LOG RADAR™

SIMPLIFIED SECURITY MANAGEMENT

technology by **TecForte**

Log Radar v3.2 User Manual

Trademarks

Warning and Disclaimer

Contents

1. Getting Started

1.1 - System Requirements

Minimum requirements:

- Processor – Intel Xeon Quad Core 2.5 GHz or higher
- Memory – 4GB
- Operation System – Server 2003 64-bit
- Disk Space for Application - 390 MB
- Disk Space for Logs (subject to traffic volume and log rotation policy)

1.2 - Installation

For information on installing Log Radar, please refer to the Log Radar Installation Guide.

1.3 - Starting Log Radar

1. Go to Start > All Programs >Log Radar SE > Log Radar Console.
2. The Login screen appears.
3. Enter the user name and password and click Sign In.
4. The Log Radar Program opens.

Alternatively, you can start Log Radar by typing the installed Web site URL in the address bar of the browser window.

Important: Please use the following administrator login information for first time sign in and you are advised to change the default password for the administrator account as soon as possible (see *Chapter 9: User Administration*).

Username: admin
Password: admin

The Setup Wizard will guide you through the initial settings (see *Chapter 2: Setup Wizard*).

For further configurations (see *Chapter 10: Configuration*) and create user accounts (see *Chapter 9: User Administration* before using the software.

Add a new device for Log Radar to receive logs from (see *Chapter 8: Device Management*) to get software to start processing logs. The number of devices permitted is governed by the number of licenses purchased.

1.4 - Technical Support

For updated product documentation, technical support information, and other resources, please visit the TecForte official web site at http://www.tecforte.com.

Technical support is available through email from info@tecforte.com

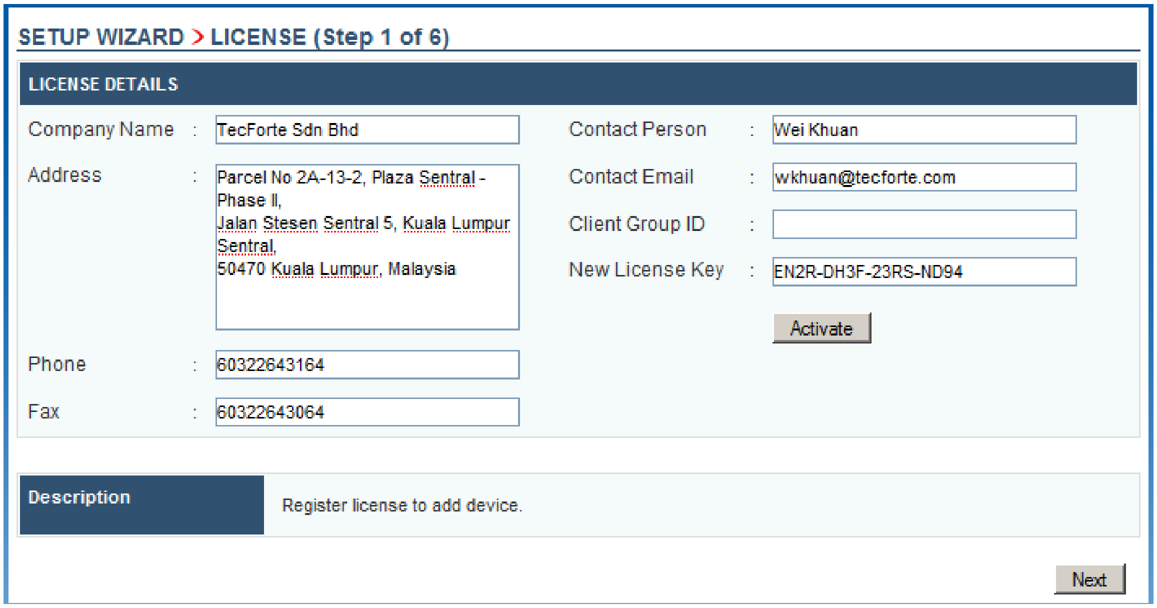
When requesting technical support, please provide the following information:

- your name
- your company's name and location
- your email address
- your telephone number
- your support contract number (if applicable)
- a detailed description of the problem

2. Setup Wizard

Setup wizard has been designed to guide you through some initial settings to get the software up and running. To change these settings in the future, go to the respective configuration pages.

2.1 - License Configuration



Company Name : TecForte Sdn Bhd
Address : Parcel No 2A-13-2, Plaza Sentral - Phase II,
Jalan Stesen Sentral 5, Kuala Lumpur Sentral,
50470 Kuala Lumpur, Malaysia
Phone : 60322643164
Fax : 60322643064
Contact Person : Wei Khuan
Contact Email : wkhuan@tecforte.com
Client Group ID :
New License Key : EN2R-DH3F-23RS-ND94

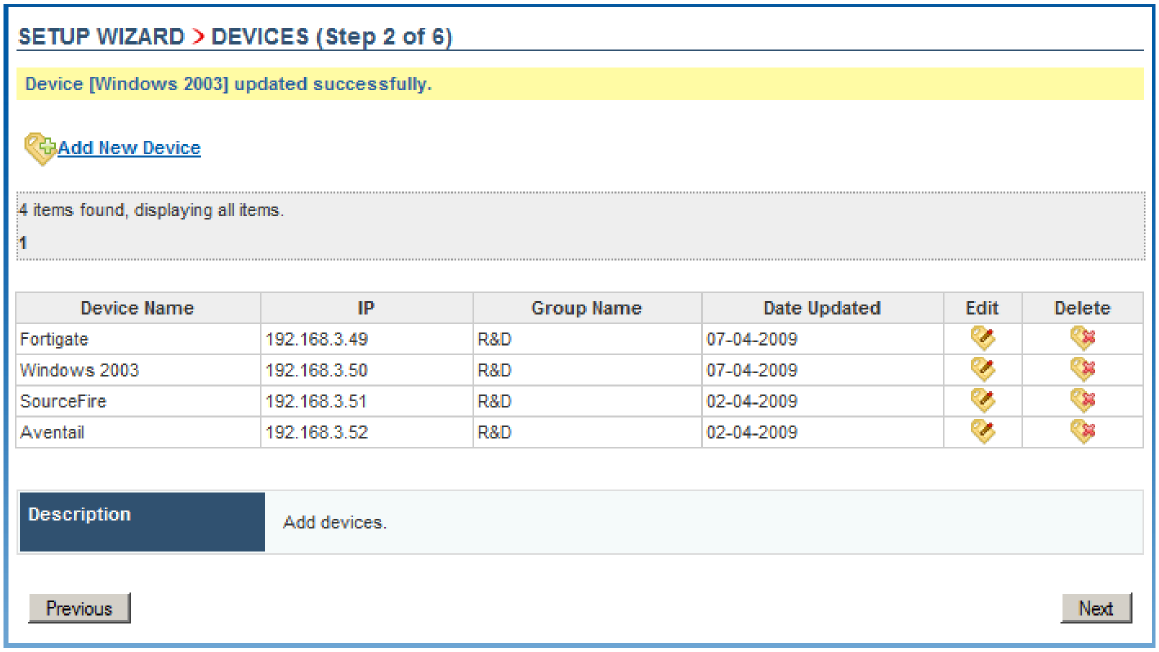
Description: Register license to add device.

Steps to follow:

License Registration	1. Enter all the information for each textbox. 2. The Client Group ID can be left blank. 3. Key in the License key with the (-) marks, *e.g ERJ3-JU29-TY6U-M283B* 4. Click Activate button to register the license. 5. Click Confirm button when requested to double-check on the information to be submitted. 6. Click Next button to proceed to the next step. **Note**: For Evaluation version, you do not have to key in any license information.

2.2 - Device Configuration

The Device Configuration page allows you to add, edit and delete the Devices used in Log Radar. Logs sent by those Devices will be received by Log Radar, and processed according to the selected category. The number of devices allowed to be registered will be limited by the license that you have purchased.



SETUP WIZARD > DEVICES (Step 2 of 6)

Device [Windows 2003] updated successfully.

Add New Device

4 items found, displaying all items.

1

Device Name	IP	Group Name	Date Updated	Edit	Delete
Fortigate	192.168.3.49	R&D	07-04-2009	✎	✗
Windows 2003	192.168.3.50	R&D	07-04-2009	✎	✗
SourceFire	192.168.3.51	R&D	02-04-2009	✎	✗
Aventail	192.168.3.52	R&D	02-04-2009	✎	✗

Description	Add devices.

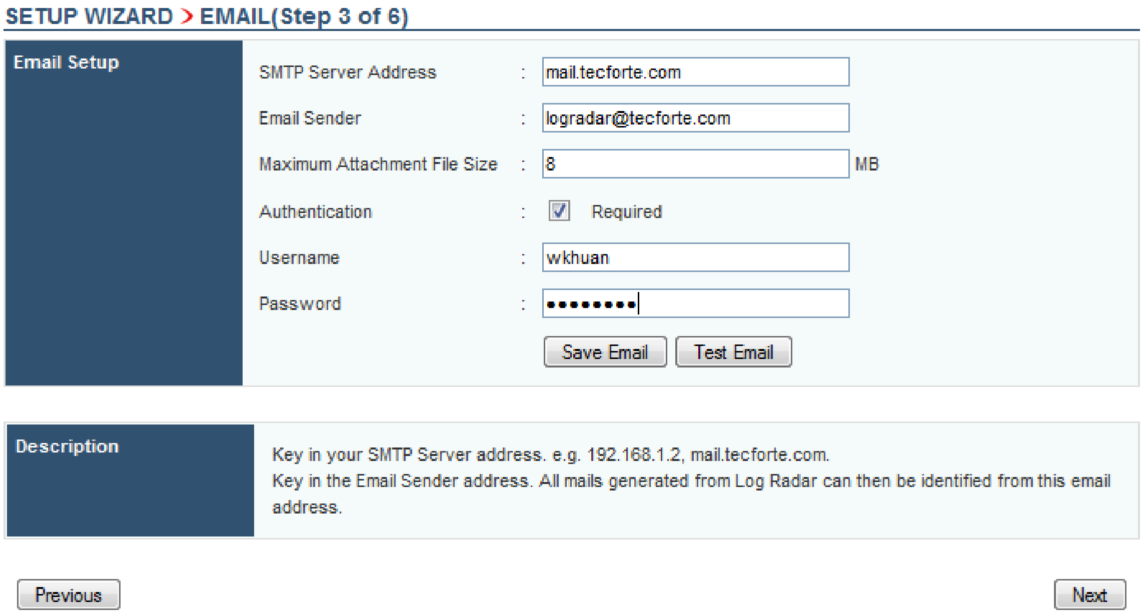
Steps to follow:

To **Add** Device	1. Click on link Add New Device 2. Enter Device Details 3. Assign Group 4. Click Add button to save the new Device
To **Edit** Device	1. Find the Device you want to edit 2. Click on ✎ to edit 3. Make the desired changes

	4. Click Update button to save the changes
To **Delete** Device	1. Find the Device you want to delete 2. Click on ✖ to delete 3. Click Delete Device button to confirm **Warning:** Deleting a Device means that logs from the Device will no longer be processed, and you will not be able to use Log Radar to investigate any existing logs.

2.3 - Email Configuration

The Email Configuration settings are necessary so that Log Radar can send out emails. This must be done before Users are added, as the initial passwords must be sent out by email. Log Radar can also send out emails for Real-Time Threat Alerts, Automated Reports, Automated Asset Discovery scan notifications, etc. The maximum file size attachment can also be set if there are any worries in congesting the email server with heavy attachments like reports and log analytics results.



SMTP Server Address	:	mail.tecforte.com
Email Sender	:	logradar@tecforte.com
Maximum Attachment File Size	:	8 MB
Authentication	:	☑ Required
Username	:	wkhuan
Password	:	•••••••••

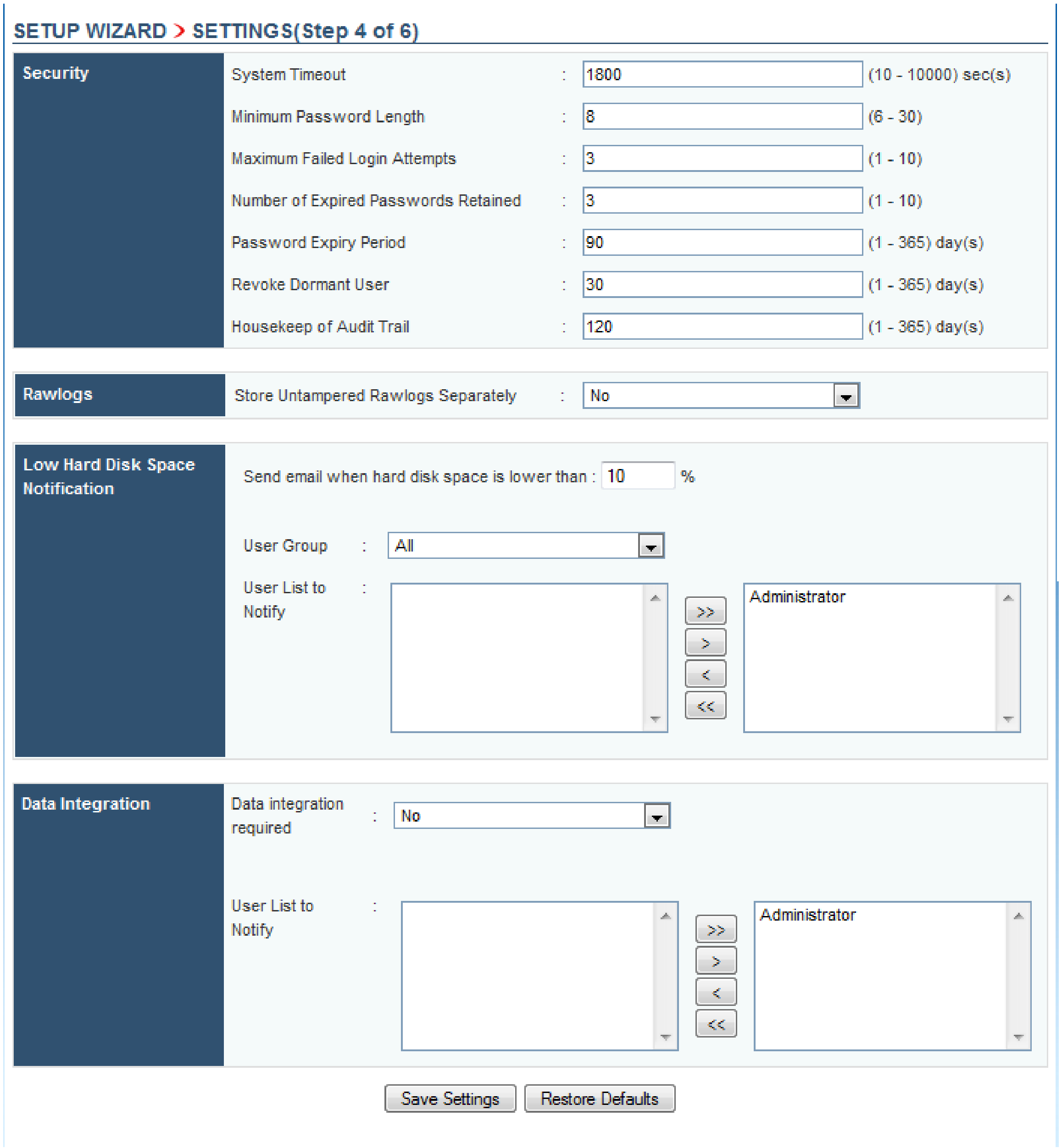
Key in your SMTP Server address. e.g. 192.168.1.2, mail.tecforte.com.
Key in the Email Sender address. All mails generated from Log Radar can then be identified from this email address.

Steps to follow:

Email Setup	1. Enter SMTP Server Address 2. Enter an Email Sender address 3. Enter the maximum attachment file size allowed. 4. If Authentication is required, check the box and enter the username and password. Otherwise, leave box unchecked 5. Click Next button to proceed to the next step.
Test Email	1. Click on Test Email button 2. Enter a valid email address 3. Click Send Email button 4. If the test email does not reach your mailbox, then you need to recheck the configuration.

2.4 - Settings

The default settings provide a reasonable level of security; however you may wish to configure different levels. The default levels can be restored at any time.



SETUP WIZARD > SETTINGS(Step 4 of 6)

Security

System Timeout : 1800 (10 - 10000) sec(s)
Minimum Password Length : 8 (6 - 30)
Maximum Failed Login Attempts : 3 (1 - 10)
Number of Expired Passwords Retained : 3 (1 - 10)
Password Expiry Period : 90 (1 - 365) day(s)
Revoke Dormant User : 30 (1 - 365) day(s)
Housekeep of Audit Trail : 120 (1 - 365) day(s)

Rawlogs

Store Untampered Rawlogs Separately : No

Low Hard Disk Space Notification

Send email when hard disk space is lower than : 10 %
User Group : All
User List to Notify : Administrator

Data Integration

Data integration required : No
User List to Notify : Administrator

The available settings are:

Security Settings

- *System Timeout* - this determines the maximum period of inactivity before a session is automatically ended.
- *Minimum password length* - this determines the least number of characters that a password for a User may contain.
- *Maximum Failed Login Attempt* - this determines the maximum number of times a User can enter an incorrect password before being suspended.

- *Number of Expired Passwords Retained* - this determines how many previously used passwords will be kept. A User will be unable to reuse a password while it is being retained.
- *Password Expiry Period* - this determines the how frequently a User must change their password. The User will be suspended if the password is not changed within this period.
- *Revoke Dormant User* - this determines the period to revoke a dormant user.
- *Housekeep of Audit Trail* - this determines the period during which recorded user activities will be stored in the Audit Trail. Once the period has passed, the data will be archived. See *Section 9.5 Audit Trail Archive* for more details.

Rawlogs

- *Store Untampered Rawlogs Separately* – this determines if the rawlogs should be saved separately or not. These extra set of rawlogs will be saved in a separate folder, compressed and hashed on a daily basis, to prevent tampering of information. Regardless of the setting here, all rawlogs will still be processed into Log Radar like normal.

Low Hard Disk Space Notification

- *Send email when hard disk space is lower than* – this determines the threshold for the notification. A notification email will be sent to the list of selected users by 2.00am, when threshold has been exceeded.
- *User List to Notify* – select the list of users to be notified when hard disk space usage has exceeded the threshold.

Data Integration

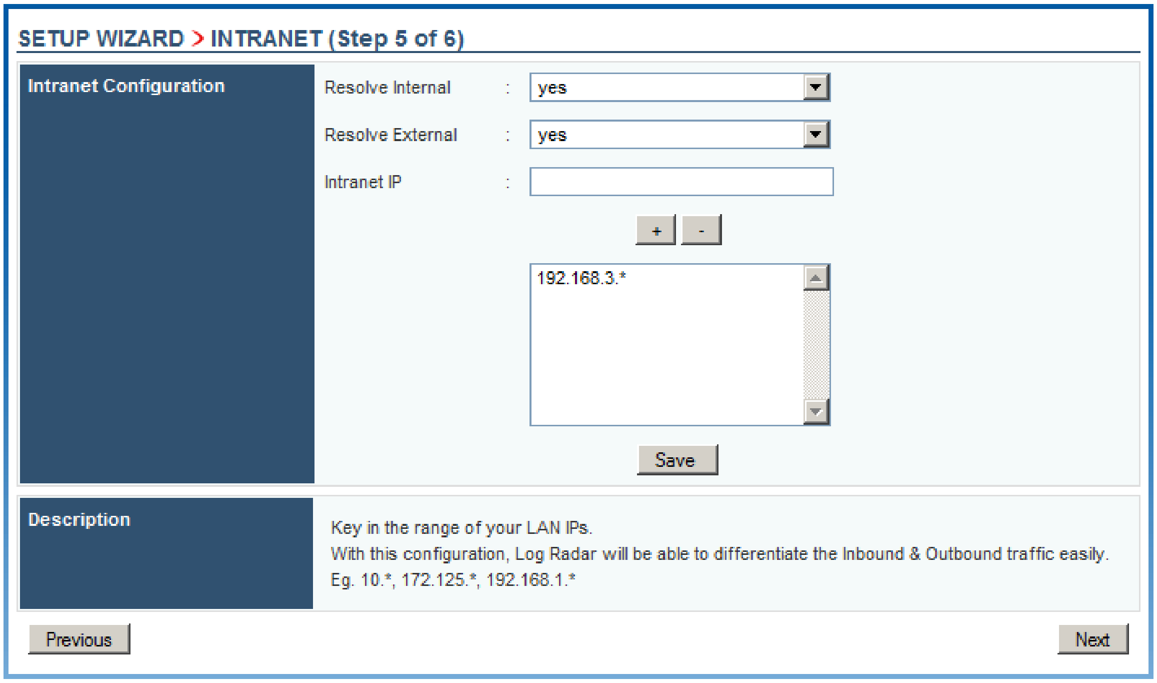
- *Data integration required* – if this server is deployed in a distributed architecture and will be sending/receiving logs from other branches, select Yes.
- *Local Host as* – this selection will appear if Data integration required is selected as Yes. If this server will act as the Master/HQ Log Radar, select Destination. If this server will act as the Slave/Branch Log Radar, where it will be sending logs back to the Master/HQ Log Radar, select Source.
- *User List to Notify* – select the list of users to be notified when data transfer fails, etc.

Steps to follow:

Security Settings	1. Enter desired values for each setting 2. Click Save Settings button to save the entered information 3. Click Next button to proceed to the next step
Restore Defaults	1. Click on Restore Defaults button 2. Click Save Settings button to save the restored information 3. Click Next button to proceed to the next step

2.5 - Intranet Settings

The Intranet Configuration allows you to specify the IP addresses of your internal network. It is important that Log Radar is able to distinguish between internal and external IP addresses, so that for example each traffic flow can be classified as Internal, Inbound, Outbound, etc.



SETUP WIZARD > INTRANET (Step 5 of 6)

Intranet Configuration

Resolve Internal : yes

Resolve External : yes

Intranet IP :

192.168.3.*

Description

Key in the range of your LAN IPs.
With this configuration, Log Radar will be able to differentiate the Inbound & Outbound traffic easily.
Eg. 10.*, 172.125.*, 192.168.1.*

Additionally, you can use this page to set whether to resolve IP addresses. When this is set to “yes”, then Log Radar will attempt to resolve the IP Address into a host name, which will be stored in the "Host Name" field for normalised logs.

Steps to follow:

Intranet Configuration	1. Enter IP Addresses in the field **Intranet IP**, and click the + button to enter. You can enter individual IP Addresses, or use a wildcard (e.g. 192.168.2.*) 2. Click Next button to proceed to the next step.

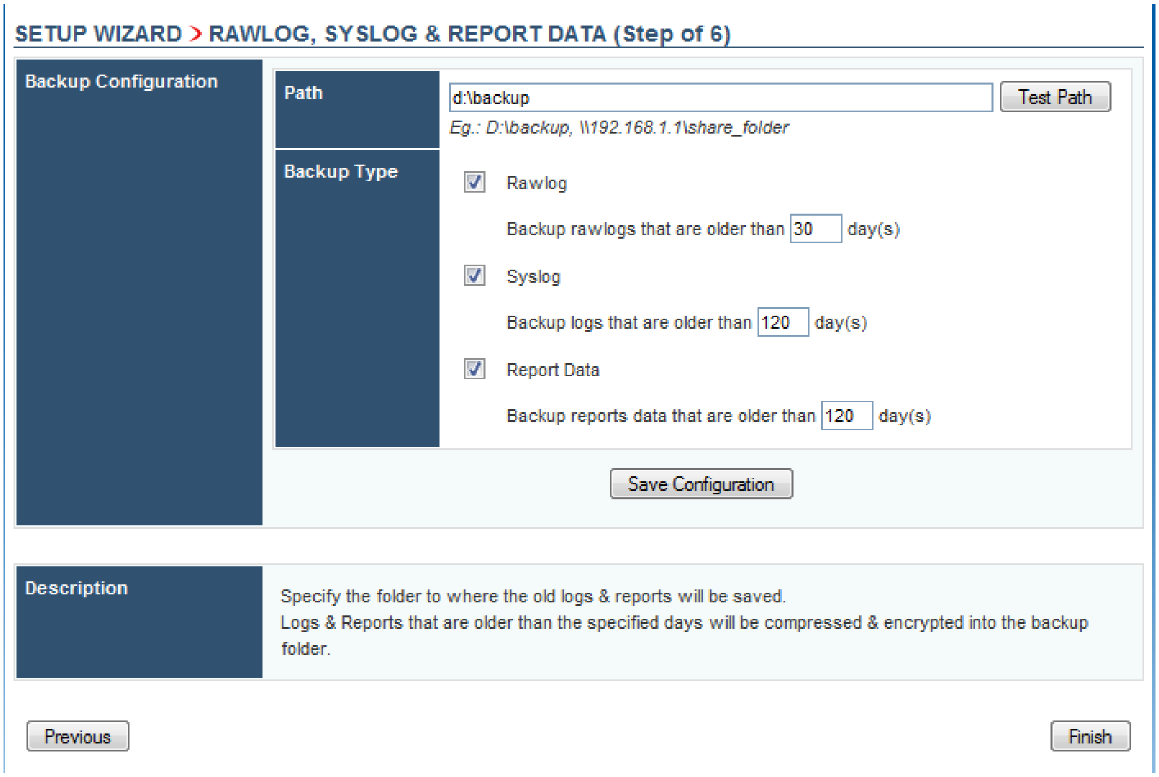
2.6 - Rawlog, Syslog & Report Data Backup Configuration

This step allows you to specify your old Syslogs, Reports metadata and Rawlog archival schedule. These files will be compressed and encrypted into the backup folder.

After archival, the disk space in the local disk will be freed up, however, log analysis will not be able to be performed on the old Syslogs. To perform log analysis on these old files, they will have to be restored (see *Chapter 10.7: Rawlog, Syslog & Report Data Backup/Restore*).

The archived reports are the metadata to perform reports generation. The generated report files PDF & CSV will not be archived.

The compressed rawlogs and hash file will be archived as well. However the archival will not affect the hashing information and will not tamper the rawlogs.



SETUP WIZARD > RAWLOG, SYSLOG & REPORT DATA (Step of 6)

Backup Configuration

Path: d:\backup

Eg.: D:\backup, \\192.168.1.1\share_folder

Backup Type

☑ Rawlog

Backup rawlogs that are older than 30 day(s)

☑ Syslog

Backup logs that are older than 120 day(s)

☑ Report Data

Backup reports data that are older than 120 day(s)

Description

Specify the folder to where the old logs & reports will be saved.
Logs & Reports that are older than the specified days will be compressed & encrypted into the backup folder.

Steps to follow:

Data Backup Configuration	1. Enter a local path or a mapped network drive path 2. Click <u>Test Path</u> button 3. If the test failed, then you need to recheck on your path again. **Note:** The backup folder can be in the local server or in a different server; however, the network folder has to be mapped to the local Log Radar server.
Backup Type Rawlog, Syslog & Report Data	1. Populate the checkboxes to backup the selected files 2. Enter the age of the files type to be backup 3. Click <u>Save Configuration</u> button to save all the configurations and end the Setup Wizard.

	Note: The Rawlog selection will not appear if the Store Untampered Rawlogs Separately in Settings page was not selected.

3. Dashboard

3.1 - Overview

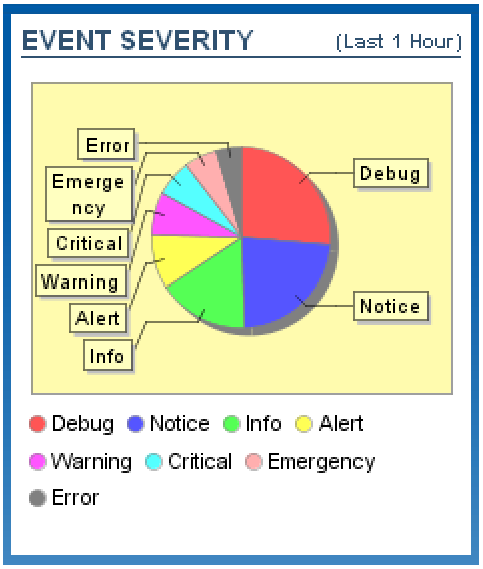
The Log Radar Dashboard provides an overview of the state of your network, based on the logs received. Information is provided both in graphical forms, as pie charts, and in tables, showing various statistics. Anomalies in the log data will be shown up here, and can be further investigated clicking on the statistics itself or by using the Log Analytics module.

The Dashboard also shows the results of the Asset Discovery scans, notifications of any logs which cannot be handled correctly, and any other system messages as required.

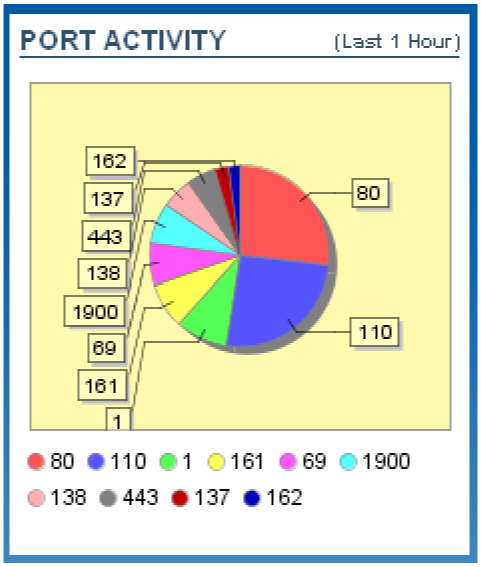
3.2 - Graphical Charts

There are three charts shown on the dashboard:

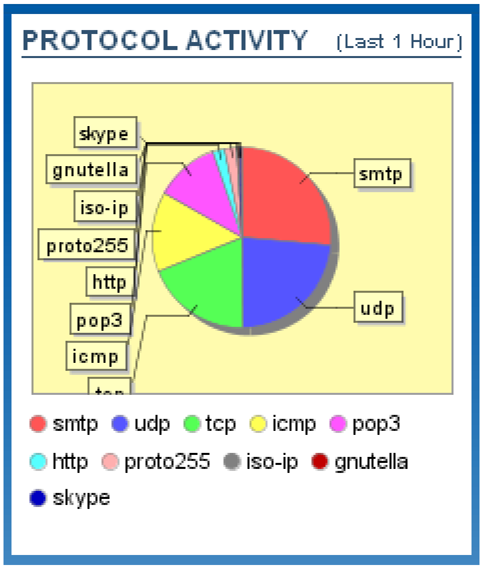
- *Event Severity* - Shows the breakdown of Severity for the logs received. The Severity levels are based on the SysLog standard: Emergency, Alert, Critical, Error, Warning, Notice, Information and Debug. By default, the chart shows all data from the previous one hour.



- *Port Activity* - Shows the breakdown of activity by Destination Port. Only the top ten Ports will be shown. By default, the chart shows all data from the previous one hour.

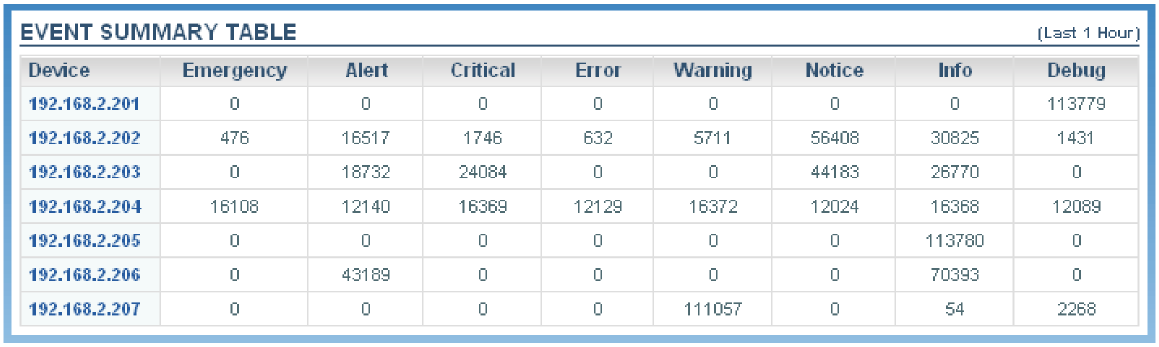


- *Protocol Activity* - Shows the breakdown of activity by Protocol. Only the top ten Protocols will be shown. By default, the chart shows all data from the previous one hour.



3.3 - Event Summary Table

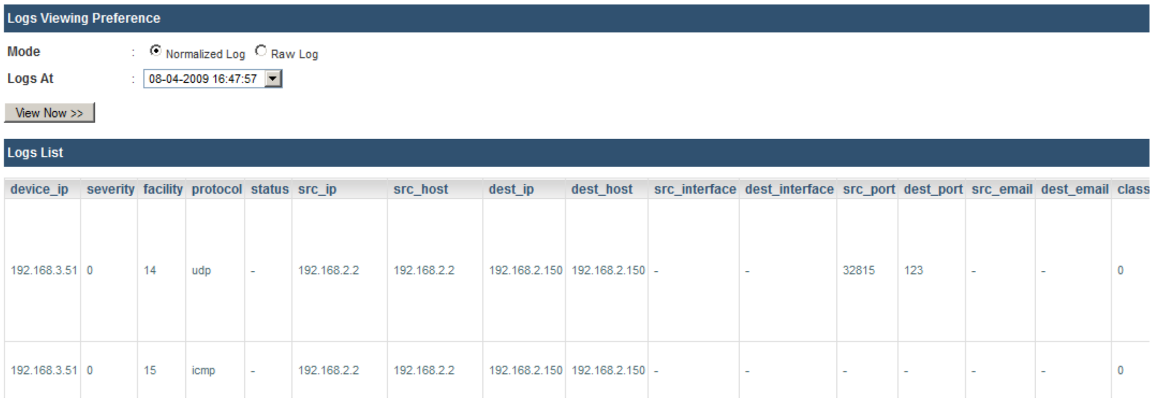
The Event Summary Table shows the total logs received, by device and by severity. By default, the chart shows all data from the previous one hour. You can also click onto the numbers to view the normalized logs and raw logs.



EVENT SUMMARY TABLE (Last 1 Hour)

Device	Emergency	Alert	Critical	Error	Warning	Notice	Info	Debug
192.168.2.201	0	0	0	0	0	0	0	113779
192.168.2.202	476	16517	1746	632	5711	56408	30825	1431
192.168.2.203	0	18732	24084	0	0	44183	26770	0
192.168.2.204	16108	12140	16369	12129	16372	12024	16368	12089
192.168.2.205	0	0	0	0	0	0	113780	0
192.168.2.206	0	43189	0	0	0	0	70393	0
192.168.2.207	0	0	0	0	111057	0	54	2268

Once clicked from the Event Summary Table, it will display the 1st 100 logs collected for the latest minute. To view other logs for that minute, click on *Download Complete Logs* button at the end of the page. You can also view logs for other minutes.



Logs Viewing Preference

Mode : ● Normalized Log ○ Raw Log
Logs At : 08-04-2009 16:47:57

Logs List

device_ip	severity	facility	protocol	status	src_ip	src_host	dest_ip	dest_host	src_interface	dest_interface	src_port	dest_port	src_email	dest_email	class
192.168.3.51	0	14	udp	-	192.168.2.2	192.168.2.2	192.168.2.150	192.168.2.150	-	-	32815	123	-	-	0
192.168.3.51	0	15	icmp	-	192.168.2.2	192.168.2.2	192.168.2.150	192.168.2.150	-	-	-	-	-	-	0

Steps to follow:

To **View the Normalized** logs	1. Click on to the statistics of the Event Summary Table. 2. Click on the radio button *Normalized Log*.

	3. Choose the desired minute from the *Logs At* drop-down menu. 4. Click on the *View Now* button. 5. It will display the first 100 logs of the minute only. 6. To view complete logs of the minute, go to Download Complete Logs steps. 7. To view other minute's logs, repeat step 2 – 4 again.
To **View the Raw Logs**	1. Click on to the statistics of the Event Summary Table. 2. Click on the radio button *Raw Log*. 3. Choose the desired minute from the *Logs At* drop-down menu. 4. Click on the *View Now* button. 5. It will display the first 100 logs of the minute only. 6. To view complete logs of the minute, go to Download Complete Logs steps. 7. To view other minute's raw logs, repeat step 2 – 4 again.
To **Download Complete Normalized Logs**	1. Click on to the statistics of the Event Summary Table. 2. Click on the radio button *Normalized Log*. 3. Choose the desired minute from the *Logs At* drop-down menu. 4. Click on the *View Now* button. 5. Click on the *Download Complete Logs* button at the end of the page to download all the normalized logs of the minute. 6. To download other minute's normalized logs, repeat step 2-5.
To **Download Complete RawLogs**	1. Click on to the statistics of the Event Summary Table. 2. Click on the radio button *Raw Log*. 3. Choose the desired minute from the *Logs At* drop-down menu. 4. Click on the *View Now* button. 5. Click on the *Download Complete Logs* button at the end of the page to download all the normalized logs of the minute.

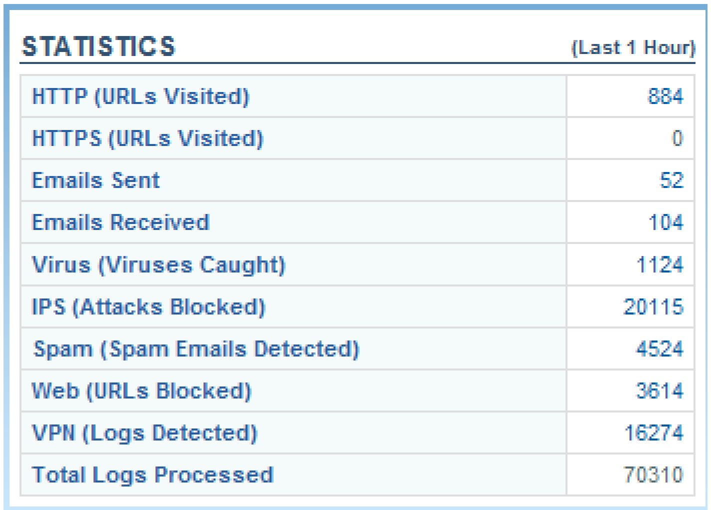
	6. To download other minute’s raw logs, repeat step 2-5.

3.4 - Statistics

The Statistics show the total logs for various categories. By default, the chart shows all data from the previous one hour. You can also click on the statistics to view the logs of that hour.

Categories shown:

- *HTTP* - total of URLs visited, using non-secure HTTP protocol
- *HTTPS* - total of URLs visited, using secure HTTPS protocol
- *Email sent* - total of all sent emails
- *Email received* - total of all received emails
- *Virus* - total of all caught viruses
- *IPS* - total of all blocked attacks
- *Spam* - total of all detected spam emails (spam emails detected)
- *Web* - total of all attempts to access blocked URLs
- *VPN* - total of all detected logs using VPN
- *Total Logs* - total of all processed logs



STATISTICS (Last 1 Hour)

HTTP (URLs Visited)	884
HTTPS (URLs Visited)	0
Emails Sent	52
Emails Received	104
Virus (Viruses Caught)	1124
IPS (Attacks Blocked)	20115
Spam (Spam Emails Detected)	4524
Web (URLs Blocked)	3614
VPN (Logs Detected)	16274
Total Logs Processed	70310

Steps to follow:

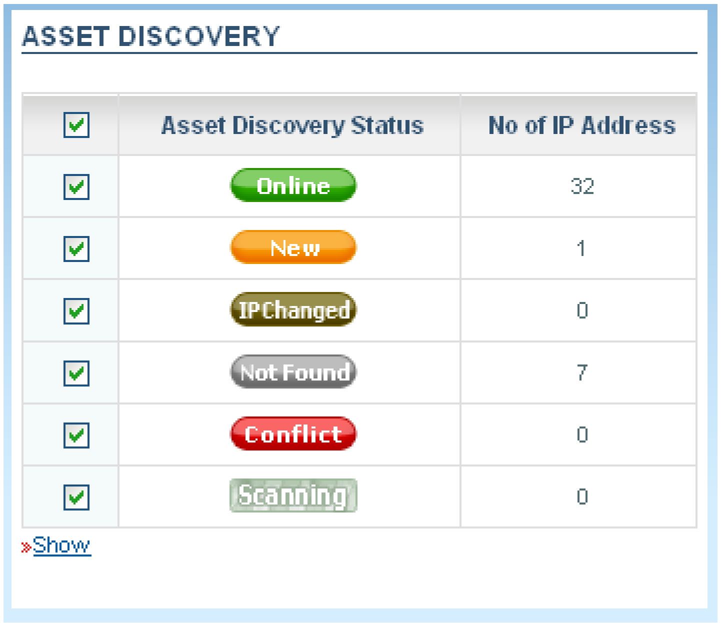
To V**iew the Normalized** logs	1. Click on to the statistics of the Statistics Table. 2. Click on the radio button *Normalized Log*. 3. Choose the desired minute from the *Logs At* drop-down menu. 4. Click on the *View Now* button. 5. It will display the first 100 logs of the minute only. 6. To view complete logs of the minute, go to Download Complete Logs steps. 7. To view other minute's logs, repeat step 2 – 4 again.
To **View the Raw Logs**	1. Click on to the statistics of the Statistics Table. 2. Click on the radio button *Raw Log*. 3. Choose the desired minute from the *Logs At* drop-down menu. 4. Click on the *View Now* button. 5. It will display the first 100 logs of the minute only. 6. To view complete logs of the minute, go to Download Complete Logs steps. 7. To view other minute's raw logs, repeat step 2 – 4 again.
To **Download Complete Normalized Logs**	1. Click on to the statistics of the Event Summary Table. 2. Click on the radio button *Normalized Log*. 3. Choose the desired minute from the *Logs At* drop-down menu. 4. Click on the *View Now* button. 5. Click on the *Download Complete Logs* button at the end of the page to download all the normalized logs of the minute. 6. To download other minute's normalized logs, repeat step 2-5.
To **Download Complete RawLogs**	1. Click on to the statistics of the Event Summary Table. 2. Click on the radio button *Raw Log*. 3. Choose the desired minute from the *Logs At* drop-down menu.

	4. Click on the *View Now* button. 5. Click on the *Download Complete Logs* button at the end of the page to download all the normalized logs of the minute. 6. To download other minute's raw logs, repeat step 2-5.

3.5 - Asset List

The assets found by the most recent Asset Discovery scan are displayed on the Dashboard. The totals for each Status are shown. Use the checkboxes and click on "Show" to view the details for the selected statuses.

The results will not be shown while a scan is in progress.



ASSET DISCOVERY

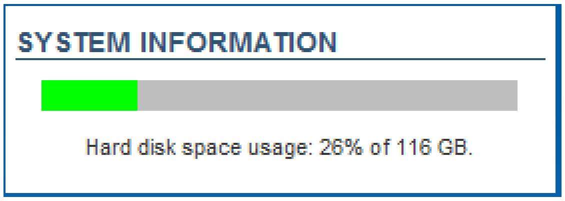
☑	Asset Discovery Status	No of IP Address
☑	Online	32
☑	New	1
☑	IPChanged	0
☑	Not Found	7
☑	Conflict	0
☑	Scanning	0

»Show

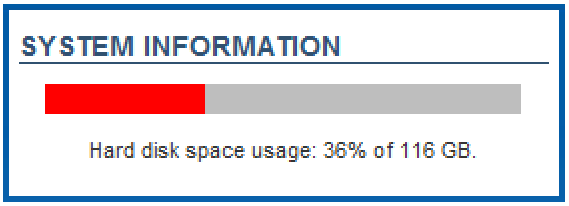
See Chapter 3: Asset Discovery for further information on this module.

3.6 - Hard Disk Space Notification

Log Radar detects the hard disk space of the drive where the program files are saved. The threshold can be set to your preference. When the hard disk space usage exceeds the threshold, the bar will be red in colour and an email notification will be sent out at 2.00am to the administrators. Green colour denotes that there is still free disk space available.



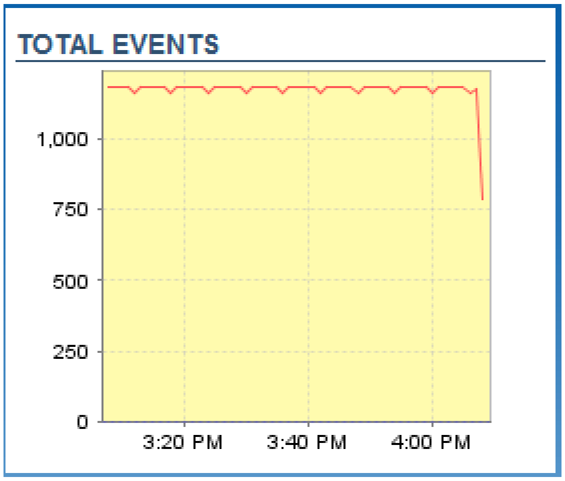
Hard disk space usage: 26% of 116 GB.



Hard disk space usage: 36% of 116 GB.

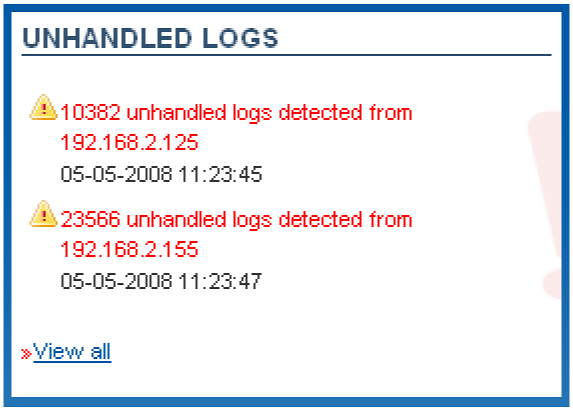
3.7 - Total Events

The time graph displays total events collected per minute from all devices. The time graph is updated every 1 minute. By default, it displays information up to the last 1 hour.



3.8 - Unhandled Logs

Any logs which cannot be handled correctly by Log Radar will be displayed on the Dashboard. The display is also shown for modules other than the Dashboard, so that the User is kept informed of this situation, and appropriate action can be taken.



UNHANDLED LOGS

⚠ 10382 unhandled logs detected from 192.168.2.125
05-05-2008 11:23:45

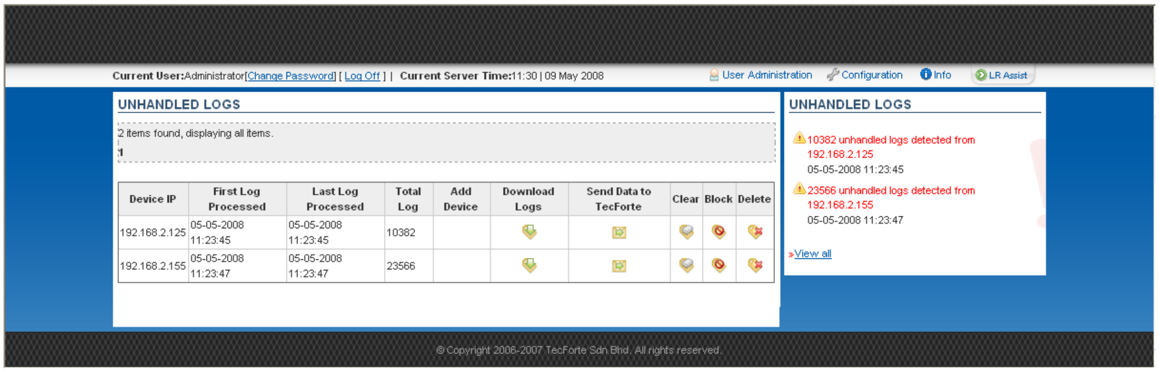
⚠ 23566 unhandled logs detected from 192.168.2.155
05-05-2008 11:23:47

There are two reasons why this may occur:

- Logs may be received from a Device for which Log Radar has no details. In this situation, the Unhandled Logs list will provide a shortcut to quickly add the Device details. See *Chapter 8: Device Management* for further information on adding Devices.
- Log Radar may be unable to parse the log. Possible reasons for this include a log being badly formed, a Device being recently updated, the Device details entered incorrectly, etc. In this situation, a shortcut is provided to email the unparsed logs to TecForte for further analysis.

If for any reason you do not want to add the Device details, or to email the logs to TecForte, then there are additional options:

- *Download Logs* - the logs can be stored locally as a zipped file for future reference.
- *Clear* - this will remove the unhandled logs from the server, and reset the counter to 0.
- *Block* - this will reject all logs from this particular IP Address. The IP Address can also be unblocked in the same way. Note that this will be overruled if the IP Address is used in any Device details.
- *Delete* - all records of the unhandled logs and the IP Address are deleted.



Current User: Administrator[Change Password] [Log Off] | **Current Server Time:**11:30 | 09 May 2008

UNHANDLED LOGS

2 items found, displaying all items.
1

Device IP	First Log Processed	Last Log Processed	Total Log	Add Device	Download Logs	Send Data to TecForte	Clear	Block	Delete
192.168.2.125	05-05-2008 11:23:45	05-05-2008 11:23:45	10382						
192.168.2.155	05-05-2008 11:23:47	05-05-2008 11:23:47	23566						

UNHANDLED LOGS

10382 unhandled logs detected from 192.168.2.125
05-05-2008 11:23:45

23566 unhandled logs detected from 192.168.2.155
05-05-2008 11:23:47

»View all

© Copyright 2006-2007 TecForte Sdn Bhd. All rights reserved.

3.9 - Licensing

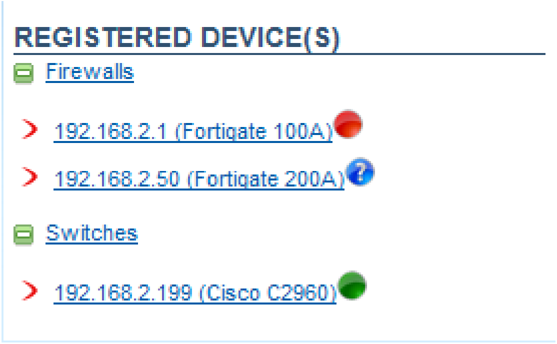
The current licence key information is shown here. The table shows the Registered Owner, the Activation and Expiry Dates, and the number of devices which are allowed/in use/available.

Clicking the Renew button takes you to the page where an updated licence key can be entered.

3.10 – Registered Device(s)

With the new integration of SNMP function, users can also see the device status from the dashboard. The device status query is performed every 5 minutes. To activate the Device Status query for the devices, see *Chapter 8: Device Management* for further information.

- Question Mark Icon – this means that the device was not configured for SNMP. This can be the case if the device is a purely Syslog device. This does not indicate malfunction, just that the device query for this device was not activated.
- Green Icon – this means that the device is up, and the SNMP configurations for this device is correct.
- Red Icon – this means that the device cannot be detected. It may point out to wrong SNMP configuration or due to the network latency, the response was not received in time, or the device may be down.



REGISTERED DEVICE(S)

Firewalls

- 192.168.2.1 (Fortigate 100A)
- 192.168.2.50 (Fortigate 200A)

Switches

- 192.168.2.199 (Cisco C2960)

4. Asset Discovery

4.1 - Overview

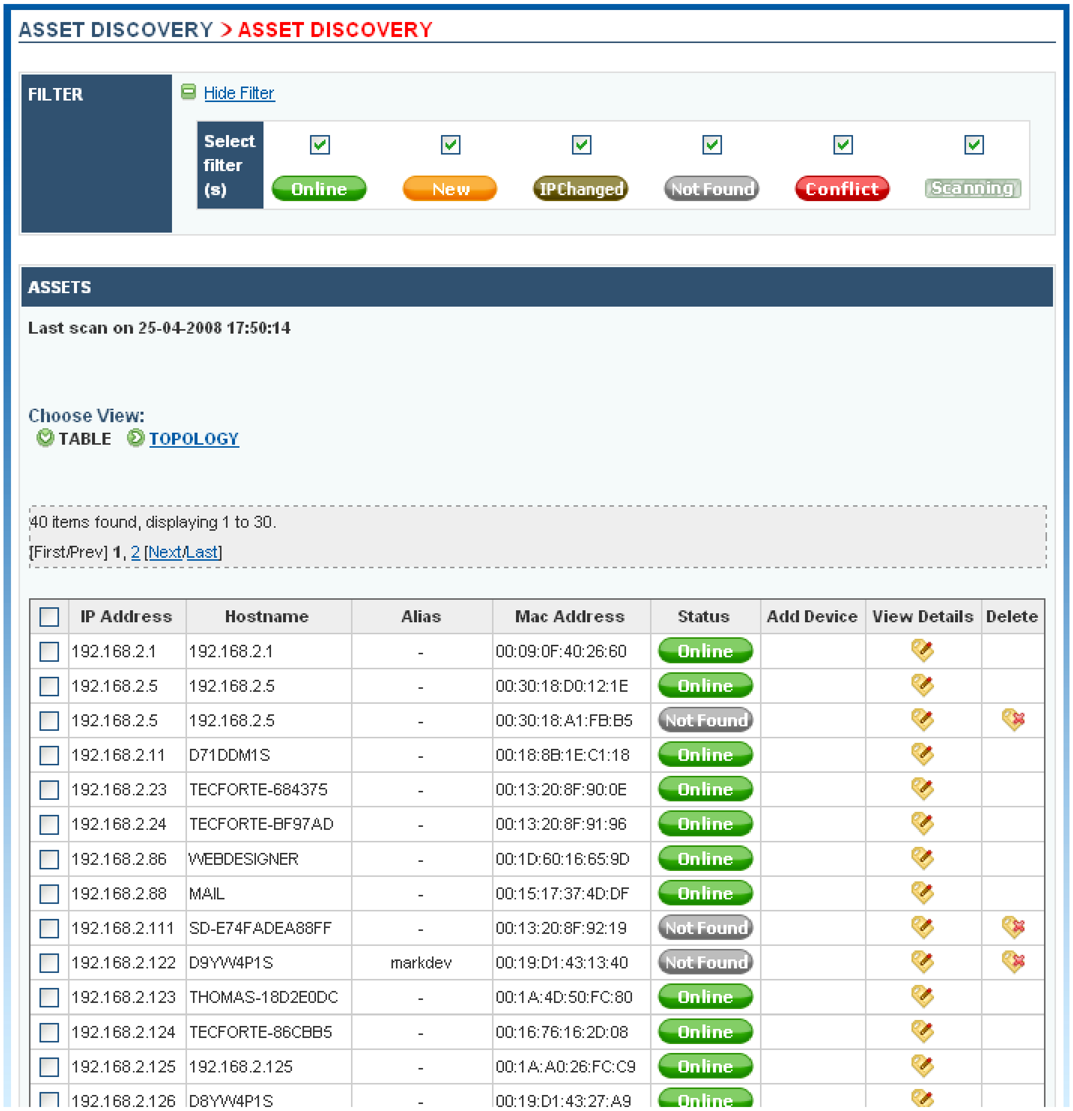
The Asset Discovery helps in managing the client environment and gives a complete view of assets and their details such as the operating system, IP address, Mac address, port and protocol. It also allows tracking of asset availability.

A network scan can be performed manually, or as a regular automated process. The Asset List will show the results from the most recent scan. Assets can also be rescanned individually to detect availability.

4.2 - Asset List

The Asset List will show all assets discovered by scanning the network. The Status of each asset is shown:

- *Online* - the asset is already known to Log Radar, and was found as expected by the scan
- *New* - the asset has been found by the scan for the first time
- *IP Changed* - the asset is already known to Log Radar, identified by the MAC address, but the IP Address was different in the previous scan. Note that this would be common in a DHCP network.
- *Not Found* - an asset is known to Log Radar, but was not found by the scan. This generally means that the asset was offline, but could also because of temporary network interruption, etc.
- *Conflict* - an asset was found on the network with an IP Address which is already associated with another asset.
- *Scanning* - the asset is currently being scanned. The Status will update when this has finished.



ASSET DISCOVERY > ASSET DISCOVERY

FILTER

Hide Filter

Select filter (s): ☑ Online ☑ New ☑ IPChanged ☑ Not Found ☑ Conflict ☑ Scanning

ASSETS

Last scan on 25-04-2008 17:50:14

Choose View:
TABLE TOPOLOGY

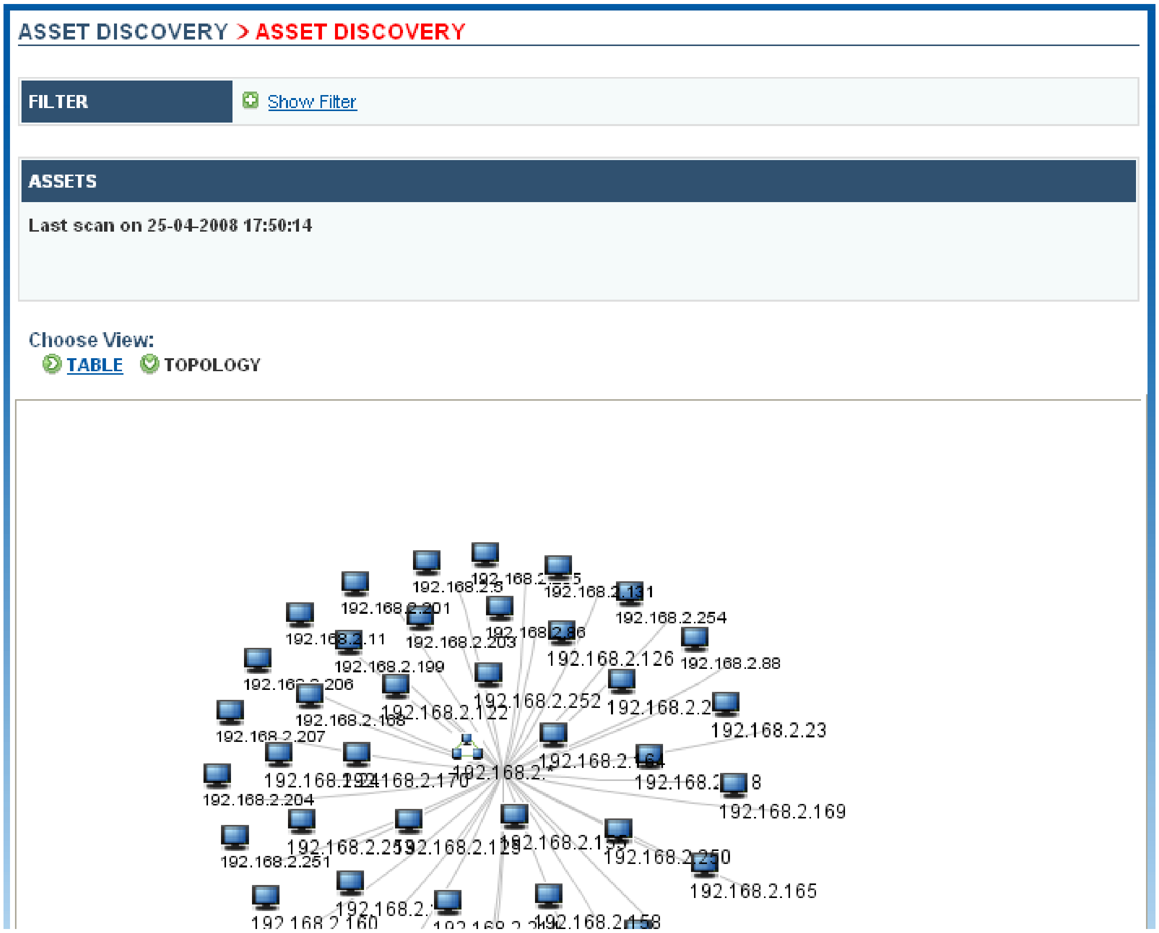
40 items found, displaying 1 to 30.
[First/Prev] **1**, 2 [Next/Last]

☐	IP Address	Hostname	Alias	Mac Address	Status	Add Device	View Details	Delete
☐	192.168.2.1	192.168.2.1	-	00:09:0F:40:26:60	Online		✎	
☐	192.168.2.5	192.168.2.5	-	00:30:18:D0:12:1E	Online		✎	
☐	192.168.2.5	192.168.2.5	-	00:30:18:A1:FB:B5	Not Found		✎	✗
☐	192.168.2.11	D71DDM1S	-	00:18:8B:1E:C1:18	Online		✎	
☐	192.168.2.23	TECFORTE-684375	-	00:13:20:8F:90:0E	Online		✎	
☐	192.168.2.24	TECFORTE-BF97AD	-	00:13:20:8F:91:96	Online		✎	
☐	192.168.2.86	WEBDESIGNER	-	00:1D:60:16:65:9D	Online		✎	
☐	192.168.2.88	MAIL	-	00:15:17:37:4D:DF	Online		✎	
☐	192.168.2.111	SD-E74FADEA88FF	-	00:13:20:8F:92:19	Not Found		✎	✗
☐	192.168.2.122	D9YW4P1S	markdev	00:19:D1:43:13:40	Not Found		✎	✗
☐	192.168.2.123	THOMAS-18D2E0DC	-	00:1A:4D:50:FC:80	Online		✎	
☐	192.168.2.124	TECFORTE-86CBB5	-	00:16:76:16:2D:08	Online		✎	
☐	192.168.2.125	192.168.2.125	-	00:1A:A0:26:FC:C9	Online		✎	
☐	192.168.2.126	D8YW4P1S	-	00:19:D1:43:27:A9	Online		✎	

The Asset List provides two alternative views.

List View shows the IP Address, the Hostname, the Alias, the MAC Address, and the Status.

Topology View shows a graphical representation of the network assets.



ASSET DISCOVERY > ASSET DISCOVERY

FILTER

Show Filter

ASSETS

Last scan on 25-04-2008 17:50:14

Choose View:

TABLE TOPOLOGY

Additional Information:

- *Alias* **-** each asset can be identified by entering an Alias. If the asset is already entered as a Device in Log Radar, then the Device Name will be used by default.
- *Add Device* - the Asset Discovery scan provides an easy way to find and add Device information to Log Radar. Each asset will provide a shortcut to add the Device details. See Chapter 7: Device Management for further information on adding Devices.
- *View Details* - the scan can provide more information on each asset, such as port status, transmitting services, OS, IP Class, etc.
- *Delete* - once an asset is known to Log Radar, it will appear in the results for every further scan. If the actual asset has been removed from the network, it will always be shown with status **Not Found**. To prevent this from reoccurring, the asset details can be deleted from the list. If the IP Address is found in a later scan, it will be given status **New**.

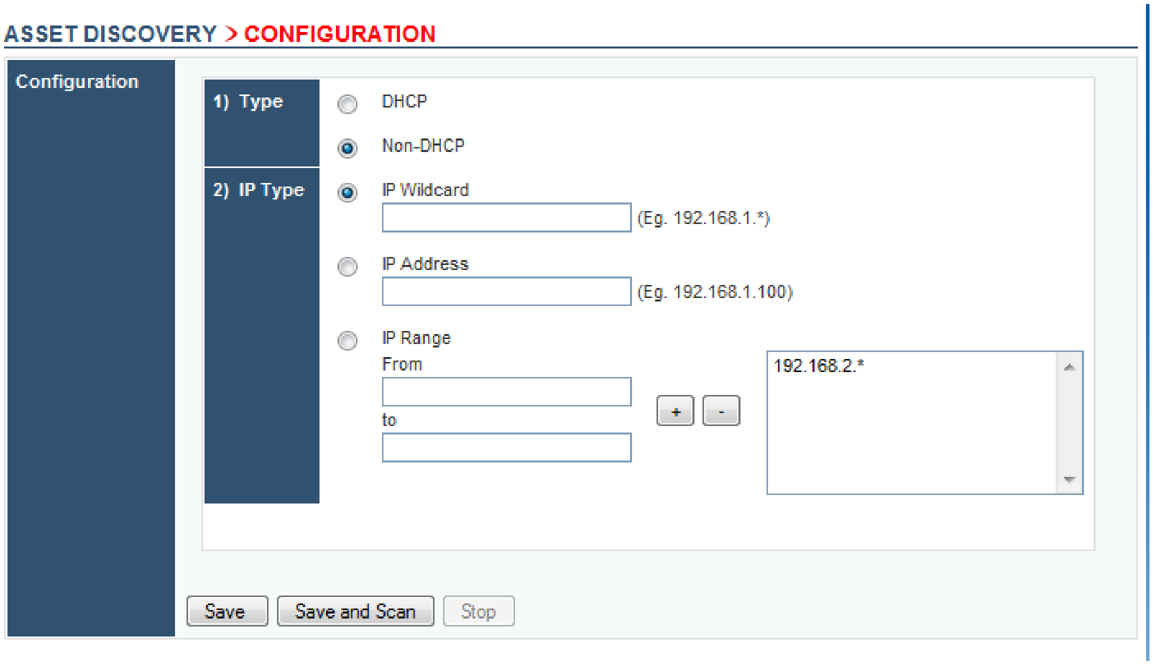
Steps to follow:

To **View Details**	1. Menu -> Asset Discovery -> Asset List 2. Find the asset you want to check details for 3. Click on <u>View Details</u> shortcut 4. Details discovered by the scan appear in a new window
To **Detect Availability**	1. Menu -> Asset Discovery -> Asset List 2. Check the boxes for each asset that you want to be rescanned 3. Click on <u>Detect Availability</u> button 4. The Status will show **Scanning** for each selected asset 5. As each asset is rescanned, the Status field will update to show the new information **Note:** Using this feature with individual assets is not recommended in a DHCP network. Instead, the entire network should be rescanned. See next section for more details.
To **Delete** an asset	1. Menu -> Asset Discovery -> Asset List 2. Find the asset you want to check details for 3. Click on ✖ to delete 4. Click <u>Delete Asset</u> button to confirm **Note:** Only assets with a status **Not Found** can be deleted. If a deleted asset is found by a later scan, it will appear back in the list with a status of **New**

4.3 - Configuration

The Asset Discovery Configuration page is where you can specify the range of IP Addresses to be scanned. You can select your entire network, or a particular subset of IP Addresses. The scan can be manually started from this page, or configured for the automated scanning instead. See next section for information on automated scanning.

The Network Type will need to be set before a scan can take place. In a non-DHCP Network there would generally be a stable relationship between MAC Address and IP Address. In a DHCP Network, the IP Addresses are assigned dynamically, and so the IP Address for a particular asset would be expected to change in between scans. In this case it is not recommended to scan individual assets as conflicts may be incorrectly reported - instead the entire network should be rescanned each time.



ASSET DISCOVERY > CONFIGURATION

Configuration

1) Type

○ DHCP

● Non-DHCP

2) IP Type

● IP Wildcard (Eg. 192.168.1.*)

○ IP Address (Eg. 192.168.1.100)

○ IP Range

From

to

192.168.2.*

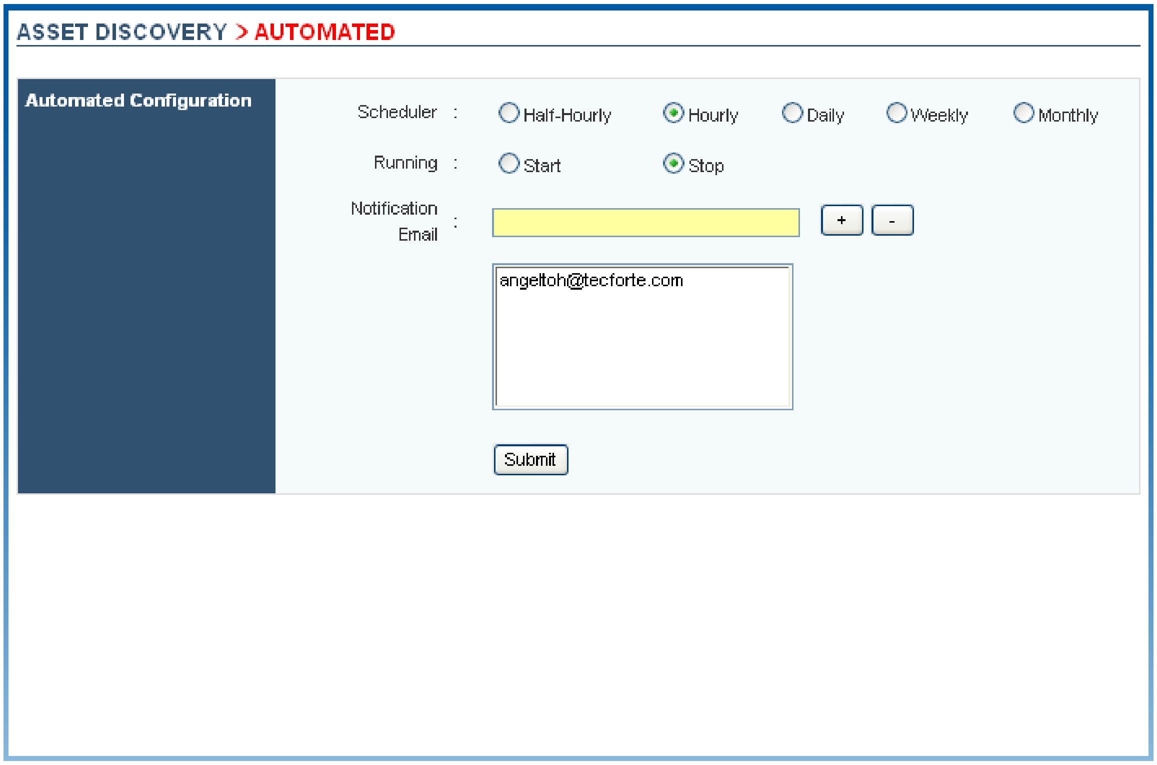
Steps to follow:

To **Save** configuration without scanning	1. Menu -> Asset Discovery -> Configuration 2. Enter the Network Type: DHCP or non-DHCP 3. Enter the IP Addresses you want to be scanned. You can enter these as a range, or using wildcards (e.g. 192.168.4.*) 4. Click on <u>Save</u> button 5. The entered information will be saved, and used the next time a scan is started
To **Save and Scan**	1. Menu -> Asset Discovery -> Configuration 2. Enter the Network Type: DHCP or non-DHCP 3. Enter the IP Addresses you want to be scanned. You can enter these as a range, or using wildcards (e.g. 192.168.4.*) 4. Click on <u>Save and Scan</u> button 5. The entered information will be saved, and a scan will begin based on the entered information **Note:** A new scan cannot be started while another scan is in progress. This includes automated scans, manual scans, and detecting availability on individual assets.
To **Stop** a scan in progress	1. Menu -> Asset Discovery -> Configuration 2. Click on the <u>Stop</u> button 3. The Scan in progress will be stopped **Note:** It can take a while to stop the scanning process. During this time, a new scan cannot be started.

4.4 - Automated

The Asset Discovery Automated Configuration page allows you to schedule a full network scan to occur as a repeating process. The scan will be based on the IP range defined in the Asset Discovery Configuration page - see *Section 4.4 Automated Asset Discovery* for more details.

The results of each automated scan will appear in the Asset List when the scan has completed. The results can also be sent out by email.



Scheduler : ○ Half-Hourly ● Hourly ○ Daily ○ Weekly ○ Monthly

Running : ○ Start ● Stop

Notification Email :

angeltoh@tecforte.com

Steps to follow:

To **Start** running the automated scans	1. Menu -> Asset Discovery -> Automated 2. Enter the frequency to perform the scans 3. Check the Start checkbox 4. If required, enter email addresses and add them

	with the + button 5. Click on Submit button to save the changes
To **Stop** running the automated scans	1. Menu -> Asset Discovery -> Automated 2. Check the Stop checkbox 3. Click on Submit button to save the changes
To **Enter email addresses**	1. Menu -> Asset Discovery -> Automated 2. Enter an email address in the Notification Email field 3. Press + button to add the entered email address 4. Repeat steps 2 and 3 to enter additional email addresses 5. Click on Submit button to save the changes.

5. Real-time Threats

5.1 - Overview

Managing a network has been a critical task, involving manual procedure of log and alert monitoring, false positive detection, events and logs filtration. The crucial of this activity depends on the size of network and number of devices. Analyzing logs from every device, correlating and concluding it the traditional way is not possible for real time attack detection.

Real Time Threats will perform real time analysis on logs NOT BY querying from the database but collecting real time logs by streaming from all devices, consolidating to one point and analyzing it in Log Radar's Correlation engine which will handle further analysis on the logs.

The Correlation architecture has a standalone function called the global counter which keeps count of the IP Address of every inbound and outbound log in the network. The main engine has few filters which are created dynamically when a rule is created or edited. Raw logs will be passed to the filter to match the criteria, keyword, pattern, threshold, frequency and event classification using AND, OR, FollowBy function.

Using Correlation will help:

- reduce data by removing of duplicate logs and categorizing it as an event,
- with the use of Threshold and Frequency, no more redundant alert,
- prevent false positive logs with meaningful Correlation,
- alert based on Correlation and network event classification,
- getting less triggered event, rather than huge triggered logs,
- Sequential event detection to get an event-trail.

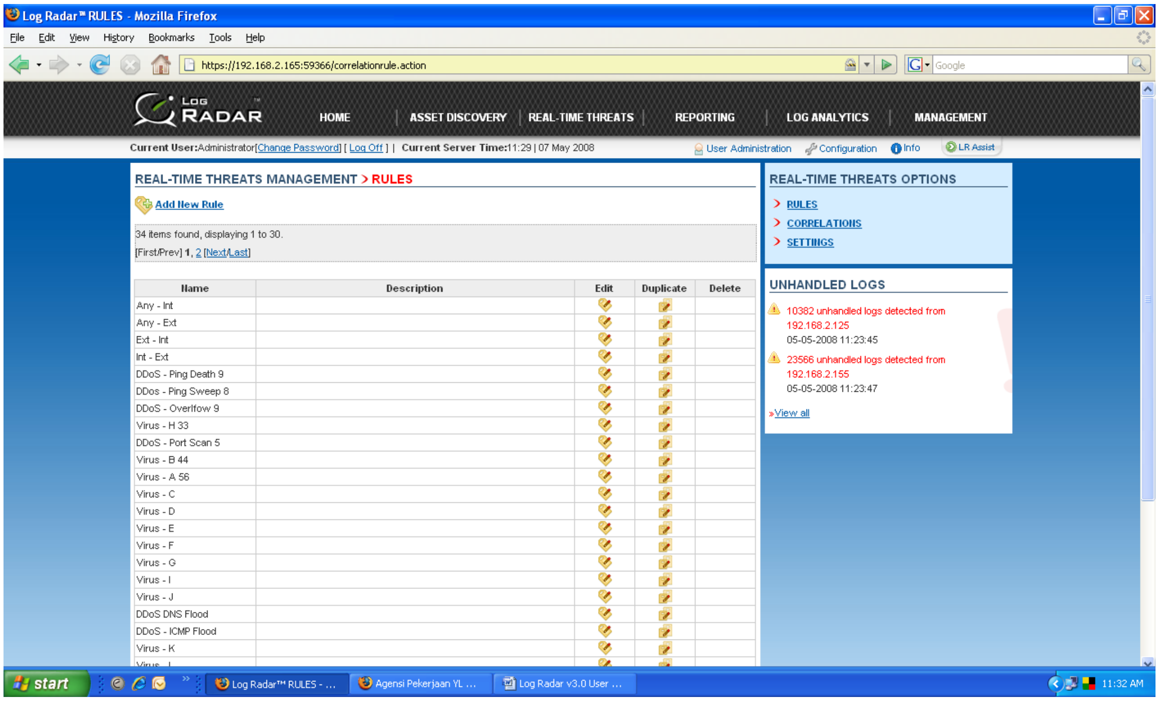
But,

- creating correlation can be very complicating,
- need IDS/ network security knowledge,
- If not created wisely, will use up a lot of resources.

It is useful for network/ system administrators or users who work on privacy & security to get an intelligent report on the event happening on the network. This module will solve the problems addressed above efficiently.

5.2 - Rules

Rule’s main page displays rule name, its description and [Actions: Edit, Duplicate, Delete] allowed for the particular rule.



Current User:Administrator[Change Password] [Log Off] | Current Server Time:11:29 | 07 May 2008

REAL-TIME THREATS MANAGEMENT > RULES

Add New Rule

34 items found, displaying 1 to 30.
[First/Prev] **1**, 2 [Next/Last]

Name	Description	Edit	Duplicate	Delete
Any - Int		✎	✎	
Any - Ext		✎	✎	
Ext - Int		✎	✎	
Int - Ext		✎	✎	
DDoS - Ping Death 9		✎	✎	
DDos - Ping Sweep 8		✎	✎	
DDoS - Overlfow 9		✎	✎	
Virus - H 33		✎	✎	
DDoS - Port Scan 5		✎	✎	
Virus - B 44		✎	✎	
Virus - A 56		✎	✎	
Virus - C		✎	✎	
Virus - D		✎	✎	
Virus - E		✎	✎	
Virus - F		✎	✎	
Virus - G		✎	✎	
Virus - I		✎	✎	
Virus - J		✎	✎	
DDoS DNS Flood		✎	✎	
DDoS - ICMP Flood		✎	✎	
Virus - K		✎	✎	

REAL-TIME THREATS OPTIONS

- RULES
- CORRELATIONS
- SETTINGS

UNHANDLED LOGS

10382 unhandled logs detected from 192.168.2.125
05-05-2008 11:23:45

23566 unhandled logs detected from 192.168.2.155
05-05-2008 11:23:47

»View all

Criteria Information

Information Tab
Rule name * - enter something related to the rule criteria
Description - must be understood by all

Devices Tab
Device *[+] -logs will be filtered from the selected device only.

[+] Multiple entries allowed * Compulsory

Criteria Tab

Select and fill up the following, and must fulfil at least one criterion.

Note: Selection of "Any" is not considered as a "criteria"

a. Source / Destination IP* – select either 1 from below
    - Any,
    - Internal Any,
    - External Any,
    - Fixed IP and Range - Predefined / Manual entry [+]

b. Source / Destination Port* - select either 1 from below
    - Any,
    - Fixed Port and Range -Predefined / Manual entry [+]

c. Source / Destination Host
    - Manual entry on the hostname

d. Username
    - Manual entry on the username

e. Packets / Bytes Sent and Received
    - Manual entry on Integer

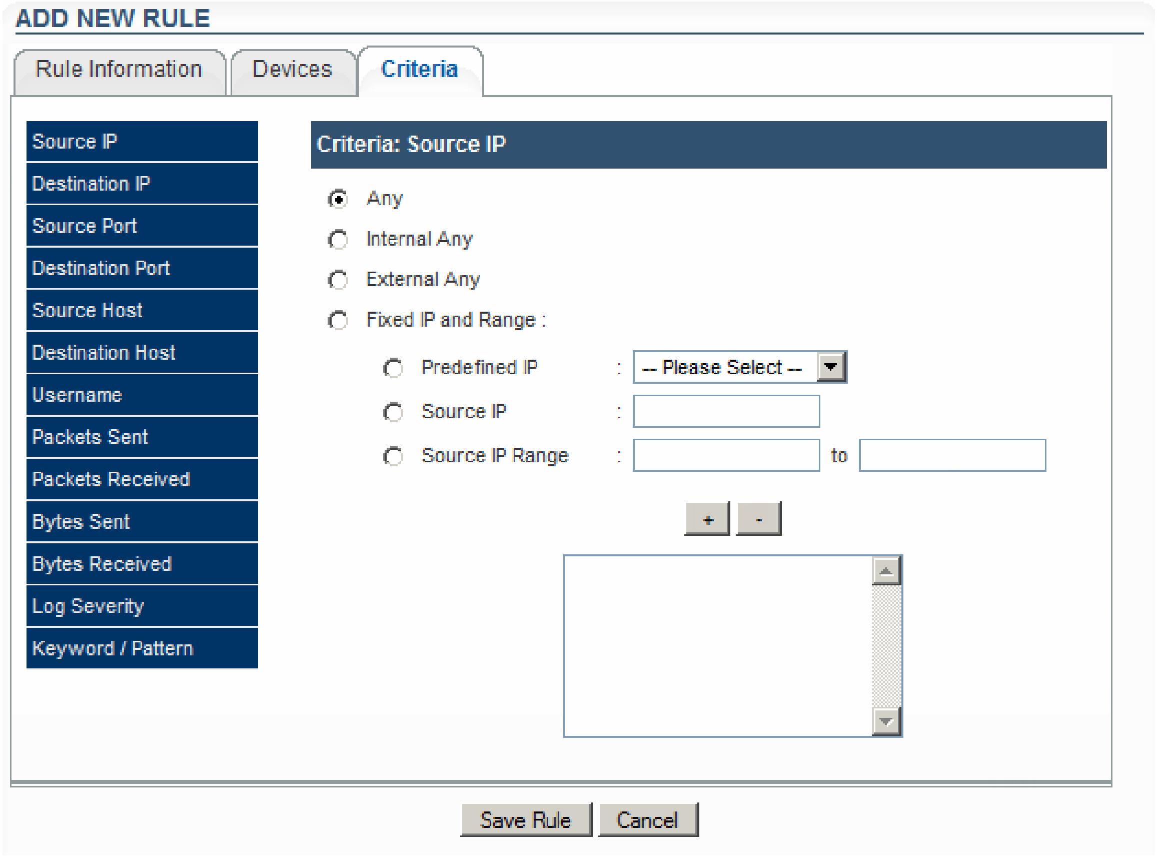
f. Log Severity
    - Selection box [+]

g. Keyword / Pattern Matching- select either 1 from below

    i. Keyword – (dependent: auto populated based on selection)
        - Keyword Category, - select first
        - Keyword List, - select second
        - Related Keyword [+] - select last

    ii. Pattern Matching
        - Manual entry of word or string pattern to filter

[+] Multiple entries allowed *Compulsory



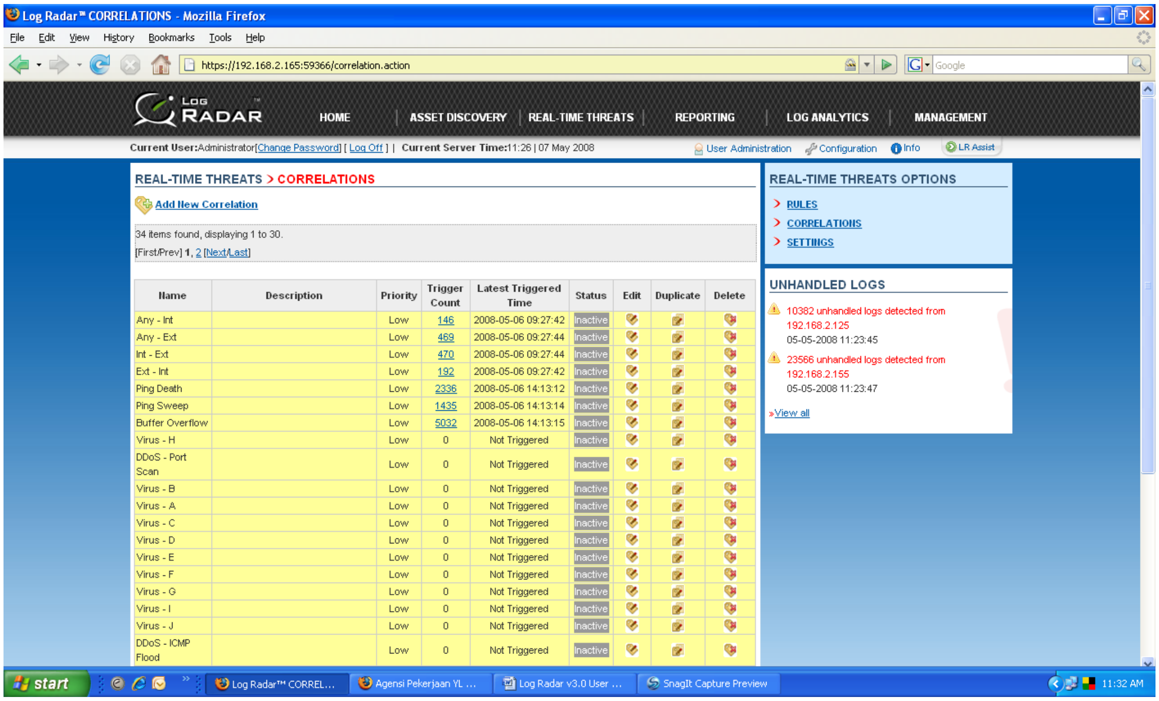
Steps to follow:

To **Add** Rule	1. Menu -> Real-Time Threats -> Rules 2. Click on link Add New Rule 3. Enter Rule Information 4. Select Devices 5. Enter Criteria 6. Click Save Rule button to save the new Rule **Note:** Existing Rules can be duplicated to save user's time.
To **Edit** Rule	1. Menu -> Real-Time Threats -> Rules 2. Find the Rule you want to edit 3. Click on ✎ to edit

	4. Make the desired changes 5. Click <u>Save Rule</u> button to save the changes and restarts the search **Note:** Editing Rules is not allowed if they are used on any Active Correlations. The Correlations must be made Inactive first.
To **Delete** Rule	1. Menu -> Real-Time Threats -> Rules 2. Find the Rule you want to delete 3. Click on ✖ to delete 4. Click <u>Delete Rule</u> button to confirm **Note:** Deleting Rules is not allowed if they are used on any Correlations. The Correlations must be edited to remove the Rule first.

5.3 - Correlations

Correlation’s main page displays Correlation name, description, priority, trigger count, latest triggered time, [Status: Active/ Inactive] and [Actions: Edit, Duplicate, Delete] allowed.



Current User:Administrator[Change Password] [Log Off] | Current Server Time:11:26 | 07 May 2008

REAL-TIME THREATS > CORRELATIONS

Add New Correlation

34 items found, displaying 1 to 30.

[First/Prev] **1**, 2 [Next/Last]

Name	Description	Priority	Trigger Count	Latest Triggered Time	Status	Edit	Duplicate	Delete
Any - Int		Low	146	2008-05-06 09:27:42	Inactive	✎	⧉	✖
Any - Ext		Low	469	2008-05-06 09:27:44	Inactive	✎	⧉	✖
Int - Ext		Low	470	2008-05-06 09:27:44	Inactive	✎	⧉	✖
Ext - Int		Low	192	2008-05-06 09:27:42	Inactive	✎	⧉	✖
Ping Death		Low	2336	2008-05-06 14:13:12	Inactive	✎	⧉	✖
Ping Sweep		Low	1435	2008-05-06 14:13:14	Inactive	✎	⧉	✖
Buffer Overflow		Low	5032	2008-05-06 14:13:15	Inactive	✎	⧉	✖
Virus - H		Low	0	Not Triggered	Inactive	✎	⧉	✖
DDoS - Port Scan		Low	0	Not Triggered	Inactive	✎	⧉	✖
Virus - B		Low	0	Not Triggered	Inactive	✎	⧉	✖
Virus - A		Low	0	Not Triggered	Inactive	✎	⧉	✖
Virus - C		Low	0	Not Triggered	Inactive	✎	⧉	✖
Virus - D		Low	0	Not Triggered	Inactive	✎	⧉	✖
Virus - E		Low	0	Not Triggered	Inactive	✎	⧉	✖
Virus - F		Low	0	Not Triggered	Inactive	✎	⧉	✖
Virus - G		Low	0	Not Triggered	Inactive	✎	⧉	✖
Virus - I		Low	0	Not Triggered	Inactive	✎	⧉	✖
Virus - J		Low	0	Not Triggered	Inactive	✎	⧉	✖
DDoS - ICMP Flood		Low	0	Not Triggered	Inactive	✎	⧉	✖

REAL-TIME THREATS OPTIONS

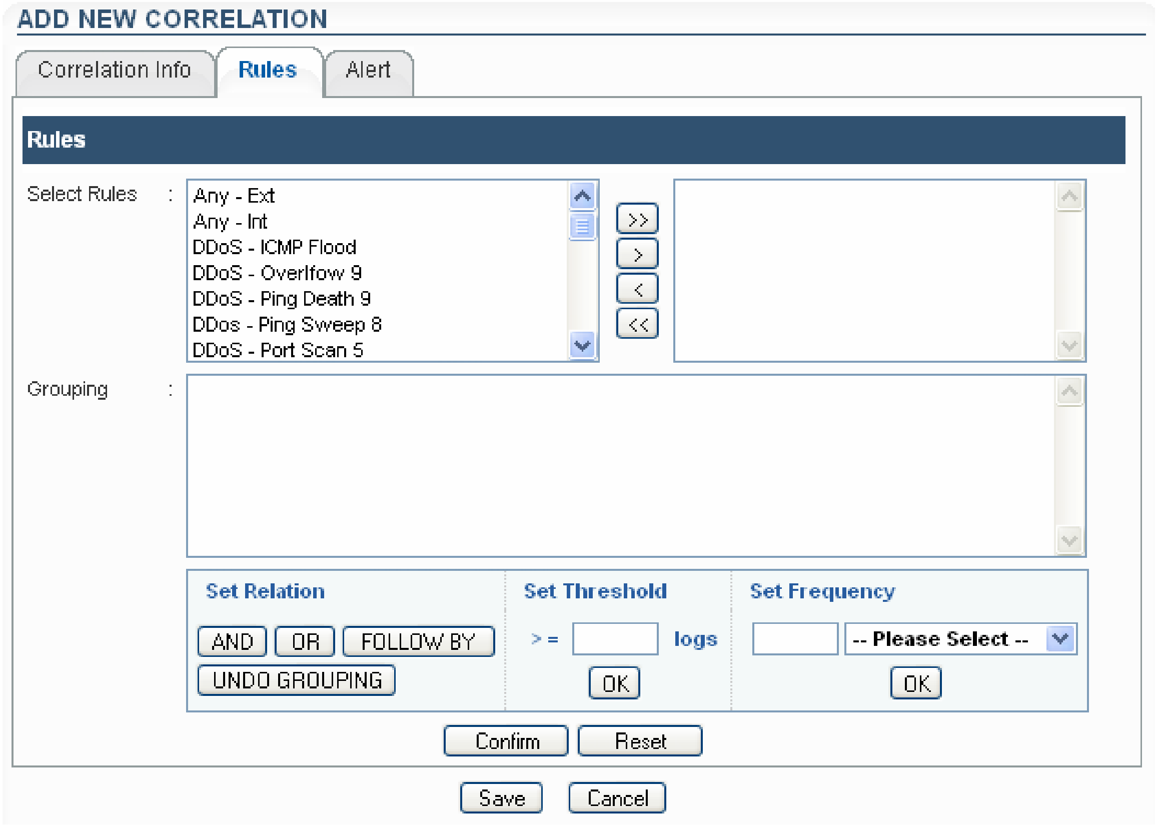
- RULES
- CORRELATIONS
- SETTINGS

UNHANDLED LOGS

⚠ 10382 unhandled logs detected from 192.168.2.125
05-05-2008 11:23:45

⚠ 23566 unhandled logs detected from 192.168.2.155
05-05-2008 11:23:47

»View all



Correlation Info Tab

Correlation Name*	- something related to the event to be triggered
Description	- brief explanation about the correlation
Importance *	- selection [High / Med / Low]
Status *	- selection [Active/ Inactive]

Rules Tab

Select Rules*[+]	- select rules to be used in correlation
Rule Grouping*	- see below (Instructions on Rule Grouping)
Undo Grouping	- to undo the last step of rule grouping
Threshold*	- entry of number of logs to trigger
Frequency*	- entry of secs / minutes to trigger

[+] Multiple entries allowed *Compulsory

Button: Confirm*	- to confirm the grouped rules
Button: Reset	- to reset the page
Button: Save*	- save the correlation

Alert Tab

Alert Name	- by default will be correlation name
Action	- email / log only
User Group	- populated from user Management group
User List [+]	- selection from list of the group above

Instructions on Rule Grouping

Rule Tab:

1. Select one/ more rule(s) to be correlated. Selected rules will appear in the Grouping Box.

2. Click on the Rule in the Grouping box to set Threshold and Frequency.*

3. Select rules in the Grouping box to be grouped with AND, OR, and FOLLOW BY relation and make sure the correct rules are highlighted, and then click on the appropriate button.

4. To group the rules with AND, OR, and FOLLOW BY relation, it must meet some conditions which are listed in the next line.

5. Rule Grouping Condition:

    i. Every grouped rule must have threshold and frequency.
    ii. Triggers only when it hits the threshold within the frequency.

    AND
    i. Used with more than one ungrouped rule
    ii. Both rules are not set with threshold and frequency yet.
    iii. Both rules are set with threshold but not with frequency yet.
    iv. Triggers only when both rules have triggered at the backend.

    OR
    i. Used with more than one ungrouped rule
    ii. Both rules are not set with threshold and frequency yet.
    iii. Both rules are set with threshold but not with frequency yet.
    iv. Triggers when any one of the rule had triggered.

[+] Multiple entries allowed *Compulsory

    FOLLOW BY
    i. Used with more than 1 grouped rule
    ii. Both rules must be grouped and have threshold and frequency.

iii. When the first grouped rule had triggered, it will start executing the second group of rule and so on.
iv. Triggers when all the grouped rules have triggered.

Example:

a. **Single grouped rule**
(Rule1; threshold=? frequency=? secs/ mins)

b. **AND / OR**
((Rule1 AND Rule2); threshold=? frequency=? secs/ mins)

((Rule1 OR Rule2); threshold=? frequency=? secs/ mins)

((Rule1; threshold=? AND Rule2; threshold=? ;) frequency=? secs/ mins)

((Rule1; threshold=? OR Rule2; threshold=? ;) frequency=? secs/ mins)

c. **FOLLOW BY**
((Rule1; threshold=? frequency=? secs/ mins) FollowBy (Rule2; threshold=? frequency=? secs/ mins))

(((Rule1; threshold=? AND Rule2; threshold=? ;) frequency=? secs/ mins) FollowBy ((Rule3; threshold=? OR Rule4; threshold=? ;) frequency=? secs/ mins))

Steps to follow:

To **Add** Correlation	1. Menu -> Real-Time Threats -> Correlations 2. Click on link Add New Correlation 3. Enter Correlation Information 4. Select Rules, and complete Grouping 5. Enter Alert actions 6. Click Save Correlation button to save the new Correlation

To **Edit** Correlation	1. Menu -> Real-Time Threats -> Correlations 2. Find the Correlation you want to edit 3. Click on ✎ to edit 4. Make the desired changes 5. Click Save Correlation button to save the changes **Note:** You can quickly switch the status between Active/Inactive by clicking on the Correlation List.
To **Delete** Correlation	1. Menu -> Real-Time Threats -> Correlations 2. Find the Correlation you want to delete 3. Click on ✗ to delete 4. Click Delete Correlation button to confirm **Note:** Deleting Correlations is not allowed if it is Active. The Correlation must first be set to Inactive.

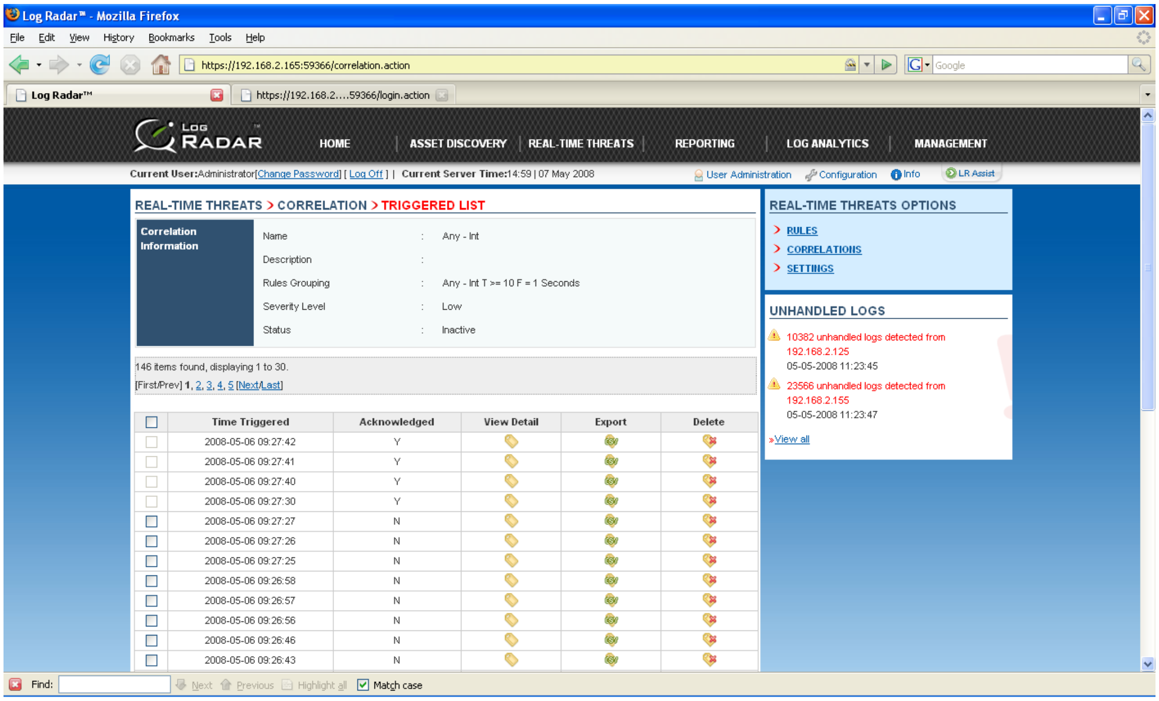
Trigger

Once correlation is created, it immediately initiates at the back-end to capture logs and match the rule's criteria, count the threshold within the frequency.
If it fulfils all the above, then a trigger signal is sent to update required files and increase the 'trigger count' in the database and refresh the display at Correlation Main Page together with 'last triggered time'.

Trigger Details

To view the trigger details, user must click on the 'trigger count' which will open a new window with all the trigger count files. Click on the View Details icon to view a particular triggered 'Date & Time' view the detail of triggered report.

Upon viewing, the report can be acknowledged by checking the check box on the side every triggered date time of the report and clicking on Acknowledge button.



Current User:Administrator[Change Password] [Log Off] | Current Server Time:14:59 | 07 May 2008

REAL-TIME THREATS > CORRELATION > TRIGGERED LIST

Correlation Information

Name : Any - Int
Description :
Rules Grouping : Any - Int T >= 10 F = 1 Seconds
Severity Level : Low
Status : Inactive

146 items found, displaying 1 to 30.
[First/Prev] 1, 2, 3, 4, 5 [Next/Last]

☐	Time Triggered	Acknowledged	View Detail	Export	Delete
☐	2008-05-06 09:27:42	Y	🏷	CSV	✗
☐	2008-05-06 09:27:41	Y	🏷	CSV	✗
☐	2008-05-06 09:27:40	Y	🏷	CSV	✗
☐	2008-05-06 09:27:30	Y	🏷	CSV	✗
☐	2008-05-06 09:27:27	N	🏷	CSV	✗
☐	2008-05-06 09:27:26	N	🏷	CSV	✗
☐	2008-05-06 09:27:25	N	🏷	CSV	✗
☐	2008-05-06 09:26:58	N	🏷	CSV	✗
☐	2008-05-06 09:26:57	N	🏷	CSV	✗
☐	2008-05-06 09:26:56	N	🏷	CSV	✗
☐	2008-05-06 09:26:46	N	🏷	CSV	✗
☐	2008-05-06 09:26:43	N	🏷	CSV	✗

UNHANDLED LOGS

10382 unhandled logs detected from 192.168.2.125
05-05-2008 11:23:45

23566 unhandled logs detected from 192.168.2.155
05-05-2008 11:23:47

Viewing the triggered report will show report on all the grouped rules in correlation but to view a particular Rule's report, click on the Rule name displayed in the grouping above and it will show report for individual rule.

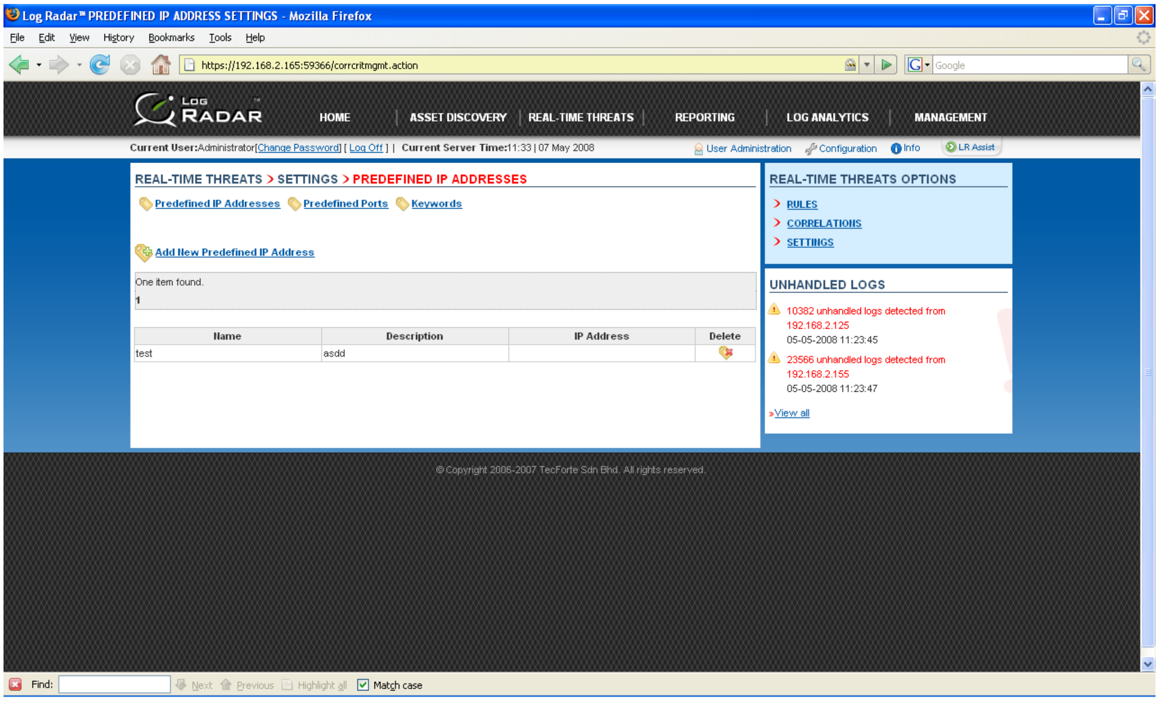
Steps to follow:

To **Acknowledge Trigger Reports**	1. Menu -> Real-Time Threats -> Correlations 2. Find the Correlation you want to view results for 3. Click on the Trigger Count to see the Triggered List 4. Check the boxes for all Trigger Reports that you wish to acknowledge. 5. Click on Acknowledge button 6. The Acknowledged Status will change to **Y** for each selected Trigger Report
To **Delete Trigger Reports**	1. Menu -> Real-Time Threats -> Correlations 2. Find the Correlation you want to delete Trigger Reports for 3. Click on the Trigger Count to see the Triggered List

	4. Find the Trigger Report that you want to delete 5. Click on 🏷✖ 6. Click <u>Delete Report</u> to confirm
To **View Normalized Log information**	1. Menu -> Real-Time Threats -> Correlations 2. Find the Correlation you want to view results for 3. Click on the Trigger Count to see the Triggered List 4. Find the Trigger Report that you want to view 5. Click on 🏷 6. The log information will open in a new window, showing the normalised log information.
To **View Raw Log information**	1. Menu -> Real-Time Threats -> Correlations 2. Find the Correlation you want to view results for 3. Click on the Trigger Count to see the Triggered List 4. Find the Trigger Report that you want to view 5. Click on 🏷 6. The log information will open in a new window, showing the normalised log information. 7. Select the **Raw Log** checkbox, and click <u>View Now</u> button
To **Export Log information**	1. Menu -> Real-Time Threats -> Correlations 2. Find the Correlation you want to export results for 3. Click on the Trigger Count to see the Triggered List 4. Find the Trigger Report that you want to view 5. Click on CSV 6. Click <u>Save</u> button 7. Enter location to save the CSV file, and click <u>Save</u>

5.4 - Predefined Data

This is where data is maintained for all predefined entries used during adding new rule. There are 3 main categories can be predefined by users, Predefined IP Address, Predefined Ports and Keywords.



Current User:Administrator[Change Password] [Log Off] | Current Server Time:11:33 | 07 May 2008

REAL-TIME THREATS > SETTINGS > PREDEFINED IP ADDRESSES

One item found.
1

Name	Description	IP Address	Delete
test	asdd		

UNHANDLED LOGS

10382 unhandled logs detected from 192.168.2.125
05-05-2008 11:23:45

23566 unhandled logs detected from 192.168.2.155
05-05-2008 11:23:47

© Copyright 2006-2007 TecForte Sdn Bhd. All rights reserved.

5.4.1 Predefined IP Address

Displays all pre-defined IP Addresses with description.

Add New Predefined IP Address
Name* -new entry
Description

*At least one entry for either one **
IP [+] -new entry
IP Range [+] -new entry

[+] Multiple entries allowed * Compulsory

5.4.2 Predefined Ports

Displays all pre-defined port names and numbers.

Add New Predefined Ports
- Name* -new entry
- Description

*At least one entry for either one **
- Port [+] -new entry
- Port Range [+] -new entry

5.4.3 Keyword

Displays Keyword Category and Related Keyword.

Add New Keyword
- Keyword Name * - new entry
- Keyword Category * - selection

*At least one entry for either one **
- Related keyword List [+] - selection
- New related keyword Name [+] - new entry

[+] Multiple entries allowed * Compulsory

6. Log Analytics

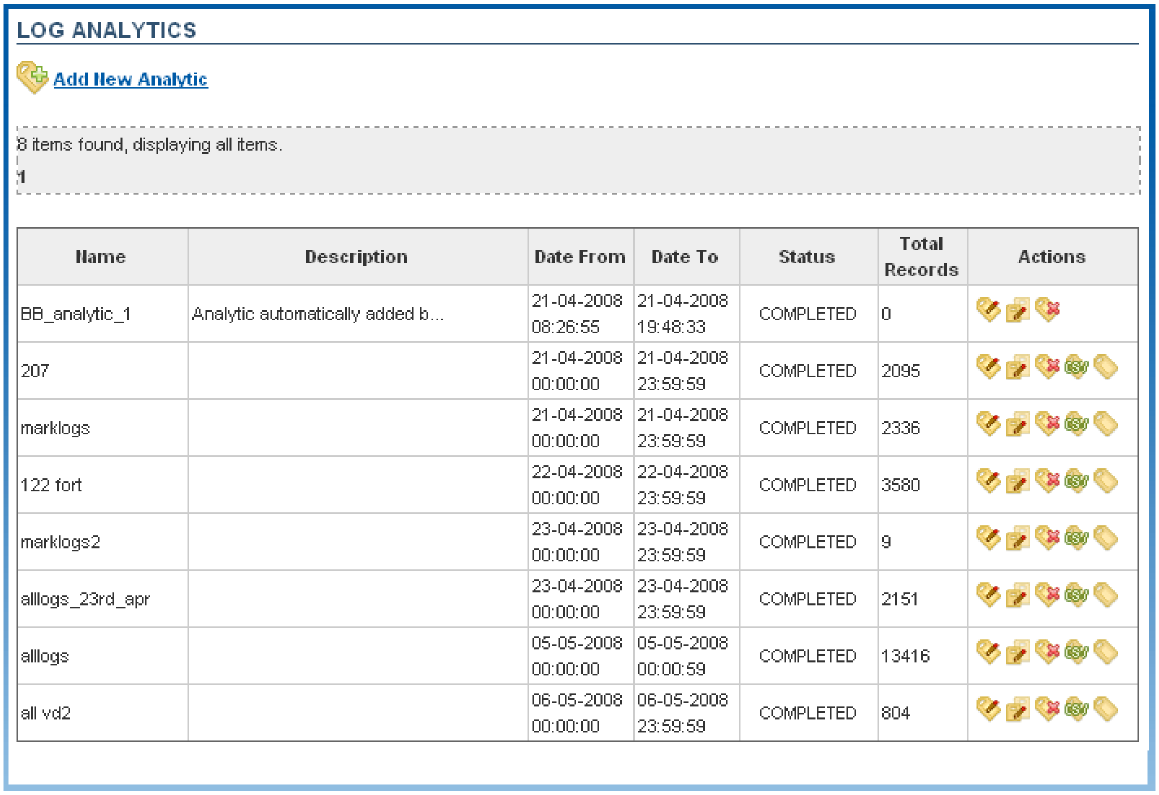
6.1 - Overview

The Log Analytics module is for performing forensic searches on the log data. Several different criteria options are provided to allow maximum flexibility in returning the desired logs as quickly and efficiently as possible.

The results of a Log Analytic search can be viewed within Log Radar. You can select to view both the normalised data, and the raw log information. The results can also be exported locally in CSV format.

6.2 - Log Analytics List

The Log Analytics list shows the past searches performed, together with the dates of the search, and the total records found. The results of a past search can be viewed and exported without needing to rerun the search.



LOG ANALYTICS

Add New Analytic

8 items found, displaying all items.
1

Name	Description	Date From	Date To	Status	Total Records	Actions
BB_analytic_1	Analytic automatically added b...	21-04-2008 08:26:55	21-04-2008 19:48:33	COMPLETED	0	
207		21-04-2008 00:00:00	21-04-2008 23:59:59	COMPLETED	2095	CSV
marklogs		21-04-2008 00:00:00	21-04-2008 23:59:59	COMPLETED	2336	CSV
122 fort		22-04-2008 00:00:00	22-04-2008 23:59:59	COMPLETED	3580	CSV
marklogs2		23-04-2008 00:00:00	23-04-2008 23:59:59	COMPLETED	9	CSV
alllogs_23rd_apr		23-04-2008 00:00:00	23-04-2008 23:59:59	COMPLETED	2151	CSV
alllogs		05-05-2008 00:00:00	05-05-2008 00:00:59	COMPLETED	13416	CSV
all vd2		06-05-2008 00:00:00	06-05-2008 23:59:59	COMPLETED	804	CSV

For every Log Analytic, the following fields are necessary:

- *Name* - this is to identify the Analytic
- *Date From/Time From* - Only logs received after this date/time will be returned
- *Date To/Time To* - Only logs received before this date/time will be returned
- *Devices* - only logs received from the selected Devices will be returned
- *Criteria* - only logs matching the entered criteria will be returned. You must enter one or more criteria to perform a search. The available criteria are:
    - Source IP
    - Destination IP
    - Source Port
    - Destination Port
    - Source Host
    - Destination Host
    - Username
    - Packets Sent
    - Packets Received
    - Bytes Sent
    - Bytes Received
    - Severity
    - Pattern Matching
    - IP Classification

Steps to follow:

To **Add** Analytic	1. Menu -> Log Analytics 2. Click on link Add New Analytic 3. Enter Analytic Information 4. Select Devices 5. Enter Criteria 6. Click Save Analytic button to save the new Analytic and begin the search **Note:** Existing Analytics can be duplicated to save user's time.

To **Edit** Analytic	1. Menu -> Log Analytics 2. Find the Analytic you want to edit 3. Click on ✎ to edit 4. Make the desired changes 5. Click <u>Save Analytic</u> button to save the changes and restarts the search **Note:** Editing an Analytic will always restart the search according to the entered criteria, even when no changes have been made. To close the window without restarting the search, click the <u>Cancel</u> button instead.
To **Delete** Analytic	1. Menu -> Log Analytics 2. Find the Analytic you want to delete 3. Click on ✖ to delete 4. Click <u>Delete Analytic</u> button to confirm
To **View Normalized Log information**	1. Menu -> Log Analytics 2. Find the Analytic you want to view results for 3. Click on 🏷 4. The log information will open in a new window, showing the normalised log information.
To **View Raw Log information**	1. Menu -> Log Analytics 2. Find the Analytic you want to view results for 3. Click on 🏷 4. The log information will open in a new window, showing the normalised log information. 5. Select the **Raw Log** checkbox, and click <u>View Now</u> button
To **Export Log information**	1. Menu -> Log Analytics 2. Find the Analytic you want to export results for 3. Click on CSV 4. Click <u>Save</u> button 5. Enter location to save the CSV file, and click <u>Save</u>

7. Reporting

7.1 - Overview

The Reporting module provides centralized data management and analysis to assist users in review and monitor of network traffic to understanding over the Network Behaviour. Reporting is also acting as a tool to assist user to identify the source of attack and manage the traffic bandwidth usage base on devices. Drill Down functionality is also include into reporting module to allowed user to see the details behind the summary statistic which is helping in data filtering and data extraction needs in an indirect manner.

LR Reporting is appearance with 8 Category and each of the categories is grouping the report base on the log that collected from the devices.

1. Attack
2. Event
3. Traffic
4. Virus
5. Anti Spam
6. Web Activity
7. VPN
8. Windows
9. Performance & Utilization

The Compliance Report provides a collection of reports required by the Regulatory Compliance.

1. PCI DSS
2. SOX (COBIT)
3. HIPAA
4. ISO 27002

7.2 - List of Reports by Category

Category: ATTACK	Description
Top Attackers Report	List of the top Attackers over the selected time period, by Source/Protocol. Drilldown on each Source/Protocol combination to view the details of the Attacks.
Top Targets Report	List of the top Targets over the selected time period, by Destination/Protocol. Drilldown on each Destination/Protocol combination to view the details of the Attacks.
Top Protocol Used by Attack Report	List of the top Protocols used by Attacks over the selected time period. Drilldown on each Protocol to view the details of the Attacks.
Top Attacks Report	List of the top Attacks over the selected time period, by Attack Type. Drilldown on each Attack Type to view the details of the Attacks.
Top Internal Attackers Report	List of the top Internal Attackers over the selected time period, by Source. Drilldown on each Source to view the details of the Attacks.
Top External Attackers Report	List of the top External Attackers over the selected time period, by Source. Drilldown on each Source to view the details of the Attacks.
Top Internal Targets Report	List of the top Internal Targets over the selected time period, by Destination. Drilldown on each Destination to view the details of the Attacks.
Top External Targets Report	List of the top External Targets over the selected time period, by Destination. Drilldown on each Destination to view the details of the Attacks.
Top Attack Destination Port Report	List of the top attacks destination port over the selected time period, by attack type. Drilldown on each attack type to view the details of the attacks.
Category: EVENT	**Description**
Summary of Event Report	Summary of all Event logs over the selected time period, by Severity and Number of Hits. Total Bytes Sent/Received also shown for each Severity. Drilldown on each Severity to view the Sources of the Events. Drilldown further on each Source to view the details of the Events.
Top Generator Report	List of the top Event logs over the selected time period, by Source and Severity.

	Drilldown on each Source/Severity combination to view the details of the Events.

Category: VIRUS	Description
Top Virus Sources Report	List of the top Sources of Virus intrusions over the selected time period. Drilldown on each Source to view the details of the Virus messages.
Top Virus Destination Report	List of the top Destinations of Virus intrusions over the selected time period. Drilldown on each Destination to view the details of the Virus messages.
Top Protocol Used by Virus Report	List of the top Protocols used in Virus intrusions over the selected time period. Drilldown on each Protocol to view the details of the Virus messages.
Top Virus Report	List of the top Virus intrusions over the selected time period, by Virus Name. Drilldown on each Virus Name to view the details of the Virus messages.
Hourly Viruses Blocked Report	List of the top virus intrusions over the selected time period, by virus name. Drilldown on each virus name to view the details of the virus messages.
Daily Viruses Blocked Report	List of the top virus intrusions over the selected time period, by virus name. Drilldown on each virus name to view the details of the virus messages.
Top Blocked Viruses Report	List of the top virus intrusions over the selected time period, by virus name. Drilldown on each virus Name to view the details of the virus messages.

Category: TRAFFIC	Description
Summary of Traffic Report	Summary of all Traffic Flows over the selected time period, by Classification and Status. Drilldown on each Classification/Status combination to view the details of the Traffic Flows.
Summary of Bandwidth Usage Report	Summary of Bandwidth Usage over the selected time period, by Classification, Number of Hits, and Bytes Transferred. Drilldown on each Classification to view the details of the Traffic Flows.
Top Traffic Source Report	List of the top Traffic Flow Sources over the selected time period, by Source/Protocol and Status. Drilldown on each Source/Protocol/Status combination to view the details of the Traffic Flows.
Top Allowed Traffic Source Report	List of the top allowed Traffic Flow Sources over the selected time period, by Source/Protocol. Drilldown on each Source/Protocol combination to view the details of the allowed Traffic Flows.

Top Denied Traffic Source Report	List of the top denied Traffic Flow Sources over the selected time period, by Source/Protocol. Drilldown on each Source/Protocol combination to view the details of the denied Traffic Flows.
Top Traffic Destination Report	List of the top Traffic Flow Destinations over the selected time period, by Destination/Protocol and Status. Drilldown on each Destination /Protocol/Status combination to view the details of the Traffic Flows.
Top Allowed Traffic Destination Report	List of the top allowed Traffic Flow Destinations over the selected time period, by Destination /Protocol. Drilldown on each Destination /Protocol combination to view the details of the allowed Traffic Flows.
Top Denied Traffic Destination Report	List of the top denied Traffic Flow Destinations over the selected time period, by Destination /Protocol. Drilldown on each Destination /Protocol combination to view the details of the denied Traffic Flows.
Top Protocol Used by Traffic Report	List of the Traffic Flow Classifications showing the top Protocol used over the selected time period, by total hits. Drilldown on each Classification to view more detailed reports showing all Protocols used. Drilldown further on each Classification/Protocol/Status combination to view the details of the Traffic Flows.
Top Allowed Traffic Protocol Report	List of the top allowed Traffic Flow Protocols used over the selected time period, by total hits. Drilldown on each Protocol to view the details of the allowed Traffic Flows.
Top Denied Traffic protocol Report	List of the top denied Traffic Flow Protocols used over the selected time period, by total hits. Drilldown on each Protocol to view the details of the denied Traffic Flows.
Top Bandwidth User Report	List of the top Traffic Flow Sources over the selected time period, by total Bandwidth Usage. Drilldown on each Source to see the details of the Traffic Flows.
Top Traffic Destination Port Report	List of the traffic destination port by port number over the selected time period, by total hits. Drilldown on each destination port to see the details of the traffic flows.
Top Inbound Traffic Destination Port Report	List of the inbound traffic by port number over the selected time period, by total hits.

	Drilldown on each destination port to see the details of the traffic flows.
Top Outbound Traffic Source Port Report	List of the outbound traffic by port number over the selected time period, by total hits. Drilldown on each source port to see the details of the traffic flows.
Top Outbound Traffic Destination Port Report	List of the outbound traffic by port number over the selected time period, by total hits. Drilldown on each destination port to see the details of the traffic flows.
Top Inbound Traffic Report	List of the inbound traffic flow by destination over the selected time period, by total Hits. Drilldown on each destination to see the details of the traffic flows.
Top Outbound Traffic Report	List of the outbound traffic flow by sources over the selected time period, by total hits. Drilldown on each Source to see the details of the traffic flows.
Top Inbound Bandwidth Usage Report	List of the inbound traffic flow by destination over the selected time period, by total bandwidth usage. Drilldown on each destination to see the details of the traffic flows.
Top Outbound Bandwidth Usage Report	List of the outbound traffic flow by sources over the selected time period, by total bandwidth usage. Drilldown on each source to see the details of the traffic flows.
Top Inbound Traffic Protocol Report	List of the inbound traffic by port number over the selected time period, by total hits. Drilldown on each destination port to see the details of the traffic flows.
Top Outbound Traffic Protocol Report	List of the outbound traffic by port number over the selected time period, by total hits. Drilldown on each source port to see the details of the traffic flows.
Category: ANTISPAM	**Description**
Email Usage by Status Report	Summary of all emails over the selected time period, by Status and Number of Hits. Drilldown on each Status to view the details of the emails.
Summary of Email Usage by Flow Classification Report	Summary of all emails over the selected time period, by Flow Classification and Number of Hits. Drilldown on each Flow Classification to view the details of the emails.
Top Sender Report	List of the top email senders over the selected time period, by Number of Hits.

	Drilldown on each sender to view the details of the emails sent.
Top Sender by Status Report	List of the Statuses showing the top email sender for each Status over the selected time period, by Number of Hits. Drilldown on each Status to view more detailed reports showing all email senders. Drilldown further on each email sender to view the details of the emails sent.
Top Recipient Report	List of the top email recipients over the selected time period, by Number of Hits. Drilldown on each recipient to view the details of the emails received.
Top Recipient by Status Report	List of the Statuses showing the top email recipient for each Status over the selected time period, by Number of Hits. Drilldown on each Status to view more detailed reports showing all email recipients. Drilldown further on each email recipient to view the details of the emails received.
Top Detected Spam Sender Report	List of the top detected spam email senders over the selected time period, by number of hits. Drilldown on each sender to view the details of the emails sent.
Top Blocked Spam Sender Report	List of the top blocked spam email senders over the selected time period, by number of hits. Drilldown on each sender to view the details of the emails sent.
Top Sender by Domain Report	List of the top email sender domains over the selected time period, by number of hits. Drilldown on each domain to view the details of the emails sent.
Top Recipient by Domain Report	List of the top email recipient domains over the selected time period, by number of hits. Drilldown on each domain to view the details of the emails received.
Top Detected Spam Sender by Domain Report	List of the top detected spam email sender domains over the selected time period, by number of hits. Drilldown on each sender domain to view the details of the spams sent.
Top Blocked Spam Sender by Domain Report	List of the top blocked spam email sender domains over the selected time period, by number of hits. Drilldown on each sender domain to view the details of the spams sent.
Category: WEB ACTIVITY	**Description**
Top Visited Website Report	List of the top URLs visited over the selected time period, by the Number of Hits. Total Bytes Sent/Received also shown for each URL.

	Drilldown on each URL to see the details of the visits.
Top Blocked Website Report	List of the top URLs blocked over the selected time period, by the Number of Hits. Drilldown on each URL to see the details of the attempts.
Top Web User Report	List of the top Web Users over the selected time period, by the Number of Hits. Total Bytes Sent/Received also shown for each User. Drilldown on each User to see the details of the visits/attempts.
Top Blocked Web Visitor Report	List of the top blocked Web Users over the selected time period, by the Number of Hits. Drilldown on each User to see the details of the attempts.
Top Allowed Web Visitor Report	List of the top allowed Web Users over the selected time period, by the Number of Hits. Total Bytes Sent/Received also shown for each User. Drilldown on each User to see the details of the visits.
Hourly Web Filter Statistic Report	Total Web Filter Hits per Hour of Day over the selected time period, by Status. Drilldown on each Hour/Status combination to view the details of the Web Filter Hits.
Hourly Bandwidth Usage Statistic Report	Total Bandwidth Usage per Hour of Day over the selected time period. Drilldown on each Hour to view the details of the Web Filter Hits.
Daily Web Filter Statistic Report	Total Web Filter Hits per Day over the selected time period, by Status. Drilldown on each Day/Status combination to view the details of the Web Filter Hits.
Daily Bandwidth Usage Statistic Report	Total Bandwidth Usage per Day over the selected time period. Drilldown on each Day to view the details of the Web Filter Hits.
Top Blocked Categories Report	List of the top blocked Categories over the selected time period, by Number of Hits. Drilldown on each Category to view the details of the attempts.
Top Allowed Categories Report	List of the top allowed Categories over the selected time period, by Number of Hits. Drilldown on each Category to view the details of the visits.
Top Website by Bandwidth Usage Report	List of the top urls visited over the selected time period, by total bandwidth usage. Total bytes sent/received also shown for each url. Drilldown on each url to see the details of the visits.
Top Categories by Bandwidth Usage Report	List of the top categories over the selected time period, by total bandwidth usage. Total bytes sent/received also shown for each category.

	Drilldown on each category to see the details of the visits.
Top Web User by Bandwidth Usage Report	List of the top web users over the selected time period, by total bandwidth usage. Total bytes sent/received also shown for each user. Drilldown on each user to see the details of the visits.
Category: VPN	**Description**
Summary of VPN Unique client Activity Report by Selected Date	Summary of VPN Activity per Day over the selected time period. Drilldown on each Day to view the details of the VPN Activities.
Weekly Total Unique Client IP Report	Summary of VPN Activity per Weekday over the selected time period. Drilldown on each Weekday to view the details of the VPN Activities.
Hourly Unique Client Login Activity Report	Summary of VPN Activity per Hour of Day over the selected time period. Drilldown on each Hour to view the details of the VPN Activities.
Top VPN User Access Report	List of the top VPN Users over the selected time period, by Number of Unique Client IPs. Drilldown on each User to see the details of the VPN Activities.
Top URL Access Report	List of the top URLs accessed over the selected time period, by Number of Access. Drilldown on each URL to see the details of the VPN Activities.
Top VPN Protocol Report	List of the top VPN Protocols used over the selected time period, by Number of Access. Drilldown on each Protocol to see the details of the VPN Activities.
Top Used Services Report	List of the top Destination Ports used over the selected time period, by Number of Access. Drilldown on each Destination Port to see the details of the VPN Activities.
Top Bandwidth Usage Report	List of the top VPN Users/Usage Types over the selected time period, by total Bandwidth Usage. Drilldown on each User/Usage Type combination to see the details of the VPN Activities.
Top Bandwidth Usage by Usage Type Report	List of the top VPN Usage Types over the selected time period, by total Bandwidth Usage. Drilldown on each Usage Type to see the details of the VPN Activities.
Category: WINDOWS	Description
Top Failed Logon Report	List of the logon failure user over the selected time period, by user name.

	Drilldown on each user combination to view the details of the logon.
Top Failed Logon Message Report	List of the top logon failure message over the selected time period, by user name. Drilldown on each message/user combination to view the details of the logon failure.
Top Password Changed Report	List of the top password changes account over the selected time period, by user name. Drilldown on each user name combination to view the details of the changes to the account.
Hourly Logon Report	Total logon hits per hour of day over the selected time period. Drilldown on each hour combination to view the details of the logon.
Hourly Logout Report	Total logout hits per hour of day over the selected time period. Drilldown on each hour combination to view the details of the logout.
Summary of Windows Event Report	Summary of all event log over the selected time period, by severity and number of hits. Drilldown on each severity to view the type of the events. Drilldown further on each event types to view the details of the events.
Top Logon Report	List of the successfully logon user over the selected time period, by user name. Drilldown on each user combination to view the details of the logon.
Top Logout Report	List of the successful logout logs over the selected time period, by user name. Drilldown on each user combination to view the details of the logout.
New User Account Report	Total hits of new user account created per day of month over the selected time period. Drilldown on each day of month to view the details of the new account.
Top Account Lockout Report	List of the top locked out account over the selected time period, by user name. Drilldown on each user name combination to view the details of the locked out account.
Top Account Changed Report	List of the top accounts changed over the selected time period, by user name. Drilldown on each user name combination to view the details of the changes to the account.
User Account by Status Report	List of the user accounts over the selected period, by status Drilldown on each status combination to view the details of the account.
Top Process by Event Severity	List of the top process severity for a specific host over the selected time period,

Report	by hostname and process severity. Drilldown on each hostname-severity combination to view the details of the events.
Top Object Access by User Report	List of the top object accessed for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the objects.
Top Object Deletion by User Report	List of the top object deleted for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the deletion.
Top Registry Access by User Report	List of the top registry access for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the registry access.
Category: PERFORMANCE & UTILIZATION	Description
Top SNMP Error Report	List of the top SNMP errors by selected device and time period. Drilldown on each error to view its details.
Top CPU Usage Report	List of the top CPU usage by selected device and time period. Drilldown on each CPU ID to view its hourly usage. Drilldown on total usage to view CPU usage at certain point of time.
Top Disk Usage Report	List of the top disk usage by selected device and time period. Drilldown on each disk label to view its hourly usage. Drilldown on total usage to view disk usage at certain point of time.
Top Memory Usage Report	List of the top memory usage by selected device and time period. Drilldown on each interface to view its hourly usage. Drilldown on total usage to view memory usage at certain point of time.
Top Bandwidth Usage Report	List of the top bandwidth usage by selected device and time period. Drilldown on each device to view its hourly usage. Drilldown on total bandwidth to view bandwidth usage at certain point of time.
Top Interfaces Bandwidth Usage Report	List of the top interface bandwidth usage by selected device and time period.

	Drilldown on each interface to view its hourly bandwidth usage. Drilldown on total bandwidth to view bandwidth usage at certain point of time.

7.3 - List of Reports by Compliance

PCI DSS Compliance

Compliance: PCI DSS	Description
Top Attackers Report	List of the top Attackers over the selected time period, by Source/Protocol. Drilldown on each Source/Protocol combination to view the details of the Attacks.
Top Targets Report	List of the top Targets over the selected time period, by Destination/Protocol. Drilldown on each Destination/Protocol combination to view the details of the Attacks.
Top Protocol Used by Attack Report	List of the top Protocols used by Attacks over the selected time period. Drilldown on each Protocol to view the details of the Attacks.
Top Attacks Report	List of the top Attacks over the selected time period, by Attack Type. Drilldown on each Attack Type to view the details of the Attacks.
Top Internal Attackers Report	List of the top Internal Attackers over the selected time period, by Source. Drilldown on each Source to view the details of the Attacks.
Top External Attackers Report	List of the top External Attackers over the selected time period, by Source. Drilldown on each Source to view the details of the Attacks.
Top Internal Targets Report	List of the top Internal Targets over the selected time period, by Destination. Drilldown on each Destination to view the details of the Attacks.
Top External Targets Report	List of the top External Targets over the selected time period, by Destination. Drilldown on each Destination to view the details of the Attacks.
Top Attack Destination Port Report	List of the top Attacks destination port over the selected time period, by Attack Type. Drilldown on each Attack Type to view the details of the Attacks.
Top Generator Report	List of the top Event logs over the selected time period, by Source and Severity. Drilldown on each Source/Severity combination to view the details of the Events.
Top Emergency Event Report	List of the top Emergency Event logs over the selected time period, by Source. Drilldown on each Source combination to view the details of the Events.
Top Alert Event Report	List of the top Alert Event logs over the selected time period, by Source.

	Drilldown on each Source combination to view the details of the Events.
Top Critical Event Report	List of the top Critical Event logs over the selected time period, by Source. Drilldown on each Source combination to view the details of the Events.
Top Warning Event Report	List of the top Warning Event logs over the selected time period, by Source. Drilldown on each Source combination to view the details of the Events.
Top Virus Sources Report	List of the top Sources of Virus intrusions over the selected time period. Drilldown on each Source to view the details of the Virus messages.
Top Virus Destination Report	List of the top Destinations of Virus intrusions over the selected time period. Drilldown on each Destination to view the details of the Virus messages.
Top Protocol Used by Virus Report	List of the top Protocols used in Virus intrusions over the selected time period. Drilldown on each Protocol to view the details of the Virus messages.
Top Virus Report	List of the top Virus intrusions over the selected time period, by Virus Name. Drilldown on each Virus Name to view the details of the Virus messages.
Top Traffic Source Report	List of the top Traffic Flow Sources over the selected time period, by Source/Protocol and Status. Drilldown on each Source/Protocol/Status combination to view the details of the Traffic Flows.
Top Allowed Traffic Source Report	List of the top allowed Traffic Flow Sources over the selected time period, by Source/Protocol. Drilldown on each Source/Protocol combination to view the details of the allowed Traffic Flows.
Top Denied Traffic Source Report	List of the top denied Traffic Flow Sources over the selected time period, by Source/Protocol. Drilldown on each Source/Protocol combination to view the details of the denied Traffic Flows.
Top Traffic Destination Report	List of the top Traffic Flow Destinations over the selected time period, by Destination/Protocol and Status. Drilldown on each Destination /Protocol/Status combination to view the details of the Traffic Flows.
Top Allowed Traffic Destination Report	List of the top allowed Traffic Flow Destinations over the selected time period, by Destination /Protocol. Drilldown on each Destination /Protocol combination to view the details of the allowed Traffic Flows.

Top Denied Traffic Destination Report	List of the top denied Traffic Flow Destinations over the selected time period, by Destination /Protocol. Drilldown on each Destination /Protocol combination to view the details of the denied Traffic Flows.
Top Bandwidth User Report	List of the top Traffic Flow Sources over the selected time period, by total Bandwidth Usage. Drilldown on each Source to see the details of the Traffic Flows.
Top Traffic Destination Port Report	List of the inbound traffic by port number over the selected time period, by total hits Drilldown on each destination port to see the details of the traffic flows.
Top Inbound Traffic Destination Port Report	List of the Inbound Traffic by Port Number over the selected time period, by total Hits. Drilldown on each Destination Port to see the details of the Traffic Flows.
Top Outbound Traffic Source Port Report	List of the outbound traffic by port number over the selected time period, by total hits. Drilldown on each source port to see the details of the traffic flows.
Top Outbound Traffic Destination Port Report	List of the outbound traffic by port number over the selected time period, by total hits. Drilldown on each destination port to see the details of the traffic flows.
Top Inbound Traffic Report	List of the inbound traffic flow by destination over the selected time period, by total Hits. Drilldown on each destination to see the details of the traffic flows.
Top Outbound Traffic Report	List of the outbound traffic flow by sources over the selected time period, by total hits. Drilldown on each Source to see the details of the traffic flows.
Top Inbound Bandwidth Usage Report	List of the inbound traffic flow by destination over the selected time period, by total bandwidth usage. Drilldown on each destination to see the details of the traffic flows.
Top Outbound Bandwidth Usage Report	List of the Outbound Traffic Flow by Sources over the selected time period, by total Bandwidth Usage. Drilldown on each source to see the details of the Traffic Flows.
Top Inbound Traffic Protocol Report	List of the Inbound Traffic by Port Number over the selected time period, by total Hits. Drilldown on each Destination Port to see the details of the Traffic Flows.
Top Outbound Traffic Protocol	List of the Outbound Traffic by Port Number over the selected time period, by

Report	total Hits. Drilldown on each Source Port to see the details of the Traffic Flows.
Top Sender Report	List of the top email senders over the selected time period, by Number of Hits. Drilldown on each sender to view the details of the emails sent.
Top Sender by Status Report	List of the Statuses showing the top email sender for each Status over the selected time period, by Number of Hits. Drilldown on each Status to view more detailed reports showing all email senders. Drilldown further on each email sender to view the details of the emails sent.
Top Recipient Report	List of the top email recipients over the selected time period, by Number of Hits. Drilldown on each recipient to view the details of the emails received.
Top Recipient by Status Report	List of the Statuses showing the top email recipient for each Status over the selected time period, by Number of Hits. Drilldown on each Status to view more detailed reports showing all email recipients. Drilldown further on each email recipient to view the details of the emails received.
Top Detected Spam Sender Report	List of the top detected spam email senders over the selected time period, by Number of Hits. Drilldown on each sender to view the details of the emails sent.
Top Blocked Spam Sender Report	List of the top blocked spam email senders over the selected time period, by Number of Hits. Drilldown on each sender to view the details of the emails sent.
Top Visited Website Report	List of the top URLs visited over the selected time period, by the Number of Hits. Total Bytes Sent/Received also shown for each URL. Drilldown on each URL to see the details of the visits.
Top Blocked Website Report	List of the top URLs blocked over the selected time period, by the Number of Hits. Drilldown on each URL to see the details of the attempts.
Top Web User Report	List of the top Web Users over the selected time period, by the Number of Hits. Total Bytes Sent/Received also shown for each User. Drilldown on each User to see the details of the visits/attempts.
Top Blocked Web Visitor Report	List of the top blocked Web Users over the selected time period, by the Number of Hits. Drilldown on each User to see the details of the attempts.
Top Allowed Web Visitor	List of the top allowed Web Users over the selected time period, by the Number

Report	of Hits. Total Bytes Sent/Received also shown for each User. Drilldown on each User to see the details of the visits.
Hourly Web Filter Statistic Report	Total Web Filter Hits per Hour of Day over the selected time period, by Status. Drilldown on each Hour/Status combination to view the details of the Web Filter Hits.
Hourly Bandwidth Usage Statistic Report	Total Bandwidth Usage per Hour of Day over the selected time period. Drilldown on each Hour to view the details of the Web Filter Hits.
Daily Web Filter Statistic Report	Total Web Filter Hits per Day over the selected time period, by Status. Drilldown on each Day/Status combination to view the details of the Web Filter Hits.
Daily Bandwidth Usage Statistic Report	Total Bandwidth Usage per Day over the selected time period. Drilldown on each Day to view the details of the Web Filter Hits.
Top Website by Bandwidth Usage Report	List of the top URLs visited over the selected time period, by total Bandwidth Usage. Total Bytes Sent/Received also shown for each URL. Drilldown on each URL to see the details of the visits.
Top Web User by Bandwidth Usage Report	List of the top Web Users over the selected time period, by total Bandwidth Usage. Total Bytes Sent/Received also shown for each User. Drilldown on each User to see the details of the visits.
Top Bandwidth Usage Report	List of the top VPN Users/Usage Types over the selected time period, by total Bandwidth Usage. Drilldown on each User/Usage Type combination to see the details of the VPN Activities.
Top Bandwidth Usage by Usage Type Report	List of the top VPN Usage Types over the selected time period, by total Bandwidth Usage. Drilldown on each Usage Type to see the details of the VPN Activities.
Top Failed Logon Report	List of the Logon Failure user over the selected time period, by User Name. Drilldown on each User combination to view the details of the logon.
Top Failed Logon Message Report	List of the top Logon Failure Message over the selected time period, by user name. Drilldown on each Message/User combination to view the details of the Logon failure.
Top Password Changed Report	List of the top Password changes account over the selected time period, by user name. Drilldown on each User name combination to view the details of the changes to

	the account.
Hourly Logon Report	Total Logon Hits per Hour of Day over the selected time period. Drilldown on each Hour combination to view the details of the logon.
Hourly Logout Report	Total logout Hits per Hour of Day over the selected time period. Drilldown on each Hour combination to view the details of the logout.
Summary of Windows Event Report	Summary of all event log over the selected time period, by Severity and Number of Hits. Drilldown on each Severity to view the Type of the Events. Drilldown further on each Event Types to view the details of the Events.
Top Logon Report	List of the successfully logon user over the selected time period, by user name. Drilldown on each user combination to view the details of the logon.
Top Logout Report	List of the successful logout logs over the selected time period, by user name. Drilldown on each user combination to view the details of the logout.
New User Account Report	Total hits of new user account created per day of month over the selected time period. Drilldown on each day of month to view the details of the new account.
Top Account Lockout Report	List of the top locked out account over the selected time period, by user name. Drilldown on each user name combination to view the details of the locked out account.
Top Account Changed Report	List of the top accounts changed over the selected time period, by user name. Drilldown on each user name combination to view the details of the changes to the account.
User Account by Status Report	List of the user accounts over the selected period, by status. Drilldown on each status combination to view the details of the account.
Top Process by Event Severity Report	List of the top process severity for a specific host over the selected time period, by hostname and process severity. Drilldown on each hostname-severity combination to view the details of the events
Top Object Access by User Report	List of the top object accessed for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the objects.
Top Object Deletion by User	List of the top object deleted for a specific host by a user the selected time

Report	period, by hostname and username. Drilldown on each hostname-username combination to view the details of the deletion.
Top Registry Access by User Report	List of the top registry access for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the registry access.

SOX (COBIT) Compliance

Compliance: SOX (COBIT)	Description
Top Attackers Report	List of the top Attackers over the selected time period, by Source/Protocol. Drilldown on each Source/Protocol combination to view the details of the Attacks.
Top Targets Report	List of the top Targets over the selected time period, by Destination/Protocol. Drilldown on each Destination/Protocol combination to view the details of the Attacks.
Top Protocol Used by Attack Report	List of the top Protocols used by Attacks over the selected time period. Drilldown on each Protocol to view the details of the Attacks.
Top Attacks Report	List of the top Attacks over the selected time period, by Attack Type. Drilldown on each Attack Type to view the details of the Attacks.
Top Internal Attackers Report	List of the top Internal Attackers over the selected time period, by Source. Drilldown on each Source to view the details of the Attacks.
Top External Attackers Report	List of the top External Attackers over the selected time period, by Source. Drilldown on each Source to view the details of the Attacks.
Top Internal Targets Report	List of the top Internal Targets over the selected time period, by Destination. Drilldown on each Destination to view the details of the Attacks.
Top Attack Destination Port Report	List of the top Attacks destination port over the selected time period, by Attack Type. Drilldown on each Attack Type to view the details of the Attacks.
Top Generator Report	List of the top Event logs over the selected time period, by Source and Severity. Drilldown on each Source/Severity combination to view the details of the Events.
Top Emergency Event Report	List of the top Emergency Event logs over the selected time period, by Source. Drilldown on each Source combination to view the details of the Events.
Top Alert Event Report	List of the top Alert Event logs over the selected time period, by Source. Drilldown on each Source combination to view the details of the Events.
Top Critical Event Report	List of the top Critical Event logs over the selected time period, by Source. Drilldown on each Source combination to view the details of the Events.
Top Warning Event Report	List of the top Warning Event logs over the selected time period, by Source.

	Drilldown on each Source combination to view the details of the Events.
Top Virus Sources Report	List of the top Sources of Virus intrusions over the selected time period. Drilldown on each Source to view the details of the Virus messages.
Top Virus Destination Report	List of the top Destinations of Virus intrusions over the selected time period. Drilldown on each Destination to view the details of the Virus messages.
Top Protocol Used by Virus Report	List of the top Protocols used in Virus intrusions over the selected time period. Drilldown on each Protocol to view the details of the Virus messages.
Top Virus Report	List of the top Virus intrusions over the selected time period, by Virus Name. Drilldown on each Virus Name to view the details of the Virus messages.
Top Traffic Source Report	List of the top Traffic Flow Sources over the selected time period, by Source/Protocol and Status. Drilldown on each Source/Protocol/Status combination to view the details of the Traffic Flows.
Top Traffic Destination Report	List of the top Traffic Flow Destinations over the selected time period, by Destination/Protocol and Status. Drilldown on each Destination /Protocol/Status combination to view the details of the Traffic Flows.
Top Protocol Used by Traffic Report	List of the Traffic Flow Classifications showing the top Protocol used over the selected time period, by total hits. Drilldown on each Classification to view more detailed reports showing all Protocols used. Drilldown further on each Classification/Protocol/Status combination to view the details of the Traffic Flows.
Top Bandwidth User Report	List of the top Traffic Flow Sources over the selected time period, by total Bandwidth Usage. Drilldown on each Source to see the details of the Traffic Flows.
Top Traffic Destination Port Report	List of the Traffic Destination Port by Port Number over the selected time period, by total Hits. Drilldown on each Destination Port to see the details of the Traffic Flows.
Top Inbound Traffic Destination Port Report	List of the inbound traffic by port number over the selected time period, by total hits. Drilldown on each destination port to see the details of the traffic flows.
Top Outbound Traffic Source Port Report	List of the outbound traffic by port number over the selected time period, by total hits. Drilldown on each source port to see the details of the traffic flows.
Top Outbound Traffic	List of the outbound traffic by port number over the selected time period, by total

Destination Port Report	hits. Drilldown on each destination port to see the details of the traffic flows.
Top Inbound Traffic Report	List of the inbound traffic flow by destination over the selected time period, by total Hits. Drilldown on each destination to see the details of the traffic flows.
Top Outbound Traffic Report	List of the outbound traffic flow by sources over the selected time period, by total hits. Drilldown on each Source to see the details of the traffic flows.
Top Inbound Bandwidth Usage Report	List of the inbound traffic flow by destination over the selected time period, by total bandwidth usage. Drilldown on each destination to see the details of the traffic flows.
Top Outbound Bandwidth Usage Report	List of the outbound traffic flow by sources over the selected time period, by total bandwidth usage. Drilldown on each source to see the details of the traffic flows.
Summary of Email Usage by Flow Classification Report	Summary of all emails over the selected time period, by flow classification and number of hits. Drilldown on each flow classification to view the details of the emails.
Top Sender Report	List of the top email senders over the selected time period, by Number of Hits. Drilldown on each sender to view the details of the emails sent.
Top Recipient Report	List of the top email recipients over the selected time period, by Number of Hits. Drilldown on each recipient to view the details of the emails received.
Top Web User Report	List of the top Web Users over the selected time period, by the Number of Hits. Total Bytes Sent/Received also shown for each User. Drilldown on each User to see the details of the visits/attempts.
Hourly Bandwidth Usage Statistic Report	Total Bandwidth Usage per Hour of Day over the selected time period. Drilldown on each Hour to view the details of the Web Filter Hits.
Daily Bandwidth Usage Statistic Report	Total Bandwidth Usage per Day over the selected time period. Drilldown on each Day to view the details of the Web Filter Hits.
Top Web User by Bandwidth Usage Report	List of the top Web Users over the selected time period, by total Bandwidth Usage. Total Bytes Sent/Received also shown for each User. Drilldown on each User to see the details of the visits.
Top Failed Logon Report	List of the Logon Failure user over the selected time period, by User Name.

	Drilldown on each User combination to view the details of the logon.
Top Failed Logon Message Report	List of the top Logon Failure Message over the selected time period, by user name. Drilldown on each Message/User combination to view the details of the Logon failure.
Top Password Changed Report	List of the top Password changes account over the selected time period, by user name. Drilldown on each User name combination to view the details of the changes to the account.
Hourly Logon Report	Total Logon Hits per Hour of Day over the selected time period. Drilldown on each Hour combination to view the details of the logon.
Hourly Logout Report	Total logout Hits per Hour of Day over the selected time period. Drilldown on each Hour combination to view the details of the logout.
Summary of Windows Event Report	Summary of all event log over the selected time period, by Severity and Number of Hits. Drilldown on each Severity to view the Type of the Events. Drilldown further on each Event Types to view the details of the Events.
Top Logon Report	List of the successfully logon user over the selected time period, by user name. Drilldown on each User combination to view the details of the Logon.
Top Logout Report	List of the successful logout logs over the selected time period, by user name. Drilldown on each User combination to view the details of the Logout.
New User Account Report	Total Hits of New User Account created per day of month over the selected time period. Drilldown on each Day of Month to view the details of the new account.
Top Account Lockout Report	List of the top locked out account over the selected time period, by user name. Drilldown on each user name combination to view the details of the locked out account
Top Account Changed Report	List of the top accounts changed over the selected time period, by user name. Drilldown on each user name combination to view the details of the changes to the account
User Account by Status Report	List of the User accounts over the selected period, by Status. Drilldown on each Status combination to view the details of the account
Top Process by Event Severity	List of the top process severity for a specific host over the selected time period,

Report	by hostname and process severity. Drilldown on each hostname-severity combination to view the details of the events
Top Object Access by User Report	List of the top object accessed for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the objects.
Top Object Deletion by User Report	List of the top object deleted for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the deletion.
Top Registry Access by User Report	List of the top registry access for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the registry access.

HIPAA Compliance

Compliance: HIPAA	Description
Top Attackers Report	List of the top Attackers over the selected time period, by Source/Protocol. Drilldown on each Source/Protocol combination to view the details of the Attacks.
Top Targets Report	List of the top Targets over the selected time period, by Destination/Protocol. Drilldown on each Destination/Protocol combination to view the details of the Attacks.
Top Protocol Used by Attack Report	List of the top Protocols used by Attacks over the selected time period. Drilldown on each Protocol to view the details of the Attacks.
Top Attacks Report	List of the top Attacks over the selected time period, by Attack Type. Drilldown on each Attack Type to view the details of the Attacks.
Top Internal Attackers Report	List of the top Internal Attackers over the selected time period, by Source. Drilldown on each Source to view the details of the Attacks.
Top External Attackers Report	List of the top External Attackers over the selected time period, by Source. Drilldown on each Source to view the details of the Attacks.
Top Internal Targets Report	List of the top Internal Targets over the selected time period, by Destination. Drilldown on each Destination to view the details of the Attacks.
Top External Targets Report	List of the top External Targets over the selected time period, by Destination. Drilldown on each Destination to view the details of the Attacks.
Top Attack Destination Port Report	List of the top Attacks destination port over the selected time period, by Attack Type. Drilldown on each Attack Type to view the details of the Attacks.
Top Emergency Event Report	List of the top Emergency Event logs over the selected time period, by Source. Drilldown on each Source combination to view the details of the Events.
Top Alert Event Report	List of the top Alert Event logs over the selected time period, by Source. Drilldown on each Source combination to view the details of the Events.
Top Critical Event Report	List of the top Critical Event logs over the selected time period, by Source. Drilldown on each Source combination to view the details of the Events.
Top Warning Event Report	List of the top Warning Event logs over the selected time period, by Source.

	Drilldown on each Source combination to view the details of the Events.
Top Virus Sources Report	List of the top Sources of Virus intrusions over the selected time period. Drilldown on each Source to view the details of the Virus messages.
Top Virus Destination Report	List of the top Destinations of Virus intrusions over the selected time period. Drilldown on each Destination to view the details of the Virus messages.
Top Protocol Used by Virus Report	List of the top Protocols used in Virus intrusions over the selected time period. Drilldown on each Protocol to view the details of the Virus messages.
Top Virus Report	List of the top Virus intrusions over the selected time period, by Virus Name. Drilldown on each Virus Name to view the details of the Virus messages.
Hourly Viruses Blocked Report	List of the top Virus intrusions over the selected time period, by Virus Name. Drilldown on each Virus Name to view the details of the Virus messages.
Daily Viruses Blocked Report	List of the top Virus intrusions over the selected time period, by Virus Name. Drilldown on each Virus Name to view the details of the Virus messages.
Top Blocked Viruses Report	List of the top Virus intrusions over the selected time period, by Virus Name. Drilldown on each Virus Name to view the details of the Virus messages.
Top Traffic Source Report	List of the top Traffic Flow Sources over the selected time period, by Source/Protocol and Status. Drilldown on each Source/Protocol/Status combination to view the details of the Traffic Flows.
Top Allowed Traffic Source Report	List of the top allowed Traffic Flow Sources over the selected time period, by Source/Protocol. Drilldown on each Source/Protocol combination to view the details of the allowed Traffic Flows.
Top Denied Traffic Source Report	List of the top denied Traffic Flow Sources over the selected time period, by Source/Protocol. Drilldown on each Source/Protocol combination to view the details of the denied Traffic Flows.
Top Traffic Destination Report	List of the top Traffic Flow Destinations over the selected time period, by Destination/Protocol and Status. Drilldown on each Destination /Protocol/Status combination to view the details of the Traffic Flows.
Top Allowed Traffic Destination Report	List of the top allowed Traffic Flow Destinations over the selected time period, by Destination /Protocol.

	Drilldown on each Destination /Protocol combination to view the details of the allowed Traffic Flows.
Top Denied Traffic Destination Report	List of the top denied Traffic Flow Destinations over the selected time period, by Destination /Protocol. Drilldown on each Destination /Protocol combination to view the details of the denied Traffic Flows.
Top Protocol Used by Traffic Report	List of the Traffic Flow Classifications showing the top Protocol used over the selected time period, by total hits. Drilldown on each Classification to view more detailed reports showing all Protocols used. Drilldown further on each Classification/Protocol/Status combination to view the details of the Traffic Flows.
Top Bandwidth User Report	List of the top Traffic Flow Sources over the selected time period, by total Bandwidth Usage. Drilldown on each Source to see the details of the Traffic Flows.
Top Traffic Destination Port Report	List of the Traffic Destination Port by Port Number over the selected time period, by total Hits. Drilldown on each Destination Port to see the details of the Traffic Flows.
Top Inbound Bandwidth Usage Report	List of the Inbound Traffic Flow by Destination over the selected time period, by total Bandwidth Usage. Drilldown on each Destination to see the details of the Traffic Flows.
Top Outbound Bandwidth Usage Report	List of the Outbound Traffic Flow by Sources over the selected time period, by total Bandwidth Usage. Drilldown on each source to see the details of the Traffic Flows.
Top Inbound Traffic Protocol Report	List of the Inbound Traffic by Port Number over the selected time period, by total Hits. Drilldown on each Destination Port to see the details of the Traffic Flows.
Top Outbound Traffic Protocol Report	List of the Outbound Traffic by Port Number over the selected time period, by total Hits. Drilldown on each Source Port to see the details of the Traffic Flows.
Top Sender Report	List of the top email senders over the selected time period, by Number of Hits. Drilldown on each sender to view the details of the emails sent.
Top Recipient Report	List of the top email recipients over the selected time period, by Number of Hits. Drilldown on each recipient to view the details of the emails received.
Top Detected Spam Sender Report	List of the top detected spam email senders over the selected time period, by Number of Hits.

	Drilldown on each sender to view the details of the emails sent.
Top Blocked Spam Sender Report	List of the top blocked spam email senders over the selected time period, by Number of Hits. Drilldown on each sender to view the details of the emails sent.
Top Web User Report	List of the top Web Users over the selected time period, by the Number of Hits. Total Bytes Sent/Received also shown for each User. Drilldown on each User to see the details of the visits/attempts.
Top Blocked Web Visitor Report	List of the top blocked Web Users over the selected time period, by the Number of Hits. Drilldown on each User to see the details of the attempts.
Hourly Web Filter Statistic Report	Total Web Filter Hits per Hour of Day over the selected time period, by Status. Drilldown on each Hour/Status combination to view the details of the Web Filter Hits.
Hourly Bandwidth Usage Statistic Report	Total Bandwidth Usage per Hour of Day over the selected time period. Drilldown on each Hour to view the details of the Web Filter Hits.
Daily Web Filter Statistic Report	Total Web Filter Hits per Day over the selected time period, by Status. Drilldown on each Day/Status combination to view the details of the Web Filter Hits.
Daily Bandwidth Usage Statistic Report	Total Bandwidth Usage per Day over the selected time period. Drilldown on each Day to view the details of the Web Filter Hits.
Top Website by Bandwidth Usage Report	List of the top URLs visited over the selected time period, by total Bandwidth Usage. Total Bytes Sent/Received also shown for each URL. Drilldown on each URL to see the details of the visits.
Top Web User by Bandwidth Usage Report	List of the top Web Users over the selected time period, by total Bandwidth Usage. Total Bytes Sent/Received also shown for each User. Drilldown on each User to see the details of the visits.
Top Bandwidth Usage Report	List of the top VPN Users/Usage Types over the selected time period, by total Bandwidth Usage. Drilldown on each User/Usage Type combination to see the details of the VPN Activities.
Top Bandwidth Usage by Usage Type Report	List of the top VPN Usage Types over the selected time period, by total Bandwidth Usage. Drilldown on each Usage Type to see the details of the VPN Activities.

Top Failed Logon Report	List of the Logon Failure user over the selected time period, by User Name. Drilldown on each User combination to view the details of the logon.
Top Failed Logon Message Report	List of the top Logon Failure Message over the selected time period, by user name. Drilldown on each Message/User combination to view the details of the Logon failure.
Top Password Changed Report	List of the top Password changes account over the selected time period, by user name. Drilldown on each User name combination to view the details of the changes to the account.
Hourly Logon Report	Total Logon Hits per Hour of Day over the selected time period. Drilldown on each Hour combination to view the details of the logon.
Hourly Logout Report	Total logout Hits per Hour of Day over the selected time period. Drilldown on each Hour combination to view the details of the logout.
Summary of Windows Event Report	Summary of all event log over the selected time period, by Severity and Number of Hits. Drilldown on each Severity to view the Type of the Events. Drilldown further on each Event Types to view the details of the Events.
Top Logon Report	List of the successfully logon user over the selected time period, by user name. Drilldown on each User combination to view the details of the Logon.
Top Logout Report	List of the successful logout logs over the selected time period, by user name. Drilldown on each User combination to view the details of the Logout.
New User Account Report	Total Hits of New User Account created per day of month over the selected time period. Drilldown on each Day of Month to view the details of the new account.
Top Account Lockout Report	List of the top locked out account over the selected time period, by user name. Drilldown on each user name combination to view the details of the locked out account
Top Account Changed Report	List of the top accounts changed over the selected time period, by user name. Drilldown on each user name combination to view the details of the changes to the account
User Account by Status Report	List of the User accounts over the selected period, by Status. Drilldown on each Status combination to view the details of the account

Top Process by Event Severity Report	List of the top process severity for a specific host over the selected time period, by hostname and process severity. Drilldown on each hostname-severity combination to view the details of the events
Top Object Access by User Report	List of the top object accessed for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the objects.
Top Object Deletion by User Report	List of the top object deleted for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the deletion.
Top Registry Access by User Report	List of the top registry access for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the registry access.

ISO 27002 Compliance

Compliance: ISO 27002	Description
Top Attackers Report	List of the top Attackers over the selected time period, by Source/Protocol. Drilldown on each Source/Protocol combination to view the details of the Attacks.
Top Targets Report	List of the top Targets over the selected time period, by Destination/Protocol. Drilldown on each Destination/Protocol combination to view the details of the Attacks.
Top Protocol Used by Attack Report	List of the top Protocols used by Attacks over the selected time period. Drilldown on each Protocol to view the details of the Attacks.
Top Attacks Report	List of the top Attacks over the selected time period, by Attack Type. Drilldown on each Attack Type to view the details of the Attacks.
Top Internal Attackers Report	List of the top Internal Attackers over the selected time period, by Source. Drilldown on each Source to view the details of the Attacks.
Top External Attackers Report	List of the top External Attackers over the selected time period, by Source. Drilldown on each Source to view the details of the Attacks.
Top Internal Targets Report	List of the top Internal Targets over the selected time period, by Destination. Drilldown on each Destination to view the details of the Attacks.
Top Attack Destination Port Report	List of the top Attacks destination port over the selected time period, by Attack Type. Drilldown on each Attack Type to view the details of the Attacks.
Top Generator Report	List of the top Event logs over the selected time period, by Source and Severity. Drilldown on each Source/Severity combination to view the details of the Events.
Top Emergency Event Report	List of the top Emergency Event logs over the selected time period, by Source. Drilldown on each Source combination to view the details of the Events.
Top Alert Event Report	List of the top Alert Event logs over the selected time period, by Source. Drilldown on each Source combination to view the details of the Events.
Top Critical Event Report	List of the top Critical Event logs over the selected time period, by Source. Drilldown on each Source combination to view the details of the Events.
Top Warning Event Report	List of the top Warning Event logs over the selected time period, by Source.

	Drilldown on each Source combination to view the details of the Events.
Top Virus Sources Report	List of the top Sources of Virus intrusions over the selected time period. Drilldown on each Source to view the details of the Virus messages.
Top Protocol Used by Virus Report	List of the top Protocols used in Virus intrusions over the selected time period. Drilldown on each Protocol to view the details of the Virus messages.
Hourly Viruses Blocked Report	List of the top Virus intrusions over the selected time period, by Virus Name. Drilldown on each Virus Name to view the details of the Virus messages.
Daily Viruses Blocked Report	List of the top Virus intrusions over the selected time period, by Virus Name. Drilldown on each Virus Name to view the details of the Virus messages.
Top Traffic Source Report	List of the top Traffic Flow Sources over the selected time period, by Source/Protocol and Status. Drilldown on each Source/Protocol/Status combination to view the details of the Traffic Flows.
Top Protocol Used by Traffic Report	List of the Traffic Flow Classifications showing the top Protocol used over the selected time period, by total hits. Drilldown on each Classification to view more detailed reports showing all Protocols used. Drilldown further on each Classification/Protocol/Status combination to view the details of the Traffic Flows.
Top Bandwidth User Report	List of the top Traffic Flow Sources over the selected time period, by total Bandwidth Usage. Drilldown on each Source to see the details of the Traffic Flows.
Top Traffic Destination Port Report	List of the Traffic Destination Port by Port Number over the selected time period, by total Hits. Drilldown on each Destination Port to see the details of the Traffic Flows.
Top Inbound Traffic Destination Port Report	List of the inbound traffic by port number over the selected time period, by total hits. Drilldown on each destination port to see the details of the traffic flows.
Top Outbound Traffic Source Port Report	List of the outbound traffic by port number over the selected time period, by total hits. Drilldown on each source port to see the details of the traffic flows.
Top Outbound Traffic Destination Port Report	List of the outbound traffic by port number over the selected time period, by total hits.

	Drilldown on each destination port to see the details of the traffic flows.
Top Inbound Traffic Report	List of the Inbound Traffic Flow by Destination over the selected time period, by total Hits. Drilldown on each Destination to see the details of the Traffic Flows.
Top Outbound Traffic Report	List of the Outbound Traffic Flow by Sources over the selected time period, by total Hits. Drilldown on each Source to see the details of the Traffic Flows.
Top Inbound Bandwidth Usage Report	List of the Inbound Traffic Flow by Destination over the selected time period, by total Bandwidth Usage. Drilldown on each Destination to see the details of the Traffic Flows.
Top Outbound Bandwidth Usage Report	List of the Outbound Traffic Flow by Sources over the selected time period, by total Bandwidth Usage. Drilldown on each source to see the details of the Traffic Flows.
Top Inbound Traffic Protocol Report	List of the Inbound Traffic by Port Number over the selected time period, by total Hits. Drilldown on each Destination Port to see the details of the Traffic Flows.
Top Outbound Traffic Protocol Report	List of the Outbound Traffic by Port Number over the selected time period, by total Hits. Drilldown on each Source Port to see the details of the Traffic Flows.
Summary of Email Usage by Flow Classification Report	Summary of all emails over the selected time period, by Flow Classification and Number of Hits. Drilldown on each Flow Classification to view the details of the emails.
Top Sender Report	List of the top email senders over the selected time period, by Number of Hits. Drilldown on each sender to view the details of the emails sent.
Top Recipient Report	List of the top email recipients over the selected time period, by Number of Hits. Drilldown on each recipient to view the details of the emails received.
Top Detected Spam Sender Report	List of the top detected spam email senders over the selected time period, by Number of Hits. Drilldown on each sender to view the details of the emails sent.
Top Blocked Spam Sender Report	List of the top blocked spam email senders over the selected time period, by Number of Hits. Drilldown on each sender to view the details of the emails sent.
Top Visited Website Report	List of the top URLs visited over the selected time period, by the Number of Hits. Total Bytes Sent/Received also shown for each URL.

	Drilldown on each URL to see the details of the visits.
Top Web User Report	List of the top Web Users over the selected time period, by the Number of Hits. Total Bytes Sent/Received also shown for each User. Drilldown on each User to see the details of the visits/attempts.
Top Blocked Web Visitor Report	List of the top blocked Web Users over the selected time period, by the Number of Hits. Drilldown on each User to see the details of the attempts.
Hourly Web Filter Statistic Report	Total Web Filter Hits per Hour of Day over the selected time period, by Status. Drilldown on each Hour/Status combination to view the details of the Web Filter Hits.
Hourly Bandwidth Usage Statistic Report	Total Bandwidth Usage per Hour of Day over the selected time period. Drilldown on each Hour to view the details of the Web Filter Hits.
Daily Web Filter Statistic Report	Total Web Filter Hits per Day over the selected time period, by Status. Drilldown on each Day/Status combination to view the details of the Web Filter Hits.
Daily Bandwidth Usage Statistic Report	Total Bandwidth Usage per Day over the selected time period. Drilldown on each Day to view the details of the Web Filter Hits.
Top Website by Bandwidth Usage Report	List of the top URLs visited over the selected time period, by total Bandwidth Usage. Total Bytes Sent/Received also shown for each URL. Drilldown on each URL to see the details of the visits.
Top Web User by Bandwidth Usage Report	List of the top Web Users over the selected time period, by total Bandwidth Usage. Total Bytes Sent/Received also shown for each User. Drilldown on each User to see the details of the visits.
Top Bandwidth Usage Report	List of the top VPN Users/Usage Types over the selected time period, by total Bandwidth Usage. Drilldown on each User/Usage Type combination to see the details of the VPN Activities.
Top Bandwidth Usage by Usage Type Report	List of the top VPN Usage Types over the selected time period, by total Bandwidth Usage. Drilldown on each Usage Type to see the details of the VPN Activities.
Top Failed Logon Report	List of the Logon Failure user over the selected time period, by User Name. Drilldown on each User combination to view the details of the logon.
Top Failed Logon Message	List of the top Logon Failure Message over the selected time period, by user

Report	name. Drilldown on each Message/User combination to view the details of the Logon failure.
Top Password Changed Report	List of the top Password changes account over the selected time period, by user name. Drilldown on each User name combination to view the details of the changes to the account.
Hourly Logon Report	Total Logon Hits per Hour of Day over the selected time period. Drilldown on each Hour combination to view the details of the logon.
Hourly Logout Report	Total logout Hits per Hour of Day over the selected time period. Drilldown on each Hour combination to view the details of the logout.
Summary of Windows Event Report	Summary of all event log over the selected time period, by Severity and Number of Hits. Drilldown on each Severity to view the Type of the Events. Drilldown further on each Event Types to view the details of the Events.
Top Logon Report	List of the successfully logon user over the selected time period, by user name. Drilldown on each User combination to view the details of the Logon.
Top Logout Report	List of the successful logout logs over the selected time period, by user name. Drilldown on each User combination to view the details of the Logout.
New User Account Report	Total Hits of New User Account created per day of month over the selected time period. Drilldown on each Day of Month to view the details of the new account.
Top Account Lockout Report	List of the top locked out account over the selected time period, by user name. Drilldown on each user name combination to view the details of the locked out account
Top Account Changed Report	List of the top accounts changed over the selected time period, by user name. Drilldown on each user name combination to view the details of the changes to the account
User Account by Status Report	List of the User accounts over the selected period, by Status. Drilldown on each Status combination to view the details of the account
Top Process by Event Severity Report	List of the top process severity for a specific host over the selected time period, by hostname and process severity. Drilldown on each hostname-severity combination to view the details of the events

Top Object Access by User Report	List of the top object accessed for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the objects.
Top Object Deletion by User Report	List of the top object deleted for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the deletion.
Top Registry Access by User Report	List of the top registry access for a specific host by a user the selected time period, by hostname and username. Drilldown on each hostname-username combination to view the details of the registry access.

7.4 - Automated

Automated method generates reports based on selected categories in an automated way with option to send to user's email. Report can be output into two format which is PDF and CSV format.

The main interface from Automated Report is showing the summary of the created automated report. Summary of the report will display the task and status of each report that is created. Next Run Time and Last Run Time will be updated every time when the automated report has been executed. Status of the report involve: Pending, Complete and in Progress

Steps to follow:

To **Add** Automated Report	1. Menu -> Reporting -> Automated 2. Click on link Add New Report 3. Enter the report name. 4. Select Date Range for the LR reports: • Today • Last 7 Days • Last 30 Days • Custom Start date – End date 5. Select the Devices. 6. Select IP Classes if required. 7. Select Report Types. The reports can be selected based on the all the reports under the category, or it can be chosen based on the individual reports. 8. Select the Scheduler to use, or add/edit one if required. (See Schedulers section.) 9. Enter email addresses, if required. All the LR reports generated will be sent to each address entered. 10. Select at least one Output format for the LR reports: • PDF • CSV 11. Click Add Report to save the entered details.
To **Edit** Automated Report	1. Menu -> Reporting -> Automated 2. Find the Automated Report you want to edit.

	3. Click on to edit. 4. Make the desired changes. 5. Click Update button to save the changes
To **Delete** Automated Report	1. Menu -> Reporting -> Automated 2. Find the Automated Report you want to delete. 3. Click on to delete. 4. Make the desired changes 5. Click Delete Report button to confirm
To **Download** generated LR reports	1. Menu -> Reporting -> Automated 2. Find the Automated Report you want to download generated LR reports from. 3. Click on to open the list of generated reports. 4. Find the generated reports you wish to download - they are listed by Start and End Run Times 5. Click CSV to download in CSV format, or click to download in PDF format 6. Enter location to save the file, and click Save
To **Delete** generated LR reports	1. Menu -> Reporting -> Automated 2. Find the Automated Report you want to delete generated LR reports from. 3. Click on to open the list of generated reports 4. Find the generated reports you wish to delete - they are listed by Start and End Run Times 5. Click to delete the generated reports. 6. Click Delete File(s) to confirm

7.5 - Schedulers

Scheduler is the tools that use to store the schedule information for an automated report to execute. You can find the scheduler when adding the automate report.

There are five standard schedule frequencies and each of the frequency is carry different execution pattern:

1. Hourly
    - Execute the reports after a number of hours (user can select 1,3,6, or 12)
2. Daily
    - Execute the reports at a particular time each day (user can select either everyday or weekdays only)
3. Weekly
    - Execute the reports on particular days each week (user can select which days of the week; multi-selection is allowed)
4. Monthly
    - Execute the reports once per month (user can select which months; multi-selection is allowed)
5. One Time Only
    - Execute the report once only at a specific time.

Steps to follow:

To Add the Scheduler:	1. Menu -> Reporting -> Automated 2. Click on link Add New Report or edit an existing report to view the Scheduler list. 3. Click on Add under the Scheduler section 4. Enter the Scheduler Name 5. Select the required schedule frequency. 6. Click Next button. 7. Select the Start Date and Start time Note: Start Date and Time must be later than current time. 8. Select the Execution information if required. 9. Click Ok to create the Scheduler **Note:** The Scheduler names must be unique. When a Scheduler is One Time Only, it will not appear for selection in the list after the Start time has passed, but it will still exist in the database.

To Edit the Scheduler:	1. Menu -> Reporting -> Automated 2. Click on link <u>Add New Report</u> or edit an existing report to view the Scheduler list. 3. Find the Scheduler name that you want to edit 4. Click on <u>Edit</u> 5. Make the required changes. 6. Click <u>Ok</u> to update the Scheduler **Note:** Editing a Scheduler will affect all reports that the Scheduler is used on.
To Delete the Scheduler:	1. Menu -> Reporting -> Automated 2. Click on link <u>Add New Report</u> or edit an existing report to view the Scheduler list. 3. Find the Scheduler name that you want to delete 4. Click on <u>Delete</u> 5. Click <u>Delete</u> to confirm **Note:** A Scheduler cannot be deleted if it is in use on any Automated Reports.

7.6 - On-Demand

On-Demand is the additional way to generate the single report based on specific conditional situation. On-Demand report is able to target the type of activity you need to focus on by narrowing down the scope of the report and focuses on the specific trend behaviour. You can choose to report on the activities that occurs within a single, specific window of time; or you can choose to regularly report the activities observed each day, week, or month. At the others words, on-Demand report is run a one-time report that occurred within a specific window of time. The report output can be displayed in the Web interface, PDF and CSV format. It is also able to export to local drive in PDF or CSV format.

Instead of just reading the summary of the report in the static way, On-Demand Report is come with drill down function which is able to view the details behind the summary report. With the advance functionality, quality and efficiency output performance will be much more granted.

With the improved architecture of the back-end engine, it will even calculate and estimate the expected time to generate the reports. If the reports that are to be generated is estimated to take lesser time than the Threshold Waiting Time, it will be generated on the browser. However, if the report is estimated to take longer than the Threshold Waiting Time, then the Log Radar will then advise the user to generate this report in Automated Report module. When the user agrees to this, all the name, date, category and other values will be imported into the Automated Report module automatically.

The estimated time is compared against a value called the Threshold Waiting Time. The estimated time is calculated based on the file size of the report metadata. Generating reports based on many days will naturally have bigger file size, which will then result in longer time to generate the report. Networks which have vast variety of data will also generate report metadata files that are large in size. The default Threshold Waiting Time set by Log Radar is 30 seconds. However this can be changed according to the user expectancy time. This value can be changed by accessing the configuration file in Program Files/Tecforte/Log Radar SE/config/web.properties file. Edit the below value to the expected time.

```
report_generation_wait_time=30000
```

On-Demand Reporting Centre is reachable through *Reporting* > *On-Demand*. The homepage of the reporting centre will state the 9 Categories and the report of the category respectively. There will be a brief explanation to each report for user’s better understanding.

The generated On-Demand Report will based on the selected Values and Reports.

Steps to follow:

To **Open Reporting Centre**	1. Menu -> Reporting -> On Demand 2. The Reporting Centre will open, and show brief descriptions of all available reports.
To **Generate an On Demand Report** from the Reporting Centre	1. Click on Edit Report Filter on the Left Menu. 2. Select the Date From and Date To. 3. Select Devices. 4. Select IP Classes if required. 5. Click on Save Filter button to save the reports criteria. 6. Click on a report name to view the data. 7. Repeat steps 1 and 6 to view different reports.
To **Drilldown on Report data**	1. Each report shows aggregate data over the time period selected - you can drilldown on each row to see more details. 2. Click on any field showing a link, to see the details for that row. 3. Each drilldown report will open in a new window. The drilldown report title will specify the data that is being shown.
To **Export Report data**	1. The data on both the main reports and the drilldown reports can be exported. 2. Click CSV to download in CSV format, or click 📄 to download in PDF format 3. Enter location to save the file, and click Save

7.7 - Compliance

As more companies are rushing towards compliance, generating reports that conforms to the regulatory has become a new task.

Compliance Reporting Centre has about 244 pre-configured compliance reports. Instead of having to search through the whole database to find the relevant reports, we have all the relevant reports grouped according to the Compliance.

Just like the On-Demand Report, Compliance Report comes with drill down functions where viewing of the details of the statistics is possible.

Compliance Reporting Centre is reachable through *Reporting > Compliance*. The homepage of the reporting centre states the lists of reports relevant to the regulatory. There will be a brief explanation to each report for user's better understanding.

The Threshold Waiting Time is also applicable under the Compliance reports. Reports that are estimated to take a long time to be generated, may be advised to be generated under the Automated Report Module.

Editing the Report Filter allows manipulation of the details of reports to be generated.

Report Filter bar displays information that is used to generate the Compliance Report.

Steps to follow:

To **Open Reporting Centre**	1. Menu -> Reporting -> Compliance 2. The Reporting Centre will open, and show brief descriptions of all available reports.
To **Generate a Compliance Report** from the Reporting Centre	1. Click on <u>Edit Report Filter</u> on the Left Menu. 2. Select the Date From and Date To. 3. Select Devices. 4. Select IP Classes if required. 5. Click on <u>Save Filter</u> button to save the reports criteria. 6. Click on a report name to view the data.

	7. Repeat steps 1 and 6 to view different reports.
To **Drilldown on Report data**	1. Each report shows aggregate data over the time period selected - you can drilldown on each row to see more details. 2. Click on any field showing a link, to see the details for that row. 3. Each drilldown report will open in a new window. The drilldown report title will specify the data that is being shown.
To **Export Report data**	1. The data on both the main reports and the drilldown reports can be exported. 2. Click CSV to download in CSV format, or click 📄 to download in PDF format 3. Enter location to save the file, and click <u>Save.</u>

8. Device Management

8.1 - Overview

The Device Management module allows you to add, edit and delete the Devices used in Log Radar. Logs sent by those Devices will be received by Log Radar, and processed according to the selected category. The logs can be in Syslog or in SNMP protocol. Users can also remote console to the device from the Log Radar software without having to open another browser or by using an extra SSH tool.

Syslogs

Syslogs will only be generated by the device when an event occurs. It can be attacks blocked, emails sent/received and even traffic activities. This is a one-way traffic where the device will only send Log Radar logs when necessary.

SNMP

Log Radar supports SNMP v2c and v3. In comparison to Syslog, using SNMP protocol, Log Radar will periodically “question” the device and it will respond to Log Radar with the “answer”. The “answers” from the SNMP will contribute to the Performance & Utilization Report category, which ranges from Memory usage to Hard disk usage.

Using the SNMP protocol, Log Radar will also periodically “ping” the device. When the device fails to respond, its status will be flagged as “down” and can be seen on the Dashboard.

The default setting for the periodical “question” is set to 5 minutes. If the Administrator decides to change this value, it can be done in Program Files/Tecforte/Log Radar SE/config/ssvr.properties.

```
snmp_walker_run_interval_minutes = 5
```

When configuring for SNMP v2c, the community name will be critical, where when configuring the SNMP v3, the authentication has to be correct to allow Log Radar to communicate with the device.

Users can choose to receive only Syslog messages, SNMP traps or even use both the protocols at the same time.

Remote Console

User can choose to remote console to the device without having to open another browser. From the dashboard, user can gain access to the Device Console page via HTTP/HTTPS.

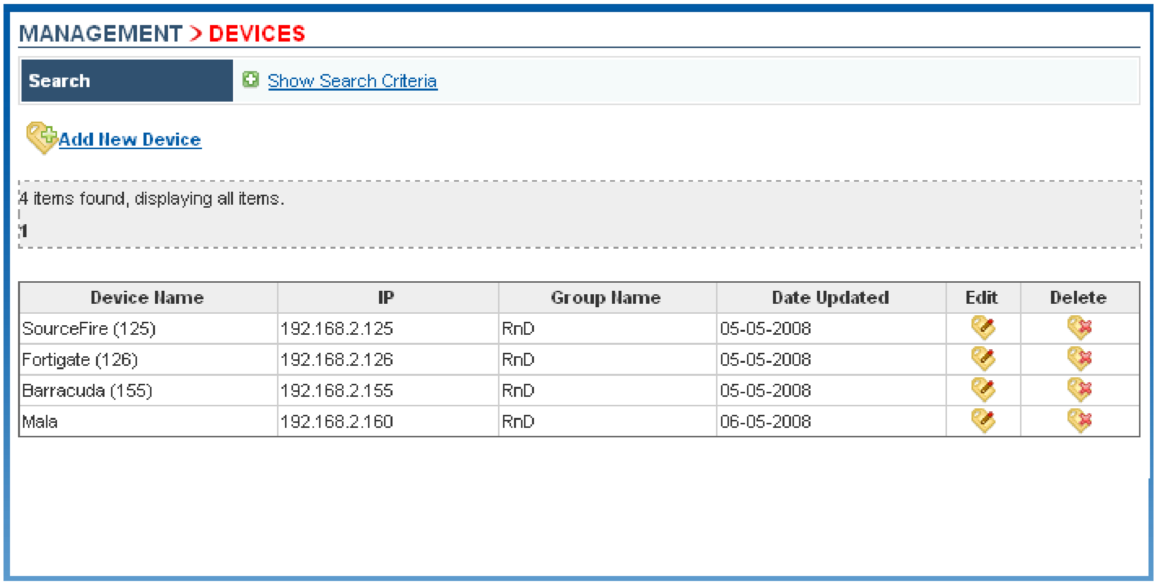
Users can also make changes to the settings of the device using SSH protocol (for SSH supported devices only).

Device Groups
Devices can be organised into Device Groups, to reflect their usage in your network.

Device License
The number of Devices allowed is limited by the license. Contact TecForte Sales Representative at any time to request a new licence to allow additional Devices.

8.2 - Devices

The list of current Devices is shown here, together with the Device IP Address, the Device Group, and the date last updated. To search for a specific Device or Devices, click on the link Show Search Criteria.



4 items found, displaying all items.
1

Device Name	IP	Group Name	Date Updated	Edit	Delete
SourceFire (125)	192.168.2.125	RnD	05-05-2008	✎	✗
Fortigate (126)	192.168.2.126	RnD	05-05-2008	✎	✗
Barracuda (155)	192.168.2.155	RnD	05-05-2008	✎	✗
Mala	192.168.2.160	RnD	06-05-2008	✎	✗

For every Device in Log Radar, the following fields are necessary:

- *IP Address* - this will allow Log Radar to recognise and process logs sent from the Device.
- *Device Name* - this will be displayed within Log Radar, used to identify the particular Device.
- *Device Category* - this allows Log Radar to parse the log format correctly.

Syslog

- *Protocol*
- *Port Number*
- *Port Number/Protocol* - this will establish the connection between Log Radar and the Device. 514/UDP is the standard protocol used for system logging, but you can use any valid combination for each separate Device. Note that you cannot use the same Port Number to listen on both TCP and UDP.

SNMP

- SNMP Version
- Community
- Username
- Security Level
- Authentication Protocol
- Authentication Password
- Privacy Protocol
- Privacy Password

Device Console

- URL

SSH

- Host
- Port
- Username

Assign Group

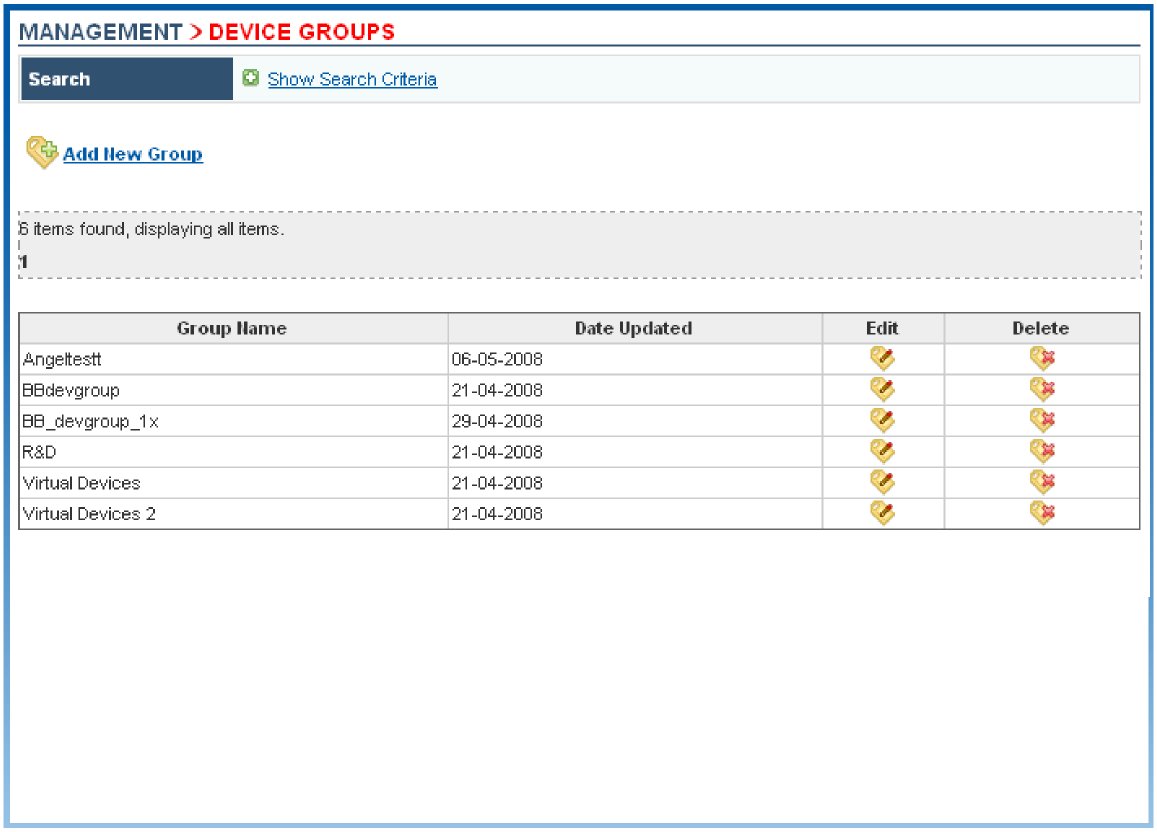
- *Group Name* - this will group together different Devices. An existing Device Group can be selected from the dropdown list, or a new one can be created when the Device is saved.

Steps to follow:

To **Add** Device	1. Menu -> Management -> Devices 2. Click on link Add New Device 3. Enter Device Details 4. Assign Group 5. Click Add button to save the new Device
To **Edit** Device	1. Menu -> Management -> Devices 2. Find the Device you want to edit 3. Click on ✎ to edit 4. Make the desired changes 5. Click Update button to save the changes
To **Delete** Device	1. Menu -> Management -> Devices 2. Find the Device you want to delete 3. Click on ✖ to delete 4. Click Delete Device button to confirm **Warning:** Deleting a Device means that logs from the Device will no longer be processed, and you will not be able to use Log Radar to investigate any existing logs.

8.3 - Device Groups

The list of current Device Groups is shown here, together with the date last updated. To search for a specific Device Group or Groups, click on the link Show Search Criteria.



MANAGEMENT > DEVICE GROUPS

6 items found, displaying all items.

1

Group Name	Date Updated	Edit	Delete
Angeltestt	06-05-2008	✎	✖
BBdevgroup	21-04-2008	✎	✖
BB_devgroup_1x	29-04-2008	✎	✖
R&D	21-04-2008	✎	✖
Virtual Devices	21-04-2008	✎	✖
Virtual Devices 2	21-04-2008	✎	✖

For every Device Group in Log Radar, the following fields are necessary:

- *Group Name* - this is used to group together different Devices. Other Log Radar modules will allow you to use the Group Names to make selection of Devices easier.

Steps to follow:

To **Add** Device Group	1. Menu -> Management -> Device Groups 2. Click on link Add New Group 3. Enter Group Details 4. Click Submit button to save the new Device Group
To **Edit** Device Group	1. Menu -> Management -> Device Groups 2. Find the Group you want to edit 3. Click on ✎ to edit 4. Make the desired changes 5. Click Update button to save the changes
To **Delete** Device Group	1. Menu -> Management -> Device Groups 2. Find the Group you want to delete 3. Click on ✖ to delete 4. Click Delete Group button to confirm **Warning:** Deleting a Group will also delete all Devices assigned to that Group. Logs from those Devices will no longer be processed, and you will not be able to use Log Radar to investigate any existing logs.

9. User Administration

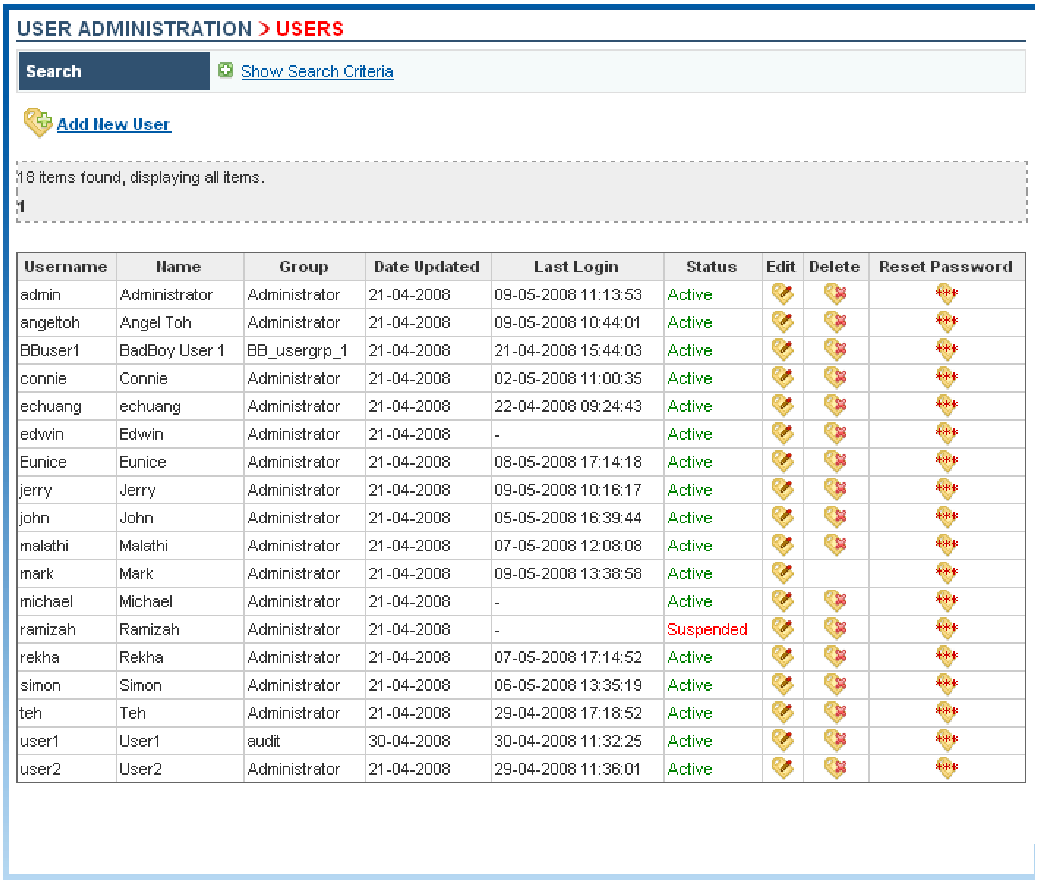
9.1 - Overview

The User Administration module allows you to add, edit and delete Users, and to control which areas of Log Radar the users can access. An Audit Trail is provided which will keep a record of all access to the system.

It is important to protect the system from unauthorized access. The Administrator user provided by default has full access to the system, but it is recommended that each user is given only the rights they need to perform their job function, and no more.

9.2 - Users

The list of current Usernames is shown here, together with the Name, the User Group, the date last updated, the last login date/time, and the Status. To search for a specific User or Users, click on the link Show Search Criteria.



18 items found, displaying all items.

1

Username	Name	Group	Date Updated	Last Login	Status	Edit	Delete	Reset Password
admin	Administrator	Administrator	21-04-2008	09-05-2008 11:13:53	Active	✎	✖	***
angeltoh	Angel Toh	Administrator	21-04-2008	09-05-2008 10:44:01	Active	✎	✖	***
BBuser1	BadBoy User 1	BB_usergrp_1	21-04-2008	21-04-2008 15:44:03	Active	✎	✖	***
connie	Connie	Administrator	21-04-2008	02-05-2008 11:00:35	Active	✎	✖	***
echuang	echuang	Administrator	21-04-2008	22-04-2008 09:24:43	Active	✎	✖	***
edwin	Edwin	Administrator	21-04-2008	-	Active	✎	✖	***
Eunice	Eunice	Administrator	21-04-2008	08-05-2008 17:14:18	Active	✎	✖	***
jerry	Jerry	Administrator	21-04-2008	09-05-2008 10:16:17	Active	✎	✖	***
john	John	Administrator	21-04-2008	05-05-2008 16:39:44	Active	✎	✖	***
malathi	Malathi	Administrator	21-04-2008	07-05-2008 12:08:08	Active	✎	✖	***
mark	Mark	Administrator	21-04-2008	09-05-2008 13:38:58	Active	✎		***
michael	Michael	Administrator	21-04-2008	-	Active	✎	✖	***
ramizah	Ramizah	Administrator	21-04-2008	-	Suspended	✎	✖	***
rekha	Rekha	Administrator	21-04-2008	07-05-2008 17:14:52	Active	✎	✖	***
simon	Simon	Administrator	21-04-2008	06-05-2008 13:35:19	Active	✎	✖	***
teh	Teh	Administrator	21-04-2008	29-04-2008 17:18:52	Active	✎	✖	***
user1	User1	audit	30-04-2008	30-04-2008 11:32:25	Active	✎	✖	***
user2	User2	Administrator	21-04-2008	29-04-2008 11:36:01	Active	✎	✖	***

For every User in Log Radar, the following fields are necessary:

- *Username* - this is used to login to Log Radar
- *Name* - this is to identify the full name of the User
- *Email* - this is used to communicate the initial password to the User
- *User Group* - this is used to control which Log Radar features the User can access. See below for details.

There is also an optional *Description* field, which you can use to enter additional text.

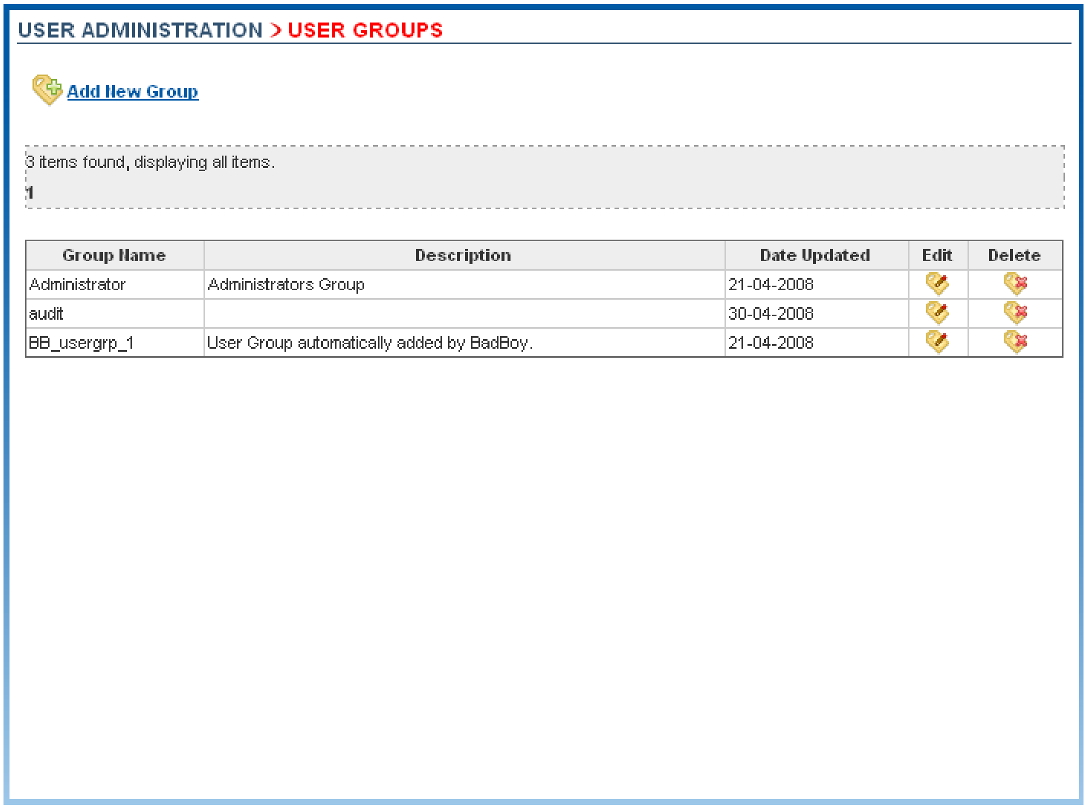
Steps to follow:

To **Add** User	1. User Administration -> Users 2. Click on link Add New User 3. Enter User Details 4. Click Submit button to save the new User **Note:** A secure initial password will be generated and emailed to the User. After the first successful login, the User will be prompted to change the password, and will be unable to gain access until this done.
To **Edit** User	1. User Administration -> Users 2. Find the User you want to edit 3. Click on ✎ to edit 4. Make the desired changes 5. Click Update button to save the changes
To **Delete** User	1. User Administration -> Users 2. Find the User you want to delete 3. Click on ✖ to delete 4. Click Delete User button to confirm
To **Reset** User Password	1. User Administration -> Users 2. Find the User you want to delete 3. Click on *** to reset

	4. Click Reset User button to confirm **Note:** A User may be suspended due to incorrect login attempts or a period of inactivity. The thresholds for these are set using the Settings Configuration - see *Section 10.3 Settings* for more details. Resetting the password will reactivate the User, and a new secure password will be generated and emailed to the User. After the first successful login, the User will be prompted to change the password, and will be unable to gain access until this done. Reset Password can also be used when a password is forgotten by the User.

9.3 - User Groups

The list of current User Groups is shown here, together with the description and the date last updated.



USER ADMINISTRATION > USER GROUPS

3 items found, displaying all items.
1

Group Name	Description	Date Updated	Edit	Delete
Administrator	Administrators Group	21-04-2008	✎	✗
audit		30-04-2008	✎	✗
BB_usergrp_1	User Group automatically added by BadBoy.	21-04-2008	✎	✗

For every User Group in Log Radar, the following fields are necessary:

- *Group Name* - this is used to identify the User Group in Log Radar.
- *Selected Modules* - this is used to control which Log Radar modules the User can access. Each module has a number of sub-modules which can be selected. Note that there are some dependencies, e.g. if “Edit Device” is selected, then “Device List Page” will be automatically selected too.

There is also an optional *Description* field, which you can use to enter additional text.

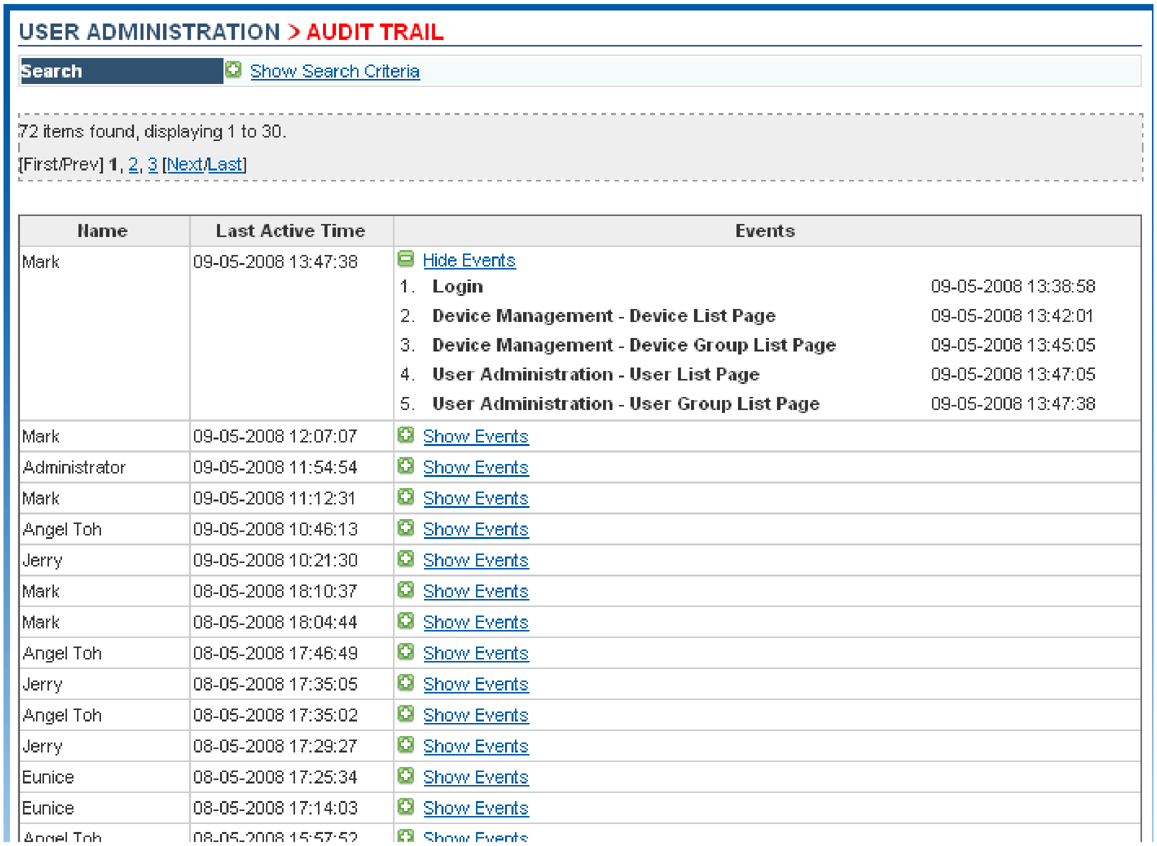
Steps to follow:

To **Add** User	1. User Administration -> User Groups 2. Click on link Add New Group 3. Enter User Group Details 4. Click on each desired Main Module, and select the desired Sub-modules. You can quickly give access to an entire module by using the >> button, otherwise select specific sub-modules using the > button. 5. Click Add button to save the new User Group
To **Edit** User	1. User Administration -> User Groups 2. Find the User Group you want to edit 3. Click on ✎ to edit 4. Make the desired changes 5. Click Update button to save the changes
To **Delete** User	1. User Administration -> User Groups 2. Find the User Group you want to delete 3. Click on ✖ to delete 4. Click Delete Group button to confirm **Note:** A User Group cannot be deleted when it is in use. All Users assigned to a Group must be reassigned first.

9.4 - Audit Trail

All User activity is recorded in the Audit Trail, for security and forensic purposes. The Audit Trail page shows each User Session, together with the time last active. You can drilldown on each session to see the Events recorded during the session.

To search for a specific Event or Events, click on the link Show Search Criteria. The Audit Trail can be searched by User, by Activity, or by Date.



USER ADMINISTRATION > AUDIT TRAIL

72 items found, displaying 1 to 30.

[First/Prev] 1, 2, 3 [Next/Last]

Name	Last Active Time	Events
Mark	09-05-2008 13:47:38	Hide Events 1. **Login** 09-05-2008 13:38:58 2. **Device Management - Device List Page** 09-05-2008 13:42:01 3. **Device Management - Device Group List Page** 09-05-2008 13:45:05 4. **User Administration - User List Page** 09-05-2008 13:47:05 5. **User Administration - User Group List Page** 09-05-2008 13:47:38
Mark	09-05-2008 12:07:07	Show Events
Administrator	09-05-2008 11:54:54	Show Events
Mark	09-05-2008 11:12:31	Show Events
Angel Toh	09-05-2008 10:46:13	Show Events
Jerry	09-05-2008 10:21:30	Show Events
Mark	08-05-2008 18:10:37	Show Events
Mark	08-05-2008 18:04:44	Show Events
Angel Toh	08-05-2008 17:46:49	Show Events
Jerry	08-05-2008 17:35:05	Show Events
Angel Toh	08-05-2008 17:35:02	Show Events
Jerry	08-05-2008 17:29:27	Show Events
Eunice	08-05-2008 17:25:34	Show Events
Eunice	08-05-2008 17:14:03	Show Events
Angel Toh	08-05-2008 15:57:52	Show Events

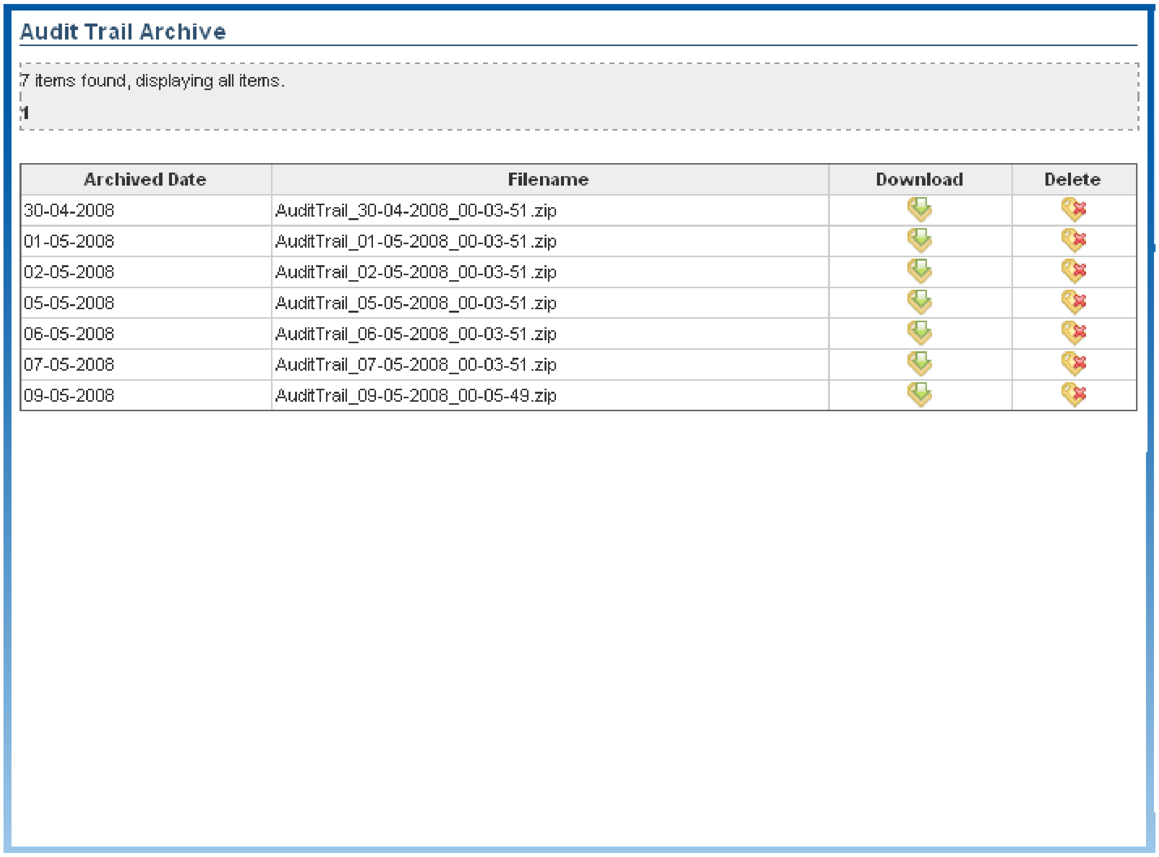
To prevent the Audit Trail from growing too large, there is regular housekeeping activity, where all data older than a set period will be archived. It will not be removed from the system, but will no longer be shown on this page. See below for more details.

The current Audit Trail data can be exported by clicking on the CSV link at the bottom of the page.

9.5 - Audit Trail Archive

When Audit Trail data is older than a set period, it will be archived, and can be accessed from this page. This housekeeping period is set using the Security Configuration - see *Section 10.3 Settings* for more details.

The Audit Trail Archive list will show the Archived Date, and the Filename. These zipped files can be downloaded if required, and they can be permanently deleted from the system.



Audit Trail Archive

7 items found, displaying all items.
1

Archived Date	Filename	Download	Delete
30-04-2008	AuditTrail_30-04-2008_00-03-51.zip	⬇	✖
01-05-2008	AuditTrail_01-05-2008_00-03-51.zip	⬇	✖
02-05-2008	AuditTrail_02-05-2008_00-03-51.zip	⬇	✖
05-05-2008	AuditTrail_05-05-2008_00-03-51.zip	⬇	✖
06-05-2008	AuditTrail_06-05-2008_00-03-51.zip	⬇	✖
07-05-2008	AuditTrail_07-05-2008_00-03-51.zip	⬇	✖
09-05-2008	AuditTrail_09-05-2008_00-05-49.zip	⬇	✖

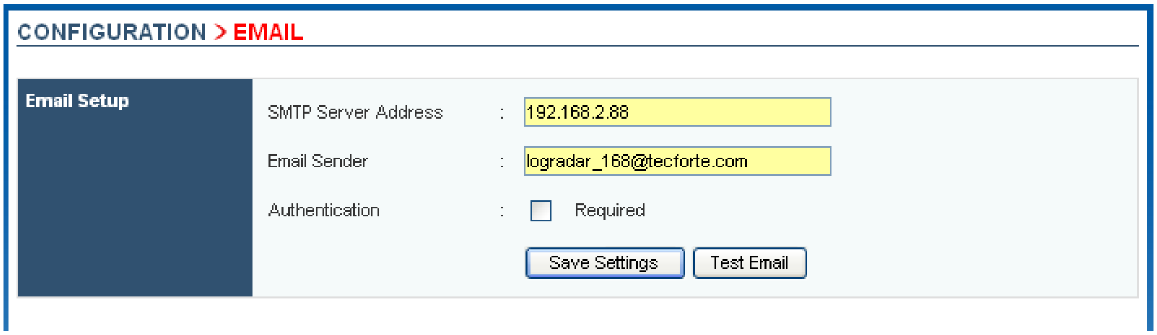
10. Configuration

10.1 - Overview

After the installation, it is necessary to set some configuration settings before using Log Radar. The security settings already have default values; however, you may modify these based on your preference at any time.

10.2 - Email

The Email Configuration settings are necessary so that Log Radar can send out emails. This must be done before Users are added, as the initial passwords must be sent out by email. Log Radar can also send out emails for Real-Time Threat Alerts, Automated Reports, Automated Asset Discovery scan notifications, etc.



CONFIGURATION > EMAIL

Email Setup

SMTP Server Address : 192.168.2.88
Email Sender : logradar_168@tecforte.com
Authentication : ☐ Required

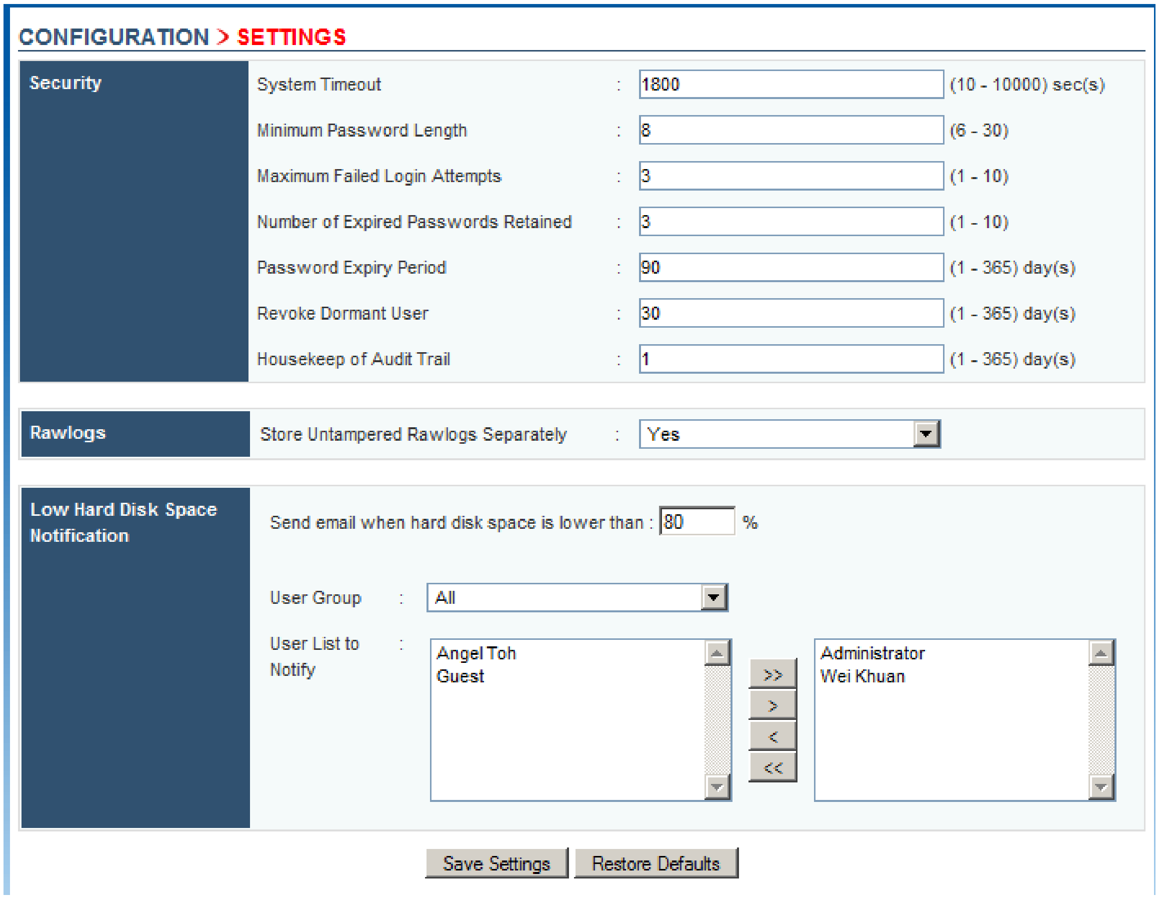
Steps to follow:

Email Setup	1. Configuration -> Email 2. Enter SMTP Server Address 3. Enter an Email Sender address 4. If Authentication is required, check the box and enter the username and password. Otherwise, leave box unchecked 5. Click <u>Save Settings</u> button to save the entered information

Test Email	1. Configuration -> Email 2. Click on Test Email button 3. Enter a valid email address 4. Click Send Email button 5. If the test email does not reach your mailbox, then you need to recheck the configuration.

10.3 - Settings

The default settings provide a reasonable level of security; however you may wish to configure different levels. The default levels can be restored at any time.



CONFIGURATION > SETTINGS

Security

System Timeout : 1800 (10 - 10000) sec(s)
Minimum Password Length : 8 (6 - 30)
Maximum Failed Login Attempts : 3 (1 - 10)
Number of Expired Passwords Retained : 3 (1 - 10)
Password Expiry Period : 90 (1 - 365) day(s)
Revoke Dormant User : 30 (1 - 365) day(s)
Housekeep of Audit Trail : 1 (1 - 365) day(s)

Rawlogs

Store Untampered Rawlogs Separately : Yes

Low Hard Disk Space Notification

Send email when hard disk space is lower than : 80 %
User Group : All
User List to Notify : Angel Toh, Guest
Administrator, Wei Khuan

The available settings are:

Security Settings

- *System Timeout* - this determines the maximum period of inactivity before a session is automatically ended.
- *Minimum password length* - this determines the least number of characters that a password for a User may contain.
- *Maximum Failed Login Attempt* - this determines the maximum number of times a User can enter an incorrect password before being suspended.
- *Number of Retain Expired Password* - this determines how many previously used passwords will be kept. A User will be unable to reuse a password while it is being retained.

- *Password Expiry Period* - this determines the how frequently a User must change their password. The User will be suspended if the password is not changed within this period.
- *Revoke Dormant User* - this determines the period to revoke a dormant user.
- *Housekeep of Audit Trail* - this determines the period during which recorded user activities will be stored in the Audit Trail. Once the period has passed, the data will be archived. See Section 8.5 for more details.

Rawlogs

- *Store Untampered Rawlogs Separately* – this determines if the rawlogs should be saved separately or not. These extra set of rawlogs will be saved in a separate folder, compressed and hashed on a daily basis, to prevent tampering of information. Regardless of the setting here, all rawlogs will still be processed into Log Radar like normal.

Low Hard Disk Space Notification

- *Send email when hard disk space is lower than* – this determines the threshold for the notification. If the threshold has been exceeded, a notification email will be sent to the list of selected users by 2.00am daily.
- *User List to Notify* – select the list of users to be notified when hard disk space usage has exceeded the threshold.

Data Integration

- *Data integration required* – if this server is deployed in a distributed architecture and will be sending/receiving logs from other branches, select Yes.
- *Local Host as* – this selection will appear if Data integration required is selected as Yes. If this server will act as the Master/HQ Log Radar, select Destination. If this server will act as the Slave/Branch Log Radar, where it will be sending logs back to the Master/HQ Log Radar, select Source.
- *User List to Notify* – select the list of users to be notified when data transfer fails, etc.

Steps to follow:

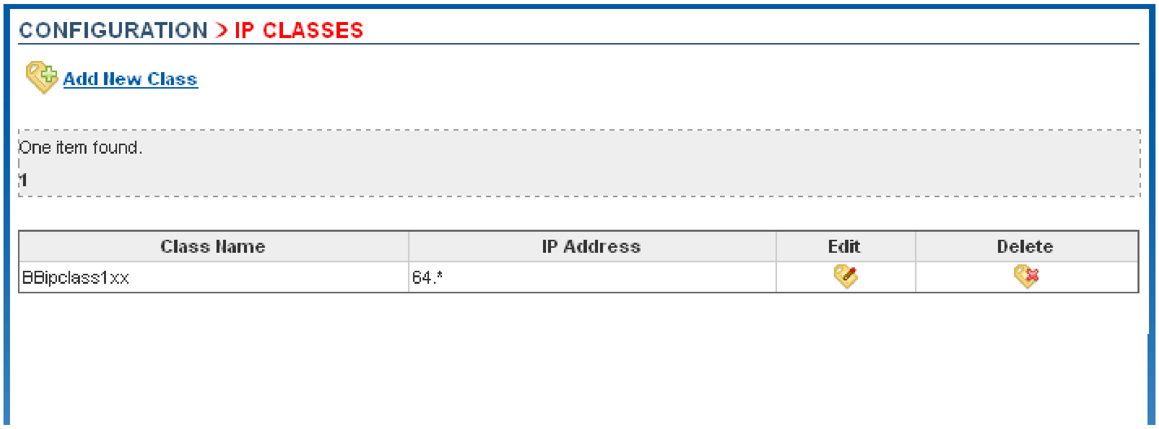
Security Settings	1. Enter desired values for each setting 2. Click Save Settings button to save the entered information

Restore Defaults	1. Click on Restore Defaults button 2. Click Save Settings button to save the restored information

10.4 - IP Classes

IP Classes provide the ability to analyse, correlate, and report on log information by a user-defined classification policy. Log Radar will classify each log it processes, or record it as “unclassified”. The match will be based on the IP Addresses used in the Class definition, and the Destination IP of the log.

The classification of logs is maintained in all historical logs even if the class is modified or deleted.



CONFIGURATION > IP CLASSES

Add New Class

One item found.

1

Class Name	IP Address	Edit	Delete
BBipclass1xx	64.*	✎	✖

Steps to follow:

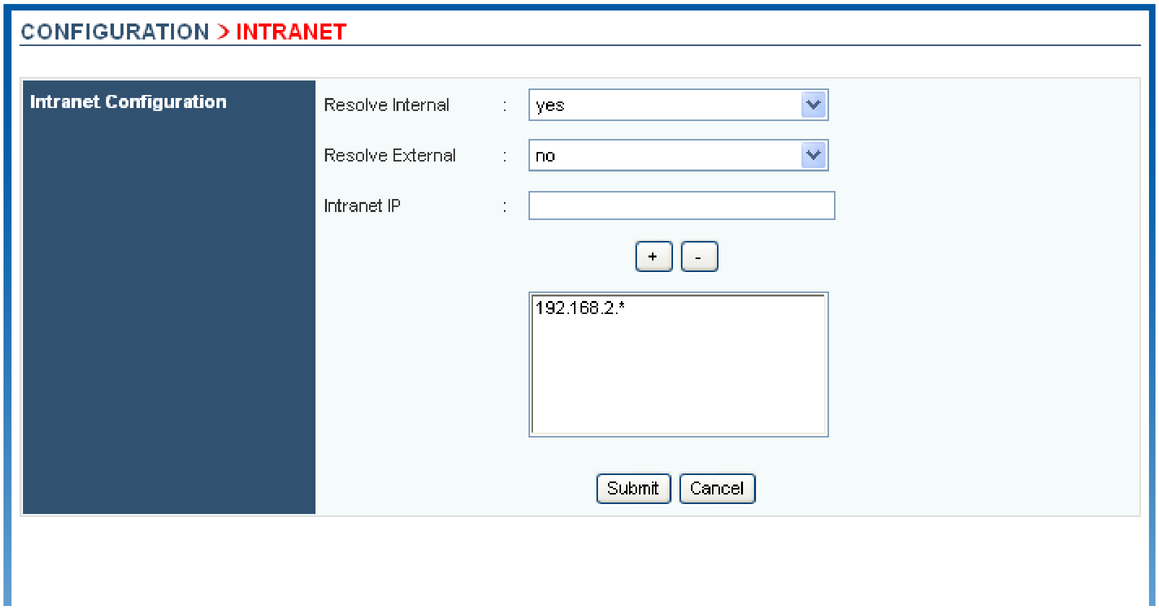
To **Add** IP Class	1. Configuration -> IP Classes 2. Click on link <u>Add New Class</u> 3. Enter IP Class Details 4. Enter IP Addresses and click the <u>+</u> button to enter. You can enter individual IP Addresses, or use a wildcard (e.g. 192.168.4.*) 5. Click <u>Submit</u> button to save the new IP Class **Note:** The entered IP Addresses must not overlap with those in any existing Classes. This is because a log can be classified to at most one IP Class.
To **Edit** IP Class	1. Configuration -> IP Classes 2. Find the IP Class you want to edit 3. Click on ✎ to edit

	4. Make the desired changes 5. Click <u>Update</u> button to save the changes **Note:** Only the Class Name and Description fields can be edited. It is not possible to edit the selected IP Addresses.
To **Delete** IP Class	1. Configuration -> IP Classes 2. Find the IP Class you want to delete 3. Click on ✖ to delete 4. Click <u>Delete Class</u> button to confirm **Note:** Deleting an IP Class means that logs will no longer be assigned to that IP Class. Any existing logs will retain their classifications, and the deleted IP Class will still be available for selection in Reporting and Log Analytics.

10.5 - Intranet

The Intranet Configuration allows you to specify the IP addresses of your internal network. It is important that Log Radar is able to distinguish between internal and external IP addresses, so that for example each traffic flow can be classified as Internal, Inbound, Outbound, etc.

Additionally, you can use this page to set whether to resolve IP addresses. When this is set to “yes”, then Log Radar will attempt to resolve the IP Address into a host name, which will be stored in the "Host Name" field for normalised logs.



Resolve Internal : yes
Resolve External : no
Intranet IP :
192.168.2.*

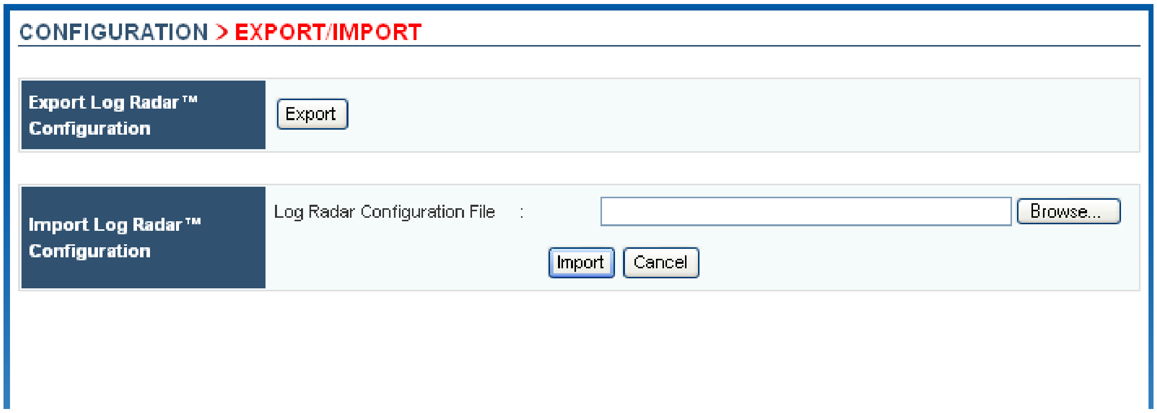
Steps to follow:

Intranet Configuration	1. Configuration -> Intranet 2. Enter IP Addresses in the field **Intranet IP**, and click the + button to enter. You can enter individual IP Addresses, or use a wildcard (e.g. 192.168.4.*) 3. Click Submit button to save the new configuration
Resolve Internal IP	1. Configuration -> Intranet

Addresses	2. Set the field **Resolve Internal** to “yes” 3. Click Submit button to save the new configuration **Note:** It is not possible to resolve Internal IP Addresses unless the Intranet range has been defined, as above.
Resolve External IP Addresses	1. Configuration -> Intranet 2. Set the field **Resolve External** to “yes” 3. Click Submit button to save the new configuration **Note:** It is not possible to resolve External IP Addresses unless the Intranet range has been defined, as above.

10.6 - Export/Import

Log Radar can export and import the user-entered data. This may be useful when backing up, lots of alerts, new installation, etc.


CONFIGURATION > EXPORT/IMPORT
Export Log Radar™ Configuration
Export
Import Log Radar™ Configuration
Log Radar Configuration File :
Browse...
Import
Cancel

The Export file will include the following data:

- Asset Discovery Configurations
- Real-Time Threats Rules & Correlations Configurations
- Reporting Configurations
- User & User Group
- Email Configurations
- Settings Configurations
- IP Classes Configurations
- Intranet Configurations
- Backup/Restore Configurations

Note: The Export/Import feature only works for **user-entered** data. It does **not** include the logs which have previously been received and processed and all results of Asset Discovery, Real-Time Threats, Report Files and Log Analytics.

Steps to follow:

To **Export** Log Radar Configuration	1. Configuration -> Export/Import 2. Click Export button

	3. Click Save button 4. Enter a location to save the file to, and click Save
To **Import** Log Radar Configuration	1. Configuration -> Export/Import 2. Enter or browse to the location of the desired configuration file 3. Click Import button 4. Click OK button to confirm **Warning:** Importing a configuration file will overwrite the current configuration. You will lose all of the existing user-entered data, and so caution is advised.

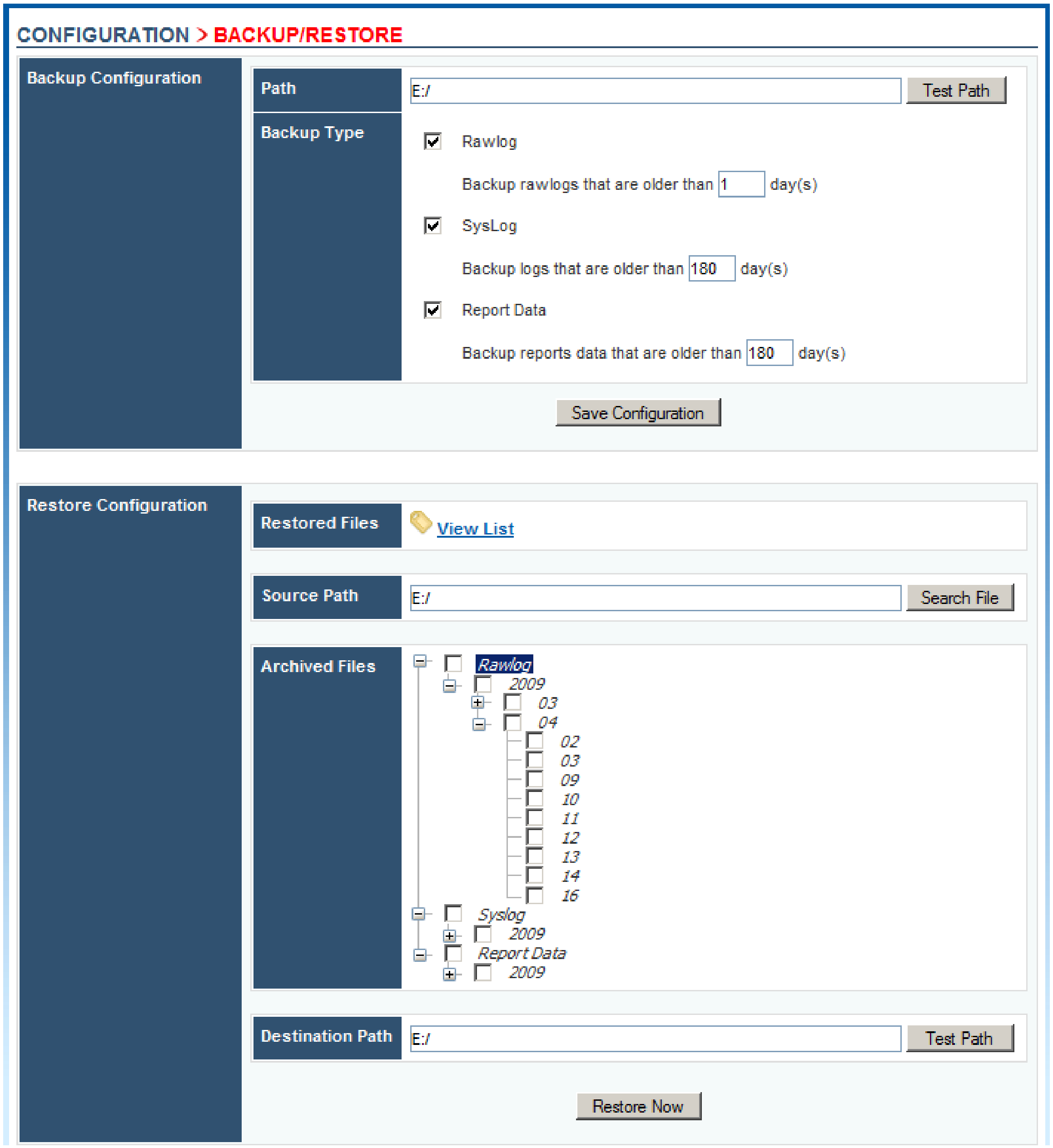
10.7 - Rawlog, Syslog, Report Data Backup/Restore

This step allows you to specify your old Rawlogs, Syslogs and Report Data archival schedule.

These files will be compressed and encrypted into the backup folder. After archival, the disk space in the local disk will be freed up.

However, do note that after archival, Log Analysis will not be able to be performed on the old Syslogs and you will not be able to generate Reports from the old report data. To perform log analysis and reports from these archived files, they will have to be restored.

When the Rawlogs are being backup, it will not affect the hashing information. The hash file will also be included when the rawlogs are being backup.



CONFIGURATION > BACKUP/RESTORE

Backup Configuration

Path: E:/

Backup Type:

☑ Rawlog

Backup rawlogs that are older than 1 day(s)

☑ SysLog

Backup logs that are older than 180 day(s)

☑ Report Data

Backup reports data that are older than 180 day(s)

Restore Configuration

Restored Files: View List

Source Path: E:/

Archived Files:

- ☐ Rawlog
  - ☐ 2009
    - ☐ 03
    - ☐ 04
      - ☐ 02
      - ☐ 03
      - ☐ 09
      - ☐ 10
      - ☐ 11
      - ☐ 12
      - ☐ 13
      - ☐ 14
      - ☐ 16
- ☐ Syslog
  - ☐ 2009
- ☐ Report Data
  - ☐ 2009

Destination Path: E:/

Steps to follow:

To **Backup** Syslog, Report Data & Rawlog	1. Configuration > Backup/Restore > Data 2. Enter a local path 3. Click <u>Test Path</u> button 4. If the test failed, then you need to recheck on your path again.

	5. Enter the age of the syslog, reports & rawlog to be backup 6. Click Save Configuration button to save all the configurations. **Note:** The backup folder can be in a different folder, however it has to be located in the same physical server.
To **Restore** Rawlog, Syslog & Report Data	1. Configuration > Backup/Restore > Data 2. Enter the local path or mapped network drive where the files were saved to 3. Click Search File button 4. Select the dates of the files to be restored 5. Enter another local path or mapped network drive where the files will be restored to 6. Click Test Path button 7. Click Restore Now button to restore the selected files. **Note:** The backup folder can be in a different folder, however it has to be located in the same physical server.

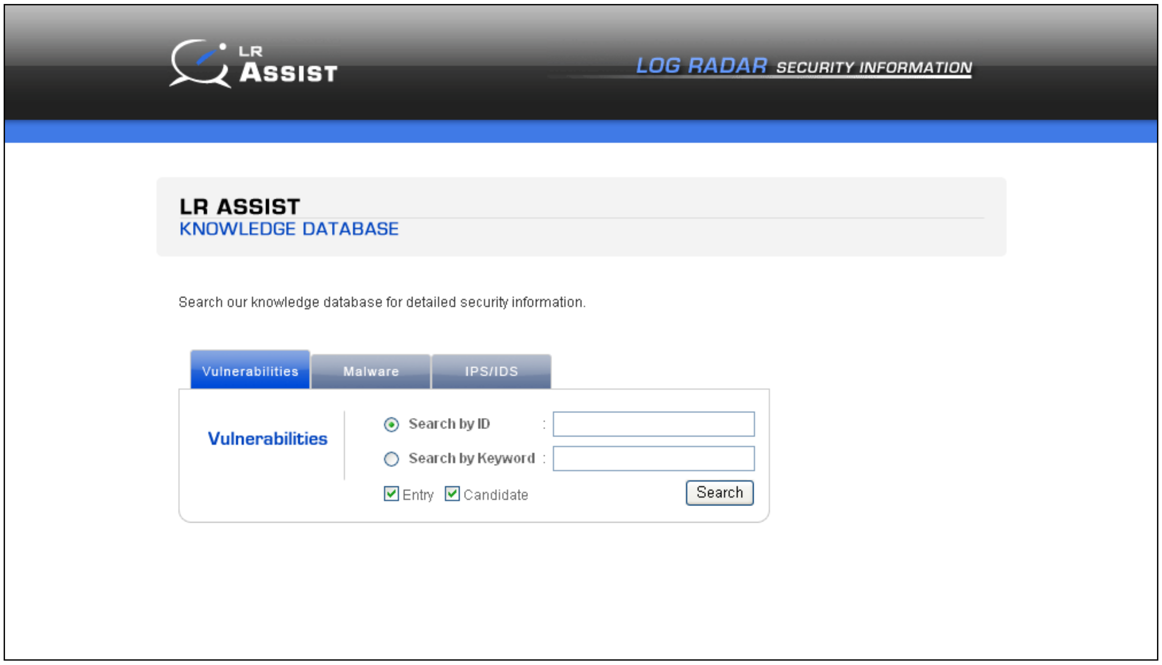
11. LR Assist

11.1 - Overview

LR Assist is an online store of security information, which is available exclusively to Log Radar customers. The database includes Vulnerabilities, Malware, and IPS/IDS information.

11.2 - Starting LR Assist

LR Assist can be easily accessed from every page of Log Radar. Simply click on the link in the top right-hand corner, and the LR Assist search page will be opened in a new window. If this is the first time you have used LR Assist, you will need to enter your company username and password.



LR ASSIST
KNOWLEDGE DATABASE

Search our knowledge database for detailed security information.

● Search by ID :

○ Search by Keyword :

☑ Entry ☑ Candidate

11.3 - Searching for Vulnerabilities Information

To find a particular vulnerability using the CVE ID number:

1. Click on the Vulnerabilities Tab.
2. Use the checkboxes to indicate whether you wish to restrict the search to Entry or Candidate status only.
3. Enter the ID into the "Search by ID" text box, and then press Enter or click on Search button.
4. From the result page, click 'Back to Search' link to go back to the search page.

To search for information using keywords:

1. Click on the Vulnerabilities Tab, check on the criteria box.
2. Use the checkboxes to indicate whether you wish to restrict the search to Entry or Candidate status only.
3. Enter keyword(s) into the "Search by Keyword" text box, and then press Enter or click on Search button.
4. From the result page, click 'Back to Search' link to go back to the search page.

11.4 - Searching for Malware Information

To find a particular virus, worm or trojan using the CME ID number:

1. Click on the Malware Tab.
2. Enter the ID into the "Search by ID" text box, and then press Enter or click on Search button.
3. From the result page, click 'Back to Search' link to go back to the search page.

To search for information using keywords:

1. Click on the Malware Tab.
2. Enter keyword(s) into the "Search by Keyword" text box, and then press Enter or click on Search button.
3. From the result page, click 'Back to Search' link to go back to the search page.

11.5 - Searching for IPS/IDS Information

To find a particular rule using the Snort ID number:

1. Click on the IPS/IDS Tab.
2. Enter the ID into the "Search by ID" text box, and then press Enter or click on Search button.
3. From the result page, click 'Back to Search' link to go back to the search page.

To search for information using keywords:

1. Click on the IPS/IDS Tab.
2. Enter keyword(s) into the "Search by Keyword" text box, and then press Enter or click on Search button.
3. From the result page, click 'Back to Search' link to go back to the search page.

11.6 - Further Help

If you require more information on any security topic after using LR Assist, contact support@tecforte.com.

Appendix A: Glossary

Term	**Description**
Alert	Refers to a warning message that will be sent to user via email when there is a trigger.
Automated Report	Refers to the details of a process for generating a set of LR reports according to the selected Scheduler.
Bytes Received	Refers to total received by destination device.
Bytes Sent	Refers to total bytes sent by source device.
Compliance	Refers to the reports that captures information required by the regulations for future analysis
Correlation	Refers to grouping set of rules using some relational function and with threshold and frequency value.
Destination	Refers to the IP Address or the Host name receiving message.
Device	Refers to a security device on your network which is capable of generating logs to be collected by Log Radar
Device Group	Refers to a user-defined label which can be used to sort different types of Devices, to allow for easier selection in Log Radar modules
Frequency	Refers to time limit or time frame for a rule to detect logs before a trigger. Usually in seconds or minutes.
Importance	Refers to the importance attached to a Correlation - can be high, medium or low.
IP / IP Range	Refers to one / range of IP Address (es).
IP Classification / IP Class	Refers to the optional classification of logs based on the Destination IP.
Keyword	Refers to a word or key value which is used to find the exact keyword from a log, by matching every char.

Log Analytic	Refers to a forensic search which can be carried out on historic Log Radar data, using a variety of different criteria.
Packets Received	Refers to number of packets received by destination device.
Packets Sent	Refers to number of packets sent by source device.
Pattern	Refers to a word or string which is used to find the exact string match from a log, using regex.
Port / Port Range	Refers to one / range of device port number(s).
Predefined IP	Refers to set of IP addresses which have been added earlier in the system with name and description.
Predefined Port	Refers to set of ports which have been added earlier in the system with name and description.
Reporting Centre	Refers to the on-demand reporting feature, where a user can instantly generate LR reports.
Rule	Refers to a directive statement that is used to query logs which matches to it.
Scheduler	Refers to a user-defined entry to control when the Automated Report generation will commence.
Source	Refers to the IP Address or the Host name sending out message.
Status	Refers to the condition of the correlation, usually Active / Inactive. Active: Executing; and Inactive: Sleep mode.
Threshold	Refers to number of logs to be detected before a trigger.
Trigger	Refers to a signal sent to the system when the backend engine detects rules which hits the threshold and frequency.

Appendix B: Security Information

Vulnerabilities

The LR Assist vulnerabilities information is provided by CVE.

CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration."

CVE-compatible means:

- CVE SEARCHABLE - A user can search using a CVE Identifier to find related information.
- CVE OUTPUT - Information is presented that includes the related CVE Identifier(s).
- MAPPING - The repository owner has provided a mapping relative to a specific version of CVE, and has made a good faith effort to ensure accuracy of that mapping.
- DOCUMENTATION - The organization's standard documentation includes a description of CVE, CVE compatibility, and the details of how its customers can use the CVE-related functionality of its product or service.

Malware

The LR Assist malware information is provided by CME.

The Common Malware Enumeration (CME) initiative aims to provide single, common identifiers to new virus threats (i.e., malware) and to the most prevalent virus threats in the wild for the benefit of the public.

CME reduces confusion by assigning a single CME identifier to a particular threat so that anti-virus entities, as well as other security-related entities, can include it along with their proprietary information. In this way the public may cross-reference the disparate virus names through a common identifier.

CME defines malware as any computer code such as a virus, worm, etc., with the potential to damage a computer system or network. Spyware and adware will not receive CME identifiers.

---- END ----