



**SendQuick Server
Licensing Agreement and
Administration User Manual
Version 4.3.3 - 21st July 2020**

Prepared by

TalariaX Pte Ltd

76 Playfair Road
#08-01 LHK2
Singapore 367996

Tel: +65 62802881
Fax: +65 62806882

E-mail: info@talariax.com
Web: www.talariax.com

SendQuick Server Software License Agreement

For SOFTWARE PRODUCT, content and software information marked with © TalariaX or © TalariaX 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. 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 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. 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.

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 include 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 grants 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 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 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 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” or “© TalariaX 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 disclaims 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 has 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 warrants 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 reserves the right to amend the limited warranty period without prior notice.

Customer remedies

TalariaX Pte Ltd entire liability and your exclusive remedy shall be, at TalariaX 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 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 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 has been advised of the possibility of such damages. In any case, TalariaX 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 cannot guarantee that messages sent by using TalariaX's SOFTWARE PRODUCTS for wireless (SMS) messaging reach their addressees. Neither can TalariaX guarantee that the SOFTWARE PRODUCT receives all messages through the used mobile equipment they have been sent to.

TalariaX is 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:

TalariaX Pte Ltd

76 Playfair Road

#08-01 LHK2

Singapore 367996

Tel: 65 – 62802881

Fax: 65 – 62806882

E-mail: info@talariax.com

Web: www.talariax.com

sendQuick Server

Server Administration Manual

Table of Contents

1.0 INTRODUCTION.....	7
2.0 SET-UP PROCEDURE.....	7
3.0 SET-UP AND CONFIGURATION.....	8
3.1 Physical Connections.....	8
3.2 Login Procedures.....	8
4.0 Dashboard.....	9
4.1 System Overview.....	9
4.2 System Usage.....	10
4.3 Modem Status.....	12
5.0 Server Setup.....	14
5.1 IP Configuration.....	14
5.2 SMTP Routing.....	16
5.3 Optional Network Setup.....	17
5.4 High Availability Setup.....	19
5.5 HTTP/HTTPS Proxy.....	19
5.6 System Date & Time Setup.....	20
5.7 Web Interface Logo.....	20
6.0 Messaging Setup.....	21
6.1.1 SMS Messaging Setup - SMS.....	21
6.1.2 SMS Messaging Setup - Email.....	22
6.2 SMS Queue Monitoring.....	23
6.3 SMS Response Action.....	25
6.4 sendQuickASP Routing.....	26
6.5 Sqoope Routing.....	28
6.6 Direct Connection.....	30
6.6.1 Direct Connection – Send SMS (Provider = Other).....	32
6.6.2 Direct Connection – Check Status (Provider = Other).....	35
6.6.3 Direct Connection – Send SMS (Provider = ASP).....	38
6.7 SMPP Route.....	39
6.8 Mobile Instant Messaging Routing.....	41
6.9 Alert Profiles.....	43
7.0 Modem Setup.....	44
7.1 Modem License.....	44
7.2 Modem Dispatch Mode.....	45
7.3 Modem Routing.....	45
7.4 Virtual Modem Routing.....	47
7.5 Modem Monitoring & Respool.....	47
7.6 Modem Priority.....	48
7.7 Modem Time Control.....	48
7.8 IMEI SIM Card Mapping.....	49
7.9 MPM Routing.....	49
8.0 Phone Book & Roster (Optional Item in sendQuick Alert Plus. Default in sendQuick Entera).....	50
8.1 Phone Book Records.....	50
8.1.2 Phone Book Records – Upload by CSV File.....	52
8.1.3 Phone Book Records – by AD/LDAP Setup.....	55
8.2 MIM Phone Book Records.....	58
8.3 Roster Management.....	58
8.4 AD/LDAP OU Alert.....	60
8.5 Delete AD/LDAP Contacts.....	61
9 Filter Rules.....	62

9.1 Email Filter.....	62
9.2 SNMP Trap Filter.....	67
9.3 Syslog Filter.....	68
10 Network Monitor.....	69
10.1 Ping Check.....	69
10.2 URL Check.....	70
10.3 Port Check.....	71
11 Security Setup.....	73
11.1 HTTP Host Permission.....	73
11.2 SMTP Host Permission.....	74
11.3 Email User Permission.....	75
11.4 Relay Host Permission.....	76
11.5 Database Connection Permission.....	77
11.6 Mobile Number Permission.....	78
11.7 System Services.....	79
11.8 SSH Remote Access.....	80
11.9 How to enable SSL Service.....	81
11.9.1 How to Generate SSL Key and Certificate.....	84
11.10 Token Management.....	88
12 Password Management.....	89
12.1 Server Admin Web Login.....	91
12.2 Supervisor Web Login.....	94
12.3 Operator Web Login.....	97
12.4 Console Login.....	100
12.5 SSH Login Account.....	100
12.6 FTP Login Account.....	101
12.7 Database Access Account.....	102
12.8 User Web Access Login.....	102
13 Backup & Diagnostic.....	103
13.1 Generate Backup File.....	103
13.2 Automated Backup.....	104
13.3 Restore Backup File.....	104
13.4 Generate Diagnostic File.....	105
13.5 Apply Patch.....	106
14 Usage Logs.....	107
14.1 Message Log.....	107
14.2 Conversation Summary.....	108
14.3 Email Log.....	109
14.4 Alert Log.....	110
14.5 System Log.....	111
14.6 Audit Log.....	112
14.7 Usage Statistic.....	113
14.8 Maintenance and Report.....	114
15 System Test Tools.....	116
15.1 SMTP Connectivity Test.....	116
15.2 Ping Test.....	116
15.3 Traceroute Test.....	117
15.4 Port/Telnet Test.....	117
15.5 Send Test SMS.....	118
15.6 Web Based Terminal.....	120
15.7 Debug Mode.....	120
16 SMS Specifications.....	121
16.1 Email API.....	121
16.2 REST API - SMS.....	122
16.3 REST API - MIM.....	124
16.4 Receive SMS via sendQuick Server.....	126
16.5 Sending Message to Overseas Mobile Number.....	127
17 Shutdown, Restart and Logout from the System.....	127
18 HIGH AVAILABILITY CONFIGURATION.....	128

19	CONSOLE CONFIGURATION AND SETTINGS.....	131
19.1	Configure sendQuick IP via Console.....	131
19.2	Reset Web Login Password.....	133
20	TROUBLE SHOOTING.....	134
20.1	I have forgotten the IP address of my sendQuick server. How do I check?.....	134
20.2	I have done all the set-up. I tried to SMS via the web interface as explained in section 3.12 but no SMS was received. Why?.....	134
20.3	I set the entire configuration in the server set-up accordingly but I still cannot send e-mail to SMS from my e-mail software. Why?.....	134
20.4	I cannot access the sendQuick Server from my local PC even though it is already in the network and some of my other colleagues can use it. Why?.....	135
20.5	I realized that the server only provides for one e-mail and one HTTP response. How do I allow SMS enquiries to more than one applications at one instant?.....	135
20.6	I am getting email alerts on my administrator email account stating that the modem is not found or having problem. What should I do?.....	135
20.7	I am getting continuous alert messages stating that there is no modem and the alert message is occurring every second or I cannot send SMS despite able to access the system via web interface. What is the solution?.....	136
20.8	The system is not sending SMS. What are the troubleshooting steps?.....	136
20.9	had configured the reminder and escalation function and I am receiving the SMS. However, the Reminders and Escalations are sent even after I sent the correct reply (Acknowledgment).....	137
20.10	How to correctly activate or restart the modem.....	137
20.11	When sendQuick cannot detect modem.....	138
20.12	How modem works.....	138
20.13	How to perform modem hard reset.....	138
20.14	Why SIM Barring / Fair-Use Policy.....	138
21	Modem Error Code.....	139
	Error code 3: SIM not allow to register to the network.....	139
	Error code 10: SIM card not detected.....	139
	Error code 13: Modem error status, SIM failure.....	139
	Error Code 21: SMS Rejected.....	139
	Error Code 38: SIM card failed.....	140
	Error code 111: Operator Network Coverage issue.....	140
	Error code 429: Too many request.....	140
	Error code 500: Operator reject code.....	140
	Error code 512/513: Operator Explicit Deny or Network Error.....	141

SENDQUICK SERVER ADMINISTRATION MANUAL

1.0 INTRODUCTION

Welcome to sendQuick Server Administration User Manual. This document is prepared for the administrator, as a guide for configuring the sendQuick SMS Server for sending and receiving SMS.

The Administrator will configure the sendQuick Server for it to work in your company's network to send and receive SMS. The Administrator will need to work on the network configuration first, which is the Server Setup. Once you had configured the IP address and the relevant network setup, you can access sendQuick from any workstations using a web browser.

This manual is a consolidated document for all sendQuick servers. Therefore, some of the items are found in some sendQuick models. There will be an indication on the features of they are not applicable for some of the models.

2.0 SET-UP PROCEDURE

The sendQuick Server is designed to be set up and configured easily. It will save you time and resources and enable your corporation to have a SMS server within 10 - 20 minutes.

The following are the steps to set-up the system fully.

1. Connect the power supply and monitor to the system
2. Power-up the system and wait for the system to be fully started (the IP routing table shown on the monitor. Refer to section 5.0)
3. Connect a cross cable to ETH0, launch a web browser and access via the default IP 192.168.1.8. Login using the username & password : The default username and password can be found in the "your password" envelope or contact support@talariax.com.
4. Configure the Server Set-up (IP address and others)
5. Configure the SMS System Set-up.
6. Plug in the Ethernet (LAN) cable
7. Connect the GSM/3G/4G modem and insert the SIM card in the modem

You will be ready to send and receive SMS messages when you have performed the steps above.

<p>Note: Get assistance from your system administrator if you do not have the IP addresses for the server and gateway</p>
--

3.0 SET-UP AND CONFIGURATION

3.1 Physical Connections

The first step in configuring the sendQuick Server is to establish all the physical connections. This includes power cable, modem connection (USB or serial), SIM card, keyboard (optional), mouse (optional) and monitor. The Ethernet (LAN) connection will be connected at a later stage (we will advise you in this document) after the Server Setup is completed.

Note: We suggest that you connect the Ethernet (LAN) later as the default IP setting (192.168.1.8) may conflict with your existing network.

3.2 Login Procedures

After completing the physical connections, you can power-up the system and wait for it to start. It will take about 1-2 minutes to be fully started. The system is fully started once the IP routing information is shown on the monitor

Connect a cross-cable to ETH0, use a web browser to access default IP: 192.168.1.8 and you will see the web login page as shown on Figure 3-1. If you did not see 'Admin Login' button on this screen, please click the 'Administrator Login' that displayed on your screen.

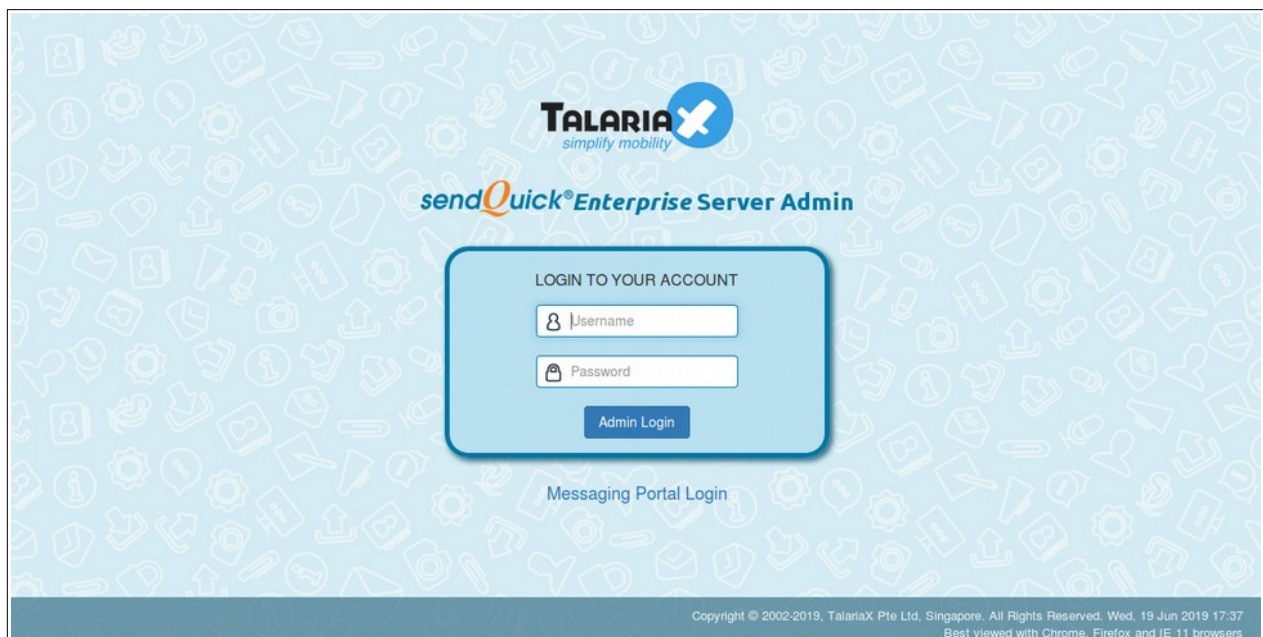


Figure 3-1: Web Administrator Log-in Page

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 or contact support@talariax.com.

For security reason, please change the default passwords to something new regularly. You can change the password through the **Password Management** menu after logging-in. The procedure to change password

is explained in Section 12.

4.0 Dashboard

4.1 System Overview

After logging-in, you will be directed to the **Dashboard** screen as shown in Figure 4-1:

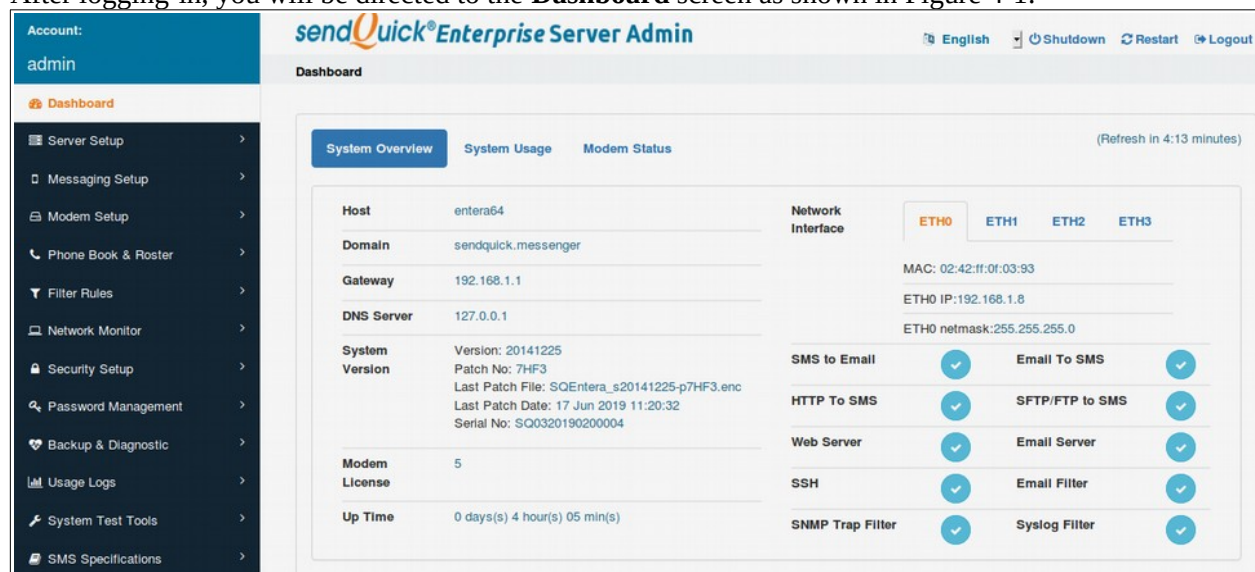


Figure 4-1: Dashboard

The information that displays on this screen (Figure 4-1) are System's Host name, Domain name, Gateway, DNS Server, System version, Number of modem license, System up time, IP addresses for ETH0, ETH1, ETH2, ETH3 and sendQuick system services that enabled or disabled.

By scrolling down the Dashboard > System Overview screen, system displays the health status for the last 6 hours by default (Figure 4-2). You will have a real-time overview of the system health status of CPU Usage, Memory Usage, sendQuick Derive, Message Storage and System Drive.

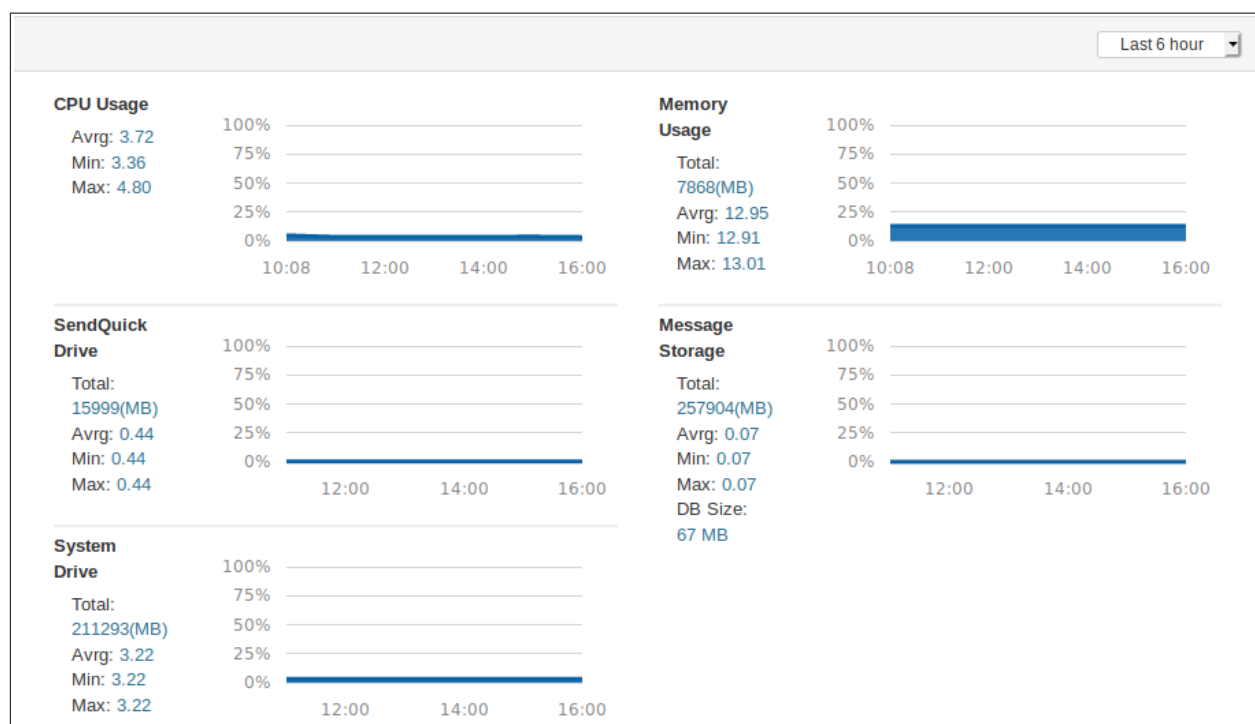


Figure 4-2: Dashboard – System Health Status

Should you required to check a longer period for the system health status, select the predefined ranges from 'Last 6 hour' till up to 'Last 30 days' from System Overview screen (Figure 4-3).

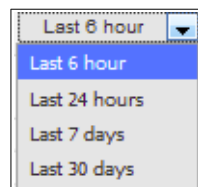


Figure 4-3: System Health Status Duration

From the Dashboard, user can quickly access information to System Usage and Modem Status screens.

4.2 System Usage

From Dashboard > System Usage. Figure 4-4 below shows the sendQuick's System Usage in real-time. Access to the SMS, Sqoope, MIM or Email menu tabs follow-by respective 'Functional Color buttons' to view the status for SMS Queue, SMS Sent, SMS Received and Unsent SMS.

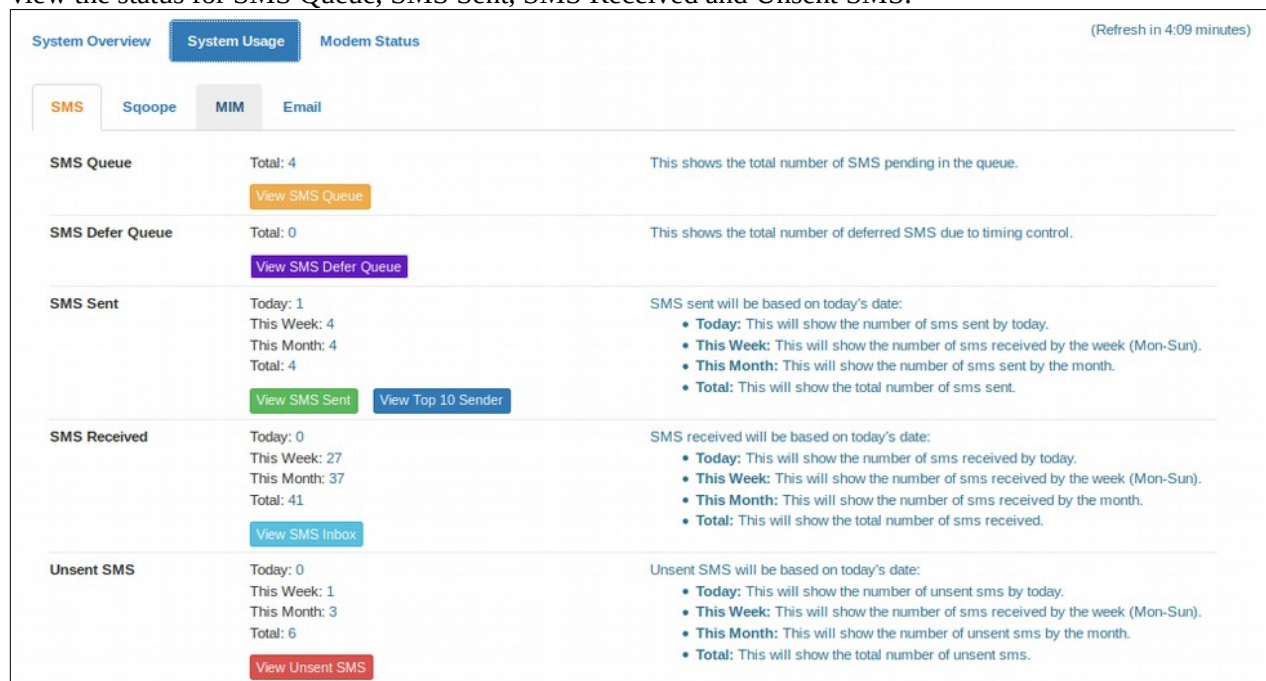


Figure 4-4: System Usage - Overview

By selecting the respective 'Function Color button' from Figure 4-4 System usage – Overview screen, for example '**Green – View SMS Sent**', system will display SMS Sent status in detail (Figure 4-5).

Usage Logs > Message Log

Queue Sent Unsent Inbox

SMS MIM Sgoope

Search From 20/12/2019 To 20/12/2019

Show 100 entries Search:

No	Date & Time	Delivery Date	Turnaround Time	Sender	Mobile Number	Message	IMEI	Priority	
1	20/12/2019 10:37:41	20/12/2019 10:37:47	00:12	192.168.1.95 (admin)	94506718	testing no 2	359180083538501	1	<input type="checkbox"/>
2	20/12/2019 10:37:39	20/12/2019 10:37:43	00:09	192.168.1.95 (admin)	94506718	testing no 3	352561050728968	1	<input type="checkbox"/>

Save CSV Save Excel Save PDF Refresh Empty Outbox Delete

Showing 1 to 2 of total 2 records Previous 1 Next

Figure 4-5: System Usage – Sent – SMS

SMS(es) that sent successfully will be shown on this screen (Figure 4-5), users are able to view the detail by filtering the From/To duration by date, save the data to CSV, Excel or PDF format or to delete one or multiple records from the audit log.

SMS(es) that sent unsuccessfully will be shown on 'Unsent' section (Figure 4-6), users are able to filter the detail by selecting the date range (From/To), save the data to CSV, Excel or PDF format or to delete one or multiple records.

On the Remark column, system will highlight the possible cause of the error when failed to send a sms. Should user wish to resend the SMS in Unsent status, checked the checkbox of the SMS follow by select the Resend button, system will try to resend the sms.

Usage Logs > Message Log

Queue Sent Unsent Inbox

SMS MIM Sgoope

Search From 20/12/2019 To 20/12/2019

Show 100 entries Search:

No	Date & Time	Sender	Mobile Number	IMEI	Message	Remark	
1	20/12/2019 10:51:30	192.168.1.95 (admin)	987654321	352561050728968	test	Error:513 ; mobile network or target recipient error	<input type="checkbox"/>

Save CSV Save Excel Save PDF Refresh Resend Empty Unsent Delete

Showing 1 to 1 of total 1 records Previous 1 Next

Figure 4-6: System Usage – unsent – SMS

4.3 Modem Status

From Dashboard > Modem Status. Figure 4-7 below shows the Modem Status - Overview, which displays modem overview status like Number of modem(s) detected and activated, Modem Host and Modem IMEI, whereby;

- Modem Host = Localhost, modem(s) that connected directly to sendQuick server.
- Modem Host = ModemPool, modem(s) that connected to a modem pool appliance.

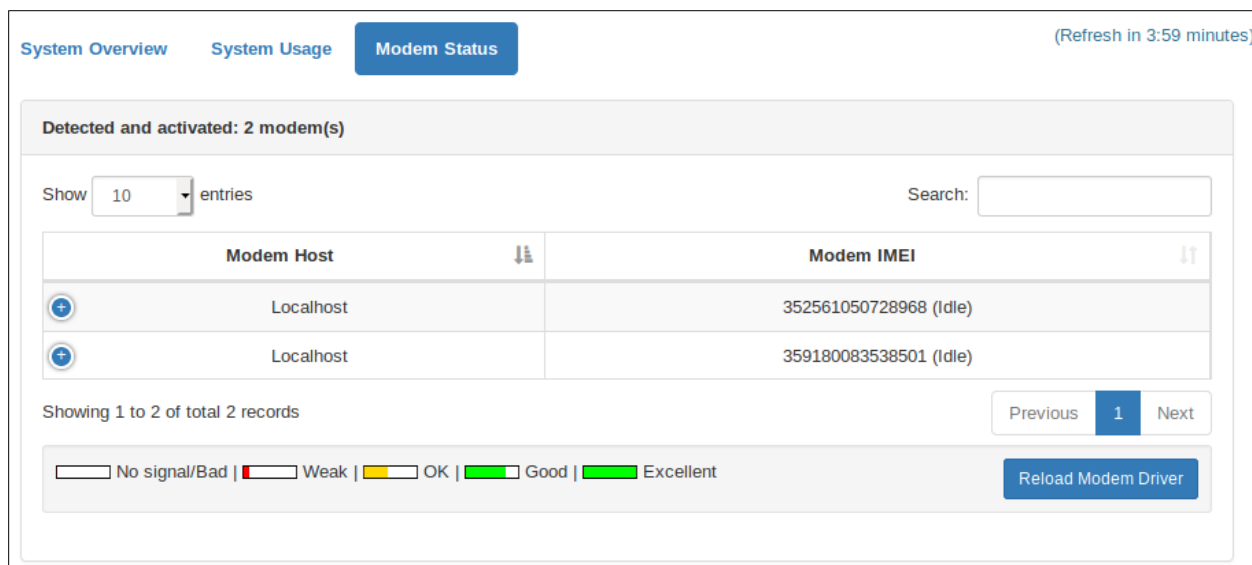


Figure 4-7: Modem Status – Overview

Select the 'Blue +' sign on on Figure 4-7, system will expand the display as per figure 4-8.

Figure 4-8 displays modem status detail such as the Modem IMEI, Modem manufacture data, SMSC (short message service center), Operator Info (Telco/Carrier network), SIM Card Number (user definable on Modem Setup > IMEI SIM Card Mapping) and the Signal Strength of each connected modem.

User will only see the modem status when a modem is detected with a valid SIM card, otherwise please consult your distributor or TalariaX.

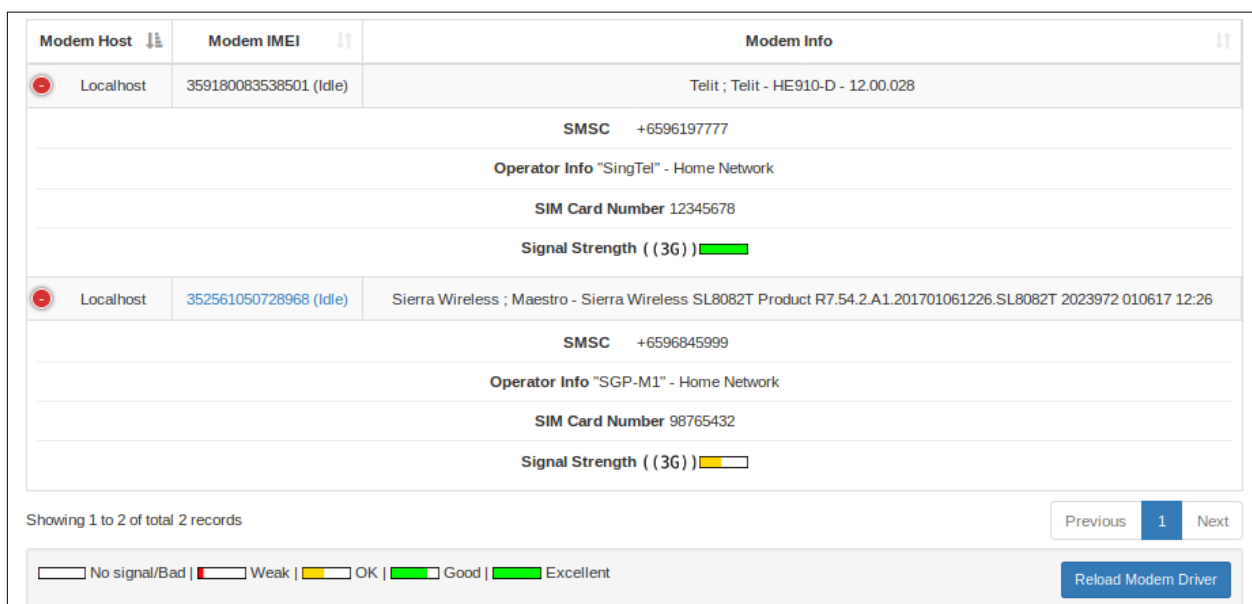


Figure 4-8: Modem Status - detail

On the left is the navigation (Menu) bar for the sendQuick server. Each menu refers to a specific function as described below:

- a) **Server Setup**
 - to prepare and configure the server to connect to the network in a proper manner
- b) **Messaging Setup**
 - to configure the system for sending and receiving messages, as well as to interface with external application for receiving SMS messages
- c) **Modem Setup**
 - to view the modem status, configure the modem configuration and routing information
- d) **Phone Book & Roster**
 - to create shifts and phone book for filter rules usage
- e) **Filter Rules**
 - to perform the filter configuration (Email/SNMP Trap/Syslog) for selective SMS messaging based on configured rules
- f) **Network Monitor**
 - to perform the ICMP Ping, Port Check and URL Check for monitoring IP address and send SMS when IP is unavailable and restored
- g) **Security Setup**
 - to configure the permission for certain IP addresses that are allowed to send SMS messages for sendQuick server
- h) **Password Management**
 - change the default log-in password in the system
- i) **Backup and Diagnostic**
 - to backup and restore the configuration settings as well as generating diagnostic file
- j) **Usage Logs**
 - to view the logs of the system and messages (sent, received, failed and in queue)
- k) **System Test Tools**
 - perform sending SMS for testing or for other route testing information
- l) **SMS Specifications**
 - these are the specifications and format to send messages to sendQuick server.

5.0 Server Setup

The administrator will need to set-up the important network configurations here. Items to be configured as described below:

- IP Configuration
- SMTP Routing
- Optional Network Setup
- High Availability Setup
- HTTP/HTTPS Proxy
- System Date & Time Setup
- Web Interface Logo

5.1 IP Configuration

Server Setup > IP Configuration

Host and Domain name

Host: This is the host and domain of the system. A typical example: smsgateway.company.com, whereby the hostname = smsgateway and the domain = company.com.

Domain:

IP Address This set the TCP/IP IP address. Please refer to the network administrator for the exact value.

Netmask This set the TCP/IP network mask. Please refer to the network administrator for the exact value.
(If unsure, set to: 255.255.255.0)

Gateway This set the network gateway. Please refer to the network administrator for the exact value.

DNS Server
 This set the domain name service server. Basically it will be used by the system to perform domain or host name resolution to the corresponding IP. Please refer to the network administrator for the exact value.
(If unsure, set to: 127.0.0.1)

Email Gateway ☒ Check to use hostname for all emails.

Figure 5-1: IP Configuration

a) Host and Domain name

The server hostname is the name assigned for the server. This can be of any name, like 'sendquick', or use a name that is related to your company. Domain is the registered domain in your network, e.g.: company.com.sg. Use a valid name if you have a DNS to perform name resolution.

b) IP Address

This is the IP address assigned to the sendQuick server. You can use an internal or public IP, depending on your network configuration. This IP is used to identify the server and will be used in all communications between sendQuick and external applications. The default IP is 192.168.1.8.

c) Netmask

This is the subnet mask value of the network. This defines the network that you are connected to. Most networks use 255.255.255.0, which is also the default value in the system.

d) Gateway

This refers to the IP address of your machine that does routing to other machines in another network. For most networks, this refers to your router's IP address.

e) DNS Server

This refers to machines that will resolve a valid hostname and domain name. This is usually a server that is connected to the Internet with the capability to update the hostname via the public Internet or via an internal network (for internal DNS). If you do not have a DNS server, set the IP to 127.0.0.1. This allows sendQuick to obtain updates from Internet periodically. If there is more than one DNS server IP, enter each IP address line by line.

Note: If you are using a firewall, please configure your firewall to allow UDP connection (port 53) as DNS server (127.0.0.1) uses UDP for data update.

f) Check to use Hostname for all emails

By checking on this field, all emails that are sent out from sendQuick server (e.g. failure notice, incoming SMS and others.) will bear the Hostname that you had configured in the Hostname section in the Server Setup.

When you have completed the server set-up, select the '**Save**' button (Figure5-1). This however does not activate the server with the newly assigned IP address, to enable sendQuick with newly assigned IP, simply click on the '**Activate Setting**' button (Figure 5-2) when prompted. After activation, you will be prompted to login to the system again with the new IP address.

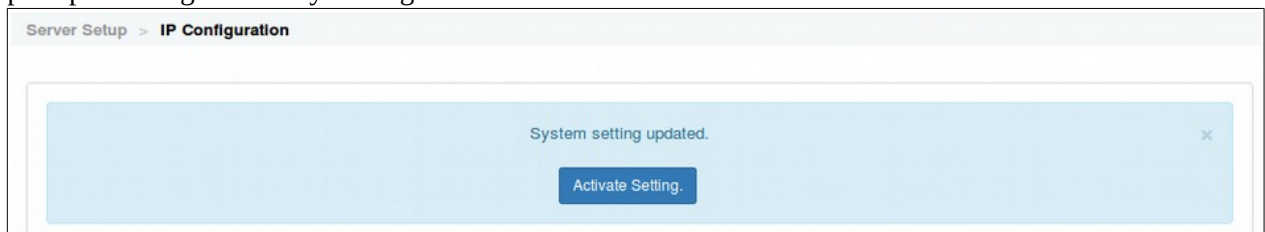


Figure 5-2: Activate Setting

After this configuration, you can choose to access the server from other computers on your network and not directly from the server. If you wish to do so, just perform the following steps:

Action:

1. Open your Internet browser.
2. Type in [http://the new IP address](http://192.168.1.8). If your new IP is 192.168.1.8, you should access <http://192.168.1.8>
3. You should see a screen as depicted in Figure 3-1.

Note: Please remember to plug-in the ethernet (LAN) cable before you access the server via the network. You can connect the ethernet cable to the server now.

5.2 SMTP Routing

The screenshot shows the 'SMTP Routing' configuration page. At the top, there's a 'Default Email Gateway' section with a text input 'Localhost' and buttons 'Edit' and 'Test Connection'. Below this is the 'Static Email Route' section. It includes a 'Show' dropdown set to '10' and a 'Search' input. A table lists the static email routes:

No	Target Email/Domain/Host	SMTP Server IP/Host	Require Authentication	Description	Connection	
1	mail.talariax.com	mail.talariax.com	✓	Talariax email Server	Test	<input type="checkbox"/>

Below the table are buttons 'Add New Record' and 'Delete'. At the bottom, it says 'Showing 1 to 1 of total 1 records' and has 'Previous', '1', and 'Next' navigation links.

Figure 5-3: SMTP Routing Configuration

- Default Email Gateway.** Select the **Edit** button from Figure 5-3, this refers to the SMTP server that will send email out to the Internet. If you have an email server or use an email SMTP gateway (check with your email administrator), use that IP in the sendQuick server. Else, insert 127.0.0.1 to use the internal SMTP in sendQuick server.

Figure 5-4 is an example of the SMTP gateway configuration:

The screenshot shows the 'Edit Default Email Gateway' dialog box. It contains the following fields and options:

- SMTP Server IP/Host ***: mail.talariax.com
- Port ***: 587
- Require Authentication**: ☒
- Connection Security**: SSL/TLS (dropdown)
- Authentication Method**: LOGIN (Default) (dropdown)
- Username**: support@talariax.com
- Password**: (masked with dots)

At the bottom right are 'Save' and 'Cancel' buttons.

Figure 5-4: SMTP Default Email Gateway

- Static Email Route.** You can also fix the SMTP static routing in this configuration by matching destination host or domain. This can be configure by selecting **Add New Record** from Figure 5-3.

Note: If you are using Exchange/Lotus Notes as your SMTP, please configure the DNS to assign a valid domain as well as the MX record (in Exchange/Lotus) for proper SMTP routing.

5.3 Optional Network Setup

sendQuick supports up to four (4) network ports. This section allows administrator to configure the additional 3 optional network ports (ETH1, ETH2 and ETH3)

Server Setup > **Optional Network Setup**

Network Interface: **ETH1** | ETH2 | ETH3

MAC: 00:90:0b:37:89:00

ETH1 IP:

ETH1 netmask:

This will set the IP and netmask for ETH1. Please consult your network administrator for correct settings.

Figure 5-5: Optional Network Setup – eth ports

These 3 optional network ports (ETH1, ETH2 and ETH3) allows sendQuick to be connected to additional 3 different network segments and accept request to send SMS from these segments. Hence, sendQuick can support up to four (4) different network segments in one (1) appliance.

Static TCP/IP Route

This set the additional static network routing into the system. This option facilitate the system to access a server that require different gateway instead of the default gateway specified above. Format: *target machine:target gateway* eg: If a machine IP: 10.1.1.10 require specific gateway 10.1.1.2, set as: 10.1.1.10:10.1.1.2

Static TCP/IP Network Route

This set the additional static network routing. This option facilitate the system to access a network that require different interface. Format: *target network:target netmask::target gateway:network interface* eg: If a network: 10.1.1.0 with netmask 255.255.255.0, interface is eth1 and default gateway is 10.1.1.1, set as: 10.1.1.0:255.255.255.0:10.1.1.1:eth1

Email Virtual Domain

Additional email domain for sendQuick to accept emails other than the Host + Domain configuration in the Server Setup page. Specify each additional domain as a new line. Leave blank if not applicable.

Open Default Web Service port 80 ☒ Yes ☐ No

Additional Web Service TCP Port

This will enable the web server to listen to additional TCP port for web connection. Leave blank or 'NA' if not applicable

System Email Address

Set the default sender address for system generated email. Default is sms@<sendquick IP or domain>

Email Size Limit MB Default to 15MB

Figure 5-6: Optional Network Setup

By scrolling down from the Figure 5-5, user will be able to configure the optional parameters of the optional network setup (Figure 5-6) for:

- **Static TCP/IP route.** This set the additional static network routing into the system. This option facilitate the system to access a server that require different gateway instead of the default gateway specified above. Format: *target machine:target gateway* eg: If a machine IP: 10.1.1.10 require specific gateway 10.1.1.2, set as: 10.1.1.10:10.1.1.2
- **Static TCP/IP Network Route.** This set the additional static network routing. This option facilitate the system to access a network that require different interface. Format: *target network:target netmask::target gateway:network interface* eg: If a network: 10.1.1.0 with netmask 255.255.255.0, interface is eth1 and default gateway is 10.1.1.1, set as: 10.1.1.0:255.255.255.0:10.1.1.1:eth1
- **Email Virtual Domain.** Additional email domain for sendQuick to accept emails other than the Host + Domain configuration in the Server Setup page. Specify each additional domain as a new line. Leave blank if not applicable.
- **Open default Web Service Port 80.** default is Yes, select 'No' to disabled the port 80.
- **Additional Web Service TCP Port.** This will enable the web server to listen to additional TCP port for web connection. Leave blank or 'NA' if not applicable
- **System Email Address.** Set the default sender address for system generated email. Default is sms@<sendquick IP or domain>
- **Email Size Limit.** Default is 15MB

5.4 High Availability Setup

sendQuick supports High Availability (HA) to ensure continuous SMS delivery for your applications. This is an optional item (contact your distributor or TalariaX for pricing) and is only available for selected models; **sendQuick Alert Plus**, **sendQuick Entera**, **sendQuick Conexa** and **sendQuick Avera**. A step-by-step approach is documented in section 18 in this Manual.

5.5 HTTP/HTTPS Proxy

sendQuick supports HTTP/HTTPS Proxy. This section allows administrator to configure the optional HTTP/HTTPS proxy (Figure 5-7).

Server Setup > HTTP/HTTPS Proxy

Status: Enable

Proxy Server IP: 192.168.1.10

Port: 1080

User Name: admin

Password: *****

Confirm Password: *****

Exclude IP List: 192.168.1.15, 192.168.1.20, 10.10.1.8

Domain/IP in the list will bypass this proxy server.

Test Connection Save Reset

Figure 5-7: HTTP/HTTPS Proxy Setup

The available parameters on HTTP/HPPTS Proxy setup screen are:

- Status – Disable / Enable
- Proxy Server IP
- Port
- User Name
- Password
- Confirm Password
- Exclude IP List, domain/IP in the list will be bypass this proxy server.

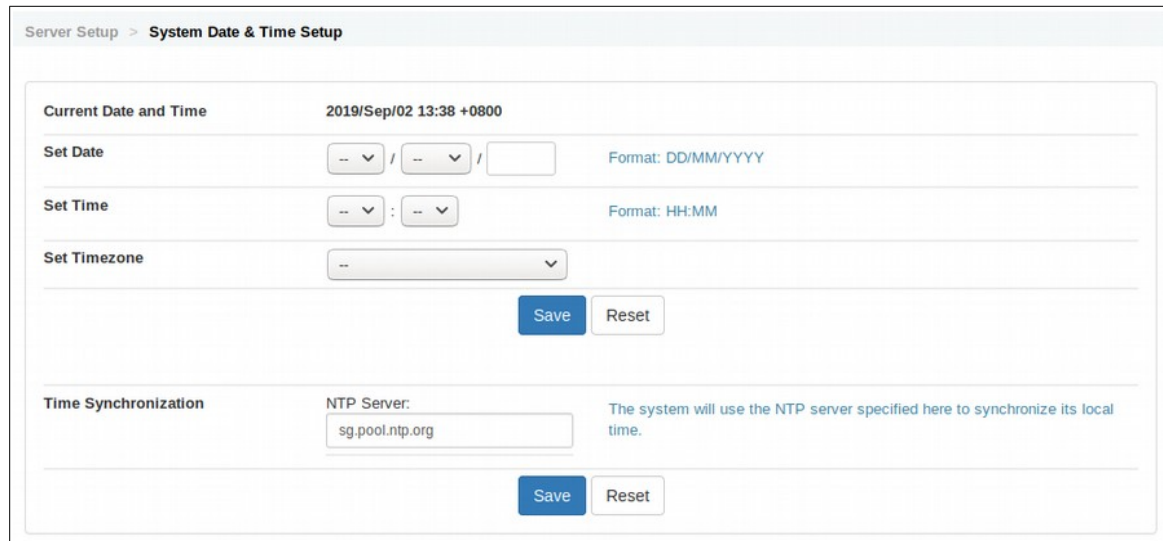
Click on the '**Test Connection**' button when ready for initial testing

When you have completed the set-up, select the 'Save' button.

Click the 'Reset' button to clear the screen and reenter the parameters

5.6 System Date & Time Setup

The server time is configured manually or automatically updated with NTP servers eg 'sg.pool.ntp.sg' (Figure 5-8). You can also manually configure the date, time and timezone as shown in Figure 5-8.



The screenshot shows the 'System Date & Time Setup' page. At the top, it says 'Server Setup > System Date & Time Setup'. Below this, there's a section for 'Current Date and Time' showing '2019/Sep/02 13:38 +0800'. Underneath, there are three rows: 'Set Date' with dropdowns for day, month, and year, and a text field for the year, with a format hint 'Format: DD/MM/YYYY'; 'Set Time' with dropdowns for hour and minute, and a text field for the minute, with a format hint 'Format: HH:MM'; and 'Set Timezone' with a dropdown menu. Below these are 'Save' and 'Reset' buttons. The next section is 'Time Synchronization', which has a text field for 'NTP Server:' containing 'sg.pool.ntp.org', a description 'The system will use the NTP server specified here to synchronize its local time.', and another set of 'Save' and 'Reset' buttons.

Figure 5-8: System Date & Time Setup

5.7 Web Interface Logo

This enables administrator to add the company logo to the login page and also at the header of each of the page (Figure 5-9). Supported image formats are gif, jpeg, jpg, png and bmp. All images will be converted to a maximum height of 40 pixels.



The screenshot shows the 'Web Interface Logo' page. At the top, it says 'Server Setup > Web Interface Logo'. Below this, there's a section for 'Select Image File' with a 'Choose File' button and a text field showing 'No file chosen'. To the right, there's a note: 'Image format allowed : (gif,jpeg,jpg,png,bmp). All images will be converted to maximum height of 40 pixels'. Below the 'Choose File' button are 'Upload' and 'Remove Current Image' buttons.

Figure 5-9: Web Interface Logo

6.0 Messaging Setup

Messaging Setup describes the interaction between sendQuick server and your applications for sending and receiving SMS. 2 main functions to be configured are SMS and Email Pattern:

6.1.1 SMS Messaging Setup - SMS

Figure 6-1: SMS Messaging Setup - SMS

- a) **Total SMS per Message.** Messages can be combined into long SMS (concatenated SMS) if it is selected. Do note that the ability to display long message format is phone dependent. This will set the maximum number of SMS per message. If "long SMS" is enabled, the system will attempt to send the SMS as concatenated messages. Mobile phone that support concatenated messages will join all messages and display it as a single SMS. Note:
 - For concatenated SMS, maximum length for each part is 153 characters.
 - Some phone may not support concatenated SMS, such phone may not display the the received SMS properly.

- b) **SMS to Email Function.** The administrator can enable or disable this function by selecting the checkbox. This will allow users to send email to SMS message.

The format to send is: ***EM<space>Recipient Email Address<space>Message Content.***

Send this SMS (in the format stated) to your SIM card number attached to the server. This SMS message will be converted to an email message and sent to the intended recipient.

- c) **Email to SMS Service.** The function can be enabled or disabled, If its disabled, all email send too SMS request will be discarded.

Enable message status return to sender, if user require the status of email SMS to be auto response to sender, please select the checkbox to enable this function.

- d) **HTTP to SMS Service.** This option will enable or disable this function, if disabled, all HTTP to SMS request will be discarded.
- e) **SFTP/FTP to SMS Service.** This option will enable or disable FTP to SMS service. If disabled, all FTP to SMS request will be disabled.

6.1.2 SMS Messaging Setup - Email

This feature will scan and search for the mobile (phone) number by using Regular Expression to match the numbers found in the email content. The matched numbers will be used as the recipient mobile (phone) to send the SMS message.

Messaging Setup > SMS Messaging Setup

SMS **Email**

Email SMS Format

Includes: (Please check at least one)

- ☐ Sender Email Address
- ☒ Subject
- ☒ Message Body
- ☒ Enable to Preserve Content Formatting
- ☒ Enable to auto-convert HTML entity

This defines how the incoming email will be formatted to send out as SMS.

This feature will scan and search for the mobile (phone) number by using Regular Expression to match the numbers found in the email content. The matched numbers will be used as the recipient mobile (phone) to send the SMS message.

Email Address Username

RegEx Pattern To Extract Mobile Number

Sample Regular Expression:

<code>(d+)</code>	The system will extract all integer numbers from the message content.
<code>([+65]d{10} [89]d{7})</code>	Regular expression for Singapore Mobile numbers. The system will extract all numbers start with +65 or 8 or 9

Save **Reset**

Figure 6-2: Email Pattern Matching

The available parameters on how to define the incoming email to be formatted are:

- Sender's email addressees
- Emails' Subject/Header
- Email's Messages Body
- Enable to Preserve Content Formatting
- Enable to auto-convert HTML entity

Checked/Unchecked on the selection box to enable or to disable the functional.

Regular Expression Pattern to Extract Mobile number, as per figure 6-2, sendQuick will search and extract incoming emails with predefined patterns, the mobile number should be prefixed with 8 or 9 follow-by 7 digits number or if prefixed with 65, sendQuick will read the next 10 digits number to form a complete mobile number for Singapore, following are the valid mobile numbers for Singapore as an example:

- ✓ 81234567
- ✓ 91234567
- ✓ 6581234567
- ✓ 6591234567

6.2 SMS Queue Monitoring

a) Queue Threshold Monitoring – Threshold Counter

This feature allows the administrator to be alerted if there is more than X number of messages in the SMS queue. The alerts can be via email or SMS. The messages to be sent (when threshold exceeded and back to normal) is configurable. To disable, set it to 0 or Threshold Exceed alert message is leave blank or set as 'NA',

b) Queue Threshold Monitoring – Threshold Time (in minute)

This feature allows the administrator to be alerted within the predefined threshold timing in minute if there is more than X number of messages in the SMS queue. To disable, set it to 0.

c) Failure Notice Email Account

When there is an error SMS message or if the message is not sent, sendQuick server will inform the sender via HTTP Post or E-mail. Please specify the HTTP URL address or e-mail address for this purpose. You can enter multiple email address by entering one (1) email per line.

d) Threshold Exceed Message

The system will send a notification to administrator with the message specified in the Threshold Exceed Message. If Threshold Exceed Message is left blank or set as 'NA', no SMS will be sent to mobile number when the pending SMS is reached the Threshold Counter.

e) Threshold Normalize Message

The system will send a notification to end users with the message specified in the Threshold Normalize message. If Threshold Normalize message is left blank or set as 'NA', no SMS will be sent to mobile number when the pending SMS is less than the Threshold Counter.

f) Spool expiry (in hour(s))

The system will delete expired messages from the queue according to the duration (hour) configured here. To disable, set to '0'.

g) Failure Notice URL

This URL will be used by the system to reply to an application (using HTTP Post) if the SMS failed to send. Set to 'NA' to disable it.

h) Failure Notice Email Account

The system will send an email notification to administrator if the SMS failed to send. Set to 'NA' or leave it blank to disable it.

Queue Threshold Monitoring	Threshold Counter: <input type="text" value="100"/>	<p>Enter the number of SMS in the queue that would trigger the alert.</p> <p>NOTE:</p> <ul style="list-style-type: none"> The system will send the Threshold Exceed alert to the list of mobile numbers or emails (one entry per line) if the SMS pending in the queue reach the Threshold Counter. Once the pending message is less than the Threshold Counter, the system will send a notification to end users with the message specified in the Threshold Normalize message. If Threshold Normalize message is left blank or set as 'NA', no SMS will be sent to mobile number when the pending SMS is less than the Threshold Counter. Queue Threshold Monitoring will be disabled if Threshold counter is set as '0', mobile number list or Threshold Exceed alert message is leave blank or set as 'NA'.
	Threshold Time (in minute): <input type="text" value="10"/>	
	Mobile number:	
	Email:	
	Threshold Exceed Message:	
	Threshold Normalize Message:	
Spool expiry	<input type="text" value="3"/> hour(s)	The system will delete expired messages from the queue according to the duration configured here. To disable, set to '0'.
Failure Notice URL	<input type="text" value="https://192.168.1.20/testreceive.php"/>	This URL will be used by the system to reply to the application (using HTTP Post) if the SMS failed to send. Set to 'NA' to disable it.
Failure Notice Email Account	<input type="text" value="alerter1@talarix.com"/> <input type="text" value="alerter2@talarix.com"/>	The system will send an email notification if the SMS failed to send. Set to 'NA' or leave it blank to disable it.
<input type="button" value="Save"/> <input type="button" value="Reset"/>		

Figure 6-3: SMS Queue Monitoring

6.3 SMS Response Action

- a) When there is a SMS message received by the server (incoming SMS message), sendQuick server will inform the recipient via HTTP Post or E-mail. Please specify the HTTP URL address or email address for this purpose.
- b) SMS Reply for Unmatched Keyword is to send an automated SMS reply if the incoming SMS does not match any keyword. Keyword is user definable as the first word in the incoming SMS messages and is configurable via the User Admin web interface.

The screenshot shows the 'SMS Response Action' configuration page. At the top, a breadcrumb trail reads 'Messaging Setup > SMS Response Action'. Below this, a light gray box contains the text: 'Incoming SMS will be converted to different application messaging format which can be integrated to any applications supporting the formats.' The main configuration area has three rows, each with a label, a text input field, and a descriptive note. The first row is 'SMS Response URL' with the value 'https://192.168.1.21/testreceive.php' and the note 'This will be used by the system to send received SMS message. Set to 'NA' to disable.' The second row is 'SMS Response Email' with the value 'alerter1@talariax.com' and 'alerter2@talariax.com' on separate lines, and the note 'This will be used by the system to send received SMS message. Set to 'NA' to disable.' The third row is 'SMS Response Reply (SMS back to user)' with the value 'error', 'alert', and 'warning' on separate lines, and the note 'This will be used by the system to send received SMS message back to the sender if no **Keyword** is match. Set to 'NA' to disable.' At the bottom right of the form are two buttons: 'Save' (blue) and 'Reset' (gray).

Field	Value	Description
SMS Response URL	https://192.168.1.21/testreceive.php	This will be used by the system to send received SMS message. Set to 'NA' to disable.
SMS Response Email	alerter1@talariax.com alerter2@talariax.com	This will be used by the system to send received SMS message. Set to 'NA' to disable.
SMS Response Reply (SMS back to user)	error alert warning	This will be used by the system to send received SMS message back to the sender if no Keyword is match. Set to 'NA' to disable.

Figure 6-4: SMS Response Action

6.4 sendQuickASP Routing

This is to send SMS using sendQuickASP cloud SMS service provided by TalariaX. The advantage of this service is fast throughput as well as the ability to configure a SenderID on the SMS. If the connection fails, it will use the Modem as backup transmission. please contact your distributor or TalariaX for sendQuick ASP subscription.

Access to Menu > Messaging Setup > sendQuick Routing to configure sendQuickASP routing (Figure 6-5):

Messaging Setup > sendQuickASP Routing

SMS messages can be sent using Direct Connection to the mobile operators (carriers) to send the messages to the recipients. sendQuickASP is a cloud based service for delivering SMS using this method.

Show 10 entries Search:

No	Application Description	Prefix	Prepend Number	Status	Caller ID	
1	ASP1	Route all		Disable/F	6594506718	<input type="checkbox"/>
2	ASP2	Route all		Disable/F	71888	<input type="checkbox"/>
3	Talariax ASP	Route all		Disable/F	8888	<input type="checkbox"/>

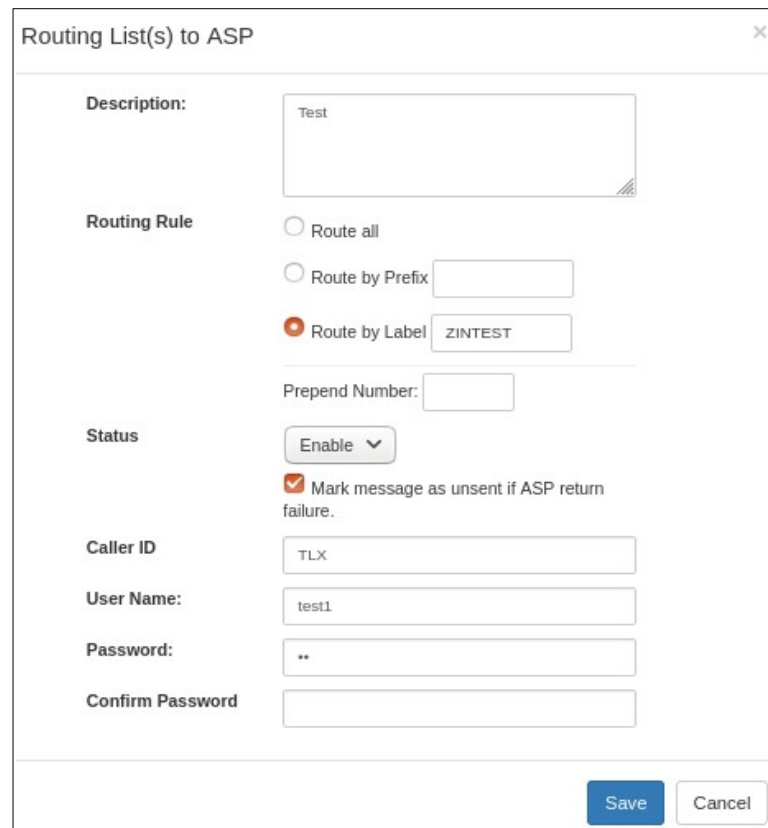
Add New Record Delete

Showing 1 to 3 of total 3 records Previous 1 Next

Figure 6-5: sendQuickASP Routing configuration screen

Select **Add New Record** and Figure 6-6: sendQuickASP Routing configuration detail popup screen will be shown.

Fill up required info follow by **Save** button to create this newly created route.



The image shows a 'Routing List(s) to ASP' configuration window. It contains the following fields and options:

- Description:** A text box containing 'Test'.
- Routing Rule:** Three radio button options: 'Route all' (unselected), 'Route by Prefix' (unselected), and 'Route by Label' (selected). The 'Route by Label' option has a text box next to it containing 'ZINTEST'.
- Prepend Number:** A text box.
- Status:** A dropdown menu set to 'Enable'. Below it is a checked checkbox with the text 'Mark message as unsent if ASP return failure.'.
- Caller ID:** A text box containing 'TLX'.
- User Name:** A text box containing 'test1'.
- Password:** A text box containing two asterisks '**'.
- Confirm Password:** An empty text box.
- At the bottom right are 'Save' and 'Cancel' buttons.

Figure 6-7: sendQuickASP Routing configuration detail popup screen

Description : Enter the prefer name/description for the ASP routing rule.

Routing Rules: Available options are:

- **Route All:** all messages will be routed to this ASP entry.
- **Route by prefix:** route by mobile number (eg: 94506718 / +6594506718), Prefix or Country code +65, +6012 and etc.
- **Route by Label:** route by Modem Label say 'marketing' and 'operations', the modem label that you had configured on Modem Setup > Modem Routing section.

Prepend Number: any text or numbers insert before the digits or text associated with a caller ID.

Status: To enable or to disable this routing rule.

Caller ID: The name appear in the SMS From field or SenderID on the SMS, we will need to apply for permission to have the 'Caller ID' to be registered and shown.

User Name, Password and Confirmed Password: Valid login name and password to logon to sendQuick ASP Server, please contact TalariaX for sendQuick ASP subscription.

6.5 Sqoope Routing

Sqoope is a Mobile Messaging App designed for sendQuick appliances. Sqoope allows for secure, private and confidential messaging service within a organization. Having Sqoope and sendQuick working together, this allows companies to send messages using Sqoope as well as sendQuick (SMS) to achieve a multi-channel messaging. Using this routing mechanism, messages will be routed to Sqoope server and subsequently delivered as a mobile app message, which is sent to the Sqoope messaging app (Android and iOS supported). This is the configuration integration to the Sqoope server., please contact your distributor or TalariaX for discussion.

Access to Menu > Messaging Setup > Sqoope Routing for configuration (Figure 6-8):

Messaging Setup > Sqoope Routing

Messages will be routed to Sqoope server and subsequently delivered as a mobile app message, which is sent to the Sqoope messaging app. This is the configuration integration to the Sqoope server.

Show 10 entries Search:

No	Description	Route Condition	Sqoope Server	Status	
1	SQ's Sqoope2	Route by Label: testlabel	im.sqoope.net	Disable/F	<input type="checkbox"/>
2	SQOOPE Alert	Route all	im.sqoope.net	Enable/F	<input type="checkbox"/>
3	sqoope mars	Route all	mars.sqoope.net	Disable/T	<input type="checkbox"/>

Add New Record Delete

Showing 1 to 3 of total 3 records Previous 1 Next

Figure 6-8: Sqoope routing configuration screen

Select **Add New Record** and Figure 6-9: Sqoope routing configuration detail popup screen will be shown.

Fill up required info follow by **Save** to save this newly created route.

Figure 6-9: Sqoope routing configuration detail popup screen

Description : Enter the prefer name/description for the routing rule.

Routing Rules: Available options are:

- **Route All:** all messages will be routed to Sqoope Server.
- **Route by prefix:** route by mobile number (eg: 94506718 / +6594506718), Prefix or Country code +65, +6012 and etc.
- **Route by Label:** route by Modem Label say 'marketing' and 'operations', the modem label that you had configured on Modem Setup > Modem Routing section.

Status: To enable or temporary to disable this routing rule.

Sqoope Server: the register domain name of the Sqoope Server.

Client ID: enter the Client ID receive from Sqoope.

Authentication ID: enter the Authentication ID receive from Sqoope.

Status URL: Enter URL path to Sqoope server.

Timeout Interval: The default timeout interval is 1 minutes, set to a higher value should you required longer timeout.

Retry Sqoope: checked or unchecked, when a message failed to send via Sqoope beyond the predefined timeout interval, sendQuick will retry again.

Retry SMS: checked or unchecked, when a message failed to send via Sqoope beyond the predefined timeout interval, sendQuick will retry to send the message as SMS to user(s)

6.6 Direct Connection

SMSes can be send using SMS Provider's API to the mobile operator (carrier) to send the messages to the recipients instead of using traditional modem approach for sending SMS. please contact your distributor or TalariaX for discussion on the subscription package.

Access to Menu > Messaging Setup > Direct Connection for configuration (Figure 6-6-1):

Messaging Setup > Direct Connection

SMS messages can be sent using SMS Provider's API to the mobile operators (carriers) to send the messages to the recipients.

Show 10 entries Search:

No	Description	Routing Rule	Status	Routing Sequence	Connection	
1	ASP to Web	Route all	Enable/F	1	Test	<input type="checkbox"/>
2	ASP1	Route all	Enable/F	2	Test	<input type="checkbox"/>

Add New Record Delete

Showing 1 to 2 of total 2 records Previous 1 Next

Figure 6-6-1: Direct connection configuration screen

Select **Add New Record** and Figure 6-6-2: Direct connection configuration detail popup screen will be shown.

Fill up required info follow by **Save** button to create this newly created route.

Edit Routing to SMS Provider

Description * ASP to Web

Routing Sequence * 1

Routing Rule * ☒ Route all
☐ Route by Prefix
☐ Route by Label
☐ Route by Pattern

Prepend Number For All Numbers Number :

Status * Enable

☐ Mark message as unsent if SMS Provider return failure

Timeout * 30 seconds

Maximum Retry * 3

Figure 6-6-2: Direct connection configuration detail popup screen

Description : Enter the prefer name/description for this SMS Provider.

Routing Sequence: default as 1, this is applicable if you have multiple routing channels.

Routing Rules: Available options are:

- **Route All:** All messages will be routed to this SMS Provider.
- **Route by prefix:** Route by mobile number (eg: 94506718 / +6594506718), Prefix or Country code +65, +6012 and etc.
- **Route by Label:** Route by Modem Label say 'marketing' and 'operations', the modem label that you had configured on Modem Setup > Modem Routing section.
- **Route by Pattern:** Regular Expression Pattern to Extract Mobile number, for example '([+65]\d{10}|[8|9]\d{7})', an example of the regular expression for Singapore Mobile numbers. The system will extract all numbers start with +65 or 8 or 9
- **Remove '+' sign from prefixes:** Checked to remove the mobile number prefix eg '+65', some SMS provider do not required the '+' sign for sending SMS.

Prepend Number: To define text or numbers insert before the digits or text associated with a caller ID.

Status: To enable or temporary to disable this service.

Timeout: Default as 30 seconds.

Maximum Retry: Default as 3 times.

Provider: select 'Others'.

Direct connection configuration detail popup screen (Figure 6-6-2) consist of 2 sub-functional screens which are '**Send SMS**' and '**Check Status**' for checking send sms status.

6.6.1 Direct Connection – Send SMS (Provider = Other)

HTTP, SOAP and JSON are the 3 integration methods that are supported with SMS providers, select **Send SMS** functional sub menu and Figure 6-6-3 will be shown.

a) When selected **Type = HTTP**, these are parameters that require to be filled, please refer to sendQuick Menu > SMS Specification > REST API > SMS tab > section HTTP method to prepare the required data.

The screenshot shows a configuration window for sending SMS via HTTP. The window has two tabs: 'Send SMS' (active) and 'Check Status'. The form contains the following fields and values:

- Type ***: HTTP (dropdown)
- HTTP/S URL ***: https://web.sendquickasp.com/client_api/index.php?route_to=api_send_sms
- Method**: POST (selected), GET
- Username**: username= (masked)
- Password**: passwd= (masked)
- Mobile No. ***: tar_num=xNUMx
- Message ***: tar_msg=xMSGx
- Language**: Normal Text (selected), UTF-8 (dropdown)
- Message ID**: <Parameter name>=xMSGIDx
- Caller ID**: callerid= (masked)
- Other Query String**: param1=value1¶m2=value2
- Success Response**: sent
- Get message ID**: Disable (dropdown)

At the bottom right, there are 'Save' and 'Cancel' buttons.

Figure 6-6-3: Direct connection configuration detail popup screen – Send SMS – HTTP

- Username : username={check with your supplier}
- Password : passwd={check with your supplier}
- Mobile No. : tar_num=xNUMx
- Message * : tar_msg=xMSGx
- Caller ID : callerid={check with your supplier}
- Success Response : sent

b) When selected **Type = SOAP**, these are parameters that require to be filled, please refer to sendQuick Menu > SMS Specification > REST API > SMS tab > section SOAP method to prepare the required data.

The screenshot shows a configuration interface for sending SMS via SOAP. At the top, there are two tabs: 'Send SMS' (active) and 'Check Status'. Below the tabs, the 'Type' is set to 'SOAP'. The 'HTTP/S URL' field contains 'https://'. Under the 'Raw Message' section, there are two text areas: 'ASCII Text (ISO-8895-1)' and 'UTF-8 (Unicode)'. Above these text areas, a list of variables is provided: xNUMx : Recipient's Mobile Number, xMSGx : Message Content, xMSGIDx : Message ID, and xSENDERx : Message Sender. At the bottom, there is a 'Success Response' field with the value '200' and a 'Get message ID' dropdown menu set to 'Disable'.

Send SMS Check Status

Type * SOAP ▾

HTTP/S URL * https://

Raw Message

Variables:
xNUMx : Recipient's Mobile Number
xMSGx : Message Content
xMSGIDx : Message ID
xSENDERx : Message Sender

ASCII Text (ISO-8895-1)

UTF-8 (Unicode)

Success Response 200 ?

Get message ID Disable ▾

Figure 6-6-4: Direct connection configuration detail popup screen – Send SMS – SOAP

c) When selected **Type = JSON**, these are parameters that require to be filled, please refer to sendQuick Menu > SMS Specification > REST API > SMS tab > section JSON method to prepare the required data.

The screenshot shows a configuration window for sending SMS via JSON. At the top, there are two tabs: 'Send SMS' (active) and 'Check Status'. Below the tabs, the 'Type' is set to 'JSON'. The 'HTTP/S URL' field contains 'https://'. The 'Raw Message' section lists variables: xNUMx (Recipient's Mobile Number), xMSGx (Message Content), xMSGIDx (Message ID), and xSENDERx (Message Sender). Below this, there are two text input fields for 'ASCII Text (ISO-8895-1)' and 'UTF-8 (Unicode)'. The 'Success Response' field contains '200'. The 'Get message ID' dropdown is set to 'Disable'.

Send SMS Check Status

Type * JSON ▾

HTTP/S URL * https://

Raw Message

Variables:
xNUMx : Recipient's Mobile Number
xMSGx : Message Content
xMSGIDx : Message ID
xSENDERx : Message Sender

ASCII Text (ISO-8895-1)

UTF-8 (Unicode)

Success Response 200 ?

Get message ID Disable ▾

Figure 6-6-5: Direct connection configuration detail popup screen – Send SMS – JSON

6.6.2 Direct Connection – Check Status (Provider = Other)

Select Check Status functional sub menu with **Status = Enable**, this function menu will allow user to configure the check SMS status for the HTTP, SOAP and JSON method.

Figure 6-6-6: Direct connection configuration detail popup screen – Check Status – Enable

a) When **Check Status = Enable** and the selected **Type = HTTP** (Figure 6-6-7), these are parameters that require to be configured, please refer to sendQuick Menu > SMS Specification > REST API > SMS tab > section HTTP method to prepare the required data.

Figure 6-6-7: Direct connection configuration detail popup screen – Check Status – HTTP

b) When **Check Status = Enable** and the selected **Type = SOAP** (Figure 6-6-8), these are parameters that require to be configured, please refer to sendQuick Menu > SMS Specification > REST API > SMS tab > section SOAP method to prepare the required data.

Send SMS | Check Status

Check Status *

Type

Check Status URL

Raw Message

Variables:
xDCMIDx : SMS Provider's Message ID
xMSGIDx : SendQuick's Message ID

RegEx for returned status

Status Time

Format :

Delivered

Failed/Undelivered

Final Status

Time Interval min(s)

Expiry min(s)

Check Mode

Continuous : Check delivery status continuously until the response match with final status or expired
Interval : Check delivery status at specific time interval until the response match with final status or expired

Figure 6-6-8: Direct connection configuration detail popup screen – Check Status - SOAP

c) When **Check Status = Enable** and the selected **Type = JSON** (Figure 6-6-9), these are parameters that require to be configured, please refer to sendQuick Menu > SMS Specification > REST API > SMS tab > section JSON method to prepare the required data.

Send SMS | Check Status

Check Status * Enable

Type JSON

Check Status URL

Raw Message

Variables:
xDCMIDx : SMS Provider's Message ID
xMSGIDx : SendQuick's Message ID

RegEx for returned status

Status Time

Format ?

Delivered

Failed/Undelivered

Final Status

Time Interval min(s)

Expiry min(s) ?

Check Mode Continuous

Continuous : Check delivery status continuously until the response match with final status or expired
Interval : Check delivery status at specific time Interval until the response match with final status or expired

Figure 6-6-9: Direct connection configuration detail popup screen – Check Status – JSON

6.6.3 Direct Connection – Send SMS (Provider = ASP)

Some SMS ASP provides will provide simple direct connect which required only the Username and Password, select the Provide = ASP# accordingly:

Edit Routing to SMS Provider

Description *

Routing Sequence *

Routing Rule * ☒ Route all
☐ Route by Prefix
☐ Route by Label
☐ Route by Pattern

☒ Remove '+' sign from prefixes

Prepend Number Number :

Status *

☐ Mark message as unsent if SMS Provider return failure

Timeout * seconds

Maximum Retry *

Provider *

Username *

Password *

Caller ID *

Figure 6-6-10: Direct connection – ASP

- Username : username={check with your supplier}
- Password : passwd={check with your supplier}
- Caller ID : callerid={check with your supplier}

6.7 SMPP Route

SMSes can be send via SMPP (Short Message Peer-to-Peer) via SMSC service (Short Message Service Center (SMSC)).

User required to perform one time configuration for the SMSC login data, access to Menu > Messaging Setup > SMSC Setup for configuration (Figure 6-7-1), fill in the requested info:

Messaging Setup > SMPP Route

SMSC Setup **SMPP Route**

System ID The system id is used to identify the ESME system when requesting to bind with the SMSC.

Password The password is used by the SMSC to authenticate the ESME requesting to bind.

Port The SMPP Server Port Number. Port number should be greater than 1024.

Status This option will enable or disable SMPP SMSC service.

Figure 6-7-1 SMPP Route – SMSC Setup

System ID: The system id is used to identify the ESME system when requesting to bind with the SMSC.

Password: The password is used by the SMSC to authenticate the ESME requesting to bind.

Port: The SMPP Server Port Number. Port number should be greater than 1024.

Receive MO: To receive Mobile Originated message(s), ESME must bind as Transceiver or Receiver.

Status: This option will enable or disable SMPP SMSC service.

Select **Save** to continue or **Reset** to redo.

To configure the SMPP route, access to Menu > Messaging Setup > SMPP Route > SMPP Route for setup:

Messaging Setup > SMPP Route

SMSC Setup **SMPP Route**

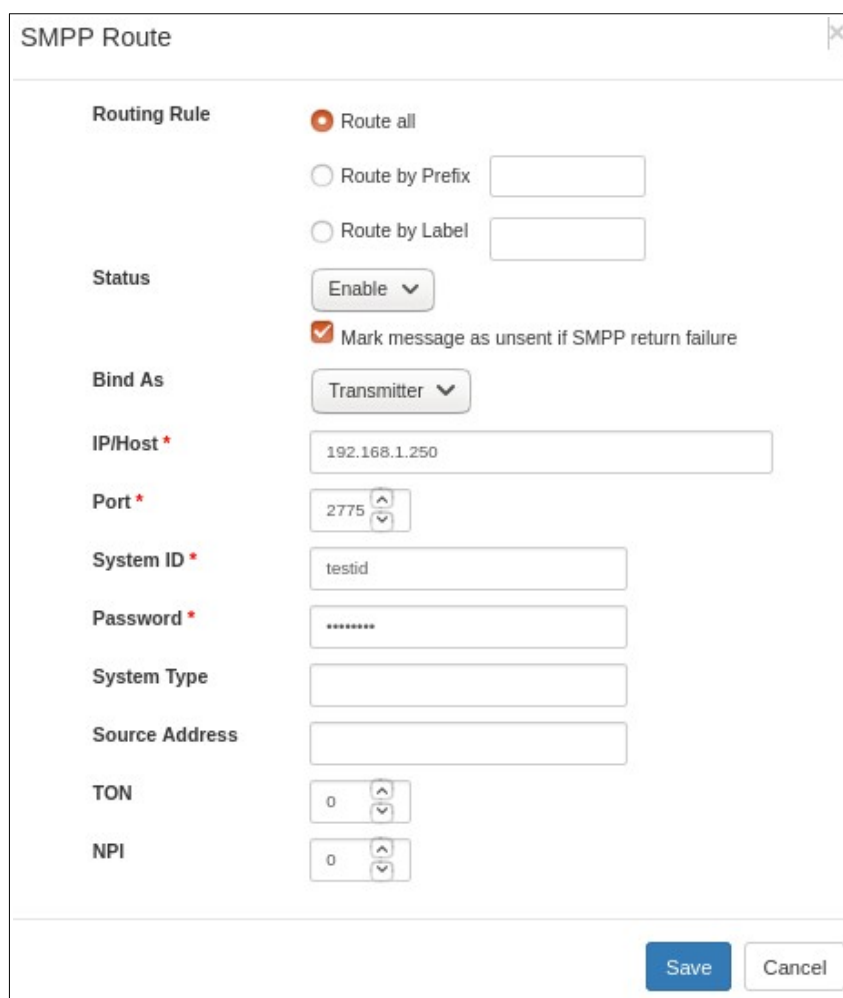
Show entries Search:

No	IP/Host	Port	System ID	Routing Rule	Status	
1	10.1.1.10	2775	smplogin	Route all	Enable/T	<input type="checkbox"/>
2	192.168.1.250	2775	testid	Route all	Enable/T	<input type="checkbox"/>

Showing 1 to 2 of total 2 records Previous **1** Next

Figure 6-7-2 SMPP Route – setup

Select **Add New Record** and Figure 6-7-3 will be shown.



The image shows a 'SMPP Route' configuration window. It contains the following fields and options:

- Routing Rule:** Radio buttons for 'Route all' (selected), 'Route by Prefix' (with an empty text box), and 'Route by Label' (with an empty text box).
- Status:** A dropdown menu set to 'Enable' and a checked checkbox for 'Mark message as unsent if SMPP return failure'.
- Bind As:** A dropdown menu set to 'Transmitter'.
- IP/Host *:** A text box containing '192.168.1.250'.
- Port *:** A spinner box set to '2775'.
- System ID *:** A text box containing 'testid'.
- Password *:** A text box with masked characters '*****'.
- System Type:** An empty text box.
- Source Address:** An empty text box.
- TON:** A spinner box set to '0'.
- NPI:** A spinner box set to '0'.

At the bottom right are 'Save' and 'Cancel' buttons.

Figure 6-7-3 SMPP Route – setup detail pop up screen

Fill in the required parameters:

Routing Rules: Available options are:

- **Route All:** All message will be routed to this SMS Provider.
- **Route by prefix:** Route by mobile number (eg: 94506718 / +6594506718), Prefix or Country code +65, +6012 and etc.
- **Route by Label:** Route by Modem Label say 'marketing' and 'operations', the modem label that you had configured on Modem Setup > Modem Routing section.

Status: To enable or temporary to disable this service.

Blind As: Transmitter or Transceiver

IP/Host: The IP address or hostname of the SMPP server.

Port: the interfacing port eg 2775.

System ID: enter your given login id.

Password: enter your given login password.

System Type: Optional login parameter that should be set only if required by the SMPP server.

Source Address: Optional IP for the SNMP Server.

TON: Type of Number, select the given number.

NPI: Numbering Plan Identification assigned, select the given number

6.8 Mobile Instant Messaging Routing

With integration of official messaging APIs provided by mobile instant messaging platforms like Line, Facebook Messenger, Slack, Viber, WeChat, Telegram, Microsoft Teams, Webex Teams, Whatsapp and Wechart Work, Globe Labs, WhatsApp DC and Line Notify are now able to deliver alerts to these platforms with minimal setup. This feature is to complement existing delivery channels (SMS & Email) by providing an additional alert transmission mode. Figure 6-8-1 below shows the summary of created mobile instant messaging routes.

Messaging Setup > Mobile Instant Messaging Routing

Show 10 entries Search:

No.	Description	Type	Maximum Retry	Webhook	Enable?	Edit	
1	WECHAT MIM Route	WECHAT	3	http://192.168.0.200/appliance/webhook/5/pWLRHwuO7YNjGhswfclfhLwWHOJRS6w/	Yes	Edit	Delete
2	LINE MIM ROUTE	LINE	3	http://192.168.0.140/appliance/webhook/1/XMihblt2LqAcrsMRDg09k0ziEbnyxatG/	Yes	Edit	Delete
3	VIBER MIM Route	VIBER	3	http://192.168.0.200/appliance/webhook/4/TEECgj4hiOYMggYFbVQtwcPu5fOSIGVE/	Yes	Edit	Delete
4	SLACK MIM Route	SLACK	2	http://192.168.0.140/appliance/webhook/3/PyoYq3qJkhdcVwhLdlHQ3luyACTBV2hsU/	Yes	Edit	Delete
5	FB MIM Route	FACEBOOK	2	http://192.168.0.140/appliance/webhook/2/F0DI6pvLpRCvDQ48xC48bMFAyzQ4yjb1/	Yes	Edit	Delete

[Add New Record](#) [Delete](#)

Figure 6-8-1: Mobile Instant Messaging Routing

Click on “**Add New Record**” and Figure 6-8-2 will be shown. Fill up all the necessary data fields, press “Generate new webhook” to generate a unique webhook URL. Webhook URL allows sendQuick to receive messages from mobile instant messaging platform. Press “**Save**” button to save this newly created route.

Mobile Instant Messaging Routing

Description: LINE MIM Route

Status: Enable

Type: LINE

Channel Access Token: channelAccessToken

Channel Secret: channelSecret

Webhook: http://192.168.0.200/appliance/webhook/1/prnPwuhzQgZhfVbWhHpFDstsWW62JXcmW/

Generate new webhook

Timeout: 60 seconds

Retry?: ☒ Yes

Maximum Retry: 3

[Save](#) [Cancel](#)

Figure 6-8-2: Mobile Instant Messaging Routing detail

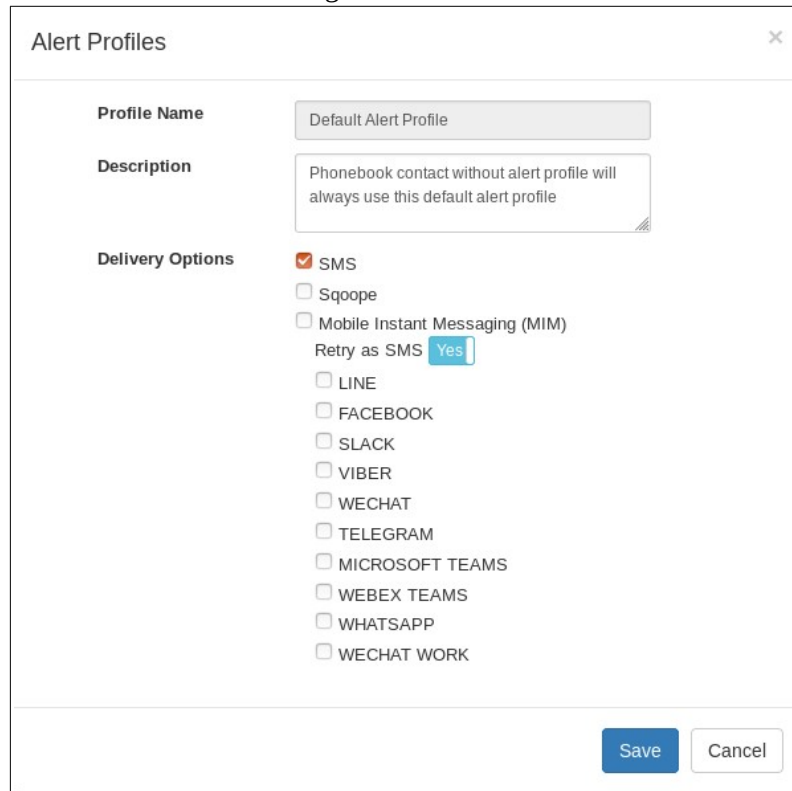
* Network administrator must ensure Webhook URL is secured by a valid SSL, public facing and accessible from Internet.

Additional outgoing URL/Port to be opened:

Platform	URL	Port
LINE	https://api.line.me/v2/bot/message/push	443
LINE	https://api.line.me/v2/bot/profile	443
Facebook	https://graph.facebook.com/v2.6/me/messages	443
Facebook	https://graph.facebook.com/v2.6	443
Slack	https://slack.com/api/chat.postMessage	443
Slack	https://slack.com/api/users.profile.get	443
Slack	https://slack.com/api/im.list	443
Slack	https://slack.com/api/users.list	443
Telegram	https://api.telegram.org/bot{token}/sendMessage	443
Viber	https://chatapi.viber.com/pa/get_user_details	443
Viber	https://chatapi.viber.com/pa/send_message	443
WeChat	https://api.wechat.com/cgi-bin/user/info	443
WeChat	https://api.wechat.com/cgi-bin/message/custom/send	443
WeChat	https://api.wechat.com/cgi-bin/token	443

6.9 Alert Profiles

Alert Profile acts as a universal gatekeeper to control outgoing alerts. Generated alerts will first go through Alert Profile to find out which delivery options were being assigned to transmit the alerts. Various delivery options can be selected as shown in figure 6-7 below:



The screenshot shows a window titled "Alert Profiles" with a close button (X) in the top right corner. The window contains three main sections:

- Profile Name:** A text field containing "Default Alert Profile".
- Description:** A text area containing the text "Phonebook contact without alert profile will always use this default alert profile".
- Delivery Options:** A list of checkboxes for different delivery methods:
 - ☒ SMS
 - ☐ Sqoope
 - ☐ Mobile Instant Messaging (MIM)
 - Retry as SMS:** A blue button with the text "Yes".
 - ☐ LINE
 - ☐ FACEBOOK
 - ☐ SLACK
 - ☐ VIBER
 - ☐ WECHAT
 - ☐ TELEGRAM
 - ☐ MICROSOFT TEAMS
 - ☐ WEBEX TEAMS
 - ☐ WHATSAPP
 - ☐ WECHAT WORK

At the bottom right of the window are two buttons: "Save" (blue) and "Cancel" (white).

Figure 6-9-1: Alert Profiles

If “Retry as SMS” option is enabled, SMS will be triggered if and only if all selected mobile instant messaging channels fail to deliver an alert. Alert Profile is designed such that in any circumstances, it sends out at most 1 SMS only.

7.0 Modem Setup

This section indicates whether the GSM modem is connected and detected by sendQuick server, and for configuration of various modem functions as described below:

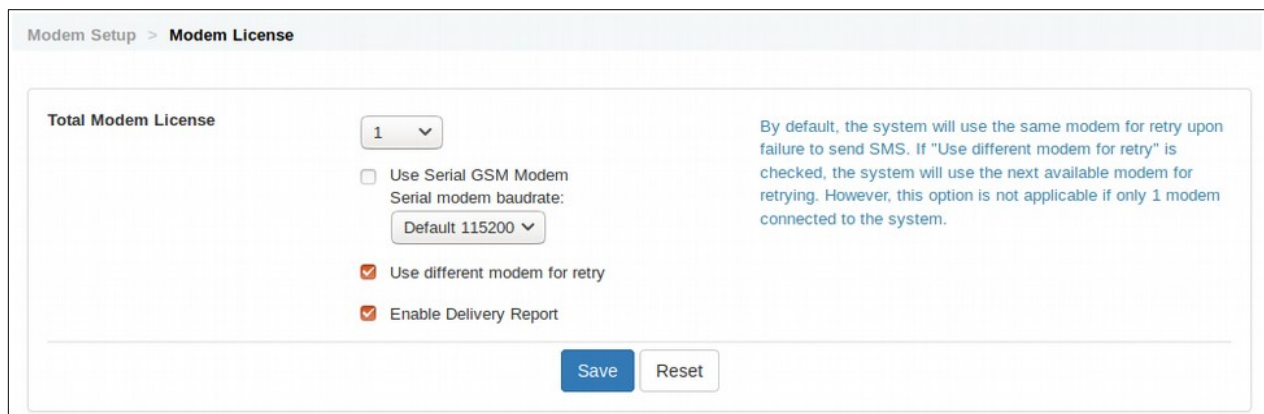
7.1 Modem License

The default modem connection is USB connection and you need to select the number of modems to be activated (license fee applicable). This is an option to purchase more modems licenses, please contact your distributor or TalariaX for pricing.

To active the modem license, select a number from the drop-down list, 'Save' when ready

By default, the system will use the same modem for retry upon failure to send SMS. If "**Use different modem for retry**" is checked, the system will use the next available modem for retrying. However, this option is not applicable if only 1 modem connected to the system.

An **SMS delivery report** (Enable or Disable, default is Enable) is a message from your SMS server (known in the industry as an SMSC) that tells you that the SMS message you sent was delivered to the phone of the recipient.



The screenshot shows the 'Modem Setup > Modem License' configuration page. It features a 'Total Modem License' dropdown menu set to '1'. Below this, there are three checkboxes: 'Use Serial GSM Modem' (unchecked), 'Use different modem for retry' (checked), and 'Enable Delivery Report' (checked). The 'Use Serial GSM Modem' option has a sub-label 'Serial modem baudrate:' with a dropdown menu set to 'Default 115200'. A blue text box on the right side of the page provides a default behavior note: 'By default, the system will use the same modem for retry upon failure to send SMS. If "Use different modem for retry" is checked, the system will use the next available modem for retrying. However, this option is not applicable if only 1 modem connected to the system.' At the bottom right, there are 'Save' and 'Reset' buttons.

Figure 7-1: Total Modem Connections

Note: When you switch between USB and Serial connection and vice versa, please remember to shutdown the server, connect the relevant modem and restart the server. You need to restart the server as sendQuick may not be able to detect the modem properly. This is more evident in the USB modem.

7.2 Modem Dispatch Mode

Messages are usually sent on a **FIFO** (first-in-first-out) mode as it is the most efficient way to send the messages. However, other options to send messages in different ways are available, including **Even Mode** (allowing messages to be distributed evenly between modems) and Strict FIFO. Strict **FIFO** means messages will be sent in a FIFO order and may cause inefficiency in message distribution. Figure 7-2 below shows the options for selection.

sendQuick® Entera Server Admin

English Shutdown Restart Logout

Modem Setup > Modem Dispatch Mode

Modem Dispatch Mode

- ☐ Even mode This will dispatch the message in the queue evenly among the modems.
- ☒ FIFO mode This will try to dispatch the message as first in first out among the modems.
- ☐ Strict FIFO mode This will cause the system to dispatch the next message after it has been processed by the modem.
NOTE: This option will severely reduce sending SMS throughput.

Save Reset

Figure 7-2 Modem Dispatch Mode

7.3 Modem Routing

You can send SMS by choosing a specific modem by domain name, mobile prefix or modem label. Incoming SMS can be processed specifically to an email (Response Email) or URL (Response URL). You can also designate which modem is the default modem or select any modem that is available to send SMS

Figure 7-3 shows a modem routing configured for different modem IMEI.

Modem Setup > Modem Routing

Show 10 entries Search:

No	Modem IMEI	Domain	Prefix	Response URL	Response Email	Modem Label	Exclude Keyword Mgmt	Default Modem	
1	359180082892503	sendquick.com		https://192.168.1.20/testreceive.php	alerter@talariax.com	marketing D: Yes A: Yes	Yes	Yes	<input type="checkbox"/>
2	359180087149628 (Active)		+6012				No	No	<input type="checkbox"/>

Add New Record Delete

Showing 1 to 2 of total 2 records Previous 1 Next

D - Designated Modem
A - Use Alternative Modem

Figure 7-3: Modem Routing

Click on “**Add New Record**” and Figure 7-4 will be shown. Fill up all the necessary data fields, press “**Save**” button to save this newly created route.

Edit Modem Routing setting

Modem IMEI

Modem Label

☐ Only for designated request

☒ Use alternative modem if modem for this label not found.

Domain

Prefix Number

Response Email

Response URL

Unlimited Quota ☒

☐ Exclude from keyword management

☐ Set as default modem pool (not applicable if modem label is set)

Save **Cancel**

Figure 7-4: Modem Routing setting

Modem IMEI

- Refer to Dashboard > Modem Status > Modem IMEI for your modem IMEI number.

Modem Label

- assigned modem label, eg marketing, it etc.

Domain:

- Domain(s) that authorized to use this modem.

Prefix Number:

- Mobile number with the specified prefix that will be diverted to this modem, eg +65, +6012 etc

Response Email

- Received SMS will be forwarded to this email.

Response URL

- Received SMS will be forwarded to this URL.

Unlimited Quote

- checked - not limit on number of sms can be send by this modem.
- Unchecked – to set the limit of sms allow to send by daily or monthly

7.4 Virtual Modem Routing

The Virtual Modem routing allows two (2) sendQuick servers to share the modem to send and receive SMS. This is particularly useful if the sendQuick servers are located in different geographical region (different countries) and they can be used to send SMS locally in their own country. The filtering will be done based on the mobile number (prefix).

Figure 7-5 below shows a summary of the virtual modem routing for different prefix number via different server.

Modem Setup > Virtual Modem Routing

Show 10 entries Search:

No	Application IP	Application Description	Routing Rule	Status	
1	10.10.1.20	For mobile number prefix with +65	Route by Prefix: +65	Normal Queue	<input type="checkbox"/>
2	192.168.1.10	For mobile number prefix with +6012	Route by Prefix: +6012	Normal Queue	<input type="checkbox"/>
3	192.168.1.100	For mobile number prefix with +882	Route by Prefix: +882	Normal Queue	<input type="checkbox"/>
4	192.168.1.105	for label = marketing	Route by Label: marketing	Upon Unsent	<input type="checkbox"/>

Add New Record Delete

Showing 1 to 4 of total 4 records Previous 1 Next

Figure 7-5: Virtual Modem Routing

7.5 Modem Monitoring & Respool

Respool a SMS to retry to re-send if failed. The priority range value is from 1-99. If set to 0, SMS will not be re-sent. If the value is set too high, it will cause a delay in sending SMS as messages retry times increased. (Figure 7-6). Other parameters are:

- **Alert Mobile Number.** Define the mobile number(s) to received the alert if re-spool occurred.
- **Alert Email Address.** Define the email(s) to received the alert if re-spool occurred.
- **Alert Message:** Define your preferred 'alert message' in free text format.

Modem Setup > Modem Monitoring & Respool

Maximum number of respool per message: 1. This is the maximum number of respool per message. This should be a numeric value not more than 99. Default would be set to 1.

Alert Mobile Number: 91234567, 87654321. This is the mobile number for the alert.

Alert Email Address: alert1@talariax.com, alert2@talariax.com. This is the Email address for the alert.

Alert Message: Warning !!!, error on SMS Server. This is the message details for the alert.

Save Reset

Figure 7-6: Modem Monitoring & Respool

7.6 Modem Priority

This is to configure the priority to send the SMS for HTTP host or SMTP Source, the The priority range value is from 1-99, 1 being the highest priority. (Figure 7-7).

Modem Setup > **Modem Priority**

Show entries Search:

No	Remote IP / Sender Email	Description	Type	Priority	Status	
1	192.168.1.10	Management	HTTP	1	Enable	<input type="checkbox"/>
2	192.192.168.1.200	Marketing	HTTP	5	Enable	<input type="checkbox"/>
3	john@talariax.com	CEO: Mr. John Smith	HTTP	1	Enable	<input type="checkbox"/>
4	david@talaria.com	COO	HTTP	2	Enable	<input type="checkbox"/>
5	192.168.1.150	IT Department	HTTP	9	Enable	<input type="checkbox"/>

Showing 1 to 5 of total 5 records Previous **1** Next

Figure 7-7: Modem Priority

7.7 Modem Time Control

This allows the modem or system to send or not to send the SMS based on time of day. If control is enabled, SMS is sent within the specified time frame (Figure 7-8).

Modem Setup > **Modem Time Control**

Show entries Search:

No	Modem IMEI	Sender	Sun	Mon	Tues	Wed	Thu	Fri	Sat
1	359180082892503	contains(Promotion)	Y(09:00-13:00)	N	N	N	N	Y(00:00-00:00)	Y(00:00-00:00)
2	359180083532587	does not contain(urgent)	N	Y(09:00-17:00)	Y(09:00-17:00)	Y(09:00-17:00)	Y(09:00-17:00)	Y(09:00-17:00)	N

Showing 1 to 2 of total 2 records Previous **1** Next

Figure 7-8: Modem Time Control

7.8 IMEI SIM Card Mapping

This page is designed to map the SIM card (mobile number) to the modem (IMEI) that is connected to the sendQuick servers. It is meant for tracking purpose, especially if you use multiple modems but this is an optional configuration (Figure 7-9).

Modem Setup > IMEI SIM Card Mapping

Show 10 entries Search:

No	IMEI	SIM Card Number	<input type="checkbox"/>
1	359180082892503	94726517	<input type="checkbox"/>
2	359180087149628	80951634	<input type="checkbox"/>

Add New Record Delete

Showing 1 to 2 of total 2 records Previous 1 Next

Figure 7-9: IMEI SIM Card Mapping

7.9 MPM Routing

sendQuick supports MPM routing, to configure the MPM Server IP/Host, click on the 'Add New Record' as show on Figure 7-10 and fill on the server's configuration data accordingly.

Modem Setup > MPM Routing

Show 10 entries Search:

No	MPM Server IP/Host	MPM Server Port	Description	Client IP/Host	Token	Status	View SSH	<input type="checkbox"/>
1	10.1.1.20	25	routing form network 50 to 20	10.1.1.50	2	Y	View	<input type="checkbox"/>
2	192.168.1.8	25	routing form network 100 to 8	192.168.1.100	1	Y	View	<input type="checkbox"/>

Add New Record Delete

Showing 1 to 2 of total 2 records Previous 1 Next

Figure 7-10: MPM Routing

8.0 Phone Book & Roster (Optional Item in sendQuick Alert Plus. Default in sendQuick Entera)

The Phone Book & Roster is an optional module that can be added to sendQuick Alert Plus. It is a default function in sendQuick Entera. The purpose of the Phone Book & Roster is to provide an easy management of the recipients in the filter rules. With the creation of the address list in the phone book, the recipients can be added and amended from the phone book and the changes will be effected to all the relevant rules.

8.1 Phone Book Records

Start the Phone Book record creation by selecting the **Phone Book Records** from the navigation menu and a summary list of the records are shown in Figure 8-1-1 below. The summary list shows the respective users, mobile number, email address, group that they belong to and the roster that they had been allocated. This roster is configured in **Roster Management** as described Section 8.3 later.

Phone Book & Roster > Phone Book Records

Show 25 entries Search:

No	User Name	Display Name (AD)	Mobile Number	MIM Subscription	Email Address	Group	Roster	Modem Label	Type	OU Name	
1	Luke		+6512345678		support@talariax.com		All day		LOCAL		<input type="checkbox"/>

[Add New Record](#)
[Upload CSV](#)
[AD/LDAP Setup](#)
[Delete](#)

Showing 1 to 1 of total 1 records Previous 1 Next

Figure 8-1-1: Phone Book Records

Select **Add New Record** and Figure 8-1-2 will be shown. Enter the username, mobile number (preferably in international format with a '+' sign), email address (where required). Then, select the groups whom this user will belong to. You can select multiple or no group assignment. To create a new group, enter the group name in the **New group** text box. Select the roster and model label to be allocated for the user from the drop-down menu (if applicable). If user has opt-in to receive alerts in mobile instant messaging platform, respective chosen platform will be shown in MIM Subscription. Finally, assign Alert Profile to user contact. Alert Profile is useful in controlling outgoing messages of individual user.

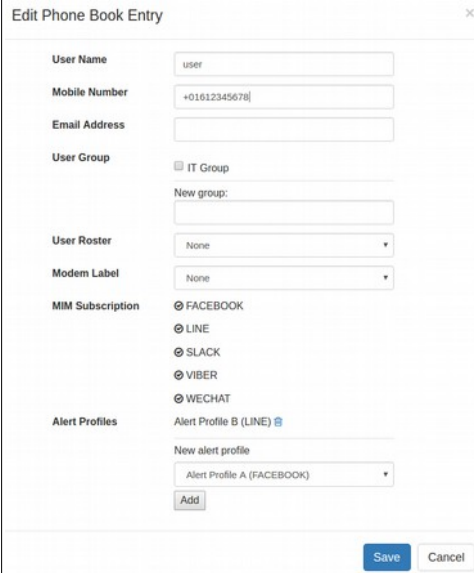


Figure 8-1-2: New Phone Book Entry

Select **Save** once done and the record will be created. The same interface will appear for editing the phone book. The system can support unlimited number of records for the Phone Book.

Note: All Phone Book Records **MUST** have a valid and assigned Roster/Shift before the phone numbers are able to receive SMS text. User Roster CANNOT be None.

8.1.2 Phone Book Records – Upload by CSV File

The alternative way to create phone book record is by uploading CSV record(s).

Please note that All Phone Book Records MUST have a valid and assigned Roster/Shift before the phone numbers are able to receive SMS text. User Roster CANNOT be None. Refer to section 8.3 Roster Management for detail.

Please prepare your CSV record(s) that ‘Group by Roster’ in this format:

User Name,Mobile Number,Email,Call Number,User Group

Sample data as follow:

CheeKiongLee,94506718,cheekiong@talariaix.com,62806882,IT
 JohnSmith,91234567,johnsmith@talariaix.com,61234568,Sales
 DavidBeckham,97654321,davidbeckham@talariaix.com,61234569,Marketing
 OliviaWong,81234567,oliviawong@talariaix.com,61234570,Marketing

When your CSV file is ready, select ‘Upload CSV’ from figure 8-1-1 Phone Book Records screen, the ‘New Phone Book Entry By File Upload’ popup screen display:

New Phone Book Entry By File Upload

Upload *

Browse... PhonebookCSV

CSV Format:
 User Name,Mobile Number,Email Address,Call Number,User Group[,User Group]

User Group

☐ IT
☐ Marketing
☐ Sales

User Roster

8to5

Modem Label

None

Upload Cancel

Figure 8-1-3: New Phone Book Entry by File Upload

‘Browse and locate’ your CSV file, select ‘User Roster’ accordingly follow by Upload when ready.

Verify the uploaded data on the Preview Phone Book Entry screen, select Save to proceed, otherwise select Cancel to undo.

Preview Phone Book Entry

Show 10 entries

Search:

No	User Name	Display Name (AD)	Mobile Number	Call Number	Email Address	Group	OU Name
1	CheeKiongLee		94506718	61234567	cheekiong@talariaix.com	IT	
2	DavidBeckham		97654321	61234569	davidbeckham@talariaix.com	Marketing	
3	JohnSmith		91234567	61234568	johnsmith@talariaix.com	Sales	
4	OliviaWong		81234567	61234570	oliviawong@talariaix.com	Marketing	

Showing 1 to 4 of total 4 records

Previous

1

Next

Save

Cancel

Figure 8-1-4: Preview Phone Book Entry

Upon your confirmation, the Phone Book Records are uploaded:

Phone Book & Roster > Phone Book Records

Phone Book Records

Addressbook Group

Show 25 entries

Search:

No	User Name	Display Name (AD)	Mobile Number	Call Number	MIM Subscription	
1	CheeKiongLee		94506718	61234567		<input type="checkbox"/>
2	DavidBeckham		97654321	61234569		<input type="checkbox"/>
3	JohnSmith		91234567	61234568		<input type="checkbox"/>
4	OliviaWong		81234567	61234570		<input type="checkbox"/>

Add New Record

Upload CSV

AD/LDAP Setup

Delete

Showing 1 to 4 of total 4 records

Previous

1

Next

Figure 8-1-5: update Phone Book Records

Select the ‘+’ sign to expend a user’s information on screen, to undo, select the ‘-’ sign.

Phone Book & Roster > Phone Book Records

Phone Book Records

Addressbook Group

Show 25 entries

Search:

No	User Name	Display Name (AD)	Mobile Number	Call Number	MIM Subscription	
<div>-</div> 1	CheeKiongLee		94506718	61234567		<div></div>
Email Address cheekiong@talariaix.com						
Group IT						
Roster 8to5						
Modem Label						
Type CSV						
OU Name						
<div>+</div> 2	DavidBeckham		97654321	61234569		<div></div>
<div>+</div> 3	JohnSmith		91234567	61234568		<div></div>
<div>+</div> 4	OliviaWong		81234567	61234570		<div></div>

Add New Record

Upload CSV

AD/LDAP Setup

Delete

Figure 8-1-6: Phone Book Records with expended information

8.1.3 Phone Book Records – by AD/LDAP Setup

sendQuick's Phone Book Records can be linked with AD/LDAP, this can be achieved with 2 steps:

1. Configure the interfacing parameters that required by AD/LDAP as per figure 8-1-7: AD/LDAP Setup.
2. Download Contact from AD/LDAP.

Figure 8-1-7: AD/LDAP Setup

The AD/LDAP Setup screen will required the following parameters:

- **Primary Server and Port:** enter the Primary AD/LDAP Server's IP and Interface port.
- **Secondary Server and Port:** optional, enter the Secondary AD/LDAP Server's IP and Interface port.

The default interface port with AD/LDAP server is port '389'.

- **Service Account DN:** AD/LDAP server's login account and password.
- **Search Base DB:** default as 'dc=testserver,dc=com'.
- **Search Scope:** Sub / One / Base.
- **Search Filter String:** default as 'samaccountname'.

If you are not sure the search string for your group, login to your AD > Group name > Properties > Attribute Editor and you can check, also work with your AD/LDAP system administrator for the detail, the Search Filter String very much depends on the AD/LDAP Server setup, ensure that each user(s) must be configured with OU.

- **Attributes Names:**

AD/LDAP records with empty value in both Mobile Number and Email Address attributes will not be downloaded or synced.

- **User Name:** default as 'samaccountname'.
- **Display Name:** default as 'displayname'.
- **Mobile Numbering:** default as 'mobile'.
- **Email Address:** default as 'mail'.

When the one time setup is ready, access to Download Contact (Tab), select the required parameters follow by Download to proceed:

The screenshot shows the 'Download Contact' tab with the following settings:

- User Group:**
 - ☐ Use AD/LDAP group (memberof)
 - ☒ IT
 - ☐ Marketing
 - ☐ Sales
- User Roster:** 8to5
- Modem Label:** None

Buttons: Download, Cancel

Figure 8-1-8: Download Contact

Depending on the parameters that defined on Figure 8-1-7: AD/LDAP Setup, sendQuick will extract the required data accordingly from AD/LDAP Server, check and Preview the uploaded detail and select 'Save' to proceed, otherwise select Cancel and redefine your parameter on Figure 8-1-7: AD/LDAP Setup.

Preview Phone Book Entry

Show entries Search:

No	User Name	Display Name (AD)	Mobile Number	Call Number	Email Address	Group	OU Name
1	BulkUser1	Bulk User 1	900000001				BulkOU
2	BulkUser10	Bulk User 10	900000010				BulkOU
3	BulkUser100	Bulk User 100	900000100				BulkOU
4	BulkUser1000	Bulk User 1000	900001000				BulkOU
5	BulkUser101	Bulk User 101	900000101				BulkOU
6	BulkUser102	Bulk User 102	900000102				BulkOU
7	BulkUser103	Bulk User 103	900000103				BulkOU
8	BulkUser104	Bulk User 104	900000104				BulkOU
9	BulkUser105	Bulk User 105	900000105				BulkOU
10	BulkUser106	Bulk User 106	900000106				BulkOU

Showing 1 to 10 of total 992 records

Previous **1** 2 3 4 5 ... 100 Next

Save Cancel

Figure 8-1-9: Preview Phone Book Entry

Upon user's confirmation, the AD/LDAP data will be uploaded to sendQuick's Phone Book.

Phone Book Records									
Addressbook Group									
Show 10 entries		Search: <input type="text"/>							
No	User Name	Display Name (AD)	Mobile Number	Call Number	MIM Subscription	Email Address	Group	Roster	
1	BulkUser1	Bulk User 1	900000001				M15907372189	8to5	<input type="checkbox"/>
Modem Label									
Type AD									
OU Name BulkOU									
2	BulkUser10	Bulk User 10	900000010				M15907372189	8to5	<input type="checkbox"/>
3	BulkUser100	Bulk User 100	900000100				M15907372189	8to5	<input type="checkbox"/>
4	BulkUser1000	Bulk User 1000	900001000				M15907372189	8to5	<input type="checkbox"/>
5	BulkUser101	Bulk User 101	900000101				M15907372189	8to5	<input type="checkbox"/>
6	BulkUser102	Bulk User 102	900000102				M15907372189	8to5	<input type="checkbox"/>
7	BulkUser103	Bulk User 103	900000103				M15907372189	8to5	<input type="checkbox"/>
8	BulkUser104	Bulk User 104	900000104				M15907372189	8to5	<input type="checkbox"/>
9	BulkUser105	Bulk User 105	900000105				M15907372189	8to5	<input type="checkbox"/>
10	BulkUser106	Bulk User 106	900000106				M15907372189	8to5	<input type="checkbox"/>
Add New Record Upload CSV AD/LDAP Setup Delete									

Figure 8-1-10: Phone Book records

SendQuick allows user to define 'Auto Sync on Phone Book', access to Auto Sync Contact(tab) to defined your prefer timing:

AD/LDAP Setup		Download Contact	Auto Sync Contact				
Auto Sync Status	<input type="text" value="Enable"/>						
Auto Sync Group	<input type="text" value="Disable"/>						
Auto Sync Time (HH : MM)	<input type="text" value="21"/> : <input type="text" value="30"/>						
					Auto Sync AD/LDAP Group (memberOf) to Phone Book Group		
					<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Figure 8-1-11: Auto Sync Contact

- **Auto Sync Status:** Disable/Enable.
- **Auto Sync Group :** Disable/Enable.
- **Auto Sync Time (HH:MM):** define your prefer timing to perform auto sync with AD/LDAP Server.

8.2 MIM Phone Book Records

Start the MIM Phone Book record synchronize by selecting the **MIM Phone Book Records** from the navigation menu, select the 'Sync Recipient' button, a summary list of the records will be shown in Figure 8-3 below. The summary list shows the respective Recipient ID, Recipient Name, Type MIM Origin, MIM Routing and Opt-in Date.

Phone Book & Roster > **MIM Phone Book Records**

Show 10 entries Search:

No	Recipient ID	Recipient Name	Type	MIM Origin	MIM Routing	Opt-In Date	
1	0bc662fa-6a15-4504-1e3e-8780ea4cbcd5		Group	MICROSOFT TEAMS		22/12/2019	<input type="checkbox"/>
2	d77e58fc-bf29-eb41-b374-f811269d0710		Group	LINE	Line Notify - YM test	08/10/2019	<input type="checkbox"/>
3	f3a71572-a86b-2b66-4d04-01c3adfd5f1f		Individual	FACEBOOK	Conversa - sendquick - FB Bot	16/12/2019	<input type="checkbox"/>
4	16fcd6c1-5960-145a-4440-1c9ad353cdb2		Group	WEBEX TEAMS	Wafie WEBEX TEAMS	23/12/2019	<input type="checkbox"/>
5	9848392b-7073-2d5c-ecef-101c13aefec6		Individual	FACEBOOK	AI Chat Bot - FB	25/10/2019	<input type="checkbox"/>
6	cd137466-0194-e289-1688-485e8b2f3389		Individual	FACEBOOK	FB SQBOT	07/08/2019	<input type="checkbox"/>
7	005e201c-9934-0ee0-e28f-cd2eb3ac686e		Group	MICROSOFT TEAMS	MSTeamsTestBot	22/12/2019	<input type="checkbox"/>
8	1cbe67b0-b84a-2bc5-699d-7edb93aff772		Individual	LINE	LINE SQBOT	06/11/2018	<input type="checkbox"/>
9	814dcbc7-f57e-cb11-e41d-7116679e5585	01	Individual	WECHAT WORK	Test Wechat Work	13/03/2019	<input type="checkbox"/>
10	aefc1501-cc3d-2836-9640-4da0da37ab0d	0131.80	Individual	TELEGRAM	TELEGRAM SQBOT	09/05/2019	<input type="checkbox"/>

Save CSV Sync Recipient Delete

Showing 1 to 10 of total 272 records

Previous 1 2 3 4 5 ... 28 Next

Figure 8-3: MIM Phone Book Records

8.3 Roster Management

The Roster Management defines the time period and the days that a particular individual (groups) will receive the SMS if the event is triggered. This is also commonly known as duty roster module.

Select the **Roster Management** (in the Navigation Menu) and the summary will be shown (Figure 8-4). The Roster Management section needs to be configured first before allocating the roster to the users in the Phone Book Rerecords module (Section 8.1).

Phone Book & Roster > **Roster Management**

Show 10 records Search:

No	Roster Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	
1	All Day	Y (0000-2359)	Y (0000-2359)	Y (0000-2359)	Y (0000-2359)	Y (0000-2359)	Y (0000-2359)	Y (0000-2359)	
2	Night Shift	N	Y (1800-2359,0000-0600)	Y (1800-2359,0000-0600)	Y (1800-2359,0000-0600)	Y (1800-2359,0000-0600)	Y (1800-2359,0000-0600)	N	
3	Weekend Shift	Y (0000-2359)	N	N	N	N	Y (1800-2359,0000-0600)	Y (0000-2359)	

Add New Record Delete

Showing 1 to 3 of total 3 records

Previous 1 Next

Figure 8-4: Roster Management

Select the **Add New Record** button and Figure 8-5 for creation of a new roster will be shown. Specify the **Roster Name**, select the relevant **Day** and insert the **Shift Time** in 24 hour (HHMM) format. The time range will be in the form of HHMM-HHMM. If there are multiple time slots per day, use a comma to separate the different time slots. Click **Save** once done.

New Roster

Roster Name

New roster

Day Selected:

☐ Sunday

Roster Time:

☒ Monday

Roster Time:

0900-1700

☒ Tuesday

Roster Time:

0900-1700

☒ Wednesday

Roster Time:

0900-1700

☒ Thursday

Roster Time:

0900-1700

☒ Friday

Roster Time:

0900-1700

☐ Saturday

Roster Time:

Roster Time format is HHMM-HHMM, eg: 1pm to 6pm is 1300-1800. Use ',' to separate different time range.

☒ No specific day selection.

Save

Cancel

Figure 8-5: New Roster

There are instances where a shift is only for a particular period and not repeated, eg, from 8 April to 12 April only. In this instance, un-check the **No Specific Day Selection** option and a calendar as shown in Figure 8-6 below appears. Browse to the relevant month and select the dates that are applicable. All required dates need to be selected. To un-select, click on the selected dates again and the highlight will disappear.

☐ No specific day selection.

☒ Selected days are included for alerts. Uncheck will set the day as day NOT receiving alerts.

«

April 2019

»

Su	Mo	Tu	We	Th	Fr	Sa
31	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	1	2	3	4
5	6	7	8	9	10	11

Save

Cancel

Figure 8-6 New Roster Specific Day Selection

You can also select the dates across different years. Once the selection is completed, select **Save** and the dates are saved for the Shift.

8.4 AD/LDAP OU Alert

This function will allow administrator to configure the feature that scan the incoming email with DD/LDAP OU Name, eg email Template: [ou_name]@SendQuick IP/Host.Domain]. The matched email will trigger alerts to members in the OU. Define the parameters accordingly follow by Save to proceed.

Phone Book & Roster > AD/LDAP OU Alert

AD/LDAP OU Alert
OU Group Settings

This feature will scan the incoming emails with AD/LDAP OU Name. Email Template : [ou_name]@[SendQuick IP/Host.Domain]. The matched email will trigger alerts to members in the OU.

Buffer Threshold

Count : 5 times

Time : 3 minutes

Configure buffer threshold for Email to OU alerts, to avoid repeated SMS alerts. Only email alerts will be sent after buffer threshold.
Count - Number of times of the event/message.
Time - Buffer time in minutes.

OU SMS Alert Template

xSUBx xMSGx

Variables
xFRx : Original Email From
xSUBx : Original Email Subject
xMSGx : Original Email Message Content

[Default value](#) : xSUBx xMSGx

OU Email Alert Template

OU Email From
xFRx

OU Email Subject
xSUBx

Email Message Template
xSUBx xMSGx

Variables
xFRx : Original Email From
xSUBx : Original Email Subject
xMSGx : Original Email Message Content

[Default values](#)
From : xFRx
Subject : xSUBx
Content : xMSGx

Save Reset

Figure 8-7: New Roster Specific Day Selection

8.5 Delete AD/LDAP Contacts

This function will allow administrator to delete the configured AD/LDAP Contacts. Select the checkbox beside the record follow by **Delete** button to proceed.

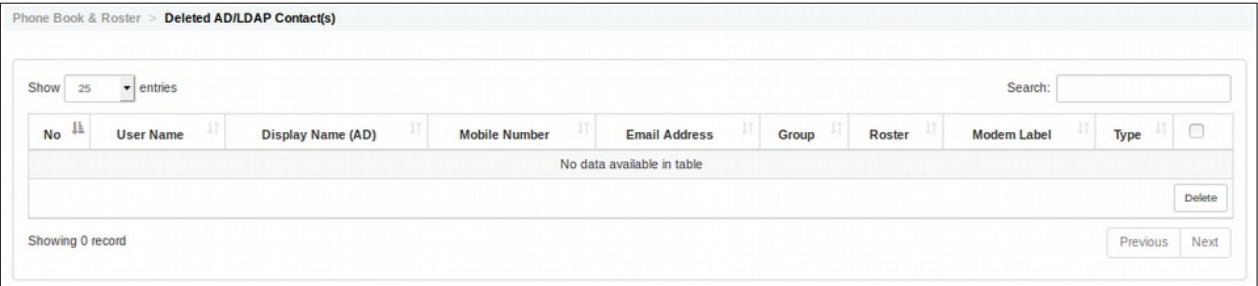


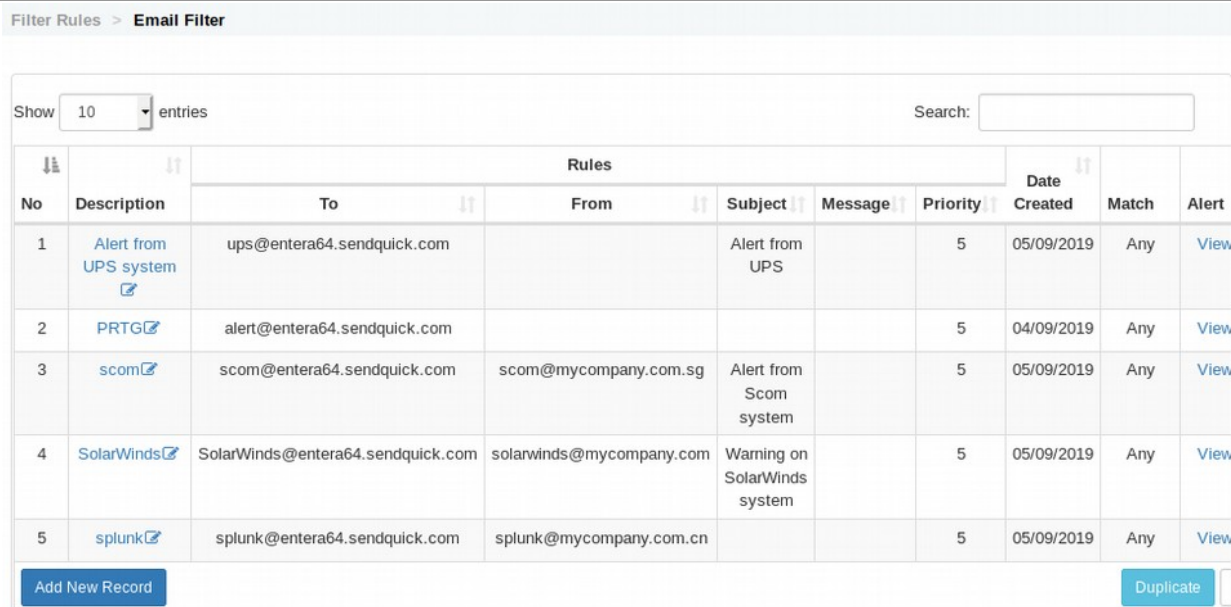
Figure 8-8: New Roster Specific Day Selection

9 Filter 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.

9.1 Email Filter

The Email Filter is for 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 SMS text to the recipients. All messages that were sent to Email Filter will be filtered in accordance to the message filter rules (Figure 9-1).



The screenshot shows the 'Filter Rules > Email Filter' page. It includes a 'Show 10 entries' dropdown and a search bar. Below is a table with 10 columns: No, Description, To, From, Subject, Message, Priority, Date Created, Match, and Alert. There are 5 rows of filter rules listed. At the bottom, there are 'Add New Record' and 'Duplicate' buttons.

No	Description	To	From	Subject	Message	Priority	Date Created	Match	Alert
1	Alert from UPS system	ups@entera64.sendquick.com		Alert from UPS		5	05/09/2019	Any	View
2	PRTG	alert@entera64.sendquick.com				5	04/09/2019	Any	View
3	scom	scom@entera64.sendquick.com	scom@mycompany.com.sg	Alert from Scom system		5	05/09/2019	Any	View
4	SolarWinds	SolarWinds@entera64.sendquick.com	solarwinds@mycompany.com	Warning on SolarWinds system		5	05/09/2019	Any	View
5	splunk	splunk@entera64.sendquick.com	splunk@mycompany.com.cn			5	05/09/2019	Any	View

Figure 9-1: Email Filter summary

Select the **Email Filter** from the navigation menu and the **Email Filter Summary** will be shown (in Figure 9-1). The Message Filter section need to be configured carefully to provide the right rules for SMS alert. It is fine if you configure the Message Filter on a later stage as it has no impact on the operation of sendQuick system. The Message Filter will be useful for the selective sending of alert messages using SMS.

The email summary list all the message filters that had been created in the system. You can create as many message filters as required. In Figure 9-2, **Email Forwarding** button is for creating email address to forward (redirect) the email to other email addresses. Select on the **Email Forwarding** button (in Figure 9-1) and Figure 9-2 with configuration option will be shown. You can also configure the time buffer that will ignore any repeated messages during the buffer period (Figure 9-3 below).

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 buffer timer (Figure 9-3) 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.

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** (eg, 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 (in Figure 9-2) 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.

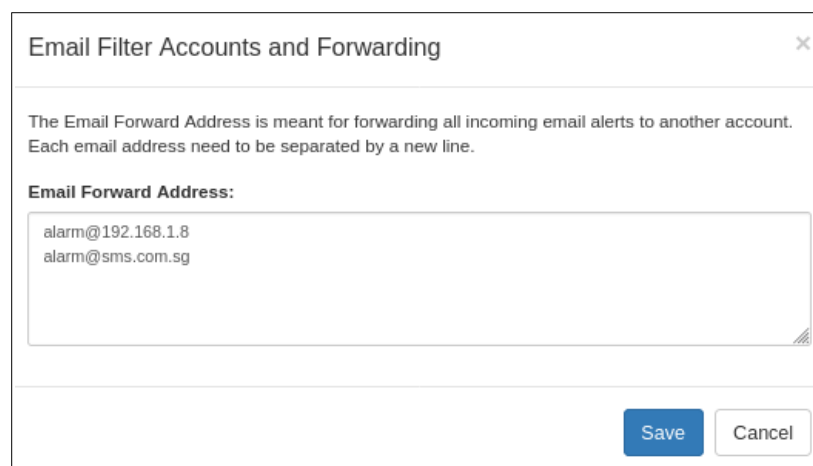


Figure 9-2: Email Filter Accounts and Forwarding

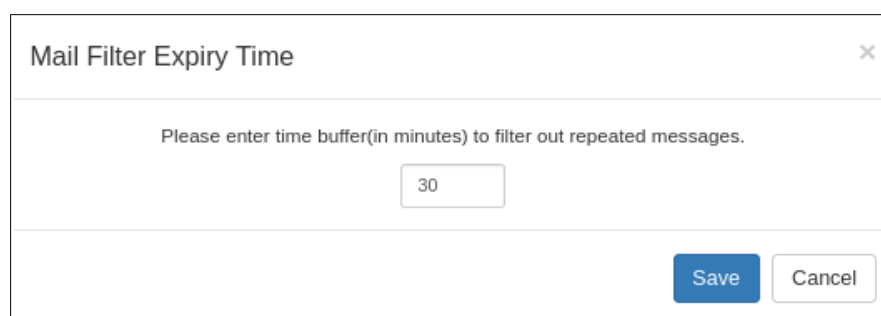


Figure 9-3: Mail Filter Expiry Time

a) Create New Message Filter

The administrator can create new message filters by selecting the **Add New Record** button. The interface to add a new filter rule is shown in Figure 9-4 below.

Edit Mail Filter Rule

Description: PRTG

Variables Usage

Mail To ☒ prtgalerts@entera.sendquick.asp.com

Mail From ☐

Subject ☐

Message ☐

Match Mode: ☐ ALL ☒ ANY

Priority: 5

Save Cancel

Figure 9-4: Add Mail Filter Rule

The filter works by checking on the attributes of the email message. They are the receiver email address (**To**), sender email address (**From**), **Subject** field and **Message** body content. There is a checkbox on the side of the field name. If the desired field name is required for filtering, just checked the box. Then, fill in the required content that will be used to filter the messages. You can select more than one checkbox and determine the relationship as AND (All) and OR (Any) relationship. The SMS alert will be sent only if the criteria are fulfilled.

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 is in the Variable Usage as shown in Figure 9-4 above.

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

<i>Sentence</i>	<i>Match Status</i>	<i>Reasons</i>
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' occur and not the whole phrase
There is an error message from system	Yes	The whole phrase 'error message' appears in the sentence.

Click **View** from the selected Email Filter summary as shown in Figure 9-1, and you will see the View Alert list page (Figure 9-5).

Alert SMS			Alert Email		Alert Message	R	E	Rpt	Edit
No	Manual Input	Phone Book User	Manual Input	Phone Book User					
1		Manager(+6512345670)	admin@talariax.com		xFRx:xSUBx:MSGx	Y	Y	Y	Edit

Showing 1 to 1 of total 1 records

Figure 9-5: View Alert

Select **Add New Record** to add a new alert list to that rule. Once the system matched the relevant words (or characters) and phrase, it will send the SMS messages to the mobile number, email or group as indicated in the **Alert Receiver** field (Figure 9-6). You can insert more than one mobile number/email, one record per line. To send to overseas numbers, please include the '+' sign and country code, followed by the mobile number, e.g. +6512345670 for Singapore mobile number, where the prefix '+65' is the country code for Singapore.

The default message is: xFRx:xSUBx:MSGx where:

- xFRx is From
- xSUBx is the Email subject
- xMSGx is the Email message

Figure 9-6: Add Alert – Alert Receiver

If the Phone Book module is added, you can select the Alert Receiver directly from the Phone Book by clicking the **Select from Phone Book** button.

The actual content of the SMS alert will be the original content of the email message and the fields to be sent (FROM, SUBJECT and MESSAGE) will depends on the selection in the SMS Messaging Setup in Section 6. The message can be customised if there are characters inserted in the **Text Box** shown in Figure 9-6. The customised message can include additional words and the original FROM, SUBJECT and MESSAGE from the email notifications by placing the variable **xFRx** (FROM Field), **xSUBx** (SUBJECT Field) and **xMSGx** (MESSAGE Field).

The message length and other content of the email alert message (that will be sent via SMS if the message alert checkbox is not selected) will be determined in the **SMS System Setup** under the

multiple SMS per email and other functions in the set-up section. Please refer to the SMS System Setup in the manual for more information.

b) Configure Reminder, Escalation and Report

The next configuration is the **Reminder**, **Escalation** and **Report** function as shown in Figure 9-7 below.

Figure 9-7: Add Alert – Reminder, Escalation and Report

Choose either the **Reminder**, **Escalation** or **Report** tab. Then select the **Yes** checkbox to activate the setting and complete the time setting in minutes. The value means how long does the time lapse before a SMS is sent. The reminder will only be sent if there is no acknowledgment within the time set. If you wish to always include SMS in reminder, escalation or report delivery, just tick “Always include SMS”. This option will overwrite Alert Profile to include SMS delivery.

When either reminder or escalation is selected (activated), the SMS message will include an ID value (e.g., ID: 25) which is a numeric value. To respond to the case, reply the SMS with the number (e.g., 25) and send back to sendQuick. This SMS acknowledgment will stop the reminder and escalation process. However, if no acknowledgment is received (from any alertee), the reminder (once) and then escalation will be triggered.

For acknowledgment reply, user will need to reply the message with the message ID that appears on the SMS message. The reply message must have the message ID as the first word. The email reminder and escalation has no acknowledgment function. It serves as information purposes only.

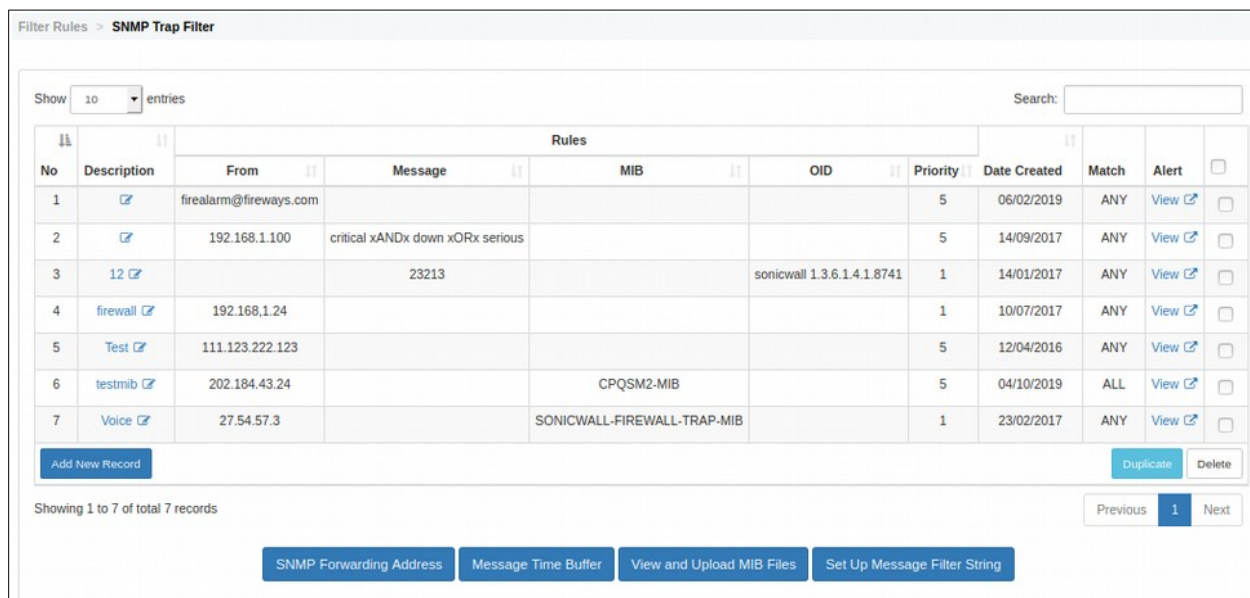
The phone numbers to receive the reminder will be the original alertee list that was configured to receive the SMS. For escalation, you can select from the Phone Book or group or insert the numbers in the text box provided. Similarly, if the SMS is acknowledged before the escalation is triggered, the escalation message will not be sent.

If there is no SMS acknowledgment from any recipients despite the reminders and escalation, a SMS summary report will be sent at the end of the time session that was configured for the **Report**. The report will consist of the summary of the mobile numbers that acknowledged and those that did not.

9.2 SNMP Trap Filter

sendQuick 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 SMS message. Select the SNMP Trap Filter option on the left navigation bar and you will see the SNMP Trap Filter Summary page (Figure 9-8).

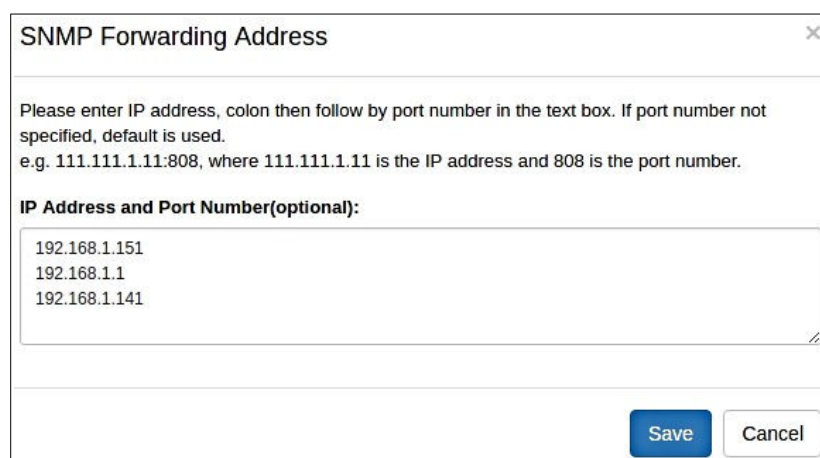


The screenshot shows the 'SNMP Trap Filter' summary page. It features a table with 7 records, each representing a filter rule. The table columns include No, Description, From, Message, MIB, OID, Priority, Date Created, Match, Alert, and a checkbox. Below the table are buttons for 'Add New Record', 'Duplicate', and 'Delete'. At the bottom, there are buttons for 'SNMP Forwarding Address', 'Message Time Buffer', 'View and Upload MIB Files', and 'Set Up Message Filter String'. The status bar indicates 'Showing 1 to 7 of total 7 records'.

No	Description	From	Message	MIB	OID	Priority	Date Created	Match	Alert	
1	firealarm	firealarm@fireways.com				5	06/02/2019	ANY	View	<input type="checkbox"/>
2	critical xANDx down xORx serious	192.168.1.100				5	14/09/2017	ANY	View	<input type="checkbox"/>
3	23213				sonicwall 1.3.6.1.4.1.8741	1	14/01/2017	ANY	View	<input type="checkbox"/>
4	firewall	192.168.1.24				1	10/07/2017	ANY	View	<input type="checkbox"/>
5	Test	111.123.222.123				5	12/04/2016	ANY	View	<input type="checkbox"/>
6	testmib	202.184.43.24		CPQSM2-MIB		5	04/10/2019	ALL	View	<input type="checkbox"/>
7	Voice	27.54.57.3		SONICWALL-FIREWALL-TRAP-MIB		1	23/02/2017	ANY	View	<input type="checkbox"/>

Figure 9-8: SNMP Trap Filter summary

Before configuring any trap messages, you may wish to configure the SNMP Forwarding which allows all incoming SNMP Trap messages to be forwarded to another server as Syslog messages. The interface to configure is as shown in Figure 9-9 below.



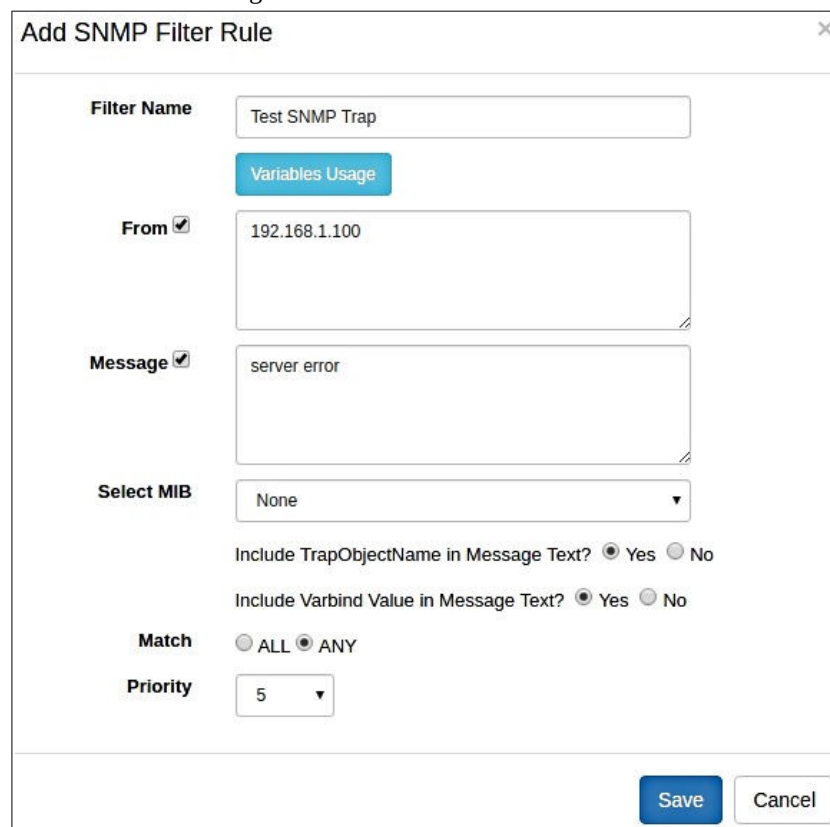
The dialog box is titled 'SNMP Forwarding Address'. It contains instructions: 'Please enter IP address, colon then follow by port number in the text box. If port number not specified, default is used. e.g. 111.111.1.11:808, where 111.111.1.11 is the IP address and 808 is the port number.' Below this, there is a section 'IP Address and Port Number(optional):' with a text input field containing the following text: '192.168.1.151', '192.168.1.1', and '192.168.1.141'. At the bottom right, there are 'Save' and 'Cancel' buttons.

Figure 9-9: SNMP Forwarding Address

You can also set the message time buffer, which will ignore repeated messages if it occurs within the time buffer. The time buffer setting is in minutes and similar to Figure 9-9 above.

When configuring a new SNMP Trap filter, enter the relevant data and select ALL or ANY for the filter relationship. The key difference is the FROM field is the IP address of the incoming SNMP Trap device (Figure 9-10). The actual process is similar to Email Filter as illustrated in **Section 9.1** above.

Figure 9-10: Add SNMP Filter Rule



The 'Add SNMP Filter Rule' dialog box contains the following fields and options:

- Filter Name:** Text input field with 'Test SNMP Trap'.
- Variables Usage:** Blue button.
- From:** Text input field with '192.168.1.100' and a checkmark icon.
- Message:** Text input field with 'server error' and a checkmark icon.
- Select MIB:** Dropdown menu with 'None' selected.
- Include TrapObjectName in Message Text?:** Radio buttons for 'Yes' (selected) and 'No'.
- Include Varbind Value in Message Text?:** Radio buttons for 'Yes' (selected) and 'No'.
- Match:** Radio buttons for 'ALL' and 'ANY' (selected).
- Priority:** Dropdown menu with '5' selected.
- Buttons:** 'Save' (blue) and 'Cancel' (white) at the bottom right.

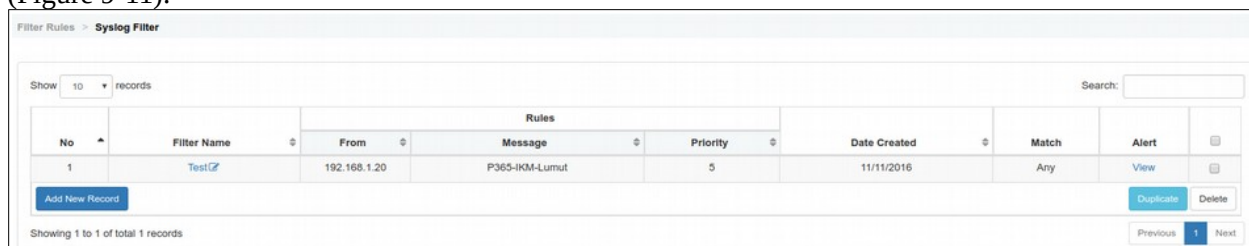
You can also upload the MIB file and select the MIB file for filtering. The MIB upload can be done by selecting **View and Upload MIB Files** in the SNMP Trap Filter Summary (Figure 9-8).

Similar to Email Filter, you can configure the SMS and Email alerts as well as a custom message for alerting. The escalation options are also similar to Email Filter and you can refer to **Section 9.1** for more details.

9.3 Syslog 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** and SendQuick uses RFC3164 as default syslog message template.

Select the Syslog Filter option on the left navigation bar and you will see the Syslog Filter summary (Figure 9-11).



The Syslog Filter summary table displays the following data:

No	Filter Name	From	Message	Priority	Date Created	Match	Alert
1	Test	192.168.1.20	P365-RM-Lumut	5	11/11/2016	Any	View

Below the table, there is an 'Add New Record' button and a status bar indicating 'Showing 1 to 1 of total 1 records'. At the bottom right, there are 'Duplicate' and 'Delete' buttons, and a pagination control showing 'Previous', '1', and 'Next'.

Figure 9.11: Syslog Filter summary

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. The interface to configure is similar to SNMP Trap as shown in Figure 9-8.

The rest of the process is also similar to Email Filter and you can refer to **Section 9.1** for more details.

10 Network Monitor

10.1 Ping Check

SendQuick (Alert Plus and Entera) has a server monitoring function using ICMP Ping, Port (Entera only) checks (Entera only) feature. This allows sendQuick to ping and check another machine and send a SMS alert if there is no server response within the specified time. Select **Network Monitor > Ping Check** (as an example) from the menu and the summary is shown in Figure 10-1 below.

Network Monitor > Ping Check

Expand

🟢 = Normal Interval (minute) 🟡 = Failure Interval (minute)

Show 5 entries Search:

No	Server Info	Message Receiver	Message	Status	Enable	Edit
1	192.168.1.8 (Web Server) 🟢 10 🟡 5 Priority: 5 Status Alert: Disable	Alert Mode: Continuous Alert Message: N/A Alert Email: N/A Alert Voice: N/A Alert Group: N/A	xIPx is not reachable From: system@entera64.sendquick.me Subject: Ping Check Alert => Host: xIPx Message: xIPx is not reachable xIPx is not reachable	🟢	Y	Edit

Create Enable Rule Disable Rule Delete

Figure 10-1: Ping Check

Select the **Create** button and you can add a server to monitor as shown in Figure 10-2 below. Enter the information required as described in the table below follow by SAVE.

Network Monitor > Add a Server to Monitor

Description: Our Web Server

Server IP: 192.168.1.151

Priority: 5

Alarm Trigger Mode: 1st Trial Failed
 1st Trial Fail - If no response, the system will be marked as fail, and the alert will be triggered immediately once all test ping packet failed.
 2nd Trial Fail - If no response, the system will be marked as fail, but the alert will be triggered on the 2nd fail attempt. The frequency of the 2nd fail attempt will be based on the Monitoring Frequency Upon Failure.

No. of Attempts: 10
 If No. of Attempt is set to 0 or left blank, it will be defaulted to 1.

Attempt Timeout: 5 seconds
 If Attempt Timeout is set to 0 or left blank, it will be defaulted to 5 seconds.

Alarm Threshold: 10
 The threshold that will be used to trigger the alarm. The value should be lower than the No. of Attempt. If it exceeds the value, it will only trigger the alarm upon all failed attempts.

Monitoring Interval (Time): 10 minutes
 If set to 0, the system monitoring will be disabled. It is not recommended to set lower than 5 minutes for production system, as ICMP ping will generate a lot of network traffic.

Monitoring Interval (Upon Failure): 5 minutes
 If set to 0, the system will use the value defined in the Monitoring Interval.

Server Status Alert: Disable
 * If alert is hourly, set in minutes.
 * HH is from 00 - 23.

Figure 10-2 Add a Server to Monitor

You can also **Enable** or **Disable** the defined rule(s) by selecting the respective functional button on Figure 10-1. This will assist when the rule need to be suspended during a maintenance process.

10.2 URL Check

The URL Check service is similar to Ping Check. SendQuick (Alert Plus and Entera) has a URL monitoring function, the URL Checks (Entera only) function allows sendQuick to monitor another machine and send a SMS alert if there is no server response within the specified time. Select Network Monitor > URL Check (as an example) from the menu and the summary is shown in Figure 10-3 below.

Network Monitor > URL Check

Expand

🟢 = Normal Interval (minute) 🚫 = Failure Interval (minute)

Show 5 entries Search:

No	Server Info	Message Receiver	Message	Status	Enable	Edit
1	google.com (Google) 🟢 10 🚫 5 Priority 5 Status Alert Disable	Alert Mode: Continuous Alert Message N/A Alert Voice N/A Alert Email N/A Alert Group N/A	xURLx is not reachable From: system@entera64.sendquick.me Subject: URL Check Alert => Host: xURLx Message: xURLx is not reachable xURLx is not reachable	🚫 ⚠️	Y	Edit 🗑️

Create Enable Rule Disable Rule Delete

Figure 10-3 URL Check

Select the **Create** button and you can add a server to monitor as shown in Figure 10-4 below. Enter the information required as described in the table below follow by SAVE.

Network Monitor > Edit a URL to Monitor

Description: Google

Target URL: google.com

Priority: 5

Alarm Trigger Mode: 1st Trial Failed

1st Trial Fail - If no response, the system will be marked as fail, and the alert will be triggered immediately once all test ping packet failed.
 2nd Trial Fail - If no response, the system will be marked as fail, but the alert will be triggered on the 2nd fail attempt. The frequency of the 2nd fail attempt will be based on the Monitoring Frequency Upon Failure.

No. of Attempts: 10

If No. of Attempt is set to 0 or left blank, it will be defaulted to 1.

Attempt Timeout: 5 seconds

If Attempt Timeout is set to 0 or left blank, it will be defaulted to 5 seconds.

Alarm Threshold: 10

The threshold that will be used to trigger the alarm. The value should be lower than the No. of Attempt. If it exceeds the value, it will only trigger the alarm upon all failed attempts.

Monitoring Interval (Time): 10 minutes

If set to 0, the system monitoring will be disabled. It is not recommended to set lower than 5 minutes for production system, as ICMP ping will generate a lot of network traffic.

Monitoring Interval (Upon Failure): 5 minutes

If set to 0, the system will use the value defined in the Monitoring Interval.

Server Status Alert: Disable

* If alert is hourly, set in minutes.
 * HH is from 00 - 23.

Figure 10-4 Add a URL to Monitor

You can also **Enable** or **Disable** the defined rule(s) by selecting the respective functional button on Figure 10-4. This will assist when the rule need to be suspended during a maintenance process.

10.3 Port Check

The Port Check service is only available in sendQuick Entera and is similar to Ping Check.

Network Monitor > Edit a Server & Port to Monitor

Description	Alert Server - 96		
Server IP	192.168.1.96		
Port No	25		
Priority	5 ▼		
Alert Mode	Continuous ▼	Continuous - the system will send the SMS alert based on the Monitoring Frequency defined. Once - the system will send the SMS alert once only, upon detecting the server offline.	
Alarm Trigger Mode	1st Trial Failed ▼	1st Trial Fail - If no response, the system will be marked as fail, and the alert will be triggered immediately once all test ping packet failed. 2nd Trial Fail - If no response, the system will be marked as fail, but the alert will be triggered on the 2nd fail attempt. The frequency of the 2nd fail attempt will be based on the Monitoring Frequency Upon Failure.	
No. of Attempts	10	If No. of Attempt is set to 0 or left blank, it will be defaulted to 1.	
Attempt Timeout	5 seconds	If Attempt Timeout is set to 0 or left blank, it will be defaulted to 5 seconds.	
Alarm Threshold	10	The threshold that will be used to trigger the alarm. The value should be lower than the No. of Attempt. If it exceeds the value, it will only trigger the alarm upon all failed attempts.	
Monitoring Interval (Time)	10 minutes	If set to 0, the system monitoring will be disabled. It is not recommended to set lower than 5 minutes for production system, as ICMP ping will generate a lot of network traffic.	
Monitoring Interval (Upon Failure)	5 minutes	If set to 0, the system will use the value defined in the Monitoring Interval.	
Server Status Alert	Disable ▼	* If alert is hourly, set in minutes. * HH is from 00 - 23.	
	Time: (HHMM)		
Send this message for alert:	ASCII Text (ISO-8895-1) ▼	The system will use the default message if alert message is set to blank. The default message is: xIPx is not reachable. Variable options: <ul style="list-style-type: none"> • xIPx is the server IP • xDESCx is the description • xDTMx is the date & time 	
	xIPx is not reachable		
Server online message:	ASCII Text (ISO-8895-1) ▼	If this field is left blank, no SMS will be sent. Use variable xIPx to display the server IP.	
	Alert Server - 96 is back to operation.		
Mobile Number to Receive SMS	Mobile Number to Receive Alert	Email Address to Receive Alerts	Group to Receive Alert
	94506718	alerter@talariax.com	
	Select from Phone Book		Select from Phone Book
<div>Save Cancel</div>			

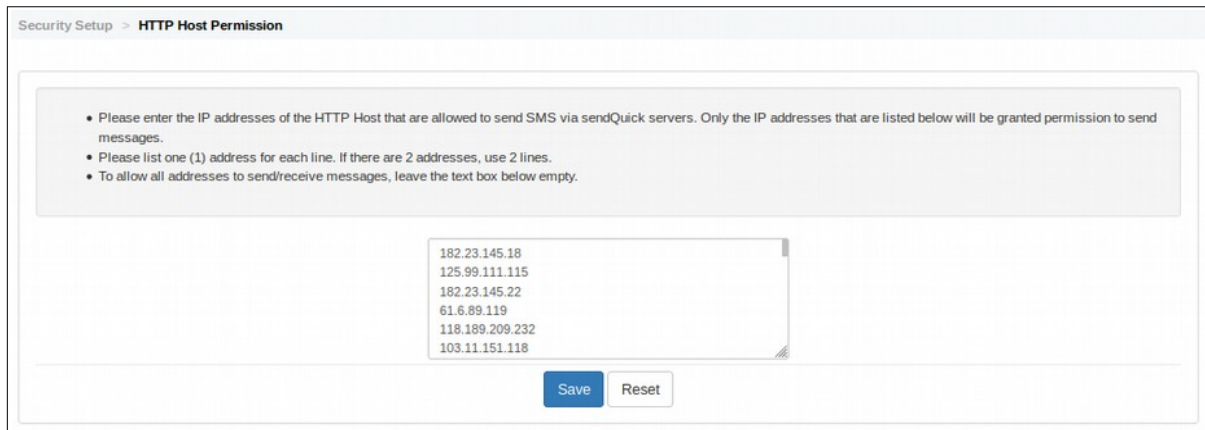
Figure 10-2: Add a Server to Monitor setting

Configuration	Description
Server IP/ Target URL	The IP address of the server for PING, Checking or the URL address
Port No	The port number for the port check service
Alert Mode	Either Once Only or Continuous. Once Only refers to sending SMS only one time when a check is failed. Continuous will send SMS for every check attempt that failed. <i>Note: The checking process will continue even if the response is failed.</i>
Alarm Trigger Mode	Configurable to trigger on the first time or the second time failure. 2nd Trial Failed means SMS will only be triggered when two consecutive failures occur.
No. of Attempts	Total number of test ping packet (or Port check or URL check) that will be sent.
Attempt Timeout	Refers to the waiting time to receive the response packet. If it is longer than the time configured (in seconds), the checking will fail.
Alarm Threshold	Total number of failed test packets before the SMS is sent. The higher the number, the less SMS will be triggered as it is less sensitive to failure.
Monitoring Interval	The time interval (in minutes) to perform each check. It is advised to be wide (> 10 minutes) to avoid any system and network overload due to too much traffic generated by the PING, Port and URL check packets.
Monitoring Interval (Upon Failure)	The interval (usually shorter) that will be used if there is a failure in server response. This will allow a more frequent checking when a failure occurs.
Server Status Alert	To enable/disable the successful server check status via SMS. It can be configured to send hourly or daily.
Message for alert	The system will use the default message if alert message is set to blank. The default message is: xIPx is not reachable. Use variable xIPx to display the server IP.
Server online message	The SMS message sent when the server is back online (failure is restored)
Mobile Number to Receive SMS	The list of phone numbers to receive the alerts when there is a failure or when server is back online. If Phone Book is present, just select the required numbers or groups or it can be a mixture of all entries. <i>Note: Email alerts will be sent together if the Phone Book entry contains email addresses.</i>

11 Security Setup

11.1 HTTP Host Permission

The sendQuick server Security Setup is done by allowing/disallow message sending by restricting the IP address of the originating message. This is done by blocking the IP addresses of the unapproved HTTP access.



Security Setup > HTTP Host Permission

- Please enter the IP addresses of the HTTP Host that are allowed to send SMS via sendQuick servers. Only the IP addresses that are listed below will be granted permission to send messages.
- Please list one (1) address for each line. If there are 2 addresses, use 2 lines.
- To allow all addresses to send/receive messages, leave the text box below empty.

182.23.145.18
125.99.111.115
182.23.145.22
61.6.89.119
118.189.209.232
103.11.151.118

Save Reset

Figure 11-1: HTTP Host Permission

To block these IP addresses, insert the IP addresses allowed into the text area provided under the relevant classification. Only one IP can be listed on one line. If more than one IP address, please use the next line. This approach is applicable to HTTP Host allow. If you wish to allow all IPs to access and send SMS, just leave the text box empty.

Please refer to Figure 11-1 for example and the table below for description.

Security Items	Description
HTTP Host Permission	The IP address that is allowed to send HTTP Post to sendQuick. If empty, all IPs allowed (no control).

11.2 SMTP Host Permission

The sendQuick server Security Setup is done by allowing/disallow message sending by restricting the IP address of the originating message. This is done by blocking the IP addresses of the unapproved SMTP host gateway IP (for e-mail to SMS).

Security Setup > SMTP Host Permission

- Please enter the IP addresses of the SMTP Host that are allowed to send SMS via sendQuick servers. Only the IP addresses that are listed below will be granted permission to send messages.
- Please list one (1) address for each line. If there are 2 addresses, use 2 lines.
- To allow all addresses to send/receive messages, leave the text box below empty.

110.5.104.50
202.184.41.231
192.168.3.69
52.51.2.152

Save Reset

Figure 11-2: SMTP Host Permission

To block these IP addresses, insert the IP addresses allowed into the text area provided. Only one IP can be listed on one line. If more than one IP address, please use the next line. This approach is applicable to SMTP Host Allow. If you wish to allow all IPs to access and send SMS, just leave the text box empty.

Please refer to Figure 11-2 for example and the table below for description.

Security Items	Description
SMTP Host Permission	The SMTP IP address that is allowed to send SMTP email to sendQuick (email to SMS). If empty, all IPs allowed (no control).

11.3 Email User Permission

The sendQuick server Security Setup is done by allowing/disallow message sending by restricting the email addresses of the originating SMS sender. This is done by blocking the email addresses of the unauthorized access.

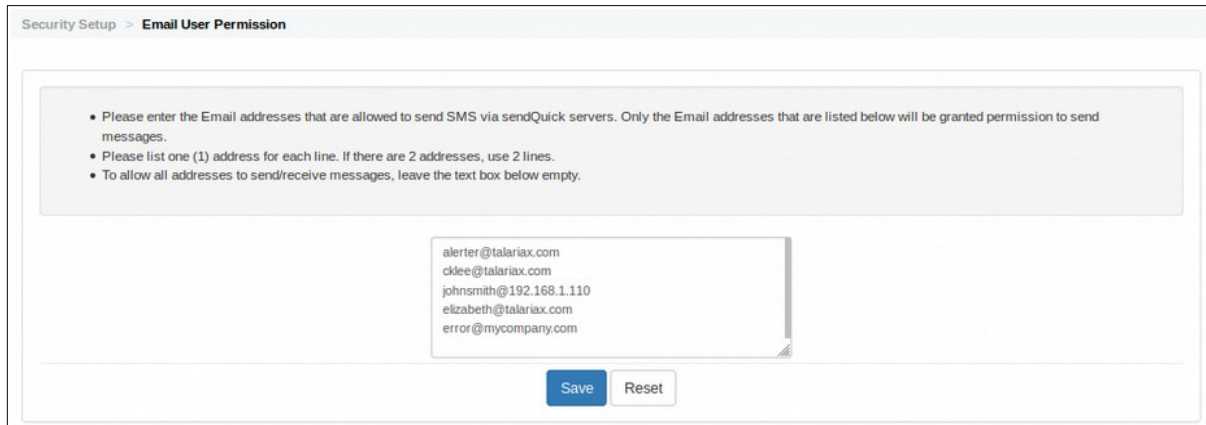


Figure 11-3: Email User Permission

To block these email addresses, insert the email addresses allowed into the text area provided. Only one email can be listed on one line. If more than one email address, please use the next line. This approach is applicable to email address allow. If you wish to allow all emails to access and send SMS, just leave the text box empty.

Please refer to Figure 11-3 for example and the table below for description.

Security Items	Description
Email User Permission	The email address (From) that is allowed to send Email-to-SMS. If empty, all email address is allowed.

11.4 Relay Host Permission

The sendQuick server Security Setup is done by allowing/disallow message sending by restricting the SMTP gateway IP address of the originating message. This is done by blocking the SMTP gateway IP addresses of the unapproved SMTP gateway IP (for e-mail to SMS).

Security Setup > Relay Host Permission

- SMTP Relay Host Permission is only meant for machines which need to use the sendQuick servers as SMTP gateway. Only the IP addresses that are listed in the text box will be granted permission for SMTP relaying.
- Please list one (1) address for each line. If there are 2 addresses, use 2 lines.
- To block all addresses, leave the text box below empty.

182.20.1.18
192.168.1.8
10.10.1.8
172.168.1.100

Save Reset

Figure 11-4: Relay Host Permission

To block these IP addresses, insert the IP addresses allowed into the text area provided. Only one IP can be listed on one line. If more than one IP address, please use the next line. This approach is applicable to SMTP Host Allow. If you wish to allow all IPs to access and send SMS, just leave the text box empty.

The system also allows user or server to use sendQuick as a SMTP relay. No SMTP relay allowed (no IP address specified) by default. If you wish to allow SMTP relay for some servers or users, please include their IP addresses in the box provided. Please refer to Figure 11-4 for example and the table below for description.

Security Items	Description
Relay Host Permission	The SMTP IP that are allowed to perform email relay using sendQuick. If no IP stated, NO SMTP relay is allowed (relay disallowed)

11.5 Database Connection Permission

The sendQuick server Security Setup is done by allowing/disallow database access by restricting the IP address of the system. This is done by blocking the IP addresses of the unapproved Database access.

Security Setup > Database Connection Permission

- Please enter the IP addresses of the Database Connection that are allowed to send SMS via sendQuick servers. Only the IP addresses that are listed in the text box below will be granted permission to send messages.
- Please list one (1) address for each line. If there are 2 addresses, use 2 lines.
- To allow all addresses to send/receive messages, leave the text box below empty.

192.168.3.68
192.168.1.20
10.1.1.8

Save Reset

Figure 11-5: Database Connection Permission

To block these IP addresses, insert the IP addresses allowed into the text area provided. Only one IP can be listed on one line. If more than one IP address, please use the next line. This approach is applicable to Database connection allow. If you wish to allow all IPs to access the Database, just leave the text box empty.

Please refer to Figure 11-5 for example and the table below for description.

Security Items	Description
Database Connection Permission	The Database server IP that are allowed to perform ODBC connection to sendQuick. If not IP stated, no ODBC connection is allowed.

11.6 Mobile Number Permission

The sendQuick server Security Setup is done by allowing/disallow message receiving by restricting the mobile number of the receiver.

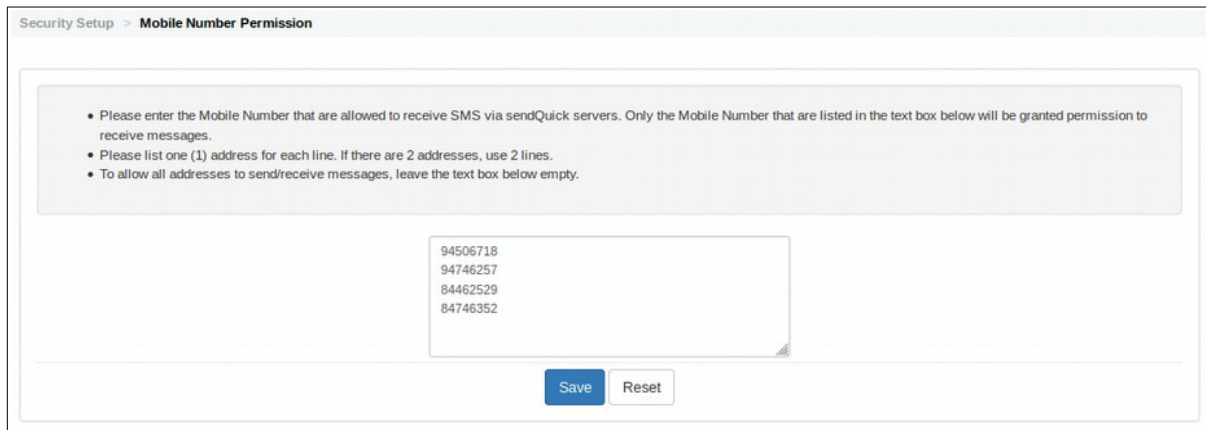


Figure 11-6: Mobile Number Permission

To block these mobile number, enter the mobile number that allowed into the text area provided. Only one mobile number can be listed on one line. If more than one mobile number, please use the next line. If you wish to allow all mobile numbers to receive SMS, just leave the text box empty.

Please refer to Figure 11-6 for example and the table below for description.

Security Items	Description
Mobile Number Permission	The list of mobile numbers that will receive SMS from sendQuick. If no numbers in the list, sendQuick can send to any number.

11.7 System Services

sendQuick also allows you to control the system services to enhance the security access. Administrator can choose to turn-on/turn-off the services as and when required. Select **System Services** from the menu and the list of services will be shown as in Figure 11-7 below.

Security Setup > System Services

These are the services used by sendQuick. You may enable or disable these services by selecting the checkbox below.

Search:

No	Description	Protocol	Port Number	Enable	Priority
1	PostgreSQL port. Internal application specific port	TCP	5432	Enable	Mandatory
2	FTP. For FTP-SMS feature	TCP	21	<input checked="" type="checkbox"/>	Optional
3	SSH port	TCP	22	<input checked="" type="checkbox"/>	Optional
4	SMTP. For SMTP-SMS and mail filtering feature.	TCP	25	<input checked="" type="checkbox"/>	Optional
5	DNS caching service. Only used by internal task for host and domain resolution	UDP	53	<input checked="" type="checkbox"/>	Optional
6	SNMP Trap, for SNMP Trap filtering	UDP	162	<input checked="" type="checkbox"/>	Optional
7	Syslog, for Syslog filtering	UDP	514	<input checked="" type="checkbox"/>	Optional

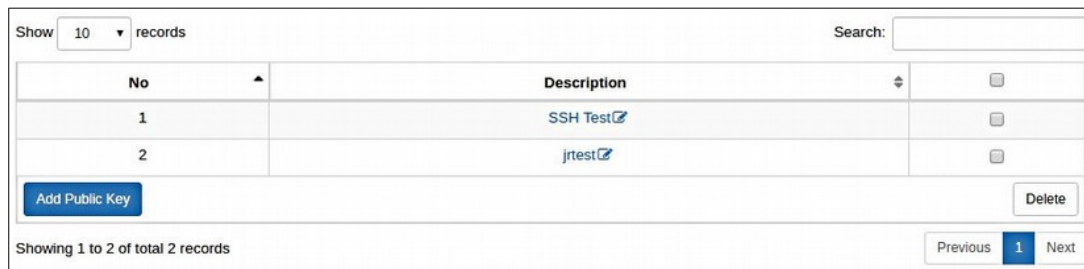
Figure 11-7: System Services

Apart from the default/compulsory services, you can uncheck the non-essential service and select Save. This will disable the service in sendQuick.

11.8 SSH Remote Access

Another enhanced security function in sendQuick is the SSH Remote Access. This is a more secure implementation as it requires more than just username and password. Before using this function, you need to create a public key with a key generator (e.g.: PuTTYGen) (Figure 11-8)

Select **Add Public Key**, provide a **Key Description**, **paste the Key**, **Enable** the key and Save (Figure 11-9). The public key will be uploaded to sendQuick and you can access using SSH '**sqguest**' account from a laptop/PC with the relevant private key installed.

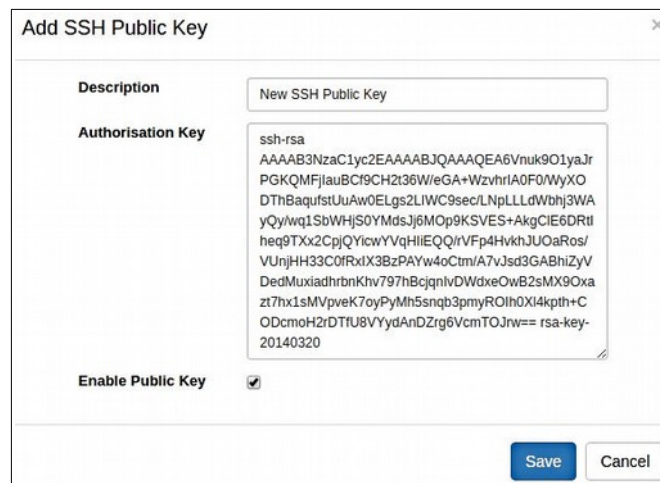


The screenshot shows a web interface for managing SSH public keys. At the top, there is a 'Show' dropdown set to '10' and a 'Search' input field. Below this is a table with three columns: 'No', 'Description', and an action column with a delete icon. The table contains two entries: '1' with description 'SSH Test' and '2' with description 'jrttest'. Below the table is a blue 'Add Public Key' button and a 'Delete' button. At the bottom, it says 'Showing 1 to 2 of total 2 records' and has 'Previous', '1', and 'Next' navigation links.

No	Description	
1	SSH Test	
2	jrttest	

Showing 1 to 2 of total 2 records

Figure 11-8: SSH Remote Access



The screenshot shows a dialog box titled 'Add SSH Public Key'. It has two main sections: 'Description' and 'Authorisation Key'. The 'Description' field contains the text 'New SSH Public Key'. The 'Authorisation Key' field contains a long string of characters, starting with 'ssh-rsa' and ending with 'rsa-key-20140320'. Below these fields is a checkbox labeled 'Enable Public Key' which is checked. At the bottom right are 'Save' and 'Cancel' buttons.

Figure 11-9: Add SSH Public Key

11.9 How to enable SSL Service

sendQuick support SSL / HTTPS be default. In case you will need to reconfigure a SSL certificate on sendQuick. The setup page can be found on menu > Security Setup > SSL Setup (Figure 11-10). Please enable/update the SSL service under HTTP service, this is a precaution step because if setup is not successfully, you can still able to access sendQuick via HTTP.

Figure 11-10: SSL Setup

3 files are required to complete the SSL setup:

- i) SSL Key (a private key generated by your customer while initiating CSR to purchase SSL)
- ii) SSL Cert (given by SSL issuer)
- iii) CA Cert (given by SSL issuer)

You can open the SSL Key and SSL Cert with Text Editor, simply copy and paste the SSL info accordingly.

☒ Enable SSL service.

Please make sure the following data is valid. Else SSL service will fail to start

SSL Key

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,57EAC18A8F8B7C54

kWqyJcmY0eTcUiuX3o0Z7r5mjukbE1SQpFU21pprUBR0gAmaxXUwtkVweERmsEVO
SeUEX+8tWy3U4F8aO0ghvLhdiedO9X9agaNUtuw+Snrlpi5R0Qsz9HGK9Oo80yv
UQm+Uj8ELEGOQ0+sEoFw54nBmWOpSqVtDo8RNs7BaxJ1/FX9iQbsJQizliFCxQ7
H0clN4Mx05LcBmW033PDjeldcGPWyihqErbpeDwqghl6dDk8Gj0wK6+Kwwn4m03
5b7eBoKLdIU6o7kLfeGvVtSHvTB6IsnuctgLUplCQ9VqMRyDrLz87HoL1gdS74
NF5is9x7bAErmlewfqyyJRPxS1znyroo/jqB9v1nY1UkrKwk4WX6oQRa6GMBhb
TJN66dJ6XxdU3ga5ch5WsX0sGED18V3LifoiEU4Nwr5JpRGwXqJOZ+485w0t6jv
Q26hjOYgMRKlqWNR7iQsv6RfzIkN5PAG8Lfz0KSzYiYNiQpCTOeiViHDz/PjE+E
t0WRVrnyNKEgHzGpvY4Lb1b5BJw3HPrJbFSUUBXj6yulM97I80cLul7Xd8pPesg
Cg4JkSUNvBFSKaLgAkSuK9sh95qrHozuikNZTTZMOZ4Riu87cnzHmzusVhuWTRB9
7gKEEIRQHBA3Pb8yNKLqjpJk86bu80KigWL8r7eBzkTVxHu/KZAJ3SDiwPxxvRzo
MaYPwXA69xFmyKtwm6iktLljBfM0sejBvVaRyDMeei5+4nRG+w5rDldfJ4JmRoM
-----
```

Copy and Paste SSL Key in here

SSL Certificate

SSL CA ☒ Use CA File No file selected.

SSL Cipher Strength 128 & 256 bit

SSL Protocol TLSv1.2 (Recommended)

SSL Password *

Verify Password *

Enter the SSL Password here

Figure 11-11: SSL Setup – SSL Key

First, select the **Enable SSL** check box. Then, you will need to provide the SSL Key and SSL Certificate, and 'copy and paste' into the space provided. sendQuick accepts keys that are Apache compatible. If there is a CA file provided, select the check box **Use CA File** and upload the CA file.

Select the SSL Cipher Strength, Protocol and provide a SSL Password and Confirm the Password. Select **Save** once it is done.

Copy and Paste SSL Cert
in here

SSL service setup successfully ✓

0 1

11.9.1 How to Generate SSL Key and Certificate

Note: For proper SSL certification, please purchase the required SSL Certificate from Certificate Authorities only.

Herein is a demonstration on how to generate SSL key and Cert using
- [xampp-windows-x64-7.1.33-0-VC14-installer.exe](#).

i) Access to Xampp Control Panel v3.2.4:

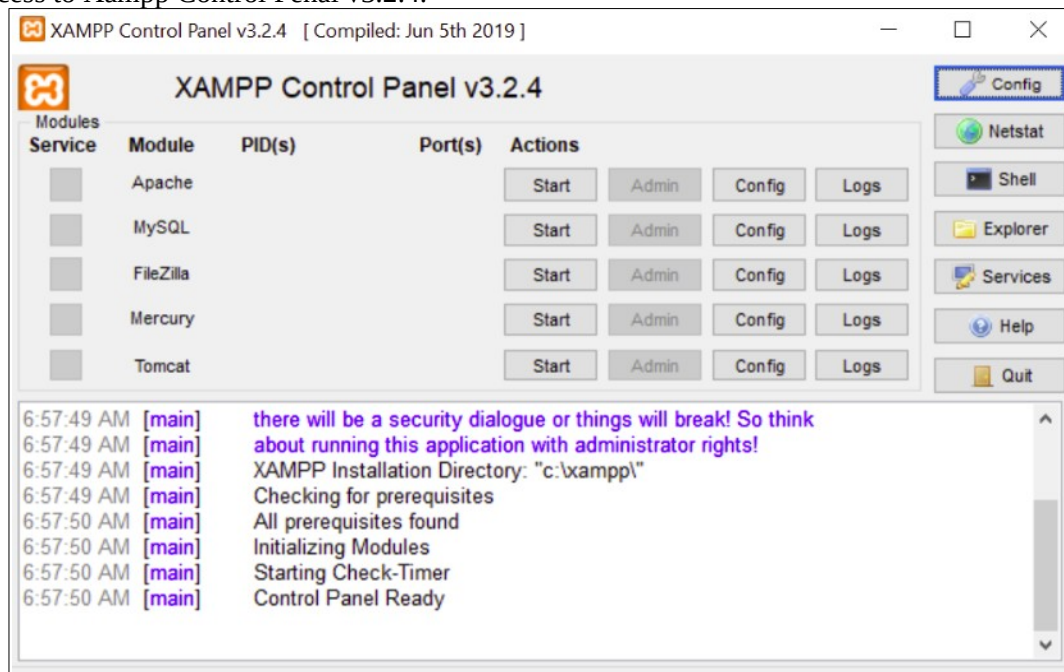


Figure 11-14: XAMPP Control Panel

ii) Access to **Shell** (select from the Figure 11-14's Shell button):

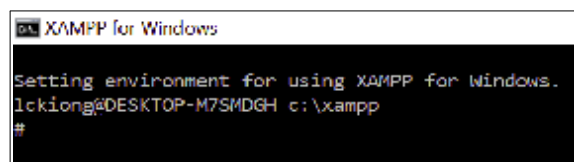


Figure 11-15: XAMPP Shell command prompt

iii) System prompted : lckiong@DESKTOP-M7SMDGH c:\\xampp, basically the login name@computer name, can ignore.

Use the following commands accordingly when prompted:	
Prompt	Command / Sample Data
# cd apache\bin	Change working folder to c:\apache\bin
# openssl	Command to active openssl
OpenSSL> genrsa -des3 -out myssl.key 4096	To generate 'myssl.key' with 4096 bits, replace your filename for the key accordingly.
Enter pass phrase for myssl.key:	Password for the SSL key, eg: 'password', replace your password accordingly and remember this password.
Verifying - Enter pass phrase for myssl.key:	Reconfirm the entered password
# openssl req -new -x509 -days 365 -key myssl.key -out myssl.crt	To generate 'myssl.crt' cert with 365 days validity using 'myssl.key'. Replace your filename for the key and cert accordingly.
Enter pass phrase for myssl.key:	Enter the password of the 'myssl.key' (eg: password)
<p><i>You are about to be asked to enter information that will be incorporated into your certificate request.</i></p> <p><i>What you are about to enter is what is called a Distinguished Name or a DN.</i></p> <p><i>There are quite a few fields but you can leave some blank</i></p> <p><i>For some fields there will be a default value,</i></p> <p><i>If you enter '.', the field will be left blank. -----</i></p>	
Country Name (2 letter code) [AU]:	SG
State or Province Name (full name) [Some-State]:	Singapore
Locality Name (eg, city) []:	Singapore
Organization Name (eg, company) [Internet Widgits Pty Ltd]:	Talariax Pte Ltd
Organizational Unit Name (eg, section) []:	Support Dept
Common Name (e.g. server FQDN or YOUR name) []:	sendQuick
Email Address []:	support@talariax.com

```
XAMPP for Windows

Setting environment for using XAMPP for Windows.
lckiong@DESKTOP-M7SMDGH c:\xampp
# cd apache\bin

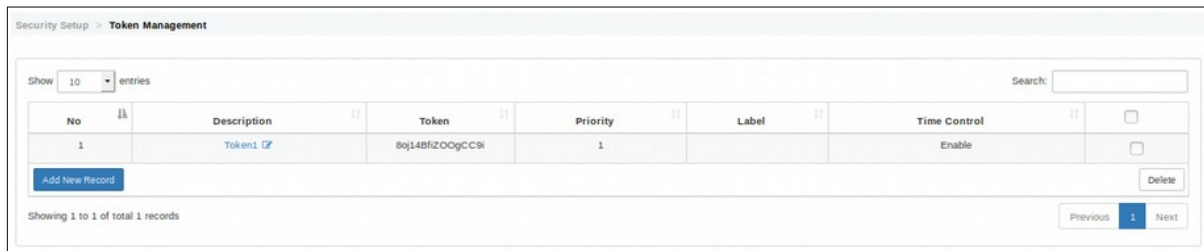
lckiong@DESKTOP-M7SMDGH c:\xampp\apache\bin
# openssl
OpenSSL> genrsa -des3 -out myssl.key 4096
Generating RSA private key, 4096 bit long modulus
.....+++++
.....
unable to write 'random state'
e is 65537 (0x10001)
Enter pass phrase for myssl.key:
Verifying - Enter pass phrase for myssl.key:
OpenSSL>
lckiong@DESKTOP-M7SMDGH c:\xampp\apache\bin
# openssl req -new -x509 -days 365 -key myssl.key -out myssl.crt
Enter pass phrase for myssl.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:SG
State or Province Name (full name) [Some-State]:Singapore
Locality Name (eg, city) []:Singapore
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TalariaX Pte Ltd
Organizational Unit Name (eg, section) []:Support Dept
Common Name (e.g. server FQDN or YOUR name) []:sendQuick
Email Address []:support@talariax.com

lckiong@DESKTOP-M7SMDGH c:\xampp\apache\bin
#
```

Figure 11-16: SSL key and cert generator

11.10 Token Management

To define token(s). Select the **Add New Record** on the Token Management screen (Figure 11-17), the Edit Token configuration screen (Figure 11-18) display, enter the data accordingly follow by **Save**.



Security Setup > Token Management

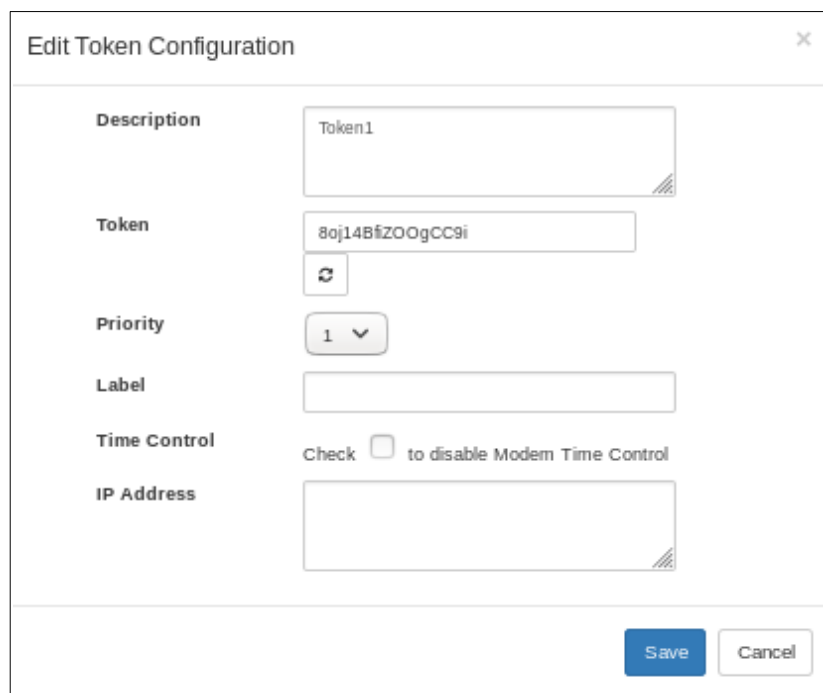
Show 10 entries Search:

No	Description	Token	Priority	Label	Time Control	
1	Token1	8oj14BfZOOGCC9i	1		Enable	<input type="checkbox"/>

[Add New Record](#) [Delete](#)

Showing 1 to 1 of total 1 records [Previous](#) [1](#) [Next](#)

Figure 11-17: Token Management screen



Edit Token Configuration

Description Token1

Token 8oj14BfZOOGCC9i

Priority 1

Label

Time Control Check ☐ to disable Modem Time Control

IP Address

[Save](#) [Cancel](#)

Figure 11-18: Edit Token Configuration screen

12 Password Management

The administrator can change the password for prudent system management. There are eight (8) passwords that can be changed. They are:

<i>User Type</i>	<i>User Name</i>	<i>Description</i>
Server Admin Web login	admin	Password for web administrator login. The default login name and password can be found in the "your password" envelope or contact support@talariax.com.
Supervisor web login	supervisor	Password for Supervisor access. (No default password, please set before use)
Operator Web login	operator	Password for web operator access. (No default password, please set before use)
Console login	admin	Password for console login using direct monitor and keyboard or serial cable (default password: sqroot)
SSH Login Account	sqguest	Password for access via SSH for limited SSH and web shell access. (No default password. Please set before use)
FTP Login Account	smsapp	Account to upload file to sendQuick to send SMS. (No default password, please set before use)
Database Access Account	smsapp	Account for JDBC access. (No default password, please set before use)
User Web Access Login	useradmin	The default login name and password can be found in the "your password" envelope or contact support@talariax.com.

Access Matrix of Web Administrator and Operator

SendQuick support both Administrator and Operator user type for ease of management. The access rights of both user types are as below.

Features	Administrator	Operator
Dashboard	Yes	Yes
Server Setup	Yes	No
Messaging Setup	Yes	No
Modem Setup	Yes	No
Phone Book & Roster	Yes	No
Filter Rules	Yes	No
Network Monitor	Yes	No
Security Setup	Yes	No
Password Management	Yes	No
Backup & Diagnostic	Yes	Yes
Usage Logs	Yes	Yes
System Test Tools	Yes	Yes
SMS Specifications	Yes	Yes

12.1 Server Admin Web Login

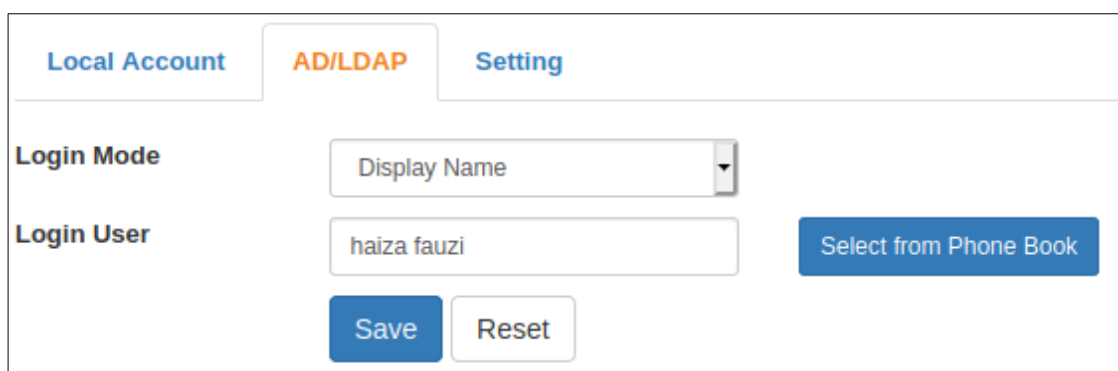
The menu option allowing sendQuick's default Administrator to update his/her login name and password and to assign AD/LDAP user as sendQuick System Administrator:

- I. On **Local Account** (tab), this menu option allowing administrator to the change Username(login name) and Password for the 'admin' login. Password must meet the following requirements:
 - Minimum password length: 8
 - Maximum password length : 16
 - At least one character from this group [A-Z]
 - At least one character from this group [a-z]
 - At lease one character from this group [0-9]

Figure 12-1-1: Server Admin Web Login

- II. On **AD/LDAP** (tab), this menu option allowing administrator to assign administrator from AD/LDAP via Phone Book.

Refer to chapter '8.1.3 Phone Book Records – by AD/LDAP Setup' on how to import AD/LDAP data to Phone Book.

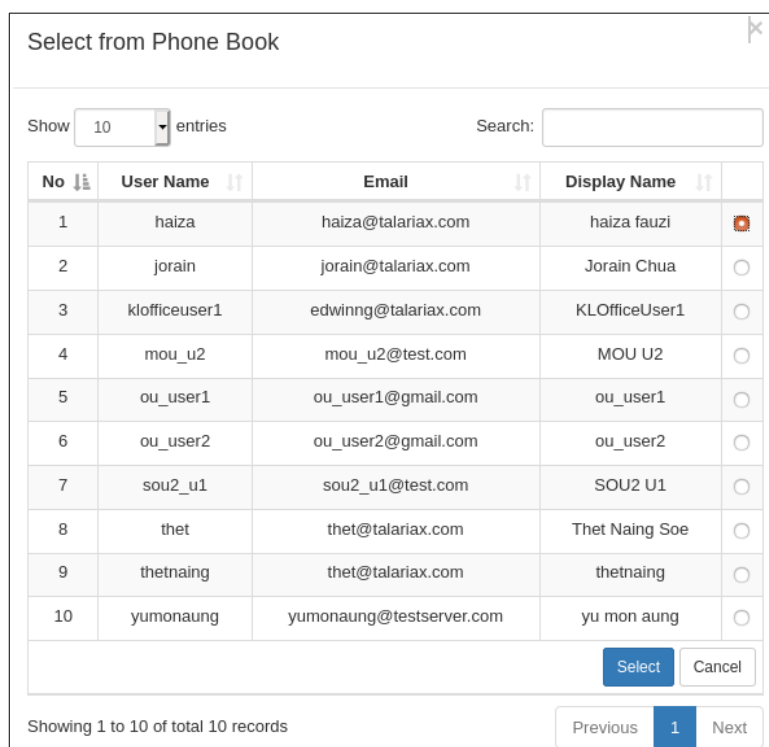


The screenshot shows the 'AD/LDAP' tab in the 'Local Account' section. It features a 'Login Mode' dropdown menu currently set to 'Display Name'. Below it, the 'Login User' field contains the text 'haiza fauzi'. To the right of this field is a blue button labeled 'Select from Phone Book'. At the bottom of the form are two buttons: 'Save' and 'Reset'.

Figure 12-1-2: Server Admin Web Login AD/LDAP Screen

Login Mode: Select the prefer login mode; by, User Name / Email / Display Name.

Login User: click on the 'Select from Phone Book' to access the 'Select From Phone Book' (Figure 12-1-3) list, pick and Select a name from Phone Book:



The 'Select from Phone Book' dialog displays a table of 10 entries. At the top, there is a 'Show' dropdown set to '10' and a 'Search' input field. The table has columns for 'No', 'User Name', 'Email', and 'Display Name'. The first entry, 'haiza', is selected, indicated by a red square icon in the rightmost column. Below the table are 'Select' and 'Cancel' buttons. At the bottom, it shows 'Showing 1 to 10 of total 10 records' and pagination controls with 'Previous', '1' (selected), and 'Next' buttons.

No	User Name	Email	Display Name
1	haiza	haiza@talariax.com	haiza fauzi
2	jorain	jorain@talariax.com	Jorain Chua
3	klofficeuser1	edwinng@talariax.com	KLOfficeUser1
4	mou_u2	mou_u2@test.com	MOU U2
5	ou_user1	ou_user1@gmail.com	ou_user1
6	ou_user2	ou_user2@gmail.com	ou_user2
7	sou2_u1	sou2_u1@test.com	SOU2 U1
8	thet	thet@talariax.com	Thet Naing Soe
9	thetnaing	thet@talariax.com	thetnaing
10	yumonaung	yumonaung@testserver.com	yu mon aung

Figure 12-1-3: Select From Phone Book

Select 'Save' when ready from Figure 12-1-2, the selected user will be able to login to sendQuick system as 'administrator'.

III. Access to '**Setting**' (tab), this sub-menu option allowing sendQuick admin to configure how often the local data will be synchronized with AD/LDAP Server.

Local Account	AD/LDAP	Setting
Authentication		
		Local and Active Directory
Session timeout	30	minute(s)
Lockout threshold	0	invalid attempt(s) <small>To disable lockout, set to '0'</small>
Password expiry	0	day(s) <small>To disable password expiry, set to '0'</small>
Password expiry reminder	0	day(s) prior to expiration
Change password at next logon	<input type="checkbox"/>	
<div>Save Reset</div>		

Figure 12-1-4: Server Admin Web Setting screen

Authentication: Local and Active Directory / Local only / Active Directory only.

Session timeout: default as '30 minutes'.

Lockout threshold: Number of invalid attempt(s), to disable lockout, set to '0'.

Password expiry: Password will be expired in day(s), to disable password expiry, set to '0'

Password expiry reminder: day(s) prior to expiration.

Change password at next logon: checked to enable.

Select 'Save' when ready.

12.2 Supervisor Web Login

The menu option serving 3 functions:

- I. On **Local Account** (tab) menu option allowing administrator to the change username and password for the 'supervisor' login. Password must meet the following requirements:
 - Minimum password length: 8
 - Maximum password length : 16
 - At least one character from this group [A-Z]
 - At least one character from this group [a-z]
 - At lease one character from this group [0-9]

The screenshot shows a web interface for 'Password Management > Supervisor Web Login'. It features a tabbed interface with 'Local Account' selected. The page is titled 'Change Supervisor Web Login Username and Password'. Under the 'Local Account' tab, there are two sections. The first section is for 'Username', with a text input field containing 'supervisor' and 'Save' and 'Reset' buttons. The second section is for 'New Password' and 'Confirm Password', each with a text input field and 'Save' and 'Reset' buttons. To the right of the password fields, a list of requirements is displayed: 'Password must meet the following requirements: Minimum password length: 8, Maximum password length: 16, At least one character from this group [A-Z], At least one character from this group [a-z], At least one character from this group [0-9]'. The 'Save' buttons are blue, and the 'Reset' buttons are white with blue borders.

Figure 12-2-1: Supervisor Web Login – Local Account

- II. On **AD/LDAP** (tab), this menu option allowing administrator to assign Supervisor from AD/LDAP via Phone Book.

Refer to chapter '8.1.3 Phone Book Records – by AD/LDAP Setup' on how to import AD/LDAP data to Phone Book.

Figure 12-2-2: Supervisor Web Login – AD/LDAP

Login Mode: Select the prefer login mode; by, User Name / Email / Display Name.

Login User: click on the 'Select from Phone Book' to access the 'Select From Phone Book' (Figure 12-2-3) list, pick and Select a name from Phone Book:

No	User Name	Email	Display Name	
1	haiza	haiza@talariax.com	haiza fauzi	<input type="radio"/>
2	jorain	jorain@talariax.com	Jorain Chua	<input checked="" type="radio"/>
3	klofficeuser1	edwinng@talariax.com	KLOfficeUser1	<input type="radio"/>
4	mou_u2	mou_u2@test.com	MOU U2	<input type="radio"/>
5	ou_user1	ou_user1@gmail.com	ou_user1	<input type="radio"/>
6	ou_user2	ou_user2@gmail.com	ou_user2	<input type="radio"/>
7	sou2_u1	sou2_u1@test.com	SOU2 U1	<input type="radio"/>
8	thet	thet@talariax.com	Thet Naing Soe	<input type="radio"/>
9	thetnaing	thet@talariax.com	thetnaing	<input type="radio"/>
10	yumonaung	yumonaung@testserver.com	yu mon aung	<input type="radio"/>

Figure 12-2-3: Supervisor Web Login – Phone Book

Select 'Save' when ready from Figure 12-2-2, the selected user will be able to login to sendQuick system as 'supervisor'.

III) Access to '**Setting** (tab), this sub-menu option allowing sendQuick admin to configure how often the local data will be synchronized with AD/LDAP Server.

Local Account	AD/LDAP	Setting
Authentication Local and Active Directory		
Session timeout	30	minute(s)
Lockout threshold	0	invalid attempt(s) <small>To disable lockout, set to '0'</small>
Password expiry	0	day(s) <small>To disable password expiry, set to '0'</small>
Password expiry reminder	0	day(s) prior to expiration
Change password at next logon	<input type="checkbox"/>	
Save Reset		

Figure 12-1-4: Server Admin Web Setting screen

Authentication: Local and Active Directory / Local only / Active Directory only.

Session timeout: default as '30 minutes'.

Lockout threshold: Number of invalid attempt(s), to disable lockout, set to '0'.

Password expiry: Password will be expired in day(s), to disable password expiry, set to '0'

Password expiry reminder: day(s) prior to expiration.

Change password at next logon: checked to enable.

Select 'Save' when ready.

12.3 Operator Web Login

The menu option serving 3 functions:

- I. On **Local Account**(tab), this menu option allowing administrator to the change username and password for the ‘operator’ login. Password must meet the following requirements:
 - Minimum password length: 8
 - Maximum password length : 16
 - At least one character from this group [A-Z]
 - At least one character from this group [a-z]
 - At lease one character from this group [0-9]

The screenshot shows a web interface for 'Password Management > Operator Web Login'. The main heading is 'Change Server Operator Web Login Username and Password'. There are three tabs: 'Local Account' (selected), 'AD/LDAP', and 'Setting'. The 'Local Account' section contains a 'Username' field with the value 'operator' and 'Save' and 'Reset' buttons. Below this are 'New Password' and 'Confirm Password' fields, each with a red asterisk, and 'Save' and 'Reset' buttons. To the right of the password fields, a list of requirements is displayed: 'Password must meet the following requirements: • Minimum password length: 8 • Maximum password length: 16 • At least one character from this group [A-Z] • At least one character from this group [a-z] • At least one character from this group [0-9]'. The interface is clean with a light blue header and a white main area.

Figure 12-3-1: Operator Web Login – Local Account

- II. On **AD/LDAP** (tab), this menu option allowing administrator to assign Operator from AD/LDAP via Phone Book.

Refer to chapter '8.1.3 Phone Book Records – by AD/LDAP Setup' on how to import AD/LDAP data to Phone Book.

Figure 12-3-2: Operator Web Login – AD/LDAP

Login Mode: Select the prefer login mode; by, User Name / Email / Display Name.

Login User: click on the 'Select from Phone Book' to access the 'Select From Phone Book' (Figure 12-3-3) list, pick and Select a name from Phone Book:

No	User Name	Email	Display Name	
1	haiza	haiza@talariax.com	haiza fauzi	<input type="radio"/>
2	jorain	jorain@talariax.com	Jorain Chua	<input type="radio"/>
3	klofficeuser1	edwinng@talariax.com	KLOfficeUser1	<input type="radio"/>
4	mou_u2	mou_u2@test.com	MOU U2	<input type="radio"/>
5	ou_user1	ou_user1@gmail.com	ou_user1	<input type="radio"/>
6	ou_user2	ou_user2@gmail.com	ou_user2	<input type="radio"/>
7	sou2_u1	sou2_u1@test.com	SOU2 U1	<input type="radio"/>
8	thet	thet@talariax.com	Thet Naing Soe	<input checked="" type="radio"/>
9	thetnaing	thet@talariax.com	thetnaing	<input type="radio"/>
10	yumonaung	yumonaung@testserver.com	yu mon aung	<input type="radio"/>

Figure 12-3-3: Operator Web Login – Phone Book

Select 'Save' when ready from Figure 12-3-2, the selected user will be able to login to sendQuick system as 'operator'.

III) Access to '**Setting** (tab), this sub-menu option allowing sendQuick admin to configure how often the local data will be synchronized with AD/LDAP Server.

Local Account	AD/LDAP	Setting
Authentication		
		Local and Active Directory
Session timeout	30	minute(s)
Lockout threshold	0	invalid attempt(s) <small>To disable lockout, set to '0'</small>
Password expiry	0	day(s) <small>To disable password expiry, set to '0'</small>
Password expiry reminder	0	day(s) prior to expiration
Change password at next logon	<input type="checkbox"/>	
<div>Save Reset</div>		

Figure 12-1-4: Server Admin Web Setting screen

Authentication: Local and Active Directory / Local only / Active Directory only.

Session timeout: default as '30 minutes'.

Lockout threshold: Number of invalid attempt(s), to disable lockout, set to '0'.

Password expiry: Password will be expired in day(s), to disable password expiry, set to '0'

Password expiry reminder: day(s) prior to expiration.

Change password at next logon: checked to enable.

Select 'Save' when ready.

12.4 Console Login

The menu option allowing administrator to change password for the 'admin' login for console access, new password must meet the following requirements:

- Minimum password length: 8
- Maximum password length : 16
- At least one character from this group [A-Z]
- At least one character from this group [a-z]
- At lease one character from this group [0-9]

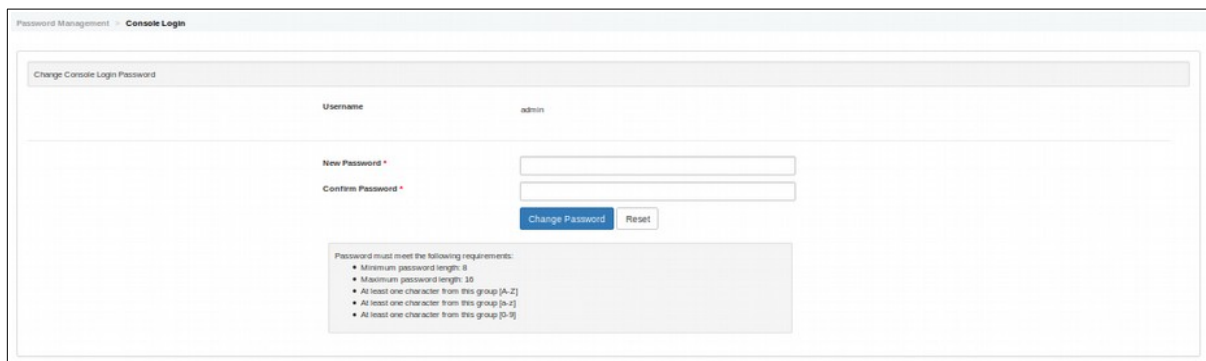
The screenshot shows a web interface titled "Console Login" under a "Password Management" header. The main heading is "Change Console Login Password". Below this, the "Username" field is pre-filled with "admin". There are two input fields for "New Password" and "Confirm Password", both marked with a red asterisk. Below the input fields are two buttons: "Change Password" (in blue) and "Reset" (in grey). A box at the bottom lists the password requirements: Minimum password length: 8, Maximum password length: 16, At least one character from this group [A-Z], At least one character from this group [a-z], and At least one character from this group [0-9].

Figure 12-4: Console Login

12.5 SSH Login Account

The menu option allowing administrator to change password for the 'sqguest' access for SSH access, new password must meet the following requirements:

- Minimum password length: 8
- Maximum password length : 16
- At least one character from this group [A-Z]
- At least one character from this group [a-z]
- At lease one character from this group [0-9]

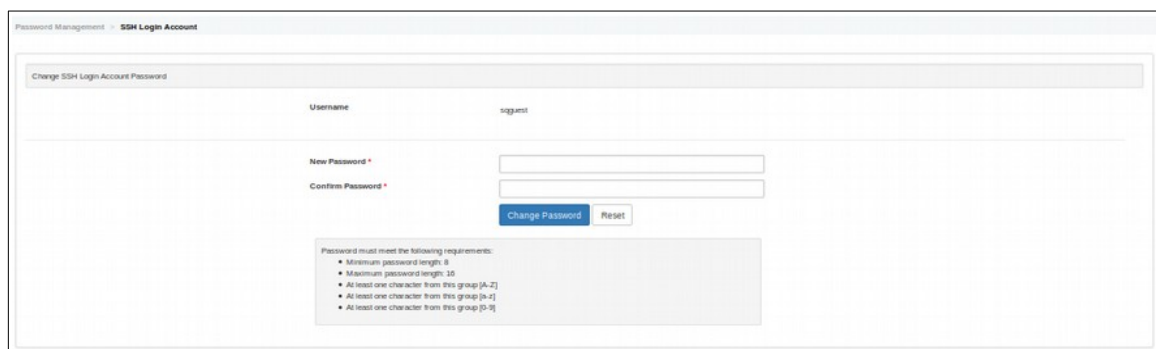
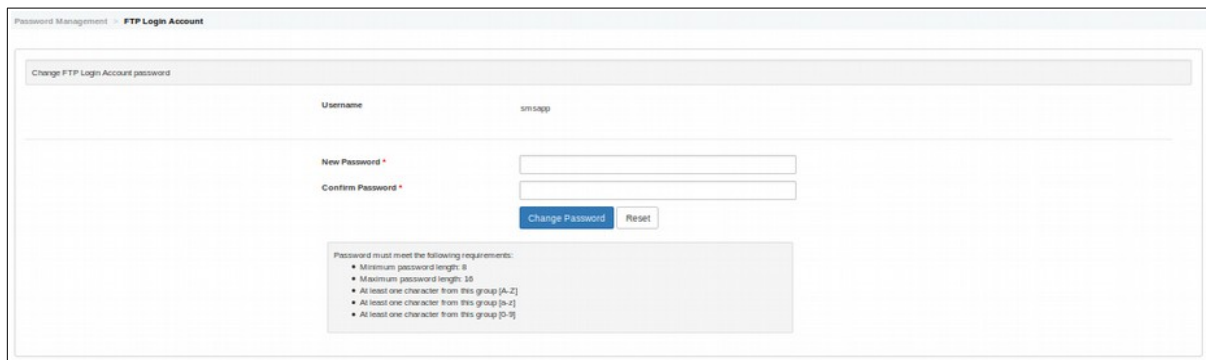
The screenshot shows a web interface titled "SSH Login Account" under a "Password Management" header. The main heading is "Change SSH Login Account Password". Below this, the "Username" field is pre-filled with "sqguest". There are two input fields for "New Password" and "Confirm Password", both marked with a red asterisk. Below the input fields are two buttons: "Change Password" (in blue) and "Reset" (in grey). A box at the bottom lists the password requirements: Minimum password length: 8, Maximum password length: 16, At least one character from this group [A-Z], At least one character from this group [a-z], and At least one character from this group [0-9].

Figure 12-5: SSH Login Account

12.6 FTP Login Account

The menu option allowing administrator to change password for the 'smsapp' access for FTP access, new password must meet the following requirements:

- Minimum password length: 8
- Maximum password length : 16
- At least one character from this group [A-Z]
- At least one character from this group [a-z]
- At lease one character from this group [0-9]



The screenshot shows a web interface for changing the FTP Login Account password. The page title is "Password Management - FTP Login Account". The main heading is "Change FTP Login Account password". Below this, there is a form with the following fields and elements:

- Username:** A text field containing the value "smsapp".
- New Password:** A text field with a red asterisk indicating it is required.
- Confirm Password:** A text field with a red asterisk indicating it is required.
- Buttons:** Two buttons, "Change Password" (in blue) and "Reset" (in grey), are located below the password fields.
- Requirements:** A box below the buttons lists the password requirements:
 - Password must meet the following requirements:
 - Minimum password length: 8
 - Maximum password length: 16
 - At least one character from this group [A-Z]
 - At least one character from this group [a-z]
 - At least one character from this group [0-9]

Figure 12-6: FTP Login Account

12.7 Database Access Account

The menu option allowing administrator to change password for the 'smsapp' access for database access, new password must meet the following requirements:

- Minimum password length: 8
- Maximum password length : 16
- At least one character from this group [A-Z]
- At least one character from this group [a-z]
- At lease one character from this group [0-9]

Figure 12-7: Database Access Account

12.8 User Web Access Login

The menu option allowing administrator to reset password to manufacturer setting for the 'useradmin', select the **Reset** button to proceed.

Figure 12-8: User Web Access Login

13 Backup & Diagnostic

This section explains how to perform backup, restore, update and diagnostic process in sendQuick servers. To start, select **Backup & Diagnostic** in the navigation menu and you will see the options below.

13.1 Generate Backup File

You can back-up the system configuration and alert rules in sendQuick server. Save the backup file once it is generated (Figure 13-1).

Note: *When the backup process is in progress, do not close the browser as it may affect the process and impacts sendQuick subsequently. Just wait patiently until the process completes and you will be prompted to save the file.*

You will notice that sendQuick backup files are named in accordance to the 'bakfiletype_date' with an extension '**.enc**'. This is a proprietary format for sendQuick and can be used for sendQuick server only. Please use the same file when you restore the configuration or alert rules respective.

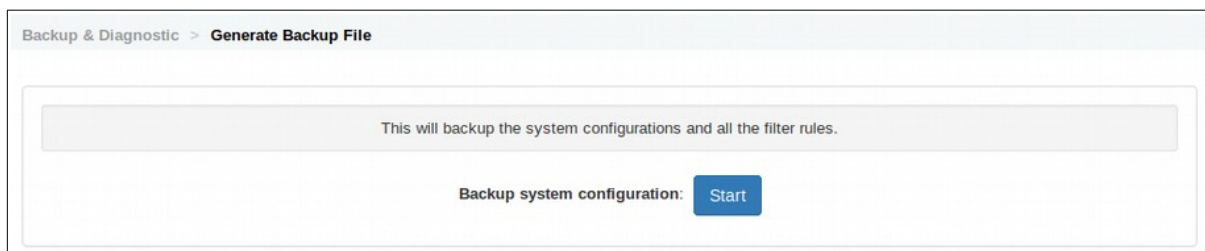


Figure 13-1: Generate Backup File

13.2 Automated Backup

This allows the sendQuick server to be backed-up automatically to the designated FTP directory/server at a selected period (daily, weekly, monthly) and at a certain specified time.

This set the schedule backup of the system configuration:

- Disable : This will disable the auto backup.
- Daily : The backup will be generated daily.
- Weekly : The backup will be generated on every Monday.
- Monthly : The backup will be generated every 1st day of the month.

Backup & Diagnostic > Automated Backup

Schedule Backup

Schedule Time

FTP Server

FTP Username

FTP Password

Confirm Password

FTP Directory

This set the schedule backup of the system configuration:

- Disable: This will disable the auto backup.
- Daily: The backup will be generated daily.
- Weekly: The backup will be generated every Monday.
- Monthly: The backup will be generated every 1st day of the month.

Figure 13-2: Automated Backup

13.3 Restore Backup File

The process to restore the backup and configuration, please note that the backup file can only be applied to the same version creation number.

Backup & Diagnostic > Restore Backup File

This will restore the backup system configurations and restore the filter rules.

Please specify backup No file selected.

Figure 13-3: Restore Backup File

13.4 Generate Diagnostic File

A diagnostic file is a sendQuick system image file that will capture all the essential system information, logs and other relevant information in sendQuick. This file is very useful for sendQuick technical team to review when it is required to troubleshoot any problems in sendQuick (Figure 13-4).

The creation process may take a few minutes (depending on the file size), so do be patient. Similarly, **DO NOT CLOSE THE BROWSER** when the creation process is in progress (for a few minutes and may be as long as 10 minutes). Once completed, the browser will refresh and a Download link will appear. Save the file and send it to sendQuick technical for review. The file is an encrypted file with '.enc' extension.

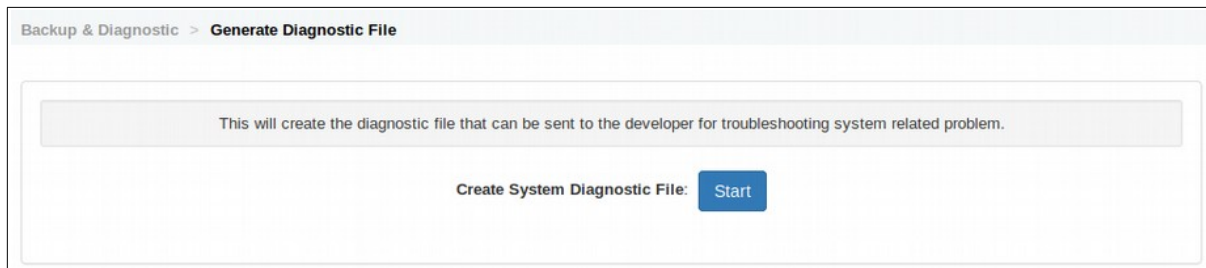


Figure 13-4: Generate Diagnostic File

13.5 Apply Patch

TalariaX will release new patches for sendQuick, which can be applied to update the sendQuick servers. Similarly, if the technical team discovered some problems, the issues can be resolved by applying patch to the system (Figure 13-5).

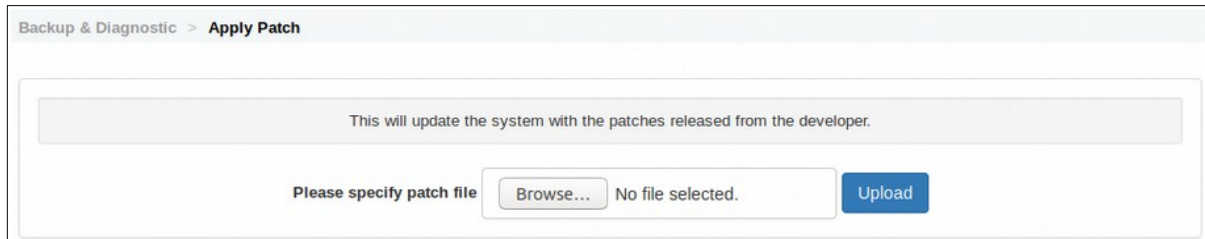


Figure 13-5: Apply Patch

Please note that the patch file is a file with extension '**.enc**' and is provided by TalariaX for generic patch, access to sendQuick's Dashboard / System Overview / System version (Version Creation number) and patch number (Patch Version number) to understand the system version that installed on your sendQuick device.

Prior to any system patching, its to have a good habit that always to perform a system backup and to kept the backup file in a safe folder/system, you can always perform system backup from menu option Backup & Diagnostic > Generate Backup File.

Do not close the browser while the updating is in progress. The browser may experience connection issue during applying the patch file to the appliance, if happen, just wait a few seconds and manually refresh the browser to continue the patching process.

System patching MUST be performed always in this order:

- i. Kernel patch follow by system reboot. (When required)
- ii. Basepackage patch. (When required)
- iii. System patch.

If the system is configured as HA, patching must be performed on Secondary server first follow by Primary server.

Different version creation number is not compatible with each other, despite being the same product model. Each version creation number will have their own patched versions.

14 Usage Logs

The sendQuick server has a comprehensive log system that records every transaction in the server. Select the **Usage Logs** on the navigation bar and you will see the options, as explained below:

14.1 Message Log

This log consist of messages in Queue, Send, Unsent and Inbox messages for SMS, MIM and Sqoope. These logs are for SMS messages that were sent and received by sendQuick. All the messages will be recorded with their respective date & time, sender, mobile number, message content, modem IMEI and priority. A sample of the SMS Sent log is shown in Figure 14-1.

All message logs can be searched (by date range and keyword) for easy reference. You can also save and archive the logs manually. At the bottom left of the log is a **Save** button which will save the messages selected for the specified period.

Usage Logs > Message Log

Queue Sent Unsent Inbox

SMS MIM Sqoope

Search From 17/07/2019 To 17/07/2019

Show 100 entries Search:

No	Date & Time	Delivery Date	Turnaround Time	Sender	Mobile Number	Message	IMEI	Priority	
1	17/07/2019 10:29:49	17/07/2019 10:29:51	00:09	192.168.1.95 (admin)	94506718	hello	357364080178469	1	<input type="checkbox"/>

Save CSV Save Excel Save PDF Refresh Empty Outbox Delete

Showing 1 to 1 of total 1 records Previous 1 Next

Figure 14-1: Message Log

To delete a record(s), **select/un-select** the desired records and click **Delete**.

14.2 Conversation Summary

This log is for SMS messages that were sent and received by sendQuick. All the messages will be recorded with their respective date & time, mobile number, message content, A sample of the SMS conversation summary is shown in Figure 14-2.

To filter the conversation, enter the Mobile number to retrieve the data accordingly.

The screenshot displays a web interface titled 'Usage Logs > Conversation Summary'. It features a search section with three input fields: 'Search From' (containing '17/07/2019'), 'To' (containing '17/07/2019'), and 'Mobile Number' (empty). Below the search fields, there is a list of conversation entries. The first entry is for mobile number '94506718'. It shows a message from '94506718' at '17/07/2019 10:29:49' with the content 'hello'. The second entry is for mobile number '6594506718', showing a message at '17/07/2019 10:40:06' with the content 'How are you'. A third entry for '96946237' is partially visible at the bottom.

Figure 14-2: Conversation Summary

14.3 Email Log

This log is for Email messages that were sent by sendQuick server on SMTP (email) activities. All the messages will be recorded with their respective date & time, Sender and Recipient, message content, A sample of the Email Log is shown in Figure 14-3.

To filter the data, enter the content search on the 'Search' field.

The screenshot displays the 'Email Log' interface within a 'Usage Logs' section. It features three tabs: 'Email Queue' (selected), 'Email Sent', and 'Email Unsent'. Below the tabs, there are search filters for 'Search From' (10/07/2019) and 'To' (17/07/2019), a 'Show 100 entries' dropdown, and a 'Search:' input field. The main area contains a table with the following data:

No	Date & Time	Email Sender	Email Recipient	Remark	
1	17/07/2019 11:21:57	abc@abc.com (127.0.0.1)	cheekiong@talariax.com	SMTP connection drop ; cheekiong@talariax.com ; Target: 117.120.2.23 ; 451 ; 182.23.145.18 is not yet authorized to deliver mail from <abc@abc.com> to <cheekiong@talariax.com>. Please try later. ; Size:317 bytes ; Retrying...	<input type="checkbox"/>

Below the table, there is a 'Refresh' button, an 'Empty Queue' button, and a 'Delete' button. At the bottom, it shows 'Showing 1 to 1 of total 1 records' and a pagination control with 'Previous', '1' (selected), and 'Next' buttons.

Figure 14-3: Email Log

14.4 Alert Log

This log is for Alert messages that received by sendQuick server. All the messages will be recorded with their respective date & time, From, To, subject and message content, A sample of the Alert Log is shown in Figure 14-5.

To filter the data, enter the content search on the 'Search' field.

Usage Logs > Alert Log

Received Discarded

Search From 06/09/2019 To 06/09/2019

Show 10 entries Search:

No	Date & Time	From	To	Subject	Message	Reason	
1	06/09/2019 17:35:36	prtg@talariax.com	93873088@192.168.1.95	This is a test email from PRTG	Please use a HTML capable email client for reading this email. For notifications you can alternatively switch to 'Text' format in the notification settings	Sender not allowed	<input type="checkbox"/>
2	06/09/2019 17:35:15	prtg@talariax.com	93873088@192.168.1.95	[PRTG Network Monitor (ACERV13)] 192.168.1.49 SSL Security Check (Port 443) (SSL Security Check) Dow...	Sensor: SSL Security Check (Port 443) (SSL Security Check) *** http://acerV13.talariax.com/sensor.htm?id=2087 New Status...	Sender not allowed	<input type="checkbox"/>
3	06/09/2019 17:35:14	prtg@talariax.com	93873088@192.168.1.95	[PRTG Network Monitor (ACERV13)] 7 Summarized Notifications	7 Summarized Notifications 1. [PRTG Network Monitor (ACERV13)] 192.168.1.64 FTP (FTP) Down (before: Unknown) (Failed to establish secure connection [Step 0] Socket Error # 10060 Connection timed out...	Sender not allowed	<input type="checkbox"/>
4	06/09/2019 17:34:01	prtg@talariax.com	93873088@192.168.1.95	[PRTG Network Monitor (ACERV13)] 11 Summarized Notifications	11 Summarized Notifications 1. [PRTG Network Monitor (ACERV13)] 192.168.1.69 FTP (FTP) Down (before: Unknown) (Failed to establish secure connection [Step 0] Socket Error # 10060 Connection timed ou...	Sender not allowed	<input type="checkbox"/>
5	06/09/2019 17:34:01	prtg@talariax.com	93873088@192.168.1.95	[PRTG Network Monitor (ACERV13)] 192.168.1.69 SSL Certificate Sensor (Port 443) (SSL	Sensor: SSL Certificate Sensor (Port 443) (SSL Certificate) *** http://acerV13.talariax.com/sensor.htm?id=2205 New Statu...	Sender not allowed	<input type="checkbox"/>

Figure 14-5: Alert Log

14.5 System Log

This log display the sendQuick server activities for SMS and Email in real-time, select the SMS or Email tab on the screen accordingly., a sample System Log is shown in Figure 14-6.

You can download and save the log data by selecting the ‘**Download**’ button.

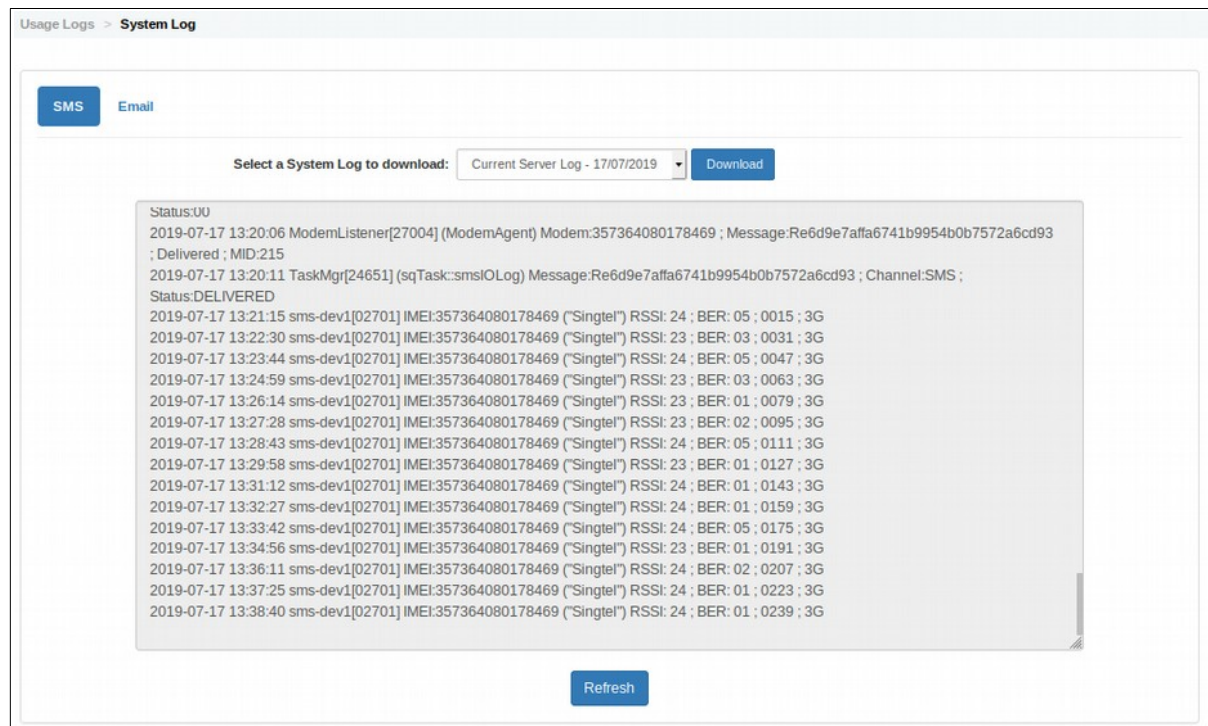


Figure 14-6: System Log

14.6 Audit Log

This log capture and display the user activities on sendQuick server real-time, A sample Audit Log is shown in Figure 14-7.

To filter the data, enter the content search on the 'Search' field or by selecting the data range or show the number of entries.

Usage Logs > **Audit Log**

Search From: 17/07/2019 To: 17/07/2019

Show: 100 entries

Search:

No	Date & Time	Username	IP	Action
1	17/07/2019 13:32:38	admin	192.168.1.1	Login - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:68.0) Gecko/20100101 Firefox/68.0
2	17/07/2019 13:18:42	admin	192.168.1.1	DELETE - Ping Check
3	17/07/2019 13:18:22	admin	192.168.1.1	Login - Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
4	17/07/2019 12:04:16	admin	192.168.1.1	Session expired
5	17/07/2019 11:33:18	admin	192.168.1.1	ENABLE - Ping Check
6	17/07/2019 11:33:05	admin	192.168.1.1	ADD - Ping Check: 192.168.93.1
7	17/07/2019 11:19:52	admin	192.168.1.1	Login - Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
8	17/07/2019 09:51:34	admin	192.168.1.1	Login - Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
9	17/07/2019 09:43:52	admin	192.168.1.1	RESET - User Web Access Login Password
10	17/07/2019 09:13:27	admin	192.168.1.1	Login - Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
11	17/07/2019 09:00:44	admin	192.168.1.1	Login - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:68.0) Gecko/20100101 Firefox/68.0

Save CSV Save Excel Refresh

Showing 1 to 11 of total 11 records

Previous 1 Next

Figure 14-7: Audit Log

14.7 Usage Statistic

This screen display the sendQuick server system usage in real-time, A sample Usage Statistic is shown in Figure 14-8.

To filter the data, select the Period, Type, Status and Usage from the respective drop down menu accordingly.

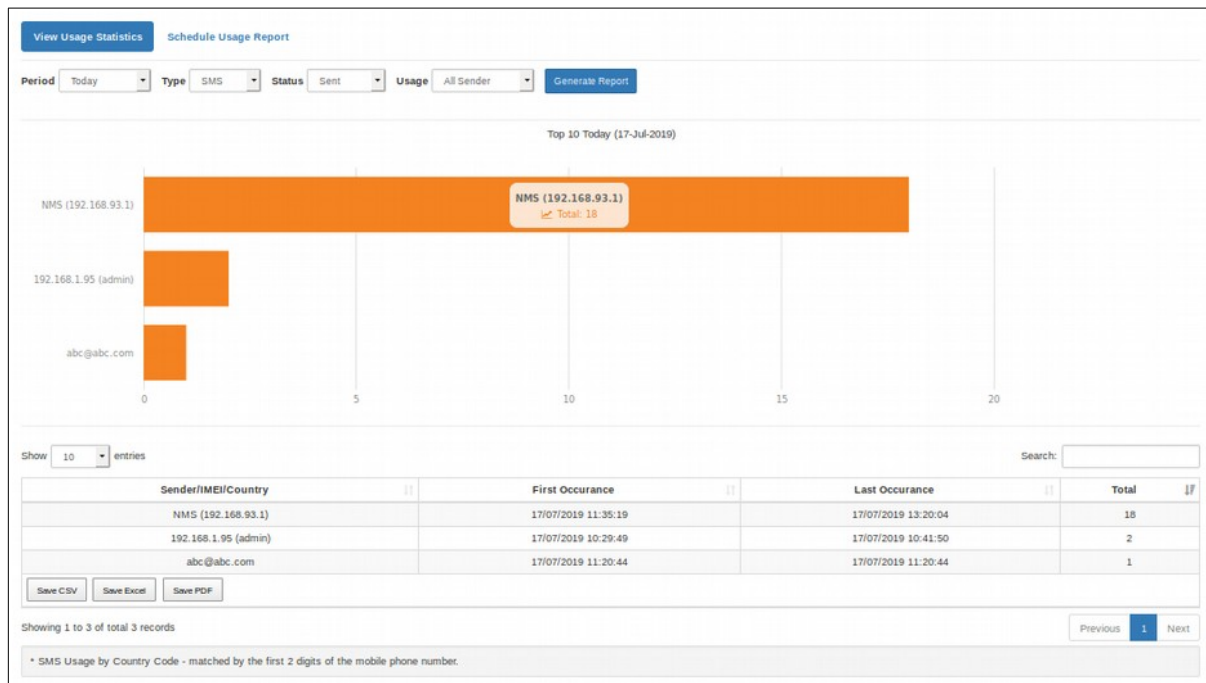


Figure 14-8: Usage Statistic

14.8 Maintenance and Report

- (a) **Log Maintenance** refers to the duration to keep the messages in sendQuick server by the number of days (old) from current date. Example, if the days are set to 180 days, messages older than 180 days will be deleted automatically. This allows the system to perform automatic data deletion and housekeeping.

The screenshot shows the 'Maintenance & Report' section of the 'Usage Logs' page. It features two tabs: 'Log Maintenance' (active) and 'Usage Report'. The 'Log Maintenance' section is divided into three main areas: 'SMS Log Maintenance', 'Email Log Maintenance', and 'Syslog Server'. Each area contains configuration options for message retention duration in days. The 'SMS Log Maintenance' section includes settings for Outbox, Inbox, Unsent, and Discarded messages, all set to 180 days. The 'Email Log Maintenance' section includes settings for Sent and Unsent emails, also set to 180 days. The 'Syslog Server' section has a text input field set to 'NA'. A 'Save' button and a 'Reset' button are located at the bottom right of the configuration area. A help text on the right side explains that the system will keep messages according to the duration set, and that setting it to '0' will keep messages indefinitely.

Section	Configuration Item	Value	Unit
SMS Log Maintenance	Delete Outbox messages after	180	day(s)
	Delete Inbox messages after	180	day(s)
	Delete Unsent messages after	180	day(s)
	Delete Discarded mail after	180	day(s)
Email Log Maintenance	Delete Sent emails after	180	day(s)
	Delete Unsent emails after	180	day(s)
Syslog Server	Syslog Server IP	NA	

Figure 14-9: Log Maintenance

- (b) **Usage Report** tab consists of the following setting:
- **Report Schedule:** Allowing administrator to configure the SMS Usage report with the following parameters:
 - **Disable:** This will disable the usage report.
 - **Daily:** The report will be generated daily.
 - **Weekly:** The report will be generated every Monday.
 - **Monthly:** The report will be generated every 1st day of the month.
 - **Email Usage Report:** This set the Email address that will receive the SMS usageReport.
 - **FTP Usage Report:** For setting the Host-name or Machine IP address when shared folder is located.

Usage Logs > Maintenance & Report

Log Maintenance Usage Report

Report Schedule

Type: Daily

Time: 1100

SMS usage report will contain the report for sent, received and unsent SMS. Available options:

- Disable: This will disable the usage report.
- Daily: The report will be generated daily.
- Weekly: The report will be generated every Monday.
- Monthly: The report will be generated every 1st day of the month.

Email Usage Report

This set the Email address that will receive the SMS usage Report.

FTP Usage Report

☐ Use Secure FTP

Server/Host: NA The FTP server hostname or IP

Port: The Port Number of FTP serverhost

Directory: NA The Directory where files would be uploaded

Username: NA The FTP login account name

Password: The FTP login password for file transfer

Confirm Password: (type again to confirm)

Save Reset

File Sharing Service

☐ Enable

Hostname or IP: Set Hostname or Machine IP address where shared folder is located

Workgroup Name (Domain Name): NA Set Workgroup Name or Domain Name to access shared folder

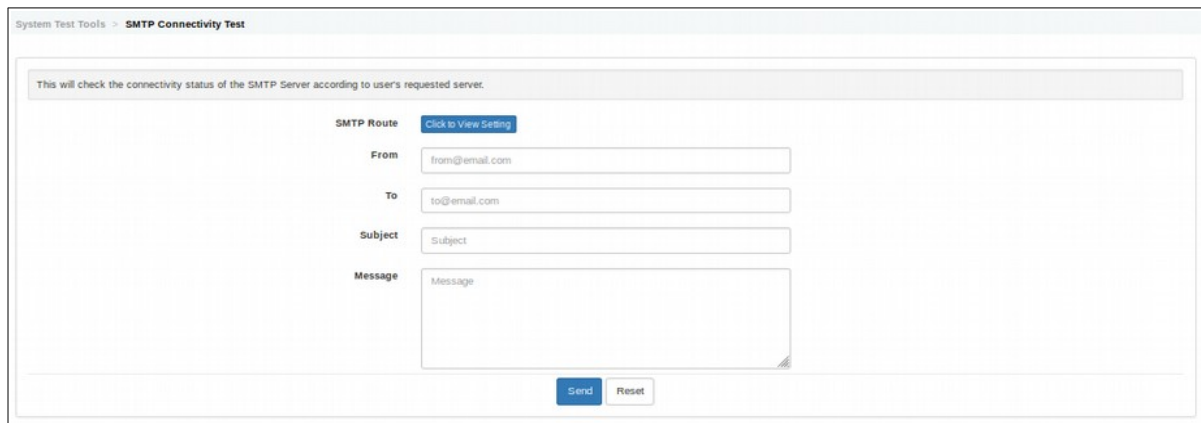
Figure 14-10: Report Schedule

15 System Test Tools

To ensure that the server is functioning properly, sendQuick has built-in tools for you to verify the SMTP or network connectivity, and also to send test messages.

15.1 SMTP Connectivity Test

You may use this tool to test your email server setting. Just fill in the SMTP server IP address, From (sender email), To (receiver email), Subject, Message and click Send (Figure 15-1)

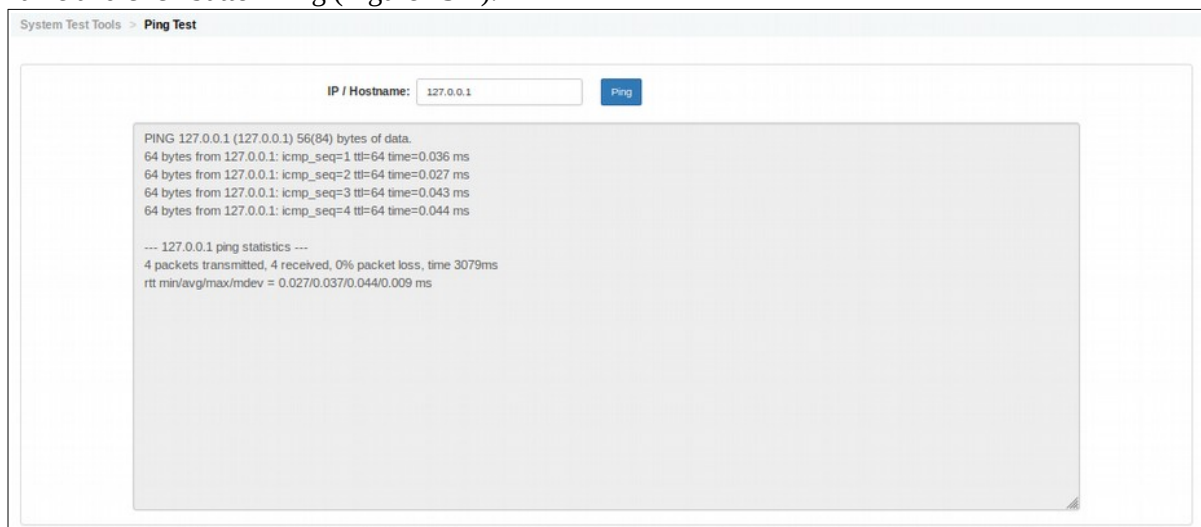


The screenshot shows the 'SMTP Connectivity Test' interface. At the top, it says 'System Test Tools > SMTP Connectivity Test'. Below this, a message states: 'This will check the connectivity status of the SMTP Server according to user's requested server.' The form includes an 'SMTP Route' section with a 'Click to View Setting' button. The main form fields are: 'From' (with placeholder 'from@email.com'), 'To' (with placeholder 'to@email.com'), 'Subject' (with placeholder 'Subject'), and 'Message' (a large text area). At the bottom right, there are 'Send' and 'Reset' buttons.

Figure 15-1: SMTP Connectivity Test

15.2 Ping Test

You may use this tool to perform simple network connectivity test. Just enter the desired IP or domain name and click button Ping (Figure 15-2).



The screenshot shows the 'Ping Test' interface. At the top, it says 'System Test Tools > Ping Test'. The form has an 'IP / Hostname' field with '127.0.0.1' entered and a 'Ping' button. Below the form, the test results are displayed in a text box:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.036 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.027 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.043 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.044 ms  
  
--- 127.0.0.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3079ms  
rtt min/avg/max/mdev = 0.027/0.037/0.044/0.009 ms
```

Figure 15-2: Ping Test

15.3 Traceroute Test

You may use this tool to perform Traceroute testing, Just enter the desired IP or domain name and click button Traceroute (Figure 15-3).

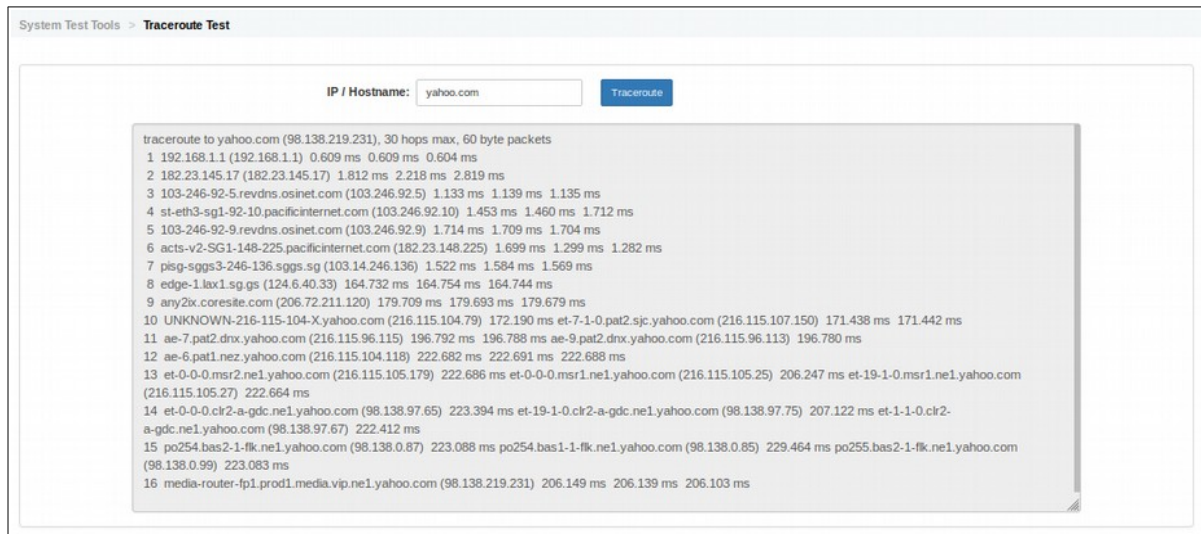


Figure 15-3: Traceroute Test

15.4 Port/Telnet Test

You may use this tool to perform Traceroute testing, Just enter the desired IP or domain name, Port number and click button Telnet (Figure 15-4).

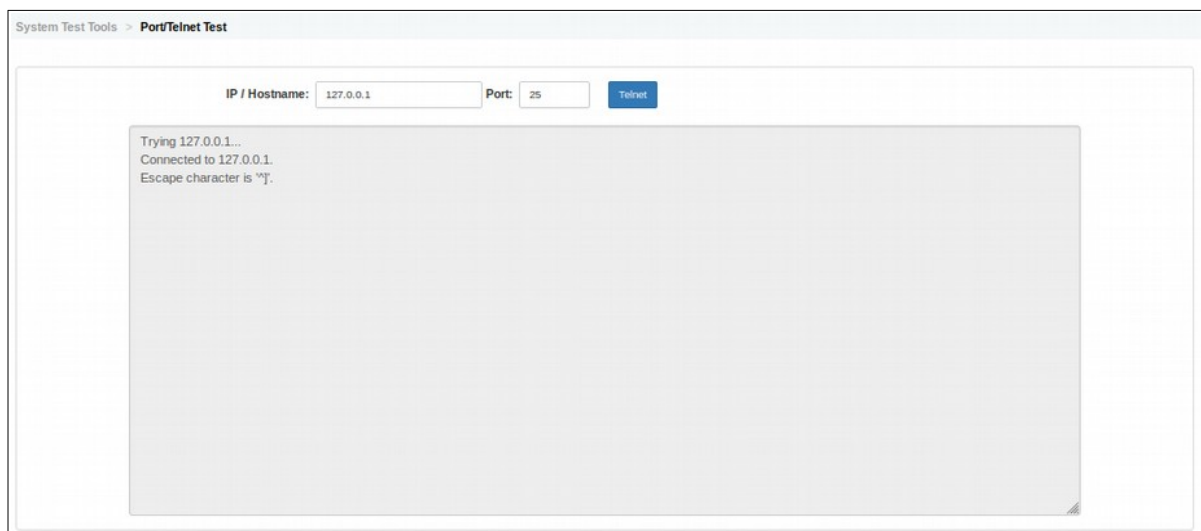


Figure 15-4: Port/Telnet Test

15.5 Send Test SMS

a) Single SMS

Use to send a test sms to your number. Select the language (your message is written in), enter the hand phone number, message and click Submit once done (Figure 15-5).

The screenshot shows a web interface titled "System Test Tools > Send Test SMS". On the left, there is a sidebar with the heading "Single SMS". The main content area contains the following fields:

- Language Used:** A dropdown menu with "ASCII Text (ISO-8859-1)" selected.
- Handphone number:** A text input field containing "94506718".
- Message:** A text area containing "Hi, this is testing message from sendQuick :0". Below the text area, it says "45 characters".
- Message Label:** An empty text input field.
- Priority:** A dropdown menu with "1" selected.

At the bottom of the form are two buttons: "Submit" (in blue) and "Reset" (in white).

Figure 15-5: Single SMS

b) File Upload

SendQuick has a feature that allows users to send mass SMS (broadcast) using either Comma Separated Value (CSV) or Tab Delimited value. These two formats are supported by most database or spreadsheet software, like Microsoft Excel, Access, MS SQL, GoldMine, ACT! and others.

The files need to be formatted (or exported in the relevant format) and saved as either CSV (.csv) or TXT (.txt) extensions. For Comma Separated Value, the file can be either CSV or TXT. For Tab Delimited, it will need to be in TXT format.

Data Format: The data format should be segmented in 2 columns: hand phone number and message content. The table below shows the example of the data format in the CSV and TXT file.

Data Format in the Files	Example
Comma Delimited Value (CSV)	91234567,hello how are you?
Tab Delimited Value (TXT)	91234567 hello how are you?

For exporting data from database or Microsoft Excel, your data in the software should be organized as shown below. The extreme left column is the mobile phone number followed by the Message in the next column. This format had to be followed strictly or will result in processing error.

96367680	Hi! This is a message for you
96189556	Hello, greetings from Singapore

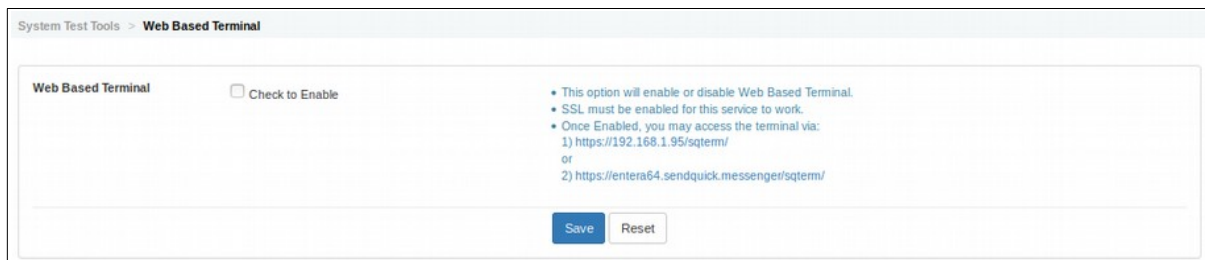
To send messages using either of these two file formats, select the **Language** (your message is written in), **File Format** and **Choose File** to select the file. Select **Submit** once you are ready (Figure 15-6).

The screenshot shows a web form titled 'File Upload'. It contains three main sections: 'Language Used' with a dropdown menu showing 'ASCII Text (ISO-8859-1)'; 'File Format' with a dropdown menu showing 'Comma Delimited (.csv, .txt)'; and 'File to upload:' with a 'Browse...' button and the text 'No file selected.'. Below these are 'Submit' and 'Reset' buttons. To the right of the form, there is a 'File Content' section with a list of fields: 'Mobile : Mandatory', 'Message : Mandatory', 'Priority : Optional. Default : 9', and 'Label : Optional. SMS with invalid modem label will not be sent.'. A 'Download Sample CSV file' button is located below this list.

Figure 15-6: File Upload

15.6 Web Based Terminal

SendQuick has tools for easy support in an event of technical issues. Apart from the patch and diagnostic approach, there is a Web Based Terminal for easy support for all systems. This service is only available through HTTPS access. Once enabled (In Figure 15-7 below), enter the URL as shown in the page to login user **sqguest** account.

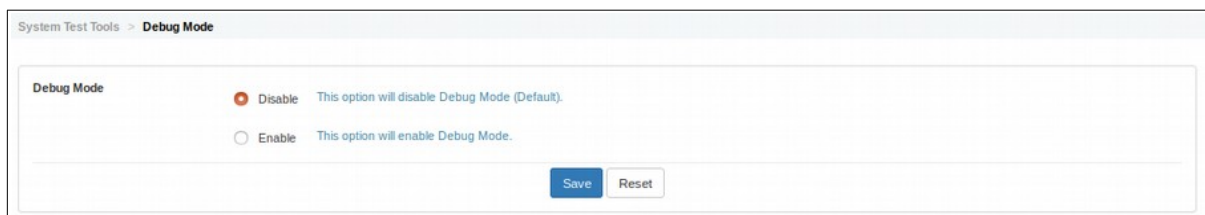


The screenshot shows the 'Web Based Terminal' configuration page. At the top, there is a breadcrumb 'System Test Tools > Web Based Terminal'. The main section is titled 'Web Based Terminal' and contains a checkbox labeled 'Check to Enable'. To the right of the checkbox, there are three bullet points: 'This option will enable or disable Web Based Terminal.', 'SSL must be enabled for this service to work.', and 'Once Enabled, you may access the terminal via:'. Below the bullet points, there are two numbered options: '1) https://192.168.1.95/sqterm/' and '2) https://entera64.sendquick.messenger/sqterm/'. At the bottom of the form, there are two buttons: 'Save' and 'Reset'.

Figure 15-7: Web Based Terminal

15.7 Debug Mode

SendQuick has option to enable to to disable the debug mode for the system.



The screenshot shows the 'Debug Mode' configuration page. At the top, there is a breadcrumb 'System Test Tools > Debug Mode'. The main section is titled 'Debug Mode' and contains two radio button options. The first option is 'Disable', which is selected (indicated by a red dot), and has a description 'This option will disable Debug Mode (Default)'. The second option is 'Enable', which is not selected, and has a description 'This option will enable Debug Mode.'. At the bottom of the form, there are two buttons: 'Save' and 'Reset'.

Figure 15-8: Debug Mode

16 SMS Specifications

This section documents the specifications to send and receive SMS, to and from sendQuick server, using either Email or REST methods. A copy of the detailed specifications is included in the sendQuick CD-ROM and can also be downloaded from the **Download Specifications (PDF)** menu.

Note: All SMS can only receive 160 characters per message. Please do not use more than 160 characters in the message body for both e-mail and HTTP Post connection.

16.1 Email API

You can send SMS via sendQuick either using HTTP Post or E-mail-to-SMS. The sending methods are tied to the IP address of the server.

Note: You should configure the Server with the correct fixed IP and should not change them unless absolutely necessary.

The specification for sending SMS messages to sendQuick are as follow:

a) Email method (no modem designation)

Email 1) <Mobile Number>@192.168.1.95 or

Email 2) <Mobile Number>@entera64.sendquick.messenger

b) Email method (with modem designation)

Email 1) <Label> – <Mobile Number>@192.168.1.95 or

Email 2) <Label> – <Mobile Number>@entera64.sendquick.messenger

The SMS message will be the email message content. Label is optional (only applicable if set in the system).

16.2 REST API - SMS

You can send SMS via sendQuick with the following REST API method for SMS:

i) HTTP Method

URL 1) `http://{sendQuick's IP}/cmd/system/api/sendsms.cgi` or

URL 2) `http://{sendQuick.name.com}/cmd/system/api/sendsms.cgi`

ii) XML Method

URL 1) `http://{sendQuick's IP}/api/sendsms_xml.php` or

URL 2) `http://{sendQuick.name.com}/api/sendsms_xml.php`

The XML attributes:

```
<?xml version="1.0"?>
<info>
<tar_num>-- The target mobile number.</tar_num>
<tar_msg>-- The target mobile number.</tar_msg>
<tar_mode>-- The message mode. Either 'text' or 'utf'.</tar_mode>
<label>-- Target modem label (optional). Only applicable if set in the
system.</label>
<clientid>-The identifier tag to easily trigger if there are more than
one applications running on the same server. (optional) </clientid>
</info>
```

iii) JSON Method

URL 1) `http://{sendQuick's IP}/api/sendsms_json.php` or

URL 2) `http://{sendQuick.name.com}/api/sendsms_json.php`

The JSON Attributes:

```
{
"tar_num": "-- The target mobile number.",
"tar_msg": "-- The message for the user.",
"tar_mode": "-- The message mode. Either 'text' or 'utf'.",
"label": "-- Target modem label (optional). Only applicable if set in
the system.",
"clientid": "-The identifier tag to easily trigger if there are more
than one applications running on the same server. (optional) " }
```


iv) SOAP Method

URL 1) `http://{sendQuick's IP}/api/sendsms_soap.php` or

URL 2) `http://{sendQuick.name.com}/api/sendsms_soap.php`

The SOAP Attributes:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:tns="urn:apiwsdl"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:wsdl="http://schemas.xmlsoap.org/
wsdl/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Body>
<mns:processAPI xmlns:mns="urn:apiwsdl"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<tar_num xsi:type="xsd:string"></tar_num>
<tar_msg xsi:type="xsd:string"></tar_msg>
<tar_mode xsi:type="xsd:string"></tar_mode>
<label xsi:type="xsd:string"></label>
<clientid xsi:type="xsd:string"></clientid>
</mns:processAPI>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

16.3 REST API - MIM

You can send SMS via sendQuick with the following REST API method for MIM:

URL 1) `http://{sendQuick's IP}/api/message.php` or

URL 2) `http://{sendQuick.name.com}/api/message.php`

i) HTTP Method

Header: Content-Type: application/x-www-form-urlencoded

- action -- "send"
- id -- The target mobile number.
- text -- The message for the user.
- type -- The message mode. Either 'text' or 'utf'.
- clientid --The identifier tag to easily trigger if there are more than one applications running on the same server. (optional)

ii) XML Method

Header: Content-Type: application/xml

XML Attributes:

```
<?xml version="1.0"?>
```

```
<data>
```

```
  <action>send</action>
```

```
  <payload>
```

```
    <message>
```

```
      <type>-- The message mode. Either 'text' or 'utf'.</type>
```

```
      <text>-- The message for the user.</text>
```

```
      <clientid>--The identifier tag to easily trigger if there are more than one  
applications running on the same server. (optional) </clientid>
```

```
    </message>
```

```
    <recipients>
```

```
      <id>-- The target mobile number.</id>
```

```
    </recipients>
```

```
  </payload>
```

```
</data>
```

iii) JSON Method

Header: Content-Type: application/json

JSON Attributes:

```
{  "action": "send",
  "payload": {
    "message": {
      "type": "-- The message mode. Either 'text' or 'utf'.",
      "text": "-- The message for the user.",
      "clientid": "-- The identifier tag to easily trigger if there are more than one
applications running on the same server. (optional) ",
    },
    "recipients": [
      { "id": "-- The target mobile number." }
    ]
  }
}
```

16.4 Receive SMS via sendQuick Server

After you have defined the receive SMS path and method (for your application server to receive the replied SMS) in Section 3.4 above, you will need to configure your applications to accept the messages in the following format and predefined variables. These format and variables are predefined by sendQuick and cannot be changed. It defines the way that your applications are able to recognize the information sent from sendQuick.

Please refer to the format below for the HTTP Post and E-mail communication methods.

Example of http response from the server:

`http://<response_url>?mno=91234567&txt=Testing&dtm=02/06/10,14:19:18&charset=utf-8`

Where:

mno -- the mobile phonnumber

txt -- the text message

dtm -- the date and time of the SMS received.

charset – language character set

As for e-mail, the received SMS message will be sent to the e-mail specified in Section 3.4. An example of the received e-mail is as below.

From : 91234567@192.168.1.8
Date : Monday, June 10, 2002 2:31 PM
To : sh_ang@yahoo.com <sh_ang@yahoo.com>
Subject : SMS From 91234567

Sender: 91234567
Timestamp: 10/06/02,14:32:54
Message: Test

You will need to configure your back-end system and applications to receive the messages in the format mentioned above.

16.5 Sending Message to Overseas Mobile Number

Sending SMS to overseas user is network (or SIM) dependent. This means that your SIM card and mobile network must be able to send to an overseas number directly.

For sending via email to SMS, start the email address with (+)(country code). Example, if you are a using the server in Singapore and intend to send to Malaysia, your email will look like:

+60121234567@192.168.1.8

where +60 is the added country code for overseas (international) SMS.

If you are using HTTP Post method, the (+) and country code need to be added to the mobile phone (tar_num) field. The hex-value for (+) is %2B for HTTP Post method.

17 Shutdown, Restart and Logout from the System

To Shutdown, Restart or Logout, just select the relevant button from the navigation menu located at the top right hand corner of the interface (Figure 17-1). You will see a successful message when the task is confirmed.



Figure 17-1: Shutdown, Restart or Logout

18 HIGH AVAILABILITY CONFIGURATION

HA module is configurable in the admin interface via the **Server Setup** menu. As the configuration requires certain understanding, we do advise all administrators to read this section before actual configuration to avoid any confusion and misconfiguration. When in doubt, please contact TalariaX for clarifications. The step-by-step approach is documented below.

Before you proceed with the configuration, please make sure you have the following prepared:

- 1 x Cross cable for heartbeat checking
- 2 x IP address set for heartbeat checking (this can be internal IP set)
- 2 x IP address set of the primary and secondary server (configure the servers as normal configuration first)

Select the **High Availability Setup** menu and the interface below will be shown (Figure 18-1).

The screenshot shows a web-based configuration interface for High Availability Setup. It features a 'System Mode' dropdown menu set to 'Primary'. Below this is a checkbox labeled 'Check to suspend the clustering mode' with a descriptive note: '(Use this only if there is a need to shutdown the system for maintenance. NOTE: Both machines need to be in Suspended mode manually. Not applicable for Standalone mode.)'. A 'Server Name' dropdown is set to 'B', with a note: 'If the server is in "Data Synchronization" mode, one of the servers should have named "A" and the other should have named "B".'. At the bottom, there is a section for 'Primary/Secondary' IP addresses, with 'Local IP' set to '10.1.1.10' and 'Remote IP' set to '10.1.1.11'.

System Mode	Primary ▼
<input type="checkbox"/> Check to suspend the clustering mode (Use this only if there is a need to shutdown the system for maintenance. NOTE: Both machines need to be in Suspended mode manually. Not applicable for Standalone mode.)	
Server Name: B ▼ If the server is in "Data Synchronization" mode, one of the servers should have named "A" and the other should have named "B".	
Primary/Secondary	
Local IP	10.1.1.10
Remote IP	10.1.1.11

Figure 18-1: High Availability Setup

First, select the **System Mode**, you can choose to suspend the HA service (select only when you need to perform system maintenance, else do not select). The description for the System Mode options is as below:

System Mode	Description
Stand Alone	The system act as a single machine and no HA is required. By default, this is selected. Hence, the system can function as a normal single unit, if required.
Primary	Primary server refers to the system that is being used by the applications, and perform the load distribution and replication with the secondary server. This also serves as the controller in the HA configuration.
Secondary	Secondary server serves as a backup for the Primary. It synchronized all the configuration of the Primary and will assume Primary server IP when primary is not working.

System Mode	Description
Data Sync (exclude Network Monitoring Rules)	The system will synchronize the data except the rules created under Network Monitoring. This option is for systems which are not in the same VLAN network.
Full Data Sync	The system will synchronize the data including the rules created under Network Monitoring. This option is for systems which are set up in the same VLAN network.

The next section is to configure the cross IP checking performed by the two (Primary and Secondary server) servers with each other. This is also known as the **heartbeat** between the two systems.

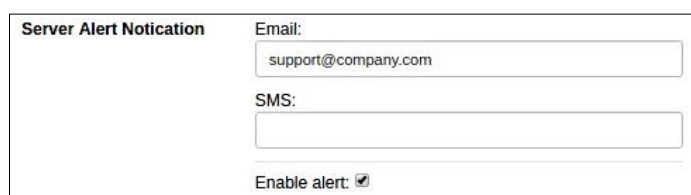
The **heartbeat checking is configured on eth1 or E2** (as labeled on the LAN port).

The **Local IP** refers to the IP of the machine (that you are configuring) for the heartbeat LAN port. If the server is a Secondary Server, this is the heartbeat IP of the secondary server. **Remote IP** is the IP address that will be checked by the Local IP. E.g. if secondary server, Remote IP is Primary Server heartbeat IP port.

Note: The IP (Local and Remote) in Figure 18-1 above is NOT the IP that is configured for the servers (Primary & Secondary) respectively, which was configured in the Server Setup section (Section 5). In fact, the (local and remote) has to be a totally different network range from the IP address in the Server Setup.

In the setup above, always perform the configuration in the secondary server first. The reason is once you complete the Primary server configuration, it will need to search and replicate to the secondary server. (refer to the step by step guide for the right order).

Then, configure the email and SMS notification for switch-over and restoration alerts.



The screenshot shows a 'Server Alert Notification' window. It contains three input fields: 'Email' with the value 'support@company.com', 'SMS' which is empty, and 'Enable alert' which is checked with a checkbox.

Figure 18-2: Server Alert Notification

When saving as Primary server, the system will show a configuration process and Secondary server

will be updated automatically. If the update is successful or unsuccessful, it will be displayed on the web interface.

Note: Please have the cross cable connected between the Primary and Secondary servers' E2 before the Primary server can activate the Secondary server.

Once the configuration is completed, the two (2) servers are already in HA mode.

The HA function is sendQuick works with an actual IP on actual LAN. **SendQuick does not use a virtual LAN for HA.** Hence, when there is a failure, the **Secondary server will restart and will reconfigure itself as the Primary server IP**, ensuring there is continuous performance and no changes done at the application layer. Applications can continue to send SMS as the IP will be consumed by the Secondary server. The switch over downtime is about 30 seconds.

When the Primary server is restored and turned on, the two servers will be synchronized and their roles will be reverted to their original configuration automatically. This process will take about 30 seconds as well.

In summary, the step-by-step guide to configure HA systems is as below:

Step	Materials Required	Configuration
1	IP address set	Configure the IP, Netmask and Gateway of Primary and Secondary server IP as explained in section 5.
2	LAN cable	Connect the LAN cable to port Eth1 of both Primary and Secondary servers and ensure the IP is accessible via the network
3	Cross cable	Connect the cross cable between ports Eth2 of both Primary and Secondary servers
4	Laptop/PC in the LAN Local and Remote IP for Eth2 for Secondary server	Access Secondary server IP and configure the HA (cluster) configuration with the Remote and Local IP for secondary on port Eth2. Save the setting.
5	Laptop/PC in the LAN Local and Remote IP for Eth2 for Primary server	Access Primary server IP and configure the HA (cluster) configuration with the Remote and Local IP for primary on port Eth2. Save the setting and you will notice a process where Secondary server is being configured and synchronized. Please ensure the web interface shows a successful configuration. The process is completed once it is successfully configured.

19 CONSOLE CONFIGURATION AND SETTINGS

While the main access approach to sendQuick is via web browser, you can also perform some simple configuration and settings via the console. Console access will require the monitor and keyboard connected to the system.

- Connect the monitor to the VGA Port
- Connect the USB/PS2, whichever is applicable

Once the sendQuick is fully started, you will see the IP routing table on the monitor screen. The display is shown in Figure 19-1 below:

```
Mounting non-root local filesystems:
tmpfs on /dev/shm type tmpfs (rw,mode=0755)
tmpfs on /tmp type tmpfs (rw,size=512M,mode=1777)
tmpfs on /var/run type tmpfs (rw,mode=0755)
Using /etc/random-seed to initialize /dev/urandom.
INIT: Entering runlevel: 3
Going multiuser...
Starting syslogd daemons: /usr/sbin/syslogd -r process `syslogd' is using obsolete setsockopt SO_B
SDCOMPAT
/usr/sbin/klogd -c 3 -x
Scanning all LUNs for additional hardware: /sbin/rescan-scsi-bus -l
Host adapter 0 (mptspi) found.
Scanning hosts 0 channels 0 for
  SCSI target IDs 0 1 2 3 4 5 6 7 , LUNs 0 1 2 3 4 5 6 7
0 new device(s) found.
0 device(s) removed.
Starting Internet super-server daemon: /usr/sbin/inetd
Starting OpenSSH SSH daemon: /usr/sbin/sshd
Updating shared library links: /sbin/ldconfig
Updating X font indexes: /usr/X11R6/bin/fc-cache
Starting ACPI daemon: /usr/sbin/acpid
/usr/local/apache/bin/apachectl start: httpd started
postmaster starting
SIOCGMIIPHY on 'eth0' failed: Operation not supported

-----
IP address
eth0 (00:0C:29:E8:4C:64): 192.168.1.111
-----

Kernel IP routing table
Destination      Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.1.0      0.0.0.0         255.255.255.0   U        0 0          0 eth0
127.0.0.0        0.0.0.0         255.0.0.0       U        0 0          0 lo
0.0.0.0          192.168.1.1    0.0.0.0         UG        0 0          0 eth0
-----
```

Figure 19-1: IP Routing Table

In the monitor console, the administrator can perform the following functions:

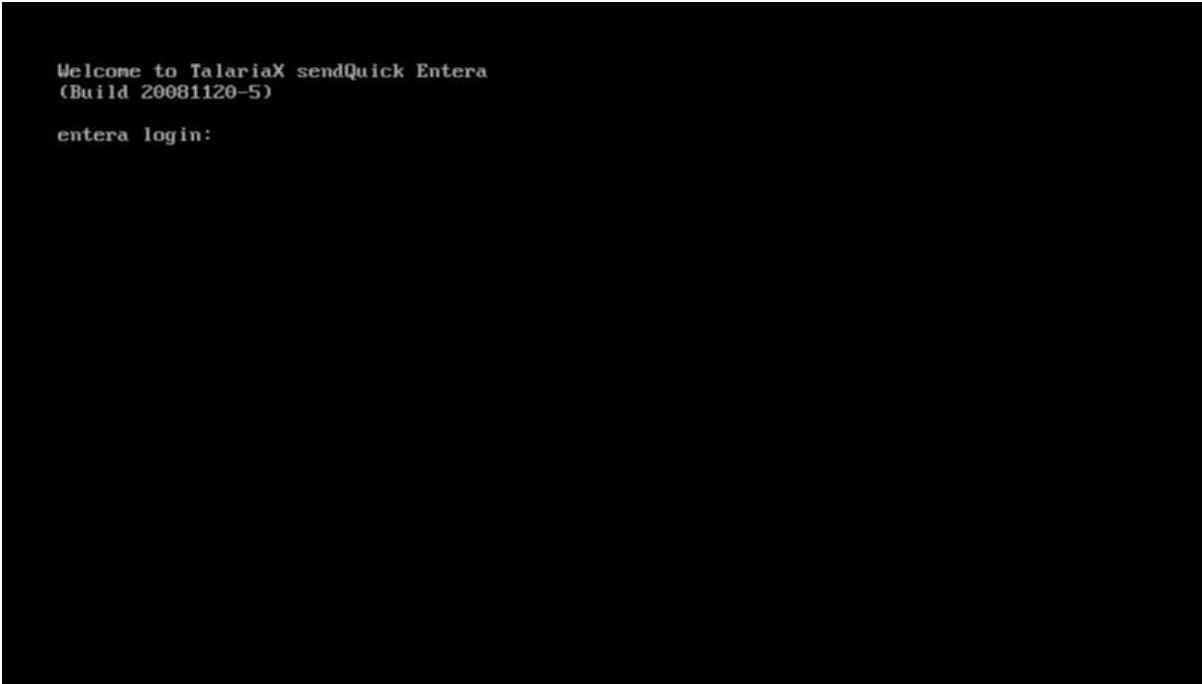
- Configure IP address of sendQuick system
- Change sendQuick Web Admin Password

19.1 Configure sendQuick IP via Console

First, you need establish the physical connection as described above. Then, enter **ALT and F4** simultaneously. You will see the login page as shown in Figure 19-2 and enter the default username and password below.

Console Username: admin


Console Password: sqroot



```
Welcome to TalariaX sendQuick Entera
(Build 20081120-5)

entera login:
```

Figure 19-2: Console Login Prompt



```
Activate Base Setup

IP Address:
192.168.1.8_____

Netmask:
255.255.255.0_____

Gateway:
192.168.1.1_____
Set Reset
```

(Text entry field) Enter text. Use UP or DOWN arrows or tab to move off.
Enter text into the field by typing on the keyboard
Ctrl-U to delete all text in field, [Backspace] to delete a character

Figure 19-3: Change IP Address

19.2 Reset Web Login Password

Another function that can be performed from the console is to reset the web login password back to the default **admin123**. To perform this, enter **Ctl-ALT- F3 (or Alt+F3)** on the keyboard and the **Reset Password Prompt** is shown on the screen as seen in Figure 19-4.

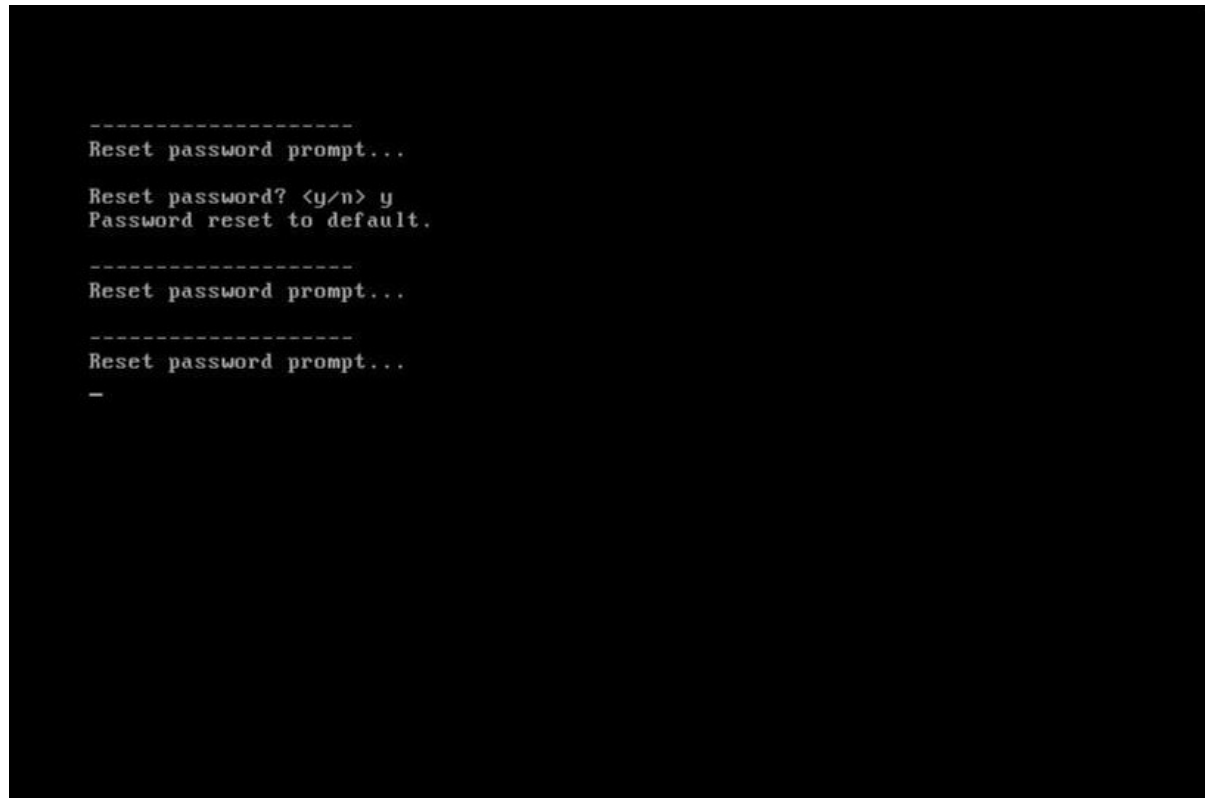


Figure 19-4: Reset Password Prompt

Follow the instructions that are shown on the screen the reset password will be executed. Once the reset has been done, you can perform the web login with the following:

Username: admin Password: admin123

20 TROUBLE SHOOTING

You may encounter some common problems when using sendQuick Server. This section serves to address these common problems and how to overcome them.

20.1 I have forgotten the IP address of my sendQuick server. How do I check?

If the system is powered up, connect a monitor to the VGA port and notice the IP address in the IP routing table (Figure 5-1). The IP address is the IP on eth0.

20.2 I have done all the set-up. I tried to SMS via the web interface as explained in section 3.12 but no SMS was received. Why?

You could be facing the following problems:

- (i) Modem connection is not properly attached. Please check the USB connection
- (ii) The SIM card is not placed properly or not working. Try with another SIM card.
- (iii) The SIM card is not activated (see Question 6.8)

20.3 I set the entire configuration in the server set-up accordingly but I still cannot send e-mail to SMS from my e-mail software. Why?

There may be a few reasons for this. We will review the possible reasons accordingly.

- (i) The physical network connection may be faulty. Try to ensure that the network cable is plugged-in properly and do not use an old cable. Once the cable is fine, then,
- (ii) Try to 'ping' the sendQuick Server from a remote machine. If there is no reply, there are some problems with the network or connection or the switch (some switch requires hard reboot to activate a new connection). Please check. If you get a ping reply, then,
- (iii) Check your e-mail server setting. Your mail server may not be supporting the e-mail address for SMS as it does not contain a valid DNS or name server (when you use an IP). You need to configure a static mail routing in your e-mail server. You can also try by changing the SMTP server in your e-mail client configuration to the IP address of sendQuick Server. If it works after you change the SMTP server, then it is a problem with your e-mail server concerning the mail routing information. Contact your administrator for assistance (*If sending email via Exchange or Domino, please ensure you register the SMS domain in the DNS, perform mail routing in Exchange/Domino – MX or A records for proper email routing*).
- (iv) Your modem connection could be loose. Try to fasten the modem (especially the USB version) and restart the server if necessary. Restart using hard reboot.

20.4 I cannot access the sendQuick Server from my local PC even though it is already in the network and some of my other colleagues can use it. Why?

This could happen if there exist some sub-networks in your company's network. You may need to check with your system administrator and ensure that the router allows the different networks to send data to each other.

20.5 I realized that the server only provides for one e-mail and one HTTP response. How do I allow SMS enquiries to more than one applications at one instant?

The sendQuick server is designed as a 'black-box' solution for sending and receiving SMS. We understand that most of our customers would want to interact with more than one server. In order to make things easy for all, we designed a single response URL and e-mail to make sendQuick very easy to configure and hassle free. To connect to multiple applications, you just need to develop a simple script to process the replies from sendQuick (either HTTP or e-mail) and make your own distribution to the respective applications. This can be done by setting unique codes (keyword) for each SMS when they were sent to sendQuick and processed by your script.

In this way, you will not have any constraints on any number of application servers that can use sendQuick. You can also purchase sendQuick Entera or sendQuick Enterprise that has built-in Keyword Management module.

20.6 I am getting email alerts on my administrator email account stating that the modem is not found or having problem. What should I do?

The sendQuick server is designed as a 24x7 system with a built-in self-checking mechanism to the modem and SIM card availability. Hence, if there is any failure to detect the modem or SIM, it will generate an error message and email to the administrators email account.

If the error messages is not frequent (that is, the alert message is occasional and not continuous for every second), there is no cause for alarm. An instance that may cause this problem is when there is an intermittent weakness in the GSM network or the system cannot find modem at that point of time. However, if the error message is continuous (for every second) and still happening at the point when you read the messages, then there is an indication that there is some modem or SIM problem with the system (see question 6.7).

20.7 I am getting continuous alert messages stating that there is no modem and the alert message is occurring every second or I cannot send SMS despite able to access the system via web interface. What is the solution?

If either of the above happened, there could be a problem with the GSM network, SIM card or GSM modem. Troubleshoot by checking the following areas:

- (i) Check that the SIM card is still in service or there is sufficient credit (for prepaid card) by calling (dialing) the SIM card number and you should hear a dialing tone (indicates it is normal).
- (ii) Check that the GSM modem is properly connected and the LED indicator is blinking (normal). If the LED is not blinking (continuous light), either the SIM is not working, fail to connect to GSM network or modem not properly connected
 - You can try by remove and then plug in the modem again
 - Remove and insert the SIM card again. Please make sure the GSM modem cover is properly covered

20.8 The system is not sending SMS. What are the troubleshooting steps?

If you cannot send SMS from your applications, there are a few possibilities. Do the following actions to determine the possible point of failure.

- (i) Ping the sendQuick server and see if there is a response. If yes, try step (ii). If no response, check your network connection to sendQuick server or to your application server. You may wish to access the sendQuick using the direct console access. If you cannot access or you see an error message on the console, contact TalariaX for technical support.
- (ii) Access sendQuick using the web browser. If yes, try step (iii). If you cannot browse the server, try to access via the console. If you cannot access or you see an error message on the console, contact TalariaX for technical support.
- (iii) Use the browser access, go to Send SMS section and send a test SMS message to yourself. Check the modem status and log file to ensure messages are processed and sent. If you receive the SMS sent, then the problem lies with the application server. If you did not receive a SMS message, there could be a problem with the SIM card or GSM modem.
- (iv) Check that the SIM card has sufficient credit (for prepaid) or that the GSM modem is blinking. You can try to remove and reinsert the SIM or to unplug and replug the modem into the USB/serial slot.
- (i) If you are using a new SIM card, please ensure that the SIM (PIN number) lock has been disabled or unlock. Please perform a SMS or phone call with the new SIM card (in a phone) to ensure the SIM is activated. If all fails, contact TalariaX for technical support.

20.9 had configured the reminder and escalation function and I am receiving the SMS. However, the Reminders and Escalations are sent even after I sent the correct reply (Acknowledgment).

There are two possible causes:

- (i) The SMS acknowledgement was received (about the same time) as the reminder or escalation message was sent. Therefore, the messages were generated while the acknowledgement was received. In this case, please set the reminder/escalation timing interval with a larger value
- (ii) The acknowledgement SMS format and the Number list need to be an exact match. Most incoming SMS has an international format with a plus '+' sign. In order to have a match in the acknowledgement, change the number format (in the alertee list) to an international format with a '+' sign.

20.10 How to correctly activate or restart the modem.

If the modem is directly using USB power:

1. Remove the USB modem from the appliance if it is connected to it.
2. Make sure the SIM has been inserted correctly into the modem.
3. Wait 2-3 mins before reconnecting the USB to the system.
4. Wait for roughly 2-3 mins and check LED status. The Modem LED must be blinking at a regular interval. It's should be 'Single blink', not 'Double blink'.

Single Blinking patten: blink--pause--blink--pause--blink...

5. Check the sendQuick for modem connection status (Dashboard → Modem Status)

If the modem is using its own power adapter:

1. Make sure the modem is not connected to the appliance. If the modem uses USB-serial adapter, make sure the USB-serial is disconnected from the system.
2. Make sure the modem is power off.
3. Make sure the SIM has been inserted correctly into the modem.
4. Power ON the modem.
5. The Modem LED must be blinking at a regular interval. It's should be 'Single blink', not 'Double blink'.

Single Blinking patten: blink—pause—blink--pause--blink...

6. Wait 2-3 mins before reconnecting the USB to the system
7. Wait for 2-3 mins and check the sendQuick for modem connection status (Dashboard → Modem Status).

NOTE:

- **Do not power on the modem before SIM card is inserted.**
 - **Do not swap the SIM card while the modem is in operation.**
- These actions may cause damage to the modem or modem hanged.**

20.11 When sendQuick cannot detect modem.

- I. Check modem's Power/USB cable is connected correctly.
- II. Check modem physically, the Modem's LED must be blinking at a regular interval, otherwise try to reset modem by power off/on, disconnect the Power/USB cable, wait for 2 minutes and reconnect the cable again.
- III. Make sure that SIM is valid and has been inserted correctly into the modem, use a physical mobile phone to test the SIM card, try to send and receive SMS. If you are unable to send SMS from your mobile phone, please contact telco for advice.
- IV. Login to sendQuick, access to menu > Usage Logs > System Log, check if any error code, please refer to section 21 – Modem Error code for detail.

20.12 How modem works

- I. Modem will get power from sendQuick device.
- II. Detect mobile network (with a valid SIM card installed).
- III. Detect Telco's signal.
- IV. Try to register to Telco base station.
- V. Upon successfully registered, the modem's status will display on sendQuick's Dashboard → Modem Status.
- VI. If failed to register to telco, the modem will reset by itself and try again from step II.

20.13 How to perform modem hard reset

When you remove the modem and power off/power on, you are actually perform modem hard reset and the telco system re-register the SIM again.

20.14 Why SIM Barring / Fair-Use Policy

Every mobile operator (telco) may impose their rules on fair use of SMS transmission (Fair Use Policy).

The telco may bar the SIM from sending SMS if they decided that the SIM has violated their fair use policy. For example if your SIM send more than 1,000 SMS per day or more than 10,000 per month (This apply to Singapore operator, other countries may have similar or different policies). Example of fair use policy states that if the SIM is used in an automated system to send SMS, they can block the SIM. Please consult your local Telco(s) for detail and advice on the appropriate type of SIM to be used with automated system (modem).

sendQuick has built-in feature to send messages via Internet connection (Section 6.4: sendQuickASP Routing) or using social messenger like WhatsApp or Telegram and others (Section 6.8: Mobile Instant Messaging Routing) that can send messages without SIM. Do contact TalariaX at info@talariax.com for more details.

21 Modem Error Code

Error code 3: SIM not allow to register to the network

Telco has been barring SIM cards from sending SMS when your volume is high due to the Fair Use policy. The log shows error 3, which is not allowed the SIM to register to the network. Please contact Telco, let them know the SIM card number and request for them to unbar the SIM.

Error code 10: SIM card not detected

Error code 10 is returned by the modem when it does not detect a SIM card. Usually, this means that the SIM card is missing or is not inserted properly in the SIM card slot of the modem.

Error code 13: Modem error status, SIM failure

Please check from Menu > Dashboard > Modem Status, check if you can see any modem is detected and online.

Please follow these steps to troubleshoot.

- i. Power off the modem.
- ii. Disconnect the Modem cable from sendQuick.
- iii. On modem, remove the SIM card(s) card.
- iv. Use a physical mobile phone to test the SIM card (one at a time), try to send and receive SMS.
- v. If you are unable to send SMS from your mobile phone, please contact telco for advice.
- vi. If you are able to send SMS from your mobile phone, please proceed the next steps.
- vii. Inset the SIM card(s) back to the modem.
- viii. Power on the modem, observe the modem's LED light(s) (it will take a while), the LED light should 'blink' in a correct interval.
- ix. Connect the Modem's USB cable to sendQuick.
- x. Login to sendQuick as Admin, access to menu > Dashboard > Modem Status; you should see the detected modem on this screen.

Error Code 21: SMS Rejected

Error 21 means 'Short message transfer rejected'. It indicates that the mobile service does not accept the message but it does not give the exact reason why. It could be an invalid number, insufficient SMS credits or a number of other reasons.

Error Code 38: SIM card failed

Error 38 means 'Network out of order'. Please check with the Operator for this error.

This error message comes from the modem, it means that the message could not be sent because there is a problem with the connection of the modem to the mobile network. The error messages that GSM modems give back do not always reflect the real cause of the problem. This error could also mean that the network has rejected the message for some reason, for instance when there are insufficient SMS credits for your SIM card. This error can also be triggered if the mobile network operator rejects the messages to prevent spam or high cost caused by an (for normal phone use) unusual high amount of SMS messages.

Error code 69: Suspected Spam

The SIM has been blocked by telco to broadcast sms to the recipient(s), eg suspected spam sms or user blacklisted sender's number or phone number is invalid, try without country code.

Error code 111: Operator Network Coverage issue

Error **111** is related to operator coverage issue. Such error can be intermittent and could be due to telco signal is weak at your area/server room. You can try to have a long antenna cable that able to locate your antenna outside your Server room/DC.

Error code 429: Too many request

Error 429 is related to Too Many Request error occurs when a user tries to perform too many requests within a certain time frame. This error is triggered based on the particular rate-limiting settings that a service provider's servers have in place. Rate limiting is used in order to **limit the number of requests** a user is able to perform to help reduce the risk of their server's being overloaded.

Error code 500: Operator reject code

We would suggest check with your local operator of your mobile plan subscription and make sure it didn't hit any limit.

In some country, telco set a limit of number of SMS per month. eg If it hits to 10k limit, some sms were be rejected by operator

Please also check the number of sms send by customer per day, per week and per month.

The error could also means:

- I. The mobile number you try to send your message to is invalid. Eg home line, mobile number is no longer in used etc.
- II. There is no network coverage.
- III. You don't have enough money on a prepaid subscription.
- IV. The short message service center of the GSM network operator is temporarily out of service.
- V. The GSM cell is overloaded.

Error code 512/513: Operator Explicit Deny or Network Error

The above error codes is an operator returned failure, some messages were rejected by the operator. For example(in some country), telco(s) will limit it to 1,000+- sms per day or 10,000 per month per sim. Once it hit the quota, they will start to block/throttle the traffic. we would suggest check with telco on your mobile plan subscription and make sure it didn't hit any limit. From our experience, Telco will start to reject sending some messages if it exceed 1,000+- per day or 10,000 SMS per SIM per month. Also, can face sim card failure and the system does not detect the modem. but , if you restart the modem, SIM will re-register to Operator again and can send out few SMS for a period of time.

Check the system Usage Log > SMS sent and see the log/number of records for last 30 days. If you have sent more than 10k SMS per modem (or close to it), it is an issue with telco SIM, especially if you are using SingTel. Singtel is blocking all SIM cards that send close to or more than 10,000 SMS per month per SIM or more than 1,000 per day.