



SendQuick Avera Licensing Agreement and User Manual

Version 3.0 (2 July 2025)

SendQuick Pte Ltd

76 Playfair Road

#08-05 LHK2 Building

Singapore 367996

Tel: +65 6280 2881 Fax: +65 6280 6882

Email: info@sendquick.com

www.SendQuick.com

SendQuick Server Software License Agreement

For SOFTWARE PRODUCT, content and software information marked with © TalariaX, © TalariaX Pte Ltd, © SendQuick, or © SendQuick Pte Ltd the following license agreement applies to you:

This is a legal agreement between you, the end user or User Corporation, and TalariaX Pte Ltd, Singapore, and SendQuick Pte Ltd, Singapore. By purchasing and starting (power-up) the Server with the SendQuick software (SOFTWARE PRODUCT) installed in the Server, you agreed to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, promptly stop the start-up process by shutting down the system and return the product package to the place you obtained it for a full refund (subject to relevant terms and conditions for refund) provided the product package is in its original condition.

1. Grant of license

TalariaX Pte Ltd, and SendQuick Pte Ltd grants you the right to use one copy of the enclosed SOFTWARE PRODUCT - the SOFTWARE - on a single Server that it is being installed in by TalariaX and SendQuick. The SOFTWARE is in use on a computer when it is loaded into memory or installed into permanent memory of that computer. This license is attached with the hardware (Server) that was originally installed by TalariaX and SendQuick.

This license does not permit or allow or warrant any rights to redistribute, duplicate, compile, reverse compile or any acts that will remove or seek to remove the SOFTWARE from the original server that it was installed in. The effort for the above stated actions includes both software or hardware related including but not exclusive to hard disk duplication, network transfer, network duplicate or any acts that may cause the removal of the SOFTWARE from the original storage position. Any of such acts stated herein shall amount to a breach of the copyright and this licensing agreement and is punishable by the Court of Law in Singapore and your respective countries. Duplication, copying or whatsoever acts or intent pertaining to remove the SOFTWARE from this server is strictly prohibited.

2. Additional grant of license

In addition to the rights granted in Section 1, TalariaX Pte Ltd and SendQuick Pte Ltd grant you a nonexclusive right to use the SOFTWARE in the Server by an unlimited number of users or application servers to send messages to an unlimited number of recipients.

3. Copyright

This software is owned by TalariaX Pte Ltd and SendQuick Pte Ltd or its suppliers and is protected by Singapore and international copyright laws and treaties. Therefore, you must treat the SOFTWARE like any other copyrighted material. Except that if the SOFTWARE is not copy protected you may either make one copy of the SOFTWARE solely for backup purpose or transfer the SOFTWARE to a single hard disk provided that you keep the original for backup or archive purposes. You may not copy the product manuals or any written material accompanying the SOFTWARE.

Some of the components that support the SOFTWARE are owned by independent owners and developers. The copyrights of these components are owned by their respective owners and developers and TalariaX and SendQuick does not claim to own or develop these components.

Some of the components distributed with this SOFTWARE are owned by independent owners and developers, and the respective licenses contained in the package which distributes this SOFTWARE (e.g. GNU General Public Licenses, Apache Licenses) apply to such components. TalariaX Pte Ltd and SendQuick Pte Ltd does not claim to own or develop any of the copyright or any other rights in the components distributed with the SOFTWARE which have copyright notices other than "© TalariaX", "© TalariaX Pte Ltd", "© SendQuick", or "© SendQuick Pte Ltd".

- For programs under the GNU General Public License: The programs are free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version. The programs are distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with the programs. If not, see <<http://www.gnu.org/licenses/>>.

- For programs under the Apache License, Version 2.0: you may not use those files except in compliance with the Apache License, Version 2.0. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>. Unless required by applicable law or agreed to in writing,

software distributed under the Apache License, Version 2.0 is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the Apache License, Version 2.0 for the specific language governing permissions and limitations under the license.

The receiver of this SOFTWARE is expected to abide by the terms and conditions of all of the licenses contained in this package.

TalariaX Pte Ltd and SendQuick Pte Ltd disclaim all liability for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, infringement of local regulation, or other pecuniary loss) arising out of the use of or inability to use this SOFTWARE product and/or the components distributed with this SOFTWARE product, even if TalariaX Pte Ltd and SendQuick Pte Ltd have been advised of the possibility of such damages, to the maximum extent permitted by law.

4. Other restrictions

You may not rent or lease the SOFTWARE, but you may transfer your rights under this license agreement on a permanent basis if you transfer all copies of the SOFTWARE with the server hardware and all written material, and if the recipient agrees to the terms of this agreement.

You may not reverse engineer, de-compile or disassemble the SOFTWARE and any such acts and intent is considered a violation of copyright law in Singapore and your respective countries.

Limited warranty

TalariaX Pte Ltd and SendQuick Pte Ltd warrant that the SOFTWARE will perform substantially in accordance with the accompanying product manual(s) or the online manual for a period of 365 days from the purchase date. This limited warranty period also applies to the hardware and the GSM modem. TalariaX and SendQuick reserve the right to amend the limited warranty period without prior notice.

Customer remedies

TalariaX Pte Ltd and SendQuick Pte Ltd entire liability and your exclusive remedy shall be, at TalariaX Pte Ltd's and SendQuick Pte Ltd's option, either

- a return of the price paid or
- repair or replacement of the SOFTWARE that does not meet the limited warranty and which is returned with a copy of your receipt

The limited warranty is void if failure of the SOFTWARE has resulted from accident, abuse or misapplication by the user/licensee. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period but at least for 30 days.

No other warranties

To the maximum extent permitted by applicable law, TalariaX Pte Ltd and SendQuick Pte Ltd disclaims all other warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to the SOFTWARE, hardware, the accompanying product manual(s) and written materials. The limited warranty contained herein gives you specific legal rights.

No liability for consequential damage

To the maximum extent permitted by applicable law, TalariaX Pte Ltd and SendQuick Pte Ltd and its suppliers shall not be liable for any other damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, infringement of local regulation, or other pecuniary loss) arising out of the use of or inability to use this SOFTWARE PRODUCT, even if TalariaX Pte Ltd and SendQuick Pte Ltd have been advised of the possibility of such damages. In any case, TalariaX Pte Ltd's and SendQuick Pte Ltd's entire liability under any provisions of this agreement shall be limited to the amount actually paid by you for this SOFTWARE.

TalariaX and SendQuick cannot guarantee that messages sent by using TalariaX's and SendQuick's SOFTWARE PRODUCTS for wireless (SMS) messaging reach their addressees. Neither can TalariaX and SendQuick guarantee that the SOFTWARE PRODUCT receives all messages through the used mobile equipment they have been sent to.

TalariaX and SendQuick are not liable for any consequential damages arising from the fact that messages tried to send by SendQuick Server products do not reach their target addressees (mobile

phones, pagers) or that messages sent to the mobile equipment used with the SOFTWARE PRODUCT will be recognized and read by the SOFTWARE PRODUCT.

For any clarifications, please contact:**SendQuick Pte Ltd**

76 Playfair Road

#08-05 LHK2

Singapore 367996

Tel: 65 – 62802881

Fax: 65 – 62806882

E-mail: info@sendquick.comWeb: www.sendquick.com

Table of Contents

1.0	Introduction.....	6
2.0	Set-Up & Configuration.....	6
2.1	<i>Login Procedures.....</i>	<i>6</i>
2.2	<i>Report.....</i>	<i>7</i>
2.3	<i>Send SMS.....</i>	<i>15</i>
2.4	<i>SMS Transaction.....</i>	<i>16</i>
2.5	<i>User Management.....</i>	<i>19</i>
2.6	<i>Device Profile.....</i>	<i>25</i>
2.7	<i>Network Monitor.....</i>	<i>27</i>
2.8	<i>Message Filter.....</i>	<i>40</i>
2.9	<i>Adhoc Scanning.....</i>	<i>55</i>
2.10	<i>Admin.....</i>	<i>57</i>
2.11	<i>Configuration Template.....</i>	<i>62</i>
3.0	References.....	65
3.1	<i>SMS Check Template.....</i>	<i>65</i>
3.2	<i>SMS Acknowledgement Templates.....</i>	<i>67</i>
3.3	<i>Windows Server WMI Configuration.....</i>	<i>68</i>

SendQuick Avera User Manual

1.0 Introduction

Welcome to SendQuick Avera User Manual. This document is prepared for the administrator user, as a guide for configuring the SendQuick Avera for monitoring servers and sending alerts.

2.0 Set-Up & Configuration

2.1 Login Procedures

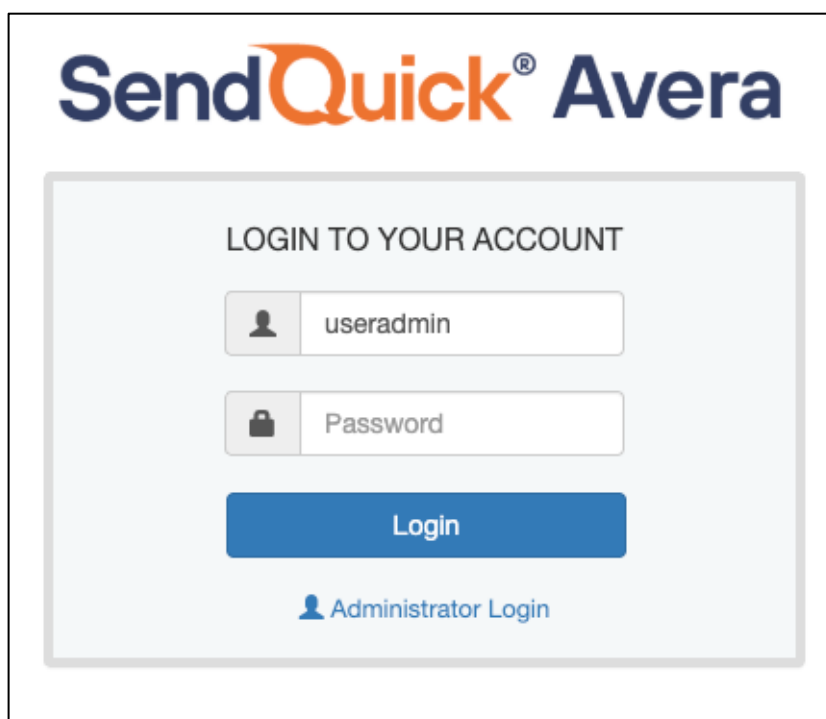


Figure 2-1: Login Page

Use a web browser to access SendQuick Avera's server IP, you will be redirected to Avera's login page.

URL: [http\[s\]://\[Avera's server IP\]/avera](http[s]://[Avera's server IP]/avera)

Enter the default Administrator's Log-in Name and Password to access the system. The default username and password can be found in the Your Password envelope. For further assistance please contact support@sendquick.com via email.

You can change the password through the "Change Password" link at top right corner

after logging-in.

2.1.1 Login Types

There are four (4) types of user accounts:

1. Super Admin
2. Admin
3. Operator
4. User

Super Admin and Admin have full access rights to every features. The only difference is Super Admin 'useradmin' account is the default admin account and cannot be deleted.

Operator has all access rights except the 'Admin' settings, checking server log and network tools.

User has view-only access rights to monitoring rules configuration. User can login to update personal details, acknowledge case, send SMS and view reports.

2.2 Report

2.2.1 Dashboard

This page will display summaries for all monitored rules. User can enter report period (Today, Yesterday, Last 7 Days, Last 30 Days, This Week, Last Week or By Date Range) and total records (1 to 20) to generate summary report. This page will auto-refresh every 5 minutes.

The screenshot shows the SendQuick Avera dashboard for a user named 'useradmin'. The dashboard is titled 'Report / Dashboard' and features a sidebar with navigation options: Report, Dashboard (selected), Summary, Server Availability, Alert, Ping Response Time, Disk Utilization, CPU Utilization, Memory Utilization, Send SMS, SMS Transaction, User Management, Device Profile, Network Monitor, Message Filter, Adhoc Scanning, Admin, and Configuration Template. The main content area displays a report generation form with 'Period' set to 'Today' and 'Total Record' set to '5'. A 'Generate Report' button is visible. Below the form, the dashboard shows data for 'Today (18-Jun-2025)'. There are six summary cards: 'Top 5 Server Availability', 'Recent Alerts' (with a table header: No, Rule Name, Rule Type, Message, Alert Time), 'Top 5 Disk Utilization', 'Top 5 CPU Utilization', 'Top 5 Memory Utilization', and 'Top 5 Slowest Ping Response Time'.

Figure 2-2: Dashboard

2.2.2 Summary

Users can generate summary report for specific servers or rules in this page. Before generating, they can specify the report period and the server or rule to generate report. Report can be exported as PDF or Excel format.

2.2.2.1 Server Summary

Show server availability based on the ICMP Ping results, Latest Server Utilization if rules are configured, all monitoring rules status and recent alerts.

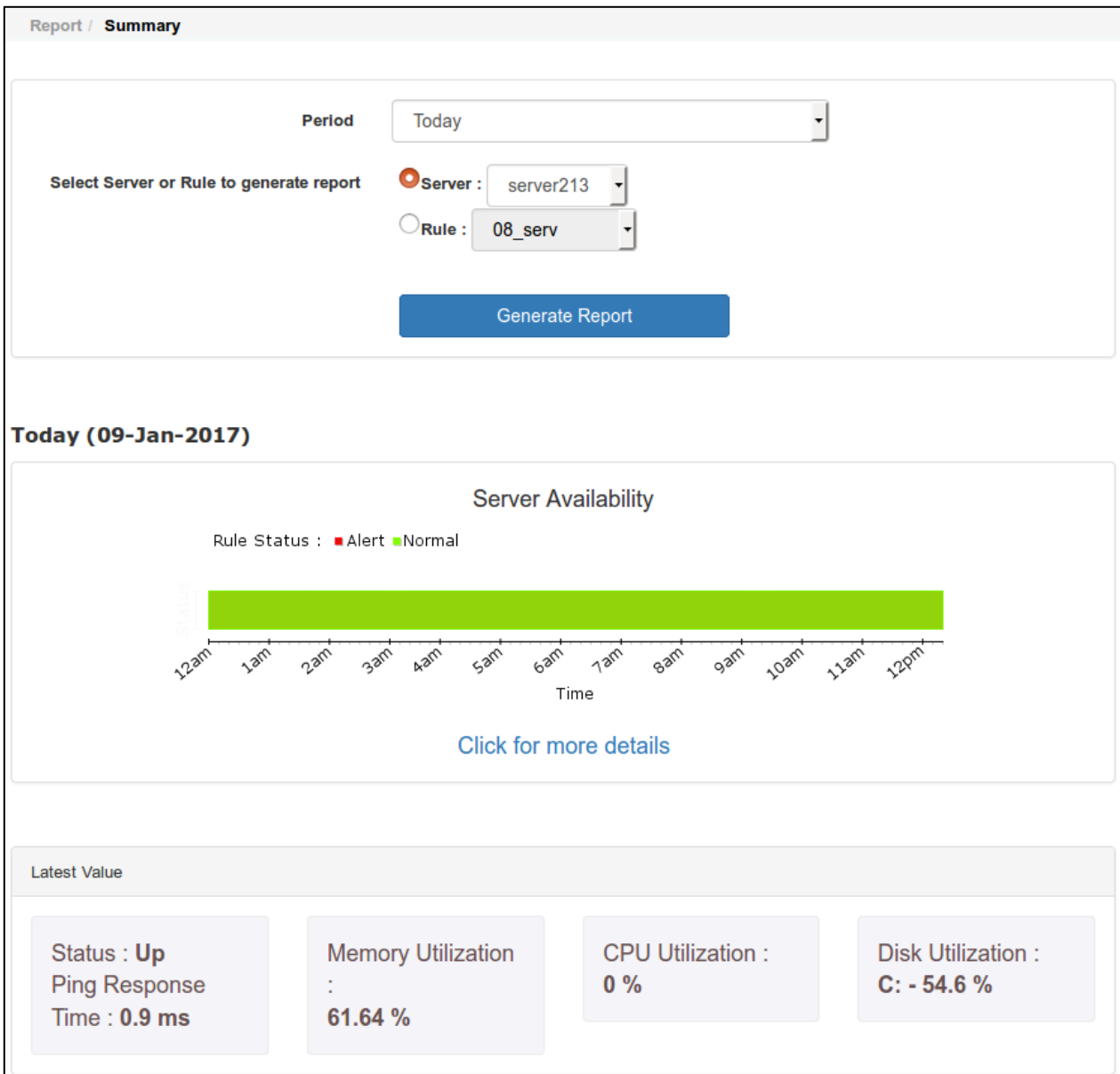


Figure 2-3: Sample Server Summary Report

To check server health status, please create the following monitoring rules.

ICMP	Server availability and Ping Response Time based on ping result of the server IP.
CPU Check	CPU usage of the server
Disk Check	Disk utilization of any particular partition in server. Create several disk usage rules to monitor different partition.
Memory Check	Memory usage of the server

Adhoc Scanning - Display all rules created under this server. To view more details about a rule, navigate to the corresponding rule category under Network Monitor in the navigation bar.

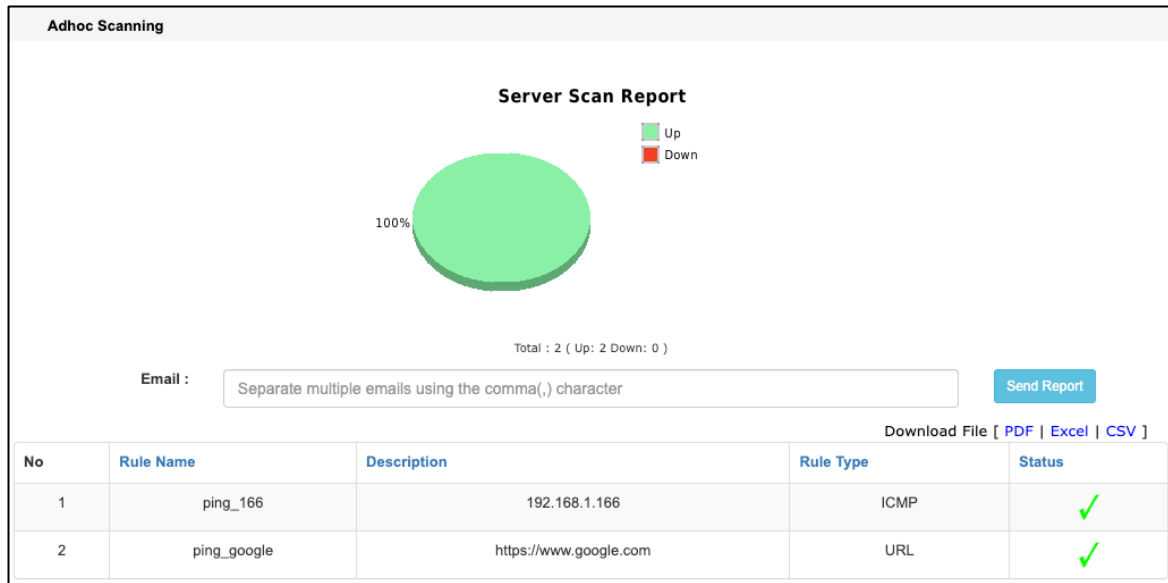


Figure 2-4: Sample Monitoring Rules

Recent alert - Recent alerts from all the rules under this server.

2.2.2.2 Rule Summary

Recent Alerts				
No	Rule Name	Rule Type	Message	Alert Time
No Alerts				

Figure 2-5: Recent Alert List

The chart will display rules status (Up or Alert) and line graph of CPU, Disk and Memory usage. Report can be exported as PDF or Excel format.

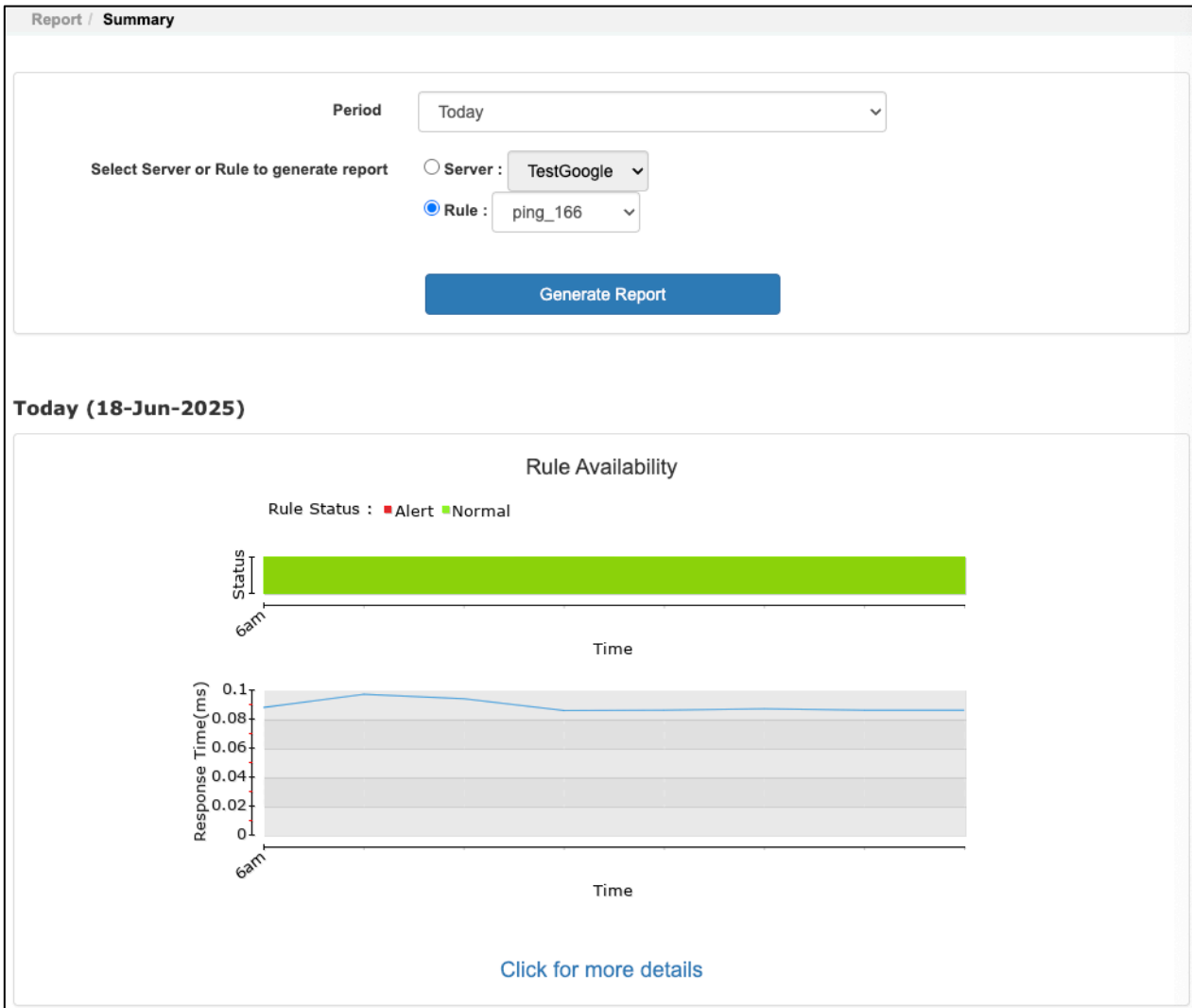


Figure 2-6: Report Summary – Rule

Recent alert - Recent alerts from all the rules under this server.

Download File [[PDF](#) | [Excel](#)]

Recent Alerts				
No	Rule Name	Rule Type	Message	Alert Time
No Records.				

Figure 2-7: Report Summary Recent Alerts

2.2.3 Server Availability

Show server or rule availability within the selected report period.

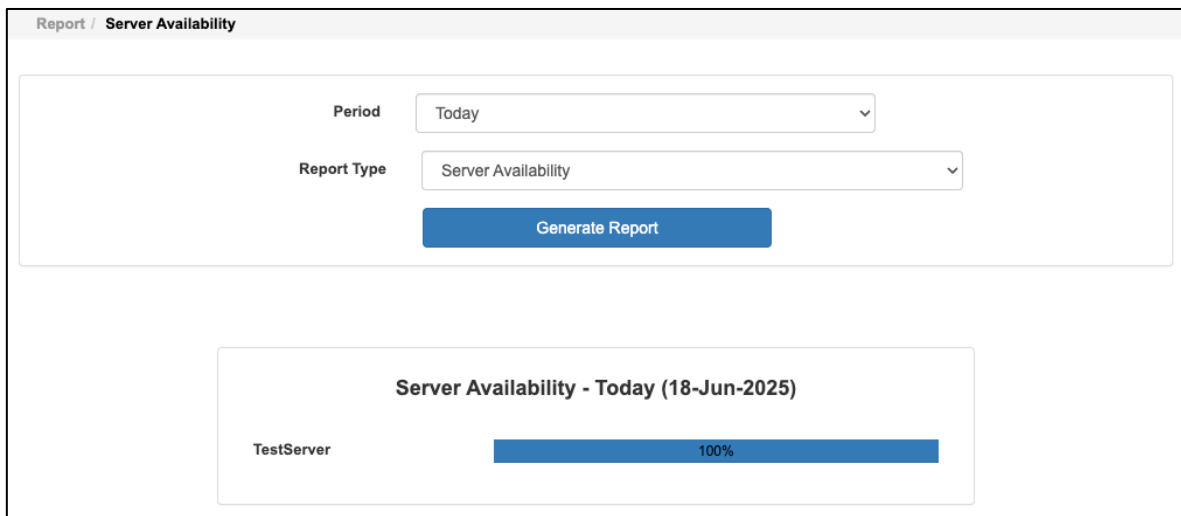


Figure 2-8: Server Availability Overview

2.2.4 Alert

Show all alerts within the selected report period.

The screenshot displays the 'Alert Logs' interface. At the top, there is a header 'Report / Alert'. Below this, there is a 'Period' dropdown menu set to 'Today' and a blue 'Generate Report' button. Below the button, there is a section titled 'Recent Alerts'. This section includes a 'Show' dropdown set to '10' entries and a 'Search:' input field. Below this is a table with the following columns: 'No', 'Rule Name', 'Rule Type', 'Message', and 'Alert Time'. The table contains one entry:

No	Rule Name	Rule Type	Message	Alert Time
1	ping_google	URL	ID:M1,8.8.8.8:ping_google is not reachable.	2025-06-18 06:12:06

Below the table, it says 'Showing 1 to 1 of Total 1 entries'. At the bottom right, there are navigation buttons: 'Previous', '1', and 'Next'.

Figure 2-9: Alert Logs

2.2.5 Ping Response Time

Show all active ICMP rules and the Ping Response Time within the searched period.

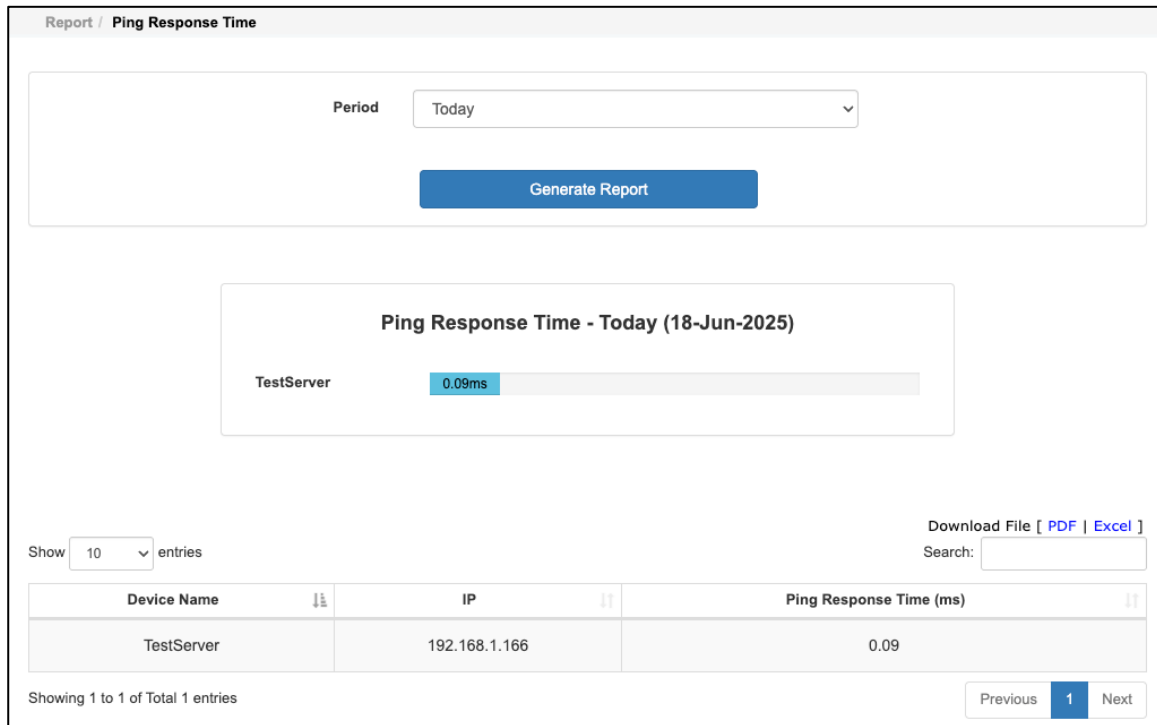


Figure 2-10: Ping Response Time

2.2.6 Disk Utilization

Show all the Disk Utilization within the searched period.

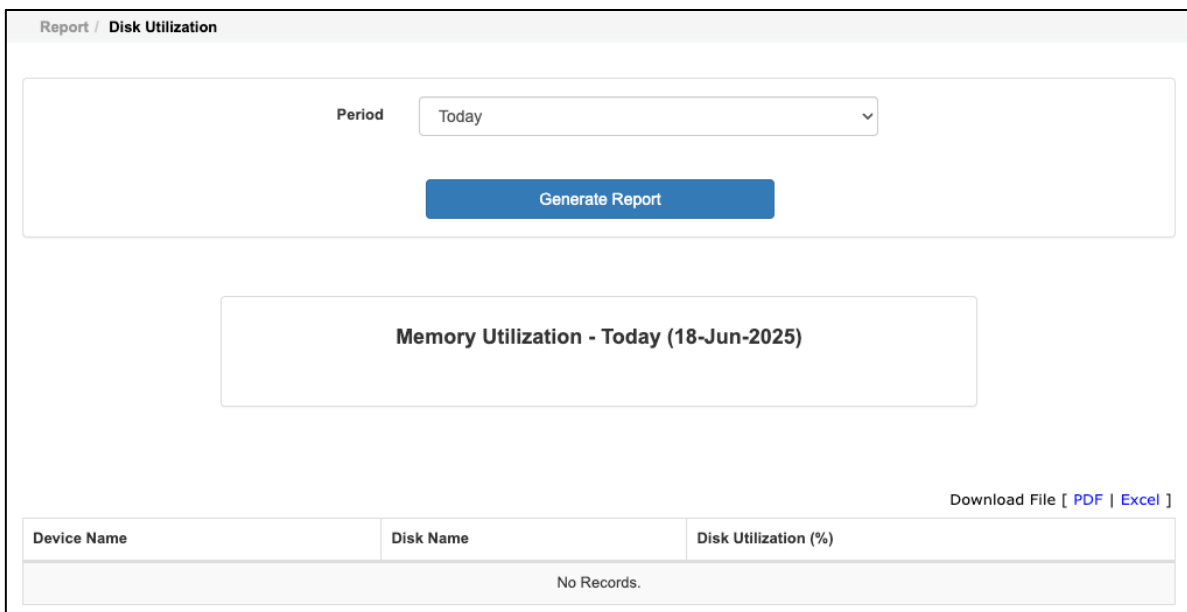


Figure 2-11: Disk Utilization

2.2.7 CPU Utilization

Show all the CPU Utilization within the searched period.

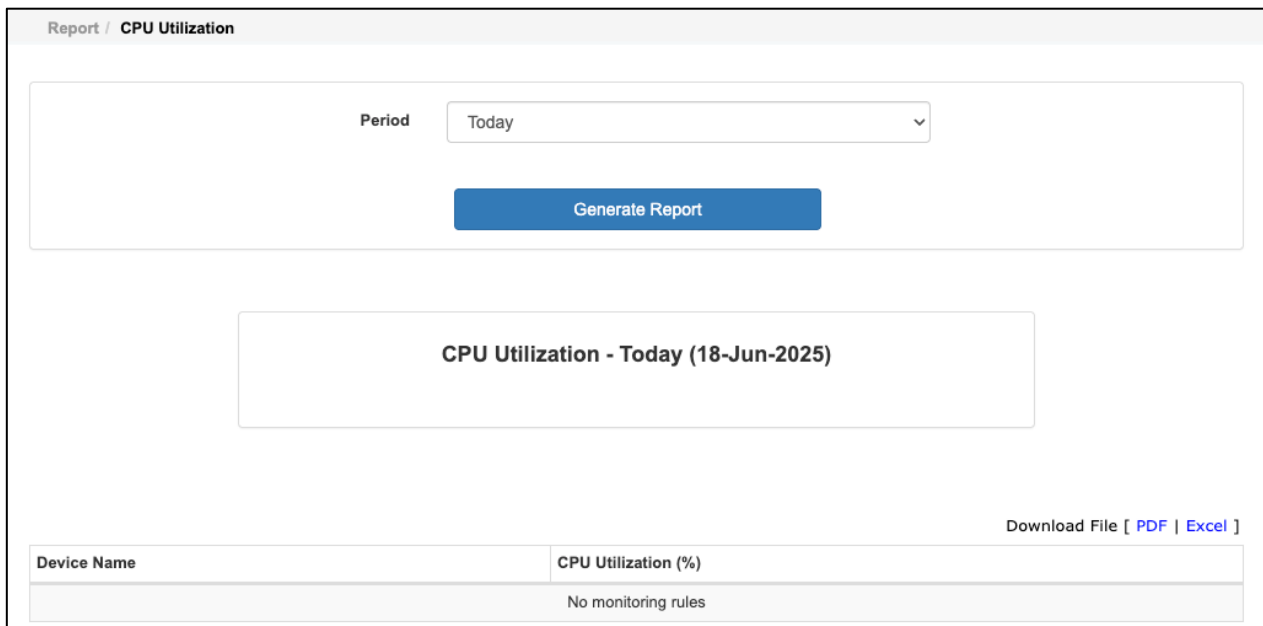


Figure 2-12: CPU Utilization

2.2.8 Memory Utilization

Show all the Memory Utilization within the searched period.

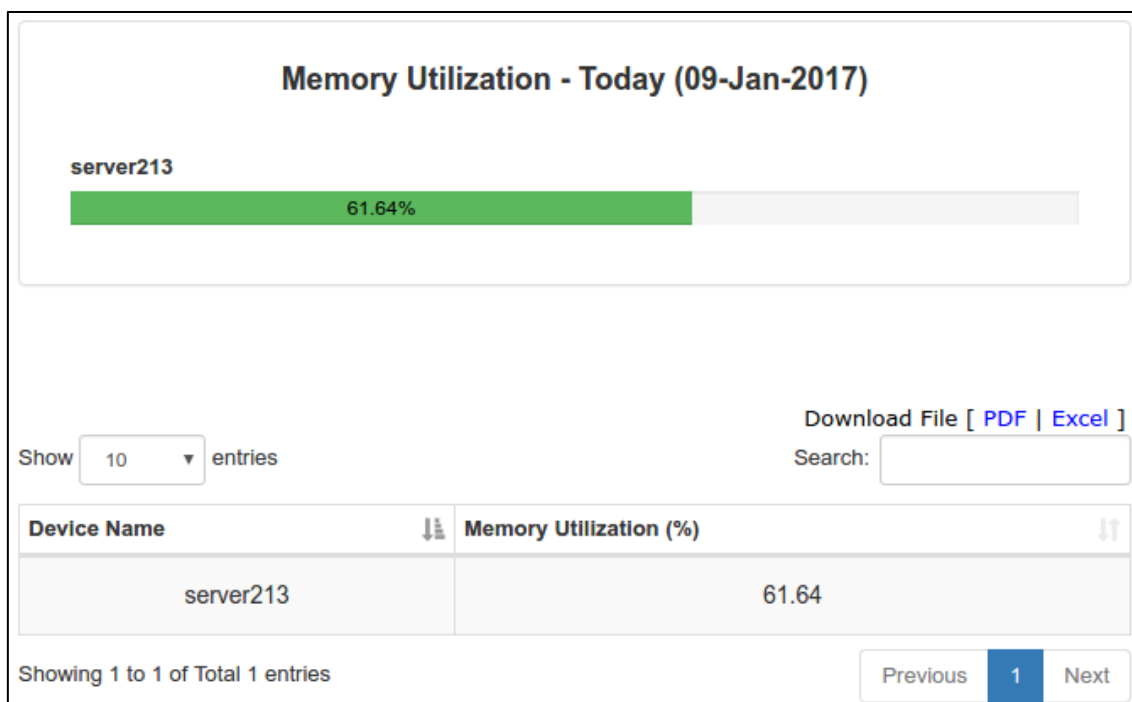


Figure 2-13: Memory Utilization

2.3 Send SMS

Send test messages or broadcast alert messages to users.

2.3.1 Send SMS

The screenshot shows the 'Send SMS' configuration window. It has a title bar 'Send SMS / Send SMS' and a main heading 'Send SMS'. The form contains the following elements:

- Enter The Mobile Number(s) In The Textbox :** A text area containing 'Operator 1', 'User 1', and '91234567'. A blue button 'Select from Address Book' is below it. A note says 'Separate Each Entry With A New Line'.
- Priority SMS :** A dropdown menu showing '5'.
- Enter The Message Text In The Textbox :** A text area containing 'Test Message 1'. A blue button 'Select from Message Template' is below it. A note says 'Please note the case id will be auto-generated and appended in the beginning of the message text entered. Current SMS will be assigned with <ID:2>'.
- Character Set :** A dropdown menu showing 'ASCII/Text'.
- At the bottom are 'Send' and 'Cancel' buttons.

Figure 2-14: Send SMS Configuration

Mobile numbers	Mobile number can be selected from address book or manually inserted in this text box with one number for each line.
Priority SMS	1 to 9. Set the priority for these SMS. 1 is the highest priority.
Message Text	Compose the text message or select the predefined messages from message template. The character count and number of SMS messages are shown below the message box.
Character Set	ASCII – Normal English Message UTF8 – Non-English Text Message

2.3.2 Message Template

Create/Edit/Delete text messages as template for future use. Having message templates allow user to easily retrieve the message, perform some simple edit (or no editing) and use them to send SMS.

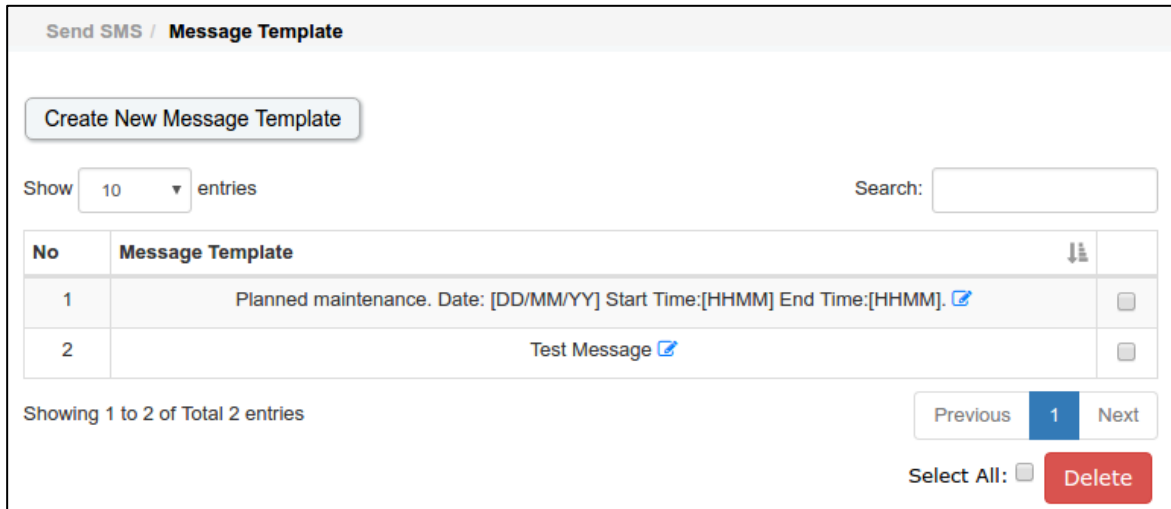


Figure 2-15: Message Templates

2.4 SMS Transaction

User can check all the transaction cases and the report.

2.4.1 SMS Broadcast

All transaction of SMS Broadcast ([Refer to 2.3.1](#)) can be searched and displayed in this page. Every SMS Broadcast has a unique [Case ID], which is prefixed to the text message. Recipient can reply 'ACK <case_id>' to simply acknowledge receipt of this SMS. All acknowledgement records will be logged under 'ACK' column.

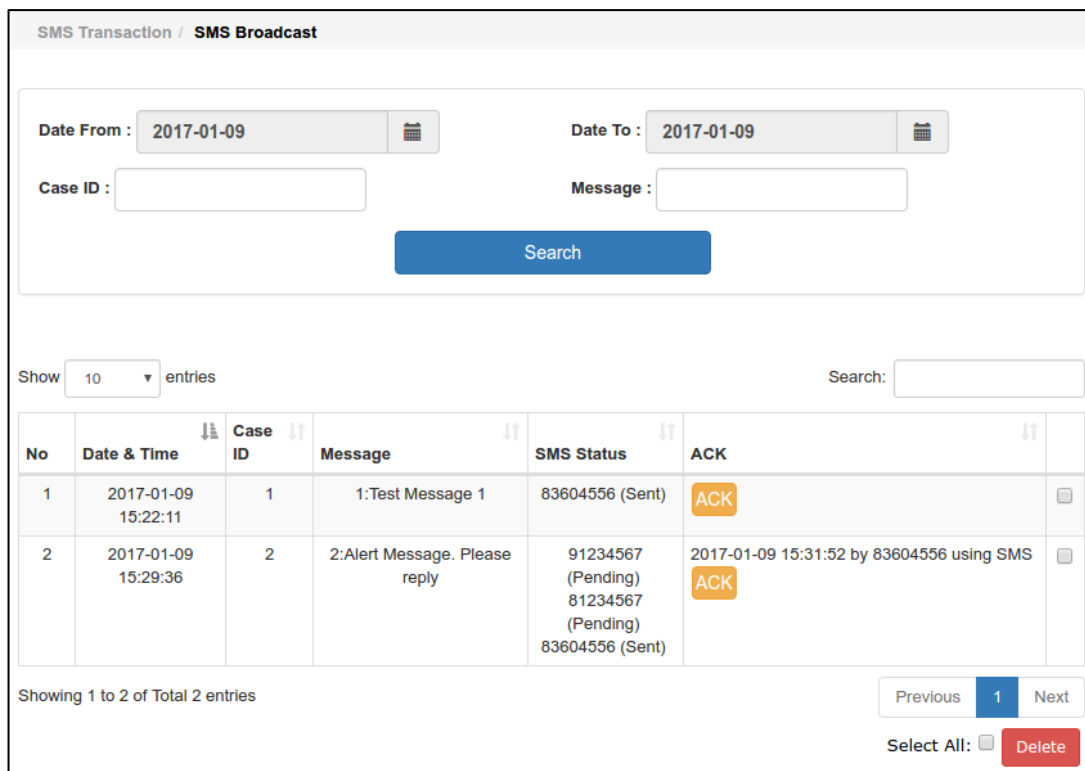


Figure 2-16: SMS Broadcast

2.4.2 SMS Check

All incoming SMS Check request and the response message will be displayed here. User can click on 'SMS Check Template' to view the template of SMS request. ([Refer to 3.1 SMS Check Template](#))

SMS Transaction / SMS Check

Date From : 2017-01-09 Date To : 2017-01-09

Request Content : From Mobile :

Show entries

No	Date & Time	Request Content	From Mobile	Return Message	
1	2017-01-09 15:45:50	ping 192.168.1.1	83604556	ICMP Ping to 192.168.1.1 -> SUCCESS	<input type="checkbox"/>
2	2017-01-09 15:46:10	telnet 192.168.1.105 80	83604556	TELNET to IP:192.168.1.105 PORT:80 -> SUCCESS	<input type="checkbox"/>

Showing 1 to 2 of Total 2 entries

Select All:

Figure 2-17: SMS Check

2.4.3 Network Monitor

All transaction of Network Monitoring alerts ([Refer to 2.7](#)) can be searched and displayed in this page. User can reply 'ACK <case_id>' to simply acknowledge receipt of this SMS or stop escalation alerts. Reply 'RES <case_id> <log>' is used to stop escalation alerts and save a resolved log to this case. All ACK and RES records will be logged.

The screenshot displays the 'Network Monitor' interface. At the top, there are search filters for 'Date From' and 'Date To' (both set to 2017-01-09), 'Case ID', 'Rule Name', 'Rule Type' (set to 'All'), and 'Process Status' (set to 'All'). A blue 'Search' button is located below these filters. Below the search filters, there is a 'Show 10 entries' dropdown and a 'Search:' input field. The main content is a table with the following columns: No, Date & Time, Case ID, Rule Name, Rule Type, Process Status, Sent SMS, ACK, and RES. The table contains one entry with the following details: No: 1, Date & Time: 2017-01-09 15:42:34, Case ID: M78, Rule Name: ping227, Rule Type: ICMP (Once), Process Status: End, Sent SMS: 83604556, ACK: 2017-01-09 15:43:59 by 83604556 using SMS (with an orange ACK button), and RES: 2017-01-09 15:44:45 by 83604556 using SMS Log:resolved on 3:44pm (with a blue RES button). Below the table, there is a 'Showing 1 to 1 of Total 1 entries' indicator, a pagination control with 'Previous', '1', and 'Next' buttons, and a 'Select All: [checkbox] Delete' button.

No	Date & Time	Case ID	Rule Name	Rule Type	Process Status	Sent SMS	ACK	RES
1	2017-01-09 15:42:34	M78	ping227	ICMP (Once)	End	83604556	2017-01-09 15:43:59 by 83604556 using SMS ACK	2017-01-09 15:44:45 by 83604556 using SMS Log:resolved on 3:44pm RES

Figure 2-18: Network Monitor

2.4.4 Message Filter

All transaction of Message Filtering alerts ([Refer to 2.8](#)) can be searched and displayed in this page. User can reply 'ACK <case_id>' to simply acknowledge receipt of this SMS or stop escalation alerts. All ACK records will be logged.

SMS Transaction / Message Filter

Date From : 2017-01-09

Date To : 2017-01-09

Case ID :

Alert Message :

Type : All

Process Status : All

Show 10 entries Search:

No	Date & Time	Case ID	Alert Message	Type	Process Status	Sent	ACK	
1	2017-01-09 15:49:39	F2	nms@talariax.com:application 1 is down:please check	Mail Message Filter (Escalation & Report)	End	83604556	<input type="button" value="ACK"/>	<input type="checkbox"/>

Showing 1 to 1 of Total 1 entries Previous Next

Select All:

Figure 2-19: Message Filter

2.5 User Management

2.5.1 User Management

List all the users of SendQuick Avera.

User Management / User Management

Show 10 entries Search:

No	Login ID	User Name	Mobile	Email	Designation	Group Name	Shift Name	User Type	Suspend	
1	admin <input type="checkbox"/>	Admin A	--	admin@talariax.com			--	Admin	No	<input type="checkbox"/>
2	operator1 <input type="checkbox"/>	Operator 1	--	operator1@talariax.com			--	Operator	No	<input type="checkbox"/>
3	user1 <input type="checkbox"/>	User 1	--	user1@talariax.com			--	User	No	<input type="checkbox"/>

Showing 1 to 3 of Total 3 entries Previous Next

Select All:

Figure 2-20: User Management

Create or Update User Accounts

User Management / User Management / New User

Create New User

User Name : Name of the user

Login ID : User ID and password to login. Login ID is unique.

Login Password :

Confirm Password :

Mobile : Mobile number to receive SMS alert or send request

Email : Email address to receive alert

User Type : 3 types of user account.

- **Admin** - Have access rights to all
- **Operator** - Have all access rights except admin settings
- **User** - Edit his/her own personal details, view rules, adhoc scan rules and generate report.

Designation : User's designation

Group Name : Assign a new or existing group to user.

Suspend : Enable to suspend user from receiving alerts

On Leave Date : Click to highlight the date, which user is on leave and disable alerts for user.

June 2025						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Customize Shift : This indicator used to personalize the shift for each users. If Customize Shift is set to No, whenever the Primary Shift's info changed, system will auto update the user's shift info who had assigned to the same shift. Otherwise, system will not update the user's shift info which had personalized.

Shift Name : Assign shift to user. User without any shift will not receive alerts. Shift date and time will be shown below once shift name is selected. Shift is customizable for each user.

MIM Subscriptions : -

Alert Profile :

New Alert Profile

Figure 2-21: Create New User

User Name	Name of the user
Login ID & Password	User ID and password to login. Login ID is unique.
Mobile Number	Mobile number to receive SMS alert or send SMS Check requests.
Email	Email address to receive alert
Designation	User's designation
Group Name	Assign a new or existing group to user. Multiple groups can be selected. Group can be created under User Group Management. (Refer to 2.5.2 User Groups)
User Type	[Admin Operator User] Different access rights of user. (Refer to 2.1.1 Login Types)
Suspend	Enable or Disable user's suspend mode. Suspended user account will not receive any alert.
On Leave Date	Click and highlight the date when user is on leave and ignore alerts to user on that day.
Customize Shift	Customize a standard shift for user.
Shift Name	Select shift for user. Note that user without a shift will not receive any alerts. Shift can be created under shift management. (Refer to 2.5.3 Shift Management)
Specific Date	Select specific date range for this user. Useful for temporary and contract staff, which will receive alerts during the specific period only.

2.5.2 User Groups

List all user groups and member users.

The screenshot shows the 'User Management / User Groups' interface. At the top, there is a 'Create New Group' button. Below it, there is a 'Show 10 entries' dropdown and a search box. The main content is a table with the following data:

No	Group Name	Group Members	User Name & Mobile
1	IT	2	Operator 1 (81234567) User 1 (91234567)

At the bottom of the table, it says 'Showing 1 to 1 of Total 1 entries'. There are navigation buttons: 'Previous', '1', and 'Next'. Below that, there is a 'Select All' checkbox and a 'Delete' button.

Figure 2-22: User Groups

Create or Update user group

Figure 2-23: Edit User Group

Group Name	Unique group name
Users	Select user from address book and assign to this group. Each user can be assigned to multiple groups.

2.5.3 Shift Management

Show all shifts for receiving alerts from Avera.

Figure 2-24: Shift Management

Create or Update Shift

Shift Name :

24 x 7

Assign shift to user. User without any shift will not receive alerts. Shift date and time will be shown below once shift name is selected. Shift is customizable for each user.

Select Day :

Mon 0000-2359

Tue 0000-2359

Wed 0000-2359

Thu 0000-2359

Fri 0000-2359

Sat 0000-2359

Sun 0000-2359

Day of week to receive alert

- Time of each day to receive alert.
- In 24-hr format, eg. 0000-2359,1200-1900,0800-1800
- Multiple time slots should be separated by comma (,)

Specific Date :


No

Highlight specific date to receive alert.

Figure 2-25: Edit Shift

Shift Name	Unique shift name
Day of week	Select day of week to receive alert
Time of alert	Time of each day to receive alert. In 24-hr format, eg. 0000-2359,1200-1900,0800-1800 Multiple time slots should be separated by comma (,)
Specific Date	Highlight specific date to receive alert

Assign Shift

Click on the  button to assign shift to users.

Select User(s) for shift : 24 x 7
✕

Show 10 entries Search:

	Login ID	User Name	Current Shift	Customize Shift	Group Name
<input type="checkbox"/>	admin	Admin A			
<input checked="" type="checkbox"/>	operator1	Operator 1			IT
<input type="checkbox"/>	user1	User 1			IT

Showing 1 to 3 of Total 3 entries Previous 1 Next

Select All Close Assign

View Shift

Click on the 👁 button to view the shift members.

Shift Name : 24 x 7
✕

Show 10 entries Search:

No	Login ID	User Name	Group Name
1	operator1	Operator 1	IT

Showing 1 to 1 of Total 1 entries Previous 1 Next

Close

2.5.4 Duty Roster

This feature enable user to check who is on duty on a specific date.

User Management / Duty Roster

On Duty Date :

Search Rule Name :

Search User :

Duty Roster

Show entries Search:

No	User Name	User Type	Shift Name	On Duty Date	Rule List
1	Operator 1	Operator	24 x 7	0000-2359	213_dns

Showing 1 to 1 of Total 1 entries Previous **1** Next

Figure 2-26: Duty Roster

2.6 Device Profile

This page shows all the monitoring rules configured in Avera and its status, whether it's up, down or disabled.

Device Profile

● Up , ● Down , ● Disabled

Show entries Search:

No	Device Name	IP	Rule Status							Enable			
			ICMP	TCP	URL	Service	Process	CPU	Disk			Memory	
1	server213	192.168.1.213	● (1)			● (1)			● (1)	● (1)	● (1)	Y	<input type="checkbox"/>
2	testmpm	192.168.1.105	● (1)									Y	<input type="checkbox"/>
3	win12_vm	192.168.1.227	● (1)			● (1)						Y	<input type="checkbox"/>

Showing 1 to 3 of Total 3 entries Previous **1** Next

Select All:

Figure 2-27: Device Profiles

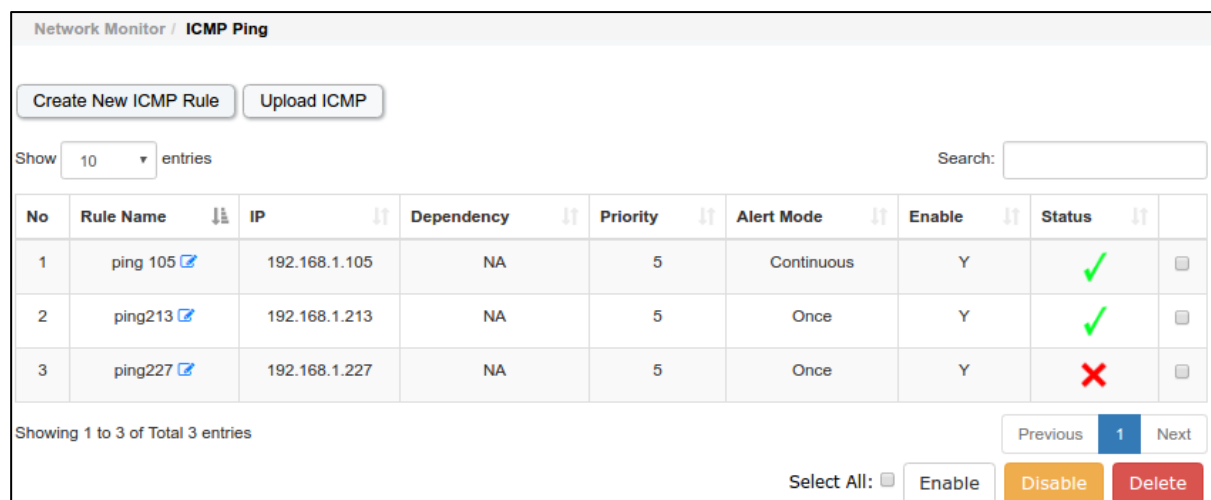
2.6.1 Create or Update device profile

Server IP	Server's IP Address
Server Name	Unique name for each device
Server Description	Short description for device
Server Location	Short description of server's location
Server Platform	[Redhat SUSE Windows 2003 Server Windows 2008 Server Windows 2012 Server] Select the server's operating system.
Login Name	Server's login name. This is required for some monitoring types like windows service check, windows process check, CPU, disk and memory.
Login Password	For windows server, this is required for WMI remote access to gather server's information and remote control (restart service, restart server and shutdown server). For Linux server, this is required only if the 'SSH By' is set to password.
SSH By	[Password Key] This is only available for Linux server. <ul style="list-style-type: none"> • Password: SSH login via login name and password as configured above. • Key: SSH login via ssh key. Users need to add Avera's key to server's authorized key file.
Test Connection	Click to check server connection with the login credential provided.
Authorized Mobile & Authorized Group	Authorized mobile numbers & groups to send in SMS and query this server's data. Refer to 3.1 SMS Check Template

2.7 Network Monitor

SendQuick Avera is able to monitor different types of rules, which are ICMP, TCP, URL, Windows Service and Process, CPU, Disk and Memory. Every rule is tied to a server, which is configured under Device Profile ([Refer to 2.6 Device Profile](#)).

2.7.1 ICMP Ping



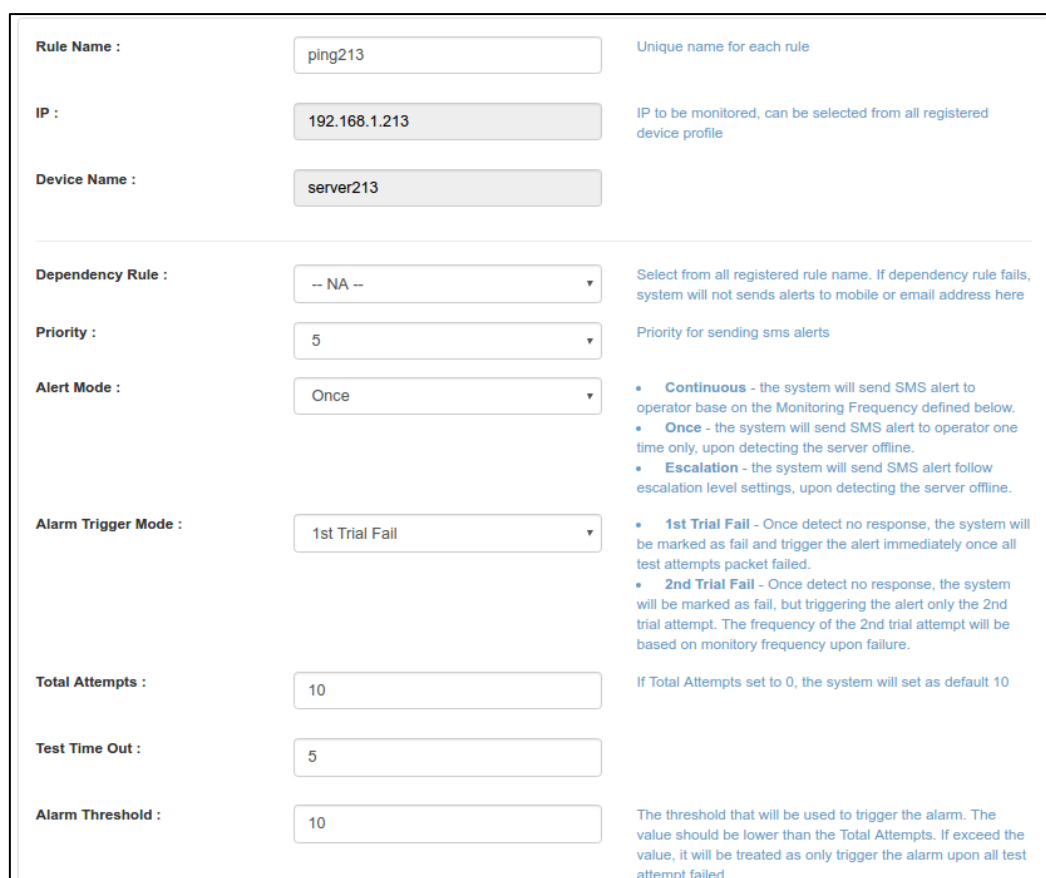
The screenshot shows the 'Network Monitor / ICMP Ping' interface. At the top, there are buttons for 'Create New ICMP Rule' and 'Upload ICMP'. Below these, there is a 'Show' dropdown set to '10' entries and a search box. The main part of the interface is a table with the following columns: No, Rule Name, IP, Dependency, Priority, Alert Mode, Enable, and Status. There are three rows of data:

No	Rule Name	IP	Dependency	Priority	Alert Mode	Enable	Status
1	ping 105	192.168.1.105	NA	5	Continuous	Y	✓
2	ping213	192.168.1.213	NA	5	Once	Y	✓
3	ping227	192.168.1.227	NA	5	Once	Y	✗

At the bottom of the table, it says 'Showing 1 to 3 of Total 3 entries'. There are navigation buttons for 'Previous', '1', and 'Next'. Below the table, there is a 'Select All:' checkbox and three buttons: 'Enable', 'Disable', and 'Delete'.

Figure 2-28: ICMP Ping

2.7.1.1 Create or Update network monitoring rules



The screenshot shows the 'Update ICMP Ping' configuration form. It contains the following fields and options:

- Rule Name :** ping213 (Unique name for each rule)
- IP :** 192.168.1.213 (IP to be monitored, can be selected from all registered device profile)
- Device Name :** server213
- Dependency Rule :** -- NA -- (Select from all registered rule name. If dependency rule fails, system will not sends alerts to mobile or email address here)
- Priority :** 5 (Priority for sending sms alerts)
- Alert Mode :** Once
 - Continuous** - the system will send SMS alert to operator base on the Monitoring Frequency defined below.
 - Once** - the system will send SMS alert to operator one time only, upon detecting the server offline.
 - Escalation** - the system will send SMS alert follow escalation level settings, upon detecting the server offline.
- Alarm Trigger Mode :** 1st Trial Fail
 - 1st Trial Fail** - Once detect no response, the system will be marked as fail and trigger the alert immediately once all test attempts packet failed.
 - 2nd Trial Fail** - Once detect no response, the system will be marked as fail, but triggering the alert only the 2nd trial attempt. The frequency of the 2nd trial attempt will be based on monitoring frequency upon failure.
- Total Attempts :** 10 (If Total Attempts set to 0, the system will set as default 10)
- Test Time Out :** 5
- Alarm Threshold :** 10 (The threshold that will be used to trigger the alarm. The value should be lower than the Total Attempts. If exceed the value, it will be treated as only trigger the alarm upon all test attempt failed.)

Figure 2-29: Update ICMP Ping

Monitoring Frequency :	<input type="text" value="10"/>	<ul style="list-style-type: none"> The frequency (interval) between each Attempt test in minutes. If set to 0, the system will disable the monitoring. It is not recommended to set lower than 5 minutes for actual deployment of the system, as Multiple Windows Service Check will generate quite a lot of network traffic
Monitoring Frequency : (Upon Failure)	<input type="text" value="5"/>	<ul style="list-style-type: none"> The frequency (interval) between each Attempt test when a test failure had been detected. Customer may prefer to have a smaller value (in minutes) to allow a more regular (frequent) checking when there is a failure. If set to 0, the system will use the value defined in the Monitoring Frequency.
Server Status Alert :	<input type="text" value="Disable"/>	<ul style="list-style-type: none"> Send an alert message to the administrator, to indicate that the sendQuick server is still functioning. This can be configured to be on a certain time of the day (time in HH:MM) or in hourly manner(00-59 minutes)
Server Status Alert Mode :	<input type="text" value="Both"/>	
Server Status Alert Time :	<input type="text" value="-HH-"/> <input type="text" value="-MM-"/>	<ul style="list-style-type: none"> HH - Hour (00 - 23) MM - Minute (00 - 59)

Figure 2-30: Update ICMP Ping (2)

Rule Name	Unique name for each rule
IP Address	IP to be monitored, can be selected from all registered device profile
Device Name	Server's name of this IP. If this is a new IP, assign a unique name for this server and new device profile will be created.
Dependency Rule	Select from all registered rule name. If dependency rule fails, system will not send alerts to mobile or email address here
Priority	Priority for sending SMS alerts
Alert Mode	<p>Continuous - the system will send SMS alert to operator base on the Monitoring Frequency defined below.</p> <p>Once - the system will send SMS alert to operator one time only, upon detecting the rule down.</p> <p>Escalation - the system will send SMS alert follow escalation level settings, upon detecting the rule down.</p>
Alarm Trigger Mode	<p>1st Trial Fail - Once detect no response, the system will be marked as fail and trigger the alert immediately once all test ping packet failed.</p> <p>2nd Trial Fail - Once detect no response, the system will be marked as fail but triggering the alert only the 2nd trial attempt. The frequency of the 2nd trial attempt will be based on monitory frequency upon failure.</p>
Total Attempts	If set to 0, the system will set as default 10
Test Time Out	Timeout for each Ping Test, in seconds. If Ping Timeout is set to 0, the system will set as default 5 seconds.
Alarm Threshold	The threshold that will be used to trigger the alarm. The value should be lower than the Total Test Ping. If exceed the value, it will be treated as only trigger the alarm upon all test ping

	failed.
Monitoring Frequency	The frequency (interval) between each Ping test in minutes. If set to 0, the system will disable the monitoring. It is not recommended to set lower than 5 minutes for actual deployment of the system, as ICMP ping generate quite a lot of network traffic
Monitoring Frequency (Upon Failure)	The frequency (interval) between each Ping test when a test failure had been detected. Customer may prefer to have a smaller value (in minutes) to allow a more regular (frequent) checking when there is a failure. If set to 0, the system will use the value defined in the Monitoring Frequency.
Server Status Alert	Send an alert message to the administrator, to indicate that the SendQuick server is still functioning or down. This can be configured to be on a certain time of the day (time in HH:MM) or in hourly manner (00-59 minutes)
Server Status Alert Mode	[SMS Email Both] Server Status Alert delivery method
Server Status Alert Time	HH - Hour (00 - 23) MM - Minute (00 - 59)

Alert Settings (Once / Continuous)

Figure 2-31: Create New ICMP Ping – Alert Settings (Once/Continuous)

SMS Mobile	Mobile Number to receive SMS alerts.
Email Address	Email addresses to receive alerts.
Select from Address Book	Select mobile or email or both from address book contacts. Selected user name will be inserted to the text box above.
Select Group	Select group to receive alerts.

Alert Settings (Escalation)

Total Escalation Level : • Total escalation level - 1 to 5

Escalation Level 1

SMS Mobile :
• SMS Mobile - SMS to receive alerts

Email Address :
• Email - Email to receive alerts

Select Group :
• Select Group - Select group contacts

Group Name	Group Members
<input type="checkbox"/> IT	Operator 1, User 1

Select from Address Book

Escalation Level 2

Escalation Interval : Minutes

• Escalation Interval - Interval to send alerts between previous level and current level.

Figure 2-32: Create New ICMP Ping – Alert Settings (Escalation)

Total Escalation Level	[1 to 5] Select up to 5 levels of escalation alerts.
SMS Mobile	Mobile Number to receive SMS alerts.
Email	Email addresses to receive alerts.
Select from Address Book	Select mobile or email or both from address book contacts. Selected user name will be inserted to the text box above.
Select Group	Select group to receive alerts.
Escalation interval	Interval (in minutes) to send alerts between previous level and current level.

Alert Text Message

<p>Alert Text Message :</p>	<p>ASCII/Text</p> <p>xIPx:xRULEx is not reachable.</p>	<p>The system will use the default message if alert message is set to blank. The default message form is: xIPx:xRULEx is not reachable. User can change the message format by creating the text in the textarea above.</p> <p><input type="button" value="Variables in Alert Message"/></p>
<p>Send Second Alert :</p>	<p>Disable</p>	<p>Send Second Alert (for "once" alert mode in ICMP rule)</p> <ul style="list-style-type: none"> • Enable system to send second alert to mobile and email <p>If this field is leave blank, no SMS will be sent.</p>
<p>Alive Text Message :</p>	<p>ASCII/Text</p>	

Figure 2-33: Alert Text Message Fields

Alert Text Message	The system will use the default message if alert message is set to blank. The default message form is: xIPx:xRULEx is not reachable. User can change the message format by creating the text in the textarea above.
Send Second Alert (Only available for ICMP's 'once' alert mode)	<p>Enable system to send second alert to mobile and email</p> <p>Second Alert Interval - Interval to send second alert if ping check is still down.</p> <p>Second Alert Text Message - The system will use the default message if alert message is set to blank. The default message form is: xIPx:xRULEx is not reachable. User can change the message format by creating the text in the text area above.</p>
Alive Text Message	If this field is leave blank, no SMS will be sent.
Variables in Message Template	<ul style="list-style-type: none"> • xRULEx - Rule name • xIPx - Server IP • xPORTx - Port number in TCP Port Check rule • xURLx - Target url in url rule • xSERVICEx - Seervice name in Windows Service rule. • xPROCESSx - Process name in Windows Process rule. • xMULTISERVICEx - Service list in Multiple Windows Service rule. • xCPUUTILx - Last CPU utilization in percentage. • xDISKUTILx - Last Disk utilization in percentage.

- **xMEMUTILx** - Last Memory utilization in percentage.
- **xDTMx** - Server date and time of this alert message

2.7.1.2 Upload ICMP

User can create ICMP rules by file upload option. Download the sample file as template and add the rule name, desired IP address and device name for each ICMP rule. Select templates from the list and upload. SendQuick Avera will create ICMP rules based on the configuration template file. [Refer to 2.11 Configuration Template](#) for more details.

Network Monitor / ICMP Ping / File Upload

File Upload

Select target CSV File : upload_icmp.csv

The CSV file must be COMMA delimited, new record start with new line and with the fields:

- **Rule Name** - Max 30 characters.
- **IP Address** - Max 15 characters. Contain valid IP only
- **Device Name** - Max 50 characters. Contain alphabets, digits and - _ () only.

Records with existing Rule Name will be ignored.

Dependency Rule :

Rule Configuration Template :

Alert Configuration Template :

Select from all registered rule name. If dependency rule fails, system will not send alerts.

Select template from predefined rule configuration templates.

Select template from predefined alert configuration templates.

Please do not close this window before the process is completed.

Figure 2-34: Upload ICMP Ping – File Upload

2.7.2 TCP Port Check

Monitoring TCP port number, trigger alerts when the port of that server is unavailable.

Port Number : TCP Port Number to monitor

Figure 2-35: TCP Port Check – Port Number

Port Number	TCP Port Number to be monitored
-------------	---------------------------------

[Refer to 2.7.1.1](#) for the other configurations.

2.7.3 URL Check

Monitoring URL, trigger alerts when the URL response is unsuccessful.

Target URL :	<input type="text" value="http://www.google.com"/>	Target URL to monitor
--------------	--	-----------------------

Figure 2-36: URL Check – Target URL

Target URL	Target URL to be monitored. Prefix with http:// or https:// to determine the protocol.
------------	--

[Refer to 2.7.1.1](#) for the other configurations.

2.7.4 Windows Service Check

2.7.4.1 Single Service

Monitoring Single Windows Service via WMI connection. Alerts will be triggered in one of the following situations:

- Server IP is not reachable
- WMI Connection to windows server is not successful
- Windows service is not available or not running
- Windows service is not restarted if it is expected to be restarted if not running.

To select windows service, select server name from the Windows Server list (created in Device Profile).

Click on [Select Service](#) to retrieve all windows services from that windows server in real time.

Server Name :	<input type="text" value="server213"/>	Select windows server from all registered device name. Windows login name and password are needed to trigger WMI check.
	Select Service	Click to select service to monitor. Windows Server must be specified first.

Figure 2-37: Windows Service Check (Single) – Server Name

Select windows service to be monitored.

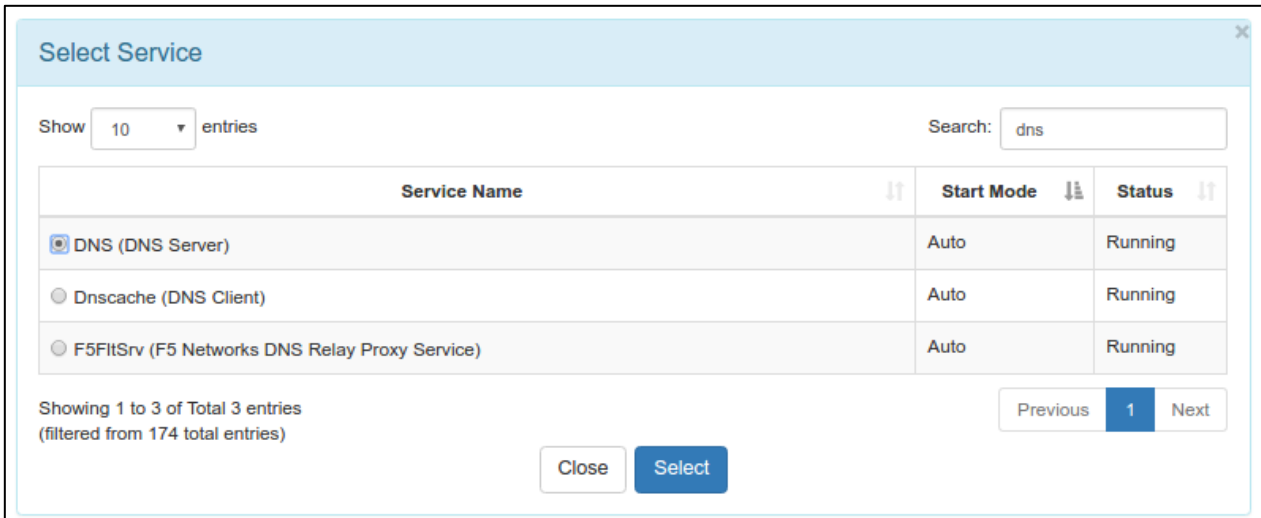


Figure 2-39: Service Selection

Once selected, Service Name and Service Description will be updated.

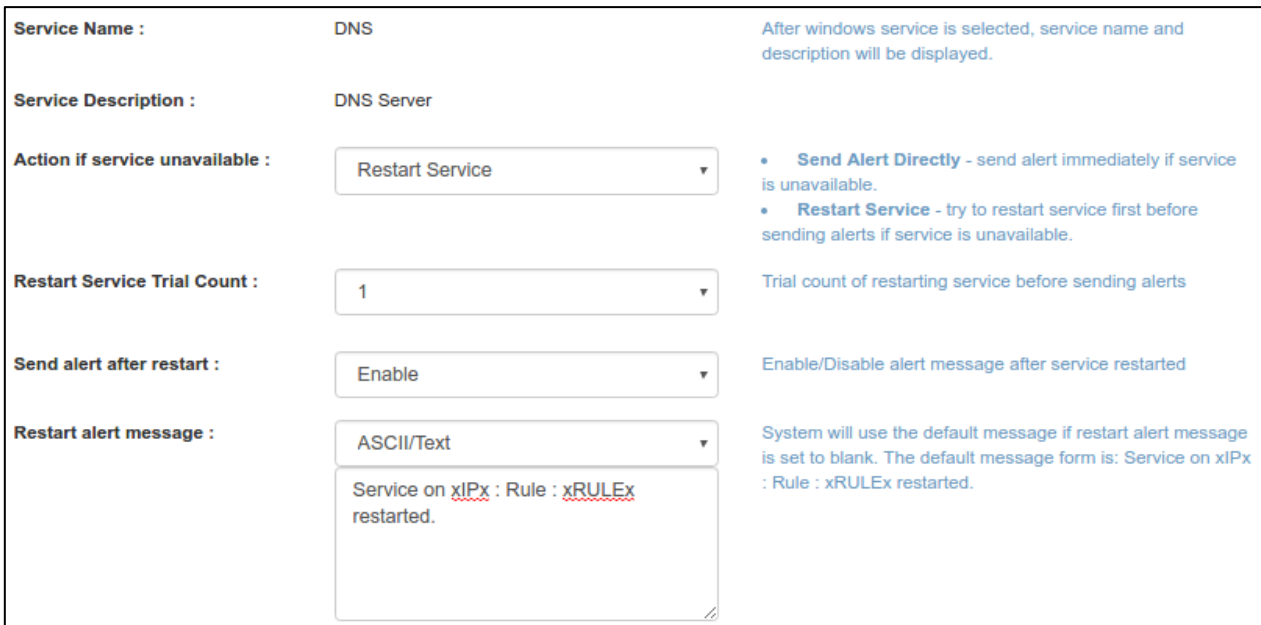


Figure 2-38: Updated Service Name & Service Description

Action if service unavailable	[Send Alert Directly Restart Service] Send Alert Directly - send alert immediately if service is unavailable Restart Service - try to restart service first before sending alerts if service is unavailable
Restart Service Trial Count	Trial count of restarting service before sending alerts
Send alert after restart	Enable/Disable alert message after service restarted
Restart alert message	System will use the default message if restart alert message is set to blank. The default message form is: Service on xIPx : Rule : xRULEx restarted. User can change the message format by creating the text in the text area. Use variable xRULEx for the displaying of

	rule name.
--	------------

Refer to [2.7.1.1](#) for the other configurations.

2.7.4.2 Multiple Service

Monitoring Multiple Windows Service via WMI connection. Alerts will be triggered in one of the following situations:

- Server IP is not reachable
- WMI Connection to windows server is not successful
- One of the Windows services is not available or not running
- Windows services not restarting if it is expected to be restarted if not running.

To select windows services, select server name from the Windows Server list (created in Device Profile).

Click on [Select Service](#) to retrieve all windows services from that windows server in real time.

Server Name :	server213	<p>Select windows server from all registered device name. Windows login name and password are needed to trigger WMI check.</p> <p>Click to select service to monitor. Windows Server must be specified first.</p>
	Select Service	

Figure 2-40: Windows Service Check (Multiple) – Server Name

Select windows services to be monitored.

Select Service x

Show entries

Search:

<input checked="" type="checkbox"/>	Service Name	Start Mode	Status
<input checked="" type="checkbox"/>	VMAuthdService (VMware Authorization Service)	Auto	Running
<input checked="" type="checkbox"/>	VMnetDHCP (VMware DHCP Service)	Auto	Running
<input checked="" type="checkbox"/>	VMUSBArbService (VMware USB Arbitration Service)	Auto	Running
<input checked="" type="checkbox"/>	VMware NAT Service (VMware NAT Service)	Auto	Running
<input checked="" type="checkbox"/>	vmware-converter-agent (VMware vCenter Converter Standalone Agent)	Auto	Running
<input checked="" type="checkbox"/>	vmware-converter-server (VMware vCenter Converter Standalone Server)	Auto	Running
<input checked="" type="checkbox"/>	vmware-converter-worker (VMware vCenter Converter Standalone Worker)	Auto	Running

Showing 1 to 7 of Total 7 entries
 (filtered from 174 total entries)

Previous 1 Next

Close
Select

Figure 2-41: Service Selections

Once selected, list of service name and description will be updated.

Services :	<ol style="list-style-type: none"> 1. VMAuthdService (VMware Authorization Service) 2. VMnetDHCP (VMware DHCP Service) 3. VMUSBArbService (VMware USB Arbitration Service) 4. VMware NAT Service (VMware NAT Service) 5. vmware-converter-agent (VMware vCenter Converter Standalone Agent) 6. vmware-converter-server (VMware vCenter Converter Standalone Server) 7. vmware-converter-worker (VMware vCenter Converter Standalone Worker) 	Click to select process to monitor. Windows Server must be specified first.
Action if service unavailable :	Restart Service	<ul style="list-style-type: none"> • Send Alert Directly - send alert immediately if service is unavailable. • Restart Service - try to restart service first before sending alerts if service is unavailable.
Restart All Service :	No	Restart all services OR restart failed services only.
Restart Service Trial Count :	1	Trial count of restarting service before sending alerts
Send alert after restart :	Enable	Enable/Disable alert message after service restarted
Restart alert message :	ASCII/Text Service on xIPx : Rule : xRULEx restarted.	System will use the default message if restart alert message is set to blank. The default message form is: Service on xIPx : Rule : xRULEx restarted.

Figure 2-42: Updated List of Services

Action if service unavailable	[Send Alert Directly Restart Service] Send Alert Directly - send alert immediately if service is unavailable Restart Service - try to restart service first before sending alerts if service is unavailable
Restart All Service	Restart all services OR restart failed services only.
Restart Service Trial Count	Trial count of restarting service before sending alerts
Send alert after restart	Enable/Disable alert message after service restarted
Restart alert message	System will use the default message if restart alert message is set to blank. The default message form is: Service on xIPx : Rule : xRULEx restarted. User can change the message format by creating the text in the text area. Use variable xRULEx for the displaying of rule name.

[Refer to 2.7.1.1](#) for the other configurations.


2.7.5 Windows Process Check

Monitoring Windows Process via WMI connection. Alerts will be triggered in one of the following situations:

- Server IP is not reachable
- WMI Connection to windows server is not successful
- Windows Process is not available or not running
- Memory usage of the Windows Process exceeded threshold

To select windows process, select server name from the Windows Server list (created in Device Profile).

Click on **Select Process** to retrieve all windows processes from that windows server in real time.

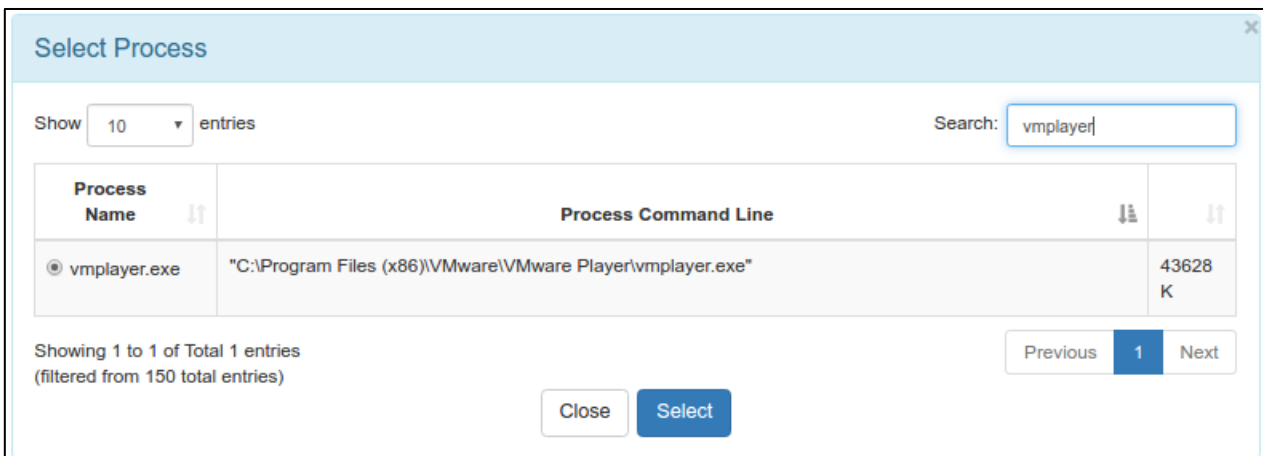


Server Name : Select windows server from all registered device name. Windows login name and password are needed to trigger WMI check. Click to select process to monitor. Windows Server must be specified first.

Select Process

Figure 2-43: Window Process Check – Server Name

Select windows process to be monitored. Filter result by the Search box.



Select Process

Show entries Search:

Process Name	Process Command Line	
<input checked="" type="radio"/> vmplayer.exe	"C:\Program Files (x86)\VMware\VMware Player\vmplayer.exe"	43628 K

Showing 1 to 1 of Total 1 entries
(filtered from 150 total entries)

Previous **1** Next

Figure 2-44: Process Selection

Once selected, list of process name and process command line will be updated.

Process Name :	vmplayer.exe	After windows process is selected, process name and command line will be displayed.
Process Command Line :	"C:\Program Files (x86)\VMware\VMware Player\vmplayer.exe"	
Process Memory Threshold :	<input checked="" type="radio"/> 80 % <input type="radio"/> <input type="text"/> K	Action taken if the windows process memory usage meet this threshold percentage
Action if meet threshold :	<input type="text" value="Kill Process and Send Alert"/>	<ul style="list-style-type: none"> • Send Alert Directly - send alert immediately. • Kill Process and Send Alert - kill process first, then send alerts

Figure 2-45: Updated Process Details

Process Memory Threshold	Action taken if the windows process memory usage meet this threshold percentage(%) or value (in K)
Action if meet threshold	[Send Alert Directly Kill Process and Send Alert] Send Alert Directly - send alert immediately Kill Process and Send Alert - kill process first, then send alerts

[Refer to 2.7.1.1](#) for the other configurations.

2.7.6 CPU Check

Monitoring CPU utilization for Windows via WMI connection or Linux server via SSH connection. Server login credential is required and configured in Device Profile. ([Refer to 2.6 Device Profile](#))

Alerts will be triggered when

- Server IP is not reachable
- For Windows: WMI Connection is not successful
- For Linux: SSH Connection is not successful
- CPU usage of the server exceeded threshold

Server Name :	server213	Select server from all registered device name. Server administrator credential is required and can be configured in Device Profile management.
CPU Utilization Threshold :	80 %	Trigger alert when server's cpu usage meet this threshold percentage

Figure 2-46: CPU Check Fields

Server Name	Select server from all registered device name. Server administrator credential is required and can be configured
-------------	--

CPU Utilization Threshold	in Device Profile management.
	Alerts will be triggered when server's CPU usage meet this threshold.

[Refer to 2.7.1.1](#) for the other configurations.

2.7.7 Disk Check

Monitoring Disk utilization for Windows via WMI connection or Linux server via SSH connection. Server login credential is required and configured in Device Profile. ([Refer to 2.6 Device Profile](#))

Alerts will be triggered when

- Server IP is not reachable
- For Windows: WMI Connection is not successful
- For Linux: SSH Connection is not successful
- Disk usage of the server exceeded threshold

Server Name :	<input type="text" value="server213"/>	Select server from all registered device name. Server administrator credential is required and can be configured in Device Profile management.
	<input type="button" value="Select Disk"/>	Select Disk Drive to monitor

Figure 2-47: Disk Check – Server Name

To select disk/partition, select server name from the server list (created in Device Profile).

Click on to retrieve all partitions from that server in real time.

Select disk to be monitored. Create multiple disk utilization rules if need to monitor multiple partitions.

Select Disk
✕

Show entries Search:

Disk Name	Total	Free	Usage
<input type="radio"/> E:	368.10G	134.24G	63.53%
<input type="radio"/> C:	465.76G	211.22G	54.65%
<input type="radio"/> F:	97.66G	66.44G	31.97%

Showing 1 to 3 of Total 3 entries

Figure 2-48: Disk Selection

Once selected, Disk Name will be updated.

Disk Name :	C:	
Disk Utilization Threshold :	80	%
		Trigger alert when server's disk usage meet this threshold percentage

Figure 2-49: Disk Details Updated

Disk Utilization Threshold	Alerts will be triggered when disk/partition usage meet this threshold.
----------------------------	---

[Refer to 2.7.1.1](#) for the other configurations.

2.7.8 Memory Check

Monitoring memory utilization for Windows via WMI connection or Linux server via SSH connection. Server login credential is required and configured in Device Profile. ([Refer to 2.6 Device Profile](#))

Alerts will be triggered when

- Server IP is not reachable
- For Windows: WMI Connection is not successful
- For Linux: SSH Connection is not successful
- Memory usage of the server exceeded threshold

Server Name :	server213	Select server from all registered device name. Server administrator credential is required and can be configured in Device Profile management.
Memory Utilization Threshold :	80	%
		Trigger alert when server's memory usage meet this threshold percentage

Figure 2-50: Memory Check Fields

Server Name	Select server from all registered device name. Server administrator credential is required and can be configured in Device Profile management.
Memory Utilization Threshold	Alerts will be triggered when server's CPU usage meet this threshold.

[Refer to 2.7.1.1](#) for the other configurations.

2.8 Message Filter

There are 3 types of message filtering type, which are filter by Email, SNMP Trap or SYSLOG Message. Alerts will be triggered when SendQuick Avera receive the message

which is match with the filtering rules.

The Filter Rules will be useful for selective sending of alert messages using SMS. The Filter Rules section needs to be configured carefully to provide the right rules for SMS alert. It is fine if you configure the Filter Rules on a later stage as it has no impact on the operation of SendQuick system.

2.8.1 Mail Message Filter

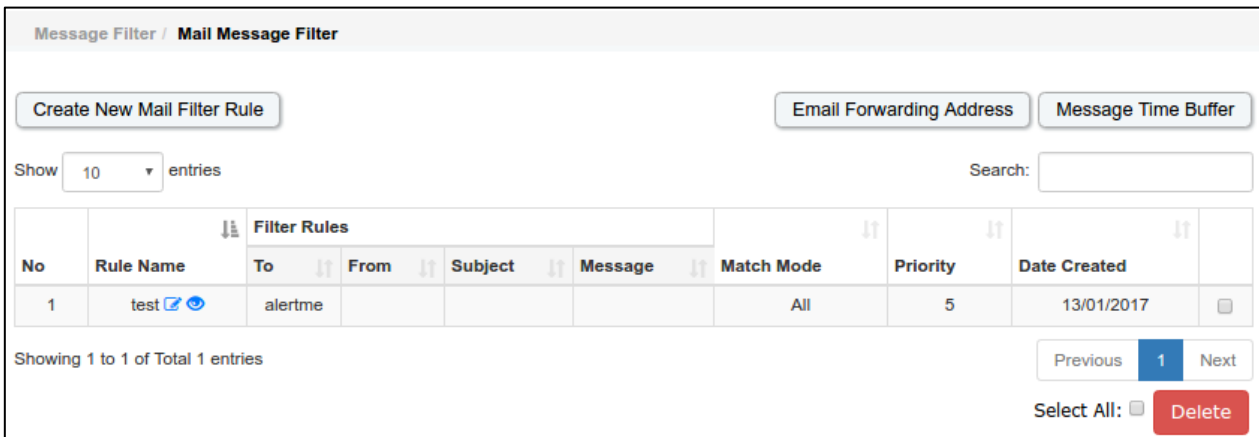


Figure 2-51: Mail Message Filter

The Mail Message Filter is used to filter the email notifications from your devices or systems (example firewall, anti-virus, IPS, UPS and others) to SendQuick and applied with the Email Filter policies to determine whether to send alerts (Email/SMS) to the recipients. All messages that were sent to Email Filter will be filtered in accordance with the message filter rules.

All emails that need to be filtered will be sent to SendQuick servers, either using SendQuick domain (FQDN) or IP address. The format is 'username@sendQuickIPorDomain'. As SendQuick is a mail server, it can process all emails that has the server destination as itself, meaning SendQuick IP or domain. Hence, SendQuick is able to accept all emails sent to SendQuick address.

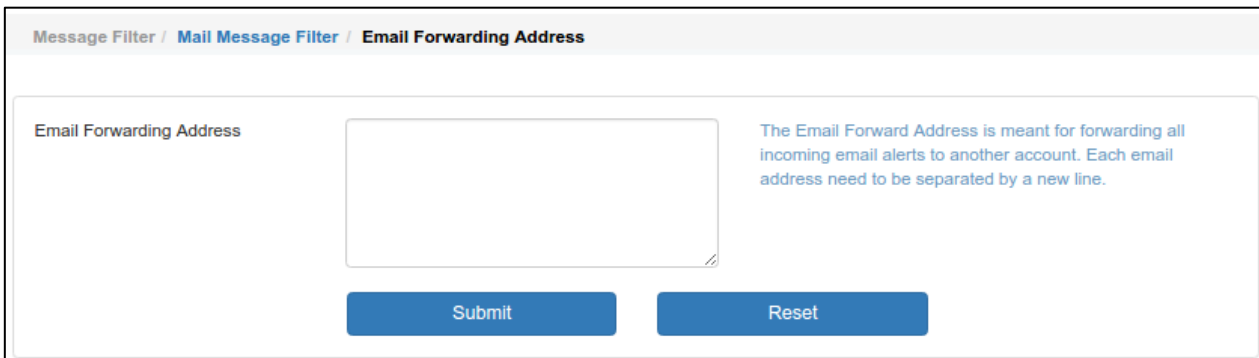
The email address to process the filter messages (filter email) is any email address with SendQuick IP (or domain) as the destination server. Hence, the username section can be any alphanumeric value. For example it can be alarm, support, technical123 and others. The exceptions are the word 'SMS' and the numeric only username (e.g., 1234567)

For example, if the SendQuick server has an IP of 192.168.1.8 or a server name (FQDN) of sms.com.sg, then the email addresses created can be as follow (if the email username is **alarm**):

alarm@192.168.1.8 or *alarm@sms.com.sg*

All the messages that were sent to the filter accounts can be forwarded to other email addresses as well as sent to the Mail Filter for processing. The emails will be checked against the Mail Filter configuration based on the Filter Policy. Hence, it is very important for the emails to be sent correctly to SendQuick. It is very important to understand the email address (to SendQuick Filter Account) as explained above.

2.8.1.1 Email Forwarding Address

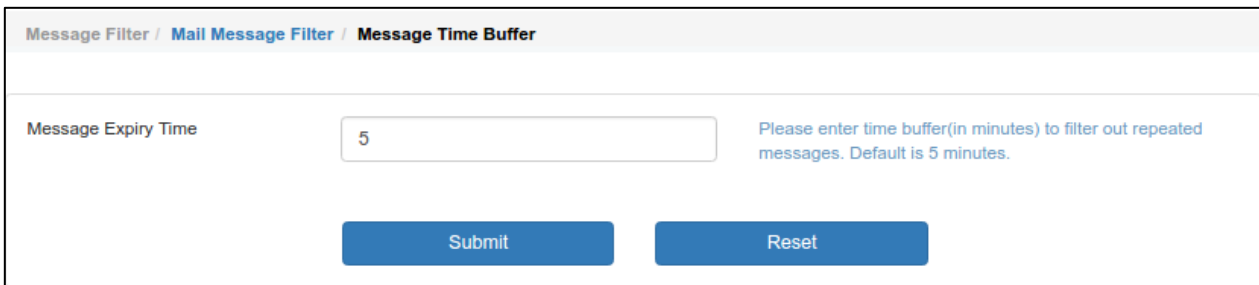


The screenshot shows a web interface for configuring the 'Email Forwarding Address'. At the top, there is a breadcrumb trail: 'Message Filter / Mail Message Filter / Email Forwarding Address'. Below this, the main heading is 'Email Forwarding Address'. To the right of the heading, there is a blue text box containing the instruction: 'The Email Forward Address is meant for forwarding all incoming email alerts to another account. Each email address need to be separated by a new line.' In the center, there is a large, empty text input field. Below the input field, there are two blue buttons: 'Submit' and 'Reset'.

Figure 2-52: Mail Message Filter – Email Forwarding Address

All the messages that were sent to the filter accounts can be forwarded to other email addresses. The Email Forward Address is meant for forwarding all incoming email alerts to another account. Each email address needs to be separated by a new line.

2.8.1.2 Message Time Buffer



The screenshot shows a web interface for configuring the 'Message Time Buffer'. At the top, there is a breadcrumb trail: 'Message Filter / Mail Message Filter / Message Time Buffer'. Below this, the main heading is 'Message Time Buffer'. To the left of the heading, there is a label 'Message Expiry Time'. To the right of the label, there is a text input field containing the number '5'. To the right of the input field, there is a blue text box containing the instruction: 'Please enter time buffer(in minutes) to filter out repeated messages. Default is 5 minutes.' Below the input field, there are two blue buttons: 'Submit' and 'Reset'.

Figure 2-53: Mail Message Filter – Message Time Buffer

Message Time Buffer is a configuration to avoid repeated SMS when the device generates or sends repeated messages to SendQuick. The value inserted in the Message Expiry Time means any repeated messages sent to SendQuick within the buffer time will be discarded. To avoid more repeated messages, set the time buffer to a higher value.

2.8.1.3 Create or Update Mail Message Filter Rule

Click on [Create New Mail Filter Rule](#) button to create new rule or [✎](#) to update existing mail message rule.

Rule Name :	<input type="text" value="test"/>	Name for this rule. <input type="text" value="Variable Usage (For To, From, Subject and Message)"/>
To :	<input type="text" value="alertme"/>	Trigger alert when receive message from this receiver.
From :	<input type="text"/>	Trigger alert when receive message from this sender.
Subject :	<input type="text"/>	Trigger alert when receive email with this subject.
Message :	<input type="text"/>	Trigger alert when receive message match with this content.
Match Mode :	<input checked="" type="radio"/> All <input type="radio"/> Any	<ul style="list-style-type: none"> All - the system will trigger alert when all of the above filter rules matched. Any - the system will trigger alert when any of the above filter rules matched.
Priority :	<input type="text" value="5"/>	Alert's SMS Priority

Figure 2-54: New Mail Filter Rule

Rule Name	Name for this rule.
To	Trigger alerts when the Email Recipient match with this value.
From	Trigger alerts when the Email Sender match with this value.
Subject	Trigger alerts when the Email Subject match with this value.
Message	Trigger alerts when the Email Contents match with this value.
Match Mode	All: Trigger alerts when received email match with all configured fields. Any: Trigger alerts when received email match with any configured fields.
Priority	SMS Alert Priority. 1 is the highest priority and 9 is the lowest priority.

The filtering engine is based on matching the exact words or character and the phrase filled in the space provided, for each relevant field. You can also set the AND and OR relationship in the text box. The instructions are in Variable Usage.

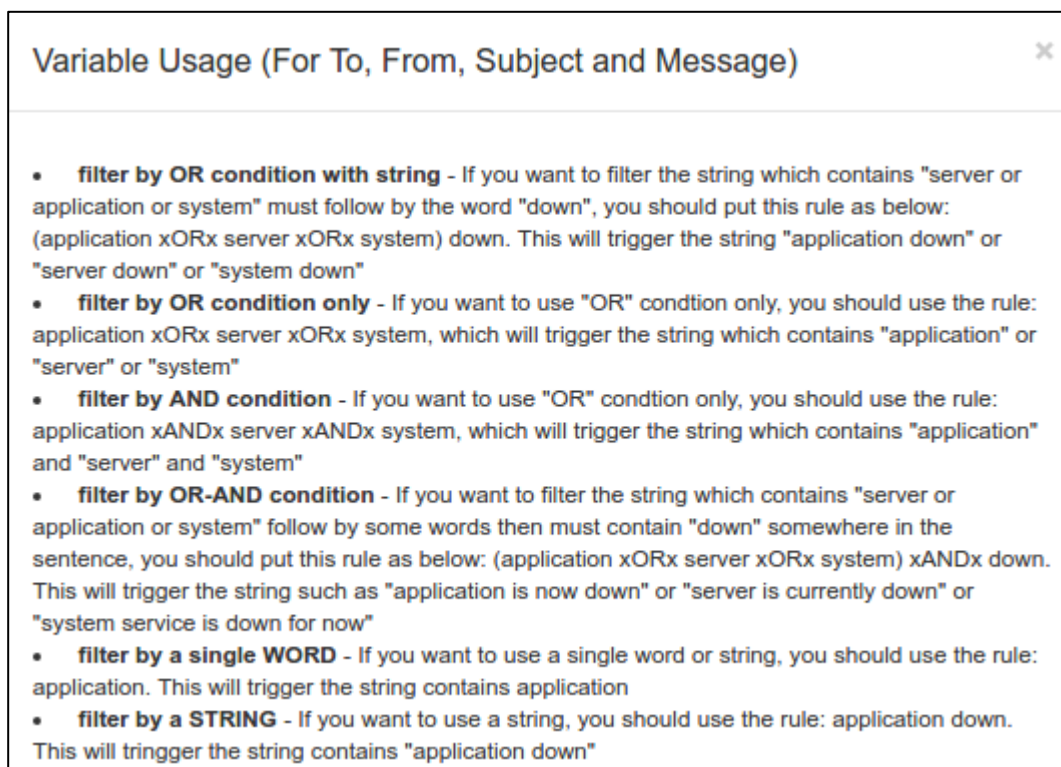


Figure 2-55: Variable Usage Window

Example, if the Subject field is entered with 'error message' the various scenarios is illustrated below:

Sentence	Match Status	Reasons
There is an error in the system message	No	Though the words 'error' and 'message' appears in the sentence, they are individual words and not a phrase.
This is a system error	No	Only the word 'error' occurs and not the whole phrase
There is an error message from system	Yes	The whole phrase 'error message' appears in the sentence.

2.8.1.3.1 Create or Update Alert List

From Mail Message filter list, click on  to view the alert list.

Message Filter / Mail Message Filter / Alert List

Mail Message Filter Rules

Rule Name: test

To: alertme

From:

Subject:

Message:

Match Mode: All

Priority: 5

Create New Alert List

Show 10 entries Search:

No	Alert Name	SMS Mobile	Email Address	Group Name	Alert Text Message	Alert Mode
1	alert1	Alert 91234567 User 1	Alert user1@talariax.com User 1	Alert IT	xFRx:xSUBx:MSGx	Once
2	alert2	Alert Level 1 81234567 Operator 1 Alert Level 2 91234567 Report fff Operator 1	Alert Level 1 user2@talariax.com Operator 1 Alert Level 2 user3@talariax.com Report Operator 1	Alert Level 1 Alert Level 2 IT Report	xFRx:xSUBx:MSGx	Escalation & Report

Figure 2-56: Mail Message Filter – Alert List

Click on to create new alert list or to update existing alert list.

Alert Name :

Alert Mode :

- **Once** - the system will trigger alert to operator one time only.
- **Once and Report** - the system will trigger alert to operator one time only, then send report to operator.
- **Escalation** - the system will trigger alert according to escalation level settings
- **Escalation and Report** - the system will trigger alert according to escalation level settings, then send report to operators.

Figure 2-57: Add Alert List

Alert Name	Name for the alert list.
Alert Mode	<p>Once - the system will send SMS alert to operator one time only, upon detecting mail message filter rules.</p> <p>Once And Report - the system will send SMS alert and send report to operator one time only, upon detecting mail message filter rules.</p> <p>Escalation - the system will send SMS alert follow escalation level settings, upon detecting mail message filter rules.</p> <p>Escalation And Report - the system will send SMS alert follow escalation level settings and send report to operator, upon detecting mail message filter rules.</p>

2.8.1.3.2 Alert Settings (Once / Once and Report)

SMS Mobile :	91234567 User 1	• SMS Mobile - SMS to receive alerts				
Email Address :	user1@talariax.com User 1	• Email - Email to receive alerts				
Select Group :	<div style="background-color: #4a86e8; color: white; padding: 2px; text-align: center; margin-bottom: 5px;">Select from Address Book</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f2f2f2;"> <th style="padding: 2px;">Group Name</th> <th style="padding: 2px;">Group Members</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;"><input type="checkbox"/> IT</td> <td style="padding: 2px;">Operator 1, User 1</td> </tr> </tbody> </table>	Group Name	Group Members	<input type="checkbox"/> IT	Operator 1, User 1	• Select Group - Select group contacts
Group Name	Group Members					
<input type="checkbox"/> IT	Operator 1, User 1					

Figure 2-58: Alert Settings (Once / Once & Report)

SMS Mobile	Mobile Number to receive SMS alerts.
Email Address	Email addresses to receive alerts.
Select from Address Book	Select mobile or email or both from address book contacts. Selected user name will be inserted to the text box above.
Select Group	Select group to receive alerts.

2.8.1.3.3 Alert Settings (Escalation / Escalation and Report)

Total Escalation Level : • Total escalation level - 1 to 5

Escalation Level 1

SMS Mobile :
• SMS Mobile - SMS to receive alerts

Email Address :
• Email - Email to receive alerts

Select Group :
• Select Group - Select group contacts

81234567
Operator 1

user2@talariax.com
Operator 1

Group Name	Group Members
<input type="checkbox"/> IT	Operator 1, User 1

Select from Address Book

Escalation Level 2

Escalation Interval : Minutes

• Escalation Interval - Interval to send alerts between previous level and current level.

SMS Mobile :
• SMS Mobile - SMS to receive alerts

Email Address :
• Email - Email to receive alerts

Select Group :
• Select Group - Select group contacts

Operator 1
91234567

Operator 1
user3@talariax.com

Group Name	Group Members
<input checked="" type="checkbox"/> IT	Operator 1, User 1

Select from Address Book

Figure 2-59: Alert– Escalation Settings

Total Escalation Level	[1 to 5] Select up to 5 levels of escalation alerts.
SMS Mobile	Mobile Number to receive SMS alerts.
Email Address	Email addresses to receive alerts.
Select from Address Book	Select mobile or email or both from address book contacts. Selected user name will be inserted to the text box above.
Select Group	Select group to receive alerts.
Escalation interval	Interval (in minutes) to send alerts between previous level and current level.

2.8.1.3.4 Alert Text Message Settings

Alert Text Message :	ASCII/Text xFRx:xSUBx:MSGx	The system will use the default message if alert message is set to blank. The default message form is: xFRx:xSUBx:MSGx.
-----------------------------	-------------------------------	---

Figure 2-60: Alert Text Message

Alert Text Message	Alert Message Content to be sent to recipients. Default is xFRx:xSUBx:MSGx
---------------------------	--

2.8.1.3.5 Report Settings (Once and Report / Escalation and Report)

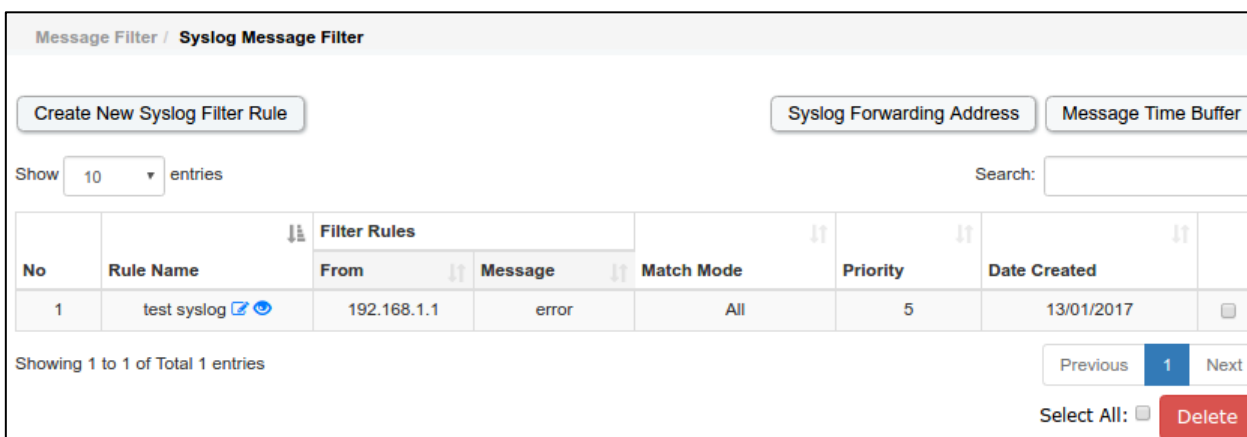
Report

Report Interval :	10					
SMS Mobile :	91234567	• SMS Mobile - SMS to receive alerts				
Email Address :	Admin A	• Email - Email to receive alerts				
Select Group :	<input type="button" value="Select from Address Book"/> <table border="1" style="margin-top: 5px;"> <thead> <tr> <th style="width: 30%;">Group Name</th> <th>Group Members</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> IT</td> <td>Operator 1, User 1</td> </tr> </tbody> </table>	Group Name	Group Members	<input type="checkbox"/> IT	Operator 1, User 1	• Select Group - Select group contacts
Group Name	Group Members					
<input type="checkbox"/> IT	Operator 1, User 1					

Figure 2-61: Alert – Report Settings

Report Interval	Interval (in minutes) to send report after escalation completed if there is no acknowledgement from user. Report will be sent immediately if Avera received acknowledgement from user.
SMS Mobile	Mobile Number to receive SMS alerts.
Email Address	Email addresses to receive alerts.
Select from Address Book	Select mobile or email or both from address book contacts. Selected user name will be inserted to the text box above.
Select Group	Select group to receive alerts.

2.8.2 Syslog Message Filter



Message Filter / Syslog Message Filter

Create New Syslog Filter Rule Syslog Forwarding Address Message Time Buffer

Show 10 entries Search:

No	Rule Name	Filter Rules		Match Mode	Priority	Date Created	
		From	Message				
1	test syslog	192.168.1.1	error	All	5	13/01/2017	

Showing 1 to 1 of Total 1 entries

Previous 1 Next

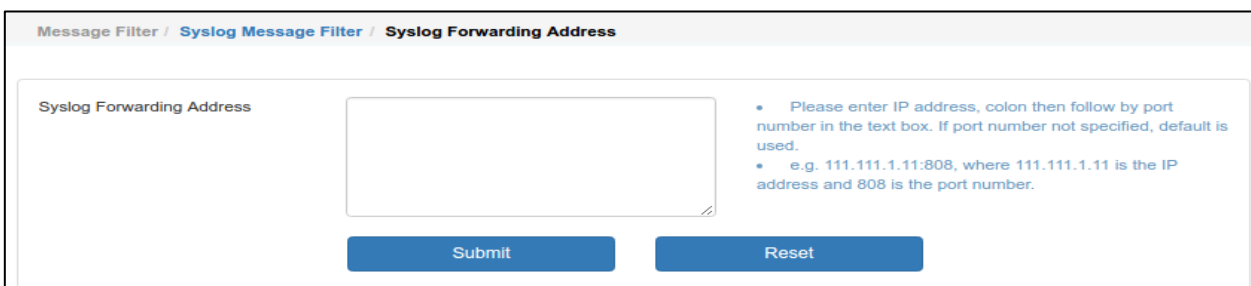
Select All: Delete

Figure 2-62: Syslog Message Filter

To capture the Syslog, just point the Syslog messages (from the devices and equipment) to the SendQuick server. The default port (in SendQuick) for Syslog is **514**.

Before configuring any Syslog messages, you may wish to configure the Syslog Forwarding which will allow all incoming Syslog messages to be forwarded to another server.

2.8.2.1 Syslog Forwarding Address



Message Filter / Syslog Message Filter / Syslog Forwarding Address

Syslog Forwarding Address

Please enter IP address, colon then follow by port number in the text box. If port number not specified, default is used.
e.g. 111.111.1.11:808, where 111.111.1.11 is the IP address and 808 is the port number.

Submit Reset

Figure 2-63: Syslog Message Filter – Syslog Forwarding Address

All the Syslog messages that were sent to SendQuick Avera can be forwarded to other Syslog server. Each Syslog server need to be separated by a new line.

2.8.2.2 Message Time Buffer

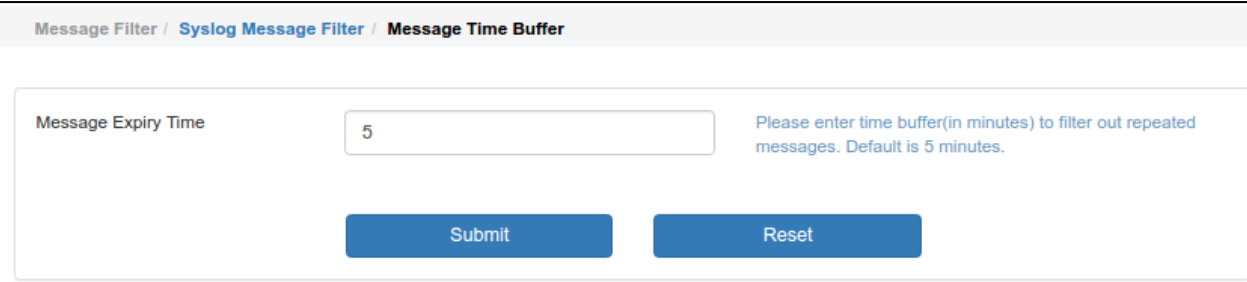



Figure 2-64: Syslog Message Filter – Message Time Buffer

Message Time Buffer is a configuration to avoid repeated alerts when the device generates or sends repeated Syslog messages to sendQuick Avera. The value inserted in the Message Expiry Time means any repeated Syslog messages sent to sendQuick within the buffer time will be discarded. To avoid more repeated messages, set the time buffer to a higher value.

2.8.2.3 Create or Update Syslog Message Filter Rule

Click on [Create New Syslog Filter Rule](#) button to create new rule or  to update existing mail message rule.

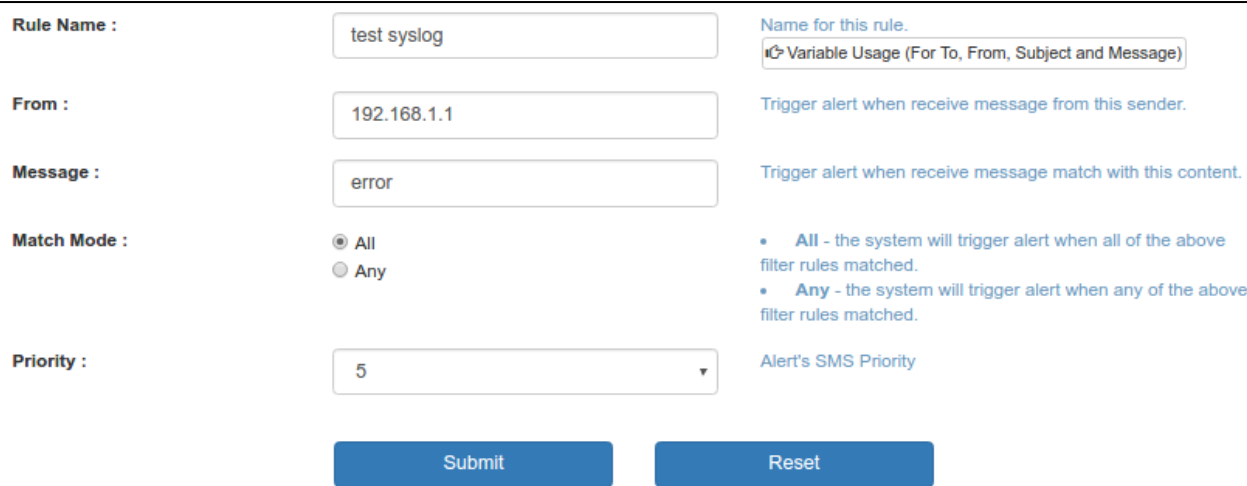


Figure 2-65: New Syslog Filter Rule

Rule Name	Name for this rule.
From	Trigger alerts when the Syslog message sender match with this value.
Message	Trigger alerts when the Syslog message contents match with this value.
Match Mode	<p>All: Trigger alerts when received Syslog message match with all configured fields.</p> <p>Any: Trigger alerts when received Syslog message match with any</p>

	configured fields.
Priority	SMS Alert Priority. 1 is the highest priority and 9 is the lowest priority.

The filtering engine is based on matching the exact words or character and the phrase filled in the space provided, for each relevant field. You can also set the AND and OR relationship in the text box. The instructions are in the Variable Usage.

[Refer to 2.8.1.3](#) for more details.

2.8.3 SNMP Message Filter

Message Filter / SNMP Message Filter

Create New SNMP Filter Rule SNMP Forwarding Address Message Time Buffer MIB Files Message Filter String

Show 10 entries Search:

No	Rule Name	From	Message	MIB	OID	Match Mode	Priority	Date Created
1	snmp_fw	192.168.1.1		SONICWALL-FIREWALL-IP-STATISTICS-MIB.MIB	sonicCurrentCPUUtil	All	5	16/01/2017
2	testsnmp1		down	None	None	All	5	16/01/2017

Showing 1 to 2 of Total 2 entries Previous 1 Next Select All: Delete

Figure 2-66: SNMP Message Filter

SendQuick Avera also supports SNMP (Simple Network Management Protocol) to SMS/Email function. To capture the SNMP trap, just point the SNMP trap messages (from the devices and equipment) to the SendQuick server. The default community setting and port (in SendQuick) is **Public** and **162**.

Once you have configured the SNMP trap to SendQuick server, you can configure the relevant trap messages that will trigger the alert message.

2.8.3.1 SNMP Forwarding Address

Message Filter / SNMP Message Filter / SNMP Forwarding Address

SNMP Forwarding Address

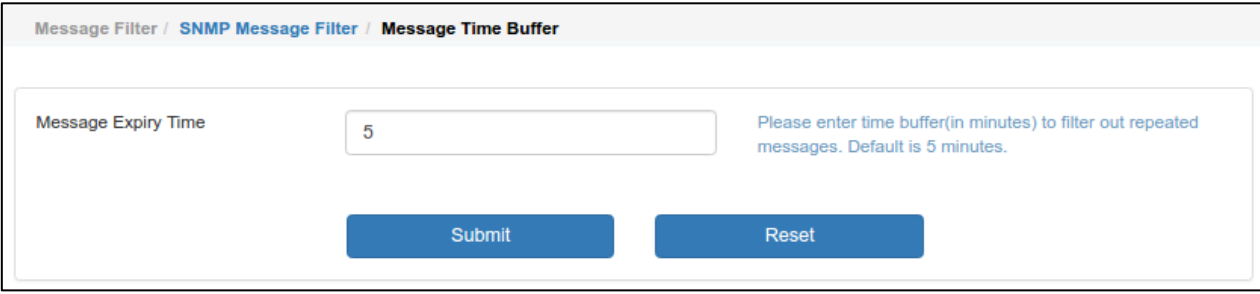
Please enter IP address, colon then follow by port number in the text box. If port number not specified, default is used.
e.g. 111.111.1.11:808, where 111.111.1.11 is the IP address and 808 is the port number.

Submit Reset

Figure 2-67: SNMP Message Filter – SNMP Forwarding Address

All the SNMP trap messages that were sent to SendQuick Avera can be forwarded to another server as Syslog message.

2.8.3.2 Message Time Buffer

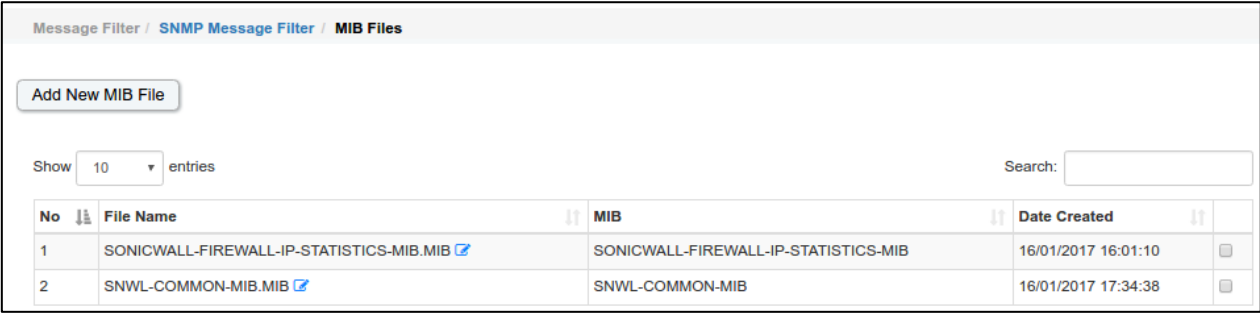


The screenshot shows the 'Message Time Buffer' configuration page. At the top, there is a breadcrumb trail: 'Message Filter / SNMP Message Filter / Message Time Buffer'. Below this, there is a form with a label 'Message Expiry Time' and a text input field containing the number '5'. To the right of the input field, there is a blue instruction text: 'Please enter time buffer(in minutes) to filter out repeated messages. Default is 5 minutes.' At the bottom of the form, there are two blue buttons: 'Submit' and 'Reset'.

Figure 2-68: SNMP Message Filter – Message Time Buffer

Message Time Buffer is a configuration to avoid repeated alerts when the device generates or sends repeated SNMP traps to SendQuick Avera. The value inserted in the Message Expiry Time means any repeated SNMP traps sent to SendQuick within the buffer time will be discarded. To avoid more repeated messages, set the time buffer to a higher value.

2.8.3.3 MIB Files



The screenshot shows the 'MIB Files' configuration page. At the top, there is a breadcrumb trail: 'Message Filter / SNMP Message Filter / MIB Files'. Below this, there is a button labeled 'Add New MIB File'. Underneath, there is a 'Show' dropdown menu set to '10' and the text 'entries'. To the right, there is a 'Search:' label followed by an empty text input field. Below these elements is a table with the following data:



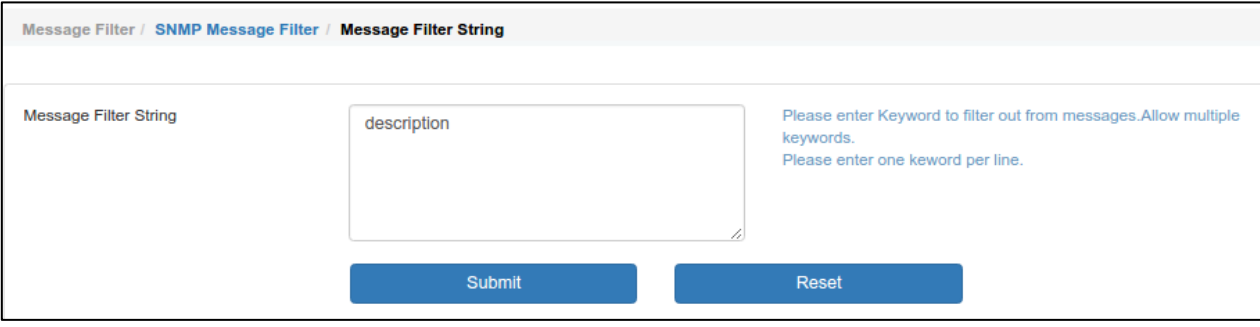
No	File Name	MIB	Date Created	
1	SONICWALL-FIREWALL-IP-STATISTICS-MIB.MIB 	SONICWALL-FIREWALL-IP-STATISTICS-MIB	16/01/2017 16:01:10	<input type="checkbox"/>
2	SNWL-COMMON-MIB.MIB 	SNWL-COMMON-MIB	16/01/2017 17:34:38	<input type="checkbox"/>

Figure 2-69: SNMP Message Filter – MIB Files

User can upload the MIB files (*.mib) to SendQuick Avera for monitoring particular OID string value. Once uploaded to Avera, user can select the MIB file and OID string to be monitored from the SNMP rules setting. ([Refer to 2.8.3.5 Create or Update SNMP Message Filter Rules](#))

2.8.3.4 Message Filter String



The screenshot shows the 'Message Filter String' configuration page. At the top, there is a breadcrumb trail: 'Message Filter / SNMP Message Filter / Message Filter String'. Below this, there is a form with a label 'Message Filter String' and a text area containing the word 'description'. To the right of the text area, there is a blue instruction text: 'Please enter Keyword to filter out from messages.Allow multiple keywords. Please enter one keyword per line.' At the bottom of the form, there are two blue buttons: 'Submit' and 'Reset'.

Figure 2-70: SNMP Message Filter – Message Filter String

The system will split SNMP message content by delimited character comma (,) and then equal (=).

If the configured keyword is equal to the left side word of equal (=), the system will send the string on the right side as alert message.

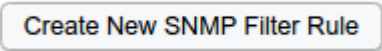

If the keyword is empty or is not found in the message content, the system will send the whole SNMP message content as alert message.

Example SNMP Message Content:

```
applicationSpecificAlarmID=LINK_DOWN:10.40.29.13:If: GigabitEthernet1/0/11,  
reportingEntityAddress=10.40.29.13.  
lastModifiedTimestamp=Thu May 22 15:23:24 SGT 2014,  
alarmCreationTime=2014-05-15 17:01:31.314,  
eventCount=1,mayBeAutoCleared=false,  
instanceId=13747878,  
severity=3,  
eventType=LINK_DOWN(39),  
authEntityId=7247240,  
applicationCategoryData=LINK_DOWN,  
previousSeverity=CLEARED,  
category=Switches and Hubs(268438038), source=10.40.29.13,  
notificationDeliveryMechanism=SNMP_TRAP,  
instanceVersion=0,  
description=Port 'GigabitEthernet1/0/11' is down on device '10.40.29.13'.,  
isAcknowledged=false,authEntityClass=-927529445,
```

If filter keyword is **description**,
alert message will be Port 'GigabitEthernet1/0/11' is down on device '10.40.29.13'.

2.8.3.5 Create or Update SNMP Message Filter Rule

Click on  button to create new rule or  to update existing mail message rule.

Rule Name :	<input type="text" value="snmp_fw"/>	Name for this rule. <small>Variable Usage (For To, From, Subject and Message)</small>
From :	<input type="text" value="192.168.1.1"/>	Trigger alert when receive message from this sender.
Message :	<input type="text"/>	Trigger alert when receive message match with this content.
Select MIB File :	<input type="text" value="SONICWALL-FIREWALL-IP-STATISTICS-MIB.MIB"/>	
Select OID String :	<input type="text" value="sonicCurrentCPUUtil 1.3.6.1.4.1.8741.1.3.1.3"/>	
	Include TrapObjectName in Message Text? <input checked="" type="radio"/> Yes <input type="radio"/> No	
	Include Varbind Value in Message Text? <input checked="" type="radio"/> Yes <input type="radio"/> No	
Match Mode :	<input checked="" type="radio"/> All <input type="radio"/> Any	<ul style="list-style-type: none"> All - the system will trigger alert when all of the above filter rules matched. Any - the system will trigger alert when any of the above filter rules matched.
Priority :	<input type="text" value="5"/>	Alert's SMS Priority
<input type="button" value="Submit"/> <input type="button" value="Reset"/>		

Figure 2-71: Create/Update SNMP Filter Rule

Rule Name	Name for this rule.
From	Trigger alerts when the SNMP traps sender match with this value.
Message	Trigger alerts when the SNMP message contents match with this value.
Select MIB File	Select MIB from the uploaded MIB files. (Refer to 2.8.3.3 MIB Files)
Select OID String	Select OID string from the selected MIB file.
Include TrapObjectName	Include SNMP TrapObjectName in the alert message content if checked.
Include Varbind value	Include SNMP Varbind value in the alert message content if checked.
Match Mode	<p>All: Trigger alerts when received SNMP traps match with all configured fields.</p> <p>Any: Trigger alerts when received SNMP traps match with any configured fields.</p>
Priority	SMS Alert Priority. 1 is the highest priority and 9 is the lowest priority.

[Refer to 2.8.1.3](#) for more details.

2.9 Adhoc Scanning

This feature allows user to check current statuses by particular rules, certain monitoring types or particular servers. Once the scanning process end, the following page will be shown. User can download the report in PDF, CSV or Excel format or email to desired email addresses.

2.9.1 Scan All Rules

Adhoc Scanning

Server Scan Report

Total : 11 (Up: 8 Down: 3)

Email : [Send Report](#)

Download File [[PDF](#) | [Excel](#) | [CSV](#)]

No	Rule Name	Description	Rule Type	Status
1	ping213	192.168.1.213	ICMP	✓
2	213_cpu	192.168.1.213	CPU Check	✓
3	213_diskC	192.168.1.213 (disk:C:)	Disk	✓
4	213_mem	192.168.1.213	Memory Check	✓
5	213_dns	192.168.1.213 (service:DNS)	Wins Service	✓
6	ping227	192.168.1.227	ICMP	✗
7	ping 105	192.168.1.105	ICMP	✓
8	google	http://www.google.com	URL	✓
9	vmplayer	192.168.1.213 (process:vmplayer.exe)	Wins Process	✗
10	yahoo	http://www.yahoo.com	URL	✓
11	klserver_disk	192.168.1.213	Disk	✗

Figure 2-72: Adhoc Scanning – All Rules

Scan all active/enabled monitoring rules from all monitoring types.

2.9.2 Scan By Rule Type

Scan all active/enabled monitoring rules in one of the monitoring types:

- ICMP Ping
- TCP Port Check
- URL Check
- Single Service
- Multiple Services
- Windows Process
- CPU Check
- Disk Check
- Memory Check

2.9.3 Scan By Server

Select server from the list and click on

Scan Now

System will scan all the active/enabled monitoring rules registered under this server.

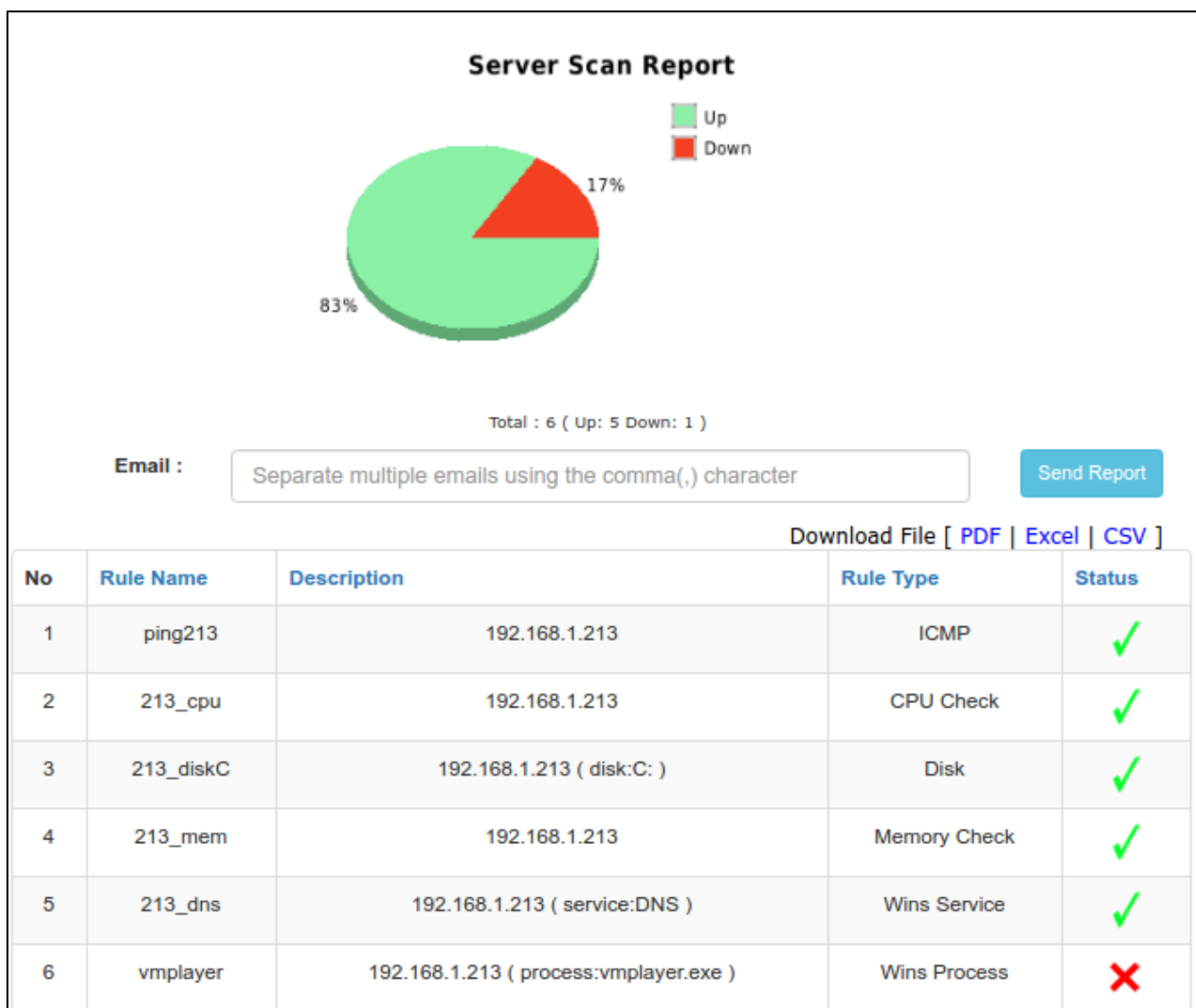


Figure 2-73: Adhoc Scanning – Server Scan

2.10 Admin

This menu is only accessible from Super Admin or Admin accounts.

2.10.1 Settings

Admin / Settings

Settings

Max number of device IP :	Unlimited (Used: 4)	
Max number of rules :	Unlimited (Used: 6)	
Suspend Network Monitoring :	<input type="text" value="Disable"/>	Enable to suspend all network monitoring process
Debug Mode :	<input type="text" value="Disable"/>	Enable to save more debug logs for troubleshooting before generating diagnostic file. Debug logs will be stored in system for maximum 2 days.
Default Character Set :	<input type="text" value="ASCII/Text"/>	Select the default character set for new rule's alert message and SMS broadcast message.
Allow Acknowledgement SMS :	<input type="text" value="Enable"/>	Enable to allow ACK and RES SMS from authorized mobile number to stop escalation alerts.
Allow SMS Check :	<input type="text" value="Enable"/>	Enable to allow SMS from authorized mobile to check current status of IP, Port, URL, Windows Service, Windows Process, CPU, Disk and Memory
SMS Check Authorized Mobile (PING, TCP, URL) :	<input type="text" value="83604556"/> <input type="button" value="Select from Address Book"/>	<ul style="list-style-type: none">Authorized mobile to check PING, TELNET and URL only.For SERVICE, PROCESS, CPU, DISK and MEMORY checking, authorized mobile is tied with device profile.
SMS Check Authorized Group (PING, TCP, URL) :	<input type="checkbox"/> IT	
Allow SMS Restart Server :	<input type="text" value="Enable"/>	Enable to allow SMS from authorized mobile number to restart registered device.
Allow SMS Shutdown Server :	<input type="text" value="Enable"/>	Enable to allow SMS from authorized mobile number to shut down registered device.
Allow SMS Restart Windows Service :	<input type="text" value="Enable"/>	Enable to allow SMS from authorized mobile number to restart windows service on registered device.

Figure 2-74: Administrative Settings

Max number of device IP and rules	Indicate total licensee and number of used license.
Suspend Network Monitoring	Enable to suspend all network monitoring process.
Debug Mode	Enable to save more debug logs for troubleshooting before generating diagnostic file. Debug logs will be stored in system for maximum 2 days.
Default Character Set	Select the default character set for new rule's alert messages and SMS broadcast.
Allow Acknowledgement SMS	Enable to allow ACK and RES SMS from authorized mobile number to stop escalation alerts.
Allow SMS Check	Enable to allow SMS from authorized mobile to check current status of IP, Port, URL, Windows Service, Windows Process, CPU, Disk and Memory
SMS Check Authorized Mobile (PING, TCP, URL)	Authorized mobile to check PING, TELNET and URL only. For SERVICE, PROCESS, CPU, DISK and MEMORY checking, authorized mobile is configured under device profile.
SMS Check Authorized Group (PING, TCP, URL)	Authorized mobile to check PING, TELNET and URL only. For SERVICE, PROCESS, CPU, DISK and MEMORY checking, authorized mobile is configured under device profile.
Allow SMS Restart Server	Enable to allow SMS from authorized mobile number to restart registered device.
Allow SMS Shutdown Server	Enable to allow SMS from authorized mobile number to shut down registered device.
Allow SMS Restart Windows Service	Enable to allow SMS from authorized mobile number to restart windows service on registered device.

2.10.2 To Do Items

Admin can utilize this feature as the notes of tasks with description, status, date due and date completed.

The screenshot shows a form for creating or updating a 'To Do List' item. It includes the following fields and instructions:

- Description :** A text area containing 'Add ICMP rules'. Instruction: 'A short description of the task to be performed.'
- Status :** A dropdown menu set to 'Completed'. Instruction: 'Use the status field to indicate if the item is completed, postponed, or open.'
- Date Due :** A date picker set to '2017-01-16'. Instruction: 'The date when the task is to be completed. Date should in YYYY-MM-DD format.'
- Date Completed :** A date picker set to '2017-01-16'. Instruction: 'The date when the task is completed. Date should in YYYY-MM-DD format.'
- Notes :** A text area. Instruction: 'Extra wording to describe the task.'

At the bottom of the form are two buttons: 'Submit' and 'Reset'.

Figure 2-76: Create/Update To Do List

Description	A short description of the task to be performed.
Status	Use the status field to indicate if the item is completed, postponed, or open.
Due Date	The date when the task is to be completed.
Date Completed	The date when the task is completed.
Notes	Extra wording to describe the task.

2.10.3 Server Logs

This page shows the server logs for monitoring process. Administrator can check the rule checking status for every rule. Server log will be kept in Avera for maximum 7 days. Admin can download certain day's log and send to SendQuick support team for troubleshooting.

Admin / **Server Logs**

Server Logs

```
2017-01-16 18:20:58 NMNotify[2730] (NMRule) 7|ICMP:<192.168.1.227> Total test:5 ; OK: 0 ; NOK: 5 ; TH: 5 ; stat:0
2017-01-16 18:21:34 NMCheck[3426] (NMRule) 6|Windows Service:DNS Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:21:54 NMCheck[3658] (NMRule) 9|HTTP:http://www.google.com Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:21:59 NMNotify[3455] (NMRule) 7|ICMP:<192.168.1.227> Total test:5 ; OK: 0 ; NOK: 5 ; TH: 5 ; stat:0
2017-01-16 18:22:35 NMCheck[4176] (NMRule) 6|Windows Service:DNS Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:22:55 NMCheck[4425] (NMRule) 9|HTTP:http://www.google.com Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:23:00 NMNotify[4202] (NMRule) 7|ICMP:<192.168.1.227> Total test:5 ; OK: 0 ; NOK: 5 ; TH: 5 ; stat:0
2017-01-16 18:23:36 NMCheck[4920] (NMRule) 6|Windows Service:DNS Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:23:48 NMCheck[4784] (NMRule) 11|HTTP:http://www.yahoo.com Total test:10 ; OK: 10 ; NOK: 0 ; TH: 10 ; stat:1
2017-01-16 18:23:55 NMCheck[5170] (NMRule) 9|HTTP:http://www.google.com Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:24:00 NMNotify[4947] (NMRule) 7|ICMP:<192.168.1.227> Total test:5 ; OK: 0 ; NOK: 5 ; TH: 5 ; stat:0
2017-01-16 18:24:37 NMCheck[5660] (NMRule) 6|Windows Service:DNS Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:24:53 NMNotify[5689] (NMRule) 10|Windows Process:vmplayer.exe Total test:10 ; OK: 0 ; NOK: 10 ; TH: 10 ; stat:0
2017-01-16 18:24:56 NMCheck[5943] (NMRule) 9|HTTP:http://www.google.com Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:25:01 NMNotify[5691] (NMRule) 7|ICMP:<192.168.1.227> Total test:5 ; OK: 0 ; NOK: 5 ; TH: 5 ; stat:0
2017-01-16 18:25:37 NMCheck[6498] (NMRule) 6|Windows Service:DNS Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:25:57 NMCheck[6730] (NMRule) 9|HTTP:http://www.google.com Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:26:02 NMNotify[6523] (NMRule) 7|ICMP:<192.168.1.227> Total test:5 ; OK: 0 ; NOK: 5 ; TH: 5 ; stat:0
2017-01-16 18:26:38 NMCheck[7228] (NMRule) 6|Windows Service:DNS Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:26:58 NMCheck[7454] (NMRule) 9|HTTP:http://www.google.com Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:27:02 NMNotify[7256] (NMRule) 7|ICMP:<192.168.1.227> Total test:5 ; OK: 0 ; NOK: 5 ; TH: 5 ; stat:0
2017-01-16 18:27:39 NMCheck[7947] (NMRule) 6|Windows Service:DNS Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:27:59 NMCheck[8185] (NMRule) 9|HTTP:http://www.google.com Total test:2 ; OK: 2 ; NOK: 0 ; TH: 2 ; stat:1
2017-01-16 18:28:03 NMNotify[7974] (NMRule) 7|ICMP:<192.168.1.227> Total test:5 ; OK: 0 ; NOK: 5 ; TH: 5 ; stat:0
2017-01-16 18:28:19 NMCheck[8433] (NMRule) 1|ICMP:<192.168.1.213> Total test:10 ; OK: 10 ; NOK: 0 ; TH: 10 ; stat:1
2017-01-16 18:28:21 NMCheck[8429] (NMRule) 3|DISK: C: (192.168.1.213), TH:80% Total test:10 ; OK: 10 ; NOK: 0 ; TH: 10 ; stat:1
2017-01-16 18:28:23 NMCheck[8436] (NMRule) 4|MEMORY (192.168.1.213), TH:80 % Total test:10 ; OK: 10 ; NOK: 0 ; TH: 10 ; stat:1
```

[Refresh](#)

[Download Log Files](#) : [Current Log](#) | [Log 1](#) | [Log 2](#) | [Log 3](#) | [Log 4](#) | [Log 5](#) | [Log 6](#)

Figure 2-77: Server Logs

2.10.4 Ping Test

Admin can use this page to check the IP connectivity to another server or device. Enter the IP address or Hostname to perform the real time ICMP Ping.

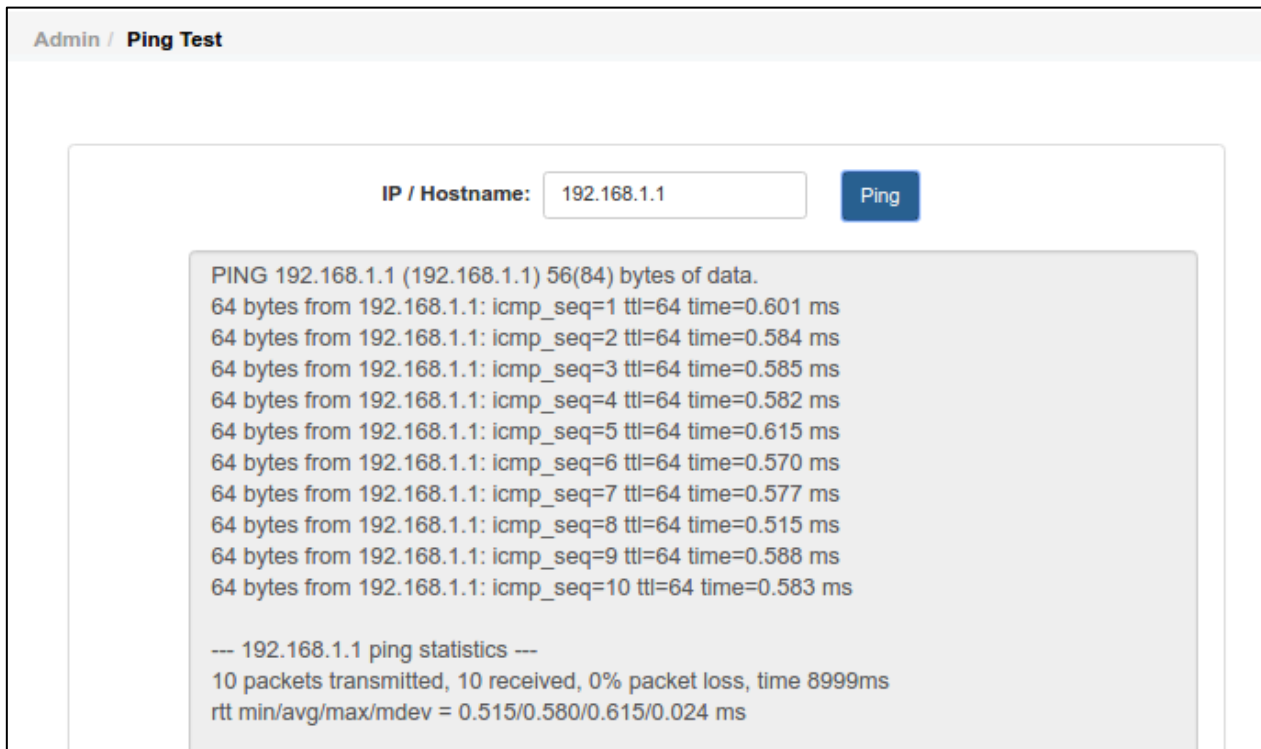


Figure 2-78: Ping Test

2.10.5 Traceroute Test

To perform the traceroute command, enter IP or Hostname and click on “Traceroute” button.

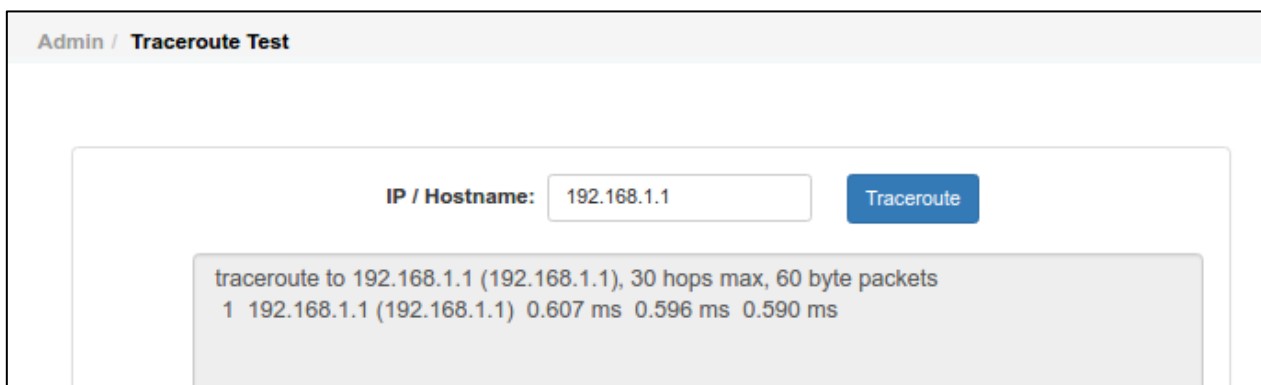


Figure 2-79: Traceroute Test

2.10.6 Telnet/Port Test

To perform the telnet command, enter IP/Hostname and TCP Port number, then click on “Telnet” button.

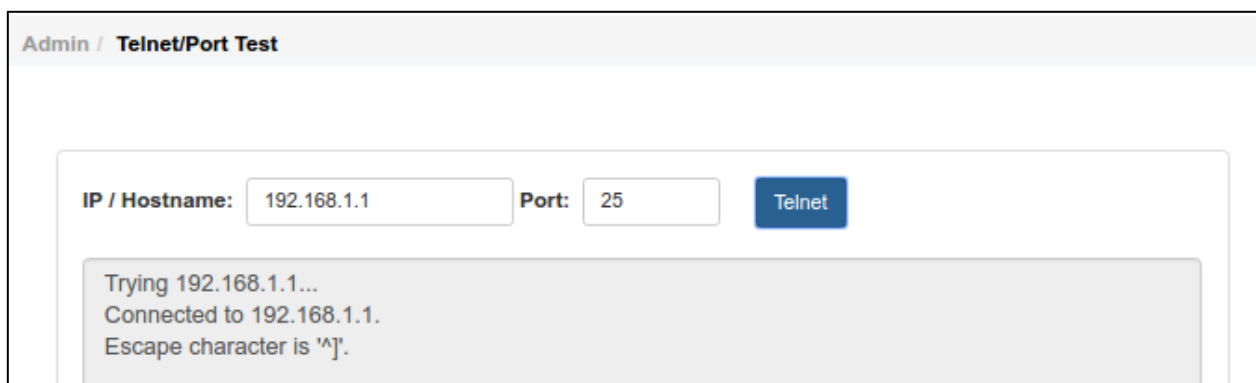


Figure 2-80: Telnet/Port Test

2.11 Configuration Template

User can create rule configuration template and alert configuration template as the template for creating ICMP rule by file upload. [Refer to 2.7.1.2 Upload ICMP](#) for more details.

2.11.1 Rule Configuration Template

Create rule related configuration template, such as priority, alarm trigger mode, monitoring frequency and server status alert.

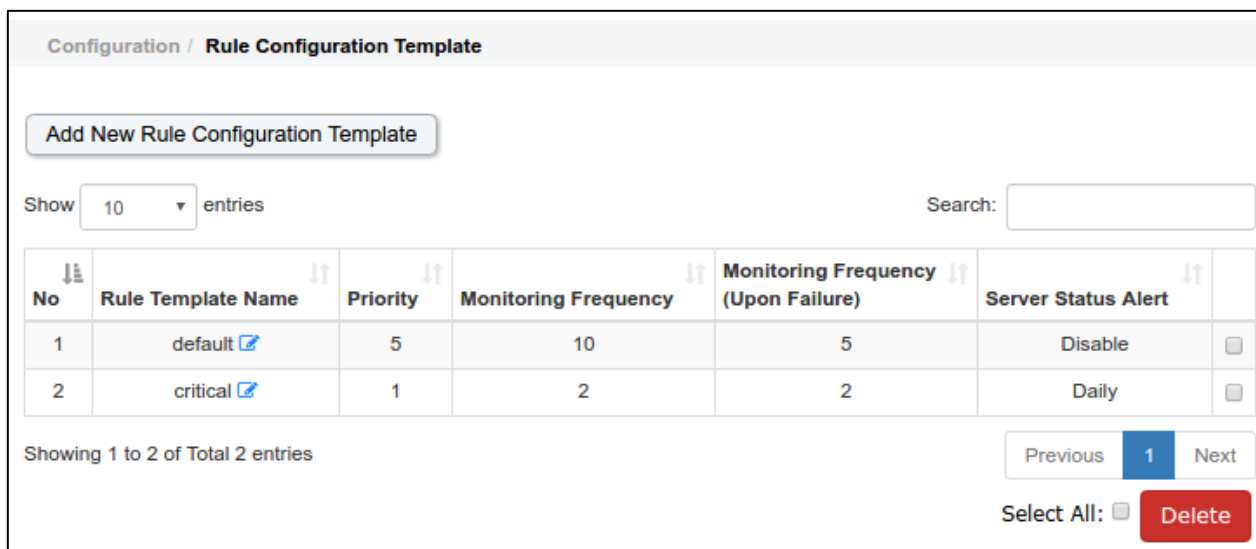


Figure 2-81: Rule Configuration Template

Rule Template Name :	<input type="text" value="critical"/>	Unique name for Rule Configuration Template
Priority :	<input type="text" value="1"/>	Priority for sending sms alerts
Alarm Trigger Mode :	<input type="text" value="1st Trial Fail"/>	<ul style="list-style-type: none"> 1st Trial Fail - Once detect no response, the system will be marked as fail and trigger the alert immediately once all test attempts packet failed. 2nd Trial Fail - Once detect no response, the system will be marked as fail, but triggering the alert only the 2nd trial attempt. The frequency of the 2nd trial attempt will be based on monitoring frequency upon failure.
Total Attempts :	<input type="text" value="5"/>	If Total Attempts set to 0, the system will set as default 10
Test Time Out :	<input type="text" value="5"/>	
Alarm Threshold :	<input type="text" value="5"/>	The threshold that will be used to trigger the alarm. The value should be lower than the Total Attempts. If exceed the value, it will be treated as only trigger the alarm upon all test attempt failed.
Monitoring Frequency :	<input type="text" value="2"/>	<ul style="list-style-type: none"> The frequency (interval) between each Attempt test in minutes. If set to 0, the system will disable the monitoring. It is not recommended to set lower than 5 minutes for actual deployment of the system, as Multiple Windows Service Check will generate quite a lot of network traffic.
Monitoring Frequency (Upon Failure) :	<input type="text" value="2"/>	<ul style="list-style-type: none"> The frequency (interval) between each Attempt test when a test failure had been detected. Customer may prefer to have a smaller value (in minutes) to allow a more regular (frequent) checking when there is a failure. If set to 0, the system will use the value defined in the Monitoring Frequency.
Server Status Alert :	<input type="text" value="Daily"/>	<ul style="list-style-type: none"> Send an alert message to the administrator, to indicate that the sendQuick server is still functioning. This can be configured to be on a certain time of the day (time in HH:MM) or in hourly manner(00-59 minutes)
Server Status Alert Mode :	<input type="text" value="Both"/>	
Server Status Alert Time :	<input type="text" value="08"/> <input type="text" value="-MM-"/>	<ul style="list-style-type: none"> HH - Hour (00 - 23) MM - Minute (00 - 59)
<input type="button" value="Submit"/> <input type="button" value="Reset"/>		

Figure 2-82: Create/Update Rule Template

[Refer to 2.7.1.1](#) for more details.

2.11.2 Alert Configuration Template

Create alert related configuration template, such as alert mode, alert recipients and alert text message.

Configuration / Alert Configuration Template

Show entries Search:

No	Alert Template Name		Alert Text Message	Alive Text Message	
1	alert544 ✎	Continuous	xIPx:xRULEx is not reachable.	test msg	<input type="checkbox"/>
2	alert_infra ✎	Continuous	xIPx:xRULEx is not reachable.	xIPx:xRULEx is reachable.	<input type="checkbox"/>
3	default ✎	Continuous	xIPx:xRULEx is not reachable.		<input type="checkbox"/>

Showing 1 to 3 of Total 3 entries

Select All:

Figure 2-83: Alert Configuration Template

Edit Alert Configuration Template

Alert Template Name : Unique name for Alert Configuration Template

Alert Mode :

- Continuous - the system will send SMS alert to operator base on the Monitoring Frequency defined below.
- Once - the system will send SMS alert to operator one time only, upon detecting the server offline.
- Escalation - the system will send SMS alert follow escalation level settings, upon detecting the server offline.

Alert Settings

SMS Mobile : SMS Mobile - SMS to receive alerts

Email Address : Email - Email to receive alerts

Select Group :

Group Name	Group Members
IT	Operator 1, User 1

Select Group - Select group contacts

Alert Text Message :
The system will use the default message if alert message is set to blank. The default message form is: xIPx:RULEx is not reachable. User can change the message format by creating the text in the textarea above.

Variables in Alert Message

Alive Text Message :
If this field is leave blank, no SMS will be sent.

Figure 2-84: Create/Update Configuration Template

[Refer to 2.7.1.1](#) for more details.

3.0 References

3.1 SMS Check Template

SMS Check is the feature that allow user to send SMS to SendQuick Avera to query real time status or perform server shutdown/restart. Please note that **Allow SMS Check** must be enabled in **Admin Settings**. ([Refer to 2.10.1](#)).

Allow SMS Check : <input type="text" value="Enable"/>	<small>Enable to allow SMS from authorized mobile to check current status of IP, Port, URL, Windows Service, Windows Process, CPU, Disk and Memory</small>
---	--

Figure 3-1: Administrative Settings – Allow SMS Check

Request Type	SMS Template	Description
ICMP Ping	PING <IP>	ICMP Ping to any IP address. Authorized mobile numbers can be configured under 'Admin -> Settings -> SMS Check Authorized Mobile or Group'. Requests from unauthorized mobile number will be ignored.
TCP Port Check	TELNET <IP> <PORT>	Telnet to any Port from any IP address. Authorized mobile numbers can be configured under 'Admin -> Settings -> SMS Check Authorized Mobile or Group'. Requests from unauthorized mobile number will be ignored.
URL Check	URL <URL>	Checking URL. Authorized mobile numbers can be configured under 'Admin -> Settings -> SMS Check Authorized Mobile or Group'. Requests from unauthorized mobile number will be ignored.
Windows Service	SERVICE <DEVICE NAME> <SERVICE NAME>	Checking windows service Authorized mobile numbers can be configured under 'Device Profile -> Authorized Mobile or Group'. This mobile list is authorized to check the service name on this particular device profile only. Requests from unauthorized mobile number will be ignored.
Windows	PROCESS <DEVICE	Checking windows process

Process	NAME> <PROCESS NAME>	Authorized mobile numbers can be configured under 'Device Profile -> Authorized Mobile or Group'. This mobile list is authorized to check the process's memory on this particular device profile only. Requests from unauthorized mobile number will be ignored.
CPU Usage	CPU <DEVICE NAME>	Checking CPU utilization on device Authorized mobile numbers can be configured under 'Device Profile -> Authorized Mobile or Group'. This mobile list is authorized to check the cpu usage on this particular device profile only. Requests from unauthorized mobile number will be ignored.
DISK Usage	DISK <DEVICE NAME> <DISK NAME>	Checking Disk utilization on device Authorized mobile numbers can be configured under 'Device Profile -> Authorized Mobile or Group'. This mobile list is authorized to check the particular disk's usage on this device profile only. Requests from unauthorized mobile number will be ignored.
Memory Usage	MEMORY <DEVICE NAME>	Checking Memory utilization on device Authorized mobile numbers can be configured under 'Device Profile -> Authorized Mobile or Group'. This mobile list is authorized to check the memory usage on this particular device profile only. Requests from unauthorized mobile number will be ignored.
Restart Server	RESTARTSERVER <DEVICE NAME>	Restart server (Note : 'Admin -> Settings -> Allow SMS Restart Server' must be enabled.) Authorized mobile numbers can be configured under 'Device Profile -> Authorized Mobile or Group'. This mobile list is authorized to restart this particular server only. Requests from

		unauthorized mobile number will be ignored.
Shutdown Server	SHUTDOWNSERVER <DEVICE NAME>	Shutdown server (Note : 'Admin -> Settings -> Allow SMS Shutdown Server' must be enabled.) Authorized mobile numbers can be configured under 'Device Profile -> Authorized Mobile or Group'. This mobile list is authorized to shutdown this particular server only. Requests from unauthorized mobile number will be ignored.
Restart Windows Service	RESTARTSERVICE <DEVICE NAME> <SERVICE NAME>	Restart windows service (Note : 'Admin -> Settings -> Allow SMS Restart Windows Service' must be enabled.) Authorized mobile numbers can be configured under 'Device Profile -> Authorized Mobile or Group'. This mobile list is authorized to restart the windows service on this particular server only. Requests from unauthorized mobile number will be ignored.

All SMS Check requests and results will be logged under **SMS Transaction > SMS Check** ([Refer to 2.4.2](#))

3.2 SMS Acknowledgement Templates

User can send Acknowledgement SMS to stop escalation or simply acknowledge receipt of SMS. Please note that **Admin > Settings > Allow Acknowledgement SMS** must be enabled.



Figure 3-2: Administrative Settings – Allow Acknowledgement SMS

3.2.1 SMS Broadcast

User can acknowledge receipt of the SMS by replying 'ACK <case_id>', where <case_id> is the first number appended to message content.

For example,

SMS Message:

5:testing 12345 please acknowledge

In this example, <case_id> = 5 and user should reply with text: ACK 5

All records will be logged under **SMS Transaction > SMS Broadcast** ([Refer to 2.4.1](#))

3.2.2 Network Monitor

User can send ACK or RES to stop escalation of network monitoring alert case. Please note that all case ID for network monitoring transaction has prefix 'M'.

- SMS Template: **ACK <case_id>**
E.g.: ACK M123
- SMS Template: **RES <case_id> <resolved_log>**
E.g.: RES M123 maintenance

All records will be logged under **SMS Transaction > Network Monitor** ([Refer to 2.4.3](#))

3.2.3 Message Filter

User can send ACK to stop escalation of message filtering alert case. Please note that all case ID for message filtering transaction has prefix 'F'.

- SMS Template: **ACK <case_id>**
E.g.: ACK F25

All records will be logged under **SMS Transaction > Message Filter** ([Refer to 2.4.4](#))

3.3 Windows Server WMI Configuration

WMI connection is required to access Windows Server for the following tasks:

1. Retrieve system information (CPU, Disk, Memory utilization)
2. Monitor windows services & Restart windows services if needed
3. Monitor windows processes & Kill windows process if needed
4. Shutdown or Reboot windows server

Enable Remote WMI Access

1. In Windows Server, go to **Administrative Tools > Computer Management**.

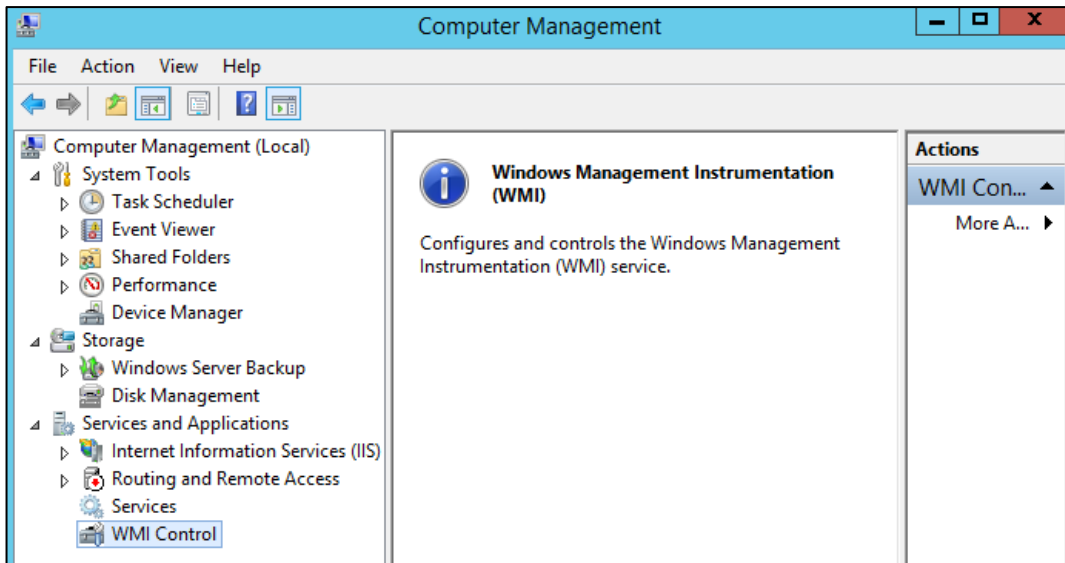


Figure 3-3: Computer Management

2. Right Click on **WMI Control** and select **Properties**.

3. Go to the **Security** tab.

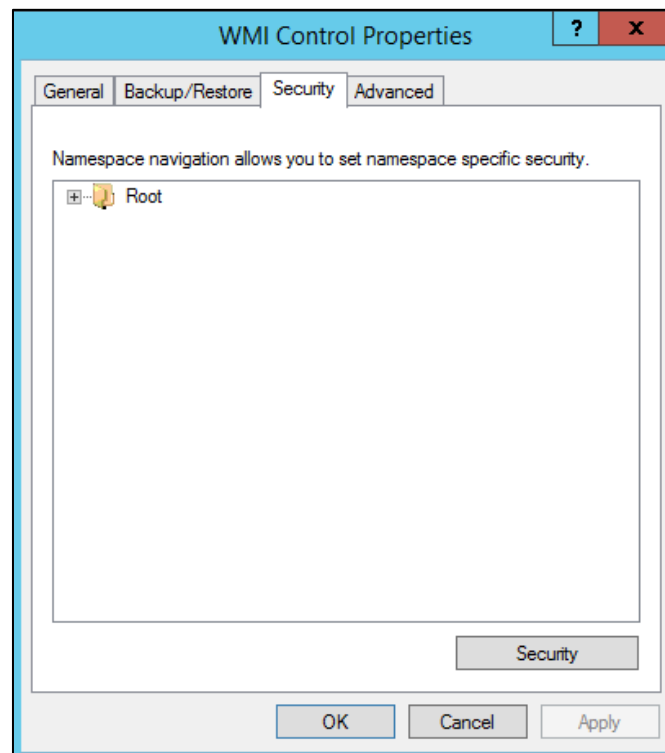


Figure 3-4: WMI Control Properties – Security

4. Select authorized group or username, make sure **Remote Enable** is allowed.

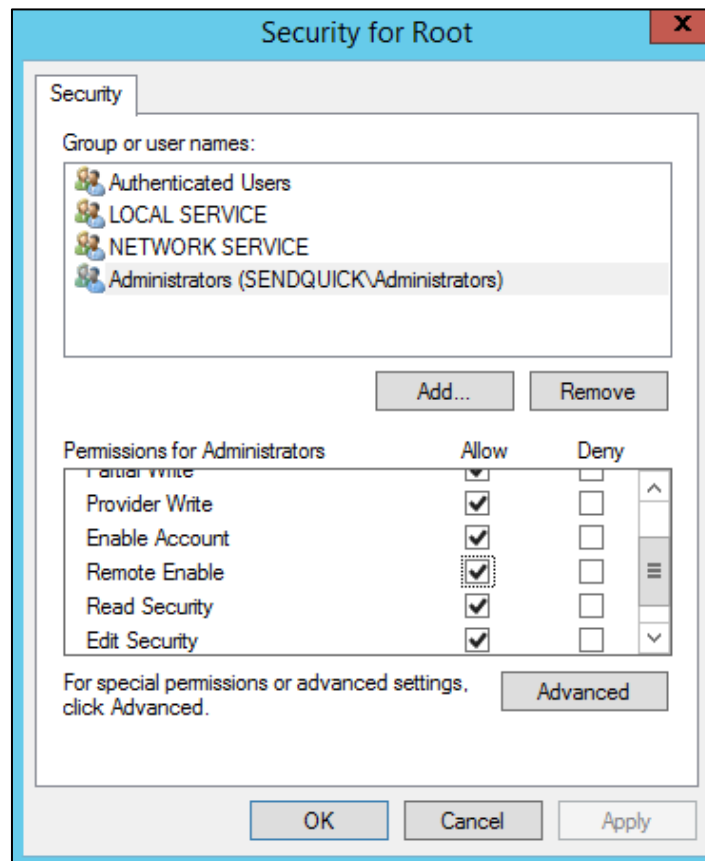


Figure 3-5: Root Permission Configuration