



# AlertDispatcher v5.0

## Quick Start User Guide

Last update: August 27, 2015

## **Copyright**

This publication is protected by copyright and distributed under licenses restricting its use, copying and distribution. No part of this publication may be reproduced in any form by any means without prior written authorization of Click And Deploy Pte Ltd.

## **Disclaimer**

This publication is provided "AS IS", without a warranty of any kind. All express or implied representations and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are hereby excluded. Click And Deploy Pte Ltd may make any improvements or changes in the product(s) or the program(s) described in this publication at any time. This document is subject to change without notice.

## Table of Contents

1. System Preparation .....	5
1). Working SIM card .....	5
2). Working GSM or GPRS modem .....	5
3). Windows PC/Server/Virtual Machine (System Requirements) .....	6
4). Disable System Standby (For XP, 7 and workstation OS) .....	7
5). Setup considerations for API / Email-to-Alert (Email2SMS) / HTTP-to-Alert / SNMP trap receiver interface .....	8
a). Resolving possible port conflicts .....	8
b). Add server ports to Firewall .....	9
c). DEP exception list. ....	11
6). Obtaining an SMTP or Email account .....	13
2. Installation, Upgrade, Migration and Configuration .....	14
1). Installation / Upgrade / Migration .....	14
a). Upgrade / Migration .....	14
b). Installation .....	14
2). Configure Modem .....	17
a). Add modem .....	17
b). Troubleshooting modem connection issues .....	19
c). Send test SMS .....	20
3). Configure System and Alerts Setup .....	22
a). System Setup - General .....	22
b). System Setup - Send Message Filter .....	24
i). "SendByKeyword" filter .....	24
c). System Setup – System Alerts/Email Setup .....	25
d). System Setup - Modems .....	27
e). System Setup – Outgoing Message Filter .....	27
f). System Setup – Reporting .....	28
g). System Setup – High Availability .....	29
i). Network Load Balancing Cluster .....	29
ii). Enable Replication and Message Failover .....	30
iii). Mirror Pending Messages .....	30
iv). Operation Mode .....	30
4). Configure Users and Departments .....	34
a). Create user .....	34
b). Create new user types .....	35
c). Create departments .....	35
d). Connecting client to remote server .....	36
5). Configure SMTP Server Setup .....	37
a). SMTP Server Setup – General Setup .....	37
b). SMTP Server Setup – POP3 Client Setup .....	39
c). SMTP Server Setup - MAPI Setup .....	39
d). SMTP Server Setup – Email Notifications .....	41
e). SMTP Server Setup – LDAP Query Setup .....	43
6). Configure HTTP Server Setup .....	44

7). Configure Server Monitoring .....	46
8). Configure SNMP Trap Receiver Setup .....	48
9). Loading your Contact List into Addressbook Groups, setup Duty Schedule, Basic Escalation and Emergency Recall Notification .....	49
a). Addressbook Setup .....	49
b). Basic Escalation Setup .....	53
i). Overview .....	53
ii). Acknowledging by SMS reply .....	55
iii). Acknowledging by email reply .....	56
iv). Acknowledging via AlertDispatcher Client Console .....	57
iv). Acknowledging via link embedded in email .....	58
b). Emergency Recall Notification Setup .....	61
10). Configure Message Templates .....	62
11). Configure Receive SMS Setup (Forward to Addressbook / Forward to Email / Execute SQL / Send HTTP GET request / Execute DOS Command) .....	64
a). Forward to Addressbook .....	64
b). Forward to Email .....	65
c). Execute SQL .....	66
d). Send HTTP GET request .....	68
e). Execute DOS Command .....	69
11). Configure Reports .....	70
3. License Registration using Activation Code .....	71
1). Register via SMS .....	71
2). Register via Internet .....	72
4. Interfacing with AlertDispatcher using SMTP/HTTP/DOS .....	74
1). Using AlertDispatcher built-in SMTP Server to send Alerts (Email-to-SMS/Email) .....	74
2). Sending Alerts (SMS/Email) by executing an SQL Stored Procedure (MSSQL) .....	74
3). Sending Alerts (SMS/Email) using HTTP or from a web browser .....	74
4). Sending Messages/Query Status from Windows Command Line or Batch File .....	81
5). Interfacing from Dot Net or Java using COM DLL .....	85
5. Appendix A- Preparing your GSM/GPRS modem .....	86
1). Preparing the GSM modem .....	86
2). Checking SIM card .....	88
6. Appendix B - Troubleshooting Checklist .....	89
1). SIM Card is activated, Modem is setup properly and connected to the PC .....	89
2). Required Services Started, and Windows Firewall configured, AlertDispatcher Client and Service added to Windows DEP exception list (for the case of Vista/2008) .....	89
3). Send test SMS using AlertDispatcher .....	95
7. Appendix C - FAQ and Tips .....	97
1). Question: I do not know how to pause and delete the SMS that I send wrongly .....	97
2). Question: Where do I find the server and activity logs? .....	97
3). Question: My modem is connected but I can't send SMS? .....	97

# 1. System Preparation

This Quick Start Guide will help you deploy and configure AlertDispatcher within 1-3 hours (depending on the features you use).

Here's a checklist of what you need to prepare before installing AlertDispatcher.

## 1). Working SIM card

If you need to send SMS, an activated GSM/GPRS/3G SIM card\* is required (**with no PIN password set**).

**Note:**

1. Some prepaid SIM cards need to be activated by voice call before SMS is enabled. Please test the SIM card using a mobile phone if required.

\*2. If you're using a 3G modem, you will need to get a 3G SIM card. If unsure, please contact your mobile service provider or test before actual deployment.

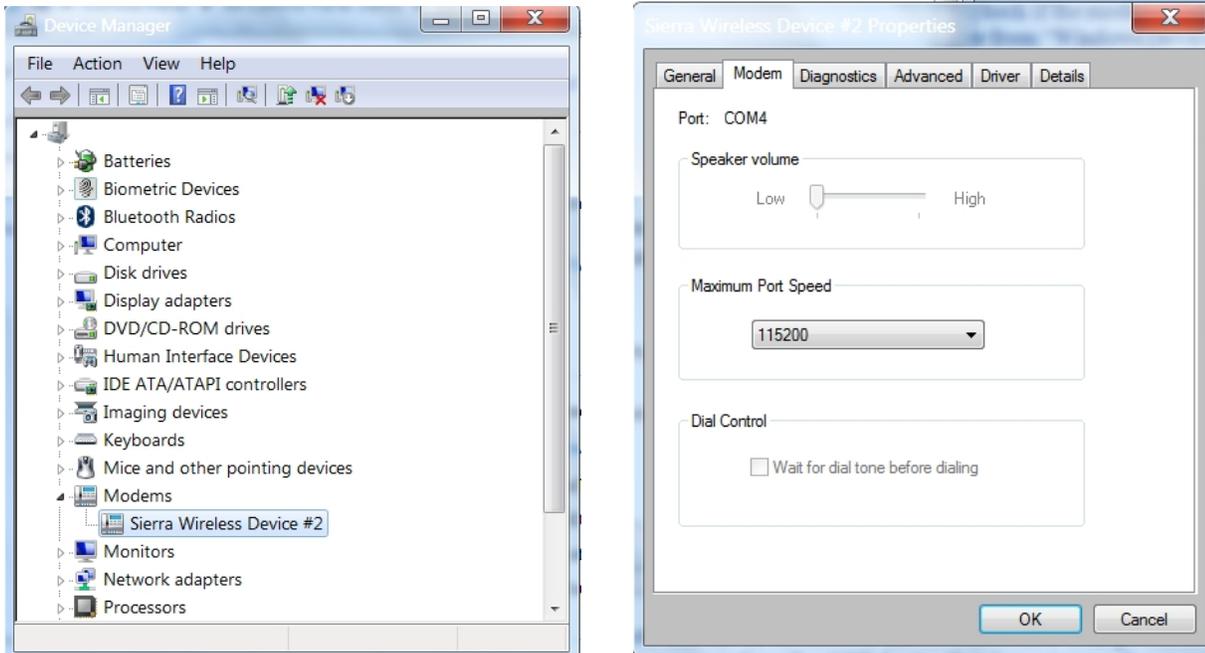
3. If you need to change your SIM card, before removing the SIM card, please **always turn off** the power supply or remove the power supply cable from the modem. You may reconnect the power supply after you have installed the new SIM card.

## 2). Working GSM or GPRS modem

A Compatible GSM, GPRS or 3G modem is required to send SMS (Please contact your dealer if you do not have one).

If you are using a serial modem, please ensure that your PC has a DB9 serial port. If there is no available DB9 serial port, you may install third party PCI DB9 RS232 serial card. STLab Serial cards are reliable and known to work with most serial GSM/GPRS modems.

USB modems generally require modem drivers to work. After installing the modem driver, go to *Start* → *Control Panel* → *System* → *Hardware Tab* → *Device Manager* → *Modems* and ascertain the COM port onto which the modem driver has been installed.



**Note:** Refer to Appendix A for more details on preparing the GSM modem.

### 3). Windows PC/Server/Virtual Machine (System Requirements)

If possible, please prepare a clean installed Windows PC/Server with the following specifications. The following hardware specifications are recommended for a deployment with up to 4 modems attached and processing up to 10,000 messages per day.

If you're installing onto a virtual machine, and the modems are connected to the "host machine", ensure that you are able to access your modem COM port on the "guest machine". If you're not able to access the COM ports on the guest machine, you'll need to use a [Serial Device Server](#) to connect a serial GSM/GPRS modem to the VM. Do not use a USB Device Server as they don't work properly with USB modems.

*Minimum Processor:* Pentium 4 for Windows XP / Pentium Core 2 Duo for higher versions of Windows.

*Operating System:* Windows XP (Service pack 3) / Windows 7 / Windows 2003 Server / Windows 2008 Server / Windows 8 / Windows 2012 Server

*RAM:* Minimum 2 GB RAM (for Windows XP). Minimum 4 GB RAM (for higher versions of Windows).

*SIM card:* Activated and working SIM card from your mobile operator.

*GSM Signal:* Location of server/PC must have good GSM reception. You may compare the signal strength for various SIM card providers using the software – signal strength will be displayed on the Client console.

*USB port:* Required for USB modems – as USB modems draw power from the USB port, you may need to use an externally powered USB hub if you have attached other USB devices to your PC/Server.

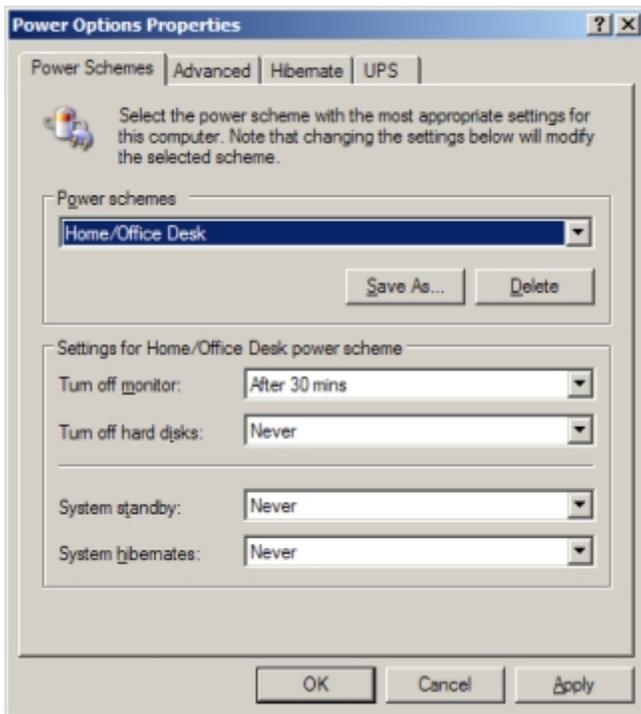
*Serial port:* Required for Serial modems – ST Lab 2 & 4 port serial cards are supported.

**Note:** We would recommend that you install antivirus software if you need to login to the system regularly.

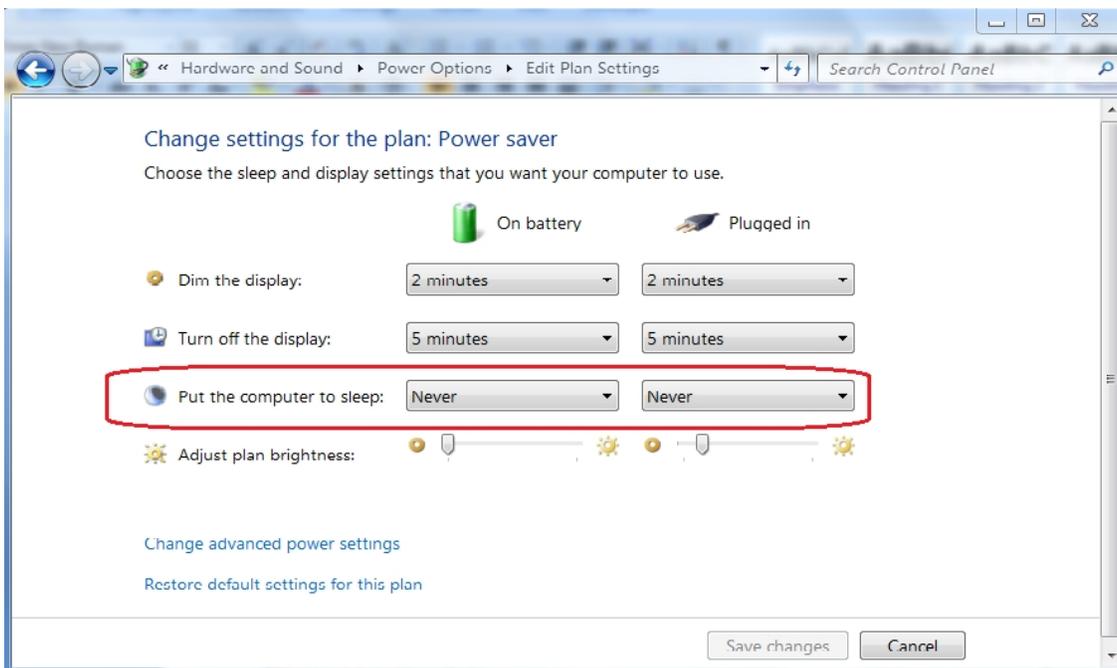
#### 4). Disable System Standby (For XP, 7 and workstation OS)

If you are installing AlertDispatcher on a workstation OS, e.g. Windows XP, Vista or 7, please ensure that system standby/sleep and turn off hard disk settings are changed to 'Never'.

Setting for XP:



Setting for Windows 7:



## 5). Setup considerations for API / Email-to-Alert (Email2SMS) / HTTP-to-Alert / SNMP trap receiver interface

### a). Resolving possible port conflicts

AlertDispatcher comes with built-in TCP/IP Servers - HTTP Server (Web Server), SMTP Server and SNMP Trap Receiver so you can send Alerts (Email/SMS) using the HTTP and SMTP (Email) application interfaces provided and convert SNMP traps into Alerts. The built-in servers use the following default ports for their respective protocol.

<i>Server Protocol</i>	<i>Default Port</i>	<i>Remarks</i>
HTTP Server	80	
SMTP Server	25	
SNMP Trap Receiver	162	
AlertDispatcher Server	5556	<i>Used by AlertDispatcher Client and DLL API</i>

In order for TCP/IP application interfaces to work, there must not be conflicting services running on your system occupying the same ports. If there is a conflicting service using the same port, the following error will be written to the AlertDispatcher event log: “Could not bind to socket”.

The screenshot shows the AlertDispatcher Enterprise v5.0.0.0.509 interface. The window title is "AlertDispatcher Enterprise v5.0.0.0.509 (Authorized User: Click And Deploy) MaxRecipients: 20". The interface includes a menu bar with options like Templates, Server Monitoring, Automation Setup, Help/Registration, Modem Setup, Instant Messaging (IM) Setup, System Setup, Servers Setup (SMTP/HTTP/SNMP), and Receive SMS Setup. Below the menu is a "Server Status" section with buttons for Start, Stop, Restart, and Emergency Pause. The status shows "Server running". A "Modem Signal" section displays "COM22" and "Operator: Singtel (HSPA 3.5G)". A red box highlights an error message in the log: "2015.08.20 22:39:02:046 [!] HTTP Server failed to start: Could not bind socket. Address and port are already in use. Please ensure that IIS World Wide Web Publishing Service or any other HTTP service is not using the same port." Below this, a successful log entry is visible: "2015.08.20 22:38:41:125 AlertDispatcher Service Started! Modems initialized successfully - COM22". The bottom status bar shows "Server running" and a signal strength indicator "9 (Very poor)".

For SMTP Server interface, check whether Windows ‘Simple Mail Transfer Protocol (SMTP)’ service exists and is set to run automatically. If ‘Simple Mail Transfer Protocol (SMTP)’ service exists, stop and disable Windows SMTP service.

For HTTP Server, ensure that Windows World Wide Web Publishing Service, or IIS isn't running on the same port (default port for HTTP server is 80).

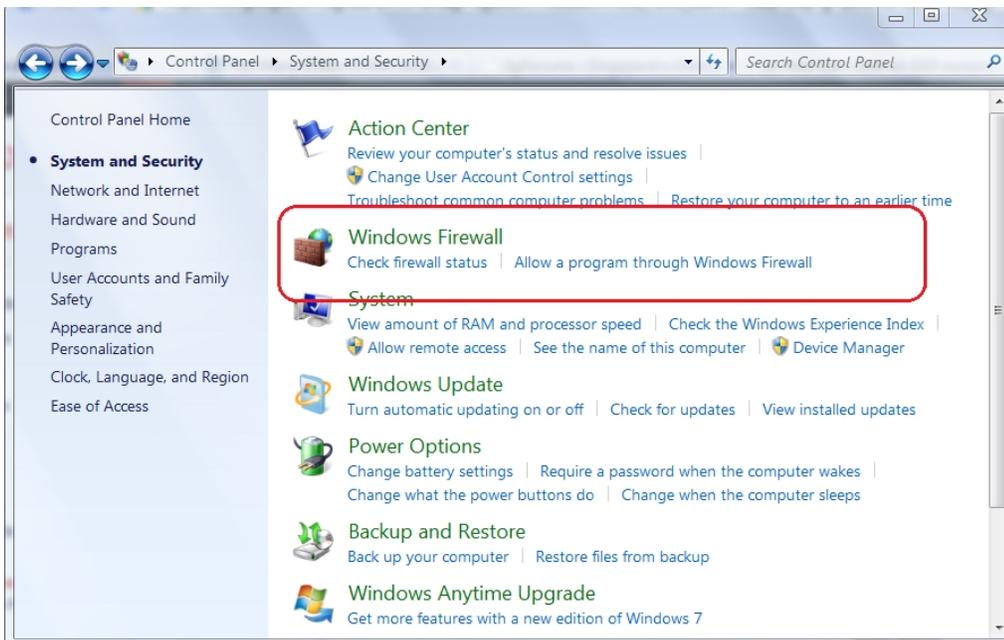
For SNMP Trap Receiver, if you have installed Windows SNMP Trap service, please ensure that the service is stopped or change to a different port (default port for Trap Receiver is 162).

b). Add server ports to Firewall

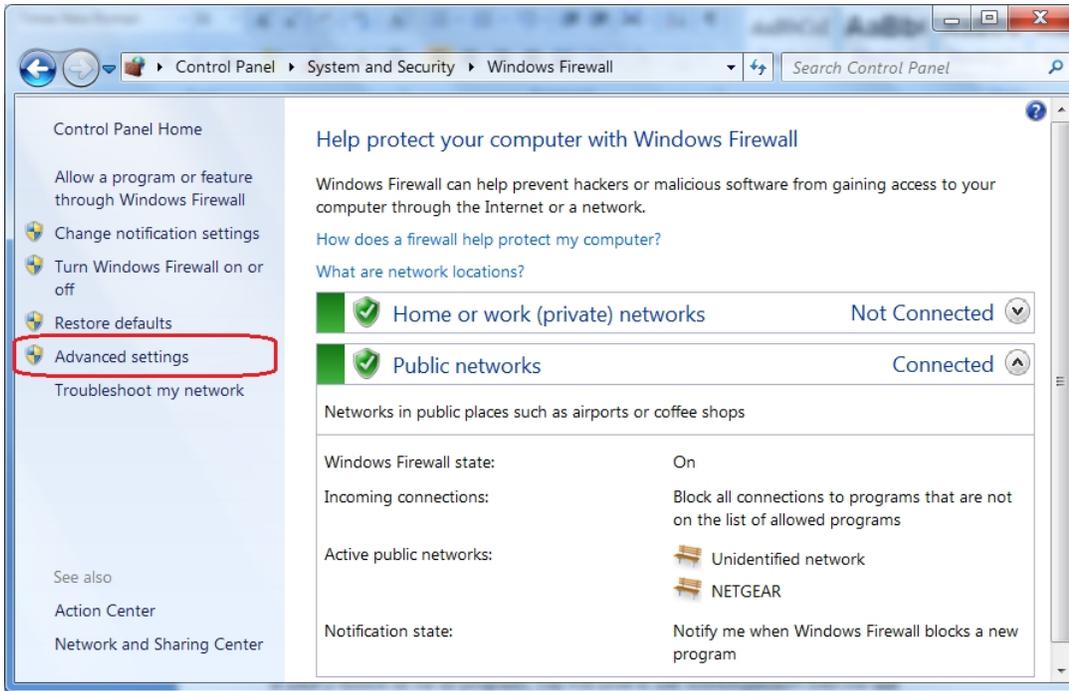
If you need to be able to access AlertDispatcher Server from the network, you must add the ports used by the services you require to your firewall list of "allowed ports" if firewall is active.

To add port exceptions to Windows Firewall exception list:

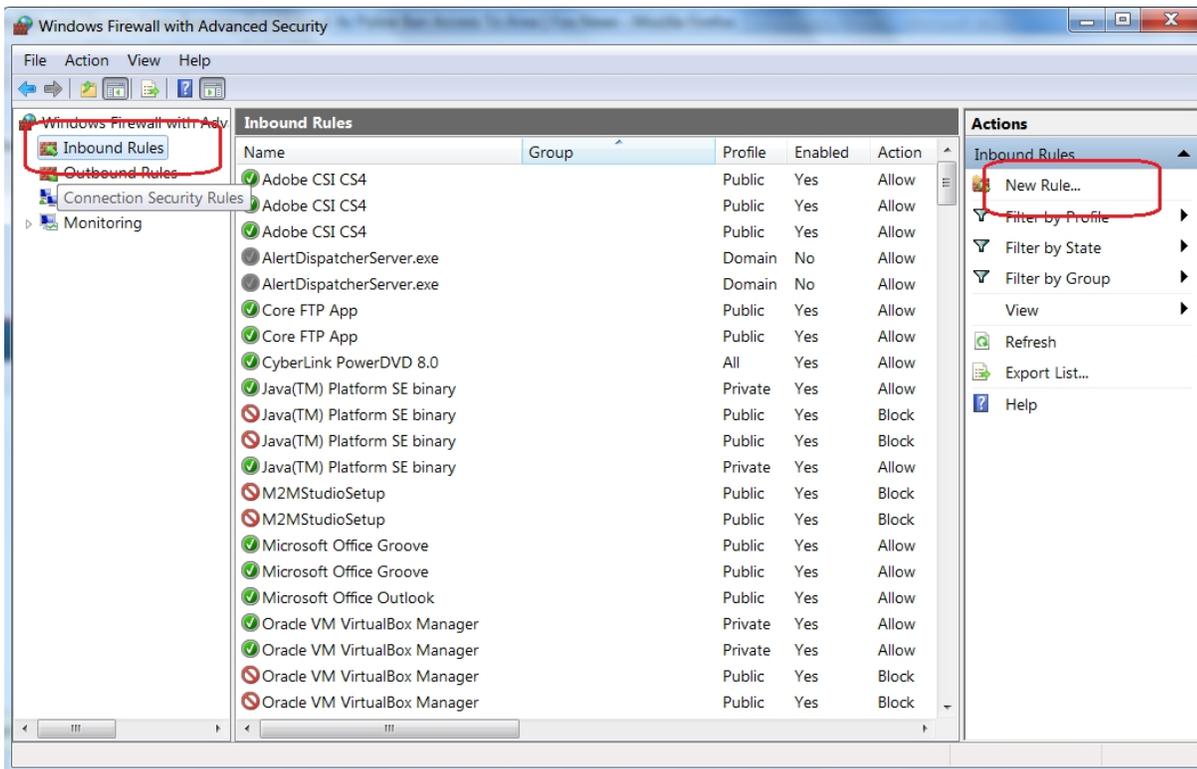
Go to *Start* → *Control Panel* → *Windows Firewall*.



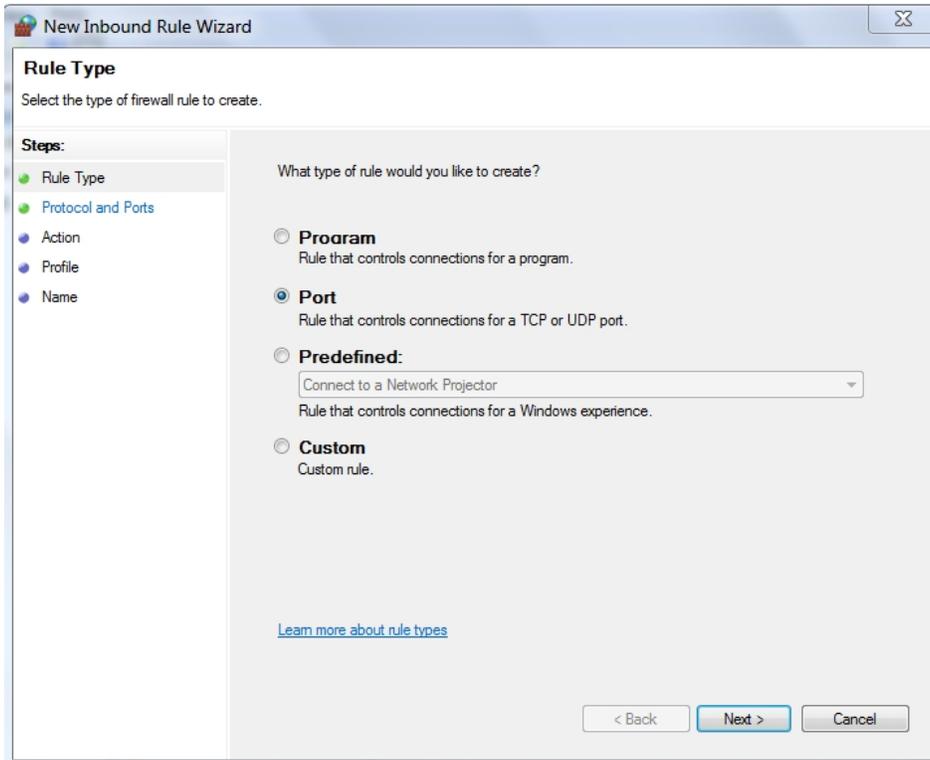
Click "Advanced settings".



Click Inbound Rules, followed by “New Rule”.



Toggle “Port”, click Next.



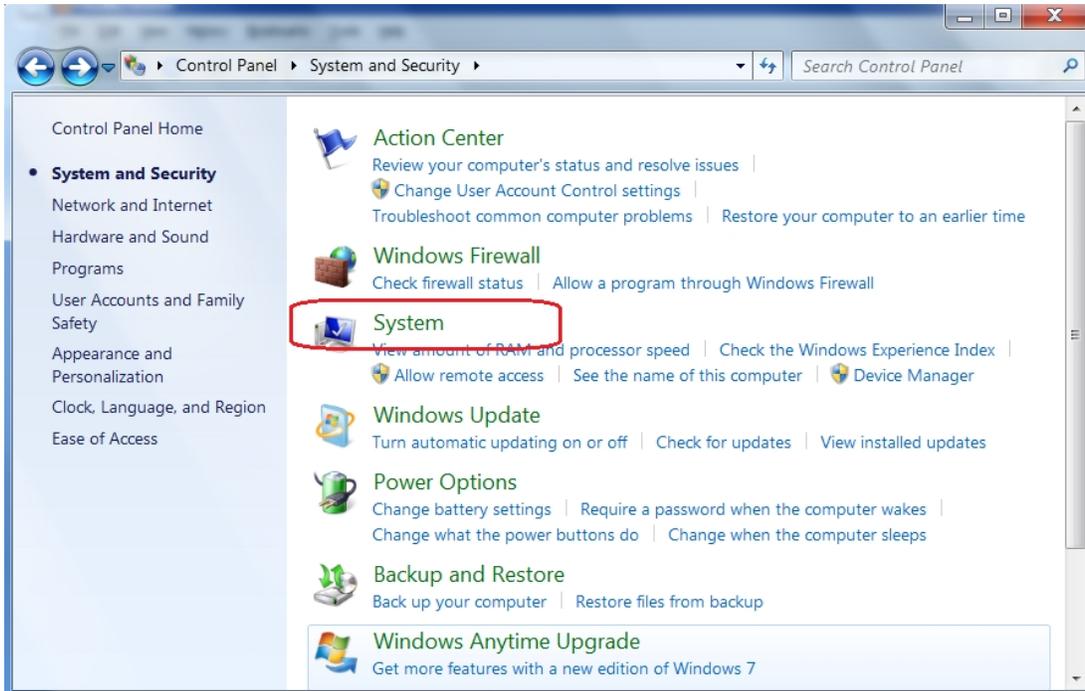
Under “Specific local”, enter “25, 80, 162, 5556” or any other ports you wish to use.

If you are using a 3<sup>rd</sup> party firewall, check with your IT administrator or the firewall vendor.

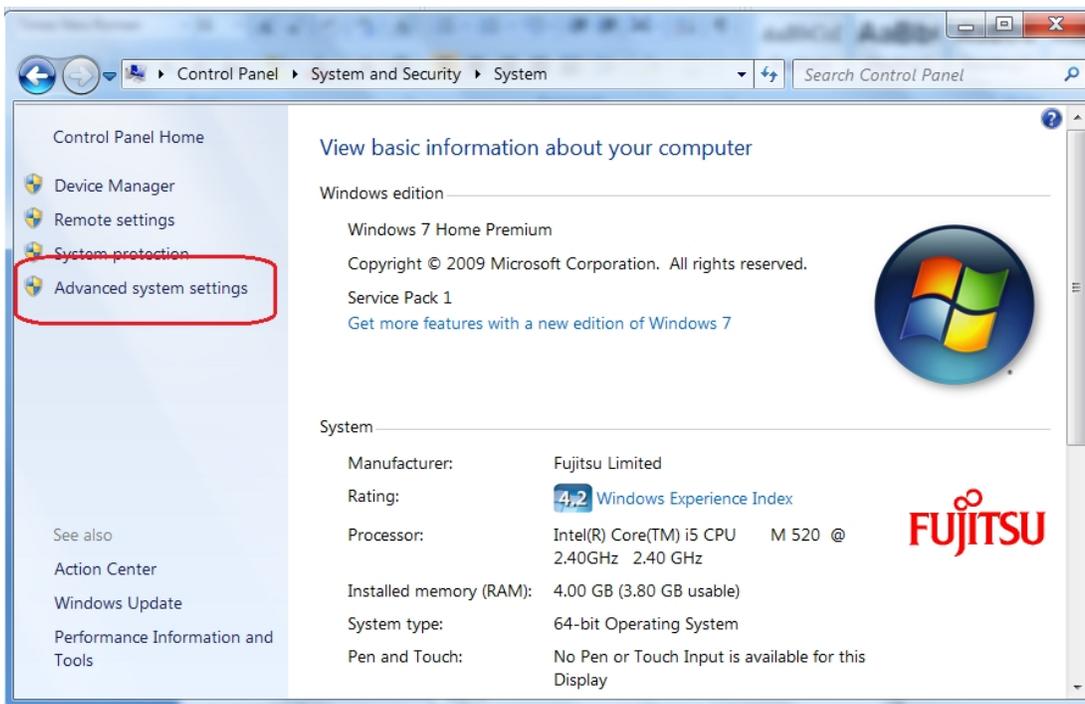
c). DEP exception list.

If DEP is turned on for all programs, you will need to add AlertDispatcherClient.exe and AlertDispatcherServer.exe to the exception list. This is usually done automatically by the installer when you install AlertDispatcher for the first time.

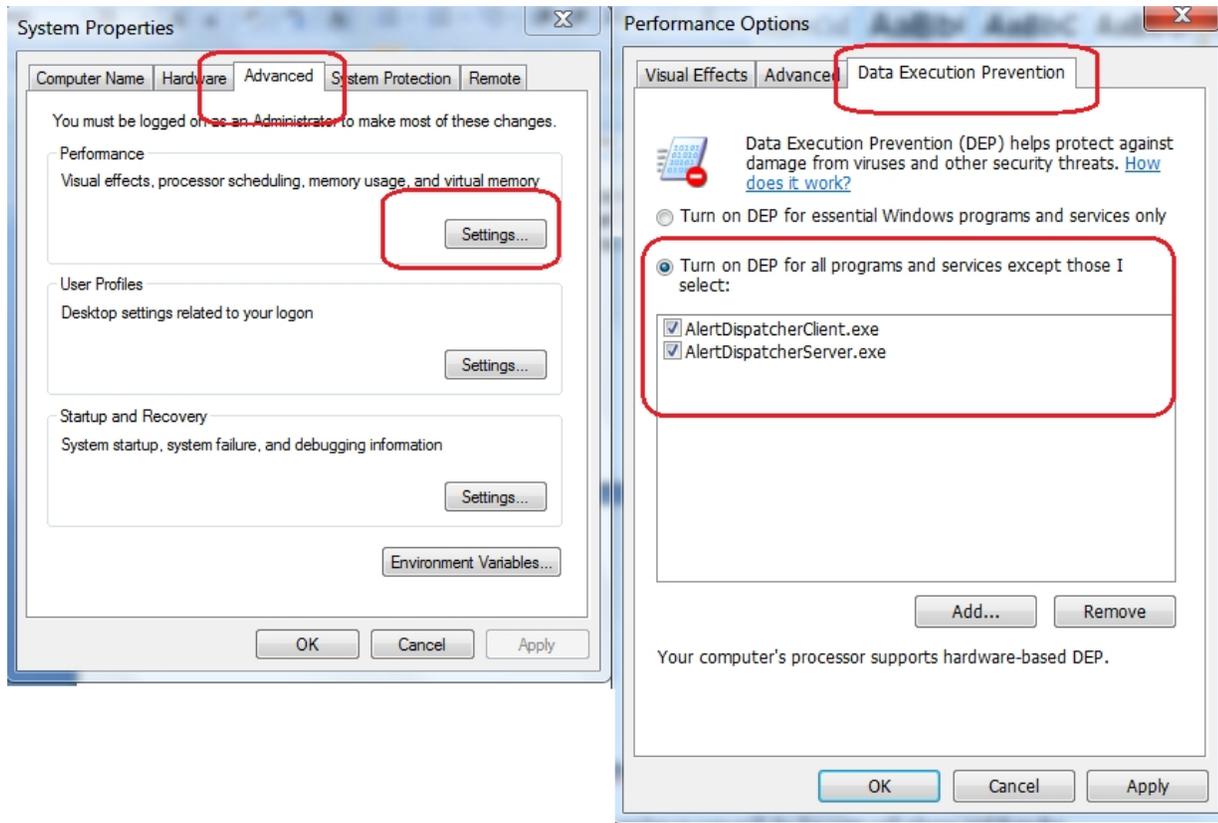
Go to Start → Control Panel → System



Click “Advanced system settings”, “Advanced” tab, followed by “Data Execution Prevention” tab.



If the radio button for “Turn on DEP for all programs and services except those I select:” is checked, please add C:\Program Files\AlertDispatcher\AlertDispatcherClient.exe and C:\Program Files\AlertDispatcher\AlertDispatcherServer.exe to the exemption list.



## 6). Obtaining an SMTP or Email account

In order for AlertDispatcher to send out Emails, you must configure an SMTP user account under “*System Alerts/Email Setup*”. Obtain the SMTP Server address and SMTP username and password from your company email administrator, e.g. Exchange administrator. As far as possible, do not use your email account or an existing email account in case you change your password and forget to update the password set on AlertDispatcher. Create a new email account, e.g. alertdispatcher@yourcompanydomain.

If you do not have a company SMTP Server, you can use your ISP SMTP Server or register a free GMAIL account (GMAIL SMTP Server uses port 587 instead of the standard port 25). Take note that GMAIL has a daily send limit of between 100 to 500 messages, so you must not send to too many recipients to avoid exceeding the limit.

**Note:** In the event that all modems are offline, AlertDispatcher can only send out system alerts via email, so you will need to configure an SMTP account in order to receive such alerts. This is highly recommended if you are using AlertDispatcher for critical purpose.

## 2. Installation, Upgrade, Migration and Configuration

### 1). Installation / Upgrade / Migration

#### a). Upgrade / Migration

If you are upgrading, you may run the new installer onto your existing AlertDispatcher installation (without uninstalling the latter). The new installer will not override your existing configuration. AlertDispatcher will automatically detect and then upgrade your old installation.

To keep this quick start guide as concise as possible for first time user, we have created a separate guide for upgrades and migration - please refer to the “*AlertDispatcher Upgrade and Migration Guide.pdf*” for details.

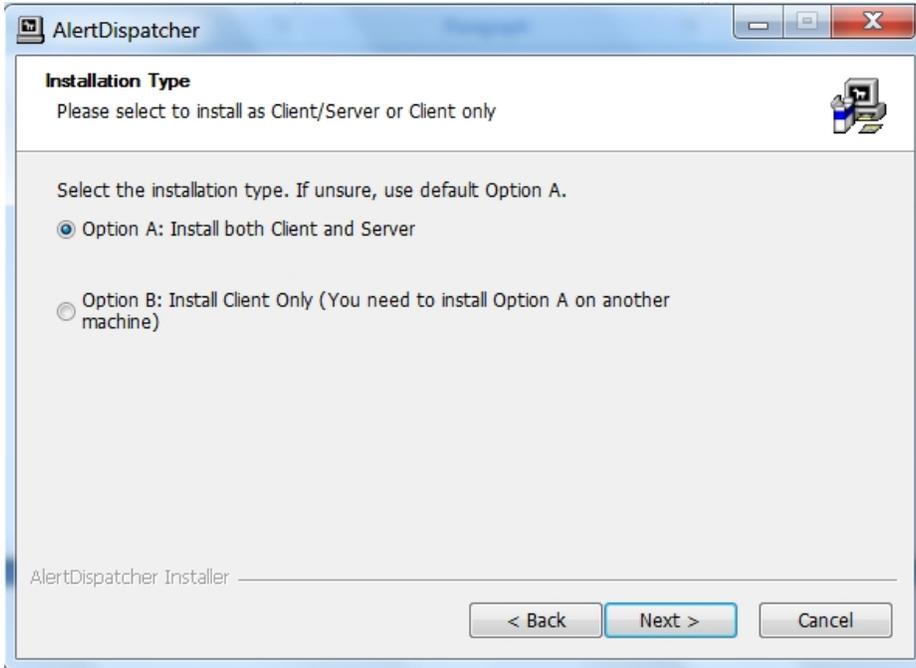
#### b). Installation

Insert the AlertDispatcher CDROM into your PC that you wish to install AlertDispatcher, run AlertDispatcher\_Setup.exe. Follow through the steps in the Setup Wizard.

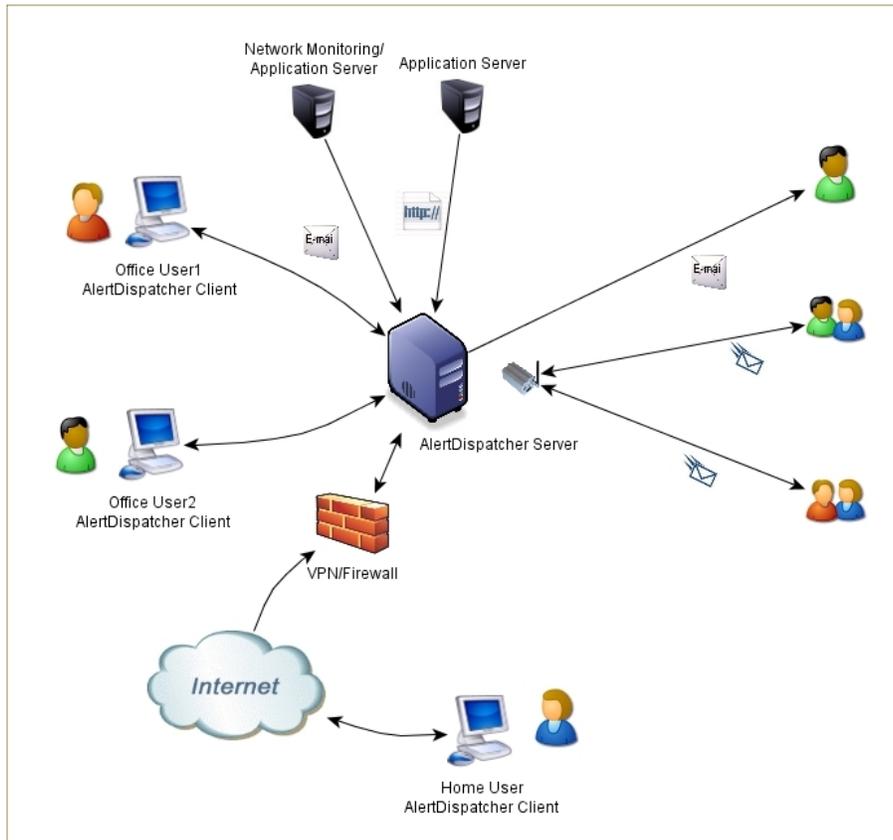


The installer will prompt you whether to install as Client and Server or as a Client only (usually on a workstation). The Client is the management application you use to view messages and to configure and manage AlertDispatcher Server (which may be located on a separate machine).

**Note:** Please install AlertDispatcher Client only if you have purchased the Corporate (or higher) license.



As illustrated in the diagram below, an operator may install AlertDispatcher Client to connect to AlertDispatcher Server remotely. There is no limitation on the number of Client installations.



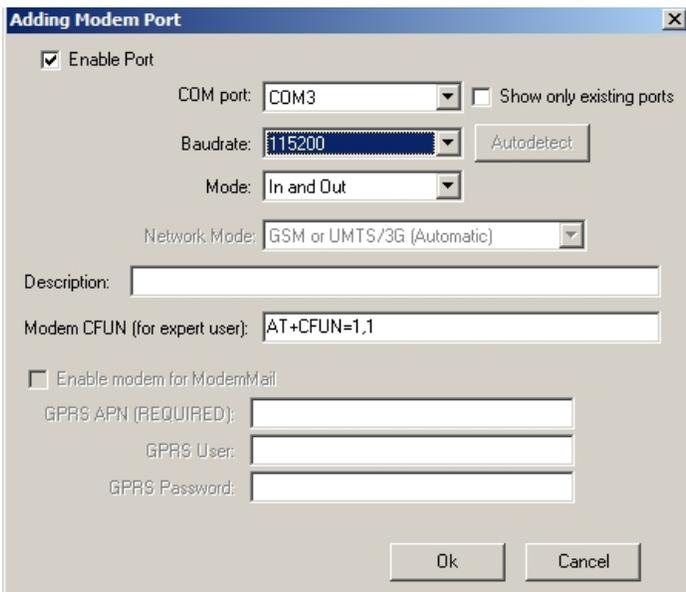
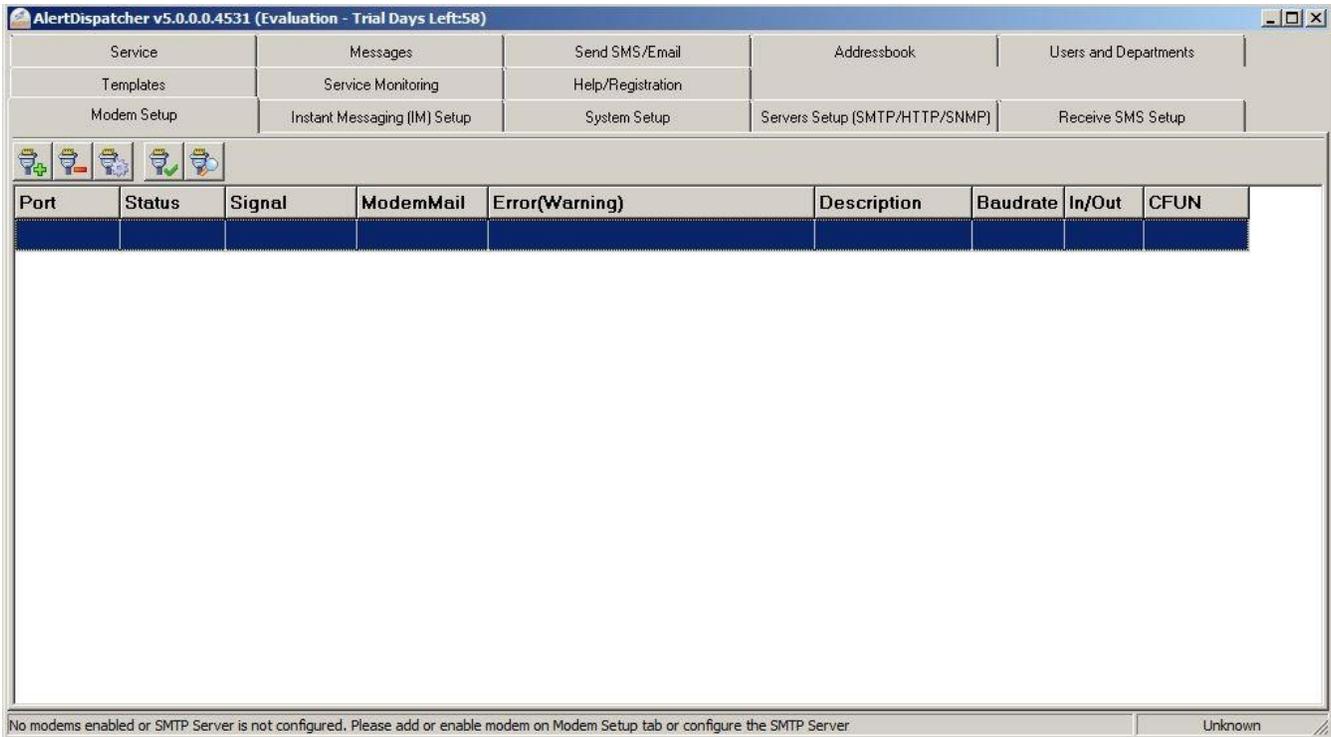
The installer is simple to use, if in doubt, always choose the default or 'Yes' or 'OK' selection when prompted for a selection.

## 2). Configure Modem

a). Add modem

**Note:** If you are using a USB modem, please configure your modem driver as shown in Appendix A.

After installing, run AlertDispatcher Client using the shortcut from Windows Desktop. Plug your modem to your machine and then go to 'Modem Setup', click on the 'Add Modem Port' button .



Check *'Show only exist ports'* – this will display only valid COM ports on the system. Select the COM port which your modem is connected to, followed by the baud rate. The most common baud rate is 115200. If unsure, click *'Ok'* button to create the Modem Port, and then select the Modem Port you have just created from

the list. Click on *'Setup Modem Port'* button  and then click *'Autodetect Baudrate'*. AlertDispatcher will then attempt to connect to the modem using all available baud rates - this may take a few minutes. Alternatively, if you are using a USB modem, you may to *Start* → *Control Panel* → *System* → *Hardware Tab* → *Device Manager* → *Modems* to ascertain the COM port and baud rate onto which the modem driver has been installed.

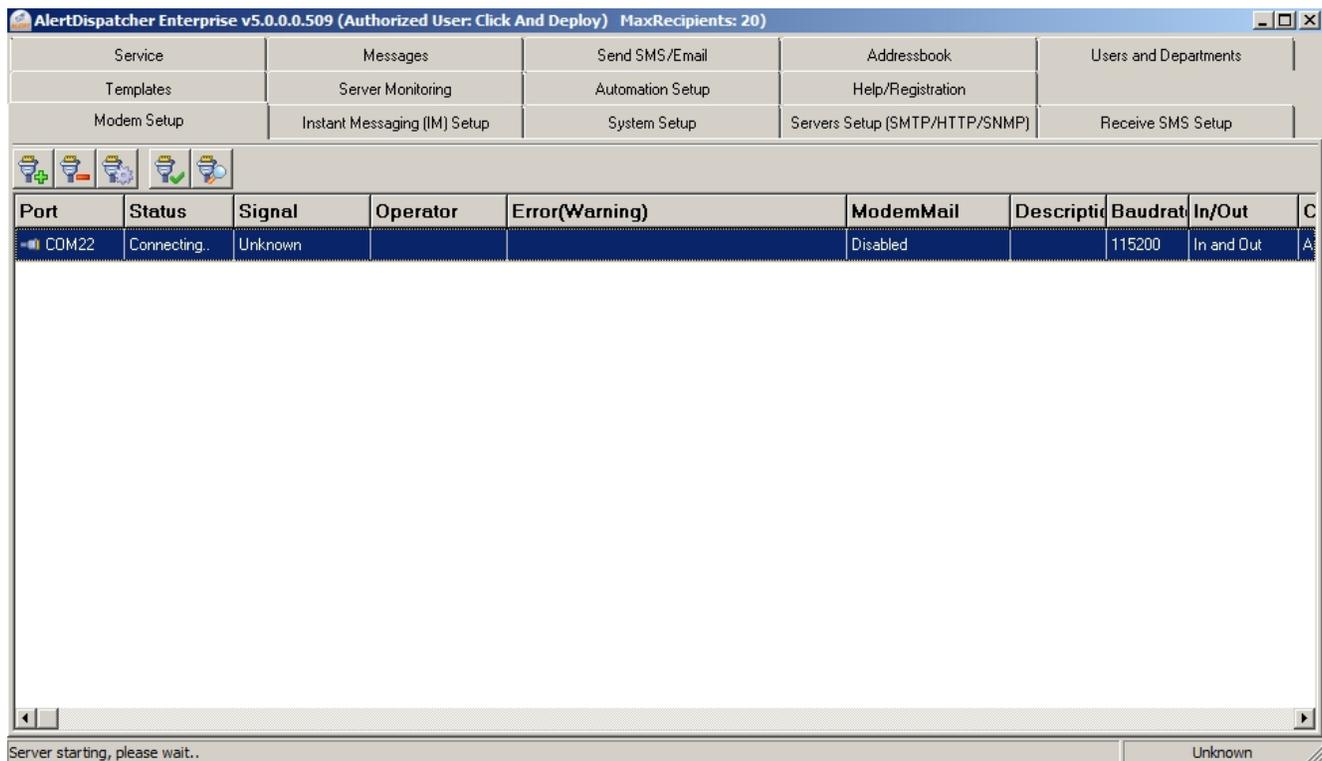
If you're using a supported 3G modem, you can use *'Network Mode'* to configure the modem to connect to 2G or 3G networks.

Next click *'Ok'* button - you will see the *'Server starting, please wait'* message at the status bar at the bottom left of the Window.

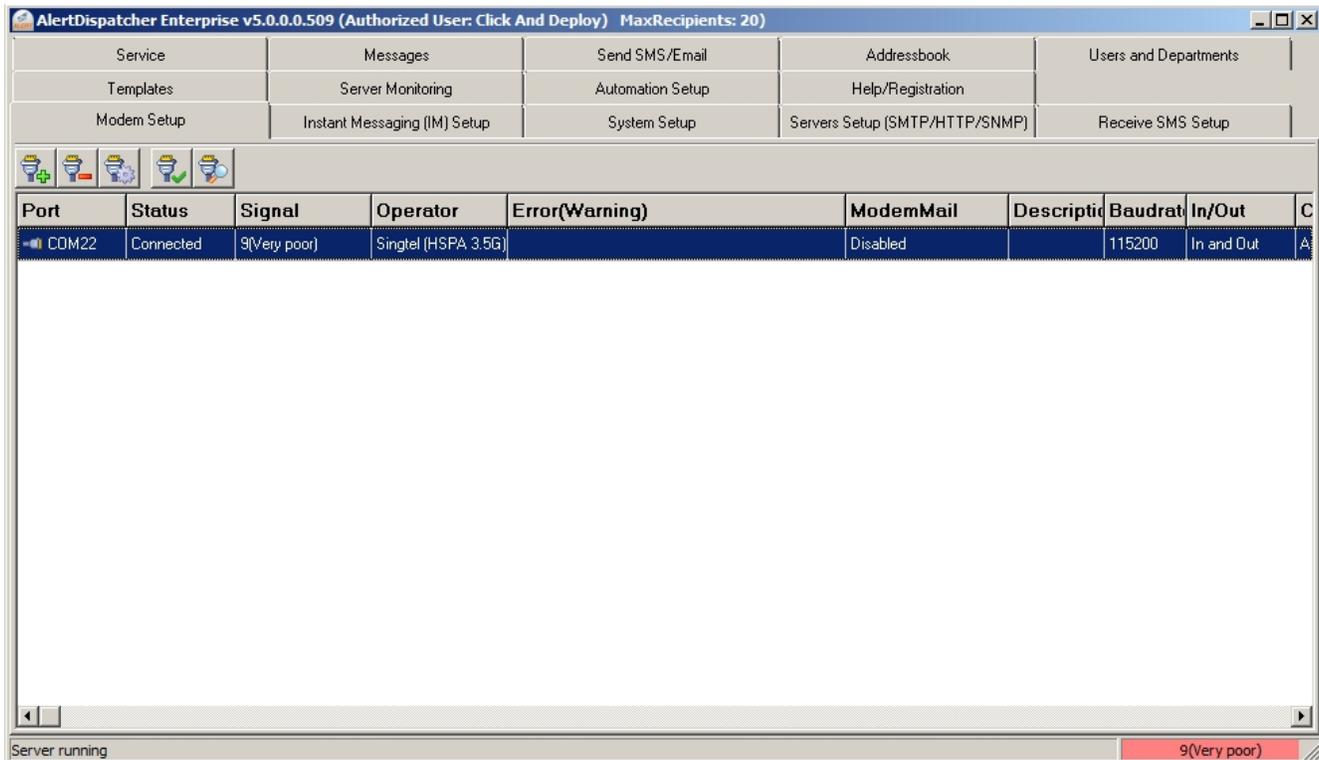
### Note:

a). The setting *'Modem CFUN (for expert user):'* is used for modems that use a different CFUN setting, e.g. Huawei modems. Please do not change this setting unless you know what you're doing.

b). The setting *'Enable modem for ModemMail'* is required only if you need to send Email using the GPRS modem – only works for selected modems. Note that you will need to enable ModemMail under Alerts/Email Setup before you can toggle this setting.



If the setup is correct, you will see the *'Server running'* along with the signal strength on the right corner, otherwise an error message such as the following may appear (see below).



## b). Troubleshooting modem connection issues

If you're getting an error, check the following:

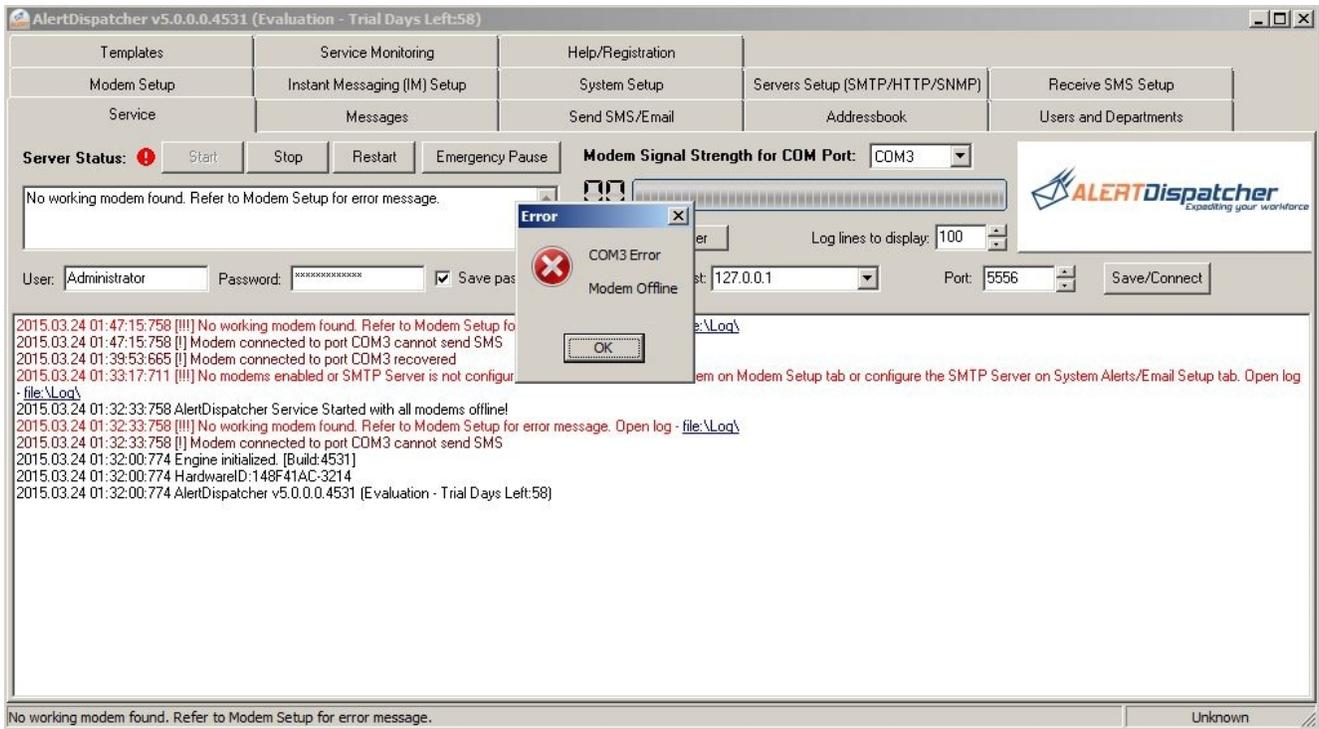
1. Ensure that the modem is connected to the COM port which you have previously configured. If you are using the PC original COM ports, it should be either COM 1 or COM2. Ensure that the COM port is not occupied by another application.

If you are using USB or external serial card, the driver must be installed. You can usually locate the COM port from *Start → Control Panel → System → Hardware Tab → Device Manager → Modems* or *Start → Control Panel → System → Hardware Tab → Device Manager → Ports (COM & LPT)*.

2. A working SIM card with no PIN protection is inserted into the modem. Most modems come with a network indicator light that will flash or blink if the modem is connected to the GSM network. You should also be able to send SMS Alerts if you insert the SIM card into your cell phone.

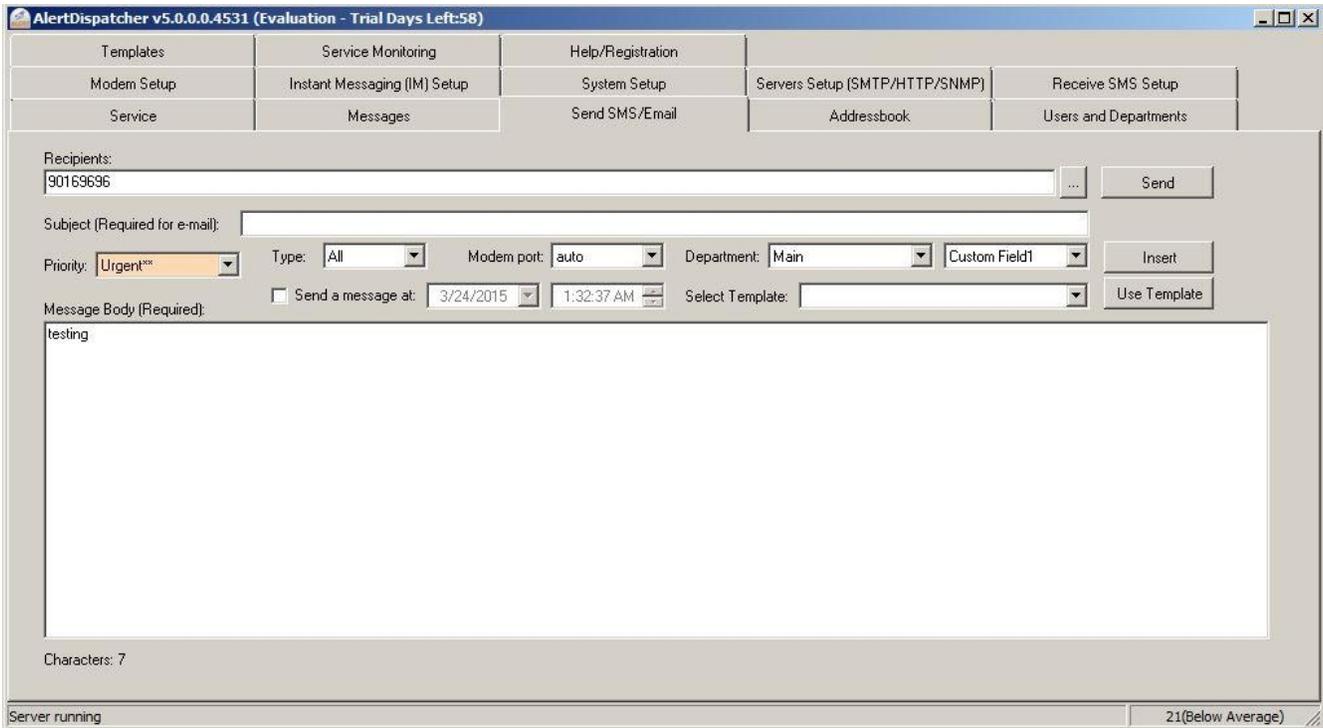
If the modem network indicator light is not blinking, check that the SIM card is properly inserted and then reset or switch off and on the modem. Also refer to [Appendix A](#) for details on preparing the GSM modem.

3. Verify that you are using the correct baud rate. The most common baud rate is 115200. If unsure, click 'Autodetect Baudrate' – this may take a few minutes.

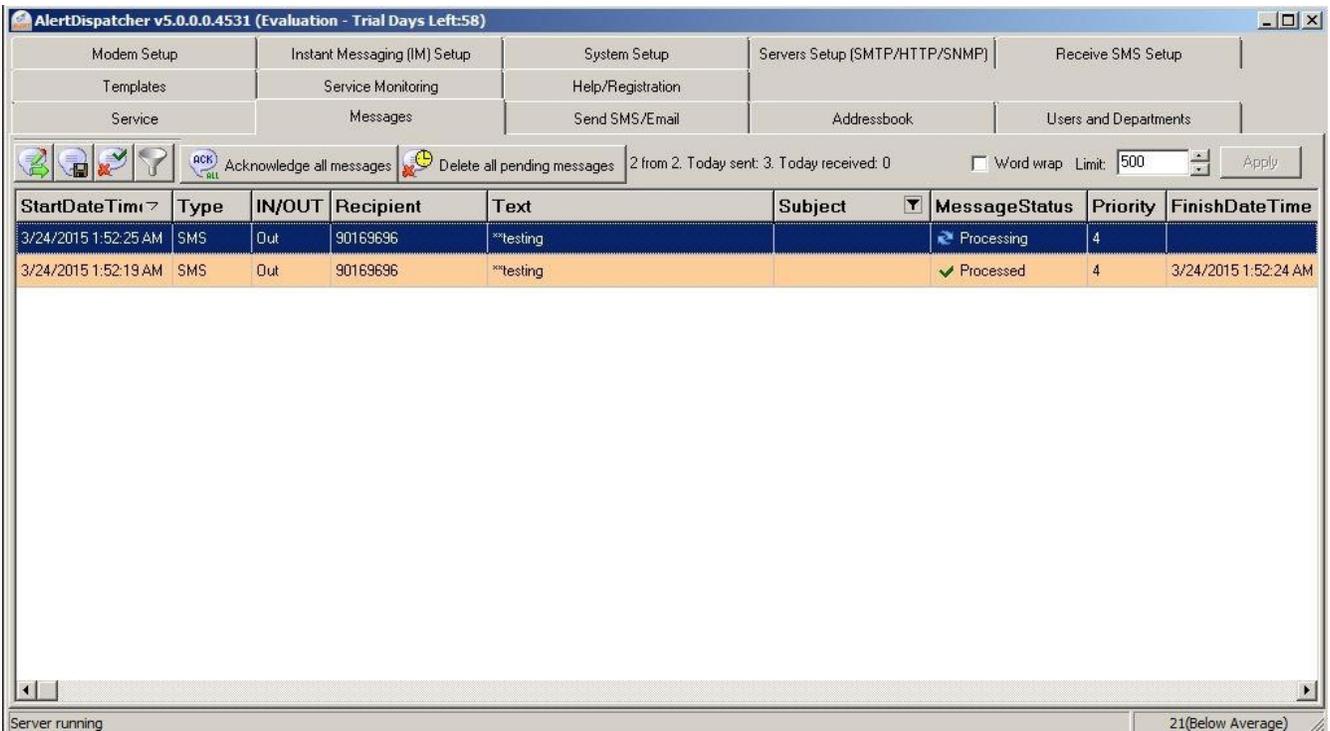


### c). Send test SMS

Once the modem has been successfully detected, you can test by sending a test Alert SMS to yourself. Go to 'Send SMS/Email' Tab, type in your phone number as you will do for your cell phone and then the message. Click 'Send' button.



If the phone number is correct and the modem is working, you should get the following screen. If not, verify that the SIM card is working using your cell phone.

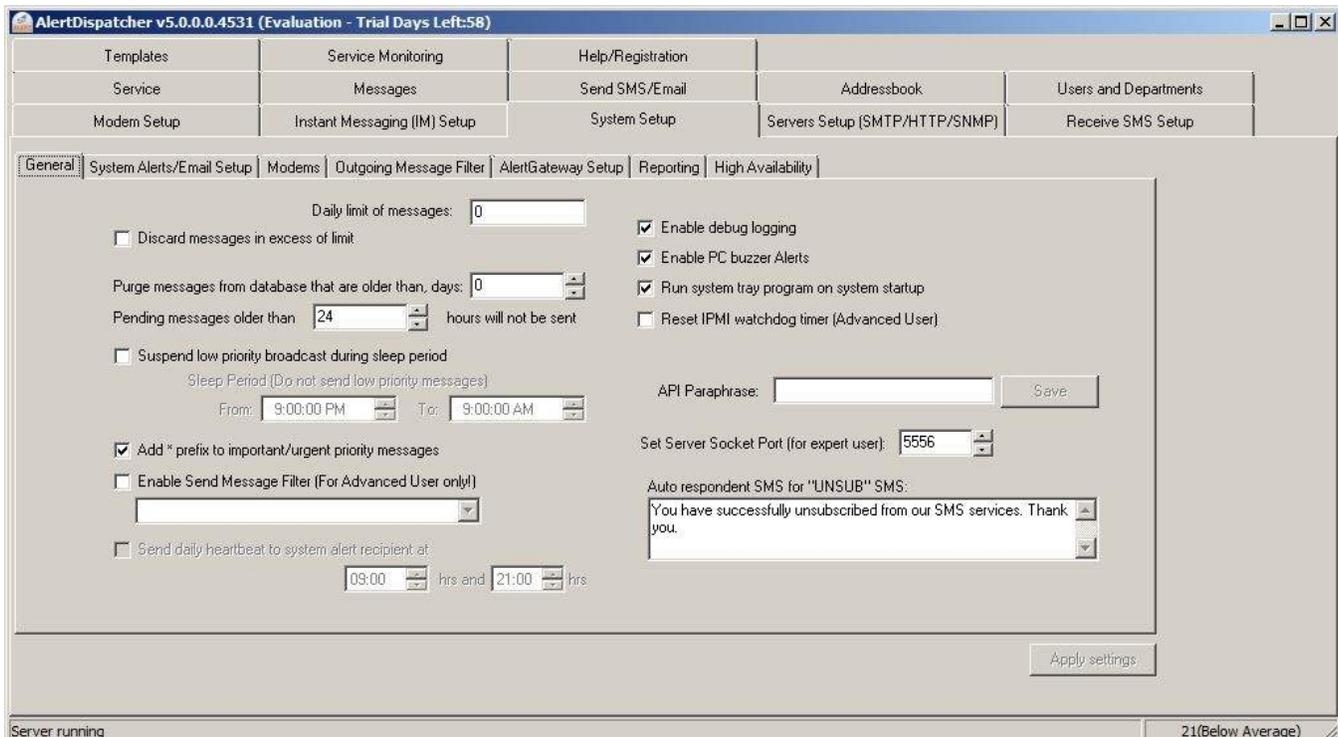


**Note:** You still can't send email until you have configured the SMTP Server and credentials AlertDispatcher will use to dispatch Emails. See "Configure System and Alerts Setup" for details.

### 3). Configure System and Alerts Setup

#### a). System Setup - General

AlertDispatcher comes with some configurable settings which you can modify. The default settings are recommended values and should work for a typical installation.



The *'Daily limit of messages'* setting limits the maximum number of messages that can be sent in one day. To impose no limit, set *'Daily limit of messages'* to 0 (default value).

**Note:** The daily message limit defaults to 2000 for AlertDispatcher versions earlier than v3.1.

To discard excess messages (above the daily limit), enable *'Discard messages in excess of limit'*.

*'Purge messages from database that are older than x days'* setting runs a task that purges old messages from the database that are older than the configured number of days. This task runs once a day.

**Note:** For performance reason, AlertDispatcher will only keep up to 100,000 messages in the database. When this limit is exceeded, the oldest 10,000 messages will be automatically purged.

*'Suspend priority 1 broadcast during sleep period'* setting allows you to setup a *'sleep period'* in which all priority 1 broadcasts are suspended during that period of time. Broadcast will resume after the time period has ended. **Note:** Messages with priority higher than 1 will still be sent during this *'sleep period'*.

*'Enable Send Message Filter'* is available for Corporate and higher licenses only. Do not enable unless you have consulted with your vendor as doing so may disrupt services. See next section for more information.

'*Send daily heartbeat to system alert recipient*' is used to schedule a twice daily heartbeat alert (SMS/Email) – see example below - to the system alert recipient configured under "*System Alerts/Email Setup*". You must configured the system alert recipient before you can enable '*Send daily heartbeat to system alert recipient*'.

*[ALERTSERVER]: HeartBeat at 17:00 hrs.  
Status: AlertDispatcher - Running  
[Created: 17:00:00 2014-03-13]*

'*Enable debug logging*' is used to debug modem communication and modem hardware issues and for new installations, you're recommended to enable it.

'*Enable PC buzzer Alerts*' is used to sound the PC buzzer on AlertDispatcher Server and AlertDispatcher Clients whenever there is an error. For example, a continuous melody will be played if a modem cannot be detected. You can stop this melody either by rectifying the modem issue or acknowledging the Alert using AlertDispatcher Client.

'*API Paraphrase*' is used to protect access to AlertDispatcher Server via API. If high security is required, you should configure a password for API Paraphrase.

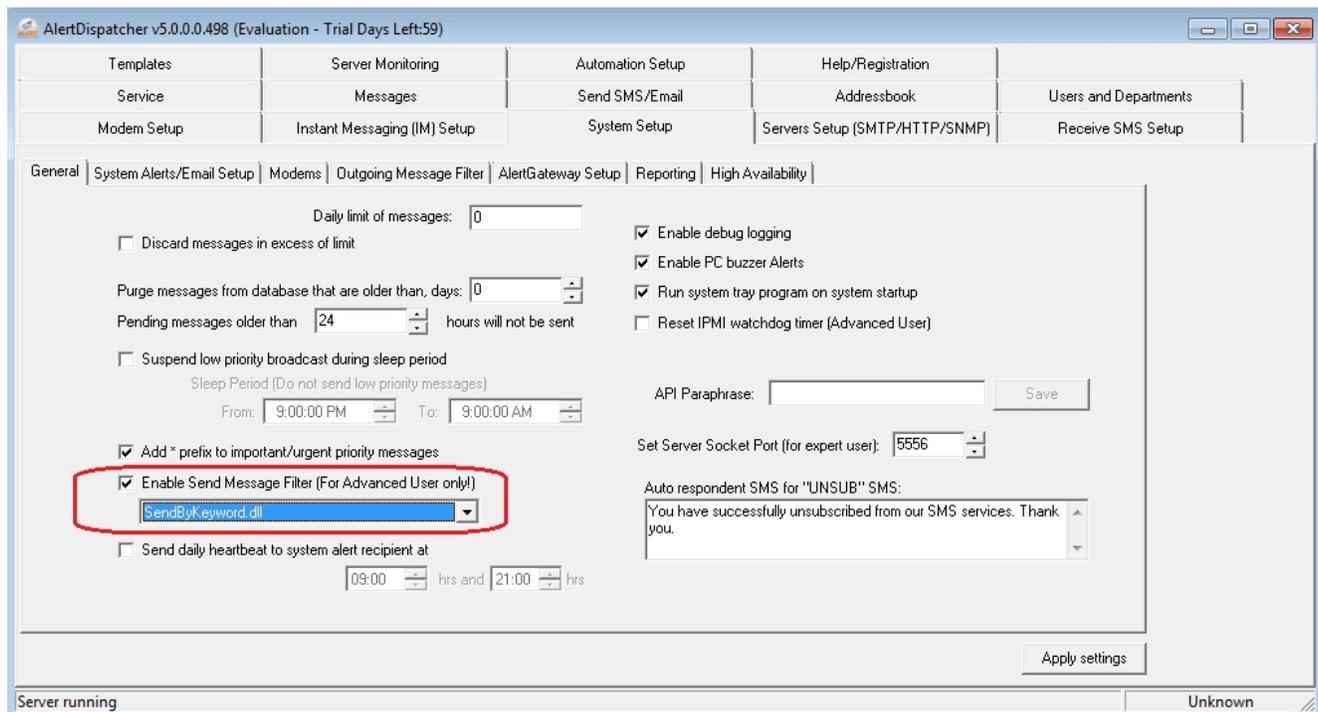
'*Set Server Socket Port (for expert user)*' allows you to change the default port 5556 which the server uses to communicate with AlertDispatcher Client and APIs. Please refrain from changing this setting unless necessary.

## b). System Setup - Send Message Filter

*i). "SendByKeyword" filter*

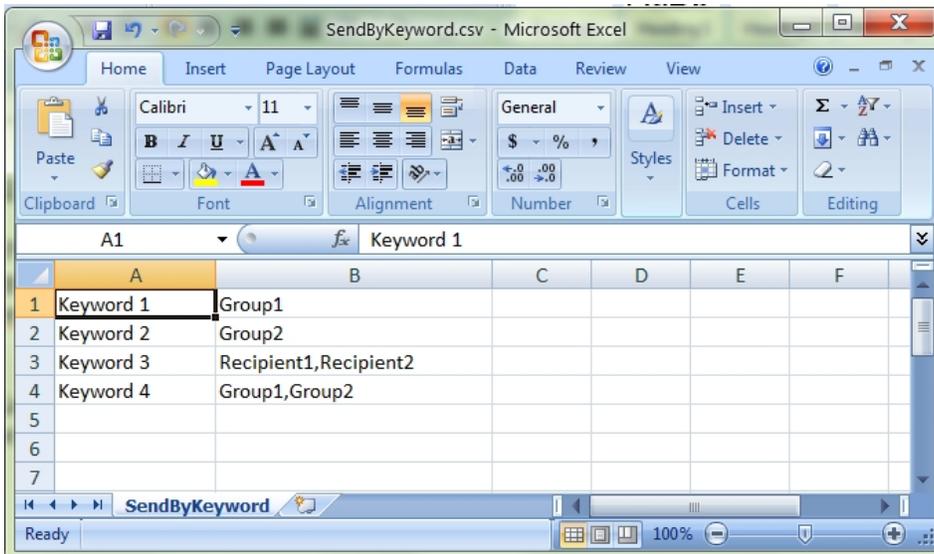
The "SendByKeyword" Send Message Filter (*SendByKeyword.dll*) is used to redirect messages to different groups of recipients based on the message keyword. This is done using the CSV file (C:\Program Files\AlertDispatcher\Configuration\SendByKeyword.csv) that will act as a lookup table matching the recipients to a keyword. A keyword can be associated with multiple recipients/recipient groups.

The SendByKeyword filter is useful in scenarios where there are a large number of unique items or identifiers that need to be matched to different recipients, e.g. building alarms with hundreds or even thousands of automation point identifiers that need to be sent different groups of recipients.



A sample "SendByKeyword.csv" will be installed by default. You can open the sample CSV file using Excel and make changes onto it directly. To save your changes to the CSV file, click on the "Save" button.

See C:\Program Files\AlertDispatcher\Configuration\SendByKeyword.ini for more configuration options.



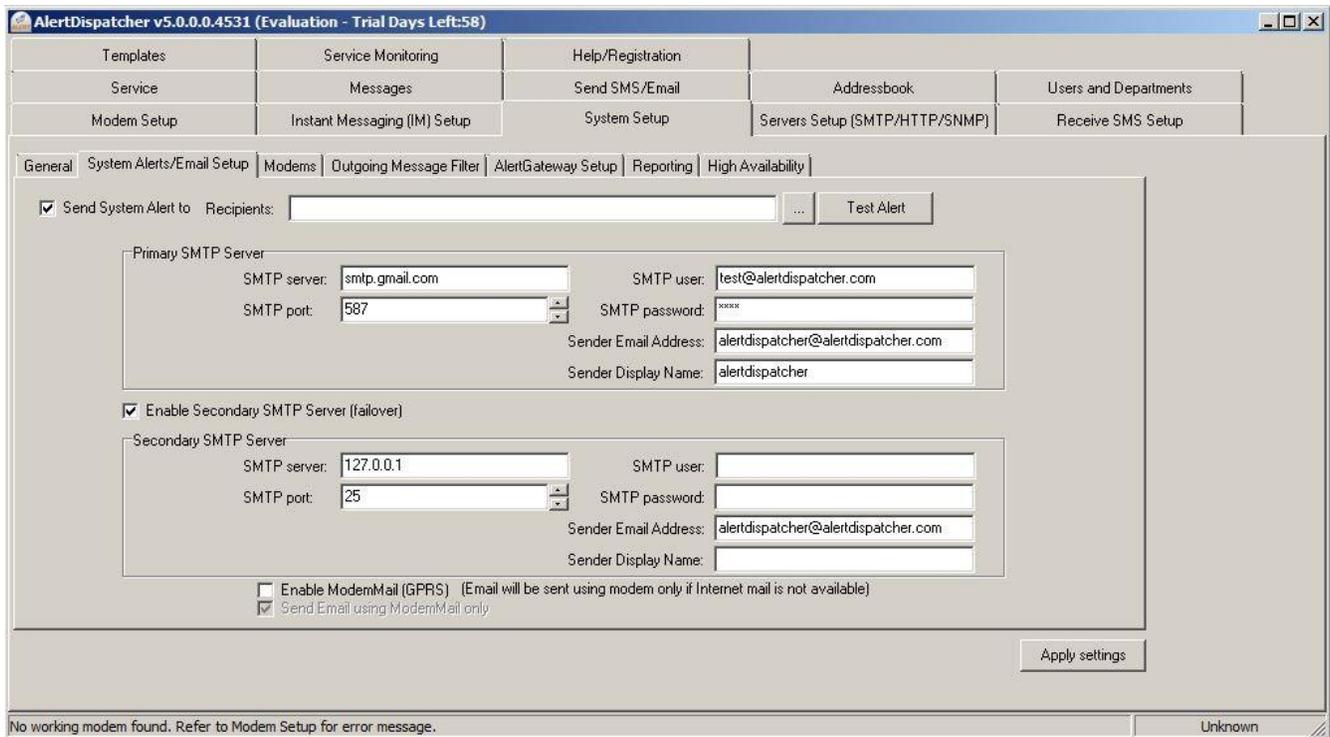
**Warning:** Enabling the Send Message Filter incorrectly may cause service disruption. Please consult with your vendor if in doubt.

### c). System Setup – System Alerts/Email Setup

In order for AlertDispatcher to send out Emails, you must configure an SMTP user account under “*System Alerts/Email Setup*”.

AlertDispatcher can be configured to send a system alert message (Email/SMS) on encountering a modem or system error. You can configure the system alert recipient under “*Send System Alert to:*”. This is highly recommended if you are using AlertDispatcher for critical purpose.

Click "Test Alert" to test send an email and check the Messages tab for the send status.



Obtain the SMTP Server address and SMTP username and password from your company email administrator, e.g. Exchange administrator. As far as possible, do not use your email account or an existing email account in case you change your password and forget to update the password set on AlertDispatcher. Create a new email account, e.g. alertdispatcher@yourcompanydomain.

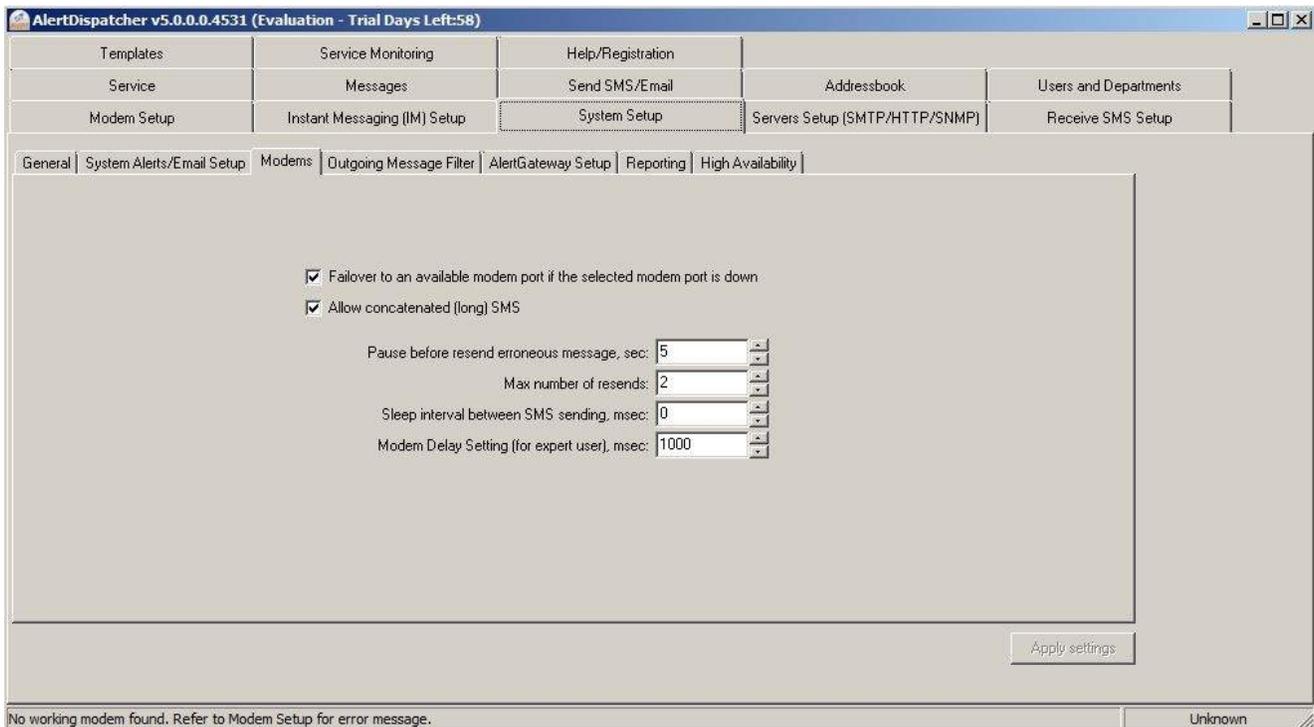
If you do not have a company SMTP Server, you can use your ISP SMTP Server or register a free GMAIL account (GMAIL SMTP Server uses port 587 instead of the standard port 25). Take note that GMAIL has a daily send limit of between 100 to 500 messages, so you must not send to too many recipients to avoid exceeding the limit.

If you are using the Corporate license (or higher licenses), you can configure a Secondary/failover SMTP Server in case emails cannot be sent out using the Primary SMTP Server. This is recommended if you are using AlertDispatcher for critical purpose as emails can fail to send out for multiple reasons besides server failure, e.g. email password has been changed and not updated over at AlertDispatcher, email user has been deleted, emails recipients blocked by SMTP Server, etc.

**Note:** You must enable '*Enable ModemMail (GPRS)*' if you want to allow AlertDispatcher to be able to send Email using the GPRS modem. Please do not enable this feature unless you need it as it may incur additional GPRS costs on your SIM card bill.

If '*Send Email using ModemMail only*' is not enabled (the default setting), AlertDispatcher will attempt to send out Emails via TCP/IP network first, and only if that method fails, failover to ModemMail.

## d). System Setup - Modems

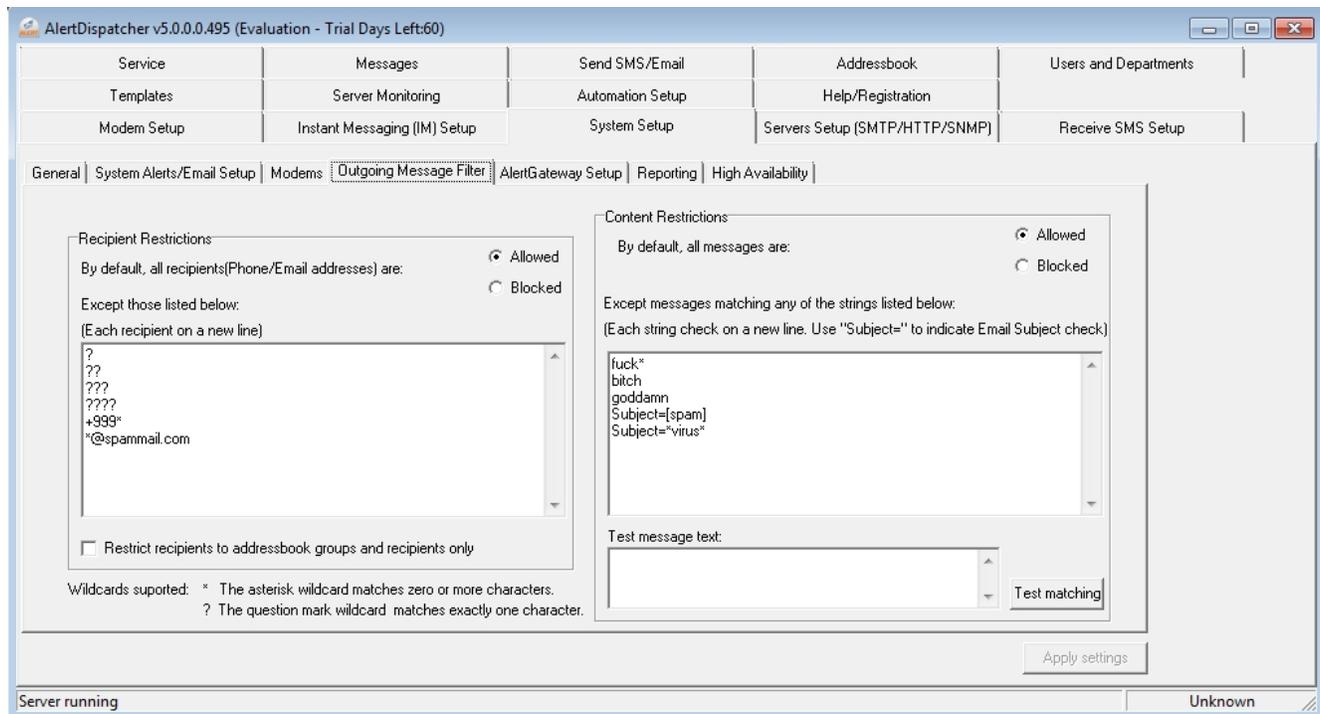


By default, AlertDispatcher will automatically failover to an available modem port if the selected modem is not working. The default setting is recommended for critical operations.

If '*Allow concatenated (long) SMS*' is not enabled, messages will be truncated to 160 characters for ASCII text and 70 characters for Unicode text. More phones made within the last 5 years can support concatenated SMS of up to 6 SMS in length.

## e). System Setup – Outgoing Message Filter

You can setup '*Outgoing Message Filters*' to block Email and SMS messages to particular recipients (wildcard characters supported) and also messages that contain certain strings. The asterisk wildcard character matches zero or more characters. The question mark wildcard character matches exactly one character.



In the above example, recipients containing 1 to 4 characters only (? , ?? , ??? , ????) , and recipients beginning with +999 (+999\*) , e.g. +9991234567 are restricted. To block all international SMS, simply block the prefix, e.g. +\* or 00\* (different networks use different prefixes).

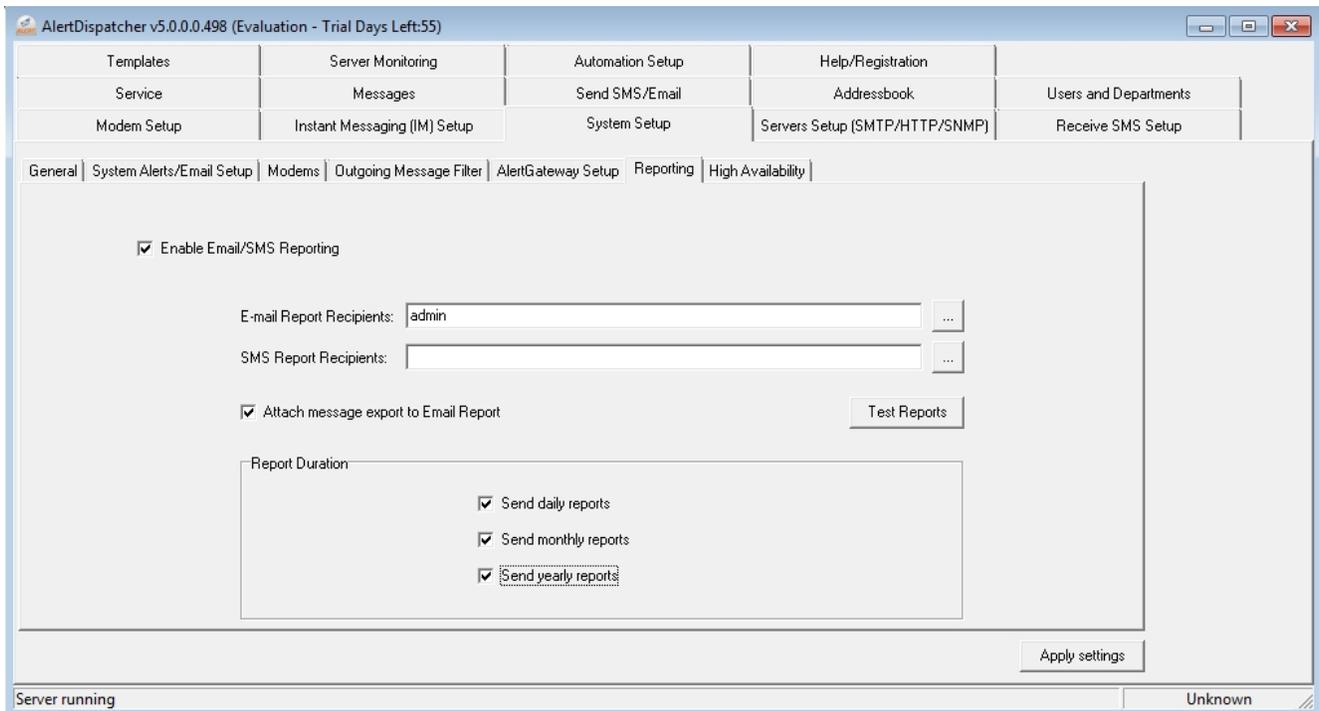
The check string *'bitch\*'* will block all messages with the keyword *'bitch'* followed by any other characters, e.g. *'bitch!'* and *'bitchyou!'* will be restricted. However, *'hibitch'* will be allowed.

Note that for the case of phrases (more than one word separated by spacing), the asterisk wildcard will be automatically added to the beginning and end of the phrase. For example, the check string *'god damn'* will block the message *'God Damnit!'*.

The "Restrict to recipients addressbook groups and recipients only" setting will block all messages sent to recipients not defined in the addressbook if enabled.

#### f). System Setup – Reporting

AlertDispatcher can be configured to send Daily/Monthly/Yearly usage reports by SMS or/and Email (breakdown by department/sender). Message export in CSV format for the report time period can be attached to Email reports.



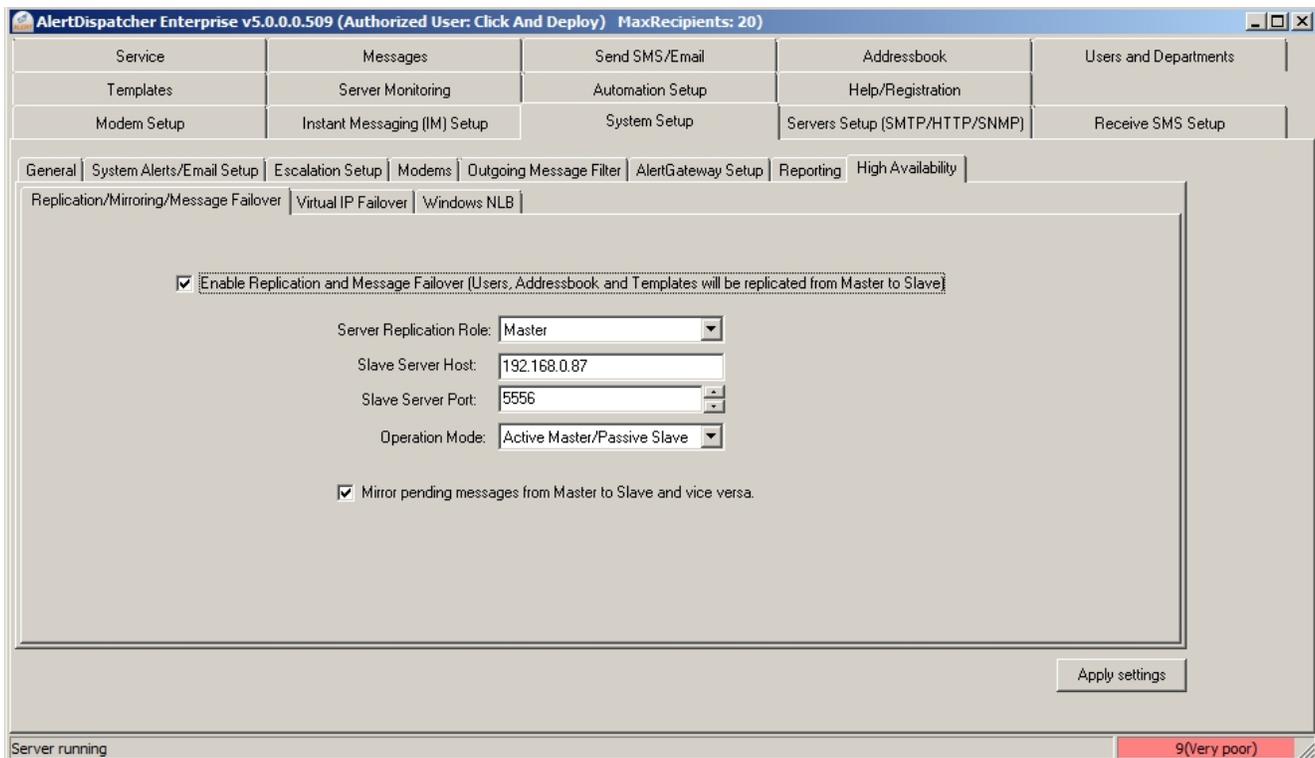
### g). System Setup – High Availability

AlertDispatcher deployed in a standalone node provides limited high availability by monitoring and reporting errors in communication channels (signal quality, network access) and automatic failover to redundant communication channels (modems and SMTP servers).

To provide real high availability, it is necessary to add a redundant AlertDispatcher node to form a server cluster. You can install AlertDispatcher on a Windows Network Load Balancing Cluster (or NLB cluster) to distribute messages across cluster nodes.

#### *i). Network Load Balancing Cluster*

If you are using the Corporate license (or higher licenses), you can add "application-aware" failover capability to your Windows cluster by enabling the setting *“Automatically Remove local host from Windows Network Load Balancing Cluster on server failure or when no modems are working...”*. When this setting has been enabled, AlertDispatcher will remove failed nodes from the cluster automatically so that messages won't be sent to these nodes.



### *ii). Enable Replication and Message Failover*

If you are using the Enterprise license, you can enable the setting “*Enable Replication and Message Failover (Users, Addressbook and Templates will be replicated from Master to Slave)*” to enable automatic message failover (both ways) across the Master and the Slave node – in a replication setup, a node can be configured as either a *Master* or a *Slave* role using the “*Server Replication Role*” setting. Changes to Users, Addressbook, Template, System Alert Recipient and Daily Heartbeat setting on the Master node will be replicated to the Slave node – you can only update users and addressbook on the Master node.

### *iii). Mirror Pending Messages*

The “*Enable Replication and Message Failover*” setting does not ensure message persistency, so messages already queued on a node that failed will be lost. To ensure message persistency, you need to enable an additional setting “*Mirror pending messages from Master to Slave and vice versa*”.

This setting provides additional high availability by replicating messages queued on either Slave or Master node on the other node. If a particular node fails or crashes, pending messages that are in queue in the failed node will be sent using the other node automatically. This is possible because all queued messages will be replicated on the other node.

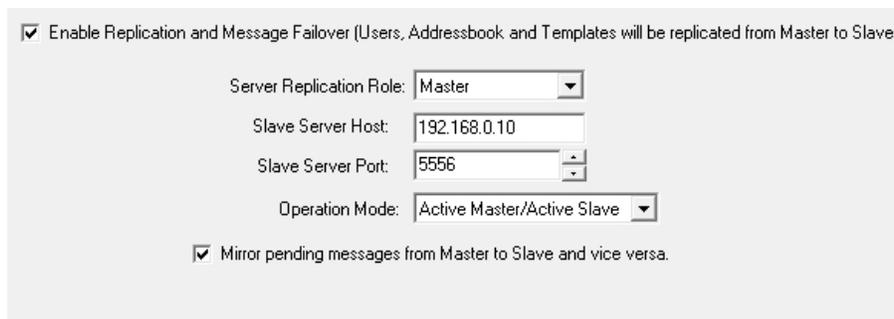
### *iv). Operation Mode*

The “*Operation Mode*” setting determines whether the “Slave” is an “Active” Slave or a “Passive” backup - a “Passive” backup does not process messages until the “Active” node fails. For simplicity, the Master node will always be the first active node. The Slave node can be either Active (2nd Active node) or Passive according to “*Operation Mode*” setting.

If "*Operation Mode*" is "*Active Master/Active Slave*" (the default setting), both Master and Slave nodes will process messages sent to them concurrently (by interfacing application) and act as backup for each other (2-way message replication) in the event of failover of either node.

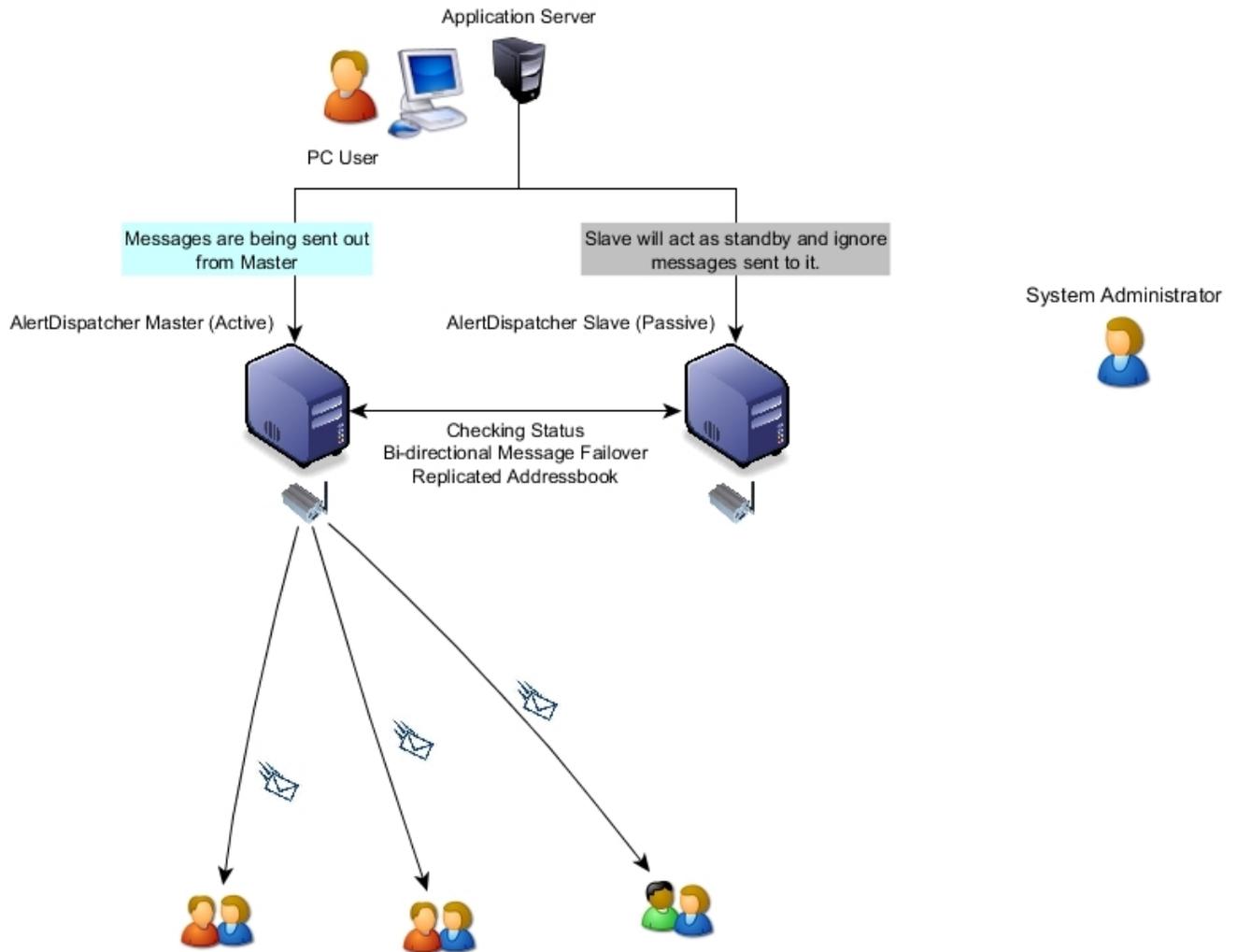
If "*Operation Mode*" is changed to "*Active Master/Passive Slave*", messages sent to Slave node will be ignored until the Master node is offline. If the interfacing application can send the same message to both nodes, this setup confers an additional level of high availability. The message sent to Slave node (passive) will be ignored as long as the Master node is online. In the event of failure of the Active Master, the message sent to the Passive Slave node will be processed and sent out.

**Note:** You do not need to install Windows Network Load Balancing Cluster to make use of the "Enable Replication and Message Failover" and "Mirror pending messages from Master to Slave and vice versa" setting.

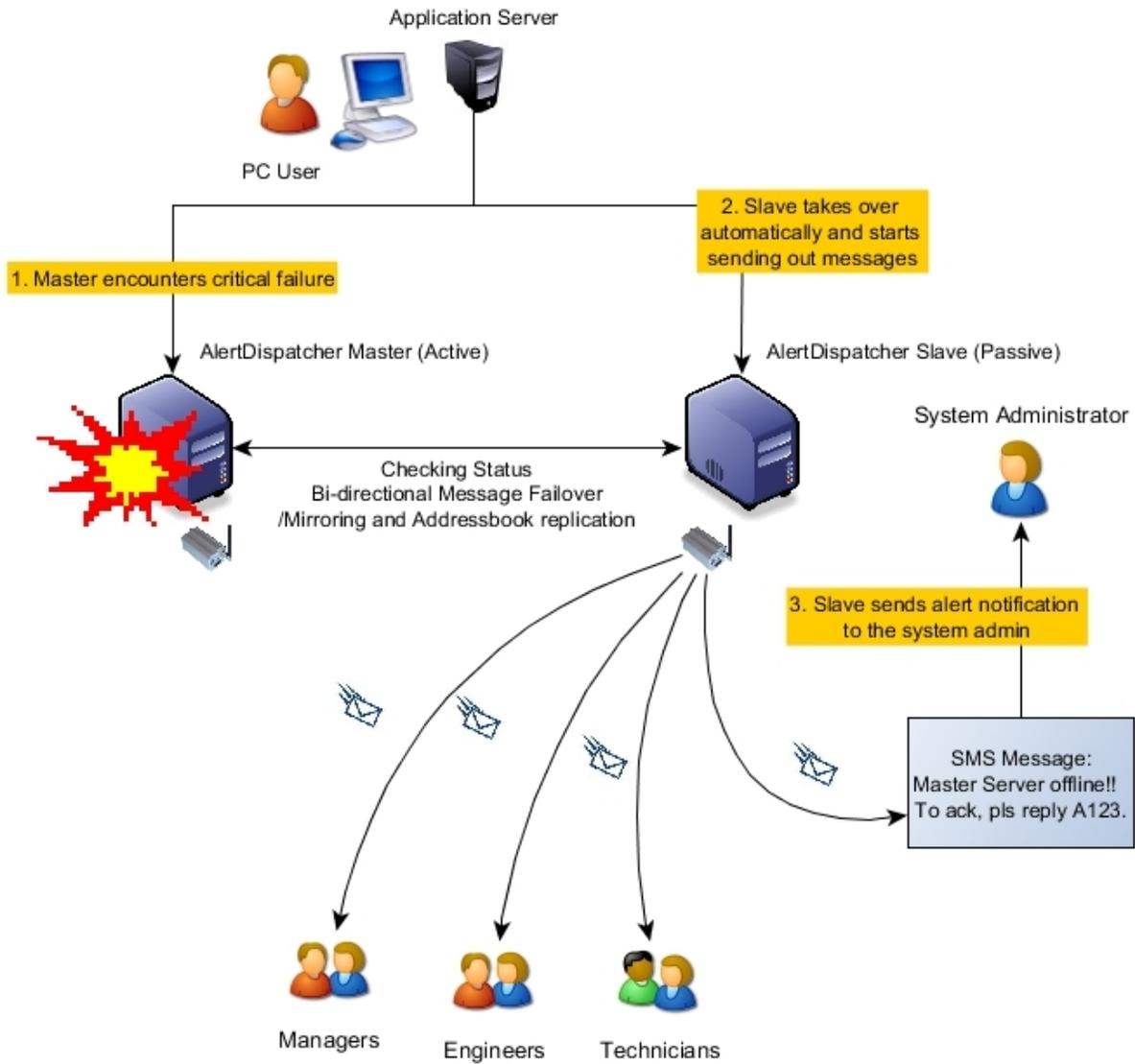


The screenshot displays a configuration window for AlertDispatcher. At the top, there is a checked checkbox labeled "Enable Replication and Message Failover (Users, Addressbook and Templates will be replicated from Master to Slave)". Below this, there are four input fields: "Server Replication Role" is a dropdown menu set to "Master"; "Slave Server Host" is a text box containing "192.168.0.10"; "Slave Server Port" is a spinner box set to "5556"; and "Operation Mode" is a dropdown menu set to "Active Master/Active Slave". At the bottom, there is another checked checkbox labeled "Mirror pending messages from Master to Slave and vice versa."

The following diagram shows normal operation for an Active Master/Passive Slave cluster.



Upon failure of the Active Master node, the Passive Slave takes over.



## 4). Configure Users and Departments

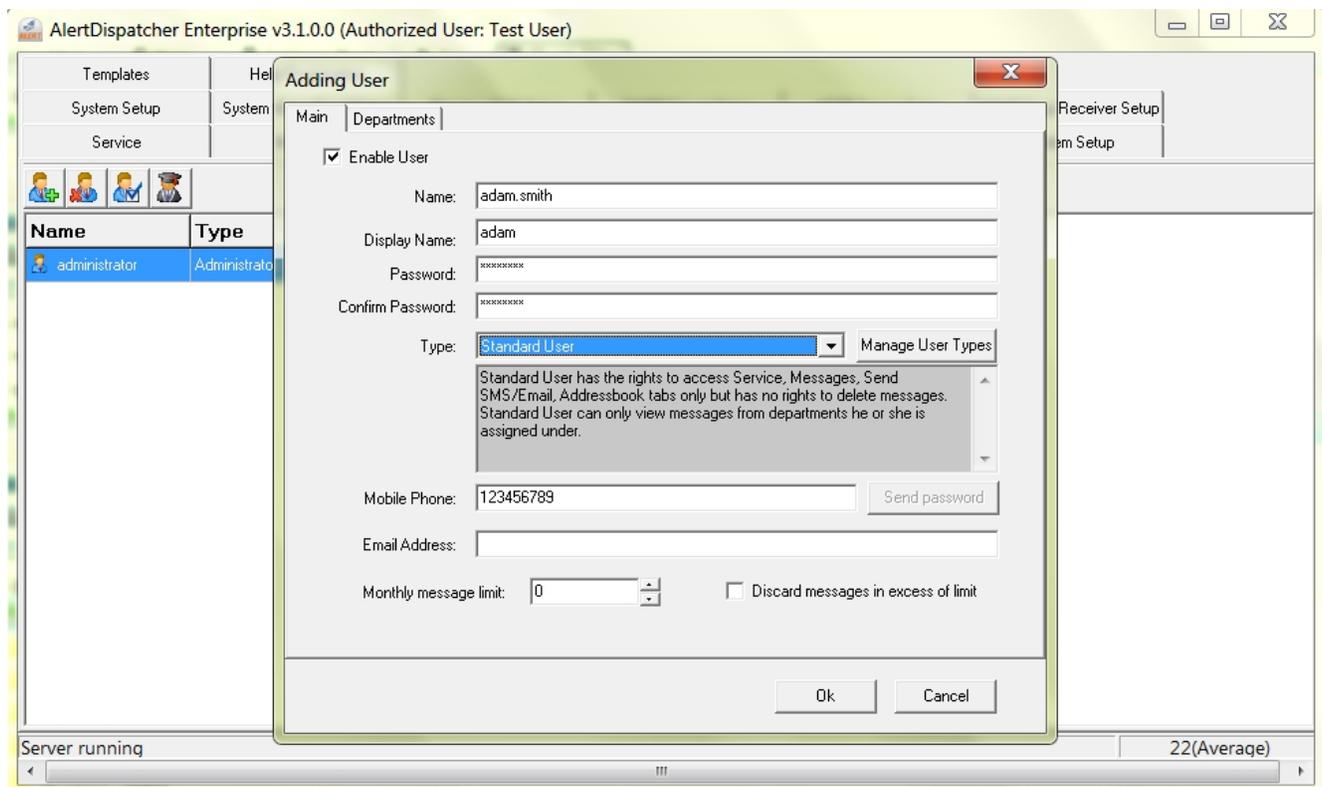
### a). Create user

If you are using the Corporate license (or higher licenses), you can install AlertDispatcher Client on workstations and configure the client to connect to AlertDispatcher Server remotely.

You can create multiple login Users of different “User Types” (each user type has a different combination of access rights). Every login user is assigned to a user type and the user will in turn inherit all the rights configured for that user type. Login users are used for both AlertDispatcher Client and Web Portal login.

For your convenience, the following user types are created upon installation – Administrator, Basic User, Department Leader, Manager and Standard User.

In the example shown below, the newly created user “adam.smith” is assigned the user type “Standard User”. Standard User has the rights to access Service, Messages, Send SMS/Email, Addressbook tabs only but has no rights to delete messages. Standard User can only view messages from departments he or she is assigned under.

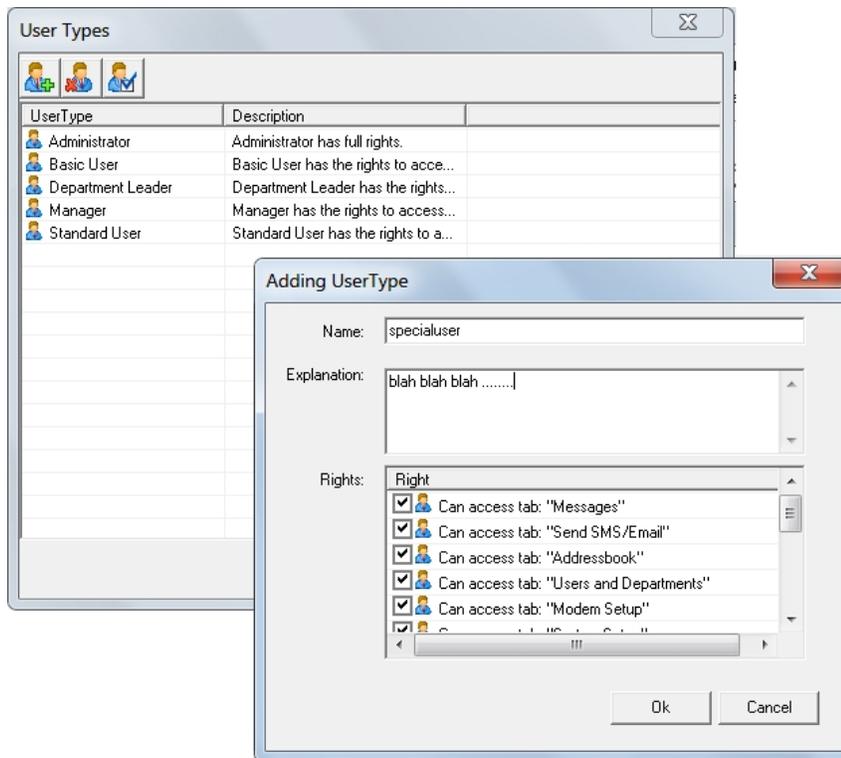


Users can also be individually assigned a monthly SMS send limit (0 for unlimited). A warning email will be sent to the user if the monthly limit has been exceeded (email template configurable under ‘Servers Setup -> SMTP Server Setup’ tab, ‘Email Notifications’ setup).

**Note:** The User “Administrator” is created automatically. The password is “administrator” (caps sensitive). You are advised to change this password as soon as possible.

## b). Create new user types

If you need a user type with a combination of access rights not found in any of the default user types, you can create your own user type.



## c). Create departments

To allow groups of users to work together distinctly from the rest of the organization, you can create new "Departments" (Users are assigned to the "main" department by when they are created and cannot be removed from "main" department).

You can create new departments and assign users to the newly created departments. Once the users are in different newly created departments, you can restrict a user to view/delete only messages generated by fellow members of the department. Users with the right to access messages from different departments can choose to filter messages displayed in the Messages display grid by department.

Addressbook Recipients/Groups and Message Templates are also restricted to users from a specific department ("main" department by default). If you create a new department, e.g. 'IT', and assign recipients/groups or a message template to this new department, users assigned to only 'main' department will not be able to send to these recipients and groups or access this message template.

**Tip:** If you want a recipient or group or message template to be accessible by all users, simply restrict the recipient/group or template to 'main' department. As all users are assigned to the default 'main' department, so recipients/groups and message templates assigned to 'main' are accessible by all users.

**New Department**

Main | Users

Enable Department

Name: Accounting

Email Report Recipients:

Sms Report Recipients:

Escalation rule if received SMS is not READ (for Sound Buzzer Alert Action)

If the received SMS is not READ within 0 minutes forward SMS to Phone/Email address(s):

Ok Cancel

d). Connecting client to remote server.

The ability to create multiple users is especially useful if you are using the Corporate (of higher) license which supports multiple remote clients. You may connect to a remote server using by editing 'Remote Server Host' as shown below.

AlertDispatcher v5.0.0.0.4531 (Evaluation - Trial Days Left:58)

Templates | Service Monitoring | Help/Registration | Servers Setup (SMTP/HTTP/SNMP) | Receive SMS Setup

Modem Setup | Instant Messaging (IM) Setup | System Setup | Addressbook | Users and Departments

Service | Messages | Send SMS/Email

Server Status:  Start  Stop  Restart  Emergency Pause

Server running

Modem Signal Strength for COM Port: COM3

22

Open Log Folder | Log lines to display: 100

User: Administrator Password: \*\*\*\*\*  Save password Remote Server Host: 192.168.0.6 [Master] Port: 5556 Save/Connect

2015.03.24 03:08:09:366 [!] Modem connected to port COM3 recovered  
 2015.03.24 03:08:09:334 Modem connected to COM3 recovered  
 2015.03.24 03:00:27:006 Failover Client Connected to 192.168.0.10:5556  
 2015.03.24 03:00:26:037 [!] Unknown recipient(s) or group(s): "sysalerts" when parsing: "sysalerts"  
 2015.03.24 02:37:43:022 AlertDispatcher Service Started with all modems offline!  
 2015.03.24 02:37:43:022 [!!!] No working modem found. Refer to Modem Setup for error message. Open log - file:\Log\  
 2015.03.24 02:37:43:022 [!] Modem connected to port COM3 cannot send SMS  
 2015.03.24 02:37:09:897 Engine initialized. [Build:4531]  
 2015.03.24 02:37:09:897 Upgrade Success!  
 2015.03.24 02:37:09:881 HardwareID:148F41AC-3214  
 2015.03.24 02:37:09:881 AlertDispatcher v5.0.0.0.4531 (Evaluation - Trial Days Left:58)

Server running 22(Average)

## 5). Configure SMTP Server Setup

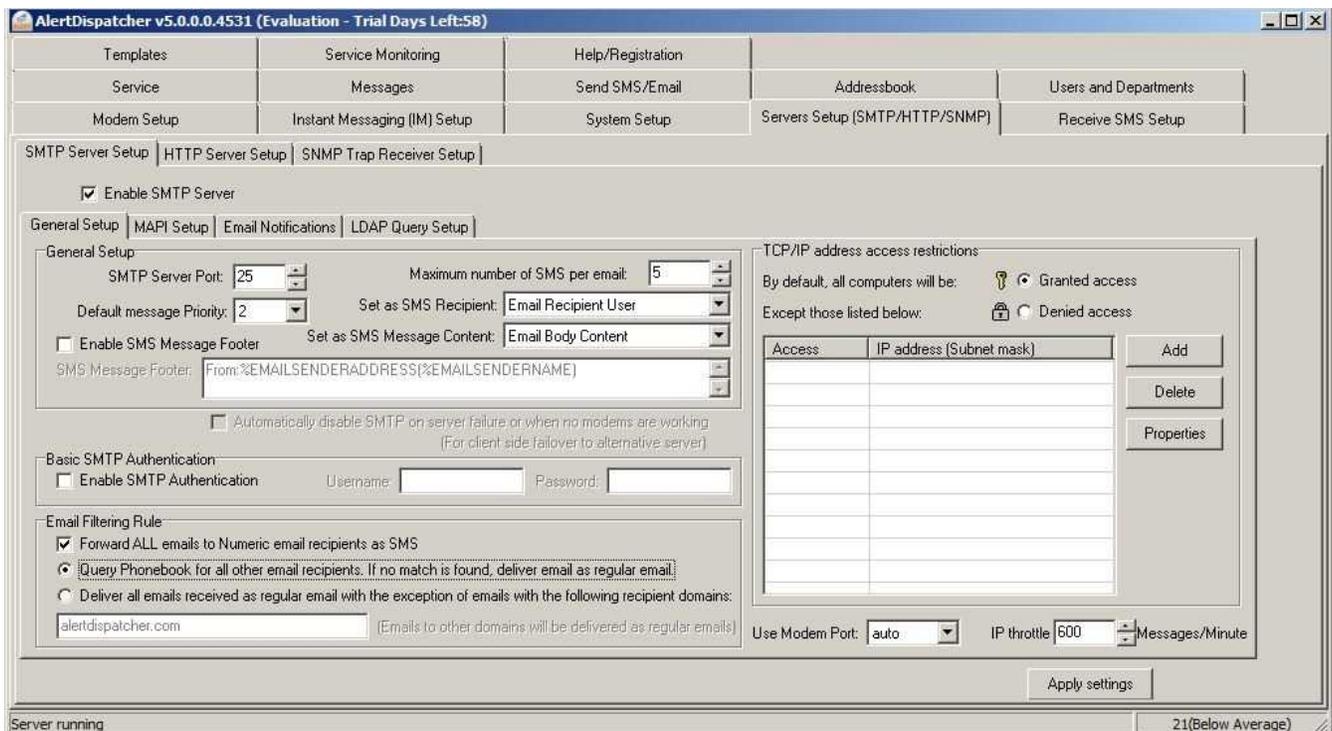
### a). SMTP Server Setup – General Setup

AlertDispatcher has a built-in SMTP Server that listens to port 25 (default). The built-in SMTP Server allows AlertDispatcher to be used as an Email-to-Alert (Email/SMS) gateway. You can configure MS Exchange or Lotus Notes to forward Emails to AlertDispatcher which will deliver them as SMS and/or Email using configurable rules.

**Note:** This setting is different from the 'SMTP Server' setting found under 'Systems Setup --> Alerts/Email Setup' tab – which allows AlertDispatcher to relay Email (as an Email client) to network based SMTP Servers.

The SMTP interface is required for some of the APIs such as the SQL Server stored procedure. As SMTP is a common protocol, the SMTP interface allows you to send Alerts from any programming language or software that can send out Email.

By default, AlertDispatcher will set the Email Body of Emails received by the SMTP Server as the Alert message. You can change this to Email Subject or to both Email Subject and Body. The recommendation is to use Subject if you do not need to type long messages.



By default, the Alert recipient will be taken from the recipient Email Address before the @ symbol. e.g. [+65912345678@clickndeploy.com](mailto:+65912345678@clickndeploy.com) or [groupname@clickndeploy.com](mailto:groupname@clickndeploy.com) (Note: groupname must be configured within the Addressbook). You may change to SMS recipient to take from Email Subject instead.

You may append a message footer to all Alerts sent out from the SMTP Server.

The "Automatically disable SMTP Server on server failure when no modems are working" setting is disabled by default and you should only enable it if you are using an SMTP Client with a failure over to alternate server

capability.

Using the *'Email Filtering Rule'*, you can selectively forward Emails to either SMS or relay as regular Email. If you check *'Forward ALL Emails to Numeric Email recipients as SMS'*, all Emails sent to recipient Email addresses in the following format: [+12345678@anydomain.com](mailto:+12345678@anydomain.com) or [12345678@anydomain.com](mailto:12345678@anydomain.com) will be forwarded as SMS.

You can toggle between *'Query Addressbook for all other Email recipients. If no match is found, deliver Email as regular Email.'* or *'Deliver all Emails received as regular Email with the exception of Emails with the following recipient domains:'*.

If set to *'Query Addressbook for all other Email recipients. If no match is found, deliver Email as regular Email.'*, AlertDispatcher will search the Addressbook for the group or recipient that exactly matches the username of the recipient Email address.

For example, if the recipient Email address is [john@mydomain.com](mailto:john@mydomain.com), and if the group or recipient 'john' exists in the Addressbook, that Email will be forwarded to the recipients defined in the Addressbook entry for 'john'. Otherwise, the Email will be relayed to [john@mydomain.com](mailto:john@mydomain.com) as a regular Email.

Conversely, if set to *'Deliver all Emails received as regular Email with the exception of Emails with the following recipient domains:'*, AlertDispatcher will only forward Emails with recipient Email address that matches a specified domain name(s). All other Emails destined for other domains will be sent as regular Email.

For example, if you indicate *'Alertdispatcher.com'* (default), only Emails with recipient Email address in the following format [+65912345678@Alertdispatcher.com](mailto:+65912345678@Alertdispatcher.com) will be converted into SMS. All other Emails will be delivered as regular Email\*. You can specify more than one domain name.

The Email filtering rule is a powerful feature enables 3<sup>rd</sup> party software to send both SMS and Email via a single SMTP Server.

The configuration *'TCP/IP Address access restrictions'* allows you to whitelist or blacklist specific computers or specific groups of computers by IP address. In the above example, all computers with the IP Address 192.\* are permitted to send Email to AlertDispatcher SMTP Server.

*'Use Modem Port'* feature allows you to specify which modem to use SMS messages relayed through the SMTP Server. The default setting is 'Auto'. This feature allows you to setup an active (primary) – passive (secondary) modem array in which the failover “passive” modem will be used only if the primary “active” modem fails.

*'IP Trottle'* controls the maximum number of emails per minute that the SMTP Server will process. Excess emails will be rejected.

**Note:**

- 1). You can send Alerts (both SMS and/or Email) to a group of people by configuring their Email and SMS contact in the Addressbook.
- 2). If Windows Firewall is enabled, you must open access to port 25 in order for SMTP Server interface to work. For details, please refer to the section *'Setup considerations for API / Email-to-Alert (Email2SMS) / HTTP-to-Alert / SNMP trap receiver interface'* on this guide.

*For advanced Users Only:*

You can also indicate the Priority (Parameter **P**) and Scheduled date time (Parameter **D**) to send the Alert by appending the following the parameters to the end of the Email message sent to AlertDispatcher (you may be required to append to Email Subject instead of Body, depending on your SMTP Server Setup). **P** and **D** are optional parameters.

`D==YYYY-MM-DD HH:MM:SS P==Priority`

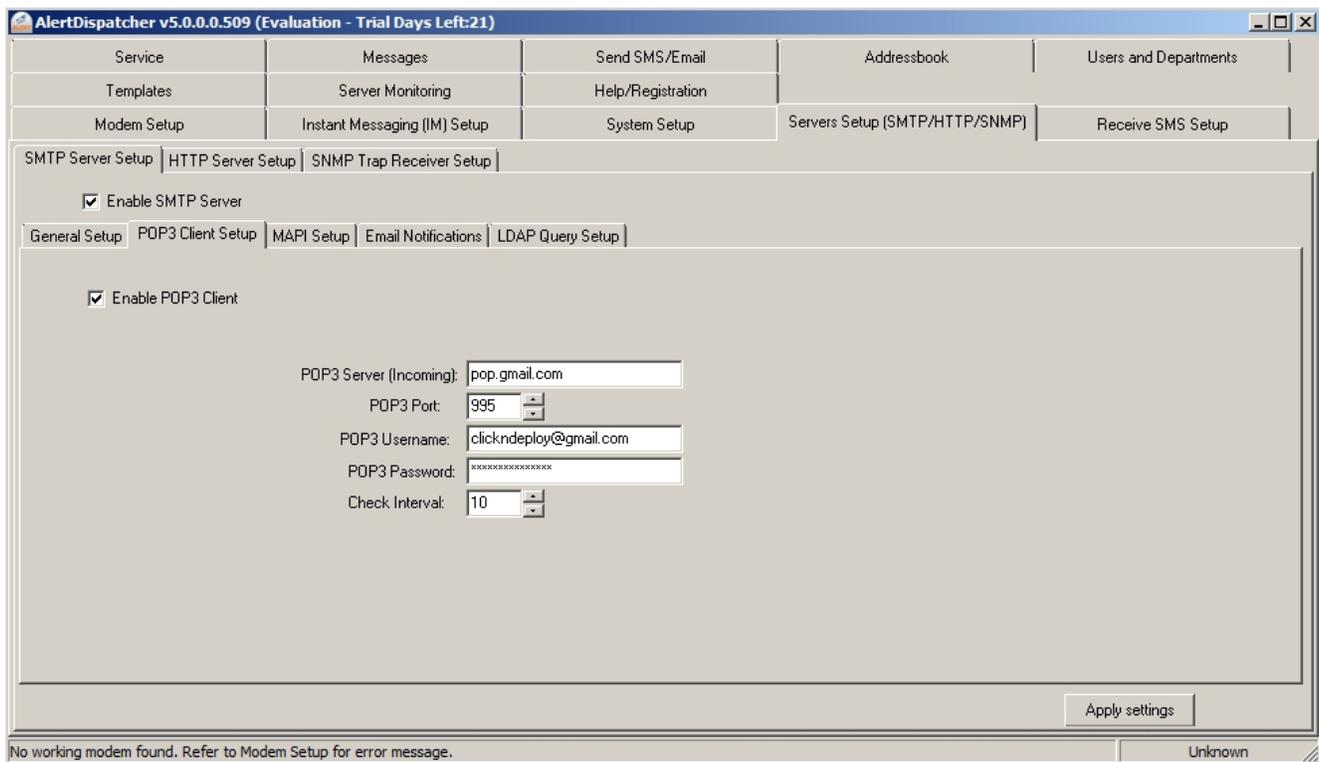
e.g. If you have defined the Alert message to be taken from the Email subject, you can indicate the Email subject as follows:

`Hi, how are you? D==2010-12-01 20:00:00 P==4`

## b). SMTP Server Setup – POP3 Client Setup

The POP3 Client allows you to query a mailbox using the POP3 (default port: 110). Emails retrieved from the mailbox will be converted into Alerts (Email/SMS) based on the same SMTP Server rules under General Setup. The POP3 Client functionality runs concurrently with the SMTP Server so you can use both at the same time.

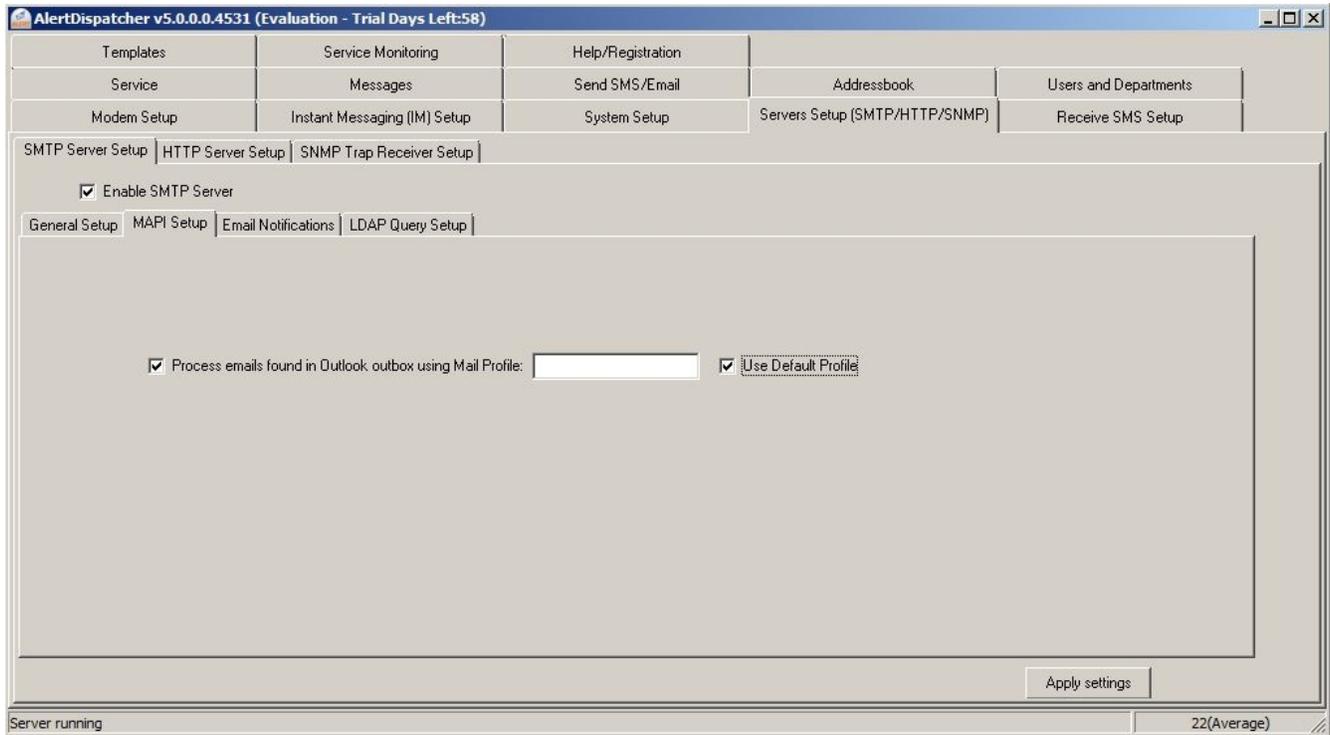
**Note:** To use it, you may need to reset the setting "Set as SMS Recipient" to "Email Subject".



## c). SMTP Server Setup - MAPI Setup

If your application uses Outlook to send messages (via **MAPI**), you may configure AlertDispatcher to process email found in Outlook outbox directly as shown in the screen below.

Using this method, you do not need to run Outlook all the time – however, you must still install and configure Outlook profile to point to AlertDispatcher Server. Processing emails directly is more stable because Outlook can hang if there are too many messages.

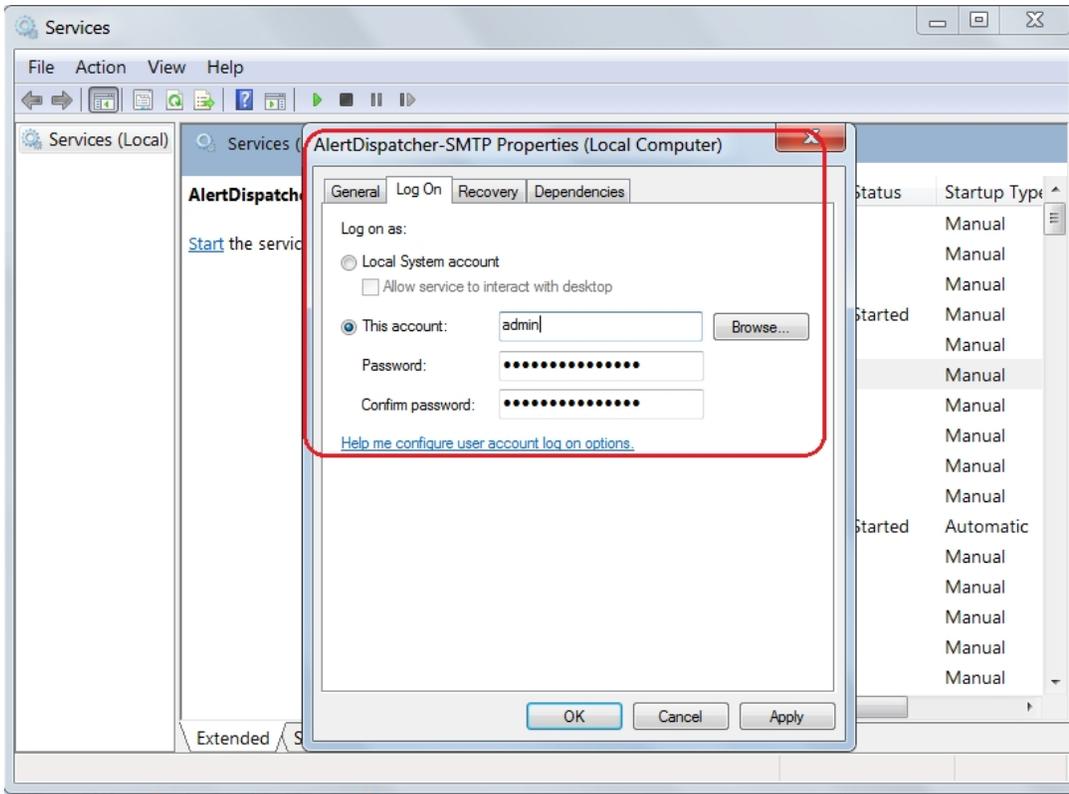


You must also logon “AlertDispatcher-SMTP” service as a local user (NOT domain user) with administrator rights. After that, restart AlertDispatcher-SMTP service.

After 2-3 minutes, refer to C:\Program Files (x86)\AlertDispatcher\Log \SMTPServer.log. If the following error appears, you need to verify that the username you used has administrator rights and you are using the default profile. If there is more than one profile, please enter the profile name which you have created.

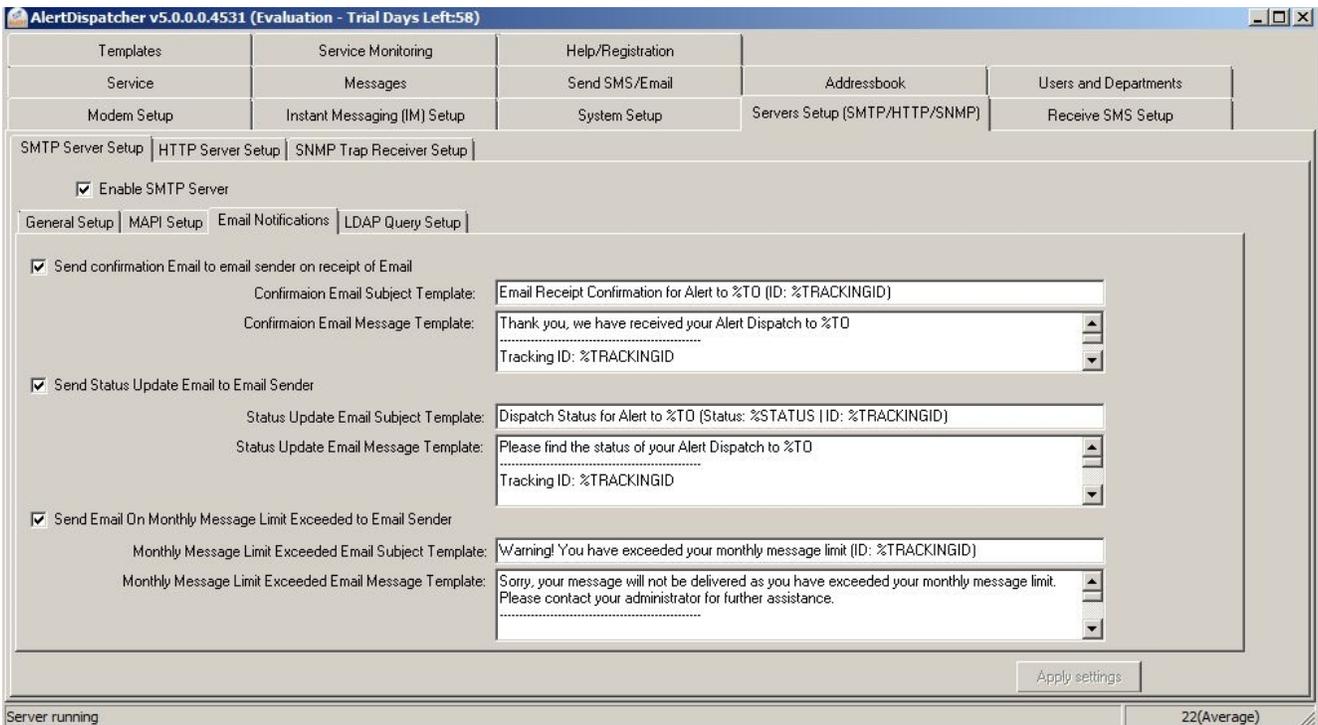
*2013.03.07 14:07:32:994 SmtP Server Socket opened on Port: 25*

*2013.03.07 14:09:14:653 Failed to connect to MAPI! Please configure Alertispatcher-SMTP to logon as the Windows logon user using Windows Services console. Error: Error (0x80040111) occurred when logging into the extended MAPI subsystem via the Profile: "".2013.03.07 14:09:14:731 <-- OK*



d). SMTP Server Setup – Email Notifications

You can also setup AlertDispatcher to send an auto response Email to the sender of the Email. This is useful if you are routing Emails via Exchange or Lotus to AlertDispatcher SMTP Server. The sender of the Email will be informed on the delivery status of the SMS by the auto response Email. The auto response Email template can be amended as shown above.



Please refer to the following section for more information: [Interface with AlertDispatcher using SMTP/HTTP/DOS](#)

Go to C:\Program Files\AlertDispatcher\APIs files to access the files for Command Line API and SQL Server stored procedure.

## e). SMTP Server Setup – LDAP Query Setup

The LDAP Query Setup allows you to limit the monthly usage of email users that are members of an LDAP directory (or Active Directory). You can set a default monthly usage limit and a different usage limit for up to 3 LDAP groups or Active Directory security group.

AlertDispatcher does this by creating a user for each new email user that sends over an email. You also can assign the department for each user by defining the LDAP attribute for department. This is useful where reporting is enabled and you want to be able to view usage by department if email reporting is enabled.

AlertDispatcher v5.0.0.0.4531 (Evaluation - Trial Days Left:58)

Service Messages Send SMS/Email Addressbook Users and Departments  
 Templates Service Monitoring Help/Registration  
 Modem Setup Instant Messaging (IM) Setup System Setup Servers Setup [SMTP/HTTP/SNMP] Receive SMS Setup

SMTP Server Setup HTTP Server Setup SNMP Trap Receiver Setup

Enable SMTP Server

General Setup MAPI Setup Email Notifications LDAP Query Setup

Enable LDAP Query

LDAP Host: 192.168.0.10 LDAP Login Name: admin\_user@your\_domain.com  
 LDAP Port: 389 LDAP Login Password:   
 LDAP Object Base: dc=your\_domain,dc=com Confirm LDAP Login Password:   
 Set Username to attribute: mail  
 Set Dept to attribute: department

Default Monthly Message Limit: 1000000

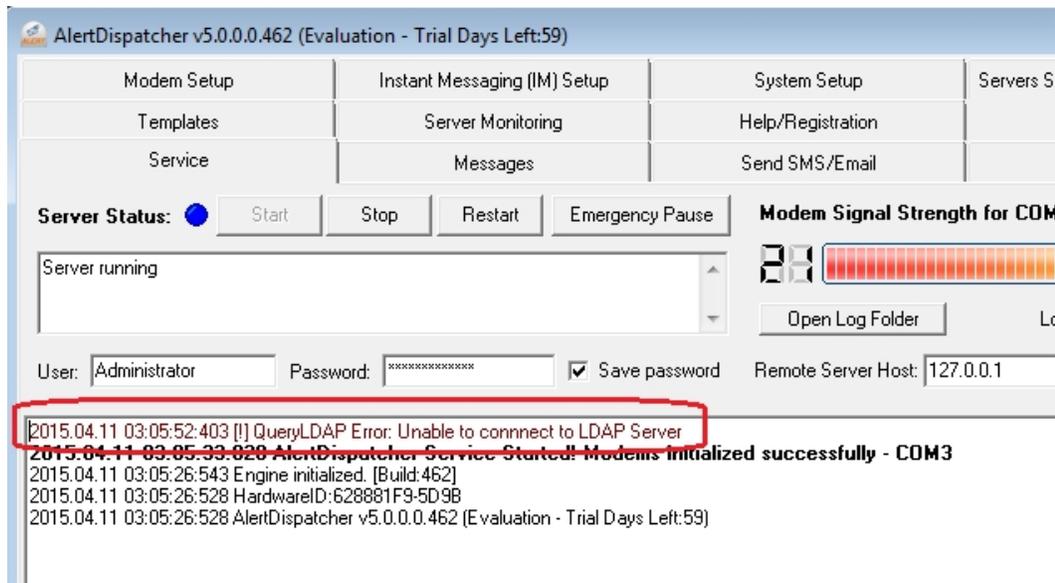
Tier 1: Monthly Message Limit of 1000000 for users belonging to LDAP group:   
 Tier 2: Monthly Message Limit of 1000000 for users belonging to LDAP group:   
 Tier 3: Monthly Message Limit of 1000000 for users belonging to LDAP group:

Apply settings

Server running 22(Average)

To debug your LDAP Query settings, please send an email and then refer to your AlertDispatcher event log for possible errors.

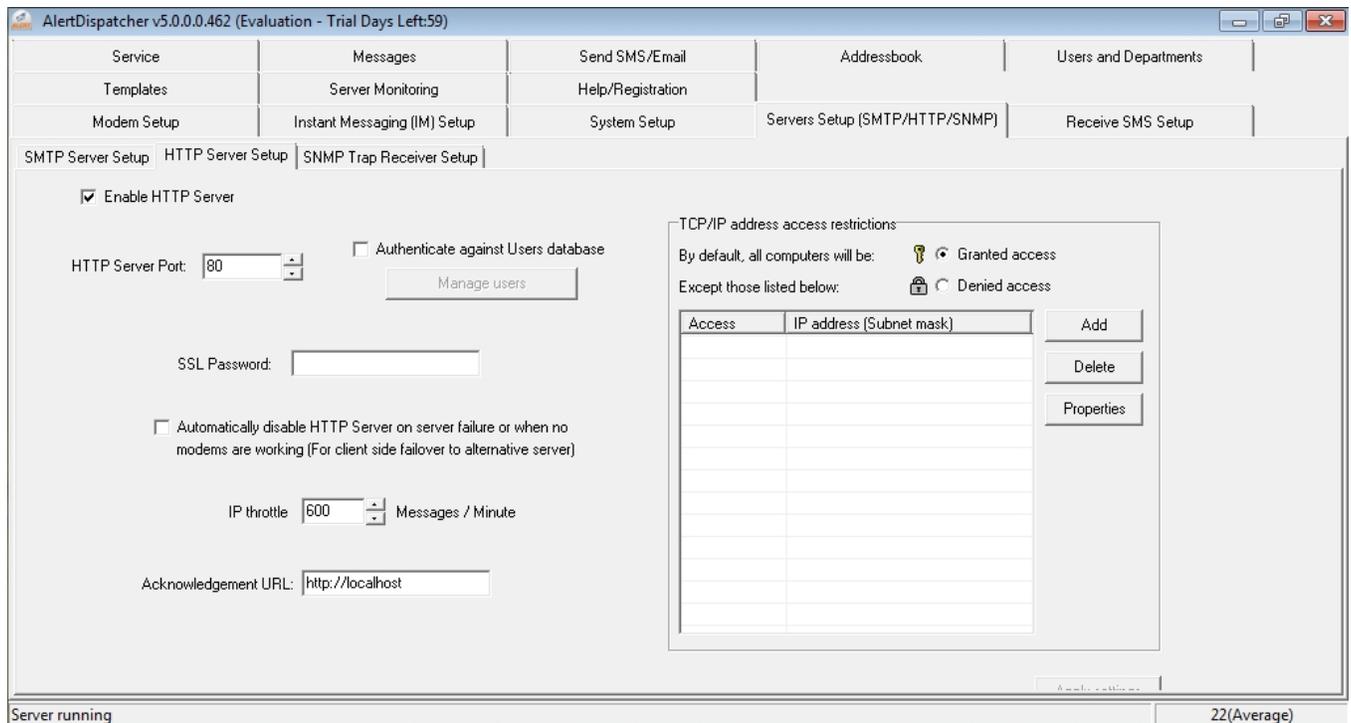
**Note:** The LDAP Query feature is only available for AlertDispatcher Corporate License (or higher).



## 6). Configure HTTP Server Setup

AlertDispatcher HTTP interface is enabled and listens to port 80 by default. This allows your server to be used as a HTTP-to-SMS gateway by calling the URL

<http://smsservername/sendsms?N=phonenumber&M=messagebody>. You can protect the URL by enabling the “Authenticate against the Users database” setting as shown below.



The "Automatically disable HTTP Server on server failure when no modems are working" setting is disabled by default and you should only enable it if you are using an HTTP Client with a failure over to alternate server capability.

**Note:** If Windows Firewall is enabled, you must open port 80 in order for HTTP interface to work. If Windows IIS World Wide Web service is running, you need to change HTTP interface port to a different one from what IIS is using. For details, please refer to the section '[Setup considerations for API/Mail-to-SMS interface](#)' on this guide.

And similarly to the SMTP interface, the configuration '*TCP/IP Address access restrictions*' allows you to whitelist or blacklist specific computers or specific groups of computers by IP address. In the above example, only computers with the IP address 192.168.0.6 and 192.168.0.100 are permitted to interface with AlertDispatcher via HTTP.

'*IP Trottle*' controls the maximum number of HTTP requests per minute that the HTTP Server will process. Excess requests will be rejected.

'Acknowledgement URL' refers to the URL used in Acknowledgement links sent in Basic Escalation and Emergency Mobilization messages.

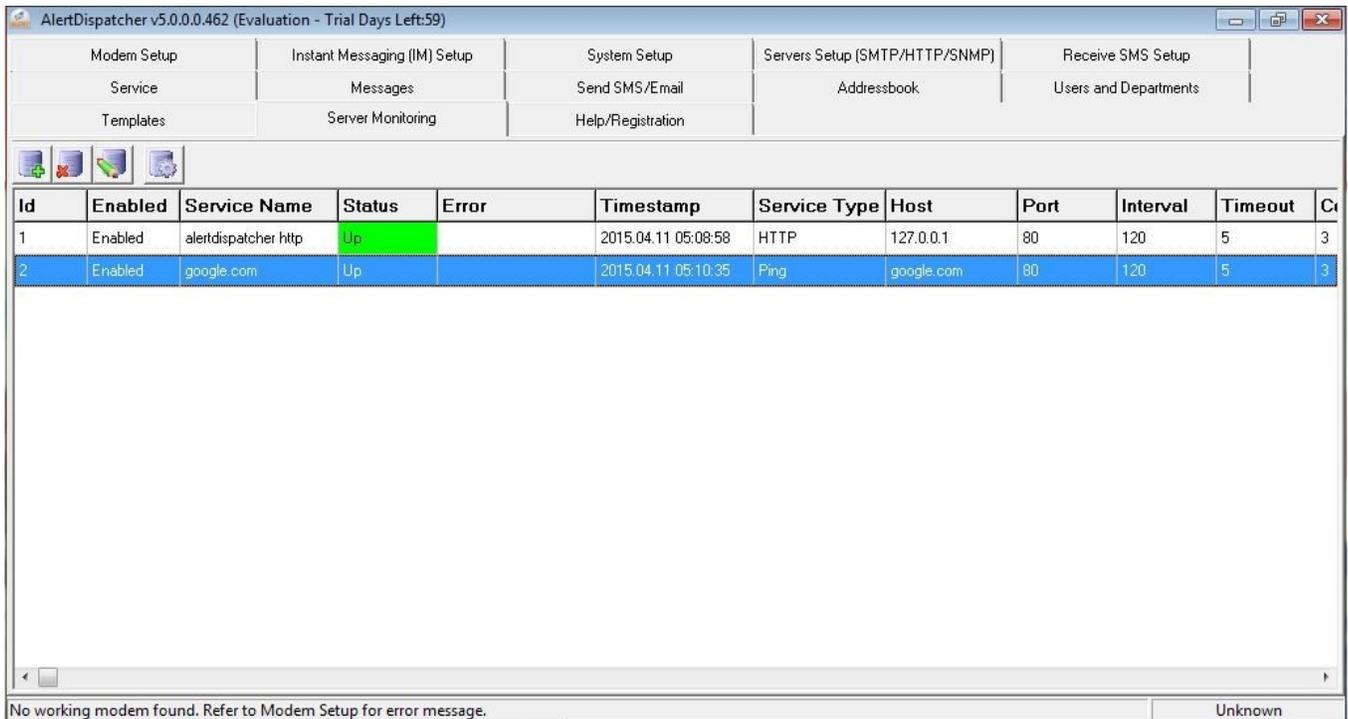
**Note:**

- 1). Internal addresses such as <http://192.168.0.111> or <http://localhost/> are not accessible from the Internet, i.e. you can't use them from smart phones.
- 2). Do not include the port number, e.g. <http://localhost:88>

Please refer to the following section for more information: [Interface with AlertDispatcher using SMTP/HTTP/DOS](#)

## 7). Configure Server Monitoring

AlertDispatcher v5 (or newer) comes with a built-in server monitoring feature that allows you to monitor applications and servers on the network ("services") and generate an alarm and alert when a service becomes unavailable for more than a defined period of time.



The screenshot shows the AlertDispatcher v5.0.0.0.462 (Evaluation - Trial Days Left:59) interface. The top navigation bar includes: Modem Setup, Instant Messaging (IM) Setup, System Setup, Servers Setup (SMTP/HTTP/SNMP), and Receive SMS Setup. Below this, there are sub-sections: Service, Messages, Send SMS/Email, Addressbook, and Users and Departments. A secondary row contains: Templates, Server Monitoring, and Help/Registration. The main area displays a table with the following data:

Id	Enabled	Service Name	Status	Error	Timestamp	Service Type	Host	Port	Interval	Timeout	Count
1	Enabled	alerdispatcher http	Up		2015.04.11 05:08:58	HTTP	127.0.0.1	80	120	5	3
2	Enabled	google.com	Up		2015.04.11 05:10:35	Ping	google.com	80	120	5	3

At the bottom of the window, there is a status bar with the text: "No working modem found. Refer to Modem Setup for error message." and "Unknown".

"Service Type" refers to the type of Service being monitored or the method of monitoring, e.g. Ping, HTTP.

You can configure check intervals, timeout, and count failures, which is the total number of consecutive failures before the DOWN alarm is raised. "OK response keyword" refers to the response that will indicate a successful check response. "BAD response keyword" refers to the response that will indicate a failed check response.

After the first alarm alert has been sent, you can optionally configure an escalation of the alarm alert to another recipient (or to the first recipient) if the service does not recover within a specified time period (minutes). The escalation alarm alert can act as a reminder message in case the recipient fails to take notice of the first alarm alert.

Note that this alarm escalation feature is different from the addressbook escalation setting which requires acknowledgement by the recipient to stop further escalation.

**Editing Monitoring, Id: 1**

Enable Server Monitoring

Service Name:

Service Type:

Host:  Port:

Interval, sec:   Use default

Timeout, sec:   Use default

Count Failures:   Use default

Check HTTP response:

OK HTTP response keyword:   Use default

BAD HTTP response keyword:   Use default

Alert Recipients:   Use system alert recipient

Escalate alert to recipient   Use system alert recipient  
if service is still down after:  mins.

Escalate alert to recipient   Use system alert recipient  
if service is still down after another:  mins.

Id	Enable
1	Enabled
2	Enabled

Interval	Timeout	Count
120	5	3
120	5	3

## 8). Configure SNMP Trap Receiver Setup

AlertDispatcher will capture SNMP Traps (v1 and v2) sent to the built-in SNMP trap receiver (which listens at the default port 162) and then formulate the alert message using the alert message template and the information derived from the SNMP trap. The alert is then sent to the list of Email and SMS recipients defined in the setup (default is no recipients).

You can customize the template for the alert and configure AlertDispatcher to strip unnecessary text from the message before it is sent. You can also set AlertDispatcher to send a single “digest alert” for SNMP traps received within a short interval so as to reduce the number of alerts.

The screenshot displays the 'SNMP Trap Receiver Setup' window in AlertDispatcher v5.0.0.0.509. The window title bar indicates it is an evaluation version with 21 trial days left. The interface includes a navigation menu at the top with options like Service, Messages, Send SMS/Email, Addressbook, Users and Departments, Templates, Server Monitoring, Help/Registration, Modem Setup, Instant Messaging (IM) Setup, System Setup, Servers Setup (SMTP/HTTP/SNMP), and Receive SMS Setup. The 'SNMP Trap Receiver Setup' tab is active, showing sub-tabs for 'General Setup' and 'Script'. Under 'General Setup', the 'Enable Trap Receiver' checkbox is checked. The 'Trap Receiver Port' is set to 162, and the 'Recipients' field is empty with a red error message 'Please enter recipients'. There are two sections for alert message templates: 'Alert Message template (First Half)' for SNMP v1 and v2, each with a 'Set to default' button and a list of variables (Timestamp, Source, Generic, Specific, Enterprise, EnterpriseDescr, Community). To the right, there is a 'Strip the following keywords from the message' section with a text area for keywords. Below this, there is an unchecked checkbox for 'Enable alert digests for traps received.', a field for 'Send an alert digest for SNMP traps received within the following interval, secs' set to 5, a field for 'Max number of SNMP traps per alert digest' set to 3, and an 'IP throttle' field set to 600 Messages / Minute. An 'Apply settings' button is at the bottom right. A status bar at the bottom left shows 'No working modem found. Refer to Modem Setup for error message.' and the bottom right shows 'Unknown'.

**Note:** The SNMP Trap Receiver feature is only available for AlertDispatcher Corporate License (or higher).

**Note:** If Windows Firewall is enabled, you must open port 162 in order for SNMP Trap interface to work. If Windows SNMP Trap service is installed and running, you need to either stop the service or change to another port. For details, please refer to the section ‘[Setup considerations for API / Mail-to-SMS / SNMP trap receiver interface](#)’ on this guide.

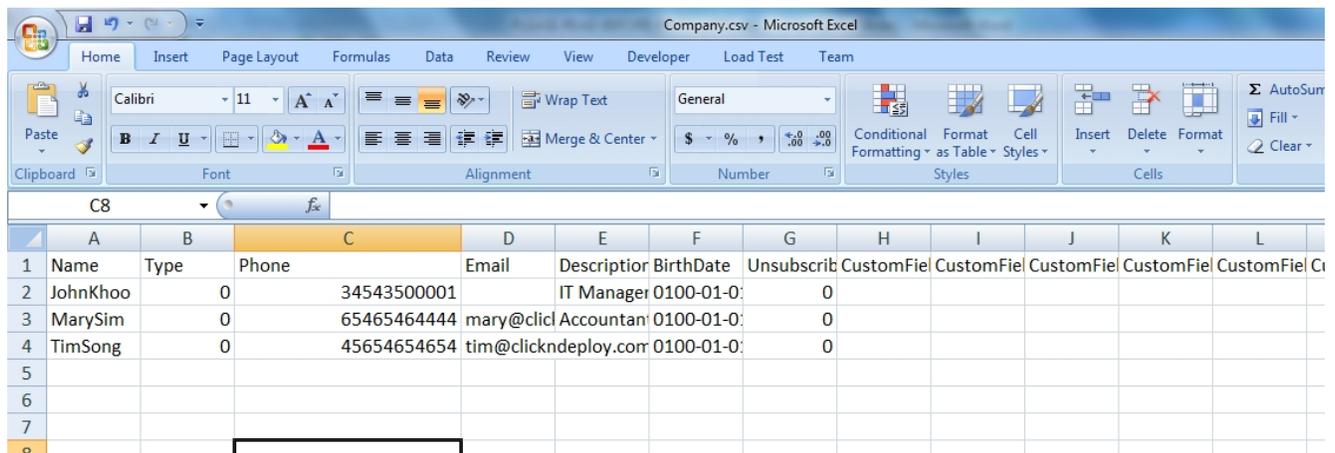
## 9). Loading your Contact List into Addressbook Groups, setup Duty Schedule, Basic Escalation and Emergency Recall Notification

### a). Addressbook Setup

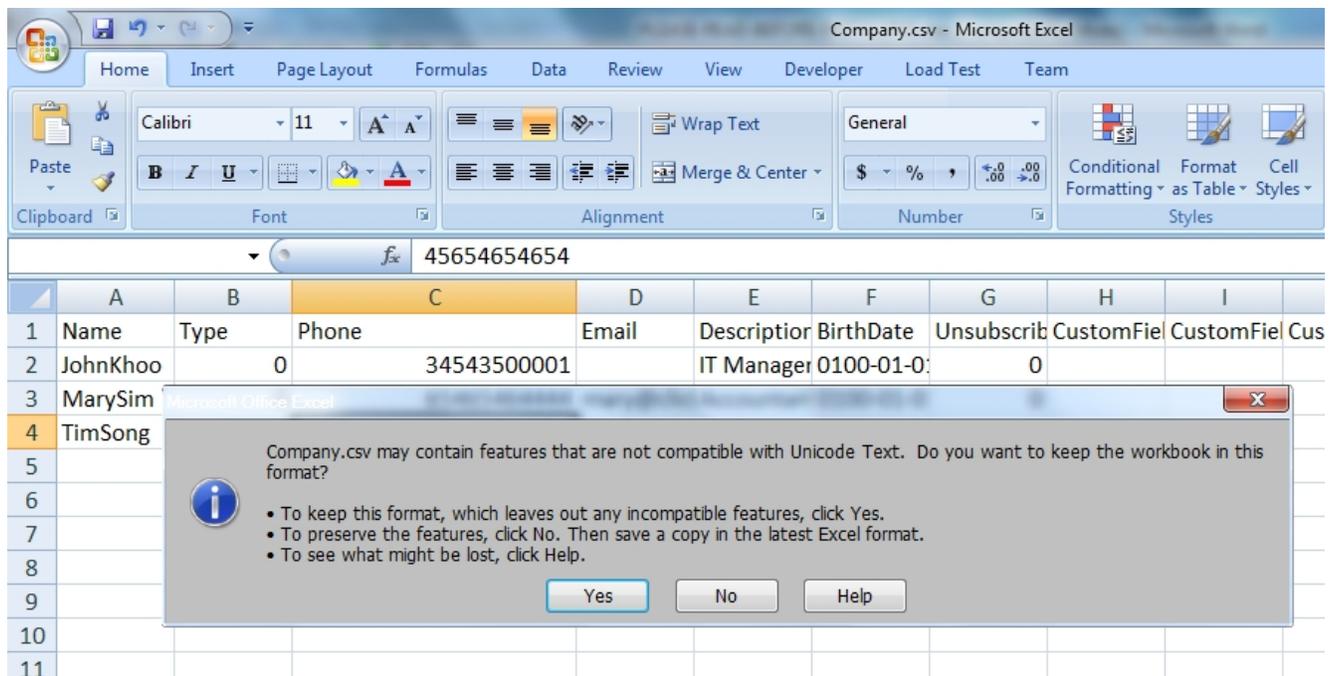
AlertDispatcher allows you to create multiple groups of recipients which you can import from CSV (if you are using Excel, you can save to CSV format). You can broadcast Alerts (SMS/Email) to groups with as many as 5000 recipients at a time.

You can find a sample group at C:\Program Files\AlertDispatcher\SampleGroup.csv. Modify to your own values using spreadsheet software such as MS Excel. Click on the Save icon. Click 'Yes' on the next prompt to ensure the file is saved in CSV format. Please do not attempt to use "Save As".

**Note:** Import/Export from CSV only works after registration (please refer to '[License Key Registration](#)'). Each group can only have up to 10,000 recipients. If you have more than 10,000 records, please split into multiple CSV files. The Addressbook can store up to 200 groups and 50,000 recipients (across all groups).



	A	B	C	D	E	F	G	H	I	J	K	L
1	Name	Type	Phone	Email	Descriptor	BirthDate	Unsubscribe	CustomField1	CustomField2	CustomField3	CustomField4	CustomField5
2	JohnKhoo	0	34543500001		IT Manager	0100-01-01	0					
3	MarySim	0	65465464444	mary@clcd	Accountant	0100-01-01	0					
4	TimSong	0	45654654654	tim@clickndeploy.com		0100-01-01	0					
5												
6												
7												
8												



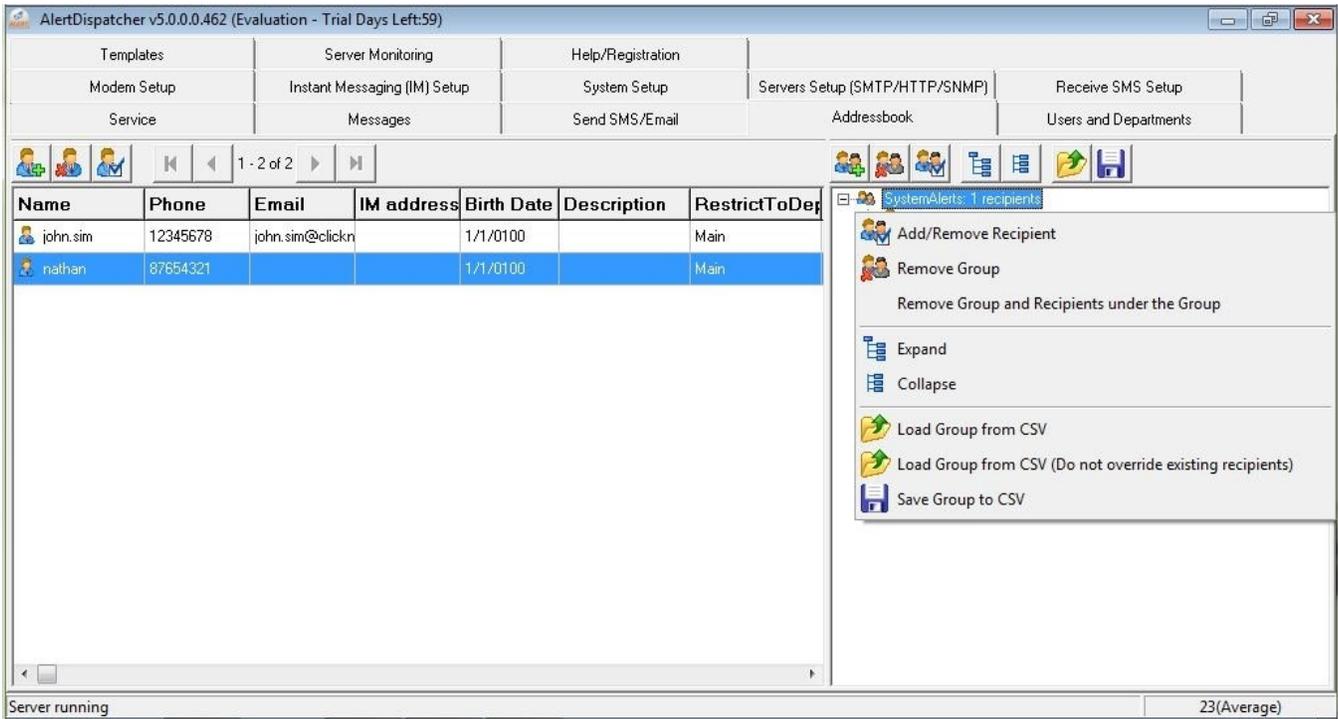
	A	B	C	D	E	F	G	H	I
1	Name	Type	Phone	Email	Descriptor	BirthDate	Unsubscribe	CustomField1	CustomField2
2	JohnKhoo	0	34543500001		IT Manager	0100-01-01	0		
3	MarySim								
4	TimSong								
5									
6									
7									
8									
9									
10									
11									

Company.csv may contain features that are not compatible with Unicode Text. Do you want to keep the workbook in this format?

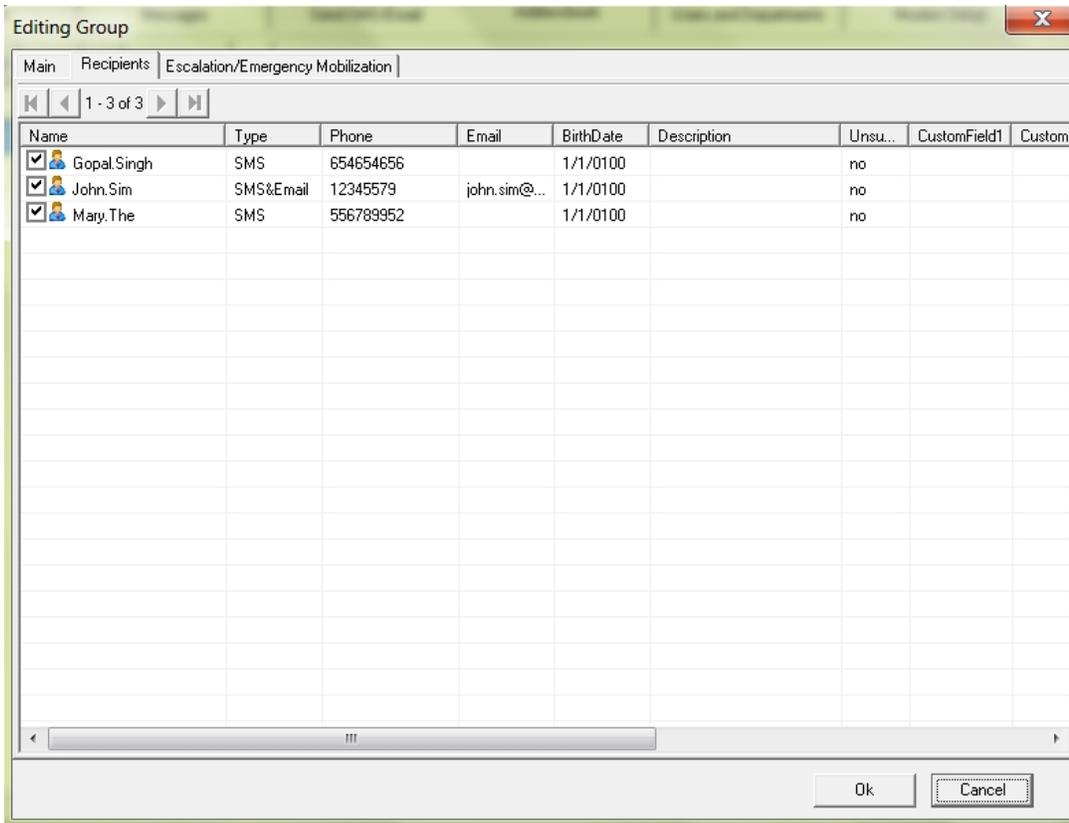
- To keep this format, which leaves out any incompatible features, click Yes.
- To preserve the features, click No. Then save a copy in the latest Excel format.
- To see what might be lost, click Help.

Yes No Help

Click on the 'Add Group' button  to create a new group, e.g. IT. Click right on the newly created group and select 'Load Group from CSV'.



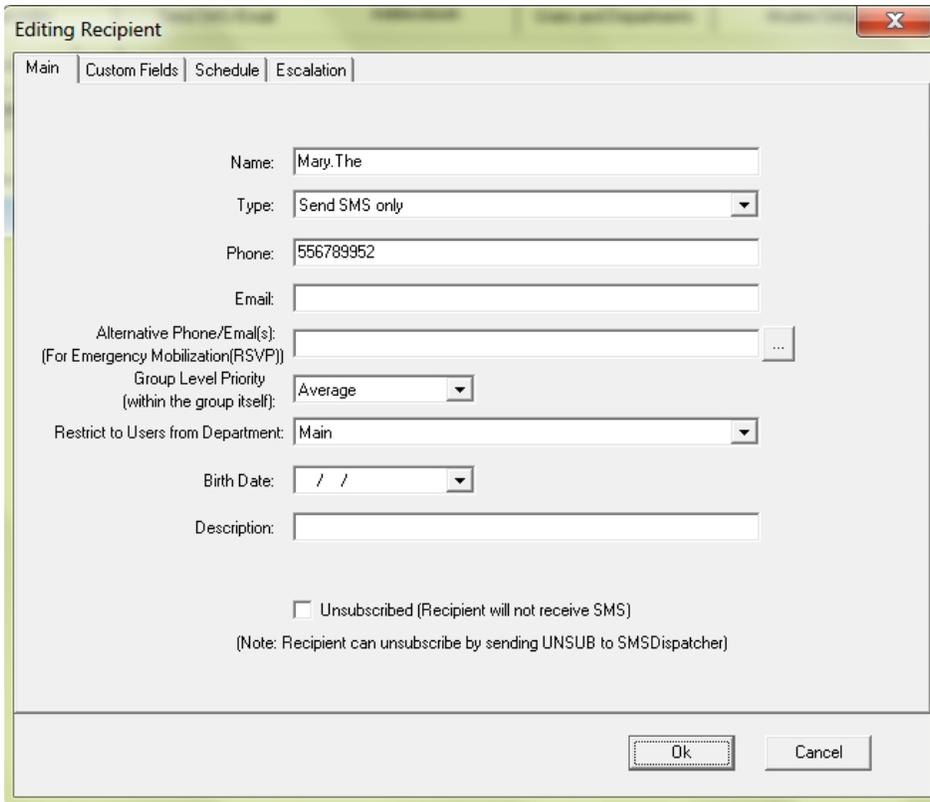
To test your newly created group, go to 'Send SMS/Email' Tab, click on  to open the Addressbook selection dialog. You may also add or remove recipients assigned to the group.



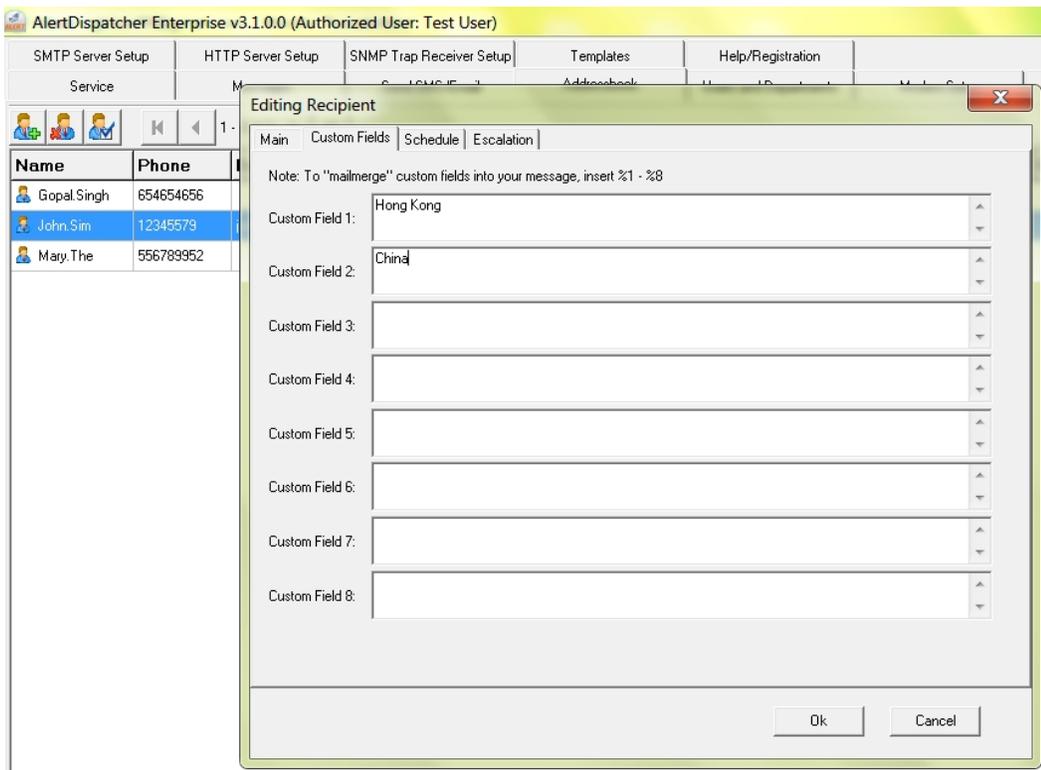
Alternative, you can also enter the recipients manually using , and then assign them to groups. You can define the 'Group Level Priority' for individual recipients. This setting takes effect when sending to a group of recipients with different priority. The recipient with higher Group Level Priority will receive the alerts first.

You can also restrict a recipient or group to users from a specific department. By default, only users under the default 'Main' department are allowed to send to a newly created recipient or group. Newly created users are assigned to the 'Main' department.

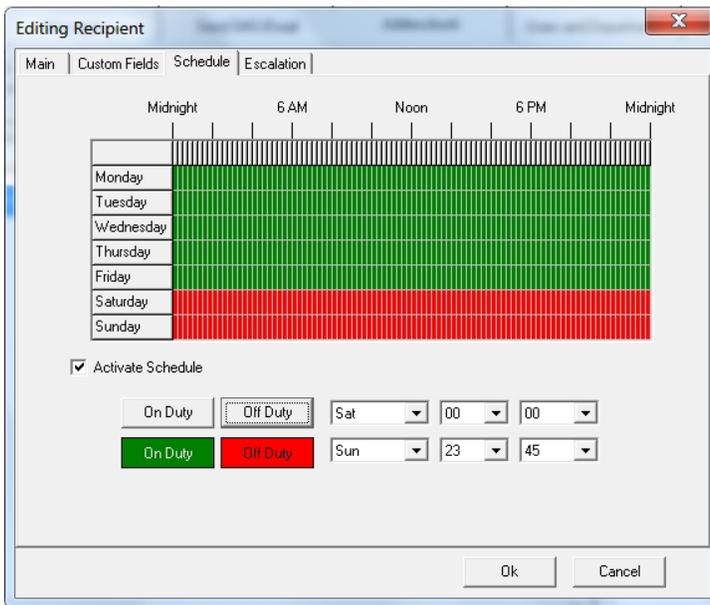
**Note:** A user can be assigned to multiple departments and thus will have the right to send to recipients and groups that are restricted to all departments which the user has been assigned with.



You can setup up to 8 Custom Merge Fields for every recipient. To merge the Custom Merge Field into your messages, simply type {CustomFieldNo.}, e.g. {CustomField5} for Custom Field 5.



You can define the duty schedule for the recipient on a weekly basis. Alerts will not be sent to recipients that are off duty.



## b). Basic Escalation Setup

### *i). Overview*

You can enable '*Basic Escalation*' for specific addressbook groups and also for individual recipients. If Basic escalation is enabled for a group, all messages sent to the group must be acknowledged. Any one of the recipients can acknowledge on behalf of the entire recipient group. This is done by sending an SMS or Email reply or by clicking on an acknowledgement link embedded in email.

If no one acknowledges, you can configure AlertDispatcher to escalate the message to another recipient, resend to the same recipient or call a recipient phone (cellular/fixed line). Up to 10 escalation levels can be configured.

Editing Group

Main Recipients Escalation/Emergency Recall Notification

Enable Escalation/Emergency Recall Notification

Basic Escalation: If none of the recipients have acknowledged within:

Emergency Recall Notification: If there is ANY recipient that has not acknowledged within:

Next	15	mins.	escalate to:	michael.smith
Next	15	mins.	escalate to:	
Next	15	mins.	ring phone (for 6 econds):	
Next	15	mins.	call phone till pickup:	
Next	15	mins.	escalate to:	
Next	15	mins.	escalate to:	
Next	15	mins.	escalate to:	
Next	15	mins.	escalate to:	
Next	15	mins.	escalate to:	
Next	15	mins.	escalate to:	
Next	15	mins.	escalate to:	

Append acknowledgement link to SMS sent to recipients

Append acknowledgement link to Email sent to recipients

Acknowledging any message will acknowledge all messages sent to recipient

Acknowledgement footnote: ACK: Reply {CODE} + msg

Do NOT escalate message if message contains ANY of the following keywords:

return to normal, back to normal, recovered, normal

Notify everyone that has been contacted whenever anyone makes an acknowledgement or makes a subsequent comment

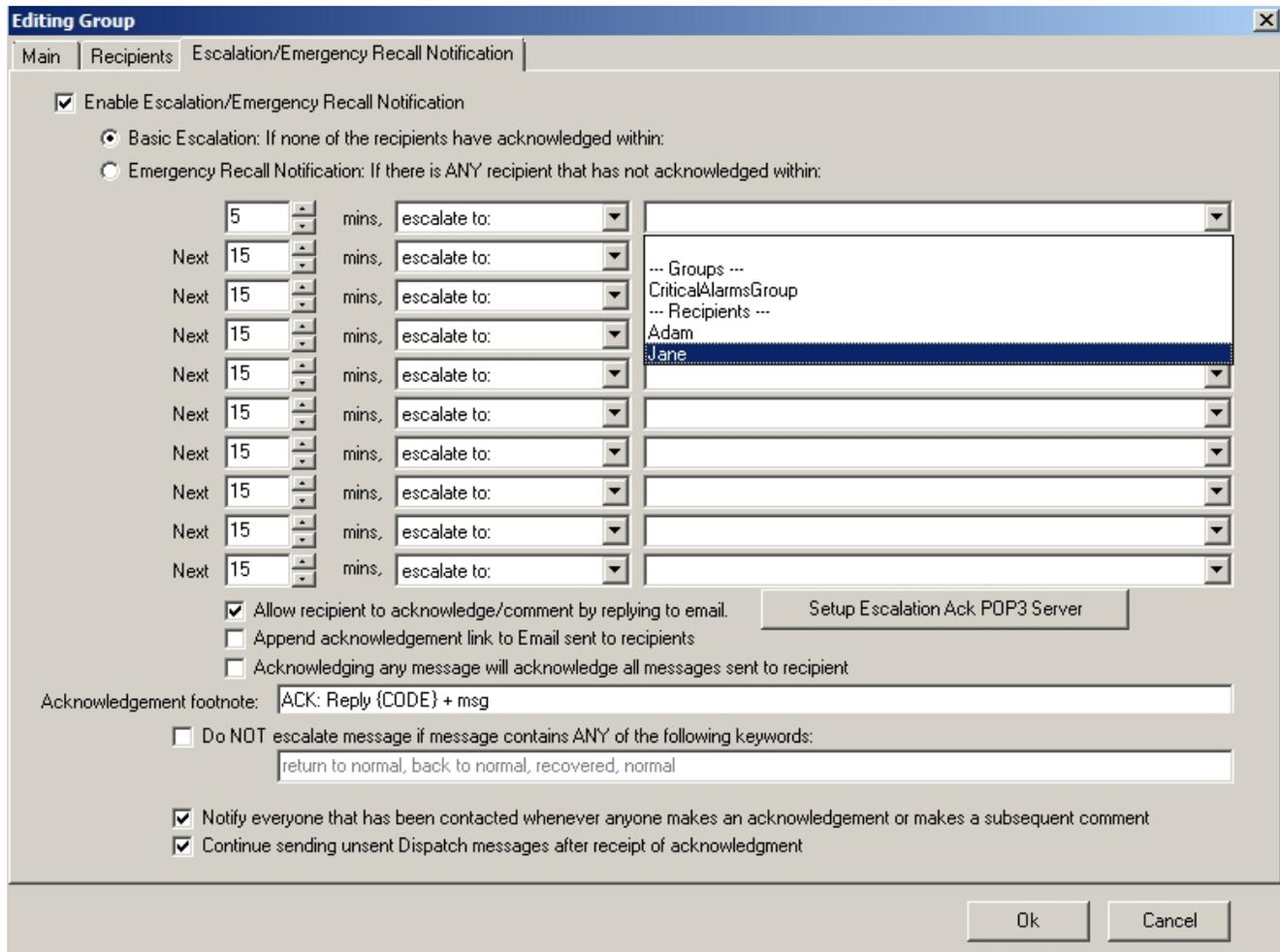
Continue sending unsent Dispatch messages after receipt of acknowledgment

Ok Cancel

Recipients can also add personal comments which would be forwarded by AlertDispatcher to other recipients. The acknowledgment footnote is configurable and can be disabled.

If "Acknowledging any message will acknowledge all messages sent to the recipient" setting is enable, a recipient can acknowledge all messages by acknowledging anyone of the escalation messages received. This makes it more convenient for the recipient but the downside is we can't ensure that the recipient has actually received or read all the messages.

You can exempt specific messages bearing certain keywords from the acknowledgement requirement by indicating them under the "Do NOT escalate messages if message contains ANY of the following keywords". This setting is useful for situations in which you do not want to escalate the message.



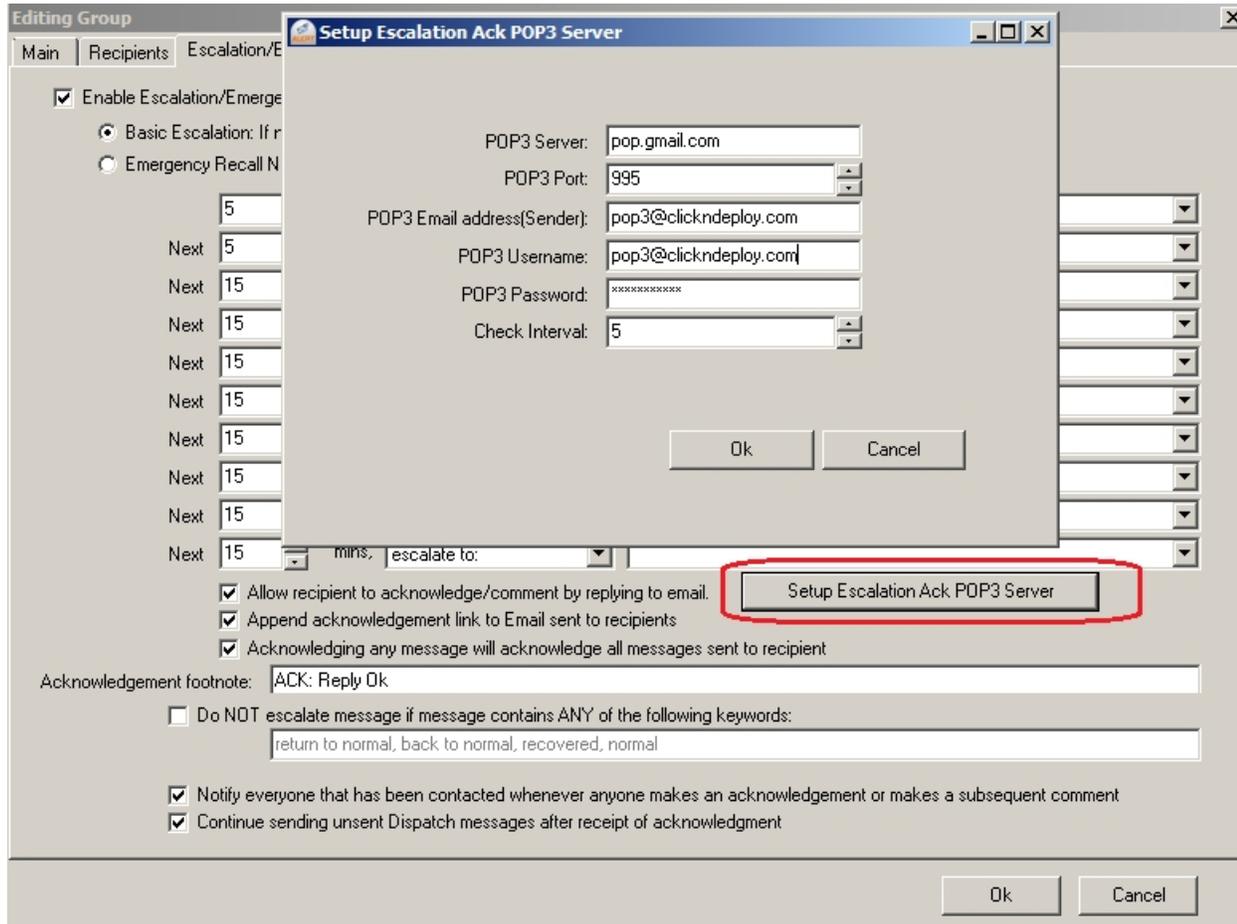
*ii). Acknowledging by SMS reply*

Recipients can acknowledge escalation messages sent via SMS by replying to the SMS. The recipient can acknowledge multiple messages (comma separated) in one SMS, e.g. A123, A456, A678.



*iii). Acknowledging by email reply*

Recipients can acknowledge escalation messages sent through email by replying to email if "Allow recipients to acknowledge/comment by replying to email" setting is enabled, and the POP3 Server credential is correctly configured using the "Setup Escalation Ack POP3 Server" button.



If the POP3 Server credential is incorrectly, the following error will be shown:

AlertDispatcher Enterprise v5.0.0.0.510 (Authorized User: Click And Deploy) MaxRecipients: 20

Modem Setup | Instant Messaging (IM) Setup | System Setup | Servers Setup (SMTP/HTTP/SNMP) | Receive SMS Setup

Templates | Server Monitoring | Automation Setup | Help/Registration

Service | Messages | Send SMS/Email | Addressbook | Users and Departments

Server Status:  Start  Stop  Restart  Emergency Pause

Modem Signal: COM22 Operator: Singtel (HSPA 3.5G)

Server running

User: administrator Password:  Save password  Open Log Folder

Remote Server Host: 127.0.0.1 Port: 5556 Save/Connect

```

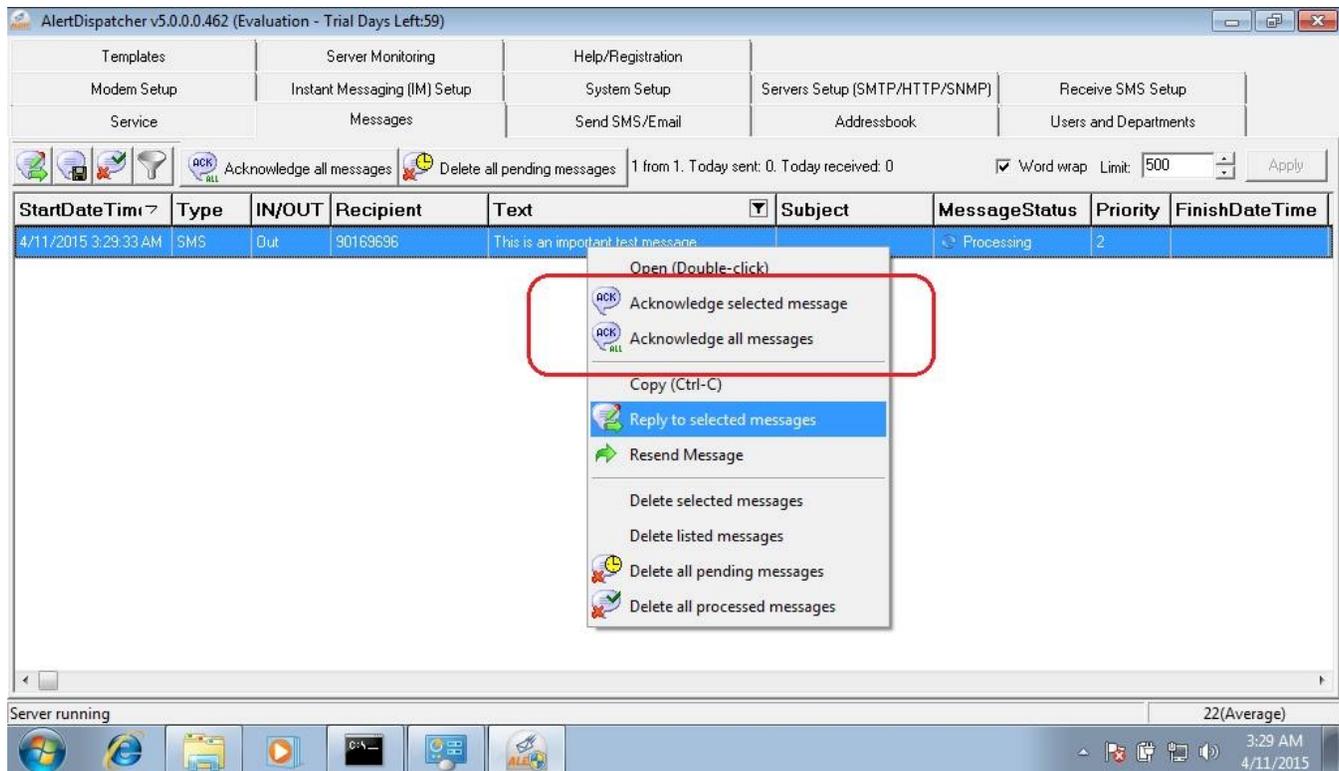
2015.08.27 10:21:25:656 AlertDispatcher Service Started! Modems initialized successfully - COM22
2015.08.27 10:21:35:468 [!] Escalation Ack POP3 server pop.gmail.com not available. Error:ERR [SYS/TEMP] Temporary system problem. Please try again later. so19mb426341017ec
2015.08.27 10:21:34:609 Engine initialized. [Build 510]
2015.08.27 10:21:24:531 Vendor:ClickNDeploy
2015.08.27 10:21:24:531 HardwareID:797A65CF-FD7C
2015.08.27 10:21:24:531 AlertDispatcher Enterprise v5.0.0.0.509 (Authorized User:Click And Deploy)
2015.08.27 10:21:24:531 ServerMonitoring: Disabled
2015.08.27 10:21:24:531 LicenseExpiry:0
2015.08.27 10:21:24:531 MaxEmergencyRecipients:20
2015.08.27 10:21:24:531 MaxModemNum:8
2015.08.27 10:21:24:531 sVendorEmail:
2015.08.27 10:21:24:531 sVendor:ClickNDeploy
2015.08.27 10:21:24:531 sRegisteredName:Click And Deploy
  
```

Server running 13(Poor)

#### *iv). Acknowledging via AlertDispatcher Client Console*

A PC operator can acknowledge any or all escalation messages on behalf of recipients on the AlertDispatcher client interface as shown in the next screen capture. This is useful if the recipient is in front of a PC.

Other than acknowledging through SMS, an operator can also acknowledge escalation messages using the AlertDispatcher GUI client as shown below. No acknowledgement confirmation will be sent to recipients when escalation messages are acknowledged via the AlertDispatcher GUI client.

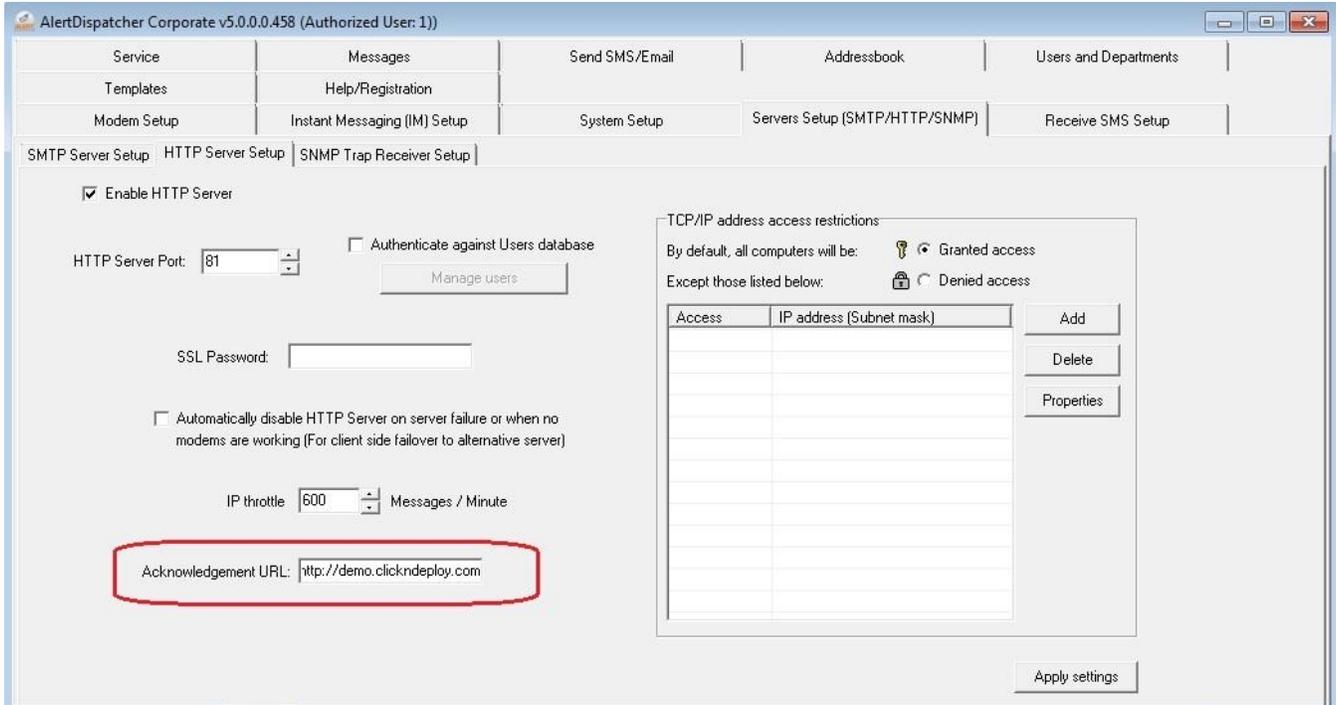


#### *iv). Acknowledging via link embedded in email*

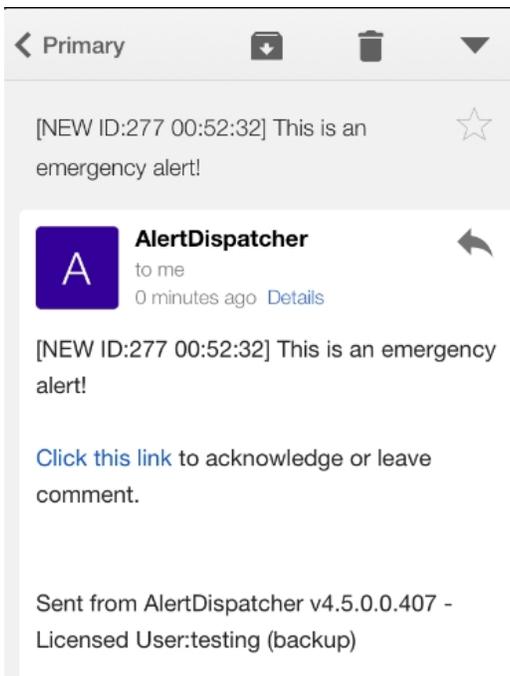
Recipients can acknowledge escalation messages by clicking on the acknowledgement link embedded in the email. Before the acknowledgement link can work, you will need to setup the acknowledgement link URL and ensure that the URL can resolve to AlertDispatcher HTTP Server (port 80 by default).

The default URL is "http://localhost" which is useful only for testing purpose as it will only work on the AlertDispatcher machine and won't work if you are connecting over the Internet, e.g. from your Smartphone. For actual usage, you will need to configure an Internet accessible URL, usually a domain or sub-domain or fixed IP address that resolves to your AlertDispatcher server.

If you're using a broadband router that has Dynamic DNS feature, you can use it to create a hostname for your URL and use port forwarding (or virtual server) feature to direct HTTP traffic to your AlertDispatcher machine.



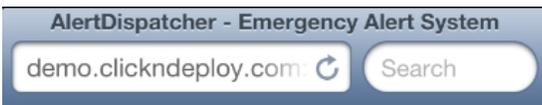
The URL "http://demo.clickndeploy.com" resolves to AlertDispatcher server as shown in the next 2 screen captures.





Note: If your AlertDispatcher is located on a LAN behind your Internet router, you will need to setup your Internet router to forward requests to port 80 (or whichever port you have configured) to your AlertDispatcher Server. If you don't have a static IP address, you will need to use a Dynamic IP address service. For more information on how to setup, please contact your company network administrator.

To know if you have configured your router correctly, you should be able to access the following page by accessing your Acknowledgement URL.



## b). Emergency Recall Notification Setup

Other than 'Basic Escalation', you can also enable 'Emergency Recall Notification' (only available for Enterprise License) for Groups. While any one of the recipients of a *Basic Escalation* can acknowledge to stop further escalation, Emergency Recall requires every recipient of the message to acknowledge. Recipients can acknowledge by sending an SMS or Email reply or by clicking on an acknowledgement link.

If any recipient does not acknowledge within the configured period of time, the message is escalated using several options which includes "resend to recipients that have yet to acknowledge", "call phone of recipients, that have yet to acknowledge, for 6 seconds", "resend to alternative contacts of recipients that have yet to acknowledge", etc.

The settings for Emergency Recall is similar to Basic Escalation.

**Editing Group** [X]

Main | Recipients | Escalation/Emergency Recall Notification

Enable Escalation/Emergency Recall Notification

Basic Escalation: If none of the recipients have acknowledged within:

Emergency Recall Notification: If there is ANY recipient that has not acknowledged within:

	5	mins, escalate to	resend to recipients that have yet to acknowledge
Next	5	mins, escalate to	ring phone of recipients, that have yet to acknowledge, for 6 seconds
Next	5	mins, escalate to	call phone of recipients that have yet to acknowledged
Next	5	mins, escalate to	resend to alternative contact of recipients that have yet to acknowledge
Next	5	mins, escalate to	send report to sender
Next	5	mins, escalate to	ring phone of alternative contact of recipients that have yet to acknowledge, for 6 seconds
Next	5	mins, escalate to	ring phone of recipients, that have yet to acknowledge, for 6 seconds
Next	5	mins, escalate to	
Next	5	mins, escalate to	
Next	5	mins, escalate to	

Allow recipient to acknowledge/comment by replying to email. Setup Escalation Ack POP3 Server

Append acknowledgement link to Email sent to recipients

Acknowledging any message will acknowledge all messages sent to recipient

Acknowledgement footnote:

Alternative contact header:

Require send confirmation for Emergency Recall Notification messages received from user via SMS or Email

Forward all comments made by recipients to the sender

Do not send message header, e.g. [NEW ID:276 21:22:24]

Ok Cancel

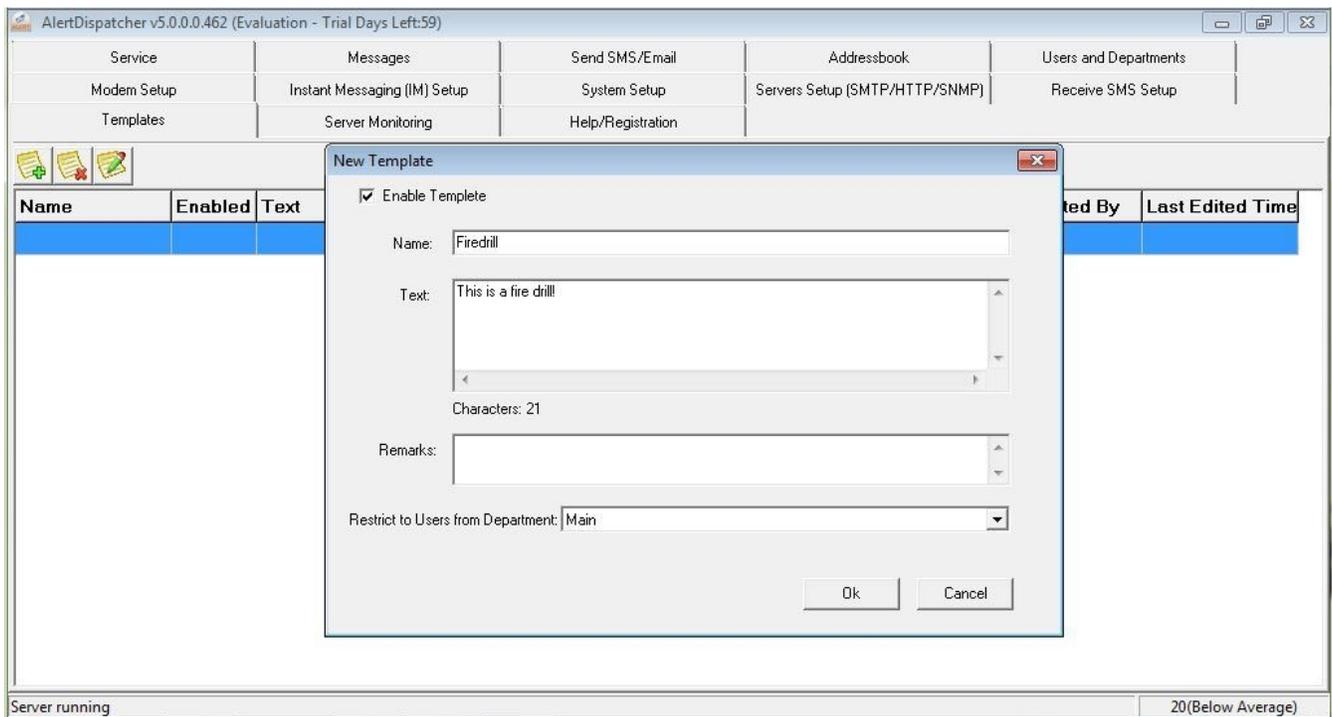
## 10). Configure Message Templates

You can create and configure message templates using the *'Templates'* tab on AlertDispatcher Client.

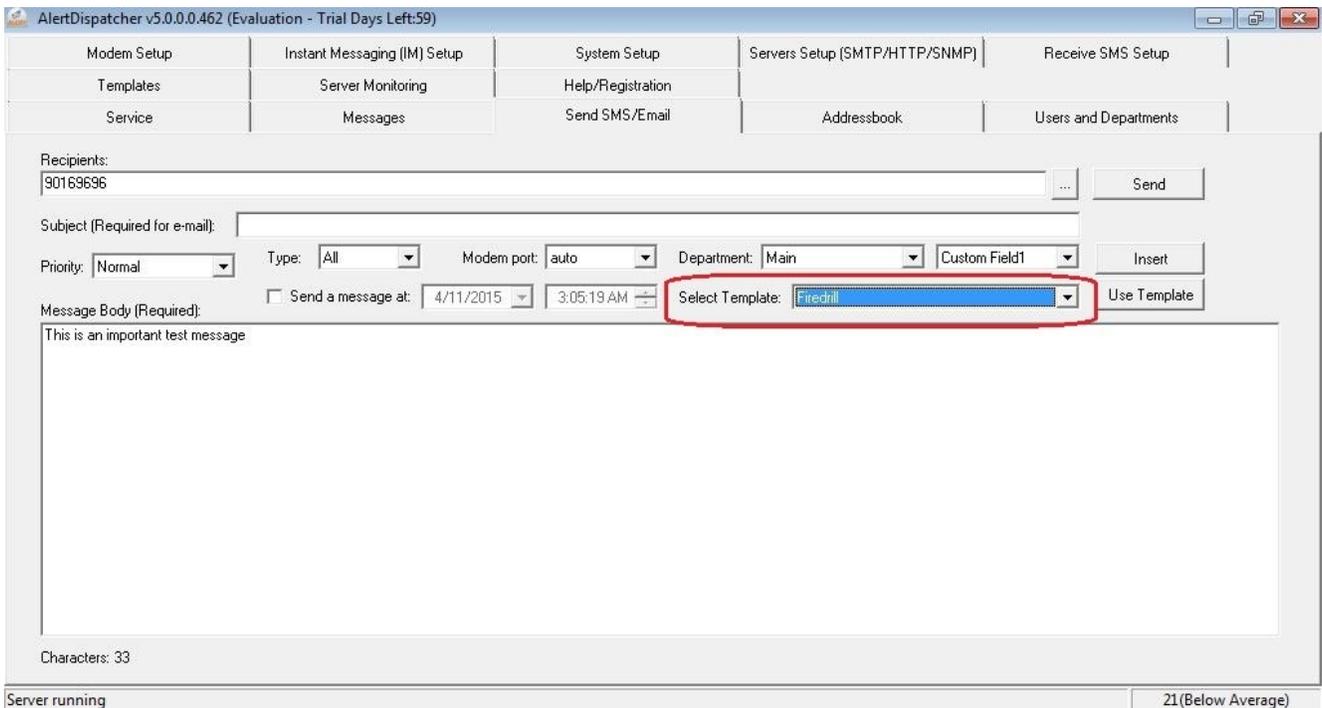
Message templates are restricted to Users from a specific department (*'main'* department by default).

If you create a new department, e.g. *'IT'*, and create a template that is restricted to this new department, users assigned to only *'main'* department will not be able to access this template.

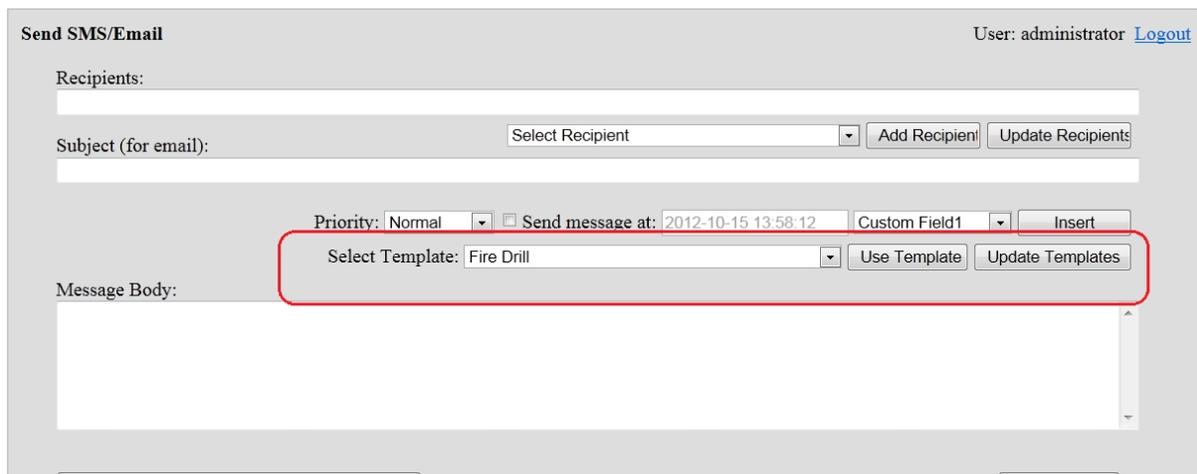
**Tip:** If you want a template to be accessible by all users, simply restrict the template to *'main'* department. As all users are assigned to the default *'main'* department, so Message templates assigned to *'main'* are accessible by all users.



Templates are accessible from both the *'Send SMS/Email'* tab and the web portal.



 **AlertDispatcher - Test User Alert System**

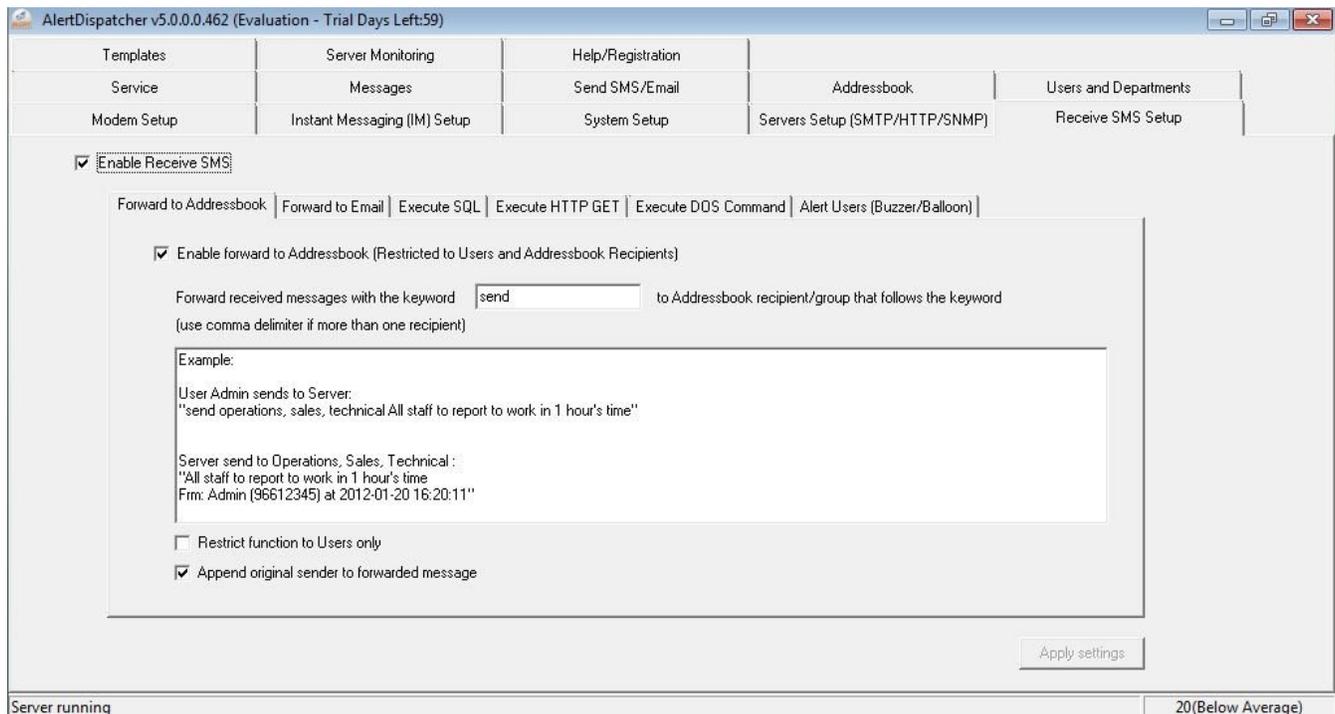


## 11). Configure Receive SMS Setup (Forward to Addressbook / Forward to Email / Execute SQL / Send HTTP GET request / Execute DOS Command)

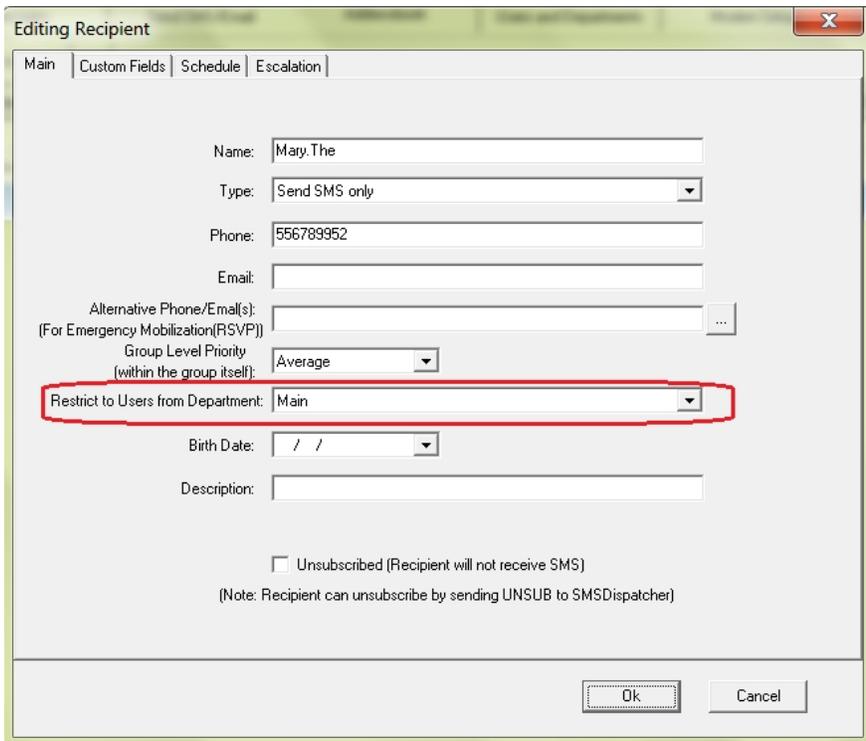
AlertDispatcher allows you to forward to addressbook, forward SMS received to Email, execute an SQL command, send an HTTP GET request and execute a DOS Command on receiving an SMS. You can enable/disable each feature individually.

### a). Forward to Addressbook

Enabling '*Forward to Addressbook*' feature allows users and addressbook recipients to forward/broadcast their SMS to addressbook recipients and groups. You have the option to restrict this feature to users only.

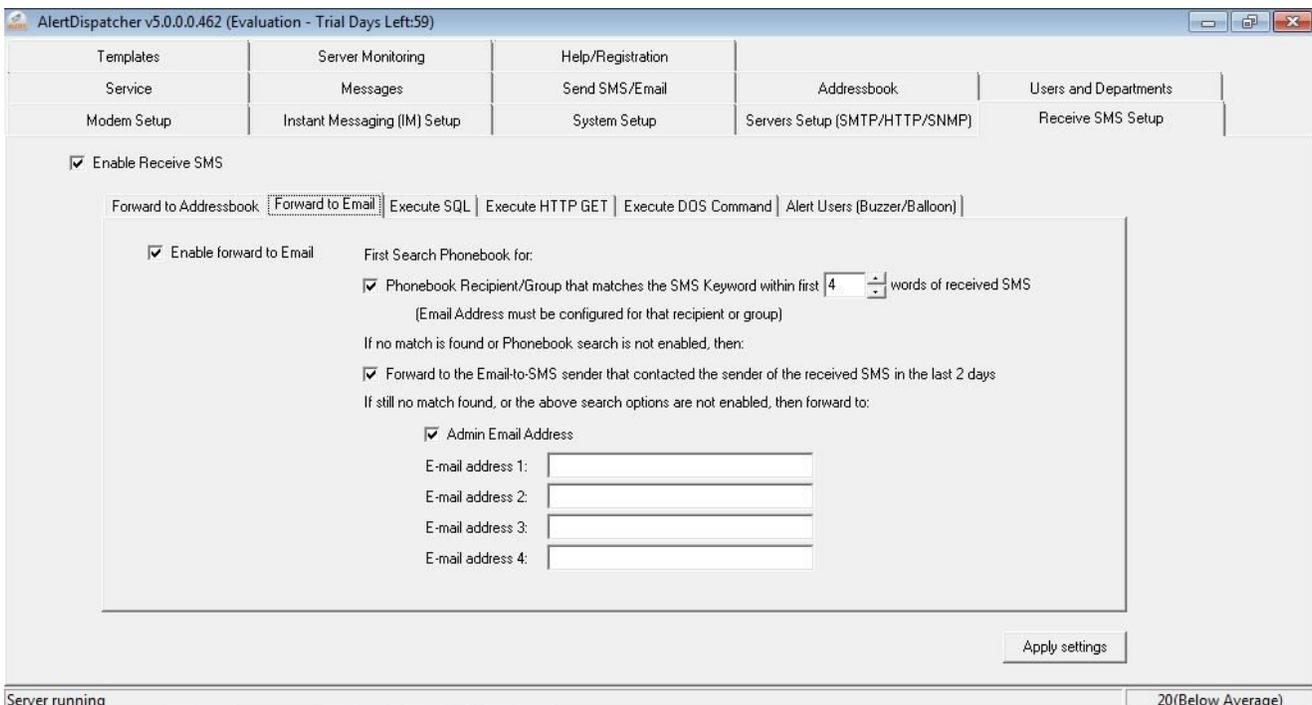


**Note:** Using the '*Restrict to Users from Department*' setting under Edit Recipient/Group, you can further restrict users from only a specific department to have the right to send to a particular group or recipient.



b). Forward to Email

You need to configure Alerts/Email Setup before you can enable *'Forward to Email'* feature (see the section *'Configure System and Alerts Setup'*). Ensure that the SMTP configuration you use is working using the Test Alert Email button; otherwise this feature will not work. The status of the test Alert Email will be displayed in the Messages tab.



AlertDispatcher will first search the Addressbook for names that match a keyword in the first X (default four) words of the received SMS.

For example, if the SMS message is *“Tom, please come here”*, a copy of the SMS will be forwarded to his Email address as defined in the Addressbook (see below screen capture). AlertDispatcher is intelligent enough to detect *‘tom’* within the first few words of the SMS.

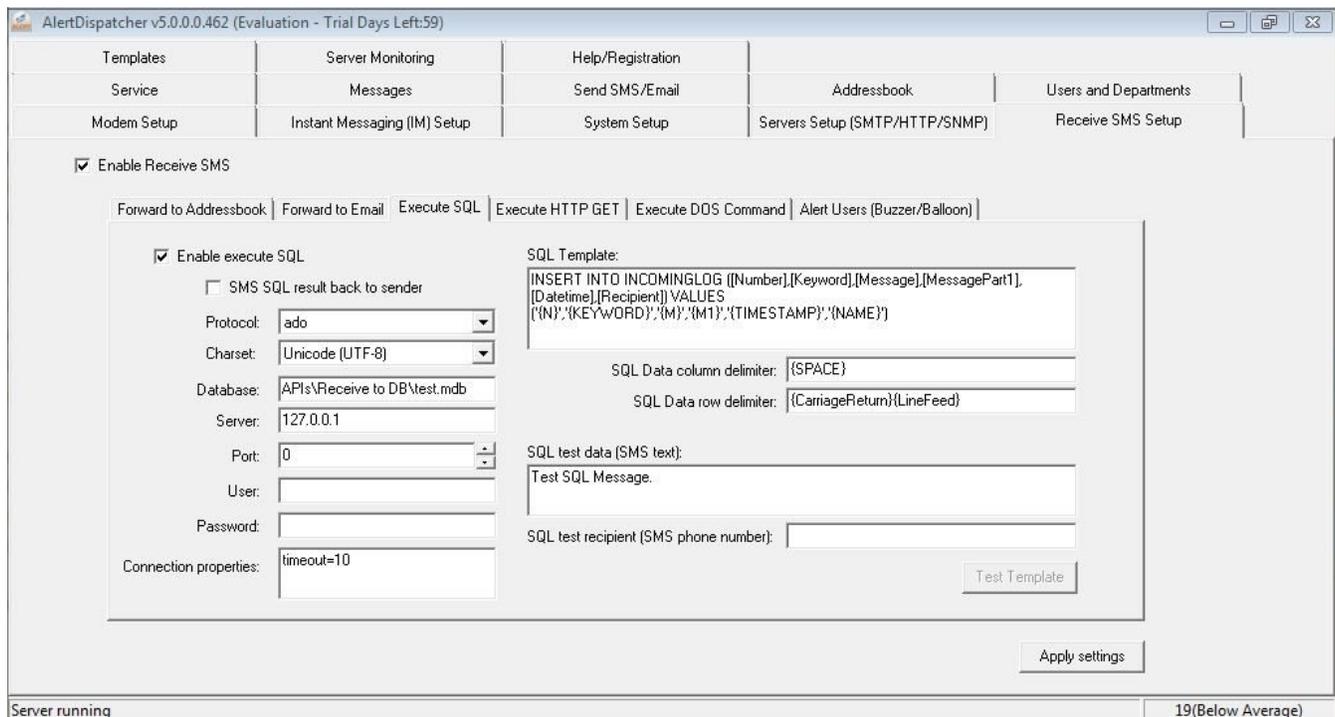
Note that if you include the surname in the recipient name, e.g. *‘tom sawyer’*, the keyword will be *‘tom sawyer’*, e.g. *“Tom sawyer, please come here”*.

If no match is found within the Addressbook, AlertDispatcher will then search the Message log for Email-to-SMS users that have contacted the sender of the received SMS within the last 2 days. By comparing the contents of SMS sent and received, particularly names addressed in the messages, AlertDispatcher will forward the SMS received to the Email-to-SMS user who is the most likely intended recipient for the SMS reply. If a good match cannot be determined, AlertDispatcher will forward the SMS to all Email-to-SMS users that had contacted the sender within the last 2 days.

Last, if no matches are found, AlertDispatcher will (only then) forward the SMS to the Admin Email Address – as configured under Alerts/Email Setup and up to 4 unique Email addresses.

### c). Execute SQL

AlertDispatcher also allows you to execute an SQL query based on the SMS received by the modem.



The following example will execute the following SQL statement against the MSSQL Server mypc/sqlexpress.

```
INSERT INTO INCOMINGLOG ([Number],[Keyword],[Message],[MessagePart1],[Datetime],[Recipient])
VALUES('{N}','{KEYWORD}','{M}','{M1}','{TIMESTAMP}','{NAME}')
```

*{N}* represents the mobile number of the sender.

*{KEYWORD}* represents the first section of the SMS message delimited by the first instance of the data delimiter which is *{SPACE}* by default. You can also use asterisk (please use the original \* symbol in the setting), hex or any other symbol.

*{M}* represents the entire SMS message including the keyword.

*{M1}* represents the second section of the SMS message after the first delimiter and before the second delimiter.

*{NAME}* represents the Addressbook entry of the sender.

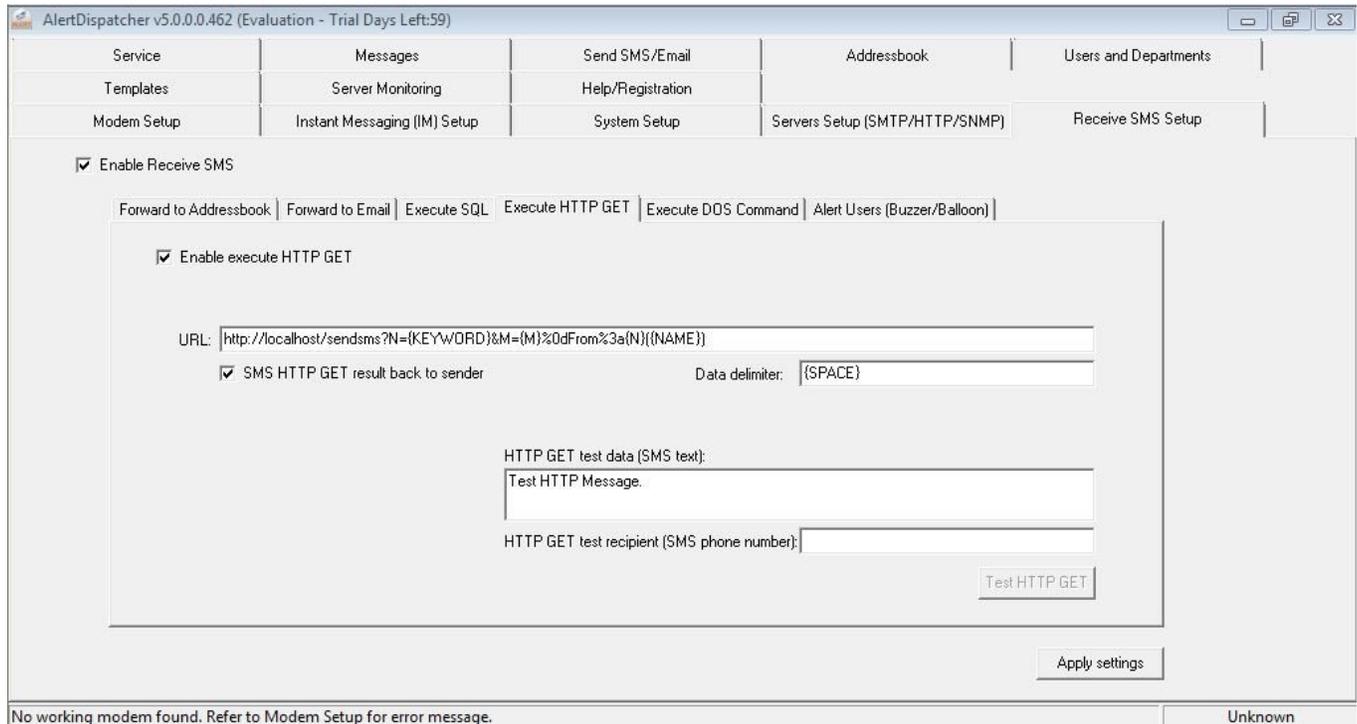
For example, if the SMS message is “How are you?” by “Tom” from his mobile phone number “+44123456789”, the following SQL query will be executed by AlertDispatcher:

```
INSERT INTO INCOMINGLOG ([Number],[Keyword],[Message],[MessagePart1],[Datetime],[Recipient])
VALUES( '+44123456789', 'How', 'How are you ', 'are', '2010-01-01 00:00:01', 'Tom' )
```

If the SQL execution returns a result as is the case of a SELECT statement, you can send the result back to sender by enabling “SMS SQL result back to sender”.

## d). Send HTTP GET request

AlertDispatcher also allows you to send an HTTP GET requests based on the SMS received by the modem.



The following example will issue the following HTTP GET request, which will forward SMS received by AlertDispatcher back to the built-in HTTP Server (SMS loop back). The KEYWORD of the SMS received would be the assigned recipient.

*SMS Message: 9123456789 test sms*  
*From Phone Number: 812345678*

*URL setting: http://localhost/sendsms?N={KEYWORD}&M={M}%0dFrom%3a{N}({NAME})*

Where,

*{N} represents the mobile number of the sender.*

*{KEYWORD} represents the first section of the SMS message delimited by the first instance of the SQL data delimiter which is {SPACE} by default. You can also use asterisk (please use the original \* symbol in the setting), hex or any other symbol.*

*{M} represents the entire SMS message including the keyword.*

*{M1} represents the second section of the SMS message after the first delimiter and before the second delimiter.*

Hence,

*{KEYWORD} = 912345678*  
*{M} = 912345678 test sms*

{MI} = test

{N} = 812345678

{NAME} = tom

Actual HTTP GET Request:

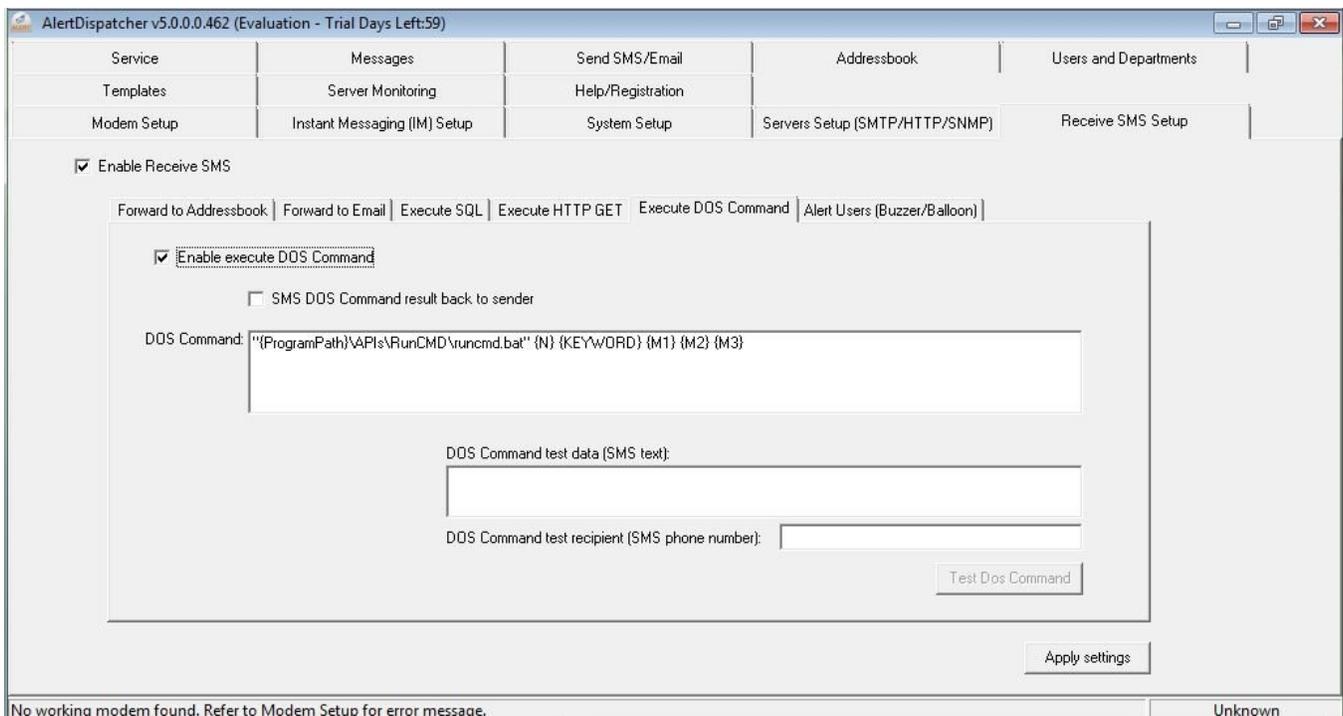
[http://localhost/sendsms?N=912345678&M=912345678%20test%20sms%0dFrom%3a812345678\(tom\)](http://localhost/sendsms?N=912345678&M=912345678%20test%20sms%0dFrom%3a812345678(tom))

If successful, it will send the message “912345678 test sms From:812345678(tom)” to “912345678”.

If ‘SMS HTTP GET result back to sender’ is enabled, the HTTP response would be sent back to the sender.

#### e). Execute DOS Command

AlertDispatcher also allows you to execute a DOS Command and return the result back to the sender. The given example executes runcmd.bat provided in the installation.



Please refer to [Appendix C – FAQ and Tips](#).

If you are still facing problems, send a detailed description of the issue you are facing along with the log files located in C:\Program Files\AlertDispatcher\Log to your vendor.

You may also refer to [Appendix B - Troubleshooting Checklist](#).

## 11). Configure Reports

If you're using the Corporate License (or higher), you can configure AlertDispatcher to send daily/monthly/yearly reports containing usage statistics via SMS or Email. A message export can be optionally attached to Email reports. From v4.5, usage reports will be breakdown by users, by departments (of users) and by modem (for SMS).

Here's an example of an Email report.

**Subject:** [COMPAQSERVER] Daily Report generated for 07 04, 2011, Period: 2011-07-04 00:00:00 to 2011-07-04 23:59:59  
**From:** AlertDispatcher <AlertDispatcher@ismsgateway.com>  
**Reply-To:** AlertDispatcher@ismsgateway.com  
**Date:** 7/5/2011 12:00 AM  
**To:**

[COMPAQSERVER] Daily Report generated for July 4, 2011, Period: 2011-07-04 00:00:00 to 2011-07-04 23:59:59

#### SMS Statistics

- 1). Number of SMS successfully sent: 5
- 2). ACTUAL number of SMS successfully sent: 5
- 3). Number of SMS that failed to send: 37
- 4). Number of SMS received: 4

#### Email Statistics

- 1). Number of Emails successfully sent: 1
- 2). Number of Emails that failed to send: 0

Please refer to CSV attachment for the SMS log.

Note: For item 1 of SMS Statistics, a long or concatenated SMS is treated as one SMS.

Sent from AlertDispatcher v1.5.0.0 - Licensed User:UNLICENSED - TESTING USE ONLY



report\_2011\_07...4\_23\_59\_59.zip

### 3. License Registration using Activation Code

Once you have successfully setup and configured your AlertDispatcher installation, the software will work fully for 60 days until you registered your software.

To register, run AlertDispatcher Client, and click on the 'Register Software' button on the splash screen. Alternatively, you can launch AlertDispatcher Client and navigate to the "Help/Registration" Tab on the main page.



You may register **via Internet** or **via SMS**.

#### 1). Register via SMS

If you do not have access to Internet connection, you may try to register **via SMS** by ticking the checkbox "Register via SMS". If you are not able to tick "Register via SMS", please ensure you have configured a modem and inserted a working SIM card and restart AlertDispatcher service. You may send a test SMS to verify your configuration is correct.

Alternatively, you can perform Internet activation by copying the registration link generated on the AlertDispatcher server (which does not have Internet) to another machine with Internet connection (for example your laptop). **Warning:** You must not generate the registration link on your laptop as the key will fail to work as it is for your laptop and not for AlertDispatcher server.

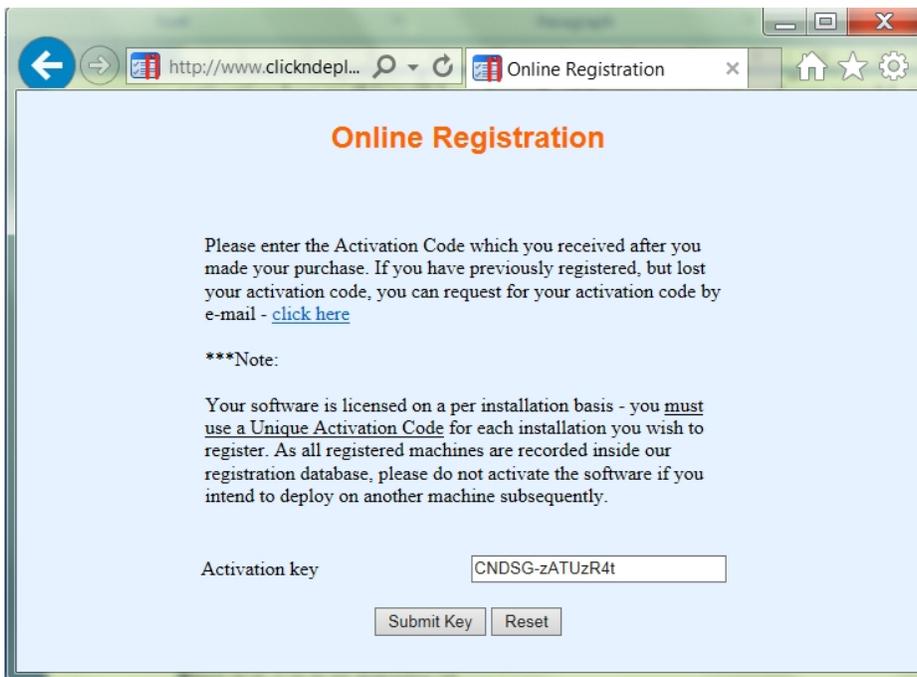
 The image is a screenshot of a Windows-style dialog box titled 'Register Software'. It has a green header bar with the title and standard window controls (minimize, maximize, close). The main area is white with a light gray border. On the left, there is a button labeled 'Register via Internet'. To its right, there is a text box containing the instruction: 'Click on this button to register or upgrade your license. Requirement: Software activation code (you can either find it in your CDFROM package or obtain it from your vendor.)'. Below this, there is a checked checkbox labeled 'Register via SMS'. Underneath the checkbox, there are four input fields: 'Activation Code:' with the value 'CNDSG-zATUzR4t', 'Organization Name:' with 'Click And Deploy Pte Ltd', 'Contact Person:' with 'Michael Tan', and 'Contact Person Email:' with 'michael.tan@clickndeploy.com'. To the right of these fields is a button labeled 'Activate via SMS'.

## 2). Register via Internet

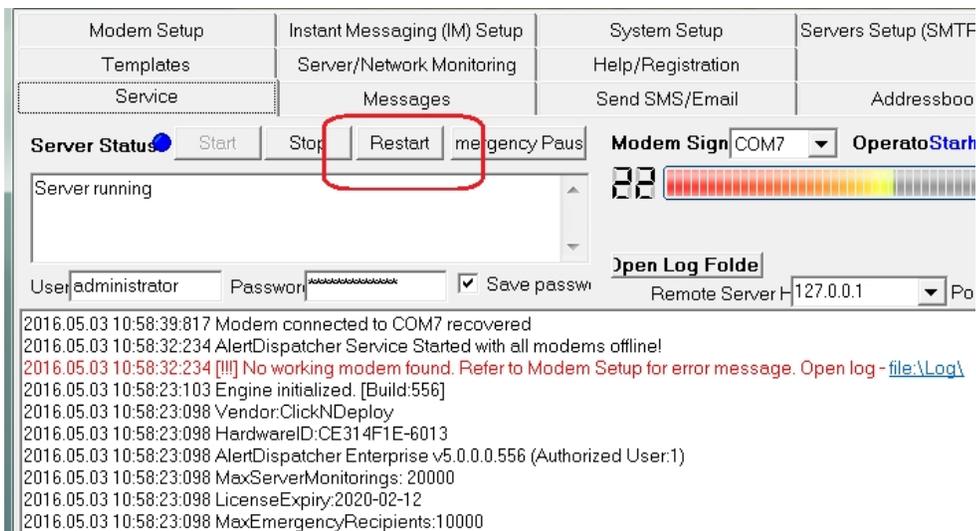
After clicking "Register via Internet", the following website will load. Enter your license Activation Code which is in the format "CNDSG-zATUzR4t". Note: "CNDSG-zATUzR4t" is only an example, please do not use this code.

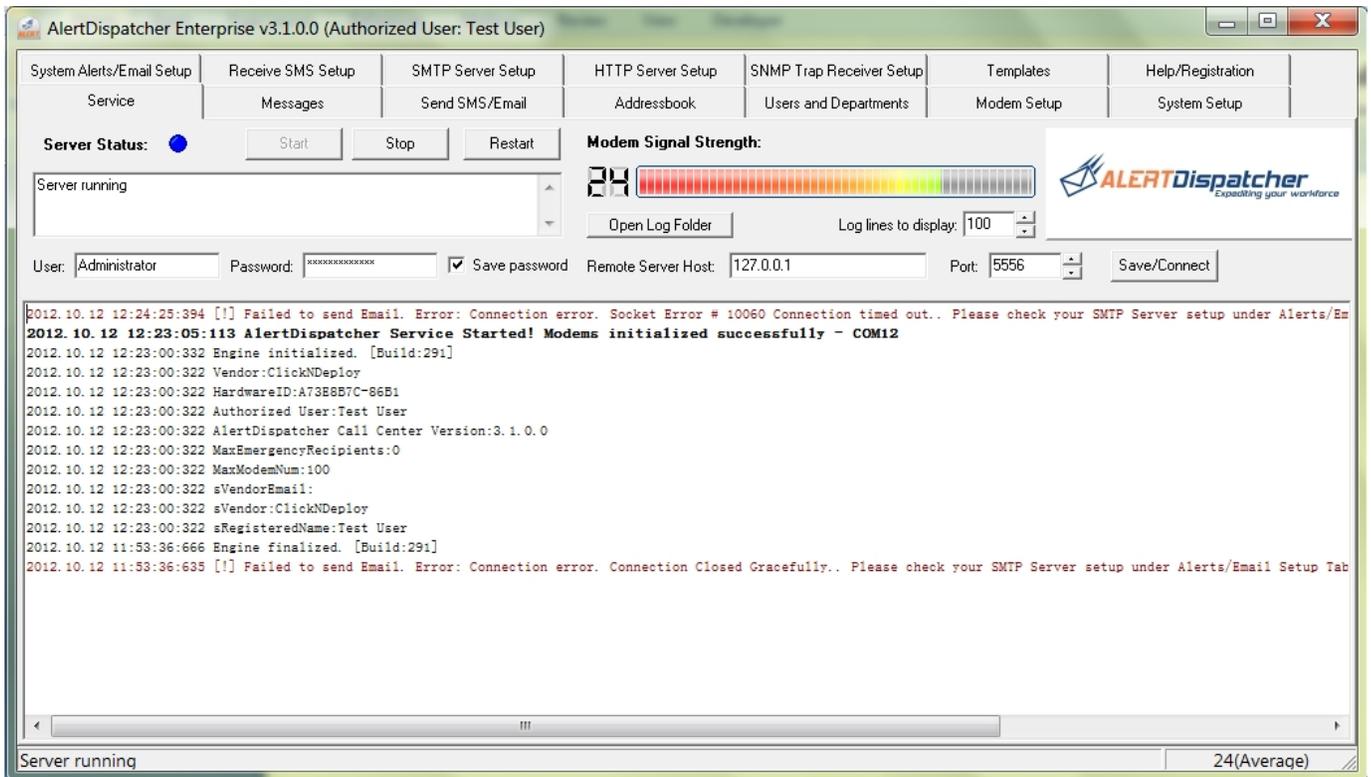
The Activation Code can be found on your CDROM or the Email sent to you after you have made your order. If you do not have this code, please contact your software vendor. The software code will be sent to you by Email. Please check your spam folder if you cannot find your activation Email.

The Activation Code is unique to your machine; please do not use it to register multiple machines as it may cause the Activation Code to be voided.



After you have applied downloaded the registration key (for case of Internet registration), please restart AlertDispatcher Service to confirm that your software has been registered.





Congratulations, you have successfully installed and registered your AlertDispatcher software. Please refer to [Appendix C – FAQ and Tips](#).

If you are still facing problems, send a detailed description of the issue you are facing along with the log files located in C:\Program Files\AlertDispatcher\Log to your vendor.

You may also refer to [Appendix B - Troubleshooting Checklist](#).

## 4. Interfacing with AlertDispatcher using SMTP/HTTP/DOS

### 1). Using AlertDispatcher built-in SMTP Server to send Alerts (Email-to-SMS/Email)

AlertDispatcher has a built-in SMTP Server that listens to port 25 (default). The built-in SMTP Server allows AlertDispatcher to be used as an Email-to-SMS/Email gateway. You can configure MS Exchange or Lotus Notes to forward Emails to AlertDispatcher which will deliver them as SMS and/or Email using configurable rules.

**Note:** This setting is different from the '*SMTP Server*' setting found under '*System Setup --> Alerts/Email Setup*' tab – which allows AlertDispatcher to relay Email (as an Email client) to network based SMTP Servers.

The SMTP interface is required for some of the APIs such as the SQL Server stored procedure. As SMTP is a common protocol, the SMTP interface allows you to send Alerts (SMS/Email) from any programming language or software that can send out Email.

Refer to '*Configure SMTP Server Setup*' for more information.

### 2). Sending Alerts (SMS/Email) by executing an SQL Stored Procedure (MSSQL)

Database Mail is a feature of SQL Server 2005 (and higher versions) that allows you to send email using SQL. Using Database Mail, you can use AlertDispatcher's SMTP server to send SMS/Email from your database/SQL applications. You can find an example in C:\Program Files\AlertDispatcher\APIs\SQLServer\.

Database Mail will send Email to AlertDispatcher's SMTP server, so your SQL Server must have network connectivity to AlertDispatcher server, and if there's a firewall running, please ensure that port 25 is opened.

Finally, the following example shows how you can use Database Mail to send Alerts:

```
-----
EXEC msdb.dbo.sp_send_dbmail @recipients='+44123456789@alertydispatcher.com',
@body = 'Place Alert Message here';
-----
```

Refer to the readme file found in C:\Program Files\AlertDispatcher\APIs\SQLServer\ for the complete setup and usage information for Database Mail.

### 3). Sending Alerts (SMS/Email) using HTTP or from a web browser

Besides the SMTP Server, AlertDispatcher also comes with a built-in HTTP or Web Server which you can use to send out Alerts from a HTTP client or your web browser. A web form is also provided for end users. The HTTP Server is set to listen to port 80 by default. If you have another HTTP Server using port 80, you will need to amend this to another port, e.g. port 81 by configuring HTTP Server Setup.

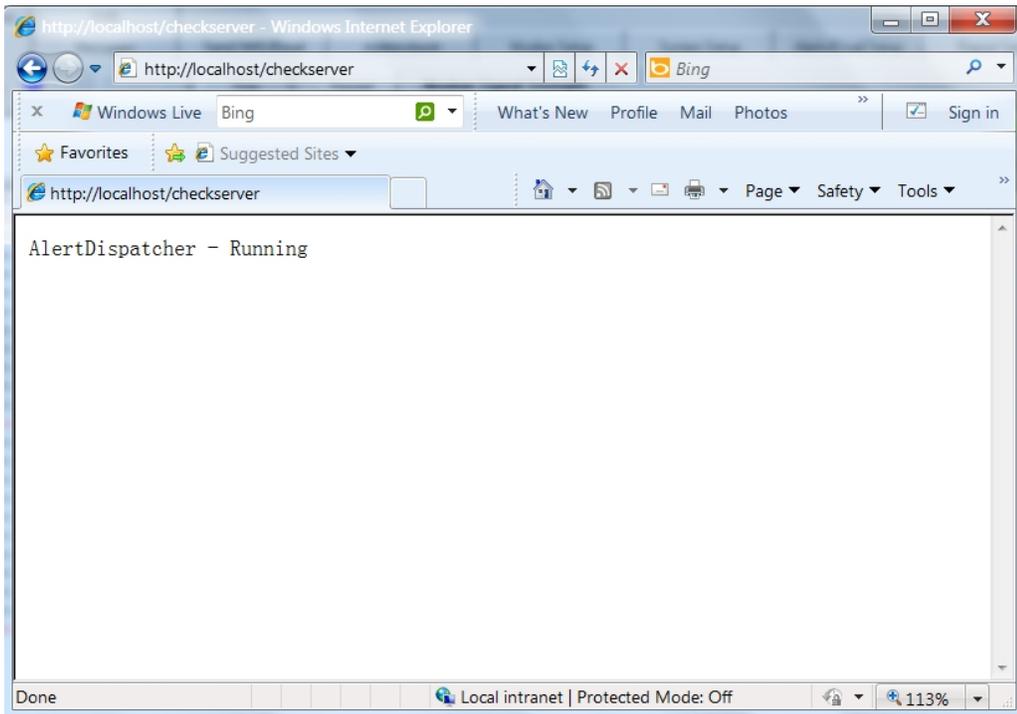
To check whether the HTTP Server is running, go to <http://localhost/> using your web browser. You will see the following login page on successful connection. You may access this URL from a remote PC and download AlertDispatcher Client using the '*Click here to download AlertDispatcher Client*' link. No installation is

required to run AlertDispatcher Client.

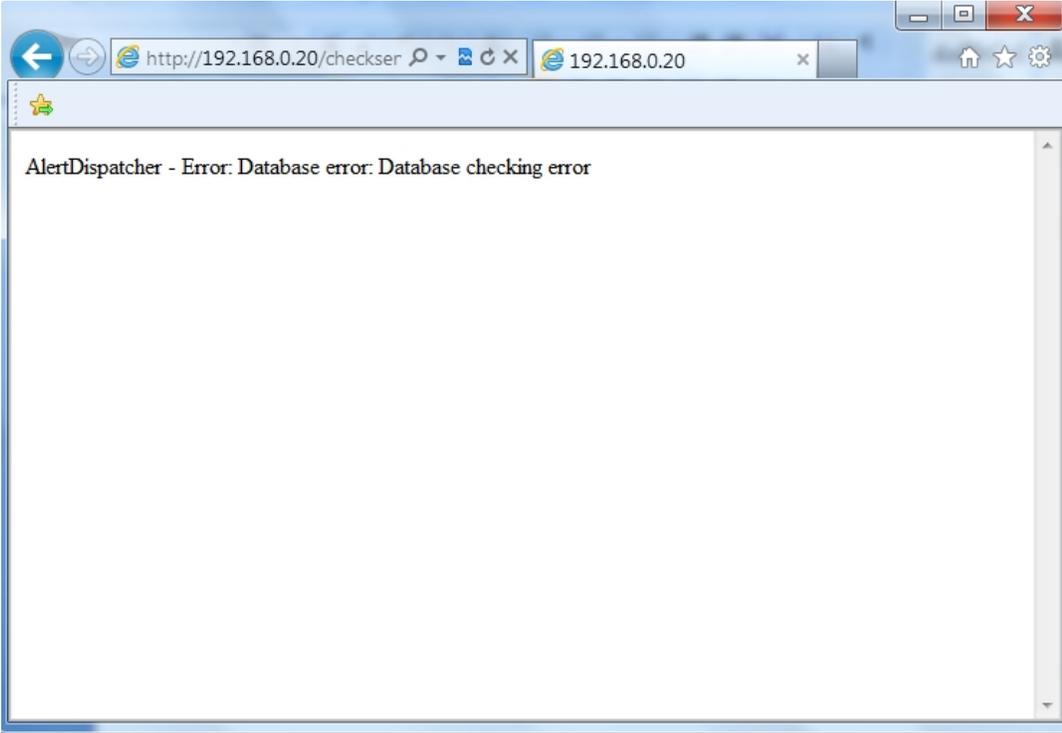
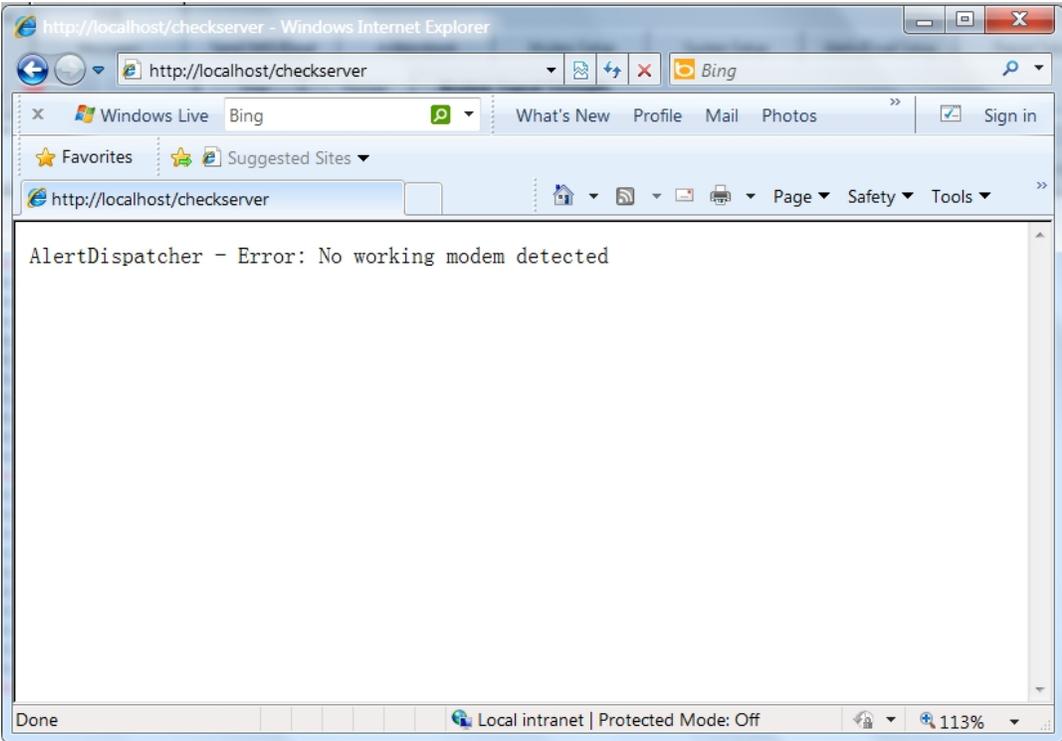


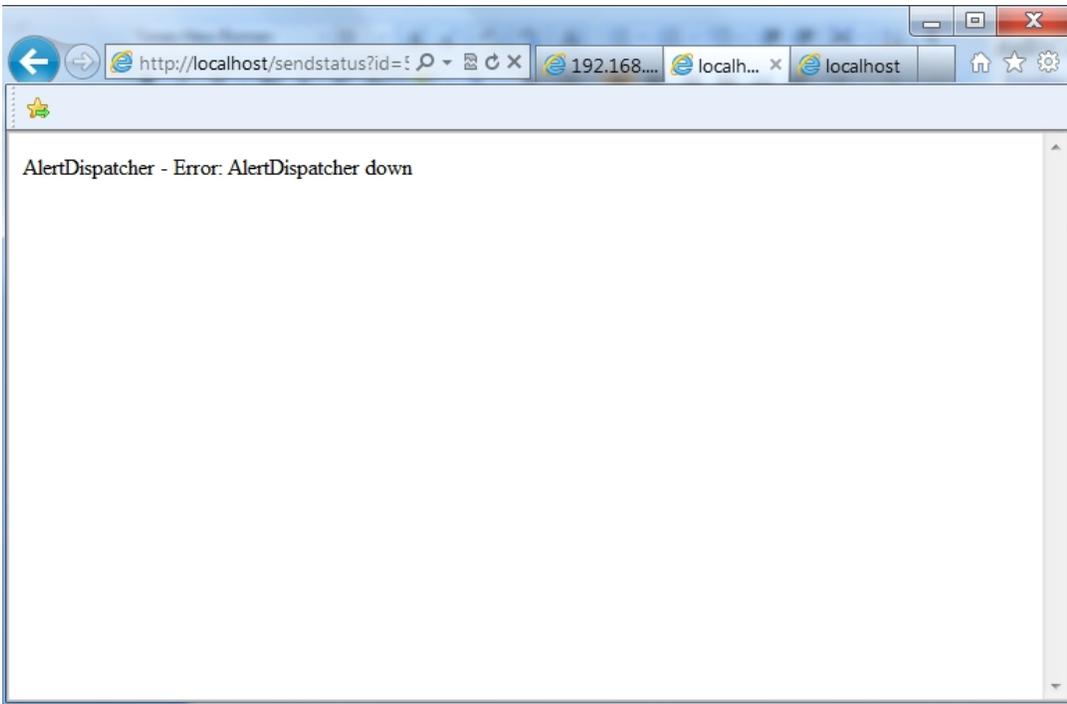
You can check the status of the AlertDispatcher and the modem by going to <http://localhost/checkserver> or <http://localhost/checkserver?USERNAME=your-user-name&PASSWORD=your-user-password> (if "Authenticate against the Users database" setting under "HTTP Server Setup" Tab is enabled).

If everything works, AlertDispatcher will return "AlertDispatcher - Running".



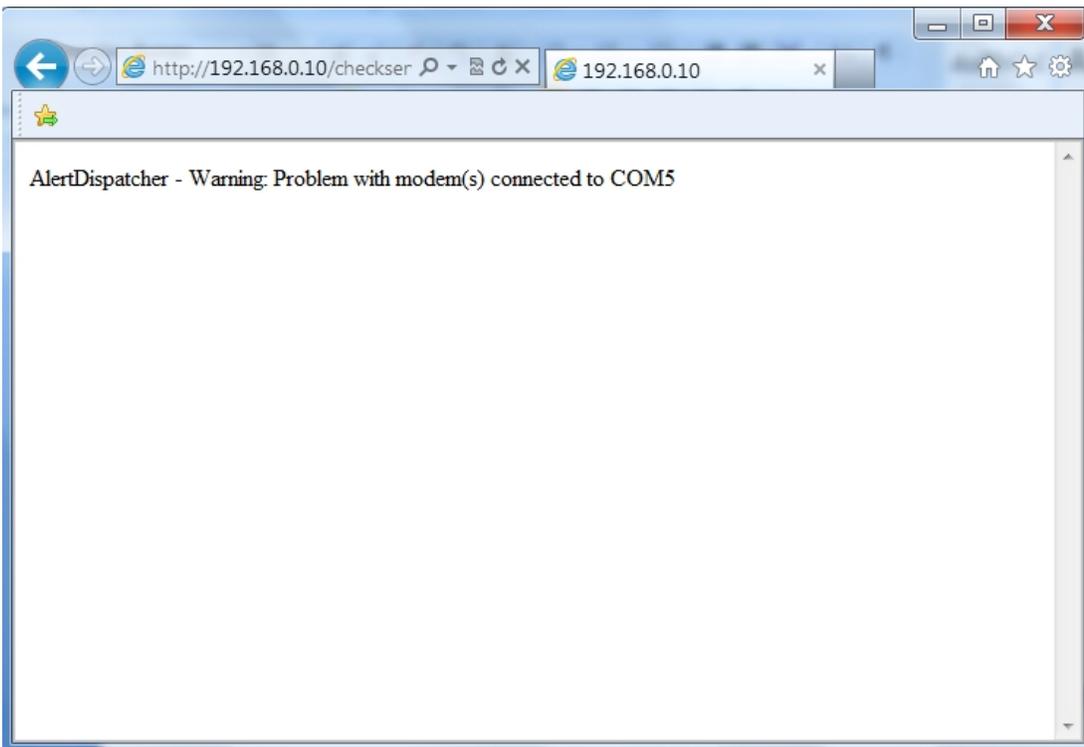
If there are critical errors such as when all modems are down, AlertDispatcher will return 'Error:' followed by the error message. Here are some examples:





For non-critical errors, AlertDispatcher will return ‘Warning:’ followed by the error message.

In the following example, the modem connected to COM5 has errors, however there are other working modems connected to the server.



To send an Alert, append command 'sendsms' followed by the **N** parameter (the Mobile number, Email address, or the Addressbook user/group name - use comma separator if there is more than one item), the **M** parameter (message text), and the optional **P** parameter (message priority), **D** parameter (scheduled date time to send), **MODEMPORT** parameter, **USERNAME** and **PASSWORD** parameters. Only **N** and **M** parameters are compulsory, the rest are optional (**USERNAME** and **PASSWORD** parameters are only required if "Authenticate against the Users database" setting under "*HTTP Server Setup*" Tab is enabled).

e.g. <http://localhost/sendsms?N=+6590169696&M=Hello World&P=4&D=2010-12-01 20:00:00&MODEMPORT=4&USERNAME=test&PASSWORD=test>

The format for parameter **D** is: YYYY-MM-DD HH:MM:SS

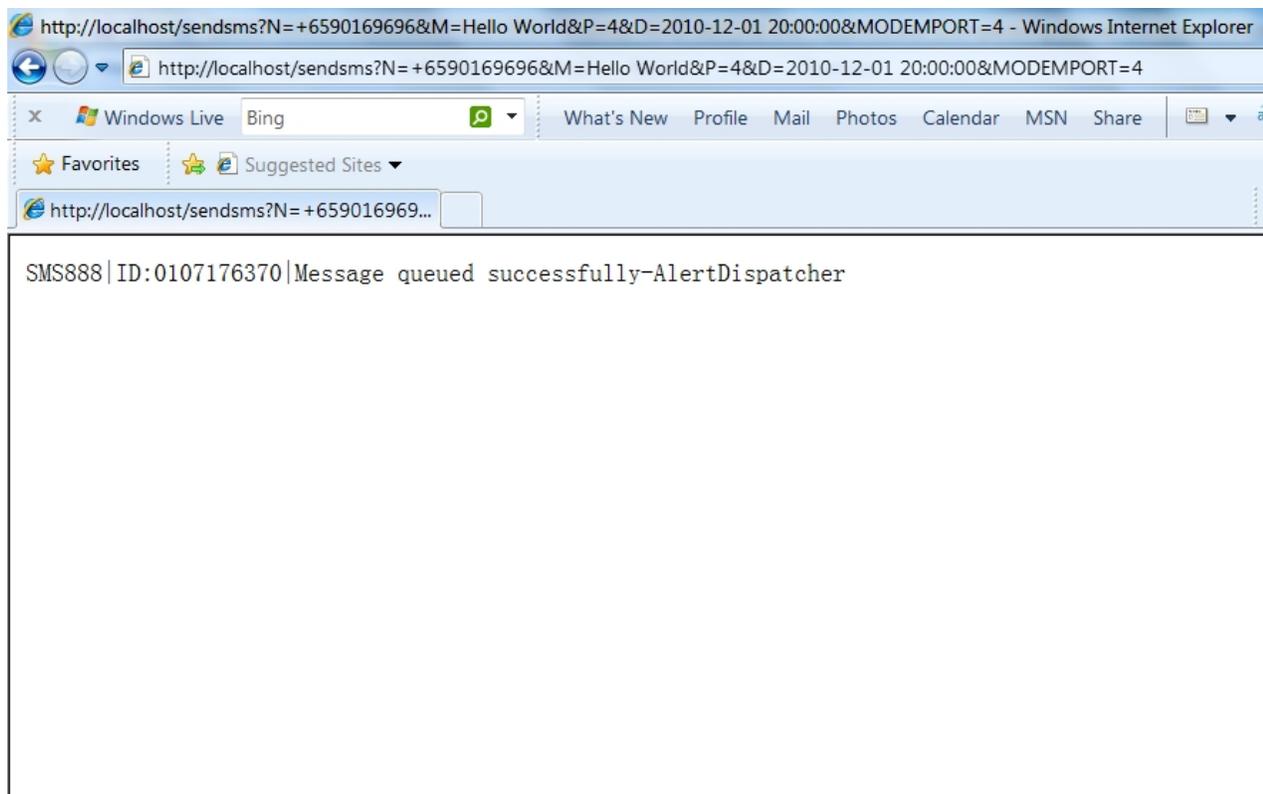
**P** ranges from 1 (lowest priority) to 4 (highest priority). Default is 2.

**MODEMPORT** refers to the COM port of the modem you intend to use. This is optional. If you do not specify this parameter, the server will use each available modem in a rotating round robin manner.

The above URL GET will send "Hello World" to +6590169696 on the 1<sup>st</sup> December 2010 at 20:00:00 hrs using the modem connected to COM 4.

On success, the web server will return: *SMS888/ID:1661540085/Message queued successfully-AlertDispatcher*

**Note: The above URL example only works on a browser for testing purpose. For actual URL sent by your application/script, please use full URL encoding for all variable values. For example, space should be encoded to "%20" (not "+" sign) and "+" sign should be encoded to "%2B".**



'SMS888' indicates send success.

Other return codes:

SMS007|Destination Missing-AlertDispatcher

SMS014|Content Missing-AlertDispatcher

SMS008|Access Denied-AlertDispatcher

SMS015|[Variable Error Message\\*](#)-AlertDispatcher

\*For example, the following would mean the AlertDispatcher is down or not started.

SMS015|Can't connect to 127.0.0.1:5556-AlertDispatcher

'1661540085' is a tracking message ID which you can use to enquire the send status using the command 'sendstatus'.

e.g. <http://localhost/sendstatus?ID=1661540085&USERNAME=test&PASSWORD=test>

The web server returns: ID:1661540085 | STATUS:4 | ERROR: | SENTTIME:2011-04-21 01:23:56

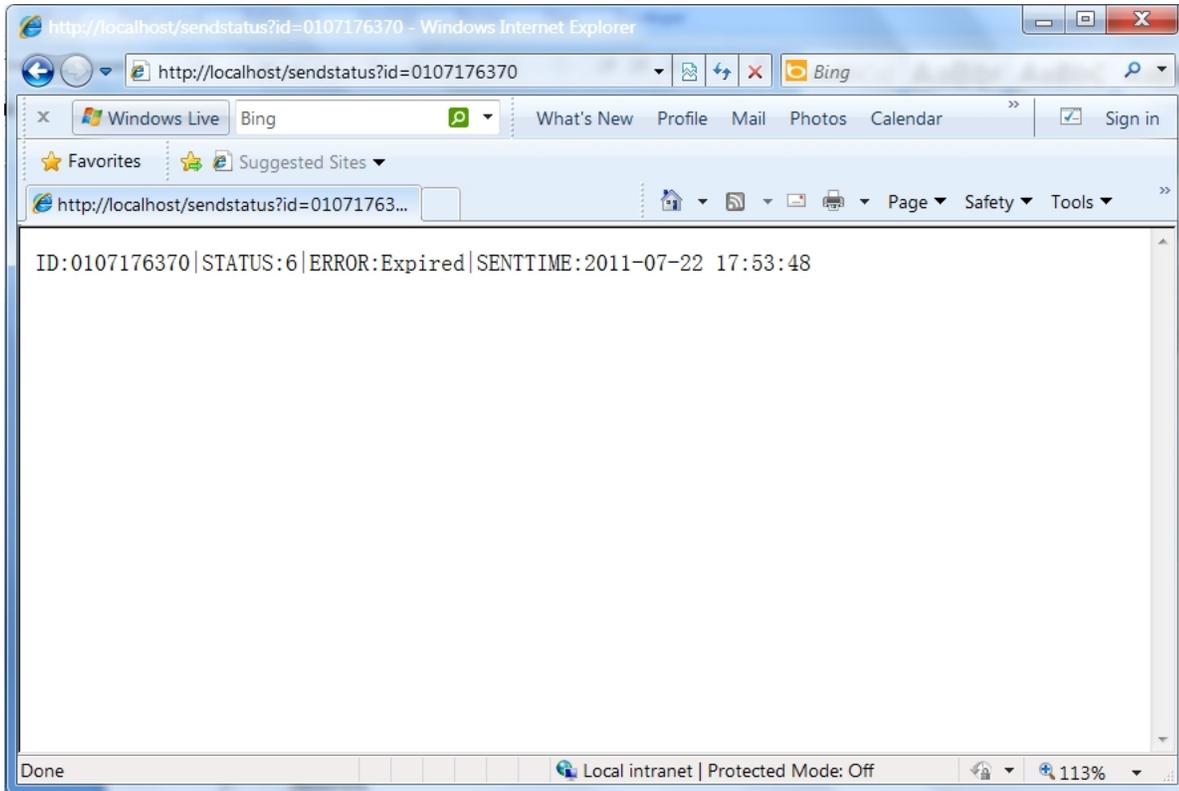
If the tracking ID is not found, which could happen if the message has been deleted, the web server returns:

ID:1661540085 | STATUS:0 | ERROR:Message not found

STATUS refers to the send status – 4 indicates the message has been successfully sent out (see list below for the status code definition).

ERROR refers to the error message if available.

SENTTIME refers to the sent out timestamp in the format YYYY-MM-DD HH:MM:SS.

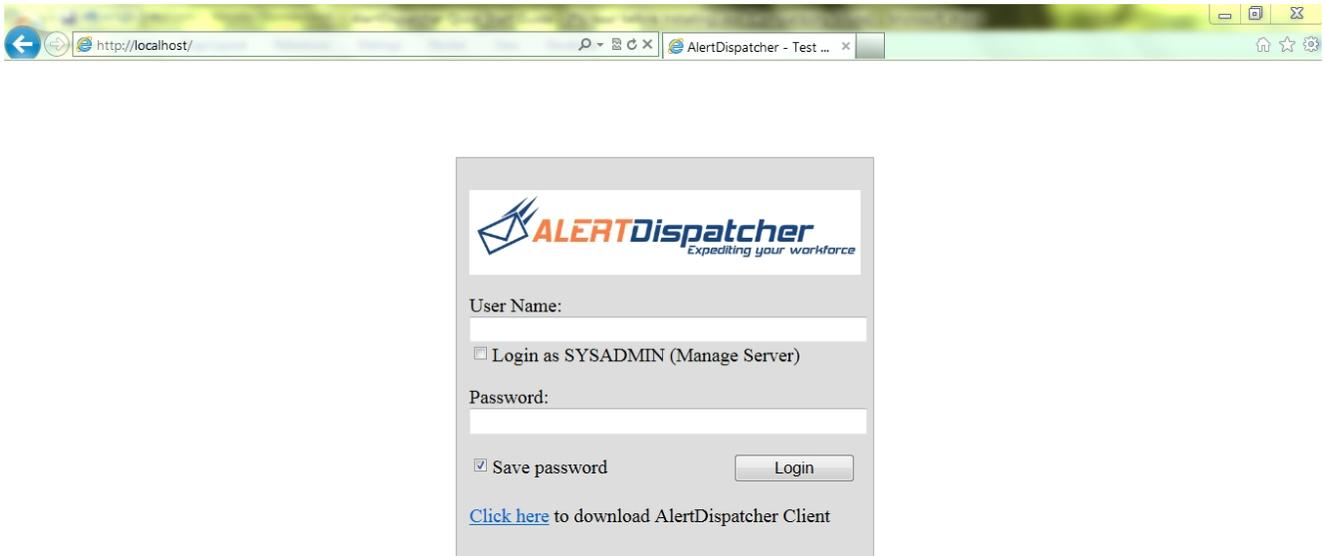


#### MESSAGE STATUS CODE DEFINITION

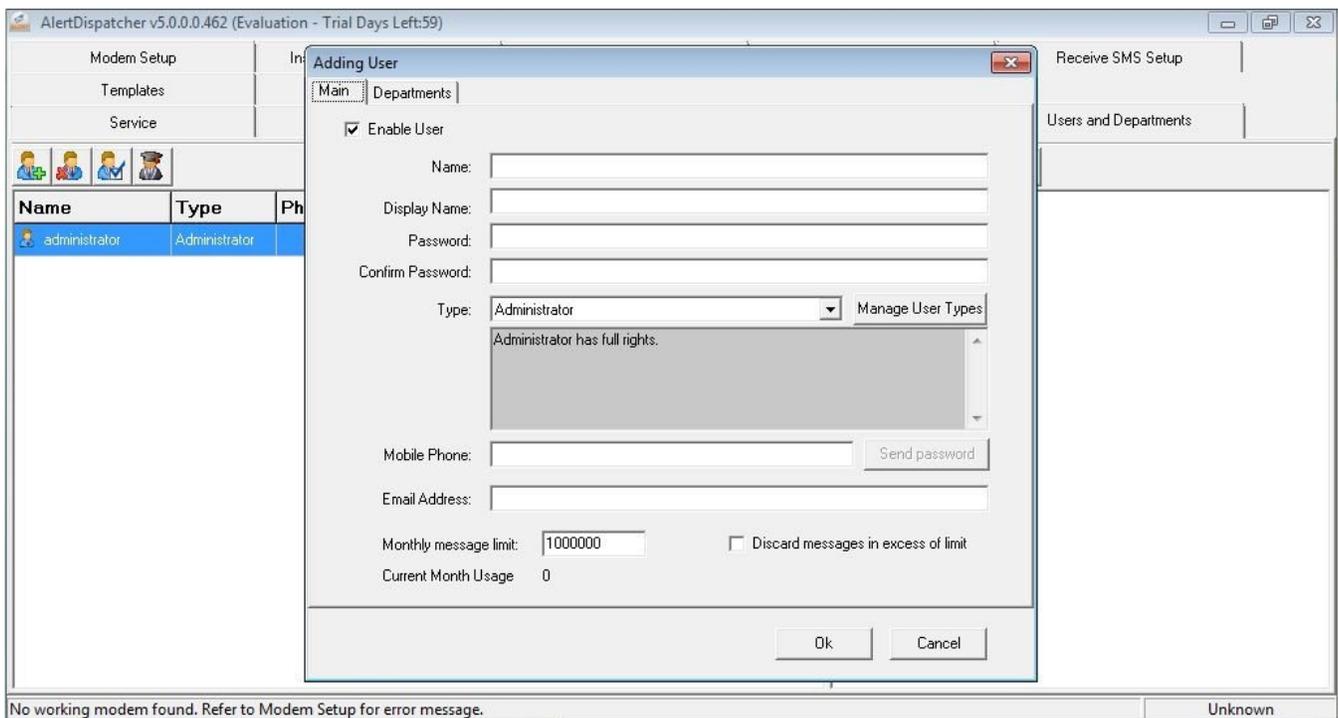
0:	Unknown
1:	[Out]WaitingForSend'
2:	[Out]Sending
3:	[Out]ReSending
4:	[Out]Sent
5:	Aborted
6:	[Out]Error
13:	[Out]Waiting
14:	[Out]PendingAcknowledge
15:	[Out]Acknowledged
16:	[Out]Escalated
17:	[Out]AcknowledgeTimeout

**Note:** If you have enabled "Authenticate against the Users database" setting under "HTTP Server Setup" tab, you must use the USERNAME and PASSWORD parameter for all requests sent to the HTTP Server.

You may login to the web portal via <http://localhost> to send messages. The user 'administrator' (password: 'administrator') is created by default.



You may manage users using the ‘Users and Departments’ tab on AlertDispatcher Client.



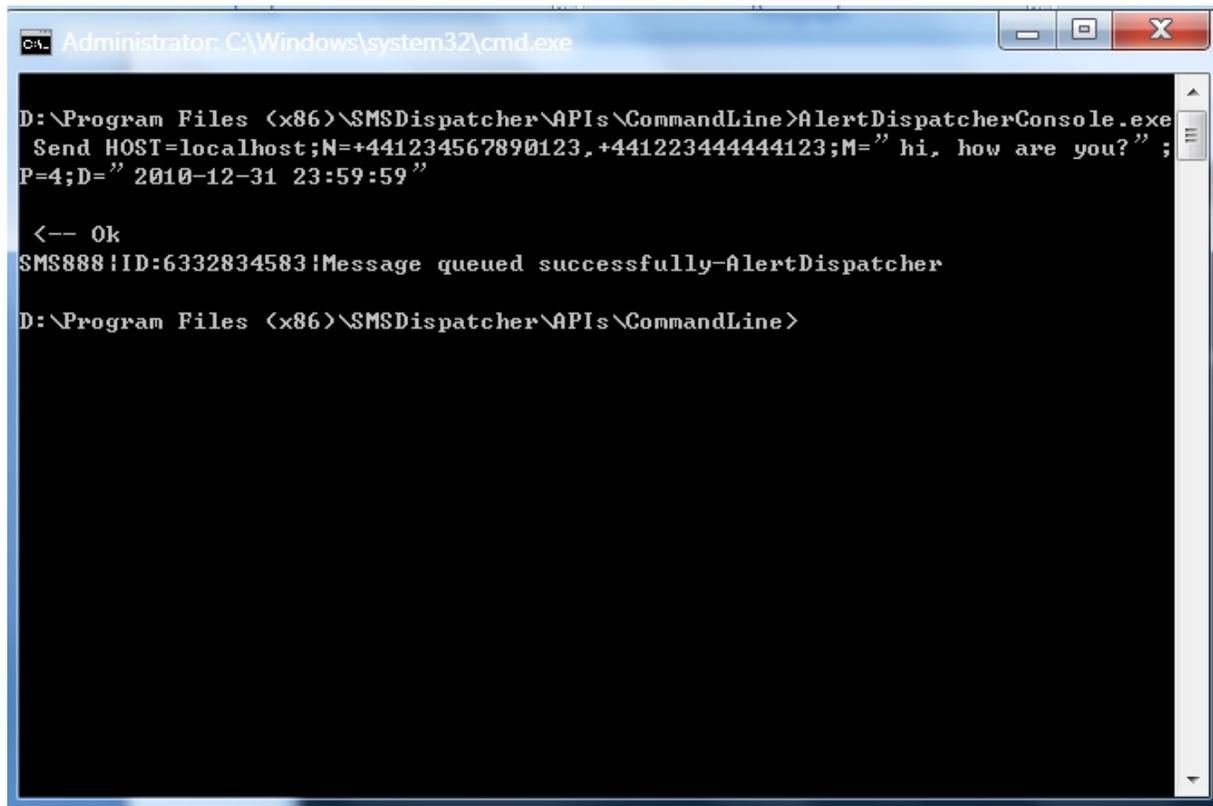
#### 4). Sending Messages/Query Status from Windows Command Line or Batch File

You can also send Alerts (SMS/Email) from command line using C:\Program Files\AlertDispatcher\APIs\CommandLine\AlertDispatcherConsole.exe to a local or remote AlertDispatcher Server.

```
e.g. AlertDispatcherConsole.exe Send
HOST=localhost;N=+441234567890123,+441223444444123;M="hi, how are
you?";P=4;D="2010-12-31 23:59:59"
```

Where **HOST** parameter is the AlertDispatcher Server IP address or hostname (default to localhost), **N** parameter is a list of recipient(s) delimited by commas, **M** parameter is the SMS message, **S** parameter is the subject (for Email), optional **P** parameter is the priority which ranges from 1 (lowest priority) to 4 (highest priority), optional **D** parameter (scheduled date time to send), and optional **MODEMPORT** parameter (0 = Auto).

'SMS888' indicates send success. '6332834583' is a tracking message ID which you can use to enquire the send status using the command 'sendstatus'.



```
Administrator: C:\Windows\system32\cmd.exe
D:\Program Files (x86)\SMSDispatcher\APIs\CommandLine>AlertDispatcherConsole.exe
Send HOST=localhost;N=+441234567890123,+441223444444123;M="hi, how are you?";
P=4;D="2010-12-31 23:59:59"
<-- Ok
SMS888!ID:6332834583!Message queued successfully-AlertDispatcher
D:\Program Files (x86)\SMSDispatcher\APIs\CommandLine>
```

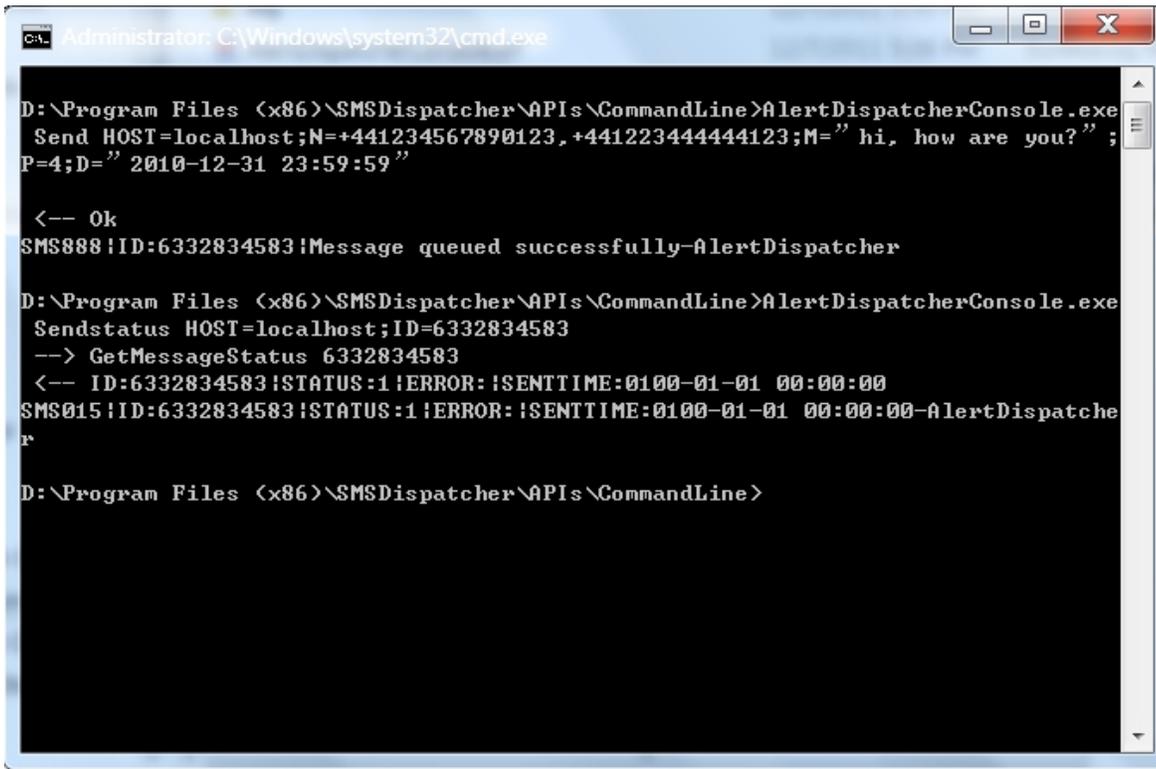
AlertDispatcherConsole also allows you to define a failover/alternate AlertDispatcher Server if the primary HOST is down and can also send an alert to a recipient defined by you when a failover or recovery (of primary host) occurs.

```
e.g. AlertDispatcherConsole.exe Send
HOST=localhost;FAILOVERHOST=192.168.0.10;ALERTRECIPIENT=sysadmin;N=+4412345
67890123;M="hi, how are you?"
```

Where **FAILOVERHOST** parameter is optional and is the failover/alternate AlertDispatcher Server IP address or hostname, and **ALERTRECIPIENT** parameter is a list of recipient(s) delimited by commas for alerts sent when a failover or recovery (of primary host) occurs.

You can also query the status of messages sent.

e.g. AlertDispatcherConsole.exe Sendstatus HOST=localhost;ID=6332834583



```
Administrator: C:\Windows\system32\cmd.exe
D:\Program Files (x86)\SMSDispatcher\APIs\CommandLine>AlertDispatcherConsole.exe
Send HOST=localhost;N="+441234567890123,+441223444444123;M="hi, how are you?";
P=4;D=" 2010-12-31 23:59:59"

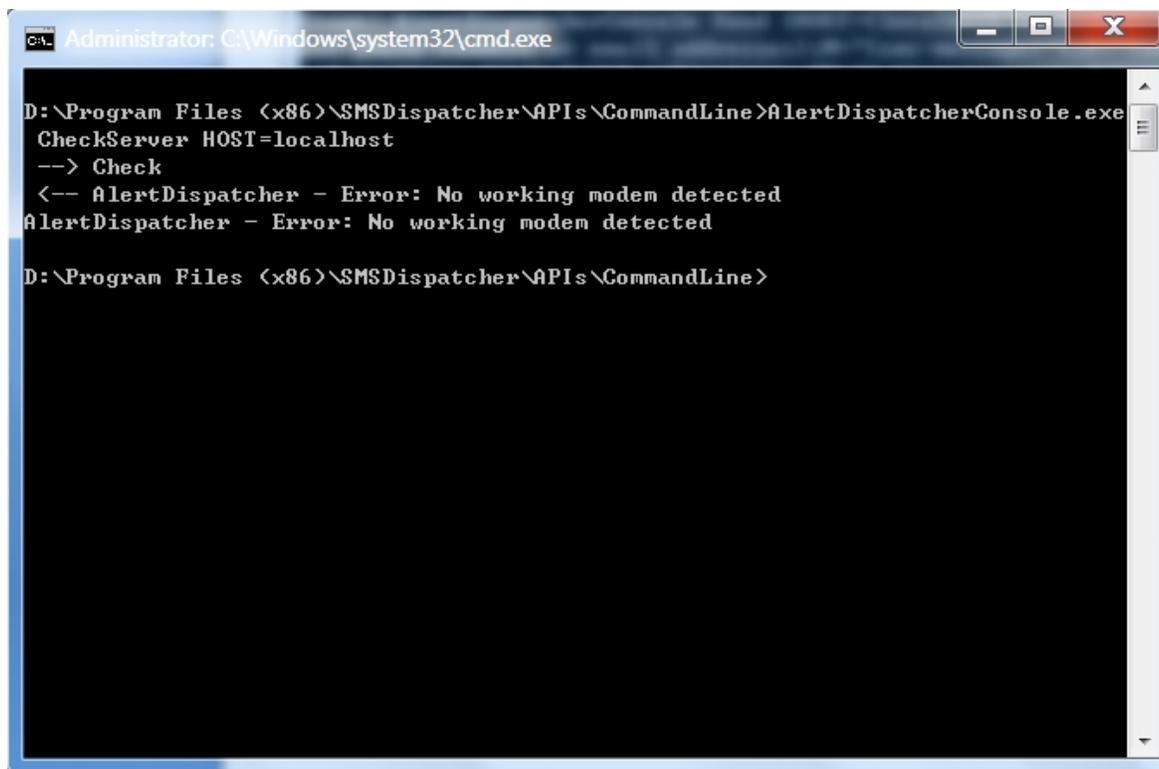
<-- Ok
SMS888!ID:6332834583!Message queued successfully-AlertDispatcher

D:\Program Files (x86)\SMSDispatcher\APIs\CommandLine>AlertDispatcherConsole.exe
Sendstatus HOST=localhost;ID=6332834583
--> GetMessageStatus 6332834583
<-- ID:6332834583!STATUS:1!ERROR:!SENTTIME:0100-01-01 00:00:00
SMS015!ID:6332834583!STATUS:1!ERROR:!SENTTIME:0100-01-01 00:00:00-AlertDispatcher

D:\Program Files (x86)\SMSDispatcher\APIs\CommandLine>
```

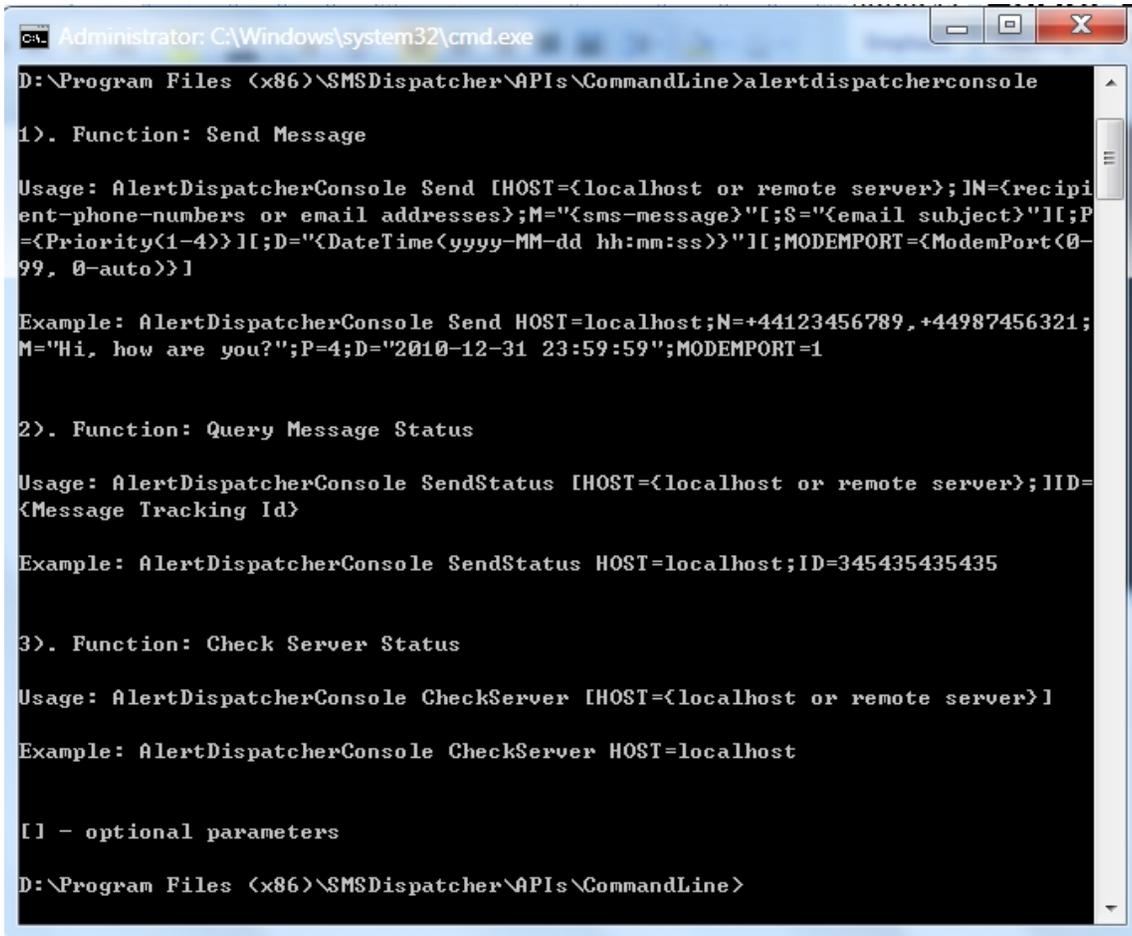
You can also check the status of AlertDispatcher Server.

e.g. AlertDispatcherConsole.exe CheckServer HOST=localhost



```
Administrator: C:\Windows\system32\cmd.exe
D:\Program Files (x86)\SMSDispatcher\APIs\CommandLine>AlertDispatcherConsole.exe
CheckServer HOST=localhost
--> Check
<-- AlertDispatcher - Error: No working modem detected
AlertDispatcher - Error: No working modem detected
D:\Program Files (x86)\SMSDispatcher\APIs\CommandLine>
```

Full Syntax:



```
Administrator: C:\Windows\system32\cmd.exe
D:\Program Files (x86)\SMSDispatcher\APIs\CommandLine>alrtdispatcherconsole

1). Function: Send Message

Usage: AlertDispatcherConsole Send [HOST=<localhost or remote server>;IN=<recipient-phone-numbers or email addresses>;M="{sms-message}"[;S="{email subject}"]I;P=<Priority<1-4>>]I;D="{DateTime<yyyy-MM-dd hh:mm:ss>}"I;MODEMPORT=<ModemPort<0-99, 0-auto>>]

Example: AlertDispatcherConsole Send HOST=localhost;N="+44123456789, +44987456321;M="Hi, how are you?";P=4;D="2010-12-31 23:59:59";MODEMPORT=1

2). Function: Query Message Status

Usage: AlertDispatcherConsole SendStatus [HOST=<localhost or remote server>;IID=<Message Tracking Id>]

Example: AlertDispatcherConsole SendStatus HOST=localhost;ID=345435435435

3). Function: Check Server Status

Usage: AlertDispatcherConsole CheckServer [HOST=<localhost or remote server>]

Example: AlertDispatcherConsole CheckServer HOST=localhost

[] - optional parameters

D:\Program Files (x86)\SMSDispatcher\APIs\CommandLine>
```

## 5). Interfacing from Dot Net or Java using COM DLL

Please refer to 'AlertDispatcher DLL API Guide' for more information.

## 5. Appendix A- Preparing your GSM/GPRS modem

### 1). Preparing the GSM modem.

Plug your GSM modem (with working SIM card inserted) into your PC. If you are using a USB modem, Windows will prompt for driver. You will need to insert the modem driver CDROM, and install the driver. If you are using a serial modem, driver is not required.

**Note:**

a). If you are using a USB modem, you must install the modem driver and then find the baud rate and COM port number from your modem driver under Windows Device Manager.

If you are using **Sierra Wireless GL6110 USB modem** or **Maestro 3G modem**, please install the modem driver in your CDROM – path - \Sierra Wireless Modem Driver\XP-2003-2008-Vista-7\USBDriverInstaller.exe.

JRE 6 (Java Runtime Environment) is a pre-requisite – the modem driver installer will automatically prompt you if JRE 6 needs to be installed. You can find JRE 6 installer in your CDROM - \Sierra Wireless Modem Driver\XP-2003-2008-Vista-7\USBDriverInstaller.exe - \Sierra Wireless Modem Driver\jre-6u22-windows-i586-s.exe.

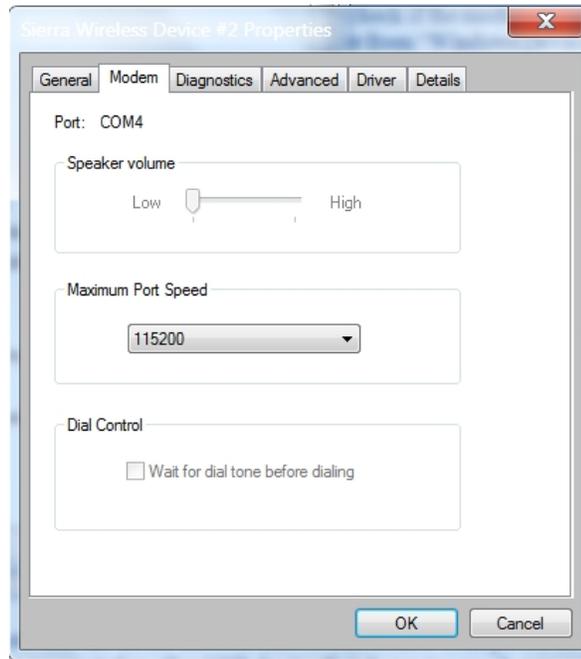
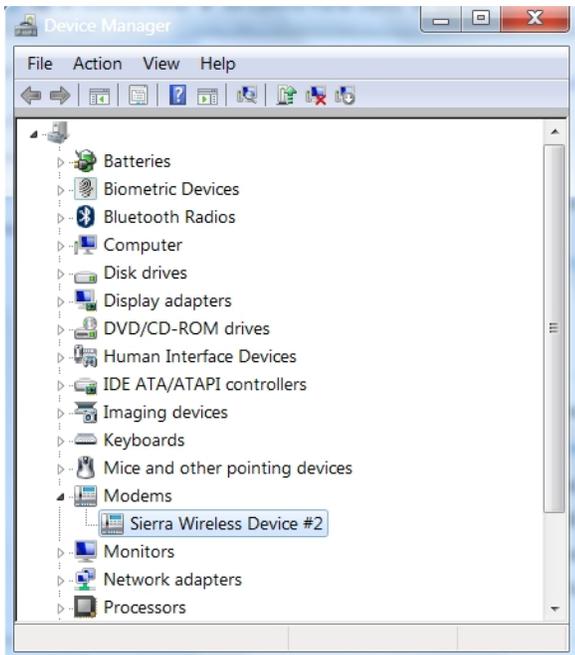
**Important:** For 64 bits Windows, you'll also need to install *jre-6u23-windows-x64.exe* in addition to *jre-6u22-windows-i586-s.exe*.



After installing the driver, insert the SIM card\* and then connect the modem to an available USB port. If Windows “Add New Hardware Wizard” appears, please direct Windows to find the driver under c:\Windows\System32\Drivers. If you are using Vista or 7 or 2007, the driver should be automatically detected. The modem should light up after the driver has been properly installed.

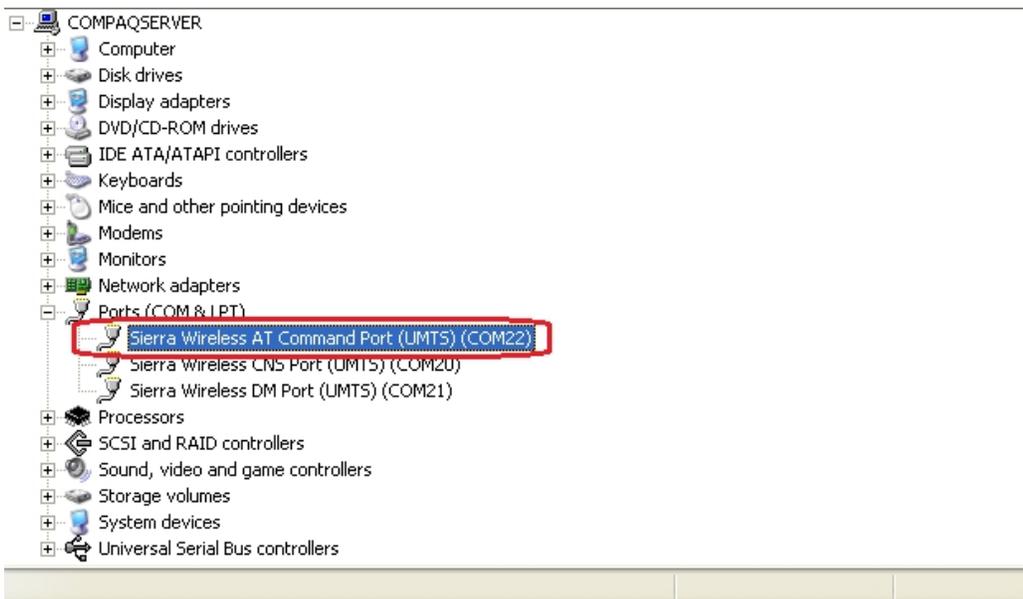
\*Note that you should insert the SIM card such that it is facing upwards and golden metal strip nearest to the opening. If you insert the SIM card incorrectly, the modem may not blink – no signal detected.

After that, check the modem COM port assigned to your modem under Windows Device Manager. **The USB modem uses a baud rate of 115200bps**. If you cannot find the Sierra Wireless modem device or the power indicator light does not light up, please check if the modem is properly connected to a working USB port, you may also try removing the modem driver from “Windows Device Manager” and then reboot your PC.



\*Note that the Sierra Wireless GL6110 GPRS modem draws considerable USB power so if you are using an USB extension cable or you have connected another USB device that draws too much power (on some PC, power is shared across all the USB ports), the modem may also fail to work or become unstable. You may try removing other USB devices from your PC or using a powered USB hub from a reputable brand such as Belkin.

For the Maestro 3G modem, the modem COM port to use can be found under *"Ports (COM & LPT) --> Sierra Wireless AT Command Port (UMTS)"*.



b). If you are using Wavecom Fastrack Supreme, Cinterion or any serial modems, please ensure that your PC has a DB9 serial port.

If there is no DB9 serial port, please obtain a PCI DB9 serial card (Low profile PCI card is required for small

chassis PC/Server). Not all Serial-to-USB cards will work with GSM modems and some are not stable.

You will also need to insert your SIM card carefully in the correct manner – see screen capture below. **The serial modem is usually installed onto COM2 or COM1 at a baud rate of 115200bps.**

\*Note that the antenna connector on the right hand side and you should insert the SIM card such that it is facing upwards and golden metal strip nearest to the opening. If you insert wrongly, the SIM card may drop inside the chassis and you will have to use a screw driver to open the aluminum plate directly above the SIM card opening in order to take it out.

The FASTRACK Supreme has now implemented a SIM connector having a carrier with lock. This helps ensuring the user to have proper SIM card insertion and locked before proper use of GSM network.



**Warning:** If you're using a GSM modem with an attachable antenna, please exercise caution on attaching the antenna to the antenna connector. If there's a nut attached to the modem casing, please ensure it does not turn when you are connecting the antenna to the modem. Failure to do so may cause damage to the modem.

## 2). Checking SIM card.

After you have installed the Modem and the SIM card, turn on the power (for Serial modems), and check that the red or yellow light on the modem blinks after 20 seconds. If it does not blink, please check whether the SIM card is properly inserted and activated by your GSM provider – you need to call them to find out whether it is activated.

The modem may also not blink if there is weak or no network coverage for that SIM card. If network coverage is unavailable, you may try relocating the modem or change to a provider with better network coverage in that location.

**Note:** If you need to change your SIM card, before removing the SIM card, **please always turn off the power supply** or remove the power supply cable from the modem. You may reconnect the power supply after you have installed the new SIM card.

## 6. Appendix B - Troubleshooting Checklist

### 1). SIM Card is activated, Modem is setup properly and connected to the PC

First check that your SIM card is activated and you're able to send SMS using your cellphone. Next check that the modem is attached tightly to the correct PC. If you are using Wavecom modems or compatible devices, the indicator light on the modem should be blinking 15 seconds after powering up. A constant light will mean that the SIM card cannot be detected or network coverage is unavailable.

If the light fails to blink, disconnect the modem from the power source, check that you have inserted the SIM card correctly, and then reconnect the power supply, wait 15 seconds for the modem to boot up.

If network coverage is unavailable, you may try relocating the modem or change to a provider with better network coverage in that location.

Once done, restart AlertDispatcher service and proceed to step 3 to test send an SMS.

**Note:** If you need to change your SIM card, before removing the SIM card, please **always turn off the power supply** or remove the power supply cable from the modem. You may reconnect the power supply after you have installed the new SIM card.

### 2). Required Services Started, and Windows Firewall configured, AlertDispatcher Client and Service added to Windows DEP exception list (for the case of Vista/2008)

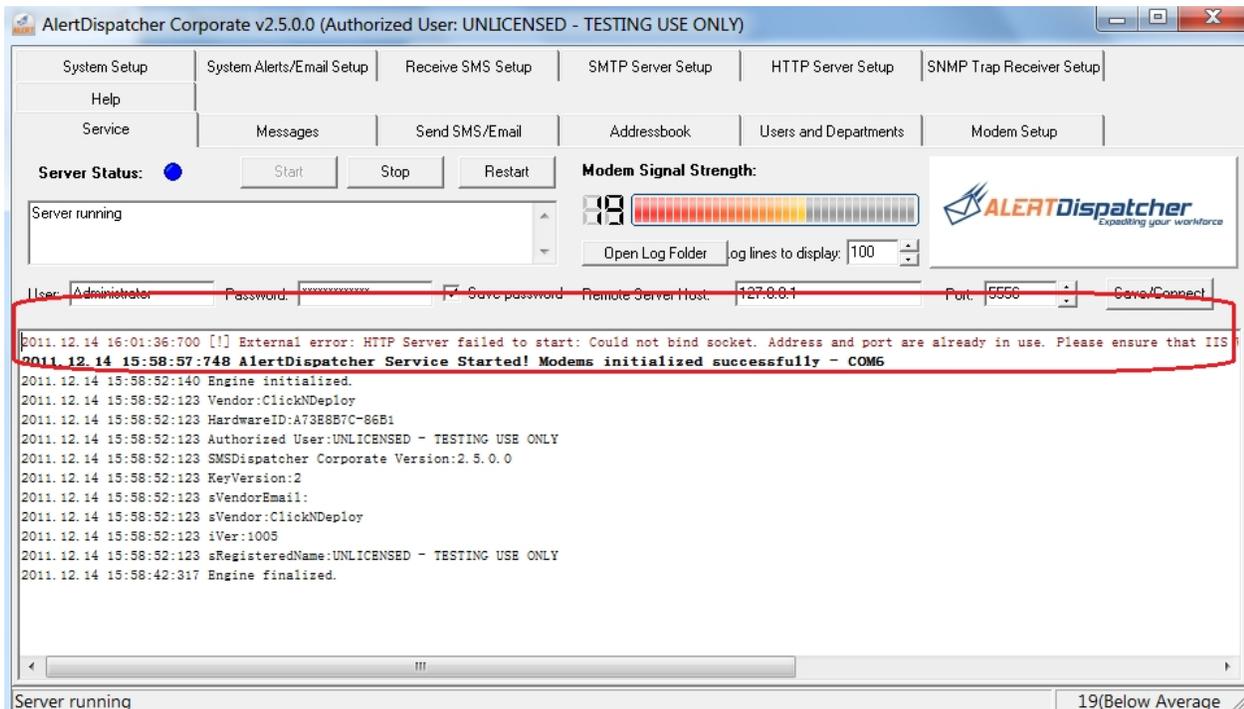
Go to *Start* → *Control Panel* → *Administrative Tools* → *Services*

Ensure that 'AlertDispatcher' has started.

If you intend to use the SMTP, HTTP, or SNMP Trap Receiver interface on AlertDispatcher, please ensure that the services 'AlertDispatcher-SMTP', 'AlertDispatcher-HTTP' and 'AlertDispatcher-SNMP' are running.



In order for these interfaces to work, there must not be conflicting services running on your system occupying the same ports. If there is a conflicting service using the same port, the following error will appear: "Could not bind to socket".



For example, for SMTP Server interface, you may check whether Windows ‘Simple Mail Transfer Protocol (SMTP)’ service exists and is set to run automatically. If yes, stop and disable the service, and then restart ‘AlertDispatcher-SNMP’ service.

For HTTP Server, ensure that Windows World Wide Web Publishing Service, or IIS isn’t running on the same port (default port for HTTP server is 80).

For SNMP Trap Receiver, if you have installed Windows SNMP Trap service, please ensure that the service is stopped or change to a different port (default port for Trap Receiver is 162).

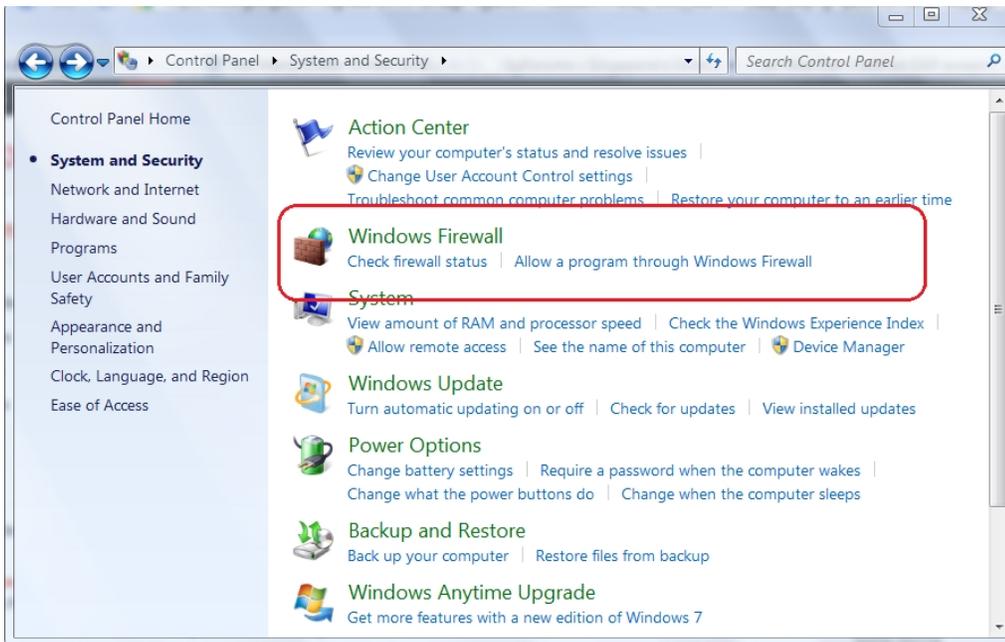
If you need to be able to access AlertDispatcher Server from the network, and there is a firewall running on your system, you must add the ports used by the services you require to your firewall list of “allowed ports”.

<i>Server Protocol</i>	<i>Default Port</i>	<i>Remarks</i>
HTTP Server	80	
SMTP Server	25	
SNMP Trap Receiver	162	
AlertDispatcher Server	5556	<i>Used by AlertDispatcher Client and DLL API</i>

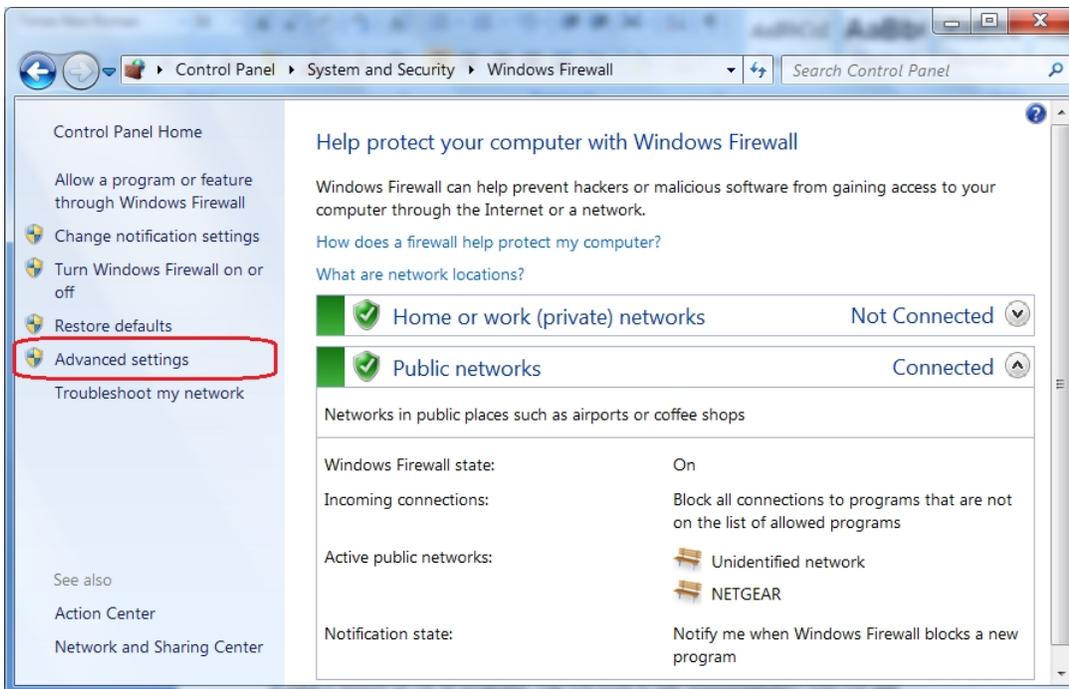
Next, we shall describe how this can be done for Windows Firewall. If you are using a 3<sup>rd</sup> party firewall, check with your IT administrator or the firewall vendor.

To add ports to Windows Firewall exception list:

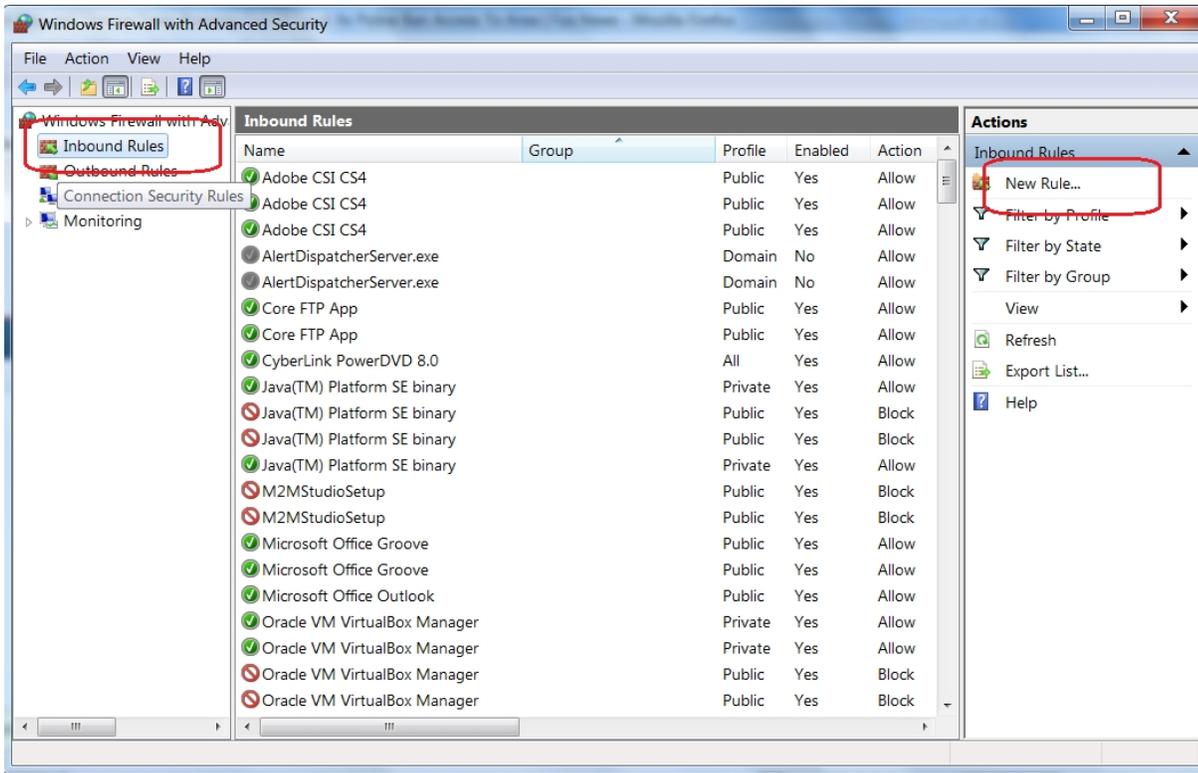
Go to *Start* → *Control Panel* → *Windows Firewall*.



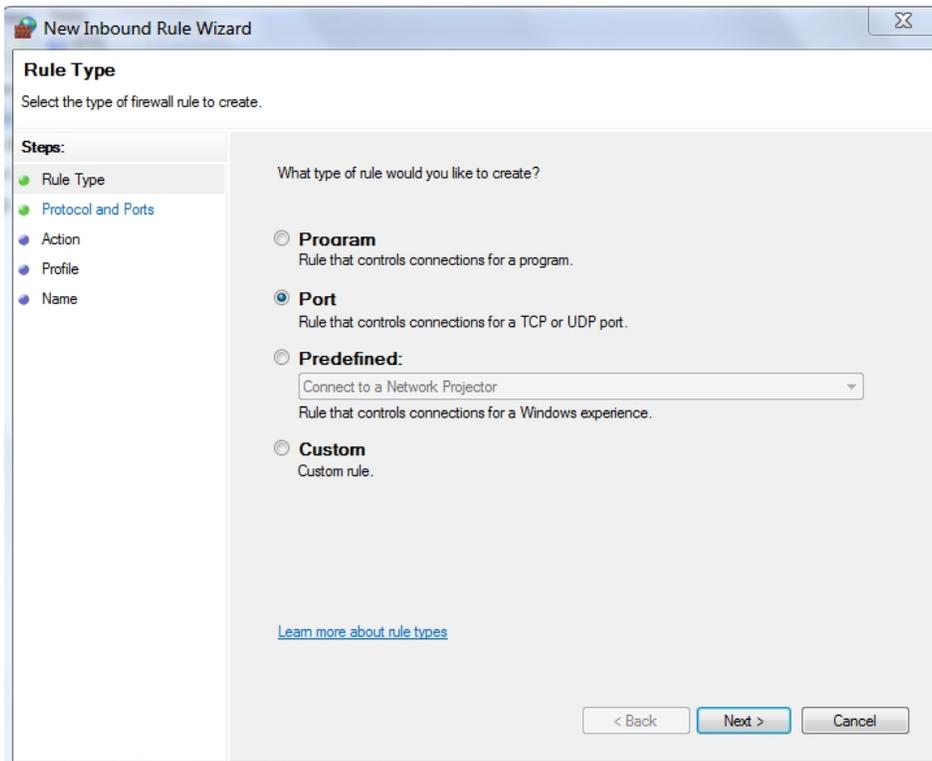
Click “Advanced settings”.



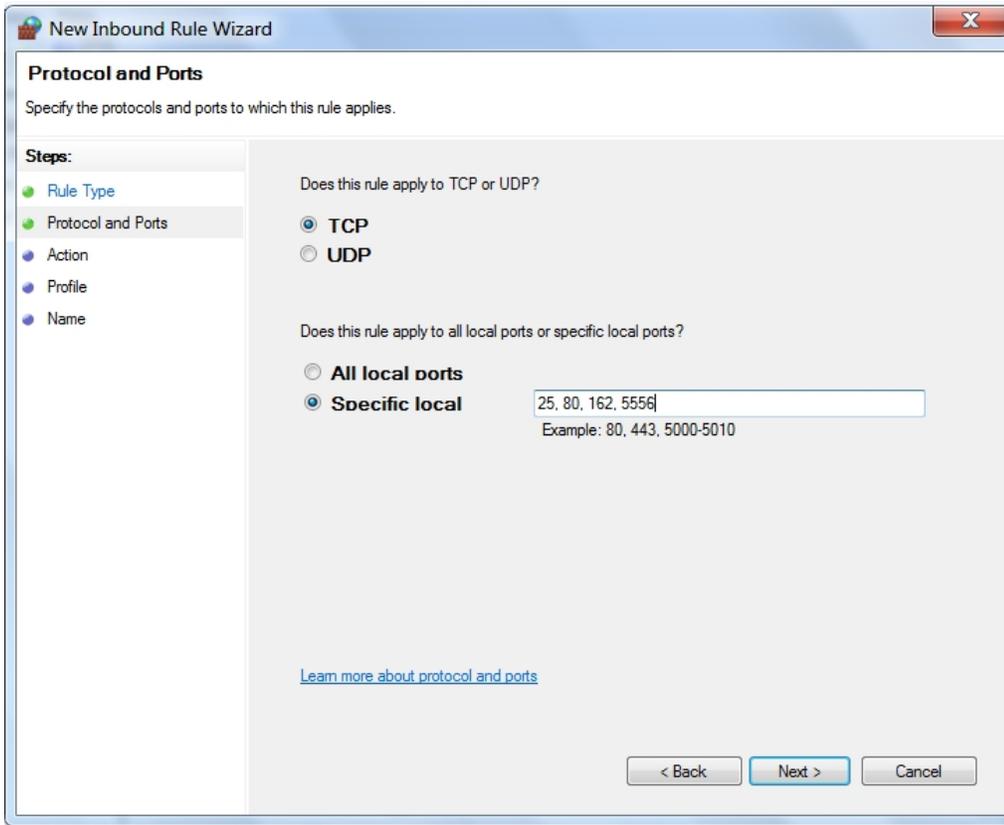
Click Inbound Rules, followed by “New Rule”.



Toggle “Port”, click Next.



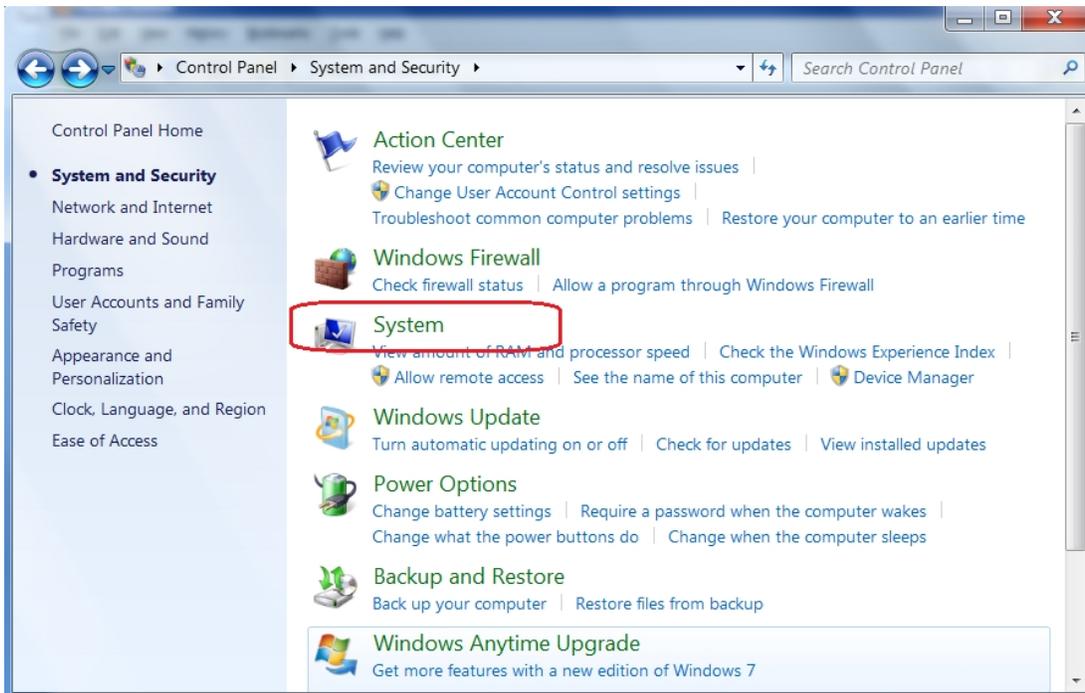
Under “Specific local”, enter “25, 80, 162, 5556” or any other ports you wish to use.



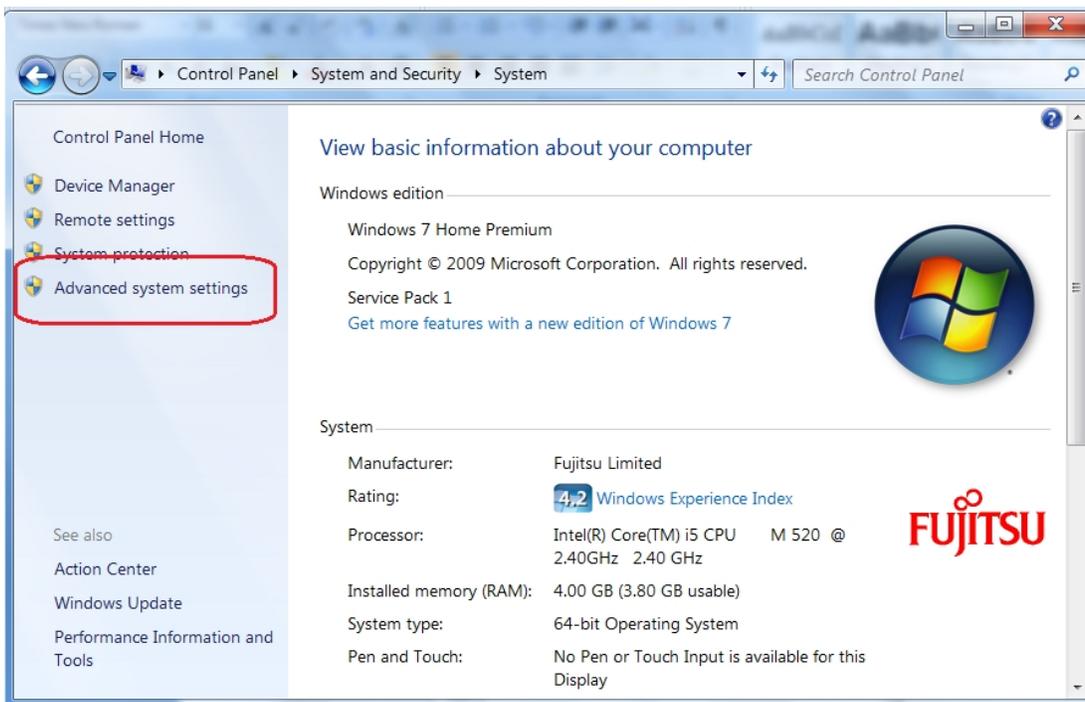
If DEP is turned on for all programs, you will need to add AlertDispatcherClient.exe and AlertDispatcherServer.exe to the exception list. This is usually done automatically by the installer when you install AlertDispatcher for the first time.

**Note:** For Windows 2008, DEP is turned on for all programs by default so this step is essential for Windows 2008.

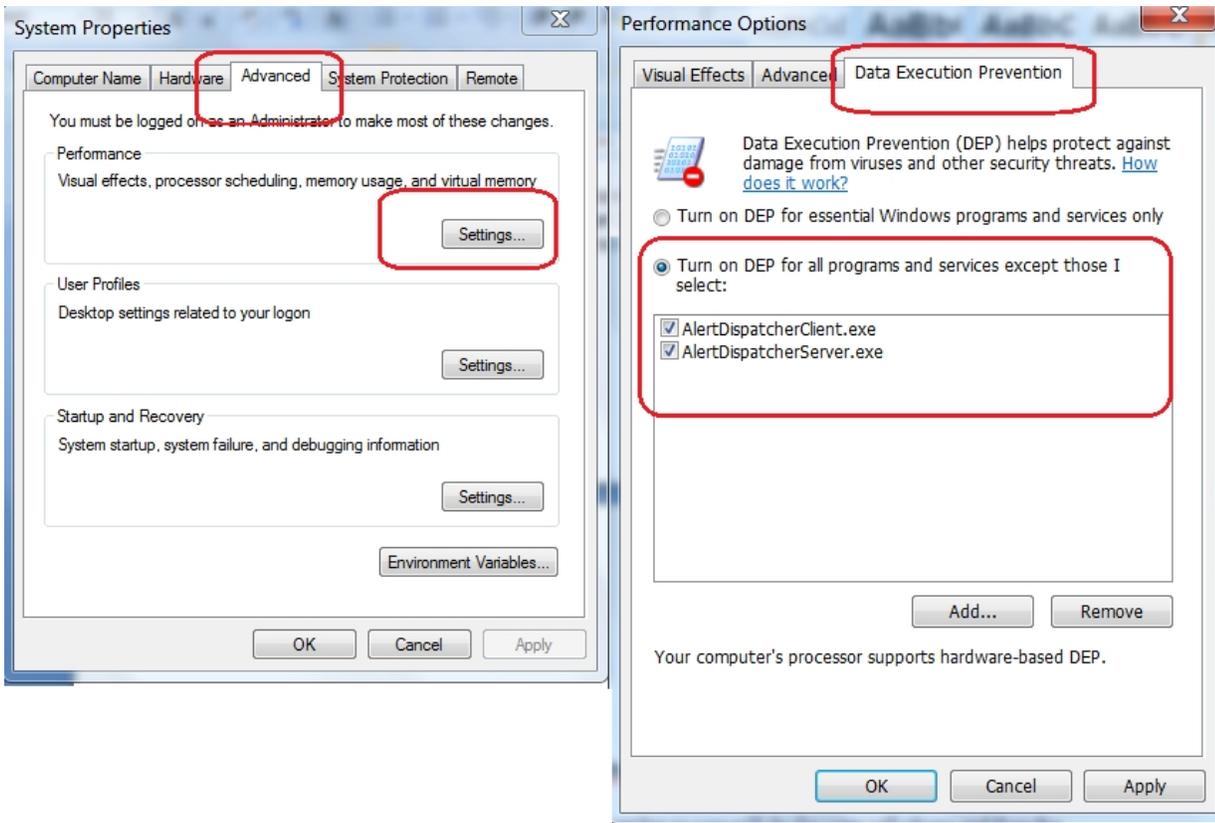
Go to Start → Control Panel → System



Click “Advanced system settings”, “Advanced” tab, followed by “Data Execution Prevention” tab.

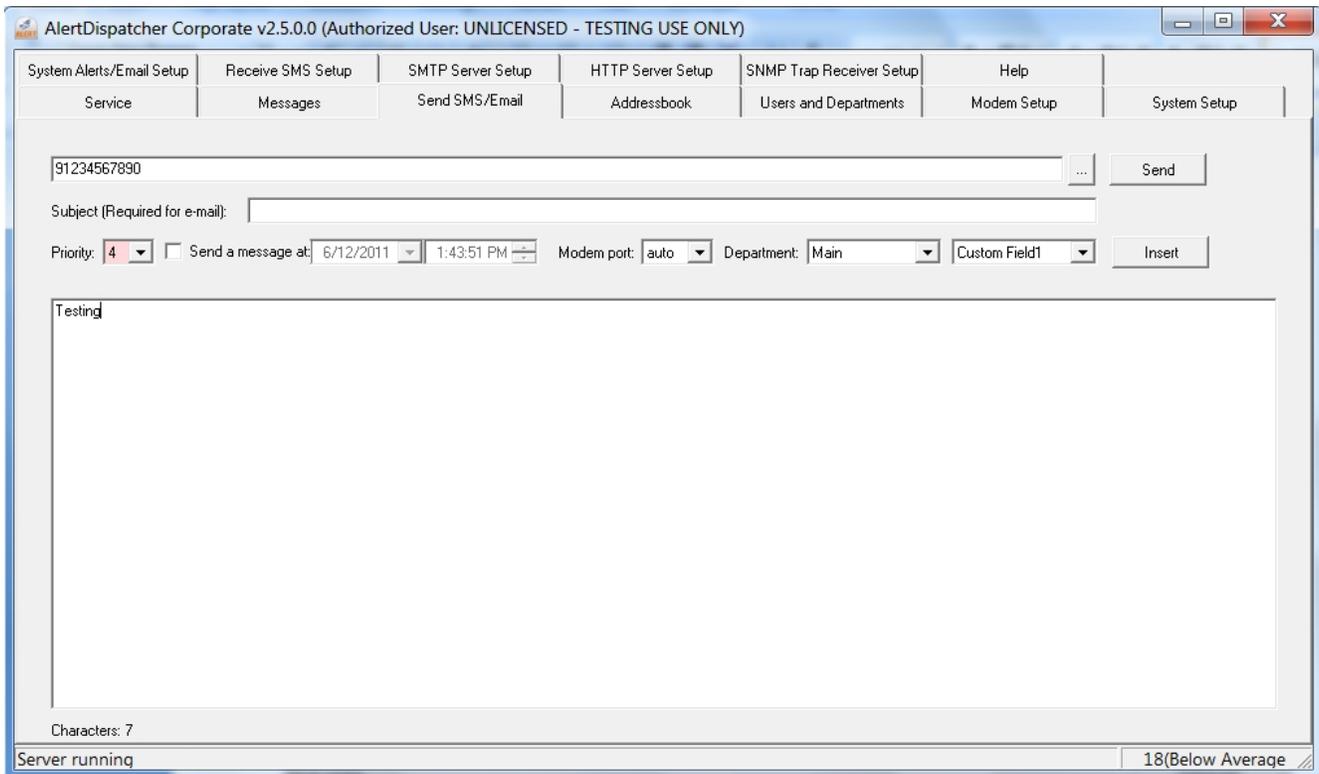


If the radio button for “Turn on DEP for all programs and services except those I select:” is checked, please add C:\Program Files\AlertDispatcher\AlertDispatcherClient.exe and C:\Program Files\AlertDispatcher\AlertDispatcherServer.exe to the exemption list.

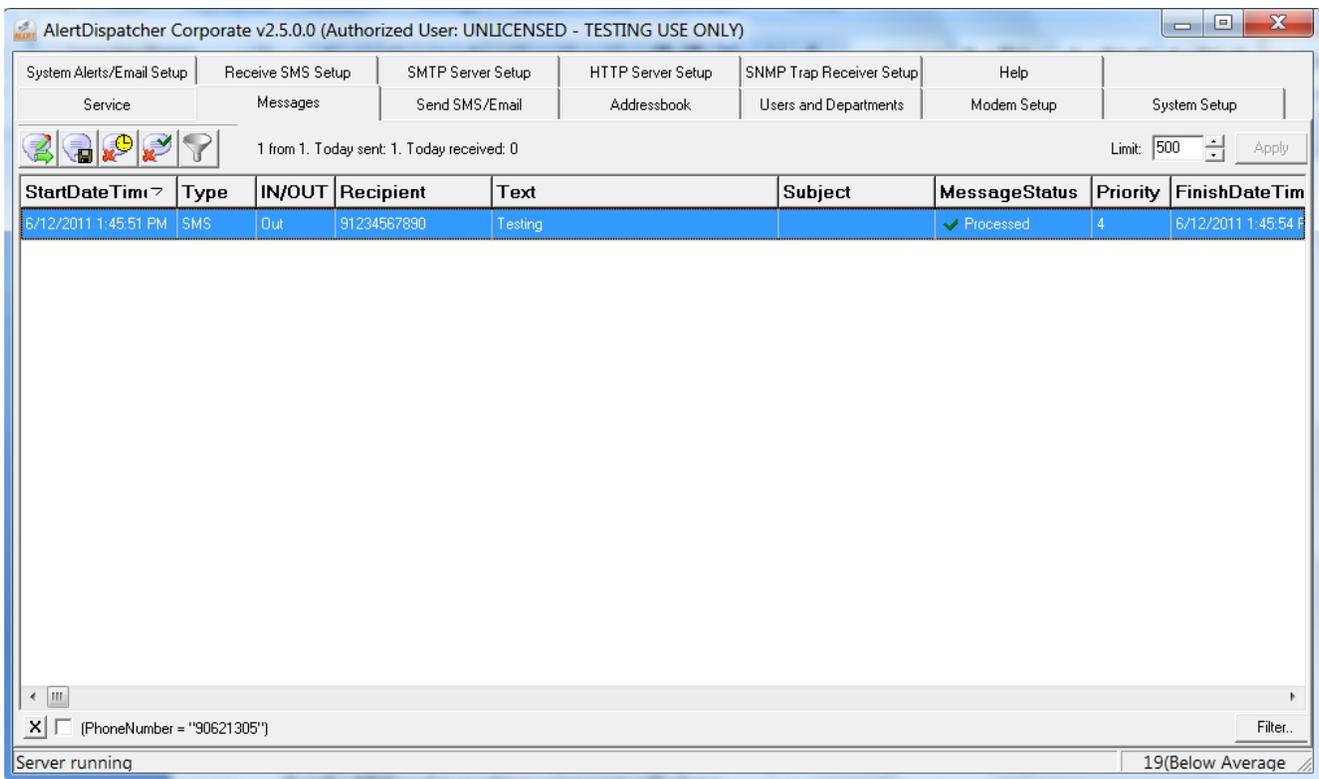


### 3). Send test SMS using AlertDispatcher

Go to 'Send SMS/Email' Tab, type in your phone number as you will do for your cell phone and then the message. Click 'Send'.



If the phone number is correct and the modem is working, you should get the following screen. If not, verify that the SIM card is working using your cell phone.

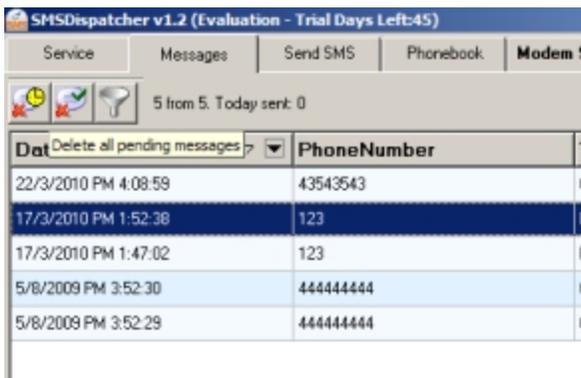


## 7. Appendix C - FAQ and Tips

**1). Question: I do not know how to pause and delete the SMS that I send wrongly.**

**Solution:**

Use the  'Delete all pending messages' to clear the inbox of pending messages.



**2). Question: Where do I find the server and activity logs?**

**Solution:**

They can be found under C:\Program Files\AlertDispatcher\Log.

**3). Question: My modem is connected but I can't send SMS?**

**Solution:**

First stop AlertDispatcher Service. Then disconnect the modem power supply, check that the SIM card is properly inserted, connect the modem power supply, wait 15 seconds, start AlertDispatcher Service, try again.

If this fails, refer to ['Appendix B - Troubleshooting Checklist'](#).