

User Guide for

MAILSCAN 3.X

FOR LAN-PROJEKT WINPROXY

Basic information

We recommend program **MailScan** as antivirus solution for **WinProxy**. Antivirus control is performed in real-time and that is why **WinProxy** sends and stores emails into local mail boxes already virus free. Thanks to transparency **MailScan** can be run together with **WinProxy** on the same PC without conflicts.

MailScan is world-first antivirus working in network layer, so that it works transparently as a gateway without difficult configuration. It's a stand-alone product with settings, which have no influence on **WinProxy** settings.

Program **MailScan** differs from other antivirus programs by its distinctive added value. Besides antivirus control it performs content filtering and mail scanning, which could be greatly appreciated by firm owners. It is possible to automatically scan e-mails content against special keywords or block e-mails from certain domains (spammers, competitors...).

LAN-PROJEKT is authorized **MailScan** distributor for both **WinProxy** users and for users, who will decide to purchase **WinProxy** in the future. **WinProxy** users will thus have several advantages (special prices, licence extensions..)

Licence Policy

Licence policy of **MailScan** is different from **WinProxy**. Price of **MailScan** is based on number of **WinProxy** local mail boxes. Price is then made according to No. of mailboxes and different ranges (1 - 5 mail boxes, 6 - 10 mail boxes atd.). Price for one user is lower when version for more users is selected.

Product **Mailscan** can be used free for 15 days and after this trial period it must be activated by entering activation key otherwise it will stop working.

Price List

For current price list see <http://www.winproxy.net/price.html>

Instalation

Program **MailScan** must be installed on PC with direct Internet accesss and it's also PC where is or will be installed **WinProxy**.

Instalation starts running installation file named MSWP.EXE from CD or downloaded from <ftp://ftp.lanprojekt.cz/pub/winproxy/mswp.exe>

Registration

Program **MailScan** can be distributed free of charge as time limited demoverision. Product **MailScan** can be used free for 15 days and after this trial period it must be activated by entering activation key otherwise it will stop working. Activation key can be entered at window **Help / Licence Information**.

Technical support

We offer free technical support for current or future **WinProxy** users at email address winproxy@winproxy.net

Welcome

MailScan for Mail Servers provides provide a blanket, round-the-clock security screen against viruses delivered mail server. After the software is installed it is always active. You carry out your normal work, surf the net, exchange mails, download your favorite programs, run them and so on, secure in the knowledge that you are protected from virus attacks.

- [About this Guide](#)

About this Guide

This chapter provides details about the following topics:

- [Audience](#)
- [How this guide is organized](#)
- [Typographical Conventions](#)
- [Mouse Conventions](#)
- [Keyboard Conventions](#)
- [Contact Us](#)

Audience

This Guide is for system administrators and users involved in installing and using the application.

How this guide is organized

This guide is organized into separate books and chapters. The first four books describe basic tasks like getting started, navigation, Installation etc. MailScan Administrator provides all details to run MailScan for Mail Server. Each screen and field occurring in the user interface is explained in detail along with the relevant screen shots.

Overview: Provides details of MWL technology (MicroWorld Winsock Layer) technology on which our products are built and MailScan Products, which gives a break up of different MailScan products and modules available with them. Also listed are detailed Features of MailScan.

Installation: Gives the Software and Hardware requirements to run the application along with Prerequisites you have to complete before the installation. Details of Installation Process are given along with screen shots.

Getting Started gives information about a typical screen, its components, types of fields, dialog boxes, tab pages and how to validate them.

MailScan Administrator: Provides detailed information to run MailScan. There are three main menus: Admin, View and Help. Admin includes details to run: Scanner Administration, Content Control, Compression Control, MailScan Messages, License Information, Virus Test Mail and Send Debug Information. View provides information to: View Log Files, Flush Logs, MailScan Reports and Help includes information to Send EICAR Virus Test Mail, MailScan Help, License Information and information to Change Password.

Appendix Provides answers to Frequently Asked Questions. Also given are details on availing our Support, tips on Safe Computing, a brief History of Virus and a Glossary of terms occurring in the guide. Included is an Index of words occurring in this guide.

Typographical Conventions

The following typographical conventions are used in this guide.

This	Represents
Bold	A Menu or a menu option. When enclosed in “ “, the name is as displayed in the screen.
“ “	A long name is denoted by the first few words. It is enclosed between ‘ ‘.
SMALL CAPS	Buttons on dialog boxes/child windows.

<i>Italics</i>	Entry Fields in dialog boxes/child windows.
Type	Information you need to enter.
<u>Hyperlink</u>	Is a hyperlink. Click to access related topics.
<u>Tasks</u>	Represents a key task of feature.

- When you have to navigate between menus the following convention is used: **menu > menu >...**

For e.g. **MailScan > Monitor > Settings**. Means: in MailScan, **select** (click) the Monitor menu and **choose** (click) Settings.

Mouse Conventions

The following table describes some of the terms referred to throughout this Guide:

Term	Means
Point	Move the mouse until the tip of the mouse pointer rests on the screen object or area you want to point to.
Click	Point to the item you want to select and then press and release the mouse button immediately without moving the mouse.
Double-click	Point to the item you want to activate and then rapidly press and release the mouse button twice without moving the mouse.
Drag-and-drop	To click an item on the screen, move the mouse keeping the mouse button clicked (drag) and releasing the mouse button (drop).

Note

The mouse has two buttons. The left button is used for most actions. All the above actions can be done, with both the right as well as the left mouse

button. By default, use only the left mouse button unless specified otherwise. This book assumes that you have not swapped the left and right mouse buttons using the Control Panel.

Keyboard Conventions

The following conventions are used to describe keys and key combinations:

- Key names appear in small capital letters and are referred to by their names. For example, “press SHIFT” means press the key labeled “Shift.”
- A plus sign (+) between two key names means you hold the first key while you press the second key. For example, “press CTRL+C” means hold down the CTRL key, and then press and release the C key.
- A comma (,) between key names means you press and release the first key, and then press and release the second key. For example, “press ALT, M, P” means press Alt and release it, press M and release it and press I and release it.

Related Topics

Provides a cross-reference to a related topic.

Note

Provides additional information about a certain topic.

- Bulleted lists provide information or indicate procedures with steps

that you carry out sequentially.

Contact Us

If you have any queries about our products or have suggestions and comments about this guide, please send them to:

LAN-Projekt
Placheho 17
301 26 Plzen
Czech Republic

Tel +420 377 993 155

Fax +420 377 993 159

For sales enquiry, e-mail: sales@winproxy.net

For support enquiry, e-mail: winproxy@winproxy.net

For more information about our products please visit
<http://www.winproxy.net/>

Overview

About MailScan

MailScan for LAN-Projekt WinProxy is a comprehensive Content Security and Traffic Scanning software package that checks the content in e-mails and its attachments for viruses. Checks are done for viruses, restricted words and phrases, embedded objects such as Java applets etc, before the e-mails reach you. It thus offers unprecedented "real-time" security at various levels in any organization, from the Internet Gateway to your desktop. It is also synchronized with the Internet to provide real-time security for your organization. It offers a Centralized Security Management System. This feature allows your network administrator to configure Global Security Policies for the organization from a single console.

MailScan is also designed to understand different file types, data streams and compression formats. It can look inside data streams and identify complex file architecture. It has a user-friendly interface and you can automatically download Updates from our download site. This gives you the "ultimate convenience and confidence in computing".

This chapter provides details about the following topics:

- [MWL Technology](#)
- [MailScan Products](#)
- [Features of MailScan](#)

MWL Technology

Our products are built on the **MicroWorld Winsock Layer Technology** (MWL) (patent pending). This technology gives products a more advanced means to protect your computer from virus and other attacks. When you connect to the Internet, you do so through the Windows Socket (**Winsock**) layer. The Winsock layer acts as an interface between your computer application and the Internet. It does its work very efficiently and you can surf the net, download programs etc unhindered. But it never distinguishes between a virus infected file and a clean one.

Our **MWL** layer sits on the Winsock layer. It checks and analyzes all traffic between your system and the Internet. All e-mails, attachments, downloads etc are scanned before they enter your system thus providing you a secure blanket. Our applications have a vast database of all known viruses and other threats. MWL ensures that any files with these known threats are barred from entering your system.

Virus infected files display suspicious forms, content or have strange codes. MWL recognizes any file, e-mail, attachment etc, which look strange or suspicious. Such objects are barred from entering your system. Products made by other manufacturers do not stop threats from entering your system. They allow them entry, permit them to infect files and then wait for the obsolete Anti-Virus software you have installed to identify them. IF and when these threats are identified, then the obsolete Anti-Virus software tries to disinfect the files. The whole process is subject to jargon like 'possible scenarios' 'threat perception' etc. You loose priceless data and spend valuable time in removing a threat, which should not have been allowed into your system in the first place.

Producer endorses the timeless proverb "prevention is better than a cure". Stop the threat from entering your system. There is no way a threat can bypass the MWL technology and compromise your system. The first time you install our product, our Anti-Virus software thoroughly checks your system and removes all known virus. If new or unknown threats are discovered, you can delete or quarantine these files. Mail us a copy of the file and we will get back to you with possible means to tackle them.

We provide constant updates in dedicated download sites to tackle new threats. These updates are typically up to 10 KB and download very fast. You can set up our Anti Virus application to automatically connect to these sites, download updates and run them on your system.

MailScan Products

MailScan products are created for specific mail server types. Given below is a list of different MailScan products. Product name has two parts: first part denotes the latest MailScan version number and second part denotes the mail server for which it is used. For e.g. MailScan 3.6a for Avirt means MailScan version 3.6a is the latest product for Avirt mail servers. The mail servers are created or marketed by others.

- MailScan 3.5a for 1st UpMailServer
- MailScan 3.6a for Avirt
- MailScan 3.5a for CommuniGate Pro
- MailScan 3.5a for Internet Anywhere
- MailScan 3.6a for LAN-Projekt WinProxy
- MailScan 3.5a for Lotus Notes
- MailScan 3.5a for Mail Server
- MailScan 3.5a for MailMax
- MailScan 3 for Mdaemon
- MailScan 3.5a for Merak
- MailScan 3.5a for Mailtraq 2
- MailScan 3.5a for Microsoft Exchange Server
- MailScan 3.5a for NetNow
- MailScan 3.5a for PostMaster
- MailScan 3.5a for ShareMail Pro
- MailScan 3.5a for SMTP Servers (for non Windows platforms)
- MailScan 3.5a for SpearMail
- MailScan 3.5a for VOPMail
- MailScan 3.5a for VP0P3
- MailScan 3.5a for WinRoute

Features of MailScan

The main features and tasks MailScan does for you are:

Content Security: Checks files and e-mails for restricted content. It restricts infected files from entering the system.

E-mail Content Scanning: Checks the e-mail body for confidential data (specified keywords, phrases, etc.), file size (you can specify that files above a certain size should not be allowed out) and prohibited content.

Detects Viruses on-the-fly: Protects applications and Operating Systems by detecting viruses as you download files from the Internet, browse Websites, copy files from floppies and CD ROMs, start applications from the network or open Microsoft Word or Excel documents.

Unparalleled Virus detection for complete protection: Offers comprehensive protection using the world's best Anti Virus Scanning Engine.

Highly Effective Heuristic Code Analysis: MailScan's heuristic algorithm is able to detect and remove unknown viruses.

Easy to Manage And Control: Easy to manage and control with features such as automated installation, centralized deployment, automatic downloads of Updates and Enterprise Logging and Messaging.

Very simple and easy to use: MailScan has point and click features. It automatically updates its security policies from the Internet. This frees you from the hassle of keeping track of latest updates.

Centralized Security Policy Management: MailScan configures global security policies for your organization and automatically refreshes servers within the company with pre-defined security policy.

Comprehensive Object Management: MailScan understands different file types, compression formats and data streams. It looks inside the Internet traffic and identifies complex architecture.

Fast Updates reduce download time: MailScan downloads the latest Anti-Virus Updates quickly and efficiently. Using an incremental update procedure, it downloads only the changes in the virus pattern file. This

ensures that downloads are restricted to only fresh items and you do not upload older material.

Safe e-mail Virus Scanning: E-mails that you receive in your POP3 mailbox (Outlook, Netscape, Eudora, etc) are automatically scanned for virus. Personal Folders that allow you to store your e-mails and other data locally are also scanned for viruses.

Centralized Messaging Options: MailScan allows System Administrators to collect scanning and Anti Virus activity reports centrally, consolidate them and e-mail them (via SMTP) to any e-mail ID. This helps them to keep track of outbreaks and their source.

Automatic Central Logging: MailScan clients automatically send their logs to the MailScan Server, which in turn keeps full reports of all virus incidents on the company's network.

Extended Security Features: Self-checks of all its files make MailScan literally tamper-proof.

An Expert On-Line Help System: MailScan provides on-screen support to simplify software installation and update procedures.

On-the-fly Disinfections: When viruses are detected, they are automatically removed by MailScan.

MailScan Tasks

MailScan has a group of tasks for Content Security and Anti-Virus scanning. By default, the software is configured to execute them automatically. You can run some of the tasks manually. This section provides a list of different tasks, manually run with MailScan. Detailed explanations of the tasks, meanings of fields etc are described in successive individual chapters.


- [Topics in MailScan Tasks](#)

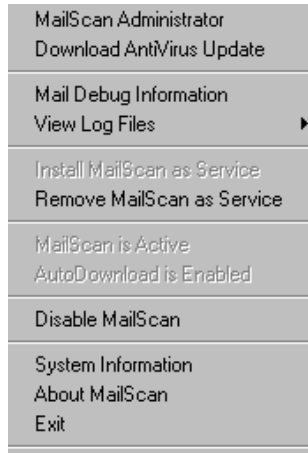
Topics in MailScan Tasks

The chapter provides details about the following topics:

- [To launch MailScan tasks](#)
- Details of MailScan tasks

To launch MailScan tasks

- After the application is installed, in the application status bar, right click on .
- A drop-down menu shown below is displayed. Tasks are displayed as links. Click on the task to open it.



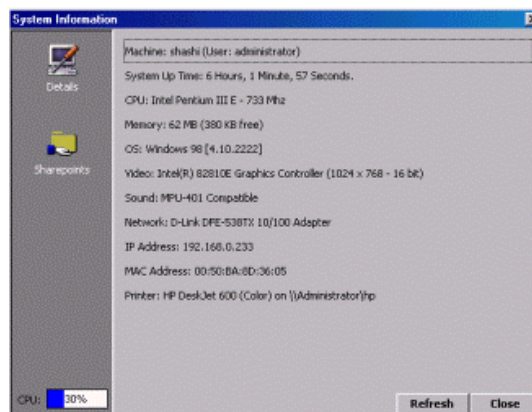
Details of MailScan tasks

To access the tasks, please refer to [To launch MailScan tasks](#)

- Details of each item are explained in the following table.

Task Name	Function
MailScan Administrator	Starts MailScan Administrator on your system by which you can modify the default settings. Once the software is installed, it is activated automatically at system startup. For more details, refer MailScan Administrator
Download Anti-Virus Update	Begins auto-download of Anti-Virus updates.
Mail Debug Information	Sends e-mail of bugs and other problems to the system administrator. For more details, refer Send Debug Information .
View Log Files	Allows you to view log files that display details of MailScan activity in your system. For details, refer View Log Files .
Install MailScan as	By default MailScan is installed as a Service and this button is disabled. This increases performance of

Service	MailScan.
Remove MailScan as Service	You can install MailScan as an application. This provides a command line (DOS prompt) window that you use to control and analyze MailScan activity.
MailScan is Active	Button is disabled and signifies that MailScan is active and running.
Auto-Download is Enabled	Button is disabled and signifies that auto download of updates is enabled.
Disable MailScan	Disables or stops MailScan from running. Producer recommends that you exercise this option with forethought, as your mail server is unguarded when MailScan is disabled.
System Information	Displays details of system where MailScan is installed. Following screen is displayed. There are two links in the left frame: Details and Sharepoints .

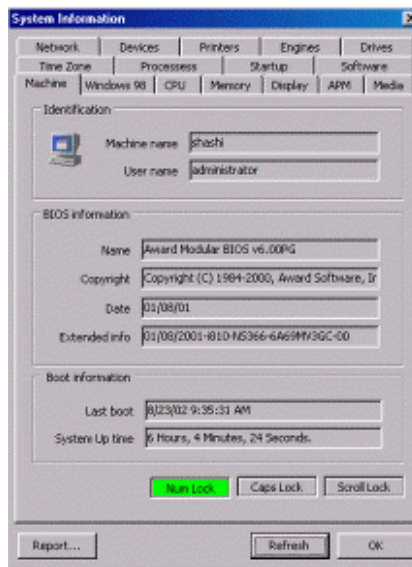


“Details”

Provides details of individual system components. Select the link to see Figure Details of System. There are different tabs pages. A brief description of each is given.

Machine All your system details are displayed. These include: machine identification, BIOS info, boot information etc.

Network Displays network details like: Network adapters, IP addresses, protocols, services, clients, and details of Winsock etc.



Devices Displays all software and hardware devices connected to the system.

Printers Displays all printer devices like hard copy printers, pdf writers etc and the port they connect.

Engines Shows names of all database engines, drivers and devices on your system.

Drives Details of drives on the machine, CPU size and free space, pattern of use etc. are displayed.

Time Zone Displays time zone details where the system is located.

Processes Displays list of all active applications running on your system.

Startup Displays applications loaded at start up.

Software Lists all software's, installed and available on the system.

Windows 98 Displays operating system details like name, version etc. Also listed are the default application folders of the system, their path and location, environment, etc.

CPU Displays details of the central processing unit of your system. Details like identification, features, cache, etc are given.

Memory Shows details of system memory like: memory measuring, memory utilization memory properties, etc.

are displayed.

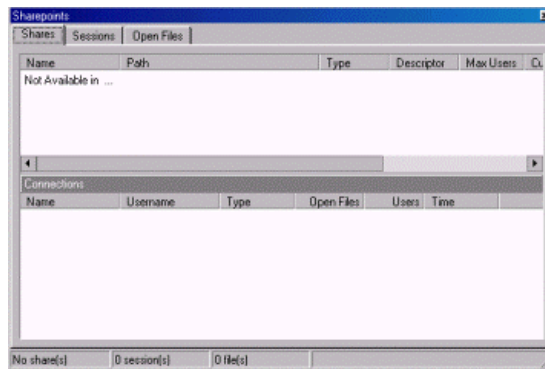
Display Gives details of adapters, its properties, capabilities etc.

APM Shows status of advance power management, battery status, etc.

Media Lists names of available devices and sound devices.

Sharepoints

Provides details of components of your system, accessed by other systems. Select link to see following screen. The features are only enabled for Win NT/2000/ XP. There are three tab sheets.



Shares There are two frames. Top frame, displays all folders shared by your system with other machines. Bottom frame shows all list of all machines connected to your system.

Sessions Displays list of machines connected to your system. Details like username, type, files accessed etc. are shown.

Open Files Displays list of all files that are accessed, name of machine accessing the file etc.

About MailScan

Displays splash screen of MailScan installed on your system.

Exit

Select the link to exit.

Installation

This chapter provides information about the software and hardware requirements of your machine for using our products and provides step-by-step instructions on installation.

- Topics in Installation

Topics in Installation

This chapter provides details about the following topics:

- Software and Hardware Requirements
- Prerequisites for Installation
- Installation Process

Software and Hardware Requirements

Your system should have **Windows 95 (II nd Edition)/NT** and Internet Explorer 4 or above installed.

Your system should have minimum of **64 MB RAM, 50 MB** of free hard disk space and a CD ROM player.

Prerequisites for Installation

Before installing the software ensure that the following are done:

- Operating System [version and build and the Service Pack if applied.
- Ensure that the Mail Server is installed and configured.
- Uninstall other Anti Virus software including previous versions of our products.
- Check for the largest drive/partition and install MailScan/MailScan on that drive/partition.
- Valid Username and Password for Logon on the PC and the Net Connectivity.
- Primary Domain name of the Mail Server (normally this is read automatically from the Mail Server Configuration when you install MailScan).
- Administrator or Postmaster ID or e-mail Address.
- Other software like Proxy; Firewall, DHCP installed on your system and third party software used for downloading.

- SWAP Partition Size.

Installation Process

Installation is very simple, a point and click operation and done using the built-in install wizard. A user-friendly interface prompts you and presents a range of choices. Instructions are displayed in the screens that give you specific information. To abort installation, select “Cancel” in any of the screen. This section gives the step-by-step installation process.

- The software is sent to you in a CD. Load the CD in the player and open the CD Rom directory.
- Select “**autorun**” icon. Screen in Figure 1.1 is displayed. This is the start up screen for installing the application.



Figure 1.1 Install – Opening Screen

- In Figure 1.1, select **Next** to begin installation. Screen in Figure 1.2 is displayed.
- This screen shows the license agreement between you and Producer. Read the instructions and select “**Yes**” if you accept the terms. Select “**No**” if you do not accept the terms in which case the installation process is aborted.



Figure 1.2 License Agreements

- If you select “**Yes**”, screen in Figure 1.3 is displayed.
- You select the directory to install the application. The default path is displayed. To change the location, browse your PC and select the directory.

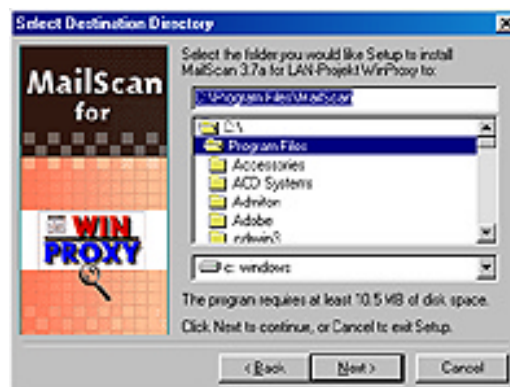


Figure 1.3 Select Destination Directory

- Select “**Next**”. Screen in Figure 1.4 is displayed.
- The application is ready to be installed. Select **Install**.

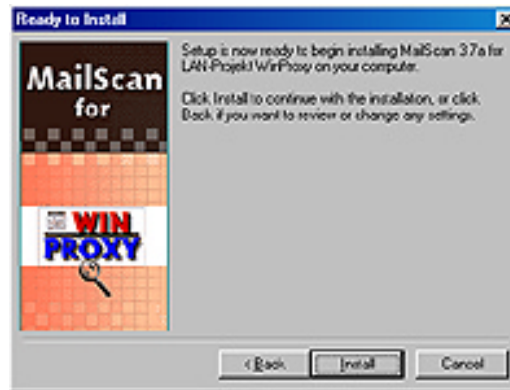


Figure 1.4 Begin Installation

- The software is copied and uploaded into the directory you have selected. A folder with the applications name is created.
- Enter the primary domain name and select Finish.

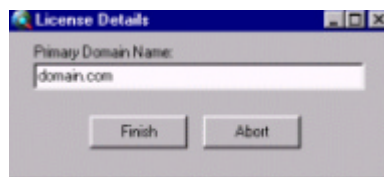


Figure 1.5 Installation progress bar

- Screen in Figure 1.6 is displayed.

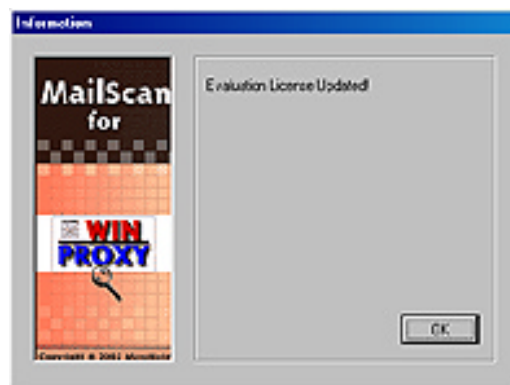


Figure 1.6 Evaluation License

- After the files are copied, MailScan makes the program groups and necessary changes to the required files. Screen in Figure 1.7 is displayed.
- Use the scroll bar in the screen to view the full text and select **Next**.

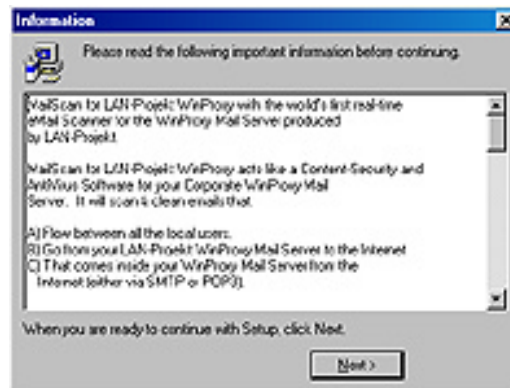


Figure 1.7 Important MailScan Information

- You must restart your system. Click **Finish** in Figure 1.8.

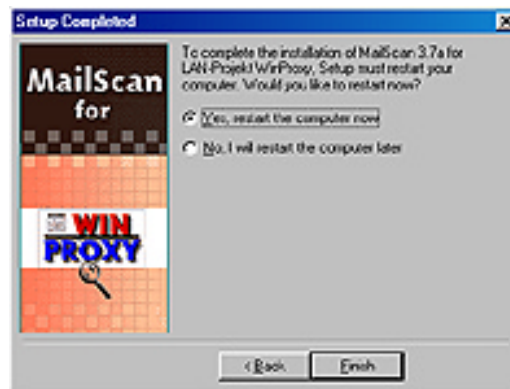


Figure 1.8 Restart Computer

- You have installed the software on your machine.
- Reboot the machine so that the software initializes

Getting Started

This chapter gives details of standard conventions used in this guide. Also included are components of a typical user interface, how to navigate the screens, meanings of various symbols and buttons, types of fields and how to enter values in them.

- Topics in Navigation

User Interface

User interface is the front end of the software. The software is made of different screens. You carry out tasks; enter values, set preferences, etc., using screens. This section explains the components of a typical user interface.

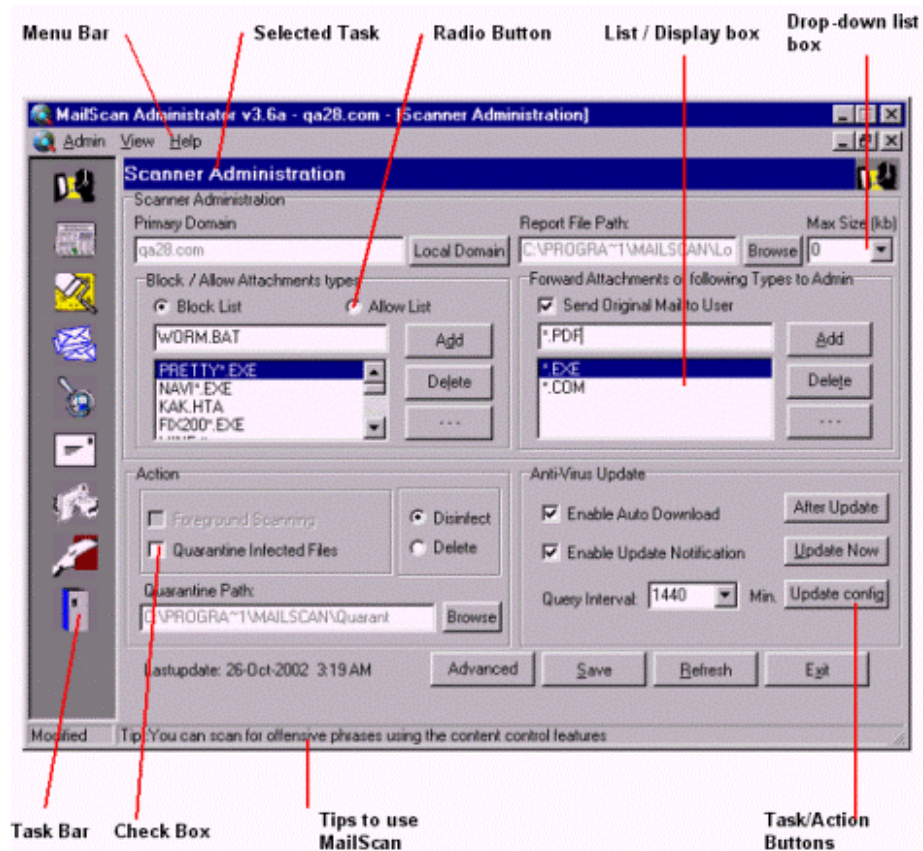


Figure 2.1 Typical User Interface

Screen Components

Typical screen components are explained below:

Screen Component	Function
Menu Bar:	These are the main menus that contain similar group of sub-menus. You perform specific tasks with them. The menus and their sub-menus are explained below.
Admin	Performs MailScan Administration related tasks. Has the following sub-menus: Scanner Administration : Perform scanner administration tasks. Content Control : Perform Content Control tasks.

[Compression Control](#): Configure attachment auto compress tasks.

[MailScan Messages](#): Set customized messages and alerts.

[Scan Control](#): Set e-mails IDs from whom e-mails should be scanned, deleted or exempted from scanning.

View	Allows you to view log files and MailScan reports.
Help	Allows you to access on-line help and other features of MailScan.
Selected Task	Current task name you are running or the task name that is open is displayed here.

Task Bar: Carries icons of tasks. These are shortcuts to quickly start a task and run it. Tasks and their icons are listed below:

MailScan Icon represents MailScan.



eScan Content Security and Anti-Virus Icon signifies that eScan Content Security and Anti-Virus is active and running. The settings for eScan are preconfigured for best performance and you cannot open or modify the application.



Scanner Administration Perform [Scanner Administration](#) tasks.



Content Control Perform [Content Control](#) tasks



Compression Control Configure attachment auto [Compression Control](#) tasks



MailScan Set customized [MailScan Messages](#) and alerts

Message



Scan Control

Set [Scan Control](#) for e-mails IDs, from whom e-mails should be scanned, deleted or exempted from scanning.



License Information

Provides information to enter [License Key Information](#) to register MailScan.



Virus Test Mail

Run a [Virus Test Mail](#) to see if MailScan is configured properly in your system.



Send Debug Information

[Send Debug Information](#) to system administrator.



Exit

Exit from MailScan. It continues to run in the background.



Action Buttons

Help you perform and execute functions related to tasks. Refer to the section “Action Buttons” for detailed explanation about different action buttons.

Action Buttons

These enable you to perform tasks and carry out work related to a feature. You select preset values or ask the software to accept a value, which is used to run the application. Some of the action buttons appear on a few screens

and dialog boxes. This section provides information about these buttons and explains their significance and use. Detailed explanation is provided in the section where they occur.

Action Button

Function

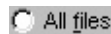
Check Box



Allows you to select a function of the screen. There are two parts: on the left is the check box and on the right is the function it performs. To begin with the box is blank. To enable the function, click in the check box. A ✓ symbol appears in the check box meaning that you have selected the function shown on the right side. To deselect, click again in the box and the symbol disappears. Producer assigns certain default selections and some of the check boxes are enabled when you start the application.

Some check boxes are enabled after other check boxes, radio buttons, etc. are selected.

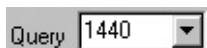
Radio Button



Allow you to select a function of feature. There are two parts: on the left is the radio button and on the right is the function it performs. To begin with the button is blank. To enable the function, click on the radio button. A • symbol appears in the radio button meaning that you have selected the function shown on the right side. To deselect, click again on the box and the symbol disappears.

Some radio buttons are enabled after other check boxes, radio buttons etc are selected.

Dropdown list box



The field has two parts. Label on left/right side tells you what the function does. Box on the right has preset values hard coded by Micro World. You can assign only one of them. To assign a value, select the arrow to view the list and choose one of them.

Selection Button

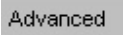
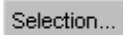







In some screens, when you move the mouse over the menu tree, the cursor changes to a mouse cursor. You can drop the symbol over a file or folder and set it up for additional actions. To deselect, move the cursor over the object and click.

Browse


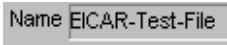


Allows you to browse your PC for a file or folder. It also opens a new dialog box.

	Allows you to make advanced settings. Select the button to open a new dialog box.
	Allows you to select files or folders and set them up for further action. A new dialog box is displayed and you make your selection in it.
	Add selections to the screen or dialog box.
	Change selections made in the screen or dialog boxes.
	Delete selections made in the screen or dialog box.
	Select to accept all changes done in a dialog box or screen
	Select to cancel changes made to a dialog box or screen

Entering Values

The user interface is typically point and click. You select preset values in the form of radio buttons; check boxes etc in almost all areas and screens. Values need to be entered in a few screens or dialog boxes. You enter values in fields. This section provides details about different fields and how to enter values for them. .

Field Type	Function
Editable Fields 	Fields where you enter valid values. To enter the value, click in the field and type. These fields can be mandatory, where in a value must be entered or they can be optional, wherein entry may be skipped. Producer recommends that all fields be validated. The software does not accept invalid entries and gives an error message.
Non-editable display fields 	Values for these fields are extracted from the records and displayed here. They are read-only and cannot be edited.

Dialog Boxes

These are provided in a screen and allow you to enter values or select among a range choices. They may have elements like drop-down list boxes, radio buttons, check bpxes, action buttons that open a new screen or dialog boxes, editable and non-editable fields, etc. Dialog boxes are displayed when specific buttons or selections are made. Following table shows a typical dialog box. The dialog boxes are explained in greater detail in screens where they occur.

**Dialog Box
Type**

Function

**Value
Entry**

This type of dialog box has a field where values are entered; a drop-down list box where preset values are selected and action buttons to enable or disable selections



Tab Pages

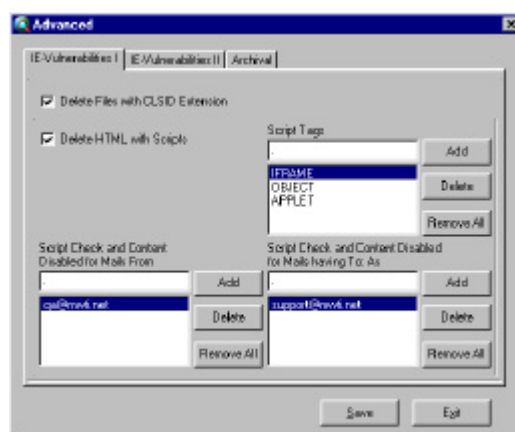
Tab pages are nested in a dialog box or screen. They are displayed when an action button or fields are selected. These perform tasks related to the main screen. They may have various components like action buttons, radio buttons, fields, links, etc.. The tab page is identified by a name that appears on the header area of a dialog box. To open a tab page, select the relevant tab name. Following table shows a typical dialog box with tab pages. The tab pages are explained in greater detail in screens where they occur

Tab Page Type

Function

Tab Page

This type of dialog box has tab pages. Each tab page may have a screen with radio buttons; check boxes etc., where values are uploaded. Make the appropriate selections and select the relevant action button.



MailScan Administrator

MailScan administrator feature of MailScan, allows you to monitor and administer Internet traffic flowing into or out of your mail server. You can set security policies to: check **e-mail** traffic for specific words or phrases like xxx, naked, etc.; prohibit or allow: exchange of specific attachment types, enable their auto compression, send warning messages to sender, receiver or others when the security policies are violated. A very important feature is **block** and **allow** access to specific **sites** or pages with restricted words.

New features that are added include Popup Filter menu, which allows you to block popup from being displayed on your screen and Browser CleanUp, which protects your privacy by removing tracks in your system that reveal details about sites you have visited

What MailScan Administrator does for you:

Offensive e-mails: It is a great tragedy that a productive tool like e-mail is used to send offensive messages. Offensive mails include words and phrases, which offend you senses. MailScan allows you to specify such words and phrases. Any e-mail, that has such words in the subject line or the body, can be blocked. You can even specify e-mail IDs that send such offensive mails. Such IDs are blocked. This feature even blocks **Spam's**.

Attachment Blocking Picture this: your employees e-mailing source

codes, company financial info, marketing plans, etc. to your competitors, as an attachment. MailScan allows you to block attachments of specific type like .doc, .exe, etc. from leaving or entering your organization. You can also set the option for auto compress of all outbound and incoming mails.

Scan Control: Allows you specify IDs of specific users or domains. You can monitor e-mails sent or recieved through these IDs

Warning Message: You can create customized messages that are sent when e-mails that violate your security ploicy are sent or recieved in your system.

There are three main menus on the tool bar:

- [Admin](#)
- [View](#)
- [Help](#)
-

Topics in MailScan Content Administrator

Topics in MailScan Content Administrator

This chapter provides details about the following topics:

- [Admin](#)
 - [Scanner Administration](#)
 - [Content Control](#)
 - [Compression Control](#)
 - [MailScan Message](#)
 - [Scan Control](#)
 - [License Information](#)
 - [Virus Test Mail](#)
 - [Send Debug Information](#)
- [View](#)
 - [View Log Files](#)

- [Flush Logs](#)
- [Mail Debug Information](#)
- **[Help](#)**
 - [Send EICAR Virus Test Mail](#)
 - [MailScan Help](#)
 - [License Information](#)
 - [To Change Password](#)

Important Terms in Content Administration

Alerts Message sent when a virus is detected in a mail or when the security policy is violated.

Attachment Types Depending on the application there are different types of attachments. It is identified by the file extension. A document created in MS Word will have the extension. doc.

Compress Files can be compressed by using the built-in compress feature. This packs the file tightly, without affecting the contents. Compressing a file and then mailing it conserves the available bandwidth.


Disclaimer When a mail that violates the security policy is detected, certain pre-set actions like delete, quarantine, etc., are carried out. In such cases, MailScan sends a notification message, called the disclaimer.

IE Vulnerability Internet explorer has certain loopholes or vulnerabilities. Virus and other threats can gain an entry into your system through these vulnerabilities. MailScan has features that can be configured to plug some of the loopholes.

Restrictive words/phrases Words like xxx, naked etc., which you do not want in your system are called restrictive words and phrases. MailScan, allows you to specify a list of such words. Any mail, which has such words in the subject or body, can be detected and further pre-set actions for such mails can be run.

Security Policy Refer to the rules that govern Internet traffic in your system.

To launch MailScan Administrator

- In the application status bar, right click on .
- In the displayed drop-down menu, select **“Start MailScan Content Administrator”**.
- Screen in Figure 3.1 is displayed.

This is the opening screen of Content Administrator. There are six menus or tasks displayed in the left panel. Select the menus, to view screens related to these menus. To execute tasks, select the respective buttons. The related screen is displayed. Brief description of the menus or tasks follows:

The next sections describe in detail about different tasks and how to validate fields.

Admin

This section provides details about the following tasks:

- [Scanner Administration](#)
- [Content Control](#)
- [Compression Control](#)
- [MailScan Message](#)
- [Scan Control](#)
- [License Information](#)
- [Virus Test Mail](#)

- [Send Debug Information](#)


Scanner Administration

The menu allows you to perform crucial tasks like: add local primary domain, configure settings for auto-download of updates, and plug Internet Explorer vulnerabilities that allow virus to enter your system. Certain types of attachments are prone to virus infections. This feature allows you to block or allow such e-mail attachments, to enter or leave your system. Auto compression of attachments is another feature that allows automatic compression of outgoing and incoming attachments.

Topics in Scanner Administration

- [To Add a Local/Primary Domain](#)
- [To block/allow attachments](#)
- [Auto-Download Updates](#)
- [To set time for updates auto download](#)
- [Set auto actions after update downloads](#)
- [General Config](#)
- [FTP Config](#)
- [HTTP Config](#)
- [UNC Config](#)
- [To Plug Internet Explorer Vulnerabilities](#)
- [To archive mails/attachments](#)

To Launch Scanner Administration

- In Figure 3.1, select .
- You configure settings as explained in the following table.

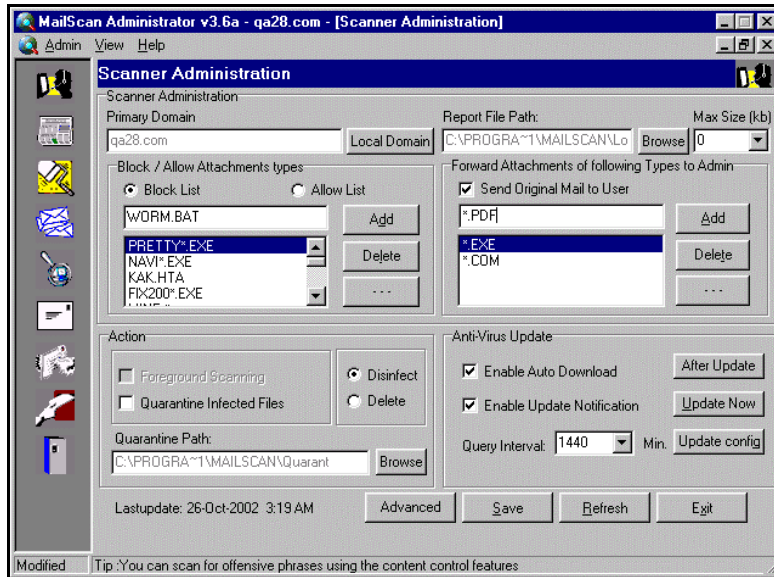


Figure 3.1 Scanner Administration

Field Name

Description

Scanner Administration This frame allows you to specify Scanner Administration settings.

Primary Domain

In a Win OS environment, the Primary Domain manages the master database of your domain and provides access to applications and resources. It serves individual machines and local domains.

Local Domain

Select the button to view **Domain Details** dialog box. You can set a range of local domains, and the port settings for SMTP and POP3 server.

Primary Domain: Primary Domain server name is displayed in the non-editable display field.



Local Domain: This is a server that acts as a back up domain server. The primary domain periodically sends copies of the master database. You can add any number of servers as a local domain. If required, the local

domain can be turned into the primary domain.

To Add a Local/Primary Domain: Enter the local domain URL in the field and select **Add**. The name is displayed in the list box. To make the listed local domain as a Primary Domain, select the name from the list box and select **Make Primary**. To delete a local domain, click on the name displayed in the list box and select **Delete**.

SMTP to Listen on Port: Port number of your mail server that receives mails from other domains (default 25).

POP3 to Listen on Port: Clients of your mail server connect to this port to receive e-mails (default 110).

Warnings To SMTP Server: Enter IP address of SMTP relay server. Notifications are sent to this server.

Warnings To SMTP Port: Enter port number of above SMTP server to which notifications are sent.

Authentication User Name: Enter user name for SMTP server authentication.

Authentication Password: Enter password for SMTP server authentication.

Enter the appropriate values and select **Save**.

Report File Path Location of log files and reports are stored in your system, the name and path of which is displayed in the field. Select Browse to choose a new location.

Max Size (kb) Maximmm size of the log file. Default value "0" signifies that the log file size is unlimited.

Block Allow Attachments You specify attachments that can be allowed or prohibited to enter or leave your system.

To block/allow attachments:

Block List Select the radio button to view or add to the list of all attachment types that are blocked from entering or leaving your system. The list is shown in the display box.

Allow List Select the radio button to view list of all attachment types that are allowed to enter or leave the system. The list is shown in the display box.



Display box has two frames. Bottom frame shows a list of attachment types. Based on the selection done for allow/block radio button, the list refers to attachments either allowed or blocked. These are non-editable display fields.

Top frame allows you to enter the attachment type that are blocked or allowed. To **add** an attachment type to the **block list**: select the radio button for Block List, enter the attachment type in the top frame and select **Add**.

To **add** an attachment type to the **allow list**: select the radio button for Allow List, enter the attachment type in the top frame and select **Add**. To delete a name from the list repeat the above process and select **Delete**.

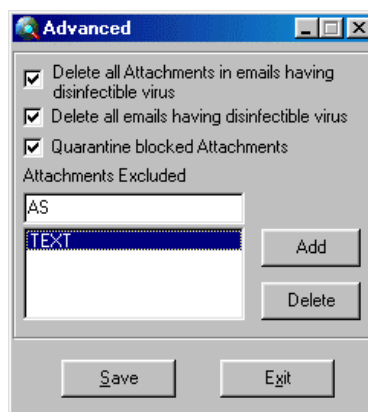


Select the button to view the dialog box shown below. You perform advanced tasks with it.

“**Delete all Attachments....**” Select the check box to delete infected attachments whose virus cannot be removed.

“**Delete all emails....**” Select the check box to delete infected e-mails whose virus cannot be removed.

“**Quarantine blocked....**” Select the check box to allow the software to quarantine the restricted attachments.



“**Attachments Excluded**” The field allows you to exclude specific attachments from the above actions. Enter the file type extension in the field and select **Add**. It is displayed in the display box.

To delete the item, click on it and select **Delete**.

Select **Save** and **Exit**.

Forward Attachments of following Types to Admin: When violations regarding barred attachments occur, this frame allows you to specify actions to be taken.

Send Original Mail to User

Select the check box to forward the mail that has restricted e-mail attachments to the person sending it.



The list box allows you to specify type of restricted attachments that are forwarded to the system administrators. There are two frames in the box.

The top frame allows you to enter names of attachment types and the bottom frame displays attachment types that are already included in the list.

To add an attachment type: Enter name in the top frame and select **Add**. It is displayed in the bottom frame. To delete a name from the list, click on the name in the display box and select **Delete**.

Add

Select the button to add the attachment type name, entered in the above field. The item is now added to either the block or allow list.

Delete

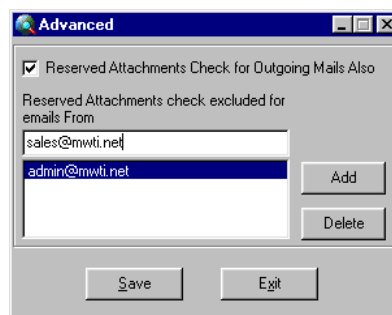
Select the button to delete the attachment type name, displayed in the display box.



The button allows you to specify if checks should be run on outgoing e-mails with attachments.

Reserved Attachments Check for Outgoing Mails

Also: Select the check box to check outgoing e-mails for any restricted attachments.



Reserved Attachments check excluded for emails

From: The list box allows you to enter e-mail IDs, whose outgoing mails can include restricted attachment types.

To specify e-mail ID whose attachments can be allowed:

Enter the e-mail ID in the field above the list box and select **Add**. The name is displayed in the list box. To delete an e-mail ID from the list, click on the name and select **Delete**.

Select **Save** to close the list box and return to the main screen.

Action: The frame allows you to specify actions to be run when infected e-mails or attachments are detected.

Foreground Scanning Not available in this module.

Quarantine infected Files Select the check box to quarantine infected files. Such files are encrypted and stored in a safe location.

Disinfect Select the radio button to disinfect infected files.

Delete Select the radio button to delete infected files.

Anti-Virus Update: The frame allows you to specify how and from where to download vaccine updates, actions run after updates are successfully downloaded, interval for down loads, etc.

Auto-Download Updates

Enable Auto Download Select the check box to enable auto download of updates. The system initiates automatic downloads of updates as per the settings you enable using “Update config” and “Query Interval”

Enable Update Notification Select the check box to notify system administrator when updates are downloaded.

Query Interval To set time for updates auto download: You can specify the time interval at which MailScan should initiate automatic down load of updates Select the appropriate query interval in minutes from the drop-down list. Download begins automatically as per this frequency.

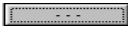
For example: If “1440” is selected then MailScan connects to the site every 1440 minutes (24 hours) to begin downloads.

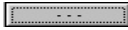
After Update

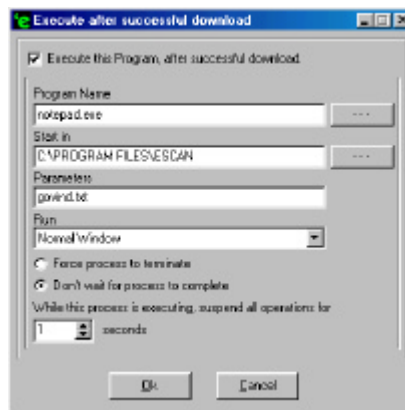
Set auto actions after update downloads: Button is enabled only if “Enable Autodownload” check box is selected. Dialog box shown below is displayed. You assign program files to be executed after updates are

downloaded.

“Execute this...”: Select the check box if the update is to be launched automatically after download. Other fields in this dialog box are enabled only if the checkbox is selected.

“Program Name”: Enter program to be run after update is downloaded You can select the  button to browse your system and select the executable program. The name and path are displayed in the field.

“Start in”: Specify directory or folder of the program. You can select the  button to browse your system and select the executable program. The name and path are displayed in the field.



“Parameters”: Enter the parameter for the program to be run, in this field. The parameter in the screen shown above is a file name.

“Run”: Select the manner in which the file should run, from the drop-down list.

Select **“Normal Windows”** to run it in the windows mode.

Select **“Minimized”** to run it in minimized mode.

Select **“Maximized”** to run it in the maximized mode

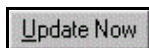
Select **“Hidden”** to hide it from view.

“Force Process to terminate”: Select the radio button if the download process should terminate the launched program after waiting for the set time interval.

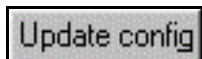
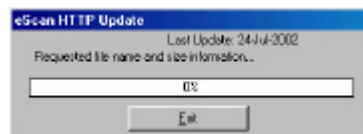
“Don’t wait for process to complete”: The download process will complete and wait for the set interval time even if the program has not completed.

“While this ...”: While the program is running, all other PC operations will be suspended as per the time interval selected from the spin button.

Select **Ok** to accept changes or **Cancel** to discard them.



After settings are modified, select the button to begin downloading updates. Progress bar shown below displays download progress.



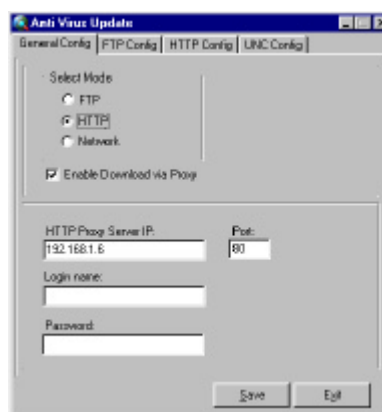
The button provides details on setting up and configuring the settings for Update configuration. You assign the access mode your system uses to connect to the Internet, proxy IP addresses, time interval at which the system should download updates, etc. Typically the updates are up to 10 KB in size, so downloads are fast.

There are four tab pages that allow you to select the mode of download and configure the settings for the selected download mode.

General Config

The tab page allows you to select access mode, enable or disable download notification and auto downloads; download through proxy and assign the IP address of server from which downloads are done. You set the time interval for automatic downloads of updates from the Internet.

Select Mode Updates are available on our designated mirror web sites. You connect to the mirror website and download updates using one of the connectivity modes. The three modes are: HTTP, FTP and UNC.



FTP: (File Transfer Protocol) FTP offers the most stable means to transfer data. Use this mode when you have problems connecting using HTTP. Advantage with FTP protocol is that if connection breaks during download, it commences from the point where it broke in the previous attempt. Configuring FTP for a proxy server is more complicated when compared to configuring HTTP with the proxy-server. These are reputed to be slower than HTTP.

Select the radio button to download using FTP protocol. Tab page "FTP Config" is enabled only if this radio button is selected

HTTP: (File Transfer Protocol) FTP offers the most stable means to transfer data. Use this mode when you have problems connecting using HTTP. Advantage with FTP protocol is that if connection breaks during download, it commences from the point where it broke in the previous attempt. Configuring FTP for a proxy server is more complicated when compared to configuring HTTP with the proxy-server. These are reputed to be slower than HTTP.

Select the radio button to download using FTP protocol. Tab page "FTP Config" is enabled only if this radio button is selected

Network: (Universal Naming Convention) UNC is the standard for naming network drives. For example, UNC directory path has the following form:
\\server\folder\subfolder\filename. In a multi MailScan Server environment, when only one system has Internet connectivity and updates are to be transferred to many machines, choose this mode. If your machine does not have Internet access, you can choose

any machine in the LAN and assign it to download updates. This ensures that updates are transferred to individual machines.

Select the radio button to download using Network mode. Tab page "UNC Config" is enabled only if this radio button is selected

Enable Download Via Proxy: Select the check box if your MailScan server is behind a proxy server.

HTTP Proxy Server IP: Enter the TCP/IP address on which your proxy server listens for HTTP requests, in this field.

Port: Enter the port number on which the proxy server listens for HTTP requests, in this field.

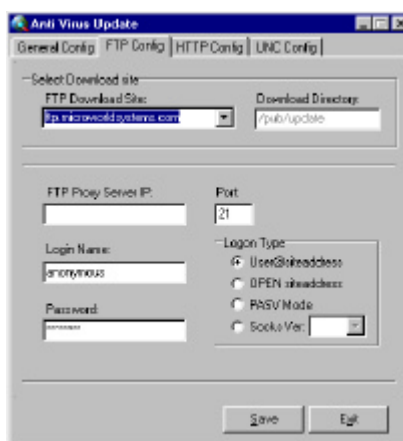
Login name: Enter login name of the user, in this field. System allows access only for this login name.

Password: Password ensures that only the above login name is allowed access. It can be alphanumeric and must be of minimum six characters.

Select **Save** to save and return to the main screen.

FTP Config

The tab page allows you to change the default settings for FTP mode of download. The fields are enabled only if "FTP" is selected as the mode and "Enable Download via Proxy" check box is selected in "General Config tab page



FTP Download Site: [Select update download FTP site](#)
Producer stores updates in dedicated FTP servers. The

sites are defined in the software and displayed in the drop-down list. Select the appropriate FTP site from the drop-down list. The application connects to this site to download updates. The default site is displayed in the field.

Download Directory Updates are stored in the FTP sites in a specific directory. Based on the selection done in "FTP Download Site" the relevant directory name is displayed in the non-editable display field. Default directory name is displayed in the field.

FTP Proxy Server IP: Enter the TCP/IP address on which your proxy server listens for FTP requests.

Port: Enter port number on which you're your proxy server listens for FTP requests.

Login Name: Enter the login name for proxy authentication. System allows access only for this login name. If your proxy server does not require authentication, then retain the displayed default name "Anonymous".

Password: Password ensures that only the above login name is allowed access the application. Enter the password in this field.

Logon Type When a client connects to the Internet) via a proxy server, additional configuration is required to download the updates. Via Proxy' check box is selected in "General Config" tab page. [Select FTP Logon type:](#)

User@siteaddress: This is the format the proxy or the firewall between the client and the Internet, expects the logon command. Select the radio button if proxy used is Winproxy, etc.

OPEN siteaddress: This is the format the proxy or the firewall between the client and the Internet, expects the logon command. Select the radio button if logon type is Cproxy, etc.

PASV Mode: When you connect to a serve with a firewall, the firewall filters unwanted data and access may not be granted. . By using the passive or PASV mode, the server opens a random port, unsecured by the firewall and allows you to connect. Select the radio button if logon type is of Firewall type.

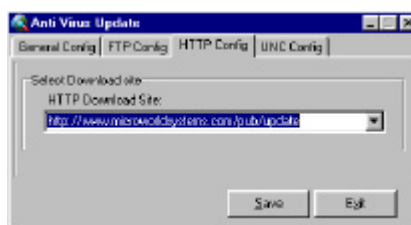
Socks: Select the radio button if Socks proxy is used as

the logon type. The drop-down list box is enabled only if the radio button is selected. Version specification numbers for the Socks Server are displayed in the drop-down list. Select the appropriate value.

HTTP Config

The tab page allows you to change the default settings for HTTP mode of download. The fields are enabled only if “HTTP” is selected as the mode in “General Config” tab page.

HTTP Download Site: A list of HTTP download sites for updates is displayed in the drop-down list. Select the appropriate site. The default HTTP site “http://www.microworldsystems.com/pub/update” is displayed in the field.

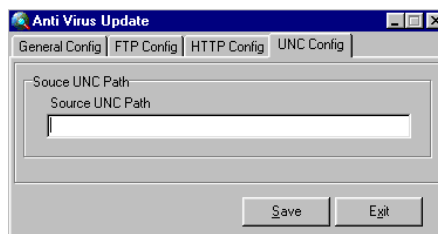


Select **Save** to save and return to the main screen.

UNC Config

UNC mode of download is required when only one server has Internet access in a MailScan environment with multiple MailScan servers and updates need to be transferred to them.

This tab page allows you to change the default settings for Network mode of download. The fields are enabled only if “Network” is selected as the mode in “General Config” tab page.



Source UNC Path: Enter the name and the shared drive path of the network server in this field. For example: \\qa6\c\pub\update

Select Save to save and return to the main screen.

Action: Fields in this frame allow you to set auto actions for infected mails and attachments. Actions are: Quarantine, Delete, Disinfect.

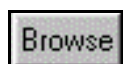
Quarantine Infected Files Select the check box to quarantine infected e-mails and attachments. If an unknown virus infects e-mail, it cannot be immediately removed. In such cases, the e-mails and attachments are isolated in a safe default folder, whose path is shown in the “Quarantine Path:” field. If required, you can select a different folder to store the infected files.

Disinfect Select the check box to disinfect infected e-mails and attachments.

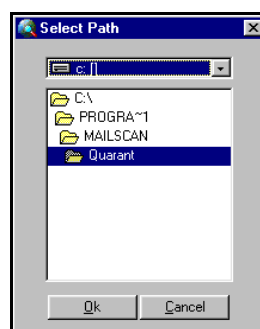
Delete Select the check

Quarantine Path When you select “Quarantine Infected Files” radio button, any

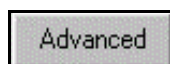
infected e-mail and attachment that cannot be cleaned is stored in a quarantine folder, whose path are displayed in the non-editable display field.



Select the button to view the Select Path dialog box. The box allows you to specify a new folder to store quarantined e-mails and attachments.



Browse your system or network and click on the drive or folder name and select Ok. The selected directory and path name is displayed in the previous field.



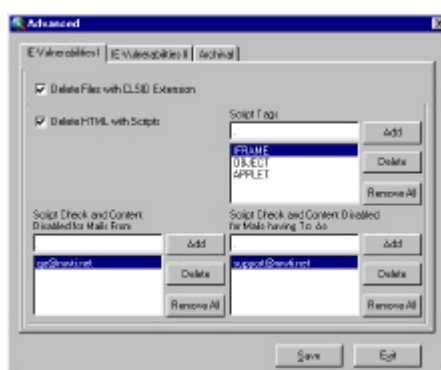
The button allows you to specify advanced settings to plug Internet Vulnerabilities and archive e-mails and attachments. Select the button to view the following dialog box. There are three tab pages that allow you to configure settings for IE Vulnerabilities and Archive e-mails.

IE – Vulnerabilities I

[To Plug Internet Explorer Vulnerabilities:](#) IE has

certain loopholes or vulnerabilities, through which viruses are delivered. Since Outlook Express and other mail clients are from the same product stable, delivery of viruses into your system becomes easier.

The tab page allows you to auto delete mails with CLSID extension and HTML embedded script tags.



“Delete Files with CLSID Extension” Attachments that end with a Class ID (CLSID) file extension do not show the actual file extension with Internet Explorer. This allows dangerous file types to look harmless. Select the check box to auto delete such files.

“Delete HTML with Scripts” HTML e-mails can be used to transmit virus through embedded scripts. Above selection box displays a few known script tags. Select the check box to delete all mails with such scripts.

Script Tags Enter the new script tag in this field and select **Add**. The script tag is added to the list in the selection box. Mails with the tag are deleted. This field is enabled only when “Delete HTML with Scripts” check box is selected. To remove script from the list, click on the tag and select **Delete**.

Script Check and Content Disabled From You can specify that mails from specific e-mail IDs be allowed, even though they have the banned script. Enter the e-mail ID in the field and select **Add**. To remove, select ID and choose **Delete**.

Script Check and Content Disabled For Mails having To As: You can specify that mails to specific e-mail IDs be allowed, even though they have the banned script. Enter the e-mail ID in the field and select **Add**. To remove, select ID and choose **Delete**.

IE –

Some virus-infected files can have multiple extensions

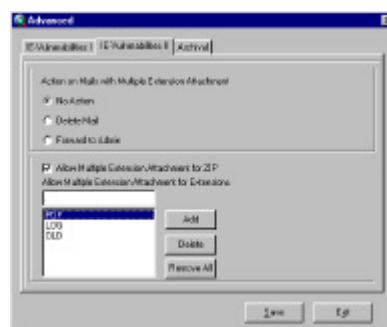
Vulnerabilities II

like. doc.exe. Clean compressed files can also have double extension (e.g.. pdf.zip). The tab page allows you to specify actions for such files.

“No Action” Select the radio button to allow free entry for mails with double extensions.

“Delete Mail” Select the radio button to delete mails with double extensions.

“Forward to Admin” Select the radio button to forward files with double extension to the system administrator.

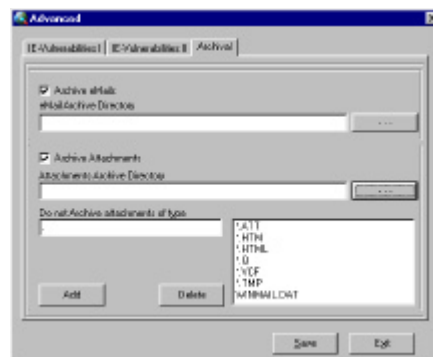


Allow Multiple Extension Attachments to ZIP

Clean compressed files like .zip that have multiple extensions can be allowed entry. Select the check box and enter the extension name in the field and select **Add**. The extension is displayed in the list box. To remove the name, select it and choose **Delete**.

Archival

To archive mails/attachments: All e-mails and attachments flowing in or out of the system can be archived or saved into a specified location. The tab page allows you to specify the location for e-mails and attachments and also exclude specific attachment types from being archived.



“Archive emails” Select the check box to archive e-

mails. Enter the path where the e-mails should be saved. You can browse and select the location using the adjacent browse button. The field and button are enabled only when “Archive emails” check box is selected.

“**Archive Attachments**” Select the check box to allow attachments to be archived. Enter the path where the attachments should be saved. You can browse and select the location using the adjacent browse button. The field and button are enabled only when “Archive Attachments” check box is selected.

“**Do not Archive Attachments of type**” Enter the attachment type that should not be archived and select **Add**. The name is displayed in the list box. To remove the name, select it and choose **Delete**.

- Select **Refresh** to view the updated list and select **Save**


Content Control

This menu allows you to specify restricted words or phrases in e-mails that should be detected by MailScan in your MailServer. E-mails with such words anywhere in the subject, body, tags can be deleted or quarantined. You can add a customized disclaimer for outgoing or incoming attachments.

This section provides details in enabling controls for web access. They key tasks are:

- [To Add a Restricted Phrase](#)
- [To set Actions for e-mails with offensive Phrase](#)
- [To Add Disclaimer to e-mails](#)
- [To select Disclaimers](#)

To Launch Content Control

- In Figure 3.1, select 
- Screen in Figure 3.2 is displayed.

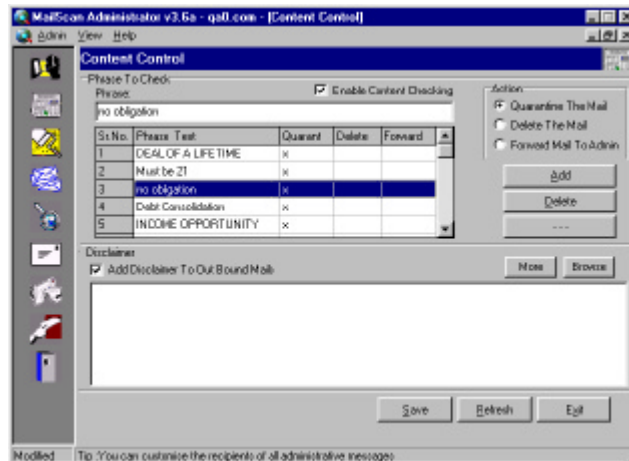


Figure 3.2 Content Control

Fields and their meanings are described in the following table

Field Name

Description

Enable Content Checking Select the check box to allow MailScan to run its content checking feature on your mail server. Fields in this screen are enabled only if the check box is selected.

Phrase To Check: This frame allows you to specify offensive words and phrases that should be checked in e-mails. You can specify the action: Quarantine, Delete or Forward e-mails that have such phrases or words.

Phrase Allows you to enter an offensive word or phrase. List box displays default phrases, added by Producer. Each phrase has an action associated with it: Quarantine, Delete or Forward.

Sr.No.	Phrase Text	Quarant	Delete	Forward
1	DEAL OF A LIFETIME	x		
2	home financing		x	
3	Must be 21	x		
4	no obligation	x		
5	Debt Consolidation	x		

To Add an offensive Phrase: Enter the phrase in the “**Phrase:**” field and select **Add**. The phrase is displayed in the list box.

To Delete an offensive Phrase: You can remove an offensive phrase from the list box. Select the phrase and click **Delete**.

Action

Frame allows you to set action for e-mails that have the offensive phrases displayed in the list box. Radio button allows you to assign the associated action.

Quarantine The Mail E-mails with offensive phrases is quarantined.

Delete The Mail: E-mails with offensive phrases are Deleted.

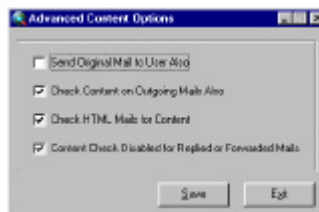
Forward Mail To Admin: E-mails with offensive phrases are forwarded to system administrators.

To set Actions for e-mails with offensive Phrase: Default action is Quarantine. In the list box, click on the restricted phrase and select the radio button for the appropriate **Action**. Next click **Add**.



Select the button to view the Advanced Content Options dialog box. The box allows you to set advanced content checking options. Select the check box for the option to enable it.

Send Original Mail to User Also: Original offensive mail is sent to receiver also.



Check Content in Outgoing Mail Also: Content check for offensive words is done for Outgoing e-mails also.

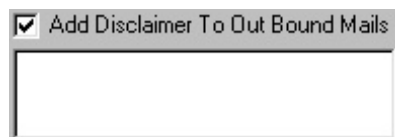
Check HTML Mails for Content: E-mails in HTML format are also checked.

Content Check Disabled for Replied or Forwarded Mails: Select the check box to disable content checking for e-mails that are sent in reply or forwarded.

Disclaimer

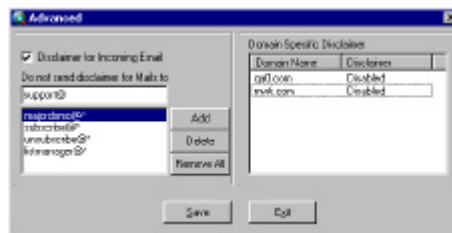
You can add customized disclaimers to outgoing and incoming mails.

To Add Disclaimer to e-mails: Select the check box to send disclaimer to outgoing mails. Click in the dialog box and type the disclaimer.



More

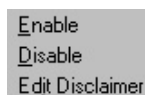
Select the button to view the Advanced dialog box. You can configure advanced settings for disclaimers.



Disclaimer for Incoming Email: Send disclaimer along with all incoming e-mails.

Do not send disclaimer for Mails to: You can specify e-mails IDs, whose e-mails should not carry the disclaimer. Enter the e-mail ID in the field and select Add. The ID is listed in the display box.

Domain Specific Disclaimer: You can specify customized disclaimers for specific domains. Local domains have been defined in [Local Domain](#) and are displayed in the list box. Right click on the domain to view the following pop-up. You perform additional tasks.



Enable: Click on the link to allow disclaimers to be sent.

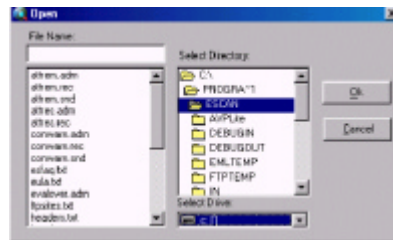
Disable: Click on the link to disable disclaimers.

Edit Disclaimer: Allows you to edit an existing disclaimer. You can also create a new disclaimer file.

Browse

Select the button to view the following selection box. The box allows you to select disclaimer files.

To select Disclaimers: Browse to the required directory and select the file. Contents of the selected file are sent as disclaimers. The button is enabled only when “Add Disclaimer To Out Bound Mails” check box is selected.




- Refresh** Select the button to refresh the screen
- Save** Select the button to save the entries.

Compression Control

Auto compression of attachments is a feature that allows automatic compression of outgoing and incoming attachments. This feature allows you to specify if outbound/inbound attachments should be automatically compressed or uncompressed; exclude and include specific attachments from auto compress; specify the minimum attachment size that should be auto compressed, etc.

To Launch Scanner Administration

- In Figure 3.1, select 
- Screen in Figure 3.3 is displayed. You configure settings as explained in the following table

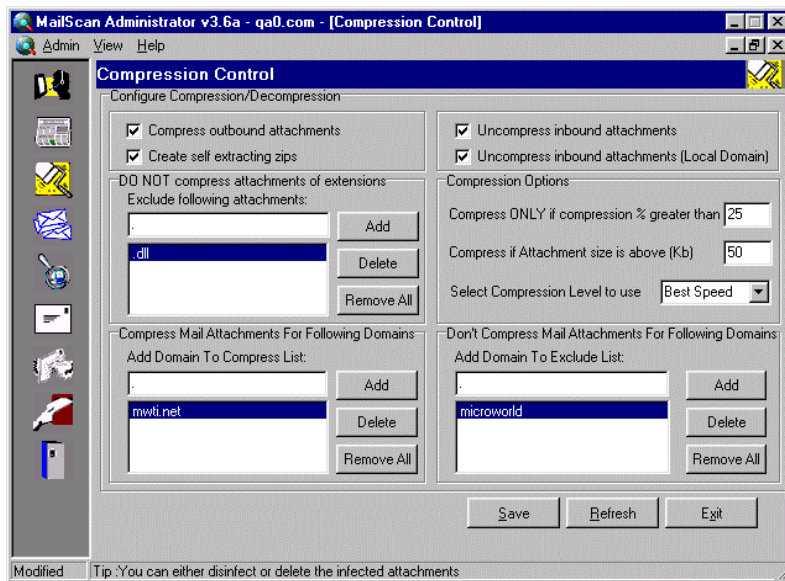


Figure 3.3 Compression Control

Field Name	Description
Compress outbound attachments	Select the check box to allow auto compression of all outgoing attachments. Compressing is done as per the compression options.
Create self-extracting zips	Select the check box to create self-extracting zip files of outgoing attachments. This is useful when the recipient does not have the software to uncompress attachments. This field is enabled only if “Compress outbound attachments” check box is selected.
Uncompress inbound attachments	Select the checkbox to allow auto uncompress of all incoming attachments. All incoming attachments are automatically uncompressed and scanned for virus before they are sent to the receiver. Currently only .zip formats are supported.
Uncompress inbound attachments (Local Domain)	Select the checkbox to allow auto uncompress of incoming attachments from the local domain. This field is enabled only if “Uncompress inbound attachments” check box is selected.
Compress ONLY if compression % is greater	Some files cannot be compressed beyond a limit. You can specify the minimum compress percentage in the adjacent field. Any file, which cannot be compressed beyond the specified value, is not left as is.

Field Name	Description
Compress if Attachment is above (Kb)	You can specify that attachments only beyond a certain size should be compressed. Enter the value in the field.
Select Compression Level to use	Select the appropriate compression from the drop-down list. The available values are: Default, Best Compression and Best Speed. “Default” Ensures the optimum balance between speed and compression quality. “Best Compression” Ensures the maximum amount of compression but may take more time on a slower machine. “Best Speed” Ensures the best speed of compression. Quality of compression may not be optimized.

There are three frames that allow you to specific attachments for auto compress. Each frame has a field and a list box that displays selection you make or previously entered values. To add a value, enter it in the field and select **Add**. The value is displayed in the list box. To remove a value from the list box, select it and click **Delete**.


DO NOT compress attachments of extensions	Specify type of attachments that should be excluded from auto-compression.
Compress Mail Attachments For Following Domains	Specify domain names for which attachments should be compressed.
Don't Compress Mail Attachments For Following Domains	Specify domain names for which attachments should not be compressed.

- Select **Refresh** to view the updated list and select **Save**.

Scan Control

This feature allows you to specify e-mails IDs whose e-mails should be scanned or exempted for virus scanning. You can also specify IDs whose e-mails should be deleted.

To Launch Scan Control

- In Figure 3.1, select .
- Screen in Figure 3.4 is displayed.

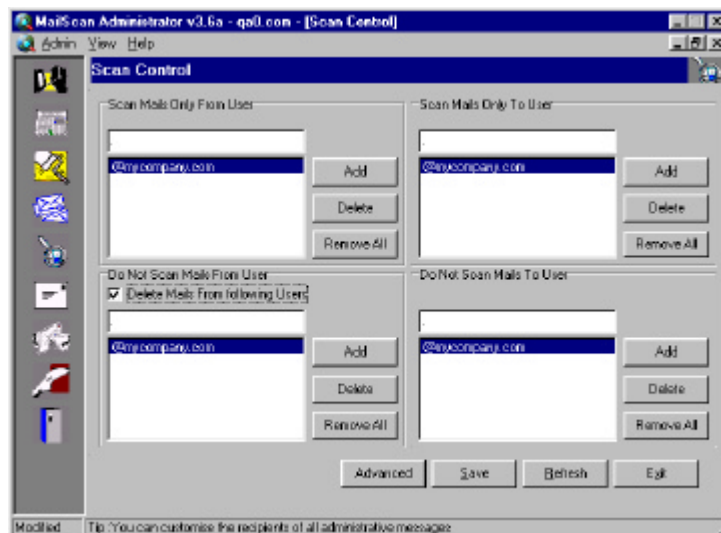


Figure 3.4 Scan Control

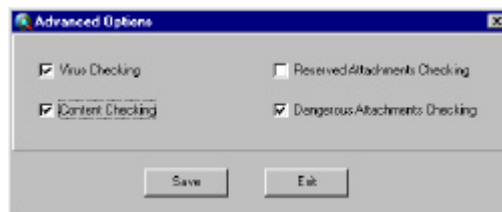
Field Name

Description

There are four frames that allow you to perform specific tasks. Each frame has a field and a list box below it. The list box displays the available e-mail IDs assigned to the frame. To add a new value: Enter the name in the field and select **Add**. The value is displayed in the list box. To remove the value, select it from the list box and click **Delete**. **Remove All** clears the list box.

Scan Mails Only From User All mails from the user are scanned.

Field Name	Description
Scan Mails Only To User	All mails to the user are scanned
Do Not Scan Mails To User	Mails sent to the user are not scanned.
Do Not Scan Mails From User	E-mails from the user are not scanned.
Delete Mails from Following Users	All e-mails from the ID entered in the frame are deleted if the check box is selected.
Advanced	Select the button to view Advanced Options dialog box shown below. You can specify certain common actions for e-mails IDs, selected in the previous frames. Virus Checking: E-mails are scanned for virus. Reserved Attachments Checking: Restricted attachments are scanned.



Content Checking: E-mail contents are checked for offensive words and phrases.

Dangerous Attachments Checking: Checks dangerous e-mail attachments for virus. These are specified in [To block/allow attachments](#)

- Select Refresh and Save.


MailScan Messages

When a virus is detected in mails and attachment or restricted words and phrases are found in them that violate the security policy, the e-mail and

attachment can be deleted, quarantined or disinfected. A customized notification message can be sent to the sender, receiver or others, informing them about the action taken.

This section provides details on creating customized notification messages.

To launch MailScan Messages

- In Figure 3.1, select .
- Screen in Figure 3.5 is displayed.

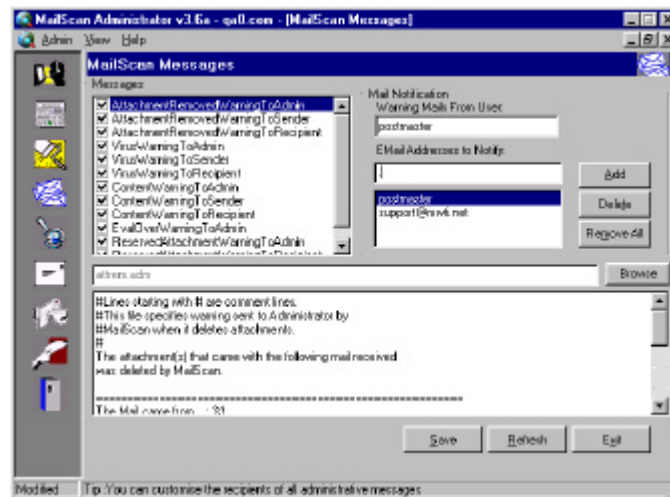


Figure 3.5 MailScan Messages

Field meanings are described in the following table

Field Name	Description
Mail Notification	The frame allows you to specify e-mails ID that sends and receives warning messages Warning messages are sent when violations occur. Different types of warning messages are listed in the adjacent list box.
Warning Mails From User	Enter e-mail ID from which warning messages are sent.
Email Address to Notify	Enter e-mail ID that receives warning messages.

Messages

A list of warning message types is displayed here. These are hard coded by Producer. There is a check box on the left side, which shows ✓ icon by default. This means that the message is sent to the specified ID. Details of the message are displayed in the list box.



'List Box'

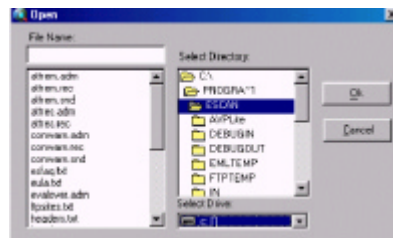
When you click on a message in the 'Messages' list box, its details are displayed in the list box. To edit the message, click in the box and edit the message.



Browse

Select the button to view the following selection box. The box allows you to select files, carrying warnings.

To select warning message: Browse to the required directory and select the file to be sent. Contents of the selected file are sent as warnings. The button is enabled only when "Add Disclaimer to outbound Mails" check box is selected.



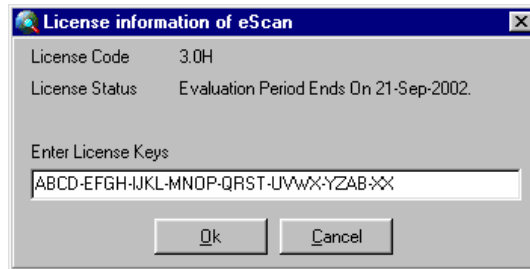
- Select **Refresh** to view the updated list and select **Save**.

License Information

License information key allows you to use the software for the duration, set by Producer. If you are using an evaluation version of the software, then the

key is mandatory to run the application beyond the period. To obtain your License key, please contact sales@winproxy.net.


Key is entered by clicking on the **License icon** or the **License Information** sub menu in **Help** menu. Following dialog box is displayed. Enter the key serial number and select **OK**.

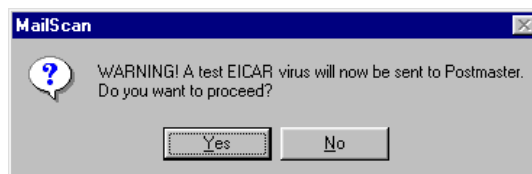


Virus Test Mail

This feature allows you to test MailScan for Anti-Virus effectiveness. E-mail is sent to the local domain, carrying a test virus. If you have configured the system correctly, the e-mail is detected and actions you have specified like Quarantine, Delete or Forward to Admin, is run.




- In Figure 3.1, Select .
- The following warning message is displayed.
- Select **Yes** to send the test virus.

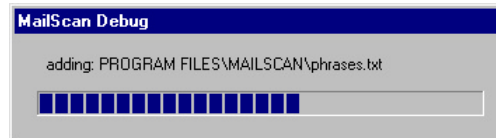


Send Debug Information

Creates a .zip file of the log and.ini files within MailScan, and sends it to the system administrator. The log files allow you to trace any bugs and rectify

minor configuration problems in MailScan. Our support team studies the information and suggests means to rectify the bugs.

- In Figure 3.1, select .
- MailScan collates the .log and .ini files and creates a .zip file. Following screen shows the progress.



After the process is over, MailScan asks you if the debug information should be sent to MailScan Administrator. Select **Yes**.

View Logs and Reports

You can view log files and reports of MailScan activity using the View menu.

Topics in View

The following topics are explained:

- [View Log Files](#)
 - [View MailScan Log](#)
 - [View Auto Update Log](#)
 - [View Download Log](#)
 - [View Weekly Virus List](#)
 - [View Full Virus List](#)
- [Flush Logs](#)
- [Mail Debug Information](#)
 - [MailScan Reports](#)

View Log Files

MailScan generates a variety of log files that gives system administrators an overview and detailed information of MailScan activity in the network.

The following log files are generated:

- [View MailScan Log](#)
- [View Auto Update Log](#)
- [View Download Log](#)
- [View Weekly Virus List](#)
- [View Full Virus List](#)

View MailScan Log

The log provides details of MailScan activity for a period. Details displayed include: Version of MailScan currently running, total size of e-mails sent in a period, e-mail IDs of sender and receiver, attachment details, port configuration and other details through which e-mails are sent, information about warning message like sender/receiver and subject information, etc.

Following Figure shows a typical MailScan Log file.

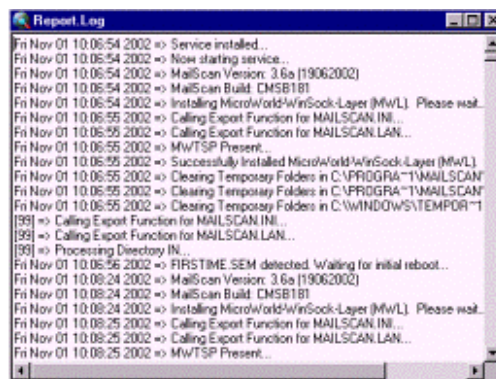


Figure 3.6. MailScan Log File

View Auto Update Log

The log provides details of updates downloaded by MailScan. Details displayed include: MailScan build version currently started, proxy IP used to

download updates, whether new Anti-Virus Version matches found in Producer's download site, etc.

Screen in Figure 3.7 displays a typical Auto Update Log.

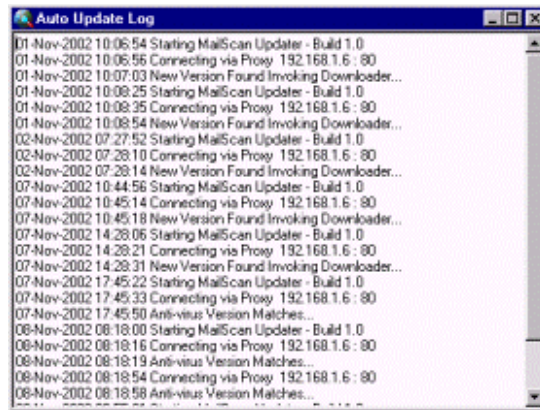


Figure 3.7. Auto Update Log File

View Download Log

The log provides details of updates downloaded from Producer updates download sites. Details displayed include: date and time when download was initiated, Producer's download site URL, proxy IP, files downloaded (update.txt, remove.ini, avp.set, daily.avc) and file size, mode used for download (HTTP or FTP), etc.

Screen in Figure 3.8 displays a typical Download Log file.

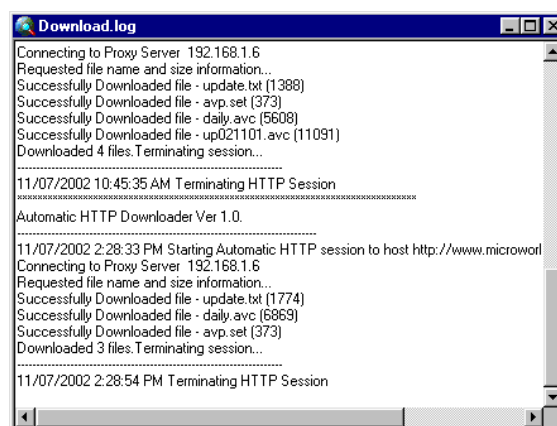


Figure 3.8. Download Log File

View Weekly Virus List

Producer provides a list of new virus, active in the current week. Download updates regularly from Producer to remove the listed virus from your system.

Screen in Figure 3.9 displays a typical Weekly Virus List.

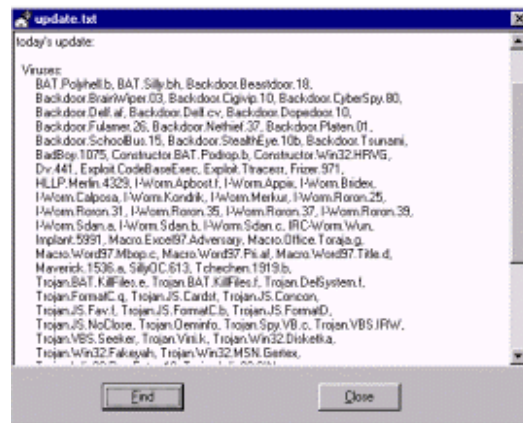


Figure 3.9. Weekly Virus List

View Full Virus List

Producer provides a full list of viruses that have appeared at some point of time. Updates from Producer include vaccines for all virus listed in the file.

Screen in Figure 3.10 displays a typical Full Virus list.

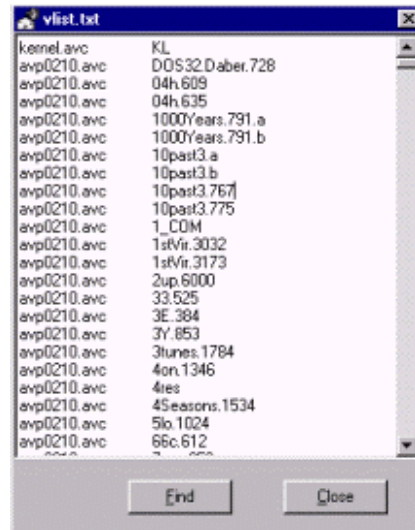


Figure 3.10. Weekly Virus List

Flush Logs

This feature allows you to clear all the log files that are built up over a period of time. Producer strongly advises you to save the log files before flushing them.

The process is run automatically and you are not presented any screen or dialog boxes.

Mail Debug Information

Creates a .zip file of the log and.ini files within MailScan, and sends it to the system administrator. The log files allow you to trace any bugs and rectify minor configuration problems in MailScan.

For details refer [Send Debug Information](#).

MailScan Reports

This feature provides a report of MailScan activity for a period. There are five tab pages that provide reports about different MailScan tasks. The tab pages are: Mails Sent From Local Domains, Mail Details, Alt. Details, Mails Received from Local Users, Mails Received from Foreign Domains and Daily Analysis.

Tab pages are briefly described below:

Mails Sent From Local Domains: Select date to view details of mails sent from the local domain. Details displayed include: domain name from which e-mails are sent, user or person sending e-mails, total number and size of all e-mails sent by the user.

Mail Details: Select date to view details of e-mails sent to a user in your system. Details displayed include: date message is sent, senders name, domain name from which e-mails is sent, message size in bytes, e-mail subject, recipient details, attachment name and size.

Alt. Detail: Select date to view other details of e-mails sent to a user in your system. Details displayed include: attachment file name, size and extension, total infections or virus in the file and if infected number of virus deleted or cleaned.

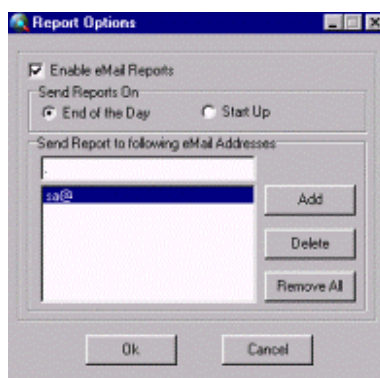
Mails Received by Local Users: Select date to view details of mails received by local users. Details displayed include: domain name from which e-mails are received, user or person sending e-mails, total number and size of all e-mails sent to the user and number of infections detected.

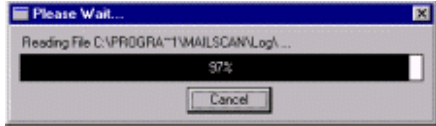
Daily Analysis: Select date range to view details of mails received and sent through your system. For a date, details displayed include: total mails sent and received, total mails sent and size in bytes, total mails received and size in bytes, total number of infections and how many mails were cleaned and deleted.

Common features of tab pages are described below. Fields and features may appear in only some of the tab pages.

Field Name	Description
From Date/To Date	You can select the range of dates to be covered in the report. Click on the dropdown list to open the calendar and select the dates. Report will display details for the period you select for the From and To fields. These two fields are available only for "Daily Analysis" report. Other tab pages have only a single date field and the report is generated for the selected date.
Filter	Filters the report for the selected date range.
S. No	Represents the serial number of the activity.

Field Name	Description
Msg Date	Date the message was sent.
Total Mails	Total number of mails sent and received during the period
Mails Sent	Total number of e-mails sent during the period.
Mail Sent in Bytes	Mails sent size in Bytes
Mails Received	Total e-mails received
Total Infections	Displays total number of infected mails
Deleted	Displays number of mails that were deleted
Cleaned	Displays total number of mails that were cleaned
Foreign Domain	Displays external domain name from which e-mails were received
Size	Displays total size of e-mails received.
Domain Name	Displays domain name from which local users have received e-mails.
User	Displays user name or person who received e-mails.
Email Id	Displays e-mail ID of person receiving e-mails.
Senders Name	Displays senders e-mail ID.
Options	Select the button to view Report Options dialog box, shown below. It allows you to select the time when reports should be e-mailed and e-mail ID to whom they should be sent.



Field Name	Description
Today	<p>Allows you to generate reports for all tab pages for the current system date. Fields in all the tab pages are populated with relevant values.</p> <p>The process is run automatically. Following status bar is displayed.</p>
	
Print	You can print the report of the current screen or the open tab page. Page layout screen is displayed and you can set the page width, zoom to a detail, export the report to Excel, etc.
Refresh All	Refreshes all tab pages.
Refresh	Refreshes current page.
Close	Closes the screen and displays MailScan Administrator screen.

Help

This menu carries tools that allow you to: run the EICAR virus test mail, access the meticulous on-line help, enter the license key and change the password.

This section provides information about the following topics:

- [Send EICAR Virus Test Mail](#)
- [MailScan Help](#)
- [License Information](#)
- [To Change Password](#)

Send EICAR Virus Test Mail

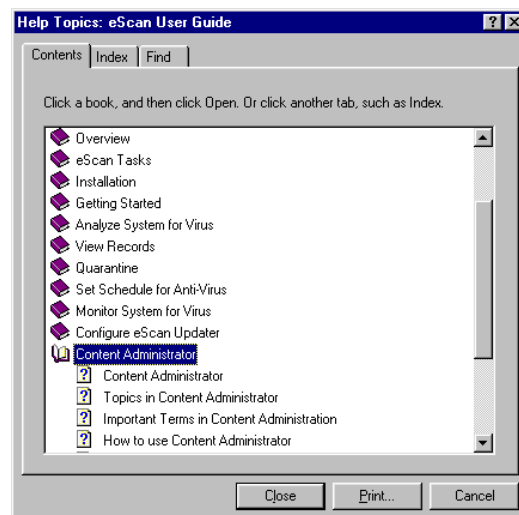
This feature allows you to test if MailScan Anti-Virus feature is installed properly. When you select the link, an e-mail, carrying a test virus is sent to your local domain. If you have configured the system correctly, the virus is



detected and Anti-Virus actions you have specified like Quarantine, Delete or Forward to Admin, are run

For more details, refer [Virus Test Mail](#).

MailScan Help

Producer has provided an on-line help with the software. All features and menus are documented in the file. Select the menu to view the help file shown below.



There are three tab pages. Topics are displayed in the **Contents** tab page. Click on the  icon. It expands and changes to . Individual topics in the books are displayed. A separate window for the topic is displayed.

The **Index** tab page carries a list of all key words. Select the key word or type the phrase in the field and choose **Display**. Relevant topics are displayed in a pop up.

License Information

License information key allows you to use the software for the duration, set by Producer. If you are using an evaluation version of the software, then the key is mandatory to run the application beyond the period. To obtain your License key, please contact sales@winproxy.net.

For details refer [License Information](#).

To Change Password

Producer recommends that you change your password often. In the **Help** menu, select **Change Password**. Enter relevant information in the following dialog box. You must have the old password, to enter the new one. Select **OK**.



The image shows a standard Windows-style dialog box titled "Change Password". It features a blue title bar with a small icon on the left and standard window control buttons (minimize, maximize, close) on the right. The main area of the dialog is light gray and contains three text input fields. The first field is labeled "Enter Old Password", the second "Enter New Password", and the third "Confirm Password". At the bottom of the dialog, there are two buttons: "Ok" and "Cancel".

Frequently Asked Questions

This section gives answers to frequently asked questions.

How does MailScan 3.0 work?

MailScan 3.0 installs a layer known as the MicroWorld WinSock Layer (MWL) that sits in between the WinSock Layer and the Mail Server software. So any e-mail traffic that comes in or goes out necessarily passes via MWL of MailScan.

Since all the traffic passes via MailScan, will it scan the HTTP & FTP traffic?

Producer is working on supporting these protocols. Currently, MailScan scans internal, inbound and outbound SMTP & POP3 traffic.

Does MailScan process the messages before the Mail Server gets them?

Yes. All e-mail traffic that comes in or goes out necessarily passes via MWL of MailScan before reaching the Mail Server.

Does MailScan 3.0 process Local Queue and Remote Queue of the Mail Server?

No. MailScan 3.0 does not process Local Queue and Remote Queue of the Mail Server.

Apart from port 25, I have SMTP traffic coming on port 8025 also. Will MailScan scan these too?

Not automatically. MailScan tries to identify the default port settings being used by the Mail Server and automatically implements scanning of those port settings. You will then have to manually configure MailScan to scan SMTP or POP3 traffic on other ports via MailScan Admin program.

Will MailScan scan ETRN traffic?

Yes. MailScan scans ETRN traffic.

Will MailScan scan ATRN traffic?

Yes. The default port for scanning ATRN traffic is 366.

Will MailScan disturb the anti-Spam & relay-check functionalities defined using the Mail-Server?

No. MailScan will not disturb the anti-Spam & relay-check functionalities defined using the Mail-Server.

I have SMTP authentication enabled on the Mail Server. Will MailScan still scan the traffic?

Yes. MailScan will still scan the traffic.

Why is eScan anti-virus required?

eScan is a Virus Scanning solution from Producer that MailScan uses in addition to providing content security.

Does MailScan work like a packet-sniffer?

No. A packet-sniffer works on a much lower level. MailScan-MWL works on the IP layer (same layer on which Microsoft Proxy works).

Will MailScan cause instability and performance hit?

Since MailScan works well above the "raw-packet" layer (MailScan-MWL) on its own, it should not cause any instability and/or performance hit. However, please note that the anti-virus and content check components of MailScan do

use CPU and RAM resources.

How does MailScan intercept the e-mails?

Just like a proxy, MailScan transparently lies between any application and the WinSock layer. Therefore, when SMTP or POP3 transactions take place, all of these go via MailScan-MWL.

In other words, MailScan acts like a "transparent buffer" between the application and the WinSock layer.

Is there a possibility of the application timing out when MailScan is doing the scanning?

Producer has implemented various methods to ensure that any application or your server is "kept alive" when MailScan is receiving (buffering) and processing the mails. This has been extensively tested internally with many popular applications.

Note - In case a time-out problem occurs with a particular application, please contact Producer immediately so that appropriate measures can be taken

Are there any incompatibility issues pertaining to MailScan-MWL?

The WinSock standards are very well defined and documented. These standards are implemented by millions of applications. MailScan works reliably, provided that applications properly implement these standards.

Also, any application that does not properly implement these standards, risks serious compatibility problems when working with other applications. However, please do not hesitate to contact Producer immediately if you are experiencing a compatibility problem, so that appropriate measures can be taken at the earliest.

Noted exceptions:

a) Producer is currently in the process of resolving certain issues with Lotus Notes R4.6 and SendMail NT. It will be completed shortly and an appropriate product update will be issued immediately thereafter.

b) Producer has also identified an issue pertaining to platforms running Novell Client/32 with WinSock 2. They do not seem to interoperate. Producer is trying to resolve this issue.

I use MS-Exchange in my organization. My Mail Server downloads the messages from the Internet and gives it to Exchange. Exchange then forwards all the outgoing mails to the Mail Server, which in turn, sends it out to the Internet. Will MailScan scan these mails?

Yes. When the Mail Server is downloading the messages, MailScan-MWL checks them. Similarly, when Exchange hands over the messages to the Mail Server via SMTP, MailScan-MWL will scan these too.

I use MS-Exchange in my organization. But there is a Gateway that downloads the messages from the Internet and gives it to Exchange. Exchange also forwards all the outgoing mails to the Gateway, which in turn, sends it out to the Internet. Where should I install MailScan and will MailScan scan these mails?

MailScan should be installed on the Gateway. MailScan will scan all the messages that are downloaded by the Gateway from the Internet before passing these to MS-Exchange Server.

It also scans all the messages that are forwarded by the MS-Exchange Server to the Gateway before these are sent across to the Internet.

Note - MailScan does not scan internal mails only in the scenarios where Lotus Notes and MS-Exchange Server are installed.

Do I need more than one license copy of MailScan if the Mail Server and Exchange are on the same platform?

No. MailScan is licensed on 'per installed platform' basis. However, the number of mailboxes will be those of the Mail Server plus those of Exchange.

Do I need more than one license copy of MailScan if the Mail Server and Exchange are on different platforms?

Yes. MailScan is licensed on 'per installed platform' basis.

I use Outlook Express on the Mail Server machine to download e-mails from my POP account. Will MailScan check these too?

Yes.

I use a web e-mail client (i.e., browser-based e-mail client) to send

and receive the messages. Will MailScan scan these?

If MailScan is installed on the actual Mail Server platform concerned, then all the e-mail messages accessed via the web client will be checked.

However, if MailScan is running on another platform (for example, local workstation running the web client) that accesses the Mail Server using HTTP, then the e-mail messages will not be scanned (until MailScan-MWL supports HTTP scanning).

I access my e-mails through my Hotmail account. Will MailScan check these e-mails?

No. Hotmail accesses e-mails via HTTP and not via POP3. MailScan therefore does not scan these currently. However, this feature will be made available as soon as Producer completes the implementation of HTTP scanning support.

The Mail Server is installed on Windows 2000 and is running as a Service. How can I ensure that MailScan starts its' operations before the Mail Server starts?

MailScan is programmed in such a way that whenever the first TCP-IP based application starts, MailScan starts automatically. Technically, whenever the WinSock DLL loads, MailScan starts automatically.

I am using another anti-virus software. Can I use this instead of eScan? Alternatively speaking, can eScan be disabled?

Whilst eScan can be disabled, many features that are 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 by eScan) give MailScan its "ultimate edge" over any other package. Therefore, Producer strongly recommends using eScan.

What action does MailScan take when a virus-infected e-mail is detected?

The e-mails are first cleaned and then passed to the Mail Server application. In other words, the SMTP Server or POP3 client will always receive a "clean" message. A copy of the mail is forwarded to the Administrator and warning messages are sent across to the actual sender of the mail.

What happens if I have instructed MailScan to delete the e-mails having harmful content?

In this case, MailScan will generate the message "e-mail has been deleted at the Server as it contained restricted content".

Can MailScan handle ZIP files in transit?

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 the appropriate action.

If the option "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.

Can I develop plug-ins for MailScan that can do other work on the e-mail body and/or attachments? (For example, I would like to encrypt the messages and attachments while sending the e-mails).

Once Producer finishes documenting the APIs and associated standards, this feature will be immediately made available.

Is MailScan similar to Gateway scanning that is provided by other anti-virus software packages?

No. The following are the disadvantages of other software's that provide Gateway scanning.

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

After installing MailScan do I need to reboot the machine?

Yes. Producer recommends rebooting the machine after the installation of MailScan is complete.

How do I check whether MailScan is active or not?

Any one of the following methods can be used to check whether MailScan is active or not:

a) Run the MailScan Administrator, click on 'Send Test EICAR Virus' and then check the LOG files. MailScan is correctly installed if the LOG files show that the warning messages have been sent.

b) Run "TELNET 127.0.0.1 25" (the IP-address of your Mail Server followed by the SMTP port on which your Mail Server is listening). Then type "HELO test-domain" and wait for a response. If MailScan is correctly installed and enabled, you will get the response: "250 MailScan - Welcome to MailScan enabled MailServer".

What is the EICAR Test Virus?

EICAR stands for "European Institute for Computer Anti-Virus Research". This organization has developed a small test string to help other organizations test the Anti-Virus packages. The EICAR test virus is harmless. To get more information, visit <http://www.eicar.com>.

What happens after the license period expires? Will MailScan stop scanning my e-mails?

After the license period expires, MailScan will continue to scan your e-mails but it will stop receiving updates. It will also inform the MailScan Administrator about the end of the subscription.

How frequently is MailScan's virus database updated?

The websites and the FTP sites are normally updated once a day. On certain occasions, they may be updated more frequently (in response to a virus epidemic like the Love-Bug virus).

How do I update MailScan with the latest virus updates?

eScan that is incorporated with MailScan, automatically keeps its' virus

database updated. It checks for availability of an Internet connection. If it detects a connection, it 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.

Can I configure the frequency of update checks?

Yes. You can easily configure the intervals at which MailScan will check for updates.

Can MailScan download the updates via FTP or HTTP? Will it work through a normal proxy or Socks proxy server?

Yes. Updates can be downloaded via FTP or HTTP. You can use normal proxy or Socks proxy server for downloads.

Can MailScan download the updates through a Firewall?

Yes. This can be done either by using HTTP downloads or by using Passive FTP.

Does MailScan work with all the versions of Windows?

MailScan works with all the versions of Windows except Windows 3.x.

Does MailScan scan inside the ZIP files?

Yes. MailScan scans inside the ZIP files.

Other than ZIP, which types of archives does MailScan virus scanning support?

MailScan virus scanning supports 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 regularly updated so that the range of formats supported will automatically remain current (provided MailScan and eScan are kept updated).

Does MailScan scan inside the compressed executable files?

Yes. MailScan scans inside the compressed executable files.

What decompression formats are supported by MailScan?

Following decompression formats are supported by MailScan:

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, SCRINCH, 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.

Does MailScan scan and clean Microsoft Outlook TNEF (WINMAIL.DAT) attachments?

Yes. MailScan scans and cleans Microsoft Outlook TNEF (WINMAIL.DAT) attachments.

Does MailScan scan the body of the e-mails?

If the body of the e-mail is using the HTML format, it is scanned. However, MailScan does not scan the body of 'Plain Text' format e-mails, as these cannot carry viruses, macros, etc.

What exactly is "HTML.SecurityBreach.2"?

Many times MailScan deletes the HTML format e-mails with a warning message "HTML.SecurityBreach.2".

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

The "Scriptlet.TypeLib" object has a vulnerability factor that may enable a

script to write files on the local computer.

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

For more information on this vulnerability, please read the article available at the following URL:

<http://support.microsoft.com/support/kb/articles/Q240/3/08.ASP>

Producer strongly recommends all the users using Internet Explorer 5.x to install the security update available at <http://www.microsoft.com/technet/security/bulletin/ms99-032.asp>

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

For incoming e-mails, run 'MailScan Admin' and then select the checkbox "Quarantine Unsafe Attachments". This will ensure that any VBS or JS attachments are "quarantined" and not deleted. Please note that this approach could be dangerous for your network.

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

When I send a large-sized e-mail to my Mail Server, I observe NOOP commands being processed by the Server. Is this normal?

Yes. This is normal. It is a function used by MailScan-MWL to keep the Mail Server alive.

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

Yes. These are MailScan "Process-threads" that start if an e-mail is to be scanned anytime. They 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.

I see four icons in the system tray after installing MailScan and eScan. What are these? Are these required?

You would already be aware of the MailScan icon - the white envelope that

controls the MailScan functions.

The Red Shield icon is the eScan Anti-Virus Monitor that is responsible for 'controlling' the anti virus functions.

The green icon takes care of the automatic updates for eScan.

The circular eScan Management-Console icon controls the distribution and sharing of updates to the Workstations and MailScan itself.

MailScan is shipped along with a single Enterprise edition of eScan.

Can I change the default eScan settings?

You can, but this is not recommended. The eScan settings for MailScan have been tuned to achieve maximum throughput and efficiency.

Even after I install MailScan as a normal application, I do not see the MailScan Activity Console Window. Why?

MailScan-MWL, as explained earlier, starts as soon as WinSock starts. WinSock starts even before you login to your machine. So MailScan-MWL, despite not being installed as service, will start before you login and hence, will not be displayed in the Activity Console Window.

Support

This section gives details to obtain support from Producer. We offer support to our customers through e-mail.

E-Mail support

We provide e-mail support.

- Drop us a line at support@winproxy.net

Our offices

LAN-Projekt

Placheho 17

301 26 Plzen

Czech Republic

Tel +420 377 993 155

Fax +420 377 993 159

For more information about our products please visit: www.winproxy.net

Safe Computing

The first line of defense in the fight against viruses is You. Producer strongly recommends that you follow the following steps to begin safe computing:

- Install the latest version of Anti-Virus software from Producer.
- Open mails and attachments from only people you know. If you are not sure about the origin, do not even open the e-mail.
- If you want to open an attachment, first scan it with our MailScan Anti-Virus software. Known virus will be detected and removed. For unknown virus or files with suspicious content and extensions, quarantine them and then try to remove the virus. If this does not work, then mail us a copy of the file. We will analyze it and get back to you.
- Files like mpeg, games, movies etc are prone to viruses, which use them as carrier files. Be extra careful with such files and scan them thoroughly before running them.
- Chain mails, strange or free offers etc, often carry virus. Do not open such mails. Be careful when using floppies, CD ROMS that have been run on other machines.
- Regularly download Updates from our download sites. Our Anti-Virus package is equipped to remove all viruses, known till it was released. More than 500 viruses are 'released' every month. Only Updates have the means to remove them.
- Take backups of valuable files. Backups could be on another machine, CD ROMS, Floppies etc.

History Of Virus

This section provides a brief history of viruses.

In the Year	What happened ...
1981	Elk Cloner , the first virus spreads from Apple II floppies. It displays a rhyme "It will get on all your disks, It will infiltrate your chips, Yes it's Cloner!"
1983	Fred Cohen writes a paper "Computer Viruses - Theory and Experiments". Len Adelman coins the term Virus . They create the first virus on a VAX 11/750 machine running on Unix.
1986	Basit and Amjad, replace the executable code in boot sector of a floppy with their own program. When the floppy is run, the program installs itself in the computers memory. Any floppy accessed by the drive, has the code written into it. Ralf Burger creates a virus, which copies itself to other files. He calls it Virdem .
1987	A PC support lady at the University of Delaware sees a volume with the label © Brain on floppies. It is the Brain Virus and all it does is, copy itself on a disk and create a volume in its name. File Viruses appear which infect COM files. 'Popular' types are Leigh (Jerusalem) , Surv 01 and 02. IBM Christmas Worm hits IBM mainframes. It replicates half a million times per hour. Stoned , a virus, which displays the message "Your PC is now stoned", appears from the University of Wellington, New Zealand.
1988	MacMeg , a hypercard virus hits Macintosh machines. Internet Worm causes the first Internet crisis and shuts down many computers.
1989	Aids Trojan sent out in the guise of AIDS information hits the computer Industry. It encrypts the hard drive and wants payment for the decryption key.

- Datacrime** virus threatens IBM computers. It was supposed to get launched on Friday the 13th.
- 1990** Bulgarian virus exchange factory (VX) BBS starts in a big way. Virus authors form a 'forum' to exchange tips and tricks.
- Mark Ludwig writes a book "The Little Black Book of Computer Viruses" which tells you how to write virus programs.
- 1991** **Tequila** comes from Switzerland. It is the first Polymorphic virus and changes itself to avoid detection.
- 1992** **Michelangelo** appears. Induces hysteria with threats of massive damages, but actually very little happened.
- Two new 'tool kits' are released: **Dark Avenger Mutation Engine** (DAME) and **Virus Creation Laboratory** (VCL). They can help you create your own viruses.
- 1995** The **Internet Liberation Front** virus hits Griffith Air Force Base, Korean Atomic Research Institute, NASA, Jet Propulsion Laboratory, GE, IBM and other companies on Thanksgiving Day.
- The first macro virus to attack Word files, **Concept**, is released.
- 1996** **Boza**, the first virus designed specifically for Windows 95 files arrives.
- Laroux**, the first Excel macro virus appears.
- Staog**, the first Linux virus attacks Linux machines
- 1988** **Strange Brew**, the first Java virus attacks. **Back Orifice**, the first Trojan works as a remote administration tool that allows a computer via to be controlled via the Internet.
- 1999** **Melissa**, the first combination Word macro virus and worm to use the Outlook and Outlook Express address book sends itself through e-mail.
- Corner** is the first virus to infect MS Project files.
- Tristate**, the first multi-program macro virus that infects Word, Excel, and PowerPoint files appears.
- Bubbleboy**, the first concept worm that activates when an e-mail message is opened in Microsoft Outlook or Outlook Express.). No attachment required.

- 2000** **Denial of Service (DoS)** attacks shut down Yahoo, Amazon etc.
- Love Letter worm** shuts down e-mail systems around the world.
- Timofonica** worm sends messages to Internet-enabled phones in the Spanish telephone network.
- Liberty**, the first worm for PDA's is accidentally released.
- Pirus**, a concept virus attempts to add to HTML and PHP files.
- 2001** **Gnuman** (Mandragore) appears. This worm disguises as an MP3 file.
- Winux**, which hits Windows and Linux machines, appears from the Czech Republic.
- LogoLogic-A** spreads via MIRC chat and e-mail.
- AppleScript** worm using Outlook Express or Entourage on the Macintosh spreads via e-mail to address book entries.
- PeachyPDF** worm, the first to spread using Adobe's PDF software appears.
- Nimda, Sircam, CodeRed, BadTrans** worms demonstrate massive firepower in bringing down whole networks and organizations.
- 2002** **LFM-926**, the first virus to infect Shockwave Flash (.SWF) files appears. Named for the message it displays while infecting: "Loading.Flash.Movie..."
- Donut** shows up as the first worm directed at .NET services.
- Sharp-A**, the first native .NET worm written in C# is seen. It is also unique as it is one of the few malware programs reportedly written by a woman.
- SQLSpider** worm is released. It attacks applications using Microsoft SQL Server technology.
- Benjamin** uses the KaZaa peer-to-peer network to spread.
- Perrun** virus, attaches itself to JPEG image files.
- Scalper** worm attacks FreeBSD/Apache Web servers. The worm is designed to set up a flood net (stable of zombies used to overwhelm one or more systems).

Klez.H, a stealth virus appears. It spreads using a Windows system hole that allows file names with double extensions.

I-Worm.Cervinec, **I-Worm.MyLife.b**, **Zircon C**, worms that attach to e-mails, appear. They are .exe files.

Glossary

This section provides a glossary of terms related to our application.

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

A

Access 97 macro virus Affects MS Access 97 or later on any operating system. Written in VBA macro language.

Address Coded representation of the origin or destination of data.

AppleScript worm Is a script that uses the functionality of AppleScript to spread to other computers or scripts an email application to send itself out.

ASCII American Standard Code for Information Interchange - A seven-level code (128 possible characters) used for data transfer.

Anonymous FTP Downloading public files using the File Transfer Protocol (FTP). Called anonymous because you don't need to identify yourself before accessing files.

Attachment A file attached to an e-mail message.

Anti-Virus Software Scans computer's memory and disk drives for viruses. When it finds one, it informs you and allows you to clean, delete or quarantine files, directories or disks infected by it.

Armored Virus Tries to prevent analysis of its code.

Attack An attempt to compromise or bypass a system's security.

B

Batch file worm Affects Computers connected to a network with DOS, Windows 95/98/Me and Windows NT/2000 operating systems. Spreads by searching for shared areas on remote computers to which it can copy itself.

Bandwidth Range of frequencies passing through a given circuit. Greater the bandwidth faster is the information sent or accessed through the circuit.

Background scanning Feature in some anti-virus software to automatically scan files and documents as they are created or run.

Bit Smallest unit of information in a binary system. Represents either a one or zero ("1" or "0").

Bimodal Virus Infects boot records and files.

BIOS (Basic Input/Output System) Part of the operating system that identifies a set of programs used to boot the computer before locating the system disk. It is located in the ROM and is usually stored permanently.

Blended Threat Combines characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to attack the system. Uses multiple means to spread rapidly and cause widespread damage.

Booting Starting the computer. Booting runs various programs to check and prepare the computer for use.

Boot Sector Area on the first track of disk. Contains the boot record.

Boot Record Program in the boot sector. Contains information about characteristics and contents of the disk and booting the computer. If PC is booted with a floppy disk, the system reads the boot record from that disk.

Boot Sector Virus Places its code in the boot sector. When the computer tries to read and execute the program in the boot sector, the virus lodges itself in the PC memory and gains control over the PC. From here it spreads

to other drives on the system. Once the virus is running, it usually executes the normal boot program, which it stores elsewhere on the disk.

Bugs Are not viruses but are unintentional errors in programs.

Byte A group of bits normally 8 bits in length.

C

Cavity Virus Overwrites part of its host file without increasing the file size.

Checksum Identifying number calculated from file characteristics. Any change in a file changes the checksum.

Cluster Virus Changes directory table entries. Virus starts before other programs so they may appear to infect every program on a disk. Virus code exists in one location, but running any program runs the virus.

Configure To set up a program or computer system for a particular application.

. COM Files Executable file limited to 64 KB with the extension. COM. Used by utility programs and routines. As COM files are executable, viruses can infect them.

Companion virus Renames either itself or its target file to trick the user into running the virus rather than another program. For example, a companion virus attacking a file named MOVIE.EXE may rename the target file to MOVIE.EX and create a copy of itself called MOVIE.EXE.

Corel Script virus Affects Corel SCRIPT files. Uses Corel SCRIPT macro language.

Crack To copy commercial software illegally by breaking (cracking) the various copy protection and registration techniques being used.

Client Application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

Cluster Is a logical disk-partitioning unit. A Cluster consists of one or several logical disk sectors, sequentially located. The Length of the cluster on floppy disks usually equals to 1 or 2, on hard disk - 4 or 8.

D

Daemon Pronounced demon or 'Damon'. Is a process that runs in the background and performs specified operations at predefined times or in response to certain events. Typical daemon processes include print spoolers,

e-mail handlers, and other programs that perform administrative tasks for the operating system. The term comes from Greek mythology, where daemons were guardian spirits.

Denial of Service (DoS) Attack preventing normal functioning of a system. Genuine users are denied access. Hackers can cause DoS attacks by destroying or modifying data or by overloading system's servers.

Direct Action Virus Immediately loads itself into the memory, infects other files, and then unloads itself.

Distribution Measure of how quickly a threat spreads

Disassembler A utility performing transformation, reverse to assembling, i.e. transforming machine codes to assembler language. Such utilities are required not only for debugging programs but also for virus analysis.

Downloads Process of copying a file from an online service to one's own computer. Also refers to copying a file from a network file server to a computer on the network. The opposite of download is upload, which means to copy a file from your own computer to another computer.

Dropper A file created specifically to introduce a virus, worm or Trojan into a system. The file may be different type from the virus, worm or Trojan it introduces.

E

Encryption Virus Its code begins with a decryption algorithm and continues with scrambled or encrypted code. Each time it infects, it automatically encodes itself differently, so its code is never the same.

e-mail Name that identifies an electronic post office box on a network where e-mail can be sent.

e-mail Client Application that runs on a personal computer or workstation and enables you to send, receive and organize e-mail. Called a client because e-mail systems are based on client-server architecture.

Exploit Program or technique that takes advantage of vulnerability in software that can be used for breaking security or otherwise attacking a host over the network.

Excel formula virus Affects MS Excel 5 or later running on any operating system. Uses Excel formula language. When an infected document is opened the viral formula sheet is copied into a file in the XLSTART directory. This is automatically loaded into other documents when they are opened.

.EXE Files Executable file. Run by double-clicking its icon or a shortcut on the desktop, or by entering the program name at a command prompt. Are

also run from other programs, batch files or various script files.

F

False Negative Error Occurs when the anti-virus software fails to indicate an infected file is really infected.

False Positive Error Occurs when the anti-virus software wrongly claims a clean file is infected. Error occur when the string chosen for a given virus signature is also present in another program.

FAT (File Allocation Table) Stores the addresses of all the files contained on a disk. In MS-DOS and Windows the FAT is located in the boot sector of the disk. Viruses and normal use can damage the FAT. If damaged or corrupt, the operating system is unable to locate files on the disk.

File Viruses Replace or attach themselves to COM and EXE files. They also infect files with extensions: SYS, DRV, BIN, OVL and OVY. They can be resident or non-resident, the most common being resident or TSR (terminate-and-stay-resident) viruses. Many non-resident viruses infect other files when an infected file runs.

Firewall A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. A firewall is considered a first line of defense in protecting private information.

FTP (File Transfer Protocol) Protocol used to send files on the Internet.

G

Gateway Points of entrance and exit from a communications network. Viewed as a physical entity, a gateway is the node that translates between two otherwise incompatible networks or network segments. Gateways perform code and protocol conversion to facilitate traffic between data highways of differing architecture.

H

Heuristic Scanning Behavior-based analysis of a computer program by anti-virus software to identify a potential virus. Anti Virus software sends

alerts when a file has suspicious code or content.

Hijack An attack where an active and legitimate session is intercepted and taken over. Remote hijacking can occur via the Internet.

Host File to which a virus attaches itself. Virus is launched when the host file is run.

Hoaxes Are not viruses, but are deliberate or unintentional e-messages, warning people about a virus or other malicious software program. They create as much trouble as viruses by causing massive amounts of unnecessary e-mail.

HTTP (Hypertext Transfer Protocol) Main protocol used by the World Wide Web. Defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

I

Internet Address Also known as an IP address. Is a 32-bit hardware-independent address assigned to hosts using the TCP/IP protocol suite.

Infection Length Size of viral code inserted into a program by a virus. If it is a worm or Trojan horse the length represents the file size.

IP (Internet Protocol) Networking protocol for providing connectionless services to the higher transport protocol. It is responsible for discovering and maintaining topology information and for routing packets across homogeneous networks. Combined with TCP, it is commonly known as the TCP/IP platform.

IP Address Uniquely identifies each host on a network or Internet.

J

JavaScript virus Affects JavaScript scripting files, HTML files with embedded scripts, Microsoft Outlook and Internet Explorer.

Joke Programs These are not viruses, but may contain a virus if infected or otherwise altered.

K

Keys The Windows Registry uses keys to store computer configuration settings. When a new program is installed or the configuration settings are altered, values of these keys change. Virus modifies these keys and cause damages.

L

LAN (Local Area Network) Network that interconnects devices over a geographically small area, typically in one building or part of a building. The most popular LAN type is Ethernet, a 10 Mbps standard that works with 10BaseT, 10Base2, or 10Base5 cables.

Library File Contains groups of frequently used computer code shared by different programs. Developers use these codes to make their programs smaller. A virus infecting a library file may appear to infect any program using the library file. In Windows systems, the most common library file is the Dynamic Link Library with extension .DLL.

Linux worm Take advantage of flaws in networking code to gain unauthorized access to remote computers running Linux. They can spread rapidly between computers permanently connected to the Internet because they require no user intervention to function.

Log On To make a computer system or network recognize you so that you can begin a computer session. Most personal computers have no log-on procedure -- you just turn the machine on and begin working. For larger systems and networks, however, you usually need to enter a username and password before the computer system will allow you to execute programs.

M

Macro Set of mini programs that simplify repetitive tasks within a program such as Microsoft Word, Excel or Access. Macros run when a user opens the associated file. Viruses can infect macros.

Macintosh file virus Infect Macintosh computers.

Mailbomb Many e-mails (thousands of messages) or one large message, sent to the system to make it crash.

Master Boot Record A 340-byte program in the master boot sector. It reads the partition table, determines what partition to boot and transfers control to the program stored in the first sector of that partition. There is only one master boot record on each physical hard disk.

Master Boot Sector First sector of a hard disk located at sector 1, head 0, and track 0. Contains the master boot record.

Master Boot Sector Virus Infects the master boot sector of hard disks. They spread through the boot record of floppy disks. The virus stays in memory and infects the boot record of floppy read by DOS.

Mid infecting A prefix to denote viruses that infect the middle of a file.

Mime (Multipurpose Internet Mail Extensions) Specification for formatting non-ASCII messages so that they can be sent over the Internet. Many e-mail clients now support MIME, which enables them to send and receive graphics, audio, and video files via the Internet mail system. In addition, MIME supports messages in character sets other than ASCII.

MPEG (Moving Picture Experts Group) Pronounced m-peg is a working group of ISO. Term refers to the family of digital video compression standards and file formats developed by the group. MPEG generally produces better-quality video than competing formats, such as Video for Windows, Indeo and QuickTime. MPEG files can be decoded by special hardware or software.

Multipartite Virus Infect documents, executables and boot sectors. They first become resident in system memory and then infect the boot sector of the hard drive and the entire system.

Mutating Virus Changes or mutates as it runs through its host files. Disinfection is more difficult.

MWL (MicroWorld Winsock Layer) Anti Virus and content security concept introduced and used by MicroWorld technologies Inc. MWL is placed above the Winsock layer and acts as a secure blanket between the Internet and your system. Any type of data exchanged through your system is monitored by MWL. This stops potential threats from entering your system. While other products allow threats to enter your system and then try to diffuse them, MWL technology has the key advantage of barring them from entering.

N

Network Group of computers connected to each other within an organization. Organization may be spread across a wide geographical area.

O

Operating System The underlying software that allows you to interact with the computer. It controls the computer storage, communications and task management functions. Examples: MS-DOS, MacOS, Linux, Windows 98, UNIX etc.

Overwriting Virus Copies its code over the host file's data destroying the original program. Disinfections are possible, although files cannot be recovered. It is usually necessary to delete the original file and replace it with a clean copy.

P

Payload Defines extent of damage caused by a virus.

Port Interface of a computer from where an application or physical devices connect.

Protocol Formal set of conventions governing the formatting and relative timing of message exchange between two communicating systems.

POP (Post Office Protocol) Protocol used to retrieve e-mails from a mail server. Most e-mail applications (sometimes called an e-mail client) use the POP protocol, although some can use the newer IMAP (Internet Message Access Protocol).

Password Secret series of characters that enables a user to access a file, computer, or program. Password can be a combination of numbers and alphabets in a random sequence.

Polymorphic Virus Creates varied copies of itself to avoid detection from anti-virus software. Some use different encryption schemes and require different decryption routines. So the same virus may look completely different on different systems or even within different files. Other polymorphic viruses vary instruction sequences and use false commands to mislead anti-virus software. Some use mutation-engines and random-number generators to change their virus code and decryption routine.

Program Infector Infects other program files after an infected application is run.

Q

Quarantine To move an infected file, such as a virus, into an area where it cannot cause more harm. Antivirus software's come with quarantine options so that the user also can keep track of virus activity.

R

Register Storage device capable of receiving and holding a number of digits

Real-time Scanner An anti-virus software application that operates as a background task. Computer continues working at normal speed.

Resident Virus Loads into memory and remains inactive until a trigger event occurs like date or time. When this event occurs the virus is activated. All boot and file viruses are of this type.

Removal Measure of skill level needed to remove the threat. The three levels are difficult (requires an experienced technician), moderate (requires some expertise), and easy (requires little or no expertise).

Rogue Program Malicious program intended to damage programs or data, or to breach system security. It includes Trojans, logic bombs, viruses etc.

S

Scalable Allows to be changed in size or configuration to suit changing conditions. For example, a scalable network can be expanded from a few nodes to thousands of nodes.

Self-encrypting Virus Conceal themselves from anti-virus programs. Most anti-virus programs attempt to find viruses by looking for certain patterns of code (known as virus signatures) that are unique to each virus. Self-encrypting viruses encrypt these text strings differently with each infection to avoid detection.

Self-garbling Virus Attempts to hide from anti-virus software by garbling its own code. When these viruses spread, they change the way their code is encoded so anti-virus software cannot find them. A small portion of the virus code decodes the garbled code when activated.

Signature A search pattern, often a simple string of characters or bytes, expected in every instance of a particular virus. Usually, different viruses have different signatures. Anti-virus scanners use signatures to locate specific viruses.

Sparse-infecter Virus Uses conditions before infecting files. Examples include files infected only on the 12th execution or files of 128kb.

Stealth Virus Conceal their presence from anti-virus software. Many stealth viruses intercept disk-access requests, so when an anti-virus application tries to read files or boot sectors to find the virus, the virus feeds the program a "clean" image of the requested item. Other viruses hide the actual size of an infected file and display the size of the file before infection. Stealth viruses must be running to exhibit their stealth qualities.

Subject of e-mail Indicates the subject line of the email sent by the worm.

Synchronous Transmission Transmission in which data bits are sent at a fixed rate, with the transmitter and receiver synchronized.

SMTP (Simple Mail Transfer Protocol) Protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application.

Spam Electronic junk mail, junk newsgroup postings or unsolicited mail.

T

TCP/IP (Transmission Control Protocol/Internet Protocol) – Also known also as the Internet protocol suite. Combines both TCP and IP. Widely used applications, such as Telnet, FTP and SMTP, interface to TCP/IP.

Technical Description Describes technical details of the virus such as registry entry modifications and files that are manipulated by the virus.

Threat Assessment Gives severity rating of the threat. Includes damage that the threat causes, how quickly it can spread and how widespread the infections are known to be (wild).

Threat Containment Measure of how well current Anti virus technology can keep the threat from spreading. The measures are Easy (the threat is well-contained), Moderate (the threat is partially contained), and Difficult (the threat is not currently containable).

Time Bomb Malicious action triggered at a specific date or time.

TOM (Top of Memory) A design limit at the 640kb-mark on most PCs. Often the boot record does not completely reach top of memory, thus leaving empty space. Boot sector infectors often try to conceal themselves by hiding here. Checking the TOM value for changes can help detect a virus. The value can change for non-viral reasons also.

Trojan Destructive program that masquerades as a benign application. Unlike viruses, Trojans do not replicate themselves but they can be just as destructive. One of the most insidious types is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

TSR (Terminate and Stay Resident) TSR programs stay in memory after being executed. Allow user to quickly switch back and forth between programs in a non-multitasking environment, such as MS-DOS. Some viruses

are TSR programs that stay in memory to infect other files and program.

Tunneling Virus technique designed to prevent anti-virus applications from working correctly. Anti-virus programs work by intercepting the operating system actions before the OS can execute a virus. Tunneling viruses try to intercept the actions before the anti-virus software can detect the malicious code. New anti-virus programs can recognize many viruses with tunneling behavior.

U

User Name Name used to gain access to a computer system. Usernames, and often passwords, are required in multi-user systems. In most such systems, users can choose their own usernames and passwords.

UNC (Universal Naming Convention) Is the standard for naming network drives. For example, UNC directory path has the following form:
\\server\microworld\subfolder\filename.

Unix worm Takes advantage of flaws in networking code called buffer overflows to gain unauthorized access to remote computers running Unix.

V

Vaccination Technique of some anti-virus programs to store information about files in order to notify user about file changes. Internal vaccines store the information within the file itself, while external vaccines use another file to verify the original for possible changes.

Variant Modified version of a virus. Usually produced on purpose by the virus author or person amending the virus code. If changes to the original are small, most anti-virus products will also detect variants. If the changes are major, the variant may be undetected by anti-virus software.

Virus Program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Virus Signature A unique string of bits, or the binary pattern, of a virus.

The virus signature is like a fingerprint in that it can be used to detect and identify specific viruses. Anti-virus software uses the virus signature to scan for the presence of malicious code.

Vulnerability Characteristic of a system that will allow someone to keep it from operating correctly, or that will let unauthorized users take control of the system.

W

WAN (Wide Area Network) Network that typically spans nationwide distances and usually utilizes public telephone networks.

WinSock (Windows Socket) Is an Application Programming Interface (API) for developing Windows programs that can communicate with other machines via the TCP/IP protocol. Windows 95 and Windows NT comes with Dynamic Link Library (DLL) called winsock.dll that implements the API and acts as the glue between Windows programs and TCP/IP connections.

Wild Measures the extent to which a virus is spreading. Asses number of independent sites and systems infected, geographic distribution of infection, ability of current technology to combat the threat, and the complexity of the virus. When a virus has attacked an external system it is termed as being 'in the wild'.

Worm A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

X

XML (Extensible Markup Language) A specification developed by the W3C. XML is a pared-down version of SGML, designed especially for Web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.

Y

Yankee Doodle Type of memory resident virus. Plays the tune Yankee Doodle when activated.

Z

Zombie A computer that has been implanted with a daemon that puts it under the control of a malicious hacker without the knowledge of the computer owner. Zombies are used by malicious hackers to launch DoS attacks. The hacker sends commands to the zombie through an open port. On command, the zombie computer sends an enormous amount of packets of useless information to a targeted Web site in order to clog the site's routers and keep legitimate users from gaining access to the site. The traffic sent to the Web site is confusing and therefore the computer receiving the data spends time and resources trying to understand the influx of data that has been transmitted by the zombies.

Zoo Collection of viruses used for testing by researchers.

Zoo Virus Exists in the collections of researchers.