JunkMail Manual

Declude Junkmail

Declude Junkmail runs the message through a variety of spam tests. All of the spam tests are defined in the global.cfg, so if you do not want a test run, you can take it out of the global.cfg file or simply comment out the test by adding a # to the beginning of the line where the test is located. The most popular (and debated!) tests are the ip4r category of tests (CBL, SPAMCOP, etc.). These work by taking the IP address of the machine that connected to MAILSERVER, reversing the order, and running a DNS lookup on a specific domain. If the DNS A record exists and matches a certain string, the email fails the test (and is considered spam).

For each test, you can determine what action will be taken on the email. For example, you can have any email that fails the SPAMCOP test (which rarely lets legitimate email through) held in the "spam" directory so that you can later check the messages to verify that they are spam. You could then have email that fails the ORDB test (which often lets legitimate email through) just have a warning message added to the headers.

In the case that an email fails 2 or more tests, the stricter action will be taken. In the above example, if a message failed the ORDB test and the SPAMCOP test, it would be held in the "spam" directory.

By default, Declude Junkmail will log every email that it scans. It will report in there any tests that the message fails along with the action that was taken on the message. Be sure to check Release Notes for new functionality.

Declude Main Files

Declude.exe – In Declude versions prior to 3.x, this was the main Declude executable file and was automatically started by the MAILSERVER as needed. In Declude versions 3.x and above, the declude.exe is used to move email messages to the \spool\proc directory so that the decludeproc service can pick them up and process them this is ony applicable in version 2.x of SmarterMail and all versions of Imail

Note that declude.exe must be in the MAILSERVER directory, not the Declude\ directory.

Decludeproc.exe – decludeproc.exe is the declude service which is the core of declude it will bring files to be processed into the \work directory, once the thread has processed the message decludeproc.exe will move the message to the Mail Servers spool or other appropriate directory.

global.cfg - This contains the "global" Declude settings. It includes standard settings, test definitions and the actions to take for outgoing E-mails. This is not a script (Declude doesn't use scripts), it is a standard configuration file, so there is no order to it (when adding lines you can put them anywhere in the file).

$default$.junkmail - This file is the one you will use most. It simply determines the actions to take when incoming E-mail (spam) fails the various tests. Each line determines the action to take for a specific test; for example, "ORBZ WARN" lets Declude know to add a standard "X-RBL-Warning:" header for E-mail that fails the ORBZ test.

virus.cfg – This file holds many directives that will tell the Declude virus scanner (Built-in or external) how to handle email based on certain criteria.

hijack.cfg – This is the default configuration file for Declude Hijack that you do not have to change. The main configuration consists of RELAYTHRESHOLD1 and RELAYTHRESHOLD2. These define the two thresholds (when a user reaches the first, the mail is held temporarily; when the user reaches the second, the mail is held permanently)

declude.cfg – This file contains advanced directives that can be used within Declude.

virus_domains.txt - Declude allows you to choose which domains will have their mail scanned. This is done with the virus_domains.txt file. You will read more about how to use this file later in this manual.

virus_users.txt - Declude allows you to choose which users will have their mail scanned. This is done with the virus_users.txt file. You will read more about how to use this file later in this manual.

all_list.dat - This file is used by the geolocation in Declude JunkMail. It has a list of IP ranges and the countries they were allocated to.

Other Files - Any other files in the Declude\ directory (or its subdirectories) are "per-user" or "per-domain" configuration files (see the "Per-User" and "Per-Domain" sections of this manual for more information). These files are in the exact same format as the Declude\$default$.junkmail file.

Basic Configuration (JunkMail)

By default, Declude will add one warning to the headers of the email for each spam test that the email fails. You may want to run it like this for a few days, and look at the emails you receive (and/or the Declude log file) to see what it considers spam.

Note that many of the tests (such as REVDNS and SPAMHEADERS) will catch a large amount of spam, but will also have many false positives. If spam tests were 100% perfect, there would only be one spam test. Therefore, most people will not block email on many of the tests. If you want to quickly start blocking spam, you should consider blocking the mail that fails the WEIGHT10 test (or WEIGHT20 test, to allow more spam through in order to further reduce false positives). The weighting tests will significantly reduce false positives, by only catching mail that fails several tests.

To change the actions that Declude takes on spam (for example, to delete it), you need to edit the $default$.JunkMail file. This file has one line for each test that will be run. Each line has the name of the test, followed by the action to take. For example, a line that says "ORBZ WARN" means that Declude will add a warning to the headers of the email if it fails the ORBZ test.

If you wanted to have Declude hold emails that is listed in ORBZ, you would change the line "ORBZ WARN" to "ORBZ HOLD". A list of the various actions that can be taken are as follows later.

Advanced Configuration (JunkMail)

Junkmail Logs

LOGFILE

These are the Declude JunkMail options available in the global.cfg This specifies the location for the log file. If "####" is found in this entry, it will be replaced with the current 2-digit month and 2-digit date (so on December 1st, it would appear as "1201"). It can either take a relative path ("Declude\Logs\dec####.log") or a hard-coded parth ("D:\MAILSERVER\Declude\Logs\dec####.log").

LOGFILE Declude\Logs\dec####.log

LOGLEVEL

To specify the logging level for Declude. It takes one parameter (the level), which (in order) can be:

- NONE No logging information
- ERROR Will only record error messages (*not recommended*)
- WARN Will also record warning messages
- LOW Report basic information about each message
- MID Report slightly more information
- HIGH Report a lot of information
- DEBUG Report thorough diagnostic messages (this should normally only be used at the request of our support department).

LOGLEVEL DEBUG

LOG_OK

To prevent the logging of information that would normally appear for "good" If you do not want Declude JunkMail to record to the log file any E-mail that is not spam.

LOG_OK NONE

EVENTLOG

To instruct Declude JunkMail to record log file entries to the event log. use the following:

EVENTLOG ON

Adding headers to the E-mail

XOUTHEADER & XINHEADER

Declude has several ways that you can add headers to the E-mail that it processes. The standard way is as an action, for example "ORBZ WARN" will add a warning to the headers if the E-mail comes from an IP address listed in the ORBZ spam database. To add a header to all incoming E-mail or all outgoing E-mail, you can use the XINHEADER and XOUTHEADER configuration options. See the "variables" section for a list of the variables you can use.

XOUTHEADER X-Note: Please send abuse reports to abuse@%LOCALHOST%
XINHEADER X-Note: Please send abuse reports to abuse@%LOCALHOST%

XSENDER

If you want to record the name of the sender (according to the SMTP Envelope) in the E-mail headers, you can use the XSENDER configuration option. To do this, add a line to the global.cfg file as:

XSENDER ON

XSPOOLNAME

If you want to log the spool file name of the E-mail in the headers, you can use the configuration option "XSPOOLNAME"This is useful for finding the Declude log file entry for an E-mail.
Note that this will appear on all E-mail, whether or not any actions are taken. To do this, add a line to the

global.cfg file as

XSPOOLNAME ON

XWHITELIST (4.10.42)

Gives the reason for why the email was WHITELISTED in the header of the email.

XWHITELIST ON

OUTBOUNDSCANNINGSPAM & INBOUNDSCANNINGSPAM

Acting as a gateway for domains on other servers

Declude can be set up to scan E-mail for domains that are not hosted on your MAILSERVER. First, you need to set up your MAILSERVER to accept mail to the gateway domains and pass on the mail to the correct server (you need to set up the MX records to point to the MAILSERVER, and follow the instructions in the manual or MAILSERVER Knowledge Base for a gateway domain). The only catch as far as Declude is concerned is that MAILSERVER will treat the E-mail to the gateway domain as outgoing mail, since it is not stored on the MAILSERVER. Therefore, by default, the outgoing actions in the global.cfg file will be used. To get around this, you can set up per-domain configuration files for the gateway domains.

As of Declude version 4.3.14, Spam checking for inbound/outbound scanning can be turned on/ off easily. Located as a directive in the global.cfg file.

OUTBOUNDSCANNINGSPAM ON
INBOUNDSCANNINGSPAM ON

DECODE

Specifies that Declude JunkMail should attempt to decode messages (such as MIME decoding and removing HTML tags). Having this option turned off, saves a bit of CPU time, but makes filters less effective.

DECODE ON

CONSOLE

Determines whether Declude should should write the console.txt to the \Directory which contains the number of messages processed and number of messages reaching the spam threshold since the last start of the decludeproc service.

CONSOLE ON

SWITCHRECIP

Using the actual recipient instead of intended recipient for settings

Your MAILSERVER will report two addresses for each recipient of an E-mail, the "Intended recipient" (the one that the E-mail was addressed to), and the "Actual recipient" (the address after aliases have been accounted for). The configuration files in Declude are based on the actual recipient. If for some reason you would like to override this behavior (and have the configuration files based on the intended recipient), you can add a line to the global.cfg file. However, this is not normally recommended.

SWITCHRECIP ON

DOSENDERACTIONS

Declude JunkMail should use sender actions. When enabled, Declude JunkMail will look for per-user/per-domain settings *.junkmail for the sender of an E-mail. Used specifically for OUTBOUND per-user/per-domain settings.

DOSENDERACTIONS ON

ZEROHOUR

This directive is used for CommTouch Zero-Hour Virus Protection and Recurrent Pattern Detection Technology. If you are subscribed to Declude for the CommTouch add-in as a perpetual license customer or have a subscription, to enable, add/use the ZEROHOUR directive in the global.cfg file to control the weight associated with this test.

CT-SPAM	**COMMTOUCH**	X	4	**20**
CT-BULK	**COMMTOUCH**	X	3	**8**
CT-SUSPECT	**COMMTOUCH**	X	2	**4**

Versions prior to 4.10.72 use the configuration below

COMMTOUCH	**ZEROHOUR**	X	X	**12**

Versions prior to 4.10.43 use the configuration below

ZEROHOUR 12

STOPPROCESSINGONFIRSTDELETE

This setting will stop processing of the email if an action of DELETE was found to be true. This will allow Declude to be more efficient but will not log information about the other recipients in that email.

STOPPROCESSINGONFIRSTDELETE ON

COPYFILEACTIONWITHHEADERS

This setting is married to the COPYFILE action and will ensure that header information is added to the mail message before the copy is performed.

COPYFILEACTIONWITHHEADERS ON

ACTIONSONCOPYALL (Imail Only)

Deleting email has changed since Declude version 1.82 allowing you to delete email on a per user level. A bug was found that actions were not applied on the copyall account. Defining ACTIONSONCOPYALL ON in global.cfg, will enable declude to apply actions on that account on a per user (user.junkmail) or global ($defautl$.junkmail) setting. This needs to be in the global.cfg.

ACTIONSONCOPYALL ON

NOACTIONSONCOPYALLWHENWHITELISTED (Imail Only)

If a email is whitelisted and had the copyall account added in the headers and the ACTIONSONCOPYALL directive is defined, it will not take actions on the copyall account for the one email. This needs to be in the global.cfg.

NOACTIONSONCOPYALLWHENWHITELISTED

LOOSENSPAMHEADERS

Instructs Declude JunkMail to change the SPAMHEADERS test so that it will not be triggered on E-mails that have no Message-ID: header. This option is not recommended, as that is one of the most useful parts of the SPAMHEADERS test (but also may cause false positives).

LOOSENSPAMHEADERS ON

HOP & HOPHIGH

Scanning different hops

Declude allows you to work over multiple hops. This means that if E-mail isn't delivered directly to your MAILSERVER (for example, if the MX record for your domain points to a virus scanner or gateway mailserver, that then forwards to your MAILSERVER), you can still use Declude. If you have a set number of hops in front of your MAILSERVER, which you may not know the IPs of, the **HOP** option may be useful.

When set to 0 (the default), Declude JunkMail uses the IP address of the mail server that connected to your MAILSERVER.

HOP 0

Spammer 1.1.1.1 --> Relay 2.2.2.2 --> Declude (Declude will check 2.2.2.2)

If you set it to 1, Declude JunkMail will check the IP address 1 hop away. You would use this if you have 1 SMTP server before your MAILSERVER

HOP 1

Spammer 1.1.1.1 --> Relay 2.2.2.2 --> Declude (Declude will check 1.1.1.1)

If you want to scan a range of hops, you can use the **HOP** option along with the **HOPHIGH** option. In this case, you would set HOP to the first hop that you want to scan, and **HOPHIGH** tothe last hop that you want to scan. If you want to scan the IP of the mail serverthat connected to yours, as well as the one that connected to it, you would set **HOP** to 0 and **HOPHIGH** to 1. Be aware that every hop you scan will require extra time for DNS checks.

HOP 0
HOPHIGH 1

Spammer 1.1.1.1 --> Relay 2.2.2.2 --> Declude (Declude will check 1.1.1.1 and 2.2.2.2)

Normally, you will leave the **HOP** setting at **HOP** 0 and use an **IPBYPASS** line for each gateway or backup mailserver.

Email should never be sent directly from a senders client (other than your own users) to your mail server as these are Dial-up or Dynamic Ip addresses. Therefore Declude will ignore any test that contains DUL, DYNA, DUHL in the name after the first HOP.

IPBYPASS

Skipping your backup mail server or gateways

If you have a backup mail server, the normal E-mail routing can be changed. Rather than remote mail servers delivering mail directly to the primary mail server, the mail can sometimes go through the backup. In this case, Declude will by default scan the IP address of your backup server (since it doesn't know that it is your backup mail server).

To do this, you need to let Declude JunkMail know the IP address(es) of your backup/gateway mail server(s). This is done by adding an IPBYPASS line in the \Declude\global.cfg file for each backup/gateway mail server. Declude will skip over that hop, and automatically start scanning based on the IP of the mail server that connected to the backup mail server. For example, if you have 2 backup mail servers with the IPs 192.0.2.25 and 192.0.2.26, you would add the following lines to your global.cfg file:

```
IPBYPASS 192.0.2.25
IPBYPASS 192.0.2.26
```

Then, Declude JunkMail will be able to see the IP address that connected to your backup mail server, and process the E-mail correctly. You can have up to 20 IPBYPASS lines in the global.cfg file. Declude Version 4.10.42 allows for CIDR ranges to be used.

DNS

DNS Server

By default, Declude uses the same DNS server that MAILSERVER uses. If you want to use a different DNS server, you need a line in the global.cfg starting with "DNS", followed by the IP of your DNS server. Only 1 DNS server can be specified.

```
DNS             198.6.1.2
```

HIDETESTS

Hiding tests from the X-Spam-Tests-Failed: header

Declude has a HIDETESTS option that lets you specify tests that should not be listed in the X-Spam-Tests-Failed: header. This is useful for tests that are not indicative of spam (such as the CATCHALLMAILS test, which all E-mails will trigger). To use this option, just list any such tests in the HIDETESTS line in the \global.cfg file

```
HIDETESTS       CATCHALLMAILS IPNOTINMX NOLEGITCONTENT
```

Whitelisting email

If you need to whitelist mail (make sure that it passes all the spam tests), you can do so, based on the IP address, the return address, or text that appears within the E-mail.

WARNING: White listing is a last resort to accept mail from poorly administered mail servers, and will often allow spam through if you are not careful.

WHITELIST HABEAS

Habeas headers will appear in legitimate E-mail from sources that are approved to use the headers. Any spammers that get whitelisted due to the Habeas headers can be reported to www.habeas.com, and legal action will likely be taken against them. This is a good way to help prevent false positives -- people whose E-mail gets caught as spam can just go to the URL shown to find out how to add the Habeas headers to their E-mail.

Whitelist E-mail with the Habeas Headers by adding a line the following line to your global.cfg

```
WHITELIST    HABEAS
```

WHITELIST LOCAL

This directive causes all email between local domains (all domains hosted on the local server) to be whitelisted. The sender and *all* recipients must be local. A single remote recipient will cause the email not to be whitelisted

```
WHITELIST    LOCAL
```

WARNING: If a spammer spoofs a users email address as being the sender the email will be whitelisted.

DOMAINWHITELISTS

This is an advanced option and instructs Declude JunkMail should use domain whitelists. When enabled, Declude JunkMail looks for a \Declude\example.com\whitelist.txt file which is a per-domain setting. The format of the whitelist.txt file is the same as the format used for WHITELISTFILE.

```
DOMAINWHITELISTS    ON
```

PREWHITELIST

When turned off Declude JunkMail will notrun whitelists before tests are run. If the E-mail is whitelisted, the tests are not run. Useful when using the BYPASSWHITELIST test.

NOTE:
[1] not all whitelists will be run this way, in which case the E-mail will be whitelisted but the tests will be run.

[2] some people do not want this option enabled (to ensure that external tests are run on legitimate mail, too).

PREWHITELIST ON

WHITELIST AUTH

Whitelisting Authenticated Users

To automatically whitelist your own users that authenticate. This is useful to help ensure that the E-mail your users send does not get caught, especially if they are using a mail client such as Outlook that may fail several anti-spam tests. To do this, you just need to add a line to your global.cfg

WHITELIST AUTH

NOTE: Versions of IMail proir to 8 do not support this directive.

AUTOWHITELIST

Automatic Whitelisting

You can automatically whitelist E-mail addresses that are listed in the recipient's address book. To do this, you just need to add a line to your global.cfg

AUTOWHITELIST ON

With this feature enabled, when an E-mail is received, Declude JunkMail will check to see if the sender is listed in the recipient's web messaging address book. If so, the E-mail will automatically be whitelisted. This feature can help reduce false positives. If you are using Smartermail Declude will also chech the user and domain trusted senders list.

WHITELIST IP

Whitelist an IP address, add a line to your global.cfg (replacing 127.0.0.1 with the IP you wish to whitelist).

WHITELIST IP 127.0.0.1

Whitelist a range of IP addresses such as 127.0.0.0 through 127.0.0.255, which will whitelist any E-mails from mail servers with an IP address that contains 127.0.0. you can do so by adding a line:

WHITELIST IP 127.0.0.

You can also use a CIDR range (see www.DNSstuff.com site's CIDR tool for assistance), such as:

WHITELIST IP 127.0.0.0/8
WHITELIST IP 127.0.0.0/24

WHITELIST FROM

Whitelist an E-mail address, add a line to your global.cfg (replacing user@example.com with the address you wish to whitelist):

WHITELIST FROM user@example.com

Whitelist a domain, add a line to your global.cfg (replacing @example.com with the domain you wish to whitelist):

WHITELIST FROM @example.com

Whitelist a sub-domain add a line to your global.cfg (replacing subdomain and example.com with the subdomain and domain you wish to whitelist):

WHITELIST FROM @subdomain.example.com

Whitelist all sub-domains add a line to your global.cfg (replacing example.com with the domain you wish to whitelist):

WHITELIST FROM .example.com

NOTE: that WHITELIST FROM will whitelist a *return address* (like **Imail** does in the Kill List), which may be different from the From: or Reply-To: addresses. You need to look at the X-Declude-Sender: header (if you use the XSENDER ON option) or the MAIL FROM: line in the **MAILSERVER** SMTP log file to find the return address.

WHITELIST FROM@hotmail.com

Will allow a LOT of spam through as this is often forged.

WHITELIST FROMmail.com

Would whitelist mail from mail.com and hotmail.com

WHITELIST FROMyour_domain.com

WARNING: Never whitelist your own domain (since many spammers will use a made-up return address on your domain). If you do not understand these warnings, you should not use whitelists.

WHITELIST (text)

Whitelist text You can whitelist text that appears anywhere in the headers or body of the E-mail, add a line to your global.cfg (replacing "text" with the text you wish to use for whitelisting).

```
WHITELIST    ANYWHERE    text
WHITELIST    BODY    The secret code is 12345
```

Any E-mail containing "The secret code is 12345" would be whitelisted.

WHITELIST TODOMAIN

Whitelist mail TO a certain domain add a line to your global.cfg (replacing example.com with the domain you wish to whitelist TO):

```
WHITELIST    TODOMAIN    @example.com
WHITELIST    TODOMAIN    example.com
```

You do not need to enter domain aliases if do not want to. (If you have the domain name as "example.com" with "mail.example.com" as an alias, both will be whitelisted).

WHITELIST TO

Whitelist mail TO a certain user add a line to your global.cfg (replacing user@example.com with the user address you wish to whitelist TO):

```
WHITELIST    TO    user@example.com
```

WHITELISTFILE

Whitelist Limit

You can have up to 200 of the WHITELIST entries in the global.cfg file. They only work in the global.cfg file. Also, they work on a "partial match", so you should not remove the "@" from E-mail addresses (or domains) that you whitelist, without thinking of the consequences.

If you need to have unlimited whitelist entries, or if you need per-user or per-domain whitelisting, you may find the WHITELISTFILE option helpful.

To use this option, you need to add a line to the appropriate $default$.junkmail configuration file or the per-user/per-domain configuration file you wish to use the whitelists with:

```
WHITELISTFILE    C:\MAILSERVER\Declude\mywhitelist.txt
```

The mywhitelist.txt file would then contain either:

```
#E-mail address
user@example.com

#Domain
@example.com

#Subdomain
.example.com
```

One entry per line per line. The whitelist files can have unlimited entries in them.

NOTE: the file you use with the WHITELISTFILE option does NOT use the same format as the WHITELIST entries in the global.cfg file. and that the WHITELISTFILE option does not work in the global.cfg file.

Whitelist Reference Located in the global.cfg

Feature	Sample Format	How matches work
Whitelist - 'Anywhere'	WHITELIST ANYWHERE some text	Partial match (matches any E-mail with 'some text' in it)
Whitelist - Habeas Headers	WHITELIST HABEAS	n/a - whitelists all E-mail with Habeas headers
Whitelist - HELO/EHLO	WHITELIST HELO example.com	Partial match (matches any HELO/EHLO data 'example.com' in it)
Whitelist - IP	WHITELIST IP 192.168.100.1	Partial match (matches 192.168.100.1 and 192.168.100.10)
Whitelist - IP Range	WHITELIST IP 192.168.100.0/24	Matches a CIDR range
Whitelist - Recipient	WHITELIST TO user@example.com	Exact match (matches if any recipient is 'user@example.com')
Whitelist - Recipient Domain	WHITELIST TODOMAIN @example.com	Partial match (matches any recipient address with '@example.com' in it)
Whitelist - Reverse DNS	WHITELIST REVDNS .example.com	Partial match (matches any return address with '.example.com' in it)
Whitelist - Sender	WHITELIST FROM	Partial match (matches any return address with

Whitelist - Sender	user@example.com	'user@example.com' in it)
Whitelist - Sender Domain	WHITELIST FROM @example.com	Partial match (matches any return address with '@example.com' in it)
Whitelist - Sender Subdomain	WHITELIST FROM .example.com	Partial match (matches any return address with '.example.com' in it)
Whitelist - Subject	WHITELIST SUBJECT Make Money Fast	Partial match (matches any subject with "Make Money Fast" in it)

NOTE: other formats will not work; for example, using a "*" or "-" in an IP address will not work. Secondly no #comments can be placed after the entry.

- Whitelisting is not working

With Declude , you can add your own IP blacklist (a list of IP addresses that you will treat differently -- that you delete, bounce, add a warning to the headers of, etc.).

```
BLACKIP  IPFILE
```

Your own IP blacklists

First, you need to create a text file that lists one IP address per line, followed by the reason for blocking it.

```
127.0.0.1This is a test block
```

Next, you need to define a new Declude test. In the global.cfg file, you can add a line n your global.cfg

```
TESTNAME    IPFILE    C:\MAILSERVER\Declude\ipfile.txt    x    5    0
```

"TESTNAME" is the name of your new test, followed by the word "ipfile" (which is the test type), followed by the name of the file you have the IPs listed in, "x" as a placeholder, followed by the weight (5) and a 0

Once you have defined the blacklist, you can use whatever actions you would like in the configuration files (per-user, per-domain, or default, just like the other tests).

You can define as many different IP blacklists as you like, so you could, for example, have a list of IPs that you will not accept mail from, and another that would just result in a warning in the headers.

To blacklist a range of IPs, you can use CIDR style IP ranges this would blacklist all addresses from 127.0.0.0 through 127.255.255.255.

```
127.0.0.0/8  Spammer
```

This would blacklist the Class C range from 127.0.0.0 through 127.0.0.255. For assistance on CIDR ranges, you can use the CIDR tool at DNSstuff.com

```
127.0.0.0/24  Spammer
```

```
BLACKIP  IPFILE
```

Your own sender blacklists

With Declude , you can add your own sender blacklist (a list of return addresses or domains that you will treat differently -- that you delete, bounce, add a warning to the headers of, etc.). This works on the return address (where bounce messages would be sent, as seen in the X-Declude-Sender: header), which may be different from the "From:" address in the headers. Note that the return address is *not* visible in the headers unless you use the "XSENDER ON" option (you can later find out what the return address was by checking the **MAILSERVER** SMTP log files for the "MAIL FROM:" line).

First, you need to create a text file that lists one address or domain per line, followed by the reason for blocking it.

```
@example.com  This domain sends spam
vilperson@hotmail.comThis guy was mailbombing us
```

To block a domain, you can either use the format "@example.com" to block just example.com, or you can use just "example.com" which would block mail from "user@example.com", "user@mail.example.com", and even "user@another_example.com".

Next, you need to define a new Declude test. In the global.cfg file, you can add a line:

```
TESTNAME    FROMFILE    C:\MAILSERVER\Declude\badaddresses.txt    x    5    0
```

where "TESTNAME" is the name of your new test, followed by the test type ("fromfile"), followed by the name of the file you have the addresses and/or domains listed in, followed by a placeholder, and the two weights for the test

Once you have defined the blacklist, you can use whatever actions you would like in the configuration files (per-user, per-domain, or default, just like the other tests).

You can define as many different sender blacklists as you like.

Blacklist Reference

Located in the global.cfg

Feature	Sample Filename	Sample Format	How matches work
Blacklist - IP	ipblacklist.txt	192.168.100.1	Exact match (only matches 192.168.100.1)
Blacklist - IP Range	ipblacklist.txt	192.168.100.0/24	Matches a CIDR range
Blacklist - Sender	fromblacklist.txt	user@example.com	Exact match (only matches 'user@example.com')
Blacklist - Sender Domain	fromblacklist.txt	@example.com	Partial match (matches any return address with '@example.com' in it)
Blacklist - Sender Subdomain	fromblacklist.txt	.example.com	Partial match (matches any return address with '.example.com' in it)

NOTE: other formats will not work; for example, using a "*" or "-" in an IP address will not work.

- Blacklisting not working ?

Test Definitions

Tests are defined in the global.cfg file. The format of a test definition is the name of the test, followed by the test type, followed by two test-specific pieces of information, followed by two weights: The weight that will be assigned to the test if an E-mail fails the test, and the weight that will be assigned if the E-mail does not fail the test (normally 0).

The ORDB test might be defined as:

```
ORDB    IP4R    relays.ordb.org    127.0.0.2    5    0
```

This would mean that the test named ORDB is an "ip4r" test type (for "dnsbl" style DNS lookups), using the zone relays.ordb.org, and looking for a result of 127.0.0.2. If an E-mail fails the test, the test would have a weight of 5; otherwise, it would have a weight of zero.

Multiple actions per test

Declude does not support multiple actions per test. When it was designed, it was assumed that people would only want to use one of the two actions that other anti-spam products use: WARN or BOUNCEONLYIFYOUMUST. However, since Declude allows so many different actions to be taken on E-mail, a number of people have requested the ability to use multiple actions per test. Although Declude does not support this, there is a way to accomplish the same end result. You just need to define two copies of the same test, each with a different name.

If you wanted to have the SPAMCOP test use both the WARN and SUBJECT actions, you would change add a new test SPAMCOP2. The global.cfg defines the SPAMCOP test as:

```
SPAMCOP    IP4R    bl.spamcop.net    127.0.0.2    7    0
```

You would add another entry that is identical except with a different name, so you would now have:

```
SPAMCOP    IP4R    bl.spamcop.net    127.0.0.2    7    0
SPAMCOP2   IP4R    bl.spamcop.net    127.0.0.2    7    0
```

Then, in your $default$.junkmail file, you could have:

```
SPAMCOP    WARN
SPAMCOP2   SUBJECT Spam
```

Now, both actions will be used. There are some combinations of actions that will not work together (such as DELETE and HOLD, which logically can't both be used), but most will. Also, if you use the weighting system, you should set the weights of the second test to 0, so that you do not end up with double the weight.

Copy All account

If you have a "Copy All" account set up in **MAILSERVER** (such that all E-mail is copied to a specific mail account), and use Declude , you should set up a per-user setting for that account (with the actions set to IGNORE). Otherwise, your per-user settings may not work as expected.

External Tests

Declude JunkMail supports external tests -- tests that use third-party spam detection programs (such as Message Sniffer, or your own custom programs).

```
SPAMCHK    external    nonzero "C:\MAILSEVER\Declude\spamchk\spamchk.exe"    5    0
INV-URIBL  external    nonzero "C:\MAILSEVER\Declude\INVURIBL\invURIBL.exe %WEIGHT%%REMOTEIP%"
  10   0
SNIFFER    external    nonzero "C:\MAILSEVER\Declude\Sniffer\SNFClient.exe"    12    0
```

Your program will get called by Declude , with the name of the spool file containing the E-mail as a parameter:

("yourfile.exe c:**MAILSERVER**\spool\D1234567.SMD", for example). The file contains the complete E-mail, including headers and body. Your program should only read this file, not write to it.

After your program is finished, it needs to return an exit code to Declude (in C/C++, this is done simply with "return code;" at the end of the main function; you can (carefully!) use the Windows ExitProcess( ) function in

other languages).

To define the test, you need a line in the format 'TESTNAME external returnvalue "filename"'. TESTNAME is the name of your test, "returnvalue" is the code your program will return when it detects spam (or "nonzero" for any code other than zero), and the name of your file needs to be in quotes. You can add weights, by adding two numbers at the end of the line: the first one is the standard weight (the weight if the test fails), the second is the "negative weight" (the weight if the test does not fail, usually 0). The test will then work in Declude just like any other test.

For more flexibility, you can have Declude pass parameters to your program, using variables. For example, you can set up the test as 'TESTNAME external returnvalue "filename %INOROUT%"', which would send the %INOROUT% variable as a parameter to your program (which would be "incoming" for an incoming E-mail, or "outgoing" for an outgoing E-mail).

External tests - whitelisting E-mail

An external test can whitelist E-mail by using the "externalplus" test type. With the externalplus test type (using a test definition such as 'MYTEST externalplus nonzero "C:**MAILSERVER**\Declude\myprog.exe"'), you can return 0 if an E-mail is not considered spam, 1 if it should be whitelisted, or a value of 10 or higher if the E-mail is considered spam. Note that return values of 2 through 9 are reserved for future use.

External tests - returning a weight

An external test can return a weight by using "weight" in the test definition instead of the exit code that it will be returning. So you would use a format such as 'TESTNAME external weight "filename"'.

Actions (Junkmail)

Located in the $default$.junkmail for incoming messages or global.cfg for outgoing messages. Actions are a very important concept with Declude . See the "Basic Configuration" section for how to set up the actions. Note that the actions are listed here in order with the lowest priority tests listed first; this order will be used to determine what action is taken when an E-mail fails multiple tests. For example, if an E-mail fails two tests, one using the "HOLD" action, and the other using the "DELETE" action, the DELETE action will take priority.

The actions currently available are:

Action Name	Description
IGNORE	Does nothing (except add a log entry). Same as LOG action. Note that this does not ignore the test. The test will still run, but nothing will be added to the header if the test is triggered.
LOG	The LOG action places an entry into the log file (C:**MAILSERVER**\spool\dec####.log by default).
BEEP	The BEEP action will cause a beep to be heard at the server. You can choose the frequency (in hertz) and duration (in milliseconds); for example, "ORBZ BEEP 1000 100" would sound a 1000hz tone for 100ms (1/10 second).
COPYFILE	This action will copy the **MAILSERVER** D*.SMD and Q*.SMD files into a directory of your choice. For example, "WEIGHT10 COPYFILE C:**MAILSERVER**\spool\weight10\" will copy all E-mail with a weight of 10 or higher into a directory C:**MAILSERVER**\spool\weight10.
COPYTO	The COPYTO action will send a copy of the E-mail to another address of your choosing (as well as to the intended recipient). This may be useful in determining which tests to use. To use it, just add the E-mail address you want to send the spam to -- for example, "WEIGHT10 COPYTO user@example.com".
WARN	The WARN action is the same action that most spam control programs use. It simply adds an extra SMTP header to the E-mail, in the format "X-RBL-Warning: (description)" The user will usually NOT see this warning. However, they can set up their E-mail client to filter based on this header. You can create your own warning header to use; for example, "ORBZ WARN X-RBL-Warning: This E-mail is probably spam." If you use your own warning header, you MUST make sure that it is a valid header -- if you don't know, don't use your own warning header (just use "TESTNAME WARN").
FOOTER	The FOOTER action adds a footer to the bottom of the E-mail. This likely isn't too useful for most people, as by the time someone reads it, they know the E-mail is spam. You need to specify the text of the footer; for example, "ORBZ FOOTER [This may be spam]".
HEADER	The HEADER action adds a header to the top of the **body** of the E-mail. This may make it easier for the recipient to quickly determine that the mail is a spam. You need to specify the text of the header; for example, "ORBZ HEADER [This may be spam]". **NOTE**: This will appear in the **body** of the E-mail; to have a warning appear in the headers, you should use the WARN action.
SUBJECT	The SUBJECT action adds "SPAM: " to the subject of the E-mail. This is an easy way to let users know that the mail is probably spam, but lets them decide whether or not to read it. You can use your own text in the subject; for example, "ORBZ SUBJECT [Spam]".
	The ATTACH action converts a spam into a much friendlier E-mail. By

ATTACH ("SpamHider")	default, the subject is "You have spam!", and the body contains the sender's address, the subject, and which tests the spam failed. Then, there is a link the recipient can click if they want to view the original E-mail. NOTE: If you use per-user or per-domain settings, a spam sent to multiple recipients at the same time may will be sent this way if any of them use the ATTACH action. You need to place the spamattach.eml file in your **MAILSERVER**\Declude directory for this to work.
MAILBOX	The MAILBOX action will send an E-mail to a specific mailbox (folder) for the recipient. For example, you can have E-mail moved to a "spam" mailbox that the user can check via web messaging or IMAP (or POP3, by setting up a special account in the format "user-mailbox"). To use it, just include the name of the mailbox to use -- for example, "WEIGHT10 MAILBOX spam".

ALERT	The ALERT action will send a standard "bounce" message back to the sender of the E-mail, but will also deliver the E-mail to the recipient. To send a customized message, you need to create a file named **MAILSERVER**\Declude\TESTNAMEalert.eml (replacing TESTNAME with the name of the test you want the alert to be for; for example, **MAILSERVER**\Declude\BADHEADERSalert.eml). The .EML file needs to have a To:, From:, and Subject: before the first blank line; for example:
	
	`To: %MAILFROM%`
	`From: postmaster@%LOCALHOST%`
	`Subject: Deliverable mail`
	
	`Your mail was delivered, but may not be read by the recipient`
	`because it contains invalid headers that are not RFC compliant.`
	`Original message follows:`
	
	`%FULLMSG%`

ROUTETO	The ROUTETO action will re-route an E-mail to another address (without delivering it to the intended recipient). For example, you could have all mail failing the WEIGHT10 test delivered to weight10@example.com. This can be used so that you can have an E-mail address that monitors spam. To use it, just add the address after "ROUTETO" -- for example, "WEIGHT10 ROUTETO user@example.com".
HOLD	The HOLD action will move the E-mail into the **MAILSERVER**\spool\spam directory. This way, you can check messages to make sure they are spam before deleting them manually (or, you can move the files (Q*.SMD and D*.SMD for Imail or *.EML and *.HDR for SmarterMail) back to the spool directory to have them delivered on the next queue run (about 20-30 minutes)). **Specify the directory to hold spam in:** HOLD [Path] **Automatically create a date directory to hold spam:** HOLD %DATE% Assuming the current date is Jan 1, 2005, this will place spam in MAILSERVER\spool\spam\01 Jan 2005 HOLD [Path]\%DATE% Assuming the current date is Jan 1, 2005, this will place spam in [Path]\01 Jan 2005. %DATE% is the only available format, other variables like %EURDATE% will NOT work. The folder will automatically be created each day.

BOUNCEONLYIFYOUMUST	**DO NOT USE THIS ACTION** unless you understand FULLY that spammers will NEVER receive the bounce message. The BOUNCEONLYIFYOUMUST action will send a standard "bounce" message back to the supposed sender of the E-mail. To send a customized message, you need to create a file named **MAILSERVER**\Declude\TESTNAMEbounce.eml (replacing TESTNAME with the name of the test you want the bounce to be for; for example, **MAILSERVER**\Declude\BADHEADERSbounce.eml). The .EML file needs to have a To:, From:, and Subject: before the first blank line; for example:
	
	`To: %MAILFROM%`
	`From: postmaster@%LOCALHOST%`
	`Subject: Undeliverable mail`

	Your mail was not delivered because it contains invalid headers that are not RFC compliant. Original message follows: %FULLMSG% **Note, however, that about 99% of all spammers use forged return addresses, and will never see the bounce message.** Because of this, the BOUNCEONLYIFYOUMUST action should only be used if there is a good chance that the E-mail is not spam, and you fully understand *why* you want to bounce the E-mail. In most cases, it wastes bandwidth, and inconveniences innocent victims (the people whose addresses are forged by the spammers).
DELETE_RECIPIENT	The DELETE_RECIEPIENT will REMOVE the recipient from the email header. If a multiple recipient email is processed (user1@domain.com and user2@domain.com)and the DELETE_RECIEPIENT is triggered on user1@domain.com, user1@domain.com will be removed and the email will ONLY be received by user2@domain.com. If all recipients are removed, the email will be deleted.
DELETE	The DELETE action should NOT BE USED, unless you are sure that you want to delete the messages. At the very least, you should use one of the other actions first to verify that important messages will not get caught by the test. This is the most common action used by spam control programs, but one you have to use at your own risk.

Directives (JunkMail)

The following is a list of directives that are used or can be used in the global.cfg file.

LOGFILE	This option has one parameter, which specifies the location for the log file. If "####" is found in this entry, it will be replaced with the current 2-digit month and 2-digit date (so on December 1st, it would appear as "1201"). It can either take a relative path ("Declude\dec####.log") or a hard-coded path ("[path]\Declude\dec####.log").
LOGLEVEL	This option specifies the logging level for Declude JunkMail. It takes one parameter (the level), which (in order) can be used : **NONE / ERROR / WARNING / LOW / MID / MEDIUM / HIGH / DEBUG**
EVENTLOG	This option has one parameter, **ON**, which indicates that Declude JunkMail should record log file entries to the event log.
XINHEADER	This option lets users add a custom header to the E-mail headers of incoming E-mail. It takes one parameter (the header to add), which can include spaces. Multiple XINHEADER lines can be used (the total length of added headers is limited to 4,096 bytes).
XOUTHEADER	This option lets users add a custom header to the E-mail headers of outgoing E-mail. It takes one parameter (the header to add), which can include spaces. Multiple XINHEADER lines can be used (the total length of added headers is limited to 4,096 bytes).
XSENDER	This option takes one parameter, **ON**. The presence of this line will add an X-Declude-Sender: header to the E-mail, showing who sent the E-mail and the IP address it came from. The newer XINHEADER/XOUTHEADERS can do the same thing with more flexibility.
XWHITELIST	This option takes one parameter, **ON** Givese the reason for why the email was WHITELISTED in the header of the email.
XSPOOLNAME	This option takes one parameter, **ON**. The presence of this line will add an X-Declude-Spoolname: header to the E-mail, showing the Imail or Smartermail spool name of the message. This can be handy for tracking messages down in the Declude logs if needed.
CONSOLE	This option takes one parameter, ON or OFF (default), which determines whether Declude should look for and run the \IMail\deccon.exe program (the "Declude Console", which is required for Declude Hijack, but which can run with other Declude programs).
IPBYPASS	This option has one parameter, which is a single IP address (no CIDR ranges allowed) that should be bypassed by Declude JunkMail (so Declude JunkMail will scan the E-mail based on the IP that connected to the IP listed here, rather than scanning based on the IP listed here). There can be up to 100 of these lines in the config file. Max allow IPBYPASS directives is 100
HOP	This option has one parameter, which specifies the first hop that Declude JunkMail should look at. By default, it is set to 0 (the IMail server). This option should normally not be used (so the default setting of 0 will be used). In its place, the IPBYPASS option should be used.
HOPHIGH	This option has one parameter, which specifies the last hop that Declude JunkMail should look at. It is rarely used today, but was useful years ago when spammers would use a dialup connection to send mail through an open relay (in which case the dialup IP would appear in the headers, and could be blocked). The overhead of using this option (twice as many DNS lookups as using a single IP) explain why it is rarely used today.
	This option is used for debugging purposes.. It takes one parameter, "ON", which instructs Declude JunkMail to add the PID (Process ID) to the log file

PID	which instructs Declude JunkMail to add the PID (Process ID) to the log file entries. With this, if a process hangs, it is possible to find all the log file entries pertaining to the process that hung.
PIDDEBUG	This option is used for debugging purposes. It takes one parameter, "ON", which instructs Declude JunkMail to create separate debug log files (which get saved in the spool directory, with the pid number and a ".pid" extension, such as \spool\1242.pid). This allows us to get debug information on a hung process, without the customer having to use LOGLEVEL DEBUG until the problem occurs again.
SWITCHRECIP	This option is rarely used. It takes one parameter, "ON", which instructs Declude JunkMail to use the intended recipient where the actual recipient would normally be used, and vice versa. Customers must use this at their own risk, as there could be unintended side effects. This is normally used if people want per-user settings for aliases (as Declude JunkMail will normally look at the E-mail address the alias points to).
LOOSENSPAMHEADERS	This option has one parameter, "ON", which instructs Declude JunkMail to change the SPAMHEADERS test so that it will not be triggered on E-mails that have no Message-ID: header. This option is not recommended, as that is one of the most useful parts of the SPAMHEADERS test (but also the one that causes the most false positives).
DAISYCHAIN	This option is used to allow other programs to share the hook that Declude uses with IMail. It takes one parameter, the path/name of the executable that Declude should call. If this option is used, Declude will call the program when Declude has finished scanning the E-mail. The program is called in exactly the same way that IMail would call it.
DECODE	This option has one parameter, OFF, which specifies that Declude JunkMail should not attempt to do any message decoding (such as MIME decoding and removing HTML tags). This saves a bit of CPU time, but makes filters less effective.
DOSENDERACTIONS	This option has one parameter, ON, which indicates that Declude JunkMail should use sender actions. When enabled, Declude JunkMail will look for per-user/per-domain settings for the sender of an E-mail. This option is not widely used.
DNS	This option has one parameter, which specifies the DNS server to use. The default is to use the first DNS server listed in the IMail SMTP settings. Declude JunkMail will only use a single DNS server (since multiple processes cannot effectively communicate to each other if one of multiple DNS servers are down). This option is rarely used.
HIDETESTS	This option lists tests that Declude JunkMail should not include in the X-Spam-Tests-Failed: header. This option takes one parameter, which is a list of tests separated by spaces and/or tabs. This is used for spam tests that aren't real spam tests (such as IPNOTINMX and NOLEGITCONTENT), to prevent end users from thinking there is a problem with E-mails that have no problem.
PREWHITELIST	This option takes one parameter, ON, which indicates that Declude JunkMail should try to run whitelists before tests are run. If the E-mail is whitelisted, the tests should not be run. **Note:** [1] not all whitelists will be run this way, in which case the E-mail will be whitelisted but the tests will be run. [2] some people do not want this option enabled (to ensure that external tests are run on legitimate mail, too).
WHITELIST	This option allows users to whitelist E-mails. It takes two parameters, a whitelist type and the data to whitelist on (the IP address, E-mail address, etc.). Declude JunkMail looks at up to the first 64 characters of the data to whitelist on. There can be up to 200 of these lines in the config file. Allow Types: **FROM** **IP** **ANYWHERE** **TO** **TODOMAIN** **HABEAS** **REVDNS** **HELO** **SUBJECT** **AUTH**
AUTOWHITELIST	This option takes one parameter, "ON", which instructs Declude JunkMail to use its "autowhitelist" feature. This feature will check the web messaging address books of the recipients, to see if the sender is listed in any of them. If so, the E-mail will be whitelisted.
OUTBOUNDSCANNINGSPAM	This option takes two parameters, "ON" or "OFF". Spam checking for outbound email can be turned on/ off easily with this directive.
INBOUNDSCANNINGSPAM	This option takes two parameters, "ON" or "OFF". Spam checking for inbound email can be turned on/ off easily with this directive.
ZEROHOUR	This directive is used for CommTouch Zero-Hour Virus Protection and Recurrent Pattern Detection Technology. If you are subscribed to Declude for the CommTouch add-in, to enable, add/use the ZEROHOUR directive in the global.cfg file to control the weight associated with this test.
DOMAINWHITELISTS	This option has one parameter, ON, which indicates that Declude JunkMail should use domain whitelists. When enabled, Declude JunkMail looks for a \Declude\example.com\whitelist.txt file.

Pre-Defined Declude Tests

Declude comes with a variety of tests already defined for you. It is also possible to define new tests as they come out, or create tests of your own.

Test Name	Description
[DNS-based]	There are **over 50 different "ip4r" format DNS tests** available; click the link to the left for more information on tests not listed below.
BADHEADERS	This test checks the E-mail for illegal headers that are common in spam, but not common in legitimate E-mail. This test can catch about 50% of all spam, with the only false positives being mail that comes from broken mail clients. This is a very good test to use.
BASE64	This test will catch E-mail that uses MIME "base64" encoding for text or HTML segments. Using base64 encoding in these segments is becoming common in spam, as it allows spammers to bypass most filtering systems. However, there is no advantage for legitimate mail to be sent this way (worse, it ends up causing the size of the E-mail to be greater). Very few legitimate E-mails will be caught by this test.
BCC	This test will catch E-mail that has a lot of local recipients that are not listed in the E-mail headers. This test is normally only used in advanced setups, as most mailing list E-mail has many recipients not listed in the headers.
BITMASK	This is a type of external test that allows multiple test results to be returned by a single value. An example: ESPAM bitmask 0 "[drive]\[path]\execfile.exe" 0 0 ESPAM-URIBL bitmask 1 "ESPAM" 8 0 ESPAM-PHISH bitmask 2 "ESPAM" 4 0 ESPAM-BULK bitmask 4 "ESPAM" 6 0 The first line with a bitmask 0 defines the master test, which must contain the complete path to the executable. The actual subtests define the bits of the values that will be analyzed when the executable ends. The value following the bitmask directive is the bit value, not the bit position. Not all bits have to be used. After the bit value is the name of the master test of which these subtests are a part. The subtests must be contiguous and must immediately follow the master test. If the executable returns a value of 5, it would mean that the email failed both the first and the third tests.
BYPASSWHITELIST	This optional test instructs Declude to bypass any whitelisting for E-mails with at least a specific number of recipients and at least a specific weight. For example, you could define a test with the following line in the global.cfg file: BYPASSWHITELIST bypasswhitelist 60 5 0 0. The 60 refers to the weight the E-mail must reach, and the 5 refers to the minimum number of recipients. In this case, it would attempt to bypass the whitelisting for E-mail with 5 or more recipients and a weight of 60 or higher.
CATCHALLMAILS	This one isn't really a test. Declude will mark all E-mail as spam if you use the CATCHALLMAILS test. This might be useful if you wanted to add a footer to all E-mails in a certain domain, for example.
CMDSPACE	The CMDSPACE test looks for a technical violation of the RFCs. This test works very well because it catches about half of all spam, while no legitimate mail servers fail this test. The one drawback is that some mail clients will fail this test, so the test is most useful if you whitelist your own users (see the "WHITELIST AUTH" option), or do not have very strict anti-spam settings.
COMMENTS	The COMMENTS test will catch spam that uses HTML comments to bypass filters. It is a very effective test, since it will not catch standard comments that occasionally appear in legitimate bulk mail; it only catches comments that are designed to bypass filters.
CONTSPACES	This optional test will tell Declude to test to see if an E-mail has a specific number of continuous spaces in the subject. For example, you could define a test with the following line in the global.cfg file: "CONTSPACES contspaces 5 x 0 0", which would be triggered for E-mail with more than 5 continuous spaces in the subject.
DNSBL	The "dnsbl" test type is used to support future DNS-based spam databases, that use something other than the IP address (ip4r) or return address (rhsbl) to detect spam.
DOW	This optional test will tell Declude to test to see if an E-mail arrived during a specific day of the week. For example, you could define a test with the following line in the global.cfg file: "DOW dow 1 5 0 0", which would be triggered for E-mail that came in between Monday (1) and Friday (5).
EXTERNAL	The "external" test type will let Declude work with other anti-spam programs, such as Message Sniffer
FROMNOMATCH	Available in Declude version 3.1 and Declude 4.x or later. This test type, checks the sender of the message in the envelope and compares it to the sender specified in the FROM: line in the header of the message. If the sender in the envelope and the FROM: line in the header do not match the test is triggered. This test should not be weighted to high as many legitimate bulk mail newsletters, email lists, notifications and email being forwarded from another email system will fail this test.
FILTER	The "filter" test type will let you create your filters that can work with Declude's actions. See the "Filtering" section of the manual for more details.
HELOBOGUS	This test will detect bogus (non-RFC-compliant) "HELO/EHLO" data. When another mail server connects to yours, it will identify itself using an SMTP command (either "HELO" or "EHLO"). It is required to send a valid host name. However, spammers (and a few poorly designed mail servers) will occasionally not send a valid host name, which will trigger this test.
HOUR	This optional test will tell Declude to test to see if an E-mail arrived during a specific range of hours. For example, you could define a test with the following line in the global.cfg file: "HOUR hour 9 16 0 0", which would be triggered for E-mail that came in

	between 9:00AM and 4:00PM (16:00).
IPNOTINMX	This test should NOT be used to detect spam! It will be triggered when an E-mail is sent from an IP address that is not in its MX record. Although this test will catch a lot of spam (perhaps 80%), it will also catch a lot of legitimate mail (as quite a few larger mailers will send their mail through a different mail server than they use to receive mail). What this test is good for is helping reduce false positives. By default, Declude will *subtract* several points from the weighting system when an E-mail does *not* fail this test (which is very different from the way a spam test normally works).
MAILFROM	This test checks the SMTP envelope "Mail From:" address (which should be the sender of the E-mail) and makes sure that the domain name it is coming from is valid. This way, if mail is sent from "user@$$$success$$$.com", it will get caught (since "$$$success$$$.com" is not a valid domain).
NOLEGITCONTENT	This test should NOT be used to detect spam! It will be triggered Declude does not detect any legitimate content in an E-mail. Note that a lot of legitimate E-mail will fail this test, but almost all spam will fail it. Like the IPNOTINMX test, this test is good for helping reduce false positives. By default, Declude will *subtract* several points from the weighting system when an E-mail does *not* fail this test (which is very different from the way a spam test normally works).
NONENGLISH	The NONENGLISH test will catch a lot of E-mail that is in languages other than English. If your organization does not receive any E-mail in languages other than English, this test may be useful, as it will catch spam in Japanese, Chinese, Taiwanese, Korean, and several other languages common in spam.
PERCENT	This test will catch all mail with "To:" addresses that contain a percent sign. The percent sign indicates an outdated routing method that can be used by spammers to bypass closed relays.
REVDNS	This test will check to see if the remote mail server (or client) has a reverse DNS entry. If not, it will fail this test. All Internet hosts are required to have a reverse DNS entry, although most do not. Most mail servers do have the required reverse DNS entry, but there are still large numbers that do not, so it is likely that this test will catch a lot of legitimate mail. A warning in the headers might be appropriate for this test.
ROUTING	This test will analyze the route that an E-mail takes, and look for highly inefficient routing that is very common in spam. For example, an E-mail might get caught if it is sent from a dialup in the U.S. to another account in the U.S., but is routed through a server in China, but not if it goes from a mail server in China directly to a U.S. mail server. This may occasionally produce false positives, especially if a mailing list is hosted outside of the United States. This test will probably not work well if your mail server is located outside of the United States.
SIZE	Available in Declude version 3.1 and Declude 4.x or later. This test type, checks the message size. The size is specified in KB as in the example above 500. If the message reaches the size specified or greater then the test is triggered. The test could be used multiple times in a scaled set up as in the example below. SIZE-500KB size 500 x -1 0 SIZE-750KB size 750 x -2 0 SIZE-1MB size 1000 x -3 0 Another way this test can be used by ISP's is to prevent large files being sent to dial-up customers Mail Clients. To do this you would use a per-user configuration with the test ACTION set to MAILBOX Large in your user.junkmail file, where large emails would be redirected to the Mail Servers Web Account Folder rather than be downloaded. SIZE-1MB size 1000 x 0 0
SPAMHEADERS	This test checks the E-mail for headers that are common in spam, but not common in legitimate E-mail. This test is very similar to the BADHEADERS test, except the problems this test looks for are not RFC violations, so there's a good chance the test will catch a small amount of legitimate E-mail (typically mail sent from mail clients written by webmasters rather than programmers).
SPAMDOMAINS	This test will catch E-mail that is not coming from a mail server that it should be coming from. This test will *only* work if you set up a file listing domains that you wish to be included in this test. Specifically, it will check the return address of the E-mail, and then check to see if the reverse DNS entry of the IP that the E-mail was sent from contains the domain name. If not, the E-mail fails the test. For example, if "hotmail.com" is listed in the **MAILSERVER**\Declude\spamdomains.txt file, then an E-mail coming from "law2.hotmail.com" would not fail the test, but an E-mail from "mail.example.ru" would fail the test.
SPFFAIL	This test will be triggered if an E-mail fails **SPF** Note that it will not be triggered for E-mail that has other problems (no SPF record, unknown results from the SPF record, etc.). So any E-mail failing the SPFFAIL test is E-mail that is not authorized per the administrator of the domain the E-mail is being sent from.
SPFPASS	This test will be triggered if an E-mail passes **SPF** Note that normally no weight should be added to the E-mail for triggering this test, as it indicates that the E-mail came from an IP that the domain it was sent from allows mail to be sent from.
SUBJECTCHARS	The "subjectchars" test type will catch E-mail that has a certain number of characters in the subject. This test is normally used only in very advanced setups.
SUBJECTSPACES	The "subjectspaces" test type will catch E-mail that has a certain number of spaces in the subject. This test is normally used only in very advanced setups.
WEIGHT10	This test will catch E-mail that has a total "weight" of at least 10. This will occur if the E-mail fails several different spam tests.
	This test will catch E-mail that has a total "weight" of at least 20. This will occur if the

WEIGHT20	E-mail fails a number of different spam tests. Although less spam will fail the WEIGHT20 test than the WEIGHT10 test, the WEIGHT20 test will be less likely to have false positives.

Declude.cfg

NOTE: As the declude.cfg file is read in when the decludproc service starts any changes made to the Declude.cfg file do require a restart of the Decludeproc service.

THREADS

This number indicates the maximum allowed threads which the decludeproc service can spawn to process emails. More threads does not always mean more performance. Performance can vary due to server configuration, CPU load, available memory, email traffic, the suggested THREADS is 25 per 1 GHZ CPU. To find peak performance increase your threads so that your CPU usage bounces to the 100% mark and down again. If your CPU is pegged at 100% try reduce the threads by increments of 5 each time till you see the desired result.

If you are running a dual processor or dual core 2.4 Ghz or more Decludeproc can easily run 200 threads.

THREADS 15

WAITFORMAIL

Defined in milliseconds eg. 5000 = 5 seconds this can be changed to set the wait time that decludeproc will wait before checking the \proc directory once empty for new messages. Do not set this value to low (lower than 1000) as this will cause unessecary use of resources

WAITFORMAIL 5000

WAITFORTHREADS

Defined in milliseconds eg. 1500 = 1.5 seconds this can be changed so that when the maximum threads are in use this time specifics the wait before checking to launch more threads.

WAITFORTHREADS 1500

WAITBETWEENTHREADS

Defined in milliseconds eg. 1 = 1 millisecond The time to wait between spawning one thread and starting to process another thread.

WAITBETWEENTHREADS 1

INVITEFIX

Fix for Outlook meeting requests appearing as text only.

INVITEFIX ON

POSTINIFIX (4.10.42)

Postini is a large managed email service which amend the header structure. The Postini fix helps Declude correctly identify Postini headers.

POSTINIFIX ON

WINSOCKCLEANUP

Fix for some Imail customers having issues related to their network stack causing loss of functionality for basic network operations

WINSOCKCLEANUP ON

AUTOREVIEW

If the decludeproc service is unexpectedly stopped eg. server reboot etc email in the \work directory is moved to the \review directory. With this directive on email in the \review directory is automatically moved to the \proc directory when the service starts or when the proc directory is empty.

WARNING: If the reason for the unexpected stop of the declueproc service was due to a badly formed email this would cause a loop.

AUTOREVIEW ON

AVGUPDATEFREQHRS

Provides the ability to configure the built-in AVG virus signature update interval which checks for updates. Defined in hours, minimum is 1 hour

AVGUPDATEFREQHRS 23

BANCHARSET

Will quarantine messages using specified character sets in the \spool\charset directory

BANCHARSET iso-2022-jp
BANCHARSET koi8-r

CharsetFriendlyName	Preferred Charset Label	Aliases
Arabic (ASMO 708)	ASMO-708	
Arabic (DOS)	DOS-720	
Arabic (ISO)	iso-8859-6	arabic, csISOLatinArabic, ECMA-114, ISO_8859-6, ISO_8859-6:1987, iso-ir-127
Arabic (Mac)	x-mac-arabic	
Arabic (Windows)	windows-1256	cp1256
Baltic (DOS)	ibm775	CP500
Baltic (ISO)	iso-8859-4	csISOLatin4, ISO_8859-4, ISO_8859-4:1988, iso-ir-110, l4, latin4
Baltic (Windows)	windows-1257	
Central European (DOS)	ibm852	cp852
Central European (ISO)	iso-8859-2	csISOLatin2, iso_8859-2, iso_8859-2:1987, iso8859-2, iso-ir-101, l2, latin2
Central European (Mac)	x-mac-ce	
Central European (Windows)	windows-1250	x-cp1250
Chinese Simplified (EUC)	EUC-CN	x-euc-cn
Chinese Simplified (GB2312)	gb2312	chinese, CN-GB, csGB2312, csGB231280, csISO58GB231280, GB_2312-80, GB231280, GB2312-80, GBK, iso-ir-58
Chinese Simplified (HZ)	hz-gb-2312	
Chinese Simplified (Mac)	x-mac-chinesesimp	
Chinese Traditional (Big5)	big5	cn-big5, csbig5, x-x-big5
Chinese Traditional (CNS)	x-Chinese-CNS	
Chinese Traditional (Eten)	x-Chinese-Eten	
Chinese Traditional (Mac)	x-mac-chinesetrad	
Cyrillic (DOS)	cp866	ibm866
Cyrillic (ISO)	iso-8859-5	csISOLatin5, csISOLatinCyrillic, cyrillic, ISO_8859-5, ISO_8859-5:1988, iso-ir-144, l5
Cyrillic (KOI8-R)	koi8-r	csKOI8R, koi, koi8, koi8r
Cyrillic (KOI8-U)	koi8-u	koi8-ru
Cyrillic (Mac)	x-mac-cyrillic	
Cyrillic (Windows)	windows-1251	x-cp1251
Europa	x-Europa	
German (IA5)	x-IA5-German	
Greek (DOS)	ibm737	
Greek (ISO)	iso-8859-7	csISOLatinGreek, ECMA-118, ELOT_928, greek, greek8, ISO_8859-7, ISO_8859-7:1987, iso-ir-126
Greek (Mac)	x-mac-greek	
Greek (Windows)	windows-1253	
Greek, Modern (DOS)	ibm869	
Hebrew (DOS)	DOS-862	
Hebrew (ISO-Logical)	iso-8859-8-i	logical
Hebrew (ISO-Visual)	iso-8859-8	csISOLatinHebrew, hebrew, ISO_8859-8, ISO_8859-8:1988, ISO-8859-8, iso-ir-138, visual
Hebrew (Mac)	x-mac-hebrew	
Hebrew (Windows)	windows-1255	ISO_8859-8-I, ISO-8859-8, visual
IBM EBCDIC (Arabic)	x-EBCDIC-Arabic	
IBM EBCDIC (Cyrillic Russian)	x-EBCDIC-CyrillicRussian	
IBM EBCDIC (Cyrillic Serbian-Bulgarian)	x-EBCDIC-CyrillicSerbianBulgarian	
IBM EBCDIC (Denmark-Norway)	x-EBCDIC-DenmarkNorway	
IBM EBCDIC (Denmark-Norway-Euro)	x-ebcdic-denmarknorway-euro	
IBM EBCDIC (Finland-Sweden)	x-EBCDIC-FinlandSweden	
IBM EBCDIC (Finland-Sweden-Euro)	x-ebcdic-finlandsweden-euro	
IBM EBCDIC (Finland	x-ebcdic-finlandsweden	

IBM EBCDIC (Finland-Sweden-Euro)	x-ebcdic-finlandsweden-euro	X-EBCDIC-France
IBM EBCDIC (France-Euro)	x-ebcdic-france-euro	
IBM EBCDIC (Germany)	x-EBCDIC-Germany	
IBM EBCDIC (Germany-Euro)	x-ebcdic-germany-euro	
IBM EBCDIC (Greek Modern)	x-EBCDIC-GreekModern	
IBM EBCDIC (Greek)	x-EBCDIC-Greek	
IBM EBCDIC (Hebrew)	x-EBCDIC-Hebrew	
IBM EBCDIC (Icelandic)	x-EBCDIC-Icelandic	
IBM EBCDIC (Icelandic-Euro)	x-ebcdic-icelandic-euro	
IBM EBCDIC (International-Euro)	x-ebcdic-international-euro	
IBM EBCDIC (Italy)	x-EBCDIC-Italy	
IBM EBCDIC (Italy-Euro)	x-ebcdic-italy-euro	
IBM EBCDIC (Japanese and Japanese Katakana)	x-EBCDIC-JapaneseAndKana	
IBM EBCDIC (Japanese and Japanese-Latin)	x-EBCDIC-JapaneseAndJapaneseLatin	
IBM EBCDIC (Japanese and US-Canada)	x-EBCDIC-JapaneseAndUSCanada	
IBM EBCDIC (Japanese katakana)	x-EBCDIC-JapaneseKatakana	
IBM EBCDIC (Korean and Korean Extended)	x-EBCDIC-KoreanAndKoreanExtended	
IBM EBCDIC (Korean Extended)	x-EBCDIC-KoreanExtended	
IBM EBCDIC (Multilingual Latin-2)	CP870	
IBM EBCDIC (Simplified Chinese)	x-EBCDIC-SimplifiedChinese	
IBM EBCDIC (Spain)	X-EBCDIC-Spain	
IBM EBCDIC (Spain-Euro)	x-ebcdic-spain-euro	
IBM EBCDIC (Thai)	x-EBCDIC-Thai	
IBM EBCDIC (Traditional Chinese)	x-EBCDIC-TraditionalChinese	
IBM EBCDIC (Turkish Latin-5)	CP1026	
IBM EBCDIC (Turkish)	x-EBCDIC-Turkish	
IBM EBCDIC (UK)	x-EBCDIC-UK	
IBM EBCDIC (UK-Euro)	x-ebcdic-uk-euro	
IBM EBCDIC (US-Canada)	ebcdic-cp-us	
IBM EBCDIC (US-Canada-Euro)	x-ebcdic-cp-us-euro	
Icelandic (DOS)	ibm861	
Icelandic (Mac)	x-mac-icelandic	
ISCII Assamese	x-iscii-as	
ISCII Bengali	x-iscii-be	
ISCII Devanagari	x-iscii-de	
ISCII Gujarathi	x-iscii-gu	
ISCII Kannada	x-iscii-ka	
ISCII Malayalam	x-iscii-ma	
ISCII Oriya	x-iscii-or	
ISCII Panjabi	x-iscii-pa	
ISCII Tamil	x-iscii-ta	
ISCII Telugu	x-iscii-te	
Japanese (EUC)	euc-jp	csEUCPkdFmtJapanese, Extended_UNIX_Code_Packed_Format_for_Japanese, x-euc, x-euc-jp
Japanese (JIS)	iso-2022-jp	
Japanese (JIS-Allow 1 byte Kana - SO/SI)	iso-2022-jp	_iso-2022-jp$SIO
Japanese (JIS-Allow 1 byte Kana)	csISO2022JP	_iso-2022-jp
Japanese (Mac)	x-mac-japanese	

Japanese (Shift-JIS)	shift_jis	csShiftJIS, csWindows31J, ms_Kanji, shift-jis, x-ms-cp932, x-sjis
Korean	ks_c_5601-1987	csKSC56011987, euc-kr, iso-ir-149, korean, ks_c_5601, ks_c_5601_1987, ks_c_5601-1989, KSC_5601, KSC5601
Korean (EUC)	euc-kr	csEUCKR
Korean (ISO)	iso-2022-kr	csISO2022KR
Korean (Johab)	Johab	
Korean (Mac)	x-mac-korean	
Latin 3 (ISO)	iso-8859-3	csISO, Latin3, ISO_8859-3, ISO_8859-3:1988, iso-ir-109, l3, latin3
Latin 9 (ISO)	iso-8859-15	csISO, Latin9, ISO_8859-15, l9, latin9
Norwegian (IA5)	x-IA5-Norwegian	
OEM United States	IBM437	437, cp437, csPC8, CodePage437
Swedish (IA5)	x-IA5-Swedish	
Thai (Windows)	windows-874	DOS-874, iso-8859-11, TIS-620
Turkish (DOS)	ibm857	
Turkish (ISO)	iso-8859-9	csISO, Latin5, ISO_8859-9, ISO_8859-9:1989, iso-ir-148, l5, latin5
Turkish (Mac)	x-mac-turkish	
Turkish (Windows)	windows-1254	ISO_8859-9, ISO_8859-9:1989, iso-8859-9, iso-ir-148, latin5
Unicode	unicode	utf-16
Unicode (Big-Endian)	unicodeFFFE	
Unicode (UTF-7)	utf-7	csUnicode11UTF7, unicode-1-1-utf-7, x-unicode-2-0-utf-7
Unicode (UTF-8)	utf-8	unicode-1-1-utf-8, unicode-2-0-utf-8, x-unicode-2-0-utf-8
US-ASCII	us-ascii	ANSI_X3.4-1968, ANSI_X3.4-1986, ascii, cp367, csASCII, IBM367, ISO_646.irv:1991, ISO646-US, iso-ir-6us
Vietnamese (Windows)	windows-1258	
Western European (DOS)	ibm850	
Western European (IA5)	x-IA5	
Western European (ISO)	iso-8859-1	cp819, csISO, Latin1, ibm819, iso_8859-1, iso_8859-1:1987, iso8859-1, iso-ir-100, l1, latin1
Western European (Mac)	macintosh	
Western European (Windows)	Windows-1252	ANSI_X3.4-1968, ANSI_X3.4-1986, ascii, cp367, cp819, csASCII, IBM367, ibm819, ISO_646.irv:1991, iso_8859-1, iso_8859-1:1987, ISO646-US, iso8859-1, iso-8859-1, iso-ir-100, iso-ir-6, latin1, us, us-ascii, x-ansi

CONCATENATELOGS

Located in the Declude.cfg file. This feature will lessen the disk stress on the dec#####.log file by creating individual log files per message, and then appending them to the dec#####.log file in a batch.

CONCATENATELOGS ON

CONCATENATELOGSTHRESHOLD

Located in the Declude.cfg file. This is how many separate message file logs should be created before appending the seperate loges to the dec#####.log file in a batch.

CONCATENATELOGSTHRESHOLD 10

KEEPINDIVIDUALLOGS

Located in the Declude.cfg file. This determines whether to keep the individual seperate log files

KEEPINDIVIDUALLOGS ON

HOMEREGION (4.10.53)

Allow the user to specify HOMEREGION specifically designed for users outside of North America and applies to the ROUTING test. Add one of the following depending on your region to the declude.cfg (North America is the default)

HOMEREGION Afrinic

HOMEREGION Afrinic
HOMEREGION Apnic
HOMEREGION Anic
HOMEREGION Lacnic
HOMEREGION Ripe_ncc

More information on your specific country can be found here

Filtering

The Declude JunkMail filters, can count towards the weighting system, and you can use actions of your choice.
Click here for quick start to use filters

WARNING: Filters (in Declude, IMail, SmarterMail, or anywhere else) can be very dangerous if you are not careful.

Filtering for swear words can catch unrelated words:

- assassin
- document
- chardonnay
- Mr. Hitchcock

Step 1
Define the test. Add a line to the global.cfg file in the following format:

```
MYFILTER    filter    C:\MAILSERVER\Declude\filters\myfilter.txt    x    5    0
```

This will define a test named MYFILTER, that will be a filter using your filter file at C:**MAILSERVER**\Declude\filters\myfilter.txt.

A weight of 5 will be added to every E-mail that is caught by your filter.

Step 2
Create the filter file (myfilter.txt in the example above). Each line contains one filter, in the following format:

LOCATION WEIGHT FILTERTYPE FILTERTEXT

Options for Location
This is where where the filter will be searching:

BODY
HEADERS
HELO
MAILFROM
REMOTEIP
REVDNS
ALLRECIPS
ANYWHERE
TESTSFAILED
SUBJECT

Options for Weight
The weight to be added to the E-mail if the filter matches. Several options can be used besides just a weight value.

END

To stop processing of the test at that point

```
BODY    END    CONTAINS    password
```

STOPALLTESTS

If you want to stop all further filters (not just the current filter), preventing further processing of this filter or any other filters after it.

```
BODY    STOPALLTESTS    CONTAINS    Evil Spammer
```

WHITELIST

If you want to whitelist an email based on a filter line.

```
SUBJECT    WHITELIST    CONTAINS    password
```
Automatically whitelists any E-mails containing the word "password" in the subject.

Options for FilterType

CONTAINS
STARTSWITH
ENDSWITH
NOTCONTAINS
NOTENDSWITH
NOTIS
IS
CIDR

Options for FilterText

The text being searched for (case insensitive, so "hello" will match both "hello" and "hELLo").

Examples
Looking for HELO/EHLO text that contains "localhost" in it (and if it does, a weight of 8 will be added to the weight of the E-mail)

```
HELO 8 CONTAINS localhost
```

Looking for an E-mail that contains "enlarge" in the Subject: then add 3 to the weight of the E-mail if there is match.

```
SUBJECT 3 CONTAINS enlarge
```

Looking for a return address beginning with "$$$success$$$@" then add 3 to the weight of the E-mail if there is a match.

```
MAILFROM 3 CONTAINS $$$success$$$@
```

Looking for "To unsubscribe, click here" in BODY then add 3 to the weight of the E-mail if there is a match.

```
BODY 3 CONTAINS To unsubscribe, click here
```

NOTE: These weights are **in addition to** whatever action you have set for the test, so if you have the following in your $default$.JunkMail file:

```
MYFILTER WARN X-Warning: This E-mail was filtered.
WEIGHT10 HOLD
```

E-mail with "$domain" in the HELO/EHLO text would be held and have a warning in the headers, and be held (since the MYFILTER test was defined to have a weight of 5, and the "$domain" in the HELO/EHLO added 8 to the weight).

You can also use negative weights, such as:

```
REVDNS -5 CONTAINS .yahoo.com
```

There is no limit to the number of lines in a filter file.

Advanced Filtering
There are several options to help save CPU usage if you have lots of filters.

STOPATFIRSTHIT

A single line located at the top of your filter file, which instructs Declude JunkMail to stop the processing of the filter as soon as the first hit occurs in the filter.

SKIPIFWEIGHT

A single line located at the top of your filter file, which will instruct Declude JunkMail to skip the test if a certain weight is reached (either when the test is run, or at any point during processing) At the top of the filter file (where 20 is the weight to stop processing at.)

```
SKIPIFWEIGHT 20
```

MINWEIGHTTOFAIL

This will instruct Declude JunkMail not to trigger the test unless a minimum weight is reached. Would require that the filter add at least 4 points to the weight of the E-mail in order for the test to be triggered).

```
MINWEIGHTTTOAIL 4
```

MINWEIGHT & MAXWEIGHT

You can also use MINWEIGHT and MAXWEIGHT to specify minimum and/or maximum weights that the test can add. Would make sure that the filter did not add more than 20 points to the weight of the E-mail.

```
MAXWEIGHT 20
MINWEIGHT 5
```

PCRE

Regular Expression Filtering

Declude 4.3.40 or later includes the ability to use Regular Expressions within the filters. Regular expressions are used to recognize patterns within emails. They evaluate the text of an email and return either a match or nomatch. That is, either the expression correctly describes the text of the email or it doesn't. This enables you to specify a filter to easily identify certain kinds of email text or patterns.

PCRE (Perl Compatible Regular Expression) is the library that is used with Declude. PCRE is much faster than regular pattern matching within Declude filters. You do NOT require Perl to be installed on the server to use these regular expressions.

The syntax within Declude filters is the following:

LOCATION WEIGHT PCRE EXPRESSION

#VIAGRA
BODY 5 PCRE (?i:v\s*[i!]+\s*a\s*g\s*r\s*a)

For more information on syntax please visit http://www.pcre.org/pcre.txt

---

Per-Domain Configuration (JunkMail)

Declude allows you to have different settings for each domain that you have. These will let you have different actions for each domain.

In order to do this, you first need to create a subdirectory off of the Declude directory, with the same name as the domain you wish to change. For example, to add a per-domain configuration for "example.com", you would create the directory **MAILSERVER**\Declude\example.com. Note that this needs to be the **official domain name, not a domain alias** (so if you have a domain "mail.example.com" with "example.com" as an alias, the directory should be "**MAILSERVER**\Declude\mail.example.com\"). The exception is that if you have a user alias, the domain you use in the alias will take priority (for example, if the alias is "sales" that points to "salesman@example.com", you would need to use the directory "example.com").

It may be necessary to use two different directories, if you have users aliases pointing to domain aliases (a quirk in IMail).

The next step is to copy the $default$.JunkMail file into that directory. Then, edit that file to reflect the settings you want for that domain.

Or, to quickly disable spam control for a specific domain, you can whitelist all mail to the domain by using the "WHITELIST TODOMAIN @example.com" setting in the global.cfg file.

NOTE: You should not delete the $default$.Junkmail file. If that file does not exist, there will be no default settings for E-mail addressed to domains that do not have their own per-domain settings.

REDIRECT

Redirecting (groups)

Another way for you to use per-domain configurations is by using redirecting, or groups. The REDIRECT command in a config file will instruct Declude JunkMail to use a different configuration file for a specific user or domain. When Declude JunkMail sees this line, if it is processing mail to @example.com, Declude JunkMail will instead use the C:**MAILSERVER**\Declude\filename.cfg file for determining the action to take on the E-mail. To use this, the $default$.Junkmail (or any of the per-user or per-domain config files) can have a line in the format:

REDIRECT@example.com C:\MAILSERVER\Declude\filename.cfg

Note that while this option can be used in any of the Declude JunkMail configuration files, it will only be used in whatever configuration file that Declude JunkMail is using for an E-mail. For example, if you have a REDIRECT line in the **MAILSERVER**\Declude\example.com\$default$.JunkMail file, Declude JunkMail won't use it for an E-mail to user@example.NET.

Per-User Configuration (JunkMail)

Declude allows you to have different settings for each user on your system. These will allow you to have different actions for each user.

First, you need to create a subdirectory off of **MAILSERVER**\Declude for the domain the user is on (if the directory doesn't yet exist). For example, if you want per-user settings for "myname@example.com", you would create the directory **MAILSERVER**\Declude\example.com.

Next, copy the $default$.Junkmail into this directory, and rename it to the users' name followed by ".JunkMail" (be sure not to overwrite the existing $default$.JunkMail file in this directory, if there is one -- it is the per-domain configuration file). For example, if you want a separate configuration for "john.doe@example.com", you would copy the $default$.JunkMail file to **MAILSERVER**\Declude\example.com\john.doe.JunkMail

Then, edit that file to reflect the settings you want for that user.

Or, to quickly disable spam control for a specific user, you can whitelist all their E-mail by using the "WHITELIST TO user@example.com" setting in the global.cfg file.

Note that you should not delete the $default$.Junkmail file. If that file does not exist, there will be no default settings for E-mail addressed to domains or users that do not have their own settings.

Declude Variables

Declude has a number of "variables" that can be used in the configuration files. These variables will be replaced with certain information; for example, if Declude sees "%REMOTEIP%" in a warning header, it will replace it with the IP address of the remote mail server. These can be used with certain actions (WARN, SUBJECT, HEADER, FOOTER), and in "bounce" messages.

Variable	Description

%AUTH%	Authenticated Sender
%ALLRECIPS%	Recipients of the E-mail
%DATE%	Today's date (MM/DD/YYYY format)
%FULLMSG%	Inserts the original E-mail (headers and body)
%HEADERS%	Inserts the headers of the E-mail.
%HEADERCODE%	Shows the code used by the BADHEADERS/SPAMHEADERS tests
%INOROUT%	"incoming" or "outgoing"
%LOCALHOST%	Local host name (a domain on your mail server)
%MAILFROM%	Sender of the E-mail
%MSGID%	Message-ID of the E-mail
%NRECIPS%	Number of recipients of this E-mail
%QUEUENAME%	Queue file name of the E-mail (IE Q1234567.SMD)
%RECIPHOST%	Host name of the recipient
%REMOTEHOST%	Remote host name (the remote domain)
%REMOTEIP%	Adds the IP address of the remote mail server
%REVDNS%	Inserts the reverse DNS entry of the remote mail server
%SENDERHOST%	Host name of the sender
%SUBJECT%	Inserts the subject of the E-mail
%TESTNAME%	The name of the test (IE "ORBZ")
%TESTDOMAIN%	The zone used by DNS-based tests (IE "relays.orbz.org")
%TESTSFAILED%	Shows a list of all the tests that the E-mail failed
%TESTSFAILEDWITHWEIGHTS%	Shows a list of all the tests that the E-mail failed, as well as the weight assigned to each test
%TIME%	Current time (HH:MM:SS format)
%VERSION%	Inserts the version of Declude that is running
%WARNING%	Inserts information from the current test that normally is seen in an X-RBL-Warning: header
%WEIGHT%	Displays the total weight of the E-mail

Weighting System (Junkmail)

Declude has a weighting system, designed to improve spam detection while minimizing false positives. It accomplishes this by assigning a weight to each test, and calculating the total weight of all tests that fail. For example, if the MAILFROM test is given a weight of 5 and the REVDNS test is given a weight of 7, an E-mail failing both tests would have a total weight of 12. The higher the weight, the more likely an E-mail is to be spam.

The default configuration files include weighting information, along with a WEIGHT10 test (which is set up to be triggered if the total weight of the E-mail is 10 or greater) and a WEIGHT20 test (which gets triggered if the total weight of the E-mail is 20 or higher).

You can add your own weight level to look for by adding a line such as the example to define a new WEIGHT15 test in the global.cfg file.:

```
WEIGHT15    weight    x    x    15    0
```

You could then add a line to the $default$.Junkmail file, which would hold any E-mail with a total weight greater than or equal to 15.

```
WEIGHT15    HOLD %DATE%
```

Weight Ranges

For more advanced usage, you can define a test that will only get triggered when a certain range of weights is reached. For example, you can have a test that will only get triggered when the total weight of the E-mail is between 10 and 20. You can define a weight range test by adding a line in the format:

```
WEIGHT15    weightrange    x    x    10    20
```

the name of the test, followed by "weightrange", two placeholders, and the low weight and high weight. This will catch any E-mail with a total weight in a range between and including 10 and 20.

Exact Weights

To catch a single weight, such as only E-mail with a weight of 10, you can use the "weightmatch" test type, by defining a test such as

```
WEIGHT10    weightmatch    x    x    10    0
```

This will catch mail with a total weight of exactly 10 (but not catch any E-mail with a weight of less than 10, or more than 10).

Negative Weights

There are some tests in Declude that should be assigned a negative weight. The first set of tests are called IP4R HAM TESTS. These tests should be assigned a negative weight because if they are triggered, it means that the senders IP is listed with the companies who administer these lists. By doing this, they are “proving” that their servers are not affiliated with spam.

Here is a list of the tests:

BONDEDSENDER - A whitelist of E-mail senders that have posted a bond to help prove that their E-mail is legitimate.

IADB - Email Senders Accreditation program available to email marketers and email senders.

MXRATE-ALLOW - This source is rated as a normally good sender.
Substantial number of allowable messages have been reported.

AHBL-EXEMPT - The AHBL Exemptions allows mail from known good sources, even if they are blacklisted elsewhere.

BGISOCWL - Bulgarian Spam Prevention System Whitelist. Designed primarily to protect isoc.bg's members from receiving Bulgarian spam; this is a WHITELIST, which lists 'good' IPs. No TXT records, missing test entry 127.0.0.2. Warning: Is not testable. The second set of negative weight tests work a bit differently from the set mentioned above. Unlike the IP4R HAM TESTS which assign a negative weight when triggered, this next set of tests assign a negative weight when they are NOT triggered. The tests are:

Other type tests includes:

IPNOTINMX - The IPNOTINMX test is good for helping reduce false positives. By default, Declude JunkMail will subtract several points from the weighting system when an email does not fail this test (which is very different from the way a spam test normally works). **WARNING:** The IPNOTINMX should NOT be used to detect spam! It will be triggered when an email is sent from an IP address that is not in its MX record. Although this test will catch a lot of spam (perhaps 80%), it will also catch a lot of legitimate mail (as quite a few larger mailers will send their mail through a different mail server than they use to receive mail).

NOLEGITCONTENT - Like the IPNOTINMX test, the NOLEGITCONTENT test is good for helping reduce false positives. By default, Declude JunkMail will subtract several points from the weighting system when an email does not fail this test (which is very different from the way a spam test normally works). **WARNING:** The NOLEGITCONTENT test should NOT be used to detect spam! It will be triggered Declude JunkMail does not detect any legitimate content in an email. **NOTE:** Some legitimate email will fail this test, but almost all spam will fail it.

FROMNOMATCH - This test type, checks the sender of the message in the envelope and compares it to the sender specified in the FROM: line in the header of the message. If the sender in the envelope and the FROM: line in the header do not match the test is triggered. This test should not be weighted to high as many legitimate bulk mail newsletters, email lists, notifications and email being forwarded from another email system will fail this test.

Testing Declude Junkmail

Making E-mail fail a test:
There are three ways to do this. First, you can send an E-mail to an account at your domain where the first line starts with "rsp set off ", and then has the name of a test. For example, "rsp set off ORDB" will trigger the ORDB test. Note that the test name is CASE SENSITIVE (ORDB not ordb). This ONLY will work if your E-mail client does NOT send HTML (which places other lines before the "rsp set off" line).

Second to make an E-mail fail a test is to use an autoresponder set up to do so. You can find some at http://www.crynwr.com/spam/, but these *only work if you subscribe to the www.mail-abuse.org tests*. You send an E-mail to one address; one reply should PASS Declude JunkMail's tests, the other one should FAIL one of the tests. Note that the E-mail you get back will be VERY MISLEADING, saying that it didn't work, whether or not it did. Also note that RBL, RSS, and DUL now require a SUBSCRIPTION (see http://www.mail-abuse.org).

Third, use the declude tools: http://tools.declude.com/

How to disable/uninstall Declude

How to disable Declude JunkMail (but leave Declude running)

To disable Declude JunkMail (but allow the core Declude code and other Declude programs you may have to continue running), simply rename the global.cfg file to global.bak. This will prevent Declude JunkMail code from running, but will still allow the core Declude code to run.

How to disable Declude in IMail (but leave Declude running)

Normally, you should never need to uninstall Declude. However, if you do need to, it is possible with one change in the registry (which will disable ALL Declude programs you may be running):

1. Stop the IMail SMTP service
2. Go to the Advanced tab in the SMTP settings in IMail Administrator, and change the "Delivery Application" option so that the part reading "declude.exe" is changed to "smtp32.exe" (for example, if it reads "C:\IMail \Declude.exe", change it to "C:\IMail\smtp32.exe"). If you are using an older version of IMail without that option, you will need to use regedit to change the HKEY_LOCAL_MACHINE\Software\Ipswitch\ IMail\Global\SendName key so that the part reading "declude.exe" is changed to "smtp32.exe"
3. Restart the IMail SMTP service
4. Copy any files from \ IMail \spool\proc to \ IMail \spool.

Next, check to make sure that incoming mail is delivered -- if not, check that registry key to make sure you didn't make a typo.

This will prevent Declude from scanning any messages. To let Declude scan messages again, just repeat the process, but change the "smtp32.exe" back to "Declude.exe", and stop/restart the IMail SMTP service.

How to disable Declude in Smartermail (but leave Declude running)

Uncheck Declude under the anti-spam administrations settings of SmarterMail.

How to uninstall Declude completely

To fully uninstall Declude, you must do the following:

1. Stop the Decludeproc service in your Microsoft services.msc console.
2. Open a command prompt and browse to the location of your decludeproc.exe 3. Type the command [decludeproc -u] hit enter.
4. The service is now unregistered, you can delete the decludeproc.exe. In IMail you will also delete the file declude.exe.
5. It is now safe to remove the \Declude directory.
6a. IMAIL ONLY - In the IMail admin under the services>advanced tab change the "default delivery application" from declude.exe to SMTP32.exe stop/start SMTP service.
6b. SMARTERMAIL ONLY - In the SM admin under the security>antispam administration tab be sure to uncheck the Declude checkbox and save settings.

Declude is now fully uninstalled and is removed from the mail flow process. We leave behind a registry key that can be safely removed if desired. That key is:
HKEY_LOCAL_MACHINE>SOFTWARE>COMPUTERIZEDHORIZONS

The following is a list of the most frequently asked questions pertaining to Declude JunkMail

How can I catch more spam?

Make sure that Declude knows about any backup mail servers or gateways that may send mail to your **MAILSERVER**. You should have an "IPBYPASS" line in your global.cfg file for each backup mail server or gateway.

Make sure that you do not have any whitelists that will allow a lot of spam through. The #1 problem with whitelisting is that people whitelist E-mail from their own domain. However, many spammers will send mail with a return address on the same domain that they are sending to, so you should not whitelist E-mail from your domain. Also, note that "WHITELIST FROM mail.com" will whitelist all E-mail from @hotmail.com (since it contains "mail.com"); instead, you would want to use "WHITELIST FROM @mail.com". One last note… it is better to whitelist the IP address of a sender instead of their email address or domain name. Spammers can easily spoof email addresses and domains, but they can't spoof IP addresses.

Make sure that you remove any dead spam tests from your global.cfg file, and check with the latest global.cfg file to see if there are new spam tests to use.

No/not enough spam is getting caught, why?

If you just installed Declude, the default settings will only add a standard X-RBL-Warning: header (the WARN action) when spam is detected. If you want to quickly start blocking some spam, you may want to try changing the "WEIGHT14 SUBJECT **SPAM**" line in the $default$.Junkmail file to "WEIGHT14 HOLD %DATE%".

We have a large selection of content filters that can be used with Declude to catch a lot more spam. You can review these filters at the following website: http://filters.declude.com. The username for the site is "filters" (without the quotes). The password is "decfilters" (without the quotes). You should probably only use 5 or 6 filters at a time, depending on the speed of your processor and amount of memory in your server. If you don't see a filter at the site that can help you, contact us at support@declude.com and we can build you custom filters for your needs.

There are a few 3rd party add-ons and plug-ins that can be used with Declude to help catch even more spam. Here is a list of the most common:

CommTouch - Based on RPD™ (Recurrent Pattern Detection) and other proprietary technologies, the Commtouch Detection Center analyzes the distribution patterns of billions of email messages per month. Based on these patterns, Commtouch identifies new malware outbreaks-as soon as they are introduced into the Internet. The result is that users are protected from emerging malware in real-time, all the time. For example, viruses are detected and blocked within minutes, hours before signatures are released. To learn more about CommTouch, visit the following link: http://www.commtouch.com/Site/Company/about.asp

Message Sniffer - Message Sniffer (SNF), from ARM Research Labs, is a high performance message scanning engine that uses advanced pattern recognition and collaborative machine learning technologies to accurately identify spam and email borne security threats (viruses, malware) at your email server or gateway (before it gets to your inbox). The engine is designed for high-speed, high-availability applications on many platforms including Windows, Linux and BSD based systems. A professionally managed rulebase is provided via subscription and is updated frequently throughout the day (24x7) by analysts and intelligent monitoring systems. Learn More.

invURIBL - invURIBL is a tool that is used to identify SPAM by extracting URI's (domain names in links) from emails and checking them against URI based blacklists. Our application extends basic URI checking functionality by incorporating features that will allow you to check the URI's IP address and name servers against DNS based blacklists. In addition, we have added a unique feature that allows you to check the URI's IP address and remote mail server against Senderbase, the world's leading email traffic monitoring network. To learn more about invURIBL, visit the following link: http://www.invariantsystems.com/invURIBL/

VSIMAGE - This tool is an External Agent for Declude that improves image spam detection capabilities. To learn more about VSIMAGE, visit the following link: http://www.vamsoft.com/vsimagespam/

I don't think that Declude JunkMail is working what should I do?

First, make sure that the \Declude\global.cfg file exists and is named "global.cfg" Stop/Restart the decludeproc

service. This will create a diagnostic file called diag.txt located in the \Declude folder that you can send to support@declude.com for assistance.

A lot of legitimate mail is being caught, why?

Most likely, you set up all or many of the spam tests to use the HOLD or DELETE action. All spam tests have flaws, and many of the spam tests are not designed to catch spam alone (but work well towards the weighting system). For example, lots of legitimate mail from poorly designed web servers will fail the SPAMHEADERS test. You should make sure to only use tests that you understand. Rather than blocking mail that fails individual tests, we recommend blocking mail that fails the WEIGHT14 test (or WEIGHT10 test, if you can deal with a bit of legitimate E-mail getting caught in exchange for more spam caught).

Why didn't Declude add the weights correctly?

Often, a customer will see that an E-mail failed certain spam tests, but has a weight lower than what they expect. For example, if an E-mail fails just the SPAMCOP test (which has a weight of 7 points), the total weight of the E-mail may be 4. This will occur if the E-mail did *not* fail certain tests that are set up with a negative weight. For example, the IPNOTINMX and NOLEGITCONTENT tests are designed to help legitimate E-mail rather than hurt spam. As a result, E-mails that fail those tests will have not have any points added to them, but E-mails that do not fail them will have points subtracted from their total weight.

Why did this E-mail get marked as spam (or deleted)?

This is a question we often receive, and since we often can't easily answer the question, we felt it would be a good idea to have a section about this in the manual.

If an E-mail is marked as spam (if it is held in the **MAILSERVER**\spool\spam directory, for example), it is because it failed one or more spam tests. So the real question is "What tests did the E-mail fail?".

The easiest way to find out is to have a line (in your global.cfg file) that says "XINHEADER X-Spam-Tests-Failed: %TESTSFAILED%.". This will place a header in the E-mail that lists the tests that failed, making it easy to determine which test(s) failed.

The other way to find out is to look at the Declude JunkMail log file. If you use the "XSPOOLNAME ON" option in the global.cfg file, it will be easy to find the entries for the E-mail in the log file. If you do not use the XSPOOLNAME ON option, you may need to look at the **MAILSERVER** SMTP log file to file the queue file name of the E-mail, and search the Declude JunkMail log file for it (minus the first character and extension; for example, if you see "Q1234567.SMD" in the **MAILSERVER** log, you would search the Declude JunkMail log for "1234567").

Now that you have found the E-mail in the log file, you know which test(s) it failed.

Why did this E-mail NOT get marked as spam?

There are three common reasons for this:

1.) The E-mail didn't fail any spam tests

2.) The E-mail failed spam test(s), but the actions you are using for those spam tests did not mark the E-mail as spam (for example, if you use the WARN action, the spam will be delivered and will seem like normal E-mail to many E-mail clients).

3.) The E-mail was **whitelisted**. If you have any WHITELIST entries in your global.cfg file, you'll need to check them all to see if they could have whitelisted the E-mail. Remember, whitelisting is a last resort.

Why did an E-mail fail the SPAMHEADERS test?

To find out, you need to find the code that Declude JunkMail assigned the E-mail (such as "40000202"). If you use the WARN action, this will appear in the E-mail headers. Otherwise, you will need to look in the log file.

You can look up the code using the "BADHEADERS lookup" at http://tools.declude.com

The most common reason an E-mail will fail the SPAMHEADERS test is because it is missing a Message-ID: header. The Message-ID: is not required in order for an E-mail to be valid, but the RFCs say that it "SHOULD" be there. "SHOULD" in RFC terminology means that the header must be there *unless* there is a good reason for it not to be there, and the consequences of it not being there are known. I can't think of a good reason for the Message-ID: header not to be present (except that it saves programming time). The consequences of not having a Message-ID: header is that the mail may or may not be delivered if it is missing.

FYI, IMail does add a Message-ID: header if there isn't one already (since IMail knows the importance of the header). So, even though you see one, it was added by IMail. The problem can usually be fixed by upgrading the software used to send the E-mail.

Why did an E-mail fail the BADHEADERS test?

To find out, you need to find the code that Declude assigned the E-mail (such as "80200202"). If you use the WARN action, this will appear in the E-mail headers. Otherwise, you will need to look in the log file.

You can look up the code using the "BADHEADERS lookup" at http://tools.declude.com. The most common reason an E-mail will fail the BADHEADERS test is because it is missing a Date: header (or has no time zone or an incorrect time zone). This is illegal, and will often cause E-mail to get "lost" on a server or mail client. Upgrading the software sending the E-mail will take care of the problem in almost all cases.

If spam gets held in the \spool\spam directory, how can I get it delivered?

IMail stores E-mails in two separate files, that both have the same name except that one begins with a "D" (which contains the actual E-mail), and one begins with a "Q" (which contains other information about the E-mail). You

need to copy both of those files (for example, "Q1234567.SMD" and "D1234567.SMD") back to the spool directory. The E-mail will get delivered automatically on the next queue run (for faster delivery, you can use "Send One" from "View Queue" in the IMail Administrator).

Smartermail stores E-mails in two separate files, that both have the same name except that one ends with a ".eml" extension (which contains the actual E-mail), and one ends with a ".hdr" extension (which contains other information about the E-mail). You need to copy both of those files (for example, "1234567.HDR" and "1234567.EML") back to the spool directory. The E-mail will get delivered automatically on the next queue run

Will gateway (store-and-forward) domains get scanned?

Yes. However, the **MAILSERVER** treats those domains as outgoing E-mail, since they are not stored locally. Therefore, the outgoing actions (from the global.cfg file) will be used. If you want to use different actions for the gateway domains, you can set up per-domain settings for the domain.

Which version of Declude am I running?

To find out, you can type "**MAILSERVER**\Decludeproc -v" from a command prompt.

Can I run Declude Virus or Declude Hijack with Declude JunkMail?

Yes. All of the Declude programs can run together on the same server. Many of our customers run multiple Declude programs on the same server.

The following is a list of troubleshooting tips pertaining to Declude

Declude completely stopped working

After An Upgrade Of Imail - This may happen after an upgrade of IMail, which may overwrite the registry entry that Declude uses. To fix the problem, goto Imail Administrator --> SMTP --> Advanced --> Delivery Application and ensure that the executable is declude.exe then stop/restart the IMail SMTP service (so it recognizes the change).

Rare Issue After An Upgrade Of Imail - Another rarer problem during an IMail upgrade (happening to about 5% of the 7.05 and 7.06 upgrades) is that the IMailupgrade may change the Official Host Name of your mailserver. To fix this, just change the Official Host Name ("Host Name" on the General tab of IMail Administrator, when "localhost" is highlighted on the left side of the screen) back to its original name.

Decludeproc crash and didn't restart or decludeproc keeps crashing and restarting every few seconds – This may happen from time to time if a badly malformed message comes into your mail server. To ensure that the decludeproc service restarts itself automatically upon a crash, go to your Windows Services and find the decludeproc service in the list. Right-click the service and go to properties. Click on the Recovery tab. Choose "Restart The Service" in all 3 pop down boxes that you see. Click Apply then OK. Also, go to your Declude directory and open your declude.cfg file. Make sure that your AUTOREVIEW directive is set to OFF. If it is not, turn it off, save and close the declude.cfg file and then restart the decludeproc service. This will prevent the malformed message from being reprocessed over and over if decludeproc crashes.

After an upgrade to Declude version 4.3.40 – When you upgrade to Declude version 4.3.40, you may see an Invalid Key or Expired Key message in the diags.txt file. If this happens, you must flush your local DNS cache and your local OS DNS cache. Here is how to do so:

Flushing the cache of a network DNS depends on the DNS server being used.

BIND8- restart the ISC Bind Service

BIND 9 - go to the Bind install directory with rndc.exe in it and type rndc flush

MSDNS- Go into the dnsmgmt console and right click on your server name. Click Clear Cache.

To flush the local OS DNS type ipconfig /dnsflush at the command prompt.

After upgrading from Declude version 1x, 2x or 3x to 4x – Versions 1.x through 3.x of Declude use codes that are placed in the global.cfg, virus.cfg and hijack.cfg file. After you upgrade to Declude 4.x, these codes are no longer needed in those files. However you still need a code to run Declude.

Code for Imail – If you're running an Imail server, you will be given a code by us to put into your declude.cfg file. You can find the code on the lower left-hand side of your account page when you log in. When you open the declude.cfg file you will see this line:

CODE [PLACE YOUR DECLUDE CODE HERE].

Remove that line completely and replace it with the following:

CODE XXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXX

Be sure to change the X's to your own code. Save and close the declude.cfg file.

Code for Smartermail – If you are running a Smartermail server, you must provide us with your Smartermail registration key to add to our system. This will act as your Declude key. You do not need to add a code to your declude.cfg file. If you are running a free version of Smartermail, you do not need to provide us with a key because free Smartermail does not come with one.

The per-user (or per-domain) settings are not working

The most likely reason for this is that the directory you are using for the per-user or per-domain settings does not match the "real" domain name. For each domain, **MAILSERVER** has one "real" domain name and sometimes

one or more aliases. If you have a domain listed in **MAILSERVER** as "host.example.com" with "example.com" as an alias, the per-user and per-domain settings should be in the **MAILSERVER**\Declude\host.example.com\ directory, not the **MAILSERVER**\Declude\example.com\ directory. Also, if a user alias is used, the account that it points to is used for the per-user settings.

Blacklisting is not working

The "fromfile" type of blacklisting checks the domain name or E-mail address that is in the "return address" (where bounce messages go; this is also the "MAIL FROM" in the SMTP envelope). This may be different than the "From:" or "Reply-To:" headers in the E-mail. If you use the "XSENDER ON" option, this address will appear in the X-Declude-Sender: header of the E-mail. Otherwise, you will need to look at the "MAIL FROM" line in the **MAILSERVER** SMTP log file to find this address.

Whitelisting is not working

The "WHITELIST FROM" type of whitelisting checks the domain name or E-mail address that is in the "return address" (where bounce messages go; this is also the "MAIL FROM" in the SMTP envelope). This may be different than the "From:" or "Reply-To:" headers in the E-mail. If you use the "XSENDER ON" option, this address will appear in the X-Declude-Sender: header of the E-mail. Otherwise, you will need to look at the "MAIL FROM" line in the **MAILSERVER** SMTP log file to find this address.

The wrong action is taken on E-mail

If you find that the wrong action is being taken on an E-mail (for example, if you see an X-RBL-Warning: header for a specific test, but you thought that E-mail failing that test should be held instead), the most likely problem is that Declude is not using the configuration file that you thought it would use. You can use "LOGLEVEL HIGH" (in the global.cfg file) to help here, as Declude will report to the log file which configuration file it is using.