



**This document provides information to install and use
eScan Anti-Virus for Linux Server**

User Guide

eScan Anti-Virus for Linux Server

eScan Anti-Virus User Guide for Linux Server

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 : LINODS/8.06.04

Copyright Notice

Copyright (C) 2004. All rights Reserved.

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, MailScan are trademarks of MicroWorld.

Red Hat, Red Hat Press, and the Red Hat Press logo are trademarks or registered trademarks of Red Hat, Inc. Linux is a trademark or registered trademark of Linus Torvalds.

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 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

August, 2004

Table of Contents

Welcome	5
CONTACT US	6
About MicroWorld	7
FEATURES OF eSCAN FOR LINUX SERVER	8
Getting Started	9
SCREEN COMPONENTS	9
On Demand Scanner (ODS)	11
OPTIONS	11
VIRUS CHECK	11
STARTUP	14
UPDATE	14
LOG	15
MONITOR	16
SETTINGS	16
ACTIONS	17
TARGETS	18
Status	19
Actions	20
CHECK SELECTED DIRECTORIES/FILES	20
CHECK ALL HOME DIRECTORIES	21
CHECK COMPUTER	21
CHECK RUNNING PROCESSES	22
Scheduler	23
ADD	23
JOB NAME	24

ANALYSIS.....	24
SCHEDULE.....	24
VIRUS CHECK	25
EDIT	25
DELETE	26
Log	27
Index	28

Welcome

The increasing use of Linux as an alternate operating system has increased the number of viruses targeting Linux machines. eScan for Linux Server provides protection for Linux based Servers from viruses. The software works as an 'on-demand' scanner and you can execute it as and when you need to scan a file or directory. This document provides information to use eScan for Linux Servers.

This guide is organized into separate chapters.

[About MicroWorld](#): Provides overview of MicroWorld. 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, files, and 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.

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.

Head Office: MicroWorld Technologies Inc. 33045 Hamilton Court East, Suite 105 Farmington Hills, MI 48334-3385 USA Tel: (248) 848 9081/9084 Fax: (248) 848 9085	Asia Pacific: 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
--	---

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 headquarters in New Jersey, 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 for Linux operating systems. Details about its features, how to use it, what to do when you have a virus, etc is provided.

The increasing use of Linux as an alternate operating system has increased the number of viruses targeting Linux machines.

eScan for Linux Servers checks removable drives and files for viruses. 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 automatically downloads Updates from our download site.

Features of eScan for Linux Server

The main features and tasks eScan does for you are:

Detects Viruses on Demand: Protects applications and Operating Systems by detecting viruses when you want.

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

Comprehensive Object Management: eScan understands different file types, compression formats and data streams




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.











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.

Screen Components

Typical screen components are explained below:

Screen Component	Function
	Allows you to view status of On Demand Scanner (ODS) activity.
	Allows you to run Virus Checks .
	Allows you to Schedule Scan Settings to scan your system at a predetermined time.


Screen Component	Function
	Provides a log of ODS activity
	Exits from the application
	Checks selected directories or files
	Checks specific home directories for viruses
	Checks your system for viruses
	Checks your running process, system memory
	Allows you to set options for virus checks like type of scanning action to be taken when infected files are detected.
	Provides a quick link to the MicroWorld website where information about the latest viruses is available.
	Access the online help.
	Provides information about MicroWorld Technologies Inc. the creator of eScan for Linux.

On Demand Scanner (ODS)

On Demand Scanner 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 files for memory resident viruses.

Options



- Select . The *Options* dialog box is displayed. There are four tabs that allow you to set scanning options

Virus Check

This screen allows you to specify action to be taken 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 the action to be taken when virus infected files are detected. Drop down box displays the actions and you can select a suitable action:</p> <p>Automatic: Default value. eScan takes automatic action for infected files.</p> <p>Prompt Required Action: eScan displays a message asking you what to do with 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, Skip): eScan tries to disinfect the infected file. If this is not possible, then the file is skipped.</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 disinfecting it.</p>

Field	Description
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 the checkbox. The objects in the screen are:</p> <p>Packed Files: Files that specially compressed executables created to reduce file size.</p> <p>Mail Databases: Scans the database of your mail server</p> <p>Recursive: Scans directories and their sub directories recursively</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>Plain Mail Files: Scans mails in plain text format</p> <p>Unknown Virus Modifications: Scans files that are probably modified after viruses infected them</p> <p>Cross File System: In Linux you have different file systems mounted at different location. Crossing the file systems means checking files on different partitions and/or network mounted file systems.</p> <p>Self Extracting Archived File: Scans files that are of self extracting type.</p>

Field	Description
Symbolic Links	<p>Symbolic links allow you to access one file from another through links. There are options to scan such files:</p> <p>All: Checks all symbolic files</p> <p>Specified: Checks specified linked files</p> <p>None: No checks done for linked files.</p>

- Click **Ok** to save changes you have made or **Cancel** to discard them.

Startup

The startup tab allows you to specify attributes that should be run or displayed on the eScan screen at startup.

Alert if Virus Definitions are: You can select the number of days after which, if updates are not downloaded, an alert is displayed.

Do a Scan of ALL Running Processes at Startup: At startup, all processes that are running are checked for memory resident and other viruses.

Update

MicroWorld technologies stores the latest anti-virus signatures 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.

Field	Description
Update Server	Enter the server path from which updates are downloaded
Use Proxy	If you use a proxy to download updates, select the check box. Enter the IP of your proxy server and the port number. If User Authentication is needed, then enter the user name and password. A screen asking you to authenticate the entry is displayed.

Log

This Log menu allows you to specify the path or location where the Log of anti-virus activity is stored.

The screen also allows you to assign the monitor log file name and its location.

You can also set a level from 0 to 3.

Monitor

This screen has three tabs that allow you to configure monitor settings.

Settings

This screen allows you to configure the following settings:

Field	Description
Cache Size	Enter the cache size in KB that should be allocated from the system resources to the application.
No. of Threads	Enter the maximum number of mails that should be scanned simultaneously.
Maximum File Size	Enter the maximum file size in bytes. Files below this size will not be scanned.
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 the checkbox. The objects in the screen are:</p> <p>Archived Files: Scans zipped and archived files.</p> <p>Mail Databases: Scans the database of your mail server</p> <p>Packed Files: Files that specially compressed executables created to reduce file size.</p>

Field	Description
	Heuristic: The system is checked for unusual sequence, pattern or content and when such files are detected, the software displays an alert message.
	Unknown Virus Modifications: Scans files that are probably modified after viruses infected them Plain Mail Files: Scans mails in plain text format Self Extracting Archived File: Scans files that are of self extracting type.

Actions

This screen allows you to configure the following scan actions:

Field	Description
Quarantine	Select the check box to quarantine suspicious files.
Quarantine Location	Enter the location for quarantined files.
Exclude Mask by	Mask means the file extension like .doc or .txt. Select the check box to exclude specific file type from scanning.


Field	Description
Exclude Masks	You can specify the file extensions that should not be scanned. Enter the name in the field and select Add .

Targets

This screen allows you to specify the directories to be included or excluded from scanning.

Field	Description
Include Directories	Select the directories to be included in scanning. Click the Browse button, select the directory and click Add .
Exclude Directories	Select the directories to be excluded in scanning. Click the Browse button, select the directory and click Add .

Status

This menu provides the Status of anti-virus activity in your system. Click .

Status is given about the following items:

Engine Version: Displays version number of eScan for Linux currently running on your system.

Date of virus signature: Date when last virus signature was downloaded.


Virus Count: Total number of viruses that can be detected and removed by the last virus signature

Reload Virus Signatures: Virus signatures are loaded/reloaded in the AV engine

Manual Update: Allows you to manually download updates.


Actions

eScan allows you to detect and clean viruses from your system, specific directories 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.

- Click  and Start
- 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.

Check selected directories/files

You can scan a specific files or directory using this option. To select and scan a specific

file or directory, click  .

- A dialog box showing your directory structure is displayed. Expand the nodes and select the file or directory to be scanned.
- Click Done. The selected item is scanned for viruses.

Check all home directories


You can scan all the home directories. Home directories are specific to a user. Only the administrator of the machine can alter the system files.

- Click . The **Scan Process** screen is displayed.

The scan process box is displayed and it shows statistics like total number of files scanned, total number of files disinfected, deleted, and renamed. The total number of errors is also shown.

Check Computer

This menu allows you to scan your system for viruses.


- To check your computer for viruses, click  and **Start**. Scanning of your system is started.

The scan process box is displayed and it shows statistics like total number of files scanned, total number of files disinfected, deleted, and renamed. The total number of errors is also shown.

The lower frame lists the infected file name, its path and the status.


Check running processes

This menu allows you to check your system, memory and processes running in the background for memory resident and other viruses.

- To check your system memory click  and **start**.
- The eScan Anti-Virus Tool Kit is run. Starts scanning of your system. The frame **Files 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**.

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 carried out 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 Schedule Scan Settings 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 delete a schedule, select the schedule from the list and click **Delete**.
- To create a new schedule, click **Add**. The Automatic Virus Check screen is displayed.
- To edit a schedule, select the schedule and click **Edit**.

Add

You can add a new schedule to scan your system at a predetermined time. Adding a schedule is done by entering information in different tab pages. You begin with assigning a name for the schedule and specifying hard drives, directories and files for scanning. Next you need to select the time when the scanning should start and specify what types of files should be scanned.

The tab pages are explained in the next sections:

Job Name

This tab allows you to assign a name for the schedule. Enter a name for the schedule. After you save the entries, the name is listed in the Schedule screen.

Analysis

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 directories to be scanned

Fields are:

Check local hard drives: System hard drives and all directories are scanned.

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

Schedule

The tab allows you to set the time when auto scanning should be started. 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, or Monthly.

- 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 the action to be taken when infected files are detected, set the priority for scanning, specify file types that should be scanned.

Fields are explained in [Virus Check](#).

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

Edit

After the schedule is created, it is listed in the screen. To edit a schedule, select the schedule and click **Edit**.

Screen displayed while adding a schedule are displayed with values filled in. You can edit values for all the fields. Only the schedule name cannot be edited.

The four tabs are:

Job Name: Schedule job name is displayed in the non-editable field.

Analysis: For details, please refer [Analysis](#).


Schedule: For details, please refer [Schedule](#).

Virus Check: For details, please refer [Virus Check](#).

Delete

This link allows you to delete a schedule listed in the Schedule Scan Settings page. To delete a schedule, click on the schedule and select **Delete**.

Log

eScan provides a detailed Log of anti-virus activity. Click  to view the Records screen. A list of logs is displayed giving the file name, date the log was generated and the file size.

There are two buttons:

View: Select a name from the list and click **View** to view the log.

Clear: Select a name from the list and click **Clear** to remove it from the list.

Index

A

About MicroWorld, 7
Actions, 20
Active/inactive, 19
All subfolders, 11
Analysis Extent, 24
At, 14
Automatic Updates, 14

C

Check CD ROM, 21
Check directories/files, 21
Check disk, 20
Contact Us, 6
Copyright Notice, 2

D

Daily, 24
Default, 12
Definitions, 14
Details, 7, 12

Disinfect, 12

F

features, 5, 8
**Features XE "features"
of eScan, 5, 8**

G

Getting Started, 5, 9

H

Hourly, 24

M

Monthly, 24

N

New, 23

O

Once, 24
Options, 11

Overview, 5

P

Processes, 14

S

sales enquiry, 6
Save, 25
Schedule, 9, 23, 24, 25
Schedule Virus Check, 25
Screen Components, 9
Services, 2, 6
Startup, 14
Status, 19

U

User, 1, 2, 15

W

Weekly, 24