AlertDispatcher IT Security Guide

Last update: 1st Sept 2022

Copyright

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). Introduction

The AlertDispatcher IT Security Guide teaches you how to secure your AlertDispatcher from external IT security threats and from internal misuse. We recommend taking some time to read this guide. Implementing even basic security measures can help you to avoid downtime from most security breaches and malware. If implemented correctly, AlertDispatcher system is very secure.

The AlertDispatcher IT Security Guide is divided into two parts. Part one covers securing your system and Windows. Part two covers securing AlertDispatcher.

Note: *This is only a basic guide only covers basic security measures. For critical system, please consult with your corporate IT security team or consultant before deploying your system. Refer to the disclaimer on the beginning of the document.*

2). Securing the System/Windows

One important approach to improving information security is to reduce the attack surface of a system or software. By turning off unnecessary functionality, limiting network access and user access to these functionality, there would be fewer security risks.

Note: *Before hardening any system, please ensure AlertDispatcher works first and turn off functionality in batches so that if AlertDispatcher stops working, you can reverse that change.*

a). Limiting network access to AlertDispatcher system

i). Scenario A: No corporate network access is required

1. Unplug from local network

If you're only sending SMS using SMS modem, and you're using AlertDispatcher as a standalone system and do not need to connect AlertDispatcher to other systems on your corporate network, you may disconnect your AlertDispatcher system from your corporate network switch as AlertDispatcher does not require Internet or network connection in order to send SMS.

If your application/management software is on another system, you may connect it to AlertDispatcher system directly (local network) instead of through the corporate network switch.

ii). Scenario B: Network access is required

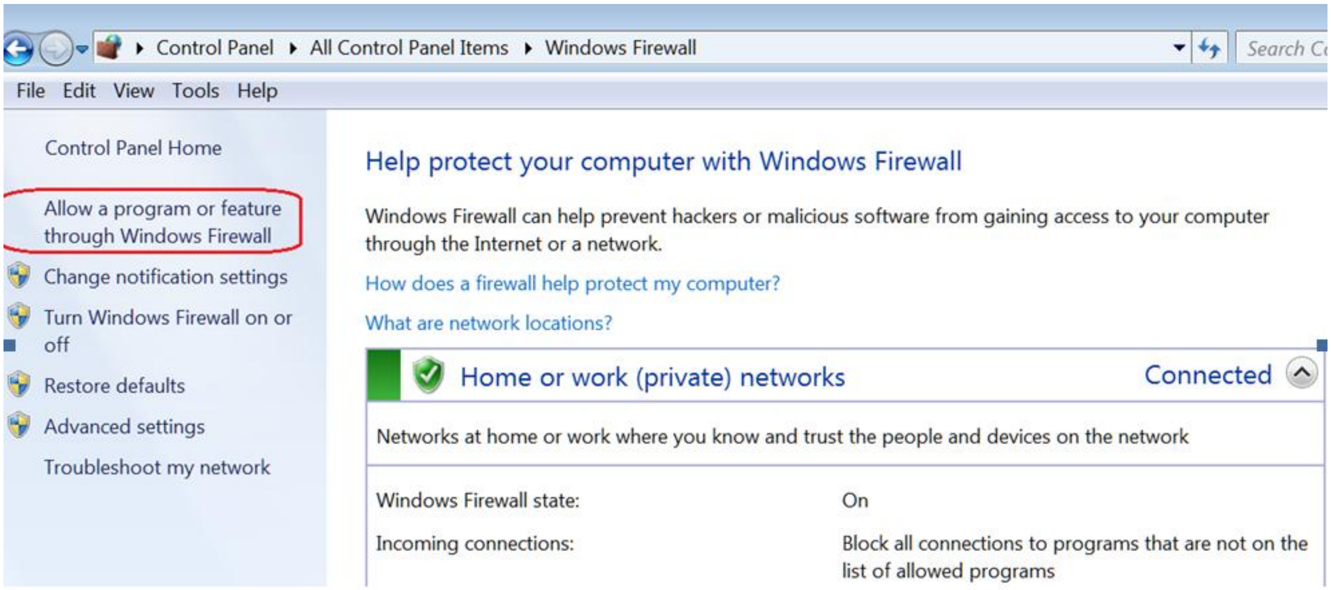
If you need to connect AlertDispatcher system to other systems on your corporate network, the following actions are recommended.

1. Enable Windows Firewall

Go to *Start* → *Control Panel* → *Windows Defender Firewall*, enable Windows Firewall.

Windows Firewall should be enabled even if you're using a hardware firewall appliance. After that, you would need to add AlertDispatcher applications that need to be allowed to communicate through Windows Firewall.

Server Protocol	Port	Purpose/Protocol	Service Application Path (default)
HTTP Server	80 TCP	Receiving alarms via HTTP GET/POST	C:\Program Files (x86)\AlertDispatcher\HTTPListener.exe
SMTP Server	25 TCP	Receiving alarms via Email (SMTP)	C:\Program Files (x86)\AlertDispatcher\SMTPListener.exe
SNMP Trap Receiver	162 UDP	Receiving alarms via SNMP Traps	C:\Program Files (x86)\AlertDispatcher\SNMPTrapReceiver.exe
AlertDispatcher Server	5556 TCP	AlertDispatcher Heartbeat/Failover (For Master/Slave redundancy Setup)	C:\Program Files (x86)\AlertDispatcher\AlertDispatcherServer.exe


Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search C
File Edit View Tools Help
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
How does a firewall help protect my computer?
What are network locations?

Help protect your computer with Windows Firewall

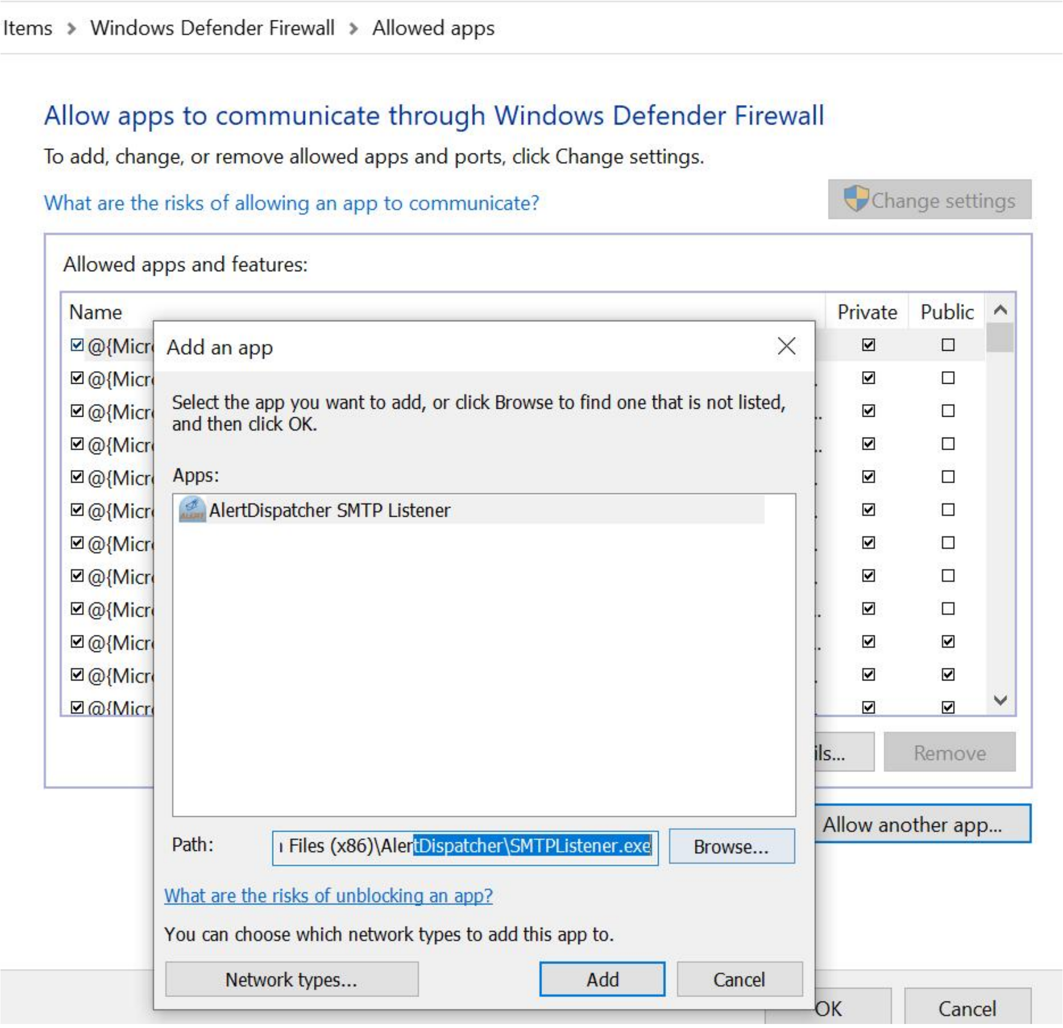
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

Home or work (private) networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state: On

Incoming connections: Block all connections to programs that are not on the list of allowed programs



Items › Windows Defender Firewall › Allowed apps

Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☑ @{Micr	☑	□
☑ @{Micr	☑	□
☑ @{Micr	☑	□
☑ @{Micr	☑	□
☑ @{Micr	☑	□
☑ @{Micr	☑	□
☑ @{Micr	☑	□
☑ @{Micr	☑	□
☑ @{Micr	☑	□
☑ @{Micr	☑	☑
☑ @{Micr	☑	☑
☑ @{Micr	☑	☑

Add an app

Select the app you want to add, or click Browse to find one that is not listed, and then click OK.

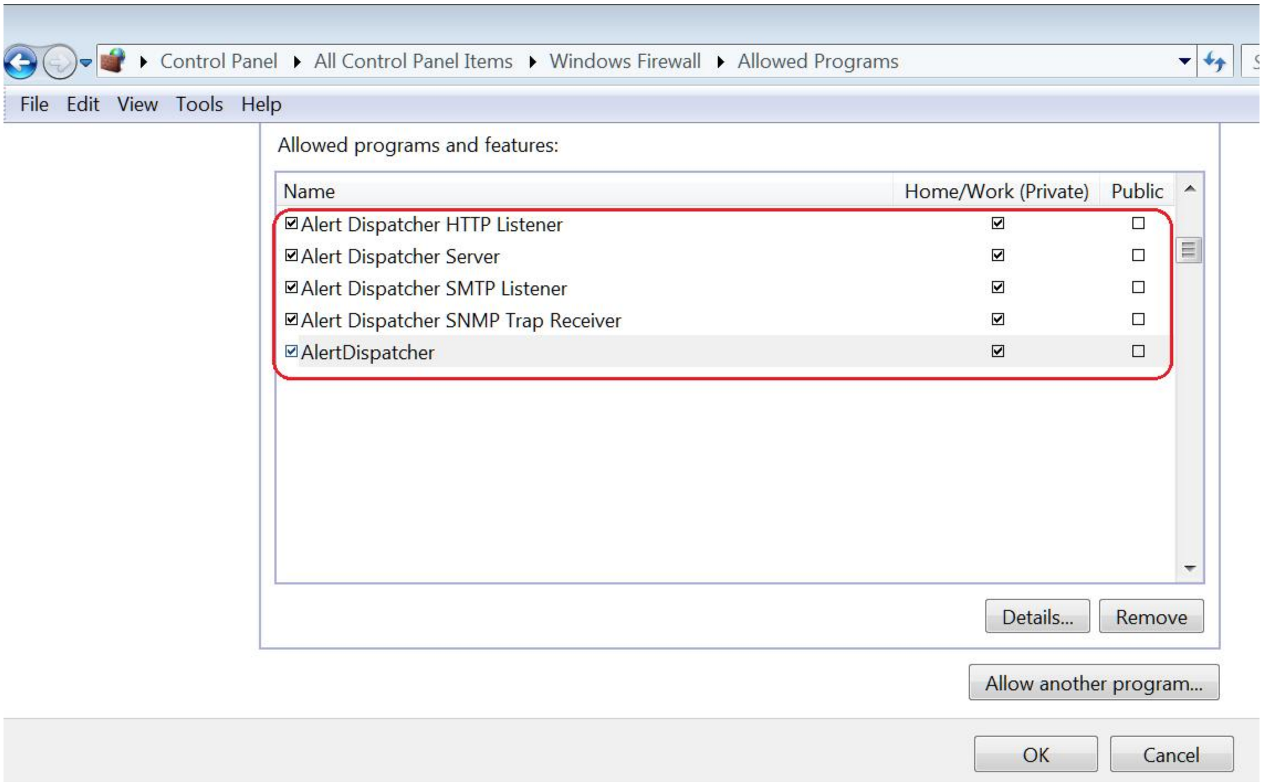
Apps:

AlertDispatcher SMTP Listener

Path: ı Files (x86)\AlertDispatcher\SMTPListener.exe

What are the risks of unblocking an app?

You can choose which network types to add this app to.


Control Panel ▸ All Control Panel Items ▸ Windows Firewall ▸ Allowed Programs
File Edit View Tools Help
Details...
Remove
Allow another program...
OK
Cancel

Allowed programs and features:

Name	Home/Work (Private)	Public
☑ Alert Dispatcher HTTP Listener	☑	□
☑ Alert Dispatcher Server	☑	□
☑ Alert Dispatcher SMTP Listener	☑	□
☑ Alert Dispatcher SNMP Trap Receiver	☑	□
☑ AlertDispatcher	☑	□

***Note:** For full details of ports and firewall configuration, please refer to "AlertDispatcher Pre-installation & Firewall Ports Checklist.pdf".*

2. Install anti-virus software

Install anti-virus software on your AlertDispatcher system. Configure your anti-virus for maximum security. If you do not have an anti-virus software, you can turn on Windows Defender.

Note:

1. Some anti-virus software heuristic scan are very sensitive and may detect AlertDispatcher and its components as a malware. To avoid positive false positive detections that may disable AlertDispatcher functionality without notice, you may consider adding a folder exclusion for AlertDispatcher program folder – "C:\Program Files (x86)\AlertDispatcher". This should be done only after you have done a complete system scan to ensure the system is free from malware. Kindly please inform us of any AV detections and submit a screen capture.

2. Some antivirus software such as McAfee VirusScan may block SMTP email interfacing to AlertDispatcher so you will need to add an exception. Refer to the "AlertDispatcher Quick Installation Guide.pdf" for details.

b). Limiting personnel access to AlertDispatcher system / Removing admin rights for users

As far as possible, do not install AlertDispatcher on workstations where users logon to perform their daily tasks. It is preferable to install AlertDispatcher on a dedicated machine, a file server or database server. The AlertDispatcher system can be installed on a Windows workstation or Server OS.

To manage AlertDispatcher installed on a separate machine, you may install AlertDispatcher Client on a workstation (Client only installation), and configure it to logon to remote AlertDispatcher system. Allowing users to RDP into remote server is not recommended. ***Note:*** *This functionality is only available for AlertDispatcher Corporate and Enterprise Editions.*

If you are required to install AlertDispatcher onto a workstation, please remove administrator and software install rights for users that logon to this workstations. It is not necessary to have administrator right to use AlertDispatcher.

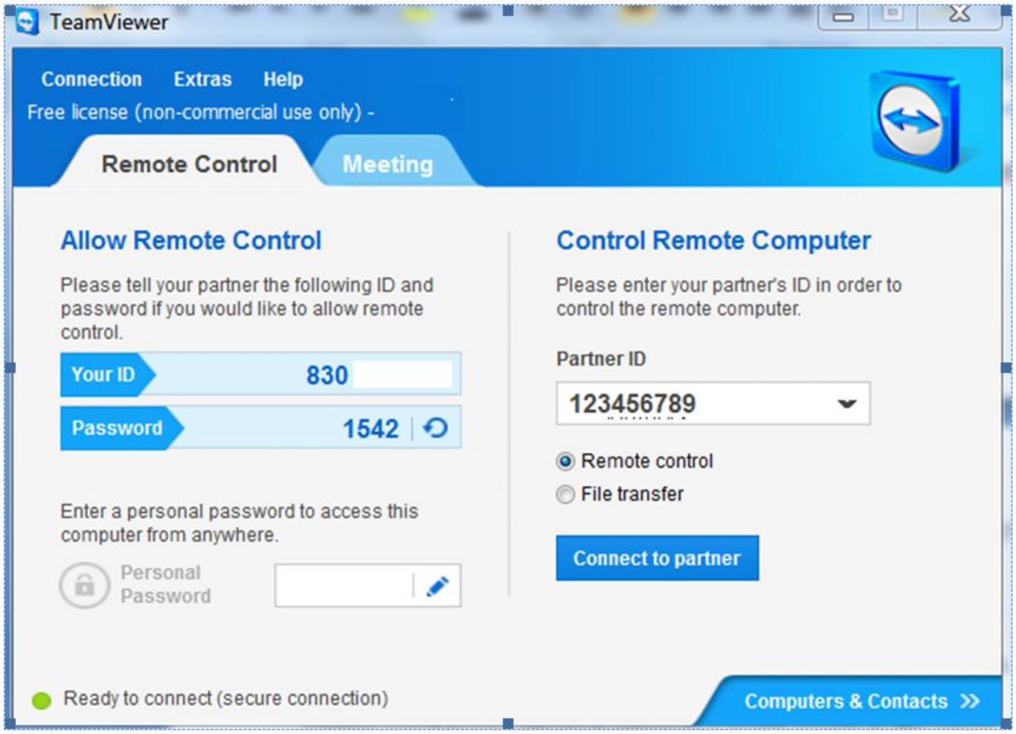
c). Using complex and unique passwords for Windows and any third party remote access software used to access to server.

If you are accessing the server via remote access such as using Windows RDP or any third party remote access software such as Teamviewer, you should secure the access by making the following changes:

i). Use a difficult to guess password.

Do not use simple passwords such as ‘1234’ or ‘8888’ as a hacker may gain access to your system by brute force password guessing. Do not reuse password. You may add project name for easy recall. A secure password will look like this – “SMSAlert28@168!&”.

Windows passwords should preferably be at least 12 characters long, and contain upper and lower cases letters, numerals and punctuation mark. Ensure the password is unique and not used for other application login. To avoid forgetting the password, you can write it down on paper or store it in an encrypted password protected file.



Please tell your partner the following ID and password if you would like to allow remote control.

Your ID 830

Password 1542

Enter a personal password to access this computer from anywhere.

Personal Password

Please enter your partner's ID in order to control the remote computer.

Partner ID 123456789

● Remote control

○ File transfer

Ready to connect (secure connection)

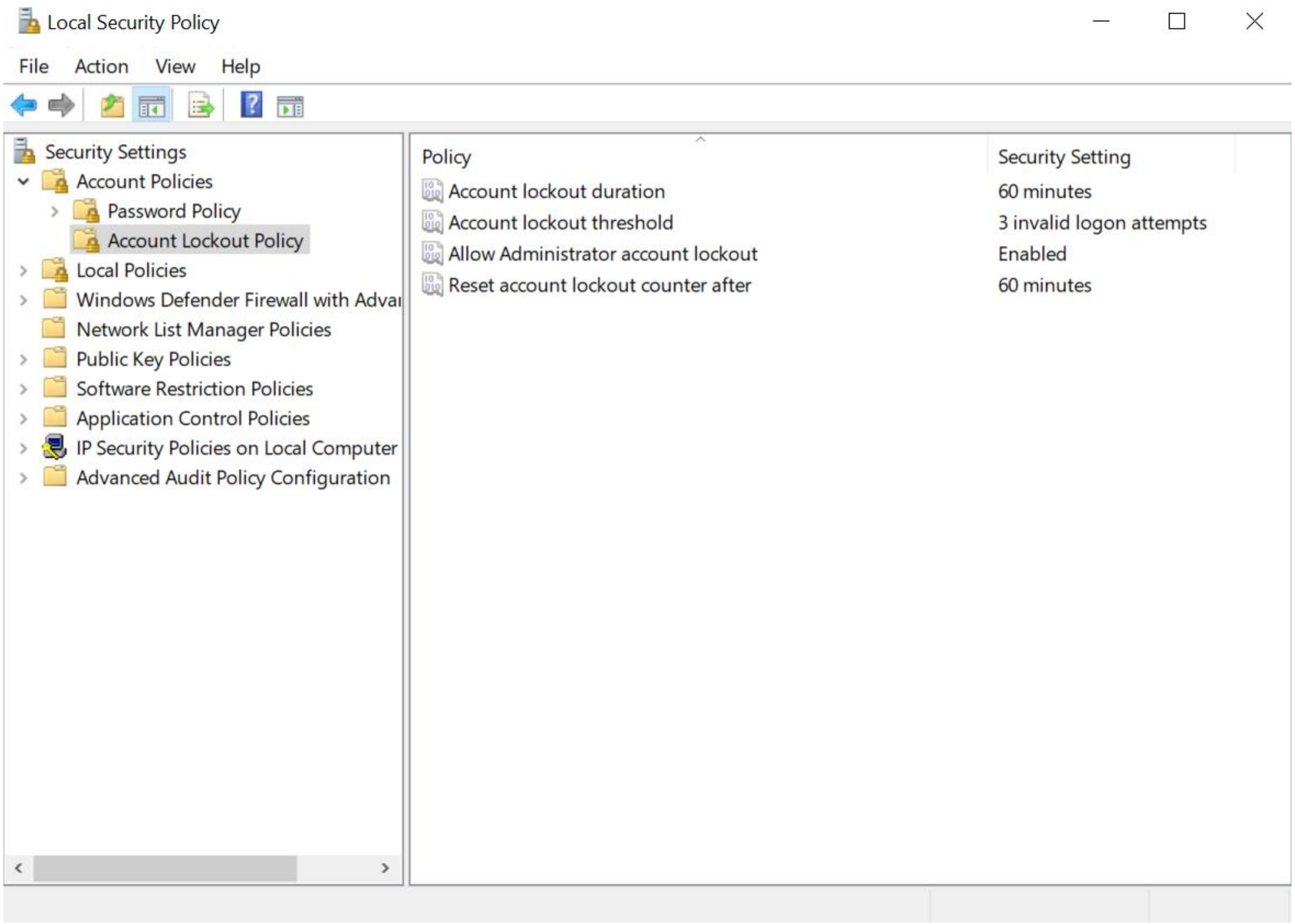
ii). Set an account lockout policy for RDP access.

If RDP access is enabled on your AlertDispatcher system, you should always set an account lockout policy to deter brute force password guessing attacks. From the same Local Security Policy screen from before, go to Account Policies → Account Lockout Policy.

Account lockout duration: This is how long the user will be unable to logon after several failed attempts. This should be set to at least 15 minutes.

Account lockout threshhold: This is the number of failed logon attempts before the user is locked-out. Three is usually sufficient to indicate someone is trying to break in.

Allow Administrator account lockout: This will apply account lockout policy to even local administrator accounts.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Advai
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	60 minutes
Account lockout threshold	3 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	60 minutes

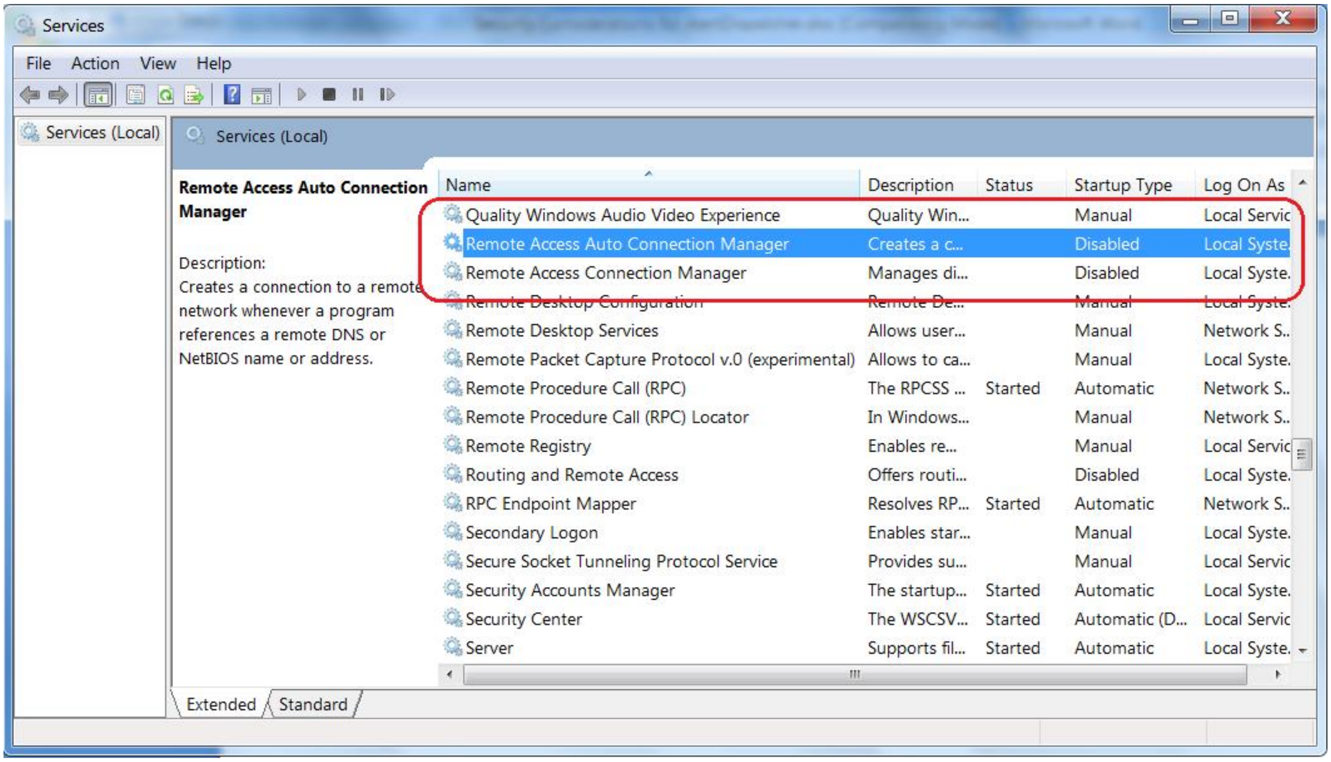
d). Update Windows Regularly

Run Windows update and download the latest Windows security patches.

***Note:** If you need to upgrade to latest Windows, e.g. Windows 10 or 11, please ensure that your AlertDspatcher version is compatible. Always test your AlertDispatcher after every update.*

e). Disable and Uninstall Unnecessary Windows Services

Disable and if possible uninstall Fax, Telephony, Remote Access Connection Manager, and Remote Access Auto Connection Manager Services on your machine if you do not use them. These services are not required by AlertDispatcher.



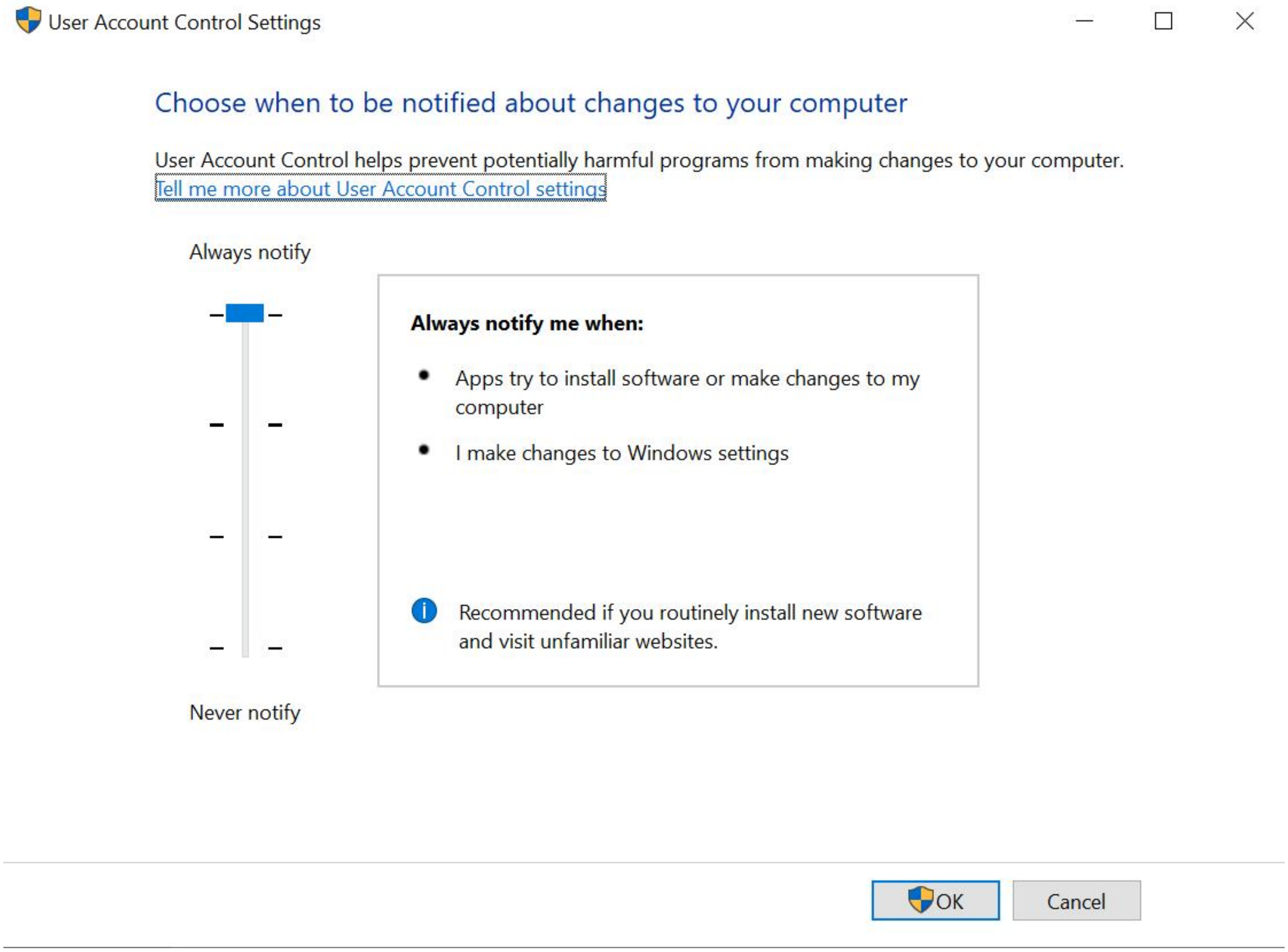
Remote Access Auto Connection Manager

Description:
Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.

Name	Description	Status	Startup Type	Log On As
Quality Windows Audio Video Experience	Quality Win...		Manual	Local Servic
Remote Access Auto Connection Manager	Creates a c...		Disabled	Local Syste.
Remote Access Connection Manager	Manages di...		Disabled	Local Syste.
Remote Desktop Configuration	Remote De...		Manual	Local Syste.
Remote Desktop Services	Allows user...		Manual	Network S..
Remote Packet Capture Protocol v.0 (experimental)	Allows to ca...		Manual	Local Syste.
Remote Procedure Call (RPC)	The RPCSS ...	Started	Automatic	Network S..
Remote Procedure Call (RPC) Locator	In Windows...		Manual	Network S..
Remote Registry	Enables re...		Manual	Local Servic
Routing and Remote Access	Offers routi...		Disabled	Local Syste.
RPC Endpoint Mapper	Resolves RP...	Started	Automatic	Network S..
Secondary Logon	Enables star...		Manual	Local Syste.
Secure Socket Tunneling Protocol Service	Provides su...		Manual	Local Servic
Security Accounts Manager	The startup...	Started	Automatic	Local Syste.
Security Center	The WSCSV...	Started	Automatic (D...	Local Servic
Server	Supports fil...	Started	Automatic	Local Syste.

f). Turn on User Account Control (UAC) and set to highest

Turn on User Account Control (UAC) and set to “Always notify me…”.



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

Always notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

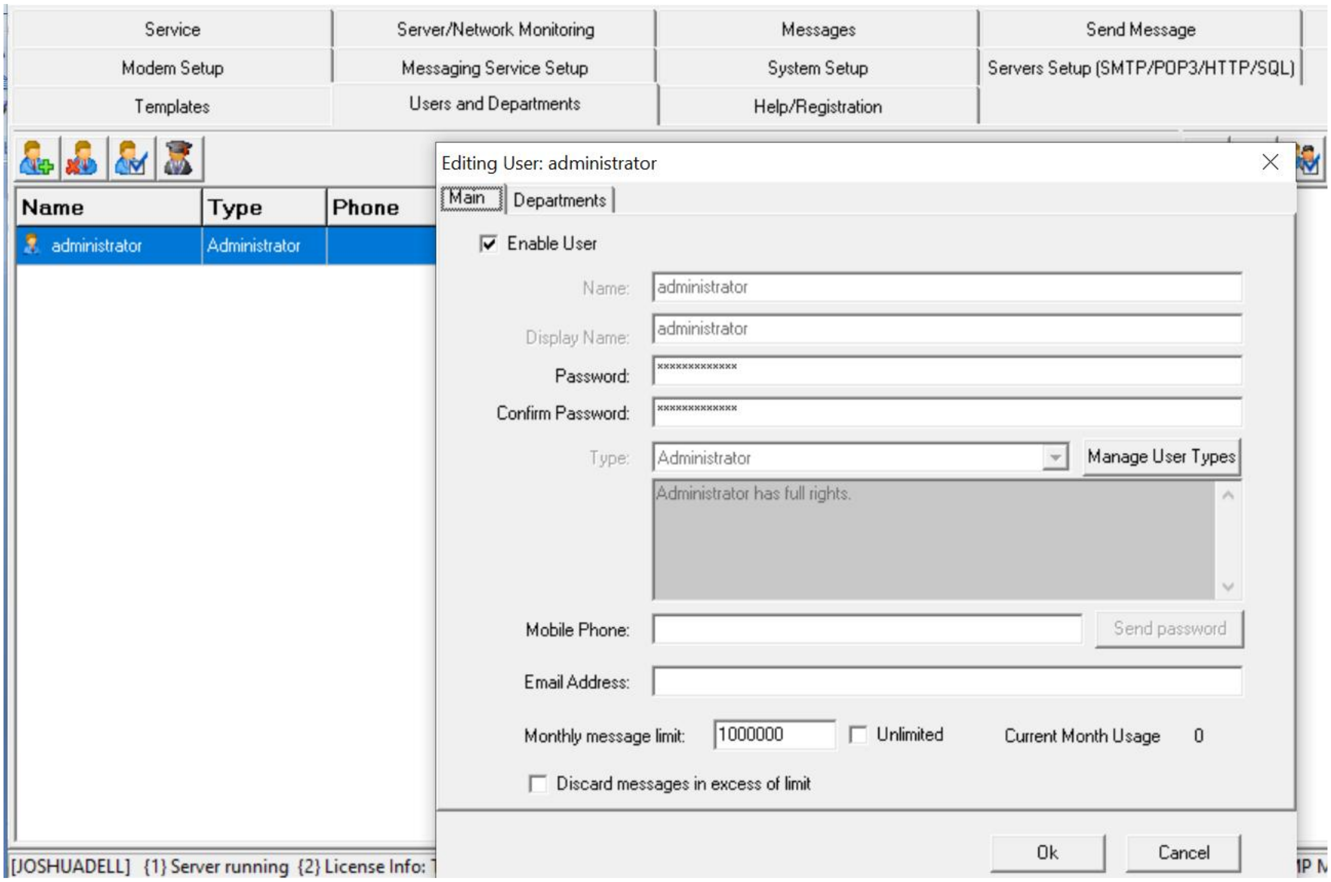
Recommended if you routinely install new software and visit unfamiliar websites.

Never notify

3). Securing AlertDispatcher

a). Change AlertDispatcher Administrator password and create users with lower rights.

Change the default password for “administrator”.



Editing User: administrator

Name	Type	Phone
administrator	Administrator	

☑ Enable User

Name: administrator

Display Name: administrator

Password: **************

Confirm Password: **************

Type: Administrator

Administrator has full rights.

Mobile Phone:

Email Address:

Monthly message limit: 1000000 □ Unlimited Current Month Usage 0

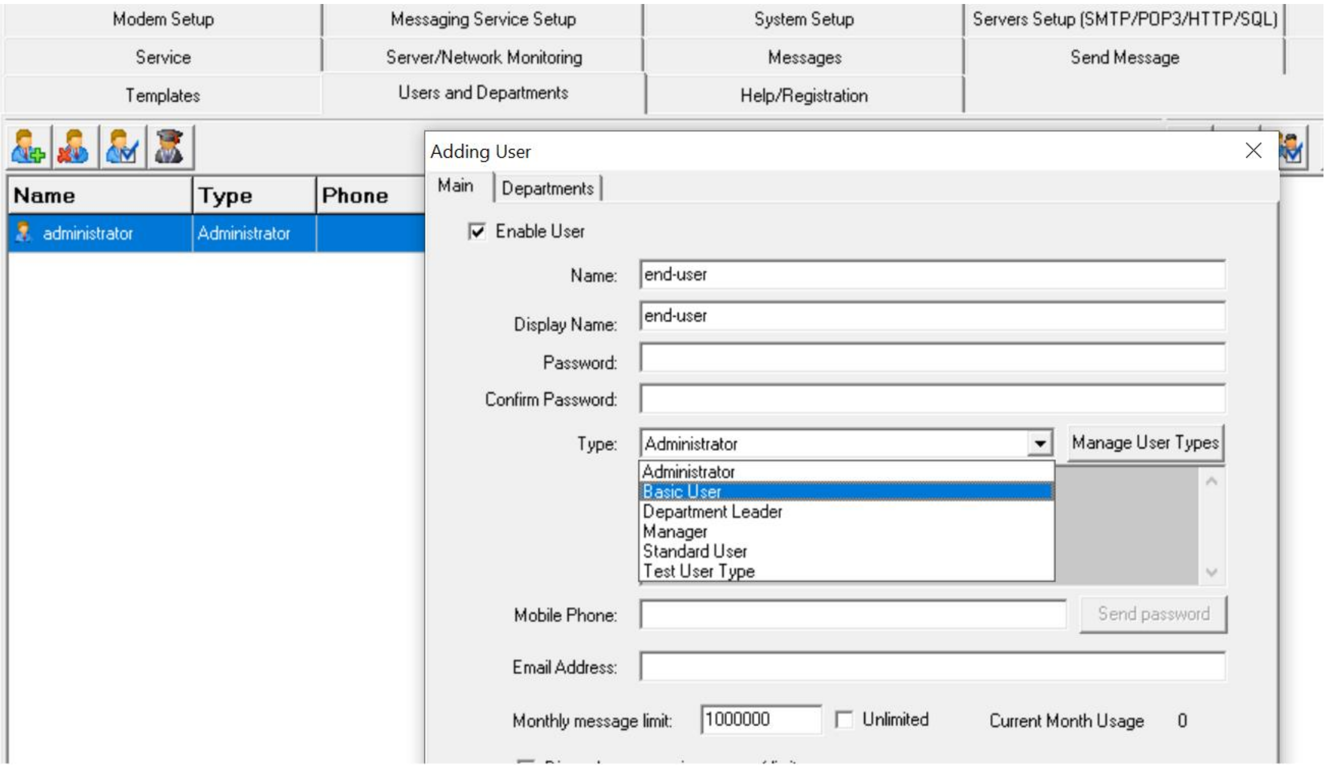
□ Discard messages in excess of limit

[JOSHUADELL] {1} Server running {2} License Info:

If you’re using the Corporate license (or higher), you can create a separate login user account with limited access right for each user. ***Tip:*** *If AlertDispatcher is installed on a server, you can copy the AlertDispatcher Client to a workstation and configure it connect to the server using a login user account (AlertDispatcher) with lower access rights.*

Every login user created is assigned to a user type that has a different set of access right. The following user types are pre-created – 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.



Name	Type	Phone
administrator	Administrator	

☑ Enable User

Name: end-user

Display Name: end-user

Password:

Confirm Password:

Type: Administrator

- Administrator
- Basic User
- Department Leader
- Manager
- Standard User
- Test User Type

Mobile Phone:

Email Address:

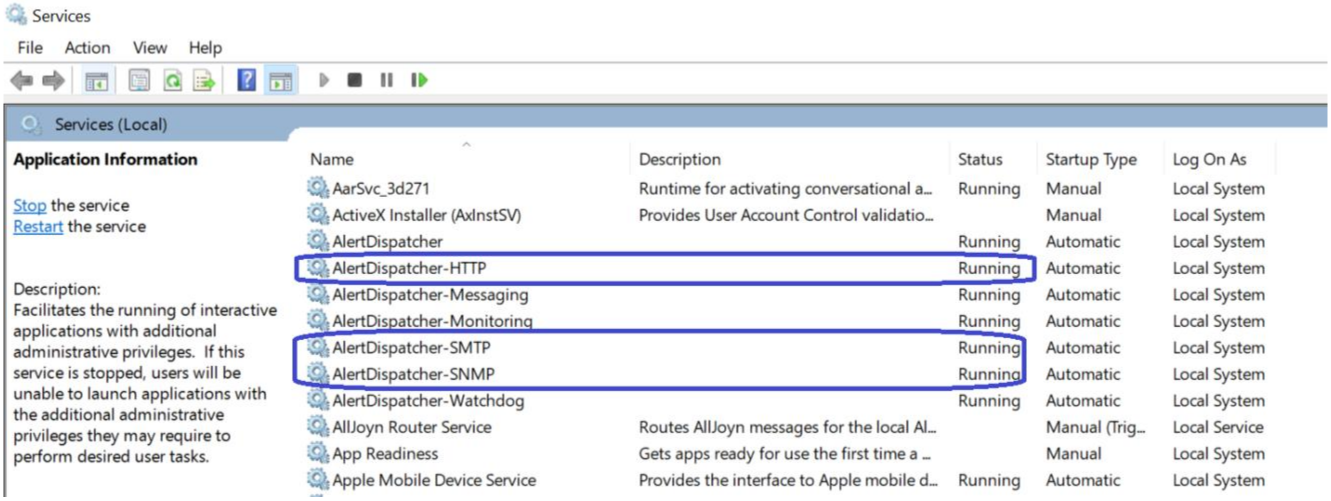
Monthly message limit: 1000000 □ Unlimited Current Month Usage 0

b). Disable or limit AlertDispatcher Network and API interfaces that you do not require.

i). Disable AlertDispatcher network services that are not required.

For the convenience of new users, AlertDispatcher built-in SMTP, HTTP and SNMP Server interfaces maybe enabled by default. You can shutdown and disable any of these services that are not required by using Windows Service Manager.

Go to *Start* → *Control Panel* → *Administrative Tools* → *Services* and ensure that AlertDispatcher-HTTP, AlertDispatcher-SMTP and AlertDispatcher-SNMP services are stopped and disabled.



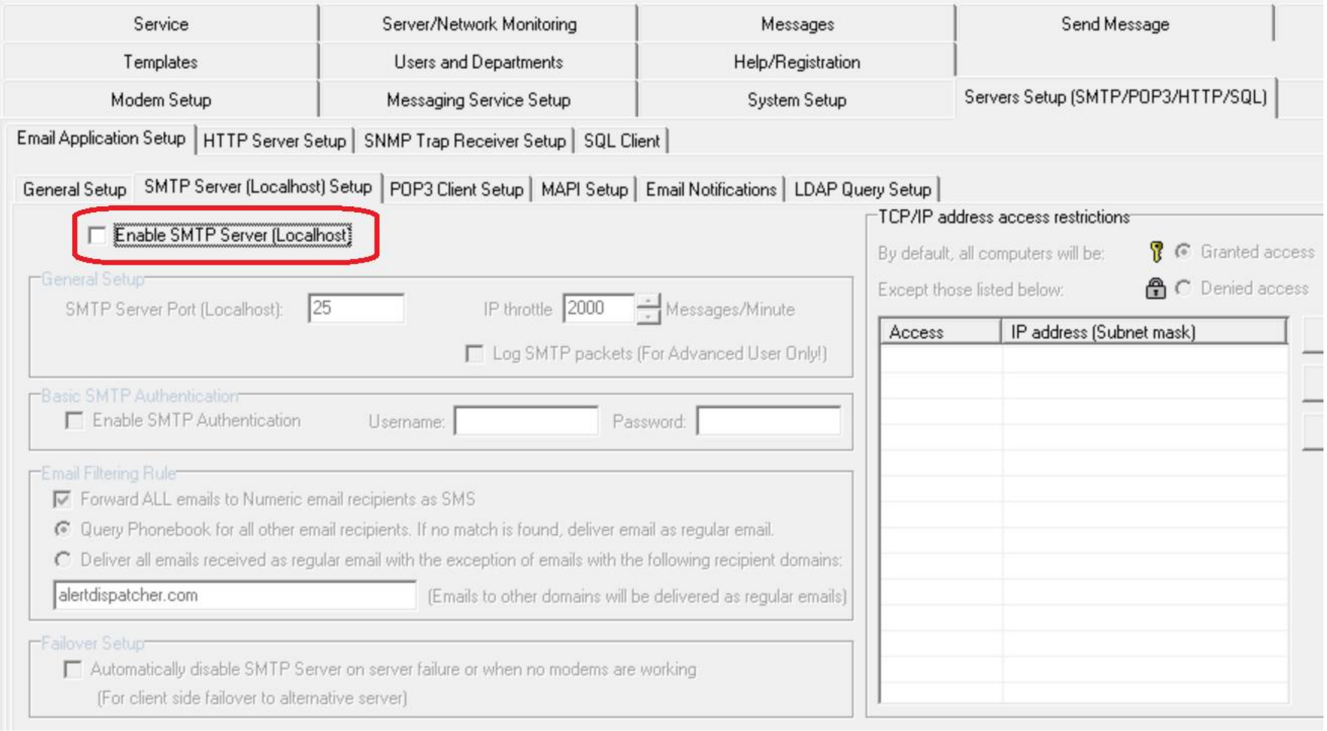
Application Information

Stop the service
Restart the service

Description:
Facilitates the running of interactive applications with additional administrative privileges. If this service is stopped, users will be unable to launch applications with the additional administrative privileges they may require to perform desired user tasks.

Name	Description	Status	Startup Type	Log On As
AarSvc_3d271	Runtime for activating conversational a...	Running	Manual	Local System
ActiveX Installer (AxInstSV)	Provides User Account Control validatio...		Manual	Local System
AlertDispatcher		Running	Automatic	Local System
AlertDispatcher-HTTP		Running	Automatic	Local System
AlertDispatcher-Messaging		Running	Automatic	Local System
AlertDispatcher-Monitoring		Running	Automatic	Local System
AlertDispatcher-SMTP		Running	Automatic	Local System
AlertDispatcher-SNMP		Running	Automatic	Local System
AlertDispatcher-Watchdog		Running	Automatic	Local System
AllJoyn Router Service	Routes AllJoyn messages for the local Al...		Manual (Trig...	Local Service
App Readiness	Gets apps ready for use the first time a ...		Manual	Local System
Apple Mobile Device Service	Provides the interface to Apple mobile d...	Running	Automatic	Local System

Alternatively, you can disable the Server interfaces using the Client.



□ Enable SMTP Server (Localhost)

General Setup

SMTP Server Port (Localhost): 25

IP throttle 2000 Messages/Minute

□ Log SMTP packets (For Advanced User Only!)

Basic SMTP Authentication

□ Enable SMTP Authentication Username: Password:

Email Filtering Rule

☑ Forward ALL emails to Numeric email recipients as SMS

● Query Phonebook for all other email recipients. If no match is found, deliver email as regular email.

○ Deliver all emails received as regular email with the exception of emails with the following recipient domains:

alertdispatcher.com (Emails to other domains will be delivered as regular emails)

Failover Setup

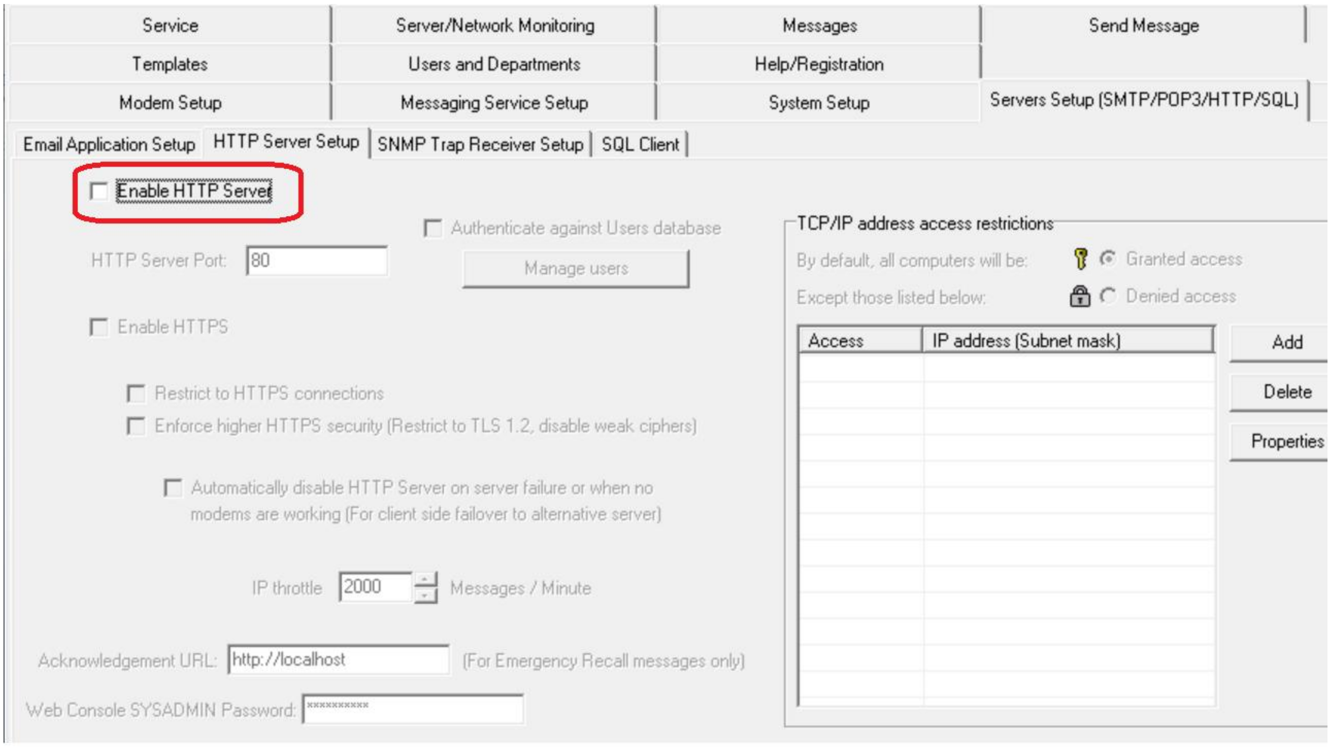
□ Automatically disable SMTP Server on server failure or when no modems are working (For client side failover to alternative server)

TCP/IP address access restrictions

By default, all computers will be: ● Granted access

Except those listed below: ○ Denied access

Access	IP address (Subnet mask)



□ Enable HTTP Server

□ Authenticate against Users database

HTTP Server Port: 80

□ Enable HTTPS

□ Restrict to HTTPS connections

□ Enforce higher HTTPS security (Restrict to TLS 1.2, disable weak ciphers)

□ Automatically disable HTTP Server on server failure or when no modems are working (For client side failover to alternative server)

IP throttle 2000 Messages / Minute

Acknowledgement URL: http://localhost (For Emergency Recall messages only)

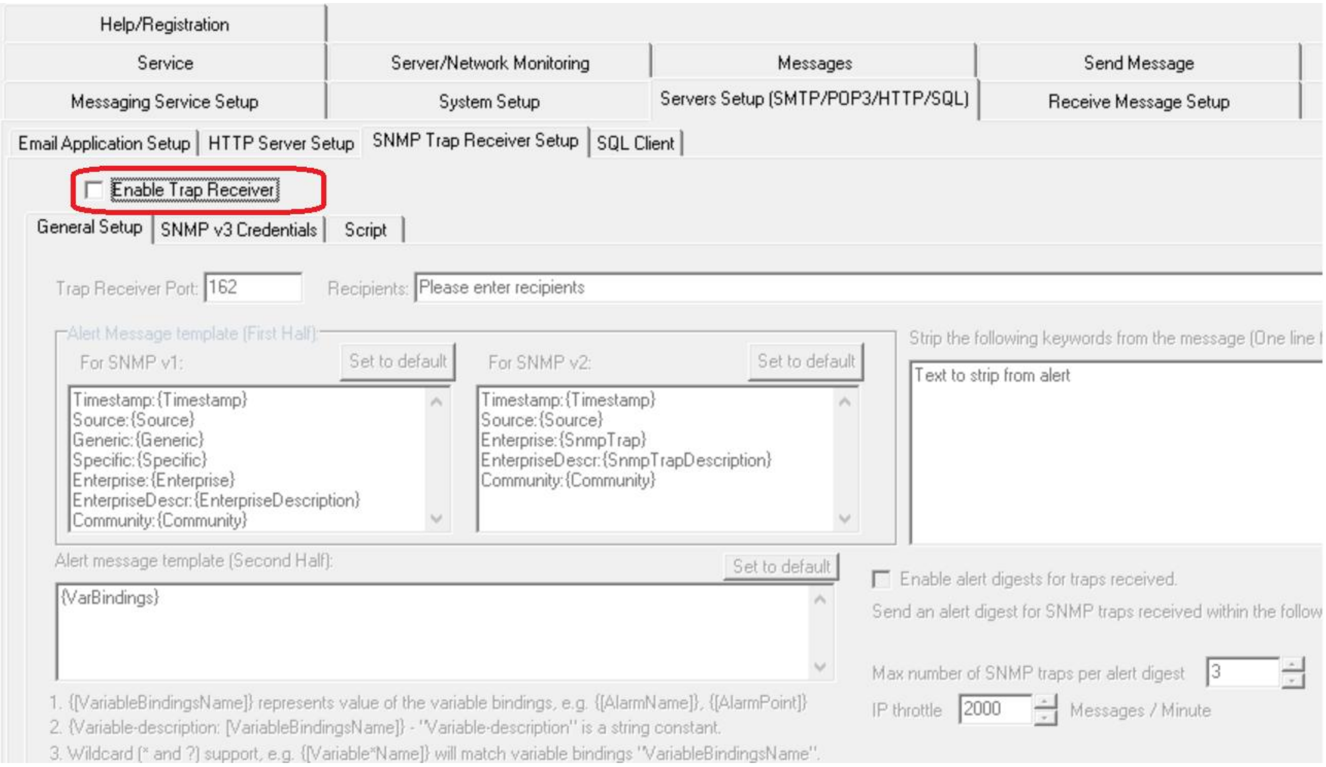
Web Console SYSADMIN Password: **********

TCP/IP address access restrictions

By default, all computers will be: ● Granted access

Except those listed below: ○ Denied access

Access	IP address (Subnet mask)



□ Enable Trap Receiver

Trap Receiver Port: 162

Recipients: Please enter recipients

Alert Message template (First Half)

For SNMP v1:

```
Timestamp:{Timestamp}
Source:{Source}
Generic:{Generic}
Specific:{Specific}
Enterprise:{Enterprise}
EnterpriseDescr:{EnterpriseDescription}
Community:{Community}
```

For SNMP v2:

```
Timestamp:{Timestamp}
Source:{Source}
Enterprise:{SnmpTrap}
EnterpriseDescr:{SnmpTrapDescription}
Community:{Community}
```

Strip the following keywords from the message (One line f

Text to strip from alert

Alert message template (Second Half):

```
{VarBindings}
```

1. {[VariableBindingsName]} represents value of the variable bindings, e.g. {[AlarmName]}, {[AlarmPoint]}
2. {Variable-description: [VariableBindingsName]} - "Variable-description" is a string constant.
3. Wildcard (* and ?) support, e.g. {[Variable*Name]} will match variable bindings "VariableBindingsName".

□ Enable alert digests for traps received.

Send an alert digest for SNMP traps received within the follow

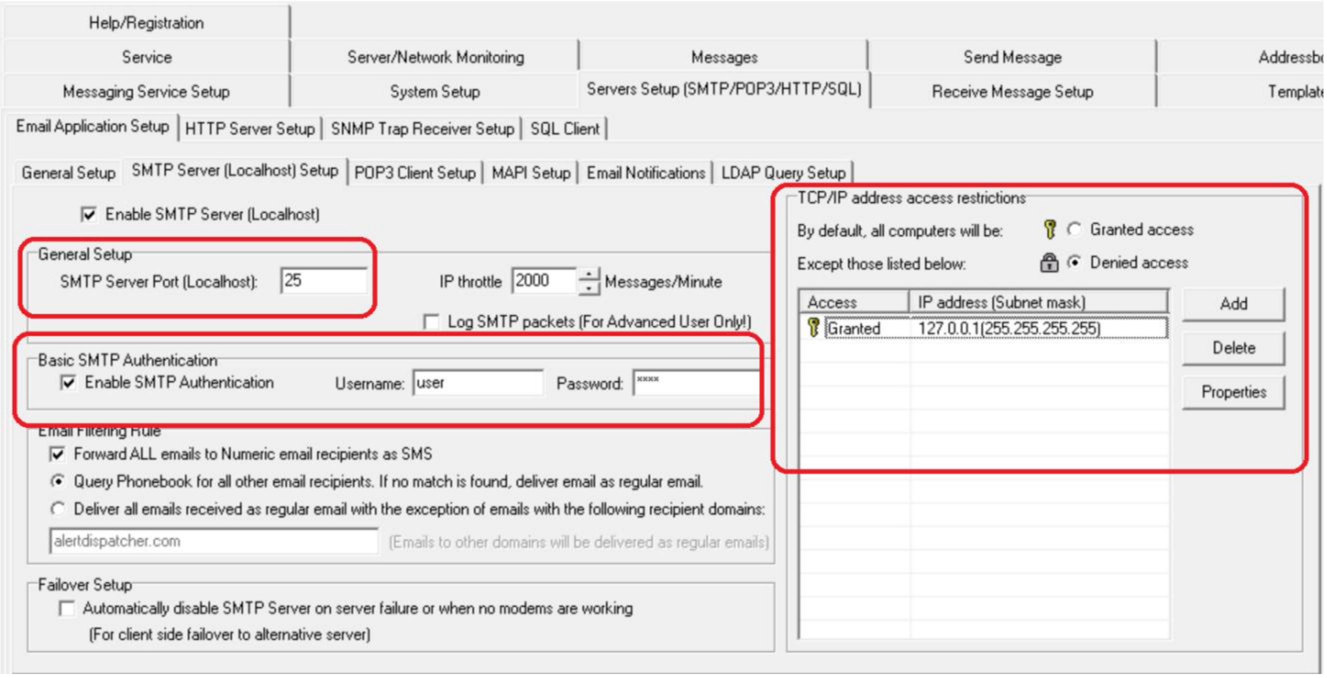
Max number of SNMP traps per alert digest 3

IP throttle 2000 Messages / Minute

ii). Authenticate clients and change default ports.

The AlertDispatcher SMTP Server interface supports Basic SMTP Authentication (disabled by default). You can also limit access to SMTP clients on predefined IP addresses. The SMTP Server listens to port 25 by default.

Access to SMTP Server can also be restricted to specific IP address or IP address ranges.



☑ Enable SMTP Server (Localhost)

General Setup

SMTP Server Port (Localhost): 25

IP throttle 2000 Messages/Minute

□ Log SMTP packets (For Advanced User Only!)

Basic SMTP Authentication

☑ Enable SMTP Authentication Username: user Password: ****

Email Filtering Rule

☑ Forward ALL emails to Numeric email recipients as SMS

● Query Phonebook for all other email recipients. If no match is found, deliver email as regular email.

○ Deliver all emails received as regular email with the exception of emails with the following recipient domains:

alertdispatcher.com (Emails to other domains will be delivered as regular emails)

Failover Setup

□ Automatically disable SMTP Server on server failure or when no modems are working (For client side failover to alternative server)

TCP/IP address access restrictions

By default, all computers will be: ○ Granted access

Except those listed below: ● Denied access

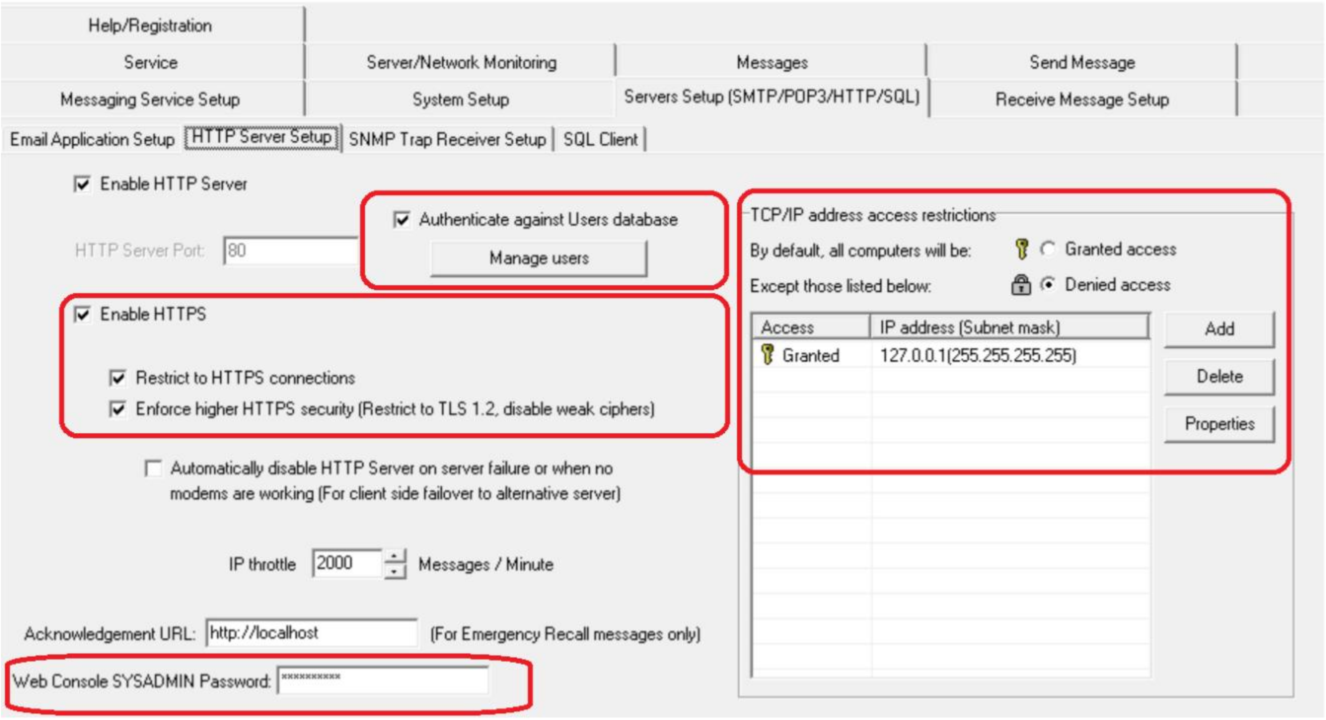
Access	IP address (Subnet mask)
Granted	127.0.0.1(255.255.255.255)

You can setup the credential for HTTP Server interface as shown below. If “Authenticate against Users database” is checked, any send message or check server request sent to the HTTP Server interface will have to be furnished with username and password – see “Users and Departments” tab.

For added security, enable HTTPS and restrict to HTTPS connections only.

Similarly as for SMTP Server, you can restrict access to HTTP Server to specific IP address or IP address ranges.

The Web Console SYSADMIN password can also be changed. This should be changed if you’ve enabled the HTTP Server interface.



☑ Enable HTTP Server

HTTP Server Port: 80

☑ Authenticate against Users database

☑ Enable HTTPS

☑ Restrict to HTTPS connections

☑ Enforce higher HTTPS security (Restrict to TLS 1.2, disable weak ciphers)

□ Automatically disable HTTP Server on server failure or when no modems are working (For client side failover to alternative server)

IP throttle 2000 Messages / Minute

Acknowledgement URL: http://localhost (For Emergency Recall messages only)

Web Console SYSADMIN Password: **********

TCP/IP address access restrictions

By default, all computers will be: ○ Granted access ● Denied access

Except those listed below:

Access	IP address (Subnet mask)
Granted	127.0.0.1(255.255.255.255)

b). Divert calls to another phone and restricting access to the SMS modem (SIM Card).

To prevent strangers from trying to call the SMS modem, you can place the SIM card into your cellphone and divert all voice calls to another line. This will prevent anyone from dialing directly to the SMS modem. Your telco may also provide SIM cards where voice calls are disabled.

Note: *AlertDispatcher will terminate all phone calls to the SMS modem even if you do not divert the call. However, the call will still ring for a few seconds.*

c). Refrain from sending credentials and private information via AlertDispatcher

We would not recommend sending private information such as public IP addresses, user login IDs and user login passwords via AlertDispatcher. For mission critical operations, you may consult with your vendor for further discussion.