Connect
Manuals
EVA Manual
Hijack Manual
Interceptor Alligate Manual
JunkMail Manual
Release Notes
Self Support
Knowledge Base
Install & Upgrade Guide
Feedback Loops
Tips & Tricks
AHBL Setup
Filter Configuration

EVA Manual

Declude EVA (Virus and Vulnerability Detection)

After Declude EVA is installed, it will intercept every E-mail that is sent or received through SMTP (for outgoing web messaging E-mails, you can have an on-access scanner scanning only the \spool\ directory). Declude EVA will decode any attachments, and save them to a file (with a file name generated by Declude, for security reasons). Then, it will create a process to run your anti-virus software. Once the anti-virus software has scanned the file, Declude EVA will take the appropriate action. By default, Declude EVA will log to Declude\Logs\vir####.log every E-mail that it scans. It will report in there any viruses that are caught. Any viruses are placed into a quarantine directory.

Declude EVA 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 only 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.

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.

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.

NOTES

- You can use the Test Mail Sender at http://tools.declude.com
- When making configuration changes to Declude EVA, you do *not* need to stop/restart any services or reboot. Declude EVA detects the changes automatically.

EVA 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\vir####.log") or a hard-coded path ("D:\MAILSERVER\Declude\Logs\vir####.log").

LOGFILE Declude\Logs\vir####.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).

DOEVENTLOG

Will turn on event logging. All log file entries for an E-mail will be saved to the event log together. This feature is for Somix Logalot, which can't read standard log files, but can read the event logs.

DOEVENTLOG ON

Basic Configuration

F-Prot Help

If you are using the F-Prot virus scanner, Declude Virus uses the F-Prot command line scanner, which is included in both their DOS and Windows version (the command line scanner in both is identical). The Windows version also includes a scheduler for automated downloading of updates, which can be very useful.

Windows Version

When installing the Windows version, you need to make sure that it does not install the "RealTime Protector" (their on-access scanner), since it can interfere with Declude's operation. To prevent it from installing, do a Full Install, and unselect the "RealTime Protector".

DOS Version

When installing the DOS version, you need to make sure to delete the F-Prot.PIF file that F-Prot installs (it is installed in the same directory as F-Prot.EXE). Note that if you are using Windows Explorer and have it set to hide file extensions, you may need to enable the file extensions in order to distinguish the F-Prot.PIF from the F-Prot.EXE file.

Configuration

See the next Basic Configuration section below for the recommended settings for F-Prot.

McAfee Help

McAfee Versions

You can use either McAfee's VirusScan product or their NetShield product with Declude EVA. There are several other McAfee products that include VirusScan or NetShield, those will work as well.

If you are running Windows NT Server or Windows 2000 Server, and use VirusScan, you will need to use the MultiPlatform version of VirusScan (this is included in their VirusScan Security Suite). The standard version of VirusScan will not install on NT/2000 Server. It is very difficult to find their MultiPlatform version of VirusScan online (and their sales reps will try very hard to get you to buy a more expensive program).

Configuration

See the next Basic Configuration section below for the recommended settings for McAfee. If you use NetShield, you may need to do a Full Install in order to have the command line virus scanner installed. With VirusScan, you may need to run the "Install.bat" program (possibly in the CMD directory on the CD-ROM). Also, make sure that you use **SCAN.EXE** in the Declude Virus SCANFILE configuration option, and not SCAN32.EXE (which is not a command line scanner). McAfee may require a Full Install to install the scan.exe file; it may install into a directory other than the one you tell McAfee to install to.

Scanfile Settings

In order for Declude to start your anti-virus software, it will need to know how to start it. The Declude EVA configuration file (\Declude\virus.cfg) has a line that begins with "SCANFILE". You need to enter the command line used to start your virus scanner. For example, if it is called SCAN.EXE in the D:\Scanner directory, and you want to use the options /NOBEEP and /NOMEM, you would make sure to have a line in your configuration file:

```
SCANFILE  D:\Scanner\SCAN.EXE /NOBEEP /NOMEM
VIRUSCODE 13
```

Declude will then call the scanner in that way for every attachment (and non-text MIME segment) that comes through your mail server. Be sure to use the *short* path name (as in the examples below), as spaces may not work properly. The "VIRUSCODE 13" lets Declude know the code that the virus scanner uses to indicate a virus was found (and is on a line separate from the SCANFILE line).

Read through the configuration options of your command line virus scanner to make sure that it is going to do what you want. The options shown below are typical; "/ALL" will scan all E-mail regardless of extension; "/NOMEM" will prevent the mail server memory from being scanned for viruses.

Product	Suggested Settings
	SCANFILE *[Drive:]**[Path]*\Grisoft\AVG7\avg.exe /NOBOOT /NOMEM /NOSELF /ARC /REPORT=report.txt VIRUSCODE 4 VIRUSCODE 5 VIRUSCODE 6 VIRUSCODE 7 VIRUSCODE 9 REPORT identified

AVG AntiVirus	or SCANFILE *[Drive:]\[Path]*\Grisoft\AVG7\avgscan.exe /NOMEM /NOSELF /ARC /REPORT=report.txt VIRUSCODE 4 VIRUSCODE 5 VIRUSCODE 6 VIRUSCODE 7 VIRUSCODE 9 REPORT identified
ClamAV	SCANFILE *[Drive:]\[Path]*\bin\clamscan.exe --quiet --log-verbose --no-summary --max-ratio 0 -l report.txt VIRUSCODE 1 or SCANFILE *[Drive:]\[Path]*\clamwin\bin\clamscan.exe --verbose --database="*[Drive:]\[Path]*\db" --tempdir="c:\Temp" --no-summary -l report.txt VIRUSCODE 1 ** If you use option 2 ensure you have a C:\Temp dir
Command AV	SCANFILE *[Drive:]\[Path]*\Comman~1\F-PROT.exe /TYPE /SILENT /NOMEM /ARCHIVE /NOFLOPPY /NOBOOT /DUMB /REPORT=report.txt VIRUSCODE 3 VIRUSCODE 6 REPORT Infection
Dr. Solomon	SCANFILE *[Drive:]\[Path]*\viruss~1\4.0.xx\scan.exe /ALL /NOMEM /NOBEEP /NODDA /UNZIP VIRUSCODE 13
eTrust	SCANFILE *[Drive:]\[Path]*\ca\etrust~1\etrust~1\vet32.exe /nobootscan/display=none /logfile="report.txt" VIRUSCODE 66 OKCODE 2 REPORT -
F-Prot	SCANFILE *[Drive:]\[Path]*\fpcmd.exe /TYPE /SILENT /NOMEM /ARCHIVE=5 /NOBOOT /DUMB /REPORT=report.txt VIRUSCODE 3 VIRUSCODE 6 VIRUSCODE 8 REPORT Infection:
F-Secure	SCANFILE *[Drive:]\[Path]*\F-Secure\anti-v~1\fsav.exe /ALL /ARCHIVE /NOBOOT /SILENT VIRUSCODE 23 # Note: F-Secure may require a user to be logged on in order to function.
Inoculan InnoculateIT	SCANFILE *[Drive:]\[Path]*\Comput~1\Inocul~1\inocucmd.exe /LIS .\report.txt VIRUSCODE 100 VIRUSCODE 101 REPORT infected by virus or *SCANFILE [Drive:]\[Path]*\CA\Common\ScanEn~1\inocmd32.exe /ARC /LIS:report.txt VIRUSCODE 100 VIRUSCODE 101 REPORT infected by virus
Kaspersky	SCANFILE *[Drive:]\[Path]*\Kasper~1\Antivi~1\avp32.exe /S /Q /N VIRUSCODE 3 VIRUSCODE 4 or SCANFILE *[Drive:]\[Path]*\Kasper~1\kavshell.exe SCAN /FA /DISINFECT /WA:scan.log VIRUSCODE 3 VIRUSCODE 4
McAfee VirusScan or NetShield	SCANFILE *[Drive:]\[Path]*\networ~1\viruss~1\4.0.xx\scan.exe /ALL /NOMEM /NOBEEP /NOBREAK /UNZIP /SILENT /NODDA /REPORT report.txt VIRUSCODE 13 REPORT Found # WARNING: You MUST use SCAN.EXE and not SCAN32.EXE (you may need to do a full

	# WARNING: You MUST use SCAN.EXE and not SCAN32.EXE (you may need to do a full install to get SCAN.EXE)
NOD32	SCANFILE *[Drive]\[path]*\NOD32.exe /selfcheck- /sound- /quit+ /scanboot- /scanmbr- /arch+ /all VIRUSCODE 1 VIRUSCODE 13
Norman Virus Control	SCANFILE *[Drive:]\[Path]*\nvc\bin\nvc32.exe /AF /B /BS- /C /N /Q /LF:.\report.txt VIRUSCODE 1 REPORT ->\ or *SCANFILE [Drive:]\[Path]\nvc\bin\nvcc.exe /B /BS- /C /N /Q /LF:.\report.txt* VIRUSCODE 1 REPORT ->
Norton	
Panda	SCANFILE *[Drive:]\[Path]*\PandaS~1\PandaA~1.0\pavcl.exe /NOM /NOB /AEX /CMP /NOS /NOR VIRUSCODE 13 VIRUSCODE 16777472
Pest Patrol	SCANFILE *[Drive:]\[Path]*\PestPa~1\PestPatrolCL.exe /Extensions=ALL /NoSound /NoPause VIRUSCODE 2
Sophos	SCANFILE *[Drive:]\[Path]*\Sophos~1\sav32cli.exe -ns -p=report.txt -mac -archive VIRUSCODE 6 REPORT >>> Virus or *SCANFILE [Drive:]\[Path]\Sophos~1\sweep.exe -nb -nm -nk -ns -ZIP*) VIRUSCODE 3 VIRUSCODE 6 REPORT >>> Virus
Trend Micro PCScan	SCANFILE *[Drive:]\[Path]*\pcscan.exe /NB /NM /NC VIRUSCODE 8 VIRUSCODE 22
TrendMicro OfficeScan	SCANFILE *[Drive:]\[Path]*\vscantm.bin /NB /NM /NC VIRUSCODE 1

Advanced Configuration

[*You only need to worry about this section if you want to fine-tune Declude.*]

Acting as a gateway for domains on other servers

Declude EVA can be set up to scan E-mail for domains that are not hosted on your mail server . First, you need to set up your mail sever 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 mail sever, and follow the instructions in the manual or mail sever Knowledge Base for a gateway domain).

The only catch as far as Declude EVA is concerned is that mail severwill treat the E-mail to the gateway domain as outgoing mail, since it is not stored on the mail sever. You should be aware of this if you set up Declude EVA to scan only incoming E-mail or outgoing E-mail.

Integrated AVG

BUILTINSCANNER

Declude has AVG virus scanner directly integrated into Declude. This directive turns on or off the internal AVG scanner.

BUILTINSCANNER ON

AVGUPDATE (4.3.48)

Located in the Declude.cfg This directive turns on or off the internal AVG scanner signature updates.

AVGUPDATE ON

Quarantine Directory

VIRDIR

You need to specify the directory in which Declude will store E-mails that contain viruses. This option lets you choose what directory to store them in (if the directory does not exist, it will be created).

VIRDIR spool\virus

Directional Scanning

INCOMING / OUTGOING

The following options allow you to limit scanning to only incoming or outgoing E-mail.

INCOMING ON
OUTGOING ON

Order of Scanning

AVAFTERJM

Change the order in which JunkMail and Declude EVA scan. The default is JunkMail followed by Declude EVA

AVAFTERJM ON

EXITSCANONVIRUSDETECT

This directive, will cause Declude to stop calling the remaining scanners after a virus has been detected. This directive has meaning only when there is more than one scanner listed. The default behavior is for Declude to call all scanners.

EXITSCANONVIRUSDETECT ON

MAXATONCE

The MAXATONCE option limits the number of AV processes. For example,MAXATONCE 1 will only allow 1 AV process to run at once (for licensing purposes). A value of 0 (or commenting it out) allows unlimited processes to run at the same time.

MAXATONCE 0

Virus scanners that delete files

ONACCESS

Declude EVA does not officially support virus scanners that scan files as they are written to the disk ("on access" scanners, these are not command line virus scanners). This is because we can not be sure exactly when the files are scanned, and when it is safe to assume that a file that has not been deleted is virus-free. Although they should work, we do not recommend using them.

The ONACCESS option should be set to OFF unless you have an on-access virus scanner that will be deleting attachments with viruses. It is recommended NOT to have an on-access scanner interfering, and to leave this at OFF.

ONACCESS OFF

SCANNERTIMEOUT

The SCANNERTIMEOUT option lets you choose the number of seconds that Declude will wait for the virus scanner to finish. The minimum value is 10 seconds. Most scanners will not need to take that long. This option is mainly to prevent defective scanners (that never finish) from interfering with your outgoing E-mail. Raising this will NOT help if your virus scanner always times out.

SCANNERTIMEOUT 60

PRESCAN

Declude EVA Pro has the option for pre-scanning E-mail, which can significantly improve performance. Declude can pre-scan HTML files. If no dangerous code is detected, the virus scanner will not get called. This can significantly cut down on CPU usage. Since the majority of E-mails are really plaintext with a "cute" HTML version of the E-mail attached (that is usually identical to the plain text version), a lot of scanning may be done that isn't necessary. Plain HTML files (without any scripts or other potentially dangerous code) are safe. The pre-scanning in Declude EVA will check HTML segments to see if there is any potentially dangerous code (JavaScript, Active-X, plugins, etc.). If so, it will send them to the virus scanner as they usually would be. Otherwise, it will let them pass through unscanned, which will improve performance.

PRESCAN ON

FOOTER

The FOOTER lines will add a footer to the bottom of E-mails that are scanned. This may not be visible if you send HTML or attachments with the E-mail.

FOOTER [This E-mail scanned for viruses by Declude]

DELIVERERRORS

The DELIVERERRORS option, when set to ON, will treat errors from the virus scanner as if no virus was found. When set to ON, this could cause viruses to get through in rare situations, but will also prevent legitimate mail from being quarantined due to an error in the scanner. It is recommend to leave this at ON.

DELIVERERRORS ON

Skipping virus notifications for certain viruses (such as Klez)

SKIPIFVIRUSNAMEHAS

Declude EVA can be set up not to send out E-mail notifications for specific viruses. This is useful for viruses that forge the return address (in which case a "You have a virus" notification would get sent to someone without a virus). To prevent a notification from getting sent out, you can add a line "SKIPIFVIRUSNAMEHAS Virusname" to the beginning (before the first blank line) of any of the \Declude*.eml files (typically just the sender.eml and otherpostmaster.eml files). "Virusname" should be replaced with a string that always appears in the name of the virus and any variants; for example "SKIPIFVIRUSNAMEHAS Klez". Note that there can only be one space (or tab) between "SKIPIFVIRUSNAMEHAS" and the virus name. To prevent the notifications from being sent for multiple viruses, you need to have a SKIPIFVIRUSNAMEHAS line for each virus.

SKIPIFVIRUSNAMEHAS Klez

Vulnerability Options

A vulnerability is a method that people can use to bypass virus scanning. Clearly, this is something that hackers and virus writers like to do. An E-mail that takes advantage of vulnerability may or may not actually contain a virus. By default, Declude EVA will catch all vulnerabilities as if they were viruses. This has stopped a number of new viruses before virus definitions were available to stop them. False positives are not common, but when they occur almost always turn out to be spam.

CLSID Vulnerability: This vulnerability occurs when an E-mail uses a 'CLSID' as an extension. A CLSID is a long string that identifies a certain program (such as Notepad), and using the CLSID instead of a standard file extension will cause Windows to use the program identified by the CLSID to open the file. Windows will not display the CLSID extension, so a file with an innocent name such as "cutedog.jpg" could cause another program to run.

Conflicting Encoding Vulnerability: This vulnerability occurs when the headers of an E-mail claim that two or more different encoding types are used. A MIME segment can only be encoded in one way, so if there are more than one encoding types listed, it is possible that the mail server virus scanner and the mail client will use different decoding methods on the E-mail. If this happens, a virus could bypass virus scanning on the mail server.

Outlook 'Blank Folding' Vulnerability: This vulnerability occurs when there is a line in the headers with just a single space or a single tab character. Outlook can treat this as the end of the headers, allowing it to see a virus that is embedded in the headers. RFC822 3.2.3 says that it is not valid to have such lines, nor is there any legitimate reason for an E-mail to contain a blank line in the headers with a single space or tab (note that it is OK to have a line with a single space or tab in the E-mail body, just not the headers).

Outlook 'Boundary Space Gap' Vulnerability: This vulnerability occurs when there is a space or tab in the MIME boundary. This is not RFC-compliant, but Outlook will treat it as valid and be able to see a virus that virus scanners will not usually see. There is no legitimate reason for an E-mail to be formed like this.

Outlook 'CR' Vulnerability: This vulnerability occurs when an E-mail contains a single 'CR' character within the E-mail headers (as opposed to a 'CR' followed by an 'LF', which is used to end a line in SMTP). Outlook can treat this as the end of the headers, which would allow Outlook to see a virus that was embedded in the headers. RFC2822 2.2 says that CR and LF characters cannot appear alone in the headers. Also, there is no legitimate reason for an E-mail to contain a lone 'CR' in the headers.

Outlook 'Long Boundary' Vulnerability: This vulnerability occurs when an E-mail has a MIME boundary that is longer than allowed by the RFCs. Outlook may see a virus when a virus scanner will not. There is no legitimate reason for an E-mail to be sent like this.

Outlook 'Long Filename' Vulnerability: This vulnerability occurs when an E-mail has an attachment with a name longer than 256 characters long. When this occurs, it is possible for Outlook not to see the correct file extension, causing Outlook to think that a dangerous E-mail is actually safe.

Outlook 'MIME header' Vulnerability: This vulnerability occurs when certain safe MIME types are used, but a potentially dangerous file type is attached. Outlook may execute the attachment automatically, without looking at its file extension. There is no legitimate reason for an E-mail to be sent like this, and a number of viruses use this vulnerability.

Outlook 'MIME segment in MIME postamble' Vulnerability: This vulnerability occurs when it appears as

though a MIME segment is occurring after the end of the MIME body (specifically, a MIME segment with a boundary other than the one specified appears in the MIME postamble). Outlook may see this as an attachment. Although technically valid, there is no legitimate reason for an E-mail to be sent like this.

Outlook 'MIME segment in MIME preamble' Vulnerability: This vulnerability occurs when it appears as though a MIME segment is occurring before it should (specifically, a MIME segment with a boundary other than the one specified appears in the MIME preamble). Outlook may see this as an attachment. Although technically valid, there is no legitimate reason for an E-mail to be sent like this.

Outlook 'Space Gap' Vulnerability: This vulnerability occurs when there is a space in one of the MIME headers where there is not normally a space (such as "Content-Type :" instead of "Content-Type:"). This is not RFC-compliant, but Outlook will treat it as valid and be able to see a virus that virus scanners will not usually see. There is no legitimate reason for an E-mail to be formed like this.

Partial (Fragmented) Vulnerability: This vulnerability occurs when one E-mail is split into separate parts, each in a separate E-mail. Although this is legal, it will bypass virus scanners, and therefore will likely soon be deprecated.

DELETEVULNERABILITIES

By default, emails with vulnerabilities will be quarantined. You may, however, choose to delete these vulnerabilities.

DELETEVULNERABILITIES OFF

BANCRVIRUSES

To prevent vulnerabilities (such as the Outlook Blank Folding and Outlook MIME Headers exploit) from being detected, you can have a line "BANCRVIRUSES OFF" in your It is **not** recommended that you turn the vulnerability detection off, as it will almost certainly allow future viruses through undetected! The BANCRVIRUSES option will automatically treat E-mail with malformed headers that could contain a virus as if they did contain a virus.

BANCRVIRUSES ON

ALLOWVULNERABILITIESFROM

This option instructs Declude EVA to allow vulnerabilities from a specific E-mail address or domain.

ALLOWVULNERABILITIESFROM example@example.com

ALLOWVULNERABILITIESTO

This option instructs Declude EVA to allow vulnerabilities to a specific E-mail address or domain.

ALLOWVULNERABILITIESTO example@example.com

ALLOWVULNERABILITY

You may selectively allow certain vulnerabilities not to be blocked by Declude EVA.

ALLOWVULNERABILITY OBJECTDATA
ALLOWVULNERABILITY OLCR
ALLOWVULNERABILITY OLSPACEGAP
ALLOWVULNERABILITY OLBLANKFOLDING
ALLOWVULNERABILITY OLMIMEHEADER
ALLOWVULNERABILITY OLMIMESEGMIMEPRE
ALLOWVULNERABILITY MIMESEGMIMEPOST
ALLOWVULNERABILITY OLLONGBOUNDARY
ALLOWVULNERABILITY OLBOUNDARYSPACEGAP
ALLOWVULNERABILITY OLLONGFILENAME
ALLOWVULNERABILITY NONSTANDARDHDR

Please note that the description that follows the directive is for informational purposes only and must NOT be included in the virus.cfg:

DIRECTIVE	VARIABLE	DESCRIPTION
ALLOWVULNERABILITY	OBJECTDATA	HTML Object Data Vulnerability
ALLOWVULNERABILITY	OLCR	Outlook CR Vulnerability
ALLOWVULNERABILITY	OLSPACEGAP	Outlook Space Gap Vulnerability
ALLOWVULNERABILITY	OLBLANKFOLDING	Outlook Blank Folding Vulnerability
ALLOWVULNERABILITY	OLMIMEHEADER	Outlook MIME Header Vulnerability
ALLOWVULNERABILITY	OLMIMESEGMIMEPRE	Outlook MIME Segment in MIME Preamble Vulnerability
ALLOWVULNERABILITY	MIMESEGMIMEPOST	Outlook MIME Segment in MIME Postamble Vulnerability
ALLOWVULNERABILITY	OLLONGBOUNDARY	Outlook Long Boundary Vulnerability
ALLOWVULNERABILITY	OLBOUNDARYSPACEGAP	Outlook Boundary Space Gap Vulnerability
ALLOWVULNERABILITY	OLLONGFILENAME	Outlook Long File Name Vulnerability

BANCLSID / BANPARTIAL

Declude EVA can block treat files using CLSID extensions as viruses. This type of extension will force a certain type of program to be run, while making the file appear to be a .TXT or other safe file. There is no known legitimate reason to send this type of file through E-mail. BANPARTIAL ON bans the Partial Vulnerability.

BANCLSID ON

BANPARTIAL ON

Virus Options

DELETEVIRUSES

You can automatically delete viruses (instead of quarantining them). E-mails that are blocked but not virus is detected (such as banned file extensions and vulnerabilities) will not be deleted as they have the potential of being legitimate E-mails. It is recommended to leave this at OFF, just to be safe, but many people set this to ON.

DELETEVIRUSES OFF

SKIPEXT

The SKIPEXT option will let you skip scanning of certain file extensions. For example, a GIF file can't contain a virus, so there is no need to scan it.

SKIPEXT GIF

Banning files based on their name

BANNAME

The BANNAME option that can be used to specific specific filenames that should be banned. This can be useful if a new virus starts spreading, and virus definitions have not yet been updated for it You can ban up to 50 files by name. When a banned file is detected, the BANnotify.eml file will be sent out.

BANNAME account-details.zip

Banning files based on extension

BANEXT

Declude EVA will let you ban E-mails that have specific type of file attachments, if you desire. For example, you can ban all .SCR attachments. If a file arrives with a banned attachment, it will be quarantined. You can ban up to 100 file extensions. The BANEXT option will let you ban file extensions. E-mails containing attachments with these file extensions will be quarantined, and if you have a BANnotify.eml file, it will be sent out.

BANEXT EXE

BANEXT (Encrypted Zips)

In March, 2004, viruses started spreading in encrypted .ZIP files. While it was known that such files could not be scanned properly for viruses (since the virus scanner cannot know the password), nobody expected that end users could be convinced to actually open the files. Although viruses in encrypted archive files rarely spread (they usually spread in both the encrypted and non-encrypted files, with the non-encrypted files spreading much faster), they need to be caught.

Declude can automatically ban all encrypted archive (.ZIP or .RAR) files. That way, any encrypted archive files will be blocked. This is necessary, as virus scanners normally cannot detect viruses in encrypted archive files (some AV programs are able to detect *some* viruses in archive files, but not all).The BANEXT EZIP line blocks all encrypted .ZIP and .RAR files, which is necessary to be fully protected against viruses (since it is impossible to detect a well-constructed virus within an encrypted .ZIP or .RAR file)

BANEXT EZIP

BANZIPEXTS

File extensions within .ZIP files can be banned. For example, if you have a line BANEXT EXE and BANZIPEXTS ON then .EXE files within .ZIP files will be blocked.

BANZIPEXTS OFF

BANEZIPEXTS

Declude Virus should look within encrypted .ZIP files to see if there are files whose extensions are blocked with the BANEXT option. If so, they are banned.

BANEZIPEXTS OFF

FORGINGVIRUS

The FORGINGVIRUS option is used to list viruses that forge the return address, so Declude can replace the name of the sender with "[Forged]".

Per-Domain and Per-User Settings

Declude EVA Standard allows you to choose which domains will have their mail scanned, and Declude EVA Pro will allow you to also choose which users will have their mail scanned. This is done with two extra configuration files, virus_domains.txt and virus_users.txt.

To set up per-domain settings (for Standard and Pro versions):

Place the virus_domains.txt file in your \Declude\ directory.

Next, decide what the default domain settings should be. Do you want to scan all domains by default? If so, you need a line "DEFAULT ON". If you want to disable scanning for any domains that are not listed, use "DEFAULT OFF". To default to scanning only E-mail to or from a domain, you can use "DEFAULT INONLY" (to scan E-mail to a domain) or "DEFAULT OUTONLY" (to scan E-mail from a domain).

Now, you can add the domains that you want to handle differently than the default setting. To do this, just add a line with the domain name, and how you want the mail handled. For example, to scan all mail going to "example.com", you would add a line "example.com ON". To turn off all scanning for a domain, you would add a line "example.com OFF". In rare situations, you may instead wish to use the INONLY or OUTONLY settings (to scan only E-mail to or from a domain).

Example:

```
DEFAULT          ON

example.com      OFF

mail.example.com OFF
```

This will scan all E-mail except for mail addressed to or from users at @example.com or @mail.example.com. Note that domain aliases (such as "mail.example.com") only need to be added if they are actually used in E-mail addresses (for example, if some people would send E-mail to "username@mail.example.com", rather than "username@example.com").

To set up per-user settings:

The per-user settings require that you have a per-domain file set up, to let Declude EVA know the default. Place the virus_users.txt file in your \Declude\ directory.

Then, for any user that you want to have special settings for, just add their E-mail address followed by either "ON" (to scan all their mail), "OFF" (to disable scanning of their mail), "INONLY" (to only scan E-mail to them), or "OUTONLY" (to only scan E-mail from them). Example:

```
user1@example.com          ON

user2@example.com          INONLY
```

This will force all E-mail to user1@example.com to be scanned (even if the settings for example.com or the default settings are different), and user2@example.com's incoming mail will be scanned (but not his outgoing mail).

Other information about per-domain and per-user settings

- Per-user settings override per-domain settings, and per-domain settings override the default settings.
- It is OK to have duplicate entries, such as "DEFAULT ON" and "example.com ON".
- Per-user settings: You need to enter the intended recipient address (whatever the sender enters as the E-mail address)

Multiple Scanners

Declude EVA Pro allows you to have use to 5 different virus scanners.

You add them by adding the same "SCANFILE", "VIRUSCODE", "REPORT" and "OKCODE" lines that you would normally add, except there will be a number after them to indicate which scanner it applies to. So, where you might have the following now:

```
SCANFILE C:\Scanner\scan.exe /ALL

VIRUSCODE 13

REPORT  Found
```

You might change it to:

```
SCANFILE1 C:\Scanner\scan.exe /ALL

VIRUSCODE1 13

REPORT1  Found

SCANFILE2 C:\Scanner2\scanner.exe

VIRUSCODE2 3

VIRUSCODE2 6

REPORT2  Infection
```

Note that if you don't include the scanner number, "1" is assumed (so you don't have to change the existing settings).

Testing

It's important to know how to SAFELY test Declude Virus:

First, it's important to test to make sure that Declude EVA is scanning your mail properly. If it isn't, you're receiving no protection. On the other hand, though, you have to know how to safely test virus software.

The key to doing this is a file called **EICAR.COM**. Eicar is an organization of anti-virus experts, and they designed a very small program that is *not* a virus and does *not* have an virus code in it, but which anti-virus software will recognize and report as though it was a virus. Because of these characteristics, it is completely safe.

It is best to send this file using our Test Mail Sender at http://tools.declude.com. This will let you send the file in various formats that your E-mail client may not normally send in (you only need to test using one of them, but can try more than one for peace of mind if you want). Sending the mail from our web page prevents problems such as the eicar.com file being deleted before it is sent, or having the eicar.com sent as a text file (which can't be exectuted, so it won't get caught).

If the E-mail with the eicar.com file is delivered, something is not set up properly.

You should *NOT* try testing Declude or your anti-virus software with real viruses. If you are not careful (or even if you are!), you can damage your entire network, and possibly spread the virus to other systems. The only way to safely test anti-virus software with real viruses is in a virus lab (such as the one that we have set up), that is designed specifically so that a known amount of acceptable damage will occur in the event of an outbreak.

Types of Virus Scanners

There are two main types of virus scanners: *on-access* scanners, and *on-demand* scanners. Command-line scanners (the type Declude uses) are on-demand scanners.

An on-demand scanner is run when the user requests it. It can either be a command-line scanner, or a standard Windows program. The command line scanner works well with Declude because it can be set to scan specific files, and be configured in Declude by adding command line parameters to the file name.

An on-access scanner scans all files that are written to the hard drive. These usually just cause unnecessary overhead when run with Declude, as the files will end up getting scanned twice.

It is possible to use an on-access scanner with Declude, although it is not recommended. Once we have done more testing to determine the safety of using on-access scanners, we may recommend this type of a setup. The problem is that Declude has no way of knowing how long to wait to determine if the scanner has scanned the file. In most cases, though, this should work.

Advanced Scanner Configuration

At the beginning of this manual is a list of scanners and the best options for them. However, you may have a program or version that we have not tested. Here are a couple of pointers for common configuration options:

Memory: /NOMEM or /M-. This option will prevent the virus scanner from scanning the server's memory. This is important because it takes time to scan the memory, and there is no need to scan it for each incoming E-mail.

Boot Sector: /NOBOOT. This option will prevent the virus scanner from scanning the boot sector of the hard drive. This is important because it takes time to scan the boot sector, and there is no need to scan it for each incoming E-mail.

Beeping: /NOBEEP. Most virus scanners give you the option of beeping whenever a virus is found. Depending on your environment, you may or may not want to disable this.

Heuristics. Many virus scanners let you determine whether or not they use heuristics to try to detect new viruses. Using heuristics will increase the amount of time scanning each file, and will only catch unknown viruses. It may be better just to keep your scanner up to date.

File Name: Do NOT use a file name or directory name. Declude will automatically instruct the command line scanner which file(s) to scan.

E-mail Notifications

Declude EVA allows you to send notifications to the recipient of a virus, the sender, and/or third parties.

To accomplish this, you need to have "E-mail template files" in the \Declude\ directory. These files can have any name, but must have the extension ".eml". When Declude finds a virus, it will search the \Declude\ directory for any .eml files (except ones used by other Declude programs), and it will send out one E-mail for each E-mail template file.

Each E-mail template file needs a To:, From:, and Subject: line, followed by a blank line, and then the body of the message. For E-mail notifications, you can copy the Recipient E-mail Template, Postmaster E-mail Template (and the Sender E-mail Template and Remote Postmaster E-mail Template here

There are also a number of variables that you can use:

Variable	Description
%ALLRECIPS%	Recipients of the E-mail
%BANEXT%	Shows the file extension that was banned (for banned attachments)
%DATE%	Today's date DD MMM YYYY
%EURDATE%	Today's date DD/MM/YYYY
%HEADERS%	Inserts the headers of the E-mail with the virus
%INOROUT%	"incoming" or "outgoing"
%ISODATE%	Today's date YYYY-MM-DD
%LOCALHOST%	Local host name (a domain on your mail server)
%LOCALRECIPS%	Displays a list of just the local recipients of the E-mail
%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
%SENDERHOST%	Host name of the sender
%SUBJECT%	Inserts the subject of the E-mail
%TIME%	Current time (HH:MM:SS format)
%USDATE%	Today's date MM/DD/YYYY
%VIRUSFILE%	Used with the REPORT configuration option
%VIRUSNAME%	Used with the REPORT configuration option
%VERSION%	Inserts the version of Declude that is running

With Declude EVA, you can also restrict who the notification is sent to, using certain commands in the E-mail template files. Each command needs to be on a line by itself. You need to make sure that these options (and any To:, From:, or Subject: lines) appear before the first blank line in the E-mail template file. The available commands are:

Command	Restriction	Usage
ONLYSENDIFIP	Will only send the notification if the virus came from an IP with the text you specify	ONLYSENDIFIP 192.0.2.1
ONLYSENDIFLOCALSENDER	Will only send the notification if the sender of the virus is a local user.	ONLYSENDIFLOCALSENDER
ONLYSENDIFRECIP	Will only send the notification if one of the recipients is one you specific	ONLYSENDIFRECIP user@example.com
ONLYSENDIFREMOTESENDER	Will only send the notification if the sender of the virus is a remote user.	ONLYSENDIFREMOTESENDER
ONLYSENDIFSENDER	Will only send the notification if the sender of the virus is one you specify.	ONLYSENDIFSENDER user@example.com ONLYSENDIFSENDER @example.com
ONLYSENDIFLOCALRECIPIENT	Will only send the notification if the recipient of the virus is a local user.	ONLYSENDIFLOCALRECIPIENT
ONLYSENDIFREMOTERECEIPIENT	Will only send the notification if the recipient of the virus is a remote user.	ONLYSENDIFREMOTERECIPIENT
ONLYSENDIFVIRUSNAMEHAS	Will only send the notification if the virus name has the text you specify.	ONLYSENDIFVIRUSNAMEHAS Vulnerability
SKIPIFEXT	Will not send the notification if a specific extension is detected	SKIPIFEXT pif
SKIPIFFORGING	Will not send the notification if a forging virus is	SKIPIFFORGING

	automatically detected	
SKIPIFSENDER	Will not send the notification if the sender of the virus is one that you specify.	SKIPIFSENDER SendsLotsOfViruses@example.com SKIPIFSENDER @example.com
SKIPIFRECIP	Will not send the notification if the recipient of the virus is one that you specify.	SKIPIFRECIP DoesNotLikeVirusNotifications@example.com SKIPIFRECIP @example.com
SKIPIFVIRUSNAMEHAS	Will not send the notification if the virus name has the text that you specify.	SKIPIFVIRUSNAMEHAS Klez
SKIPIFVIRUSNAMEDOESNOTHAVE	Will not send the notification if the virus name does not have the text that you specify.	SKIPIFVIRUSNAMEDOESNOTHAVE Vulnerability

A sample E-mail notification might look like:

```
SKIPIFVIRUSNAMEHAS Klez

SKIPIFVIRUSNAMEHAS Vulnerability

SKIPIFSENDER @boss.com

ONLYSENDIFREMOTERECIPIENT

From: postmaster@%LOCALHOST%

To: %MAILFROM%

Subject: WARNING: YOU MAY HAVE A VIRUS

The Declude Virus software on %LOCALHOST% has reported that you

sent an E-mail to %ALLRECIPS%, containing the %VIRUSNAME% virus

in the %VIRUSFILE% attachment.  The subject of the E-mail was

"%SUBJECT%".

The E-mail containing the virus has been quarantined to prevent

further damage.

Headers Follow:

%HEADERS%
```

Virus Name and Virus Attachment Name

The only thing that scanners can report directly to Declude is a code that indicates whether or not a virus is present in a file.

However, many people want to know what virus is present, and which attachment it was found in. In order for the virus scanner to get this information to Declude, and you are not using a common scanner, you may need to do some work.

First, you need to get your virus scanner to save a file called "report.txt" in whatever directory that the virus scanner is currently scanning in. It **must** be named exactly that, and **MUST** be in whatever directory the virus scanner is scanning in (which is always different). With McAfee, you would add "/REPORT report.txt" to the SCANFILE option in \Declude\virus.cfg. With F-Prot, you would add "/REPORT=report.txt". With Norman AntiVirus, you would add "/LF:.\report.txt". *Do not use a path name to the report.txt file; if you do, there WILL be problems*.

Next, you need to tell Declude what to look for in the report.txt file. You need to use the "REPORT" configuration option (in \Declude\virus.cfg) to let Declude know a word that appears after the file name, and before the name of the virus. For Mcafee, you would add a line "REPORT Found". For F-Prot, you would add a line "REPORT Infection". For Norman AntiVirus, you would add a line "REPORT ->".

Finally, you need to add the %VIRUSNAME% and %VIRUSFILE% variables to the E-mail templates where you want the virus name and attachment name to occur.

WARNING: You MUST make sure that if you use the REPORT configuration option, that your virus scanner DOES save the report.txt file. Otherwise, Declude will see one less file in the temporary directory than there should be, and assume that an on-access scanner deleted it because it found a virus.

Automatic detection of forging viruses

Declude EVA will by default automatically attempt to determine if a virus is forging or not. This is useful, as it will automatically suppress inappropriate notifications that should not be sent out when a forging virus is detected. It works by connecting to a Declude, Inc. server, sending the name of the virus and the IP it came from, and our

server reports back whether or not the virus is forging.

If for some reason you do not wish to use this feature, you can add a line "AUTOFORGE OFF" to your \Declude\virus.cfg file.

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

Troubleshooting

- You must have a file \Declude\virus.cfg (named *exactly* that).
- The filename/path listed in the SCANFILE option must *not* have any spaces in it.
- It is a good idea to check the log file for obvious error messages.
- On-access virus scanners can interfere with Declude's operation; you should try disabling them.

No declude\logs\vir####.log file is created.

This file should exist after Declude is installed and it has scanned its first E-mail. If it does NOT exist, there is a problem. The #### is replaced with the current date, so if today is January 31st, the log file should be named \spool\vir0131.log. If the file does NOT exist, check to make sure that you have a file \Declude\virus.cfg (spelled correctly: "virus.cfg"; *NOT* "virus_cfg" or "virus.cfg.txt"), and that you have the correct activation code in there. The log file may be placed in a different location, if the LOGFILE option in \Declude\virus.cfg is set to something other than \spool\virus.cfg.

I send the eicar.com file, but it isn't caught.

There are a number of possible reasons for this. There could be a virus scanner on the machine you are

sending the eicar.com file from that could be deleting the attachment, so that Declude won't see it. Or, the mail client could be treating the eicar.com file as a text file (in which case it shouldn't appear as a downloadable/saveable attachment). ***Solution:*** You should then try sending the eicar.com file through our web site (http://tools.declude.com , click on "Test Mail Sender"). It will send the attachment properly. If the \spool\vir####.log file says "ERROR: Incorrect Declude Virus code...", then the activation code is not the correct one for your mail server. You will need to contact us in this case.

The eicar.com file sent from http://tools.declude.com doesn't get caught.

The most likely reason for this is that you have an "on-access" scanner that is deleting (or otherwise altering) the attachment when Declude decodes it. Then, the command line scanner will report that no virus was found (since the virus is now gone), and the E-mail will be delivered. ***Solution:*** Disable the on-access scanner, or change the "ONACCESS OFF" line in \Declude\virus.cfg to "ONACCESS ON".

The eicar.com file STILL doesn't get caught.

One last thing to check is to make sure that you haven't disabled short file names -- some virus scanners require them (the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation registry entry needs to be set to 0 if your virus scanner requires short file names). If there is no \spool\vir####.log file, look at the Troubleshooting section "No \spool\vir####.log file is created". If the log file is created, please contact us and we will instruct you on how to enable the debugging mode.

I see lots of .vir directories in my work directory.

Declude Virus uses these temporary directories to scan attachments. It is normal to see them appear for short periods of time. If they are not being deleted, there is a problem! The two common causes are either that you entered an invalid program name in the SCANFILE option in \Declude\virus.cfg (make sure there are no spaces in the path), or your virus scanner is leaving files behind that prevent Declude from deleting the directory (it may be saving a report file that Declude doesn't know about). This could also happen if you are using the REPORT configuration option and do not have a report.txt file being saved properly (you can NOT use a path name for the report.txt file).

Legitimate E-mail is caught with vulnerabilities

When this happens, the typical question is "How do I disable the vulnerability detection?". However, this is not the right question. Legitimate E-mail with a vulnerability is still E-mail with a vulnerability, and is dangerous. If you turn off vulnerability detection, you will almost certainly receive new viruses in the future, even if your virus definitions are up to date. Also, it is extremely likely that this legitimate mail will get caught by other virus scanners in the near future. When this happens, we recommend that you send us a copy of the E-mail that was caught (from your \spool\virus directory), and we can contact the sender to let them know how to fix the problem.

I see "ERROR: Virus scanner didn't finish after [number] seconds" in the log.

Normally, a virus scanner should be able to scan an E-mail within a second or two. If it always takes more than 30 seconds, there is a problem. Most likely, the virus scanner is waiting for input from you (you can verify this by temporarily setting the loglevel to DEBUG) -- but obviously you shouldn't have to be at the server 24 hours a day! This should only happen with non-automated scanners.

Solution 1: If you are using F-Prot, make sure to DELETE the F-Prot.PIF file.

Solution 2: If you go to a command prompt and start the scanner, and a window pops up, you are using the wrong scanner. You may need to do a full install of your virus scanner to get it to install the correct scanner ("command line scanner").

E-mail notifications are not sent out.

The files must have a ".eml" extension and be in the \Declude\ directory. Also, they must have "To: ", "From: ", and "Subject: " lines before the first blank line in the file. Finally, E-mail notifications will not be sent out if the virus scanner is reporting an error (rather than a "virus found" code) -- if the log file says "error in virus scanner", the E-mail notifications will not get sent.

I get an error 'No recipients in .eml file'

This warning occurred because one of your \Declude*.eml files (the E-mail template files for virus notifications) did not have a 'To:' line before the first blank line in the file. The .eml files need to have To:, From:, and Subject: lines before the first blank line in the file.

What version of Declude Virus am I running?

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

Help, Declude for IMail stopped working!

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).

Another rarer problem during an IMail upgrade (happening to about 5% of the 7.05 and 7.06 upgrades) is that the IMail upgrade 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.

Footers are not appearing in some E-mails.

Note that Declude Virus adds the footer to the end of the body of the E-mail. Depending on the mail client, this may or may not be visible if the E-mail is sent using MIME.

Support

*Do **not** send us any viruses.* Unless we request you to send a virus to us (we will give you a special address to send it to), you must not send us any viruses. E-mails with viruses may be politely ignored or deleted; that's a risk you run when spreading dangerous E-mails. Also, please send any files as *attachments* please (not in the body of the E-mail).

Standard Support

If you need support, you can send an E-mail to support@declude.com. For many support issues, we will need a copy of your \Declude\virus.cfg and \spool\vir####.log log file, so sending those files may speed up resolution of your problem.

Emergency/urgent support

Mail servers are vital to the operation of most of our customers. In the rare cases where normal mail delivery is interrupted, or there is another urgent problem, you should send an E-mail to to urgent@declude.com. If you are not receiving mail, you should use an E-mail address that uses another mail server. When sending E-mail to urgent@declude.com, be sure to include your \Declude\virus.cfg and most recent \spool\vir####.log file.

Release Notes

You can view the Release Notes online

User License Agreement

You can view the EULA online