

FAQ on MailScan for CommuniGate Pro.

The FAQs detailed below are loosely grouped under the following headings:

- * What is MailScan?
 - * MailScan Versus eScan
 - * MailScan Licensing
 - * Product and Signature File Updates
 - * How does MailScan work?
 - * Configuration and Operation
 - * Performance and Compatibility
 - * Scanning - Attachment and Infections
 - * Add-On Products
-

Q. What is MailScan?

A. MailScan is an advanced, integrated AntiVirus and Content Security product.

Normally you must purchase, install, configure and maintain two separate and disparate products in order to obtain the same type of functionality that is provided as standard by MailScan.

Q. What is eScan?

A. eScan is the Content-Scanning and Virus-Scanning Software from MicroWorld that MailScan uses to check for harmful content & viruses.

Q. Is eScan part of MailScan?

A. Yes.

Each MailScan license is shipped with and installs a single Enterprise edition license of eScan.

Q. Which versions of CommuniGate Pro is supported by MailScan?

A. CommuniGate Pro versions 3.4 and above.

Q. I have CommuniGate Pro version 3. What product should we use to give protection to our CommuniGate Pro Server?

A. Use MailScan for Mail Servers. Visit <http://www.mwti.net> to get more information on MailScan for Mail Servers.

Q. Why is eScan required?

A. Many of the features supported by MailScan - including those of proper reporting, "Automatic Internet Check" and "Incremental Updates" - either depend upon or are provided by eScan and give MailScan its "ultimate edge" over any other package.

Q. Is MailScan similar to Gateway scanning given by other AntiVirus software packages?

A. No. Because

- a) With gateway scanning packages, you will often need an additional machine, through which you have to "route" your emails.

- b) When using a Gateway scanning package, you will have to "sacrifice" the anti-SPAM, recipient-check, SMTP-Authentication, and other services provided by the Mail Server.
- c) Gateway Scanning packages "normally" do not provide POP3 scanning capability.
- d) To use a Gateway scanning package, you generally need to modify the configuration of the Mail Server.
- e) Gateway Scanning packages often have a "serious security flaw" wherein they keep the SMTP ports open, which hackers can take advantage of!

As MailScan transparently plugs itself in between the Mail Server and the Internet, it does not have any of the above disadvantages.

Q. How is MailScan licensed?

A. MailScan is provided under a software subscription license. The license may be valid for 12, 24 or 36 months, depending upon your choice at the time of purchase.

The subscription license covers you for all product updates and generic content filter updates during the term of the License.

Q. What is the difference between an `update' and an `upgrade'?

A. An `update' is:

- a) a minor point release for the product (e.g. v2.1 updated to v2.2 or build 150 updated to build 160).
- b) new virus signatures

An `upgrade' is a major product release (e.g. v2.x upgraded to v3.x).

Q. What happens after the subscription period expires? Will MailScan stop scanning my emails?

A. At the end of the subscription period, MailScan will continue to scan your emails but it will **stop updating**.

The Corporate edition will also inform the MailScan Administrator about the end-of-subscription.

Q. I have one primary Mail Sever plus a second configured as a secondary or Backup Server in case the primary fails. Do I need one MailScan license or two?

A. You will need two MailScan licenses.

Q. Does MailScan (and eScan) automatically download, install and re-configure itself for product updates? What about product upgrades?

A. 'Yes' - MailScan updates is virus signatures and other Content Rule-Sets automatically.

Product updates (eg v2.2 to v2.3) must be downloaded and installed manually.

Product upgrades (e.g. v2.x to v3.x) must be downloaded and installed manually.

Q. How frequently is MailScan's (eScan's) Virus Database updated?

A. The Web and FTP sites are normally updated once, every day.

On certain occasions, they may be updated more frequently, in response to a virus epidemic (e.g. the Love-Bug virus).

Q. How do we update MailScan (eScan) with the latest virus updates?

A. eScan automatically keeps its virus database updated.

It checks for availability of Internet connection. If it detects that Internet connectivity is present, it then checks to see if a new update is available.

If new updates are available, they are downloaded and implemented automatically.

The default frequency for update checks is currently set at 1-hour intervals, but can be manually configured for other periods.

Q. Can we configure the frequency of update-checks?

A. Yes.

Q. Can eScan download updates via FTP or HTTP? Will it work through my normal Proxy or SOCKS Proxy Server?

A. Yes

Q. Can eScan download updates through my Firewall?

A. Yes. Either using HTTP downloads or using Passive FTP.

Q. How does MailScan intercept emails?

A. MailScan uses CommuniGate Pro's Content-Filtering API techniques to intercept emails & scan them.

Q. Will MailScan disturb my anti-SPAM & mail-relay check functions configured on the Mail Server?

A. No.

Q. Does MailScan work with any version of Windows?

A. Yes.

The MailScan Server can only be installed upon a Win9x, WinME, WinNT or Win2000 platform however.

Q. After installing MailScan, do we need to reboot the machine?

A. Yes.

Q. I understand that I can install MailScan by itself just by 'double-clicking' the MailScan .exe file.

If I also have eScan installed on all of my other platforms (e.g. desktops), how do I configure MailScan to auto-update them (i.e. how do I install eServ - eScan's Management Console Program)?

A. eServ is, by default, installed when MailScan is installed. But it is kept disabled. In order to enable eServ, double-click on the circular eScan Management-Console icon and select the "Start FTP Server" and "Start Announcement" options.

Q. I see 4 (four) icons on my task-tray bar, after installing MailScan and eScan. What are these? Are these required?

A. The four Icons are as follows:

- a) The white envelope icon controls MailScan functions.
- b) The Red Shield icon is the eScan AntiVirus Monitor, responsible for controlling the AntiVirus functions.
- c) The green 'e' icon controls the automatic updates of eScan.
- d) The circular, eScan Management-Console icon, controls the distribution and sharing of updates to workstations and MailScan itself.

Q. What is the EICAR Test Virus?

A. EICAR stands for "European Institute for Computer AntiVirus Research". This organization has developed a small test string to help organizations test AntiVirus packages. The EICAR test virus is harmless. To get more info, visit <http://eicar.com>

Q. Why do I see multiple instances of MailScan running in the background? Is this normal?

A. Yes. These are MailScan "Process-threads" which will start if anytime an email is to be scanned. They will also "die" automatically after 5-minutes, if no activity is assigned to them.

The number of such "Process-threads" depends on the setting in MAILSCAN.INI, MaxThreads=, parameter.

Q. When installing MailScan, I did not install eScan. Now I want to install eScan also. Do I need to re-install MailScan?

A. No. To now install eScan, go to [program files\mailscan] directory and run the program LAUNCHIT.EXE. This will then install eScan for you.

Q. Can eScan be disabled? I am already using another AntiVirus Software product - can I use this instead of eScan?

A. Whilst eScan can be disabled, many of the features supported by MailScan (including those of proper reporting), depend upon eScan functionality.

Many of these features, such as "automatic Internet check" and "Incremental updates" (provided via eScan) gives MailScan

its "ultimate edge" over any other package.

We therefore strongly recommend using eScan.

Q. Can I change my default eScan settings?

A. This is not recommended - the eScan settings for MailScan have been tuned to achieve maximum throughput and efficiency.

Q. I have made a VBS/JS file for my company. If I send this VBS file to any of our email addresses, MailScan deletes the file, thinking it to be a virus of some sort. How do I prevent this from happening?

A. For Incoming email, Run 'MailScan Admin'. Select the checkbox "Quarantine Unsafe Attachments". This will ensure that any VBS or JS attachments are "quarantined" rather than deleted.

Please note that this approach could be dangerous to your network.

Another way will be to edit the MAILSCAN.INI file and set the parameter "ReservedAttachmentsExcluded=" in the [General] section to the file you want (this is a comma separated list). Henceforth, the attachments listed on this line will be ignored by MailScan's "Unsafe Attachments Engine".

Q. Does MailScan scan the body of emails?

A. MailScan does not scan the body of `Plain Text' format emails, as these cannot carry Viruses, Macros or the like.

However, if the body of the email is using the HTML format, it is scanned.

Q. Does MailScan Scan inside ZIP files?

A. Yes.

Q. Can MailScan handle ZIP files in Transit?

A. Yes. If you have enabled the option "Uncompress Files", MailScan will uncompress the ZIP, check the files inside the zip for objectionable content and then take any appropriate action.

If the option to "Uncompress Files" is not enabled, ZIP files will still be scanned. However, if an infection is found inside the ZIP file, the entire ZIP file will be deleted, not disinfected.

Q. Other than ZIP, which types of Archives does MailScan Virus Scanning support?

A. ARJ, CAB, WiseSFX, WiseSFX Dropper, GZIP, Embedded, MSO, Embedded PowerPoint inflate, Tar, LHA, RAR, ProCarry, DiskDupe, TeleDisk, DiskImage, WinBackup, Effect Office, UPX, CreateInstall, Inno Installer, Stardust Installer and SetupFactory.

This list is continuously updated so that, provided MailScan and eScan are kept updated, the range of formats

supported will automatically remain current.

Q. Does MailScan Scan inside compressed-executable files?

A. Yes.

Q. What decompression formats are supported by eScan?

A. SCAN/AV, Diet, Apack, AVPACK, Com2Com, Com2Txt.Nide, Com2Txt.Comt, Com2Txt.Dandler, Com2Txt.Tseng, Com2Txt.XP, Com2Txt.Yaaa, COMPACK, Crypt, Crypt.Dismember, Crypt.Alex, Crypt.C-Crypt, Crypt.ComLock, Crypt.Hac, Crypt.Quarantine, Crypt.THC, Crypt.USCC, Elite, Epack, Exe2Com, ExePack, HackStop, Jam, LzExe, LzCom, MegaCrypt, PGMPAK, PkLite, Pksmart, Protect.2.0, Protect.3.0, Protect.4.0, Protect.5.0, ProtEXE, Rerp, Rjcrush, Scramb, SCRNCH, Six-2-Four, Syspack, T-Pack, Tinyprog, Trap, TT, UCExe, UPD, UPX, Vacuum, WWPack, EncrCom, Mscan-vac, DebugScript, VBSCcomment, ASPack, BJFnt, CodeCrypt, CodeSafe, Exe32Pack, Neolite, PCPEC, PECompact, PE-Crypt, PECrypt32.Kila, PE-Diminisher, PE-Pack, PE-Protect, PE-Shield, Petite, Shrinker, SMT-protect, VGCrypt, WWPack32, Html2Rtf, ARF, AVL, CPAV, Crunch, Scrambler, Crypt.a, CryptCOM, CryptCOM.b, Dropper.b, Dropper.c, Dropper.d, F-XLOCK, Faila, FileShield, ICE, MAV, Protect.1.0, Protect.2.0, CryptGeneric, Exe-embedded, MS TypeLib, Com2Exe, ObjectModule, HDD Image and Boot BIN Image.

This list is continuously updated so that, provided MailScan and eScan are kept updated, the range of formats supported will automatically remain current.

Q. Does MailScan Scan & Clean inside Outlook Express TNEF (WINMAIL.DAT) attachments?

A. Yes.

Q. What exactly is "HTML.SecurityBreach.2"?

A. Many times MailScan will delete an HTML-format email with the warning message "HTML.SecurityBreach.2".

HTML pages that contain the initializing "Scriptlet.TypeLib" ActiveX object, eScan (AVP) produces message "suspicion: HTML.SecurityBreach".

The "Scriptlet.TypeLib" object has a vulnerability that may enable a script to write files on to the local computer.

This breach is used by many trojans and worms like I-Worm.KakWorm, I-Worm.BubbleBoy and others.

For more information on this vulnerability, please read the article:
<http://support.microsoft.com/support/kb/articles/Q240/3/08.ASP>

We strongly recommend that anyone using Internet Explorer 5.x should install the Security update available from :
<http://www.microsoft.com/technet/security/bulletin/ms99-032.asp>

Q. What action does MailScan take when a Virus infected email is seen?

A. The email is cleaned and then passed-on to the Mail Server

application. In other words, the SMTP Server or POP3 Client will see a "cleaned" message.

Q. What happens if we have instructed MailScan to delete the email having harmful-content?

A. In this case, MailScan will generate a "dummy email" which will say that the "eMail has been deleted at the Server as it included restricted contents".

Q. Can MailScan be configured to quarantine the message instead of deleting it? What other alternatives do I have?

A. You can either quarantine the message, delete the message or forward the message to the Administrator.

Q. My email server is just an email server. There are no files passing through, no disks are ever put in. The computer is not used for anything else.

I do not want eScan software scanning my drivers, and everything else. How can I configure eScan and MailScan to avoid this overhead?

A. Just click on Start - Programs - eScan for Windows - eScan for Windows click on Monitor - click on ... of User-defined Remove all entries - EXCEPT *.ATT and *.COM Click on OK - click on Apply.

Now eScan will scan only the emails. Other parts will not be touched by eScan.

Q. I do not want to see any of the eScan icons on my task-tray. How can I set this up?

A. Run Regedit

Go to HKEY_LOCAL_MACHINE\Software\G Data\AVKWaechter Set the value of Tray to 0 (it will be 1). Reboot & you will not see any of the eScan icons.

Q. I have installed MailScan on my email Server. But on sending the test EICAR virus, I do not get any warnings! What changes should be done on MailScan?

A. MailScan, by default, sends warning messages to SMTP host 127.0.0.1. If your Mail-Server's port 25 is *not* bound to 127.0.0.1, than warning messages will not come.

Click on Start - MailScan - MailScan Administrator.

Click on Admin - Scanner Administration.

Click on Local Domain button.

Type the IP number of your MailScan machine in the textbox titled "Warnings to SMTP Server"

Click on Save and Exit out of MailScan Administrator.

This should solve your problem.

Q. When the auto-update runs there is activity showing in the WWW proxy in WinGate. It appears that MailScan is trying to go to <http://www.microworldsystems.com/sendinfo>. Any ideas why the auto update would try to go to that URL?

A. <http://www.microworldsystems.com/sendinfo/index.htm> is a page which has the date and time of the last updated file.

MailScan Auto-Updater downloads this information after a scheduled interval to check whether new updates have arrived. Once MailScan gets this info, it then contacts one of the many FTP servers to download the latest update.

Microworld's FTP server is the first FTP-server to get updated. Updates are mirrored to all other FTP servers from our server.

If you disable Automatic Updates, the access to sendinfo will stop.

Q. Though MailScan catches viruses properly, I do not get warning Messages! What could be wrong?

A. The following possibilities are there:

1. MailScan, by default, sends warning messages to SMTP Server on 127.0.0.1 port 25. It is quite possible that your Mail-Server does not give SMTP Services on 127.0.0.1. If this is so, please start MailScan Administrator, Go to Scanner Administration, Click on Domains and give the machines actual IP address in the field "Warning to SMTP Server".

2. MailScan, by default, sends warning messages with From: as postmaster@primary_domain.

Your Mail-Server might not be having postmaster as a user name & hence is not accepting warning messages.

Please create a user called Postmaster or change the From: in MailScan. To change the From: address in MailScan, start MailScan Administrator - Admin - MailScan Messages and type the From: email ID in the field: "Warning Mails From User".

Q. After installing/upgrading MailScan on 95/98/Me, my machine does not shutdown properly. What should I do?

A. Pls reboot ur machine in Safe Mode and then restart your machine. This should solve your problem.

Q. MailScan has expired and I get the "Please renew your MailScan subscription" message from MailScan. How can I stop this message?

A. Edit the file MailScan.ini. Here, you will find a section
[UpdatedMessageToAdmin]
Enabled=1
Filename=update.adm

Just set enabled to 0 and save the file. This should solve the problem.

Q. In case of content-scanning, is there any option that allows for the message to be delivered (as addressed) and a copy of the message to be sent to the administrator?

A. Yes. Run MailScan Administrator

Click on Scanner Administration

Advanced

Attachments Control

Enable - In case of reserved contents, send original mail to user also.