

# White Paper eScan for Linux Server

eScan for Linux (eScan) is a real-time virus scanning software for workstations and servers running on Linux. It offers a complete and reliable anti-virus security solution that detects and removes over 1,00,000 viruses, Trojans and other threats. This white paper explains the key features of eScan for Linux Servers and demonstrates how it detects and removes viruses.

#### Is a Anti-Virus solution needed for Linux

About 90% of the viruses today enter the organizations via Internet and through emails. The only solution is to provide a software application that works in real-time and is intelligent enough to detect and remove viruses.

There is a false feeling of security that Viruses do not infect Linux systems. To a certain extent this is true since in the architecture of Linux systems, the 'Root' or administrator owns the Programs and other users in a Linux network use the non-privilege account.

But many Linux users use Open Office for word processing and import documents created in MS Word. In some cases Linux machines directly connect to Windows machine and exchange files. Script and macro viruses can be present in the documents and while they may not harm Linux machines, they can find a safe haven and remain hidden there. When Linux users transfer or mail such documents to Windows based machines, the viruses are launched.

# **Features of eScan for Linux Servers**

#### Features of eScan for Linux Server:

- Real-time Intelligent Monitor to guard your system
- Configuration and management through a web interface
- Ability to scan files automatically as they are modified and closed in real time
- Quarantine the infected filed
- Skip scanning of files with specified extensions
- Scans files in real time with the specified include directories
- Exclude scanning files in real time with the specified exclude directories
- Command line scanner for automation and scheduling
- Automatic and manual download of updates

# eScan for Linux is available for Workstations and Servers. The server version has a web interface also.

Screenshots of key features and their brief explanation are given in the next sections for both versions of eScan for Linux Servers.



#### **Monitor Options**

eScan for Linux Servers has a feature called the **Monitor** which allows you to configure settings like the cache size, number of threads (files) that can be scanned simultaneously and set the maximum size up to which files should be scanned. You can also Quarantine infected files. Other features include setting the quarantine path and excluding files with specific masks (like .pdf, .txt) from scanning. Monitor allows you to exclude specific directories from scanning.

This menu is available only for eScan for Linux Servers.

Set cache size, numl Max file size f	
• Options	
Virus Check     Startup     Update       Settings     Actions     Targets       Configuration     Cache Size (256 - 1000) :     No Of Threads (2 - 5):       Maximum FileSize (0 - 1000)     No Of Threads (2 - 5):	1000 \$ 5 \$
Settings Archived Files Packed Files Unknown Virus Modific Self Extracting Archived	
	Apply Save Cancel

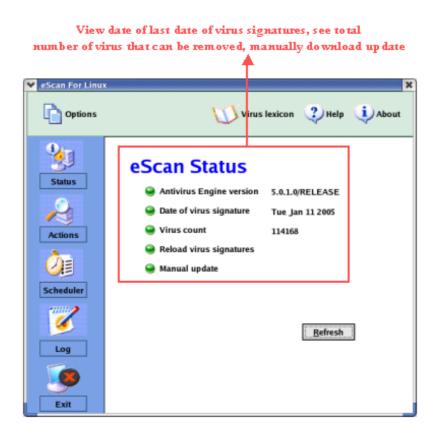
Select file types that should be scanned



	Settings	Acti	ions	Monitor
Status				
	Configuration			
Monitor		Cache Size (In KB)	1000	
a		Number Of Threads (2-5)	5	
<b>1</b>		Maximum File Size (In KB)	0	
eScan				
	Settings			
Logs		Packed Files	🔽 Mail Database	
		Heuristic	Archived Files	
· · · · · · · · · · · · · · · · · · ·		Plain Mail Files	Self Extracting Ar	chived Files
Help		🔲 Unknown Virus Modificatio	n	
Logout		Activate C	hanges Reset	

#### eScan Status

eScan for Linux Servers has a menu that gives important information such as the date when virus signatures were downloaded, anti-virus engine version and the total number of known virus that can be detected and removed.

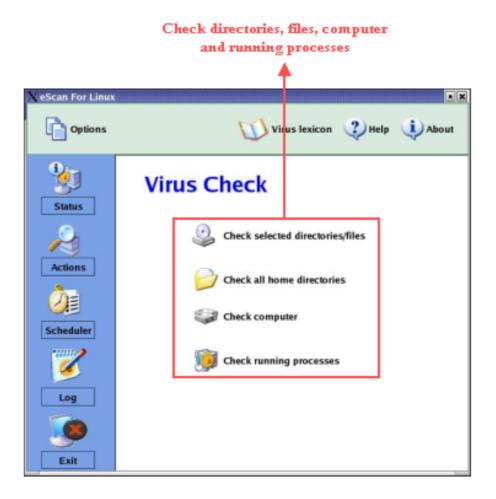




#### **Virus Scanning Features**

#### SCANNING FILES AND DIRECTORIES

eScan allows you to select different objects in your system and scan them for viruses. You can select and scan any directory or file, your whole computer, directories in your system and also running process for memory resident viruses





#### SET ACTIONS FOR INFECTED FILES

.

When infected files are detected, you can set the action to be taken. The actions that can be preset include rename the infected file, disinfect the file and if that fails, either rename or delete the file, etc.

You can select specific file types for scanning. Different file types like packed, mail databases, archived, plain mail, self-extracting archived files, etc. can be selected.

rus Check	Startup	Update	Log		
n the case o	of Infectior	Delet	le Infected	I	•
settings					
Packe	ed Files		🗹 Ma	il Database	s
Recu	rsive		🗹 Her	uristics	
🗹 Archi	ved Files		🗹 Pla	in Mail File	s
🗹 Unkn	own Virus	Modificatio	n 🗹 Cro	ss File Sys	stems
🗹 Self E	Extracting /	Archived Fi	le		
Symbo	lic Links I	○ Specifi	ed O	None	
				_	Gancel
			Apply	<u>Save</u>	

Select file types to scan and set scan options



	Settings	Virus Definitio	n Updates	Schedule	?
Status					
	Virus Checks:				
Monitor		In Case Of Infection	Automatic		
R -	Settings				
		Packed Files	🗖 Mail Database		
eScan		Recursive	Heuristic		
<b>E b</b>		🔽 Archived Files	🔽 Plain Mail Files		
<u> </u>		🔽 Unknown Virus Modification	🔽 Cross File System		
Logs		🔽 Self Extracting Archived Files			
Help	Symbolic Links	C All	C Specified	<li>None</li>	
<b>3</b>	Alert If Virus Definition Are 1	5 Days Old.			
Logout	🔽 Do a Scan Of All Running Pro	ocesses At Startup.			
		Activate Char	nges Reset		



# **Download Updates**

Each day sees new viruses appearing. Updates are vaccines that detect and remove new viruses. The software must have the means to identify new viruses and remove them. Updates are available as free downloads from our mirror download sites. eScan can be configured to connect automatically to these sites and download updates.

-	ownload status			
Update				
Download Progress:				
Lowinoau Piogress.				
	11%			
File Progress:				
	21%			
Files Done:	7/26			
Bytes Done:	455086/3800572			
Current File:	avp0406.avc			
rile status:				
krnmacro.avc: OK		•		
krnengn.avc: OK krndos.avc: OK		_		
smart.avc: OK		-		
	<b></b>			
	<u>U</u> p date	<u>C</u> ancel		



The same settings can be done with the **web interface**:

<b>-</b>	Settings	Virus Definition Updates	Schedule	2
Status				
	Update VIRUS Definition Databases:	Update NOW!		
Monitor	🗹 Auto Update Databases	Auto Update Schedule Time:	Hour Mins	
4 Contraction of the second se	Send Update Notification To:		<b>T</b>	
eScan		http://ftp.microworldsystem.com/linu	n (undeter	
Logs	List of Update Servers:	nttp://ttp.microworldsystem.com/ inu	x/updates	
<b>P</b> Help		Activate Changes Reset		
<u>.</u>	☐ HTTP/FTP Proxy Server for Updates:	Proxy Address: Proxy Port:		
Logout	Proxy Server Authentication Info:	Username:		
		Password:		
		Activate Changes Reset		



## Auto Scan Schedule

You can set a schedule to automatically scan your system at a preset time. You can also set the actions that should be run when virus infected files are detected.

ob Name Analysis	Schedule	Virus check	ĸ		
Execute     Once     Hourly     Daily		<ul> <li>Weekly</li> <li>Monthly</li> </ul>			
Month: 6	Date: 29	<b>•</b>	Time:	20:56	~

Select time to run scan schedule



	Settings	Virus	Definition Updates	Schedule	2
Status					
Monitor		Name Fi	equency Date Time Objects		
Geo		,	Delete		
eScan					
Logs	Job Name	[			
Logs					
<b>P</b> Help	Objects To Be Checked				
<u></u>	Execute				
Logout		Once	C Weekly		
		C Hourly	C Monthly		
		C Daily			
	Date 1	Month 1	Hour 0	Minutes 0	



## View eScan Log

eScan generates a comprehensive log of scanning activity. The log shows date and time when scanning was done and path of objects scanned. You can also view the scan report. There are three log levels: 0 level logs all scanning activity, 1 level logs only infected files and scan report, 2 level logs only scan report.

Vie	w Lo	gs										
Tu	e lur	1 29	20:5	3:35	20041	Sca	nnina	Proces	s File:	/usr/b	in/evol	u F
[Tu	e Jur	1 29	20:5	3:35	2004]	Sca	nning	Proces	s File:	/usr/b	in/evol	4
[Tu	e Jur	1 29	20:5	3:35	2004]	Sca	nning	Proces	s File:	/usr/b	in/evol	a
[Tu	e Jur	1 29	20:5	3:35	2004]	Sca	nning	Proces	s File:	/usr/b	in/evol	u
[Tu	e Jur	1 29	20:5	3:35	2004]	Sca	nning	Proces	s File:	/usr/b	in/ssh	
[Tu	e Jur	1 29	20:5	3:35	2004]	Sca	nning	Proces	s File:	/usr/b	in/ncftp	e.
[Tu	e Jur	1 29	20:5	3:35	2004]	Sca	nning	Proces	s File:	/opt/M	licroWo	я
[Tu	e Jur	1 29	20:5	3:35	2004]	Sca	nning	Proces	s File:	/usr/s	bin/ssh	d
[Tu	e Jur	1 29	20:5	3:35	2004]	Sca	nning	Proces	s File:	/usr/s	bin/ssh	d
[Tu	e Jur	1 29	20:5	3:36	2004]	Sca	nning	Proces	s File:	/bin/b	ash	
Tu	e Jur	1 29	20:5	3:36	2004]	Sca	nning	Proces	s File:	/usr/b	in/man	
Tu	e Jur	1 29	20:5	3:36	2004]	Sca	nning	Proces	s File:	/bin/b	ash	
Tu	e Jur	1 29	20:5	3:36	2004]	Sca	nning	Proces	s File:	/bin/b	ash	
Tu	e Jur	1 29	20:5	3:36	2004]	Sca	nning	Proces	s File:	/usr/b	in/less	
[Tu	e Jur	1 29	20:5	3:36	2004]	Sca	nning	Proces	s File:	/home	/vikash	1/
Tu	e Jur	1 29	20:5	3:36	2004]	Sca	nning	Proces	s File:	/tmp/E	Eqt	1
[Tu	e Jur	1 29	20:5	3:36	2004]	Sca	nning	Proces	s File:	/opt/M	licroWo	n.
[Tu	e Jur	1 29	20:5	3:36	2004]	Sca	nning	Proces	s File:	/opt/M	licroWo	1
•					-111						3	



<b>A</b>	Escan I	Logs	Monitor Logs	Update Lo	gs (
Status	Log Location	/var/MicroWor	rld/var/log/escan/	Log Level	2 💌
Monitor			Activate Changes		
400			Refresh		
eScan		[Thu Jan 13 17:54:44 2005] [Thu Jan 13 17:54:44 2005] [Thu Jan 13 17:54:44 2005] [Thu Jan 13 17:54:44 2005] [Thu Jan 13 17:54:44 2005]	/opt/MicroWorld/var/www/htdocs/escan/filter /opt/MicroWorld/var/www/htdocs/escan/contr /opt/MicroWorld/var/www/htdocs/escan/contr /opt/MicroWorld/var/www/htdocs/escan/REAI /opt/MicroWorld/var/www/htdocs/escan/REAI /opt/MicroWorld/var/www/htdocs/escan/actio /opt/MicroWorld/var/www/htdocs/escan/Actio	ol_checks.php OK he_pb.gif OK ol_about.php OK DME OK n.php OK	
Logout		[Thu Jan 13 17:54:43 2005]	/opt/MicroWorld/var/www/htdocs/escan/AV_s /opt/MicroWorld/var/www/htdocs/escan/AV_ /opt/MicroWorld/var/www/htdocs/escan/AV_s	ustomalerts.php OK	

# **System Requirements**

- Red Hat Linux 9 or higher should be installed on the system.
- 40 MB of free disk space

### Contact us

For details, please visit	www.mwti.net
For sales enquiries	sales@mwti.net
For support	support@mwti.net