logtype	From_email	To_email	Actiontaken	Subtype_desc	Message	Proto
		TrafficAud								
1	N/A	TrafficAudit	FortiGate	Firewalls			tunnel-up	vpn	IPsec connection status cha...	Unas
2	N/A	TrafficAudit	FortiGate	Firewalls			tunnel-up	vpn	IPsec connection status cha...	Unas
3	alpatash	TrafficAudit	FortiGate	Firewalls			tunnel-up	vpn	SSL tunnel established	Unas
4	N/A	TrafficAudit	FortiGate	Firewalls			tunnel-up	vpn	IPsec connection status cha...	Unas
5	N/A	TrafficAudit	FortiGate	Firewalls			tunnel-up	vpn	IPsec connection status cha...	Unas

Steps for editing reports:

1. On the Left pane,
2. Click Edit Report

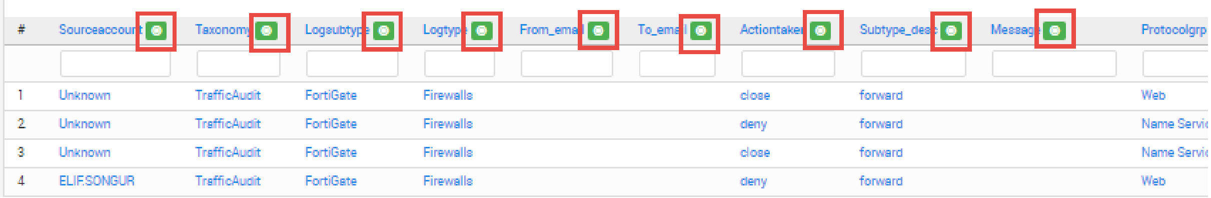
Steps for deleting reports:

1. On the Left pane,
2. Click Delete Report



Creating Dynamic Top List Reports

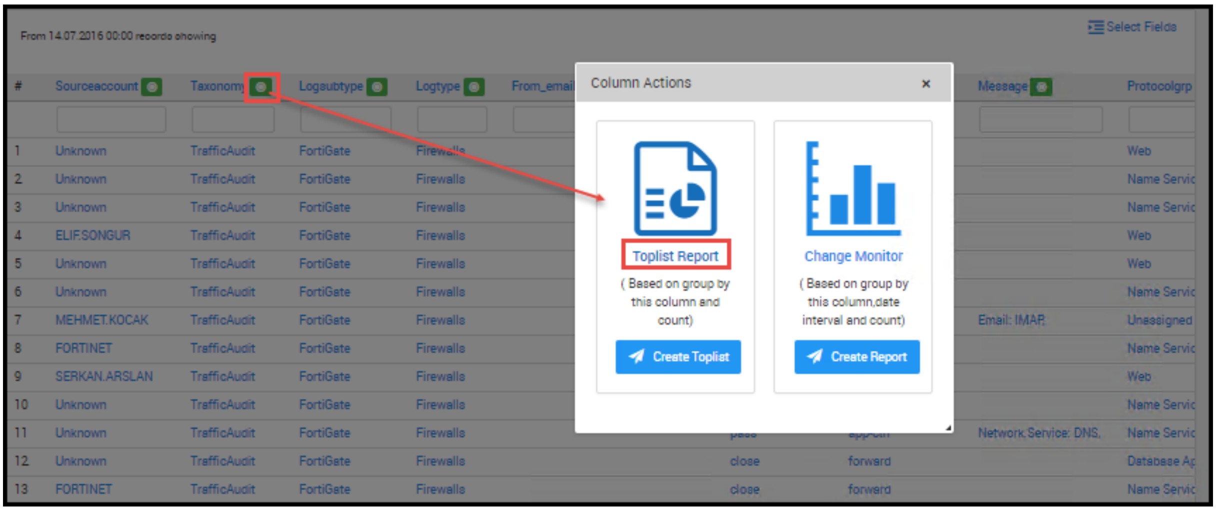
On the View pane, click the button near the column where the Top List and Change Monitor report will be created



#	Sourceaccount	Taxonomy	Logsubtype	Logtype	From_email	To_email	Actiontaker	Subtype_desc	Message	Protocolgrp
1	Unknown	TrafficAudit	FortiGate	Firewalls			close	forward		Web
2	Unknown	TrafficAudit	FortiGate	Firewalls			deny	forward		Name Servic
3	Unknown	TrafficAudit	FortiGate	Firewalls			close	forward		Name Servic
4	ELIF.SONGUR	TrafficAudit	FortiGate	Firewalls			deny	forward		Web

Top List Report

For Top List Report Select the appropriate parameters for the top list



From 14.07.2016 00:00 records showing

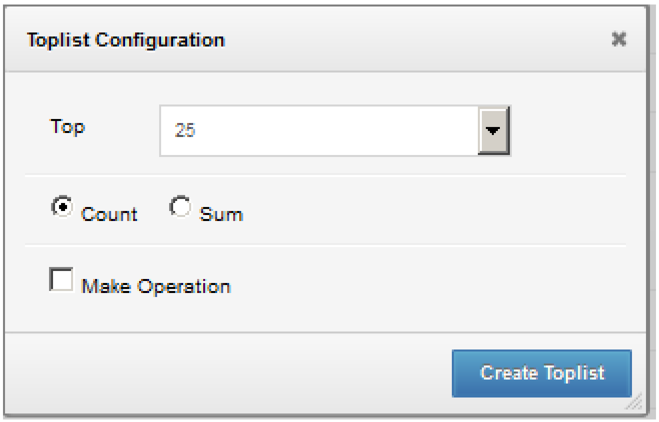
Select Fields

#	Sourceaccount	Taxonomy	Logsubtype	Logtype	From_email			Message	Protocolgrp
1	Unknown	TrafficAudit	FortiGate	Firewalls					Web
2	Unknown	TrafficAudit	FortiGate	Firewalls					Name Servic
3	Unknown	TrafficAudit	FortiGate	Firewalls					Name Servic
4	ELIF.SONGUR	TrafficAudit	FortiGate	Firewalls					Web
5	Unknown	TrafficAudit	FortiGate	Firewalls					Web
6	Unknown	TrafficAudit	FortiGate	Firewalls					Name Servic
7	MEHMET.KOCAK	TrafficAudit	FortiGate	Firewalls				Email: IMAP,	Unassigned
8	FORTINET	TrafficAudit	FortiGate	Firewalls					Name Servic
9	SERKAN.ARSLAN	TrafficAudit	FortiGate	Firewalls					Web
10	Unknown	TrafficAudit	FortiGate	Firewalls					Name Servic
11	Unknown	TrafficAudit	FortiGate	Firewalls		pass	app-ctrl	Network Service: DNS,	Name Servic
12	Unknown	TrafficAudit	FortiGate	Firewalls		close	forward		Database Ap
13	FORTINET	TrafficAudit	FortiGate	Firewalls		close	forward		Name Servic

Column Actions

Toplist Report
(Based on group by this column and count)

Change Monitor
(Based on group by this column,date interval and count)

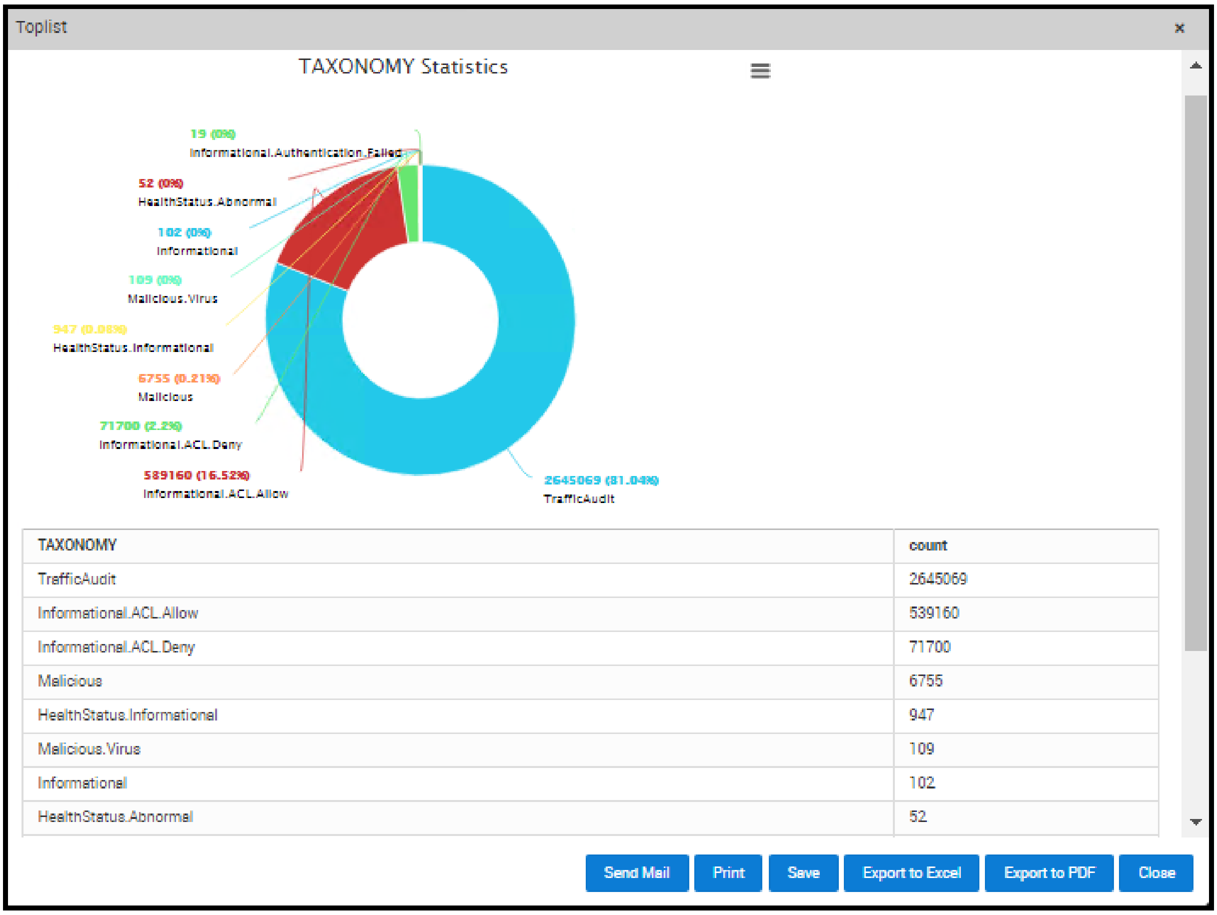


Top: N parameters for the top list

Count: Initiate a count operation over the selected columns

Sum: Initiate a sum operation over the selected columns

Make Operation: Do summation, subtraction, division, or multiplication operations over a counted or summed value

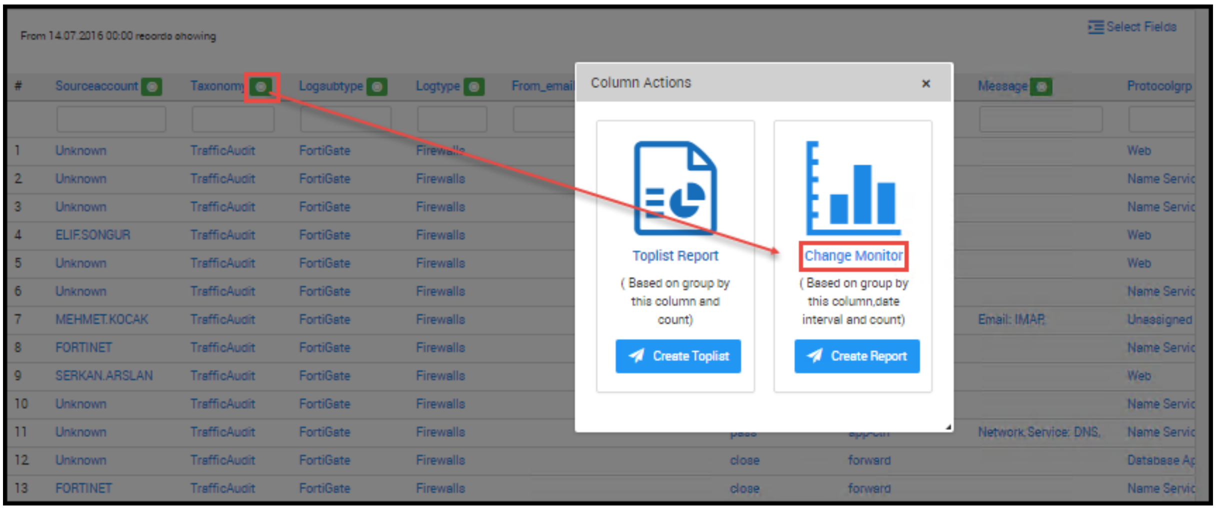


TAXONOMY	count
TrafficAudit	2645069
Informational.ACL.Allow	539160
Informational.ACL.Deny	71700
Malicious	6755
HealthStatus.Informational	947
Malicious.Virus	109
Informational	102
HealthStatus.Abnormal	52

You can send Top list report by email, print it, save it, and export it to Excel and PDF.

Change Monitor Report

For Change Monitor Report Select the appropriate parameters for the top list



From 14.07.2016 00:00 records showing

#	Sourceaccount	Taxonomy	Logsubtype	Logtype	From_email			Message	Protocolgrp
1	Unknown	TrafficAudit	FortiGate	Firewalls					Web
2	Unknown	TrafficAudit	FortiGate	Firewalls					Name Servic
3	Unknown	TrafficAudit	FortiGate	Firewalls					Name Servic
4	ELIF.SONGUR	TrafficAudit	FortiGate	Firewalls					Web
5	Unknown	TrafficAudit	FortiGate	Firewalls					Web
6	Unknown	TrafficAudit	FortiGate	Firewalls					Name Servic
7	MEHMET.KOCAK	TrafficAudit	FortiGate	Firewalls				Email: IMAP,	Unassigned
8	FORTINET	TrafficAudit	FortiGate	Firewalls					Name Servic
9	SERKAN.ARSLAN	TrafficAudit	FortiGate	Firewalls					Web
10	Unknown	TrafficAudit	FortiGate	Firewalls					Name Servic
11	Unknown	TrafficAudit	FortiGate	Firewalls		pass	app-ctrl	Network Service: DNS,	Name Servic
12	Unknown	TrafficAudit	FortiGate	Firewalls		close	forward		Database Ap
13	FORTINET	TrafficAudit	FortiGate	Firewalls		close	forward		Name Servic

Column Actions ×

Toplist Report

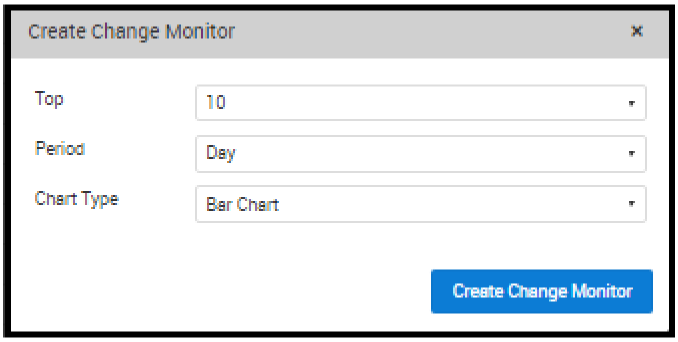
(Based on group by this column and count)

Create Toplist

Change Monitor

(Based on group by this column,date interval and count)

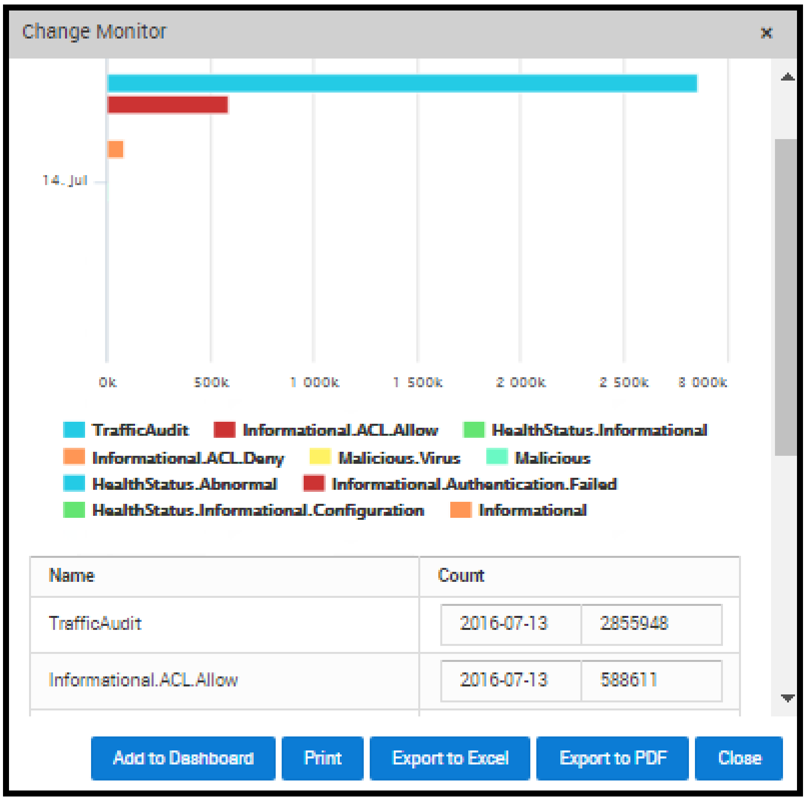
Create Report



Create Change Monitor ×

Top	10
Period	Day
Chart Type	Bar Chart

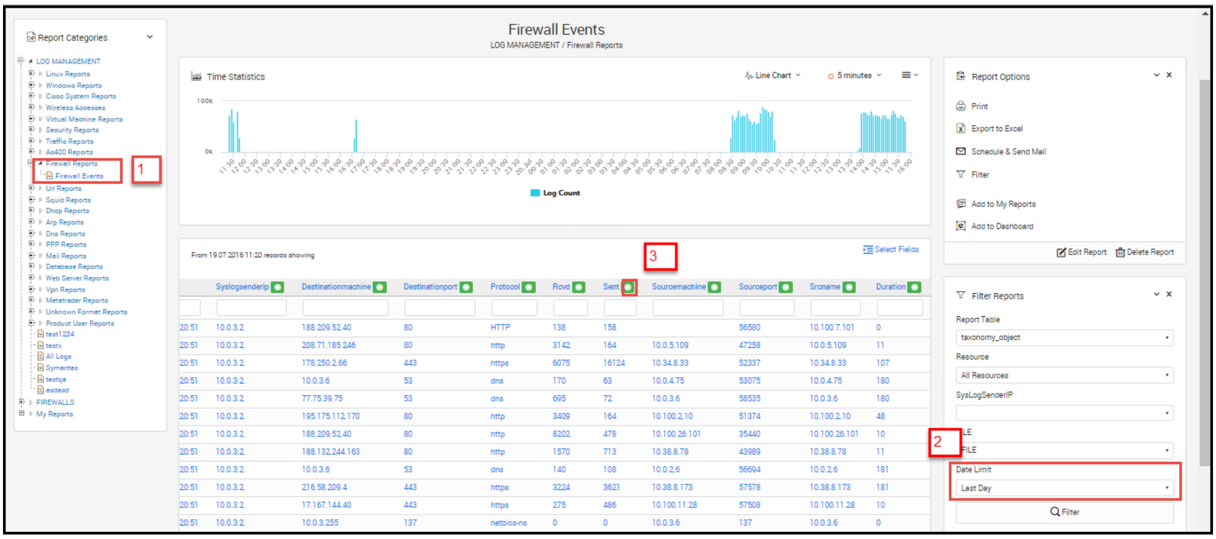
Create Change Monitor



Name	Count	
TrafficAudit	2016-07-13	2855948
Informational.ACL.Allow	2016-07-13	588611

You can send Change Monitor report by email, print it, save it, and export it to Excel and PDF.

Example Creating Last Day Toplist Sent Data(KB) Report according to sourcemachine and adding to dashboard

1. 

From 19.07.2016 11:20 records showing

	Syslogsenderip	Destinationmachine	Destinationport	Protocol	Rcvd	Sent	Sourcemachine	Sourceport	Srcname	Duration
20:51	10.0.3.2	188.209.52.40	80	HTTP	138	158		56580	10.100.7.101	0
20:51	10.0.3.2	208.71.185.246	80	http	3142	164	10.0.5.109	47258	10.0.5.109	11
20:51	10.0.3.2	178.250.2.66	443	https	6075	16124	10.34.8.33	52337	10.34.8.33	107
20:51	10.0.3.2	10.0.3.6	53	dns	170	63	10.0.4.75	53075	10.0.4.75	180
20:51	10.0.3.2	77.75.39.75	53	dns	695	72	10.0.3.6	58535	10.0.3.6	180
20:51	10.0.3.2	195.175.112.170	80	http	3409	164	10.100.2.10	51374	10.100.2.10	48
20:51	10.0.3.2	188.209.52.40	80	http	8202	478	10.100.26.101	35440	10.100.26.101	10
20:51	10.0.3.2	188.132.244.163	80	http	1570	713	10.38.8.78	43989	10.38.8.78	11
20:51	10.0.3.2	10.0.3.6	53	dns	140	108	10.0.2.6	56694	10.0.2.6	181
20:51	10.0.3.2	216.58.209.4	443	https	3224	3621	10.38.8.173	57578	10.38.8.173	181
20:51	10.0.3.2	17.167.144.40	443	https	275	486	10.100.11.28	57508	10.100.11.28	10
20:51	10.0.3.2	10.0.3.255	137	netbios-ns	0	0	10.0.3.6	137	10.0.3.6	0

Report Table: taxonomy_object

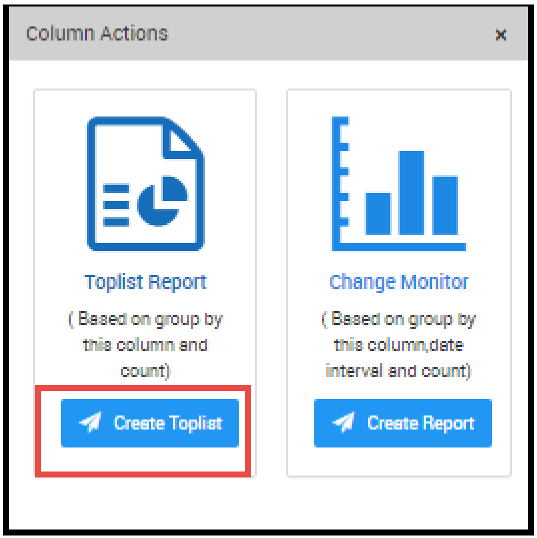
Resource: All Resources

SysLogSenderIP:

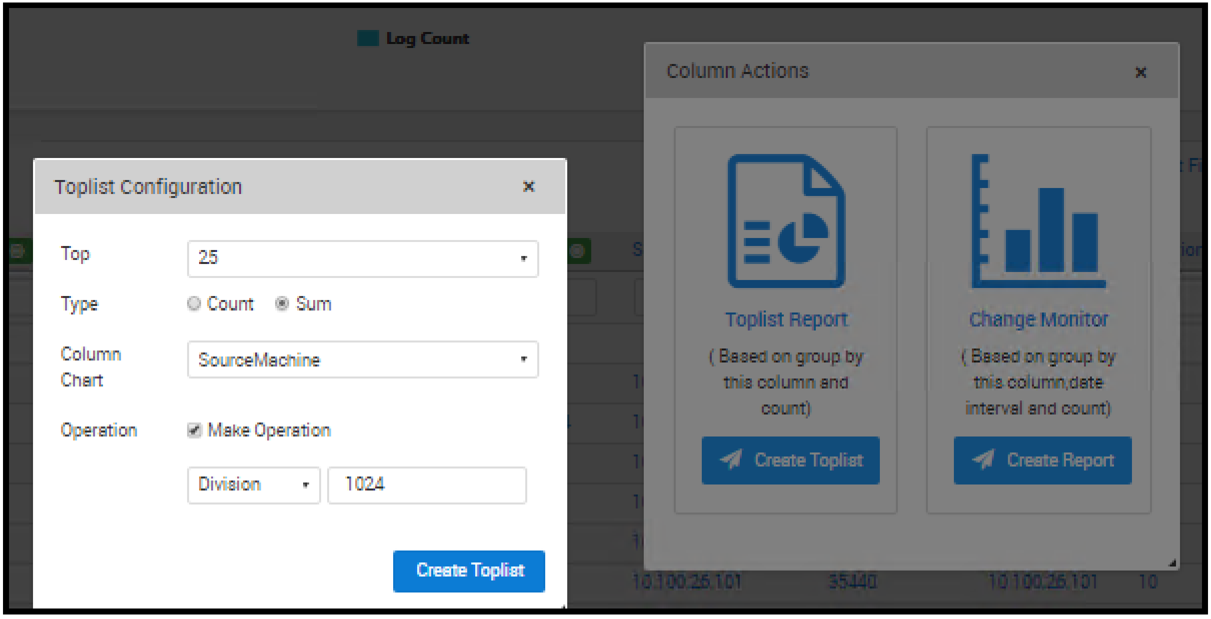
LE: FILE

Date Limit: Last Day

2.


Column Actions
×
Toplist Report
(Based on group by this column and count)
Create Toplist
Change Monitor
(Based on group by this column,date interval and count)
Create Report

3.



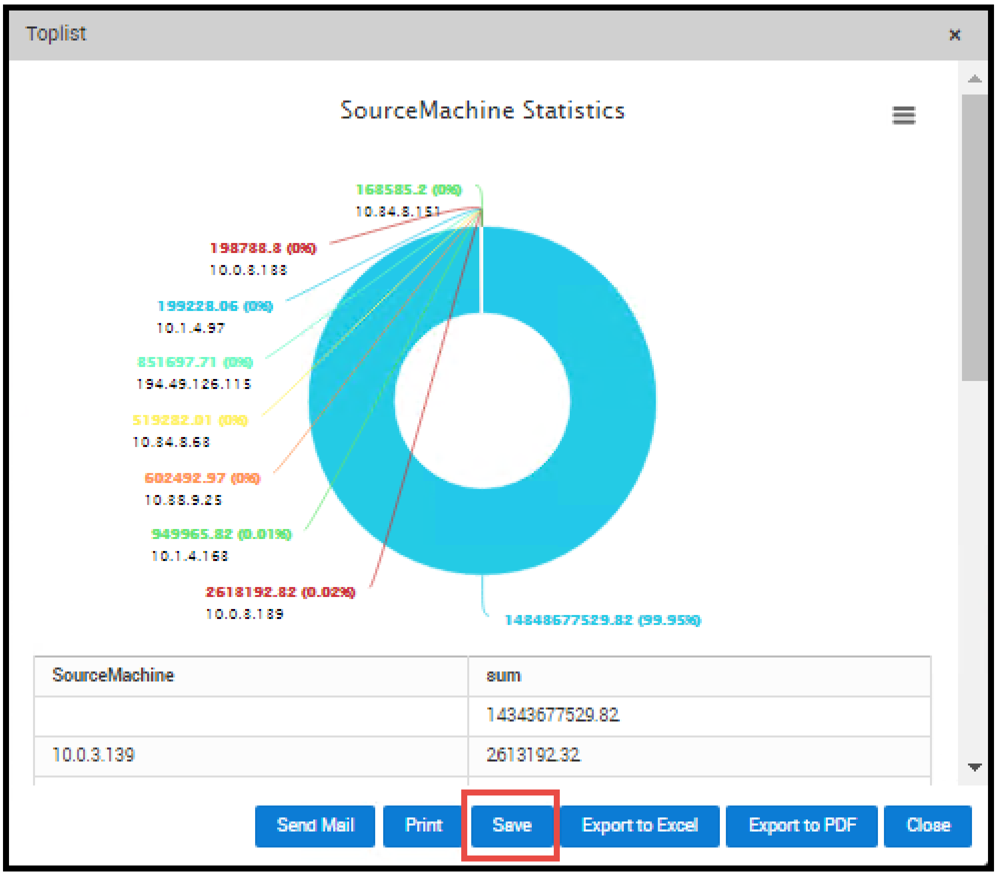
Top: 25

Type: ○ Count ● Sum

Column Chart: SourceMachine

Operation: ☑ Make Operation

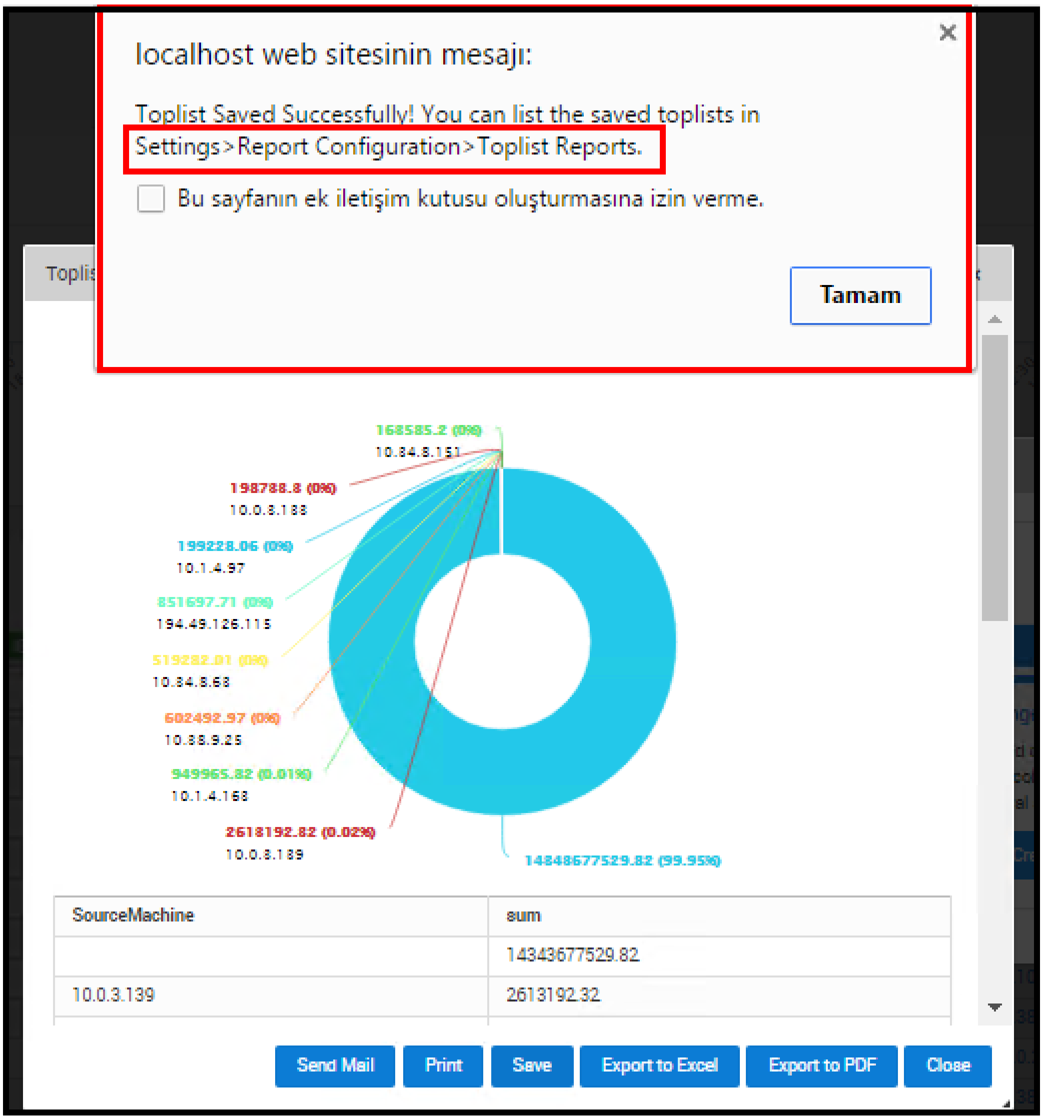
Division 1024



SourceMachine	sum
	14343677529.82
10.0.3.139	2613192.32

4.

5. You can find the report under Settings→Report→Configuration→Toplist Reports



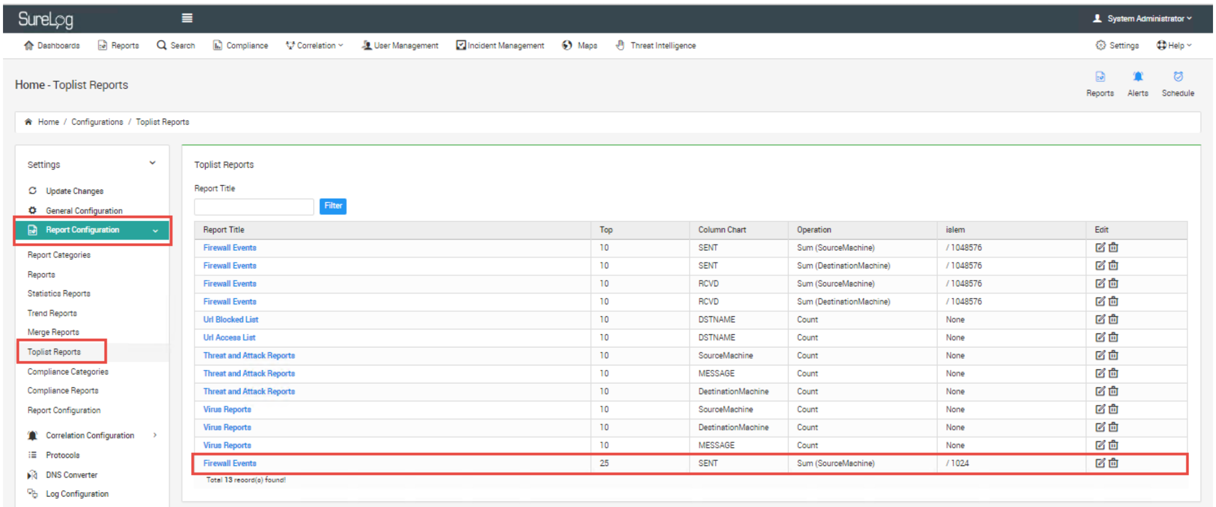
localhost web sitesinin mesajı:

Toplist Saved Successfully! You can list the saved toplists in Settings>Report Configuration>Toplist Reports.

□ Bu sayfanın ek iletişim kutusu oluşturmasına izin verme.

SourceMachine	sum
	14343677529.82
10.0.3.139	2613192.32

6.



Home - Toplist Reports

Home / Configurations / Toplist Reports

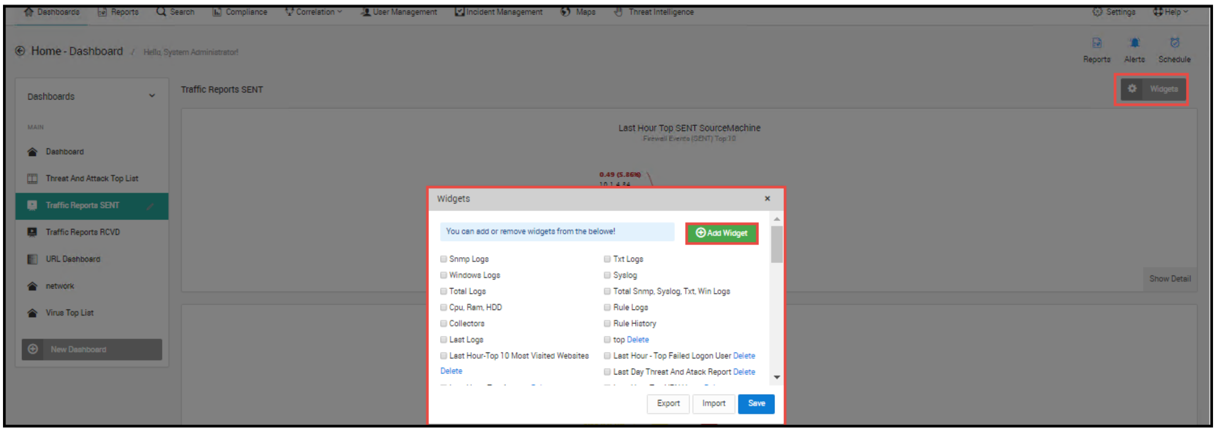
Toplist Reports

Report Title

Report Title	Top	Column Chart	Operation	islem	Edit
Firewall Events	10	SENT	Sum (SourceMachine)	/ 1048576	
Firewall Events	10	SENT	Sum (DestinationMachine)	/ 1048576	
Firewall Events	10	RCVD	Sum (SourceMachine)	/ 1048576	
Firewall Events	10	RCVD	Sum (DestinationMachine)	/ 1048576	
Url Blocked List	10	DSTNAME	Count	None	
Url Access List	10	DSTNAME	Count	None	
Threat and Attack Reports	10	SourceMachine	Count	None	
Threat and Attack Reports	10	MESSAGE	Count	None	
Threat and Attack Reports	10	DestinationMachine	Count	None	
Virus Reports	10	SourceMachine	Count	None	
Virus Reports	10	DestinationMachine	Count	None	
Virus Reports	10	MESSAGE	Count	None	
Firewall Events	25	SENT	Sum (SourceMachine)	/ 1024	

Total 13 record(s) found!

7. Adding this report to dashboard



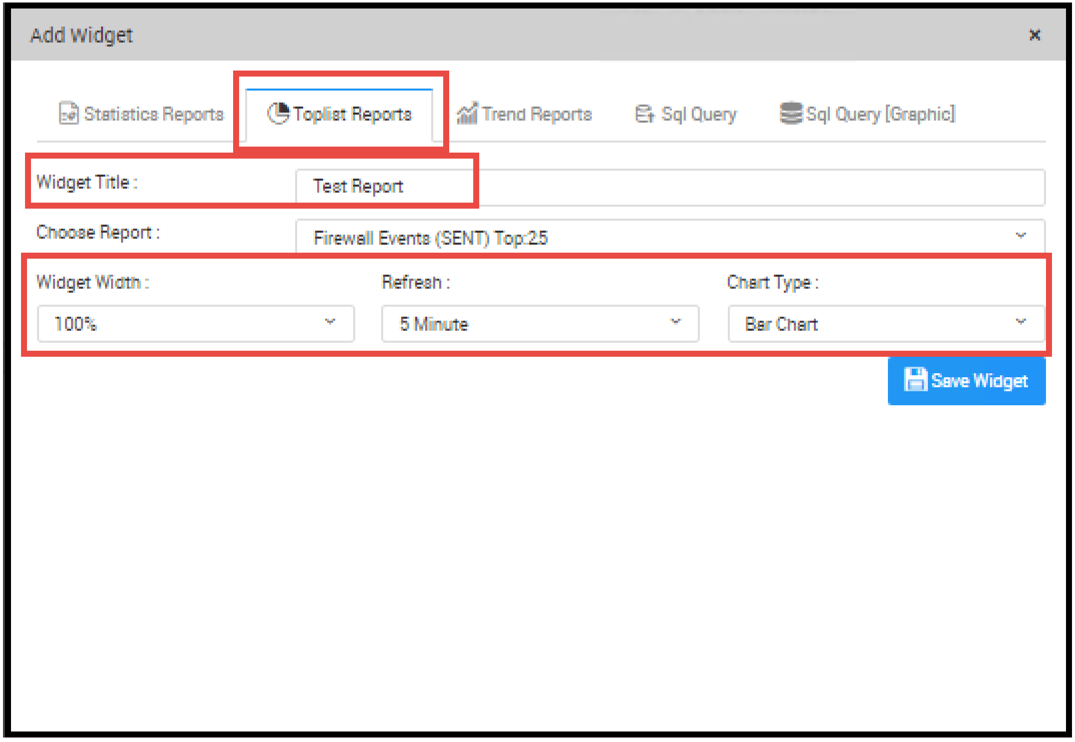
Widgets

You can add or remove widgets from the belowe!

Add Widget

- □ Snmp Logs
- □ Windows Logs
- □ Total Logs
- □ Cpu, Ram, HDD
- □ Collectors
- □ Last Logs
- □ Last Hour-Top 10 Most Visited Websites Delete
- □ Txt Logs
- □ Syslog
- □ Total Snmp, Syslog, Txt, Win Logs
- □ Rule Logs
- □ Rule History
- □ top Delete
- □ Last Hour - Top Failed Logon User Delete
- □ Last Day Threat And Atack Report Delete

Export Import Save

8. 

Add Widget

Widget Title : Test Report

Choose Report : Firewall Events (SENT) Top:25

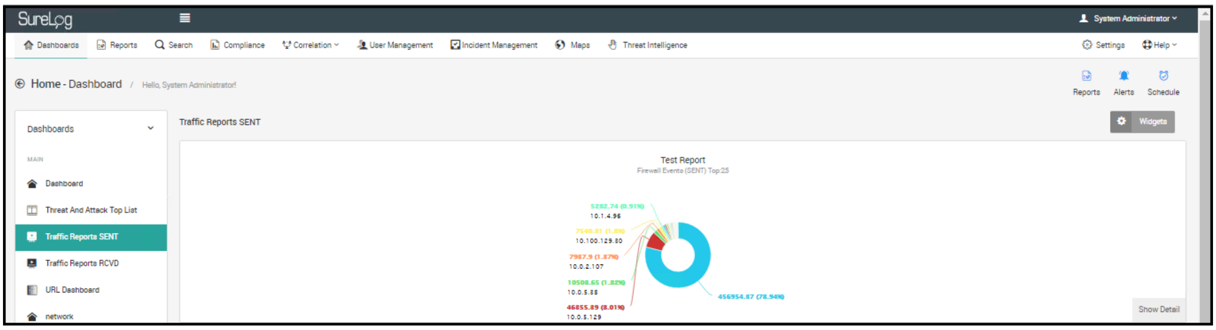
Widget Width : 100%

Refresh : 5 Minute

Chart Type : Bar Chart

Save Widget

Report is shown below



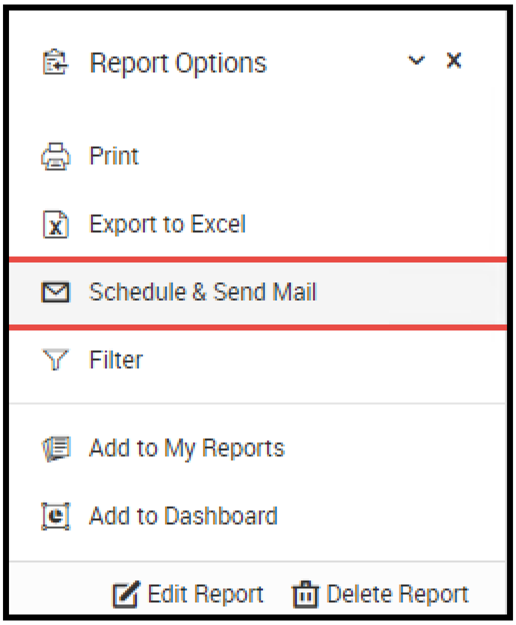
You can add several report like this

Schedule Reports

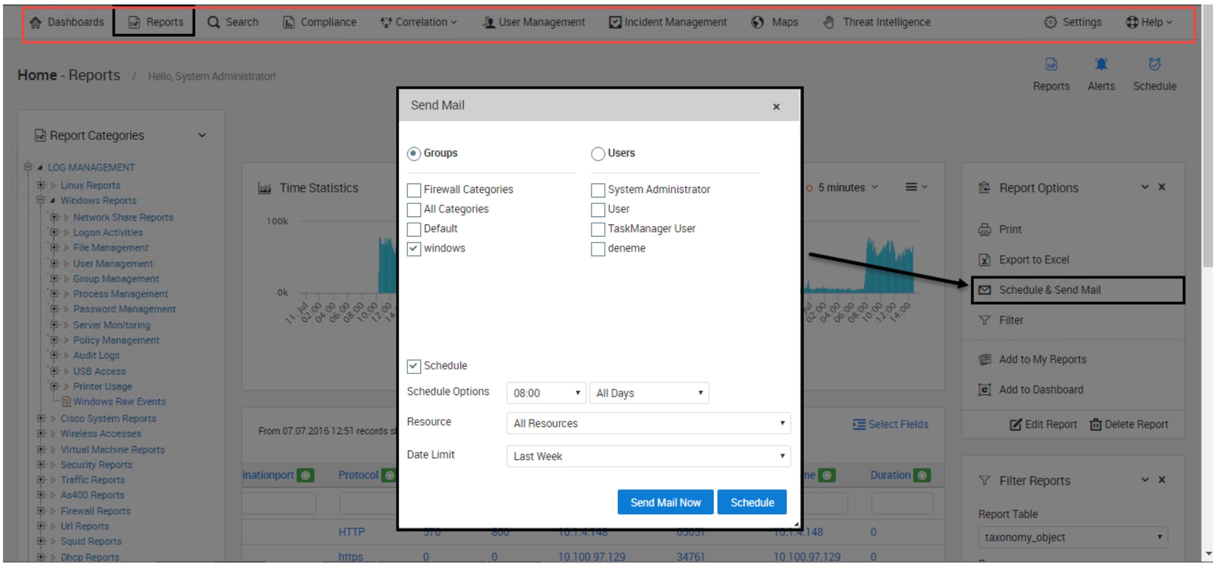
SureLog generates many reports that help analyze the security and performance over a period of time. Using this option, a user can schedule the time at which the reports need to be generated.

Steps for scheduling reports:

1. On the Report pane, select the Schedule button



1. Select Schedule button.
2. Select users (Groups or Users)
3. Select Schedule option
4. Select Schedule period



Send Mail

● Groups ○ Users

Groups	Users
□ Firewall Categories	□ System Administrator
□ All Categories	□ User
□ Default	□ TaskManager User
☑ windows	□ deneme

☑ Schedule

Schedule Options: 08:00 ▾ All Days ▾

Resource: All Resources ▾

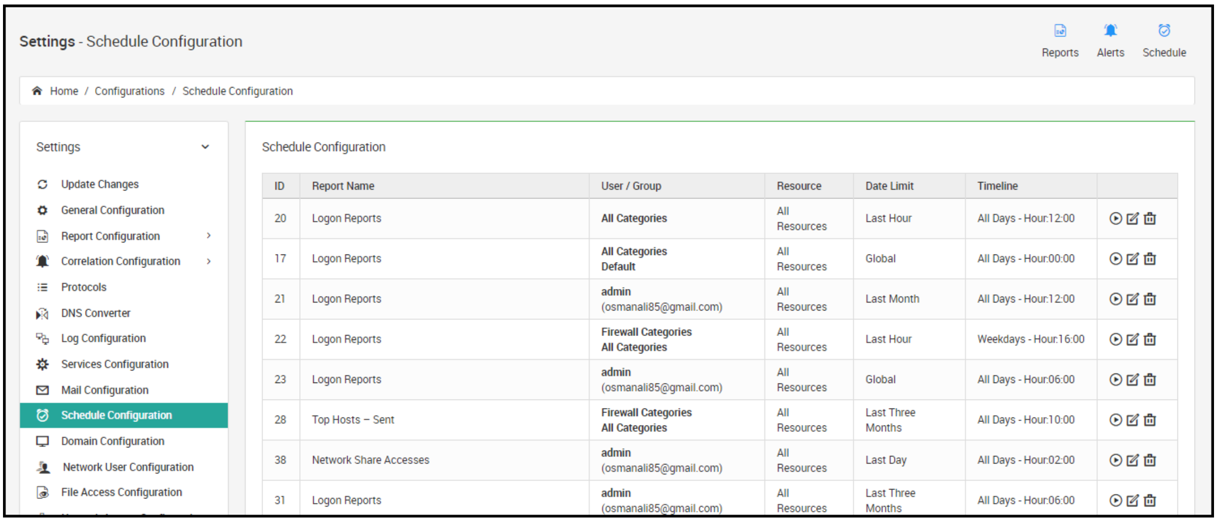
Date Limit: Last Week ▾

Send Mail Now | Schedule

5. Click Schedule button to schedule the report.

Steps for configuring scheduled reports

1. Select Settings, then Schedule Configuration



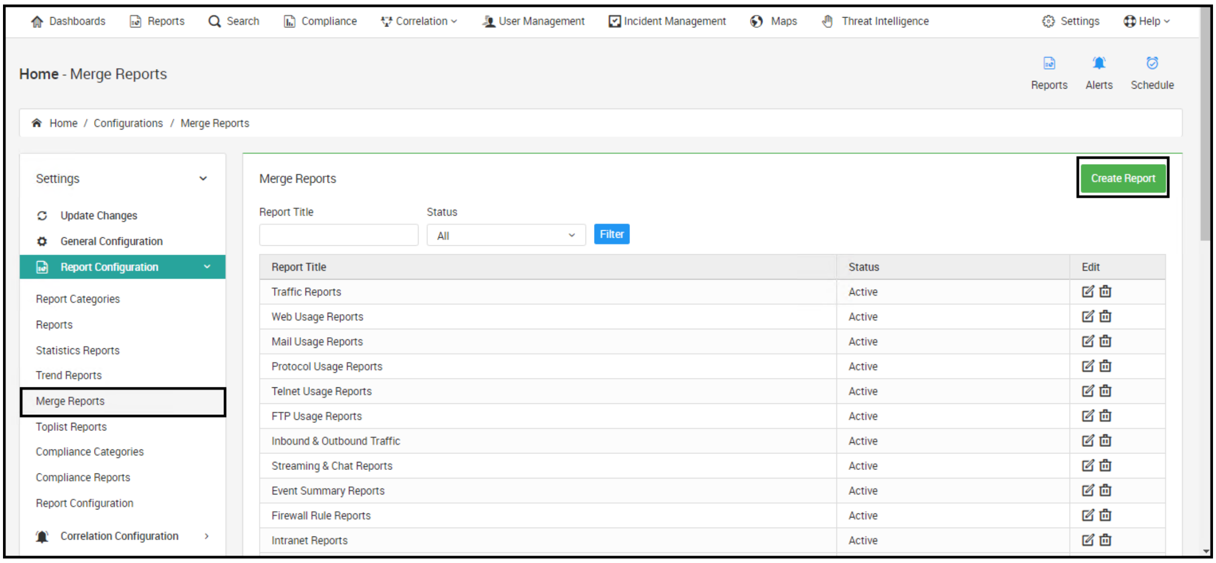
ID	Report Name	User / Group	Resource	Date Limit	Timeline	
20	Logon Reports	**All Categories**	All Resources	Last Hour	All Days - Hour:12:00	▶ ✎ 🗑
17	Logon Reports	**All Categories** **Default**	All Resources	Global	All Days - Hour:00:00	▶ ✎ 🗑
21	Logon Reports	**admin** (osmanali85@gmail.com)	All Resources	Last Month	All Days - Hour:12:00	▶ ✎ 🗑
22	Logon Reports	**Firewall Categories** **All Categories**	All Resources	Last Hour	Weekdays - Hour:16:00	▶ ✎ 🗑
23	Logon Reports	**admin** (osmanali85@gmail.com)	All Resources	Global	All Days - Hour:06:00	▶ ✎ 🗑
28	Top Hosts – Sent	**Firewall Categories** **All Categories**	All Resources	Last Three Months	All Days - Hour:10:00	▶ ✎ 🗑
38	Network Share Accesses	**admin** (osmanali85@gmail.com)	All Resources	Last Day	All Days - Hour:02:00	▶ ✎ 🗑
31	Logon Reports	**admin** (osmanali85@gmail.com)	All Resources	Last Three Months	All Days - Hour:06:00	▶ ✎ 🗑

The users can also send scheduled reports by email with **Send Mail Now** Button.

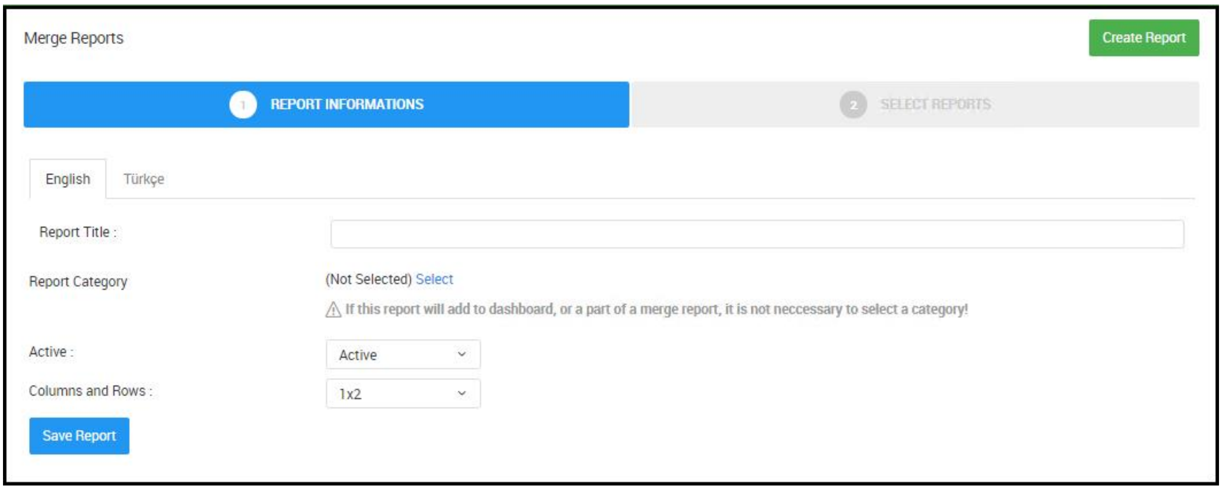
Combining Reports

Multiple reports can be combined into a single report by:

1. Select Settings
2. Select Report Configuration
3. Select Merge Reports
4. Select Create Report



Report Title	Status	Edit
Traffic Reports	Active	✎ 🗑
Web Usage Reports	Active	✎ 🗑
Mail Usage Reports	Active	✎ 🗑
Protocol Usage Reports	Active	✎ 🗑
Telnet Usage Reports	Active	✎ 🗑
FTP Usage Reports	Active	✎ 🗑
Inbound & Outbound Traffic	Active	✎ 🗑
Streaming & Chat Reports	Active	✎ 🗑
Event Summary Reports	Active	✎ 🗑
Firewall Rule Reports	Active	✎ 🗑
Intranet Reports	Active	✎ 🗑



Merge Reports

Report Title :

Report Category: (Not Selected) Select

⚠ If this report will add to dashboard, or a part of a merge report, it is not neccessary to select a category!

Active : Active

Columns and Rows : 1x2

5. Enter data into the following fields:

Report Title: Title of the new report

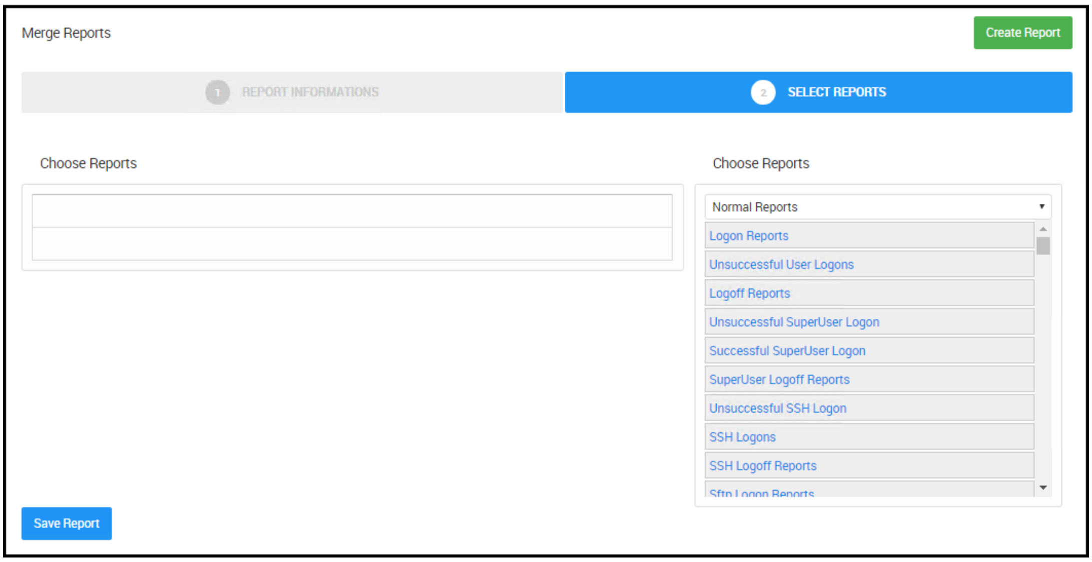
Report Category: The category to which this report will belong to

Active: Status

Columns and Rows : Number of rows and columns desired for this new report

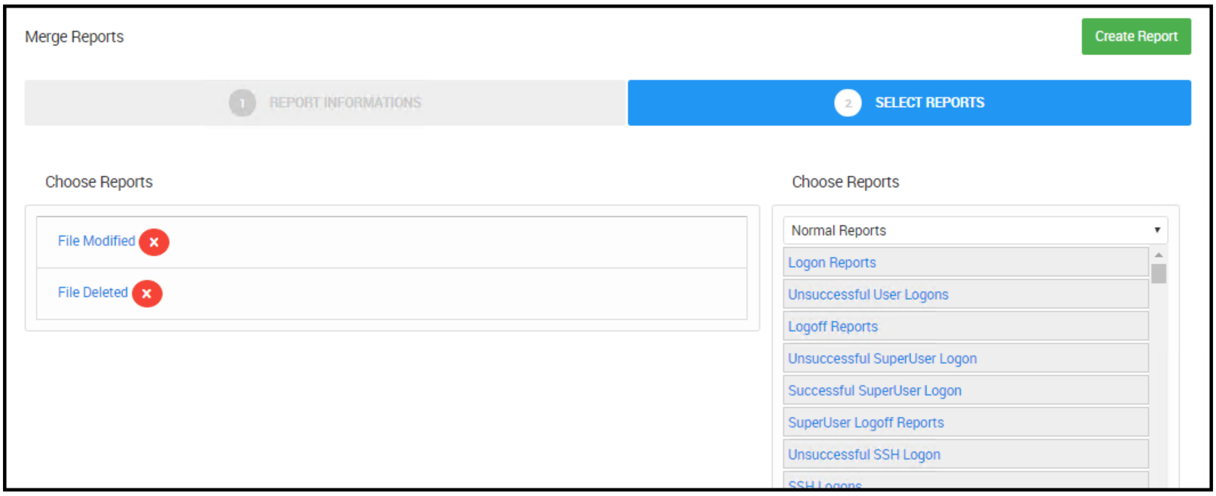
6. Select Save Report

7. A new frame for creating merged reports will be shown



Merge Reports

8. Select an available report from the list using the drag and drop selection method by dragging the desired report and drop pingit into the desired cell



Merge Reports

Create Report

1 REPORT INFORMATIONS

2 SELECT REPORTS

Choose Reports

- File Modified ×
- File Deleted ×

Choose Reports

Normal Reports ▾

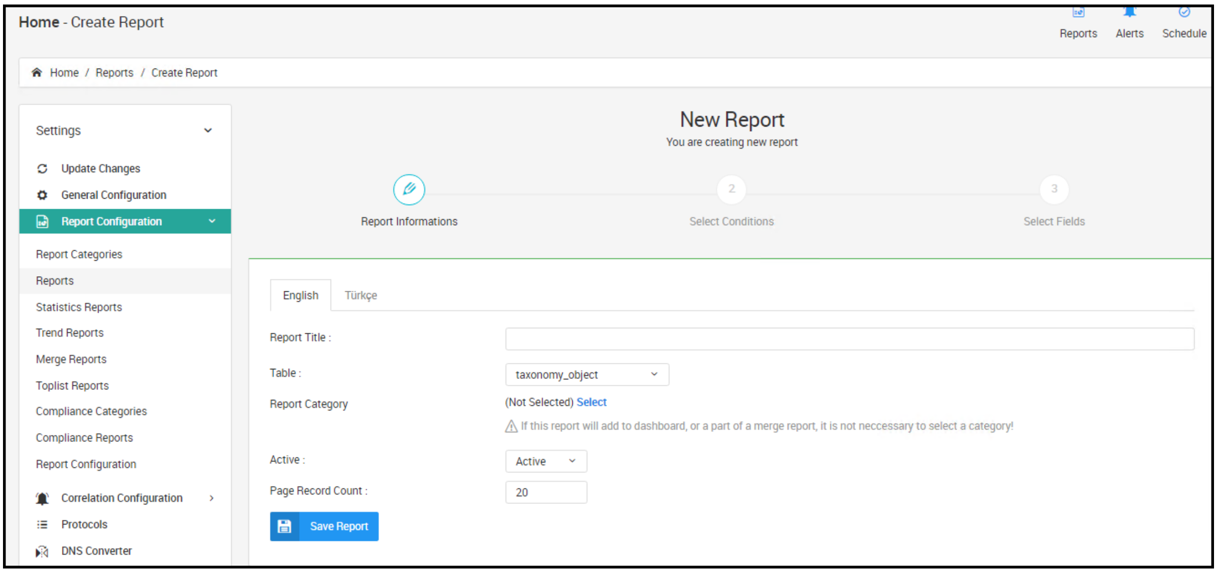
- Logon Reports
- Unsuccessful User Logons
- Logoff Reports
- Unsuccessful SuperUser Logon
- Successful SuperUser Logon
- SuperUser Logoff Reports
- Unsuccessful SSH Logon
- SSH Logons

9. Select the Save Report button available at the end of the page

Creating Reports

Steps for creating reports

1. Select Settings
2. Select Report Configuration
3. Select Reports
4. Select Create Report



Home - Create Report

Home / Reports / Create Report

New Report

You are creating new report

Report Title :

Table : taxonomy_object

Report Category (Not Selected) Select

⚠ If this report will add to dashboard, or a part of a merge report, it is not neccessary to select a category!

Active : Active

Page Record Count : 20

Save Report

5. Enter data into the following fields:

Report Title: Title of the new report

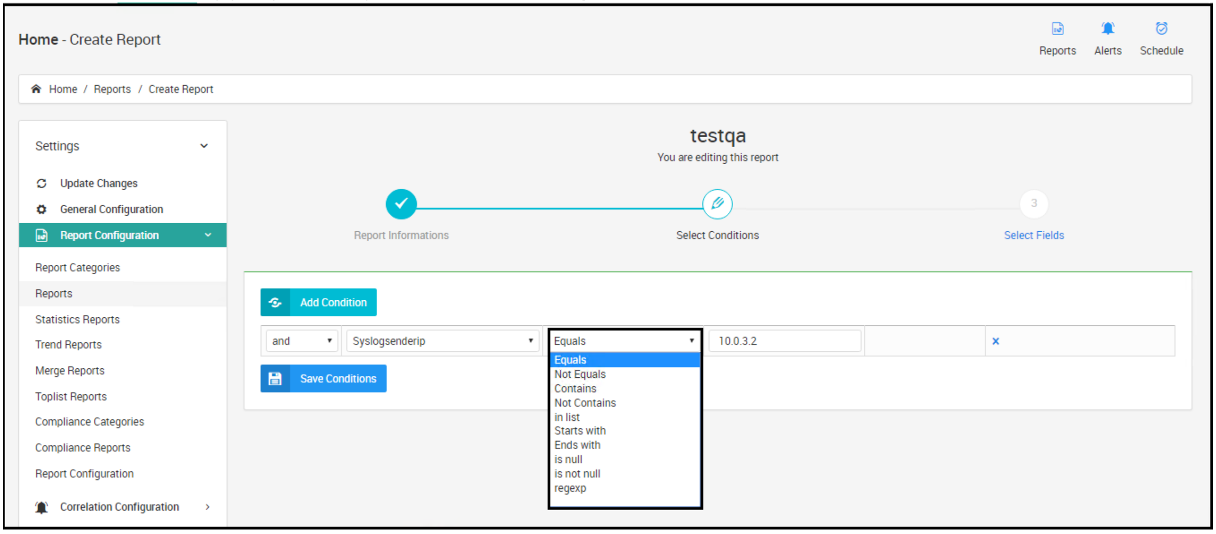
Report Category: The category to which this report will belong to

Report Table: Logs from which this new report will be created

Active: To be visible or not

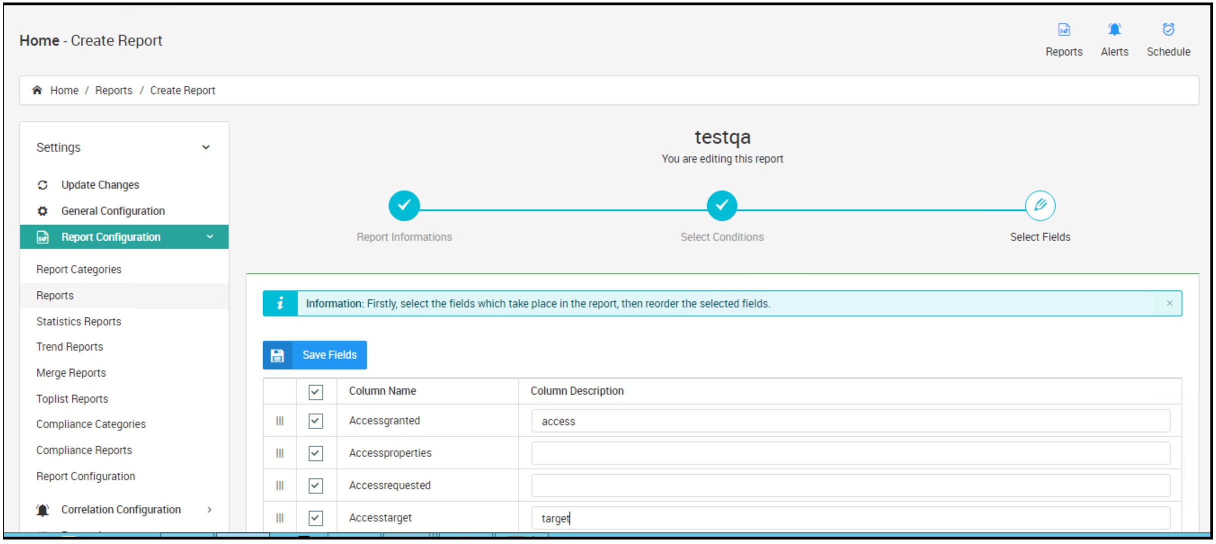
Record Count Per Row: Select the report table row size

6. Select Save Report
7. Select fields and appropriate operator to filter logs



and | Syslogsenderip | Equals | 10.0.3.2

8. Select Save Reports
9. Select appropriate fields to be shown on the screen
10. Enter a name for each column in the Columns Description field



Information: Firstly, select the fields which take place in the report, then reorder the selected fields.

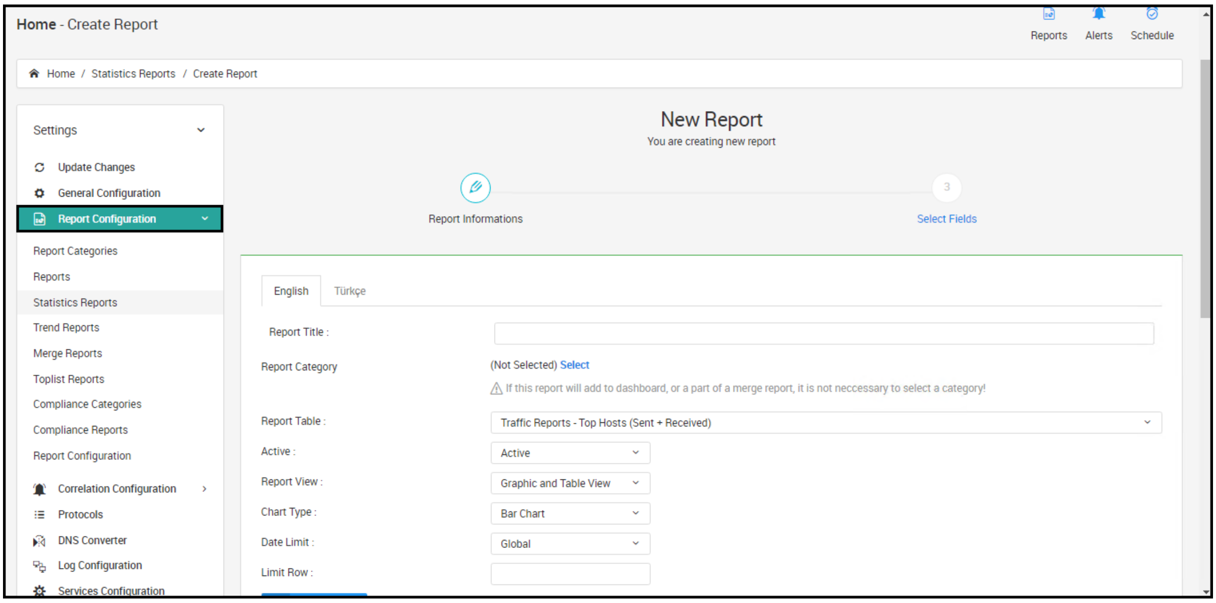
	☑	Column Name	Column Description
‖	☑	Accessgranted	access
‖	☑	Accessproperties	
‖	☑	Accessrequested	
‖	☑	Accesstarget	target

11. Select Save Reports

Creating Statistics Reports

Steps for Creating Statistics Reports

1. Select Settings
2. Select Report Configuration
3. Select Statistics Reports
4. Select Create Report



Home - Create Report

Reports Alerts Schedule

Home / Statistics Reports / Create Report

Settings

- Update Changes
- General Configuration
- Report Configuration
- Report Categories
- Reports
- Statistics Reports
- Trend Reports
- Merge Reports
- Toplist Reports
- Compliance Categories
- Compliance Reports
- Report Configuration
- Correlation Configuration
- Protocols
- DNS Converter
- Log Configuration
- Services Configuration

New Report

You are creating new report

Report Informations — 3 Select Fields

English | Türkçe

Report Title :

Report Category: (Not Selected) Select

⚠ If this report will add to dashboard, or a part of a merge report, it is not neccessary to select a category!

Report Table : Traffic Reports - Top Hosts (Sent + Received)

Active : Active

Report View : Graphic and Table View

Chart Type : Bar Chart

Date Limit : Global

Limit Row :

5. Enter data into the following fields:

Report Title: Title of the new report

Report Category: The category to which this report will belong to

Report Table: Select available statistics parameters from a list

Active: To be visible or not

Report View: Select between graphic and/or table view

Chart Type: Select chart types such as bar chart, line chart, area chart, and column chart

Add to Dashboard: Select this field to display the data on the Dashboard

Trend Report: By selecting this option, data will be grouped by TIME which produces trend reports.

Date Limit: Select a time frame. If the user selects global time, the system will be adjusted to the system global time, which is configured within the reports module. Other options include:

- Last Hour
- Last Day
- Last Week
- Last Month
- Last Three Months
- Last Six Months
- Last Year

Limit Row: Data limit and Row Number

8. Click the Save Report Button

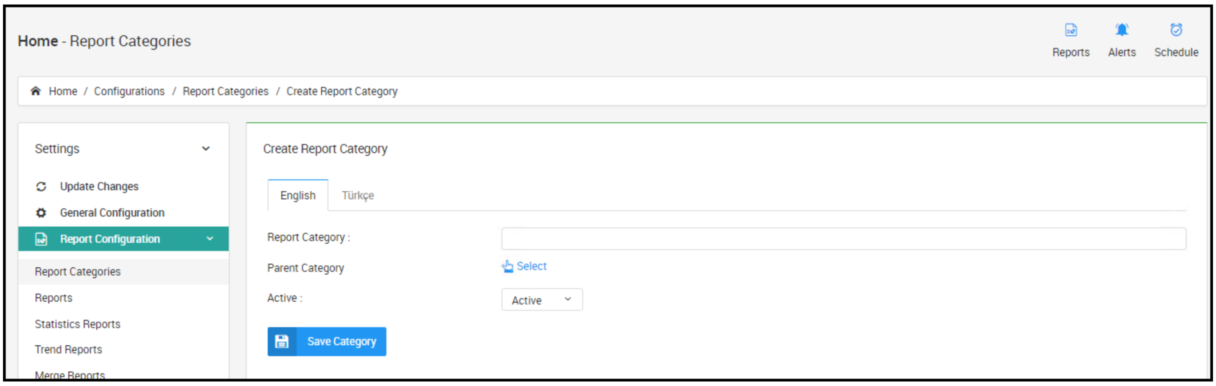
9. The Select Fields form will be shown on the screen. Select the desired fields to display on the dashboard or reports. If uncertain, select all the fields.

Creating Report Categories

Report categories are used to group related reports (both log management and statistic data).

Steps for Creating Report Categories

1. Select Settings
2. Select Report Configuration
3. Select Report Categories
4. Select Add Category
5. Add Report Category



6. Enter data into the following fields:

Report Category: Name of the new category

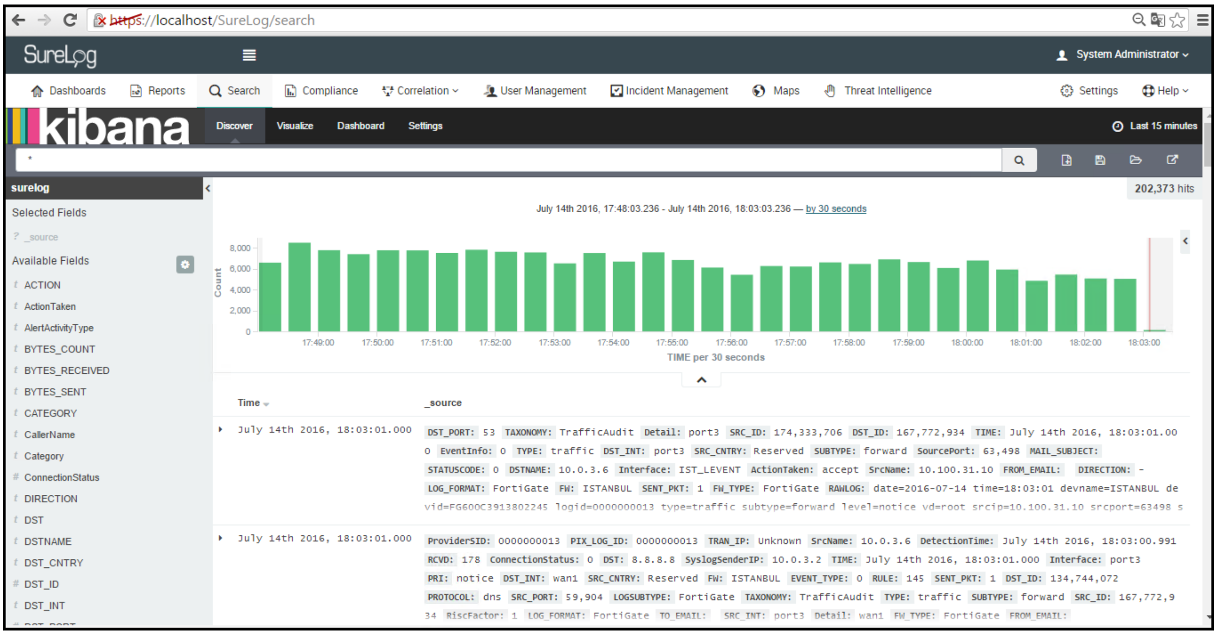
Parent Category: Used to create a category under another available category, otherwise select a Main Category

Active: To be visible or not

Chapter 7: Search

Google like Search

You can interactively explore your data from search page. You have access to every document in every index that matches the selected index pattern. You can submit search queries, filter the search results, and view document data. You can also see the number of documents that match the search query and get field value statistics. If a time field is configured for the selected index pattern, the distribution of documents over time is displayed in a histogram at the top of the page.



```
July 14th 2016, 18:03:01.000   DST_PORT: 53 TAXONOMY: TrafficAudit Detail: port3 SRC_ID: 174,333,706 DST_ID: 167,772,934 TIME: July 14th 2016, 18:03:01.00
                               0 EventInfo: 0 TYPE: traffic DST_INT: port3 SRC_CNTRY: Reserved SUBTYPE: forward SourcePort: 63,498 MAIL_SUBJECT:
                               STATUSCODE: 0 DSTNAME: 10.0.3.6 Interface: IST_LEVENT ActionTaken: accept SrcName: 10.100.31.10 FROM_EMAIL:  DIRECTION: -
                               LOG_FORMAT: FortiGate FW: ISTANBUL SENT_PKT: 1 FW_TYPE: FortiGate RAWLOG: date=2016-07-14 time=18:03:01 devname=ISTANBUL de
                               vid=FG600C3913802245 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=10.100.31.10 srcport=63498 s

July 14th 2016, 18:03:01.000   ProviderSID: 0000000013 PIX_LOG_ID: 0000000013 TRAN_IP: Unknown SrcName: 10.0.3.6 DetectionTime: July 14th 2016, 18:03:00.991
                               RCVD: 178 ConnectionStatus: 0 DST: 8.8.8.8 SyslogSenderIP: 10.0.3.2 TIME: July 14th 2016, 18:03:01.000 Interface: port3
                               PRI: notice DST_INT: wan1 SRC_CNTRY: Reserved FW: ISTANBUL EVENT_TYPE: 0 RULE: 145 SENT_PKT: 1 DST_ID: 134,744,072
                               PROTOCOL: dns SRC_PORT: 59,904 LOGSUBTYPE: FortiGate TAXONOMY: TrafficAudit TYPE: traffic SUBTYPE: forward SRC_ID: 167,772,9
                               34 RiscFactor: 1 LOG_FORMAT: FortiGate TO_EMAIL:  SRC_INT: port3 Detail: wan1 FW_TYPE: FortiGate FROM_EMAIL:
```

You can search the indices that match the current index pattern by submitting a search from the Discover page. You can enter simple query strings, use the Lucene query syntax, or use the full JSON-basedElasticsearch Query DSL.

When you submit a search, the histogram, Documents table, and Fields list are updated to reflect the search results. The total number of hits (matching documents) is shown in the upper right corner of the histogram. The Documents table shows the first five hundred hits. By default, the hits are listed in reverse chronological order, with the newest documents shown first. You can reverse the sort order by by clicking on the Time column header. You can also sort the table using the values in any indexed field.

To search your data:

1. Enter a query string in the Search field:

- To perform a free text search, simply enter a text string. For example, if you're searching web server logs, you could enter safari to search all fields for the term safari.
- To search for a value in a specific field, you prefix the value with the name of the field. For example, you could enter status:200 to limit the results to entries that contain the value 200in the status field.
- To search for a range of values, you can use the bracketed range syntax, [START_VALUE TO END_VALUE]. For example, to find entries that have 4xx status codes, you could enter status:[400 TO 499].
- To specify more complex search criteria, you can use the Boolean operators AND, OR, and NOT. For example, to find entries that have 4xx status codes and have an extension of php or html, you could enter status:[400 TO 499] AND (extension:php OR extension:html).

NOTE

These examples use the Lucene query syntax. You can also submit queries using the Elasticsearch Query DSL. For examples, see query string syntax in the Elasticsearch Reference.

2. Press **Enter** or click the **Search** button to submit your search query.

Structured Search

The Search tab offers numerous options for making data searches more precise and efficient in regards to the Aggregated Logs Database.

In Advanced Search, the user can search logs for selected devices from the aggregated logs database, in addition to defining matching criteria.

Sample search criteria for the Aggregated Logs Database include: Protocol, Source, Destination, User, Virus, Attack, URL, Rule, Category, sender mail address, logon type, etc.

In general, sample Log search criteria can be the following:

Criteria	**Description**
Protocol	Refers to the list of protocols and protocol identifiers that are available in the Protocol Groups page (Settings >> Protocol Groups) *example: 8554/tcp, rtsp, IPSec*
Source	Refers to the source host name or IP address (also in CIDR format) from which requests originated
Destination	Refers to the destination host name or IP address (also in CIDR format) to which requests were sent
User	Refers to the authenticated user name required by some firewalls *example: John, Kate*
Virus	Refers to the virus name. *examples: JS/Exception, W32/Mitglieder*
Attack	Refers to the attack name. *examples: UDP Snort, IP Spoof*
Severity	Refers to the event severity
URL	Refers to the URL desired to search
Status	Refers to the event status
Rule	Refers to the Firewall Rule desired to search
VPN	Refers to the VPN details
Duration	Refers to the duration reference in the log
Bytes	Refers to the bytes transferred information in the log
Category	Refers to the log category
Device	Refers to the device from which logs are collected
Message	Refers to the log message texts stored in the database (DB)

VPN Group	Refers to the VPN group details

- If the search string exists, then the search result will be intelligently displayed based on the report category in which it occurred.
- By default, the search is carried out for the time period selected in the Global Calendar present .

Chapter 8: Correlation

Why Use Correlation?

Correlation allows users to:

- Reduce the mass of information to monitor
- Compensate for inconsistency among security device-generated messages
- Automate the response after receiving a message
- Enhance the quality of the diagnosis

To Reduce the Amount of Information to Monitor

Security administrators and analysts are facing a mass load of information coming from numerous security devices. This quantity of information cannot be easily monitored, therefore a grouping method must be applied to the various messages. Correlation rules allow for this type of bundling.

To Automate the Response after Receiving a Message

Once correlation has been performed and according to the configuration of the correlation rule, an immediate action can take place such as the:

- Automatic creation of an alert
- Modification of the event's severity
- Sending of an alert or event from one SMP to another in a multi-instance environment
- Mailing of the event to contacts
- Automatic creation of an incident from the alert
- Creation of a scenario based on rules

To Enhance the Quality of the Diagnosis

By using the Asset Database, the correlation process can meet a user's business security demand. Once a user's business environment has been correctly configured in SureLog (vulnerabilities, list of computers, etc.) and with the help of the events generated by vulnerability scanners, a user can obtain an alert with information about the installed base. Therefore, an alert linked with a critical server from the asset database will be considered more important than an alert about a less sensitive server. Its severity will be modified and the alert will be processed by priority. The information contained in the asset database will also be taken into account to fill the alerts' messages such as the IP address of a workstation.

To Compensate for the Lack of Consistency among Security Device-Generated Messages

Messages generated by equipment are very different. Through correlation and standardization, messages will be classified so that events with the same information will always have the same description.

For example, if a detected port scan occurs, the following happens:

- a Checkpoint firewall will generate a Port Scanning message
- a NetASQfirewall will generate a Possible port scan message
- a Snort detection probe will generate a Port Scan detected message

Therefore, all these events can be correlated into one alert, simply titled "Port Scan".

SureLog Correlation GUI

The Correlation view is used to create, configure, and manage a user's rules. Rules are used to monitor and respond to alert traffic. They permit for an automatic notification or response to security events in real-time, whether a user is monitoring the WEB Console or not. When an alert or a series of alerts meets a rule's conditions, the rule automatically takes action. This includes actions like notifying the appropriate users or performing a particular active response. A user can use the view's Rule Creation tool to create custom rules and variations to any existing rules.

The SureLog also comes equipped with a set of preconfigured rules that a user can begin using immediately. Moreover, a user can work with the view's Rule Creation tool to create custom rules and variations on any existing rules.

In addition, SureLog allows users to work with preconfigured template rules or create rules using a wizard. For those users with java knowledge, SureLog allows code development.

SureLog Advanced Correlation Engine

A correlation engine is a software application that programmatically understands relationships. Correlation engines are used in systems 'security tools to aggregate, normalize, and analyze event log data using predictive analytics and "fuzzy" logic to alert the system administrator when there is a problem or risk.

Sample Correlation Rules

The following are sample correlation rules supported by SureLog"

User Authentication

- Alert on 5 or more failed logins in 1 minute on a single user ID

Attacks on the Network

- Alert on 15 or more Firewall Drop/Reject/Deny Events from a single IP Address in one minute
- Alert on 3 or more IPS Alerts from a single IP Address in five minutes

Virus Detection/Removal

- Alert when a single host sees an identifiable piece of malware
- Alert when a single host fails to clean malware within 1 hour of detection
- Alert when a single host connects to 50 or more unique targets in 1 minute
- Alert when 5 or more hosts on the same subnet trigger the same Malware Signature (AV or IPS) within a 1 hour interval

Web Server

- Files with executable extensions (cgi, asp, aspx, jar, php, exe, com, cmd, sh, bat) are posted to a web server from an external source

Black-listed applications

- Alert when an unauthorized application (e.g. TeamViewer, LogmeIn, Nmap, Nessus, etc.) is run on any host

Monitored Log Sources

- Alert when a monitored log source has not sent an event in 1 Hour

User Activity Reports

- All Active User Accounts (any successful login grouped by account name in the past XX days)
- Active User List by Authentication type
    a) VPN Users
    b) Active Directory Users
    c) Infrastructure Device Access (Firewalls, Routers, Switches, IPS)
- User Creation, Deletion, and Modification (A list of all user accounts created, deleted, or modified)
- Access by any Default Account – (Guest, Root, Administrator, or other default account usage)
- Password resets by admin accounts in the past 7 days.

Access Reports

- Access to any protected/monitored device by an untrusted network
    a) VPN Access to Server Zone
    b) Access by a Foreign Network to Server Zone

Malware

- A list of host addresses for any identified malware or attack - grouped by malware name
- A count of any given malware (grouped by Anti-Virus Signature) over the past XX days

Email activity

- Top 10 email subjects
- Top 10 addresses to send email
- Top 10 addresses to receive email
- Top 10 addresses to send email with the largest total size (MB)
- Top 10 addresses to receive email with the largest total size (MB)

Web Content

- Top 10 destinations by domain name
- Top 10 blocked destinations by domain name
- Top 10 blocked sources by IP address
- Top 10 blocked categories
- Total sent and received bytes grouped by IP addresses

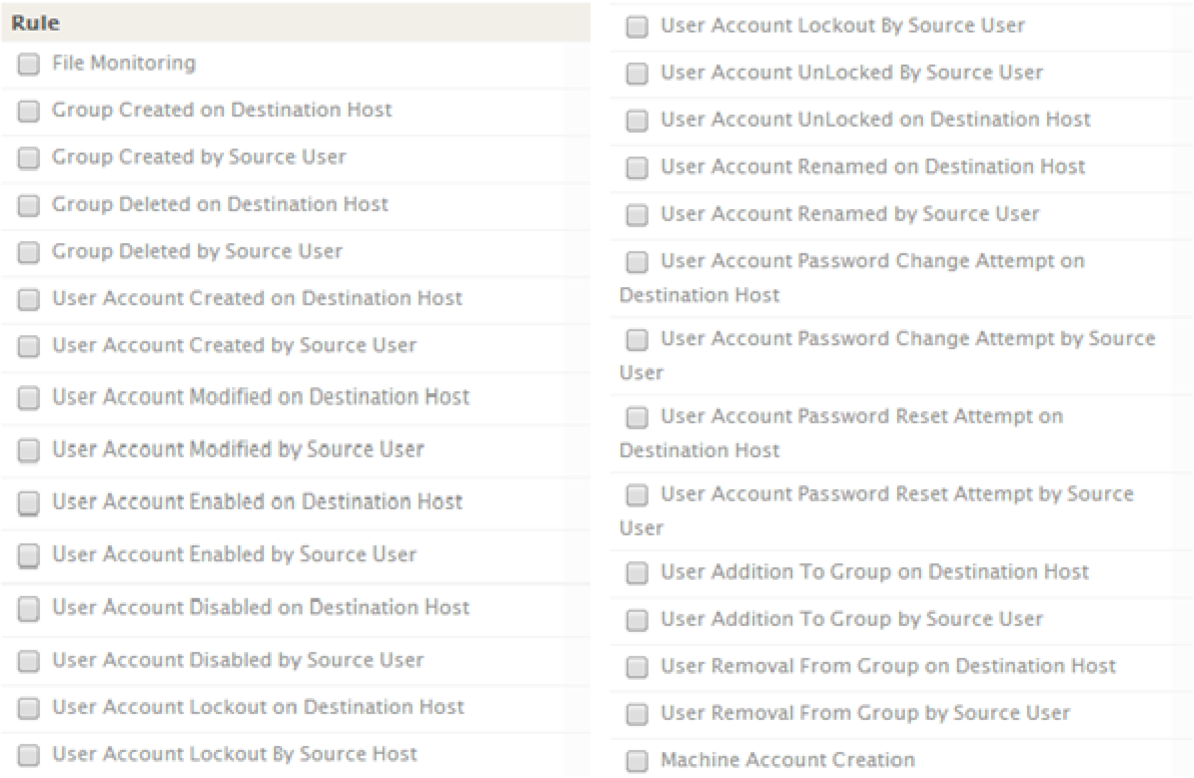
User Account activity

- Top 10 failed logins

Out-of-the-Box Correlation Rules

SureLog provides more than 450 pre-defined rules on various categories such as Group Management, User Management, Machine Management, Authentication, Windows Firewall rules, Authorization, Audit Policy, and Software Management.

The SureLog Correlation engine is different and very powerful while containing simple rules such as:



Rule

☐ File Monitoring

☐ Group Created on Destination Host

☐ Group Created by Source User

☐ Group Deleted on Destination Host

☐ Group Deleted by Source User

☐ User Account Created on Destination Host

☐ User Account Created by Source User

☐ User Account Modified on Destination Host

☐ User Account Modified by Source User

☐ User Account Enabled on Destination Host

☐ User Account Enabled by Source User

☐ User Account Disabled on Destination Host

☐ User Account Disabled by Source User

☐ User Account Lockout on Destination Host

☐ User Account Lockout By Source Host

☐ User Account Lockout By Source User

☐ User Account UnLocked By Source User

☐ User Account UnLocked on Destination Host

☐ User Account Renamed on Destination Host

☐ User Account Renamed by Source User

☐ User Account Password Change Attempt on Destination Host

☐ User Account Password Change Attempt by Source User

☐ User Account Password Reset Attempt on Destination Host

☐ User Account Password Reset Attempt by Source User

☐ User Addition To Group on Destination Host

☐ User Addition To Group by Source User

☐ User Removal From Group on Destination Host

☐ User Removal From Group by Source User

☐ Machine Account Creation

SureLog has also more complex rules that:

1. Look for a new account being created followed by immediate authentication activity from that same account. It would detect the backdoor account creation followed by the account being used to telnet back into the system
2. Check whether the source of an attack was previously the destination of an attack (within 15 minutes)
3. Check whether there are 5 events from host firewalls with severity 4 or greater in 10 minutes between the same source and destination IP
4. Detect an unusual condition where a source has authentication failures at a host, but is not followed by a successful authentication at the same host within 2 hours
5. Detect the same source having excessive logon failures at distinct hosts
6. Look for a new account being created, followed shortly by access/authentication failure activity from the same account
7. Detect potential server compromise
8. Detect logon attempts to disabled accounts
9. Detect account lockout caused by excessive logon failures
10. Monitor new service installation
11. Monitor system access outside of business hours
12. Detect an unusual condition where a source has authentication failures at a host, is not followed by a successful authentication at the same host within 2 hours

Advantages of SureLog Correlation Engine

Below are some advantages of SureLog:

- It's fast-Supports 50,000 EPS with thousands of rules

- It can trace multiple logs with different types within a defined time frame. A sample rule to support this advantage is: Detect an unusual condition where a source has authentication failures at a host, but is not followed by successful authentication at the same host **within 2 hours**

- It can correlate different logs (Example: Windows User Creation Event and Telnet Event) according to related fields. A sample rule to support this advantage is: Look for a **new account being created** followed by immediate authentication activity from that same account. It would detect the backdoor account creation followed by the **account being used** to telnet back into the system

- It can trace a log being created with desired parameters or not. A sample rule to support this advantage is: Detect an unusual condition where a source has authentication failures at a host, **is not followed** by a successful authentication at the same host within 2 hours

- It can audit privileged user activity such as new account creation for greater operational transparency

- It can correlate privileged user behavior with specific network activity. A sample rule to support this advantage is: Look for a new account being created followed by immediate authentication activity from that same account. It would detect the backdoor account creation followed by the account being used to telnet back into the system

- Its correlation rule editor is simple to use
- It has multiple filtering options

- It has a compression-based correlation feature: SureLog can monitor multiple occurrences of the same event, removes redundancies, and reports them as a single event

- It has a threshold-based correlation: SureLog has a threshold to trigger a report when a specified number of similar events occur

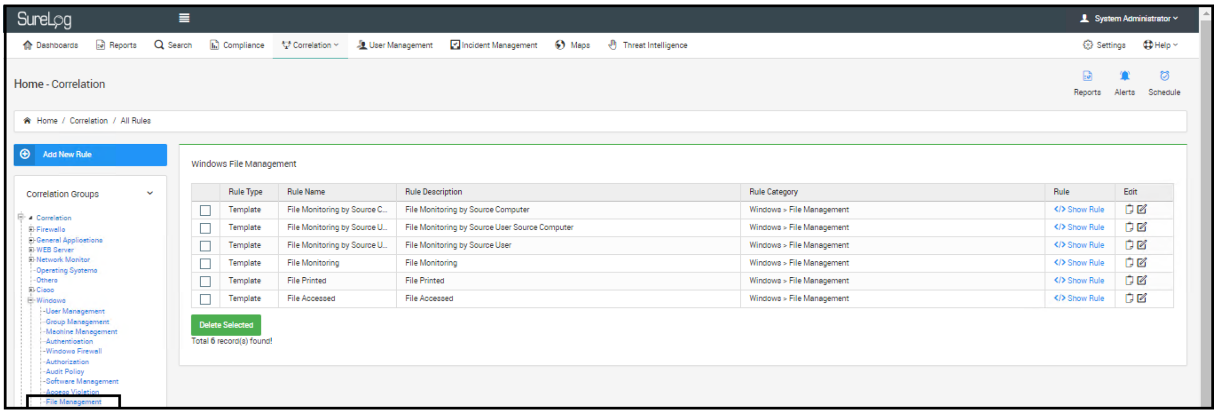
- It has a filter-based correlation: SureLog Inspects each event to determine if it matches a pattern defined by a regular expression. If a match is found, an action may be triggered as specified in the rule.

- It has a sequence-based correlation: SureLog helps establish causality of events. Events can be correlated based on specific sequential relationships. For example, synchronizing multiple events such as "Event A" being followed by "Event B" to trigger an action.

- Its time-based correlation is useful for correlating events that have specific time-based relationships. Some problems can be determined only through temporal correlation. For example, time-based correlation can be used to implement cleanup rules given a specific interval

Template Rules

Template rules are preconfigured rules. The SureLog platform comes with a set of preconfigured rules that users can begin using immediately:



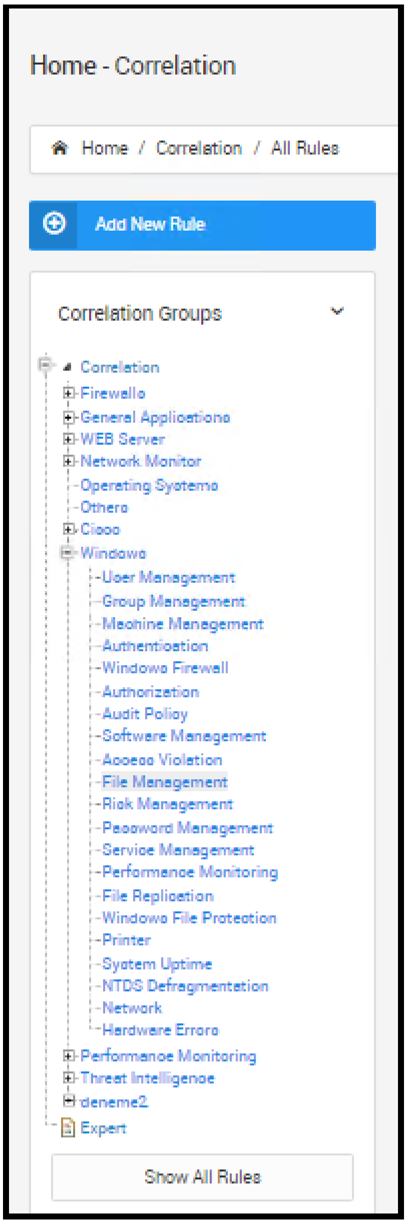
Windows File Management

	Rule Type	Rule Name	Rule Description	Rule Category	Rule	Edit
□	Template	File Monitoring by Source C...	File Monitoring by Source Computer	Windows > File Management	</> Show Rule	
□	Template	File Monitoring by Source U...	File Monitoring by Source User Source Computer	Windows > File Management	</> Show Rule	
□	Template	File Monitoring by Source U...	File Monitoring by Source User	Windows > File Management	</> Show Rule	
□	Template	File Monitoring	File Monitoring	Windows > File Management	</> Show Rule	
□	Template	File Printed	File Printed	Windows > File Management	</> Show Rule	
□	Template	File Accessed	File Accessed	Windows > File Management	</> Show Rule	

Total 6 record(s) found!

Steps for using template rules:

1. Select Correlation
2. Select correlation group from the left pane
3. Select a sub-rule category

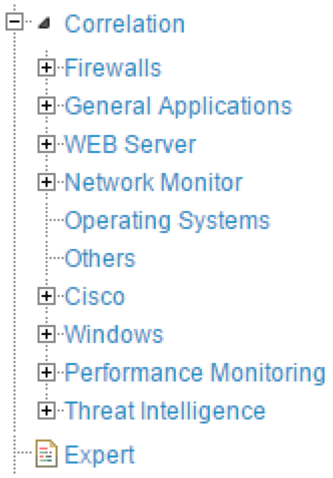


4. Select a rule, then select the Edit button
5. Edit the required fields:

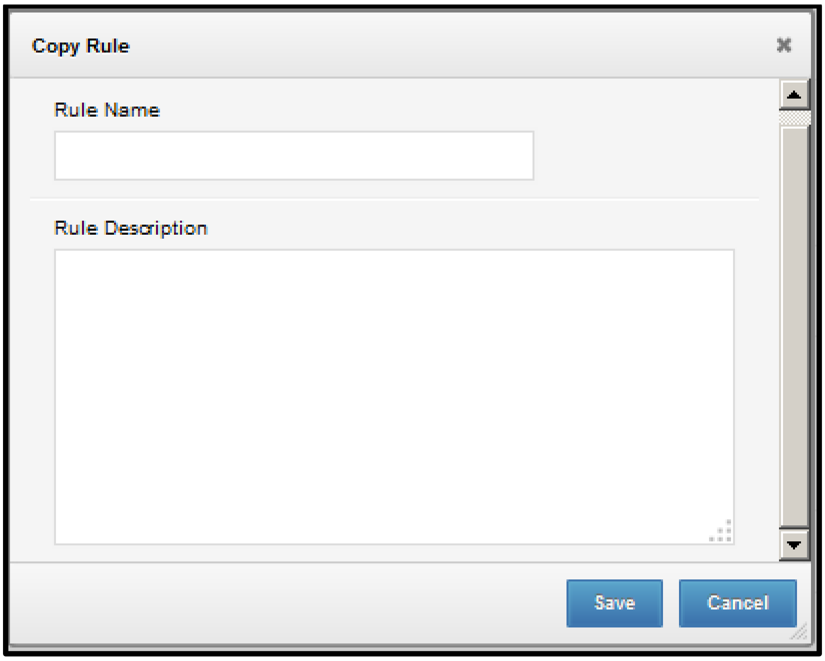
- Rule Category
- Rule Name
- Rule Description
- Username
- Computer name

Steps for cloning template rules:

1. Select Correlation
2. Select Template from the left pane
3. Select a sub-rule category



4. Select a rule and then select the Copy Rule button
5. Enter data into the Rule Name and Rule Description fields

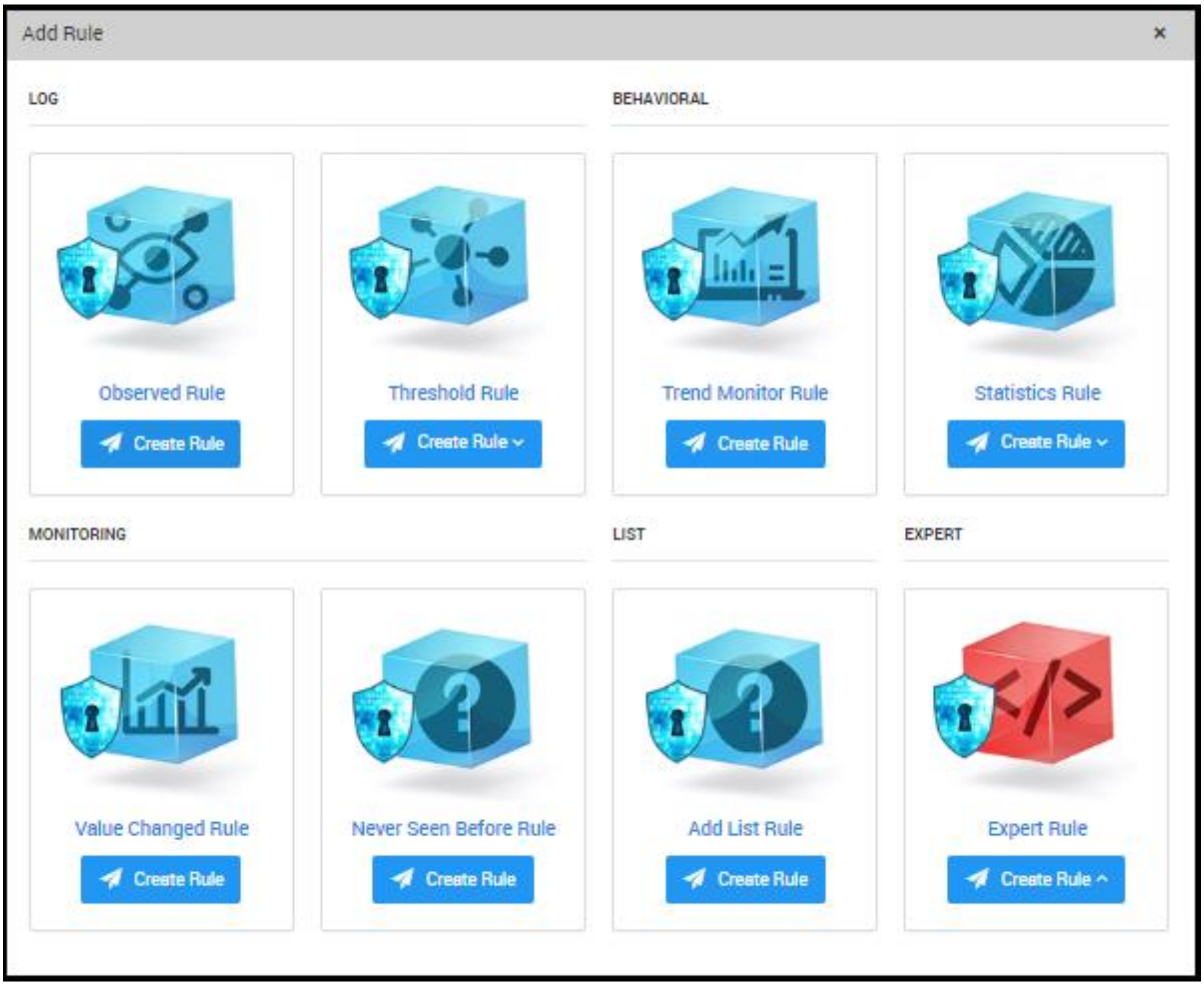


Chapter 9: Creating Custom Correlation Rules

A user can create rules by using template rules or the wizard.

To create rules using the wizard:

1. Open the Correlation pane.
2. Click the Create Rule button
3. Enter data into the Rule Name and Rule Description fields (required)



Add Rule ×

LOG

BEHAVIORAL

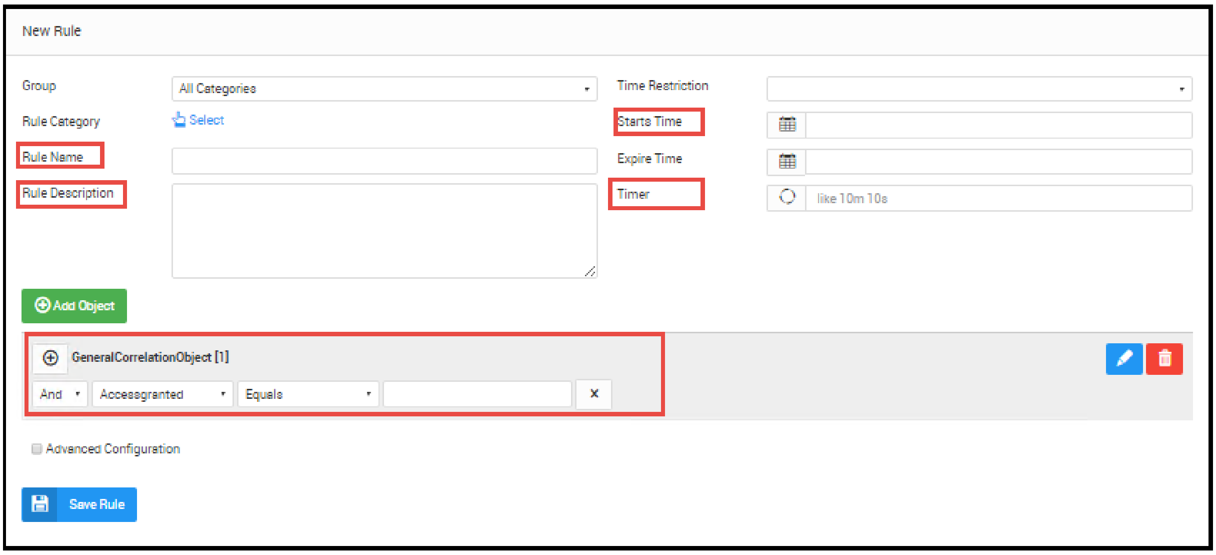
MONITORING

LIST

EXPERT

Observed Rule

For Observed Rule, you should fill related fields:



New Rule

Group	All Categories	Time Restriction	
Rule Category	Select	Starts Time	
Rule Name		Expire Time	
Rule Description		Timer	like 10m 10s

GeneralCorrelationObject [1]

And | Accessgranted | Equals | ×

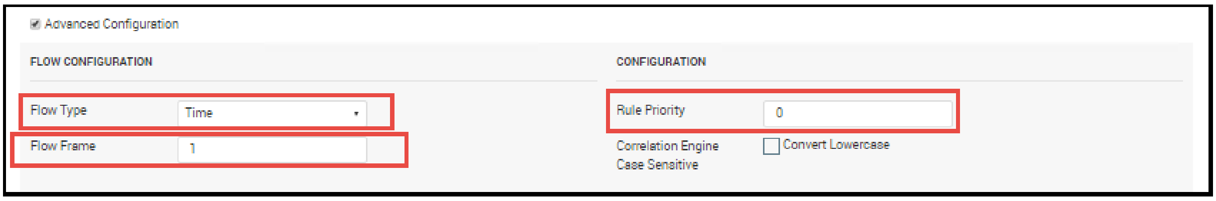
□ Advanced Configuration

The user can also set rule priority. To set rule priority:

1. Open the correlation rule view.
2. Click the Advanced Configuration
3. Set the priority value as follows

The rules running order can be set by priority values. If the priority value is set to the smallest value for a rule. That rule runs firstly.

4. The rule considered previous Flow type as time and count (this time and count determined in flow frame in ms or number)



☑ Advanced Configuration

FLOW CONFIGURATION

Flow Type: Time

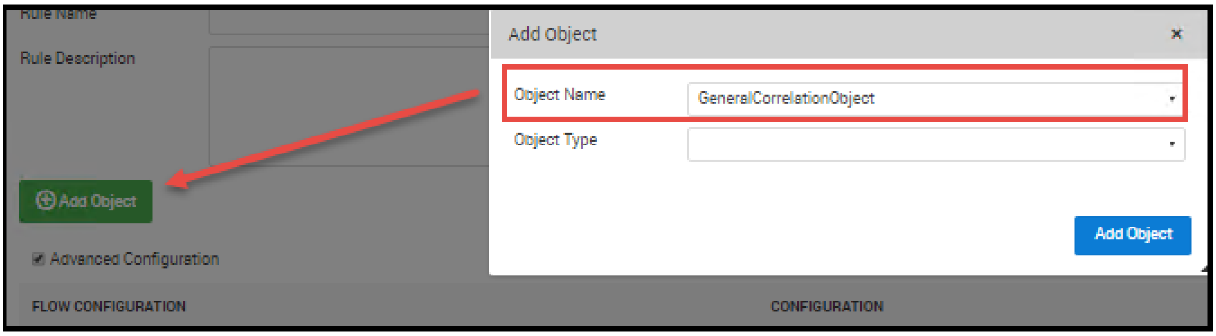
Flow Frame: 1

CONFIGURATION

Rule Priority: 0

Correlation Engine Case Sensitive: □ Convert Lowercase

5. Click the Add Object button

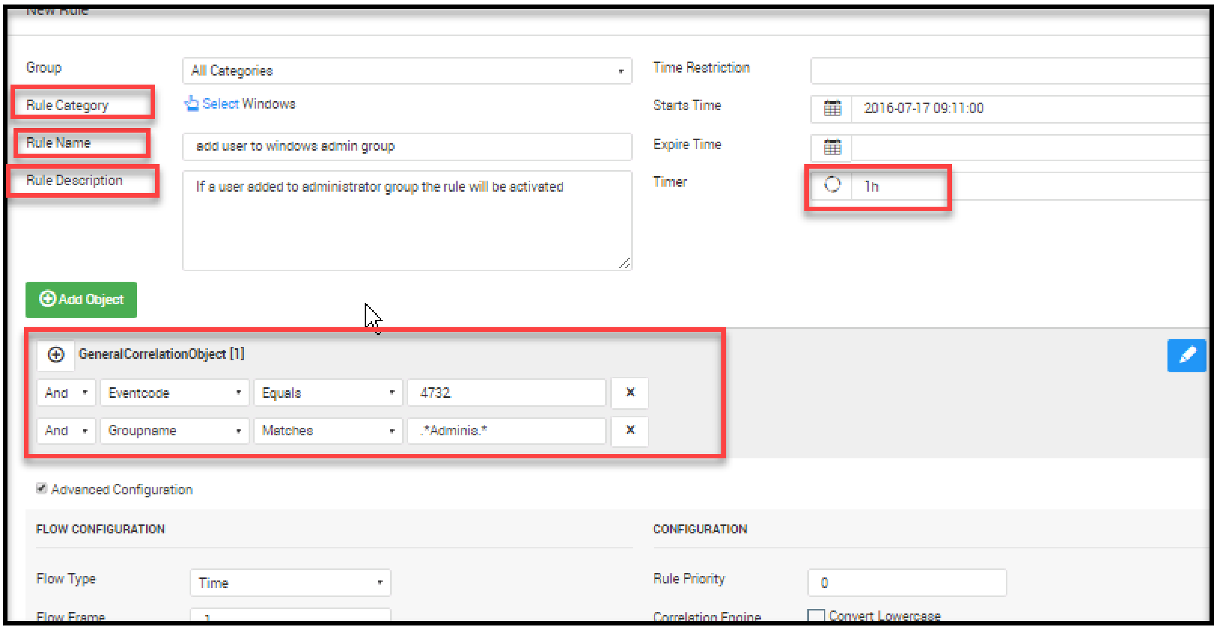


Add Object

Object Name: GeneralCorrelationObject

Object Type:

6. Select the log fields (each log type has its own fields)



New Rule

Group: All Categories

Rule Category: Select Windows

Rule Name: add user to windows admin group

Rule Description: If a user added to administrator group the rule will be activated

Time Restriction:

Starts Time: 2016-07-17 09:11:00

Expire Time:

Timer: 1h

GeneralCorrelationObject [1]

And | Eventcode | Equals | 4732

And | Groupname | Matches | .*Adminis.*

☑ Advanced Configuration

FLOW CONFIGURATION

Flow Type: Time

Flow Frame: 1

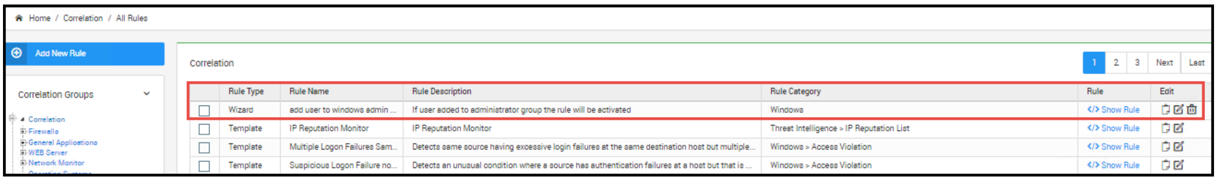
CONFIGURATION

Rule Priority: 0

Correlation Engine: □ Convert Lowercase

7. Select save to save the changes.

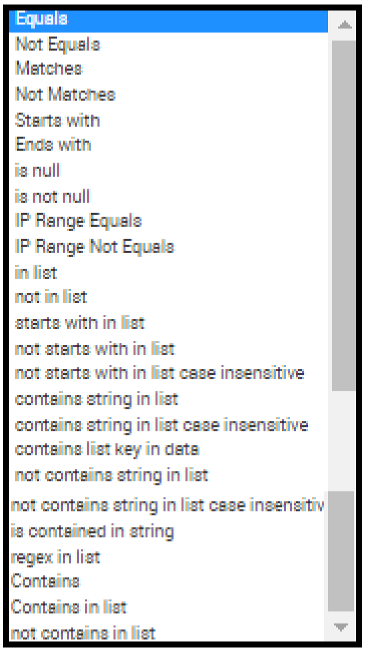
After saving the rule, the rule is listed in Correlation rules list as shown in the following figure:



	Rule Type	Rule Name	Rule Description	Rule Category	Rule	Edit
☐	Wizard	add user to windows admin ...	If user added to administrator group the rule will be activated	Windows	</> Show Rule	
☐	Template	IP Reputation Monitor	IP Reputation Monitor	Threat Intelligence > IP Reputation List	</> Show Rule	
☐	Template	Multiple Logon Failures Sam...	Detects same source having excessive login failures at the same destination host but multiple...	Windows > Access Violation	</> Show Rule	
☐	Template	Suspicious Logon Failure no...	Detects an unusual condition where a source has authentication failures at a host but that is ...	Windows > Access Violation	</> Show Rule	

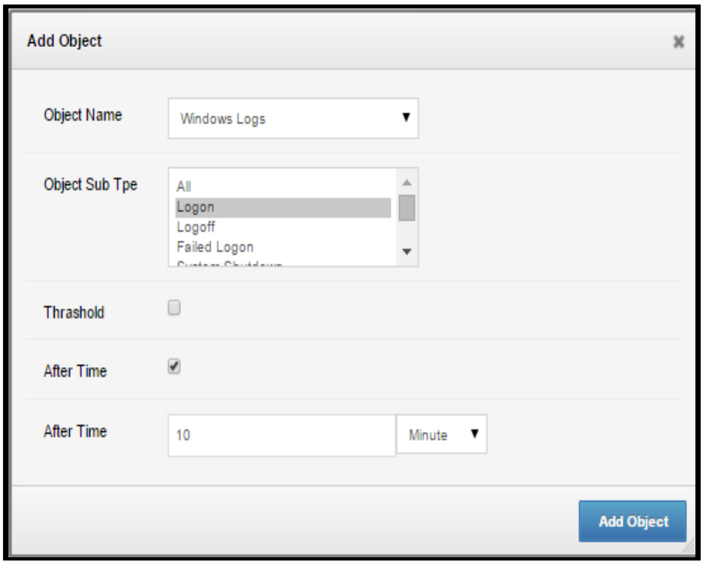
You can copy, edit, and delete any rule as shown in the figure above.

Note the available logic operators:



Relations Between Logs

1. If the user wishes to define relations between logs, they can add another log object



Object Name: Windows Logs

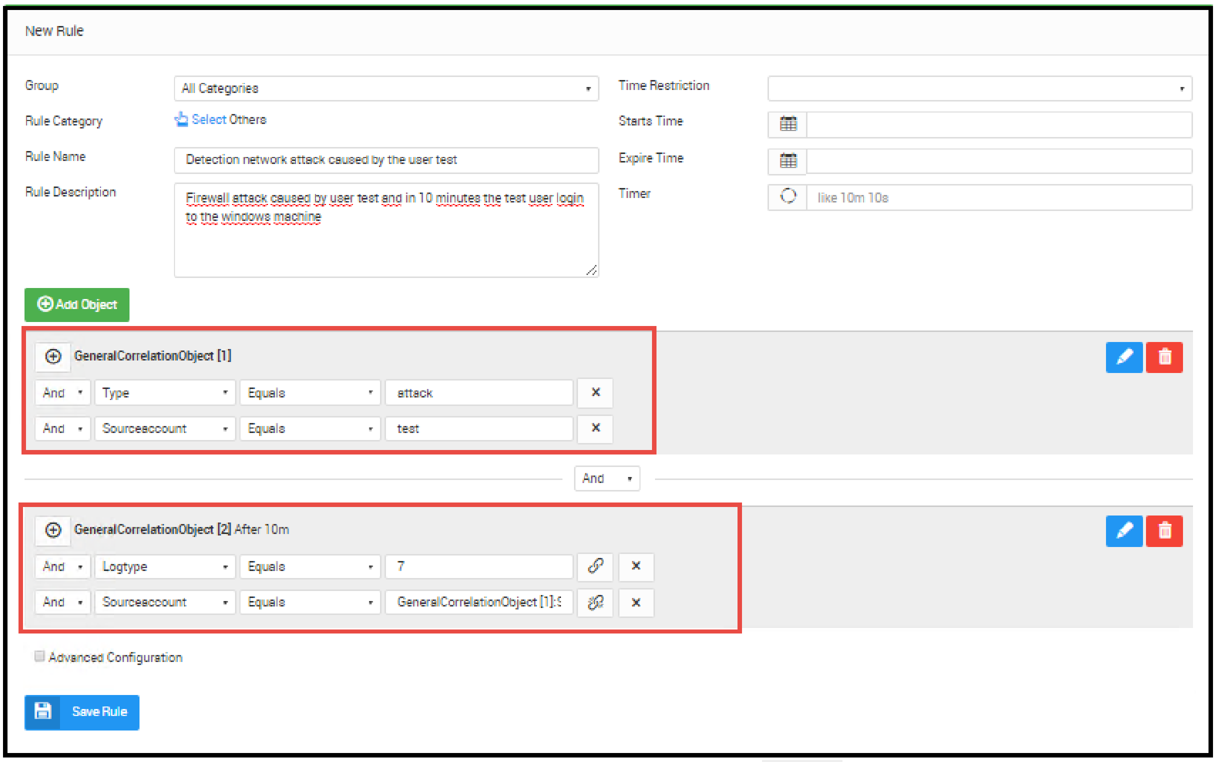
Object Sub Tpe: All, Logon, Logoff, Failed Logon

Thrashold: ☐

After Time: ☑

After Time: 10 Minute

2. If the user wishes to establish a time relation between logs, select After Time. A sample rule that can be used in this scenario would be: Detect a Firewall attack caused by user test and in 10 minutes if user test logs into Windows machine.
3. The user can connect log objects with AND, OR, or NOT logic operators as shown below:



New Rule

Group: All Categories

Rule Category: Select Others

Rule Name: Detection network attack caused by the user test

Rule Description: Firewall attack caused by user test and in 10 minutes the test user login to the windows machine

Time Restriction:

Starts Time:

Expire Time:

Timer: like 10m 10s

Add Object

GeneralCorrelationObject [1]

And	Type	Equals	attack
And	Sourceaccount	Equals	test

And

GeneralCorrelationObject [2] After 10m

And	Logtype	Equals	7
And	Sourceaccount	Equals	GeneralCorrelationObject [1]:S

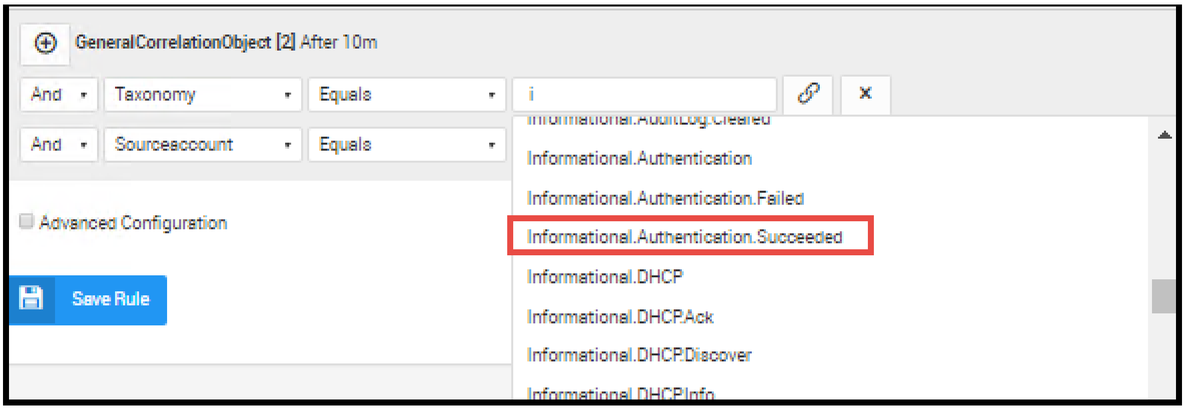
□ Advanced Configuration

Save Rule

4. The user can then link multiple logs by selecting the link button 🔗 and connect log fields with each other. The user can link as many fields as they require.

   GeneralCorrelationObject[2] Sourceaccount is linked to the GeneralCorrelationObject[1] Sourceaccount with link button as shown in the figure below:

5. Windows login condition shown in figure above can also be ensured by using taxonomy in the condition. This way, the login condition is instructed to taxonomy module as Windows login. There are 1536 taxonomy groups in SureLog. The users can use different taxonomies in formulating their rules. The Window login condition is ensured with taxonomy as shown in the figure below:



GeneralCorrelationObject [2] After 10m

And	Taxonomy	Equals	i
And	Sourceaccount	Equals	

Informational.AuditLog.Cleared
Informational.Authentication
Informational.Authentication.Failed
Informational.Authentication.Succeeded
Informational.DHCP
Informational.DHCP.Ack
Informational.DHCP.Discover
Informational.DHCP.Info

□ Advanced Configuration

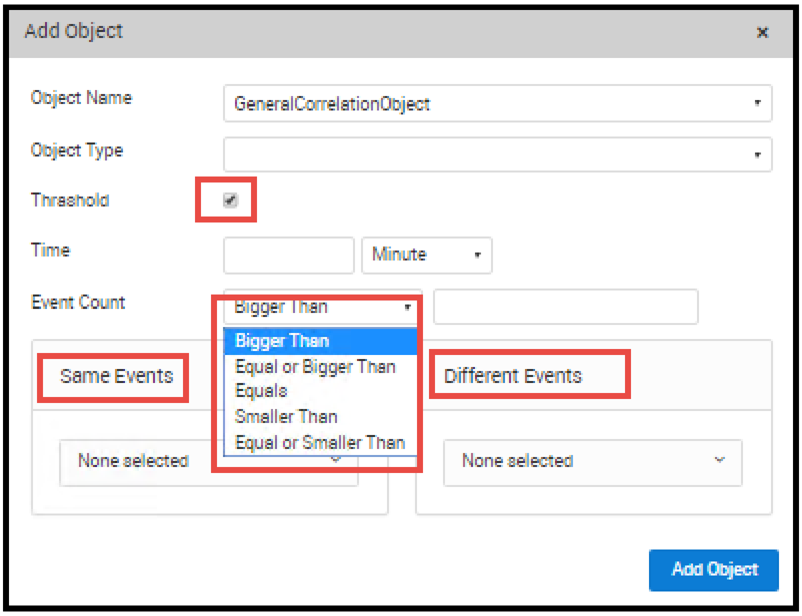
Save Rule

Treshold Rule

For Treshold Rule, you can chose two option which are count and sum threshold rule :

Count Treshold Rule

In Count threshold rule you can fill related fields;



Add Object ×

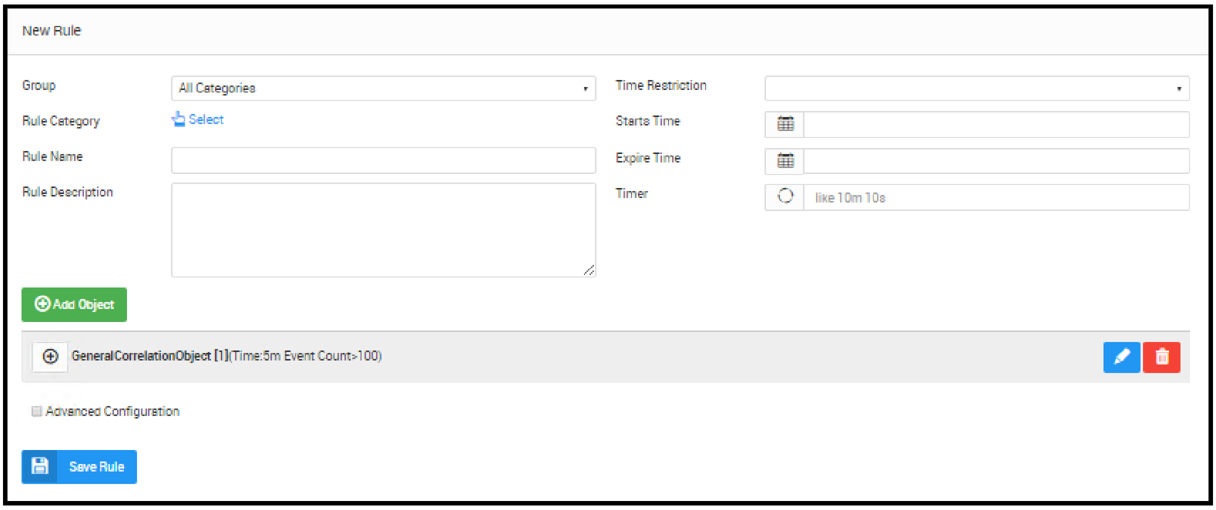
Object Name: GeneralCorrelationObject

Object Type:

Threshold: ☑

Time: Minute

Event Count: Bigger Than



New Rule

Group: All Categories

Rule Category: Select

Rule Name:

Rule Description:

Time Restriction:

Starts Time:

Expire Time:

Timer: like 10m 10s

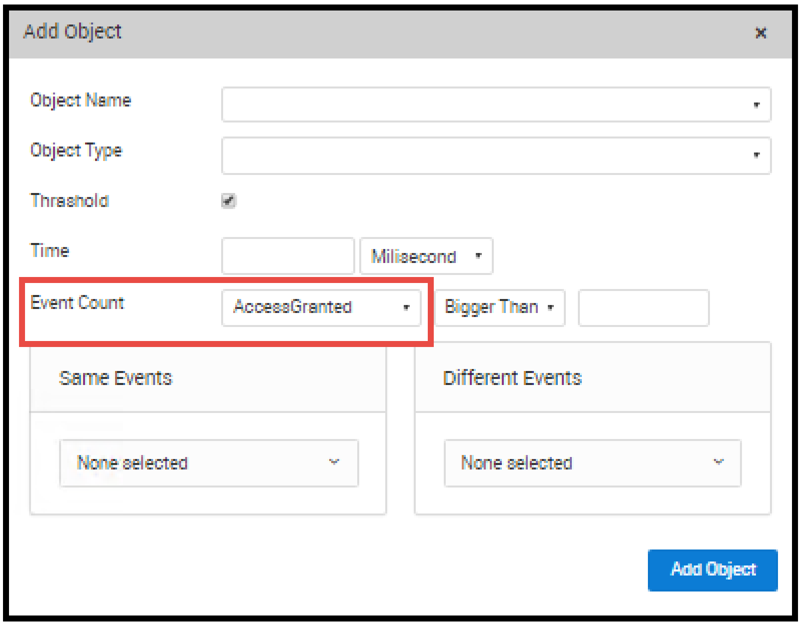
GeneralCorrelationObject [1](Time:5m Event Count>100)

□ Advanced Configuration

<u>The only difference count threshold rule from sum threshold rule</u> is related to upon to database field which is shown below;

<u>Count threshold rule triggers when</u> specified number of similar events occur

Sum Threshold Rule



Add Object

Object Name

Object Type

Threshold ☑

Time | Milisecond

Event Count | AccessGranted | Bigger Than

Same Events: None selected

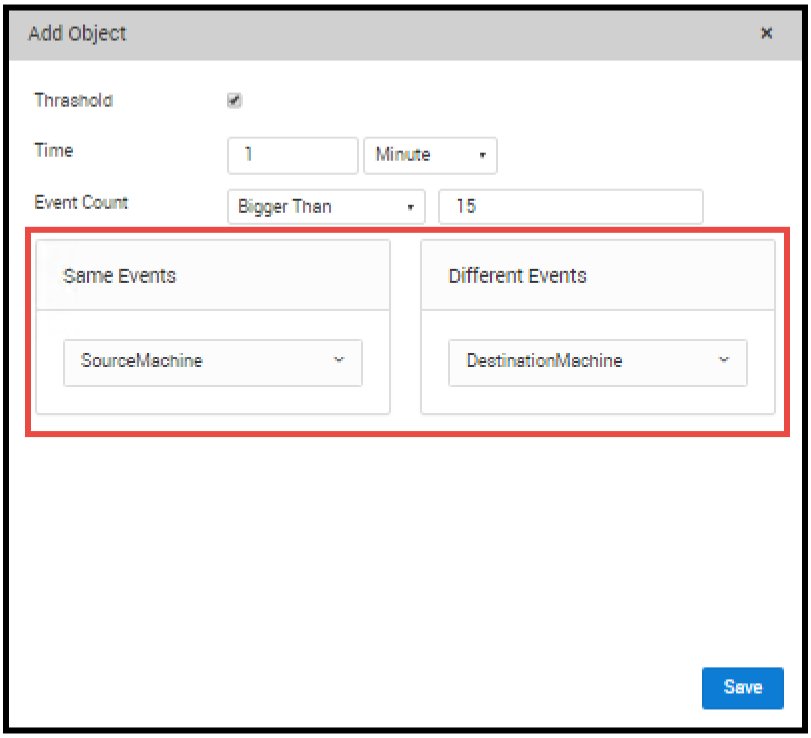
Different Events: None selected

Example of threshold rule;

Attack firewall from different sources

15 attack packets are directed to firewall from different destination machine to same source machine in one minute

- Select the log fields (each log type has its own fields)



Add Object

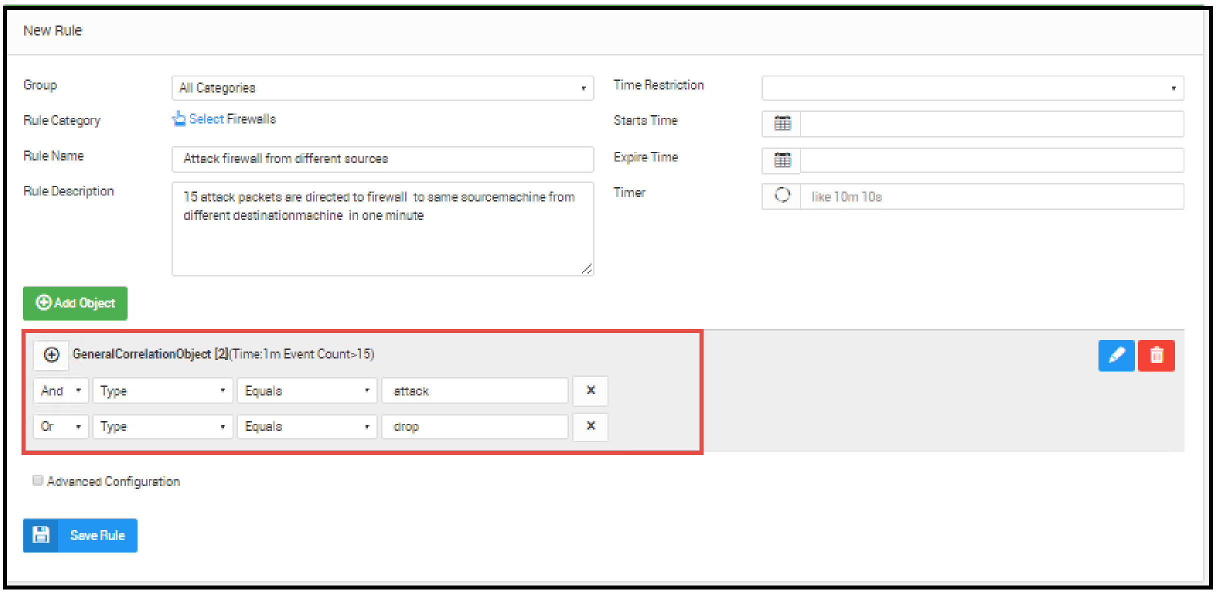
Threshold ☑

Time: 1 | Minute

Event Count: Bigger Than | 15

Same Events: SourceMachine

Different Events: DestinationMachine



New Rule

Group	All Categories	Time Restriction	
Rule Category	Select Firewalls	Starts Time	
Rule Name	Attack firewall from different sources	Expire Time	
Rule Description	15 attack packets are directed to firewall to same sourcemachine from different destinationmachine in one minute	Timer	like 10m 10s

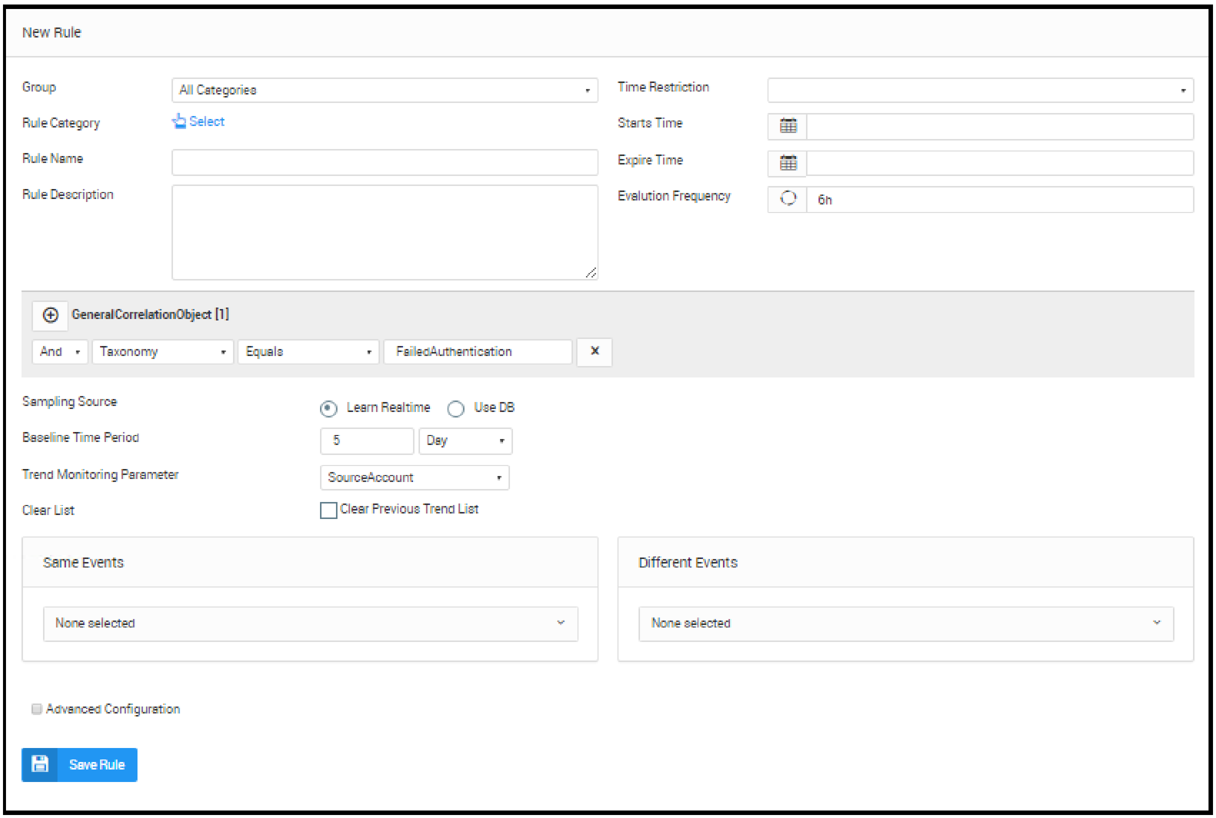
GeneralCorrelationObject [2](Time:1m Event Count>15)

And	Type	Equals	attack	×
Or	Type	Equals	drop	×

□ Advanced Configuration

Trend Monitor Rule

The rule runs for last 5 day data(every 6 hour period of evalution frequency like cronjob) that Sourceaccounts are failed authentication in taxonomy



New Rule

Group	All Categories	Time Restriction	
Rule Category	Select	Starts Time	
Rule Name		Expire Time	
Rule Description		Evalution Frequency	6h

GeneralCorrelationObject [1]

And	Taxonomy	Equals	FailedAuthentication	×

Sampling Source	● Learn Realtime ○ Use DB
Baseline Time Period	5 Day
Trend Monitoring Parameter	SourceAccount
Clear List	□ Clear Previous Trend List

Same Events	Different Events
None selected	None selected

□ Advanced Configuration

Statistic Rule

Statistic Count Rule

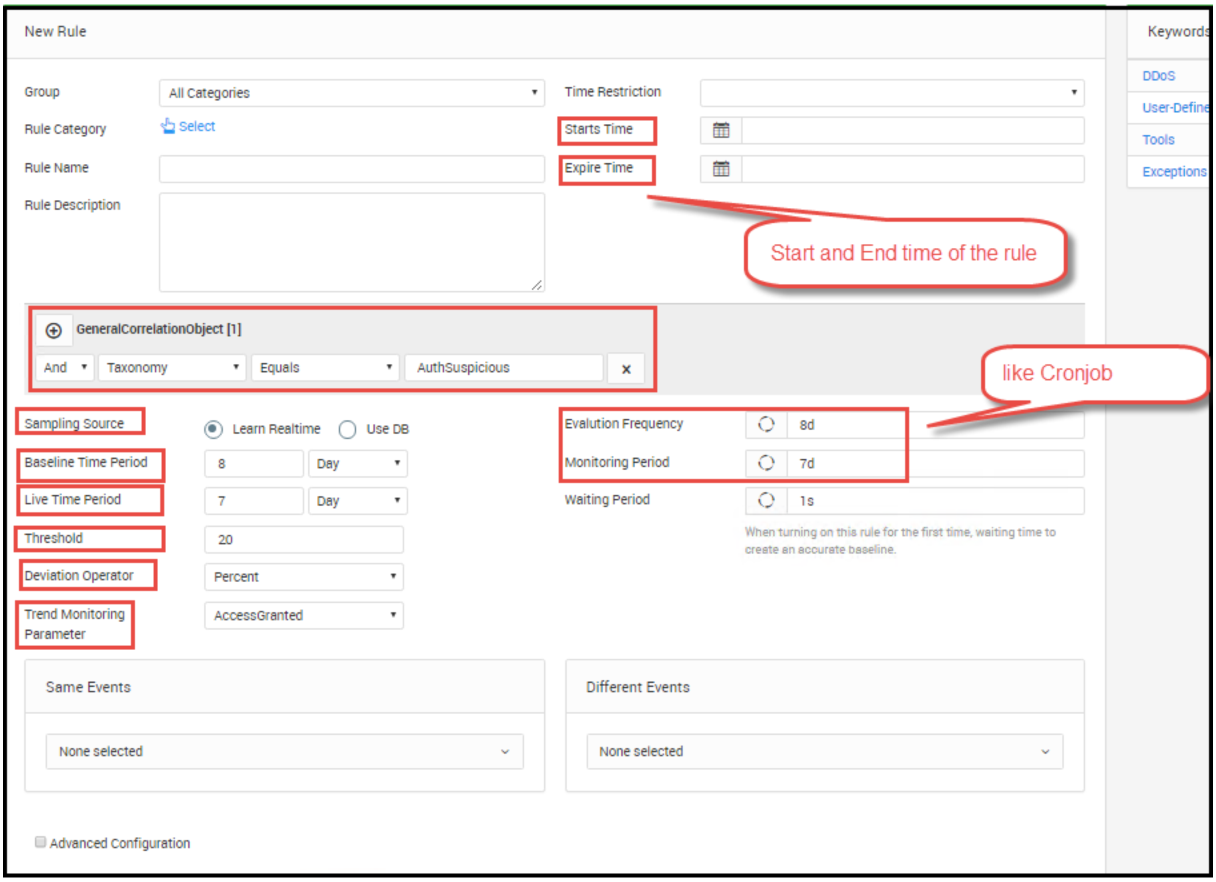
Example:

It calculates count of last 7 day data which taxonomy equals AuthSuspicious of Accessgranted.

Rule which calculates 20 percent of AccessGranted data has standard deviation , is triggered.

Generally evalution Frecuency like cronjob and its value same as Baseline Time Period value and Monitoring Period value same as Live Time Period value.

You can reach this value in realtime by using memory or database



New Rule

Group	All Categories ▾	Time Restriction	▾
Rule Category	Select	Starts Time	
Rule Name		Expire Time	
Rule Description			

Start and End time of the rule

GeneralCorrelationObject [1]

And ▾	Taxonomy ▾	Equals ▾	AuthSuspicious

Sampling Source	● Learn Realtime ○ Use DB	Evalution Frequency	8d
Baseline Time Period	8 Day ▾	Monitoring Period	7d
Live Time Period	7 Day ▾	Waiting Period	1s
Threshold	20		When turning on this rule for the first time, waiting time to create an accurate baseline.
Deviation Operator	Percent ▾		
Trend Monitoring Parameter	AccessGranted ▾		

like Cronjob

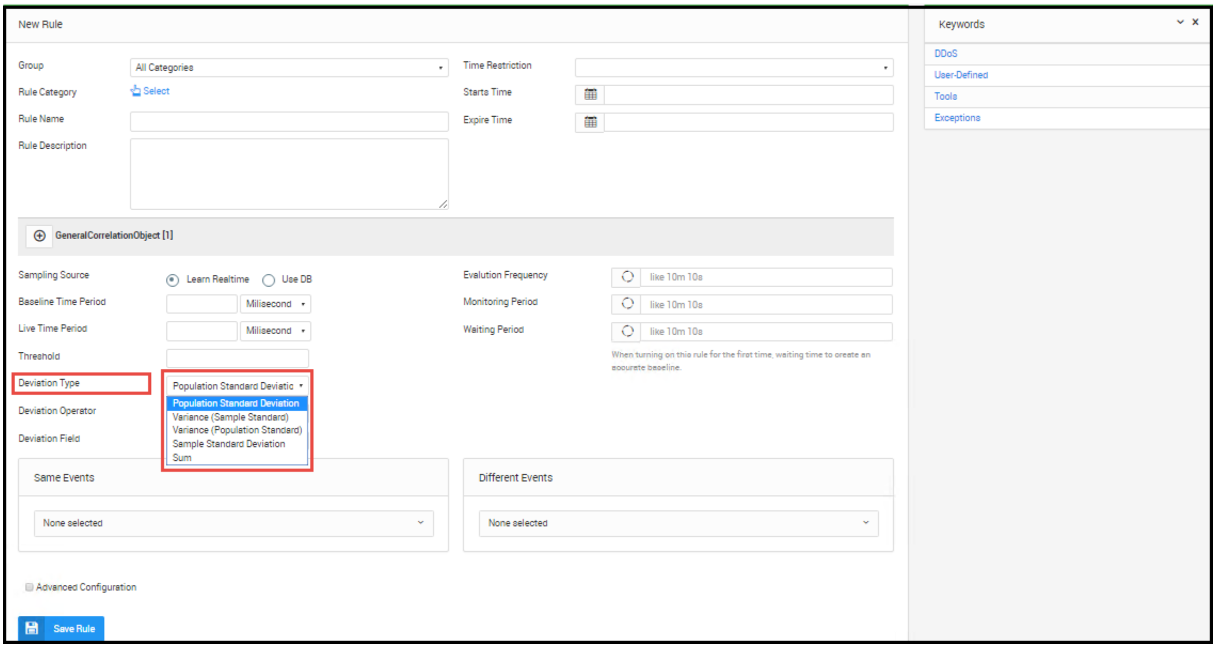
Same Events: None selected

Different Events: None selected

□ Advanced Configuration

Statistic Average Rule

Apart from statistic count rule you can choose one of the scientific statistic calculation in combobox



New Rule

Group: All Categories

Rule Category: Select

Rule Name:

Rule Description:

Time Restriction:

Starts Time:

Expire Time:

GeneralCorrelationObject [1]

Sampling Source: ● Learn Realtime ○ Use DB

Baseline Time Period: Milisecond

Live Time Period: Milisecond

Threshold:

Deviation Type: Population Standard Deviatic

Deviation Operator:

Deviation Field:

Evalution Frequency: like 10m 10s

Monitoring Period: like 10m 10s

Waiting Period: like 10m 10s

When turning on this rule for the first time, waiting time to create an accurate baseline.

Same Events: None selected

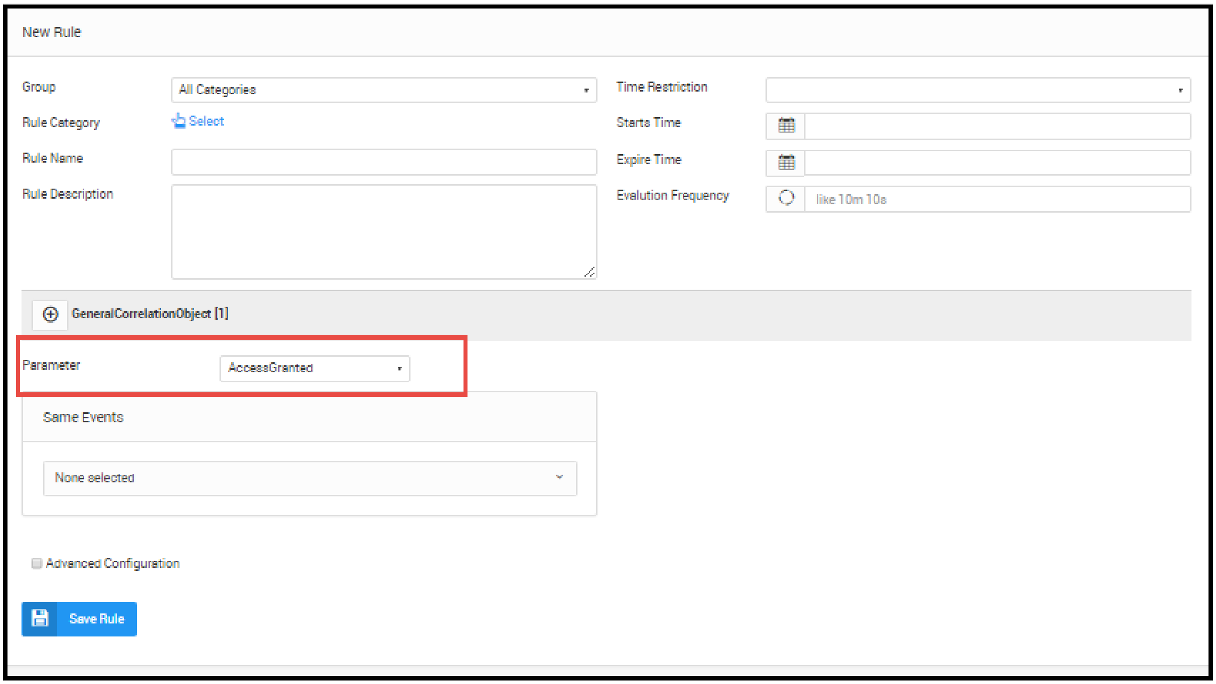
Different Events: None selected

□ Advanced Configuration

Population Standard Deviation
Variance (Sample Standard)
Variance (Population Standard)
Sample Standard Deviation
Sum
Keywords
DDoS
User-Defined
Tools
Exceptions
Save Rule

Value Changed Rule

Apart from other correlation rules the main difference is that change parameter.it is triggered when this parameter value changes.



New Rule

Group: All Categories

Rule Category: Select

Rule Name:

Rule Description:

Time Restriction:

Starts Time:

Expire Time:

Evalution Frequency: like 10m 10s

GeneralCorrelationObject [1]

Parameter: AccessGranted

Same Events: None selected

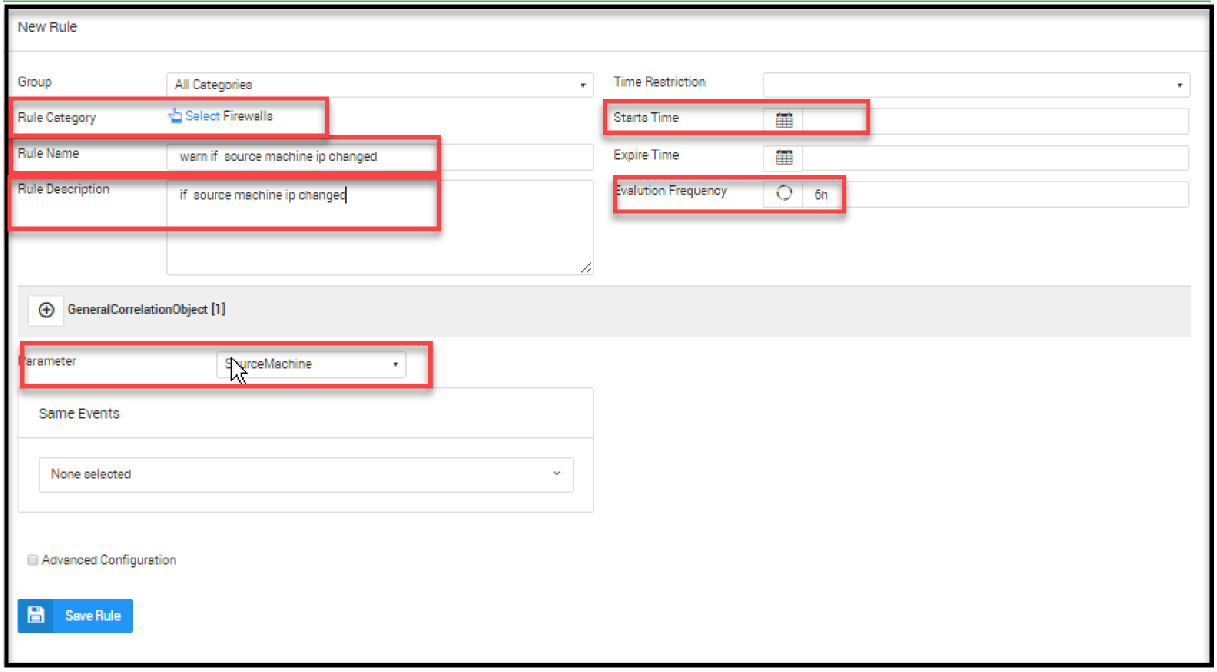
□ Advanced Configuration

Never Seen Before Rule

It is triggered when this parameter never seen before in log flow.

Example :

Warn if sourcemachine ip never seen before



New Rule

Group	All Categories	Time Restriction	
Rule Category	Select Firewalls	Starts Time	
Rule Name	warn if source machine ip changed	Expire Time	
Rule Description	if source machine ip changed	Evalution Frequency	6h

GeneralCorrelationObject [1]

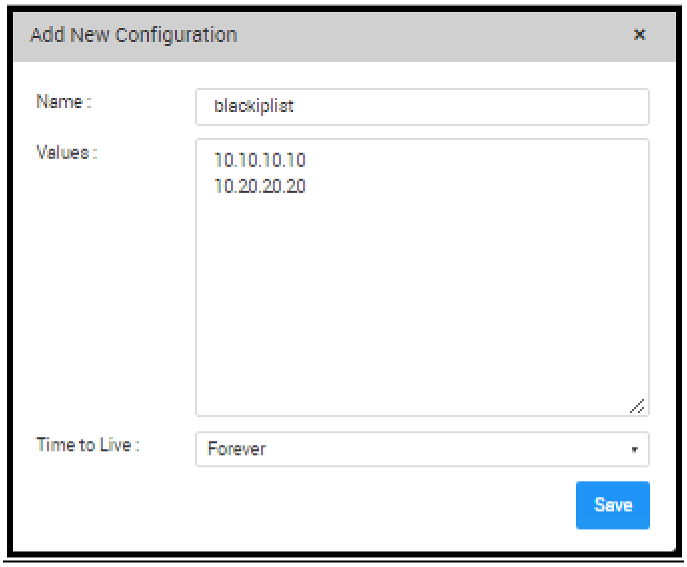
Parameter: SourceMachine

Same Events: None selected

□ Advanced Configuration

Add List Rule

You can create list from
Setting →Correlation Configuration→Define List

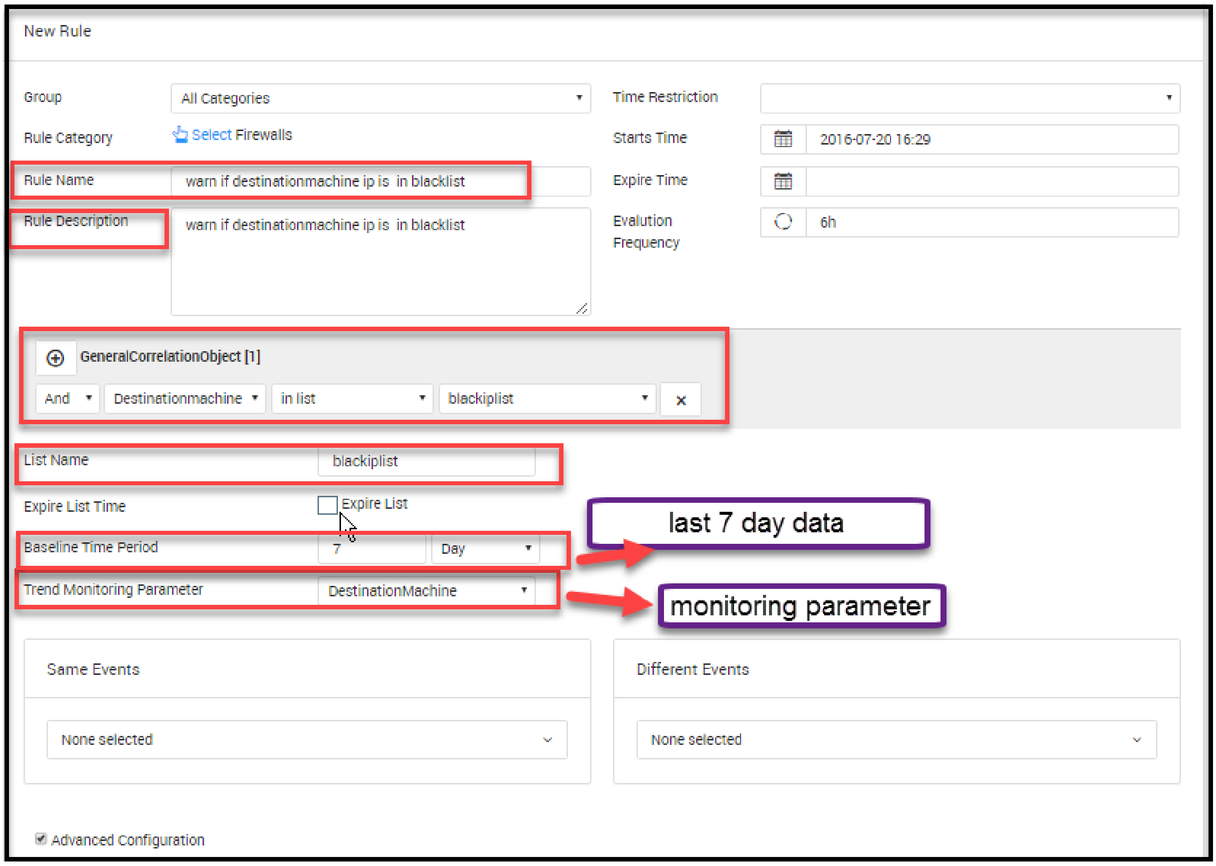


Add New Configuration

Name : blackiplist

Values :
10.10.10.10
10.20.20.20

Time to Live : Forever



New Rule

Group	All Categories	Time Restriction	
Rule Category	Select Firewalls	Starts Time	2016-07-20 16:29
Rule Name	warn if destinationmachine ip is in blacklist	Expire Time	
Rule Description	warn if destinationmachine ip is in blacklist	Evalution Frequency	6h

GeneralCorrelationObject [1]

And | Destinationmachine | in list | blackiplist

List Name	blackiplist
Expire List Time	□ Expire List
Baseline Time Period	7 Day
Trend Monitoring Parameter	DestinationMachine

Same Events: None selected

Different Events: None selected

☑ Advanced Configuration

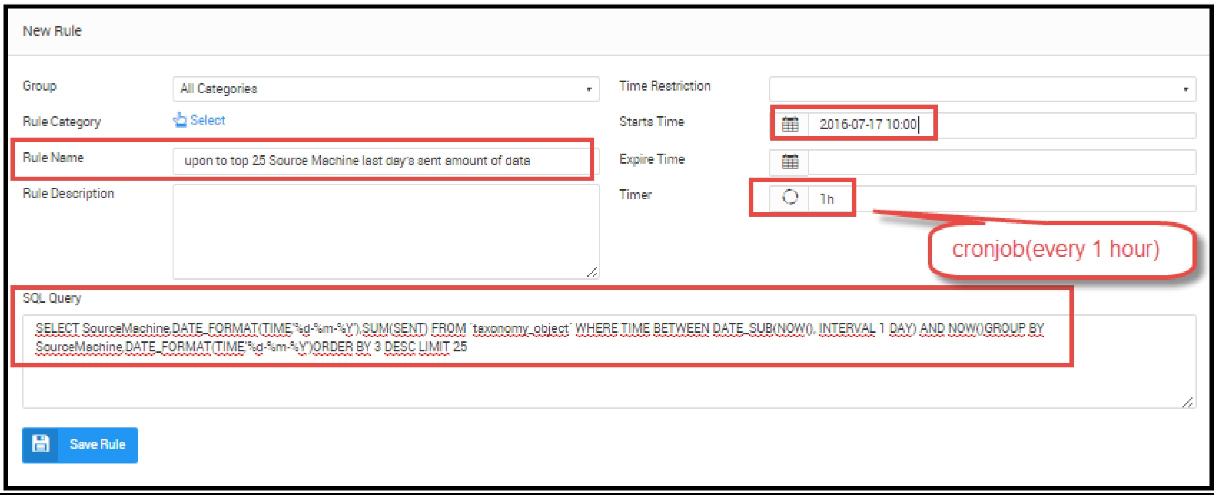
Expert Rule

You can write rule by yourself with using SQL Statement and java code

Example with sql statement
upon to top 25 Source Machine last day’s amount of sent data(byte)

SQL query

```
SELECT SourceMachine,DATE_FORMAT(TIME,'%d-%m-%Y'),SUM(SENT) FROM
`taxonomy_object` WHERE TIME BETWEEN DATE_SUB(NOW(), INTERVAL 1 DAY) AND
NOW()GROUP BY SourceMachine,DATE_FORMAT(TIME,'%d-%m-%Y')ORDER BY 3 DESC LIMIT
25
```



New Rule

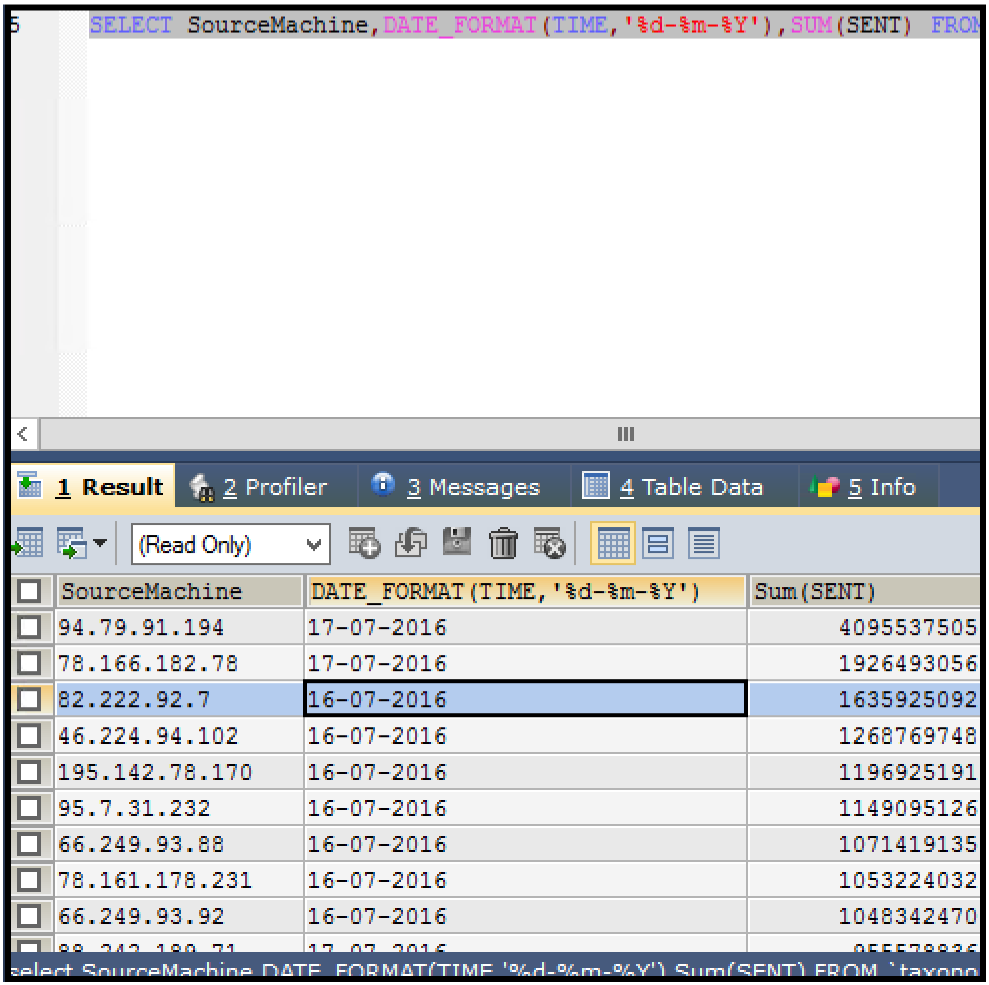
Group	All Categories
Rule Category	Select
Rule Name	upon to top 25 Source Machine last day's sent amount of data
Rule Description	
Time Restriction	
Starts Time	2016-07-17 10:00
Expire Time	
Timer	1h

cronjob(every 1 hour)

SQL Query

```
SELECT SourceMachine,DATE_FORMAT(TIME,'%d-%m-%Y'),SUM(SENT) FROM `taxonomy_object` WHERE TIME BETWEEN DATE_SUB(NOW(), INTERVAL 1 DAY) AND NOW()GROUP BY SourceMachine,DATE_FORMAT(TIME,'%d-%m-%Y')ORDER BY 3 DESC LIMIT 25
```

<u>Output will be like below</u>



```
SELECT SourceMachine,DATE_FORMAT(TIME,'%d-%m-%Y'),SUM(SENT) FRO
```

SourceMachine	DATE_FORMAT(TIME,'%d-%m-%Y')	Sum(SENT)
94.79.91.194	17-07-2016	4095537505
78.166.182.78	17-07-2016	1926493056
82.222.92.7	16-07-2016	1635925092
46.224.94.102	16-07-2016	1268769748
195.142.78.170	16-07-2016	1196925191
95.7.31.232	16-07-2016	1149095126
66.249.93.88	16-07-2016	1071419135
78.161.178.231	16-07-2016	1053224032
66.249.93.92	16-07-2016	1048342470

```
select SourceMachine,DATE_FORMAT(TIME,'%d-%m-%Y'),Sum(SENT) FROM `taxono
```

Chapter 10: Alerts

Activating an alert

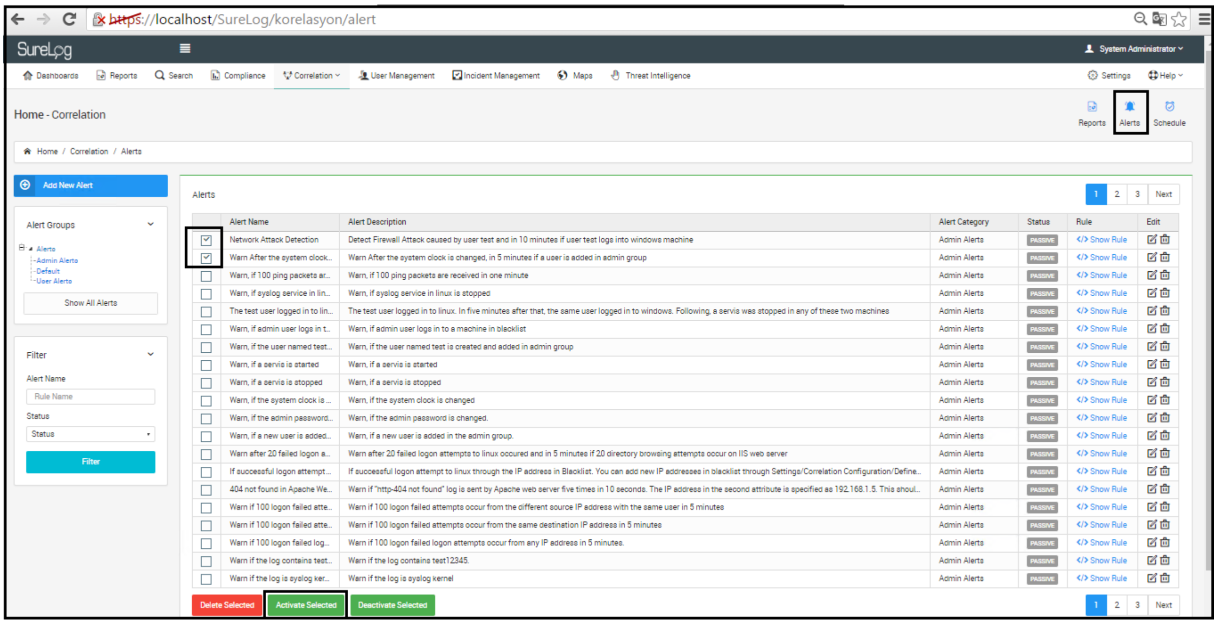
SureLog only uses activated alerts and ignores all other alerts. Therefore, SureLog cannot use alerts until the user activates them. This is done by using the Alerts menu and activating selected alerts.

To enable alerts:

1. Open the Alerts view
2. In the left pane, select the desired to alerts enable
3. In the Alerts grid, select the alerts (or alerts) for activation
4. Enable the alerts as follows:
   To enable a single alert, click the Activate Selected button
   To enable multiple rules, select the alerts first and then click the Activate Selected button

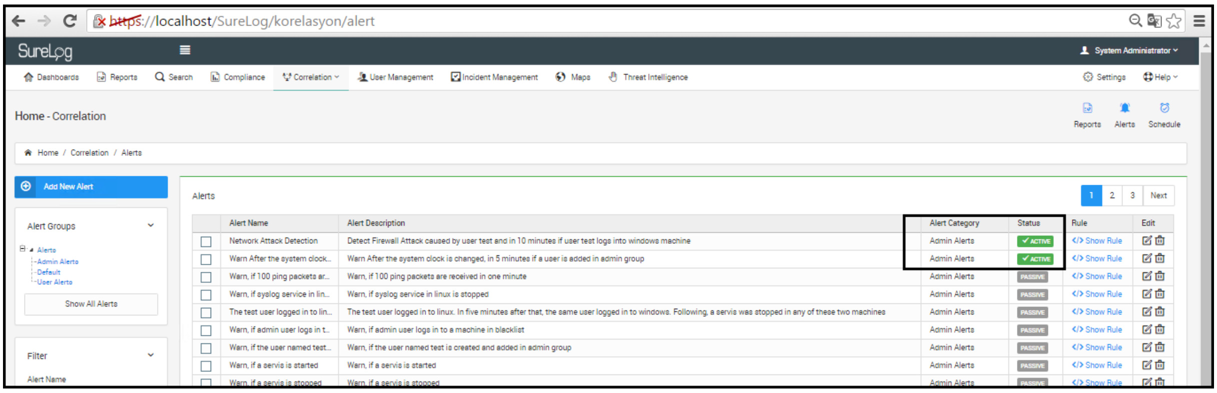
   The in the below shows how the users activate multiple alerts:
   1. Select the alerts to be activated

   2. Select Activate Selected button



	Alert Name	Alert Description	Alert Category	Status	Rule	Edit
☑	Network Attack Detection	Detect Firewall Attack caused by user test and in 10 minutes if user test logs into windows machine	Admin Alerts	PASSIVE	</> Show Rule	
☑	Warn After the system clock...	Warn After the system clock is changed, in 5 minutes if a user is added in admin group	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if 100 ping packets ar...	Warn, if 100 ping packets are received in one minute	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if syslog service in lin...	Warn, if syslog service in linux is stopped	Admin Alerts	PASSIVE	</> Show Rule	
□	The test user logged in to lin...	The test user logged in to linux. In five minutes after that, the same user logged in to windows. Following, a servis was stopped in any of these two machines	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if admin user logs in t...	Warn, if admin user logs in to a machine in blacklist	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if the user named test...	Warn, if the user named test is created and added in admin group	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if a servis is started	Warn, if a servis is started	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if a servis is stopped	Warn, if a servis is stopped	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if the system clock is ...	Warn, if the system clock is changed	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if the admin password...	Warn, if the admin password is changed.	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if a new user is added...	Warn, if a new user is added in the admin group.	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn after 20 failed logon a...	Warn after 20 failed logon attempts to linux occured and in 5 minutes if 20 directory browsing attempts occur on IIS web server	Admin Alerts	PASSIVE	</> Show Rule	
□	If successful logon attempt...	If successful logon attempt to linux through the IP address in Blacklist. You can add new IP addresses in blacklist through Settings/Correlation Configuration/Define...	Admin Alerts	PASSIVE	</> Show Rule	
□	404 not found in Apache We...	Warn if "http-404 not found" log is sent by Apache web server five times in 10 seconds. The IP address in the second attribute is specified as 192.168.1.5. This shoul...	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn if 100 logon failed atte...	Warn if 100 logon failed attempts occur from the different source IP address with the same user in 5 minutes	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn if 100 logon failed atte...	Warn if 100 logon failed attempts occur from the same destination IP address in 5 minutes	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn if 100 logon failed log...	Warn if 100 logon failed logon attempts occur from any IP address in 5 minutes.	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn if the log contains test...	Warn if the log contains test12345.	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn if the log is syslog ker...	Warn if the log is syslog kernel	Admin Alerts	PASSIVE	</> Show Rule	

The figure in the below shows activation of the alerts after the steps pointed out above:

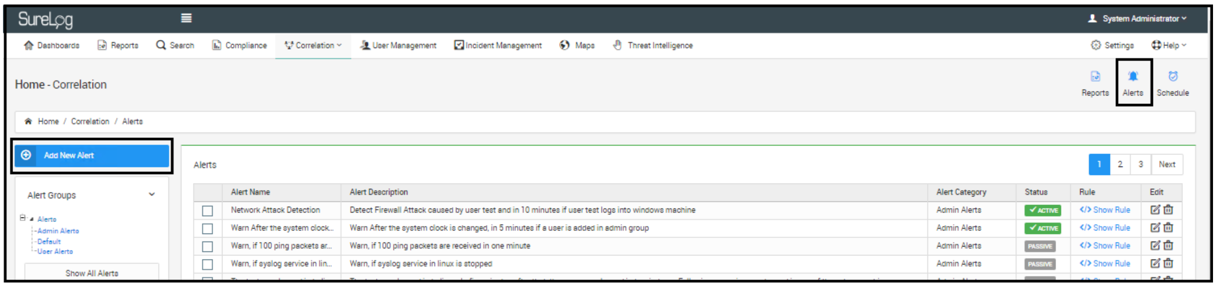


	Alert Name	Alert Description	Alert Category	Status	Rule	Edit
□	Network Attack Detection	Detect Firewall Attack caused by user test and in 10 minutes if user test logs into windows machine	Admin Alerts	✓ ACTIVE	</> Show Rule	
□	Warn After the system clock...	Warn After the system clock is changed, in 5 minutes if a user is added in admin group	Admin Alerts	✓ ACTIVE	</> Show Rule	
□	Warn, if 100 ping packets ar...	Warn, if 100 ping packets are received in one minute	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if syslog service in lin...	Warn, if syslog service in linux is stopped	Admin Alerts	PASSIVE	</> Show Rule	
□	The test user logged in to lin...	The test user logged in to linux. In five minutes after that, the same user logged in to windows. Following, a servis was stopped in any of these two machines	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if admin user logs in t...	Warn, if admin user logs in to a machine in blacklist	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if the user named test...	Warn, if the user named test is created and added in admin group	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if a servis is started	Warn, if a servis is started	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if a servis is stopped	Warn, if a servis is stopped	Admin Alerts	PASSIVE	</> Show Rule	

Note that in case a rule is updated, an alert related with that rule should be re-activated.

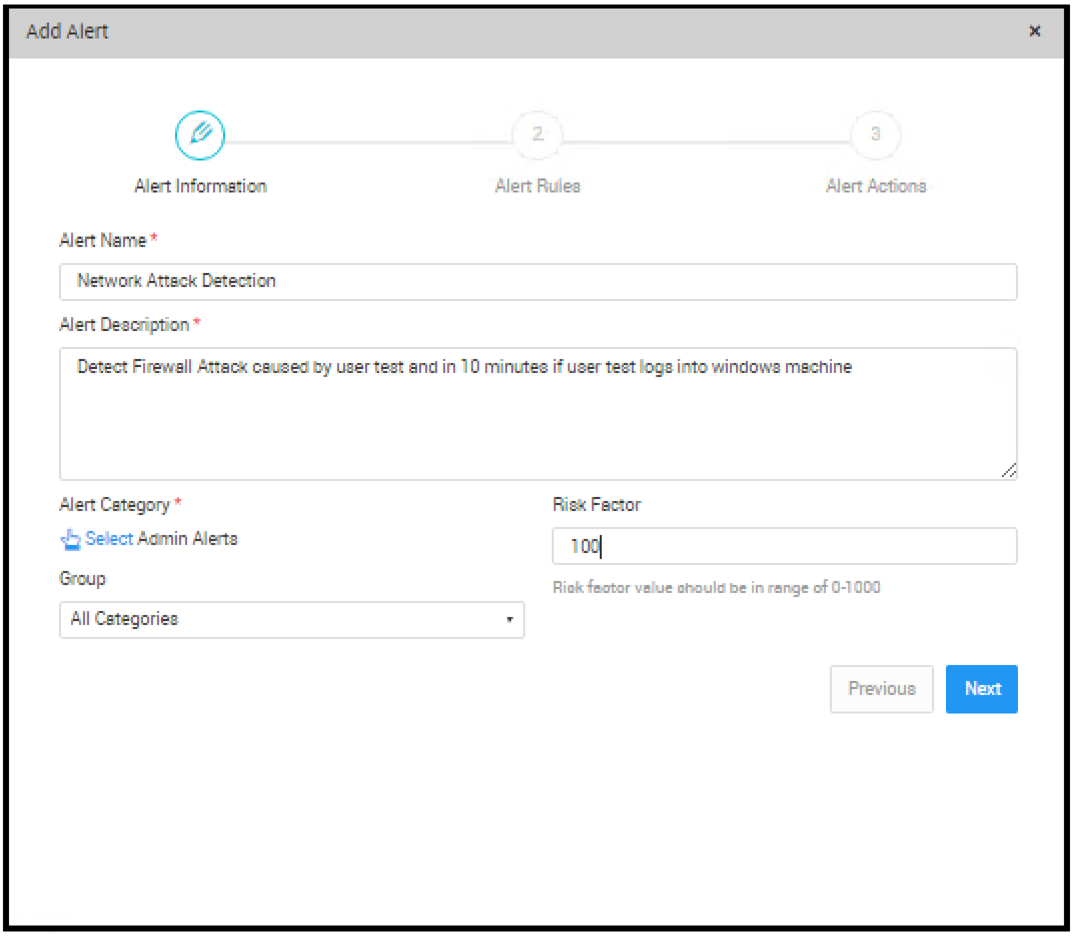
To add an alert for a rule:

1. Open the Alerts view
2. In the left pane, select Add New Alert button



	Alert Name	Alert Description	Alert Category	Status	Rule	Edit
□	Network Attack Detection	Detect Firewall Attack caused by user test and in 10 minutes if user test logs into windows machine	Admin Alerts	✓ ACTIVE	</> Show Rule	
□	Warn After the system clock...	Warn After the system clock is changed, in 5 minutes if a user is added in admin group	Admin Alerts	✓ ACTIVE	</> Show Rule	
□	Warn, if 100 ping packets ar...	Warn, if 100 ping packets are received in one minute	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if syslog service in lin...	Warn, if syslog service in linux is stopped	Admin Alerts	PASSIVE	</> Show Rule	

3. Enter a **name** and **description** for the alert as shown in the figure below



Alert Name *
Network Attack Detection

Alert Description *
Detect Firewall Attack caused by user test and in 10 minutes if user test logs into windows machine

Alert Category *
Select Admin Alerts

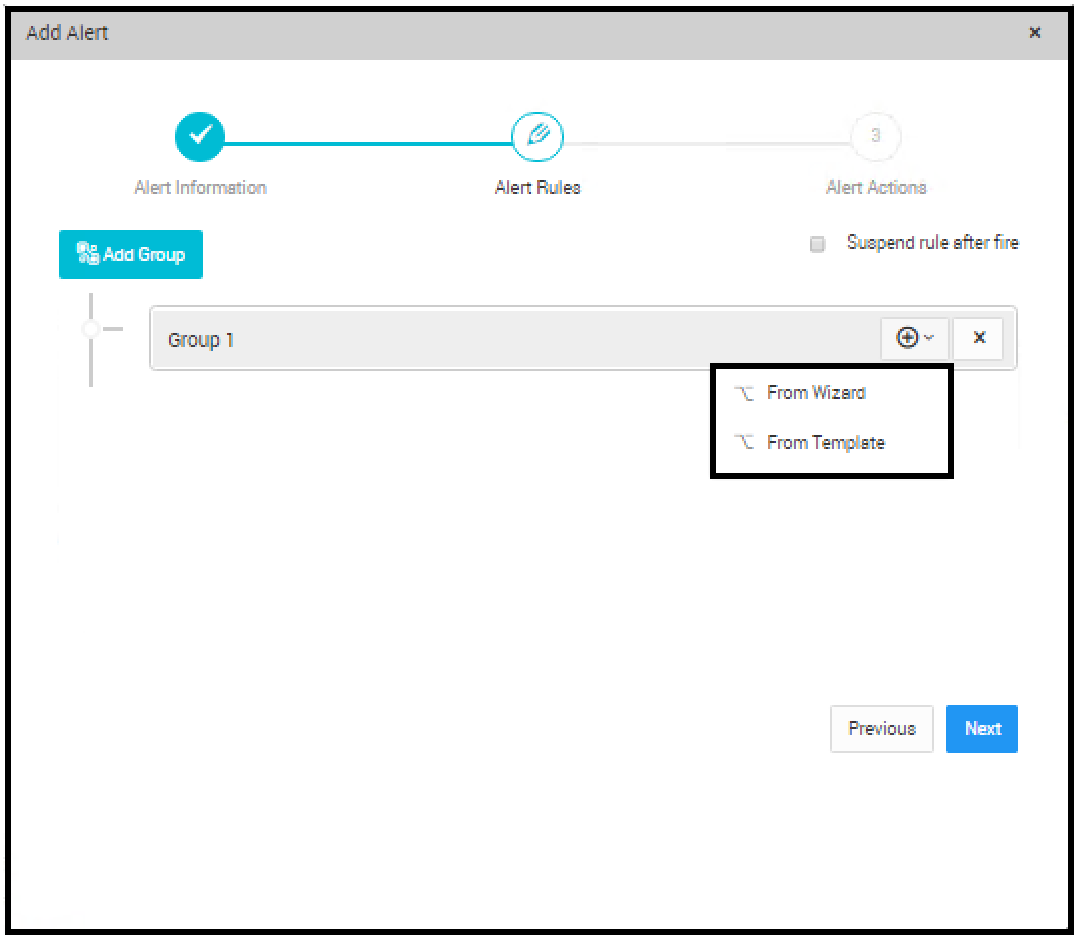
Risk Factor
100

Risk factor value should be in range of 0-1000

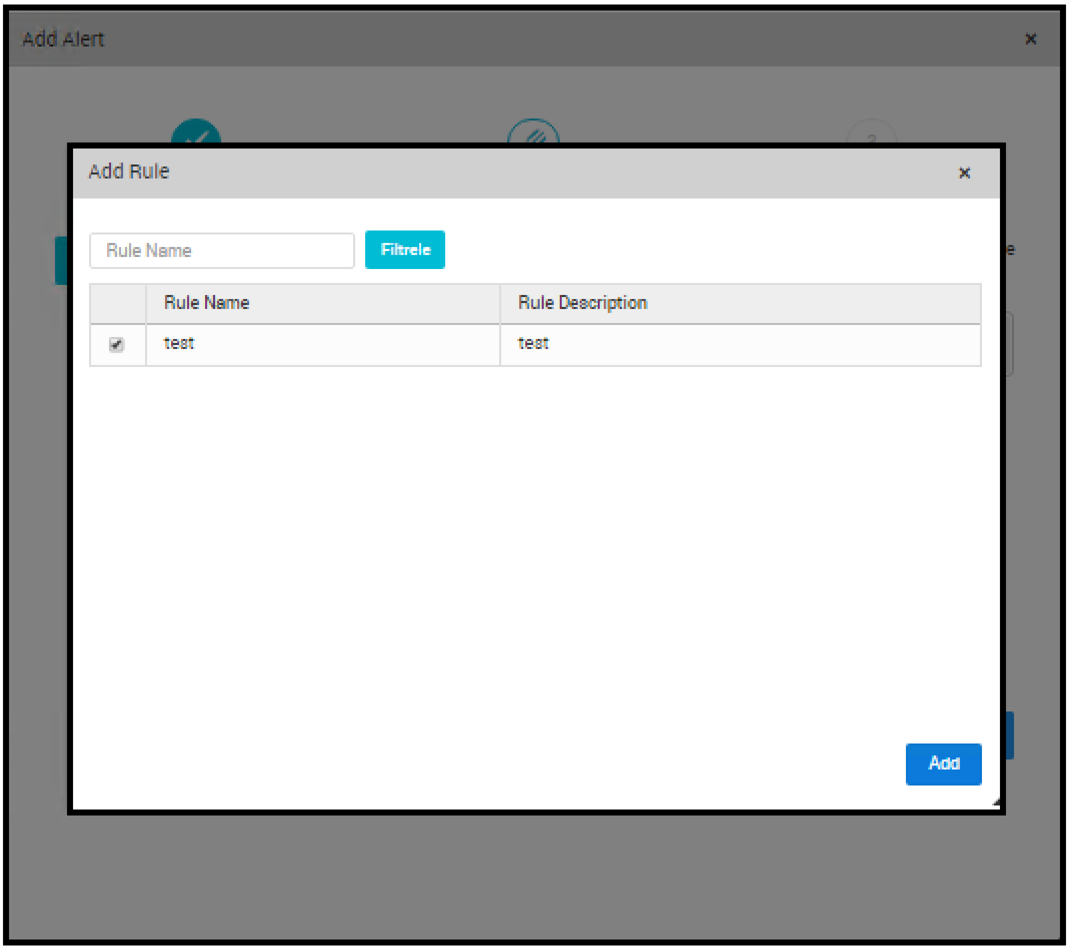
Group
All Categories

4. Select Add Rule Tab in the figure above to add a rule

Here the user can select From Wizard to add a custom rule or From Template to add a template rule in the figure below



5. Select From Wizard to add the custom rule
6. Mark the rule from the list and select Add

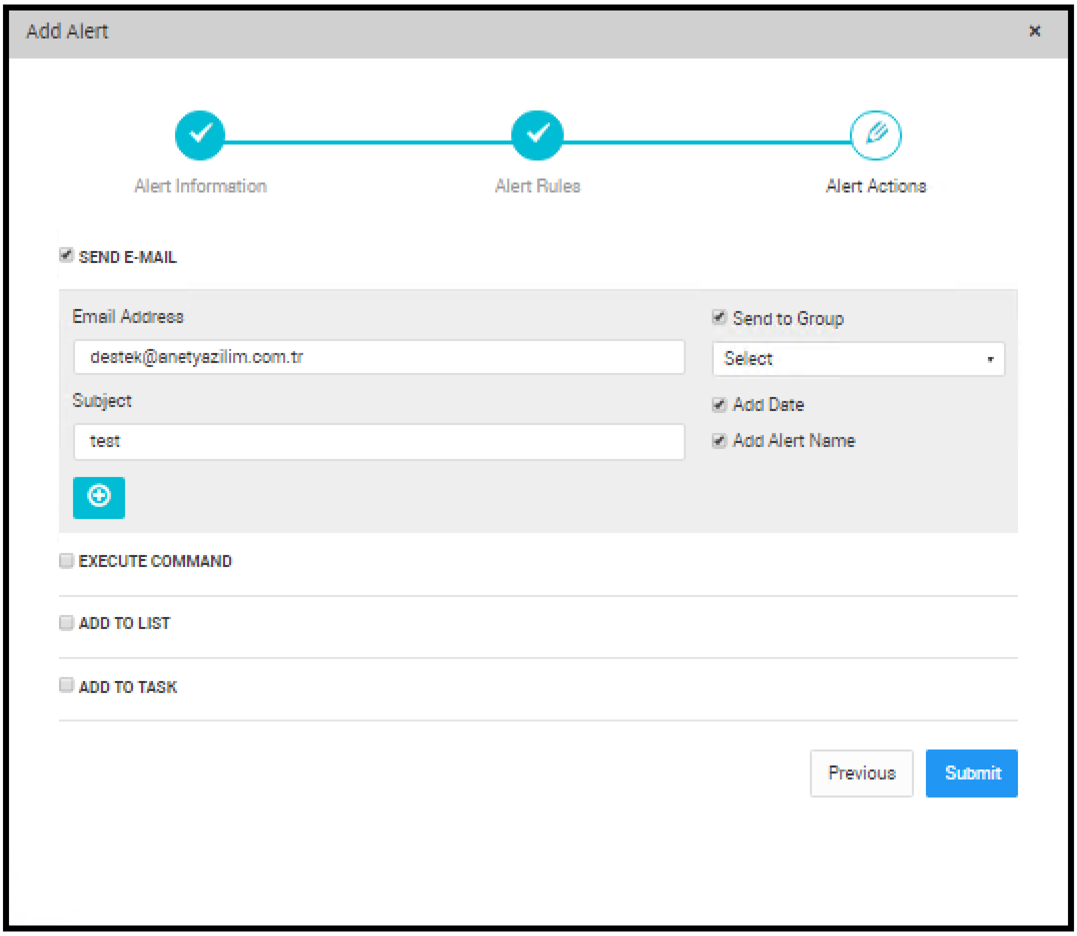


Add Alert

Add Rule

	Rule Name	Rule Description
☑	test	test

7. Mark Send E-mail so that the alert can be sent to the user via E-mail
8. Mark Send to Group so that the alert can be sent to group via E-mail
9. Enter a subject line for E-mail
10. Mark Add Date and Add Alert Name to include date and alert name in the E-mail



☑ SEND E-MAIL

Email Address: destek@anetyazilim.com.tr

Subject: test

☑ Send to Group: Select

☑ Add Date

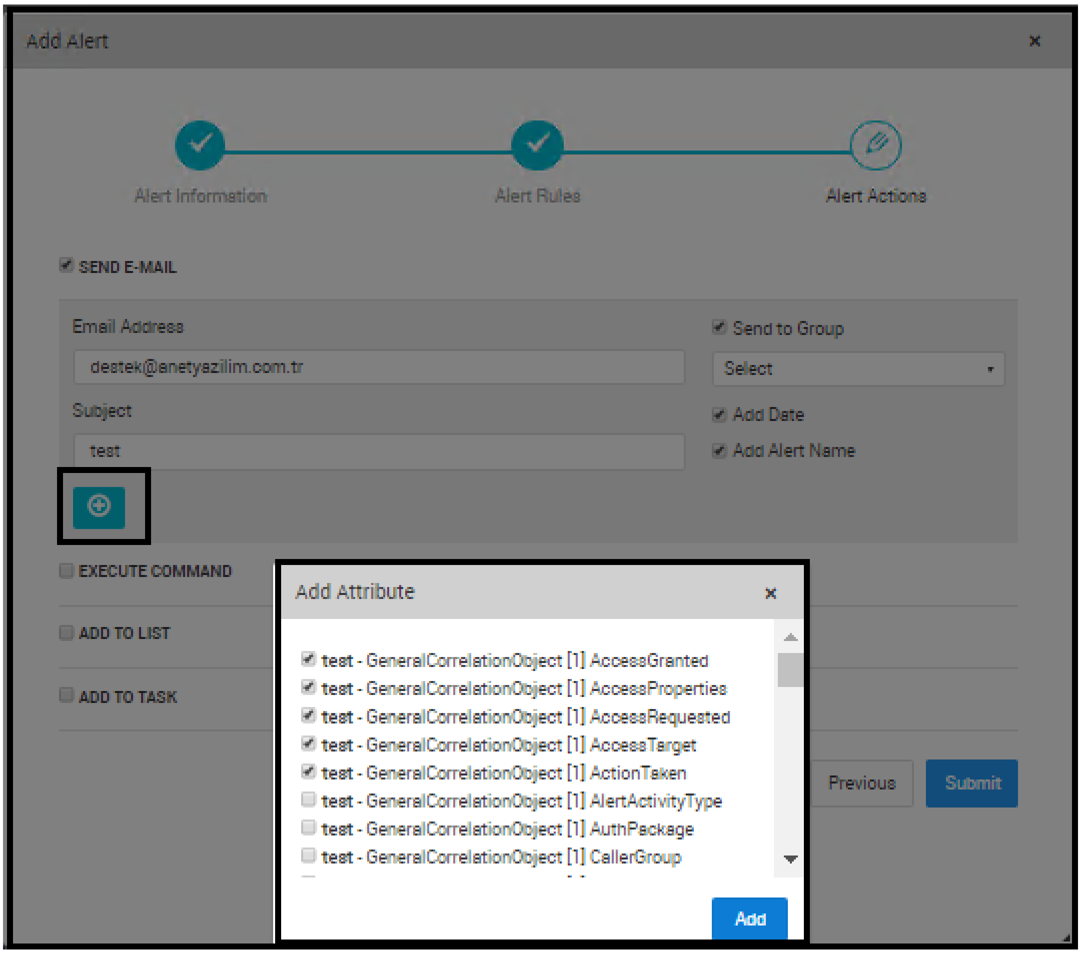
☑ Add Alert Name

□ EXECUTE COMMAND

□ ADD TO LIST

□ ADD TO TASK

11. Select Add Attributes to add attributes to E-mail



Add Alert

Alert Information · Alert Rules · Alert Actions

☑ SEND E-MAIL

Email Address: destek@anetyazilim.com.tr

Subject: test

☑ Send to Group

Select

☑ Add Date

☑ Add Alert Name

□ EXECUTE COMMAND

□ ADD TO LIST

□ ADD TO TASK

Add Attribute

☑ test - GeneralCorrelationObject [1] AccessGranted

☑ test - GeneralCorrelationObject [1] AccessProperties

☑ test - GeneralCorrelationObject [1] AccessRequested

☑ test - GeneralCorrelationObject [1] AccessTarget

☑ test - GeneralCorrelationObject [1] ActionTaken

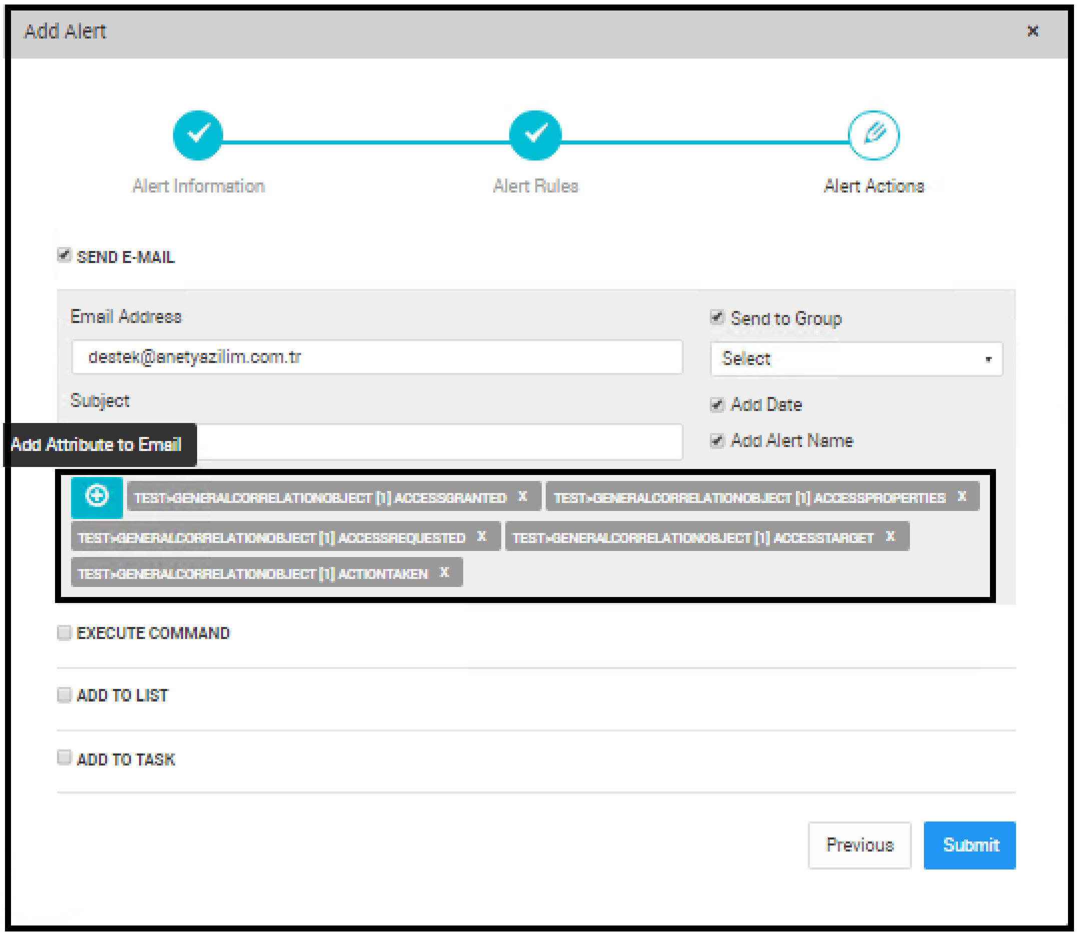
□ test - GeneralCorrelationObject [1] AlertActivityType

□ test - GeneralCorrelationObject [1] AuthPackage

□ test - GeneralCorrelationObject [1] CallerGroup

12. Select the relevant attributes

13. Select Add button to add the selected attributes



Add Alert ×

Alert Information — Alert Rules — Alert Actions

☑ SEND E-MAIL

Email Address: destek@anetyazilim.com.tr

☑ Send to Group: Select

Subject

☑ Add Date

☑ Add Alert Name

Add Attribute to Email

TEST>GENERALCORRELATIONOBJECT [1] ACCESSGRANTED X
TEST>GENERALCORRELATIONOBJECT [1] ACCESSPROPERTIES X
TEST>GENERALCORRELATIONOBJECT [1] ACCESSREQUESTED X
TEST>GENERALCORRELATIONOBJECT [1] ACCESSTARGET X
TEST>GENERALCORRELATIONOBJECT [1] ACTIONTAKEN X

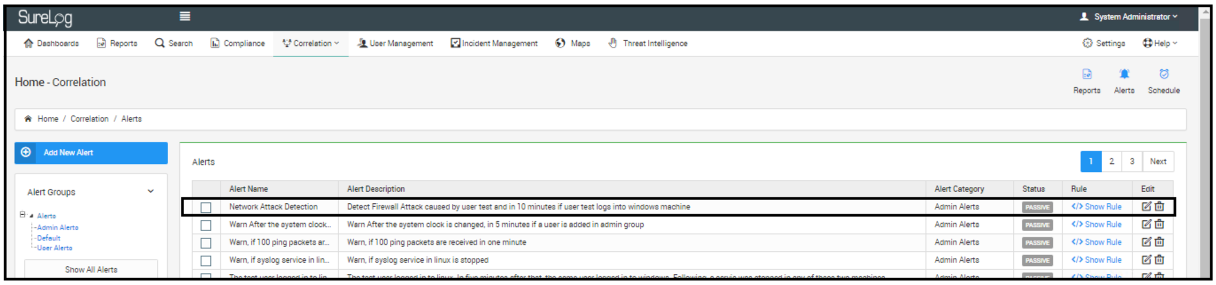
□ EXECUTE COMMAND

□ ADD TO LIST

□ ADD TO TASK

14. Select Submit Tab to save the alert

15. Check that the alert is appeared in the Alerts list as shown in the figure below:



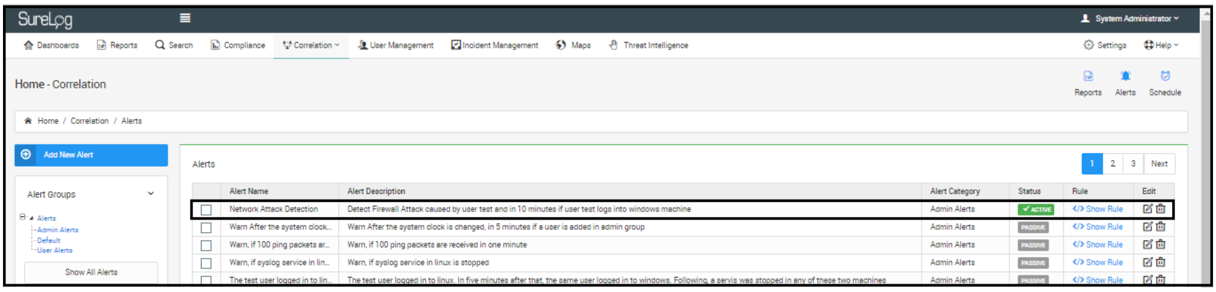
Home - Correlation

Home / Correlation / Alerts

Alerts

	Alert Name	Alert Description	Alert Category	Status	Rule	Edit
□	Network Attack Detection	Detect Firewall Attack caused by user test and in 10 minutes if user test logs into windows machine	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn After the system clock...	Warn After the system clock is changed, in 5 minutes if a user is added in admin group	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if 100 ping packets ar...	Warn, if 100 ping packets are received in one minute	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if syslog service in lin...	Warn, if syslog service in linux is stopped	Admin Alerts	PASSIVE	</> Show Rule	

16. Mark the check box in front of the alert name and select Activate Selected button to activate the alert.



Home - Correlation

Home / Correlation / Alerts

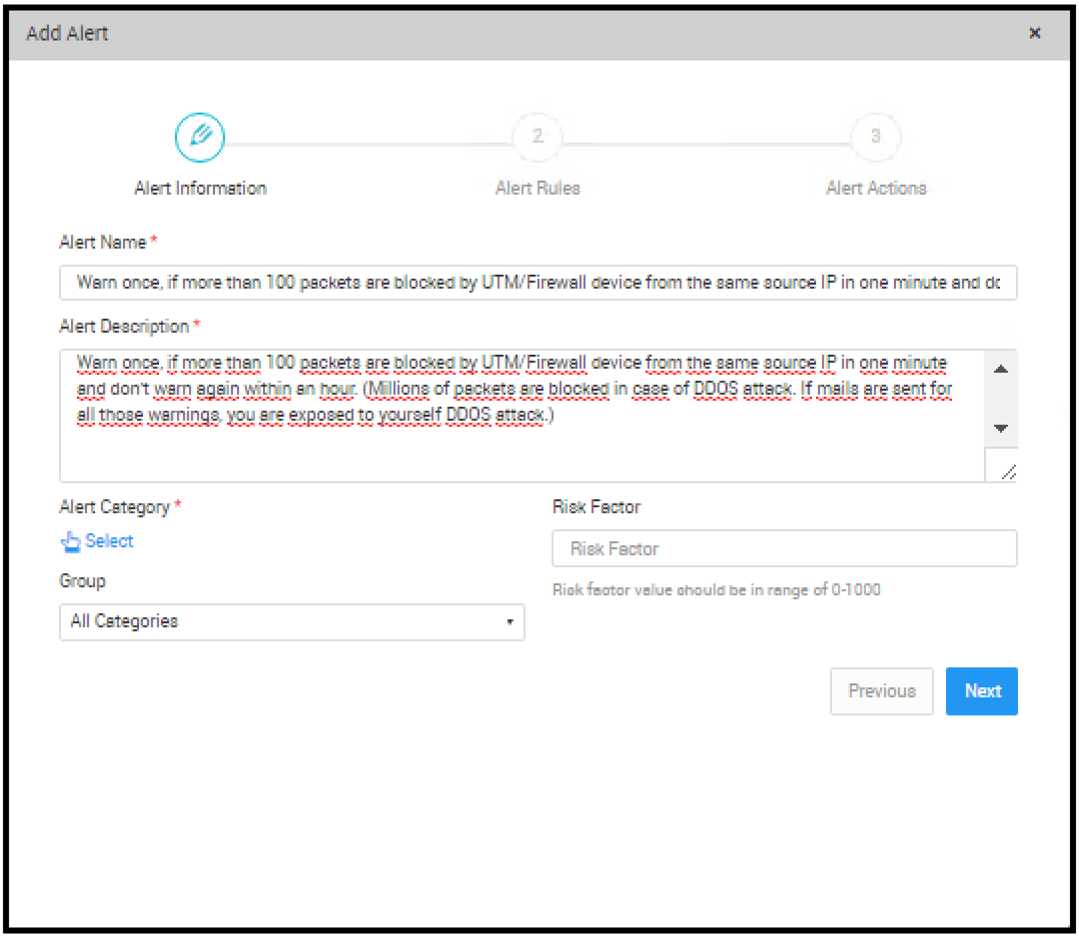
Alerts

	Alert Name	Alert Description	Alert Category	Status	Rule	Edit
□	Network Attack Detection	Detect Firewall Attack caused by user test and in 10 minutes if user test logs into windows machine	Admin Alerts	✓ ACTIVE	</> Show Rule	
□	Warn After the system clock...	Warn After the system clock is changed, in 5 minutes if a user is added in admin group	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if 100 ping packets ar...	Warn, if 100 ping packets are received in one minute	Admin Alerts	PASSIVE	</> Show Rule	
□	Warn, if syslog service in lin...	Warn, if syslog service in linux is stopped	Admin Alerts	PASSIVE	</> Show Rule	
□	The test user logged in to lin...	The test user logged in to linux. In five minutes after that, the same user logged in to windows. Following, a servis was stopped in any of these two machines	Admin Alerts	PASSIVE	</> Show Rule	

The users can set suspend time for a rule to limit mail sending rate. This situation can be explained with the following sample scenario:

Warn once, if more than 100 packets are blocked by UTM/Firewall device from the same source IP in one minute and don’t warn again within an hour. (Millions of packets are blocked in case of DDOS attack. If mails are sent for all those warnings, you are exposed to yourself DDOS attack.)

The user can set suspend time as 1 hour for the sample scenario explained above as shown in the figure below:



Alert Name *

Warn once, if more than 100 packets are blocked by UTM/Firewall device from the same source IP in one minute and dc

Alert Description *

Warn once, if more than 100 packets are blocked by UTM/Firewall device from the same source IP in one minute and don't warn again within an hour. (Millions of packets are blocked in case of DDOS attack. If mails are sent for all those warnings, you are exposed to yourself DDOS attack.)

Alert Category *

Select

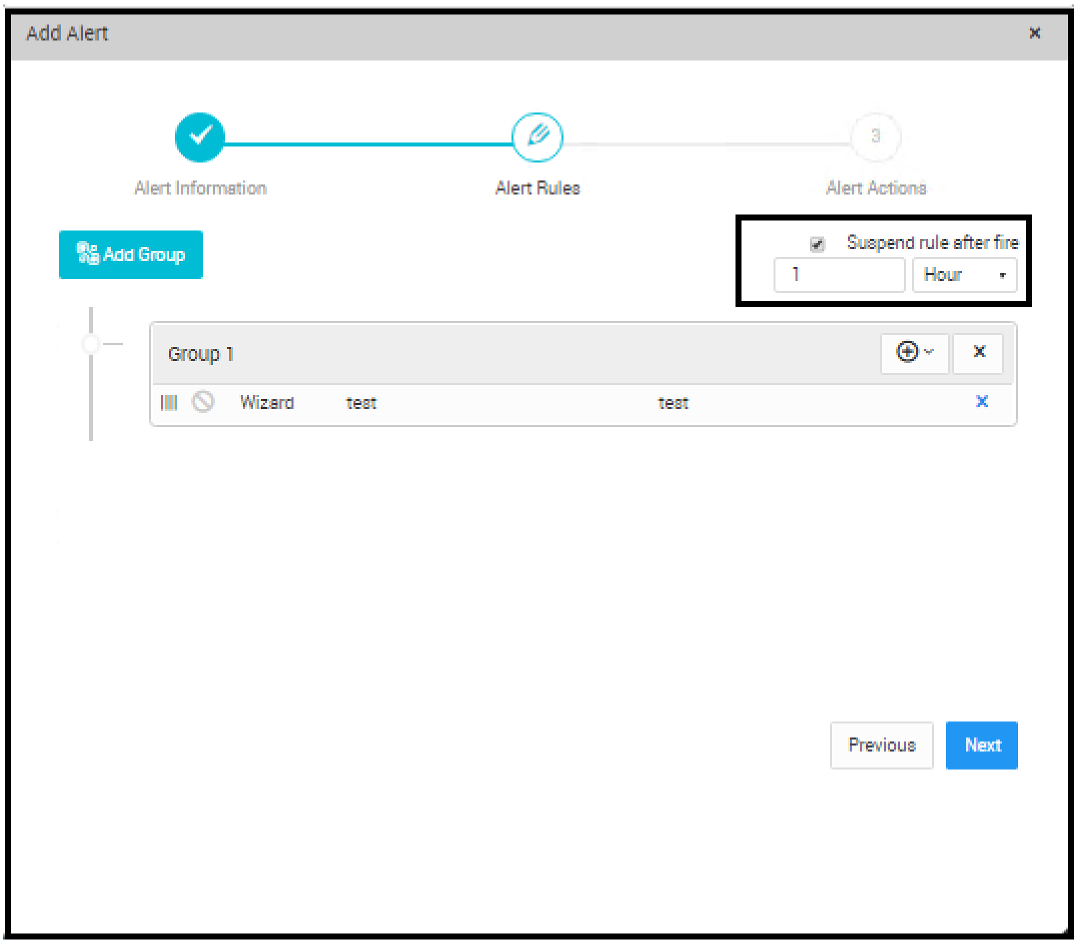
Group

All Categories

Risk Factor

Risk Factor

Risk factor value should be in range of 0-1000



Add Alert

Alert Information · Alert Rules · Alert Actions

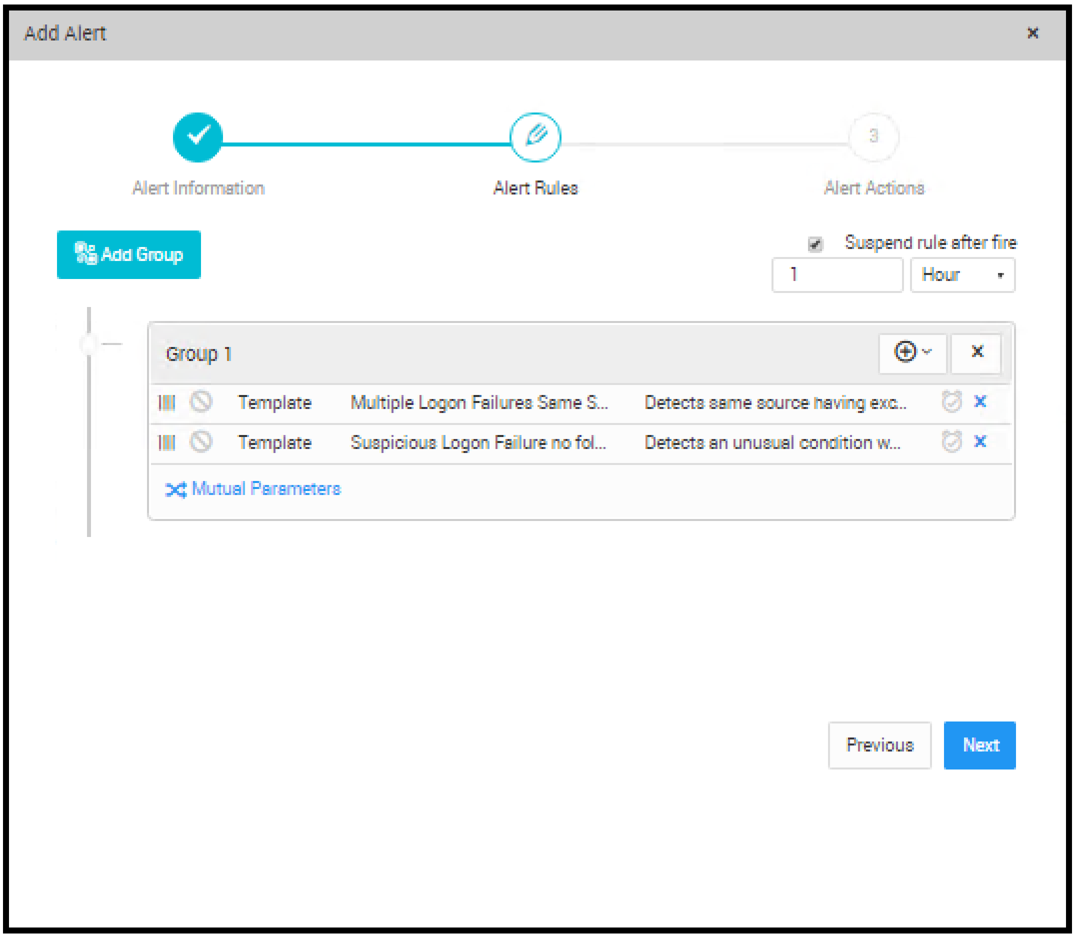
☑ Suspend rule after fire

1 Hour

Group 1

Wizard test test

The user can combine multiple correlation rules in an alert as shown in the figure below:



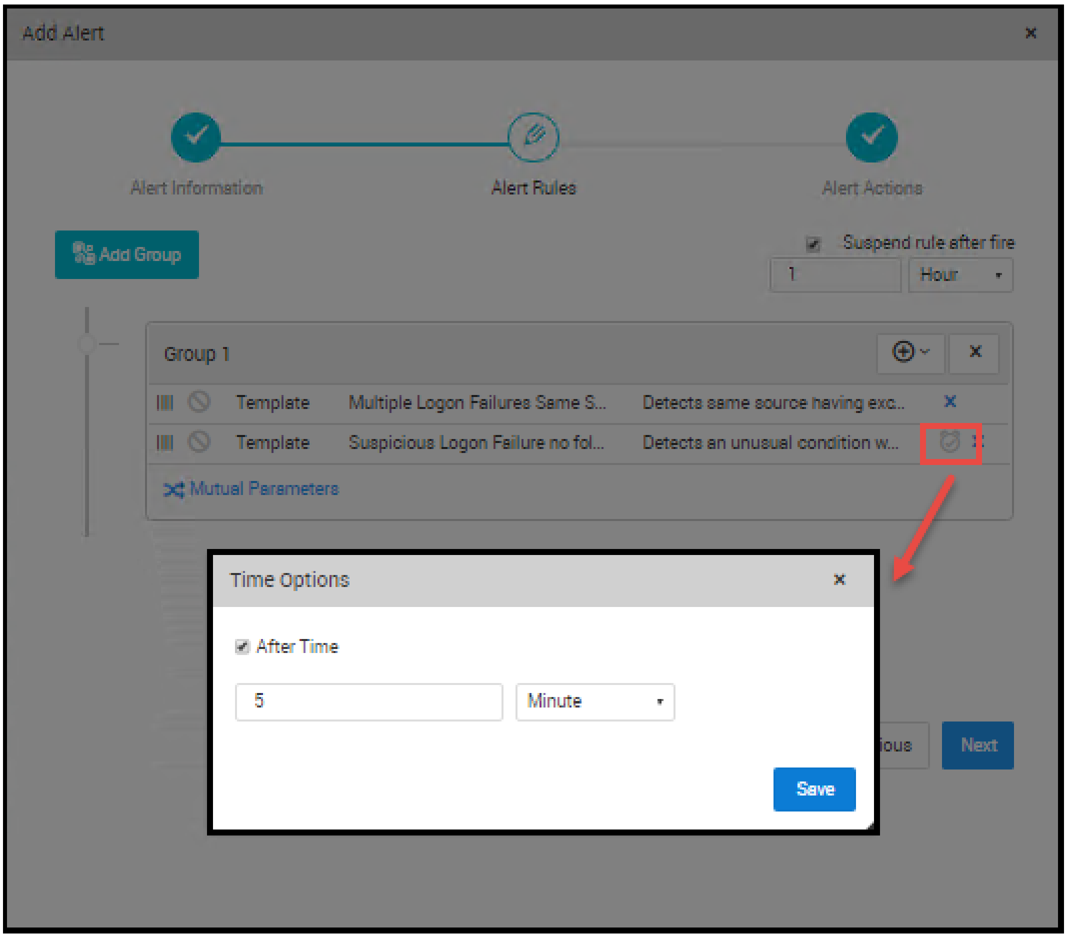
Add Alert

☑ Suspend rule after fire: 1 Hour

Group 1

Template	Multiple Logon Failures Same S...	Detects same source having exc...	×
Template	Suspicious Logon Failure no fol...	Detects an unusual condition w...	×

The user can add time period for consecutive rules as shown in the figure below:



Add Alert

☑ Suspend rule after fire

1 Hour

Group 1

Template	Multiple Logon Failures Same S...	Detects same source having exc...
Template	Suspicious Logon Failure no fol...	Detects an unusual condition w...

Time Options

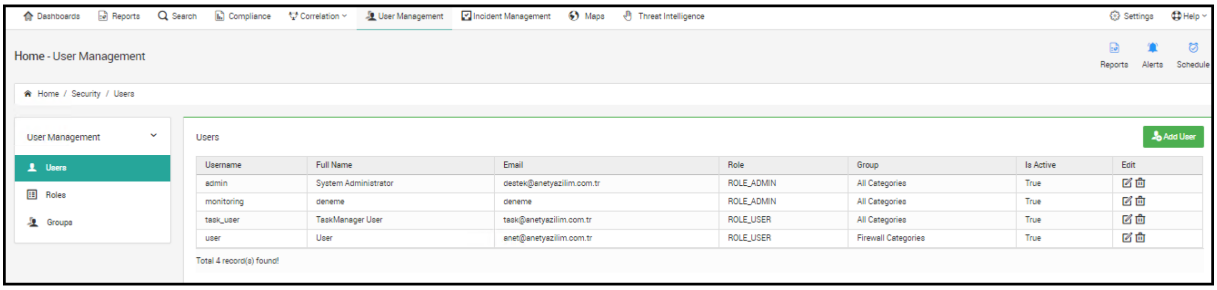
☑ After Time

5 Minute

According to figure shown above, the first rule will run firstly and in 5 minutes the second rule will run. The running of all these rules triggers the alert.

Chapter 11: User Management

The new user accounts can be created in SureLog and the management domain of each user account can be limited for specific tasks. We can either add the users which handle similar tasks in the system to standard groups such as All Categories, Firewall Categories, and Default or to custom created groups such as Linux, Network, System, and Security as shown in the following figure. We can add specific roles to groups to limit users domain areas in SureLog.



Home - User Management

Home / Security / Users

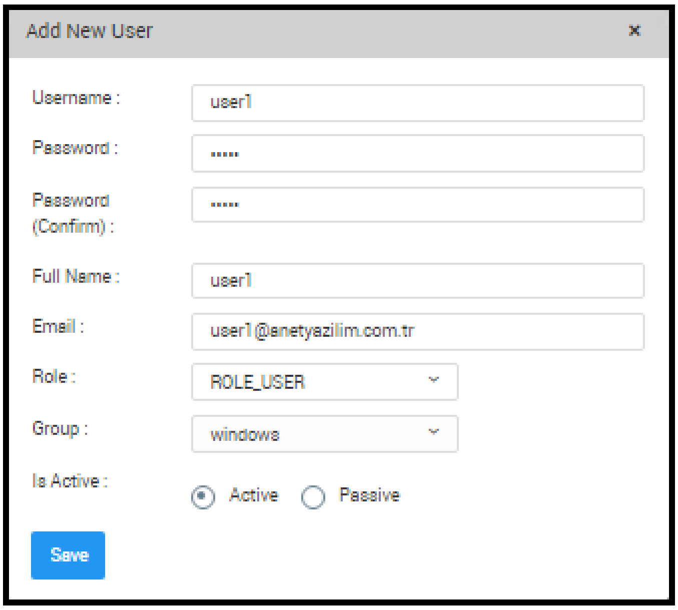
Users

Username	Full Name	Email	Role	Group	Is Active	Edit
admin	System Administrator	destek@anetyazilim.com.tr	ROLE_ADMIN	All Categories	True	
monitoring	deneme	deneme	ROLE_ADMIN	All Categories	True	
task_user	TaskManager User	task@anetyazilim.com.tr	ROLE_USER	All Categories	True	
user	User	anet@anetyazilim.com.tr	ROLE_USER	Firewall Categories	True	

Total 4 record(s) found!

To create a new user:

1. Select Add User button
2. Enter the following configurations into the appropriate fields:



Add New User ×

Username : user1

Password : •••••

Password (Confirm) : •••••

Full Name : user1

Email : user1@anetyazilim.com.tr

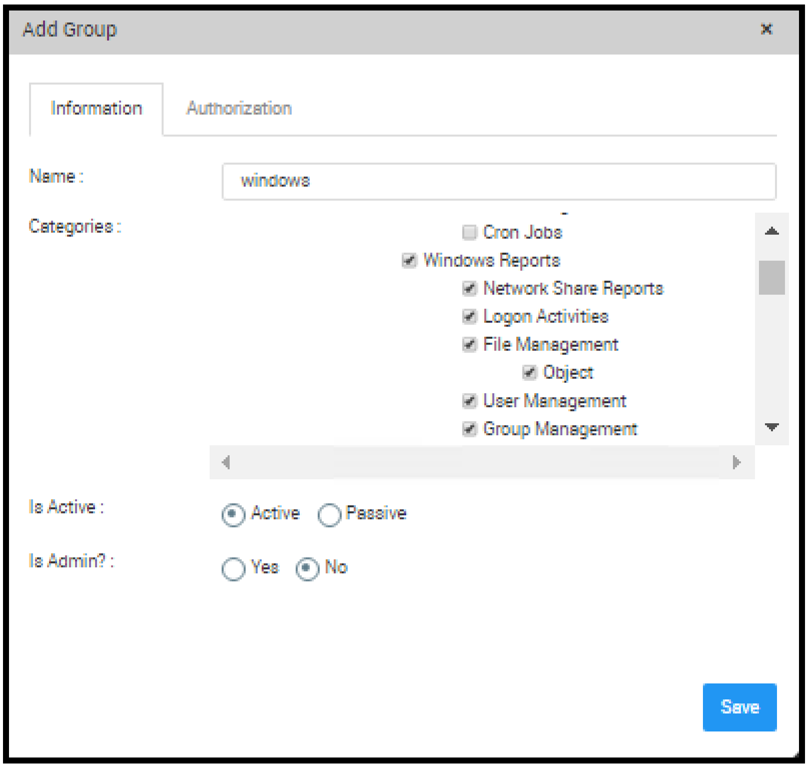
Role : ROLE_USER

Group : windows

Is Active : ● Active ○ Passive

To create a new group:

1. Select Group from User Management
2. Enter the following configurations into the appropriate fields:



Add Group ×

Name : windows

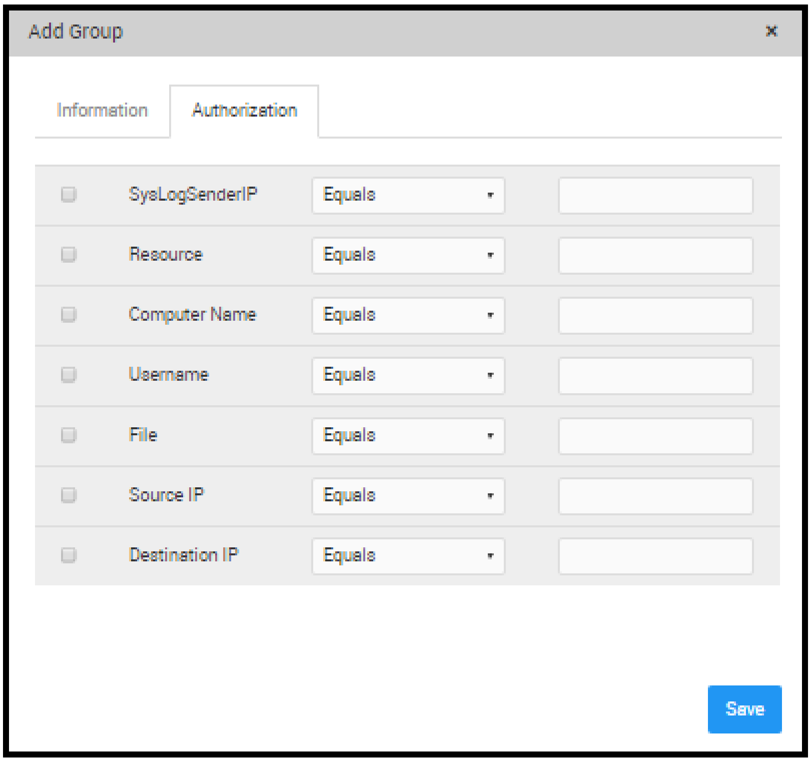
Categories :

- □ Cron Jobs
- ☑ Windows Reports
  - ☑ Network Share Reports
  - ☑ Logon Activities
  - ☑ File Management
    - ☑ Object
  - ☑ User Management
  - ☑ Group Management

Is Active : ● Active ○ Passive

Is Admin? : ○ Yes ● No

The user can be authorized on from which sources they will get logs as shown in the figure below:



Add Group ×

Information | Authorization

□	SysLogSenderIP	Equals ▾	
□	Resource	Equals ▾	
□	Computer Name	Equals ▾	
□	Username	Equals ▾	
□	File	Equals ▾	
□	Source IP	Equals ▾	
□	Destination IP	Equals ▾	

Chapter 12: Incident Management

Incident management (IcM) is describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence. These incidents within a structured organization are normally dealt with by either an Incident Response Team (IRT), or an Incident Management Team (IMT). These are often designated before hand, or during the event and are placed in control of the organization whilst the incident is dealt with, to restore normal functions.

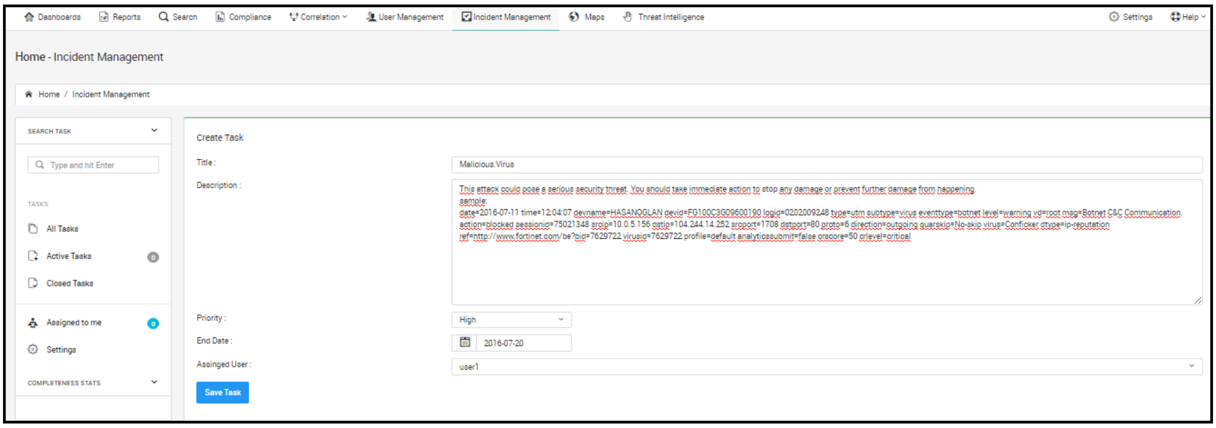
An incident is an event that could lead to loss of, or disruption to, an organization's operations, services or functions. If not managed an incident can escalate into an emergency, crisis or a disaster. Incident management is therefore the process of limiting the potential disruption caused by such an event, followed by a return to business as usual.

From ITIL point of view, the activities of Incident Management are:

- **Identification** - detect or reported the incident
- **Registration** - the incident is registered in an ICM System
- **Categorization** - the incident is categorized by priority, SLA etc. attributes defined above
- **Prioritization** - the incident is prioritized for better utilization of the resources and the Support Staff time
- **Diagnosis** - reveal the full symptom of the incident
- **Escalation** - should the Support Staff need support from other organizational units
- **Investigation and diagnosis** - if no existing solution from the past could be found the incident is investigated and root cause found
- **Resolution and recovery** - once the solution is found the incident is resolved
- **Incident closure** - the registry entry of the incident in the ICM System is closed by providing the end-status of the incident

Example:

When you detect a problem Malicious.Virus via periviously adjusted as alarm or scheduled report, you can create a task as below,



Create Task

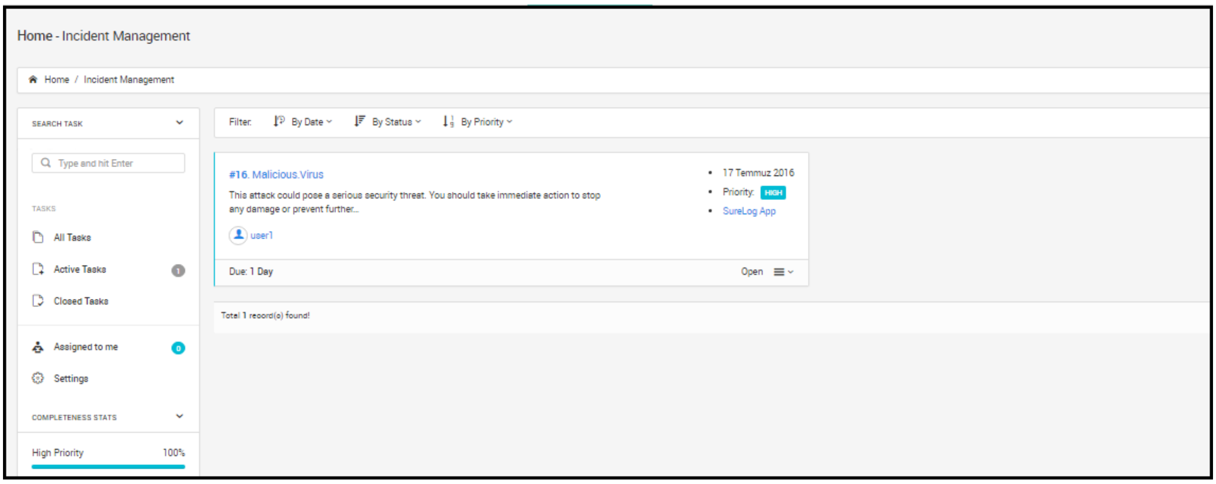
Title : Malicious.Virus

Description : This attack could pose a serious security threat. You should take immediate action to stop any damage or prevent further damage from happening.
sample:
date=2016-07-11 time=12:04:07 devname=HASANOGLAN devid=FG100C3G09600190 logid=0202009248 type=utm subtype=virus eventtype=botnet level=warning vd=root msg=Botnet C&C Communication. action=blocked sessionid=75021348 srcip=10.0.5.156 dstip=104.244.14.252 srcport=1708 dstport=80 proto=6 direction=outgoing quarskip=No-skip virus=Conficker dtype=ip-reputation ref=http://www.fortinet.com/be?bid=7629722 virusid=7629722 profile=default analyticssubmit=false crscore=50 crlevel=critical

Priority : High

End Date : 2016-07-20

Assinged User : user1



#16. Malicious.Virus

This attack could pose a serious security threat. You should take immediate action to stop any damage or prevent further...

user1

- 17 Temmuz 2016
- Priority: HIGH
- SureLog App

Due: 1 Day   Open

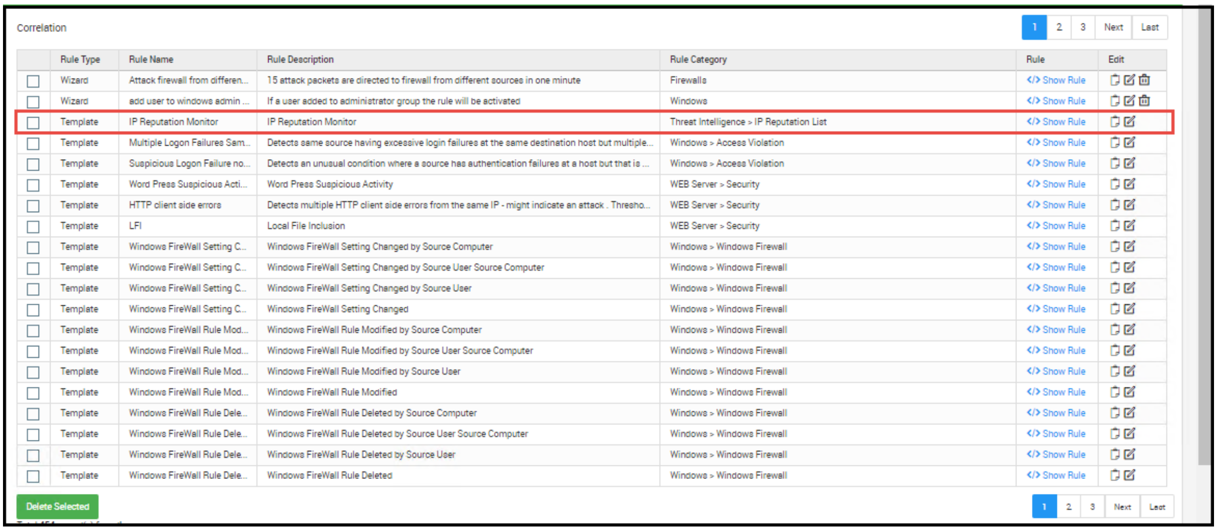
Total 1 record(s) found!

High Priority 100%

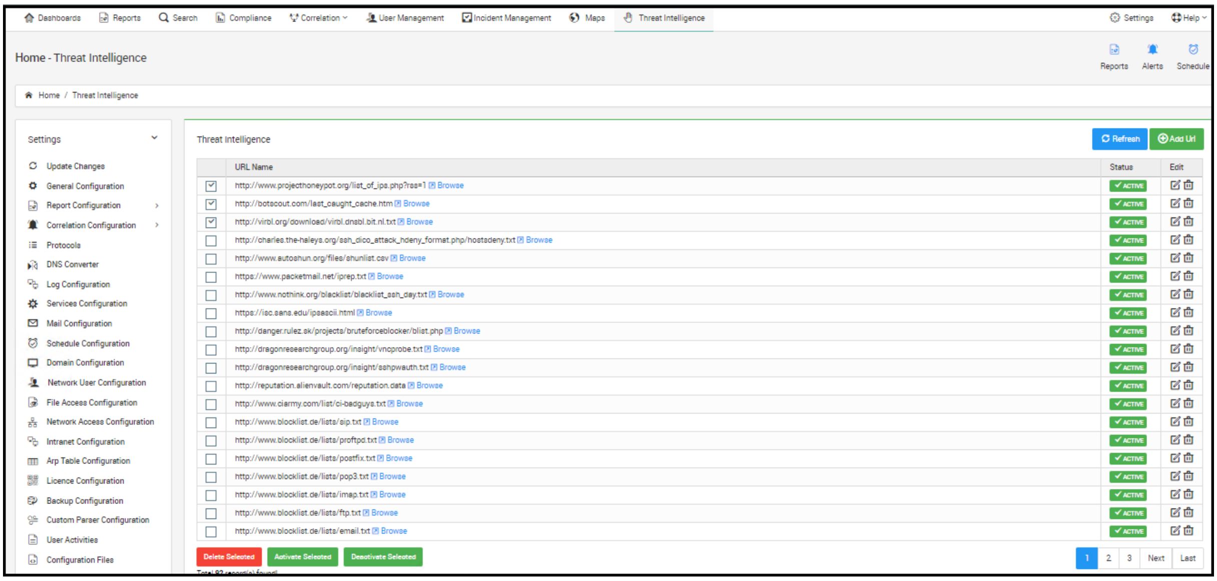
Chapter 13: Threat Intelligence

The total “campaign” involved in an advanced threat scenario may lead us to ask such questions as: “Who is targeting us?” “What methods are they using?” and “What systems are they after?” Understanding what you want to know about threat actors and their methods, and how to prevent or detect attacks, can help immensely when shaping policies and actions and allotting time to mitigate.

When IP Reputation Monitor correlation rules is triggered ,source and destination IPs are search in threat intelligence URL’s and warning us via e-mail.



	Rule Type	Rule Name	Rule Description	Rule Category	Rule	Edit
□	Wizard	Attack firewall from differen...	15 attack packets are directed to firewall from different sources in one minute	Firewalls	</> Show Rule	
□	Wizard	add user to windows admin ...	If a user added to administrator group the rule will be activated	Windows	</> Show Rule	
□	Template	IP Reputation Monitor	IP Reputation Monitor	Threat Intelligence > IP Reputation List	</> Show Rule	
□	Template	Multiple Logon Failures Sam...	Detects same source having excessive login failures at the same destination host but multiple...	Windows > Access Violation	</> Show Rule	
□	Template	Suspicious Logon Failure no...	Detects an unusual condition where a source has authentication failures at a host but that is ...	Windows > Access Violation	</> Show Rule	
□	Template	Word Press Suspicious Acti...	Word Press Suspicious Activity	WEB Server > Security	</> Show Rule	
□	Template	HTTP client side errors	Detects multiple HTTP client side errors from the same IP - might indicate an attack . Thresho...	WEB Server > Security	</> Show Rule	
□	Template	LFI	Local File Inclusion	WEB Server > Security	</> Show Rule	
□	Template	Windows FireWall Setting C...	Windows FireWall Setting Changed by Source Computer	Windows > Windows Firewall	</> Show Rule	
□	Template	Windows FireWall Setting C...	Windows FireWall Setting Changed by Source User Source Computer	Windows > Windows Firewall	</> Show Rule	
□	Template	Windows FireWall Setting C...	Windows FireWall Setting Changed by Source User	Windows > Windows Firewall	</> Show Rule	
□	Template	Windows FireWall Setting C...	Windows FireWall Setting Changed	Windows > Windows Firewall	</> Show Rule	
□	Template	Windows FireWall Rule Mod...	Windows FireWall Rule Modified by Source Computer	Windows > Windows Firewall	</> Show Rule	
□	Template	Windows FireWall Rule Mod...	Windows FireWall Rule Modified by Source User Source Computer	Windows > Windows Firewall	</> Show Rule	
□	Template	Windows FireWall Rule Mod...	Windows FireWall Rule Modified by Source User	Windows > Windows Firewall	</> Show Rule	
□	Template	Windows FireWall Rule Mod...	Windows FireWall Rule Modified	Windows > Windows Firewall	</> Show Rule	
□	Template	Windows FireWall Rule Dele...	Windows FireWall Rule Deleted by Source Computer	Windows > Windows Firewall	</> Show Rule	
□	Template	Windows FireWall Rule Dele...	Windows FireWall Rule Deleted by Source User Source Computer	Windows > Windows Firewall	</> Show Rule	
□	Template	Windows FireWall Rule Dele...	Windows FireWall Rule Deleted by Source User	Windows > Windows Firewall	</> Show Rule	
□	Template	Windows FireWall Rule Dele...	Windows FireWall Rule Deleted	Windows > Windows Firewall	</> Show Rule	



	URL Name	Status	Edit
☑	http://www.projecthoneypot.org/list_of_ips.php?rss=1 Browse	✓ ACTIVE	
☑	http://botscout.com/last_caught_cache.htm Browse	✓ ACTIVE	
☑	http://virbl.org/download/virbl.dnsbl.bit.nl.txt Browse	✓ ACTIVE	
□	http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt Browse	✓ ACTIVE	
□	http://www.autoshun.org/files/shunlist.csv Browse	✓ ACTIVE	
□	https://www.packetmail.net/iprep.txt Browse	✓ ACTIVE	
□	http://www.nothink.org/blacklist/blacklist_ssh_day.txt Browse	✓ ACTIVE	
□	https://isc.sans.edu/ipsascii.html Browse	✓ ACTIVE	
□	http://danger.rulez.sk/projects/bruteforceblocker/blist.php Browse	✓ ACTIVE	
□	http://dragonresearchgroup.org/insight/vncprobe.txt Browse	✓ ACTIVE	
□	http://dragonresearchgroup.org/insight/sshpwauth.txt Browse	✓ ACTIVE	
□	http://reputation.alienvault.com/reputation.data Browse	✓ ACTIVE	
□	http://www.ciarmy.com/list/ci-badguys.txt Browse	✓ ACTIVE	
□	http://www.blocklist.de/lists/sip.txt Browse	✓ ACTIVE	
□	http://www.blocklist.de/lists/proftpd.txt Browse	✓ ACTIVE	
□	http://www.blocklist.de/lists/postfix.txt Browse	✓ ACTIVE	
□	http://www.blocklist.de/lists/pop3.txt Browse	✓ ACTIVE	
□	http://www.blocklist.de/lists/imap.txt Browse	✓ ACTIVE	
□	http://www.blocklist.de/lists/ftp.txt Browse	✓ ACTIVE	
□	http://www.blocklist.de/lists/email.txt Browse	✓ ACTIVE	

Chapter 14: Settings

The settings section, the settings section includes all the necessary settings for configuring the SureLog. To mention for each setting in this section:

The Update Changes

The Update change section: updates the latest changes made in the system.

After any configuration change, the changes must be applied

Steps for filtering logs:

- Select Settings

- Then select the option to update changes

Changing Theme

Steps for changing theme, company name, Logo, etc.:

1. Select Settings
2. Enter General Settings

General Configuration

The report configuration section, you can take different reports such as statistics reports, Trend reports, Merge reports, Top list reports, and compliance as either word or pdf file format. You can also create your own report by using report tab. I will later on show how to create your own report.

General Configuration

In general configuration section, you can specify the title, theme, language, company name, logo, and date format.

Managing Protocol Groups

A protocol group is a set of related protocols typically used for a common purpose. The Protocol Groups link lets a user define protocols as well as protocol groups, so that they can identify traffic that is unique to their enterprise. Most of the common enterprise protocols are already included in SureLog under appropriate groups.

Some of the important protocol groups include the following:

Protocol Group Protocols included Description

Web HTTP, HTTPS and Gopher Includes protocols used to access IP traffic (the Internet)

Mail, POP, SMTP and IMAP includes protocols used to send or receive e-mail traffic

FTP, TFTP, FTPS includes protocols used to transfer files through FTP

Telnet   Includes protocols used to access telnet services

Click the Protocol Groups link to view the list of protocol groups and the corresponding protocols. The View by Group box lets the user view the list one protocol group at a time.

The Unassigned protocol group contains all the protocols that are not assigned to any group.

Some firewalls interpret protocols at Layer 4 (Application Layer), which means that a combination of port and protocol is identified as an application and written into the log file. For example, TCP Protocol on Port 80 is identified as HTTP traffic. Hence, HTTP is shown in the Protocols column. Other firewalls interpret protocols at Layer 3 only, which means only the port and protocol values are written into the log file. Therefore, in the same example, TCP/80 is shown in the Protocols column.

Operations on Protocols

Click the Delete icon next to a protocol to delete it from the protocol group. Once a protocol is deleted, all the database records related to that protocol will be deleted. Click the Move icon to move a protocol from the current protocol group to another.

Click the Add Protocol link or the add icon next to it to add a new protocol and assign it to a protocol group. Remember to enter the protocol value exactly as it appears in the log file. If you want to add it to a new protocol group, click the add icon next to the Protocol Group text box to add a New Protocol Group and enter the name of the new protocol group, followed by clicking the Add option. From the list of Available Protocol Identifiers, move the required protocols to the Selected Protocol Identifiers to be included in this protocol group. Please note that a protocol can belong to only one protocol group at a time.

Click the Add Protocol Identifier link or the Add icon to add a new protocol identifier.

Operations on Protocol Groups

Click the Add Protocol Group link or add icon next to it to add a new protocol group. In the pop-up window that is presented, enter a unique group name and a short description. From the list of protocols currently not assigned to any protocol group, choose the protocols to be included in this protocol group. Please note that a protocol can belong to only one protocol group at a time.

Select the protocol group from the list and click the Edit Protocol Group option or Edit icon to edit the properties of that protocol group. In the pop-up window that is presented, that user can edit the protocol group's description, add currently ungrouped protocols, or remove existing protocols from this protocol group.

To delete a protocol group, select the protocol group from the list and click the Delete Protocol Group link or the Delete icon next to it. The protocol group is deleted and all associated protocols are put in the Others protocol group.

DNS Converter

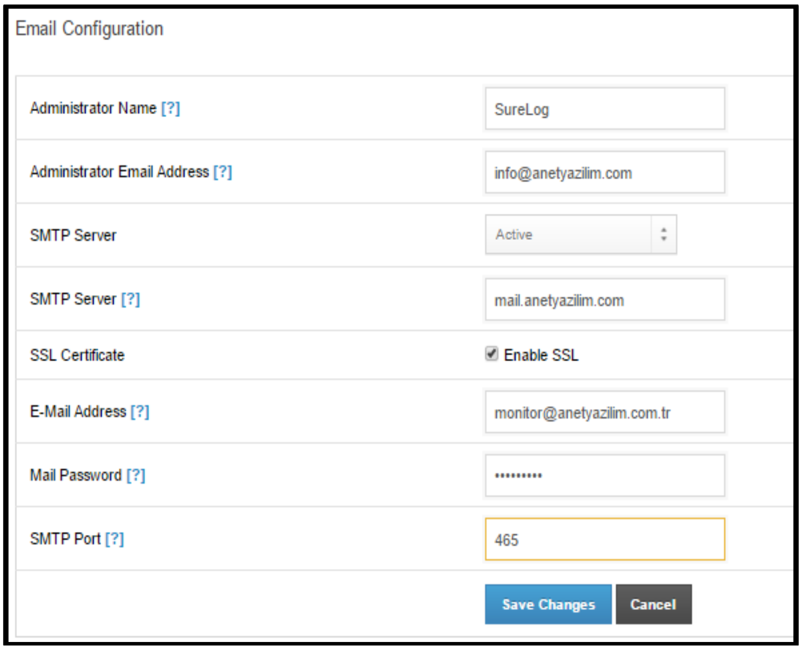
If a log doesn’t include hostname, reverse DNS lookup is done to determine hostname through to IP to hostname resolution process. This process has a negative impact on the performance of SureLog. Because, it communicates with DNS server to find out the hostname by making IP to hostname resolution. This causes the delay for SureLog. This configuration option is not used by default.

Mail Configuration

We configure mail settings from here. This way; for example, if something happens with log source, the system administrator is informed via email. In other words; after a correlation rule or a scheduled report runs, the system administrator is informed on what is happening in the log source through an email specified here. Moreover, the alerts generated by the system are sent to the email address specified in this part.

The sample mail configuration steps are shown in the figure:

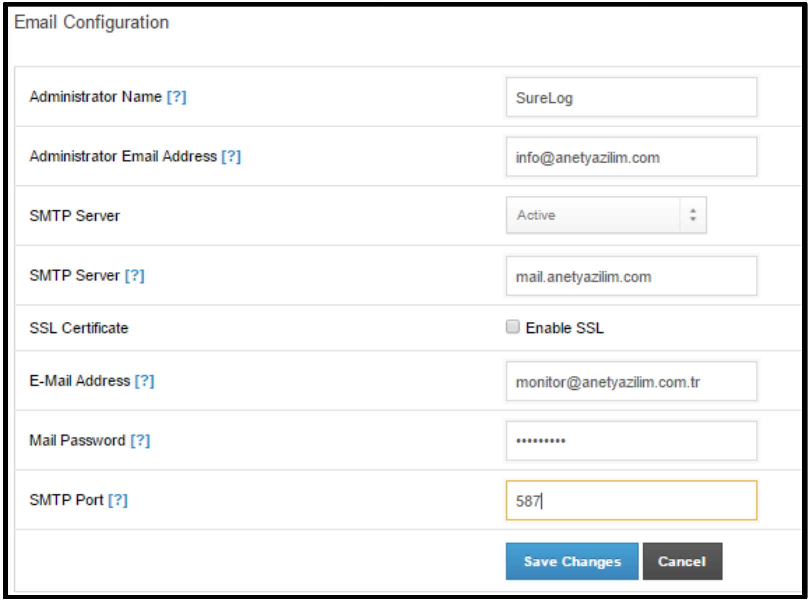
1. Select Settings in the view pane
2. Select Mail Configuration
3. Enter configurations shown in the figure below



Email Configuration

Administrator Name [?]	SureLog
Administrator Email Address [?]	info@anetyazilim.com
SMTP Server	Active
SMTP Server [?]	mail.anetyazilim.com
SSL Certificate	☑ Enable SSL
E-Mail Address [?]	monitor@anetyazilim.com.tr
Mail Password [?]	•••••••••
SMTP Port [?]	465

4. The configuration without using SSL is shown in the figure below:



Email Configuration

Administrator Name [?]	SureLog
Administrator Email Address [?]	info@anetyazilim.com
SMTP Server	Active
SMTP Server [?]	mail.anetyazilim.com
SSL Certificate	☐ Enable SSL
E-Mail Address [?]	monitor@anetyazilim.com.tr
Mail Password [?]	•••••••••
SMTP Port [?]	587

Log Configuration

In log configuration section, we define the log sources, through which SureLog collects logs. The logs are collected or sent with agent or agentless methods. If the logs are collected with an agentless method, we add log sources through Add Log tab. When we click Add Log tab, we see that we can collect with different logs as agent less such as syslog, textlog, snmp trap, WMI, and ftp.

The logs can also be collected by installing agent software, which collects the logs from the system, on which it is installed and sends them to SureLog either as syslog or textlog.

If the logs are collected through syslog, the logs are sent to SureLog through a listened port such as port514, 1514 etc which are mostly used. It is not important from which port the log comes. SureLog can collect syslog logs from any port configured. If the logs are collected as textlog, SureLog fetches to the log source after a specified time and collects the logs. I will later on mention about how to configure log sources via this Log Configuration section.

The Syslog Server Settings page lets a user manage the various virtual syslog servers set up to receive exported logs at different ports.

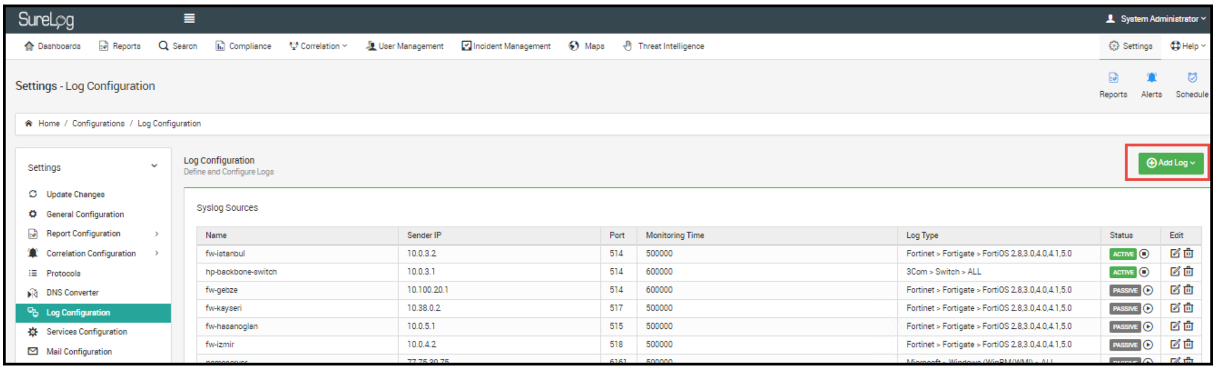
The defaulted listener ports for the Syslog server in SureLog are 514 and 1514. If the user's firewalls are exporting log files to either of these ports, no virtual syslog servers are required.

The Syslog Servers table shows the various virtual syslog servers set up so far, along with their IP address, listener port, and status. A user can delete a virtual Syslog server by clicking the Delete icon. Once a virtual Syslog server is deleted, the corresponding listener port is also freed. A user can also stop the Syslog collection by clicking the stop icon and restart the Syslog collection by clicking on the restart icon

Adding a New Log Collector

The **Settings** tab lets a user configure several system settings for the server running SureLog, as well as other settings. Follow the procedure given below to configure the new log collector:

- Select the **Settings** on the left side of the screen
- Select Add Log Tab



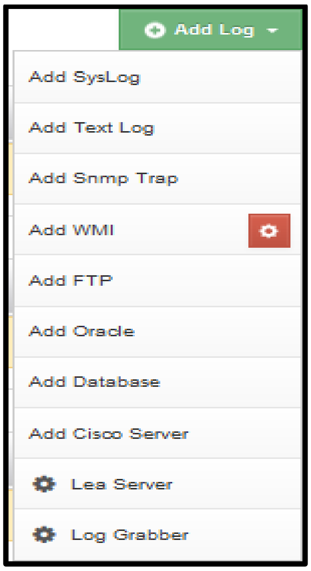
Settings - Log Configuration

Log Configuration
Define and Configure Logs

Syslog Sources

Name	Sender IP	Port	Monitoring Time	Log Type	Status	Edit
fw-istanbul	10.0.3.2	514	500000	Fortinet > Fortigate > FortiOS 2.8,3.0,4.0,4.1,5.0	ACTIVE	
hp-backbone-switch	10.0.3.1	514	600000	3Com > Switch > ALL	ACTIVE	
fw-gebze	10.100.20.1	514	600000	Fortinet > Fortigate > FortiOS 2.8,3.0,4.0,4.1,5.0	PASSIVE	
fw-kayseri	10.38.0.2	517	500000	Fortinet > Fortigate > FortiOS 2.8,3.0,4.0,4.1,5.0	PASSIVE	
fw-hasanoglan	10.0.5.1	515	500000	Fortinet > Fortigate > FortiOS 2.8,3.0,4.0,4.1,5.0	PASSIVE	
fw-izmir	10.0.4.2	518	500000	Fortinet > Fortigate > FortiOS 2.8,3.0,4.0,4.1,5.0	PASSIVE	

- Select Log source type



Adding a New Syslog Server

The Add Syslog Server box lets a user add a new virtual syslog server and begin listening for a new port for exported log files.

Enter a unique SysLog Server Name for the new virtual Syslog server and the listener port. The Host Name/IP Address field is currently not editable and automatically takes the IP address of the machine on which the SureLog server is running.

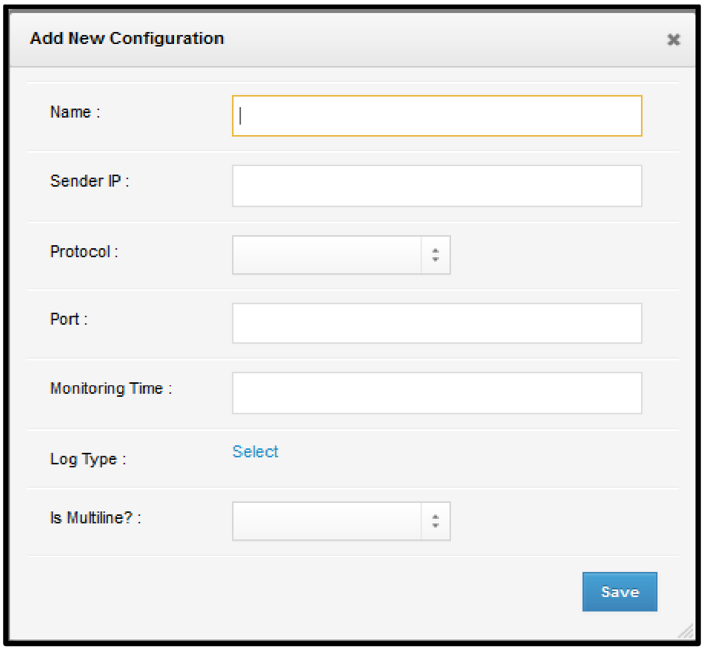
Click the Add Syslog Server option to add this virtual Syslog server and begin listening for log files at the specified port.

Configuring Log Source Availability Alerts

In SureLog, alerts can be triggered, if the log source stopped sending logs. The alert trigger is configurable and can even be setup to notify users through e-mail.

Follow the procedure below to configure the triggering of alert:

- Select the **Settings** tab in the Web Client. On the left side of the screen, the **Log Configuration** section is presented below the parameter section



Add New Configuration

Name :

Sender IP :

Protocol :

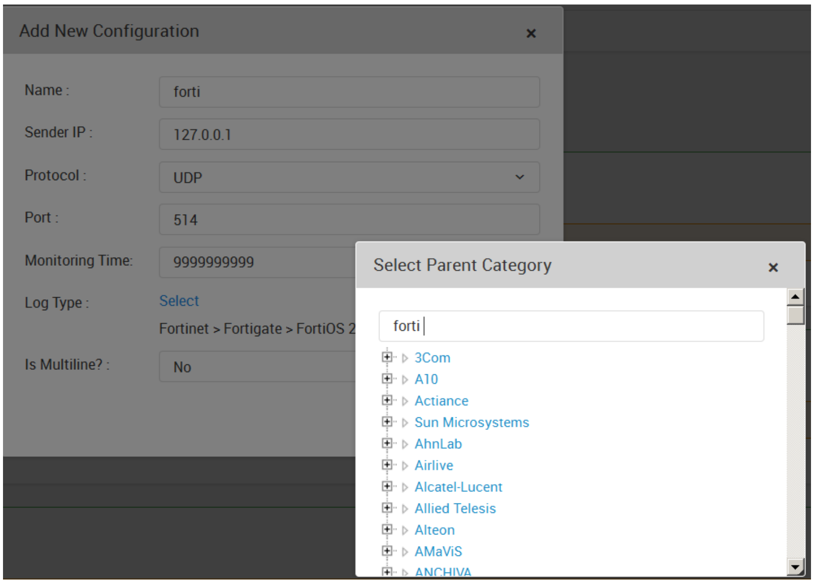
Port :

Monitoring Time :

Log Type : Select

Is Multiline? :

Columns	Description
Name	The name of the log source, for which this alert will be triggered, if the log source fails to send logs.
Sender IP	Log source IP
Protocol	Protocol
Port	Port
Monitoring Time (seconds)	The time duration within which a log should be received by the SureLog. Failure to receive a log within this time period will trigger this alert.
Log Type	Type of log source such as: Fortinate, Cisco, Windows
Is Multiline	Select as No



Add New Configuration

Name : forti

Sender IP : 127.0.0.1

Protocol : UDP

Port : 514

Monitoring Time: 9999999999

Log Type : Select

Fortinet > Fortigate > FortiOS 2

Is Multiline? : No

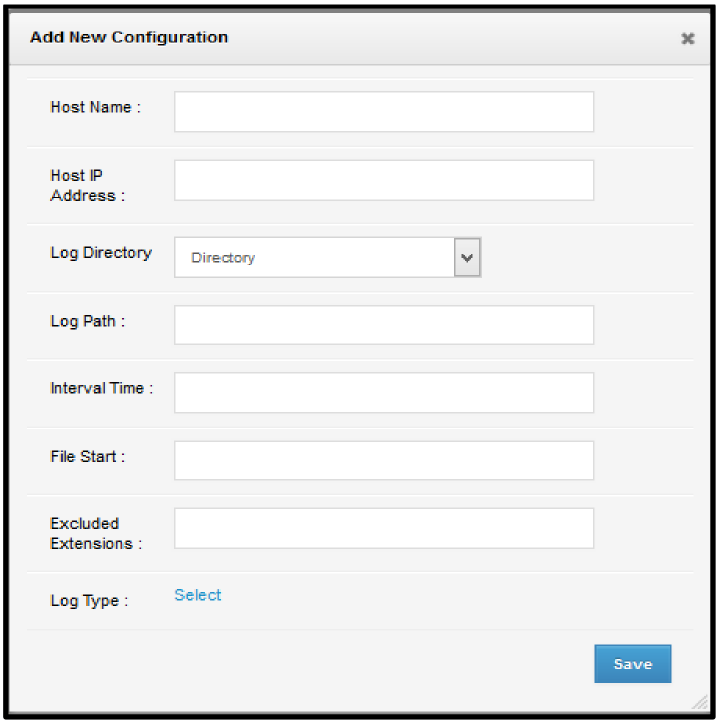
Select Parent Category

forti

Add Text Logs

Add Text Logs link lets a user import a log file from a local machine or remotely through DNS, DHCP, Exchange and such that.

SureLog monitors the file or directory for any changes in real-time. In addition, SureLog reads a file from the beginning or from a defined starting point.



Add New Configuration

Host Name :

Host IP Address :

Log Directory: Directory

Log Path :

Interval Time :

File Start :

Excluded Extensions :

Log Type : Select

Hostname: The name of the host from which the logs will be received.

Host IP Address: The IP address of the host from which the logs will be received.

Log Directory: The pattern of the log source in terms of file or directory

Log Path: A local or map network folder (UNC path) of the log file or directory

Interval Time: The period for change detection time (ms) in a log file or directory

File Start: The file name selection pattern for the file and directory monitor

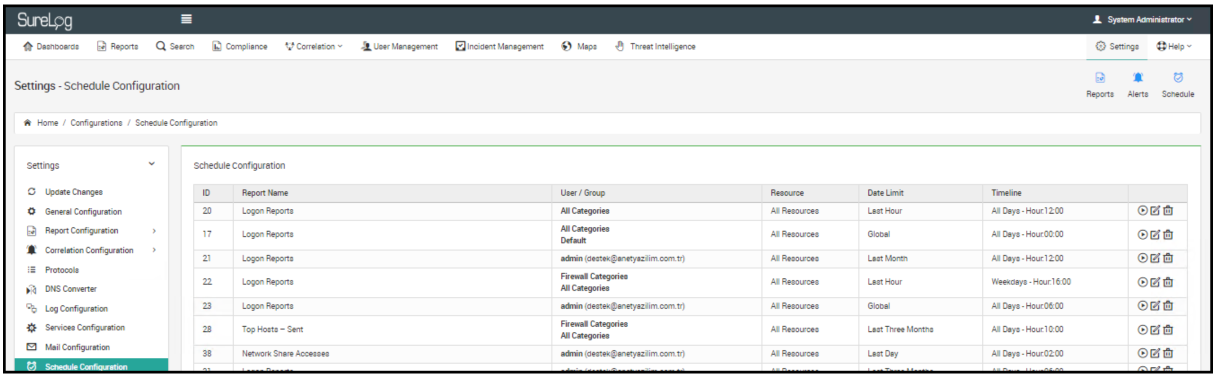
Excluded Extensions: The excluded extensions from file and directory monitoring

Log Type: Type of log source such as: Fortinate, Cisco, Windows

Schedule Configuration

Steps for scheduling reports

1. Select Settings
2. Schedule Configuration
3. The user can send the reports via email as shown in the figure below.

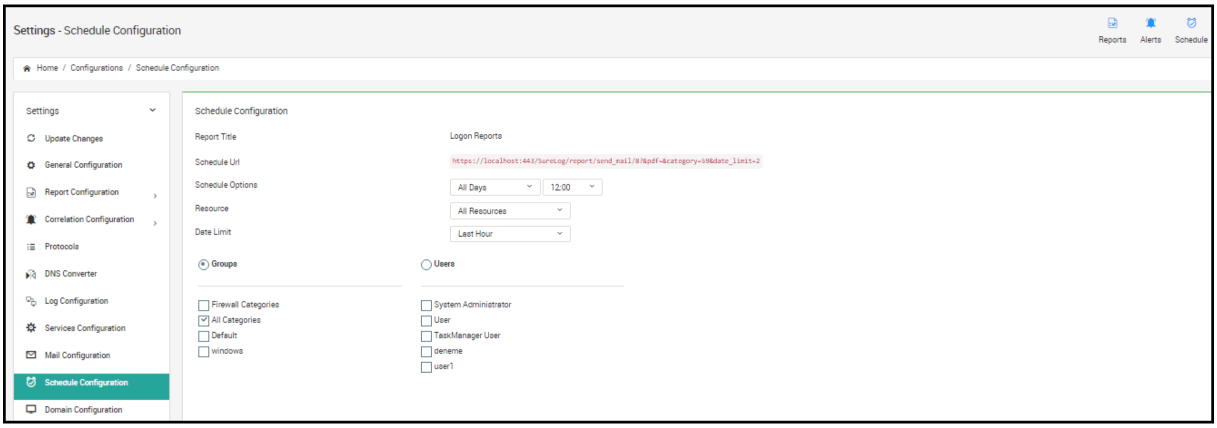


Settings - Schedule Configuration

Schedule Configuration

ID	Report Name	User / Group	Resource	Date Limit	Timeline
20	Logon Reports	**All Categories**	All Resources	Last Hour	All Days - Hour:12:00
17	Logon Reports	**All Categories** **Default**	All Resources	Global	All Days - Hour:00:00
21	Logon Reports	**admin** (destek@anetyazilim.com.tr)	All Resources	Last Month	All Days - Hour:12:00
22	Logon Reports	**Firewall Categories** **All Categories**	All Resources	Last Hour	Weekdays - Hour:16:00
23	Logon Reports	**admin** (destek@anetyazilim.com.tr)	All Resources	Global	All Days - Hour:06:00
28	Top Hosts – Sent	**Firewall Categories** **All Categories**	All Resources	Last Three Months	All Days - Hour:10:00
38	Network Share Accesses	**admin** (destek@anetyazilim.com.tr)	All Resources	Last Day	All Days - Hour:02:00

4. The user can edit the scheduled reports as shown in the figure below:



Settings - Schedule Configuration

Schedule Configuration

Report Title: Logon Reports

Schedule Url: https://localhost:443/SureLog/report/send_mail/8?&pdf-&category-59&date_limit-2

Schedule Options: All Days, 12:00

Resource: All Resources

Date Limit: Last Hour

● Groups

□ Firewall Categories
☑ All Categories
□ Default
□ windows

○ Users

□ System Administrator
□ User
□ TaskManager User
□ deneme
□ user1

5. The users can specify to which user or groups the reports will be sent as shown in the figure above

6. The user can also delete the scheduled report by selecting ✖ symbol in report view

Domain Configuration

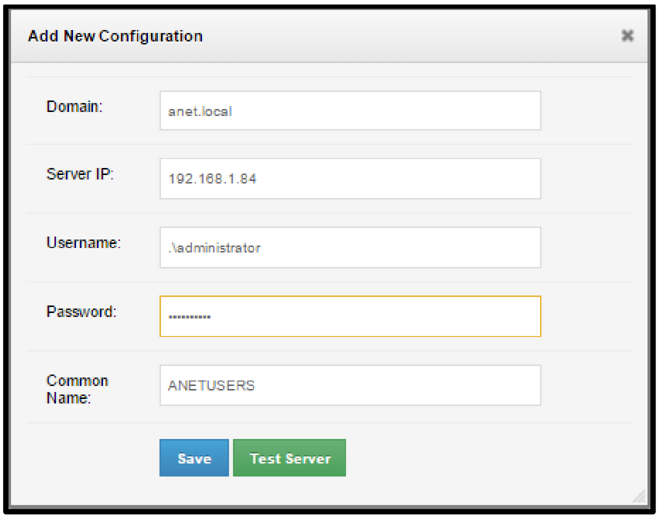
If we use Active Directory in our network, here we can add our domain. This way, for example, if we have an ANETUSERS organizational unit in the domain, then the logs for each computer in ANETUSERS OU are automatically collected through WMI without making WMI configuration setting for each computer in ANETUSERS OU. In this section, we can also add the servers individually.

In order to collect Windows events by WMI, the user has 2 options:

1. Configuring domain settings
2. Adding each log source individually

Steps for configuring domain:

1. Select Settings
2. Enter domain configuration
3. Select the Add Domain Server button



Add New Configuration

Domain: anet.local

Server IP: 192.168.1.84

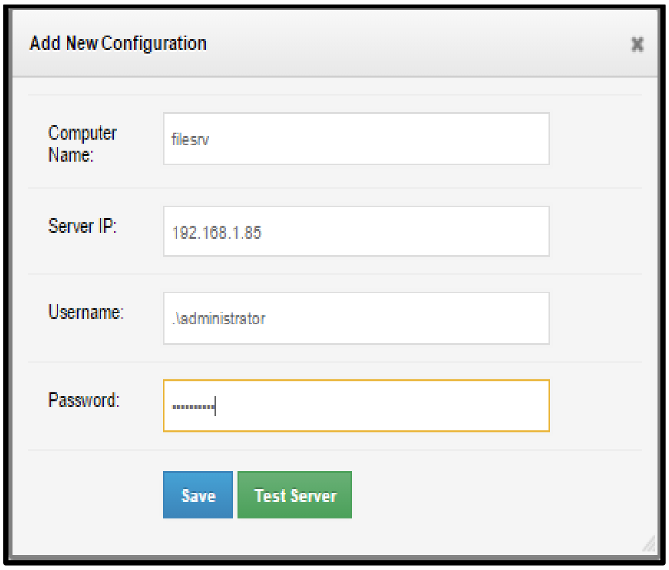
Username: .\administrator

Password: ....

Common Name: ANETUSERS

Steps for adding a Windows server:

1. Select Settings
2. Enter domain configuration
3. Select the Add Windows Server button



Add New Configuration

Computer Name: filesrv

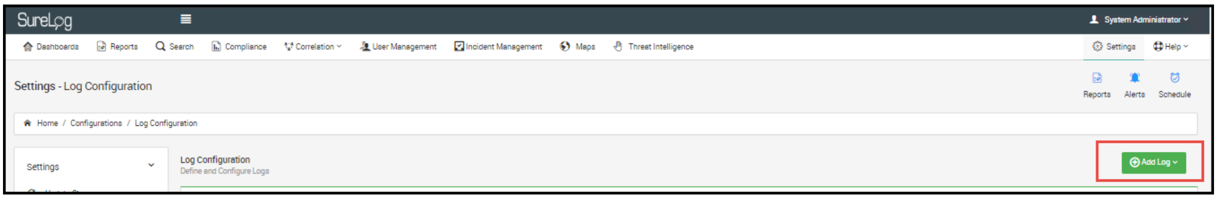
Server IP: 192.168.1.85

Username: .\administrator

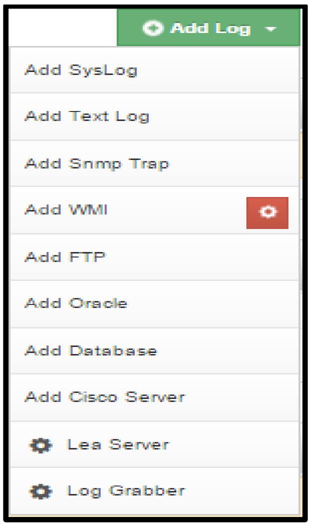
Password: ....

After making the configuration in the figure above, the user should add the log source as WMI as shown in the figure below:

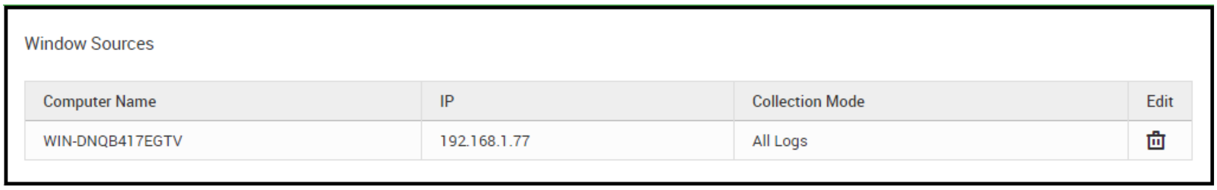
1. Select Settings
2. Select Log Configuration
3. Select Add button in the Log Configuration view pane



4. Select Add WMI



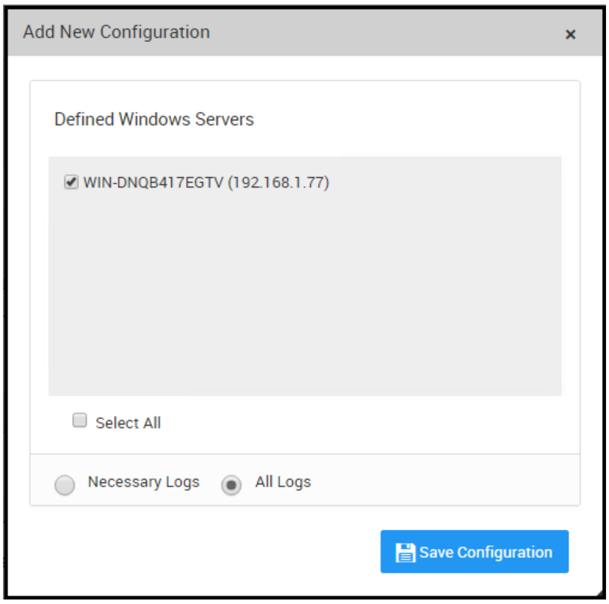
If the user select ⚙ symbol as shown in the figure above, the logs shown in the figure below are sent from log source to SureLog log collector. This way the necessary logs are sent to SureLog log collector.



Window Sources

Computer Name	IP	Collection Mode	Edit
WIN-DNQB417EGTV	192.168.1.77	All Logs	🗑

5. Select log source with All Logs (The user can also select necessary logs as shown in the figure above.)



Add New Configuration ×

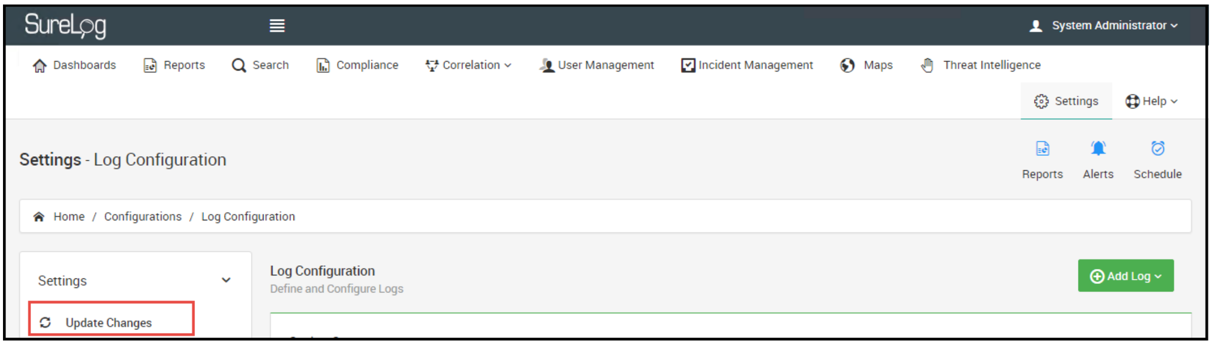
Defined Windows Servers

☑ WIN-DNQB417EGTV (192.168.1.77)

□ Select All

○ Necessary Logs ● All Logs

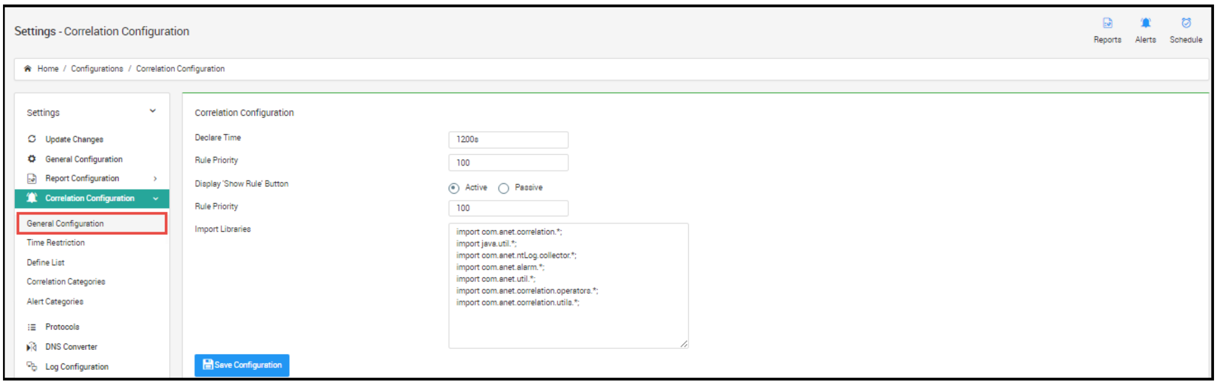
6. After making the configuration steps shown above, the user should select Update Changes Tab. This restarts the services related with the changes made in the background.



Correlation Configuration

In correlation configuration section, in general configuration tab; if the users define the declare time, the users can specify the reservation time for the log in the correlation memory. If the system detects the bigger reservation time in any rule, the reservation time is automatically is set to the bigger one.

If we define the rule priority; this is a default value for any rule. If the users set rule priority value less than 100 for a rule, the priority is given for the operation of that work.



Correlation Configuration

Declare Time: 1200s

Rule Priority: 100

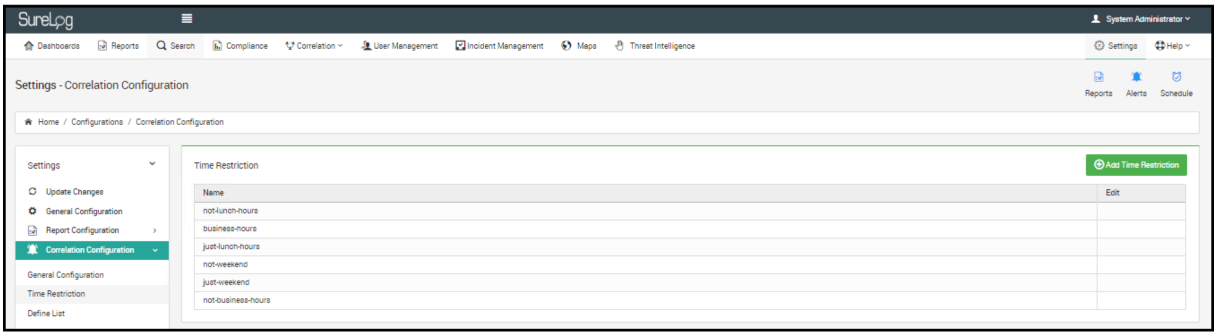
Display 'Show Rule' Button: ● Active ○ Passive

Rule Priority: 100

Import Libraries:

```
import com.anet.correlation.*;
import java.util.*;
import com.anet.ntLog.collector.*;
import com.anet.alarm.*;
import com.anet.util.*;
import com.anet.correlation.operators.*;
import com.anet.correlation.utils.*;
```

If we mention about time restriction, There are default time zones, which can be used in the correlation rules. Here, you can also set your own specific time zone through Add Time Restriction tab.



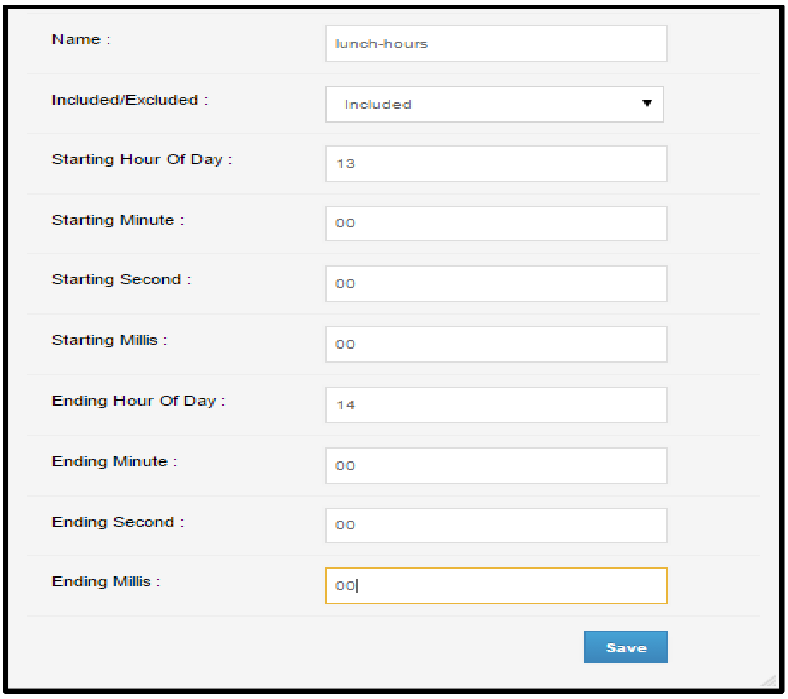
Settings - Correlation Configuration

Time Restriction

Name	Edit
not-lunch-hours	
business-hours	
just-lunch-hours	
not-weekend	
just-weekend	
not-business-hours	

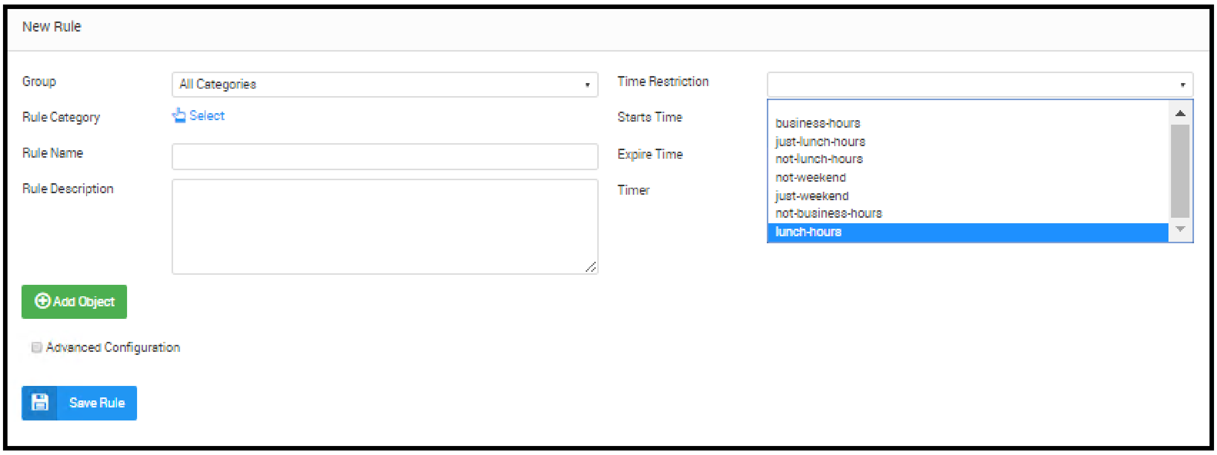
To add Time Restriction:

1. Select Settings
2. Select Correlation Configuration
3. Select Time Restriction
4. Select Add Time Restriction
5. Enter the configurations shown in the figure below:



Name :	lunch-hours
Included/Excluded :	Included
Starting Hour Of Day :	13
Starting Minute :	00
Starting Second :	00
Starting Millis :	00
Ending Hour Of Day :	14
Ending Minute :	00
Ending Second :	00
Ending Millis :	00

6. The users can use new Time Restriction in Correlation rule configuration as shown in the figure below:



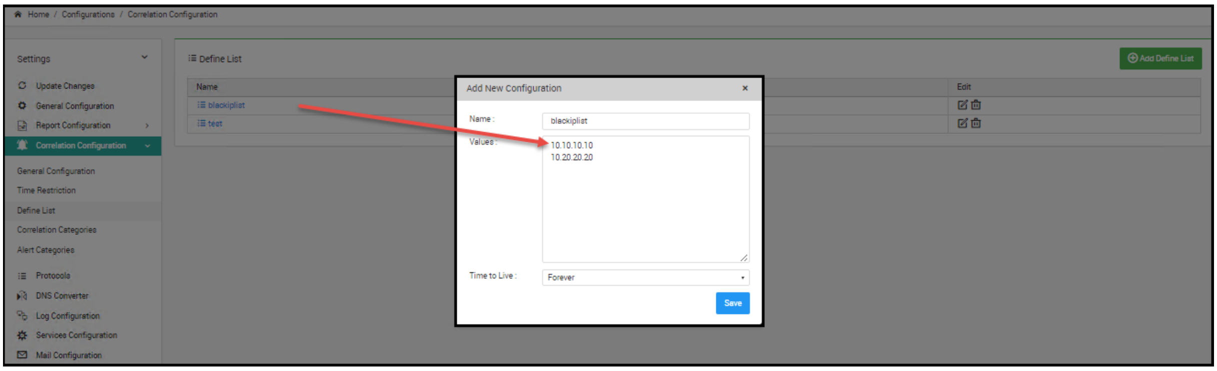
Group: All Categories
Rule Category: Select
Rule Name:
Rule Description:
☐ Advanced Configuration
Time Restriction:
Starts Time
Expire Time
Timer

business-hours
just-lunch-hours
not-lunch-hours
not-weekend
just-weekend
not-business-hours
lunch-hours

If we mention about define list, the users can define specific lists, which can be used later on in the correlation. For example, the users can create a blacklisted IP group and then the users can add blacklisted IPs in this group. The users can later on use the blacklisted IP group in the correlation.

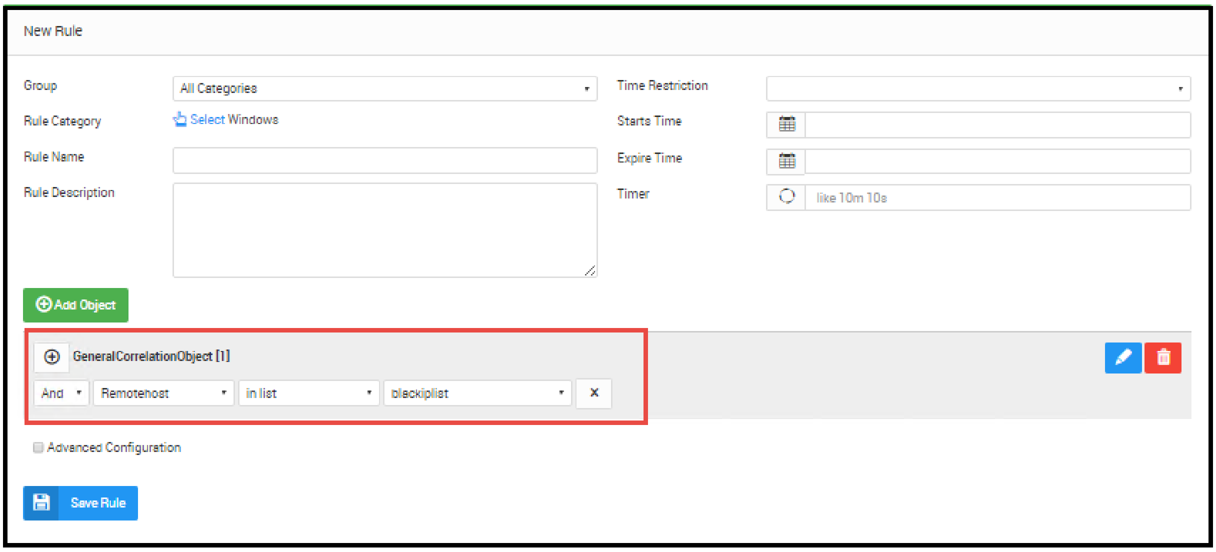
To add a Define List:

9. Select Settings
10. Select Correlation Configuration
11. Select Define List
12. Select Add Define List button



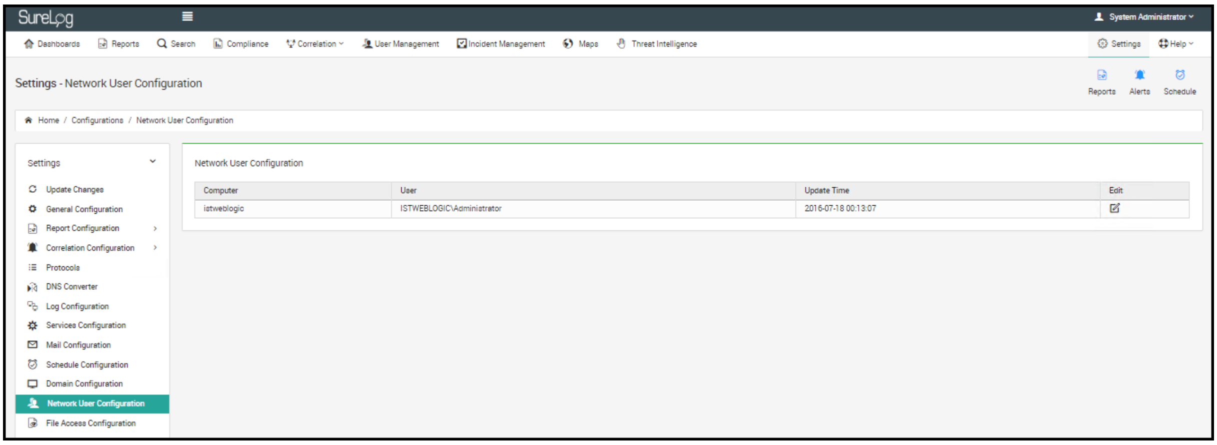
Name : blackiplist
Values : 10.10.10.10
10.20.20.20
Time to Live : Forever

13. The user can use the define list named blacklist created above in the correlation rule as shown in the figure below:



Network User Configuration

In network user configuration section, the servers, which are added through Domain or individually arelisted here as shown in the figure below:



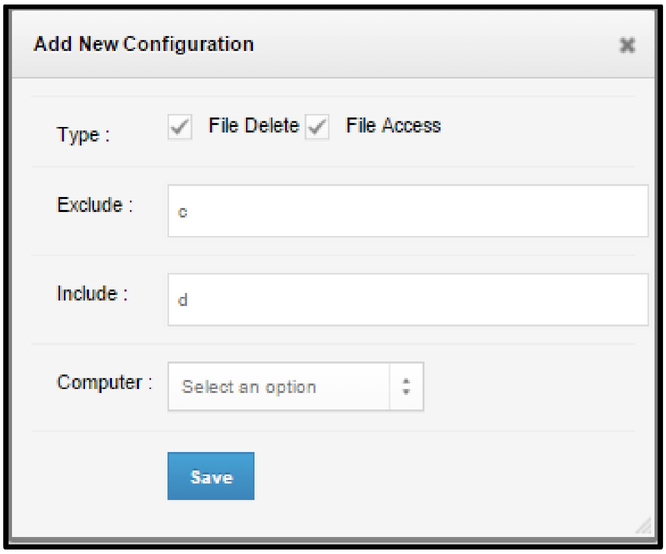
Computer	User	Update Time	Edit
istweblogic	ISTWEBLOGIC\Administrator	2016-07-18 00:13:07	✎

File Access Configuration

In file Access configuration section, through Add File Access tab, we can specify on which drive File Delete and File Access operations are included and on which drive they are excluded by specifying the computer name.

The users can make File Access Configurations as in the steps below:

1. Select Settings
2. Select File Access Configuration
3. Select Add File Access button in the upper right pane.
4. Enter the configurations as in the figure below:



Add New Configuration

Type : ☑ File Delete ☑ File Access

Exclude : c

Include : d

Computer : Select an option

Network Access Configuration

In network Access configuration section, the users can monitor the defined IP and MAC addresses in the system from here.

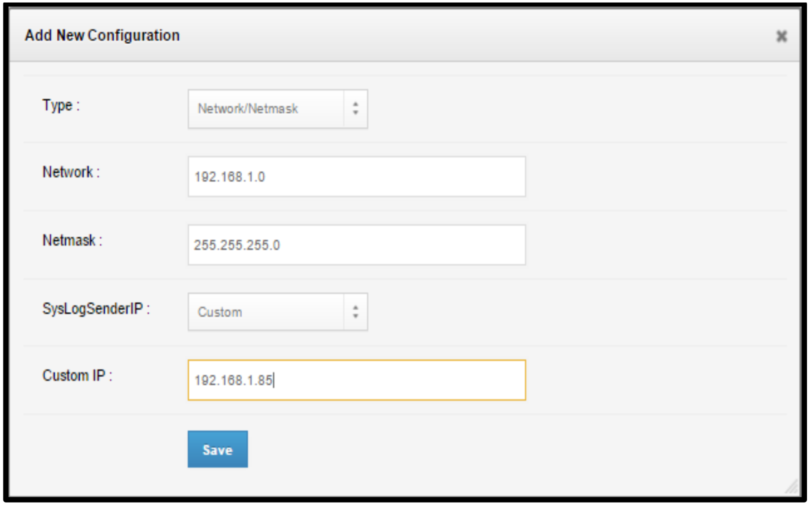
Through ADD MAC IP, if the MAC and IP addresses in the system change, you will be notified through email. For example, if the MAC of an IP address changes, you will be noticed by email.

Intranet Configuration

In intranet configuration section, the users define an IP block or IP range with a custom syslog sender IP. The aim here is to identify if the direction of the network traffic is originated from inside to outside or from outside to inside network.

The users can make Intranet Configurations as in the steps below:

1. Select Settings
2. Select Intranet Configuration
3. Select Add Intranet button in the upper right pane.
4. Enter the configurations as in the figure below:



Add New Configuration

Type : Network/Netmask

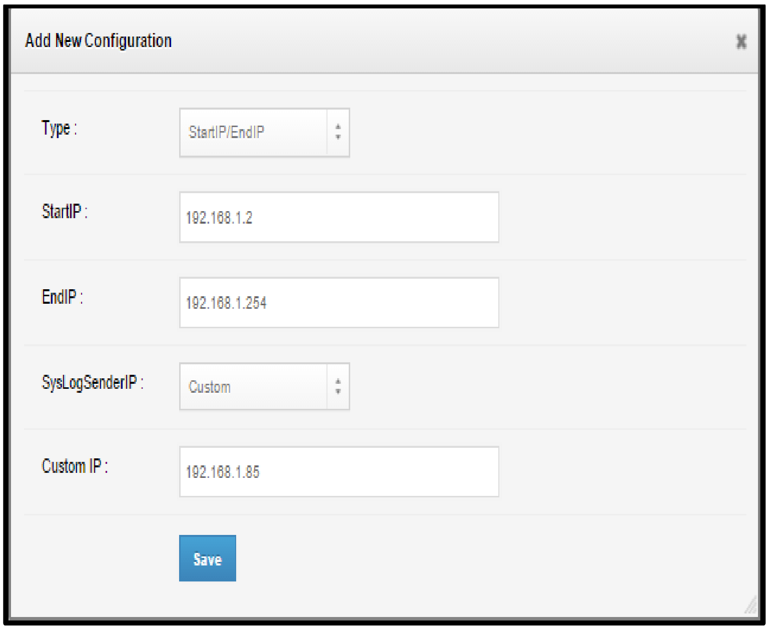
Network : 192.168.1.0

Netmask : 255.255.255.0

SysLogSenderIP : Custom

Custom IP : 192.168.1.85

5. The users also select type field as **StartIP/EndIP**as shown in the figure below:



Add New Configuration ×

Type : StartIP/EndIP

StartIP : 192.168.1.2

EndIP : 192.168.1.254

SysLogSenderIP : Custom

Custom IP : 192.168.1.85

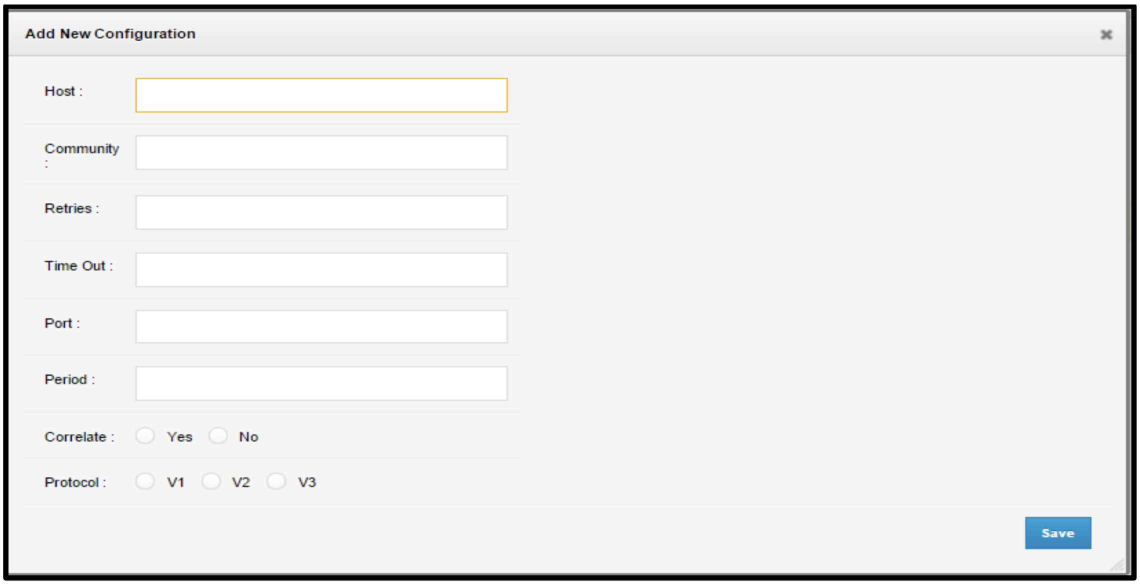
Save

ARP Table Configuration

In the ARP table configuration section, IP addresses with their corresponding MAC addresses are kept in the ARP table. The main purpose of this configuration is to keep IP to MAC addresses matches in case DHCP server is not accessed.

The user can make ARP Table Configuration as in the steps below:

1. Select Settings
2. Select ARP Table Configuration
3. Select Add ARP Table tab in the upper right pane
4. Enter the configurations as in the below:



Add New Configuration ×

Host :

Community :

Retries :

Time Out :

Port :

Period :

Correlate : ○ Yes ○ No

Protocol : ○ V1 ○ V2 ○ V3

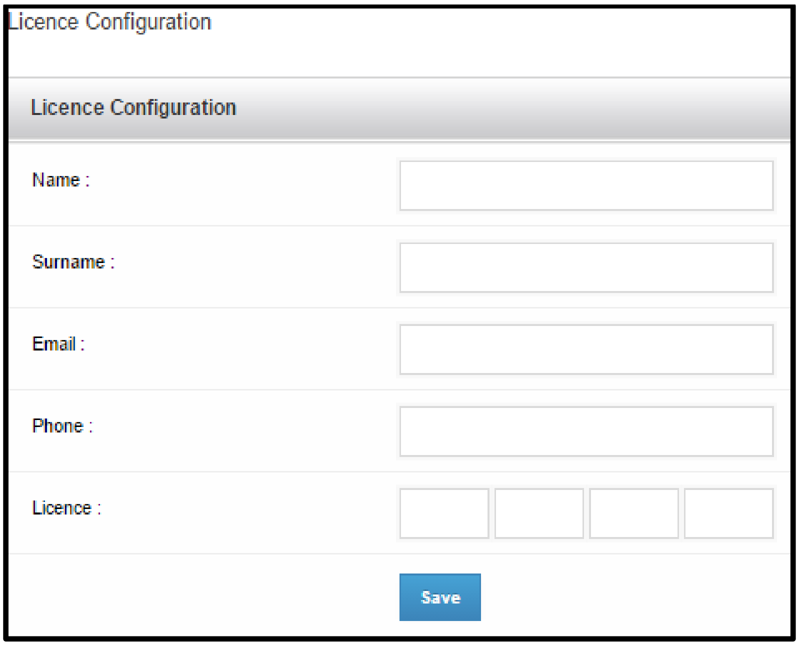
Save

License Configuration

In license configuration section, here the users license SureLog international edition.

The user can make ARP Table Configuration as in the steps below:

1. Select Settings
2. Select License Configuration
3. Enter the configurations as in the below:



Licence Configuration

Licence Configuration

Name :

Surname :

Email :

Phone :

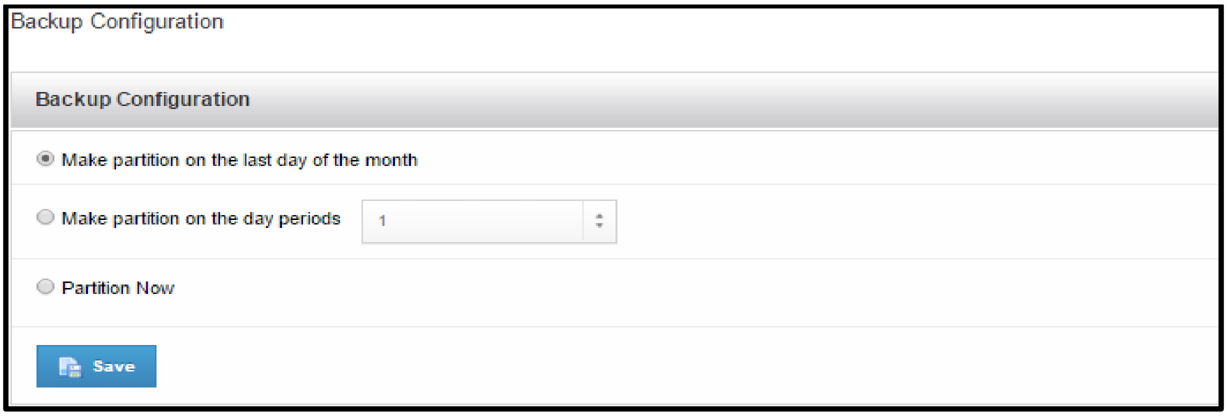
Licence :

Backup Configuration

In backup configuration section, the users can take the backup of the tables in the database in specific time periods such as on the last day of the month, on the day periods or now.

The user can make Backup Configuration as in the steps below:

1. Select Settings
2. Select Backup Configuration
3. Enter the configurations as in the below:



Backup Configuration

Backup Configuration

● Make partition on the last day of the month

○ Make partition on the day periods 1

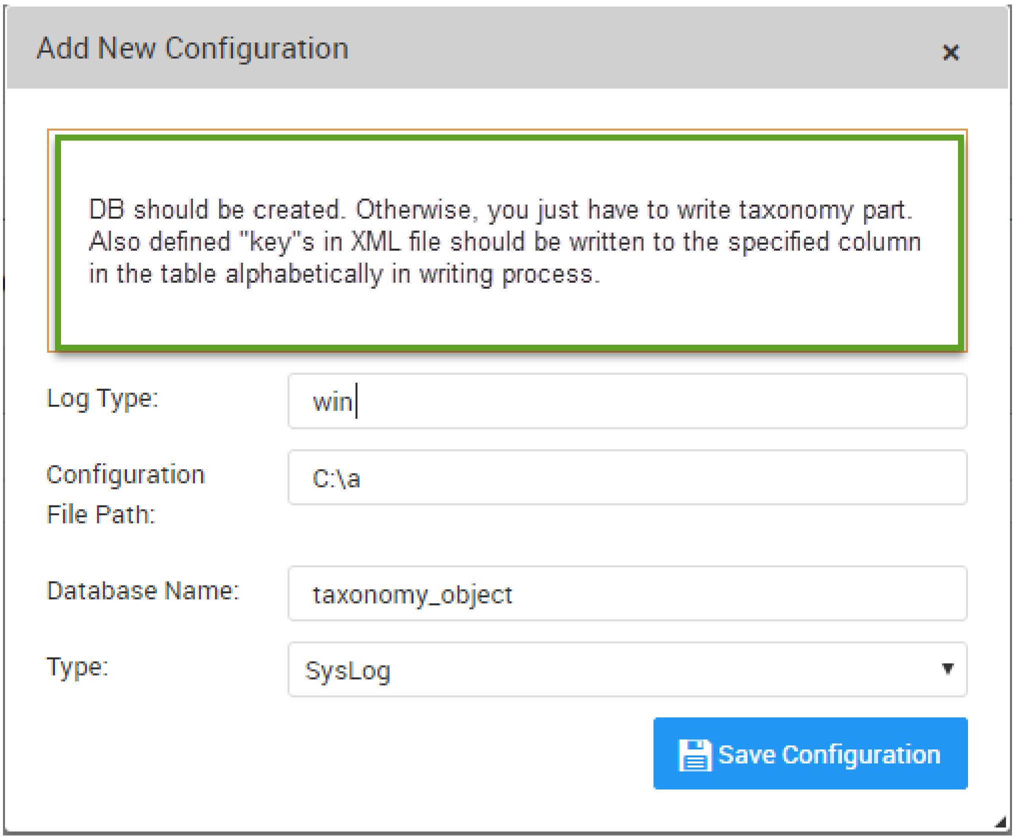
○ Partition Now

Custom Parser Configuration

In custom parser configuration section, the users can add a custom parser to SureLog for any log source.

The users can make Custom Parser Configuration as in the steps below:

1. Select Settings
2. Select Custom Parser Configuration
3. Select Add Custom Parser tab in the upper right pane
4. Enter the configurations as in the below:



Add New Configuration

DB should be created. Otherwise, you just have to write taxonomy part. Also defined "key"s in XML file should be written to the specified column in the table alphabetically in writing process.

Log Type: win

Configuration File Path: C:\a

Database Name: taxonomy_object

Type: SysLog

File should be in C:\a\win.xml folder.

Database Name: to which table the logs will be written in the database.

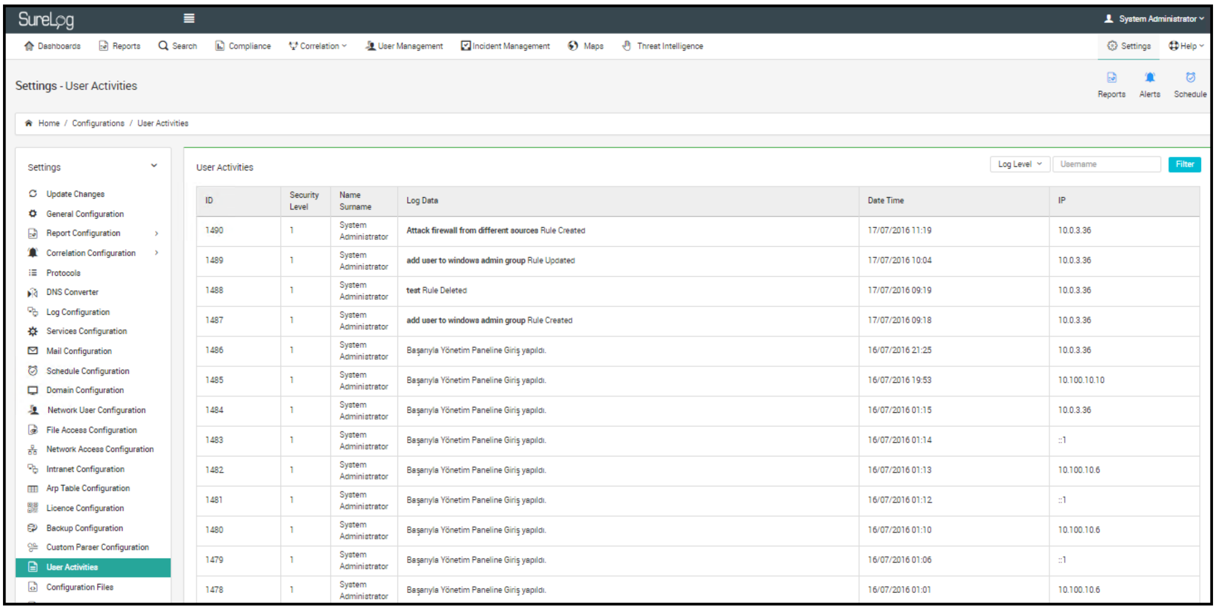
Type: How the logs will be collected, as syslog, snmp or text ?

User Activities:

In user activities section, the users can monitor which tasks or activities the users perform in the system.

To monitor the users' activities in the system:

1. Select Settings
2. Select User Activities



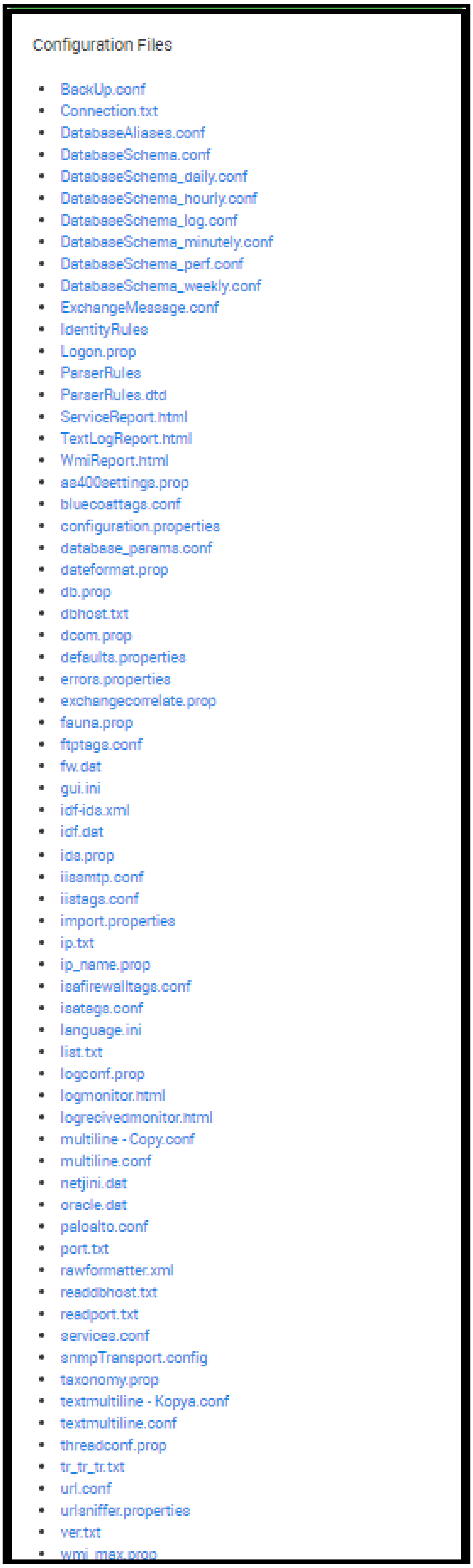
ID	Security Level	Name Surname	Log Data	Date Time	IP
1490	1	System Administrator	**Attack firewall from different sources** Rule Created	17/07/2016 11:19	10.0.3.36
1489	1	System Administrator	**add user to windows admin group** Rule Updated	17/07/2016 10:04	10.0.3.36
1488	1	System Administrator	**test** Rule Deleted	17/07/2016 09:19	10.0.3.36
1487	1	System Administrator	**add user to windows admin group** Rule Created	17/07/2016 09:18	10.0.3.36
1486	1	System Administrator	Başarıyla Yönetim Paneline Giriş yapıldı.	16/07/2016 21:25	10.0.3.36
1485	1	System Administrator	Başarıyla Yönetim Paneline Giriş yapıldı.	16/07/2016 19:53	10.100.10.10
1484	1	System Administrator	Başarıyla Yönetim Paneline Giriş yapıldı.	16/07/2016 01:15	10.0.3.36
1483	1	System Administrator	Başarıyla Yönetim Paneline Giriş yapıldı.	16/07/2016 01:14	::1
1482	1	System Administrator	Başarıyla Yönetim Paneline Giriş yapıldı.	16/07/2016 01:13	10.100.10.6
1481	1	System Administrator	Başarıyla Yönetim Paneline Giriş yapıldı.	16/07/2016 01:12	::1
1480	1	System Administrator	Başarıyla Yönetim Paneline Giriş yapıldı.	16/07/2016 01:10	10.100.10.6
1479	1	System Administrator	Başarıyla Yönetim Paneline Giriş yapıldı.	16/07/2016 01:06	::1
1478	1	System Administrator	Başarıyla Yönetim Paneline Giriş yapıldı.	16/07/2016 01:01	10.100.10.6

Configuration Files:

In configuration files section, the users can edit or make changes on the configuration files.

The users can make changes on the configuration files as in the steps below:

1. Select Settings
2. Select Configuration Files
3. Select the configuration file for editing as in the figure below



Configuration Files

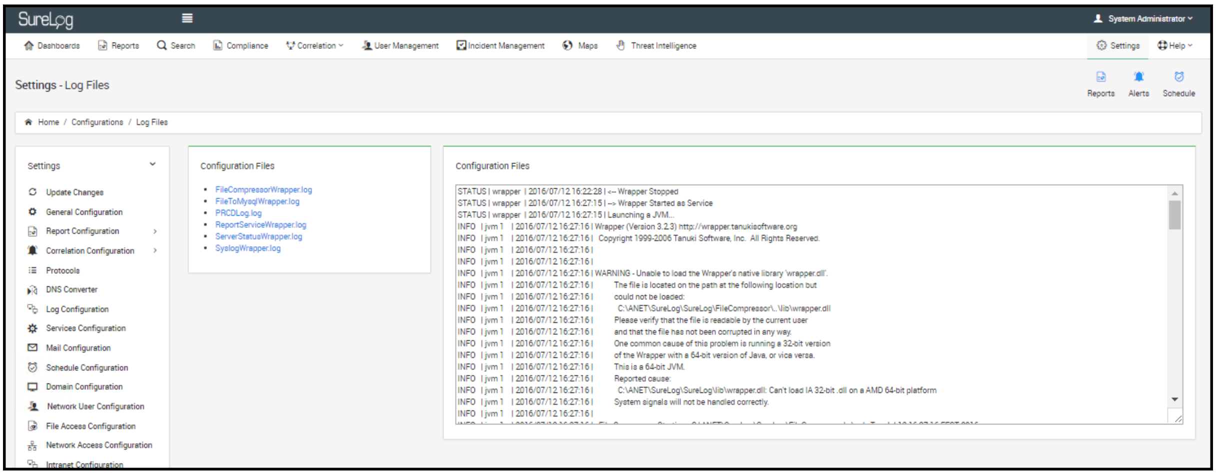
- BackUp.conf
- Connection.txt
- DatabaseAliases.conf
- DatabaseSchema.conf
- DatabaseSchema_daily.conf
- DatabaseSchema_hourly.conf
- DatabaseSchema_log.conf
- DatabaseSchema_minutely.conf
- DatabaseSchema_perf.conf
- DatabaseSchema_weekly.conf
- ExchangeMessage.conf
- IdentityRules
- Logon.prop
- ParserRules
- ParserRules.dtd
- ServiceReport.html
- TextLogReport.html
- WmiReport.html
- as400settings.prop
- bluecoattags.conf
- configuration.properties
- database_params.conf
- dateformat.prop
- db.prop
- dbhost.txt
- dcom.prop
- defaults.properties
- errors.properties
- exchangecorrelate.prop
- fauna.prop
- ftptags.conf
- fw.dat
- gui.ini
- idf-ids.xml
- idf.dat
- ids.prop
- iissmtp.conf
- iistags.conf
- import.properties
- ip.txt
- ip_name.prop
- isafirewalltags.conf
- isatags.conf
- language.ini
- list.txt
- logconf.prop
- logmonitor.html
- logrecivedmonitor.html
- multiline - Copy.conf
- multiline.conf
- netjini.dat
- oracle.dat
- paloalto.conf
- port.txt
- rawformatter.xml
- readdbhost.txt
- readport.txt
- services.conf
- snmpTransport.config
- taxonomy.prop
- textmultiline - Kopya.conf
- textmultiline.conf
- threadconf.prop
- tr_tr_tr.txt
- url.conf
- urlsniffer.properties
- ver.txt
- wmi_max.prop

Log Files:

In log files section, the logs for each SureLog service are kept here in the wrapper log files specific to each service. The users can troubleshoot the problems with Surelog by checking and analyzing these service specific wrapper log files.

The users can view log files as in the steps below:

1. Select Settings
2. Select Log Files
3. Select the Log File for viewing as in the figure below



Settings - Log Files

Configuration Files

- FileCompressorWrapper.log
- FileToMysqlWrapper.log
- PRCDLog.log
- ReportServiceWrapper.log
- ServerStatusWrapper.log
- SyslogWrapper.log

Configuration Files

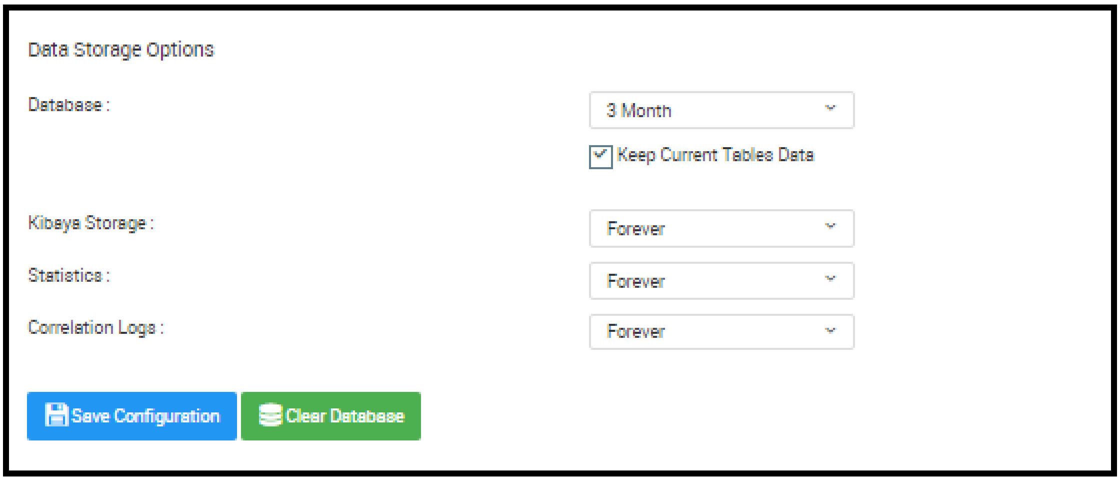
```
STATUS | wrapper  | 2016/07/12 16:22:28 | <-- Wrapper Stopped
STATUS | wrapper  | 2016/07/12 16:27:15 | --> Wrapper Started as Service
STATUS | wrapper  | 2016/07/12 16:27:15 | Launching a JVM...
INFO   | jvm 1    | 2016/07/12 16:27:16 | Wrapper (Version 3.2.3) http://wrapper.tanukisoftware.org
INFO   | jvm 1    | 2016/07/12 16:27:16 |   Copyright 1999-2006 Tanuki Software, Inc.  All Rights Reserved.
INFO   | jvm 1    | 2016/07/12 16:27:16 |
INFO   | jvm 1    | 2016/07/12 16:27:16 |
INFO   | jvm 1    | 2016/07/12 16:27:16 | WARNING - Unable to load the Wrapper's native library 'wrapper.dll'.
INFO   | jvm 1    | 2016/07/12 16:27:16 |           The file is located on the path at the following location but
INFO   | jvm 1    | 2016/07/12 16:27:16 |           could not be loaded:
INFO   | jvm 1    | 2016/07/12 16:27:16 |             C:\ANET\SureLog\SureLog\FileCompressor\..\lib\wrapper.dll
INFO   | jvm 1    | 2016/07/12 16:27:16 |           Please verify that the file is readable by the current user
INFO   | jvm 1    | 2016/07/12 16:27:16 |           and that the file has not been corrupted in any way.
INFO   | jvm 1    | 2016/07/12 16:27:16 |           One common cause of this problem is running a 32-bit version
INFO   | jvm 1    | 2016/07/12 16:27:16 |           of the Wrapper with a 64-bit version of Java, or vica versa.
INFO   | jvm 1    | 2016/07/12 16:27:16 |           This is a 64-bit JVM.
INFO   | jvm 1    | 2016/07/12 16:27:16 |           Reported cause:
INFO   | jvm 1    | 2016/07/12 16:27:16 |             C:\ANET\SureLog\SureLog\lib\wrapper.dll: Can't load IA 32-bit .dll on a AMD 64-bit platform
INFO   | jvm 1    | 2016/07/12 16:27:16 |           System signals will not be handled correctly.
INFO   | jvm 1    | 2016/07/12 16:27:16 |
```

Data Storage Options:

In data storage options sections, here the users can specify in the setting that the logs are retained in the tables for a certain time. After that, they will be deleted. The log files are retained as signed for a certain time before inserted into the database. After that, those log files will be deleted.

The users can configure Data Storage Options as in the steps below:

1. Select Settings
2. Select Data Storage Options
3. Enter the configurations as in the below:



Data Storage Options

Database : 3 Month
☑ Keep Current Tables Data

Kibaya Storage : Forever

Statistics : Forever

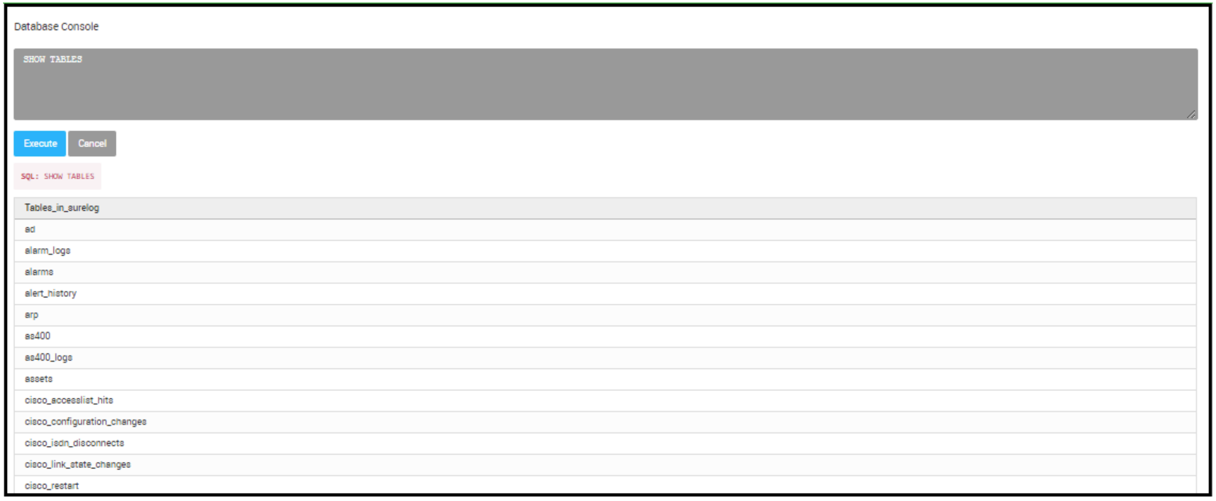
Correlation Logs : Forever

Database Console:

In database console section, the users can execute SQL queries on the database console.

The users can execute a sample SQLquery on the database console as in the steps below:

1. Select Settings
2. Select Database Console
3. Run a sample SQL query as in the figure below:



```
SHOW TABLES
```

SQL: SHOW TABLES

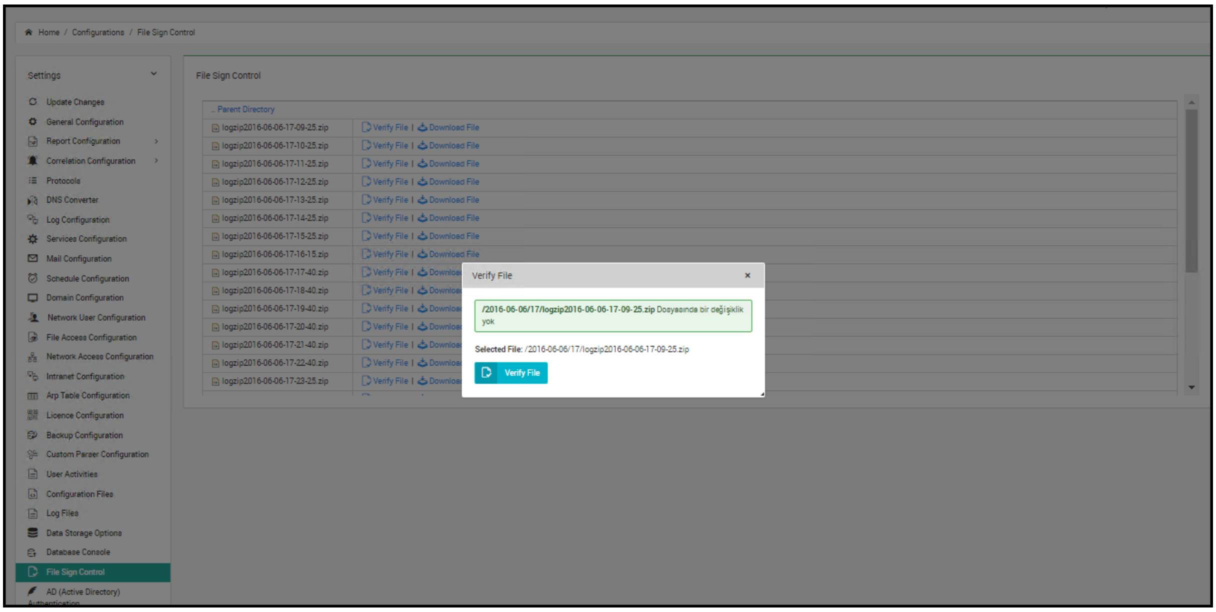
Tables_in_surelog
ad
alarm_logs
alarms
alert_history
arp
as400
as400_logs
assets
cisco_accesslist_hits
cisco_configuration_changes
cisco_isdn_disconnects
cisco_link_state_changes
cisco_restart

File Sign Control:

In File sign control section, the users can check if the log files are changed or not.

The users can make File Sign Control as in the steps below:

1. Select Settings
2. Select File Sign Control
3. Select the file and verify its integrity



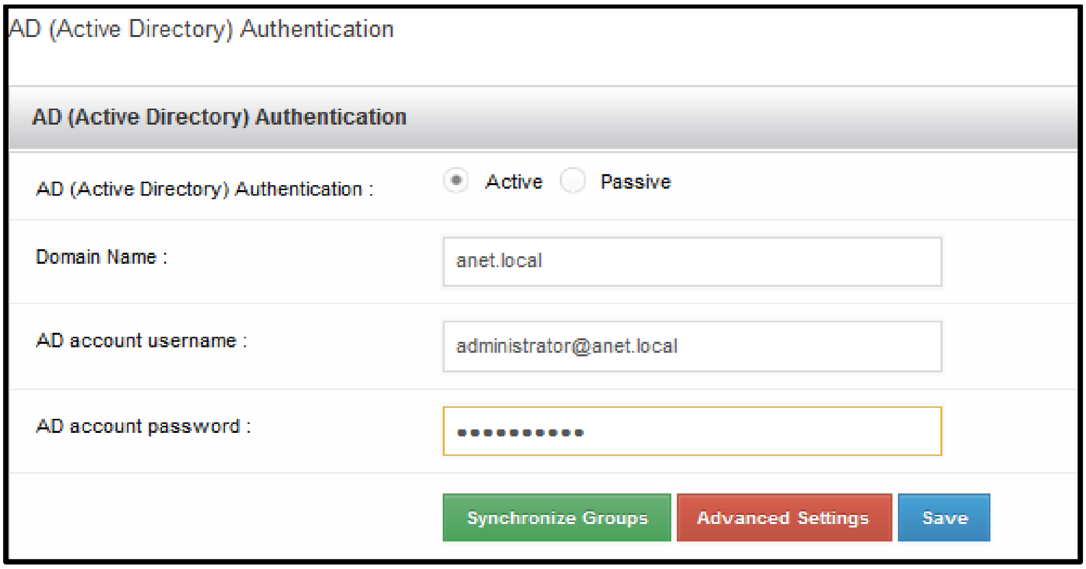
.. Parent Directory	
logzip2016-06-06-17-09-25.zip	Verify File | Download File
logzip2016-06-06-17-10-25.zip	Verify File | Download File
logzip2016-06-06-17-11-25.zip	Verify File | Download File
logzip2016-06-06-17-12-25.zip	Verify File | Download File
logzip2016-06-06-17-13-25.zip	Verify File | Download File
logzip2016-06-06-17-14-25.zip	Verify File | Download File
logzip2016-06-06-17-15-25.zip	Verify File | Download File
logzip2016-06-06-17-16-15.zip	Verify File | Download File
logzip2016-06-06-17-17-40.zip	Verify File | Downloa
logzip2016-06-06-17-18-40.zip	Verify File | Downloa
logzip2016-06-06-17-19-40.zip	Verify File | Downloa
logzip2016-06-06-17-20-40.zip	Verify File | Downloa
logzip2016-06-06-17-21-40.zip	Verify File | Downloa
logzip2016-06-06-17-22-40.zip	Verify File | Downloa
logzip2016-06-06-17-23-25.zip	Verify File | Downloa

/2016-06-06/17/logzip2016-06-06-17-09-25.zip Dosyasında bir değişiklik yok

Selected File: /2016-06-06/17/logzip2016-06-06-17-09-25.zip

AD (Active Directory) Authentication

In Active Directory authentication section, we can authenticate SureLog with Active Directory.



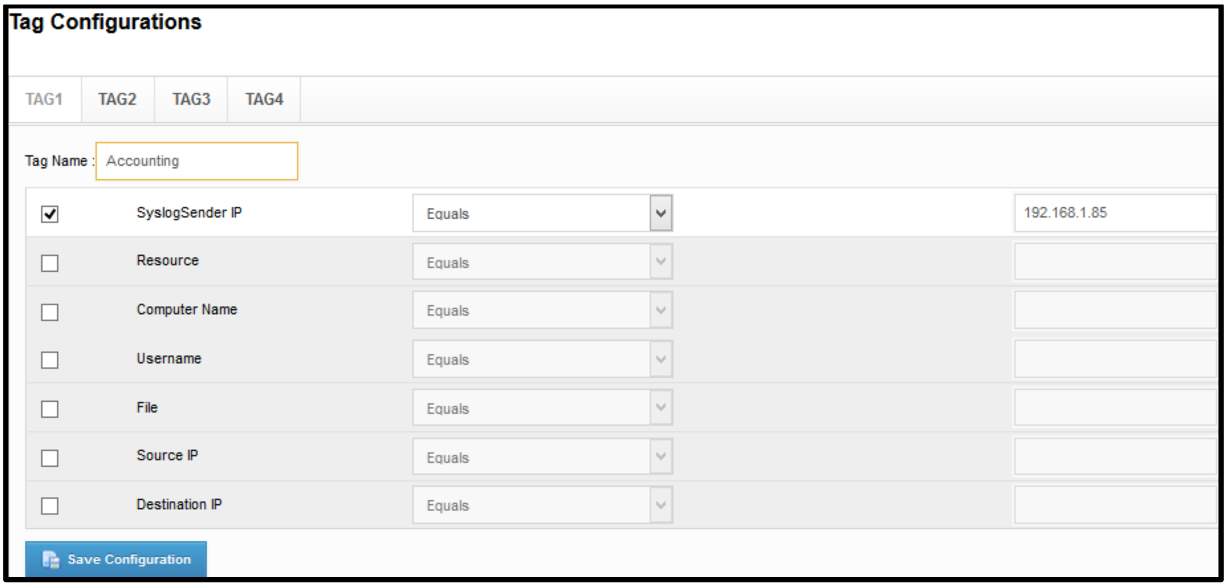
AD (Active Directory) Authentication

AD (Active Directory) Authentication

AD (Active Directory) Authentication :	● Active ○ Passive
Domain Name :	anet.local
AD account username :	administrator@anet.local
AD account password :	●●●●●●●●●●●

Tag Configurations

In TAG configuration section, the keywords such as Accounting, Helpdesk, marketing, and such are added into the log according to the source of log, computer name, username, syslog sender ip, and such. For example, we can add logs accounting tag coming from accounting department.



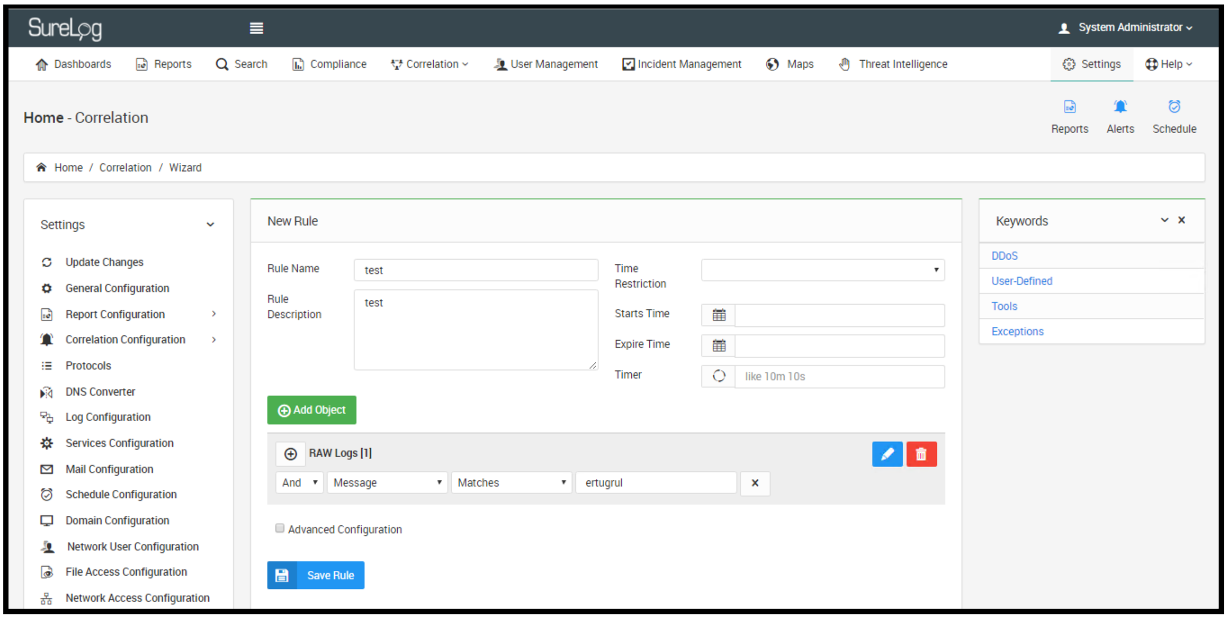
Tag Configurations

Tag Name : Accounting

☑	SyslogSender IP	Equals	192.168.1.85
☐	Resource	Equals	
☐	Computer Name	Equals	
☐	Username	Equals	
☐	File	Equals	
☐	Source IP	Equals	
☐	Destination IP	Equals	

Preparser Rule

Preparser rule block log matches in the rule configuration.



New Rule

Rule Name: test

Rule Description: test

Time Restriction:

Starts Time:

Expire Time:

Timer: like 10m 10s

RAW Logs [1]

And | Message | Matches | ertugrul

□ Advanced Configuration