AlertDispatcher IT Security Guide

Last update: 1 May 2026

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 explains how to secure AlertDispatcher against external IT security threats and internal misuse. We recommend that administrators read this guide before installing or operating the system.

Even basic security measures can help reduce the risk of downtime caused by security breaches, malware, or incorrect settings. When installed and maintained correctly, AlertDispatcher can be made very secure.

This guide is divided into two parts:

Part One covers general system and Windows security.
Part Two covers AlertDispatcher-specific security.

Important Note:

1. This guide provides general security recommendations and cannot cover every possible setup or situation. For critical systems, please consult your corporate IT security team or a qualified security consultant before deployment.

2. This guide is intended to support, not replace, standard Windows hardening, host firewall configuration, and proper network firewall controls.

2). Securing the System/Windows

One important way to improve security is to reduce the system's attack surface. This means turning off functions that are not needed, limiting network access, and allowing only authorised users to access the required functions. With fewer exposed functions and access points, there are fewer security risks.

Note: Before hardening any system, make sure AlertDispatcher is working properly. Turn off functions one at a time and test along the way, so if AlertDispatcher stops working, you can identify the cause and reverse the change.

a). Limiting network access to AlertDispatcher system

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

1. Unplug from local network

If you are only sending SMS using an SMS modem, and AlertDispatcher is used as a standalone system, it does not need an Internet or network connection to send SMS.

If AlertDispatcher does not need to connect to other systems on your corporate network, you may disconnect it from the corporate network switch.

If your application or management software is installed on another system, you may connect that system directly to the AlertDispatcher system using a local network connection, instead of connecting through the corporate network switch.

ii). Scenario B: Network access is required

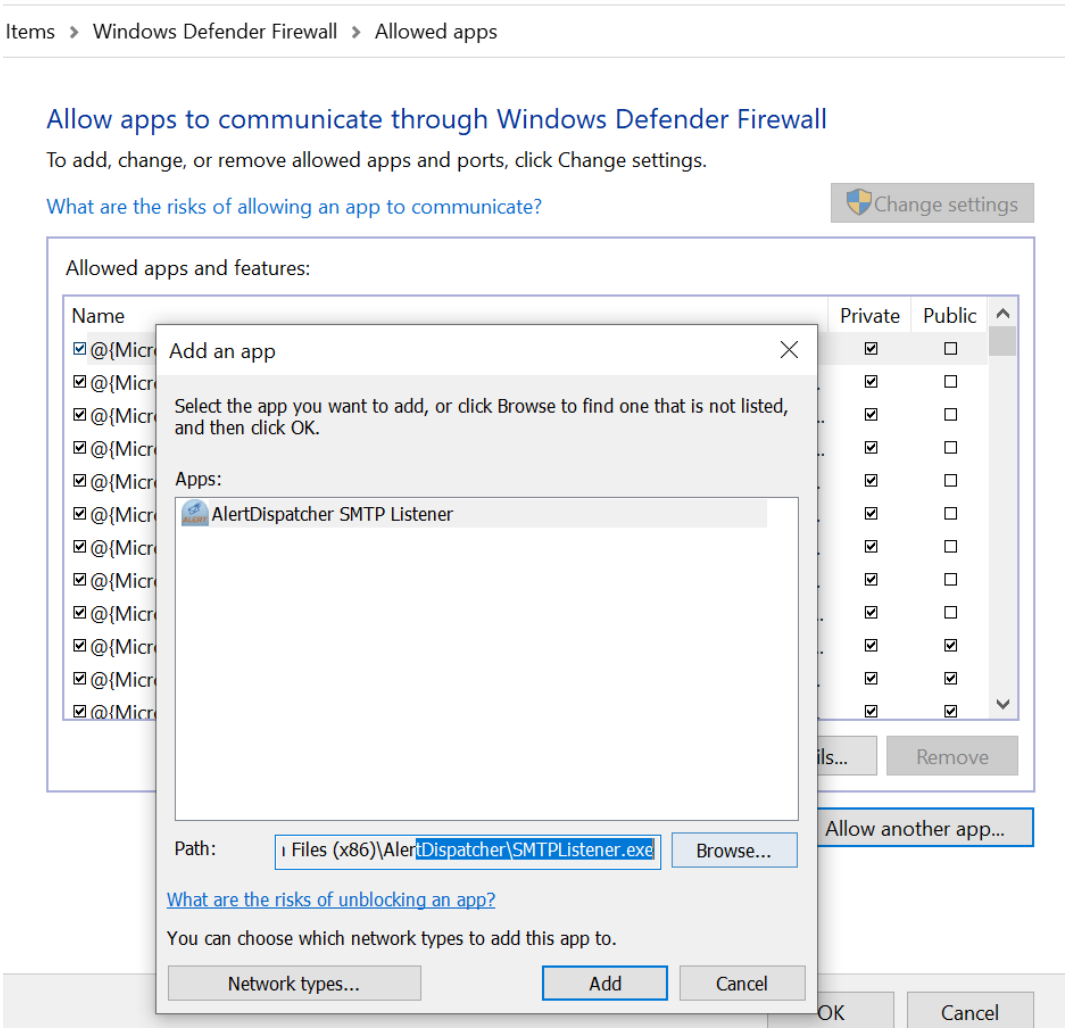
If you need to connect AlertDispatcher system to other systems on your corporate network, the following actions are recommended.

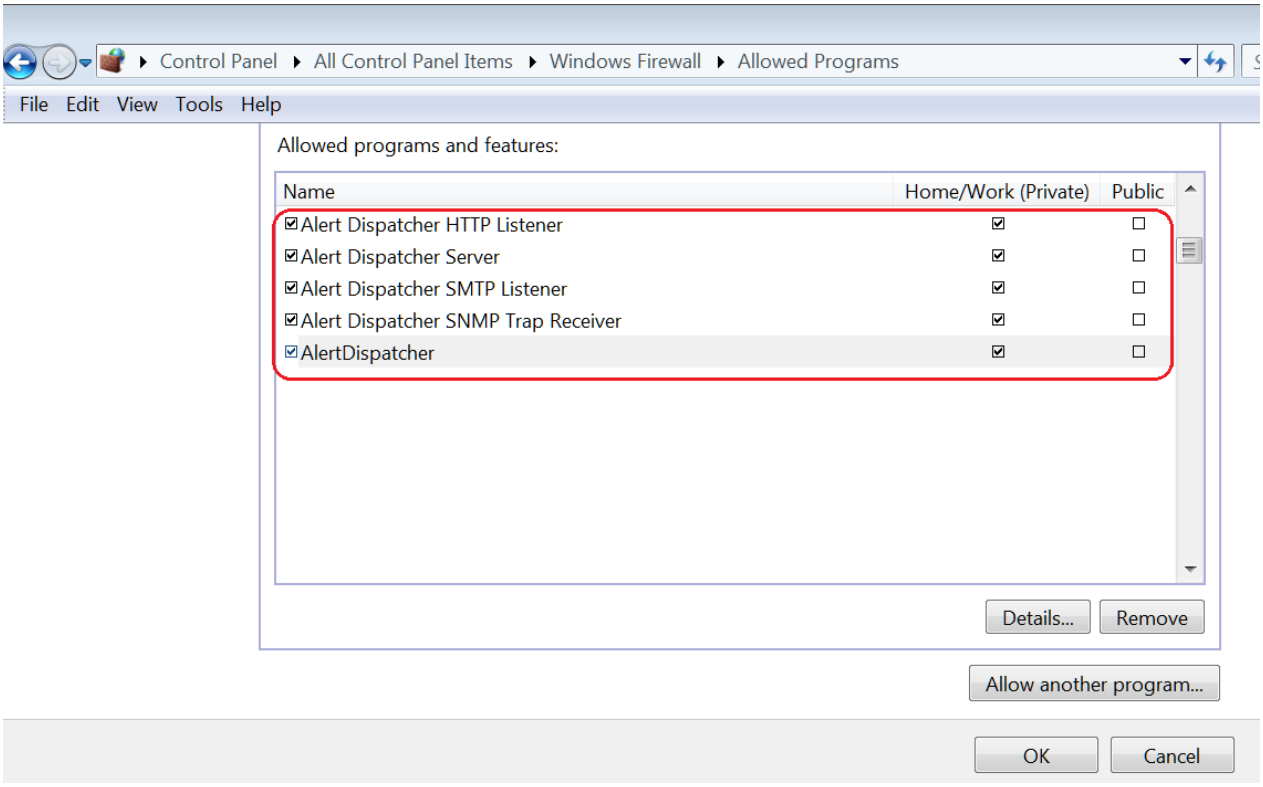
1. Enable Windows Firewall

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

Windows Firewall should remain enabled even if a network firewall is already in use. After enabling Windows Firewall, allow only the required AlertDispatcher applications and ports to communicate through it. Please only allow the required server protocols. If you're unsure, consult with your vendor.

Server Protocol	Port	Purpose/Protocol	Service Application Path (default)
HTTP Server	80/443 TCP	Receiving alarms via HTTP/HTTPS GET/POST	C:\Program Files (x86)\AlertDispatcher\HTTPListener.exe
SMTP Server	25/587 TCP	Receiving alarms via Email (SMTP/SMTP TLS)	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


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?
Change settings
Allowed apps and features:
Name
Private
Public
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:
Files (x86)\AlertDispatcher\SMTPListener.exe
Browse...
What are the risks of unblocking an app?
You can choose which network types to add this app to.
Network types...
Add
Cancel
Remove
Allow another app...
OK
Cancel



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 antivirus software on the AlertDispatcher system and configure it for strong protection. If no third-party antivirus software is installed, enable Windows Defender.

Note:
1. Some antivirus software, such as McAfee VirusScan, may block SMTP email communication with AlertDispatcher. If this happens, add the required exception in the antivirus settings. Refer to "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 used by users for their daily work. It is better to install AlertDispatcher on a dedicated machine, file server, or database server.

AlertDispatcher can be installed on either a Windows workstation OS or Windows Server OS.

To manage AlertDispatcher on a separate machine, you may install *AlertDispatcher Client* on the user's workstation using the *Client Only* installation option. The client can then be configured to log on to the remote AlertDispatcher system.

Allowing users to RDP into the AlertDispatcher server is not recommended.

Note: Remote client access is only available in *AlertDispatcher Corporate* and *Enterprise Editions*.

If AlertDispatcher must be installed on a workstation, remove administrator rights and software installation rights from users who log on to that workstation. Administrator rights are not required to use AlertDispatcher.

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

Important: We strongly discourage the use of third-party remote access software, such as AnyDesk or TeamViewer, because of the risk of security vulnerabilities and unauthorised access.

If remote access is required, RDP access from outside the site should only be allowed through a secure VPN. Enable Network Level Authentication where possible. Disable RDP if it is not required.

If you need to access the server remotely using Windows RDP or third-party remote access software, secure the remote access by applying the following settings:

i). Use a strong password

Do not use simple passwords such as "1234" or "8888". These passwords can be easily guessed by attackers using brute-force methods.

Do not reuse passwords from other systems or applications. Each system should have its own unique password.

A strong password should preferably be at least *12 characters long* and include:

* Uppercase letters
* Lowercase letters
* Numbers
* Symbols or punctuation marks

Example of a stronger password:

SMSAlert28@168!&

You may include a project name or system name in the password to make it easier to remember, but the password should still be difficult to guess.

To avoid forgetting the password, you may write it down and keep it in a secure place, or store it in an encrypted, password-protected file.

ii). Set an account lockout policy

If RDP access is enabled on the AlertDispatcher system, you should set an *account lockout policy*. This helps reduce the risk of brute-force password guessing attacks.

From *Local Security Policy*, go to:

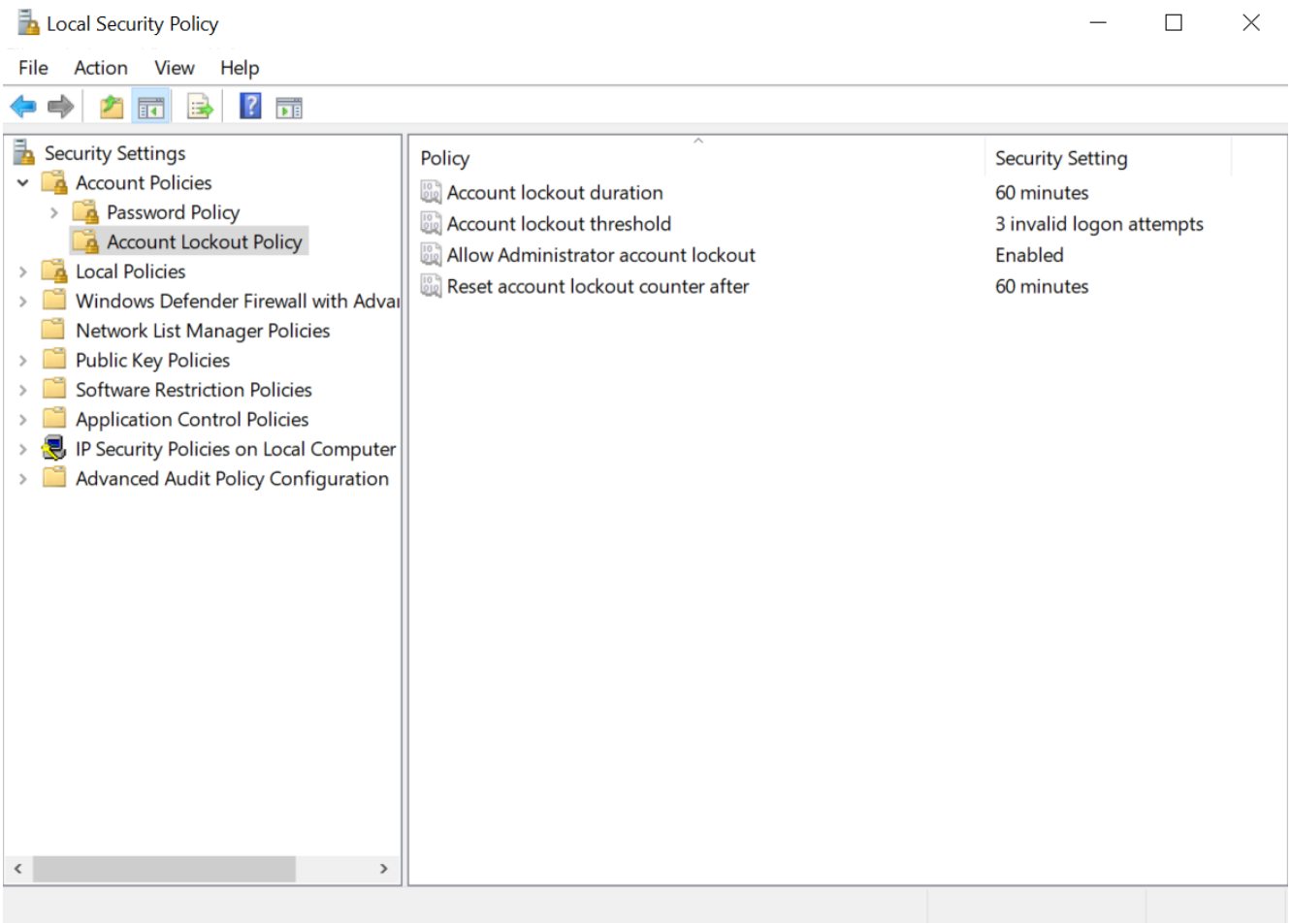
Account Policies → Account Lockout Policy

Recommended settings:

Account lockout duration
This is how long the user account will be locked after several failed login attempts. Set this to at least 15 minutes.

Account lockout threshold
This is the number of failed login attempts allowed before the account is locked. A setting of *3 failed attempts* is usually sufficient.

Allow Administrator account lockout
Enable this setting so that the account lockout policy also applies to local Administrator accounts.



d). Update Windows Regularly

Run Windows Update regularly and install the latest Windows security patches.

Note: If you need to upgrade to a newer Windows version, such as Windows 10 or Windows 11, make sure your AlertDispatcher version is compatible before upgrading.

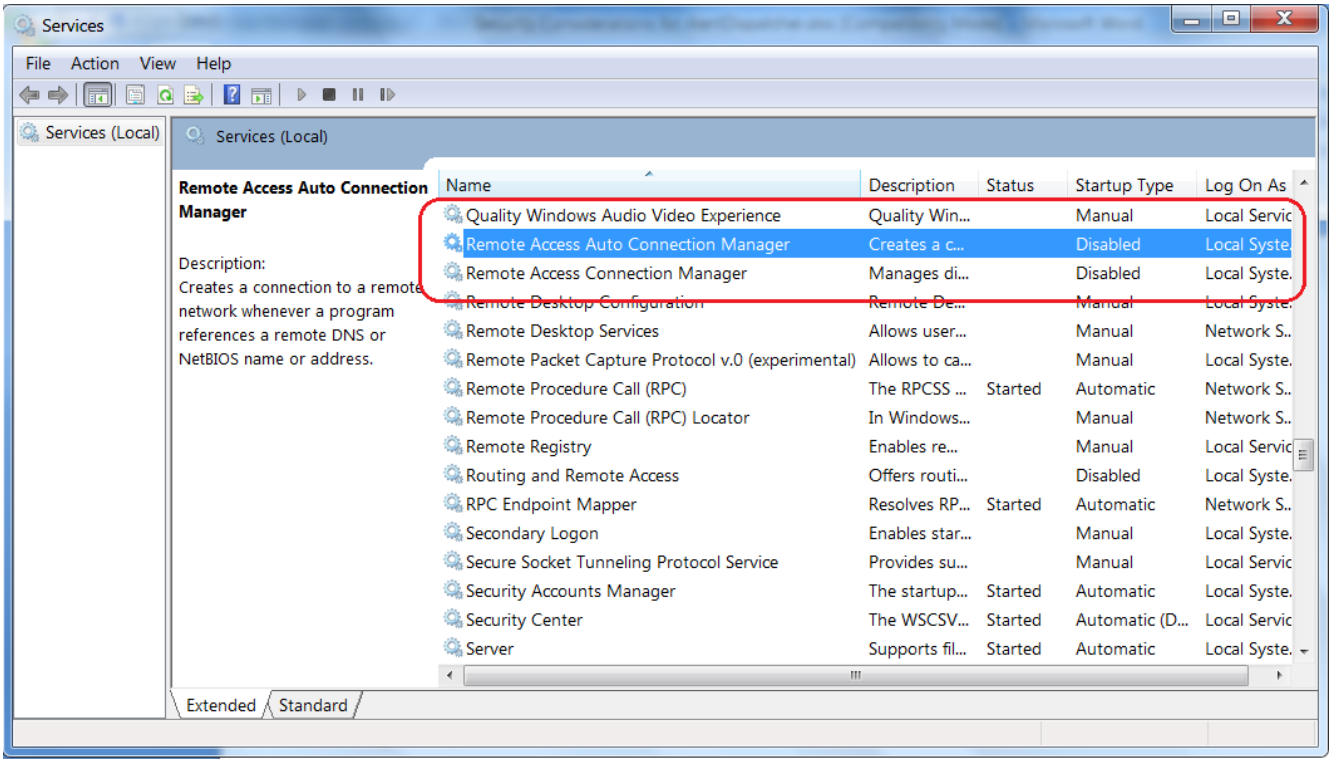
Always test AlertDispatcher after each Windows update or upgrade to confirm that it is still working properly.

e). Disable and Uninstall Unnecessary Windows Services

Disable, and where possible uninstall, the following Windows services if they are not used:

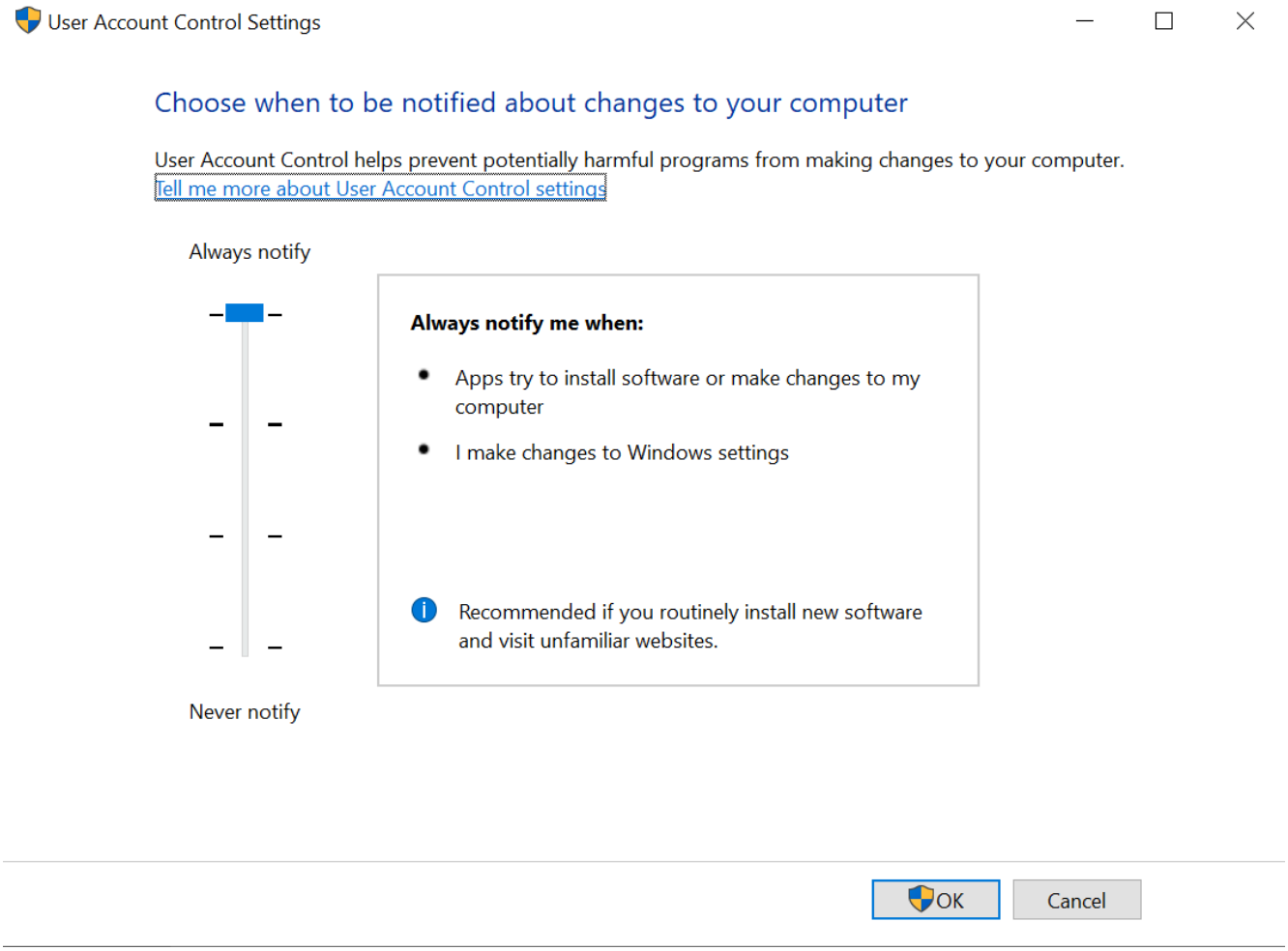
* Fax
* Telephony
* Remote Access Connection Manager
* Remote Access Auto Connection Manager

These services are not required by AlertDispatcher. Disabling unused services helps reduce the system's attack surface.



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

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



3). Securing AlertDispatcher

a). SMS Modem and Network Security

SMS modem and SIM card security is important to the security of the AlertDispatcher system.

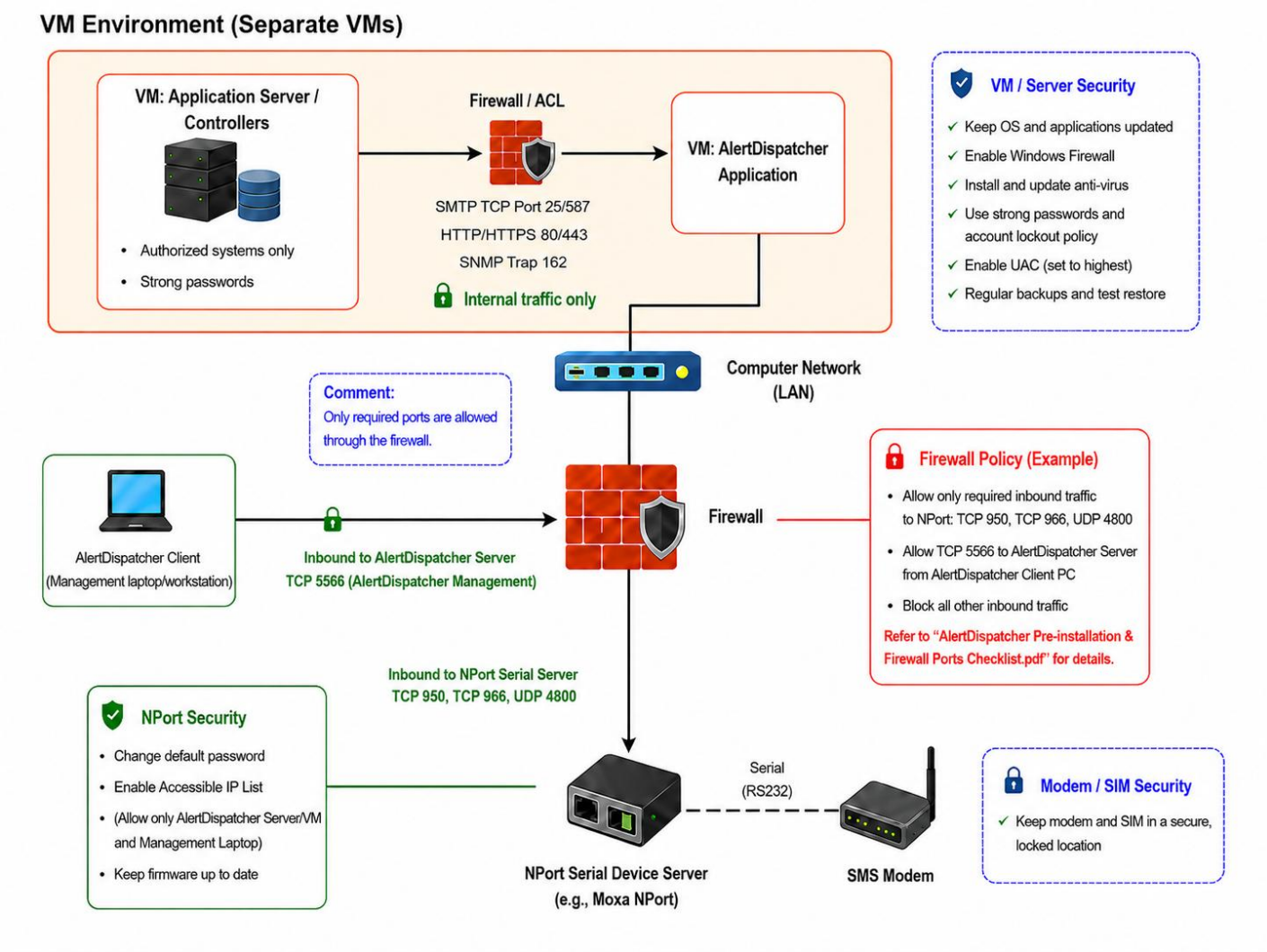
* Keep the AlertDispatcher server, SMS modem, and SIM card in a secure location, such as inside a locked server rack. Where possible, install AlertDispatcher on a server located in the server rack instead of on a workstation in the control room. This helps limit physical access to the server and SMS modem.

* Connect the SMS modem using its RS232 serial port instead of the modem’s USB interface, where possible. This is recommended because RS232 provides a simple serial communication interface and avoids exposing the modem as a USB device to the host operating system.

If the PC or server does not have a built-in RS232 serial port, use a reliable "USB-to-Serial converter" based on an FTDI chipset, such as the FTDI Chipi-X10, to connect the modem's RS232 port to the host. In this setup, the host communicates with the modem through a serial COM port, instead of connecting directly to the modem’s USB interface.

If AlertDispatcher is hosted on a VM, use a reliable "Serial Device Server", such as a Moxa NPort device, to connect the SMS modem's RS232 serial port to the network and map it to the VM as a virtual COM port. Log in to the Serial Device Server management console and change the default password. You may also enable the "Accessible IP List" to restrict access so that only the AlertDispatcher server/VM and your authorised management laptop can connect to the device.

Access to the Serial Device Server should be restricted to the AlertDispatcher host or VM only. This can be done by firewall configuration, allowing only the required inbound TCP ports, such as TCP 950 and TCP 966, to the Moxa NPort device. For details, please refer to "AlertDispatcher Pre-installation & Firewall Ports Checklist.pdf".



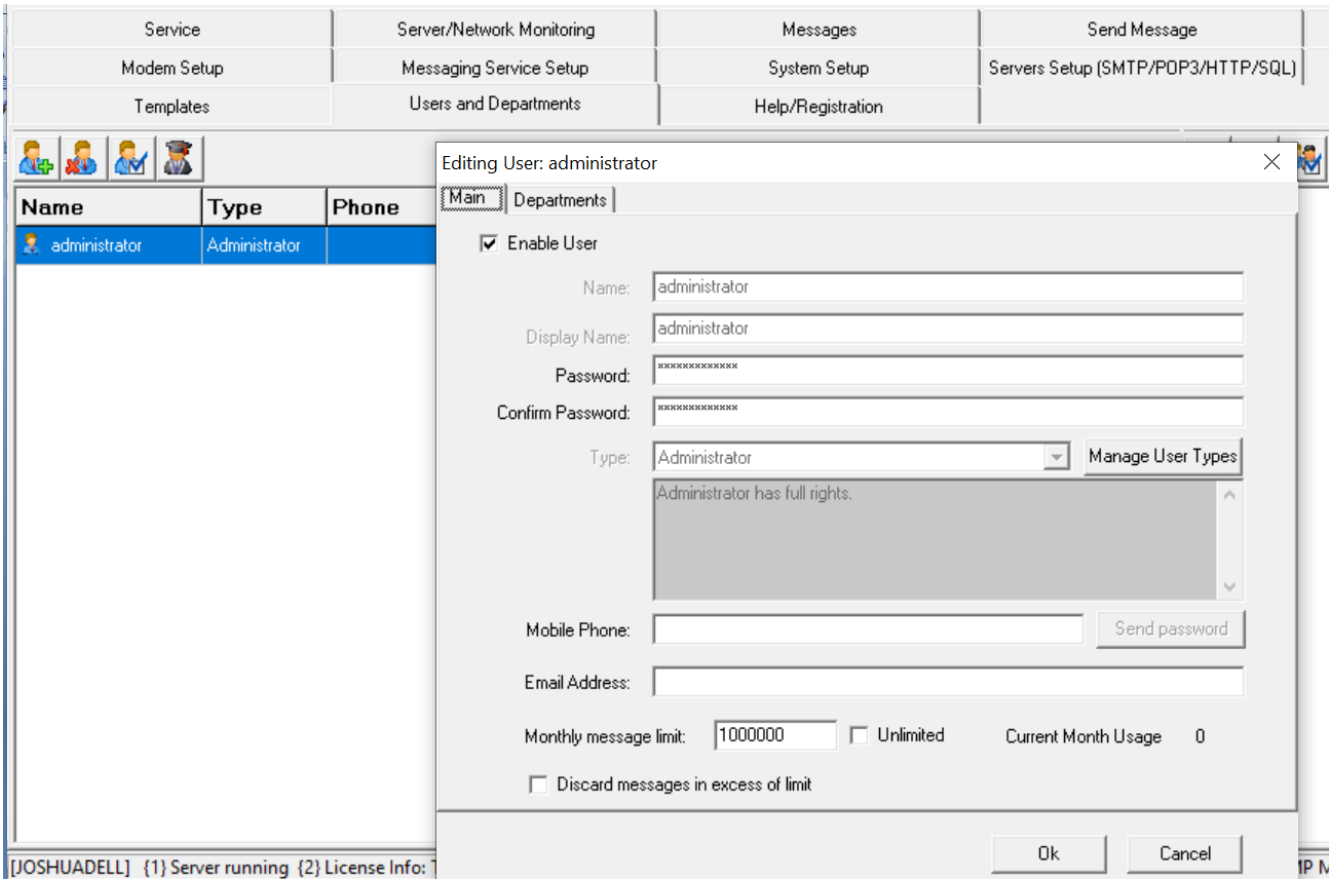
* To prevent unwanted calls to the SMS modem, you can insert the SIM card into a mobile phone and divert all voice calls to another number. This helps prevent people from calling the SMS modem directly.

You may also check with your telco if they can provide a SIM card with voice calls disabled.

Note: AlertDispatcher will automatically terminate incoming calls to the SMS modem. However, the call may still ring for a few seconds before it is terminated.

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

Change the default password for “administrator”.



If you are using AlertDispatcher Corporate Edition or higher, you can create a separate login account for each user and assign only the access rights they need.

Tip: If AlertDispatcher is installed on a server, you can install or copy AlertDispatcher Client to a user workstation and configure it to connect to the AlertDispatcher server. The user can then log in using an AlertDispatcher account with lower access rights.

Each login user is assigned to a User Type, which controls what the user can access. The following user types are pre-created:

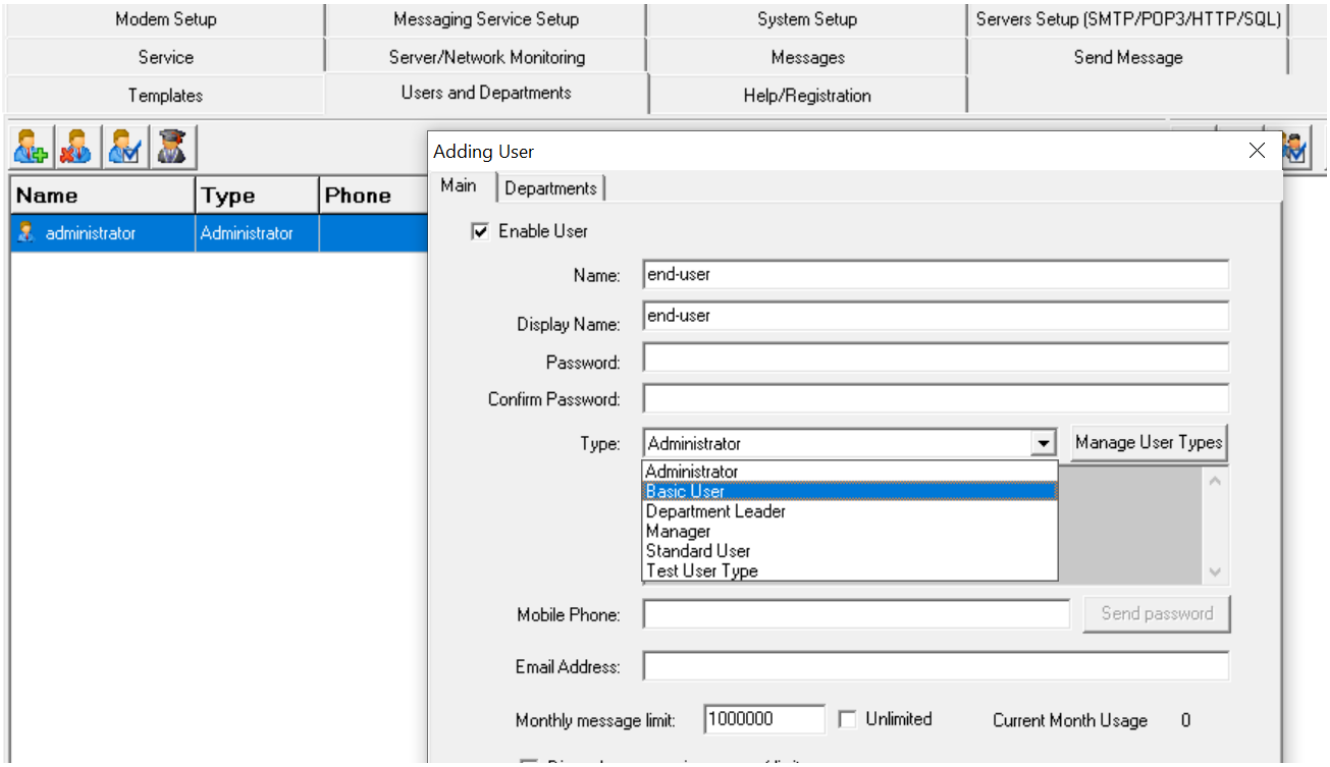
* Administrator
* Basic User
* Department Leader
* Manager
* Standard User

In the example below, the new user "adam.smith" is assigned the Standard User type.

A Standard User can access only the following tabs:

* Service
* Messages
* Send SMS/Email
* Addressbook

A Standard User cannot delete messages and can only view messages from the departments assigned to that user.



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

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

AlertDispatcher's built-in SMTP Server and SNMP Server interfaces are enabled by default in the software configuration. In newer versions of AlertDispatcher, the HTTP Server interface is disabled by default for security.

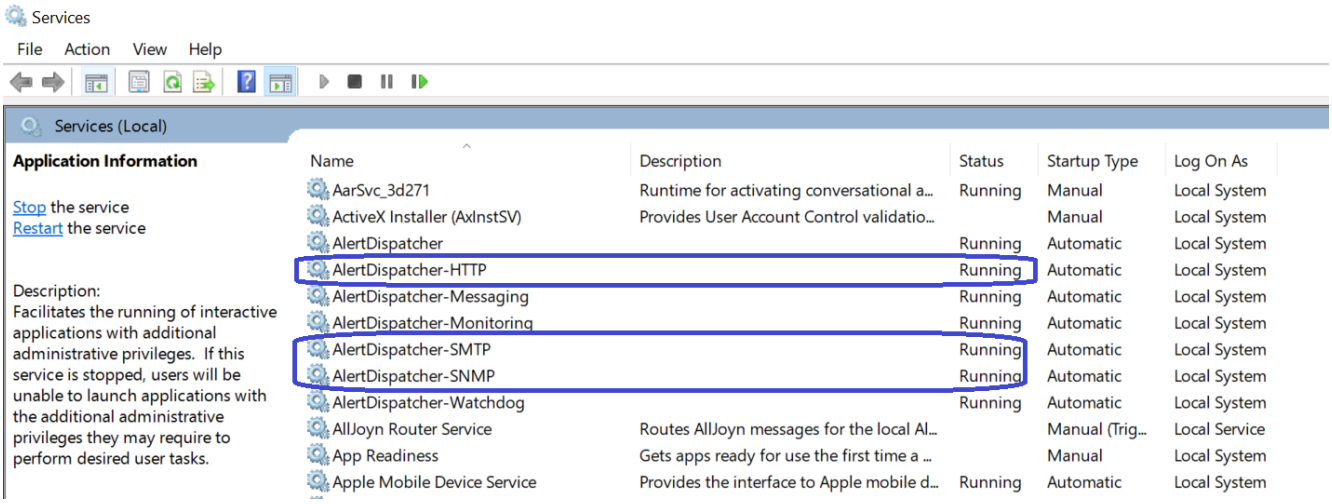
If these interfaces are not required, you should disable them. They can be disabled either from the AlertDispatcher software configuration or by disabling the related Windows services.

To disable the services in Windows, go to:

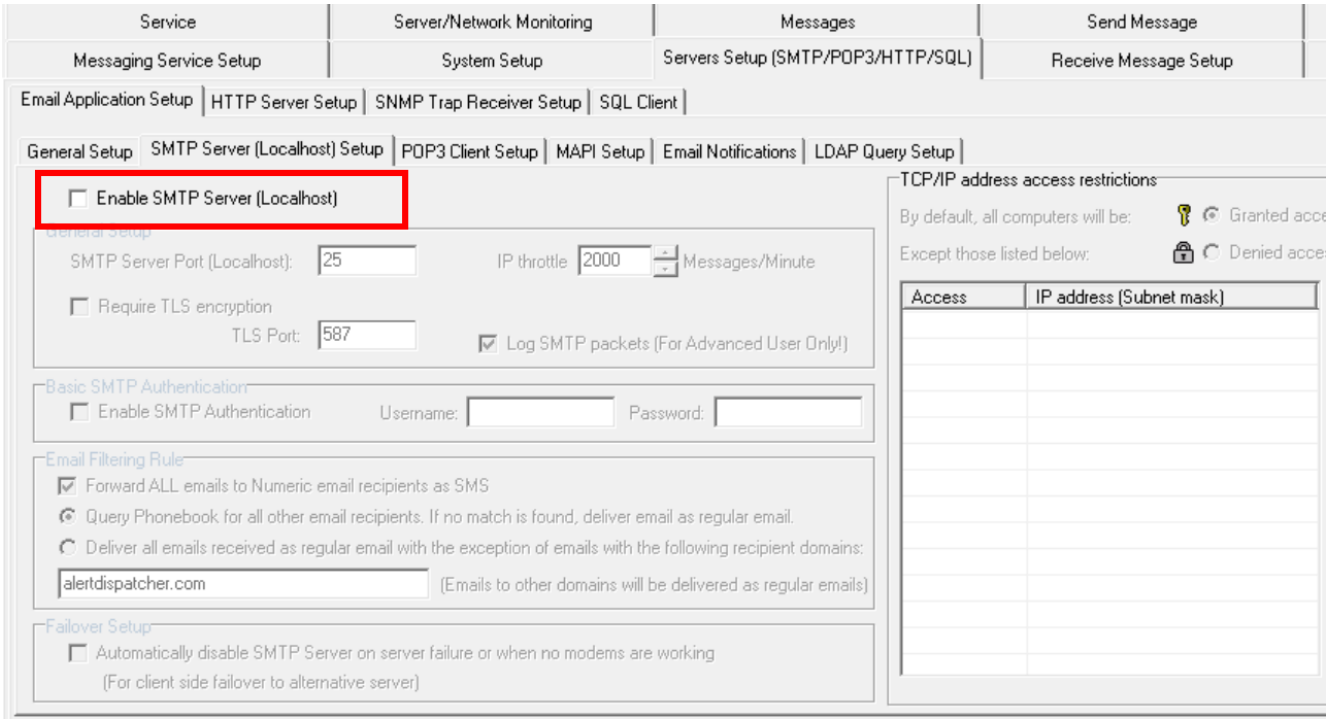
Start → Control Panel → Administrative Tools → Services

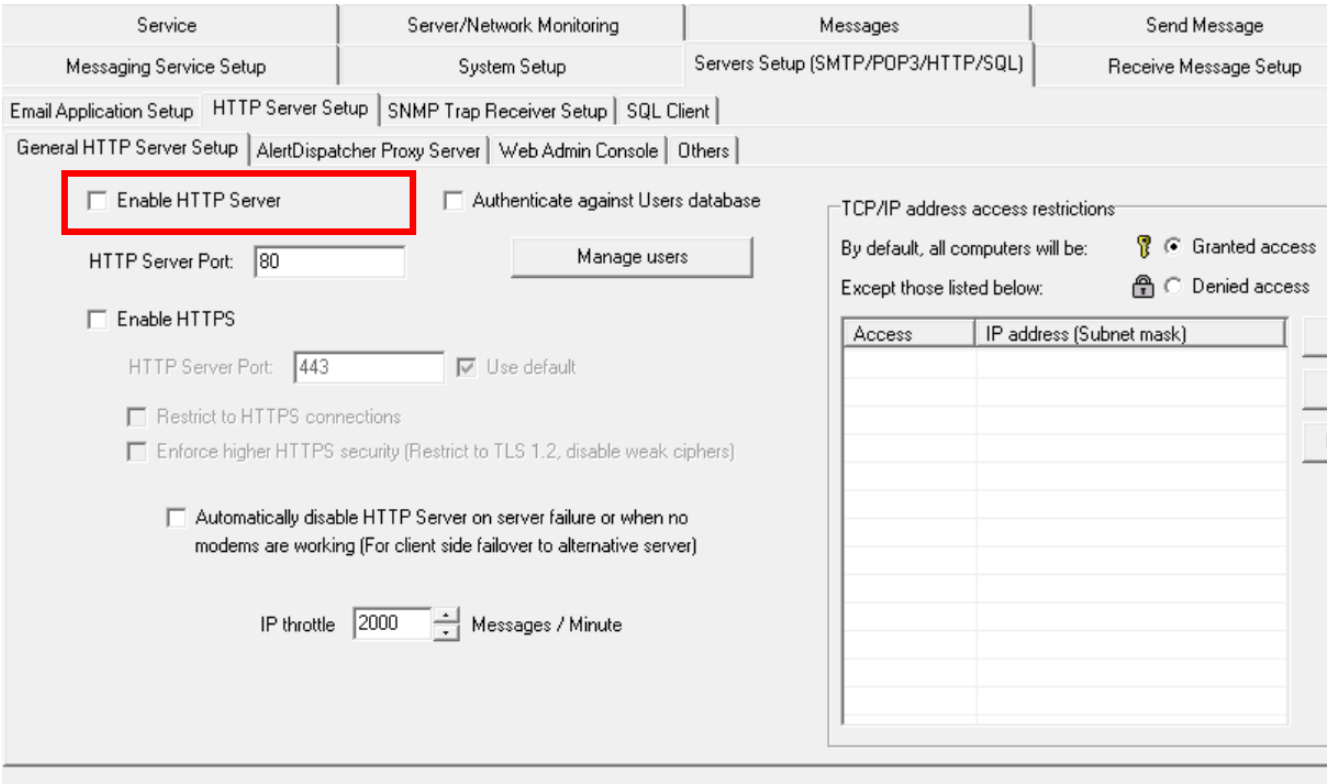
Then make sure the following services are stopped and disabled if they are not used:

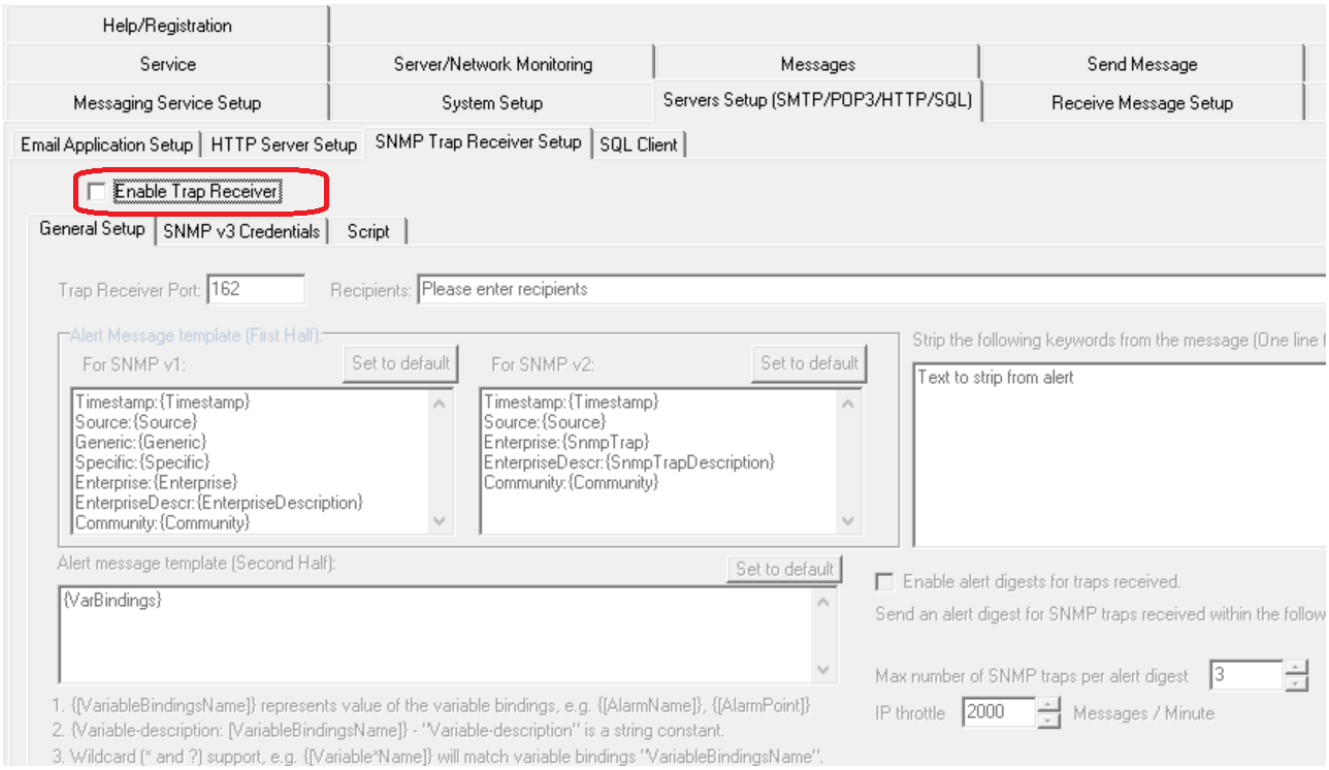
* AlertDispatcher-HTTP
* AlertDispatcher-SMTP
* AlertDispatcher-SNMP



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





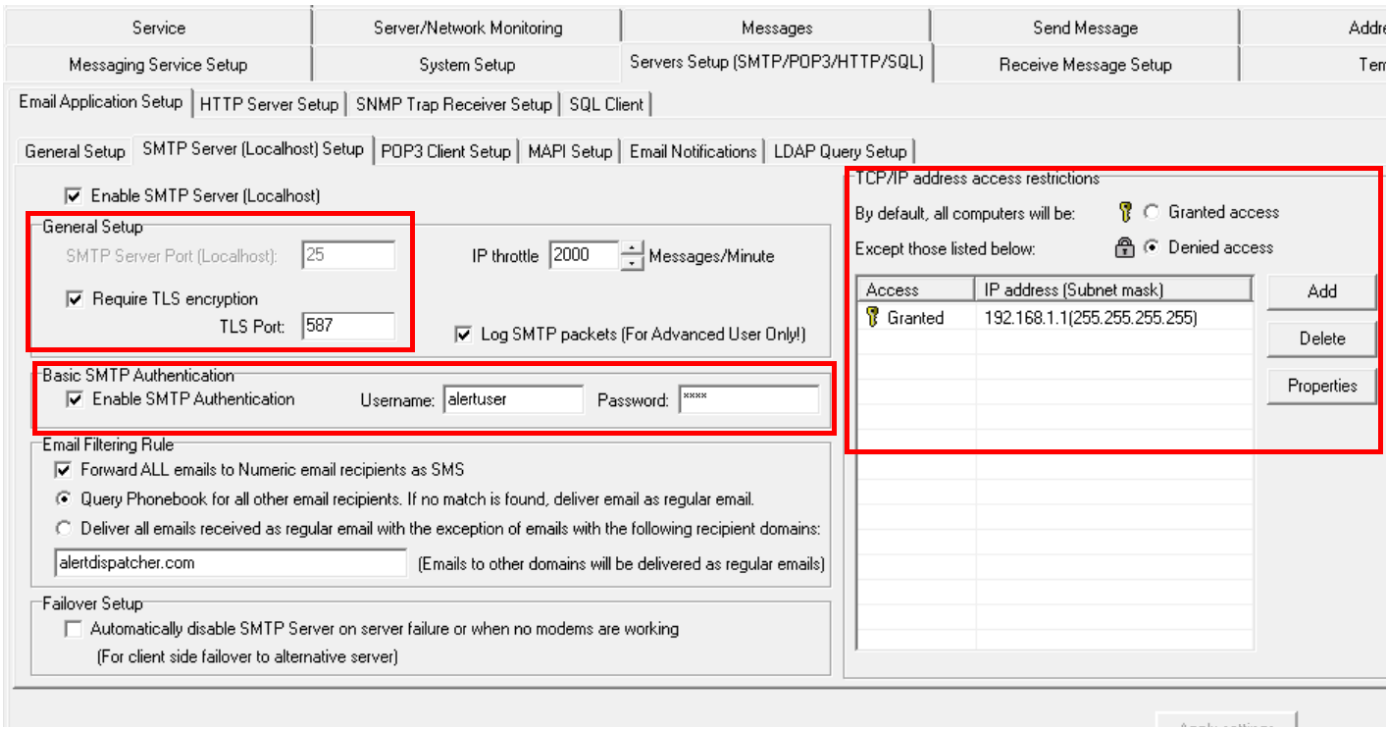

Help/Registration
Service
Server/Network Monitoring
Messages
Send Message
Messaging Service Setup
System Setup
Servers Setup (SMTP/POP3/HTTP/SQL)
Receive Message Setup
Email Application Setup
HTTP Server Setup
SNMP Trap Receiver Setup
SQL Client
Enable Trap Receiver
General Setup
SNMP v3 Credentials
Script
Trap Receiver Port: 162
Recipients: Please enter recipients
Alert Message template (First Half):
For SNMP v1:
Set to default
Timestamp:{Timestamp}
Source:{Source}
Generic:{Generic}
Specific:{Specific}
Enterprise:{Enterprise}
EnterpriseDescr:{EnterpriseDescription}
Community:{Community}
For SNMP v2:
Set to default
Timestamp:{Timestamp}
Source:{Source}
Enterprise:{SnmpTrap}
EnterpriseDescr:{SnmpTrapDescription}
Community:{Community}
Strip the following keywords from the message (One line
Text to strip from alert
Alert message template (Second Half):
Set to default
{VarBindings}
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
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".

ii). Secure the AlertDispatcher network services

The AlertDispatcher SMTP Server interface supports *Basic SMTP Authentication+, which is disabled by default. For better security, SMTP Authentication should be enabled if the SMTP Server interface is used.

SMTP TLS is also disabled by default. It should be enabled if the interfacing application server supports SMTP TLS.

Access to the AlertDispatcher SMTP Server interface can also be restricted to specific IP addresses or IP address ranges.



Warning: The HTTP Server interface is disabled by default in newer versions of AlertDispatcher. Do not enable it unless it is required.

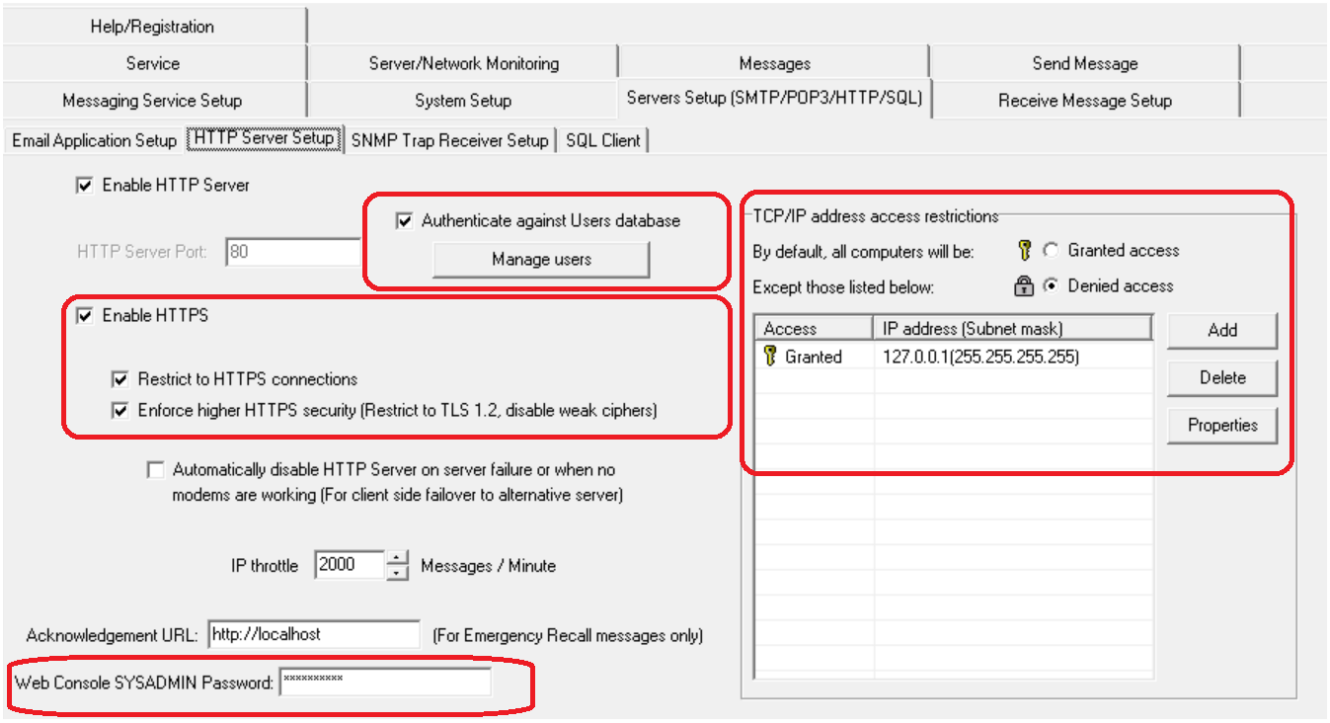
If the HTTP Server interface is used, configure a username and password for access.

If "Authenticate against Users database" is enabled, any request sent to the HTTP Server interface, such as sending a message or checking the server status, must include a valid username and password. These users are configured under the "Users and Departments" tab.

For better security:

* Enable "HTTPS"
* Restrict access to "HTTPS only"
* Enable "Enforce higher HTTP security"
* Restrict access to specific IP addresses or IP address ranges

The Web Console SYSADMIN password should also be changed if the HTTP Server interface is enabled.



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

We do not recommend sending sensitive information through AlertDispatcher, such as:

* Public IP addresses
* User login IDs
* User login passwords
* Other confidential system or security information

For mission-critical operations, please consult your vendor or IT security team for further advice.