

AlertDispatcher v7.0

How-To Guide

Last update: 1 May 2026

Table of Contents

1. For End User

1). How to Launch AlertDispatcher Client

After you have installed AlertDispatcher, launch the Client from Windows Desktop.

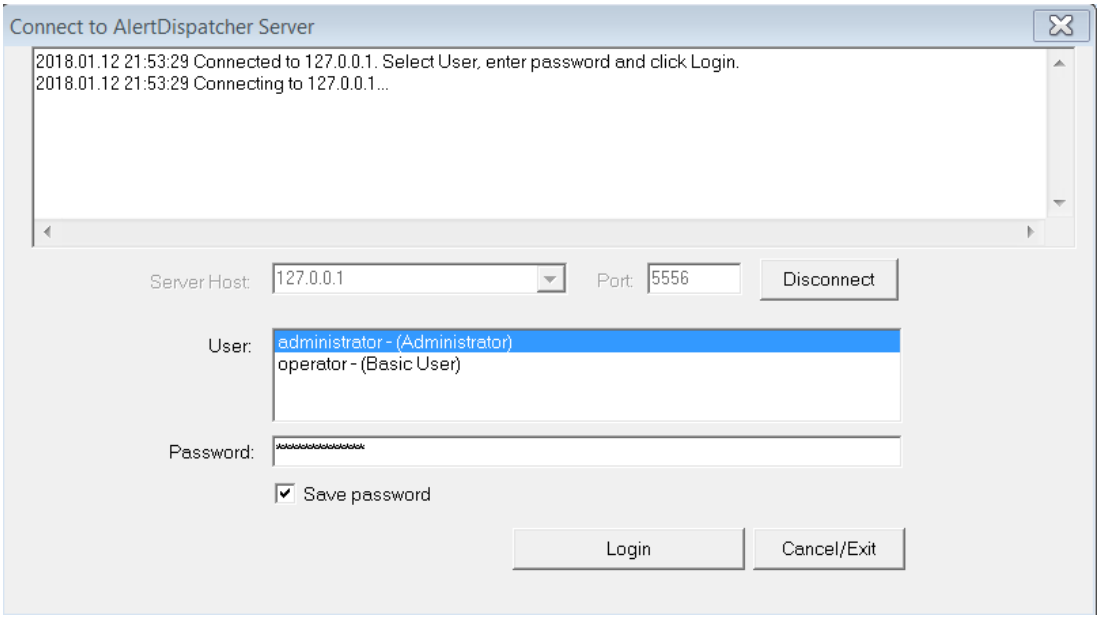
Note: AlertDispatcher Client is only used to configure and manage AlertDispatcher Server. AlertDispatcher Server works as a background service and starts automatically when you boot up your server. You do not need to keep the Client open after you have finished using it.

Select User and enter Password to login. The following users are created by default,

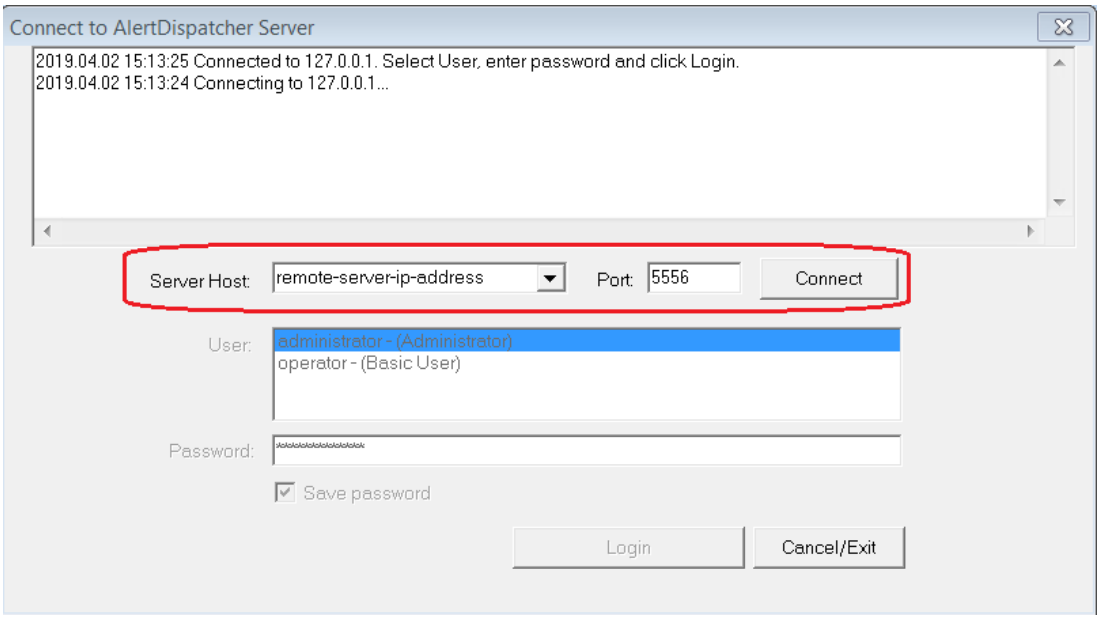
1. administrator user: *'administrator'*, password: *'alert123'*
2. basic user: *'operator'*, password: *'operator'*

An administrator user has full rights while a basic user can only view, send messages and can't delete any message or manage the address book. You are advised to change the administrator user password as soon as possible. The default password for *'operator'* is *'operator'*.

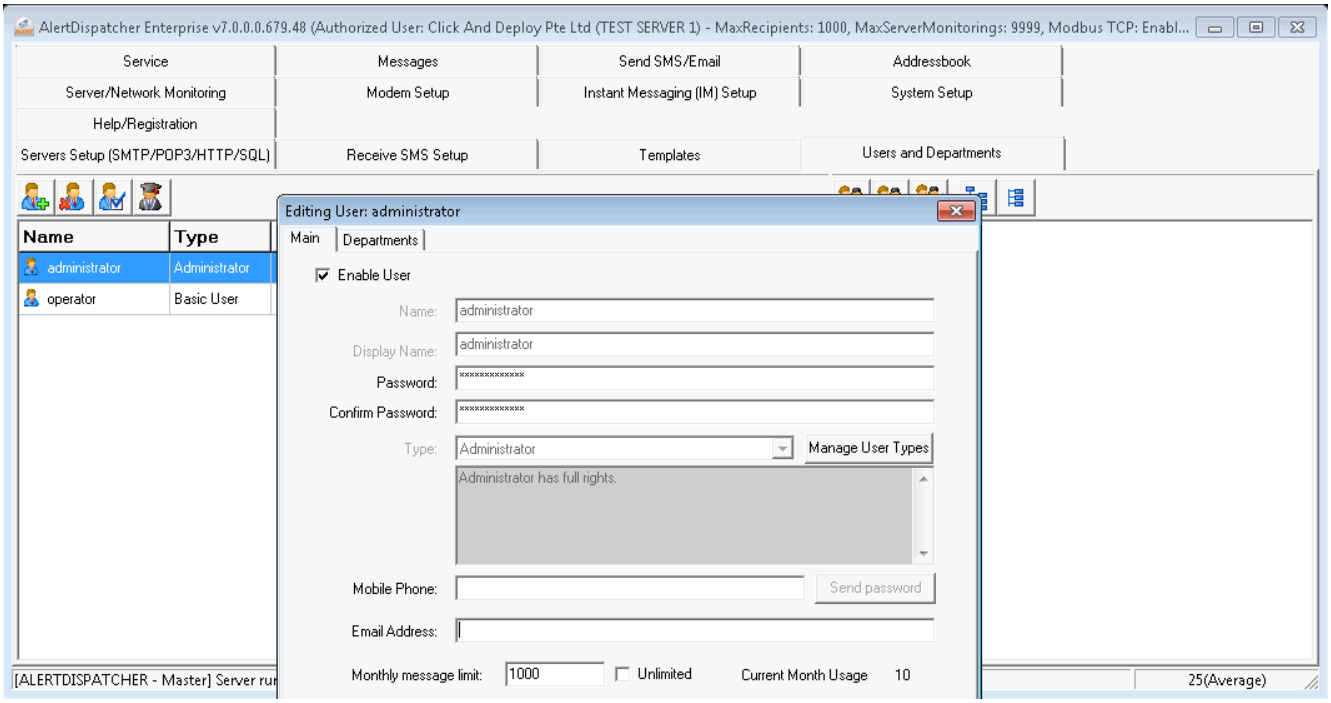
For better security, uncheck "Save password" so that the next user will have to enter password to login.



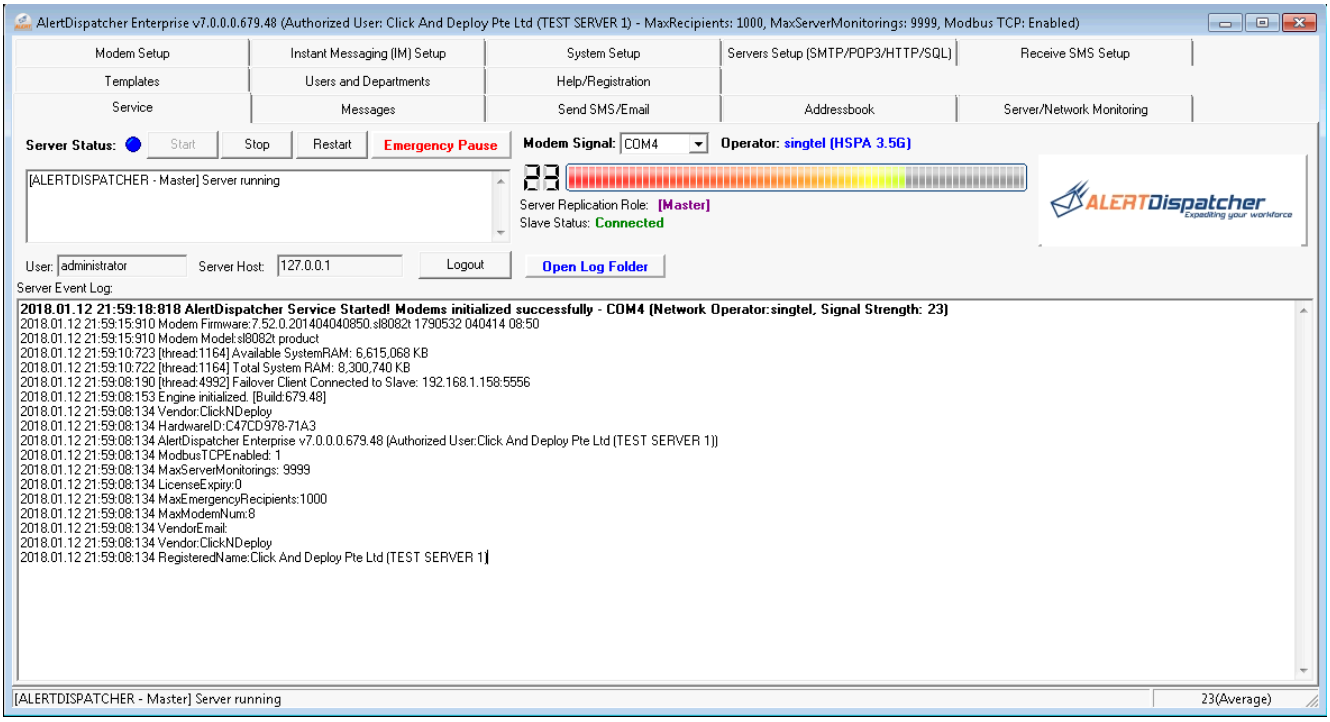
Note: If you're using Corporate or Enterprise License, you can install and connect AlertDispatcher Client to a remote AlertDispatcher Server. If the remote AlertDispatcher server has firewall enabled, then you may need to configure the firewall to "allow" incoming requests to AlertDispatcher TCP port 5556. Refer to Appendix A - How to Add (allow) server ports to Firewall.



Note: You can create new users and change passwords under "Users and Departments" tab.



After successfully login, you will see the following screen.

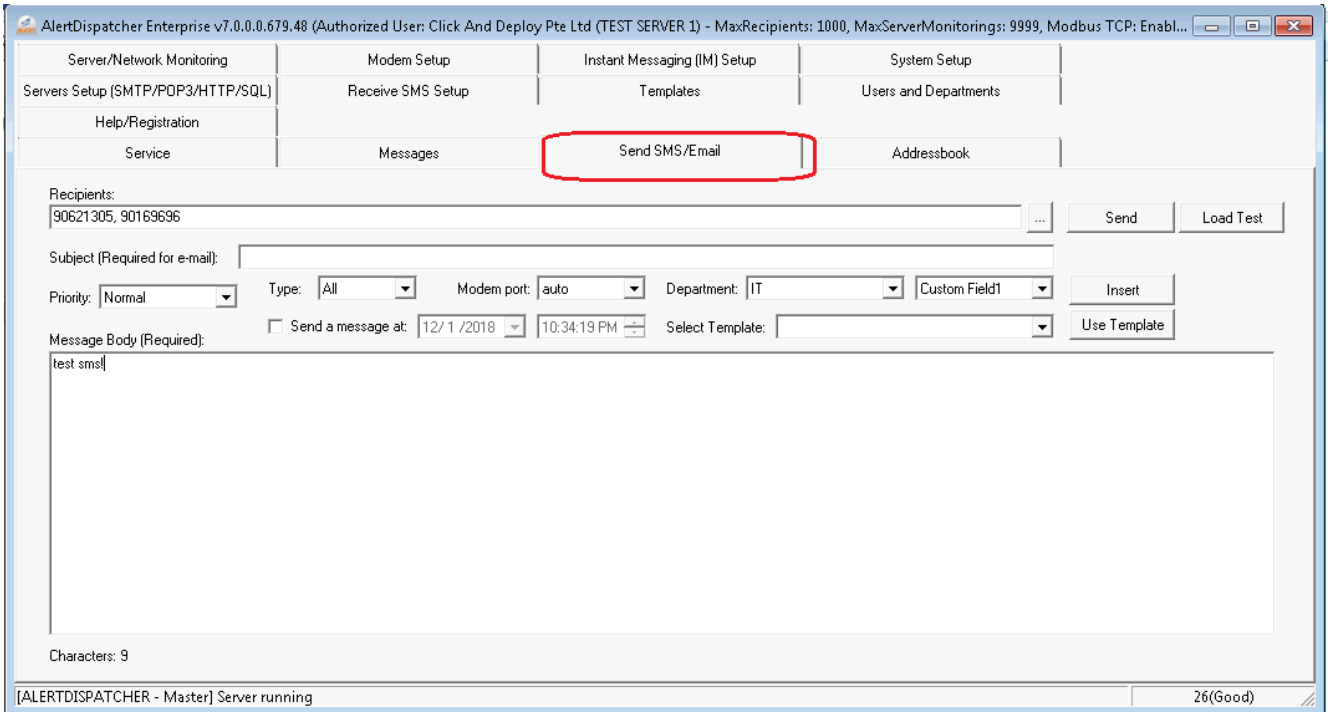


2). How to Send Test Message, Check Status and Troubleshoot Message Failures

a). Sending Test Message from AlertDispatcher Client

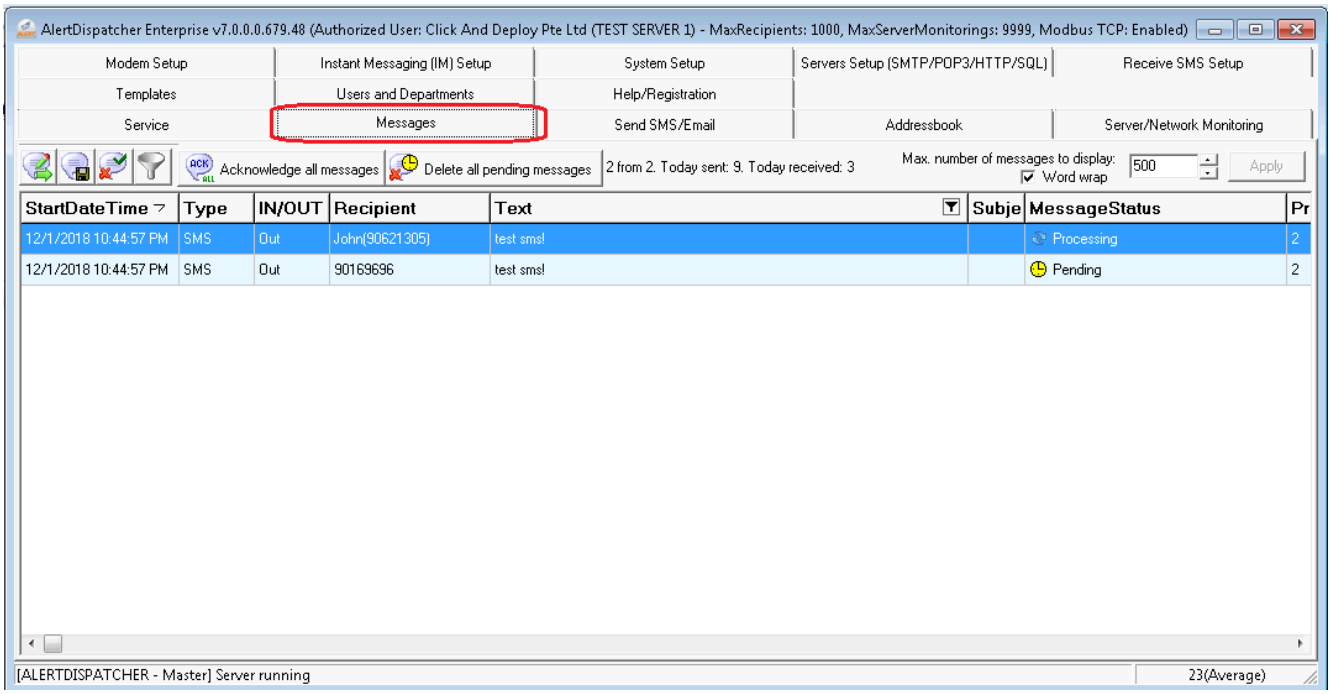
Navigate to the “Send SMS/Email” tab. Click on the “Send” button to send the message to yourself. If there's a backlog of messages that hasn't been sent, you may set your message Priority to "Important" or "Urgent" to bypass any pending message with a Normal priority.

Note: You only need to add the + country code sign unless you’re sending to a foreign number.



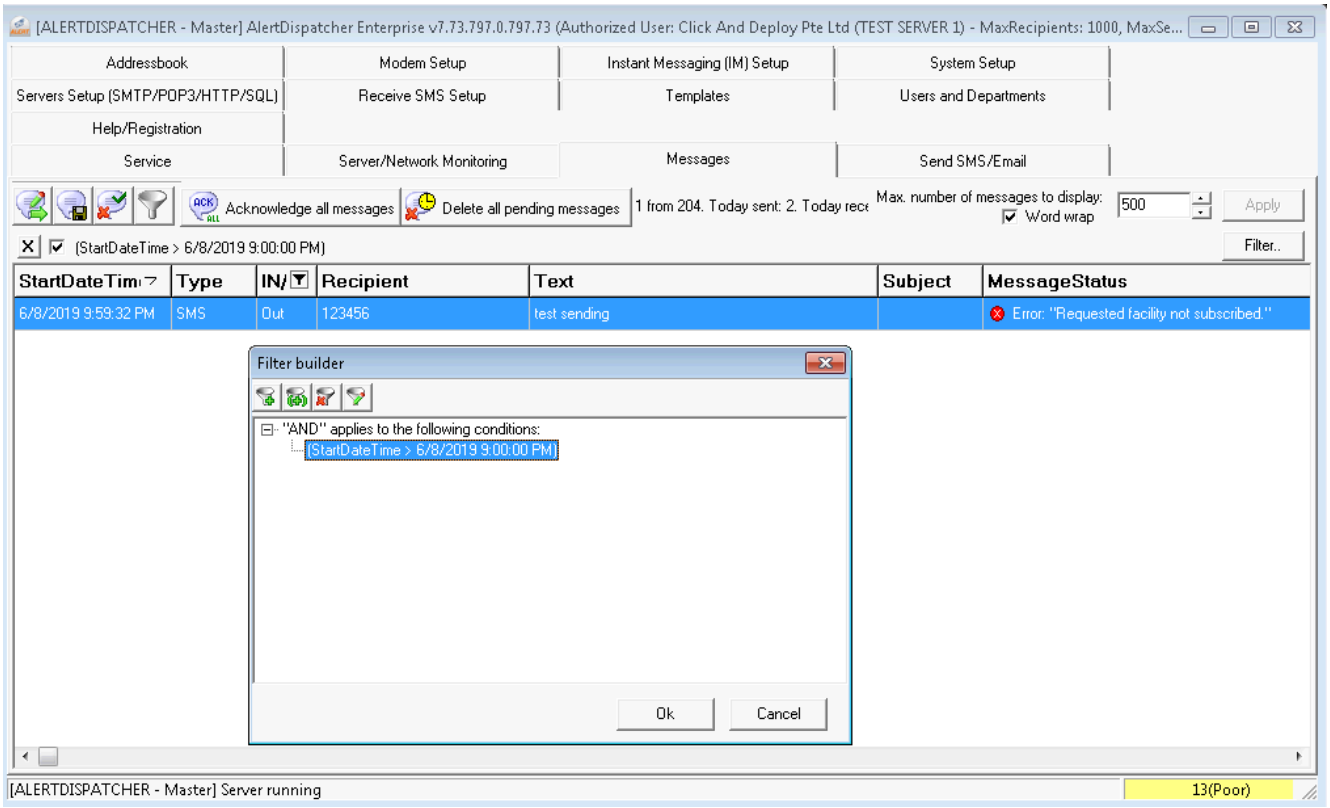
b). Checking Message Send Status on AlertDispatcher Client

Navigate to the “Messages” Tab to check the status of your sent message. The "MessageStatus" column will indicate whether the message is sent or not sent. "Processed" means the message has been successfully sent out. Any send error will be display under "MessageStatus" and will be critical for troubleshooting.



If you can't find your message, you may use the filter button to filter by date and time range and adjust the Max. number of messages to display setting.

Refer to AlertDispatcher logs to see details of errors - [5). How to Retrieve Logs for Troubleshooting]

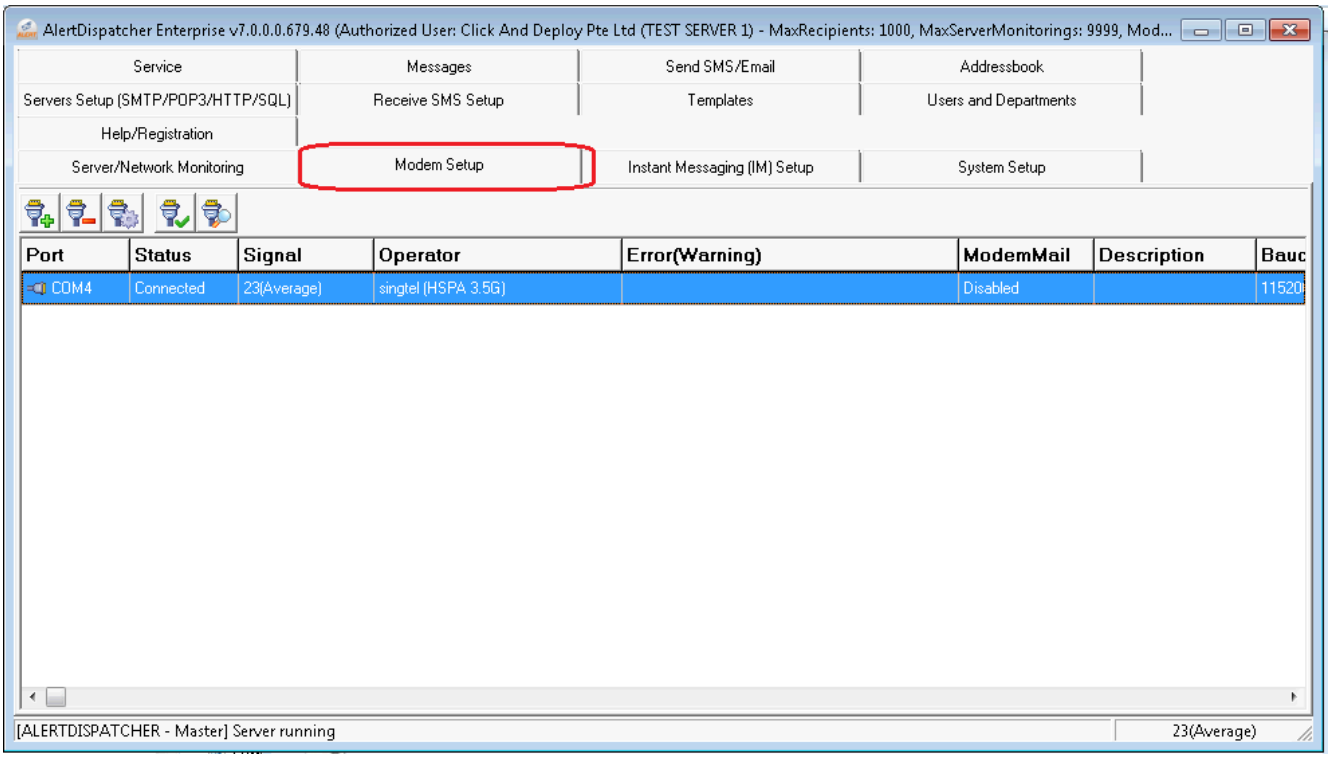


c). Troubleshooting Send SMS/Email and Modem/SMTP Server Issues

For email to be sent out, a valid and working SMTP Server has to be configured. Refer to 2). How to setup AlertDispatcher to send Email/Alert Emails

For SMS to be sent out, a working modem needs to be configured. If the SMS can't be sent, go to "Modem Setup" and check if the modem is connected, and there is a signal and operator detected. The LED light on the modem must be on and the SIM card properly inserted. Note that some SIM card adapters may not fit well so you may try changing to another SIM card to try out.

Warning: Please read the modem installation guide for the modem you're using before installing/uninstalling the modem /modem driver or when installing/uninstalling the SIM card - http://www.clickndeploy.com/clients/downloads.php?action=displaycat&catid=19

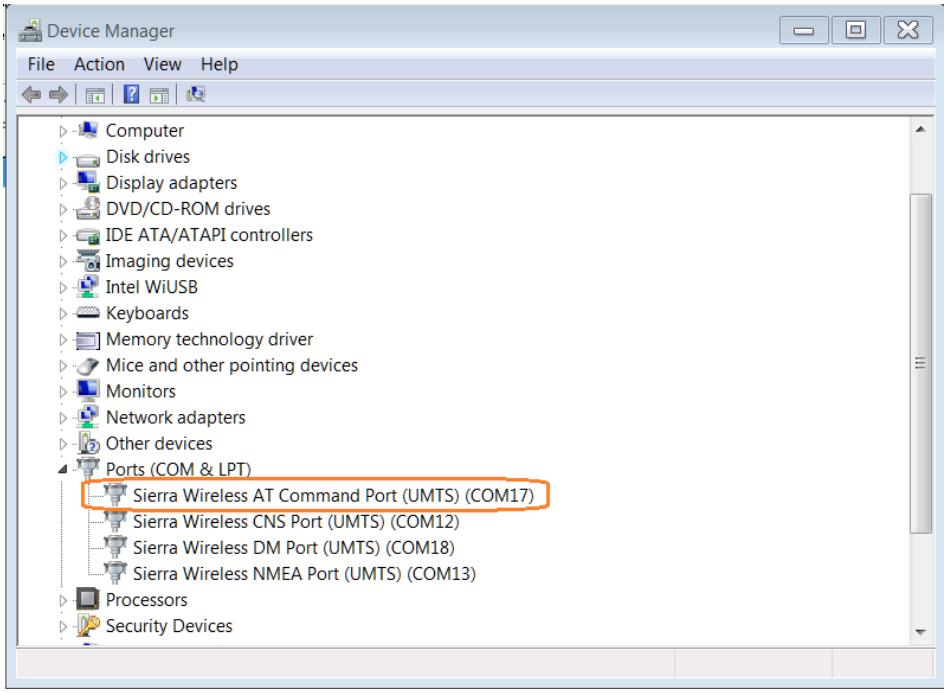


A modem may not be detected due to mis-configured COM port or if the modem driver has not been installed for the modem device.

Go to "Windows Device Manager" and locate the modem device. In the following example, the modem port is COM17. After reconfiguring the modem COM port, it may take up to 30 seconds for the modem to be detected.

If the modem device is "unknown", ensure you have installed the correct USB driver for the modem and right click on the device and select "Update driver software".

Warning: Please do not make any amendments to the Modem Setup unless you know what you're doing!



Under certain conditions, a weak GSM signal may cause SMS messages to fail to send. The GSM signal strength and quality at your deployment location is dependent on the presence of GSM repeaters in the vicinity. Generally speaking, GSM signal will be better in offices than in industrial buildings and data centers, and is especially poor in basements and server rooms enclosed by reinforced concrete walls with fire-rated doors and no windows. If your deployment site has very poor signal, please refer to point 2 and 3.

You can use your cellphone to gauge the signal strength. There should at least be 2 bars. Alternatively, you can also compare the signal strength for various SIM card providers using the software – signal strength will be displayed under Modem Setup and the signal reading will refresh every 20 seconds.

If the signal is very poor at your selected location (1 bar on your cellphone), please consider shifting the entire setup to another location. If you're installing the modem in an enclosed rack, extend the antenna out of the rack. You also may use an "active" USB extender to extend the modem to a location with better signal - click here for an example.

If you're still not able to send your message, contact your mobile carrier company for technical assistance.

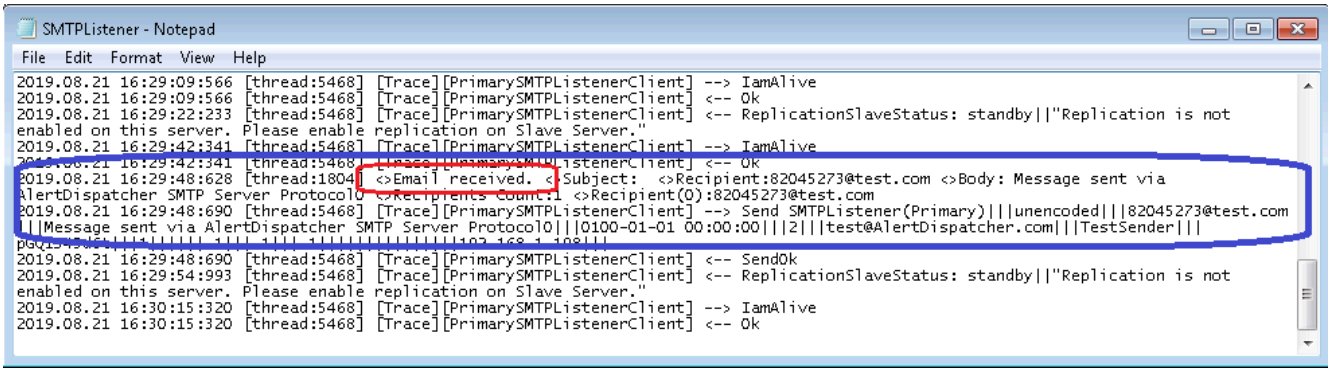
d). Troubleshooting Messages Sent From Third Party Systems

Third party systems (interfacing clients) can interface with AlertDispatcher using the following server protocols:

Server Protocol	*Message Format*	*Default Port*	*Windows Service Name*	*Log Name*
1. HTTP Server 2. SMTP Server 3. SNMP Trap Receiver 4. AlertDispatcher DLL API	HTTP Request SMTP Email SNMP Trap N.A.	80 25 162 5556	AlertDispatcher-HTTP AlertDispatcher-SMTP AlertDispatcher-SNMP N.A.	HTTPListener.log SMTPListener.log SNMPTrapReceiver.log N.A.

For example, for SMTP Email messages sent to AlertDispatcher SMTP Server, you can search the corresponding log file, SMTPListener.log for the keyword "Email received" and find your messages.

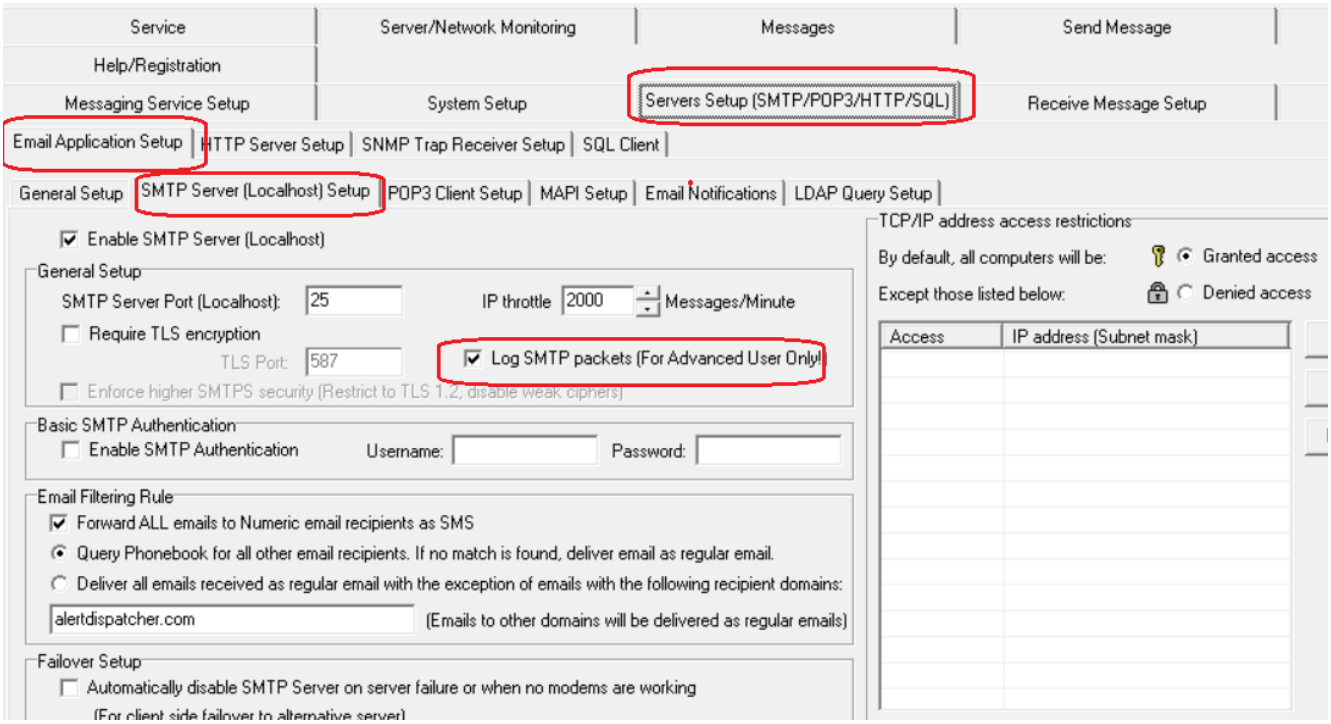
Log location: *C:\Program Files (x86)\AlertDispatcher\Log*



If you can't find the message in SMTPListener.log, check if firewall is enabled on your AlertDispatcher PC and if so, you need to add firewall exception - see A. How to Add (allow) server ports to Firewall

For hardware or switch based firewalls, please check your network administrator.

Note: The default SMTPListener.log will only show messages that have been successfully captured from the third party system. If the SMTP transaction fails halfway, it will not be captured. For detailed SMTP logging, please enable "Log SMTP packets (For Advanced User Only!)" under "Servers Setup", "Email Application Setup", "SMTP Server (Localhost) Setup" and click "Apply settings". This will allow all SMTP packets sent by your application to be captured regardless of whether they are successful.



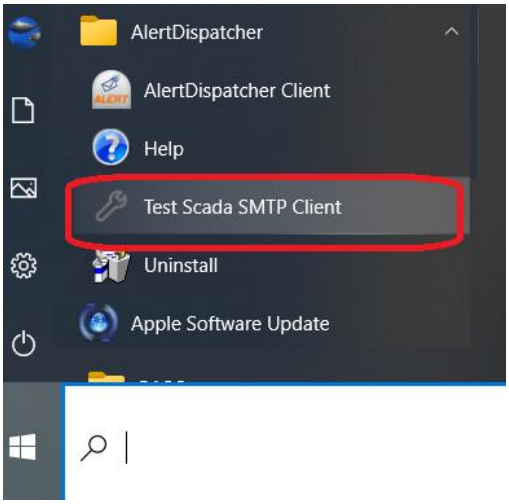
Here is what the SMTPListener.log looks like after "Log SMTP packets" has been enabled.

If AlertDispatcher is still not getting the messages sent to it after disabling firewall/ports, you can test independently of your system using 3rd party SMTP clients.

There are 2 options - Option 1 uses the Test SCADA SMTP Client which is installed by default along with AlertDispatcher by the setup is the easiest. Option 2 is to use a Telnet client to issue manual SMTP commands to AlertDispatcher. You can use both options if required.

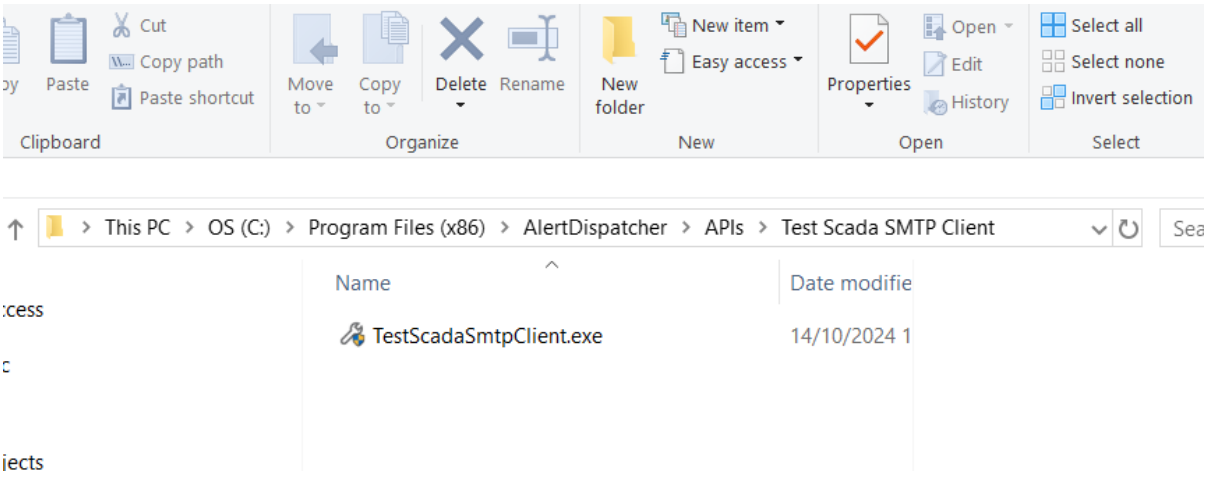
i. Option 1: Test sending SMTP mail to AlertDispatcher using "Test SCADA SMTP Client"

You can simulate the SMTP message using the "Test SCADA SMTP Client" that is installed by default along with AlertDispatcher (if it's missing, it's possible excluded during the setup). You can launch the Test SMTP Client from Windows Start Menu → AlertDispatcher → Test SCADA SMTP Client.



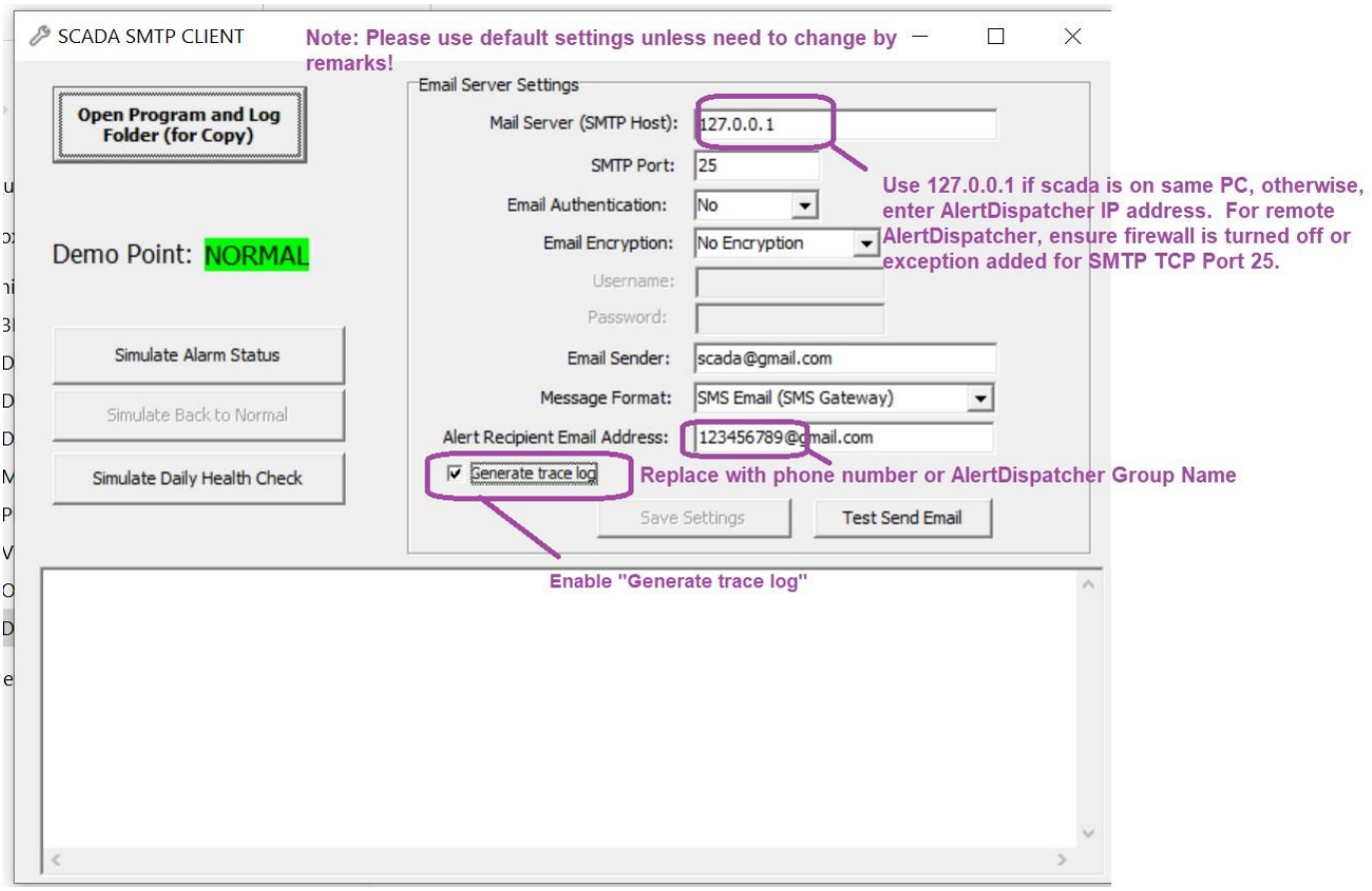
If the "Test SCADA SMTP Client" is missing from the Windows Start Menu, please go to "C:\Program Files (x86)\AlertDispatcher\APIs\Test Scada SMTP Client" and run it directly.

If the third party system is not on the same server as AlertDispatcher, it is also advisable to copy the Test SCADA SMTP Client to the same machine as the third party system after you have performed the local test. This is to determine if firewall settings or networking is the issue.



You can also download the Test SCADA SMTP Client from this link - https://www.clickndeploy.com/clients/dl.php?type=d&id=48

After you have launched the test SMTP Client, configure using the settings as shown below.

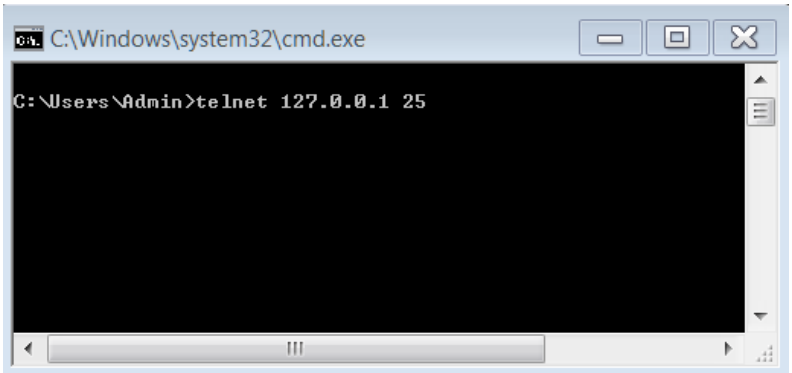


ii. Option 2: Test sending SMTP mail to AlertDispatcher using Telnet Client

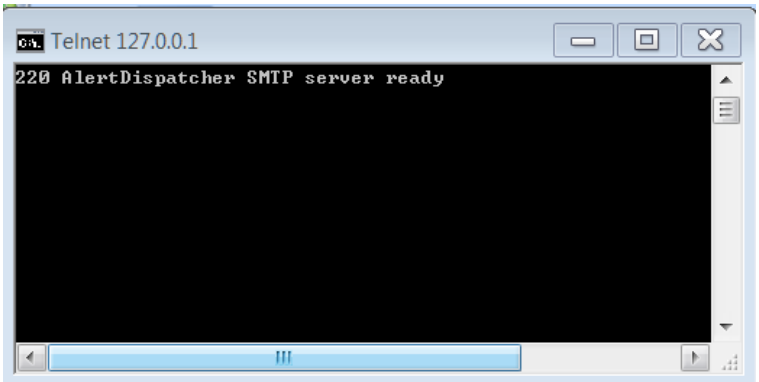
Option 2 is to use a Telnet Client such as the Windows Telnet Client to issue manual SMTP commands to AlertDispatcher. You can test locally first, and then remotely Also see - b). How to verify your SMTP Server credentials using Windows Telnet Client and Blat.

The example shown below shows a local test to 127.0.0.1 port 25. This is assuming your AlertDispatcher is locally. If AlertDispatcher is installed remotely, please replace 127.0.0.1 with the server name or IP address.

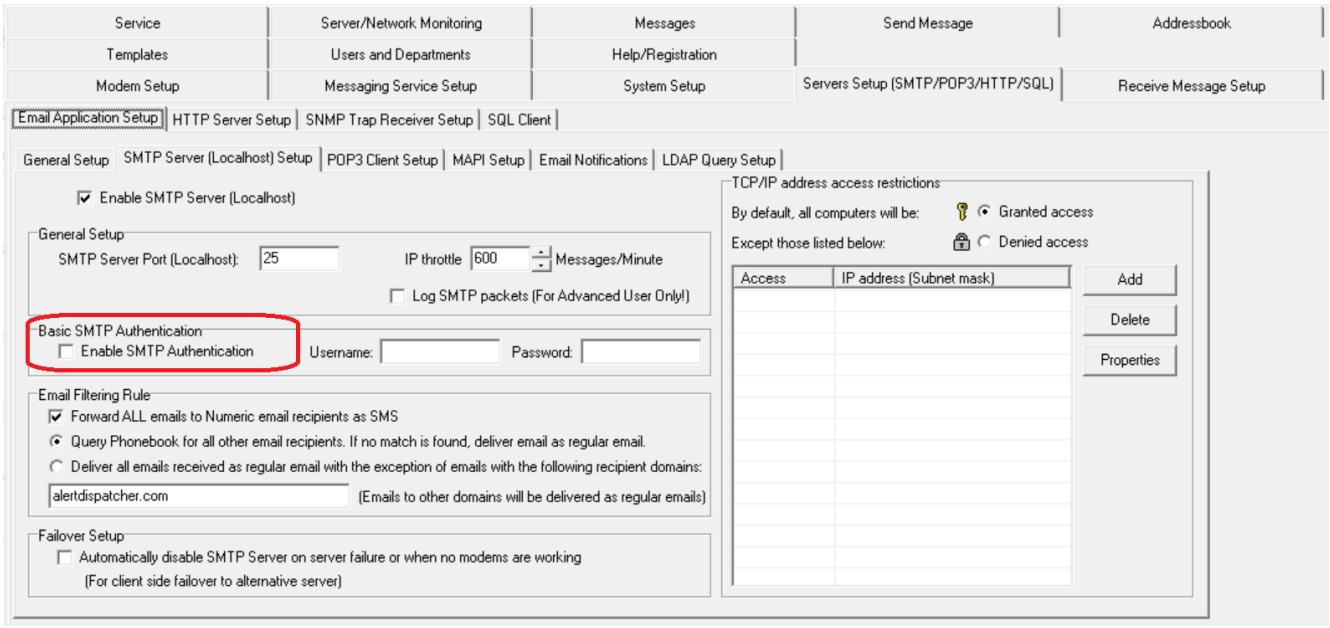
Note: The Telnet Client test only works for TCP port 25. It will not work if you have enabled TLS encryption for AlertDispatcher SMTP Server (using port 587).

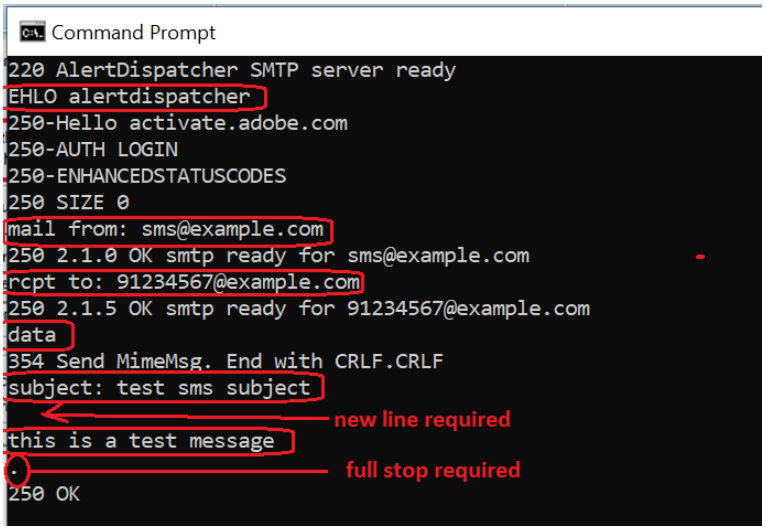


If you get "220 AlertDispatcher SMTP server ready", this means the SMTP port is open and you will be able to send email to AlertDispatcher SMTP server.



You can use Telnet Client to send email to AlertDispatcher SMTP server using the commands marked in red. If Basic SMTP Authentication is enabled, please temporarily disable it for this test.



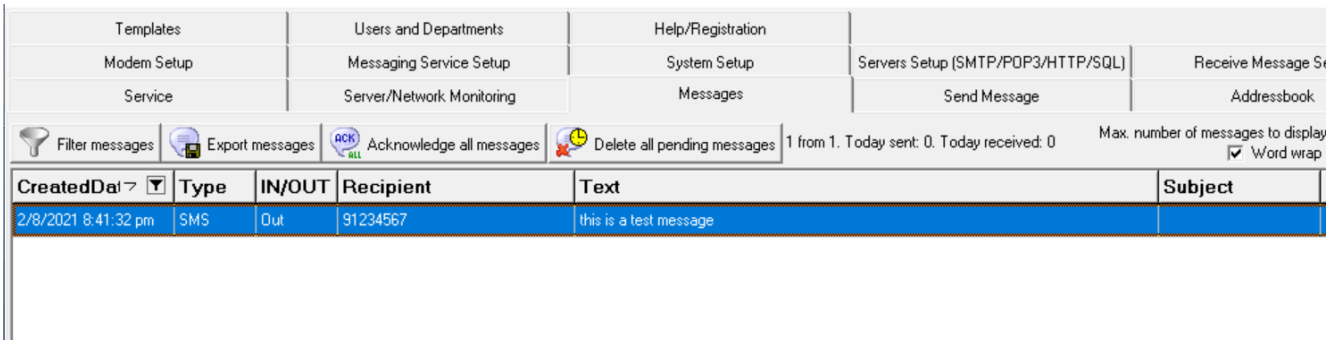


"250 OK" response means that the email is successfully sent.

EHLO alertdispatcher
mail from: sms@example.com
rcpt to: 91234567@example.com → *replace "91234567" with your mobile number*
data
subject: test sms subject

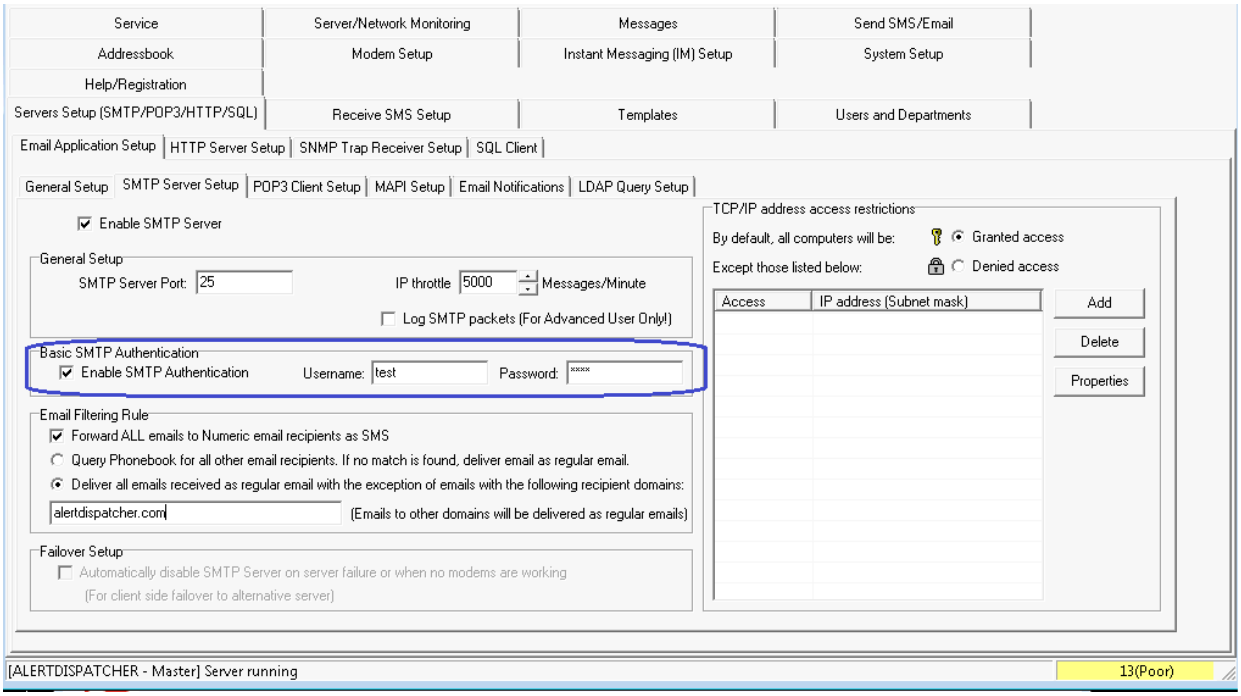
this is a test message
.

The email will appear in AlertDispatcher as shown below.

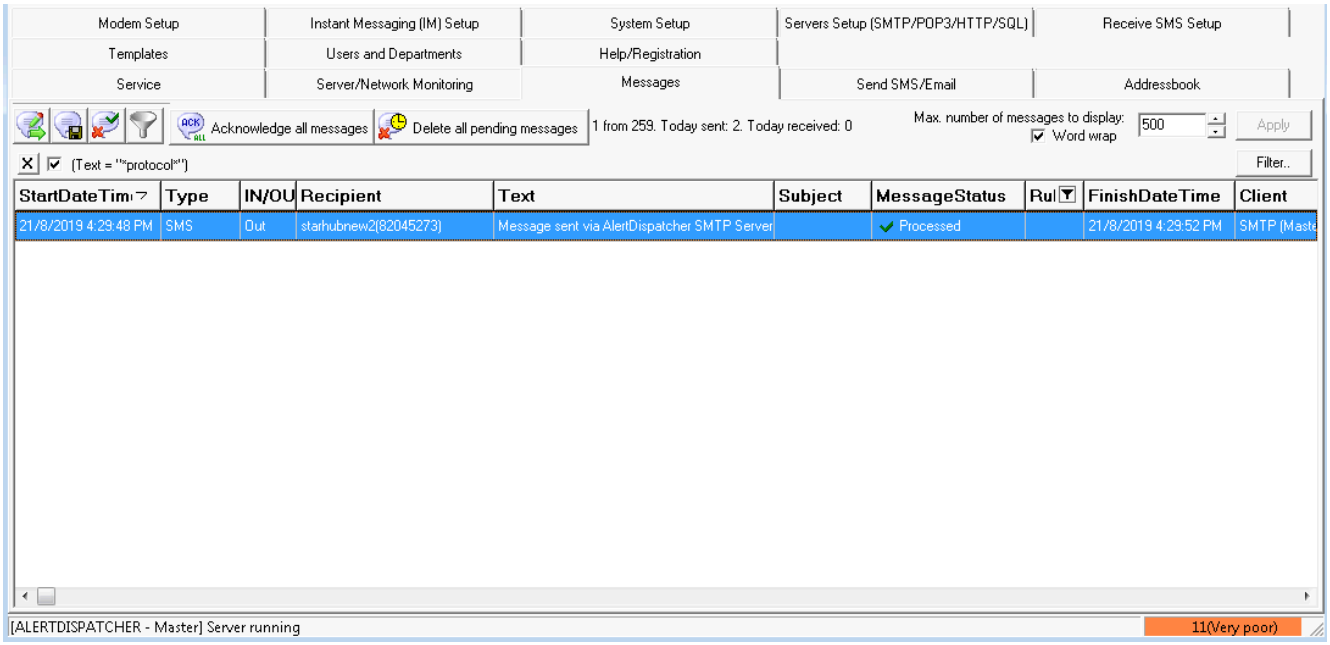


If Option 1 and 2 are both working, and there is no issue with firewall or network access, please check SMTPListener.log (with "Log SMTP packets" enabled) and also the interfacing 3rd party system logs for further clues on why the message hasn't been transmitted.

Please note that if SMTP authentication username and password is enabled on the 3rd party interfacing system, you need to configure the same for AlertDispatcher. Note: To allow quick interfacing, basic authentication is disabled on AlertDispatcher by default.



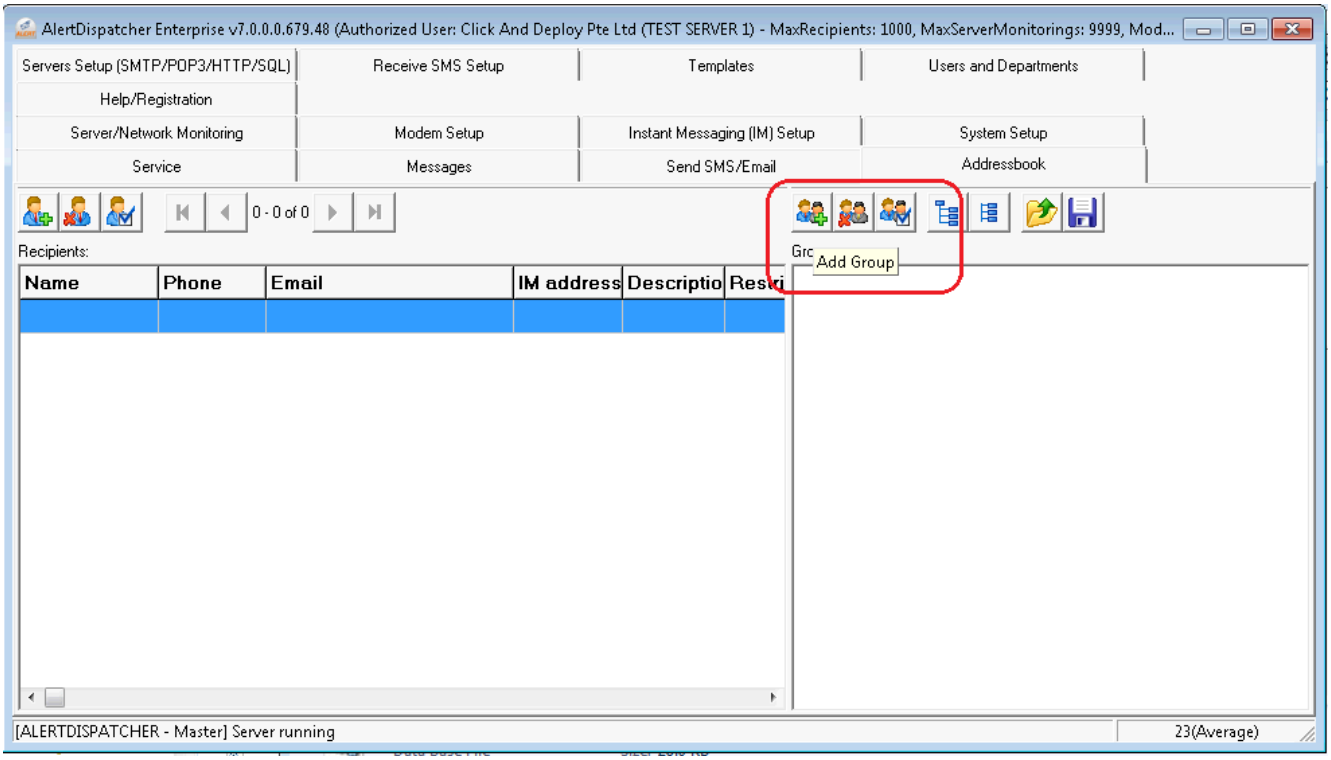
Once AlertDispatcher successfully receives the email sent from interfacing system, it will be reflected on AlertDispatcher Client. Note that this will happen regardless of whether the message can be successfully processed by AlertDispatcher.


Modem Setup
Instant Messaging (IM) Setup
System Setup
Servers Setup (SMTP/POP3/HTTP/SQL)
Receive SMS Setup
Templates
Users and Departments
Help/Registration
Service
Server/Network Monitoring
Messages
Send SMS/Email
Addressbook
Acknowledge all messages
Delete all pending messages
1 from 259. Today sent: 2. Today received: 0
Max. number of messages to display:
500
Apply
Word wrap
(Text = '*protocol*')
Filter..
StartDateTim
Type
IN/OU
Recipient
Text
Subject
MessageStatus
Rul
FinishDateTime
Client
21/8/2019 4:29:48 PM
SMS
Out
starhubnew2(82045273)
Message sent via AlertDispatcher SMTP Server
Processed
21/8/2019 4:29:52 PM
SMTP (Maste
[ALERTDISPATCHER - Master] Server running
11(Very poor)

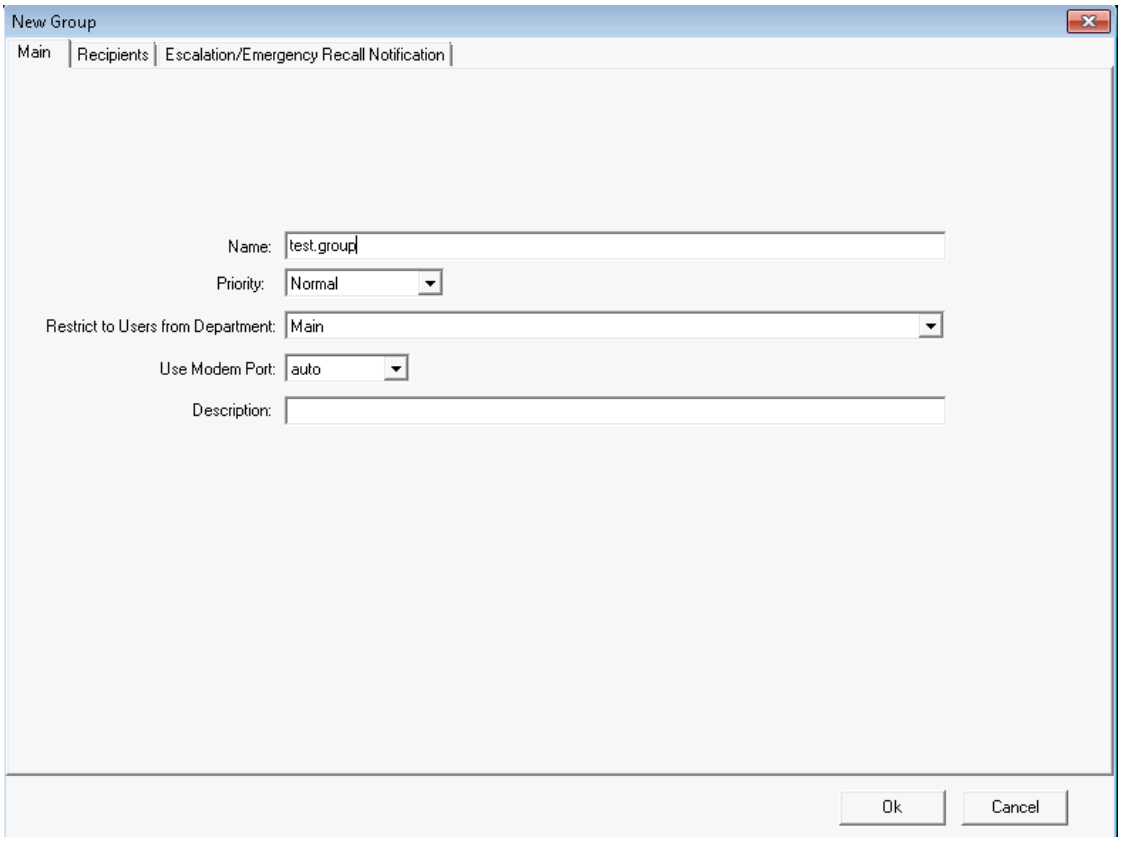
3). How to use the Addressbook and setup Escalation

a). Adding Group and Recipient

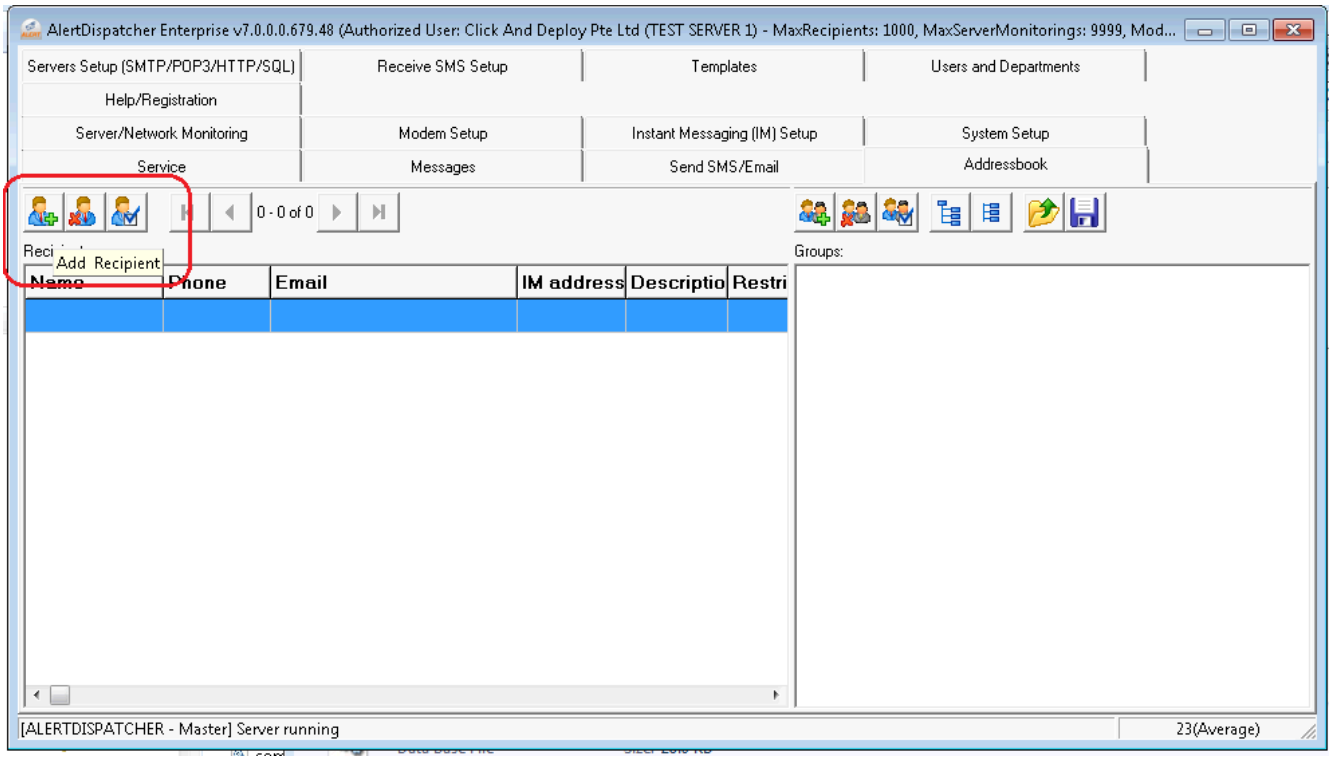
Navigate to the “Addressbook” tab, and then click on the “Add Group” icon.



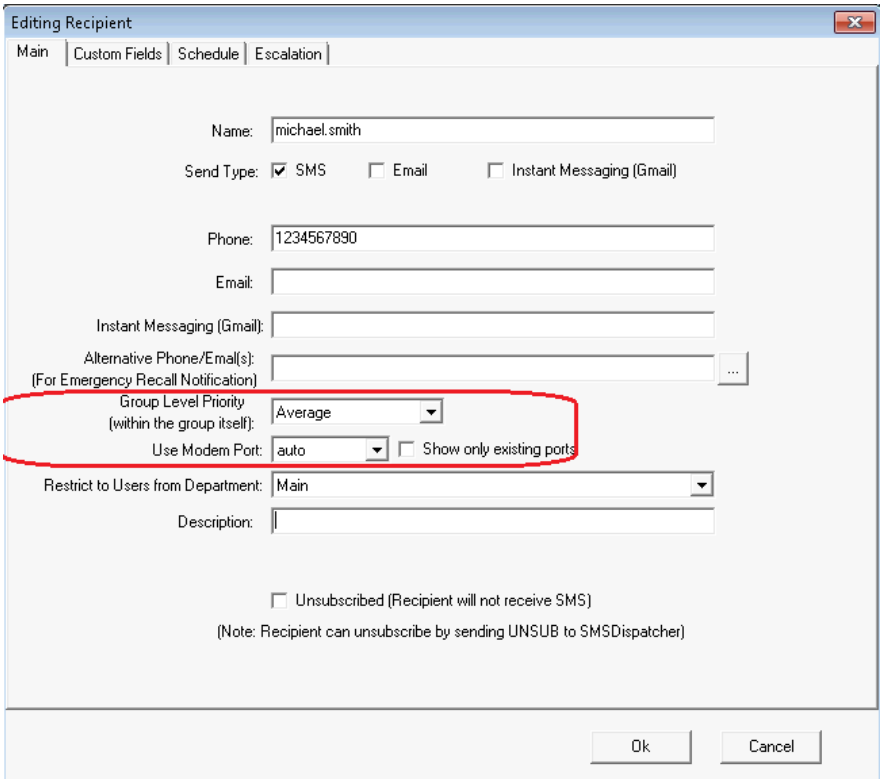
You can assign priority to your group. Messages sent to groups with higher priority will be sent out first.



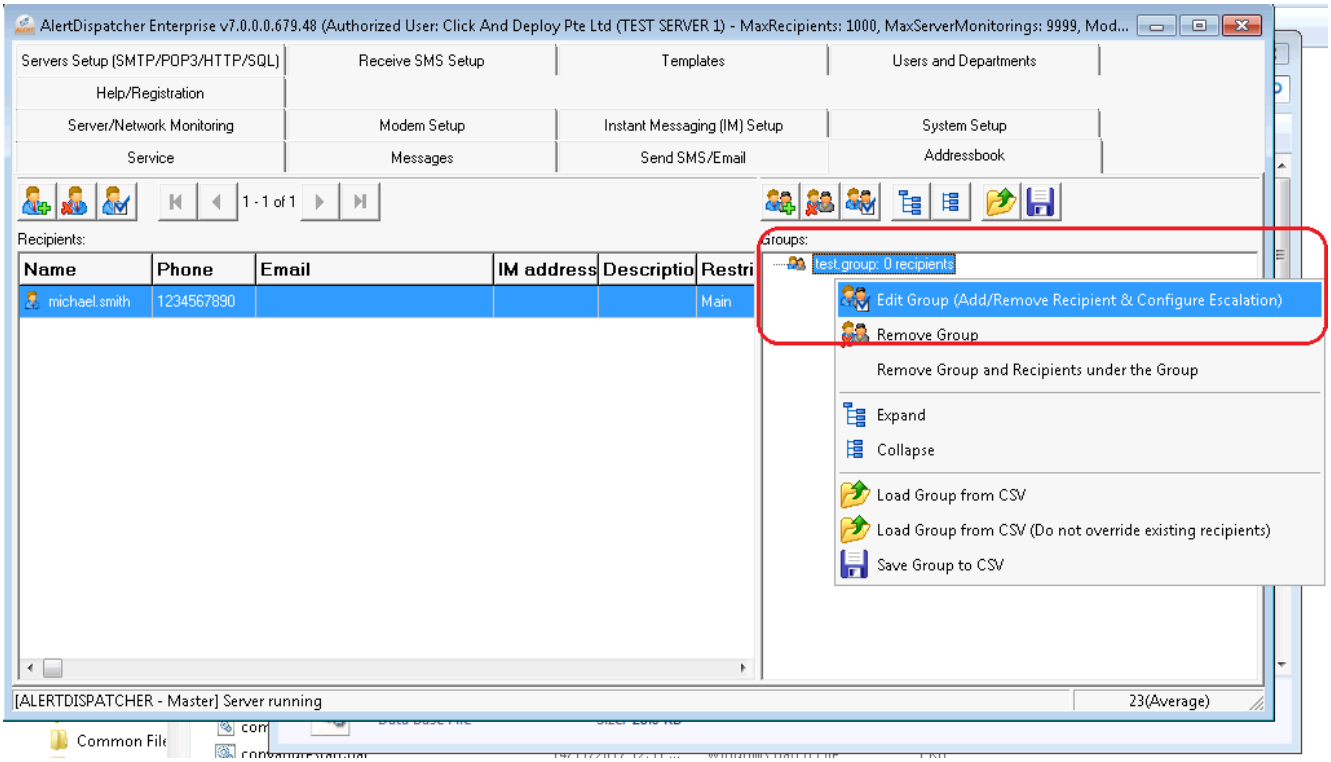
Next, click on "Add Recipient" button to create recipients.



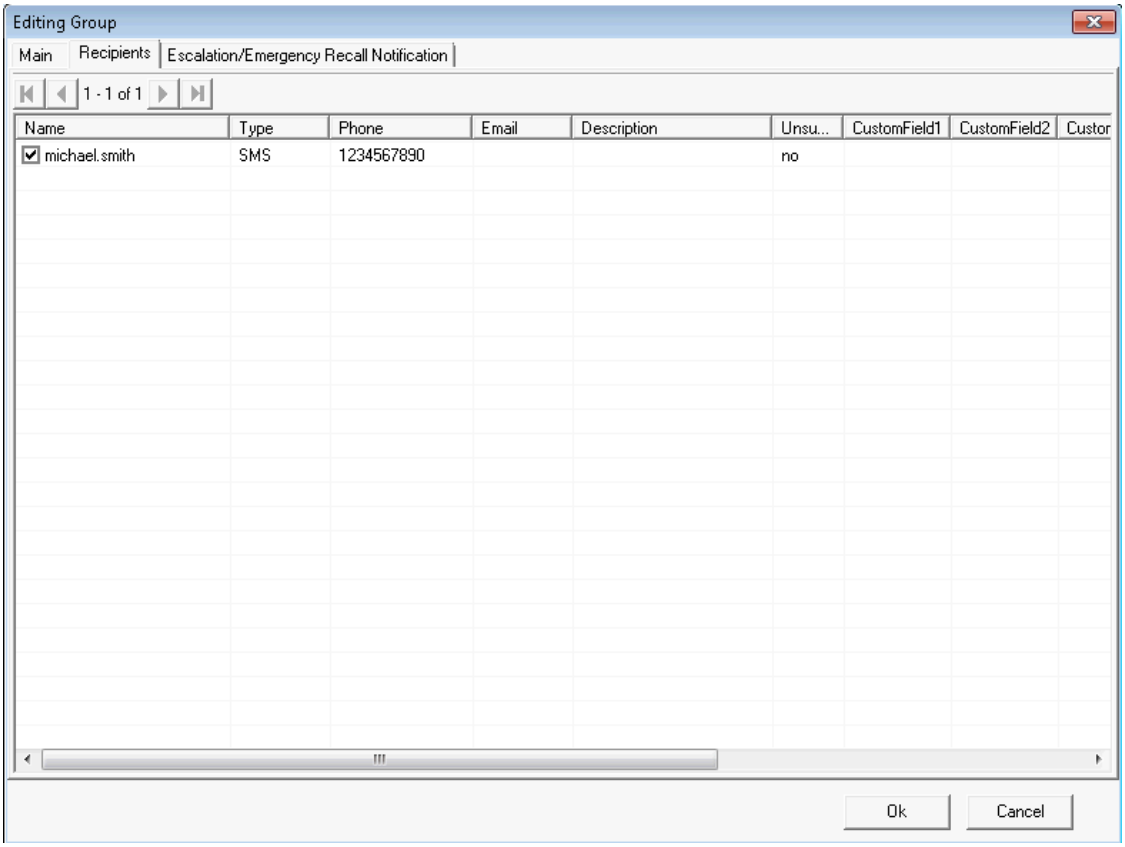
You can assign group level priority to recipients. If you have a modem pool, you can select the preferred modem to use for the recipient. This is useful if you need to split sent messages across different SIM cards for accounting purpose. For example, each SIM card may have a free SMS limit of X number of SMS per month. To optimise your usage, you would want to split your messages across the modem pool.



To assign recipients to the group you have just created, right click on the group, select “Edit Group (Add/Remove recipient & Configure Escalation)”. Alternatively, you can just double click on the group itself.



Use the checkboxes to add recipients to the group.



b). Setting up Basic Escalation

i. Overview

To ensure that critical messages are received and acted upon by recipients, you can define an escalation sequence for an addressbook group so that messages sent to the group need to be acknowledged by recipients within a defined time interval, failing which they will be escalated to the next level (tier) of recipients or resent to the same group.

There are two types of escalation that can be enabled for groups : a). *Basic Escalation,* and b). *Emergency Recall Notification.*

For Basic Escalation, any of the recipients from the group may acknowledge the message on behalf of the entire group. However, for Emergency Recall Notification, all recipients must personally acknowledge the escalation messages sent to them. Any recipient that has not acknowledged will receive escalation messages as configured.

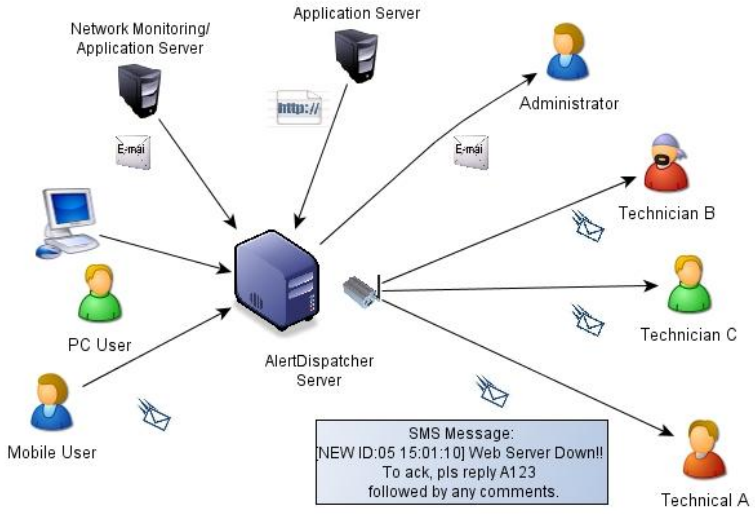
Any Basic Escalation message that is not acknowledged by any of the recipients that received the message can be escalated up to 50 times to another recipient/group (or back to the original escalation group).

There are 2 ways to configure Basic Escalation. The most popular way is to send to a group of recipients and hope that any of the recipients will acknowledge. If no acknowledgement is received after a defined time interval, the message is escalated to another group of recipients, e.g. the managers. This method is useful in reaching a group of recipients as quickly as possible, which is useful in case not everyone is able to receive or read the message in time. For example, some recipients might have turned off their phones or maybe asleep.

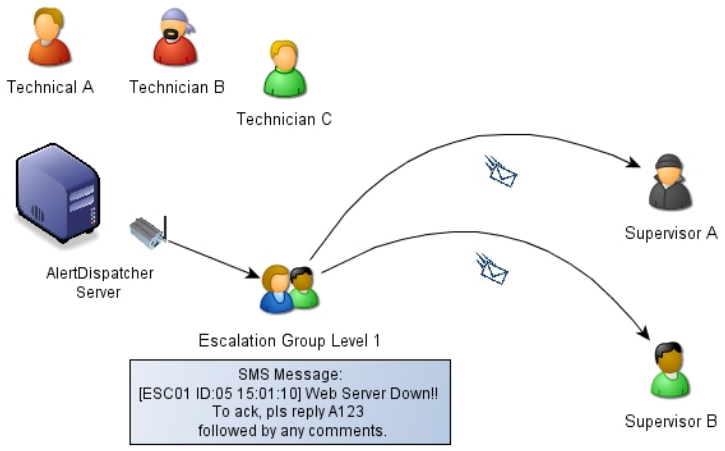
The other way is to send to just 1 recipient (you can add only 1 recipient to the group), and then escalate to a 2nd recipient if that single recipient does not acknowledge, and then if the 2nd recipient also does not acknowledge, escalate to 3rd recipient and so on.

Note: For discussion purpose, 'escalation messages' refers to messages that require recipient acknowledgement, and 'escalation groups' refers to groups with either basic escalation or emergency recall notification configured.

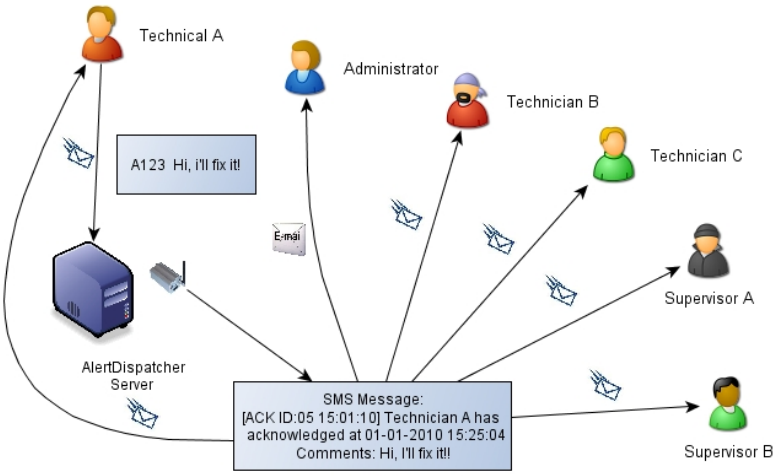
1. Broadcast to Tier 1



2. Escalate to Tier 2



3. Someone in Tier 2 acknowledges



ii. Pros, Cons and Important Good Practices for using Escalation

There are pros and cons to using escalation messages.

Pros:
1. Ensures that someone reads the message.
2. Escalates to management if no one acknowledges.

Cons:
1. Generates greater message volume depending on how the escalation is configured, and especially so if lower escalation level recipients don't acknowledge promptly. The increase in message volume may slow down the system, especially if there is a surge or outage that generates a lot of original messages.
2. Increases the workload of recipients that need to acknowledge the messages.

Here are some good practices to ensure that escalation messages works for you without the drawbacks.

Important Good Practices to follow when setting up escalation:

1). Create a test group to test out escalation messages before enabling escalation for actual AlertDispatcher Groups.

2). Enable escalation messages only for critical alarms groups. You can use separate groups for critical and non-critical alarms.

3). Minimizing the number of recipients in each Tier would limit the increase in message volume, especially when *"Notify everyone that has been contacted whenever anyone makes an acknowledgement"* checkbox is enabled.

For example, if there are 3 "Tier 1" recipients configured and someone in Tier 1 acknowledges before the message is escalated to Tier 2, the total number of messages generated is 3 original messages + 3 acknowledgement confirmation messages equals 6 messages in total. Therefore, the fewer recipients are in Tier 1, the lesser the number of messages sent in total.

4). Configure an escalation time interval that is sufficient for recipients to make a successful acknowledgement. 15 minutes is the lowest recommended time interval but you configure 20 or 30 minutes if possible.

5). Train your recipients to make multiple acknowledgements in a single reply, e.g. A123, A456, A678.

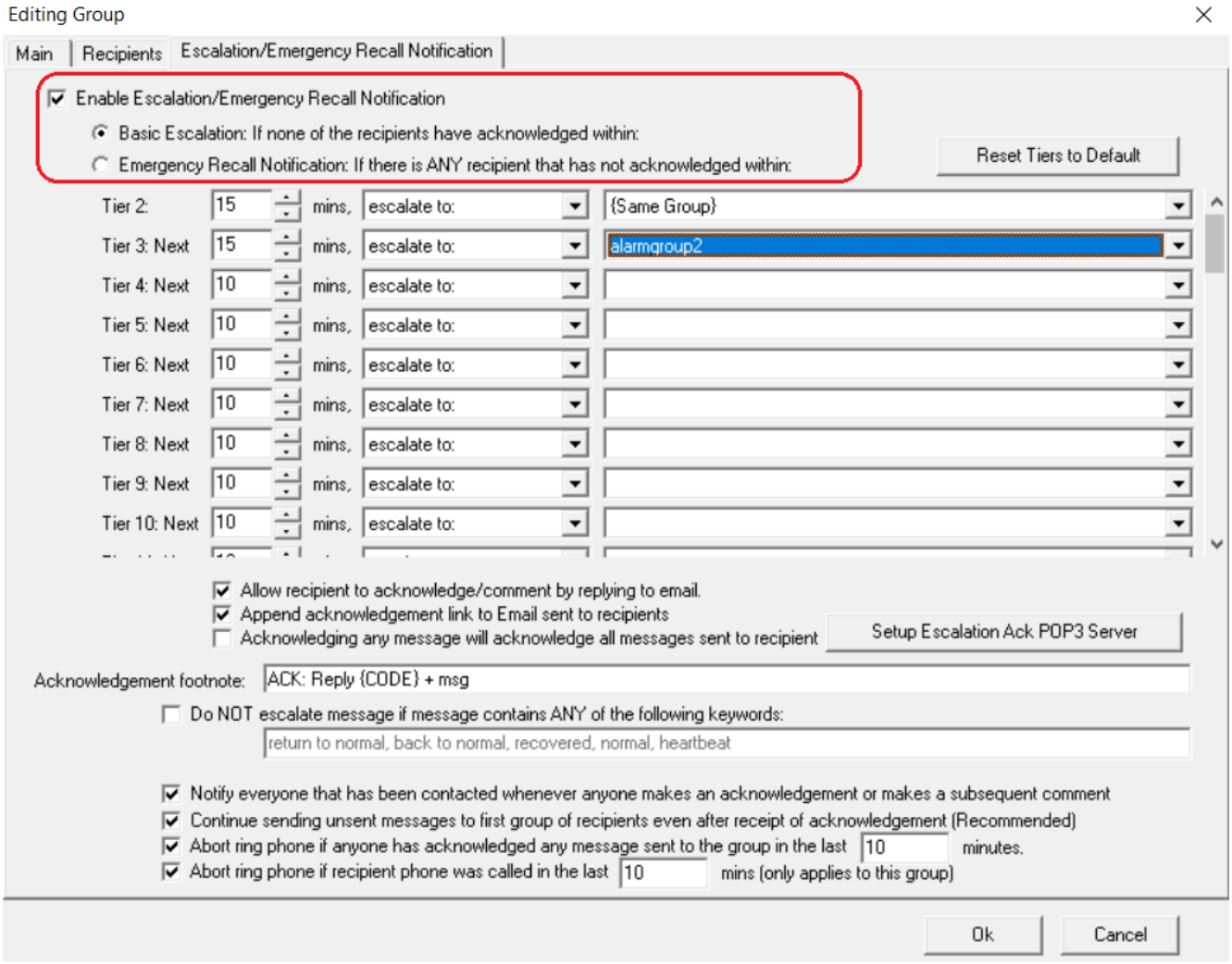
6. Exempt return-to-normal messages from escalation using the *"Do NOT escalate messages if message contains ANY of the following keywords"* setting.

7. Allow recipients to acknowledge once by enabling the *"Acknowledging any message will acknowledge all messages sent to the recipient*" checkbox.

iii. How to configure Basic Escalation for Addressbook Groups

To setup Basic Escalation for an addressbook group, under *"Escalation/Emergency Recall Notification"* tab, *select "Basic Escalation"*. If Basic Escalation is enabled, escalation messages sent to the group must be acknowledged by any recipient in the group by SMS or Email reply.

You can configure AlertDispatcher to escalate the message to another recipient or group if no one acknowledges within the defined time interval, resend to the same group, or ring/call recipient phones (cellular/fixed line). Up to 50 tiers or levels of escalations can be configured.



Recipients can include comments in their acknowledgement SMS/Email and these comments will be forwarded to other recipients. The acknowledgment footnote is configurable.

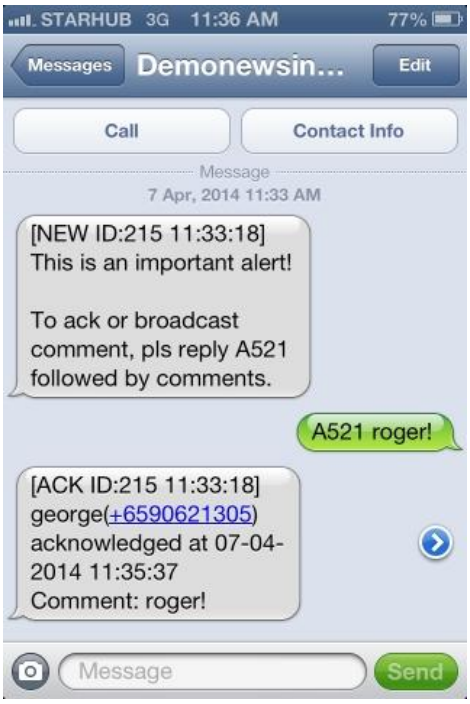
If you want to allow recipients to acknowledge all escalation messages received using a single reply, you can enable *"Acknowledging any message will acknowledge all messages sent to the recipient"*. This makes it more convenient for the recipient but the downside is we can't ensure that the recipient has actually received or read all the messages.

You can exempt specific messages bearing certain keywords from the acknowledgement requirement using the "*Do NOT escalate messages if message contains ANY of the following keywords*" setting.

iv. Acknowledging by SMS reply

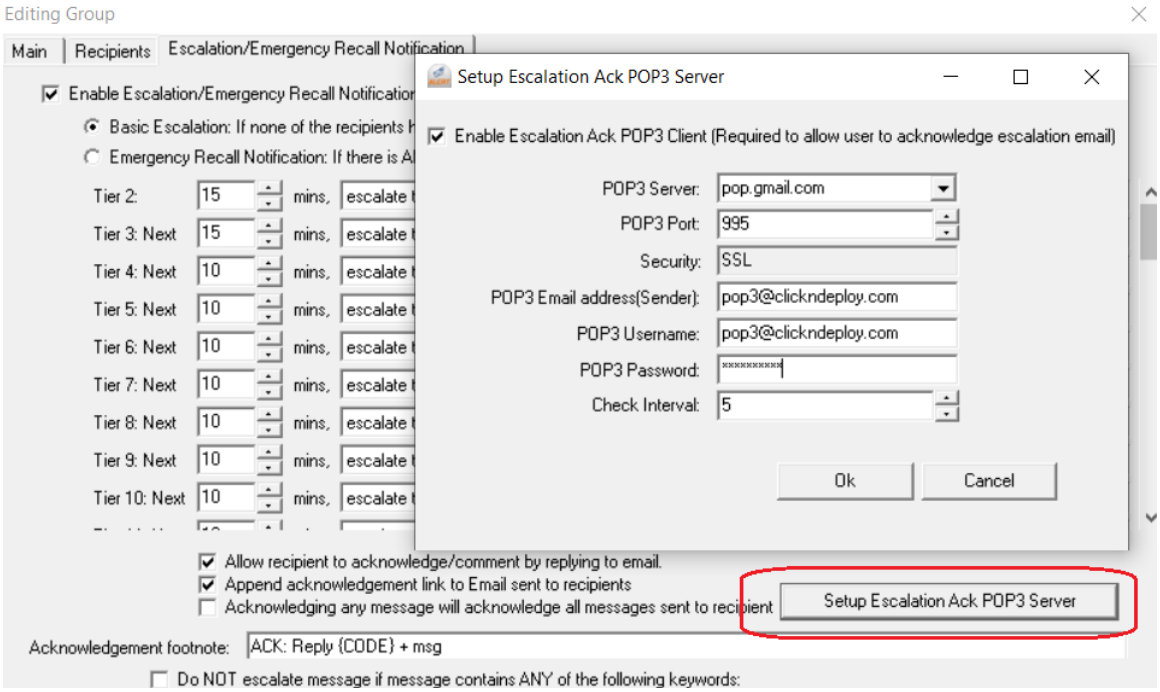
Recipients can acknowledge escalation messages received via SMS by replying a code. Multiple messages can be acknowledged in a single reply by including all the acknowledgement codes (comma separated), e.g. *A123, A456, A678.*

Alternatively, if *"Acknowledging any message will acknowledge all messages sent to the recipient"* setting is enabled, a recipient can acknowledge all messages by acknowledging any of the escalation messages received.

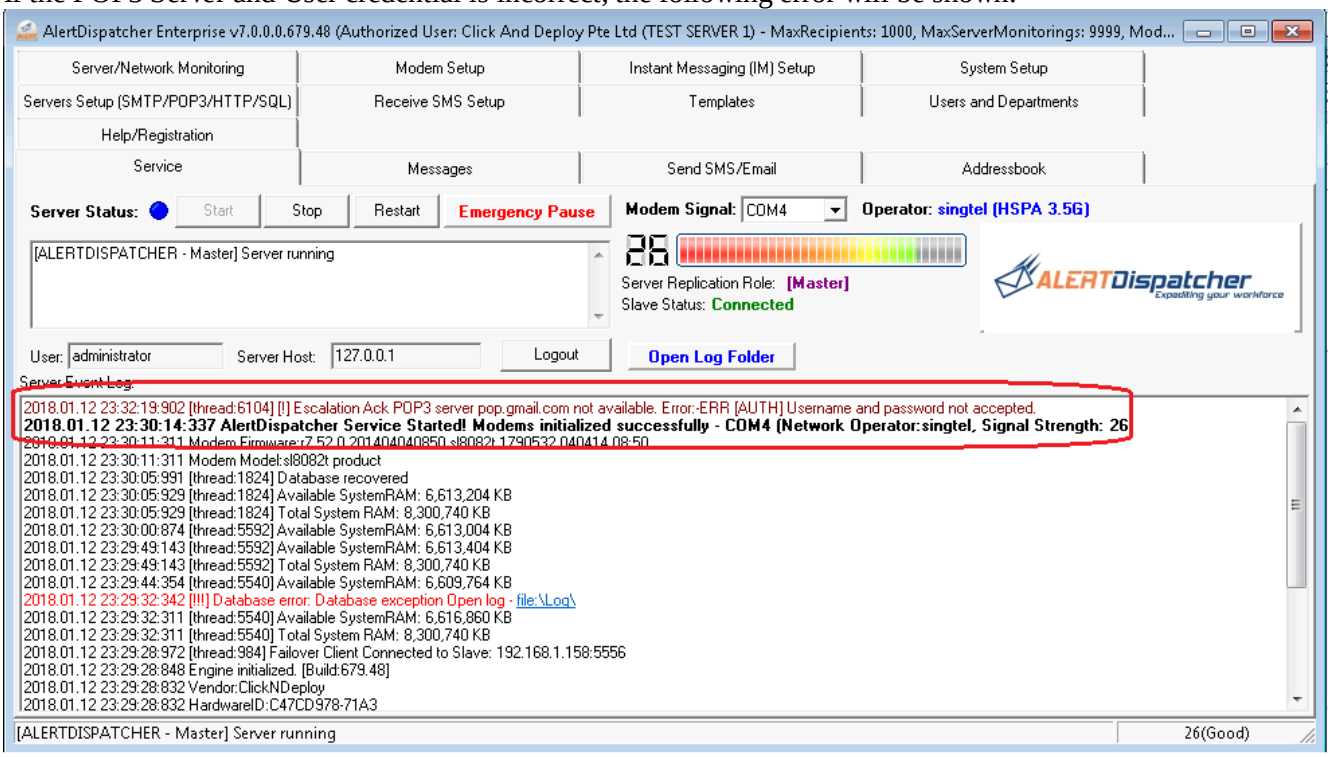


v. Acknowledging by Email reply

In order to allow recipients to acknowledge by email reply, you must enable *"Allow recipients to acknowledge/comment by replying to email"* setting and configure the POP3 Server and User credentials using the "Setup Escalation Ack POP3 Server" button.

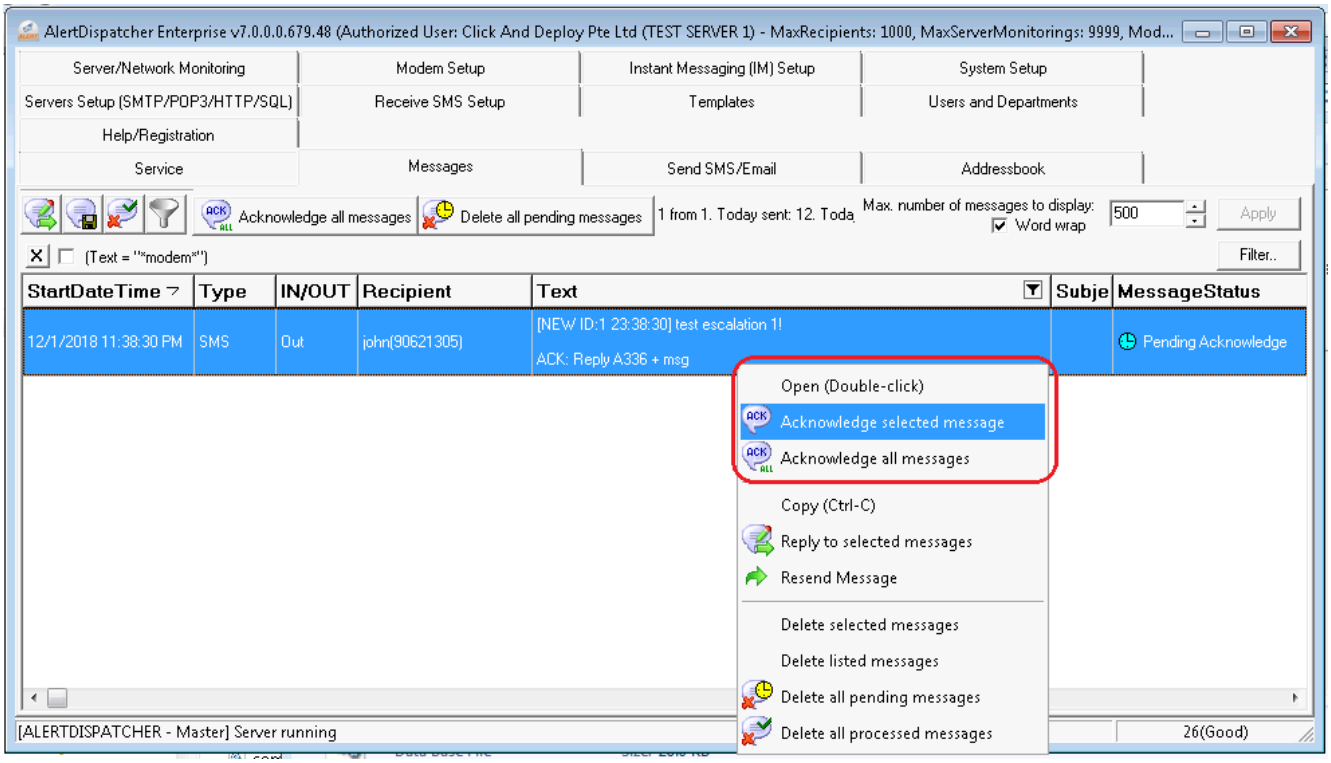


If the POP3 Server and User credential is incorrect, the following error will be shown:



vi. 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 previously mentioned, up to 50 tiers/levels of escalation actions can be assigned for each group. You can escalate the message to another recipient or group, back to the same group or call a recipient phone (cellular/fixed line).

c). Setting up Emergency Recall Notification

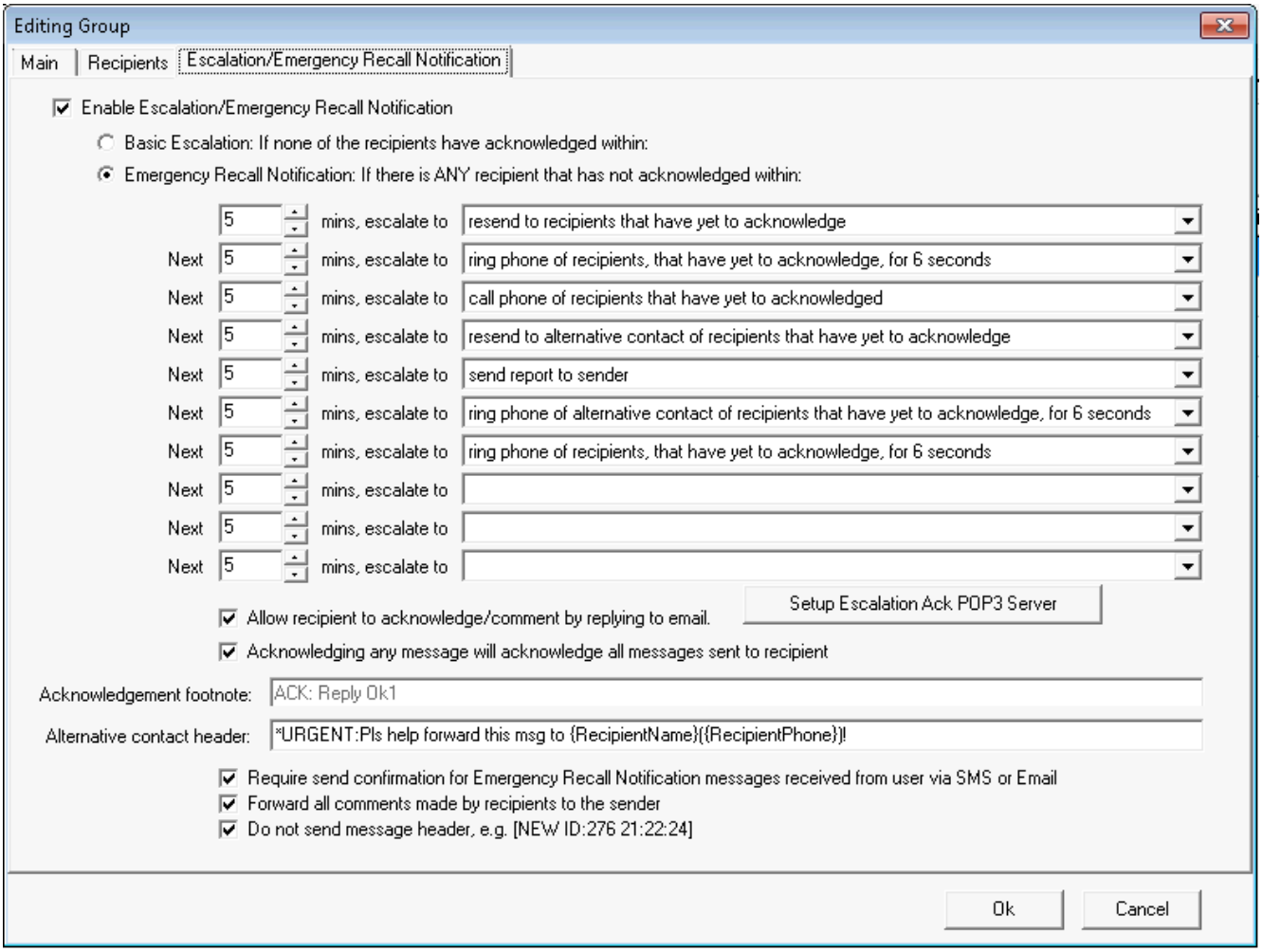
i. Overview

While Basic Escalation allows any recipient in the group to acknowledge on behalf of the group, Emergency Recall Notification requires that every recipient in the addressbook group personally acknowledge the message sent to them. Any recipient that has not acknowledged will receive escalation messages as configured.

The Emergency Recall feature is especially useful in emergency or disaster scenarios where you would want reach out a group of recipients and can be initiated by a user via SMS or AlertDispatcher Web Login.

ii. How to configure Emergency Recall for Addressbook Groups

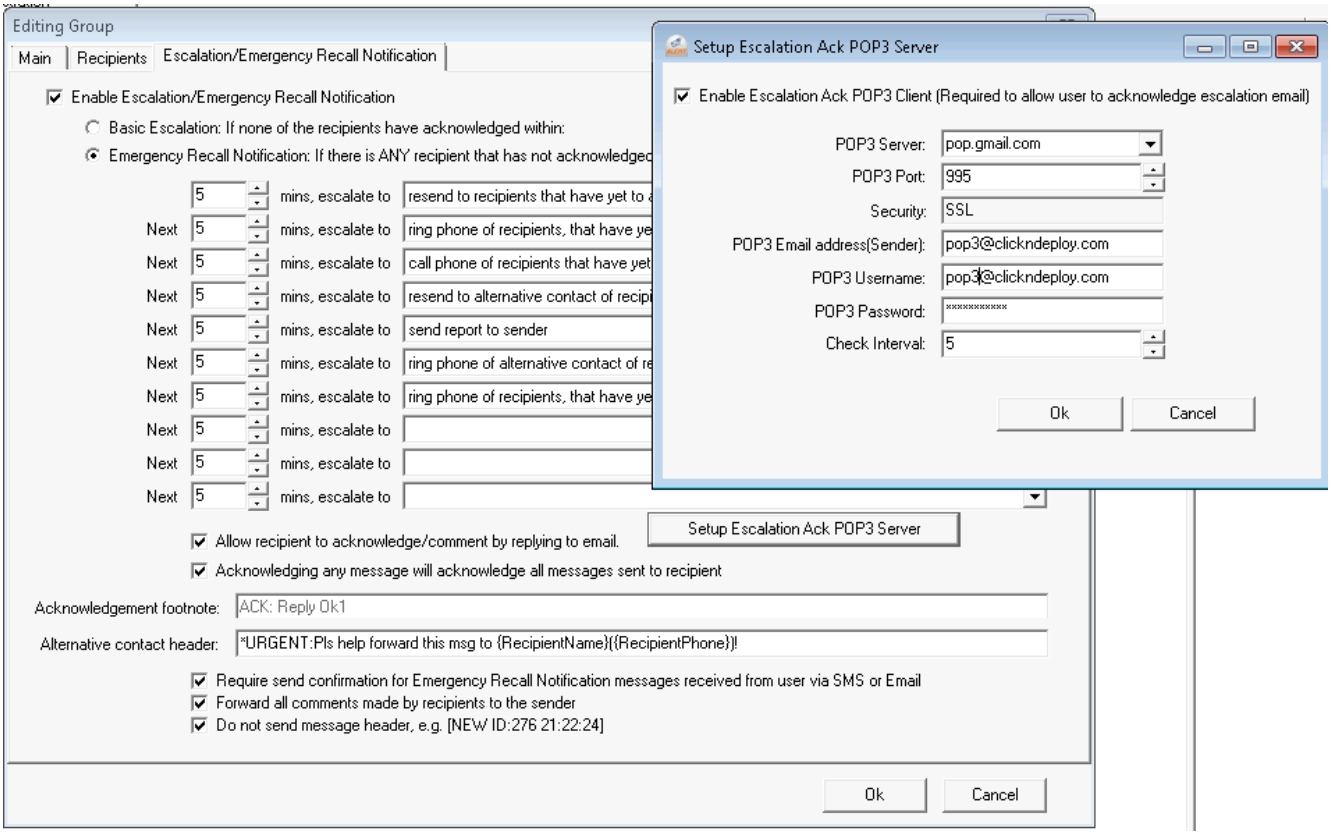
To setup Emergency Recall Notification an addressbook group, under *"Escalation/Emergency Recall Notification"* tab, select "Emergency Recall Notification". Up to 50 tiers/levels of escalations can be configured.



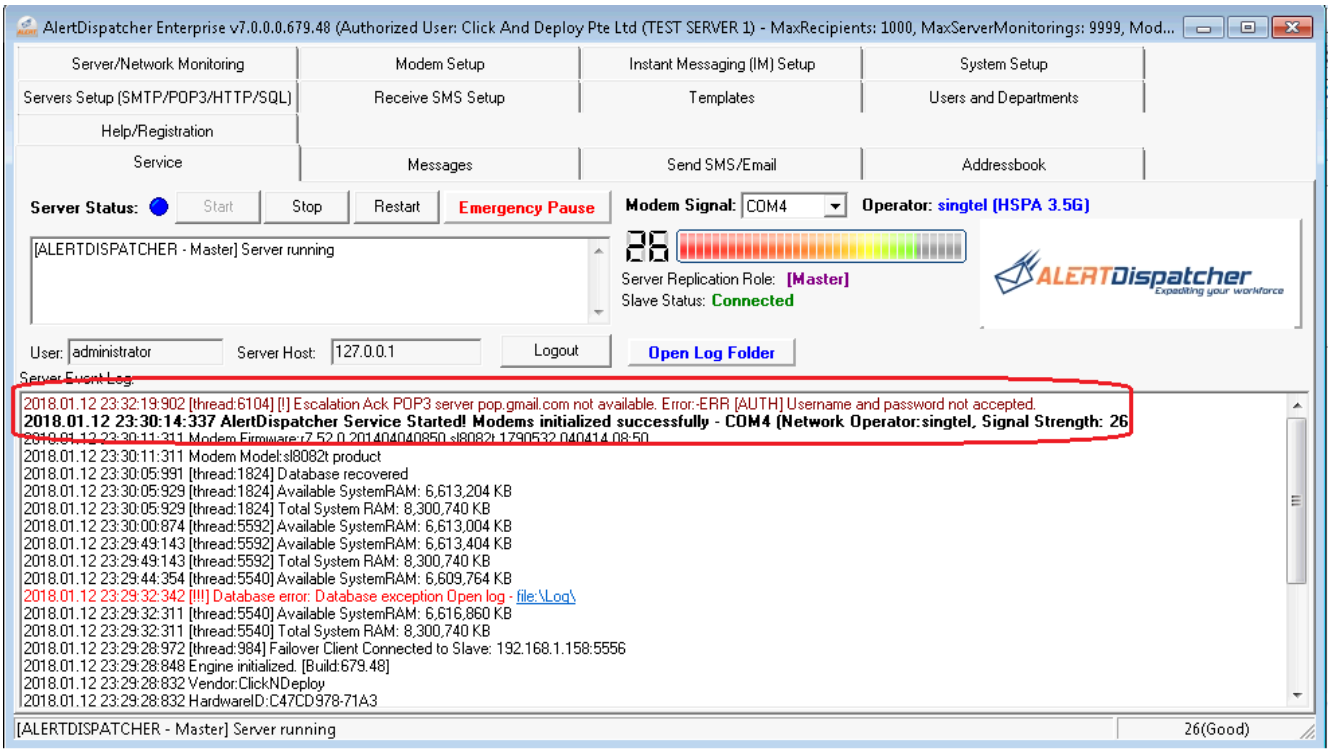
If you want to allow recipients to acknowledge all Emergency Recall messages received using a single reply, you can enable *"Acknowledging any message will acknowledge all messages sent to the recipient"*. This makes it more convenient for the recipient but the downside is we can't ensure that the recipient has actually received or read all the messages.

If *"Require send confirmation for Emergency Recall Notification messages received from user via SMS or Email"* setting is enabled, users can review and then choose to confirm the message.

If you want to allow recipients to acknowledge by email reply, you must enable *"Allow recipients to acknowledge/comment by replying to email"* setting and configure the POP3 Server and User credentials using the "Setup Escalation Ack POP3 Server" button.


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
mins, escalate to
Next
resend to recipients that have yet to
ring phone of recipients, that have ye
call phone of recipients that have yet
resend to alternative contact of recipi
send report to sender
ring phone of alternative contact of re
Setup Escalation Ack POP3 Server
Allow recipient to acknowledge/comment by replying to email.
Acknowledging any message will acknowledge all messages sent to recipient
Acknowledgement footnote:
ACK: Reply Ok1
Alternative contact header:
*URGENT:Pls help forward this msg to {RecipientName}({RecipientPhone})!
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
Setup Escalation Ack POP3 Server
Enable Escalation Ack POP3 Client (Required to allow user to acknowledge escalation email)
POP3 Server:
pop.gmail.com
POP3 Port:
995
Security:
SSL
POP3 Email address(Sender):
pop3@clickndeploy.com
POP3 Username:
pop3@clickndeploy.com
POP3 Password:
Check Interval:
5
Ok
Cancel

If the POP3 Server and User credentials is incorrect, the following error will be shown:

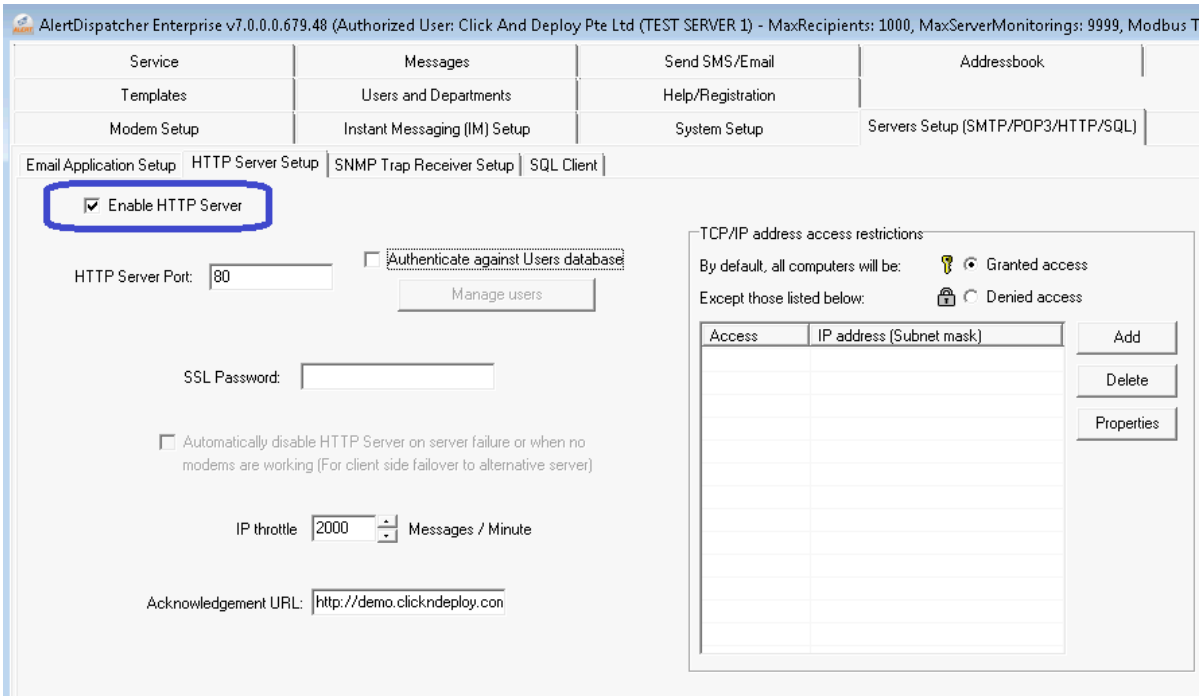


iii. Initiating Emergency Recall via AlertDispatcher Web Login

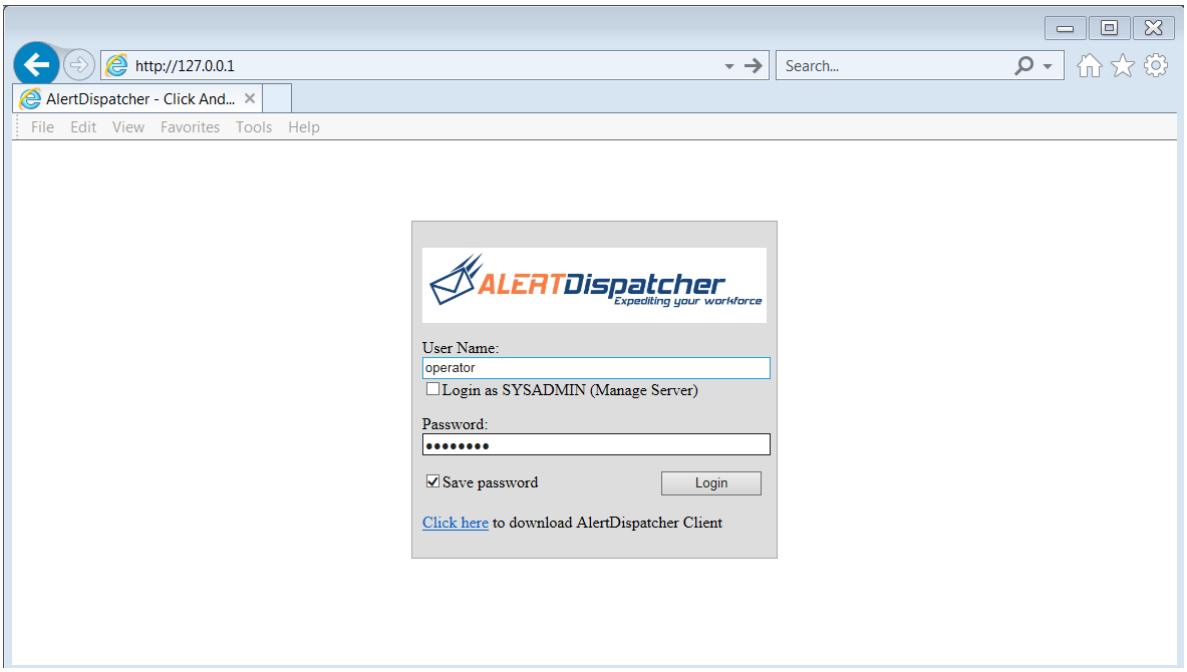
The best way to initiate an Emergency Recall is through the AlertDispatcher Web Login as you can monitor the progress of the recall real-time on your browser.

For Web Login to work, AlertDispatcher HTTP Server must be enabled. If you need to allow users to access the Web Login remotely from another workstation on the network, please ensure that Windows firewall does not block the configured HTTP Server Port (by default port 80).

Note: If there's another conflicting web server using the default port 80, you should change the AlertDispatcher HTTP Server Port, e.g. to port 8000.

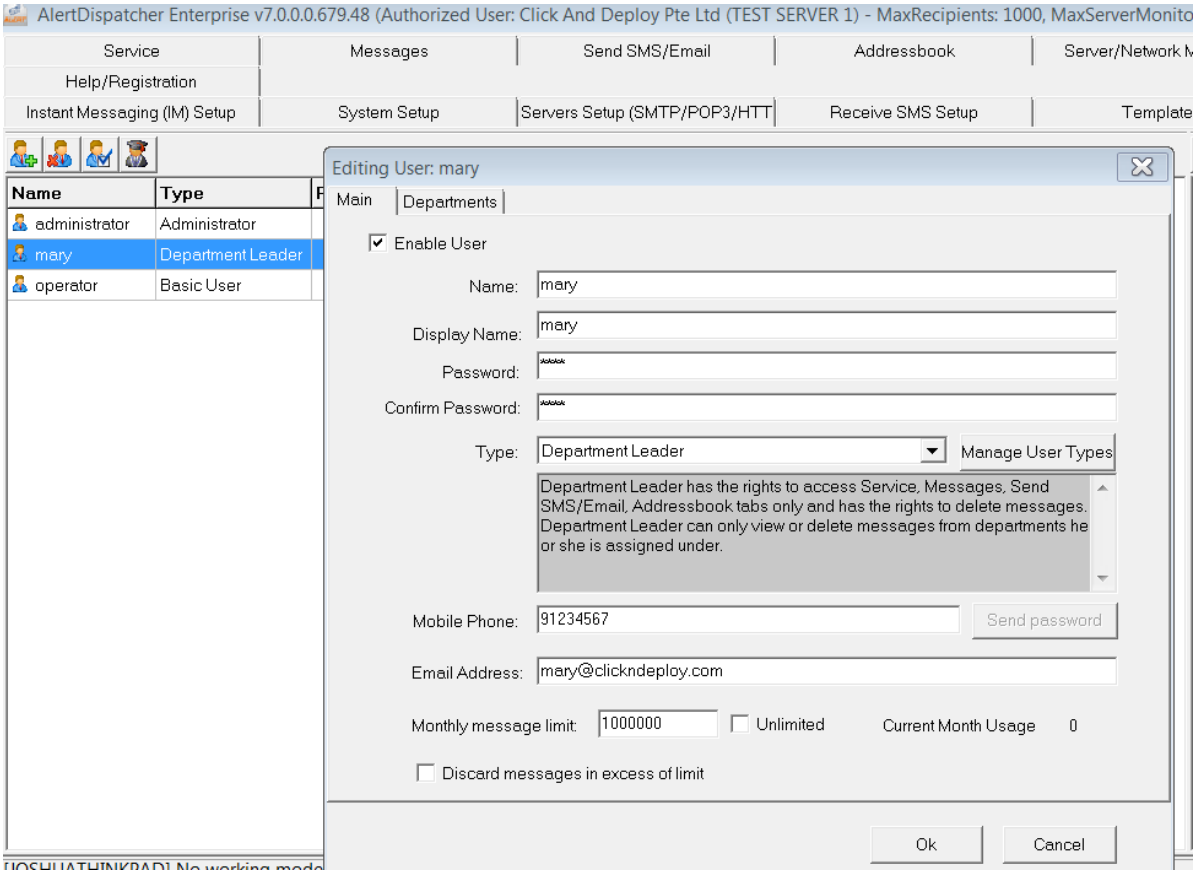


To test, access AlertDispatcher Web Login page on AlertDispatcher Server locally through your web browser, e.g. http://127.0.0.1/

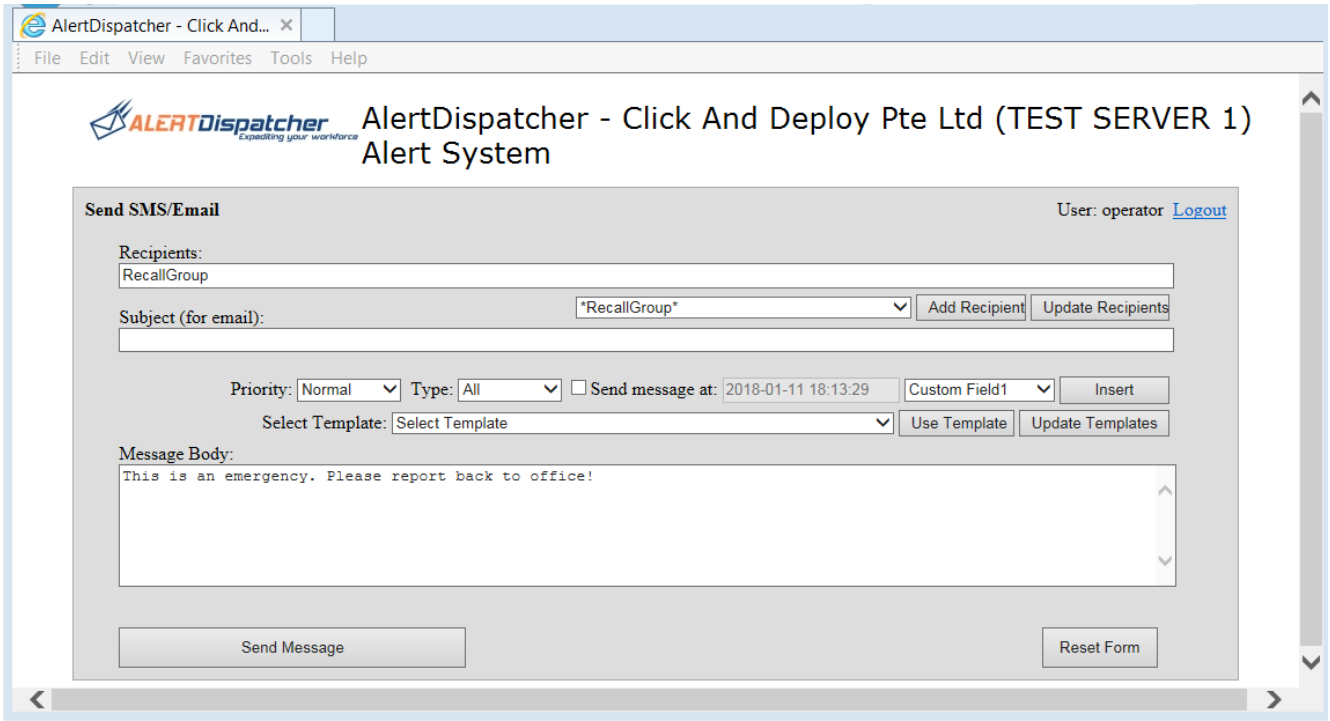


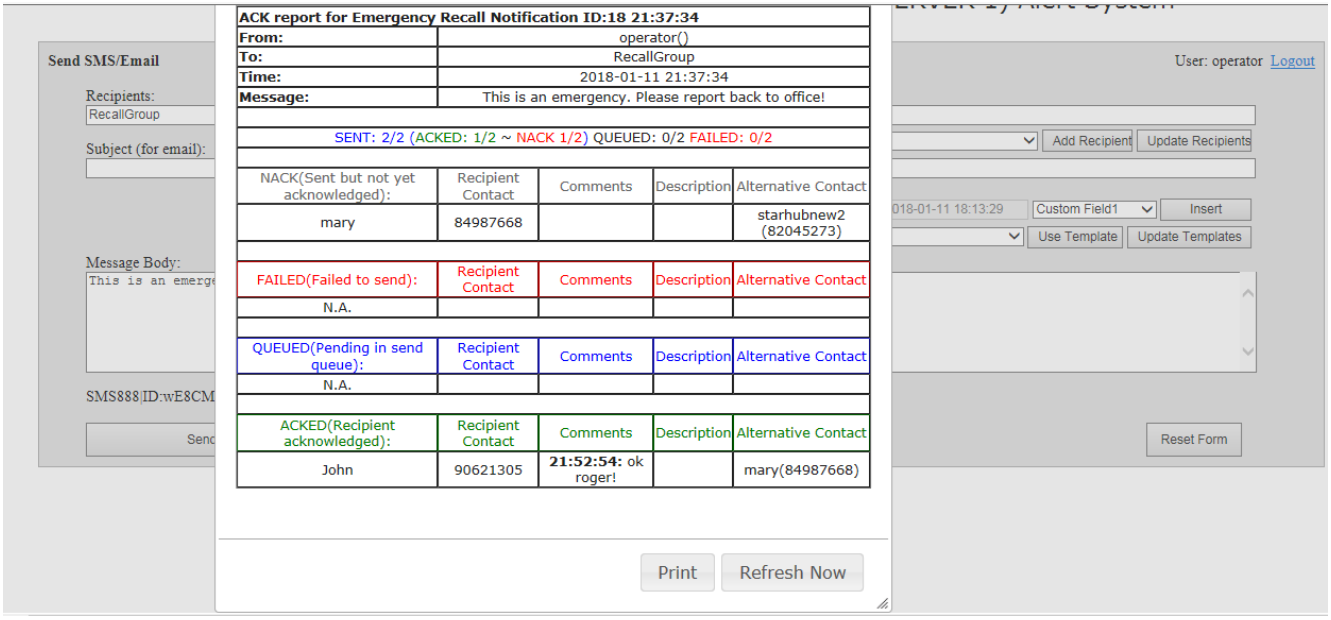
For login user, you can create a new user under *"Users and Departments"* tab, or you can use the automatically created "operator" user to login (default password: "operator").

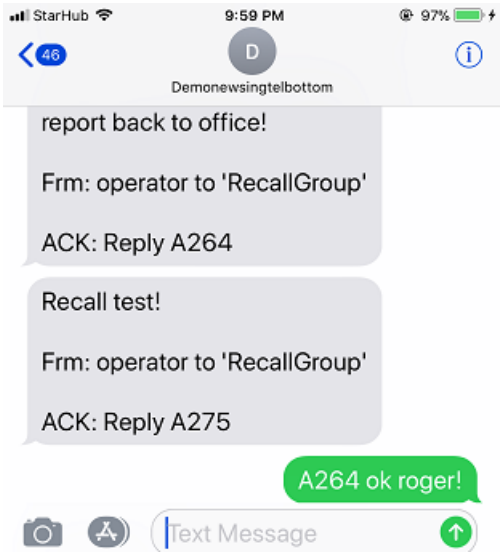
Note: Please change this password as soon as possible using the "Users and Departments" tab to prevent unauthorized usage.



After you have successfully login, select the group that is configured for Emergency Recall Notification, compose your message, and click "Send Message".




Send SMS/Email
Recipients:
RecallGroup
Subject (for email):
Message Body:
This is an emerge
SMS888|ID:wE8CM
Send
User: operator Logout
Add Recipient
Update Recipients
018-01-11 18:13:29
Custom Field1
Insert
Use Template
Update Templates
Reset Form
ACK report for Emergency Recall Notification ID:18 21:37:34
From: operator()
To: RecallGroup
Time: 2018-01-11 21:37:34
Message: This is an emergency. Please report back to office!
SENT: 2/2 (ACKED: 1/2 ~ NACK 1/2) QUEUED: 0/2 FAILED: 0/2
NACK(Sent but not yet acknowledged): | Recipient Contact | Comments | Description | Alternative Contact
mary | 84987668 | | | starhubnew2 (82045273)
FAILED(Failed to send): | Recipient Contact | Comments | Description | Alternative Contact
N.A.
QUEUED(Pending in send queue): | Recipient Contact | Comments | Description | Alternative Contact
N.A.
ACKED(Recipient acknowledged): | Recipient Contact | Comments | Description | Alternative Contact
John | 90621305 | 21:52:54: ok roger! | | mary(84987668)
Print
Refresh Now


StarHub
9:59 PM
97%
46
D
Demonewsingtelbottom
report back to office!
Frm: operator to 'RecallGroup'
ACK: Reply A264
Recall test!
Frm: operator to 'RecallGroup'
ACK: Reply A275
A264 ok roger!
Text Message

iv. Initiating Emergency Recall via SMS

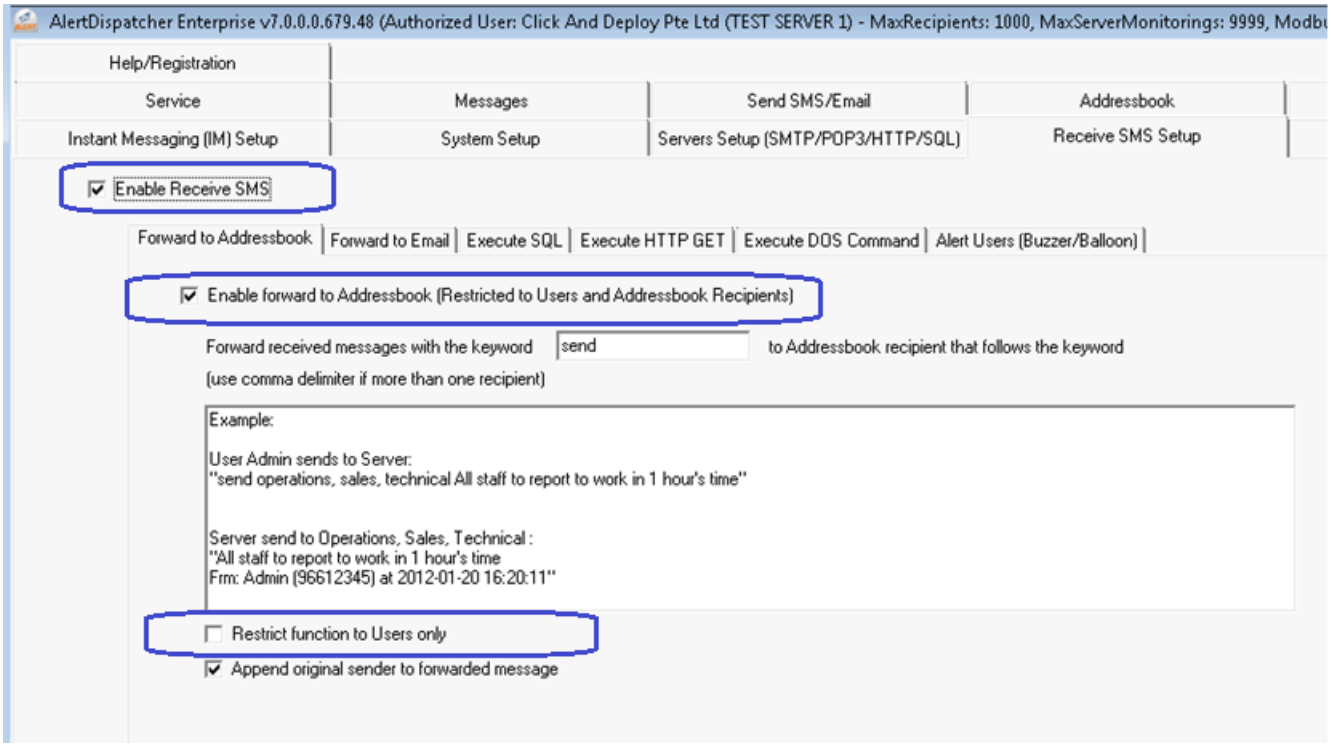
A user can also initiate an Emergency Recall remotely by sending an SMS to the server.

SMS Format:

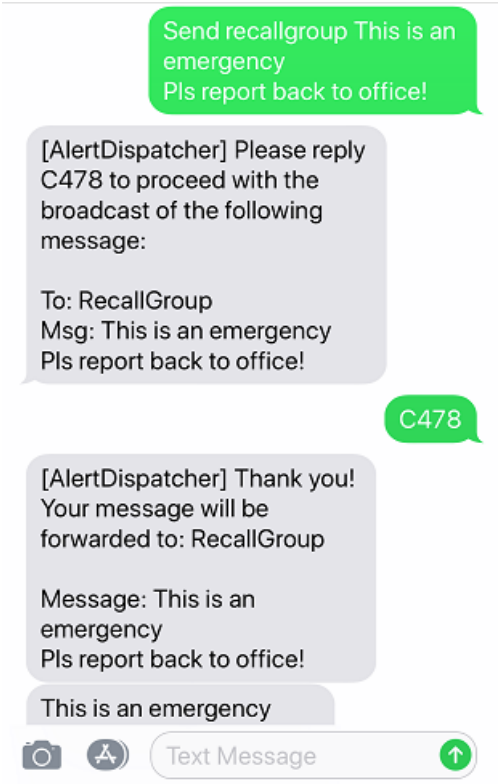
"Send {GroupName} {Message}"

The requirement is that *"Enable Receive SMS"* and *"Enable forward to Addressbook"* settings under *"Receive SMS Setup"* tab must be enabled. For security, the user's mobile phone number must be found in the addressbook (recipient) or inside one of the login users (setup under "Users and Departments" tab).

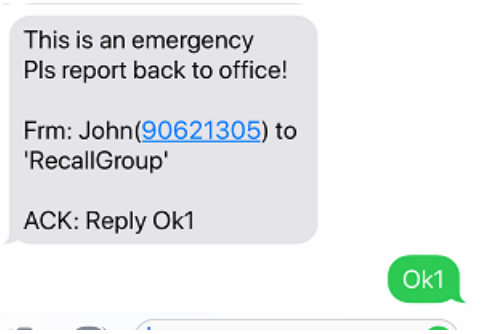
Note: You can restrict this capability to login users only by enabling the *"Restrict function to Users only"* setting under "*Receive SMS Setup*", *"Forward to Addressbook"* tab.



In the following example, a user initiates an Emergency Recall to "RecallGroup" group by sending an SMS *"Send recallgroup This is an emergency. Pls report back to office!"*.

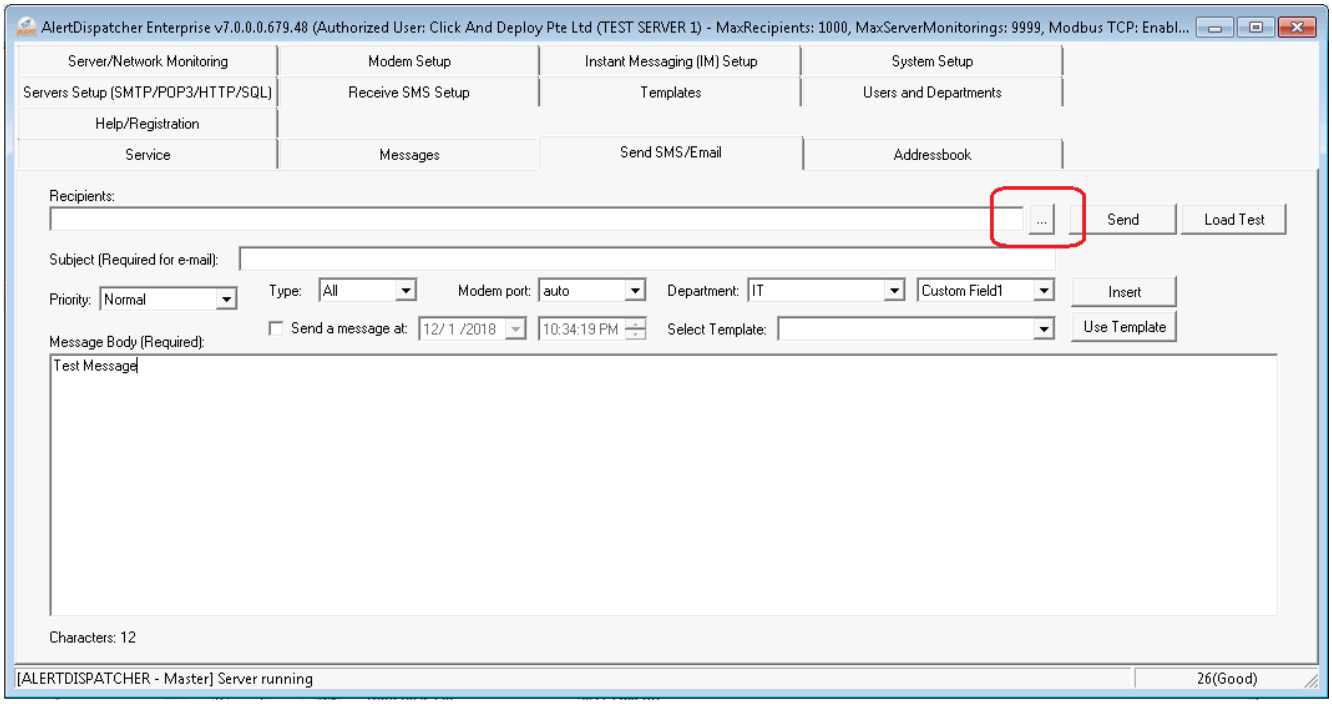


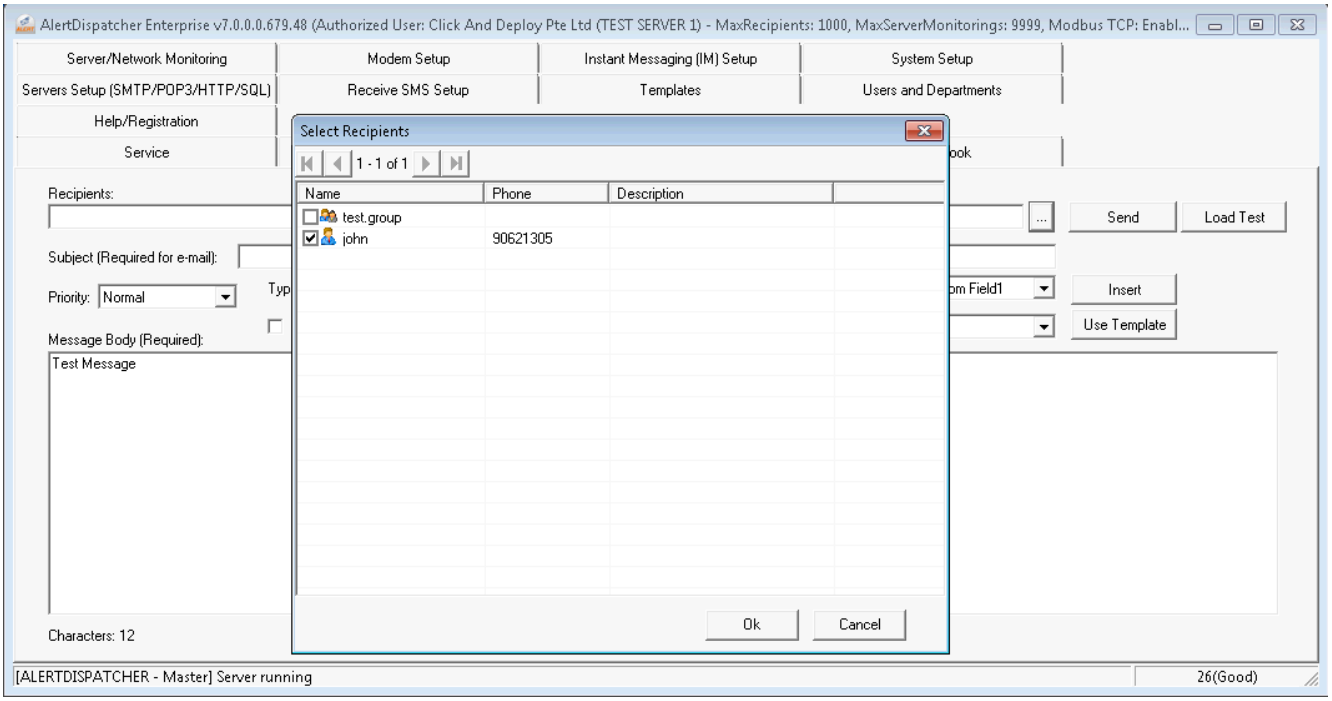
A recipient receives the SMS and sends Ok1 to acknowledge.



d). Send Test Message

To test your newly created addressbook group, navigate to the "Send SMS/Email" tab, click on the '…' button and select the group.

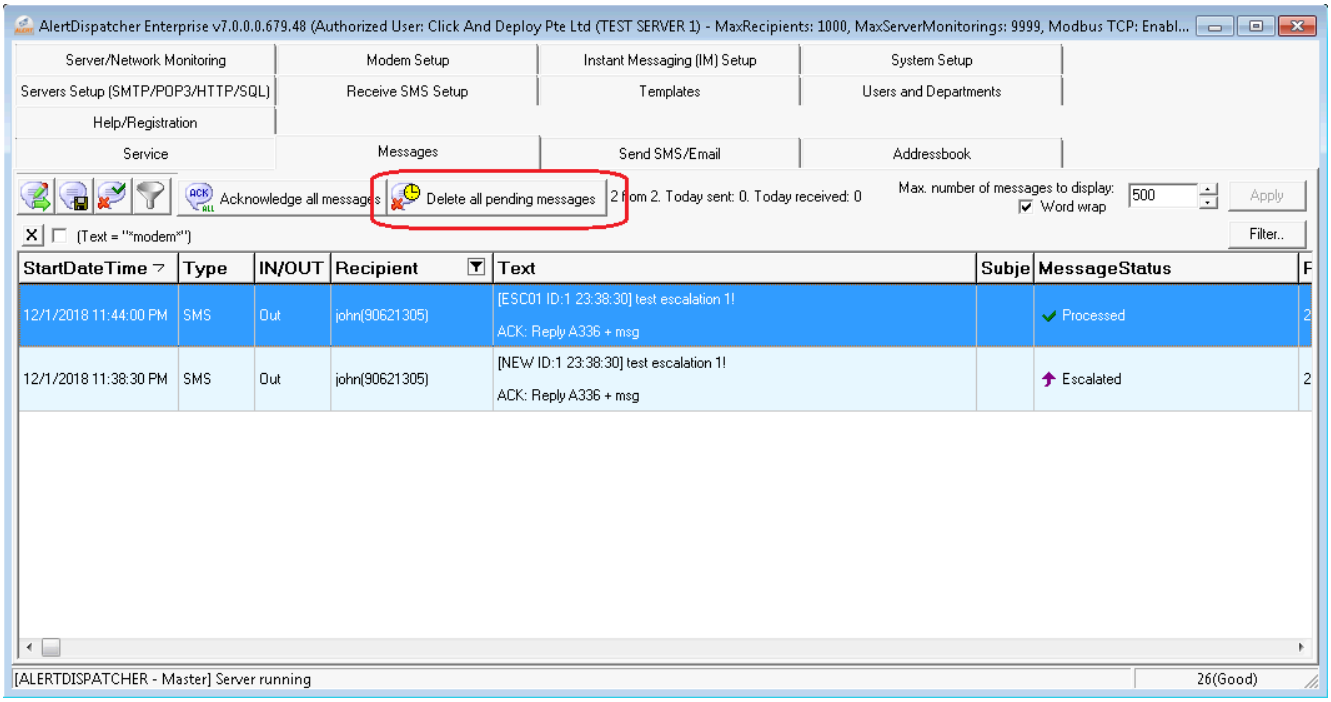




Click "Send" button to send the message.

4). How to Delete Pending Messages

You can all delete pending messages (messages that have not been sent out by the system) by right clicking on the message grid and select “Delete all pending messages”.



5). How to Export Messages to Excel

Navigate to the “Messages” tab. Change the Max. number of messages to display from the default "500" to "10000" (Step 1). Click "Apply" button.

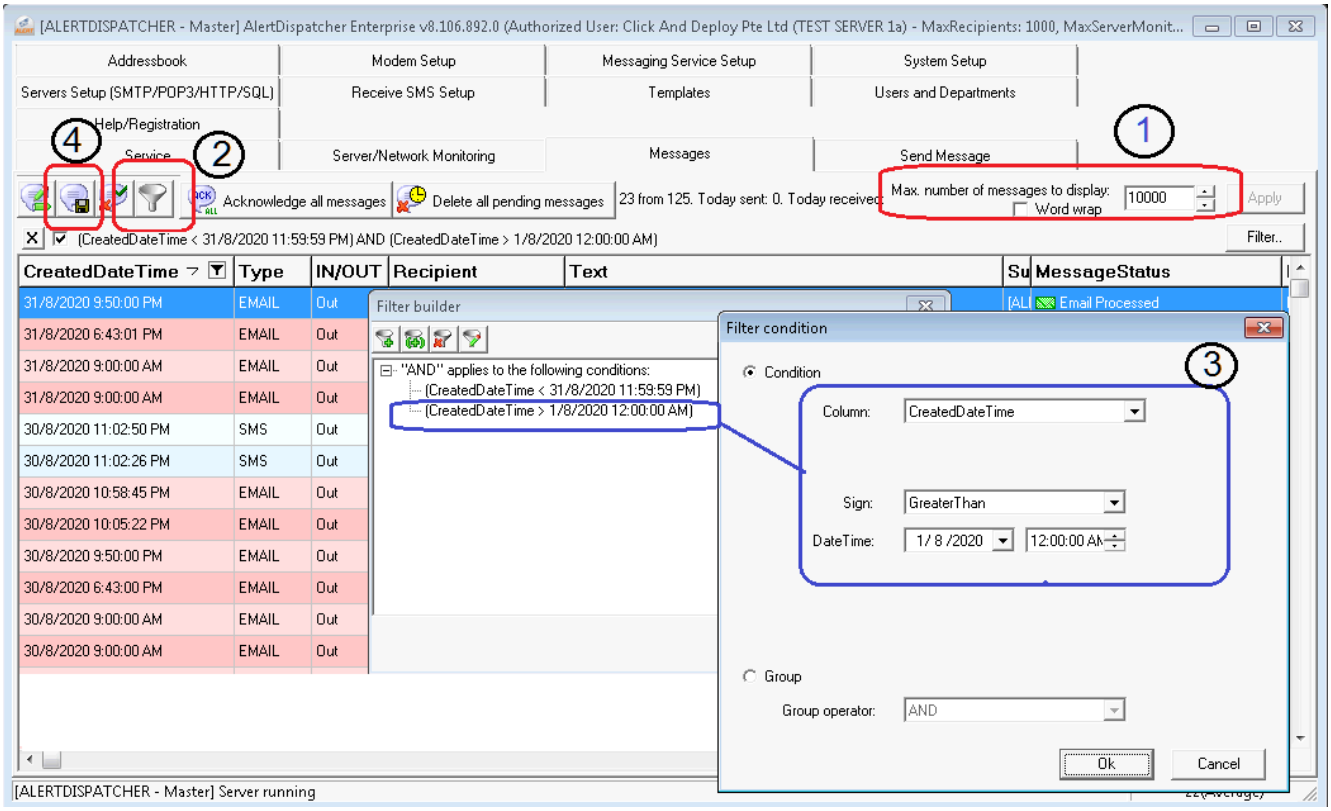
Note: After you have completed the message export, please reset back to 500 to avoid slowing down your system.

Click on "Filter" button (Step 2), and add 2 "CreatedDateTime" conditions with Sign "GreaterThan" and "LessThan" to define the date range of messages you want to filter (Step 3).

For example, to set filter to show messages only in the month of August 2020, create the following 2 "CreateDateTime" conditions, 1). CreatedDateTime "GreaterThan" 1/8/2020 12:00:00 AM. 2). CreatedDateTime "LessThan" 31/8/2020 11:59:59 PM.

Note: Messages tab can only display up to 10000 messages. If there are more than 10000 messages in the month of August, you will need to reduce the date range defined in the filter.

Click on "Export to CSV" button (Step 4). You can use MS Excel to open the file.



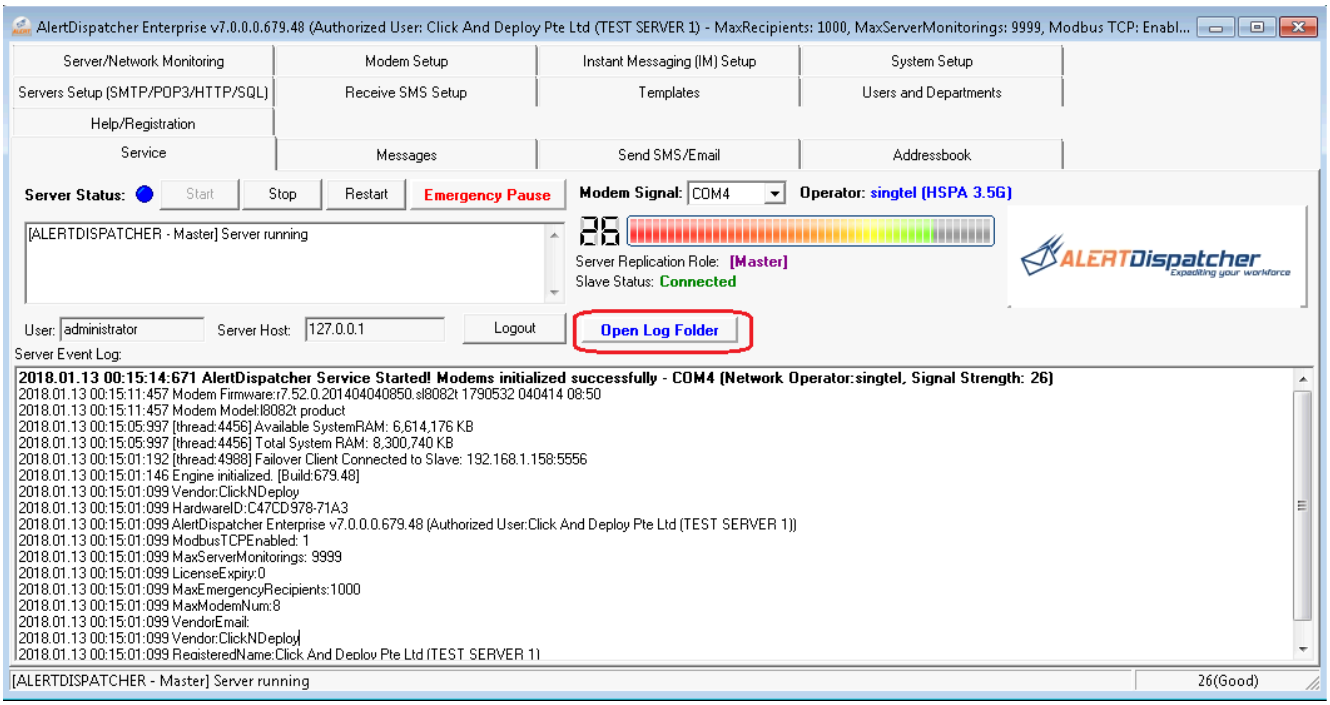
6). How to Retrieve Logs for Troubleshooting

You can retrieve your logs by clicking on the "Open Log Folder" button.

The most useful logs are the AlertDispatcherServer, AlertDispatcherServer_events and AlertDispatcherSignal logs. If you're interfacing 3rd party applications with AlertDispatcher, the relevant logs include SMTPListener, HTTPListener and SNMPTrapReceiver logs.

Note: Logs will be automatically archived to the \archive subfolder when they reach 10MB in size. To identify which archived log is relevant, please sort the files by date and then open log file to verify that it contains the log when the error occurred.

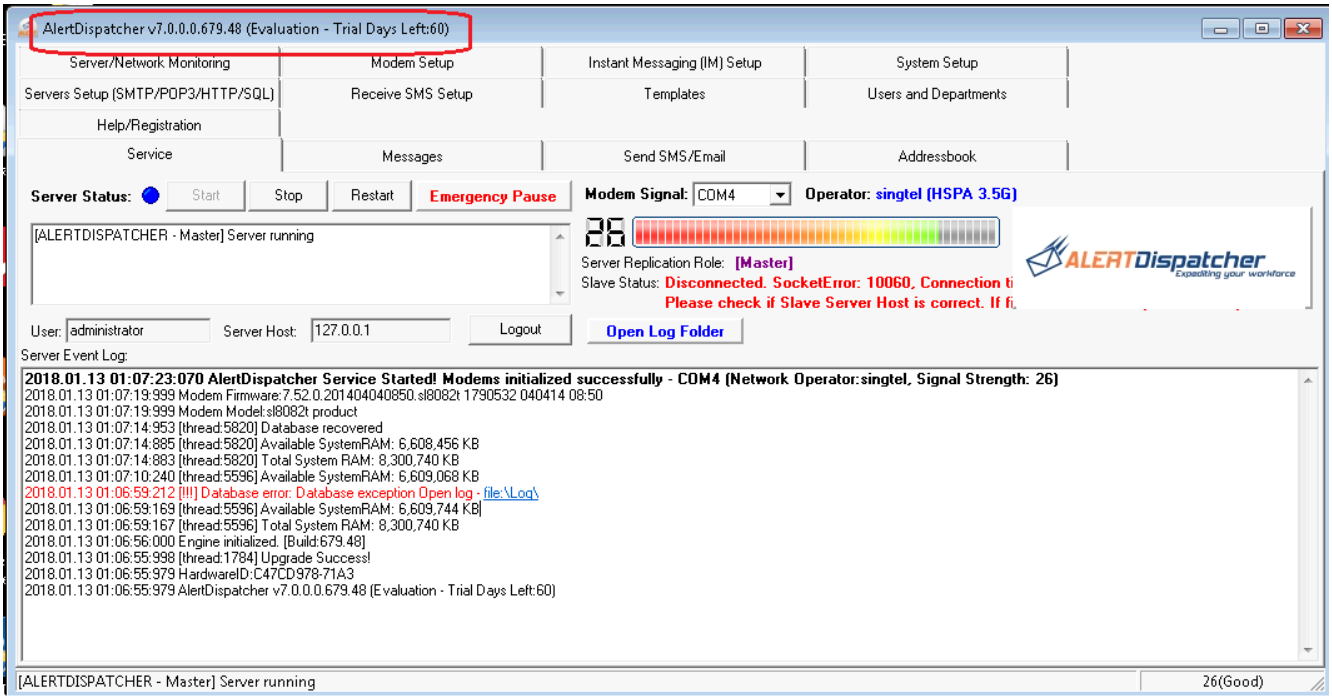
To obtain support from your vendor, you'll also need to submit your AlertDispatcher database and configuration. Refer to the *"Log Submission Guide"* on how to obtain the relevant files to your vendor for further technical assistance - http://www.clickndeploy.com/clients/dl.php?type=d&id=41



2. For Administrator

1). How to activate AlertDispatcher license using Activation Code

Once you have successfully setup and configured your AlertDispatcher installation, the software will work for 60 days without license activation. To use beyond 60 days, please activate your license by SMS or Internet.

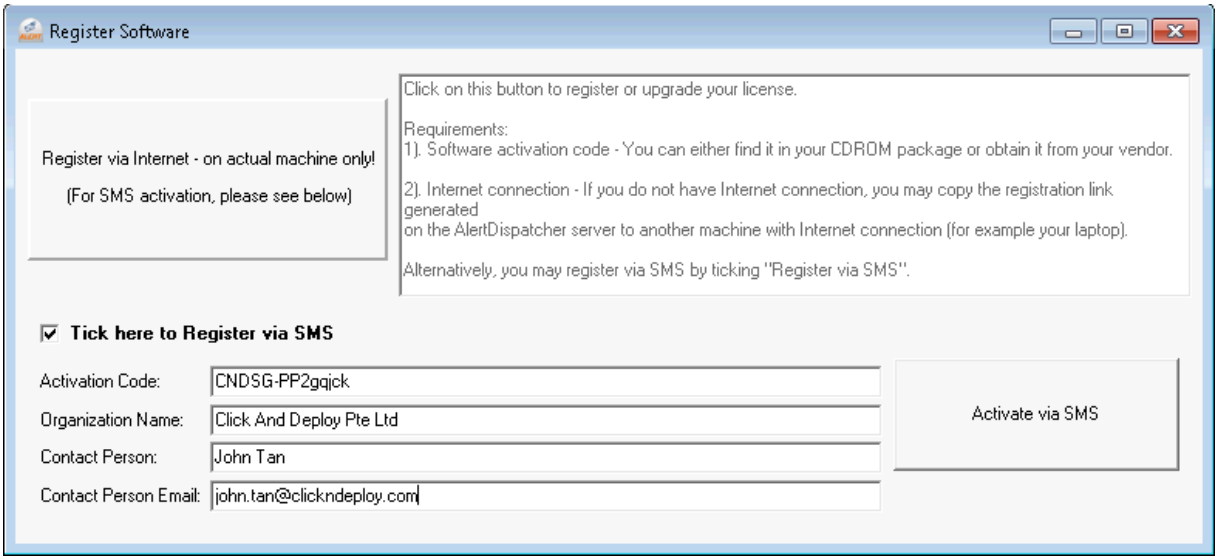


To register, run AlertDispatcher Client, and click on the *'Register Software'* button on the splash screen. Alternatively, you can launch AlertDispatcher Client and navigate to the *"Help/Registration"* Tab on the main page.

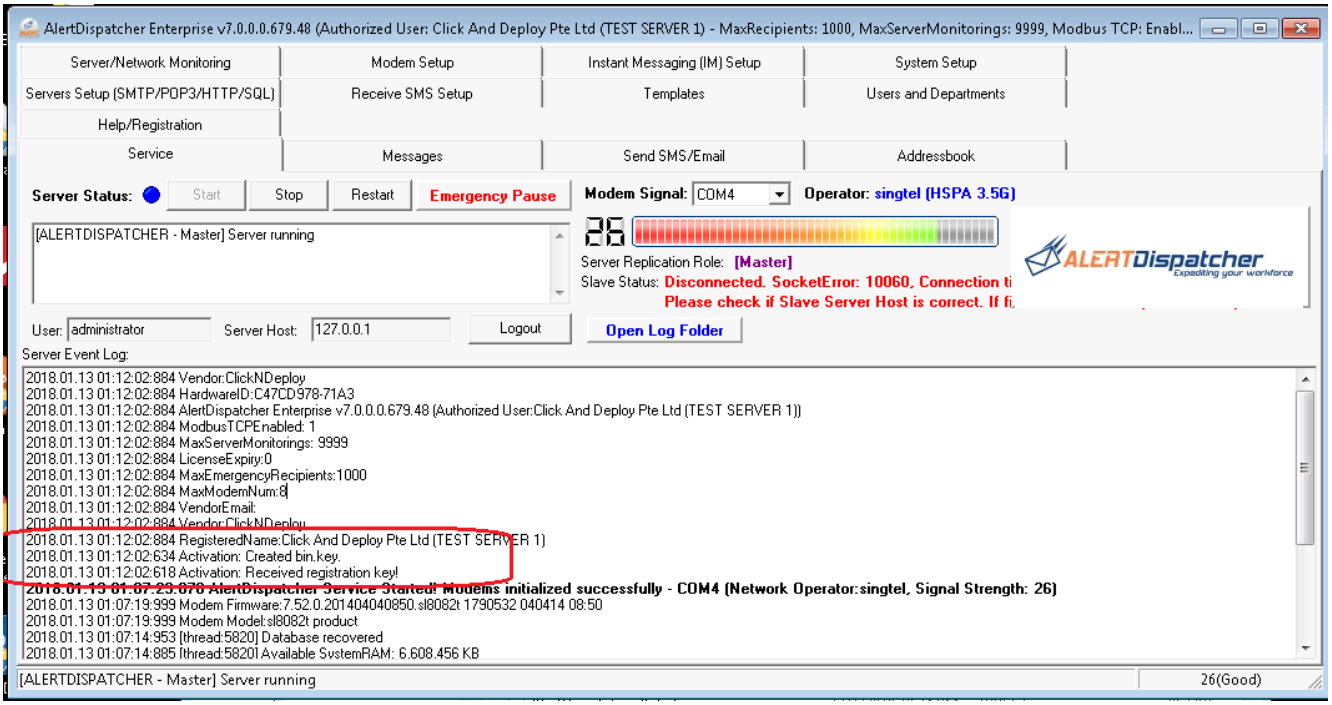
You may register via Internet or via SMS.

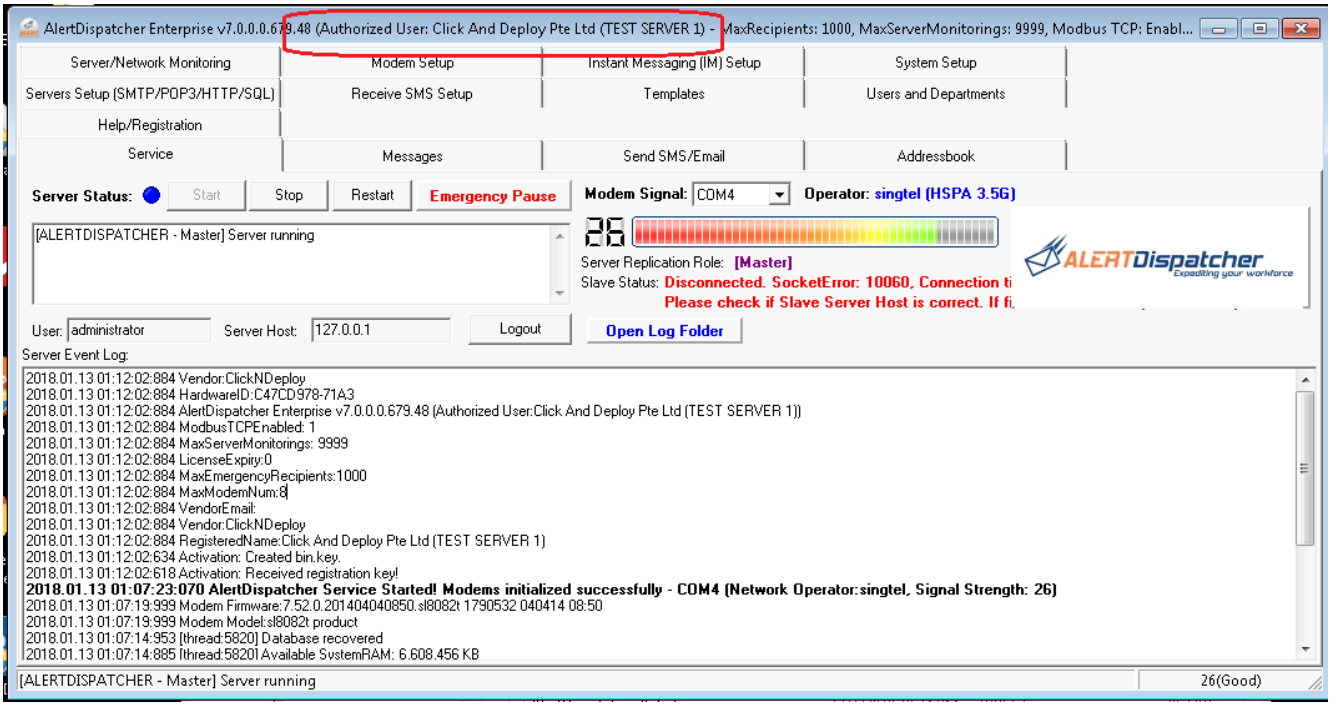
a). Register via SMS (Modem and SIM Card required)

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.



Upon receiving the license key via SMS, the "Evaluation - Trial Day Left" should be replaced by "Authorized User" as shown below. You may need to manually restart AlertDispatcher Service to see the new license.





If SMS activation don't work for you, you can activate via Internet 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 using AlertDispatcher installed on your laptop as the key generated using your laptop will work for your laptop but will fail to work on the server.

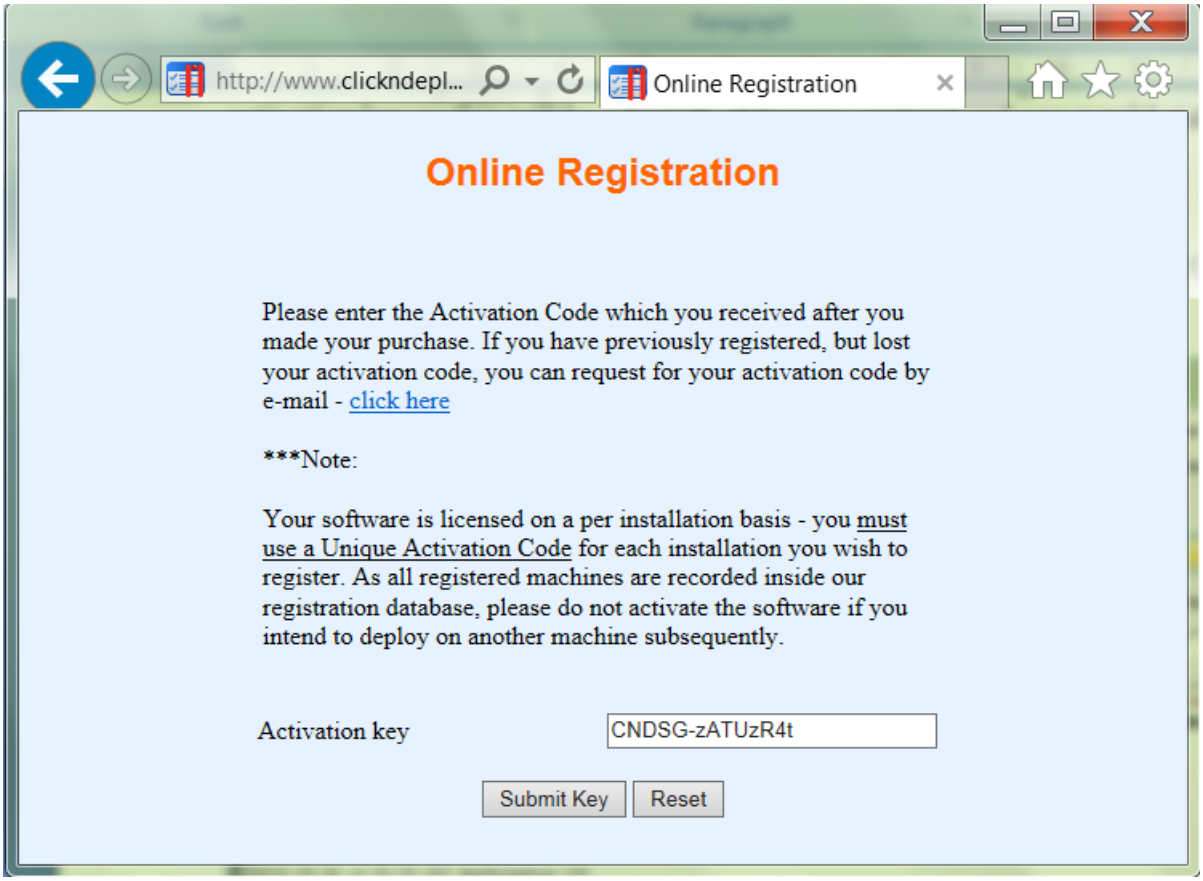
b). Register via Internet

After clicking "Register via Internet", enter your license Activation Code, e.g. "*CNDSG-zATUzR4t*".

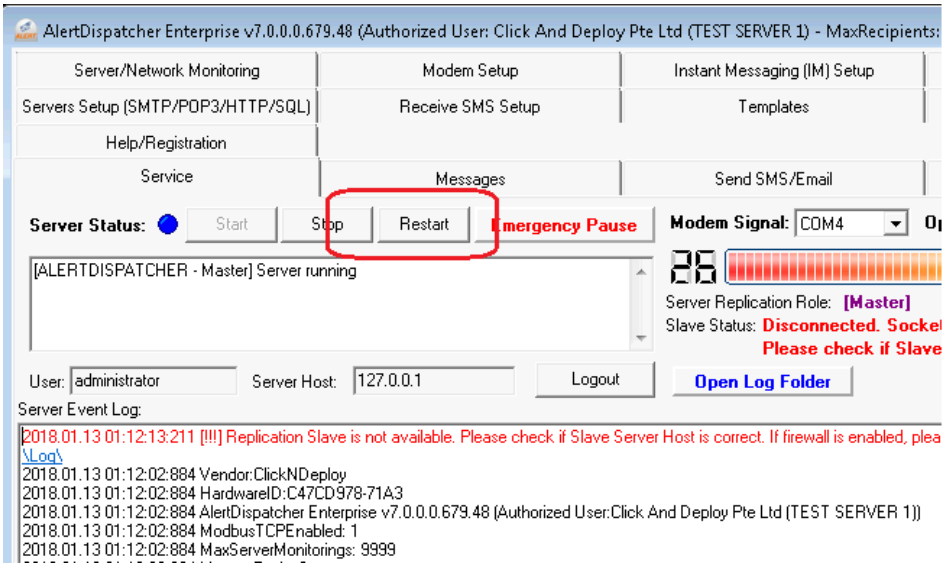
Note: If you do not have Internet access on your AlertDispatcher PC, you can copy the browser link generated on AlertDispatcher PC to a laptop or office PC with Internet access to continue with the registration. Please do not attempt to install AlertDispatcher on your laptop and try to perform the activation as the key won't work on the actual PC.

You can find the Activation Code 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.

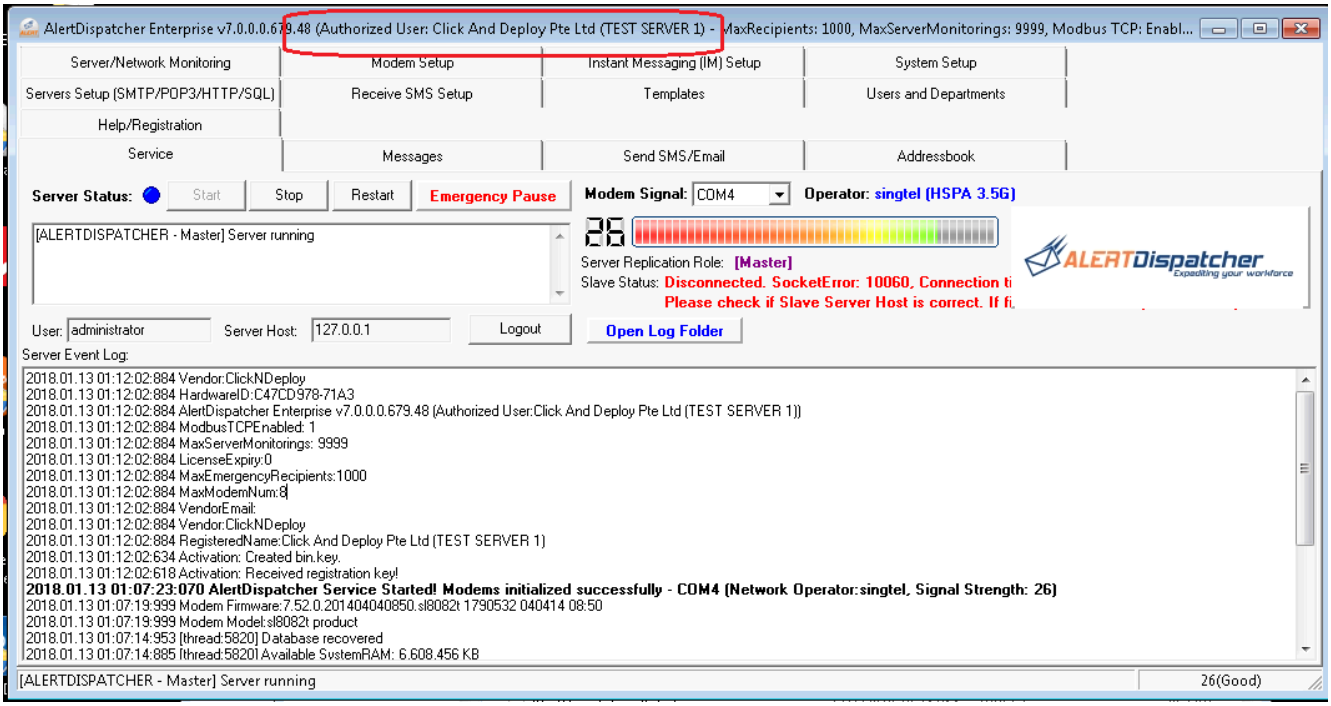
The Activation Code is unique to your machine; please do not use it to register multiple machines as it may cause the Activation Code to be voided.



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.



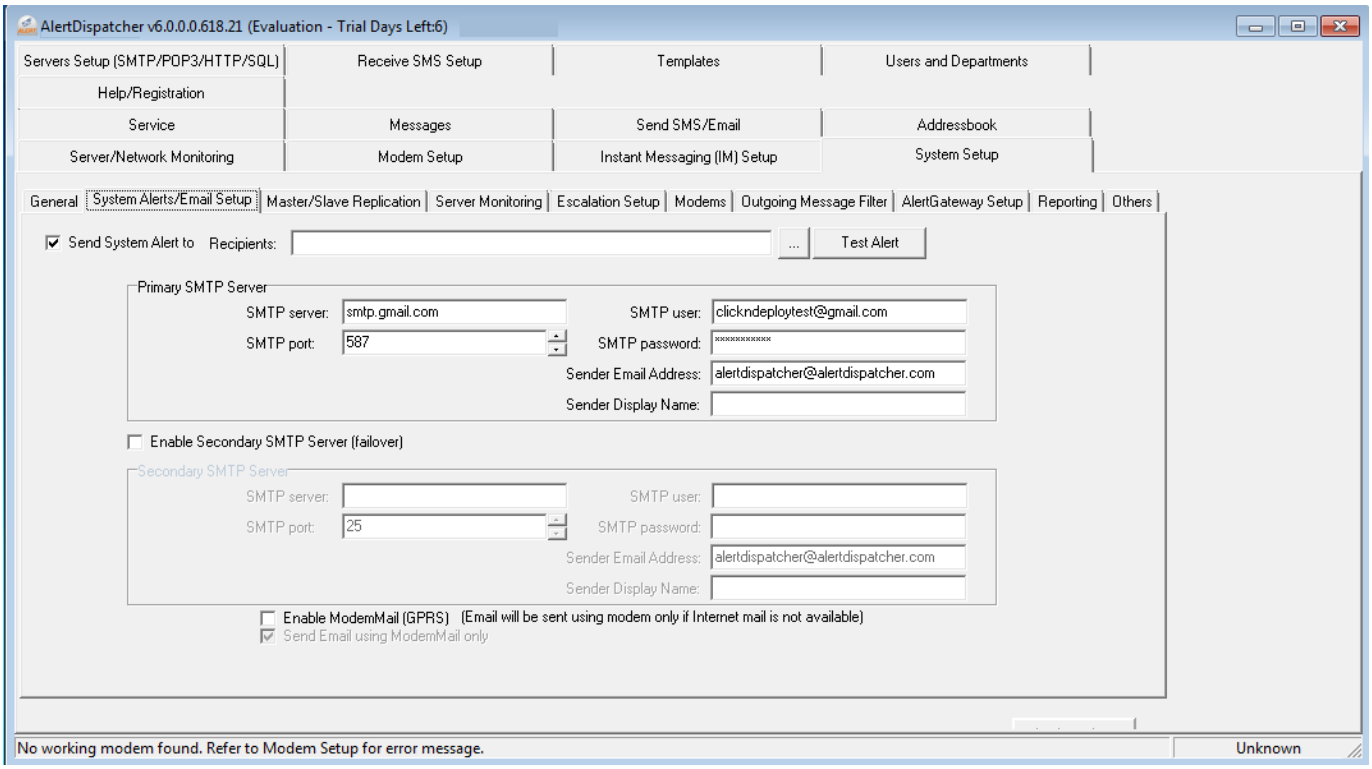
Upon successful activation, the "Evaluation - Trial Day Left" should be replaced by "Authorized User" as shown below.


AlertDispatcher Enterprise v7.0.0.0.679.48 (Authorized User: Click And Deploy Pte Ltd (TEST SERVER 1) - MaxRecipients: 1000, MaxServerMonitorings: 9999, Modbus TCP: Enabl...
Server/Network Monitoring
Modem Setup
Instant Messaging (IM) Setup
System Setup
Servers Setup (SMTP/POP3/HTTP/SQL)
Receive SMS Setup
Templates
Users and Departments
Help/Registration
Service
Messages
Send SMS/Email
Addressbook
Server Status:
Start
Stop
Restart
Emergency Pause
Modem Signal: COM4
Operator: singtel (HSPA 3.5G)
[ALERTDISPATCHER - Master] Server running
26
Server Replication Role: [Master]
Slave Status: Disconnected. SocketError: 10060, Connection ti
Please check if Slave Server Host is correct. If fi
ALERTDispatcher
Expediting your workforce
User: administrator
Server Host: 127.0.0.1
Logout
Open Log Folder
Server Event Log:
2018.01.13 01:12:02:884 Vendor:ClickNDeploy
2018.01.13 01:12:02:884 HardwareID:C47CD978-71A3
2018.01.13 01:12:02:884 AlertDispatcher Enterprise v7.0.0.0.679.48 (Authorized User:Click And Deploy Pte Ltd (TEST SERVER 1))
2018.01.13 01:12:02:884 ModbusTCPEnabled: 1
2018.01.13 01:12:02:884 MaxServerMonitorings: 9999
2018.01.13 01:12:02:884 LicenseExpiry:0
2018.01.13 01:12:02:884 MaxEmergencyRecipients:1000
2018.01.13 01:12:02:884 MaxModemNum:8
2018.01.13 01:12:02:884 VendorEmail:
2018.01.13 01:12:02:884 Vendor:ClickNDeploy
2018.01.13 01:12:02:884 RegisteredName:Click And Deploy Pte Ltd (TEST SERVER 1)
2018.01.13 01:12:02:634 Activation: Created bin.key.
2018.01.13 01:12:02:618 Activation: Received registration key!
2018.01.13 01:07:23:070 AlertDispatcher Service Started! Modems initialized successfully - COM4 (Network Operator:singtel, Signal Strength: 26)
2018.01.13 01:07:19:999 Modem Firmware:7.52.0.201404040850.sl8082t 1790532 040414 08:50
2018.01.13 01:07:19:999 Modem Model:sl8082t product
2018.01.13 01:07:14:953 [thread:5820] Database recovered
2018.01.13 01:07:14:885 [thread:5820] Available SystemRAM: 6.608.456 KB
[ALERTDISPATCHER - Master] Server running
26(Good)

2). How to setup AlertDispatcher to send Email/Alert Emails

In order for AlertDispatcher to send out Emails, you must configure the Primary SMTP Server 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 a critical purpose.

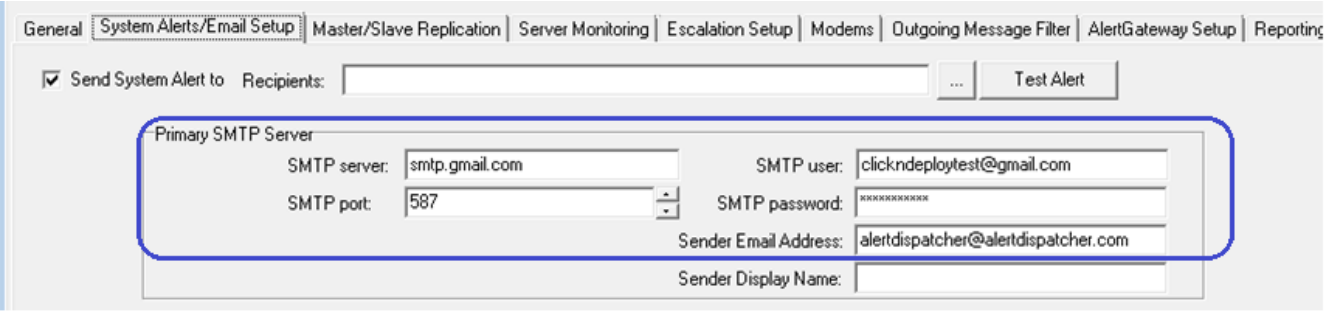


a). Configure Primary SMTP Server and credentials and Gmail SMTP example

Obtain the following SMTP Server settings from your company email administrator and ensure the firewalls are opened for the SMTP Server port and AlertDispatcher Server IP address. Note that username and password is not always required.

1. SMTP Server address (IP address or hostname).
2. SMTP Server port, e.g. port 25.
3. SMTP username (if authentication is required).
4. SMTP password (if authentication is required).
5. Sender Email address (required for some email servers).

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



Note:

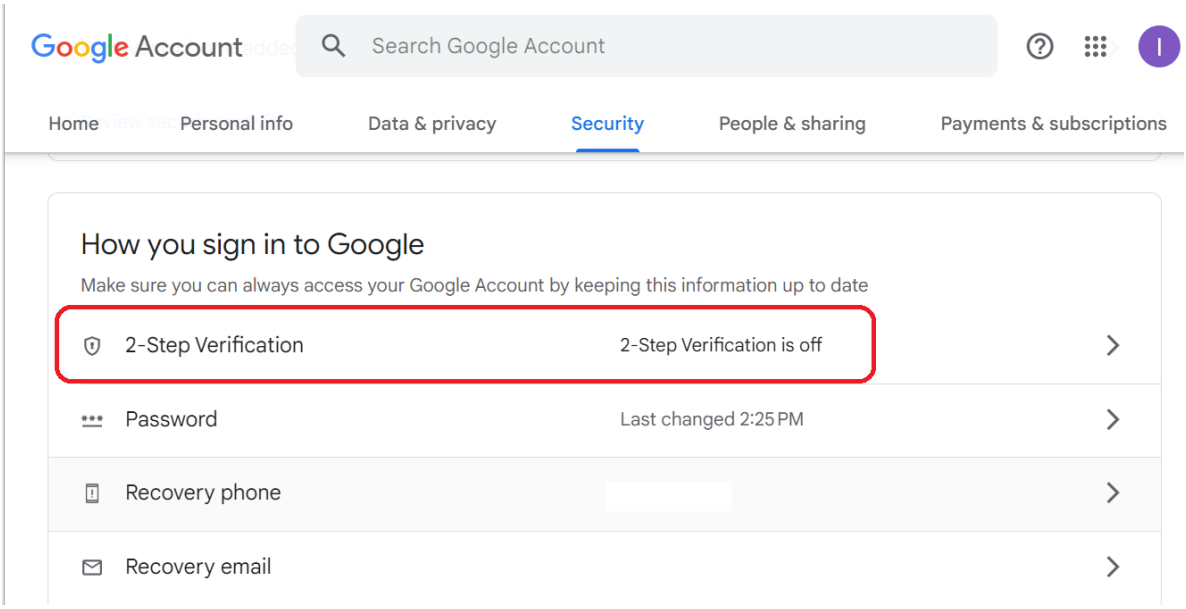
1). As far as possible, do not use your email account or an existing email account just in case you need to change your password in the future, and forget to update the password set on AlertDispatcher. Create a new email account, e.g. alertdispatcher@yourcompanydomain.

2). If you do not have a company email or 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 2000 emails a day.

In order to enable SMTP access from your setup, you must also login to your GMAIL account on the same workstation you installed AlertDispatcher and perform the following steps:

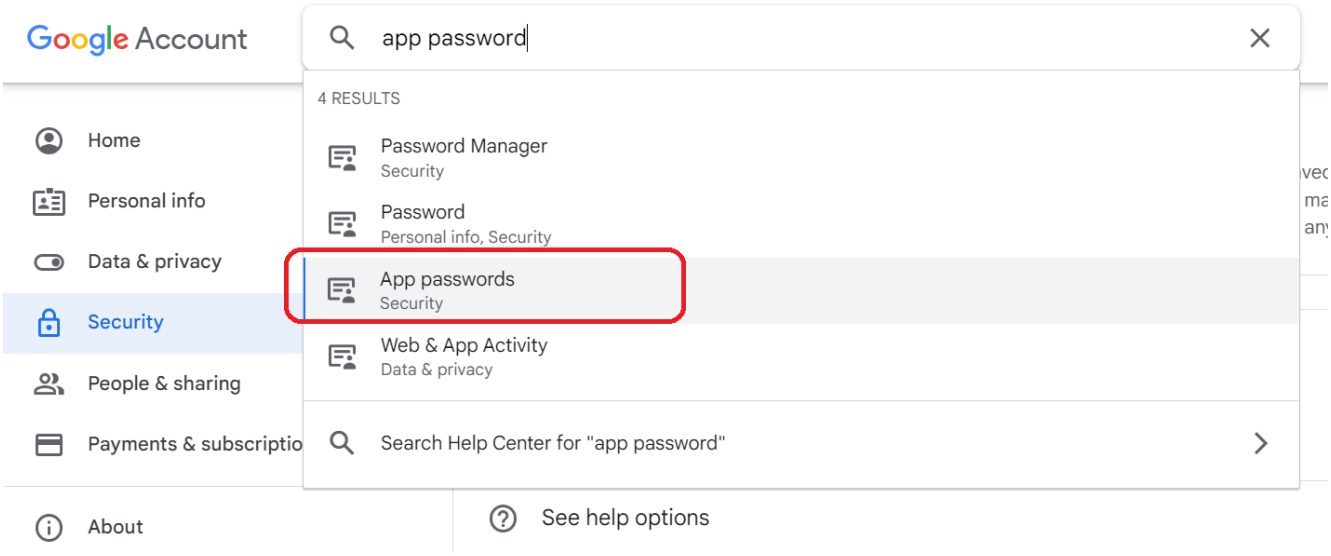
<u>1. Enable 2-Step Verification.</u>

After you have created the Gmail account, go to Google account, Security and enable 2-Step Verification. This is needed to be able to setup an App password that you can use to send emails from AlertDispatcher.

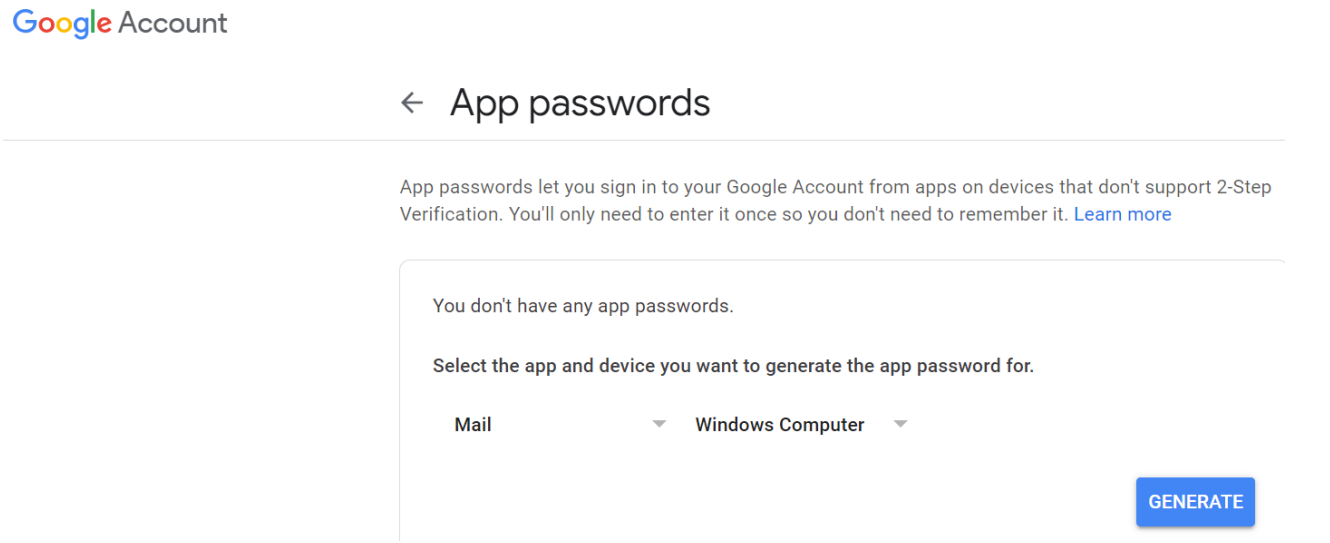


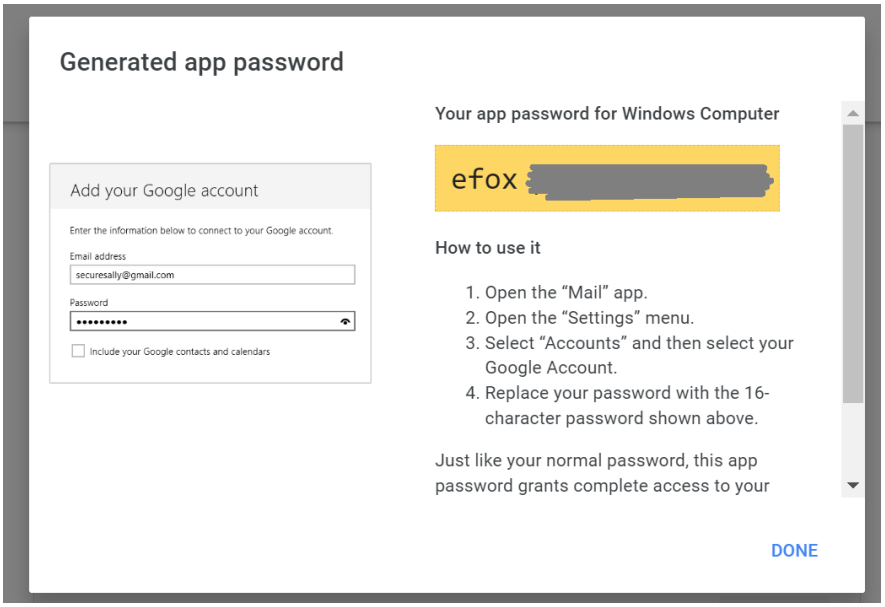
2. Generate App password

Search for App passwords.



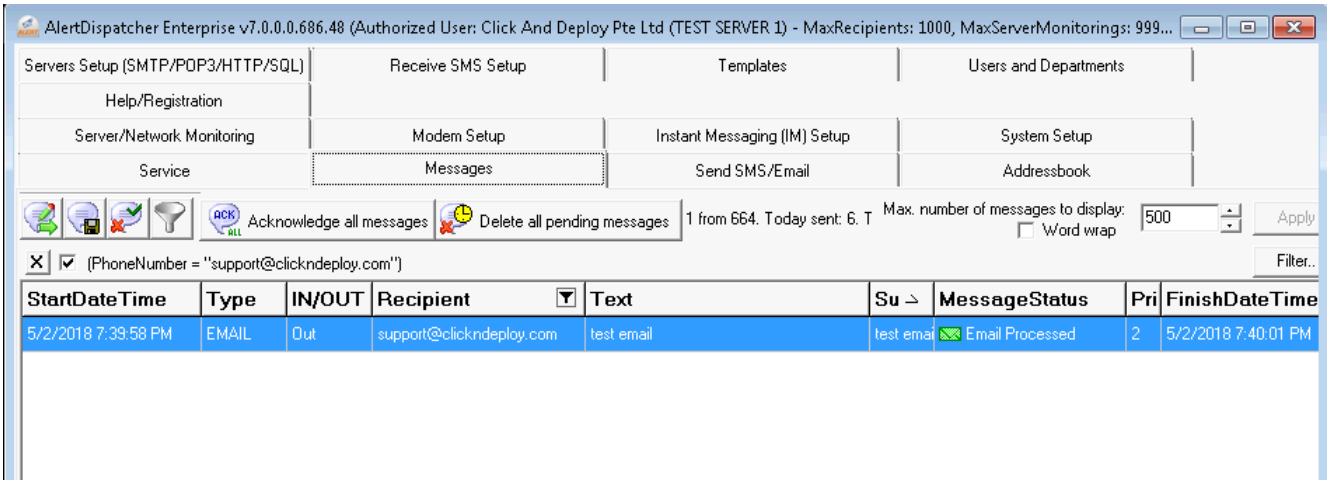
Generate App password.



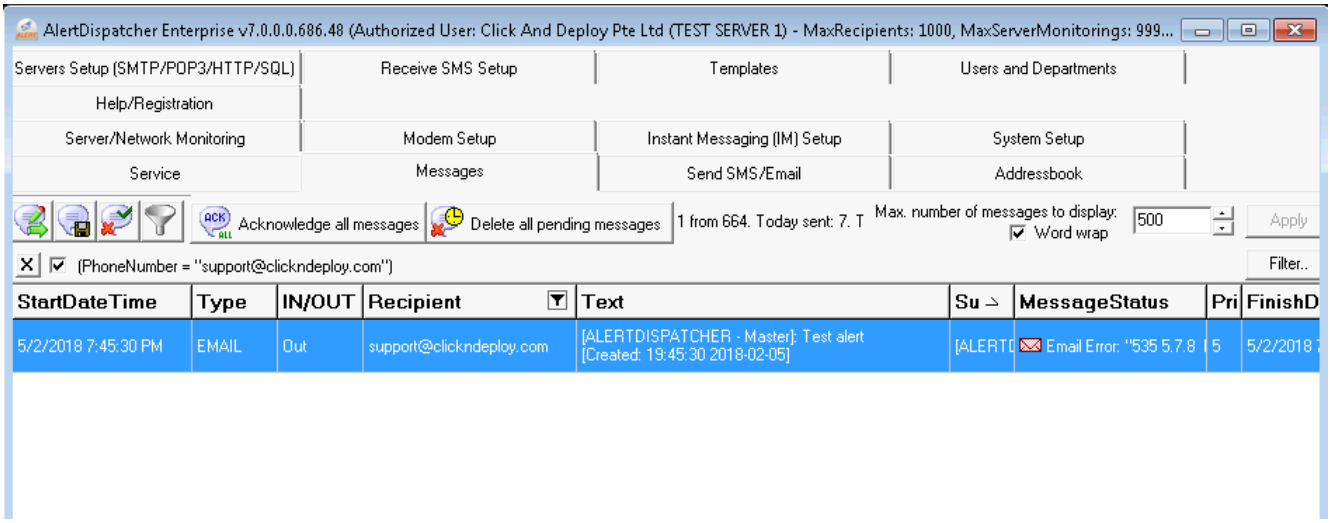


This app password will be your SMTP password (instead of your Gmail password).

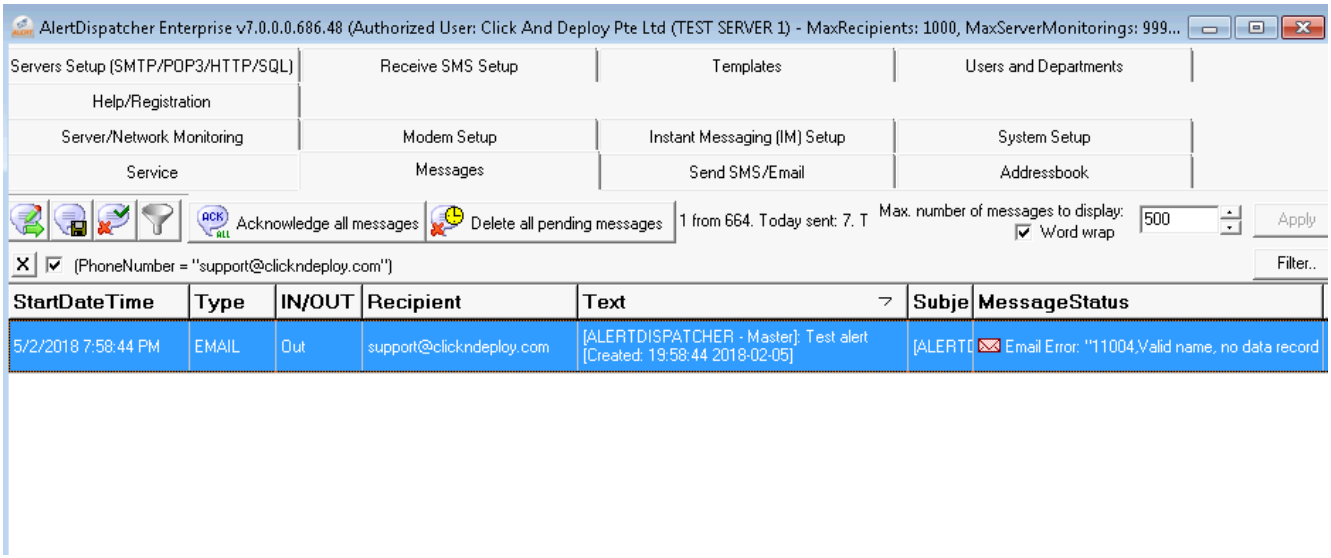
The following screen shows a successful test.



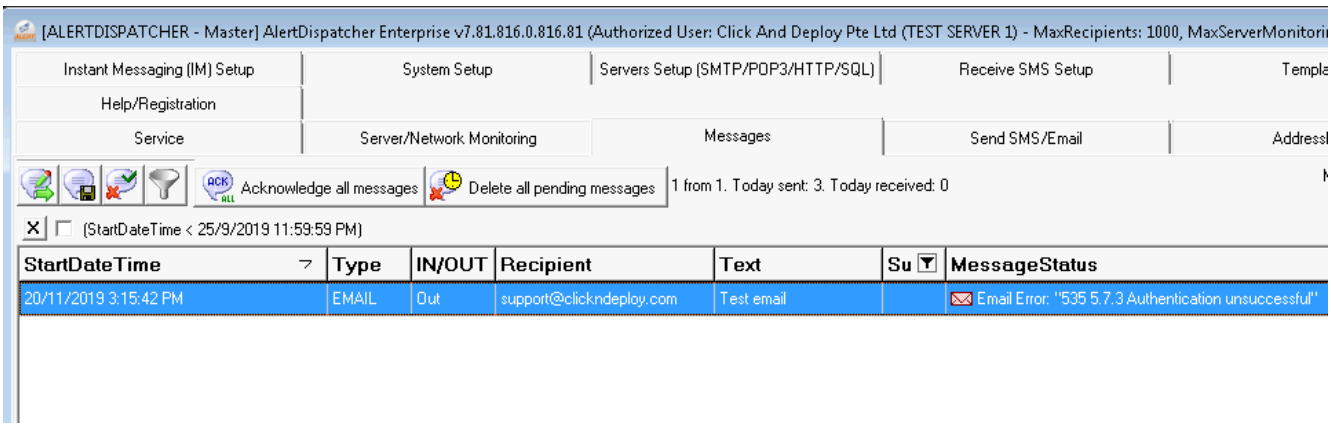
If the SMTP Server setup is not correctly configured or if your AlertDispatcher hasn't been authorized to send email to the SMTP Server, the error will be shown under MessageStatus column. Please show this error to your company email server administrator.



Error: "11004,Valid name, no data record of requested type" is a socket error, and indicates that AlertDispatcher is unable to connect to the SMTP Server. Please check if the configured Primary SMTP Server and Port are correct, and there is no firewall blocking the connection.



If the SMTP Server is configured correctly and there is network connectivity but the email is still being rejected by the SMTP Server, you might receive the following error:

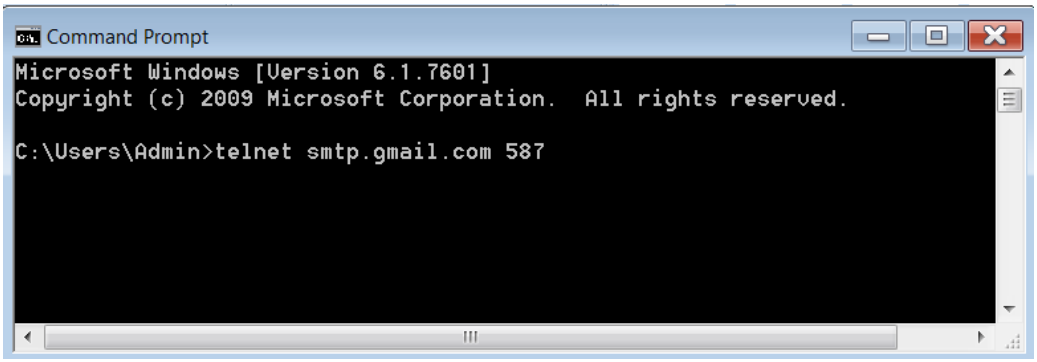


Please check EmailSenderSMTPDebug.log - refer to 5). How to Retrieve Logs for Troubleshooting

b). How to verify your SMTP Server credentials using Windows Telnet Client and Blat.

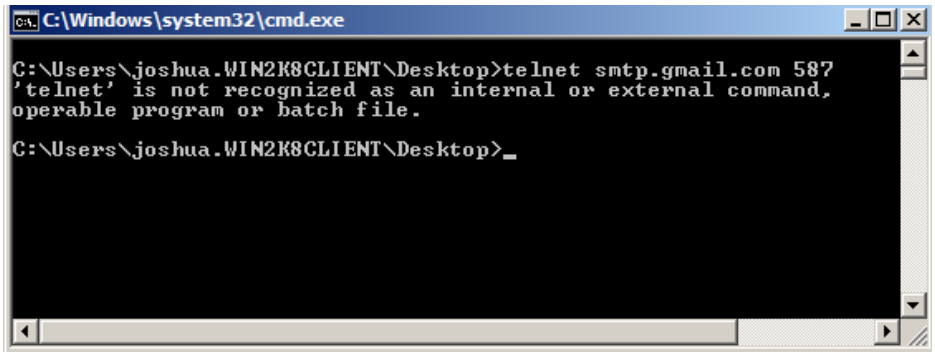
You can use Windows Telnet Client to check network connectivity and open port access to the SMTP Server. To determine if your SMTP Server credentials are correct, you will need to use an SMTP client such as Blat - Blat is a free command-line based SMTP client.

On your AlertDispatcher installation, launch Telnet client to verify that you are able to connect to the SMTP Server. The following example tries to connect to GMAIL SMTP Server at port 587. Note: Your corporate email server may use port 25 instead,

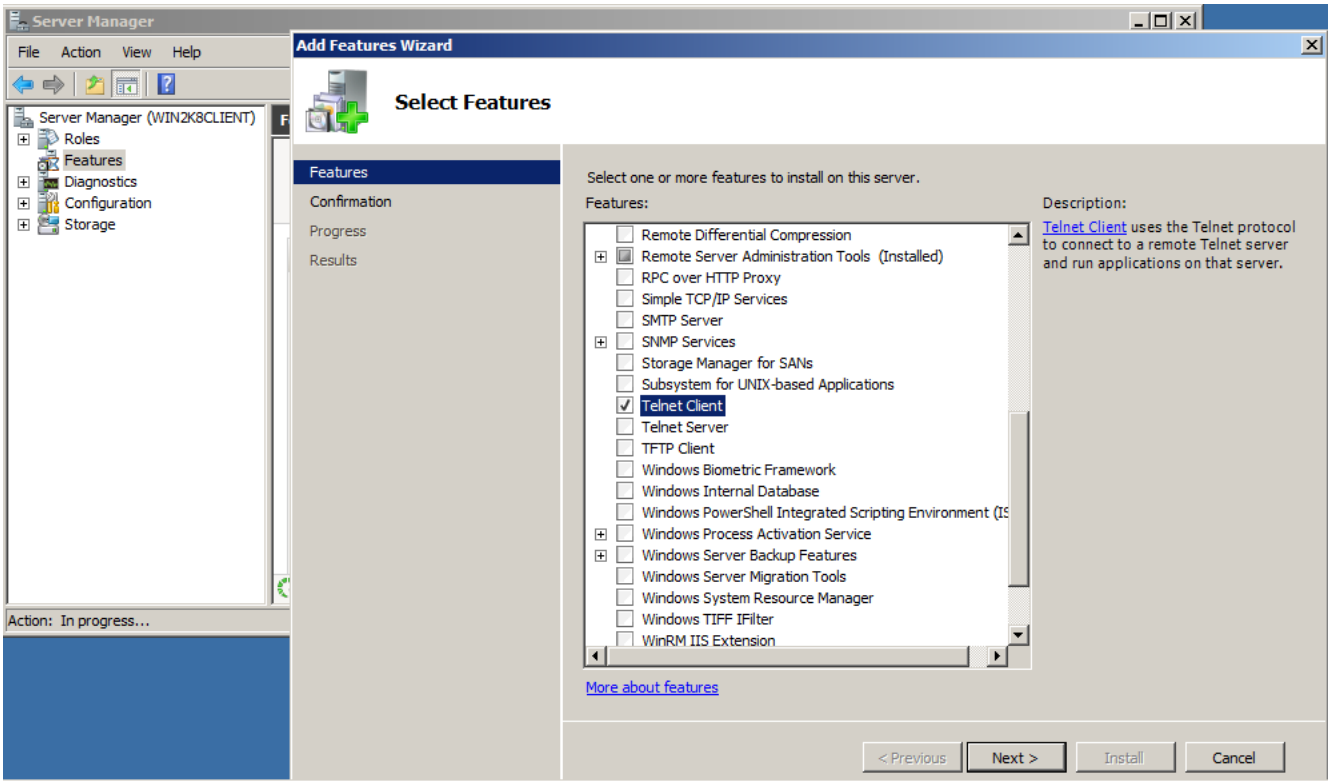


On successful connection, it will return the code "220".

If you're getting the error "'telnet' is not recognized as an internal or external command", this means Telnet Client is not installed on your Windows machine.



To install Telnet Client, go to *Windows Control panel -> Programs and Features -> Turn Windows features on or off -> Server Manager -> Features -> Add Feature*, and then add Telnet Client.



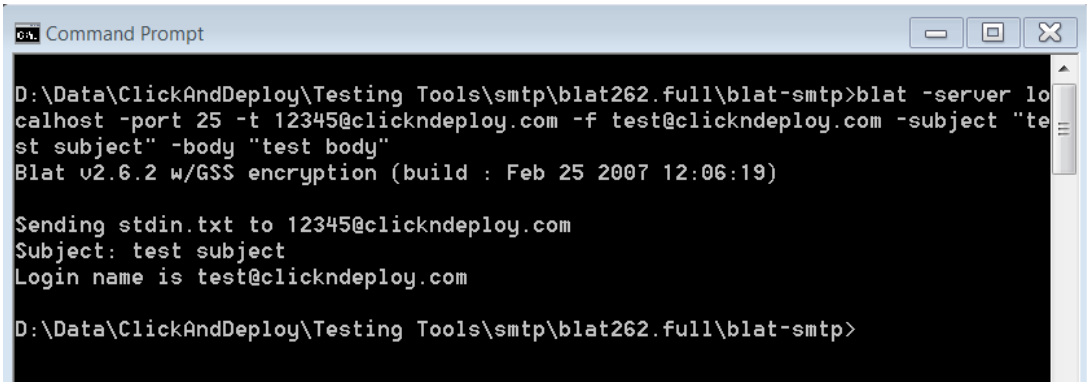
If Telnet works, but you're still not able to send email successfully, you can test using the free command line SMTP client Blat which you can download from http://www.clickndeploy.com/downloads/blat-smtp.zip.

For testing with SMTP Server without authentication:

blat -server {smtp-server-hostname} -port {smtp-port} -t {to-recipient} -f {sender-email} -subject {email-subject} -body {email-body}

Example:

blat -server localhost -port 25 -t 12345@clickndeploy.com -f test@clickndeploy.com -subject "test subject" -body "test body"



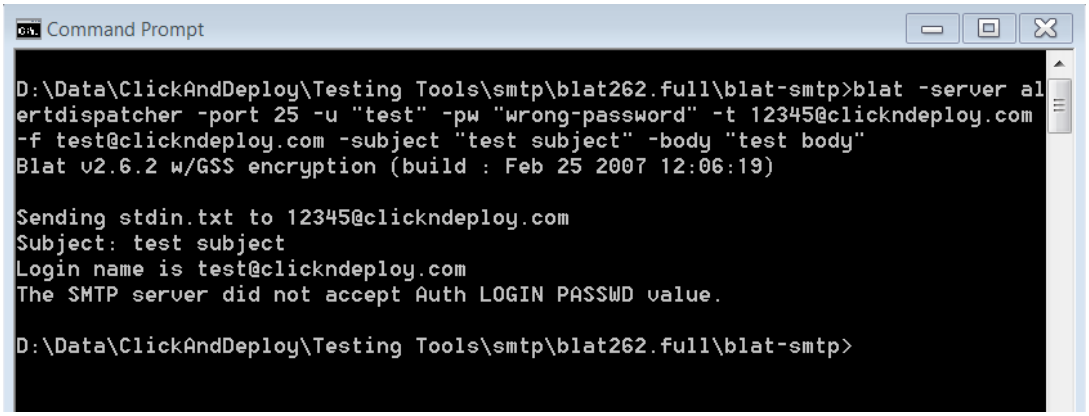
For testing with SMTP Server with authentication:

blat -server {smtp-server-hostname} -port {smtp-port} -u {username} -pw {password} -t {to-recipient} -f {sender-email} -subject {email-subject} -body {email-body}

Example:

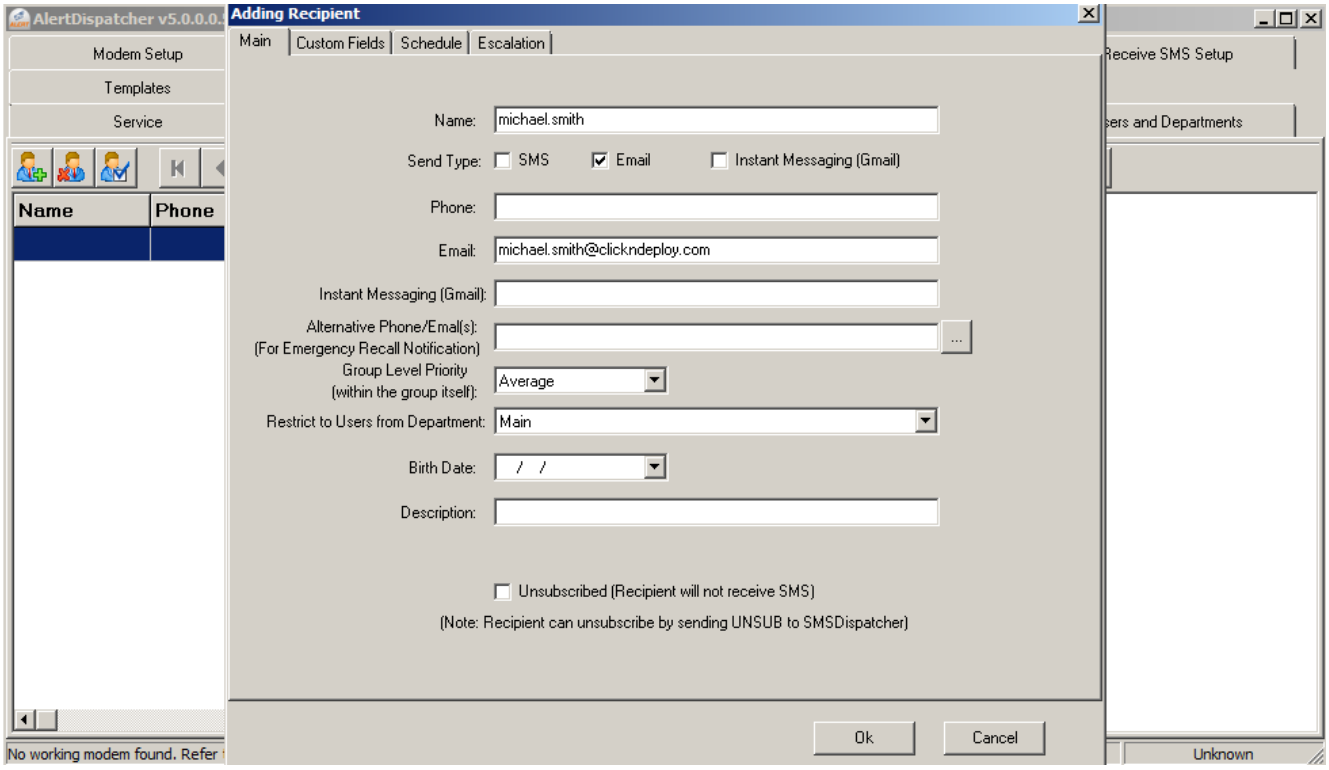
blat -server localhost -port 25 -u "test" -pw "test" -t 12345@clickndeploy.com -f test@clickndeploy.com -subject "test subject" -body "test body"

If password is wrong:



c). Configure email recipients in the Addressbook

To send email through the Addressbook, you can add the recipient email address as shown below.


AlertDispatcher v5.0.0.0
Modem Setup
Templates
Service
Name
Phone
No working modem found. Refer
Adding Recipient
Main
Custom Fields
Schedule
Escalation
Name: michael.smith
Send Type: SMS Email Instant Messaging (Gmail)
Phone:
Email: michael.smith@clickndeploy.com
Instant Messaging (Gmail):
Alternative Phone/Emal(s):
(For Emergency Recall Notification)
Group Level Priority
(within the group itself): Average
Restrict to Users from Department: Main
Birth Date: / /
Description:
Unsubscribed (Recipient will not receive SMS)
(Note: Recipient can unsubscribe by sending UNSUB to SMSDispatcher)
Ok
Cancel
Receive SMS Setup
sers and Departments
Unknown

3). How to setup AlertDispatcher High Availability (Master/Slave Cluster Redundancy)

If you are using the Enterprise License, you can setup Master/Slave cluster redundancy on AlertDispatcher installations using 2 different *"Operation Modes"*, a). *Active Master/Active Slave* (default), b). *Active Master/Passive Slave*.

When configured as *"Active Master/Active Slave cluster"* (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. To ensure that there is no duplicate messages, the interfacing application should only send to one node at any one time and be able to enact a failover to the other node.

When configured as *"Active Master/Passive Slave cluster"*, messages sent by the interfacing application to the 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:

1. For both operation modes, changes to Users, Addressbook, Template, System Alert Recipient and Daily Heartbeat setting can only be done on the Master node and will be replicated to the Slave node.

Modem settings including the required NPort setting "Modems are connected to IP network, cater for modem response…" are to be configured or enabled separately on Master and Slave node separately.

2. A redundant server is only useful if it works, configure Heartbeat / Healthcheck alerts to be sent once or twice daily for both Master and Slave nodes - refer to page 20 of the "AlertDispatcher Quick Installation Guide.pdf"

a). Active Master/Active Slave Operation Mode

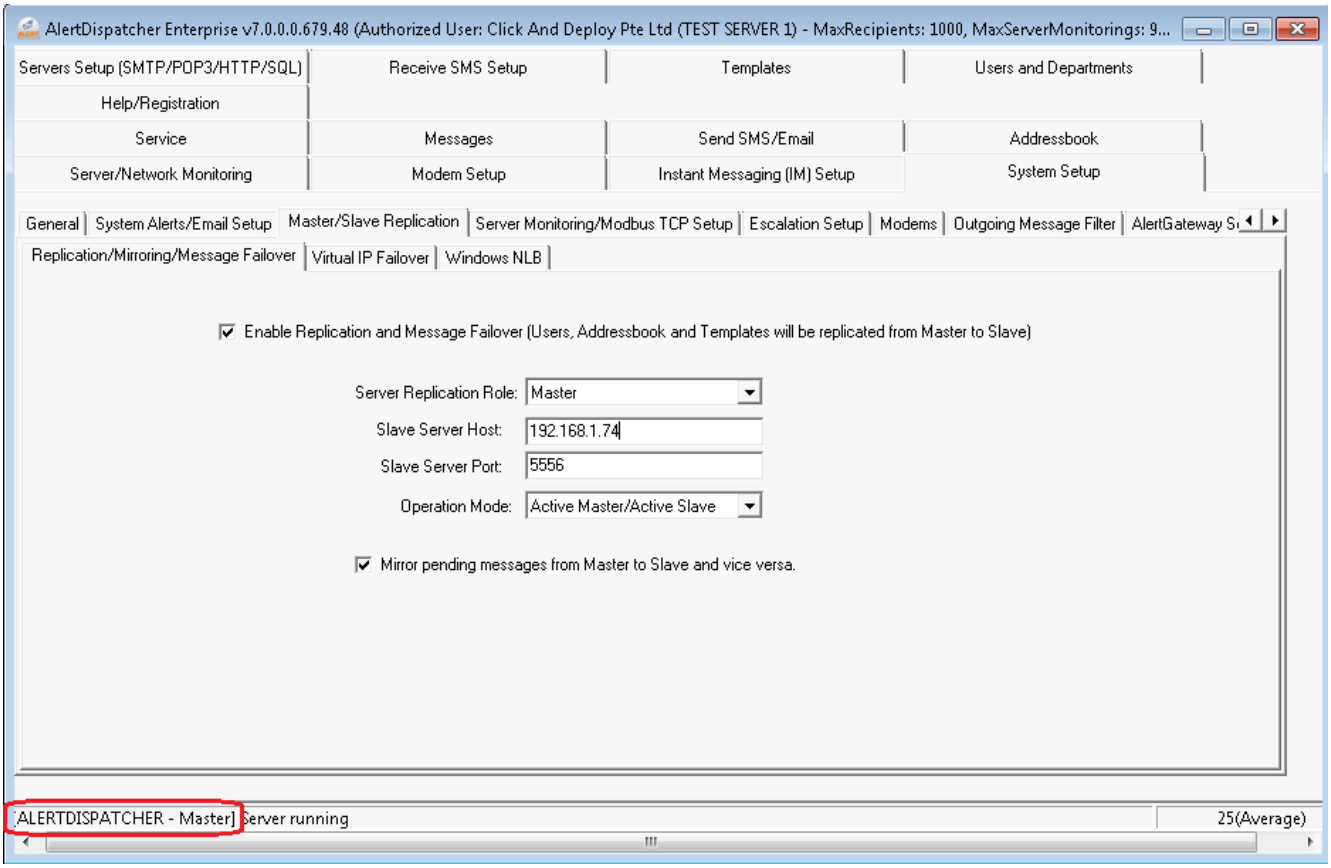
To configure your AlertDispatcher as Active Master/Active Slave, first enable the setting *"Enable Replication and Message Failover (Users, Addressbook and Templates will be replicated from Master to Slave)"* to enable automatic message failover (both ways) across the Master and the Slave node.

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.

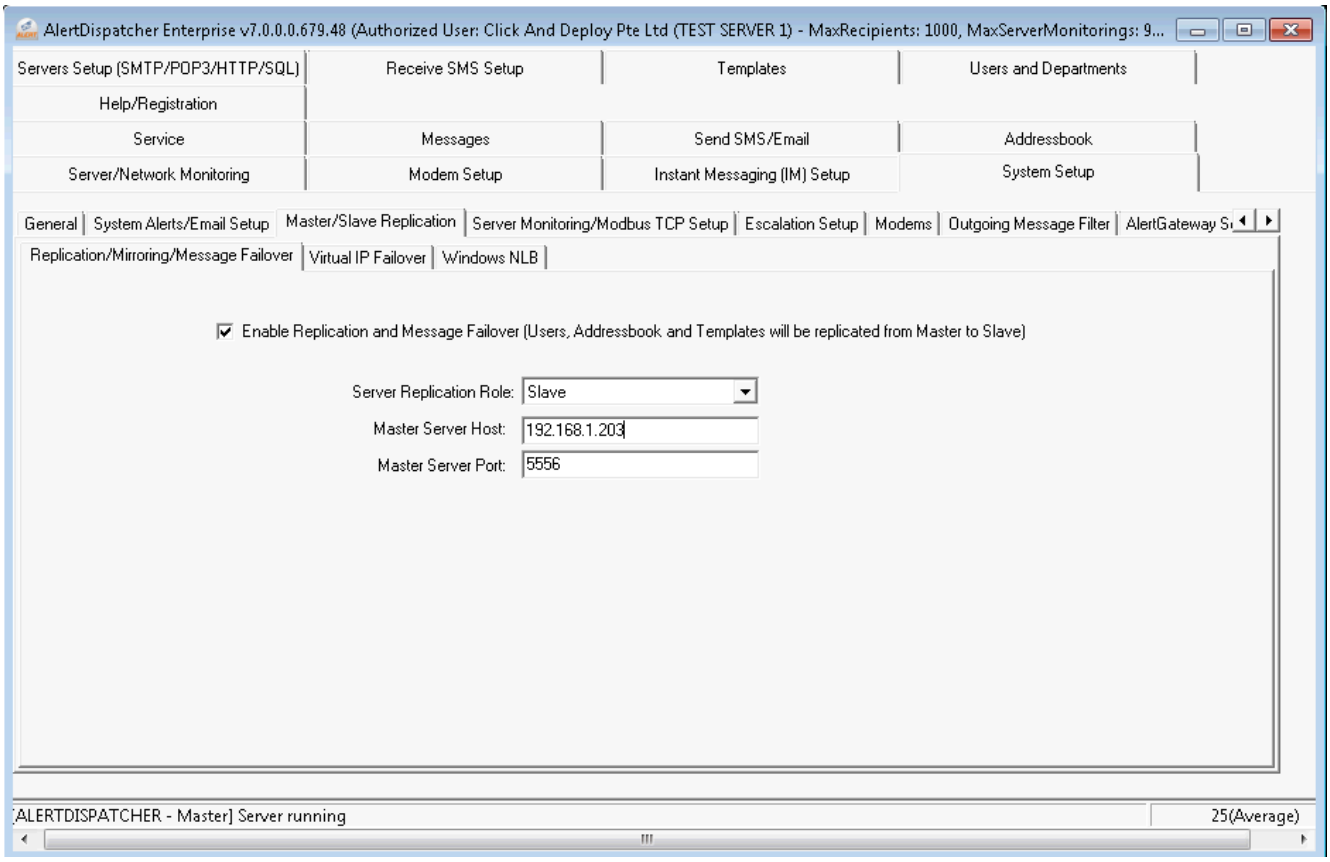
Note: Firewall may prevent Master and Server from connecting to each other so if you have firewall enabled on either or both servers, please add firewall rule to "allow" AlertDispatcher TCP port 5556. Refer to Appendix A - How to Add (allow) server ports to Firewall.

In the following example, the Active Master node IP address is 192.168.1.203 and the Active Slave node IP address is 192.168.1.74.

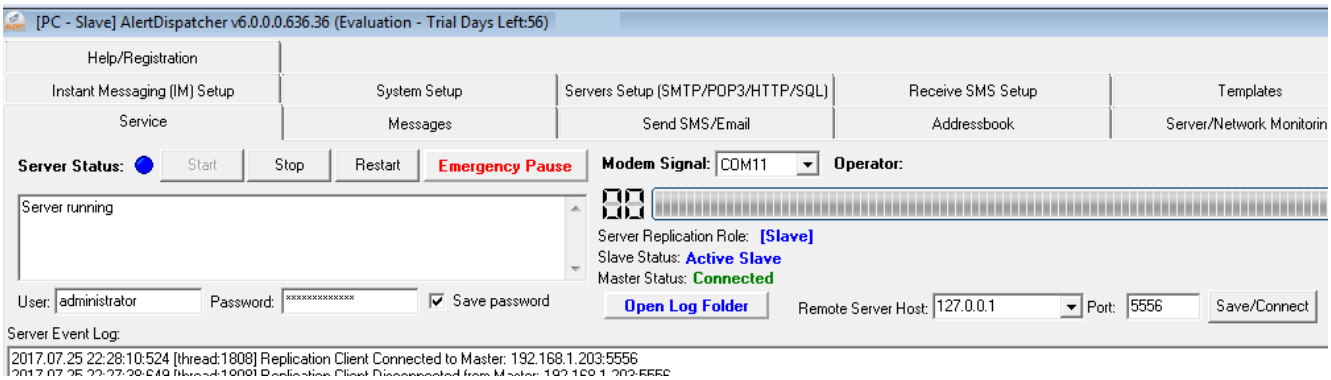
Active Master Node:



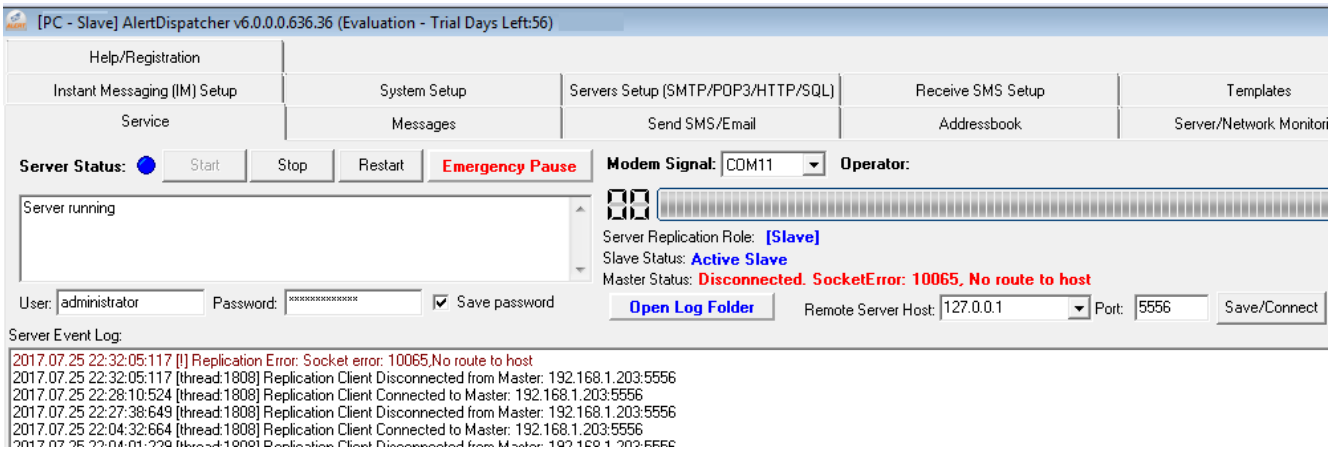
Active Slave Node:



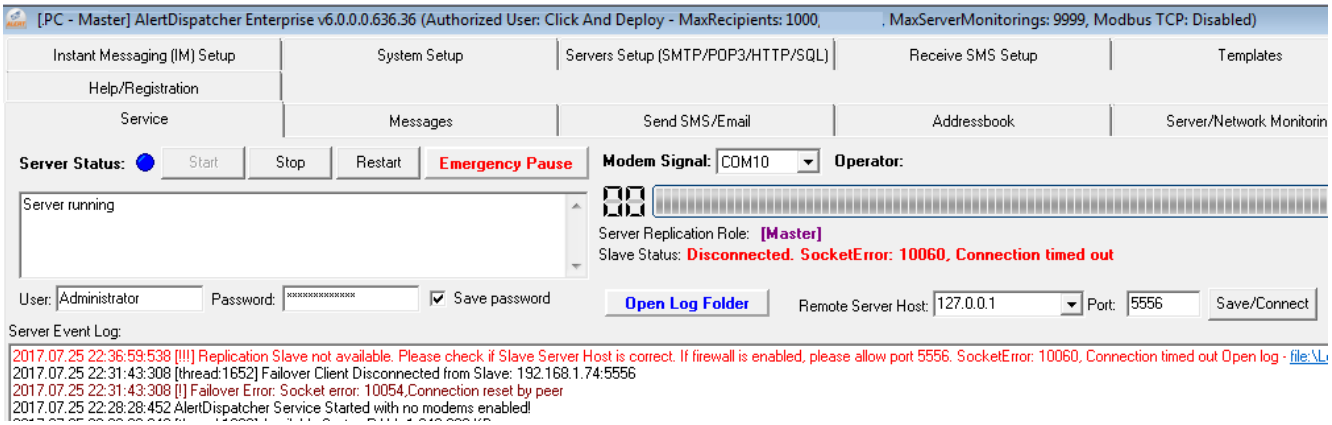
The connection status to the Active Master is displayed on the Active Slave. The following screen shows Active Slave as connected to the Active Master.



The following shows Active Slave as disconnected from the Active Master.



The disconnected status is also displayed on the Active Master.



b). Active Master/Passive Slave Operation Mode

To configure your AlertDispatcher as Active Master/Passive Slave, first 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.

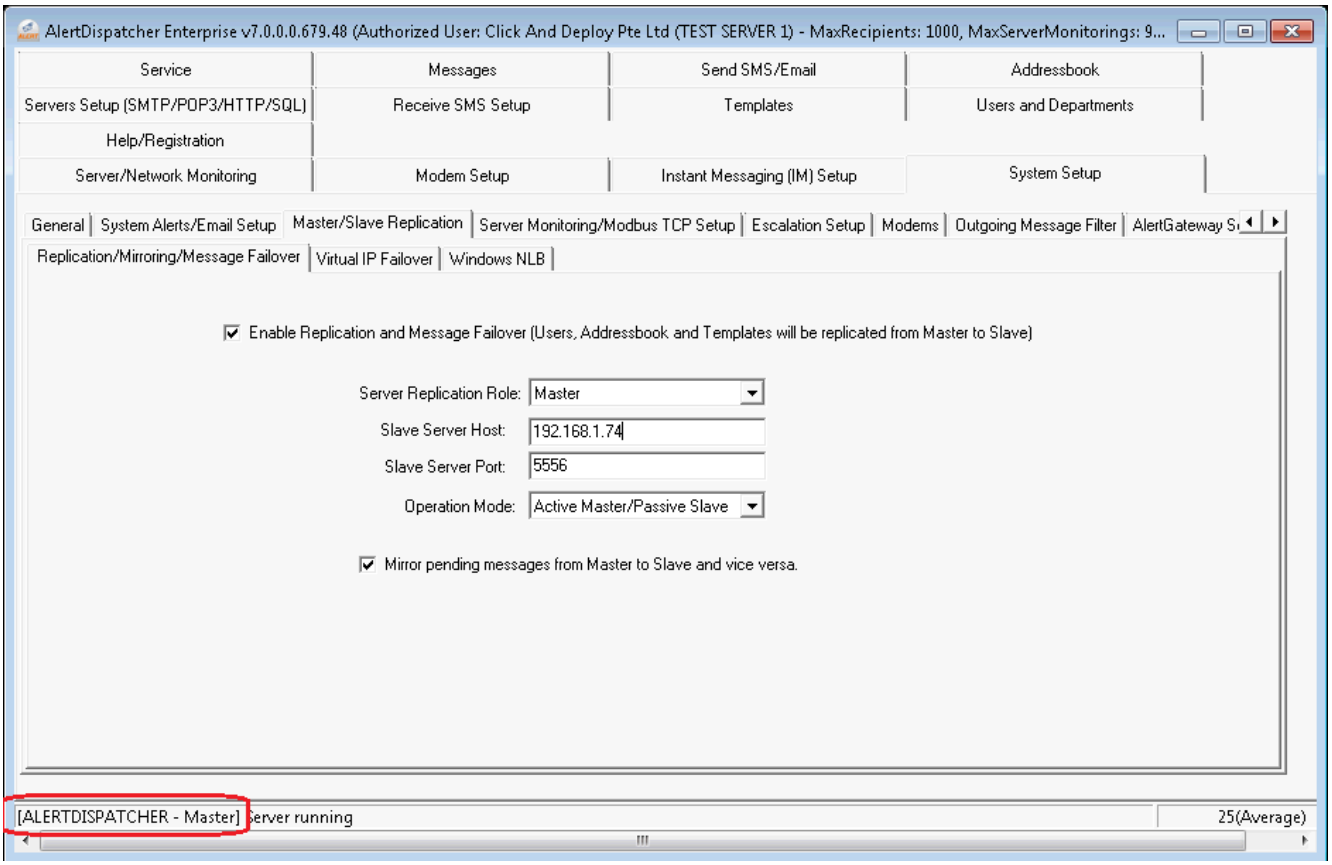
The *"Enable Replication and Message Failover"* setting does not ensure message persistency, so messages already queued on a node that failed will be lost. To ensure message persistency, you need to enable an additional setting "Mirror pending messages from Master to Slave and vice versa".

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.

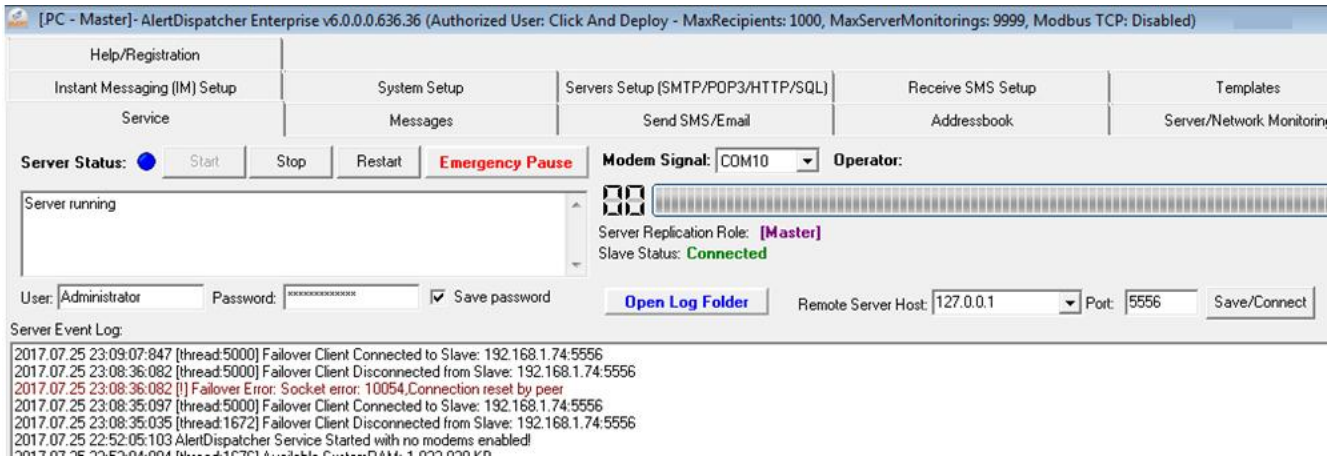
Note: Firewall may prevent Master and Server from connecting to each other so if you have firewall enabled on either or both servers, please add firewall rule to "allow" AlertDispatcher TCP port 5556. Refer to Appendix A - How to Add (allow) server ports to Firewall.

In the following example, the Active Master node IP address is 192.168.1.203 and the Passive Slave node IP address is 192.168.1.74.

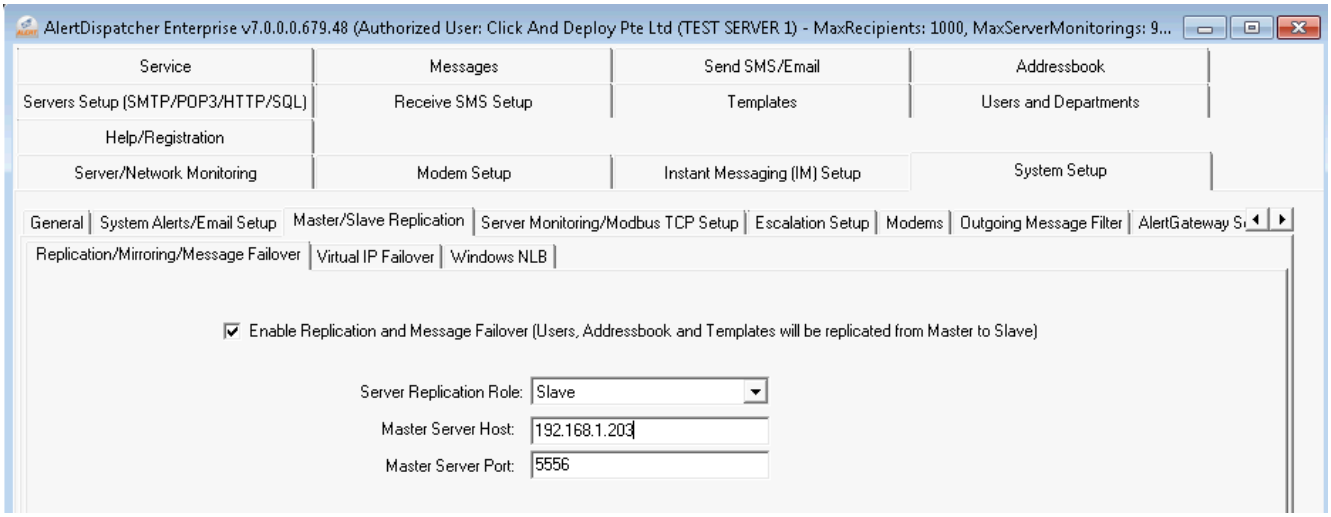
Active Master Node:



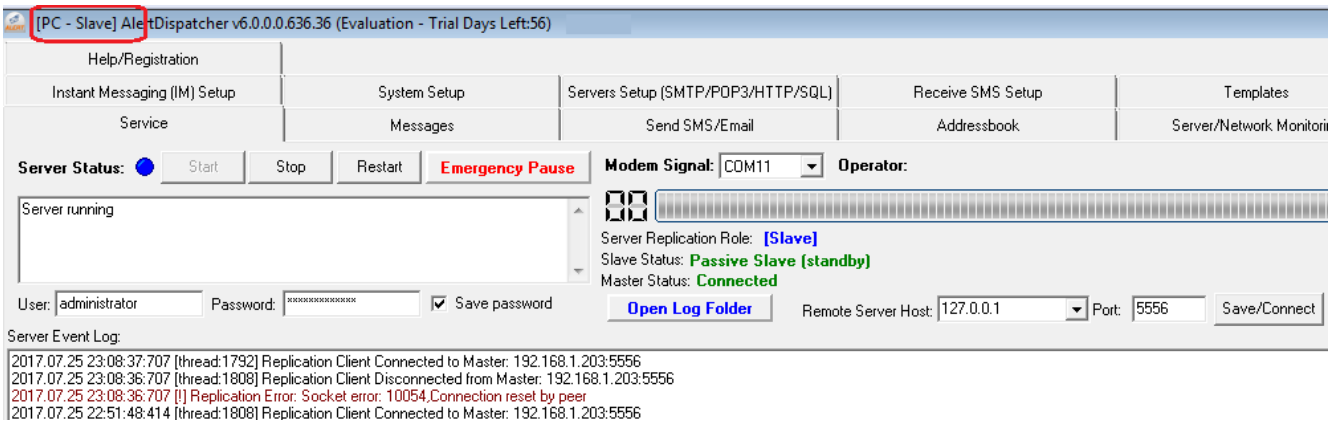
In the following screen, the Active Master is shown as connected to the Passive Slave.



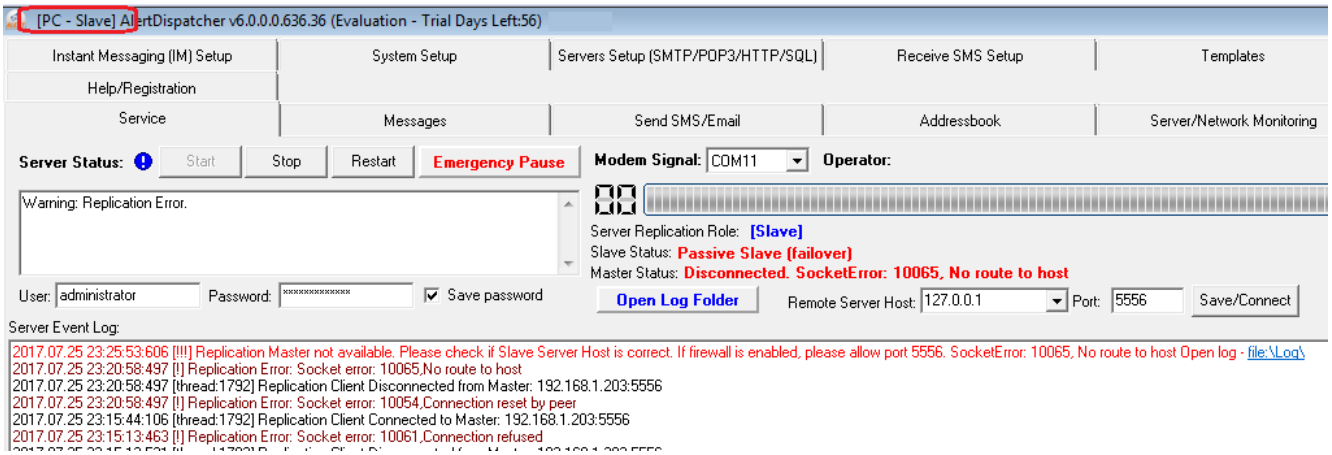
Passive Slave Node:



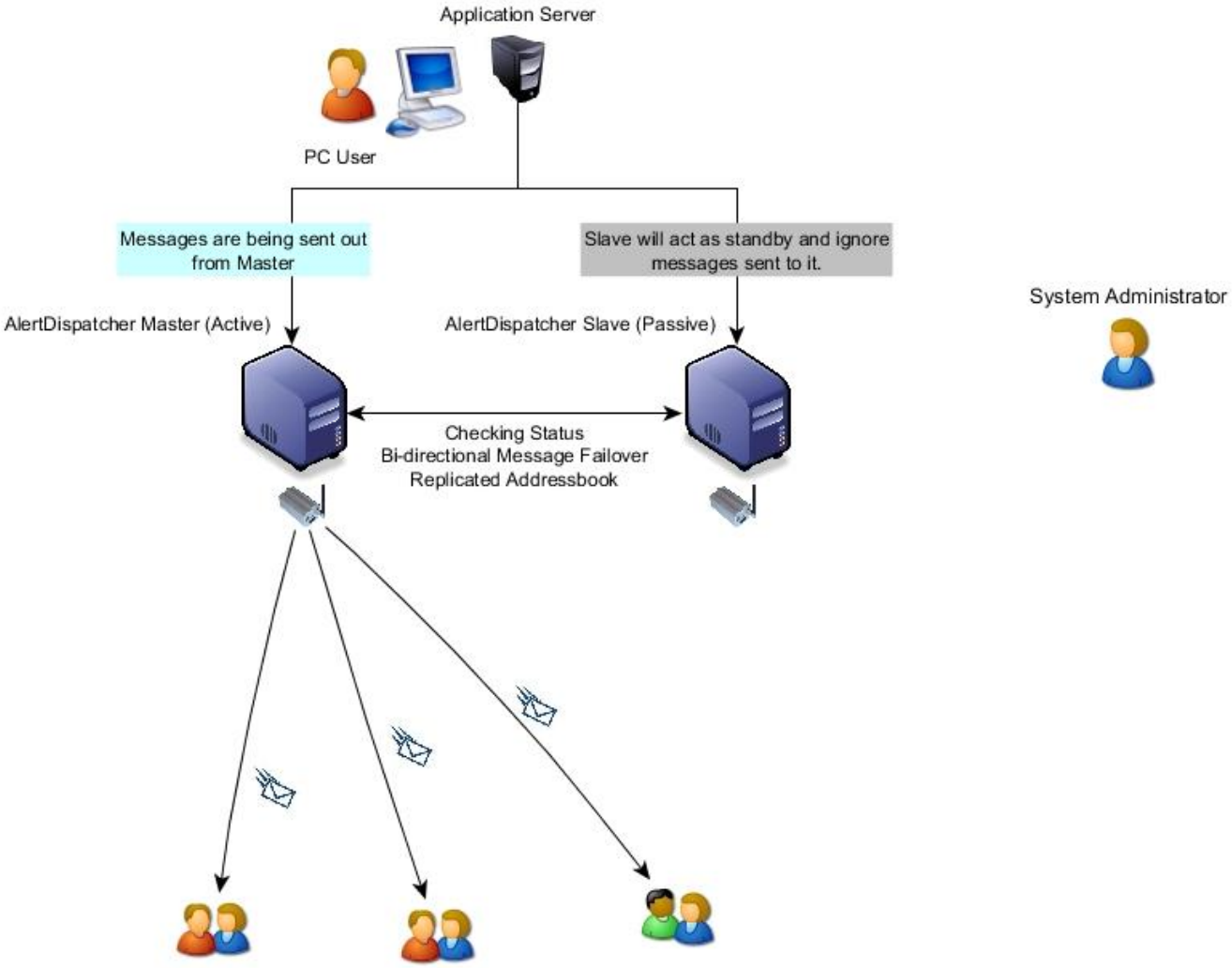
In the following screen, the Passive Slave is shown as connected to the Active Master. The Passive Slave status is "Standby" which means it doesn't process any messages until the Active Master is down or becomes disconnected from the Passive Slave.



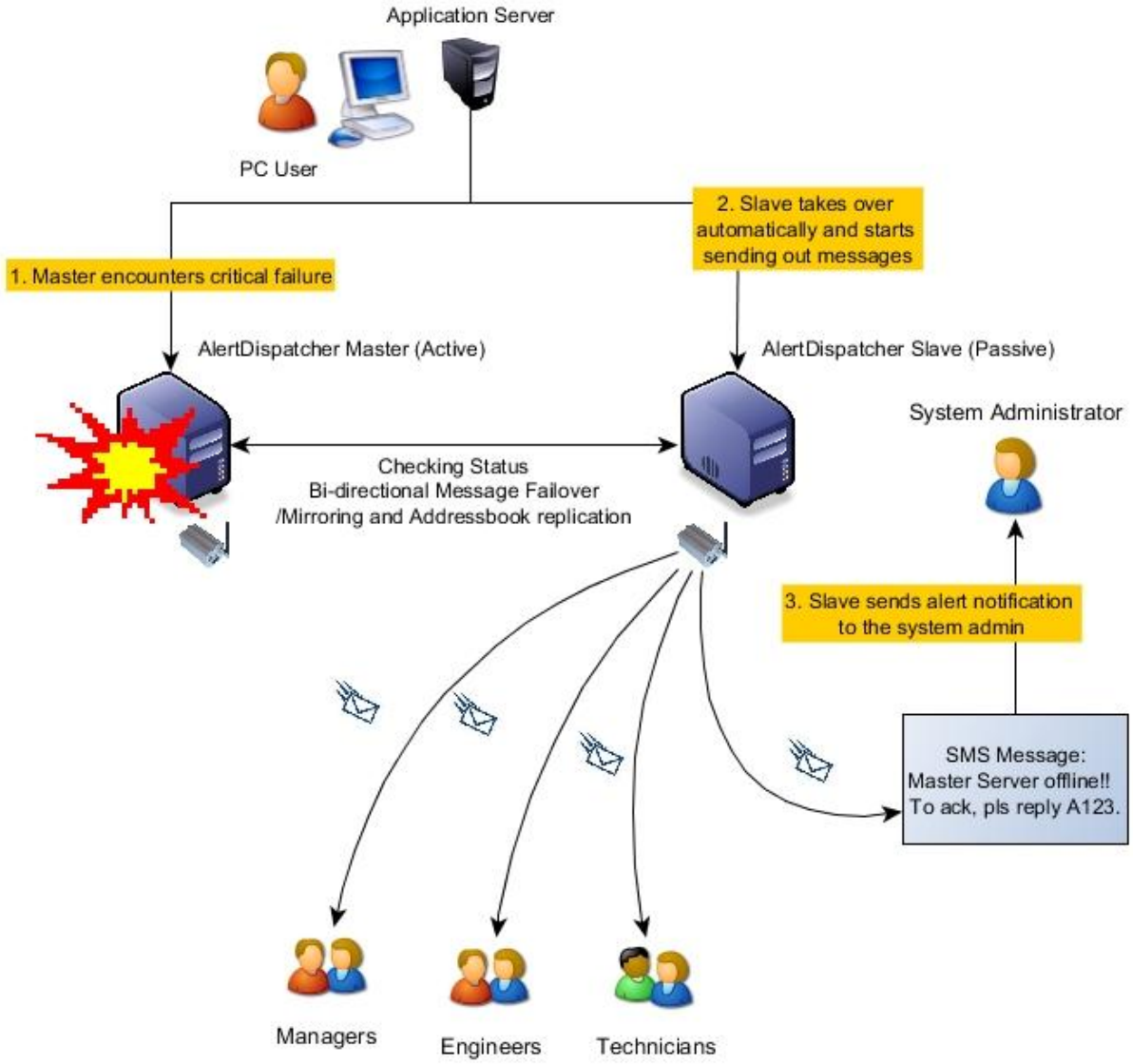
The following screen will be shown if the Passive Slave is disconnected from the Active Master. The Passive Slave status will then change to "failover" which means all messages sent to it will be processed.


[PC - Slave] AlertDispatcher v6.0.0.0.636.36 (Evaluation - Trial Days Left:56)
Instant Messaging (IM) Setup
System Setup
Servers Setup (SMTP/POP3/HTTP/SQL)
Receive SMS Setup
Templates
Help/Registration
Service
Messages
Send SMS/Email
Addressbook
Server/Network Monitoring
Server Status:
Start
Stop
Restart
Emergency Pause
Modem Signal: COM11
Operator:
Warning: Replication Error.
Server Replication Role: [Slave]
Slave Status: Passive Slave (failover)
Master Status: Disconnected. SocketError: 10065, No route to host
User: administrator
Password:
Save password
Open Log Folder
Remote Server Host: 127.0.0.1
Port: 5556
Save/Connect
Server Event Log:
2017.07.25 23:25:53:606 [!!!] Replication Master not available. Please check if Slave Server Host is correct. If firewall is enabled, please allow port 5556. SocketError: 10065, No route to host Open log - file:\Log\
2017.07.25 23:20:58:497 [!] Replication Error: Socket error: 10065,No route to host
2017.07.25 23:20:58:497 [thread:1792] Replication Client Disconnected from Master: 192.168.1.203:5556
2017.07.25 23:20:58:497 [!] Replication Error: Socket error: 10054,Connection reset by peer
2017.07.25 23:15:44:106 [thread:1792] Replication Client Connected to Master: 192.168.1.203:5556
2017.07.25 23:15:13:463 [!] Replication Error: Socket error: 10061,Connection refused

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 and starts processing messages.



4). How to configure Moxa NPort to allow AlertDispatcher to connect a modem via network

Directly connecting a modem to the server using USB or Serial cable is the most reliable way of deploying a modem, but this may not be possible for the following scenarios, 1). AlertDispatcher is installed on a virtual machine, 2). There is no network in the server room and the modem needs to be relocated to another room.

You can connect an RS232 serial modem to your computer network using a serial device server such as the Moxa NPort - https://www.moxa.com/product/NPort_5110.htm.

Due to the greater risk of failure for such a deployment as compared to a deployment in which the modem is directly connected to the server, we will recommend using 2 sets of modems and device servers for redundancy.

Tip:
1). Before configuring the NPort device, please obtain the network configuration information (IP address/Netmask/Gateway) from your IT department, and confirm that the necessary firewall ports are all opened – see Procedure below.
2). As some corporate networks may not allow Broadcast search across VLANs, it's recommended that you configure the NPort network settings by connecting it to your laptop directly.

Important: Please go through all the steps in the Procedure first to ensure you do not miss any step as it maybe more difficult to troubleshoot if any one step is not done correctly.

Procedure:

1). Connect the serial cable of your modem to the NPort device. Connect the NPort device to your switch using an RJ45 cable. Your switch must support 10/100 Mbps.

2). Install the latest version of Moxa NPort Administrator on your AlertDispatcher server (or VM guest instance). For convenience, you can download Moxa NPort Administrator and NPort Windows Driver Manager from this link (pls check if it's the latest version from Moxa website).

Note:
If you encounter the "Fail to start Real COM driver" during installation, you'll not be able to create a virtual COM Port on Windows so you'll need to install the "NPort Windows Driver Manager" (different from Windows Device Manager) which will be used in step 5. You'll still be able to search and configure your NPort device using Moxa NPort Administrator.

NPort COM ports (COM mapping) created using the NPort Windows Driver Manager may not appear in NPort Administrator COM mapping. To avoid orphaned COM ports that will block working ports, please create all your COM mappings under either Moxa NPort Administrator or NPort Windows Device Manager, and not both.

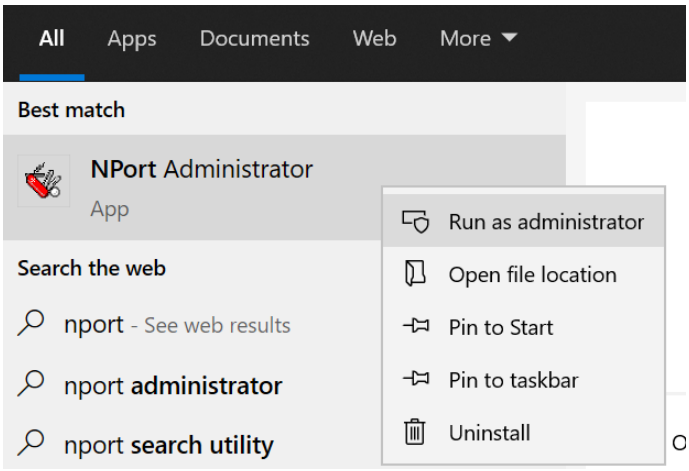
If there is a firewall between your Server and the NPort device (both Windows and Network firewall), please

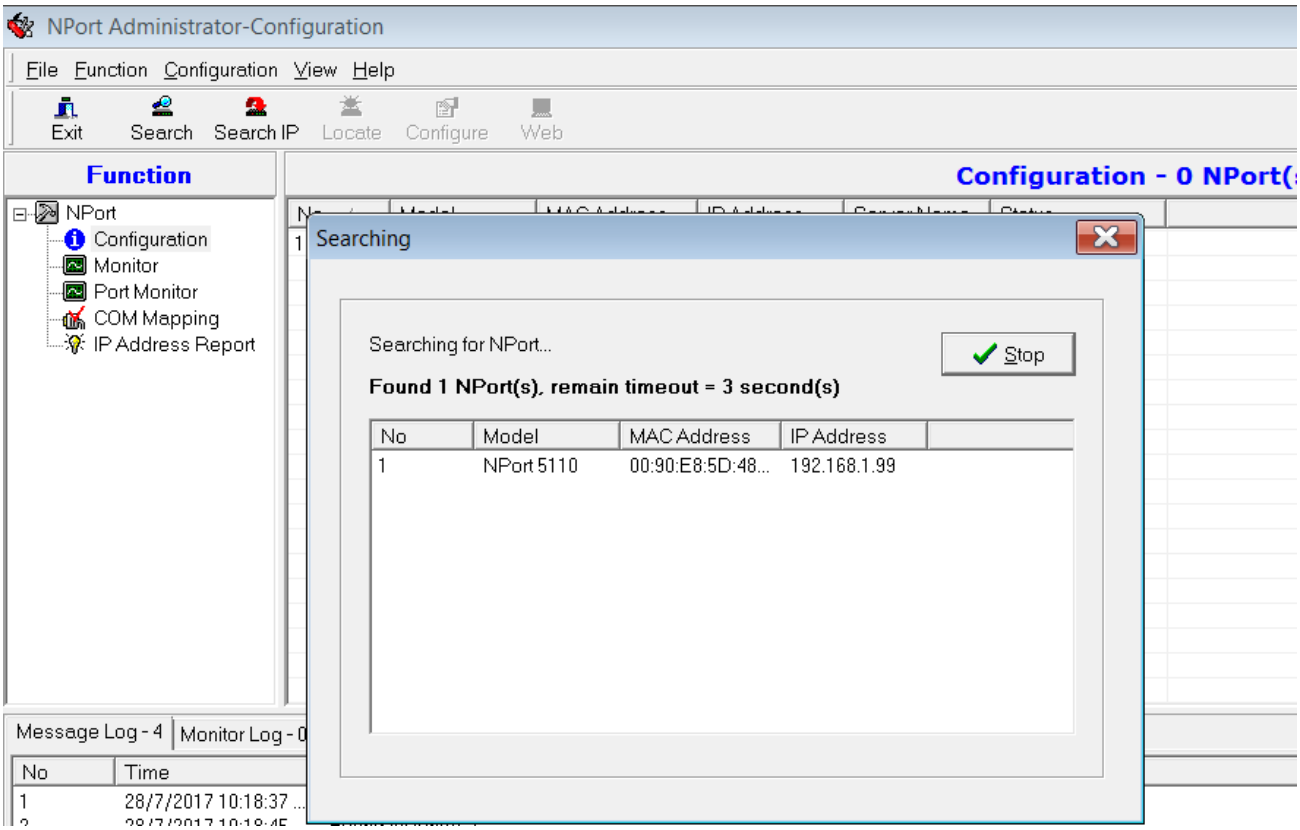
ensure that TCP Port 80, 950, 966 and UDP Port 4800 are open for your Moxa NPort device and assigned IP address.

[For NPort 5000 Series; NPort 5000A, NPort IA5000A, NPort P5150A, NPort W2x50, NE-4100 and MiiNePort Series] – Device Servers

Protocol	Port No.	Purpose
TCP	80	Web Console
TCP	950(~965)	Data Port
TCP	966(~981)	Command Port
UDP	4800	Broadcast, Monitor, Get current settings, RealCOM Port mapping

3). Run NPort Administrator (**right click to run as administrator**) and click "Search". If UDP Port 4800 is open on your NPort device and the NPort is connected to the same network or VLAN, you should be able to automatically locate your modem (or modems) as shown below.



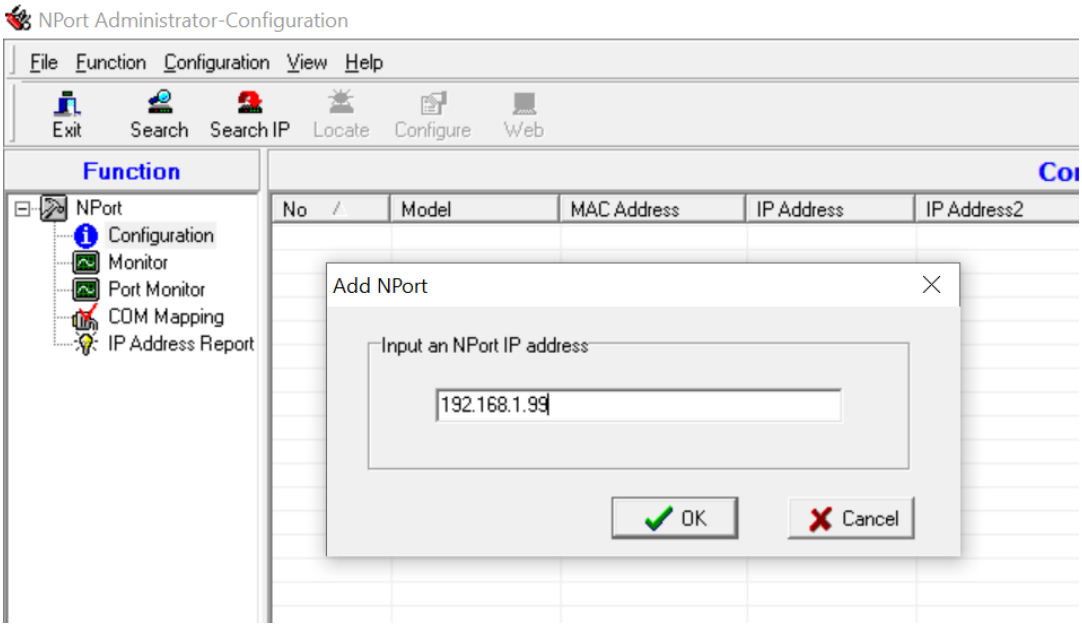


Steps if Search button fails:

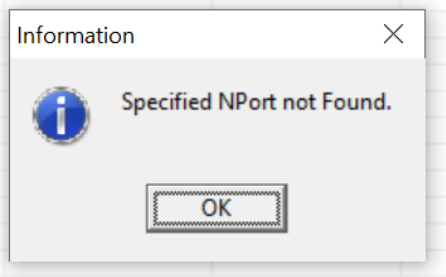
1. If broadcast is blocked, you'll not be able to locate the NPort device using the "Search" button. Please configure NPort network settings by connecting it to your laptop directly and repeating the step again. You will also need to install NPort Administrator on your laptop. *Tip: You can also enter the Factory Default IP address: 192.168.127.254 using Search IP.*

> **Note:** If "Search" button fails even with your laptop directly connected to the Moxa NPort device, please use Search IP button, enter 192.168.127.254 (factory default IP address). If this fails, reset the device to factory fault by inserting a paper clip into the reset button next to the LAN port and press for 10-20 seconds. The power must be on during the reset.

2. Once step 1 is done, reconnect the NPort device back to your network, and then click "Search IP" and enter the IP address you have just configured for the NPort device.

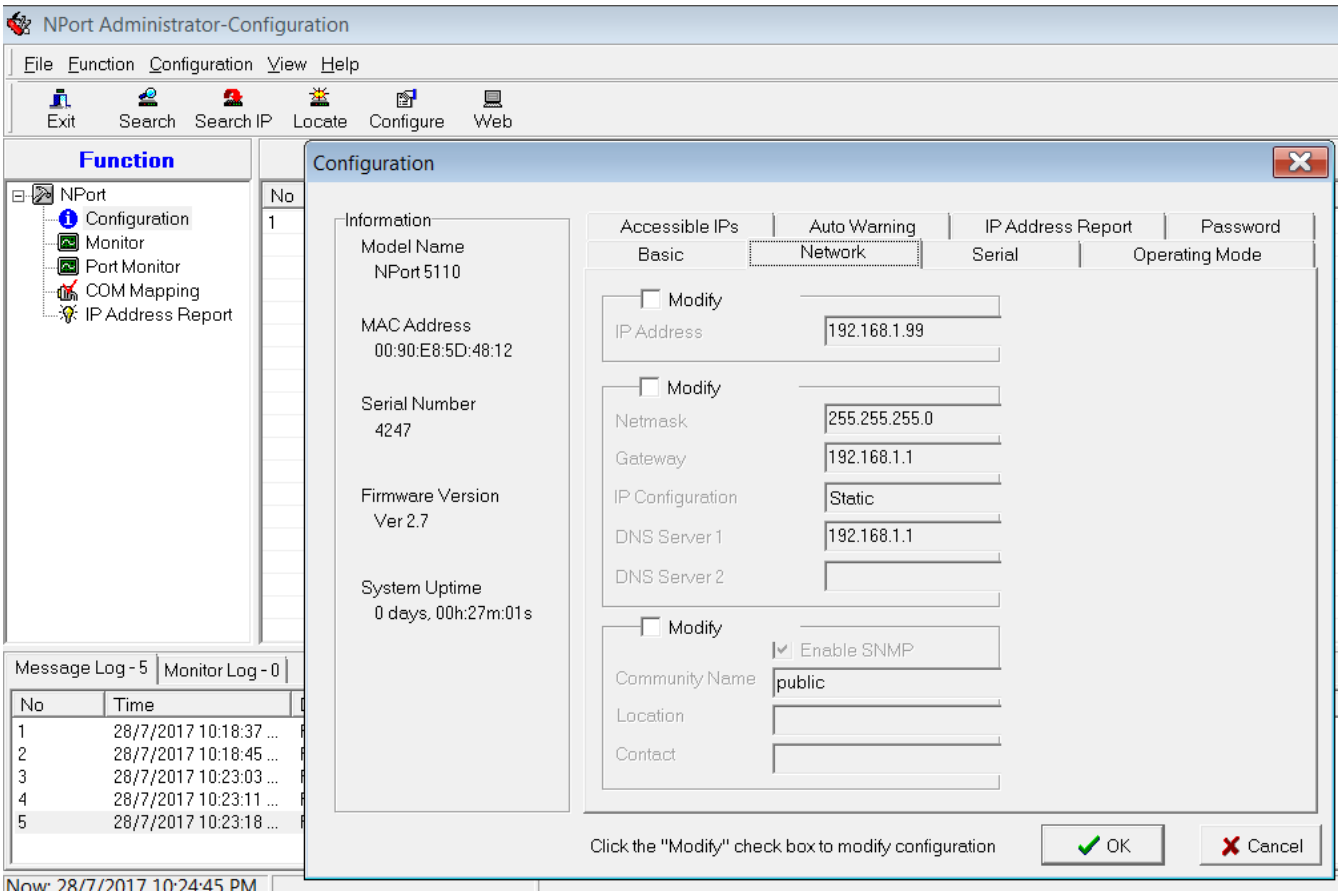


If an error "Specified NPort not Found" pops out, skip Step 4 and proceed to Step 5.

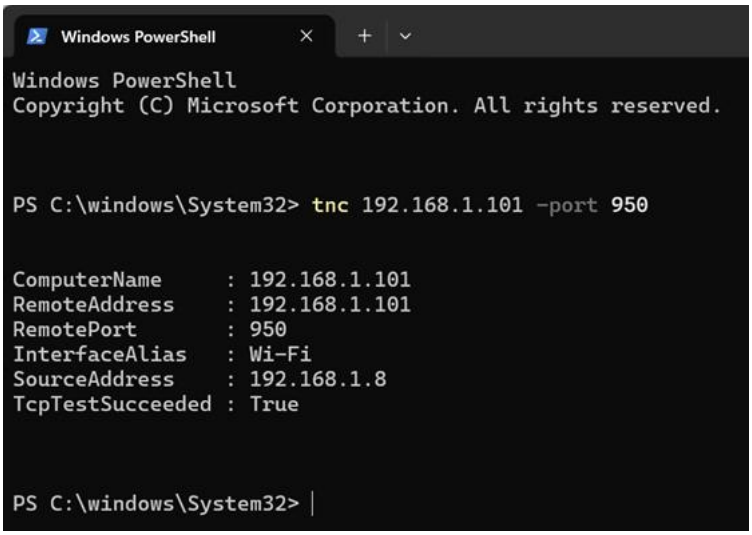


4). This step is applicable only if Step 3 is successful. Right click on the NPort device to unlock it. The default password is: **moxa**.

Configure the network for your NPort device (**IP address, Netmask and Gateway**). Please use a static IP address that is on the same subnet as your AlertDispatcher machine. For example, if the IP address of your AlertDispatcher machine is 192.168.1.100, the NPort device IP address can be 192.168.1.101. If a different subnet is used, please consult a network expert on the networking setup.

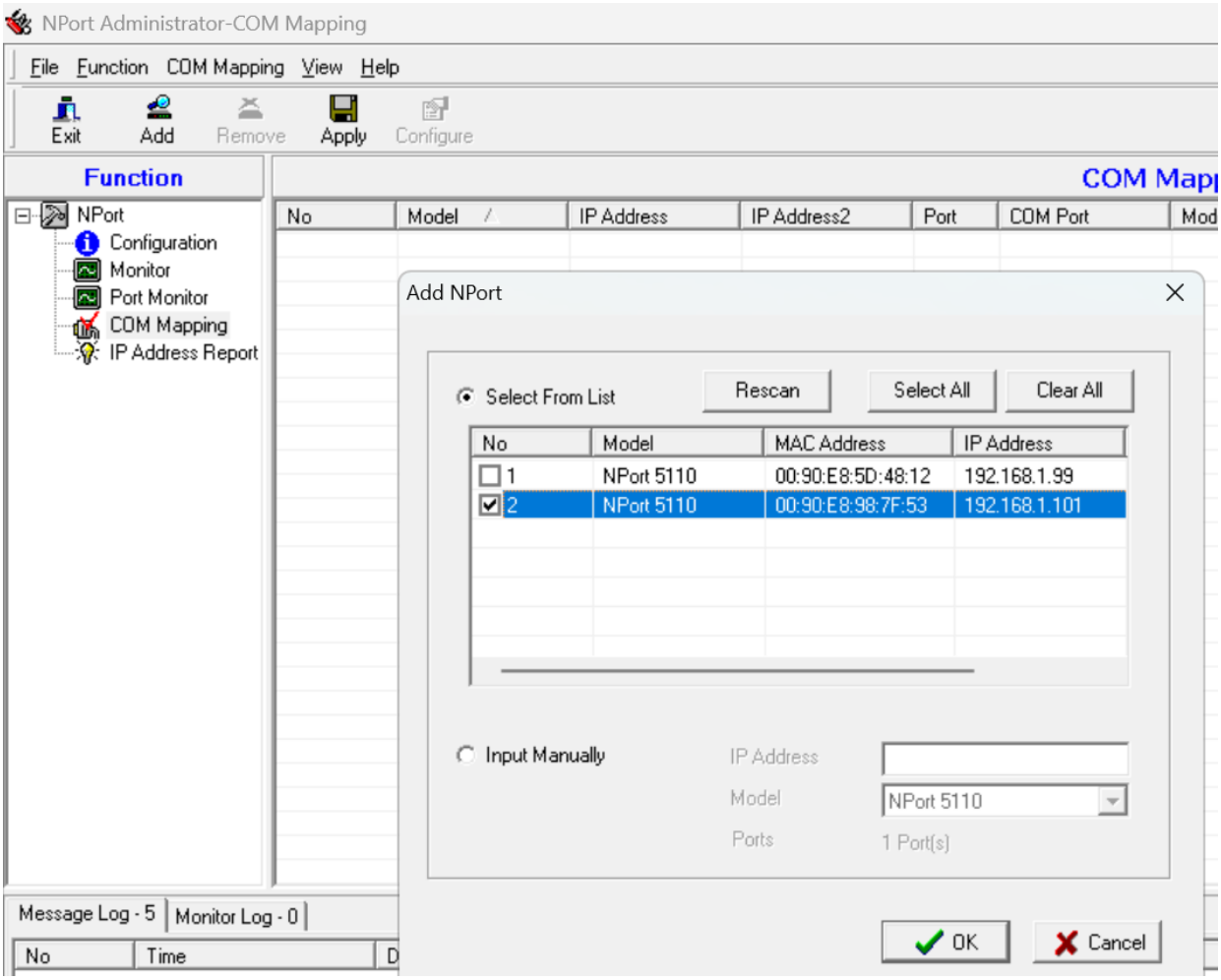


After you have configured the NPort device network, you should be able to PING the NPort device. If PING is not enabled on your network, you can also run Powershell to connect to the NPort data port 950 – tnc 192.168.1.101 950



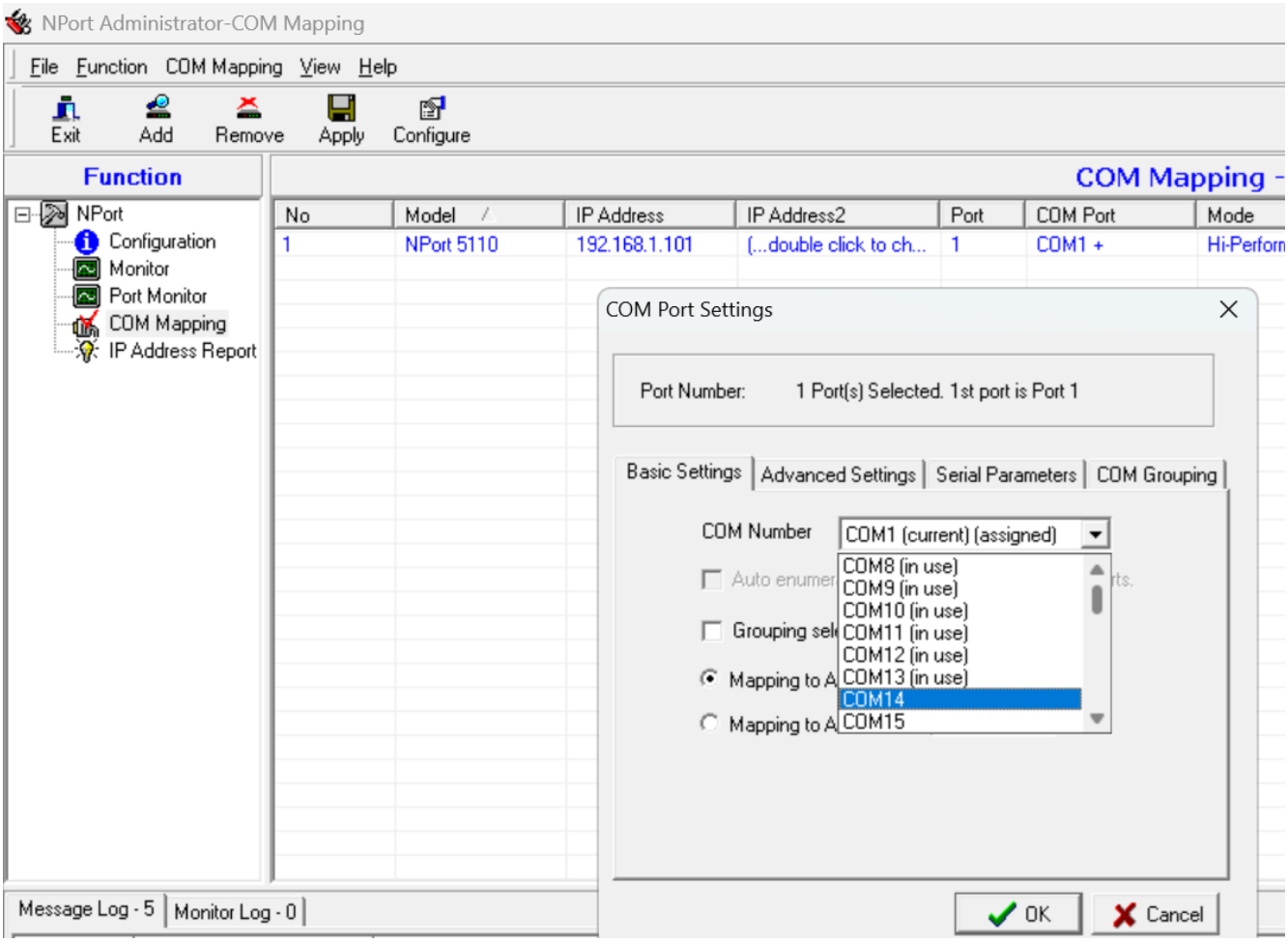
Warning: Please double check your network configuration and ensure that the IP address assigned is valid and available as you may not be able to connect to the device again if the configuration is wrong. After configuring the network, always record the NPort network settings.

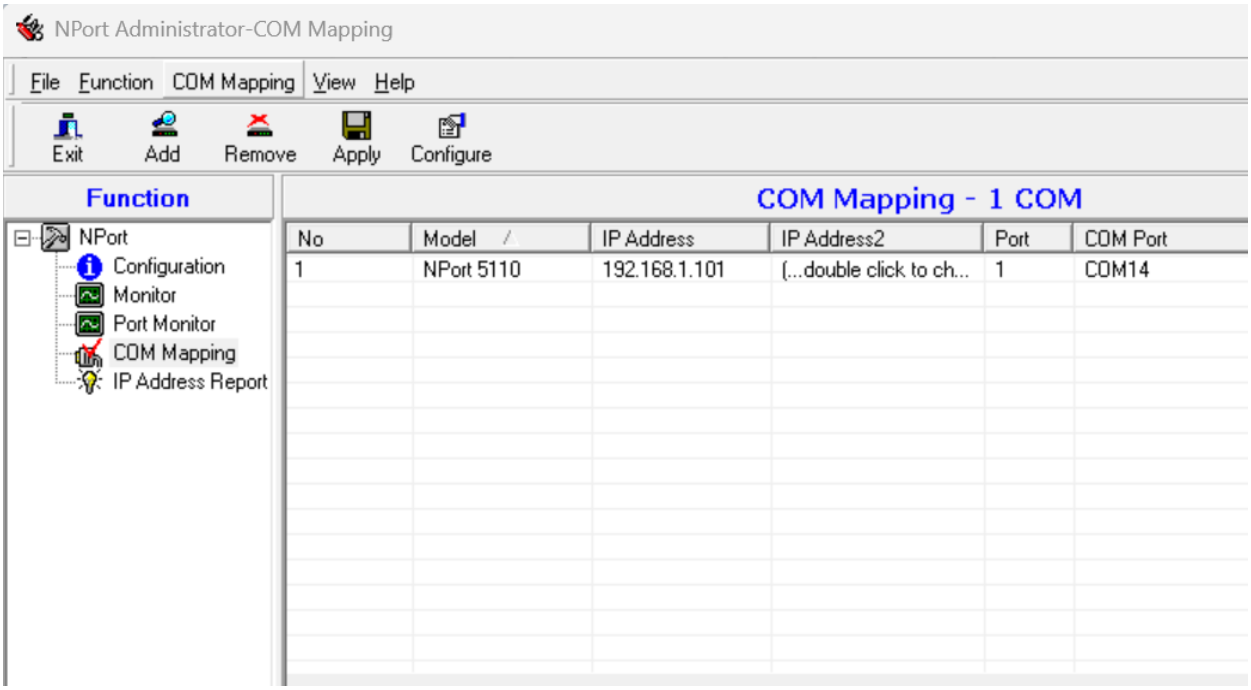
5). Right click on "COM Mapping", select "Add Target" and select the NPort device that you link from your machine.



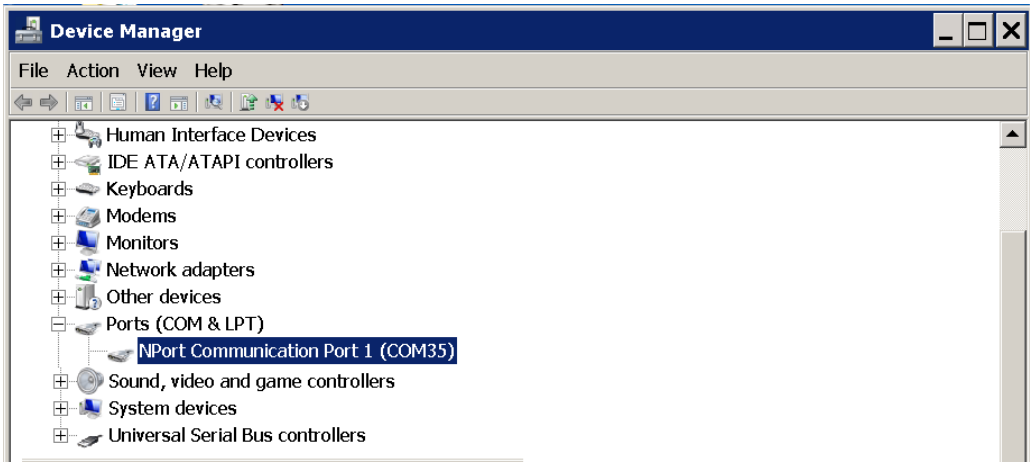
On successful creation, take note of the Virtual COM Port created as you would use it when you configure AlertDispatcher under Modem Setup. Click "Apply" to save the configuration.

Note: If the automatically assigned Virtual COM port is COM1 or COM2, this may cause conflict on some systems rendering the COM Port inaccessible from AlertDispatcher. To avoid this, you are advised to change it to another COM port, e.g. COM14 as shown in the example below.



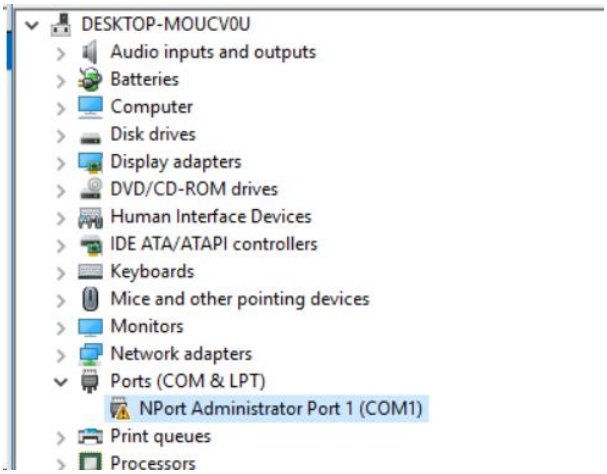


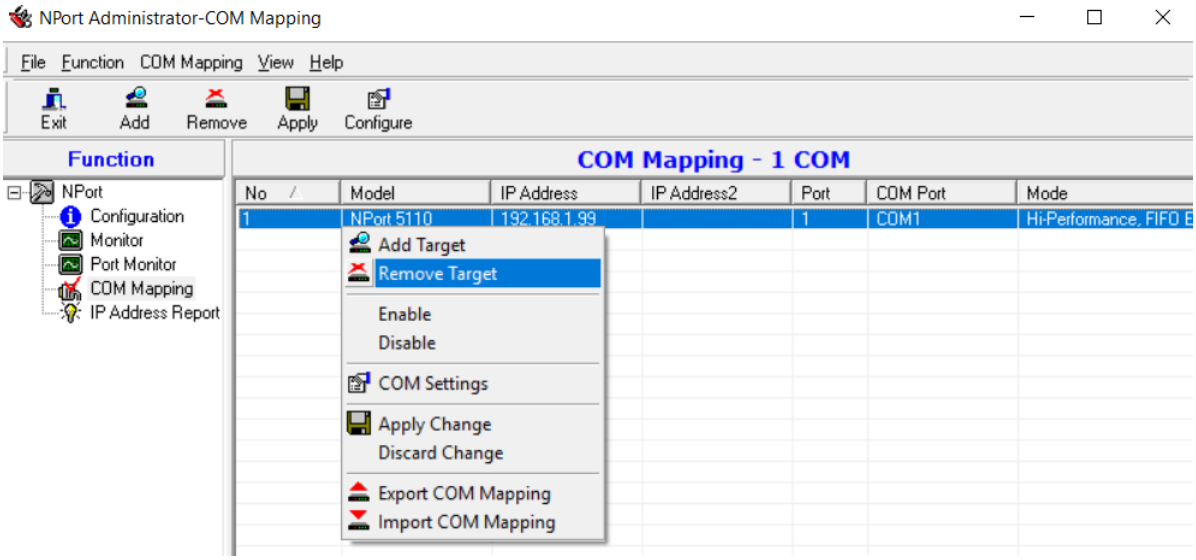
The COM Port will appear on Device Manager under Ports (COM & LPT). Note: For newer version of NPort Administrator, it may appear as "NPort Administrator Port".



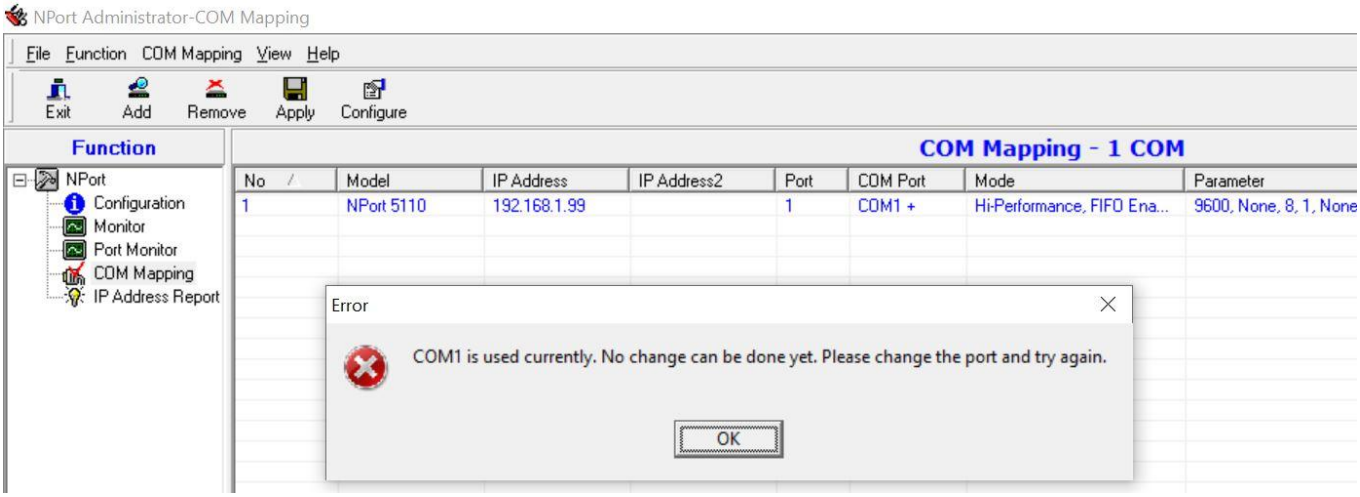
Note:

1. If NPort Administrator Port device has an error as shown below, remove the COM Mapping you just created for the NPort, click Apply button, uninstall NPort Administrator using windows “Add or remove programs”. Reboot your server and then reinstall NPort Administrator using the default program path provided (do not change path), and repeat the initial configuration, add COM Mapping.





2. If you're getting "COM is used currently…" error, you'll need to install NPort Windows Driver Manager in order to add the virtual COM port to your server – see Step 6.

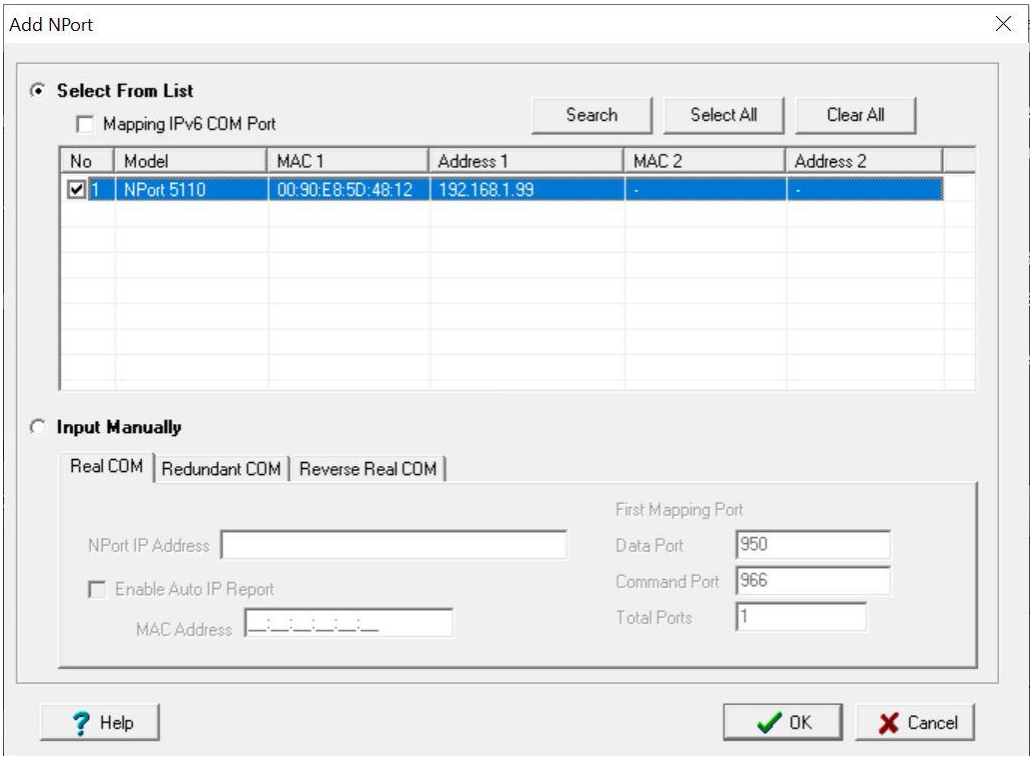


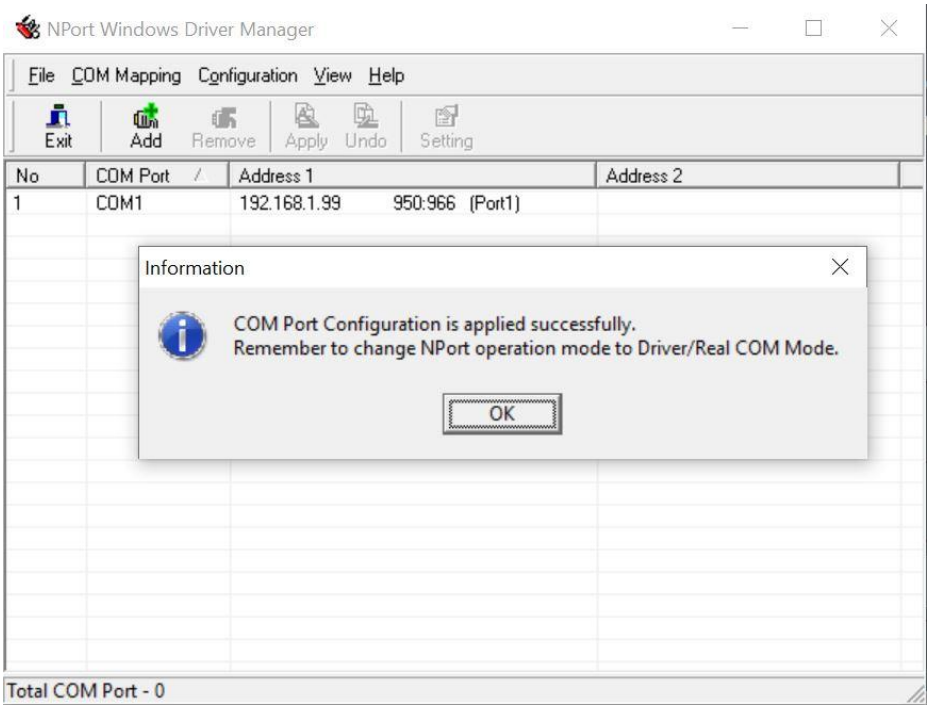
6). This step is applicable only if you have failed to add the NPort COM Port using NPort Administrator. Otherwise, please skip this step and proceed to Step 7.

First download and install NPort Windows Driver Manager from -
http://www.clickndeploy.com/downloads/NPort_Administrator.zip

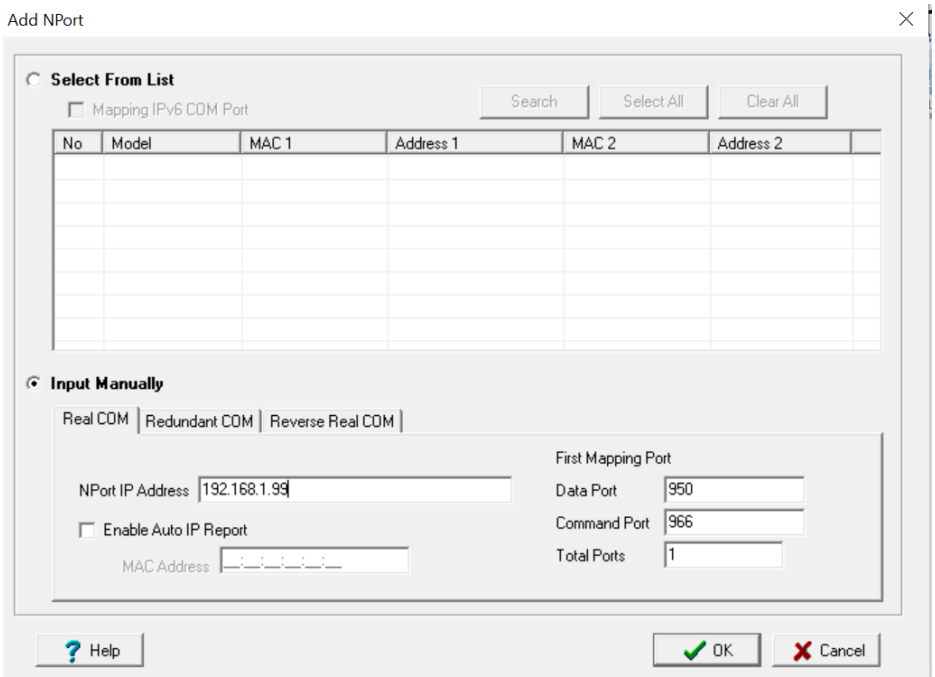
Note: Configuration of NPort Device (IP address, etc) is still done using NPort Administrator so do not uninstall the NPort Administrator software.

Go to Windows search, type NPort, select to launch NPort Windows Driver Manager. Use NPort Windows Driver Manager to add your NPort COM port. Click "Apply" button.



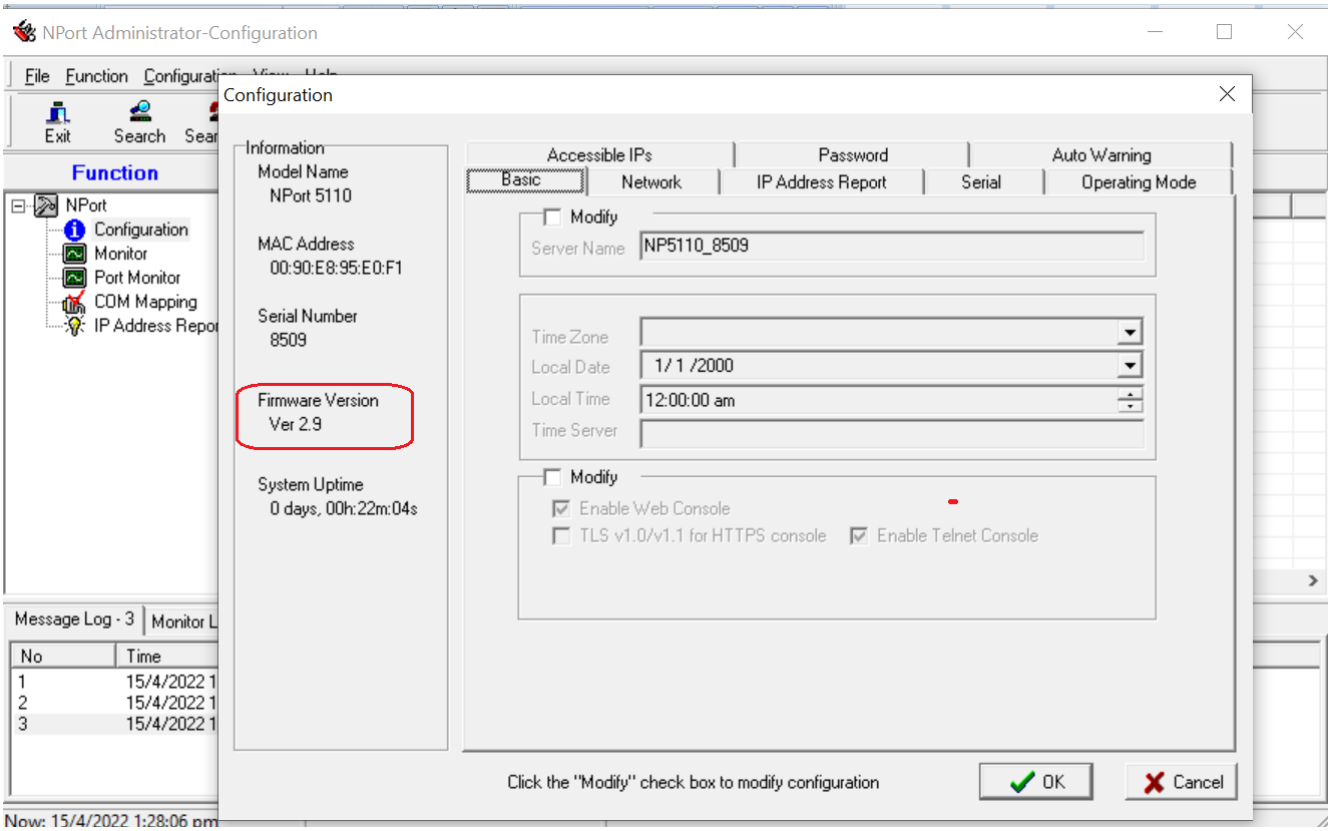


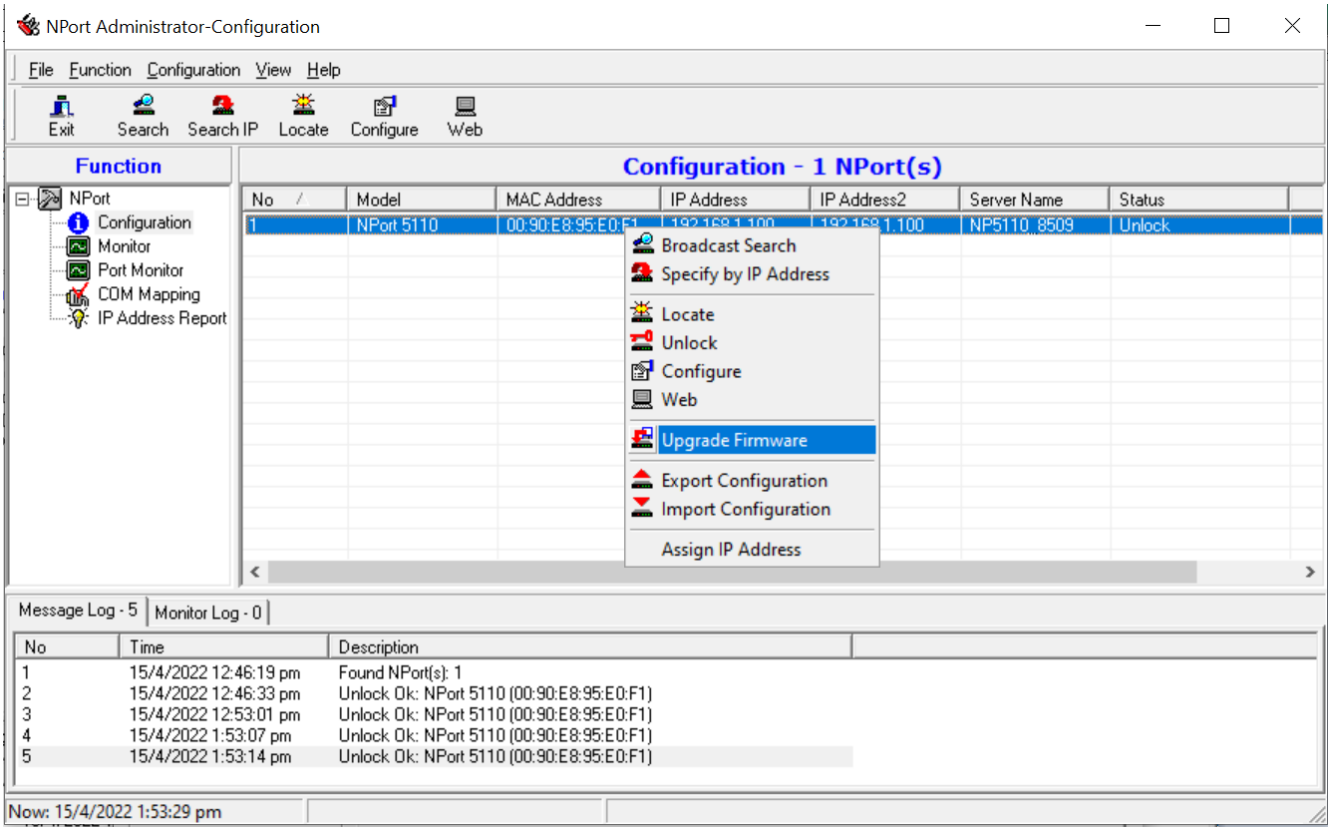
If you're unable to Search for the NPort Device, please use the "Input Manually" option. After that click "Apply" button and proceed to step 7.

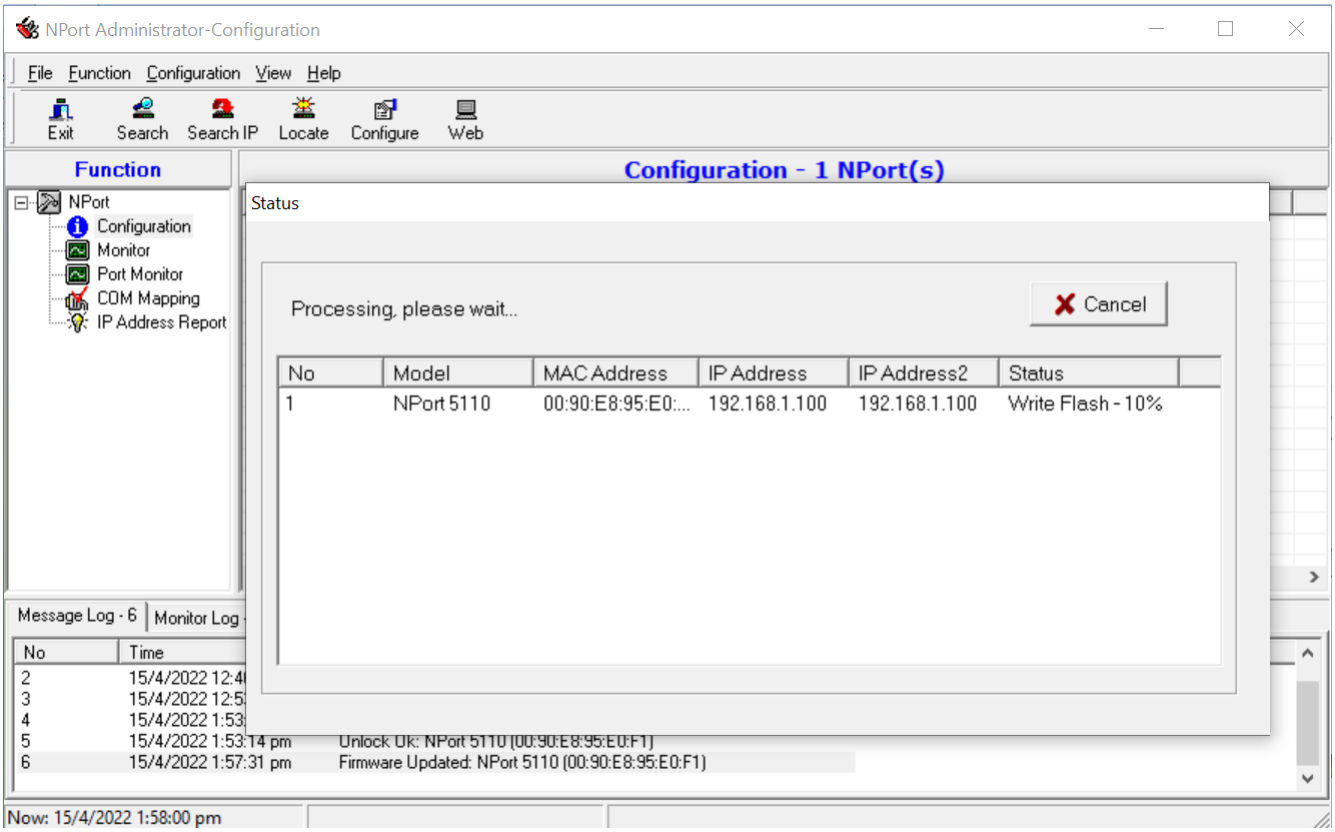


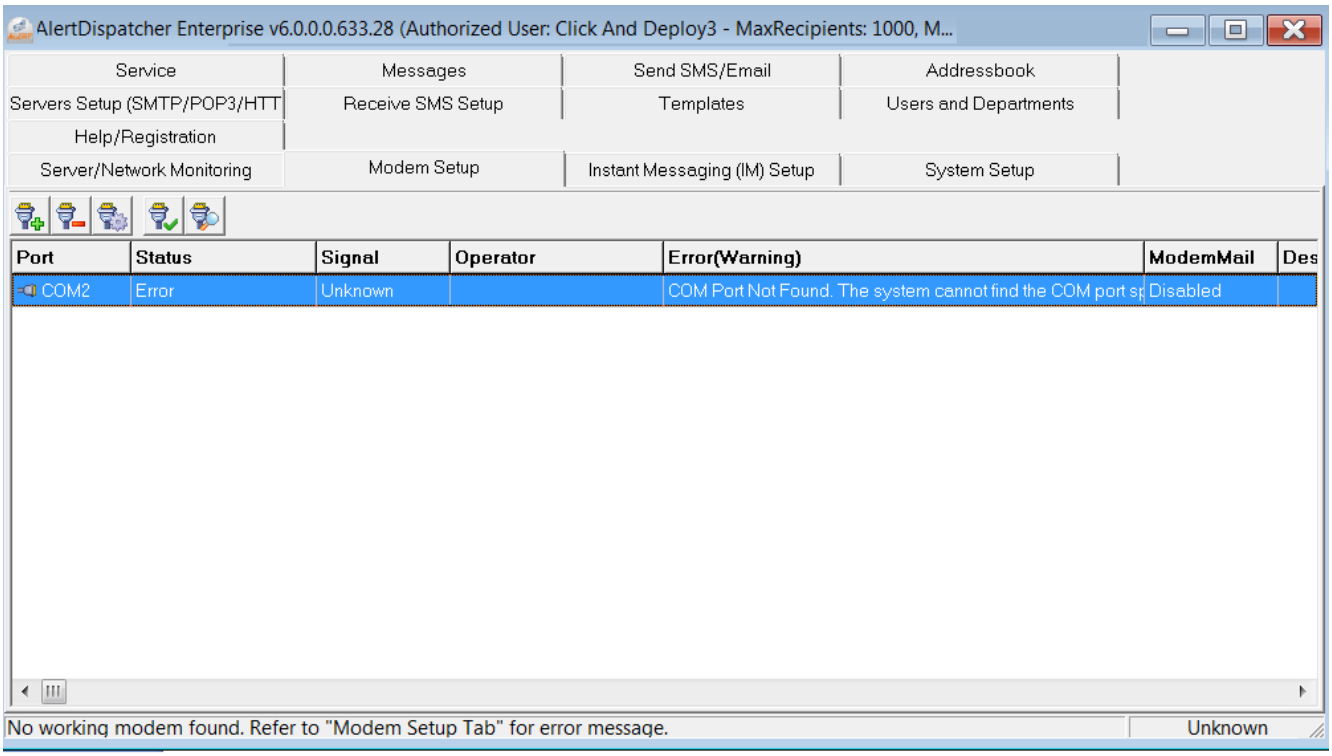
7). If you're told by your vendor to upgrade your firmware, you can do this using the NPort Adminstrator.

IMPORTANT: Please ensure that your NPort Firmware Version is Ver 2.9 (or higher). Lower version maybe unstable.

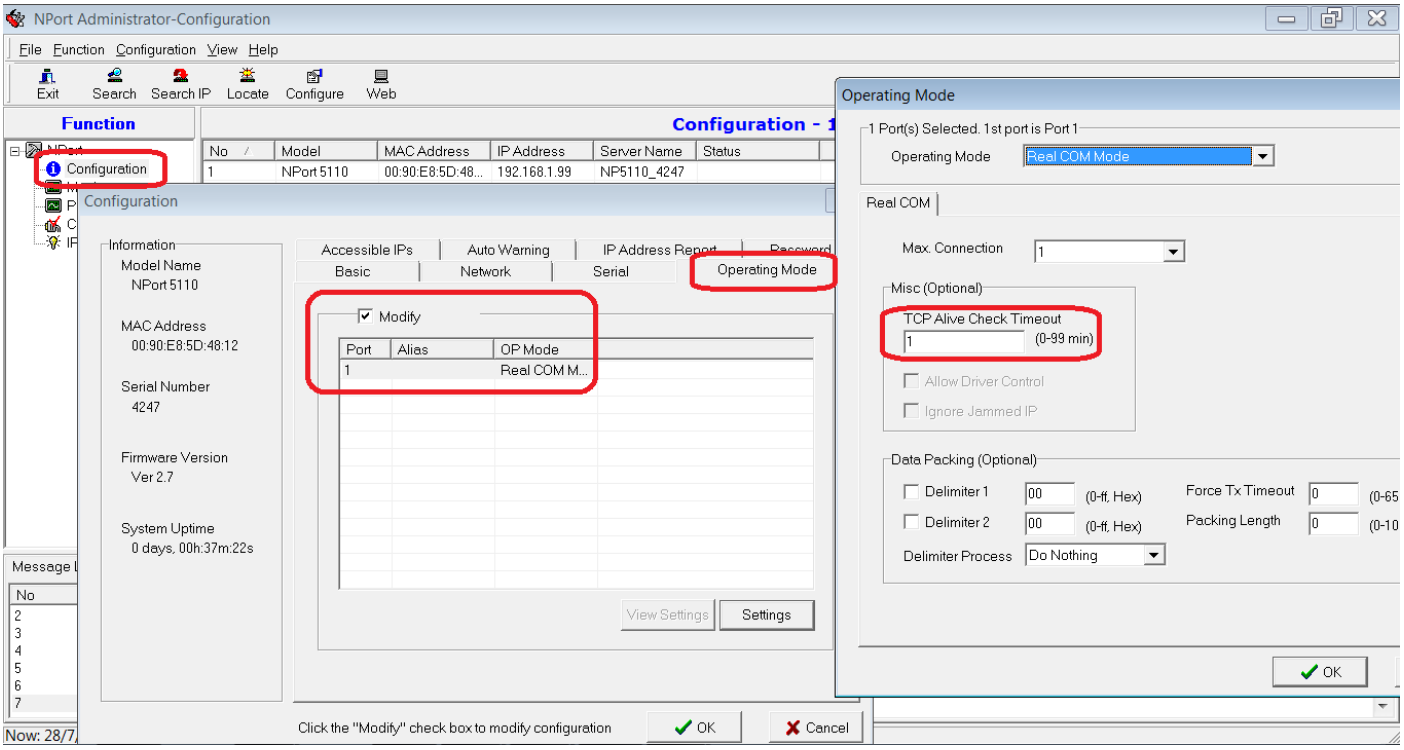



NPort Administrator-Configuration
File Function Configuration View Help
Exit Search Search IP Locate Configure Web
Function
NPort
Configuration
Monitor
Port Monitor
COM Mapping
IP Address Report
Configuration - 1 NPort(s)
No Model MAC Address IP Address IP Address2 Server Name Status
1 NPort 5110 00:90:E8:95:E0:F1 192.168.1.100 192.168.1.100 NP5110_8509 Unlock
Broadcast Search
Specify by IP Address
Locate
Unlock
Configure
Web
Upgrade Firmware
Export Configuration
Import Configuration
Assign IP Address
Message Log - 5
Monitor Log - 0
No Time Description
1 15/4/2022 12:46:19 pm Found NPort(s): 1
2 15/4/2022 12:46:33 pm Unlock Ok: NPort 5110 (00:90:E8:95:E0:F1)
3 15/4/2022 12:53:01 pm Unlock Ok: NPort 5110 (00:90:E8:95:E0:F1)
4 15/4/2022 1:53:07 pm Unlock Ok: NPort 5110 (00:90:E8:95:E0:F1)
5 15/4/2022 1:53:14 pm Unlock Ok: NPort 5110 (00:90:E8:95:E0:F1)
Now: 15/4/2022 1:53:29 pm

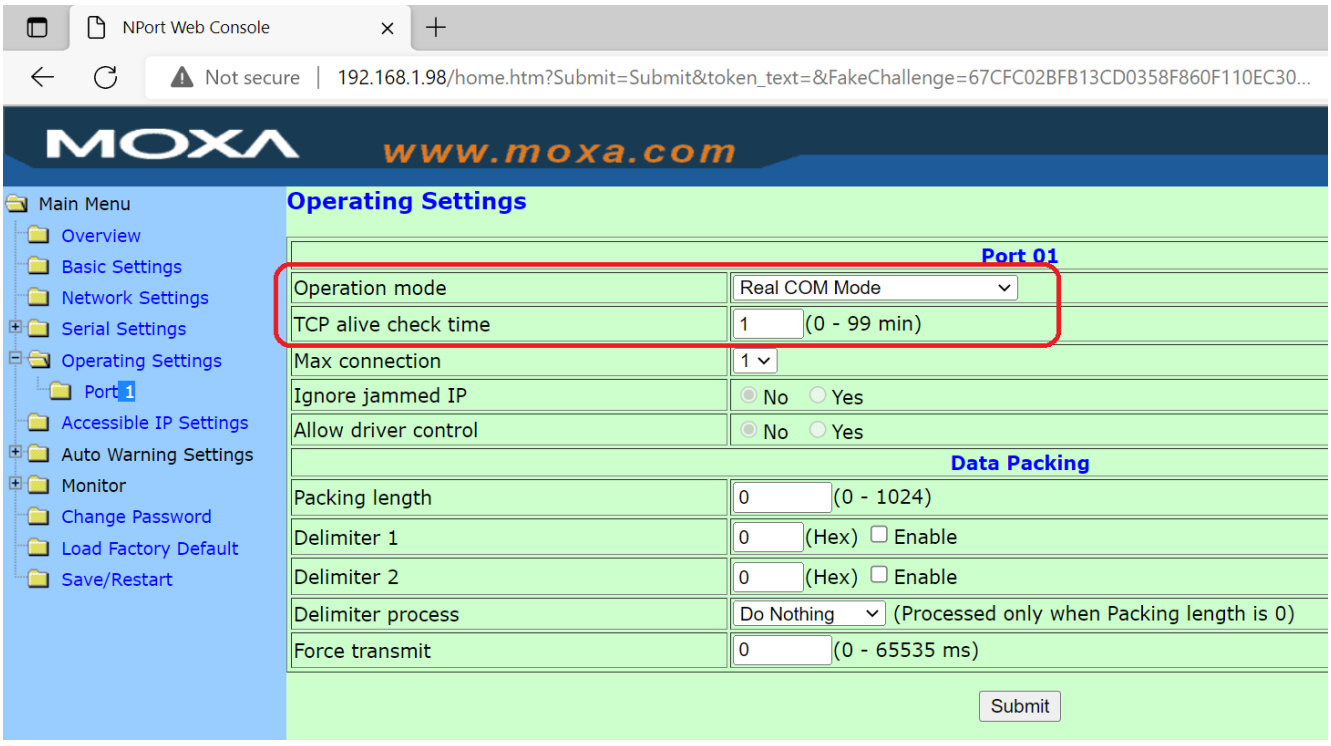

NPort Administrator-Configuration
File Function Configuration View Help
Exit Search Search IP Locate Configure Web
Function
NPort
Configuration
Monitor
Port Monitor
COM Mapping
IP Address Report
Configuration - 1 NPort(s)
Status
Processing, please wait...
Cancel
No Model MAC Address IP Address IP Address2 Status
1 NPort 5110 00:90:E8:95:E0:... 192.168.1.100 192.168.1.100 Write Flash - 10%
Message Log - 6
Monitor Log
No Time
2 15/4/2022 12:4
3 15/4/2022 12:5
4 15/4/2022 1:53
5 15/4/2022 1:53:14 pm Unlock Ok: NPort 5110 (00:90:E8:95:E0:F1)
6 15/4/2022 1:57:31 pm Firmware Updated: NPort 5110 (00:90:E8:95:E0:F1)
Now: 15/4/2022 1:58:00 pm


AlertDispatcher Enterprise v6.0.0.0.633.28 (Authorized User: Click And Deploy3 - MaxRecipients: 1000, M...
Service
Messages
Send SMS/Email
Addressbook
Servers Setup (SMTP/POP3/HTT
Receive SMS Setup
Templates
Users and Departments
Help/Registration
Server/Network Monitoring
Modem Setup
Instant Messaging (IM) Setup
System Setup
Port
Status
Signal
Operator
Error(Warning)
ModemMail
Des
COM2
Error
Unknown
COM Port Not Found. The system cannot find the COM port sp
Disabled
No working modem found. Refer to "Modem Setup Tab" for error message.
Unknown

8). Launch NPort Administrator, click on Configuration, double click on your NPort Device. Modify the TCP Alive Check Timeout of your Modem Port or Ports from 7 min (default) to 1 min. This setting is necessary to ensure that the NPort Device can be redetected within 1 minute of any network disruption.

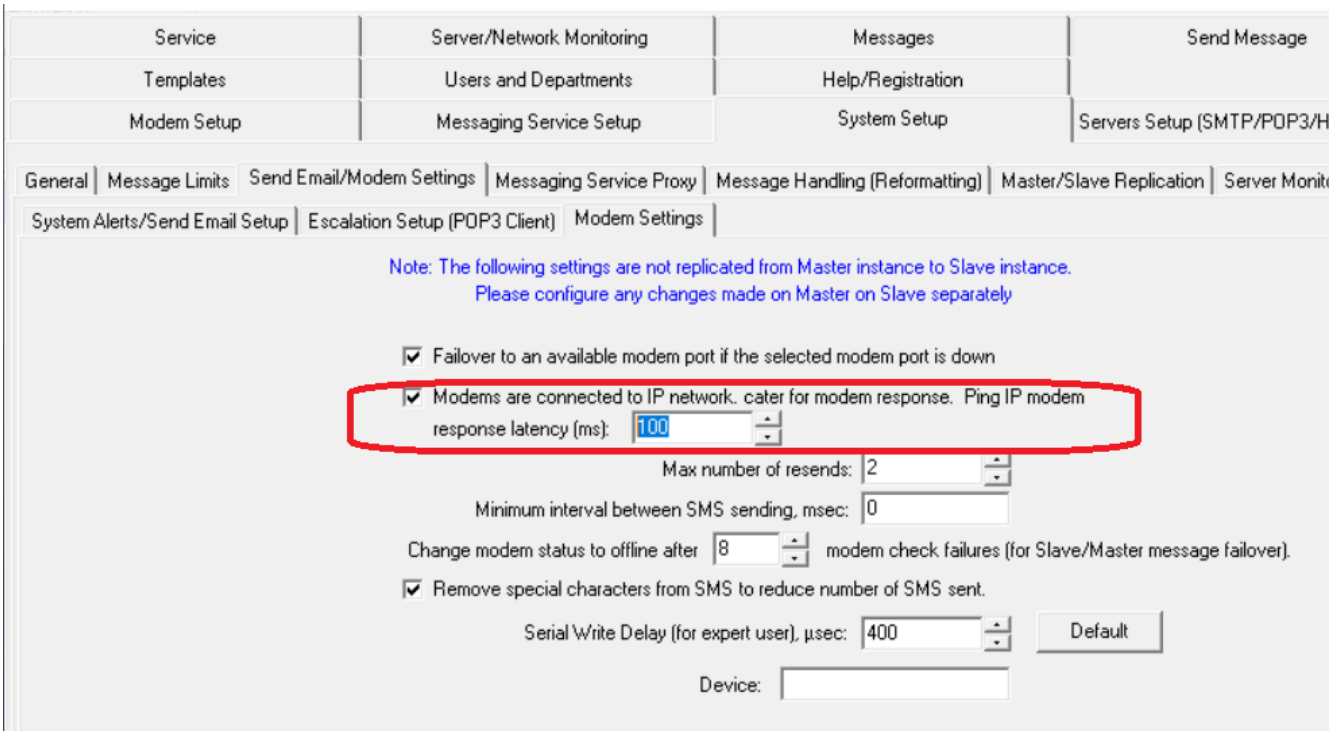


Note: If you're unable to use NPort Administrator to access your NPort device, you can configure the TCP Alive Check Timeout using a web browser.

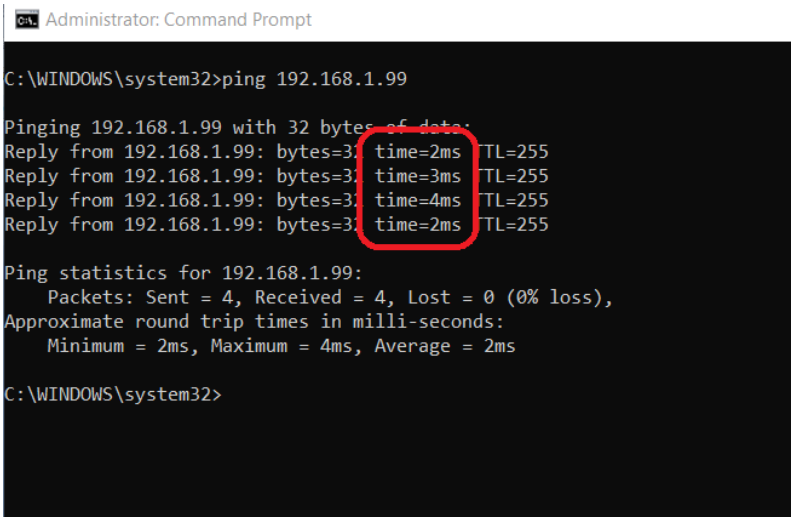


9). If your NPort is connected to a high traffic network with many servers and controllers, to cater for network congestion, please go to AlertDispatcher Client, under "System Setup", "Modem Settings", enable "Modems are connected to IP network, cater for modem response…" checkbox. The default value is 100ms. You may try to ping your Moxa NPort IP address to determine a suitable Ping IP modem response latency setting.

Note: If you're using Master/Slave setup, please configure this on both Master and Slave AlertDispatcher separately.



For example, the ping response is 2ms-4ms for the below test, which is lower than the default 100ms. For this case, you can leave the default. If the ping response is above 50ms, please increase the value to 200ms to cater for traffic fluctuation and network congestion situation.



Troubleshooting notes:

If AlertDispatcher fails to detect the Modem via the added COM port, perform the following:

Step 1: Ensure the serial cable is tightly connected to the NPort and modem device. The modem power is turned on and SIM card properly inserted. You may test the modem using your laptop to confirm that it is working. If this doesn't work, proceed to Step 2.

Step 2: Check if there's another AlertDispatcher installed on another Windows machine that is connected to the same NPort device/Modem. Disable the modem port on that AlertDispatcher. Disable all Firewall including Network firewalls. If this doesn't work, proceed to Step 3.

Step 3. Disable the modem port under AlertDispatcher "Modem Setup". Remove all the COM ports added under COM Mapping, click "Apply" and then reboot your server. Launch NPort administrator or NPort Windows Driver again, and then select "Add Target" under COM Mapping. If the COM ports have changed, update the COM ports configured under AlertDispatcher, "Modem Setup".

Step 4. Reset the IP address of NPort device to a new IP address (unused) and repeat step 3.

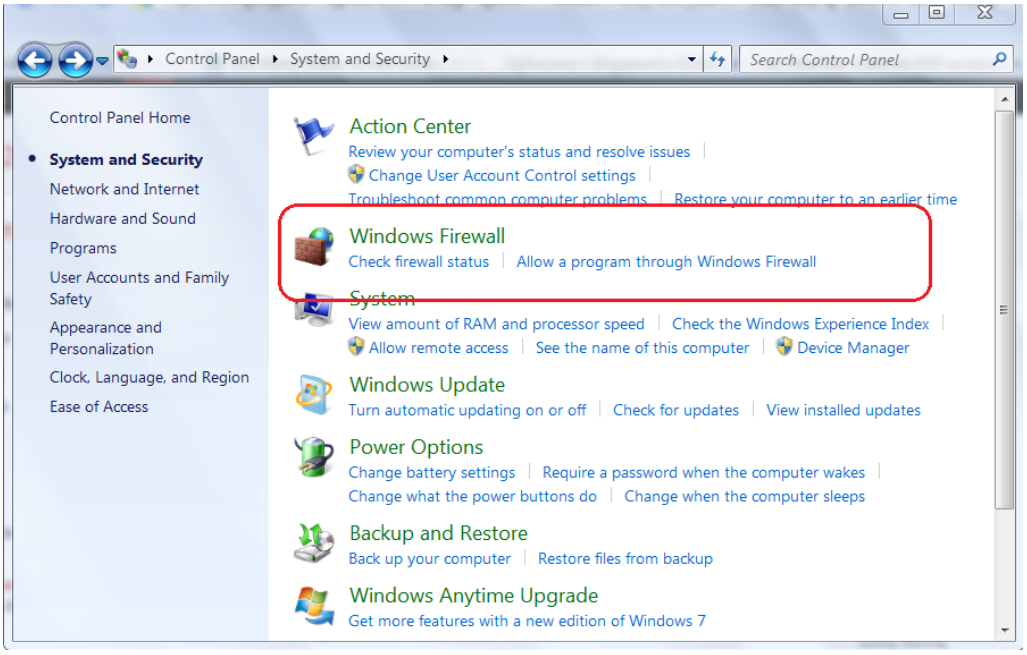
3. Appendix

A. How to Add (allow) server ports to Firewall

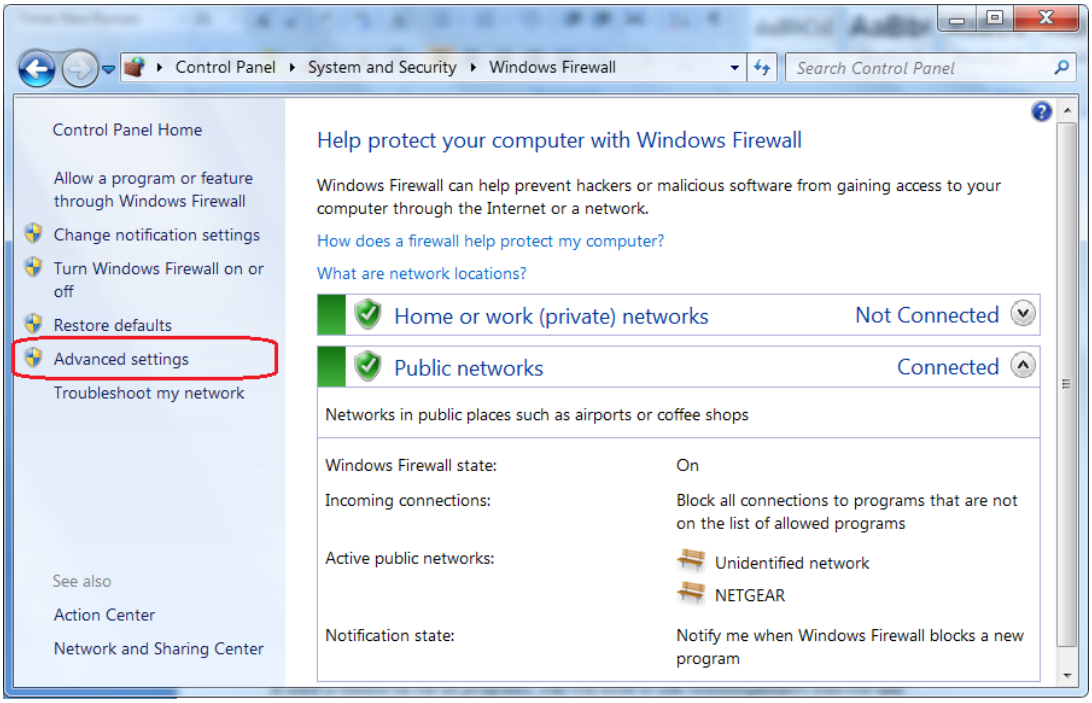
If you need to be able to access AlertDispatcher Server from the network, you must add the ports used by the services you require to your firewall list of "allowed ports" if firewall is active.

To add port exceptions to Windows Firewall exception list:

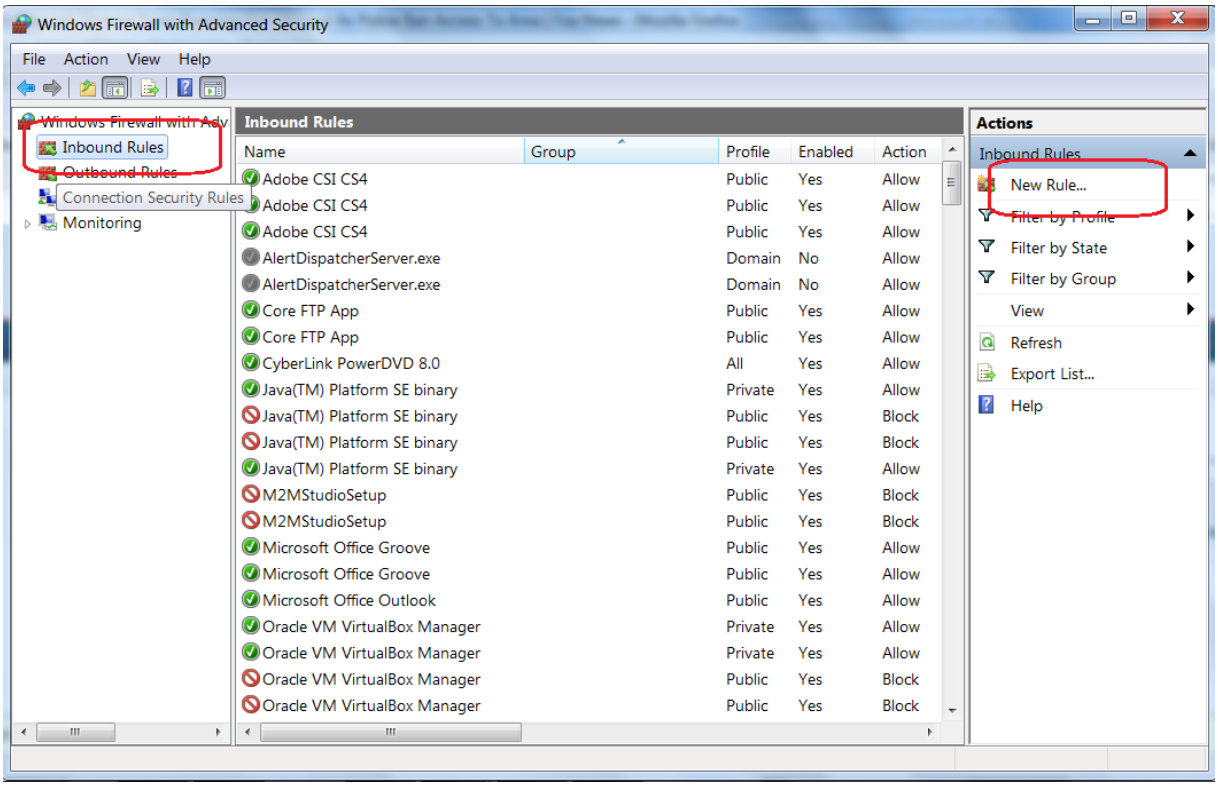
Go to *Start* → *Control Panel* → *Windows Firewall*.



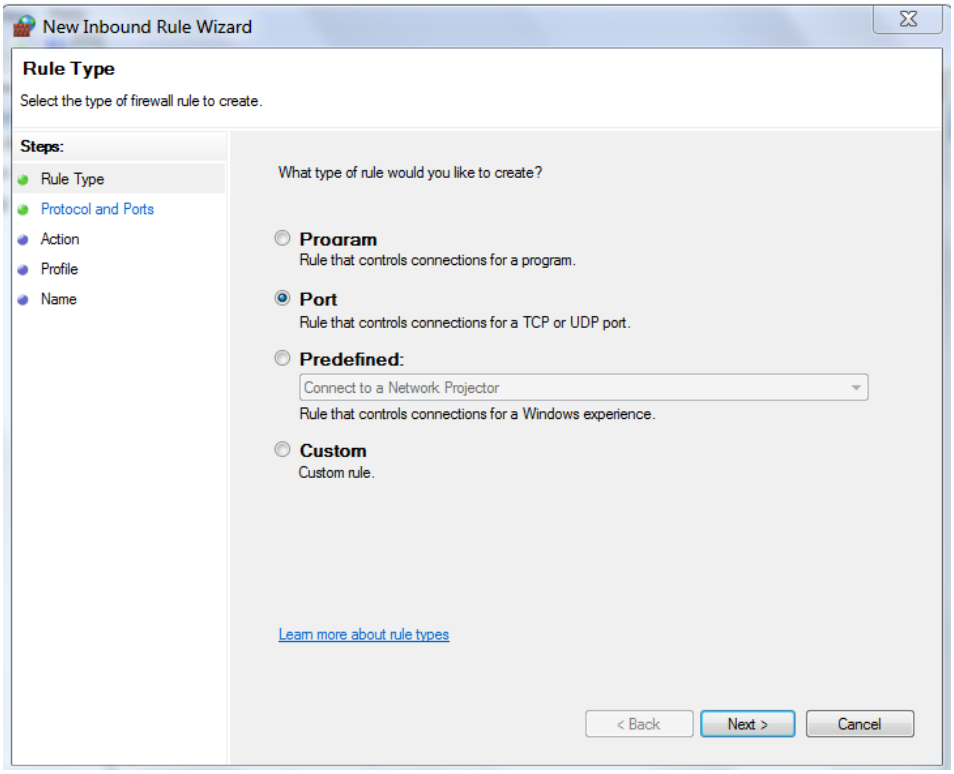
Click "Advanced settings".



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 3rd party firewall, check with your IT administrator or the firewall vendor.

Server Protocol	***Default Port***	***Remarks***
1. HTTP Server 2. SMTP Server 3. SNMP Trap Receiver 4. AlertDispatcher Server	80 25 162 5556	*Used by AlertDispatcher Client, DLL API and AlertDispatcher High Availability (Master/Slave Cluster Redundancy)*