# sendQuick Server Licensing Agreement and Administration Manual

Version 4.6

**TalariaX Pte Ltd**
76 Playfair Road
#08-01 LHK2 Building
Singapore 367996
Tel : +65 6280 2881    Fax : +65 6280 6882
Email : info@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 of 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 Administration Manual

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
4.4 Menu Items 13
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 18
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 SMS Messaging Setup - SMS 21
6.2 SMS Messaging Setup - Email 22
6.3 SMS Queue Monitoring 23
6.4 SMS Response Action 24
6.5 sendQuickASP Routing 25
6.6 Sqoope Routing 27
6.7 Direct Connection 29
6.7.1 Direct Connection – Send SMS (Provider = Other) 31
6.7.2 Direct Connection – Check Status (Provider = Other) 34
6.7.3 Direct Connection – Send SMS (Provider = ASP) 37
6.8 SMPP Route 38
6.9 Mobile Instant Messaging Routing 40
6.10 Alert Profiles 42
7.0 Modem Setup 43
7.1 Modem License 43
7.2 Modem Dispatch Mode 44
7.3 Modem Routing 44
7.4 Virtual Modem Routing 46
7.5 Modem Monitoring & Respool 46
7.6 Modem Priority 47
7.7 Modem Time Control 47
7.8 IMEI SIM Card Mapping 48
7.9 MPM Routing 48
8.0 Phone Book & Roster 49
8.1 Phone Book Records 49
8.1.1 Phone Book Records – Upload by CSV File 50
8.1.2 Phone Book Records – by AD/LDAP Setup 52
8.2 MIM Phone Book Records 57
8.3 Roster Management 57
8.4 AD/LDAP OU Alert 59
8.5 Delete AD/LDAP Contacts 59
9.0 Filter Rules 60
9.1 Email Filter 60
9.2 SNMP Trap Filter 65
9.3 Syslog Filter 67
10.0 Network Monitor 68
10.1 Ping Check 68

10.2 URL Check 69
10.3 Port Check 70
11.0 Security Setup 73
11.1 HTTP Host Permission 73
11.2 SMTP Host Permission 74
11.3 Email User Permission 74
11.4 Relay Host Permission 75
11.5 Database Connection Permission 76
11.6 Mobile Number Permission 77
11.7 System Services 77
11.8 SSH Remote Access 79
11.9 How to enable SSL Service 80
11.9.1 How to Generate SSL Key, Certificate or CSR 83
11.9.2 How do I know if https is enabled? 87
11.9.3 How do I check my SSL certificate details? 87
11.9.4 How to View SSL Certificate Details in Each Browser ? 87
11.9.5 Token Management 88
12.0 Password Management 89
12.1 Server Admin Web Login 90
12.2 Supervisor Web Login 94
12.3 Operator Web Login 97
12.4 Console Login 99
12.5 SSH Login Account 99
12.6 FTP Login Account 99
12.7 Database Access Account 100
12.8 User Web Access Login 100
13.0 Backup & Diagnostic 101
13.1 Generate Backup File 101
13.2 Automated Backup 101
13.3 Restore Backup File 102
13.4 Generate Diagnostic File 102
13.5 Apply Patch 103
14.0 Usage Logs 104
14.1 Message Log 104
14.2 Conversation Summary 104
14.3 Email Log 105
14.4 Alert Log 105
14.5 System Log 106
14.6 Audit Log 107
14.7 Usage Statistic 107
14.8 Maintenance and Report 108
15.0 System Test Tools 109
15.1 SMTP Connectivity Test 109
15.2 Ping Test 109
15.3 Traceroute Test 111
15.4 Port/Telnet Test 111
15.5 Send Test SMS 112
15.6 Web Based Terminal 113
15.7 Debug Mode 113
16.0 SMS Specifications 114
16.1 Email API 114
16.2 REST API - SMS 114
16.3 REST API - MIM 115
16.4 Receive SMS via sendQuick Server 116
16.5 Sending Message to Overseas Mobile Number 117
17.0 Shutdown, Restart and Logout from the System 118
18.0 High Availability Configuration 118
19.0 Console Configuration and Settings 121
19.1 Configure sendQuick IP via Console 121
19.2 Reset Web Login Password 123
20.0 Troubleshooting 124
20.1 I have forgotten the IP address of my sendQuick server. How do I check? 124

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? 124

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? 124

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? 124

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? 125

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? 125

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? 125

20.8 The system is not sending SMS. What are the troubleshooting steps? 126

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). 126

20.10 How to correctly activate or restart the modem. 126

20.11 When sendQuick cannot detect modem. 127

20.12 How a modem work 127

20.13 How to perform modem hard reset 128

20.14 Why SIM Barring / Fair-Use Policy 128

20.15 Why Need to Perform Modem Reset 128

20.16 I am getting Delivery Date (DR) blank, does it means SMS is not sent ? 129

20.17 What is the definition of the Turnaround time ? 129

20.18 The modem should be detected by the sendQuick even if a sim is not installed? 129

20.19 SMS fail to send with “Invalid Format” in Unsent Box. 129

20.20 Modem stay stuck in "Modem Init" State, Modem Info SMSC, Operator Info stays in "Detecting" state. 129

20.21 How do I generate a CA Cert ? 130

21.0 Modem Error Codes 130

CME Error code 3: SIM not allow to register to the network 130

CME Error code 10: SIM card not detected 130

CME Error code 13: Modem error status or SIM card failure 130

CMS Error Code 21: SMS Rejected 130

CME Error Code 30: No network service / Unknown subscriber 130

CMS Error Code 38: SIM card failed 131

CMS Error code 69: Suspected Spam 131

CMS Error code 111: Operator Network Coverage issue or Invalid Phone number 131

CMS Error code 310: SIM not inserted 131

CMS Error code 500: Operator reject code, mobile network or target recipient error 131

CMS Error code 512/513: Operator Explicit Deny or Network Error 131

# 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 function in the network of your organisation. 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.

Please note that this manual is a consolidated document for all sendQuick servers. Therefore, some of the features are found only in some sendQuick models and this will be highlighted when applicable.

## 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 organisation 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)**
4. Login using the username & password: The default username and password can be found in the "your password" envelope or contact support@talariax.com to get assistance.
5. Configure the Server Set-up. (IP address and others)
6. Configure the SMS System Set-up.
7. Plug in the Ethernet (LAN) cable.
8. 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.

**Note:** Get assistance from your system administrator if you do not have the IP addresses for the server and gateway

# 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.

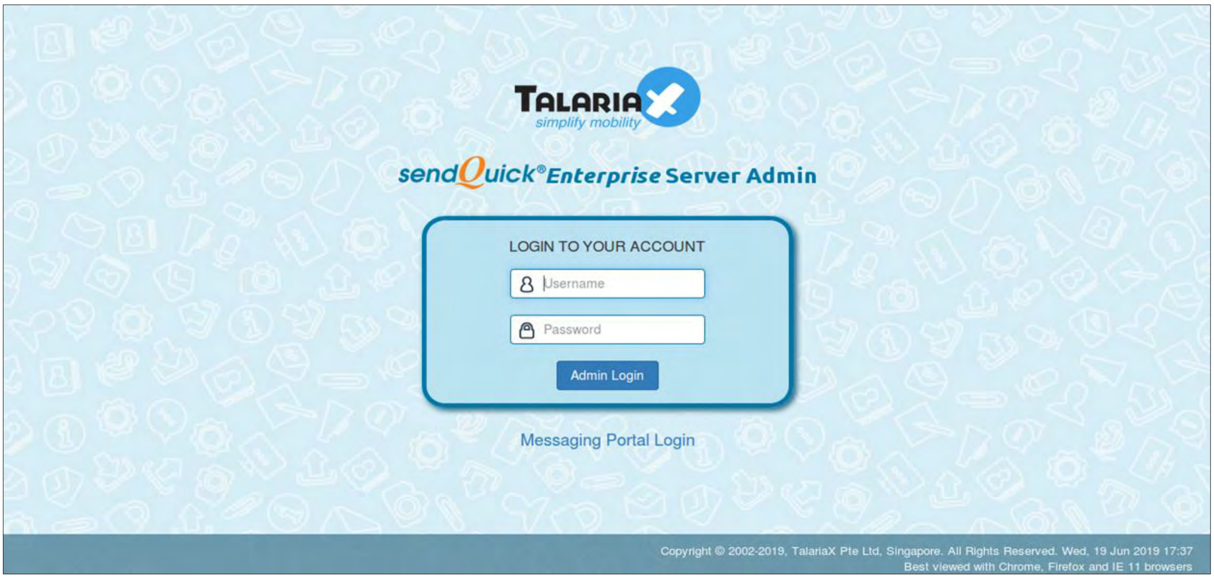

TALARIA X
simplify mobility
sendQuick® Enterprise Server Admin
LOGIN TO YOUR ACCOUNT
Username
Password
Admin Login
Messaging Portal Login
Copyright © 2002-2019, TalariaX Pte Ltd, Singapore. All Rights Reserved. Wed, 19 Jun 2019 17:37
Best viewed with Chrome, Firefox and IE 11 browsers

*Figure 3-1 : Web Administrator Log-in Page*

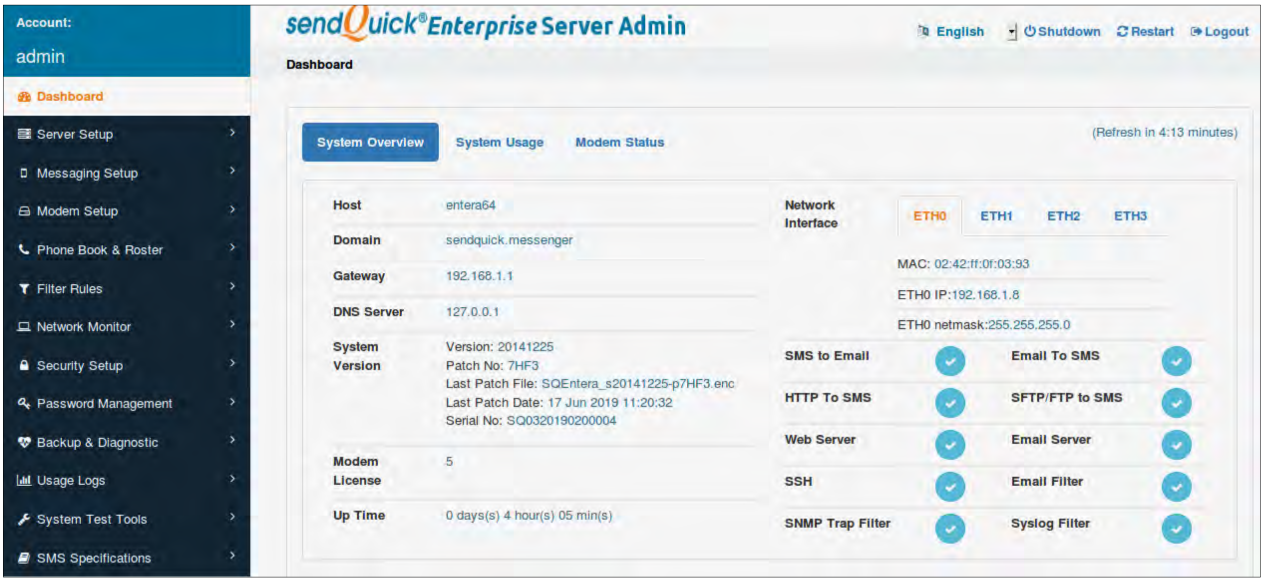
Enter the default Administrator's Log-in Name and Password to access the system. The default username and password can be found in the "your password" envelope. For further assistance please contact support@talariax.com via email.

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 Password Management.

# 4.0 Dashboard

## 4.1 System Overview

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



(Refresh in 4:13 minutes)

| | |
|---|---|
| Host | entera64 |
| Domain | sendquick.messenger |
| Gateway | 192.168.1.1 |
| DNS Server | 127.0.0.1 |
| System Version | Version: 20141225<br>Patch No: 7HF3<br>Last Patch File: SQEntera_s20141225-p7HF3.enc<br>Last Patch Date: 17 Jun 2019 11:20:32<br>Serial No: SQ0320190200004 |
| Modem License | 5 |
| Up Time | 0 days(s) 4 hour(s) 05 min(s) |

Network Interface: ETH0

MAC: 02:42:ff:0f:03:93

ETH0 IP:192.168.1.8

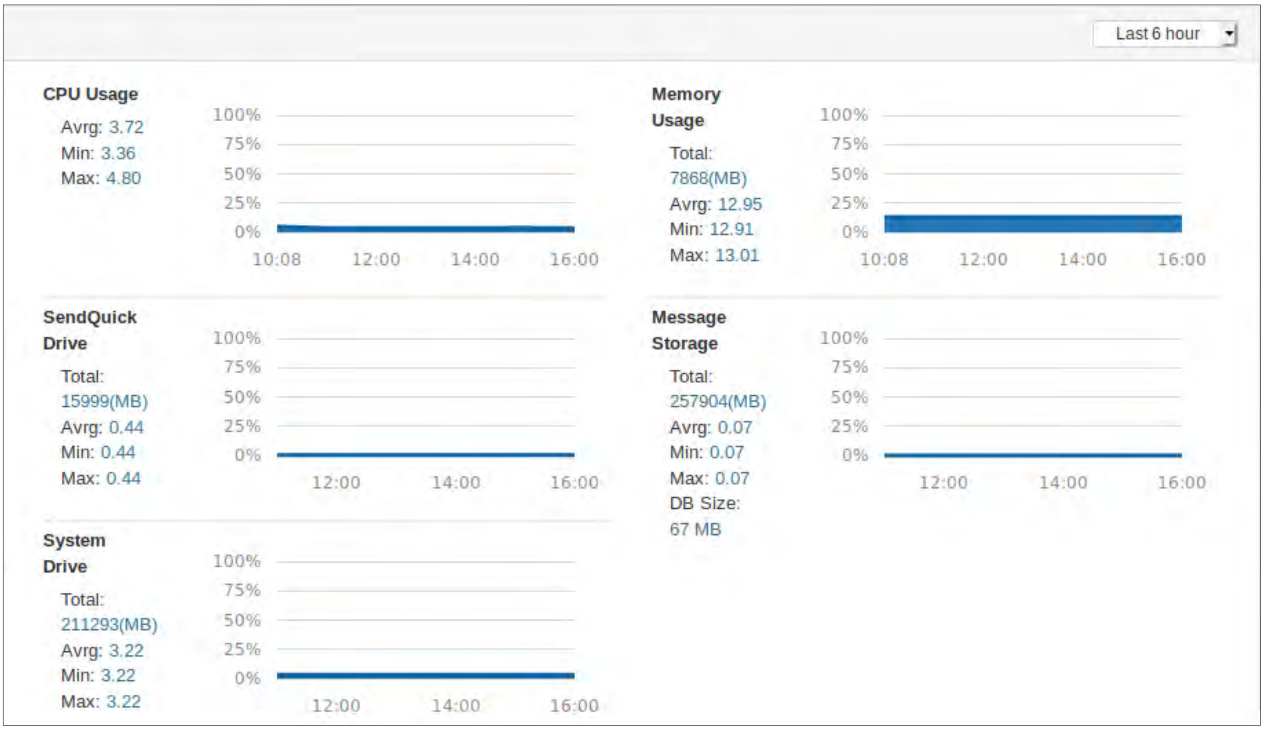
ETH0 netmask:255.255.255.0

| | | | |
|---|---|---|---|
| SMS to Email | ✓ | Email To SMS | ✓ |
| HTTP To SMS | ✓ | SFTP/FTP to SMS | ✓ |
| Web Server | ✓ | Email Server | ✓ |
| SSH | ✓ | Email Filter | ✓ |
| SNMP Trap Filter | ✓ | Syslog Filter | ✓ |

*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 are 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 Drive, Message Storage and System Drive.



CPU Usage
Avrg: 3.72
Min: 3.36
Max: 4.80

Memory Usage
Total: 7868(MB)
Avrg: 12.95
Min: 12.91
Max: 13.01

SendQuick Drive
Total: 15999(MB)
Avrg: 0.44
Min: 0.44
Max: 0.44

Message Storage
Total: 257904(MB)
Avrg: 0.07
Min: 0.07
Max: 0.07
DB Size: 67 MB

System Drive
Total: 211293(MB)
Avrg: 3.22
Min: 3.22
Max: 3.22

*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).

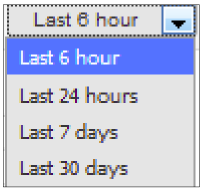
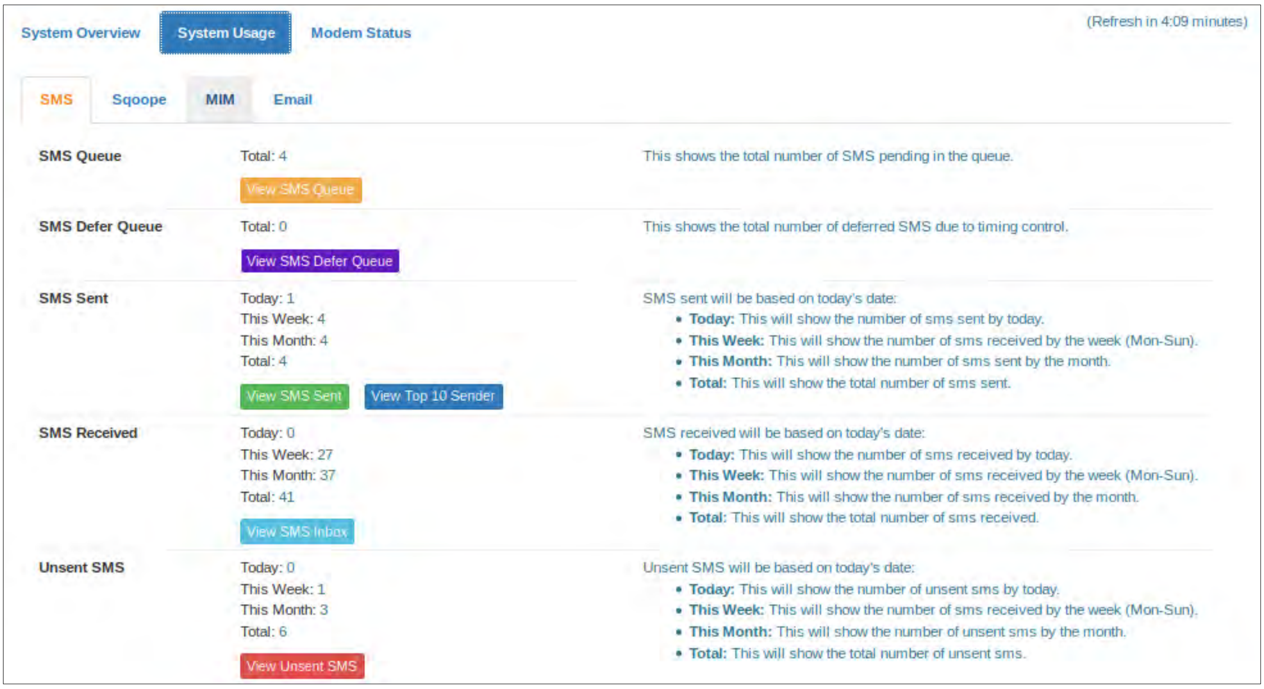


*Figure 4-3 : System Health Status Duration*

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

## 4.2 System Usage

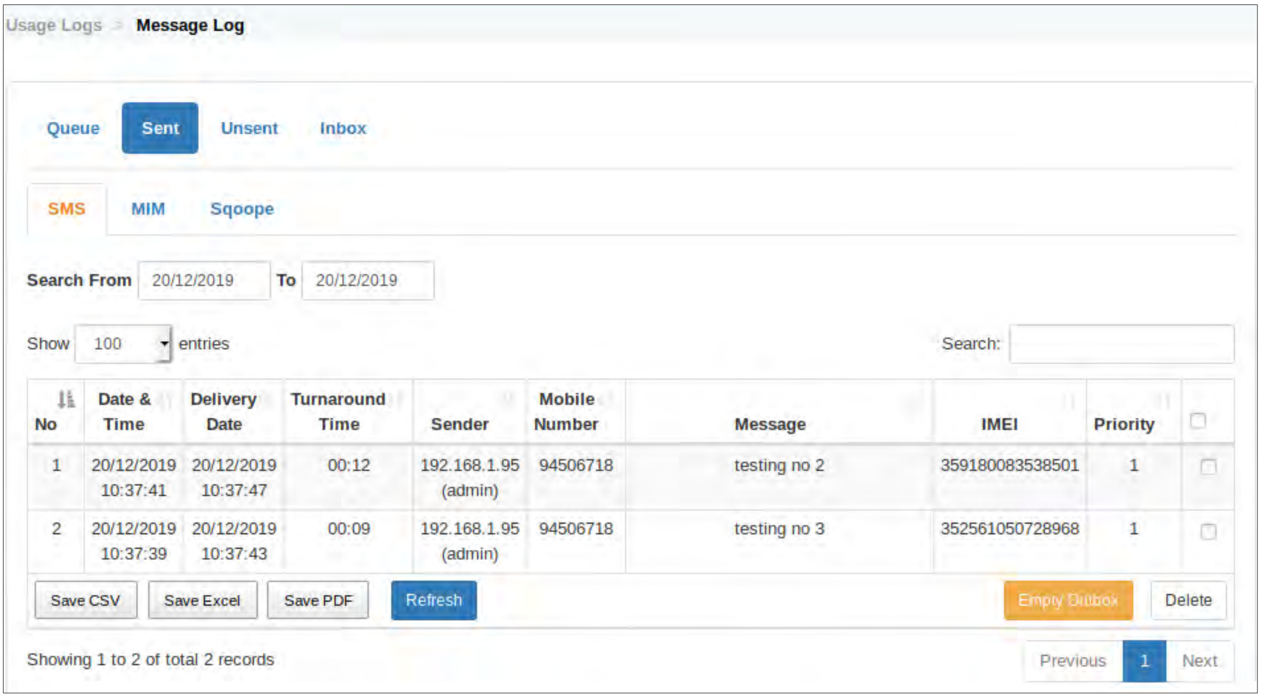
Go to **Dashboard > System Usage**. Figure 4-4 below shows the sendQuick’s System Usage in real-time. Access to the SMS, Sqoope, MIM or Email menu tabs follow-by respective ‘<Functional Color buttons>’ to view the status for SMS Queue, SMS Sent, SMS Received and Unsent SMS.



| | | |
|---|---|---|
| **SMS Queue** | Total: 4<br>View SMS Queue | This shows the total number of SMS pending in the queue. |
| **SMS Defer Queue** | Total: 0<br>View SMS Defer Queue | This shows the total number of deferred SMS due to timing control. |
| **SMS Sent** | Today: 1<br>This Week: 4<br>This Month: 4<br>Total: 4<br>View SMS Sent View Top 10 Sender | SMS sent will be based on today's date:<br>• **Today:** This will show the number of sms sent by today.<br>• **This Week:** This will show the number of sms received by the week (Mon-Sun).<br>• **This Month:** This will show the number of sms sent by the month.<br>• **Total:** This will show the total number of sms sent. |
| **SMS Received** | Today: 0<br>This Week: 27<br>This Month: 37<br>Total: 41<br>View SMS Inbox | SMS received will be based on today's date:<br>• **Today:** This will show the number of sms received by today.<br>• **This Week:** This will show the number of sms received by the week (Mon-Sun).<br>• **This Month:** This will show the number of sms received by the month.<br>• **Total:** This will show the total number of sms received. |
| **Unsent SMS** | Today: 0<br>This Week: 1<br>This Month: 3<br>Total: 6<br>View Unsent SMS | Unsent SMS will be based on today's date:<br>• **Today:** This will show the number of unsent sms by today.<br>• **This Week:** This will show the number of sms received by the week (Mon-Sun).<br>• **This Month:** This will show the number of unsent sms by the month.<br>• **Total:** This will show the total number of 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).



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

Show 100 entries Search:

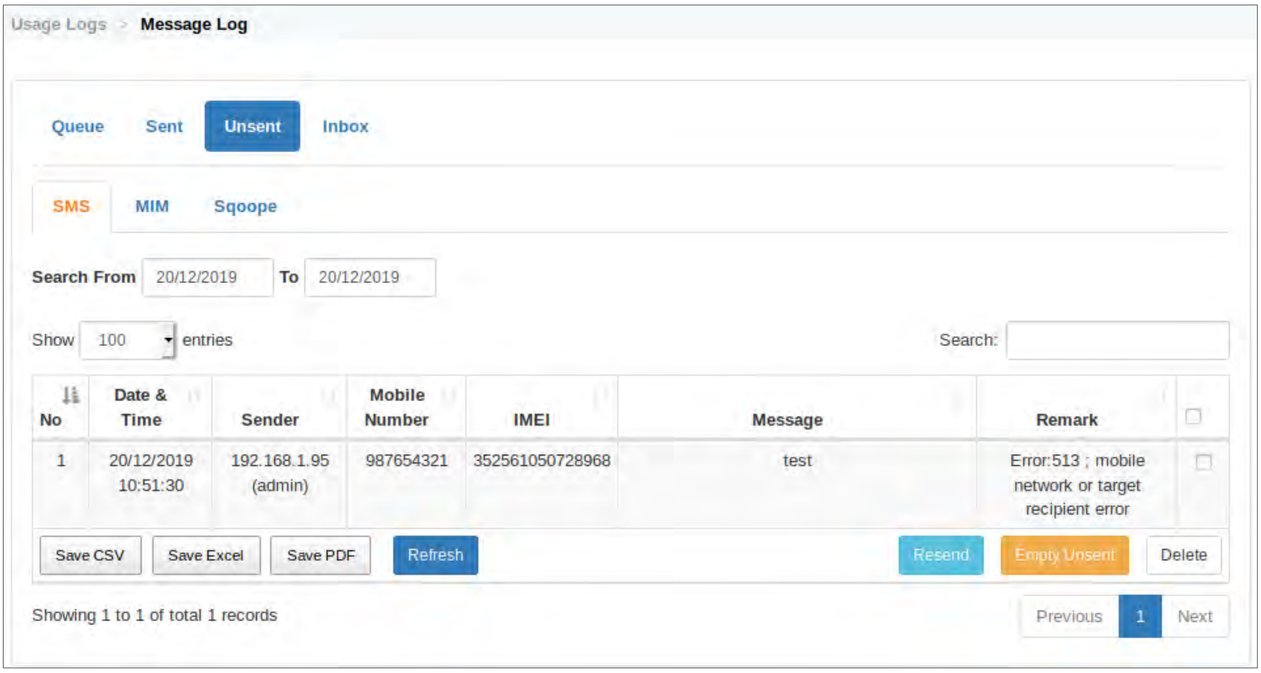
| No | Date & Time | Delivery Date | Turnaround Time | Sender | Mobile Number | Message | IMEI | Priority | □ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 20/12/2019 10:37:41 | 20/12/2019 10:37:47 | 00:12 | 192.168.1.95 (admin) | 94506718 | testing no 2 | 359180083538501 | 1 | □ |
| 2 | 20/12/2019 10:37:39 | 20/12/2019 10:37:43 | 00:09 | 192.168.1.95 (admin) | 94506718 | testing no 3 | 352561050728968 | 1 | □ |

Showing 1 to 2 of total 2 records

*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.



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 | □ |

Showing 1 to 1 of total 1 records

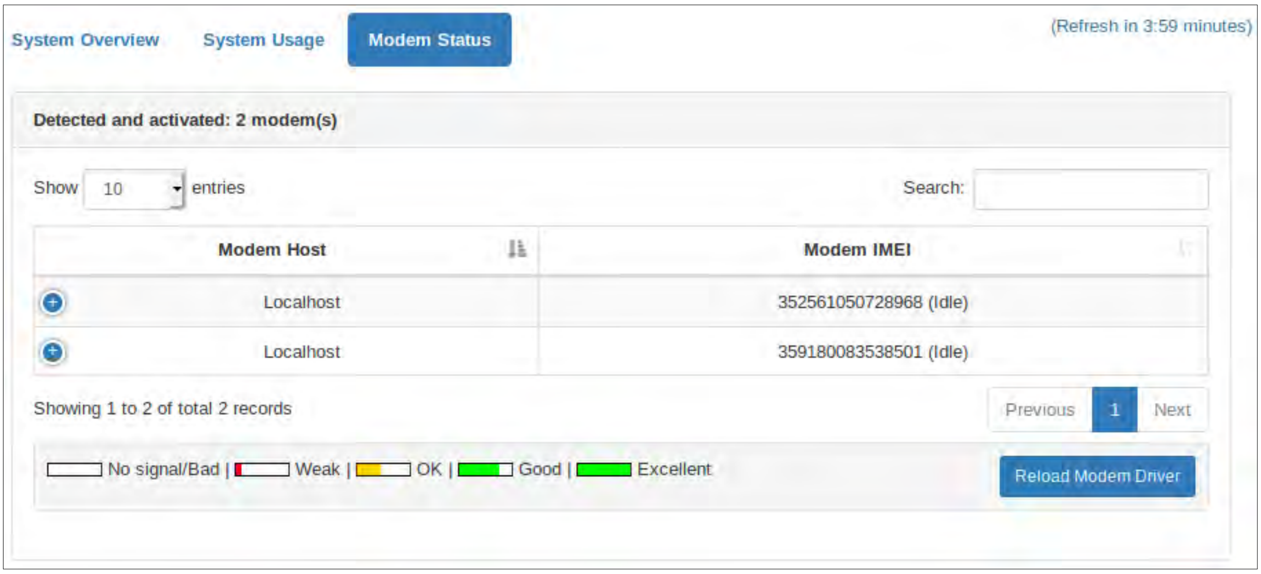
*Figure 4-6 : System Usage – unsent – SMS*

On the Remark column, system will highlight the possible cause of the error when sending of sms has failed. 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.

## 4.3 Modem Status

Go to **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.



Detected and activated: 2 modem(s)

| Modem Host | Modem IMEI |
|---|---|
| Localhost | 352561050728968 (Idle) |
| Localhost | 359180083538501 (Idle) |

Showing 1 to 2 of total 2 records

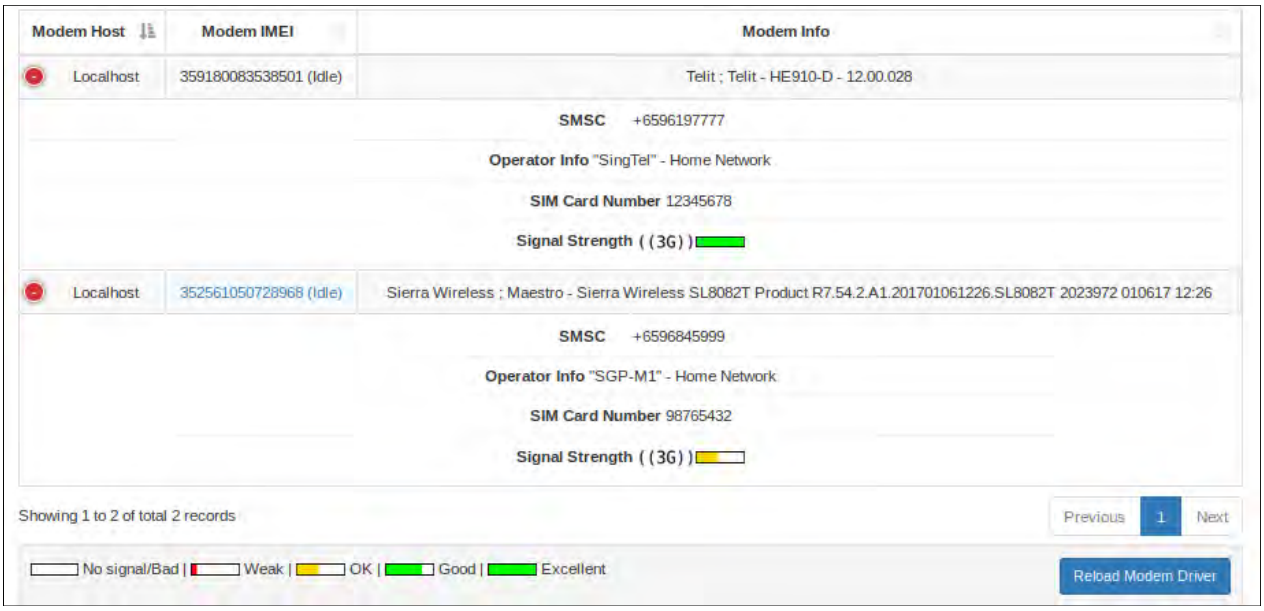
□ No signal/Bad | 🟥 Weak | 🟨 OK | 🟩 Good | 🟩 Excellent

*Figure 4-7 : Modem Status – Overview*

Select the '**<Blue> +**' sign 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.



| Modem Host | Modem IMEI | Modem Info |
|---|---|---|
| Localhost | 359180083538501 (Idle) | Telit ; Telit - HE910-D - 12.00.028 |
| | | **SMSC** +6596197777<br>**Operator Info** "SingTel" - Home Network<br>**SIM Card Number** 12345678<br>**Signal Strength** ((3G)) 🟩 |
| Localhost | 352561050728968 (Idle) | Sierra Wireless ; Maestro - Sierra Wireless SL8082T Product R7.54.2.A1.201701061226.SL8082T 2023972 010617 12:26 |
| | | **SMSC** +6596845999<br>**Operator Info** "SGP-M1" - Home Network<br>**SIM Card Number** 98765432<br>**Signal Strength** ((3G)) 🟨 |

Showing 1 to 2 of total 2 records

□ No signal/Bad | 🟥 Weak | 🟨 OK | 🟩 Good | 🟩 Excellent

Figure 4-8 : Modem Status - detail

## 4.4 Menu Items

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**
Prepare and configure the server to connect to the network in a proper manner

b) **Messaging Setup**
Configure the system for sending and receiving messages, as well as to interface with external application for receiving SMS messages

c) **Modem Setup**
View the modem status, configure the modem configuration and routing information

d) **Phone Book & Roster**
Create roster of shifts and phone book for filter rules usage

e) **Filter Rules**
Perform the filter configuration (Email/SNMP Trap/Syslog) for selective SMS messaging based on configured rules

f) **Network Monitor**
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**
Configure permissions 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**
Backup and restore the configuration settings as well as generating diagnostic file

j) **Usage Logs**
View 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

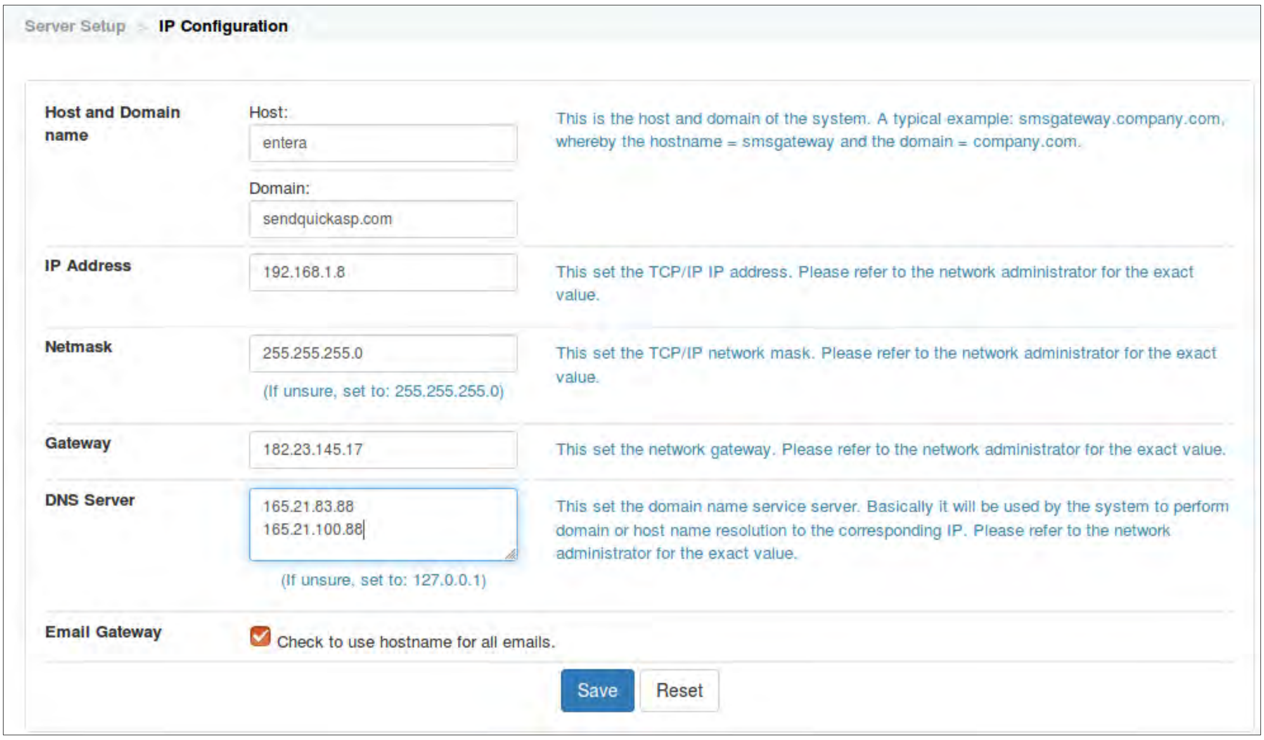
l) **SMS Specifications**
These are the specifications and format to send messages to sendQuick server.

# 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: entera<br>Domain: sendquickasp.com | This is the host and domain of the system. A typical example: smsgateway.company.com, whereby the hostname = smsgateway and the domain = company.com. |
| **IP Address** | 192.168.1.8 | This set the TCP/IP IP address. Please refer to the network administrator for the exact value. |
| **Netmask** | 255.255.255.0<br>(If unsure, set to: 255.255.255.0) | This set the TCP/IP network mask. Please refer to the network administrator for the exact value. |
| **Gateway** | 182.23.145.17 | This set the network gateway. Please refer to the network administrator for the exact value. |
| **DNS Server** | 165.21.83.88<br>165.21.100.88<br>(If unsure, set to: 127.0.0.1) | 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. |
| **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.

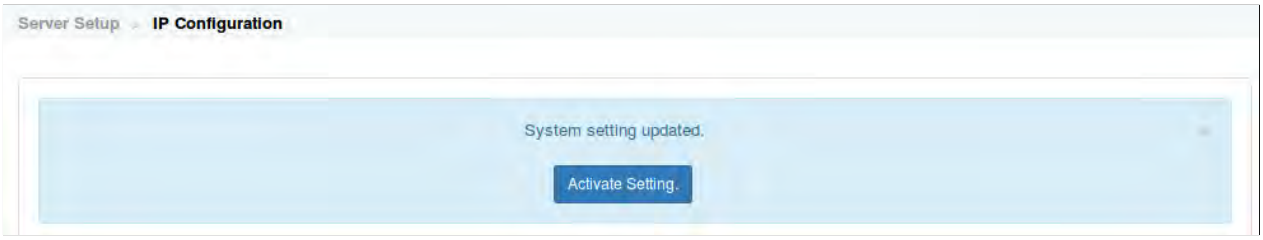
c) **Netmask**
This is the subnet mask value of the network. This defines the network that you are connected to. Most networks use 255.255.255.0, which is also the default value in the system.

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 yet. 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.



System setting updated.

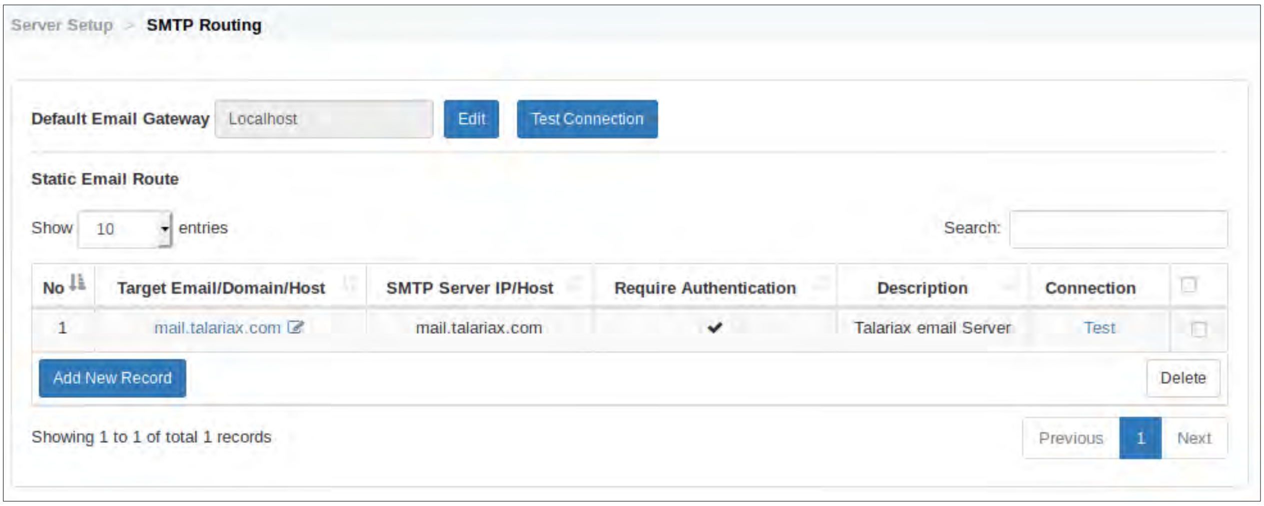
*Figure 5-2 : Activate Setting*

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>. 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



Server Setup > **SMTP Routing**

**Default Email Gateway** Localhost

**Static Email Route**

Show 10 entries Search:

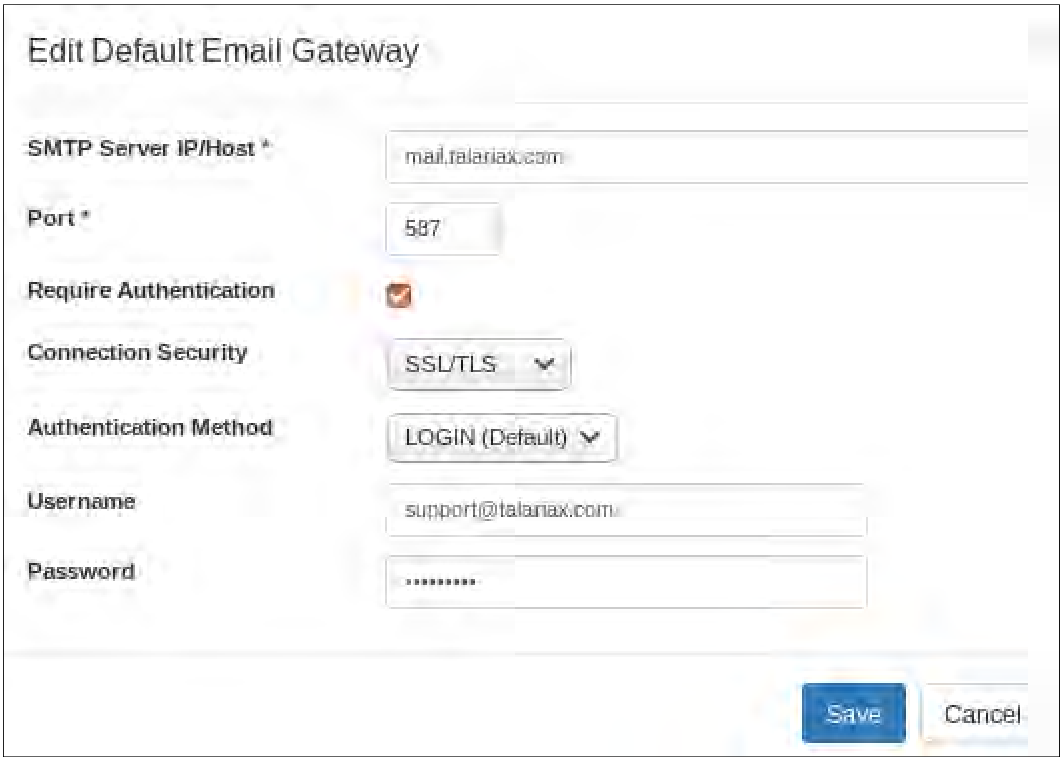
| No | Target Email/Domain/Host | SMTP Server IP/Host | Require Authentication | Description | Connection | □ |
|---|---|---|---|---|---|---|
| 1 | mail.talariax.com | mail.talariax.com | ✓ | Talariax email Server | Test | □ |

Showing 1 to 1 of total 1 records

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:



Edit Default Email Gateway

| | |
|---|---|
| SMTP Server IP/Host * | mail.talariax.com |
| Port * | 587 |
| Require Authentication | ☑ |
| Connection Security | SSL/TLS |
| Authentication Method | LOGIN (Default) |
| Username | support@talariax.com |
| Password | •••••••••• |

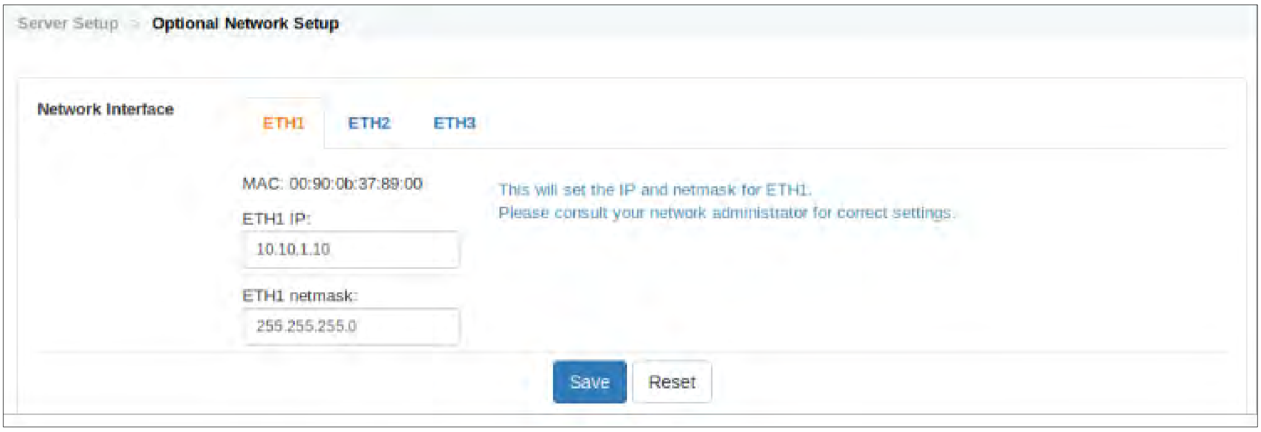
Figure 5-4 : SMTP Default Email Gateway

- **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)



Network Interface

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

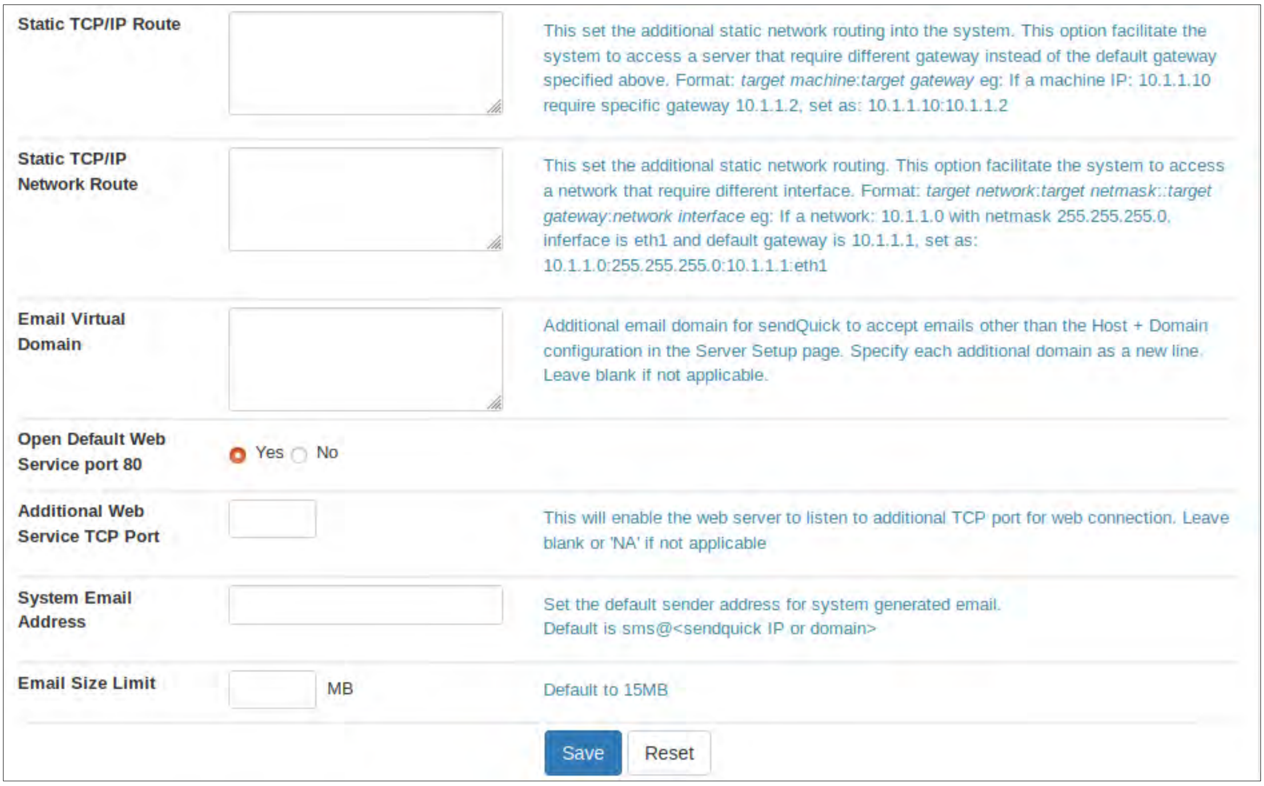
ETH1 IP: 10.10.1.10

ETH1 netmask: 255.255.255.0

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, inferface 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.<br>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>*

Example:
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*>

  Example:
  If a network: 10.1.1.0 with netmask 255.255.255.0, inferface 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.

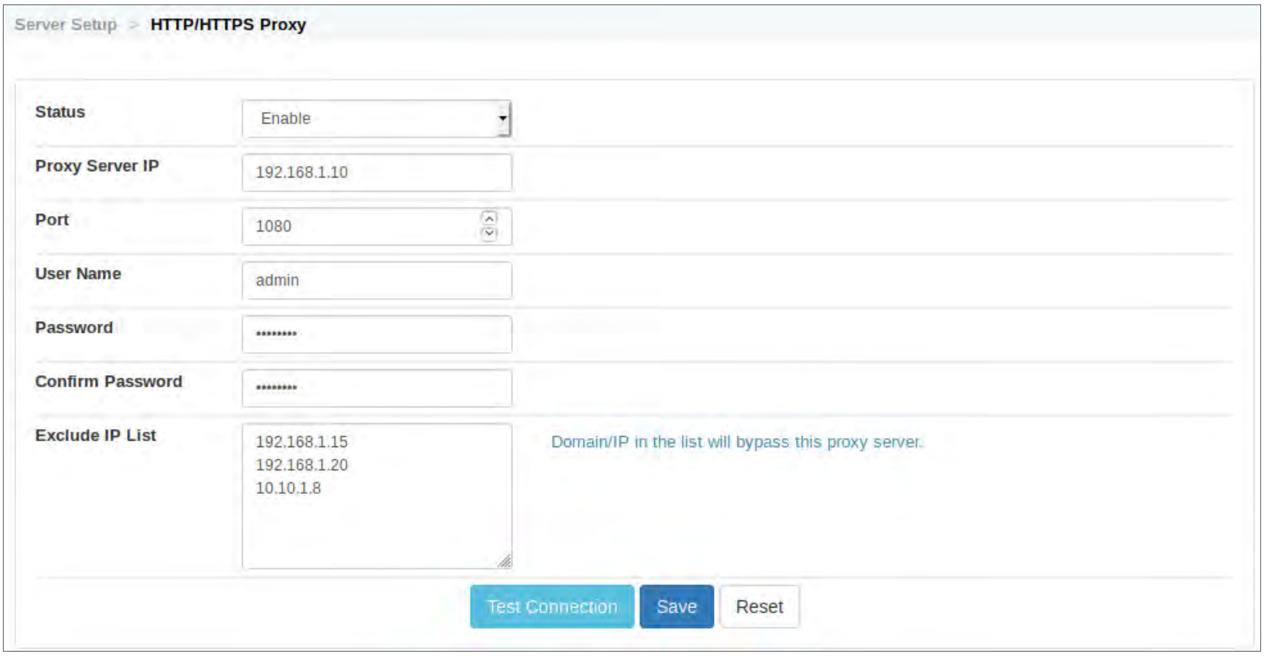
This is an optional item (contact your distributor or TalariaX for pricing) and is only available for selected models;

- **sendQuick Alert Plus**
- **sendQuick Entera**
- **sendQuick Conexa**
- **sendQuick Avera**.

A step-by-step approach is documented in section 18 High Availability Configuration 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<br>192.168.1.20<br>10.10.1.8 |

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

*Figure 5-7 : HTTP/HTTPS Proxy Setup*

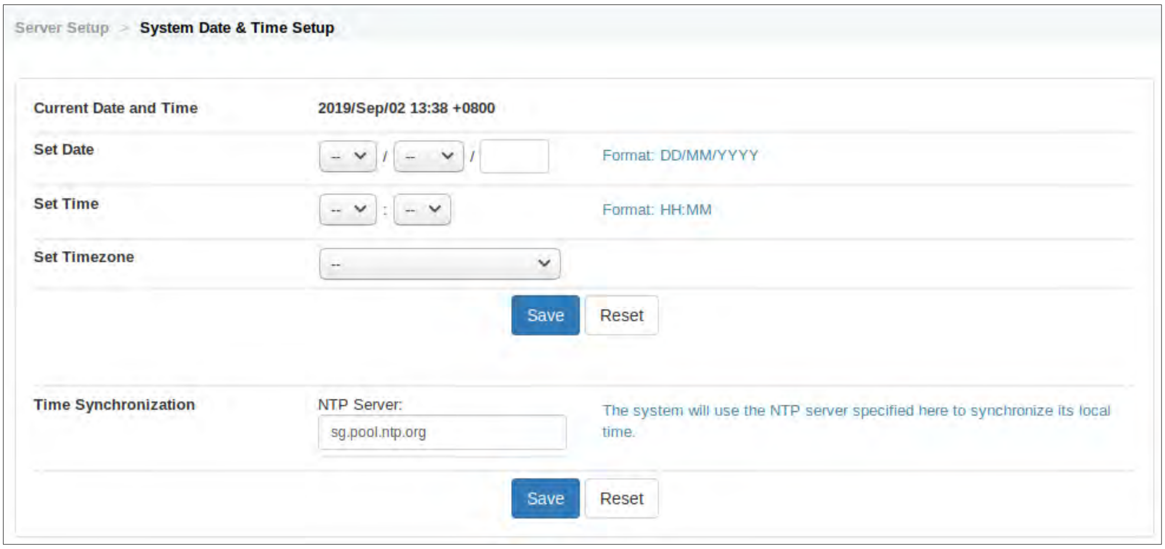
The available parameters on HTTP/HPPTS Proxy setup screen are:

- 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.



Server Setup > System Date & Time Setup

Current Date and Time: 2019/Sep/02 13:38 +0800

Set Date: -- / -- / Format: DD/MM/YYYY

Set Time: -- : -- Format: HH:MM

Set Timezone: --

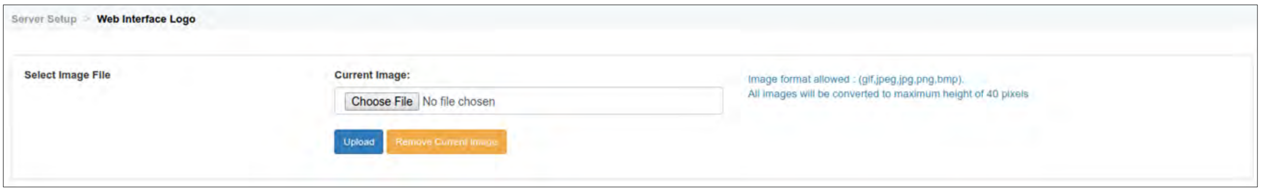
Time Synchronization: NTP Server: sg.pool.ntp.org

The system will use the NTP server specified here to synchronize its local time.

*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.



Server Setup > Web Interface Logo

Select Image File

Current Image:

Choose File No file chosen

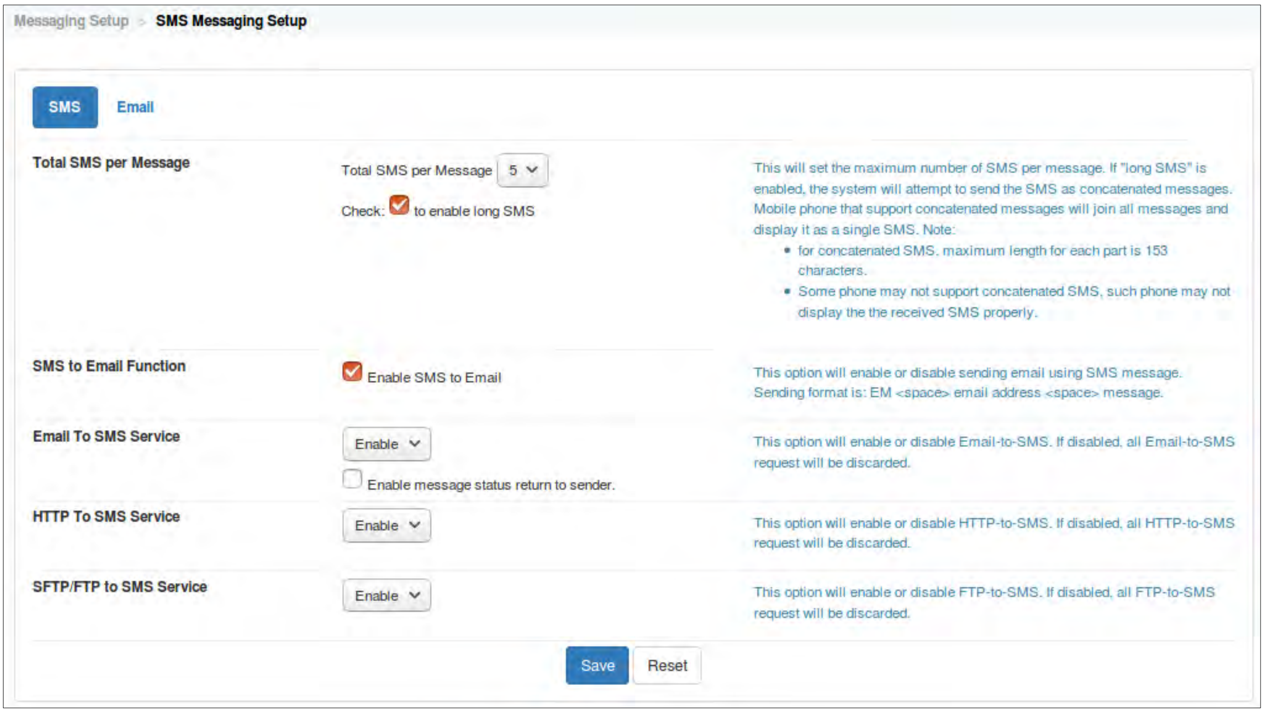
Image format allowed : (gif,jpeg,jpg,png,bmp).
All images will be converted to maximum height of 40 pixels

*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. Two main functions to be configured are the SMS and the Email Pattern settings:

## 6.1 SMS Messaging Setup - SMS



**Total SMS per Message**

Total SMS per Message 5

Check: ☑ to enable long SMS

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.

**SMS to Email Function**

☑ Enable SMS to Email

This option will enable or disable sending email using SMS message. Sending format is: EM <space> email address <space> message.

**Email To SMS Service**

Enable

□ Enable message status return to sender.

This option will enable or disable Email-to-SMS. If disabled, all Email-to-SMS request will be discarded.

**HTTP To SMS Service**

Enable

This option will enable or disable HTTP-to-SMS. If disabled, all HTTP-to-SMS request will be discarded.

**SFTP/FTP to SMS Service**

Enable

This option will enable or disable FTP-to-SMS. If disabled, all FTP-to-SMS request will be discarded.

*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 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.

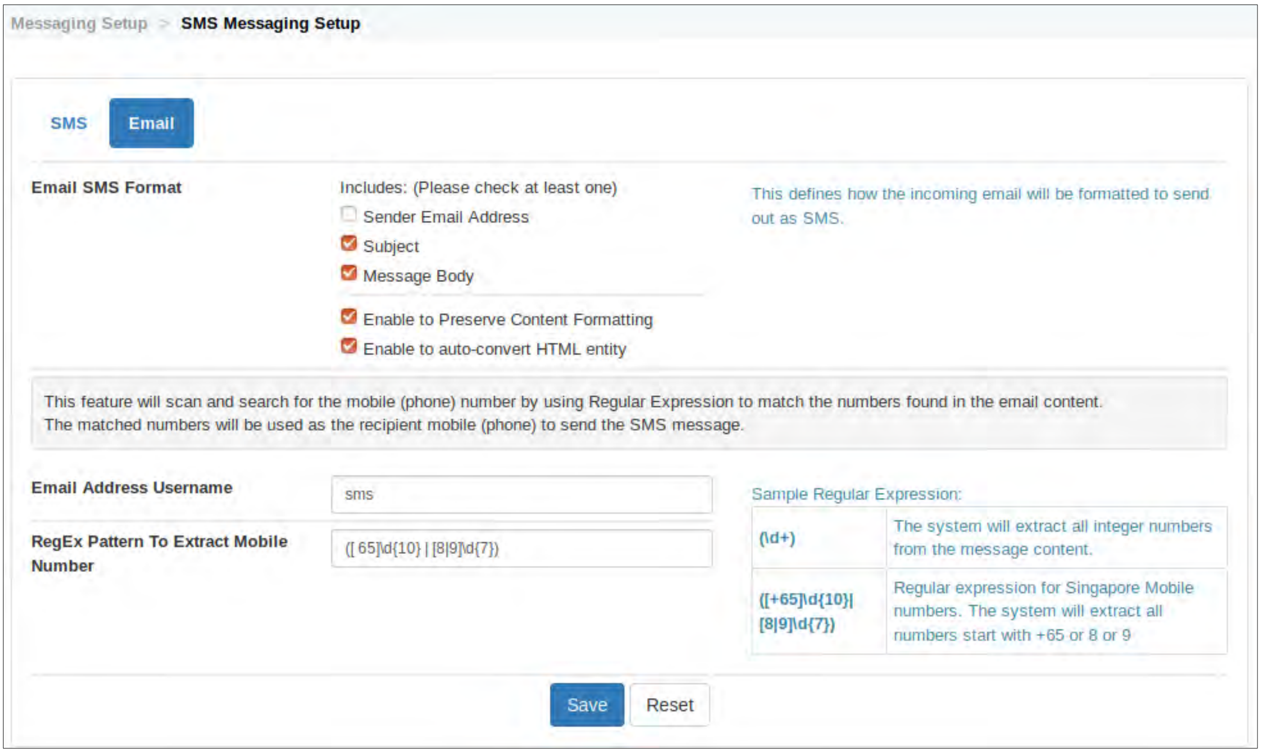
c) **Email to SMS Service.** The function can be enabled or disabled, If its disabled, all email send too SMS request will be discarded.
**Enable message status return to sender**, if user require the status of email SMS to be auto response to sender, please select the checkbox to enable this function.

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 disable, all FTP to SMS request will be disabled.

## 6.2 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.



**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** | sms |
| **RegEx Pattern To Extract Mobile Number** | ([ 65]\d{10} \| [8\|9]\d{7}) |

Sample Regular Expression:

| | |
|---|---|
| **(\d+)** | The system will extract all integer numbers from the message content. |
| **([+65]\d{10}\|[8\|9]\d{7})** | Regular expression for Singapore Mobile numbers. The system will extract all numbers start with +65 or 8 or 9 |

*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 corresponding function.

For the field, **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:

✓ **8**1234567
✓ **9**1234567
✓ **65**81234567
✓ **65**91234567

## 6.3 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.

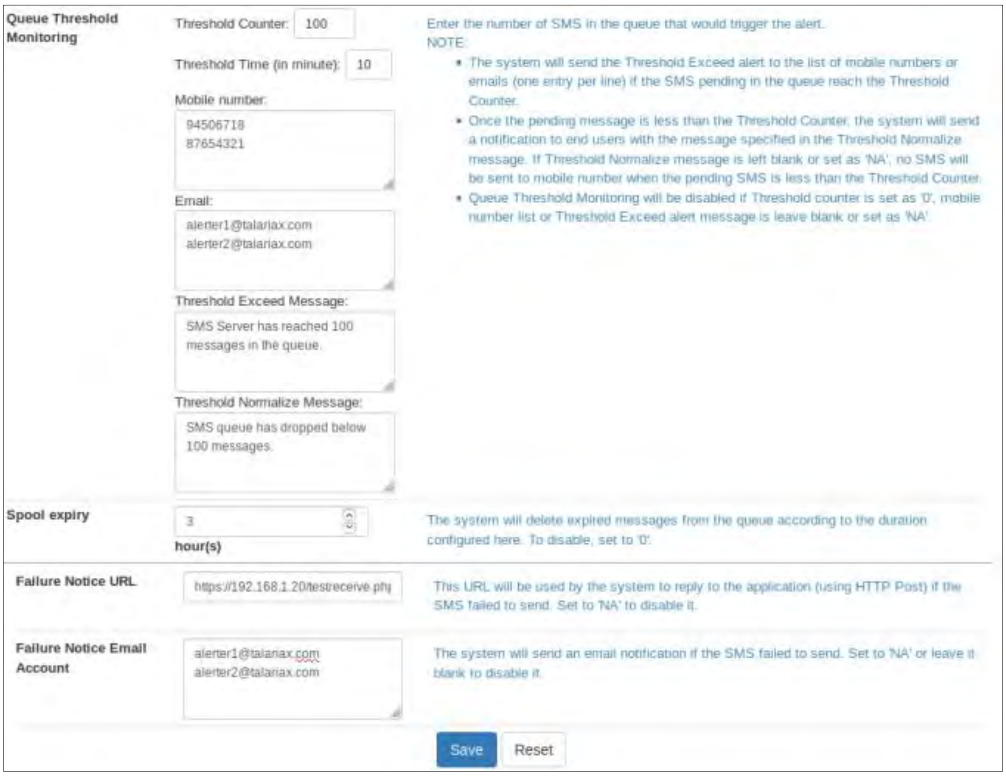
d) **Threshold Exceed Message**
The system will send a notification to administrator with the message specified in the Threshold Exceed Message. If Threshold Exceel Message is left blank or set as 'NA', no SMS will be sent to mobile number when the pending SMS is reached the Threshold Counter.

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 alerter(s) when there is a modem failure or SMS Failure. Set to 'NA' or leave it blank to disable it.



**Queue Threshold Monitoring**

Threshold Counter: 100

Threshold Time (in minute): 10

Mobile number:
94506718
87654321

Email:
alerter1@talariax.com
alerter2@talariax.com

Threshold Exceed Message:
SMS Server has reached 100 messages in the queue.

Threshold Normalize Message:
SMS queue has dropped below 100 messages.

Enter the number of SMS in the queue that would trigger the alert.
NOTE:

- 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'.

**Spool expiry** 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** https://192.168.1.20/testreceive.phj 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**
alerter1@talariax.com
alerter2@talariax.com

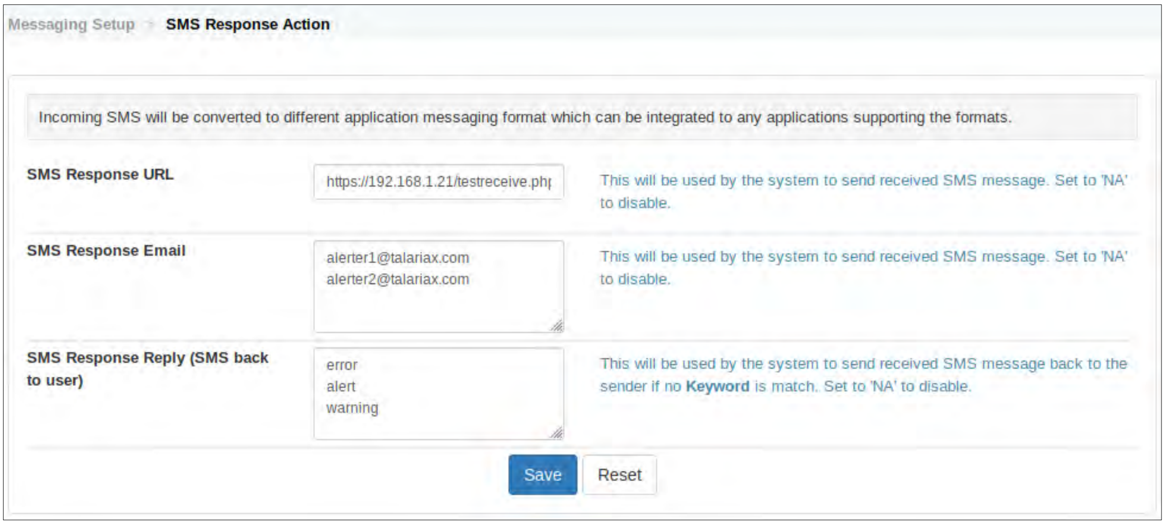
The system will send an email notification if the SMS failed to send. Set to 'NA' or leave it blank to disable it.

*Figure 6-3 : SMS Queue Monitoring*

## 6.4 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.



Incoming SMS will be converted to different application messaging format which can be integrated to any applications supporting the formats.

**SMS Response URL** https://192.168.1.21/testreceive.phj 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

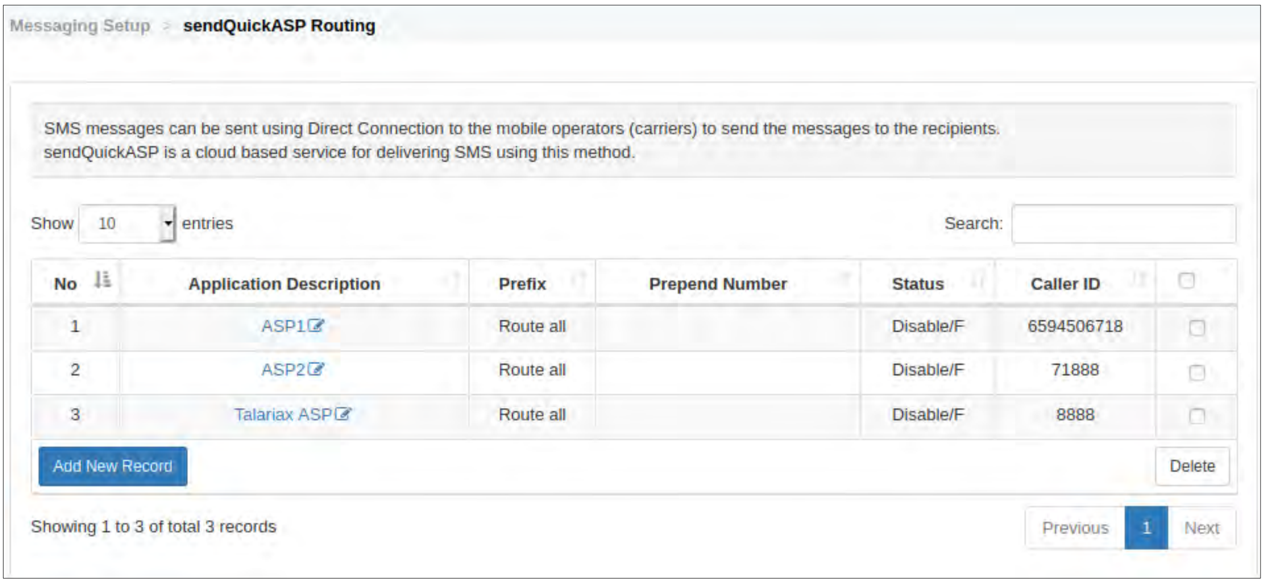
This will be used by the system to send received SMS message back to the sender if no **Keyword** is match. Set to 'NA' to disable.

*Figure 6-4 : SMS Response Action*

## 6.5 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 > sendQuickASP 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.

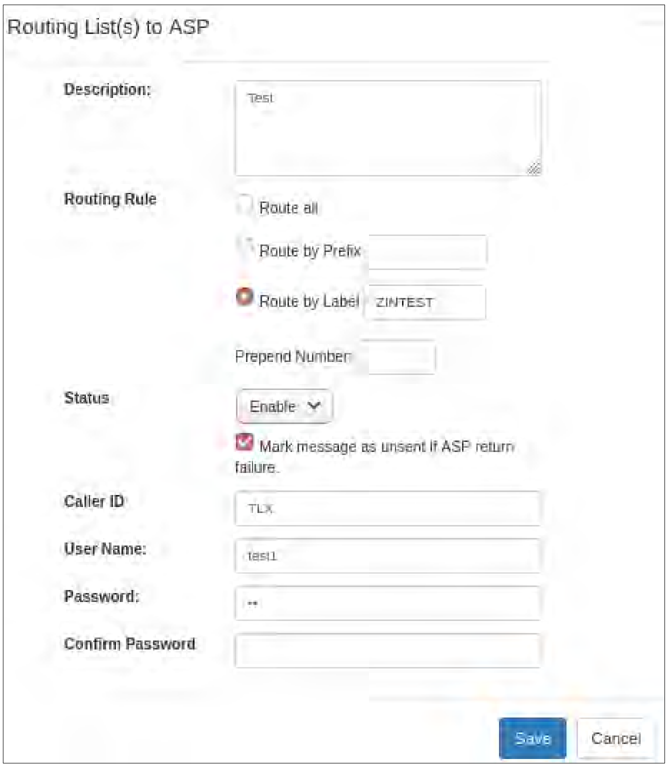
Show 10 entries Search:

| No | Application Description | Prefix | Prepend Number | Status | Caller ID | □ |
|---|---|---|---|---|---|---|
| 1 | ASP1 | Route all | | Disable/F | 6594506718 | □ |
| 2 | ASP2 | Route all | | Disable/F | 71888 | □ |
| 3 | Talariax ASP | Route all | | Disable/F | 8888 | □ |

Showing 1 to 3 of total 3 records

*Figure 6-5 : sendQuickASP Routing Configuration Screen*

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



Routing List(s) to ASP

| | |
|---|---|
| Description: | Test |
| Routing Rule | ○ Route all<br>○ Route by Prefix<br>● Route by Label ZINTEST<br>Prepend Number |
| Status | Enable<br>☑ Mark message as unsent if ASP return failure. |
| Caller ID | TLX |
| User Name: | test1 |
| Password: | ** |
| Confirm Password | |

*Figure 6-6 : sendQuickASP Routing Configuration Detail Popup*

Fill up the required information and click on **Save** button to create this newly created route.

**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 (For example: 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.

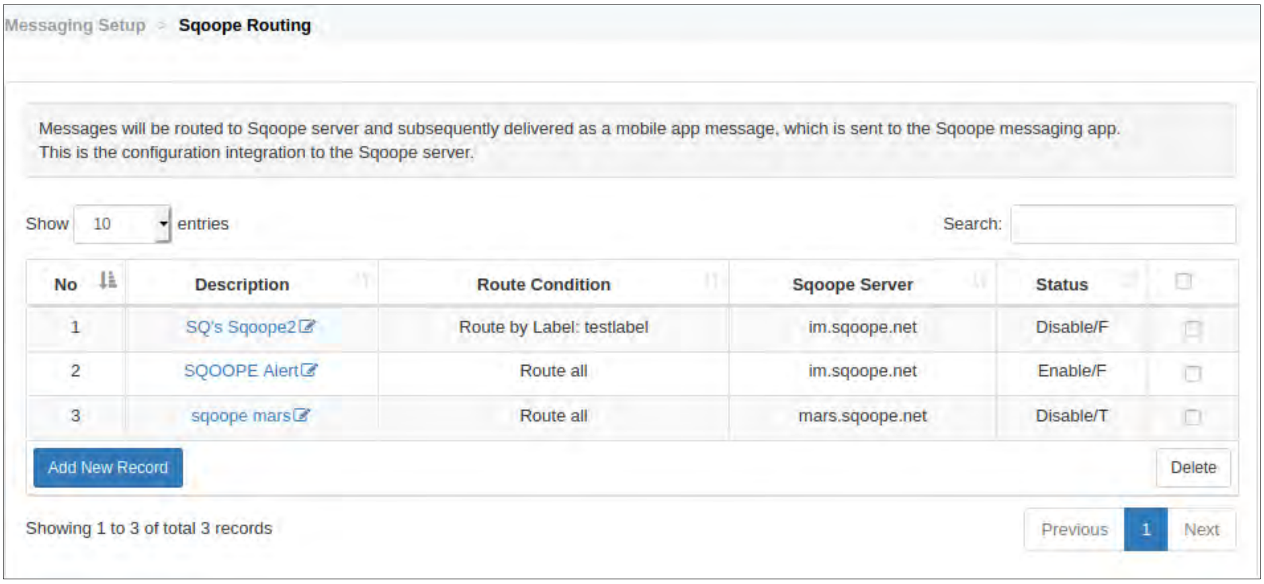
**Status**: To enable or to disable this routing rule.

**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.

## 6.6 Sqoope Routing

Sqoope is a Mobile Messaging App designed for sendQuick appliances. Sqoope allows for secure, private and confidential messaging service within an organisation. Having Sqoope and sendQuick working together, allow companies to send messages via Sqoope as well as sendQuick (SMS) to achieve a multi-channel messaging strategy. 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 on the mobile devices (Android and iOS supported). This is the configuration settings to integrate to the Sqoope server. To find out more regarding Sqoope, please contact your distributor or TalariaX.



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 | □ |
| 2 | SQOOPE Alert | Route all | im.sqoope.net | Enable/F | □ |
| 3 | sqoope mars | Route all | mars.sqoope.net | Disable/T | □ |

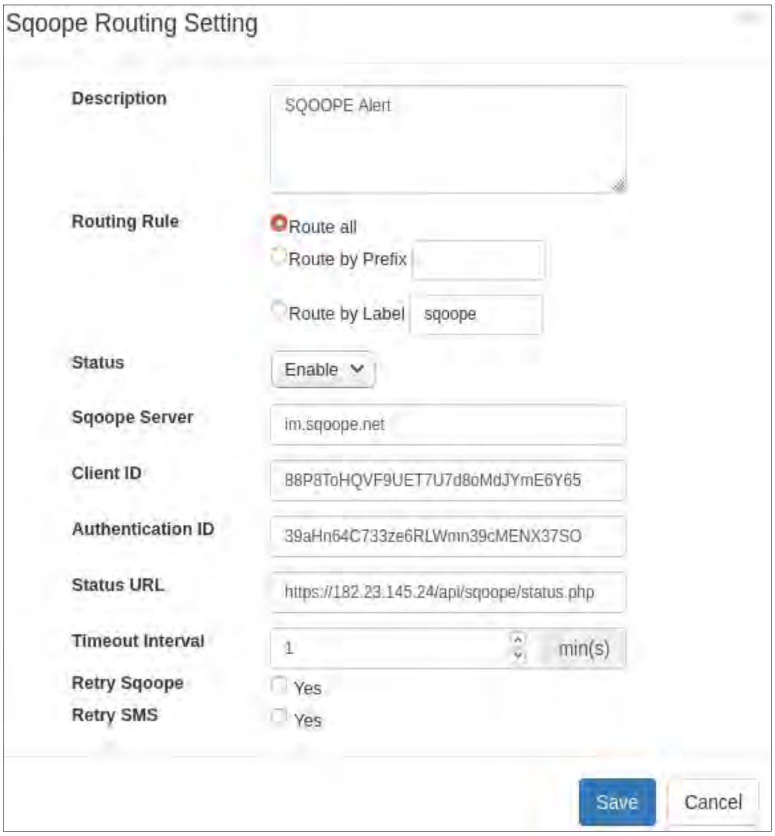
Showing 1 to 3 of total 3 records

*Figure 6-7 : Sqoope Routing Configuration*

**Access to Menu > Messaging Setup > Sqoope Routing** for configuration (Figure 6-7):

Select **Add New Record** and Figure 6-8: Sqoope routing configuration detail popup screen will be shown.

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



Sqoope Routing Setting

| | |
|---|---|
| Description | SQOOPE Alert |
| Routing Rule | ● Route all<br>○ Route by Prefix<br>○ Route by Label sqoope |
| Status | Enable |
| Sqoope Server | im.sqoope.net |
| Client ID | 88P8ToHQVF9UET7U7d8oMdJYmE6Y65 |
| Authentication ID | 39aHn64C733ze6RLWmn39cMENX37SO |
| Status URL | https://182.23.145.24/api/sqoope/status.php |
| Timeout Interval | 1 min(s) |
| Retry Sqoope | □ Yes |
| Retry SMS | □ Yes |

*Figure 6-8 : 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 a predefined Modem Label e.g. 'marketing' and 'operations', the modem label that you had configured on **Modem Setup > Modem Routing** section.

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

**Sqoope Server**: The registered domain name of the Sqoope Server.

**Client ID:** Enter the Client ID ( provided by Sqoope)

**Authentication ID**: Enter the Authentication ID (provided by Sqoope)

**Status URL**: URL path to Sqoope server.

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

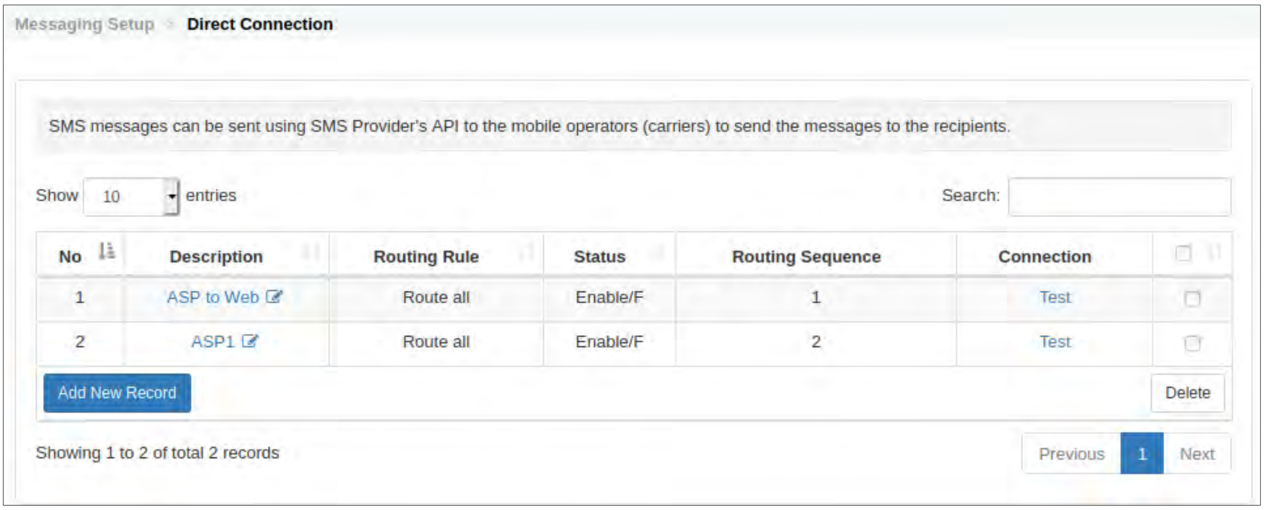
**Retry Sqoope**: Check 'Yes' if you want sendQuick to retry in event a message failed to be sent via Sqoope beyond the predefined timeout interval.

**Retry SMS**: Check 'Yes' if you want sendQuick to retry sending SMS message to user in event a message failed to be sent via Sqoope beyond the predefined timeout interval.

## 6.7 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 of direct connection.



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.

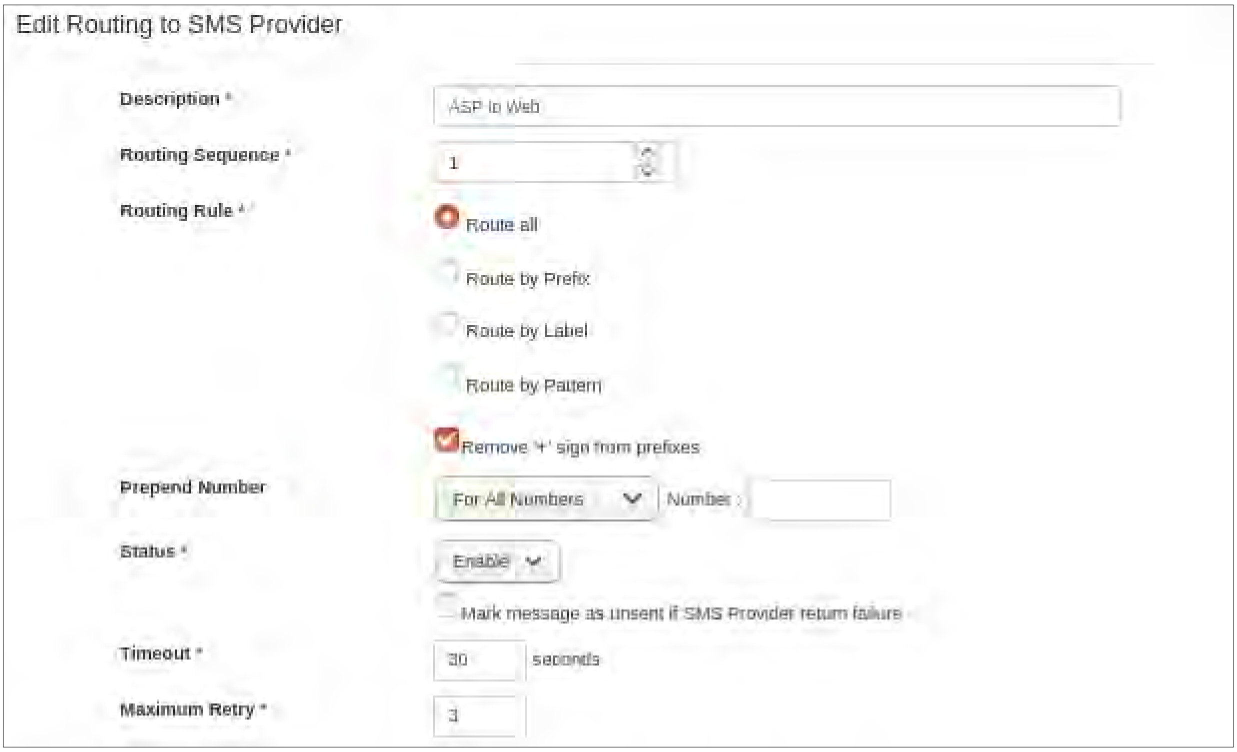
Show 10 entries Search:

| No | Description | Routing Rule | Status | Routing Sequence | Connection | □ |
|---|---|---|---|---|---|---|
| 1 | ASP to Web | Route all | Enable/F | 1 | Test | □ |
| 2 | ASP1 | Route all | Enable/F | 2 | Test | □ |

Showing 1 to 2 of total 2 records

*Figure 6-9 : Direct connection configuration screen*

Select **Add New Record** and Figure 6:10 : Direct connection configuration detail popup screen will be shown.



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

☑ Remove '+' sign from prefixes

Prepend Number : For All Numbers Number :

Status * : Enable

□ Mark message as unsent if SMS Provider return failure

Timeout * : 30 seconds

Maximum Retry * : 3

*Figure 6-10 : Direct connection configuration detail popup screen*

Fill up the required information and click on **Save** button to create this newly created route.

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

**Routing Sequence:** Default is 1, this is only 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 a predefined Modem Label e.g. '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})', this is 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 require 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 disable this service.

**Timeout**: Default as 30 seconds.

**Maximum Retry**: Default as 3 times.

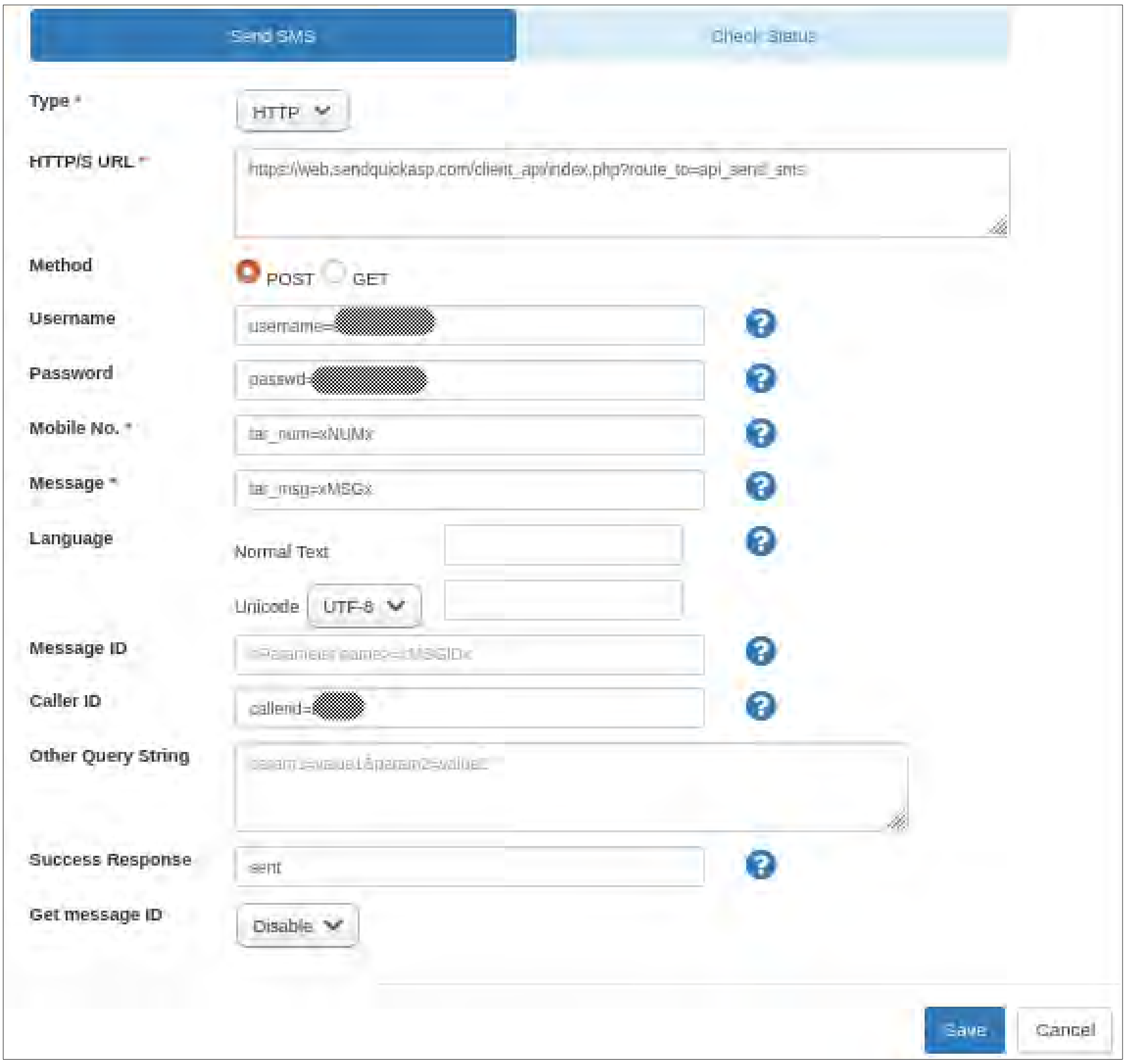
**Provider**: Select 'Others'.

Direct connection configuration detail popup screen (Figure 6-10) consist of 2 sub-functional screens which are '**Send SMS'** and '**Check Status**' for checking send sms status.

### 6.7.1 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 6-11 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.

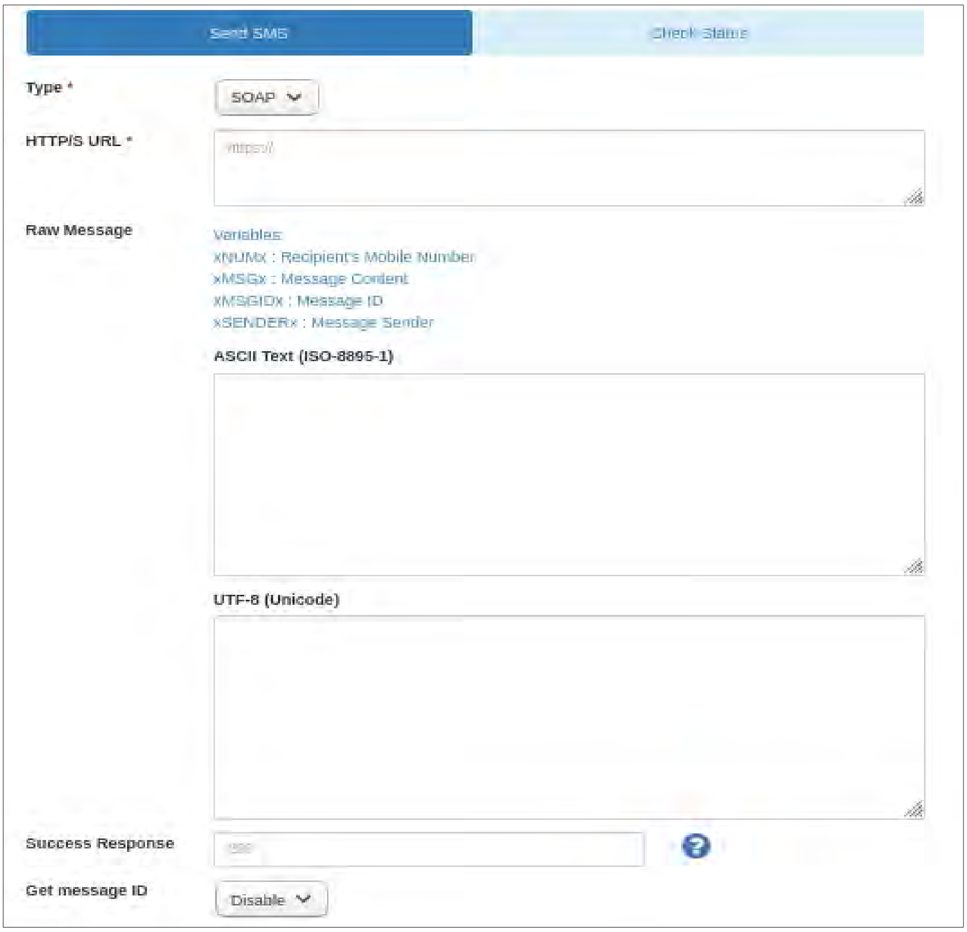


| | |
|---|---|
| Type * | HTTP |
| HTTP/S URL * | https://web.sendquickasp.com/client_api/index.php?route_to=api_send_sms |
| Method | ● POST ○ GET |
| Username | username=[redacted] |
| Password | passwd=[redacted] |
| Mobile No. * | tar_num=xNUMx |
| Message * | tar_msg=xMSGx |
| Language | Normal Text |
| | Unicode UTF-8 |
| Message ID | <Parameter name>=xMSGIDx |
| Caller ID | callerid=[redacted] |
| Other Query String | param1=value1&param2=value2 |
| Success Response | sent |
| Get message ID | Disable |

*Figure 6-11 : 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.



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)

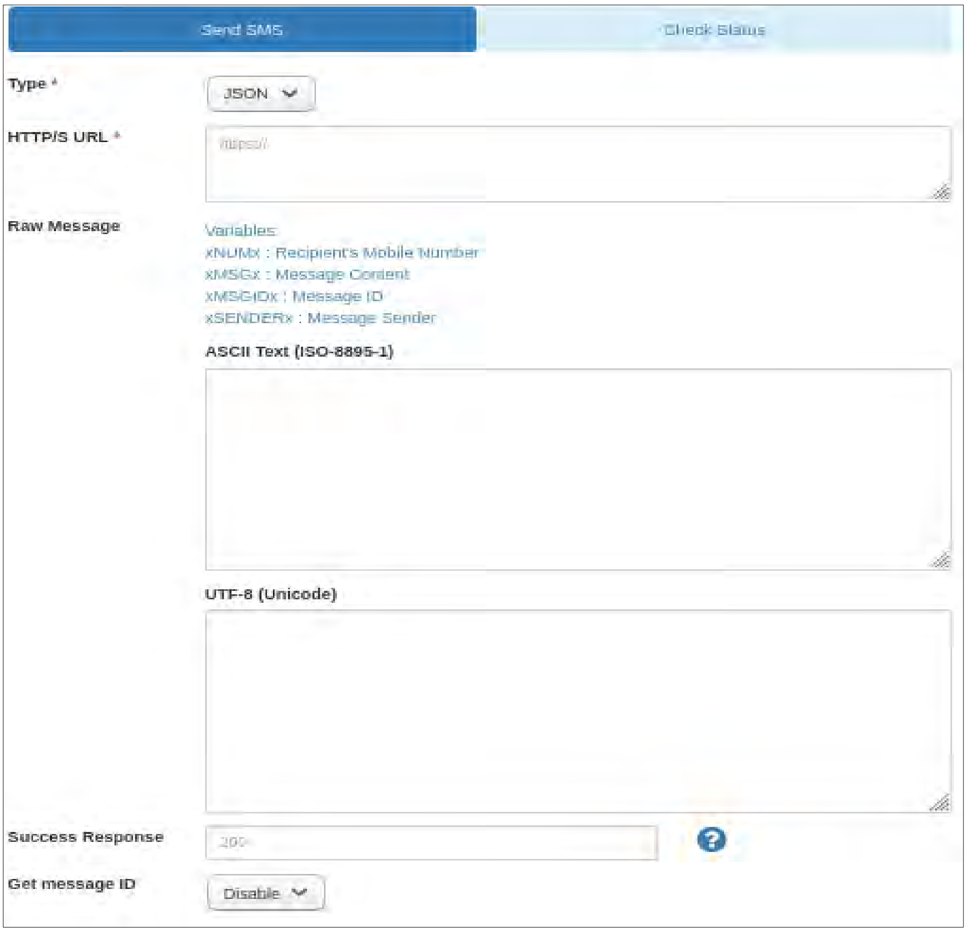
UTF-8 (Unicode)

Success Response

Get message ID Disable

*Figure 6-12 : 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.



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)

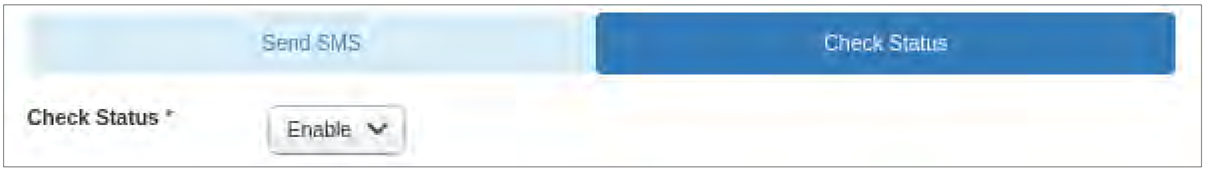
Success Response 200

Get message ID Disable

*Figure 6-13 : Direct connection configuration detail popup screen – Send SMS – JSON*

### 6.7.2 Direct Connection – Check Status (Provider = Other)

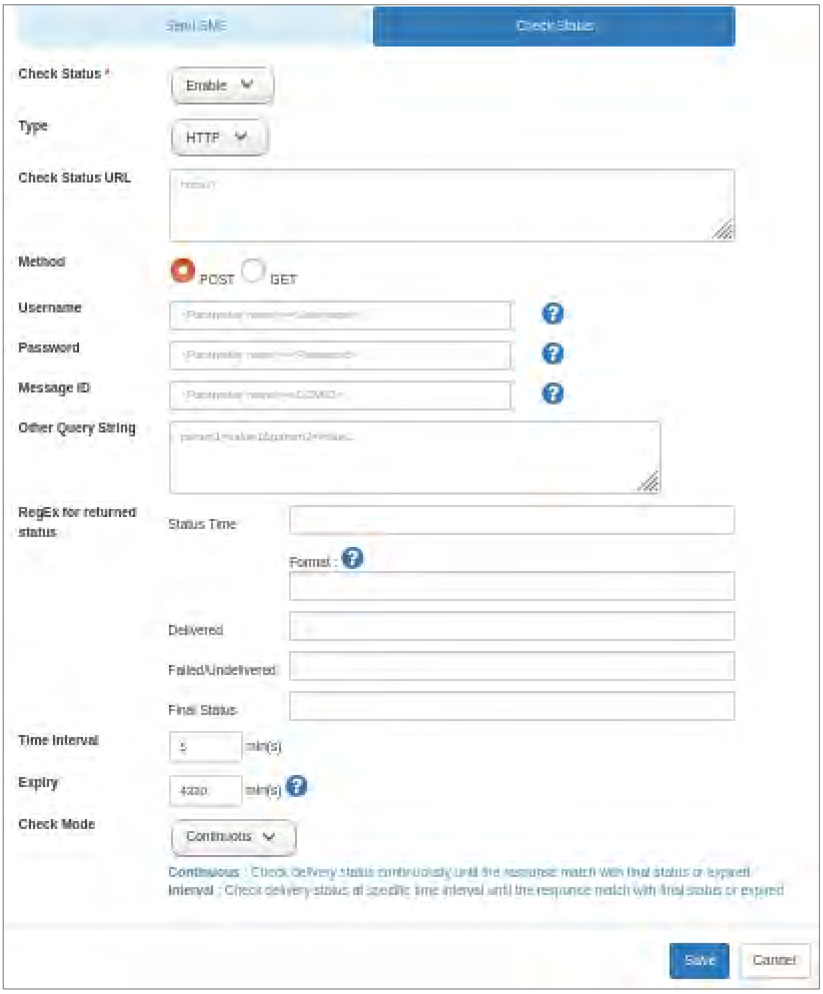
Select Check Status functional sub menu with **Status = Enable**, this function menu will allow user to configure the check SMS status for the HTTP, SOAP and JSON method.



Check Status * Enable

*Figure 6-14 : Direct connection configuration detail popup screen – Check Status – Enable*

a) When **Check Status = Enable** and the selected **Type = HTTP , 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.



Check Status * Enable

Type HTTP

Check Status URL http://

Method ● POST ○ GET

Username <Parameter name>=<Username>

Password <Parameter name>=<Password>

Message ID <Parameter name>=<MSGID>

Other Query String param1=value1&param2=value2

RegEx for returned status

Status Time

Format :

Delivered

Failed/Undelivered

Final Status

Time Interval 5 min(s)

Expiry 4320 min(s)

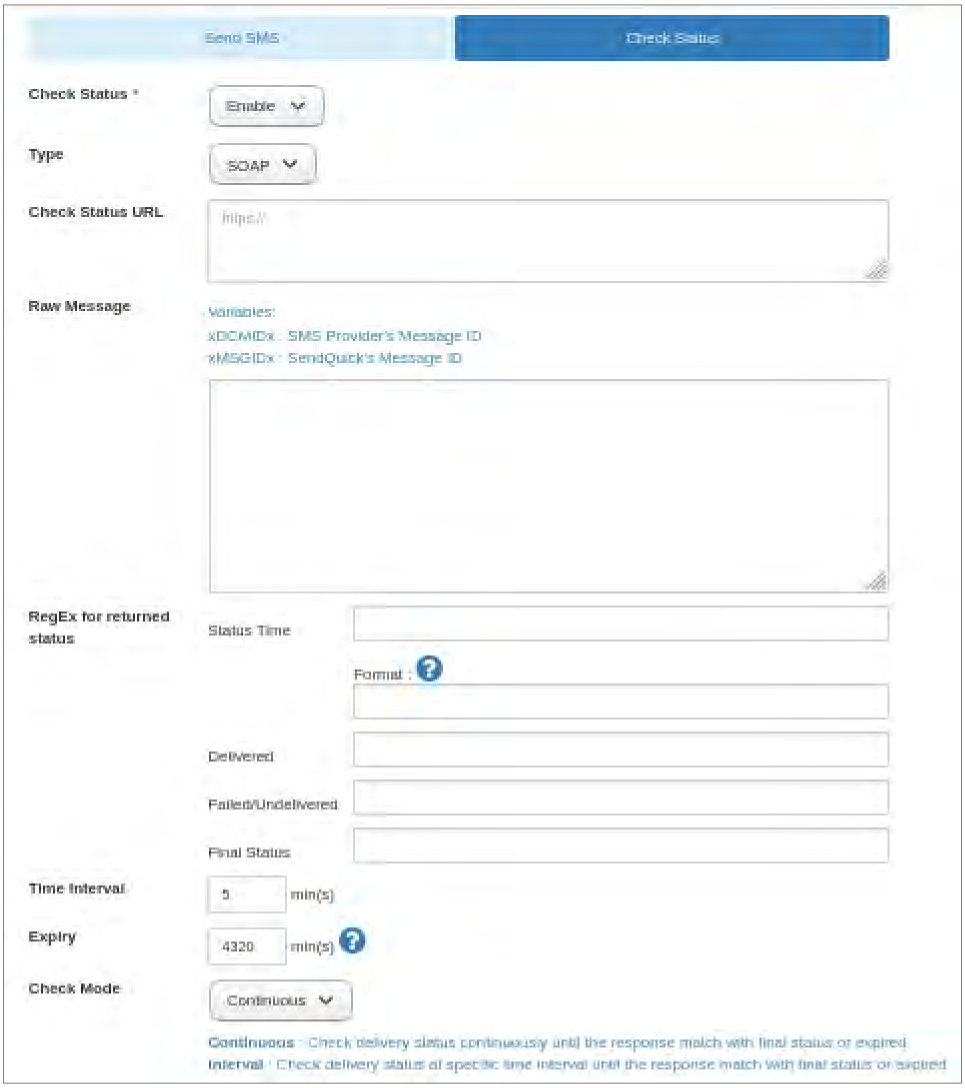
Check Mode Continuous

**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 6-15 : 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.



Check Status * : Enable

Type : SOAP

Check Status URL : https://

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 : 5 min(s)

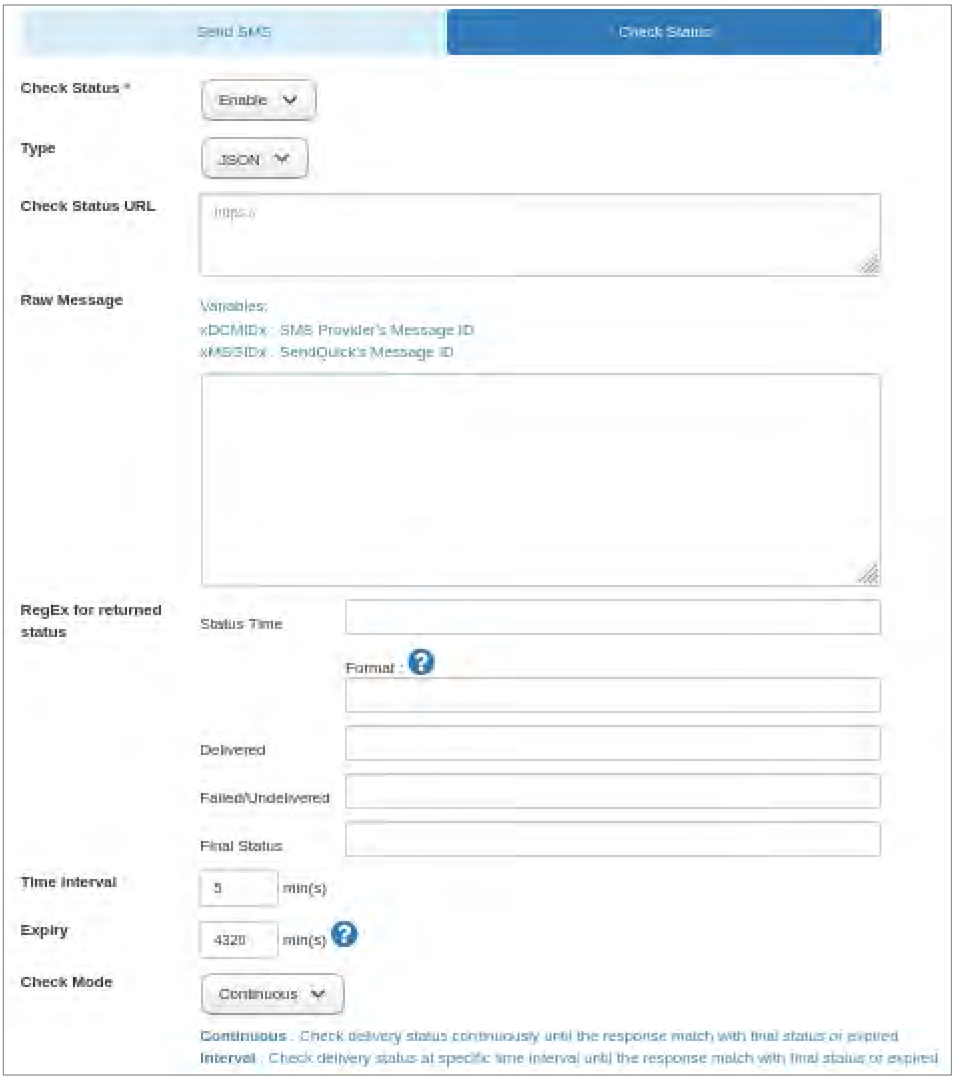
Expiry : 4320 min(s)

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 6-16 : 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.



Check Status * Enable

Type JSON

Check Status URL https://

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 5 min(s)

Expiry 4320 min(s)

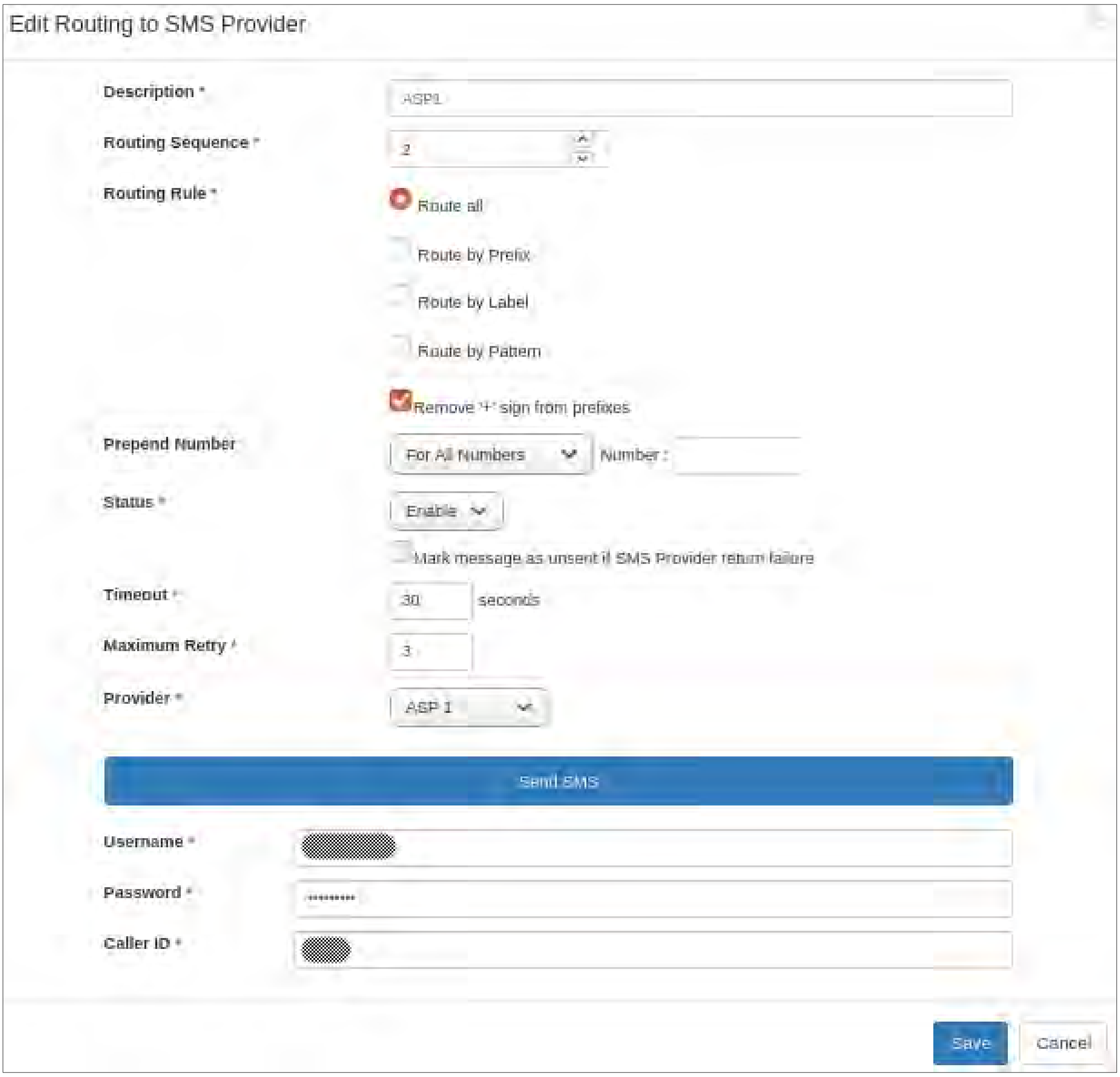
Check Mode Continuous

**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 6-17 : Direct connection configuration detail popup screen – Check Status – JSON*

### 6.7.3 Direct Connection – Send SMS (Provider = ASP)

Some SMS ASP provider will provide simple direct connect that requires only the Username and Password. Select the Provider = ASP# accordingly:



Edit Routing to SMS Provider

Description * ASP1

Routing Sequence * 2

Routing Rule *
● Route all
○ Route by Prefix
○ Route by Label
○ Route by Pattern
☑ Remove '+' sign from prefixes

Prepend Number For All Numbers Number :

Status * Enable
☐ Mark message as unsent if SMS Provider return failure

Timeout * 30 seconds

Maximum Retry * 3

Provider * ASP 1

Username * [redacted]

Password * **********

Caller ID * [redacted]

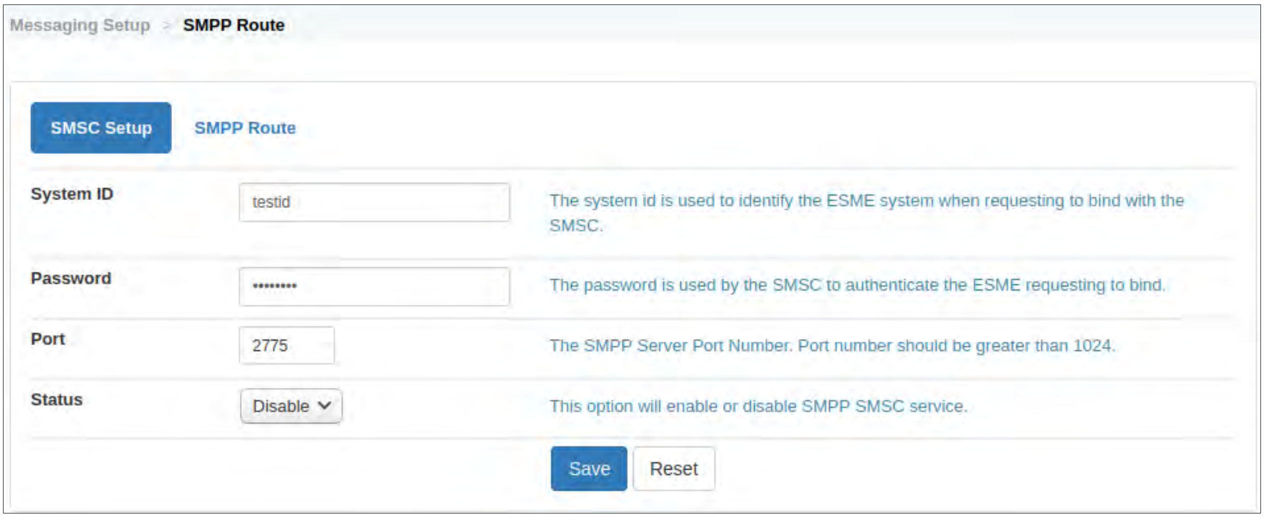
*Figure 6-18 : Direct connection – ASP*

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

## 6.8 SMPP Route

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

User is required to perform a one-time configuration for the SMSC login data.
**Access to Menu > Messaging Setup > SMSC Setup** for configuration and fill in the requested information:



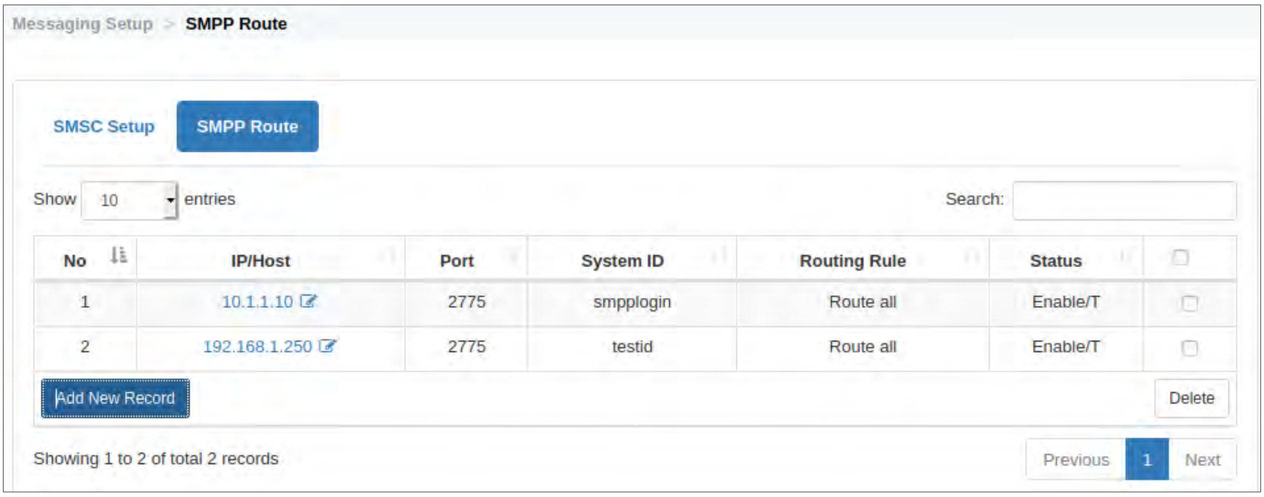
Messaging Setup > SMPP Route

| | | |
|---|---|---|
| **System ID** | testid | 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** | 2775 | The SMPP Server Port Number. Port number should be greater than 1024. |
| **Status** | Disable | This option will enable or disable SMPP SMSC service. |

*Figure 6-19 : 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.



Messaging Setup > SMPP Route

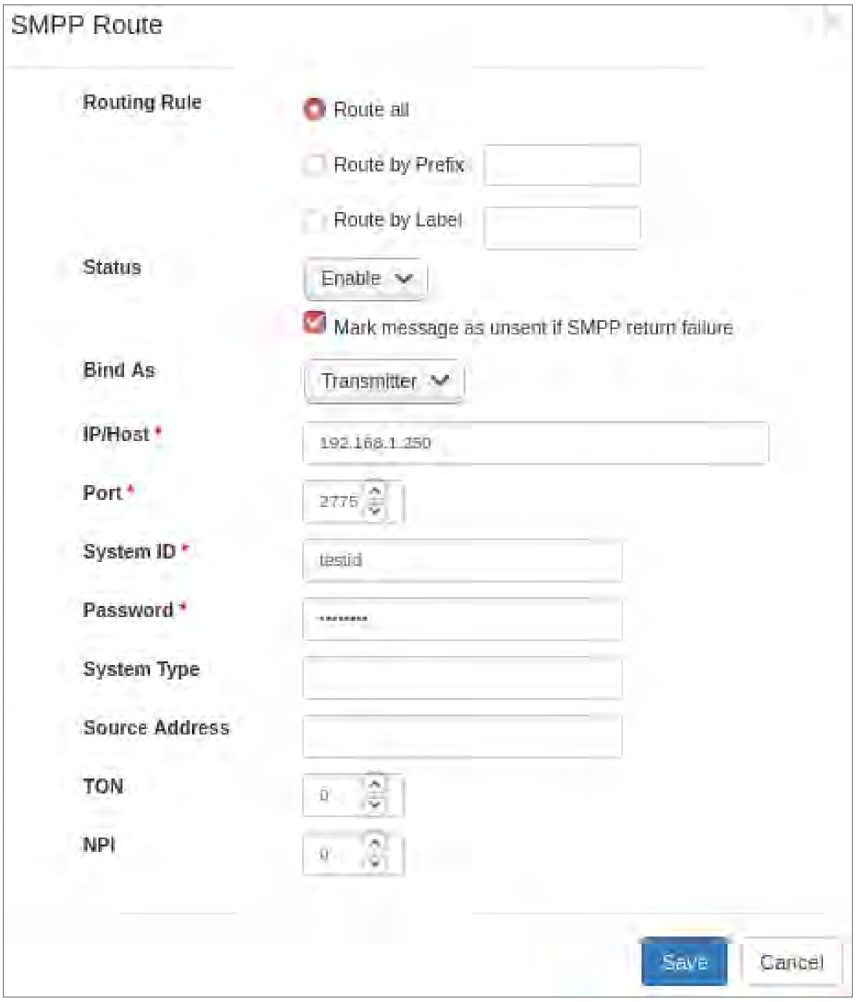
| No | IP/Host | Port | System ID | Routing Rule | Status | □ |
|---|---|---|---|---|---|---|
| 1 | 10.1.1.10 | 2775 | smpplogin | Route all | Enable/T | □ |
| 2 | 192.168.1.250 | 2775 | testid | Route all | Enable/T | □ |

Showing 1 to 2 of total 2 records

*Figure 6-20 : SMPP Route – setup*

To configure the SMPP route, **access to Menu > Messaging Setup > SMPP Route > SMPP Route**

Select **Add New Record** and the following will pop up.



SMPP Route

Routing Rule ● Route all
○ Route by Prefix
○ Route by Label

Status: Enable
☑ Mark message as unsent if SMPP return failure

Bind As: Transmitter

IP/Host *: 192.168.1.250

Port *: 2775

System ID *: testid

Password *: ********

System Type:

Source Address:

TON: 0

NPI: 0

*Figure 6-21 : SMPP Route – setup detail pop up screen*

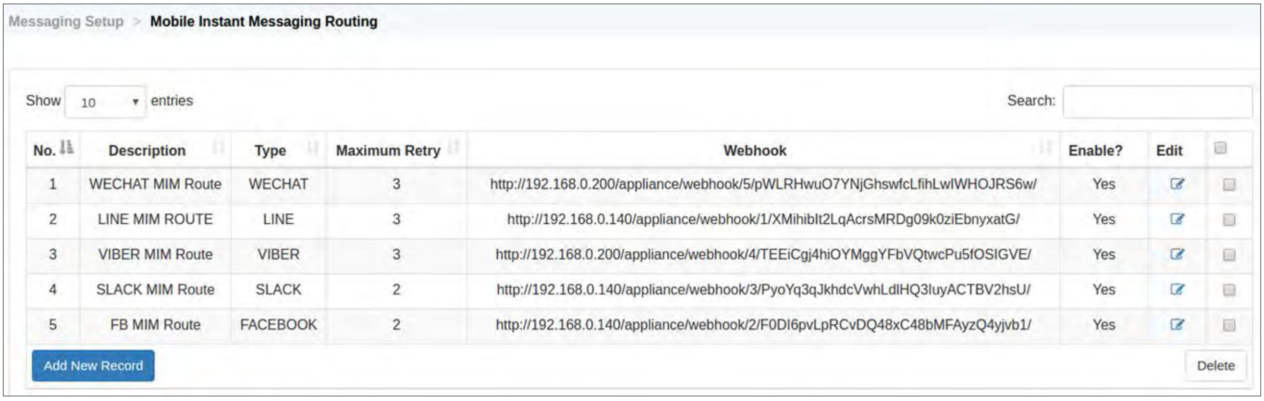
Fill in the required parameters:
**Routing Rules**: Available options are:

- **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 a predefined Modem Label say 'marketing' and 'operations', the modem label that you had configured on Modem Setup > Modem Routing section.

**Status**: To enable or temporary disable this service.
**Bind As**: Select Transmitter or Transceiver
**IP/Host**: The IP address or hostname of the SMPP server.
**Port**: The interfacing port e.g.2775.
**System ID:** Your given login id.
**Password**: 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

## 6.9 Mobile Instant Messaging Routing

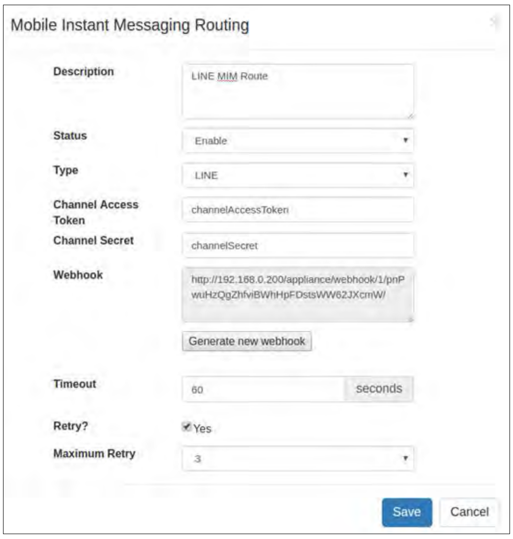
With integration of official messaging APIs provided by mobile instant messaging platforms such as Line, Facebook Messenger, Slack, Viber, WeChat, Telegram, Microsoft Teams, Webex Teams, Whatsapp, Wechat Work, Globe Labs, WhatsApp DC and Line Notify, sendQuick is now able to deliver alerts to these platforms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



| No. | Description | Type | Maximum Retry | Webhook | Enable? | Edit | □ |
|---|---|---|---|---|---|---|---|
| 1 | WECHAT MIM Route | WECHAT | 3 | http://192.168.0.200/appliance/webhook/5/pWLRHwuO7YNjGhswfcLfihLwlWHOJRS6w/ | Yes | ✎ | □ |
| 2 | LINE MIM ROUTE | LINE | 3 | http://192.168.0.140/appliance/webhook/1/XMihibIt2LqAcrsMRDg09k0ziEbnyxatG/ | Yes | ✎ | □ |
| 3 | VIBER MIM Route | VIBER | 3 | http://192.168.0.200/appliance/webhook/4/TEEiCgj4hiOYMggYFbVQtwcPu5fOSIGVE/ | Yes | ✎ | □ |
| 4 | SLACK MIM Route | SLACK | 2 | http://192.168.0.140/appliance/webhook/3/PyoYq3qJkhdcVwhLdIHQ3IuyACTBV2hsU/ | Yes | ✎ | □ |
| 5 | FB MIM Route | FACEBOOK | 2 | http://192.168.0.140/appliance/webhook/2/F0DI6pvLpRCvDQ48xC48bMFAyzQ4yjvb1/ | Yes | ✎ | □ |

Figure 6-22 : Mobile Instant Messaging Routing

Click on "**Add New Record**" and the following will pop up. 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/pnPwuHzQgZhfviBWhHpFDstsWW62JXcmW/ |
| Timeout | 60 seconds |
| Retry? | ☑ Yes |
| Maximum Retry | 3 |

Figure 6-23 : Mobile Instant Messaging Routing

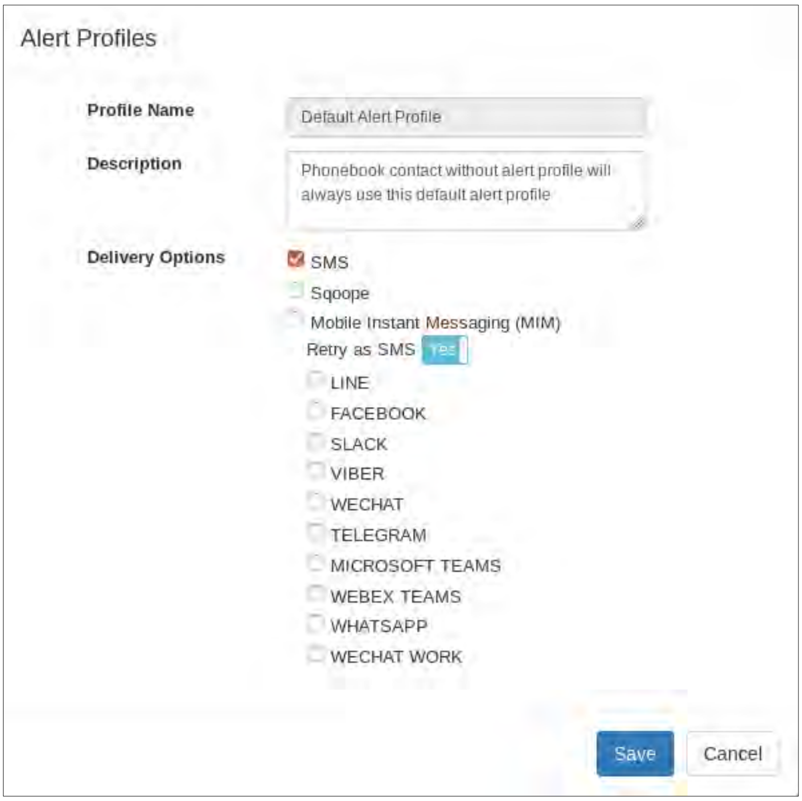
* Network administrator must ensure Webhook URL is secured by a valid SSL, public facing and accessible from Internet.

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 |

## 6.10 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 below:



Alert Profiles

Profile Name: Default Alert Profile

Description: Phonebook contact without alert profile will always use this default alert profile

Delivery Options:
- ☑ SMS
- □ Sqoope
- ○ Mobile Instant Messaging (MIM)
- Retry as SMS: Yes
  - □ LINE
  - □ FACEBOOK
  - □ SLACK
  - □ VIBER
  - □ WECHAT
  - □ TELEGRAM
  - □ MICROSOFT TEAMS
  - □ WEBEX TEAMS
  - □ WHATSAPP
  - □ WECHAT WORK

*Figure 6-24 : 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.

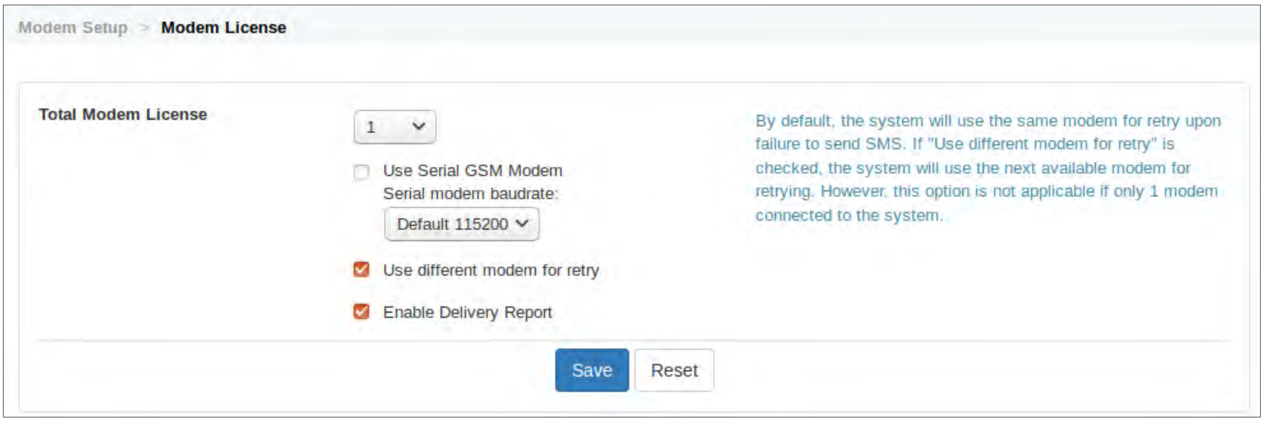
# 7.0 Modem Setup

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.



Total Modem License: 1

□ Use Serial GSM Modem
Serial modem baudrate: Default 115200

☑ Use different modem for retry

☑ Enable Delivery Report

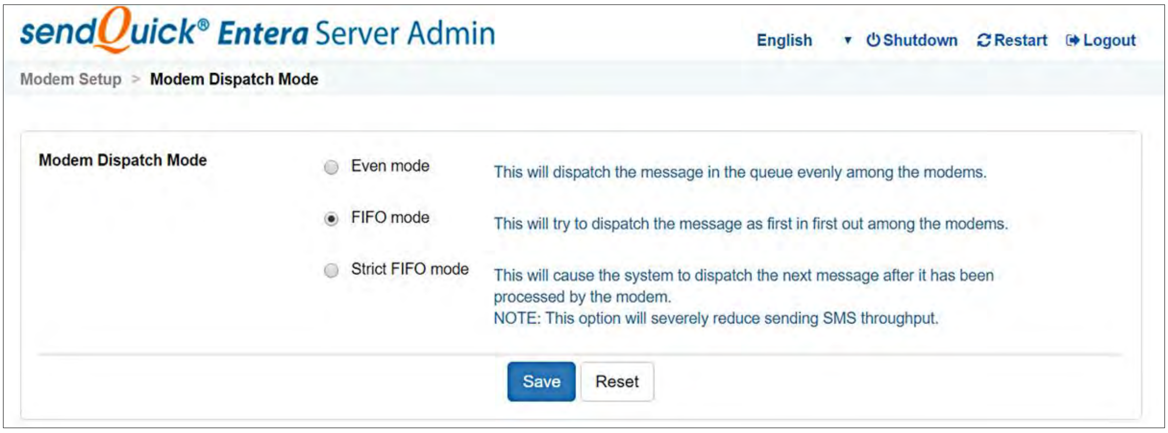
By default, the system will use the same modem for retry upon failure to send SMS. If "Use different modem for retry" is checked, the system will use the next available modem for retrying. However, this option is not applicable if only 1 modem connected to the system.

*Figure 7-1 : Total Modem Connections*

| | |
|---|---|
| **Note:** | When you switch between USB and Serial connection and vice versa, please remember to shut down 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 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.

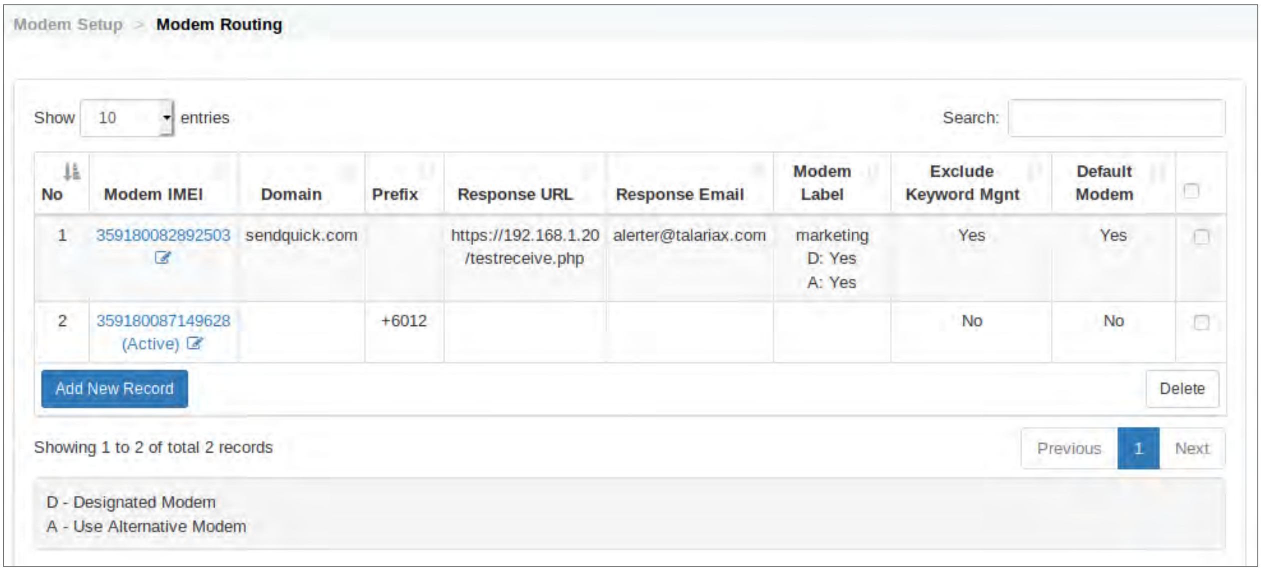
○ Strict FIFO mode — This will cause the system to dispatch the next message after it has been processed by the modem.
NOTE: This option will severely reduce sending SMS throughput.

*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 below shows a modem routing configured for different modem IMEI.



Modem Setup > Modem Routing

Show 10 entries Search:

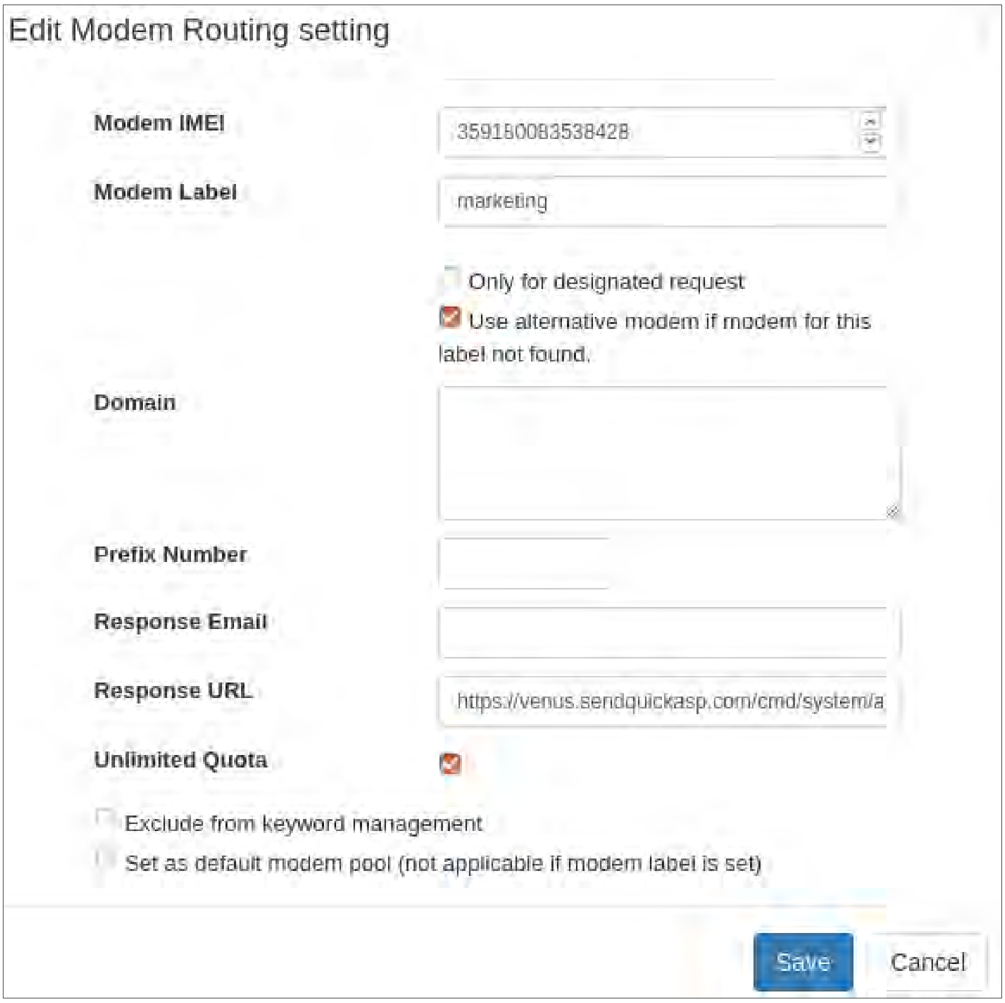
| No | Modem IMEI | Domain | Prefix | Response URL | Response Email | Modem Label | Exclude Keyword Mgnt | Default Modem | □ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 359180082892503 | sendquick.com | | https://192.168.1.20/testreceive.php | alerter@talariax.com | marketing<br>D: Yes<br>A: Yes | Yes | Yes | □ |
| 2 | 359180087149628 (Active) | | +6012 | | | | No | No | □ |

Showing 1 to 2 of total 2 records

D - Designated Modem
A - Use Alternative Modem

*Figure 7-3 : Modem Routing*

Click on "Add New Record" and the following will pop up. Fill up all the necessary data fields, press "Save" button to save this newly created route.



Edit Modem Routing setting

Modem IMEI: 359180083538428

Modem Label: marketing

☐ Only for designated request

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

Domain:

Prefix Number:

Response Email:

Response URL: https://venus.sendquickasp.com/cmd/system/a

Unlimited Quota ☑

☐ Exclude from keyword management

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

*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.

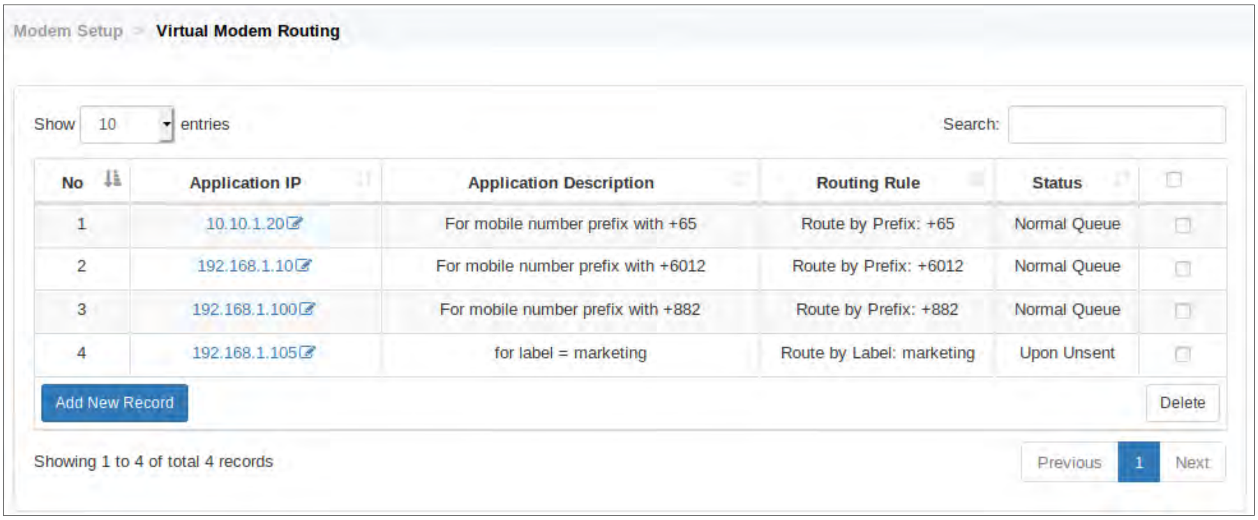
**Unlimited Quota**

- Checked - No limit on number of sms can be send by this modem.
- Unchecked – 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.



| 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 | □ |
| 2 | 192.168.1.10 | For mobile number prefix with +6012 | Route by Prefix: +6012 | Normal Queue | □ |
| 3 | 192.168.1.100 | For mobile number prefix with +882 | Route by Prefix: +882 | Normal Queue | □ |
| 4 | 192.168.1.105 | for label = marketing | Route by Label: marketing | Upon Unsent | □ |

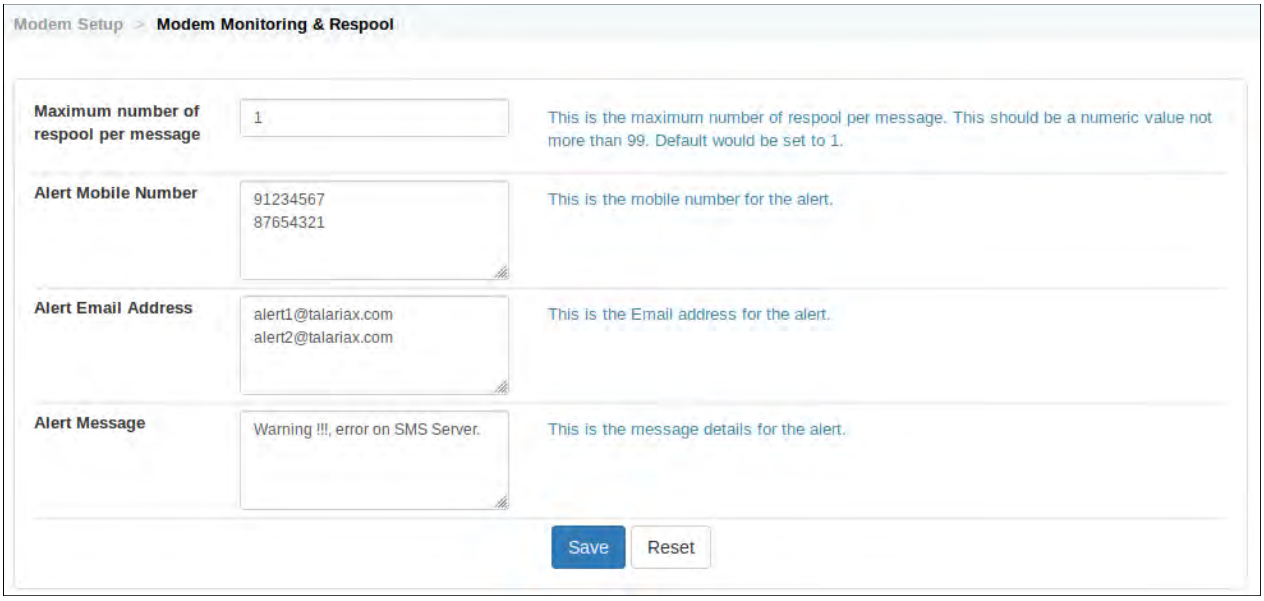
Showing 1 to 4 of total 4 records

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

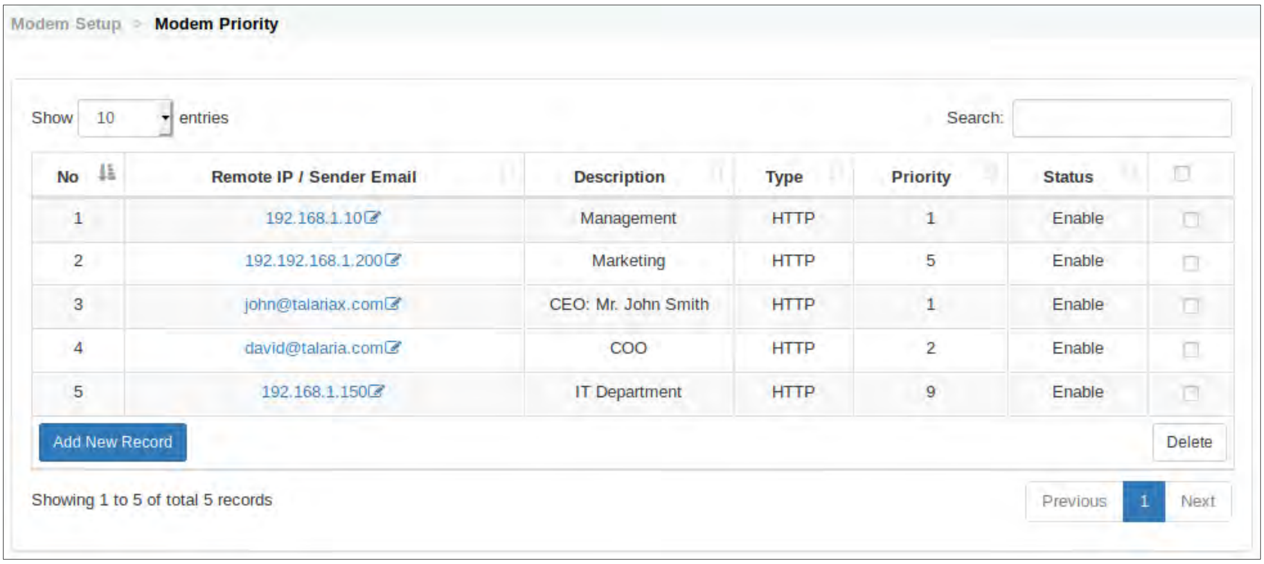


| | | |
|---|---|---|
| Maximum number of respool per message | 1 | This is the maximum number of respool per message. This should be a numeric value not more than 99. Default would be set to 1. |
| Alert Mobile Number | 91234567<br>87654321 | This is the mobile number for the alert. |
| Alert Email Address | alert1@talariax.com<br>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. |

*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).



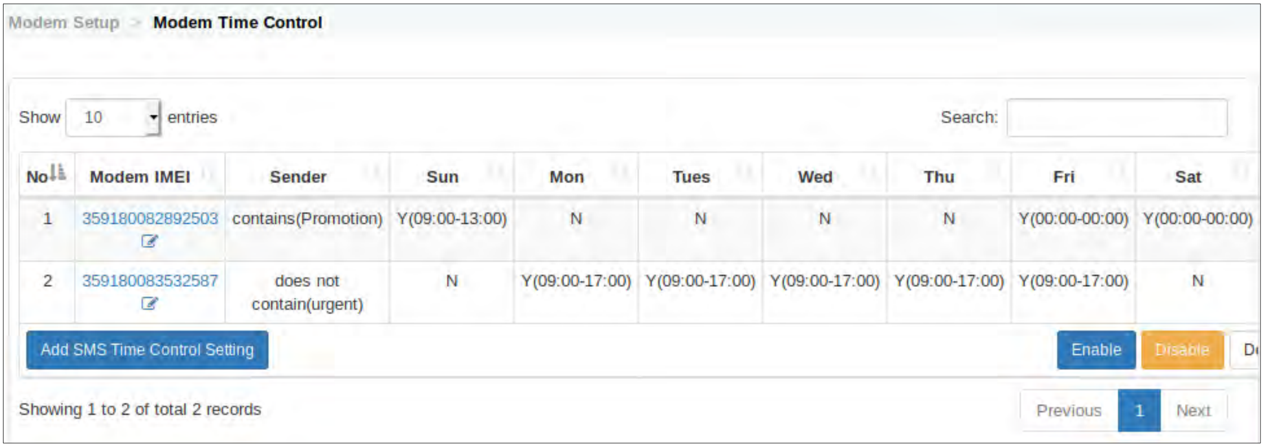
| No | Remote IP / Sender Email | Description | Type | Priority | Status | □ |
|---|---|---|---|---|---|---|
| 1 | 192.168.1.10 | Management | HTTP | 1 | Enable | □ |
| 2 | 192.192.168.1.200 | Marketing | HTTP | 5 | Enable | □ |
| 3 | john@talariax.com | CEO: Mr. John Smith | HTTP | 1 | Enable | □ |
| 4 | david@talaria.com | COO | HTTP | 2 | Enable | □ |
| 5 | 192.168.1.150 | IT Department | HTTP | 9 | Enable | □ |

Showing 1 to 5 of total 5 records

*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 10 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 |

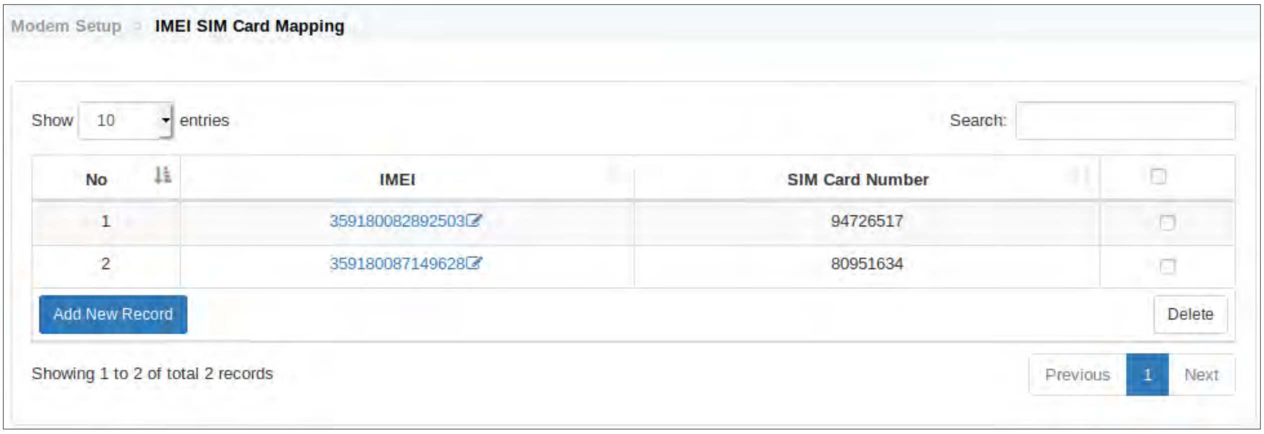
Add SMS Time Control Setting
Enable
Disable
De
Previous
1
Next

Showing 1 to 2 of total 2 records

*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:

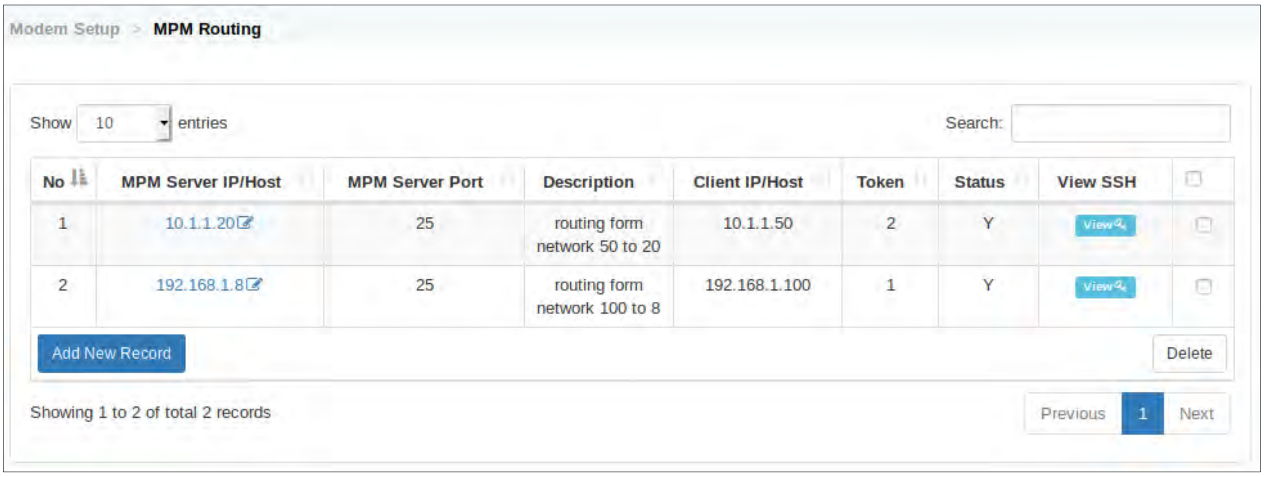
| No | IMEI | SIM Card Number | □ |
|---|---|---|---|
| 1 | 359180082892503 | 94726517 | □ |
| 2 | 359180087149628 | 80951634 | □ |

Showing 1 to 2 of total 2 records

*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 | □ |
|---|---|---|---|---|---|---|---|---|
| 1 | 10.1.1.20 | 25 | routing form network 50 to 20 | 10.1.1.50 | 2 | Y | View | □ |
| 2 | 192.168.1.8 | 25 | routing form network 100 to 8 | 192.168.1.100 | 1 | Y | View | □ |

Showing 1 to 2 of total 2 records

*Figure 7-10 : MPM Routing*

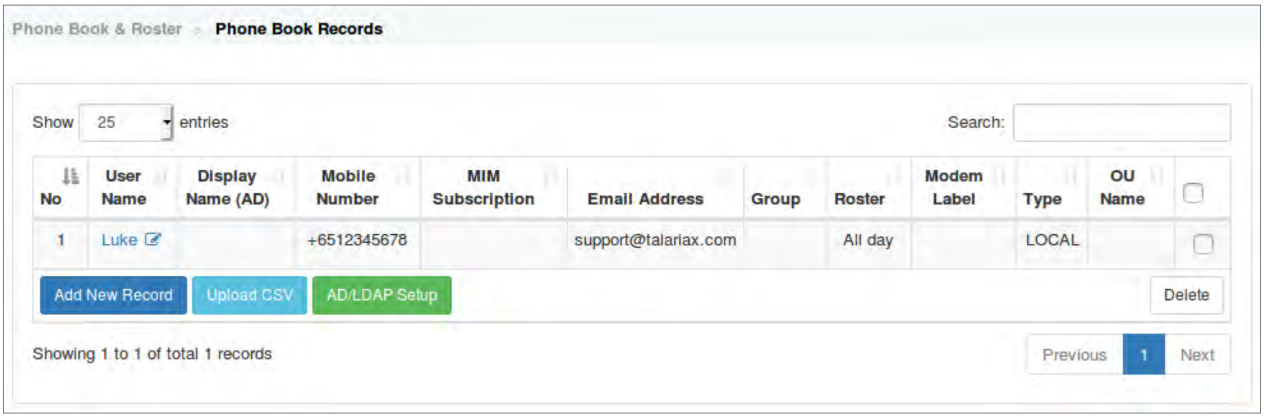
# 8.0 Phone Book & Roster

**(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 | | □ |

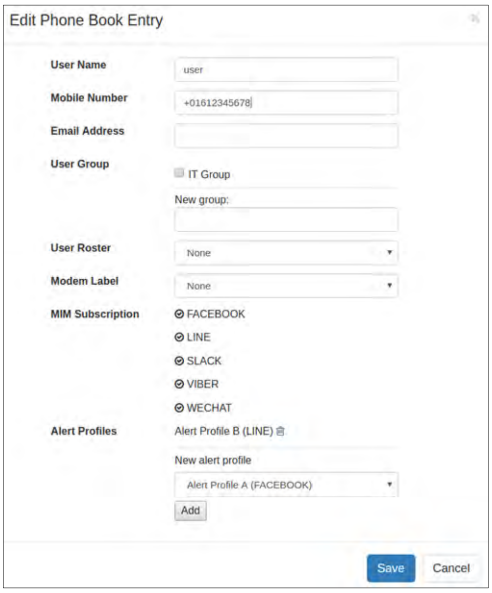
Showing 1 to 1 of total 1 records

*Figure 8-1 : Phone Book Records*

Select **Add New Record** and the following will pop up. 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.



Edit Phone Book Entry

User Name: user

Mobile Number: +01612345678

Email Address:

User Group: □ IT Group

New group:

User Roster: None

Modem Label: None

MIM Subscription:
- FACEBOOK
- LINE
- SLACK
- VIBER
- WECHAT

Alert Profiles: Alert Profile B (LINE)

New alert profile: Alert Profile A (FACEBOOK)

*Figure 8-2 : 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.

### 8.1.1 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 more details.

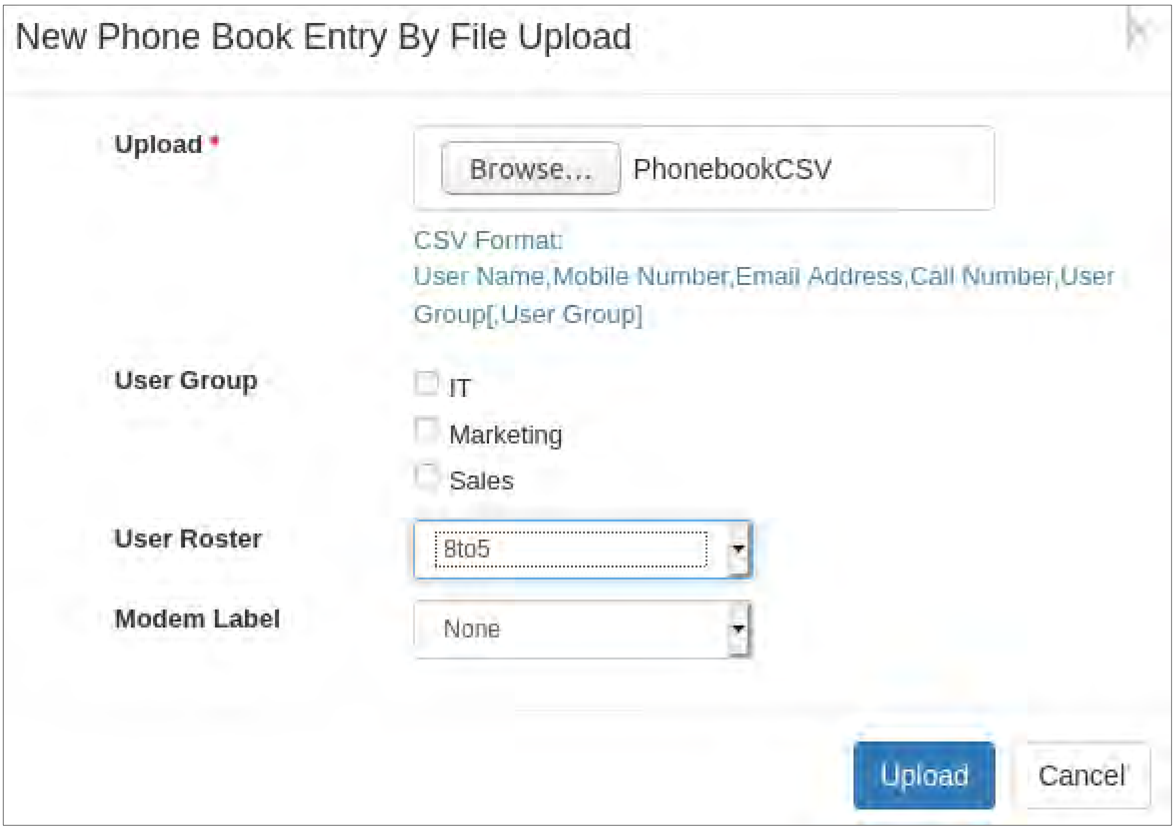
Please prepare your CSV record(s) that 'Group by Roster' in this format:

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

Sample data as follow:

```
MohdAli, 91234567,mohdali@talariax.com,61234567, IT
JohnDoe,91234568,johndoe@talariax.com,61234568,Sales
DavidTan,912345679,davidtan@talariax.com,61234569,Marketing
SanjayV,912345670,sanjayv@talariax.com,61234570,Marketing
```

When your CSV file is ready, select 'Upload CSV' from Figure 8-1 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

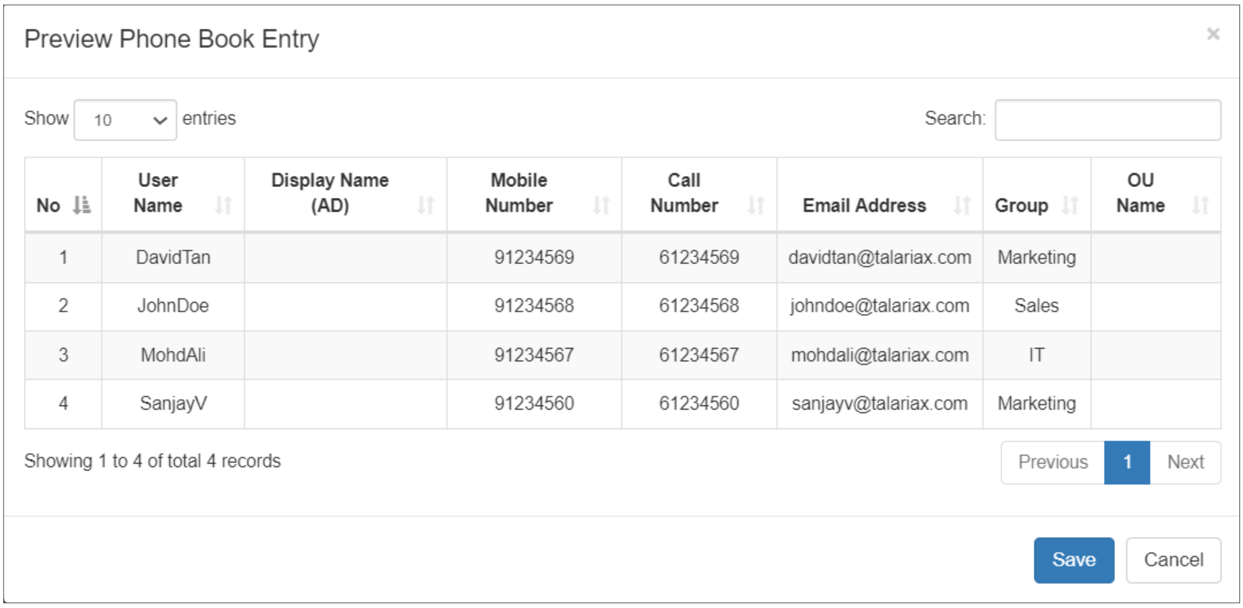
User Roster: 8to5

Modem Label: None

*Figure 8-3 : 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

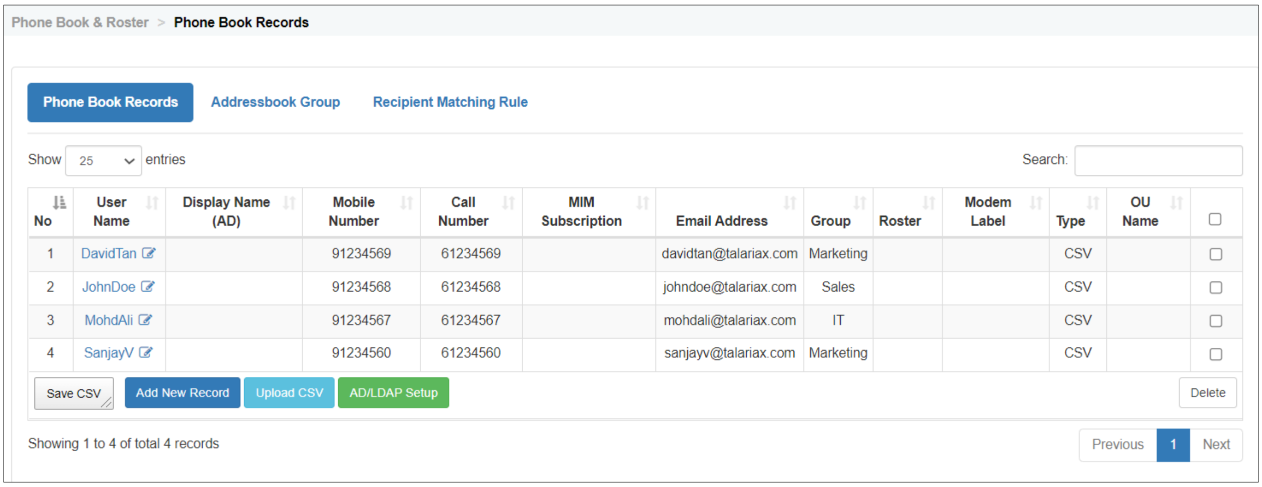
Show 10 entries    Search:

| No | User Name | Display Name (AD) | Mobile Number | Call Number | Email Address | Group | OU Name |
|---|---|---|---|---|---|---|---|
| 1 | DavidTan | | 91234569 | 61234569 | davidtan@talariax.com | Marketing | |
| 2 | JohnDoe | | 91234568 | 61234568 | johndoe@talariax.com | Sales | |
| 3 | MohdAli | | 91234567 | 61234567 | mohdali@talariax.com | IT | |
| 4 | SanjayV | | 91234560 | 61234560 | sanjayv@talariax.com | Marketing | |

Showing 1 to 4 of total 4 records

*Figure 8-4 : Preview Phone Book Entry*

Upon your confirmation, the Phone Book Records are uploaded:



Phone Book & Roster > Phone Book Records

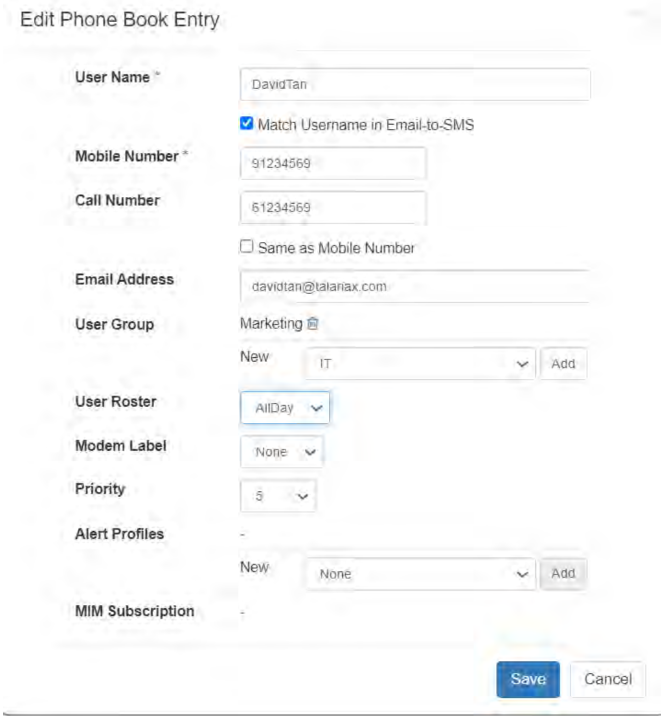
Show 25 entries Search:

| No | User Name | Display Name (AD) | Mobile Number | Call Number | MIM Subscription | Email Address | Group | Roster | Modem Label | Type | OU Name | □ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | DavidTan | | 91234569 | 61234569 | | davidtan@talariax.com | Marketing | | | CSV | | □ |
| 2 | JohnDoe | | 91234568 | 61234568 | | johndoe@talariax.com | Sales | | | CSV | | □ |
| 3 | MohdAli | | 91234567 | 61234567 | | mohdali@talariax.com | IT | | | CSV | | □ |
| 4 | SanjayV | | 91234560 | 61234560 | | sanjayv@talariax.com | Marketing | | | CSV | | □ |

Showing 1 to 4 of total 4 records

*Figure 8-5 : Updated Phone Book Records*

Click on Username to edit user's information on screen.



Edit Phone Book Entry

User Name * DavidTan

☑ Match Username in Email-to-SMS

Mobile Number * 91234569

Call Number 61234569

□ Same as Mobile Number

Email Address davidtan@talariax.com

User Group Marketing

New IT

User Roster AllDay

Modem Label None

Priority 5

Alert Profiles -

New None

MIM Subscription -

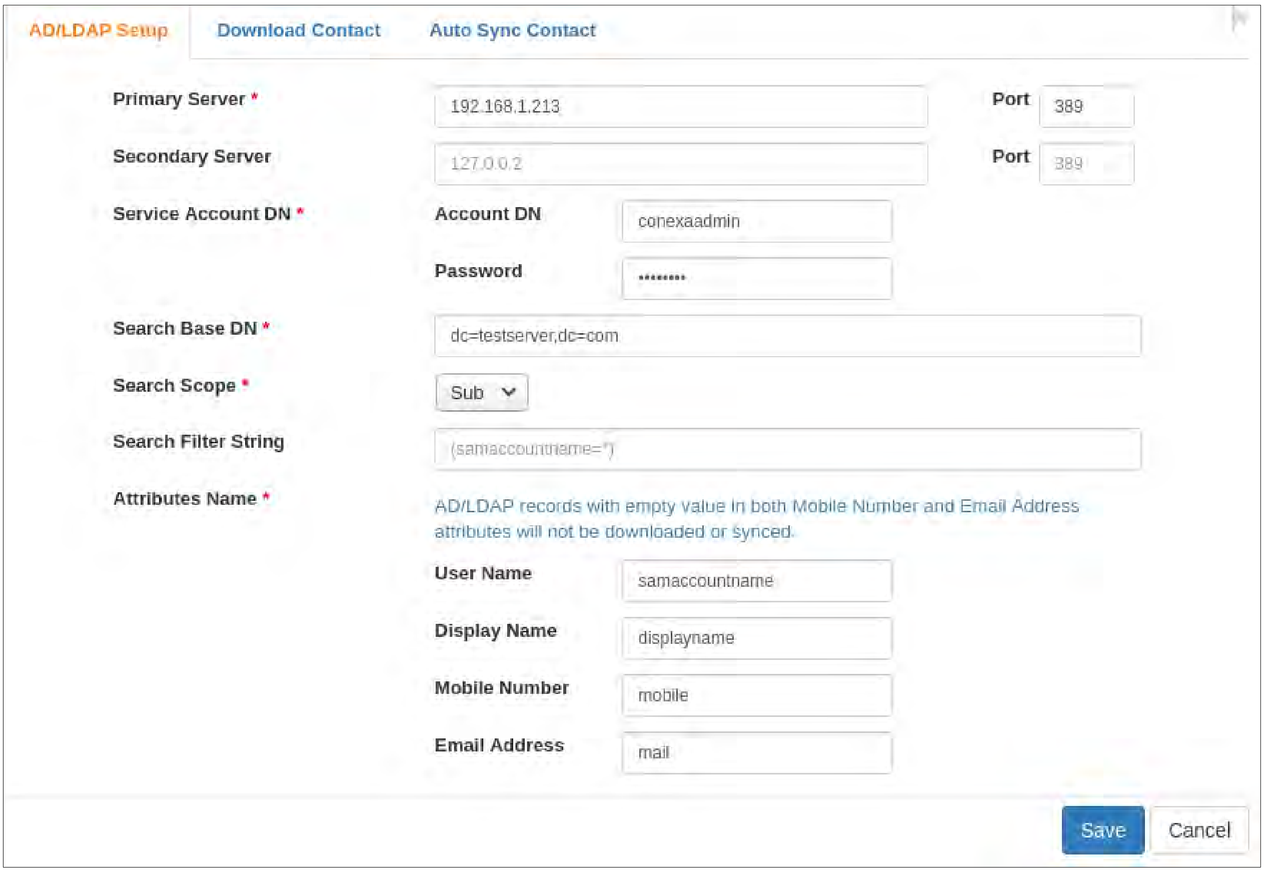
*Figure 8-6 : Edit Phone Book Entry*

## 8.1.2 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 8-7: AD/LDAP Setup.
2. Download Contact from AD/LDAP.

*Figure 8-7 : Phone Book Records with expanded information*



Primary Server *: 192.168.1.213 Port: 389

Secondary Server: 127.0.0.2 Port: 389

Service Account DN *: Account DN: conexaadmin; Password: ••••••••

Search Base DN *: dc=testserver,dc=com

Search Scope *: Sub

Search Filter String: (samaccountname=*)

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

User Name: samaccountname

Display Name: displayname

Mobile Number: mobile

Email Address: mail

Figure 8-8 : 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'.

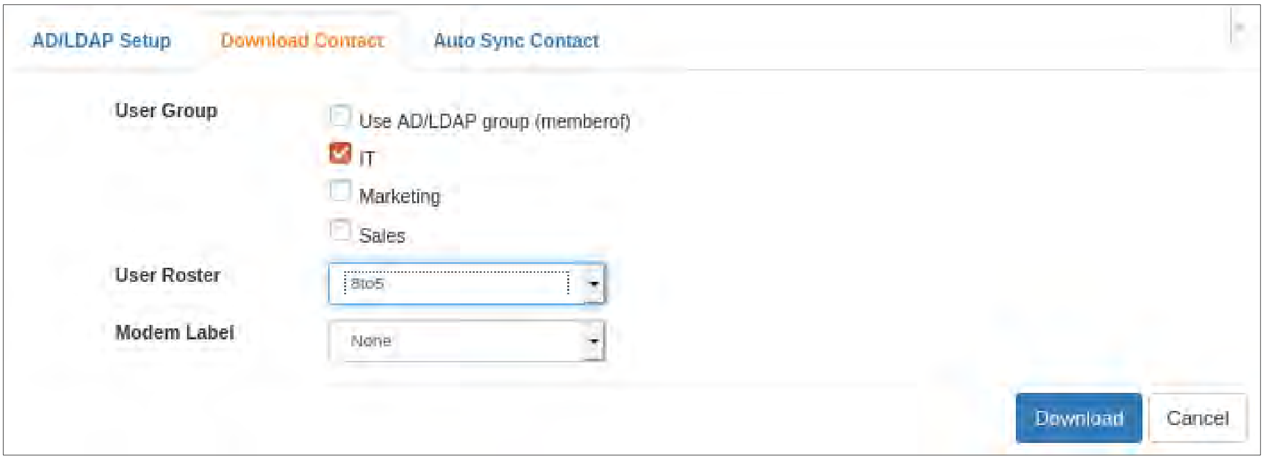
- **Service Account DN**: AD/LDAP server's login account and password.
- **Search Base DB**: default as 'dc=testserver,dc=com'.
- **Search Scope**: Sub / One / Base.
- **Search Filter String**: default as 'samaccountname'.

*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:



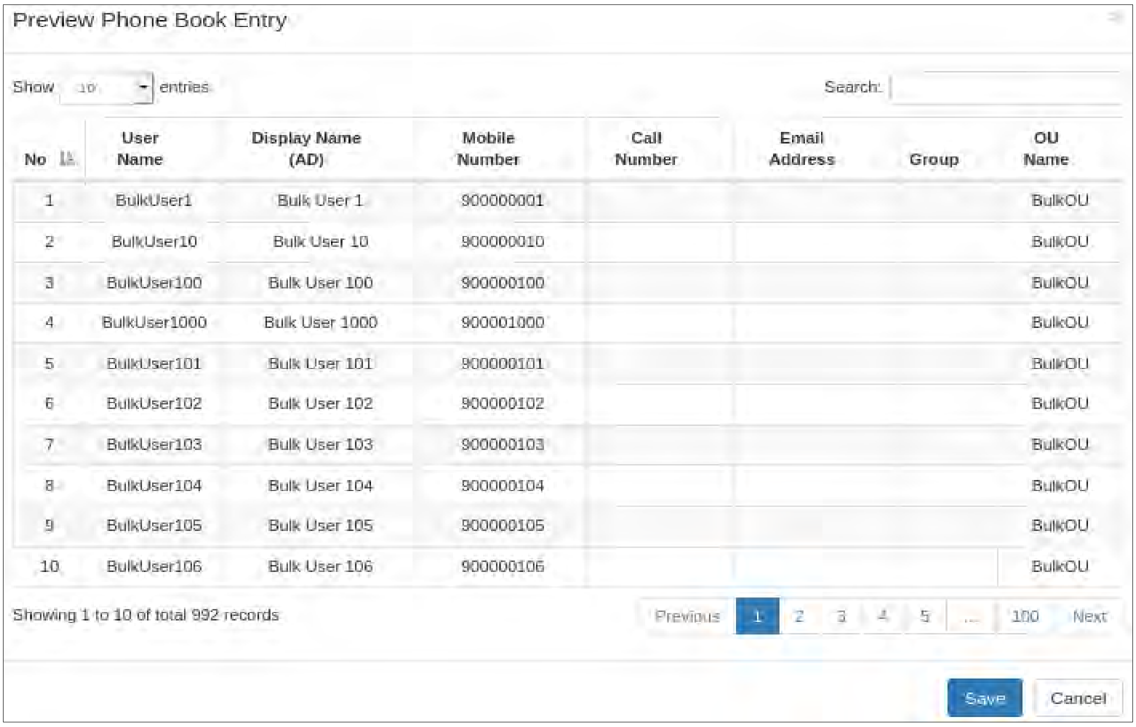
User Group
□ Use AD/LDAP group (memberof)
☑ IT
□ Marketing
□ Sales

User Roster: 8to5

Modem Label: None

*Figure 8-9 : Download Contact*

Depending on the parameters that defined on Figure 8-7: 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 8-7: AD/LDAP Setup.



Preview Phone Book Entry

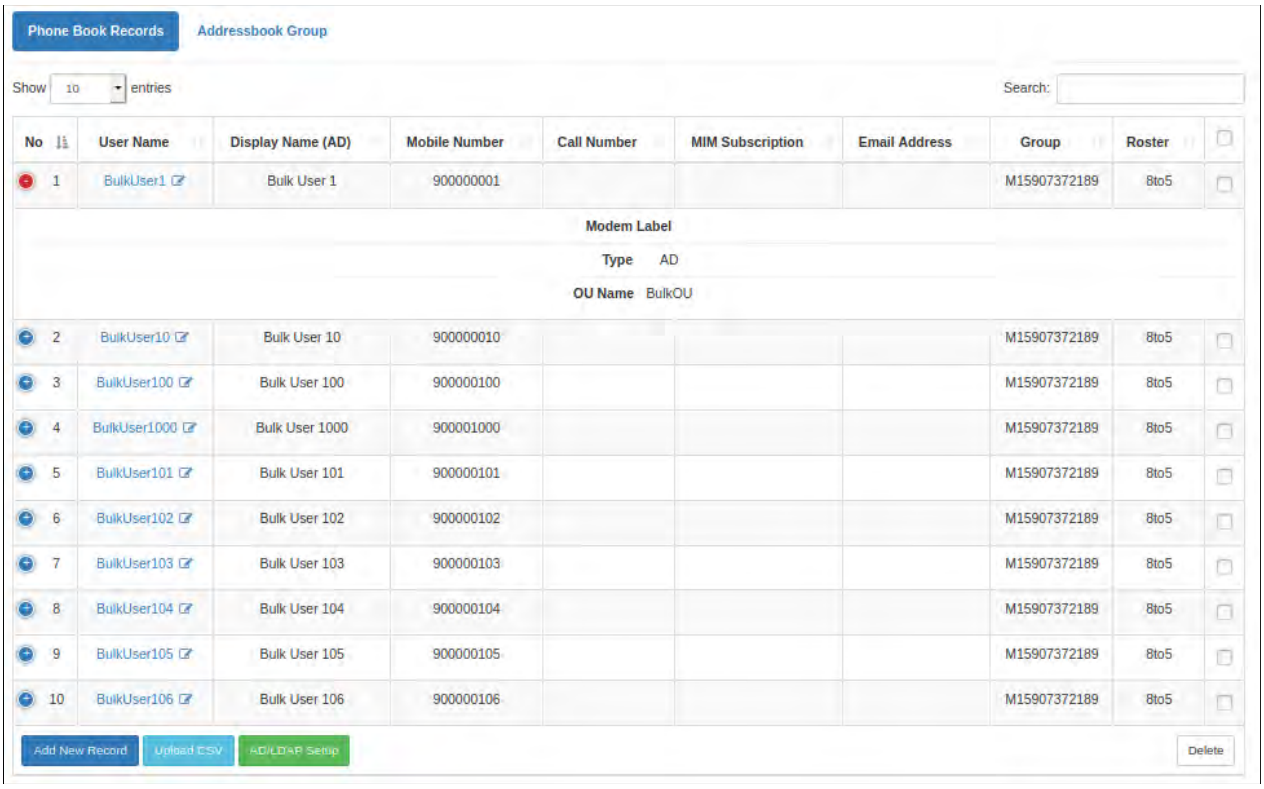
Show 10 entries Search:

| 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

Figure 8-10 : Preview Phone Book Entry

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



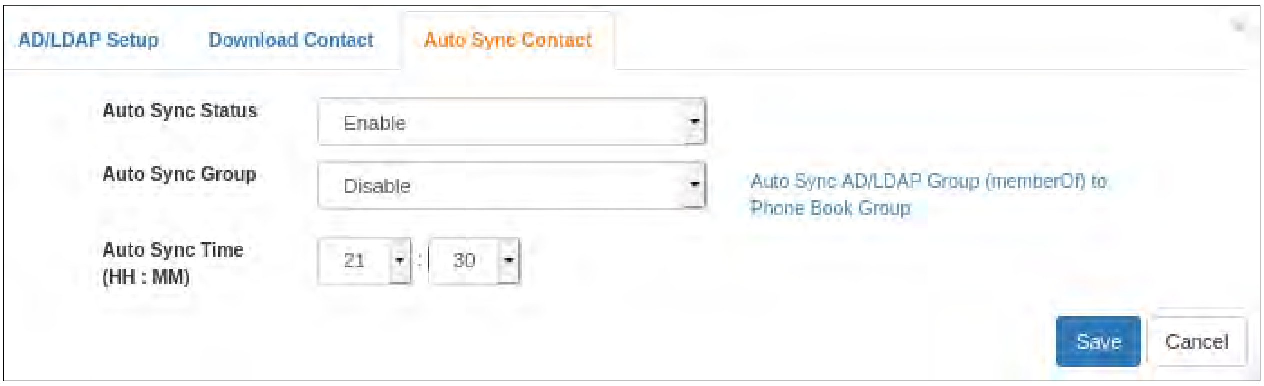
Show 10 entries Search:

| | No | User Name | Display Name (AD) | Mobile Number | Call Number | MIM Subscription | Email Address | Group | Roster | □ |
|---|---|---|---|---|---|---|---|---|---|---|
| ⊖ | 1 | BulkUser1 | Bulk User 1 | 900000001 | | | | M15907372189 | 8to5 | □ |
| ⊕ | 2 | BulkUser10 | Bulk User 10 | 900000010 | | | | M15907372189 | 8to5 | □ |
| ⊕ | 3 | BulkUser100 | Bulk User 100 | 900000100 | | | | M15907372189 | 8to5 | □ |
| ⊕ | 4 | BulkUser1000 | Bulk User 1000 | 900001000 | | | | M15907372189 | 8to5 | □ |
| ⊕ | 5 | BulkUser101 | Bulk User 101 | 900000101 | | | | M15907372189 | 8to5 | □ |
| ⊕ | 6 | BulkUser102 | Bulk User 102 | 900000102 | | | | M15907372189 | 8to5 | □ |
| ⊕ | 7 | BulkUser103 | Bulk User 103 | 900000103 | | | | M15907372189 | 8to5 | □ |
| ⊕ | 8 | BulkUser104 | Bulk User 104 | 900000104 | | | | M15907372189 | 8to5 | □ |
| ⊕ | 9 | BulkUser105 | Bulk User 105 | 900000105 | | | | M15907372189 | 8to5 | □ |
| ⊕ | 10 | BulkUser106 | Bulk User 106 | 900000106 | | | | M15907372189 | 8to5 | □ |

Modem Label
Type AD
OU Name BulkOU

Figure 8-11 : Phone Book records

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



Auto Sync Status: Enable

Auto Sync Group: Disable

Auto Sync AD/LDAP Group (memberOf) to Phone Book Group

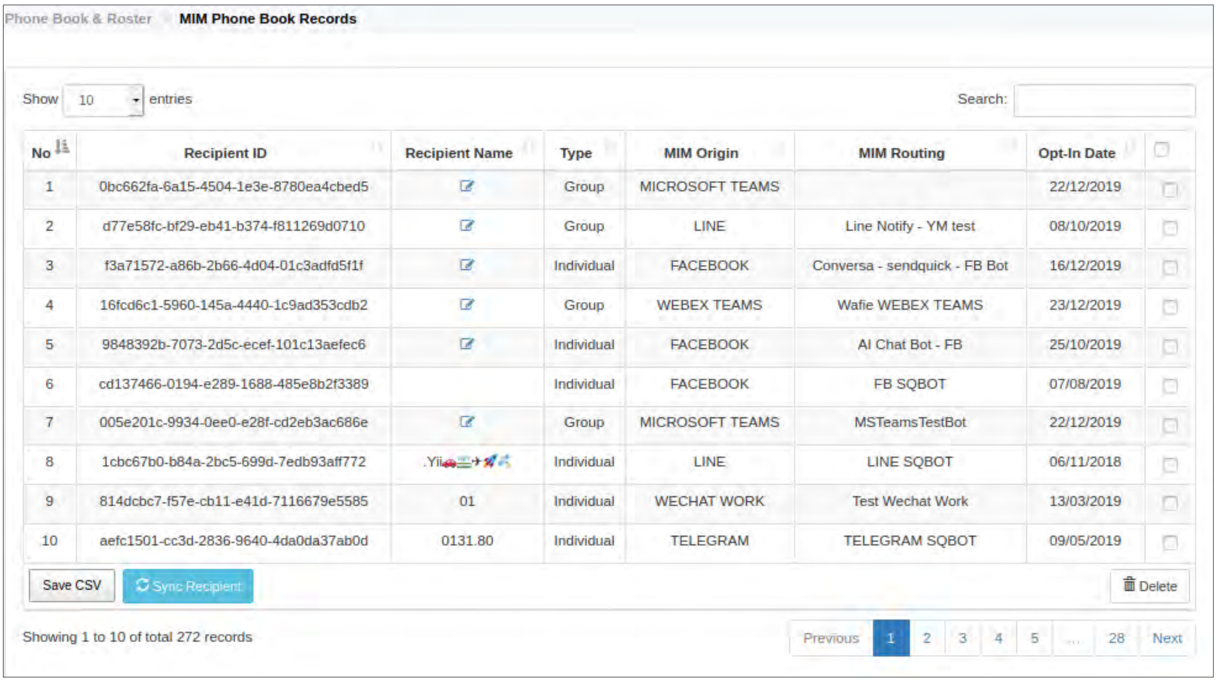
Auto Sync Time (HH : MM): 21 : 30

*Figure 8-12 : 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-8780ea4cbed5 | ✎ | Group | MICROSOFT TEAMS | | 22/12/2019 | □ |
| 2 | d77e58fc-bf29-eb41-b374-f811269d0710 | ✎ | Group | LINE | Line Notify - YM test | 08/10/2019 | □ |
| 3 | f3a71572-a86b-2b66-4d04-01c3adfd5f1f | ✎ | Individual | FACEBOOK | Conversa - sendquick - FB Bot | 16/12/2019 | □ |
| 4 | 16fcd6c1-5960-145a-4440-1c9ad353cdb2 | ✎ | Group | WEBEX TEAMS | Wafie WEBEX TEAMS | 23/12/2019 | □ |
| 5 | 9848392b-7073-2d5c-ecef-101c13aefec6 | ✎ | Individual | FACEBOOK | AI Chat Bot - FB | 25/10/2019 | □ |
| 6 | cd137466-0194-e289-1688-485e8b2f3389 | | Individual | FACEBOOK | FB SQBOT | 07/08/2019 | □ |
| 7 | 005e201c-9934-0ee0-e28f-cd2eb3ac686e | ✎ | Group | MICROSOFT TEAMS | MSTeamsTestBot | 22/12/2019 | □ |
| 8 | 1cbc67b0-b84a-2bc5-699d-7edb93aff772 | .Yii🚗🛤✈🚀 | Individual | LINE | LINE SQBOT | 06/11/2018 | □ |
| 9 | 814dcbc7-f57e-cb11-e41d-7116679e5585 | 01 | Individual | WECHAT WORK | Test Wechat Work | 13/03/2019 | □ |
| 10 | aefc1501-cc3d-2836-9640-4da0da37ab0d | 0131.80 | Individual | TELEGRAM | TELEGRAM SQBOT | 09/05/2019 | □ |

Save CSV  Sync Recipient  Delete

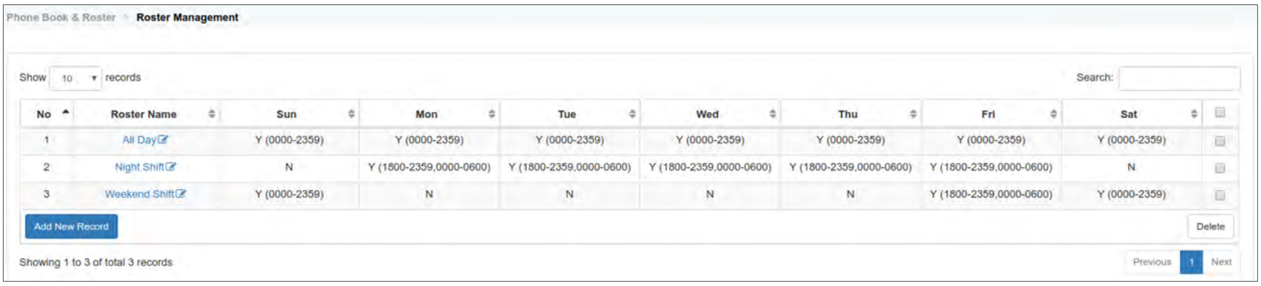
Showing 1 to 10 of total 272 records  Previous 1 2 3 4 5 ... 28 Next

*Figure 8-13 : 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 in the figure below. 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:

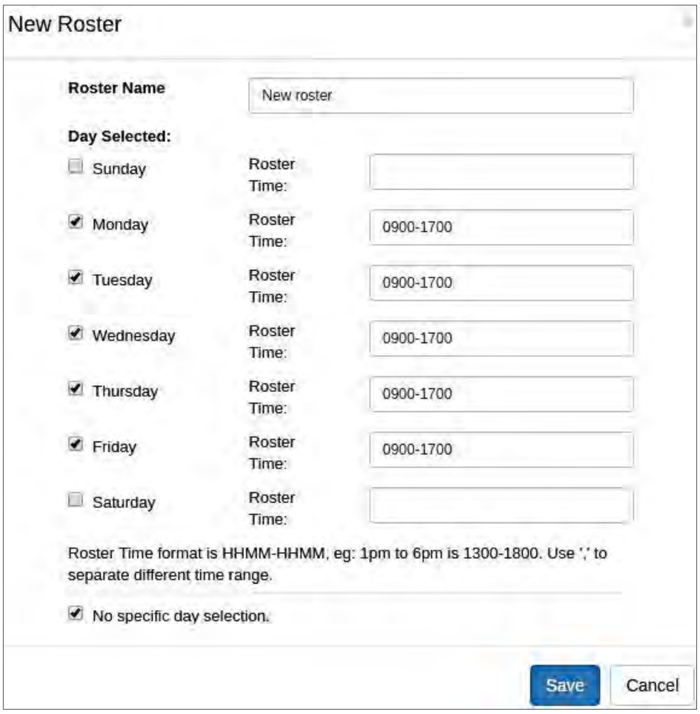
| No | Roster Name | Sun | Mon | Tue | Wed | Thu | Fri | Sat | □ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | All Day✎ | Y (0000-2359) | Y (0000-2359) | Y (0000-2359) | Y (0000-2359) | Y (0000-2359) | Y (0000-2359) | Y (0000-2359) | □ |
| 2 | Night Shift✎ | N | Y (1800-2359,0000-0600) | Y (1800-2359,0000-0600) | 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 8-14 : Roster Management*

Select the **Add New Record** button and the following window will pop up for creation of a new roster. 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:

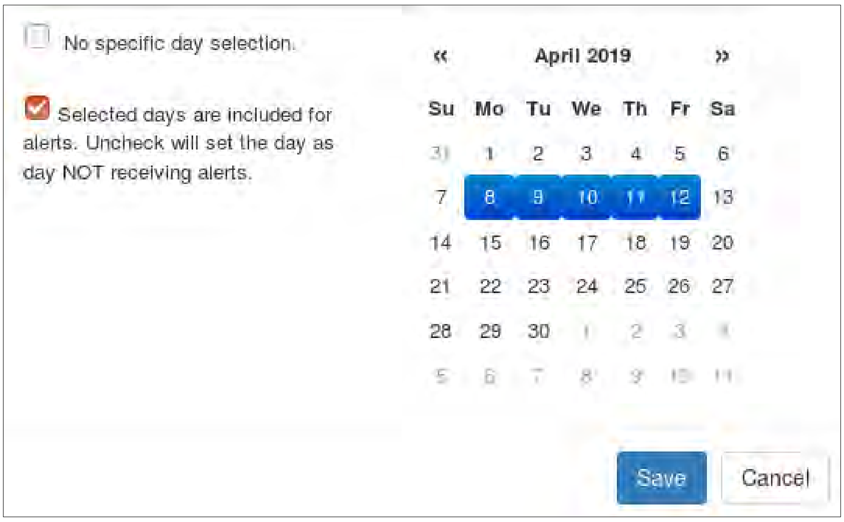
| | | |
|---|---|---|
| □ Sunday | Roster Time: | |
| ☑ Monday | Roster Time: | 0900-1700 |
| ☑ Tuesday | Roster Time: | 0900-1700 |
| ☑ Wednesday | Roster Time: | 0900-1700 |
| ☑ Thursday | Roster Time: | 0900-1700 |
| ☑ Friday | Roster Time: | 0900-1700 |
| □ Saturday | Roster Time: | |

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

☑ No specific day selection.

*Figure 8-15 : New Roster*

There are instances where a shift is only for a particular period and not repeated, e.g., 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 »

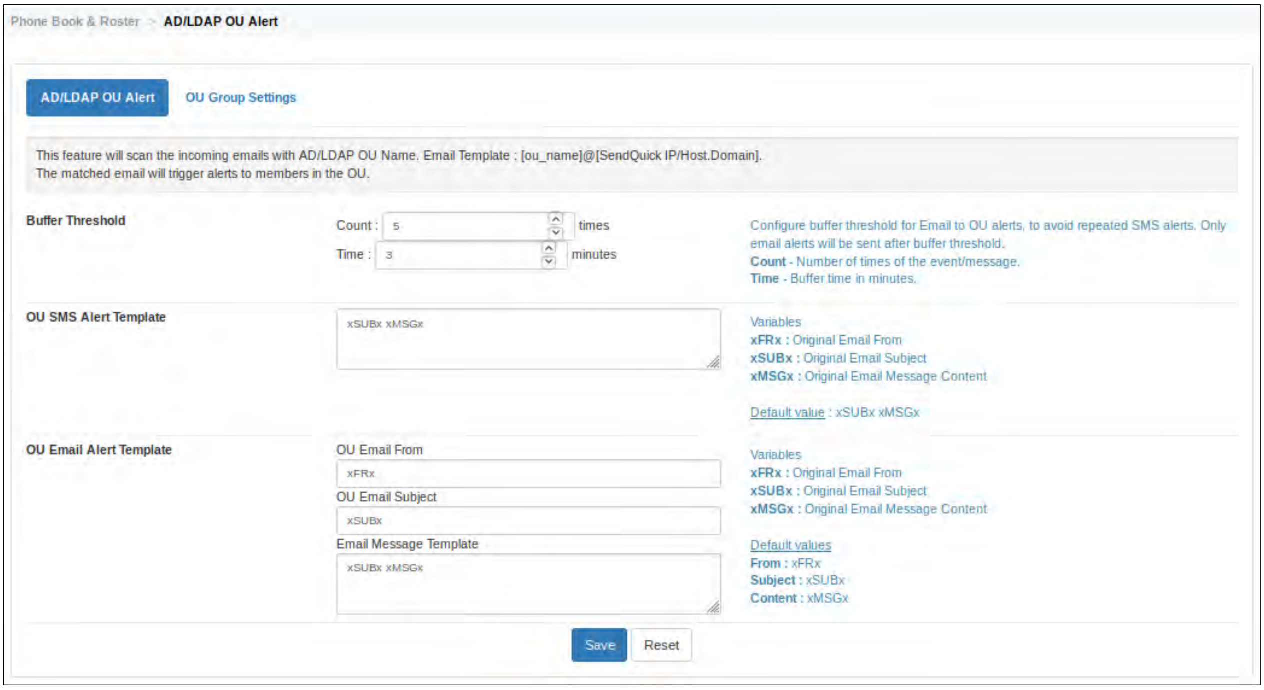
| Su | Mo | Tu | We | Th | Fr | Sa |
|---|---|---|---|---|---|---|
| 31 | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 28 | 29 | 30 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |

*Figure 8-16 : 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.



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.

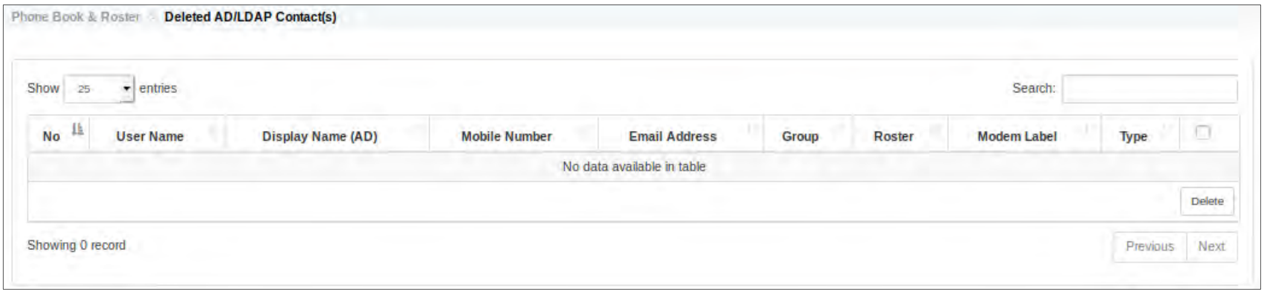
OU SMS Alert Template
xSUBx xMSGx
Variables
**xFRx :** Original Email From
**xSUBx :** Original Email Subject
**xMSGx :** Original Email Message Content
Default value : xSUBx xMSGx

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

*Figure 8-17 : 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.



| No | User Name | Display Name (AD) | Mobile Number | Email Address | Group | Roster | Modem Label | Type | □ |
|---|---|---|---|---|---|---|---|---|---|
| No data available in table | | | | | | | | | |

Showing 0 record

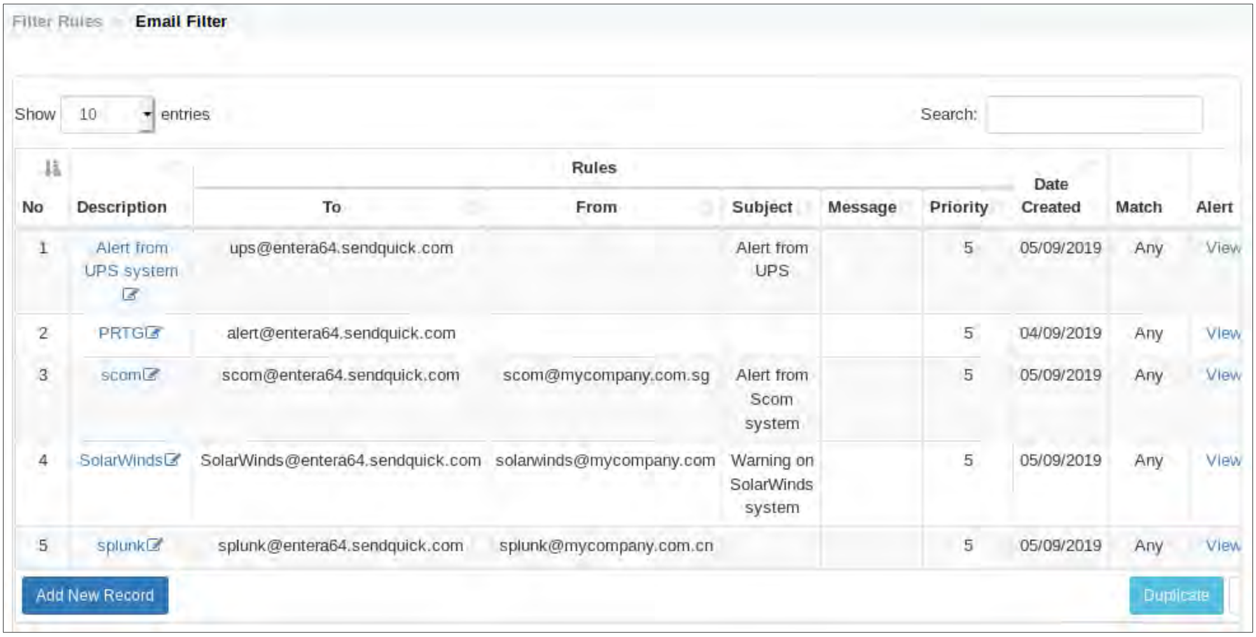
*Figure 8-18 : Delete AD/LDAP Contacts*

# 9.0 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 at a later stage as it has no impact on the operation of sendQuick system.

## *9.1 Email Filter*

The Email Filter is for filtering the email notifications from different systems (example firewall, anti-virus, IPS, UPS and others) to sendQuick and applied with the Email Filter policies to determine the corresponding recipients to receive SMS messages. All messages that were sent to Email Filter will be filtered in accordance to the message filter rules (Figure 9-1).



| No | Description | Rules | | | | | Date Created | Match | Alert |
|---|---|---|---|---|---|---|---|---|---|
| | | To | From | Subject | Message | Priority | | | |
| 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. The Message Filter will be useful for the selectively sending alert messages to only the corresponding recipients.

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.

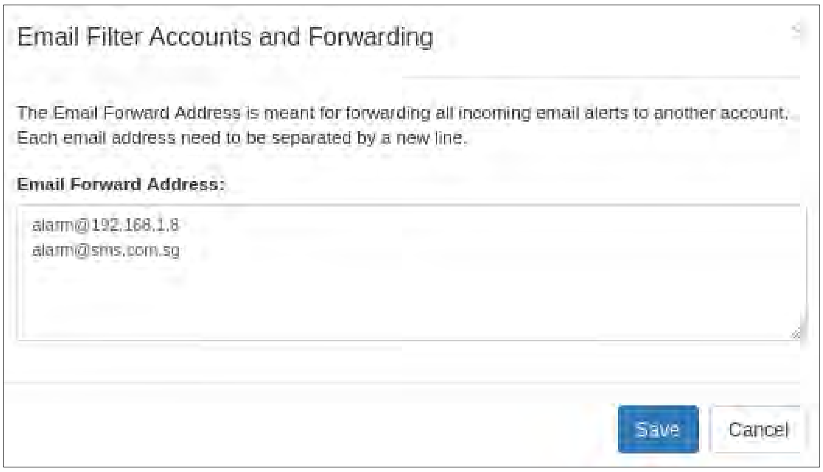
All emails that need to be filtered will be sent to sendQuick servers, either using sendQuick domain (FQDN) or IP address. The format is **'username@sendQuickIPorDomain'**. As sendQuick is a mail server, it can process all emails that has the server destination as itself, meaning sendQuick IP or domain.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



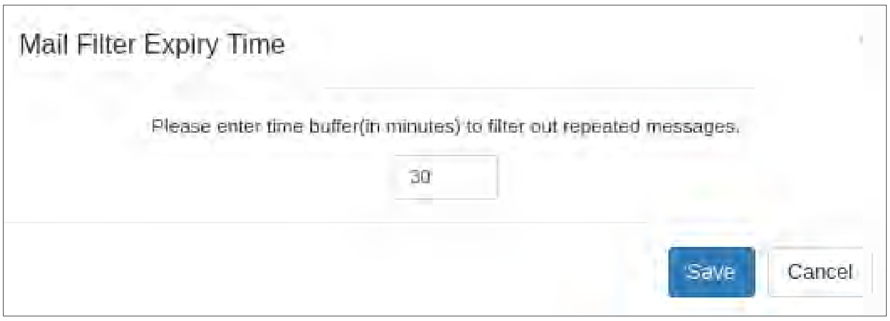
Email Filter Accounts and Forwarding

The Email Forward Address is meant for forwarding all incoming email alerts to another account. Each email address need to be separated by a new line.

Email Forward Address:

alarm@192.168.1.8
alarm@sms.com.sg

Figure 9-2 : Email Filter Accounts and Forwarding



Mail Filter Expiry Time

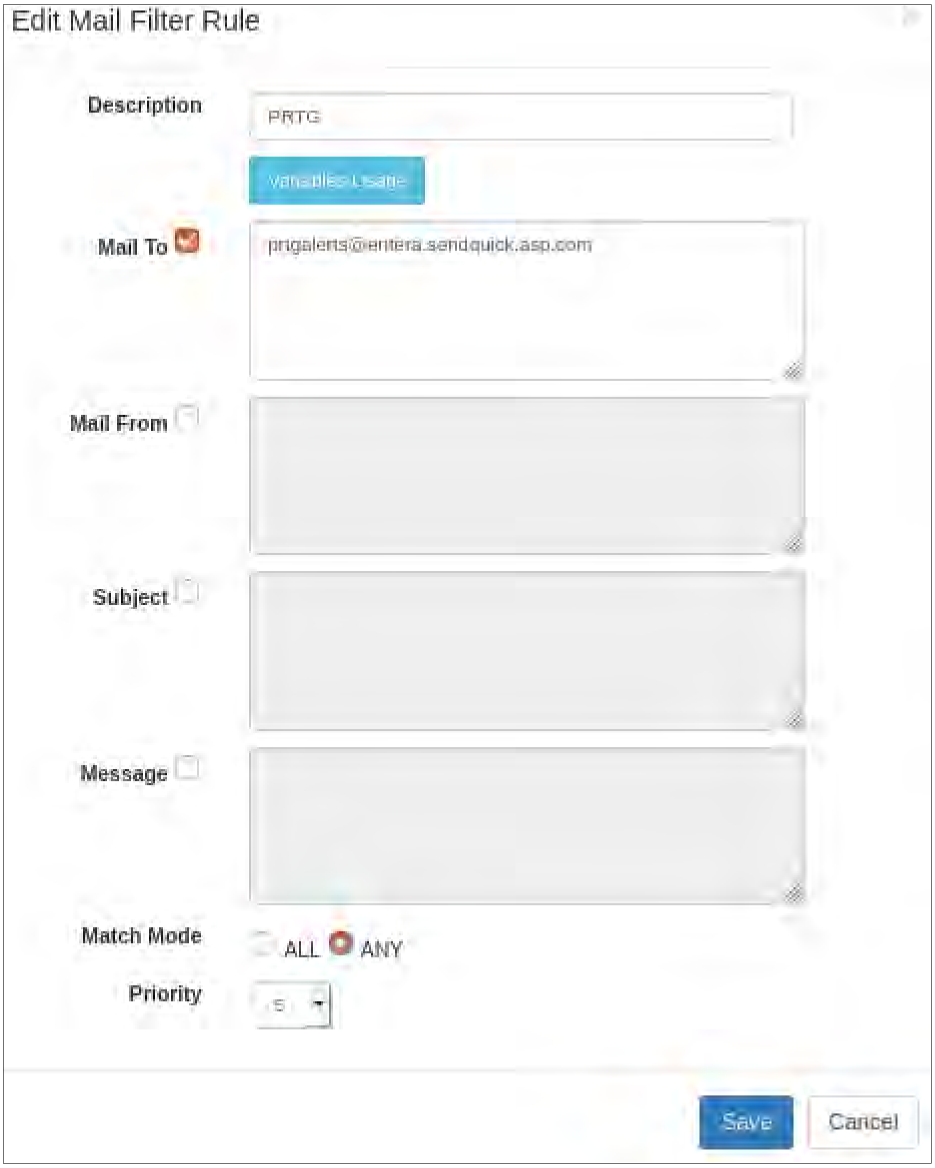
Please enter time buffer(in minutes) to filter out repeated messages.

30

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

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

Mail From □

Subject □

Message □

Match Mode ○ ALL ● ANY

Priority 5

*Figure 9-4 : Add Mail Filter Rule*

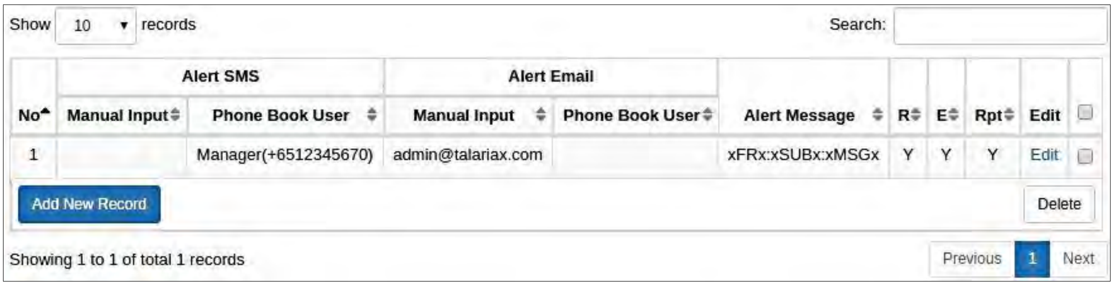
The filter works by checking on the attributes of the email message. They are the receiver email address (**To**), sender email address (**From**), **Subject** field and **Message** body content. There is a checkbox on the side of the field name. If the desired field name is required for filtering, just 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:

| ***Sentence*** | ***Match Status*** | ***Reasons*** |
|---|---|---|
| There is an error in the system message | No | Though the words 'error' and 'message' appears in the sentence, they are individual words and not a phrase. |
| This is a system error | No | Only the word 'error' 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).



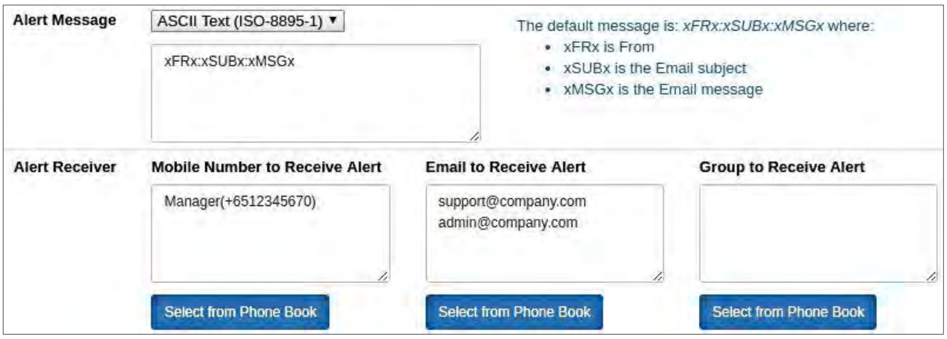
Show 10 records Search:

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



Alert Message: ASCII Text (ISO-8895-1)

xFRx:xSUBx:xMSGx

The default message is: *xFRx:xSUBx:xMSGx* where:
- xFRx is From
- xSUBx is the Email subject
- xMSGx is the Email message

Alert Receiver

Mobile Number to Receive Alert: Manager(+6512345670)

Email to Receive Alert: support@company.com<br>admin@company.com

Group to Receive Alert:

*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.

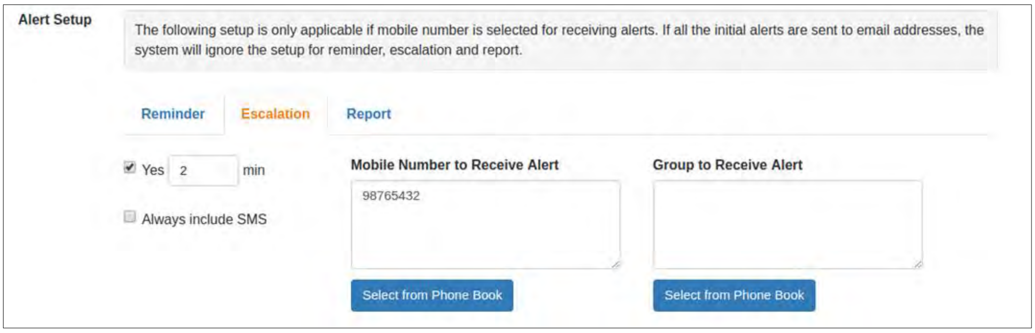
The actual content of the SMS alert will be the original content of the email message and the fields to be sent (FROM, SUBJECT and MESSAGE) will depends on the selection in the SMS

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.



Alert Setup

The following setup is only applicable if mobile number is selected for receiving alerts. If all the initial alerts are sent to email addresses, the system will ignore the setup for reminder, escalation and report.

*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.

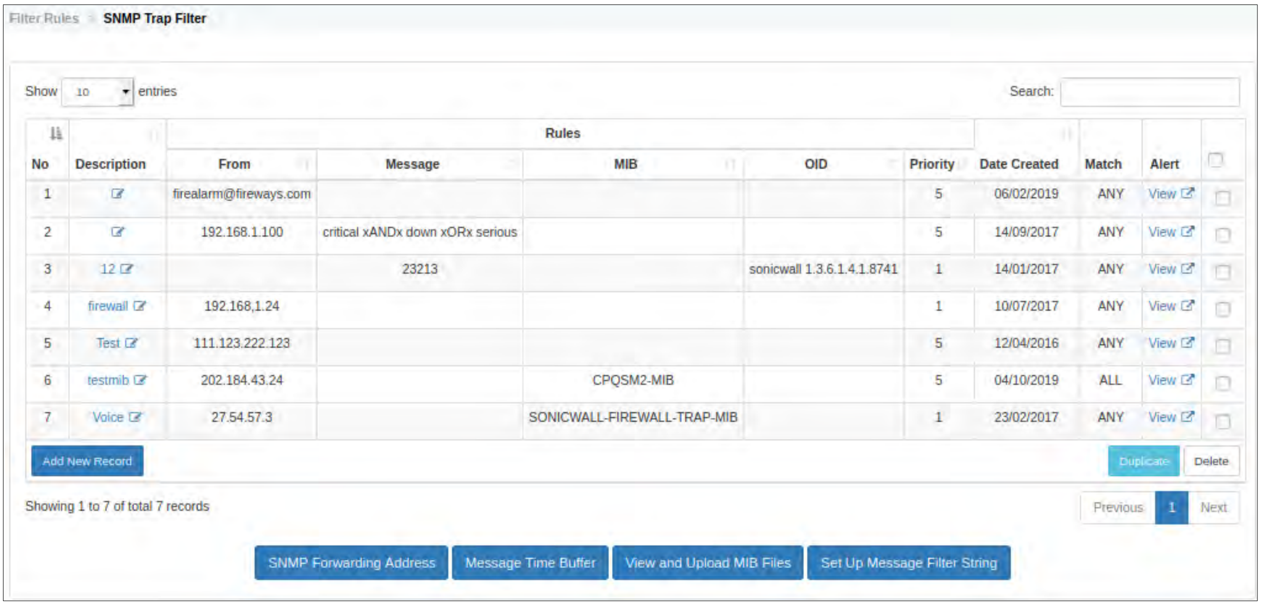
If there is no SMS acknowledgment from any recipients despite the reminders and escalation, a SMS summary report will be sent at the end of the time session that was configured for the

**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**. The SNMP Trap filter support SNMP v1 and v2 only.

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).

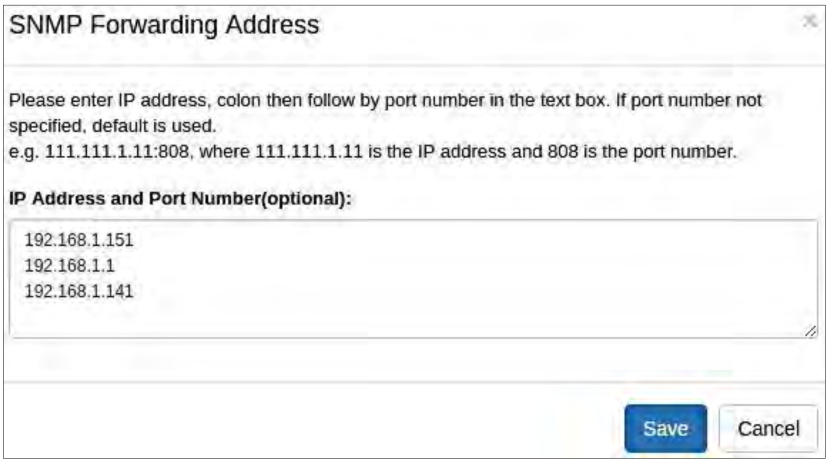


| | | Rules | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| No | Description | From | Message | MIB | OID | Priority | Date Created | Match | Alert | □ |
| 1 | | firealarm@fireways.com | | | | 5 | 06/02/2019 | ANY | View | □ |
| 2 | | 192.168.1.100 | critical xANDx down xORx serious | | | 5 | 14/09/2017 | ANY | View | □ |
| 3 | 12 | | 23213 | | sonicwall 1.3.6.1.4.1.8741 | 1 | 14/01/2017 | ANY | View | □ |
| 4 | firewall | 192.168,1.24 | | | | 1 | 10/07/2017 | ANY | View | □ |
| 5 | Test | 111.123.222.123 | | | | 5 | 12/04/2016 | ANY | View | □ |
| 6 | testmib | 202.184.43.24 | | CPQSM2-MIB | | 5 | 04/10/2019 | ALL | View | □ |
| 7 | Voice | 27.54.57.3 | | SONICWALL-FIREWALL-TRAP-MIB | | 1 | 23/02/2017 | ANY | View | □ |

Showing 1 to 7 of total 7 records

*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.



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.

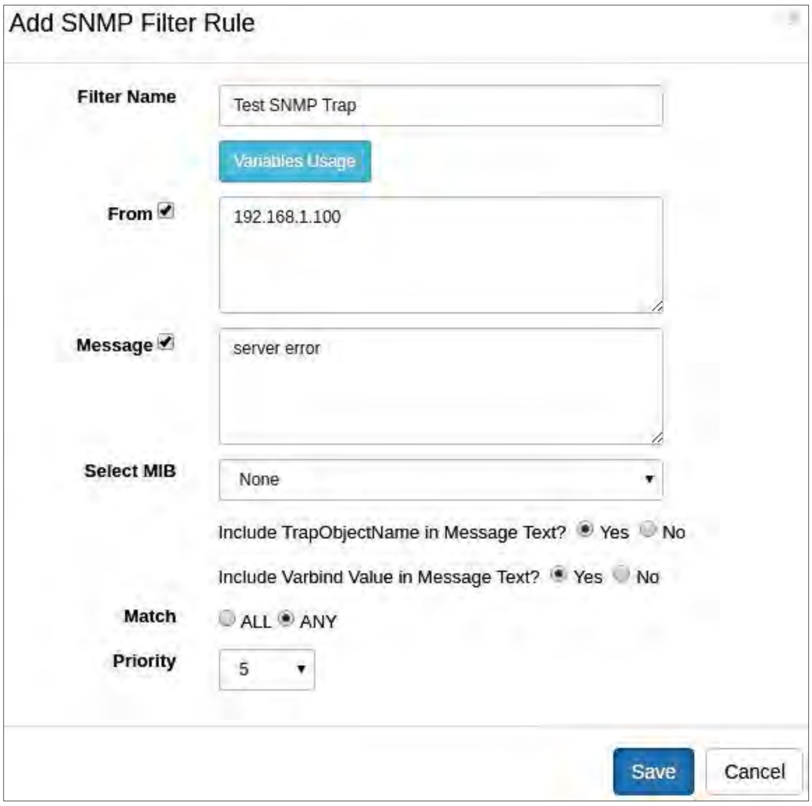
**IP Address and Port Number(optional):**

192.168.1.151
192.168.1.1
192.168.1.141

*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 Email Filter above.



Add SNMP Filter Rule

Filter Name: Test SNMP Trap

From ☑: 192.168.1.100

Message ☑: server error

Select MIB: None

Include TrapObjectName in Message Text? ● Yes ○ No

Include Varbind Value in Message Text? ● Yes ○ No

Match: ○ ALL ● ANY

Priority: 5

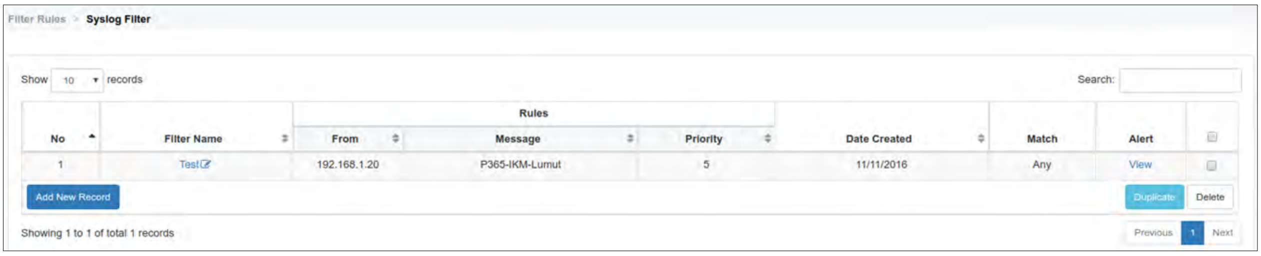
You can also upload the MIB file and select the MIB file for filtering. The MIB upload can be done by selecting **View and Upload MIB Files** in the SNMP Trap Filter Summary (Figure 9-8).

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).



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

*Figure 9-11 : Syslog Filter summary*

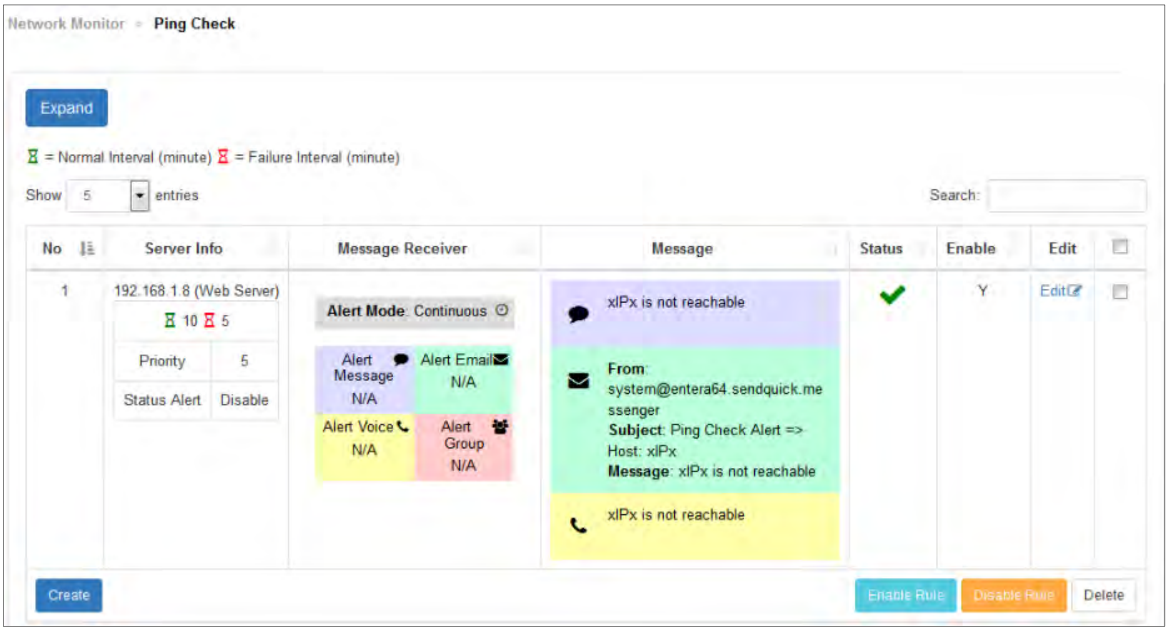
Before configuring any Syslog messages, you may wish to configure the Syslog Forwarding which will allow all incoming Syslog messages to be forwarded to another server. The interface to configure is similar to SNMP Trap as shown in Figure 9-8.

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

# 10.0 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

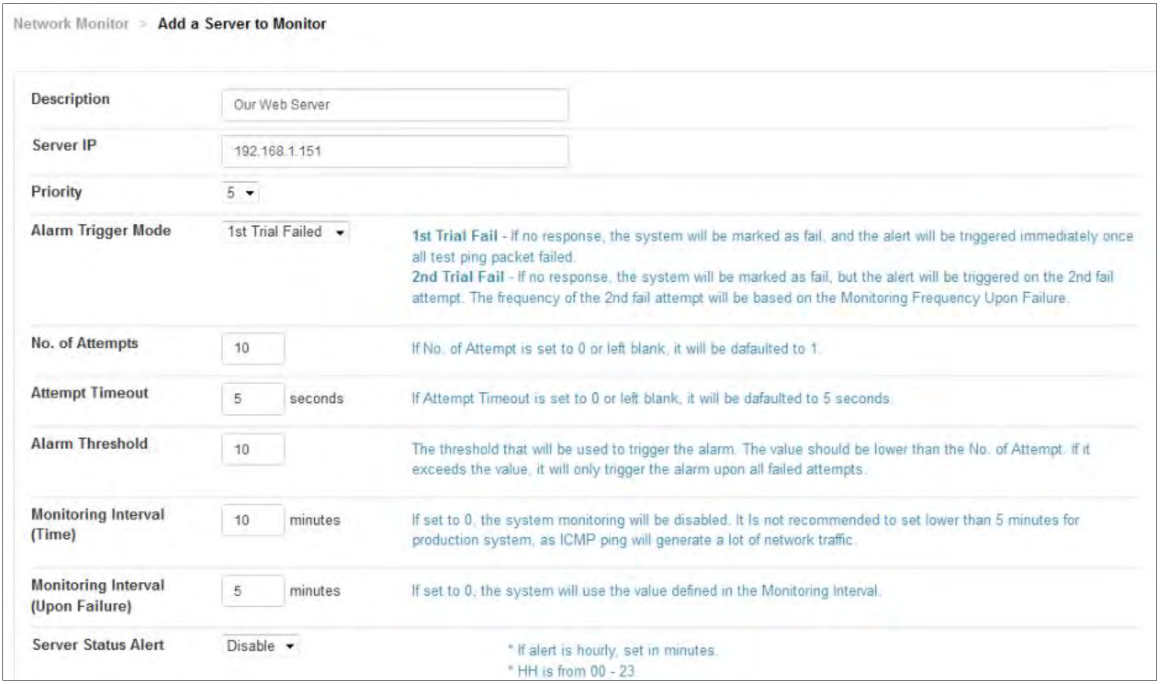
⌛ = Normal Interval (minute) ⌛ = Failure Interval (minute)

Show 5 entries Search:

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

Create  Enable Rule  Disable Rule  Delete

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.<br>**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 dafaulted to 1. |
| Attempt Timeout | 5 seconds | If Attempt Timeout is set to 0 or left blank, it will be dafaulted 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.<br>* HH is from 00 - 23 |

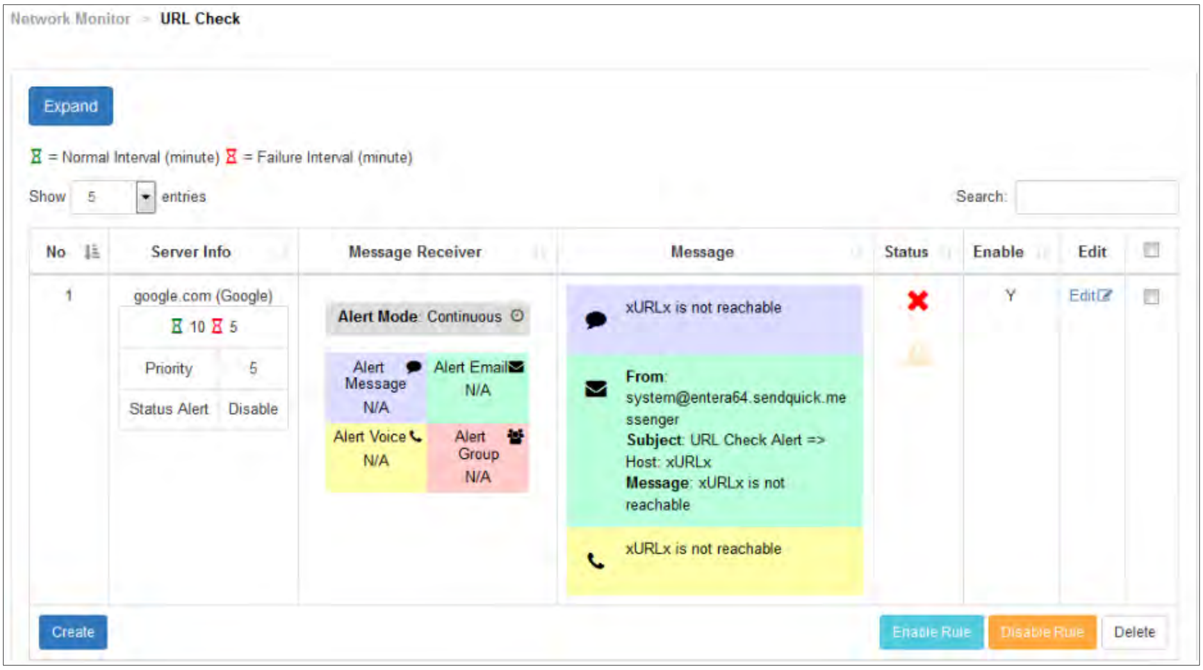
*Figure 10-2 : Add a Server to Monitor*

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.

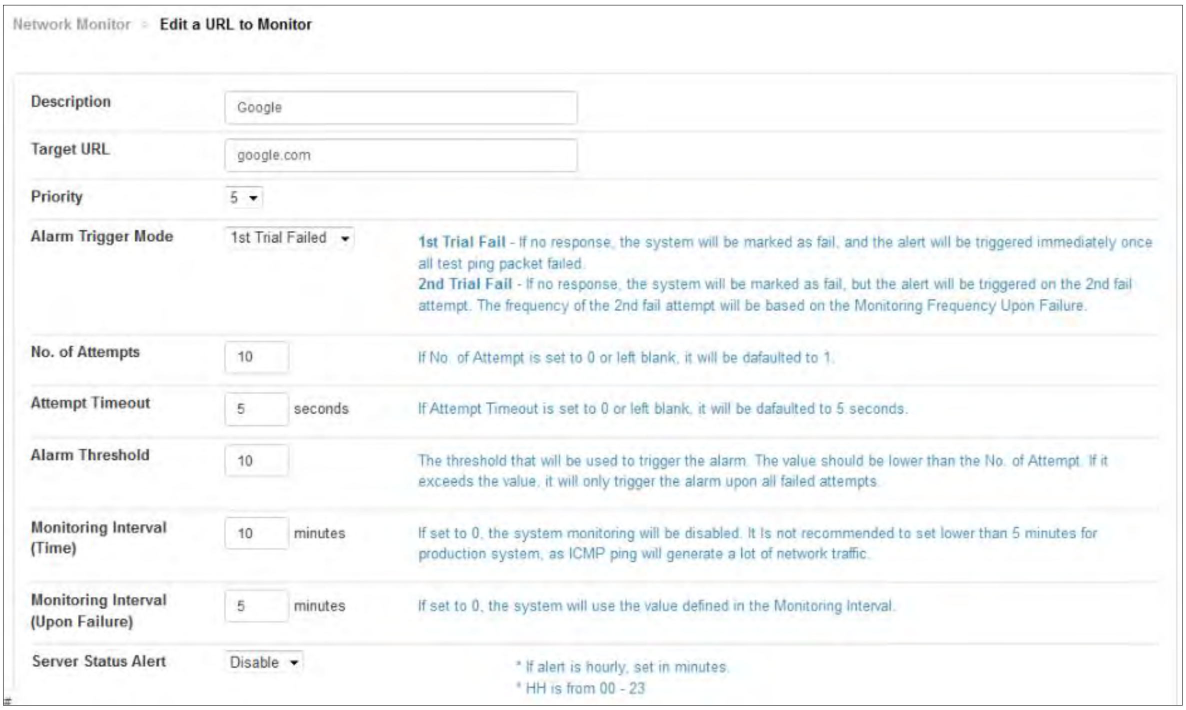


⌛ = Normal Interval (minute) ⌛ = Failure Interval (minute)

| No | Server Info | Message Receiver | Message | Status | Enable | Edit | □ |
|---|---|---|---|---|---|---|---|
| 1 | google.com (Google)<br>⌛ 10 ⌛ 5<br>Priority 5<br>Status Alert Disable | **Alert Mode**: Continuous<br>Alert Message N/A<br>Alert Email N/A<br>Alert Voice N/A<br>Alert Group N/A | xURLx is not reachable<br>**From**: system@entera64.sendquick.messenger<br>**Subject**: URL Check Alert => Host: xURLx<br>**Message**: xURLx is not reachable<br>xURLx is not reachable | ✖ | Y | Edit | □ |

*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**

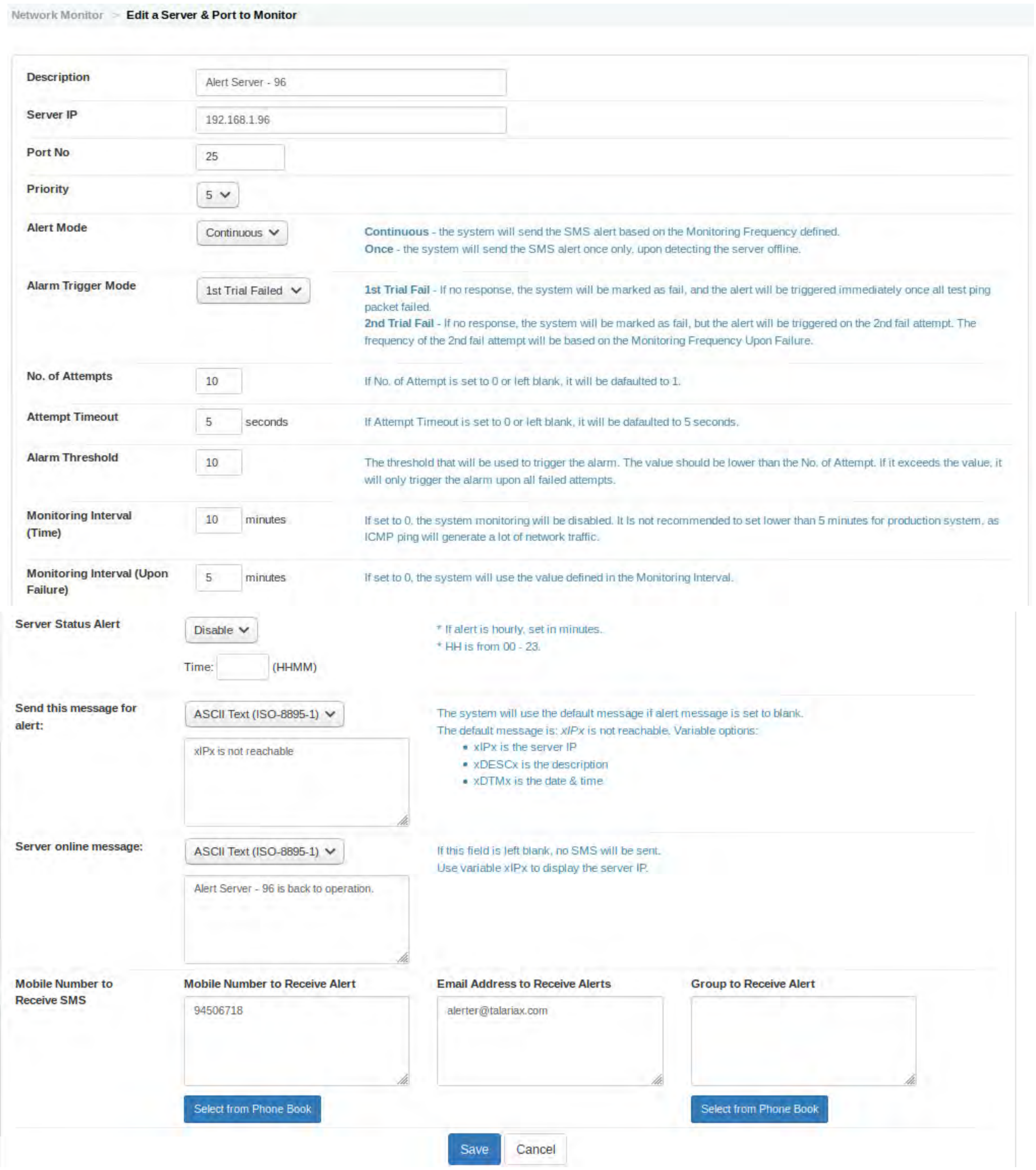
| | | |
|---|---|---|
| **Description** | Google | |
| **Target URL** | google.com | |
| **Priority** | 5 ▾ | |
| **Alarm Trigger Mode** | 1st Trial Failed ▾ | **1st Trial Fail** - If no response, the system will be marked as fail, and the alert will be triggered immediately once all test ping packet failed.<br>**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 dafaulted to 1. |
| **Attempt Timeout** | 5 seconds | If Attempt Timeout is set to 0 or left blank, it will be dafaulted 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.<br>* 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.<br>**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.<br>**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 dafaulted to 1. |
| **Attempt Timeout** | 5 seconds | If Attempt Timeout is set to 0 or left blank, it will be dafaulted 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<br>Time: (HHMM) | * If alert is hourly, set in minutes.<br>* HH is from 00 - 23. |
| **Send this message for alert:** | ASCII Text (ISO-8895-1)<br>xIPx is not reachable | The system will use the default message if alert message is set to blank.<br>The default message is: *xIPx* is not reachable. Variable options:<br>• xIPx is the server IP<br>• xDESCx is the description<br>• xDTMx is the date & time |
| **Server online message:** | ASCII Text (ISO-8895-1)<br>Alert Server - 96 is back to operation. | If this field is left blank, no SMS will be sent.<br>Use variable xIPx to display the server IP. |

| | | | |
|---|---|---|---|
| **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 |

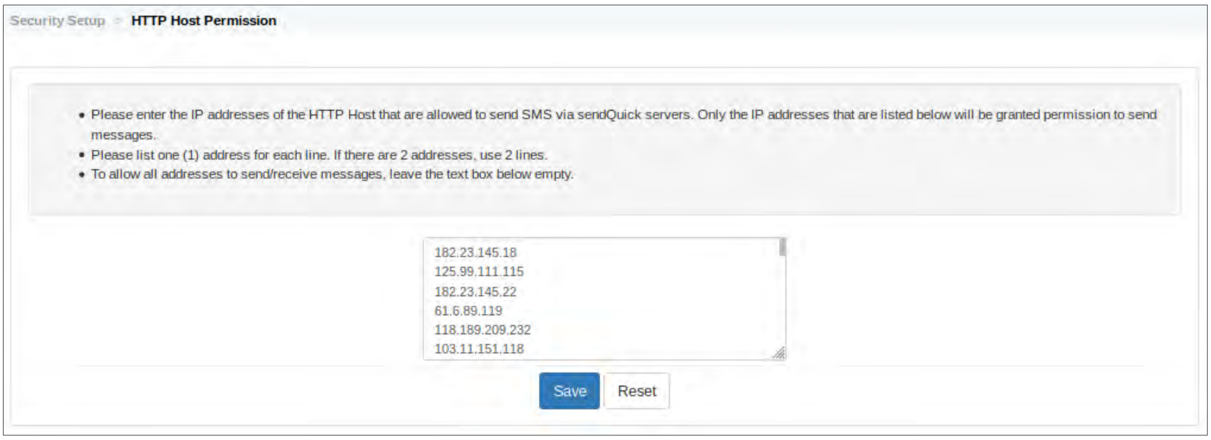
*Figure 10-5 : Add a Server to Monitor setting*

| 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.<br>Once Only refers to sending SMS only one time when a check is failed.<br>Continuous will send SMS for every check attempt that failed.<br>*Note: The checking process will continue even if the response is failed.* |
| Alarm Trigger Mode | Configurable to trigger on the first time or the second time failure.<br>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.<br>*Note: Email alerts will be sent together if the Phone Book entry contains email addresses.* |

# 11.0 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 and allowing only those specified to have access.



- 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
```

*Figure 11-1 : HTTP Host Permission*

Insert the IP addresses of those 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. Any IP address **NOT** in this list will be blocked.

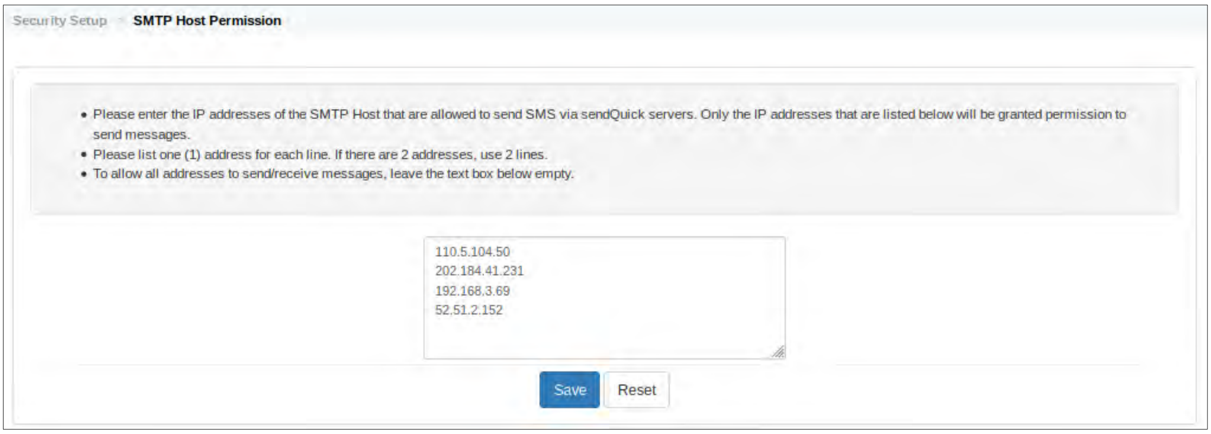
If the text box is left empty, it will allow any IP addresses to have access.

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) and allowing only those specified to have access.



- 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
```

*Figure 11-2 : SMTP Host Permission*

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. Any IP address **NOT** in this list will be blocked.

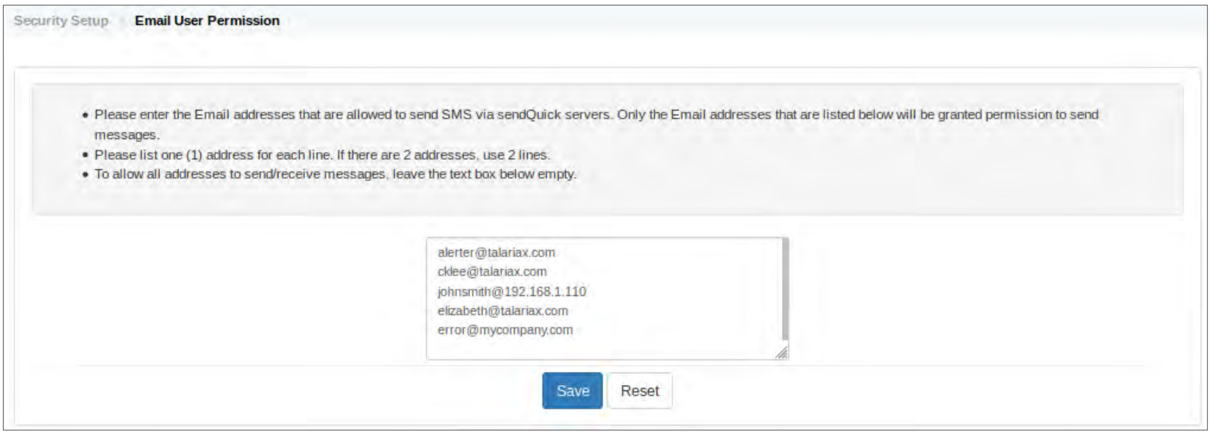
If the text box is left empty, it will allow any IP addresses to have access.

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 unauthorised access and allowing only those emails listed to have access.



- Please enter the Email addresses that are allowed to send SMS via sendQuick servers. Only the Email 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.

```
alerter@talariax.com
cklee@talariax.com
johnsmith@192.168.1.110
elizabeth@talariax.com
error@mycompany.com
```

Insert the email addresses allowed to send messages 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. Any email address **NOT** in this list will be blocked.

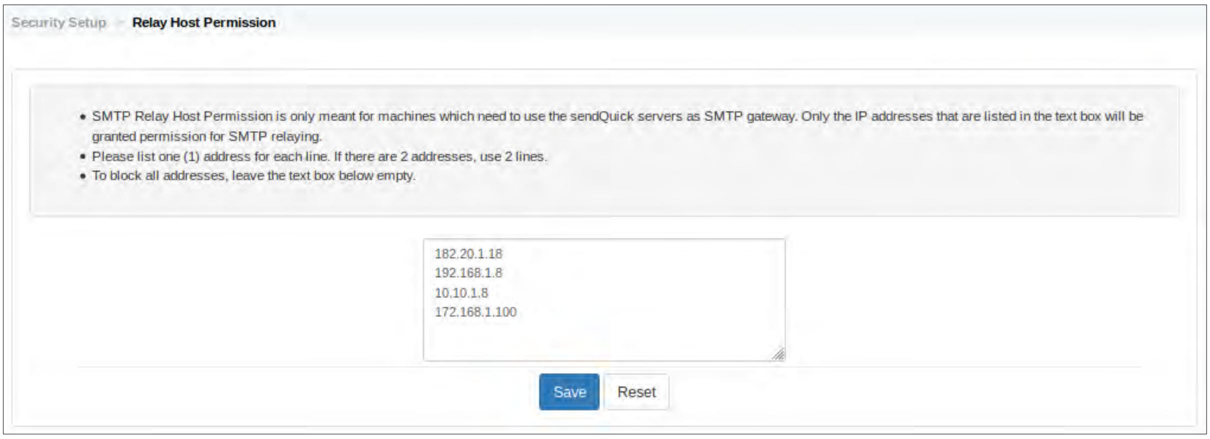
If the text box is left empty, any email addresses will be allowed access to send SMS.

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) and allowing only those specified to have access.



- 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
```

*Figure 11-4 : Relay Host Permission*

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. Any IP address **NOT** in this list will be blocked.

*Figure 11-3 : Email User Permission*

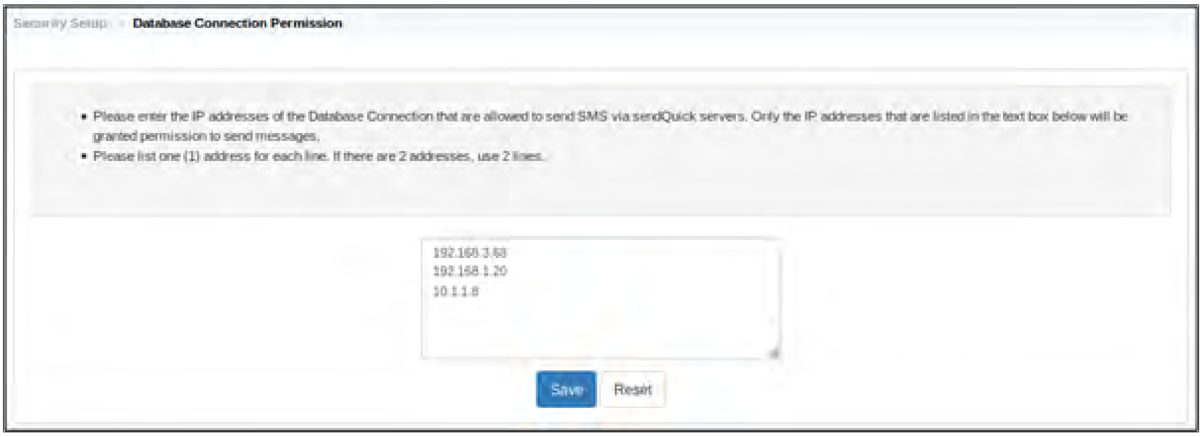
If the text box is left empty, it will block **ALL** IP addresses to have access.

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 and allowing only those specified to have 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.

```
192.168.3.63
192.168.1.20
10.1.1.8
```

*Figure 11-5 : Database Connection Permission*

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. Any IP address **NOT** in this list will be blocked.

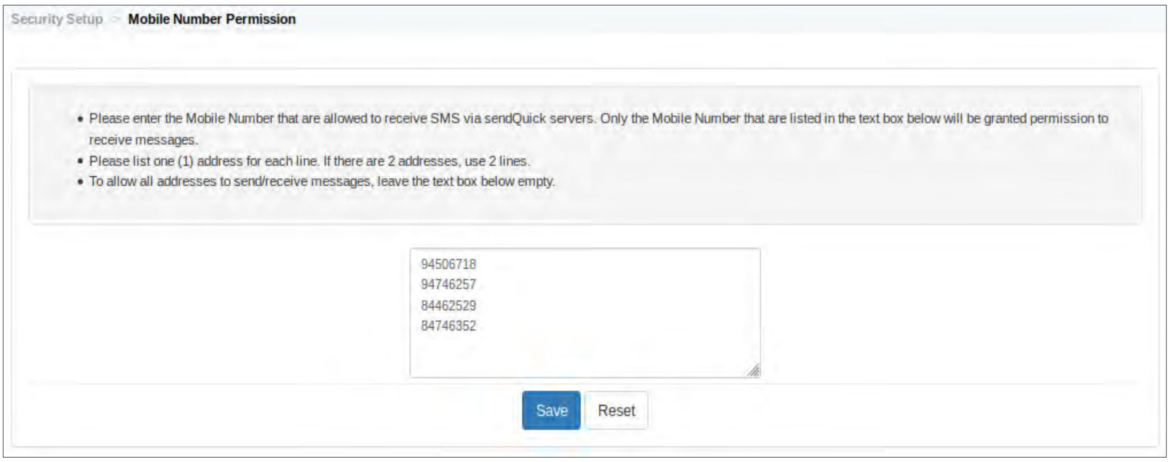
If the text box is left empty, no ODBC connection is allowed.

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 no 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. Only the mobile numbers that are listed in the text box will be granted permission to receive messages.



- Please enter the Mobile Number that are allowed to receive SMS via sendQuick servers. Only the Mobile Number that are listed in the text box below will be granted permission to receive 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.

```
94506718
94746257
84462529
84746352
```

*Figure 11-6 : Mobile Number Permission*

Enter the mobile numbers that are allowed to receive messages in 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.

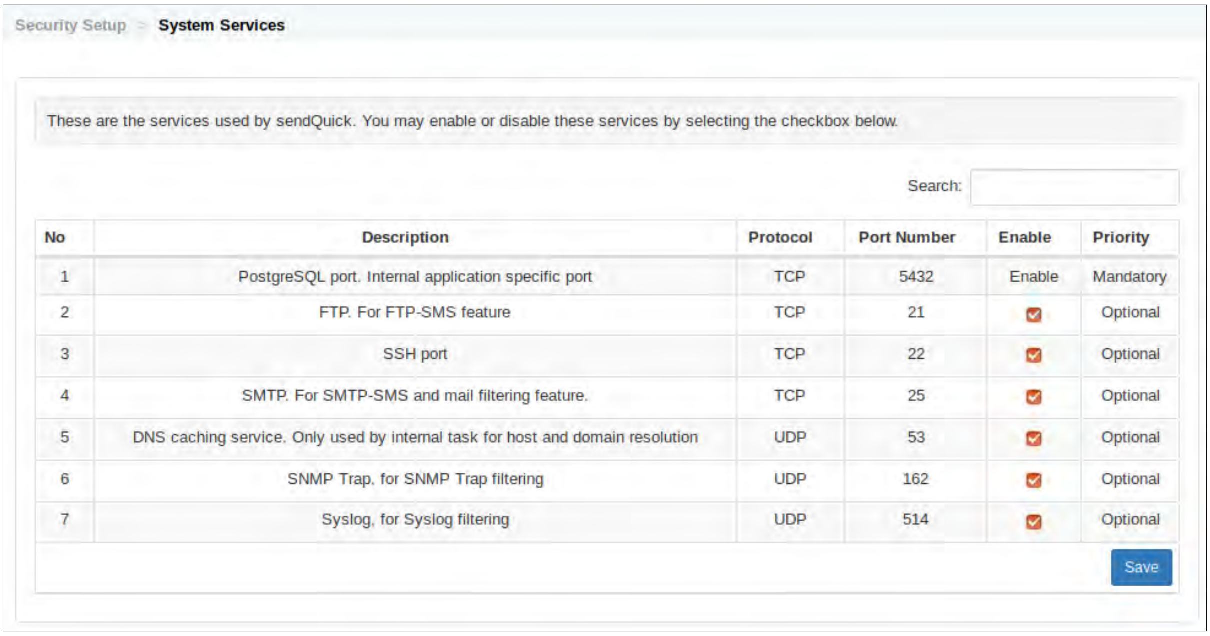
If the text box is left empty, any mobile number will be allowed access to receive SMS.

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.



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

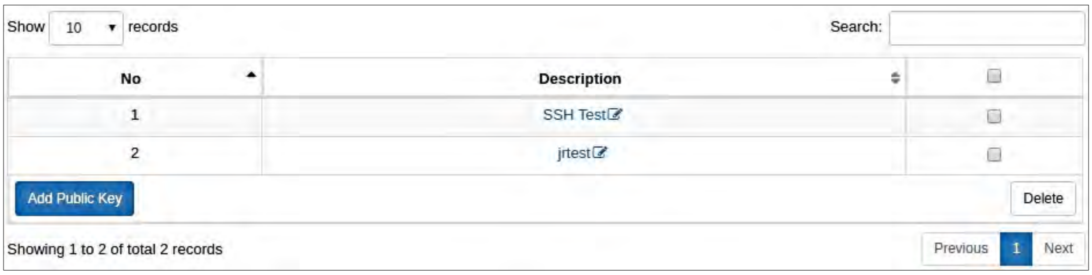
| No | Description | Protocol | Port Number | Enable | Priority |
|---|---|---|---|---|---|
| 1 | PostgreSQL port. Internal application specific port | TCP | 5432 | Enable | Mandatory |
| 2 | FTP. For FTP-SMS feature | TCP | 21 | ☑ | Optional |
| 3 | SSH port | TCP | 22 | ☑ | Optional |
| 4 | SMTP. For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

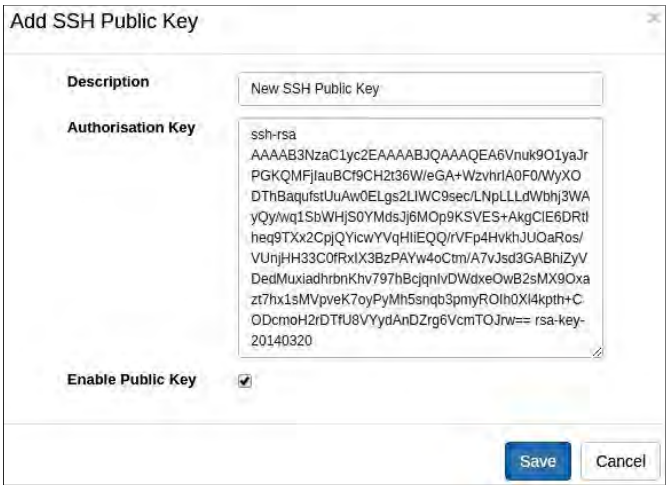


| No | Description | □ |
|---|---|---|
| 1 | SSH Test | □ |
| 2 | jrtest | □ |

Showing 1 to 2 of total 2 records

*Figure 11-8 : SSH Remote Access*

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.



Add SSH Public Key

Description: New SSH Public Key

Authorisation Key:

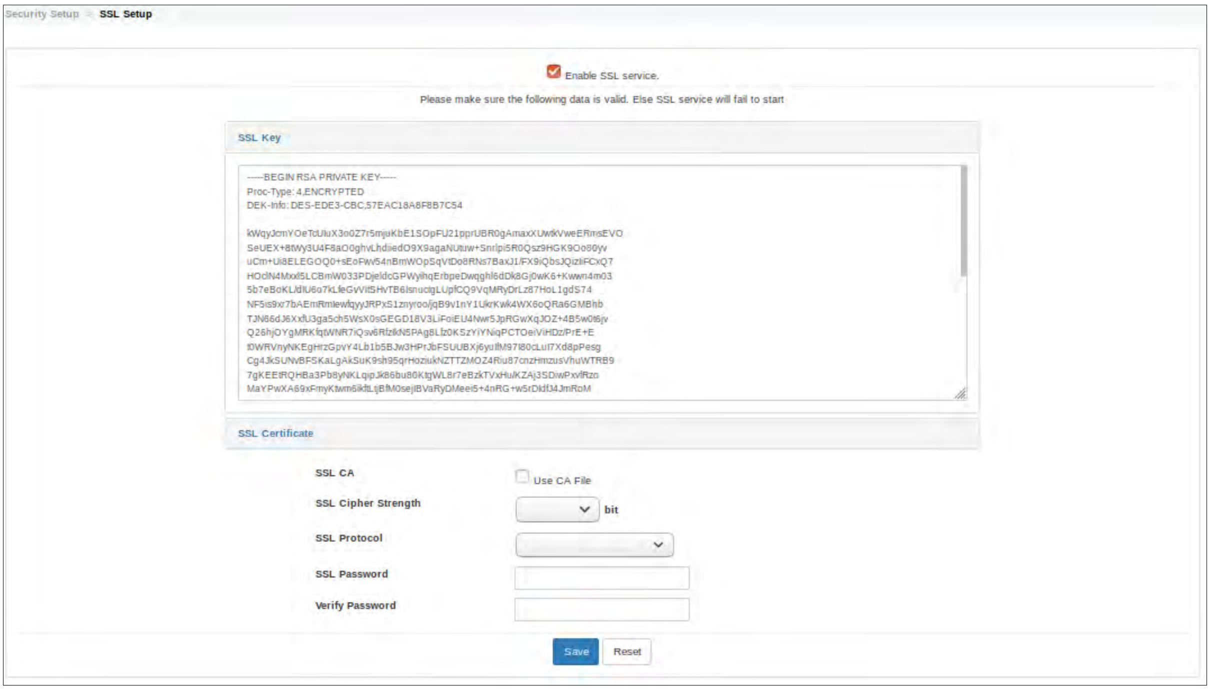
```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEA6Vnuk9O1yaJr
PGKQMFjIauBCf9CH2t36W/eGA+WzvhrIA0F0/WyXO
DThBaqufstUuAw0ELgs2LIWC9sec/LNpLLLdWbhj3WA
yQy/wq1SbWHjS0YMdsJj6MOp9KSVES+AkgClE6DRtl
heq9TXx2CpjQYicwYVqHIiEQQ/rVFp4HvkhJUOaRos/
VUnjHH33C0fRxIX3BzPAYw4oCtm/A7vJsd3GABhiZyV
DedMuxiadhrbnKhv797hBcjqnIvDWdxeOwB2sMX9Oxa
zt7hx1sMVpveK7oyPyMh5snqb3pmyROIh0XI4kpth+C
ODcmoH2rDTfU8VYydAnDZrg6VcmTOJrw== rsa-key-
20140320
```

Enable Public Key: ☑

*Figure 11-9 : Add SSH Public Key*

## 11.9 How to enable SSL Service

sendQuick support SSL / HTTPS by 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.



☑ 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

kWqyJcmYOeTdUluX3o0Z7r5mjuKbE1SOpFU21pprUBR0gAmaxXUwtkVweERmsEVO
SeUEX+8tWy3U4F8aO0ghvLhdiiedO9X9agaNUtuw+Snrlpi5R0Qsz9HGK9Oo80yv
uCm+Ui8ELEGOQ0+sEoFwv54nBmWOpSqVtDo8RNs7BaxJ1/FX9iQbsJQizIiFCxQ7
HOdN4Mxd5LCBmW033PDjeldoGPWyihqErbpeDwqghl6dDk8Gj0wK6+Kwwn4m03
5b7eBoKL/dlU6o7kLfeGvVltSHvTB6lsnuclgLUpfCQ9VqMRyDrLz87HoL1gdS74
NF5is9xr7bAEmRmlewfqyyJRPxS1znyroo/jqB9v1nY1UkrKwk4WX6oQRa6GMBhb
TJN66dJ6XxfU3ga5ch5WsX0sGEGD18V3LiFoiEU4Nwr5JpRGwXqJOZ+4B5w0t6jv
Q26hjOYgMRKfqtWNR7iQsv6RfzlkN5PAg8Llz0KSzYiYNiqPCTOeiViHDz/PrE+E
t0WRVnyNKEgHrzGpvY4Lb1b5BJw3HPrJbFSUUBXj6yuIlM97I80cLuI7Xd8pPesg
Cg4JkSUNvBFSKaLgAkSuK9sh95qrHoziukNZTTZMOZ4Riu87cnzHmzusVhuWTRB9
7gKEEtRQHBa3Pb8yNKLqipJk86bu80KtgWL8r7eBzkTVxHu/KZAj3SDiwPxvlRzo
MaYPwXA69xFmyKtwm6ikltLtjBfM0sejIBVaRyDMeei5+4nRG+w5rDldfJ4JmRoM
```

SSL Certificate

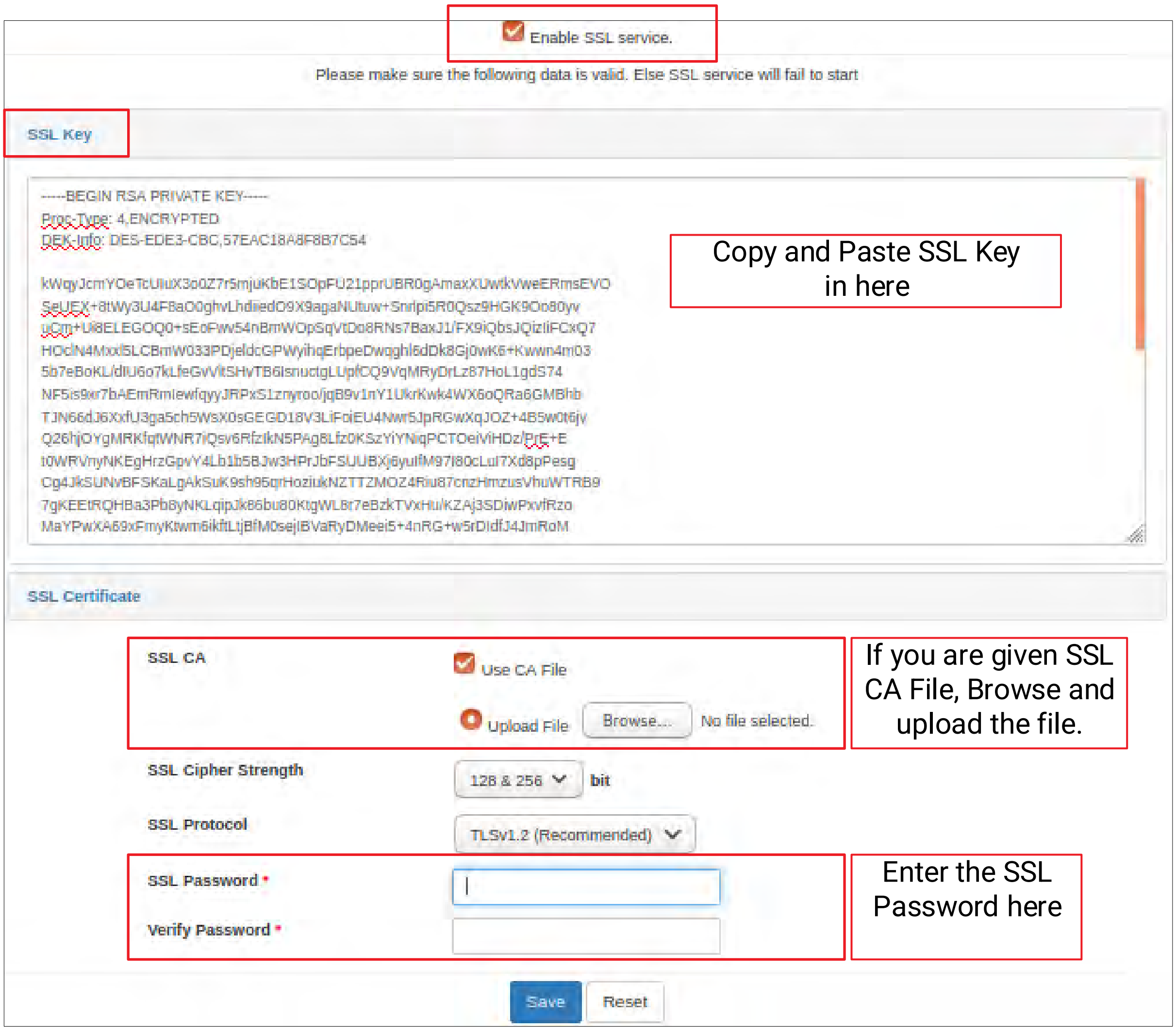
| | |
|---|---|
| SSL CA | ☐ Use CA File |
| SSL Cipher Strength | bit |
| SSL Protocol | |
| SSL Password | |
| Verify Password | |

*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

kWqyJcmYOeTcUIuX3o0Z7r5mjuKbE1SOpFU21pprUBR0gAmaxXUwtkVweERmsEVO
SeUEX+8tWy3U4F8aO0ghvLhdiiedO9X9agaNUtuw+Snrlpi5R0Qsz9HGK9Oo80yv
uCm+Ui8ELEGOQ0+sEoFwv54nBmWOpSqVtDo8RNs7BaxJ1/FX9iQbsJQizliFCxQ7
HOdN4Mxxl5LCBmW033PDjeldcGPWyihqErbpeDwqghl6dDk8Gj0wK6+Kwwn4m03
5b7eBoKL/dlU6o7kLfeGvVitSHvTB6IsnuctgLUpfCQ9VqMRyDrLz87HoL1gdS74
NF5is9xr7bAEmRmlewfqyyJRPxS1znyroo/jqB9v1nY1UkrKwk4WX6oQRa6GMBhb
TJN66dJ6XxfU3ga5ch5WsX0sGEGD18V3LiFoiEU4Nwr5JpRGwXqJOZ+4B5w0t6jv
Q26hjOYgMRKfqtWNR7iQsv6RfzIkN5PAg8Lfz0KSzYiYNiqPCTOeiViHDz/PrE+E
t0WRVnyNKEgHrzGpvY4Lb1b5BJw3HPrJbFSUUBXj6yulfM97I80cLuI7Xd8pPesg
Cg4JkSUNvBFSKaLgAkSuK9sh95qrHoziukNZTTZMOZ4Riu87cnzHmzusVhuWTRB9
7gKEEtRQHBa3Pb8yNKLqipJk86bu80KtgWL8r7eBzkTVxHu/KZAj3SDiwPxvfRzo
MaYPwXA69xFmyKtwm6ikftLtjBfM0sejIBVaRyDMeei5+4nRG+w5rDIdfJ4JmRoM
```

Copy and Paste SSL Key in here

**SSL Certificate**

| | |
|---|---|
| SSL CA | ☑ Use CA File<br>● Upload File Browse... No file selected. |
| SSL Cipher Strength | 128 & 256 bit |
| SSL Protocol | TLSv1.2 (Recommended) |
| SSL Password * | |
| Verify Password * | |

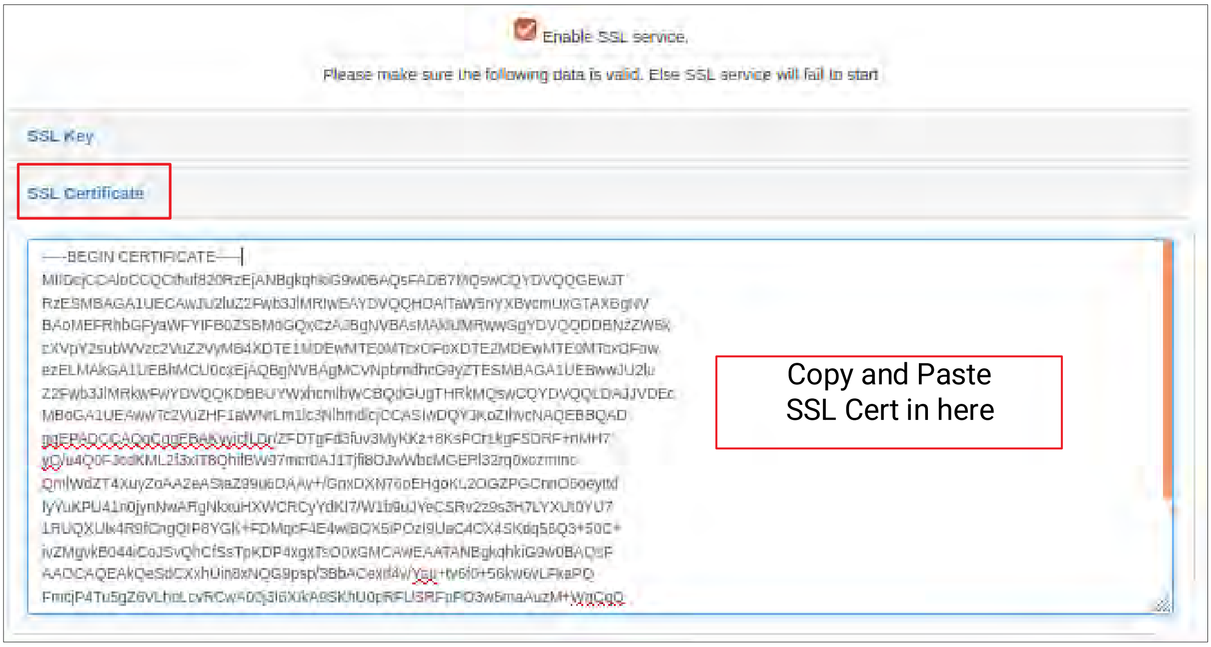
If you are given SSL CA File, Browse and upload the file.

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.



☑ Enable SSL service.

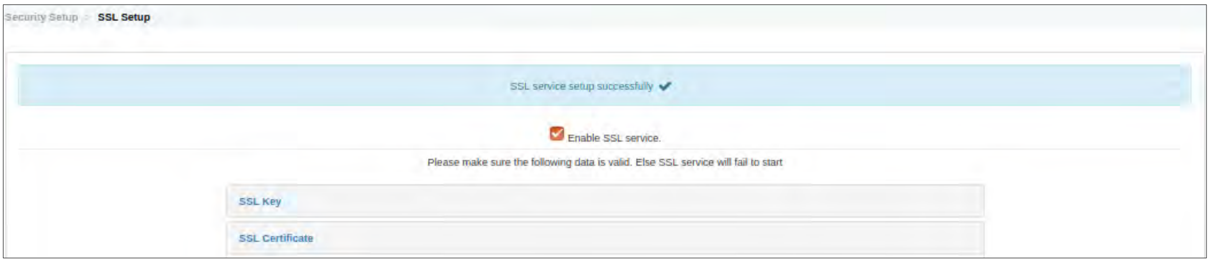
Please make sure the following data is valid. Else SSL service will fail to start

```
-----BEGIN CERTIFICATE-----
MIIDejCCAloCCQCifuf820RzEjANBgkqhkiG9w0BAQsFADB7MQswCQYDVQQGEwJT
RzESMBAGA1UECAwJU2luZ2Fwb3JlMRIwEAYDVQQHDAlTaW5nYXBvcmUxGTAXBgNV
BAoMEFRhbGFyaWFYIFB0ZSBMdGQxCzAJBgNVBAsMAklUMRwwGgYDVQQDDBNzZW5k
cXVpY2subWVzc2VuZ2VyMB4XDTE1MDEwNTE0MTcxOFoXDTE2MDEwNTE0MTcxOFow
ezELMAkGA1UEBhMCU0cxEjAQBgNVBAgMCVNpbmdhcG9yZTESMBAGA1UEBwwJU2lu
Z2Fwb3JlMRkwFwYDVQQKDBBUYWxhcmlhWCBQdGUgTHRkMQswCQYDVQQLDAJJVDEc
MBoGA1UEAwwTc2VuZHF1aWNrLm1lc3NlbmdlcjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAKwyidLDr/ZFDTgFd3fuv3MyKKz+8KsPCr1kgF5DRF+nMH7
yQ/u4Q0FJedKML2i3xIT8QhilBW97mcr0AJ1Tjfi8OJwWbcMGEPl32rq0xozminc
QmlWdZT4XuyZoAA2eA5taZ99u6DAAv+/GnxDXN76oEHgoKL2OGZPGCnnO5oeytd
IyYuKPU41n0jynNwARgNkxuHXWCRCyYdKI7/W1b9uJYeCSRv2z9s3H7LYXUt0YU7
1RUQXUk4R9fCngQIP8YGK+FDMqcF4E4wBQX5iPOzI9UaC4CX4SKdq58Q3+50C+
ivZMgvkB044iCoJSvQhCfSsTpKDP4xgxTsO0xGMCAwEAATANBgkqhkiG9w0BAQsF
AAOCAQEAkQeSdCXxhUin8xNQG9psp/3BbACexd4v/Ygu+tv6i0+56kw6vLFkaPQ
FmcjP4Tu5gZ6VLhoLcvRCwA0Qj3I6XJkA9SKhU0pRFUSRFpPO3w5maAuzM+WgCqQ
```

Copy and Paste SSL Cert in here

Figure 11-12 : SSL Setup – SSL Certificate

When the SSL service setup successfully, you can now access to sendQuick with HTTPS:



SSL service setup successfully ✓

☑ Enable SSL service.

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

Figure 11-13 : SSL Setup – SSL Enabled

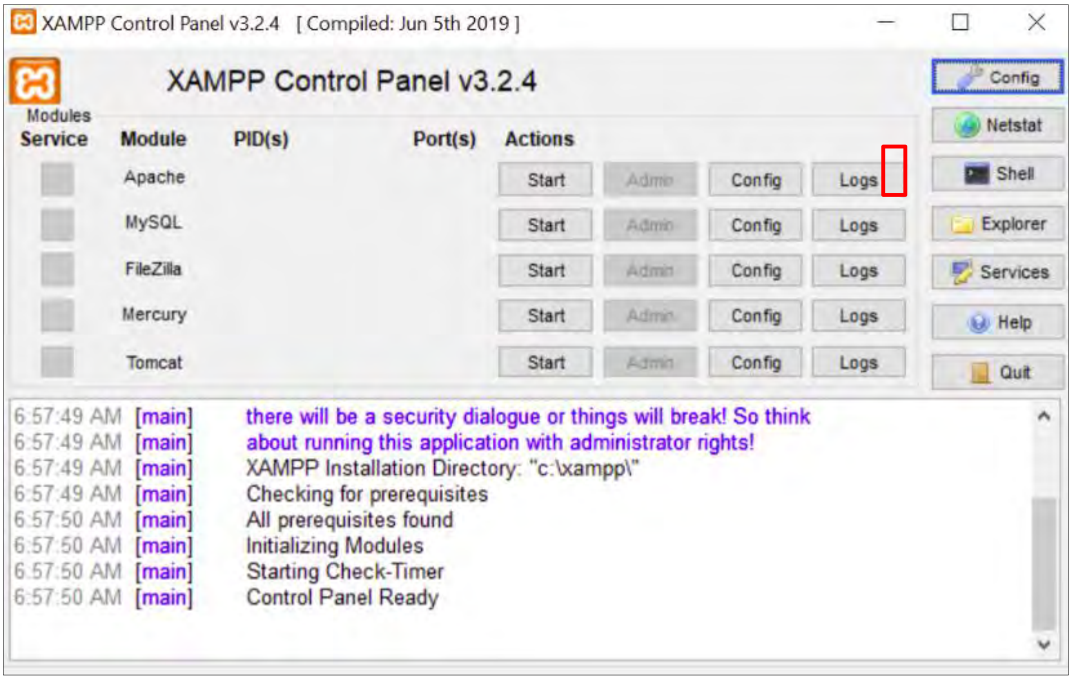
For more on how to generate SSL Key and Certificate for your own use, please refer to the next section.

### 11.9.1 How to Generate SSL Key, Certificate or CSR

***Caution**: For proper SSL certification, please purchase the required SSL Certificate from Certificate Authorities (CA) only. This example is self-signed certificate and will fail on all Vulnerability Report Test. Understand the Risk of Using Self-Signed certificate, please read more from https://en.wikipedia.org/wiki/Self-signed_certificate*

Here is a demonstration on how to generate SSL key, Cert or CSR files using XAMPP, download and install from https://www.apachefriends.org/download.html

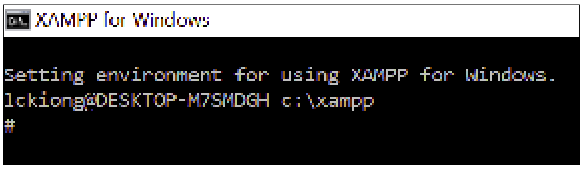
i) Access to Xampp Control Panel v3.2.4



```
6:57:49 AM  [main]   there will be a security dialogue or things will break! So think
6:57:49 AM  [main]   about running this application with administrator rights!
6:57:49 AM  [main]   XAMPP Installation Directory: "c:\xampp\"
6:57:49 AM  [main]   Checking for prerequisites
6:57:50 AM  [main]   All prerequisites found
6:57:50 AM  [main]   Initializing Modules
6:57:50 AM  [main]   Starting Check-Timer
6:57:50 AM  [main]   Control Panel Ready
```

*Figure 11-14 : XAMPP Control Panel*

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

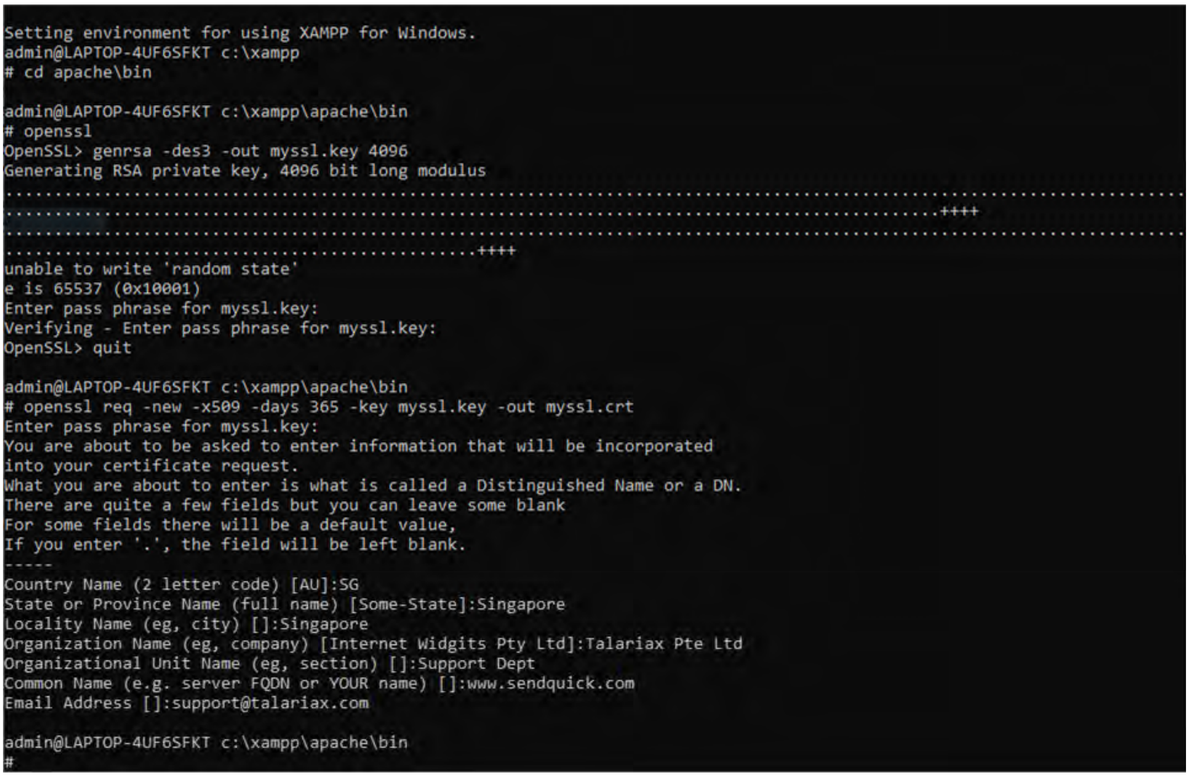


```
Setting environment for using XAMPP for Windows.
lckiong@DESKTOP-M7SMDGH c:\xampp
#
```

*Figure 11-15 : XAMPP Shell command prompt*

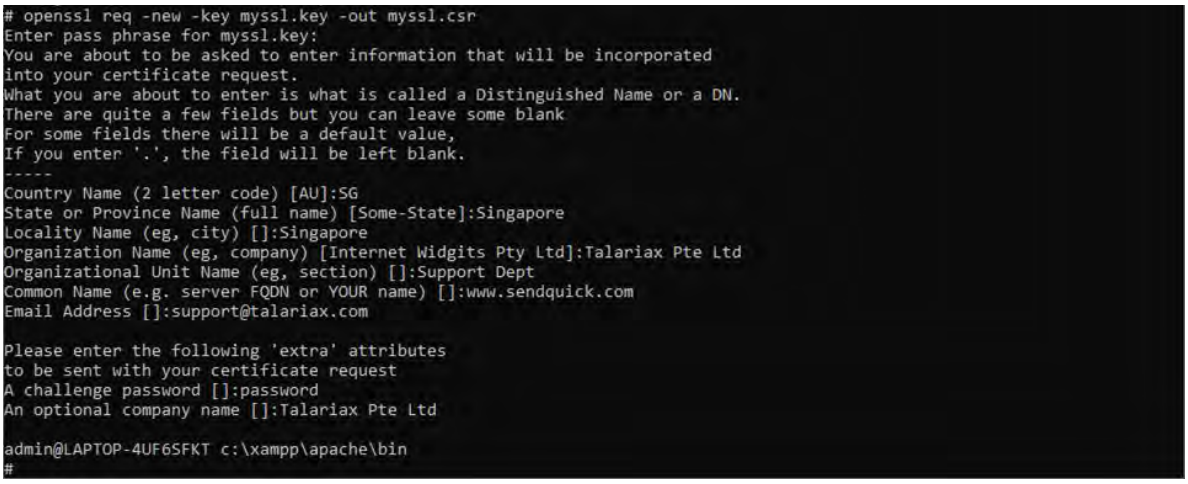
iii) System prompted : ~@DESKTOP-M7SMDGH c:\xampp, basically the login name@computer name, can ignore.

| Use the following commands accordingly when prompted: | |
|---|---|
| **when prompted** | **Command / Sample Data for referance only** |
| # cd apache\bin | Change working folder to c:\apache\bin so that your will know where to copy the generated 'myssl files'. |
| # openssl | Command to active the openssl |
| OpenSSL> genrsa -des3 -out myssl.**key** 2048 | To generate 2048 bits 'myssl.key', replace the filename for your own 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 > quit | exit the OpenSSL prompt |
| # 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. |
| # openssl req -new -key myssl.**key** -out myssl.**csr**<br>or<br># openssl req -sha256 -new -key myssl.**key** -out myssl.**csr** | To generate 'myssl.csr'.<br>or<br>-sha256 option is to use SHA2 fingerprints. |
| Enter pass phrase for myssl.**key**: | Enter the password of the 'myssl.key' (eg: password) |
| *You are about to be asked to enter information that will be incorporated into your certificate request.*<br>*What you are about to enter is what is called a Distinguished Name or a DN.*<br>*There are quite a few fields but you can leave some blank*<br>*For some fields there will be a default value,*<br>*If you enter '.', the field will be left blank. -----* | |
| Country Name (2 letter code) [AU]: | SG (example) |
| State or Province Name (full name) [Some-State]: | Singapore (example) |
| Locality Name (eg, city) []: | Singapore (example) |
| Organization Name (eg, company) [Internet Widgits Pty Ltd]: | Talariax Pte Ltd (example) |
| Organizational Unit Name (eg, section) []: | Support Dept (example) |
| Common Name (e.g. server FQDN or YOUR name) []: | sendQuick's Host+Domain.<br>Server Name, eg: 'sendquick.messenger', the fully qualified domain name that clients will use to reach your server. For example, to secure https://www.example.com, your common name must be www.example.com or *.example.com for a wildcard certificate. |
| Email Address []: | support@talariax.com (example) |



```
Setting environment for using XAMPP for Windows.
admin@LAPTOP-4UF6SFKT c:\xampp
# cd apache\bin

admin@LAPTOP-4UF6SFKT 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> quit

admin@LAPTOP-4UF6SFKT 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) []:www.sendquick.com
Email Address []:support@talariax.com

admin@LAPTOP-4UF6SFKT c:\xampp\apache\bin
#
```

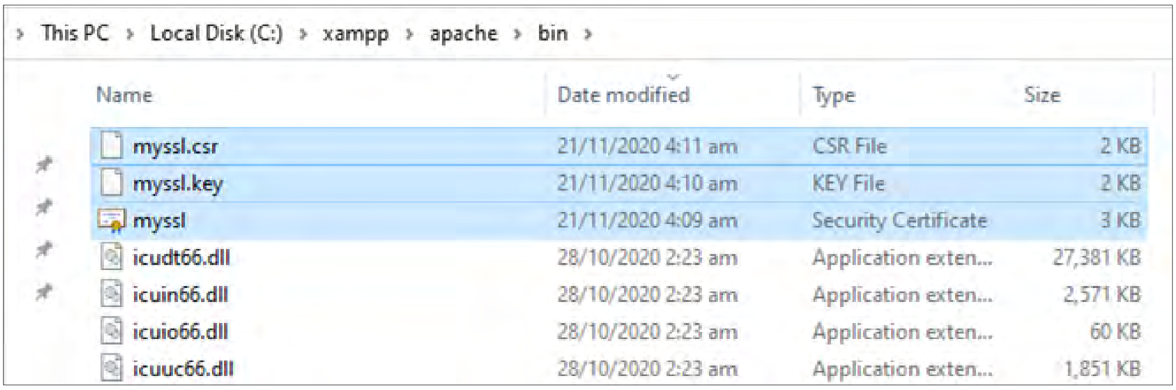
Figure 11-16 : SSL key and cert generator



```
# openssl req -new -key myssl.key -out myssl.csr
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) []:www.sendquick.com
Email Address []:support@talariax.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:password
An optional company name []:Talariax Pte Ltd

admin@LAPTOP-4UF6SFKT c:\xampp\apache\bin
#
```

Figure 11-17 : SSL key and CSR generator

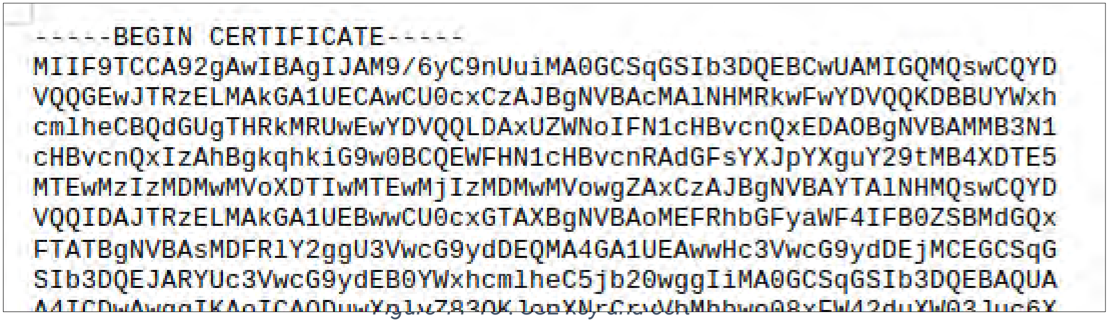
v) access to C:\xampp\apache\bin, copy the **myssl.key, myssl.crt** and **myssl.csr** to desktop



› This PC › Local Disk (C:) › xampp › apache › bin ›

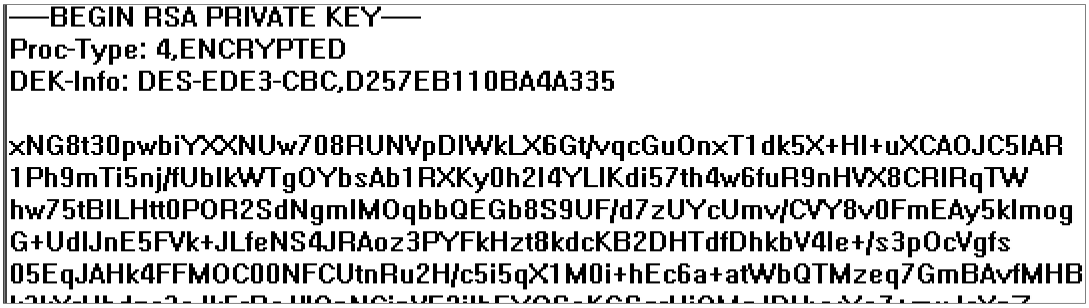
| Name | Date modified | Type | Size |
|---|---|---|---|
| myssl.csr | 21/11/2020 4:11 am | CSR File | 2 KB |
| myssl.key | 21/11/2020 4:10 am | KEY File | 2 KB |
| myssl | 21/11/2020 4:09 am | Security Certificate | 3 KB |
| icudt66.dll | 28/10/2020 2:23 am | Application exten... | 27,381 KB |
| icuin66.dll | 28/10/2020 2:23 am | Application exten... | 2,571 KB |
| icuio66.dll | 28/10/2020 2:23 am | Application exten... | 60 KB |
| icuuc66.dll | 28/10/2020 2:23 am | Application exten... | 1,851 KB |

vi) open the **myssl.key** and **myssl.crt** with notepad and paste to sendQuick SSL.



```
-----BEGIN CERTIFICATE-----
MIIF9TCCA92gAwIBAgIJAM9/6yC9nUuiMA0GCSqGSIb3DQEBCwUAMIGQMQswCQYD
VQQGEwJTRzELMAkGA1UECAwCU0cxCzAJBgNVBAcMAlNHMRkwFwYDVQQKDBBUYWxh
cmlheCBQdGUgTHRkMRUwEwYDVQQLDAxUZWNoIFN1cHBvcnQxEDAOBgNVBAMMB3N1
cHBvcnQxIzAhBgkqhkiG9w0BCQEWFHN1cHBvcnRAdGFsYXJpYXguY29tMB4XDTE5
MTEwMzIzMDMwMVoXDTIwMTEwMjIzMDMwMVowgZAxCzAJBgNVBAYTAlNHMQswCQYD
VQQIDAJTRzELMAkGA1UEBwwCU0cxGTAXBgNVBAoMEFRhbGFyaWF4IFB0ZSBMdGQx
FTATBgNVBAsMDFRlY2ggU3VwcG9ydDEQMA4GA1UEAwwHc3VwcG9ydDEjMCEGCSqG
SIb3DQEJARYUc3VwcG9ydEB0YWxhcmlheC5jb20wggIiMA0GCSqGSIb3DQEBAQUA
```

Figure 11-19 : Sample SSL Certificate



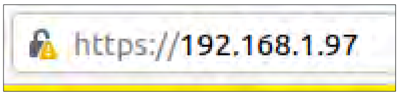
```
—BEGIN RSA PRIVATE KEY—
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,D257EB110BA4A335

xNG8t30pwbiYXXNUw708RUNVpDIWkLX6Gt/vqcGuOnxT1dk5X+HI+uXCAOJC5IAR
1Ph9mTi5nj/fUbIkWTgOYbsAb1RXKy0h2I4YLIKdi57th4w6fuR9nHVX8CRIRqTW
hw75tBILHtt0POR2SdNgmIMOqbbQEGb8S9UF/d7zUYcUmv/CVY8v0FmEAy5kImog
G+UdIJnE5FVk+JLfeNS4JRAoz3PYFkHzt8kdcKB2DHTdfDhkbV4Ie+/s3pOcVgfs
05EqJAHk4FFMOC00NFCUtnRu2H/c5i5qX1M0i+hEc6a+atWbQTMzeq7GmBAvfMHB
```

Figure 11-20 : Sample SSL key

Refer to Section **11.9** – SSL Setup on how to setup SSL key and cert on sendQuick.

### 11.9.2 How do I know if https is enabled?

If the URL begins with “https” instead of “http,” then the site is secured using an SSL certificate. A padlock icon displayed in a web browser also indicates that a site has a secure connection with an SSL certificate.

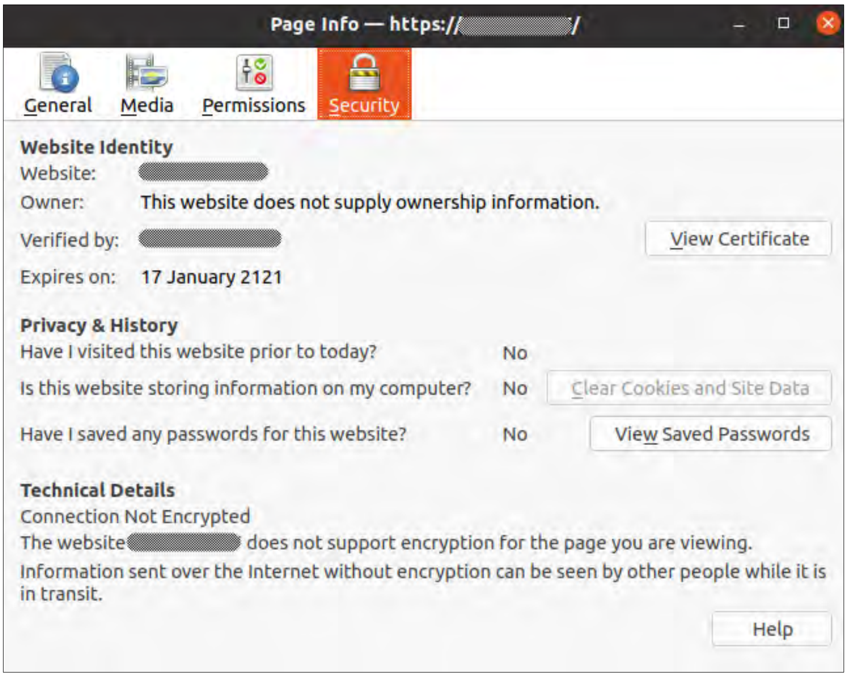


https://192.168.1.97

*Figure 11-21: Site installed with SSL*

### 11.9.3 How do I check my SSL certificate details?

Clicking the padlock in the address bar brings up a preliminary dropdown that indicates a secure connection when properly configured SSL is in place. Click the arrow to the right of the dropdown to view more information about the certificate.



Page Info — https://[redacted]/

**Website Identity**

Website: [redacted]

Owner: This website does not supply ownership information.

Verified by: [redacted]

Expires on: 17 January 2121

**Privacy & History**

Have I visited this website prior to today? No

Is this website storing information on my computer? No

Have I saved any passwords for this website? No

**Technical Details**

Connection Not Encrypted

The website [redacted] does not support encryption for the page you are viewing.

Information sent over the Internet without encryption can be seen by other people while it is in transit.

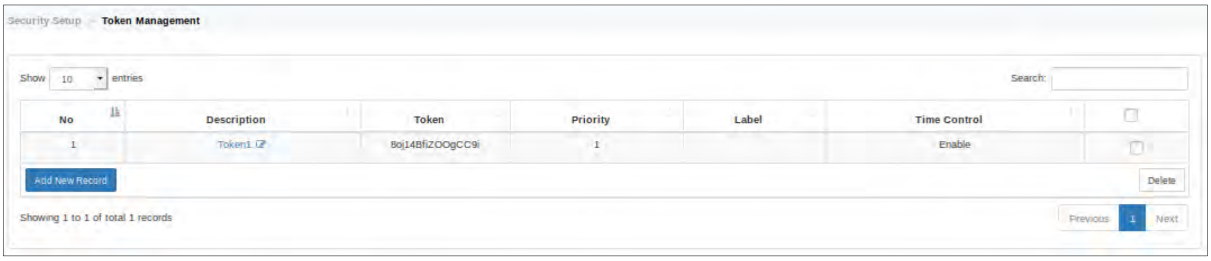
*Figure 11-22 : SSL’s Page Info*

### 11.9.4 How to View SSL Certificate Details in Each Browser ?

Refer to https://www.globalsign.com/en/blog/how-to-view-ssl-certificate-details

### 11.9.5 Token Management

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



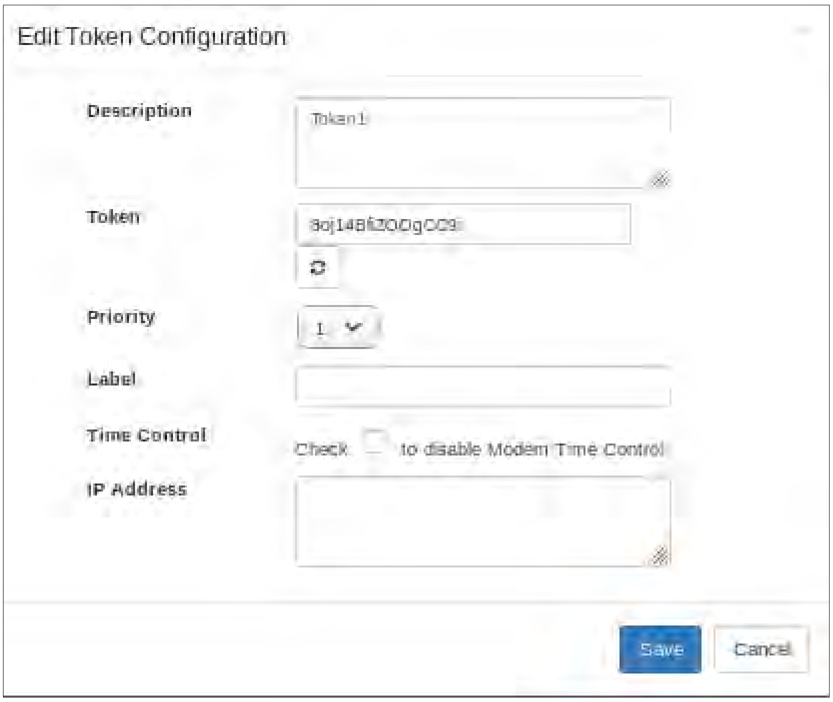
Security Setup Token Management

Show 10 entries Search:

| No | Description | Token | Priority | Label | Time Control | □ |
|---|---|---|---|---|---|---|
| 1 | Token1 | 8oj14BfiZOOgCC9i | 1 |  | Enable | □ |

Showing 1 to 1 of total 1 records

Figure 11-23 : Token Management screen



Edit Token Configuration

Description: Token1

Token: 8oj14BfiZOOgCC9i

Priority: 1

Label:

Time Control: Check □ to disable Modem Time Control

IP Address:

Figure 11-24 : Edit Token Configuration screen

# 12.0 Password Management

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

| User Type | User Name | Description |
|---|---|---|
| Server Admin Web login | admin | Password for web administrator login.<br>The default login name and password can be found in the "Your Password" envelope or contact support@talariax.com.<br>Reset password will be your sendQuick's serial number.<br>Access rights: Full access on Server Administration. |
| Supervisor web login | supervisor | Password for Supervisor access.<br>(No default password, please set before use)<br>Access rights: Full access as 'admin' but cannot change the admin's password. |
| Operator Web login | operator | Password for web operator access.<br>(No default password, please set before use)<br>Access rights: Read only access to view the SMS Queue and Sent log. |
| Console login | admin | Password for console login using direct monitor and keyboard or serial cable. Check with our technical support if you do not know the password |
| SSH Login Account | sqguest | Password for access via SSH for limited SSH and web shell access.<br>(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.<br>(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**

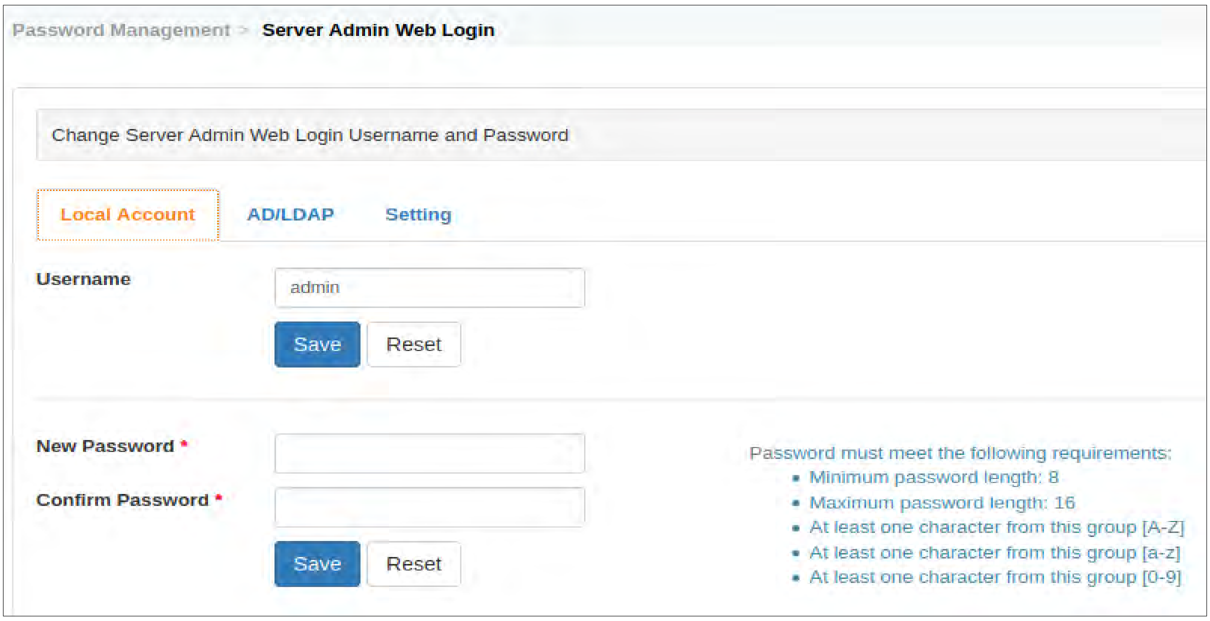
sendQuick support both Administrator and Operator user type for ease of management. The access rights of both user types are as below.

| **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 least one character from this group [0-9]



Password Management > **Server Admin Web Login**

Change Server Admin Web Login Username and Password

**Username**: admin

**New Password** *

**Confirm Password** *

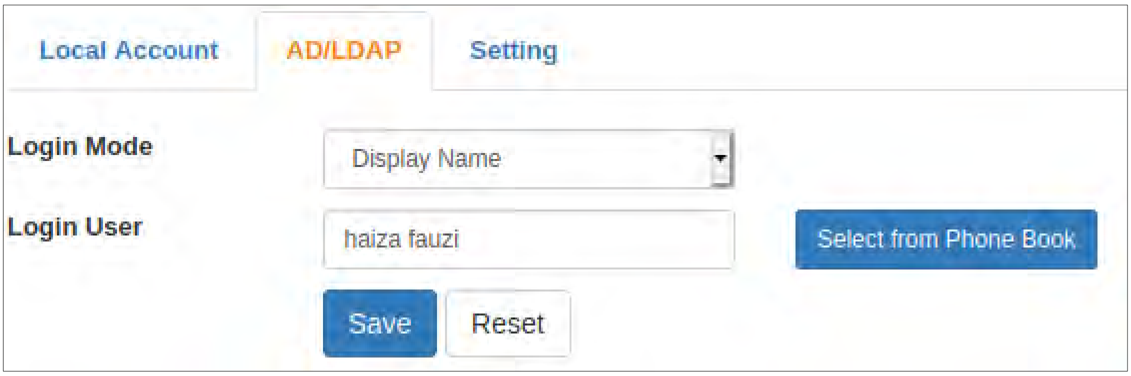
Password must meet the following requirements:

- 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 12-1 : 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 Section 8.1.2 Phone Book Records – by AD/LDAP Setup on how to import AD/LDAP data to Phone Book.*



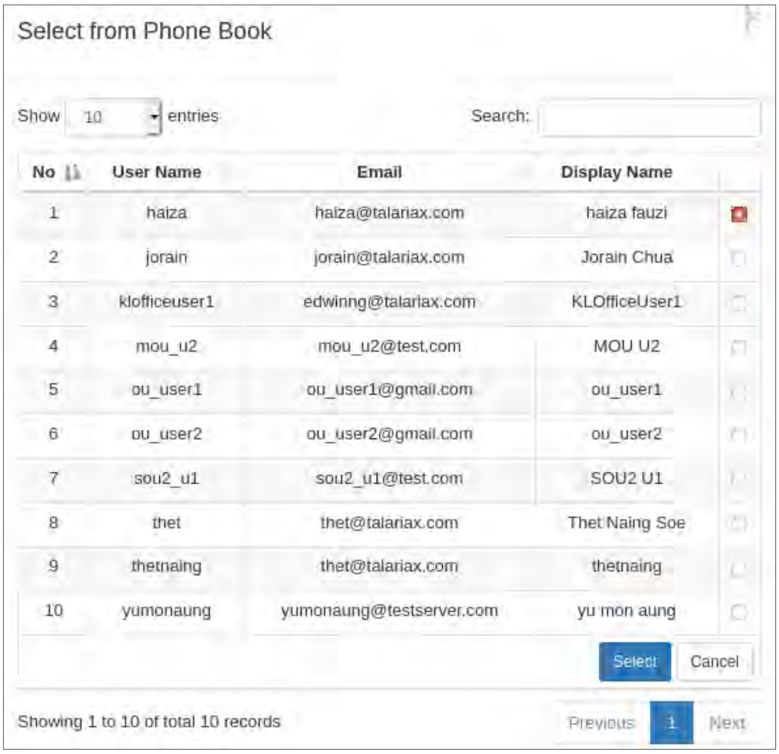
**Login Mode**: Display Name

**Login User**: haiza fauzi

*Figure 12-2 : 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' list, pick and Select a name from Phone Book:



Select from Phone Book

Show 10 entries Search:

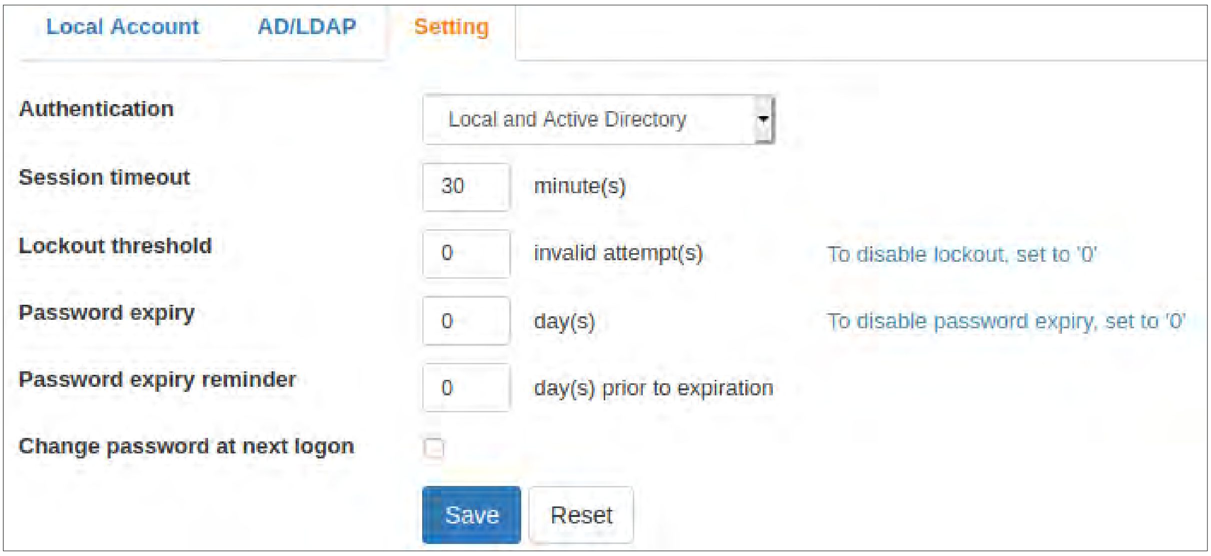
| No | User Name | Email | Display Name | |
|---|---|---|---|---|
| 1 | haiza | haiza@talariax.com | haiza fauzi | ☒ |
| 2 | jorain | jorain@talariax.com | Jorain Chua | □ |
| 3 | klofficeuser1 | edwinng@talariax.com | KLOfficeUser1 | □ |
| 4 | mou_u2 | mou_u2@test.com | MOU U2 | □ |
| 5 | ou_user1 | 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 | □ |

Showing 1 to 10 of total 10 records

*Figure 12-3 : Select From Phone Book*

Select ‘Save’ when ready from Figure 12-2, 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.



| | | | |
|---|---|---|---|
| Authentication | Local and Active Directory | | |
| Session timeout | 30 | minute(s) | |
| Lockout threshold | 0 | invalid attempt(s) | To disable lockout, set to '0' |
| Password expiry | 0 | day(s) | To disable password expiry, set to '0' |
| Password expiry reminder | 0 | day(s) prior to expiration | |
| Change password at next logon | □ | | |

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

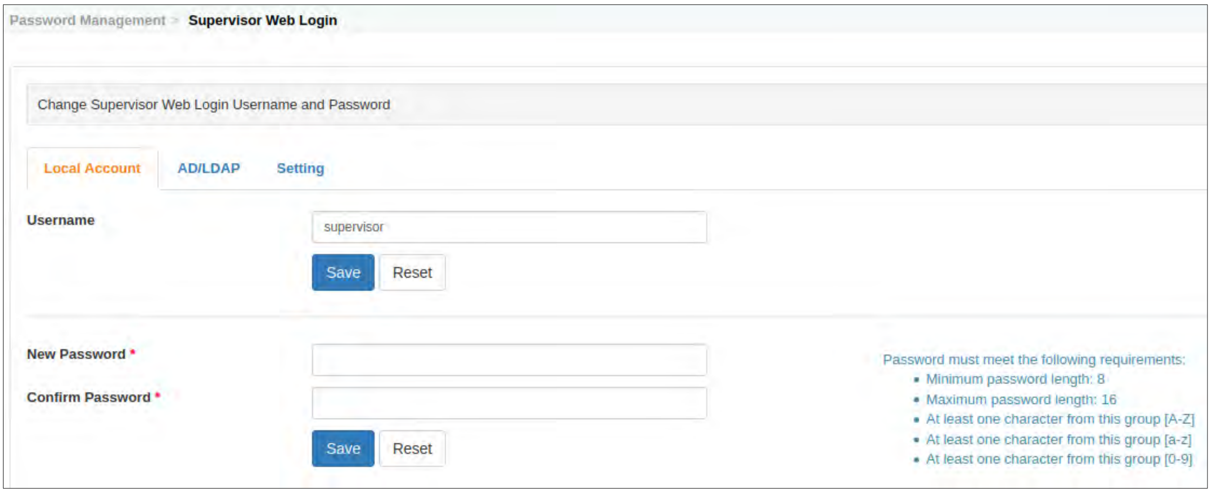
**Authentication**: Local and Active Directory / Local only / Active Directory only.
**Session timeout**: default as ‘30 minutes’.
**Lockout threshold**: Number of invalid attempt(s), to disable lockout, set to '0'.
**Password expiry**: Password will be expired in day(s) specified in this field. To disable 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 least one character from this group [0-9]


Password Management > Supervisor Web Login
Change Supervisor Web Login Username and Password
Local Account
AD/LDAP
Setting
Save
Reset
Save
Reset

Username: supervisor

New Password *

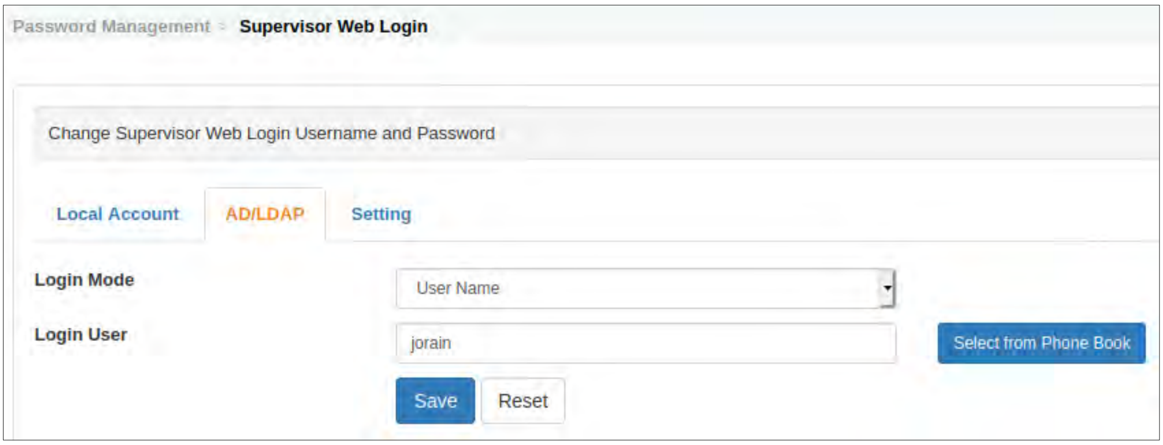
Confirm Password *

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 12-5 : 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 'Section 8.1.2 Phone Book Records – by AD/LDAP Setup' on how to import AD/LDAP data to Phone Book.*



Password Management > Supervisor Web Login

Change Supervisor Web Login Username and Password

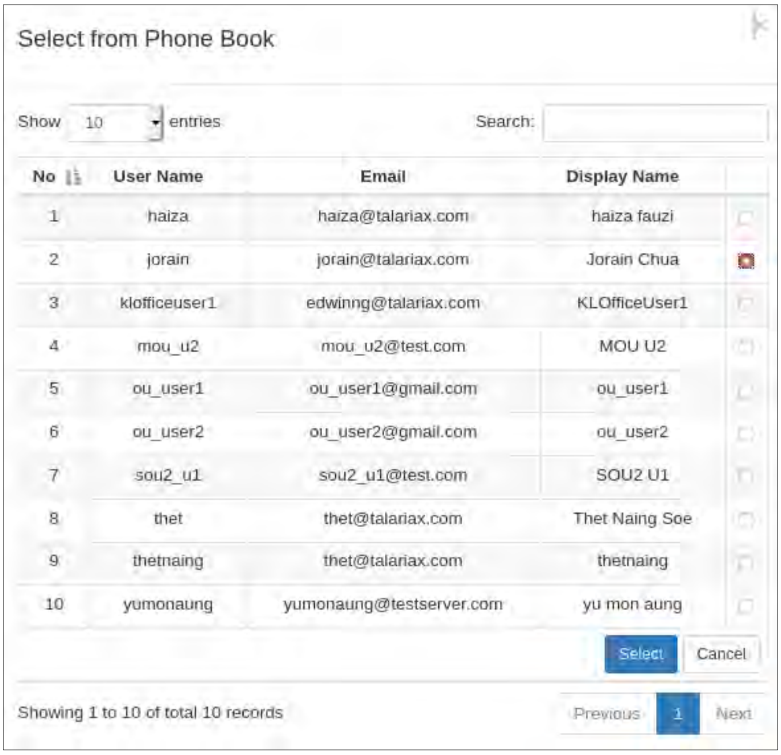
Login Mode: User Name

Login User: jorain

Figure 12-6 : 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' list, pick and Select a name from Phone Book:



Select from Phone Book

Show 10 entries

Search:

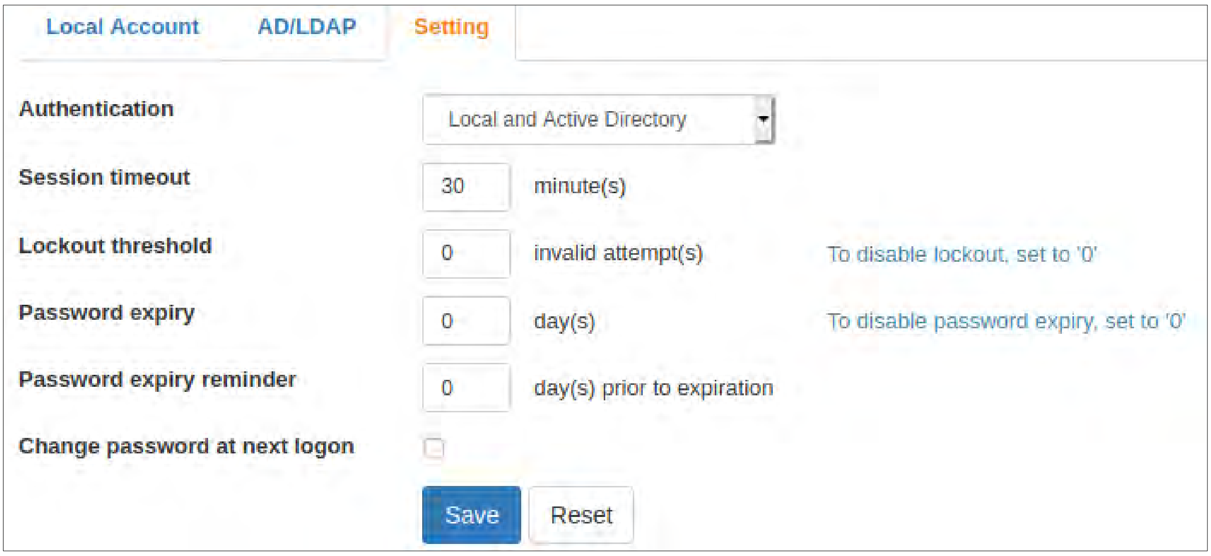
| No | User Name | Email | Display Name | |
|---|---|---|---|---|
| 1 | haiza | haiza@talariax.com | haiza fauzi | □ |
| 2 | jorain | jorain@talariax.com | Jorain Chua | ☑ |
| 3 | klofficeuser1 | edwinng@talariax.com | KLOfficeUser1 | □ |
| 4 | mou_u2 | mou_u2@test.com | MOU U2 | □ |
| 5 | ou_user1 | 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 | □ |

Showing 1 to 10 of total 10 records

Figure 12-7 : Supervisor Web Login – Phone Book

Select 'Save' when ready from Figure 12-6, 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.



Authentication: Local and Active Directory

Session timeout: 30 minute(s)

Lockout threshold: 0 invalid attempt(s) To disable lockout, set to '0'

Password expiry: 0 day(s) To disable password expiry, set to '0'

Password expiry reminder: 0 day(s) prior to expiration

Change password at next logon: □

*Figure 12-8 : 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) specified in this field. To disable password expiry, set to '0'
**Password expiry reminder**: day(s) prior to expiration.
**Change password at next logon**: checked to enable.

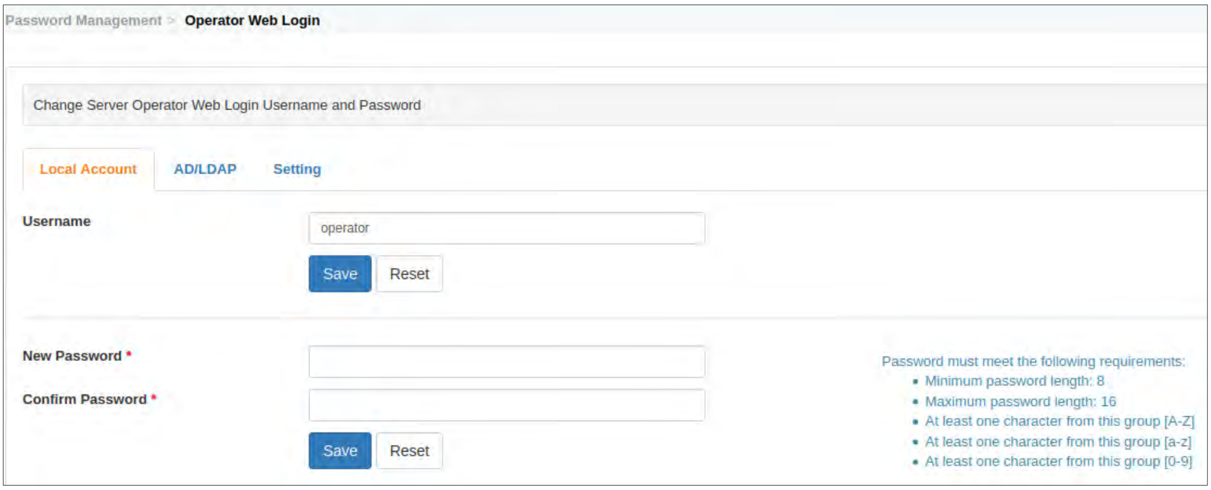
Select ‘Save’ when ready.

## 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 least one character from this group [0-9]


Password Management > Operator Web Login
Change Server Operator Web Login Username and Password
Local Account
AD/LDAP
Setting
Save
Reset
Save
Reset

Username: operator

New Password *

Confirm Password *

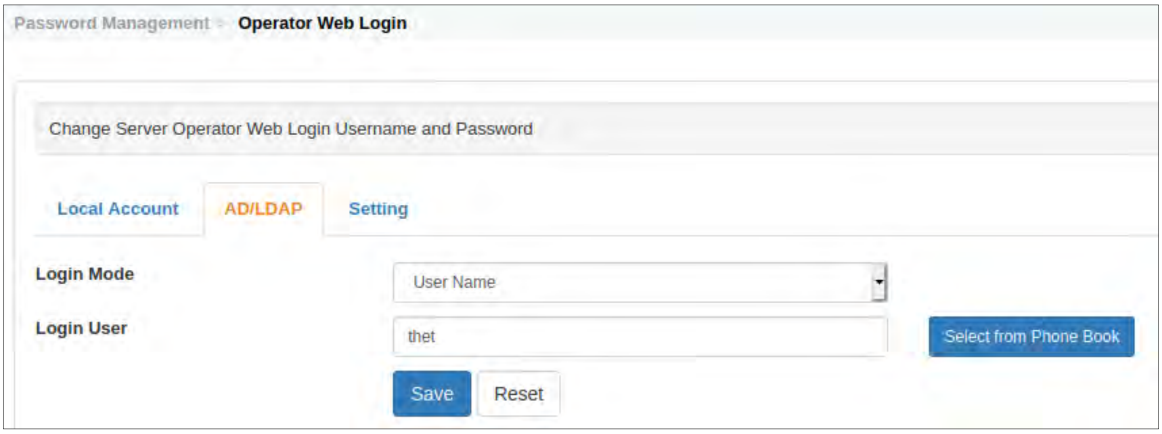
Password must meet the following requirements:

- 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 12-9 : 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 '[Section 8.1.2 Phone Book Records – by AD/LDAP Setup'](#) on how to import AD/LDAP data to Phone Book.*


Password Management > Operator Web Login
Change Server Operator Web Login Username and Password
Local Account
AD/LDAP
Setting
Select from Phone Book
Save
Reset

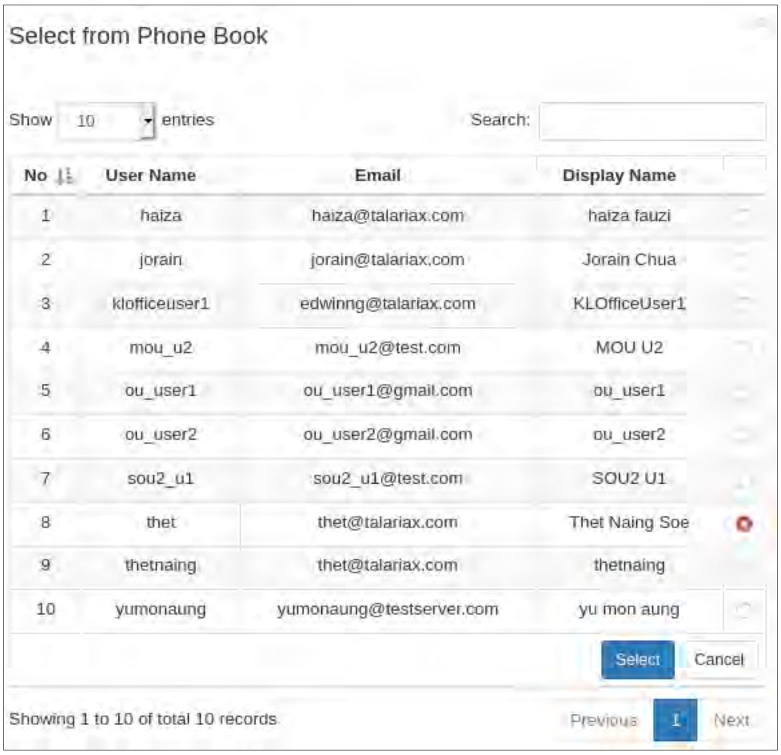
Login Mode: User Name

Login User: thet

Figure 12-10 : 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' list, pick and Select a name from Phone Book:



Select from Phone Book

Show 10 entries Search:

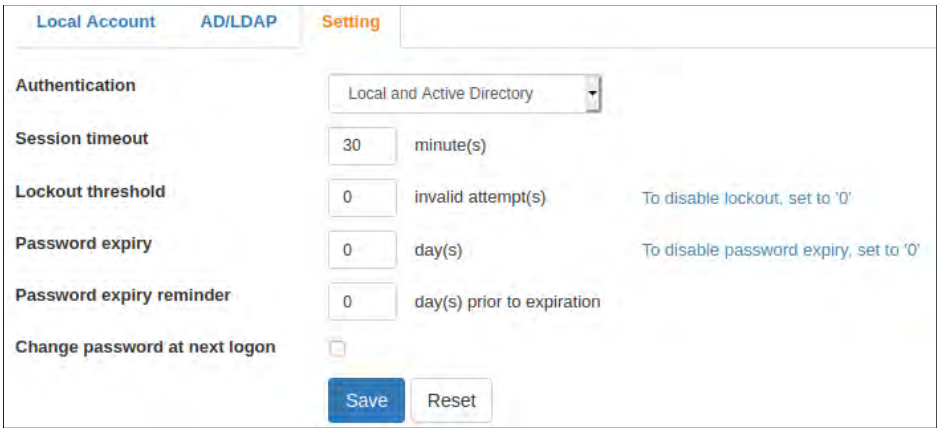
| No | User Name | Email | Display Name | |
|---|---|---|---|---|
| 1 | haiza | haiza@talariax.com | haiza fauzi | ○ |
| 2 | jorain | jorain@talariax.com | Jorain Chua | ○ |
| 3 | klofficeuser1 | edwinng@talariax.com | KLOfficeUser1 | ○ |
| 4 | mou_u2 | mou_u2@test.com | MOU U2 | ○ |
| 5 | ou_user1 | 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 | ○ |

Showing 1 to 10 of total 10 records

*Figure 12-11 : Operator Web Login – Phone Book*

Select 'Save' when ready from Figure 12-10, 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.



| | | | |
|---|---|---|---|
| Authentication | Local and Active Directory | | |
| Session timeout | 30 | minute(s) | |
| Lockout threshold | 0 | invalid attempt(s) | To disable lockout, set to '0' |
| Password expiry | 0 | day(s) | To disable password expiry, set to '0' |
| Password expiry reminder | 0 | day(s) prior to expiration | |
| Change password at next logon | □ | | |

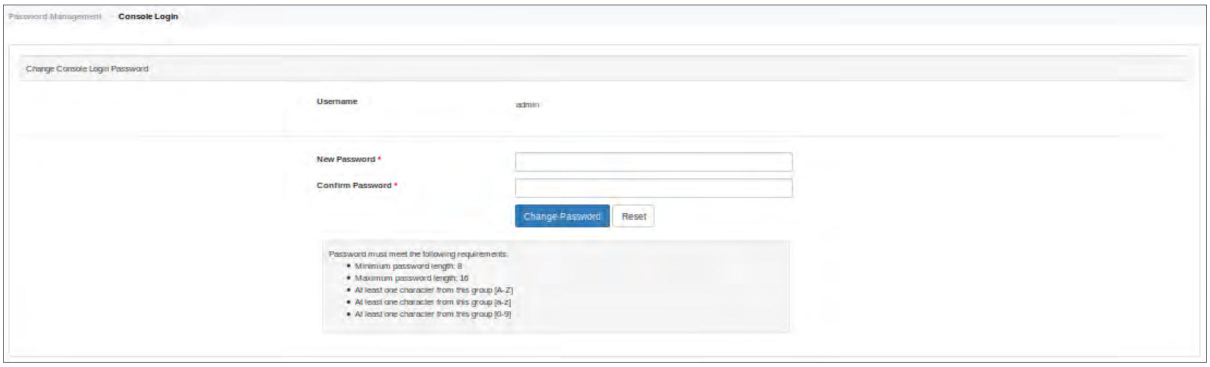
*Figure 12-12 : Server Admin Web Setting screen*

**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) specified here. 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 least one character from this group [0-9]



Username admin

New Password *

Confirm Password *

Password must meet the following requirements:

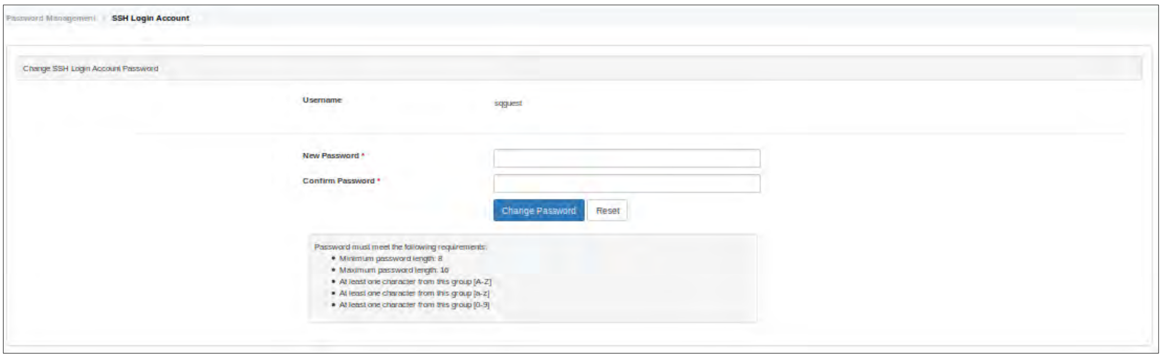
- Minimum password length: 8
- Maximum password length: 16
- At least one character from this group [A-Z]
- At least one character from this group [a-z]
- At least one character from this group [0-9]

Figure 12-13 : 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 least one character from this group [0-9]



Username sqguest

New Password *

Confirm Password *

Password must meet the following requirements:

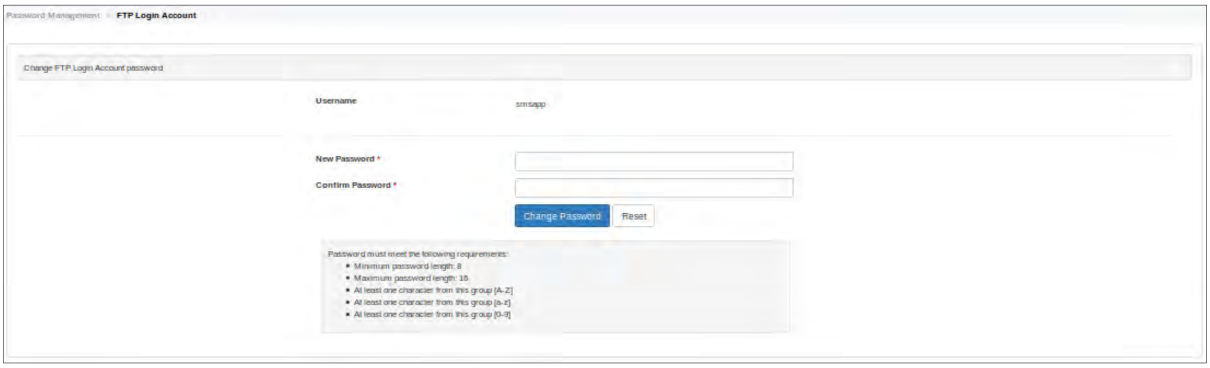
- Minimum password length: 8
- Maximum password length: 16
- At least one character from this group [A-Z]
- At least one character from this group [a-z]
- At least one character from this group [0-9]

Figure 12-14 : 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]



Change FTP Login Account password

Username: smsapp

New Password *

Confirm Password *

Password must meet the following requirements:

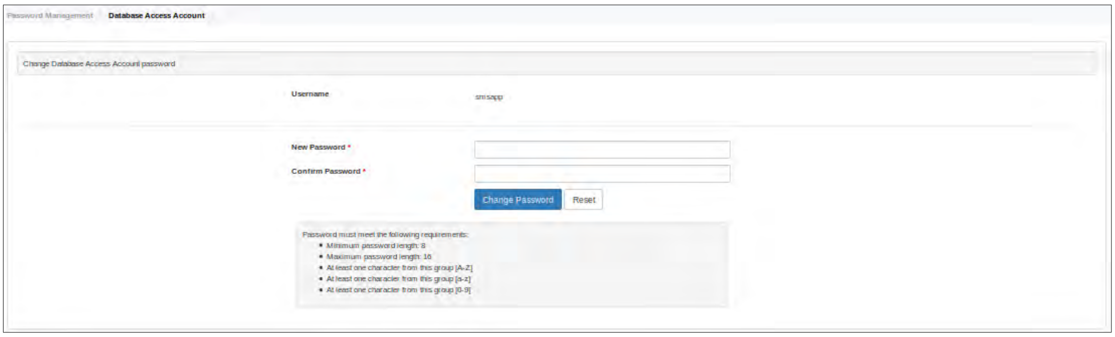
- Minimum password length: 8
- Maximum password length: 16
- At least one character from this group [A-Z]
- At least one character from this group [a-z]
- At least one character from this group [0-9]

*Figure 12-15 : 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 least one character from this group [0-9]



Change Database Access Account password

Username: smsapp

New Password *

Confirm Password *

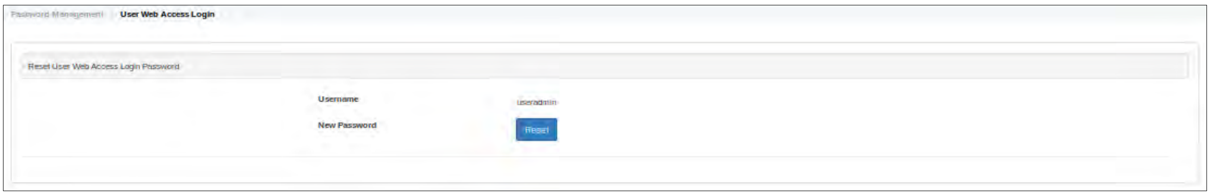
Password must meet the following requirements:

- 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 12-16 : 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.



Reset User Web Access Login Password

Username: useradmin

New Password

*Figure 12-17 : User Web Access Login*

# 13.0 Backup & Diagnostic

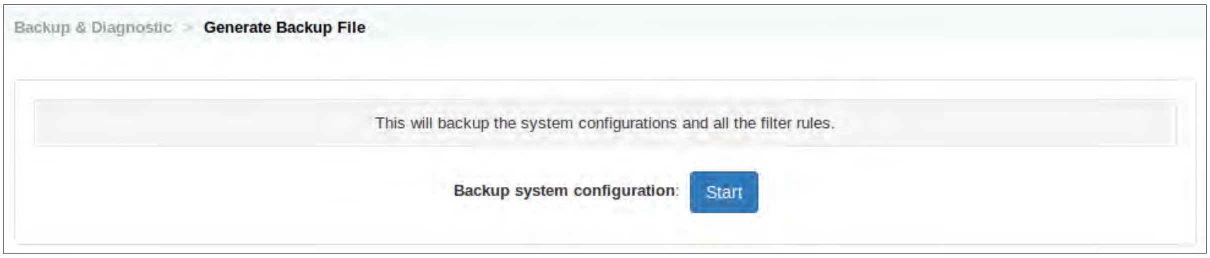
This section explains how to perform backup, restore, update and diagnostic process in sendQuick servers. To start, select Backup & Diagnostic in the navigation menu and you will see the options below.

## 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.



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

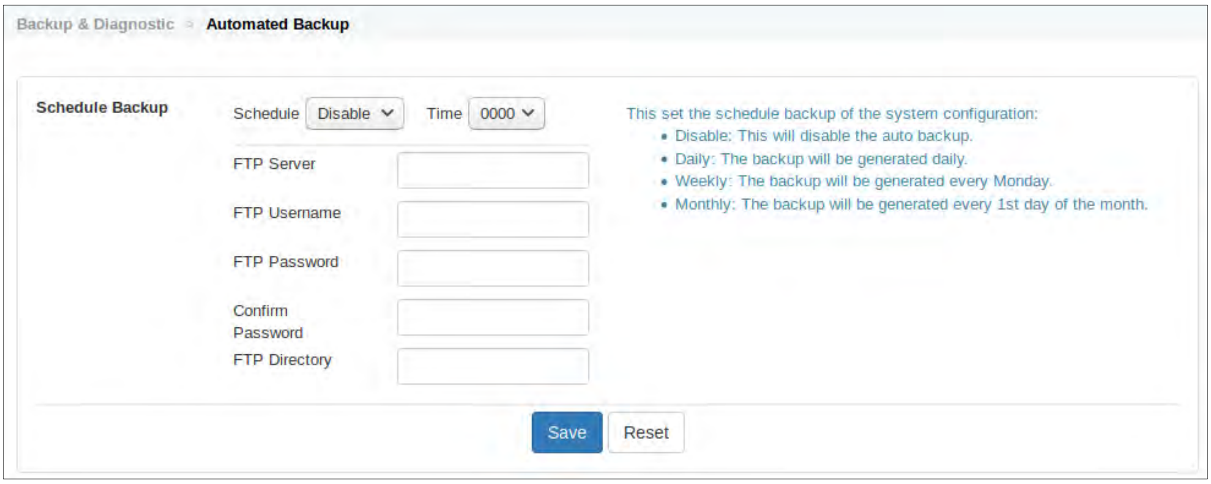
Backup system configuration: Start

*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. |



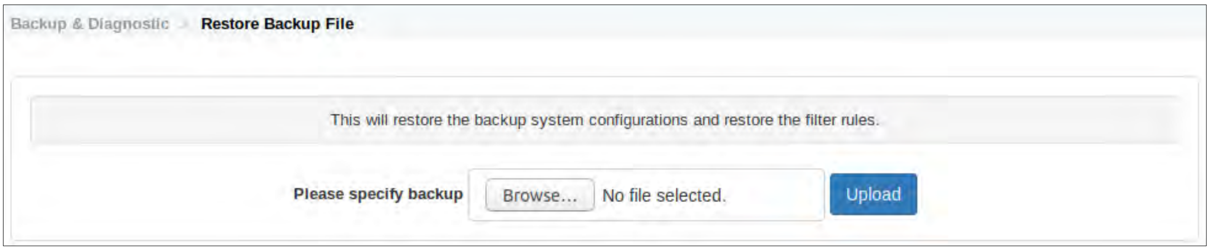
This set the schedule backup of the system configuration:

- 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.



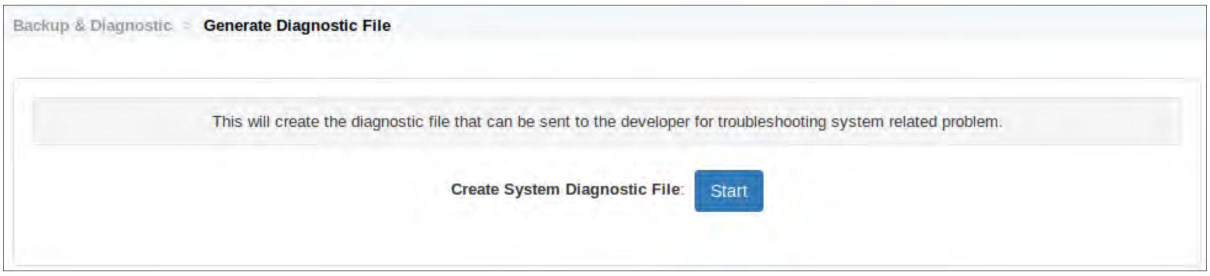
This will restore the backup system configurations and restore the filter rules.

*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.

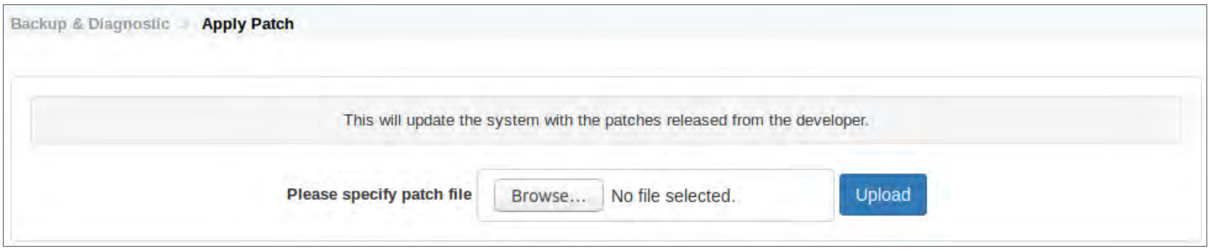


This will create the diagnostic file that can be sent to the developer for troubleshooting system related problem.

*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).



This will update the system with the patches released from the developer.

Please specify patch file: No file selected.

*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, it is recommended to perform a system backup and to keep the backup file in a safe folder/system. Perform the 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 when applying the patch file to the appliance In the event it happens,  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.***

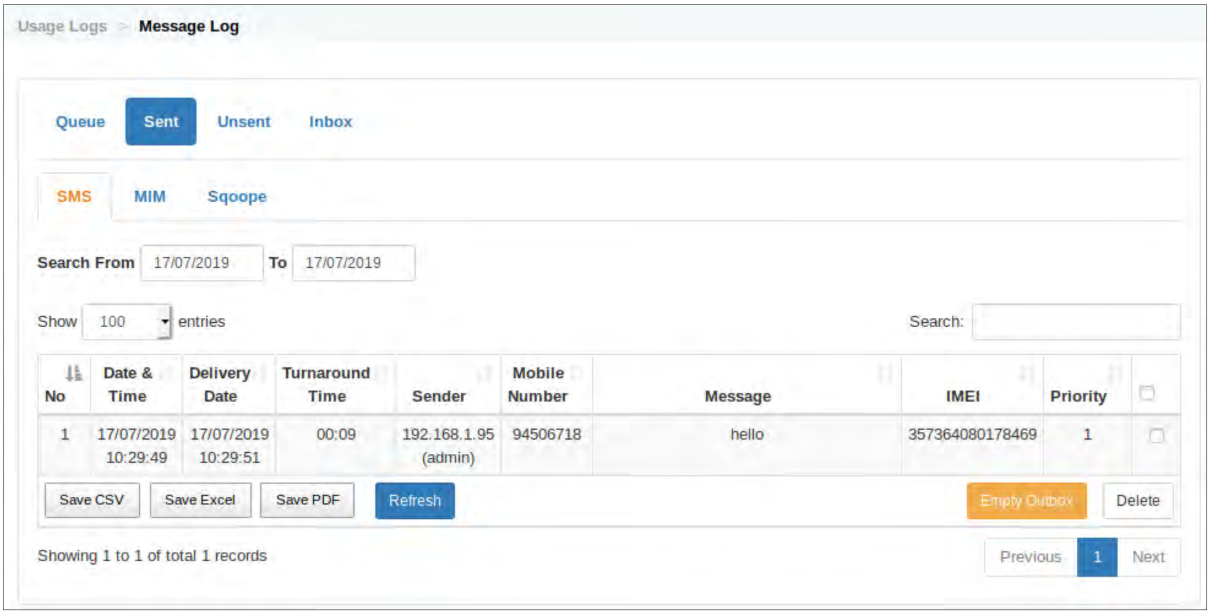
# 14.0 Usage Logs

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.



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 | □ |

Showing 1 to 1 of total 1 records

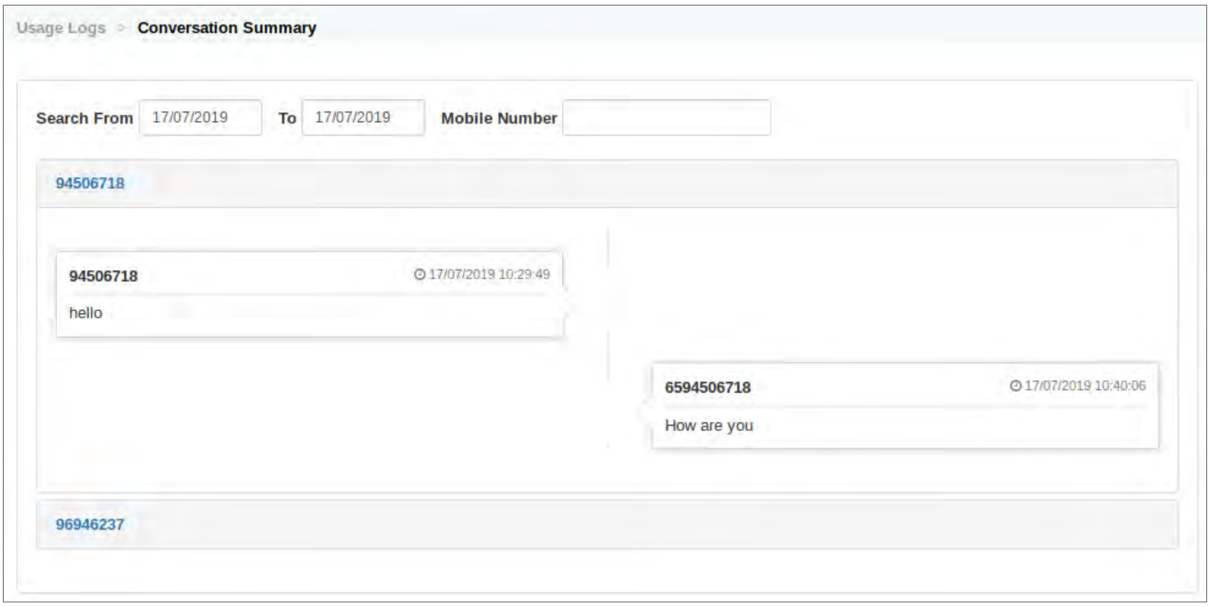
*Figure 14-1 : Message Log*

To delete a record(s), **select/unselect** 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.



Usage Logs > **Conversation Summary**

Search From 17/07/2019 To 17/07/2019 Mobile Number

94506718

94506718 17/07/2019 10:29:49
hello

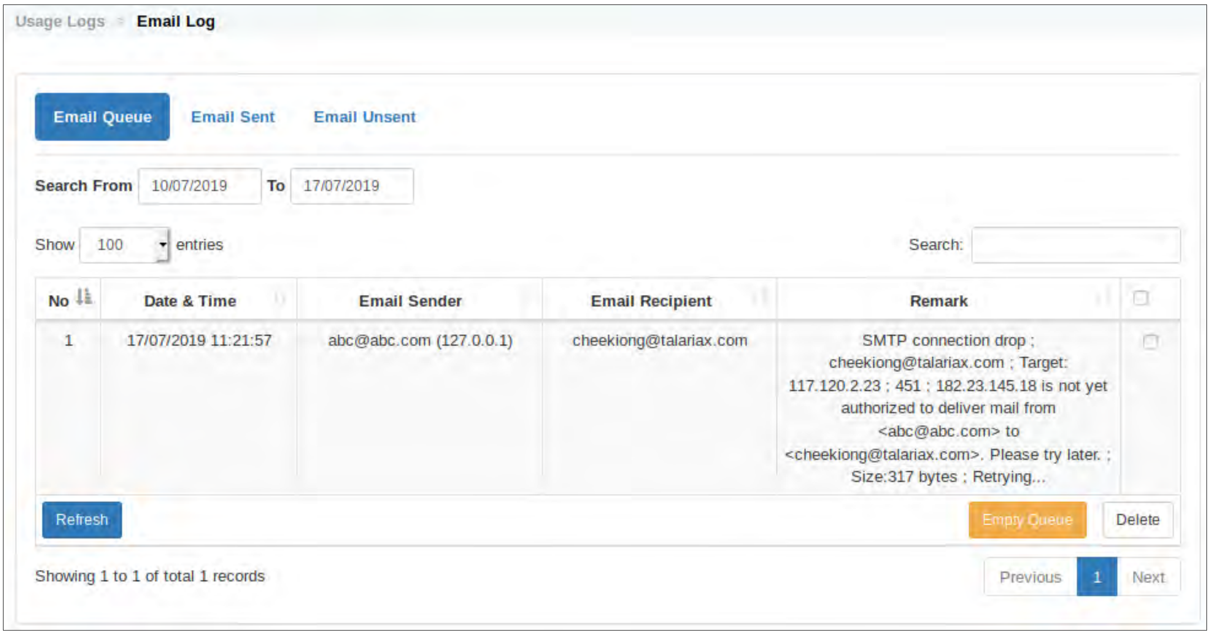
6594506718 17/07/2019 10:40:06
How are you

96946237

*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.



Usage Logs > **Email Log**

Search From 10/07/2019 To 17/07/2019

Show 100 entries Search:

| 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... | ☐ |

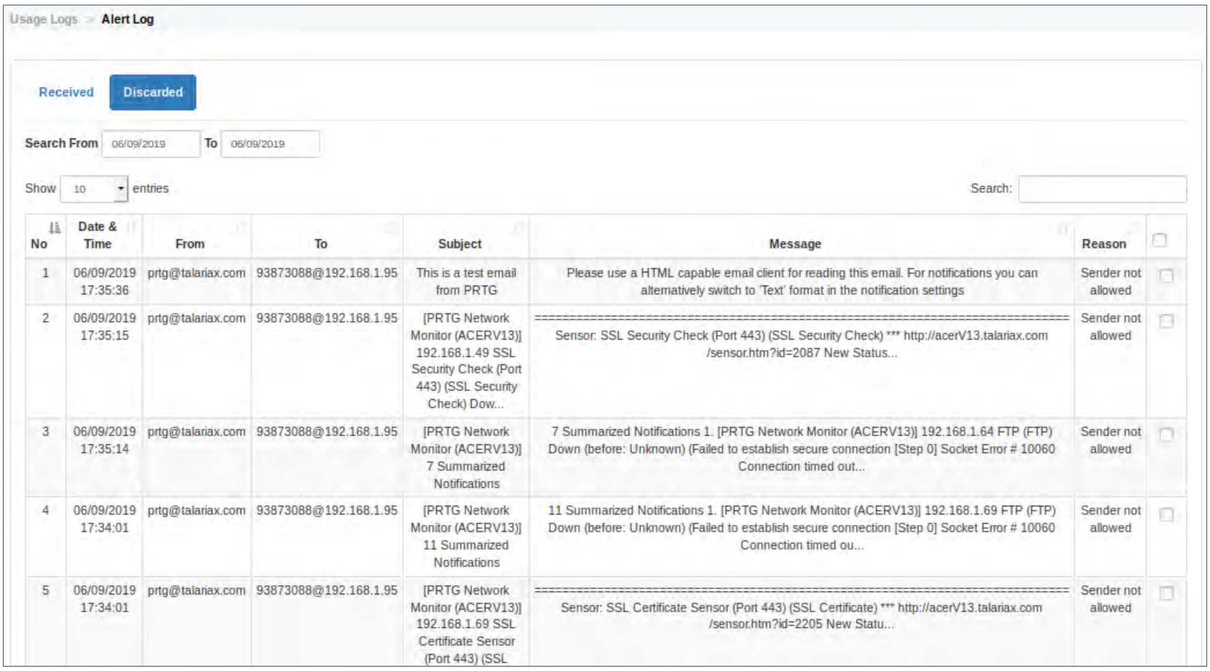
Showing 1 to 1 of total 1 records

*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 14-4.

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



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

Show 10 entries

Search:

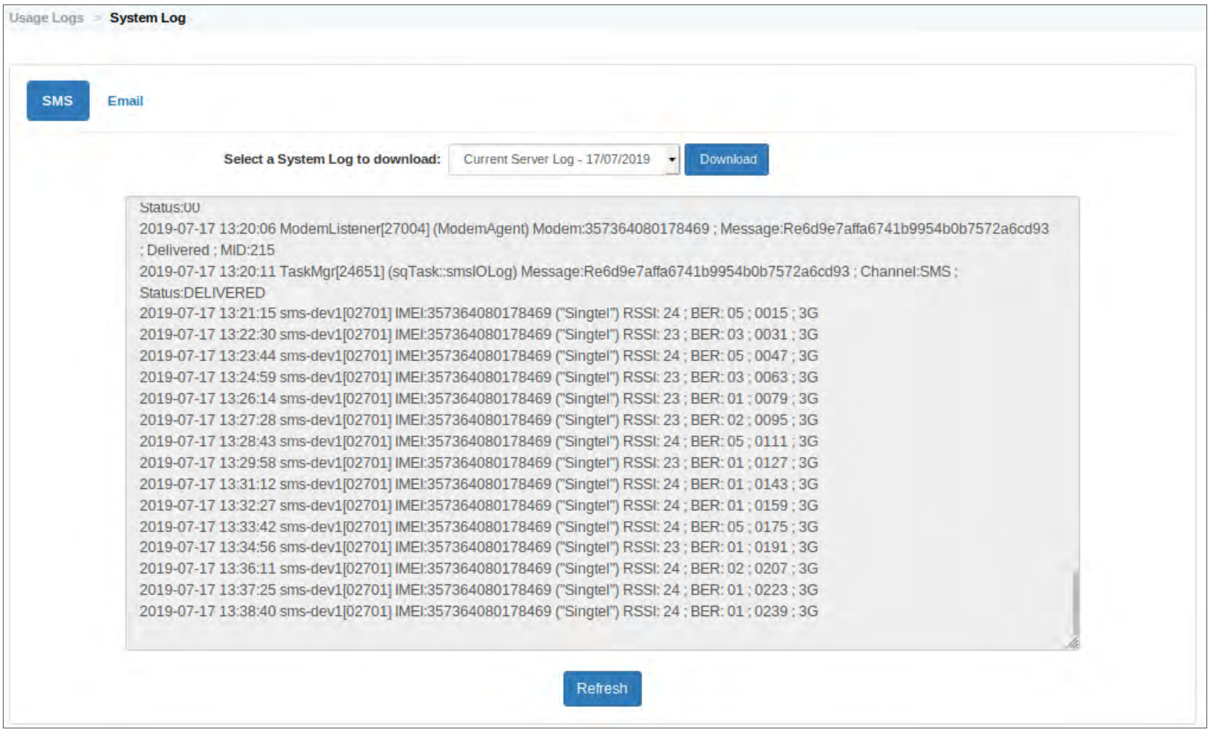
| No | Date & Time | From | To | Subject | Message | Reason | □ |
|---|---|---|---|---|---|---|---|
| 1 | 06/09/2019 17:35:36 | prtg@talariax.com | 93873088@192.168.1.95 | This is a test email from PRTG | Please use a HTML capable email client for reading this email. For notifications you can alternatively switch to 'Text' format in the notification settings | Sender not allowed | □ |
| 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 | □ |
| 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 | □ |
| 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 | □ |
| 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 | □ |

*Figure 14-4 : 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 14-5.

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



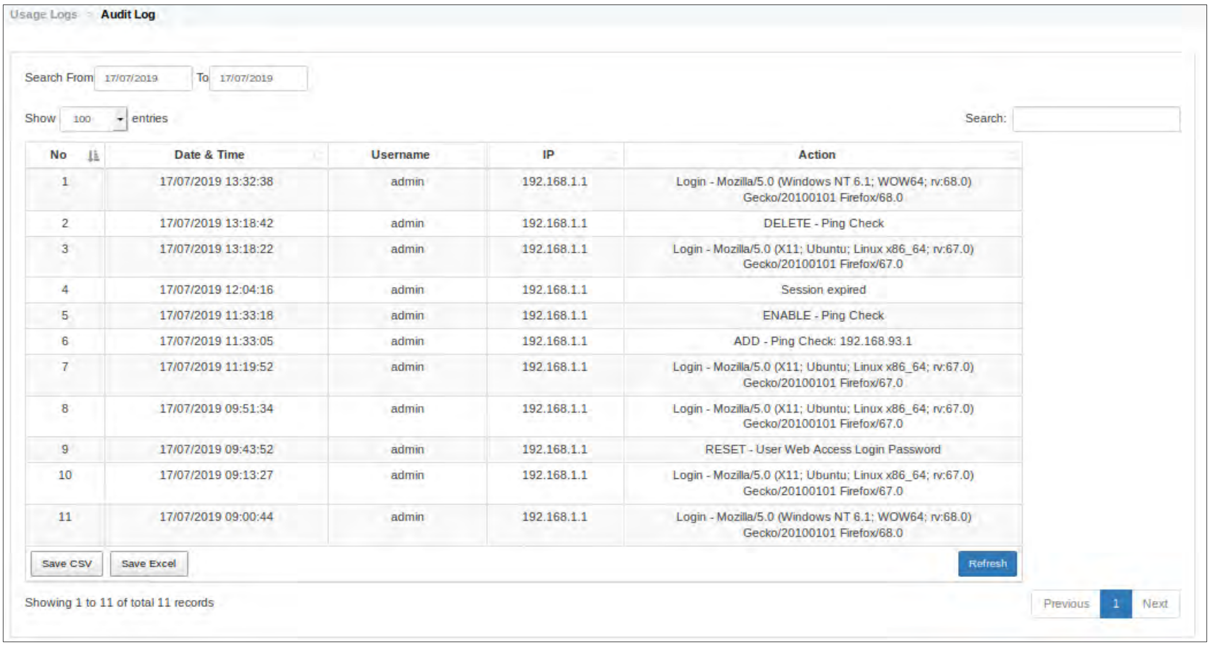
Select a System Log to download: Current Server Log - 17/07/2019

```
Status:00
2019-07-17 13:20:06 ModemListener[27004] (ModemAgent) Modem:357364080178469 ; Message:Re6d9e7affa6741b9954b0b7572a6cd93
; Delivered ; MID:215
2019-07-17 13:20:11 TaskMgr[24651] (sqTask::smsIOLog) Message:Re6d9e7affa6741b9954b0b7572a6cd93 ; Channel:SMS ;
Status:DELIVERED
2019-07-17 13:21:15 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 24 ; BER: 05 ; 0015 ; 3G
2019-07-17 13:22:30 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 23 ; BER: 03 ; 0031 ; 3G
2019-07-17 13:23:44 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 24 ; BER: 05 ; 0047 ; 3G
2019-07-17 13:24:59 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 23 ; BER: 03 ; 0063 ; 3G
2019-07-17 13:26:14 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 23 ; BER: 01 ; 0079 ; 3G
2019-07-17 13:27:28 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 23 ; BER: 02 ; 0095 ; 3G
2019-07-17 13:28:43 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 24 ; BER: 05 ; 0111 ; 3G
2019-07-17 13:29:58 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 23 ; BER: 01 ; 0127 ; 3G
2019-07-17 13:31:12 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 24 ; BER: 01 ; 0143 ; 3G
2019-07-17 13:32:27 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 24 ; BER: 01 ; 0159 ; 3G
2019-07-17 13:33:42 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 24 ; BER: 05 ; 0175 ; 3G
2019-07-17 13:34:56 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 23 ; BER: 01 ; 0191 ; 3G
2019-07-17 13:36:11 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 24 ; BER: 02 ; 0207 ; 3G
2019-07-17 13:37:25 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 24 ; BER: 01 ; 0223 ; 3G
2019-07-17 13:38:40 sms-dev1[02701] IMEI:357364080178469 ("Singtel") RSSI: 24 ; BER: 01 ; 0239 ; 3G
```

*Figure 14-5 : 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 14-6. To filter the data, enter the content search on the 'Search' field or by selecting the data range or show the number of entries.



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

Show 100 entries

Search:

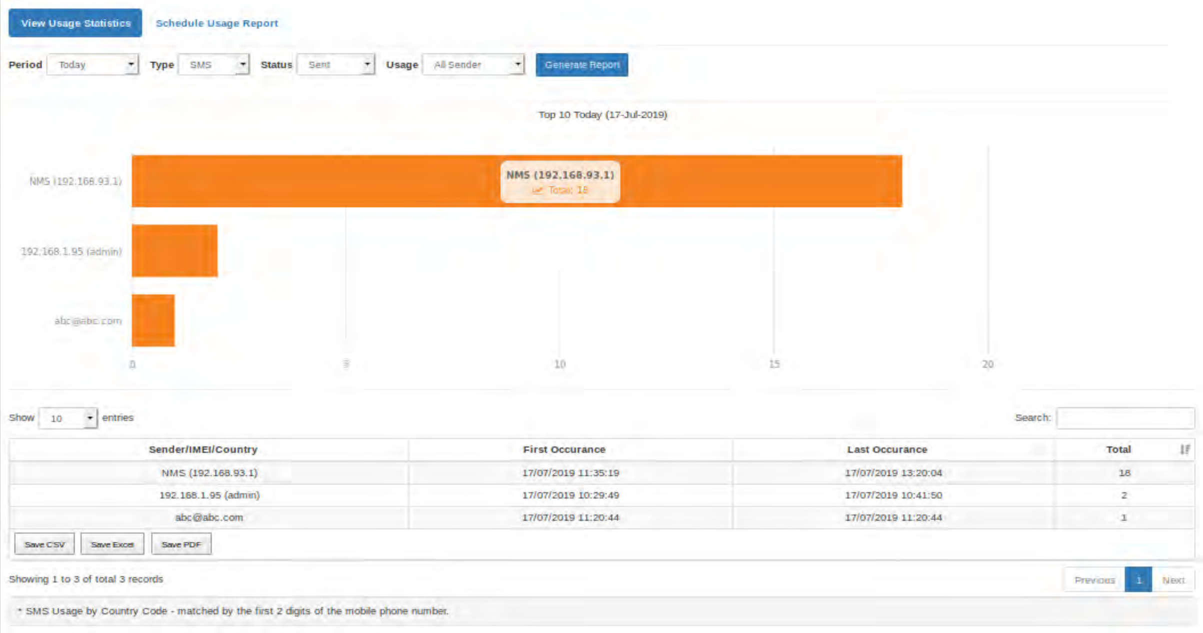
| No | Date & Time | Username | IP | Action |
|---|---|---|---|---|
| 1 | 17/07/2019 13:32:38 | admin | 192.168.1.1 | Login - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:68.0) Gecko/20100101 Firefox/68.0 |
| 2 | 17/07/2019 13:18:42 | admin | 192.168.1.1 | DELETE - Ping Check |
| 3 | 17/07/2019 13:18:22 | 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 |

Showing 1 to 11 of total 11 records

Figure 14-6 : 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 14-7. To filter the data, select the Period, Type, Status and Usage from the respective drop down menu accordingly.



Period Today Type SMS Status Sent Usage All Sender

Show 10 entries

Search:

| Sender/IMEI/Country | First Occurance | Last Occurance | Total |
|---|---|---|---|
| NMS (192.168.93.1) | 17/07/2019 11:35:19 | 17/07/2019 13:20:04 | 18 |
| 192.168.1.95 (admin) | 17/07/2019 10:29:49 | 17/07/2019 10:41:50 | 2 |
| abc@abc.com | 17/07/2019 11:20:44 | 17/07/2019 11:20:44 | 1 |

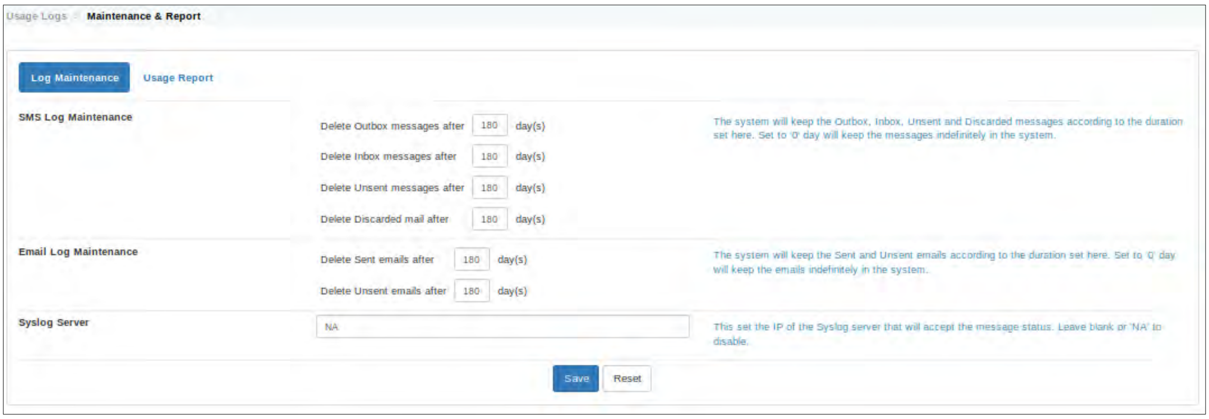
Showing 1 to 3 of total 3 records

* SMS Usage by Country Code - matched by the first 2 digits of the mobile phone number.

Figure 14-7 : 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.



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)

The system will keep the Outbox, Inbox, Unsent and Discarded messages according to the duration set here. Set to '0' day will keep the messages indefinitely in the system.

Email Log Maintenance

Delete Sent emails after 180 day(s)

Delete Unsent emails after 180 day(s)

The system will keep the Sent and Unsent emails according to the duration set here. Set to '0' day will keep the emails indefinitely in the system.

Syslog Server: NA

This set the IP of the Syslog server that will accept the message status. Leave blank or 'NA' to disable.

*Figure 14-8 : Log Maintenance*

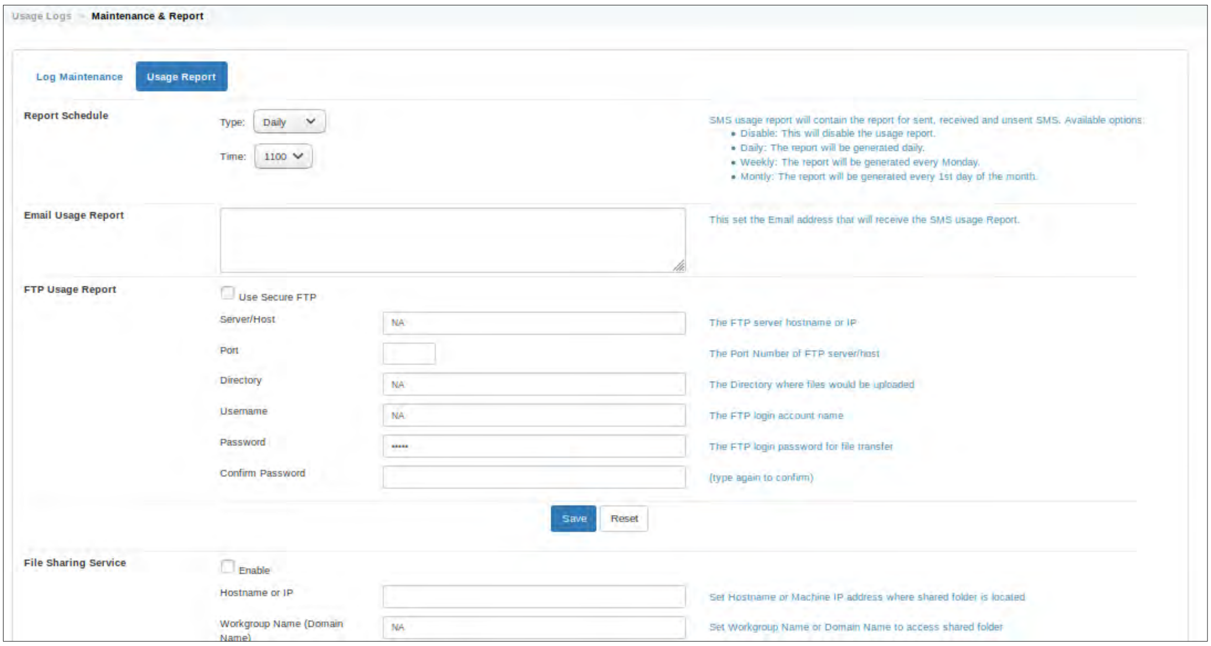
(b) **Usage Report** tab consists of the following setting:

◦ **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.



**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.
- Montly: 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 server/host |
| 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) |

**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 |

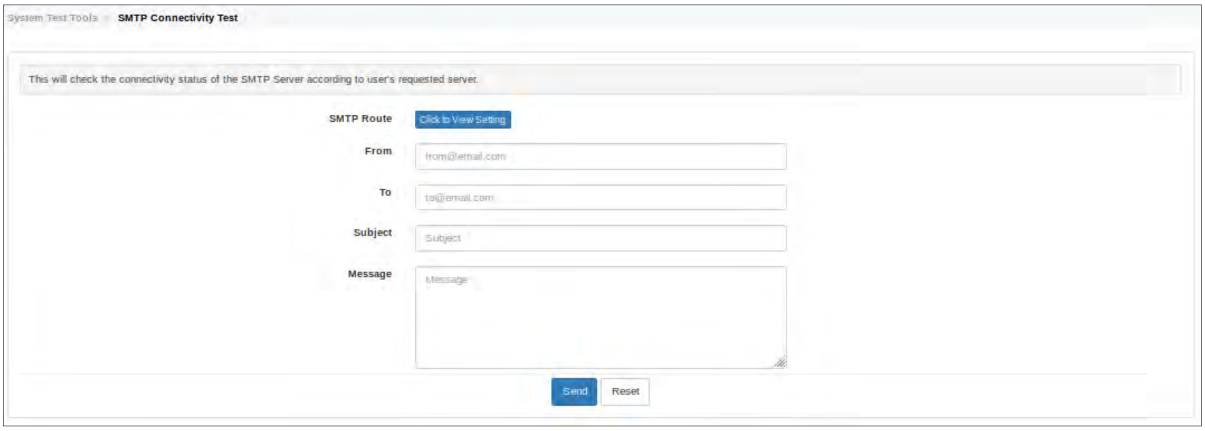
Figure 14-9 : Report Schedule

# 15.0 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)



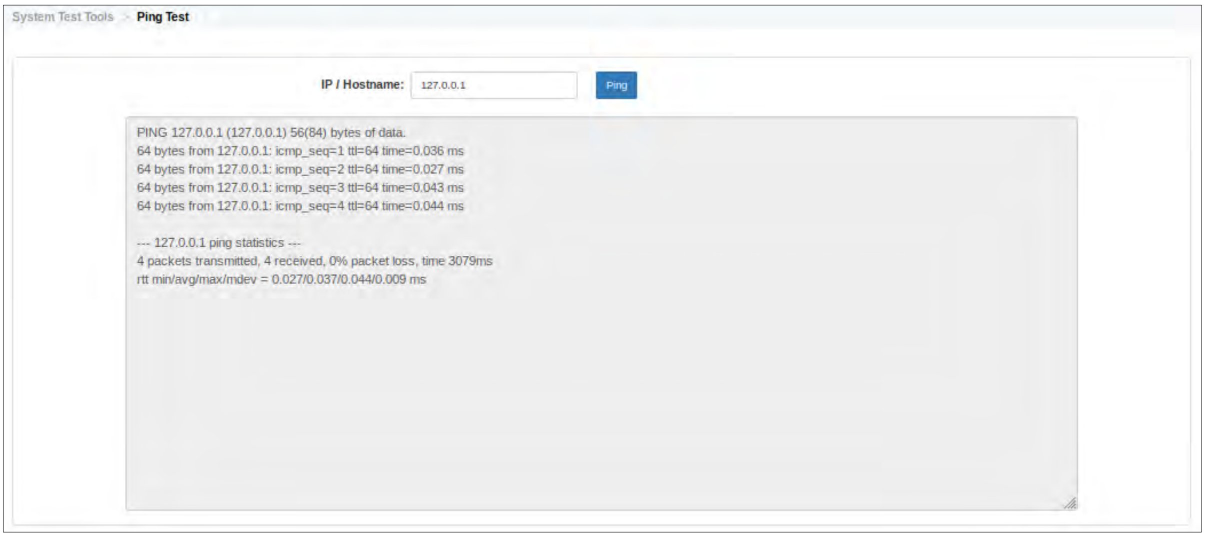
This will check the connectivity status of the SMTP Server according to user's requested server.

| | |
|---|---|
| SMTP Route | Click to View Setting |
| From | from@email.com |
| To | to@email.com |
| Subject | Subject |
| Message | Message |

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).



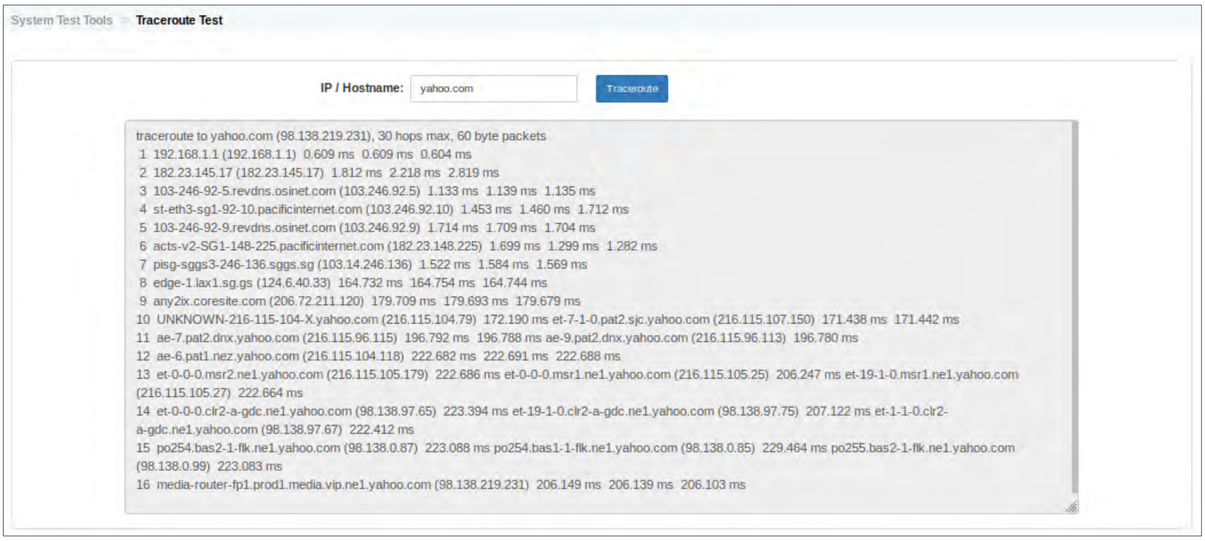
127.0.0.1

```
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).



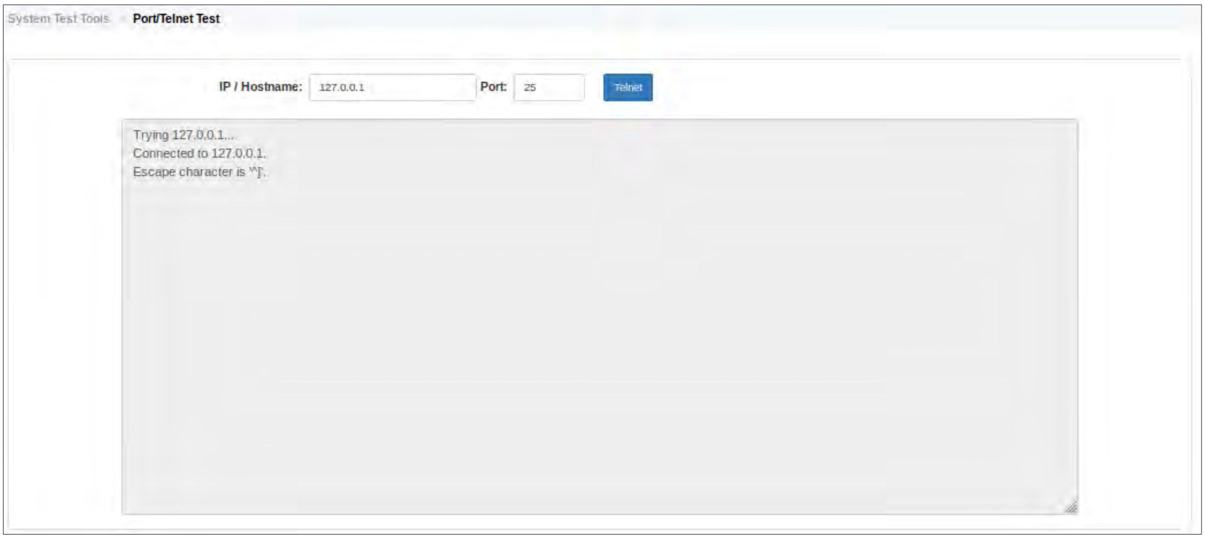
IP / Hostname: yahoo.com

```
traceroute to yahoo.com (98.138.219.231), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  0.609 ms  0.609 ms  0.604 ms
 2  182.23.145.17 (182.23.145.17)  1.812 ms  2.218 ms  2.819 ms
 3  103-246-92-5.revdns.osinet.com (103.246.92.5)  1.133 ms  1.139 ms  1.135 ms
 4  st-eth3-sg1-92-10.pacificinternet.com (103.246.92.10)  1.453 ms  1.460 ms  1.712 ms
 5  103-246-92-9.revdns.osinet.com (103.246.92.9)  1.714 ms  1.709 ms  1.704 ms
 6  acts-v2-SG1-148-225.pacificinternet.com (182.23.148.225)  1.699 ms  1.299 ms  1.282 ms
 7  pisg-sggs3-246-136.sggs.sg (103.14.246.136)  1.522 ms  1.584 ms  1.569 ms
 8  edge-1.lax1.sg.gs (124.6.40.33)  164.732 ms  164.754 ms  164.744 ms
 9  any2ix.coresite.com (206.72.211.120)  179.709 ms  179.693 ms  179.679 ms
10  UNKNOWN-216-115-104-X.yahoo.com (216.115.104.79)  172.190 ms et-7-1-0.pat2.sjc.yahoo.com (216.115.107.150)  171.438 ms  171.442 ms
11  ae-7.pat2.dnx.yahoo.com (216.115.96.115)  196.792 ms  196.788 ms ae-9.pat2.dnx.yahoo.com (216.115.96.113)  196.780 ms
12  ae-6.pat1.nez.yahoo.com (216.115.104.118)  222.682 ms  222.691 ms  222.688 ms
13  et-0-0-0.msr2.ne1.yahoo.com (216.115.105.179)  222.686 ms et-0-0-0.msr1.ne1.yahoo.com (216.115.105.25)  206.247 ms et-19-1-0.msr1.ne1.yahoo.com
(216.115.105.27)  222.664 ms
14  et-0-0-0.clr2-a-gdc.ne1.yahoo.com (98.138.97.65)  223.394 ms et-19-1-0.clr2-a-gdc.ne1.yahoo.com (98.138.97.75)  207.122 ms et-1-1-0.clr2-
a-gdc.ne1.yahoo.com (98.138.97.67)  222.412 ms
15  po254.bas2-1-flk.ne1.yahoo.com (98.138.0.87)  223.088 ms po254.bas1-1-flk.ne1.yahoo.com (98.138.0.85)  229.464 ms po255.bas2-1-flk.ne1.yahoo.com
(98.138.0.99)  223.083 ms
16  media-router-fp1.prod1.media.vip.ne1.yahoo.com (98.138.219.231)  206.149 ms  206.139 ms  206.103 ms
```

*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).



IP / Hostname: 127.0.0.1 Port: 25

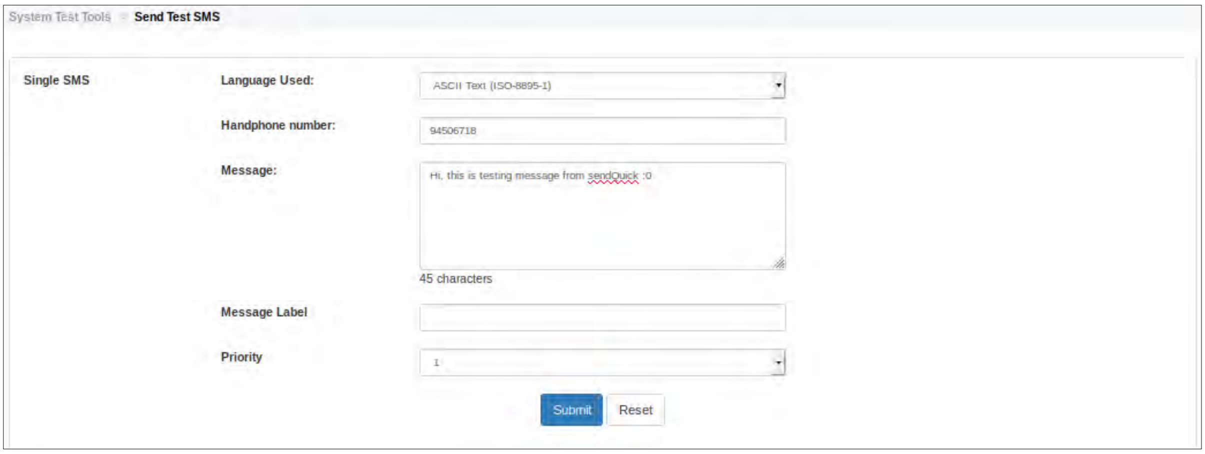
```
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
```

*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).



Language Used: ASCII Text (ISO-8895-1)

Handphone number: 94506718

Message: Hi, this is testing message from sendQuick :0

45 characters

Message Label

Priority: 1

*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.

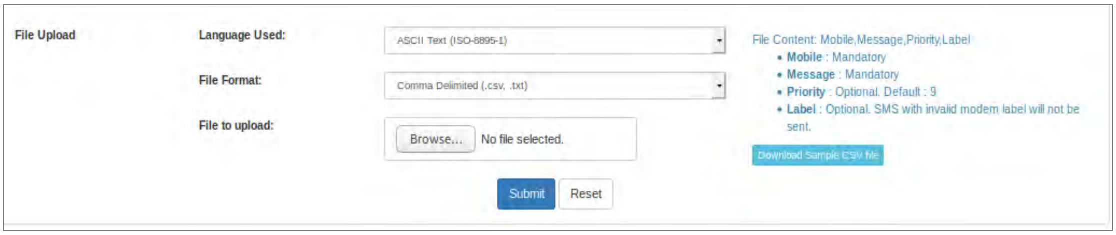
***Data Format:*** The data format should be segmented in 2 columns: hand phone number and message content. The table below shows the example of the data format in the CSV and TXT file.

| **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).



File Upload

Language Used: ASCII Text (ISO-8895-1)

File Format: Comma Delimited (.csv, .txt)

File to upload: Browse... No file selected.

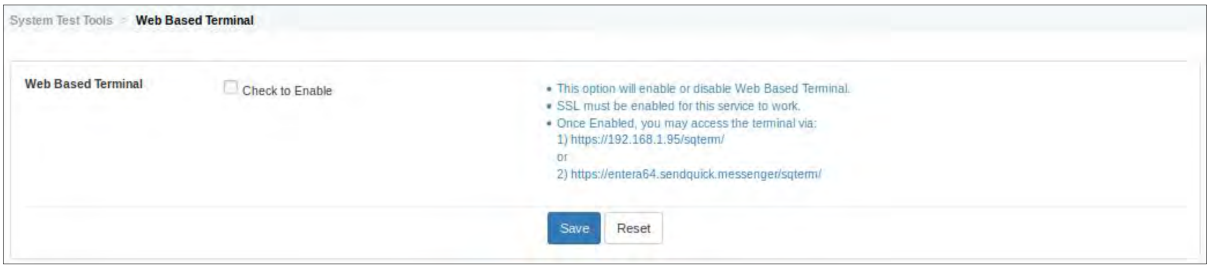
File Content: Mobile,Message,Priority,Label

- **Mobile** : Mandatory
- **Message** : Mandatory
- **Priority** : Optional. Default : 9
- **Label** : Optional. SMS with invalid modem label will not be sent.

*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.



Web Based Terminal

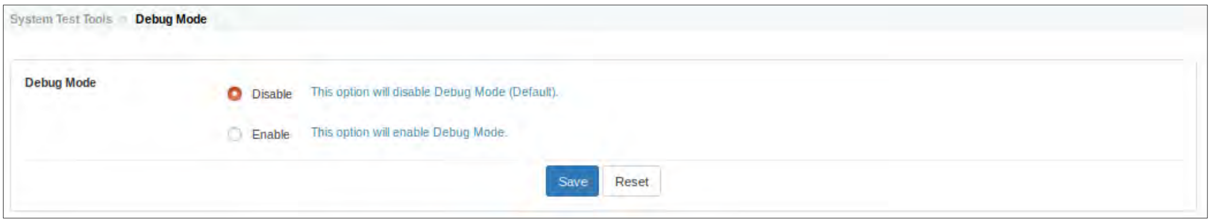
□ Check to Enable

- This option will enable or disable Web Based Terminal.
- SSL must be enabled for this service to work.
- Once Enabled, you may access the terminal via:
  1) https://192.168.1.95/sqterm/
  or
  2) https://entera64.sendquick.messenger/sqterm/

*Figure 15-7 : Web Based Terminal*

## 15.7 Debug Mode

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



Debug Mode

● Disable This option will disable Debug Mode (Default).

○ Enable This option will enable Debug Mode.

*Figure 15-8 : Debug Mode*

# 16.0 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/enve-
lope/"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://sche-
mas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Body>
<mns:processAPIxmlns:mns="urn:apiwsdl" SOAP-ENV:encodingStyle="http://sche-
mas.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&char-
set=utf-8
```

Where:

mno -- the mobile phone number<br>
txt -- the text message

dtm – the date and time of the SMS received.<br>
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.

# 17.0 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.

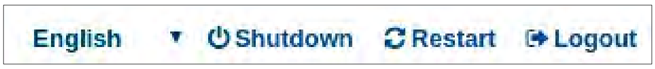


*Figure 17-1 : Shutdown, Restart or Logout*

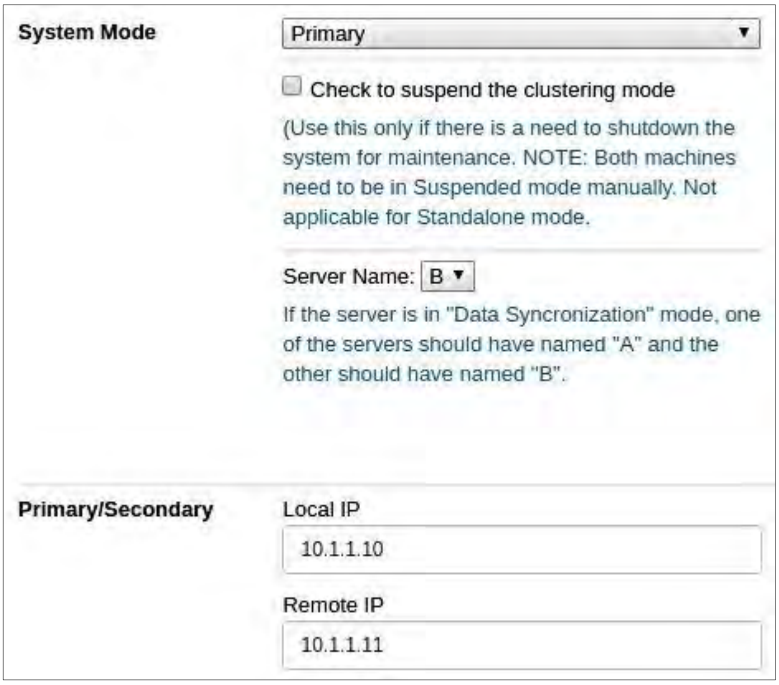
# 18.0 High Availability Configuration

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).



System Mode: Primary ▼

□ 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 Syncronization" 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.

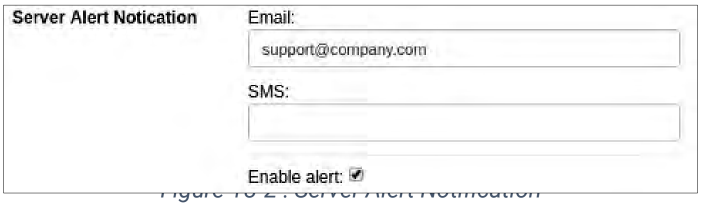
The **heartbeat checking is configured on eth1 or E2** (as labeled on the LAN port).

The **Local IP** refers to the IP if 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.



Server Alert Notication

Email: support@company.com

SMS:

Enable alert: ☑

*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:

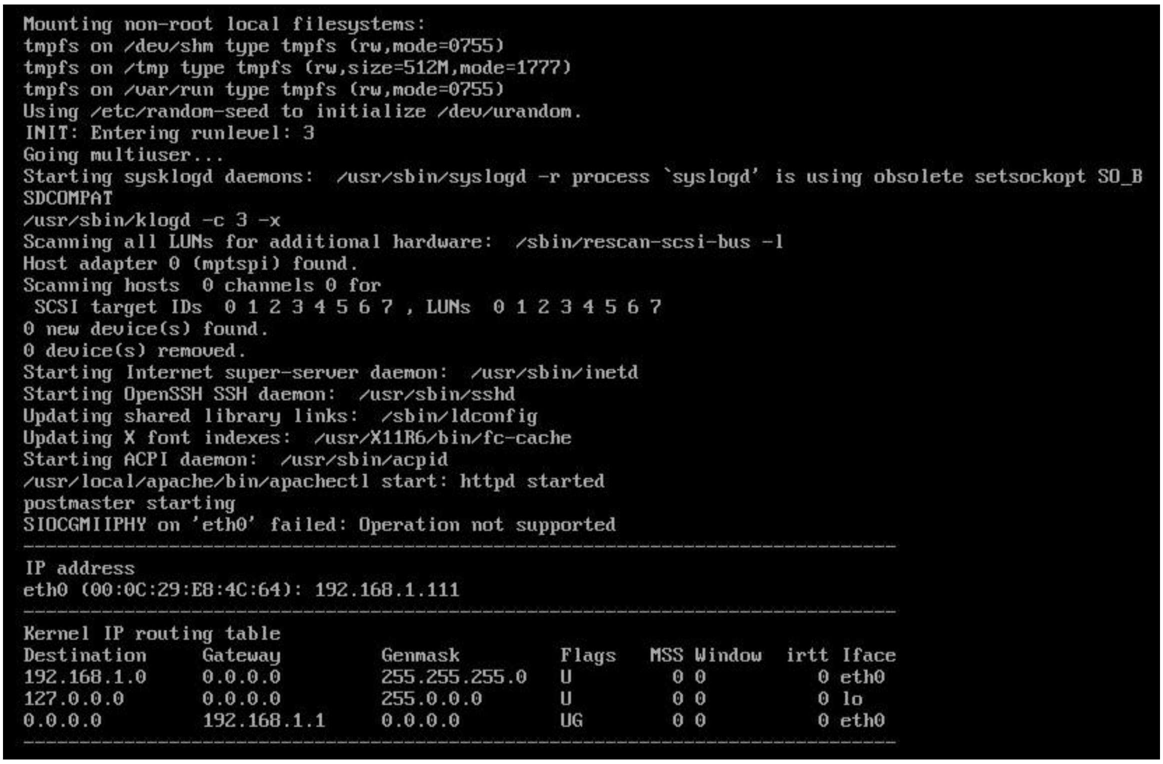
| Step | Materials Required | Configuration |
|---|---|---|
| 1 | IP address set | Configure the IP, Netmask and Gateway of Primary and Secondary server IP as explained in section 5. |
| 2 | LAN cable | Connect the LAN cable to port Eth1 of both Primary and Secondary servers and ensure the IP is accessible 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<br>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<br>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. |

# 19.0 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 sysklogd 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*

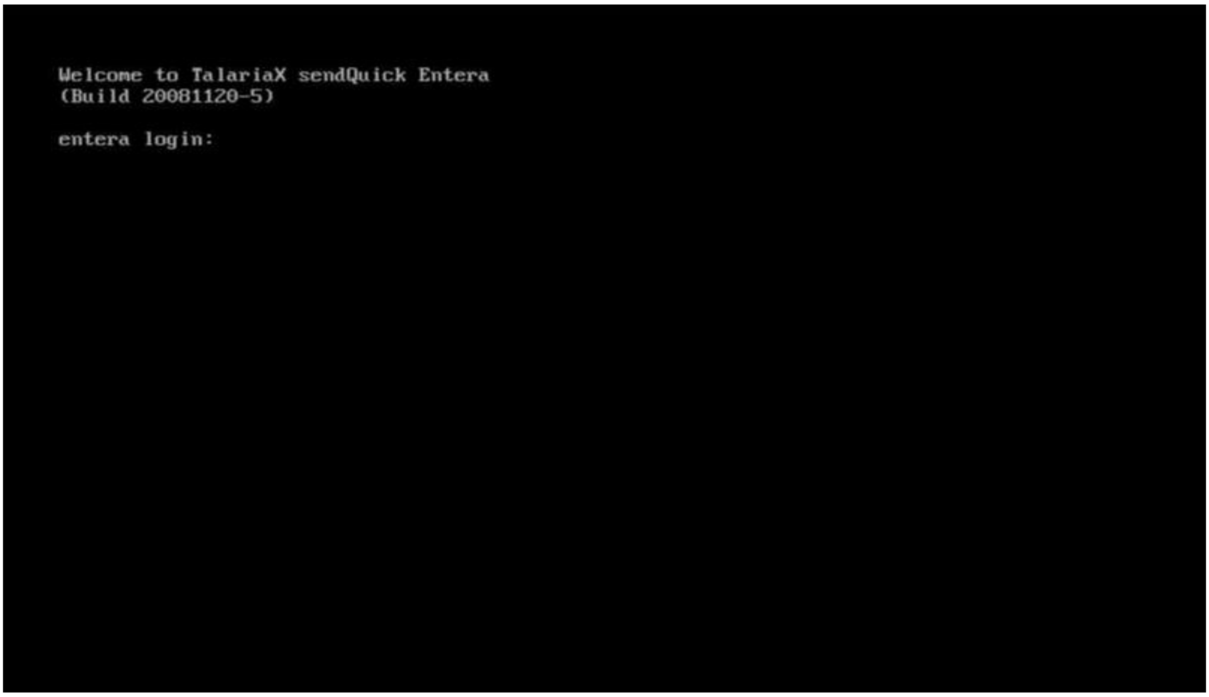
In the monitor console, the administrator can perform the following functions:

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

## 19.1 Configure sendQuick IP via Console

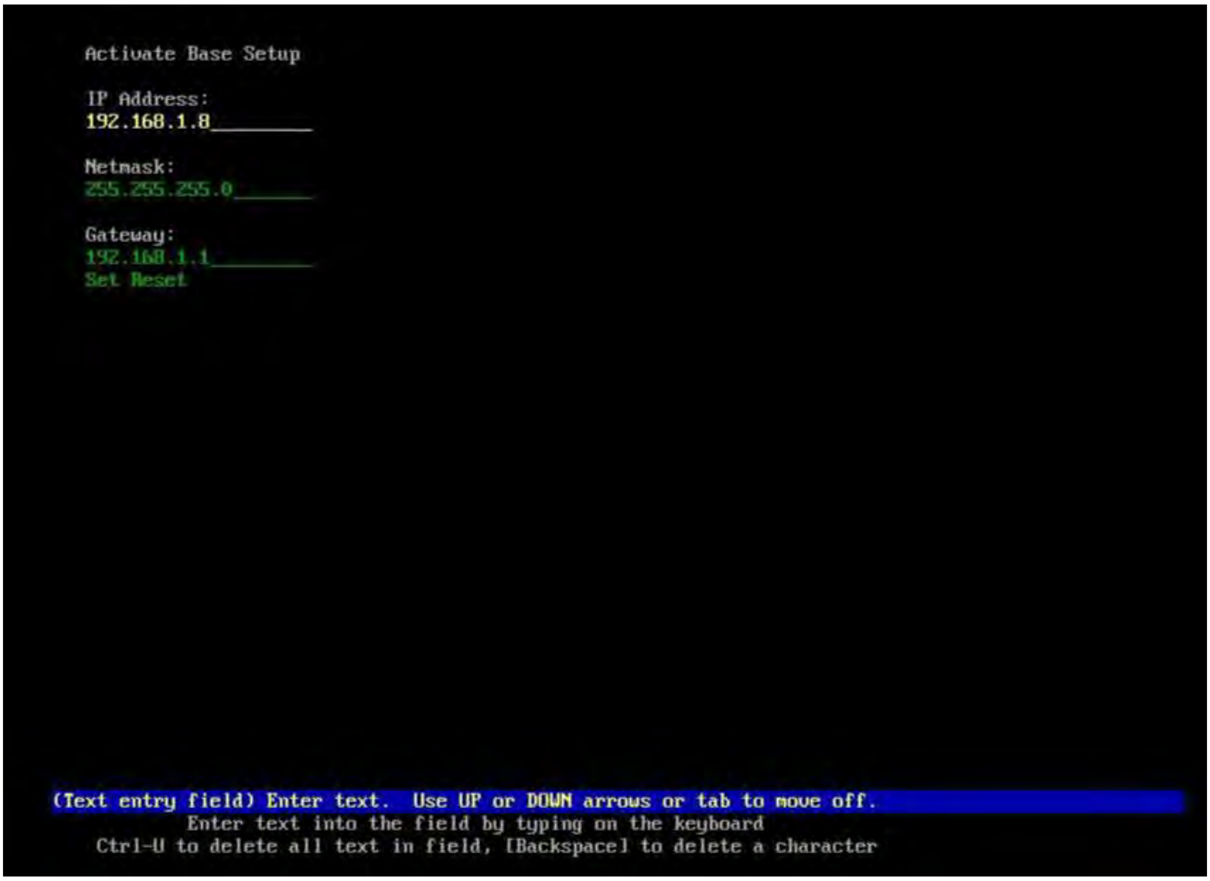
First, you need establish the physical connection as described above. Then, enter **ALT and F4** simultaneously. You will see the login page as shown in Figure 19-2 and enter the default username and password below. (Contact support@talariax.com if you have forgotten the password)

```
Console Username: admin
Console Password: (check with our support team at support@talariax.com if
you have forgotten the password)
```



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

entera login:
```

Figure 19-2 : Console Login Prompt



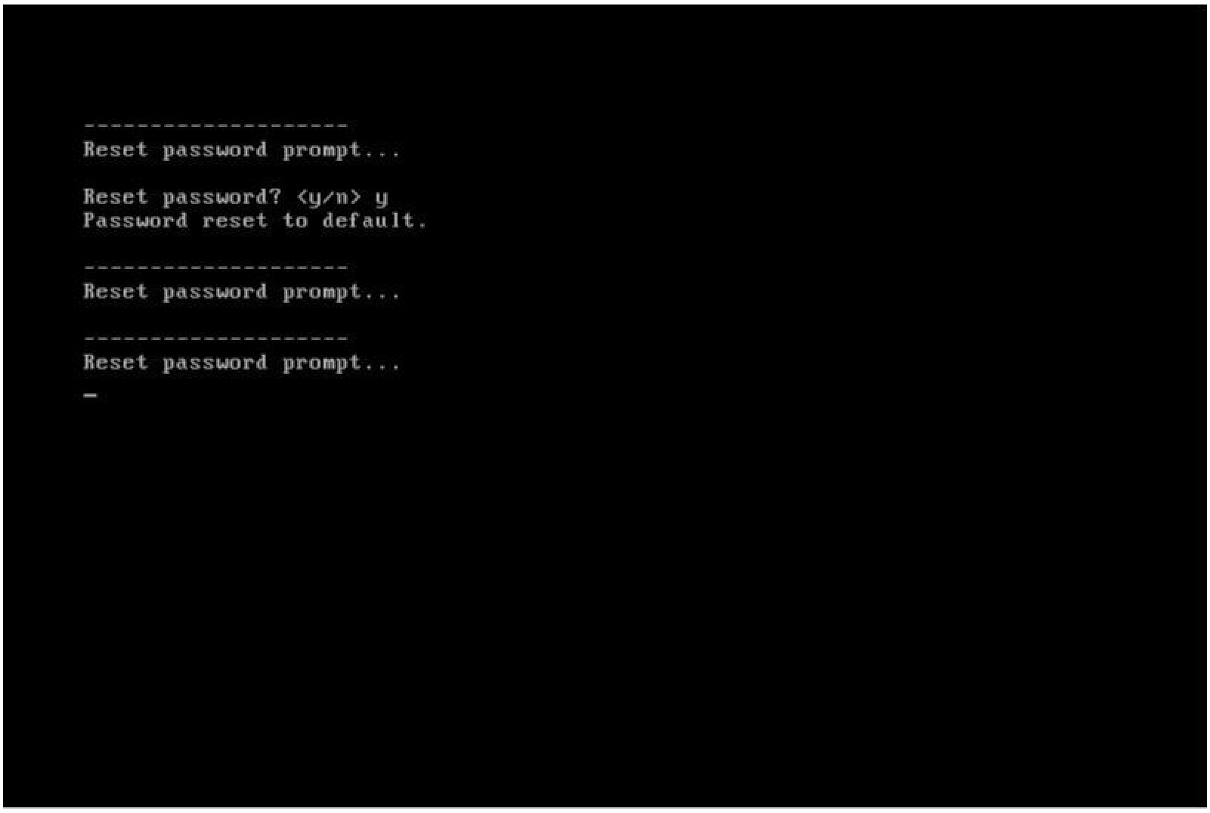
```
Activate Base Setup

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 password (Check with support@talariax.com if you have forgotten what the default password is).

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.



```
--------------------
Reset password prompt...

Reset password? <y/n> y
Password reset to default.

--------------------
Reset password prompt...

--------------------
Reset password prompt...
_
```

*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:(see *Note)
```

***Note:** the Alt+F3 reset password will be the sendQuick's serial number for:

- Entera series : patch p9HF16 and onward.
- AlertPlus series : patch p8HF7 and onward.

# 20.0 Troubleshooting

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 is 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 in 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 for 2-3 minutes before reconnecting the USB to the system.
4. Wait for about 2-3 minutes and check the 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. Power off the modem.
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 a 'Double blink'.

   *Single Blinking patten:* blink—pause—blink–pause--blink…

6. Wait for 2-3 minutes before reconnecting the USB to the system
7. Wait for 2-3 minutes 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.**
  **<u>These actions may cause damage to the modem or cause the modem to hang.</u>**

## 20.11 When sendQuick cannot detect modem.

I. Check the modem's Power/USB cable is connected correctly.

II. Check the 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 and try to send and receive SMS if the SIM is not working in a modem. 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 > SMS Log, check if any error code, please refer to section 21 – Modem Error code for detail.

## 20.12 How a modem work

The modem connection perform a certain number of steps to connect to the network. The sequence to check the modem connection as explained below.

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 successful registration, the modem's status will display on sendQuick's Dashboard > Modem Status.

VI. If it failed to register to the telco network, 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 600 SMS per day or more than 10,000 per month (This apply to Singapore operator, other countries may have similar or different policies), you may have violated their Fair Use Policy.

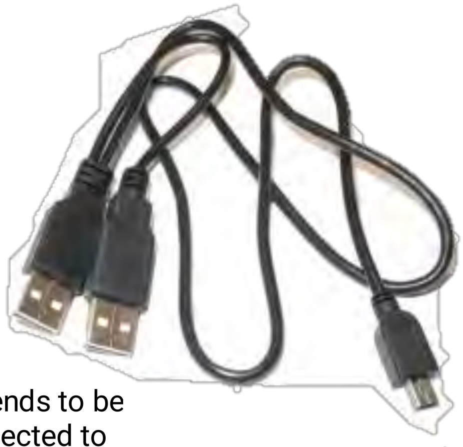
sendQuick has built-in feature to send messages via Internet connection (Section 6.4: sendQuickASP Routing) or using social messenger like WhatsApp or Telegram and others (Section 6.8: Mobile Instant Messaging Routing) that can send messages without a SIM. Do contact TalariaX at info@talariax.com for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

## 20.15 Why Need to Perform Modem Reset

When the telco block/throttle sending of SMS, the modem will encounter errors It may think there is a fault/problem and try to resend the messages again. When it fails (due to telco block), it will reset the modem and try again. During this reset process, modem will 'drop off' from the system. Since system did not detect modem, it will try to reset and cycle continue.

This will cause the modem to be undetected. In order to perform hard reset, remove the modem from the system and wait for 2-3 minutes and plug in again. This will cause the task to exit and perform a task restart. This will perform a disconnection and re-connection to the telco network and may be allowed to reconnect and register. This may lead to the modem able to reconnect and send messages again.

Note: Modem reset can work on USB Y-cable only (without external power). If your modem is installed with its own power supply, the reset function will not work correctly. Please contact TalariaX for more information.



Both ends to be connected to sendQuick

To Modem

## 20.16 I am getting Delivery Date (DR) blank, does it means SMS is not sent ?

If DR is blank, this means that the system did not receive the reply from telco. The DR is non-guaranteed and a blank DR does not mean it is not sent/delivered. It just simply means DR is not received.

## 20.17 What is the definition of the Turnaround time ?

Turnaround time is the total time taken when the messages first reach sendQuick (SMS Queue) to when it actually sent (SMS Sent). Turn-around time is the amount of time the messages in the queue, please see the example below:

_Example_
The message reached sendQuick at 10:00am. As the queue is busy (could be due to delay can be due to load or when modem is not available, it stay there for 20mins and was sent at 10:20am. The message was delivered to the phone and sendQuick received a DR at 10:21am from telco, based on above, the time stamp will be:

a) SMS Queue date and time : 10:00:00 am <-- This data is not capture on the 'Sent box'
b) SMS Sent Date and Time : 10:20:00 am
c) SMS Sent Delivery Date (DR) : 10:21:00 am <-- This time is from Telco / It can be blank if Telco did not reply.
d) SMS Sent Turnaround time : 00:20:00 minutes (the time format is hh:mm:ss)
(d) = (b) - (a).

➢ The above date/time format will be 'DD/MM/YYYY hh:mm:ss'

## 20.18 The modem should be detected by the sendQuick even if a sim is not installed?

sendQuick will only detect and displays the modem until when a valid SIM with sms service is fully detected and registered to telco network. Hence if there is no SIM inserted or faulty SIM or invalid SIM card, no modem will be shown on sendQuick.

## 20.19 SMS fail to send with "Invalid Format" in Unsent Box.

Access to menu > Server Admin > Security setup > Mobile number allow > check if any entry in here? If yes, please remove them. This allow list means only messages in this format are allowed to send. If the list is empty, we will then need the diagnostic file to check.

## 20.20 Modem stay stuck in "Modem Init" State, Modem Info SMSC, Operator Info stays in "Detecting" state.

Modem Init could be due to modem not able to complete the registration to the telco or there could be messages (invalid) stuck in the queue and cause the operator to reject the messages and cause the modem to reset.
- Check your SIM card, remove the SIM card, put in a phone and test to send a message.
- Try to use another valid SIM card.

### 20.21 How do I generate a CA Cert ?

For CA Cert, please generate CSR and assign the CSR to your CA server.

# 21.0 Modem Error Codes

Below is a list of error codes that may experience when sending SMS. There are two types of error codes. CME (Equipment Error Codes) and CMS (Network Type Error Codes). These are error codes that responded from the modem when interact with the Telco network.

### CME 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.

### CME 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.

### CME Error code 13: Modem error status or SIM card failure

If your SIM card is 'too old', suggest to replace with a new SIM card.

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

Please follow these steps to troubleshoot the problem.

- **i.** Power off the modem.
- **ii.** Disconnect the Modem cable from sendQuick.
- **iii.** Remove the SIM card from the modem
- **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 regular 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.

### CMS 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.

### CME Error Code 30: No network service / Unknown subscriber

Please ensure that your SIM card is valid, the subscriber is not registered to any network. Try to use a physical mobile phone to test the SIM card (one at a time), try to send and receive SMS.

## CMS Error Code 38: SIM card failed

Error 38 means 'Network out of order'. Please check with the Operator for this error.  This error means that the message could not be sent because there is a problem with the connection of the modem to the mobile network. 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 (compare with a normal phone usage) unusual high amount of SMS messages that system is sending.

## CMS 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 or try without country code.

## CMS Error code 111: Operator Network Coverage issue or Invalid Phone number

Error 111 is related to modem or operator coverage issue. Such error can be intermittent and could be due to telco signal is weak at your area/server room (could be intermittent). You can try to have a longer antenna cable that able to locate your antenna outside your Server room/DC. Check the mobile signal strength. We would recommend a minimum of 15% to have sufficient signal for to send and receive messages.

Error 111 could be modem specific and modem related. Do perform a modem reset or contact TalariaX for assistance.

## CMS Error code 310:  SIM not inserted

No SIM card is detected, please check the modem, try to eject the SIM card (if any) and reinsert again.

## CMS Error code 500:  Operator reject code, mobile network or target recipient error

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

The error could also means:

**i.** The mobile number you try to send to is invalid. Eg fixed line, mobile number is no longer in used etc.
**ii.** There is no network coverage.
**iii.** You don't have enough money/credits 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.

## CMS 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 600+- 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 to check with telco on your mobile plan subscription and make sure it didn't hit any limit.

Check the system Usage Log > SMS sent and see the log/number of records for last 30 days. If you have sent more than the number mentioned, per modem (or close to it), it is an issue with telco SIM.

Other possible reasons to experience this error includes Mobile Network issue, Modem related problem, SIM card problem or other issues like USB/serial cable and antenna.