

ModusGate Installation Guide

A quick guide
to securing your e-mail flow

www.vircom.com



© 2004 Vircom, Inc. All rights reserved.

Table of contents

1	Overview.....	2
2	To download ModusGate3.....	2
3	Installation.....	2
3.1	License key	2
3.2	Modules to be installed.....	2
3.3	Installation Path.....	2
3.4	Postmaster notices	2
3.5	Configuration	3
4	Recommended settings and actions to take.....	3
4.1	General settings	3
4.2	Connecting ModusGate3 to your mail server	6
4.3	E-mail clients.....	11

ModusGate3 installation guide

A quick guide to securing your e-mail flow

1 Overview

The intent of this document is to minimize the effort required to install your ModusGate3 solution as part of a product trial or for first-time setups. This document is a quick installation guide and as such does not replace all the information available in the user manual or the various “How-to” papers available from our support web site. It will get a new ModusGate3 system up and running in minutes.

2 To download ModusGate3

Go to www.vircom.com and click on the “My Vircom” link. You will be required to enter the license key provided by Vircom. Once the key has been validated, you will be presented with a screen showing all the products associated with this license key, along with the applicable patches and documents. Please make sure to install all the appropriate patches along with the software provided.

3 Installation

Before you start the ModusGate3 installation, make sure the prerequisites are installed (MDAC and .NET). If not install them from the ModusGate3 setup.

The installation of ModusGate3 has been designed for ease of use and requires very little technical knowledge of e-mail systems. Even though a “custom configuration” option is available, we recommend you use the “automatic configuration” option and change the appropriate settings later.

3.1 License key

Enter the license key provided by Vircom. Press the validate button and verify the information displayed in the grayed text boxes. If the information appears to be incorrect, please contact Vircom. If it is correct, proceed to the next screen.

3.2 Modules to be installed

For a trial version, we recommend that the default values be used.

Make sure that:

- “Mail Component” is checked and that “Server and administration console” is selected.
- “Web components” is checked

3.3 Installation Path

If possible, leave the values as is, as it makes supporting the product easier, but if needed change the paths to reflect your IT policies.

3.4 Postmaster notices

Uncheck “Send delivery failure notices to this e-mail address”.

3.5 Configuration

Select “Automatic configuration”. All modifications to the configuration can be done through the ModusGate3 administration console once the installation is finished. The recommended modifications are discussed in the following sections.

4 Recommended settings and actions to take

4.1 General settings

We recommend changing some default settings for first-time users of ModusGate3.

- 1) Go into the Anti-virus screen, click the auto-update tab and press “Update now” to get the latest version of the anti-virus protection.

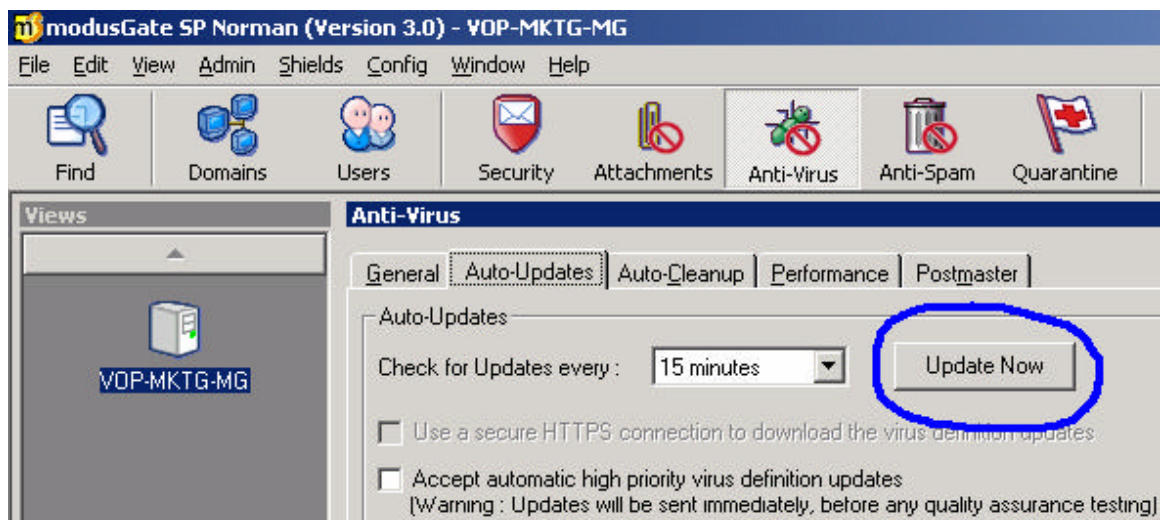


Figure 1 - Anti-Virus updates

- 2) Go into the Anti-Spam screen, click the auto-update tab and choose “6 hours” as the frequency of Anti-Spam auto-updates. This will ensure that the system responds faster to the evolving spam problem. Press “Update now” to get the latest version right away.

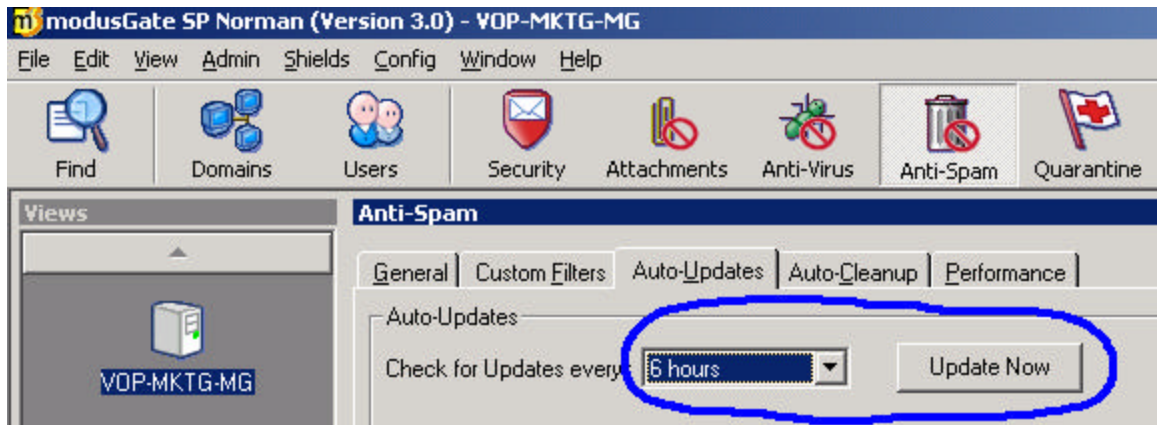


Figure 2 - Anti-Spam updates

3) We don't recommend using Real-time Blacklists (RBLs) as they create their share of problems (high false-positives amongst others) but if RBLs are required, we recommend increasing the cache to the "last 600 entries, for 60 minutes". Some reputable RBLs to use are:

- sbl.spamhaus.net
- bl.spamcop.net
- relays.ordb.org

To set this up, go to the Security screen and click on the "Real-Time Blacklist". Remember to enter your own IP into the "IP Exclusion" list.

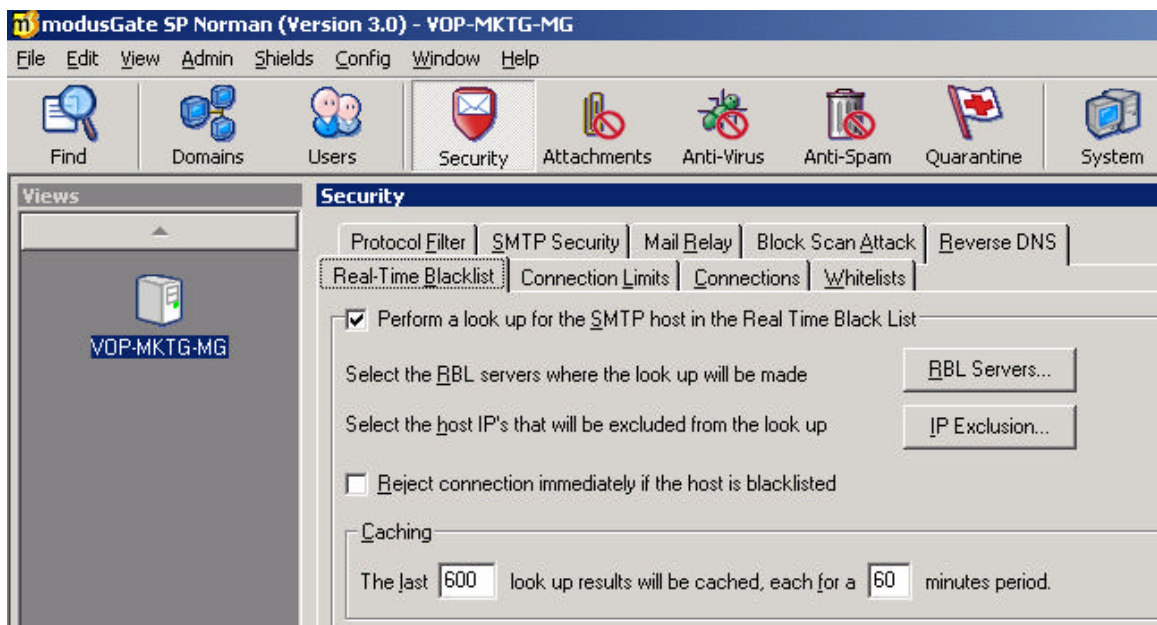


Figure 3 - Real-Time Blacklist

- 4) Go into the Security screen, "Block Scan attacks" and Disable scan attack blocking.

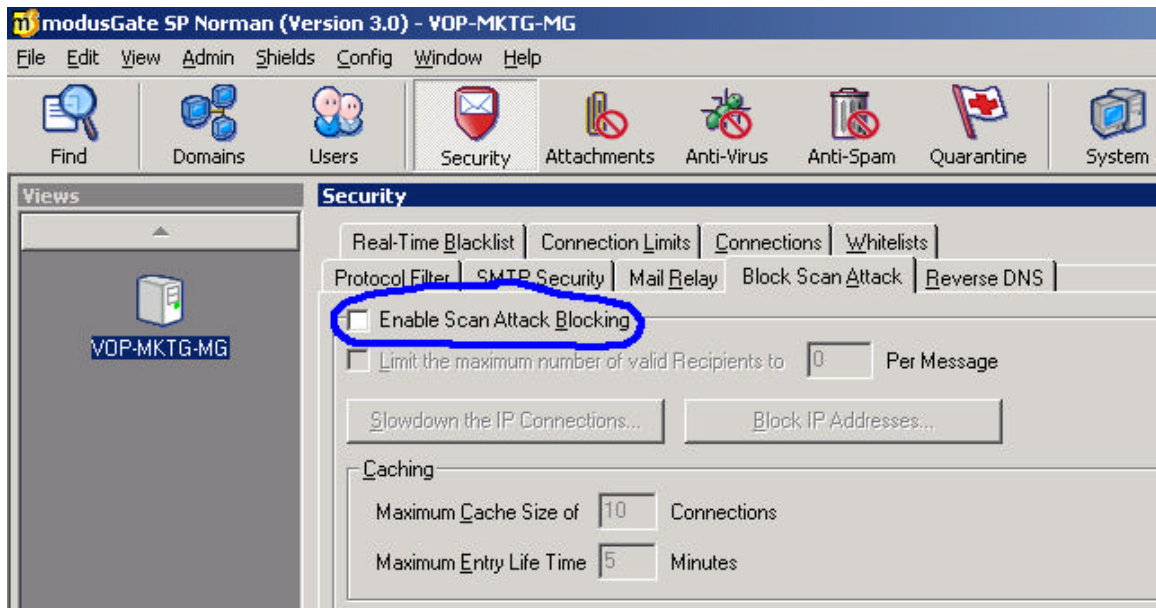


Figure 4 - Scan Attack Blocking

- 5) If there is any security features on the mail server being protected by ModusGate3, make sure the IP of the Gate is considered trusted since the mail server will be sent all legitimate mail from ModusGate.
- 6) Right-click on the "My Computer" icon on the desktop, click on "properties", go into the "Network Identification" tab, click on "Properties" and then "more". Make sure there is a valid entry in the "Primary DNS Suffix" field. If not, the SMTP service will not start properly.
- 7) Make sure all the services are started in ModusGate3's "System" screen (Services).

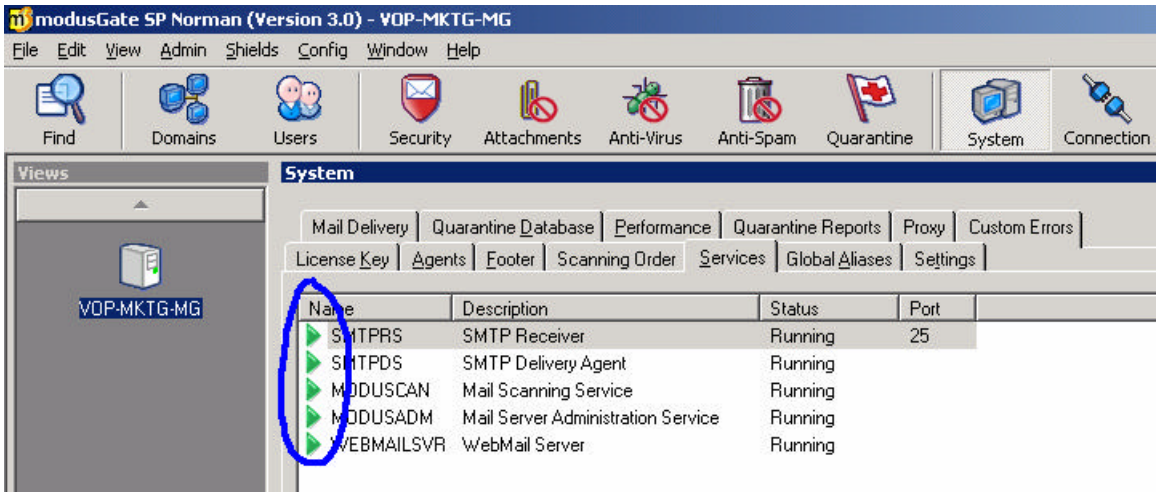


Figure 5 - Services

- 8) If you plan on storing more than 100,000 spam messages in the quarantine, we recommend installing an MS-SQL DB. Please see the *How-To: Use MS-SQL instead of the built in MDB database for Quarantine storage* document available in our support web site.

4.2 Connecting ModusGate3 to your mail server

- 1) Go into the “Connection” screen. Click “Add domain” and add the domain for which you want to take mail. For example, if your e-mail server processes mail for “somecompany.com”, enter “somecompany.com” as the Domain mask. Make sure “Route for incoming mail (Internal Domain)” is selected.

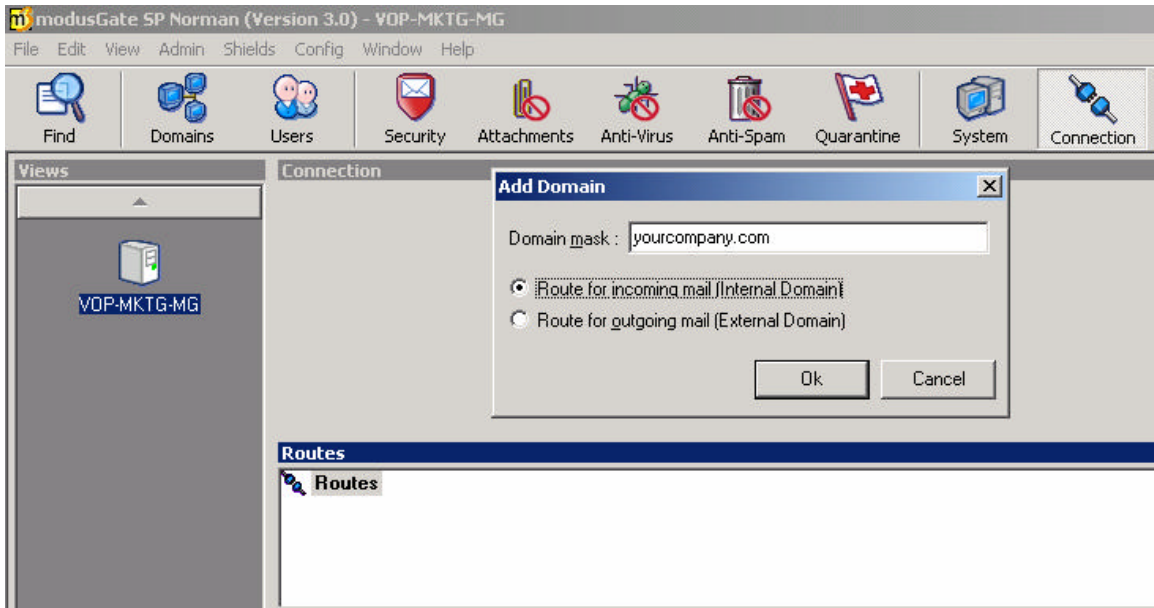


Figure 6 - Adding a Domain

- 2) Click on the newly created domain and click "Add route". Simply add in the IP of the mail server that should be getting the mail for this domain.

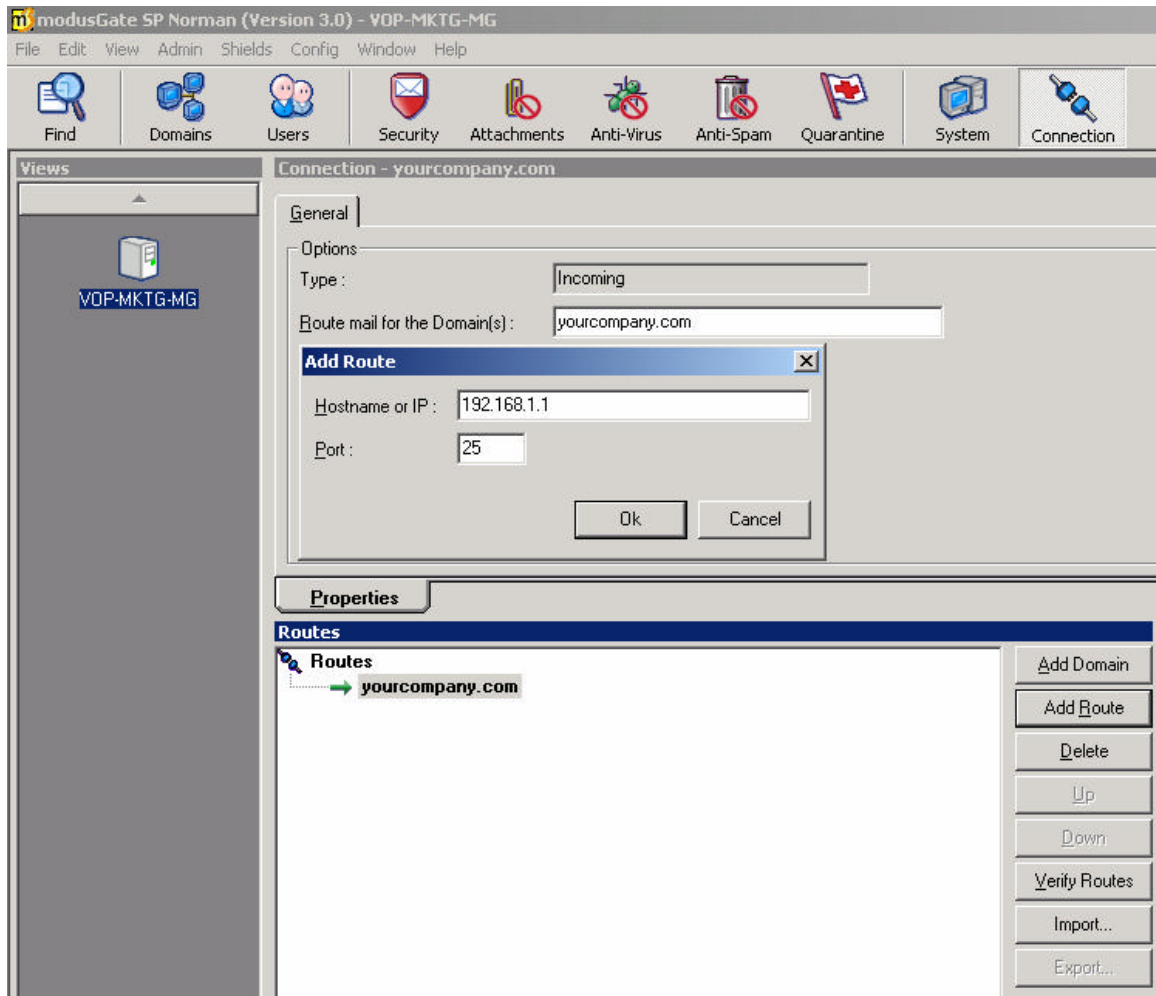


Figure 7 - Adding a Route to the Domain

- 3) To ensure that only valid users are created at the ModusGate level, click on the newly created route, go into the “Pre-Authentication” tab and select the appropriate authentication method. In most cases, it will be SMTP_VRFY. If you are using Exchange 2000, use the Exchange method (LDAP). If you are using Exchange 5.5, you can use either Exchange (LDAP method) or SMTP_VRFY (don't forget to turn on SMTP_VRFY at the Exchange level). For Exchange 5.5, we recommend SMTP_VRFY as it is easier to setup.

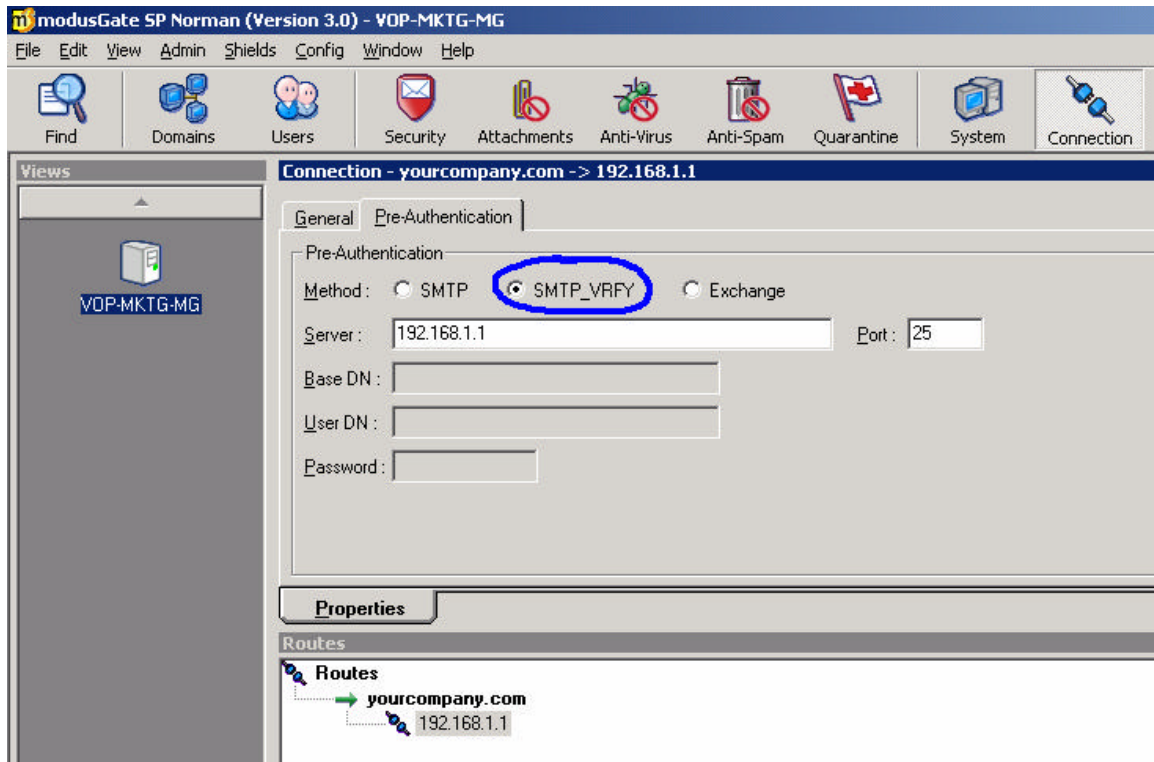


Figure 8 - Setting up authentication method

- 4) Finally, because you are most likely trying ModusGate3 for the first time if you are reading this, Vircom recommends that you only TAG spam for a few hours/days until you feel comfortable with deleting spam or putting it in quarantine. Do not underestimate the confusion of end-users use to getting spam every few minutes! Go into the Anti-Spam screen, click on the "Preferences" tab (bottom tabs) and choose "TAG and let message pass through". Make sure you enter an easily recognizable string in the text box (i.e.: SPAM).

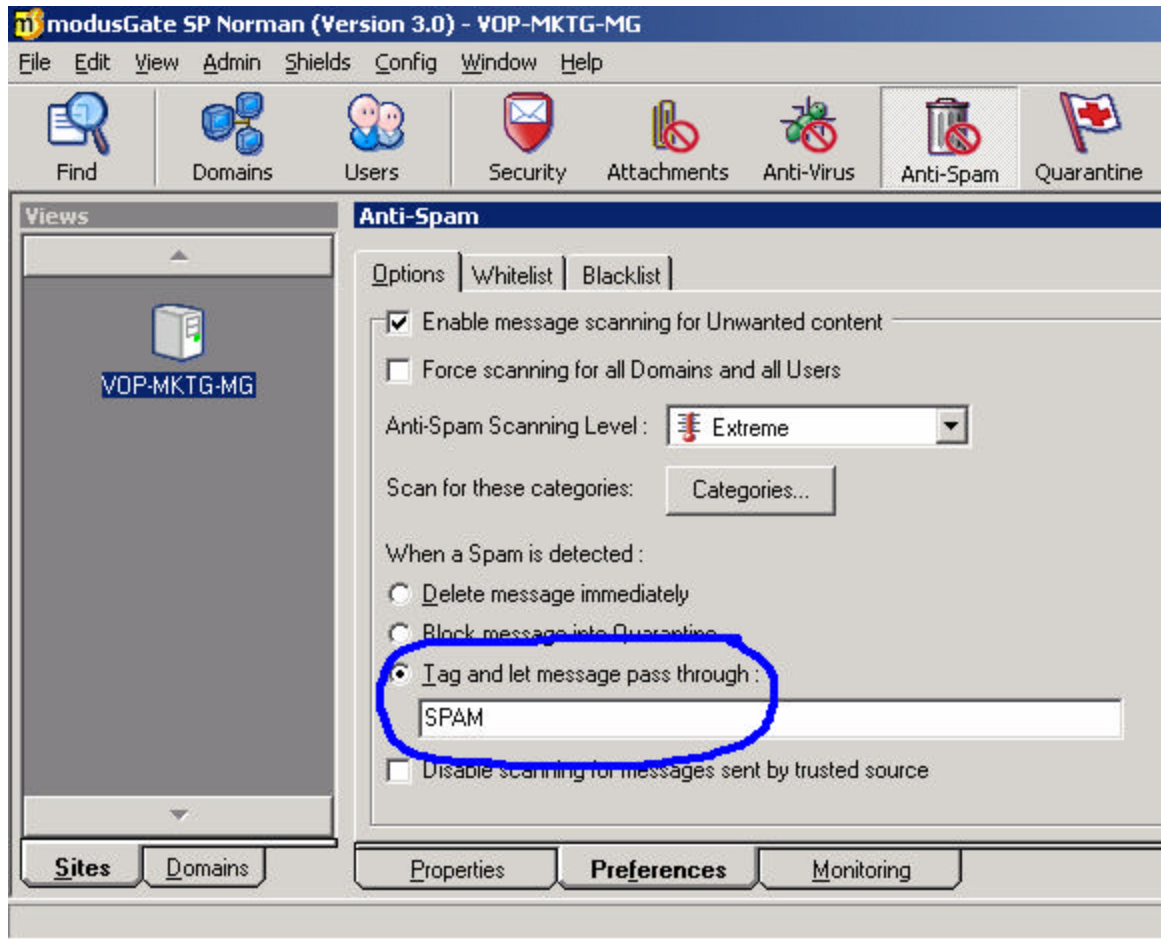


Figure 9 - Tagging Spam

- 5) In the same screen, make sure you uncheck "Disable scanning for trusted sources". Leaving this option checked makes it difficult to test the catch rate as everything sent from your local users will be trusted and not scanned for spam.

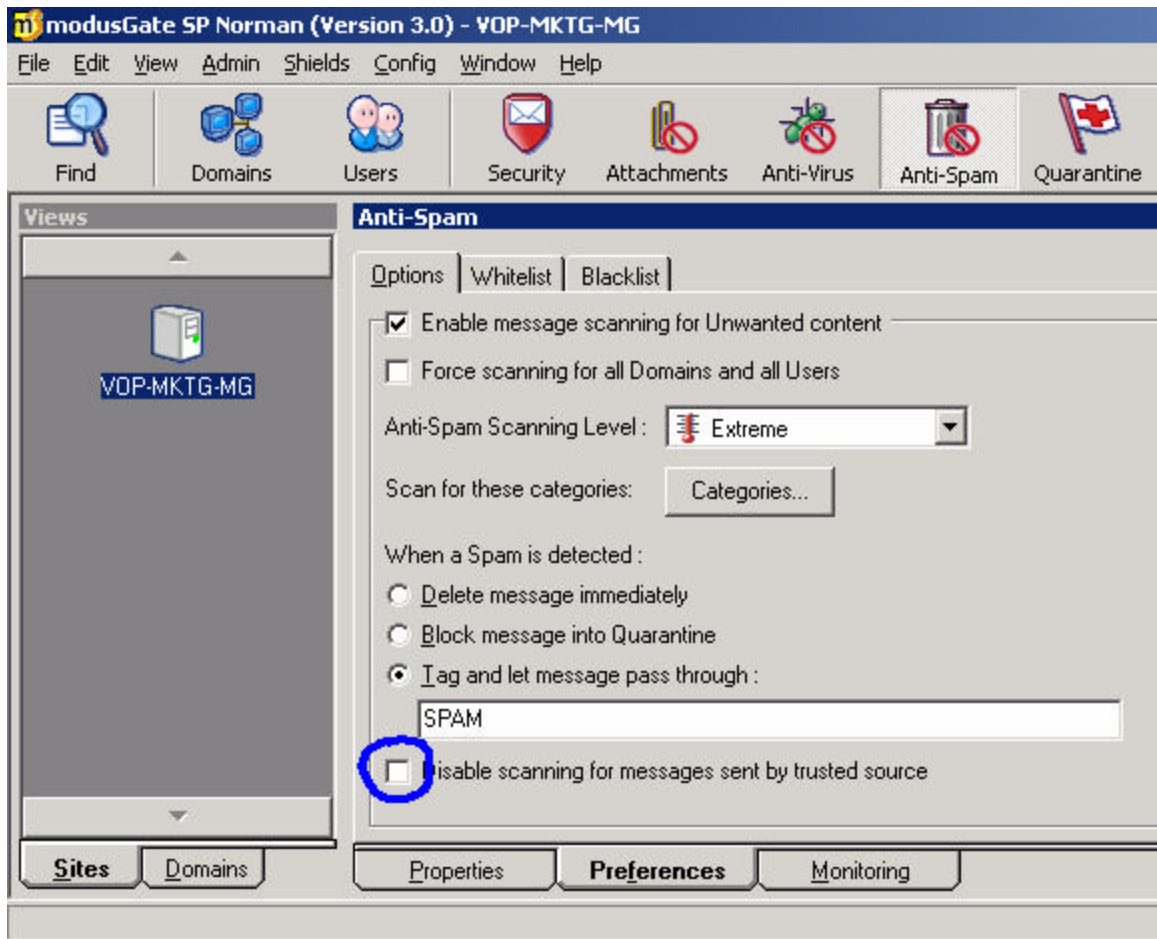


Figure 10 - Trusted Sources scanning

4.3 E-mail clients

You will have to configure the e-mail clients to use *SMTP Auth* to send out mail. Their login **has** to be the fully qualified domain name ([username@somedomain.com](#)). The following page displays an example of Outlook Express' E-mail account screen.

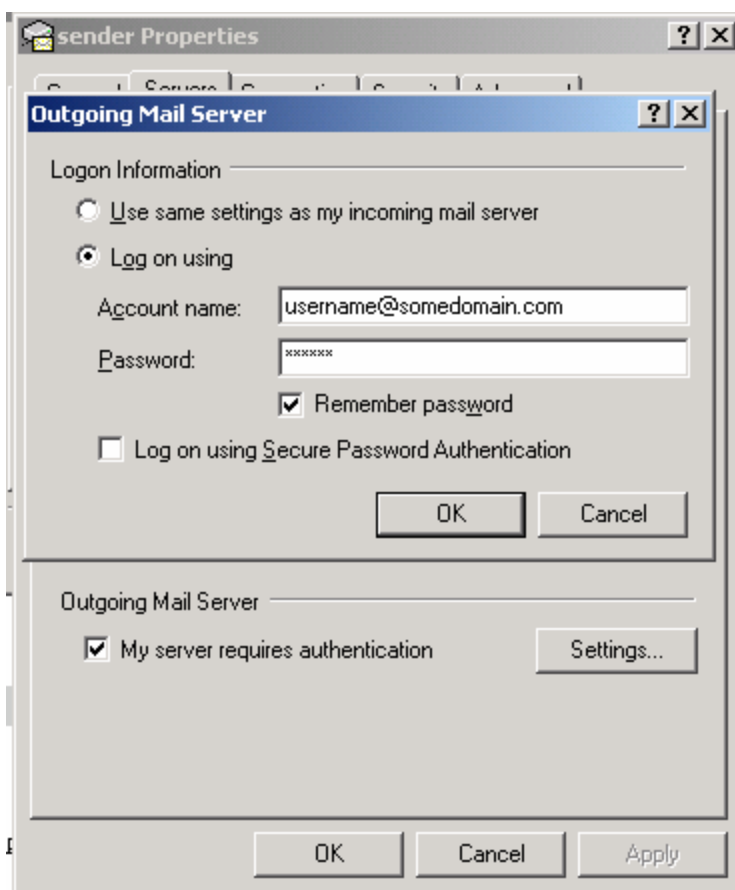


Figure 11 - Outlook Express SMTP Auth configuration