



G Data  
TechPaper #0252

**G Data MailSecurity  
on Microsoft<sup>®</sup> Exchange<sup>™</sup> 2007**

G Data Serviceteam

**G Data. Security Made in Germany.**



# Table of Contents

<b>0. Typographic conventions.....</b>	<b>2</b>
<b>1. Introduction.....</b>	<b>2</b>
<b>2. Prior to installing.....</b>	<b>2</b>
<b>3. Installation.....</b>	<b>3</b>
<b>4. Exchange 2007 configuration .....</b>	<b>3</b>
a) Sending email via SMTP .....	3
b) Receiving Emails via SMTP .....	5
c) Receiving Emails via POP3.....	7
d) Querying multiple POP3 servers .....	7
<b>5. G Data MailSecurity configuration .....</b>	<b>8</b>
a) Incoming (SMTP).....	8
b) Outgoing (SMTP) .....	9
c) Incoming (POP3).....	10



## 0. Typographic conventions

To emphasize and clarify some details in this document, the critical passages will be made prominent using color or a different font.

Command line input, folder paths and registry paths will use a monospaced font

*Any window titles, settings or menu sequences will be printed in italic*

In case a passage has to be emphasized to avoid undesired consequences, it will be prefixed with the word "**Caution**", printed in **red** color and **bold**.

## 1. Introduction

This document will cover the installation and configuration of G Data MailSecurity in a Microsoft Exchange environment. It contains all the required settings that require changing to ensure proper email processing. Note that this document is based on a default installation of Microsoft Exchange. Instructions in this document may be subject to changes that might be necessary in your environment.

## 2. Prior to installing

Before installing the G Data MailSecurity Gateway, make sure that:

- The *Data Execution Prevention* (DEP) feature in Windows is set to *only for necessary Windows programs and services*  
In Windows Server 2003/2008 and Windows XP this option is located in the *Advanced System Settings* which are accessible via *Start > Control Panel > System > Advanced > Performance Settings > Data Execution Prevention*
- Any AV software which was used previously is thoroughly removed from the system and the registry. It is recommended to use the cleaning / removal tool provided by the vendor of the previously used AV solution.
- All important Windows updates are applied and available Service Packs are installed (Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP1)
- The contents of all TEMP folders have been deleted
- Port monitoring for POP3, IMAP and SMTP is disabled in any installed G Data Security Client

### 3. Installation

Make sure to only install the latest available version of the software.  
The latest setup file can be requested from our support team.

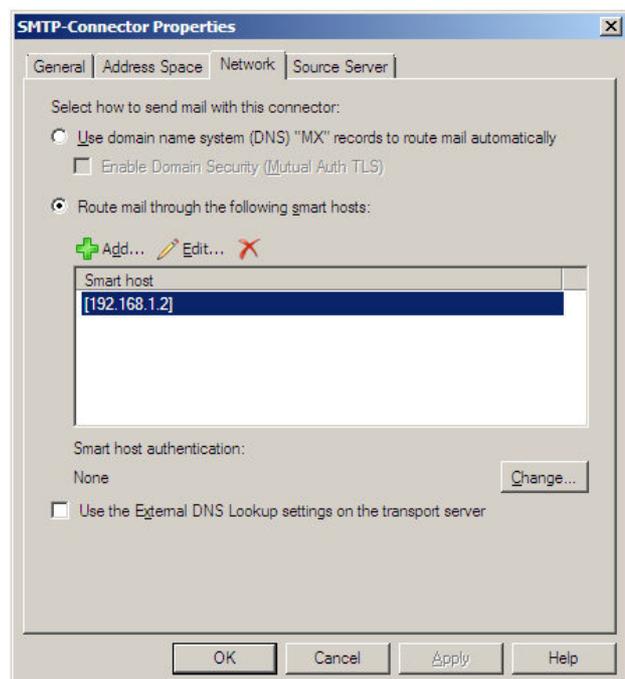
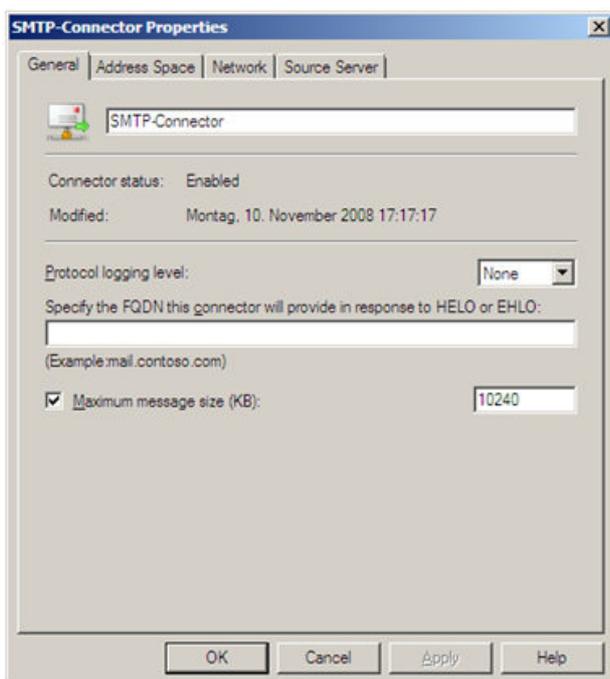
### 4. Exchange 2007 configuration

#### a) Sending email via SMTP

Open your Exchange Management Console and navigate to:

- **Organization configuration**
- **Hub Transport**
- **Send connectors > Properties**

Change the Smarthost address to the local IP address.



**Caution:**

**Never use "localhost" or 127.0.0.1.**

**Always use the server's IP address.**

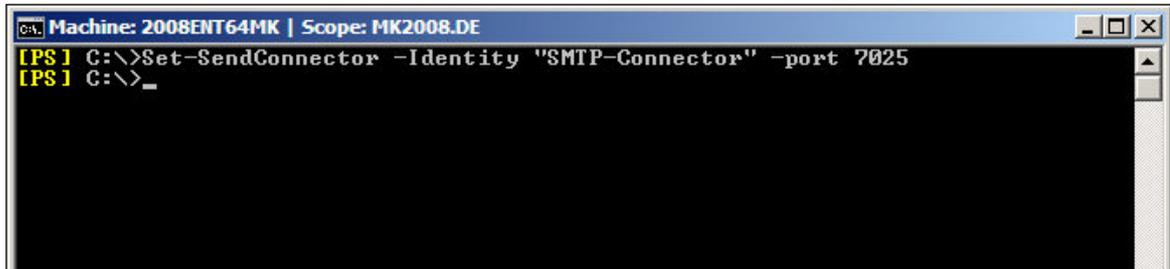
**Using localhost or 127.0.0.1 may result in failures to process emails correctly.**

**Restart all Exchange Services to apply the settings!**

It is also recommended to change the port for outbound STMP traffic to a different port (e.g. 7025 instead of 25). The Exchange Management Shell can be used to achieve this.

Open the Exchange Management Shell and issue the following command:

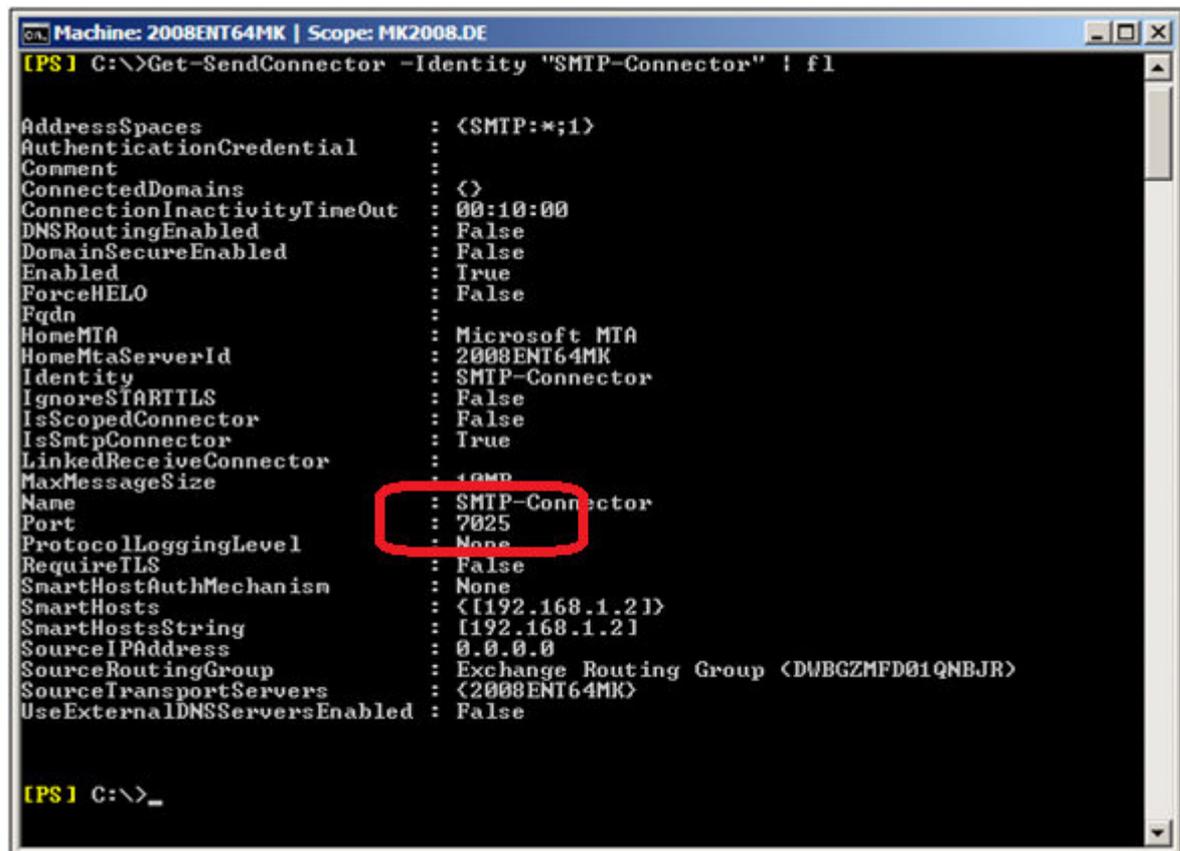
```
Set-SendConnector -Identity "SENDCONNECTORNAME" -port 7025
```



```
Machine: 2008ENT64MK | Scope: MK2008.DE
[PS] C:\>Set-SendConnector -Identity "SMTP-Connector" -port 7025
[PS] C:\>_
```

Verify the changes using the command

```
Set-SendConnector -Identity "SENDCONNECTORNAME" | fl
```



```
Machine: 2008ENT64MK | Scope: MK2008.DE
[PS] C:\>Get-SendConnector -Identity "SMTP-Connector" | fl
AddressSpaces           : <SMTP:*;1>
AuthenticationCredential :
Comment                 :
ConnectedDomains       : <>
ConnectionInactivityTimeout : 00:10:00
DNSRoutingEnabled      : False
DomainSecureEnabled    : False
Enabled                 : True
ForceHELO              : False
Fqdn                   :
HomeMTA                : Microsoft MTA
HomeMtaServerId        : 2008ENT64MK
Identity                : SMTP-Connector
IgnoreSTARTLS          : False
IsScopedConnector      : False
IsSntpConnector        : True
LinkedReceiveConnector :
MaxMessageSize         : 10MB
Name                   : SMTP-Connector
Port                   : 7025
ProtocolLoggingLevel   : None
RequireTLS              : False
SmartHostAuthMechanism : None
SmartHosts             : <[192.168.1.2]>
SmartHostsString       : [192.168.1.2]
SourceIPAddress        : 0.0.0.0
SourceRoutingGroup     : Exchange Routing Group (DWBGZMFD01QNBJR)
SourceTransportServers : <2008ENT64MK>
UseExternalDNSServersEnabled : False

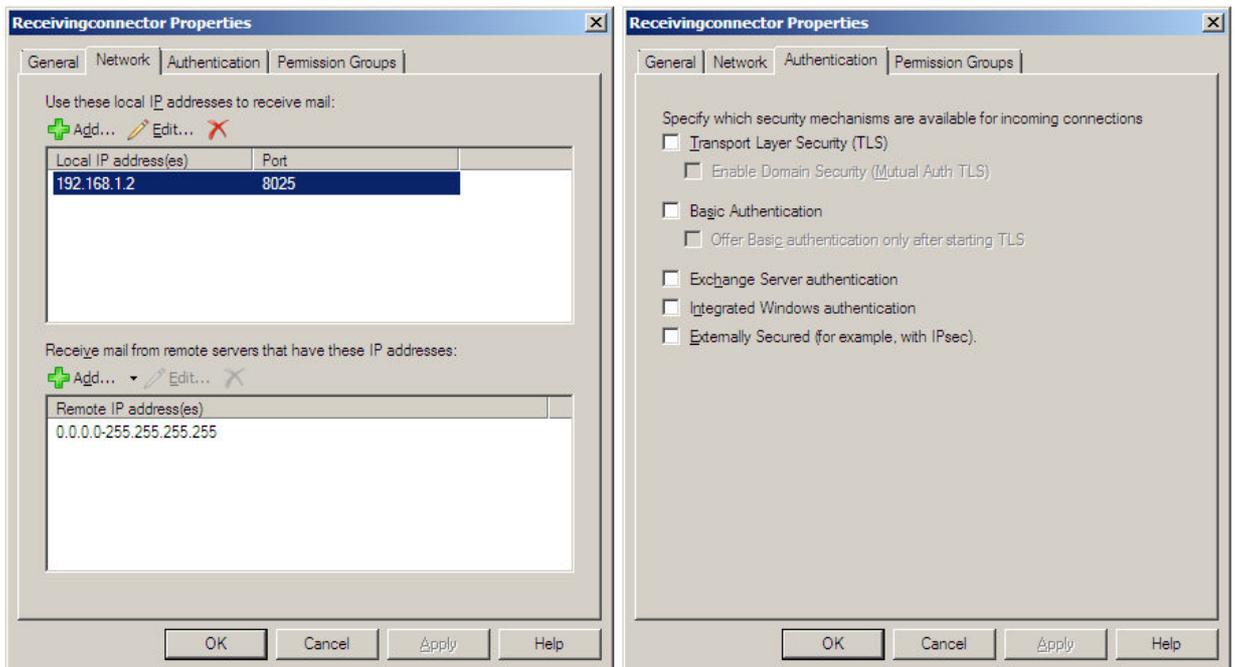
[PS] C:\>_
```

## b) Receiving Emails via SMTP

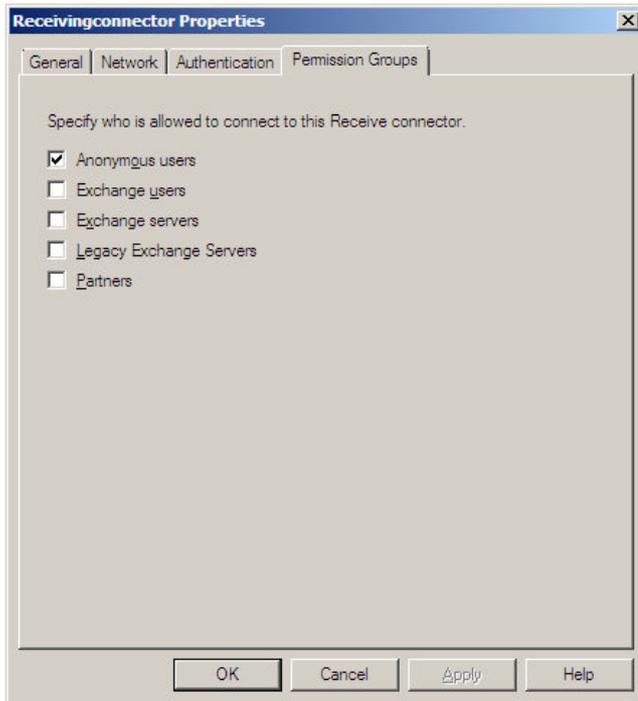
The port for inbound SMTP traffic must be changed from 25 to a different port (e.g. 8025).  
In your Exchange Management Console navigate to:

- **Organization configuration**
- **Hub Transport**
- **Receiving connectors > Properties**

Make sure to apply the port settings and authentication as shown below:



In *Permission Groups*, connections for anonymous users must be set to “Allowed”:



**Caution:**  
**Restart all Exchange Services to apply the settings!**



## c) Receiving Emails via POP3

In order to receive POP3 emails through MailSecurity, a third party POP3 connector must be used.

This is what your user account settings for a POP3 account will most likely look like:

User name:           John.Doe  
Password:           \*\*\*\*\*  
POP3 server:        *pop3.provider.com*  
Port:                110

To get the accounts set up for use with G Data MailSecurity, apply the following changes:

User name:           *John.Doe* (as before)  
Password:           \*\*\*\*\* (as before)  
POP3 server:        192.168.1.2  
Port:                7110

**Caution:**

**Restart all Exchange Services as well as your POP3 connector's service to apply the settings!**

## d) Querying multiple POP3 servers

If multiple POP3 servers are to be queried, no POP3 server must be entered in MailSecurity under "*Incoming (POP3)*". The server name is transmitted via the user name; enter the POP3 server name followed by a colon (":"), then enter the user name.

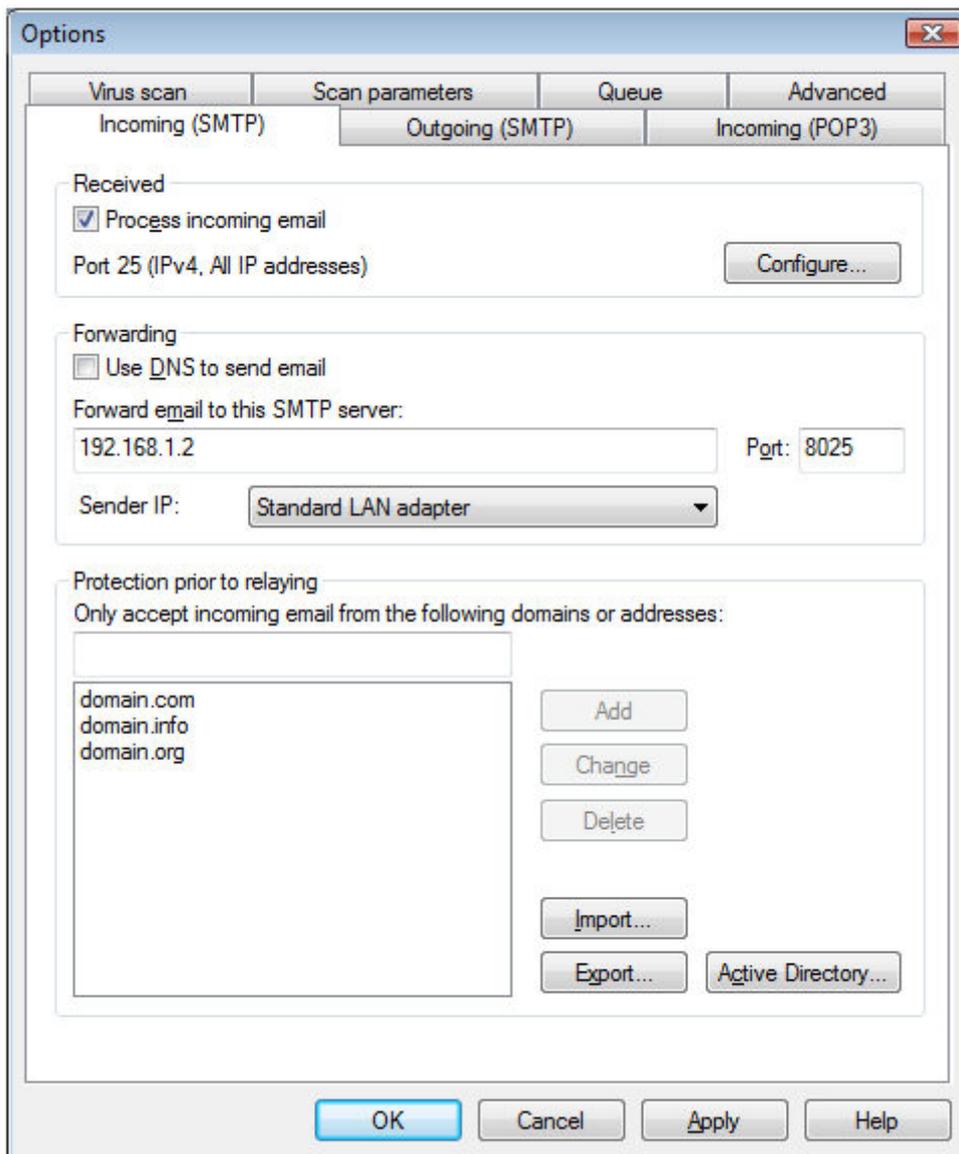
**Example:**

User name:           *pop3.provider.com:John.Doe*  
Password:           \*\*\*\*\* (as before)  
POP3 server:        192.168.1.2  
Port:                7110

## 5. G Data MailSecurity configuration

### a) Incoming (SMTP)

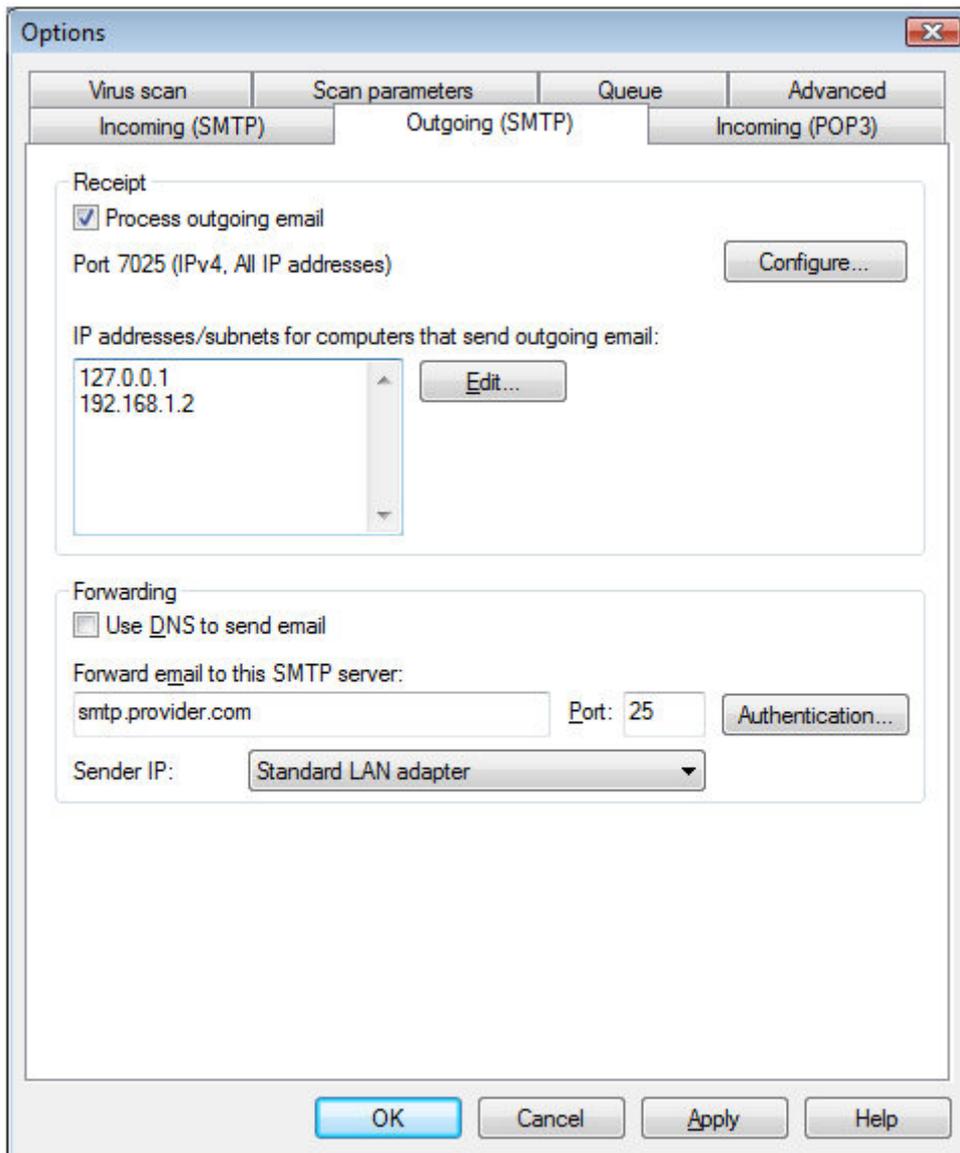
Apply the following settings for SMTP email delivery:



**Caution:**

**Incoming (SMTP) should be disabled if emails are received via POP3 only.**

## b) Outgoing (SMTP)



**Options**

Virus scan | Scan parameters | Queue | Advanced

Incoming (SMTP) | **Outgoing (SMTP)** | Incoming (POP3)

**Receipt**

Process outgoing email

Port 7025 (IPv4, All IP addresses) Configure...

IP addresses/subnets for computers that send outgoing email:

127.0.0.1  
192.168.1.2 Edit...

**Forwarding**

Use DNS to send email

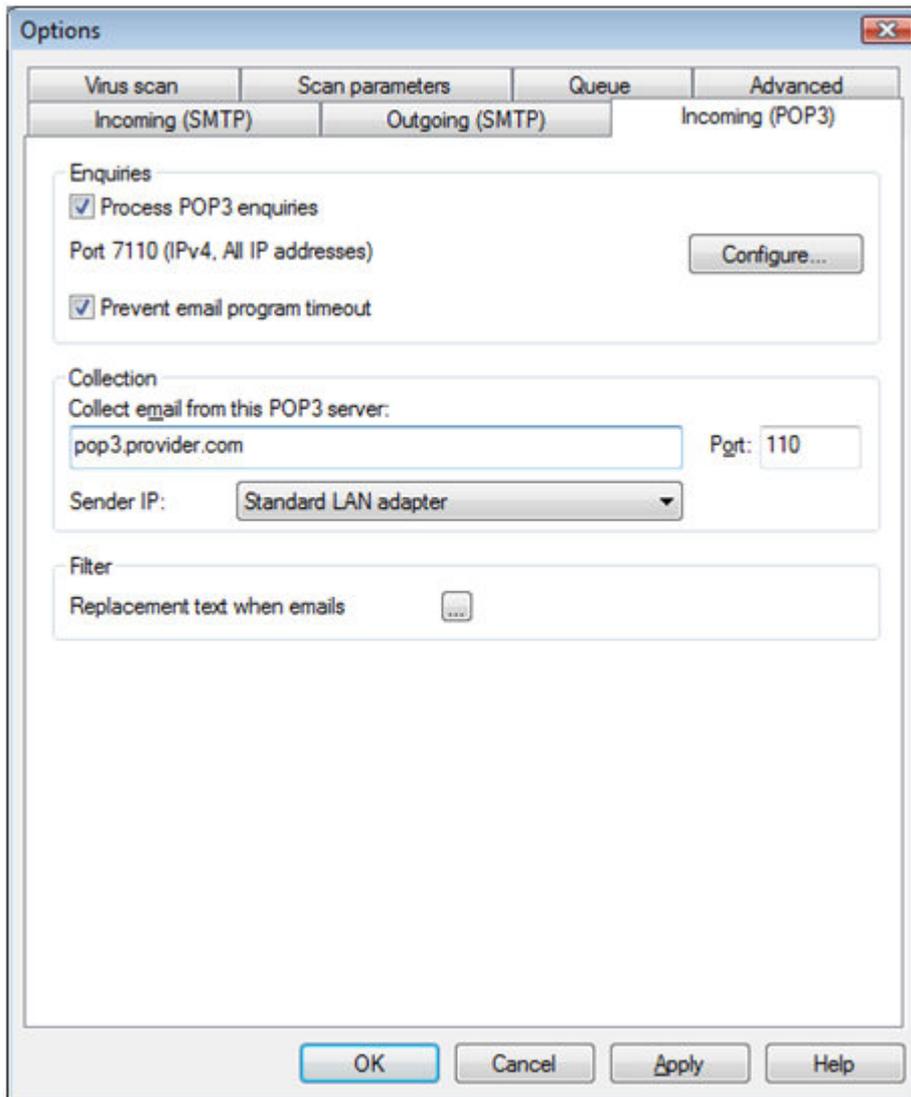
Forward email to this SMTP server:

smtp.provider.com Port: 25 Authentication...

Sender IP: Standard LAN adapter

OK Cancel Apply Help

### c) Incoming (POP3)



The screenshot shows the 'Options' dialog box with the 'Incoming (POP3)' tab selected. The dialog has a title bar with a close button. Below the title bar are four tabs: 'Virus scan', 'Scan parameters', 'Queue', and 'Advanced'. Under 'Advanced', there are three sub-tabs: 'Incoming (SMTP)', 'Outgoing (SMTP)', and 'Incoming (POP3)'. The 'Incoming (POP3)' sub-tab is active.

**Enquires**

- Process POP3 enquiries
- Port 7110 (IPv4, All IP addresses) Configure...
- Prevent email program timeout

**Collection**

Collect email from this POP3 server:

pop3.provider.com Port: 110

Sender IP: Standard LAN adapter

**Filter**

Replacement text when emails ...

At the bottom of the dialog are four buttons: OK, Cancel, Apply, and Help.