GRAYWALL

Graylist Mercury/32 daemon

Version 1.0.0

Introduction

Graywall is a program that adds a graylist (or greylist) feature to the Mercury/32 SMTP server. It uses the Mercury/32 API facility that has been introduced in version 4.51. You must have at least this version of Mercury/32 to run Graywall!

Information about graylisting in general can be found at: http://en.wikipedia.org/wiki/Greylist. We recommend that you read this first.

Note that graylisting techniques can only be used when e-mail is delivered by SMTP; hence Graywall can only be used in conjunction with Mercury's SMTP server, MercuryS. (However, Graywall's companion product, Spamhalter, can be used for both SMTP and POP3 e-mail delivery, so, with a Mercury system which collects e-mail using SMTP, best spam protection will be achieved by using both products.)

The basic features of Graywall are as follows.

- It accepts some incoming SMTP sessions and rejects others according to certain conditions.
- Authorized connections, or connections from specified IP addresses, are not affected by Graywall.
- Graywall is compatible with the sending of SMTP mail by server farms.
- Graywall is compatible with the "reverse delivery test" used by some systems as an anti-spam test (for example, Sourceforge.net).
- Servers which successfully pass mail through are whitelisted by Graywall for the specific mail domain, and subsequent messages are not delayed by Graywall.

What defeats Graywall?

- Backup mail servers. If an e-mail sent directly to your Mercury system is initially rejected by Graywall and is consequently re-sent by one of your ISP's backup servers/relays, then all these backup servers must also be protected by graylisting.
- Forwarding e-mail accounts. If your incoming external e-mail is forwarded on to you by another server (rather than being sent to you directly as a result of MX records for your domain), the forwarding server will always try to re-send any message including spam. The retrying of forwarded mail will defeat Graywall.

Installing Graywall

Installing Graywall is simple. In fact, installing (or upgrading to) Mercury 4.51 will optionally install Graywall for you. Otherwise you should proceed as follows (Stage 4 is also needed if Mercury has installed Graywall for you).

1) Stop your Mercury/32 system.
2) Run the Graywall installer.
3) Start Mercury/32.
4) Use Configuration | Graywall to configure the system.

Uninstalling Graywall

You can uninstall Graywall using Control Panel | Add/Remove Programs in the same way that you uninstall any other application.

Graylisting in depth

Please read http://en.wikipedia.org/wiki/Greylist before studying this section.

If an incoming SMTP connection does not come from a defined IP address known to Graywall, or if the sender is not in the Graywall whitelist, or the sender's domain is unknown, then Graywall inspects a triplet consisting of the sender's reduced IP address, the sender's e-mail address and the receiver's e-mail address. From this information is computed a hash code.

Graywall then searches its internal database for this hash code. Messages are allowed through if the previous delivery attempt occurred within the time interval defined in Graywall's configuration menus. Graywall then opens up delivery for this group of servers and for the sender's mail domain. Subsequent delivery attempts from this server or a similar one with the same sender's mail domain are allowed.

If the previous delivery attempt is not found in Graywall's database, or this delivery attempt is not with a defined timescale, then the SMTP session is refused, and a temporary server error is sent back in an e-mail to the originator. Because this is not hard error, all correctly written mail servers should try to deliver the message again later. However most of spam tools or viruses will not try to deliver it again. This is the basis of graylisting.

Information about allowed servers and mail domains expires after a defined period of inactivity.

Statistics

Graywall stores usage statistics in a file called graystat.txt file within the Graywall data directory.

The statistics file contains the following information.

From – Statistics are counted from this point.

All – count of all detected SMTP sessions.

Whitelisted – This number of SMTP sessions have been opened by previous successful graylisting.

WhitePercent – The 'Whitelisted' count as a percentage of the 'All' count.

New – A count of new (ie not seen before) delivery attempts.

OK – A count of SMTP sessions that have been allowed by Graywall because they have retried delivery within the specified time limits.

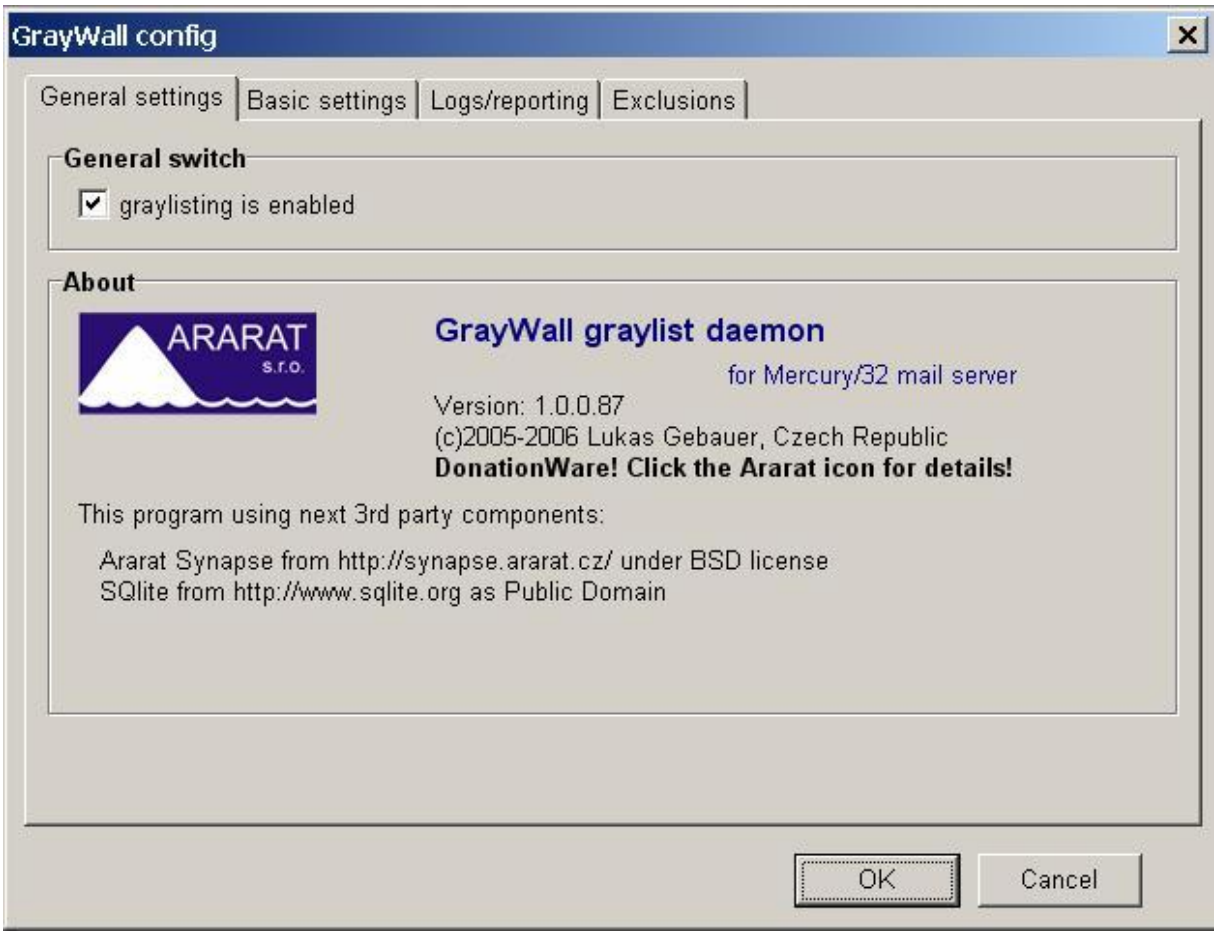
OKPercent – The ‘OK’ count as a percentage of the ‘New’ count. Here you can see the efficiency of graylisting!

Here is an example of a graystat.txt statistics file

[stat]
from=29.6.2007 15:04:34
all=167485
ok=8809
new=90996
whitelisted=44503
whitepercent=26,57%
okpercent=9,68%

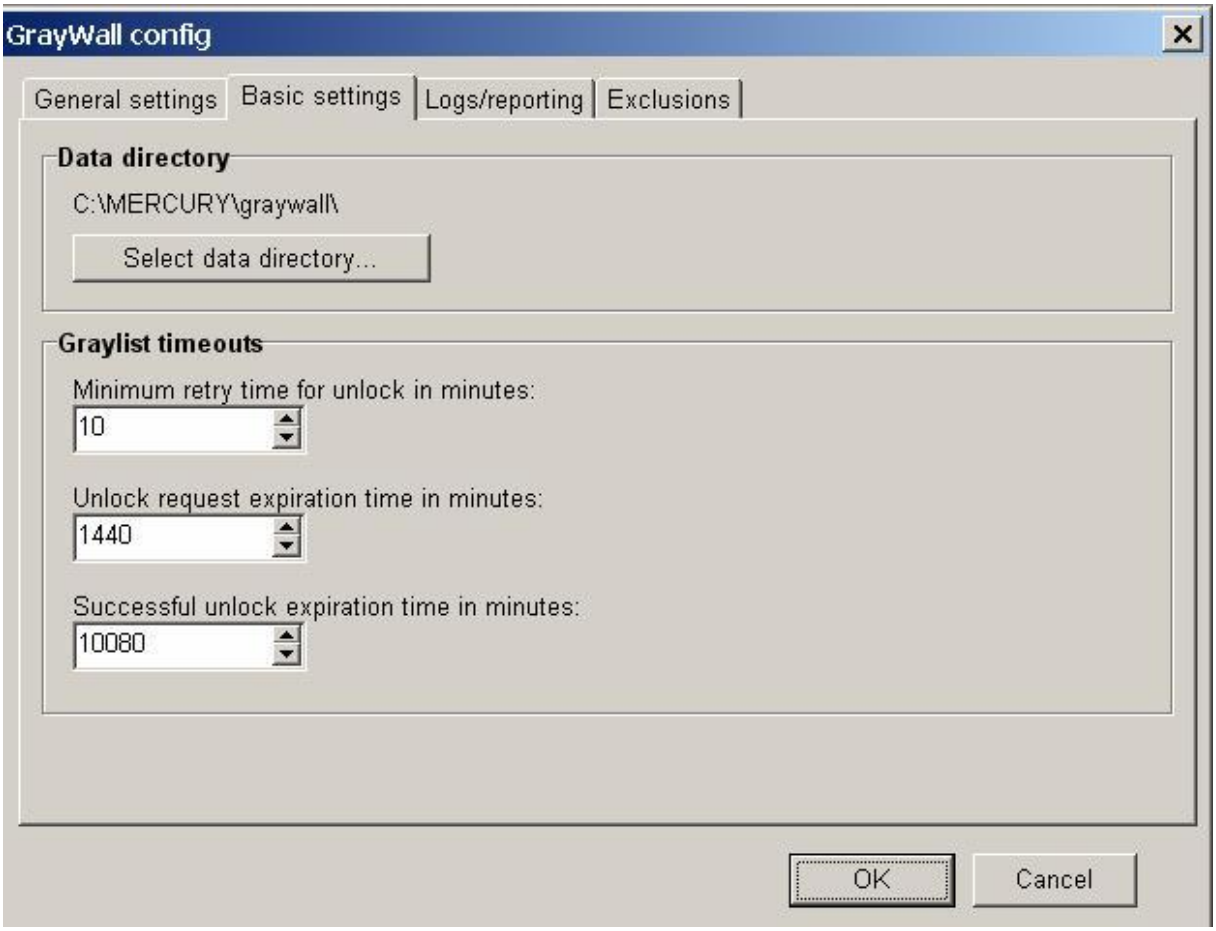
Graywall Configuration screens:

*The **[section] item** are the items in the graywall.ini file.*



General Switch

Enables the Graywall daemon ***[Graywall] Enabled***



Data directory

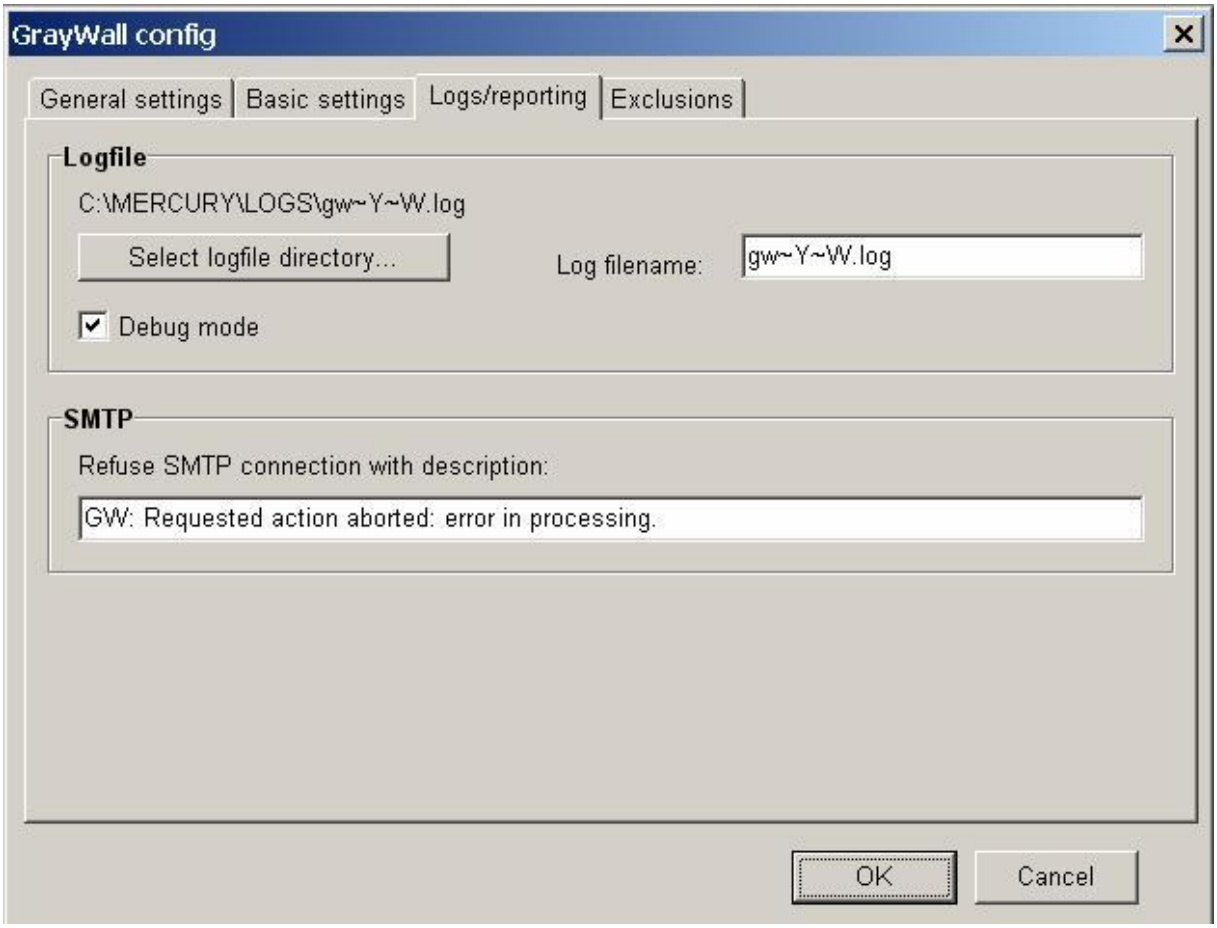
Select the directory in which Graywall's database and statistics file are stored. By default this is the Graywall subdirectory of your existing Mercury/32 directory. The directory name must end with a trailing backslash! ***[Graywall] GrayDataDir***

Graylist timeouts

Minimum retry time in minutes for unlocking a delivery – Delivery is unlocked only if the next delivery attempt is detected at least this time interval after first delivery attempt. ***[Graywall] unlock***

Unlock request expiration time in minutes – Each delivery request is registered in Graywall's database. A lot of these requests are not retried later. Registered requests are deleted from the database after this time value. ***[Graywall] expire***

Successful unlock expiration time in minutes – Opened servers (having a locked specified mail domain) are removed from the database after this time of inactivity and must be graylisted again in future. ***[Graywall] whiteexpire***



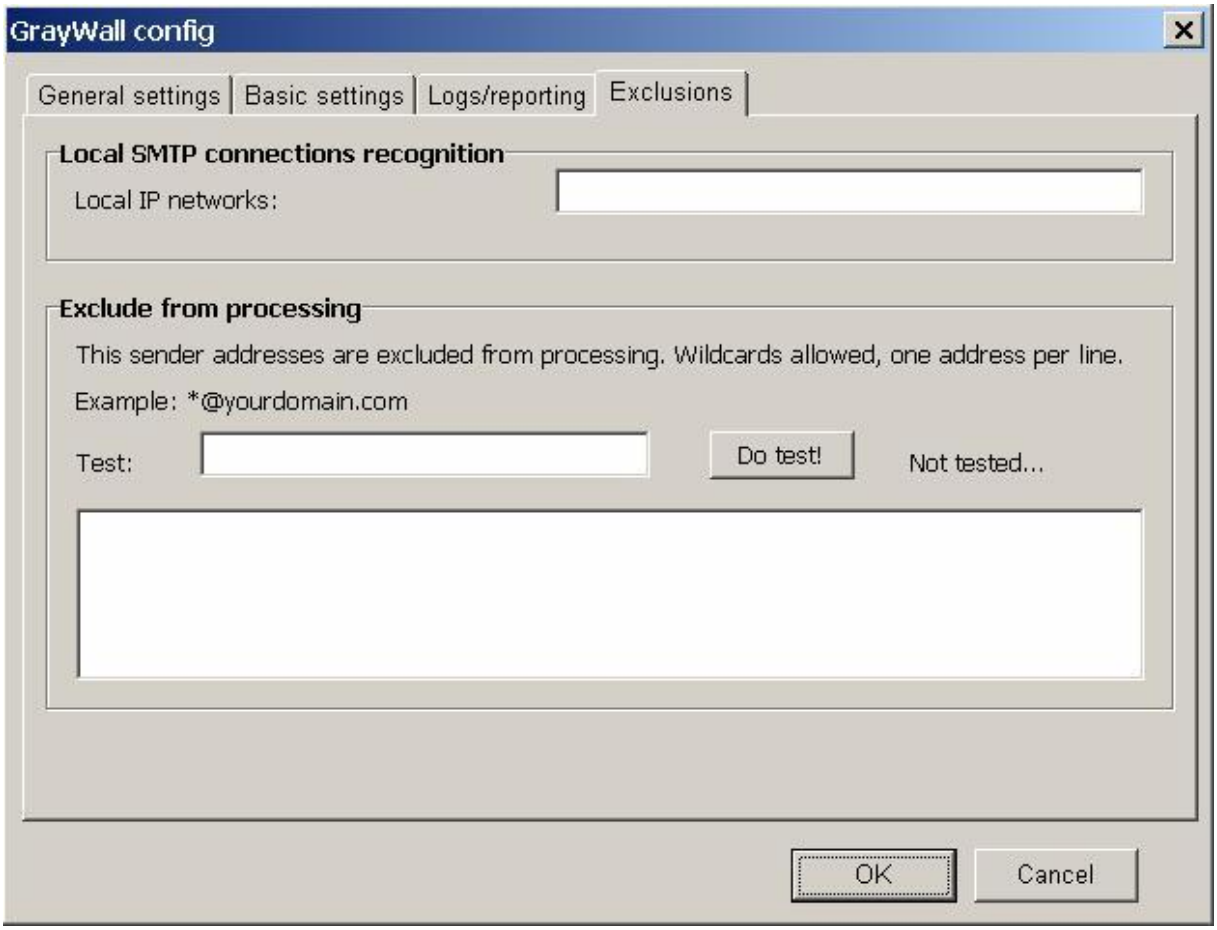
Logfile

File for Graywall logging. You can use the same name “special characters” in the name as can be used for log file names in Mercury. ***[Graywall] logfile***

If Debug mode is checked, Graywall writes debugging information to your logfile.
[Clamwall] Debug

SMTP

When Graywall rejects an SMTP session, this description of the SMTP error is used in the e-mail sent back to the originator. ***[Graywall] SmtpText***



Local SMTP connections recognition

SMTP connections from local IP addresses are not graylisted at all. You can specify here your Local IP addresses as IP networks. For example: 10.0.0.0/8, 192.168.0.0/16, 172.16.1.1/32

You can also use this feature for whitelisting specific servers on the Internet. ***[Graywall] LocalIP***

Exclude from processing

You can exclude senders' addresses from graylisting. But be careful, because spammers often forge sender's addresses! You can use wildcards here.

Excluded addresses are stored in gwexlist.txt file within your Graywall data directory.