

This document provides information to install and use eScan Anti-Virus

eScan Anti Virus User Guide

eScan Anti-Virus User Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Document Number : 5BESAV/17.12.05/8.x

Copyright Notice

Copyright (C) 2006. All rights Reserved.

Portions (C) by Kaspersky Labs International Limited.

Any technical documentation that is made available by MicroWorld is the copyrighted work of MicroWorld and is owned by MicroWorld.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and MicroWorld makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user.

Documentation may include technical or other inaccuracies or typographical errors. MicroWorld reserves the right to make change without prior notice.

No part of this publication may be copied without the express written permission of MicroWorld.

Trademarks.

MicroWorld, MicroWorld Logo, eScan, eScan logo, MWL, MailScan are trademarks of MicroWorld.

Windows is a registered trademark of Microsoft Corporation; Kaspersky is a registered trademark of Kaspersky Labs.

All product names referenced herein are trademarks or registered trademarks of their respective companies. MicroWorld Software Services Pvt. Ltd. (MicroWorld) disclaims proprietary interest in the marks and names of others. Although MicroWorld makes every effort to ensure that this information is accurate, MicroWorld will not be liable for any errors or omission of facts contained herein. MicroWorld Software Services Pvt. Ltd. reserves the right to modify specifications cited in this document without prior notice.

Companies, names and data used in examples herein are fictitious unless otherwise noted.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MicroWorld Software Services Pvt. Ltd.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Technical Support: support@mwti.net

Sales: sales@mwti.net

Printed : MicroWorld

Jan, 2006

Table of Contents

Welcome	6
Documentation	7
How this guide is organized	8
Contact Us	9
About MicroWorld	10
MWL Technology	11
eScan Products Suite and Features	Error! Bookmark not defined.
Features of eScan	13
Getting Started	14
Screen Components	14
On Demand Scanner (ODS)	15
Status	16
Virus Monitor	16
Automatic Updates	16
Date of Virus Signatures	17
Last Computer Scan	17
Actions	17
Check Memory & Registry	18
Check Computer	18
Check Floppy disk	19
Scheduler	20
Job	21
Analysis Extent	22

Schedule	22
Virus Check	23
Log	23
Options	24
Virus Check	24
Alert	28
Restrictions	29
eScan Monitor	31
Functions and Features	31
How to start, disable and enable your eScan Monitor	31
Monitor System Menu	32
eScan Monitor Settings Interface	33
Main window	33
Menu	34
Work-area	34
Objects, Options, Customize and Statistics categories	35
Buttons	35
Changing Settings	36
Object monitoring settings	36
General Settings: Options	42
Advanced Settings: Customize	43
Previewing Settings before the Monitoring	44
Disabling and Enabling eScan AV Monitor	45
Loading, disabling and enabling eScan AV Monitor	45
Working with Settings' Tree	45
What is Settings' tree	45
Working with Settings' tree	46

Control Types	47
Check box	47
Text field	48
Input field defining the path to...	49
Input field defining the number of ...	49
Drop-down list	50
Control Indicators	51
Control indicators	51
Heuristic checking tool (Code Analyzer)	52
Index	55

Welcome

MicroWorld Content Security and Anti-Virus products, provide a blanket, round-the-clock security screen against viruses delivered into your PC or network. After the software is installed it is always active. You can 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.

eScan Content Security and Anti-Virus application is delivered in Six modules:

eScan for Windows: Provides an On Demand Scanner (ODS) to quickly scan your system for virus and other threats.

eScan Anti-Virus Monitor: Provides an Anti-Virus engine to scan and protect your system against virus and other threats.

eScan Updater: Allows you to download updates to detect and remove new viruses.

Content Administrator: Allows you to set security policies to permit or prohibit specific type of content from being accessed.

eScan Management Console. Allows you to remotely configure and administer the eScan network, installed on multiple clients.

eScan Remote Administrator Tool : Allows you to remotely administer the eScan server using a Web-browser.

Documentation

eScan user guides are provided in four books. Each book covers a specific module(s). Following table provides details of the user guides and the eScan product for which they are provided.

Manual Name	Description	eScan Products covered
eScan Quick Reference Guide	Instructions to install eScan products and a quick reference guide for all modules.	Common guide for all eScan products.
eScan Anti Virus User Guide	Instructions to use eScan ODS and AV Monitor.	Common guide for all eScan products
eScan Content Security User Guide	Instructions to use Content Administrator and eScan Updater	Provided for eScan Corporate and eScan for Proxy Servers
Management Console User Guide	Instructions to use eServ also called as eScan Management Console	Provided for eScan Corporate and eScan for Proxy Servers

How this guide is organized

This guide is organized into separate chapters.

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

Getting Started Gives a list of key symbols and their functions.

eScan On Demand Scanner (ODS): ODS allows you to scan your system, registry, files, directories when needed. This chapter explains key features of On Demand Scanner and how to use them to protect your system from virus and other threats.

eScan AV Monitor: eScan is built using the powerful MWL technology. MWL turns eScan into a powerful anti-virus engine that detects and removes known and unknown viruses. This chapter gives information about different features of the eScan AV Monitor and explains how to use them.

Contact Us

We offer 24x7 support to our customers through e-mail, telephone and Chat.

Chat Support

Chat with our support team at 'escanchat' using: AOL; MSN or Yahoo messenger service.

E-Mail Support

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

<p>Head Office:</p> <p>MicroWorld Technologies Inc. 33045 Hamilton Court East, Suite 105 Farmington Hills, MI 48334-3385 USA Tel: (248) 848 9081/9084 Fax: (248) 848 9085</p>	<p>Asia Pacific:</p> <p>MicroWorld Software Services Pvt Ltd.. Plot No 80, Road 15, MIDC, Marol, Andheri (E), Mumbai, INDIA. Tel (91) - 22- 28265701 - 05 Fax (91) - 22-28304750</p>
--	---

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

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

About MicroWorld

MicroWorld is one of the leading solution providers in the areas of content security and Anti-Virus products. With its corporate head quarters in MI, USA and development center in Mumbai, India, we offer round-the-clock support, through our regional offices and over 10,000 channel partners spread across the globe. This section provides information about eScan. Details about its features, how to use it; what to do when you have a virus etc is given.

eScan 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.

eScan 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

eScan Products

Features of eScan

MWL Technology

Our products are built on the **MicroWorld Winsock Technology** (MWL) (patent pending). This technology gives MicroWorld 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 analysis 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.

MicroWorld 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 setup eScan to automatically connect to these sites, download updates and run them on your system.

eScan Products Suite and Features

Feature	Web& Mail Filter	eScan AV	eScan VC	eScan Pro	eScan ISS	eScan Corp	eScan WSS *	eScan TSS **	eScan Enterprise	eScan SBS 4.5/2000	eScan Proxy ##
MWL Scanning	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Real-Time AVScanning	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Auto Attachment Compression	✓	-	✓	✓	✓	✓	✓	✓	✓	✓	-
Block offensive mails	✓	-	✓	✓	✓	✓	✓	✓	✓	✓	-
Block Spam	✓	-	✓	✓	✓	✓	✓	✓	✓	✓	-
Real-time email Scan	✓ #	-	✓	✓	✓	✓	✓	✓	✓	✓	-
NetBIOS Firewall	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
HTTP Scanning	✓	-	-	✓	✓	✓	✓	✓	✓	✓	✓
Block sites with restricted words	✓	-	-	✓	✓	✓	✓	✓	✓	✓	✓
Auto Updates	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Block Content(Multi-media& Applications)	✓	-	-	✓	✓	✓	✓	✓	✓	✓	✓
Block Applets, cookies, scripts	✓	-	-	✓	✓	✓	✓	✓	✓	✓	✓
Privacy Protection	✓	-	-	-	✓	✓	✓	-	✓	✓	✓
Block Pop Ups	✓	-	-	-	✓	✓	✓	-	✓	✓	✓
Warning Messages	✓	-	✓	✓	✓	✓	✓	✓	✓	✓	-
Management Console	-	-	-	-	-	✓	✓	✓	✓	✓	✓
MailScan Lite	-	-	✓	✓	✓	✓	✓	-	-	-	-
SpyWare & KeyLoggers	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓ \$
MailScan Full Version	-	-	-	-	-	-	-	✓	✓	✓	-
eScan RemoteAdmin	-	-	-	-	-	✓	✓	✓	✓	✓	✓
View TCP Toolkit	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Max Users	UNL	50	50	50	50	UNL	25	25	UNL	UNL	UNL
Supported OS	WKS	WKS	WKS	WKS	WKS	SRV WKS	SRV WKS	SRV WKS	SRV WKS	SRV WKS	SRV WKS
Recommended For Use @	Home	Home	Home	Home	Home	Lan/ Wan	SME	SME	Enterprise Networks	SBS Server	Proxy Server

* **WSS**: eScan Corp for SME ** **TSS**: MailScan (Except MailScan for SMTP) + eScan Corp
UNL – Unlimited User License **SME** – Small/ Medium Enterprise

Proxy Servers : MS ISA Proxy Server, WinRoute Proxy Server, WinGate Proxy Server
Platform Class : SRV – Server Class OS -> WinNT/ Win2000 / Win2003
WKS – WorkStation OS -> Win9x/ NT WorkStation/ Win2k Pro/ WinXP

VC: Virus Control **Pro**: Professional **ISS**: Internet Security Suite **Corp**: Corporate **WSS**: WorkGroup Security Suite **TSS**: Total Security Suite
Content and attachment only, mails will not be scanned for virus **\$** Enterprise networks with FileServers, Desktops & MailServers

Features of eScan

The main features and tasks eScan does for you are:

Content Security: Checks and blocks e-mails and websites for restricted content.

E-mail Content Scanning: Checks the e-mail body for confidential data (specified keywords, phrases, etc.) 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.

Parental Control: eScan auto blocks access to porn, gambling & other sites that have harmful content. You can specify restricted words like xxx, sluts, etc. that should be blocked. Any web page with such words is blocked.

Easy to Manage and Control: Easy to manage and control with features such as automated installation, centralized deployment, automatic downloads of updates.

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

eScan Remote Administrator Tool : Allows you to remotely administer the eScan server using a Web-browser.

Fast Updates reduce download time: eScan 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 download 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. It also scans mails sent through SMTP.

Messaging Options: eScan 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.










Network Monitoring : Allows to view active connections over TCP and UDP



MicroWorld AntiVirus Toolkit Utility : Provides inbuilt Spyware/ Adware/ Keylogger scanner.

Access to these modules depends on the version of eScan you are using.

Getting Started

Screen Components

Screen Component	Function
 Status	Allows you to view status of On Demand Scanner (ODS) activity.
 Actions	Allows you to run ODS tasks.
 Scheduler	Allows you to schedule ODS to scan your system at a predetermined time.
 Log	Provides a log of ODS activity.
 Options	Offers choice of Advanced Tuning for Virus check, Alert & Restriction
	Checks your computer memory and registry
	Checks and remove viruses from your floppy.
	Checks your for computer viruses.
	Checks specific files and directories for viruses.

Screen Component	Function
	Link to MicroWorld website for information on the latest viruses
	Access the online help

On Demand Scanner (ODS)

On Demand Scanner is a module of eScan that helps you to immediately scan your system for viruses and other threats. It also has the **eScan Anti-Virus Toolkit** that allows you to scan your system and registry files for memory resident viruses.

Status



Select **Status**. This menu provides the Status of anti-virus activity in your system. Status is given about the following:



Virus Monitor

Virus Monitor acts like a shield for your system against all virus and other threats. When such threats appear, they are detected and the application runs the actions you have specified. The Virus Monitor should always be enabled.

This section allows you to specify type of scanning and actions to be taken when viruses are detected.

Automatic Updates

MicroWorld technologies stores the latest anti-virus vaccines, also called Updates, on dedicated mirror download sites. These are available for free downloads. You can configure your system so that it connects to the sites automatically at a fixed time and downloads updates.

Updates are typically a few KB in size and take just a few seconds to download. The feature should be always active.

To download automatic updates, click **Automatic Update**.

A screen "Should the virus signature be updated now" is displayed. Click Yes.

Updates are downloaded and run on your system. A status bar showing download progress is displayed.

Date of Virus Signatures

Virus signatures are details of viruses. eScan needs to have this information, so that it knows which vaccine to use when a virus is detected. Date of the last virus signature downloaded is displayed here.

Last Computer Scan

This link shows last time the computer was checked for viruses. If you surf regularly, then your system must be scanned at least once everyday after downloading Anti-Virus updates


To begin scanning, double click the link or click **Last Computer Scan**. A screen asking you if you want your system to be scanned for viruses is displayed. Click **Yes**.

Statistics giving details of the scanning activity are displayed in the frame *Statistics*.

To stop scanning, click **Cancel**.

Actions



Click  The Virus Check screen is displayed. You can select objects to set them up for scanning. The objects that can be scanned are explained in the next sections.

eScan allows you to detect and clean viruses from your system, specific folders and files, floppy and zip drives and even CD ROMs. In the case of CD ROMs, since it is read only, it is possible to only detect viruses and you cannot remove them.



Check Memory & Registry

To check your systems memory and registry, click  **Check memory & registry** and **Start**.

Scanning of your system memory & registry is started. The frame **Objects Scanned** shows names of scanned files. The frame **Results**, show scanning results.

Select **Log** to see details of files scanned. To stop scanning, select **Cancel**.

Check Computer

To check your computer for viruses, click  **Check computer** and **Start**.

Scanning of your system is started. The frame **Files Scanned**, shows the files scanned. The frame **Results**, show scanning results.

Select **Log** to see details of files scanned. To stop scanning, select **Cancel**.

Check Floppy disk

To check your Floppy or Zip drives for viruses, click



Check floppy disk

and **Start**. Scanning

of your floppy/ Zip disk is started. The frame **Files Scanned**, shows the files scanned. The frame **Results** shows scanning results.

Select **Log** to see details of files scanned. To stop scanning, select **Cancel**.

Check CD ROM

To check your CD ROM for viruses, click



Check CD-ROM

and **Start**. You are asked a CD

into the drive. Scanning of your CD ROM is started. You can only check for viruses from CD ROMs but cannot remove any detected viruses.

Scanning of your system is started. The frame **Files Scanned**, shows the files scanned. The frame **Results** shows scanning results.

Select **Log** to see details of files scanned. To stop scanning, select **Cancel**.

Check directories/files



Check directories/files

Click **Start** To select the objects for scanning. The Screen Directory and file selection is displayed.

Click the files and folders to be scanned and click Add. The selected objects are displayed in the lower frame Selected Folders & Files.

Click on any item in the lower frame and click Scan. Scanning of the object is started.


Detailed scanning statistics are displayed in the frame Statistics. To stop scanning, click Cancel.

To remove an object from the selected folders and files list, click on the item and click Remove.

Scheduler

eScan allows you to set a schedule to auto scan your system at any hour or day. This feature ensures that periodic scanning is done and even if you forget to scan, eScan will do the work automatically. If you need to go elsewhere for a short while from your system (lunch break) you can schedule the scan



during this time. To set a schedule for scanning, click . The Automatic Virus Check screen is displayed.

A list of schedules, already created is displayed on the screen. Schedule name, time when it should start, when it is next due and the last time the schedule was run are displayed.

To immediately start scanning, using the settings of the listed schedule, select the schedule and click Start now.

To edit the settings for a schedule, select the schedule and click Edit. Screens displaying previously assigned values are displayed. You can change all the values except the job name.

To create a new schedule, click **"Add New Task"**. The Automatic Virus Check screen is displayed.

This contains four tabs and they are explained in the next sections.

Job

This tab allows you to assign a name for the schedule. Following table gives names of different fields.

Field Name	Field Description
Name	Enter a name for the schedule
Active	To enable the schedule select the checkbox. If you don't want the schedule to run then unselect the checkbox.
Start Type	<p>There are two types of scanning. Select the radio button for the required type.</p> <p>Start in foreground Runs analysis in the foreground. The task becomes the primary one on your system. This option allows you to monitor the scanning activity.</p> <p>Start in background Runs analysis as a background task. Your other computer tasks continue to run. MicroWorld recommends you select this option.</p>
Quit	<p>You can specify what should be done when viruses are detected. Select the appropriate value from the drop down. This drop down is enabled only if you select <i>Start in background</i> radio button.</p> <p>Never quit automatically After analysis is over; the application asks your permission before closing the window.</p> <p>Do not quit if virus is detected If viruses are detected, the application will not close the process for your response, but will proceed as per other selected options.</p> <p>Always quit After scheduled analysis is complete eScan will close the application</p>

Analysis Extent

This tab allows you to specify what objects should be scanned in the schedule. You can either choose to scan your systems hard drives or specify files and folders to be scanned – fields are

Check local hard drives: System hard drives and all folders and sub folders are scanned.

Check following directories and files You can select specific files and folders to be included in the schedule. Click the adjacent browse button. Make the selections as explained and click **Ok**. The selected files and folders are displayed in the bottom display box.

Schedule

The tab allows you to set the time when auto scanning should be done. Features of the screen are:

Radio buttons in Execute frame allow you to specify the hour and minute for the scan to run Once, Hourly, Daily, Weekly, Monthly and With system startup.

Spin buttons allow you to set the hour in the Time frame. Based on the radio button selected in the Execute frame, additional buttons are displayed in the Time frame.

Virus Check

This screen allows you to specify what should be done when infected files are detected, set the priority for scanning, specify file types that should be scanned and select settings that should be followed during scanning.


Details are explained in Virus Check. Only one field is different in this screen.

Calculate analysis extent before checking: Allows you to calculate the time required for the scheduled job to run.


Click **OK** to accept the settings. The new job is listed in the main Schedule screen.

Log

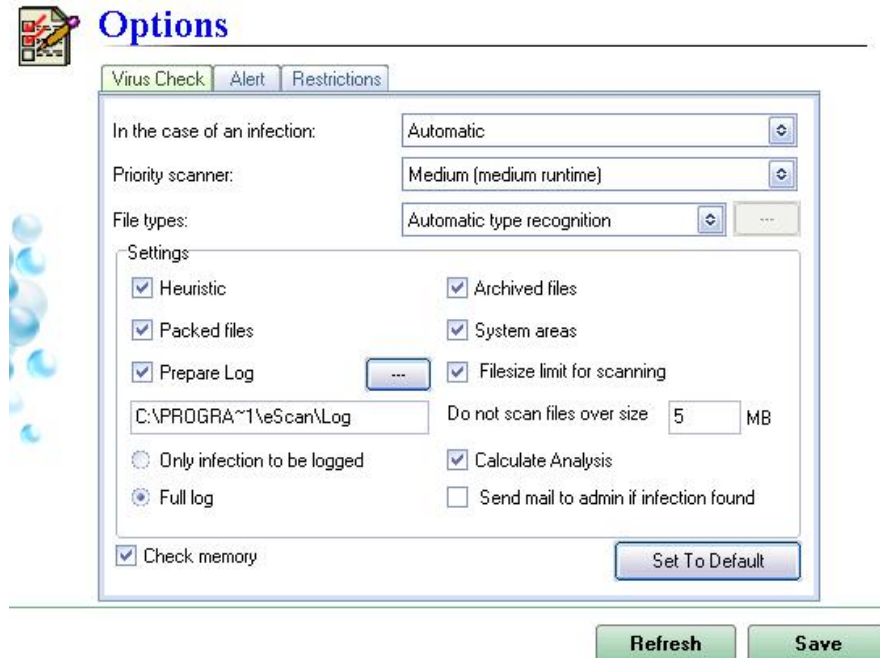


eScan provides a detailed Log of anti-virus activity. Click  to view the Records screen. Details of eScan version, files and folders scanned, etc. are displayed.

Options


Select . The *Options* dialog box is displayed.

Virus Check



This screen allows you to specify what should be done when infected files are detected, set the priority for scanning, specify file types that should be scanned and select settings that should be followed during scanning. Fields are explained in the following table.

Field	Description
In case of an infection	<p>You can specify what should be done when virus infected files are detected. Drop down box displays the actions and you can make a suitable selection:</p> <p>Automatic: Default value. eScan takes automatic action for infected files.</p> <p>Prompt Required Action: eScan displays a message asking you what should be done for the infected file.</p> <p>Log only: Details of the infected file with the file name and path are stored in the logs. No other action is taken and scanning of other files continues.</p> <p>Disinfect (if not possible, rename file): eScan tries to disinfect the infected file. If this is not possible, then the file is renamed. This prevents infection from spreading.</p> <p>Disinfect (if not possible, delete file): eScan tries to disinfect the infected file. If this is not possible, then the file is deleted.</p> <p>Rename infected file: eScan renames the file without trying to disinfect it.</p> <p>Delete infected file: eScan deletes the file without trying to disinfect it.</p>
Priority Scanner	<p>Allows you to set the priority for scanning. Drop down allows you to set the priority:</p> <p>Medium (medium runtime)</p> <p>High (short runtime)</p> <p>Low (long runtime)</p>
File types	<p>You can select the types of files that should be scanned. File types are specified by their extensions like .doc, .xls. Choose the appropriate value from the drop down list.</p> <p>Automatic Type recognition: Scans all file headers irrespective of file</p>

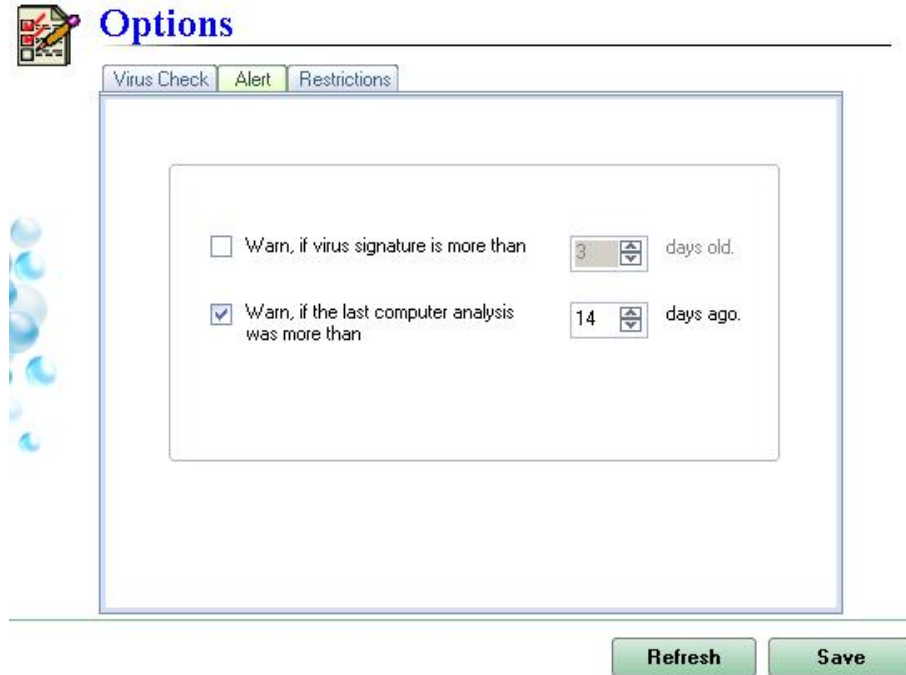
Field	Description
	<p>extensions.</p> <p>Only program file: Scans all executable files with .COM, .dll and .EXE extensions.</p> <p>User defined: You can specify new files types. Adjacent  button is enabled only when “User defined” is selected. User defined file types dialog box is displayed. Box is used to add new file types for scanning. There are two boxes for selecting the file type. Lower frame, lists selected file type. Enter the file type extension in the upper frame and choose Add.</p> <p>The name appears in the lower box. To change or delete the entry, select the name. It appears in the upper frame. Delete unwanted entries using the Remove button. Select OK.</p>
Settings	<p>The frame allows you to select the objects that will be automatically scanned and also other actions. Names of the objects are given beside a check box. To select the object, click in the . The objects are:</p> <p>Heuristic: The system is checked for unusual sequence, pattern or content and when such files are detected, the software displays an alert message.</p> <p>Archived Files: Scans zipped files.</p> <p>Packed Files: Files that are zipped or archived.</p> <p>System Area: Scans system area. Includes disks, files and operative memory.</p> <p>Prepare log: A log of scanning activity is generated. This includes details of when the scan was run, infected file names and their path.</p> <p>Do not Scan files over size: You can set the maximum size of files in MB that need to be scanned. Files above this size are not scanned.</p> <p>Only Infection to be Logged: Log file entries of only infected files are made. This makes the file size smaller.</p>

Field	Description
	<p>Full Log: Detailed log files are created.</p> <p>Send mail to admin if infection found: An alert mail is sent to the network admin if any infection is found.</p> <p>Calculate Analysis: Calculates the extent of scanning to be done.</p>

Click **SAVE** to retain changes you have made or Refresh to discard them.

The tick mark against the Check Memory box is the default action and allows us to check System RAM for viruses. Click on the button "Set to Default" to restore all the settings to their original values.

Alert



eScan gives warning messages when virus signatures are not downloaded and if the system is not scanned as per the prescribed time. You can configure the settings in this screen.

You need to set period for two values. To set the time, click on the down or up arrow of the spin buttons.

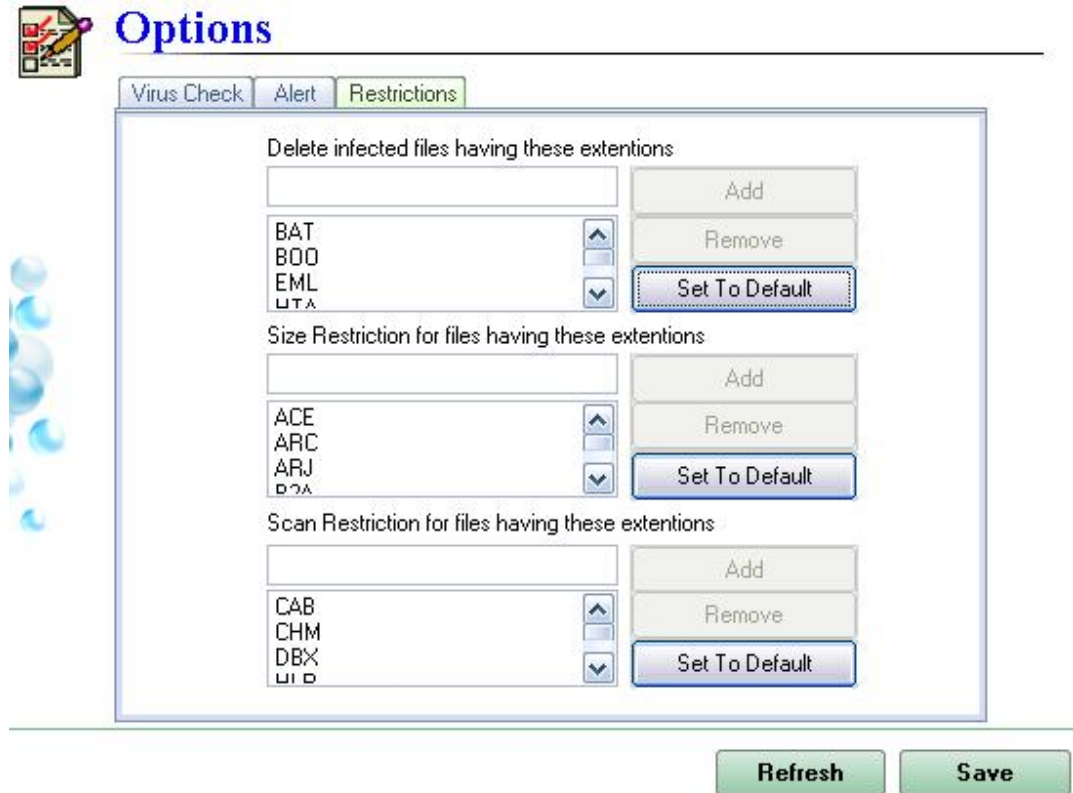
Warn, if virus signature is more than: It is strongly recommended that virus signatures be downloaded everyday. Each day sees more than 5 to 10 new viruses appearing. To make eScan effective, you must download signatures everyday. The signatures are just a few KB in size and take a few seconds to download.

Warn, if the last computer analysis was more than: If you access the Internet and download data everyday, then your system must be scanned everyday. Set the value as 1 to X days, depending on the

download frequency.

Click **SAVE** to retain changes you have made or Refresh to discard them.

Restrictions



The Restrictions tab allows you to specify file types that should be scanned and deleted if found having a virus. In the Restriction tab, you can specify the file types. Click **Save** to retain changes or **Refresh** to restore default settings.

Field	Description
Delete infected files having these extensions	You can add files types (e.g. .doc. .txt, etc.) that should be deleted if infected. To Add file types, enter the name in the field and click Enter.
Size Restrictions for files having these extensions	You can add files types (e.g. .doc. .txt, etc.) that should not be scanned if they are larger than the size in MB, specified in the Virus Check field.. To Add file types, enter the name in the field and click Enter.
Scan Restrictions for files having these extensions	You can add files types (e.g. .doc. .txt, etc.) that should not be scanned To Add file types, enter the name in the field and click Enter.

eScan Monitor

Functions and Features

eScan Anti-Virus Monitor (eScan Monitor) is a memory resident program that monitors files when these are accessed. Whenever somebody refers to an object, the monitor checks the object to make sure that it is free of viruses. If the object is found to be infected, the program will attempt to disinfect the object, delete it, move it to a quarantine folder or allow it to be accessed, depending on the options that were selected. This way the anti-virus monitor allows you to detect and delete viruses before the system is actually infected.

Here we must note that there are more than one term describing programs similar to the eScan anti-virus Monitor, for example, people call them resident scanners, or anti-virus filters, or on access scanners etc.

How to start, disable and enable your eScan Monitor


There are several ways to start your anti-virus monitor:

Using the **Windows Start** menu command.

From the **StartUp** menu (automatically).


From eScan Control Center (automatically).

By entering the appropriate command in the command line.

You can quickly start your anti-virus monitor using the appropriate Windows Start menu command. To do it, click the **Start** button on your Windows desktop, point to **Programs**, point to **eScan for Windows**, then click the **eScan Monitor** command. The monitor icon  will appear next to the clock on the Windows taskbar.


And finally, to start your anti-virus monitor from the command line, you must go to the **eScan** Anti-Virus directory and execute the file `avpm.exe`.


If your anti-virus monitor is enabled,

You can see the icon  next to the clock on the Windows taskbar.

When you place your mouse cursor on the icon , the following prompt will pop-up: **eScan Anti-Virus Monitor is enabled.**

If your anti-virus monitor is disabled,

You can see the icon  next to the clock on the Windows taskbar.

When you place your mouse cursor on the icon , the following prompt will pop-up: **eScan Anti-Virus Monitor is disabled**

The monitor system menu contains the following command: Enable Monitoring.

We do not recommend you to run two anti-virus monitors from different manufacturers on the same computer, because it may result in conflicts and false alarms.

Monitor System Menu

Right Click the green eScan client-updater/ Auto-updater Tray Icon -> Left click 'Monitor settings'
(Applicable only in case you have eScan Corporate or eScan for Proxy installed)

A menu appears showing the the following commands:

eScan Monitor Settings – Displays the program main window.





Disable/ Enable eScan Monitor– Disables/enables the program to monitor for viruses in files.

Unload eScan Monitor – to unload the Monitor from memory – the red shield icon vanishes

Set to default – Starts the anti-virus bases updating program.

eScan Monitor Settings Interface

Clicking on the eScan Monitor Settings in the Monitor Systems Menu displays the screen outlined below.

	Menu to select objects in eScan Anti-Virus Monitor
	Menu to set scan options in eScan Anti-Virus Monitor
	Menu to customize options in eScan Anti Virus Monitor
	Menu to get scan statistics of eScan Anti-Virus Monitor

It appears in each of two modes – Standard and Expert. The default mode is standard Mode wherein THREE Panes appear left to right.

In EXPERT mode an additional pane appears at the bottom right hand side of this screen. This mode allows for fine-grained control over the objects desired to be scanned (explained later).

Main window

The eScan Monitor main window allows you to change the monitor settings, to disable/enable the monitor and to view the performance statistics. You may exit the window without unloading the program out of your computer memory.

The eScan AV Monitor main window contains the following items:

Menu

Toolbar

Work-area

OK, Cancel, Apply and Help buttons.

Menu

At the top of the eScan Monitor main window you can see a *menu bar* with drop down menus. Some commands in these menus may be activated using appropriate key combinations or toolbar buttons. The key combination that may be used instead of a command is defined at the right of this command in the corresponding drop down menu.

Menu → command	Function (The menu command allows you to...)
File → Unload eScan Anti-Virus Monitor	unload eScan Monitor from the computer memory
File → Close window	close the eScan Monitor main window
Monitor → Enable monitoring / Disable monitoring	enable / disable the program to monitor for viruses
Monitor → View monitoring options	display your monitor settings in the form of a text
Help → Contents	display the Help topics window
Help → eScan Anti-Virus on the Web	start your web browser and take you to the MicroWorld website

Work-area

Work-area of the main window is divided into two frames. The left frame contains icons with the following names: **Objects**, **Options**, **Customize** and **Statistic**. The right frame displays settings that correspond to a left frame icon that is currently pressed.

The **Objects** frame allows you to define the locations and the objects that must be checked for viruses, and to specify how the monitor must process objects that have been defined as infected. All these settings are arranged into the special control—*objects' settings hierarchy*.

The **Options** frame allows you to define certain general settings, and you can use a *settings' tree* in the **Customize** frame to define advanced settings of your eScan Monitor.

The **Statistic** frame displays a table with the monitor performance statistics.

Every item of the settings' tree has a right-click menu with commands applicable to this certain item.

To display the right-click menu of an item in the settings' tree,

Place your mouse cursor on the required item.

Click your mouse right button. The appropriate right-click menu will appear on your screen.

Objects, Options, Customize and Statistics categories

The main window work-area is divided into two frames. The left frame contains icons with the following names: **Objects**, **Options**, **Customize** and **Statistics**. The right frame displays settings corresponding to a left frame icon that is currently pressed.

The **Objects** frame allows you to define a location to be checked (the list of drives and folders), objects to be checked (e.g. sectors, files, mail databases), and rules to be followed while handling the infected objects (see topic *Defining the location to be monitored*). All these settings are arranged into the special control—*objects' settings hierarchy*.

The **Options** frame allows you to define certain general settings, and you may use *a settings' tree* in the **Customize** frame to define advanced settings of your eScan Monitor (see topics *Reporting options*, *Renaming options*, *Advanced settings: Customize*).

The **Statistic** frame displays a table with the monitor performance statistics.

Buttons

At the bottom of the main window you can find the following buttons: **OK**, **Cancel**, **Apply**. Use these buttons to apply new settings or to cancel changes. Click the **Help** button to display the Help topics.

Changing Settings

Object monitoring settings

The **Objects** frame allows you to define the locations and the objects that must be monitored for viruses, specify how the monitor handles infected and suspicious objects and to enable/disable the advanced monitoring tools.

Defining the location to be monitored

The **Objects** frame in the work-area allows you to choose locations and objects to be monitored for viruses. You may do it by selecting appropriate options in the frame hierarchies. These options may be viewed in the following two modes: **Standard** and **Expert**. To switch between these modes use the corresponding buttons in the left frame of the window work-area.

With the Standard mode enabled the Objects frame is divided into two sub-frames: in the left sub-frame you may see the list of computer disks, and the right sub-frame displays settings for the item selected in the left sub-frame list.

With the Expert mode enabled the Objects frame is divided into three sub-frames: in the upper left sub-frame you may find the file-system hierarchy, the upper right sub-frame displays settings for the item selected in the upper left sub-frame hierarchy, and the lower sub-frame displays the list of files located in the root of the object selected in the upper left sub-frame. Besides in this mode the Network Neighborhood item is added to the file-system hierarchy.

Use the (upper) left sub-frame to define the location that must be monitored for viruses. Check a box to define the corresponding object as to be checked. If you uncheck a box , the corresponding object will be defined as to be skipped during the monitoring.

For the program to monitor for viruses in a location within your file system, you must check a checkbox at the left of the area name.

For the program to monitor a group of disks, check the My Computer box in the (upper) left sub-frame and the required check-box in the (upper) right hierarchy.

Scan local removable disk drives — monitors all removable disks. This checkbox is available, only

if you checked the My Computer box in the (upper) left sub-frame. For the same result you may check boxes of all your removable disks in the (upper) left sub-frame.

Scan local hard disk drives — monitors all local hard disks. This checkbox is available only if you checked the My Computer box in the (upper) left sub-frame. For the same result you may check boxes of all your local hard disks in the (upper) left sub-frame.

Scan network drives — scans all available network disks. This checkbox is available only if you checked the My Computer box in the (upper) left sub-frame. For the same results you may check boxes of all available network disks in the (upper) left sub-frame.

If you check a box of some certain location within your file system, boxes of all the locations included in the checked item will also be automatically checked. However, when in the Expert view mode you can mark the required sub-locations as to be excluded from the check.

For example, you defined the disks C: and D: as to be checked for viruses, but want the D:\public\archives directory to be excluded from the location defined as to be checked. In this case you must check the C: and D: check boxes, and then you must uncheck the archives box.

If you excluded a folder from the location defined as to be checked, a triangle will appear in the checked boxes of all the parent locations: instead of . If you excluded some location from the larger location that is defined as to be checked for viruses, it means that the monitor will not check it at all or will not check it using the rules defined for the parent location. You may eliminate (disable) this difference inside the larger location, or keep it for some certain period of time.

For every defined location within your file system you can specify separate monitoring settings. For every defined location-to-be-checked you can also specify the objects-to-be-checked by using the settings' tree in the right-hand pane.

Defining objects to be monitored

For locations that correspond to different levels of the file-system hierarchy the (upper) right frame displays different groups of settings. The maximum quantity of settings is displayed for the **My Computer** location. Here you can set your monitor to check your computer memory, boot sectors and groups of disks. When defining settings for a disk you can enable the check of boot sectors and file-system located on this disk. For a folder you cannot disable the check of file-system. But you can define how the monitor must process infected and suspicious objects, in what type of files it must check for viruses. You can also enable/disable the advanced monitoring tools to be used for all the locations in the (upper) left frame.

Scan files of following types — monitors files in the corresponding location (including System, Hidden and Read Only files). This check-box is available if you checked the My Computer or a disk box in the (upper) left sub-frame. You cannot uncheck it for a folder or file. If you checked this box, you must define file types to be checked for viruses:

All infectable — Monitors all files that are able to carry a virus.

All — Monitors each file.

By mask — Monitors the file types defined by user in the text fields below. You can specify the unlimited quantity of file types, but make sure that one text field contains only one file type.


Exclude by mask — excludes from checking the file types defined by user in the text fields below. You can specify the unlimited quantity of file types, but make sure that one text field contains only one file type.

Scan sectors — monitors boot sectors (Master Boot Record and boot sectors). This checkbox is available only if you checked the My Computer or a disk box in the (upper) left sub-frame.

Scan memory — Scans the memory. This checkbox is available only if you checked the My Computer box in the (upper) left sub-frame.

If you check the **Scan sectors** and **Scan memory** check boxes sectors and memory will be checked only once, when the monitoring is started. Besides, if you check the **Scan memory** check box the program will monitor for viruses in the memory of launched programs. eScan AV Monitor performs this check, right after it is loaded, and also every time you update your anti-virus databases. If the infected memory of a program cannot be disinfected, this program is forced to abort the program.

Handling infected and suspicious objects

 Actions in case of virus detection — in case of detecting the infected or suspicious objects, the program will perform one of the following actions.

Ask user — eScan AV Monitor will open up the **dialog box**. This dialog box contains a name of infected file, name of the detected virus and the list of possible actions to be performed with infected object, that is a list of all possible actions.

Besides, the appearing dialog box contains the Apply to all infected objects check box; by checking it, you can apply the selected action to all infected objects that will be detected later, and that you previously predefined as to be handled by opening the dialogue box. Then upon detecting the next infected object,

the dialog box will not appear again. The following two buttons are located at the bottom of this dialog box: OK (accepts the selected action), Cancel (closes the dialog box and proceeds with monitoring).

Report only — the program will only **report** the infected and suspicious objects. The check report can be viewed by starting the report viewer, MicroWorld Report Viewer.

Disinfect — the program will try to cure all infected objects without asking first. As a result, the detected viruses will be removed, and the object will be restored as an operable one.

Make backup file before disinfections — to create a copy of the infected object before starting a cure. A directory where the copy will be created is specified in a settings' tree of the Options category (see topic **Renaming options**). The copy will not be deleted upon completion of a treatment.

If disinfections is impossible — not all infected objects can be cured, because some viruses damage the computer data irreversibly. In this case, eScan AV Monitor can operate using one of the following three methods:

Report only— that is to inform about unsuccessful attempt of treatment, Rename object — that is to rename the unrecoverable file, Delete object — that is to delete the damaged file.

Rename object — the program will rename all infected objects. The renaming rules are specified in a settings' tree of the Options category.

Delete object— the program will delete all infected objects without warning.

The **Delete object** and the **Rename object** options are applied to infected archives, only if you checked the **Enable delete or rename non-disinfected archives** box on the **Options** page. Otherwise, if you select those options, the program will not delete or rename infected archives.

Advanced monitoring tools

Monitoring compound objects

You can enable the advanced monitoring modes to check for viruses in archives, packed files, mail databases, plain mail formats and embedded objects. All these modes are united in the following single branch of the settings' tree:

Scan compound files of the following types — check this box to process compound objects as folders containing a set of objects.

Monitoring archives and self-extracting files

It is absolutely essential for anti-virus software to be capable of checking archives. An infected file can stay in an archive for a long time, even years, with the virus inactive and therefore invisible to you, but when the day comes that you extract this file the virus may break loose and destroy your system.

Archives — check this box to search for viruses in files archived using ZIP, ARJ, LHA, RAR, CAB and some other archiving utilities.

MicroWorld Anti-Virus is not able to delete viruses from archives, it is able only to detect them. Besides, MicroWorld Anti-Virus does not extract password-protected archives.

Therefore, if you set your eScan AV Monitor to delete or rename infected objects, it is advisable that you check the **Archives** box and uncheck the **Enable delete or rename infected archives** box on the **Options** page. In this case the program will only report the infected file detected within an archive, but it will not delete or rename the archive itself. Later, you will be able to extract the archive and delete viruses from extracted files by using your eScan AV Scanner.

If the **Enable delete or rename infected archives** box is checked, you can lose data that can be recovered later.

Archives with self-extractors — check this box to search for viruses in self-extracting archives, i.e. executable files that can be started to extract the archived files. Some self-extracting archives also immediately start one of the extracted files.

The extracting tool is able to correctly extract files that have been compressed multiple times. It can also deal with some versions of immunizers, programs protecting executable files from viruses by attaching checking code blocks (CPAV and F-XLOCK) and enciphering programs (CryptCOM) to them.

Monitoring mail databases and plain mail files

The program is able to search for viruses in mail databases and plain mail files.

Mail databases — check this box to search for viruses in mail databases of the following formats.

Microsoft Outlook, Microsoft Exchange (the .pst and the .pab extension files, the MS Mail archive type).

Microsoft Internet Mail (the .mbx extension files, the MS Internet Mail archive type).

Eudora Pro & Lite.

Pegasus Mail.

Netscape Navigator Mail.

JSMail SMTP/POP3 server (user database).

If the mail database monitoring mode is enabled, eScan AV Monitor checks every entry in mail databases and scans attached files. The following formats are supported:UUEncode; XXEncode; btoa (up to 5.0); btoa 5.*; BinHex 4.0; ship; NETRUN 3.10; NETSEND 1.0 (not packed); NETSEND 1.0C (packed); MIME base64.

Plain mail— check this box to search for viruses in plain mail files of the formats: Eudora Pro & Lite, Pegasus Mail, Netscape Navigator Mail, JSMail, user database on the SMTP/POP3 server. If the plain mail check mode is enabled, MicroWorld Anti-Virus checks every file for message header. If the message header is detected, the program searches for attached data (UUEncode, XXEncode and etc.) and checks it for viruses.

The mail database and plain mail modes noticeably slow down the eScan AV Monitor performance rate. Therefore we do not recommend their use in a regular virus-monitoring.

Monitoring embedded objects

The program allows you to check for viruses not only in files, but also in the objects embedded to these files using the OLE technology.

Embedded objects — check this box to search for viruses in OLE objects embedded in the examined files.

Heuristic detecting tool

You can enable the built-in **heuristic detecting tool** to scan for viruses that are unknown to the program (they are not described in current anti-virus bases).


Enable Code analyzer— check this box to monitor for viruses using the heuristic detecting tool.


General Settings: Options

General settings: Options

The **Options** frame contains options allowing you to choose how the monitor should report the performance statistics and rename the infected files it detected.

Reporting options

 **Save report file** — check this box to save the report to a file. If you check the box, you will be able to monitor the performance of eScan AV Monitor using MicroWorld Report Viewer. When displaying the performance results, this program will use settings defined in the Save report file branch.

 **Report file name** – use this field to define the report file name. By default the report file is created in a directory that you specified during the program installation. If the program is not launched from eScan AV Control Centre, you can re-define this directory by specifying the full path to your report file. If the program is controlled by eScan AV Control Centre, you cannot re-define this directory.


Show pack info in the report — check this box to be reported about packed and archived objects. These messages have the following format in the eScan Report Viewer table: the Object column shows the object name, the Result column shows the Packed or Archive strings and the Description column shows a name of the corresponding compressing or archiving utility.


Show clean object info in the report — check this box to be reported about virus-free objects. These messages have the following format in the eScan Report Viewer table: the Object column shows the object name, the Result column shows the OK string.


Append — check this box to append new reports to the existing report file. This is useful if you want to keep reports on several or all the previous checks. If the box is not checked, every time eScan AV Monitor is started it will create a new report file.

Limit size to (Kb) — check this box to limit size of the report file to the value specified in the below field. The default value is 2048 Kb

Renaming options

 **For renaming or copying of infected objects use** — these option buttons allow you to choose between moving infected objects to a special folder and renaming them. The program will apply this setting to those objects for which you selected the **Rename object** option in the **Objects** settings' tree.

 **Special folder** — this option button moves infected objects to a special directory defined in the below text field. In this case, infected objects are moved to the folder with their names and extensions unchanged.

 **The object folder** — this option button renames infected objects, i.e. changes their extensions for the one defined in the **Extension of infected file** field.

Enable delete or rename infected archives – check this box to allow the program to delete or rename infected archives. This check box is used only for those objects for which you selected the **Delete object** or the **Rename object** options (respectively) in the **Objects** settings' tree. It is not advisable to check this box, since you may lose data that can be recovered later.


 **Limit size compound files to (Kb)**
 50


Default limit of the compound file is 50KB

Advanced Settings: Customize

Advanced settings: Customize

The **Customize** frame contains options allowing you to define advanced settings of the program.

 **Use sound effects for the following events** — check this box to play sounds while monitoring for viruses.

 **Infected object found**— allows defining the sound file that is played every time an infected object is detected. While selecting files in the corresponding window you can use the Test button to listen to it.

Display attention messages — check this box to display other warning messages.

Check new updates — check this box to automatically start the anti-virus databases updating program on a regular basis. In the Check interval (days) dialog box, define the required interval between two automatic starts (the dialog box is displayed right after you checked this box).

If you are working with the program settings from eScan AV Control Center, you will not find some of the **Customize** settings. These settings make no sense, if you are using MicroWorld AV Control Center.

Previewing Settings before the Monitoring

Previewing settings before the monitoring

You can review your monitor settings in the form of a text. This kind of text describes rules specified for all the objects of your file system: from **My Computer** to separate files. For example, if the rules that your eScan AV Monitor uses to check and process the autoexec.bat file differs from those used for the parent object - System disk (C:), a list of these rules will be displayed separately.

To review the text describing your eScan AV Monitor settings, select the **View monitoring options** command from the **File** menu.

The **Monitoring Options** windows containing values of the **Objects** and **Options** settings will appear on your screen. You can view and copy the setting values. When you finished working with this window click **OK**.

The monitor settings in the form of a text are also recorded in the beginning of your report file.

Disabling and Enabling eScan AV Monitor

Loading, disabling and enabling eScan AV Monitor

You can manually load your anti-virus monitor from eScan AV Control Centre or from the eScan AV Monitor main window. You can also use eScan AV Control Centre to schedule your anti-virus monitor automatic start.

After the program is started to monitor for viruses you can disable it, and then resume the process.

	Main menu → command	System menu
Disabling	Monitor Disable monitoring	Disable monitoring
Enabling	Monitor Enable monitoring	Enable monitoring

Working with Settings' Tree



What is Settings' tree

The eScan Anti-Virus interface frequently uses the so-called Settings' tree which presents data in the form of a tree with conventional controls as joints (buttons, drop-down lists, checkboxes and etc.).

This technology provides the clear and easy-to-understand picture of interrelations between various settings and makes it easy to study the program.






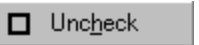
In this book, all the controls are illustrated by pictures. So that you could see how do they look like in the program windows.

Working with Settings' tree

Every joint of a settings' tree may have branches. If a branch is visible the corresponding joint looks similar to this , and if the branch is hidden the corresponding joint will change for .

To change some certain setting you must make its branch visible.

To display and hide a branch, use the following methods:

What to do	How it might be done (By using...)
To display a branch (joint looks like )	the key  on your keyboard. the command  from the right-click menu. the key "*" on your keypad (all branches of the joint become visible).
To hide a branch (joint looks like )	the key  on your keyboard. the command  from the right-click menu. the key "-" on your keypad (all branches of the joint disappear from your screen).


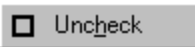
Control Types

Check box

A checkbox may be

- New directories** — unchecked meaning that this type of virus-monitoring will not be performed.
- New directories** — checked meaning that the program will perform this type of virus-monitoring.

To check and uncheck a box you must use the following methods:

What to do	How it might be done (by using...)
To check the box	the SPACE key on your keyboard. the command  from the right-click menu. your mouse to click on it.
To uncheck the box	the SPACE key on your keyboard. the command  from the right-click menu. your mouse to click on it.

Text field

To edit value of the **text field** you must use your keyboard. You may see the text field current value enclosed with angle brackets at the right of the field name.

 New Value — the text field.

To edit a text field value use the following methods:

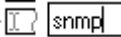
What to do

How it might be done (by using...)

To edit the field value

your mouse to click on the field icon.


the command  from the right-click menu.

the F2 key on your keyboard. The text field will change its appearance for: 

After you finish editing the text field value press the **ENTER** key on your keyboard or click with your mouse outside of this text field. You can cancel changing this text field and return to the previous value by pressing the **ESC** key on your keyboard.

Input field defining the path to...


To edit value of the **path field** you must use the conventional Windows dialog allowing to select the directory or file.

 D:\Program\Kaspersky Lab\Kaspersky Anti-Virus Inspector — the path input field.

To edit a path field value use the following methods:

What to do	How it might be done (by using...)
------------	------------------------------------


To edit the field value	your mouse to click on the field icon.
-------------------------	--

the command  from the right-click menu.

the F2 key on your keyboard.

Input field defining the number of ...

To input new value in the **number field** you must type it in from your keyboard or use the cursor controlling keys to change the current value. You may see the number field current value enclosed with angle brackets at the right of the field name.

 if larger then <180> kb. — the number input field.

To edit a number in the field use the following methods:





What to do	How it might be done (by using...)
------------	------------------------------------

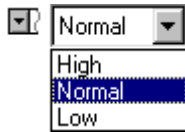
To edit the field value	your mouse to click on the field icon.
-------------------------	--

the command  from the right-click menu.

the F2 key on your keyboard.

Drop-down list

Drop-down list allows you to select one of the items from this list. To browse the list you must use the  and  keys on your keyboard. To automatically scroll down/up the list you must use the **CTRL+**  and **CTRL+**  key combinations.



Drop-down list

Control Indicators

Control indicators

When setting your anti-virus to check for viruses in the disk hierarchy (see topic [Defining the location to be monitored](#)) you must use the so-called Rules of Succession, i.e. if you define some settings for the **My computer** item, they will be automatically assigned for all disks on your computer.

Every item of the hierarchy is associated with a *control indicator* (that can be enabled or disabled) and *rules* (applied to this item). A control indicator indicates whether the corresponding hierarchy item must or must not be checked for viruses, and the rules describe methods that will be applied when handling this item.

All the hierarchy items by default *inherit rules of the group* these are included in. If you change the rules to be applied to a group, the group item rules will change either.

You can assign independent rules to an item or change status of its control indicator. These items may *have independent rules*. If you change the rules to be applied to the group, these items will keep their processing rules. However, by changing the group indicator status you can restore these items as inheriting the group rules.

By selecting the Set Strict command from the right-click menu you can completely disable the rule-inheriting mode for the selected item. If you select this command, the corresponding control indicator will look like a red box with a black tick inside. Items with indicators in this condition have *strictly independent rules* assigned. These items will keep their rules even after you change the group indicator status. To restore these items as inheriting the group rules, you must select the Remove Strict command from the right-click menu.

The control indicator may look similar to the following:

Looks like	Description	Meaning
<input checked="" type="checkbox"/>	A square with a tick inside. The square may be red or black.	The check mode is enabled. The square is red – the inheriting mode is disabled. The square is black – the inheriting mode is

		enabled.
<input checked="" type="checkbox"/>	A square with the tick inside and the triangle in the right-bottom corner. The triangle may be red or black.	<p>The inheriting mode is enabled, but some objects are excluded from the group and have their own settings.</p> <p>The triangle is red – for one or more objects the inheriting mode is disabled.</p> <p>The triangle is black – for one or more objects the rule is changed.</p>
<input type="checkbox"/>	A square without the tick and with the triangle in the right-bottom corner. The triangle may be red or black.	<p>The check mode is disabled, but for one or more objects this mode is enabled.</p> <p>The triangle is red – for one or more objects the inheriting mode is disabled.</p> <p>The triangle is black – for one or more objects the rule is changed.</p>

Heuristic checking tool (Code Analyzer)

The heuristic detecting tool (Code Analyzer) checks file and sector codes down the various MicroWorld Anti-Virus algorithmic legs searching for virus-similar instructions (such as - to open a file, to write into it, to intercept the interrupt vectors or etc.) and generates appropriate alerts.

Of course, just like any other of the type the heuristic algorithm may occasionally produce false alarms, however Code Analyzer has been tested many times and checked a large number of files, and has not so far been actually deceived. If you do encounter a false alarm while checking files using Code Analyzer, please let us know and send us copies of the virus free files that were identified as infected so that we could study them at MicroWorld

When scanning a code the heuristic detecting tool examines the structure of a program down to several sub-levels. This device detects 92 % of the viruses (including many encrypted ones) in the MicroWorld's database, and we believe that new viruses that aren't yet in the database will be detected with the same degree of probability.

The current version of *Code Analyzer* does not remove viruses from files and sectors that are identified as suspicious. To remove a new virus from a file refer to a system programmer or directly to the anti-virus

support department of MicroWorld.

The Code Analyzer alerts' format is the following:

Suspicion: <TYPE>

where <TYPE> is replaced by one of the following strings:

Com — the file seems to be infected by a virus that infects .COM files;

Exe — the file seems to be infected by a virus that infects .EXE files;

ComExe — the file seems to be infected by a virus that infects both .COM and .EXE files;

ComTSR, ExeTSR, SysTSR, ComExeTSR — the file seems to be infected by a resident virus that infects .COM, .EXE and .SYS files;

Boot — the file/sector seems to be infected by a boot virus or looks like a boot virus installer;

Trojan — the file looks like a Trojan;

Trivial — the file seems to be infected by an unknown virus replacing executable files in a current directory by its own codes (usually the virus size doesn't exceed 300 bytes);

HLL — the file seems to be infected by an unknown virus infecting executable files. The virus is written in a high-level programming language (C, Pascal);

Win32 — the file seems to be infected by an unknown Windows virus;

Formula — the Excel file contains suspicious instructions;

Macro.Word97.Fs — the file seems to be infected with a Macro.Word97.Fs family virus.

RemoteTemplate — the document contains a link to the template which is automatically loaded when the file is opened;

HTML.SecurityBreach.2 — the HTML file or the HTML message is linked to a suspicious object;

IRC-Worm.generic — the file seems to be infected by an unknown worm transmitting itself via the IRC channels;

BAT — the file seems to be infected with an unknown virus infecting BAT files;

VBS.I-Worm — the file seems to be infected by an unknown worm transmitting itself with email messages.

Index

A

About MicroWorld, 10
Actions, 17
Active/inactive, 16
Administrator, 13
advanced monitoring modes, 39
advanced settings, 43
advanced tasks, 8
All subfolders, 24
ANALYSIS EXTENT, 22
Archived Files, 24
attachment, 8
Automatic, 13
Automatic Type, 24
Automatic Updates, 16

B

buton, 35

C

categories, 35
CD ROMs, 17
check box, 47
CHECK CD ROM, 18
CHECK DISK, 19
Checks, 10, 13
Code, 13
code analyzer, 52, 53
Common Installation Process, 8
Computing, 8
Contact Us, 9
Content-, 6, 8, 10, 12, 13
Content Control, 8
Content Scanning, 13
Control, 13
control indicators, 51
customize, 35, 43

D

Daily, 22
Details, 8, 10
detect, 13
development, 10
disable, 31
drop-down list, 50
DVD, 18

E

enable, 31
eScan Corporate, 8, 12
eScan Management Console, 8,
12
eScan Products, 10, 12
eScan Server, 13
exchange, 6
eScan Rad,6

F

Features of eScan, 13
field, 48, 49
FLOPPY, 19
Frequently Asked Questions, 8

G

Gateway, 10
general settings, 42
Get eScan Status, 16
Getting Started, 8, 14
Glossary, 8

H

Help, 13

Heuristic, 13
heuristic tool, 39, 52
Hourly, 22
How this guide is organized, 8

I

ID, 13
Include subfolders, 24
incremental, 13
indicators, 51
infected object, 38, 39
input field, 49
Installation, 8
Internet traffic, 13

L

Last Computer Analysis, 16, 17
launch, 31
launching monitoring, 45
load, 45
location to be monitored, 36

M

main window, 33
Management, 10, 13
menu, 32, 34
monitor, 45
Monitor System, 8
monitoring, 36, 37, 38
monitoring compound objects, 39
monitoring tools, 39
Monthly, 22
MWL, 8, 10
MWL Technology, 10

N

New, 10, 20

number field, 49

O

objects, 35, 36, 37
Once, 6
options, 35, 36, 42, 43, 47
Our Asia Pacific office, 9
Our Head Office, 9

P

Packed Files, 24
path field, 49
preview settings, 44
Priority Scanner, 24
Prompt Required Action, 24

R

real-time, 10
Records, 8
renaming objects, 43
renaming options, 43
report, 42
remote administration ,6

S

Safe Computing, 8
sales enquiry, 9
Schedule, 22
SCHEDULE VIRUS CHECK, 23
Scheduler, 20
Services, 9
settings, 35, 36, 42, 43, 44, 46
settings' tree, 45, 46
Simple, 13
solution, 10
start, 31
Startup., 22
statistics, 35
STATISTICS, 17, 19
STATUS, 28
Support, 8
suspicious object, 38
System Area, 24

T

terminating monitoring, 45
text field, 48
Time, 22
Timeframe, 22
tree, 45, 46

Tcp connction ,13

U

Updates, 8, 10, 13, 16
User-defined, 24

V

View Records, 8
Virus Check, 24
Virus Monitor, 16
VIRUS SIGNATURE, 17
VIRUSES, 17
View TCP,13

W

Weekly, 22
Winsock, 8
work area, 34

Z

ZIP, 19